Contents lists available at ScienceDirect

Forensic Science International: Synergy

journal homepage: www.sciencedirect.com/journal/forensic-science-international-synergy

Interpol review of digital evidence for 2019–2022

Paul Reedy

4th Street Global, USA

1. Introduction

When compiling the digital evidence review for 2019–2022, the first thought that came to mind was “we have come so far … we have so far to go”. There has been considerable progress in the field over the past three years and the twenty years before that, but there is still a long way to go.

This review cites approximately 260 references that were published from late 2019 until as recently as possible prior to November 2022. Although this is not an exhaustive list, some of the journals from which articles were drawn include:

- Forensic Science International: Digital Investigation and its predecessor Digital Investigation
- Forensic Science International: Synergy
- Forensic Science International
- Indian Journal of Law and Technology
- IEEE various proceedings, for example Fuzzy Systems
- Concurrency Computation Practice and Experience
- Journal of Parallel and Distributed Computing
- Journal of Information Security and Application
- International Criminal Law Review
- Journal of Cybersecurity and Digital Forensics
- Journal of Digital Forensics, Security and Law
- Etc.

A small minority articles have been included with which, as the reviewer, I disagree. Such articles have been included as they do contribute to the knowledge in the field and the field is strengthened with a range of views. In short, the primary reason for which I disagree is the author(s) has/have paid insufficient regard to the forum in which the output of the digital forensics process is ultimately assessed and in which decisions are made. The court of law is the forum in which the facts are determined and from which essential feedback is provided to the field and to the practitioners. While testimony in both written and oral forms might be technically correct, the ability of the expert to accurately convey that testimony in an understandable form with an appropriate weighting is occasionally given insufficient attention. It is my hope that those continuing to work in the field both in operational and academic roles are mindful of this in their future endeavours.

There has been a substantial change and development in the field over the three years of the review. The previous (2016–2019) review included seven broad topics, whereas the current (2019–2022) review includes nine topics. Notably, the previous seven topics have been absorbed into two of the topics in the current review. (See Fig. 1)

Some notable observations of the current review include:

- digital forensics, now increasingly being referred to as digital forensic science, has reached a threshold of maturity both as computer science and forensic science
- there is greater collaborations between researchers and practitioners
- bias remains a concern, especially in the context of artificial intelligence as human biases might be replicated by machine learning systems; and it is hard to explain why a machine came up with a particular answer.

Each of these issues and much more will be presented in the review.

1.1. *Overview*

1.1.1. *Digital investigation and forensic science*

A person’s activities, including mobility across time and interactions, can be reconstructed in great detail using digital evidence. Some digital devices capture biometric characteristics in addition to contextual information, such as time and location, which can be used for investigative and forensic purposes. Digital investigations can uncover connections that traditional forensic disciplines cannot, and they can prevent criminal acts by intercepting them in the planning stages. The application of artificial intelligence is bolstering these formidable skills. How, given their efficacy, can digital investigations benefit from closer ties to Forensic Science? [1].

Digital forensic skills are being given to non-scientists for the preservation of digital evidence and the triage scanning of computers and smartphones for investigation reasons. Errors in the United Kingdom illustrate the negative impact of disregarding Forensic Science concepts and practices. A House of Lords investigation is examining issues about digital forensics, and the Forensic Science Regulator is pursuing digital forensic service provider accreditation.

Forensic Science techniques for understanding and assessing evidence can improve digital investigations. Common forensic science practices, such as cognitive bias reduction, aid in preventing erroneous

E-mail address: paul.l.reedy@gmail.com.

https://doi.org/10.1016/j.fsisyn.2022.100313

Available online 31 January 2023

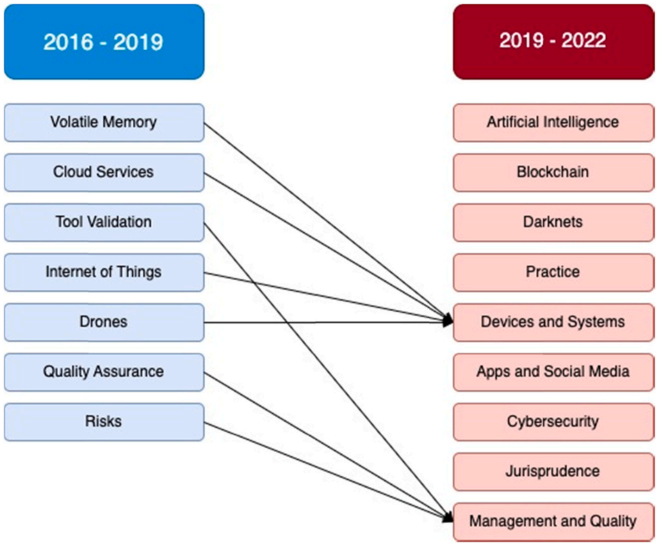

Fig. 1. Comparison of topics from the 2016–2019 review to the 2019–2022.

judgements, costly wasted effort, and miscarriages of justice. Digital forensic effective practice guidelines, error reduction measures, and related training must be updated to incorporate modern Forensic Science principles.

In certain contexts, like as the courtroom, it is advantageous to strictly adhere to Forensic Science's formalities. However, they are not as useful when digital forensics is used to combat terrorist activities or to prevent recurrent financial crime and fraud. In order to fix immediate difficulties, protect victims, and catch offenders, these operations must be nimble. After addressing crucial operational challenges, forensic science becomes relevant and adds value.

Digital forensics can benefit from the application of Forensic Science techniques, particularly for expert testimony in court. To prevent obsolescence, Forensic Science must adapt to the digitalized world and undergo digital transformations. In addition to digital evidence, these transformations involve the treatment of all traces with big data analysis and forensic intelligence tools. There are numerous digital investigative decisions that can be made with a lower confidence level.

1.1.2. Maturation

In 2019, digital forensics reached the threshold of maturation both as computer science and forensic science. This issue shows the power of collaboration between researchers and practitioners to create new knowledge that directly impacts digital investigations. Enhanced techniques for treating damaged or secured embedded systems to obtain needed digital evidence are presented in two highly specialised papers. Bias Mitigation is crucial as more digital evidence is stored on embedded systems that require forensic micro-repair or chip-off. Everyone who employs digital forensics has a responsibility to implement strategies that mitigate those influences which might interfere with accurate observations and inferences in forensic decision making. There is a pressing need to update digital forensic effective practice guidelines, error mitigation strategies, and associated training to include bias mitigation practices [2]. The importance of bias mitigation extends to uses of artificial intelligence (AI) that support decision making across all forensic disciplines. As stated by Jan Collie during the UK House of Lords Inquiry:

> *"human biases might be replicated by some of these machine-learning systems" and … "with artificial intelligence, it is very hard to explain what happened and how the machine came up with a particular answer" (Report - Forensic science and the criminal justice system: a blueprint for change, Science and Technology Committee, 1 May 2019)*

The demand for unbiased explainable AI is growing in digital forensics, including automated classification and source identification. The success of such systems depends on practitioner involvement to ensure that the results are reliable, understandable, and useable in digital investigations.

Digital forensics has matured considerably over the past 10 years, with researchers and practitioners working together to tackle difficult problems in both computer science and forensics science. Multiple organizations now recognize digital forensics as a forensic science discipline, including the American Academy of Forensic Sciences (AAFS), European Network of Forensic Science Institutes (ENFSI), Organization of Scientific Area Committees (OSAC) and UK Forensic Science Regulator. Formalizing collaboration between Digital Investigation and FSI is one of the most significant milestones in the journals' history, and will ultimately have a profound effect on both digital Forensics and forensic science.

2. Crimes

As almost every human activity leaves a digital trace, it can be assumed that every crime leaves some form of digital evidence. Some examples of cases reported during the review period include:

2.1. Encrochat

- Operation Venetic (National Crime Authority, United Kingdom)
- Operation Emma 95 (Gendarmerie, under the supervision of the Specialised Inter-Regional Juridiction (JIRS) of Lille, France)
- Operation Lemant (Dutch National Prosecution Service, Netherlands)

Analysts infiltrated the EncroChat mobile phone telephone system used by criminal networks around the world. The highly encrypted communication platform was hosted in France for which users could subscribe for £1600 per month, of which there were 60,000 users around the world and 10,000 in the United Kingdom. Users within the criminal networks used EncroChat to underpin international operations by transmitting images of guns and drugs, laundering money and organising contract murders. The system included preprogrammed time codes that automatically wiped data automatically. The NCA seized 106 EncroChat handsets among other contraband [3]. In the United Kingdom, 746 preferred to as "… suspected top-tier criminals …" were arrested. The EncroChat handsets were modified Android devices, many of them based on the BQ Aquaris X2 released by a Spanish electronics company. The marketing guaranteed perfect anonymity that included "… dual operating systems – a normal one and a hidden one to conduct secret messaging …". Additional modification included the removal of the camera, microphone, GPS transponder and USB port. Users could immediately delete all of the messages on the device on entering a PIN code or when incorrect passwords were repeatedly entered. The service was also capable of remote wiping. User hotspots were particularly prevalent in countries associated with trade in cocaine and cannabis sources and destinations. Investigators believe that the successful operation had prevented the murder of up to 200 people [4].

EncroChat first came to the notice of the French Gendarmerie in 2017 when they noticed that they regularly encountered the devices when conducting operations against organised crime networks. It appears that French investigators hacked the network, rather than decrypt messages, read messages and share the messages with other agencies [5]. The Gendarmerie entered into a joint investigation with the Netherlands with the participation of Europol. A large team at Europol was able to analyze the millions of messages and data in real time and to coordinate information exchange with concerned countries, including some who were not involved in the joint investigation team, including the United Kingdom, Sweden and Norway [6].

2.2. Fraud

Cyber fraud continues to be rampant. In April 2020, Domain Tools identified over 65,000 websites as fraud scams. Reporting of frauds are grossly underreported to law enforcement. Due to policing budgets and the resources required for effective cybercrime investigations, private sector firms are heavily relied upon to conduct the investigations and recover the funds for which a quick response is required. Perpetrators are increasingly using artificial intelligence tools to automate various aspects of the fraud process [7].

2.2.1. Payment diversion fraud

A victim makes a direct payment from their account to a false supplier or other entity using real time payment methods. Other terms associated with this type of fraud include supply chain fraud, mandated fraud and business email compromise. It is believed to have had a bigger impact than Brexit on the United Kingdom economy and the FBI regards it as one of the costliest forms of cyber-enabled fraud affecting American companies. Earlier versions of the fraud used telephone calls and phishing emails, whereas fraudsters are now monitoring potential victims' networks, phone and Internet of Things systems to gain an understanding of business and cultural patterns before sending out apparent legitimate requests from senior or known persons seeking payment.

The initial reconnaissance of publicly available information is now automated using crawlers in a similar way in which search engines retrieve results of search queries. The process is efficient and does not require a lot of time on the part of the attacker. Scripts are used to scrape useful information from websites and compile it into a useful and structured format, then blended with other information such as travel and conference information, to create a list of suitable victim organizations. AI techniques can assist in this process.

One an attacker has gained access to a network, they then seek to escalate privileges to allow them to move freely through the network. Rainbow tables and similar tools are used to steal credentials. It has been found that, as of 2018, an intruder can reside in a system for an average of 208 days before detection during which time they are looking for vulnerabilities and studying the organization's practices and behaviours. Attackers are using machine learning algorithms to observe user behavior, then to mimic typical user behavior allowing them to stay undetected in the system for longer. It is anticipated that AI will continue to be developed and used by attackers to automate vulnerability discovery and exploitation.

In a case study of this type of fraud, the CEO of a company instructed the immediate payment of a supplier's invoice on the supplier's letterhead with identical details to the supplier's previous invoices except for a change in Swift cade and banking details. The payment was made, as instructed, to an account belonging to a shell company that had no relationship with the supplier, which was then distributed to another three shell companies with bank accounts located in tax haven jurisdictions. It was found that three fraudulent payments had been made.

Forensic examination revealed some slightly unusual activity over the course of a year in an account belonging to a compromised employee with systems admin clearance. The employee was 'whitelisted' which explicitly allows additional and higher system privileges, services, mobility, access or recognition. Some time before the fraud had been detected, the employee's compromised account had sent a phishing email to the CEO which resulted in the download of malicious software that enabled the installation of a rootkit onto the CEO's computer. It was found that the silent, hidden surveillance of the network was partially automated possibly using AI.

2.2.2. Ransomware

Malicious software prevents legitimate users from accessing their system, usually by locking the system using encryption, until a ransom is paid, invariably by cryptocurrency. Criminals can purchase a collection of ransomware code for as little as $750 (US). AI engineered malware that mimics human behavior and specifically designed to attack the intended is now emerging. Ransomware is also used as a decoy attack to distract the victim while the attacker accesses and publishes the victim's data in illegal websites for further financial gain.

Ransomware differs from other malware attacks as the victim is acutely aware that they have been exploited and are given directions on how to be released from the exploit.

In the initiation, the attackers identify the target for their attack using similar information gathering methods as described above for payment diversion fraud. The attacker then seeks to infect the victim's systems using a specific attack vector and social engineering techniques. Once infected, the malicious program searches for the victim's device, system or network to encrypt specific files, folders, disk drives, network share drives and to delete any backup folders and restore points. During the extortion phase once the encryption process is complete, the victim is given a deadline for payment in exchange for a decryption key, with the payment usually made with cryptocurrencies to avoid detection. Once the payment is made, the decryption key is usually sent although that is not always the case as the criminals might go for additional payments. If it hasn't already, it is expected that AI will be used in the initial compromise of the target system.

In recent years, ransomware assaults have become more prevalent. Several government and non-government institutions have been impacted, particularly in the fields of education, health, business, research, and insurance. Techniques such as social engineering attacks, password cracking, network attacks, etc., have been used to seize control of the user's system and resources in order to cause more disruption and harm. The large cost of damage caused by ransomware attacks is due to downtime of the live system, interruption of regular operations, cost for forensic investigation, restoration cost, loss due to reputational injury, and cost for cyber security training.

Ransomware uses cryptographic techniques to encrypt and lock the system, as well as to interact with the command-and-control server. It requires consumers to pay with cryptocurrencies in order to regain access to their original data, but the recovery of their original files is not guaranteed. Ransomware exploits system vulnerabilities, such as the Windows SMB (Server Message Block) Remote Code Execution Vulnerability, in order to encrypt and lock the system.

Crypto ransomware and Locker ransomware are the two primary classifications of ransomware. Crypto ransomware encrypts the data on an infected computer system and holds the contents hostage until the ransom is paid in bitcoin. The identity of the virus author is concealed through bitcoin payments. In most cases, paying a ransom enables the decryption of encrypted files, allowing users to recover their original, readable data. Locker, on the other hand, only encrypts the data. Users may retrieve the encrypted contents by physically relocating the hard disc to a secure place or computer system.

2.2.3. Financial technology

Financial technologies, becoming known as Fintech, is emerging as a sub-discipline of digital forensics. Digital transformation is leading to the emergence of new technologies for payments, funds transfer and other transactions. The technologies themselves involve hardware, software, application programming interfaces, cryptography and network protocols. The new systems create new opportunities for fraud, extortion, money laundering, financing of criminal activities, tax avoidance and other criminal activities. The technological basis for the new financial technologies means that digital forensics is well placed with the knowledge and skills to be prominent in the investigation of these activities.

Nikkel (2020) notes the gap between traditional fraud investigators and traditional digital forensic examiners, each group having complementary skills and knowledge [8]. Further, Nikkel defines Fintech Forensics as "The application of digital forensic science to financial technologies for the purpose of investigating and reconstructing criminal financial activity."

Some examples of where Fintech forensics can be applied include:

- Phishing for committing financial fraud where victims are deceived in to divulging the access details to their financial accounts such as bank accounts, credit cards etc. by impersonating a bank or other financial institution. Victims are usually approached via an electronic communication such as email, message, voice, or Twitter. Fintech forensics would assist in understanding and the reconstruction of the attack.
- ATMs and payment card terminals can be targeted for the theft of payment card information that can be obtained from the magnetic strip on the card. Criminal techniques include skimming, shimming (intercepting the data as it transfers from the card's chip to the chip reader), comprising the computer within an ATM, and compromising the central control systems of ATM networks.
- Online banking trojans that infect devices used for banking that provide unauthorized access to bank accounts.
- Rogue mobile banking apps produced by criminals which they make available on mobile app stores. The rogue apps impersonate existing financial institutions and claim to provide a financial service.
- Extortion and ransom attacks can involve DDoS for Bitcoin (DD4BC) involve threats of a distributed denial of service if a payment of crypto currency is not forthcoming; ransomware involves the encryption of an organization's data for which a decryption key will be provided in exchange for the payment of a fee paid in crypto currency, and sextortion claiming that the victim's computer has been infected and embarrassing videos have been made.
- Online social engineering attacks to commit fraud usually involving persuasion that a victim has a technical issue with their computer for which fake support is provided over the phone in exchange for credit card details. On occasions, remote access software is installed on the victim's computer that might include the ability to highjack online banking.
- Business Email Compromise and CEO impersonation involving unauthorized access to business email accounts, or fraudulent email accounts, for the purpose of sending impersonated payment requests and invoices.
- Compromised payment processing infrastructure of financial systems, such as the SWIFT payment network that allows funds transfer between banks.
- Online money laundering can involve the use of money mules where illicitly gained money is transferred to a mule's account who then withdraw cash, keep an agreed portion and forward the rest to another recipient. For large amounts, companies provide MaaS (Mules as a Service) which can be hired. Increasingly cryptocurrencies are used to launder money although for some currencies (for example, Bitcoin) the transactions are recorded on a public blockchain ledger. However, tumblers and mixers are used to mix the cryptocurrency with other funds to obfuscate the transactions.
- Criminal financing through the use of cryptocurrencies to purchase goods and services on darknet marketplaces, much of which can be purchased as CaaS (Crime as a Service).

In each of the above examples of Fintech, there is a need for specialist digital forensic knowledge and skills to be applied to investigations to reconstruct the incident and transactions, identify the participants and produce a brief of evidence. A substantial research program is also required to better understand the flow and transfer of money, criminal attribution, real time anomaly detection and correlating log information with criminal activity.

2.3. Cyberbullying

Cyberbullying concerns the verbal abuse of victims using technology, primarily via social media. The presence of specific, charged language on Twitter was used to identify to sample and identify a dataset of 140,000 tweets collected over a one week period. The dataset was analysed through regression to develop a model for the identification of language behavior that can be applied to locating cyberbullying hotspots [9].

2.4. Sexual predatory chats

By using social media platforms to specifically target minors online, predators commit the crime of online sexual grooming. For digital forensic investigators, examining sexually predatory communications online is a challenging process. Digital forensics has employed machine learning models to combat social cyber-related issues like intrusion detection and digital text forensics. Machine learning can be used to categorize language as predatory or non-predatory in the case of online sexual predation. The classification process must be understood by digital forensic investigators. In order to ensure openness and justice, it is also important to recognize when the model fails [10].

The rising use of social media platforms has created a number of difficulties for online safety. Children often face problems with deceit (such as online sexual predators) and cyberbullying, to name just two. As a result, it's critical to spot particular behavioural trends in an online communication that most accurately characterize a sexually predatory conversation.

A strategy to divide online chats into three stages of sexual grooming has previously been proposed. This staged approach can be used to determine whether or not a communication is predatory. Usinga machine classifier, accuracy can be improved when categorizing online grooming phases. Other researchers have suggested using a two-pronged strategy to identify an adult impersonating a child in an online chat, while others have used Markov chains to analyze a sampling dataset to identify typical behavior. To comprehend a predator's grooming language, the Corpus Assisted Discourse technique and the Linguistic Inquiry and Word Count tool have been previously been proposed. Online sexual behavior identification has grown in significance as more conversation systems migrate to platforms like WhatsApp and Telegram, to mention a few, instead of using massive chat rooms. The Digital Forensic Process Model, with a focus on the Digital Forensic Investigation phase was applied to the study.

The sexual predator identification task was first introduced in 2012 by Plagiarism analysis, Author identification and Near-Duplicate detection. Data was gathered from online conversations with the following characteristics: a small percentage of true positives (i.e., non-consensual and sexually predatory chats); a large percentage of false positives (consensual conversations with similar topics to "sexual predatory chats"); and a large percentage of false negatives (general conversations between people talking about any other topic). A nonprofit group called Perverted Justice gathered the real positives. This organization uses trained volunteers to speak with prospective sexual predators online while posing as kids.

Perverted Justice's decoys wait for their predator to make physical contact with them rather than the other way around to avoid criminal entrapment. Instead of the other way around, Justice's decoys wait for their predator to make the first move. The data comprises XML-formatted training and testing corpora. To understand how machine learning models would recognize predatory chats, the researchers looked at the behavior of sexual predators in online chat logs.

According to the theory, key elements like phrases or words are linked to an online predatory discourse. For categorization, four different types of models were used: long short-term memory, multilayer perceptrons, XGBoost, and logistic regression. Deep learning was used for dimensionality reduction effectively reflecting the key components of the data. To extract the most features from 100 k documents and train XGBoost, Multilayer Perceptrons, and Logistic Regression, word frequency-inverse document frequency was employed. The next step is to use a feature selection approach to choose the features that will help solve the present problem the best.

Information up to a 150-word conversational threshold was encoded for Long Short-Term Memory. Zeros were inserted to discussions that were less than 150 words long. Based on the supplied n-grams, Logistic Regression and XGBoost produced crucial features.

The greedy search method aims to draw attention to words or phrases that are significant only in relation to the predatory classification. The entire corpus was subjected to a Term Frequency-Inverse Document Frequency analysis with unigrams, bigrams, and trigrams. Additionally, the classifiers XGBoost and Logistic Regression were trained to map each chat to its projected category. According to the findings, the conversational segments that have the highest prediction probability influence the final prediction more. For example, the vocabulary terms connected to sexually predatory behavior in conversation. Overall, it was found that the existence of features—words or phrases—from each interaction has a significant influence on the model's judgment. In contrast to what one might anticipate, machine learning models perform better on generic content. This could be a key piece of proof for digital forensic investigators that predators typically don't groom their victims with a lot of explicit sexual material.

2.5. Public vs private investigations

It has been estimated that a cybercrime investigation conducted by law enforcement can cost up to ten times that it costs for a private investigation firm, for which there are many reasons:

- Differences in jurisdiction impact on the ability of authorities to assist and cooperate with each other. Some jurisdictions might be unable or unwilling to cooperate and for which bureaucratic processes are to be followed and time is an essential factor. Warrants might be required in multiple jurisdictions which takes time and might result in the loss of intelligence and evidence. In contrast, private firms are less hampered by bureaucratic processes and can simply make a phone call or correspond by email, can respond immediately to gather intelligence and provide sufficient information for the police to move and make an arrest.
- Attribution to the suspects and the devices that are used in committing the offence and the location of the devices being used to perpetrate the crime can be more easily and quickly performed by a private firm than by police. The process for obtaining a data interception can be difficult and time consuming to complete, and is heavily reliant on the formal relationship between the jurisdictions and the similarity of the crimes under investigation. Further, there is no guarantee of success. The access to many tools and information

2.6. Threat vectors

There are several techniques that criminals use to gain unauthorized access to systems. A few of these include [11]:

- Phishing for Access in which members of a potential victim organization is sent generalised email containing a link to a fake site access page on which the recipient is encouraged to provide their organization's system credentials. The email will not contain any user specific information as would be expected in a bulk email.
- Spear-Phishing for information involves an email to a specific target. It will have the appearance as originating from a legitimate and familiar source using information obtained during the initial reconnaissance phase. Again, it will encourage the recipient to provide their system credentials.
- Password Spraying refers to attempting access through the use of common passwords through many access points, for example all of an organization's email accounts, in a short period of time.
- Drive-by-download exploits security flaws to infect devices with malware. The malware is placed on compromised websites from where it automatically downloads and self-installs on the user's device once the website is accessed. This technique can also be distributed by email.
- Unpatched system vulnerabilities are scanned by criminals for potential exploitation in order distribute a ransomware payload.
- Spear-Phishing for Escalated Privileges are sent from an organization's own user email accounts in order to gain escalated privileges. The emails usually contain a link to a site that employs social engineering to persuade the user to provide their system credentials.
- Email Spoofing involves falsifying a real email address or using an email from an attacker-owned domain that resembles the domain of the target organization.
- Malicious emails with social engineering are distributed in the same way as phishing techniques. The unsuspecting user is duped into opening an email attachment with malicious code that executes a ransomware payload.
- Brute force – Remote Desktop Protocol refers to an attacker gaining admin access to server credentials with remote access from where they can exploit administrative tools and vulnerabilities to distribute and infect other devices.
- Exploit Kits are software packages that create vulnerabilities within a system.
- Malvertising are targeted ads containing concealed malware links presented to potential victims based on their search history and web preferences. Attackers often place the ad on highly reputable websites.
- Network propagation of malware from device to device over a network.
- Propagation through shared services when, for example, malware is placed in a share file accessed from, say, a home computer that is also accessed from the workplace.

3. Artificial intelligence

More than ever before, the world is nowadays experiencing increased cyber-attacks in all areas of human daily life. This situation has made combating cybercrimes a daily struggle for both individuals and organizations. Furthermore, this struggle has been aggravated by the fact that today's cybercriminals have gone a step ahead and are able to employ complicated cyber-attack techniques. Some of those techniques are minuscule and inconspicuous in nature and often camouflage in the facade of authentic requests and commands. In order to combat this menace, especially after a security incident has happened, cyber security professionals as well as digital forensic investigators are always forced to sift through large and complex pools of data also known as Big Data in an effort to unveil Potential Digital Evidence (PDE) that can be used to support litigations. Gathered PDE can then be used to help investigators arrive at particular conclusions and/or decisions. In the case of cyber forensics, what makes the process even tough for investigators is the fact that Big Data often comes from multiple sources and has different file formats. Forensic investigators often have less time and budget to handle the increased demands when it comes to the analysis of these large amounts of complex data for forensic purposes. It is for this reason that the authors in this paper have realized that Deep Learning (DL), which is a subset of Artificial Intelligence (AI), has very distinct use-cases in the domain of cyber forensics, and even if many people might argue that it's not an unrivalled solution, it can help enhance the fight against cybercrime. This paper therefore proposes a generic framework for diverging DL cognitive computing techniques into Cyber Forensics (CF) hereafter referred to as the DLCF Framework. DL uses some machine learning techniques to solve problems through the use of neural networks that simulate human decision-making. Based on these grounds, DL holds the potential to dramatically change the domain of CF in a variety of ways as well as provide solutions to forensic investigators. Such solutions can range from, reducing bias in forensic investigations to challenging what evidence is considered admissible in a court of law or any civil hearing and many more [12].

Weak AI (reflecting current AI technology) can be defined as performing intelligent human processes without really understanding the process. Strong AI (encompassing future AI technologies) includes common sense, self-awareness and creativity [13].

AI comprises many techniques including:

- Machine learning
- Deep learning
- Speech recognition
- Natural language processing
- Neural networks which mimic the human brain to create on information processing system comprising a large number of interconnected nodes working with each other to solve a specific task. The self learning process is capable of capturing highly complex and nonlinear relationships between data. The networks extract patterns, detect relationships in data and learn through experience.
- Intelligent agents
- Artificial Immune Systems are designed based on the biological immune system to develop mathematical models. AIS comprise a number of algorithms
- Pattern recognition
- Fuzzy logic employs approximate reasoning rather than exact and fixed based on human language rules provided by the user. The rules are converted to their mathematical equivalents in order to make strict decisions. Fuzzy logic can handle problems with incomplete and imprecise data.
- Genetic algorithm is an optimization technique to find approximate solutions to search problems. It begins with a set of random or selected solutions called chromosomes which, together, form a population. The algorithm works iteratively enabling the chromosomes to improve with each iteration or generation, eventually arriving at the best solution.

3.2. *Machine learning*

Mohammad and Alqahtani (2019) [14] compared several machine learning techniques for classifying files that have been manipulated by a specific computer program by analysing the artifacts remaining following access, update, modification and deletion of a specific file system. File system, audit log entries and registry information from a Microsoft Windows 7 environment were combined when challenged with four different scenarios using 10 applications:

- Microsoft Word, Excel, PowerPoint, Access, Paint and Internet Explorer
- NetBeans
- Adobe Acrobat Reader
- VLC Media Player
- WEKA

Over 42,000 instances were collected for the training set. As most machine learning algorithms only deal with numerical values and some of the features to be analysed comprise text, the text features were converted to numerical code prior to analysis.

The following machine learning algorithms were tested:

- Feed Forward Neural Network
- Support Vector Machine-Radial Based Function
- Support Vector Machine-Polynomial Kernels
- Random Forest
- Classification and Regression Trees
- Naïve Bayes-SimpleEstimator
- Naïve Bayes-BMAEstimator

It should be noted that each of the machine learning technologies possess different training requirements; and different strengths and weaknesses. Each algorithm was tested against four scenarios and 22 digital evidence inputs were collected.

The experiments showed that the Neural Network and the Random Forest algorithms were the most accurate, both with a value of 89.0297%. In comparison, the Support Vector Machine-Radial Based Function, Support Vector Machine-Polynomial Kernels, Classification and Regression Trees, Naïve Bayes-SimpleEstimator and Naïve Bayes-BMAEstimator ranged in accuracy between 84.2772% and 87.8416%. In addition, Random Forest is more precise than the other technologies; yet the Neural Networks had better recall than all others. Notably, the results were "satisfactory" although performed to less than expectations, possibly due to some of the test applications use common elements within the file system. When considering the accuracy of each of the technologies, each of the algorithms are subjected to algorithm-specific training that is operator defined.

3.3. *Deep learning*

Deep learning enables the multi-layered neural networks to be applied to tuning machines in order to accomplish defined tasks. Deep learning is a subset of artificial intelligence that mimics the processing function of the human mind. When applied to cyber forensics, deep learning has been shown to reveal potential digital evidence from large data volumes (big data).

Karie et al. (2019) devised a generic framework through which deep learning cognitive computing concepts can be integrated into cyber forensics to improve the investigation effectiveness. Due to the large volumes and complexity of evidence, manual processing and analysis of digital traces can introduce errors into the process resulting in erroneous conclusions. Applying deep learning cognitive computing techniques to cyber forensics can be used to identify cyber-based attacks and clustering which can be used to identify patterns within log files and records and mitigate potential bias that accompanies manual analysis [15].

The authors put forward the concept of using machine learning in the various processes of an investigation, including:

- Initialization process where machine learning can be applied to the first responder's planning and scheduling of tasks
- Potential digital evidence data sources identification can benefit from the application of clustering algorithms to group sets of similar data based on defined criteria; and for the segmentation of data into groups which, when both techniques are applied, can identify relationships between different data sources
- Deep learning enabled cyber forensic investigation engine that employs algorithms with the ability to handle evidence acquisition, preservation, analysis and interpretation:
  - o Evidence collection/acquisition employs data mining algorithms to dive into the data to extract specific artifacts based on defined criteria; and association algorithms to discover duplicated or connected data obtained from different sources
  - o Evidence storage and preservation can reduce the possibility of human errors in this phase
  - o Evidence analysis can benefit from the application of clustering and classification algorithms, the status of the relationship between the evidence and the suspect and the victim can be established, together with an estimation of the weight, validity and reliability of the evidence together with any inferences that can be drawn; classification algorithms can establish the relationship between the evidence and the incident under investigation, possibly drawing attention to additional potential sources of evidence;
  - o Evidence interpretation can be assisted by the use of algorithms which will reduce the possibility of human error and release

human resources by automating a task that is usually performed by highly trained and experienced persons

- o Concurrent processes can be conducted as algorithms can ensure that all processes are contemporaneously documented as they are performed.

- Forensic reporting and preservation employs classification algorithms that draw conclusions from observed values and to determine categories for new observations.

3.4. Bias in artificial intelligence

Deep learning and machine learning are increasingly featuring in articles concerning digital evidence. The European Commission is implementing rules for and actions for trust in Artificial Intelligence. People using these automated systems should be aware of the bias in algorithms and persons using it. Journal editorial recommendations include the prevention of bias and have inclusive language. Language should make no assumptions about the beliefs or commitments of any reader. Content should contain nothing that could imply that one person is superior to the other on the grounds of age, gender, race, ethnicity, culture, sexual orientation, disability or health condition. Authors should ensure that writing is free from prejudice, stereotypes, slang, references to dominant culture and/or cultural assumptions [16].

Bias and privacy

Legal philosophy is obsessed with bloodless questions, yet human rights cases are adjudicated in spaces full of beating hearts. In rights adjudication, the concept of human dignity is interpreted in the context of its violation. The thick emotions that relate to the concept help judges see and understand human dignity violations in the evidence before the court. Most of the illegally acquired evidence is digital,' as digital evidence is easier to access, transfer, copy, and store. 'Artificial Intelligence' (AI) has been used for years already by domestic courts all around the globe in delivering civil and administrative justice, as well as commercial and investment arbitration tribunals in their awards [17].

As criminal trials demand higher procedural safeguards, its role in criminal justice faces deeper caution even more so in the People's Republic of China. No research has scrutinised AI's potential to reshape the role played by emotions, impressions, feelings, memories, and experience in the judicial approach to complex digital evidence. Whether AI should be regarded as an embryonic game-changer in international criminal trials is the subject of much study in argumentation theory, artificial intelligence and law. The endeavour is not seeking to establish whether Al could maximize the logical nexus between inferential propositions and the evidence underpinning them. Instead, the endeavour is concerned with evidentiary problems related to digital evidence in their intersection with the advent of AI.

The use of AI in international criminal justice must be contextualised within the larger informational power-asymmetries that are infecting the (international) criminal justice system. Excluding illegally obtained evidence “may prevent otherwise widely or even universally acknowledged truths from being considered judicially proven,” and rigors judicial scrutiny “may paradoxically mean that the probability of true or complete results is no greater than that which attaches to other social forms of determining truth or writing history,” are undeniable facts.

The significance of this paper lies in the observation that “to the extent that the International Criminal Court (ICC) intends to increase its use of digital evidence, including through the collection, storage, (algorithmic) analysis, verification, and dissemination of intercepted communications, bulk data sets, or computerised digital depositories, to name but a few examples, clearer policies must be implemented to ensure both the accuracy of the conclusions and the privacy of the individuals involved."

'Electronic evidence' is a generative term for two types of evidence: 'analogue evidence' and 'digital evidence'. Evidence that is recorded by an analogue device is capable of being manipulated, but alterations can be detected. Examples of digital data include anything that has been created or stored on a computer, or made available by way of the Internet. The ICTY Appeals Chamber applied the legal maxim male captus bene detentus (wrongly captured, properly detained) to justify its exercise of jurisdiction over a defendant who had been abducted. Digital evidence needs not be corroborated by witness testimony to be admitted, despite the obvious caution one should apply owing to the uncertainties which are inherent to digital evidence's authenticity and chain of custody.

The Nikolic judgment has been criticized for elevating the prosecution of 'core international crimes' above other considerations, such as abuse of process. Evidence obtained unlawfully through torture is likely to poison the justice-edifice more perniciously than that collected in breach of individuals' privacy. Digital evidence is easier to unlawfully collect compared to the non-digital one, if anything because it reduces the instances of manifest violations of States' sovereignty. As a matter of practice, 'confessions' extracted through unacceptable interrogation techniques have been consistently excluded, for instance in Delalic. It may also have been because of concerns regarding privacy in the digital age that differ significantly from those faced by lawyers in traditional criminal proceedings.

Crime victims are pulled into the inner workings of the criminal justice system by the unlawful acts of others. It is not uncommon for victims to become increasingly concerned with privacy, especially as it relates to images and information captured via digital devices. International criminal trials are already traversed by allegations of selectivity, West-centredness, and power-capture, leading inter alia to inequality of arms that encourages, in turn, a frequent recourse on the part of defence counsels to tu quoque arguments.

Judges tend to over-rely on the supposed 'objectivity' of videos because they assume the latter to show facts as they are without mediation ('naive realism'). From an anthropological standpoint, because humans fail to take images seriously enough, they have developed 'no grammar, no syntax, no canons of interpretation for the visual [judges, too] lack the ingrained, institutionalized scepticism that [they usually] bring to the text'. Judges and lawyers are trained for verbal rhetorical devices and verbally construed analogies, and judges are too; images, non-verbal sounds, and videos fall outside the scope of their current expertise. Narratology helps us to understand the reach of narrativity in human consciousness, but also to 'denaturalize' narratives. How does digital evidence modify documentary maximum length, alongside the time-limits of the proceedings as a whole?

As the ICC seems remarkably punctilious when it comes to word-count, how does it translate to digital evidence, including audio-videos being included in memorials? In the Milosevic case, International Criminal Tribunal Yugoslavia judges apparently expressed an admirable sense of self-restraint in the most delicate of the occasions, without giving way to pressures from the media throughout Europe and beyond, and dodging the trap of ascribing any weight to simple-minded sensationalism. But one shall mention at least the 'later exclusion' bias, occurring when judges decide to see and listen to pseudo-evidentiary material even when it is most probably irrelevant or unreliable, because they will anyway be able to exclude it later.

An audio recording remains crystallised over time like a photocopy, with no chance for updating and terminological-conceptual transmigration. This is one of the reasons why judges, although not trained in visual rhetoric, are sympathetic towards digital evidence. Another reason is that technological means ensure wide coverage and pervasiveness, thus allowing judges to reason 'by subtraction'. In Ruto before the ICC, the prosecution did not produce any recording of a broadcast by Mr Sang in which he made the type of statements he is accused of. Videos are helpful in a way that will sound contradictory to what was explained supra, but that should rather be understood as complementary to such explanation. They are at times best placed to represent a scene in its integral participatory fashion, because it permits to convict 'collateral perpetrators' far more easily.

Al can be of assistance in the field, through automated capturing and sharing of footages from authorities. This potentially shields prosecutors from privacy violations while also relieving them from cooperation requests, jurisdictional concerns, visa/travel restrictions, and so forth. While processing and appraising evidence through AI might become more expensive, other economic resources will be saved because of prosecutorial on-sight investigations rendered unnecessary. This could lead to massive distortive effects on the engineering of international justice. The ICC's first arrest-warrant based on open-source information concerned the Al-Werfalli case, but this kind of information had already been used in previous cases.

States might object to the creation of such a repository even in the absence of (immediate) public scrutiny, as the former would encourage prosecutorial reliance on anonymous, third-party (unlawful) leaks. This notwithstanding, benefits would abound; among them, that of no longer depending on the algorithm running social media platforms such as Twitter or YouTube. The first category of open-sourcing refers to the plain-view exception to the unlawfulness of warrantless searches; it allows for in medias res accounts of the events; it shows suffering as it happens, facilitating emotional sympathy and resonance; it obviates the need for witnesses, or places the latter in safer conditions as they are enabled to come forward anonymously. This way, prosecutors factually 'outsource' compliance with relevant laws and receive potentially evidentiary material however obtained, in defiance of any safeguards for the accused.

Al can improve the reliability of digital evidence in several ways. First, it may assist human forensic experts in spotting deepfake videos, forged handwriting, and other fabricated evidence. It may also notice correlations and nexuses among gestures, landscapes, voices, and facial expressions that escape human senses or rational judgement. Moreover, AI may verify digital evidence's chain of custody, even with the auxilium of incorporated blockchain, and it can – with degrees of limitations – scrutinize (expressed) emotions relevant for mens rea assessments. In the process of proving guilt or innocence in a criminal cases, hypothetical stories or scenarios about "what happened" in a case are constructed and arguments based on evidence or commonsens[ical] knowledge are used to support or attack these stories. There is literature advocating for plausibility to play a greater role in criminal law, AI could revive this discussion and place higher emphasis on plausibility.

Overcomplexity always brings a shift in the allocation of non-formalistic appraisal powers; digital evidence is thus presented with the conclusion already incorporated without much effort on the part of the judges. This shift of adjudicatory and fact-finding responsibility to the technician (digital forensics expert) frees time for the judges but provides them with fewer opportunities to ascertain the meaning of the evidence itself and the facts it apparently proves. AI results are portrayed in such a way that the infallibility bias already verified for digital evidence more generally is reinforced. 'The more inscrutable a machine process, the more its accusatory conveyances threaten the dignity of the accused and the perceived legitimacy of the process' 'Introducing such raw data (that is, machine-feeding data) at trial would anyway lead to reintroducing potentially 'bad evidence' (e.g. unlawfully gathered one) in the courtroom through the backdoor, leading to a circumvention of the fruit-of-the-poisoned-tree doctrine'. In the near future, malicious actors will be able to rely on predictive behavioral analysis to identify the emotional triggers that push subgroups to violence. Social engineering, psychological manipulation, and other techniques of subversion and deception will be amplified. The deployment of AI-enabled forgery technology will drastically alter the relationship to evidence and truth across journalism, criminal justice, conflict investigations, political mediation, and diplomacy. AI does not systematically eliminate the bias which is inherently part of human cognitive processing of digital evidence, it simply reiterates it in a more distributed – and thus, possibly, less 'customised' – fashion. AI reiterates human bias in its coding (source data) and through the 'big data it is fed with, originating an error propagation which is hard to control ex post, and that might assume unwarranted forms when read through the lenses of AI's own subsequent learning.

3.4.1.1. Recommendations

In light of the numerous fallacies, inaccuracies, biases, and deficiencies, the author offers fourteen policy recommendations targeted at enhancing the preparation of international criminal tribunals for digital and AI-related evidence.

1. The standards for admissibility should be raised and adhered to more strictly. Once a piece of evidence has been presented to the court, it influences their cognition and mental process, regardless of the rational weight that judges later attribute to such evidence. Both judicial experience and psychological research have established that it is cognitively difficult for a judge to completely disregard evidence against their will.
2. In order to prevent prejudicing, admissibility bars should be imposed by the Pre-Trial Chamber rather than at later stages of the proceedings, as is currently the norm.
3. Judges involved in the process of admissibility should be distinct from those in charge of the actual trial in order to reduce cognitive bias and maintain minimal evidence-related linkages with an overly active Office of the Prosecutor. This is particularly true in context-specific tribunals, such as the International Criminal tribunal for the Former Yugoslavia, where the same evidence was sometimes used to prove several offenses simultaneously.
4. In international criminal law, two fifty-dollar bills may not always equal a hundred, especially when digital evidence, with its unique cognitive and technical problems, is involved. Each accusation should be supported by at least one exhibit that practically stands on its own and requires only corroborating support from corroborating evidence to meet the required standard of proof.
5. Judges should get elementary training in information technology and cognitive psychology, as well as exhibit fundamental knowledge of forensic and computer sciences. Each court should have access to a "pool of specialists" comprised of tech-savvy judges. A lower average age among all judges can assist in keeping them abreast of technology advancements. Certain digital exhibits are extraordinarily complicated and necessitate mental flexibility for full appreciation.
6. Digital evidence collected by 'street' human rights advocates and NGOs (also known as 'user-generated' evidence) should be treated with extreme caution due to their tendency to overemphasise the significance of their findings without paying sufficient attention to the chain of custody. The fact that evidence is gathered or picked by AI-powered devices does not justify a relaxation of caution.
7. Who exactly cannot illegally collect evidence (prosecutors of international criminal tribunals, States, etc.) and under what legal regime (domestic only, international only, or both) must be addressed, as the existing "open interpretation" scenario is untenable. If it is agreed in principle that international prosecutors must adhere to international privacy norms, there will be a problem defining precisely which human rights are at stake, since there is no universally acknowledged "right to privacy."
8. Illegally collected digital evidence should always be discarded, as its untraceability contributes to the weak trustworthiness of this form of evidence in general; furthermore, if international justice is motivated by exemplarity aims, the "deterrence argument" cannot be dismissed.
9. Digital evidence should not be gathered through clandestine agreements or conspiracies between private people or agents and state or prosecuting authorities. "The prosecution must bear the

burden of proof," and a tribunal must be satisfied that there was no collaboration between private individuals or organizations and police and prosecutors.

10. In these procedures, "overall" evidentiary evaluations are not entirely avoidable, although they should be reduced to a minimum.
11. Rather than being left to the discretion of each judge, the 'overarching interests of justice' should be more precisely defined and established ex ante. The concept of the trial's overall fairness should likewise be eliminated. The road of international justice is too crucial for adjudicators to raise suspicions that they want to achieve a preset political objective.
12. International human rights law should not be employed selectively and in a decontextualized manner in criminal law procedures. International Human Rights Law, as a legal regime with its own reasoning, applicability, exceptions, and processes, is created for claims against States rather than individuals.
13. The procedural rules of international criminal tribunals must be revised to specify whether robots should be entrusted with the collection, sorting, and evaluation of evidence.
14. Al is commonly accepted as a tool to assist humans with their activities. 'Neutrality' cannot be attributed to Al computers because the data on human actions they are fed is inherently 'humanly biased' Human selection and evaluation of evidence in international criminal proceedings must be further governed by norms of procedure, and cannot be entrusted to 'intelligent' machines.

3.5. Grooming detection using AI

This study introduces an AI-based online grooming detection method to reduce human errors, save time, and handle other issues. The suggested system uses the bag of words approach to automatically identify online child grooming. Fuzzy-rough feature selection selects the most important features for classifier input. The collected features are used to train text classification with classifiers like the fuzzy twin support vector machine [18].

Two public sources provided training data. The perverted-justice website archived almost 600 child grooming conversations between abusers and adult volunteers acting as children. The other source was PAN13 dataset. As shown by the evaluation findings, using training data sets from different sources balances and diversifies the proposed system's performance.

For the purpose of identifying grooming chats, investigators frequently use keyword searches in various digital forensic technologies. Not all data can be searched immediately and easily; frequently, information must be decrypted and given in a text-searchable format. The data was indexed using forensic software tools, which identified the location of each keyword inside the data stream.

Prior research examined the efficacy of text classifiers in identifying child grooming in internet chat chats. This was accomplished by combining a novel strategy with three conventional text categorization methods, including linear or logistic regression, decision trees, and Naive Bayes. Psychometric and categorical information techniques (such as linguistic inquiry and word count) were used to improve classification performance.

The proposed grooming detection framework comprises of six consecutive phases, which are, data collection from various sources, preprocessing to guarantee all the documents are with unified format, feature extraction to build concise representation for each document, feature selection to remove redundant or noisy features in the generated document representation, normalisation to make the data more sensitive to classifiers, and finally classification for predicting the class label of a given online conversation.

This study collected data from Internet talks about child grooming and non-grooming conversations. The former contains more than 600 archived.TXT files of child grooming discussions between perpetrators and adult volunteers acting as children, from which 200 were organized by perpetrator chat usernames.

Online discussion logs must be converted into training data set format. Chat log formats differ by social network. Skype and WhatsApp save talks to a generic database file (.db), which numerous software programs may see, while Facebook Messenger conversations are downloaded in HTML format.

Online grooming detection is developed via fuzzy-rough feature selection. Using the training data set, feature selection maps high-dimensional data into lower dimensions to select a few attributes. 150 characteristics are ideal for binary classification and 30 for multi-label classification in the proposed system.

To handle the reality that some dataset features have highly diverse physical interpretations, data is normalized first. Since the selected attributes are based on different regions of the same data, their value ranges may vary greatly. Users can customize data processing with this system.

Online grooming detection is developed via fuzzy-rough feature selection. Using the training data set, feature selection maps high-dimensional data into lower dimensions to select a few attributes. 150 characteristics are ideal for binary classification and 30 for multi-label classification in the proposed system.

The proposed system contains all 6 classifiers for user flexibility. The gathered data set taught all these classifiers. The latter two classifiers use SVMs. Linear and nonlinear (RBF kernel) coordinate descent fuzzy twin support vector machine have been used.

Gaussian Naïve Bayes achieved its best performance of 58.33% using the Bag of Words features and Min-Max normalisation technique. 60.75% mean accuracy was generated by AB in using Term Frequency-Inverse Document Frequency plus Power Normalisation l1. With the involvement of Fuzzy Rough Feature Selection for the binary classification task, the performance of Gaussian Naive Bayes was boosted up to 59.08%. Gaussian Naïve Bayes produced its peak performance of 47.84% (using Term Frequency-Inverse Document Frequency features that normalized by Power Normalisation), while Random Forest reached its best performance of 55.99%. Logistic Regression produced 61.58% prediction precision using the combination of Bag of Words and Power Normalising l2. Linear Coordinate Descent Fuzzy Twin Support Vector Machine were respectively with 60.96% and 60.78%.

Based on the preceding explanation, AI-based digital forensics technologies can be used for chat log screening, but they need more development before they can help investigators. Grooming chat logs and Internet language require adaptive AI techniques, which is ongoing effort. Technically, most classifiers perform best when Fuzzy Rough Feature Selection is not used, while conventional normalisation techniques like Min-Max and l1 improve accuracy when it is used.

3.6. File type identification

In the past, data recognition was largely employed to aid users; today, it is found in numerous products, including intelligent firewalls and forensic diagnostic software. The proper identification of files, particularly the recognition of file types, is the subject of more and more research in this field. The new types of intrusion data are the foundation of many attack scenarios, making accurate identification crucial. Since the subject of file type identification has been studied for so long, numerous taxonomies have been created and investigated [19].

The entire study field has been divided into five major groups, with the three most popular classes—signature-based, statistical, and computational intelligence-based approaches—being the focus of this paper. Previous methods included "sector hashing," or the selective hashing of disc sector signatures. The issue was that these hashes were limited to using specific, predetermined block sizes. Data streams and individual files, particularly small files, were unaffected.

Another strategy involved using maps to match master files with image files. Then came the introduction of bloom filters, with similarity preserving hashing advanced processing speed. The tool “sdhash,” which had a 94% accuracy rate, was finally unveiled. Blocks with sizes of 20, 200, 500, and 1000 bytes were employed in the Byte Frequency Distribution method. 20-byte blocks had a classification success rate of 100%, but 1000-byte blocks did just 77% worse. The Rate of Change technique produced the greatest results for file types that contain a lot of 0 × 00 and 0xFF, such as the metadata of JPEG images. The accuracy of file type detection on executable code in network packets was investigated using N-grams, which depended on the size of each file fragment. For instance, whereas ZIP files only achieved an accuracy of 18%, HTML and JPEG files were categorised with a 98% accuracy. Other methods computed the standard deviation of “sliding windows” using information entropy and compressibility.

A method based on artificial intelligence comprises the third approach. Support Vector Machines (SVMs), Neural Networks, Bayesian Networks, and k-Nearest Neighbor are the most popular models of these systems. One method made use of the longest continuous streak of repeating bytes and the average consistency between bytes of sequences in natural language processing. SVM classifiers were combined with features like Hamming weight, standardised kurtosis, or maximum byte streak. To locate executable code, other researchers have combined an n-gram analyzer and a disassembler.

3.6.1. Comparison of experimental results

Two neural networks and four distinct SVMs were trained on the same dataset after six tests. A “Confusion Matrix,” which displays the prediction for each file type in rows of data, was computed for each trial.

Results indicate that at least one SVM outmatched the neural network approach. The overall accuracy did increase from 80.7% to 87.1% by increasing n by one. Contrary to expectations, the increase of computational power by increasing the size of a neural network did not improve performance. It seems to be a paradox, which also concerned Li et al. (2005), as increasing data input reduced the accuracy. SVMs mispredicted ppt files as often as jpg files and vice versa that is an interesting behavior, which might indicate a related file structure.Different types of errors infer the conclusion that both algorithms found a unique way to solve the problem.

3.7. AI in cybersecurity

Artificial intelligence techniques are rapidly being introduced to produce advanced cybersecurity solutions. AI in cybersecurity enables the handling of huge volumes of evidential datasets enabling rapid threat identification; and to improve access control and authentication.

Traditional cybersecurity techniques involved ‘fixed’ software which are unable to adapt to dynamically evolving threats. As cybersecurity threats are dynamic and continue to change their appearance, it was a continual game of catch up where cybersecurity systems were incapable of identifying new threats. AI has the ability to continuously learn from its experience with new threat data to adapt to changes in threats.

AI applications used in cybersecurity include:

- Neural Networks applied to intrusion detection systems is capable of disclosing and analysing normal and abnormal behavior of system users. Solutions can be inferred from collected data without any prior knowledge of the ‘normal’ behaviours in the data. Once an attack has been recognized by a neural network, that type of attack will be prevented in future. Training data representing attack threats and normal, non-threat data is introduced to the neural network.
- Fuzzy Logic simplicity and flexibility make it an ideal technology to be used in computer security as the intrusion detection environment is undefined. One such technique includes a Bayes classification to classify system call sequences of privileged processes as ‘anomalous’ or ‘normal’. The system can effectively detect most intrusions with a low rate of false alarms.
- Genetic Algorithm when applied in intrusion detection systems, the algorithm will automatically update itself to detect new malicious activities. Genetic algorithms have been used to derive classification rules; or in the selection of convenient features while other data mining techniques are used to define the rules.
- Artificial Immune Systems used in intrusion detection are based on negative selection where the algorithm learns to differentiate between ‘self’ and ‘non-self’ resulting in anomaly detection. The algorithm is trained in a set of normal behaviours that form the exemplar patterns from which anomalies can be later detected.

The advantages and disadvantages of artificial intelligence based intrusion detection system are summarized as follows [20]:

Technique	Advantages	Disadvantages
Neural Networks	• Effectively classifies unstructured network packets • Multi-layers in neural networks increase classification efficiency	• Requires long training phase • Requires large number of training samples • Less flexible
Fuzzy Logic	• Better flexibility to some uncertain problems	• Detection accuracy is lower than neural networks
Genetic Algorithm	• Selects best features for detection • Greater efficiency	• Complexity • Greater specificity at the expense of general approach
Artificial Immune Systems	• Excellent detection accuracy	• Requires many parameters

3.8. Malicious patterns in android applications

Mobile malware programs increased by 24 million from 2018 to 2019. In 2019 companies spent on average 2.4 million USD defending against malware. Main goal of research is to apply Natural Language Processing (NLP) techniques for finding malicious patterns in Android apps. Different NLP techniques can be used depending on the task and data involved. For example, to detect spam in email, relevant words or set of words specific to spam are extracted. Previous research has used a combination of NLP techniques to build models, such as N-gram sequences and TFIDF (commonly used technique for selecting important features from a set of extracted features) values. An NLP model of an intermediate representation (MAIL) of Android apps to analyze and detect malicious patterns in them is presented [21].

The system first converts an Android APK into a jar file using the tool DroidNative. This jar file contains all the Java classes, i.e., the structural and behavioural functionality of an Android app, in a compressed form. These bytecodes are extracted from each class and converted into a MAIL program. MAIL is an intermediate language that can be easily translated into a string, a tree, or a graph. It can be used for various analyses that is required to detect malicious patterns in an Android app.

These analyses can be a combination of pattern matching, data mining, and applying NLP techniques. A MAIL program can have multiple execution paths (control flow patterns, or MAIL CFG Paths) These paths are built up for each function in the program. MAIL CFG Paths are built for each function in a MAIL program as described above. NLP techniques reduce the words into their base/root and use the abbreviated MAIL Patterns as words for each block.

In NLP a similarity index is built to compute similarities across a set of documents. It is like a new sample equivalent to any of the samples in the corpus up to a threshold. The similarity index is used to build a model that helps to find similar malicious patterns in Android apps. The similarity index SIMP is used to find if a new sample is a malware or benign. SIMP contains tokens (important feature vectors) of malware samples. A similarity score, using the Cosine Similarity, is computed as follows.

A commonly used matrix to evaluate and visualize the performance of a binary classifier is a confusion matrix. The true positive rate is the percentage of samples correctly recognized as malware out of the total malware dataset. Two experiments, 80–20 and n–fold cross-validations, were performed to assess the performance of the model. The similarity indices of the training samples were built, already labeled as benign or malware.

The SimScore of each of the testing samples was computed, not yet labeled, i.e., unknown samples. This allowed the computation of the true positive rate, false positive rate, accuracy, and Matthews Correlation Coefficient (MCC) of the proposed model. Python was used to implement the model, which is slower than most of the compiled languages. The model achieved almost the same results when tested using both (5 and 10 folds) the cross-validations.

The proposed model excels at detecting previously known malware variants, but will only detect a zero-day (totally unknown) malware if the malicious patterns found in the new malware are similar up to a threshold to an existing malware sample. Compressed or encrypted Android apps (Java bytecodes) will not be correctly analysed. If an app requires the download of malicious code upon initial execution (i.e., dynamic code loading), such apps will also not be properly analysed. The proposed model outperforms many other comparative models achieving a true positive rate of 94.8% and false positive rate of 0.3%, with an accuracy of 97.22% and an MCC of 0.94.

3.9. Ransomware dataset

Encryption and file operations of ransomware cannot be hidden because they are the most important means to demand ransom. The authors have collected dynamic behavioural features of storage access patterns for the new dataset. The proposed dataset is one of the few open datasets consisting of dynamic features of ransomware [22].

The lack of a standard and realistic open dataset has made development of such components slower and harder. A few open datasets for dynamic analysis of ransomware have previously been released. The dataset contains dynamic features extracted from packet capture data of ransomware. The developed hypervisor can be employed on other operating systems by design. The proposed hypervisor-based method obtains ransomware behaviors without using any agent programs. Attackers can detect the presence of a hypervisor by using specially crafted fuzzing test-cases to verify whether the CPU is properly virtualized or not. The most important artifacts related to ransomware behavior are on an operating system, network, HDD, and other subsystems.

The differences in CPU architecture make static analysis difficult and increase the need for malware detection using dynamic features. Other approaches include a behavior-based malware detection approach that uses compression-based mining on quantitative data flow graphs to increase the detection rate of malware; and a real-time detection system that uses users' finger movements as a dynamic feature.

RANSAP is a new open dataset of ransomware storage access patterns that aims to solve the problem of the scarcity of realistic open datasets for dynamic analysis. It employs a hypervisor to capture ransomware's storage access patterns since it is operating system independent, and the developed thin hypervisor can watch these patterns on any operating system with minimal observer impacts. The new open dataset covers storage access patterns of ransomware and benign software, varieties of ransomware, different operating system versions, and storage devices with full drive encryption enabled. The dataset was reviewed using a prototype feature extractor, and the outcomes of a machine learning-based ransomware detection system were analysed under different situations. Experiments validated the average F1 score of 96.2% for ransomware detection, 94.1% for variant detection, 81.8% on a different version of an operating system, and 31.0% for storage devices with the entire disc encryption capability activated. Even though the new dataset has a few limitations, such as performance degradation on mixed access patterns of multiple applications and a lack of access patterns for network-based storage services and the most recent operating systems, the RANSAP dataset is one of the few realistic open datasets with dynamic features for training machine learning-based ransomware detection systems.

3.10. Ransomware detection

The proposed methodology is basically a multi-level ransomware detection framework, which comprises six major components: DLL tracker, Function call tracker, Assembly instruction tracker, Detector engine, Action engine, and Passive analyzer. The framework is run in an active mode so as to analyze the given binaries at three levels. Details of each major component is described in below sections. The detector engine works in two phases: Feature generation and Machine learning prediction. The ransomware and normal executable were reverse engineered using the Portable Executable parser tool and Object Dump Disassembler [23].

The loader consists of OS loaders and dynamic link libraries, which resolve references to the code to become a running executable. The multi-level extractor tool collects the dynamic link libraries (DLLs), function calls and assembly instructions used in a sequence for a given sample from the processed data of the pre-processor. A DLL is a library that contains code and data that can be used by more than one program at the same time. The main benefit of DLL is code re-usability and efficient memory usage. Natural Language Processing (NLP) has proved useful in recommendation systems, text classification, speech recognition and more.

In this paper, the authors have exploited some popular concepts, but applied to a unique problem domain of multi-level analysis model of ransomware detection. NLP schemes are composed of three components: N-gram generation, n-gram probability and term frequency and inverse document frequency (TF-IDF). N-gram sequence is the number of occurrences of particular n-gram sequences in a binary sample. DLL, function call and assembly instruction sequences are processed as part of the training and test datasets. Processing millions of assembly instructions takes polynomial time when using a traditional programming approach so the authors adopted a big data computing framework and used Apache Spark to train and test the labeled dataset. Supervised machine learning classifiers were used for training and evaluation of the models.

3.11. Performance of machine learning malware detectors

1. Machine Learning algorithm accuracy for N-gram probability at the DLL level
2. Machine Learning algorithm accuracy for N-gram probability at the function level
3. Machine Learning algorithm accuracy for N-gram probability at the assembly level
4. Logistic regression accuracy evaluation for N-gram TF-IDF at multi level.

The accuracy is found to be in a decreasing order while increasing the value of N. At the function call level, the highest accuracy is 93.25% at N = 2 for logistic regression classifier and SVM follows with 92.16%. A similar trend is observed in the assembly level where 80.24% is the best observed detection accuracy at this level.

3.12. Analysis of top 10 trigrams at different levels for ransomware and normal binaries

Trigram sequences with score 1.0 signify the surety of that particular sequence to be called in order. For example, kernel32, user32, advapi32 has a score of 0.40 in ransomware samples whereas the trigram sequence is different with different score for benign samples. The accuracy graph for n-gram TF-IDFs shows that the accuracy is found to be inversely proportional to the value of N. Among three levels, function call achieved improved high accuracy. There is a steep decrease in accuracy for DLL level. It is claimed that these distinct sequences built the unique feature set to achieve high detection rates using different machine learning classifiers.

3.13. Darknet markets

Dark Net markets are collections of Dark Net (DarkWeb) websites that function similarly to other online platforms facilitating trades, such as eBay or Amazon. Users' anonymity is the main feature distinguishing DarkNet markets from traditional e-commerce platforms. During the COVID-19 lockdowns, the "usual" places (streets and clubs) became inaccessible, increasing DarkNet market's attractiveness. Most DarkNet market trading is concentrated in a small number of countries with high numbers of drug end-users. There have been cases where law enforcement agencies have been able to shut down the DarkNet markets by using traceability, but it is not a repeatable or standard process.

There is interest in studying the drug trade preferences of new or potential users. ClearNet forums is a useful starting point for studying drug purchasing on DarkNets. Topic models can be used to infer latent topics from unstructured text in different domains. Since cryptocurrency is the only payment method on DarkNet, it can be assumed that the observation of the influence and consequence of the preferred cryptocurrency will provide insight.

Cryptocurrency usage is one of the few links between buyers and sellers on DarkNet. Potentially, it is possible to influence an illegal online drug sale through cryptocurrency regulation. The goal is to understand the evolution of the preferred cryptocurrency for DarkNet sales. Understanding the drug users' reaction through the forum's posts would shed light on the deterrent effect of the traceability announcement and the privacy update if any.

Illicit cryptomarkets share many common features with licit online marketplaces, but are distinguished by two anonymizing features: 1) cryptocurrency (usually Bitcoin) and 2) the Tor network [24].

The study by Tsuchiya and Hiramoto (2021) [25] examined trends in the timing of illegal transactions (illicit drugs) from darknet markets. They traced Bitcoin addresses associated with the six previously leading and most active cryptomarkets (Silk Road, Silk Road 2.0, Agora, Evolution, Nucleus and Abraxas) to identify the specific timings of the transactions.

They found most transactions take place at night in European countries (specifically Germany, Netherlands and UK), the United States, Canada and Australia, locations in which the crypto markets are most active. Most transactions occurred on Mondays through to Wednesdays and fewer on the weekend.

They also found that a specific policing effort (Operation Onymous [26]) displaced users among the market places but did not deter their activity, even in the short term, nor change their usage pattern. Further, the operation did not alter users' transaction patterns. This is consistent with previous findings.

Once a marketplace has received the Bitcoin for an item (goods or services) of value, the purchased item is shipped and the marketplace takes a commission and sends the Bitcoin to the vendor. The Bitcoin addresses owned by the online market are likely to be publicly revealed because administrators send information of their Bitcoin addresses to users in escrow. Some Bitcoin addresses owned by online markets are publicly available [27]. The known addresses can then be used to search for unknown addresses owned by the marketplaces by using the features of internal transactions such as the known amount of Bitcoin transacted [28].

3.13.1. DarkNet drug trade

On ClearNet, some forums exist where experienced and new DarkNet marketusers (DNMs)interact. r/darknet was chosen for this research project because of its size (203,000 registered members) and the length of time it has been in operation (it was created on December 26, 2009). The data was collected from January 1, 2012 to December 31, 2019. The number of posts and comments on the DarkNet forums grew substantially in the last years. The manual analysis of the forum indicated that the new users identified themselves as "newbie," "noob," "new," "beginner," or "n00b". The researchers developed a program (using flashtext) to retrieve the aforementioned keywords' posts. After obtaining the datasets only with new users' posts, CorEx was applied to identify prevalent topics [29].

"Security" and "DarkNet market payments" topics were the most popular discussions in 2019. One of the possible reasons for the "Security" topic's spike in 2013 could be the "Silk Road" shut down by the FBI. Since in the realm of DarkNet, the cryptocurrency is of interest only as a payment method, it was hypothesized that these comments were answers to the question of which cryptocurrency is best for buying drugs. VADER was applied to analyze the evolution of forum users' sentiments towards cryptocurrency-related topics for which it was known that only two cryptocurrencies: Bitcoin and Monero, were discussed.

Starting from 2017, the change in sentiment in both cryptocurrencies was traced to test the hypothesis of shifting preferences. Analysis suggests that the DarkNet market users recommended using Monero instead of Bitcoin. In 2012, the "Security" topic occupied only 20% of all topics on Dark Net forums. In 2013, the percentage was 67.7%, probably due to shut down of "Silk Road". After the Monero privacy upgrade in 2017, the percentage increased from 18.9% in 2016 to 53.18% in 2017. Analyzing the "Illegal products" topic, it was observed that the traceability announcement impacted it.

Monero's privacy update was discussed on the forum and gave another tool for avoiding surveillance. New users were less interested in the "Security" topic than all users in general. Probably, it was due to the common knowledge that first-time purchases, especially in small quantities, would not lead to sanctions. The second most popular topic, "DarkNet market discussion," was related to the Dark Net market functionalities. The most popular topics in the new users' datasets were "Security" and "DarkNet market discussion".

The subsequent spikes were at the time of media reports about DarkNet market shutdowns. According to a self-selected online review of almost 4000 respondents, 38% had completed a university degree. The founder of the "Silk Road" had a master's degree in material science and engineering. This point and the users' demographic suggest they are competent in utilizing technology to continue the illegal online drug trade.

4. Blockchain

After Satoshi Nakamoto proposed and developed Bitcoin in 2008, the blockchain, Bitcoin's underlying technology, garnered considerable attention from academia and society. People gradually grew acquainted with the characteristics of blockchain technology, such as decentralization, security, and accessibility. In academia, there is currently no consensus on the nature of blockchain, however there is a widely accepted word. Derived from Bitcoin's distributed technology, blockchain is essentially a new application paradigm that encompasses decentralized terminal transmission and cryptography, mass data storage, and other computer technologies.

The three-layer architecture is one of the most representative models of blockchain architecture. Any blockchain architecture model may be loosely broken down into the following five steps: 1) new transaction initiation, 2) P2P network dissemination, 3) node verification, 4) passing verification and network-wide broadcasting, and 5) transaction writing.

As the research progresses, a preliminary examination of a number of crucial blockchain properties has been conducted in a few specific domains. In addition to the financial sector, which is the birthplace of Bitcoin, blockchain technology is currently used in public affairs management, electric power, transportation, and logistics.

Blockchain is defined as an open, distributed ledger that can record transactions between two parties in an efficient, verifiable and permanent way. Specifically, distributed-ledger technologies are digital systems for recording the transaction of assets in which the transactions and their details are recorded in multiple places at the same time. Distributed ledgers have no central store or administrative functionality. Each node processes and verifies all data generating a record and creating a consensus of veracity. User authentication is based on cryptographic proof and stored on physical devices [30].

4.1. Blockchain applications

Blockchain applications are being developed for government use in the areas of digital identity, storage of judicial decisions, financing of school buildings, tracing financial transactions, marital status, e-voting, business licenses, passports and criminal records. Blockchain can reduce costs and complexity, share trusted processes, improve discoverability of audit trails and ensure trusted book keeping. The blocks in the blockchain are 'lots' accompanied by the dates and times of valid transactions. The creation and incorporation of a new block to the blockchain requires a processing effort to solve the proof of work involving complex computing but can be easily checked by other users. Each block contains the hash of the previous block which identifies information and ensures data integrity. As each block contains the hash of the previous block, an interdependence is created for each block in the chain.

There are three types of decentralized ledgers:

- Permissioned private ledgers in which reading from and writing to the ledger can only be performed by permissioned private participants, which provides transparency of transactions and transaction validation for the permissioned participants only:
- Permissioned public ledgers in which anyone can read from the ledger, therefore providing transparency of transactions to the public, but only permissioned participants may write to the ledger and validate transactions among each other; and
- Distributed, unpermissioned or permissionless ledgers in which anyone can take part and provides full transparency and access.

Some digital evidence is short lived and available to be visualized for a short, finite period of time. There is a need for an easy-to-use tool to be made available on the Internet that allows lay people (especially victims and witnesses) to take snapshots of certain facts (evidence) in a way that serves the needs of the justice system (criminal and civil). The evidence should be probative and admissible in a range of jurisdictional court systems. A blockchain-based platform is one such method so that the immutability of the evidence is guaranteed [31].

Photo-documentation by health practitioners benefits patients, the justice system and third parties, by enhancing and reinforcing written descriptions and hand-drawn body diagrams. However, health practitioners hesitate to use digital files for documentation purposes due to concerns less-standardised aspects of digital evidence application and management.

The creation of digital evidence requires skills that are uncommon to the medical community, such as the use of professional camera or training in specific software. Then, the storage, retention and management of the digital files will be subject to the less-disadvantageous (or most convenient) means which are most likely the less secure. Further, digital file submissions will involve consultation and coordination with different agencies, including police, courts, the patient and myriad other stakeholders and interested parties. The complexity presents ethical issues, legal responsibilities and technical problems; before even considering chain of evidence and data protection.

Healthcare professionals collect evidence during their clinical practice, including circumstances of domestic violence, suspected ill-treatment, physical abuse, physical abuse, sexual assault, injury while in police custody or their activity as pathologists. The evidence, even if not initially collected for this purpose, must be authenticated by the witness (health professional) who attests to its accuracy through chronological documentation of sequence of custody, control, transfer, analysis and disposition. The authentication process necessarily excludes the possibility of tampering or alteration.

The international forensic legal community has not reached a consensus regarding digital evidence custody and sharing. Current guidelines, as an alternative to hard copies, recommend uploading images to a secure system involving encryption, passwords and PIN codes. The initial file is regarded as best evidence and subsequent copies are regarded as working copies. Whenever the best evidence is released to other parties to the case, the chain of custody must be updated. The usual method for assuring integrity of the files is through the application of hashing techniques which is widely practiced in law enforcement but is not commonly used in healthcare.

Current chain of custody systems require a verifiable, uncompromised computer system with a secure operating system.

An alternative proposal is for evidence images to be encrypted on loading to a computer which immediately uploads the files to online storage. The cryptographic key is stored on a device that is available to all users together with the user's personal cryptographic data. The user private key is stored in a tamper-resistant hardware module that is secure against hardware attacks and computer viruses; and protected with a personal PIN. Such devices are commercially available. Only authorized users in possession of the device with their private key can decrypt and access files.

The user creates a case on the blockchain to which it adds multiple files. An identification code is generated for each file and for the case referring to which the files pertain. User notes can be stored online with the case along with the file metadata. Administrative rights are held by the supervising physician who can authorize viewing rights to other users. Importantly, no matter who is granted access, the stored files are unmodifiable, each file's hash is stored on the blockchain and user access is recorded on the blockchain.

The burden of correct evidence storage and handling is shifted from medical professional to the blockchain administration, where access is only granted to authorized users. Information sharing becomes safer and more transparent for peer review, obtaining second opinion and promoting independent interpretation for which additional reports can be added.

Ethereum claims to hold applications other than cryptocurrencies such as real estate, voting and small business contracts [32].

Blockchain technology comprises three key elements in the design and implementation:

1. Timestamping which enables the avoidance of double spending in cryptocurrency transactions. Timestamping is achieved by collecting pending transaction into the block and then calculating the hash of the block, therefore, the transaction existed at the time of creating the block as the timestamp is hashed into the block.
2. Consensus agreement of newly created versions of blocks by all nodes. The distributed consensus assists in the decision on which block out of several variants generated by different nodes would be added to the blockchain.
3. Data security and integrity preventing a malicious code from creating a fake transaction since each transaction is signed with a private key by a node or user.

   One model for IoT forensics focuses on system and event logs with the entities in the system being cloud service providers, network devices and the IoT devices. The entities serve as blockchain nodes in the network. New nodes are added to the network through a key generation process. The public key is appended to a transaction before it is written onto the block. The cloud service providers act as miners in the network. The model comprises a blockchain centre (BC), log processing centre (LPC) and user centre (UC).

- Blockchain Centre comprises a distributed ledger where each log is written into a block after processing. Each block contains a transactional value of hashed values computed from logs. The logs are extracted from the various entities, hashed and written onto the blockchain network as transactions.
- Log Processing Centre is an API that sits between the entities and the blockchain network. The LPC extracts the logs from the IoT devices, network devices and cloud layers. The extracted logs are hashed as SHA-256 and the hashed values are written onto the block as a transaction.
- User Centre comprises the judicial system and the forensic examiners. The user centre enables the forensic examiners to authenticate the logs presented by service providers and to authenticate the downstream passage of logs from one person to another in the chain of custody. The court can authenticate the logs when presented as evidence.

The digital evidence of IoT is heavily dependent on evidence provided by cloud service providers which can lead compromised evidence.

4.1.1. *Chain of custody using blockchain*

Chain of Custody (CoC) documentation is used to keep track of provenance information for forensic purposes. Using a cryptographic hashing function to authenticate the integrity of digital evidence is the most prevalent method. Unless a secure tamper-evident method is in place, a dishonest individual can alter the digital evidence and related hash value in the future. Chain of Custody e-CoC ledger is a solution to the rising demand for reliable, scalable, and automated digital evidence verification. Both public and private blockchains offer scalability and automation; there are no restrictions on the amount of blocks that can exist, and the blocks can be worked on programmatically [33].

Public blockchains are decentralized, allowing anybody to monitor the data recorded and access the blockchain. A private chain restricts access to only trusted individuals, making it more acceptable for use in criminal justice and other contexts requiring sensitive data. In legal scenarios needing a stronger chain of custody, public blockchains have a crucial role to play. A deletion or modification of a block would be quickly detected due to the invalid reference in the subsequent block. A CoC system that relies on biometric information necessitates a database of everyone who will deal with the data, which is impractical and presents data protection issues. Unlike public blockchains, however, the e-CoC ledger deployed is not decentralized.

The solution is designed for use by attorneys, decision-makers, and forensic practitioners, but can also be used to other forensic disciplines. This study expands on previous work that used a trusted entity to strengthen e-CoC by utilizing public blockchain to secure certain blocks. As soon as forensic experts acquire the evidence, they immediately calculate its hash values on the local machine. In addition, an e-CoC solution must retain its own integrity and the data it includes.

The secure e-CoC ledger is constructed of blocks, each of which corresponds to a record of an item of evidence. The first attribute is the previous hash, which serves as the block's index. It permits the block to be connected to the preceding block if its hash value matches that of the prior block. The salted hash values are then represented as hexadecimal values. The timestamp of the hash values follows, followed by the receipt number and the value of the public attribute.

Each block in the e-CoC distributed ledger includes a unique hash value. The value is the block's previous hash attribute. This element holds the name or identity of the chain used to extract the item from the public blockchain, as well as the ticket number. Each block that is sent to a public or private ledger is accompanied by a QR code containing a URL. If no such block has been sent, the secure ledger can verify the blocks' integrity without public verification if no such block has been sent.

For each block, the entire block's hash value is calculated and compared to the previous hash. This procedure is repeated for each block. Identical values indicate that the evidence has not been modified after its timestamping in the e-CoC ledger. AFF4 is a solution for encapsulating metadata that strengthens chain of custody. To illustrate how readily the e-CoC solution proposed in this study may be linked with current tools, the open-source AFF4 was chosen.

Using an Application Programming Interface (API) to the implemented e-CoC solution, any AFF 4 acquisition can automatically generate a blockchain entry and receive a PDF receipt. The provided e-CoC solution can also be readily wrapped around current tools without requiring their modification.

The greatest threat is that someone edits a stored value in the e-CoC ledger, such as the timestamp and hashes, which would break a link in the chain required for integrity verification. When a block is modified, its integrity as well as the integrity of the blocks that precede it cannot be checked. However, additional blocks added after the modified block are unaffected by this change. An attacker might theoretically edit a block of interest, as well as the previous hash and hash characteristics of subsequent blocks until the end. Due to the immutability of the value stored in the public blockchain, the difference would be discovered.

When evidence is timestamped, a new secure ledger will be established if the e-CoC ledger is destroyed from the server. This would send an email to the system administrator informing him that there is an issue. It would be prudent to send at least one block per day to prevent this from occurring. The content of the QR code contains the index of the block, the value of the salt, and the true values of the hash. The e-CoC solution contains no sensitive data.

Since it is impractical to retrace the hash's origin, the hash values are typically not sensitive information. However, an attacker may wish to determine whether a specific file has been discovered by law enforcement. Despite the fact that such an assault would not modify the secure ledger, it should be avoided nonetheless. Human verification will ensure that it was recovered from the block and not the URL contained in the QR code. In addition, there is a receipt number, which is solely saved in the e-CoC solution and printed on the receipt, and which simplifies the tracking of the receipt.

In cyber investigations, the custody chain of digital evidence is of paramount importance. The use of a hash value is insufficient to guarantee the integrity of the evidence, as it does not indicate when the hash was produced and could, therefore, be manipulated. This study presents a way for timestamping the hash values of evidence through an e-COC ledger administered by a trusted organization. This electronic CoC ledger employs blockchain technology to avoid unnoticed changes.

Moreover, some blocks are forwarded to a secure public blockchain in order to lessen the impact of a hypothetical alteration to a single block of the e-CoC ledger, as the public blockchain ledger is immutable.

The independently verifiable chronological e-CoC ledger produced in this work serves as a foundation for future growth. As more legal matters rely on digital evidence, utilizing blockchain technology is a crucial e-COC reinforcement. The solution proposed in this paper is intended to be simple for forensic software developers to apply, to aid digital forensic examiners in making digital evidence court-admissible, and to enable attorneys and decision-makers to track the e-COC in a case. Ultimately, this work provides a framework for e-CoC that can be adaptable to a variety of situations, can be easily incorporated into current tools, can be implemented using a variety of technologies, and can be extended to include additional metadata and enhanced to provide new features.

4.1.2. *Provenance*

Increasing concerns about drug trafficking, steroid use, the manufacturing of chemical weapons, financial fraud, child pornography, and other illegal activities have changed the emphasis from inspections to investigations. International organizations that investigate the purported use of chemical weapons have a growing demand for forensic expertise. Financial service providers and regulatory bodies must disclose and investigate an increasing number of fraud cases. An independently verifiable and scalable provenance tracking system is necessary for managing and maintaining oversight of this rising amount of digital data [34].

Using a public trusted blockchain, a new tamperproof timestamped provenance ledger (TTPL) was created to meet this demand. This work contributes:

- Tamperproof—Changing the provenance record is difficult and creates an inconsistency.
- Integrity verification - Timestamped provenance records in the public blockchain can verify digital data
- Cross verification - PDF documents with provenance details that may be compared to the public blockchain provenance record to validate the integrity of the original digital data.
- Reverse verification—QR codes with minimal information to easily retrieve and decrypt provenance record information.
- Independent verification and proof of work—A technique to verify that the (potentially independent) verifier retrieved and encrypted provenance record information from the public blockchain.
- Data protection - No sensitive data is saved on system servers or in the public blockchain.
- As long as the public blockchain is scalable, provenance records can grow domestically and internationally.
- Automation, Standardization, and Interoperability - Automated submission and creation of timestamped provenance records in standardised format.

The proposed technique allows the originator to generate, using a web browser, a permanent confirmation that he or she had access to the (possibly sensitive) data D at time T. The proof is based on a timestamped provenance record anchored in a public blockchain. For reasons of security and privacy, data D is neither transmitted nor stored on the web server. Representing provenance is a crucial aspect of the community-developed endeavour called Cyber-investigation Analysis Standard Expression (CASE) (CASE). The TTPL record is not yet an official component of CASE and is represented by a custom property bundle.

Authenticity and integrity of original data can be checked using the hash values provided in PDF proof documents and QR codes. The returning LID has to be cross validated directly with the Hd in the provenance record. Time to validate a transaction is less than a minute, and transaction fees are relatively low. Authentication and integrity of original material is validated by retrieving the provenance record from the public blockchain ledger.

From this information, the date and time the record was produced can be identified. Using the Hg value, the LID (ledger ID) can be deciphered. This system offers independent integrity verification, is scalable, supports automation, and provides results in a defined format for compatibility with other systems.

4.1.3. *Tainted evidence and privacy protection*

A party can contest evidence during an investigation or in court, or the prosecutor can drop it. For example, Bob is suspected to possess may child pornography and his house is searched subject to a warrant. A hard drive is confiscated during the search, recorded and entered into a chain of custody; and registered into blockchain-based evidence inventory software. Digital forensics examiners find Alice, an alleged child pornographer, on the drive. Thus, a police search of Alice's residence yields a USB stick with a lot of incriminating data. The blockchain-based program registers the USB stick as required [35].

A defense counsel later questions the legitimacy of the first police search. The court dismisses the initial police search. The second police search, a direct offshoot of the first, is also dismissed.

When a blockchain is used to construct a chain of custody, the digital evidence found at Alice's and Bob's is recorded in the ledger, but there is no way to delete it because it is designed to prevent tampering, deletion, or cancellation. With this blockchain layout, there are at least two ways to reject transactions:

1. Delete and reissue the blockchain without the discarded evidence. It entails re-issuing all transactions from the root block (except the transactions linked to the dismissed evidence of course). Although theoretically possible, it requires a lot of transaction and block validation, voting algorithms, and tracking all blockchain intra references which has significant computational complexity; or
2. Issue undo-transactions to indicate that the linked transaction is void and unusable. The blockchain has two types of transactions: evidence-registering transactions and undo-transactions for discarding evidence.

Database Management Systems commonly use undo-transactions for recovery or rollback. However, it causes complications in blockchain-based systems.

Transaction validation is the main issue. A user must check if the chain of hashes and signatures has not been broken since a certain period to validate a transaction. The transaction was entered accurately and validated according to the rules. This check does not prove that the transaction is legal because the evidence may have been thrown out afterwards. Thus, the check procedure must continue until it either detects the undo-transaction or reaches the end of the blockchain. This check requires more work than blockchain's single transaction verification protocol.

The authors propose AccessTX which gives blockchain access to InventoryTX, the inventory blockchain. Before allowing access to InventoryTX, the additional layer will verify that a transaction is legitimate. After checking, InventoryTX will validate the transaction. Access control will employ InvalidatedTX, a blockchain, to verify transaction legality. InvalidatedTX transactions include corrupted evidence transaction IDs. The jurisdiction removing contaminated evidence should sign each InvalidatedTX transaction. Since the root of InvalidatedTX, each invalidating transaction is validated as a blockchain. Only the invalidating transaction distinguishes it from a blockchain.

An example may best demonstrate the solution's components. The police may search Ms. Marple's residence. This woman may host a fugitive. Her residence has three evidentiary items:

1. Agent Poirot found a USB drive containing the searched man's identity documents and 1000 bitcoins
2. Agent Ness found a notebook with pornographic content and a web server linkage
3. Agent Loch found a love letter from the suspected man to Ms. Marple;
4. Agent Chris later finds drug recipes on the website and InventoryTX blockchain is built.

The defense claims pornographic materials and drug recipes were not subject to the search warrant. Judges Roy and Prince agree with the defence and update the InvalidatedTX blockchain.

Accessing InventoryTX evidence is legally sound. Three scenarios follow:

1. If the transaction hash is absent from InvalidatedTX but present in InventoryTX, the system will serve the transaction payload, usually a reference to a safe storage entity containing the evidence content or description.
2. The system will output a "Transaction not found" error if InvalidatedTX and InventoryTX lack the transaction hash.
3. The system will output a "Transaction invalidated by court order #xxx" exception if InvalidatedTX contains the transaction hash.

This system's advantage is its light weight. The technique for rejecting tainted evidence will prevent parties from using it, but it will not erase its history. This algorithm's evidence management flexibility may help blockchain solutions wider adoption. Since it doesn't change blockchain structure, this technique works with most blockchain implementations. The evidence data is isolated from the blockchain transaction's metadata payload.

4.1.4. BlockQuery

The following requirements must be met for a cryptocurrency examination to be forensically sound:

- Completeness: Given a public key or wallet address, any transactions made with the key or address may be retrieved.
- Integrity: The blockchain ledger being queried matches the version currently approved by the consensus network.
- Confidentiality: Information about which transactions are pertinent to the examination is not shared inadvertently [36].

The vast majority of publicly accessible tools for querying blockchains of cryptocurrencies do not meet these conditions. By keeping a comprehensive duplicate of the ledger, forensic examiners can ensure the accuracy of the data they are examining. BlockQuery, a blockchain query system, is able to locate transactions made by Hierarchical Deterministic wallets that many publicly accessible tools cannot find due to shortcomings in their address derivation techniques. Extended keys are golden tickets for associating diverse transactions with a single starting point.

The principles presented by the authors are relevant to cryptocurrencies other than Bitcoin, such as Ethereum and Litecoin, which have implemented compatible derivation. Each address type has a unique extended key representation that is used to derive addresses of that type; nevertheless, these extended key representations are easily convertible. This means that all potential wallet addresses can be derived deterministically from any non-hardened extended public key representation. A practitioner unfamiliar with Bitcoin address derivation may overlook significant chunks of forensically significant transaction history.

Most social media platforms share data centrally, however social network users' social graphs contain private information that can reveal their identities. In 2018, a poll suggested decentralized social networks to address privacy concerns. Network traffic analysis can partially map IP addresses to Bitcoin addresses.

Researchers have used Bitcoin relay traffic to deanonymize Bitcoin users at the IP level. Other methods scraped Bitcoin addresses from public forums and connected people to incomplete transactions. Blockchains are decentralized peer-to-peer pseudonymous networks where everyone may view transactions between users. Attacks on blockchain-based cloud storage network StorJ were explored with the results showing that such networks may jeopardize data privacy after storage.

The xpubscan utility of Ledger was the only tool capable of locating all of the transactions made with the query-supplied extended public keys. This is because xpub-scan generates Legacy, Native SegWit, and Nested SegWit addresses regardless of the specified key format.

In addition, the command line interface permits the user to manually alter the index range, enabling the identification of transactions that exceed the address gap restrictions specified by the standard. The program is similarly open source; however, it requires Ledger's servers to search the blockchain, and while there is an option to use cryptoapis. io as a custom data provider, information leaks cannot be prevented. None of the other technologies were capable of locating any Ledger Live transactions or addresses with abnormally large derivation gaps.

None of the evaluated tools were created with forensics in mind. Not only did six of the seven tools fail to automatically derive SegWit addresses when presented with an xpub, but several of them also failed to identify SegWit transactions when presented with the right ypub or zpub. Similarly, only two of the seven examined technologies permitted users to query local blockchain instances as opposed to third-party services. The lack of a publicly accessible tool matching forensic appropriateness requirements demonstrates the need for a dedicated open source solution. The proof of concept effectively uncovered all transactions while preserving the privacy of the searchers by avoiding the use of third-party APIs.

The query interface that allows the user to manually set the derivation depth and determine whether to derive along the internal chain, external chain, or both. Users may also command the application to re-query the indexer for a cached public key in order to check for fresh transactions. The remaining views display a relational database model that enables users to traverse through the links between keys, addresses, and transactions.

Operating a sophisticated, forensically sound cryptocurrency query platform necessitates considerable resources. At the time of writing, the Bitcoin blockchain was roughly 350 GB in size, while the Ethereum blockchain was approaching one terabyte. Similarly, the computation of all 231 potential addresses for a given extended key would necessitate a machine with significant parallel processing capability. For a local law enforcement department with insufficient resources, this may be an insurmountable obstacle.

In this situation, hosting may be provided by reputable groups, such as state and federal law enforcement agencies or universities. Consequently, forensic investigators who lack the technical expertise or finances to operate their own node can query a third party without jeopardizing the secrecy of their inquiry. Individual components can be managed by a variety of trusted organizations, making microservice-based architecture a good fit for this approach.

When creating and developing digital forensics tools, the technological barrier a user must overcome to efficiently use the tool is a significant issue. Not all investigators are expected to comprehend the complexities of Bitcoin address generation. Therefore, digital forensic toolkits must account for typical edge circumstances and interpret the user's intent broadly to ensure that all conceivable results are accessible. This design philosophy inspired the development of BlockQuery. By carefully converting and deriving all conceivable address representations, it is possible to retrieve the same data with an expanded public key. This, however, needs an in-depth comprehension of esoteric derivation rules and may be hidden from the user. An effective solution would permit an investigator to simply enter an artifact obtained through forensic investigation and receive the whole transaction history linked with this public key.

Extended public keys are beneficial for forensic investigations. During the development of BlockQuery, the absence of an open-source extended key dataset was discovered. An expanded public key dataset could be used to analyze the minor departures from the norm in various deterministic wallet clients.

4.1.5. Electronic evidence generation

By way of judicial interpretations, the definition of electronic evidence varies among nations and regions of the globe. According to the Supreme People's Court of China, electronic evidence can be separated into two categories: a limited sense and a broad meaning. The EVIDENCE Project defines electronic data as any data of possible probative value generated by, processed by, stored on, or communicated by any electronic device. In a significant number of cases, electronic data has served as the most crucial evidence. Nonetheless, a large number of instances illustrate, to varied degrees, the issues associated with electronic evidence [37].

The main disadvantage is that electronic evidence is difficult to gather and analyze. Some courts employ a transformative application program in order to effectively use electronic data. This technique renders electronic evidence, a sort of independent evidence, dependent on other types of evidence. Emerging in forensic science and technology is the use of blockchain-enabled electronic evidence. Due to the electronic and data characteristics of electronic data, it is difficult to identify frequent instances of data modification and deletion.

Distributed data storage characteristics, including peer-to-peer transmission, consensus processes, and encryption algorithms, provide significant practical benefits for maintaining the security and integrity of data. If digital evidence is put to the blockchain, it cannot be altered or removed. In this manner, the validation of the authenticity of electronic evidence can be substantially strengthened. The temporal succession structure of blockchain provides extra information to the preservation of electronic data in the forensics and examination sectors of the justice system.

The preservation of electronic evidence in the judicial field, such as forensics and examination, is enhanced by blockchain technology. Electronic evidence can be timestamped to ensure the integrity and validity of electronic data and enhance the authentication of evidentiary skills of electronic evidence. Two factors contribute to the significance of the network's independence: 1) Data processing at each node is independent, so ensuring the independence of the judiciary; and 2) All departments in all locations handle electronic data when interdepartmental and interregional cases occur.

4.1.5.1. Technical analysis of existing blockchain-enabled electronic evidence cases. In a legal proceeding in Hangzhou, China, blockchain technology has been acknowledged as admissible evidence. In the same year, the Supreme People's Court of the People's Republic of China also acknowledged blockchain-enabled electronic evidence in its decision on Internet Courts. According to the judgment, the process of becoming blockchain-enabled electronic evidence can be divided into three parts: the generation of original block information in the case, the examination of the qualifications of the evidence preservation platform, and the credibility of technical means for obtaining evidence on infringing webpages, and the integrity of blockchain electronic evidence preservation. Factom is an American firm that uses Bitcoin's blockchain technology for data management and tracking. Preprocessing the generated electronic evidence using the SHA256 method is the most important step in uploading it to the blockchain.

For messages of any length, SHA256 generates a 256-bit hash value, known as a message digest. The digest is equivalent in size to a 32-byte array. When the new block was produced, the case information was recorded and could not be edited in the Factom blockchain. The judicial examination includes an in-depth technical review of the entire case and pertinent evidence examination methods. The blockchain-enabled electronic data becomes blockchain-enabled electronic evidence at that point.

The Hangzhou Internet Court recognizes the veracity of blockchain technology as a method for collecting evidence. There is no reliable structure in place to supervise and examine evidence from its origination to its application. A chain-based electronic evidence system overseen by court bodies is envisioned, which can encrypt and store a substantial amount of evidence in the blockchain.

4.1.5.2. Design and execution of applications for electronic evidence using a consortium blockchain. Some researchers believe blockchain technology has significantly more potential in the legal area. Early developments focused on storing and securing electronic evidence data but ignored judicial procedures. Turning electronic data into electronic evidence requires data security and the legitimacy of evidence examination and authentication procedures. Electronic evidence is collected, preserved, and examined by numerous departments. Based on blockchain legal cases, blockchain can preserve evidence.

P2P networks underpin all blockchains. In such a chain, each judicial body is an autonomous node and is bound by the judicial consortium blockchain's norms. The blockchain 2.0-based electronic evidence creation method allows reliable cryptocurrency transfers and distributed smart contract execution. Its built-in Turing with full programming language lets users build, deploy, and run smart contracts. The electronic evidence is the final chain data. Blockchain-enabled electronic evidence is fresh data derived from existing data. Early on, court organizations will use blockchain smart contracts to verify the authenticity and normality of original electronic materials. For transmission and storage, Interplanetary File System-stored original electronic materials reside on the cloud platform.

The legal system is suspicious of electronic evidence due to concerns over its authenticity. The data nodes in the consortium blockchain represent judicial entities. Block data becomes blockchain-enabled evidence after judicial review. The Ethereum-specific block information contains a lot of evidence concerning transfer transactions, including gas requirements and timestamps.

Smart contracts can self-execute, self-verify, eliminate data transmission interference, and promote judicial independence. The blockchain displays the transaction timestamp of the constructed smart contract. The timestamp information and transaction hash of every transaction can be checked simply and directly after testing. After approving "transaction" information, competent judicial agencies can use the private key to decrypt the storage location of original electronic materials for judicial scrutiny. Finally, image-based electronic evidence is authoritative and credible. The necessary judicial entities that have passed nodal verification on the consortium blockchain can also verify all procedures before the block information in the judicial consortium blockchain becomes electronic evidence with judicial meaning.

Electronic evidence can be handled by incorporating digital image watermarks and digital signatures. Watermarking encryption processes the image in this test. Algorithms automatically extract, examine, and validate watermarks, which is equivalent to an initial stamp confirmation of the original material and can minimize evidence examination expenses later. Attaching cloud storage location to transaction information in the consortium blockchain system transmits these images. The Peak Signal to Noise Ratio (PSNR) is an objective criterion for evaluating an image, which is a logarithmic value of the mean square error between the original image and the processed image.

PSNR values greater than 40 dB imply outstanding image quality. Because image definition, clarity, and detail affect electronic evidence probative force, all random pictures are in uncompressed BMP format to simplify the test. Blockchain-enabled electronic evidence is generated in a robust and secure information system with strong encryption and legal and normative procedures. It can withstand electronic evidence authentication procedures.

4.1.5.3. System performance benefits. Security – the semi-closed nature of the consortium blockchain system restricts access to internal information to just judicial nodes, thereby securing it. Elliptic curve asymmetric encryption technology is used to secure nodes (judicial bodies) or judicial staff identification verification, meeting the stringent privacy and internal supervision standards of the court system. The distributed storage blockchain system guarantees block information immutability, ensuring blockchain evidence security.

Stability – the system's performance is tested using the image as representative electronic evidence. The PSNR data test results suggest that the system can better ensure image quality on the blockchain and that the system is stable, viable, and dependable. To maintain system stability, a full-type evidence creation system needs additional sophisticated algorithms for development and verification. The probative force and evidential competence of electronic evidence depend on system stability.

Traceability – Blockchain timestamps reliably record block information. All operational changes from evidence collection to examination and authentication form a time series chain, making it easy to evaluate and authenticate evidence for hearing cases and legal procedures. The court system relies on immutability and traceability of electronic evidence.

The test findings suggest that this paper's consortium blockchain-based electronic evidence creation system has great security, stability, and traceability potential. The system also verifies blockchain data validity and integrity. Applying this technology to real life is ground breaking, but there are challenges. As an emerging technology, blockchain lacks technical rules and application standards. Despite blockchain's successes in relevant domains, technical catastrophes have occurred. Many application development techniques leave the system vulnerable to security threats. Thus, system enhancement and application development security must be investigated. Political systems, specific national conditions, and other variables affect the contemporary judicial systems in all countries and areas. Practical application requires improvement and optimization. Blockchain applications and development are still in their infancy. Blockchain's rapid development requires legal credibility improvements. Judicial enforcement is unique. Thus, applying and promoting blockchain in the judicial sphere will be difficult.

4.1.6. Smart contracts

Blockchain is considered to be the new Internet value layer adding reliability, transparency and traceability to any asset-class Internet transaction (information/data and physical assets) that can be authenticated, validated, tracked and recorded in a distributed, digital point-to-point accounting system [38].

A contract (an "agreement between enemies") is a document that ratifies an agreement of wills between the parties, in order to acquire, protect, transfer, modify, preserve or extinguish rights. Smart Contracts, or chaincodes, automate the execution of contracts using communication algorithms in a computer network with interfaces available to the parties. The algorithms execute when predetermined conditions are met so that all participants can immediately be certain of the outcome without any intermediary's involvement or time loss. Smart contracts also automate a workflow, triggering the next action when conditions are met [39].

Blockchain sequentially records on a single basis, using cryptography and consensus protocol among network users to determine which new information is valid and can be recorded. As new data is inserted in to the block, instructions can be triggered to perform a task, rules can be validated or disputes can be solved without the interference of or interested and third parties.

Smart contracts can be applied in a wide range of sectors including financial services, management, health and the Internet of Things. Smart contracts allow the creation of Decentralized Autonomous Organizations, organizational entities that do not have dedicated employees but allow the management of digital assets executing the same business policies of traditional organizations through functional contracting.

Within the justice system, smart contracts can be used for:

- Transparently record citizen's votes
- Intellectual property to prove the existence and authorship of a document
- Internet to reduce censorship
- Finance to transfer funds between parties without requiring banks as intermediaries
- IoT in the automatic processing of data from sensors and perform autonomous actions
- Education to store information about the qualifications of students to reduce fraud in the job application process.

Smart contracts can be used for the recording of digital evidence which enables the evidence to be made available in the blockchain network together with the application of human judgement, a necessary element of the judicial system. In this context, Smart Contracts are used to ensure the consistent application of rules and legal agreements.

The four principles to maintaining the chain of custody for digital evidence, based on the principles for the chain of custody for all evidence, are:

1. No action should be taken by any user which could change the content of the digital evidence;
2. In circumstances of access to original data, in case of change, it should be explained the relevance and the implications of such change;
3. An audit or record of events must be produced and preserved so that an independent third party may examine the evidence and reach the same conclusion; and
4. The persons responsible for the investigation must ensure the application of these principles.

Current digital evidence storage and management systems vary widely between organizations and are generally less than ideal potentially allowing nefarious actors to alter, conceal or even erase evidence. An improvement is a system by which safe access to the evidence is available to all authorized persons at any stage of the investigation.

Evidence from smart phones are ubiquitous in all investigations and enquiries, whether criminal of civil. However, evidence might be unavailable for a range of reasons. However, once the evidence is made available, it can be placed on the blockchain platform and can be accessed by the interested parties comforted in the knowledge that it is an accurate representation of the evidence without the possibility of tampering. Blockchain smart contracts can be used for the reception, storage, maintenance and use of collected digital evidence.

Using smart contracts for the management of digital evidence, which by default includes controls on the consensus and the restricted access, has the following advantages:

- Preservation of the evidence to form a robust, secure chain of custody that allows the reception, storage, maintenance and use by interested parties.
- Improved scalability, integrity and privacy.
- Maintenance and guarantee of individual privacy of the evidence.
- Participants in the blockchain network, i.e. those who have been given permission to access the evidence, can participate in the creation of the transaction, reading, analysing and auditing all processes.
- Enable for the digital evidence to be used in multiple processes, therefore allowing for the application of "loaded evidence".
- Provide speed to the execution of letters rogatory, an international legal instrument by which a country requires the enforcement of a judicial act to the court of another country specifically in accessing the digital evidence, cooperating with the procedural act.

Whenever a new document is added to the blockchain, a hash will be generated and stored in the smart contract. The hash can be used to access the document and the hash will change whenever any changes are made to the document.

4.1.7. Storj

Storj is a platform that allows individuals to store their data on rented hard drive space from people's computers around the world through a contract-based, blockchain. This brings up the old studied claim of "a trojan made me do it", where malware could have potentially created or downloaded illicit material onto a computer [40].

Storj is an open-source peer-to-peer (P2P) decentralized cloud storage network. Renters use Storj's Client application to interact with the network; allowing files to be uploaded and downloaded to and from the cloud. Farmers are users on the network that offer space for cloud storage. Before they can access the network they must ask the bridge for permission to join the network. A renter uploads a file to farmers on the P2P storage cloud. There are several steps involved in the process of uploading a file. The renter encrypts the file and then segments it into pieces called shards. The shards are then distributed to the farmer(s) on the bridge.

4.1.7.1. Frameup attack. A nefarious Storj renter can upload unencrypted files to farmers' computers around the world, potentially consisting of malicious software, contraband material, and other content with malicious intent. This is made possible by a renter disabling the encryption process prior to file segmentation and shard uploading. An informed attacker can leverage this design characteristic to increase the precision of their attack.

The authors built a live Storj storage network where all the components such as farmers, bridge, complex, and renter nodes can be experimentally monitored. They then created a clear-text file data set which included different types of documents and multimedia files. The optimized attack encapsulated the uploaded files in HTML to better survive the file sharding process. In the case of executable content, could be encapsulated in such a way as to execute on the forensic station.

A preliminary attack is the initial phase of the frameup attack. In this attack, modified versions of the Storj client were designed to revert back to the clear-text version of the original file upon upload. It was intended to determine if the content of the files could be found in shards and viewed on the farmer.

First, two farmer nodes were registered and made available for analysis of a test dataset. The clear-text files from the test dataset were then uploaded to the private Storj network. To reduce the workload, file signatures were leveraged for most of the shards. The majority of the shards were not recognizable. Only a few file types such as AVI, MPG and PDF produced relatively high executable rates. Even though the content of TXT files were found in the shards, it is possible for the data of one TXT file to be separated between multiple shard files.

Theoretically, even though the files with extra data inserted become corrupted, the data is not lost. Separation between two string variables occur near the locations where extra bytes are inserted during the sharding process. Almost all injected byte combinations (except for the extremely rare premature occurrence of '*/' that will end early) will be interpreted as meaningless text. A feature was added to handle file types that are not suitable for display in Internet Browsers. This is so the base64 encoded data can be decoded into the original file format and be displayed on the HTML page.

The file restoration technique was applied to the following file types: AVI, FLV, MOV, MPG, DOC, XLS, PDF, ZIP, GZIP and BZ2. This technique could also be used to upload files larger than the 4 MB shard size limit imposed thus far. The clear-text files were converted to their proper HTML equivalents and uploaded to the private Storj network. To test whether the embedded file can be displayed or downloaded on the browser in this manner, all the shards on the two farmer nodes were collected and the extension of the shards changed to '.html' and attempted to open them with IE. On average, more than 55% of the uploaded files can be located and recovered by executing the shard files.

4.2. Attack evaluation with FTK

The FTK testing revealed the following attack benefits and drawbacks:

- Preliminary attack:
  - o Benefits:
    - ▪ As long as a forensic tool such as FTK is used, there is no additional step for investigators to locate the clear-text file.
  - o Drawbacks:
    - ▪ Works only for relatively tiny clear-text file sizes
    - ▪ Relies on the data carving function of the forensic tool, which may not support all file types of interest by default
    - ▪ Despite the fact that some shards are valid for the attack, their integrity cannot be assured
- Optimized attack:
  - o Benefits:
    - ▪ Equally effective for files of varied clear-text sizes.
    - ▪ The integrity of executable code (such as malicious Javascript) uploaded to farmers is assured.
  - o Drawbacks:
    - ▪ The HTML file and Javascript must be executed in a browser external to the forensic instrument to guarantee that all file effects are implemented.

Cloud storage providers might implement a variety of attack detection techniques to mitigate the risk discussed herein. Given the high entropy associated with executable, zip, and graphic file types, the entropy threshold should be set very high. Each shard could be scanned for common HTML tags or other strings common to popular applications. Farmers could be trained to detect nefarious content via n-grams and block-level entropy measures. When such signatures are found and/or content is classified as nefarious, the farmer can and should reject the uploaded content. A third solution would be for Storj to not permit a user to disable encryption of the file prior to segmentation and uploading of shards.

The high-level perspective of the process is to acquire and extract the shard table from the database in the bridge on the network. Extracting the contents of a shard is required to generate the hash of the shard on the farmer's side and verify that it has not been modified or generated by the farmer. This was achieved by using plyvel, a python library that can interact with LevelDB database files/directories.

Each shard follows the extraction process and is uniquely labeled in a dictionary within the developed tool. There are three main goals to verifying a key to defend a farmer:. 1) The shard hash in the key and the farmer, 2) The farmer's ID and 3) The exchangeresultMessage field to match either SHARD_UPLOADED or MIRROR_SUCCESS. After verifying all three of these goals the farmer has been defended since the shard was uploaded to them successfully. The key contains multiple fields that provide information about: the ID of a user, the user's hashed password, bytes downloaded in the last month, day, and hour, and the time the user was created.

This information may be helpful for identifying the owner of this client ID and prevent further harm on the network. Shards are typically 'mirrored' multiple times on the Storj network for backup purposes meaning that a 'questionable' shard may end up on more than one farmer.

The research demonstrated that it is possible to deliver unencrypted shards to computers belonging to Storj network renters. The ramifications of the work indicate that the privacy of data that is ultimately stored may be jeopardised.

4.3. Cryptocurrency transactions

Because all records are publicly accessible, identifying Bitcoin transactions on cryptomarkets shows the precise moment at which a transaction occurred. This strategy eliminates the disadvantages of web crawling, which has been widely employed in the past. In operation between 2011 and 2015 were the six largest and most active marketplaces: Silk Road, Silk Road 2.0, Agora, Evolution, Nucleus, and Abraxas. Multiple cryptomarkets have been shut down by the FBI, but the impact of police intervention has been restricted by the swift recovery of unlawful transactions on the dark web. This study seeks to determine how purchasers respond to such operations, about which little is currently known [41].

This study used three heuristics to identify and measure activity on cryptomarkets:

1. If more than two addresses are inputs of the same transaction, they are owned by the same user.
2. If an address is an input (output) to a transaction that a known address of a dark web marketplace, as an output (input), receives (sends) BTC 0.01, then the input (output) address is owned by a dark web marketplace.

3. If a transaction of an address not owned by cryptomarkets as an input has the address owned by cryptomarkets as an output, then such a transaction is identified as a purchase on these marketplaces.

Previous research disclosed more over 520,000 Silk Road transactions between June 2012 and October 2013. Internal Bitcoin transactions between the addresses in each marketplace reveal that they sent and received 0.01 BTC to/from one another. The records of Bitcoin transactions include not only the number of Bitcoins used but also the precise Coordinated Universal Time (UTC) of the transaction. UTC displays the time between 00:00 and 23:59 on a given day. This enables the detection of when customers escrow their Bitcoins for payment and their subsequent marketplace purchases. Due to the extreme volatility of Bitcoin prices, users are apprehensive about being swindled and suffering financial losses.

After the original Silk Road was shut down, Silk Road 2.0 expanded rapidly, whereas Silk Road grew steadily. When the top marketplaces disappeared, the users of these marketplaces relocated to other marketplaces. Silk Road experienced fewer than 70 transactions per hour, 1660 per day, and 11,524 per week.

At their zenith, Agora and Evolution were busier than Silk Road. This suggests that these cryptomarkets grew significantly and quickly. The majority of transactions occur on Mondays, Tuesdays, and Wednesdays, whereas fewer occur on Saturdays and Sundays. Buyers are more inclined to acquire drugs early in the week in order to receive them by the weekend, whereas users are more likely to purchase drugs on weekends and days off. Mondays through Wednesdays are prime times for drug purchases on cryptomarkets.

Due to the transnational nature of cryptomarkets, regional boundaries are unlikely to be significant. Although users' names are concealed when they order drugs, they are at risk of arrest upon receipt of the products. To minimize the greater danger of shipment interception, purchasers may be more likely to order illicit substances domestically. According to previous research, vendors ship in small amounts to minimize the danger of interception.

To comprehend the extent and growing potential of cryptomarkets as a global phenomena, it is essential to collect information on buyer conduct. On November 6, 2014, the FBI and Europol carried out Operation Onymous. One week, two weeks, and four weeks were examined prior to and after the operation, respectively. The research uncovered no indication of policing's effect on demand, although the number of cryptomarket sellers fell. This indicates that there was no large influx of new customers and migrated consumers whose trusted merchants may have relocated from the seized sites. Agora and Evolution were the major alternatives to Silk Road 2.0 marketplaces at the time.

For each transaction, the Bitcoin price on the transaction date was used. The hourly sales volume for each marketplace was calculated by summing all transactions within a given hour and multiplying them by the Bitcoin price at day's conclusion. The daily and weekly sales volumes were determined by summing the daily sales volumes for each day and week.

Seizures of particular cryptomarkets by law enforcement are unsuccessful at suppressing sales across their vast ecosystem. Users transfer to new marketplaces when existing ones are shut down, indicating that policing efforts should concentrate on buyers and sellers rather than shutting down platforms. Monitoring forums and intercepting domestic shipments are probably effective measures.

4.4. Bitcoin transactions

In February 2011, Silk Road, the first successful dark web marketplace, was created. Dark web marketplaces prioritize anonymity and security in order to reduce the likelihood of detection. Due to the quick recovery of criminal transactions on the dark web, police involvement has a limited effect. International policing initiatives are becoming increasingly vital in the fight against cybercrimes. Using simple heuristics to evaluate the transactions on the seven markets, the following results are obtained:

Between June 2012 and October 2013, the overall volume of Silk Road sales was 192,7 million USD. Following Silk Road 2.0, Agora assumed the leading position around Operation Onymous. Following the exit scam of Evolution, Agora surpassed as the dominant marketplace. Nucleus likewise exhibited tremendous expansion, and AlphaBay followed suit. The majority of transactions on the leading dark web markets are for less than 100 USD, while transactions for more than 1000 USD represent only a minor portion of the overall transactions [42].

Dark web markets provide an anonymous marketplace for a vast array of criminal goods and services, such as psychotropic substances, pornographic material, and fraudulent documents such as phony IDs. EUROPOL reveals that more than a hundred dark web marketplaces were operating for about eight months. Agora and Evolution have surpassed Silk Road and Silk Road 2.0 as the largest marketplace on the dark web. In July 2017, AlphaBay and Hansa Market were shut down by an internationally coordinated police operation. Nucleus and Abraxas were released simultaneously with AlphaBay.

Between 2013 and 2015, the most exhaustive analysis scraped 35 marketplaces a total of 1905 times and collected 78,509 product listings. Most Silk Road sellers withdrew within three months of market introduction and only 9% remained active throughout the whole survey period. Using scraped data from Silk Road and AlphaBay, commoditization on these markets was more sporadic than previously believed, despite the fact that it increased. For Agora, data was collected between November 28, 2014 and April 24, 2015, and it was calculated that the overall sales volume was around 61 million USD. Between January 2014 and March 2015, a survey revealed that Evolution had 48,026 listings and 2702 sellers.

AlphaBay was discovered to be the market leader at the end of 2015. More than four million Bitcoin transactions were done at addresses associated with AlphaBay. The anticipated overall sales volume for the pharmaceuticals division throughout the study period was 93.98 million USD. It revealed that dark web marketplaces used Bitcoin worth around 76 billion USD per year and accounted for 46% of all Bitcoin transactions.

The authors demonstrate how Bitcoin transactions using AlphaBay addresses are logged. Each address is mapped to a unique public/private key pair using a transformation function. Users transfer Bitcoins to the site's Bitcoin addresses in order to acquire unlawful goods and services. This is the first heuristic used to identify dark web marketplace transactions. For AlphaBay, 0.01 BTC transactions account for 98.1% of all transactions, while transactions above 0.1 BTC account for 1.2%.

Each of the remaining marketplaces exhibits a similar distribution of internal transactions among their respective locations. It implies that the six subsequent marketplaces received a legacy from Silk Road. The 0.01 BTC transaction between its own addresses is nearing completion on all exchanges except AlphaBay. There are 350,036 known Silk Road-owned addresses. These addresses were classified as outside addresses since Nucleus did not modify its sent-to addresses.

This causes an inflated average number of transactions in which 0.1 BTC was transmitted (received) from outside addresses to these addresses. The monthly sales volume is determined by summing the daily sales volume for a given month. For each transaction's sales volume calculation, the Bitcoin price at day's end on the date of the transaction is applied. 0.222 is the average number of transactions in which 0.01 BTC was transmitted (received) from known AlphaBay addresses to non-owned addresses. This paper's methodology provides advantages over the conventional web-scraping technique, providing that URLs belonging to dark web marketplaces are correctly detected.

It offers detailed depictions of sales volumes and earnings for any frequency (e.g., daily, monthly, and overall active period). This is due to the fact that Bitcoin transaction records reflect the amount and date of Bitcoins used. Research based on Bitcoin transactions use Heuristic 1 (if more than two addresses are inputs to the same transaction, they are owned by the same user) and follows Silk Road's Bitcoin balance. Few research have focused on Evolution, Nucleus, and Abraxas in particular. The researchers technique is more susceptible to false positives because Bitcoin transactions of 0.01 BTC may not be associated with dark web marketplaces.

The overall sales volume of the marketplaces on the dark web is 192.7 million USD for Silk Road between June 2012 and October 2013 and 166.0 million USD for AlphaBay between December 2014 and February 2016. The average monthly sales volumes for Silk Road, Agora, Evolution, and Abraxas are 10.7million USD, 10.5million USD, 4.7million USD, and 4.9million USD, respectively. The estimates, which include these marketplaces on the dark web, were 161 million USD in 2013, 227 million USD in 2014, and 366 million USD in 2015. The monthly sales volume of Evolution more than doubled between October 2014 and November 2014, from $3.4 million to $7.4 million. After Evolution's departure fraud, Nucleus flourished swiftly, and between March and June 2015, their sales volumes were more than those of AlphaBay.

It appears that the majority of users of the dark web markets that Operation Onymous shut down went to Evolution but not Agora. In 2015, with Agora's voluntary withdrawal, AlphaBay became the largest and most popular market. In November, AlphaBay's monthly sales volume hit 20 million USD and peaked in February 2016. Significant amounts of activity from Agora and Abraxas migrated to AlphaBay, indicating that AlphaBay required more sophisticated software to monitor transactions. Except for Silk Road and Nucleus, the majority of purchases on all other marketplaces are less than 100 USD.

It is hypothesized that users of dark web marketplaces purchase unlawful goods and services for their own use and not for resale or distribution. AlphaBay was the largest and most successful marketplace in terms of transaction volume when it was active. The average monthly sales volumes per purchase on the seven marketplaces on the dark web are comparable with earlier research. The decreasing trend on Agora indicates that purchases on Dark Web marketplaces have attracted more users and become more prevalent among individual users. In contrast, the increasing trend on marketplaces introduced after Agora implies that people spent more as trust in those marketplaces grew.

The level of anonymity in Bitcoin transactions is not particularly high, as the method was able to identify transactions on seven dark web markets despite the fact that individual identities were not disclosed. By aggregating these transactions by persons, further analysis may reveal a person's identify in society. Through a simulation simulating the use of Bitcoin in a university, it was determined that Bitcoin's anonymity was overestimated. Dark web vendors appear to be increasingly anxious about their anonymity, while users shift to other marketplaces when existing ones are shut down. International law enforcement initiatives and agencies are becoming increasingly significant. Other cryptocurrencies that allow for greater anonymity, such as Monero, and encrypted messaging apps enabling decentralized individual transactions have gained popularity recently.

4.5. Cryptocurrency and cryptomarkets

Since the emergence of Silk Road, the first successful dark web marketplace, in February 2011, illicit online marketplaces known as cryptomarkets have received a great deal of attention. These new online marketplaces prioritize anonymity and security to reduce the danger of identification, yet sharing many characteristics with genuine online marketplaces such as eBay.

Silk Road, the first successful cryptocurrency marketplace, was created in February 2011 and shut down in October 2013 after its founders were arrested by the US Federal Bureau of Investgation. After Evolution's exit scam, Agora assumed the leadership position and then closed willingly. Nucleus was operational from October 2014 to April 2016, whereas Abraxas was operational from December 2014 to November 2015. Numerous investigations have demonstrated that drugs constitute a significant portion of the merchandise traded on cryptomarkets. For instance, the estimated overall sales volume of Silk Road 2.0 and Agora is around 66 million and 61 million dollars, respectively.

More than sixty percent of all sales on AlphaBay were related to cocaine, cannabis, heroin, and ecstasy. The bulk of purchases are for small quantities, whereas the majority of sales are for enormous numbers. The resilience of cryptomarkets against legal enforcement and the ineffectiveness of exit schemes in discouraging customers from using them. Buyers avoid purchasing from international suppliers, preferring to purchase from many merchants inside the same country. It has been demonstrated that the geographical location of vendor origin countries affected their participation on Agora.

Typically, cryptomarkets are accompanied by frauds, hacks, and threats that are widespread on the dark web. Bitcoin accounted for 99.8% of the gathered cryptocurrency addresses, and 80% of those addresses were used for criminal activities. In addition, they assessed the market size to be approximately USD 180 million.

Bitcoin is a fully decentralized, blockchain-based digital currency. Despite the fact that all transaction data are public, Bitcoin payments are anonymous unless Bitcoin addresses and transactions can be associated with real identities. For example, to send Bitcoin to a marketplace, consumers transfer Bitcoin to the recipient's Bitcoin address. The sent Bitcoins are held in escrow until the transaction is complete, and in the case of an online marketplace, they are forwarded to the seller while a commission is retained. The records of Bitcoin transactions contain the quantity of Bitcoins used and the precise date and time in Coordinated Universal Time (UTC).

4.6. Cryptocurrency wallets

Those with access to the private keys of a cryptocurrency wallet use cryptocurrency wallets to sign transactions and send funds. In addition to forensics, volatile memory is gaining importance in every element of cybersecurity. A remote attacker might use this information to identify persons with big amounts of cryptocurrency as potential targets for kidnapping, extortion, or ransomware. Memory is observed at runtime in order to discover and extract data structures containing forensically important information, as well as conduct differential memory analysis to determine the persistence of these structures across time. The authors focus was on Ledger Nano X and Trezor One hardware wallets and their accompanying software clients [43].

A hardware wallet is a dedicated device for storing private keys. Typically, these devices exert considerable effort to cryptographically isolate the private keys from any externally accessible component. A software client is used to interface with the device via a Bluetooth- or USB-paired phone or computer.

By retrieving forensic evidence from memory, the intent is to relate several transactions with the same parent key back to a single device in this work. In 2004, the first formal memory forensics tool was introduced, and in 2007, increasingly potent open source tools such as Volatility appeared. Some researchers have recently examined the forensic memory artifacts produced by Bitcoin and Monero software clients and recovered Bitcoin and CryptoNote network protocol messages from volatile memory. Artifacts are only present on clients that run as full blockchain nodes that are directly connected to the network.

Cheat Engine, a tool used by video game hackers for real-time memory analysis, was used to locate and recognize forensically important data structures. FORESHADOW was developed to extract observed structures and analyze forensically significant data. Both Firefox and Chrome demonstrated that Trezor Wallet's memory is more stable. By halting the Virtual Machine and copying the vmem file, memory dumps were obtained. After the acquisition, a straightforward Volatility plugin was developed to encapsulate Yet Another Recursive Acronym searches.

Once YARA rules were stable, forensically relevant data extraction could commence. FORESHADOW is a plugin for Volatility that extracts forensically significant data from the Electron IPC messages of Ledger Live. A variety of changes were necessary to parse the data meaningfully. In the case that data structures are corrupted by overwrites or frees, they are discarded and printed to the command line for human inspection. Memory dumps are generated by the FORESHADOW program by pausing and unpausing the Virtual Machine and copying the virtual memory file at a 60-s interval.

Each memory dump is then processed by a Volatility plugin that traverses the physical memory space and generates a CSV file. Once a CSV has been generated for each memory dump, the files are sent to the second visualization component. The initial look of an artifact serves as a benchmark for determining its authenticity.

On the subsequent occurrence of the artifact, a bytewise and operation was conducted on the current and previous instances. This detected which bytes between memory dumps had changed. It was necessary to store a vector representing the original occurrence of the artifact's integrity. The application Ledger calculated the integrity of each artifact using a bit array comprising one bit for each byte of the artifact's contents. Each bit denotes a byte that has remained unchanged from the initial occurrence, with a zero denoting an altered artifact.

FORESHADOW is a plugin for Volatility that extracts forensically relevant information from Ledger Live's Electron IPC messages. Memory dumps are made by pausing and unpausing the Virtual Machine every 60 s and copying the virtual memory file. In the event that overwrites or frees corrupt data structures, they are discarded and printed to the command line for human review. It has been demonstrated that the amount of artifacts in the memory of the Ledger client during an experiment increases over time. The artifacts contain the public keys, transaction history, balance, path of derivation, and addresses for each extended public key.

Even after the client automatically locked itself with a passcode, a portion of the data remained in memory. This may be due to released artifacts remaining in physical memory and being cached. A data structure was discovered to include forensically useful information in both Chrome and Firefox, including the device ID and encrypted passphrase. Trezor Wallet permits users to set a password to provide an extra layer of authentication. In contrast to Firefox, the cleartext passphrase was persistent in Chrome's memory even during active program use.

YARA scans were consistently able to locate all extended public keys synchronized with the client, providing a forensic investigator with all the necessary data to examine all past and future blockchain transactions. When the application was locked at 0:30:57, the majority of memory artifacts were nearly instantly overwritten. When the process was terminated at timestamp 37:11, the remaining memory artifacts were rewritten to the point that FORESHADOW could no longer detect them.

4.7. *Evidential value of forensic cryptocurrency investigations*

This article addresses Cryptocurrency forensics and analytics from both a legal and a technological standpoint. The authors feel that it can therefore serve as a guide for law enforcement investigations, prosecutors, and Cryptocurrency analytics tool suppliers who wish to adhere to existing legislation. Bitcoin is given as an example throughout the rest of this article, however the majority of the findings may be simply applied to any UTXO (Unspent Transaction Output)-based Cryptocurrency [44].

A number of commercial (e.g., Chainalysis, Elliptic, etc.) and non-commercial analysis tools facilitate cryptocurrency investigations. They build on decades of research demonstrating that pseudonymous addresses do not provide adequate anonymity. A tag assigned to a single address inside a bigger cluster can de-anonymize hundreds of users with relative ease. Increasingly, law enforcement organizations recognize the value of sharing information to maximize investigation resources and reduce duplication of operations. In cryptocurrency forensics, this also applies to sharing attribution tags and address clusters.

Moreover, the absence of a consistent ontology and analytical methodologies exacerbates the dangers of forensic Cryptocurrency analysis, especially if attribution tags are provided in a framework that does not protect the evidentiary value of the shared content. Each clustering heuristic relies on specific behavioural patterns to group addresses that most likely belong to the same owner. These transaction systems are problematic for multi-input address clustering since the clustering algorithm would aggregate all input addresses and their associated clusters into a single entity.

There is a need for ground truth data, yet it is typically unavailable and difficult to acquire, leaving possibility for deception. A user adds (usually textual) labels or tags to shared content as part of a collaborative process known as tagging. A tag may, for instance, associate a specific Bitcoin address with a particular entity (e.g. Internet Archive). In 2005, sites such as Delicious and Flickr popularized tagging, which is now a regular feature on the majority of social media websites. Sources of information that describe the entities and activities involved in creating, transmitting, or otherwise impacting a data artifact are referred to as provenance. It provides a crucial basis for evaluating quality and authenticity and enables trust and reproducibility. In order to evaluate the authenticity, integrity, and dependability of evidence, provenance information is recorded throughout forensic investigations.

Modern forensic software can automate a significant portion of the manual labor required to generate audit trails. There is no universally appropriate model for criminal investigations. Recent research presents a conceptual digital evidence management system to enhance digital evidence chain of custody.

In law enforcement, the forensic investigation of cryptocurrency is guided by two primary interests. First, the instruments must generate meaningful, court-admissible evidence or at least reasonable suspicion for further inquiry. Second, the outcomes must adhere to general legal principles and protect the accused's right to a fair trial. Clustering and attribution algorithms are employed particularly to identify natural persons (i.e. suspects). As a result, the data pertains to identifiable natural persons and is therefore considered personal information. The necessary quality of the legal foundation relies on the level of protection and the scope of the processing.

Data gathered through established law enforcement communication channels, including SIENA, Schengen Information System (SIS), and Interpol's I24/7. The data amount (minimization of data) and retention dates (limiting of data storage) must be limited to what is required for the intended purpose. The concept of transparency compels the investigator/prosecutor to explain the processing to the data subject or the data protection authorities to a certain extent. Given that only facts can be incorrect, data protection regulation does not prevent the processing of data based on guesses (heuristics) or probabilistic measures. All forensic steps and methods involving the processing of electronically stored material must assure authenticity. This necessitates complete and accurate documentation of data sources, tools, and applicable approaches.

If inaccurate or obsolete data has been shared, the recipients must be informed. Verifying the authenticity of data necessitates knowing the original data/source and keeping track of all modifications. Cryptocurrency forensic tools that function on top of a certain cryptocurrency benefit from Blockchain technology's fundamental concepts. Given the currency code (e.g., BTC, ETH) and hash of the most recent block, as well as the analysis method, it is simple to reproduce the results of the analysis. These strategies are implemented by tools that generate new tool-specific data points that cluster known addresses into a collection of clusters, which are often identified by an identifier.

Regardless of whether the digital investigation is undertaken "in-house" or outsourced, digital evidence should be based on methodologies that are exact and scientifically validated. In the worst case scenario, a lack of scientific verifiability diminishes the evidentiary value of the discovered evidence or leads to its full loss. Information reliability can be modified on three levels: 1. the implementation of clustering heuristics, 2. annotations, and 3. the correct usage of the tools.

Clustering for law enforcement reasons must treat CoinJoins (a cryptocurrency mixing scheme) as a particular case by applying algorithms to exclude or flag probable CoinJoin transactions from clusters. The researchers found 723,247 clusters, or almost 2% of the entire 40,049,947 cluster dataset, contain at least one CoinJoin, with an average of 17 addresses involved.

Consequently, it is vital to continually reevaluate the underlying assumptions and correct the revealed flaws. The dependability of an annotation tag is heavily influenced by its origin, its development technique, and how it is assigned to a particular address or cluster by a forensic instrument. Regularly, assumptions and algorithms must be evaluated and revised. If the assumptions are known, the user's behavior can be altered to influence the results of the analysis.

Lack of expertise with IT forensic techniques can have a significant impact on investigations and the resulting evidence. There are currently no international qualifications standards for investigators and professionals managing electronic and digital evidence. To ensure minimally acceptable standards, investigators should have completed a certification course for the employed forensic software and received basic IT forensics training. Using the same mechanism that currently ensures the validity and integrity of data, it is possible to receive cryptocurrency analysis findings using forensic instruments. If Cryptocurrency clusters are generated over a specific Blockchain state (identified by block hash), then the procedure is repeatable and reproducible when applied to the same blockchain state. Evidence in criminal trials must be of the highest quality and the possibility of someone committing an infraction must be sufficiently high to convince a court beyond reasonable doubt.

This indicates that it is challenging to reconcile the normative evidence standard with the statistical outcomes of data analysis processes. When employing data analysis techniques such as address clustering, both the software tools and investigating IT professionals must be able to offer precise information regarding the evidence to be extracted from the analysis. Key to constitutional criminal proceedings is the right of the accused or his defense counsel to inspect the evidence acquired by the police and the public prosecutor's office. This privilege is designed as the right to see records in inquisitorial criminal procedure systems, such as the German criminal procedure (GERCCP, x 147). Similar rights can also result from data protection (e.g. EU-Law Enforcement Directive, Recital 38, c. f. 3.1).

When employing data analysis methods in either system, the question of what information must be revealed to the defendant and his attorneys on the software tools used and the data and information processed emerges. Law enforcement authorities have an interest in preventing criminal populations from learning the precise operation of data analysis tools. The source code alone does not account for the investigator's specific errors. A first suggestion could be to omit the software's source code in favor of a description of its functions and usage.

4.8. Key requirements summary

Lawfulness: Address clustering and annotation tags must follow data protection and legal requirements. Automated clustering of cryptocurrency addresses can only be used to make human-made decisions like ordering more investigation. Correcting pertinent results is necessary.

Integrity: The chain of custody just has to store the currency code (BTC, ETH) and the most recent block hash to verify address data authenticity and integrity. Clustering techniques require reliable cluster identifiers that change when the underlying collection of addresses changes. A "cluster hash" does this. By linking attribution tags to their sources, creators, and generating processes and digitally signing the tag and surrounding information, authenticity can be ensured. This boosts tag reliability.

Reliability: Take these steps to maximize reliability:

- Testing the formalized heuristic against some collected and confirmed ground truth, ideally a general, authoritative standard ground-truth data collection (e.g. (shared) sets of addresses from known (seized) Cryptocurrency wallets).
- Testing the clustering algorithm's reliability within specific Cryptocurrencies using traditional functional testing methodologies and providing the function implementing the clustering heuristic a set of example transactions in a black-box test.
- Reviewing and correcting clustering assumptions (e.g. multi-input heuristic).
- Intensively logging investigator software use.

Sharing analysis results: Always sharing any information needed to assess information reliability.

Qualifications: IT-forensic investigators have no international qualifications. Address clustering and annotation tagging investigators should at least have undergone a certified training on cryptocurrency architecture, clustering heuristics, the implications of adding an attribution tag to an address, and the attached provenance information.

Verifiability: Address clustering and annotation tagging can be repeated and reproduced using data authenticity and integrity methods. To ensure availability, online tags must be kept locally and permanently.

Chain of Evidence: In criminal cases, criminal lawyers must be able to subsume the results of address clustering and annotation tagging under the normative notions of the appropriate criminal procedure code. The software tools and IT professionals must provide precise information about which evidence is to be obtained from the study and what conclusions can be formed with what likelihood. The information must be in lawyer-friendly language.

Access to Records/Evidence: The applied procedures must be described as precisely as possible. This entails disclosing the heuristics, probability, and software tools employed in the specific case. The sources, process, and reliability of annotated material must be reported.

4.9. Data sharing structure

The authors emphasize the sharing of attribution tags across law enforcement authorities in a manner that facilitates compliance with essential standards such as authenticity, dependability, and chain of evidence. A single tag can deanonymize a Cryptocurrency address and, when paired with clustering algorithms, also a complete address cluster. The difficulty lies in identifying the optimal compromise between law enforcement requirements, existing legal and ethical norms, and technical effort and practicability. The data model additionally includes the authenticity and integrity requirements by translating them into equivalent data model variables. They propose extending CASE with a specific property bundle (Tag) that includes descriptive components for attribution tags in order to describe attribution tags.

A tag carries a unique identity and may refer to a digital, physical, or merely mental object (e.g. Internet Archive). All concepts and relations, as well as their instances, should have qualified names to prevent naming clashes. This can be performed by assigning name spaces expressed as Internationalized Resource Identifiers (IRI). The namespace (case.example.org/core#" title = "http://case.example.org/core#">http://case.example.org/core#) might be applied to all previously introduced concepts, characteristics, and relationships. By ensuring that all terms have dereferencable IRIs, vocabularies and classification schemes can be disseminated on the Internet. This enables online searching and browsing of accessible terms and categories, as well as automatic verification of attribution tag categories prior to their exchange. Alternately, current Git infrastructures might be used to store and publish attribution tags.

A cluster is a sort of Trace that indicates a collection of Cryptocurrency addresses. A cluster may have many tags, which may be referenced by their distinct (potentially dereferencable) IRIs. Digitally signing the cluster with all its contextually relevant properties might demonstrate its authenticity. The proposed technique for sharing address clusters draws on the previously introduced attribution tag sharing model.

There are no internationally binding standards for measuring, securing, or enhancing the evidentiary value of Address clustering and Annotation tagging outcomes. However, it is possible to develop basic requirements that can claim some legitimacy in any constitutional criminal procedure. The results must be reliable and reproducible, and the investigators employing these approaches must be suitably qualified (e.g., through certification training). The authors have developed a data sharing approach based on understanding of the technological constraints and regulatory needs of Cryptocurrency investigations. It has been demonstrated that (most) legal requirements for securing the evidentiary value and adhering to the principles of data protection can be met. The findings can serve as a template for adapting the model to the criminal procedural codes of other countries.

4.10. *Digital assets*

Castell (2019) developed a checklist as a useful guide to be used when requesting disclosure of digital assets:

- Disclosable digital assets
  - Disclose each and every entity including but not limited to:
    - Cash, currencies and any holdings or contracts denominated in all or any fiat currencies; and cryptocurrencies including Bitcoin, Ethereum and Litecoin;
    - Dematerialised data having ascribable financial or tradeable value;
    - Physical storage media and devices holding value; and
    - Banking and accounting records including account numbers and names.
  - Access methodologies
    - Disclose all data, techniques and materials to identify, access, but, sell, maintain and report on every such disclosable digital asset, including:
      - Bank accounts, wallets, user IDs, passwords, PIN codes, signing protocols, two factor authentication protocols;
      - All relevant trading, storage and or other exchanges information;
      - Software records and audits as to its reliability and security and correctness; and
      - Anything signed by or requiring signature by a digital signature or other verification process.
    - Means of repository and access
      - Disclose and confirm is any such access methodologies are held by one or more trusted third parties and, if so, disclose all details thereof;
      - If not held by one or more trusted third parties:
  - Immediately deliver up the details to [named attorney], without alteration, redaction, in complete and functional form;
  - Provide a detailed schedule of things so delivered-up/
  - Assessments and valuations of digital assets
    - Disclose existing assessments, valuations and or demands for taxes, carried out by any tax state or regulatory authorities including:
      - In the UK, HMRC;
      - In the US, the IRS
      - Any law enforcement agency or entity.

Successful asset preservation orders have been made for over £1 m of bitcoin stolen by fraudsters. In the ruling, the United Kingdom's High Court recognized Bitcoin as legal property [45].

4.11. *Privacy-oriented cryptocurrencies*

As it does not enable true anonymity, developers and consumers are focusing increasingly on privacy-focused coins. Monero, for instance, is a privacy coin, and its developers work very hard to provide users with additional protection, anonymity, and privacy. Verge was launched in 2014 as DogeDarkCoin and rebranded as Verge currency in 2016. The paper introduces the concept of privacy-focused cryptocurrencies, along with Monero and Verge and their valuable forensic artifacts [46].

There are currently numerous anonymous and privacy-focused coins with a variety of features. Monero XMR is among the top ten cryptocurrencies on CoinMarketCap, and cybercriminals use it extensively. Verge XVG, the second cryptocurrency explored, employs a 'private' blockchain with stealth addressing.

Bigger rings (also known as mixins) make it harder to trace transactions. A Monero wallet has only one public address, which the user must reveal to the sender in order to receive funds. A public address can identify a wallet on a suspect's computer system; hence, it has important forensic relevance. Monero employs transaction ids to capture blockchain transactions. With a transaction id, it is possible to determine which one-time addresses are included in a transaction.

A sample transaction identifier appears as follows: 4485151e06b936e56ce7f5f132c1026608bca716c23bfa4e4ad88a6155a88aa6. It consists of 64 hexadecimal characters and is used to spend Monero. Additionally, it is used to view older transactions that the owner has made. An investigator can retrieve a wallet without knowing the password or seed phrase using forensic techniques. The Monero wallet is comprised of three files: a wallet file, a key file, and a text file containing the public address.

A key file includes the passphrase used to encrypt and secure the wallet key file. Forensic value is derived from forensic artifacts indicating the presence of Monero software on a computer system. The Verge currency employs stealth addressing, which enables a sender to generate a one-time address depending on the recipient's stealth address. Transactions made to "standard" Verge public addresses are publicly viewable and can be tracked back to a public address on the Verge blockchain. A Verge public address begins with a capital letter and consists of 34 characters.

When a Verge public address is present on the blockchain, it is associated with a transaction. With the Private address (also known as the private key), complete control is maintained over the associated cash. Multiple private addresses with accompanying public addresses can be stored in a wallet. A Stealth Address is not publicly published in the Verge blockchain. When two users conduct a stealth transaction, the receiver must construct a stealth address within the wallet program and then give it to the sender.

The XVG transaction id is a 64-character hexadecimal string with the following format: f4393787e70802b370235bcb7e6654b399a6860eebf81cfa0efa0efa0efa032d8. With a transaction id, one may determine which public address was used to send a specific amount of XVG. Other valuable forensic artifacts are markers that reveal the presence of Verge software running on a computer system, such as the presence of Verge software installation files. Examine DNS traffic captured by a wiretap.

Criminals frequently employ cryptocurrencies, and in March 2017 an Avast researcher found what was likely the first ransomware that accepts Monero as payment. Malware that silently mines Monero on your computer, as discovered in and, is a further cybercriminal usage of the cryptocurrency Monero. Approximately 5% of all Monero coins are mined maliciously. An investigator can partially "track the money" with transaction ids, public addresses, and of course totally with the seizure of a digital wallet. In addition to the wallet passphrase, private key, and mnemonic seed phrase, evidence of the use of a cryptocurrency in network traffic from a wiretap can be a helpful asset for forensic research preparation.

In both experiments, private keys that allow an investigator to seize funds from a wallet were completely absent from memory. On the examined systems, forensic artifacts such as public addresses, stealth addresses, transaction ids, and transaction amounts are present from various sources. Not all artifacts adhere to a predefined pattern and are therefore not searchable using a regular expression, such as a passphrase. The researchers performed their investigation on the Windows operating system or mobile operating systems, and they examined different Bitcoin wallet software. None of the researchers investigated the wallet software of cryptocurrencies that prioritize privacy.

In all cases analysed, the seizure of a Monero wallet is achievable with the passphrase. On the analysed systems, other valuable forensic artifacts such as public addresses, stealth addresses, transaction ids, and transaction amounts are present from various sources. In both the Monero and Verge experiments, several sources of evidence contain valuable forensic artifacts. The forensic value of a cryptocurrency wallet can range from the seizure of the wallet and the assets it contains to indicators of the use of specific cryptocurrency software. With the outcomes of the experiments, a researcher is now aware of which artifacts should be present in various memory images.

4.11.1. Ethereum

The objective of this study is to develop a strategy for researching network transactions by comprehending the protocol and developing investigative tools. It describes a way for recording transactions for timing and setting them in a particular order, so that when data is retrieved, it can be compared to a known sequence of occurrences. Review data source analysis, data quality, and the phase of presentation. Create a standardised procedure for transaction tracking and account identification. Determine where tracking occurs after a theft by a third party, where thieves use the network to conceal or move funds [47].

The worldwide and unregulated character of cryptocurrencies may be exploited for money laundering by criminal organizations. The Internet has enabled thieves to interact electronically with buyers in online markets, which reduces the danger of detection. Darkweb markets are comparable to eBay for prohibited products like drugs, guns, and pornographic photographs of children. A investigation of drug-selling activities on the Internet identifies key detection opportunities utilizing the Hancock and Laycock script. The conceptual framework indicates places that criminals can use to expand their Internet communication capabilities.

In order to discuss how the Ethereum protocol executes network-wide transactions, a comparison to the Bitcoin protocol will help to emphasize its differences.

Bitcoin is the best-known and largest blockchain or distributed ledger technology currently in use. Bitcoin functions through the use of cryptography public/private key signature of transaction hashes. A transaction is initiated by transmitting the required Bitcoin amount and the hash value of the preceding block. This generates a chain where each link is confirmed.

It is important to separate the two types of accounts that exist on the network. These are externally owned accounts, accounts that are controlled by a private key and would include a common human user account. The other type of account is a “contract account”. This is an account that is controlled by the code it holds within the contract itself on the Ethereum network. The term “smart contract” will be used to describe this type of transaction throughout this paper.

It is considered a small program that can be executed by the Ethereum Virtual Machine. The “state” of the system is key to how Ethereum can run more complex computer operations. The ability to compute a smart contract provides new use cases for transactional behavior to encompass trust and efficiency. Smart contracts were proposed in 1997 by Nick Szabo who compared them to vending machine transactions. The system can settle financial derivatives, exchange currency from one cryptocurrency to another, or even to gambling platforms.

The term “GAS” is used when a computer performs instructions on the network and is required to be specified when a transaction or message is sent for execution. Each “account” is represented by a 20-byte long string and contains four data fields, “nonce”, current balance”, contract code” and “storage” (Foundation, 2017a):. Each message sent by an account is structured like an “object” (Buterin, 2014). A “STARTGAS” value, this represents the total number of allowed steps to be computed by the E.V.M. (EDSA signature values). The value “GASPRICE” is the fee that the sender will pay per computational step sent to the recipient.

Deduct the value of Ether as specified from the sender account to the receiving “TO” account. If the account doesn’t exist create a new account. Run the code until the contract is complete or the gas runs out. If all steps are executed then any leftover gas can be returned to the sender and the fees paid for gas used can be paid to the miner.

4.11.1.1. Situation and examination.

A transaction’s mechanics consist of the signature and the raw hash that generates the 256-byte transaction hash TXHASH. In certain account systems, such as Parity, Mist, and Meta-Mask, accounts can be represented by a colorful, blocky identicon constructed from the address’s hash. The user picks the sending account and then enters the receiving account’s address or scans its QR code.

Etherscan web services are among the most popular tools for searching and viewing network and transaction data. Etherscan is a web-based interface for searching for transactions by hash, account, block, token, or Ethereum Naming Service. Console commands are accessible via the Geth console or, as demonstrated in the sample below, the Parity Web3 console. The application binary interface is used to standardize the lengths and encodings of transaction-related data. Numerous programming errors and contract logic irregularities have resulted in considerable losses.

The ERC20 coin was created in response to an Ethereum Improvement Proposal. It is a typical procedure for introducing changes to a protocol in a controlled manner to obtain consensus among engineers, developers, and the community. This allows the decoder to read the decimal value 4 and the ASCII value dave from the input fields’ encoding. The ERC20 token is compatible with any tokenised system, including value tokens, financial derivatives, cloud computing, gambling, and storage, among others. Using battle-tested code, the standard also instills trust in developers that the smart contract logic is sound.

EIP20/ERC20/citeVogelsteller2015EIPs/eIP20.mdGitHub has the complete final specification. A coin is a contract that is deployed on the network by an account that is not owned by the network. The address field must contain the token’s contract address; each token is simply a contact with a 20-byte address. This enables the data on Etherscan to be attributed to other accounts by noting the contract originator and transaction ID when it was produced.

Using the kevalscsv.py script, the data collected from JSON files using the Etherscan API is converted into a CSV file. This allows for a rapid overview of the transactions and further ERC20 transactions utilizing the codes. A number of Key values that are advantageous to the investigation process are found. Fields used to express the quantity of gas necessary for a transaction and depending on network congestion, the cost of a slow or fast transaction can vary.

Each contract address conforms to the same format as an externally held account, as the two are equivalent. The block is also assigned a 32-byte hash address that corresponds to the block that contains the transaction. The software is not intended to execute optimal code or load data into a database, which are requirements for any production-ready solution. A script was developed for Token events; it parses the obtained transactions and retrieves their key values, including the Method ID, utilizing the returned data. As graphing became a subject in its own right, a simple structure was used as proof of concept. Graphs depict the direction and flow of funds in the previously outlined scenarios.

It is possible to see the edges or resting spots (endpoints) Endpoints could be an exchange, an ATM, a retailer, or a mixing service. To track the money, the subsequent "to" address must be downloaded in order to view the subsequent node in the chain. Using Shapeshift and Etherscan scripts, a full record of Ethereum transactions was compiled. The Jaxx wallet additionally used Shapeshift to move ETH to Golem GNT and Augur REP tokens. Kraken will maintain Know Your Customer information that is likely to be accessible to law enforcement or civil litigants if the proper court documents are produced.

A significant metric may be the number of tokens on an account and the point at which the balance reaches zero. A further little deposit is issued before the tokens can be moved. This may show ownership and affiliation, highlighting affiliated or linked accounts. The graphing in Blockseer is well-mapped, but the investigator must still make connections and conduct account research.

Cryptokitties was a digital collectible game and trade platform based on Ethereum. Following the auction, the events display "Auction-Successful" and token transfers using the same ID transfer technique as the ERC20 token. In the future, it will likely be possible to virtualize or imitate a contract for security logic testing. The Jaxx wallet features a default Gas value of 25000 and a Gas Price of 2 Gwei, whereas MetaMask had default values of 21000 and 1 Gwei. The prices paid for other services and contracts are significantly more specific to actual gas use. It should be noted that a user can modify the defaults, which may aid with identification when a user reuses a non-standard value.

4.11.1.2. Forensic analysis. In this experiment, Hashcat was used to extract the hash, place it in a Hashcat-formatted command, and crack the wallet password. The keys are stored in the "keystore," which varies slightly between operating systems. Password cracking may aid in asset recovery and the discovery of passwords for other services, such as drive encryption. Hashcat was employed to brute-force the Parity password. The cracking of the pre-sale wallet is not discussed in this thesis due to its limited utility; nonetheless, it should be noted that Hashcat implements the cracking function.

On a virtual system, Jaxx was installed and operating. In order to enable another view, testing was performed on the Desktop program running on Windows 10. Utilizing BIP39 Word Seeds enables the word seed to function as the master key to unlock the multiple public addresses and subsequent wallets in the key space. Scanning seized objects or triaging at a crime scene expressly for word seeds will open up new avenues for account recovery and discovery. The adoption of a similar standard for the structure and protocol of wallets is still based on Bitcoin BIPs Bitcoin Improvement Proposal.

The word seeds contains 12 letters. UTF-8 encoding of English words ranging in length from three to eight characters. There are further numbers of words that will be discussed in the future. The key lists are accessible in a variety of languages and are documented on the Github website, along with a list of all acceptable seed words. The previously used Jaxx wallet has a 12-word seed following decryption.

This allows the method to be tested and validated for locating the wallet's address using only the seed phrase. The derived address is displayed using the M/44'/60'/'0/0 deviation path as the root-derived account. This demonstrates that investigators may find the restoration of seed words against even all potential coins to be extremely valuable.

4.11.1.3. Network attribution. Utilizing a human-readable name can aid the user and increase Ethereum Naming Service adoption. When an ENS name is used in a cybercrime, for example, the Namehash can be cloned and searched for events on the blockchain to discover linked activity. The bid procedure was completed with a handful of failed transactions due to a high GAS network load and an initially overlooked last step. ENS functions similarly to DNS, and it is possible to transfer and redirect an IP address. Therefore, an address must be specified on the Registry contract in order to set the resolver, in this case the public resolver.

The transaction test will consist of sending ethereum from Alice's wallet to the address bob-wallet.ethereum. Reversing the name hash of the subject's human-readable name enables a search for activity or events that may allow the ENS address to be linked to an account. This could suggest that the account is domain squatting, waiting to sell, or has not yet been set up. This strategy enables complete attribution for the movement of cash and the connected ownership and management. The capability to use the ENS to point to hosted files or web content stored on the swarm distributed node network is transitioning from testing to the production network.

A man in the middle attack comparable to a DNS attack is possible. As law enforcement and Internet service providers address the sharing and storage of photos using hash sets, future enforcement will require a new set of distributed hashes. Criminals are very likely to employ mining pools to mine cryptocurrencies. Mining pools are frequently labeled on Etherscan and have a huge amount of transactions, including mined blocks, from their accounts. It is quite likely that a person is engaged in illicit activity if he or she receives frequent payments for mining without any hardware.

Because of the mining techniques, Monero and Zcash are the most popular coins. Other, more specialised assaults target Ethereum miners using insecure routers. When operating the Linux Parity node and the Windows 10 Geth-based Ethereum wallet, a snapshot of processes and network connections was recorded. Using the Ethernodes service, it is possible to discover network nodes using either the "enode" address displayed by the Parity client or the I.P and port address. There are packages and scripts for enumerating Geth nodes that can be exploited.

The stated methodologies were duplicated and tested for accuracy using both testnet and the actual network. As tools concentrate on the transfer of Ethereum from one account to another, the use of tokens and trades within the contract structure must be comprehended in order to perceive the true picture. The use of decentralized exchanges enables the transfer of different tokens from one blockchain to another, posing a new problem. New classes of tokens enable the transfer of value via digital collectibles; money laundering might be accomplished by exchanging thousands of dollars' worth of digital Cryptokitties. Using Ethereum Name Service to move funds to human-readable names based on abstract hash address values has demonstrated the capacity to identify owner accounts and track funds. The employment of ENS can also lead to distributed files or web documents, so creating a web-hosted entity that is resistant to censorship. The requirement to access event logs for an Ethereum Name Service set address function will enable wallet address attribution. MethodID registry of contract functions to parse data on transactions is necessary, as seen by display token movements.

5. Digital forensic science

The processes, procedures and tools that have been accepted and are commonly used in digital forensics can no longer meet the need for scientific rigour. The Information Environment is where humans and automated systems observe, orient, decide, and act upon information, and is therefore the principle environment for decision making.

Under the Daubert standard, Scientific knowledge = scientific method/methodology where a conclusion will qualify as scientific knowledge if the proponent can demonstrate that it is the product of sound "scientific methodology" derived from the scientific method; and relevance and reliability requires the trial judge to ensure that the expert's testimony is "relevant to the task at hand" and that it rests "on a reliable foundation". Concerns about expert testimony cannot be simply referred to the jury as a question of weight. The Daubert standard requires general acceptance of the theory and technique used in the digital forensic process to be generally accepted by the scientific community and have been peer reviewed. Most of the main tools that are in use are proprietary commercial products have no published data available on error rates. The paradox is that due to lack of a better solution, experts have shifted their risk homeostasis levels of what is acceptable for the notions of ‘rigour’ and of ’process’.

5.1. Digital forensic science practice

The National Institute of Standards and Technology (NIST) has published a digital forensic tool catalogue which it states is intended to provide an easily searchable catalog of forensic tools. However they caveat this with the cautionary note that “tool information is provided by the vendor”. The Computer Forensic Tool Testing program provides a methodology consisting of tool requirements specifications, test procedures, test criteria, test sets, and test hardware. The underlying technologies have not seen significant disruption for a number of years and disks that work in one computer can normally be expected to work in another. There is an increasing number of products on the market that contain computer processors with limited processing power and memory that may contain potential evidence and these can be classed Internet of Things (IoT) devices.

5.1.1. Rethinking digital forensics

Due to the size of storage medium and the volume of data, it is becoming increasingly difficult to capture a “full” set of data. There is the possibility of being accused of collecting only the data that supports a case and excluding exonerating evidence. Paging, caching, and the true distribution of processing and storage pose a threat to the core principles and foundations of live forensics and the quality of the data that may be obtained. Increasing use of devices with ever-increasing volatile memory capacity and devices with limited volatile storage and processing capacity (mostly IoT devices). Cloud computing represents a substantial advancement in the current state of information technology services [48].

Traditional digital forensics cannot be directly used in cloud systems. Data duplication and multi-tenancy in the cloud platforms will add to the challenge of locating, identifying and separating the data relating to suspect activity. Cloud server forensics adds to the paradox with the issues of multi-tenancy, physical inaccessibility and unknown location of the artifacts to be collected. In a highly decentralized and virtualized cloud environment it is quite common for data to be located in multiple data centers located in different geographic locations. In a traditional server based environment, where the physical locations of the systems are known, the investigators can have full control over the forensic processes.

5.1.1.1. The tools. The National Institute of Justice, in the USA, has carried out some excellent work on tests on a number of commercial data acquisition and imaging tools. While there is de-facto acceptance of their capabilities, there is increasing concern with regard to their veracity. As these tools are commercially developed, there has not been the any level of independent testing of their functionality. The average size of the Seagate HDDs is now over one terabyte. Forensically wiping one Samsung HD105SI 1 TB drive, using a tableau TD2u, was achieving an average of a 6.6 GB/min transfer rate and a projected turnaround time of 2h 30 min. A typical case would require investigators to collect, on average, more than 1 TB of data (including CDs, DVDs, internal and external HDDs/SSDs).

5.1.1.2. Potential solutions. ISO 17025:2017 (General requirements for the competence of testing and calibration laboratories) is not fit for purpose in the digital forensic environment. Consideration should be given to developing a specific standard to meet the current and developing environment of digital forensics. The National Institute of Justice and NIST’s work is of huge value but does not go far enough. Investigators need to have forensic intelligence, even for the simplest and most trivial computer-related crime, that can lead to forensic evidence. Such intelligence can be used either in a pro-active or in a re-active manner.

Computer-related criminal activities can be seen as a very complex problem combining different types of traditional criminal activities with different and innovative technologies. The Officer In Charge (OIC) must be enabled to identify physical and logical boundaries (internal and external) that are within the scope of the investigation. Any solution must not be disruptive to business and must be seen as a catalyst in ensuring business continuity. The solution must also be modular, portable, extensible and scalable.

5.1.2. Digital forensics experimentation

Experimentation is one of the most well-known and widely-used empirical approaches for generating trustworthy and statistically tested evidence. A growing number of studies have been conducted in Digital Forensics, demonstrating that it is a trustworthy field of study. In terms of experimentation specifics and its components, such as Hypothesis, variables, threats to validity, sampling procedures, and experimental design, the majority of published research provide inadequate reporting. As a crucial methodology in Computer Science, experimentation should be better understood and valued. Experiments are conducted for the purpose of evaluating software quality and management technologies and analysing effectiveness and effort-related consequences [49].

Despite disputes regarding the scientific experimental method and its function, experiments exhibit some commonly acknowledged and frequently implicit characteristics. A study investigates the topics that are deemed crucial to discuss and address for the proper acceptance of scientific information. The authors propose unexplored study fields, outlining a number of concerns and problems linked with the empirical evaluation of these solutions. In addition, they examine difficulties with the experimental validation of present techniques. In this part, the conceptual modelling of Digital Forensics studies is examined.

Concept models are tools for organising and representing knowledge, such as concepts enclosed in ringed rectangles or boxes of some form, and relationships between concepts represented by a line connecting two concepts. Planning comprises arranging the experimental setting to prevent undesired impacts and determining how to regulate and evaluate each variable individually. For tests to be valuable in Digital Forensics, they must be reproducible. An error in a forensic report or expert testimony will be ascribed to the digital investigator, regardless of who was responsible for the mistake. Even between numerous runs of the same experiment, systematic error or bias in an experiment might be difficult to identify.

The Framework for Reliable Experimental Design (FRED) aids those working in Digital Forensics. FRED focuses on the underpinning techniques involved within undertaking the reverse engineering of digital data structures and the process of obtaining and interpreting digital content in a trustworthy way. The suggested framework is intended as a tool for industry and academic professionals in the Digital Forensics sector to promote and build research best practises.

5.1.2.1. ExperDigital Forensics-CM: a conceptual model for digital forensics experiments. ExperDigital Forensics-CM is a static data model. Its conceptual data is represented by a conceptual map comprised of rectangles and connecting lines. Due to peculiarities of the Digital Forensics experimentation domain, a model based on semantic knowledge is selected. As mapping studies cannot promise 100% coverage of current studies, there might be certain topics not modelled in this study. Planning of Digital Forensics experiments is highly vital to avoid deviations during the experiment execution.

In any experiment, it is essential to precisely specify the Variables, which may be independent or dependent. An investigator wishes to observe dependent variables in relation to independent variables. The more the values of independent variables vary (cause), the more impacts may be observed. Design Type is directly proportional to the number of variables and treatments/controls. In terms of statistical testing, the analysis of an experiment is more complex as the number increases.

ANOVA may be used to evaluate hypotheses during Analysis and Interpretation. The instrument is a set of materials, e.g., source-code, questionnaires, or recommendations. They are necessary to collect data from participant behavior and maintain experiment control. Exact replications are classified into two subcategories: Dependent Replication, in which all conditions are identical or comparable, and Independent Replication, in which one or more design aspects differ.

Experiments in digital forensics are undertaken with the following steps in mind: Acquisition, Examination, Analysis, and Reporting.

Previous authors proposed the Metadata Harmonisation technique for merging data sets is used as an example of an algorithm. An operating system that executes apps for its users is a virtual machine. The apps EnCase, FTK, Recuva, R-Studio, and Stella Phoenix are examples. Training incorporates information from data sets or Benchmark, as well as an instrument from the Planning idea. Pilot projects are viewed as useful practises to modify and re-evaluate assumptions and hypotheses given for an experiment.

Experts on the subject of the experiment should be invited to take part in a pilot project. As an experiment develops, data is its foundational ingredient. To enable the testing of hypotheses, the collection of data, and the derivation of conclusions, it is necessary to draw the majority of your samples from independent variables. In the case of studies with no volunteers, algorithms, hardware, and software are used to generate data.

Data may consist of either Original Data or Duplicated Data. Once data have been gathered during an experiment, Data Plotting is undertaken to offer a graphical representation and arrangement of the experimental data. Two types of analysis are possible by graphing data: qualitative analysis, which is less typical in Digital Forensics investigations, and quantitative analysis. On obtained data, it is feasible to conduct Descriptive Statistics, Normality Test, Hypothesis Test, Correlation, and Regression for quantitative analysis. At least two of these must be performed in every digital forensics experiment for data analysis to be reliable.

Correlation may be used to evaluate a potential linear relationship between two continuous variables. For the analysis of experiment data, both linear and nonlinear regression may be used. Limitations are discussed in order to define the scope of the experiment. Threats to Validity assess the degree to which data-based inferences, constructs, and internal and external relationships among variables are accurate or logical. The Dissemination concept attempts to provide an experiment's Data Set with proper Authorship via a reliable Repository.

A publicly accessible data collection of government records including 986,278 files and an e-mail data set containing 200,399 authentic e-mails from 158 Enron workers are examples of data sets with unique IDs. A data set should be citable by providing authorship, a unique identifier, and public and permanent storage. This pertains to the handling of data during and after a research undertaking.

5.1.2.2. ExperDigital Forensics-CM feasibility evaluation survey. The conceptual model's practicality was determined by survey responses.

It was found that ExperDigital Forensics-CM is a great platform for designing, conducting, and sharing Digital Forensics experiments. According to survey responses, ExperDigital Forensics-CM can help document experiments, support replication, repetition, and reproduction of Digital Forensics experiments, retrieve experiment information, organise experiments, audit experimental processes, support meta-analysis, and improve experiment quality.

Based on the perceived ease of use of ExperDigital Forensics-CM, the following feasibility-related conclusions can be drawn: it is objective, avoiding confusing experimental terms and elements; it seems easy to use for documenting Digital Forensics experiments; it can be used as a checklist for conducting Digital Forensics experiments; it helps find error-prone identification; it requires mental effort to use correctly; and it seems easy to extend for a particular case of Digital Forensics.

Coding the open questions (OP.1, OP.2, and OP.3) revealed various open and axial codes. These codes helped to discover the association between the open questions and how respondents regarded ExperDigital Forensics-CM usage for planning and performing Digital Forensics experiments, its adoption potential, and its recommendation to the community.

Respondent quotes validate their Likert-scale responses, providing criticism and suggestions on ExperDigital Forensics-CM viability. Responses went to ExperDigital Forensics-CM evidence:

1. It facilitates developing Digital Forensics experiments, is practical, and can be used as a guideline for experiments
2. It can be used to check and validate forensics data and experiments terminology
3. It is a useful model and can be easily adopted
4. It increases users' knowledge
5. It improves the quality and efficiency of Digital Forensics experiments
6. It guides Digital Forensics phases during experimentation; and
7. It has important ease of use constraints and it needs specific improvements to improve its ease of use.

https://doi.org/10.5281/zenodo.3695857 contains all survey data.

5.1.2.2.1. Validity risks. Verifying that the open questions are completely related to the Likert-scale ones mitigates this issue. According to this poll, what was measured was strongly related to what was attempted to be measured.

This survey may be compromised by not asking respondents about Digital Forensics experimental domain characteristics. This attack was unaffected by typical Digital Forensics testing. A subsequent survey could explore certain qualities to make ExperDigital Forensics-CM cover specific use cases.

Perceived Usefulness and Ease of Use traditional measures reduce this hazard. Open questions were posed to examine how well ExperDigital Forensics-CM helps organise and execute Digital Forensics experiments and whether it should be used and recommended. Then, Likert-scale replies and open question answers were strongly correlated.

Respondents were provided in a document with multiple examples for each ExperDigital Forensics-CM aspect from published Digital Forensics trials to mitigate this issue.

Due to the small sample size, experienced practitioners who work on actual Digital Forensics projects and cases were invited to provide more accurate comments than newbies.

5.1.3. *Storage reconstruction*

Digital evidence comes in many different forms, be it video files stored on a hard disk or e-mails sent over a network. Metadata-based reconstruction of active content has the advantage of being precise. In file systems where block pointers are overwritten, reconstruction can be performed heuristically, e.g. in FAT. File carving tools are able to reconstruct files that have been deleted long ago, sometimes even if a volume has been reformatted with a different file system. This method is less precise than metadata-based reconstruction, i.e. it provides less information about the circumstances of the recovered file, but it is more complete in the sense that there is high probability that evidence is found even if it was deleted [50].

The authors introduce a model of storage abstraction layers and heuristic reconstruction modules that cover – to the best of knowledge – all reconstruction approaches known from the literature. Composition operators for these reconstruction methods that allow to combine them in useful ways are defined. LAYR is an object-oriented design that is able to reconstruct abstraction layers in a modular way through a generic interface.

The authors analysed the issue of collecting digital evidence on systems employing abstraction layers to arrange storage. On the basis of a generic concept of abstraction layers, they developed a software framework capable of generically combining various reconstruction techniques and approaches. In the framework, heuristics can be used to address particular reconstruction problems, while operators can combine them and generate complicated reconstruction sequences. The concept is applicable to the majority of published abstraction layers and can serve as the foundation for a library of reconstruction modules.

Current heuristics only accept a single storage item as input, which is a small conceptual deficiency of LAYR. This prohibits modelling abstraction layers that operate on several lower layer storage items (such as RAID systems). Similarly, it is impractical to assume that all blocks (at any level of abstraction) have the same size. Both flaws are minimal because the definition and application of heuristics are easily adaptable, but slightly more complex.

In addition, the current version of the model does not consider metadata for the sake of simplification. In addition, LAYR uses an uniform block size of 512 bytes for all layers.

LAYR can also be expanded to include more file system and carving heuristics. Due to the framework's versatility, it may be possible not only to directly reuse code from other projects, but also to incorporate closed-source products by creating wrapper classes over their interface.

In addition, heuristics could be used to construct complicated file filters, perhaps by inputting search terms or regular expressions via a (graphical) user interface. Filter heuristics could be applied to decrease the number of reconstruction outcomes in order to make them more relevant to the current investigational query. For instance, a black-and-white heuristic could produce a result set containing solely scanned papers. A further use may be a hash-based heuristic that compares results against a database of notoriously illicit content. In addition, a file name or a hate speech heuristic could return files containing specified names or terms within documents, indicating whether the file's content may be of interest.

The LAYR source code can be found at https://github.com/janineschneider/LAYR.

5.1.4. Solid state drives

The conventional hard drive (HDD) comprises a platter that spins and a read/write head that moves. An SSD is a nonvolatile data storage device that stores data in solid-state flash memory. In contrast to conventional hard discs, SSDs lack mechanical components such as a spindle motor and read/write heads. By charging and discharging electrons to and from the floating gate, the memory cell stores the bits "0" and "1". These two gates are separated from one another by a thin dielectric substance, also known as the oxide layer and functioning as an insulator [51].

To read data from a memory cell, voltage is provided to the control gate and an attempt is made to move current from source to drain. SSD controllers consist of numerous sub-modules with unique functions. Four distinct types of memory cells, namely SLC, MLC, TLC, and QLC, are used in the production of the SSD. SMART is a self-monitoring, analysis, and reporting technology monitoring system.

Encryption and decryption procedures are implemented in hardware through an encrypt and decrypt engine. For speed matching and to boost the data flow, high-speed RAM is used. Depending on the controller, the NAND memory interface may contain a single or several NAND channels. Occasionally, a power outage may occur while data is being transferred to the SSD. It is not possible to directly overwrite data on individual pages; data can only be written into blocks of vacant pages. Every time data is written, the following procedures are performed: Search for the block containing sufficient "unused" pages; determine which pages in that block are still required. Rewrite the pages mentioned in the preceding step into the reset block. Reset to blank each page in the block. The SSD controller makes every effort to minimize the reuse of previously written blocks. When writing data to the SSD, the controller will select the block with the smallest number of rewrites.

5.1.4.1. SSD forensic analysis. The majority of SSDs reserve between 5 and 10% of their storage capacity for other applications. The SSD controller pushes the data into the non-addressable pool after deletion. The erased data blocks are identified as "empty" or "trimmed." The trimmed blocks are cleaned by the garbage collection process, which is not instantaneous and runs in the background the majority of the time. DRAT and DZAT successfully prohibit data from truncated SSD blocks from being read.

Evidence integrity is significantly complicated by the garbage collection procedure. In addition to the nondeterministic nature of TRIM, errors in the SSD controller or driver software might also create a challenging environment. There is no single standard accepted by SSD manufacturers that can aid forensics examiners in recovering data in a forensically acceptable manner.

The researchers investigated the viability of recovering erased files and artifacts from SSDs. The relevant case scenario-related files were searched for the keywords "Tax," "Money," "Cash," "Paid," "Amount," and "Voucher." The primary purpose of this experiment is to determine the likelihood of recovering deleted files from an SSD, particularly when TRIM is activated and off on the host machine. During normal operation, several files were stored and removed.

In TRIM OFF mode, just a few files could be retrieved; in TRIM ON mode, no files could be retrieved. Observations indicate that the data returned from the reduced block is occasionally unpredictable and nondeterministic. Recovery of deleted artifacts from an SSD is highly dependent on whether or not the TRIM mechanism is enabled or disabled. The effect of the TRIM enabled function is entirely unpredictable. It is impractical to use normal data collecting techniques for SSD since it is difficult to demonstrate the integrity of evidence in court if it is contested.

During the acquisition procedure, forensic investigators must take every measure to prevent any loss of data or uncertainty. There is no clarification and no technical disclosures from the SSD maker to aid law enforcement with managing or suspending the waste process. If viable, the forensics expert must consult the SSD manufacturer and take all precautions to inhibit the background garbage process during forensic imaging. Experts in digital forensics should attempt to remove the SSD from the suspect's computer and acquire the data using a forensic data capture system in the lab. Multiple experts are of the opinion that SSD-recovered evidence does not meet the criteria of evidence.

Integrity of the evidence is one of the most crucial essential requirements. Using the hash value, the authenticity of evidence is demonstrated. The unregulated TRIM and garbage collection processes always cast doubt on SSD's evidence. There is potential for future study to analyze SSDs at the chip level. A unified standardised created and followed by SSD manufacturers can resolve nearly all problems.

5.2. Crime scene

5.2.1. Classifying crime scene images

Forensic science relies on information technology for administrative and analytical tasks. Forensic practitioners are increasingly overburdened by data. Crime scene photo labeling is laborious and time consuming. Large forensic image databases require computer vision and data analytics techniques. Automated computer vision tools include image classifiers and Content-based Image Retrieval (CBIR) systems which can organise and search crime scene image databases. These tools can assist in the detection, disruption, and prevention of crime. Real-world crime scene photographs are sensitive, making CBIR and categorization studies rare. Some implementations are based on commercial solutions and lack source code to adapt them to specialised databases. Previous attempts include a CBIR approach that uses color, texture, shape, object spatial connection, and numerical identification [52].

Image classification can reduce occupational health risks for practitioners cataloging sensitive and explicit material. Image classification-CBIR system research focuses on performance enhancements rather than semantic searching. One previous method was tested on 400 real-world crime scene photos with an item "frequent weighting strategy". This strategy weighted multi-object classes with a previous likelihood of occurrence. Results for "Shoeprint," "tyre patterns," and "window" classifications were good, but "physical evidence," "crime scene drawing," and "vehicle" were poor.

The Australian Federal Police (AFP) has almost 300,000 drug operation photographs. Automatic picture classification is needed for assist operations. Specialised algorithms can automatically extract image class-specific information of which this paper investigates two.

The first is a Bag-of-Visual-Words (BoVW) model, and the second is Tree-based Deep Convolution Neural Network (DCNN). Both models are chosen for their similar training and implementation complexity. A real-world automated crime scene image classification system is evaluated. Illicit drug-related photos totaled 97,287 which were manually sorted into 24 categories.

Merging several small categories with similar content balanced the dataset. Highly similar images can bias image classification findings and overestimate model effectiveness. Highly comparable captures were deleted from the experimental dataset. After image relabeling, cleaning, and balancing, the total was number of images was 60,520.

Each cross-validation repeat trained and tested BoVW on up to 1200 images per class. Repeated K-Fold Cross Validation balanced and randomized training and test subsets. A closer look of the database categories revealed a hierarchical semantic linkage. In the ImageNet Large-Scale Visual Recognition Challenge, AlexNet CNN surpassed other algorithms for image classification accuracy (ILSVRC). These models are not designed to be used with image categories that are interrelated and hierarchical within the same domain.

The classification accuracy results of the proposed BoVW-based SVM model can be summarized using a normalized confusion matrix that compares actual target with expected value average rates for each class and for all classifiers trained with the repeated K-Folds approach. Numerous classes have poor performance and are inappropriate for real-world settings requiring an adequate threshold(s) to discriminate between False Positive and True Positive occurrences. The True Positive Rate is extremely high for the majority of picture classes, with many classes achieving 100% accuracy. Softmax scores can be used to establish decision thresholds for various automated processing workflows. The overall classification performance of the CNN is optimal for an automated scenario, with three out of six classes performing flawlessly.

The general CNN model with leaf nodes is an excellent choice for automated processing for a number of classes. An investigation of the classification performance of the BoVW-based SVM model reveals that, while a few image classes exhibit acceptable performance, the vast majority of image classes have poor true positive rates. The false-negative rates for some categories are very high.

5.2.2. On-site decryption

Investigations involving digital forensics involve user authentication, encryption keys, and private key data. When the target of the search and seizure is not expected to participate, these are difficult to obtain. Live system forensics is the most realistic response option since it limits system changes throughout the investigation.

To increase anonymity, cryptocurrencies such as Zcash do not permit transaction analysis of their remittance information. From the perspective of digital forensics, the investigation response process for cryptocurrencies can be roughly separated into three categories. The first method is transaction analysis, which tracks the transaction history of cryptocurrencies. The second scenario is when the target employs untraceable privacy-centric cryptocurrencies such as Monero (XMR). The third strategy involves securing private keys to freeze or seize criminally-used cryptocurrency. Accessing data on secure messengers, i.e. those with Full Disk Encryption and/or File-Based Encryption requires decryption. However, each device includes a cloud syncing feature that enables the retrieval of smartphones' basic call history, contact list, text message history, and location data [53].

This study takes the approach of obtaining the user authentication credentials of a system and using them for device unlocking and cloud data acquisition or decryption. By obtaining the private keys, the proposed system enables the instant confiscation of cryptocurrency. It also enables the unlocking of locked devices and the decryption of data by protecting credential information.

Vision is a tool designed to acquire content on search-and-seizure sites. It provides an integrated method for accessing data that normally requires user consent by searching for and rearranging important data. During the analysis phase, an optional function has been included to permit operations linked with an investigator's auxiliary systems for a faster computation. A function for optical character recognition has been introduced to the discovery procedure in order to identify relevant words in image files. This contains the standard forms of public and private cryptocurrency keys as well as onion domain addresses.

The process of discovery includes preliminary exploration, collecting, and search and identification. Pre-exploration is required to include seized objects in a follow-up analysis if decryption or credential combinations fail in the analysis step. This includes user address storage files for cryptocurrency wallets and online browser history for clients of anonymizing services like Tor. Scanning of mapping tables, pattern formation, and word generation constitute the bulk of the reconstruction stage.

5.2.3. Case studies with vision

1. The investigation was able to estimate the total amount of damages and comprehend the number of victims through the information obtained. The addresses containing the magnitude of damages were secured in two laptops, and a seizure (to the tune of USD 500,000 at the time of the search and seizure) was made with a paper wallet prepared in advance.
2. A residential search and seizure were conducted on a drug buyer who was identified in a different case. Two locked smartphones (one of them lacking a SIM card) and a laptop were found at the scene. An investigation was able to confirm locations that consistently appeared in the GPS location information. The laptop confirmed the login records for an online cryptocurrency wallet service but failed to find the password.
3. Various devices, including computers, smartphones, feature phones, tablet PCs, and a USB storage device were found at the scene. During the pre-exploitation stage of the discovery process, the investigation found that Bitlocker was activated in a storage device installed in the relevant system. The USB storage device lacked a file system, and the investigation was able to identify randomized values. Analysis identified a fixed string of lowercase English letters by identifying noticeable password patterns used on the web browser. The investigation confirmed the source code and development log of the program used during the crime.

5.2.4. Learning efficacy

In 2015, $13 billion was spent on education-related hardware technology. Due to the 2019–2020 Corona Virus Disease (COVID-19) pandemic, remote learning had become crucial for the survival of academic institutions [54]. Concerns exist over the utility of virtual reality in digital forensics and cybersecurity instruction. Course design considerations for computer forensics instruction in an online environment were first described in 2007 noting the importance of hands-on exercises.

Since then, academics have concentrated on developing a Virtual Crime Scene Simulator with the capacity to interact with and perform real-time triage of routinely discovered digital devices. A literature study of digital forensics education reveals that little to no work has been done on the development, evaluation, and dissemination of an immersive, simulated, virtual reality learning environment. Immersion places a learner in a simulated or real-world physical and social situation, while directing, structuring, and facilitating participatory metacognition.

Before and after accessing the learning environment, participants performed a multiple-choice test on digital forensics-related concepts. To teach students how to employ digital forensics in the real world, an immersive virtual reality experience was designed. It comprised a lecture, an investigation on-site, and a gamified laboratory experience. In the laboratory, volunteers assumed the role of an investigator and were tasked with gathering certain pieces of evidence.

Given a specific scenario and laboratory activity in Bagging & Tagging a digital forensics crime scene, the scores of students who learnt in virtual reality or physical space were not significantly different. As results may differ amongst virtual reality encounters, additional testing would be required. It may be possible to equip law enforcement with more effective training as digital evidence increases. There was no statistically significant difference in the pre- and post-test scores of those who completed the virtual reality vs the physical experience, according to the findings. These findings may suggest that the use of virtual reality to teach digital forensics (at least within the context of lectures and the Bagging & Tagging laboratory exercise) is a successful method.

Purchasing a virtual reality headset could be a less expensive and more practical alternate technique for teaching these subjects, while still achieving the same level of student comprehension. Test this form of learning on participants while teaching more complicated and technical computing-based tasks, such as coding and programming exercises, would be another possibility for future research.

5.2.5. *Contemporaneous notes*

No competent forensic scientist in other areas of forensic science would conduct an examination without taking extensive records of his investigation and the reasons for his judgments in the twenty-first century [55].

In R v. Smith [2011] EWCA Crim 1296 (also emphasised in The Forensic Science Regulator's (2019) 'Legal Obligations' literature), doubts were made about the practise of taking contemporaneous notes as part of any investigation. While the emphasis in R v. Smith remained on fingerprint evidence, it is clear that practitioners of all forensic science fields are expected to take proper notes. As a result, the development of examination case notes should be regarded as a fundamental component of any forensic investigation process.

The keeping of examination notes is a primary tool for quality assurance and control. Almost often, case notes will assist the investigating practitioner not only during the examination, but also in the writing of their report. In reality, not all digital forensics case notes are contemporaneous, but, given the complexity and depth of many studies, they should undoubtedly strive to be. In digital forensics, contemporaneous notes should be viewed as a support mechanism during an investigation and during the creation of any report. In certain cases, retrospectively recorded notes may be the only viable alternative for a practitioner; nonetheless, they are required to precisely recall all pertinent information requiring notation.

The Association of Chief Police Officers' Good Practice Guide for Digital Evidence states that an audit trail or other record of all processes used to digital evidence should be developed and maintained. Principle three of its four guiding principles stipulates that a "audit trail" of acts must be maintained. During the period of September 2018 to April 2019, the UKAS conducted 29 surveillance visits of ISO 17025-accredited digital forensic units in England and Wales when concerns were expressed about "inaccurate or insufficient information being documented in notes or supporting quality documents."

The creation of contemporaneous notes is deceptively straightforward, although the UK Forensic Regulator shows that there is opportunity for improvement in this area. In addition, those participating in the education and training of the future generation of forensic practitioners must take the time to define and create acceptable noting practises. Following the discovery of unprotected contemporaneous notes practises, the Regulator expressed concern. In the majority of instances, clarity and additional explanation can be offered in any additional text that references previously incorrect notes. This gives process openness and should not impair an examination's credibility.

Note entries should correspond to the normal phases of an enquiry, including exhibit handling, data collecting, data analysis, interpretation of findings, and reporting. In addition, it should be emphasised that these basic phases may be considered "placeholders," with each stage including several subtasks and complications that will likely need to be noted. Multiple factors will influence the level of information in a practitioner's Contemporaneous Notes, including the subject's complexity, the aims of the investigation/analysis, the stages of research a device is undergoing, and the available time and resources. Contemporaneous notes should begin with exhibit handling in the lab, not "at the scene." It is also essential that this information be provided to the practitioner in charge in order to assist future examination decisions.

It is essential to guarantee that instructions are appropriately transcribed and comprehended, regardless of their complexity and depth. The collecting of data can be a component of the stage of exhibit handling, and contemporaneous notes should include the following information. The level of complexity involved in describing the acquisition process and configuration will vary based on the device requiring acquisition. Methods of video collection that are extremely complex or require an extended period of setup or device activation should be considered. Standard investigative procedures that have been tested and deemed appropriate for use in a working laboratory may be used for data collection and analysis.

Scanning digital content frequently involves an element of automation via the use of tools (in certain circumstances, "off-the-shelf" tools). The data identified by these procedures is subsequently subjected to analysis. In practise, data processing and interpretation may occur concurrently with the examination phase. In such situations, the contemporaneous notes should describe the design, testing, and use of a suitable approach. When data is analysed and highlighted as pertinent to an investigation, it is necessary to record all pertinent metadata.

In the majority of instances, contemporaneous notes should be needed as part of the peer-review procedure, allowing reviewers to examine examination procedures. The use of counter signatories (another lab member) to verify the signing procedure should also be considered. As a mechanism of keeping note information, encryption should be explored or extra encrypted containers may be deployable. Contemporaneous notes in digital forensics must contain enough information to be of enduring value. As part of their standard functionality, tools can record information about completed/incomplete procedures and returned results.

The conclusion of all interactions should also be documented, especially if additional investigative risks or procedural disputes were raised. Practitioners of digital forensics must ensure that all crucial decisions made throughout the examination process are documented, along with the data required to reach any conclusions. Inadequate decision-making can lead to examination-error sources in which cognitive bias can play a role. Any methods implemented by the practitioner and/or laboratory to mitigate these side effects should be specified and described.

5.3. *Digital forensic examinations*

5.3.1. *Manual examination*

A device manual examination involves the use of a device's user interface to manually examine and collect content. This typically requires a first responder/practitioner to methodically access any device's menus/settings and then record what is displayed on-screen using some form of camera device. A DME is not suitable for use in all inquiries, where forensic acquisition/extraction methods may be preferred. It must be acknowledged that in some cases this approach will not be viable, particularly if the type of content being captured on the device is sensitive or subject to legislation. Complainant devices and the digital forensic science device extraction and examination processes can be considered invasive [56].

Often, when these are deployed it is to try and access all available information in order to ascertain whether inquiry-relevant content may exist - to facilitate 'an investigation' of the device. The seizure of a device and subsequent forensic extraction and analysis of its content may not be necessary in all cases involving a complainant device. Device manual examination approaches are arguably both less intrusive and less impactful upon the complainant's privacy, as a device may contain data that a complainant does not wish to be viewed, and which is also non-relevant to the inquiry. Device manual examinations require no specialist software/hardware to interact with a device.

There is a cost-effectiveness argument to be made in terms of a lack of need to equip first responders/investigators with licenced software for at-scene examinations. A device manual examination is a 'live' process that is carried out on a potential evidential exhibit. It is by no means a replacement for an in-lab device interrogation where extraction and analysis of device content has taken place using specialist software. Device manual examinations may compromise available evidence brought about through changes to the device.

The use of a DME may become a more frequent option for first responders/investigators to deploy when inquiry-relevant data exists upon their devices. In light of the impending accreditation deadline in England and Wales of 2022, the proposed manual examination procedure is designed to help formalise the decision making process. A device manual examination is not a replacement for a traditional device forensic analysis, yet neither should it be considered a shortcut tool. A process that must be deployed in circumstances when it is correct to do so and any first responder/investigator must evidence that they have given thought to this. Device manual examination should not be used to compensate for a first responders lack of tool awareness or training, or even if a tool is unavailable.

It is important to consider who the first responder is that may be in a position to consider a DME an appropriate method to conduct as part of an inquiry. Whilst in some cases it may be those who are qualified to handle and interrogate digital devices, it may also be front line police officers who may not have had relevant formal training. It is arguably important that all front line staff are provided with fundamental training in regards to DMEs.

5.3.2. *Timestamps*

Timestamps are an excellent source of evidence for examiners in the reconstruction of computer crimes. Timestamps are part of the metadata which have always been an important part of digital forensics but are becoming increasingly so. Timestamps are relatively easy to alter with open source tools resulting in them being repeatedly called into question when presented in evidence. Conversely, detecting timestamp manipulation is not a simple task.

A mechanism employed by adversaries and malware is to use 'timestomping', mechanisms to alter timestamps to hide traces of their nefarious activities. Sophisticated groups and state actors now commonly add timestomping capabilities into their malware. Best practice for identifying timestomping in Windows NTFS has been to analyze the values for `$MFT` (the database of all folders and files on the volume) and `$LogFile` (maintains the record of changes made to files).

Researchers considered five timestamp artifacts (`$LogFile`, Prefetch Files, `$USNjrnl`, LNKs (Link files) and Windows event files, which were subjected to experimentation with three timestomping tools (Timestomp, SetMACE and nTimestmp).

- $LogFile maintains the record of changes made to files to help the system recover from a crash. It generally holds two to 3 h of information in normal usage.
- *Prefetch* files are created whenever a program is executed for the first time and are used to speed up subsequent executions of the program.
- $USNjrnl records the time that any changes are made to files. This record can be used to identify when a timestomping tool first arrived on a system. A file creation record was also created for Prefetch associated with the timestomping tools.
- LNKs act as shortcuts to local files and created whenever as local file is created or opened for the first time.
- Windows event *files* records event logs including the application log, system log and security log. It is possible to create a timeline of when the user was active which can be referenced with other timestamps. If other log times occur outside of these active sessions, it is an indicator that some timestamp manipulation might have occurred.

Each of the artifacts provide diversity and depth in sources of timestamp data available to examiners to determine the possibility pf timestamp manipulation. None of the artifacts alone were a consistently reliable source for identifying timestamp manipulation as they were not enabled by default in the case of one, or they could be deleted/exploited. The presence of timestomping tools could be detected through the *prefetch* files although it is possible for an adversary to hide the use of such tools. In conclusion, the researchers proposed five rules to detect timestamp inconsistencies in NTFS [57].

5.3.3. *Timestamps on Unix systems*

A software stack is a collection of software subsystems that can function independently of other software. When running an end-user application, the application is at the top of the stack, while the OS kernel and drivers are at the bottom. On both the software (firmware) and hardware levels, what occurs on the drive itself was excluded [58].

When the kernel writes to the file system, genuine modifications occur at the very bottom of the stack, which causes timestamp updates. Regarding timestamp updates, the behavior of applications and libraries is not specified. Regardless of how many files an application accesses, the operating system's mount option may prohibit updates to the access time.

Our project profiles generate system-running timestamps dynamically. Noise from other applications or the operating system, such as a file indexer or an IDE (Integrated Development Environment), might modify the results, and users must interpret the results carefully to filter out the noise. Similarly, the tested systems must be configured so that timestamp updates are not skipped. Particularly Linux is tested with the non-default mount option strictatime, the default relatime choices functioning as a filter for timestamp updates at the base of the program stack. To keep tables up-to-date, it will be necessary to test the same systems on different versions and to apply new updates. With the exception of kernel bug fixes and substantial modifications such as the addition of new file systems, few changes to working IO implementations are anticipated. In fact, programs utilizing GIO for IO are unlikely to change, given it largely functions as intended. Middleware and application bugs are not usually rapidly addressed and are suitable candidates for forensics artifacts to identify application use, as the 11-year-old GIO bug impacting Nautilus demonstrates.

5.3.4. *Browser*

Drive-By-Download assaults have been used extensively in Advanced Persistent Threat (APT) attacks that exploit zero-day vulnerabilities. Utilizing exploit kits, attackers infect large numbers of victims' computers. A significant portion of these attacks are transmitted to the user's computer via the web browser, which increases the importance and necessity of web browser forensics. The authors seek to improve the precision and speed of web browser forensics investigation by integrating concepts from digital forensics and artificial intelligence to create an intuitive toolkit for forensic analysts [59].

The AI model has a classification accuracy of 99.8% for malicious code and benign web pages. Behavior-based detection operates by loading a page through an emulator and recording and examining the run functions. This approach offers the advantage of quickly determining whether a masked website is harmful. It is challenging to detect fraudulent web pages that involve user activity, such as clicks or drags, especially when numerous pages are interconnected.

Existing research lack a remedy for false negatives, which can cause analyses to be muddled. These concerns will be exacerbated by the increasing size of modern websites. It is challenging to use machine learning for digital forensics in the real world due to the wide variety of event types and the low categorization accuracy.

After gathering the web page's content from each browser's cache, the AI model examines it for malicious elements. To choose a superior feature, the source code of a large number of legitimate and fraudulent websites was evaluated. Malicious web pages have a number of distinguishing characteristics, including special character features, JavaScript keyword features, and statistical features.

For injecting shellcode or obfuscating strings, special character features include hexadecimal characters. Additional characteristics include file size, total number of lines, and maximum line length. Malicious web pages contain well-known exploit kits such as RIG, Angler, Blackhole, Nuclear, and Phoenix, as well as code that exploits browser vulnerabilities in HTML and Javascript parsers.

The model was trained using 46,500 datasets, whereas test-sets comprised 6000 datasets separate from the training dataset. In this experiment, three learning algorithms were used: Support Vector Machine (SVM), Deep Neural Network (DNN), and Random Forest (RF). The Random Forest model had a remarkable 99.8% accuracy. Since this is a model based on trees' votes, the probability can be determined by tallying the number of trees that voted affirmatively.

The AI Browser Forensic Toolkit (AIBFT) was developed based on Section 3's research. After collecting the web browser's cache file, AIBFT automatically decides whether or not a web page is harmful using an AI model. Since it can be organized and reviewed in the order of high probability of being malicious, it can detect False Negatives considerably more quickly than randomly evaluating all pages.

AIBFT includes both a command line interface and a graphical user interface, enabling analysts to analyze in a variety of contexts. It enables file viewing, search, and filtering capabilities for analysis without the need for extra software. A timeline analysis tool is offered to visually classify suspicious web pages fast and intuitively. In addition, the AI model used for detection and probability measurement is a Random Forest model by default, but the DNN model can be selected as needed.

Several antiviruses were tested alongside the detection of harmful samples to confirm their detection accuracy. The testing sample includes of browser Common Vulnerabilities and Exposures vulnerability Proof-of-Concept code, obfuscated exploit kit code, and a web page for mining. Using the script function, investigators may easily discover and examine if online sites are dangerous.

5.3.5. Geolocation

Identifying the place from which resources were taken is anticipated to be an effective investigative tool. VBL approaches have been developed primarily in the realm of robotics, specifically autonomous driving. Along with the enhancement of the performance of VBL systems, research into their industrial applications has expanded into other domains, such as fashion. The Tokyo picture dataset comprises of 880 photographs captured in 10 locations throughout Tokyo. The 24/7 Tokyo dataset consists of 1125 photos captured in 125 distinct places [60].

All images have GPS data that specifies the location where they were taken. This information is read by the 'Pillow' Python package's ExifTags module (version 6.1.0). The three components of the VBL system are feature extraction, similar picture retrieval, and gunshot location prediction. DEep Local Feature (DELF) is an algorithm based on deep learning that does not involve the creation of handwritten descriptors. By virtue of DELF's attention layer, it is able to identify local features belonging to the same object instance.

One is to calculate the frequently used mean average precision (mAP) and recall in information retrieval systems. mAP represents the precision with which a system can predict or obtain user-requested database objects. Recall displays how accurately each area may be anticipated based on its own photos. In order to compare DELF's performance to that of other methodologies, NetVLAD and RootSIFT were also used. The VQ technique is suitable for approximating differences in descriptor distribution between images.

It avoids the requirement to calculate the distances between pairs of photos, which is anticipated to make the calculation significantly faster than if DELF's default option were used directly. This entire technique is identical to bag-of-visual-words using different descriptor algorithms, such as SIFT and SURF. The tree structure was designed using the open-source tool "Approximate Nearest Neighbors Oh Yeah (ANNOY)". The pairwise-image similarity with the cosine kernel (cosine similarity metric) is measured, which is equivalent to establishing a scalar selectivity function s and a vector representation F. The mapping is implemented with the "Folium" Python library (version 0.10.0).

The kernel density estimation (KDE) approach is used as a non-parametric data smoothing tool. The graphical representation of the estimated PDF facilitates easy comprehension of the degree of data point aggregation. The PDF is normalized with regard to its maximum value and put on the background map image of Stamen toner tiles to facilitate visual comprehension. This adjusted probability density function is known as the normalized existence rate (NER).

The default usage of DELF descriptors was effective enough to classify the filming locations, however it is troubling that its time complexity was too high for practical application. In the two-dimensional embedding form of the dissimilarity matrix derived from all image pairs in the Tokyo image dataset, the areas with locally aggregated points showed greater mAPs and Recalls than those with widely dispersed points.

The combination of VQ and ANNOY improved the time complexity of an aerial photograph search by a significant margin. Compared to the default use the distances between mAPs in various regions shrunk. 80% (16/20) of the photos found were captured close to the query image. This result implies that the VQ-induced blockwise separation of the DELF descriptor space confers robustness to a broad range of landscape properties, while obscuring the features of a particular landmark.

Almost all similar objects have stage frame truss constructions made of steel. These geometrical validations provide interpretability into why and to what extent the system determines pairs images to be comparable. After the user drags and drops a query image onto the upper left panel, the query information is delivered to the server over an SSH connection from the client device. When the user clicks on an image in the scroll viewer, the DELF descriptors corresponding to that image and the query image are presented. The best performance was achieved by NetVLAD, followed by DELF VQ and RootSIFT.

As described in methodology, the VBL system has three components. Algorithms can be changed with more efficient ones without affecting other components because their algorithms are independent. This exchangeability is vital for performance enhancement and system maintainability given the rapid progress in machine learning. Descriptor choice is crucial. This study extracted local feature descriptors using the DELF technique, which may not be the best for image-based geolocalization. It has previously been found that traditional descriptors like RootSIFT outperform DELF. The user's focus determines which descriptors should be used to derive query image features. To infer the shooting place from a photograph's plant vegetation, descriptors trained on a plant image database like Quantitative Plant must be used to estimate the plant's type. Thus, a good descriptor can help to harness a lot of knowledge about what experienced location recognition investigators consider in a query image. Two more elements influence descriptor selection. Image database size. If the database does not contain enough photos to cover the spatial areas of interest, a descriptor is selected that recognizes regional traits from image contents to roughly estimate their positions. Time-complexity is another. DELF + VQ was 10,000 times faster than DELF. Time complexity substantially impacts VBL system usefulness. Users should consider these factors while choosing a VBL descriptor.

NetVLAD outperformed DELF and RootSIFT. Occlusion sensitivity maps show NetVLAD's CNN's attention in the input image. DELF can match pairs images point-to-point, but occlusion sensitivity map cannot. Point-to-point matching between paired photos gives us profound insights like easy results understanding. Thus, adopting the DELF architecture into NetVLAD's CNN may be necessary to achieve great performance and acceptable interpretability.

Aerial photographs are a popular VBL method because researchers feel it is impossible to collect enough geotagged reference photos to cover full spatial areas of interest. Aerial photography's wide reach and ease of acquisition motivate these academics. CNN-based models linked ground-level and aerial photos in most of their methods. Neural network-based generative models, such as conditional generative adversarial networks, may forecast ground-level landscapes from aerial pictures in the future, facilitating this stream. An aerial photograph was used because of these outstanding advances in location estimation using sets of aerial photographs. As indicated, using solely ground-level photos to estimate firing locations is difficult because it is hard to collect enough photographs to cover complete spatial areas of interest. A web crawler through image hosting services like Flickr is a frequent way to collect geotagged images, however many of the images have little geographical information. The closed loop of ground-level images, aerial photos, and neural network-generated images may solve this issue.

An investigation assistance tool should let law enforcement agencies clearly indicate that they cannot identify photo or video locations if the tool cannot estimate them with any plausible cause. Inaccurate estimates may lead to a wrong beginning investigating strategy, wasting time and money on criminal cases. From this perspective, some types of complete end-to-end deep learning algorithms, which receive a query image and directly predict its shooting location, may offer more accurate results than systems that follow the proposed framework, but they will be impractical for forensic use due to ambiguous reasoning about why they identified locations as shooting locations. Law enforcement investigators testify as expert witnesses. Even if their estimation accuracy is inferior than state-of-the-art end-to-end deep learning models, investigation assistance tools should prioritize interpretability.

5.3.5.1. Geolocation data. In digital forensics, there is an increasing demand for the development of quantitative statistical approaches. Geolocation data logs are now frequently accessible on mobile devices. Other sorts of evidence, such as fingerprints, shoeprints, and bullet casing impressions, present a greater challenge for statistical analysis. In this study, the researchers examine the evolution of quantitative methodologies for geolocated event data forensic investigation. Specifically, the authors examine two types of ways to obtaining evidence strength: a likelihood ratio approach based on modelling the evidential data directly and a score-based likelihood ratio that models a summary estimate of the similarity of the evidence [61].

A law enforcement agency can demand information from a service provider regarding any individuals whose devices were in the area during the relevant time period. Once the identities of persons of interest have been determined, the service provider can reveal them. Determining whether or not two sets of places "match" can be challenging due to a number of factors, such as the variety of human behavior and their frequency in the population.

The researchers evaluated the score-based likelihood-ratio (SLR) methodologies for the strength of evidence for pairs of sets of sites A and B in Orange County and New York. LR and SLR values were thresholded to provide binary conclusions of same source or different source. The true and false positive rates were calculated by comparing these binary decisions to the known ground truth.

The threshold was changed to achieve various sensitivity and specificity tradeoffs. This trade-off can be summarized by the area under the receiver operating characteristic (ROC) curve, abbreviated as AUC. AUC is a measure of fit and can be interpreted as the likelihood that the approach will produce a bigger LR or SLR for a randomly selected pair of same-source observations. Across all data regimes, the SLR has a considerably greater FP rate than LR. It was discovered that the performance of the LR and SLR vary depending on the spatial region's features. The impact of varying the number of events in A and B on the behavior of the techniques is substantial. The AUC highlights this phenomena, as the AUC for each method in OC is greater than in NY. This indicates that an analyst may need to assess his or her familiarity with the region under examination.

5.3.6. Docker container logs

Docker is an open application development, distribution, and execution platform. It allows users to decouple apps from infrastructure in order to deploy software quickly. Log is a default component of the majority of containers and contains a wealth of essential information. The proposed approach can be used as a guide for retrieving container logs because the format is independent of the content. Log recovery is a subset of file recovery that restores deleted data from a host machine [62].

Few studies have examined the approaches for recovering JSON-file logs. To recover deleted files, traditional methods rely on file system metadata (such as file name and allocation information of file content). However, file carving is recommended as a solution for this issue. A log file comprises many lines, with each line containing a single message and related information (e.g. origin and timestamp). Previous work proposed using natural language processing techniques to extract features (such as unigrams and bigrams) during categorization of file fragments; while others employed the edge smoothness between two pieces to detect combination errors. The only valid values are "stdout" or "stderr" for the "stream" key. The I/O stream from which the logging driver extracts the message is represented by the string in value. There is no explicit attribute length limit. In practice, a brief list of "attributes" is sufficient to distinguish log files.

As test datasets, two new disk images are obtained, and then the performance and efficacy of the carver are assessed. The images and scripts used to operate and execute containers are all downloadable from the author's GitHub repository. Python's dictionary (Python Docs) serves as the foundation for implementations of neighboring words trees. Log line carver (LL carver) is based on the Scalpel algorithm.

The "Restore Image" feature in WinHex is used to restore a disk image to a hard disk drive. The proposed carving is superior to previous attempts in terms of log line recovery. For LL carver, the procedure and outcomes closely resemble those of a previous experiment. WinHex uses the "File Recovery by Type" function, which is dependent on file signatures. Since the scanning step size was reduced to 512 B, the amount of time required by the carver has grown significantly.

The VP tree is changed based on the characteristics of the contents to reduce the amount of calculations required for each search. 43.31% of recovered JSON-file logs that lack matching metadata and have been partially rewritten are removed. The negative impact on performance cannot be completely minimized, but additional phases can be used to reduce the quantity of input blocks during the phase of reassembling all blocks.

5.3.7. Approximate matching

The promising technology of approximate matching identifies similarities between two digital artifacts. Algorithms may either directly compare artifacts (e.g., Levenshtein distance or Hamming distance) or convert them into an intermediate representation, i.e., a digest or fingerprint. This category of algorithms began to gain popularity after 2006 with the publication of `ssdeep`. The authors create a classification of similarity digest algorithms in order to enable their description and comparison [63].

Previous attempts at categorization only addressed certain elements of algorithms, not their overall behavior. This results in a misunderstanding of how an algorithm works, which can lead to poor similarity digest algorithm selection (e.g., comparing algorithms with totally different behavior, or even not comparing them with other similar algorithms). Therefore the authors suggest a simpler classification based on complete behavior:

1. Feature Sequence Hashing: these techniques map features and measure similarity by feature sequences.
2. Byte Sequence Existence: these algorithms detect byte sequences (blocks) in the input. Comparing common blocks between similarity digests yields the similarity score.
3. Locality-Sensitive Hashing: Algorithms group related things into buckets with high probability.

The authors examine similarity digest algorithm attacks and their enabling algorithms. Set concatenation similarity digest techniques use the Bloom filter storage structure. This space-efficient probabilistic data format has a shifting issue. If an opponent knows which characteristics will be extracted from a digital artifact, s/he must modify 1 of 7 traits to lower the similarity score to zero. A competent adversary can fabricate input to get a similar block. Block similarity (selection function) and features overlap (intersection dimension yes) similarity digest techniques are vulnerable to this attack. Changing the number of successive features can challenge this method (incrementing or decrementing it by one). This attack targets similarity digest methods that create features utilizing a trigger function as a support function.

A falsified input can modify the trigger function to generate insufficient digest characteristics. ssdeep can be exploited by avoiding byte sequences that match the trigger function. A competent adversary can manufacture an input so that the digest computed after deduplication has fewer common elements than expected. This attack may require too many improvements for real-world use.

The length of the feature should be short, static, and have intersections (overlapping). The algorithms that use a dynamic feature size require an input-splitting support function. If the output produced by the mapping function output is large, bit reduction is acceptable. To prevent uncovered gaps from being used to conceal data while still achieving high similarity scores, it is preferable to have a complete coverage. It is challenging to construct a robust algorithm with this property.

The usage of dynamic-length features and a fixed-size digest is problematic when comparing inputs of vastly differing sizes (for example, ssdeep). The use of a limited cardinality of features as a representation of the whole implies incomplete coverage, exposing gaps that an attacker could exploit.

5.3.8. Semantic based methodology

A uniform representation of domain concepts could facilitate the development of a semi-automatic method to aid investigators during the analysis phase if a semantic approach is used. In addition, the use of semantic tools and software libraries simplifies the establishment of inter-entity interactions, the verification of knowledge consistency, and the inference of new information [64].

The authors present a semantic-based methodology that improves the forensic investigation analysis process in terms of evidence discovery, integrity, and correlation. Separate modules for extraction, semantic representation, analysis, and querying constitute the methodology. They are based on a domain ontology and other language artifacts that enable forensic domain definition along with improved retrieval and correlation performance. The method conducts natural language processing tasks, such as Named Entity Recognition and Co-Referencing, which enhance the number of relationships with relevant entities, such as Persons, Locations, and Organizations, among others.

Using Natural Language Processing (NLP) tools, the proposed methodology includes a Document Analysis step. The goal of natural language processing techniques is to extract structured information from unstructured or semi-structured materials written in natural language. This necessitates the development of a capacity for semantic interpretation linked to the language employed and the "domain" to which it refers. During the "Reasoning" step, an OWL-based (OWL is a family of knowledge representation languages for authoring ontologies) reasoner processes RDF-represented data (RDF refers to Resource Description Framework). During the "Ontological Representation" phase, all annotations, metadata, and structured data are represented using the subject–predicate–object format.

Each instance of the gathered data is uniquely identifiable by a Universal Resource Identifier and is described by a large number of predicates that identify the subject-object relationships. Thanks to the hierarchical nature of the classes' taxonomy, as well as ontology relations and constraints, the reasoner is able to correlate instances with greater precision than asserted data. Semantic Web Rule Language is used to represent complicated attributes on Web resources when OWL's expressive capacity is insufficient.

System setup is dependent on the accessibility of language and processing resources that describe the context. A general implementation of the proposed methodology and a description of the employed tools and techniques are offered. The binary content of documents is loaded by the Evidence Manager module, which detects the source type and confirms the file integrity. General Architecture for Text Engineering offers a collection of resources (Processing Resource) that are loaded based on the sort of analysis to be performed. Tokeniser, Sentence Splitter (splits text into sentences), Gazetteer (used for Lookup annotations), and JAPE transducer are the most important pull requests (verifies the matching between annotations). Relevant to GATE Developer is the OWLIM plugin, which is able to handle OWL ontologies in RDF/XML, N3, NTriples, and Turtle formats.

Various events in a logging system application can be automatically labeled with their corresponding event category. The detection rate of the system exceeds 85%, while the rate of false positives never exceeds 3%. Considering the two most typical groups of occurrences in the test dataset, the reasoning and rule assessment processes are evaluated.

Digital Forensics is an application field due to the fact that it frequently needs Information Extraction and Retrieval tasks and, more importantly, the correlation of information from various sources. The advantage of the semantic method is the creation of relationships between elements within a certain domain. Moreover, with the assistance of the inference mechanism typical of the current triple-store, it is possible to draw implicit knowledge from the extracted evidence.

5.3.9. Quantum computers

A forensic method that is compatible with quantum computers and that necessitates such an endeavor. Given that computer systems must adhere to the laws of physics, a connection between forensics and quantum physics is not that far-fetched. Tomorrow will see the beginning of the quantum world, and with it, a fundamental shift of the digital forensics field. "Strong facts" are the states of electrical signals, or the data represented by those signals. These signals represent 0 and 1 binary states at their core [65].

Forensic investigators will enter a universe in which common perceptions of reality disintegrate. This odd environment will no longer be characterized by position and time, but rather by ambiguity and disorder. For instance, the Uncertainty Principle describes uncertainty regarding the precise position and momentum of particles. In quantum mechanics, the instant a particle is measured, it "collapses" from coherent, indeterminate quantum "eigenstates" into a single basic state, a classical state. Quantum computing permits particles to exist in superposed and entangled states. These are important to the operation of quantum computers and the "qubits" that comprise their essence.

The authors present a proof-of-concept forensic experiment conducted to "recover" binary values from a quantum system. Quantum systems have not yet been the subject of any digital forensic investigator experiments. The success criterion for this proposal is to demonstrate an effective method for acquiring data from such a quantum system.

Using reversible quantum gates, a forensic investigator can use quantum computing in the field of forensics. These gates use the peculiar characteristics of qubits to address difficulties such as decoherence, entanglement, and error correction. For example, "contemporary quantum computers do not work exactly as specified in the circuit model," so faults should be anticipated. Some argue that the manner in which current "Noisy Intermediate Scale Quantum" (NISQ) computers and future error-correcting systems manage faults remains a fundamental distinction between the two. In quantum computing, entanglement is the concept of two qubits being in a state where describing one without the other makes little sense.

A forensic investigator must take into account noise brought into a quantum system and acknowledge that errors can and do occur in probability computations. With entanglement, other elements, such as a third party named Telamon, become immensely intriguing. One party may entanglement the qubits in order to prepare them for their peers, such as two recipients. This quantum behavior differs slightly from a conventional two-party connection.

This exotic transfer of qubits between parties cannot be achieved on IBM's current quantum hardware, although it can be shown in part. While entangled, the qubits can be completely reversed by applying the same reversible gates in the same order. To determine how this may appear in terms of probability, the researchers performed a 1000-shot reverse Bell State on ibmq_lima. And to prove the correctness of this reversible Bell state, a binary of 01 must be obtained. This will allow the forensic investigator to rebuild and trace the quantum system's inputs with the knowledge of how the system and, eventually, the qubits have been encoded.

If a third party witnesses the qubit before the system has been evaluated, the entangled data will collapse. This is because the state must be inverted from its superposition state prior to decoherence. In circumstances of entangled data, if left unattended in a quantum state, the data will decohere.

Cybercriminals may "transform" classical data into a quantum system to obfuscate it and thwart examination in the same manner that investigators will be hampered by the constraints of controlled "decoherence." For example, classical probability distributions of data could be transformed into quantum states. This method may not be more hygienic or effective than normal data deletion, and it may be more difficult. Hardware extraction of data from qubits could also pose difficulties for investigators. In some senses, the potential for live forensics is a topic for a problem that does not now exist, but may one day be of enormous importance.

To keep ahead of cybercriminals, forensic investigators must maintain an advantage in both methodology and knowledge of computer systems. Similarly, with the collaboration of the research communities, it may be possible to engineer answers to issues before they occur.

5.4. Privacy

Digital technologies and the data they contain now feature prominently in many criminal investigations. As a result, many devices become a 'digital witness' to events initiated or experienced by their user/owner. These devices are likely to contain data describing any device user's relationships with others. If such data would offer no tangible benefit to an investigation, efforts should be made to prevent its capture and analysis. It is inevitable that private information will attract the attention of investigating authorities in many cases of a suspected incident [66].

It also raises concerns in regards to potential privacy invasion. Recent attention has focused on the interrogation of smartphone data and the apprehension surrounding police approaches to the extraction and processing of their data. The needs of forensic investigators are often in direct conflict with the right to privacy of those whose actions are being investigated. Digital forensic procedures are invasive by their very nature as they are designed for data acquisition, recovery and analysis. The challenge lies with whether information can be provided in a form that allows these hypotheses to be tested without revealing all of the suspect's private information.

Data that is exposed during an investigation cannot be made private again following its completion, privacy preservation cannot be an afterthought, but rather one which requires prominence in any strategy development. Non-privacy considerate forensic strategies can have an irreversible impact on those subject to investigation. Practitioners do not initially know what data resides upon a device and therefore must treat all contents as initially private.

The remit of digital device data for supporting any number of inquiries is potentially vast as digital data is 'created in ever-increasing volumes and detail'. There is an important balancing act to be struck - the effective investigation of an alleged criminal act and the preservation of privacy for those involved. An investigation should commence without prejudice or bias, and both propositions of innocence and guilt should be evaluated. Most digital devices will contain data that is not solely attributable to its primary user; data originating from or describing non-device users (for example, friends of the device user) will also be present.

Each of the stakeholders (primary owner/user, secondary user(s), external party and service provider) in the balance between their privacy and any data held on the device. There are a number of challenges that exist to ensure that data is appropriately processed. These include obtaining consent by parties who may have data that has become part of a device examination, and challenges around the management and retention of data.

The author suggests ten Privacy-Preserving Data Processing Principles for individuals doing digital forensic examinations and interrogations of digital device data:

1. Prior to its implementation, the scope of any investigation should be established and assessed to ensure that it is both proportionate and justifiable in terms of breadth and depth. When feasible and appropriate, steps should be taken to reduce privacy invasion, and these steps should be documented.
2. The extraction and evaluation of all available digital data from a given device or combination of devices should be reserved for situations in which the use of tailored methodologies for data extraction and examination could undermine the investigation's goal.
3. When it is determined that it is necessary to extract and examine all available digital data from a given device or set of devices, this requirement must be supported by evidence and justified in light of the current investigation scenario.
4. The scope of an investigation should be considered dynamic, with maximum privacy protection measures serving as a starting point. When required, examining processes might expand their scope of investigation to explore reasonable avenues of enquiry. The investigation strategy should be well-defined and resistant to the examination of speculative data/inferences.
5. Those performing an investigation of a device must acknowledge when a predetermined investigation threshold has been reached and cease further investigation.
6. The investigative uses of any data uncovered during an investigation must be subject to oversight and comply with legal and procedural requirements.
7. Prior to "full data scrutiny," the targeted inspection of the extracted data set using relevant, evaluated screening procedures and criteria should be considered in situations where tailored data extraction from a device is not possible.
8. All decision-making processes deployed by the investigating authority leading to the development and deployment of an

examination strategy must be both documented and available for transparent evaluation by a third party.

9. The investigating authorities should take measures to define and consistently conduct digital device investigations.
10. When an acceptable relationship exists between the investigating authority and device owner, all stated investigative methods and any modifications to them should be conveyed in a timely manner and in a transparent manner.

Digital forensics and privacy are inherently incompatible notions. Legal regulation with an emphasis on digital privacy has had to be developed rapidly and is frequently reactive. Existing privacy-focused legislative provisions must be interpreted in a manner consistent with the acts done during a digital forensic examination. In addition to analysing accessible data, having access to it also presents issues in terms of protecting privacy.

Some members of the public consider the examination of electronic devices an invasion of one's mind. It may be easier for practitioners to spot potential privacy-related issues if vendors produce more transparent and comprehensive documentation. The protection of privacy should be a major concern in all investigations involving the examination of a digital device and its data. Those who initiate inquiries should not do so with the presumption of guilt.

Every enquiry has the potential to uncover that the concerns that prompted it were unfounded. The investigative process is usually intrusive, and its effects must be mitigated to allow individuals to return to their pre-investigation positions as closely as possible.

5.4.1. Privacy impact assessment

Directive (EU) 2016/680 of the European Parliament and of the Council governs the processing of personal data pertaining to large-scale digital evidence in criminal investigations (the so-called Police Directive). This legislation went into force on 5 May 2016 and repeals Framework Decision 2008/977/JHA of the Council. Article 1 mandates that data controllers conduct a Data Protection Impact Assessment (DPIA) in accordance with Article 27. The right to the protection of personal data is not absolute; its exercise may be limited to ensure the protection of other rights, such as the protection of society against crime and terrorism. The Police Data Protection Agency (PIA) can be viewed as an extension of the Data Protection Directive (DPD). Article 27(2) of the DPD specifies the minimum requirements for running a PIA. Numerous scholars, governments, Data Protection Authorities (DPAs), and standards groups propose PIA methodologies [67].

Since the mid-1990s, PIAs have been explored in depth and cover both the right to privacy and the protection of personal data. Costs associated with ignoring the singular nature of police activity can be insufficient. Hansken is the successor to Xiraf, which was an XML-based system for managing and querying forensic traces from a large volume of seized digital data. The data, software, storage, and processing capability are centralized, as opposed to the typical digital investigative procedure. Hansken was created for three primary reasons: to minimize case lead time, maximize trace coverage, and specialize interested parties. In light of the sensitive nature of the processed data on such a big data platform, the designers outlined eight design principles. Even though law enforcement processing is legally justifiable, there is always the possibility of interference with fundamental rights. To reduce this interference as much as possible, PIAs and safeguards should be incorporated into processes and systems. The Republic of Slovenia issued PIA recommendations for the adoption of new police powers in 2014. The Dutch government created its own PIA model for writing legislation pertaining not just to police powers, but also to other legal fields.

Hansken, a digital search engine from the Netherlands Forensic Institute (NFI), processes and investigates large amounts of seized digital data. Hansken handles significant amounts of special category and criminal conviction data. This processing may put human rights at risk. Hansken investigates cases at police and Public Prosecution Service request (PPS).

Hasken is also used to develop libraries, software, and Hansken courses that NFI controls. Hansken uses HDFS, which automatically replicates files three times. All central service requests—authentication, authorization, data uploads, forensic queries, content retrievals—are logged. Log messages with privacy-sensitive information are anonymised (irreversible) or deidentified.

Humans constantly make data subject decisions and Hansken analyzes big data obtained from several sources. Data are analysed to find clues for investigations. Hansken's algorithms and methods have been peer-reviewed and results were found credible in the Ennetcom case (ECLI: Netherlands: RBAMS: 2018:2504).

Because Hansken seeks links in a process that can provide evidence, all data processed are necessary for the purpose. Due to its volume and sensitivity, unauthorized data access can cause significant harm to data subjects. Personal data may be misused. Processing could also be used to manipulate evidence by altering position or movement data. If data isn't available 24/7, digital investigations will provide less evidence and take longer to solve.

Measures to address privacy risks include:

1. Only security-cleared personnel should access the platform.
2. If an investigator leaves a case, case data should be removed promptly.
3. LEAs must adhere to all data retention laws. Anonymize data for longer retention. Develop secure personal data destruction guidelines. Retention and destroy policies must be enforced by procedures.
4. Investigators should encrypt case data and trace queries.
5. Platform software, especially forensic analysis tools, should be privacy-analysed.
6. Criminal prosecution should exclude confidentiality communication, such as legal professional privilege. Unfortunately, no forensically sound technique can guarantee confidentiality communication, and present practices require manual involvement. Thus, such information should be safeguarded. To filter out privileged data, a list of keywords can be given in advance. The defence lawyer may suggest keywords. Searching for these keywords requires reason. The inquiry may fail to filter out privileged traces. An investigator may mark traces as privileged and filter them instantly. Some data may be misclassified as privileged. If so, a non-investigating officer can restore non-privileged data.
7. If personal data is disclosed, notify the supervisory authority (e.g., PPS or DPA) immediately to reduce risk.
8. Anonymize training and software testing datasets.
9. To prevent unauthorized access to sensitive data, strict access control policies are needed.
10. To detect privacy breaches and preserve evidence, user/system activity should be tracked and ascribed. The Police Directive requires logs to include the justification, date, and time of operations, as well as the identity of the person who consulted or revealed personal data and the recipients of such data. The article restricts log use. Pseudonymizing logs protects employee privacy.
11. The big data forensic platform should record user actions for purpose limitation. Audit trails can verify that forensic investigators are following a warrant/court order and strengthen evidence credibility (Adams, 2008). Unique user profiles attached to analysts that allow for varied degrees of data access based on responsibilities assigned and clearance given can improve auditing.
12. During the investigation, case data (seized digital material) must be treated cautiously when gathering data from third parties and uploading it to the platform. An exact copy of the digital material should be stored outside of the platform's processing and used for

tracing. Hash functions and MACs can be used to verify its integrity and reduce errors.

13. Classifying data by reliability ensures accuracy. UK data are categorised into five categories: (A) Directly known to the source, (B) Indirectly known but corroborated, (C) Indirectly known, (D) Not known, (E) Suspected untrue. Additionally, primary data sources (those that generate data) should be distinguished from secondary ones (those that link and (re)use them).
14. Differentiate data subjects. According to Article 6 of the Police Directive, prisoners, suspects, victims, witnesses, and third parties should have their personal data processed differently. Different data subjects may require irreversible or de-identified anonymization.
15. The training data, learning algorithm, and other potential discriminating elements should be checked for biases against humans (especially for profiling). They'll be banned.
16. The platform should employ scientifically established algorithms and methodologies. Their possible influence on natural persons should decide their margin of error.
17. Competent authorities should post their PIA reports online.

Processing of personal data in a big data forensic platform is not transparent. Data subjects such as suspects do not always know if and how their personal data are being processed. Since it is difficult to determine in advance which information is relevant to the case, data minimization might not be implemented in criminal investigations. Seized digital material may contain large amounts of common and sensitive personal data of everyone involved in a crime. Processing for forensic purposes is more likely to result in an interference in the fundamental rights of data subjects. PIAs may be of benefit to minimize this interference and should be carried out before the development of such platforms.

5.5. Phase-oriented Advice and Review Structure

Peer review is commonly viewed as the organization's final (and in some situations, primary) quality control check. It is naturally regarded as a singular item that verifies "everything" a practitioner has done at completion of their work on a particular case. A traditional peer review must evaluate the entirety of the investigative procedure. The Phase-oriented Advice and Review Structure (PARS) methodology permits more manageable sub-reviews. It also allows for the identification and correction of systematic errors that may be overlooked or difficult to discover later [68].

The five 'stages' of the proposed review structure enforce an iterative approach to peer review. Each investigation should undergo four 'Advisor Checkpoints' and a concluding 'Review.' Formally recognizing the necessity for a "conflict resolution stage" in the peer review process is required. A person performing both the 'Advisor' and 'Reviewer' jobs may be unable to provide adequate feedback at the peer review stage. It is envisioned that a single individual will serve as the Advisor, guiding the practitioner through each of the five Checkpoints.

Despite the importance of assuring scientifically sound management of digital evidence in the PARS, the Advisor's duties might be defined as a combination of investigative and forensic activities. It is believed that having a distinct Advisor for each stage could be cumbersome for an organization.

5.5.1. The PARS model

The PARS approach is intended for any organizations conducting digital forensics investigation work, including both private and public labs. This study opts to consolidate current framework debates and provides a clear necessity for peer review as a component of an investigational process. Multiple standards are required for process uniformity and quality assurance.

Each of the five stages of the digital forensics procedure includes a corresponding checklist. Each phase must be scrutinised to ensure that all pertinent information and evidence is present and verified. An enquiry that begins with a wide and comprehensive "find evidence" strategy is not necessarily effective or efficient.

In criminal investigations, it is common to formulate and test investigative hypotheses. This permits the practitioner to comprehend the expansive scope of an investigation in criminal circumstances. The majority of digital forensics work necessitates a combination of diverse knowledge components in order to conduct a thorough assessment. This comprises investigation and legal expertise, as well as the ability to anticipate where relevant digital traces may be located.

Checkpoint 1 evaluates all content prior to initiating the real investigation. Checkpoint 2 oversees the device identification, handling, preservation, and acquisition operations. The significance of Checkpoint 2 stems from the fact that mistakes at this stage of an investigation can be disastrous. Now, remote data sources must be considered in every circumstance. Mishandling a device can result in irreversible modifications or corruption of digital content. Oftentimes, errors that occur during the data gathering phase are irrevocable and may have significant ramifications for the investigation's continuation.

At this level, it is necessary to evaluate the practitioner's processes and procedures, with the following themes to be addressed:

- The behaviours associated with the offence under investigation.
- Developing a strategy for assessing whether such behavior is present on digital exhibits.
- An examination strategy should be developed based on the case information, the investigative hypotheses, and the aim of the task.
- The chosen procedure should be evaluated for suitability and lawfulness, to ensure that the evaluation does not violate privacy or legal authority.

This includes checking the setup of each instrument to ensure that it is configured to handle data in accordance with the practitioner's preferences. The case material, the investigation hypotheses, and the objective of the task should inform the formulation of an analysis strategy. Consider whether the objective is investigative guidance, an evaluative opinion, a verification/factual outcome, or a combination of these. This has ramifications for the analysis of future evidence.

A temporal analysis focuses on the time and sequence of events; a timeline provides insight into what occurred and in what order. The evidence analysis will investigate evidence ownership and accessibility. Any analysis including interpretation or evaluation must adhere to the criteria of equilibrium, rationality, rigour, and openness. For instance, a negative discovery can only be considered if the information search is completed with appropriate precision and effort.

Checkpoint 5 is a review of the four prior Checkpoints. It works as a gatekeeper, stopping investigations that are incomplete from advancing. The Advisor must first endorse the practitioner's work by "signing off" on it. If there is consensus, the practitioner might next proceed to report their findings in writing.

The product of an investigation is subjected to peer review at the reporting and presentation phase. Typically, this would comprise a written statement or report, although examination logs or notes may also give valuable information for the review. A proofread is a thorough examination of a document's spelling and grammar.

A review of sense determines if the report makes sense as evidence. Conceptual reviews evaluate the report's content without verifying the outcomes. The primary focus of the assessment will be on the report's science and reasoning. The Examiner should concentrate on the following areas of concern: ethical, legal, practitioner/team behavior, and the presumption of innocence. It is vital to note that when a Reviewer chooses a peer review type at Levels 1–4, the evaluation is based on the analysis report's statements of evidence results.

Level 7 - Reassessment: A re-examination entails a second examination, analysis, interpretation, and report by someone who has not previously worked on the case. This sort of evaluation will be the most time- and resource-intensive, but it will arguably provide the finest opportunity to examine the practitioner's outcomes.

A review process without a dispute resolution system carries the danger of reaching an impasse that cannot be resolved by the two parties (practitioner and reviewer) alone. The resolution of disputes should be escalated to the management level. Disagreements should be brought to management's notice for enquiry and recording of resolution. When a dispute is filed, formal resolution procedures must commence by including the management hierarchy. Some evidentiary circumstances may hinge on the quantity or quality of the evidence upon which a decision must be made. Occasionally, the information is insufficiently thorough or accurate for a choice to be made.

The PARS paradigm outlines two major responsibilities: Advisor and Reviewer. As the need for advice will change, advisors should dynamically dedicate their time to Checkpoints where assistance is most needed. It is not possible to assign the same amount of time to each Checkpoint due to the variable size of the tasks at each stage. The role of the Reviewer is limited to review and evaluate the stated findings of a practitioner. The amount of time provided in this section depends on the agreed-upon review option chosen from the Peer Review Hierarchy.

The evaluation criteria for each Checkpoint and subsequent peer review type are included in the associated evaluation templates. This should facilitate the installation of the PARS. Risk management and risk-based thinking are included into credible recommendations and standards, such as ENFSI and ISO 9001:2015.

Both the traits that will inevitably lead to a peer review selection and those that may lead to a greater scope should be evaluated by an organization. The PARS employs a standard "traffic light" system at each Checkpoint or review level. The Advisor's primary responsibility is to guide and advise, while the Reviewer's responsibility is to prevent subpar work from leaving the organization. Reviewer is a role reserved for senior members of an organization. A Consultant will provide guidance and assistance to the practitioner doing the evaluated task.

Both positions would require professional digital forensics knowledge and expertise. Training for the position of Advisor should preferably involve supervision instruction. Reviews are only as reliable as the knowledge of the critic. To ensure a high standard of quality, the initial examiner should be unable to appoint Reviewers. The most effective way to eliminate cognitive bias implications is to ensure that the Advisor and Reviewer are two distinct individuals.

A change in Advisor/Reviewer personnel raises the question of whether the Reviewer stage should be handled in complete secrecy. There is a substantial corpus of empirical research from various forensic science fields on the effect of contextual information on observations and conclusions. In academic journals, double-blind peer review is also typically regarded as the gold standard for peer review. Double-blind review is the gold standard for digital forensics peer review, but not all units and organizations can achieve this.

Each inquiry should maintain a single Advice and Review Structure Advisors template with the case documentation throughout its entirety. Regarding any agreed-upon activities, the practitioner and the Advisor update this document at each Checkpoint. It oversees what was inspected and evaluated as part of the evaluation. The recording of a PARS review provides three organizational advantages:

- Traditional peer review processes may have an informal structure and lack a comprehensive record of what occurred.
- Why Formalizing the PARS evaluation allows learning from previous assessments in the goal of continual improvement
- The positions in PARS are progressive, as Trainee Advisors and Reviewers may find archived reviews to be a valuable training resource, provided they have the capability to do so.

By introducing a proactive peer advise stage contemporaneous with the natural steps of an investigation, the PARS aims to improve quality prior to the peer review stage. By recognizing and preventing errors, PARS aims to enhance the quality of current digital forensics investigations. Systematically using Checkpoints for guidance would increase the organization's capacity to correct systematic errors.

Practitioners of digital forensics have the option to learn and advance their abilities with the aid of an Advisor. The Checkpoints, Peer Review Hierarchy, and Checklists of the PARS framework offer a standardised and transparent review system. This makes it possible to analyze in greater depth what has been done to improve the quality of the inquiry and keep control over its eventual outcome.

5.6. *Multimedia*

Other papers in this volume deal extensively with multimedia forensics; hence, this section will be brief and will focus on digital evidence in relation to data structure. Due to the boom of smart-phone and tablet sales, digital media (pictures and videos) are becoming an increasingly popular way to share information. Digital media can also be used for illegal activities such as film piracy, terrorist propaganda, and child exploitation. During a trial in a court of law, determining the source device of a picture or video might aid to indict a suspect.

5.6.1. *Photo response non-uniformity (PRNU)*

The camera sensor is made of a large number of small photodetectors called pixels. Pixels use the photoelectric effect to convert incident light (photons) to electrons. The PRNU noise is non-temporal, random, and unique to each camera sensor. The estimated fingerprint is made up of two components: the reference pattern (RP) and the linear pattern (LP). The reference pattern contains all the noise components that are systematically present in an image due to artifacts introduced by Color Filter Array interpolation, JPEG compression, and post-processing operations performed in the image acquisition pipeline. A fingerprint with an estimated PRNU noise can be obtained from a series of 10–25 images with flat content (blue skies or black and white walls) by averaging over several hundred thousand exposures [69].

The H.264/AVC video compression standard is the world's leading standard for video compression. It is used by almost all smart-phones and video-sharing platforms (or social media) like YouTube and Facebook. Modern video compression standards share several key operations such as block processing, prediction, transform, quantization, entropy coding. In H.264/AVC, each Macro-block has its quantization parameter which can be a scalar or a quantization matrix like in JPEG (used only in High profile encoder). Quantization is the only operation in video compression that is non-reversible.

In this section, the efficiency of the frame-based video source attribution and the block-based approach under six different scenarios is evaluated. For each scenario, all reference videos are matched against all query videos of the same device and other devices having the same resolution with video PRNU fingerprints. Block-based approach is capable to link YouTube videos with a higher accuracy than the frame-based methods. This is due to the fact that when a video has lot of motion (scene change), the encoder has to keep more non-zero DCT-AC coefficients to cope with the changes in the scene.

The proposed scheme takes into account the effect of H.264/AVC video encoding on the PRNU noise in video frames. The efficacy of the proposed method (called block-based method) is evaluated on non-stabilized videos with Receiver Operating Characteristic (ROC) plots and Area-Under-the-Curve (AUC) measurements. Using all frames (I, B, P frames) yields better source attribution accuracy than using only I frames even when the investigated videos have been recompressed by YouTube. The main advantage of the proposed method is that it uses only frame blocks that have correct PRNU components. This means that, despite of compression, there is still enough valid PRNU noise in P and B frames to improve the I-frames estimated PRNU fingerprint.

YouTube re-compresses 1080p videos using the H.264 High profile (whereas it uses the Main profile for 720p videos).

5.6.2. Multimedia analysis in Brazil

There is currently no standard tool for analysing multimedia evidence. There are certain specialist commercial tools whose purpose is to provide suitable media players and some advanced tools, such as image authentication and photogrammetry functions. Because they are primarily built for media editing and entertainment, open-source solutions are typically poorly suited to forensic investigation. Peritus is a framework for the examination of multimedia evidence built by forensic specialists with the standard forensic workflow in mind [70].

Previous authors have suggested an Integrated Digital Forensic Process Model based on these models (IDFPM). Preparation, Incident Response, Physical Investigation, Digital Forensic Investigation, Presentation, and Documentation are the components of the IDFPM. In addition, Digital Forensics as a Service, a new method for analysing digital data (DFaaS), has been proposed, in which forensic copies of digital devices are duplicated and stored in a central location, where they can be analysed using standard techniques. The improved productivity of DFaaS allowed forensic departments to reduce their backlog.

Processed data should be presented in a way that is both user-friendly and suitable for preserving processing or enhancement outcomes. The more complex the data representation at a given processing level, the more difficult it is to detect unusual tool behavior. An experiment reveals that 50% of the effort is spent on technical analysis and 30% on documenting tasks.

In Brazil, multimedia forensic services are responsible for a variety of audio, video, and image analyses, both analogue and digital. Content Analysis, Photogrammetric Analysis, Evidence Authentication, Speaker Comparison, and Facial Comparison are the most important types of tests. All of these studies necessitate a comprehensive understanding of signal processing, digital data, and multimedia technologies and tools. Criminal forensic services are a component of both state and federal law enforcement in Brazil. In addition to the National Institute of Criminalistics, the Federal Police maintains 50 specialised forensic response units.

It is the responsibility of forensic analysts to give investigators, judges, and courts an independent expert advice. In the situations of Speaker Comparison, Facial Comparison, and Evidence Authentication, the conclusions are stated using a verbal scale of likelihood ratios. The Federal Police offers thirteen distinct forensic services, including DNA, digital evidence, chemistry, ballistics, and analysis of multimedia evidence. In 2011, a countrywide survey revealed that at least 342 responding forensic units existed. In contrast, state forensic services typically have little personnel resources. Consequently, their analysts are typically chosen in a more general manner. Survey of 166 Brazilian forensic analysts who attended National Institute of Criminalistics training programmes. Results indicate that 40% of multimedia forensic analysts in Brazil are initially unprepared to deal with multimedia technologies and instruments. These professionals hail from several academic disciplines, with phonoaudiologists, physicists, and odontologists prominently represented. The considerable decentralization of public forensic services and the background diversity of forensic analysts present formidable obstacles to the uniformity of the answer.

5.6.2.1. The Peritus framework. The proposed framework does not encompass the entirety of the digital investigation like the Integrated Digital Forensic Process Model (IDFPM), but it does describe the processing of multimedia evidence and subsequent linked activities. The processes include: Exam Request, Evidence Duplication, Triage, External Interaction, Tool Selection, Analysis, Evidence Derivation, Evaluation, Presentation, Archiving, Access Control, and Documentation. Due to the sensitive and private nature of criminal investigations, it is essential that only authorized individuals have access to the supplied evidence during the whole examination phase. The preparation of working copies should be preceded by a thorough media inspection and the creation of a bitwise copy of the incoming content that has been confirmed. Notable is the significance of safeguarding the original content against accidental change.

When everything is consistent and the essential data is accessible, the inspection moves on to the Tool Selection phase. The compatibility of a tool is contingent upon the multimedia nature (picture, audio, or video) and specifics, like file format, encoding, etc. Analysis is the phase in which the received materials are processed using the previously chosen instruments. The analysis of a particular piece of evidence results in the creation of a new multimedia product. The External Interaction procedure depicts any form of interaction required with external players following the start of the tests.

The Archiving process is the point in the workflow where all pertinent material is archived for future reference and the obtained evidence is either returned to the requester or sent to a custody central. When applicable, it is advised that findings be presented using an approach based on the likelihood ratio. The software architecture is based on a modular design that permits the constant addition of new capabilities and ensures the scalability of the system via plug-ins. The system consists of three distinct components: the Core, the access Interfaces, and the Digital Processing Modules. The Core is in charge of hosting the system's workspace, analysts, report generator, and data logger.

Analysers are fully integrated with the workspace and with each other, enabling the direct invocation of an analyzer from the workspace or from another analyzer. Ongoing work can be saved in project-specific files, and completed projects can be exported to the Peritus workspace. The Report Generator is a tool for generating report draughts that can be adapted to the demands of specific system tools. A Derivation Graph for every derived piece of evidence in the case, inclusive of processing functions and parameters. The entirety of a case's information is included within an archiveable XML file.

The system can register images and user-supplied descriptive information for each imported media, such as kind, brand, nominal capacity, serial number, etc. Each Analyzer must provide its own Interfaces for plug-in access. Workspace-related interfaces give access to registered analyzers, imported files, the background task processing service, as well as metadata and JPEG information readers.

The software is created in C++ utilizing the QT Framework for cross-platform and graphical user interface support. It combines the OpenCV library for image processing with the FFmpeg multimedia package. DocxFactory, used to generate report draughts in MS Word-compatible format, is the lone exception, as it is only compatible with the Windows operating system. Video Content Analysis tools are intended to enhance the effectiveness of Content Analysis examinations. This suit provides interfaces and features to assist the manual comparison of the questioned face and the reference face. Included are instruments for face alignment, side-by-side facial comparison, Region of Interest (ROI) definition, and annotation of significant facial traits.

The software also includes a camera calibration tool to compensate for CCTV distortions. During the analysis, an optimal navigation approach is provided for switching between numerous videos, each in a separate instance of the Video Analyzer. If necessary, the analyst has access to a collection of video filters. The ability to launch several instances of the analyzers allows for adaptability to differing work contexts. Both collected and processed images on the Frames List serve as markers for direct seeking of video position.

When an image is selected inside the Content Analysis Tool, it is added to a list for use by the Report Generator at a later date. On the associated Report Generator component, the analyst can select from a variety of predefined formatting options to generate the report draught. The Report Generator is the major tool offered by the Peritus program to assist analysts with the Presentation procedure. When a file is double-clicked, the corresponding Analyzer is automatically selected and loaded. The Core automates the majority of the Evidence Derivation process.

Evaluation is complete once all Analysis rounds have concluded and their results have been exported to the workspace. The Peritus program was formally introduced during the first semester of 2019, and since then, the majority of multimedia forensics training events have been wholly or mostly based on the software. Currently, the Access Control process is mostly based on physical control, but among the planned additions is the deployment of integrated access control techniques based on digital certificates. The National Institute of Criminalistics in Brazil has sponsored two training courses for the creation of new Peritus solutions. Existence of a chosen forensic instrument is vital for bringing academia and forensic services closer together and fostering cooperation. Since its inception, the software has been applied a variety of Content Analysis, Facial Comparison, and Photogrammetry scenarios.

5.6.3. *Image provenance*

In a forensic investigation, it is not uncommon to examine hard drives with thousands of images. An investigator is forced to sift through this data if some of the images are assumed to be connected to the case. Investigators need methods to quickly and reliably group these images into helpful classes. New smartphones, compact cameras and DSLRs are released to the public every month, making it hard to keep up-to-date information about camera make and model. The researchers propose considering the task of forensic source grouping from image headers as an open-set problem, and to develop strategies to perform source grouping in presence of an incomplete dataset [71].

The goal of source identification is to detect the acquisition device, make, or model of a picture. This task was also subject of the “Forensic Camera Model Identification Challenge” at the IEEE Signal Processing Cup 2018. The results show that new models share common parameters with known models. They also show that smartphone apps oftentimes do not significantly change the header information, while desktop software oftentimes does. Many software packages preserve some or all of the header information, and oftentimes leave additional characteristic traces that allow to fingerprint software packages.

This work reports that 69.1% of the collected image headers are unique to one specific model. Since it is unlikely that the software stack is fundamentally different from other models, it is hypothesized that the make can be successfully predicted although the model itself is unknown.

5.6.3.1. Tackling the open-set problem. The open-set problem questions how a picture captured by a camera model that has never been observed before can be correlated with known training data. The researchers treat the camera model as one piece in a hierarchy of identifying camera features. Although the make is a less precise indicator than the model, it is possible to make such a forecast. The researchers gathered 2,833,349 photos and their corresponding usernames from Flickr.

The make in the EXIF:Make tag is normalized manually. Images that do not conform to the JPEG standard are discarded. Images having header information indicating the usage of image processing software were not discarded. This kind of data collection is a use case that closely resembles actual settings. The provided values likely represent a minimum for a perfectly clean, thoroughly regulated dataset.

At https://faui1-gitlab.cs.fau.de/mullanptr/flickr data, scripts are provided that enable the download of the dataset from their individual URLs. The number of entries in each of the five EXIF directories and the additional ICC Profile directory are counted, resulting in a six-dimensional integer feature vector. For the encoding-specific parameters, JPEG quantization tables are considered. Following the JPEG zigzag pattern, the quantization matrix is linearized, and each coefficient is employed as a separate feature. These tables can be read directly from the header without image decoding.

Inherently, supervised categorization operates on a closed set of data, meaning that specific labels cannot be assigned to unknown classes. In the circumstance of an unknown camera model j, it is proposed to predict its make I since there are considerably less makes than models, and it can be pretty reliably believed that cameras of the same make are included in the dataset.

5.6.3.2. Variability of header information. Previous study demonstrated that many headers are model-specific. The variety of header information directly affects the difficulty of guessing a model’s manufacturer. This study describes the distribution of metadata extracted from EXIF tags and the color profile. These results are interpreted as a first signal that brand distinction is achievable with such metadata. One group of Canon cameras always has 38 key-value pairs in the ExifIFD directory.

Numerous Nikon models have a median value near the quartile limit, indicating a skewed distribution of values. This preliminary research suggests that header information can discriminate across makes, but models may cluster within a single make. The median number of quantization tables for Nikon models is 91, whereas Canon models with the highest diversity had 64 tables. Only 38% of photos for the Nikon model with the most identical tables shared the most popular one. Multiple Canon models produced identical picture tables in excess of 80% of the time.

The authors claim that this variety of matrices should be taken into account to reduce the number of false-negative assignments. These results are additional evidence for the possibility of associating brands with quantization matrices. Each model consists of at least 100 photographs, and if there are more than 1000 images, 1000 are selected at random from the pool.

This 10-to-1 class imbalance is a result of the significant diversity among models per manufacturer. Accuracy represents the proportion of photos in which the model’s manufacturer is properly identified. The classification algorithm is trained on training data to predict the brand. The performance of Samsung devices is the poorest, with a median accuracy of just over 20%. Apple continues to perform the best, but its precision has decreased significantly.

A classifier can be successfully trained for source association with an accuracy of 90% or higher due to the relative robustness of the metadata structure across numerous manufacturer models. The performance of the combined feature vector in LABEL:et allfeatures does not surpass that of metadata directory features. A mapping of the quantization features to a lower-dimensional space could be advantageous to this combined feature combination. In the preceding experiment, a random forest was trained using photos that had been processed by third-party software.

Here, a classifier is trained on photos where the EXIF:Program field contains the name of a processing software and attempt to identify the camera manufacturer. Overall, the median accuracy of all photos with an Exif:Software field is between 50 and 75% for mobile applications and between 10 and 50% for desktop software. The performance of the classifier is evaluated on images that have undergone significant software processing changes. The authors hypothesize that apps are more likely to reuse library functions from the smartphone operating system stack, which has a smaller impact on the JPEG headers than desktop program processing. Several versions of Camera can be recognized with recognition accuracies ranging from 77% to 90%, however version “2863" can only be recognized with a recognition accuracies of 43%.

5.6.4. *Picture acquisition timeslot*

Temporal digital evidence can provide details of event sequences, activity levels and timing. Images and other visual recordings are important means to document at any instant in time the condition of specific subjects [72].

It is crucial that every possible measure should be taken to ensure the reliability and accuracy of picture dating. Digital image forensics aims to estimate the time of acquisition of digital pictures taken by a camera and to know the conditions under which each picture was taken, such as exposure, date and time. Increasing importance of temporal information has created a need to develop the forensic techniques for temporal forensic image analysis. Defective pixels located in an image sensor often produce output differently from the neighboring pixel outputs. This damage is actually due to the impact of cosmic ray radiations that causes defective pixels, not material degradation.

The most prominent defective pixel types which occur in the sensor over its lifetime are stuck and hot pixels. The quality of digital images produced by digital sensors are mostly affected by dark current and hot pixels. Hot pixel defects growth rate become higher when the pixel size is reduced to 1 μm. Results on cell phones indicate that defect density increases below 2 μm. These potential pixels are permanent parts of the digital camera sensor.

The proposed system is divided into three stages to estimate the acquisition time of digital images. The first stage aims at extracting a number of potential defective pixel locations from every image block. In the second stage, the system is retrained only for the best selected locations of pixel defects. The proposed system uses a number of pixel locations to extract reliable features for acquisition time estimation. The behavior of pixels over time is analysed to identify the reasonable candidates of the defective pixels.

The predicted virtual timeslots are then considered in the reconstruction step to determine the predicted actual timeslot for a query image and fused in a majority voting method. In each block, all pixel locations are used to train classifiers accordingly and assess their performance on a validation subset. In the training stage, location-based decisions in the form of class labels for each image block are first obtained for virtual subclasses.

Each trained classifier corresponding to a specific defective pixel location can predict a virtual timeslot, accordingly. The last stage combines the predicted class labels on a number of image blocks to boost the performance of the system.

The database of natural images called Northumbria Temporal Image Forensics (NTIF) is considered. A total of 41,684 images were captured from 10 digital cameras with different models and brands. This makes the NTIF dataset unique and beneficial for this particular problem. In the first set of experiments, pixel neighborhood features (i.e., the neighborhood of the centre pixel) are considered using a single image block of size 200 × 200 where the window size for constructing the feature vector is 3 × 3. The system is then re-trained with combined training and validation images using the selected 100 defective pixel locations.

Results show that the combination of pixel neighborhood and local variation features has enhanced the performance of the system for all the tested digital cameras and classifiers. Similar to the previous experiment, the KNN classifier is clearly superior over other classifiers for picture acquisition timeslot prediction. In this experiment, the contribution of multiple non-overlapping image blocks is combined through majority voting using the same dataset. It can be seen that the proposed system improves considerably with an accuracy ranging from 88 to 93. Once the classifiers are trained, the decision can be reached in a much faster fashion.

5.7. Memory forensics

Formal memory forensics arrived on the scene as early as 2001. Much work has subsequently been conducted in the areas of memory acquisition, and memory analysis. Memory forensics seems to add complexity, but it is needed for an increasingly complex digital world. Data extraction, being an important goal of memory analysis can be heavily reliant on reverse engineering. Manual searches can be time consuming and lag behind the most current operating system version. With YARA, a useful pattern matching tool for malware detection, textual and binary patterns can be quickly identified.

5.7.1. Memory acquisition techniques

Main memory analysis has become an essential digital forensic technique due to the increased prevalence of encryption and cloud storage. Important information such as encryption keys, the location of network storage areas and malware analysis can be retrieved from RAM. Memory is usually acquired prior to analysis for which there are several tools available.

It is necessary to first understand several hardware concepts in order to understand the ways in which memory forensics can be applied [73].

- Privilege Rings are hierarchical levels of protection that distinguish between user and supervisor mode in common CPUs. The Intel x86-64 architecture has four native protection rings. Windows and Linux operating systems use only two rings, one each for supervisor mode in which the kernel operates and for user mode in which the applications operate. The protection rings protect assets such as memory regions, I/O ports and privileged CPU instructions. Violating the current protection ring causes a context switch to supervisor mode, allowing the operating system's kernel to manage the fault.
- Virtual Memory is used by modern processors provide hardware support for transparent memory address translations at run time. This is commonly used to separate the address spaces of the kernel and applications. A hardware memory management unit (MMU) translates a virtual address to a physical address using a set of lookup tables in memory. For speedup purposes, processors store already translated virtual to physical address mappings in special hardware caches.
- Direct memory access (DMA) is a technique used to transfer data between peripherals and a system's main memory without the interference of the CPU. DMA allows the CPU to just initiate a transfer without the necessity to wait for it to finish. In modern systems, such memory accesses can be restricted by an input/output memory management unit (IOMMU).
- Virtualizable architectures and virtualization extensions manage the virtual machine environment. A VM is an isolated execution environment that is controlled by a virtual machine monitor (VMM, or hypervisor) A VMM is responsible for scheduling physical resources between the VMs.
- Intel VT-x provides full virtualization of a CPU. The VMM has even more privileges than programs running in ring 0. This is why the privilege level of a hypervisor is usually termed as "ring 1".
- System Management Mode (SMM) is not intended to execute operating systems or user applications. Instead, it is used for low-level management functionality like power management or legacy device emulation. An unmaskable System Management Interrupt (SMI) triggers the SMM. In SMM, the address mode is similar to the 16-bit real mode, i.e., it is only possible to access four GiB of RAM. Since the SMM has even more privileges than a hypervisor, e.g., interrupts are completely disabled, its privilege level can be classified as "ring 2".
- Out-of-band management is part of Intel's Management Engine (ME). AMT is connected to the system's main memory via a DMA engine and allows to access the main CPU's system memory. Other privileged DMA-based techniques also belong into that category. Since the units have the ability to access full system memory and there exist no real control mechanisms, often termed as "ring 3".
- Hardware memory encryption and intel SGX extends modern x86-64 processors to protect user mode code and data from higher privileged layers, like the BIOS, VMM or operating system, using so-called enclaves. AMD came up with its own way to encrypt a system's volatile memory with the help of several processor extensions. The key is randomly created by a hardware random generator at each boot and cannot be accessed by an attacker. Transparent Memory Encryption for Embedded Systems (SME) and Transparent Memory Management Extensions (SEV) are designed to overcome the limitations of SGX. SVE allows software to encrypt memory on a per-page basis and does not require the existence of a VM.

5.7.2. The generic memory access hierarchy

The ring model of Intel, AMD and many other architectures, is a strictly hierarchic order of operating privilege levels that can be used to categorize memory acquisition methods. Below the operating system level is the hypervisor level where multiple OSs can be multiplexed. The SMM is an instance of a further level below which is called synchronous management level. Finally, the lowest level asynchronous is referred to as device level, since software on this level runs concurrently to the main CPU, i.e., there is an interface for that kind of software.

- System model – an address space is a set of synchronous memory that is available for, e.g., a program or the kernel and is designed to be accessed in a homogeneous way. In this context, reading memory means to be able to interpret it, i.e., if A is encrypted and the encryption key is not available within the context of B then A is not accessible from B. The accessibility relation is reflexive and transitive.
- Memory access levels with multiplexing – in a typical x86-64 system, the kernel multiplexes virtual memory by switching address spaces depending on the currently active process. This allows the kernel to maintain paging structures and to isolate the address spaces. If an application tries to access ring 0 memory, the MMU will cause a trap into the kernel.
- Memory access levels without multiplexing – there are cases in which the access hierarchy is linear and does not generally fan out. The SMM of the x86 architecture operates even below a VMM, on ring 2, and has full access to memory of all lower privileged instances. Since there is no hardware support to trap into the SMM in order to schedule several VMMs or kernels, the hierarchy is not able to do memory multiplexing.
- Accessibility with hardware memory encryption – not all access relations match the two cases above. For example, the accessibility relation of processor-based memory encryption technologies. Despite being part of an application's address space, a SGX enclave cannot be accessed from any higher privileged software like the kernel. However, the enclave is able to access the memory of the user process it is part of.
- A generic memory access hierarchy – in general, the accessibility relation will be a partial order. The address spaces A_1 and A_2 of two distinct processes cannot access each other whereas the address space of the kernel can access both. A fan out in the partial order happens when there is a higher privileged instance (e.g., the kernel) multiplexing between the lower privileged instances (e.g., the applications).
- Forensic memory acquisition - assume a program P that is of forensic interest. Investigators are prone to acquire the content of the address space A of program P that is of forensic interest. To acquire memory, assume that there exists an acquisition method Q that runs in address space B at some level of the memory access hierarchy. In case that B is on the same level as A (i.e., A ¼ B) a potential problem of anti-forensic activities and so cases where A < B are preferable in practice.

5.7.3. Taxonomy

A taxonomy of forensic memory acquisition techniques that neither relies on operating system specifics nor on specifics of a particular hardware architecture, focusing on synchronous memory and assuming that the system in question matches the general memory access hierarchy mentioned above.

If program P with address space A and program Q with address space B: The first dimension of the taxonomy is Q's privilege level in the memory access hierarchy. Since some of the acquisition methods like cold boot and SGX are tied to a physical layer, the level of the general access hierarchy is a first dimension. Consider the following ordered list of levels:

- User Level (UL)
- Kernel Level (KL)
- Hypervisor Level (HL)
- Synchronous Management Level (SML)
- Asynchronous Device Level (ADL)

An acquisition software Q is resident on level x if its highest privileged code to access P's memory is executed at level x. This also considers code that Q can request via interfaces like systems calls, and thus does not directly belong to its code base.

An important aspect is an acquisition method's installation time. Incident response teams are often forced to deploy their tools after the occurrence of an incident. However, the installation of acquisition software often alters the memory, e.g. when a kernel driver is installed and loaded, which reduces integrity.

The third dimension of the survey refers to the abort behavior of program P after the deployment of acquisition method Q. Most acquisition methods do not terminate P. However, acquisition methods that terminate the target program often achieve a higher level of atomicity than non-terminating approaches.

Memory forensics has become more important over the last decade. Malware that does not persist itself on a persistent storage device can be observed. Besides kernel level malware, there is also user space malware which uses its own set of techniques in order to get its task accomplished.

Current tools/plugins for code injection detection are not able to cope with the existing injection techniques. It is possible to exploit the paging mechanism in order to hide injected code.

5.7.4. Memory fundamentals and code injection techniques [74]

Remote Shellcode Injection is the simplest form of code injection, with only three steps:

1. Allocate memory with EXECUTE READ WRITE protection in the target remote process.
2. Shellcode is written to the target process.
3. Execute the code injection.

Reflective DLL injection attack steps are similar to Remote Shellcode Injection except that the DLL is written into the allocated memory region. Result of a successful Reflective DLL Injection are typically two new VADs in the victim process with EXECUTE_READWRITE protection and one loaded DLL.

The injection technique AtomBombing got its name from the usage of Windows' global atom table. An atom table is an indexed table, storing strings, while the atom (a 16-bit integer) serves as the index. It is possible to write code from one process to another and rebuilds the functionality of the API WriteProcessMemory.

The general strategy of Process hollowing has not changed considerably first described in 2004; it consists of the following steps.

1. Establish an operation in the suspended condition (ideally with a benign executable).
2. Unmap the executable's original memory location (e.g. via the ZwUnmapViewOfSection API).
3. Transfer the new executable to the target process (e.g. via the WriteProcessMemory API).
4. The beginning address of the paused thread is replaced with the beginning address of the new executable.
5. The thread resumes (e.g. via the ResumeThread API).

Gargoyle is not an injection, but rather a mechanism for hiding code that can be applied to injected code. The technique of Gargoyle is to set the permissions of all malicious code-containing pages to non-executable when the code does not need to run and to set them to executable when the code is running.

Private and shared memory – private memory is intended to be shared among different processes. It is, however, also used by the image loader to map executables, DLLs and device drivers into memory. Shared memory is represented by a so called section object, created with a specific protection.

Page Table Entries and the Page Frame Number database – a Page Table Entry (short PTE) is part of the translation process from a virtual to a physical address and consists of a 64 bit value, split into bitfields and flags. For an active page, it contains the so called Page Frame Number (short PFN), which points at the physical page containing the content for the virtual page. A prototype PTE tries to solve the problem of updating the information for a page shared among different processes. For private memory, this is a MMU PTE and for shared memory it is a PrototypePte. Mapping image files allows us to identify modified pages for mapped image files.

Different states of Page Table Entries – For each state of Page Table Entries, a MMU PTE can be in, there is a specific struct in Windows, describing its bitfields and flags. Depending on the state respectively applied struct, the same bits can have a different meaning.

- Hardware state – MMU PTEs can belong to a private page or to shared memory. For this differentiation the PrototypePte flag of the PFN DB entry must be examined. By checking this bit, a page's executable state as an unset NX bit in this case allows the CPU to fetch and execute instructions can be determined.
- Transition state – If the Valid flag is unset, the MMU does not process the PTE any further but a page fault is generated. While a MMU PTE in transition state is not valid (has an unset Valid flag), the corresponding physical page is still available and the PageFrameNumber still points to it.
- Proto-pointer PTE – MMU PTE is an instance of _MMPTE_PROTOTYPE and serves as a pointer to a prototype PTE. A proto-pointer PTE has the Valid flag unset and the Prototype flag set. It is used in the context of shared memory and occurs when the corresponding physical page has been accessed before, but is currently not anymore in the working set.
- Pagefile state – Another invalid state occurs when the physical page has been written to the pagefile (paged out). This state is represented by a MMU PTE instance of _MMPTE_SOFTWARE, where the Valid, Prototype and Transition flags are all unset but the PageFileHigh field has a non-zero value.
- Unaccessed state – When a VAD has been created but its page(s) not yet accessed, there is no need to actually map a physical page. This initial MMU PTE value is in this case zero and changed when the page is accessed for the first time. For private memory, such a PTE state is also called demand zero.

Large and huge pages – It is possible to allocate large and huge pages that have a size of 2-Mbyte and 1-Gbyte on x86 architectures. Some processors support configurable page sizes, but Windows does not use this feature. Large pages have bit 1 (Valid or Present flag) and 7 (LargePage or PS flag) set, marking them as a large/huge page.

5.7.5. *Memory forensics survey*

In a taxonomy, the access hierarchy level as the main ordering criterion for forensic acquisition methods and work from higher layers (least privileges) down to lower layers [75].

User level is the least privileged level, there exist only a few memory acquisition techniques. A User level acquisition method has full control over a target running on the same privilege level.

- Emulators are one possibility for acquiring memory from within the User level. Thereby, the emulator integrates the acquisition method Q and the guest program corresponds to P. As guest memory is provided by the emulator, it is trivial to create snapshots that preserve atomicity and integrity. An emulator tries to exactly mimic the original system. It fetches, decodes and executes one instruction after another. An instruction is typically represented as a function of the respective programming language. Usually, registers are implemented as global variables which are modified by the corresponding instructions. The same applies to memory, which is usually implemented as some kind of array.
- Built-in debugging interfaces as a part of a debugging interface that allow to dump P's own address space. So, in this case Q is a part of P.

Kernel level – All relevant desktop operating systems come with an integrated memory acquisition functionality – a crash dump. An image of the virtual memory of a process or even the entire physical memory is created whenever the system encounters a critical state. From the kernel level it is possible to dump P's memory, if P runs in either User level or Kernel level.

- Kernel support – most memory acquisition tools running in Kernel level are implemented as kernel drivers. This comes with a few advantages. Compared to techniques that are directly incorporated within the kernel, a kernel driver is easier to develop and faster to deploy. Pmem [76] is one of today's most sophisticated physical memory dumpers. It is part of the well-known memory forensic framework Rekall which is supported on Linux, Windows and MacOS. Pmem features the acquisition of physical memory by either requesting kernel support or by manually mapping physical frames by itself. To defend against malicious hooks that could tamper the acquisition process, Pmem barely uses any kernel APIs. Pmem supports two different memory acquisition modes, depending on the functionality offered by the respective operating system. On Linux, e. g., Pmem acquires all memory regions, that are marked as System RAM in the iomem_resource tree, by using the kernel's kmap functionality. As a second option, Pmem is able to map physical memory entirely independent of kernel APIs and allocates a single page in non-pageable memory, called the rogue page. First, Pmem's initial installation routine slightly alters the kernel's memory, which reduces the integrity of the memory dump. Second, introducing minor modifications to the target system's state is common for almost all acquisition methods at this level. Third, there is always the chance that an already compromised kernel subverts P Memb's acquisition process using antiforensic techniques.
- Crash dumps – when a system or application crashes, developers often rely on a memory dump to investigate its cause. Usually, the dump can be restricted to the address space of the kernel, an application or the entire physical address space. The crashed program or system is the program of forensic interest P while the crash dump component corresponds to the program Q.
- Hibernation files – when a computer hibernates major parts of volatile memory are written to disk in order to restore the state of the system even after power was cut. On Windows systems, the hibernation file is called hiberfil.sys and is located in the root directory (C:\). The file can be converted and analysed using standard memory forensic tools like Volatility (Foundation).
- Debuggers make use of a kernel's debugging support. The debugger (Q) can fully access (i.e., read and write) the debuggee's (P) memory. GDB, released by Stallman in 1986, is probably the most wellknown debugger for UNIX systems. It makes use of the ptrace system call to debug a process (running in user level). GDB's typical workflow can be summarized as follows:. wait for a signal from the debuggee, handle the signal and continue the execution of the target process. Using ptrace, GDB (P) requests the kernel to vicariously access the debugee's (Q) memory. Since ptrace is a standard system call provided by every Linux kernel, no additional code is installed in kernel level. A widely used debugger for the Windows platform is WinDbg (Microsoft Corporation, 2017). Using the presented technique, it is only possible to dump memory from user level applications.

Hypervisor level – Common memory acquisition tools like Pmem or LiME require OS kernel functionalities, i.e., are implemented as drivers. If malware succeeded to gain kernel-level privileges, it is able to subvert the acquisition process using anti-forensic techniques. Direct kernel object manipulation techniques can be used to tamper the output of monitoring tools like the Windows Process Explorer. To counter techniques like Shadow Walker, analysts require approaches that operate with even higher privileges than an operating system's kernel.

- Virtualization tools and Virtual Machine Introspection – standard virtualization solutions like VMware, KVM or Microsoft's Hyper-V usually integrate functionality to acquire a guest's memory. This is when Virtual Machine Introspection (VMI) comes into play. LibVMI is an API for VMI that uses several heuristics to overcome the semantic gap between a hypervisor and its guests. It provides support for KVM, Xen as wells as the creation of static memory snapshots. LibVMI evolved from the XenAccess project (Payne et al., 2007). It is executed from the privileged host system. LibVMI can retrieve information about an OS's kernel symbols but it is not able to introspect user-level symbols. It requires the respective symbol tables which, in case of Linux, cannot always be generated. LibVMI integrates into the VMM, e.g., as a patch to KVM, and must be configured towards different types of guests using a configuration file.
- Forensic post-incident hypervisors – the previous section focused on a priori acquisition techniques, the following VMMs can be installed after a potential incident. As in the previous section, the P has to be part of the running guest system. The VMM integrates the acquisition software Q. HyperSleuth is a framework for forensic live analysis leveraging Intel's VT-x. It uses processing cycles during a system's idle-state to dump memory pages (dump-on-idle). The authors claim data returned from the VMM to be trustworthy. An outer trusted host attests – using a challenge-response protocol – that the DRT is established. HyperSleuth is an anti-malware tool that can detect if a guest has tampered with the output of system monitors like process lists, network connections, loaded drivers, etc. Since it has access to the entire machine, it is able to collect relevant data from outside the VM, without support from the guest OS. Every time the guest executes a hlt instruction, i.e., the CPU is sent to idle state, the VMM dumps remaining memory pages in background. Any difference between these two data sets indicates the presence of kernel level malware. Using these techniques, it is able to acquire the guest's memory at the actual time of request.

Synchronous Management Level – Memory acquisition in SML is quite beneficial because it is independent of the OS or a VMM. Even if there is a malicious OS kernel or a subverted VMM, it is possible to reliably dump the memory of the system. The development and installation process is very different compared to common forensic software. Instead of deploying the acquisition technique into the SMRAM, it could also be integrated into the BIOS itself. The project's current state is just a proof-of-concept implementation, but it has to be installed using hardware tools. First, the motherboard's firmware is dumped via a hardware serial peripheral interface (SPI) programmer. Then, a Python tool extends the functionality of the SMI handler with the acquisition code. The modified image is subsequently written back, once again using the SPI programmer.

Asynchronous device level – All acquisition methods above ADL make use of the main CPU to obtain the target memory. For forensic investigations, it is of great advantage to be able to obtain memory without the need to install any software, simply by plugging-in external hardware. Now, the address space A can be all physical RAM and B still is completely unrelated to A because Q runs on external hardware.

- DMA-based acquisition tools create memory dumps that often do not require to be run on the target system. This is because DMA requests can be sent from an external device. Compared to conventional acquisition approaches, DMA does not interfere with the main CPU's operation, resulting in less system pollution. PCILeech is an open-source project that uses DMA over PCI Express to read and write from a target system's memory. DMA does not interfere with the main CPU's operation, resulting in less system pollution. Most configurations are based on the USB3380 development board or field-programmable gate arrays. The tool can be unplugged without causing any interruptions. To insert a kernel implant into the target system, PCILeech uses a three stage approach. It starts by locating the very end of either the kernel or a driver within the host system's memory. As these pages are already marked as executable the kernel's page tables do not require any modifications. The first page is used to establish a DMA channel from the controlling system to the kernel implant. To propagate the command buffer's base address to the host program, the thread writes its physical address to a previously arranged location. PCILeech is a DMA-based tool that can read or write to the target system's memory, access its file system or execute arbitrary code like system shells. Supported commands are basically reading or writing memory, executing additional code or simply exiting. Inception allows to bypass the Windows lock screen by searching the corresponding code in RAM and shorting the password prompt. It possesses the typical atomicity drawbacks of this class as it misses the ability to acquire memory dumps atomically.
- Cold boot is a special acquisition technique that exploits the remanence effect of DRAM to access memory. The typical scenario of a cold boot attack is to extract a full-disk encryption key. Since the target system is not running at the time of the acquisition, rootkits have no chance to tamper with the acquired memory.

5.7.6. *Hypervisor*

Rootkits are malware that conceal themselves and the malicious payload they carry. Forensics researchers used live memory acquisition to reverse engineer malware. The researchers also undertake a performance analysis of memory acquisition performance statistics on the online system. The developers of Volatility employ reverse engineering to understand the acquired memory [77].

In a few seconds, the complete memory image file is analysed. Since LiME is a pure kernel module, it is straightforward to use it in Android devices. The ARMv8 architecture includes four exception (permission) levels, so the study analyses the memory using Volatility and LiME to discover an irregular condition. LiME generates a representation of the computer's RAM by reading and writing each physical page to the disc or the network.

The researchers focus on lowering the CPU use and heat generated by LiME. Page smearing is a form of incoherent memory and occurs when a page content is modified while it is acquired. There are various reasons for incoherency, such as multiples cores, the increasing quantity of RAM and the kernel heuristics.

In this technique, LiME linearly traverses the memory, and in each cycle it verifies that the current page has not already faulted by checking the pages pool. LiME sends the duplicated page and returns it to the microvisor's pool if the page is resident in the pool. The primary transmission routine of LiME is changed to use less CPU. During the acquisition, each page accessed in Exception Level 1 (refers to the operating system) or Exception Level 2 (refers to the user-space) traps to Exception Level 2 (the hypervisor level), and consequently, must be copied and its address stored.

The hypervisor's page trap must access addresses in both virtual userspace and virtual kernel space. Unfortunately, the ARMv8-a hypervisor MMU can only handle user-space addresses (the upper 16 bits are all zeros) and does not support any kernel virtual addresses. This study quantifies the IPA overhead, presents a performance comparison between the current implementation of LiME to the microvised implementation and demonstrates how RAM incoherency is handled by this technique. RAM is obtained by repeatedly executing the sleep 1 command 50 times.

This indicates that the memory was captured by LiME while the process was running. The incoherency rate for a pool of 1000 pages should be less than 0.4% in busy mode and 0.52% in idle mode. Evidently, running LiME when the system is idle is more efficient. Even the non-linear version of LiME poses no performance problems. The trade-off is a lengthy acquisition period, in some cases exceeding an hour.

5.7.7. Live analysis for ransomware

Ransomware is one of the most pervasive and damaging threats now facing internet users. When ransomware first debuted more than three decades ago, its influence on the computing community was minimal. With the introduction of CryptoLocker ransomware in 2013, the danger environment shifted. WannaCry and NotPetya are two of the largest ransomware outbreaks that have occurred in recent years. Crypto-Ransomware is a form of malware that use distinct encryption and decryption keys [78].

In 2016, Interpol identified ransomware as the greatest malware threat to citizens and businesses. The NotPetya cyberattack is estimated to have cost $10 billion, making it the most expensive cyberattack in history. According to various estimates, WannaCry costs between $4 and $8 billion. Cryptanalysis is one of the most frequently employed forensic techniques for locating encryption keys that may be present in the memory of a computer. Previously held beliefs regarding the organization of cryptographic keys in memory have been refuted, and a number of ways for locating the keys have been offered.

Since the entropy of key data is greater than that of non-key data, one technique to locate a key is to break the data into small portions, measure the entropy of each segment, and highlight the locations where the entropy is particularly high. This research will focus on identifying the key used during the symmetric encryption phase of ransomware execution, as the private key to the asymmetric encryption is never present on the system. Advanced Encryption Standard (AES) key is the key. Some researchers consider it to be practically impregnable and impossible to decrypt without the correct key. Instead of focusing on specific API calls that ransomware may use, the technique outlined combines volatile memory analysis paired with empirical findings.

The process of encrypting a key can take several minutes to several hours, and the program may do effective key management by removing the keys from memory. The matching key schedule for larger AES keys is correspondingly greater.

Using Oracle's VirtualBox virtualization software, the environment was developed. The purpose of the experiments was to establish or reject the premise that live forensic techniques may be used to minimize ransomware attacks. The enquiry can be divided into three distinct sub-experiments, which were integrated to form the total results package. Each experiment began by launching a new version of a virtual system on a realistic workstation and executing a sample of the ransomware under investigation. Experiments on the two most popular Windows operating system versions now in use.

Memory samples were analysed in an effort to identify possible AES keys from the collected memory samples. Results can only be compared if each sample is executed in the same environment, hence a new VM was created for each experiment. Three ransomware samples were chosen for study based on their use of symmetric encryption and the fact that they all encrypted files with the same key. If any candidate keys were found during analysis, they were then used to attempt to decode the encrypted control files recovered from the virtual computer of the victim. Two victim PCs with distinct operating systems were used to test the behavior of the ransomware code, while one machine was used to provide network services.

Prior to the execution of the malware, a copy of the machine's memory was captured so that any AES keys present could be recognized and excluded from the findings. Regular memory dumps are taken throughout the duration of ransomware execution. Using one of the chosen tools, memory dumps were examined to check that the keys were still present. If no keys were discovered, the experiment was extended at 1-min intervals and new memory dumps were collected. Recording the times when the keys were present and creating a rough execution timeline for the ransomware.

5.7.7.1. NotPetya.

When the NotPetya ransomware encrypts a file, the AES Initialization Vector (IV) value is written across the first 16 bytes of the file. A programme was written that first reads the IV value from the encrypted file and then combines it with the key discovered in Experiment 1 to decrypt the file's contents.

Using the same AES key, extracted pdf, doc, docx, xls, and xlsx control files were successfully retrieved using this method. Each of these file formats needed the addition of a unique header, and some also demand the removal of bytes from the file's conclusion.

5.7.7.2. Bad Rabbit.

Bad Rabbit encrypts files using the same format as the NotPetya ransomware, and the same techniques can be used to decrypt files encrypted by Bad Rabbit. Using this method, it was possible to recover pdf, doc, docx, xls, and xlsx files encrypted with the same AES key.

5.7.7.3. Phobos.

The Phobos ransomware appends additional data to the end of a file that has been encrypted. This additional data consists of padding, followed by what is assumed to be the AES IV value, and then 128 bytes that are identical for all encrypted files. This 128-byte block is believed to be the encrypted asymmetric key. There is also a fixed string at the conclusion of the block, which in this example is 'LOCK960. However, other versions of Phobos have been detected with alternative keywords, such as 'DAT260. A program was created that first reads the IV value from the encrypted file, then combines this with the key discovered in Experiment 1 to decode the file. Using this method, it was possible to recover pdf, doc, docx, xls, and xlsx files encrypted with the same AES key.

AES key recovery from volatile memory was used to locate ransomware encryption keys, building on live forensics research. Since no research was found, TrueCrypt and Skype encryption key recovery methods were employed to find keys for recent, high-impact ransomware strains. Second, the approach attempted to establish consistent memory timelines for these keys.

Findaes and RansomAES live forensic tools have similar execution times and outcomes. The author's RansomAES tool performed similarly to findaes, demonstrating that ransomware functionality did not enhance performance. Interrogate took about 100 times longer. Despite this increased execution time, all three programs identified AES keys used by three ransomware strains on Windows 7 and Windows 10. This suggests live forensics could mitigate ransomware attacks. The interrogate tool's increased execution time may be due to its logic for identifying the AES key, which is based on findaes. Interrogate calculates the schedule for all candidate keys regardless of entropy, which may affect performance.

These results support the concept with some forensic investigation constraints. The machine has not been rebooted since the attack began, and the memory capture is done towards the start of the ransomware's execution to guarantee that the essential keys are still in memory. AES keys were not found in the Wannacry ransomware sample, showing that this method does not work for all ransomware families.

A second AES key was found in memory following a ransomware assault like Phobos, where the user could still communicate with the operating system. This key encrypts newly produced files. This method may prevent key recovery and encryption. The keys found during the investigation match earlier studies, suggesting that these supplementary AES keys should be available in memory. Ransomware samples will be analysed to see if secondary keys can be captured and used in forensic investigations.

Building on other work in the field of live forensics, AES key recovery from volatile memory techniques were successfully used to identify encryption keys being used by ransomware samples. As research in this specific area was not identified, techniques and tools used for TrueCrypt and Skype encryption key recovery were used to identify keys for recent, high impact ransomware samples. Secondly the work aimed to attempt to evaluate whether consistent timelines of when these keys where stored in memory could be generated.

Similar execution times and results were recorded for the findaes and RansomAES live forensic tools, The RansomAES tool created by the author had similar results as the pure findaes tool, indicating that the added extra functionality for ransomware did not result in an improvement in performance. The time taken for the interrogate tool to complete was almost 100 times longer. Apart from this extended execution time all three tools were shown to successfully identify AES keys being used by three ransomware samples chosen for the experiments on both windows 7 and windows 10 operating systems. This supports the hypotheses that live forensic techniques could be used to mitigate a ransomware attack. The authors believe that the increased execution time of the interrogate tool could be caused by the implementation of the logic this tool used to identify the AES key as fundamentally it is based on the same research as findaes. Interrogate seems not to take into account the entropy of the candidate keys prior to calculation of the schedule, rather it calculates the schedule for all candidate keys irrespective their entropy and this may be one reason for the impact in performance.

However these results support the hypothesis with some caveats from a forensic investigation point of view. These being that the machine has not been rebooted since the commencement of the attack, and also that the memory capture is performed near the start of the ransomware's execution, to ensure that the required keys are still present in memory. Also this technique cannot be applied to all ransomware families, as demonstrated by the analysis of the Wannacry ransomware sample, where AES keys were not able to be identified.

It was also observed that in case of a ransomware attack where the user was still able to interact with the operating system after the initial encryption has completed, such as the Phobos ransomware, a second AES key looks to be in memory. This key is being used to perform any subsequent encryption, such as on any new files created. This approach being possibly used to frustrate the recovery of the original key and protect the original encryption. The keys found during the work seem to align with suggestions from previous work, which indicate that it was likely that these secondary AES keys in theory should also be available in memory. Further research is planned to analyze various ransomware samples to determine if capture of these secondary keys is also possible and useful in a forensic investigation.

5.7.8. *Auto-start extensibility*

Windows ASEPs can be classified according to the specific OS features used or abused by malicious programs to persist in the system. There are four categories of Windows ASEPs based on the specific OS features: system persistence mechanisms, program loader abuse, application abuse, and system behavior abuse. The proposed taxonomy is independent of the type (disk or memory) of forensics analysis. Some extensibility points can require a refreshed system, i.e., the system has to be rebooted or the user session signed out and then signed in again to launch these programs. Others have different configuration scope, since they can be configured at system-level or at user-level, that is, they affect all the system or the current (signed-in) user session [79].

5.7.8.1. System persistence mechanisms. This category describes the well-known mechanisms provided by Windows to run user programs, privileged tasks, or system services, among others programs. This category includes the extensibility points: run keys, start-up folders, scheduled tasks, and services.

- Run keys are the most well-known extensibility point. These registry keys include the Run, RunOnce, and RunOnceEx. Unlike the Run registry values, the RunOnce registry values are deleted by Windows once the program starts (or when it finishes) its execution. The content of these registry keys may be present in the memory, so they could be detected in memory forensics.
- Startup folder refers to a special Windows folder in which every program or application shortcut contained in the folder is launched during system start-up. This persistent mechanism needs the user session to have been signed out and then signed in again, and its execution scope limited to the application itself.
- Scheduled task is a program that executes periodically when certain conditions are met. This ASEP does not require any freshness of the system (unless system booting or user logging are set as conditions). It affects all the system, while its execution is limited to the application itself.
- Services are background programs that have no user interaction. Like scheduled tasks, they can be triggered when certain conditions are met. Memory forensics may retrieve all registered services from a memory dump. Services are executed with admin privileges to register a new service in the system.

5.7.8.2. Program loader abuse. This category includes the following ASEPs: Image File Execution Options, extension hijacking, shortcuts manipulation and COM hijacking. These extensibility points rely on the techniques based on the abuse of the Windows program loader process. This process can be abused to transparently launch other programs when interacting with a user.

- Image File Execution Options (IFEO) is a Windows feature that allows a developer to launch certain programs directly under a software debugger. To enable it, a new registry subkey with the same name as the application to be debugged must be set in the registry path.
- Extension hijacking is an attack that hijacks the default programs associated with certain file extensions. The program is automatically launched when the user opens these files. This extensibility point may be detected through memory forensics since it relies on the Windows Registry for its existence.
- Shortcuts manipulation refers to when an attacker can change the target application by adding another program to the system. When Windows interprets the command, both programs are launched in parallel. This ASEP has a user configuration scope and thus admin privileges are not needed. It does not need freshness of system.
- Microsoft Component Object Model (COM) hijacking is a subsystem that allows a developer to create software components (such as dynamic link libraries, DLLs for short) that can interact with others. The hijacking consists in modifying the path of the associated DLL to other malicious DLLs. Hijacking does not need freshness of the system to take place. Execution privileges are inherited from the user (per-user COM objects) or from the application that loads the hijacked machine-wide COM object.
- Shim databases are designed to apply patches to a specific binary program prior to its execution. Windows loader checks if there is any patch required for the program before executing it. Shim databases are stored on disk in a path having as root folder C:\Windows \AppPatch.

5.7.8.3. Application abuse. Some popular legitimate programs have the capability to extend their features thanks to plugins extensions. This category describes the extensions of legitimate programs that are abused to persist in the system. This category includes the following ASEPs: trojanized system binaries, Office add-ins, and browser helper objects.

- Trojanized system binary attack modifies a legitimate, system binary program to load another unintended program. System DLLs are a

common target of these attacks. Trojans can be captured in a memory dump if it is running at the time of the memory snapshot.
- Office add-ins allow a user to extend the features of Microsoft Office applications. They consist of a static HTML and a piece of Office-compliant JavaScript code. The binary code is usually in the form of a DLL file, stored in the%ProgramFiles% folder.
- Browser helper objects (BHO) are DLL files that work as plugins for the Internet Explorer browser. Execution privileges are inherited from the user who launched it. Since its installation relies on the Windows Registry, this extensibility point may be tracked down in memory forensics.

5.7.8.4. System behavior abuse. The extensibility points under this category take advantage of the Windows features to launch programs.

- Winlogon is the last process in reading the on-disk hives when loading the specific user settings. It can also be configured to launch certain programs every time a user signs into the system.
- DLL hijacking attacks consist in abusing the DLL search order done by Windows. A legitimate DLL in any of these folders can be substituted with a malicious one. Such a malicious DLL will be loaded every time that a program has any dependency on the substituted legitimate DLL.
- AppInit DLLs is a Windows feature that allows any DLL to be loaded into the address space of every application with a user interface e that is, any application that loads user32.dll. This ASEP may be detected in memory forensics, since it relies on the Windows Registry.
- Active Setup is another Windows feature that enables programs to be launched when a user signs in the system (Klein, 2010). This extensibility point can be configured at system or at per-user level, depending on the root registry key used. Like the previous ASEP, it may be detected in memory forensics since it relies on the registry.

5.7.8.5. Experimental evaluation of Winesap. The tool Winesap is implemented as a Python plugin on top of Volatility. It is specially designed to track down the previously described Windows ASEPs that rely on the Windows Registry. When data is stored as binary or unknown, it tries to parse the content data as a PE header. If it succeeds, it raises a warning message indicating that a suspicious program was detected.

The tool retrieved all the described Windows ASEPs which are detected in memory forensics regardless of their configuration scope. Each extensibility point was also marked as suspicious, since the programs indicated by the extensibility point matched some of the aforementioned suspiciousness conditions. An example of the output of the tool is as follows:

```
WARNING:Suspicious path file HKLM\Software\Microsoft\Windows NT\CurrentVersion\ Image File Execution Options\firefox.exe
Debugger: REG_SZ: C:\Users\me\AppData\Roaming Yztrpxpt\cmd.exe
WARNING: Suspicious path file HKLM\Software\Wow6432Node
\Microsoft Windows\NT\CurrentVersion\WindowsAppInit_DLLs:
REG_SZ: C:\Users\me\AppData Roaming\Uxkgoeaoqbf\autoplay.dll.
```

Winesap cannot check the original ASEPs which triggered the execution of some programs. However, some actions can be performed to overcome this problem. For example, by file carving the memory dump, resource files recently freed by the OS can be obtained and checked for matching with symbolic link files whose paths point to the startup folder or whose value has been manipulated. Once a suspicious process is located, its current directory can be retrieved by means of Windows internal structures and then checked.

5.7.9. Injected code

Volatility and Rekall's malfind plugin examines the protection field of VADs. When a VAD has a specific protection that includes the WRITE and EXECUTE rights, malfind will identify this VAD as potentially malicious and report it. Malfind's VAD may contain malicious code that is not accessible by the malware. This happens when a process maps a view of shared memory with active physical pages but hasn't accessed them yet. It can also be used to hide modified mapped image files from hashtest [80].

5.7.9.1. Detecting hidden injected code. An algorithm is used to retrieve all executable pages of interest and an analysis on processes with deactivated Data Execution Prevention.

The Protection field for a page in transition state defines its protection (NX flag and so on). The OriginalPte field is used to store the protection value while the page is active. The MMU PTE would be faster regarding the plugin runtime, as the PFN DB entry wouldn't have to be read and examined. Mapping a view with READWRITE protection of a EXECUTE_READWRITE section object. The old MMU PTE value does not influence the Protection field.

The algorithm used to retrieve executable pages from memory is described which does not include in unallocated memory pages or unmodified pages of mapped image files. Further tests for some pages, besides their executable state, must be done before they are included in the collection.

Large and huge pages are not referenced by a Page-Table entry. The format of their bit fields is almost the same as for a PTE in Hardware state. This means the executable state of a large and huge page can be obtained.

If the PTE value is zero, the entry can be ignored and skipped directly. This works for private but also shared memory (both anonymous and mapped files). Skipping these PTE values also prevents the printing of never accessed shared memory.

If unset, the page is executable. If it belongs to shared memory, the corresponding VAD for a mapped image file is examined. A private page cannot be distinguished from a shared page solely by looking at the PTE's PageFrameNumber field.

The PTE containing the actual page's state is the prototype PTE. In some cases, this PTE has to be accessed in order to get a page's protection. For example, if the page does not belong to a mapped image file, it is not included.

The protection for a page in this state can be obtained from the MMU PTE by applying the _MMPTE_TRANSITION struct and reading its Protection value.

If the Valid, Prototype and Transition flags are all unset, the MMU PTE is in the pagefile state. Reaching this state means it belongs to memory which has been paged out. The Protection field of the PTE contains the page's protection information.

A mapped data file is typically used to perform read/write operations with the speed advantage of an in-memory file. It is, however, also possible to map a data file with the EXECUTE_READWRITE protection and execute code contained in that file.

DEP is the default for non-essential x86 programs and services on Windows client versions. When DEP is not active, a CPU can execute code from pages with e.g. READWRITE protection. Active MMU PTEs (instances of _MMPTE_HARDWARE) had NX bit set for executing non-executable pages.

5.7.9.2. Evaluation. The algorithm described in the previous Section has been implemented as a Rekall plugin (called ptenum). The code injection techniques were evaluated using Python version 3.7 on both, x86 and x86_64 Windows 7 and Windows 10 VMs.

Executables implement the injection techniques are available in the author's repository. Most of them are only slight modifications of the original author's code. The additional _h and _a for Gargoyle indicates whether the page containing the shellcode is currently hidden (not executable) or active (executable).

Analysis was done with API monitoring and a before and after comparison of memory dumps. No plugin, except ptenum, was able to detect all memory regions containing executable pages. Especially the executable page of Olympic Destroyer was revealed by no other plugin (in particular malfind and hashtest).

The authors demonstrate that it is possible to prevent code injection detection plugins from reporting injected code. They present a novel strategy that can discover executable pages regardless of the planned (or accidental) concealment techniques. Only DEP with paged-out pages and Gargoyle were able to evade the plugin, but this is expected because the impacted pages are not executable. This research is accompanied by a Rekall plugin that implements the proposed methodology and is made available to the public.

Due to the fact that the plugin reports all executable sites (with limitations), regardless of whether they are part of a code injection or benign, it might generate a vast amount of data that must be analysed. Changed pages of mapped picture files are the primary issue. As the plugin allows for their exclusion, it can be used as an enhanced malfind plugin (but would miss code injections in mapped image files). Aside from that, it is unsuitable for huge processes but can be used for little ones or to compare before and after. This is the reason why the plugin should be connected with code injection detection plugins, like hashtest, in order to strip harmless data and improve their results.

Paging structures are relied upon to identify executable pages, the method fails if the page tables are paged out and no pagefile is specified. In these situations, a fallback mechanism that probes all VADs, similar to the present malfind plugin, should be implemented. However, this fallback will again be vulnerable to the concealment tactics disclosed in this paper. While it is feasible to enumerate the PFN DB in order to collect page protections, this will only work for pages in the hardware and transition states, as all other states lack a corresponding PFN DB entry.

5.7.10. *Verifying trusted executable files*

During the identification and investigation phase of a security incident, computer and network forensics play a key role. Memory forensics is conducted by capturing the present state of the system's memory and writing it to a snapshot file on disc. A memory dump can then be taken off-site for analysis using specialised tools like Volatility. Several operating systems rely on code signing to alert users to potentially dangerous software activity. Malware makers sign their software with certificates that were either compromised or issued directly to them [81].

In this study, the authors discuss the restrictions memory forensics imposes on the digital signature verification procedure of Windows PE-signed files. Microsoft Authenticode is the code-signing standard that Windows employs to digitally sign files that use the Windows portable executable (PE) format. Multiple signatures can be used to dual-sign a PE file, which is strongly advised when using obsolete hashing methods such as MD5. Using X.509 chain-building rules, the certificate chain is constructed to a trusted root certificate and is required as long as the root certificate is not available in users' root stores. Signatures generated by Authenticode adhere to the DER-encoded ASN.1 format.

The signature's offset and size are stored in the data directories array of the PE optional header's security directory entry. A catalogue file (extension.cat) stores the digital signatures of any number of files. Microsoft created the subject interface package (SIP) to facilitate catalogue file generation, retrieval, hash computation, and validation. The Windows API trace of the execution of the sigcheck tool by Sysinternals is extracted and examined during the verification of an embedded-signed file. To verify the digital signature of a file, a sequence of Windows APIs from various system's dynamic link libraries (DLLs) are called.

The WINTRUST and CRYPT32 DLLs are responsible for the essential steps of the verification process. Programmatically, the verification of a catalog-signed file is performed. Obtaining a handle to a catalogue administrator context and then calling the method CryptCATAdminCalcHashFromFileHandle to calculate the Authenticode hash of the file is the proper approach to achieve this. After retrieving the required catalogue, the WinVerifyTrust function can be called to validate the file signature. A file object has a pointer to a SECTION OBJECT POINTERS structure, which is used by the memory manager and cache manager to store file-mapping and cache-related information for a file stream.

The DataSectionObject, SharedCacheMap, and ImageSectionObject opaque pointers adhere to this structure. Generally speaking, it points to memory-mapped executable files (images).

5.7.10.1. *The plugin sigcheck.*

The researchers created a Volatility plugin to validate digital signatures of executable files in memory dumps. Volatility is an open source tool that facilitates memory dump analysis on mainstream operating systems. The plugin is named sigcheck, after the Microsoft application that validates digital signatures on binary files. Algorithm 1 depicts a pseudo-algorithm of the process followed by sigcheck in order to validate the digital signature of an executable module e contained in a memory dump M. In the experiments, every file object discovered contained a legitimate DataSectionObject or ImageSectionObject pointer. The integrity of these memory zones is then evaluated.

The Authenticode signature needs the full PE file, excluding only certain parts. If only one memory page of an image file is missed, the signature of that file cannot be computed correctly. One possible solution is to guarantee that the Windows PE loader locks memory pages that contain file objects. Other solution might be a combined analysis of a memory dump and their corresponding swap files. Sigcheck is capable of reconstructing the most common image base addresses of every version of Windows OS, empirically obtained.

In 64-bit files, there are 252 possibilities for an image address value (considering an offset of 0 × 1000 between memory addresses). It is computationally infeasible to brute-force the image address. To verify a successful reconstruction, the option for using the value of the CheckSum attribute, located at the PE optional header, was selected. Many system files in Windows are catalog-signed PE files. To verify every signature, the catalog database that contains that hash signature is required.

This implies that every possible catalog file for every Windows OS flavor is needed. At the moment, there is not a centralized database of catalog data. State-sponsored CERTs could lead this initiative and maintain this database. The plugin does not detect this kind of evasion techniques. For instance, malware can inject malicious code in a legitimate process.

To be sure that the binary code of an image file was unmodified, unmapping of its corresponding process is required. The virtual address descriptor (VAD) tree of a process, looking for strange changes in the permissions of every VAD node could also be checked.

5.7.11. *BMCLeech*

Under Linux, there are numerous options for memory acquisition, such as kernel support or modules such as Lame and Pmem. Memory acquisition is most effective when it is subtle, i.e. undetectable. There are five stages that permit increasingly profound and potent memory access. The Baseboard Management Controller (BMC) is a co-processor with firmware that enables remote server monitoring and administration. BMCLeech is software that operates on BMCs and takes advantage of the fact that BMCs are typically connected to the PCIe bus, which enables direct memory access (DMA) to host memory [82].

BMCLeech is an innovative solution that combines the benefits of asynchronous device level with the advantages of open source software. It can also push and pull files, inject code into the kernel, and mount RAM as a file, in addition to reading and writing memory. This demonstrates that dependable forensic memory access may be simply implemented on server systems as part of standard system administration. BMCLeech is the first software to offer forensic readiness to the

BMC without the target host system being able to detect memory capture. Even if the host system can detect that a BMC is attached to the system, this is not suspicious because a BMC is often included with a server.

There is no additional work required to evaluate the memory of a system. Even the analyst's acquisition software does not need to be upgraded. Intel's Virtualization Technology for Directed I/O (VT-d) includes an Input-Output Memory Management Unit (IOMMU) that functions similarly to the MMU often employed to implement virtual memory. When an analyst wishes to acquire memory from the target machine, PCILeech enables retrieval of the matching memory snapshot. On the OpenBMC BMC, BMCLeech implements a PCILeech rawtcp device. It employs the libaspeedxdma library to encapsulate access to the kernel driver (aspeed-xdma). As a result, other applications on the BMC can more readily access the host memory.

Using standard memory forensic analysis tools such as Rekall or Volatility, the memory can be studied. BMCLeech does not modify memory at all during the acquisition; it fully retains integrity according to the Vo€mel and Freiling definition of integrity. Since the aim is a Linux-based system, it is believed that LiME is a suitable tool that acts as a form of baseline. The evaluation illustrates how memory changes without load over time.

Using BMCLeech, the Internet-based collection procedure takes approximately 6 min. Using OpenBMC, this amounts to around 5 MiB/s. Local tests on the BMC found that it can read memory at approximately 50 MB/s. Since a new acquisition tool is being introduced, it is necessary to demonstrate its functionality. Pagewise differences in BMCLeech are generally larger than byte-wise differences. A difference of a single byte alters the entire page relating to it.

The investigation indicated that, on average, each page differs by approximately 1200 bytes. There are numerous pages that differ by a modest number of bytes, which is a key realisation. The disparities between pictures taken concurrently (second row) and those taken simultaneously (third row) are greater at higher addresses. The differences between BMCLeech and LiME snapshots revealed that they are pretty similar. There is no evidence in the diffs that contradicts PCILeech's accuracy.

It appears that some memory locations are more volatile than others, as indicated by the red bar in the lower portion of each difference. This can be thought of as the system's memory's characteristic instability inside Dt. Its interoperability with the PCILeech framework makes it a powerful investigative tool. Memory can be acquired, code can be injected into the kernel, and files can be extracted from the host's file system.

The evaluation demonstrated that this method is beneficial and applicable. BMCLeech showcases the advanced capabilities of connecting internal and external devices to a computer system. Frequently, these devices are connected via PCIe and, as a result, have DMA access. The BMC is designed to be used in a benign manner by incident response teams in the use case. Nonetheless, one should be mindful that such components might also be used for nefarious reasons.

5.7.12. Malware

Existing malware include viruses, worms, trojans, spyware, sniffers, ransomware, and botnets, among others. Malware is analysed in order to determine its origins, characteristics, types, and damages/impacts. Malware developers have devised numerous methods to circumvent static analysis and signature detection. Packing malware is software that encapsulates one or more files into malware in order to modify its code structure. Additionally, packer virus deletes import address tables to complicate research [83].

In 2006, it was found that 92% of malware employed comparable strategies to avoid detection. A metamorphic malware possesses a mutation engine that modifies itself during each operation through the use of packaging and obfuscation techniques. Malware classification is a heavily researched topic in the literature on malware analysis. First, data mining techniques were used to detect rogue executables. Memory analysis techniques such as taint analysis and memory image differentiation are used in dynamic analysis.

Some research focuses on the issue of detection, while others investigate obfuscation, polymorphism, and self-mutation. Dynamic analysis has led to the inclusion of various features, including API call sequences and graphs, hooking behaviours, kernel-level executions, memory use, and power consumption. In dynamic taint analysis, contaminated data refers to information coming from or mathematically derived from untrusted sources, such as the network. Another study that combines memory differences has detected the alterations (changes to the file system, newly loaded drivers, or newly created images) that a rootkit makes in kernel space.

In the current research, the memory access (stack operations and instructions that interact with the memory) data is binned into distinct files based on the images in the memory. This data is mapped onto three-dimensional space in order to investigate trends of typical malware dataset behaviours. A Windows 7 virtual machine is developed and hardened for anti-analysis and evasion measures against malware. There are a total of 121 malware samples from 24 families of various sorts of malware, including trojans, ransomware, viruses, and worms.

Stack, heap, and memory image accesses are logged independently for each image in the process memory layout. Unpacking the binaries of ransomware samples produces similar patterns on 3dmemory diagrams. It has been observed that ransomware has a memory footprint that is immediately distinguishable from the memory artifacts found in this study. The files infecting other files' memory regions and their fingerprints have also been extracted from the samples.

Comparing all of the pairs within a family yields the average similarity ratio. Nine of the malware could not be mapped into 3D space on this experimental machine because the number of points was insufficient. The SSIM measure is a tool for comparing photographs, and the resulting patterns in each image sit on the same axis structure. Rex Virus and Matsnu Trojan generated identical memory pictures and patterns, although employing distinct strategies to evade signature-based detection.

The heatmap illustrating the pairwise commonalities of all malware in this dataset displays strong similarities between worms and viruses. This heatmap and its underlying data can be found on the GitHub website (https://github.com/cgyphd/Imaging-and-Evaluating-Memory-Access-for-Malware). With the development of deep learning approaches, the authors anticipate that cyber intelligence analysts would be able to identify malware in less time than is currently required.

5.7.13. Malware detection

Eliminating a significant number of improbable malware samples is one of the most crucial and initial steps in building any malware analysis. Either dynamic or static malware analysis can be used to do this part of the study. This work offers a fuzzy-import hashing technique, which is the combination of fuzzy hashing with import hashing to increase detection rate and overall performance. Malware analysis is the process of determining the origin, behavior, and potential repercussions of infection by a malware sample under investigation. Malware can be categorised into many groups based on a variety of variables, including creator, variant, code, activity, and severity [84].

For complicated malware reverse engineering, it is advantageous to undertake both static and dynamic analysis rather than choosing between the two. As they return a Boolean value indicating whether or not two files are similar, cryptographic hash algorithms are not applicable in every cybersecurity scenario. A fuzzy hashing approach divides the target file into many blocks, with each block's hash calculated independently. To assess the danger potential of files, forensic analysis of malware requires a comprehensive understanding of the degree of resemblance between known malware and harmless files.

5.7.13.1. Fuzzy hashing. SSDEEP fuzzy hashing was designed to detect spam. It breaks files into blocks based on their data. Adler32 functions in rolling hash methods create these blocks and endpoints. Each block is hashed, and then all the hashes are concatenated to get the fuzzy hash of that file. The Damerau-Levenshtein distance measure calculates file similarity.

SDHASH fuzzy hashing finds common and uncommon attributes in a file and matches them with those in another file to find the degree of similarity of interest. Entropy calculations identify attributes, which are 64-byte strings. SHA-1 and Bloom filters calculate a file's SDHASH fuzzy hash. Bloom filters are probabilistic and space-efficient data structures that determine whether an element is a set member. The Hamming distance measure calculates file similarity.

When files change slightly, the mvHASH-B fuzzy hashing approach maintains the same hash value and data integrity. However, mvHASH-B transforms input data using majority voting, encodes the majority vote bit sequence with Run-Length Encoding (RLE), and generates the fuzzy hash using Bloom filters. It also uses a hash function similar to SHA-1 but faster.

The Locality Sensitive Hashing (LSH) approach TLSH fuzzy hashing hashes identical input items into the same buckets, reducing the dimensionality of high-dimensional data. It populates an array of bucket counts with a TLSH hash value from a byte string using a 5-sliding window. The bucket array is processed to calculate the quartile points, q1, q2, and q3, and the digest/hash header values (first 3 bytes of the hash) and content. The header and body form the TLSH digest/hash. Unlike other hash techniques, the TLSH methodology gives a similarity score between 0 and 100, where 0 is a mismatch and 100 is a perfect match. The TLSH technique compares two digests/hashes of files using a distance score, where 0 means the files are identical and higher scores mean more differences.

5.7.13.2. Portable executable (PE) file based hashing. Microsoft Windows uses the Portable Executable (PE) file format for executable/DLL files. There are numerous smaller components that can be separated into the PE file format's Header and Sections. All legitimate PE files begin at memory location 0 × 54AD, which corresponds to the ASCII characters MZ (named after a former Microsoft architect Mark Zbikowski).

IMPHASH – PE file-based hashing is one of the fastest methods for comparing harmful program. This import hashing technique only generates a hash of a PE file's imports or import libraries, unlike other hashing methods. Imports/Import Libraries are routines called by a program (malware) from other programs and bound and linked to form the executable program. The Import Address Table (IAT) stores the details of Imports/Import Libraries (DLLs), which is used to build a program's IMPort HASH (IMPHASH), which depends on the order in which the Import Libraries are called. Thus, two programs with the identical code but different function/Import Library orders will produce different IMPHASH results. Import hashing, like fuzzy hashing, matches samples or doesn't.

peHash – is another PE file-based hashing approach that calculates hash values of various portions of the PE format. Image attributes, subsystem, stack commit size, heap commit size, virtual address, raw size, and section characteristics are taken into account while generating hash values. Hash values are computed for binaries in the PE format that turn structural information about a sample into a hash value. Grouping binaries by hash values generated with the new method detects multiple polymorphic samples and broken samples. The peHash technique can accomplish correct clustering for huge groups based on very basic information from the PE files without any assumptions about the contents of the individual sections, but only depending on their wealth of information. PeHash cannot cluster malware family variants because packers make the code structure transparent to it.

Malware analysis using YARA rules is the standard. YARA rules match prepared strings against the targeted samples or processes to find malware. YARA strings are reverse-engineered from malware. YARA rules have text, hexadecimal, and regular expression strings. Text strings are readable text with modifiers like nocase, ASCII, wide, and fullword to improve process management. Hexadecimal strings are raw bytes with wild-cards, jumps, and alternatives. Since version 2.0, regular expression strings are readable text with modifiers that enhance YARA rules. Escape sequences can express raw bytes in text and regular expression strings. A YARA rule's rule condition specifies which strings must match the target sample to alert it as malware. YARA rule conditions are Boolean expressions like those in other programming languages that decide whether the rule is triggered.

Ransomware is a big concern for everyday consumers and business companies. Ransomware exploits victims for financial gain, interrupts corporate activities and encrypts important data. Four types of ransomware were chosen for this study: WannaCry, Locky, Cerber, and CryptoWall. Each sample must be recognized as malicious by at least 40 detection engines on VirusTotal. Fuzzy hashing and import hashing are compact, quick and resource-optimized malware analysis approaches.

1000 goodware examples were the files obtained from ten regularly used software: JAVA, MS OFFICE, Google Chrome, MySQL, R, NMAP, McAFee, MATLAB, Python and Snort. The purpose of this experiment is to determine the similarity detection rate of each analytic technique for each malware category individually and collectively. The fuzzy similarity or degree of resemblance ranges from 1% (least matched) to 100% (most matched) (exactly matched). Typically, malware analysts select a threshold number to accept or disregard the fuzzy similarity score. This method can be applied as a preliminary way in malware analysis that may help in any advanced investigation.

The import hashing approach was used to detect similarities for each ransomware category independently. In some ransomware categories, the detection performance of import hashing was superior to fuzzy hashing, while in others it was not. The proposed fuzzy-import hashing combines fuzzy hashing and import hashing to determine the similarity of two files. Import hashing and fuzzy hashing produce slightly different results. The result of fuzzy hashing is the degree of similarity between each matched sample.

While import hashing simply indicates whether or not the sample is a match, import hashing reveals whether or not the sample is a match. Important to their integration is aligning both outputs so that they can be represented as a single integrated output. The proposed fuzzy-import hashing approach was used to independently detect similarity for each malware category. Its detection results were compared to those of the fuzzy hashing techniques SSDEEP, SDHASH, and mvHASH-B, as well as the import hashing technique. The actual operation is predicated on the fact that import hashing is relatively faster, thus it will be applied to samples first; if no match is found, fuzzy hashing will be used. This set of actions avoids applying somewhat slower fuzzy hashing on all samples and saves computing overheads.

5.7.13.2.1. Comparative evaluation. Hashing is distinct from YARA rules since rule development needs reverse engineering. Strings are taken from malware to build YARA rules after analysing the family of a particular threat. Utilizing sophisticated approaches such as Fuzzy Regular Expressions, Naive Bayes Classifier, and Gibberish Detector, this program develops two sorts of rules, ordinary rules and super rules, based on the type of malware. Fuzzy-import hashing (SSDEEP) and YARA rules are extremely similar. In malware analysis, the performance of a method is vital because it is always applied to a high sample size.

When choosing a malware analysis method, it is crucial to strike a balance between detection precision and performance. F1-Score may be more useful in identifying an appropriate method of analysis. The proposed fuzzy-import hashing technique provides valuable input for advanced analytical techniques such as clustering. Due to its fuzzy similarity scores, its results can be used in clustering, particularly in fuzzy c-means clustering. Higher values for the first three evaluation indicators indicate superior clustering outcomes.

It is crucial to compare the similarity detection results and performance of the proposed fuzzy-import hashing with currently established and successful malware analysis technique. YARA rules technique is one of the most popular and successful techniques used in malware analysis, therefore, the fuzzy-hashing result and performance is compared with YARA rules.

5.7.13.2.2. Advantages and limitations

- Fuzzy-import hashing benefits
  - Performance sustainability: Import hashing, which merely generates the IAT hash of a file, is one of the fastest analysis methods.
  - Detection Rate Improvement: When one hashing method fails to identify similarity due to its limitations, the other can help. Fuzzy-import hashing can detect more viruses than any other method.
  - Overheads Minimization: Import hashing is faster than fuzzy hashing, therefore if it is applied to samples before fuzzy hashing, only mismatched samples need to be reprocessed. Avoiding fuzzy hashing on all samples reduces overhead.
  - Result Alignment: Import hashing results (binary outcomes) can be aligned with fuzzy hashing results by treating the matching result as 1 or 100% (exact match) and the mismatched result as 0. (no match of fuzzy hashing). Fuzzy similarity scores can align the two findings.
  - Accuracy Improvement: If import hashing finds matching sample (s), the strong similarity score 1 or 100% is added to the fuzzy-import hashing similarity result, which improves the overall result and the clustering or classification results.

- Fuzzy-import hashing benefits
  - Performance sustainability: Import hashing, which merely generates the IAT hash of a file, is one of the fastest analysis methods.
  - Detection Rate Improvement: When one hashing method fails to identify similarity due to its limitations, the other can help. Fuzzy-import hashing can detect more viruses than any other method.
  - Overheads Minimization: Import hashing is faster than fuzzy hashing, therefore if it is applied to samples before fuzzy hashing, only mismatched samples need to be reprocessed. Avoiding fuzzy hashing on all samples reduces overhead.
  - Result Alignment: Import hashing results (binary outcomes) can be aligned with fuzzy hashing results by treating the matching result as 1 or 100% (exact match) and the mismatched result as 0. (no match of fuzzy hashing). Fuzzy similarity scores can align the two findings.
  - Accuracy Improvement: If import hashing finds matching sample (s), the strong similarity score 1 or 100% is added to the fuzzy-import hashing similarity result, which improves the overall result and the clustering or classification results.

- Fuzzy-import hashing has some drawbacks, including:
  - Similarity Scores: Security analysts may get diverse inferences from fuzzy-import hashing similarity scores.
  - Structural Similarity: Due to the limits of both methodologies, fuzzy-import hashing could only find structural or syntactic similarity, not behavioural or semantic similarity.
  - File/Function Size and Order: Fuzzy-import hashing similarity scores depend on file size, block size, and function order, therefore changing any of these parameters can alter the score.
  - Packed Samples: Fuzzy-import hashing may not work on packed samples due to the limits of the underlying approaches.

5.7.14. Android master key

In 2008, a method was presented to break full disk encryption, including BitLocker, TrueCrypt, and FileVault. DRAM's remanence effect allows cold boot attacks. Cooling RAM modules with sprays or freezing them might lengthen this period from a second to many minutes. The security hole opened by cold boot attacks had yet to be closed. Exploiting the remanence effect on ARM-based Android devices with hardware-backed key storages and protected boot is tough today. Memory encryption delays the system by an order of magnitude. Authorities increasingly want digital evidence to establish or deny a crime. The authors demonstrate Android key recovery and forensic toolchains in this article [85].

Unencrypted metadata can extract a list of installed programs and retrieve usage behavior, such as WhatsApp message send and receive times. Thus, smartphone basics can be used without unlocking. full disk encryption encrypts the partition over file-based encryption with metadata encryption. First decode the full disk encryption partition, then the file-based encryption-encrypted file data. Thus, full disk encryption and file-based encryption make the attack useful in contemporary devices' decrypting chains.

The open-source Sleuth Kit (TSK) analyzes file systems and partitions. Modules focus on storage layers (e.g., image, partition, file system). TSK analyzes a smartphone's storage bit-by-bit during a physical acquisition. Plaso replaces the log2timeline tool. This project enabled the generation of a super timeline with all system timestamped data. To successfully analyze and extract data from EXT4 file-based encryption, TSK must be extended with decryption functionality.

This article exploits file-based encryption's key derivation function flaw to obtain the master key needed to decrypt stored data. A memory image and user data partition copy from the attacking device are needed. Android Debug Bridge or other pre-installed developer access is usually not needed. Boot mode controls RAM access and device privileges. After a warm reboot, an early bootloader hack could allow access to this location.

The master key decrypts EXT4 file names and content and derives all data DEKf (data encryption key file or folder). The Sleuth Kit (TSK) is an EXT4 command line tool that outputs all metadata and details of a metadata address (also known as inode). The addon outputs encryption metadata.

This is useful when cold boot attacks delete memory. The descriptor master key is the two most hit 256-bit keys per nonce bin. Path specs needed serialization in Plaso. Linking path specs creates references to individual files or file content. Code was added to add path-specified master keys to the FS info object from pytsk. This ensures master key serialization and deserialization.

The experiment involved dumping the RAM of the Nexus 5× and Pixel XL using the LiME kernel module. Since one master key is 512 bits long (two keys are 256 bits long), the approach is effective. For a large number of other Android devices, the researchers ascertained the encryption strategy by, for example, extracting the encryption metadata. The master keys could be recovered from an Android Virtual Device as Android 10, the AVD also uses file-based encryption instead of full disk encryption.

The Pixel 2 was the sole smartphone that used the HEH name encryption mode, indicating that it used a new key derivation function. In this paper, the authors demonstrate how to extract encryption keys for file-based encryption, the encryption solution of choice for new smartphones and required for Android 10 and later devices. The extraction strategy, implemented in the tool fbekeyrecover, differs significantly from the full disk encryption key extraction demonstrated in prior research. This technique is resilient to a partial RAM wipe or loss of data due to the redundancy of its critical components.

5.7.15. MacOS memory analysis

Memory forensics frameworks convert a memory sample's unordered physical pages into the structured and ordered virtual address spaces used by the operating system and all running apps. Address translation matches virtual address spaces to physical pages. Each hardware architecture defines how the hardware state indicates whether a virtual memory page is in physical memory. The hardware state encodes the offset in the memory sample, making physical memory page recovery easy. The operating system defines the hardware state to encode the location of "invalid" pages, such as in a paging file, disk file, compressed data store, or elsewhere. Memory forensics requires deciphering these incorrect states and recovering the corresponding pages.

The authors demonstrate how depending simply on pages tagged as existing in physical memory leaves many pages behind and badly influences analysis results [86].

This paper describes research on macOS page queues to combine queue status analysis into memory forensics. The authors show how common incorrect page states are and how analyzing the queues makes a lot of previously unavailable data available. The Volatility framework supports analyzing these queues across operating system versions and memory samples. The presented code analyzes queues statistically and integrates data into Volatility. All Volatility plugins use the queue analysis code. The code will be published in the Volatility repository for the memory forensics community.

The RAM-tracked page relationship was found using the mac walkqs plugin. The file cache queue always contains disk-cached file sections, regardless of whether any processes are mapping the file. Invalid column count pages were stored in a tiny number of free page queues. Memory forensics has historically used stack data to find call stacks, sensitive API parameters, and more.

Applications and libraries process dynamically created data in process heaps. Metadata is needed to recover executables which the memory forensics framework uses to reassemble the program. The mac procdump Volatility plugin scans Mach-O files in memory and uses metadata to reassemble each segment to retrieve process executables.

The queue-aware address space may aid investigators and unlocks several executable headers. Memory forensics fills missing pages with zeroes (NULL bytes) to maintain alignment, which can severely impact reverse engineering and other forensics analysis. The address space facilitates mac procdump-based forensic examination.

5.7.16. Virtual reality

Virtual Environments (VEs), hosting new types of social interaction, may also be the locale for misconduct. Users may injure themselves using the systems, or defraud each other in the VEs. Ethical and legal controversy have kept a legal precedence at bay, however, these concerns should not preclude a thorough forensic evaluation. Large amounts of information, that may not be available in traditional storage can be recovered from volatile memory. With MR systems blending together virtual and physical experiences, malware targeting these devices may have a slew of additional capabilities. An immersed user is a perfect target for an attack that could even bring about physical harm. Should the VE be maliciously modified to disrupt or deceive an immersed user, the calibration between the physical and virtual space will inevitably be compromised [87].

State-of-the art work has only scratched the surface on the forensics and security of Virtual reality (VR). Currently there are three types of consumer VR systems available. The HTC Vive base configuration consists of a headset or Head Mounted Display (HMD) which is tethered to a computer. OpenVR is an API designed to free developers from relying on hardware specific Software Development Kits (SDKs). The OpenVR's developer Valve partnered with the development of the HTC Vive. In this work, the authors examine potential sources of digital evidence unique to VR systems and extract them from memory dumps [88].

The authors use memory analysis to locate potential data containing memory regions. Pointer scans are conducted to identify routes to the data and machine instructions are inspected to ensure static references. Using the machine instructions as a YARA signature, a Volatility plugin in constructed to automatically extract the data from a memory dump.

The study began with an analysis of the OpenVR API. The API documentation was surveyed to identify data structures found to contain information that may be of interest to a forensic investigator or hold Sensitive Personal Information (SPI). Some of the data structures of interest include those relevant to the tracked device.

The state of the VR system con be controlled and recorded as it is in physical space, yet much of the underlying tracking and hardware information is transparent to the user. Leveraging OpenVR, a minimal helper program was developed to output each of the components of TrackedDevicePose_t to the console.

Once the pose coordinate information is readily available via the helper program, memory search to locate the data can be conducted. Targeting the VR runtime, the search is limited to memory allocated to processes child to SteamVR. Cheat Engine allows for rounded float searching, providing the necessary tolerances for the data to be found.

Over multiple collections, data was found to be dynamically stored. To reliably locate this data in the absence of scenario information, the address must be tied to a static location. This is achieved by attaching a debugger to the process vrmonitor.exe, and observing accesses and writes to the base address.

Known virtual locations and their coordinates have been established. Memory was then collected using the tool Dumpit. This provided the physical address of the signature in the memory dump. Volatility's interactive memory image explorer, volshell, allowed for the tracing of the path to the data block.

The Volatility plugin Vivedump automates the process of locating the base address and dereferencing the chain of pointers. This is particularly favorable as VR capable machines typically have a large amount of Random-access Memory (RAM). Still the plugin's output can be improved by handling data interpretation as well.

Using the OpenVR plugin, evidentiary data such as tracked device state, activity and class from could be extracted from memory. By default the HMD occupies the first position of the TrackedDevicePose array, however a trend in array position for other devices, namely the controllers and base stations, was not observed. There is likely a race condition at startup during the initialization of these Bluetooth devices. For this reason, the type of device in the latter pose array positions must be detectable.

This information is stored to the disk in json format (chaperone_info.vrchap) and often remains in memory. Because this information is available both on disk and regularly in memory, it was not necessary to further pursue extraction. The plugin will conduct a file scan for the data in memory and if not found the file can be manually provided to the visualizer.

The plugin, utilizing the Volatility Framework, requires the memory dump, operating system profile, and the plugin directory as input. The plugin will output a textual representation of all evidentiary data, a wavefront obj formatted mesh of the VE, and pass the 3-dimensional coordinates to a Python OpenGL instance.

The pose matrix represents the devices rotation and translation with respect to the centre of the tracked area. The matrix can be transposed from its 3 × 4 arrangement to the standard 4 × 4 transformation matrix and present the user with a 3-dimensional representation of the room. The tracked device class can then be used to apply an appropriate mesh to the device for visualization. This provides context to the tracked device locations in the physical room, as the Chaperone boundaries typically outline physical walls.

The data structures that were acquired in this study were all similar in that the underlying information could be easily manipulated. Because many enumerators were used to describe device states and events and several processes are storing identical information, determining the nature of the data is impossible without some feedback. Information that is not persistent is equally difficult to locate. The memory scanning tool can easily identify pointers, but to reliably extract the data from memory the base address of the route must also be tied to a static location. Data structures that are not frequently accessed or updated pose another challenge when searching for a route to the memory region. A feature of Cheat Engine, breaking the program when the target memory region is access, allowed us to quickly identify the necessary op code signatures.

All data structures of which identified routes from a static location except for TrackedDevice Class were consistently obtainable. This was tested over multiple memory captures, with varying degrees of VR usage, connected devices, and applications. The preferred route to ascertain whether a device is connected is via the above data structures. A small program was implemented to frequently request tracked device classes which improved the likelihood of the pointer route remaining intact.

With each update to the VR runtime, a new set of signatures were required to access the data. Throughout this study, three significant updates caused changes in the opcodes that were used for the YARA scans. No false positive YARA matches were produced, simply reducing in lost computation time. Allowing searching for all signatures may be practical as the catalog of SteamVR versions remains small, yet with continued updates, conflicts and decreased efficiency may accrue.

5.7.17. SGX environments

Intel's Software Guard eXtensions (SGX) lets developers create secure memory zones, called enclaves, to protect sensitive code and data. In SGX, the entire system can be compromised, yet only the CPU is trusted. This paper identifies SGX-machine data artifacts where they investigate 45 SGX applications from popular open-source programs, research efforts, and two cutting-edge harmful enclaves. The authors propose SGX enclave finding and analysis methods [89].

The PRM contains an Enclave Page Cache Map (EPCM) to track enclave page status since SGX considers the OS is untrusted. EPCM helps the microcode block cross-enclave memory access and page allocations. Two CPU instructions trigger kernel mode code and SGX-specific functionalities to bootstrap an enclave. A third party can validate an enclave and the SGX platform using the SGX operating system. Host processes interact with enclaves using the ENCLU instruction.

An enclave trusts all code inside its ELRANGE but not outside, which may be controlled by an attacker. The development framework generates and links edge code, which contains secure and outside functions. Microsoft's Open Enclave and Google's Asylo frameworks make enclave code transferable to secure computing technologies like Trust Zone. These frameworks host a whole application in the enclave like a Virtual Machine or Docker Container.

Ordinary dump tools, which use operating system data-structures to detect data-containing memory zones, cannot dump EPC zones. CPUID queries allow an SGX dump tool to circumvent this limitation. CPU speculative attacks can dump non-debug enclaves and reveal system status. These sorts of attacks allow an attacker to leak the content of an enclave even if it is not in debug mode. The dump tool localizes EPC zones independently of OS data structures, marks them in the dump, and saves debug-mode enclave pages using EDBGRD opcode.

Analyzing kernel module data-structures can reveal SGX enclaves in a memory dump. This lets the kernel handle memory operations differently. Analysts can learn from userspace processes' untrusted memory structures. All API-like frameworks examined follow Intel's well-defined internal structure for multi-thread enclaves. The Container-like framework has a customizable enclave memory layout. The development framework determines the enclave interface (x2.2), which shows OS interaction.

An analyst can find and quantify executable pages to determine enclave code load. Writable pages (rw*) may indicate data location. Memory forensics and reverse engineering enable automatic interface extraction, then lightweight static analysis phase is used to find structures that are used (e.g., sgx ecall takes an array of function pointers as a third parameter). The framework generates predictable code, making this approach sound.

The tools obtained 45 enclaves, including 40 from development framework repositories. These demos include modest feature demonstrations to complex databases and Web servers. The enclaves were simulated in release mode and experimented in debug mode.

The study took 246.32s (4 min) every memory dump, with the commercial Conclave enclaves taking 8.59s (30 min). For API-like categories (TCS, SSA) or Container-like categories, the technique extracted valid structure addresses. Except for R-I-7, the tool successfully detected all frameworks noting that the two frameworks have numerous similarities. The acquisition tool dumped system memory from a Conclave-delivered process in an Azure VM.

The user-space analysis plugin automatically categorised the application as based on the Intel SGX SDK, however the system failed to recover the enclave interfaces out of the box. Imported symbols revealed the main application's shared library. The plugin found and reported all interfaces. SGEX-ROP uses TSX to break host application ASRL and generate ROP chains to attack the system. The standard Intel SGX SDK successfully deduced the development framework, memory structure, and interfaces for the PoC.

Enclaves can control host processes by transferring data into their memory space. SnakeGX's payload exploits outside-chains, ROP chains in untrusted memory, to interface with the OS and exfiltrate cryptographic keys on demand. Since SnakeGX infects StealthDB, the system only reports this enclave. The development framework, memory structure, and interfaces were accurately identified. Code-reuse attack could have manipulated external process execution.

The development frameworks' memory layout does not change, but interface identification would need small changes to adapt to the Windows OS. This would mostly affect static analysis, which would need to consider a different calling convention when matching specific structures and target functions.

5.7.17.1. Case studies. R3 distributes Conclave, a commercial SGX developer framework. Conclave abstracts the SGX programming paradigm for Java-based applications. It also incorporates the native libraries required for communication between the application and enclave. At the time of writing, only the new DCAP driver is compatible with Conclave. The examination of the Conclave enclave took about 30 min longer. Examining the imported symbols allowed the determination of which shared library contained the main application. The user-space plugin enabled the evaluation of this library rather than the JVM executable. This enabled the plugin to correctly identify and report all interfaces, as well as validate their validity.

The first instance of malware-enclave proposed by researchers (SGX-ROP) is studied, which uses TSX to break the ASRL of the host application and construct ROP chains to attack the system. In the Proof of Concept, the malicious payload simulates ransomware by creating a new file on the host system. This example demonstrates how the SGX analysis plugins can be used with other memory forensics techniques to acquire a more comprehensive understanding of this advanced threat.

SnakeGX infects a particular enclave, StealthDB, which is a Postgres SGX plugin. Internally, SnakeGX's payload leverages outside-chains, a series of ROP chains in untrusted memory, to interface with the operating system and exfiltrate cryptographic keys on demand. Thus, the possibility of unanticipated enclaves in the host process is eliminated which did not identify any new enclaves (active or zombie).

5.8. Network forensics

5.8.1. Packet analysis

Network packets are groupings of bits containing data as well as control information, typically referring to an OSI Layer 3 protocol data unit. They are the smallest unit of data captured and logged regarding network traffic flow transiting packet-switched networks at a certain point in time. Packets can be studied by decoding the packets' raw data and displaying the content through multiple fields. The Berkeley Packet Filter provides packet filtering, such as only receiving packets that begin a TCP connection. Port mirroring, hubbing out, using a tap, and ARP cache poisoning are the four primary approaches to capture traffic from a target device [90].

The network environment in which the device is placed determines which protocol should be used. Network packet capture files contain a wealth of information regarding online user activities that can be used for network forensics. libpcap (pcap) is the de facto standard capture format; it is a binary format that supports nanosecond-precision timestamps. In addition to dumping network packets, pcapng permits the storage of many data kinds in a generic block format. Packets on a network carry more than just transmission data and metadata.

Reconstructing files that crossed a network from network packet streams (referred to as network carving) This makes packet analysis the essential tool for network forensics traceback. It can aid in the discovery of traces of harmful online conduct and breaches affecting an organization, as well as the acquisition of host-based proof of malicious actions. Deep packet inspection (DPI) can uncover and record internet activity to the level that it raises privacy issues regarding mass government surveillance. DPI can be used to discover excessive amounts of non-business traffic, such as social media use, that must be filtered or banned in a company. It can also assist in shaping and controlling many sorts of traffic, including email, VoIP, and P2P.

Deep Packet is an approach to network packet processing based on deep learning that can recognize end-user applications such as Skype and BitTorrent. Specialised hardware, often programmed in Assembly or C, is required to do network packet analysis at speeds above 1 Gbps. Using the purpose-built packetC programming language with a parallel packet processing methodology is an alternate method.

5.8.1.1. Packet data as digital evidence. Together with data from remote network services, network packets serve as active sources of network evidence. Some believe that the use of packets as evidence is problematic if they can be spoofed. Network packets, on the other hand, can complement firewall logs and network monitoring software exceptionally well and can be regarded as the ultimate forensic evidence. When studying what occurred in a network at a specific moment in time, a comprehensive packet capture is required. There are methods and solutions available for automatically scrambling network packet capture data while maintaining binary integrity.

Based on the Organizational Unique Identifier (OUI) portion of a device's MAC address, the suspect's computer manufacturer can be determined with high confidence. Packet analyzers are created for a variety of applications and vary in their capabilities and features. Data carving, capture file quality evaluation, anomaly detection, protocol encapsulation, and customizable packet aggregation are all supported by the tools. Numerous packet analyzers enable both live packet capture and offline packet analysis. Deep packet inspection and analysis of numerous types of network traffic are only possible with analyzers that handle a large number of protocols.

Packet analysis has both hardware and software implementations. Analyzers of packets might be physical, virtual, or hybrid. Wireshark is one of the most popular graphical programs for packet capture and protocol analysis. The GNU General Public License and private licences are common licence types linked with packet analyzers. Snort is a free and open source intrusion detection and prevention system (IDS/IPS) for networks.

Dsniff is part of a series of tools developed by Song for Unix-like operating systems for network auditing and penetration testing. EtherApe is a tool for monitoring network traffic and sniffing packets on Unix. Tcpdump is a typical utility for capturing and dumping network packets for further study. The Charles Web Debugging Proxy in 2002 is an HTTP proxy; and netsniffing is a free Linux network analyzer.

Tranalyzer is a free tool for packet- and flow-based network traffic analysis and troubleshooting. WebScarab is an easy-to-use, integrated tool for penetration testing web applications. In addition to a packet analyzer, SolarWinds Network Performance Monitor offers deep packet inspection. The PRTG Network Monitor from Paessler contains a wide variety of network monitoring tools; while another packet processing tool is based on Apache Hadoop.

The CoralReef software suite from CAIDA can collect and analyze data from passive Internet traffic monitors or trace files in real time. Capsa, the Rapid7 vulnerability assessment tool, is capable of storing packets in a ring buffer and exporting them in pcap format for further analysis. SmartSniff presents captured data as a sequence of client-server interactions in ASCII mode (for text-based protocols like HTTP, SMTP, POP3, and FTP) or as a Hex dump. Moloch is a strong web-based graphical user interface that can display sessions and session profiles in tabular form. Scapy is a Python-based packet manipulation program that allows for transmitting, sniffing, analysing, and forging network packets.

Hping enables the sending of bespoke TCP/IP packets to network hosts while limiting the maximum number of packets that can be sent or received. Fragroute is a command-line packet sniffer capable of modifying and rewriting network traffic. Carving can offer both direct and indirect forensic evidence of a variety of natures. Files can be efficiently extracted from packet capture using purpose-built carvers like tcpflow, the Packet Capture Forensic Evidence eXtractor, and File-TSAR. NetworkMiner is a passive network sniffer, capable of detecting operating systems, sessions, hostnames, open ports, etc., without generating any network traffic.

Internet of Things (IoT) network packet analysis plays an increasingly vital role in combating cybercrime and mass monitoring. Rather than employing network segment packet capture files, there is an increasing demand for cloud-based packet capturing and analysis. Amazon has announced virtual private cloud (VPC) traffic mirroring, which enables the capture and examination of AWS network traffic at scale. In network forensics, analysing network packets is essential for collecting the data required to gain a comprehensive picture of online user actions. Legal challenges and concerns regarding the invasion of privacy by packet analysis of wireless network traffic and Internet of Things (IoT) devices continue to rise, necessitating additional research. Achieving a fair balance between privacy and packet analysis has been an issue for a very long time, and this paper encourages study in the area of privacy-preserving deep packet inspection.

5.8.2. Netfox detective

Network forensics seeks to comprehend/reconstruct events from network traffic, a task that frequently necessitates specialised understanding. To alleviate some of the complexity, suitable tools are required. In order to aid investigators, tools should summarise, cluster, and emphasize pertinent information. This is somewhat addressed by Netfox Detective's implementation of sophisticated capabilities such as heuristic TCP reassembling. TCPDUMP, 2020 only provides a command line interface that administrators can use to inspect incoming and outgoing network traffic [91].

Additionally, more specialist programs, such as ssldump, 2020, and tcpxtract, 2020, can extract valuable forensic information. These tools were developed to address specific issues, such as phrase searching in network communication. It is crucial that even non-specialists can run Network Forensic Analysis Tools and extract data to support their cases. Some requirements, such as the processing of massive data sources and the in-depth analysis of talks, are incompatible. These aim to facilitate analysis by automating the extraction of artifacts and offering user-friendly interfaces.

Network forensics necessitates the collection of IP addresses, packet captures, or log files that may contain sensitive information such as passwords, usernames, credit card numbers, etc. Use of Netfox Detective and other Network Forensic Analysis Tool products in the real world must adhere to legal requirements and constraints. Netfox Detective is the only open-source tool that supports Generic Stream Encapsulation for network forensic analysis. Unlike other tools, objects from HTTP transmission are extracted but also the full website is reconstructed (rewriting sources like CSS, pictures, video streams, etc.). It is also used as a standalone console application and may be integrated into automated investigation procedures.

The source code is published on GitHub under version 2.0 of the Apache License. The Netfox Detective YouTube channel has additional information: https://goo.gl/fKM8Vs.

Netfox Detective is a network forensics application designed to assist digital forensics professionals in analysing network captures and swiftly extracting evidence from packet traces. It permits accurate identification of network communications, the parsing of common Internet protocols, and the extraction of metadata and content from end-to-end transmission. The software is comprised of more than 140,000 lines of code divided into approximately 110 projects. Snoopers are designed to parse application interaction protocols and retrieve information such as files, videos, and HTTP headers. The application contains three primary regions, namely the left side, upper right, and lower right, which contain fundamental graphic components.

This structure is helpful for delivering an effective user experience when navigating across interconnected items. Conversations Explorer provides a listing of conversations linked with studied items, such as a conversation or export object. The pipeline performs:

1. packet file loading and processing
2. conversation tracking
3. application recognition; and
4. (meta)data storage from extracted data.

While data is never shared between investigations, the opening of numerous investigations (in distinct docked panes) is provided so that data from multiple sources can be compared. Conversations are viewed as the fundamental data object for subsequent examination.

The system identified conversations across multiple network tiers. Packets whose source and destination addresses are identical are part of the same network layer discussion. Netfox Detective is designed to operate in a single-user environment, i.e. on the desktop of an investigator.

Information extracted, such as talks at various layers, application layer data units, and other pertinent data, is stored in a database. The system does not include user administration, authentication, and authorization permitting investigators to extended use of the instrument.

Following the Test-Driven Development technique, tests were built, then production code that passed the tests, and then refactored the code to enhance its structure. To design and test modules (snoopers/analyzers), testing data was collected employing PCAPs or establishing ground truth using the private networks. Netfox Detective was compared to other existing tools before evaluating its performance and efficacy in the actual world. Despite the TCP reassembly of all sessions, Netfox Framework is marginally quicker than Wireshark. NetworkMiner is four to seven times slower than comparable products.

Netfox Detective supports parallel processing, making it potentially quicker than PyFlag. XPlico requires further study because it processes data in parallel. Tools should report the same number of TCP sessions if there is no packet loss. If a sequence of packets is lost, their count is unknown and can be calculated using a heuristic approach based on the maximum transmission unit or previously recorded segment sizes. Netfox Framework processes all Question, Answer, Authority, and Additional records from both packet types, whereas NetworkMiner just retrieves the response.

Netfox Detective has centred its efforts on extracting capabilities from conversations with incomplete data. NetworkMiner and XPlico rely on SPID and PIPI, but Netfox Detective uses a number of methods to detect the protocol. However, additional testing is necessary to determine which tool is the most reliable. Netfox Detective is very adaptable thanks to the Analyzer API, which enables the addition of pluggable modules. Unlike Wireshark, the development of a new snooper is accomplished by basic imperative programming.

Netfox Detective contains a large number of unique features and is actively being developed; new features can be anticipated. The Session Initiation Protocol Fraud attack takes advantage of a misconfigured Session Initiation Protocol server. The attacker attempts to deduce a secret prefix used to start a call from a VoIP network to the public switched telephone network. Once an attack (or false positive) is recognized, NEMEA (a framework for network traffic analysis) alerts the device, which subsequently collects all evidence (generates a PCAP) and stores it on the appliance's hard drive. The SnooperHTTP tool extracts and retains the contents of all HTTP objects. SnooperMAFF iterates through the HTTP objects to determine which HTML documents exist. This analysis returns all related items, such as CSS files, JavaScript scripts, media streams, etc. Reconstruction of a Web page is only possible if the session is initiated using plain HTTP.

5.8.3. SSHkex

Many users communicate with a remote resource server via a secure channel. This channel gives a high level of secrecy and discretion. Secure Shell (SSH) is one of the most popular remote server connection protocols. Encrypting network traffic between a client and a server, SSH provides privacy and secrecy. The encryption makes it difficult to learn about hostile operations using SSH, especially by merely monitoring network data. Virtual machine introspection (VMI) can overcome this problem. VMI permits direct access to the memory of a virtual machine (VM), including access to SSH process data. However, the current prototype has a large overhead because it extracts every single plain text SSH network payload from memory and the extraction operation pauses the virtual machine (VM). The authors present SSHkex, a program that uses VMI to harvest SSH session keys from a server's memory. This method only requires pausing the VM twice to extract the session keys for each SSH session, and it employs passive network monitoring that has no discernible effect on the ongoing connection. No server modifications are required to use SSHkex. Therefore, it is appropriate for intrusion detection systems and high-interaction honeypots where the server cannot be updated [92].

5.9. File carving

The amount of data to be handled during digital forensic case work is rapidly increasing and is a major challenge. The main focus of a digital forensic investigation are user activity and commonly the who, what, when, where, why and how (5WH) questions are meant to be answered. Digital forensics uses a precomputed map to show the probability of finding user data at different Logical Block Addressing (LBA) positions in NTFS formatted storage media. Precomputed maps are meant to be reusable and reusable between investigations. The mapping process is the same regardless of the type of storage media (solid-state drive (SSD) or mechanical drive). The map can still be used, but in conjunction with a translation table to restore the logical layout of the disk.

A file system is used to keep track of data stored on secondary storage. All modern file systems use index allocation, where the addresses of the file data blocks are held in an index separated from a file's data. There are also a number of algorithms used for handling the free space that is to be populated by new files. Windows in combination with NTFS is using an index allocation strategy. The problem of space being wasted when using index allocation is solved by storing the data of smaller files (up to 700 B) in the meta data records themselves. There are indications of the actual behavior of the allocation algorithm in a Superuser Q&A.

The digital forensics research field of hash-based carving compares hashes of known file blocks to equally sized blocks from a suspects hard drive. In that way even files that are partially overwritten or damaged can be identified. The roots of the research field can be traced back to the spamsum tool.

The concept of data persistence is relevant because the persistence at different areas of storage media indicates that they are not reused. This information is valuable when creating a precomputed map of a generic storage media. Differential forensic analysis has been used to compare snapshots of file systems in use and follow the decay of deleted files over time.

An EnScript module to the EnCase software can be used to create a map of the recoverable sectors of a file found in a file system. Also, a decision-theoretic approach has been researched for application to data mapping but is not generally applicable [93].

PNG is a popular image file format which is widely used especially on web pages. There are techniques to hide exploits or malicious payloads in PNG files, therefore PNG is of high interest and most certainly encountered during a forensic investigation. A PNG file is an extensible file format for the lossless, portable, well-compressed storage of raster images. The most recent PNG specification was published in 2003 and is the main reference to gain knowledge about the internal structure, the data streams, and the syntax of PNG files. PNG defines the IHDR, IDAT, IEND and PLTE chunk types as critical chunks. Therefore every implementation of the PNG standard should be able to correctly parse and render these chunks. An IEND chunk does not contain any data and is, therefore, equal for all PNG files. There are existing approaches which can be applied to carve PNGs, including header-embedded-length carving to find a file's length [94].

Then, the bytes from the header plus the number of bytes parsed from the length field are carved. PNG file header does not have a global length field to indicate the size of the complete file. There are length fields within the individual chunks, though. The existing approaches do not implement what would be considered as syntactical file carving. There are approaches which only use the file structure in a very rudimentary way. The syntax of a file format can be used to aid in the reassembly of fragmented files.

5.9.1. PNG data detector

File fragment classification enables the collection and recovery of data and files by digital forensic tools, especially file carvers. One such file carver is DECA (decision-theoretic carving). DECA originally implemented a JPEG data detector that makes use of escape sequences that appear in JPEG data. The authors decided to create a PNG data detector for DECA. To accomplish this, they looked into the PNG file format specification and PNG data files for a unique and consistent characteristic or feature that shows up frequently in the PNG datastream, thus allowing the design of a means of uniquely classifying or detecting PNG data fragments in data blocks [95].

The unique byte values found in the PNG datastream are PNG signature, chunk type fields, and the IEND trailer. While these values do not occur frequently and consistently, it seemed the best way to identify PNG file fragments in memory.

The detector works with three different components. One component looks for the existence of the byte representation of chunk type field value, another looks for the PNG signature and the other looks for the IEND trailer byte values.

When DECA is operating in its sampling mode, it uses the PNG data detector to verify if a data block may contain the starting point of a PNG chunk. If successfully discovered, DECA switches to its actual file carving process, where it goes back to the block just after the previous block it inspected, and then it switches into its linear carving mode to identify the PNG signature and start extracting the PNG data till it gets to the IEND trailer.

The algorithm for PNG data detector was implemented using the C programming language. It is now stored in DECA's code repository after been integrated into DECA's source code. As part of the development of the PNG data detector, experiments were designed to determine how well the PNG data detector integrated into DECA would perform. Disk images from NIST's Computer Forensic Reference Data Sets (CFReDS) were used, retrieved from the computer forensic tool testing section of the National Institute of Standards and Technology website. In addition, disk images that were produced from an alleged recruit's computer hard-disk, from a simulated terrorist recruitment activity exercise. DECA's code repository now has this disk image and the image files stored in it.

Points of interest from these experiments were the number of PNG files extracted in the quickest processing time while looking out for the amount of false-positives or false-negatives in the output. It was established that operating in sampling mode would extract fewer files than most linear carvers, which was consistent with the results from these experiments. Also based on the results, knowing and specifying the likely partition or volume to find the desired data as part of the argument for DECA's PNG file carving operation will produce faster results. The results from the experiments show that DECA integrated with the PNG data detector works best in scenarios where PNG data are complete and are stored in contiguous data blocks.

5.9.1.1. Carving PNG files.

Each chunk in a PNG file starts with a four byte integer specifying its length. This information enables the easy computation of the expected location of the signature of the next chunk. For non-fragmented PNGs, this results in carving the whole file. The PNG start signature is compulsorily followed by the IHDR chunk. Once a chunk type is known, a series of checks is performed to ensure that it is a valid PNG chunk type. The Cyclic Redundancy Check (CRC) of the current chunk is compared to the value stored at the end of the chunk. This process is repeated until the last chunk of the PNG file, the IEND chunk, is reached. During this step, all non-fragmented files are carved [96].

All chunk jumps, except for the last one, should end at another chunk. It is expected that a PNG chunk type signature will follow a valid chunk jump. Storage devices use a fixed block size which allows a reduction in the number of candidates, and candidates which are located at an incompatible offset are filtered out. By exploiting the syntax of PNG, the detected chunk signatures can be used as anchor points during the carving process. This reduces the problem of carving a whole PNG file at once to the task of carving each chunk individually.

The sliding window block generator succeeds only PNG files containing at most bifragmented chunks. If a chunk is split into more than two fragments, one of its fragments does not contain a PNG chunk signature and, thus, no syntax is available. However, the expected amount of data in between the first and last fragment is known.

As a last resort, the brute force block generator is used to generate all possible disk image combinations. This approach is very time consuming even for a small number of blocks and, thus, most likely not feasible for realistic disk images.

A PNG is considered corrupted when all block generators fail (e.g. by CRC mismatch) or when the number of available blocks is smaller than the required number of blocks. In such cases everything of the file that has been validated is carved. This means that all of the correct data will still be viewable.

The number of block combinations can be drastically reduced as soon as there are blocks that do not have to be considered. Such blocks are for instance those that belong to an already successfully carved file. All of this is possible due to the syntax of PNG files enabling us to identify and validate fragments independently from other carving processes.

5.9.2. File carving datasets

Less than 4% of the datasets created for research are made available and shared with the public afterwards. This makes a meaningful comparison between methods and tools very difficult. The goal was to provide an easy-use framework for the creation of file carving scenarios similar to those covered in the DFRWS challenges. The DFRWS challenges from 2006 to 2007 featured datasets covering various scenarios for the evaluation of file carvers. As these images did not include any PNG files, the decision was made to recreate the scenarios using the framework.

A scenario acts as a wrapper around its fragments making it possible to perform various operations. For most of the scenarios in the DFRWS challenge, an exact order has been provided. The order of the fragments in the intertwined scenarios, though, does not appear to be following a particular ordering scheme. Some scenarios contain PNG files missing their beginning. In these cases, it will not be possible to display these PNGs even if they were carved.

The approach was able to carve files correctly even in complex fragmentation scenarios. There are still some limitations including, in cases of missing fragments in the middle of a PNG file, the approach restores the first part and discards the rest. Padding the missing parts in these cases is not useful, since such PNGs can only be displayed up to the padded part anyway. Syntactical file carving uses the syntax of a file format to the maximum extent.

Using PNG as an example, this approach enables effective file carving even in very complex fragmentation scenarios. Due to the lack of suitable datasets to evaluate the approach, the authors created a framework allowing the easy and automated creation of dataset which can be used in the assessment of file carvers.

5.9.3. *Location of user data*

The experiment conducted by Karresand et al. (2019) [97] is based on iterating over the same process a predefined number of times. The goal is to keep the NTFS file system as pristine as possible to allow the study the allocation algorithm from the start of the life of the file system. Sixteen virtual machines use exactly the same file operation pattern to test if there is any deterministic behavior connected to the allocation patterns.

The $Bitmap file from the MFT is used to check which clusters are affected by each file operation. Each virtual machine has a 64 GiB fixed virtual disk. The disks are given their full size directly when created, which makes them behave as real hard disks.

The virtual disk files can be handled by standard Linux file carving tools, such as dd. There are limits on the usage of the storage area to simulate a user that fills a hard disk with files over time and then erases a certain amount when the hard disk is believed to be full. The assumption is that a user who is web surfing will create mostly small files (cached data and logs) and a file sharing user will create a high amount of large files. Every file operation is logged in a file external to the virtual disk.

The log contains the sequence number, the name of the affected file, the size factors, the current random size number and the current file size. The $Bitmap file is used to represent the allocation status of 4 KiB NTFS clusters as the smallest unit for each operation.

All existing files containing the string “Windows” somewhere in their paths were extracted. The files containing “Users/" were then filtered out to avoid contaminating the result with user data. As the behavior of the OS cannot be controlled, any allocation changes induced by the OS are also included.

The $Bitmap files extracted during the experiment contain traces of the file operations executed by the scripts, but also those of the operating system (OS). The start and stop phases of an iteration will induce changes to the file system. An MFT record is 1 KiB in size and the smallest allocatable unit in a 64 GiB NTFS partition is 4 KiB. Every fourth file creation will give rise to a new cluster due to new MFT records being created. The minimum requirement for free hard disk space for a Windows 7, 8, 8.1 and 10 installation is 20 GiB for 64-bit systems according to Microsoft.

The distribution and positions of the system files (OS and installed software) is uncertain. What is known empirically is that the MFT starts its allocation at exactly 3 GiB into the partitions. The sub-experiment only included three different versions of Windows (7, 8.1 and 10). Yet it is possible to see similarities with the results of the other experiments.

The algorithm might still behave differently in partitions larger than 256 GiB. This is left as future work due to the current limitations in the hardware available to us. The OS files written during installation are placed at the beginning of a partition. The Windows 7 SP1 partition even has two vertical bends, the second bend probably originates from the Service Pack installation. The more irregular shape of the real-life hard disk curves comes from a more frequent usage and longer life span than for the virtual machines.

An experiment showing the placement of OS files is based on only seven hard disks, including four that are virtual and specifically prepared for the experiment. The result should be seen more as an indicator of approximately where on disk system files reside, not as the truth. The selection of files to be included is based solely on the existence of the word “Windows” in the path of the files. The allocation algorithm is allocating free areas in order of increasing size which contradicts a strict best fit behavior. The behavior gives a high fragmentation of files, but preserves any large unused areas.

The mapping concept is also beneficial to the daily work of the digital forensic investigator by introducing the possibility to plan the forensic process in a better way. Currently hard drives and other storage media are treated as black boxes and scanned from start to end before the analysis. Using the map, the forensic investigators can focus on relevant areas of the storage media and postpone, or even skip, less relevant areas. The map is also applicable when imaging storage media. By starting the imaging process at the most probable area of user data and continue in decreasing order of relevance some of the analysis work can be started immediately rendering results faster.

5.9.4. *Time carving*

File carving is a technique that extracts files from unallocated spaces based on signatures inside the file’s content, as opposed to file system metadata. While incredibly beneficial, file carving has certain obstacles. When attempting to carve a fragmented file, certain carving techniques fail because they rely on the assumption that files have contiguous blocks, which is not the case. On the basis of a common identifier, the authors seek to identify file or directory information structures from diverse file systems. They identify potential timestamps using a basic string matching method and then interpret the expected file system metadata to eliminate false positives by a large margin [98].

The method is suitable for recovering metadata and file content from reformatted storage media. It is not sufficient to identify the metadata in order to establish a connection between file content and metadata, as the content may be overwritten by allocated files. The authors explain the necessity of performing a manual evaluation of information, content, and context; then they further strengthen the evidentiary value of the recovered files by precisely relating the metadata to their corresponding file contents.

MFT entries could be located in numerous locations, including memory dumps, unallocated space, and allocated system files such as $MFTMirr and hiberfil.sys. If a data run discovered in a recovered metadata structure uses one or more clusters allocated by a file in the new file system, it is assumed that the file’s content has been partially rewritten. It has been demonstrated that popular digital forensic tools, such as the most recent versions of X-Ways or Encase, do not necessarily locate the MFT entries when the NTFS file system is converted to exFAT. This may lead the investigator to wrongly employ file carving, which does not include the file’s information but merely its content. High precision and recall do not imply that this programme will locate almost all metadata items without error, but it does indicate that it will perform well if the metadata structures contain repeated timestamps.

The approach does not distinguish between MFT records/inodes in the MFT/inode table and occurrences in the journal or elsewhere. This is not a limitation, but a feature, as remnants of metadata structures that describe files can be dispersed throughout the file system.

The experiments demonstrated that a collection of comparable timestamps can be used as a sort of dynamic signature (magic identifier), and these are carved using a straightforward byte-matching technique. It is suggested that a context-based, manual evaluation of the dependability of the link between metadata and file content is required, and that this evaluation must be performed manually for non-resident file content. The approach had 100% accuracy when extracting inodes from both the original Ext4 file and the reformatted image. Inodes for 5755 of the 25050 identified files and directories within the original image could be retrieved. Since at least 20257 of the 25050 inodes were removed from their respective inode tables, it is possible to retrieve 963 inodes. File recovery automation is conceivable, but requires context-aware capabilities.

5.10. File systems analysis

5.10.1. Selective imaging of file systems

Storage device size increases are causing digital forensic investigators challenges. Selective imaging is recommended for these issues in the literature. Only replicating selected data objects creates a partial image that takes less time and space. The proposed Selective Imaging Tool (SIM) can selectively image live Windows file systems. It uses current investigative software like the DFIR ORC framework and AFF4 as its forensic container format. No other open-source program collects live system evidence with comparable dependability and integrity [99].

A live selective imaging strategy offers a number of major advantages and, in certain instances, is the only viable choice. Significant difficulties arise while working on live systems, which are frequently outside the investigator's control prior to access. Some of these obstacles exacerbate issues inherent to selective imaging in general, while others are unique to the live environment. Implementation-wise, the selection process should be treated independently from the imaging instrument. It is preferable to use analysis tools with minimal side effects. To satisfy the verifiability and chain of evidence requirements, the selection procedure must be sufficiently transparent.

SIM collects file system-level forensic artifacts and information. It integrates the results into an Advanced Forensics File (format) 4 forensic image and checks for unexpected outcomes and external interference. Portable binary software was required. SIT has four logical modules. They can run sequentially, independently, or disabled.

Each module logs pertinent actions and provides rich console output. If the live system unexpectedly shuts down, the interim results can continue the process. The open, ZIP-based, expandable AFF4 stores evidence and case information. It stores data objects, information, and references in a central data store using an object-oriented paradigm. The resolver can identify each AFF object by its URN and associate its metadata.

The AFF4 source code includes the verification module. The SIM binary uses the same image archive access functions. All image artifacts are copied into a temporary directory and MD5, SHA1, and SHA256 hash codes are calculated to verify the hash. The artifact module's hash values from acquisition are compared to these.

5.10.2. Windows file history

Users can quickly remove and restore backed-up files using the File History function in Windows 8. The authors were able to extract a collection of backup files and examine artifacts that demonstrate user actions [100].

The suggested process entails finding file history traces inside target storage devices, identifying all devices connected to file history, and retrieving backup file data. The generation and change of configuration XML files can be used to determine when backup settings for file history were initially specified or updated. Examiners can locate host Windows systems and storage systems by using Config.xml to identify them. It includes precise identifiers related to a storage device, a user account that enabled file history, and (1) a host system with data that will be backed up. It is important to extract a list of backed up files and examine the metadata of the files using EDB (Extensible Storage Engine database) files found in the aforementioned configuration directories after identifying file history linked host Windows systems and storage devices from Config.xml files.

Each file that is backed up keeps its original folder structure and modification timestamp, but when a file is created, new creation and access timestamps are given to it. Experiments demonstrated that the traits are constant no matter what. For backup storage devices, filesystems like FAT32, exFAT, NTFS, and ReFS are used. The following are the file history's default backup folders: Contacts, Desktop, Favorites, Music, Pictures, Videos, and Documents. Pictures, Searches, 3D Objects, OneDrive, Saved Games, Links, and Downloads were all included by Windows 10.

File history enables users to access a network location shared through HomeGroup in Windows 10 versions 1709 and before. Users can still set up a shared network drive as a backup storage location for file history even after Windows 10 version 1803 eliminated the HomeGroup capability from the operating system. In order to assist examiners who need to thoroughly comprehend any aberrant information that could be formed as file history associated artifacts, this section investigates the effects of four potential anti-forensic actions.

Users can always restore backed-up files and erase previous backup versions using the file history feature. Although they can also be used for anti-forensics, these qualities are crucial for backup operations. A list of files that have been backed up by file history is displayed by Windows Explorer's "Previous Versions" feature. Users have the option to selectively open or restore a file that has been backed up at a specific period using the Previous Versions.

Data recovery is expected to reveal more details regarding file history's operations to investigators. If a user often resets file history, numerous file history backup folders with consecutive numbers may exist. Examiners must use Config.xml to check the current (active) backup storage path and must conduct an aggregated analysis of all backed-up files located in various backup folders. Because external storage devices can be used to backup files, it is simple to detach an active backup storage from a PC that is already running.

The Python3-based EFIC (extract file history IntelligenCe) comprises two phases: "preprocessing" and "information filtering and normalisation." First step gathers information from file history-related files from a forensic picture. The second phase normalizes and stores the extracted information in a database. The source code under development is available for anybody to use, modify, and validate.

5.10.3. NTFS

The volume of data to be processed during digital forensic investigation is a formidable obstacle. Previous researchers have independently proposed using the inherent data structures to enhance the digital forensics process. Digital forensics is based on utilizing the inherent structures of data, but the concept of utilizing the inherent structures introduced by the storage process in stored data is relatively new and has not been thoroughly explored. Therefore, it is necessary to determine the actual behavior of the allocation algorithm for each relevant file system. Making use of the pattern introduced by the allocation algorithm is the foundation of this idea. This paper tests information on the allocation behavior of NTFS in newer Windows versions (versions 7 to 10). This includes adherence to the optimal allocation approach and an even distribution of activity across the (logical) storage area's addresses [101].

It is also determined if the allocation algorithm used by Windows and NTFs is version and/or size dependent. A weighted random distribution is applied to write, expand, shrink, and delete files in four distinct Microsoft Windows versions (7, 8, 8.1 and 10). Following each procedure, the current cluster allocation status was extracted from the Master File Table (MFT). The allocation status was then used to determine the difference between each operation's cluster allocation. Microsoft Windows' NTFS file system uses an index allocation mechanism.

By keeping the data of smaller files (up to approximately 700 B1) within the MFT records themselves, the issue of wasted space while employing index allocation is resolved. In addition, a number of techniques are employed to manage the empty space in the data portion that will be populated with new files. A file can either be written as a stream or as one enormous block at once. When a file is written as a stream, the operating system cannot optimize the allocation since it does not know the file's eventual size. This frequently results in file fragmentation, but this tendency is partially alleviated by the operating system's internal buffering. The $MFT began precisely 3 GiB into the NTFS partitions of over 30 actual hard drives. The partition with the highest activity included around 10 GiB. The outcomes were determined using a small number of writing operations, Windows versions, and partition sizes.

Casey (2018) [102] introduces digital stratigraphy, a new branch of digital forensic investigation. It is influenced by archaeology, which shares many characteristics with digital forensics. The concept is to see file system processes as hierarchical layers (strata). This structure can be used to supplement, enhance, and increase the data currently collected from hard drives and disk images. The MFT records of an NTFS partition should be extracted first. The analysis method is used to impact the imaging process by prioritizing particular sections.

A framework for studying the persistence of (deleted) files on storage medium shows that the file system may not reuse deleted files. Maximum and median fragment sizes in Windows 7 exhibit linear features that are absent in Windows 10. Additionally, there are sections of the file system that are rarely accessed, generating bands of low allocation activity throughout the file systems. The outcomes can be used to establish the sequential order of files and estimate the appropriate size of file fragments to be carved.

Throughout each iteration, the $Bitmap files extracted during the experiment contain evidence of the file actions done by the scripts and the operating system. MFT records are 1 KiB in size, while the smallest unit that may be allocated on a 64 GiB NTFS system is 4 KiB. Every fourth file creation may result in the allocation of a new cluster in the MFT (not until the preallocated MFT space is used up). The location in the file system where the operating system files are written during installation is identical for Windows 7 and Windows 10. Windows 7 and 10 are less likely than Windows 8 and 8.1 to allocate files in that location.

The vacant space in the centre of the dividers may possibly be an experimental artifact. Since it was attempted to make the virtual computers equal, an OS installation issue might have had a significant effect on the results. However, the fact that half of the included virtual machines executed unique file operations sequences while retaining the same unused space contradicts the installation fault idea. The phenomena of the maximum allocation position, described as the mountain range's leeward effect on clouds, is intriguing.

There is a distinct difference between Windows 7 and 10, with Windows 10 favoring continued use of any high allocation addresses. This indicates that Windows 10 uses storage space more efficiently than Windows 7. NTFS's best fit allocation technique aims to reduce file fragmentation by optimizing the used area in relation to lost space at the endpoints of the allocated free area. Fitting an allocation into the void created by the deletion of a file actually results in less free space surrounding the allocated area than would be the case if the big empty area at the end of the partition was used. Since all virtual drives were configured to simulate mechanical hard drives, this distinction cannot account for observed behavior.

It was demonstrated that the allocation algorithm's top priority is to eliminate gaps caused by file deletions, not to use the entire disk. The knowledge gathered from the experiment is particularly useful for file carving, where the objective is to reconnect file fragments with their originals. The outcomes can also be used to enhance the development of time lines (work as another source of time stamp information).

5.10.3.1. NTFS cluster allocation. $LogFile is an NTFS (New Technology File System) metafile. It logs data from file system operations such as file creation, deletion, data modification, and name change. Data on all file-level operations conducted on the file system over a particular time period is recorded and can be analysed. The $LogFile comprises 4096-byte pages and is separated into a restart area and a logging section. This enables examiners to collect the time and file revision of the update to the file for each task performed by the user, which is now impossible with the conventional method. Depending on the technique used to open the file, the file data may be kept in a distinct location for each alteration. A record comprises a header and data, the Record Offset and Attribute Offset, information on the place within the $MFT entry used by the operation. The record's Redo OP and Undo OP values are set based on the type of operation being executed [103].

The NTFS Data Tracker offers file data viewing, file data recovery, search, and CSV export capabilities. An image file containing the $LogFile and $MFT must be received as input in order to examine and recover the file data. Downloadable from the URL below is a user guide containing comprehensive descriptions of the tool's features and contents. Results of a comparison between common forensic tools and NTFS Data Tracker for each function targeting the provided test image. By evaluating the $LogFile and $MFT data, each tool should have been able to extract the events of each file, the time of each event, and the file data information when the event occurred.

The NTFS Data Tracker can follow the history of file data that other programs were unable to analyze. At each correction point, it was able to acquire the data runs, resident data, and modification time. It also enabled data history grouping, enabling the integration of histories that were recognized as belonging to distinct files into a single data history. In this study, the SMT (Simulation of MFT Transaction) technique was used to examine $LogFile entries. This allowed the monitoring of the revision history of a file's data from beginning to end. Then it may be possible to detect behaviors that were not previously detectable utilizing strategies presented in prior research.

The tool is freeware and can be downloaded from https://sites.google.com/site/forensicnote/ntfs-data-tracker.

5.10.4. ZIP format

ZIP files are popular as they are provided as standard during operating systems installation. ZIP files store compression target file times, therefore they reveal the creation and modification environment. Artifact analysis helps identify file sources. A ZIP file's structure analysis and decompressed file and folder attributes can reveal its origins. The ZIP file's signature is '0 50 4B 03 04' [104].

Windows stores it in a central directory header-only field. In macOS and Ubuntu, the local file header additional field contains time information. Ubuntu's extra time field allows nanoseconds, even though it's not NTFS. When macOS or Ubuntu compress a ZIP file, the header ID is 0 5455 (Extended timestamps), which encodes time information in 32-bit Unix time format (4 bytes), and 0 7875 (UNIX UID). The time zone can usually be calculated by subtracting the two time information values from the additional field.

Bandizip, Compress, zip on Mac and Ubuntu can identify the system environment in which the file was created or updated. ZIP file structure can reveal account and ID values (UID and GID) used to compress it. A compressed ZIP file's file name creates a Unicode Path Extra Field. This field holds the file name's language type or system setting's language encoding. The extra field's header ID is 0 7075 to save the file's name in Unicode.

The order of header IDs in an Extra Field in a file or central directory header might be used to identify it. Mac OS X uses Korean phoneme units, while Windows uses NFC (Normalisation Form Canonical Composition) encoding. ZIPs compress each file. Recompression is not done on ZIP files that have been compressed enough. Recompressing a ZIP file loses its structure.

Windows WinRAR can compress files in a different order than folder-name. Only the ZIP file can reveal its creation environment. The ZIP file's system metadata reveals the compression environment's OS. Compress automatically constructed a data descriptor with the signature '0 50 4B 07 08'.

The ZIP file format mirrors the OS and programs. Thus, ZIP files created by the same application on different operating systems have different file fingerprints. If two ZIP files are created by the same application, the additional field will be the same, but the central directory header will indicate the operating system. MacOS uses NFD UTF-8, but Windows and Ubuntu use NFC, hence the same Korean alphabet letters have different hexadecimal values. The ZIP file's source attributes should be examined since file fingerprints combine operating system and program characteristics.

Header ID is the extra field ID value when the ZIP file is produced. The extra field timestamp storage approach reflects the 100 ns NTFS time accuracy discrepancy for each compression application. Encoding is the header's file name field value. When a subdirectory-structured or empty folder in the compression target is compressed, a header is generated. Root folders determine whether headers are generated and if the file name field of headers includes the root folder when compressed. Double zipping means recompressing ZIP files in the compression target. The compressed file header's compression order.

An automatic classifier to detect a ZIP file's system environment was constructed. Structural ZIP file analysis combines operating system and application characteristics with the compressing-target file determining some properties. System artifact analysis is recommended for some low-reliability features.

Depending on the configuration and use of the computer, the operating systems and applications created many ZIP files and revealed whether the ZIP files were local or imported. Operating systems and applications have different ZIP fingerprints. Multiple systems in a ZIP file indicate multiple modifications.

5.10.5. *Resilient File System*

Digital forensic tools should ideally be compatible with all file systems currently in use and potentially encountered during a forensic investigation. New filesystems, such as APFS and Resilient File System, were created due to the shortcomings of conventional file systems, such as poor performance, limited capacity, and incompatibility with solid-state drives. These new file systems must be supported by open source forensics applications and documentation. The Sleuth Kit is an open-source forensic tool for filesystems. It was designed with a focus on portability and extensibility. The Sleuth Kit's strong extensibility enables developers to expand its features. The authors investigated Resilient File System v3.4's allocation technique, which affects the recoverability of previous file states [105].

Resilient File System partitions feature two checkpoint structures that are written alternately so that at least one checkpoint will be valid in the event of a system failure. A system crash reverts the system to its most recent valid state and undoes any changes made in the meantime. Every batch transaction that was successfully executed is also recorded in a sequential log file. According to its properties, data must be rearranged in a multitiered storage system. To accomplish this restructuring, it is possible to exchange bands and, by extension, their contents, between various storage levels.

Before they can be used, nearly all Resilient File System addresses must be converted into real addresses. The Object ID Table stores the addresses and checksums of the tables it refers in addition to their most recent log sequence number in the file system journal. The real addresses of all Directory Tables are contained within this table. Recovery approaches that aim to restore Resilient File System directories should prioritize recovering rows from this table. The ID of the root Directory Table is 0×600, but the IDs of all additional Directory Tables are more than 0×700.

A directory link primarily associates a name with a directory ID, which may be retrieved from the Object ID Table. For all files in a Directory Table, a second item type exists, called ID2 that offers a mapping between the metadata address of a file and its current handle. Files and folders are uniquely addressed using metadata addresses. The majority of data in Resilient File System are arranged in key-value stores, often known as tables. The behavior of NTFS attributes is comparable to that of file-descriptor tables.

This method also makes it simple to locate a relative offset in a file, as the tree used to store data runs is ordered by the relative beginning of a data run. When an entry is removed from a B-tree node, only a link to a data chunk is removed and not the entry itself. This process propagates to the root node, where pointer modifications generate a new root node. The Copy-On-Write technique also copies this non-referenced data. To retrieve entries from nodes, the entire partition must be scanned for indicators.

The Sleuth Kit includes a list of filesystem openers that can be used to attempt opening unknown filesystem types. The opener returns a context object that retains fundamental information about a filesystem, such as the block size, the first/last block of the file system, and the addresses of the metadata. By reading the initial sector of the file system, the opener parses and verifies (with signatures and checksums) the boot sector. It is feasible for many tree structures to comprise a directory. This behavior is mostly caused by the Copy-On-Write procedure, which writes the root nodes of tables to new pages continuously. It is essential to not only read all ordinary entries in the Object ID Table, but also recover deleted entries that can be identified by signatures in their keys.

Large portions of the NTFS implementation were repurposed for this implementation. Multiple copies of a file with a shared metadata address are not addressed with the Sleuth Kit. The user may supply an image and an offset to the carver, which will then attempt to recover lost files and directories from the image.

It searches the full input image for blocks that resemble tree node pages. In each stage, the page header within the first 80 bytes of a read block is validated. If these bytes meet the criteria for a page header, the page is retained for further processing. When searching for the key to a directory table in this map, the caller may retrieve a list of all pages that contain information pertinent to this table. The number of addresses stored in the page header is used to determine if the page belongs to a volume with a 4 KiB or 64 KiB cluster size.

Additionally, the carver must know at which disc offset the volume began. In the reconstruction phase of a volume, the internal representation of files and directories is initially analysed. The carver looks for signatures that can be used to recognize files, directory links, and directory descriptors. Upon discovering a signature, the carver attempts to interpret it as the structure it believes it to be. Additionally, it must restore the subtree established by directory descriptor tables and file tables in order to retrieve their attributes and runtime data.

No current research focuses on restoring files and folders from file systems formatted with Resilient File System. Multiple test scenarios representing fictitious file system usage were created. The distribution of the actions, however, was based on previous authors' arbitrary estimations of how frequently certain events occur. The file system's final state contains all existing files and directories. The only results of the single-executed procedures are the logging of file modifications and directory creations.

As a deliberate decision regarding the weighting of the results, the changes in the metadata of directories caused by file activities were not reported. In this examination, the capacity to recover deleted files and rebuild past file and folder states is compared. The outputs of the generated tools to the action trace log that was recorded during the development of the test image are also compared. The primary disadvantage of the carver is that it cannot distinguish between existing and deleted files. In this analysis, the effect of the Copy-On-Write mechanism on the recovery of historical file states is examined.

A small application that stores text in a Resilient File System file was developed. Text was generated artificially at the rate at which a human types (175 characters per minute). The text file was saved every 2 min, along with a checksum of its current intermediate state and metadata. If this address is used for a subsequent allocation, this state can no longer be restored. All of the older pages in this page chain that are not reallocated may still contain significant information.

5.10.6. *Google's Fuschia*

Google is actively developing the open source "modular, capability-based" operating system Fuchsia. Unlike Google's other operating systems, Fuchsia uses a Zircon microkernel instead of the Linux kernel. The presence of ex-Android leaders has led to rumors that Fuchsia may be a replacement for the Android operating system as a whole. Google is developing the Open Source Fuchsia operating system for use on a range of devices, including previously unknown ones, inferring its potential use in Internet of Things devices. A lack of available metadata can hamper the capacity of digital forensic investigators to determine which user or application accessed or modified certain data sets. This has repercussions for digital forensic investigations [106].

Fuchsia defines a variety of unique file systems for the Fuchsia Volume Manager (FVM). BlobFS provides a flat file system for "write-once, read-only" data, such as system service application packages. The operating system also employs a transparent disk encryption mechanism called zxcrypt, which appears to operate similarly to the Linux kernel's dm-crypt (Device Mapper crypt).

Examining the data structures contained on Fuchsia storage drives and determining their unique identities. This enables the identification of the slices' physical placement on disk and offers context for their virtual presence within file systems. Also studied was the content of the superblocks, FVM Partition Table, and Slice Allocation Table. The data structures used by the partitions within FVM were examined and the associated metadata was identified. It was discovered that the Superblock for both BlobFS and MinFS outlines crucial structural characteristics for each partition.

This enables the identification of the sizes and physical locations of referenced data on the disk, as well as, with MinFS, the creation and modification times and file names of particular objects. The absence of data entries in the Journals of both MinFS and BlobFS continues to cause confusion. This may be due to the relatively tiny sizes of each partition or the unfinished nature of the underlying codebase. The use of zxcrypt by default on MinFS partitions permits the encryption of the area of greatest relevance to forensic practitioners. In the absence of a technique to bypass or extract the TPM's keys, investigators may be compelled to operate off-device or on the live system.

The compressed BootFS filesystem detected within the ZIRCON partition(s) should be investigated further. This may be valuable for examining and comprehending Fuchsia's kernel and security model implementation. Analysis of the codebase and interaction with the operating system are required to determine the true use of the two extra bytes present in each FVM slice table entry. It is necessary to conduct additional research into the Fuchsia data block allocation mechanism to verify the viability of accurate data recovery using file carving or other means. Examination and identification of system-level artifacts of forensic importance (system logs, user list, and user apps, etc.) will be required as the OS continues to grow. Digital investigators lack the appropriate tools to solve this issue.

5.10.7. Distributed file systems

The challenge to managing big data in distributed file systems is met through the management of metadata via a master server. The Hadoop Distributed File System achieves this by managing the metadata details of structure of the distributed file system abstraction through file and directory attributes, mapping of data to data storage locations and namespace hierarchy. The Hadoop ecosystem comprises four layers in varying configurations that provide data storage and processing solutions. A subset of metadata at the Hadoop Distributed File System can be used to reconstruct file system operations and to map data to the physical storage location. Once it has been mapped. The digital evidence can be prioritised and targeted for preservation and further analysis.

The researchers found that audit logs revealed data block node destinations (location) including for deleted files, via IP addresses and port numbers. The probability of deleted file recovery is dependent on block pool space, post-deletion writes to disc, disc drive types and the local file system disc management protocol in addition to other factors [107].

5.10.8. Machine learning for file systems analysis

In most instances, digital forensics analysis is a manual procedure. However, the true worth of data is determined by its ability to generate information that can aid in decision-making. When the number and dimension of data expand, investigation costs rise, and forensic analysis becomes more complex, the manual process can degrade rapidly. Machine learning appears to be an excellent way for facilitating the production of potentially helpful information for decision makers [108].

This paper investigates the applicability of Machine Learning approaches to the reconstruction of cybercrime incidents. It will compare the performance of multiple Machine Learning-based models for determining which application software accesses which file system. In 2001, a road map for digital forensic research was published. This road map is regarded as the foundation for all subsequent proposed models. The processes of conducting a digital forensics investigation comply with steps of constructing Machine Learning models. However, they all agree that the incident reconstruction process is a vital element for any productive investigation. Email is a fundamental mode of communication and, as such, constitutes an important potential source of evidence. Globally, there are more than 3 billion email accounts, with 25% being business email accounts. A crucial responsibility when dealing with emails is to ensure authorship verification and attribution.

Event reconstruction has successfully adopted an ontology-based technique. Support Vector Machine as well as clustering techniques were applied with encouraging results. Shellbags store user preferences, such as the position and size of windows, the location of folders, etc. In addition, they give information about files and folders even after they have been removed, relocated, or modified.

This collection of tests tries to assess the competence of multiple Machine Learning algorithms in classifying which files have been changed by a computer programme. Several footprints (features) associated with file system activities (file system metadata) and system event audit log entries have been collected in a training dataset. Identifying the collection of files affected by an incident would simplify the reconstruction of past events. The total number of incidents collected was 42,528. These application programmes were executed under four distinct circumstances.

The files for MS-applications, NetBeans, Adobe Acrobat Reader, VLC, WEKA, and MS-Paint were previously stored on the hard drive. In Internet Explorer, many tabs were launched, loading a protected website (https) and an unsecured page (http) (http). Preprocessing is the process of grouping values in order to reduce the number of different states a feature can have. Before presenting certain features to the Machine Learning algorithm, they should be discretized. Outliers in input data can distort and mislead the training process of Machine Learning algorithms resulting in longer training times and less accurate models.

This study uses the "min-max" technique for normalising the collected dataset. It seeks to choose a subset of input qualities that significantly contribute to predicting the class variable's value (output feature). Data dimensionality will also be reduced during feature selection, resulting in time and memory savings during the training of the Machine Learning algorithm. Too many features may be derived from file system, audit logs entries, and registry information (source of training dataset in this research) (source of training dataset in this research).

Machine Learning approaches are tested for recreating cyber-crime incidents by recognizing the right files. This study considered these Machine Learning algorithms:

1. WEKA's Feed Forward Neural Network algorithm. Neural Networks are computer models of the human brain and nervous system. Nodes represent neurones or processing units. Connection weights (synapse strengths) determine the node's output. Weights indicate a processing unit's relative value to each input and are modified numerous times during learning. Delta rule or "Widrow–Hoff learning rule" is used to correct weights.
2. Support Vector Machine: SVM produces a hyperplane or set of hyperplanes in a high or infinite-dimensional space for classification, regression, and other applications. A hyperplane divides samples

with differing class memberships into a clear gap as big as possible. SVM handles numerous, continuous, and categorical variables.

3. Random Forest: generates a random forest of Decision Trees, usually bagged. Bagging uses many learning models to improve results. Most machine learning systems solve classification and regression problems.
4. Classification and regression trees use a decision tree technique. Recursive binary splits partition the training dataset. It works well as a simple decision tree algorithm.
5. Naïve Bayes: a basic, effective, and popular machine learning classifier that classifies using the Bayesian "Maximum A Posteriori" judgement rule.

These algorithms were chosen because they use distinct classifier techniques and are commonly used to create classification models.

Digital forensics must create a timeline of the activities conducted on seized computers(s) which aids in highlighting the user's access to the investigated machine. A study of which file system is read, changed, or deleted by which application software is a crucial step towards precisely reconstructing events timeline. The purpose of this study is to determine whether Machine Learning techniques may be successfully employed to this objective. The margin between the highest and lowest accuracy rates produced by the investigated algorithms was 4.7525%, indicating that the accuracy rates produced by each algorithm were relatively similar. These results suggest that the Machine Learning methodology can be successfully implemented in digital forensics investigations.

The Neural Network algorithm outperforms all other Machine Learning algorithms in terms of recall. All considered Machine Learning methods generated reasonable results, however they were less than ambitious. Support Vector Machine-RBF produced the lowest F1-Score when compared to other algorithms.

5.10.9. *File system interpretation*

The file system contains the vast majority of digital evidence. Access to and accurate interpretation of the data structures are crucial to the investigation of crimes using digital data. Validation and verification of the precision of file system interpretation by tools and auditors are still in their infancy. The rapid advancements in digital forensics render many existing validation schemas obsolete, alter reproducibility studies and disturb accuracy testing, as well as in the subsequent court evaluations. The author contends that formal, agreed-upon, and enforceable validation methods are necessary [109].

A literature analysis on file system reverse engineering seeks to identify a new framework for verifying the trustworthiness of digital forensics. If fields in a structure are required for a functional file, it is essential that Law Enforcement Agencies comprehend their significance. This information can be used to generate alternative and null hypotheses for testing. Alternative file system drivers may be able to modify file access timings or file sizes post-creation to conceal malicious behavior. By physically evaluating the structures and performing black-box testing, reverse engineering can be used to comprehend and interpret the file system. The most critical LEA user needs are that the results are accurate and trustworthy, and that errors and bias concerns are mitigated. Additionally, the reverse engineering approach should be documented so that it can be evaluated by peers or contested.

Digital forensics tool and process validation is not standardised, and court standards for digital evidence trustworthiness vary by jurisdiction. The lack of large, centralized validation and reproducibility studies has been noted in previous papers. The current paper considers standards and academic principles to develop appropriate validation criteria. NIST tested the most common mobile acquisition tools used by non-experts to obtain file system data and to analyze "unexpected" data from the most popular instant messaging apps, social networking sites, and file systems.

This study reveals that the tool creator cannot evaluate tools, hence an independent European or worldwide agency should verify and validate them. Testing software and hardware need meaningful, acceptable, and proportional data sets; while peer-review should be conducted by competent, analyst peers who were not involved in the original examination. The ENFSI recommendations advise labs to check with their legal department before reverse engineering third-party software. The UK forensic science regulator is the first independent authority to mandate ISO/IEC 17025 lab and network forensics accreditation.

As practitioners fail to review, verify, and justify changes to procedures, such as software updates, validation decreases. Most methods fail to meet known error rates and lack testing resources and data sets. Digital forensics tool limits and need for more robust file system interpretation. Carrier claims that most digital forensic file system analysis tools display recently deleted files and folders and sometimes recover them. The report claims that developers must release source code used to generate proof.

Dual-tool verification compares the output of two or more digital forensic tools in an opaque-box investigation to determine accuracy. To confirm file system interpretation results, digital forensic investigators need numerous tool suites. When separately designed and tested on the same input data set, tools with the same or similar features should not have the same mistakes. Dual-tool verification resembles N-version programming, especially when considering tool characteristics.

"Opaque box" investigations of practitioner success or failure under diverse test situations might help assess expert outcomes, although it is inefficient. Digital forensics results are generalizable, reliable, and reproducible due to data set quality, amount, and availability.

This study addresses digital forensics file system analysis, not acquisition or encryption. Numerous file systems are either proprietary, patented, or a hybrid of open and closed source. Reverse engineering is required because the vendor documentation is either unavailable, regarded as a trade secret, or unsuitable for law enforcement purposes. The methodology of validation in this paper is primarily based on and expands upon the Daubert criteria.

The proposed validation model outlines the information that must be documented to evaluate the validity of file system reverse engineering for investigative purposes. On the technology, technique, and application levels, a validation procedure and minimum documentation are defined for each criterion. It overcomes the constraints of existing technology level testing (e.g., dual-tool verification, opaque-box testing) and enables the daily validation of more robust and advanced approaches such as reverse engineering. On a technological, technique, and application level, this validation framework requires the reporting of a variety of faults and specialised abilities. The framework can inform examiners of the minimum documentation necessary for validation and serve as a guide for their daily work.

Even though this test focuses on file system reverse engineering, the model may be reused and expanded to encompass more methodologies and tools. The documentation must describe the file system, test setup, and test data set. Quantifying the suitability of the data sets for the reverse engineering experiments. In order to characterize the results' dependability, it is essential to specify precision and recall results on a methodological level.

The examiner takes the assumption that the file system will behave identically regardless of whether the input is synthetic or actual data. The examiner's ability to execute file system reverse engineering can be supported by certification or other evidence of domain-specific expertise, knowledge, or experience.

The testing methodology for the ExFAT file system's low level structures is not documented. He does not explain which reverse engineering tools were used. There was no description of previous problems, validation or verification reports. The results are presented in the form of offset tables that describe significant structures and their interpretation.

Reverse engineering was used to investigate the APFS file system. At the time of reversal, no information was known on the file system's low-level structures, and the available digital forensic tools did not support this file system. It is not specified how reverse engineering or testing was conducted. There is no description of the used data sets.

The first reverse engineering of the Resilient File System that was peer-reviewed was performed in 2019. The study concentrated on recognizing metadata structures and explaining their significance in the context of digital forensics. In addition, new techniques for metadata carving and file recovery were presented. The addition allows investigators to validate the results of other digital forensics tools with ReFS support. The study outlined the type of analysis conducted, as well as the exclusions. The FRED framework served as a guide, at least for the creation of trials to validate tool outcomes.

A second reverse engineering of the Resilient File System was conducted in 2020 which provided a high-level description of certain ReFS structures and a Sleuthkit module for parsing the file system. There is no previous validation or verification of comparable tools, nor are there any error reports. The experiments for reverse engineering are not disclosed, but the tests of the tools are.

Even if a paper satisfies all of the suggested validation model's requirements, this does not imply that the paper is validated. It just means that it can be validated if it meets customer specifications. Since validation is all about meeting the criteria of the customer, the same procedure may be valid for a security business performing incident response but not for law enforcement agencies obtaining all required data. Commercial versus open source is an important topic to debate while evaluating the veracity of outcomes. Intellectual property rights may impede the ability to evaluate the dependability of the tool's outputs without resorting to alternative approaches.

If the source is available, it does not necessarily imply that the results are reliable, but it does allow for an evaluation of the source code. It is essential to measure precision (the accuracy with which artifacts are located) and recall (how many relevant artifacts are included in the results). A cryptographic hash function is a non-reversible mathematical function that accepts any quantity of data as input and produces a string of defined length. High precision is frequently accompanied by a large number of false negatives, resulting in a low recall. Some hash function flaws have an effect on the credibility of the evidence.

It is essential, while performing reverse engineering on file systems, to explain the scope of the reverse engineering (analysis scope). The size of a file may influence how metadata is structured, and the selection of features may influence the dependability of the findings. This is especially significant if the researcher is evaluating file system topologies using a machine learning technique. There are no agreed-upon ideal competency requirements for a researcher to undertake forensic analysis, but it is essential to describe how the paper/method was examined and the topic expertise of the reviewers. Even if the tool validation and method peer-review were performed correctly, there is no assurance that the examiner will use them properly or that the results would be trustworthy.

The authors evaluated research publications on file system reverse engineering for digital forensics. Important validation criteria, which they explored and defended as a baseline necessity for documentation, are not described in the selected publications and prevalent practices. Quality and amount of data sets for testing and calculating error rates are typical obstacles. The authors proposed a fresh model for validation that takes into account technological, methodological, and application viewpoints. The proposed validation methodology is also applicable to the interpretation of apps that store their own metadata structures. Such a template has simply the bare minimal documentation requirements; expanded versions can be built by additional research. Future efforts can be devoted to establishing an autonomous EU agency specializing in digital forensics tools and techniques.

5.11. Encryption decryption

Decrypting malicious communications offers opportunities to discover useful information. MemDecrypt implements a novel approach to decrypting SSH traffic by analyzing target memory extracts. Mechanisms to discover cryptographic artifacts in memory in a manner that allows the target device to continue to operate normally while remaining undetectable is of particular interest. In MemDecrypt, memory can be extracted at any stage after the handshake completes to decrypt a captured network session.

There is no published research into finding cryptographic artifacts in Android smartphone and IOT device memory, but desktop and server memory has been studied. Entropy measures have frequently been used as a filtering mechanism to discover keys. Keys were discovered in Linux client virtual machine sessions by searching for bit strings where the counts of 0's and 1's suggested randomness. The MemDecrypt framework decrypts entire sessions for both the SSH and TLS protocols where different encryption algorithms have been applied for Windows clients and Linux servers. Memory extractions are independent of message type and discovery of candidate initialization vectors drives the decryption process. Encryption keys can be discovered by intercepting encryption function calls to extract parameters. This approach may not be effective against malicious insiders, especially when the target device runs Windows.

5.11.1. Encryption algorithms

Encryption algorithms for secure communications are asymmetric or symmetric. For encryption and decryption, asymmetric algorithms use different keys whereas symmetric operations use the same keys. Asymmetric algorithms attain security through complexity, which takes processor time, making them considerably less CPU efficient than symmetric algorithms. Although the Advanced Encryption Standard (AES) block algorithm may be the gold standard, vulnerability and performance concerns have led to the adoption of ChaCha20 stream algorithm with Poly-1305 authentication. It performs 20 rounds of mathematical operations starting from a base structure consisting of a constant string of 16 bytes, a generated 32-byte key, a 4-byte counter, and a 12-byte IV. After successful authentication, a file transfer requires the establishment of a secure channel to support the secure file transfer protocol. Secure file transfer (SFTP) is an SSH sub-system particularly worthy for investigation as significant potential exists for it to transfer confidential files out of a system.

5.11.2. Memory access

Memory acquisition tools assist forensic analysis. Android smartphone volatile memory is accessible. As Androids run Linux, memory acquisition tools such as the Linux Memory Extractor ('LiME) application may suffice. LiME depends on compiled kernel modules for the target's Linux version, support by the smartphone and kernel level execution. AMExtractor requires kernel execution privilege but no compilation is required and so is potentially less restrictive. IoT device memory may also be acquired by flashing memory, running Linux dump commands, or accessing device circuitry.

5.11.3. Android

Consumers use smartphone backups to safeguard personal data such as contact information, text messages, call logs, and calendars on external storage devices such as USB drives, SD cards, and personal computers. In investigations, backup data can supply investigators with crucial evidence for resolving events. The researchers offer a methodology for the efficient analysis and decryption of encrypted backup data that can be broadly used to a variety of smartphone backup solutions on Android platforms. The most frequent method for smartphone backup is to connect the device to a computer through USB. Each component file can be kept in ordinary, compressed, or encrypted form, and backup data have a manufacturer-specific file structure [110].

The researchers were able to identify every encryption mechanism used by Samsung cellphones' basic and security backups. Classifying the destination file format of data generated by each backup is the first step.

There are three sorts of target file formats: plain, encrypted, and compressed. Determining the encryption location of backup files beforehand enables the execution of reverse engineering more efficiently.

Key Derivation Functions (KDFs) commonly use hash functions such as the MD5 and SHA series to produce the encryption key. Except for user-supplied information such as a PIN or password, parameters typically have set values within the source code or backup data. A fixed value is a value obtained once the backup has been completed. To decrypt backup files generated by a secure backup, it is necessary to recover the security key. Except for the secret, parameters typically have known values that are contained in the backup data or are hardcoded in the source code.

A known-plaintext attack with an authenticator that can validate the proper secret is one approach for recovering the secret. A hidden feature is discovered that can be used to enter developer mode and extract additional info. The analysis is based on substantial computing capacity, which enables recovery of a secret at a significantly faster rate than with a single computer. During the backup procedure, the USB packets were examined to discover where the encrypted data are located. During the Samsung smartphone backup procedure, files were encrypted using one of the following six encryption methods: AES, AES-GCM, AES-256, AES-256-GCM.

Using the value corresponding to the EncodedCode that is generated only when the SecurityLevel is Level 3, the authenticator can be calculated. After generating the encryption key using the assumed PIN, the encrypted file can be decrypted and its signature used as the authenticator. A Samsung SmartSwitch Mobile secret feature was discovered using reverse engineering.

5.11.4. Samsung smartphone backups

Smartphone manufacturers provide backup programs for user data in the event of device loss, theft, or malfunction. Backup files contain smartphone-related user information, which can be used as an analysis target in digital forensic investigations. In this study, the authors investigate backup data from Samsung, the smartphone manufacturer with the biggest global market share [111].

Samsung's Smart Switch backup application is available in both PC and mobile formats. The mobile Smart Switch allows two Samsung Android handsets to exchange data. Additionally, it allows for the backup of smartphone data to SD card and PC. Users can select which data to back up partially, and previously backed-up data can be restored. In both the Windows and Mac environments, a backup folder is created with the selected backup item's name when selecting backup items.

Users can enable the "encrypt backup data" capability via the PC Smart Switch settings using a PIN. The data created during a backup is identical regardless of whether "encrypt backup data" is enabled. There are discrepancies between the backupHistoryInfo.xml, ReqItemsInfo.json, and SmartSwitchBackup.json files' internal contents. In a simple backup, backup data are encrypted with a predetermined value, however in a PIN-based backup, the user enters the encryption key. This enables the determination of whether a PIN was used. The Smart Switch mobile application and PC program were reverse engineered to reveal the backup data processing. Android, Windows, and macOS Smart Switch applications were analysed using both static and dynamic analysis to conduct an efficient analysis. Each tool makes it simple to view the various import/export APIs used by a running APK or PC application.

The memory and register values used in the encryption process were collected. This allowed determination of the exact encryption parameters employed. The Smart Switch was encrypting the backup data when it was utilizing the static analysis-guessed functions. Each setting's associated data was stored in a zip file within the SETTINGS folder. Each setting is saved in a separate folder following the update. Seven techniques were required for file decryption and PIN verification. The most recent Smart Switch, however, discloses that backup data are encrypted using nine techniques. Eight of the nine methods studied in the most recent edition are compatible with both Windows and macOS. One of the current techniques altered the encryption/decryption variables in part.

This article examined Samsung's latest Smart Switch backup application in Windows and macOS. Smart Switch's latest version changes the backup data's format and encryption technique. The update encrypted and stored SSM DummyValue, which generated the encryption key, and compressed encrypted data. It was found that data decryption requires nine algorithms and nine techniques were used to decrypt six backup data formats. Thus, the latest Windows and macOS Smart Switch decrypted all backup data. The backup PIN was user-entered. The PIN verification method was used to measure PIN recovery time and recommend a reasonable GPU count. It was concluded that Smart Switch backup data from diverse environments can be used as a source of evidence.

5.11.5. Password cracking

Encryption—how is it dealt with? Since robust and common procedures are available to everyone, direct attacks on the encryption method are unlikely. Existing solutions, particularly for data at rest, are password-based (the encryption method used in data in transit can be totally transparent to the user). Human-chosen passwords, on average, are the weakest link in the security chain. Password cracking methods typically generate generic candidates that match the most prevalent passwords or patterns. This method is sufficient for penetration testing a system's average security. One user password could damage a system. Law enforcement targets individuals or groups. In protected content, generic password cracking methods may work better with a more specialised approach. Humans create simple passwords. Jeremy Hammond, a wanted hacker, used his cat's name as a password, a frequent approach [112].

5.11.5.1. Password analysis. A password is a string of alphanumeric and/or special characters used to authenticate a user's access to a computer system, an application, or an online service. From 27 in one online study to 191 in another, the average number of passwords that users must remember is constantly changing and varies greatly. When considering data breaches, password reuse presents one of the greatest security risks. In the first nine months of 2019, about 8 billion records were released due to multiple data breaches, potentially allowing access to numerous other services. Participants in one poll not only underestimated the enhanced security of appending symbols or digits to the end of passwords, but also frequently reused passwords or password components.

Considered to be more remembered are passwords based on significant common terms, personal information, and patterns. Users are prepared to accept more challenging authentication techniques for financial and e-mail accounts, but not for infrequently accessed web accounts. One method for enhancing the security of a service is to ensure that the user-selected password will withstand the efforts of a possible attacker. Due to the fact that passwords are written down rather than memorised, knowledge-based authentication techniques have an inherent flaw. Weak passwords are easier to remember, whereas strong ones are more likely to be written down.

According to another study, an increase in the entropy of passwords is frequently correlated with a decrease in their usability, suggesting a trade-off between these two characteristics. Training on password security helps bridge the divide between IT administrators and end users. It is best suited for gaining access to local machines and is prohibitively expensive to implement in other situations. Entropy, which has typically been used to measure the strength of a password, is insufficient when it comes to intelligence-based assaults.

Recently, new password strength meters have been created, each taking a unique method. Dropbox employs one of the most generally accepted password meters, `zxcvbn`. The meter assigns passwords to one of five classes, ranging from 0 to 4, based on numerous characteristics, including length. As long as appropriate dictionaries exist/can be developed, this change can be extended to other languages. Dictionary attacks involve evaluating potential password possibilities against a dictionary. Each entry can be evaluated following the application of modifications known as mangling rules. Modern methods rely on a machine-learning strategy that exploits the vast quantity of actual passwords chosen by humans from leaked databases. Probabilistic Context-Free Grammars (PCFG) is one such contemporary method.

5.11.5.2. Open Source Intelligence. With a more targeted strategy to breaking passwords, law enforcement may achieve greater outcomes. Open Source Intelligence (OSINT) could be a useful source of information in this regard. Before World War II, OSINT tactics appeared and were known as overt intelligence. It can be claimed that this method of obtaining information rarely delivered major revelations, but it did present a coherent picture of popular opinion. The argument against defining OSINT as intelligence is that it is not obtained through clandestine means and does not require special handling like material obtained secretly.

Intelligence services have traditionally used keyword sampling and other filtering techniques to sift through vast quantities of data. Social Media Intelligence (SOCMINT) can be used to identify and predict online threats, as well as to get insight into group dynamics and online interactions. Crowdsourcing differs from outsourcing in that it uses the contributions of a virtual population to complete particular jobs. From their computers, users from all over the world can participate in crowdsourcing activities such as CCTV monitoring and film analysis. Crowdsourcing is easily scalable from the local to the global level.

Social Network Analysis (SNA) is used by law enforcement authorities to determine the relationships between various criminal network entities. Integrating social media sources into an investigation enables law enforcement to make better informed conclusions. SNA is effective for gathering evidence, analysing interactions and online activities, generating information about criminal conduct and the patterns and links of the relevant individuals, and analysing interactions and online activities. Monitoring public or semi-public locations through private or public means enables the Law Enforcement Agency to obtain information that would otherwise be considered ephemeral and transform it into intelligence. The same may be true for internet surveillance of open sources and social media accounts where users engage in face-to-face interactions.

During the first year of the Trace an Object programme, citizens submitted 21,000 leads for 119 objects. However, the Law Enforcement Agency must create methods for handling and evaluating this information due to the overwhelming number of leads. One framework titled DFINT + OSINT, which intends to use OSINT in tandem with the previously used digital forensic intelligence. The potentially invasive character of OSINT and, in particular, SOCMINT cannot be overlooked. How law enforcement officials can collect information with regard to the privacy and confidentiality of residents requires the establishment of guidelines. Similar to traditional and digital investigations, a methodology should be followed, such as audit trail, chain of custody, etc.

5.11.6. Decrypting live SSH traffic using MemDecrypt

MemDecrypt discovers cryptographic artifacts and quickly decrypts live SSH malicious communications including the detection and interception of data exfiltration of confidential data. MemDecrypt consists of network and data collection, memory analysis, and decrypt analysis components [113].

Network and Memory Extract. In MemDecrypt unusual events trigger memory extracts. This approach is less intrusive than continuous memory monitoring. The quantity and timing of memory extraction events depend on the target device. Where memory is classifiable, the read/write memory of the encryption program is extracted for size minimization.

Memory analysis. Candidate encryption keys and initialization vectors (IVs) are identified in the memory extracts. Although largely protocol specific, there are common features. Key randomness makes it different from many other types of memory regions. Key randomness means that the sequence of bits cannot be easily predicted. The randomness of keys can be evaluated using entropy, a measure of the amount of information in a key. In contrast with IVs, keys do not generally change during a session.

Decrypt analysis. Decrypt validation uses information derived from specific encrypted fields. Candidate keys and IVs identified in memory analysis are used in decrypting network packets until a valid key and IV combination has been found. SSH encrypted data blocks are of the following format:

Packet Length (4 bytes) | Padding Length (1 byte) | Payload (variable bytes) | Padding (variable bytes) MAC.

Packet length is the sum of the padding length size, the payload, and padding fields. The minimum SSH block size is 21 bytes comprising a packet length of 4 bytes, a padding length of 1 byte, and the payload and padding which is at least one block. The probability of an incorrect decrypt producing the correct header data is 1-in-4,294,967,275.

The MemDecrypt framework is implemented on the Xen hypervisor. Xen’s small trusted computing base makes it potentially less prone to vulnerabilities than hypervisors with larger footprints. The LibVMI library for Xen enables efficient access to live memory of Windows or Linux virtual machines.

Network traffic is inspected by redirecting each packet to a local queue and analyzing protocol fields. When unusual activity is detected, the component stores the network packet and deconstructs the message. Memory is extracted for any 2 outgoing SSH messages after a New Keys message. Client and server versions, and application if available are obtained from the protocol version exchange.

Analysis approaches vary according to encryption mode and operating system. For AES-CTR, candidate IVs are discovered first. Memory blocks that change are subject to further analysis. Key segment entropies are calculated for key length segment sizes. If an entropy exceeds a threshold, the segment is compared with the equivalent segment in a later extract.

MemDecrypt decryption algorithm is based on pycrypto 2.6.1. For a correct decrypt the first four plaintext bytes are the packet length. With a valid key and IVs, MemDecrypt decrypts each block and deconstructs the SSH plaintext stream.

MemDecrypt is evaluated by running a sequence of experiments.

Experiments investigate decrypting SSH traffic encrypted with AES under different conditions. One set evaluates decrypt effectiveness for Windows 7 and Windows 10 clients. Another set evaluates the effectiveness of 128-bit, 192-bit and 256-bit keys in AES-CBC and AES-CTR modes. A fourth set uploads files in text, pdf, Excel, and execu formats between 1 KB and 500 KB.

The probability of an incorrect combination generating a packet length meeting the decryption test is 0.00000002% (1 in 4,294,967,275). MemDecrypt decrypts SSH traffic with a high degree of certainty. It can assist in the prevention of further malicious activity, perhaps by dropping packets or hijacking the session. For experiments accessing Ubuntu server memory with the default encryption algorithm, i.e. AES with 256-bit key length and CTR mode, all client and server packets are correctly decrypted.

The data collection component obtains process lists and extracts process heap from the Ubuntu virtual machine in 0.3 s. MemDecrypt performance may suffice when extracts are obtained for Windows clients or Ubuntu servers. Where the distance is known, and the program identified from the SSH version message, memory analysis and decrypt analysis components take 1 s. Multi-threading supports simultaneous analysis of multiple files and decrypts.

MemDecrypt assumes candidate AES-CTR IVs are located at the same memory locations in each extract. For entropy, less randomness makes key regions less evident but key unpredictability is an essential requirement. Testing on a Linux heap extract produced delays of less than 0.5 s.

5.11.7. AI for triage of encrypted containers

Under U.S. law, the government's prosecutorial reach is limited in accordance with constitutional and legislative provisions. The Fourth Amendment gives "the people" broad privacy rights against intrusion by the government. If AI can be leveraged to identify whether any person knowingly has child pornography in their possession at a time when they are engaged in interstate commerce, real progress can be made. The Supreme Court held that to access data stored on a suspect's phone requires a warrant, and barring exigent circumstances, not obtainable through a search-incident-to-arrest. In contrast, the Fifth Circuit's interpretation provides Fourth Amendment protections to aliens in domestic matters. This paper assumes all aliens, legal or illegal, are afforded Fourth Amendment rights against search and seizure [114].

Technology-based searches make up a narrow category in case law, which makes it difficult to discern how the Supreme Court would interpret AI. It is concluded an AI technique can be used to facilitate the automated search of a suspect's cellular device. This technique would minimize the potential for violating the suspect's privacy by only presenting investigators with evidence relevant to the search. In Carpenter v. United States, the Supreme Court distinguished "a cell phone [as] almost a 'feature of human anatomy,'" noting studies of how ingrained phones have become to the physical location.

Technology that is used to gather evidence from a device's otherwise non-publicly emitted signatures, is likely an unconstitutional warrantless search. A signature that a user's device broadcasts to the public for any agent so inclined to detect, is presumably within the purview of the Constitution. In 2016, the Supreme Court reiterated an earlier ruling, to hold, a "breath test does not implicate a significant privacy concern". Supreme Court has held, unlike the breath test, a blood test must be based on more than search-incident-to-arrest. However, the Court has conceded that some high-risk occupations may justify the use of such tests. In 1989, the Supreme Court held that "mandat[ory] blood and urine tests of [railroad] employees who are involved in certain train accidents".

The U.S. Supreme Court has held that border searches are not subject to the same degree of privacy restraint as other searches under the Fourth Amendment. The Supreme Court has held that "routine searches of the persons and effects of entrants are not subject to any requirement of reasonable suspicion, probable cause, or warrant". The Court held that on objective suspicion of alimentary canal smuggling, a customs agent is entitled to carry out a cavity search.

The U.S. Customs and Border Protection (CBP) has issued a directive on searches of electronic devices at the border. This directive governs all searches performed by and at the request of a CBP officer, on all inbound and outbound electronic devices. The CBP classifies these searches into two categories: basic and advanced. The directive does not distinguish between basic and advanced searches, and consequently, ICE Special Agents potentially could be heavy-handed in their approach. Under the directive, a device can be detained for further review either on-site or off-site "[a]t any point during the border search".

If the algorithm fails to meet the probable cause threshold, the device cannot be retained by the CBP and potentially incriminating evidence will have to be deleted. In the reading of case law from 1998 to 2018, it was possible to group evidence sufficient to give rise to probable cause for a search related to child pornography into ten categories. An affidavit could be used to find encrypted evidence sufficient to meet one of the following ten categories:. IP address, type of software used, prior convictions, training, knowledge of the affiant, and more. The U.S. Customs has the authority to stop, search, and examine a person or property introduced into the United States where there is reason to suspect there is imported merchandise contrary to law. The Stored Communications Act makes it an offence to intentionally access or exceed authorized access to stored wire or electronic communication held by service providers.

Developing an AI model capable of analyzing encrypted data containers, without the need to first decrypt the content, would be necessary. Such a model would facilitate the investigation of online child abuse materials, and should be designed to complement existing systems such as Microsoft's PhotoDNA and Child Exploitation Tracking System. The AI model could use machine learning/deep learning approaches such as deep neural fuzzy classification techniques to provide a certainty rate for similarities between contents. It is not realistic to assume that law enforcement agencies have access to all potential commercial encryption tools. However, it is plausible to build AI models capable of accurately predicting the features of the original data.

To be efficacious, the AI model would need to support both "basic search" and "advanced search" purposes. Agents could leverage the model to discover previously undiscoverable encrypted data while avoiding the intrusiveness of a person searching the device. Most AI researchers will not have legal access to the appropriate datasets (e.g., child exploitation/abuse materials). Such development would require the cooperation of researchers and the government. It is proposed to set up a private and trustworthy data sharing platform for participating law enforcement agencies. Such a platform provides data processing and model training as a service.

Anonymity of devices being searched at the border, and the technological efficacy of using AI to reduce human intrusion, improves personal privacy rather than erodes. Such a model will grow to be increasingly accurate in identifying child abuse materials and respective to the sample size of materials. In its evolution, the AI model will "train" by incorporating new combinations of encryption schemas into its selection criteria. The more agencies that use it, the more efficiently and effectively it will run.

5.12. Anti-forensics

One question that courts will consider when assessing the weight to be assigned to digital evidence is its authenticity. Digital evidence that has been modified or subject to tampering might compromise its interpretation. The court will be interested in understanding what steps have been taken to provide assurance to the court that all of the evidence has been assessed and what steps have been taken to authenticate the evidence. If evidence has been modified or manipulated, it can lead to false interpretation and false conclusions that are put before the court. A simple example would be that a specific entry is found in the browser history that suggests the user has visited a certain website. However, the user might not have visited that website and the browser had been manipulated by the planting of evidence to mislead the investigation. There exists a common perception that digital evidence can be more easily tampered with and compromised than can physical evidence and that the manipulation can be harder to detect than with physical evidence.

In order to address the courts' concerns, the digital evidence examiner must assess the plausibility of evidence tampering. An assessment usually follows a pathway of reasoning: if there are no clear signs of reasoning, the effort of tampering is high and absent of any identified motivation nor competence for manipulation, then it is unlikely that the evidence has been subject to tampering [115]. Past studies in this area had found that to correctly identify untampered evidence took longer than to identify evidence that had been tampered with.

Due to the numerous crimes related with data breaches and data loss, data in the twenty-first century has become a symbol of controversy. When they are no longer necessary, stolen, or lost, the vast majority of physical drives used to hold corporate or personal data are often sold. With the 'rapid' format of drives, if the hard disc is used, data is not destroyed because formatting just reinitializes the drive's file system.

The belief that after a file has been erased from a recycling bin or a drive has been formatted, the data is irretrievable. When the Recycle bin or Trash folder is emptied, only pointers to the deleted data are removed by the operating system. The information remains on the hard drive until it is overwritten by another file. This misunderstanding has resulted in several data breaches and the disclosure of sensitive information to identity thieves and hackers.

'Some criminals are aware of the techniques available to law enforcement and try to hide their digital activity. The processes they use, known as anti-forensics, tend only to occur in the most complex cases'. This view was expressed recently by The Parliamentary Office of Science and Technology in the United Kingdom. Any course of action which prohibits the effective investigation of a criminal act will naturally instill concern in the digital forensic community'. The use of digital forensic tools by criminals to gain a mechanical advantage in many forms of illicit activities needs to be considered [116].

The need to increase research activity in the anti-forensic area stems from the potential for those encountering such processes within an investigation failing to fully understand the impact they have had on a device under investigation. There is limited evidence justifying concern, but this should not be grounds for overlooking the threat posed by applications and procedures designed to frustrate a digital forensic investigation.

The potential impact of under-researched anti-forensic processes is threefold:-

1. Failing to detect anti-forensic process usage on a system may prevent an effective investigation of both the local device being carried out and crucially, external sources of information.
2. Under researched anti-forensic procedures may lead to missed forensic opportunities where tools and procedures may leave behind 'digital tools marks'.
3. Under researched anti-forensic procedures provide a barrier to establishing the true capability and effectiveness of these features.

5.12.1. *Categories of concern*

5.12.1.1. Dedicated anti-forensics tools. For simplification of arguments, those tools designed for anti-forensics purposes can be typically placed in one of the following six classifications.

1. Data hiding may arguably be the weakest of the anti-forensic techniques available to a potential offender. Successful data hiding may rely upon placing content in uncommon system locations. In such cases, reliance is placed on the weakness of the investigating practitioner and their likelihood to overlook content (or through lack of knowledge).
2. Data removal techniques are designed to place target information stored on digital media beyond the powers of recovery of digital forensic techniques. Data removal involves the intentional and timely removal of data from a device's hard drive.
3. Data obfuscation is the use of algorithms and techniques to obscure data. The aim of obfuscation methods is to provide access to content only to those who have been predetermined. This may be as simple as supplying the correct authentication credentials to decrypt data.
4. Data manipulation/editing/masking take existing and meaningful data which describe a set of events on a system and change it. When undetected, erroneous examination results may be acquired.
5. Data adding refers to the removal of a user's incriminating interactions on their system.
6. Physical destruction is a traditional anti-forensics method and relies on a threshold of destruction being reached which places a device beyond the powers of specialist digital device recovery.

5.12.1.2. Disruptive technologies. The second category of processes are defined as 'disruptive technologies' - they have a primary legitimate function and purpose but may also have a detrimental impact on relevant digital data. A disk defragmentation utility, for example, is not anti-forensics but can impact the recoverability of data found in unallocated regions of a disk. This raises an issue within the context of a digital forensic examination - 'what distinguishes a malicious defrag from a normal one?'.

There are two obstacles associated with the use of disruptive technologies in digital forensic investigations:

1. Detecting that a disruptive technology has been employed in a specific instance, given that its function is authorized system activity that can be difficult to distinguish from ordinary user behavior in some instances.
2. Detecting that a disruptive technology has been employed with the goal of being anti-forensics, differentiating its use from instances such as real privacy or performance improving activities.

The second category of processes are defined as 'disruptive technologies'. Disruptive technologies have a primary legitimate function and purpose, which may also have a detrimental impact on relevant digital data on a device in any subsequent investigation. An example of such an issue would be the use of a disk defragging utility, a process of reducing file defragmentation to improve the efficiency of a system drive (Microsoft [20]). This feature is non-anti-forensics, yet its use can impact the recoverability of data found in unallocated regions of a disk. As a result, any tool or process of this type is categorised as a disruptive technology which can be used anti-forensically. The tool itself is not anti-forensics, but subject to identifying the requisite intention of a suspect, it may be used in an anti-forensics manner. This raises an issue within the context of a digital forensic examination - 'what distinguishes a malicious defrag from a normal one?'

The challenge with disruptive technology usage in a digital forensic investigation is twofold:

1. Detecting that a disruptive technology has been used in a particular instance, given their function is legitimate system activity which in some cases may be difficult to distinguish from typical user behavior.
2. Detecting that a disruptive technology has been used with the intention to be anti-forensics, distinguishing their use from instances such as genuine privacy or performance enhancing acts.

The challenge of establishing malicious disruptive technology usage is arguably impossible in many cases. The problem lies with establishing normal behaviours on a computer system - does a 'normal' user defrag their disk every week? Use private browsing functions for every session? Encrypt their devices by default? There is likely no way to distinguish such actions and doing so risks undermine the conscientious user.

Disruptive technologies can also be sub-grouped into three distinct areas for classification, notably privacy enhancing technologies, operating system functionality and device functionality. For example, passwords, encryption and wiping on an iPhone are designed for privacy enhancement and personal data protection. None of these processes are marketed for the purpose of anti-forensics by Apple.

5.12.2. *Trustworthy tools*

Forensic investigators must be armed with a methodology that enables them to evaluate any computer forensic tool for any specific scenario at the individual level [117]. Most computer forensic tools are proprietary software, they are closed source and knowledge of their implementation is unknown. Closed-box testing-principles-based methodology is the most appropriate. This methodology aligns with the Daubert guidelines, especially since many of the tools used by law enforcement are closed-source forensic tools. The tools tested included:

1. The Sleuth Kit (TSK)
2. EnCase
3. FTK
4. OSForensics

None of the computer forensic tools evaluated were able to detect secure-deletion attack. This implies that in the presence of such an attack, the evidence collected will not be complete. Wiping tools are fairly simple to use and wipe out the information by either overwriting with 0's or 1's, or with random data. Computer forensic tools can arm themselves with the knowledge of wiping patterns and footprints to identify and locate areas affected by an anti-forensic attack. Only EnCase and FTK were able to detect the cover file that contained hidden data. TSK and OSForensics failed to identify the existence of a steganographic attack. This can be primarily attributed to the lack of SAFDB database for these tools, whereas EnCase and FTK both have this feature.

Computer forensic tools are inherently flawed when it comes to dealing with anti-forensic attacks. In case of magic-number modification attack, all computer forensic tools mounted the disk images as raw, therefore failing to detect the attack. Computer forensic tools can be augmented to force mount a raw partition as any specific file system by the investigator.

This research has numerous ramifications for practitioners and academics. In the presence of file system anti-forensic attacks, such as secure-deletion, data concealment, and timestamp forgery, investigators cannot rely solely on computer forensic techniques since they may capture evidence that is insufficient and unverifiable. File system anti-forensic attacks, such as compression-bomb and sparse-file attacks, tend to use computer forensic tools against forensic operations by eliminating digital evidence located in various areas inside the file system. In the field of computer forensics, research is required to solve the problems of computer forensic tools and combat file system anti-forensic attacks.

5.12.3. Data erasing tools

The sanitization of media is of great importance to both corporate organizations and individuals. The NIST SP 800-88 Guidelines to Media Sanitization by the National Institute of Standards and Technology (2014) categorizes media into two types; Hard Copy and Electronic or Soft Copy [118]. Discarding, Clearing, Purging, and Destroying are four different types of sanitization.

The following tools were tested [119].

Hard Wipe for desktop is a popular erasing tool that has a portable version, which enables users to boot from a USB drive. The tool also has the facility for the cleaning of the recycle bin, page file, and free space. It integrates with the Windows file explorer, which allows users to right-click in order to gain access to the software.The wiped disk image, when viewed in WinHex showed a total of 80,026,361,856 bytes with every byte being 0's, including the boot sector. This outcome implied that the disk was wiped completely.

Eraser is a free, simple, and easy to use erasing tool that possesses many features. It allows the erasure of the recycle bin, unused disk space, partitions, SSDs, and electromechanical drives. The tool supports supporting a variety of erasing standards namely: British HMG IS5 (Baseline), US Army AR380-19, DOD 5220.22-M (ECE), US Air Force 5020, Canadian RCMP TSSIT OPS-II, German VSITR, and Schneier's Algorithm. The downside of the tool is its high memory usage and CPU time as compared to the other erasing tools. The Eraser tool does not allow the wiping of an active running Windows drive. It was found that the boot sector still contained 512 bytes of data, indicating that it did not wipe the FAT2 portion of the disk. There was no evidence of Images, Videos, Audio, databases, archives, or other deleted files from the image.

Macrorit Data Wiper is a data wiping software that has both free and commercial versions. It supports Windows XP, Vista, Windows Server 2003, 2008, 2012, Home Server 2011, Windows 7, 8, and 10. The tool allows users to wipe the recycle bin, partitions, external drives such as USB flash drives and memory sticks, and entire hard or Solid-State drives. Despite its advantages, Macrorit Data Wiper is unable to wipe the primary drive that has an active-running Windows OS installed. During the analysis phase, the erasing tool showed a minimal number of CPU cycles. The MD5 checksum of the wiped disk did not correspond with that of the Hardware wiped disk.

The Active KillDisk freeware version supports Windows, MacOS, and bootable media. It has its own "Disk Viewer", for analysis of specified devices, its own File Browser, and the ability to wipe both unused drive clusters and slack space in file clusters. The results from running the "tasklist/v" command showed that it uses enormous amounts of memory as compared to the other erasing tools. The results from running the "tasklist/v" command also showed an unfavorable quality in terms of its memory usage. Using WinHex, it was observed that all the sectors were zeroed, with the exception of the first 512 bytes. The disk image was imported into OSForensics' Raw Disk Viewer to confirm that all of the other sectors were 0's.

Disk Wipe claims permanent erasure of data on disk partitions and volumes. It has an attractive and easy-to-use User Interface. The tool supports seven erasing standards namely: One Pass Zero, One Pass Random, Russian GOST P50739-95 (2 passes), British HMG IS5 (3 passes), DoD 5220.22-M(E) (7 passes) and Gutmann's Algorithm (35 passes). It was observed that the run time of Disk Wipe was almost twice that of most erasing tools under review; this is due to the extra Secure Erase performed during the disk wiping process.

Puran Wipe Disk is a data sanitization tool which is produced by the Puran Software group. It supports only Windows OSs and is compatible with Windows XP, Vista, Windows Server 2003, 2008, Windows 7, 8, and 10. The tool has a very simple and presentable user interface and supports three data erasing standards. It also had a fairly low CPU Time as compared to the other erasing tools. The observation from the analysis performed on Puran Wipe Disk confirmed complete disk erasure.

Remo Drive Wipe is a Windows based erasing tool that supports both 32-bit and 64-bit versions of Windows 10, 8, 7, Vista, XP as well as Windows 2003, 2008 and 2012. It has both free and commercial licenses; both intended to completely wipe disks and logical drives. Analysis with WinHex confirmed that all sectors, including the boot sector, wiped and overwritten with 0's.

Super File Shredder is a file shredder that is used to destroy and remove files from storage devices. It is a free erasing tool that supports only the Windows OS and is compatible with Windows 2000, XP, 2003, Vista, Windows 7, 8, and 10. The tool also integrates with Windows Explorer, which allows users to right-click to gain access to the software. Autopsy recovered 2035 Orphan files from unallocated clusters, which had no data stored in them but had valid modified, accessed, and created dates. In addition to system files, Autopsy recovered four known directories, but these directories had no files in them apart from one that had one known video file. Some files, even though having a size of 0 bytes, had valid filenames and could be recovered after erasure using Super File Shredder.

5.12.4. Evidence tampering

Researchers in Germany conducted experiments to assess the effort required to manipulate images from main memory during an examination followed by a study of the effort to detect those manipulations. Previous experiments had shown that tampering with disc images, i.e. to create a forgery, is hard in comparison with detecting that same forgery in a blind experiment. In this experiment, the researchers design an experiment that is analogous to "… corrupt investigators who drop a packet of drugs where performing a search of the premises …".

Using a similar experimental approach to previous studies to investigate the tampering of disc images, it was found that tampering with memory images took almost twice the time and effort taken for tampering with disc images. Conversely, to correctly classify an original memory image to more effort than it took to classify a forgery, the opposite finding to the correct classification of original versus tampered disc images. It was concluded that tampering with memory images is hard probably due to a higher chance of detection that tampering has occurred [120].

5.12.4.1. Tampering. Many believe that digital evidence is easier to alter than physical proof. Standard procedures, such as the generation of hash values, are used to secure digital evidence. Some have also proposed securing the authenticity of digital evidence with blockchain technology. However, little research has been conducted on tampering in non-multimedia contexts [121].

The authors discuss the results of a series of experiments and interviews with digital forensics professionals regarding the manipulation of digital evidence. In addition, the authors review the various components of the experiments, assess the issues that have arisen, and draw three conclusions from them. The lessons learnt include how to ensure that an experiment can only accommodate a restricted number of participants.

Despite the fairly unfavorable conclusions about essential modifications, the performed tests have still provided a qualitative (and perhaps also subjective) understanding of what makes manipulations so challenging. It is the distinction between data and metadata. If metadata is engaged in the tampering effort, it appears that tampering is more likely to be detected via a measured inconsistency in data structures than if simply (content) data is involved. In fact, it may be impossible to create a perfect forgery once metadata is involved due to the difficulty of getting all metadata correct, as tampering often resembles a cat-and-mouse game in which a seemingly endless series of timestamps, reference pointers, or similar must be altered, each one causing another inconsistency that must be fixed. This not only calls to mind the distinctions made in multimedia forensics, but it also corresponds to the distinction between syntactical (internal) and semantical (external) consistency notions that permeate the common notions of integrity from computer security and cryptography. Understanding the nature of digital evidence tampering may be considerably closer to known methods of analyzing data integrity than anticipated.

5.12.5. Digital tool marks

The term ‘toolmark’ is a well established concept in the discipline of forensic science. The recovery of this characteristic (a form of physical evidence) can help identify the type of tool that was initially used. In forensic archaeology, toolmarks may be left in a grave, created by digging implements such as a spade or machine. In a fatal stabbing the analysis of a toolmark on the human body can determine the kind of instrument used by the suspect. In forensic science, the methods for analysing tool marks are improving and newer statistical models using Bayesian and likelihood ratios are improving validation. What is key to note is that forensic science have and continue develop and hone tool mark detection and identification techniques, benefiting investigation processes. Yet comparable advancements have not been made with regards to digital evidence [122].

When processes (either category 1 or 2) are initiated, their actions may leave behind information on a system which describes their usage for a given act. Examples include standard operating system usage files (e.g. prefetch, link files, executables), a tool specific footprint on an operating system and its tool-specific logs and file system metadata as a result of its use. These traces can be classified as digital tool marks. Digital tool marks indicate how a tool/process has been used on a system or even that a tool has been used at all. In the case of data removal a digital tool mark may reveal the location or type of data which has been subject to removal. Digital tool marks may also identify the data types which cannot be trusted as part of an investigation.

Private browsing does not completely preclude the chance of browser evidence recovery (for example, memory forensics and related memory artifacts may capture some browsed content). However, its core functionality of trying to prevent browsing session data from being locally stored on a device increases the potential for reduced evidence recovery. Even if a private browsing mode simply operates a basic file deletion protocol of notable session data files following the closure of a privacy browsing session, natural overwriting of data pose a threat to evidential recovery. Determining the frequency of a private browsing event and the length of time of its initiation may provide a greater understanding of a suspect’s usage of their device. In doing so, establishing the use of private browsing provision may also inform future forensic procedures. Take for example those subject to supervision orders requiring consistent checks of their Internet browsing history.

The term digital tool mark analysis should not be confused with that of anti-anti-forensics, which is a sub-discipline of digital forensic. Digital tool mark research focuses on reverse engineering leftover system data to determine any intended tool usage. As a discipline, it is necessary to be able to identify when an individual has taken steps to disrupt investigatory purposes. For digital forensic practitioners to harvest the value of digital tool marks it requires sustained research into both category 1 and 2 processes and the tools available.

A digital tool mark database would have to have vetted access and be a non-public resource. Identifying the default settings of a tool provides an evaluation of the threat it poses to an investigation. A data-removal tool by default simply deletes content and must be customised in order to securely erase content. Establishing the artifacts left on a system by a tool interacting with it may help to determine if a tool has been run and subsequently how it has run.

5.12.6. Private browsing

Sexual Harm Prevention Orders can be used to impose limits on Internet usage, such as requiring offenders to keep their Internet activity logs for periodic scrutiny by law authorities. A court may assess whether the imposition of an order reduces the risk of harm to the general public or to specific members of the public. It is anticipated that a Sexual Harm Prevention Order will demand the preservation of any Internet activity that can be reviewed by the proper parties. The interrogation of a defendant’s Internet history might be conducted “on-scene” at his or her residence. Due to a lack of time and technical competence, only a superficial inspection is conducted, targeting low-hanging fruit such as existing live history logs [123].

This could enhance the likelihood that breach-inducing behaviours go unnoticed, for instance if a perpetrator deletes content from their Internet browser. “Private browsing” is a widespread browser option that purports to give anonymity at the local level. Those who wish to engage in further order-violating behavior may do so by employing strategies meant to conceal their conduct. Detecting when an offender initiates a private browsing session becomes a potentially effective regulatory support technique for Sexual Harm Prevention Orders. On-site investigations are likely to target just existing browser history records, scanning and analysing this content in the absence of private browsing session content.

Due to resource constraints, practitioners on the scene may have as little as 1 h to triage and evaluate if a violation of a supervision order has occurred. Practitioners of Digital Forensics must assess on-site if an offender has violated the provisions of their Sexual Harm Prevention Order. Using a test version of Windows 10, the Edge, Chrome, and Firefox browsers were evaluated. Testing was unable to discover any operating system artifacts following a default system installation and configuration that kept session logs throughout the testing duration.

The monitoring of a system may be permissible if there is legal documentation outlining the terms and boundaries of the limits imposed on a suspect throughout the duration of device surveillance. This article examines two potential methods that might be used to detect and log private browsing sessions: the first, AppLocker, which is an integral element of the Windows 10 operating system, and the second, “PrivateSpy.” AppLocker by default configures event logs to be smaller than 1 MB in size (once full, event entries are overwritten). Additional setting is required to ensure that all events are logged. This is especially crucial for systems with high levels of activity over numerous days, where additional archiving settings may be required to preserve log data. AppLocker's most reliable method for detecting private browsing sessions is to compare event execution times to Internet history gaps.

This leaves the possibility of a user mistakenly opening and closing a browser window without browsing. One approach to potentially circumvent this is to configure all browsers on a suspicious machine to open a predetermined page upon execution. Private-Spy is a Python framework designed to monitor a system in real time in order to identify the presence of a private browsing window. It is intended to be installed by law enforcement on an offender's device at the beginning of a Sexual Harm Prevention Order and to remain on the device for the term of the order. Each computer session generates its own log, which is kept in a configurable directory.

In Chrome, both public and private tabs begin with the window label "New Tab - Google Chrome," which makes identification more difficult. Therefore, additional clarification of the Chrome browser's interface with the operating system is required to illustrate how Private-SpY differentiates between Chrome's window kinds. Private-Spy operates by continuously asking the operating system for open windows; when an event is identified, a back-end record of occurrences is updated with the browser launched in private mode and the occurrence's timestamp. When the time between 'New Tab' window creation events and cache content generation or re-access is greater than 1 s, a private browsing event trigger has occurred. This is because Chrome's caching performance means that when a standard browsing tab accesses the cache, it is often completed in less than 1 s.

5.12.7. Hiding process memory

Recent malware variants have begun to implement anti-forensic techniques to impede the ability of analysis tools to provide relevant conclusions. The authors offer three innovative memory subversion strategies for Windows and Linux that allow hiding harmful memory from forensic tools. This study presents unique strategies for concealing harmful process memory from memory forensics and live analysis. They contrast their method with related research that depends on anti-forensic strategies that undermine the memory perspective of forensic analysis tools. Downloadable from the online repository are the source codes and binary formats for all of the proof-of-concepts and plugins [124].

Shadow Walker, a new type of sophisticated rootkit that can conceal memory by bypassing the Windows operating system's translation process has been previously described. The current methodology, on the other hand, permits a number of methods to flip between malicious and benign memory, preventing analytic tools from employing a generic detection strategy. The strategies aim to modify the real memory layout of the user space of a process, as opposed to the shadow paging strategy, which incurs a considerable performance penalty.

Modern operating systems provide each process with its own transparent abstraction of the physical memory. These virtual address spaces are partitioned in multiple segments of predefined sizes, called pages. To map a virtual page to a physical frame, a processor's Memory Management Unit traverses a set of hierarchically ordered paging structures. Each virtual address space is subdivided into a kernel and user space portion. On Linux and Windows, shared memory is intended to be shared among processes (e.g. to allow the exchange of data) It is, however, also possible that a process uses shared memory without actually sharing it.

There are two distinct steps involved: Creating a shared memory segment and mapping it into a process, each realized by a specific API. On Windows and Linux, there are three types of shared memory segments - image, text and non-text - which each have a different management structure. Each of these structures describes a particular memory area, e.g., in regards to its protection and range. Both Windows and Linux manage the physical address space with special structures. On Windows, there is the Page Frame Number Database (Page Frame Number DB). Each page object contains a field called mapping (page- > u1- > mapping), pointing, if not null, either to an address_space or an anon_vma object.

Three innovative memory subversion techniques that enable the concealment of specific portions of the user space application's process memory are described. Similar to Direct Kernel Object Manipulation attacks, the first two methods change Memory Area Structures and Page Table Entries, necessitating kernel level access. The third strategy is based on the manipulation of shared memory mappings and does not necessitate elevated privileges. The remapping of address ranges should target memory locations of the same kind or modify their access rights appropriately. This may cause analytic tools to display incorrect data.

Analysts anticipate the discovery of code, for instance, when showing data within an executable portion of a process. Alternately, malware may reduce the address range of a benign region to remove its dangerous components. Page Table Entries are a component of the virtual-to-physical address space translation process. A Page Frame Number indicates the presence of a page and the location of its physical frame. This makes them an attractive target for adversaries, as changes may prevent bad data from being detected by different analytic techniques.

It is preferable to remap malicious pages that formerly contained executable code to page frames containing executable code. Structures of the same or different processes can be used as a signal for locating relevant memory regions. Page Table Entries of hidden memory portions must be restored prior to being accessed. Private memory data is lost as soon as it is unmapped, whereas shared memory data remains accessible and available as long as at least one process has a handle on it. This method does not involve Direct Kernel Object Manipulation and simply makes use of functionality accessible to non-privileged users.

It does not require elevated permissions and operates exclusively in user space. On Windows and Linux, the authors hooked the respective operating system's process termination algorithms to inform the virus to undo all modifications prior to the process' exit. It was necessary to adjust the Resident Set Size of a process to prevent inconsistencies between the updated virtual memory layout and its physical counterpart. In addition, concealed pages are no longer referenced by the kernel as a result of the Page Table Entries subversion tactics. This may prompt the kernel to reclaim and assign these pages elsewhere.

Changing the Page Frame Number on Windows might result in application and system problems. This discrepancy causes system crashes, such as when YARA is used to scan the process. To prevent page swapping methods from interfering with Page Table Entries subversion techniques, the malicious pages are locked in memory prior to their concealment.

The process of detecting the remapping of Memory Area Structures is the same for Linux and Windows. The Page Table Entries value further allows the retrieval of the corresponding memory content. Windows 10 introduced a feature called Memory combining, which attempts to save RAM. One mechanism of this feature is to turn identical private pages into shared memory in order to remove duplicates, which could interfere with this detection. Any page that belongs to the same mapping object for a Memory Area Structure, but is not referenced by any Page Table Entries of that same structure, is an indicator for subversion techniques. This approach can lead to false positives with Copy-on-Write memory, as the mapping points only to the new copy, and thus must be analysed manually.

It is possible to detect Page Table Entries Erasure on Windows with Working Set List Entries, a subset of physical memory pages used by a process. This approach allows the retrieval of the actual memory, as the Page Frame Number database index respectively the page structure offset already reveal the memory page's physical offset. All structures used for detecting the subversion techniques could also be manipulated, in order to evade the detection mechanisms.

A view on a shared memory segment can be created with different protections. For example, while the protection of a prototype Page

Table Entries indicates RWX permissions, the memory can be actually mapped as read-only in the process address space.

As a proof of concept, the researchers created two Rekall plugins (one for Windows and one for Linux) which implement the described detection methodology. In order to test the amount of false positives, several browsers (Firefox, Microsoft Edge, Chromium), Office applications (Microsoft Word, LibreOffice) were used and PDF Documents were opened in a reader.

The authors found that Rekall suffers from problems on Linux, which stops it from correctly dumping the contents of a file object, and the processing of handles on Windows. Malware attempts to conceal code that is executed by the controlling process during runtime. This harmful code comes in two varieties: shellcode and libraries.

On Linux, in-memory library loading was implemented whereas, on Windows, the focus was primarily on Shellcode, as techniques such as Reflective DLL Injection do not rely on operating system APIs to load a library. All subversion approaches fail to conceal memory from the yarascan plugin of Rekall. Several plugins are only able to display the hidden memory when Memory Area Structure Remapping is enabled. On Linux, dynamically loaded libraries were identified, which is not indicative of memory subversion.

Since all shellcode-related pages were loaded with RWX permissions, malfind reports these memory regions. None of the techniques could detect hidden System V shared memory portions. Memory Area Structure Remapping is the only method for discovering and revealing hidden memory. The process of remapping stopped WinDbg and Process Explorer from generating a process dump.

Three innovative strategies were demonstrated that effectively conceal memory from live analysis and memory forensics; plus a number of detection methods were described that, in some situations, enable an analyst to detect these subversion tactics and also reveal the buried memory. Other than the discovery of shared memory, the remaining procedures must be automated and assessed in the future. In addition to the subversion strategy for shared memory that has been discussed, mapping just a sub view of the shared memory while excluding the malicious portion could be a valid alternative and should thus be investigated.

5.12.8. *Validate digital forensic models*

Anti-forensics is one of the problems of digital forensics. By erasing evidence, anti-forensics is capable of delaying or preventing an investigation therefore this posing a threat to the inquiry process if appropriate safeguards are not implemented. The most advanced digital forensic models do not appear to account for anti-forensic methodology or techniques. To overcome this deficiency, this study proposes a framework and a validation principle for digital forensic models that enables an investigator to validate a digital forensic model by confirming anti-forensic attacks that fail the forensic process. This paper's primary contribution is the derivation of a mathematical approach for validating digital forensic models in order to validate detection and counter anti-forensic techniques. This addition is significant because it enables investigators to apply the validation principle to determine if their digital forensic models or frameworks are influenced or altered by an anti-forensic attack. Consequently, informing the investigator if their investigative model or framework is valid for performing an inquiry [125].

Only two digital forensic models in the literature contemplate incorporating anti-forensic strategies. In a prior examination of digital forensic models, none of the eleven evaluated models met all of the Daubert Standard's requirements. Additionally, it is argued that the digital forensic models did not encompass the entire breadth of the investigation. During the past ten years, distinct digital forensic models have been established for various areas of digital forensics, including digital triage, network forensics, mobile forensics, and Internet of Things (IoT) forensics.

It has been proposed to boost the effectiveness and efficiency of IoT investigations in conjunction with the Next-Best-Thing Triage (NBT) model. Diverse scholars additionally included International Organization for Standardization (ISO/IEC 27043:2015 standards into their digital forensic frameworks in an effort to improve or standardize their frameworks. Other frameworks comprising six phases to detect anti-forensics attacks in a cloud context have also been developed; however, the authors only discuss using attack graphs to detect anti-forensics attacks. This study focuses on the four most prevalent phases of the digital forensics procedure: Acquisition, Examination, Analysis, and Reporting.

Depending on the state of the machine, when an investigator wishes to obtain evidence, they would follow specific processes. Anti-forensic tactics could thwart the acquisition procedures. During memory acquisition, if the drivers used by a forensic tool depend on the 'KDBG' string to resolve symbols, this method may cause an interruption. In addition, if the undocumented memory enumeration application peripheral interface (API) and memory mapping API such as MmGetPhysicalMemoryRanges () and MmMapMemoryDumpMdl () are updated to return a NULL value, a modified version of the memory map would be returned.

Other methods of hiding a file to avoid investigation include manipulating specific registry keys, hiding data in the HPA and DCO regions of the hard drive, and even employing bootable USBs or DVDs. Using a system service dispatch table (SSDT) hook that can change a process and thread list, the same rootkit can also circumvent memory analysis. In addition, the encryption of certain data with robust passphrases will occupy a substantial amount of investigative time. Using steganography techniques to conceal a file within another file may cause an investigator to overlook some crucial files.

5.12.8.1. Abstraction, validation and evaluation. The investigation of digital crime involves a series of steps. This procedure may be led by a SOP or a digital forensic model. Methods and forensic instruments must be validated in order to preserve the integrity of evidence. In the United States (US), the National Institute of Standards and Technology (NIST) oversees this part of digital forensics research. As noted on their project website, the Forensic Science Regulator (FSR) has produced advice on method validation in digital forensics, FSR-G-218.

In the United States, an investigator's method or practice must follow to the Daubert Standard, which establishes a set of objective principles for determining the admissibility of scientific evidence in court. Beginning in October 2017, in the United Kingdom, all providers of digital forensic services to the criminal court system must be ISO-17025-accredited. Risk assessment must be performed prior to validation testing, per FSR-G-218. Digital Forensic Investigators frequently prepare forensic reports using forensic software tools. It has been shown that an anti-forensic strategy targets a forensic tool in order to generate misleading reports.

This can constitute a threat to the investigation in terms of the trustworthiness of evidence, which is particularly noted in Criminal Practice Direction 19A.6. The majority of digital forensic models in section 2 or the FSR-G-218 technique validation guidance for digital forensics do not address anti-forensic concerns. For the validation of a digital forensic model, each phase must be validated before moving on to the next phase. To define this procedure mathematically, specific definitions and axioms are first presented, followed by the proof of assertions. Anti-forensic attacks must be accounted for in all phases of a digital forensic model, according to the validation principle.

This is accomplished with the help of the mathematically formalized elements: the logical detector product, which indicates an anti-forensics approach can be detected; and the counter tensor product, which, along with the logical detector product, reveals if an anti-forensic product is countered. The pass function informs the investigator whether the phase has been validated, allowing the procedure to advance to the subsequent step. The implementation of this theory is illustrated using a hypothetical scenario in which a defendant is accused of launching a DDoS assault against the network of an organization using their laptop. It is assumed that the investigator adheres to a Standard Operating Procedure and applies the validation test principle to the digital forensic model of collection, examination, analysis and reporting are the steps involved.

In the example, the collecting phase is validated because the Proposition is met, and the investigator can move on to the examination step. This is a hypothetical model of the digital forensics process, which consists of four steps, with anti-forensic techniques being recognized and countered only in the third phase. This four-phase digital forensic paradigm can be considered validated.

In this article, the authors suggest a fresh validation concept for existing Digital Forensic Models. This approach can be used to identify or eliminate any risks posed by anti-forensic procedures prior to an investigation. This will be valuable for anyone creating a validation strategy or report in accordance with FSR-G-218, which is governed by Forensic Science Regulator and stipulates that all risks must be addressed prior to validating a method. Also, if the rebuttal presumption of correct operation of computers rule is used claiming anti-forensics as the reason, the validation principle could be used to prove or disprove the rationale for invoking that rule, i.e., whether that rule applies to a particular situation or not. The validation concept resides on the more abstract level. This is because the validation principle can only validate a digital forensic model if it is familiar with an anti-forensic technique beforehand. It cannot forecast new anti-forensic techniques, such as zero-day attacks, if they are not contained in the database.

5.12.9. Game theory

Anti-forensic techniques aim to disrupt forensic investigations or digital evidence. Rootkits employ diverse concealment techniques to influence forensic incident response and network monitoring. Undiscovered system vulnerabilities allow attackers to install and execute malicious malware on affected systems. This study focuses on rootkits, which an attacker employs as an offensive tool and an investigator uses as a defensive one [126].

The study determines the Nash Equilibrium of the game, which enables the investigator to defend against rootkit attacks. The proposed concept is advantageous for the industrial market. Presenting a classification of rootkit detection strategies enables investigators to select the most appropriate method. Examining system files for rootkit fingerprints, various strategies can be classified.

The researchers simulate the interactions between a rootkit-using attacker and a rootkit-using investigator. The existence of the Nash equilibrium for this game is examined and the most desirable and stable defensive methods for the investigator are determined. In Fictitious Play, players assume that the distribution of their opponents' strategies is unknown and stationary. The properties of rootkits and anti-rootkits are used to illustrate the nature of the players' strategies. The components comprise selecting the player's most desirable and consistent reaction to the opponent's strategies and updating the empirical frequency of their opponents' plans.

'Evidence' displays the quantity of malicious traces found by an anti-rootkit, while 'Detected name' displays the rootkit's title. The second function is a cost function that approximates the cost of deploying a rootkit or anti-rootkit. Actions with a greater number of attributes incur a greater implementation cost. If the attacker wants a more potent rootkit, he or she must pay a higher price to install additional malicious traits. This may involve recruiting developers in addition to evaluating the implemented rootkit.

The game is demonstrated to be convergent. The first Nash equilibrium indicates that one particular approach is the most desirable and stable for the attacker. It is demonstrated that the investigator was less interested (0.10) in playing 'Malwarebytes Anti-Rootkit Beta'. The Nash Equilibria allow the relationship between rootkit and anti-rootkit properties to be demonstrated. The game allows the investigator to discover her/his most desired defensive techniques against the most desired and stable offensive strategies of the attacker. Using these interactions, investigators can analyze the effectiveness of the internal components of anti-Rootkits. The detection based on file and file hiding are shared properties of anti-rootkits.

Experiments revealed the investigator's most successful protective tactics against the attacker. In addition, the studies uncovered the most malicious techniques the attacker may use against the investigator. A set of relationships were defined between the characteristics of rootkits and anti-rootkits using the game's Nash Equilibria. One of the correlations revealed, for instance, that 'Malwarebytes Anti-Rootkit' and 'Rootkit-Buster-Trend Micro' need enhancements for identifying file-based operations.

5.12.9.1. Game theory research challenges. Digital forensics focuses on the veracity of digital artifacts in order to combat the proliferation of digital frauds. However, anti-forensic strategies have a negative impact on the integrity of computer forensic evidence. Anti-forensics necessitate a more in-depth and exhaustive study to acquire more solid evidence, as well as mitigating strategies. In this research, a game-theoretic approach is presented for simulating the interactions between the attacker and the forensic investigator. Each player has an action space for each anti-forensics currently in play (i.e. anti-rootkits). An evaluation determines which algorithm is the most effective model or algorithm for simulating the interactions of participants in a forensic scenario. The simulation results reveal the most desired and stable strategies of the attacker as well as the investigator's preferred strategies [127].

The authors propose a taxonomy on conduct of anti-forensics and discuss each item of the taxonomy. Memory, hard drive, and video forensics are reviewed along with modification and distortion tactics, data hiding techniques, suppression of evidence discovery and rising complexity of forensic analysis. Data concealing is a major aspect of anti-forensic technologies, as is steganography, encryption, and wiping technologies enable attackers to hide evidence.

There are a variety of technologies that apply concealment strategies in varied fields of digital forensics such as image forensics, hard disk drive forensics or video forensics. Commercial anti-forensic tools remove evidence, hindering digital forensics. The fingerprints of wiping tools include installation directories, registry keys, prefetch files, etc. "IconCache.db" files have been previously tested for usability and anti-forensics, while other researchers have established a categorization on 308 collected anti-Forensic tools.

Anti-forensics now targets network security, which requires additional attention. Encryption prevents file access without a key and the structure of encrypted files help detect these nefarious methods. Anti-forensics are capable of lowering the efficiency of digital forensic techniques, for instance, they can obstruct forensic analysis employing an incremental impact on the necessary time. Depending on operating system restrictions, mobile third-party apps can be anti-forensic. Other researchers have proposed a framework that enable investigators to examine a user's browsing successfully. Forensic image, audio, and video detection methods can identify alteration, media origin, and operation history on a digital multimedia artifact. Image forensic techniques detect tampering and identify image sources.

The investigator can evaluate anti-forensics by simulating attacker-investigator interactions in a forensic context. Game-theoretic models and algorithms can simulate interactions. Game theory must first identify forensic players' interactions as all players know their opponents' past strategies in a perfect-information game.

A normal-form game uses a matrix representation to illustrate tactics and payoffs of a game. Payoff functions separate matrix games into collaborative and competitive games. An equilibrium represents a player's methods that can be applied regarding the maximization of the payoff. The equilibria in a game identify the players' optimum strategies. They adapt to an opponent-dependent interaction dynamic structure. The authors identify the most coordinated game-theoretic model or algorithm for the forensic context. The capability of game theory to meet the issues of security domains is proved. Security researchers employed game-theoretical methodologies to uncover rational attackers' expected behaviours and defenders' optimal strategy in the intrusion detection challenge.

The authors analyze a two-player security game between an attacker and a defender utilizing fictional play algorithm and Stochastic game theory. Evolutionary game theory changed populations over individuals and replaced rationality with evolutionary stability. Previous researchers have employed Markov game theory to simulate the risk assessment by an assumption that the prospective future risk impacts an appraisal of present danger.

The researchers selected the four most related game-theoretic models and methods as 1) the fictional play algorithm; 2) the gradient play algorithm, 3) the Bayesian game theory, and 4) the evolutionary game theory. They then assessed the simulation results to select the most coordinated model or algorithm for the modelling of the players' interactions. Evolutionary Game Theory predicts animal behavior using non-cooperative game theory.

Experiments indicate that the fictitious play algorithm reached equilibrium and the game's steady state at iteration 1750. The approach required 8.65E-4 ms for each iteration to model the game and consumed 2.9 bytes per iteration (5.8 KB). The algorithm is both feasible and scalable. It does not, however, guarantee Profitability, as the investigator's compensation is negative.

The Bayesian game has not reached its stable states and the game did not converged. The algorithm is compatible with Targeted Optimality, but not Auto-Compatibility.

The gradient play algorithm, like the fictitious play algorithm, provides Safety and Robustness. Each cycle of the method requires 9.50E-4 ms to execute (950 E−4 s per 100 iterations). The outcomes of the experiments are encouraging for the forensics community. At the conclusion of the game, the results demonstrate how the investigator can determine the most stable and desired protective tactics against the rootkit threat.

The investigator may use a comparable methodology to examine existing counter-anti-forensics in several fields, such as smartphone forensics, network forensics, etc. The proposed method replicated the interactions between the perpetrator and investigator (in a realistic forensic-based environment). The simulation of the interactions in the forensic environment could determine the game's Nash equilibrium (the examined equilibrium of a Bayesian game).

The imaginary play method was used to determine the best stable and preferred strategies for the player. Gradient play provided a substantial amount of the criteria that guarantee a full representation of player interactions in the forensic setting. The examination also yielded encouraging results for the forensics community, which have applications such as comprehending the attacker's behavior and enhancing existing anti-rootkits.

6. Devices and systems

6.1. Cloud forensics

Cloud computing is now revolutionizing the way individuals create, access, and store digital content. The 'Cloud' (a term often used to encapsulate all cloud technology service variants) is multifaceted with options available to the user which range from simple storage facilities, to access to specialist software and hardware platforms. One of the many benefits offered by cloud service providers is the ability for users to store their digital content within a Cloud infrastructure, which has even seen law enforcement use such platforms to store large quantities of video footage generated as part of their investigations. Cloud storage provides an alternative and popular option for robust and secure storage of personal data. While cloud storage maintains many clear benefits for the user, such platforms are abused.

The storage, processing, and transmission of digital data have been transformed by cloud computing. How to undertake digital forensics in multiple cloud computing systems is one of the most intimidating new obstacles. Work in the future will involve identifying technological and normative gaps in relation to the issues that must be addressed. Cloud forensics is the examination and interpretation of digital objects retrieved from a cloud environment that, until now, have relied upon digital forensics methods for which multiple process models have been built. To perform a search and/or seizure of data, legal permission is necessary. To ensure dependability and accuracy, forensics tools must undergo validation. Technical, legal, and organizational obstacles comprise the majority of cloud computing forensic issues. These obstacles arise when identification and acquisition tasks are hindered or when an examiner's examination and interpretation are obstructed. The inability to obtain system and network logs, multi-tenancy, and quick elasticity, which are distinctive characteristics of cloud computing, offer novel circumstances to digital investigations [128].

Companies have adopted cloud computing systems because to the increased need to cut service costs, the integration of services between non-portable and portable devices, and the ever-increasing demand for storage and computational capacity. The volume of the processing procedure is shifted to the cloud, making it important to develop forensic analysis techniques as well as address the open challenges/ limitations of forensics in this new setting.

In the era of Big Data, Virtualization, and Cloud Computing, the amount of data kept is disproportionately huge compared to its transport rate. Acquisition is the most important step in a digital evidence investigation since it provides the subject on which forensic analysis will be performed. The volume of data imposes time, cost, and validity constraints.

Cybercriminals enjoy the same advantages of cloud computing as legitimate firms. Malicious users can take use of higher computer power, expanded capacity, energy and cost savings, anonymity, and elasticity, hence enhancing their capabilities and objectives. It is now easier than ever to create and use botnets, data-mining, crypto-mining, and Command-and-Control centers. In addition to criminals' tools, though, their range of targets has expanded dramatically. Once a consumer decides to use cloud services, he/she must realize that his/her data are no longer exclusively accessible to him/her or in a certain location. When the Internet of Things/Internet of Anything aspect is added, where each device can connect and communicate with a network – typically using cloud infrastructure – both the number of targets and the complexity of assaults increase exponentially.

The lack of forensic analysis tools and methods, along with unresolved concerns, is a crucial factor in cybercriminal use of the cloud. Criminals do not even require anti-forensics if they use infrastructure outside the judicial and administrative authority of the authorities as a foundation for any harmful energy.

The log files of a system are essential for debugging and monitoring its operation and status. During a forensic investigation, these files may include pertinent information regarding the occurrence under investigation. They are one of the most important "witnesses" of what occurred in a system at a certain period.

As a cross-discipline of cloud computing and digital forensics, e-discovery, collecting, and analysis of digital evidence in cloud environments differ from in-home/corporate computer systems. The distinction resides in the absence of instruments and methods, as well as the potential geographical dispersion of the investigated system. Non-physical access to a system necessitates the provision of certain technical and legal requirements for remote access. At this time, concerns have been expressed regarding the integrity of data.

In cloud setups with voluminous log file entries, it may be difficult to discover important information. In addition, cloud-related difficulties like as fragmentation, geographical dispersion, and varying implementations make it challenging to identify meaningful information.

6.1.1. Cloud general survey

6.1.1.1. Incident-driven cloud forensics. Continuous cloud forensics includes the evaluation of forensic capabilities for an organization's cloud infrastructure. It is pivotal that forensically friendly cloud services are in place for continuous evidence collection, aggregation, and storage (coined as "forensic-by-design"). There has been ongoing work in ensuring forensic competence in cloud infrastructure, as evidenced by existing literature. There has been focus on designing secure log capturing or storage mechanisms, given the importance of logs in digital forensics and digital investigations. A forensic toolkit called FROST was developed which focuses on evidenced acquisition for virtual disks, Application Program Interface logs, and guest firewall logs. Other researchers focused on collecting relevant information from Virtual Machine files for regenerating events and further analysis [129].

6.1.1.2. Provider-driven cloud forensics. Cloud Service Providers host and control the underlying hardware infrastructure upon which consumer's application and data reside. Service models affect degree of control over a working environment and play an important role in forensics as well. Logging is a continuous activity that documents every event of the system, including both hardware and software components in a set of files referred to as log files. In cloud forensics, confidentiality and integrity of all generated logs are crucial to ensure reliable investigations. A number of authors have discussed the security aspects and forensic soundness of different logs in the cloud computing environment.

One approach is a forensic-enabled cloud architecture to monitor different activities in a cloud environment. A cloud forensic module gathers all the forensic evidence including logs from virtual machines by interacting with the underlying hypervisor. A number of authors have highlighted the importance of forensic-enabled cloud and the need for a separate module that collects forensic evidence. In the cloud, identification and collection of data is not a trivial task due to virtualization, data distribution, and replication. Log-correlation is a major consideration in cloud log analysis, although this may not be widely considered in existing works.

Proactive measurements are attempts to extract information in a non-malicious manner. Some authors have proposed infecting each virtual instance with a bot agent, whereas others have proposed a system model comprising of a forensic centre and forensic query server. Botnet-as-a-Service may be questioned in a court of law, due to the use of bot malware to compromise the suspect's or target's machine.

6.1.1.3. Consumer-drive cloud forensics. It is generally acknowledged that the Cloud Service Provider plays a crucial role in cloud forensics. Forensic investigators have to collaborate with Cloud Service Providers during the collection of evidence. The authors note that solutions between this category and storage forensics overlap as they focus on forensic artifacts on an end-user machine with physical access.

One procedure is described for the digital investigation of cloud storage applications with identification of potential artifacts on desktops and mobile phones. Another author identified remnants residing on client desktop utilizing Amazon Cloud Drive during upload, download, and delete operations. Other authors noted the forensic importance of circumventing the default and built-in SSL/TSL validations on iOS devices. A major challenge in this category is the need for physical access to the user devices. To bypass built-in validations, the authors proposed five methods (i.e., certificate common name field modification, insertion of proxy CA certificate in-app bundle of root CAs, SSL Kill Switch tool, and app binary tempering at runtime). They also listed the time difference for both the processes with a much shorter time frame for DRbSI.

A distinct server for evidence collection is a novel idea and solves many issues, including distributed evidence. Another approach involves a Forensic Monitoring Plane, placed between a consumer and a provider and a Forensic Server. Investigators could directly access the server using user credentials and acquire the evidence.

Software Application Program Interfaces are becoming a de facto standard for organizations to deliver their product and services to their consumers. FROST is reliant on trust in the underlying cloud infrastructure and does not consider insider threats, including a malicious Cloud Service Provider. Both Forensic Monitoring Plane and forensic server are vulnerable to various attacks, including Man-in-the-Middle and eavesdropping due to the placement.

6.1.1.4. Resource-drive cloud forensics. In the cloud, "compute" does not refer to the bare physical hardware, rather virtual hardware in the form of virtual machines. Multi-tenancy, data distribution, and redundancy are features of a cloud, however these features become challenges for the forensics. Resource driven forensics can be defined into three parts. One part focuses on software defined networking (software-defined networking) forensics; the second part is storage forensics with client-side artifacts; and the third part is focused on Virtual Machine forensics including Virtual Machine introspection, and Virtual Machine snapshot. Virtual Machine snapshot is a process of preserving the state and data of a virtual machine for later analysis.

Several models have been proposed for resource-driven cloud forensics including:

- examination of snapshot files without altering its original content
- leveraging the conventional intrusion detection system to identify the malicious Virtual Machine
- continuous snapshots of the complete cloud environment using Virtual Machine snapshot servers.

Live analysis overcomes the shortcomings of traditional static analysis that fails to gather volatile and continuously changing information, including process list, memory contents, open ports, and connections. Live analysis in a cloud environment is possible due to remote accessibility feature and also it does not require any shutdown of Virtual Machines. This category includes Virtual Machine isolation, Virtual Machine Introspection, and forensic hypervisor. Virtual Machine Introspection is an introspection technique to monitor the run time state of a virtual machine at the hypervisor level outside the monitored Virtual Machine. Independent agencies can acquire the runtime state information of a particular Virtual Machine such as process list and socket connections by creating a secure connection through transmission component, and save the information in a storage component using NoSQL database. A hypervisor is the middleware component that allows abstraction to host multiple virtual machines isolated from one another while sharing physical resources. Traditional hypervisors have a huge code base that make them vulnerable to various exploits and can have severe security and forensic implications.

Other authors proposed a new hypervisor, referred as ForenVisor, to address reliability and security concerns. Artifacts are the snippets of data left behind due to the interactions between the storage users such as client applications and storage services. These artifacts may comprise log files, registry entries, meta-data information, and many others, residing either on the client-side or server-side. Some authors noted the possibility of a criminal investigation involving cloud storage despite inaccessibility to the cloud servers.

When examining devices for artifacts, some researchers have identified and generated a forensic copy of memory, disk, network artifacts, logs, uploading, downloading, deletion and sharing on user devices that include Windows 8.1, iPhone 5S and Android using conventional digital forensics tools related to cloud services. Other researchers have identified artifacts related to memory and storage from the usage of BitTorrent Sync's client and web applications. A "forensic-by-design" model which is an integrated cloud incident handling approach was evaluated with multiple cloud applications such as Google Drive, Dropbox, and

OneDrive.

Data provenance refers to the documentation of all the activities and entities that influence the data over its lifetime. Provenance is a crucial aspect as it provides a view to the sequence of developments regarding a particular data object. Several contributions discussed the significance of the data provenance in general, and also in the context of forensics. Some authors identified a set of challenges based on the architectural complexity of the cloud noting the importance of securing the provenance information, especially if the stored data is sensitive, for example, health records of patients. One proposed provenance scheme uses bilinear pairings comprising five algorithms.

In-cloud forensics covers forensic investigation of various components inside the cloud provider infrastructure. The scope of in-cloud forensics varies from a single data centre network to the network of multiple data centers, dispersed geographically and connected through high-speed WANs.

There are significant differences between traditional network forensics and software defined networking with parameters including network device, forensic approach, and traceback. One proposed forensic framework comprises six components, including data acquisition, extraction, fusion, anomaly detection, security alarm, and evidence conservation.

A major shortcoming of past cloud forensics solutions is their theoretical conceptual design without any practical implementation, for example, one proposed solution was based on assumptions of security of the software defined networking architecture by placing the trust on both the network devices and controller.

6.1.1.5. Forensic tools. The US National Institute of Standards and Testing prepared a catalog of various digital forensics tools and their functionalities. Digital Forensic Framework is an open source tool for a forensic investigation that comprises identification, collection, and preservation of evidence artifacts. Encase comprises a complete investigation life-cycle. AccessData Forensic ToolKit is an entire suite of investigative tools to conduct digital investigations. The FROST tool set includes tools for the trustworthy forensic acquisition of virtual disks, Application Program Interface logs, and guest firewall logs.

VNsnap is a snapshot tool for virtual network infrastructures. LINEA is a live network evidence acquisition tool for the World Wide Web services with the assumption of availability of Trusted Third Party. In the cloud, log forensics is fundamental and part of a number of forensic solutions. There should be metrics such as "analysis time" and "effort to evaluate" for comparison. In the case of live analysis, it is crucial that system should generate quick alerts with minimum false positives.

6.1.1.6. Guidelines for cloud forensics. Investigators are confronted with multiple issues during forensic investigations in a cloud environment. Virtual machines provide a rich source of artifacts to investigators as it has a complete operating system and all the related services. Service owners have access to all these artifacts, so there is a dependency on the owners. In the scenario of non-cooperative service owner, where forensic investigators rely upon Cloud Service Providers to acquire the artifacts, it may hamper time-sensitive and real-time criminal investigations. Cloud Service Providers' infrastructure spans to tens of data centers comprising hundreds of devices including compute, storage, and network devices. Logs associated with various storage management software may aid the investigators with access information of various storage devices. Forensic investigators must acquire these artifacts from the Cloud Service Provider. Forensic examiners should place emphasis on the need for live analysis for the cloud environment.

The authors believe researchers must evaluate security information and event management solutions for the post-incident forensics in the cloud environment. Log aggregation and correlation is crucial; however, it is not a trivial task due to different types and formats of logs with different and incompatible structures. The authors believe it is time Cloud Service Providers develop strategies to provide forensic capabilities to the investigators, which may be in the form of "forensic-as-a-service". Cloud Service Providers' must focus on security mechanisms for the artifacts that are even "Cloud Service Provider proof".

Table 1
Tested note and journal apps.

Android	iOS	Android and iOS
Basicnote	Day One Journal: Private Diary	Daybook
Blacknote	DayMore	Moment Diary
Classic Notes Lite	Dairy With Password	SomNote
DailyLife	memono Notepad	Sticky Notes + Widget
Diary	MyToday Lite	Never Memo
Diary with lock	Memo Notes	Diaro
Life	Notepad+	
MemoG	N + notes	
My Secret Diary with Lock and Photo	Private Notes and Secret Diary	
Notepad	Secure Notepad – Private Notes	
Notepad Free	Sticky Notes	
Notepad Notes	Breeze	
Notes	MemoKing	
Private DIARY Free – Personal Journal	Diarium	
Private Notepad	Notebook – Take Notes, Sync	
Sticky Notes!	Simplenote	
Universum-Diary, Journal, Notes	Simple Notes – Notepad Folder	
WeNote	Notebook Diary, Journal	
MyNotes	Standard Notes	
Notes		
Simplenote		
NOTEBOOK		
Fast Notepad		
My Diary (fray)		
Private Notepad – safe notes & lists		

Privacy and evidence isolation are points of concern owing to a multi-tenant environment of a cloud and overlapping of memory and storage regions. Trusted computing addresses the problem of evidence integrity and authenticity (see Table 1).

6.1.2. NIST cloud computing forensic challenges

The National Institute of Standards and Technology sought to identify the major challenges in conducting digital forensics where the evidence resides in a cloud computing environment. The long-term objectives are to identify technology and standards gaps related to the challenges that need to be addressed and develop possible technological and standards approaches to mitigate those challenges. The NIST Cloud Computing Forensic Science Working Group intended to keep the challenges generic and disregarded the myriad architectural differences among the many cloud computing offerings. To assist in filtering out the challenges that do not have a cloud-based root cause, the team analysed each challenge through the lens of the cloud computing model. Table 2 of Annex A captures this analysis in the third column, which identifies the characteristics most relevant to each challenge [130].

Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the Provider and Consumer of the used service. The correlations between the forensic challenges and these functional capabilities were examined by determining the relationship between a particular forensic challenge and a particular functional capability. A majority of the issues are technical in nature with a major secondary group that is framed by legal and organizational issues.

Cloud forensics challenges include (but not limited to):

- Data integrity in a multi-tenant environment where data is shared among multiple computers in multiple locations and accessible by multiple parties.
- Analysis correlation, reconstruction, time synchronization, logs, metadata, timelines.
- Incident first responder confidence, competence, and trustworthiness of cloud Providers to act as first responders and perform data collection.

In traditional computer forensics, investigators have full control over the forensic artifacts (e.g., router logs, process logs, hard disks). In a cloud computing Ecosystem, control over functional layers varies among Cloud Actors depending on the cloud service model. Cloud Consumers have the highest level of control in an Infrastructure as a Service (IaaS) model and the least level of access to log data for the Consumer. To perform forensic analysis using logs with integrity on which all stakeholders can rely, the logs must be trusted. Differences in log formats, lack of accessibility to logs, and the need to preserve the chain of custody make log analysis challenging in clouds. Additionally, the use of logs in hypervisors is not well-understood and presents a significant challenge to cloud forensics.

Digital forensics needs to be able to lawfully perform remote digital forensics collections that will lower the costs associated with travel. Time is frequently a critical issue as it relates to time synchronization and the possible disappearance of evidence that is not quickly found. Location, backup and redundant storage are important. Understanding of the topology will aid in identifying physical locations of media storage. Sensitive data theft cases (insider, outsider, and both working together) are an important issue. The pervasive personal use of cloud computing environments by employees could heighten the risk of insider theft.

6.1.3. *What's in the cloud*

Anyone involved in criminal acts where liability will ensue if illegal content is found within their possession will likely view cloud storage as a method of protecting themselves by storing content in a place that may not be easily identified. Digital data which formerly resided on a local device may no longer be present following its transfer to the Cloud and any further accesses to it might occur remotely through a cloud storage portal [131].

6.1.3.1. Access to the cloud. A digital forensics practitioner can identify that a suspect has operated a cloud storage account, they may seek (with appropriate guidance and authority) to examine content stored within it. They may attempt to acquire credentials to access a cloud account (either from a seized device or suspect, accompanied by relevant legal authority) or seek legal disclosure of account information from the provider directly. If a suspect's computer or mobile device is seized, it may be possible to extract cloud storage account credentials and use them to attain a remote login to the cloud. While this option may offer a quicker route to accessing a cloud account, providers can update and change the way their service operates preventing such methods from being forensically exploited. Law enforcement must first have some form of reasonable grounds first to suspect that cloud storage facilities have been used as part of an offence, and second, maintain some indication as to what they expect to be stored within the account or how they believe it has been used.

6.1.3.2. The cache. The Internet browser cache on most mainstream browsing applications provides an insight into the content hosted on the sites visited by the user. The browser cache is frequently acknowledged but rarely the sole focus of digital forensics research. In the context of the Cloud, this is also often the case, where the focus on cloud storage application artifacts but omitting an analysis of browser-based interaction with a cloud storage account.

6.1.3.3. Dropbox. This section explores the impact on the Internet browser cache following user interaction with a Dropbox cloud storage account.

Details of the HTML structure of the cache following landing on the www.dropbox.com site are available for examination. The ‘PAGE_LOAD_TIME’: tag entry denotes a UNIX Epoch timestamp which indicates the time the page was last loaded. This time stamp allows a practitioner to determine what files were in the Dropbox account at a given time, taking into account the information discussed in the following sections.

The www.dropbox.com.htm file maintains information regarding the Dropbox web pages visited by a user, with the starting point for analysis being the Dropbox ‘Homepage’. The activity_key is a Base64 encoded value. Following testing, the RecentActivity timestamp was shown to be the same as when_milli timestamp. There appears to be a hash-type alphanumeric string (seemingly of structure type MD5) value for the user's Dropbox account. The viewing_user : value corresponds to the account ID. The home_display_type: value indicates the type of artifact where FILE indicates a stored file, and SHARED/_FOLDER indicates a shared folder item. The display_name: value is the file/folder name shown to the user, which has been assigned to the file when uploaded.

When a user navigates to the 'Files' page (which lists all files in their Dropbox account) a URL of https://www.dropbox.com/home is recorded in the address bar and Internet history. When attempting to determine the contents of this page, the event_type parenthesis contains information regarding each item shown onscreen.

Metadata regarding individual viewed files is cached in a text file which has the following “initials_url”: naming convention where%2FFILENAME reflects the name of the file on Dropbox. When comments are made, the s_xhr = true& actvity_cont = 3activity_context_data = %2FFILENA-ME.txt file maintains addition “comment”: tags. No email address information is available for the third party commenter, and the tag does not maintain the account holder's unique id, rather the value is typically set to 0.

Each Dropbox account also has a ‘Sharing’ page (visits to this page generate the URL https://www.dropbox.com/share in the Internet history), which depicts the files and folders which have been shared with the user's account. When a user interacts with this page, following an examination of the cache, no records of the page content and shared files could be located. As a result, the browser cache is unlikely to provide any records of content from a user account that has been deleted or shared.

6.1.3.4. Google Drive. Google Drive is a cloud storage service that is comparable to Dropbox. The Chrome browser cache retains limited information depicting a user's interaction with their Google Drive account. Unlike Dropbox, on-landing, site strutal.html content is not locally cached, and therefore no metadata regarding stored files can be extracted and examined from the browser cache (unlike Dropbox). When a user navigates to a folder they have created within their account; the URL is typically structured as https://drive.google.com/drive/folders/0By-CihkhmywOek1Gak4ySlhnQkk. The bolded section appears encoded and does not change when the folder is renamed.

As a result, an analysis of internet history is unlikely to reveal account usage behavior. When a user selects an office document of any type and is directed to an appropriate Google facility (either Docs, Sheets or Slides) content is not cached by Chrome.

Digital forensic practitioners face an increased likelihood that localized forms of data storage may not contain all of a user's owned and potentially evidentiary digital content. The act of accessing Dropbox via the Chrome web browser leads to what can be arguably considered comprehensive caching of their account content and its associated metadata. Localized forms of cached cloud storage activity have been overlooked by current academic research in digital forensics and cloud storage investigations.

6.1.4. Forensic by design

The term Digital Forensic Readiness was introduced in 2011 and covers three dimensions (technical, organizational, and legal). Several researchers have investigated Cloud Forensics challenges and their classification. Digital Forensic Investigation Readiness Process model has been integrated in the ISO/IEC 27043:2015 (E) standard. Its main aim is to integrate forensic requirements into every relevant phase of a system design and development stages [132].

Even if the Forensic-by-Design conceptual framework was originated for Cyber-Physical Cloud Systems, it is still interesting to assess its applicability in other domains. Forensic-by-Design aims to integrate forensics requirements during a system's life cycle, but there is no prior work on the alignment of this with System Engineering standards and best practices. The authors address this gap and envision the achievement of Forensic-by Design through System Engineering approach. The Systems Engineering approach efficiency has been already stated in terms of costs and development time optimization, requirements satisfaction, and project management.

The authors propose a Forensic-by-design framework for Cloud computing systems. The System of interest is a reference to a Cloud system and addresses the following points.

1. Motivation.
2. General guidelines.
3. Key Factors and best practices.
4. System's life cycle and System development life cycle (SLDC).
5. Validation.

Anew Forensic-by-design framework is proposed - with some emphasis on Cloud computing systems - that does not only focus on integrating the forensic requirements into the system's life cycle stages, but also enforces compliance with the Systems Engineering standards. For this purpose, the following guidances are recommended: Compliance to the ISO/IEC 24748-1:2018 (E) standard; ensure a continuous monitoring of the desired system of interest's forensic-ready state via: (1) validation and verification processes; and (2) recursive pathways in the selected system's life cycle model.

Note, that it is not realistic to list all the laws and regulations that are related to Cloud systems among multiple jurisdictions. The authors recommend using frameworks such as the NIST (2020) [133] and the ISO/IEC TR 27550:2019 (E) standard. The ISO/IEC 24748-1:2018 (E) standard provides a description of the system (or software) life cycle stages. It enumerates the activities and tasks of each stage and points out the processes that may be enacted.

In the system life cycle, there are three common phases: (1) Requirements Engineering, (2) Architecture Definition, and (3) Design Definition. Multiple stakeholders may express concerns about the system of interest. Needs are transformed into requirements, constraints on the system and other constraints (technological, agreement, integration) are included. Once the requirements are analysed, then a candidate solution is designed.

The verification process identifies anomalies (errors, defects, faults) in any information item, system elements, life cycle processes, etc. The authors argue that this process may include all kinds of verifications (security, privacy, forensic, resiliency). They compare their framework with the Architecture Reference for Cooperative and Intelligent Transportation.

ARC-IT is based on the ISO/IEC 42010:2011 (E) architecture description standard, and frames multiple stakeholders' concerns and interests. Focus will be essentially on the vehicular network (vehicular cloud) and on the supporting Cloud computing system (cloud broker). The ARC-IT document advocates the use of system engineering and the "V" model. It contains 4 different viewpoints (Communication, Physical, Functional, and Enterprise), and their associated views. The proposed key factors are also integrated, with the exception of the forensic requirements that are partially present in the incident handling concerns. Some requirement engineering activities, such as requirements identification, elicitation, and analysis have not been detailed in this mapping.

Achieving forensic-ready systems is ultimately feasible with the adoption of the System Engineering approach. As for the forensic requirements integration, there are opportunities in adapting previous efforts that have been deployed in both security engineering and privacy engineering. The proposed framework is a generic one and is not tied to a specific domain.

6.1.5. Apache CloudStack

This paper investigates how the Cloud Auditing Data Federation event model could be implemented in Apache CloudStack, whether the existing model is improved, and what test case scenarios could be considered [134].

The authors cited and built on previous studies. In 2011, while examining the Eucalyptus cloud platform, the various components' interactions were logged. This detected a Distributed Denial of Service attack that originated in the analysed cloud. In the same year, other researchers proposed the usage of a read-only API to allow cloud customers to download and provide investigators with data. If the investigation is successful and the case is resolved, the Cloud Service Provider will benefit more than the client. In 2015, the Distributed Management Task Force outlined the seven questions that must be answered in order to provide a comprehensive description of an event:

1. What was the action and what was its result
2. When did the event take place
3. Who triggered the event
4. Where was the event triggered from
5. What was the target of the action
6. Where was the event observed and reported
7. Where is the target located

Since it is possible to download virtual drives and memory dumps, the data that may be collected exceeds log files significantly. In 2016, the potential of correlating information contained in log files on the OpenStack platform was investigated from the perspective of the forensic investigator. Since existing solutions do not cover the various cloud models, it became apparent in 2017 that a centralized system for collecting log files was required. The suggested solution is to use a single format/structure for log files. The most commonly acknowledged logging standard is described in RFC 5424 as syslog.

Although it was developed as part of the "sendmail" project in 1983, it was officially recognized as a standard in 2009. Various log file formats have been proposed and used by organizations and businesses on occasion. CIM (a standard for describing software and hardware features for manufacturers) and Cloud Auditing Data Federation are two open logging standards that stand out. Cloud Auditing is a continuous procedure meant to measure and report to Cloud Service Providers on the performance and compliance with security standards of their services. Auditing should encompass administration, technical personnel, and infrastructures in addition to all development models (private, community, public and hybrid).

Customers will entrust service providers with their business and personal information, and as a result, they expect particular safeguards. In a forensic investigation, it is vital to minimize the involvement of Cloud Service Providers. Only temporary files, cookies, and session information files can be found on the customer's end. Web API (Application Programming Interface) and API Endpoints are now accessible on all cloud platforms by default. Using open standards, such as the Cloud Auditing Data Federation, may reduce the likelihood of log file interference.

Some researchers have investigated the capabilities and constraints of various forensic tools in the cloud environment. Organizations may also implement cloud-based technologies for internal use. The acceptance of a tool's results by court authorities is largely dependent on the tool's approval.

CloudStack's event logging is conducted on the cloud-server package, the core of the management server. EventVO is the built-in class responsible for describing events in Cloudstack. The "type" field holds a string indicating the resource associated with the action and response. All resources in a cloud system interact with one another and share data.

Distributed Management Task Force's Cloud Auditing Data Federation event model is the proposed model. The objective of Cloud Auditing Data Federation is to offer all resource-related data to investigators and system auditors in order to facilitate the tracking of specific operations. The approach is intended to provide answers to all seven Ws. The classification of resource entities into taxonomies (Storage, Compute, Network, Data, System, Unknown).

Inside Cadf's constructor, all required CloudStack and Cloud Auditing Data Federation data are collected and matched accordingly. A function (setCADFAction) performs pattern matching against hashmaps in order to match the CloudStack event action with a Cloud Audited Data Federation Action. It includes enumerations for fields such as eventType, Action, and Outcome, as well as string constants for taxonomy-related Reason fields. The most essential action of the Taxonomy class is the generation of matching lists between CloudStack and Cloud Audited Data Federation entities. Changes do not alter the functionality of CloudStack, but do affect its functionality. Three methods were used to test the functionality of the Cloud Auditing Data Federation model:

1. CloudStack's web interface
2. CloudMonkey CLI
3. DevCloud 4 testing environment and marvin scripts (deployDataCenter.py)

The Action Taxonomy of the Cloud Auditing Data Federation covers 26 distinct actions. It is time-consuming because it involves 352 distinct events, and it is extremely tough to integrate and merge with the original project. There is a requirement to adopt a single event type format that is unique to CloudStack and can be used to other platforms. When a CloudStack user deletes one or more events from the database, no additional action occurs besides the deletion. The deletion of an event should generate an EVENTSDELETE event.

Any action that deletes event records must be regarded an event in its own right. Only in this way, a malicious erasure of a history of actions from CloudStack may be recognized. The process of removing recorded events does not qualify as an event and is not recorded by the CloudStack platform. Using an event logging standard eliminates the requirement for developers to research and implement event analysis tools. A tool for all platforms can pass the required tests for NIST certification.

The documents of the Cloud Auditing Data Federation (CADF) are produced in a range of languages and formats. Under the Apache 2.0 license, an attempt to comprehend the CEDF documentation is provided in a public repository on GitHub. The input is a log file containing JSON-encoded CDF log records. The output is stored using the open-source version of MongoDB Community Server in a NoSQL database.

This paper proposes the Cloud Auditing Data Federation event model implementation as the primary logging format for the Apache CloudStack project. Cloud Auditing Data Federation is a straightforward, extensible, and robust architecture that focuses on events rather than the cloud infrastructure's underlying technology. OpenStack, in its current iteration, uses Cloud Auditing Data Federation; OpenStack was the intended platform for Cloud Auditing Data Federation. However, not even OpenStack fully implements Cloud Auditing Data Federation. This paper's implementation of CloudStack does not fully exploit the features of Cloud Auditing Data Federation. In order for an event model to collect as much information as possible, it must interact with each and every event that occurs on the platform. It must be part of the platform's basic design. It cannot be added later as an enhancement because it would result in significant modifications and side consequences for the entire project. Any platform or project that can be hacked, attacked, or used in any way by cybercriminals should be as forensically friendly as feasible. The engineering team and the security team must collaborate to not only test a project for vulnerabilities, but also to ensure that, in the event of an incident, all pertinent data is collected in accordance with the Cloud Auditing Data Federation standard.

6.1.6. Storj

Security risks in the correctness of users' data across a distributed cloud has been a major issue. Fortunately, unique methods have been developed for mitigating this highly discussed issue. A new efficient variation of the provable data possession (PDP) scheme has been developed. Proofs of retrievability (POR) schemes should be employed in environments where data stored in the cloud is highly-sensitive. Another proposed method for data integrity verification is an identity-based remote data integrity checking (ID-based RDIC) scheme [135].

This concept uses a group manager to help members generate authenticators to protect the identity privacy along with two lists for tracing members who performed modifications on each block. A Trusted Third Party (TTP) is presented as a way to ensure the authentication, integrity, and confidentiality of involved data and communications. Cloud forensics poses significant challenges to digital forensics, and a set of procedures for cloud investigations is needed. One of the main challenges is the identification, acquisition, and preservation of data in a cloud environment. Having a framework to follow or tools at your disposal greatly improves a forensic examiners' ability to acquire evidence from the cloud. Forensic investigators can efficiently and safely acquire evidence from cloud networks, including both centralized and decentralized clouds with several authors having developed and tested a range of tools.

Cloud forensics poses significant challenges to digital forensics, and a set of procedures for cloud investigations is needed. One of the main challenges is the identification, acquisition, and preservation of data in a cloud environment. The lack of international collaboration and the legal and jurisdictional issues limit access to cloud evidence.

Identifying files on cloud storage networks is a topic closely related to the findings of Zhang et al. (2019). An online cloud anomaly detection approach has been introduced to detect malicious data. The described approach detected malware with over 90% accuracy, and showed that it was successful in detecting anomalies.

6.2. Internet of Things (IoT)

The Internet of Things (IoT) paradigm is increasingly deployed in critical infrastructure sectors, including sectors that are typically not as technologically-advanced such as agriculture. Most IoT devices are low-cost/inexpensive with limited computational capabilities (i.e., battery life and processing or storage capability). The competitive landscape and technical constraints on IoT devices also mean that it will be challenging for IoT device manufacturers to design and incorporate sophisticated security features. Malfunctioning devices can also create a number of serious security vulnerabilities. Every poorly secured Internet-connected device could potentially have an impact on the security and resiliency of the Internet at large. This is due to the challenge of acquiring and curating large volumes of IoT-relevant empirical data from a large range of (heterogeneous) IoT devices. In addition, acquiring IoT-centric malware and their signatures, for example to train machine learning algorithms, is also challenging.

The continued growth of IoT devices has enabled the sharing of information within people and between the devices themselves. The direct communication between these devices is facilitated over the internet by the Application Programming Interface (API) and is controlled by

Mirai Botnet

Typical Mirai botnet components include a Command and Control (CNC) server, MySQL database server, Scan Receiver, Loading server, and DNS server. A DDoS assault is initiated by delivering a command to the CNC server from a remote terminal. The MySQL database server and target both record the command. Is sent to infected Internet of Things devices (or bots). The bots comply with the command of the controlling computer by sending a deluge of network packets to the victim server. An infected Internet of Things device can scan the network for other vulnerable devices and transmit its findings to the Scan Receiver. The information from the vulnerable device would be gathered by the Loader. The Loader would log in to the compromised device and upload malware. Once infected, the IoT device will register itself with the CNC server as a new bot. In order to accomplish this, the new bot registers with the CNC server and retrieves its IP address from a hard-coded DNS server [137].

intelligent devices of the cloud servers. According to a report by Cisco, by the year 2030, it is expected that over 500 billion devices will be connected by the internet. IoT forensic process brings with it unique and complex challenges. Digital investigators are required to create new investigative processes specific to IoT by drawing upon techniques and methods used in acquiring evidence from other established areas of digital forensics [136].

Data from IoT devices can be in vendor specific formats that deviate from normal electronic documents or file system formats. The forensic process of IoT is still in its early stages, there are few and limited researches that have been conducted. Most research that relate to the digital forensic investigative process in IoT is more theoretical than practical. The limited computing resource capabilities for many IoT devices coupled with the unique cloud-based infrastructure makes it even difficult to store data in the devices for forensic purposes. Digital forensics investigation process has been vibrant recently due to the emergence of IoT technology which is now seen as a big threat to information security.

The large volumes of data generated by IoT devices contains a huge potential of evidential data due to the large number and variety of IoT devices that are spread within a wider application area. The complexity around the extraction of data from IoT environments is a major setback in the ability to produce evidence admissible in a court of law.

Digital forensics is the field where legal investigations are assisted by analysing digital sources of evidence. In cybersecurity, the concern is to ensure the security of digital data and the privacy of their owners. Increasing availability of IoT devices across society makes it inevitable to find them in modern crime scenes. Electromagnetic (EM) Side-channel Attacks is one approach that has shown promising results. EM emissions of a device can be passively observed to infer both internal operations and the data being handled, therefore presenting the possibility for EM side-channel analysis as a potential case-advancing possibility for digital forensic analysis of IoT devices.

6.2.1. *Internet of things examinations*

Internet of Things (IoT) devices communicate with their surroundings and provide effective data gathering, monitoring, and information sharing regarding the parameters under which they operate within that environment. Due in part to the relative immaturity of the consumer IoT market and the lack of standards in the early phases of development, IoT devices are frequently characterized as insecure, and their popularity provides adversaries with a large attack surface. In addition, several organizations produce IoT devices using their own design methodology, leading in proprietary hardware and software designs that lack common interfaces and forensic acquisition techniques.

Torabi et al. (2020) create a method to assist cyber forensic analysis for IoT devices employing infrastructure for detecting attacked IoT devices and “fingerprinting their uninvited activity.” The method allowed the researchers to infer compromised IoT devices, characterize created scanning campaigns, detect IoT devices that had fallen victim to DDoS attacks, infer IoT botnets, and do temporal network forensic analysis [138].

The project uses Shodan to obtain information on Internet-connected IoT devices; the UCSD real-time network telescope (darknet) to source passive, unsolicited Internet traffic; darknet data parsing and preprocessing to identify various types of traffic, such as scanning traffic; data importing and aggregation; and dynamic device profiling to create a profile for each device. Approximately 400,000 devices, including, but not limited to, routers, IP cameras, printers, and DVRs, had their data collected. In addition, the researchers gathered 4 terabytes of passive darknet traffic, which represented millions of IoT and non-IoT hosts.

The system built by the researchers processed 4 TB of passive network traffic using frameworks for big data analytics. The testing uncovered 27,849 infected IoT devices transmitting scanning packets to the darknet. Routers, WAP (Wireless Access Point), Firewalls, and Webcams were the most often compromised devices; they were hosted in 192 countries, with the highest concentrations in Russia, the United States, Ukraine, and China.

On IoT devices, the Mirai botnet has made frequent and significant appearances. As its source code has been made public, even non-experts are able to construct their own Mirai botnet to launch Distributed Denial of Service attacks. Previous analyses of the Mirai botnet have concentrated on the executable code from infected IoT devices; however, study of the botnet’s control server(s) may provide more useful information. The investigation involved the acquisition of the disc image, memory (RAM) image, and network traffic from the control servers. The following are the sources and categories of evidence:

- Terminal of the attacker — network packets can be collected live or previous packets can be reconstructed from the memory image. The packets may contain user credentials and commands, a target IP address, its netmask, and the packet’s length time.
- Command and Control server – likely to include source code files, the database server’s IP address and login credentials, the table name of the Mirai database where the CNC user credentials and command history are stored, allowing the analyst access to the full database. There are also queues for monitoring bots, including active, removed, and aggressive bots, which offer the examiner with a list of bots. The IP address of the bot can be established.
- Database server - This server stores the Mirai database, which contains the history of commands given on the CNC server, a user’s table containing the CNC login credentials, and a whitelist table containing the IP addresses that bots are not permitted to scan. The database server is both physically and remotely accessible.
- Scan receiver and Loader – can be a source of substantial information regarding the bot list and attack history from the memory and disc image. For instance, infected IoT devices transmit packets to the Scan Receiver that contain the IP address of a vulnerable IoT device and its tested login credentials for an unauthorized login. Bot executables are placed in the Loader so they can infect IoT devices that are susceptible to infection. Therefore, it is possible to recover the bot executables from the server’s disc image. Importantly, the IP address of the DNS server is hard-coded into the executable, which can subsequently be used to monitor and collect data about future attacks.

- DNS servers can be set in a variety of ways, making it difficult to forecast the information that may be accessible. Nonetheless, the DNA server may log DNS searches and other data.

The authors present an adaptable road map for the forensic analysis of Mirai botnet server infrastructure. The test may begin on any of the five servers to which the examiners have physical access. However, the CNC server or the MySQL server should take precedence, as they will include the bot list and attack history. Second in priority are the Scan Receiver and Loader, followed by the remote terminal of the attacker and the DNS server.

6.2.2. *IoT speaker systems*

Every year, the usage and penetration of AI-powered speakers grows at a rapid rate. Diverse investigations are currently being undertaken on the collecting of artifacts from such devices. Analyzing encrypted traffic with the AI Speaker requires further research. Digital forensic investigators must be able to analyze traffic between AI Speaker and the cloud that is encrypted. Numerous forensic studies have been undertaken as the penetration rate of AI Speakers and IoT devices has grown [139].

In this study, the researchers investigate the information sent between an AI Speaker and the cloud by analyzing their encrypted traffic. By examining the encrypted data that the cloud transmits to the AI Speaker, it is possible to infer user information stored in the cloud. A Chip-off is a method for acquiring data by physically detaching NAND Flash from the PCB of a mobile device or IoT device. To examine encrypted traffic between AI Speakers and the cloud, it is necessary to analyze several elements of the AI Speaker in question. In this study, Man-in-the-Middle attacks are run on encrypted communication using the HTTP proxy tools Charles and Fiddler.

When injecting the certificate into an AI Speaker, five techniques are presented. Each approach entails a software and hardware investigation, and certain procedures involve Chip-off and BGA Rework. A forensic model is presented for examining encrypted traffic between AI Speakers and the cloud based on these methodologies. The AI Speaker is injected with a certificate utilizing the proposed forensic model and linked to Wi-Fi via the mobile hotspot capability of the laptop. Five ways for injecting a certificate into an AI Speaker and configuring a proxy are described, along with network diagrams.

This enables the certificate to be installed and a proxy to be configured using a system application that is inaccessible on conventional AI Speakers. The Kernel and Ramdisk images can be changed to run on a virtual Raspberry Pi device and can be ported as required. With this arrangement, the UART, JTAG, and other ports are implemented virtually, allowing logical debugging without physical implementation. Analyzing an image of the AI Speaker to hunt for backdoors and vulnerabilities in the device or to exploit known vulnerabilities.

6.2.2.1. Five forensic methods for encrypted traffic using certificate injection. In order to evaluate the encrypted communication between an AI Speaker and the cloud, the five approaches of the forensic model were used to an AI Speaker in the tests and results described in this part.

Man-in-the-middle is a technique for constructing a device with the same functionality as the AI Speaker by transferring data from the AI Speaker's NAND Flash to an Android handset. Samsung's Galaxy Note 3 (Android 5.1.1) was used as the porting device, and the Chip-off image was Naver Clova. Due to the fact that Android Things is used as a development platform for AI Speakers, a Raspberry Pi 3B experiment was also undertaken. In the image porting experiment on the Raspberry Pi 3B, several Android Things partitions were split in half, unlike a standard Android OS, which made the porting more challenging. On the Galaxy Note 3, "build.prop" in the system partition must be updated for the AI Speaker app to function properly. A sharedUserId-related AI Speaker system app installation problem is the primary cause of the failure.

The goal of porting AI Speaker hardware to ARM using QEMU is to allow AI Speakers to operate on a virtual Raspberry Pi. In scenario 1, a Chip-off was used to obtain an image of the AI Speaker for transferring the firmware. To match the chip-ARM off's 32-bit architecture, the Raspberry Pi 3 was used as the virtual hardware. The experiment was conducted by installing a QEMu emulator on Mac OS 10.13.6 and executing it on a standard personal computer. It is impossible to fully port all functionalities, however major systems such as microphones, speakers, and Ethernet are anticipated to operate. If the APQ8009 kernel source is used in the future, the porting should be successful. However, following a successful boot, services and other functions may not function normally.

The experiment used the AI Speaker KT GiGA Genie and the HTTP proxy application Fiddler. The mobile hotspot functionality of Windows 10 was also used to establish a Wi-Fi network to which AI Speakers may connect. Through the backdoor of KT GiGA Genie, the proxy was configured using the Wi-Fi menu of the Android system settings application. Next, a method to the APK established in a previous study was added to install the HTTP proxy tool's certificate. The location for storing certificates in an Android OS varies between versions; hence, the Android version was identified by analyzing the "build.prop" file on the system partition. This flaw opens a socket and executes all commands entered with root access.

The experiment involves connecting the UART port and host via USB to the TTY and extracting, editing, and rewriting the NAND Flash data. The USB to TTY gadget used FT232 FTDI and CP2102. Because a terminal application is necessary to read and write data from the serial device, PuTTY on Windows was used. Because SKT NUGU Candle is organized with 512 bytes each block, it is read using an MMC dump by 512 bytes. The fastboot command overwrites data in the SKT NUGU Candle's userdata partition. The maximum file size for a single image upload is less than 1 GB. The HTTP proxy tool can gather and analyze encrypted traffic if the AI Speaker boots normally. Nonetheless, SSL pinning and other factors make it difficult to analyze encrypted communication on this device. A solution for circumventing firmware tampering prevention technologies on a device is required.

By default, chip-off is done to directly change the NAND Flash data retrieved from the AI Speaker's board. This is the final option available when inserting a certificate and configuring a proxy using previous methods is not possible.

Experiments conducted using Amazon Echo Dot and Alexa Pi revealed only the addresses of cloud servers that appear to be receiving voice instructions. It is uncertain whether voice instructions are stored owing to SSL pinning. The majority of KT GiGA Genie's encrypted communications were able to be analysed. Voice query, alarm registration, device information, and user information-related traffic were all revealed, plus the researchers created a verification tool that collects cloud-based KT GiGA Genie artifacts. The program takes advantage of the capability to immediately issue a session token using credentials stored in plain text on the device. For SKT NUGU, ten distinct cloud-based artifacts could be derived. Except for KT GiGA Genie and SKT NUGU Candle, the experimental outcomes were poor. Even if the certificate is injected into the AI Speaker, SSL pinning makes it difficult to evaluate encrypted traffic. Porting will be possible in the future if the open source kernel can be obtained or a development board that employs APQ8009 is used. In this study, Man-in-the-middle-based AI Speaker certificate injection forensic models were proposed and evaluated. These techniques made use of porting, the backdoor and vulnerability of an application, the hardware interface, and a BGA Rework. Some Amazon, Naver, SKT, and KT AI Speakers were capable of analyzing encrypted traffic.

6.2.3. *Side channels*

The IoT has revolutionized the landscape of digital forensic investigations like never before. These devices are capable of storing vital information that can prove useful in a digital investigation. A medical implant, such as a pacemaker, can provide hints in an investigation about a person of interest's physical exertion or stress introduced elevation of heart rate. Forensic investigators must look for IoT data in the user's smartphone or cloud storage. EM radiation from IoT devices can be a potential non-invasive window to gather forensically useful information.

EM radiation patterns from the CPU of IoT devices sufficiently correlate to the software activities. Cryptographic algorithms running on a IoT device can be detected with 82% accuracy through EM emissions. This includes cryptographic algorithms employed to protect data stored on these devices. Modern digital computer systems depend on electric pulses or alternating currents for their operations. EM emission signals from these components contain a significant amount of information regarding the events related to software execution and data handling.

Power consumption based side-channel attacks was able to guess the encryption key accurately, given sufficient cipher texts and the power traces for those encryption operations. A metric called SAVAT (Signal AVailability for an ATtacker) that measures the EM signal power emitted when a CPU is executing a specific pair of instructions (A and B). Different selections of A/B instruction pairs emit different signal power, i.e., amplitude and frequency modulated EM emissions from CPUs.

An assembly program that executed a particular CPU operation continuously was used to generate matched-filter templates. Hilbert-transformed signals are similar to time-domain signals but perform better for the same signal-to-noise ratio (SNR) of signals. Another alternative format of representing EM emission signals is using a RF-DNA fingerprint. This technique has been used to identify rogue devices in a deployment through using their RF signals without physically inspecting them.

The continued growth of IoT devices has enabled the sharing of information within people and between the devices themselves. The direct communication between these devices is facilitated over the internet by the Application Programming Interface (API) and is controlled by intelligent devices of the cloud servers. According to a report by Cisco, by the year 2030, it is expected that over 500 billion devices will be connected by the internet. IoT forensic process brings with it unique and complex challenges. Digital investigators are required to create new investigative processes specific to IoT by drawing upon techniques and methods used in acquiring evidence from other established areas of digital forensics [140].

Data from IoT devices can be in vendor specific formats that deviate from normal electronic documents or file system formats. The forensic process of IoT is still in its early stages, there are few and limited researches that have been conducted. Most research that relate to the digital forensic investigative process in IoT is more theoretical than practical. The limited computing resource capabilities for many IoT devices coupled with the unique cloud-based infrastructure makes it even difficult to store data in the devices for forensic purposes. Digital forensics investigation process has been vibrant recently due to the emergence of IoT technology which is now seen as a big threat to information security.

The large volumes of data generated by IoT devices contains a huge potential of evidential data due to the large number and variety of IoT devices that are spread within a wider application area. The complexity around the extraction of data from IoT environments is a major setback in the ability to produce evidence admissible in a court of law.

6.2.4. IoT complexity

6.2.4.1. Factors affecting IoT forensics. The challenges posed by IoT environments in relation to forensic investigative process have attracted recent advancements in the research. The huge data generated presents digital forensics expert the difficulty of collecting and extracting evidential data in a smooth manner. The short survival period and the limited visibility of the evidence can also be viewed as challenges to the investigation process. Further research discusses IoT forensics and brings out its uniqueness of IoT to traditional forensics. Some papers do not provide any viable solutions to the highlighted challenges; however, summaries of the challenges that have been solved and not solved under what cloud service are provided [141].

There is need for tools and libraries for better management of IoT-big data. IoT devices have limited computing capabilities and rely heavily on cloud services for their functionalities. Data will be collected from the cloud infrastructures and analysed leading to a form of cloud forensics investigation. A survey seeks to analyze the state of cyber-crime in IoT environments. Issues relating to how the traditional digital forensics could be integrated into IoT cases are discussed.

The nature of work for information security experts, forensic investigators and system auditors has been hugely changed by the prevalence of Big Data. A survey conducted reviewed cloud computing and internet of things in relation to key legal issues emanating from the European Union (EU). The wider perspective on legal and regulatory aspects of cloud of things, major challenges, and complexities in the past, present, and future are highlighted. The paper outlined the various fundamental legal considerations as presently portrayed in the cloud of things. It tackled the key issues relating to identity, authenticity and trust, consumer protection, standards and the demonstration of how legal obligations can be complied.

Although little has been spoken regarding cloud and IoT forensics, this is a useful resource for the application of laws in the IOT forensics process.IoT and smart cities in relation to the legal challenges encountered in digital forensics, privacy and security was analysed with a comparative review of legal regimes in China, Korea, Hungary, European Union, and the United States of America. It was concluded that legislation needs to be clear on issues relating to the balance between public security and individual privacy freedoms.

6.2.4.2. Current research in IoT forensics. There is need for an improved proactive model under which IoT crime scenarios can be handled. The resource limited IoT devices and the volatility of the cloud needs to be considered. The Next Big Thing was designed through a top down forensic approach methodology.

The Last on Scene (LoS) algorithm works by identifying the location of evidence in such a way the first device to be investigated is the one that was seen last on communication chain. Unfortunately, the LoS Algorithm is a theoretical framework meaning that its practical implementation or application has not been tested. The Digital Forensic Investigation Framework for IoT process model is based on a generic approach that analyses digital forensics data in the IoT setup through process concurrency. It aims to establish IoT forensics readiness and increase the rate at which the digital evidence extracted is admissible in a court of law. The drawback with this model, is that it is purely based on theoretical approach in the collection of the forensic data.

The IoT mobility forensics model involves an analysis based on a scenario of attacking the collected data and proposing a forensic model that fits such scenarios. Data is collected using Wireshark; however, it is not revealed from where this data is preserved as this is very crucial in a criminal investigation.

The fog computing model, in which intelligence is pushed by a gateway to the network edge, though workable, is not suitable for a general IoT forensic investigation. It can well be implemented in a home or a controlled environment and its main purpose would be to notify of any suspicious activities.

A framework is proposed that incorporates Digital Forensics Readiness (DFR) within the IoT environments has three distinct entities which are: Proactive Process (detects pre-incidents), IoT Communication Mechanism (provides. smart communication strategies on the intelligent network for machine-to-machine devices) and Reactive Process (handles digital investigations in post-event response process).

An IoT forensics framework called Probe-IoT uses public digital ledger in searching for evidential facts in incidents in systems that are IoT based. Through the framework, interactions between IoT entities like IoT devices, IoT users and the cloud, are collected as evidence and stored securely in a blockchain.

The Forensic Evidence Acquisition and Analysis system demonstrates how smart home systems can be controlled and also provide details of when, what, and how the events take place. The IoT device forensics and data reduction process demonstrates how the acquisition process is automated and huge amounts of data is quickly analysed. Two approaches were proposed for conducting IoT investigations based on low security mechanism and constraints encountered in IoT setups.

There is a need to conduct robust experiments that can be validated scientifically. The production of IoT equipment and provision of IoT services that are readily adaptable and integrated into the current digital processes is still a challenge in digital forensics investigations. Privacy is a contentious issue in relation to investigation processes that involve personal and protected data as stipulated under EU and GDPR laws. Digital warrants could help to effectively retrieve evidence from sources discovered later in the process or along the process of an investigation. With the increase of attacks related to IoT, there is a massive need for successful prosecution of perpetrators. There is a need for intelligent and more efficient tools that are scientifically validated to ensure reliable guiding procedures leading to successful digital investigations.

6.2.5. *Contiki OS*

Due to the resource-intensive nature of data collection, a greater emphasis must be placed on prioritizing the investigation processes to increase the likelihood of gathering meaningful evidence. Volatility of data quantifies the rate at which data disappears from a system and is vital for determining the probability of gathering the most valuable evidence. An examiner can evaluate the likelihood that evidence exists using a model of volatility. This study justifies and describes a model for data volatility, and illustrates it for the Coffee File System used by Contiki OS, the operating system for IoT devices. Experiments were undertaken to see how well the model matches to the obtained simulated data and observations from file system operations were used to cross-validate the model. The results demonstrated that the volatility was underestimated by a model approximating the file system's operation. While there are several qualitative sources describing volatility, there is a paucity of quantitative research. This study is a stepping stone to understanding a quantitative method to proving volatility [142].

6.2.6. *IoT forensic methodology concept*

IoT ecosystems and associated devices differ from normal IT systems in terms of processing power, variety of firmware, proprietary data formats, data storage methods, and operational circumstances, necessitating a new approach to forensic investigation. Utilizing widely established traditional models and adapting them to the peculiarities of the Internet of Things may be an exciting technique for the construction of IoT forensic solutions in these circumstances. Consequently, the objective of this paper is to provide a conceptual technique for conducting IoT forensic investigations based on a conventional paradigm. The objective is to compile the characteristics of all IoT devices and systems in a concept proposal that covers the entire investigation process, with the expectation that it will eventually serve as both a general guideline and a foundation for the development of procedures to address specific IoT contexts [143].

The investigator must collect incident-specific information, comprehend the characteristics of the compromised IoT network and its constituent devices, and decide the appropriate level of forensic soundness. The technological characteristics and physical accessibility of the devices have a significant impact on the acquisition procedure. The frequency with which non-volatile memory is soldered to the circuit board of an IoT device is the primary difference between IoT devices and conventional ones. Only storage that is detachable permits extraction and acquisition. If the device cannot be physically accessed or if the aforementioned procedures fail, the sole alternative is live acquisition.

The optimal course of action is to eliminate network traffic from routers and IoT gateways, as they are the devices that transfer the most packets. Since intervention is required during live acquisition, as is customary in conventional forensics, the system-saved data will be modified. It is necessary to create a profile of the memory that is being acquired in order to analyze the acquired data. Online analysis is more widespread than traditional forensics due to the non-volatile memory of devices and the impossibility of assuming physical access. Because the data in the source of the evidence will have been altered, live examination compromises the forensic process's integrity.

However, in many scenarios it may be the only appropriate way for evaluating a device, thus flexibility should be granted. Three stages, each involving a number of processes, comprise the conclusion of the study. In addition to writing and presenting the forensic report, other tasks include recovering the original sources of evidence and reconstructing and restoring damaged systems. The most important purpose is to assess all relevant facts collectively and draw conclusions while taking the overall environment into account.

6.2.7. *Medical devices*

The information found on mobile phones, SIM cards, micro-SD cards, and Internet of Things devices is frequently important for court investigations because it provides a plethora of data to steer investigations, not to mention solve them. However, investigators must contend with two issues that significantly hinder the extraction of data from digital equipment: data encryption and evidence tampering (explosion, immersion, deliberate destruction, air crash, accidents). In these instances, investigators are frequently need to be inventive in order to successfully extract data from electronic devices in a legal context. Using medical equipment for data extraction is a novel approach that exemplifies this innovation, which is required or the investigator will be barred by the new protection and encryption technologies [144].

The authors describe four medical materials and pieces of equipment routinely employed in the field of forensic autopsy: the mobile 2D X-ray radiograph (used by dentists), the whole body 3D X-ray scanner, the dental control unit (burr and drill of dentists for legal odontology), and dental paste to model teeth when identifying disaster victims. This work provides medical materials and equipment that can be employed by investigators for data extraction, as well as inexpensive alternatives to costly failure analysis industry solutions. To demonstrate feasibility, they discuss experimental forensic situations in which medical devices could assist in data extraction, including reverse engineering, diagnostic samples, and the preparation of mobile phones for forensic transplantation.

The authors examine the future of legal medicine in the belief that the autopsy of the future will unquestionably need to be augmented by study of the electronic components present in the body (pacemaker, biosensor). Medical examiners and electronic experts must now collaborate to develop the forensic procedures of the future.

6.2.8. *IoT cyber threat*

Network telescopes (also referred to as darknets) are a collection of routable, allocated, yet unused IP addresses which operate no legitimate hosts. They are used solely to passively gather and amalgamate Internet-scale incoming traffic. Unsolicited/malicious IoT devices that attempt to probe the Internet space (searching for other devices or to exploit certain Internet-wide vulnerabilities) would inevitably target the network telescope space. A probing detection algorithm is used which generates darknet flows representing consecutive packets originating from each unique source IP address. The algorithm operates similar to the probing detection component embedded in Bro [145]. There is a need for identifying scans originating from IoT nodes versus those that are generated by typical hosts. The Shodan service is used which indexes

Internet-facing IoT devices. For characterization purposes, a geolocation database provided by Maxmind is leveraged to attribute the inferred unsolicited IoT sources to their hosted ISPs, ASN, cities, countries, etc. The generated IoT threat insights are made available via a frontend service at http://faculty.eng.fau.edu/ebouharb/floridasoar/index.html, which includes near real-time information related to Internet-scale compromised IoT devices (and geo-location and sector information) as well as basic Snort signatures [146] (automatically extracted from IoT-relevant darknet flows) [147].

The aim is to generate feature vectors related to the inferred IoT probing sources to facilitate the initial application of L1-PCA and subsequently the application of unsupervised data clustering on darknet data to infer orchestrated IoT campaigns. Intuition is that IoT bots operating within orchestrated campaigns share similar network traffic characteristics, which is a common “in the wild” observation. Scan Type determines whether the IoT source performs a horizontal scan, a vertical scan or a strobe scan. Scan Trend shows how the targets are being probed. Another behavioural property of an IoT scan event can be a metric to characterize how much probing traffic is dispersed or focused towards the network telescope. Dispersion measures the level of dispersion of the target IP addresses in a scan. This metric can aid in clustering orchestrated probing campaigns in scenarios when stealthy botnets assign a distinct, small sub-part of the cyber space to each of the bots to scan. It is worthy to note that this metric is very efficient in comparison with other typically employed statistical methods in terms of required memory and computation.

Principal component analysis (PCA) is a powerful dimensionality reduction tool for analyzing datasets. PCA involves finding the orthonormal basis (the principal axes of the data) over which the variance of the projected data points is maximized. L1-PCA shows remarkable relative resistance to faulty data contamination in the dataset, due to the linear emphasis placed by the L2-norm optimization metric on each data point.

6.2.8.1. Accuracy validation using the SIP scan campaign. The aim is to validate the proposed dimensionality-reduction technique on a probing campaign with a known ground truth in the presence of outliers.

Ten different test datasets were created based on merging empirical scan events extracted from:

1. A known orchestrated probing campaign (i.e., the SIP/VoIP scan campaign)
2. A recent scan events targeting the same destination port as the SIP campaign
3. Other scan events.

Note that all the scan events target the same network telescope.

For each dataset, L1-PCA is applied to reduce the dimension of the feature space by projecting them on 3 main principal components. By leveraging the Silhouette Coefficient on the dimensionality-reduced data, the optimal number of clusters can be computed to use in k-means clustering. The cluster which contains the orchestrated SIP scan events can be identified and all of its members labeled accordingly. This allows us to compare the results with the true labels and calculate the confusion matrix of this binary classification.

The severity of the insecurity of the Internet of Things (IoT) is highlighted by reporting on the exploitations of Internet-scale IoT devices. The existence of “in the wild” coordinated IoT-specific probing campaigns is revealed by applying the proposed L1-PCA technique. More than 1 TB of network telescope captured data is analysed.

Unsolicited probing activities from 129,713 unique IoT devices were inferred which were distributed in 199 countries, hosted by 43 various sectors, and hosted/operated by 8540 ISPs. The top countries hosting such compromised devices were found to be Mexico (14%), Brazil (12%), China (9%), Indonesia (5%), Russia (4%), United States (4%) and Vietnam (4%). These countries hosted 52% of the inferred devices.

Results show 921 orchestrated, IoT-centric campaigns, 142 of which possess more than 50,000 IoT bots. One of the campaigns seems to be quite distributed worldwide, involving 114 countries and 1168 ISPs, where close to 40% of its IoT bots are related to surveillance cameras from Dahua.

Scans for Memcached servers from IoT cameras were observed in one campaign, high rate probing for DNS resolvers in another campaign by MikroTik routers, and co-occurring probes towards Chargen and QoTD from AvTech sensors. Also, 11 IoT coordinated probing campaigns were observed searching for amplifiers.

Identifying technical information for Internet-wide IoT devices remains challenging. In addition, IoT malware often disable common outward facing services upon infection. The formal correlation approaches between passive measurements and malware network traffic samples to provide an attribution evidence are being investigated. This will allow a more sound estimation of compromised IoT devices within each inferred probing campaign. Large volumes of network telescope data with IoT-specific information correlated to infer and characterize Internet-scale IoT exploitations.

6.2.9. Stitcher

Internet-of-Things (IoT) technology has drawn both new adopters and opponents. In the first half of 2019, attacks on IoT devices have surged by more than 300%. IoT digital forensics is an underdeveloped field that requires additional attention. Digital Forensic Investigators with inadequate training may be unfamiliar with the structure of IoT devices and smart homes. Prior study has revealed issues in the field of digital forensics, but there has been no systematic survey of Digital Forensic Investigators that investigates the difficulties they experience [148].

STITCHER is an automated evidence classification and correlation tool meant to assist Digital Forensic Investigators with IoT data analysis. It classifies the evidence in accordance with a combination of applicable international ISO standards (ISO 27050-1:2019 and ISO 30141:2018) and then processes the evidence. The report provides the results of a user study conducted by 39 Digital Forensic Investigators using STITCHER to examine digital evidence gathered from a simulated Internet of Things (IoT) crime perpetrated by hackers resembling the most sophisticated. 96.2% of users reported that STITCHER helped them handle the investigation, and 61.5% solved the case entirely. The technology and experimental data are freely available at https://github.com/poppopretn/Stitcher for repeatability and the advancement of research in IoT digital forensics.

Preparing storage systems to retain extracted evidence, extracting relevant evidence (physical or logical), assessing evidence for data points of interest, and reaching a conclusion are all components of the examination of evidence. The authors discovered three viable sources of evidence for IoT digital forensics: firmware image, network packet captures and system activities. Digital Forensic Investigators may find it difficult to determine the original functionality of an embedded device using only static analysis. Captures of network packets provide a plethora of information that can be used to expedite an enquiry. Useful data, including source and.

Protocols, IP addresses, hardware addresses, source and destination port numbers, data payloads are tracable and retrievable from captured network packets. Investigators in the field of digital forensics face the issue of correlating different sources of evidence and analysing them for consistency. Traditional digital forensic techniques, such as disc imaging and live memory analysis, can be used to investigate criminality involving conventional computer systems.

Using specialised hardware and software, such as Cellebrite, these techniques are also possible on smartphones. As IoT is a developing field, clients and the justice system may find it difficult to comprehend the architecture of an IoT setup. Valuable evidence may be in danger of being ruled inadmissible in court.

6.2.10. IoT blockchain

Data produced in IoT environments is difficult to secure due to the heterogeneity and dynamic features of the devices (and their ecosystems). Considerable public and proprietary research work is being undertaken to ensure IoT ecosystems maintain sound data confidentiality, access control, authentication, privacy and trust. The devices contain sensitive data (and represent a large attack surface) making them a target for cyber-attack. The challenge is to conduct a sound forensic examination of the subject IoT device (and ecosystem) using traditional digital forensic techniques. One solution is to use a blockchain based model that ensures the verifiability of log produced in a blockchain model. Blockchain based evidence, including logs and other digital evidence produced by IoT environments can be verified by justice system participants. Blockchain based evidence can prevent the tendering of false evidence allowing each participant to authenticate the evidence and have confidence in an untampered chain of custody [149].

When considering the evidence from IoT, the digital evidence is wider in scope than that of other categories, for example, mobile forensics or motor vehicle digital forensics. The scope for IoT forensics (is an ecosystem rather than being limited to a single device) and includes the cloud, network, device (and phone).

6.2.11. Electro-magnetic side channel analysis

Hardware and software processes performed by computing devices unintentionally emit information that can be monitored.

Each side-channel attack on a computer system focuses on one specific unintentional leakage of information from either hardware or software. Some of such information leaking side-channels are listed include [150].

- The memory and cache spaces shared between different software.
- The amount of time a program takes to respond to different inputs.
- The sounds different components of computer hardware make.
- The amount of electricity a computer system draws.
- The EM radiation a computer hardware emits.

It has been shown that the execution time of encryption algorithms can reveal information regarding the input values provided, which includes the encryption key. Data leakages from CRT based displays have been known for several decades. Kocher et al. were the first to introduce power consumption based side-channel attacks; simple power analysis (SPA) and differential power analysis (DPA) collects power consumption variation (in mA) over time with a high sample rate, such as twice the clock frequency of target cryptographic device. DPA is a technique that can be custom tailored for specific encryption algorithms.

Electronic devices generate electromagnetic radiation on unintended frequencies as a side effect of their internal operations. These emissions are regulated by government agencies due to the possible interference they can make on legitimate wireless communication and the potential health issues they can cause.

On most IoT devices, the CPU and RAM are included in microcontroller (MCU) chips making it the most important electromagnetic source on-board. These components contain a significant amount of side-channel information regarding the events related to software execution and data handling. Electromagnetic waves can be generated by electric currents varying over time.

The electromagnetic emission frequencies of a target device are unpredictable due to its dependability on various hardware characteristics. It has been shown that small magnetic loop antennas can be used for the purpose of detecting electromagnetic emissions from computing devices. Software defined radios (SDRs) are getting increasingly popular among wireless hackers, hobbyists, and security enthusiasts who are interested in access to the radio frequency (RF) spectrum. A SDR can be used to scan through a wide range of frequencies to locate potential electromagnetic emissions from a computer system.

As a result of executing instructions in different combinations by the CPU, electromagnetic signal patterns are emitted at various frequencies and amplitudes. The most practical method is scanning a large frequency spectrum for suspected electromagnetic signals. This arduous approach is a time consuming task that requires manual inspection by a human user. Further studies are necessary to identify the effect of different CPU architectures to the produced electromagnetic emissions.

When a computing device running a program generates electromagnetic emissions, the patterns observable depend on the precise settings of the device. It is clear that the target device's system clock is the main source of electromagnetic radiation. The design of the printed circuit board (PCB), and characteristics of the electronic components provide variations to this strong signal.

It has been shown that a simple electromagnetic signal acquisition device called RTL-SDR can be used to profile computing devices uniquely. It has led to the idea that electromagnetic emissions from an electronic device owned by a person could be used as an authentication token instead of relying on RFID tags. For example, a known electronic device can be altered at the hardware fabrication level for malicious purposes, such as accessing stored data or eavesdropping on users' activities. Such hardware modifications result in a changed electromagnetic emission pattern that can be used to identify it.

When software runs on different hardware platforms, its electromagnetic emissions are influenced by the software instructions being executed. Identifying the instruction execution sequence can help to uniquely identify the software itself. The capability to detect software code execution sequence has opened up the opportunity to identify when a computing device is running software code not intended by the manufacturer or the owner. Instead of directly using time-domain electromagnetic signal traces, one such alternative format is RF-DNA fingerprinting. This is a technique to fingerprint the physical layer of RF transmitting devices, which includes WiFi, Bluetooth, Zigbee, GSM devices, and even RADAR antennas.

Electromagnetic side-channel analysis can help identify what information is contained in an electromagnetic emission trace of a particular computing system. The kind of software running on IoT devices and the data being handled by each software application are potentially of significant interest. Extracting critical information, e.g., cryptographic keys, can help progress forensic analysis.

Many mobile devices and IoT platforms tend to employ ECC algorithms to secure data. This indicates that such devices can be inspected through electromagnetic side-channels to access cryptographically protected data. Multiple published works have demonstrated the effectiveness of the SelectromagneticA approach in extracting critical data from computers.

DelectromagneticA is a variant of Differential Power Analysis (DPA) that uses the variation of electromagnetic emissions of a CPU to discover variables used in an executing program, such as encryption algorithms. While impractical to perform under real-world attack scenarios, this may be the only resort for electromagnetic side-channel analysis. DEMA attacks are possible by attacking each chunk of the key being used with the XOR operations. Such an attack reveals parts of the encryption key, which have to be combined at the end. It has been demonstrated that electromagnetic analysis is a viable option to the aforementioned power analysis attack on computer CPUs.

Asymmetric key encryption, such as RSA, can also be attacked by identifying the individual modular exponentiation operations performed within the algorithm through electromagnetic emissions. White Box Cryptography (WBC) was introduced as a solution to this; whereby cryptographic algorithms and keys are combined with random codes and data to create an obfuscation.

IoT devices are ideal candidates to be powered by wireless means. RFID based devices are being used in critical systems, such as secure access control to buildings and electronic payments. Investigating the electromagnetic side-channel capability on such devices is important from both security and forensic standpoints. Many smart-card-based frauds involve malicious devices, such as card skimmers, that can read and store data from the cards. Investigators face the challenge of identifying victims of skimming devices due to the fact that card details are encrypted when stored on these devices. It has been demonstrated that electromagnetic side-channel analysis can be even more promising in extracting such evidence.

Electromagnetic side-channel analysis has been shown to be successful on recovering data from computing devices. Various countermeasures have been explored to counteract it on both software and hardware levels. Hardware design countermeasures include minimising metal parts in a chip and using Faraday cage like packaging.

There are currently no standards or tools on electromagnetic side-channel analysis for digital forensics. It is important to review the relevant standards and tools in both hardware and software security domains. In the worst case scenario, the minimization of electromagnetic emissions may require a complete reworking of the printed circuit board used in the device. Multiple commercial and open source products exist that can be used to break encryption on microcontroller based IoT devices. A joint effort by both hardware and software developers to establish standards is necessary.

6.2.11.1. Electromagnetic analysis on IoT forensics. Using electromagnetic side-channel analysis, researchers at University College Dublin, Ireland have investigated the possibility of acquiring digital evidence from Internet of Things devices [151].

It proposes electromagnetic side-channel analysis as an alternative method for gathering forensic evidence from IoT devices when it is too difficult to acquire digital traces (EM-SCA). Operating electronic gadgets, including computers, unintentionally emit electromagnetic radiation. Various computer components (including network controllers, memory, data bus lines, video graphic controllers, etc.) emit electromagnetic radiation, with the central processing unit (CPU) being the most potent emitter. Processors' electromagnetic radiation can be caught at a reasonable distance from the emitting equipment. EM-SCA is the study of unintended electromagnetic emissions from computing machines; it has been used for detecting program behavior, software change, virus, and data extraction. The authors have created a framework known as EMvidence, which consists of a central core with numerous default modules to which third-party plug-ins can be added. EMvidence provides two data gathering methods: 1) observation of EM emission signals for a predetermined period of time without involvement or contact with the device, and 2) acquisition of EM emission signals while actively interacting with the device via an interface.

Experiments revealed that a pre-trained model can recognize the software states of IoT devices' internal components. For instance, if the gadget, such as a smart home alarm, was in an idle state when first responders arrived, it implies that the device was intentionally set to an idle state to prevent the alarm from activating. This information would prompt the first responder to examine the IoT device's button for fingerprints.

Massive amounts of data generated by EM signal collecting equipment render on-site real-time processing unfeasible. Uncertainty exists over the particular frequency channels that are leaking data; hence, a large number of alternative frequency channels must be evaluated. Using filtering techniques and machine learning algorithms, the number of data-producing channels can be reduced from over 20,000 to less than 100. EM trace files can be many gigabytes in size when devices are observed for as little as 1 min.

The researchers discovered that they were able to attain a very high degree of precision, lending credence to the belief that future IoT firmware actions will be capable of being differentiated. They describe a scenario in which Internet of Things (IoT) smart bulbs have been remotely modified to enable an attacker to turn the device on and off at whim. This makes it difficult to discern between harmful and authorized actions with a building's light bulbs. EM-SCA makes it possible for law enforcement to do a rapid EM-SCA scan at crime scenes to verify the firmware operating on the devices and the existence of malware. The reduction in the number of channels to those selected for monitoring was based on the fact that each selected channel displayed distinct software activity variances. The selected channels were unique to the ten distinct software processes that were operating. With a different set of software activities, it is possible that other EM-SCA channels would exhibit greater differential activity. This line of thought leads to the conclusion that specific previously discovered software channels can be used to identify previously known software activity. In practice, when attending a scene involving EM-SCA, the investigator should use the predetermined channels based on the software they're attempting to locate. When comparing the same set of software operations, the most appropriate channels will change based on hardware differences such as CPU, circuit board architecture, etc.

In order to observe EM emissions from a target device, the EM emission frequency needs to be determined. The processor of the Raspberry Pi emits EM radiation at several different frequencies and their associated harmonics. A software defined radio (SDR) device was used to acquire EM signals from the target device. The Raspberry Pi was programmed to run a shell script that performed encryption operations with a time gap of 1 s. The shell script used OpenSSL commands to invoke the AES-256-CBC algorithm on a large file continuously. This resulted in observations of amplitude variations in the EM signal. The blobs that occur with a 1 s gap correspond to the AES encryption operations, while the higher peaks that occur at irregular intervals are external noise [152].

High-end IoT devices tend to rely on cryptographic encryption as a security measure. Experiment investigates the possibility of using EM emissions of IoT devices to automatically detect when they perform data encryption operations.

Data Acquisition: The experiment involved a Raspberry Pi as the target device and a HackRF as the EM signal capturing device. To reduce unnecessary EM noise capture, each time the Raspberry Pi perform a cryptographic operation, it notified the host computer immediately before and after by sending UDP packets. The EM traces collected totaled about 12 GB.

Data Pre-processing: Due to multiple reasons, the acquired EM can have variable lengths in the time-domain and also may not properly enclose the cryptographic operation within its boundary. To mitigate these differences, each trace is converted into the frequency-domain by using a Fourier Transformation. These labeled EM trace samples are still unsuitable to be directly used as training samples for a machine learning-based classifier.

Classification: A neural network was implemented to classify EM traces into the correct class that had four layers; an input layer, two hidden layers, and an output layer. For each class, 600 samples were taken for the training process totalling 2400 training samples for all four classes. A 10-fold cross-validation was used to validate the classification results.

Results: The neural network classifier correctly classified the three cryptographic algorithms and the non-cryptographic scenarios with 80% accurately. The ability to distinguish between these three major encryption algorithm settings hints that it should be possible to detect cryptographic algorithms on much less capable hardware devices. Existing cryptographic key recovery attacks depend on prior knowledge of the cryptographic algorithm being employed.

Identifying what operations an IoT device is performing at the moment it is seized could prove important. The objective of this experiment was to train and test a machine learning model that can classify simple IoT firmware. In order for classification, ten Arduino programs were selected that repeatedly perform a task inside an infinite loop.

Data Acquisition: An Arduino microcontroller was programmed with ten different programs to detect. The HackRF was tuned to the information leaking 288 MHz frequency of the target device and sampled data at the rate of 20 MHz. Each program produced 600 EM traces, which resulted in 177 GB of data for the overall 6000 EM traces.

Data Preprocessing: This experiment attempts to classify 10 different cryptographic programs. From the extracted EM traces of each program class, 10 ms long segments were extracted and converted to the frequency domain. A 500 element feature vector did not seem to be effective in this case. Instead, it was empirically decided to create a feature vector of 1000 features.

Classification: A neural network with two hidden layers was designed to train and test the model to detect ten Arduino programs running on the target device. Under a 10-fold cross-validation, the classifier achieved a mean classification accuracy of 90% for an error margin of 11% within a 95% confidence interval.

A device with a modified firmware can cause malfunctions not intended by the manufacturer. Therefore, detecting such modifications to the stock firmware of an IoT device is highly necessary. It is possible to train a machine learning model to recognize anomalous EM emission patterns due to firmware changes. A one-class SVM with a non-linear kernel (RBF) provided by the scikit-learn library was used for this purpose. An Arduino program used in the software behavior detection experiment was used as the legitimate firmware of the device. Semi-supervised novelty detection by training a model with only the legitimate samples is decided the best technique.

When listening to radio frequency data with a SDR, large sampling rates are used to increase the amount of information captured. When this data is saved into files, the EM trace file sizes are considerably large even for small time windows. Thousands of such EM traces are required making the management of data extremely challenging. After capturing 600 EM traces per class, each of the trace files was down-sampled in order to create new sets of EM trace files that has various sampling rates. Using each data set (representing its unique sample rate) a Neural Network-based classifier was trained and tested.

When using EM-SCA for the live forensic analysis of IoT devices, real-time analysis is necessary. This is a challenging task since data preprocessing and classification tasks have to be performed within a tight time window. Even at the highest sampling rate of the HackRF SDR, processing delay does not exceed 40 ms, which is well below the TCP retransmission timeout.

When a computing device is subject to a digital forensic investigation, the major focus is directed towards the non-volatile storage of the device. Live data forensics can recover critical information such as temporary application data and cryptographic keys. However, this triage examination of a device is still a highly unreliable task compared to analyzing disk images. This is where EM-SCA techniques can help an investigator quickly assess an IoT device. Arduino and Raspberry Pi are representative of the two ends of the IoT device ecosystem in terms of computational resources. Further research is necessary to explore the methods of building generalised machine learning models to cover commonly encountered IoT devices in digital investigations. EM-SCA techniques can provide helpful directions for an investigator in order to uncover admissible evidence.

6.2.11.2. Deep learning-based EM side channel analysis. EM noise emission patterns from IoT devices can depend on a multitude of factors such as the type of processor and layout of the printed circuit board. This work uses 10 sorting algorithms each sorting a 100-element long randomly generated integer array. The randomness of the input data to the sorting algorithms ensures that their instructions sequences are different at each iteration. The EM noise of the processor is emitted from various regions of the chip across various frequency channels with varying amplitudes. When an H-probe antenna is placed closer to the processor chip, a weaker signal is observed with lower amplitudes and fewer frequency features [153].

With more powerful signal acquisition equipment, it would be possible to capture EM radiation from an increased distance. The data collection was performed in two phases with a time gap of 1 h between them. Even though the clock frequency of Arduino Leonardo is 16 MHz, it was empirically identified that certain harmonics of the frequency provide much stronger leakage signals.

The experiments conducted are outlined to see how well the prediction of the software activity a device is executing performs by just listening to the electromagnetic noise it produces. For each of the ten sorting algorithms, a time series of approximately 175 million raw samples was generated in the training session and 76 million samples in the testing session. Each time series was sliced into windows of consecutive time steps using a chosen time window, each of which would then be transformed into an input example through feature engineering. The first option is to transform each time window into the frequency domain by applying the Fast Fourier transform (FFT), which calculates the Discrete Fourier Transform (DFT) of a given time window. This drastically reduces the information taken by the classifier, but at the same time, it increases the computational costs.

For the deep learning model, a Convolutional Neural Network was used with four layers. The first two layers were two convolutional layers using 32 filters and 64 filters respectively. Large strides were used (2 and 4) e together with a max pooling value of 4 to increase the depth of field of each node in the first dense layer and to reduce the model complexity. The CNN model was trained with the standard Adam optimization algorithm.

The experiments demonstrate that ML models perform best when working on data in the frequency domain. One of the contributions of this work is that a consistent data recording protocol is necessary for machine learning models trained on past data to perform well on future data. In this work, this performance was achieved by fixing the location of the antenna with respect to the Arduino device. A window size of 2000 time steps (corresponding to an accuracy of 97.0%) is a sweet spot of achieving a high predictive performance of the trained model and having a low processing time. The exact antenna position during data acquisition to build deep learning models should be used consistently in an investigation scenario to acquire EM data from a target device.

The experimentation proves that it is possible to predict the activity that a device is performing from the generated EM noise with high levels of accuracy. ML classifiers are able to detect the executing algorithm even when the elements are ordered differently, which obviously requires a different order in the execution of the instructions of each sorting algorithm.

6.2.11.3. Evaluating the EMvidence framework. The EMvidence software framework is designed to be user-friendly for digital forensic investigators who are not typically EM-SCA experts. It comprises a central core with various default modules and the ability to install third-party plug-ins based on future needs. There are three basic software modules that are required for the framework to operate normally: the data acquisition module, the data visualization module, and the report production module. To manage software defined radio (SDR) interfaces, the EMvidence framework employs the GNURadio software library. This module supports two distinct techniques of data gathering [154].

Using interactive EM data gathering to profile a new form of IoT needs careful coordination between the SDR, device under test, and host computer. It can transmit commands to the target device via USB or universal asynchronous receiver/transmitter (UART) interfaces to initiate and terminate a certain task. Typically, a spectrogram is used to examine suspicious EM signals for patterns of information leakage. In this instance, an Fast Fourier Transform can be used to produce a spectrogram, a graph in which the x-axis represents observation time and the y-axis represents frequency. Users can analyze externally collected EM trace files by visually examining them with EMvidence.

EMvidence provides an application programming interface (API) allowing plug-ins to access fundamental framework features, such as providing access to real-time EM signal samples and saved EM trace files. When a user constructs a new machine learning (ML) model to recognize a certain software activity operating on a particular IoT device, this model can be readily integrated into EMvidence by encapsulating it with API calls to the framework.

Low-end and high-end IoT devices can be grouped by computing power. Power supply affects IoT device computer hardware selection. EM traces are vectors that show signal amplitude fluctuation over time. Signal acquisition hardware's fast sampling rates allow millions of data points in an EM trace lasting milliseconds.

The EMvidence framework supports and retains hash calculations for EM traces acquired in real-time. To confirm the forensic validity of EM data collecting and processing, the researchers plan to perform additional research in the future. EM-SCA based inspection of IoT devices can be useful for a number of forensic investigations. Numerous IoT devices lack standard interfaces, compelling investigators to employ riskier methods, such as chip-offs. Inadvertently erasing useful evidence from a device due to an error during such activities.

It is possible that EM side-channel mitigation measures might be incorporated into the firmware of an IoT device in order to deceive EM-SCA assaults. Increasingly, digital forensic investigations demand the extraction of digital evidence from IoT devices. The majority of forensically valuable information in IoT devices is presently acquired through intrusive hardware inspections. EMvidence is a framework that enables digital forensic investigators and researchers to use EM radiation from IoT devices. Experimentation has demonstrated that machine learning classifiers can be used to get relevant insights in IoT investigation scenarios.

6.3. Mobile devices

In the context of a case, an analysis of a call data record may be presented before the jury as a series of maps and tables, frequently accompanied with survey results. To safely understand data, competencies beyond just technical skills are essential. While survey responses yield factual information, the forensic conclusions formed from these data are prone to uncertainty and so generate opinion. Survey data should not be presented as a product in the absence of a broader evaluative framework or by a practitioner who has professional understanding of the artifacts under consideration (i.e. Call Data Records). The use of likelihood ratios is a widely established method for dealing with uncertainty in forensic judgement.

There is no universally acknowledged best survey method, and there are numerous types of surveying equipment available. Validation of the reliability of a method must address the accuracy and precision of the method, in addition to the equipment used. A vendor's test may establish with great certainty that their survey instrument functions identically to a mobile phone. Just because a survey instrument behaves like a phone does not imply that it behaves identically to other phones in use at the same location and time. It is a breach of the Forensic Science Regulator Codes of Practice to fail to comply.

As an End-User Requirement, the method's objective (i.e., what the approach is designed to accomplish) is specified. A common objective is to identify which cells can be expected to service a specific place at the time of the survey. This survey-specific user demand contributes to a broader need to evaluate whether the Call Data Records under consideration are consistent with the views made by the Prosecution and/or Defense (evaluative mode) or to provide speculative explanations for the data (investigative mode).

6.3.1. Movement and location

The digital traces left by a mobile device can reveal not just what the user did while the device was in their possession, but also what they did outside the device. They can estimate the timing of a traffic accident or the time since the user's last movement, for example (and hence presumably still was alive). The goal of this research is to locate digital traces of different types of phone motion in the iOS file system and in the files of several popular apps for the iPhone. It will be examined how well and reliably these traces can detect various kinds of motion. Information gleaned from this study can be fed into a Bayesian evaluation strategy [155].

The technique used to analyze digital traces indicating mobile phone motion has been refined, and it is quite similar to the one previously employed by the authors. Walking, driving, and brief loading (drop tests) were the movements examined here. Drop tests were conducted using a 4.95 m drop of a backpack containing three mobile phones. A calibrated watch was used to record the exact beginning and ending times of each drop.

The National Fire Institute (NFI) in London conducted a series of drop tests to simulate car-crash experiments. For each digital trace and over all movement- and usage-conditions, the proportion of correct registrations, incorrect registrations, and total registrations was calculated. Eight out of ten trials can be "properly" identified from a given digital trace if the True Positive rate (TPR = number of true positives/ total number of trials) is 80%. The False Positive Rate (FDR = number of false positives/(number of false positives + number of true positives)) is a measure of how often a device's motion detection system detects motion that is unrelated to actual device motion.

At an FDR of 20%, for instance, it can be inferred that 20% of the timestamps used to infer motion from digital traces are unreliable. The TPs are calculated by subtracting the timings of the experimental trials from the times of the trials for which digital traces were discovered.

Timestamped traces of phone movements can be extracted from log files related to WhatsApp and the iPhone system. For prolonged periods of phone movement, a number of consecutive registrations containing the text "app//shake" can occur in WhatsApp log files. This suggests there might be a connection with the shake-to-undo functionality on iPhones, which allows users to undo typing by shaking the phone. The file cache_encryptedC.db contains three tables with timestamped information related to phone movement: MotionStateHistory, StepCountHistory and NatalieHistory.

Each registration contains a timestamp in the form of the variable startTime, which is represented in Apple Epoch, i.e. the number of seconds since January 1st, 2001. It was determined experimentally by trial and error that the start of a period of movement can best be extracted from the table MotionStatehistory from the value of startTime of a registration. The table StepCountHistory contains information on number of steps and distances travelled. The start of a period of movement can be extracted from this table using the value of the variable firstStepTime. Alternatively, one might look at the variables count and distance themselves and look for two consecutive registrations for which these two variables both have the same value.

This method is called Advanced Stepdetection. Movement of the telephone can be detected in the table NatalieHistory by setting a threshold value on the variable mets (metabolic equivalent task). Different types of movement require different threshold values. Table NatalieHistory contains a number of equally cryptically named variables which contain information relevant for movement detection of the phone. Data retention in the table NatalieHistory was estimated by analyzing timestamps from different instances of the file cache_encryptedC.db, obtained over the course of this research.

The averaged accuracy of the start- and end time of periods of movement in walking and running from traces in WhatsApp log files is estimated to be about 30–40 s. Assuming false positive registrations only occur when WhatsApp is in the foreground and when the phone is unlocked, leads to an estimate of the false discovery rate FDR 1⁄4 18/(66 â‚¬18) 1/4 21%. The time history of the variable mets during a number of walking and running trials was determined experimentally by trial and error. Average accuracy of detection strongly depends on the usage condition of the phone: when the phone is unlocked, detection of periods of movement is much better than when it is locked.

The data show no big differences between the three phones with respect to the accuracy of movement detection. It was found that mets averaged over the period of movement in walking ranges between 2 and

6 (mean: 4, n ¼175) and in running between 8 and 13. This suggests that higher averaged values of mets may be indicative for running, while lower ones can be indicative of walking. More research is needed to further substantiate these provisional conclusions. In driving, the variable mets is found to alternate between its baseline value of 0.889528 and 1.30000 (with some variation in subsequent lower digits). It seems that shorter stops during driving cannot be detected from these digital traces. The registrations in iPhone 8 and iPhone X were much more reliable than those in iPhone 7 Plus. Drop tests produce a single registration with the text "app//shake" in WhatsApp log files. Repeated drop testing produced damage to the exterior of the phones, but not to such an extent that no data could be extracted.

Both WhatsApp logfiles and the file cache_encryptedC.db contain a number of intriguing and surprisingly detailed traces on phone movement. For some of the traces, especially the ones from cache_encryptedC.db, their origin and meaning are unclear. Most likely, they come from sensor information from the phone, but what processing has taken place is unknown. It would be good for appreciating the digital traces, when other types of movement (e.g. riding a train or bicycle) are investigated as well.

6.3.2. *Evaluation of location-related evidence*

It is possible for forensic practitioners and decision-makers to misread mobile device location data. The ability of any data to provide precise information on the location of a mobile device depends on the technology, the context, and the analysis technique employed. This study aims to familiarise digital forensic practitioners with the fundamentals of a fair examination of mobile device evidence. It contends that a defined scientific interpretation framework contributes to a more transparent appraisal of data and associated conclusions, and informs all parties to the potential need to address further concerns [156].

Location-related evidence comprises information created by the operation of a mobile device based on its geographic location. It might be highly specific, like the longitude and latitude provided by the Global Positioning System (GPS), or more general, like an area, geographic region, or country. The accuracy of the data must be assessed seriously, and the determined position is reached by a forensic practitioner or expert information recipient. The location methods used by mobile devices will rely on the technologies and network data obtained. GPS needs the usage of four or more satellites for positioning.

Other technologies are available, including Bluetooth and phone sensor-based approaches. In metropolitan locations, the accuracy can range from 10 to 100 m, whereas in open areas, it can be between 5 and 10 m. The accuracy of such data depends on a number of elements, such as the available information sources (GNSS, WiFi, Cellular Network; Bluetooth, sensors), the operating system, and the application seeking the position. Depending on the localisation algorithm, triangulation-based localisation has an accuracy of 0.4–4 m, whereas trilateration-based localisation has an accuracy of between 5 and 40 m. Location-related data is highly reliant on a number of variables, including network distance, signal strength and direction, atmospheric conditions, and obstructions such as buildings and trees.

Mobile devices may determine their geolocation using a technology that is available but less precise, such as WiFi location. One study examined the accuracy of Google Timeline under various conditions and forms of mobility (e.g., automobile, bicycle, tram, strolling) and discovered that 52% of the time GPS location was accurate within the circle provided by Google. Android granted developers access to GNSS raw data in 2016, allowing them to create applications that provide extremely precise localisation.

Depending on the number of access points accessible in a given place, WiFi location algorithms may have varying capabilities. A 2012 study revealed that a hand grip can cause a range inaccuracy of 9 m when the smartphone is 3 m away from the access point. Bluetooth localisation depends on the distance between the mobile device and the beacon as well as the number of beacons in the vicinity.

Evaluation of forensic evidence adheres to scientific interpretation norms. Location X is assumed to be a well-defined place or region where mobile devices perform identically with respect to geolocation measurements at every point inside the region. This is an oversimplification, but the purpose of this study is to illustrate the notion behind the interpretation of location-related information. A crucial feature of creating propositions for evaluation is that they should provide the assignment of probability to the data given the propositions of interest. Comparing the possibility of a mobile device connecting to this particular cell tower if it was in an abandoned house versus the victim's mother's residence is made possible by measuring and testing.

The case conditions could be rephrased as follows by a forensic evaluator: The body of a murder victim was discovered at Location X, but the suspect (Ms. A) maintains she was at Location Y, which is unrelated to X, when the alleged crime occurred. Her mobile device was operational, with connected calls and sent messages, as evidenced by her phone records, and she did not deny possession of it. The likelihood that Ms. A's mobile device was operating near Location X at the relevant time (Hp) is close to 1, indicating that there is no credible reason to believe that location data for Location X will be located in the database of the telecommunications service provider or on the device. Given that Location X and Location Y are unrelated, it is reasonable to assume that the probabilities of observing each location are independent.

In actuality, this case exemplifies the difficulty of judgement when an alternative defence theory is extremely uncommon or even impossible. The forensic evaluator is responsible for determining if a qualitative likelihood ratio is applicable in a certain circumstance. Given that Mr. A's mobile device was at Location X at the relevant time, it is deemed the findings in this instance to be substantially more probable than if Ms. A's mobile device had been at a different location.

Even if the recovered data are deemed accurate, extra investigation may be necessary to confirm if the device's owner was using it and was in the same place. According to the forensic evaluator, the observed location-related mobile device evidence correlates well with what would be anticipated to be found if the mobile device was in the vicinity of Location X and operational at the time in question. The case circumstances determine the probabilities that Ms. A's mobile device was at Location X while she was elsewhere (P) and that someone else discarded the victim's body (Hd). When committing a premeditated offence, perpetrators may be expected to turn off their mobile devices or not even carry them with them.

Examining location-related mobile device data in relation to higher-level hypotheses, particularly regarding alleged actions, necessitates considerations that extend beyond a technical understanding of the qualities and operations of technological equipment.

Increasingly, location-based mobile device evidence is used to answer forensic issues in criminal investigations. In order to minimize errors and misinterpretations, this evidence must be thoroughly assessed from a forensic standpoint, taking into account its accuracy and reliabilit.

Evaluation of location-related mobile device evidence and evaluative reporting in this forensic discipline are difficult due to the vast array of technological nuances that may interact with complex case circumstances. This form of digital evidence is susceptible to misinterpretation by both forensic practitioners and legal decision-makers due to these obstacles. To reduce the likelihood of misinterpretations and, consequently, misleading digital forensic conclusions, it is essential to evaluate location-related mobile device data systematically. This paper proposes that evaluation should rely on a paradigm that clearly distinguishes between what has been observed (i.e., what data are accessible) and how those data can inform uncertain target propositions, such as "Was the device operational at a certain place throughout the relevant time period?"

The proposed, structured perspective also emphasises that the types of questions that are appropriate for forensic practitioners to answer are of the form "What is the probability of observing this data if a particular allegation is true?" This leaves legal decision-makers to render direct opinions regarding the truth or falsity of particular allegations (i.e., propositions). This is due to the fact that conclusions on specific rival versions of the case require more than just location-related mobile device evidence. Indeed, as has been demonstrated, logical and balanced reasoning beyond propositions regarding a device's position at a given time, such as propositions about where a person of interest was at a given time or alleged activities in which the person of interest was involved, requires case-specific information that is most appropriately provided by an investigator or judicial authority who oversees the entire body of evidence in the case.

While this study focuses primarily on factors affecting accuracy, it is imperative that future research on the evaluation of location-related mobile device evidence address broader authentication difficulties (e.g., errors caused by evidence tampering or flawed forensic software) as a critical topic. This is analogous to the interpretation of DNA profiling results, which, based solely on conditional genotype probabilities and disregarding the possibility of error, is insufficient and may overestimate the value of DNA evidence.

This research presented a robust evaluation framework commonly employed in forensic science and examined the benefits and challenges of applying this methodology to location-based mobile device data. This study assists digital forensic practitioners in adhering to the concepts of balanced evaluation and communicating location-related mobile device evidence in a manner that permits decision-makers to comprehend the relative strength and limitations of digital forensic results.

6.3.3. *Cell site analysis*

Survey data cannot be used to make safe inferences unless they are embedded in a larger framework [157].

- The forensic strategy employed within the context of the survey is case-specific and may vary based on the examination's broader objective.
- The employment of survey equipment is a component of a broader survey method (i.e. the equipment is one part of a process, how the equipment is used is also important to that process).
- Survey data is susceptible to uncertainty, which a practitioner must comprehend. Survey information is combined with other data to generate a technical judgement.
- Dangerous and unsuitable is the presentation of technical opinions regarding the service of cells as a series of isolated observations made in isolation from each other and the larger objective of the study. The survey must be included into a larger process that addresses whether the Call Data Record would be expected given the prosecution's and defense's perspectives, or to propose possible explanations for the data if operating in an investigative capacity.
- While survey data may be "fact," inferences formed from them are not. Therefore, survey data should be used to inform rather than define opinion.
- Survey data can be used as part of a "presumptive test," for example, to highlight those cells observed to serve at a location; however, if these results are to be used as evidence (e.g., presented in court), they should be evaluated in the context of the issue to be addressed by the court, which will consider a broader range of information than just technical observations. As part of the evaluation of the entirety of the call data in the Call Data Record, this should assess whether the call data may be anticipated given propositions, for instance utilizing the AFSP standard for evaluative evidence.
- There is a risk in believing that because a survey instrument behaves like a mobile phone, it would behave similarly to other phones being used at the same location and time, or more pertinently, as the suspect mobile phone did at the time it created the Call Data Records under consideration. This assumption is plainly untrue and must be avoided.

As part of a broader evaluation of the call data against the given propositions, survey data can be used to inform opinions of whether or not various cells serve at specific locations or to provide an estimate of their coverage areas. For safe inference, uncertainties in the data analysed must be identified, quantified as much as possible, and then accounted for in the evaluation of the unique case conditions under consideration. Experts must also be aware of the uncertainties in the survey data and Call Data Records. As far as the authors are aware, there is no such thing as a flawless survey approach, hence limitations of methodologies used should be quantified and accounted for if used to provide an opinion on the broader call data.

Engineering handsets are an established method with intrinsic credibility over other survey tools because they are mobile phones and so function as mobile phones, and the majority of cell site analysis exercises take into account data generated by mobile phones.

However, there is a hidden danger in accepting such material at face value. The fact that a survey instrument behaves similarly to a mobile phone does not imply that it behaves similarly to another phone being used at the same location and time, or more pertinently, as the suspect mobile phone did at the time of the calls under consideration. As a phone can only select a single cell at a time and prefers to hold onto it, it is susceptible to incorrectly rejecting genuinely serving cells. This is true for both the suspect's phone and the engineering handset used for the survey. Aspects of this limitation could be handled by locking to carriers, for instance, but even this solution does not completely resolve the problem, as illustrated by the stochasticity analysis (for which only one set of carriers were used). Locking is also time-consuming and has a greater potential for mistaken inclusion of non-functional cells, according to anecdotal evidence. An obvious advantage of an engineering handset is the ability to measure coupled mode cells, which cannot be replicated by Software Controlled Radio.

The use of Software-Controlled Radio for forensic cell site analysis is a novel technique designed to address these deficiencies. The ICS-500 features distinct benefits and drawbacks compared to conventional handsets. Although there is no assurance that this equipment will detect all cells, it is capable of monitoring multiple carriers concurrently. The ICS-500 was more dependable than Nemo handsets at detecting stacked (overlaid) cells. Utilizing survey data for superimposed cells demonstrably reduces the probability of false-negative exclusions of actually serving cells. While it is possible that Call Data records may occasionally offer data with inaccurate azimuths, failure to account for superimposed cells in an analysis is also a clear source of potential mistake. Use of additional network information (cell queries) and/or analytics to identify overlaid cells is thus an apparent method for reducing the false-negative rate (N.B. even this would not have reduced the false negative rate for use of survey results to zero). The ICS-500 is more useful than an engineering handset for preventing cells from potentially serving at a certain place. There are numerous aspects to this, including the following:

- The ICS-500 monitors multiple carriers concurrently and also displays data for cells that are considered but not identified as "top cells." There is more data directly accessible than within the Nemo data set.
- There may be specific fields within these additional data that provide better confidence of "non-service." On GSM, for instance, the ARFCN of the cell of interest could be decoded as belonging to a different cell at the location of interest. Under these conditions, it would not be prudent to use the original cell under consideration in the Call Data Recordat that place; the ICS-500 decodes and delivers this type of data more reliably.

Therefore, the authors advocate deploying engineering handsets and SCR devices together whenever possible. This makes the "best of both worlds" approach particularly useful when the outcomes are distinct. This may not be always attainable (for example, there are many networks and technologies under assessment and there are not enough engineering devices available to deploy). Under these conditions, the ICS-500 does not produce obviously "false positive" results; therefore, the authors believe that the survey data can be relied upon, with the possible exception of the edge of service, where the authors believe that the data should be considered in fine detail as part of an expert assessment.

6.3.4. Roles and interpretation

Cell Site Analysis is referred to as an "art" by some and as "engineering" or "science" by others. Cell Site Analysis is focused on the assessment of data resulting from mobile device technology. It can be approached in the manner of forensic science and is defined in terms of processes. The question of whether a practitioner refers to their analysis as art, engineering or science is less important than whether they are presenting expert evidence [158].

Material can be understood in various ways, and each interpretation demands a certain set of skills, knowledge, and comprehension. Competencies do not necessarily transfer from one method to another. An example of "conventional" forensics would be when a practitioner prepares a sample from a suspected drug seizure and applies a proven process to obtain results that are typical of cocaine. The technological interpretation of the Call Data Record necessitates an understanding of the inherent uncertainties in its analysis. There may be only one plausible explanation for the call occurrence, so despite the technical complexity of the analysis, the test result will be factual (deductive) and devoid of opinion.

Estimating the service area of a cell, for instance, will depend on the practitioner's expertise and understanding of network configuration, radio wave propagation, and other information from technical processes used to assist the analysis. In this function, findings are used to determine if the data would be expected based on one or more hypotheses. Evaluation of two or more hypotheses is known as evaluative interpretation. For the sake of this study, this has been categorised as a form of "forensic interpretation" due to the fact that case circumstances will alter the view rendered. An expert's responsibility is to evaluate the scientific findings in relation to the offered scenarios, allowing the formation of an opinion and (if there are two scenarios) the statement of support for either proposition. An example of a deductive conclusion using Cell Site Analysis could be the study of call data with a vast spatial dispersion of cellsites in order to derive a general judgement regarding the mobility of a device over a significant distance.

The admissibility of an expert's testimony in court is determined by a number of variables, including their expertise, knowledge, and comprehension. An expert may be required to present opinion, fact, or "technically interpreted" evidence, as well as technical explanations and "factual" information. If the practitioner lacks the proper knowledge and understanding for the role in which they are operating, there is a risk that the evidence presented will be erroneous, incomplete, or deceptive. The court may be misled if only data that supports one theory are presented, or if additional data from a comparable period but not from the region of interest are not disclosed.

A practitioner's evidence is less likely to be erroneous, incomplete, or deceptive if he or she follows a method that has been adequately specified and does not need interpretation of the outcomes. It is typical for an expert in Cell Site Analysis to alternate between these modes (factual, explanatory, technical, investigative, evaluative). If the distinctions are not acknowledged and acted upon, there is a greater chance that there will be problems with the evidence provided.

It is essential to avoid or eliminate situations in which practitioners are asked, expected, or required to provide opinions on topics outside their expertise. It is improper and misleading to ask a witness giving technical "fact" evidence to interpret results in the context of a case, as this may need additional knowledge and comprehension. A witness who is not recognized by the court as an expert may be permitted to comment using "common sense." Accreditation may address components of this to ensure implementation and adherence to a suitable competency framework. Individual performance can also be evaluated using Blind Trials, where the truth is known and the expert's judgement is calibrated against (a) the actual truth for accuracy and (b) other experts for precision. As always, the judiciary plays a crucial role by recognizing and examining the procedure by which the witness's areas of competence and type of expertise are selected.

6.3.5. Android

Mobile devices are prone to forensics investigations since they hold a great deal of sensitive personal data. The average storage capacity of smartphones is predicted to increase by 80 GB by the end of 2019. The researchers investigated preprocessing techniques that organise data based on apps and to find potential evidence using Android's characteristics. There is a need for research to successfully identify crime-related mobile applications and those that store user information in their app logs. Potential evidence may include files relating to various apps for a suspect's particular activity, which may necessitate cross-analysis when examining a timeline [159].

The taxonomy of Android data and how to manage data identified as potential evidence on an app-by-app basis was investigated. As the number of Android users continues to swell, researchers are analysing the logs of popular apps such as social networking, message, map, and navigation. To preserve user privacy, applications such as Telegram, WhatsApp, WeChat, and KakaoTalk that feature app log encryption and data deletion have been introduced. The purpose of these studies is to analyze user behavior and account data by carefully examining each app. Efforts are currently undertaken to identify app-related files and evaluate the data contained within them using taint analysis and data flow analysis techniques.

By examining the app's behavior, these studies can be used to investigate malware detection and app vulnerabilities. Malware detection research primarily employs taint analysis to evaluate app behavior. For malware detection and vulnerability analysis, taint analysis or flow analysis of APKs is extremely beneficial. EviHunter has the disadvantage that it takes longer than Fordroid to examine an APK, and the majority of files are stored in the static path. People use an average of 339 apps on their test Android phones in their daily lives.

Application Profile XML (APXML) is a data abstraction standard for detecting and organising application usage evidence in a variety of investigation settings. It is the first step of a Unified Cyber Ontology (UCO) and was created using the Cyber Observable eXpression (COX) (CybOX). CybOX is a schema designed with the identification of cyber-attack patterns and cyber threat intelligence in mind. The authors examined the Android data taxonomy, which differs from earlier studies. It is comprised of file system metadata and Merkle-tree hash values from the files associated with each operation that use an XML structure. This taxonomy classifies app logs based on the app attributes information and the file holding user behavior information's internal structure information.

Each program saves the specifics of a user's behavior in its log (often files in SQLite database format) together with time stamps. If an action produced a file within the file system, the file can contain information about the file. Consequently, investigators can investigate not only incomplete user actions inside the application log, but also files created or modified as a result of the activity. Android's security design grants each app a distinct process with a unique identifier and sandboxes access to only their data. Some applications may need to use system services, access data from other applications, or generate data on the SDcard.

Android allows the program permission to do specified activities only if the necessary permissions are declared in the APK file using the uses-permission > key. These files include log files recording user action details, which are essential from a forensics perspective, as well as everything required to run the application. For apps whose AIDs for using system services are set to GIDs, there may be files that retain the history of using those services or, if necessary, files containing data from other apps. Under Locard's exchange principle, the user's activity within the application leaves traces within the app's linked files.

By identifying and cross-analyzing all of these files, it is possible to examine their genesis, causal link, and date. This procedure enables the abstraction of Android's data into Files/Groups. Almost all of Android's files are SD card files (36.13%), program logs (7.59%), and app installation files (54.63%). Targets of analysis include files associated with applications that can be used as criminal tools.

Investigators can examine all of the files on the SD card to determine if they were photographed illegally. Multimedia file formats such as JPEG and MP4 are the primary focus of examination in cases of illegal photo/video capture. PEGs incorporate as many groups connected to the type of crime as possible; nevertheless, some of these categories may be unrelated to the crime itself. The false-positive ratios were decreased for these incorrectly recognized categories by implementing two procedures: First, files based on their signatures and identified groups containing files that required analysis were categorised. Second, files in the SQLite database format were evaluated to find objects containing user data such as timestamp, ID, and geodata. SQLite, APK, and log files are the file formats most frequently evaluated for user behavior analysis. Leaks of confidential information typically target document file formats such as PDF and OOXML (DOCX, XLSX, PPTX, etc.) for analysis. Typically, JPEG and PNG files used as cache by camera and web applications do not have extensions. To appropriately choose the files under enquiry, all files in the file system must be categorised according to their signatures.

Typically, application logs are recorded in a log file in the SQLite database format with a timestamp. Other file formats include those made by users using photo and video-taking applications and those obtained via web browsers, email clients, and instant messaging applications. By finding and retrieving the user information remaining in the app log, forensic researchers examined identifying the files required for user behavior analysis. There are five different categories of user data: timestamp, ID, Geodata, URL, etc. Timestamp types consist of three Unixtime formats (second, millisecond, and microsecond), Google Chrome Time, and many text formats (YYYY-MM-DD HH:MM:SS, etc.). The formats that correspond to the ID type are those that may uniquely identify an individual for each app log event.

The overall approach for investigations provided in this paper is represented by the authors' Algorithm 3, which comprises six steps. It accepts an Android image file and generates an AFXML including data from prospective evidence. The application examines the system logs and organizes all files into the image file. The Investigator compiles a PES by accumulating potential evidence app-by-app. It examines all SQLite database files to determine which ones contain user data.

This can detect the essential application logs among the PES components. Due to the complexity of this case, the timeframe is outlined below. In the experimental scenario, the investigator determined that B was stalking A by physically accessing A's smartphone, archiving all of A's messenger conversations, and emailing them to him/her. Since A's workstation was the site of the CCTV cameras, the investigator reviewed the video files of the CCTV footage and discovered that B used A's phone while A was absent. The time corresponded to when KaKaoTalk's backup files were produced and transferred to B via Gmail.

The resultDB database file is built to hold the analysis results. It comprises tables that include metadata such as inode, type, file path, timestamp, etc. for each file in the file system. The outcome of the grouping is placed in the tsk files table of the loadDB file by adding the column id package.

6.3.6. Android encryption database

There are several ways to identify and analyze encrypted databases generated by various apps. This paper proposes automated forensic analysis of Android applications through static analysis. The method overcomes the shortcomings of manual reverse engineering and dynamic analysis of encryption methods. It requires no human intervention and takes less time. A static forensic method between components for Android applications automatically recognized the database encryption method [160].

One hundred Android applications are tested with the method as well as other static analysis platforms. The experimental results indicate that the method is more accurate and requires less time compared with the other existing frameworks. This is the first study to apply digital forensics for Android applications with an aim to automatically identify the encryption scheme of Android application-derived databases. This method can be used to analyze any Android application. The database file location of the WeChat application was discussed.

To explore the encryption program path of the database generated by Android applications, an algorithm framework was designed. The framework consists of two functional modules that establish the inter-component data flow graph and inter-component control flow graph of the analysed Android application. It then uses Amandroid to decompile the Android Application Package and build the data dependency graph and control flow graph for each component. The search results are output to a report in the form of information on the program path that the Android application may adopt.

Manual analysis yielded unsuccessful outcomes. The comparison demonstrated that the majority of failure paths occur on components with numerous target intents, a shortcoming of the probability model used to solve inter-component communication problems. The probability model selects the most probable target component, resulting in the omission of several genuine target components and a lack of reporting.

For Droid-Bench, the probability model has a greater accuracy of 73.6% than ICCTA and PRIMO (two well-known intent target component inference tools); in this instance, the method identifies more genuine intentions than ICCTA and PRIMO. The amount of intent links that the method can discover is comparable to that of other technologies, but the method is more accurate. Using a probability model, the strategy significantly minimises the number of false intent linkages.

The method successfully determines the encryption method of 584 databases with an accuracy of 82.9% and realizes the decryption of these databases. However, the analysis method still has limitations, mainly in the reverse analysis of the app program. Most of the current app programs have mature anti-reverse methods such as confusion, which is problematic for the static analysis. In addition, Android programs often call the code of the Android environment, but analysis focuses on the internal code of the program.

6.3.7. LG content lock

Some smartphone apps hide and encrypt personal data for service purposes or store it in a secure location that requires root rights. Data masking and encryption protect privacy but hinder digital forensics. Developers implement encryption differently. To facilitate digital forensic inquiry, the analyst must assess each unique technique. The security of sensitive personal information is performed not only by apps, but also by smartphone manufacturers. LG's 12% US smartphone market share ranks third. This study examined LG smartphone system apps. LG claimed it would continue to serve smartphone consumers after closing its mobile division in April 2021. Thus, this LG smartphone research remains relevant. LG smartphone system apps include Content Lock, QuickMemo, and Gallery. Content Lock authenticates users, and other apps lock content using it. Both apps employ Content Lock to protect memos and multimedia files against unauthorized access [161].

No application version demonstrated differences in algorithmic performance. Each app's locked content remains on the main path, so anyone can see if it's locked. All locked data could be acquired without rooting. Locked data could be acquired without destroying it on unrooted handsets. Content Lock does not encrypt the app. It merely verifies credentials and returns the result to the application that called the Content Lock App using Content Lock. QuickMemo+ and Gallery hide or encrypt data if verification is True. Content Lock App authenticator production and verification phases were detected as were cryptographic hash algorithms for PINs and point substitutions for patterns yield authenticators. Using authenticator generation methods, user PIN or pattern were found. System application attributes were used to bypass verification. QuickMemo+'s database and objects hide data through the Content Lock. QuickMemo locks a memo by moving it from local shared storage to local storage and preventing non-root access. Unencrypted QuickMemo+ is locked, therefore QuickMemo + artifacts were examined and a method created for unlocking data. Deleted notes were recovered; Gallery holds multimedia files encrypted with a Gmail encryption key for which a multimedia file encrypts that Gmail address. Multimedia files can be decoded without additional data. LG devices can access originals for data hidden or encrypted by system programs without specific knowledge.

6.3.8. Smart watches

Smartwatch devices are attractive for both personal and professional use, with a large number of different applications managed from the connected smartwatch. There are companies such as Apple, Fitbit, Xiaomi, Garmin or Huawei, which have the most important share in the business of smartwatch devices. Smartwatches are not used as primary means in the execution of a criminal act, although they can store relevant information. Low cost smartwatches execute a real-time operating system (RTOS) e.g. "Nucleus RTOS" which manages and stores the information in a different way. This kind of devices, in general, requires a different forensic analysis methodology. In the study, it is estimated that RTOS smartwatch market will have a growth by 2020 only exceeded by "watchOS" and "Android Wear" [162]. Previous studies have focused on the study of high-end smartwatches and analysis of artifacts that can be found in their operating systems "watchOS" or "Android". Many of these studies perform a brief analysis of the artifacts that are stored in the smartwatch.

Low-cost smartwatches as the three smartwatch models analysed are based on a RTOS that provides the basic capabilities necessary for the management of the device itself. Because "Nucleus RTOS" is a proprietary and closed-source customized version, the stored information must be studied by reverse engineering. This paper tries to answer different questions related to the data stored inside the smartwatch and that may be useful in the investigation of criminal acts. The forensic methodology followed is based on the comparative analysis of the artifacts obtained from each of the tested smartwatches at a certain time. Each item studied in the forensic analysis has been evaluated through three phases (followed sequentially for each smartwatch).

Smartwatches with MTK chips usually have a reduced storage capacity, being in many cases less than 4 MB. These memories are usually NOR flash memories, which have "wear leveling policies" and "garbage collection services" running in the Flash Translation Layer (FTL). The "wear leveling policies" distribute the information through the whole memory space, reallocating logical sectors to different physical sectors. The "garbage collection services" will then re-structure the information indicating which of those sectors are marked as occupied or free. Although these processes improve the efficiency and useful life of flash memories, from a forensic point of view it can result in a loss of information when a restructuring of the memory occurs, overwriting parts. The acquisition of this information requires the connection to the different pinouts of the JTAG port located on the PCB. Due to the size and location of these pinouts, this operation can be quite laborious and should be done by a specialist. "FlashTool" application is developed by "Mediatek Inc" to do updates and backups from their MTK chips.

It can be assumed that the acquisition process with the Read Back option makes a valid read operation, without writing the device memory. If the device is switched on, the forensic specialist can introduce a series of codes to access different configuration menus which provide more detailed information about the current smartwatch.

UFED Physical Analyzer is used to analyze the data on the different low-cost smartwatches. A series of "chains" or processes that help the forensic specialist to quickly process the data information available. The chains execute a series of scripts to perform the decoding of the information, among which is "MTK NOR", corresponding to the type of memory of the devices analysed. The analysis is carried out by means of the "Open (Advanced)" option from the "File" menu of this forensic tool. "R-Studio" tool has been used to validate the information obtained from "UFED Physical Analyzer" in the forensic analysis of different device acquisitions. This tool is commonly used by forensic analysts to acquire the device file system and file structure.

Files "NO NAME/@BTDIALER" and "ENTRY.TMP" contain the records related to the contact list of the linked smartphone device. A contact name in the phonebook of the connected smartphone can be identified and the phone number are also distinguished. It has been concluded that from the analysis on the file system of the different smartwatches, an identical copy of these data files exist.

Inside the directory "NO NAME/@BTDIALER/" is the file "FOLDER. TMP", which contains among other, the information related to the calls log. It has been concluded that from the analysis on the system of files of the different smartwatches under study, an identical copy of these files exists. The calls log located in this file are structured using the "BEGIN: vcard" and "END:vCard" tags, which can be found in the call registration (name, phone number, date, type of call registration, etc.). Several call logs contained in the file are located.

Text messages are stored in different files with nomenclature {number}".O" which are stored inside the folder "NO NAME/ @SMSBTMAPCSRV". All text messages can be stored in a single file, "msg_btmapc_node.O" located in the same folder as the call records. It is straightforward for the forensic specialist to extract the data from this structure.

The file "bt_notify_0000. xml" located inside the folder "NO NAME/ @BTNofity" is an XML file that stores the data about the last received notification on the smartwatch device. This file, among other fields, contains a numeric identifier (handle), date of dispatch (datetime), name of the application or number that sends the notification (sender_name) and the type of notification (type).

The amount of information stored inside the smartwatches implies that they should be subject to study by forensic specialists. The acquisition and forensic analysis of this type of device can be critical, when, for example, a Smartphone is blocked or damaged and the information can be extracted from its linked smartwatch. Embedded devices such as these can store contact data, call records, instant messages, multimedia files and so without requiring access to the connected smartphone.

6.3.9. Damaged devices introduction

Digital forensics labs have attempted various techniques to extract data from digital devices. A mobile device typically consists of a screen, a circuit board, a housing case, peripheral components (cameras, antennas, sensors, etc.) and a battery. A printed circuit board (PCB) is typically used for the circuit board in a mobile device.

A mobile device typically consists of a screen, a circuit board, a housing case, peripheral components, and a battery. In a working mobile device, the circuit board controls the operation of the connected components and continuously draws power from the battery. All of the processing that takes place among the components on the PCB is in the form of electrical signals. Electrical components such as resistors, capacitors, and IC chips are bonded on the electrodes of the PCB by solder. Solder is a metal alloy containing multiple kinds of metals, such as tin, silver, and copper. With the ever-shrinking size of digital devices and components, the distances among biased components on a PCB are minimized.

6.3.9.1. Water damaged devices. Digital forensics labs have attempted various techniques to extract data from digital devices. The most common scenario regarding water damaged devices is that the device does not boot properly after cleaning and drying. Chip transplantation or chip-off are the only options to forensically analyze the device. Water damage to digital devices by water submersion can be viewed as the most extreme example of humidity-based corrosion. For those devices, proper identification of faulty parts could lead to performing restoration of the target device [163].

6.3.9.2. Metal corrosion in digital devices under humidity. The most common corrosion observed on a PCB in a humid environment is electrochemical migration (ECM). ECM happens in the presence of a potential bias between two conductors that are connected by a fluid media. Since metals continue ionization, the electrode loses solid metal, which leads to an open circuit. When digital devices are submerged in water, the water works as an electrolyte conduit among different kinds of metals (Novotny et al., 1987). The movement of electrons makes current flow between two metal electrodes. As a result, the combination of those different metals and water creates a simple battery cell. Another type of corrosion that reportedly occurs on PCBs is called conductive anodic filament (CAF). CAF is a copper containing filament that grows inside a PCB under the presence of moisture. Once the filament reaches the cathode layer, a short circuit is created inside the PCB, which leads to system failure.

While submerged, all the tested devices were covered with small bubbles which is the clear sign of hydrogen production. On two phones, battery connectors and components directly connected to the batteries are severely corroded. Electrical condition of PCBs after water submersion can be affected by the presence of contaminants on those devices. Dispersive X-ray spectrometry was used to analyze the contaminants.

Some of the devices did not boot successfully when they were connected to a DC power supply. Solder abnormalities were found under some IC chips. On other devices, normal current flows were monitored on both devices after cleaning and connecting the power source. After connecting the cleaned PCB to the battery, display, and other peripheral devices, some devices successfully booted and operated normally.

The state of charge of the battery in a digital device when it makes contact with water is one of the factors critical to the level of water damage. If a mobile device PCB is connected to a battery, constant voltage is applied to the PCB until the battery level becomes empty or the battery is disconnected. When a digital device is submerged into water while it is operating, metal corrosion by ECM is promoted much quicker than when it is switched off. After two weeks of submersion, the metal corrosion becomes severe and electrical parts are detached from the PCB. Chip-off or chip transplantation is the only option for recovering the original function of the device.

6.4. Motor vehicle digital forensics

Regulations and emerging new business and service models are driving a significant transformation in the automobile sector. As modern motor vehicles integrate an increasing number of computer- and software-based components, it may be conceivable to transfer some or all digital forensic methods to the field of digital forensics of automotive systems. It is just a matter of time before digital forensic investigations are required to resolve security incidents involving vehicles. Previous authors presented a data collection model for autonomous vehicles in smart cities. They collected data from the Electronic Control Modules of the vehicles, as well as smart city data (which includes data hubs, Global Positioning System, and cellular information). The collected information was subsequently hashed and encrypted to assure its integrity and authenticity. In one scenario, diagnostic problem codes were obtained via On Board Diagnostics [164].

Automotive forensics seeks to answer a question posed by a stakeholder on a particular event, such as an accident. The results of automobile forensics should address the six Ws: who, why, where, when, what, and how. This study focuses mostly on security-related issues as opposed to accident reconstruction alone. The entity responsible for manufacturing and distributing a vehicle as a product is known as the Original Equipment Manufacturer (OEM). Any party involved in the development, production, or supply of components or services associated with an OEMA-produced vehicle.

Two types of forensic investigation applicable to automotive forensics are Live Forensics and Post-Mortem Forensics. Five groups of data are normally acceptable for forensic investigation, as determined by an analysis of multiple vehicle components. These include firmware, communication data, user data, data pertaining to safety and security. Firmware is the sole software component put on an Electronic Control Unit. An study of firmware data is suitable for detecting modifications to Electronic Control Units (e.g., manipulation, feature addition/reduction).

Communication data consists of any information delivered within a vehicle and from it to any other recipient. Data transmission may use internal bus technologies and protocols in addition to standard Information Technology (IT) methods. Use of new protocols (such as Scalable service-Oriented MiddlewarE over IP and Diagnostic Over Internet Protocol) increases the complexity of vehicle communication. The necessary storage space for Tesla and Audi navigation systems will increase from 5 GB in 2018 to 10 GB in 2020. MSAB's iVe car forensics solution enables the collection of such data from infotainment systems.

In nations such as the United States, Korea, Japan, Switzerland, and Uruguay, it is mandated that automobiles be equipped with devices that record information regarding safety-critical occurrences. The size of the Electronic Control Unit did not change between 2011 and 2019. Electronic Control Units, unlike the previously mentioned Event Data Recorder, do not have centralized storage for security occurrences. 1 min of uncompressed, 30 frames-per-second (FPS) High Definition (HD) video consumes an estimated 150 MB of storage space.

Modern vehicles are equipped with cutting-edge technology advances and may exchange data with other vehicles, infrastructure, pedestrians, and the network. The Internet-of-Vehicles ecosystem is a crucial source of digital forensic evidence due to the huge quantity of data it contains. For the future development of forensic capabilities for driverless vehicles, several academics believe that new approaches must be backed by the forensic-by-design idea.

Modern automobiles include rather large volumes of stored data (information) that can be used to identify the vehicle. Identification of any object (vehicle) can be broken down into two basic groups for civil and administrative purposes: public and non-public. Public identifiers include, e.g., license plates or VIN (Vehicle Identification Number). Public identifiers are nationally or internationally standardised and commonly used in public, commercial, administrative-management, police-safety and forensic practice. Certain public identifiers, such as VIN, can have a hidden placement character so that potential forgers cannot find it and change it with the intention to change the overall identity of the vehicle. Non-public identifiers are not intended for public usage or processing. They are standardised in certain businesses, manufacturing groups, associations, etc., in which they can have their own content, method of creation, locations, etc. These are useful for forensic purposes as they can typically be quite useful for determining the identity of a vehicle.

6.4.1. Driver identification

Individuals could be identified by capturing their natural driving behavior using in-car digital data. This could aid in the resolution of hit-and-run accidents and other incidents involving autos. Previous writers have demonstrated the utility of driver identification using data pertaining to an individual's natural driving behavior through a range of intriguing circumstances. In the present study, the authors classified drivers based on their natural driving behavior using publicly available data. This methodology can thus be applied to a greater range of digital evidence relating to the digital domain activity of persons (smart home data, typing behavior). In light of the forensics requirements, suggestions are provided for reporting model findings in a way that is both intelligible and useful [165].

In a hypothetical hit-and-run event, police were able to identify the vehicle, but not its driver. In this scenario, it is assumed that one of three suspects was the actual suspect. After the incident, driving samples were obtained from each of the three suspects. This information was used to develop a driving profile. Using machine learning algorithms and their predictions, the likelihood that a given evidence pattern belongs to the suspect class(es) may be predicted.

This is analogous to a random match probability (RMP) in a finite suspect group, except the use case involving an unknown suspect. Landscape mapping based on remote sensing classifies each pixel according to the class for which the model delivers the highest likelihood. Transferring uncertainty is possible by providing confidence intervals for the overall model quality (e.g., precision, FDR) and for each prediction. FDR might be easily translated into the proportion of wrongfully convicted individuals who are actually innocent.

Freely available South Korean data were used for this study (http://ocslab.net/Datasets/driving-dataset). The data was collected at 1 s intervals. This is quite brief in comparison to the human reaction time, and hence, this time series data was strongly autocorrelated. The international roughness index was calculated based on the velocity of the vehicle. Each of the 120 models' accuracy decline was rated.

The purpose of this study was to evaluate the viability of identifying drivers based on their normal driving behavior in a forensic setting. Across all 120 models, the roughness-features were shown to be the most relevant of the 11 features used for class separation. Due to the sample design, the majority of the original data's characteristics were heavily influenced by automobile model and were also environment-dependent. Using an excessive number of features, especially environment-dependent features, exacerbates the problem of misleading correlation caused by multicollinearity. Using only statistics, it is not possible to entirely resolve these concerns with the available data.

However, it can be mitigated by using presumed driver-dependent explanatory features and a sound training data sampling scheme. Too many features necessarily lead to model overfitting, particularly when a flexible approach such as random forest is employed. When a model's forecast matches given data too closely or precisely, it is said to be overfit. As a result, it will be incapable of predicting independent test data. This study centred on the transfer of model results in a forensic setting, taking validation and model quality metrics into account.

The lack of independence between hold-out data and training data makes models appear more reliable than they actually are. An overestimation of the model's dependability will increase the number of wrongful convictions. If computational resources are limited, data collected at 3-s intervals could be sufficient for forensic driver identification. The plausibility of the response curves, which describe an individual's driving styles, should be considered when evaluating models used to depict the natural driving behavior of a person. Bootstrapping could be used to produce confidence intervals for each point estimate.

This research lays the foundation for the development of a quantitative approach for the use of machine learning and the interpretation of outcomes in digital forensics. Drivers may have been in a different physical or mental state at the time of data collection compared to the time of the accident. This could be the result of an upset mental condition, a medical episode, exhaustion, drink, or intentional deception. Since their mental condition could be the cause of the accident, stressed drivers may be overrepresented in accidents.

6.4.2. *Motor vehicle digital identity*

A vehicle's digital identity will connect the vehicle throughout its entire life cycle, i.e., from production to its operation, servicing, maintenance, switching owners, properties or functionalities. It will also be used for its communication with all other objects: v2v (vehicle to vehicle), v2i (Vehicle to infrastructure) and so on. Digital identifiers can be classified as both public or non-public. Vehicles contain many functionally and/or materially valuable components, functional units and devices. It makes sense for the manufacturer to mark these components with the same identifier (most often using digital VINs) since stolen, crashed or "scrapped" vehicles may be taken apart and the parts sold individually [166].

Digital Vehicle Identification Numbers (VINs) are digital copies of physical vehicle VINs, but contain additional information which can be used to relate significant information important for forensic purposes to the identified object. Digital identifiers suffer from a great disadvantage as they can be easily modified by a malefactor with proper equipment, i.e., digitally altered using special software. A digital identifier can be digitally altered using the appropriate software, as long as the digital technology allows it. In practice, a manufacturer can add an identifier to an "insignificant" vehicle component that is not expected to have one. A hidden algorithm alerts the operator using specialised software that the identifier has been altered.

Digital identifiers (both public and non-public) are placed into vehicle components by their manufacturers using their own proprietary technology and reading protocols. In order to be able to read the identifiers, there must a known and acceptable communication protocol. A suitable reading device is also needed, which can only be used to read digital identifiers of certain brands. This prevents them from being used for a wide-range of investigations and foiling of criminal vehicle activity.

Digital identifiers were recognized for all brands, in varying numbers and repeatability. The higher-end (and more expensive) the vehicle, the greater the number of digital identifiers assigned to significant vehicle components. The most digitally marked vehicle components can be found in modern American vehicles. High numbers of digital VINs were also recorded in European-made vehicles e German, French and "Italian" industrial groups. Digital Vehicle Identification Numbers (VINs) are digital values that can be physically obtained by a diagnostic reading straight from the vehicle in question.

The structure and location of the physical VIN is standardised with the help of ISO 3779:2009 and ISO 3780:2009 standards. There are no standards establishing when and where to locate digital VINs, in what quantities, etc. Identification of hardware components is a well-known process in the supplier-customer chain, known as a "Bill of Materials" (BOM). A software bill of materials (SBOM) is a list of components in a piece of software. Digital Bill of Materials for a given artifact is a stack of attestations on one or more channels that relate to that artifact.

In January 2021, the Vehicle Identity II (VID II) Standard was released. This first standard focuses on the "birth" of a vehicle as minimal evidence of that vehicle's creation. Subsequent VID phases will provide additional product definition, ownership histories, and a log of key events in the vehicle's life cycle.

6.4.3. *Traffic collisions*

The Crash Data Retrieval system permits the download and decoding of the Airbag Control Module's stored data. The technology is compatible with the brands of around 80% of the world's vehivle manufacturers. The GIT Tool co. system is exclusive to Hyundai and Kia automobiles. Accident investigators must determine the vehicle's model, version, and variant. They must also be able to identify active safety measures and accident avoidance [167].

Connecting to the Diagnostic Link Connector is the primary way for downloading data from an Airbag Control Module. The Event Data Recorder is primarily used in the United States to record vehicle operating data immediately preceding and following an accident. In Europe, a legislative framework is being developed to mandate the installation of this type of data logger in various vehicle classes. It can be used for technical accident analysis by professionals.

ÚSI ŽU was the first institute in the Czech and Slovak Republic to deal with a car accident from which it was possible to read data after the accident. The Crash Data Retrieval system was able to read the data stored at the time of the accident from the memory of the unit.

Digital evidence can pinpoint the location of an accident with relative precision. For vehicles that currently feature components of autonomous control, video camera data can be used. Using digital data from navigation systems, the driving of a car can be assessed before to an accident. Data from vehicle radars and lidars can be used in the future if it is archived.

The Crash Data Retrieval system is a comprehensive tool for police, specialists, and forensic scientists. Presently, approximately 15–20% of EU vehicles are fitted with Event Data Recorders, allowing for the retrieval of accident data from these vehicles. After each collision, these cars leave so-called data evidence that, like other forensic evidence, can be analysed and used as evidence.

6.4.3.1. Fatal crash scenes. The National Highway Traffic Safety Administration estimates that roughly two percent of drivers in the United States operate handheld mobile devices while operating a motor vehicle at any given time. Officers can issue traffic fines in 47 states and the District of Columbia that prohibit drivers from texting while driving. Due to the increasing influence of technology on both the operation and operators of automobiles, it is crucial that authorities be able to use data kept on these devices while investigating fatal crashes. This study evaluated a population of line troopers and agents from two state police organizations that respond to fatal incidents [168].

Respondents were asked to indicate the digital and physical evidence they would collect at a fatal accident scene. Given the variety of information that investigators can obtain from anything that connects to an electronic network and/or stores electronic information, the phrase "digital evidence" is purposely vague. At the scene of fatal car collisions, digital evidence plays a particularly vital role. Data from a mobile device attached to a car may provide digital evidence in the form of SMS and MMS messages, call logs, email apps, Internet browser history, and social networking application activity. Crash data is one of the most crucial types of digital forensic evidence relevant to crash investigations.

Electronic control units (ECU) are embedded, specialised computers that regulate all electronic functions of a vehicle. Important ECUs include the vehicle's onboard infotainment and telematics systems. Such information may be used to create a timeline of the driver's actions leading up to the tragic collision. The sheer volume of digital evidence contained within automobiles should be a windfall for police personnel investigating fatal auto accident sites. However, there is limited information on how frequently first responders employ this knowledge in the field. If a police officer fails to properly secure devices or mishandles equipment, it may be feasible to contest the trial-produced evidence.

Local and state agencies expect line-level law enforcement officers to accurately identify and safeguard digital devices for subsequent forensic capture. Limited research reveals that line police are uncomfortable with digital forensic evidence identification and collecting practises and procedures. Respondents with prior training and field experience with digital evidence were more likely to correctly identify and seize these documents at the scene of fatal car collisions. Training in digital forensics could enhance the ability of state police agencies to create high-quality evidence for all types of investigations, regardless of whether they occur in physical or digital locations. Officers from the Midwest were more likely to know who to contact if they required help recovering digital evidence at the site of a fatal crash, and they were also more comfortable using computers.

6.4.4. Motor vehicle digital forensics readiness

Forensics readiness is necessary not only for presenting evidence to court but also for ensuring Internet of Vehicles is capable of handling attacks and developing mitigation strategies. The authors identify and present the challenges of integrating digital forensics in an Internet of Vehicle ecosystem. The challenges include collecting, analyzing, and preserving in-vehicle data that are forensically sound and maintain chain of custody. The Attack Attribution and Forensics Readiness Tool lies between the data fusion and analysis tool and the response and recover tools. It is responsible for collecting, analyzing, and preserving evidence and for enabling event reconstruction [169].

The architecture of the tool follows a harmonized process model for digital forensic investigation readiness. Plan pre-incident analysis includes the definition of strategies and tools to detect incidents by analyzing data, such as intrusion detection systems, log monitoring, and security information and event management systems. Plan incident detection identifies actions to be undertaken after the incident has occurred or has been detected. Digital Forensic Readiness: The forensic readiness serves a dual purpose with responsibility to identify the characteristics of the attack for gaining useful insights.

The forensic readiness physically is implemented through a software application installed inside the Novel Adaptive Cybersecurity Framework for the Internet of Vehicles framework. The main components of the Attack Attribution and Forensics Readiness Tool architecture are responsible for attributing the attack. The goal of this module is to prepare for an event whose occurrence cannot be predicted. The Data Acquisition sub-module collects both network data and host data.

The Digital Preservation module is responsible for preserving the chain of custody and the integrity of the evidence. Forensic Readiness Planner provides a graphical user interface to the administrators in order to manage the forensics plans and activities. Forensics Assessment provides two services: a) The reconstruction of the event, based on the collected data related to the evidence for investigation purposes and b) The assessment of the selected forensics strategy from experts. The Attack Attribution module gets the detected anomaly along with the outcome of the risk assessment from the data fusion and analysis subsystem of the Internet of Vehicles ecosystem. The Forensics Assessment module can trigger two actions: The event reconstruction and the forensics assessment.

6.4.5. Generalised approach to motor vehicle forensics

Automotive forensics must be adaptable to many vehicles and situations. Four phases: forensic readiness (A), data capture (B), data analysis (C), and documentation (D) (D). Sections describe each phase. The infotainment system and related components should be checked for vehicle data leaks. Forensic analysis uses GPS data to locate cars [170].

Using the data gathering configuration, pertinent data from in-vehicle components is acquired. Later phases will only use this step's duplicated data. In a court hearing, timelines and evidence trails must be logical and replicable. Following is a software manipulation-focused analysis timeline. This step is to provide a well-structured and thorough final report that addresses all stated questions, successful implementations, and problems that arose during analysis.

A European Original Equipment Manufacturer produced an electric vehicle with lane assistance, an infotainment system, rear and front vision cameras, and other features in 2018. Manipulation via On Board Diagnostics (OBD) or other interfaces (e.g., if JTAG is still active on an Electronic Control Unit (ECU)) can compromise the vehicle's operation and safety. Data was not physically extracted by the use of embedded forensics techniques. There is an abundance of open-source hardware and software for bus systems like Controller Area Network. The VIN of the target vehicle was retrieved in step A:1.

In step B:2, the data sources were reviewed to detect software or hardware components that had been changed. This investigation included an examination of both internal and external flash storage, in addition to EEPROM store programming timestamps. Obtaining data from OBDs via the OBD interface constituted Step B:3. Step B:4 required presenting the final acquisition configuration and inspecting the vehicle's tools and instruments. In step B:5, the logical addresses of installed OBDs were collected using the scanning application.

Over 100 logical addresses were found. Next, all accessible UDS data identifiers for each gathered TA were requested and Wireshark used to watch network activity. Once the collection was complete, the network capture was saved as a Packet Capture (PCAP) file. Positive and negative replies, a manufacturer-specific identity, and connection establishment data are included in the PCAP (e.g., TCP handshake). Next, in step C:2, the relevant data parts and events were filtered.

No modifications to the programming data for certain OBDs could be detected, therefore it was concluded that there was no vehicle manipulation. As a result, there was no need to create timeframes or trails of evidence.

The presented tool is written in Python and based on the DoIP and UDS standards. The researchers obtained an overview of the collected data and could reduce the number of relevant packets from initially 3800 down to 245. The SHA256 hash algorithm was used to ensure the integrity of the originally collected data. OBD is one of the many in-vehicle technologies used in forensic investigations. The collected information was obtained in a secure manner but state-of-the-art vehicles do not offer tamperproof storage. A dedicated security device is a possible solution but introduces a highly valuable target for attackers.

6.4.6. PCM audio recovery

Sounds captured by a dashboard camera provide crucial evidence of a vehicle's driving condition for the investigation of car accidents. In reality, when a direct impact of a vehicle equipped with a dashboard camera occurs, the power supply to the dashboard camera is abruptly terminated, and the digital video being recorded at that time may be incompletely stored; consequently, there is no location or size information to be read for image and audio decoding. In this research, the authors propose a method for recovering linear pulse code modulation (PCM) audio from a damaged MP4 file stored partially in a video event data recorder (VEDR), often known as a dashboard camera, following road vehicle accidents. This method is based on the notion of extracting an actual audio signal using the energy of each frame in the pseudo audio, which is formed from all of the data in the "mdat" section of a damaged MP4 file. The numerous video files with linear PCM audio format in the MP4 container were gathered from the various dashboard cameras for performance evaluation. As an objective evaluation, it was determined the audio recovery ratio, distance based on dynamic temporal warping (DTW), and waveform and spectrogram comparisons. In addition, the performance of the suggested technique was tested subjectively using the multiple stimuli with a hidden reference and anchor (MUSHRA) test. The evaluation demonstrates that the suggested method can recover the linear PCM audio signal from a damaged MP4 file much better than the current methods [171].

6.4.7. Gaming consoles

The original Nintendo 3DS console was released in Japan on February 26th, 2011. More than six years after its release, the console has gone through numerous iterations. The 3DS, Nintendo's highest selling active console with 73.53 million units sold worldwide has already been involved in criminal activities. It warrants particular note from the digital forensic community to improve existing methods of data extraction and analysis. JTAG has been shown as a viable method to extract the NAND, it still requires hardware modification and some other means to obtain the decryption key to make the image readable [172].

This forensic analysis will use a console purchased in the USA; it should be noted that some folder names do differ slightly between regions. A valuable source of information for folder names may be found in 3dbrew. The trust in the 3DS is the boot ROM which is burned into the System-on-Chip (SoC) during the manufacturing process. Boot9 checks if a DS cartridge is inserted and attempts to load a signed firmware from it, bypassing the firmware on the NAND. This vulnerability will continue to exist in all Nintendo 3DS devices prior to discovery of the exploit providing a permanent method to perform digital forensic analysis.

Nintendo v. Playables Ltd. addresses the issue of copy infringement and copy-protection devices. The company imported a number of flashcarts (referred to as "game copiers" in Nintendo) which fit the proprietary cartridge connection in a previous-generation console, the Nintendo DS. Under section 296 of the 1988 Copyright, Designs and Patents Act, an offence is committed if the person behind the sale of such a device knows or believes it will be used to make illegal copies of software.

6.4.8. Nintendo 3DS NAND

A reflashable R4i card is used by investigators to replace a microSD/SD card in a Nintendo 3DS with a new one that contains Boot9 code execution and the system's encryption key. The card must be pre-flashed with ntrboot_flasher (ntrteam, 2019) and pre-imaged and forensically imaged before being inserted into the 3DS.

The main console can be powered off and the microSD/SD card removed so that the data can be decrypted and stored on a computer. The Decrypt9WIP application, initialised from the microSD.SD card, will perform three functions: 1) backup of the internal NAND; 2) verification of NAND dump; and 3) backup of the unique encryption keyneeded to decrypt the NAND dump.

At this point, the analyst will have three files, the encrypted NAND.bin, the SHA256 hash stored in NAND.bin.sha and the encryption key nand.fat16.xorpad. The NAND.bin file itself contains two partitions, the backwards-compatible DSi partition and the 3DS partition (3dbrew, 2017b). The process begins with input from an XORing application, like 3DSFAT16Tool. It ends with a decrypted version of the file that can be dumped into a new FAT16 image.

A second-hand version of the new Nintendo 3DS was used for the experimentation. Results were later confirmed against a newly-purchased 3DS XL, an original 3DS and an original 2DS. AccessData's Forensic Toolkit 7.0 was used to perform forensic analysis. Within the data folder, is a directory made up of alphanumeric characters which represents a SHA256 hash of console-unique data (ID0).

The Nintendo 3DS operating system contains a number of sub-folders, each containing the actual contents of several different apps and data files. By default, there are two files 00000001 and 00000002 which are part of the core operating system. If present, 00000003 and above are created by a user's actions and have a timestamp reflecting the action taken by that individual. Of particular interest to the examiner are the contents of the camera app (f0000001) and the sound recorder app (F00002).

Within the camera app directory f0000001, the subdirectory 00000001 and 00000002 are present by default. If present, 00000005 and above contain embedded pictures (one per file - n.b. "3D" images appear as two embedded files, slightly off-centre from each other) in JPEG format. Using ExifTool a wealth of metadata was obtained. The images themselves contain a substantial amount of metadata in the EXIF headers.

Within the sound app directory f0000002, the subdirectory 00000000 contains files of interest. Files 00000003 and above contain sound recordings made by the built-in microphone. They are in the m4a format (i.e., file header 0 × 66747970). The sound clips were then deleted, and the console re-imaged. PhotoRec was able to recover all the deleted audio files. ExifTool provided an interesting insight into the metadata; the intuitively-named entries with "date" in the title were all consistent with one another, but were all incorrect by several years.

The sysdata (or system savedata) provides storage for the applications on the 3DS. Every module/application on the NAND has a savegame associated with it. Analysis was performed on both the system modules and system applications. The windows strings command was the main tool used to parse the files.

The Friends system module savegame can be located under the 00010032 folder. Within this folder is the standard 00000000 file. Analyzing this file with strings yielded the names and publicly displayed messages of all friends that have been added to the console. In addition the 3DS console's Serial number, user-name, and public message were all viewable.

The microSD Management application is specific to the New Nintendo 3DS line of 3DS consoles only. Analyzing this file with the strings command yields several things, including the SSID of any network stored within the console. The file also contains the device's required login name and PIN to gain access to it, in this case 'User' and '77XX'.

The new and original Nintendo 3DS systems have different storage formats for the web browser. The Internet Browser application savegame can be located under the 000200bb folder on the New console. Using the 3DS Save File Extraction Tool, in particular disa-extract.py, the file t.bin can be extracted from 0 × 100000080DF0A00. From this, the start of the first bookmark entry can be found 0xD8 bytes later, the first value is 0000000000000000 0000000000000101. After the last bookmark, the next timestamp is zero, but the counter and the following value are 0xFF. There appears to be enough capacity (0 × 31E30 bytes) for 0 × 63 (99 decimal) bookmarks on the new Nintendo 3DS. This is confirmed in the bookmarks function of the web browser (xx/99). An image of the NAND was taken and used to successfully retrieve all bookmarks and history entries. AccessData FTK did mark the folder 000200bb was deleted but the data could be recovered.

The 3DS has a format system memory function that can be used to write files to or from memory. Images taken with the Camera app were data-carved, erased using the function, and then imaging. After analysis, FTK confirmed the Files on Disk (FTK) format had been altered.

The methods outlined above enable an investigator to extract and decrypt the contents of a Nintendo 3DS NAND memory chip. This provides access to a number of key sources of information including deleted images, internet history items, relevant friends list information, console serial number and plaintext access point passwords. This is a more forensically sound method than that of accessing the device via the user interface and therefore provides a more in depth analysis. Open source tools and techniques to extract data from mobile devices are already available to the hacking and modding community, but should they be ignored by the forensics community? It is suggested that ignoring the fact that these tools (which are in the public domain) exist serves no useful purpose. The code is open source and can be examined and tested as in this paper and not to use these resources disadvantages the forensic examiner.

6.4.9. Nintendo Switch

Due to its portability and location data, the Nintendo Switch is a gadget deserving of forensic study. The Switch supports internet connectivity and maintains a log of all access points to which it has connected. This means that a forensic timeline can be created for the device's owner. In addition to gathering temporal data, it is useful to acquire geolocation data or data that links a person to a certain address [173].

With 61.44 million units sold globally, the Nintendo Switch is the most popular portable gaming system in the UK. The majority of data useable for forensic investigation is found on the NAND chip of which five partitions are important for forensic analysis. System and User partitions contain artifacts that are improbable to have forensic significance. The retrieved 'built-in storage' keys are the device's keys that can decrypt the NAND's AES encryption.

Exploitation to collect digital forensic data has legal and ethical implications. Microsoft has filed litigation in response to previous attempts to abuse the Xbox. Extraction of personal data from these devices should be covered by the Information Commissioners Office's exemptions for research involving personal data.

All consoles manufactured after June 2018 are have a firmware patch. It is expected that vulnerabilities will be discovered in succeeding models. All the recovered data might also be retrieved through a forensically sound "chip-off." However, an exploit would still be required to obtain decryption keys from the target device.

As the amount of functionality and, consequently, metadata given by portable consoles improves, so does the capacity to effectively extract forensic evidence.

Memory dumps have enabled the retrieval of forensic evidence from the majority of mass-market consoles. Even though the introduction of current memory security methods such as Address Space Layout Randomisation and Data Execution Prevention has made exploitation and remote code execution to retrieve forensic data more difficult, the vast majority of mass-market consoles have been exploited to date.

The authors demonstrated that it is possible to retrieve data from the Nintendo Switch console in the form of a few key forensic artifacts. They also assessed the potential value of these artifacts as evidence in an investigation. Many of these forensic artifacts remained on the device after factory resets.

The exploitation, extraction, and analysis of forensic data from video game consoles are not completely novel. However, the instructions and tools for forensically analyzing the Switch are innovative and give analysts with skills. This method may be applicable to other Nintendo Switch-related portable consoles.

7. Apps and social media

7.1. Email

Email's exponential expansion has rendered email forensics an unparalleled challenge. Unlike other data, email comprises data of two structures: the email header is structured data and the subject and body of the email are unstructured data. Most attention is dedicated to graphical forensics of metadata, which is focused on the social network relationships between senders and recipients. The system is based on the Sankey diagram, which was originally developed for the representation of energy flow, in order to facilitate the unambiguous expression of communication network structure. Extends the scope and depth of forensics in the email from numerous viewpoints by merging the email header with the email content to capture forensic information [174].

This information dimension can also be used to indicate the message's context in relation to the email's body. Many digital forensics cases rely on email metadata which focuses on establishing social networks and utilizing various algorithms to assess social links. Previous work involved automatically creating these networks from collected hard drives by scanning raw storage media for email addresses. Email datasets have the advantage of being rapid and easy to obtain, and they are typically used to uncover latent collaboration patterns in informal networks.

An automated visualization method for quick organization mapping enables its participants to better comprehend team communication networks and dynamics in a short period. By evaluating novel algorithms for establishing networks based on byte offset proximity between digital artifacts and automating stages for creating social networks, the classification technique was improved. Some information visualization technologies are built expressly for studying emails. CommViz is an information visualization tool that extends a visualization approach known as hive plots to reflect the semantic structure of the networks. It solves the problem of how to graphically display the four basic qualities of individual communication (message) in a two-dimensional, screen-based visualization for all communications in a large data set.

7.1.1. Visualization model for email forensics

The model extracts the body data of each email and selects the four attributes "From," "To," "Date," and "Message" as evidence. "Active relationship" addresses are heavier. The width of the lines in a Sankey diagram indicates the magnitude of the flow from one set of data to another. Each process stage can merge or separate flow lines. The Force-directed graph has the same effect for sender and recipient. Forensics uses Sankey diagrams. It arranges four-dimensional message attributes. Mutually parallel four-column axes indicate message attributes. Corpus extraction and data processing, Latent Dirichlet Allocation topic classification and optimization, SankeyVis presentation, and discussion comprise the experiment.

Many previous studies have employed the Enron email corpus, a large public email dataset, and the researchers got good results. The number of communications between "sender" and "receiver" is used to quantify intimacy in this study. An upgraded Sankey diagram uses an active relation address pair, a social relation email address with a social weight greater than 200. This portion extracts the email message's semantic topic. The Latent Dirichlet Allocation model's pros and cons depend on choosing the right number of topics.

This work uses coherence to estimate the appropriate number of topics for topic model validation. "L" represents the probability of a term in a topic compared to its lift. The text uses n-gram grammar to show word context. For example, topic 0's keywords are "power," "market," and "energy," indicating that it's about energy. Time-related phrases like "pmto," "Amto," and "kate" suggest "deal" information.

20 keywords explain each topic. Sankey diagrams create the Topic-From-To-Date four-dimensional forensics visualization graph. It displays the monthly themes senders and recipients discuss. A contiguous columnar image represents a keyword-paired email address in the "From" column. Outage, surgery, etc.

A floating panel displays all attribute branches the message passed from left to right when the mouse lingers over a message. The wider the grey line segment, the more the topic is discussed and the more activity occurs during this period. For senders and receivers enron.announcements@enron.com is the most commonly used address, followed by jeff.dasovich@e-mail.com, and vince.kaminski@aol.com. Hovering over the bar in the four message attributes shows input, output, and passing traffic.

This article uses a big, unlabeled Enron Group dataset containing email addresses. SankeyVis enhances Force-directed graphs' over-draw and dimensional limitations issues. It investigates the semantic patterns in the email body in depth and combines the email header to produce an evidence-based result. This project includes the development of a system for visualizing the trend of multivariate data attributes. Using confusion and consistency, the unsupervised learning model was evaluated.

In general, however, horizontal or vertical contrast trials are still difficult to do. Additionally, it is challenging to quantify and assess visualization outcomes. By systematizing the visualization of email forensics, this integrated approach enables the forensic analyst to provide more thorough and in-depth responses to typical inquiries. The SankeyVis is not restricted to visual forensics of four-dimensional data; it can be a suitable extension of the dimensions. It thoroughly examines the semantic patterns in the email body and integrates them with the email header to give analysts with more productive evidence-based results.

SankeyVis may be used for email forensics as well as forum forensics, instant messaging forensics, etc. Its seamless applicability is evident not only in the visual analysis of inter-disciplinary data, but also in a variety of scenarios within the same domain. Future research efforts will centre on figuring out how to automate the collection of collective threat intelligence data from email.

7.2. Messaging apps on android and iOS

There is a growing opportunity within the mobile application market for criminals to use ephemeral messaging applications [175]. These apps allow users to send messages/multimedia etc. to each other with the messages only lasting a certain period of time. Data in these applications is known to delete itself, which is prime for criminal communications. For example, Snapchat has a daily user total of 190 million users. The following applications were tested on an Android and/or an iOS platform:

- Snapchat
- Cyberdust
- Confide
- Facebook Messenger
- Signal; and
- Wire

With the following mobile forensic tools:

- Oxygen Forensic Detective Enterprise
- MOBILedit Forensic Express
- Andriller
- FTK Imager
- Autopsy; and
- Kali Linux

Oxygen and MOBILedit successfully recovered data on all applications: Snapchat, Cyberdust and Confide. While different artifacts and data were detected, the fact that no physical copies of messages were recovered in any application, using either of the forensic tools, proves how efficient ephemeral messaging applications are at protecting user privacy.

Oxygen Forensic Detective appears to be the most capable and reliable tool of the four tools used for Android. The application analysis performed revealed that, for the most part, the ephemeral messaging applications are secure enough to keep evidence of user activity and message contents from being identified. Despite the potentially evidence unsafe methods required by the freeware tools, both FTK Imager and Autopsy provided more forensically valuable data than Andriller.

Results show that with the rooted Android phone, more artifacts were recovered compared to the iOS phone, which was not jailbroken. One significant finding was that of the Snapchat's 'offensive words' detection, which may help aid evidence in cyberbullying cases. Confide and Wire provided the most valuable data, then Facebook messenger and then Signal with the least. It does appear that Facebook Messenger has a more secure design, in which messages cannot be recovered even through a physical acquisition. During the anti-forensic investigation, when apps were deleted from the Android phone, some valuable artifacts were recovered. For example, the media files in Wire could still be recovered but the log file was not.

7.2.1. Signal, Wickr and Threema

The authors analysed the decryption algorithms of Signal, Wickr and Threema messengers on Android devices. All of these messengers default to end-to-end encryption and encrypt not only databases but also multimedia files such as images, videos, and documents. They also support the messenger lock feature that requires password or fingerprint authentication when opening the app. Data was extracted from both unrooted and rooted devices with static and dynamic analysis performed on messenger applications. Compared to previous studies, the study found a new decryption algorithm, expanded the range of decryptable files and corrected outdated parameters. There are several studies on Signal and Wickr, which are the subject of this paper including an algorithm to decrypt the database using the passphrase set by the user and found a method to retrieve the password from volatile memory in the ChatSecure application on Android devices. It is impossible to analyze Wickr because it use its own native library for all encryption. Considering that the source code was not disclosed in this study, it was decided that manual analysis would be more efficient. Similarly, it has previously been found to be impossible to decrypt Signal as encryption is applied to databases and multimedia files [176].

The encrypted database name of the Signal app is 'signal.db'. To generate the database decryption key, a 'pref_database_encrypted_secret' value was obtained from 'org.thoughtcrime.securesms_preferences.xml' file. This value is a string with the 'data', 'iv' as a key, and a base64-encoded data as a value. It contains the ciphertext and the authentication tag of AES256-GCM, and the initial vector (IV) of the encryption key. The key for encrypting the database using the Android Keystore was obtained.

The authors developed an app to extract the key from the Android Keystore and perform decryption. To get the multimedia decryption key, they obtained a modernKey and a data_random value. Using this key they obtained the original multimedia file by decrypting the '.mms' file with AES256-CTR. The log files were also decrypted which contain information on the user's time and behavior of using Signal.

Wickr has two login methods: i) password login and ii) automatic login. The password is set by the user in Wickr messenger, so it is difficult to obtain it without the user's cooperation. In the algorithm for automatic login, the user password is not required, so the keys can be extracted from the files inside the device. Wickr stores the database with double encryption. The key for the first decryption is devinfo, which is a value created from android_id in the Android system. By hashing the generated file to SHA256, the devinfo value can be obtained.

The Threema database key can be obtained from the file 'key.dat'. Threema's multimedia decryption key is the same as the database decryption key. The Protected Flag changes depending on whether the user enable messenger lock feature. In the encrypted multimedia file, 16 bytes from offset 0 are used as iv, and the rest of the data is ciphertext. By performing AES256-CBC decryption on these values, the multimedia file can be decrypted.

The authors successfully extracted data from both unrooted and rooted devices and performed static and dynamic analysis for finding the decryption algorithms of Signal, Wickr, and Threema. As a result, the decrypted database, multimedia, log, and preferences files could be obtained from the extracted data. Forensic investigators can use these results to analyze the three apps and will be able to obtain clues to infer the user's behavior from decrypted log files.

7.2.2. Telegram

Users can use the Telegram app on mobile devices and computers with the accounts synchronized between devices. The collection of data from messenger apps from mobile devices can be difficult to collect, whereas it is easier to collect from computers running the app.

7.2.2.1. Telegram Desktop. As a case study, the authors explore the Telegram Desktop software for Windows and provide a complete analysis of the acquired memory artifacts. Using page table entries (PTEs), the virtual memory management must ensure that each thread inside a process matches to the correct physical location. Windows Memory Extractor is a command line tool that integrates seamlessly into any analysis process. An examiner may access and gather data from a machine that is powered on, unlocked, and loaded with Telegram Desktop. The report for each seized Telegram account includes recoverable chats, Telegram users linked with the account, and information about the account owner [177].

Using a running program, an examiner may also connect with a suspect's locked or logged-out computer. Knowing a suspect's networks and groups might reveal their interests. Knowing the names and kinds of sent files facilitates forensic disk examination. By locking or logging out of Telegram Desktop, memory artifacts are recovered. Although recovering deleted conversations and artifacts after logging out is problematic, the tests produced accurate results.

An examiner having access to a computer running the encrypted Telegram Desktop program would be able to access it and get the required data. Nonetheless, this procedure would drastically change the RAM's condition compared to when the device was seized. If the examiner accesses the chats to see their contents before to terminating the Telegram Desktop session, information about which conversations the suspect visited most recently will be destroyed. Knowing the time, sender, recipient, and content of each communication is often vital to investigating a crime. Participation in organizations and channels (actively or passively) may provide information about a suspect's interests. Having knowledge of the transferred file names and kinds facilitates forensic investigation of the disk.

In situations when databases or communications are encrypted, retrieving important information in decrypted form requires forensic investigation of volatile memory. In this study, a forensic analysis environment has been developed to retrieve memory artifacts from instant messaging programs. Among other things, information on the application's users and their contacts was obtained, chronologically rebuilt chats, and recovered specific artifacts that had been intentionally erased.

7.2.2.2. Telegram X. The researchers studied encrypted data from Telegram X, a clone of Telegram named Unigram, and BBM-Enterprise. These Secure Messengers, provide services on several platforms that synchronize the mobile and desktop versions. Telegram X is an Android application that is synced with Telegram and is an official application designed to enhance performance (Telegram). Unigram, in contrast, is not an official Telegram application, although it is synced with the real Telegram. Unigram for Windows is implemented using the official Telegram TDLib library in the same manner as Telegram X, as detailed on the Telegram website. Therefore, it may be considered a PC version of Telegram X. This allows users to exchange messages using any of the Telegram, Telegram X, and Unigram programs. BlackBerry's BBME is a secure messaging application that supports video, audio, images, and group chat in addition to one-on-one conversation. Blackberry Messenger (BBM) was initially a messenger for the Blackberry operating system, but it is now accessible on other platforms, including Android, iOS, and macOS. BBM was separated between a free BBM version and a premium BBME version, however the free BBM version was discontinued on May 31, 2019. BBME offers services on the same platforms as BBMs and maintains security via the use of a FIPS 140-2-certified cryptographic library and BlackBerry's security architecture [178].

The authors performed a forensics investigation using reverse engineering of the Telegram X and BBME mobile and desktop applications. All of these instant messengers encrypt the private and application data of their users. Despite the fact that investigators get instant messenger data via a variety of methods, it is difficult to use it as evidence due to encryption. Complete application data that may be used as evidence cannot be obtained. If the data is obfuscated and difficult to identify, the cryptographic algorithm is specified by using the input and output information of the function or the non-changeable constant inside the function.

The vulnerability provides a technique for getting read permission and memory data. The core data is selected which includes all the data required to gather crucial information from a digital forensics standpoint. Using a decompiler, the encryption techniques used to decode the core data are identified. Typically, cryptographic algorithms are called through APIs, in which case fixed values such as the names of cryptographic algorithms are included. If the data is obscured and difficult to recognize, the cryptographic procedure is provided by using the input and output information of the function or the non-variable constant included inside the function.

Telegram X being evaluated on Android, whereas Unigram is evaluated on Windows 10. The Telegram Database Library (TDLib) is used by TXU to store and handle sensitive data such as conversation details. The encrypted contents of the tdbinlog file include application-specific information and the Passphrase used to encrypt the db.sqlite file. The Passphrase used to encrypt the file 'td.binlog' was recovered by studying the file's structure. The key used to generate the key is PBKDF2-HMAC-SHA256, while the technique for decryption is AES256-CTR-DECRYPT.

For each operating system, it was attempted to extract BBME data. The bbmcore library controls user information and discussion history as the core of BBME. According to a Blackberry security advisory, BBME employs a 48-byte random passphrase for SQLCipher. In contrast to the description in the BBMEs' public security statement, the length of random data used for each OS was variable. The encryption algorithm for each operating system is unique. Because the Android KeyStore is connected to the Trusted Execution Environment, it has proven challenging to retrieve a stored RSA key pair for Android versions above 7.0. (TEE). The Passphrase may be derived from the BASE64 encoding of the ER. The procedure of decrypting an encrypted BBME database core.enc file on iOS is summarized by the authors. Although it is well-known that data encryption provides robust security, the lack of secure coding in apps might result in vulnerabilities. After analyzing each version of BBME, it was determined that one of the R, ER, or Passphrase variables might be used to decrypt a database. R and Passphrase are not independently kept, and ER is encrypted and stored using a secure manner such as Android KeyStore, iOS Keychain, or macOS Keychain. This indicates that the ER may have been present on the stack or in unallocated memory space throughout the decryption procedure.

The feasibility of TXU and BBME acquiring data relies on whether data can be decrypted. Each criterion for decryption is independent, and at least one must be met. The requirements for obtaining data from a PC are more relaxed than for smartphones. The requirements for decrypting data on BBME-iOS devices are less stringent than on Android smartphones. Devices can be jailbroken (A12 chipset as of February 2020, available on all devices except iOS version 13). Backup data may be retrieved using a password with known password.

7.2.3. *Note and journal applications*

Note and journal apps have been used for criminal purposes. In 2017, a boy committed suicide in India, but no evidence was found to prove that the event was suicide. In 2020, a murder case occurred, and the note app data recording the circumstances of the murder were acquired and used in the investigation. In general, the storage of note and journal apps has been insecure. Most apps store data in plaintext, or encrypted with a fixed value generated after the app operates [179].

The researchers tested 31 Android and 25 iOS note and journal apps that provide security features to protect personal information. Analysed apps can be locked using a Personal Identification Number (PIN) consisting of numbers; a password consisting of alphabetic uppercase and lowercase letters, numbers, and special characters, or a pattern.

7.2.4. *Snapchat*

The prevalence of social networking sites being used to disclose concealed information has led to the following conclusion: law enforcement and intelligence agencies can use social networking sites as a dispersed surveillance system [180]. This hypothesis raises the subsequent questions:

- Can Snapchat function as a decentralized surveillance system?
- What technique is necessary to extract content from Snapchat?
- How can Open Source Intelligence media be verified for surveillance purposes?

The authors claim that there has been no technical evaluation of Snapchat as a surveillance tool. Using the destructive capacity of the image-sharing social network, Snapchat has been assessed as a way for distributing radiology didactics. Snap Map can be scraped for user-generated content and location information. Snapchat may be a feasible alternative to the traditional classroom-mounted light boxes for diagnosis.

The authors present a technique for extracting digital media from Snapchat before analysing if it is a suitable replacement for a CCTV system. In addition, digital evidence must be extracted with due regard for the reasonable privacy of the involved parties and without compulsion or destruction. Infractions of these principles may render digital evidence inadmissible or fail to satisfy the Daubert test. The method focuses on the web-based application to capture media from the Snap Map, which, while not preventing data loss, does permit a copy of the metadata to be saved in an additional text format.

The Australia New Zealand Policing Advisory Agency/National Institute of Forensic Science framework highlights six key areas that should be met to have an effective system. In this study, 2692 Snaps were extracted from the Snap Map comprising of 2600 MP4 videos and 92 JPEG images. Both video and JPEG images were found to use Google Cloud Storage XML API with an expiration set for 90 days. No evidence of deletion was found; instead, what was indicated was key expiry.

The research suggests that media may be stored much longer than the indicated deletion time. Snapchat has the potential to meet the following needs of a conventional surveillance system: ability to identify faces, track users through a site and record number plates. The results suggest facial recognition is capable using Snapchat's Snap Map but is heavily determined by the quality of the images saved on the map. For the experienced CCTV examiner, it is likely a positive facial match would be made from extracted media.

The researchers were able to reverse engineer the timeline of a gentleman on a bucksnight due to multiple videos being taken at different places around the Adelaide (Australia). Such a method easily lends itself to automation using machine learning and object recognition algorithms so long as a sufficiently accurate training set was provided. Given the current trends of smartphone cameras and mobile networks to see increasing quality, it is suspected that this capability will become increasingly commonplace within the next decade.

Snapchat's most obvious limitation as a distributed surveillance system is the resolution of media collected through the service. Numerous variables affect this, including the quality of the imaging device and the compression applied by the system, both on the device and on the social networking site itself. As the demand for high-quality media among users grows, it is anticipated that this limitation will be eliminated over time. Snap Map contains a heat map that scales on demand and is not effective for determining the number of snaps uploaded in a certain location. During the course of the study, it was determined that the information about the location of photographs submitted to the map was inaccurate during periods of high visitor volume.

7.2.5. *Android applications*

In addition to the difficulty inherent in reverse engineering, obfuscation tactics further complicate the process. An application may be malicious by design or benign and changed to be malicious. Before performing static analysis, an examiner may be required to deobfuscate the application, depending on the technique employed [181].

Android Application Package (APK) is a compressed file type used by the Android platform to package applications. The DEX file often includes the program's core and can be easily decompiled. The Android application compilation process could be different if the app developer favored Flutter2 or React Native to construct cross-platform mobile applications. After preparing all necessary files, they are compressed into an APK file, which must be signed by the author as the final step. Prior to the widespread use of obfuscation techniques in Android development, the process of reverse engineering an Android application was considerably simpler.

It is possible to modify and repackage decompressed APKs, resulting in a valid new/modified app that must be re-signed. Attackers can sign the same repackaged program with different keys in order to deceive security products that rely on the hash value of APK files for identification. For functionality analysis, the DEX file and shared libraries are disassembled. The application can be decompiled using dex2jar, a program that converts DEX bytecode to Java bytecode.

As a result of obfuscation, the original state of an Android application can no longer be reconstructed during a forensic investigation. Consequently, conventional Reverse Engineering tools for desktop computers, such as IDA pro and Ghidra, have become the norm for forensic investigators.

7.2.5.1. Obfuscation. The Android ecosystem has extensively adopted obfuscation methods. Techniques are instruments that modify an application while maintaining its semantics. Apps commonly rely on encryption, but they may also incorporate alternative simple techniques. Malicious Behavior Evasion (MBE) is a technique designed to circumvent malware analysis software. Optimization (OPT) is used to enhance code since transformation output can be stored more efficiently.

The AndroidManifest.xml and APK files include XML-formatted metadata about the app itself. During the APK generation process, the manifest file is changed to a binary XML file, which must be reversed prior to modification. These strategies may mislead forensic analyses that do not use code analysis but instead rely on the hash value of the target APK file. DexGuard, a more potent tool than ProGuard, employs non-ASCII characters, making it more challenging to use. Alternatively, a developer may replace each character of a specified identifier with a random one, such as Variable.

In general, options are limitless and simple to apply. Code renaming and other obfuscation techniques have become the standard protective method for app/IP optimization. During an examination, certain existing library detection algorithms that rely on the names/symbols in APKs can be defeated using certain techniques. In addition to code downsizing and tree shaking, tools such as ProGuard and R87 can also delete inaccessible code and uninitialized types.

Methods such as operation instructions, unconditional jumps, and additional registers for trash operations comprise junk code. An opaque predicate is a conditional command that always yields the same result but produces two branches. One of the branches leads to the original code, while the other contains trash instructions that are unreachable. Reflection is a Java-exclusive capability used to investigate or modify an application's behavior. Reflection is typically employed to access class methods that may be loaded at runtime.

Encryption is the most complex obfuscation approach because static analysis is worthless without the matching decryption method and the key. Depending on the employed method, it may be feasible to reverse portions of the application. As the Android platform has evolved, the use of encryption techniques as a way of obfuscation has expanded. The Java Native Interface (JNI) is a Java technology that allows native applications to execute and be executed. In a more advanced approach, the original APK is encrypted and a wrapper APK is also generated. This prevents technologies that rely on static analysis from determining whether the original application is benign or malicious. Additionally, it inhibits reverse engineering.

7.2.5.2. Obfuscation detection. AndrODet uses three separate detection algorithms with various feature sets. They analyze encrypted strings to find entropy, word size in bytes, string length, and special character counts for identifier renaming (e.g., equals, dashes, slashes). Control flow obfuscation detectors analyze extracted control flow graphs. Data Stream Mining enables online learning algorithms (DSM). Identifier renaming is a popular app market tactic. DeGuard uses probabilistic learning to reverse ProGuard-obfuscated Android apps.

Renamed elements were recovered at 79.1% and third-party library detection at 91.3%. Machine learning-based deobfuscation program DEBIN predicts stripped (debug) information from binaries. HARVESTER outperforms FlowDroid and TaintDroid. It extracts the Android app's smali code, intercepts decrypt method results, and replaces encrypted strings with decrypted values. If the third-party library is open-sourced, detecting it can eliminate the deobfuscation process and reduce an investigator's workload. LibScout employs a hash (Merkle) tree profile matching technique. Obligation greatly affects malware detection.

7.2.5.3. Obfuscation affects forensic investigations. Obfuscation techniques can be/are used to evade automatic detection and inhibit forensic examination. Simple methods such as repacking and manifest transformation can invalidate application fingerprinting (via hash values) techniques. Tools have been discussed that help to detect obfuscation and sometimes even to deobfuscate (parts of) the application. Obscurity features become essential for Android malware detection but they do not truly provide many benefits for understanding the application, as typical deobfuscation techniques for malware detection-resilient obfuscation work by extracting non-code features rather than recovering the source code of the application. The possibility of using multiple obfuscation methods in sequence, i.e., creating multiple layers of obfuscation, is becoming more relevant.

7.2.6. Zoom

Due to the COVID-19 pandemic, many schools, businesses, and people have turned to the Zoom application to communicate. Security issues have led to privacy breaches through Zoom Bombings and the exploitation of basic protocols. Further vulnerabilities were found in the Zoom application and Zoom has responded with patches for these issues (Zoom, 2020c). As video conferencing applications continue to be the main communication method during events such as this pandemic, it is important that the forensic artifacts produced by these systems is understood [182].

7.2.6.1. Zoom disk artifacts. Zoom creates separate data folders for each account that was logged into the device. Each account's Jabber ID (JID) uniquely identifies individual users, as well as user chat groups. JIDs are the user's Extensible Messaging and Presence Protocol (XMPP) chat addresses. "Zoom.us" found a possible encrypted database file named zoom.sip.enc. According to Zoom, any VoIP media is encrypted with AES-128 encryption. "msg_active_devices" also stores an encoded/encrypted certificate, PEM, and password for each active device.

Zoom's Chat and Download feature stores files such as images and screenshots, along with timestamps and names of the users in the chat. This also includes messages exchanged when using the Twitter bot feature. The "zoom_mm_file" table contains partially Base64 encoded URLs of where those files are stored in a Zoom server. The main table of interest is the "zoom_mm_buddy" table which contains the names, JIDs, emails, phone numbers, profile picture active URLs and the path where those were stored locally in the device. A binary pList file titled "contacts.db" was also found masquerading as a database.

Zoom stores important data pertaining to user account and Zoom account configurations in this database. Table "zoom_conf_cc_gen2" contains information about recorded meetings saved locally on the device and any closed captioned plain text that has been provided during the meeting. The "zoom_conf_avatar_image_cache" table stores cached active profile pictures' URLs, their path location on the device, and timestamps. This table contains important account configurations such as Zoom application version, the last time the client was connected, IPs, ports, URLs Zoom uses to connect on each session.

As an attendee or panelist of a webinar, one has the chance to acquire the live database while the webinar is taking place. The Zoom webinar database stores the names of all attendees and panelists. This table is viewable depending on the type of attendee and Zoom account (Licensed or Basic). The table also stores flags pertaining to whether the question was answered live, read, dismissed, or sent in private.

Network traffic artifacts – Zoom claims that they use the 256-bit Transport Layer Security (TLS) encryption standard and Hypertext Transfer Protocol Secure (HTTPS) to secure network traffic. When using Wireshark to capture network packets, the study demonstrated that this is accurate. Usernames, JIDs (Jabber IDs), cookies, session access tokens, device IDs, MAC addresses, and other information are among them. No communications were discovered in the network traffic, according to tests conducted during video conferences and in-person conversations.

System Random Access Memory stores a plethora of information that could be very useful for investigators. This includes end-to-end encryption certificates, PEM key and passwords, chat history and file names that have been exchanged during chat sessions, scheduled meeting information such as meeting ID's and passwords. All major artifacts were found in the memory acquired when the application was opened. There is still a difference in terms of the amount of data that is collected when a process is running as opposed to when it is closed.

Anti-forensic techniques – When two people communicate through the Zoom application interface, and one person deletes a contact, an effect in both devices causes critical data to be removed. This could still be useful to identify who the user was communicating with and some of the interactions between them. However, it is an alarming breach of trust as critical information could be removed without the user's permission.

7.2.7. Microsoft skype

Microsoft provides PSTN (Public Switched Telephone Network) Calling Plans in several countries through the Office 365 subscriptions. A Calling Plan provides a phone number to make and to receive phone calls. Forensics investigators are challenged to search for evidence in VoIP calls. This paper is intended to provide a guideline to carry out forensics' analysis on Skype for Business and on future products that might share similar architecture and protocols [183].

It is important to understand the roles and protocols shown before conducting forensics analysis on Skype for Business. The architecture can be completely On-Premise or Hybrid where users and services are both On-premise and On-Cloud. It may provide security services like implementing AES (Advanced Encryption Standard) encryption, Firewall, subnetting and protection against Denial of Service attacks. The Windows Registry collects information about Skype for Business that could be useful for forensics analysis.

Microsoft believes there is a great business opportunity in the integration of the Microsoft Office suite with the VoIP communications. An efficient methodology for VoIP forensics investigations will be required. The SIP logs could allow an investigator to clear a person who was falsely accused of making a call from his device. On 22nd October 2018 Microsoft has made generally available Skype for Business Server 2019, which is the recommended solution for customers who require an on-premise environment. Some VoIP clients and some VoIP end points may not disclose this information for all their software and firmware releases.

There are two prerequisites for using codecs in Skype forensics investigations: first, the VoIP logs must be accessible, and second, the investigator must be aware of the codecs available in the devices that participated in the call; however, some VoIP clients and VoIP endpoints may not disclose this information for all software and firmware releases. In addition, it is possible for the device administrator to modify the default codec priority list. In such a circumstance, the calling device must be located and examined. A Microsoft Teams scenario does not need servers on-premise, but SBC devices may be used to provide a hybrid solution with local PSTN connectivity in a scenario called Direct Routing. In the AudioCodes Product Notice #0345 (Audiocodes, 2018) the license for Microsoft Teams automatically enables the Opus codec. Opus is an open, royalty-free, and highly versatile audio codec.

7.2.8. Realm database

The Realm database, released in 2014 and later acquired by Mongo DB in 2019, is an opensource for mobile database management. The Realm Core is written in high-speed C++ and maps objects to disk. It supports five types of Software Development Kit (SDK) that allow access to the Core API, built in Swift, Object-C, C#, JavaScript, and Java. Two apps that use Realm are

- MiniTalk – is a messenger app used in Korea for communication and location tracking between parents and their children
- Xabber – is the Extensible Messaging and Presence Protocol (XMPP, originally named Jabber) client for Android supports multiple accounts [184].

Deletion functions are classified into four types on the basis of their features. A node consists of a header of 8 bytes and a variable-sized body with an array structure. Realm DB performs operations such as insertion, modification and deletion using the copy-on-write technique, that creates a copy of the original data and then writes on the copy. The authors present a sample calculation of the size of the array and array data according to wtype, bit width and size. The standard Realm DB file extension is '.realm' and other files have the extensions 'realm.lock' and 'realm.note'.

Data recovery schemes can be divided into two types: schemes that use node types, and schemes using data types. The experiments used B-tree node types to parse deleted data from non-overwritten nodes. Two types of recovery process are described: one using root nodes, and one using leaf nodes.

Experiments were performed with the real apps MiniTalk and Xabber, and a sample app in an Android mobile device. The apps are able to store variable data such as messages, not pre-defined static data. Their Realm DB data structure corresponds with the results of the structural analysis.

In the table unit recovery method, two to three previous root nodes could be restored on the basis of the current root node and the deleted column data could be recovered. The recovery rate according to the data length and column order was examined. The difference between the data recovery rates when only the deletion function was repeated, and after new data were inserted was confirmed. Data overwriting was completed faster when data insertion occurred than when only data deletion occurred. The proposed methodology could parse non-overwritten deleted data with high probability regardless of the kind of app.

In the table unit recovery method, two to three previous root nodes could be restored on the basis of the current root node, and the deleted column data could be restored on the basis of the restored root node. Using the column unit recovery method, substantial amounts of the deleted data could be recovered. If data are recovered on the basis of data type, a large amount of data can be recovered by the field unit method compared with the table and column unit methods. However, identifying the data stored in actual columns is challenging.

Deleted data in MiniTalk and Xabber were retained for a long time even when new data were inserted after data deletion. The longer the data and the earlier the order, the lower the recovery rate would be. The proposed methodology could parse non-overwritten deleted data with high probability regardless of the kind of app.

7.2.9. Monal and siskin

Since Edward Snowden's disclosures, end-to-end encrypted communications apps like Signal and Telegram have become popular. Extremist groups and organized criminals are increasingly using them to communicate and coordinate without detection. Instant Messaging programs provide secure private communication, but users struggle to retain anonymity. iOS, macOS, Android, Linux, and Windows have various XMPP multi-client Instant Messaging programs. Monal and Siskin are iOS favorites with 3.4 and 3.5 App store ratings (at the time of writing) [185].

These apps support Multi-End Message and Object Encryption (OMEMO), a Double Ratchet and PEP-based open standard for secure end-to-end encryption. To generate as many forensic artifacts as possible, the researchers design a series of experiments that includes one-to-one chats between a local user and other users in the contacts list, exchange of multimedia files, blocking and removing contacts, group creation and chats, etc. After a sophisticated logical acquisition of the iOS internal memory, the test local user's device was inspected for forensic artifacts. Cellebrite UFED Physical Analyzer v.7.31 created a logical picture comprising SMS, text messages with attachments, and call logs. Cellebrite UFED Physical Analyzer v. 7.31 could not decode Monal and Siskin Instant Messaging app activities.

The iTunes backup, forensic extraction, files of interest, and evidential data were identical. Because checkm8 and checkra1n exploits enable iOS devices, the researchers chose sophisticated logical acquisition with iTunes backup (iPhone 5s through iPhone X).

7.2.9.1. Monal. Monal is a decentralized open-source XMPP multi-client Instant Messaging app for iOS and macOS. It automatically encrypts confirmed user chats using OMEMO. Before enabling encryption, both parties must check and trust encryption keys. In this investigation, the researchers exchange encrypted and unencrypted messages to do a complete forensic study of collected artifacts. The "G7YU7X7KRJ.SworInstant Messaging" main folder stores conversation logs and configuration files in the "Documents" and "Library" subdirectories.

"Sworim.sqlite" is the most crucial forensic database. This database stores messages, XMPP Instant Messaging account information, file exchange chronology, etc. The message history table stores local user-buddylist messages and multimedia items. This table contains the text of each message body, the contact connected with each message, the date and time a message was sent, and a status flag indicating whether the communication was encrypted or unencrypted. This table can rebuild the message timeline.

A record of each multimedia (picture) file sent is maintained as a relative URL path in the message field. AES-256 in Galois/Counter Mode encrypts a file shared with encryption using a random key and IV. This changes the HTTPS URL to an aesgcm:/URL. A copy of the encrypted file is saved on the XMPP server and when received is decrypted locally on the device using a symmetric key sent with the secure message body.

7.2.9.2. Siskin. Tigase, Inc.'s Siskin Instant Messaging app for iOS is a lightweight, decentralized open-source XMPP multi-client (Tigase, 2020). Users can send text messages, multimedia files, and VoIP calls utilizing OTR end-to-end encryption. Mails were sent without OMEMO encryption for forensic analysis. Siskin Instant Messaging stores user data in three primary iOS folders. The org.tigase.messenger.mobile folder contains solely forensic artifacts from local user-received raw photos.

The siskinim main.db database in group.siskinims.shared contains the most important forensic artifacts. Siskinim main.db's main table is chat history. It records all text messages, group chats, conversation timelines, and metadata. The chats table records the first time each contact exchanged a message, whereas the chats read table records the last time a message was read. Deleted messages, group members, and chat groups leave these records in the database. VoIP calls are possible with Siskin Instant Messaging.

The iOS file system stores raw copies of local user-downloaded files in the/private/var/mobile/Containers/Data/Application/org.tigase.messenger.mobile/Library/Application Support/download directory. Undark 0.6 failed to restore database data like Monal.

7.2.10. Matrix protocol and Riot.im application

It is free to set up and maintain a decentralized IM platform using any of a number of IM protocols. The Matrix protocol was first developed in 2014 under the name "Amdocs Unified Communications". This protocol aims to build a decentralized, open platform for real-time, secure communication. The first stable version of the Matrix protocol was launched in June 2019, and Riot.im is also quite recent. In order to fill a knowledge gap, this study offers a forensic method for examining them from the perspective of a digital investigator [186].

On Windows 10, Riot.im may be installed without requiring administrator rights. After restarting the application, a logged-in user will continue to be logged in. The program offers tools to delve deeper into the source of messages and by default allows users to view conversations as suspects may. Based on the message type, the "content" object is used to store the message's contents. The whole username of the user who sent the message is contained in the "sender" key-value pair.

Each device that supports end-to-end encryption and uses the Matrix protocol has a unique device identifier. The device's message encryption is broken using this identity along with the session keys. Key-value pairs that were not included in the signing procedure can be found in the "unsigned" object. This indicates that after signing the event, they may be changed. These values cannot be changed by a suspect after the event has been created, presuming that the suspect has no access to the server.

This description can provide information about the tools or the language a suspect is using. Temporary message events are generated by the Riot.im program, which is slightly different from the Matrix server's message events. The method used to construct a temporary event identification is the most significant distinction. The combined transaction identification and the room identifier accomplish this. Experiments revealed that it was impossible to send messages while offline.

The date and time the Matrix server created the message event were revealed to be the "origin_server_ts" key-value pair in the final message event. The trials also demonstrated that the value in the "age" key-value combination is unaffected by the date of the computer on which the Riot.im application is running. The "transaction id" key-value pair might also be used to identify which messages were sent by utilizing the Riot.im application. All messages sent in the unencrypted room were recovered using the "leveldb-tools". It appears that data that will subsequently be saved in a file with the ".ldb" extension is temporarily kept in the ".log" file.

The creators of Riot.im made the decision to produce "events.db," an encrypted SQLite database, as a secondary data repository which is kept in the location: user > AppDataRoamingRiotEventStore/. The log entries revealed details about the user and the device, including the device's unique identity; the user's entire username, including the server to which they belong; and the display name of the device.

User data for the Riot.im web browser is contained in the "profile" table. Additionally, the "rooms" table contains a unique identifier for each record in the table. This is the key-value pair of the events' "room id" that also stores the room identification. The default download directory, the most recent directory used for file uploads, and the spellcheck language are all located in the directory "preferences." This information can infer which directory was most recently used and where the downloaded files might be found.

7.2.11. Wickr

The authors examine the three Instant Messaging apps that offer security features, namely Wickr Me, Wickr Pro, and Private Text Messaging, and detail the encryption algorithms that they employ. Wickr on Android and iOS, and Private Text Messaging on Android were studied. Using reverse engineering, the process of encrypting personal data, including the key creation mechanism were studied. They identified a key to encrypt and decrypt the data, then studied the structure of the encrypted data; encrypted data, such as databases, content, and multimedia files, and demonstrate decryption; and then how to validate user-entered passwords for each app, recommend quick verification methods, and recover user-entered passwords for Private Text Messaging [187].

Wickr is a private messaging application that provides an end-to-end encrypted platform with a variety of capabilities, such as phone and video calls, file sharing, single sign-on, mobile device management integration, and app lockout.

For data extraction, both rooted and unrooted Android and jailbroken and non-jailbroken iOS handsets were used. It is possible to back up the data of pre-installed applications, multimedia files, and setting information; however, the method varies according on the manufacturer and whether data encryption is enabled. When using extra settings or encrypting data with a user-entered password, more data can be collected. First, the encryption and decryption techniques for the essential data were found. Then, it is decided whether the data are fixed, or entered externally. Following the verification of the supplied parameters, data decryption is conducted. The researchers created a tool to illustrate that the process may operate independently of apps.

Wickr is a private messaging application that provides an end-to-end encrypted platform with a variety of capabilities, such as phone and video calls, file sharing, single sign-on, mobile device management integration, and app lockout. The researchers created the extraction and decryption method for encrypted data, contents, multimedia files, and user-entered passwords.

KDF is an algorithm for deriving ciphertext decryption keys. Despite offering many KDF algorithms, the ciphertext in the sk.wic file is decrypted using just Scrypt. Scrypt accepts six input parameters: P, S, N, r, p, and dklen. P is the password entered by the user, whereas S is a 16-byte random value. As the primary evidence, the encrypted Wickr database preserves the chat history in plaintext. However, other data, including as user information, app information, and the encryption keys, are encrypted. The database's contents are encrypted using the same manner as the iOS version of Wickr.

During a chat, Wickr encrypts and stores multimedia files, which are renamed in GUID format. On both Android and iOS, the data structure of multimedia file information is identical. The CDK is encrypted and stored in the sk.wic file or ZPT column using the user's password. The authors proposed a method for determining whether or not the derived key generated from a user password guessed by the analyst is valid.

Using Wickr settings, the hashcat hash cracking tool, and an RTX 2080 Ti GPU, Scrypt benchmarks were measured. If a password has 72 characters (a-zA-Z0-9; 10 special characters), the predicted password recovery time for a single GPU is 297,414 years and for eight GPUs it is 37,176 years. This indicates that brute-force password recovery is almost difficult.

Through end-to-end encryption, the Private Text Messaging app secures personal text messages and phone calls from external attacks, such as eavesdropping. In the app, the majority of data, including the database, are secured. Described is a method for decrypting the database and recovering the password entered by the user. The PBE uses the PBKDF2-HMAC-SHA256 function as its KDF and encrypts data with AES128-CBC. Key A can be identified from Key B based on the owner ID column value.

When the most significant byte of the decrypted BLOB is removed, the upper 16-byte key is Key B and the lower one is IV B. The user-entered password can be acquired and validated in two ways: by using the password column of the kexinuser table or by processing the generation of Key A. The above procedure was discovered by analyzing the Dalvik EXecutable (DEX) file of the APK. Using hashcat and a GPU (RTX, 2080 Ti), benchmarking demonstrates that the second method is faster than the first.

Wickr encrypts the core data with AES256-GCM and stores the CDK using the password given by the user. In addition to analyzing the encrypted data's structure and the key acquisition process used for encryption and decryption, the researchers decrypted the complete encrypted data set. In this procedure, password verification methods were proposed and their recoverability was studied. It was determined that it is difficult to conduct an exhaustive search to retrieve user-entered passwords due to the fact that Wickr's KDF was implemented using Scrypt. Consequently, methods for validating user-entered passwords were presented.

Using the user-entered passwords, the Private Text Messaging application encrypts the data and keys required for data encryption. Here, two types of encryption keys used for data encryption and decryption are identified, along with a technique for validating the user's password. Private Text Messaging, unlike Wickr, sets the amount of KDF iterations used for the user-entered password to 100, enabling password recovery by exhaustive search. Finally, the full dataset was decrypted using the discovered password and each key was categorised.

7.2.12. *Vault app*

The term content hiding app refers to apps that enable users to conceal and safeguard images, videos, documents, and other files on their mobile device. These applications are also known as vault apps, safe box apps, and app lockers. The writers explain how to recognize vault applications in the App Store. Vault Identifier and Data Extraction (VIDE) is built for iOS devices, however the method may be readily adapted for Android smartphones. It could be used for forensic investigation of a live device with the necessary precautions about cloud-based data storage [188].

VIDE could also be handy for those concerned about prospective vault apps that conceal sensitive data on mobile devices. By mining program descriptions and API calls from.apk files on Android devices, previous research has classed apps by a set of capabilities ("claimed functionality"). For iOS,.ipa files are not easily accessible to third-party apps, hence API call classification is impossible. This may not be helpful for recognizing genres that span numerous categories, such as content disguising apps. Very few articles have focused on the forensics of content-hiding apps. Using reverse engineering and forensic analysis, other studies have investigated the specifics of a number of popular vault programs for Android devices, as well as the detection and analysis of vault applications on Android devices.

7.2.12.1. VIDE system design. On a smartphone, vault applications may not wish to be labeled as such. Apple has stringent review criteria, yet it may be possible to evade them and post fake information about a vault application on the App Store. The interfaces of the majority of content-hiding applications include a calculator, a keypad for entering patterns, a gaming interface, etc. The objective of the method developed by the researchers is to recover artifacts from vault apps and not from other programs on the device. Two key components comprise the system: an identification system and an extraction engine.

The authors discuss the vault detection and automated extraction technique, as well as the identification and extraction of content-hiding applications in all App Stores, not only the US App Store. Apple operates 134 App Stores in five areas (the sub-regions) at the time of the researchers' study. In the proposed method, downloading is not required in order to get the necessary information to detect apps hiding content in certain regions.

This initial categorization produces the group of apps labeled prospective vault apps (PVA). Vault App DB contains seven tables, with the applications table being the most essential. The researchers began by analyzing the whole text data for a small sample of vault applications. Then, they selected a collection of keywords that they believed would cover any content-hiding app, in the sense that at least one of the phrases must appear in the app's title for a user to discover a vault app. The app id is the primary index for the Apps Table as each app has a unique identifier.

The tag field stores the classification of a PVA as vault or non-vault based on subsequent classification. The system accounts for the use of several character sets, such as Russian, Korean, etc. The initial scan takes 48 min on a MacBook Pro with an Intel Core i5 processor and 16 GB of RAM. Of the 2364 PVAs from the US App Store, it was revealed that 178 were removed within a period of 3 months from the date of the initial scan. Unfortunately, neither the app's removal nor its cause are communicated to users. Apple erased 7.5% of PVAs within three months, indicating that many apps no longer had any information about them in the App Store.

The vault/non-vault classification is based on the presence or absence of full text information for a PVA. They evaluated Gaussian Naive Bayes, Support Vector Machine, and Decision Tree binary classifiers. For the purpose of binary classification, additional keywords (features) were added to the preceding list of 11 keywords resulting in a total of 20 keywords that were designated the feature set: private, sensitive, censor, protect, decoy, privacy, hide, vault, secure, safe, images, movies, notes, passwords, contacts, password-protected browser. Random seeds were used to divide the training and test datasets into 60% (Training Set) and 40% (Test Set), respectively.

7.2.12.2. Forensic analysis of vault apps. The experiment is based on the examination of files and folders retrieved through logical acquisition from two iPads: one non-jailbroken iPad and one jailbroken iPad. Before conducting the research, the iOS devices were factory reset to eliminate any existing data and settings. On one of the iPads, iOS 9.3.5 was installed, followed by the installation of multiple software package managers.

Typically, content-hiding applications are secured by a biometric, PIN, or alphanumeric password. Vault apps are used for a variety of purposes, including multimedia storage, password storage, private browsing, decoy mode of operation, surveillance, and the storage of encrypted content such as photographs and text. Seven well-known vault programs were studied to determine their functioning, characteristics, and data storage architectures. Apps that appear to have a different function (using a decoy interface) or contain a different data set (in decoy mode) are generally used for multimedia storage. This decoy feature adds a layer of difficulty forexaminers trying to access the iPhone of a suspect. The "My Secret folder" application's directory structure indicates the possibility to store photographs, audio, and notes. Artifacts extracted from the My Wallet Lite application's sqlite database file, located in the Documents folder. It was not necessary to know the app's passcode to view this information.

Penzu is a free multimedia journaling app. This program locks journals using alphanumeric passwords but does not encrypt information. Penzu's servers and the device save journal edits, making them more accessible. The software requires account registration before content input, making this feature available. No matter the journal's passcode, the user's data was easy to find in the Penzu program folder. This app's "Documents" directory yielded thumbnails and files. The file penzu.db is noteworthy. The remote URL in the database links to all photographs in the device's journals, allowing access to Penzu's Amazon AWS-hosted material. This image was accessible without Penzu login. Metadata: journal password hint, user first name ("Mobile"), and account password hash. Since URLs can be accessed, sensitive Cloud data can also be accessed.

My Secret Folder vaults photos, videos, and notes. My Secret Folder lets users store images in albums. The Library folder stores all data unencrypted. This application names images by album name and number. The "Audios" directory holds.m4a audio files with a recording time stamp. "Break-in reports" log invalid login attempts in this app. Every unsuccessful login in My Secret Folder takes a front-camera snapshot. Invalid logins store location coordinates. The application folder's "secretfolder.sqlite" database file recovered this data.

Secret Photos - KYMS Free (IdeaSolutions, 2018) is the only app in the research that advertises "military quality AES-encryption" for photos, videos, recordings, and documents. The backup directory structure is similar to the other apps, but it does not contain unencrypted media. Database files require keys too. "[filename].jpg.encrypted" or equivalent indicates that material has been added to the app. Unencrypted database strings were the key to retrieving user data from this application. Some database strings were plain text, but most were encrypted. KYMS keeps decoy mode content in ". collections.fake" and uses separate encryption keys.

7.2.12.3. Automated extraction engine. The extraction engine's objective is to extract as much information as possible from each vault app on an iOS device. As a high-level perspective, the extraction engine groups the extracted artifacts by the App's Bundle-ID and artifact type. In the plist/json files, this information is identified by searching for terms such as pass, passcode, cloud, sync, mode, and alternate. In addition to the data submitted by the user, Vault apps are identifiable by their Bundle-ID, which identifies features such as break-in, date and time a file/ content was stored, whether an effort was made to delete a particular content, etc. Once a vault app has been recognized by VIDE, the Manifest.db file is used to determine the app group location. The file will be stored in one of four subfolders within a folder called after the bundle identification of the application, based on its kind and content: Plists, Databases, Media, and Others.

7.3. Behavioural evidence

The utility of Behavioural Evidence Analysis has gained attention in the field of digital forensics in recent years. BEA has applicability and utility when integrated within the digital forensic investigation process in a post-mortem examination, analysis, and interpretation of the digital evidence for specific types of digital crimes. There is no digital forensic process model that provides clear, explicit, and comprehensive steps for "how" it can be performed within the investigation process. There is a gap in the literature on how behavioural evidence analysis is integrated into the digital crime investigation process. Models are being developed using real digital crime case work.

Criminal profiling aims to create a profile of the demographic and behavioural characteristics of an offender based on known characteristics of those who have committed similar crimes. It offers two distinct strategies for creating a subject profile: inductive and deductive approaches. Inductive profiling uses statistical analysis of behavioural and psychological data from convicted criminals to identify a generalised behavioural pattern and personality traits of a typical offender. Deductive profiling, on the other hand, relates to case-based investigations and analyses evidence from the case in question.

Behavioural Evidence Analysis is a deductive, case-based investigative approach that analyses evidence from a specific case to identify the specific behavioural and personality characteristics of the suspect. It uses the forensic evidence available for a case to understand and reconstruct the behavior of a criminal. This approach consists of four types of analysis: equivocal forensic analysis, victimology, identification of crime scene characteristics, and identification of offender characteristics.

Behavioural analysis of digital data can benefit the investigation of certain types of digital crimes. It helps investigators develop a more effective understanding of the individuals involved in the offence. Analysing files from their computer can reveal indicators of suspicious activity, as well as signature behavior and personalised characteristics of the offender. This helps the investigator to develop leads, and determine the location of additional sources of evidence.

Dozens of digital forensic process models have been proposed, developed and refined during the last twenty years. Many models were single tiered and focused on the higher levels of the investigative process without much detail of their underpinning principles. It has been suggested that additional specific steps within each phase are needed to provide adequate detail for them to be useful to the digital forensic investigator. There have been previous attempts to incorporate aspects if behavioural evidence analysis within the digital forensic investigation of digital crimes.

A cyberstalker profiling methodology incorporated behavioural evidence analysis elements into a standard digital forensic investigation framework. The model provided minimum detail about victim or offender behavior, probably due to the fact that it was tested using a simulation that provided limited offender and victim activities. The focus was on the technical phase of the methodology by using digital evidence to guide the search and recovery of evidence. The use of BEA stages was applied in conducting the investigation, but without any guidelines on how to conduct these stages. Further tests using existing cases and related digital evidence are needed to better evaluate the applicability and utility of the model.

Digital forensic practices place greater emphasis on the principles of computer science and engineering. As a result, the investigative process is mainly concerned with data collection, with less focus on its examination and analysis. A model was proposed which incorporated aspects of behavioural evidence analysis into the process of digital forensic investigation. This included six phases: (1) case classification, (2) context analysis, (3) data collection, statistical analysis, timeline analysis/visualization, and (6) decision/opinion.

Timeline analysis/visualization aims to combine the results from the frequency analysis phase with their associated timestamps to visualize usage of the computer. This can further assist the investigation, for example, by associating computer usage at a specific time with a specific individual (in cases where the computer has multiple users). The decision/opinion phase concentrates on producing the final report, and addresses the questions presented at the start of the investigation [189].

7.3.1. *Embedding behavioural analysis into the investigation*

Mutawa et al. (2019) [190] reported on the culmination of an extensive research effort that established a digital forensic model that incorporates behavioural evidence analysis techniques. It centred on the post-mortem laboratory inspection, analysis, and interpretation of digital evidence related to digital crimes. The crime categories of possession and distribution of indecent pictures of children (IIOC) and cyberstalking were chosen for many reasons. Digital evidence and artifacts do not reside on a single electronic media, but are dispersed over multiple platforms (e.g., the devices of the offender and the victim, as well as the online environment). The categories of IIOC and cyberstalking generate distinct forms of evidence that can be collected from digital devices during an investigation.

This evidence can then be analysed using behavioural evidence analysis to develop a profile of the offender. The selection of instances was based on the following inclusion criteria: (1) usage of a computer as the primary offending platform; (2) availability of image files; and (3) availability of interview scripts with offenders/victims. A case study approach was used to provide a descriptive, in-depth analysis of each instance and a clear, step-by-step guide for applying the model's many stages.

7.3.1.1. The behavioural digital forensics investigation model. Proposed is a digital forensic investigation model with behavioural evidence analysis. It attempts to give a realistic, systematic, multidisciplinary method to post-mortem examination, analysis, and interpretation of digital crime devices. The model follows digital forensic procedure concepts (i.e., confidentiality, integrity, and availability). The paradigm comprises four phases: review, recognition, analysis, and interpretation and reporting. These models were chosen because they include relevant components of behavioural evidence analysis.

In the first phase of an inquiry, accessible evidence and case facts pertaining to criminal behavior and victimology are reviewed. It also investigates perpetrator motivations, behavior, and features, and crime scene characteristics. This phase helps the investigator plan the inquiry (e.g., design a specific search criterion, form a specific hypothesis).

Before analyzing the evidence, the case's context must be understood. When known, suspect(s) and victim(s) must be described; and the victim and offender interview scripts and victim statements must be reviewed. This helps the investigator understand the incident. It also presents an initial offender profile that can inform further investigative stages.

Creating a victim profile (forensic victimology) helps solve case problems. It comprises demographics, technical skills, physical traits, lifestyle, and behavioural traits. This examination helps the investigator determine victimization opportunities and the victim-offender relationship. Understanding the victim helps explain the offender's reasons. Classifying the perpetrator helps design an investigation strategy.

The investigator will preview confiscated digital gadgets. This helps the investigator prioritize the devices under inquiry, select an inspection starting point, and build an examination plan. Depending on the case's complexity, the investigator may need to combine strategies to identify and collect evidence files and artifacts.

Identifying the authorship of evidence files and artifacts is vital when investigating a crime. Unless just one person accessed the device under inquiry, the investigator must link damning files to a suspect. Keystroke mouse-movement analysis, email behavior, computer usage, credit card use, and game tactics may help with author attribution.

Frequency and language analysis can help investigate digital crimes. Cyberstalkers often convey emotions in writing which can reveal the offender's motivation. Writing style and terminology might also indicate an offender's emotional state. Keystroke and mouse-movement analysis, computer usage profiling, email behavior, online gaming tactics, and credit card use are further emerging ways for author attribution.

Sorting, grouping, or filtering files can provide a representative dataset that aids in criminal interpretation and reconstruction. Analyzing a file's timestamp (made, accessed, updated) can reveal how users used it. Producing a period of user activity paired with content analysis can assist eliminate suspicions.

In the final stage of the investigation, the practitioner defines and contextualizes all crime-related occurrences to answer investigative inquiries. At this level, the practitioner must remain objective and assess all possible interpretations of the combined information and timeframes. They would develop a timeline and try to reconstruct the crime using evidence gathered in earlier steps. This would be used to create the requested report.

case study on Facebook impersonation and slander. This case demonstrates the model's use in digital forensics. Miss X complained to police that her Facebook account was impersonated and defamed. The initial inquiry traced activity to a suspect's Internet account (Mr Y). Mr. Y disputed the claims and said he didn't know Miss X. Three laptops were taken from Mr. Y's home after a search warrant.

The main researcher gathered information on the victim, suspect, and crime. She was a 32-year-old Middle Eastern single woman with a roommate. Her password-protected workstation was unlocked when she wanted to leave the office briefly. She didn't suspect anyone. Defamatory information was posted on Miss X's Facebook profile as Miss X the Frog. Miss X, her roommate, and two coworkers accessed her computers. One of them likely stole her login information. Even for a few minutes, leaving her desktop unlocked puts her at risk. Keyloggers and monitoring software can be installed in minutes. Sharing her PC enhanced her vulnerability.

Miss X's defamed Facebook page was searched on each PC. Positive search hits on Mrs. Y's PC appeared on her laptop. First, the researchers analysed Miss X's Facebook, email, and social media profiles. First string searches found no matches with her disparaging Facebook posts. Arabic phrases were translated to Unicode escape characters, and a second search was done using the comparable set. Ms X's offensive remarks received 3 and 4 hits throughout the search.

Most of Miss X's Facebook ID search hits were in index.dat (i.e., a database file used by the Internet Explorer web browser to store information on user Internet activity such as visited web URLs, and timestamps of access). Source code analysis shows the user got into Miss X's Facebook account and visited editable sites. No hacking software, keyloggers, or remote monitoring software was found. Analyzing Miss X's officemate's correspondence reveals a friendship between them. During the two months before the incident, she received several unpleasant emails about her weight and work. It showed Ms X's coworker's mood at the moment.

A Facebook user accessed Miss X's profile and edited her Work and Education sections. Miss X stated she didn't know Mrs. Y: Mr. and Mrs. Y are strangers to me. Mrs. Y's communications to a colleague suggested a second suspect (Miss X's coworker) who had unfavorable feelings about her weight and work. Miss X's workstation evidence led to the hypothesis that Mrs. Y committed the crime. Since the case was archived, the researcher could only use the available evidence. This would have led to more research to support or disprove hypotheses.

The case study highlighted the interpretive and investigative utility of merging digital forensic and behavioural evidence analysis. The proposed model is an investigative instrument that digital forensic practitioners can use to investigate situations of interpersonal crime. Following the specified approach, it took around 5 days to complete the examination and analysis of the in question laptops, which was much less time than the initial investigation's 13-day duration.

The Review step allowed the researcher to develop a clear framework for the incident's various features. The daily routines of the victim were evaluated in order to build hypotheses regarding the elements that produced potential for victimization, and possible perpetrator motivations were also explored. Prioritizing the study of Mr. Y's computers aided in accelerating the inquiry and conserving resources. The discovery of Miss X's officemate's correspondence was of great importance to the investigation. This could have supplied interrogation strategies and methods to direct inquiry and rebut false responses.

7.4. Image clustering

Images shared online can be considered as complementary information used to detect evidence in digital investigations, e.g., identity theft, online sexual harassment, piracy, cyber stalking and cyber terrorism. In tracing the history of an image, identifying the source which captured the image is of major interest. The task is more challenging when the original images and smartphones are not available. Blind analysis has to be applied to investigate the right source for an image. Clustering the collected images based on the residual noised extracted from the corresponding images, into an unknown number of groups can be a way to associate different crime scenes [191].

It can provide the investigators with more information to link the evidence to the seized hardware that are owned by the suspects, in the future. Outliers are defined by the concept of a cluster and they are recognized as the objects which are not assigned to any cluster. The method is stable against the number of shared images and the loss of image details caused by the process of image compression applied by platforms, that degrades the quality of the images. The method is evaluated on the VISION dataset, which is a public benchmark including images from 35 smartphones.

The authors uploaded and downloaded 7480 Native images taken by 35 smartphones on the main social networking platforms such as WhatsApp (W), Facebook High Resolution (FH) and Facebook Low Resolution (FL). The clustering was evaluated and it was found that Density-Based Spatial Clustering with Applications with Noise algorithm is more reliable in detecting the shared images. The number of outliers to was set to 3000 and applied another outlier detection method, Distance to K-Nearest Neighbor (DKNN). The algorithm removed successfully the outliers.

Clustering the uploaded images by users on social networking platforms is a challenging task as users may upload images from different sources. It was aimed to have the clusters with high values of Precision Rate, Purity and a low value of false positive rate. For example, merging the residual noises of different cameras into the same cluster increases false positive rate. The authors found an accurate analysis on how the shared images influence the clustering of the taken images and fingerprinting the smartphones of users. Most of the running time of the proposed method is spent for input/output, for loading residual noises into RAM. In doing so, only the correlation of the more similar residual noises are computed. Also, the adaptive threshold which is computed for the merging of the candidate clusters prevents from merging the clusters including images from identical models of smartphones.

Clustering the images uploaded by users on their profiles is a way of fingerprinting the camera sources. Users may upload different types of images, i.e., the images taken by their smartphones (taken images) and a variety images like single images from different sources. The proposed method exploits hierarchical and graph based clustering algorithms, and an adaptive threshold to cluster the images.

8. Cyber security

When a computer security incident occurs, an investigation team starts to examine the reasons behind the incident. The set of procedures employed is part of the Incident Response process/and is defined by four stages: 1) preparation; 2) detection and analysis; 3) containment, eradication, and recovery; and 4) post-incident activity (lessons learned and reporting). As in any other areas of investigation, the purpose is to answers the questions of who, what, when, where, why and how. Memory forensics is one of the fundamental steps performed during the detection and analysis stage and can be very important when access to device drives is problematic, for example, in a cloud computing environment. NIST (the US National Institute of Standards and Technology) provides a guideline to integrate forensics techniques into incident response. Any memory artifact can be retrieved from a memory dump either using the appropriate internal OS structures to go through the data content or using a pattern-like search in the full dump.

One of the most common security incidents is the presence of software specially designed with malicious purposes (known as malicious software or malware). The life cycle of malware is comprises several stages, which are similar to the stages of an Advanced Persistent Threat (APT). Some of the extensibility points in Windows OS are susceptible to be used or abused by malware so that it can persist in the system, of which there are four different categories: system persistence mechanisms, program loader abuse, application abuse, and system behavior abuse. One useful memory forensics tool is Winesap, which extends the Volatility framework and allows a memory forensic analyst to detect the presence of unknown and rare programs.

The exposure of the Industrial Control System to cyber threats could inflict serious disasters on society, as the following examples demonstrate. In 2010, a cyber-attack using Stuxnet infected the programmable logic controllers controlling the field devices of a nuclear power plant and destroyed more than 1000 centrifuges. In 2015, a malware attack using Black Energy3 against transformers in Ukraine caused a massive blackout. Most cyber-attacks targeting the Industrial Control System aim to hijack control of the physical system and cause malfunctions of the field devices. It is necessary to detect cyber threats and defend the Programmable Logic Controller, and to conduct digital forensic investigations into intrusion incidents. Data must be collected while the controller continuously is operating with the power turned on, and loss of data could be enormous. A cyber-attack on a Programmable Logic Controller (PLC) can reveal an important trace of the attacker's intention.

8.1. Programmable logic controllers

Industrial control systems (ICS) are used to regulate physical processes in vital infrastructures such as power grids, nuclear reactors, and gas pipelines. The forensic examination of suspect PLCs is essential for answering numerous issues regarding hacks. The majority of current methods for collecting the volatile memory of a PLC use an ICS protocol to read memory over a network. The study provides a forensic framework, PEM, to remotely acquire the complete memory of a PLC without interfering with the PLC's normal function; a new control-logic assault that updates in-memory firmware to be more covert and durable than existing attacks. In addition, the authors give a case study of employing PEM to investigate an assault on a gas pipeline testbed [192].

A Schneider Electric Modicon M221 PLC regulates the opening and closing of a solenoid valve and the activation and deactivation of an air compressor. The control logic of the PLC is written in ladder logic and consists of 16 rungs. It features 9 digital inputs (24 V), 2 analog inputs (0e10 V), and 7 digital outputs of relay type (5e125 V DC/5e250 V AC). An attack tailored specifically for a gas pipeline system is described.

It is presumed that the attacker is aware of the PLC model and firmware version of the target. In a closed-loop system, the difference between measured values and set points defines the control action. If a comparison operator in control logic does not yield valid results, the control actions resulting from logic execution will be incorrect. The attack modifies the table entry values for the greater-than operator at memory address 0 × 809c (0 × 8000 0 × 27 * 4). It modifies the inserted malicious operator's value to 0x1EB00.

The gas pipeline system can be physically destroyed with only 11 bytes of code. The PEM is used to acquire and examine the memory of the suspect PLC. Python is used to implement the PEM protocol. The creation of 40 duplicators with distinct source addresses and block sizes.

The objective is to extract and analyze control logic from the memory dump. Control logic is one of the most crucial artifacts for ICS security incident investigations. By examining the malicious control logic of an attacker, their goals can be determined and a more effective countermeasure devised.

Signatures indicating a zip file were discovered in the external RAM space. The zip file can be extracted and decompressed into an XML file. The XML file provides the semantics of the control logic's data items. It can be concluded from this information that ladder logic controls a physical process involving an air-pump and a solenoid valve. PEM is a framework for remote memory acquisition for PLCs that can extract the complete memory via a network while the target PLC is managing a physical operation.

8.1.1. *Control logic forensics framework*

Industrial Control Systems monitor and control industrial physical processes (such as nuclear power plants, electrical power grids, and gas pipelines). Programmable Logic Controllers are the primary target of a cyber assault designed to damage a physical process. The network traffic between the control centre and field sites will contain proof of the transfer of malicious control logic if it is collected. Reditus is a unique control-logic forensics framework for injections of control logic. Reditus automatically extracts and decompiles control logic from a network traffic dump without the need for reverse engineering. A virtual Programmable Logic Controller engages the engineering software via Industrial Control Systems network communication [193].

Gas pipelines compress and deliver gas to remote receivers. Air compressors, receiver tanks, and solenoid valves make up the physical process. The compressor compresses air and stores it in a tank connected to a receiving tank by a conduit. Solenoid valves close tanks. The valves open to enable pressurised air flow through the line to the receiving tank.

Pressure transmitters, solenoid valves, and Programmable Logic Controllers monitor and control field-site gas pipeline infrastructure. The pressure transmitter sends data to the receiving and storage tanks' PLCs. The Programmable Logic Controllers open valves to allow pressurised air to flow through the pipe to the receiving tank. Second, they release air if tank pressure rises to maintain a desired level.

HMIs, historians, and engineering workstations receive data from Programmable Logic Controllers. HMIs graphically show gas pipeline process status. The Historian database stores Programmable Logic Controller data for analytics. The Engineering Workstation remotely programs, configures, and maintains PLCs using engineering software.

Engineering software writes PLC control logic. Industrial Control Systems providers use this proprietary programming software to configure, program, and maintain their PLCs. Schneider Electric, AlleneBradley, and Omron PLCs use SoMachine Basic, RsLogix 500, and CX-Programmer.

Five PLC programming languages are defined by IEC 61131-3. Ladder logic (LL) and function block diagram (FBD) are graphical, while sequential function chart (SFC), structured text (ST), and instruction list (IL) are textual (IL). Ladder-logic displays instructions graphically. Instruction-list programs are textual, like assembly language.

Reditus is a framework designed to study control-logic injection attacks. Reditus is comprised of a virtual Programmable Logic Controller that can interface with engineering software and use its upload capability to recover high-level control logic from network data. It is a fully automatic method that requires no understanding of Industrial Control Systems protocols or the underlying binary control logic format. Reditus is a virtual Programmable Logic Controller framework that may transfer control logic via network traffic recorded during an upload or download activity. Reditus must initially discover the locations of all session-dependent variable fields within the messages.

Second, it must discover the mapping between download and upload messages in order to provide an appropriate response to the upload request. Reditus is a framework that discovers the types of fields in the upload response message from the Programmable Logic Controller (PLC) and the mapping between those fields and the corresponding fields in the download request message. Reditus is taught using only benign PCAP files to ensure it acquires the correct message format. Reditus creates groups depending on the length of messages in each pair to ensure that all communications have the same message format. It is presumed that the location or index of each message group's session-dependent field is consistent.

In the testing phase, Reditus tackles the second problem by comparing a freshly received request to comparable requests in the database. Reditus employs a heuristic approach to construct the engineering software upload template. The framework specifies the session-dependent fields of a Programmable Logic Controller's upload response (PCAP). This data is merged with the PCAP file's dynamic, control logic, and static fields to generate the template. Reditus then selects the fields that are next to, overlapping, or contained inside any of the baseline fields, while ignoring the other fields.

The assumption was made that the size of the length field is two bytes when designing Reditus. The message length is a common field in virtually every protocol. Reditus slides a window of two bytes, or four characters, to determine the precise placement of the length field in each upload request message. It then calculates the length of the message after the window and compares it to the number within the sliding window. Static fields, the portion of a message that remains constant across all upload response messages, are a crucial element of upload messages (e.g modbus function code). Reditus employs a heuristic-based strategy based on the longest common subsequence (LCS) present in both the download request and upload response.

In possession of the control logic, Reditus merges all fields to build the final template. During the testing step, Reditus examines the network capture in the form of a PCAP file. First, a database of request and answer messages present in the PCAP is generated. On the same port as the engineering workstation, it then launches a Programmable Logic Controller server. Once Reditus is operational, the control engineer is able to connect to it using engineering software.

For all new request messages from engineering software, the virtual Programmable Logic Controller discovers the most similar request message in the database and modifies the response based on the new session. It removes the control logic piece for download traffic and inserts it into the previously constructed upload template. It is presumed that the user provides the upload or download direction information to Reditus.

Reditus is distinguished by its precision and functional-level precision. Experiments revealed that Reditus could produce the correct upload template for a genuine Programmable Logic Controller with 100% accuracy throughout the full dataset. The most essential metric for evaluating Reditus is the reliability of the control logic it transfers. Reditus uploaded 40 control logic programs containing 213 rungs and 888 instructions with a transfer accuracy of one hundred percent. Reditus received 1852 unique read messages while sending 40 distinct control logic files, of which 1812 were present in the database.

8.2. *Command block collection*

The researchers intend to identify alterations in the logic data of project files used by the Engineering Workstation for operating field equipment such as PLCs. When a project file is modified, the proposed solution involves gathering the data in a different storage space and then restoring it to its pre-attack condition. Human Machine Interface refers to the software and technology that allow operators and controllers to interact [194].

Operators are able to monitor the state of the process, record data, alter the settings, send commands to predefined variables, and manage the algorithms. The Remote Terminal Unit is a data gathering and control device designed to enable Supervisory Control and Data Acquisition and Distributed Control System remote base stations. In comparison to conventional information systems, the Industrial Control System has become a comparatively simple assault target. It is susceptible to social engineering attacks employing a USB storage device or laptop computer belonging to an authorized system user. Due to the fact that such assaults use the operational layer, i.e. the Engineering Workstation, to attack field devices, specific cyber security precautions are required.

Siemens' Totally Integrated Automation Portal Step 7 is an integrated development environment tool for configuring and developing Siemens' Programmable Logic Controller programs. The project files contain all information about a programmable controller's program code blocks and configuration. Forensic investigators can identify what has been changed by analyzing tags and ladder logic areas in PLUSBLOCK. Changes to a project file can be made by an attacker directly accessing the binary code without going through the Totally Integrated Automation portal.

The authors propose a tool for collecting, retaining and recovering files by monitoring changes to project files. The collected data – including event time, hash value, and version – are stored in a pre-built database. When the Totally Integrated Automation Machine runs, it determines which version of the project file needs to be restored using the project information and event time information stored in the database. It can use this information to carve the recovery area from the original project file and calculate the hash value.

The test was conducted to verify the method of detecting project file updates and collecting and recovering data based on a scenario involving an attack on the project file. Stuxnet was used to infect the Engineering Workstation through a user's worm-infected USB. It altered the dynamic link library (DLL) related to the control logic program. It used an authorized engineer's USB to overcome the air-gap of the Siemens SIMATIC system. It manipulated the code block which set the centrifuge rotations, thereby causing the field device to malfunction.

The proposed tool was able to detect a file update when a part of the control logic was modified through the Totally Integrated Automation portal. It also confirmed that the hash values before and after the modification matched. The tool also detected an alteration when the project file PEData.plf was directly modified in a random area with a hex editor.

8.2.1. Volatility

The Volatility framework (Volatility for short) was released in 2007 at the BlackHat DC conference. Volatility supports analysis of memory dumps from Windows, Linux, and Mac OS, in both 32-bit and 64-bit environments. The Volatility Foundation organizes a contest to incorporate new features in the tool.

8.2.1.1. The Windows Registry. The Windows Registry is a hierarchical database that contains critical data for the normal operation of Windows and other applications. It stores data regarding system booting, system configuration, and (per-user) software configuration. Internally, this database is divided into files called hives, which contain a registry subtree. During system start-up, Windows maps these hives – stored on disk – into the system memory as a treelike structure (in particular, as binary trees).

When a new user account is created in the system, a file is also created and set up to represent his/her specific user configuration. This user configuration is later loaded during the system start-up process. The mapping process from on-disk hives into memory is part of the Windows boot process, and occurs at four different times. The Winboot process reads the in-file HKLM\SYSTEM hive to determine which device drivers need to be loaded and maps that hive into the memory.

During programs start-up, the interactive Windows logon manager process (Wlogon) reads the data from the user profile currently signed in and maps it into HKCU. This step allows the user to know how the system is configured and then behave accordingly.

Volatility provides a set of functions to work with the in-memory representation of the Windows Registry. These functions allow a developer to obtain the current system configuration, return a registry key, enumerate registry subkeys, and retrieve all keys in last modified order. When working with Volatility, it is necessary to first specify the on-disk hive to analyze.

8.2.2. Insider threats

Insider threats are not new, however, the increase in insider threat cases in both public and private organizations is an important security research problem among security practitioners. Insider threats domain includes a wide array of contributions that defines the notion of insider and insider threat including its types and characteristics. Superusers have complete control over the execution environment and can delete or modify the data and meta-data of potential evidential artifacts using his/her access privileges. In an extreme scenario, the superuser may even wipe out the complete system including backups. To mitigate the forensic challenges associated with insider threats, the researchers propose a "Log-of-logs" framework.

Surveys highlight the failure of enterprises in detecting insider threats within a feasible time period. A methodical forensic investigation becomes crucial and decisive for the prosecution of the personnel involved in cybercrime incidents. Forensic readiness is a fundamental necessity as insiders own detailed information about the IT infrastructure of the organization. There is a lack of comprehensive guidance in available literature for digital forensic readiness. OS-level log forensic methods are highly relevant in the case of superuser insider threats and their forensics. The malicious intent of superusers changes the administrative privileges into anti-forensic capabilities to hide the footprint of their illicit activities. Insider threats are not the focus of these contributions.

The typical user is often the weak point in the system. Attackers steal money, information and more by impersonating trusted parties. Whether phishing takes place on the clearnet or the darknet, users have to stay alert to prevent attacks. An advantage for attackers is that they can operate anonymously. The darknet is not a domain where only illegal activities happen. Establishing a phishing clone could be of interest for everyone fearing disclosure of information. A clever clone could send everything fished to the actual onion service and only filter out information unwanted by the phishing party.

8.3. Cyber attacks

Generally speaking, current attribution of cyber attacks is a manual process that is subject to the knowledge of the analyst reviewing the evidence. Attribution is, therefore, subject to bias and human error. The increasing prevalence of IoT devices means that the attack surface is much greater and more diverse presenting greater vulnerability and a more time intensive attribution process.

Karafili et al. (2020) proposed a proof of concept method for analysing the collected during a cyber attack to identify who performed the attack using both technical and social evidence [195]. As digital forensics works only with technical evidence, incomplete information leads to difficulties in reaching conclusions in cyber attack investigations. The argumentation-based reasoner can deal with incomplete and conflicting information and can also point the investigation to future investigative activities. The process, based on argumentation and abductive reasoning, comprises two main components – reasoning rules and background knowledge. Reasoning rules are extracted from public reports about past cyber-attacks and are divided into three layers: technical, operational and strategic. The combination of information in the layers aims to emulate the investigator's attribution process.

An argumentation theory is a pair (T,P) of argument rules T and preference rules P. The relationship between the preference rules is one of priority which are true at all times or under certain conditions or contexts. It allows for the introduction of new evidence which might change the result of the rule. For example, while attribution of responsibility might point to a certain entity, that entity might lack the capability to perform the action of which it is alleged.

The technical layer compromises rules that deal with evidence obtained from digital evidence processes related to the technical evidence of the attack, for example, exploiting a zero-day attack and the resources that are required to action such an attack. The operational layer comprises rules that deal with non-technical evidence related to the social aspects of the attack, for example the motives for an attack, the capabilities required to perform the attack, the political and economic context of the attack. The strategic layer comprises rules that deal with who performed the attack, for example, who will gain an advantage from the attack.

The argumentation based reasoner extracted 200 reasoning rules from publicly reported cyber attacks which have been translated into generic argumentation rules. For example, rules might address the questions of:

- Entity X is/is not the culprit taking into account motive and capability.

The model uses background knowledge comprising non-case-specific information including general knowledge and domain-specific knowledge. Background knowledge reduces analysts' work and mitigates human errors and bias. The usefulness of background knowledge is dependent on the accuracy of that same knowledge.

General knowledge makes use of language about countries' characteristics, international relations between countries and types of industries. Characteristics include language indicators such as system language settings and a country's first language; cyber capability based on the Global Cybersecurity Index Group (leading, maturing and initiating) and the cyber capabilities of countries in cyberwar(for example, cyber superpower).

Domain specific knowledge comprises information about prominent groups of attacks and past attacks, information that is used in the strategic and technical layers. For example, similarity to a past attack, such as a repeated use of specific malware, that is not available on the black market, is indicative of a previously seen attacker. The argumentation based reviewer was evaluated against three known attacks: 1) Stuxnet; 2) Sony Pictures; and 3) Conficker.

The authors acknowledge that, as the attribution is mainly human dependent, it is susceptible to bias, although mitigation of bias is an important part of the model.

8.4. Hacking

Law enforcement agencies are increasingly accessing data stored on remote computers in order to access their contents. The most spectacular so far have been the outcomes of a joint French/Dutch breach of the EncroChat secure smartphone messaging service between April and June 2020. Up to 60,000 handsets may have been "compromised" in this way. It is these contents that law enforcement agencies have sought to introduce into courts as evidence. And how should they treat it in the same way as other forms of non-testimonial evidence? [196].

In most "advanced" jurisdictions there is provision for a warranting scheme granting permission to hack. There are procedures under which disclosure of "sensitive" material may be withheld on public interest/national security grounds. This, for comparison purposes, is how things work in England and Wales (Scotland and Northern Ireland are separate jurisdictions). Intercept powers were not publicly acknowledged until the Interception of Communications Act 1985 (IoCA) but were available against a Home Office Warrant. IoCA set out publicly the need for such a warrant but also included the following: In any proceedings before any court or tribunal no evidence shall be adduced and no question in cross-examination shall be asked which (in either case) tends to suggest an offence under section 1 above has been committed.

The main UK Act covering Computer Misuse dates from 1990. Part 5 of the Act refers to "Equipment Interference". There are separate arrangements for the intelligence and security agencies. Warrants are issued by a "law enforcement chief" but is subject to approval by a judicial commissioner. In Norway, any potential evidence can be introduced unless there is a specific reason to disallow it.

In most countries disclosure/discovery is subject to a relevancy test. In the UK, following a number of justice miscarriages, the Criminal Procedure and Investigations Act 1996 imposes an obligation on a prosecutor to make the disclosure. There is however also the ability to withhold disclosure on "public interest" grounds, typically to protect sensitive sources and methods.

How does the legal framework of authorization and disclosure, in conjunction with the general expectations of forensic procedures, affect the practicability of submitting the product of equipment interference/authorized hacking as evidence? There are several issues that need to be addressed including, but not limited to:

- How do you operate covertly so as to avoid alerting your target of interest?
- Do you need a back door/remote access tool/Trojan/implant - they are all different names for the same thing.
- How extensive will your access be? The larger the volume of exfiltrated traffic and the longer the period before being detected.
- Extracting from a live environment will require removing the disk from a computer and placing it within read-only hardware. For a mobile or smartphone where the device must be powered up it is placed within a Faraday cage so that regular telecommunications traffic, wifi and Bluetooth cannot reach it.
- Is the infiltrated harvest now tendered as evidence sufficiently reliable for a court to have trust in it and depend on it? In criminal cases the standard for acceptance is "beyond a reasonable doubt" or "are you sure?". This is far beyond the civil test of "on the balance of probabilities".
- The audit trail must cover General Policies, Decisions with Reasons, Actions carried out and Mitigating Steps taken to address issues such as contamination during acquisition and the possibility that acquisition is incomplete.
- Are you prepared to identify your tools? The defence might ask reasonable questions such as:
  o Do the tools function as purported by the vendor?
  o Are they exhaustive in terms of the extracted material?
  o Have they undergone independent testing and verification?
  o How is the target protected from contamination?
  o How is the product protected against contamination?
  o Are the tools to be made accessible for testing as either operational facilities or as source code?
- Will any specialist techniques be revealed? Whatever is done will borrow the techniques of back door hacking tools, in other words a combination of social engineering and technology. It would help if this inducement had some novel or unusual feature such that a reasonably aware computer user is misled.
- The acquired exfiltrated material has to be sent and then stored to a safe location.
- It is important that any activity can be traced back to the raw material that is being exfiltered – reinforcing the need for a comprehensive audit trail.
- Proper authorising/warranting of intrusions is essential to success in the court room.
- There can be particular problems if the intrusion is initiated in one country but the target is in another. Some courts may be satisfied if they are convinced that the original authorization was legal in the country from which the intrusion was mounted. Other courts may want a great deal more.

In a high number of cases involving the remote extraction of evidence from EncroChat-encrypted mobile phones, hacked data is used as evidence across Europe. These phones were commonly used by drug traffickers, gun dealers, and money launderers. It is extremely difficult to produce hacked evidence that satisfies the majority of the requirements for trustworthy forensic evidence. However, effective prosecutions can be achieved by employing intelligence to locate traditional testable evidence. Numerous provisions allowing prosecutors and law enforcement investigators to withhold disclosure/discovery are ambiguous. Much appears to be left to the discretion of a judge, with the criterion being "in the interests of justice." It would be a simple matter of writing to rectify this in law or court procedural guidelines.

8.5. Phishing

The most simple and common way to impersonate another website is to clone and alter the content. Altering the page can usually be done automatically by replacing certain patterns like URLs and cryptocurrency addresses. The goal is identify phishing copies of hidden services by analyzing the data provided by them. The authors present algorithms and metrics to automatically detect phishing pages. Hash algorithms specifically designed for images can produce the same hash for images that are very similar to each other [197].

A simple solution to mitigate the detection of phishing sites by a tool that analyses images with cryptographic hash values is to subtly manipulate the image. A comparison metric based on image hashing for web sites is based on the percentage of identified images on both websites. It is not possible to freely choose an address nor to imitate an existing one, because the private key is only known by the legitimate owner. But one can generate key pairs until a domain with the desired properties emerges. The longer the string of common characters in the address, the higher the probability of it being deliberately similar.

The study crawled over 15,000 web pages for over 4000 individual onion services. Each of these pages is compared to all the others with a reasonable threshold. As expected, not many services can be detected by simply searching for perfect clones. However, there is no falsely detected duplicates.

Next, the service names were analysed alone. This is a really simple method that does not need any other data than the names of services. Based on how much of the addresses matched, the similarity value is calculated. A good threshold would be 0.35, which means all addresses where the first 6 characters are equal are seen as clones. Lower thresholds produce too many false positives because the chance that two addresses begin with the same string randomly grows.

With the sha image detection algorithm to identify images and a threshold of 0.1, 191 groups of cloned pages out of 4210 services were found. The most pages are cloned only a few times, with 107 services only having one clone and the other 73 pages having between 2 and 9 clones. Of those, only 11 pages are in groups with over 10 clones.

8.5.1. Online frauds and the role of forensic science

The Lausanne University School of Criminal Justice (SCJ) Director was on vacation on August 6, 2019. Rainy. A great day for hotel paper prep. The computer mailbox received spam and organization-related mail (several dozen). One email stood out when immediately scanning them. A new School employee Y sent an email. The first symptom of trouble. However, nothing happened. Just surprised [198].

The Director afterwards received an email from a colleague stating his availability but wondering if his identity was stolen. "Hello, did you get hacked into your Gmail account?" asked the second author of this study on WhatsApp. He also received "Hello are you available?" from the wrong address. Another colleague called the boss to report a weird "Are you available?" message.

The Director immediately replied to message #2 to warn him that the school was likely under a fraud attack and to stop communicating with the email sender.

These signs revealed a deception. The fraudster(s) pretended to be the Director to entice personnel. Beyond the fraud, the Director found it emotionally challenging to contemplate someone impersonating him and demanding a service from School members. He resolved to act immediately.

The Director's knowledge in computer science, crime investigation, and digital forensic science with police practice clearly drove their thinking and response. There is no "profession" that could handle this case in real time and support its interpretation. The fraud was discovered after 40% of the School's members got "Hello are you available?" The IT department's filtering system and anti-spam efforts failed to detect fraud. If the fraud's exact method had been recognized earlier, the time would have been shorter.

The volume of urgent and non-urgent messages received by university IT departments is overwhelming. Incident response and monitoring university frauds are being professionalized. However, their technique simply uses common-sense criminology, intelligence, and forensic science. Is it newsworthy? There is no knowledge to triage internet fraud operations between tiny individual offenses and large-scale, organized serial crimes that should be prosecuted.

Digital traces were extensively used for analysis and investigation. It will take time to structure the treatment of typical high-volume offenses or apply new cybersecurity incident-response methods. This area's institutions, professions, and tactics are unprepared for such ubiquitous crimes. This example supports public-private collaboration. To create an organized and resilient forensic ecosystem for the new circumstances, forensic science and digital forensics should be better integrated.

Concepts must be worked out to avoid re-inventing forensic science information. Such a view also enables for the merging of physical and digital traces to extract information about the many crimes altered by digitalization. Internet fraud relies on social engineering, making it easy to detect. Until regulations and cross-border evidence sharing are harmonized, prosecution is still too difficult, slow, or impossible in such cases. Prosecuting worldwide crimes is challenging, therefore find alternatives.

Online fraud is not policed comprehensively, from data collecting to intelligence production. To integrate digital traces and their interpretation into the process, a new, well-balanced, interdisciplinary proactive vision is needed. The conventional view of organizational settings and professions as rigid silos should be abandoned.

The Director's expertise in computer science, crime analysis, and digital forensic science with police practice definitely influenced their comprehension and response to the problem. There is no profession that effectively prepares individuals for the management of this case in real-time and for defending its overall interpretation. About forty percent of the School's members had already received the message "Hello, are you available?" before the fraud was discovered. The IT department's filtering system did not detect the scam, and anti-spam procedures were inadequate. A shorter amount of time would have transpired if the fraud's particular method of operation had been revealed sooner.

The volume of notifications with varied degrees of urgency received by university IT departments is overwhelming. They are professionalizing their approach to cybersecurity as a whole, including incident response and the monitoring of frauds that target and reach colleges. Concerns exist, however, because their approach is based solely on commonsense understanding of criminology, intelligence, and forensic science. Was it worthwhile to report? There is a dearth of knowledge to support the classification of online fraud operations as small individual offenses or large-scale, organized serial offenses that warrant punishment.

Digital traces were heavily used throughout the analysis or from a more investigative standpoint. There is a significant distance between the present and typical structured treatment of high-volume crimes and the application of new incident-response approaches in cybersecurity. Institutions, professions, and approaches in this field are not prepared to combat such ubiquitous crimes. This case substantiates the need for more coordination and collaboration between private and public institutions. Forensic science and digital forensics should be better linked in order to create an organized and resilient forensic ecosystem capable of addressing the new scenario.

In order to avoid reinventing knowledge that has been developed over years in forensic science, concepts must be developed. Such a view also permits the combination of physical and digital traces in order to extract the information they reveal about the numerous types of crimes that digitalization has revolutionized. Internet fraud is not regarded difficult from a technological or forensic perspective, as it relies mainly on social engineering. In any event, prosecution is still too tough, too slow, or impossible in such circumstances, and much more cannot be done until legislation and cross-border exchange of evidence are harmonized. The difficulty of pursuing globalized crimes need to motivate the search for alternate remedies.

There is no holistic approach to police online fraud, from the collecting of data through the generation of intelligence that would indicate the most effective remedies. It is required to establish a new, well-balanced, proactive, inter-disciplinary perspective that places digital traces and their interpretation at the centre of the process. Current organizational settings and professions should not be viewed as inflexible silos, as is commonly believed.

8.6. Cybersecurity datasets

Currently, the data sets used by the ransomware testing community are beset by a variety of obstacles. Numerous researchers manually build their own data sets, which are frequently not made public until after the research has been concluded. There are insufficient standardised data sets that are suitable for research. If a current, diverse, and representative mixed file data set could be compiled and made accessible to the public, it would improve the quality and rate of research in domains such as ransomware investigation and digital forensics [199].

For malware research, there is a paucity of publicly available mixed file data sets. This is a significant challenge for ransomware researchers. Developing a high-quality, publicly accessible data source could be quite beneficial. Two-thirds or more of the data sets used by researchers are generated experimentally, while only one-third is comprised of real-world data. Fewer than 4% of researchers disclose their data set, although over 50% use existing data sets.

Currently, the data sets used by the ransomware testing community face a number of challenges. Numerous researchers manually create their own data sets, which are frequently not made public until the research is complete. There is a lack of research-appropriate standardised data sets. If a current, diversified, and representative mixed file data set could be established and made available to the public, it would enhance the quality and pace of research in fields such as ransomware investigation and digital forensics.

The NapierOne data set contains nearly 500,000 unique files distributed between 100 separate data sets and subsets. To provide consistency across the entire data set, a standardised naming convention was used. The data set is a collection of multiple data subsets each associated with one specific file type or a specific configuration of a file type. Various techniques were employed to gather file examples from websites covered by the gov.uk domain. Some image data subsets have multiple examples of a particular file type, for example, JPG and WEBP, with differing encoding qualities and compression levels. Data subsets of ransomware encrypted files have been created for the following ransomware strains: NotPetya; Sodinokibi; Maze; Phobos; Netwalker; Dharma; and Ryuk.

While both the NapierOne and Govdocs1 datasets contain roughly 40 file types, the majority of files in the Govdocs1 collection only represent a few of these file types. The NapierOne data set is free and unrestricted for research purposes. Certain portions of data are extraordinarily large, with the overall uncompressed size of the complete data set surpassing 2 TB.

There are more instances of contemporary file formats like DOCS, PPTX, and XLSX than there are in the Govdocs1 collection. The Total archive contains every instance of the specified file type inside the dataset. Additionally, the separate archives have been merged into three bigger archives. Using this structured methodology, researchers will be able to tailor what and how much they download to their own needs.

8.7. Superuser insider threats

To illustrate superuser insider threats, the authors choose four cases to underline the nature of the threats associated with administrative privileges of superusers. These four cases strongly demonstrate the forensic repercussions of exclusive control over the system by a single entity. There are three types of insiders based on the levels of access they have: physical access, login account, and administrative access. The four cases provide generic examples of insider incidents involving superusers who own highest privileges. Most of the insider threats may not result in forensic prosecutions due to lack of evidential artifacts.

The authors introduce a forensic framework for superuser threats and document a listing of potential evidential artifacts available in the local and Log-of-logs server with regard to four superuser threat cases. They then present security analysis of the framework, evaluate and discuss the forensic framework through event reconstruction of four insider threat cases. The concept of distributed key cryptography (DKG) may be useful with respect to evidential artifacts in the form of log files/binaries.

In any scenario, it should not be considered as a ready-to-use secure solution. The proposed framework can be implemented or integrated with any of such enterprise-level tools including Elastic Stack, Splunk, Tripwire, etc. In Case I, the events of the case were recreated where financial records were deleted and modified from the database. In Case II, the network traffic was captured through tcpdump7 in the admin server and the download event of a logic bomb was identified. The framework monitors the log files and whenever the files are modified, the information is transmitted immediately.

In Case III, the superuser used his administrative privileges to disallow the organization access to its own infrastructure with login disabling and password deletion. Case IV is an absolute example of malicious usage of administrative rights in which user disabled the logging capabilities of the system. The framework allowed continuous monitoring of the logging services in admin server through the authors' Log-of-logs server. Access to the local admin server opens up several possibilities for superusers to do irreversible damage to systems and services. The superuser with malicious intent can boot the local server with external disk such as USBs and work on file systems.

A malicious superuser insider can even disable the network or may simply unplug the network from the system. In all such cases, the Log-of-logs sever will have all the artifacts stored and hash-chained securely [200].

8.8. Cybercrime in Czech Republic

Attacks on the confidentiality, integrity and accessibility of computerised data are considered typical forms of cybercrime. The Czech Criminal Code covers these attacks in the provisions of x 230 and x 231. Some crimes against data confidentiality, such as unauthorized data capture, are covered under x 182 and 183. The provisions of x 230 of the Criminal Code are somewhat complex, containing several matters. For the sake of simplicity, criminal acts can be divided as follows:. 1) Obtaining unauthorized access to computer system or part thereof by overcoming security measures (x 230 para. 1). 2) Unauthorized use of data stored in the computer system and subsequent unauthorized manipulation of that data (para. 2) [201].

Punishment is more severe if the offender gains unentitled advantage for themselves or others. Extensive damage or advantage amounting to the equivalent of 5 million CZK (V19,677) or more. Damage to or misuse of records on a data carrier was defined in the Criminal Code of 1992.2005 saw the greatest number of people prosecuted, charged and convicted for this crime (33). The largest number of convictions was made in 2002 (a total of 8 people).

Attacks on data and computer systems in the Czech Republic are not substantially different from those carried out abroad. Ascertaining who the offenders are and proving their guilt in these cases can be more difficult than in common criminal cases. The attacks are carried out on banks, news servers, national authorities and telecommunications servers. Between 2008 and 2016 the proportion of Czechs aged over 16 years who use the internet grew from 50 to 75% (CSÚ, 2017). The percentage of the population using mobile internet connections grew sharply to 50% in 2016. This analysis compares the crimes that the authorities would like to see prosecuted with those that are actually brought to court.

Of 229 cybercrime cases analysed in the Czech Republic, 79% of those cases the case was concluded with a guilty verdict. Acquittal was slightly more common (by two percentage points) in these particular cases than on average across all court judgements. The courts' judgements in cases of crimes classified under x 230 of the Criminal Code were not substantially different from their judgements of other crimes.

8.8.1. Categorizing attacks against data and computer systems in the Czech Republic

The most frequent type of attack is the misuse of passwords, which can be divided into cases in which the passwords were misused with the aim of gaining access to private data and those where the aim was to access internet banking. Other categories include hacking, database misuse, data found on USB flash drives and data deletion. The last category dealt with in Czech courts is manual manipulation of gambling machines and roulette wheels.

Perpetrators most frequently gained unauthorized access to others' data by misusing access passwords. The cases can be further divided into several groups based on the goal of the perpetrators. Most common were obtaining erotic materials, uncovering information about a previous or current partner, or simply reading messages. The offenders often made the photos and videos they had obtained public, forwarded them to others, or threatened to do so. Ex-partners' e-mail addresses and other social media accounts can be used by offenders to obtain information about their former partners. One offender installed software on his ex-girlfriend's phone that enabled him to listen into her conversations, read her messages and listen in to sounds near the mobile phone, as well as secretly tracking the phone's location. Some offenders gained access to internet banking accounts belonging to close relatives. Others found passwords written on scraps of paper at home and saved on the computer. These offenders then asked friends to send them unique codes for mobile payments. One offender observed his ex-girlfriend's password for the study system and then changed her account number in the system to his own. Courts have different approaches to the criminalization of password-related cybercrime, with some saying that such acts should be treated as administrative (not criminal) offenses, while others follow the law to the letter. The main measure of social damage should be how they use and misuse the information they have obtained or restrict others from using it. While current law is in line with the Council of Europe Convention on Cybercrime, a differently defined set of rules need to govern the extent of criminalization of password misuses. The means by which offenders gained access to others' account passwords were varied. In some cases the courts considered unlocking a smartphone with a gesture as an act of overcoming security measures. In other cases offenders used a false login page for Lide.cz, installing KeySpy software or other tracking devices, or setting up email filters while living with the account holder.

Under section 230 of the Czech Criminal Code, parties who abuse their position in order to gain access to computer systems were also criminally prosecuted. The acts can be divided into two groups, based on whether the offender misused a position in the private or public sphere. In the private sphere, the vast majority of cases involving this type of act were motivated by the hope of making a financial gain. Apart from bank employees, accountants and IT specialists, different courts in the Czech Republic have dealt with cases where police officers and policewomen abused their access to non-public databases and passed on personal information about others. In some cases the motive was to find out who owned a certain vehicle, while in others it was just to check its history. The district courts in Ostrava and Karlovy Vary convicted both policemen of passing on information about vehicles' owners, but absolved them of criminal charges. The biggest case was probably that of an IT department manager who hacked a password in order to gain access to the central server, from which he copied 54,000 publicly available files. Not even employees of the Prison Service avoided misusing their position: one was convicted for leaking a photograph of a member of parliament to a tabloid newspaper. Another passed information about prisoners to a third party but in the knowledge that party would not use it.

The record holder for hacking was a man who was found guilty on 174 charges relating to hacking into IT systems.

Cases of database misuse formed a specific group of cases; these largely involved client databases. Typical cases involved offenders copying non-public databases of customers and selling them for 125,000 CZK to other businesses. One offender downloaded information about 1572 bank clients, which he passed on to another person who used them as a financial advisor.

In one case an offender obtained log in details for internet shops from a found flash drive and then used them to order goods from the aggrieved party's accounts. Another offender used security codes found on a flash drive to gain access to internet banking and arrange a loan. One offender even offered a reward for returning a lost flash drive, and compelled the owner to pay by leaking its contents to other members of the same organization.

In one case an offender used a sewing pin to restrain the switch for the alarm signalling that the front panel of a machine has been opened. Another offender hacked into a video lottery machine by altering a metal tool in the shape of a hockey stick to prevent the service hatch from being opened. In one case a service technician deliberately increased the amount of credit on a video lottery machine, and caused it to pay him 12,000 CZK as winnings, causing a loss to the operator. Six weeks later he did this again in the same location, and made 6000 CZk. The criminal proceedings were terminated according to para. 2 letter a) of the Criminal Code, that is, there was insufficient evidence that the act had taken place.

In the Czech Republic, only "simple" cases of attacks against data and computer systems are prosecuted. Legal action is primarily not taken against more complex cases of hacking and internet fraud. Old forms of cybercrime (such as libel, leaking correspondence and destroying paper data records) are taking on new faces (old wine in a new bottle, one might say). The Czech Criminal Code makes misusing passwords a criminal offence (x 230 para. 1 of the Criminal Code), but does not make misusing the information gained through password misuse a requirement for criminality. One possible solution could be that the Czech Republic accept to adopt stricter conditions under which simple password misuse could be criminally prosecuted, similar to those set out in the Council of Europe's Convention on Cybercrime of 2001. The Police of the Czech Republic are aware of the difficulty of uncovering this type of criminal activity. As part of the reorganization of the police force in 2016 a country-wide department was created, one of whose four sections is the Section for Cybercrime. During 2016 the police received 3378 reports via that web form.

1. Jurisprudence

1.1. Jurisdiction specific issues

This section includes a small sample of digital evidence issues that are occupying the attention of political and justice systems in some jurisdictions.

1.1.1. Bosnia and Herzegovina

In Bosnia and Herzegovina (B&H), police agencies handle digital evidence differently depending on the role of holders of judicial functions, particularly prosecutors. Consequently, the objectives of this article are to define their methodologies and investigate the relationship between established patterns and the prosecutor's position from the perspective of professionals (experts) from the relevant agencies. Indirect data collection methods included content analysis, questionnaires, and semi-structured interviews with specialists from police agencies. In the analysis of the acquired data, every fundamental technique was employed. In analysing the legal framework, the dogmatic-legal technique was used. The replies of the questioned specialists represent their own opinions and experiences regarding the handling of digital evidence; hence, no generalisations can be made about the field as a whole. In addition, it was not possible to check objectively all the conditions and specifics of how the digital evidence provided by the respondents was handled. On the basis of the collected data, the authors discovered patterns in the treatment of digital evidence, as well as their key deficiencies, which may result in the evidence's illegality. This article makes a minor addition to the scientific and expert discourse on the eradication of shortcomings and the harmonisation of the investigated field. The paper's general conclusion is that the inconsistent practises of domestic police agencies in dealing with digital evidence must be eliminated by amending existing legal provisions and enacting by-laws that clearly establish rules and procedures while taking into account the unique nature of this evidence and the existing concerns and issues regarding their legality [202].

1.1.2. Ghana

Cybercrime has affected all sectors of the economy of scale, resulting in monetary losses and reputational damage. The current Inspector-General of Police in Ghana, Mr. David Asante-Apeatu has expressed concern that the emergence of ICT-facilitated crimes had become one of the many challenges confronting the adjudication of criminal offences [203].

Recognizing that cybercrime is a growing concern to the country, the government of Ghana, through the Ministry of Communications, has enacted legislation to regulate the behaviour of individuals in cyberspace.

The Parliament of Ghana in December 2008, passed the Electronic Transaction Bill into law. The Act empowers security agencies to seize a computer, electronic record, programme, information document or thing if they reasonably believe that an offence has been or is about to be committed. The ETA is not adequate and does not address fully all aspects of cyber security challenges. The National Cyber Security Advisor notes that certain gaps in the law ought to be plugged.

The National Information Technology Agency (NITA) is a Ghanaian public institution established by Act 771 in 2008. Its mandate is to regulate and monitor the activities of companies in the electronic industry of ensuring quality information delivery and standard of efficiency.

The Data Protection Act 2012 (Act 843) was passed by parliament in 2012, to protect privacy of individual and personal data. The intended purposes of the DPC are yet to be fulfilled because data are still collating from the various institutions that controlled individual's information online.

The growing Internet penetration in Ghana had opened up the country into new online trading platforms, which had empowered the average Ghanaian to transact various business operations. Some Sections of the Criminal Offences Act (29/30) are recaptured in the Electronic Transactions Act (Act 772) to prefer charges against cybercrime suspects.

Article 200 of the 1992 Constitution of the Republic of Ghana and the Police Service Act of 1970 (ACT 350) mandate the Ghana Police Service to prevent and detect crime. As cybercrime actions become more frequent, the Ghana Police Service must increasingly consider what 'prevent' and 'apprehend' imply in the context of transnational crime. Police personnel and prosecutors in Ghana have divergent opinions regarding the existence of a legal definition of cybercrime. The majority of personnel stated that there is no law in Ghana that defines cybercrime, identifies its charges, and specifies sanctions that are proportional to the crime. On the other side, the head of the Legal and Prosecution Unit claimed that "crime is crime" in opposition to this statement.

Criminologists from Ghana have suggested that the age distribution of crime is independent of a vast array of other societal factors. People who typically become victims of cybercrime in Ghana are divorcees and middle-aged women between the ages of 36 and 45 who are susceptible to romance scams. Traditional techniques of law enforcement have been unsuccessful in the face of mounting evidence that fraudsters use electronic gadgets. The Ghana Police Service's Ghana Police College offered courses aimed to update the senior corps, but cybercrime was not included in their curriculum.

The law is a potent instrument that allows the state to address new societal and security concerns, such as cybercrime. A meeting with members of the Ghana Police Service indicated that there are insufficient legal grounds for prosecuting cybercriminals when they are arrested and brought before the court. This allegation was refuted by the Director in Charge of Legal and Prosecution, who emphasised that Act 772 outlined the different internet-related offences. There is concern that cybercriminals are abusing the internet to the harm of the public and that, if allowed to continue, cybercrimes will undermine public confidence in online commercial operations such as trading, e-banking, and other services.

The Act 772 regulates transactions that occur in the electronic environment, and sections 107 to 137 of the Act outline the offences. The only portion exploited by the Police is Section 102 (2), which specifies that "a provider of an electronic communication service shall submit to a law enforcement agency any record or other information relating to a subscriber or client."

Due to the expanding use and use of communication technologies, electronic evidence is becoming increasingly important to the investigation and prosecution of cybercrime, as well as crime in general. Due to the absence of a computer forensics laboratory, it is challenging for investigators to obtain digital evidence. Therefore, if certain judges lack a fundamental understanding of cybercrimes, it hinders the police's resolve to apprehend the culprits.

Every country has jurisdiction over people within its territory. Conversely, no State can exercise authority over persons outside its boundaries unless international treaties. In the context of the internet, cyberspace has no geographical boundaries. As internet does not tend to make geographical locations clear, the cyber citizens remain in physical jurisdictions and are subject to those laws. Ghana is yet to subscribe to any cybercrime convention that can facilitate extradition.

The opportunity for the investigators is to explore the conventional treaties like INTERPOL to reach out the party concern. Specific cyber laws are requried, like the UK Computer Misuse Act which outline the various offences under clear subheadings to deal with the issue.

1. To enable national law enforcement agencies to effectively prosecute cybercriminals, the government should implement progressive capacity building programmes for officers to acquire new ICT skills and efficient methods of enforcing cyber laws.
2. To address the dynamics of cyber security risks, the government, in partnership with the Attorney General's office, should establish a periodic process of evaluating and upgrading Ghana's cyberspace legislation.
3. Government of Ghana should adhere to international cybercrime agreements and protocols to expedite the rendition and extradition

of cybercriminals between member states in order to reduce the occurrence of internet fraud.

1.1.3. India

The data 'revolution' raises novel questions from the points of view of personal privacy, due process, and civil liberties. In India, significant discussion has taken place around a legal framework for privacy and data protection in India but there is scope for deeper examination of law enforcement agency (LEA) powers under Indian criminal procedure law. There are concerns relating to the inadequacy of the procedural framework governing LEA access to data [204].

In most cases, there are no carve-outs for access to evidence stored in digital form. This paper focuses on key provisions contained within the general criminal procedural framework. Other frameworks may also provide mechanisms for LEA to access data but these provisions are not as commonly resorted to. Section 91 of the Code of Criminal Procedure, 1973 provides for the seizure and detention of letters and telegrams in transit. It also authorises LEA to compel production of such objects without judicial authorisation or adversarial process.

However, this has no affect on sections 123 and 124 of the Indian Evidence Act and Bankers' Books Evidence Act, 1891 (13 of 1891). Section 91(1) of the Criminal Procedure (CrPC) Act provides that a court may issue a summons or written order seeking production of any 'document' or 'thing' that is necessary or desirable for any investigative purpose. Expressly excluded from the scope of this provision are letters, postcards, telegrams, and 'other things' in the custody of a postal or telegraph authority.

Section 91 of the Cr.PC is commonly understood to be used by LEA to seek the production of data and other forms of electronic evidence in the possession of intermediaries and other persons. Several authors have noted and commented on this practice, while others have expressed concerns about its unilateral application. LEA tend to ignore the heightened standards of Section 92 (which the authors suggest is more appropriate) and prefer to use generic Section 91 powers which do not require judicial authorisation. Only basic subscriber information or meta-data is typically provided by intermediaries in response to Section 91 requests. Section 91 of the Cr.PC is widely used for production orders and to order other positive acts such as takedown of content. There has, till date, not been a detailed legal survey surrounding this provision.

The powers and discretion available under Section 91 are extremely wide and only subject to the restriction found in the text of the provision. Without reform, exercise of powers by LEA under this provision may be subject to increasing levels of judicial scrutiny and be set aside on privacy grounds. A verbal order or instruction issued to any person to produce a document or thing would not suffice. An order issued under Section 91 which is not in writing is likely to be liable to be set aside solely on this ground. In the context of digital evidence sought to be produced, where concerns regarding grounds of proportionality arise, the written order ensures there is a decision which may be challenged before higher courts.

1.1.4. Principles specifically relevant to the production of data

Section 91 orders need not only be directed to individuals who have in their personal possession, documents or things. Courts have interpreted the powers under this provision to extend to produce documents and things which are in the control of an individual who is holding the same on behalf of the target individual. In Surendra Mohan v K.P.M. Tripathi, the Allahabad High Court refused to interfere with a Section 91 order issued by a police officer. However, it remains an open question of how a court would consider arguments relating to impossibility (rather than inconvenience) to produce data. An order directing a bank to prevent an accused from operating his account was not something that could be authorized under any provision of the 1898 Code.

No such order could have been issued under Section 94 - the equivalent to Section 91 of the 1973 Code, the Patna High Court noted. Section 91 cannot be used to compel acts other than the mere production of documents or things. Magistrates and police officers' powers are circumscribed by Cr.PC and they must act within its four corners. LEA's interpretation would appear to be prima facie incorrect. The Cr.PC was enacted in 1973 and originally intended to restrict compelled production powers to documents.

Recently, Indian courts have been open to interpreting the term 'documents' broadly. This trend likely upsets the balance of (LEA and private) interests deemed appropriate by framers. Section 91 powers cannot be used for 'roving' or 'fishing' expeditions. In practice, this means that the particular document or thing to be produced as well as the person in whose possession the same lies must be clearly specified in an order issued under Section 91. Section 91 contains no carveouts for any specific types of sensitive documents or things (such as a diary) which might suggest that privacy was not a key consideration at the time of drafting this provision.

In K. Sureshkumar v. C. Sandhumani, Madras High Court upheld the order of a lower court declining to order Vodafone to produce "all call lists and SMS messages" emanating from an individual's mobile number. In State of Orissa v Debendra Debendra Nath Padhi, the Supreme Court has held that provision of Section 91 Cr.P.C., cannot be used for a roving enquiry. Such call details and SMS details will invade into the privacy of an individual, guaranteed by Article z1 of the Constitution of India. India's High Court has upheld the decision of a lower court not to preserve the call data record and location chart of Investigating Officer on the ground of fishing inquiry and intrusion in the privacy of I.O. These decisions, while being the exception rather than the norm, are notable for the fact they were issued prior to the decision by the Supreme Court in Puttaswamy which affirmed the right to privacy.

1.1.4.1. The future.

A key development which will likely affect the exercise of powers under Section 91 going forward is the decision of the Supreme Court in the landmark Puttaswamy case. In the majority judgment, a law which encroaches upon privacy will have to withstand the touchstone of permissible restrictions on fundamental rights. Orders under provisions such as Section 91 - when addressed to intermediaries - must satisfy the same standards as in cases where they are issued directly to the target individual. In the post-Puttaswamy era, a lower standard will not likely apply in relation to information entrusted by individuals to third parties such as banks, intermediaries or other organisations. It remains to be seen whether a written order issued by a police officer - without any form of judicial authorisation would withstand the test of being "fair, just and reasonable" in cases where personal privacy is at issue. For clear and efficient process in the long-term, which ensures respect for privacy, legislative review and reform of Section 91 is likely to be required.

The Clarifying Lawful Overseas Use of Data Act ('CLOUD Act') came into force in the United States in March 2o18. Under the Act, foreign governments can directly serve production requests on US-based entities - circumventing the MLAT mechanism. India's debate over Section 91 of the CLOUD Act is relevant only in that it relates to cross-border data requests under the Act. But there are other requirements of the Act which are not presently satisfied by Indian law. There may be ways to satisfy these requirements without substantive reforms to Section 91.

However, reform of Section 91 would likely be a necessary precondition for any such reform. The current mechanism of orders under Section 91 does not empower police or courts to issue data preservation requests. The lack of such powers may lead to loss of critical evidence from an investigative or prosecutorial viewpoint. It is presently unclear if a police officer may order production where data is stored outside his district, city, or state. This issue assumes relevance particularly in the context of cloud computing and remote services.

Section 91 does not lend itself to easy application to data stored electronically. It may be open for the target individual to argue that the production of data – as an intangible – is not recognised within the ambit of Section 91 at all. Significant questions are likely to arise regarding the appropriate substantive legal standards for compelled production of electronic data. The question is whether private intermediaries can fall within the ambit of being telegraph or postal authorities – as recognised under Sections 91(3) and 92. While a detailed analysis of this question is beyond the scope of this piece, it must be acknowledged that technological developments have been found to play an important role in the interpretational exercise.

A court may interpret a statute according to its current meaning and apply the language to cover developments in science and technology not known at the time of passing of the statute. With reference to specific developments in technology, the Supreme Court has recognised the progress of science by bringing in line the scope and meaning of existing statutes with current norms and usage. A path ahead exists for a court seeking to adopt an interpretation which reads 'postal and telegraph' authorities in a manner more appropriate to the modern context. In relation to Section 95 of the 1898 Code, the Law Commission rejected a recommendation that these powers also be granted to senior police officers. This decision arguably speaks to the acceptance of the notion that judicial officers - and not police - would be the more appropriate authority for the exercise of such powers.

1.1.5. *Indonesia*

The use and utilization of information technology must continue to be developed to maintain and strengthen national unity and integrity. Legal problems that are often faced are when it comes to the delivery of information, communication and/or transactions electronically. Information technology is currently a double-edged sword, because in addition to contributing to the improvement of welfare, progress and human civilization, it is also an effective means of acts against the law. Electronic evidence has its own uniqueness, which is different from other general evidence such as objects that can be seen with the naked eye and touched. Since the promulgation of Law No. 11 of 2008 (ITE Law), there is an expansion of the types of evidence at court, namely electronic information and/or electronic documents. This article will discuss what is the proof system adopted by the Criminal Procedure Code and how it relates to electronic evidence in criminal procedural law [205].

Evidence law is a part of criminal procedural law which regulates various types of evidence which are valid according to law. It includes the system adopted in evidence and the requirements and procedures for submitting evidence. The judge's authority to accept, reject and evaluate evidence is regulated by the system of proof. Indonesia's Criminal Procedure Code adheres to a system of proof according to law negatively. This means that in the case of evidence, whether the defendant has sufficient grounds that are supported by means of evidence determined by law (at least two pieces of evidence) and if he is sufficient, then it is questioned whether or not the judge's belief in the defendant's guilt.

Law No.19 of 2016 on amendments to Law No. 11 of 2008 (ITE Law) provides a legal basis regarding the legal strength of electronic evidence. Between electronic information and electronic documents, both can be distinguished but cannot be separated. The printout of Electronic Information or Documents is documentary evidence regulated in the Criminal Procedure Code. The ITE Law regulates that there are formal and material requirements that must be met so that Electronic Information and Documents can be used as legal evidence. To ensure the fulfillment of the material requirements referred to, in many cases a digital forensic process is needed. According to R. Atang Ranomiharjo, evidence is tools that are related to a criminal act.

The ITE Law regulates that there are formal and material requirements that must be met so that Electronic Information and Documents can be used as legal evidence. In the case of evidence, research must be carried out to determine whether the defendant has sufficient grounds that are supported by means of evidence determined by law.

1.1.6. *Lithuania*

Admissibility of evidence is one of the most important principles that law enforcement officers and prosecutors must bear in mind throughout the entire criminal proceedings. The assessment of evidence by the court depends on whether the requirements of the law have been complied with during the pre-trial investigation. Electronic evidence, like any other type of evidence in a criminal procedure, is subject to common requirements, as defined by the Code of Criminal Procedure (CCP). The law establishes the following requirements for evidence (including electronic evidence): it must be obtained in the manner prescribed by law; by lawful means, and can be verified by the proceedings laid down in the CCP. If data do not meet at least one of these criteria, the court may not consider them as evidence and may not rely on them while addressing the issue of guilt of the accused [206].

The Code of Criminal Procedure primarily governs the obtaining of electronic data. Data are usually obtained in the manner laid down by both the Law on Criminal Intelligence and other laws. Judges are required to carefully assess whether the evidence has been obtained by legal means. Electronic evidence is usually obtained by applying procedurally coercive measures, such as search and seizure.

CCP provides that a search can be carried out only by a reasoned decision of a pre-trial judge. Where there are grounds for believing that a criminal offence has taken place, the investigating officer or the prosecutor may enter any premises that may have significance to the criminal offence to search for tools, objects or documents. In cases of urgency, a pre-trial judge may also apply the procedural coercive measures. In all these cases, however, a ruling by that judge confirming the lawfulness of the application of the coercive measure must be received within three days of the adoption of the ruling. The filing of an appeal against a decision not to approve the lawful application of a coercive measure suspends the enforcement of this order.

In one appeal, a suspect claims that the court did not substantiate the validity of the search when sanctioning the search. There was a factual basis for the search, i.e. data of pre-trial investigation on the basis of which it was reasonable to assume that there were items relevant to the investigation in a particular location (cars or premises). Considering the circumstances existing at that time, there were grounds for believing that these items had to be seized immediately after the investigation was conducted.

In February of 2019 searches were carried out on nine suspects who organized multiple DDoS attacks against Lithuanian information systems. After the search, the court decided that failing to carry out a search promptly would have given rise to the risk of the loss of evidence, and retrospectively authorized the search. Since the search as a procedural coercive measure restricts a person's right to private life and inviolability of the dwelling, it can only be done by reasoned order of a pre-trial judge. It is possible to conduct a search without a pre-trial judge's order in urgent cases, i.e. when a delayed search may have negative effect on the course of investigation. A person is arrested or detained when there are sufficient grounds to believe that during the search this person is hiding objects or documents relevant to the investigation of a criminal offence.

There are many different aspects to be addressed when collecting electronic evidence, such as limitations related to a particular profession and legal professional privilege. In one case, the Supreme Court of Lithuania ruled that police access to telephone calls and electronic correspondence between a suspect and his lawyer were not in breach of the immunity of communication between a lawyer and his client as established by the Law on the Bar. The Court of Appeal rightly held that the CCP provision which prohibits interception of telephone conversations between the lawyer and the suspect or defendant, as well as control or recording of other information transmitted via telecommunication networks, was not yet in effect.

The conclusion that the communication was in a relationship between a lawyer and a client was made by the courts after they assessed the wording of 26 April 2002 agreement on legal aid. A preliminary agreement was concluded between the client and the lawyer in the smuggling case concerning the shipment of "Sovereign Classic" cigarettes which was seized on 5 July 2002. An agreement on legal aid between the lawyer and his client must provide for specific issues related to legal assistance or at least define the activity field in which the legal assistance will be provided. As a result, the findings of the courts that telephone conversations were made unlawfully P.

The law does not always keep up with rapidly evolving technologies, consequently the gathering of evidence faces challenges. A question arises whether it is legitimate to force a person to unlock the device, which is protected by biometric data. The position in Lithuania is covered by article 156 of the CCP: Taking photographs, filming, measuring, taking hand prints and sample genetic dactyloscopy. A suspect and a defendant may be photographed, filmed, measured, and their hand prints may be taken as part of an investigation. It is possible to obtain some personal biometric data and use them for the purpose of obtaining evidence during criminal proceedings.

At the time writing, there are no cases in Lithuania where it has attempted to do so. Lithuania's Supreme Court has ruled that pre-trial judges and other Lithuanian institutions are not entitled to apply coercive measures abroad, i.e. outside the limits of law of the Republic of Lithuania and the jurisdiction of law enforcement authorities. The Supreme Court of Lithuania has clarified that a pre-trial investigation judge has the right to make a ruling on the application of procedural coercive measures in foreign states.

Digital forensics examinations or specialist examinations are conducted in almost every case where the suspect's fault is based on electronic evidence. Pre-trial investigation institutions employ trained officers who can carry out simple examinations. IT specialists work in the major police units of all counties. Digital forensic examinations are performed by the Forensic Science Centre of Lithuania (FSCL). The main task of the IT Department is to carry out forensic examinations required by courts, pre-trial investigation institutions and other state agencies.

The most complex examinations are carried out by FSCL digital evidence professionals. In 2018, they participated in an inter-laboratory test on identification of passwords organized by the ENFSI working group FIT-WG (Forensic information technology working group).

1.1.7. Nepal

Cybercrime encompasses a spectrum of destructive acts and behaviours, usually grouped into four categories. According to a new UN assessment, cyber abuse is equally harmful to women as physical assault. Partners and ex-partners are responsible for ninety-five percent of aggressive conduct, harassment, abusive language, and degrading pictures in online places directed at women [207].

Cyberviolence is not a separate phenomenon from offline violence, as it frequently follows the same patterns. Cyber violence against women and girls (VAWG) comprises hate speech (the publication of a blasphemous libel), hacking (the interception of private communications), identity theft, online stalking (criminal harassment), and the utterance of threats. Internet-based commercial sex enables human traffickers to use the legal parts of commercial sex to conceal their illicit actions. The Internet is primarily used by human traffickers to advertise sex, seek victims on social media, exchange money, and organise many of the logistical activities involved in transporting victims. Hate speech is speech that criticises a person or group on the basis of particular characteristics, such as gender, race, religion, ethnicity, socioeconomic status, ideology, sexual orientation, and similar characteristics. The term "revenge porn" refers to the act of uploading intimate images or films of another person online with the intent of publicly embarrassing and humiliating them. This paper focuses on cyber VAWG in the context of Nepal and was prepared in consultation with the police personnel handling cybercrime cases and complaints in the Metropolitan Police Office and Metropolitan Crime Division of Kathmandu, the Central Bureau of Investigation, the Crime Investigation Department of the Nepal Police Headquarters, and the district government attorneys of the Kathmandu District Court.

During the first six months of the 2017/2018 fiscal year, as many as 560 occurrences of cybercrime were reported. Nepal Police describes cybercrime as harassment via social networking sites, email threats, unlawful data access, ATM breaches, server hacks, pornographic websites, copyright infringement, and phishing. In 45% of cyber crimes, women and girls were defamed by posting false information about their character, undermining their confidence to engage in any aspect of public life. 55% of the charges involved the sharing of obscene movies and images, as well as the texting of indecent messages with image alteration. Ninety percent of the cases filed against women and girls in the Kathmandu District Court were for publishing indecent videos, obscene photographs, threatening messages, and false information on social media. In 53% of cases, suspects were convicted, whereas in 47% of cases, suspects were acquitted due to hostile witnesses, hostile victims, or the incapacity of the victim to produce significant evidence.

No woman shall be subjected to physical, mental, sexual, psychological, or any other type of violence or exploitation, as stipulated in Article 38, Section 3, of the Constitution of Nepal. Only the Electronic Transactions Act 2063 BS and Electronic Transaction Rules 2064 BS are applicable to computer-related crimes. Section 47 of the Electronic Transactions Act appears to envision and limit itself to computer-related offences, such as the dissemination of illicit material and the regulation of transactions conducted via electronic media and the internet. The clause fails to take into account the rising degrees and severity of cybercrimes against women and girls on social media. The propensity of violence against women in online environments was partially recognised by the Act.

It only states that 'the act of harassing and causing unnecessary trouble against women, or act of defamation or insult of women' shall be punishable with a fine not exceeding one hundred thousand rupees. In absence of an IT Tribunal, a procedural barrier for access to legal remedies has been created in prosecution and suit of cybercrimes occurring against women and girls. The National Information and Communication Technology Policy, 2015 AD. attempts to uphold the women's right approach and gives the impression of being gender sensitive in its provisions. Recommendation No. 35 of Convention on the Elimination of all forms of Discrimination Against Women on Violence against Women lays down an obligation on the part of States in recognition of the contemporary forms of gender based violence against women occurring in the internet and digital spaces. This has equally been forwarded as a serious matter of concern by a report of the Secretary General in an 'In-depth study' in the UN General Assembly.

Nepal's internet penetration rate is nearly 63% as of Kartik 2074 is in Nepal which is a large number considering the country's underdeveloped state. Increasing acquaintances with internet, computer and smart gadgets among youths has connected them closer to global trends. This has also increased the risk of abusing the same to drive them towards cybercrime. The manifestation of cyber violence against women and girls is also a relatively new phenomenon. A vacuum created in the legal regime has disabled law enforcement authorities to react deeply into this matter.

The vagueness of the legal provision, inadequate policy framework, lack of technical knowhow among the investigation authorities and insufficient resources to locate digital evidence are critical areas for discussion. The enduring harm suffered by women in cybercrime exceeds in its impact much more than physical violence resulting in psychological stress, mental violence and in some cases violation of economic rights. In majority cases, women and girls lose their confidence in participating in public life due to the damaged reputation, character defamation and loss produced by cybercrimes.

Violence against women and girls in online spaces is gradually increasing. The legal and policy regime to address it does not seem to penetrate deep enough on the gravity and changing dynamics of the cybercrimes. Reliance on existing means of the criminal justice system does not deliver the sensible response to ensure justice to the victims of cyber violence. Creation of a safe online environment should be prioritised for prevention through programs relating to awareness on growing issues of online violence. Law enforcement authorities, prosecutors, judiciary and concerned stakeholders are required to draft long-term and sustainable evidence-based policy as well as anticipate opportunities of international cooperation for the investigation and combating of cybercrime.

ICT policies and laws should be framed to indoctrinate the concept of equality and dignity assuring women's rights and securing their safe space in the virtual world of the internet. Providing necessary resources, powers and measures for effective investigation to law enforcement authorities is also a matter of equal importance.

1.1.8. Nigeria

Under the old Nigeria Law of Evidence, 1945, opinion evidence is irrelevant in trials before the Nigerian Courts. The exceptions guarantee the admissibility of expert and non-expert opinions concerning foreign law, native law, and art. Arguably, the said definition is limited to documents that are tangible ie, something that is capable of being seen. The slow pace of development of computer & information technology infrastructure in Nigeria may have also accounted for the limited application of digital expert evidence. After the cases of R. v Onitiri and The Queen v Akpan, the Nigerian Supreme Court handed down two conflicting judgments on the admissibility of digital evidence. The Nigerian Government in 2001 commissioned a body of experts to design a National Policy on Information Technology (NPFIT) which subsequently resulted in the enactment of the National Information Technology Development Agency (NITDA) Act 2007. The 2011 Act allows the admissibility of digital forensic evidence in Nigerian courts. The practice of digital forensics has been given the force of law by section 68 of the Nigerian Evidence Act 2011. Digital forensic being 'the science of locating, extracting, and analyzing types of data from different devices' is acceptable in the Nigerian Courts [208].

It means digital forensic evidence emanating from handwriting, computer, DNA, fingerprints analysis sought to be presented in court by digital forensic experts are allowed. The recent enactment of the Nigerian Cybercrimes Act 2015 provides for cybercrime offences in Part III of the Act shows the necessity of digital forensic evidence. Digital information is often relevant in proving or disproving a fact or point in question relating to the guilt or innocence of a cybercrime perpetrator.

In Federal Republic of Nigeria v. Dr Joseph Nwobike (SAN),' the defendant was arraigned on a total of 18 count charge. The EFCC seized the defendant's Samsung Galaxy Note 4 phone and sent the same to their forensic department for analysis and extracted and published the contents. EFCC operatives illegally obtained the defendant's mobile phone and published his private and confidential text messages. The Court refused to expunge the digital forensic evidence despite overwhelming evidence of the illegality of the way and manner the EFFC obtained the evidence. It has sent a positive message to EFCC to continue trampling on the fundamental rights of innocent Nigerians.

In Jude Onwuzulike v. The State, the appellant was arraigned on a charge of kidnapping contrary to Section 315(2)(a) of the Criminal Code, Anambra State (Amendment) Law, 2009. In the course of the proceedings, the charge was amended to read Section 315(1)(b) and the appellant pleaded not guilty. He was found guilty and sentenced to life imprisonment without an option of fine in June 2014. Dissatisfied with the judgment, he appealed before the Court of Appeal, Enugu, which affirmed the decision of the trial court and dismissed the appeal. In arriving at the judgment, the court relied on a mobile forensic expert from the State Security Service.

An expert is someone especially skilled in any of the fields of foreign law, native law, or of science or act, or in identifying handwriting or finger impression. There is no specific law in Nigeria that lays down how a forensic expert skill is determined. However, for the Court to accept the digital forensic evidence or expert opinion, the expert must lay a foundation arguably through the expert's presentation of his credentials and experience. In the absence of evidence of a proper foundation of an expert's skill and experience before the Court, the Court is bound to reject the digital forensic evidence. For instance, in Harrison Odiawa v. Federal Republic of Nigeria, 'the evidence of one of the two handwriting forensic experts was rejected on the ground that he failed to give an account of his skill'.

A plaintiff realized that he had been defrauded and wrote a petition to the Economic and Financial Crimes Commission (EFCC). Subsequently, he was arrested and charged before the High Court of Lagos State (No. 40) Ikeja Judicial Division, found guilty of 48 counts, convicted and sentenced. Dissatisfied with the judgment, he appealed before the Court of Appeal. Two handwriting and document examination experts were called by the Prosecution and Defence to give their opinions on disputed documents. One incriminating and the other exonerating the appellant based on the similar disputed documents that they analysed. For a Court to discard one or the other conflicting expert evidence, it must rely on the following set out grounds:

1. Where such expert evidence or opinion is illogical and unreasonable
2. Where the expert fails to provide enough data analysis or basis to support his conclusion;
3. Where the Court itself makes its own comparison under the Evidence Act and reaches a different conclusion from that of the expert.
4. Where the expert who claims to have a particular skill in the field in question gives evidence in the Court. However, he fails to give an account of his skill, qualification, or experience in the said field. For which he is called upon to give his opinion.

A trial judge would be right to prefer credible evidence of a non-expert witness on an issue to the evidence of an expert on the same issue. In Akeredolu v Mimiko & Ors the Nigerian Supreme Court stated that "the court is not bound to accept the evidence of any expert, even one who has not disclosed incentive or motive other than helping the court in the quest for justice".

A digital forensic expert who is desirous of demonstrating how he or she arrived at his or her opinion in Court will do well to ensure that he lays the proper foundation by informing the Court either through an affidavit and showing the condition of the electronic gadget or computer sought to be used. This may also involve bringing a formal written application before the Court.

1.1.9. Turkey

IPv4 capacity is limited to 4,294,967,296 (2^{32}) addresses at maximum, but not all of the address space is useable. The temporary solution developed for IPv4 exhaustion is an IP address sharing among multiple subscribers. Less than 35% of the world uses IPv6 to access Google. Carrier-Grade Network (CGN) systems have many issues for ISPs and subscribers, yet they are still used by the majority of the ISPs. The number of CGN networks has increased significantly between 2014 and 2016. The identification of individual subscribers from internet-access logs is challenging and error-prone. This challenge may become more severe and widespread as large-scale IP address sharing increases. 90% of respondents during their investigations have encountered errors regularly related to CGN technologies [209].

A typical CGN system uses private IPv4 address, private port number, and time parameters to identify end-users uniquely. An average US customer generates 33,000 sessions per day, which would require one million customers having ISP to store 1.8 petabytes per year just for logging. The number of ports both TCP and UDP protocols can use is limited to 2^{16}, which is 65,536 ports. Some of these ports are reserved for specific uses (e.g., port 80 for HTTP).

If the IP addresses assigned to the clients were not shared, the ports would be abundant in most cases. However, when a public IP address is shared among a certain number of customers, the ports are also shared. Instead of assigning internal/external IP addresses and port numbers dynamically from available pools, a custom range of port numbers and external IP addresses are assigned to the customers with a special mapping algorithm. Deterministic CGN logging is more complex than port-assigning CGNs and requires additional work by system engineers to set up and optimize the system. Unless dynamic port range is enabled, when a subscriber consumes all of the reserved port range, further connection attempts of the subscriber would fail. If multiple clients get assigned to reserved ports at the same time, logs may be traced back to incorrect subscribers.

IP address and the timestamp are the key factors determining the prime suspects in the early stages of an investigation when a cybercrime is committed. When multiple users share the same public IP address to connect to the internet, the IP address no longer uniquely identifies the customer. Two solutions are proposed to overcome the problem. The importance of erroneous logs from a legal point is the misidentification of the subscribers as seen in criminal investigations conducted by Turkish law enforcement after 2016. If an ISP is asked to provide CGN logs, the correctness of the logs is trusted to the ISP, and it is difficult to verify its accuracy.

A CGN system has to log all of the necessary parameters explained in Section 3.1 to keep error-free logs. Incorrect logs have also been the case in the ByLock judicial trials in Turkey. ByLock was a mobile chat application, and whoever used it was deemed to be a member of the Fethullahist Terrorist Organisation (FETO). This study considers the latest list of ByLock users, which was prepared by using the CGN logs. The CGN logs provided by the BTK are flawed because of two explicit CGN errors. The missing public IP address and the port number where these two variables are mandatory for a session log to be valid in any CGN system. If there are significant differences in the public port numbers of a CGN in the same session, there might exist port-jumping errors. For each internet session, different port ranges can be assigned to the subscribers. Internet sessions can be inferred from the assigned private IP address and the session-start dates.

In some judicial trials, Historical Traffic Search (HTS) records are also requested along with CGN logs. HTS records are mainly composed of two types of data: GPRS and WAP. The whole HTS file was scanned to find both date and private IP address matching GPRS sessions with the CGN for which there are three unexplained irregularities.

One record has no upload data traffic and 60 bytes of download data traffic. It is technically impossible to generate an HTTPS web request with such an amount of upload and download traffic. It is concluded that not only logs of implemented CGN-systems but also logs of data services are error-prone. Vodafone Turkey has 1,655,000 public IPv4 addresses reserved yet they have 20 million customers. On average, 12 subscribers per public address have to be assigned.

A port-jumping error may lead to incorrect subscriber identification from the deterministic CGN logs. The 16th Criminal Chamber of the Court of Cassation has developed jurisprudence to verify the integrity of CGN logs presented to the criminal courts. This approach is also mentioned as credible evidence in a news report of the ByLock judicial case imprisonment to 6 years and 3 months. Turkcell has answered an official request and displayed which variables are kept as logs for Customer Data Record (CDR) and CGN sessions.

Analysis of data provided by Turkcell revealed that information related to the cellular station is only stored at the CDR logs of SGSN, GSN and PGW. No reverse-tracking could be found based on any judicial cases other than those in Turkey. There are cases where IP address and ISP-based data led to false arrests and judicial trials. Even truly detecting the subscriber of the IP address still does not guarantee that the subscriber has committed the crime. Denmark's decision to review over 10,000 court verdicts due to errors in their cellular networks system is an excellent example of why logs of ISPs should be cautiously used as evidence.

The Turkish agencies worked together to identify ByLock users. They identified 102,192 different people with 123,115 different mobile phone numbers and 6,748 fixed-line subscriptions. One of the agencies reverse scanned nine different IP addresses used by the server of the ByLock application. It determined who has ever made connections to one of these IP addresses from the destination IP address of CGN logs. According to estimates, the earliest date for reverse scanning was August 2014 with an end date around April 2016. In 2018, this procedure was slightly modified due to the “Morbeyin event” which led thousands of people to be released from prison and to get an acquittal. So, based on the ByLock-users list, a BDR is generated for all suspects and sent to the prosecutors to start a judicial prosecution.

Once the prosecution begins, more detailed CGN logs are requested as evidence. The 16th Criminal Chamber of the Court of Cassation made the first ruling about ByLock on 14 July 2017 (2017/1443 E, 2017/4758 K) and accepted ByLock usage as definitive evidence of FETO membership. Since membership to an armed terrorist organisation is a catalog crime, ByLock defendants were usually jailed pending trial. Until this finding was documented, the list of ByLock users composed by reverse-scanning of CGN logs was accepted as flawless. However, this procedure has changed with the “Morbeyin event".

A screenshot was taken from a digital forensic analysis report of a mobile phone officially requested by the ACPPO in a ByLock case. ByLock was a chat application similar to WhatsApp that generated hundreds of sessions in short time usage. In addition to very few connections provided in the CGN file, there are not even enough connections to register the application. If it is assumed that even as little as 1% of CGN records is inaccurate, this would result in mistrial of 1000 people on a list of 100,000 subscribers. It was demonstrated that a defendant could not have possibly used the ByLock application due to the number of CGN sessions as explained above, and yet, it was not removed from the ByLock-users list with the Morbeyin incident. The false-positive rate of reverse-scan is at least 10.75%. Although it cannot be differentiated how much of this percent is from erroneous logs or third-party apps like Freezy. The European Court of Human Rights ruled on 20 July 2021 that ByLock usage alone is not evidently sufficient for pre-trial arrest.

1.1.10. *Finland*

The evolution of information and communication technology has dramatically altered the context of legal investigation. In the past, eyewitness testimony and physical tracks and traces were the primary kinds of evidence in criminal proceedings. Increasingly, multiple sorts of computer data-based evidence are required to demonstrate the online and offline nature of suspected criminal acts and events. The law of evidence is fundamentally instrumental and not an objective in itself; it must best facilitate the pursuit of these sometimes contradictory and frequently impossible goals. For this reason, it is advantageous to explore outside of Finnish cases and law for viable answers or legislative enhancements [210].

Nordic and continental countries with similar legal histories are of special relevance, although common law jurisdictions can also provide insight. In Finland, pre-trial investigations are governed by recent legislative actions. The Coercive Measures Act (806/2011) is the key component of this framework. This statute has been in effect since January 1, 2014, when it superseded a previous statute with the same name. The dissertation consists of seven chapters, with an emphasis on the gathering of electronic evidence.

The act incorporates a number of particular regulations regarding the search and monitoring of digital devices and bolstered the general principles of proportionality, minimum involvement, and sensitivity. The Criminal Investigation Act (805/2011), which oversees criminal investigations, and the Police Act, which has powers comparable to coercive measures for the purposes of crime prevention and detection, are also significant components of the framework. Electronic evidence is frequently admissible in the Finnish court system, regardless of issues regarding its legitimacy, integrity, or reliability. The statute provides no special instruction regarding electronic evidence or other sorts of evidence. Regarding the goals of certainty, swiftness, affordability, and equity, the current law has both positive and negative aspects.

The concept of equality of arms may be at peril if there is a lack of openness, which may also impede proper dialogue. Lack of ICT knowledge and proficiency may exacerbate these issues. Financial and time savings are by no means certain. In terms of evidence-related expenses and time consumption in a particular case, the ICT expertise of the parties and court officials may be more important than the actual law.

The ten suggestions are:

1. In the context of protecting electronic evidence, adherence to data protection legislation should be highlighted.
2. Organisations (in particular) should prepare how to secure electronic evidence prior to the commission of an offence, using technical safeguards to ensure the legitimacy and integrity of any electronic traces.
3. To improve the quality of electronic evidence, a new provision should be added to the law requiring the authorities responsible for pre-trial investigation to adhere to any generally accepted best practices in the field of digital forensics, whenever these do not conflict with specific norms protecting an individual's privacy or legally privileged relationships (doctor - patient, lawyer - client, etc.).
4. Regardless of the preceding suggestion, to emphasise the significance of the chain-of-custody and the audit trail, a distinct provision should be introduced to the law.
5. The law should be amended to include a clause requiring the defendant to consent to the use of a biometric identifier in order to bypass a login mechanism or decrypt encrypted data.
6. The coercive power of extended monitoring should be redefined in light of the network environment's characteristics.
7. For the purpose of defining the offences in the investigation of which different coercive means are authorized, a simpler legislative approach should be used; concurrently, the conditions of use and definitions for particular coercive measures should be reevaluated.
8. The necessity of regulating the presentation of actual evidence should be reviewed further.
9. When determining the admissibility of illegally obtained evidence and evaluating such evidence, particular attention should be given to issues pertaining to the quality of electronic evidence.
10. In evaluating evidence, particular attention should be paid to the fundamentals of ICT and the unique characteristics of electronic evidence, and an increased emphasis should be placed on the procedures that produced the evidence.

Many of the suggestions presented here are related to very specific aspects or provisions of Finnish national law concerning coercive measures and pre-trial investigation. In contrast, the discussion on how to best evaluate real evidence in electronic and digital form is more universal. These questions have the aim of helping the trier of fact to recognise misconceptions about the meaning or relevance of computer data presented as evidence. These questions are not meant to replace existing models of evaluation, but to complement and support them. The author's view is that reasoning based on hypotheses or explanations shows more promise than probabilistic models in evidentiary scenarios typical of the network society.

1.2. *Jurisprudence in digital evidence*

1.2.1. *Convention on cybercrime*

The Convention on Cybercrime is the only international agreement on cybercrime. It is a unique agreement between the member states of the European Union, but also includes Unite States, Canada and Australia who are signatories and have ratified the agreement.

The agreement comprises three parts: substantive law, procedural requirements and international cooperation; and creates four categories of substantive offences:

1. Offences against the confidentiality, integrity and availability of computer data and systems, comprising interference and misuse of devices (hacking offences);
2. Computer-related offences such as forgery and computer fraud;
3. Content related offences, especially those related to the production, dissemination and possession of child exploitation material; and
4. Offences related to copyright infringement.

In addition, the convention addresses the procedural aspects of cybercrime to facilitate common understanding and expectations between jurisdictions:

1. Expedited preservation of stored digital evidence;
2. Expedited preservation and partial disclosure of network traffic evidence;
3. Production orders;
4. Search and seizure of stored digital evidence;
5. Real-time collection of network traffic evidence; and
6. Interception of content digital evidence.

Maurushat et al. (2019) goes on to compare the legislative provisions of the convention with the respective Canadian and Australian criminal codes [211].

1.2.2. *AI and evidence*

The authors [212] discuss the gathering and processing of evidence using Artificial Intelligence (AI) systems. AI evidence consists primarily of electronic evidence. Evidence in electronic form is capable of being altered or even deleted, deliberately or inadvertently. The main consideration is to ensure that such evidence and the systems that store, process and analyse them are trustworthy and reliable. For investigative work, police use cell phone tracking software and case-management software to streamline the collection and analysis of collected evidence. Prosecutors, lawyers and judges use case tracking and management systems to manage caseloads and dockets.

Machine Learning (ML) enables systems to directly learn from examples, data, and experience. There are three primary types of ML: supervised, semi-supervised, and reinforcement. Although powerful, ML can provide unexpected or inaccurate outcomes. Due to its reliance on human judgement and prejudices, it is prone to a variety of additional constraints. An AI system may be unstable when presented with novel combinations of data; therefore, even if it has been trained on previous decisions that have been independently verified by experts, this may not be sufficient to justify a high level of confidence in its subsequent decision. The difficulty of interpretability - the necessity to represent knowledge encoded in the learning system in a way that people can comprehend.

The presumption that computer systems are "reliable" underpins many exclusionary rules of evidence such as the best evidence rule, business records exception to the hearsay rule, and the authentication evidence rule. Judges have erroneously elevated the presumption into a legal presumption that reallocates the burden of proof, not on the proponent of electronic evidence, but on its opponent. They asked for access to the "known errors log" for the Horizon system, which would have recorded all errors that had taken place on the system. The Prosecution argued that this was not sufficiently focused and that it would be "enormously expensive" to provide this material. A judge ruled in favour of the Prosecution, holding that the Defence had ample material to test the integrity of the system before a lengthy trial in 2019.

The authors argue that the presumption of reliability should operate only to place an evidential burden on the party opposing the presumption. The Evidence Act does not prescribe how this requirement can be met, but evidence of the correct, accurate and proper operation of the system can come from users who have used it. The burden of proof remains with the proponent of electronic evidence to prove the evidence. In the Singapore Evidence Act, the presumption may be easily refuted where there is evidence sufficient to raise doubt about the presumption. The Australian Commonwealth Evidence Act uses a similar formulation in relation to its reliability presumption.

It could take very little for the presumption to be rebutted, if the party against whom the evidence was adduced could not be expected to produce more. It is not generally true that "most computer error is either immediately detectable or results from error in the data entered into the machine". Most of such blatant errors will be caught in evaluation, beta testing and unit tests, and will not make their way into production. Modern software is complex and may interact with other systems which operate their own separate and independent platforms, environments and systems. Traditional methods of testing software for mistakes such as unit tests and the unit test platforms themselves are unlikely to be very helpful.

This is especially the case when AI systems have errors embedded in them that will activate only in exceptional circumstances. An example of an "unreliable" AI system operating in such an environment is the case of the Uber autonomous vehicle that killed a pedestrian. Autonomous vehicles will have to demonstrate that they can comply with traffic signs and traffic rules. There is no limit to the type of exceptions which AI systems can be exposed to. The robustness of an AI system will largely depend on how many of these variations in environments it has been tested in.

Evidence of a statement made to a witness by a person who is not himself called as a witness may or may not be hearsay. It is hearsay and inadmissible when the object of the evidence is to establish the truth of what is contained in the statement. In Singapore, any assertion express or implied or intended - is prima facie treated as hearsay if it is tendered for the content of its assertion. The hearsay rule - that any evidence must be "testable and reliable" - has remained a tenet for both the common law and civil law systems.

Today, almost everybody uses electronic evidence and through human interactions, assessments are made to decide whether to rely on it. Information such as phishing e-mails, mobile telephone scams, false news and clickbait is constantly rejected. As such, this raises questions as to its correct treatment in a court of law. AI systems can produce many different types of evidence. Voice recognition systems can be automatically activated and store conversation snippets it has recorded. Image recognition systems such as those found on traffic enforcement cameras can capture photographs of vehicles.

Fraud detection systems can monitor credit card transactions and identify anomalous transactions for further investigation. But is such evidence allowed under the hearsay rule? Evidence produced by Category 2 devices (autonomous data processing systems that acquire input or make records without human intervention) is evidence that is substantially the product of automation and is not used testimonially. For instance, many criminal prosecutions in England have succeeded through the admission of automatic number plate recognition evidence. English courts appear relatively sanguine in admitting such evidence, with no noted hearsay challenges raised.

The reason for the absence of challenges is that such evidence is considered real evidence or "evidence produced purely mechanically without human intervention". A large majority of AI evidence will be produced by Category 3 devices (a combination of devices that accept human input and generate output with those in category two), which operate without human intervention. As supervised ML systems are trained on human-labeled data so that they can operate autonomously, therefore will invariably fall into this category.

Yet there is a limit as to how far this analogy can be stretched. ML systems that recognise handwritten numbers have been trained on the Modified National Institute of Standards and Technology dataset of handwritten digits. The hearsay rule helps to tease out the embedded human assertions from results sought to be admitted in evidence - be it the ML code or its data. If there is no opportunity for the human assertions to be tested - for instance, if the automatically-produced analysis is to be relied on but the programmer who generated the analysis is not called to testify - the analysis becomes hearsay.

Authenticity of electronic evidence is always an important issue in its admissibility because of the inherently mutable nature of electronic documents. It raises an intertwined complex of legal and technical questions about their integrity and security. The rule of hearsay assesses the reliability of the evidence by determining if the record is capable of representing the facts to which it attests. Authenticity of the electronic record means demonstrating that the evidence is genuine - that it is what it claims to be. Authentication can be the basis for raising issues as to the identity of electronic record, its integrity and immutability (whether it was altered, manipulated or damaged between the time it was created and when it was tendered in evidence), its authorship and its security.

Many judges have resiled from this evaluation because they have made erroneous assumptions about the evidence before them that are not warranted. There is an implicit willingness to assume that organisations carry on their business competently, even where the challenge goes to undermining that business competency itself. A clear procedure should be set up to prescribe how matters regarding the authenticity of electronic evidence should be raised. In criminal proceedings, the Defence should be required to provide advance warning to the trial judge that identified aspects of the evidence will be questioned.

"Deep fakes" involve the alteration of existing images or videos in which a person's image or likeness in that image or video is replaced with someone else's likeness. These modifications are made possible by using ML and AI techniques such as autoencoders and generative adversarial networks. Some techniques can even replace the audio streams of a video with synthetic speech that replicates the speech patterns of a well-known person. Digital evidence professionals are increasingly becoming aware of the issue of digital fakes, where digital images and 3D imagery have been manipulated to support fraudulent papers. Detecting a manipulated image takes time, expertise and appropriate tools, but advances in software programs mean it may not be possible to detect manipulation in the near future.

Given advancements in ML technologies, it is not expected that such systems would be able to determine if an image is real or computer generated. Courts need to develop a set of clear procedures for managing authentication issues, as discussed above, and a healthy appreciation of the limits of the presumption of reliability. Only then can a robust approach towards disclosure or discovery, which will be discussed below, be effectively elucidated.

The primary objective of discovery and disclosure is to enable a party to acquire information which he does not have concerning the issues in the proceeding. Without effective discovery, a party may not have a sufficient opportunity to challenge the opposing party's evidence. This is because only the party in possession of electronic evidence - the proponent - has the resources, access rights or knowledge to fully understand the system from which the evidence was extracted. In criminal proceedings, if the proponent is the defendant, this has the unfair effect of undermining the presumption of innocence. The introduction of electronic discovery seeks to address that imbalance. But loosely grouped documents may stymie typical searches on broad allegations and loose terms.

The use of predictive coding (another name "technology assisted review" using AI) for to help to search for relevant information can yield cost and time savings, and is often a practical necessity when the party has to deal with voluminous electronic documents. To work properly, the ML system also has to be trained properly, typically by the most experienced lawyers with requisite domain knowledge of the subject matter. It is relatively unusual for a judge to order the disclosure of relevant software, yet arguably it may be crucial to fully understand a report or test result generated by an automated system.

The court may also rule that such discovery is not necessary for disposing fairly of the action or will incur unnecessary costs. Subsequent investigations by experts suggested that the Toyota electronic throttle control system contained many software defects and that at least one of them was capable of causing a malfunction. It is only with robust operation of discovery laws that such technologies can be further refined and improved. It is proposed that prosecutors lay a foundation for the reliability of evidence generated by devices by presenting testimony about validation studies.

The authors content that validation studies are likely to be adequate only for processes with well-defined and scientifically testable processes operating on simple procedures and they are unlikely to be helpful for complex systems such as those used in AI systems. Some form of regulatory oversight will enable greater governance over such platforms and facilitate transparency of the AI system. Whether it is necessary to disclose the code for an algorithm audit and, crucially, in the case of AI systems, whether this transparency requirement extends to disclosing the training and test data themselves so that the models can be reviewed will depend on the jurisdiction of the reviewing party, actual application of the AI system and the nature of the ensuing dispute. In any event, it is in an organisation's own interest to ensure that its automated decision-making processes are explainable, transparent and fair, not only for building trust and confidence but also as part of the corporate risk management framework.

1.2.3. *Physical fruits vs digital fruits*

The Supreme Court of the United States has yet to weigh in on Fifth Amendment protections for digital devices. Digital devices contain a 'cache of sensitive personal information' pertaining to every aspect of a person's life. A person in custody and questioned by police likely does not understand that the Fifth may protect unlocking a cellphone or a statement communicating the passcode. Justices should address developments in technology in its Fifth Amendment and Miranda doctrine, like it has done for the Fourth Amendment. While Patane applies to objects like guns or drugs, the decision should not bar exclusion of highly personal records, like digital data. If a court equates the contents of digital devices with physical objects, it does not even need to rigorously analyse whether Miranda applies [213].

1.2.3.1. The 4th and 5th amendments in investigations involving digital devices. The average person may not know they have any rights when they are first detained. If the officer asks if they can look at the individual's phone, both the Fourth and Fifth Amendment protections have been bypassed for the contents of the person's device. Consent negates need for a warrant to search a phone, as is shown by the Supreme Court in Riley v. California. Miranda may only apply to certain methods police use to unlock a phone. There is a split amongst state supreme courts about when unlocking a device violates Miranda.

The Supreme Court will need to provide guidance on how the Fifth applies in cases involving modern technology. The Fourth and Fifth Amendments are inextricably linked because they address two different issues that arise during investigations and prosecutions. The Supreme Court has realigned Fourth Amendment protections with changes in technology, without addressing how the Fifth Amendment fits in. A police officer's request to "please unlock your phone" invokes both constitutional issues in one sentence. To imagine that the Fourth and Fifth Amendments do not interact is to ignore how they come up in real life.

In the 19th century, the Court linked the two amendments together in Boyd v. United States. The Court took an expansive view of what the Fifth Amendment meant, in contrast to the current Court. In Boyd, the Court took the Fifth Amendment to mean more than just statements made at trial. The Court later walked back this expansive view - as seen in Patane. Only in the past few decades has the Court narrowed Miranda by describing it as a mere prophylactic.

In many cases, the Fourth and Fifth Amendments are interwoven. This is because both "regulate government attempts to gather information," meaning potential Fifth Amendment events may also be potential Fourth Amendment events. Viewing each amendment in a silo may feel doctrinally pure, but it can lead to confusion. For police, the "golden window" to gain access to a device's contents comes before formal criminal proceedings like an indictment and via a consent search. Police are free to ignore Miranda in their pursuit of accessing all contents on the device because of how courts interpret Patane.

A request of someone in custody to open their phone may be quickly followed by a request to "take a look" at the contents of the phone. The average person is unlikely to understand that unlocking a phone and providing consent to search the phone are two different actions, with different legal consequences. It is likely that judges will likely ignore the pressures people feel to unlock phones.

1.2.3.2. The physical fruits doctrine in cases involving digital devices. In 2004, the Supreme Court decided Patane, expanding the reach of the Fifth Amendment. Justice Souter wrote a dissent that refuted the plurality's characterization that physical fruits cannot implicate the Self-Incrimination Clause. Justice Kennedy agreed admitting "non-testimonial physical fruits" does not risk admitting a person's "coerced incriminating statements" against himself.

Justices Souter, Thomas, Breyer and Thomas wrote that courts should exclude physical evidence resulting from Miranda violations for the reasons articulated by Justice Souter. Just a handful of federal courts have addressed the application of Patane to digital devices. Most post-Patane cases have addressed purely physical objects, like guns or drugs. In United States v. Stark, the Eastern District of Michigan admitted photographs found on a password-protected computer. Patane allowed the admission of "non-testimonial, i.e., physical, evidence obtained as a result of incriminating statements made in violation of Miranda".

Patane has encouraged police to disregard Miranda when physical evidence is worth more than a defendant's statements. But the court's reasoning in Djibo focused on the intensely private nature of the information. Courts should not blindly apply Patane without grappling with how digital evidence fits in with the doctrine.

1.2.3.3. Litigation strategies in cases involving digital devices. In the absence of direction from the Court, defense attorneys still need to advocate that Patane should not apply to digital devices. Attorneys can take one of two main approaches: argue that the Fifth Amendment should respond to changes in technology like the Fourth Amendment has or explain how existing Fifth Amendment principles and Patane support the exclusion of digital evidence. Kennedy's concurrence leaves room for courts to balance the interests of law enforcement and a possible need for deterrence. The Court has started to recognise this view in Riley and Carpent. One approach to litigating Patane issues in the context of digital devices is to argue that digital devices require a new rule.

Digital devices have given law enforcement multiple advantages in the Fourth Amendment context. Unlocking a device in violation of Miranda and gaining consent to search the device gives police access to digital content well beyond what they would view if they received a warrant. The balance of power shifted long ago in the Fifth Amendment context as people increasingly began to rely on digital devices. Digital devices present even greater incentive issues than traditional physical fruits for law enforcement. Introducing statements, thoughts, and locations as the defendant's - with no real way for the defense to refute without having a defendant testify - seems like a tempting proposition for police.

It is argued that courts should adopt bright-line rules responsive to new contexts and changes in the "legal ecology," like they have done in the Fourth Amendment context. The Court's Fifth Amendment doctrine needs to recognise the ways technology has changed how people communicate, express their thoughts, and process private information. Patane has already created the "unjustifiable invitation to law enforcement officers to flout Miranda when there may be physical evidence to be gained" that the dissenting justices feared. A clear rule offering additional protection for the contents of digital devices would likely make police more cautious. Advocates can also tie their arguments to underlying principles in the Fifth Amendment doctrine.

Some Supreme Court justices have long suggested that highly personal, prerecorded information - like a diary - is testimonial, and should be treated differently than other prerecorded statements or objects. Now is the time for the Court to turn back towards recognizing the interplay between the First and Fourth Amendments. Court has repeatedly expressed that the most private of papers - like a diary - may remain protected by the Fifth Amendment, even when documents like business records are not. A "diary exception" provides protection for some highly personal, but prerecorded, information, in contrast to recent restrictions to the meaning of "testimonial" evidence.

Justices and scholars have argued that invasive physical information - like breath or blood tests - differ from private documents like diaries. Diaries express statements like opinions, fears, or reflections, showing a communicative dimension not found in other physical objects. Digital devices are simultaneously physical objects and containers of vast troves of data. If law enforcement violated Miranda to unlock the device, that creates a presumption that they accessed the device's contents through compulsion or coercion. The existence of a diary is not troubling in the same way that its contents are.

The contents of digital devices look much closer to a diary than the business records in Fisher or the blood sample in Schmerber. Original understandings of the Fourth Amendment offered more protection to "papers" than "effects". Patane is a fractured decision, and confusion has led defense attorneys and courts to ignore a possible exception to the rule that physical fruits do not implicate the Fifth. Justice Kennedy seemed to signal that his opinion controlled by explicitly noting issues from Justice Thomas's opinion that he declined to address. But unlike Justice Thomas, Justice Kennedy did not categorically state that deterrence was irrelevant to the inquiry.

Justice Kennedy's concurrence leaves open the possibility that another object could, after weighing the need for deterrence compared to the item's probative value and reliability. Digital fruits may be that very situation where Justice Kennedy might have found that deterrence outweighs law enforcement need for access. The Eleventh Circuit concluded that Miranda does not require the exclusion of physical evidence that is discovered on the basis of a voluntary, although unwarned, statement. Just because courts have not applied Marks to Patane does not mean they should continue ignoring Marks. The vast majority of cases applying Patane may never need to address this nuance, but digital devices require a deeper analysis.

If anything can meet the balancing test in Justice Kennedy's concurrence, it will be the contents of digital devices. Justices' concerns about digital evidence may cut towards excluding digital from Fifth Amendment protection. Justices may believe that someone normally acquires a phone by heading out to an Apple Store and picking up a new iPhone. But many Americans acquire phones through means other than directly buying a brand new phone from a store. Digital fruits present a huge trove of information, that information often needs interpretation.

There is a strong need to protect individual rights, particularly in the context of digital evidence. Police have other options - including getting a court order requiring someone to decrypt the device. Digital evidence requires deterrence in a way not required by a purely physical object like a gun. As described in Djibo, a cell phone passcode is the proverbial "key to a man's kingdom".

1.2.4. United States – digital evidence in criminal cases before U.S. courts of appeal

The study identified 145 appeals involving legal issues related to digital evidence heard by the United States Courts of Appeal for the period 2010–2015. Of the appeals included in this study, 138 appeals (95.17%) were either affirmed or reversed for the government and seven appeals were either affirmed or reversed for the defence [214].

Adopted for the first time in 1975, the United States District Court System adheres to the Federal Rules of Evidence (FRE). The rules governing the introduction of digital evidence are comparable to those governing the introduction of other types of evidence. The legal issues that arose in the 145 cases analysed in this study were classified as Search and Seizure and Trial Evidence.

1.2.4.1. Search and seizure. Digital evidence produced at trial must have been obtained with a valid search warrant based on probable cause to search for evidence of a crime or criminal activity. If probable cause cannot be demonstrated, then evidence will likely be suppressed under the Exclusionary Rule. There are exceptions that allow law enforcement to engage in warrantless searches.

In United States v. Schesso, 730 F.3d 1040 (9th Cir. Wash. 2013), the district court for the Western District of Washington appealed a district court ruling on the suppression of evidence gained from a search of the defendant's home. The Ninth Circuit Court of Appeals reversed this decision determining that "because there was a fair probability that evidence of child pornography would be found on the computer system, the underlying facts supported a finding of probable cause".

Jack Eugene Hampton appealed his conviction on charges of receipt and possession of child pornography. Hampton argued that the affidavit used to obtain to search his residence was "stale because the warrant was executed more than ten months after German law enforcement officers observed child pornography shared through his IP address". The Sixth Circuit found that the delay did not cause the information to become stale.

Justices have consistently held that warrantless seizures are per se unreasonable, with a few exceptions. Eric J. Bradley was convicted and sentenced for receiving visual depictions of minors engaged in sexually explicit conduct. A panel from the Sixth Circuit ruled that the execution of the warrantless seizure was reasonable on the grounds that the evidence might be destroyed and the government's interest is significant.

In United States v. Evers, 669 F.3d 645 (6th Cir. Feb. 10, 2012), Ovell Evers challenged his conviction and sentence for production of child pornography, in violation of 18 U.S.C. Sections 2251(a) and 2252(a)(4)(B). In his appeal, Evers contended that the search warrant authorized the seizure of his computers, camera, and other electronic media but did not authorize a search of the hard drive. In this instance, the court affirmed both the conviction and sentence for Evers.

Guy Edward Wheelock appealed his conviction and sentence for receiving child pornography. In his appeal, Wheelock contended that an administrative subpoena violated his Fourth Amendment privacy interest. A federal court in a federal prosecution do not suppress evidence in violation of state law, so long as the search complied with the Fourth Amendment.

1.2.4.2. Evidence presented at trial. In United States v. Dixon, 589 F. App. 427 (11th Cir. Oct. 23, 2014), Travis "Rocky" Dixon was convicted of receiving child pornography and possession of child pornography, both in violation of 18 U.S.C. § 2252(a) (4) (B). Following his conviction, Dixon contended that the government produced insufficient evidence to prove beyond a reasonable doubt that he was guilty of downloading the child pornography found on a computer in his bedroom. A panel for the Eleventh Circuit found that there was sufficient evidence for a rational jury to conclude that Dixon knowingly received and possessed child pornography.

In United States v. Flyer, 633 F.3d 911 (9th Cir. Feb. 8, 2011), Andrew Flyer appealed his conviction "in the U.S. District Court for the District of Arizona" for possession of child pornography. The panel noted that no evidence was presented that Flyer knew of the presence of the contraband images in the unallocated space on his computer. Consequently, Flyer's conviction for possession of child pornography was reversed. The convictions for attempted shipping of child pornography and possession of child pornography on CDs were affirmed.

Digital evidence is relevant if it makes a fact more or less probable than it would be without the evidence. Relevant evidence may be excluded under Rule 403, Excluding Relevant Evidence for Prejudice, Confusion, Waste of Time or Other Reasons. Donald Reynolds argued that expert witness testimony based on historical cellsite data lacked relevancy. The FBI introduced historical cell phone records to help determine who was at home during the relevant download periods in their investigation. This information did not show that he was absent from the home during those download periods. His conviction and sentence were thusly affirmed by the panel from the Sixth Circuit.

In United States v. Ballard, 448 F. App. 987 (11th Cir. Dec. 15, 2011), Kenneth Allen Ballard appealed his conviction for distribution and receipt of child pornography. Ballard contended that the images unfairly prejudiced the jury and that the impact of the images offset their probative value. The Seventh Circuit found that the relevant evidence was not extrinsic to the crime, but was part of the actual pornography possessed.

Digital evidence must be authentic. Court Rule 901, Authenticating or Identifying Evidence states that to satisfy the requirement of authenticating or identifying an item of evidence, the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is. Digital evidence is subject to the Federal Rules of Evidence 1002 and 1003 for Best Evidence. Rule 1002, Requirement of the Original, states that original writing, recording, or photograph is required in order to prove its content unless these rules or a federal statute provide otherwise. In United States v. Lanzon, 639 F.3d 1293 (11th Cir. May 4, 2011), the court stated that "evidence may be authenticated through the testimony of a witness with knowledge". In United States v. Lebowitz, Adam Lebowitz appealed his convictions for producing child pornography and attempting to entice a child to engage in unlawful sexual activity. At trial, the United States District Court for the Northern District of Georgia admitted into evidence printed transcripts of chat messages with a minor. The panel found that the district court did not err in admitting the chat session printouts into evidence.

Hearsay is an out-of-court statement introduced for the truth of the matter asserted. It applies if the proponent plans to use the record's contents as substantive evidence. Hearsay generally may not be admitted as evidence. The question before the Ninth Circuit was whether a Google Earth satellite image and digital tack labeled with GPS coordinates should be considered hearsay. The panel found that Google Earth produced an exact replica of the map introduced as evidence in this case, with the GPS coordinates marked exactly as they were in evidence.

In considering whether the Google Earth image was hearsay, the panel held that a photograph isn't hearsay because it makes no assertion. Rather, a photograph merely depicts a scene as it existed at a particular time. The panel's decision upholds the defendant's conviction.

In United States v. Stanley, 533 F. App. 325 (4th Cir. July 19, 2013), Paul Stanley appealed his conviction for receipt, transportation, and possession of child pornography. Stanley argued that the district court erred in admitting expert testimony from an agent who conducted the forensic examination of Stanley's laptop computer. The U.S. Court of Appeals for the Fourth Circuit found that agent Gilmer was part of a lengthy voir dire that established her competence as an expert.

- The most common ground for an appeal was Probable Cause. For Evidence Presented at Trial, Sufficiency of Evidence was the most common ground for appeal.
- Twelve instances included in this study (8.16%) had their defence appeals upheld or reversed.
- Five of the defense's ten reversals were based on Sufficiency of Evidence.
- There were two instances in which defence judgments were upheld, one based on a defective warrant and the other based on the warrant's breadth.
- The bulk of difficulties identified in this study were associated with Search and Seizure rather than computer forensics.
- Regarding the scope of search warrants, specificity is a cause for concern. Particularity governs the scope of a government's search based on a specific factual predicate. Courts have lately resolved a number of significant instances involving particularity (Riley v. California, 134 S. Ct. 2473 (2014), and United States v. Ganias, 725 F.3d 125 (2008)). (2d Cir. 2014). This question will remain fundamental to appeals based on Search and Seizure in general, and digital evidence in particular.

1.3. *Digital evidence in legal proceedings*

Following a few examples of the way which digital evidence was accepted and interpreted in some specific cases.

1.3.1. *Bulgaria*

An appeal has been filed against the decision of First Instance for the part where the claim brought before it has been upheld with a complaint that the decision is wrong and unlawful. It is alleged that the printout of Facebook messages exchanged between the parties is not a valid proof as an objection was made with the reply to the statement of claim. A court in the Bulgarian city of Dimitrovgrad has dismissed a case brought by a veterinarian against the owner of a seven-year-old female dog of the Pekingese breed, and that of a male specimen of the same breed, born on the same day. The parties had an arrangement for the breeding of their dogs, and after birth one of the newly born had to be handed over to the appellant M. after 30 days [215].

D.M. is a veterinarian and performs procedures for artificial insemination of dogs in her laboratory in the town of Dimitrievgrad. The main dispute in the case is focused on the matter of proving the agreement reached between the parties, the default of which has given rise to the present claim. The printout of the exchanged by the parties messages on Facebook constitutes an electronic document in the sense of Art. 3, Para 1 of Electronic Document and Electronic Trust Services Act (EDETSA). Appellate Court finds that electronic document submitted in paper form constitutes valid evidence within the meaning of the CPC. The parties had reached an agreement for the breeding of the dogs of the Pekingese breed owned by them and the handing over of one of the newly born to the appellant M., which the appellant failed to fulfil.

Bulgarian court has ruled that messages exchanged over the social media website Facebook constitute a valid electronic document. 'Electronic document' means any content stored in electronic form, in particular text or sound, visual or audio-visual recording. According to the provisions of article 184 of the Bulgarian Code of Civil Procedure, the electronic document may be reproduced on paper as a copy certified by the party. A certified copy of electronic statements exchanged on Facebook complies with the requirements of Bulgarian law and may be qualified as valid evidence. The case confirms that a legally binding agreement can be constituted with a correspondence over social media. Since the authorship was not challenged, it has correctly admitted it under the provisions of article 4 of the EDETSA, according to which the author is named in the statement as such [216].

1.3.2. *China*

A mother took her 4-year-old son into the female dressing room of a swimming pool and was scolded by the manager and cried, published on Ladyfirst.com. The content and illustration of the alleged article were the same as the involved article. Lawyers argued that the defendant, Daotong, provided an exchange platform for women and fashion information, and did not earn any profit from redistributing the involved article. The parties submitted evidence in accordance with the law for their claims, and this court required the two parties to exchange and cross-examine the evidence. Regarding the certificate of labour relations, authorisation and the supplementary statement by Huatai Yimei, Daotong argued that part of the evidence was submitted after the court debate and should not be used as evidence [217].

Zhejiang Shuqin Technology Co., Ltd. (hereinafter, 'Shuqin') used the back-end code to take a screenshot of the target webpage through Google's Open Source Program 'Puppeteer' plug-in unit. The Qianmai Identification Institute issued a Judicial Identification Opinion on 20

June 2018, stating that it was entrusted by Zhejiang Shuqin Technology Co., Ltd. to identify whether the document entitled (hereinafter, 'the infringement document package') had been modified after preservation. The value is the transaction hash value of block with height of 482210, and the block time is '2017-08-27 13:31:20' (Greenwich Standard Time). The storage contents are consistent with KEYMR values in blocks in the FACTOM block chain. City Express is a legal entity in the form of a public institution.

A court in China has ruled that Huatai Yimei has the standing to sue Daotong for alleged infringement of its copyrights. The court also found that the content of the article and the attached pictures were original and protected under Chinese copyright law, and that the amount of compensation claimed by Yimei is reasonable. The court reviewed the credibility of the electronic evidence preserved in the block chain. BAOQUAN.COM server can scrape images from the target webpage by automatically calling the Google open source program Puppeteer, and at the same time obtain the target webpage source code by using Curl.

The possibility of relevant linkages being tampered is relativity low, thus the credibility of such electronic data source is relatively high. A. Review whether the electronic data uploaded is that involved in this dispute. B. Search the FACTOM Blockchain using the transaction hash value provided by Huatai Yimei to view its contents and the generated time.

The upload time and the time when the webpage's screenshots and its source code are captured using Puppeteer and Curl as indicated on the call log. This court confirms that the BAOQUAN.COM has uploaded the electronic data to the FACTOM block chain and Bitcoin block chain. In this case, the Shuqin Company is a third-party depository platform that complies with the law fixing electronic data such as infringing works. The involved work was published on the 'Ladyfirst.com.cn' operated by Daotong.

At the same time, BAOQUAN.COM uses the block chain technology that complies with relevant standards to carry out the deposit and fixation of the above electronic data. In accordance with article 48 of the Copyright Law of the People's Republic of China, anyone who commits any of the following infringements shall cease the infringement, take remedial actions, make an apology, pay damages, or/and undertake other civil liability depending on the circumstances.

1.3.3. Estonia

A court in Tallinn has sentenced an individual to two years' imprisonment and one year and six months in prison for giving false information to the tax authority. The punishment will not be enforced, provided he does not commit another intentional crime during a two-year probationary period. In the course of the tax inspection, the individual submitted incorrect information to the Tax and Customs Board [218].

The appeal seeks to refer the matter back to Harju County Court for reconsideration. The court finds that income and social tax was not payable on undisclosed fringe benefits in the form submitted in April 2011 in annex 4 to the tax declaration. The value of the fringe benefit could have been the market price of renting of the property or the difference between the rent and the discount price. The county court has failed to properly evaluate the evidence that confirms the absence of the subjective elements of the offences claimed by the accused. A Tax and Customs Board reviser admitted that the above-mentioned rental transaction generated taxable turnover for the landlord.

The county court relied primarily on the inspection protocol showing Skype conversations of the individual. The inspection protocol of 3 June 2014 in criminal case no. 12221000084 is, in the light of the circumstances in which it was prepared, an unreliable and unacceptable item of evidence. The county court is in serious violation of criminal procedural law by not having taken into account as evidence the written assessment of the accredited external expert.

The inspection of evidence was carried out by officials who did not have relevant professional competence and the protocol does not meet the content requirements. The county court has ignored the fact that in the case of VAT, a subsequent drawback has been made.

Judicial Chamber to rule on admissibility of evidence collected by surveillance activities and evidence obtained from electronic communication undertakings. Court notes that all permissions for surveillance activities in the context of criminal proceedings under review, are ruled out. Circuit Court for the Eastern Division of the District of Columbia has ruled that the county court's ruling does not comply with the requirements set forth by the Supreme Court to justify the surveillance of the individual, a businessman accused of money-laundering and other criminal offences. 'The circuit court must agree with the appellants that the permissions issued by the State Prosecutor are not duly reasoned. The reasoning in the rulings merely confines itself to arguing that other means for gathering evidence is difficult or even excluded without prejudice to the criminal proceedings'.

The chamber finds that none of the permissions contain any justification as to why the inquiries are strictly necessary. It is obvious that data obtained from a communications undertaking may be relevant for an investigation of a money laundering crime. The circuit court dismisses evidence-based surveillance actions based on the permissions and proceedings of the Harju County Court and State Attorney. It is unclear as to why the information itself is necessary for the purpose of the criminal proceedings.

The appeal raises the question of whether the handling of the file was in accordance with the Estonian Forensic Science Institute Director's directive of 19 January 2012. The chamber does not see a reason to find the search report of 14.05.2013 and of 03.06.2014 inspection protocol as unreliable evidence. The appeal finds that, since the inspection protocol does not contain a detectable conclusion on the compliance of the hash code of the object under consideration, it is not possible to reliably validate the authenticity of the data. The integrity of the files that were seized have been demonstrated in the present proceedings, despite the flaws of the protocols. The appeal does not contain any allegations of why these statements should be considered unreliable.

Pre-image resistance means that it is not possible to derive the input only from the output of the hash value. Second pre-image resistance means it is difficult to find another file with the same content that would give the same output. The appeal alleges that it is possible to provide appropriate content to a file without changing the originally calculated MD5 hash value. The minutes of the county court hearing do not show that the individual had demonstrated changing the file for which the hash value had been calculated beforehand.

The circuit court finds that there is no evidence in this case that the hash value of the image file has been matched in any other way than described before. In order to attack a software integrity protection or code signing scheme, the attacker must be able to manipulate the files before they are hashed and signed.

1.3.4. Slovakia

Digital forensics seeks to answer "what," "why," "how," "who," and "when"-type inquiries. This process involves numerous parties with diverse interests, levels of expertise, and roles. Forensic experts are necessary to satisfy legal criteria. The capability to seize digital evidence is followed by the difficulty of convincing attorneys to comprehend the data. This paper's primary objective is to examine the various aspects that influence the courts' ultimate decision when IP addresses are used as evidence [219].

Analysis can lead to the identification of gaps in the use of digital evidence, which can subsequently result in legislative action. This paper supplements studies that have primarily focused on qualitative analyses of accessible legal and policy texts that constitute the basis of state responses to the rise of cybercrime. There are numerous studies that describe the particular and peculiarities of legal requirements in various countries. Frequently, the intricacy of the topic is emphasised in studies concentrating on individual nations. Complex comparative studies are rather uncommon and are frequently authored by specialists under the auspices of international organisations.

Even in nations where there is a lack of robust and formative case law in the area of digital investigation, a broader comprehension of judicial procedure could give valuable insights. Whether or not IP addresses should be considered personal information, and if so, under what conditions, is a hotly contested issue. Previous authors have considered the possibility to identify a person based on their IP address and on the functional distinctions between IPv4 and IPv6 IP addresses. The concept of IP address as it relates to its capacity to identify a specific individual went through various stages.

These eras were determined by the development of the Court of Justice of the European Union's jurisprudence and technical progress (IPv4 vs IPv6, rise in use of proxy servers). A lack of best practises has led to inconsistency in the transmission and receiving of requests for mutual legal help. Some of the highlighted concerns involved legal requirements and the interaction between attorneys and digital forensic specialists.

Using an external GIS service, all non-anonymized IP addresses were enhanced with spatial data (such as latitude, longitude, nation, internet service provider, and time zone). The researchers evaluate the significance of individual characteristics and their explanatory capacity with regard to the court's verdict; and use logistic regression to examine how various sorts of evidence contribute to the court's ultimate conclusion.

Using an example, the authors demonstrated that there is a strong association between the IP address assigned to a device and the device's specifications. With a correlation coefficient of 0.18, there is a strong relationship between a device's specifications and the IP address time stamp requirements. This association reflects the court's propensity to first determine the device in question and only then consider who had access to it (whether it was the defendant or other people). The greater the variety of evidence shown, the greater the likelihood that the defendant will be found not guilty or that the civil case would fail. The authors have concentrated on the ability of building profiles for the investigated judgments based on the many attributes stated in the technique.

The decisions evaluated in this study were those that involved reasoning, and they were analysed using the clustering technique. The results lead to the classification of the investigated decisions into four distinct groups. Decision clusters are characterised by the high frequency of adding IP address timestamps in the decisions (71%) and the greater specificity of the defendant's relationship with the device (39%). The IP address is used in 13% of court rulings, with the highest chance of assigning the IP address to a person (13%) - without providing further information, such as timestamps (in only 9% of cases). This cluster is characterised by the high likelihood of using multiple types of evidence, including documentary evidence (93%) and expert opinions (57%) as well as witness and witness testimony (39%).

The anonymisation of 'standard' personal data should not present a challenge for the courts, given that the nature of this information as personal data is commonly recognised. In other situations (6 rulings), however, the defendant's name could be located. This is due to the fact that the individual responsible for the anonymisation procedure made a mistake and neglected to anonymise these records. Login information was the most prevalent online identifier (included in 69 choices) (e.g. account names for social media websites, forums or other pseudonyms). Email addresses were the second most frequent online identifier after usernames (present in 26 decisions).

Other online identifiers were an ICQ number or a customer-assigned ID number (1 decision), among others. Not every decision that was analysed contained an online identifier other than an IP address. In 126 of the studied choices, anonymisation did not take place. This is because there is a disparity between how 'law in books' views IP addresses (IP address as personal data) and how 'law in action' treats them ('law in action'). Other than a hypothetical error during the anonymisation process, a common element that would support this strategy was unable to be identified.

In the analysed decisions, no jurisdictional concerns were examined since the court is not compelled to assess the potential of a change in jurisdiction based on the assignment of an IP address to foreign internet service providers (ISPs). The analysis of non-anonymized IP addresses also yielded intriguing information regarding whether courts in the Slovak Republic differentiate between static and dynamic, public and private, or IPv4 and IPv6 IP addresses. The public IP addresses (derived from the non-anonymized IP addresses) were often the IP addresses of Internet service providers. A public IP address assigned to a server providing a service could also be located. This may be relevant in terms of privacy and the protection of personal data. None of the studied choices provided for this distinction between IPv4 and IPv6 IP addresses, as they were all IPv4 addresses.

The research of the courts' decision-making process revealed interesting dependencies in the dataset. The most startling finding was that more evidence increases the likelihood of acquittal or civil action failure. According to the in dubio pro reo concept in criminal law, the court needs more proof to prove guilt.

The data also reveals that courts' IP address evidence practise is flawed. Courts assign IP addresses to people even though they identify devices. Decisions rarely specify a device or consider other people with access to it besides the defendant. It is recommended that IP address evidence should be standardised in court proceedings, especially criminal ones, to solve those difficulties.

For the second study goal, IP address anonymisation may still be a problem for courts, as their approaches vary. There was no standardised anonymisation and standardising method.

The authors found that their analysis provides investigative insights into forensic examination. The findings can be used in court processes to suggest evidence to be implemented, benefiting all parties. In criminal procedures, prosecutors and investigators should focus on connecting the IP address to the person by specifying a device to which the IP address was assigned. Directly assigning the IP address to the individual without identifying the device may fail to prove one's case in court. The four categories of the court's decision-making process may also help parties prepare their strategy for the procedures, such as the evidence to be executed, which may improve the processes.

2. Management and quality

Management and quality are intertwined in any setting. Therefore, to arbitrarily separate the two is a fraught activity. This section covers some of the publications that have examined management and quality assurance in digital evidence.

The demand for digital forensic science capabilities as part of many criminal investigations worldwide is great, and this trend shows no signs of imminent change. The increasing digital footprint of individuals means an increasing digital forensic science remit and mounting pressures and backlogs of forensic units tasked with processing digital devices. Arguably, some regions may only just be beginning to recognise the value of digital evidence to criminal investigations, and therefore maintain underdeveloped infrastructure in this area of forensic analysis. There is an acknowledgement of the importance of digital forensic science and the need for further and sustained investment. Planning is required to explore how existing digital forensic science services can be streamlined and used in both an efficient and effective way, without consequence to the quality of its work.

Infrastructure development should be considered a long-term investment and project for digital forensic science, where In the short-term, consideration of how existing infrastructures can be used to best cope with demand is required. Law enforcement digital forensic science units should consider a 'Service Level' approach for the allocation of their resources. It is suggested that doing so provides clients with both an understanding of capability, and the opportunity to select an appropriate service which matches their investigative requirements.

Criminal inquiries are often informed by the examination of any digital data associated with or attributable to a suspect. Given the value of digital evidence, the first responder now carries increasing importance to the success of any given inquiry. Efforts must be made to support first responders as they evaluate any digital presence at a scene. A key area identified for assistance lies with decision-making by first responders with regards to digital evidence and its potential value to a given inquiry. This includes both the identification of any digital devices, and the unpinning decisions and processes taken by the first responder to determine the investigative worth of the device and its subsequent priority to the inquiry.

2.1. *Management of digital evidence capability*

2.1.1. *Organisational strategy*

In July 2020, the Digital Forensic Science Strategy was launched by the National Police Chiefs' Council, which had been jointly developed between the Council, Transforming Forensics, the Forensic Capability Network and the Association of Police and Crime Commissioners [220]. The foreword states:

> "Digital Forensic Science sits at the heart of delivering justice in the 21st century, spanning the entire criminal justice system, from crime scene to courtroom. It shapes policy, offers a range of capabilities that better enable us to counter new and emerging threats, and is central to achieving our shared outcomes around reducing crime and increasing public safety."

In recent years, the use of digital forensics by law enforcement has skyrocketed. However, police response has been delayed, fragmented, and piecemeal. This strategy outlines how these difficulties can be confronted. To develop a justice system that satisfies the public's expectations in the digital age while simultaneously satisfying requests for more efficiency, every aspect of digital and specifically digital forensics differently must be approached differently. The strategy for digital forensics in England and Wales is a framework for achieving the step-change in the use of technology that is recognised as necessary to offer the world-leading level of service that the public expects. It outlines a strategy for achieving police goals by 2025 and establishes the groundwork for a system that will allow the swift and effective response to threats.

Digital forensic science - the examination of digital evidence to aid in investigations and prosecutions - was originally a specialised field, but is now widely accepted. Over ninety percent of all crimes have a digital component, and as society's reliance on technology grows, the need of digital forensic science will only increase. A strategy has been developed to address the enormous opportunities and corresponding problems that this situation poses for law enforcement.

Utilization of digital technology has led to an exponential increase in the demand for digital forensic analysis. In the past three years, demand has increased by 11–16%, and this trend is expected to continue. Investigative backlogs and delays affect victims, witnesses, and suspects. They also enhance the risk of harm by delaying the prosecution of criminals.

Digital forensic examinations constitute a complex issue in and of itself. There are more sorts of devices, end-to-end encryption, and data format variants. The Internet of Things is expanding rapidly, necessitating the development of new digital forensic techniques. However, many Digital Forensic Units have limited research and development capabilities, and very few have access to external research funding. The police must proactively collaborate with the government to ensure that the legal and ethical frameworks upon which these activities are based are appropriate for the digital age.

The strategy also addresses several other pressing issues:

Digital forensic services have grown organically over the last twenty years, often operating in relative isolation. Developing digital forensic from 'cottage industry' to key investigative support function has happened outside many forces' corporate IT arrangements, therefore lacking clarity over funding and management. A lack of coordination between forces limits policing's ability to build strategic relationships with academia and industry. Less than 20% of processes requiring accreditation have achieved it, and lack of capacity makes it very challenging for forces to achieve quality accreditation. Managing and weeding legacy data puts a significant burden on forces and exposes them to compliance risks. Legacy data generated or seized for, or as a result of, past forensic examinations is stored in various formats.

Together with forces and partners, Transforming Forensics and the Forensic Capability Network will expand upon the three-tiered strategy outlined by the Digital Forensics Portfolio Board. This tiered concept will be implemented nationwide and will include national, regional, and local components. The service will be developed with continuous development at its core, utilising an adaptable system with reach beyond policing. The Forensic Capability Network Commercial will expedite interactions with market-wide vendors.

There will be more collaboration with consumer device, technology, and internet service companies in order to inform and advance digital forensic analysis skills. Science and Research and Development (R&D) must be centralised for digital forensic science to continuously progress. One or more innovation centres to consolidate R&D and specialised competencies will be constructed. Transforming Forensics and the Forensic Capability Network will establish the expectation that all digital forensic work is founded on strong scientific principles. It will ensured that digital forensic science provides the greatest potential assistance to the criminal justice system by maximising the value of the data held by law enforcement.

A national digital forensic data architecture that is compatible with the recommendations of the National Police Data System (NPDS) will assist in meeting the enormous data volume and complexity challenge. In collaboration with the College of Policing (CoP), the Forensic Capability Network Science intends to professionalise digital forensic science roles. This term must be expanded to cover all personnel whose duties involve digital forensic science, including those who use automated tools and workflows. A continuously updated knowledge base will provide quick and simple access to developing learning and novel methodologies. The Forensic Capability Network strives to assist law enforcement in maintaining adequate operational methods and governance, as well as addressing public concerns around ethics and trust.

The government will seek to guarantee that all digital forensic science activities are supported by clear authorities and nationally agreed-upon regulations and procedures. From the crime scene to the courtroom, quality standards, efficacy, and efficiency will be enhanced.

2.1.2. *Service level agreements*

Digital Forensic Science (DFS) should be considered a service which is both commissioned and deployed. As a service, DFS must ensure that it is in a position to fulfil the requirements of its clients in an effective and efficient way. It is argued that this capability can be broken down into levels of service, which can be offered by the DFS unit to the client. The use of service levels should not be seen as corner cutting or quality-degradation in regards to the examination product offered by a DFS unit. Instead, it is about recognizing the diverse needs of clients and their investigation requirements, and deploying a service which is both resource efficient whilst delivering a suitable product (in the form of case/device processing) - achieving maximum benefit for the criminal justice system [221].

Service levels may exist informally within DFS units and be deployed autonomously when assessing the needs of the client in any given case. Service level structures prevent resource-waste and mismanagement, allowing a more strategic resource deployment. This work suggests that an assessment of DFS unit service deployment is carried out. It is suggested that the defining of formal service levels brings standardization of service across all D FS units.

It is suggested that defining service levels for deployment in DFS units offers a number of operational benefits which should be explored.

Assessing and agreeing upon a level of service ensures that the DFS unit understands their obligations in-terms of service delivery, and the client acknowledges the product which they have commissioned. The use of appropriate service levels also helps to guide both the practitioner and client in their assessment of case requirements. The act of choosing a service level is not a one-time only decision. Any chosen service level can result in the escalation of a device to a more comprehensive level if it is required. It is argued that service levels are also a mechanism by which those in managerial positions in DFS units can assess case-allocation practices to their practitioners.

The proposed DFS service levels can be considered hierarchical in terms of their deployment and resource allocation by the DFS unit. The higher the numerical service level, the more complex and resource consuming the service is deemed to be. For example, consultation under 0.1 will likely concentrate on the development of a DFS strategy, in line with any given background case information/intelligence. A 0.2 consultation concerns non-standard devices, where their functionality may not be thoroughly understood by the client. An assessment of the DFS unit's capability to examine standard devices is less likely to be a point of concern.

A consultation concerns exploratory research, testing and capability assessment regarding a device. Under Service Level 1, the client assumes responsibility for the review of data and making of investigative decisions. Sub-Service Level 1.4 provides access to a 'forensic kiosk' where the client can handle, extract and interpret data themselves. Data screening can be considered the process of refining the data sample size extracted from a device through the use of defined criteria, designed to target potentially relevant content. At Service Level 2, attempts will be made to remove redundant data from the final dataset which will be supplied to the client.

At Service Level 2, the client assumes responsibility for the review of data and its interpretation. At Service Level 3, the use of device triage and preview examination techniques are offered. Preview examinations simply 'take a look' at a device and assess any initial low hanging fruit information. Sub-Service Level 3.3 involves the preview of a specific event which is believed to have occurred on a system. This narrows the scope of the service to a specific region of a device or log-type which can be quickly identified, verified and assessed in terms of whether further work is required.

A limit to the number of variables which can be searched for prevents significantly extended processing times. A Service Level 4 standard device examination and investigative report is what can be considered the anecdotal 'full examination' of a device. The use of this Service Level should be reserved for when there is an actual need for it. Expert evaluation is required at Service Level 6, where a practitioner is requested to provide an assessment of the strength of the findings in the context of alleged circumstances. Expert evaluation is considered the most resource-intensive and complex level of service which a DFS unit can offer.

It is acknowledged that defining service levels forms only half of the challenge of effective resource management and allocation in the DFS unit setting. The remaining issue to overcome lies with the development of a process which aligns a client's requirements to a service level effectively. It is suggested that service level allocation is a task which could and, arguably should, be conducted by the client in some cases. To do this requires engaging with the proposed Service Level Allocator decision model. Clients are asked 'are you able to identify a specific 'digital event' which has occurred on the device(s) which you consider to be the focus of the investigation?'.

This attempts to establish whether the client requires a target investigation, focusing on a specific event. Clients can be directed to a Service Level 0 consultation as they do not understand the digital aspects of the offence in enough detail to select a service level. Clients can target their investigation at a specific 'digital event', 'type of file' or 'software application/package'. If they are able to do so, then a Service Level 3 'Preview/Triage Examination' is selected. This may be sufficient to determine the value of the exhibit which is submitted for investigation to the case in question.

However, some results may require more in depth scrutiny where no service level is required. An investigation can be confined to files or data of a specific 'type', and the client 'understands what these files/data are'. If no screening criteria can be applied, but the client considers themselves competent and willing, a Service Level 1 'Data Extraction & Packaged Data (For Third-Party Review)' is selected (review of all extracted data). Service Levels 1–3 are all possible, dependent on the client's competence and willingness to review. It is acknowledged that it is difficult to place exact time limits on these where the time supplied for these processes should be dynamic and allocated based upon the data-source size and the number of search variables defined.

However, it is suggested that base-line figures be determined and adhered to as best as possible in order to adhere to the principle of service level delivery. DFS units should also assess the value of 'Service Level Metrics' (SLMs). SLMs can be used to provide clients with an idea of the service times offered by a DFS unit at each service level. There are now roles which sit on the periphery of DFS which may have an expectation and/or potential to engage with the interpretative process of digital data.

2.1.3. *Readiness and maturity*

Digital Forensic Readiness is an anticipatory approach that resides within the digital forensics domain. It seeks to maximise an organisation's ability to collect digital evidence while minimising the cost of such an operation. Most existing models on security are reactive rather than proactive. Digital Forensics Readiness Commonalities Framework is a framework that specifies forensic readiness by considering the interconnectedness of domains and subdomains. This framework would align with the strategies of climate change adaptation and sustainability [222].

The framework is presented in the form of a wheel with the Legal Involvement domain as the axis. It has been proposed that digital forensics laboratories should strive towards ISO17025 certification. This validates that a laboratory is proficient at constructing technically valid data and results. The successful design of the policy domain provides a foundation for the consideration of the user's compliance with the stated Digital Forensics policies. A cost/benefit analysis must be done before an investigation is commenced in order to determine the feasibility of such an investigation.

There is need for constant monitoring after training to understand the return on training investments. The framework ensures that judicial, regulatory and other laws within an organisation's realm of operation are considered and incorporated in the overall Digital Forensics Readiness strategy. An assessment model that is utilising all the components of Digital Forensics Readiness Commonalities Framework, strives to satisfy the goals and objectives of Digital Forensics Readiness and security incidents. The resulting maturity model will provide an opportunity to contribute to the enhancement of digital forensics benefits and security incidents.

An unavailability of Digital Forensic standardization has resulted in many works showing procedure and frameworks that are too technology specific. With little emphasis on policy domains or practitioner input, an integrated conceptual digital forensic framework has been proposed. Because of these technology specific applications, this paper attempts to produce a framework applicable to a variety of technologies and industries. One study has examined the impact of cloud forensic readiness on security and found an overlap of Digital Forensics Readiness and security as a converging area. Another study found prevalent incidents occur through hackers trying to break into the computer network.

These incidents have been attributed to an inadequacy of traditional digital forensic frameworks that can be used in tackling cybercrime in the public cloud. The goal of implementing Digital Forensics Readiness is to collect digital evidence targeting the potential crimes and disputes that may adversely impact an organisation. Successful implementation helps organisations to limit the number of incidents that will occur by selecting and implementing a set of controls, maximise the potential to use comprehensive digital evidence and minimize the cost of forensics during response. Assessment of Digital Forensics Readiness as part of information security has been discouraged in some organisations. Information security neglects the magnitude of developing procedures and controls that will have successful investigation outcomes. It has been found that forensics is applied to less than 30% of business security incidents. This implies that assessments are potentially based on a small percentage of security incidents. Such assessments will present a dubious view of the state of digital forensics.

In the twenty-first century, organisations without a method for measuring their security mechanism and forensic readiness run the risk of being exploited by economic crime. This study analysed the existing literature to comprehend the Digital Forensics Readiness structure and how such a structure can be used to create a maturity assessment model. A qualitative technique was used to assess the Digital Forensics Readiness structure with forensic practitioners once the structure emerged from the literature. The framework was formed by the respondents and the domains were used to develop a maturity evaluation model. Participants were presented with two techniques, but responses recommended a third approach, a combination of check list and qualitative narration.

The illustration (in the original text) [223] depicts the refined structure (domains and subdomains). Financial services organisations that invest in Digital Forensics Readiness will find the picture valuable, since it depicts the extent and structure of Digital Forensics Readiness. The diagram depicts the extended Digital Forensics Readiness Commonalities Framework v2, which resembles the Deming lifecycle: Plan, Do, Check, and Act. This is an updated version of the Digital Forensics Readiness Commonalities Framework that was produced as part of this research. This framework will be presented to the academic community and forensic practitioners. This framework complies not only with accepted industry standard principles and recommendations for forensic readiness, many of which are outlined in the report on Forensic Readiness, but also with the proposed NIST cybersecurity framework. This study employed the check-list method, which was favoured by the majority of participants.

Organisations must comprehend their forensics readiness capabilities in order to attain and maintain a state of “readiness.” A company that is aware of its preparedness status is in a better position to oversee and implement interventions aimed at attaining a maturity grade of five. Future iterations of this enhanced model should incorporate the viewpoints of more practitioners who have dealt with large incidents and who may offer more insight into the forensic readiness requirements.

2.1.4. *Decision support for first responders*

The Device Evaluation and Prioritisation Scoresheet (DEPS) is designed to support the transparent capture of first responder decision-making with regards to digital devices at the scene of an inquiry, and their assumed priority to a given inquiry. DEPS is aimed at supporting first responders in front line policing roles, rather than crime scene investigation and digital media examination positions. ‘The scene’ can be considered any immediate space in which a first responder finds themselves as part of an inquiry. The DEPS methodology is designed to become part of the inquiry paperwork bundle [224].

The DEPS methodology is offered as a structure to support first responders as they conduct an assessment of any investigative opportunities which may exist at a given scene in a digital form. It formalises both the steps a first responder must take, and the questions they should address in order to determine the investigative priority-value that a device has to the inquiry. The purpose of SCORE is twofold. First SCORE operates as a contextual reminder for first responders at the scene of an inquiry, encouraging consideration of the five categories of ‘digital investigative opportunity’ which may exist. It is important to note that digital evidence can exist on a range of devices, where SCORE helps to encourage first responders to not evaluate devices for what they are, but for what value they may hold.

Digital device content can now provide support for law enforcement as they seek to ascertain and understand the circumstances which may be relevant to a specific investigation. First responders must assess for the presence of a digital device, and consider the context in which it may add value to their investigation. The SCORE approach provides transparency as to why a device was considered as part of any inquiry.

For every device subject to the SCORE process, the first responder must proceed to address six ‘ranking’ questions which are designed to assess the ‘priority’ of the device in relation to the inquiry. Each question carries a numerical weight, where a combination of all six places the device within one of the three ‘prioritisation ranks’, namely low, medium or high. A device which is considered a primary line of enquiry must contain information on it which is either itself the product of a suspected offence, or the information is a leading source for an inquiry. A first responder who selects ‘unknown’, acknowledging that they do not know the reason as to why they need access to the data on the device is prompted to ‘EXIT’ the DEPS process. A first responder must consider data on the device to provide context or supplementary details regarding any potential offence.

Not all first responders will be confident to technically evaluate any technological devices at a scene. It is necessary to establish what beliefs regarding the potential functionality of any device that they maintain. First responders can respond in the following way: . A first responder acknowledges that they have no understanding of the device and its function. They must determine whether any potential data may be lost if excess time is taken to capture it.

If there are no apparent risks for data loss/destruction, then prioritisation should continue. But where there is a real risk of data loss if immediate (or known to occur in a specific time frame or event) action is not taken, then consider whether device prioritisation is appropriate. Question 6 requires the first responder to address - ‘what role is the device believed to play in the inquiry?’. This question asks whether the device may contain data which is ‘exculpatory’ for a given suspect (10) or ‘inculpatory’ (1) or the role of the data is yet ‘unknown’ (5).

‘Device potentially of medium-priority to inquiry’: . For a device to fall within this rank, it must have collectively scored between 11 and 21 across all six categories. Devices in this rank are considered of moderate priority in regards to the inquiry. Prior to device seizure, first responders should assess whether at-scene device interrogation/assessment is a viable option. DEPS is designed to determine the level of priority that a device may have to the first responder’s inquiry.

Although it is important to encourage critical evaluation at scene as to the need to seize a device, recognition of the risks associated with this process are noted. DEPS proceeds on the assumption that in many cases, device seizure will be common practice for those that fall within its definition. DEPS unblinds the decision making behind a first responder’s device seizure by collecting and recording their responses to core questions which underpin a decision to seize, or not. High-priority ranking devices in DEPS which are seized may be placed higher up in a case-prioritisation matrix meaning the device will be examined quicker.

Consider a child abduction inquiry where the first responder identifies the child’s laptop and considers that it may contain relevant communication data. They may know the device is capable of doing the tasks and retaining the data types they may consider relevant to the inquiry. However they may be unsure as to whether this data exists upon it (weighted ‘5′) or if it has been retained at all (weighted ‘1, 2, 3, 4). The DEPS methodology is an extension of the first responders workload at-scene, and may enable any devices submitted for examination to be correctly prioritised. The use of the ‘unknown’ rankings prevents devices from being under-prioritised due to not fully understanding their role.

The model does require all those involved in an investigative team to adopt such an approach if it is to make an impact. The receipt of a DEPS along with any submitted exhibit should be considered by first responders as evidence to support their decisions regarding how they intend to prioritise the case for examination. It is hoped that it offers consistency in the way case prioritisation in-lab occurs, leading to quick case outcomes. However this raises the concern that first responders may inflate their DEPS submission in an attempt to increase the priority and therefore speed at which their exhibits are examined.

2.1.5. Digital forensics as a service

In 2014, the Netherlands Forensic Institute conducted an analysis of the typical digital forensics investigation procedure and created Digital Forensics as a Service (DFaaS). The primary objective is to provide a service for the forensic processing of large volumes of digital data. To collaborate and share information efficiently and effectively, an open and expandable platform is needed. Digital content is uploaded to a central platform and processed using a set of tools in DFaaS. The outcomes of applying these instruments to the investigated data are kept in a central database [225].

Using the platform's Automated Programming Interface (API), these results can be accessed, filtered, and aggregated in numerous ways. In 2015, HANSKEN was introduced, the next-generation implementation of the concept, which is comprised of multiple interconnected components. The HANSKEN platform is used in over one thousand cases, including criminal cases with over one hundred terabytes of raw data and over one hundred million detected traces. In 2018, the Dutch Prosecution Office seized 3.6 million encrypted messages from Canadian mail servers that were used for secure (PGP) BlackBerry phone-based communication. The primary technologies upon which HANSKEN is based include:

- Java powers Hansken's main platform and extraction tools.
- Hansken uses Apache Zookeeper for configuration, naming, and distributed synchronisation of its services. https://zookeeper.apache.org
- Ceph, Hadoop HDFS, and others are supported by the data store. Ceph.io, Hadoop.apache.org
- Hadoop MapReduce distributes extraction. https://hadoop.apache.org
- Kafka tracks extraction progress. https://kafka.apache.org
- Elasticsearch stores trace meta data and keyword indices and powers the query, filter, and aggregation engine. https://www.elastic.co/products/elasticsearch
- Cassandra stores user preferences and project administration. It caches and stores user-added trace data. https://cassandra.apache.org
- Knockout, AngularJS - The current GUI uses Knockout (Tactical UI) and AngularJS (Expert UI). Knockoutjs.com, Angular.io
- NGINX hosts these APIs and additional documentation. https://www.nginx.com
- Offline OpenStreetMap provides graphical map data. https://www.openstreetmap.org
- GroupDocs.Viewer (commercially licenced) converts source data into HTML5 to display trace contents. GroupDocsViewer.github.com •fusepy, FUSE—The Python API (covering the REST API) supports Hansken disc image mounting using fusepy and FUSEhttps://github.com/fusepy, fuse.sourceforge.net
- Hansken uses Keycloak for user authentication, which supports single sign-on with numerous popular identity suppliers. https://www.keycloak.org
- OpenLDAP allows user authorizations. https://www.openldap.org
- Grafana monitors these services and tools. https://grafana.com
- Atlassian suite—to plan, track, test, release, and deploy Hansken products using Atlassian. https://www.atlassian.com
- Ansible Kubernetes automates deployment on changeable hardware. Hansken may be Kubernetes-containerized. Third-party systems underlie these deployments. Ansible.com, Kubernetes.io

The development organisation of Hansken is comprised of seven teams of around five individuals, each with a variety of tasks and specialities, including developer, forensic specialist, architect, operator, tester, and system engineer. An operational platform is intended for investigative reasons, not as a repository for evidence. The use of backups and archives is crucial to digital forensic investigations. HANSKEN facilitates the archiving and backup of user-added traces and annotations.

HANSKEN is intended to communicate and implement advancements in service-based, automated digital forensics. HANSKEN orchestrates a standardised procedure for a large number of specialised instruments to extract traces from system-entered data. In accordance with the development tenet of not reinventing the wheel, the project concentrated on expressing findings with existing software tools. There are numerous reasons why traces may not be discovered during a manual or automated analysis. To offer insight into the automated procedures that led to the reported traces, each trace's attributes, transformation relationship, and location are maintained.

To provide an additional software error-checking mechanism, HANSKEN counts the number of tools that are executed to evaluate a certain input. The origin of traces is crucial for their admissibility in court. This includes the chain of evidence (the relationship between the traces and the source material) as well as the procedure that led to the traces. HANSKEN provides as much information as possible regarding their internal operations.

During the extraction of traces, filters can be used to identify and flag suspicious traces. If traces are not tagged but are discovered to contain privileged communication during an investigation, the API and graphical user interfaces provide functions to conceal them. These functions assist the Prosecution Office's stated and approved processes. Digital forensics as a service (DFaaS) provides developers with access to investigational data. In the Netherlands, DFaaS installation teams typically consist of four to six members.

Digital specialists can now focus on reading and evaluating important data rather than working as data processors and transfer hubs. They must be persuaded that an agile approach to DFaaS meets their needs and specifications. A flawed or inadequate implementation might increase resistance and impede concept acceptance, hence diminishing the benefits immediately. Continuous development of digital forensics software makes it possible to meet the stringent requirements placed on digital forensics software, but may hinder investigations. Due to the fact that DFaaS implementations depend on numerous underlying technologies, updates and upgrades of these systems must also be considered.

When numerous organisations with relatively divergent perspectives on the perceived benefits are involved, it is challenging to schedule new features based on their benefits to end-users. A DFaaS platform may not be able to keep up with the requirements of each new criminal investigation or adapt to unforeseen shifts in the field. The expansive nature of digital forensics technologies can enhance the possibility for problems, but this emphasises the significance of professional culture and education. To eliminate confirmation bias and omission of alternative analysis, people must be trained to assess data critically and digital forensics experts must be consulted. On many times, the use of HANSKEN for forensic investigations has been discussed in Dutch courts.

DFaaS platforms must support worldwide standards for storing forensic data and portraying digital evidence. Focus should be placed on centralising data sharing and automating the trace extraction procedure (data structure analysis). This is a necessary skill for managing digital evidence in a criminal investigation. Digital evidence may be relevant to other investigations, including those conducted by other organisations or governments. For the receiving party to use such material as legal proof, it is crucial that the origin and presentation of the evidence are properly documented. Since 2016, a community-wide ontology titled Cyber-investigation Analysis Standard Expression has been in development to represent digital evidence (CASE).

The design of HANSKEN makes it possible to incorporate the output of third-party tools written in different languages. AFF4 and CASE formats provide Python-based tools for automating the management of stored data and evidence which facilitates their integration via an API. Investigations in digital forensics frequently rely on a collection of traces and the relationships between them. HANSKEN enables declarative domain-specific language (DSL) descriptions of binary data structures. This implies that the forensic expert just needs to specify the structure of a file format, protocol, or memory layout.

Hard and soft relationships between digital traces must be serialised on DFaaS platforms. Relations can take a variety of forms, ranging from a single integer indicating the entirety of a data set to a matrix displaying the relations between each trace and multiple or all other traces. As many of these connections can be resolved on a hit-or-miss basis, they lend themselves nicely to automation. Experts in digital forensics must frequently repeat tests to reach forensically valid conclusions. Using methodologies for behaviour-driven development (BDD) and automated testing of user interfaces, experiments can be captured and replayed.

It is possible to generate reports by dragging and dropping customizable widgets, which function as templates. The Netherlands Forensic Institute is initiating an initiative to enhance and expand the DFaaS platform HANSKEN. This comprises the forensic applications and libraries that implement the data structures and trace extractions. The platform is open to forensic science institutes, universities (of applied science), and related cooperative research initiatives for study and development. Additionally, the community needs a shared communication platform and code repository.

DFaaS is a novel approach to digital forensics that necessitates an adaptable and flexible organisation. A DFaaS implementation always necessitates both software engineering and digital forensics expertise. Case investigators' access to digital evidence is the greatest advantage. Advanced training and intuitive user interfaces aid in mitigating this danger. DFaaS is all about knowledge sharing regarding digital forensics.

DFaaS provides granular insight into the operational expenses associated with managing digital evidence, which are difficult to compare to the present costs that are dispersed among organisations, teams, and individuals. Parts of the evidence review can be automated, particularly those that are basic or well-documented, such as clock validation. DFaaS is primarily concerned with decoupling digital forensic tasks. Others' knowledge can be more easily integrated into and related to the platform. This is hastened by enabling international data storage and evidence representation standards. A Tool Development Kit should be offered to better support and encourage the centralisation of information in DFaaS platforms.

2.1.6. Forensic advisor

Almost all forensic science disciplines are faced with the situation of increasing demands without the comparable increase in resources to service those demands. In addition, there is an increasing demand for speed and responsiveness driven by investigating agencies and the communities they serve. Digital evidence has been subject to that dichotomy more than most disciplines due to the rapid advances in technology and the rapid growth in evidence volume. The priority management process employed by most agencies is substantial and in many cases, increasing backlogs; rationing of capacity which involves delay, dilution, deterrence, transfer and termination of services [226].

At the same time, investigating agencies are increasing their own in-house digital evidence capability with little regard for scientific rigour and quality assurance. Typically, at a time when digital evidence is becoming more complex, an increasing amount of work is being diverted to less skilled operators who are using commercial products with inadequate training and insufficient understanding of the limitations of the tools they are using; the increased possibility of missing or misinterpreting evidence; and insufficient awareness to the values of forensic science, intelligence and privacy. Such decentralization often occurs in the absence of assistance from forensic specialists.

The inevitable decentralization can be transitioned with and guided by forensic scientists employing scientific method to manage digital forensic capabilities with a central source of knowledge in a distributed service model, which is strengthened by the presence of a forensic advisor. The forensic advisor will apply scientific reasoning to the evaluation of digital evidence and can provide structured scientific interpretation of the process and results.

Also growing in importance to investigative capability is forensic intelligence which fuses information across cases, organisations and borders which can then be applied to emerging, or as yet opaque, investigations. The forensic advisor is a key function in the development of forensic intelligence capability.

Quality assurance, particularly accreditation to ISO 17025, is critical to an effective and competent decentralization of digital forensic science. Unfortunately, the thorough and robust frameworks and processes described here are generally absent from cybersecurity incident responses which are growing in number and complexity. The responses to these incidents are primarily focused on containment and eradication which can overlook proper evidence preservation, handling and analysis, thereby compromising any subsequent legal action. Having to pay criminals in cryptocurrency ransomware attacks is a clear sign of deficient forensic preparedness.

2.2. Quality assurance

Digital forensics began as an ad hoc, task oriented practice performed by computer professionals with no formal processes, tools or training (Garfinkel, 2010). In recent years there has been an advance within digital forensics towards a more scientifically sound handling of the evidence. Like other forensic disciplines, and science in general, there are uncertainties, limitations, vulnerabilities, and potential for error. Digital evidence is perceived as reliable and correct by many in the legal community (Van Buskirk and Liu, 2006). This should be a concern when considering the results of a recent analysis of the quality management (QM) procedures in digital forensics performed by Page et al. (2018).

There are errors that arise from both technological and human factors within forensic science, including those related to lack of scientific data, research and rigor. These cross all forensic domains (as well as other expert domains) and can lead to wrongful convictions. Within the digital forensics domain, there has been a movement from perceiving tools and technology to greater acknowledgement of the human as an important instrument for examining digital evidence. A critical element is understanding where it may come from, and how to control and minimize it.

Despite the strive for automation, digital forensics (digital forensic) examination still struggles with limited resources, overreliance on tools and subjective opinions. Digital evidence is increasingly presented and accepted in courts without scientific validation of the digital forensic methodology or tools. While classical investigative measures are subject to strict limits and fair trial guarantees, digital investigations still lack quality assurance and accountability. There are no European minimum standards for digital evidence to establish and enforce scientific validation in digital forensics.

Inappropriate use of poorly tested technology undermines the right to a fair trial, as formulated in Art.6 ECHR [227], and threatens the presumption of innocence at an early stage of an investigation. Moreover, ineffective pre-trial and trial guarantees for defendants are not suitable to validate complex digital forensic methodology and tools and the suspect/defendant position to collect or challenge digital evidence in the criminal proceedings is weak. Overreliance on and inappropriate use of technology in combination with the weak position of suspects/defendants can lead to unequal treatment of suspects/defendants and lack of legal certainty in the judicial process.

Digital evidence is the result of scientific methodologies and tools which ensures that "its authenticity and integrity can be validated".

Digital forensics began as an ad hoc, task oriented practice performed by computer professionals with no formal processes, tools or training (Garfinkel, 2010). In recent years there has been an advance within digital forensics towards a more scientifically sound handling of the evidence. Like other forensic disciplines, and science in general, there are uncertainties, limitations, vulnerabilities, and potential for error. Digital evidence is perceived as reliable and correct by many in the legal community (Van Buskirk and Liu, 2006). This should be a concern when considering the results of a recent analysis of the quality management (QM) procedures in digital forensics performed by Page et al. (2018).

There are errors that arise from both technological and human factors within forensic science, including those related to lack of scientific data, research and rigor. These cross all forensic domains (as well as other expert domains) and can lead to wrongful convictions. Within the digital forensics domain, there has been a movement from perceiving tools and technology to greater acknowledgement of the human as an important instrument for examining digital evidence. A critical element is understanding where it may come from, and how to control and minimize it.

Digital evidence and its construction process are prone to technical and non-technical errors, which may occur randomly or systematically. Task-irrelevant contextual information has shown to be a significant source of biased observations and decisions in forensic science, including digital forensics. Forensic science disciplines with a high degree of interpretation and subjectivity involved in the forensic process have a higher risk of such errors. Error mitigation is necessary to prevent and detect errors in a criminal investigation. It is argued that the forensic community should discuss the risky nature of forensic science processes and enable dialogue around the management of risk. Errors should be viewed as a natural and unavoidable part of any process involving human decision-making. Implementing systems or measures for error mitigation is vital for preventing miscarriages of justice and is also an opportunity to enhance quality through systematic improvement and learning.

While a large proportion of the research within the digital forensic domain is concerned with technology, a few empirical studies have examined digital forensic practice. Previous studies found that the context significantly affected the observations of traces, but no biasing effect was found on the interpretations or conclusions. Digital Forensic practitioners were found to be inconsistent in their decisions on which exhibits to include or exclude; the capabilities of their tools influenced their decisions; tend to use categorical conclusions and strength of support conclusion types and that the conclusions addressed source, activity, and offence levels. They used a high variation of certainty expressions but did not explain their meaning or refer to a standardised framework. Several of the identified deficiencies in digital forensic reporting practices are shared with other forensic science disciplines.

The digital forensic practitioners and their organisations should implement effective investigative strategies to manage contextual information, maintain examiner objectivity, and control evidence credibility. There is little research on digital forensic practices concerning these issues, which is crucial for designing effective quality measures. A disadvantage of close cooperation is the risk of ‘forensic confirmation bias due to the exposure of task irrelevant contextual information. What is task-irrelevant context should be critically evaluated and decided on a case-by-case basis. A survey found that many submission forms encouraged the client to include case information but had no guidance on what to leave out.

Contextual information is only one of several identified sources of bias in forensic work. The data set that is analysed may also challenge the examiner’s objectivity. An evidence file from a smartphone will expose the digital forensic practitioner to a vast amount of task-irrelevant information, which may bias the examiner’s observations and decisions. The practitioner must apply adequate techniques to maintain their objectivity during the analysis to minimize bias. It is generally accepted that digital forensic tools may produce flawed results, and that error mitigation is necessary [228].

The reliability of investigative decision making (DM) by digital forensic practitioners is both paramount and concurrently has to be questioned. Arguably no room for investigative error exists, yet such mistakes are beginning to be noted. During the presentation of oral evidence to the UK Justice Committee, Professor Peter Sommer and Dr Jan Collie raised a number of concerns surrounding digital forensics. ‘Digital forensics units are quite good at keeping up to date with technology for extracting data and making copies, but they then pass the copies, largely uninterpreted, to police officers’. ‘Lack of resources is often used as an argument for not implementing quality standards. It is important to move away from thinking of quality standards as an optional add-on, and think of them as integral to the way to deliver quality forensic science’ [229].

Digital forensics practitioners remain vulnerable to human error, limitations of knowledge and general mistake. Fostering robust investigative DM can be a preventative measure against poor examination results. It has been found that digital forensic organisations fail to develop and support appropriate investigative decision making. As of yet, there are few formalised methods to support the practitioner with their investigative judgements. Establishing sufficient confidence is a crucial element of investigative decision making. A digital forensic practitioner must possess sufficient confidence in their interpretation of any digital evidence before it can be reported. This work provides the Digital Evidence Reporting and Decision Support (DERDS) framework to support digital forensic practitioners.

Digital forensics is one of the newer sub-disciplines of forensic science. A lack of standardization and consistently applied examination techniques has led to varying levels of digital forensics casework. Cost and resourcing cuts have also led to concerns with the work produced by this field. Addressing many of these issues will take time, requiring sustained investment and development of infrastructure, knowledge and services. A digital forensics practitioner will sift through a digital device for potentially relevant information which can support the criminal justice system [230].

This process requires the practitioner to determine the relevance of digital information and present content that supports the accurate reconstruction of events. Any misinterpretation of information at this stage creates uncertainty, inaccuracies and ultimately prevents any reported information from the practitioner from being relied upon. The interpretation phase of an investigation poses a challenge to the practitioner, and there is little formalised guidance and support for this task in digital forensics. Assistance to practitioners can be provided by the Verification of Digital Evidence (VODE) framework to support their interpretation of newly encountered, undocumented digital artefacts and data. The work forms the first of two pieces concerning measures for quality assurance in digital Forensics investigations and will bring together four frameworks which are designed to support the investigatory process.

The need for knowledge sharing in digital forensics has been mooted by academics, researchers and practitioners for over 15 years. CODE is a proposed framework for the sharing of ‘new knowledge’, as discussed below. A practitioner who shares this new knowledge is providing the following potential benefits: The sharing of newly discovered accurate knowledge by a practitioner provides a benefit to those who this content is shared with. Where a certain digital trace can be consistently interpreted, this helps those who are outside of digital forensics but still engage with digital evidence are part of legal processes (criminal justice system employees, law enforcement officers) to understand the meaning of this content [231].

By sharing this information the application of its meaning by other practitioners is encouraged when they encounter the same digital trace (and the interpretation is applicable given all the facts of the case) This helps to uphold quality standards and prevents divergent interpretations from occurring. Sharing newly discovered knowledge allows peer review to occur. In an ideal world, any shared knowledge is robust, yet human error can still occur. Shared data and the associated test methodologies undertaken by a practioner can be scrutinised by others in the digital forensics field with suitable expertise. There are multiple benefits to sharing knowledge on a wide-scale consistent basis.

The importance of trust in digital forensics has received little emphasis. In the United Kingdom, for instance, the Forensic Science Regulator encourages all forensics disciplines to be grounded in "sound science." This emphasises the necessity for transparency regarding limitations and/or methods. Trust is one of the factors that unquestionably affects the dependability of any research. Digital forensics may not explicitly account for trust manifestations throughout investigations [232].

The replacement of this attitude with a presumption that computer evidence is credible unless shown differently may be a contributing factor. There is a possibility that this presumption will be replaced by a "third approach" in which courts actively evaluate whether particular evidence has been materially altered by computer mistake. The profession of digital forensics is not the only one that must face the problems posed by the question of trust. Zero Trust, a security model and mindset that allows sensitive data, systems, and services to be better secured from cyber threats, is a prevalent paradigm in network security. This is accomplished through design concepts and tactics that aim to reduce the reliance of network defenders on trust by enhancing the verification of network interactions, such as authorisation events. Recent papers highlight the significance of Zero Trust to the future of network security; consequently, it is worthwhile to investigate whether the ideas can be applied more broadly.

2.2.1. Human factors

The empirical survey data for this paper were collected during the digital forensic experiment (Sunde and Dror, 2021) [233], which was outlined in Section 1. After completing the experiment, digital forensic practitioners completed a questionnaire ('Part 2 survey') with nine questions concerning how they approached the analysis. Their responses were analysed in a combined qualitative-quantitative approach [234].

Digital forensic practitioners were asked what they thought had happened in relation to the reported incident. The qualitative analysis showed that hypotheses, scenarios, or explanations were recurring themes in the responses. Among those who did not have an opinion, the analysis found two distinct approaches, which may be conceptualised as active and passive mind-sets. 36% of participants in the digital forensic experiment had only one scenario in mind when starting the examination, which could lead to confirmation bias. Confirmation bias is a tendency to look for information that confirms the favoured hypothesis and overlook or explain away information that contradicts it.

The 'innocence' and 'strong guilt' contexts lead to a one-sided starting point of the analysis for many of the participants. Number of hypotheses does not indicate whether they facilitate a fair investigation safeguarding the presumption of innocence (European Convention of Human Rights, article 6(2). The fact that almost half (45%) of the participants considered multiple hypotheses indicates that many were aware of the risk of biased and one-sided examinations. Due to its relevance for maintaining examiner objectivity, the proportion that included an innocence hypothesis was explored.

Survey of digital forensic practitioners asked if they used techniques to safeguard their objectivity during analysis. Of the 53 participants, 18 (34%) replied that they did not use any techniques. 17 participants mentioned approaches involving hypotheses or alternative explanations. The large proportion of participants stating to have used hypotheses may signify the operationalisation of the presumption of innocence principle. The use of hypotheses may indicate that digital forensic practitioners apply the scientific method to their analysis, where hypotheses play a central part.

It may also point towards an awareness concerning the risk of cognitive bias. However, the low number of participants who stated that they would write the hypotheses down indicates an overconfidence concerning their ability to systematically test the hypotheses. This finding corresponds with the results concerning biasability in the digital forensic experiment.

'Reliability' may be associated with various meanings, and the term was not defined or explicated in the survey. Some of the reported techniques were useful for checking the reliability (consistency) of the tool interpretation. Using two different tools that share libraries, engines or methods may, in the worst-case, result in a similar but flawed interpretation of the same data. Some of the reported techniques were aimed to control the authenticity or accuracy of the findings. None stated to have used techniques for uncovering human errors, such as biased examinations or one-sided or overstated conclusions.

The problem is not just related to inadequate transparency and documentation practices, but also insufficient quality control and error mitigation practices. Many of the reports lacked detailed descriptions methods and tools used for the analysis, as well as the reliability and validity of these.

2.2.2. Hierarchy of expert performance

Work in digital forensics includes a large number of subjective and interpretive decisions and judgments. The outcome of the Digital Forensics process is based on cognitive and human variables, which might result in bias and error. Understanding the human role and sources of error is essential for the development of effective quality measures and for achieving transparency. The Hierarchy of Expert Performance is a paradigm for investigating and assessing the performance of experts in Digital Forensics. It addresses three viewpoints of decision making: first, reliability against biasability; second, observations versus conclusions; and third, discrepancies between same expert, identical evidence, at different periods. Contextual information is one of the many sources from which bias may arise. To reduce contextual bias, task-irrelevant data should be omitted from the forensic decision-making process. Due to the potentially skewed nature of contextual knowledge, the forensic examiner must disclose what they knew and when they knew it while performing their duties. Digital Forensics examiners were required to include "case information" on their Digital Forensics submission form. None of the forms specifically indicated not to submit task-irrelevant information or gave guidance for what information should (or should not) be included (or omitted) in this section [235].

The purpose of the research was twofold. First, to investigate if contextual information influences digital forensics decision-making, and second, to determine whether examiners' decisions are consistent. A letter of invitation was extended to Digital Forensics examiners via the European Union Cybercrime Task Force (EUCTF) network, the Interpol digital forensics expert network, and the Norwegian Police. The goal of the experiment was to determine whether or not participants arrived at comparable outcomes and how to document them. According to the experiment's participants, the primary processing/analysis tool used was:

- Magnet Axiom: 53%
- X-Ways: 28%
- EnCase: 6%
- Autopsy: 6%
- Forensic Toolkit (FTK): 4%
- The Sleuth Kit (TSK): 2%.
- Other: 2%

The file containing the evidence had an NTFS file system and Microsoft Windows XP as its operating system, and its timestamps were from 2008. Each participant was supplied with a scenario detailing a case of sensitive information disclosure. Participants were instructed to work independently and refrain from discussing the experiment with anyone.

The day before the experiment, a URL to download the evidence file was provided. The file may be processed in advance, but the analysis would not begin until the next morning. The participants were then instructed to write comments in the log during analysis, and the template included fields for whether the result was bookmarked and its evaluation. The results were analysed using the Kruskal-Wallis test, a non-parametric rank-based test used for small sample sizes to determine if there is a statistically significant difference between groups. In qualitative analysis, the Krippendorff's Alpha coefficient was used to determine agreement among coders and inter-coder agreement.

Digital Forensics examiners were given a file containing evidence and a scenario as a starting point, but different contextual information (indicating strong guilt, weak guilt, or innocence). A control group was given merely the scenario without any context knowledge. The traces are not particularly complex, and locating them would take only fundamental Digital Forensics skills. 26% of the subjects discovered 1–4 traces, 35% discovered 5–8 traces, and 4% discovered 8–10 traces. Intriguingly, contextual information had a statistically significant effect on the proportion of observations.

The Innocence group found the fewest traces, indicating that they were predisposed to discover less proof. The Weak Guilt group found considerably more traces than the Strong Guilt group, demonstrating that the unclear context of Weak Guilt (wage conflict in which the suspect sided with the workers) influenced this group to uncover more traces. The number of interpretations for each group did not change significantly (7 interpretations x 53 participants/4 groups = 92.75). A Kruskale-Wallis test done on the total number of observations revealed that contextual information between groups had no significant influence (p .05). Traces discovered by at least 35% of Digital Forensics examiners were included in this section.

Concerning biasability, the research question was: Are Digital Forensics examiners influenced by contextual information when making observations, interpretations of observations, or conclusions during the examination of digital traces? Results indicate that contextual information influenced the observations, with more traces identified when Guilt circumstances were introduced. At the level of interpretation and conclusion, the assessment of biasability did not produce statistically significant results. According to the poll, the proportion of observed traces is more than what is stated in the analytical results. This discrepancy suggests that the traces may have been overlooked or explained away, as opposed to not being discovered.

The findings about the observability of bias give light on the point at which prejudice begins to influence the outcome. Results indicate a low/inadequate (a 0.667) level of consistency across Digital Forensics examiners that assess the same evidence file using the same contextual information. For examiners receiving Strong Guilt context (A) and Innocence context (B), the highest reliability score was found at the observation level for traces observation (B). The greatest within-group variation at the conclusion level is the difference between evaluating a trace as a sign of guilt or innocence and not rating a trace (A1 and A6). If a Digital Forensics examiner analyses an evidence file and then reanalyses the same file, the likelihood of obtaining consistent results is minimal, according to the findings.

There are numerous causes of consistency, such as when examiners are constantly influenced by comparable contextually biassed material. Not only should tools and technology be measured for quality, but also the human element.

This is the first study to investigate the dependability and biasability of Digital Forensics decision-making. In their observations, interpretations, and conclusions, experts analysing the same evidence file with the same contextual information are found to have low reliability. It emphasises the importance of systematically implementing quality control techniques, such as blind peer review, in digital forensics exams. A bias countermeasure could be that every Digital Forensics examination begins with a balanced set of alternative hypotheses, in which both innocence and guilt are represented, and that the examiner methodically evaluates all hypotheses during the study and reports the results accordingly. Transparency regarding what they knew (what task-relevant and task-irrelevant information they were given) and whose hypotheses guided the examination is crucial for detecting biassed decision making.

The sample size of 53 Digital Forensics examiners posed a potential constraint to the study's statistical power. Since the study, like the majority of studies, relied on voluntary involvement, there is also the possibility of self-selection bias.

2.2.3. *Peer review*

Evidence entering a criminal justice system must be reliable if it is to be used as part of any legal decision making. Forensic science as a whole is littered with examples of miscarriages of justice. As digital evidence continues to feature prominently in many criminal investigations, it is arguably only a matter of time before similar issues occur. In digital forensics, essential to the assessment of evidence 'quality' are dimensions of validity and reliability. Validity could be described as "the overall probability of reaching the correct conclusion, given a specific method and data". In turn, reliability is a multi-factored construct, despite the term being often used as an umbrella kite-mark. Ineffective peer review in digital forensics has been noted for over 15 years. Standards are no absolute guarantee for quality [236].

The importance of peer review in forensic science cannot be understated. Peer review is one of the main mechanisms for vetting work for errors and to correct these where present. It forms part of the expert evidence admissibility tests seen in Daubert v Merrell Dow Pharms., 516 U S. 869.

In relation to digital forensics, the need for peer review is no different to traditional forensic science types. In part, this is due to the diversity and complexity of digital evidence types which may occur. Peer review of the methodology aspect of a physical evidence is somewhat simple due to its linear approach - identify print - capture and lift - > analyse; whereas the digital forensics practitioner may employ multiple tools within any single examination, followed by any number of features within that tool. It is assumed that peer review is currently the primary method for detecting unreliable work, but there is no consensus as to whether peer review takes place in every organisation.

The lack of a defined peer review standard means that it is currently unknown as to what shape and form a peer review in digital forensics currently takes. A key task in any peer review is the allocation of an effective peer reviewer. This is even more challenging in the laboratory environment. Consideration must be given as to the depth of analysis undertaken as part of the review process. Sufficient training is required in order to become a competent peer reviewer and to recognise what one looks like.

Approaches such as fact checking vs. procedural repeating for validation purposes both carry different advantages and disadvantages. The peer review prcess in forensic science must be efficient. Peer review mechanisms that are over-burdensome risk disengagement from staff in the laboratory environment. There is a trade-off between a robust review and one that fits the needs of the organisation.

Any peer review process should have mechanisms in place to identify poor peer reviewing. It is worth noting that being taught to peer review may not be commonly part of forensic science training. However, it may be of less risk to repeat the work where the impact of error may be seen as too severe to risk standard peer reviews. A non-standardised and non-transparent peer review process may therefore add another layer of trust to the evidence, instead of providing insight into the actual value of the evidence.

Peer review is mentioned or described in several standards relevant to digital forensics. Standards provide useful guidance for peer review but are often behind paywalls. ENFSI underlines the importance of peer review "to ensure the strength and provenance of the details being assessed". Peer reviews that begin to evaluate and interpret the findings of reported work are inevitably a more resource intensive process due to the level of required scrutiny. A 'proof check' may identify grammatical and typographical errors in a practitioners report, while a 're-examination' could discover procedural flaws and misinterpretation of evidence.

The 'administrative review' is the most basic form of peer review and focuses on whether the practitioner has followed client's requirements. The 'proof check' and 'sense reviews' are low-labor-intensive approaches to review, and arguably require limited technical knowledge to carry out. This level of review can be defined as follows: "Here, the work is proofread purely for grammatical and spelling issues".

To assess evidence descriptions and interpretations requires understanding, knowledge and expertise. This form of peer review is potentially more costly in time and resources as it requires senior staff to conduct the review. Conceptual peer review is an extensive peer review based on the practitioner's documentation derived from the analysis. A 'verification review' is in essence a second examination carried out across the principal examiners data set. Verification reviews do expose the practitioners work to a greater degree of scrutiny, but their implementation requires more effort.

Peer review structures must extend into the investigative process in order to support the practitioner from the start of their casework. As a result, peer review should not be confined to the last stage of an examination's journey. It is suggested that it is important that practitioners are supported in their investigative decision making at all stages of their cases.

This paper has outlined the necessity of peer review in digital forensics and the benefits it may offer to the field in terms of quality assurance and error reduction:

1. An evaluation of the technical and non-technical error sources in digital forensics.
2. A thorough analysis of peer review as a concept in the context of digital forensics, emphasising its possible problems and faults.
3. The 'Peer Review Hierarchy' is presented, defining seven stages of peer review that can be applied to a practitioner's findings.

2.2.4. Quality assurance systems

2.2.4.1. Formalising investigative decision making. In most digital forensic investigations, a practitioner will highlight multiple pieces of digital data which they may consider potentially evidential. Before opting to report this information to their client, their interpretation of such data must be accurate, and its impact on the investigation understood. The DERDS framework is designed to guide a practitioner through the necessary steps for determining when it is safe to report the specific findings of their examination. The DERDS framework is designed to support those who are actively involved in digital forensic case work and require additional formalised investigative DM support. The formalization of DM in digital forensics serves as a reminder of logical decision and the processes involved with attaining this [237].

While some experienced and reliable practitioners may deem such DM a natural part of their case processing, benefit from the DERDS framework in regards to mitigating the risk of mistakes. The DERDS framework provides three pathways for a practitioner to determine and test the reliability of their investigative 'inferences, assumptions or conclusions'. For those experienced, but lacking such confidence in their decision making it may serve as codified process flow for making sound judgements. The framework should be considered a quality management resource for laboratories and senior staff tasked with maintaining the standard of work.

The first stage in the DERDS framework is to determine whether the piece of potential evidence under scrutiny is comparable to that which has previously been validated and accepted in a previous case work precedent. If so, a practitioner may opt to pursue the use of this previous interpretation and rely upon it when producing a current report. Digital forensic practitioners have a duty to consider any competing hypotheses which may exist in regards to the digital data under investigation. They must also consider any impact they may have upon their understanding of the data and the reliability of their interpretation. A practitioner should also have the application of previous case work precedent to their interpretation of evidence validated by a second competent individual.

Digital forensics practitioners are asked to identify and follow the interpretation of any evidence provided in existing published works or test and validate their own findings. First a practitioner must be competent to carry out a thorough search for reliable published literature. This includes material formally published in academic journals as well as content acquired from formal training courses and institutes. If a practitioner can locate a relevant source, a measure of confidence is required regarding its reliability (Measure of Confidence 4). This is based on a number of factors including author details, location of published work, any citation information and peer-reviewed status.

The working conclusions must also be reviewed and validated by a second competent individual, should the resource be relied upon as part of the interpretation of evidence in the current case. Peer review is a crucial stage in the process of validating results and one which is difficult to apply. Questions may be raised as to whether enough practitioners with the required experience and expertise exist. Yet the burden of operating with appropriately trained and experienced staff lies with the digital forensic organisation and it remains best practice to ensure such reviews take place.

The act of testing maintains resource considerations and whilst the accuracy of any investigation should not be compromised by resource restrictions, in reality, constraints are in operation. Decision 12 provides a gateway to testing in the form of a competency test. Testing provides the foundation from which the reliable interpretation of the result is built. Flawed testing can increase the dissemination of erroneous knowledge under the guise that it is more reliable and should be treated as 'known good'. The Framework for Reliable Experimental Design framework is designed to support the robust planning and implementation of testing in digital forensics, supporting the evaluation and analysis of subsequent results. Actions 2–5 and Decision 14 provide for the key testing stages. On completion of testing, the practitioner is required to address whether they are now in a position to reliably confirm their 'inferences, assumptions or conclusions'.

A practitioner encounters an application 'X' for the first time and cannot be sure of its function. They could opt to follow previous case precedents involving examination of 'X', if any exist. Or they could seek support from senior colleagues regarding the level of confidence attributed to a past precedent. Traditionally, a practitioner must rely on published work to determine the function of 'X'. This is reliant on being able to identify an applicable, reliable source of published work. DERDS aims to increase the rigour of processes involved with the interpretation and testing of digital evidence before the reporting process.

2.2.5. Digital forensic model validation

Digital forensic science has been defined as "the application of scientifically derived and validated techniques to the preservation, gathering, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence." Anti-forensics is one of the problems of digital forensics. By erasing evidence, Anti-Forensics is capable of delaying or preventing an investigation. The authors examine digital forensic models and anti-forensic attacks that affect different aspects of the digital forensic process. The generic computer forensic investigation model created categorises prior Digital Forensic Models' common computer forensic phases [238].

The eleven phases of the Systematic Digital Forensic Investigation Model include preparation, securing the scene, survey and identification, documentation, evidence collecting, preservation, examination, analysis, presentation, and outcome and review. Some authors contend that none of the models satisfy all of the Daubert Standard's requirements. The Digital Forensic Models cannot be regarded as a standard as the error rate could not be computed. Existing models are not adaptable, as they are not generalised and cannot be applied to many digital forensics fields. Several researchers have included ISO/IEC 27043:2015 standards into their digital forensic architecture.

Previous authors have presented a five-phase digital forensic procedure that takes into account the identification of anti-forensic attacks. The framework is underpinned by a number of intricate propositions, however they fail to demonstrate exactly how their theory or proposition may identify an attack. These frameworks solely consider the analytical step, ignoring other crucial phases such as data gathering, review, and reporting. The current paper concentrates on the four most frequent phases: acquisition, analysis, examination, and reporting. When an investigator wishes to collect evidence from a machine, he or she must follow specific protocols based on the machine's condition, i.e., whether the machine is ON (live acquisition) or OFF (dead acquisition).

Anti-forensic tactics could thwart either of the acquisition procedures. For instance, if a forensic tool's drivers rely on the 'KDBG' string to resolve symbols, this strategy could halt the memory gathering operation. In addition, if the undocumented memory enumeration application peripheral interface and memory mapping such as MmGetPhysicalMemoryRanges () and MmMapMemoryDumpMdl () are updated to return a NULL value, a modified version of the memory map would be returned. This can be circumvented by encrypting the entire storage medium or certain partitions within it. Other methods proposed for hiding a file to avoid investigation include manipulating particular registry keys, storing data on bootable USBs or DVDs, and even using compression bombs.

Various techniques, including steganography, can be used to conceal data from forensic investigation. It is possible to inject harmful code into computer forensic programs in order to generate erroneous forensic results and infect the computer. The hypertext markup language (HTML) code injection technique can be used to execute this type of attack.

The investigation of digital crime is a sequential procedure that can be led by a Digital Forensic Model (DFM). Methods and forensic instruments must be validated in order to preserve the integrity of evidence. For this goal, the National Institute of Standards and Technology in the United States (US) established the Computer Forensic Tool Testing Program. In the United Kingdom, the Forensic Science Regulator's FSR-G-218 method validation in digital forensics and in the United States, the Daubert Standard validate digital forensic methods and procedures. In its code of practise, the Forensic Science Regulator makes ISO-17025 accreditation mandatory for all providers of digital forensic services to the criminal court system.

A method or procedure adopted by an investigator in the United States ideally adheres to the Daubert Standard. In 2005, the House of Commons Science Technology Committee noted that scientific methodologies are not validated prior to their admission into court. Digital Forensic Investigators frequently prepare forensic reports using forensic software tools. The majority of digital forensic models are not considered against the risk assessment methods of FSR-G-218 or any other guideline document. This poses a hazard to the enquiry in terms of the dependability of evidence.

The authors present a principle for verifying Digital Forensic Models against anti-forensic tactics that affect each phase of the digital forensic process. To validate a Digital Forensic Model, each phase must be validated before moving on to the next phase. To define this procedure mathematically, specific definitions and axioms are first presented, followed by the proof of assertions. All Digital Forensic Models are tested in accordance with the validation principle.

The implementation of this theory is illustrated using a hypothetical scenario in which a defendant is accused of launching a DDoS assault against the network of an organisation using their laptop with the assumption that each phase of the Digital Forensic Model includes two anti-forensic strategies. The benefit of this idea is that validating a phase of the Digital Forensic Model requires only four steps. The validation principle resides on the higher level of abstraction. It can only validate a Digital Forensic Model if it has prior knowledge of an anti-forensic approach, such as zero-day assaults, for which the database does not contain information.

2.2.5.1. Verification of Digital Evidence framework. The VODE framework exists to assist a digital forensics practitioner who has discovered evidence in a suspicious case. The practitioner must seek to ascertain its significance, relationship to the alleged offences, and the acts that could account for its appearance on a system. Through the interpretation of digital traces, the practitioner attempts to accurately determine whether digital events have or have not occurred [239].

'A new knowledge scenario' is a situation where a practitioner encounters a digital artefact/data or case scenario for the first time, AND it is previously undocumented by anyone OR an interpretation exists but it is unreliable. The product of a 'new knowledge scenario', generated by the practitioner following their own testing and interpretation of a digital trace. The VODE framework is designed to support the practitioner in assessing whether a given digital trace found within their current examination has previously been encountered and reliable interpreted. This includes three pathways, where the digital content in question has already been interpreted as part of a past case, or where a new knowledge situation is present.

The practitioner must understand why they have found the 'potentially relevant' digital traces on a suspect device. The formalization of initial suspicions regarding the data helps to establish the potential worth of it in regards to the case in question, following its reliable interpretation. It also helps to develop testing processes to be implemented later in the VODE framework. A practitioner should consider what a suspect has potentially done on their system in order to have generated this potentially relevant content, and why this is important to the case in question. Where the digital trace's potential case impact is low or non-crucial, a decision to not implement further testing may be necessary.

The practitioner examining the presence of digital data on a suspect device must first establish its location on a system and what this means. Data may have been created by a piece of software under suspicion (for example, a chat client which has created a chat log in a grooming offence) or via passive operating system processes. Identify any metadata which may be linked to an artefact/data which describes its function on the suspect system. This could be file system metadata following a set of actions or operating system logs and artefacts which capture data passively when the system is running. Establish why the data has occurred on the device in question and what digital actions are believed to have generated it.

A reconstructed digital environment provides the foundation for any following testing to occur. Digital traces on device occur as a result of either a singular or set of actions and where these actions appear evidentially relevant, the practitioner must attribute these to a specific action or actor. The reconstruction of digital events is a difficult but necessary task where a practitioner must recreate the believed actions of the suspect as closely as possible. Unlike the physical forensic sciences, digital forensics practitioners are in a unique position to carry out a complete reconstruction of suspect scenario. Any reconstruction which falls short of complete (for example, mismatched operating system or software versions are used) provides a level of functionality doubt, and ultimately undermines the reliability of any subsequent testing and results.

A practitioner must also consider whether the functionality of an app (or sub-function) is the same and that logging appears consistent in terms of location, structure and internal metadata types. When attempting to reconstruct a suspect environment for testing there are two options, either 'clean' of 'dirty'. A clean reconstruction involves the use of a fresh installed system, either installed on a clean disk drive to boot with physical hardware, or a virtualized version. This helps to prevent test contamination and limits the background noise that can occur on a system and make the interpretation of results more difficult. A dirty reconstruction involves the use of the suspect system itself and involves the reverse image of a suspect device onto a secondary drive, or a virtualization. This form of reconstruction places the practitioner in the position that the system was in when last used by a suspect.

Testing is undertaken to establish the correct functionality, behaviour of a particular artefact or set of data on a system and to establish what actions have caused its presence. Testing must involve the replication of those actions believed to have been carried out by a suspect on their system, on a comparable test environment. Results of these tests must be analysed for meaning, and this interpretation applied to data found on a suspect system. Black box testing involves assessing an application's behaviour by utilising a set of known inputs to generate and analyse outputs without ever knowing the internal structure and function of the software itself. This is a difficult task as without understanding internal code structures, a practitioner must use a combination of intuition, guesswork and the visible functions that the software offers the user in order to generate a comprehensive set of inputs.

In opaque box testing, the practitioner must subjectively interpret what the output data means in conjunction with the used input actions, whilst also considering the possibility that further inputs may also result in the same output. Testing is undertaken due to the need to establish the reliability of the interpretation of 'new knowledge', discovered as part of an active case. In some digital scenarios, multiple actions may result in the same output and each must be tested and verified. A practitioner must establish the validity of competing hypotheses via either further test implementations or through development of additional tests. Digital data on a system does not always permit the factual depiction of events in all circumstances and in some cases a lack of data may create uncertainty.

Forensic science provides decision-makers with trustworthy understanding of the traces in order to help them make decisions. This includes accurately interpreting the results of testing, a crucial and complex task. Any misinterpretation is both dangerous for the current case under investigation (where erroneous verdicts may be reached) and where a misinterpretation has been shared for future investigations. Best practice dictates that the production of a standard operating procedure (SOP) for the interpretation of the artefact/date in question. The final stage of the VODE framework is to apply the results of testing and the interpretation of findings to the data present on a suspect machine. The produced SOP not only ensures helps to confirm the practitioner understands the work they have done by being able to document it, but also provides a blueprint for those encountering this data-type within a prospective investigation.

2.2.6. *Structured decision making*

The utility of forensic science encompasses supporting decision making in trial, contributing to inquiry phases, bolstering policing, as well as generating knowledge about crime. Information produced by some forensic processes can also be useful for intelligence purposes. Forensic practitioners are struggling to keep pace with the rising demand for forensic analysis of digital and multimedia evidence. Decisions in operational and forensic contexts are based on a limited amount of information that continues to be updated as the investigation progresses. This work applies the same principles of scientific interpretation to decisions throughout an investigation in order to strengthen all phases of the investigative process [240].

The content of this work is focused on digital evidence in criminal investigations, but many considerations are generally true for any type of trace or investigation. There is a lack of consistency in terminology to describe decision processes in forensic science. In an effort to improve common understanding of decision processes across forensic disciplines, this work adopts the concepts and definitions developed within the National Institute of Standards and Technology, OSAC Organisation of Scientific Working Groups, Digital Multimedia Scientific Area Committee. Three defined decision processes that can be useful during any phase of an investigation are authentication, identification, and classification. Jackson et al. provide the following differentiation related to decisions made during an investigation.

- Authentication: Determining if a claim is true.
- Identification: Decision process to build adequate confidence that some identity-related information describes a specific entity in a given context, at a given moment.
- Classification: Development of taxonomies of traces and the decision process to assign a trace with sufficient confidence to its class based on features that are common among traces of the same class, distinguishing them from other classes.

In a "preliminary evaluative" context, forensic practitioners assign a value to the observed digital evidence in light of each of the plausible propositions they generated. Forensic practitioners produce values that are targeted to help differentiate between plausible and less plausible propositions. Focusing on the "fully evaluative" process for use in a court of law, forensic practitioners provide a value to the court in the form of a likelihood ratio. The resulting likelihood ratio is the ratio between the probability to observe the trace according to the first proposition and the probabilities to observe it after the second.

In both traditional and digital investigation models, the overall process of conducting an investigation consists of numerous interconnected phases in which judgments must be taken. Decisions during a criminal investigation include, but are not limited to:

1. Decision to attend the scene
2. Decision to search for evidence
3. Decision to collect potential sources of evidence
4. Decision to analyse evidence
5. Decision to use forensic observations in the inquiry
6. Decision to collate forensic observations in a structured database
7. Decision to use evidence in court

The search for digital evidence must be divided into two distinct phases: the collecting of digital objects and the decision to analyse such things in order to locate evidence. In order to do so, the forensic practitioner will need to identify the location as a scene through the process of identification and verify that pertinent information may be present at the scene. The decision to collect evidence or digital objects must reflect a balance between the collection's utility and the danger of irretrievable data loss if the collection is not performed.

For instance, an IoT device's data may be stored on the cloud, on the device itself, or on a smartphone running an application. The forensic practitioner must authenticate the evidence by determining if the information it contains corresponds to the studied previous event. The information's quality will depend on the value that can be extracted from it. Before assigning pieces of evidence to these categories, a taxonomy must be developed to categorise the forms of evidence and their respective importance. The decision on the admissibility of evidence in court is comparable to that made by a forensics practitioner during an investigation.

Certain pieces of evidence are only used for the purposes of an enquiry or intelligence gathering, whereas others are analysed for judicial use. Relevance and significance of a trace or piece of information are crucial factors in the decision-making process, as well as for the forensic practitioner. A professional in digital forensics must make decisions regarding the treatment of a crime scene, a trace, or the creation of a report. The concepts of decision theory help to structure and comprehend how current knowledge and new information support judgments.

In certain instances, it makes sense to seek a professional to determine whether or not a file was recovered correctly and in its entirety, as it would be hard to reason with the received information otherwise. The authors claim that organising these decisions in this manner will improve practise and pave the way for the development and implementation of more effective models in crime laboratories. The decision's utility is a quantification of the decision's effects. In online fraud investigations, the decision to abandon the case is frequently made if an originating Internet Protocol (IP) address is discovered to be a proxy, even if there is substantial justification for the notion that evidence may be located on the proxy computer.

A strategy for determining the true state of a variable may be useful for streamlining operational procedures through the use of acceptable assumptions. For instance, it may make sense to determine that the precision of a sequence of localisations is adequate to be regarded the current location of the device. There is no model evolved enough to manage a portion of the complexity associated with digital evidence. A report on digital evidence would include a list of unanswered issues, and the decision-maker would be required to engage in a multi-step decision-making process.

Such a procedure would be considerably too complicated and would substantially raise the possibility of erroneous and incoherent conclusions. The decision's utility is a quantification of the decision's effects. In online fraud investigations, the decision to abandon the case is frequently made if an originating Internet Protocol (IP) address is discovered to be a proxy, even if there is substantial justification for the notion that evidence may be located on the proxy computer.

2.2.6.1. Structured decision making using digital evidence. This article offers practitioners with a framework for making defensible decisions. The emphasis is on courtroom decisions, which corresponds to the definition of "completely evaluative". The current work adapts the logical framework to a more generic context in which acceptable assumptions and processes may differ in certain respects. A likelihood ratio for two competing hypotheses is the proportion of the probability of detecting the data, assuming that either of the hypotheses is correct in the long run. There are other methods, such as classifying the evidence into an ordinal scale.

It is essential to recognise that probabilities are not to be viewed in a strict frequentist manner, but rather as a measure of uncertainty. The probability of a proposal is not the only factor in a decision. If accepted as true, not all propositions have identical consequences. The investigator must consider the decision's expected benefits and disadvantages, known as the decision's utility.

It is not rare for a forensic investigator to give an opinion in an investigative situation, particularly if the probe is dominated by technical features. In an evaluative context, however, this is inappropriate due to the investigator's lack of prior knowledge and the forensic practitioner's lack of authority over the ultimate conclusion.

2.2.6.2. Case example. The authors describe a hypothetical case example. Suppose someone was radicalised in the Middle East. The decisions:

- Attending the scene – Investigators search the person's apartment. Digital forensics experts must determine whether to join the search or let detectives do it alone. Online utterances (e.g., Facebook) are more likely if the person is radicalised and violent. According to a pre-planned operating strategy, the matter is serious and complicated and requires expert intervention. This decision was mostly strategic.
- Evidence search – This suspect does not have computer interests based on contextual information. However, radicalisation suggests devices and radical communication. Thus, the professional will prioritise external memories, phones, and laptops with external connections.
- Evidence gathering – The expert finds two computers, a phone, USB keys, and an external hard drive. The digital investigator must decide if all components will be seized. Dust covers a PC, three USB keys, and a phone. The digital investigator may believe they are irrelevant to this case. This is a serious case, so the dusty computer and phone are seized even though they are unlikely to be analysed.
- Analyse evidence – A police specialist is entrusted with determining whether or not the recording was made with this gadget. It is possible to argue that this is not his/her decision and that the outcome of this analysis should be incorporated into a subsequent analysis. The stages through which this judgement is made based on contextual and technical information are outlined below. A technique of evaluation according to the OSAC Framework entails examining a sequence of videos that appear to have been filmed with the same camera. Then, a specialist analyses the videos by specifying their general properties, such as resolution, frame rate, and frame size, and runs a tool to extract a PRNU pattern from the video's frames. Overall, the specialist believes, based on his or her experience, that the data strongly supports one proposition in compared to another. Whether or not all videos were captured by this device has minimal bearing on whether the suspect will be indicted for the event captured on camera.
- Inquiry using forensic observations – According to the study, the conclusion has enough probative value for investigation. It's used at the suspect's hearing to verify his assertions and justify the investigation and relatives' hearing.
- Database decision for forensic observations – The phone's recordings and photographs were added to a terrorism database. This database can help future analysis by detecting media on a digital device faster, but it cannot link cases. Due of media sharing, it would be hard to trace these.
- Court evidence decision – After the investigation, this evidence must be reassessed to determine its court admissibility. The assessed probative value may warrant court employment.

In many types of scientific investigations, including criminal investigations, the incidence and importance of digital and multimedia evidence is increasing. To fulfil their position in an investigation, forensic practitioners must make numerous choices. Some believe that it is not the responsibility of forensic professionals to make such determinations, although the necessity of doing so in some highly technical circumstances has been shown.

2.2.6.3. Knowledge sharing and the capsule of evidence (CODE). Digital forensics professionals are subject to a "silo mentality" characterised by a reluctance to exchange knowledge. While some may believe that sharing content is an ethical and moral obligation, this cannot be expected of everyone. Knowledge-sharing should, if possible, be incentivized to promote engagement. To achieve optimum benefit from information sharing, it must be sustainable and enduring. A rule of behaviour must be implemented to protect persons from having their professional reputations or from being trolled. Disputed information must be handled in a formal and competent manner. A vessel and format for shared information that can be adopted by the field must be devised. The question "what is to be shared?" is the focal point of this work [241].

The CODE structure is a formalised guidance on the elements needed for effective knowledge sharing in digital forensics. It defines the requirement for three key categories of data descriptors; 'Submission Metadata', 'Core Continuity Elements' and 'Core Digital Data Descriptors'. All comprise of a series of sub-criteria which help to demonstrate the reliability of any 'new knowledge' contained. Capsules are designed to house reliable knowledge generated through engagement with robust forensic methodologies designed to support accurate knowledge creation. There are six core digital data descriptors which must be present in order to create a complete and reliable set of information needed for contents in the Capsule to be used by others.

Digital forensics practitioners must provide a detailed record of the circumstances surrounding each artefact/data including case type, suspected offence, file paths, naming conventions and internal structure. Each artefact copy must also be disclosed with any associated 'test actions' documented to allow for the explanation of any modifications which might be present in the data. Digital artefact research has a specific lifespan where many of the digital artefacts themselves are subject to frequent structural change following software updates. Data inside of each Capsule must be capable of being updated where additional information becomes available, with further validation records added. Each iteration must also have all six core 'digital data descriptors' for any new testing which has taken place.

A chain of validation is a list of all those who have validated the findings presented in the Capsule, as per the original submitter. This includes practitioner details and geographical location. Further, if any iteration of the data within the capsule occurs, those who engage with the capsule must note which iteration they used. This allows 'knowledge-tracing' to occur, which has two benefits. First, it helps to quantify how impactful each particular Capsule has been by determining the level of engagement with the digital forensics field. And second, if a Capsule if later found to be compromised and its content is identified are incorrect, this can be traced and any further spread of incorrect information can be prevented.

The contents of a Capsule is described in Section 2 of the Code for Advanced Digital Forensics (Capsule) project, but how is this created? A practitioner must collect data from their case and process it into a format which can be queried for analysis and search and retrieval. The burden falls on the practitioner to manually populate their Capsule, a likely burdensome task, which may deter practitioners from joining the project. The sharing of knowledge, regardless of form, should be seen as beneficial in digital forensics. Internal sharing takes place when an organisation chooses to store practitioner Capsules and make them available for their practitioners to use. Field-wide sharing is arguably the goal of any knowledge-sharing schema, but there is lack of appropriate governance models to serve as a template.

2.2.7. Credentialing

Digital forensic investigation is one of the prominent fields emerging from the broad discipline of forensic science. There are no national standards for digital forensic credentialing, and for that matter, no state-level ones. Some states have attempted to bring about such standards. These efforts have been half-hearted and somewhat disorganized, many times causing more problems on the legal realm than offering solutions. In addition, the field as currently constituted has no gold standard for certification. The National Institute of Standards and Technology (NIST) published special publication 800-181, a National Initiative for Cybersecurity Education. The author's university has applied for a program that would allow regionally accredited colleges and universities to apply for and have their curricula designated as cyber defense programs [242].

Many studies in digital forensic investigations have identified the bias in available research towards applied aspects of the domain as opposed to the development of fundamental theories. There is credence in the fact that several studies identify the lack of a proper credentialing standard as one of the main challenges facing the profession today. A good deal of research is currently dedicated to advancing training and ensuring that there is a teaching framework that can be followed successfully by most universities. A large number of studies recommend that proper standardised frameworks are brought into the frame for credentialing of digital forensic investigators.

Some authors make the bold allegation that digital forensics is not yet a profession. They argue that a profession entails specialised knowledge, specialised training, highly valuable work, self-regulation, a code of ethics, high levels of autonomy, and many other significant elements. There are no consistent accreditation frameworks for digital forensics [243], but a framework to regulate bodies that offer credentialing exists and operates with a clear mandate. OSAC has been involved in the development and promulgation of documentary standards that are used by accrediting bodies to audit forensic laboratories and carry out credentialing of forensic investigators. These include advice on training on science and law, testimony and reporting, provision of interim solutions, and accreditation and proficiency testing. Certifications are updated every 3–5 years with more material added, some outdated material removed.

The fact that there are so many private organisations offering so many certifications, many in digital forensics, is a testament to the need for credentialing and accreditation process. Private organisations are utilising this opportunity to advance their own goals, primarily financial.

The National Academy of Sciences stresses the importance of quality assurance procedures in the practice of forensic science. In digital forensics specifically, a comprehensive quality assurance/quality management plan is required to ensure the credibility of digital forensic laboratories. Failure to implement such a plan can lead to the wrongful conviction of innocent persons.

Failure to follow acceptable digital forensic procedures led to the accusation and trial of a substitute teacher alleging the teacher deliberately visited pornographic websites.Computer forensics conducted by a defence expert found that the school's antivirus software was not regularly updated nor maintained; also, no antispyware, firewall, or content filtering tool was found on the school computer. The judge refused to allow the full testimony of defense expert witness into evidence, claiming that the information to be presented by the expert was not made available during discovery prior to the trial proceedings. Ultimately, the teacher was found guilty of "Risk of Injury to a Child," and at one point faced the possible fate of a 50-year prison sentence. She pled guilty to a misdemeanor and agreed to have her teaching license terminated.

Digital forensics can lead to innocent persons being convicted of crimes, but it can also lead to guilty persons being acquitted in court. Another case is part of the phenomenon commonly known as the "Trojan horse defense," which became popular in the UK during the early 2000s (Brenner et al., 2004). A forensic examination of his computer by prosecution's expert witness found tools that could be used to launch an attack, but no trace that a Trojan horse had been planted on his computer.

More attention needs be paid to credentialing, which entails research, funding, and advocacy at the national and state levels. A national framework for developing and teaching digital forensics in order to bring standardization to the field is a necessity. Any standard(s) developed for use in the computer forensics discipline, must allow for flexibility. It is also important that computer forensic standards cover all aspects of the forensic process. Computer forensics is still considered to be in its infancy and does not yet have formal credentialing bodies or educational process. In adjudication processes, the courts accept persons as expert witnesses based on their skills and previous professional work experience.

The topic of presenting a potential full solution and/or framework for digital forensics can arguably be a doctorate dissertation in its own right. One can argue that even then it truly requires the efforts of governments, law enforcement, and academics to put forth a viable solution. The following possible outlines are intended to present the reader with some possibilities that are currently lacking in the field and could serve as starting points. A digital forensic investigation framework should be sophisticated and flexible enough to apply to a wide range of localities and entities. At the state and/or federal level, interested investigators must be required to register and take rigorous exams.

These exams must focus on assessing a test taker's ability to understand the digital forensic processes with the realization of its legal and ethical importance. The governments should spearhead curricular reinvention and development and take their active roles in the promotion of a unified credentialing framework to guide other bodies in the same direction. External certification and accreditation processes supported and approved by governments are desirable as they bring consistency and professionalism to the profession of digital forensics. There will never be perfect solutions, and any attempt at designing a framework with perfection in mind would be futile. A major issue is the application of encryption to devices.

Most devices are not encrypted and can be analysed without the worry of dealing with encryption. An investigator should have the skills to take a memory dump of the running system since memory is never encrypted. Given the large memories of today's computers, a wealth of information may be available just from the memory dump alone.

2.2.8. Codes of practice

The United Kingdom's Forensic Science Regulator has published codes of practice and conduct. The Code of Practice is aimed at all those providing forensic science services to the Criminal Justice System. Forensic units applying for accreditation to one of the international standards remain responsible for ensuring they are aware of all relevant requirements. The Code of Practice is intended to provide the public with confidence in the reliability of forensic science and to enhance customer satisfaction through the effective application of the management system [244].

Appendices specific to each forensic discipline are attached to the code. Forensic units providing digital forensic services must comply with the Codes of Practice and Conduct for Forensic Science Providers and Practitioners in the Criminal Justice System (the Codes) [245]. The provider must be accredited to ISO17020 for any inspection or testing activity at the scene of incident or ISO17025 for any laboratory function. All digital forensics methods and procedures used by a forensic unit must be validated. Software, hardware and tools where operation of these has an impact in obtaining results will require validation within the method they are deployed. The risk assessment process detailed in the Codes is intended to used be to determine the impact of the overall method used.

A formal risk assessment method should be used for each stage of the digital forensics process. This is a step-by-step analysis of each stage looking for potential weakness that might result in a failure. In some cases, the competent use of software tools or the use of visual/manual checks could be demonstrated to mitigate the identified risks. Adopted methods or software tools and scripts should follow a tailored process for the validation of measurement-based methods. In this case the Codes require confirmation of the applicability of the validation and a documented demonstration that a method works within acceptable performance parameters. There is a requirement in the Codes for the production of an available library of documents relevant to the authorisation of a method.

2.2.9. Reliability

2.2.9.1. The right to a fair trial and the presumption of innocence. Digital evidence is the result of scientific methodologies and tools which ensures that "its authenticity and integrity can be validated".

Stoykova (2021) examines the unaddressed threats to the presumption of innocence with respect to technology assisted investigations [246]. The use of technology in this context must be evaluated against fair trial and reliability standards in contrast to the prevailing presumption of digital evidence scientific robustness and the ability to corroborate every aspect of the investigation which conceals limited accountability in digital forensics. The consequence of this situation is to undermine the likelihood that the accused will receive a fair trial procedure. The author identifies three vulnerable areas of the investigational process that might undermine procedural fairness:

The presumption of innocence in technology-assisted investigations is firstly challenged given the inappropriate and inconsistent use of technology. There are considerations on the need for transparency and accountability in digital investigations and applied reliability validation of the digital forensic techniques employed. The need for harmonisation of minimum procedural guarantees in respect to intrusive investigative measures is discussed at length.

The presumption of innocence has an important role to play in the investigation stage, where data is heavily processed and corroborated in growing amounts. Particularly problematic are cases where the suspect or accused is suffering a limitation of his liberty or privacy based on vague suspicions. For example, computer surveillance is the most intrusive investigation measure, because it interferes with the rights to privacy, data protection, and telecommunication secrecy. The European Court of Human Rights has ruled that the presumption of innocence can only be violated depending on "the importance of what is at stake". The use of technology allows to circumvent the prohibition of a reversed burden of proof by extensive use of probabilities and assumptions about "digital facts", where reliability of digital evidence is challenged on legal grounds, not on forensic science grounds. Technology-assisted investigations can result in a de facto reverse burden of proof to the disadvantage of the accused. The "miscarriage of justice" occurs not on trial, but much earlier in the investigation. Time and social pressure may result in law enforcement striving for conviction and identifying the wrong person as the criminal. The amount of data available makes it easier to "gather enough evidence against this innocent suspect [and] the error will ripen into a criminal charge". Presumption of innocence can be transposed in proportionality assessment, as to whether the probability of reliable evidence discovery is high and the detriment to defendant/suspect rights infringement is low, that the asymmetric or reversal rule could be justified. Further problems occur when the de facto reversal could infringe the rights of groups of people (targeted as suspects) or be at odds with the privilege against self-incrimination.

The need for data retention for investigation purposes is well recognised by law enforcement authorities, but fundamentally questioned and criticised within the data protection community. In the Tele2Sverige case, the Court of Justice of the European Union decided that a general obligation for collection of traffic and location data by all service providers for the purpose of combating crime is not in compliance with EU data protection legislation. In Sweden, Finland and Denmark information collected during wire-tapping or computer surveillance, which exceeds the scope of the investigation, is not regulated by law. This surplus of information could be used as evidence in another case or serve for investigation and crime prevention purposes. The European Court of Human Rights (ECtHR) has endorsed the need for secure storage and security clearance for interception material to be guaranteed. Any data which is irrelevant for the purpose for which it is obtained must be immediately destroyed, storage of evidence data after the trial must be regulated by law. Some authors argue that data retention laws are "de facto legitimizing a form of mass surveillance of citizens". Such an opinion does not account for the fact that more than half of internet traffic is encrypted. The use of technology is another factor to measure against fairness standards. The great potential of more complex and volumized data for investigation purposes could only be realized if a minimum level of data accuracy and reliability is assured.

Preferring data instead of classical policing methods not only increases the danger of erroneous and premature conclusions in the investigation, but it avoids the criminal procedure altogether. Under "technological means" the police could avoid limitations imposed by fairness standards or use transnational cooperation to circumvent domestic constitutional limitations. The use of technology may conceal the intrusiveness and significance of the law enforcement operation or cross-border cooperation. Intrusive digital forensic technology must be evaluated firstly atomistically – at each stage of the processing for fair trial compliance. There is a need for oversight of the legality of a mounting up of IT investigation measures in time (periodically) or in analytical perspective. Extensive use of technology can be used for presumption of innocence evasion and side-stepping, and can potentially circumvent the criminal procedure all together.

LEAs can use mutual assistance or mutual recognition instruments in order to acquire evidence from a country where such measures are lawful. Data synced on multiple devices, backups, and cloud storage allow the same data to be retrieved from different providers and jurisdictions. Countries apply a different standard for foreign evidence and are not in a position to scrutinize complex digital evidence processing in another jurisdiction. The Encrochat operation is an example of how little consideration is given to digital forensics reliability standards and defendants' right protection in technology assisted cross-border investigations. It is unclear who had access to the originally acquired data, how it was further analysed and filtered, and how much of it was attributed to concrete suspects. Defence lawyers have to deal with the threat of evidence forum-shopping because the prosecution services are embedded in formal *trans*-border networks.

The increased use of encryption and emerging technologies by criminals and third parties creates the need for broader LEA powers such as anti-encryption laws. Broad data access and decryption powers are not legislatively complemented with requirements for reliability and accuracy of digital forensics decryption methods or defendants' rights safeguards. Further steps in data processing after collection, specifically the legal compliance of pre-processing, examination and analysis of data in law-enforcement context is not addressed in any legislative initiative.

Technology could assist every step of the investigation process, but it blurs the lines between prevention and investigation of crimes. "Preventive" policing generally must be subject to a particularly strict "necessity" and "proportionality" test. It is not realistic to assume that forensic experts can limit their collection methods to relevant data from the beginning. Analysis techniques become more reliable with a larger data set, which perversely is more privacy intrusive. For example, advanced statistics give promising results in authorship attribution and detecting cyber bullies or predators online. But require increased monitoring of social messages and chats and a significant amount of sensitive data for training the algorithms. This raises concerns about the accuracy, optimization, and validation of the implemented algorithms. The notion of a "reasonable suspicion" is insufficient and imprecise to satisfy forensic data analysis. The proportionality principle and balancing tests are notoriously vague and risk becoming completely impractical for scrutinizing digital forensics processing. In the absence of a legislative approach, such a complex legal evaluation is transgressed to law enforcement, police or digital forensic specialists, contrary to the presumption of innocence and the rule of law.

2.2.9.2. Old procedural guarantees vs. new digital evidence processes. Evidence on trial must be produced in the presence of the accused at a public hearing with a view to adversarial argument. The burden of proof requires also the prosecution to take "positive steps" for disclosure of evidence and respect the defendant's rights. In Barberà [247], the prosecutor argued that due to the volume of data and problems with reimaging the data, the defendant should only be provided with the data selected for examiner's files. The Court's emphasis on the importance of a procedure to challenge digital evidence on pre-trial is a sign of the erosion of the orality trial guarantee. The trial guarantees such as the principle of orality, disclosure and cross-examination of digital evidence are equipped to examine only the results of digital forensic processes in relation to the case. In most jurisdictions there are no clear or effective procedures to challenge expert reports or to examine the reliability of scientific findings. The use of digital forensics in criminal investigations shows deficits and a lack of solutions for validating tools, examiners, and methods as well as documentation for a reliability assessment. An examination of the equality of arms principle in the context of evidence gathering with an international component concludes that as a safeguard for the accused he has to be able to gather evidence by himself or at least passively, with the assistance of law enforcement authority.

2.2.9.3. Digital forensics – a threat to the presumption of innocence. Evidence rationalists see the need to complement the trial-based evidence evaluation with intellectual developments in adjacent forensic fields, standards for nonadjudicative decisions involving a fact-determination especially on pre-trial phase, and the extra-judicial significance of the presumption of innocence. Since digital evidence is the result of machine-human interactions, standard procedures for digital forensics must mitigate both machine and human errors. The enhanced use of automated tools to acquire and analyse digital evidence creates the false perception that technology mitigates errors and bias. Authors examine multiple biasing factors in digital investigations such as exposure to case-irrelevant information, base rate expectations from previous investigations, or failure to evaluate competitive hypothesises.

Errors related to many digital forensic activities are "systematic in nature and no statistical error rate exists". Currently, there is no standard in digital forensics for "calculating error rates for both tools and specific procedures". Cross-verification of results based on documenting the methods and tools, and the examiner interaction in the process is often more reliable than calculating statistical error rates.

2.2.9.3.1. The erroneous concept of "digital forensic investigation". A body of digital forensics literature has introduced the term "digital forensic investigation". Digital forensic investigation is defined as "the process to determine and relate extracted information and digital evidence to establish factual information for judicial review", that is identical to the traditional definition of forensic science. Forensic science is not dealing only with comparison questions, but also involves searching for evidence, identifying it, and reconstructing events. In DFI, the investigation objective is to present evidence admissible in court, but this is not an objective of digital forensics as a science.

The artificial separation of the physical and digital investigation is confusing and does not reflect reality. Digital forensics process model is suitable for standardization because it aims to ensure scientific validity irrespective of jurisdiction. Investigation is a process that develops and tests hypotheses to answer questions about events that occurred. Investigators can search and observe digital traces and form hypotheses about the case. However, they lack competence to attribute, evaluate, interpret, and reconstruct digital traces. A clear separation between investigation and digital forensics as a science, especially with respect to the European Union efforts for harmonisation and cooperation in criminal procedures is advocated.

2.2.9.3.2. Reliability crisis in digital forensics. Inference about digital evidence can be highly inaccurate if the presumption of innocence is not reinforced at an early stage of the investigation. In the examined probabilistic or falsification approaches "guilt, is measured by the relative amount of evidence for or against it or by subjecting the hypothesis to a variety of tests" [248]. European Court of Human Rights case law repeatedly confirms that exclusionary rules on evidence do not form part of the European Public Order. The introduction of presumption of innocence-based evidence rules at the investigation stage benefits quality assurance and reliability testing, which reduce the need for exclusion. Use of technology to assist investigations requires a scientific validation that can cope with the fast developments and changes in the domain and is easily verifiable by the court on trial. The presumption of innocence does not mean that someone is innocent or that they are likely to be found guilty. Inference about digital evidence can only be probabilistic in nature, as it comes from sources that are not completely credible. This raises the question of the reliability of the predictive (statistical) evidence versus the requirement of a trace-based fact-finding. Such a probability analysis could be taken into consideration when developing data retention rules or allowing enrichment of cold cases with new information.

The interpretation of digital data by law enforcement agencies and digital forensics tools for the purpose of the investigation must be made accountable and part of the validation procedure. Reasoning about the evidence during analysis and any assumptions made must be documented. Insufficient individualization and accuracy testing of the digital evidence can potentially result in fairness violations.

2.2.9.4. Current approaches to address threats to fairness. The common understanding of the burden of proof as a mechanism to allocate the risk of error in the criminal process, is dependent on accountability and integrity policies for all tools, processes and services supporting an investigation. The benefits and drawbacks of proposed legal and non-legal standards to ensure accuracy and fairness of procedure in different forensic disciplines should be outlined.

2.2.9.4.1. Reliability evaluation by the court. Given the uncertainties about digital data, its reliability on the source or during forensic processing must be never presumed but proved and recorded. One proposed solution was for the court to do a special evaluation of reliability as in other cases when scientific evidence is in question. The US Supreme Court formulated Daubert's rule which was the first decision to promote court criteria for evaluating expert evidence similar to those that scientists use. Most state courts in the US have rejected Daubert, which places judges as "amateur scientists" to evaluate complex scientific findings in a checklist fashion. This view is a misinterpretation of Daubert's objectives and does not account for the judge's pivotal role in scrutinizing the use of science for court proceedings. Judges have their important role in verifying the forensic evidence reliability, but they cannot and must not perform scientific validation of digital forensic methods and tools. It is argued that a "reliability-based admissibility standard for expert opinion evidence" is unlikely to generate the changes required to improve the quality of incriminating forensic science. Standards and formal procedures help forensic scientists to report their scientific findings clearly, allowing judges to understand and evaluate them in a routine manner. Digital forensics must not rely on trials to determine the validity of its methods and tools. Judges may stop improving certain procedures and focus on others which are known as accepted by the court. A further proposed solution is evidence reliability to be evaluated by experts before it reaches court. Data for validation and reliability assessments must be generated as part of the digital forensic process in a practical and expedited way.

2.2.9.4.2. Reliability validation during investigation. An argument is presented that taking the relevance and probative value of expert opinion as default, does not meet the requirement for procedural accuracy which presumption of innocence has to enforce. The central argument is that the standard and burden of proof can and do fail to protect innocent defendants, if not supported by procedures for error mitigation throughout the investigation. A suggested advisory panel will increase bureaucracy and formal compliance paperwork. It is questionable whether current digital forensic techniques would produce the required reliability assessment information. The panel should only give an opinion to the judge at trial, but this could strengthen the expert's evaluation to the extend where the judge's evaluation becomes a formality. Since this solution is resource demanding, it could be used in more complex digital forensic cases. It is suggested that judicial oversight could be part of the digital investigation process, as well as independent experts in data protection, IT security and digital forensics. Both propositions require further research, especially with respect to the lack of standards of procedures for working in dark web spaces. In some countries, it is accepted that an expert can demonstrate competence and scientific soundness of her/his method by referring to peer-reviewed articles or previous work. Expert impartiality in such cases may be questionable due to the small guild numbers in digital forensics and the quality of the reports may vary hugely. Some questions about digital artefacts require legal and multidisciplinary evaluation, which may induce judges to take a passive role in the cross-examination process. Having two digital forensic examinations (for the prosecution and for the defence) goes against procedural efficiency and is impossible in terms of resources, time, or trained personnel. There is a need for further research into the active participation of the defence during the digital forensic examination during the investigation. Legislation does not enforce such reliability assessment and standard validation procedures, which results in routine admission of digital evidence that does not meet forensic evidence standards.

2.3. Standards

2.3.1. Quality standards for digital forensics

Digital forensics is the process by which information is extracted from digital systems or data storage media, rendered into a useable form and processed. The scope includes aspects such as remote storage and systems associated with computing, imaging, image comparison, video processing and enhancement (including CCTV), audio analysis, satellite navigation, communications. Ensuring that digital forensics, like all forms of forensic science, is delivered to the appropriate level of quality for its use in a Criminal Justice System is not in itself contentious. Quality of digital forensics has been the subject of intense debate over the last few years. The Forensic Science Regulator's Codes of Practice and Conduct (2017) allow for use of novel methods prior to accreditation provided that the customer understands the extent to which it is validated prior to commissioning [249].

Some authors argue that, provided clear technical specifications are set, verification and validation requirements in ISO/IEC 17025 can be achievable for digital forensic technology and other authors argue against "trading justice for cost savings", given the potential impact of digital evidence on individuals' freedom. It has been observed that digital forensics could have built on learning from established disciplines, but arguably has the least robust quality management procedures. The counter argument is that ISO/IEC 17025 is ill suited for digital forensics and the Regulator's validation requirements are placing a "near unmanageable" burden on digital forensic providers. One proposal is that there should be differentiation between technical processes and scientific processes which helps determine what knowledge, training and other elements of quality assurance are fit for purpose.

There are differences between the more routine activities, such as evidence acquisition and preservation, and the more complex digital forensic activities such as interpretation and evaluation. In the UK, ISO/IEC 17020 will be required for screening, capture and preservation or analysis of data from a device conducted at scene (including but not limited to Servers and Routers) from October 2020. The workload associated with validation can perhaps only be tackled by national and/or international collaboration.

The necessity for quality standards in digital forensics is supported by evidence. Numerous technical, administrative, and management findings were presented. No matter how good the examiner, the system will not function properly if he or she is not provided with the necessary tools, resources, and regular training. Accreditation is a realistic procedure that leads to demonstrable improvement. ISO 27037 provides a framework for achieving certain of ISO/IEC 17025's technical standards. However, it is not an accreditation standard; rather, it is a technical advisory document. Focusing solely on technical criteria does not necessarily result in enhancements to the quality system as a whole. One argument that the Regulator denied was that the Regulator might modify the "should" advisory language in ISO 27037 to "must" mandatory language. Critically important is the question of whether or not the validation standards in ISO/IEC 17025 are insurmountable in a dynamic field like digital forensics. Other authors have reached the conclusion that the absence of unambiguous requirements statements (and related lack of transparency on those criteria) results in a gap in the proof of accuracy for tools and procedures. However, there are enhancements that might be implemented to facilitate validation and verification. The authors begin with the premise that it is crucial to comprehend the advantages and disadvantages of Criminal Justice System procedures.

1. Greater transparency of technical requirements would be an improvement to the way tools and methods are used. Providers would be better equipped to prioritise development in order to meet user requirements if users defined their needs in detail. In a mature customer-supplier relationship, sharing specifications and testing data would benefit all parties by eliminating duplication of effort and, consequently, costs.
2. A repository of ground truth data that is publicly accessible and kept current as technology advances would centralise a substantial amount of effort and expenditure. It is not simple to specify what such a resource might consist of, but it is worthwhile to do so. Under the aegis of the European Network of Forensic Science Institutes

(ENFSI), a study is now ongoing that could be of assistance in this area.

3. A project to validate the performance of digital “kiosks” for use by front-line officers has recently been undertaken, following the procedure set out in the Codes. There has been much learning as organisations have undertaken validation and sharing of this should be encouraged.
4. Centralised resources for tool testing and standardization have the ability to significantly reduce the amount of labour required by businesses to design and test their products.

Accreditation does not identify the specific software version used by a technique. The UKAS evaluates an organisation’s technique for upgrading software, identifying risk, and performing revalidation as necessary. A technique-based approach, as opposed to a device-based one, that aims to discover the common procedures involved in examining a wide variety of unique devices may merit additional investigation. The Chartered Society of Forensic Sciences is in the process of creating a “Generic Quality Management System.” The Regulator is coordinating with the government to investigate if such a programme could be subsidised to decrease participant fees. The authors urge for the continuous integration of digital forensics with other fields of forensic science where decades of research have been devoted to the creation of scientific techniques to evaluating evidence.

2.3.2. Imprecise language

The author maintains his earlier judgement that the materials under consideration lack what a computer scientist may perceive to be technical criteria. A perceived necessity to establish Standard Operating Procedures rapidly and a natural inclination to chronicle what was being done at the time may explain the absence of requirements. ISO/IEC 27042 promotes the use of “atomic” techniques, in which decisions are made between rather than within the procedures. Due to the probable difficulties of generating adequate tests for all possible combinations of branches, such methods are inherently complex and challenging to validate. This author, together with others, designed the set of three standards to provide a comprehensive end-to-end guide that is complimentary to and compatible with the principles of the Forensic Science Regulator’s standards [250].

2.3.2.1. Definitions. The author identifies a discrepancy between the Software Engineering and Calibration and Testing requirements definitions. In the former, the statement of need includes limits and conditions, but in the latter, the language is more generic.

The purpose of the validation procedure is to confirm that digital forensic methods meet declared needs. The Functional, Performance, Interface, Process, and Non-Functional Requirement Categories of ISO/IEC 27041. The functional and performance requirements are completely technical, as they pertain to the method’s operation and function. Depending on the type of interfacing required, interface requirements may be technical or non-technical.

ILAC G19 makes recommendations for the delivery of laboratory services to the public and private sectors. The customer is the individual or entity that requests the forensic unit to undertake all or a portion of the forensic science procedure. If work is required by law (e.g., a court order), the findings of examinations and tests may be shared with the judicial system. Validation is the evaluation and supply of objective proof that specific conditions for a particular intended application have been met. ILAC G-19 provides much more guidance on how validation should be undertaken. It is evident that client requirements are only one factor to consider when determining how to validate a process; scientific rigour, correctness, and precision must also be taken into account.

The Forensic Science Regulator’s codes of practice and conduct contain 11 pages of guidance on validation of methods. Within these pages, there are 64 sub-clauses. The author has concerns about the use of the term “verification” in the Forensic Science Regulator’s codes. In software terms, the term is used in a way which is inconsistent with accepted use in another relevant domain. There are hints that the concept of an end-user is not restricted to the Criminal Justice System. It is also noteworthy that the section on ‘Technical Requirements’ in the regulator’s codes deals only with personnel, including qualifications but excluding competence.

The author contends that the Forensic Science Regulator’s guidance on how to assess whether a method or tool is fit for purpose tends to allow the functional and performance requirements defined in ISO/IEC 27041 to be ignored for the purposes of validation. Although internal considerations for of reliability and functionality are clearly mentioned, the emphasis is very much on the “customer” throughout.

2.3.2.2. Argument. The use of overloaded words and the emphasis on ‘end-user’ Criminal Justice System customer needs has produced a situation in which it is conceivable for an organisation to be accredited yet for the accredited processes to be substandard. The existing approach has made it possible for inefficient methods that are unable to be validated to give the appearance that they are “suitable for their intended purpose.” There is a need to take a step back and analyse guidance for language and meaning consistency, as well as to examine the concept of “customer” or “end user” in context more closely. This is especially significant for in-house law enforcement laboratories, because the high level of integration into the investigative and prosecutorial culture may exacerbate the confirmation bias problem. Reviewing the nature of the customer’s instructions and, if necessary, adapting them to meet the requirements of the real end-user (Criminal Justice System) should be a necessity for organisations that are tasked with performing work.

2.3.3. Consistency

The Science and Technology Select Committee issued a severe assessment of the current state of forensic science in England and Wales in 2019. According to the committee, there is no uniformity in how the 43 Police Authorities contract forensic services. Since the government’s Forensic Science Service was disbanded in 2012, traditional forensic analysis work has been conducted under a paradigm that might be loosely described as decentralized. The digital forensics industry may be experiencing a problem with consistency, which raises questions about quality assurance and management across the field and the work it generates. In essence, the capability of a forensic provider, their knowledge, expertise, and operating practices can vary from region to region, and while all will undoubtedly attempt to conduct investigative work to the best of their abilities, there is no formal evaluation of how this is accomplished or how good their ‘ability’ is [251].

There are currently few uniform factors in the field of digital forensics, and divergent methodologies can persist throughout the entire investigation process. It may be feasible for the same crime (and surrounding circumstances) to be hypothetically committed in two distinct places and have different investigative findings due to unequal case handling. The progression of an investigation will be influenced by factors such as the type of offence, triage implementations, device seizure and backlog-management rules, and any locally determined evidence thresholds. In theory, location should not be a factor that leads to inconsistent investigations, but in practice, this may be the case. It may be the case that performance measures for a certain organisation are imposed by pressing local concerns or efforts to regulate specific “priority offence kinds.” The very act of such attempts will very probably affect the procedural priority given to such cases over others in the same region. Even national investigations of the same sort of crime may take different tactics based on local crime combating activities.

When it comes to staffing, there will inevitably be a conflict between cost and experience. In all organisations, there is a need to strike a balance between the two in order to determine the optimum working ratio. Importantly, no organisation is likely to be sustained if it consists of only one of these populations. There is no “ideal ratio” for staffing a digital forensics lab, as different organisations may take different approaches. Failure to identify and then implement the requirement for training and development poses a danger.

In addition to their training and education, digital forensics professionals are dependent on their instruments in order to do their duties. Ideally, every lab should have every forensic instrument available on the market (as some may have extra capabilities than others). However, in many instances, this is not financially feasible. Because not all staff members are familiar with every accessible tool, acquisition may also be influenced by staff knowledge and those who have been (or will be) taught to use it.

Variations in setup and the manner in which practitioners choose to employ them may result in distinct outputs, which may influence case outcomes. In recent years, the interpretation of digital forensics results has been the subject of much discussion and represents one of the field’s greatest problems to date. There is no standard way for evaluating the probability of digital evidence, and the study of cognitive bias is just beginning. Evidently, digital forensics must resolve language and definition usage conflicts in textual evidence. It would be inappropriate for this article to offer no response to the aforementioned difficulties.

It is difficult to achieve a unified strategy to digital forensics across England and Wales. It must initially occur at two primary levels: laboratory facilities and investigative procedures. Harmonized facilities bring us one step closer to consistency by allowing all organisations to potentially do the same level of analysis (knowledge permitting). It also prevents variability in examination restrictions, mobile device forensics being the greatest illustration. Harmonizing the forensic process across all locations and organisations is essential for achieving uniformity. This necessitates open and constant channels of communication between all parties in order to establish and agree upon appropriate practices, then adhere to them.

The exchange of experience and knowledge has been considered advantageous for some time, but its execution is not without its problems. The field of digital forensics in England and Wales requires a census-style collection of information on those currently operational in order to determine where everyone stands. In the future years, digital evidence is projected to appear in more criminal trials than any other forensic kind. As its rapid expansion continues, now is the time to evaluate and address evident difficulties to secure its future as a valuable and trustworthy forensic science.

2.4. Trust

Forensic service providers in all sectors are straining under the ever-expanding demand for digital evidence. They are struggling to keep pace with the rapidly growing number of investigations that have a digital nexus, often involving voluminous and varied data sources. At the same time, forensic service providers around the world are under increasing scrutiny for mistakes [252].

There is a growing trend for plaintiffs to find weaknesses in evidence handling procedures and chain of custody documentation. This approach to undermining digital evidence can be performed by non-specialists equipped with a checklist. They are more likely to find mistakes when forensic service providers are buckling under escalating caseloads and budget constraints. This trend diminishes trust in digital evidence, processes, methods and practitioners, which is detrimental to criminal justice and negatively impacts the private sector in civil matters and data breaches.

Previously in this journal (Volume 32 - Quality standards for digital forensics: Learning from experience in England & Wales), the UK Forensic Service Regulator highlighted problems experienced by forensic service providers and discussed ways to improve digital forensic science. These improvements include how to validate and verify digital forensic methods more effectively, and how to properly introduce completely novel methods rapidly.

To reinforce reliability and strengthen trust in digital evidence there is a need for strategic solutions to deal with the increasing demand, data and scrutiny.

Forensic service providers are employing different strategies to deal with digital evidence challenges.

One strategy prioritizes quality by effectively rationing forensic services, only supporting high priority investigations. This approach takes ‘investigation delayed is justice denied’ to a new level, simply denying justice by not conducting a thorough investigation.

Another strategy prioritizes timely information by putting digital forensic capabilities in the hands of non-specialists, such as easy to use kiosks for extracting limited information from mobile devices. Although this approach can be useful for investigative purposes, it raises multiple risks, including missed and misinterpreted digital evidence as discussed in the earlier editorial (Volume 31 e Trust in Digital Evidence). Ultimately, non-specialists require support from a specialised forensic advisor to treat and evaluate digital evidence properly.

Integrating forensic advisors throughout an investigation, from crime scene to testimony, is a strategy that was addressed in the previous editorial (Volume 32 e Crisis of Opportunity). This approach is more expensive than employing non-specialists but is less likely to result in rookie mistakes or overlooked evidence due to lack of knowledge and experience. However, this approach is not sufficient on its own.

Whatever general approach is taken, if there are doubts or disagreements about the quality of interpretation of digital evidence, it is generally advisable to obtain a second expert opinion.

These mounting challenges call for integration of technology, processes, personnel and research.

The demands for timely information, specialised expertise, quality assurance and scalability can all be satisfied by systematically combining knowledge from practice and research and connecting people working on digital evidence. These are the objectives of the growing CASE community (caseontology.org) and “OK Hansken” program (hansken.org).

This solution consolidates knowledge and data from different sources within a scalable system that automates routine processes, maintains detailed audit records, builds in testing and validation, and provides non-specialists with speedy access to information.

Forensic advisors can play an integral role by contributing their expertise both in codified form (e.g., developing new plugins) and personal interactions (e.g., responding to specific questions). In addition, this solution can be augmented to align with emerging standards in evidence evaluation, and to provide more advanced data analysis capabilities.

Such an integrated solution makes more effective and efficient use of resources, and helps reduce case backlogs, missed evidence, unscientific outcomes, and miscarriages of justice.

2.4.1. Zero trust

In digital forensics, the significance of trust has receoved little attention. Throughout investigations, digital forensics may not expressly account for trust manifestations. A possible contributing element is the substitution of this mindset with an assumption that computer evidence is credible unless shown otherwise. There is a potential that a “third method” will replace this presumption [253].

The paper will show that the phenomenon of trust is fundamentally linked to the processes involved in producing reliable digital forensic evidence. The specific aspect of potential tampering of digital artefacts will be proposed as an example of an aspect of digital forensic investigations that is contingent on trust. Situational trust is modelled as a constant value which can be quantified. The accuracy of such quantification also has an influence on the amount of risk being undertaken by the trusting entity. In example above, erroneous trust placed in the accuracy of digital forensic tool used for extracting the evidence from the UAV would be an example of the sorts of errors that both Casey (2019) [254] and Reedy (2020) [255] discuss. These errors are difficult to observe and explain, adding to the overall uncertainty of the investigation and undermining the soundness of the scientific method.

More work is needed by new digital forensic techniques to verify their accuracy the lack of integration between digital and physical forensics is lamented. Digital artefacts recovered and analysed during a digital forensic investigation can be tampered with before an investigation starts. This is often referred to as 'anti-forensics' in the literature and continues to be a major challenge to the field. It is unlikely that this type of situation would be accepted in physical forensic disciplines.

If artefact tampering activity is not identified, it is inevitable that this will result in any investigation producing incorrect outcomes. This can seriously undermine its reliability. If digital evidence cannot be proven to be authentic and reliable, then it is meaningless to present it in a court of law. In the absence of adequate tooling being available to digital forensic investigators to identify artefact tampering, some attempts have been made to produce generalised techniques. The sheer number of tools available is a limitation to this work.

One method relies on knowing what all these attacks would look like prior to the start of an investigation, whereas another proposed approach uses signatures of known anti-forensic tools in order to identify their use on suspect systems. A mathematical approach which could be used to identify digital artefacts that may have been tampered with. No publicly available tool was produced as a result, limiting the applicability of this approach to a wider community of practitioners. It is clear that trust is an important component of digital forensic investigations, however it is rarely, if at all, explicitly considered. This paper proposes a new model for digital forensics in order to increase the amount of trust placed in features such as provenance and device features.

"Definition. Zero Trust Digital Forensics is a strategy adopted by investigators whereby each aspect of an investigation is assumed to be unreliable until verified."

This section will examine the Zero Trust security strategy which is gaining popularity in digital forensics. A definition of 'Zero Trust Digital Forensics' will be given, and a proposal made for how Zero Trust principles could be applied to the specific risk of digital artefact tampering. In 2020, the United States National Institute for Standards in Technology (NIST) produced a special publication titled 'Zero Trust Architecture'. NIST (2020) stipulates that Zero Trust is not in fact a single architecture, but instead a set of guiding principles upon which workflows, systems and operational processes can be designed. Zero Trust is described as a mindset, with three guiding principles: 'Never Trust, always verify', 'Assume breach' and 'Verify explicitly'.

The US National Security Agency (NSA) also published a report titled 'Embracing a Zero Trust Security Model'. Digital Forensics is a strategy adopted by investigators whereby each aspect of an investigation is assumed to be unreliable until verified. The logical consequence of this is that all aspects of a digital forensic investigation need to be verifiable. Zero Trust Digital Forensics can be thought of as a strategy rather than a model to be followed by practitioners.

The concepts behind it are intended to be incorporated into every part of an investigation, regardless of the specific process or methodology being followed. When the Definition of Zero Trust Digital Forensics is applied to artefact tampering, each artefact is assumed to be completely unreliable before being subjected to one or more verification techniques. These techniques are likely to be more specific and so additional thought is needed to understand how and when to apply multiple techniques.

Common digital forensic methods do not explicitly consider the phenomenon of trust and have an inconsistent approach to dealing with its consequences. The aim of Zero Trust Digital Forensics is to increase the reliability of such investigations by identifying where trust manifests and then treating all of these features as unreliable until one or more verification techniques has been applied.

Digital Forensics requires all parties involved in investigations to identify and evaluate the role of trust in all aspects of their work explicitly. In some cases, this is already a well-understood concept, an example being the ability for digital data to change as a result of forensic actions. But identification alone is unlikely to substantially increase reliability. Digital Forensics as a community should inspire and motivate research into ways of making such a strategy realistically attainable. For it to start to become useful, more research is needed into both the wider application of current verification techniques, as well as new and more efficient verification techniques.

An understanding of the scale of these additional means in practice and how they can be minimised, for example through automation, could be a motivation for further work. Consideration is now given to how the principle of multifaceted verification of digital artefacts can be applied. It presents a small sample of the existing techniques for verifying JPEG files, but some initial observations can already be made. In order to follow a Zero Trust Digital Forensics strategy, an investigator would need a verification method for both the PUB file and the JPEG image in question before either would be considered reliable. As it stands, as far as has been established by the research conducted in this paper, no techniques have been published which can be used for verification of this artefact.

This highlights a further issue, namely the coverage that existing verification techniques provide for the different types of artefacts that may be encountered by practitioners. Further work is required to standardise verification techniques for both the PUB file and the JPEG file. It would appear prudent to provide some means for standardising and publishing the output of research into verification techniques. A further improvement would be to ensure that such research results in publicly available tools for use in practice, whether this be in standalone format or as plugins for more common tools.

2.5. *Technical reliability*

2.5.1. *Reliability through measurement science*

The formal definition of validation does not specify the quantity or quality of objective data needed to demonstrate the reliability of a process. Validation can be measured at a foundational level to address questions of whether a method or tool can be used to reliably perform a task, and at a laboratory level to show that the laboratory can reliably implement a particular tool or method. A validation study should quantify accuracy, repeatability, reproducibility, uncertainty, and error rate in measurement [256].

The concept of accuracy in digital forensics is relatively well-understood at a high-level, but the field lacks low-level measurement specifications evaluate process accuracy. Once specifications and reference data are available to assess how well a particular tool or method can correctly perform measurements, it is possible to estimate the tool's accuracy.

Repeatability and reproducibility are concepts that evaluate the ability to replicate a measurement during repeated analysis. Digital forensics process repeatability and reproducibility is relatively well-understood in the context of a single digital forensic tool as applied to the same target device multiple times. However, without low-level measurement specifications, the field cannot define cross-process reproducibility.

Uncertainty and error rate are concepts that evaluate the estimated degree of confidence in a reported value. The sources of potential error and uncertainty are understood as primarily originating from problems in the algorithms used during analysis. Quantifying the contributions of those factors remains elusive and difficult.

Formal validation needs to occur at several levels to quantify the reliability of a forensic process. In the context of digital forensics, the first level is an assessment of the tool's reliability (Garfinkel et al., 2009). The second level of assessment is at the method level, and is whether a standardised sequence of steps leads to a reliable result.

Closed box studies can be used to evaluate the reliability of a subjective methodology, or an incompletely specified methodology. A closed box study treats the examiners as a collective group to obtain method-level data. Blind proficiency testing considers each examiner as an individual to obtain more granular data. Digital forensic examiners increasingly rely upon digital forensic tools to process and analyse digital evidence. Without a discipline wide definition of "validation," the term is applied inconsistently.

NIST performs a very limited amount of digital forensic tool testing, and maintains a small corpus of digital device images. The digital forensics community needs to curate reference data that represents the full range of conditions expected during digital forensic analysis. This provides the discipline a set of uniform metrics to compare between tools. It also enables peer review and reproducibility of testing and provides some measure of traceability during validation testing. Unlike the DNA reference standards used in forensic biology, it is extremely difficult to obtain real system images to use for validation due to privacy and legal concerns.

Type An uncertainties in digital forensics are omissions or incorrect associations detected during validation studies while Type B uncertainties are undetected flaws in the implementation of the tool phase, problems correctly associating data internally or externally, or result from incomplete understanding of observed artefacts. Type B errors can be caused by a lack of data or models allowing the examiner to properly quantify the support for competing causation hypotheses. A laboratory could use hash values to get a rough estimate as to how often the method induced change in, say, boot files, system files, and user-space files depending on the evidence handling method.

Possessing statistical models to better comprehend artefacts could revolutionise the field of digital forensics. This level of insight into what could or should be seen during a particular occurrence enables the validation of associations produced by a digital forensics tool. Understanding the relationships between artefacts could improve the capacity to procedurally generate realistic reference data.

2.5.2. *Presumption concerning dependability*

The authors consider the condition set out in section 69(1)(b) of the United Kingdom's Police and Criminal Evidence Act 1984 (PACE 1984) that reliance on computer evidence should be subject to proof of its correctness, and compare it to the 1997 Law Commission recommendation that a common law presumption be used that a computer operated correctly unless there is explicit evidence to the contrary (Law Commission Presumption). It is understood that the Law Commission Presumption prevails in current legal proceedings. However, the authors demonstrate that neither section 69(1)(b) of PACE 1984 nor the Law Commission presumption reflects the reality of general software-based system behaviour [257].

In 1997, the Law Commission considered the rationale behind section 69 of the Police and Criminal Evidence Act 1984. Section 69(1)(b) of PACE 1984 stated that a statement in a document produced by a computer shall not be admissible as evidence of any fact stated therein. The Law Commission's PACE section 69(1)(b) provides that a document produced by a computer may not be adduced as evidence unless it is shown that the computer was working properly. In electrotechnical terms, "reliability" means "ability to perform as required, without failure, for a given time interval, under given conditions". Thjere are no non-trivial software-based system which can be shown to be reliable in the absolute sense given in the IEC definition.

Most software contains defects, at the rate of generally between 1 and 100 defects per 1000 lines of source code (kLOC). The authors expressed surprise to read Professor Tapper's suggestion that the Tapper Condition categorises "most computer error", even allowing that he was writing in 1991. The condition that a computer error "is immediately detectable or results from error in input data" does not appear to hold in general. In R v Cahill and R v Pugh, the assumptions of the Tapper Condition led to a criminal trial, which collapsed three years later. This case revolved around a joint IT–operational technology system that corrupted, creating fallible evidence that had not been noticed before.

In the absence of evidence to the contrary, courts will presume that mechanical instruments were in order at the material time. The Law Commission cites relatively uncomplex operational technology systems such as speedometers, traffic lights, and intoximeters as examples of such systems that can mostly satisfy the Tapper Condition. Evidence is presumed to be information, and is therefore overtly IT, although system logs may constitute such evidence. These safety properties, such as not showing "proceed" simultaneously in two conflicting directions, are generally determined by independent inspection agencies. Such rigour is not generally applied to large IT systems such as Post Office Horizon, the Law Commission concludes. Section 69 of PACE 1984 was repealed by section 60 of the Youth Justice and Criminal Evidence Act 1999. Since then, the presumption mentioned by the Law Commission in its recommendation 13.23 has prevailed as a rule of evidence. However, the authors do not consider that it appropriately considers the actual behaviour of all software-based systems.

The quality of software is traditionally taken in software engineering to be correlated with the density of (discovered) defects. A defect is, according to the influential definition used at Carnegie Mellon's Software Engineering Institute, "any flaw or imperfection in a software work product or software process". In the numbers cited below when considering lines of executable source code, 1 kLOC represents a very small program. Typical operational technology and IT software has many kLOCs, even thousands of kLOCs, and hence very many defects. Others have reported on the defect densities in safety-critical industrial software. Even the top 1% of programmers still injected 11 defects per kLOC. The current international standard for the functional safety of software is IEC 61508-3:2010. This standard classifies "formal methods" as "Highly Recommended" for the highest-dependability categories of software-implemented safety function. It does not amplify on which methods might be meant, or which use of them would be helpful or appropriate.

Any IT system of practical size will have displayed faults many times since it was first put into service. Most IT systems will have had very many faults corrected through "patches" or new releases of software. No programmer could credibly claim that they know that they have corrected the last fault in their software. It is suggested that no competent programmer would even make such a claim. In Bates v Post Office Ltd (No 6: Horizon Issues), Fujitsu maintained a Known Error Log (KEL) and kept records of reported potential anomalies and follow-up action, including remedial measures.

Fraser J was able to arrive at a judgement concerning whether the claimants might be right that anomalies in the Horizon system, and not their own malfeasance, caused the problems they were accused of by the Post Office. An IT system which serves a commercial application, but does not adhere to standard requirements within that application, can be regarded as generally less dependable. An exception to this inference may occur when the IT system is accompanied by documentation and evidence that explicitly lists the application requirements the system does and does not address.

The authors explore how this view permits a number of inferences regarding the inappropriateness of the Law Commission's remark at 13.23: "We are confident that the presumption of proper operation applies to computers … "

This phrase seems to imply that unless there is clear evidence of a software error, it should be assumed that a software error did not cause an undesirable outcome. In an ironic twist, a badly designed system that is susceptible to the impacts of bugs may also be unlikely to record trustworthy proof of its own behaviour.

In the specific example of evidence regarding the dependability of IT and non-trivial operational technology, the authors believe a court must make an opinion about the following three issues, based on the present level of knowledge in software engineering:

1. A presumption that any particular computer system failure is not caused by software is not justified, even for software that has previously been shown to be very reliable.
2. Evidence of previous computer failure undermines a presumption of current proper functioning.
3. The fact that a class of failures has not happened before is not a reason for assuming it cannot occur.

2.5.3. *Reliability assessment in Norwegian police*

Norway has one of the highest human development value indices in the world with 96.5% of the population connected to the internet. Cybercrime and the use of ICT in crime in general has increased in Norway for many years. Little is known about how investigative reports preserve chain of custody information in order to audit the digital forensic examination performed in each case. This study was limited to the minimum digital forensics process - acquisition, examination, and analysis [258].

Most digital forensics techniques have not satisfied the criteria of known error rates and a lack of resources and data sets for testing is identified. This study develops a practical reliability framework based on minimum documentation requirements for the methods, tools, and interaction of examiners across each stage of digital evidence acquisition, examination, and analysis. The Reliability Validation Enabling Framework defines the minimum requirements at technology, method, and application level that can satisfy a validation procedure at any stage of the digital forensics process. The documentation must include the name, version, configuration, and functions used. The method in this study describes the minimum information that must be documented in order to enable reliability validation of any processing stage in a digital forensics investigation.

The reliability validation criteria and evaluation requirements were used to evaluate the data set and assess the reliability of the current digital forensic work in randomly selected cases from the Norwegian police. The study was based on reports collected from a random set of criminal investigations in Norway. The case population was constructed from homicide and sexual assault cases.

The reliability validation methodology was divided according to the minimum digital forensics process, i.e. acquisition, examination, and analysis. Each reliability criteria was assigned a value depending on the data in the reports. Devices from which data is acquired must be sufficiently described in order to trace the data to its source. The acquisition space should be documented as different acquisition methods can acquire different parts of the device data. Specification of the function, file format and integrity verification are the minimum characteristics necessary to validate the method used for acquisition. Examination output and value are crucial to enable acquisition validation and ensure that the examinations and analyses are performed on a true copy of the original data. Reporting the date and time of acquisition enables the evaluation of what technology and methodology was available at the time, and impacts the justification for using it. Digital forensic tools can have bugs and errors, and the functions used might not be suitable for the task. In addition, correct functioning algorithms might produce erroneous outcomes if the wrong parameters are set. A justification of selected examination by the examiner ensures that what was done was proportional and did not exceed the scope of authorisation.

Information about acquisition was available for 75 out of the 187 devices (40%). The information was scattered across reports describing single device acquisition, acquisition of multiple devices, or reports concern both acquisition and examination. 10 reports included photographs of the device screen or screenshots. No acquisition report was found for 106 (57%) devices. The study found that only four devices were documented according to the requirements for a unique device identification.

Not all reports concerning acquisition referred to the assigned inventory number. A device description (e.g. manufacturer or model name) or an IMEI or serial number was often used instead. Both commercial and open source tools were used for data acquisition, with MD5 and SHA1 used for hash values.

17 out of 21 cases (81%) contained at least one examination report. Of the total 124 reports, 67 (54%) were categorised as examination reports. While 80 of the 187 devices (43%) were examined at least once, some devices were examined more than once leaving 107 devices not reported as examined. Out of 104 reported examinations, 90 did not describe any of the actions performed while 14 gave a partial description. None of the reported examinations gave sufficient information on the method used to enable the process to be repeated.

In 16 examinations, the examination space was described as application data (e.g. call logs or communication data) without further specification of the data location or forensic path. Findings were primarily provided through descriptions or partial reproduction of the content data (e.g. table and pictures) 33 examinations described or reproduced relevant content data, but provided no forensic path or reference to its origin. One examination concluded that the data on the device was irrelevant based on the last change date/time of the device.

53 examinations of digital artefacts provided data without stating explicitly that nothing of relevance was found. None of the analysis reports provided sufficient information for a reliability assessment. References to devices were not consistent either in their existence or format. The absence of reference to previous stages made it hard to establish the digital chain of custody and chain of evidence. Multiple manual examinations (live forensics) were performed with no justification or detailed description.

There were no audit trails that could be used to trace the processing steps backwards for a particular piece of data found to be of relevance. Inaccurate terminology such as 'draining data' and 'peruse data' were used in several reports.

The use of screenshots and photographs to acquire and preserve data is not a forensically sound method of acquisition. The results show that none of the cases were sufficiently documented to enable the assessment of reliability of the digital evidence. This lack of consistency between reports makes it nearly impossible to reliably associate data artefacts with their respective data source. Digital forensics practitioners were performing single tasks to advance investigative objectives rather than establish relevance and probative value of digital artefacts via sound digital forensics methods. The risks imposed by live examinations prior to forensic acquisition appeared not to be mitigated or addressed.

A way to comply with the principles would be to justify the use of such methods and account for the possible and probable impact imposed on data integrity. A digital forensics process and reporting system can help to create an audit trail, link together and document all the process steps and actions performed in relation to the relevant digital evidence found. A study developed and proposed a practical reliability validation method based on documenting concrete reliability criteria which can be used and extended as a template to create audit trails. The study suggests that training and expertise in mobile forensics methods, tools and techniques should be a priority.

2.6. *Tool validation*

The potential use of evidence of tool verification in support of method validation to achieve compliance with the requirements of ISO 17025 and/or ISO/IEC 27041 has been previously described. There are three scenarios in which tools may participate in methods: 1) the tool is a subset of the method; 2) the method is a subset of the tool; and 3) the tool intersects with the method.

Acquisition of physical and logical data from electronic evidence can be carried out at three stages which can be defined in terms of the Association of Chief Police Officers (replaced by the National Police Chiefs' Council) principles for electronic evidence. Remote potential digital evidence sources are those that are not amenable to physical access (e.g. cloud storage, messaging servers, social media systems, corporate servers). Such sources may even require a fully online or live examination instead of an offline, “dead box” or static approach.

Computer Forensic Tools are the workhorses of any digital forensic investigation. Anti-forensic attacks aim to prevent, hinder, or corrupt the forensic process of evidence acquisition, its analysis, and its admissibility. Attacks can hide or alter digital evidence so that it not found and hence not submitted for legal proceedings, or it misleads the jury during legal proceedings.

Many studies have attempted to evaluate Computer Forensic Tools for their vulnerabilities and shortcomings. Commercial and highly reputed forensic tools are yet to be evaluated for file system anti-forensic attacks. Evaluation and validation methodologies for Computer Forensic Tools have also been researched.

Some evaluation methodologies are not feasible because they are too complex. Closed-box testing-principle-based methodology has been proposed and was later advocated by other studies. Clearly, a general methodology to evaluate digital forensic tools for all types of scenarios is not possible.

2.6.1. *Method validation guidance*

The Forensic Science Regulator’s Codes of Practice and Conduct for Forensic Science Providers and Practitioners in the Criminal Justice System (the Codes) and the Regulator has published a general guidance document on validation (FSR-G-201). This document provides guidance and advice on how the process can be applied within the digital forensics field [259]. There are no standard methods in digital forensic science. Most methods are assumed to be at least part adopted and/or adapted methods. For accreditation purposes they are generally referred to as laboratory-developed or non-standard methods.

Even if a method has been in use for some time, if there are no reliable data on the method it may need to be treated more as if it was novel. Identifying who are the primary end users of a forensic method and how it performs can help to determine if it is fit for purpose. The requirements, in their simplest form, capture what aspects of the method the expert will rely on for their critical findings. They should focus on features that affect the ability to give reliable results. The Lord Chief Justice of England and Wales has amended the Criminal Practice Directions [1] to include factors which the court may wish to take into account in determining the reliability of evidence.

These factors include the extent and quality of the data on which the expert’s opinion is based, and the validity of the methods by which they were obtained. Whether the expert’s methods followed established practice in the field and, if they did not, whether the reason for the divergence has been properly explained. If admissibility is challenged and these factors have not been taken into account, the evidence may be excluded from the proceedings. The end-user requirement needs to be translated into a technical specification of what the method is actually expected to do. Such an open requirement may require a lot of testing, even then it is likely that commonly encountered files for the types of case expected will need to be specified.

Prior to validation, the method needs to be precisely defined. For instance, acquisition of a bit-by-bit copy of a hard disk drive would be considered to be a laboratory-developed method. The method should be sufficiently detailed to allow a competent individual to follow and contain any risk mitigation steps and/or quality controls. An appropriate and balanced risk assessment is at the core of any validation study, and should concentrate on realistic risks and not become an abstract ‘what if’ process. Significant changes may prompt re-validation of the methodology and tools used along with an update of the standard operating procedure.

A thorough understanding of the method, technique and technology should allow practitioners to identify the type of error that could occur at any stage in the series of tasks in the examination. It could also create its own risk of some cases being turned away from having any digital examination due to the resource implications. It is important to cross reference the risk with the stage in the procedure that mitigates or controls it. Identifying what controls are to be assessed during validation, and which have an alternative assurance mechanism, ensures the testing is focussed.

The scale of validation exercise will vary according to the complexity or novelty of a method. Data that are available from previous studies, evaluations or validations; the risk assessment; and what the end user actually requires the method to do. The digital forensics community is free to collaborate on aspects of the validation study. The risk assessment of the specification developed from the user requirement should focus validation activity on what will make a difference to critical findings. A working understanding of experimental design is essential when validating novel methods.

A well designed test can maximise the utility of each element of the test and ensure that the amount of testing is kept to the minimum required. Software that is deemed valid in software engineering terms forms part of a wider method. Even software developed within a suitable quality standards framework may only be as good as the technical or functional specification supplied. There should be evidence of use of a formal development method and/or a quality management systems, as well as evidence of unit and system testing, including test plans and results. Most fields in forensic science use some form of adopted methodology where some or all of the validation data is available elsewhere.

If another organisation has validated a method, complete re-validation may not be necessary. However, the method will require reviewing to see that it is fit for purpose based on the available data. A risk or impact assessment is required, which should be focused on what changes have occurred and compare these with the original validation. Changes may be within the tolerance of the original acceptance criteria or existing quality assurance methods built into the method may be quite capable mitigating against identified risks. Risk-based assessment that may have shown that the method no longer meets the original acceptance criteria, may also offer a new estimate of uncertainty resulting from this change.

This may mean that the court can still adequately evaluate the findings. If the now new method is to become part of the routine activities of the forensic unit, accreditation should always be sought. The strategy and plan for the validation of a method or set of methods should include the following requirements: Method under review, source, quantity and reliability of data used for the tests, and type of result being assessed. The validation plan should be based on good experimental design to ensure that the testing is scaled and targeted correctly. Expected outcomes should be, wherever possible, specific, quantifiable and highlight the acceptable error margin (i.e. the defined accuracy and precision required of the method).

Blind trials should focus on non-obvious situations where a failure to assess correctly is a real prospect. Acceptance criteria that demand 100% in anything other than a data set designed for evaluating a method should not be agreed to. The design of the test is dictated by end-user requirements and technical specifications, along with any relevant risk assessment. Data generated during the validation should be stored for later audit. It is not always possible to define the source data completely, but every effort should be made to select data that will robustly test the method and tool to be used.

Detailed notes are required for each test in a forensic science plan, which should include an assessment as to whether the method has passed or failed each of the tests, and is fit for purpose. Tests should not normally be limited to a single event and there should be consideration of uncertainty of measurement that usually is achieved by repeating tests. A report should be constructed that details the validation process performed. This should include the original requirement, a summary of the strategy, tests performed and the outcome of each test. It should also include any limitations of the method, the impact of these limitations, and any additional steps required to detect and mitigate them.

The Codes require that a statement or certificate of validation completion be produced by the organisation implementing the method. All that is required is a short (one or two page) summary of the validation report. The assumption is that the certificate is essentially recording approval, although it could record that the method is not recommended for use.

2.6.2. Tool trustworthiness

The potential for evidence of tool verification against disclosed requirements to be used in support of validation is real. The challenge seems to be to find a mechanism which allows tools to be verified, without exposing any of the parties involved to undue risk of liability or disclosure of commercially sensitive information. The Trustworthy Software Foundation has proposed 5 levels of software trustworthiness. These are based on audience (end users), development methods (production processes) and testing (verification). Digital forensic tools would seem to fall into TL3 or TL2 which demand, in TSF terms, that controls (i.e. requirements definitions and testing) are implemented [260].

Mandated development methods cannot be imposed for digital forensic tools, but tool providers can be encouraged to provide evidence of the trustworthiness of their claims. There are some options for performing verification and disclosing sufficient information about verification that map to Trustworthiness Levels.

Internal verification producer has carried out internal testing but does not disclose unless forced to. Computer Forensics Tool Testing can be viewed as a combination of Internal Verification, External Verification and Open Diligence. Computer Forensics Tool Testing results are produced by a crowdsourced third party rather than being commissioned by a tool producer. The major difference lies in the fact that volunteers conduct the Federated Testing and have fewer controls on how they conduct tests. The author recommends that the industry should explore the Sampled Accredited Internal Diligence option as a means for disclosing tool verification in a way which does not violate commercial confidentiality. SAID allows users to reduce their method validation costs, spreads the cost of verification more equitably and potentially removes the need for re-validation.

2.6.3. Advances in tools

The digital forensics community has a strong emphasis on application, meaning that problems are solved in practise rather than theoretically. By creating Digital Forensics Competitions, tool development is encouraged. However, no research has been conducted on the variety, accessibility, or quality of the published tools. The research was motivated by the lack of availability of forensic datasets [261].

The authors posed the following research questions:

1. What published tools exist? (categorisation)
2. Are tools accessible and/or maintained without cost? (permission, downloadable)
3. Are tools useful and applicable? (evaluation of programming style, interfaces, code quality, tested code, and documentation)
4. What are the current challenges in the development of forensic tools?

It has been previously contended that open source tools may “meet the criteria of the guidelines” of the Daubert tests:

- Testing: Can the procedure be and has it been tested?
- Error Rate: Does the procedure have a known error rate?
- Publication: Has the method been published and reviewed by peers?
- Acceptance: Is the method accepted by the scientific community?

This paper identifies software designed primarily for research purposes and evaluates any subsequent development. Both ForensicsWiki and toolcatalog.nist.gov offer a catalogue of commercial and open-source software and hardware products. The authors compiled articles from digital forensics conference proceedings and journal publications for the period 2014–2019.

The authors do not consider software like EnCase or Cellebrite to be a tool because it is a feature-rich program. Tools can be constructed in any computer language and are frequently created by individuals or groups of researchers. Autopsy, for instance, is a tool that supports plugins, which they also regard to be tools. Code review is an essential step in software development since it improves program quality. There are a variety of automated code analysis tools available, but Codacy was the only one that matched the researchers’ requirements.

A rating ranging from A to F (with A being the highest) is assigned, making it easy to evaluate the quality of each instrument. The researchers examined 799 research publications, of which 62 (7%) included tools that met the criteria. The Digital Forensics Research Workshops produced about 25% of all reviewed articles (US & EU). There were public repositories for 78.7% (26/33) of the accessible tools (Github/25 and Bitbucket/1) with others on other websites. The authors analysed the 22 tools created between 2014 and 2018 to evaluate if they were being maintained after their creation/modification.

Python was by far the most common programming language, and it is routinely used to develop plugins for existing tools like Volatility and Autopsy. There is no standard structure for developers to follow when documenting their tools, however a recommended approach has been supplied by multiple sources. Five internet libraries of forensic tools were identified through online searches. Four of the websites featured connections to an assortment of tools from various categories.

There appears to be no common technique for classifying the tools, for example, disc imaging tools are separated by operating system. The Github repository Awesome-Forensics contains a comprehensive array of forensic tools. This resource comprises over 60 tools organized into 14 categories and was most recently updated on April 29, 2019 (at the time of the original article’s publication). In addition, other repositories such as DFIR Training and DF Tools Catalogue provide tools for pentesting, malware analysis, hacking, and honeypots.

2.6.3.1. Digital forensics taxonomy. To address the first research question, the authors focused on published tools that make it easy for practitioners to select the most suitable tool for a given task. Therefore, they adhered to a digital forensics taxonomy in order to group them following a modified and expanded version of the Netherlands Register of Court Experts taxonomy. They discussed both OS-specific tools and universal tools that can be used regardless of the operating system.

Following the taxonomy, they studied tools in the following categories:

- Computer forensics
  - o Windows apps
  - o File provenance
  - o File system
  - o Triage
  - o Non-relevant data
  - o Timelines
  - o Approximate matching
  - o Litigation
  - o String search
  - o Evidence container
- Software forensics including database forensics
  - o Email
  - o Web browser
  - o Database forensics
- Multimedia forensics
  - o Video file formats
  - o Image file carving
- Device/IoT forensics
  - o Mobile devices
  - o Drone
  - o Smart home
  - o Xbox

  - o Programmable Logic Controller (PLC)/Supervisory Control and data Acquisition (SCADA)
  - o Virtual reality
- Network forensics
  - o Protocols
  - o Attack-identification
  - o Cloud
- Malware forensics
  - o Computer
  - o Mobile devices (Android)
- Memory forensics
  - o Acquisition
  - o Analysis

Digital forensics must adhere to a strict protocol for data collection, analysis, and reporting in order to be acceptable in court. In order to produce "forensically sound" digital evidence, the tools used to collect digital evidence must undergo rigorous testing. The NIST Computer Forensics Tool Testing Program is the only ongoing effort to standardise digital forensic tool testing. ISO 17025 does not mandate individual certification of tools, but it does provide standards for equipment and validation of procedures and results. Although 46 of the reviewed 62 tools have been appraised in the publications, there are variations in their evaluations.

To meet the standards of the Daubert process, the tools from peer-reviewed papers must be adequately described, updated, and have well-documented development and testing procedures, including code and data. Practitioners must be cognisant of the fact that the digital forensics landscape is always evolving, as technological advances result in the discovery of new or previously unknown digital artefacts during an investigation. Regulating the credibility of evidence produced by digital forensic techniques requires internationally established standards. In areas such as limited test data and restriction to a single image format, the NIST's tool testing standards are "narrowly defined." The fact that the lack of testing procedures for the trustworthiness of research tools extends to established tools as well must be addressed.

It is difficult to assess the impact of research on digital investigations in the real world because the parameters used to evaluate research impact are mostly academic in nature. There is a significant need for a cooperative and receptive mentality in the dissemination of research-based tools to industry actors who would not otherwise have contact with academia. In this context, certain initiatives have been made, such as the Digital Forensics and Incident Response (DFIR) Review.

By analysing the network traffic of IoT devices' communication protocols, it is possible to identify whether information is encrypted or in plaintext. Identifying and prioritising IoT devices on the network is crucial, but there is currently no technology to automate this process. More technologies are required to remove traces left by IoT apps on mobile devices and to acquire and analyse IoT device memory.

This work examined nearly 800 articles on digital forensic technologies developed since 2014. The four research questions were answered by evaluating all listed tools:

1. What tools are published? – 62 digital forensics tools were categorised according forensic subfield as defined by the Dutch Register of Court Experts (2016), which now include device/IoT forensics.
2. Are tools free and maintained? – unfortunately, only 33 of the 62 utilities were publicly available. The digital forensic community can use 80% of these Github-released products. Many of these tools were not maintained after development. 29/33 of the source code comments were complete, however their quality varied. 24 of 33 tools provided documentation, such as tool description and installation instructions. Since developers don't use a uniform format, tool documentation varies in detail.
3. Are tools useful? – many tools have not been maintained or documented since their release. Tool development is usually a byproduct of research. The digital forensic community is unlikely to adopt these technologies due to a lack of coding standards, testing, repository locations, and documentation. Forensic investigators use commercial or established open source software, so criminal cases recognise them as valid evidence. Due to a lack of tool testing standards, the tools discovered in this research may still be able to produce reliable evidence. Guidelines and criteria are needed for building and evaluating tools for quality, maintainability, and reliability.
4. What are forensic tool development challenges? – if tools are to be widely adopted, a centralised repository for tested tools is needed. Tool researchers (developers) should spend more time on code documentation and choose plugins over stand-alone tools. Reusability would rise.

Finally, IoT forensics tools are underdeveloped. Despite being a burgeoning subject, tool development to automate IoT device identification and triage and new extraction tools/methods of new traces made by IoT mobile applications is lacking. In particular notice was the need for network forensic tools to examine the various communication channels used by IoT devices. Knowing whether data is encrypted or plaintext can help extract information from the devices.

2.7. *Tool verification*

The potential for evidence of tool verification against disclosed requirements to be used in support of validation is real. The challenge seems to be to find a mechanism which allows tools to be verified, without exposing any of the parties involved to undue risk of liability or disclosure of commercially sensitive information. The Trustworthy Software Foundation has proposed 5 levels of software trustworthiness. These are based on audience (end users), development methods (production processes) and testing (verification). Digital forensic tools would seem to fall into TL3 or TL2 which demand, in TSF terms, that controls (i.e. requirements definitions and testing) are implemented.

Mandated development methods cannot be imposed for digital forensic tools, but tool providers can be encouraged to provide evidence of the trustworthiness of their claims. There are some options for performing verification and disclosing sufficient information about verification that map to Trustworthiness Levels.

Internal verification producer has carried out internal testing but does not disclose unless forced to. Computer Forensics Tool Testing can be viewed as a combination of Internal Verification, External Verification and Open Diligence. Computer Forensics Tool Testing results are produced by a crowdsourced third party rather than being commissioned by a tool producer. The major difference lies in the fact that volunteers conduct the Federated Testing and have fewer controls on how they conduct tests. The author recommends that the industry should explore the Sampled Accredited Internal Diligence option as a means for disclosing tool verification in a way which does not violate commercial confidentiality. SAID allows users to reduce their method validation costs, spreads the cost of verification more equitably and potentially removes the need for re-validation [262].

2.7.1. *ForTrace forensic data set*

To hone their expertise and evaluate their digital forensic tools, forensic professionals often require a vast quantity of training data encompassing a wide range of criminal actions. Current training materials must include connected data from numerous data sources in order to offer trainees with the most realistic experience possible. There is a need for a framework that creates simultaneously holistic data, i.e., correlated persistent, volatile, and network traces from the same device, together with a realistic and sufficient quantity of background noise for a given scenario [263].

ForTrace is a system for creating forensic data sets to facilitate digital forensics training, tool development, and evaluation. ForTrace employs a holistic strategy to generate forensically relevant data sets, allowing for the simultaneous development of persistent, volatile, and network traces. It is derived from the word "fortress" and is intended to serve as a reminder that locating the correct digital traces can be as tough as conquering a castle. ForTrace offers the exact simulation of human-computer interactions for highly customizable data production, as well as the simple synthesis of vast amounts of relevant data (i.e., incriminating traces) with the ForTrace Generator module. The capacity of the framework to simulate multiple scenarios based on the mix of modules selected in each configuration file enables the user to set the synthesis of different scenarios as desired.

ForTrace is an open-source, flexible, and comprehensive framework for data synthesis in the digital forensics domain. It permits the production of diverse data sets by simulating human-computer interaction using forensically relevant and realistic circumstances. The Generator component can manufacture a realistic number of unrelated background artefacts, such as random websites visited, information downloaded, and emails sent and received, to divert the forensic examiner's attention from the actual incriminating evidence. Special emphasis is placed on expanding the existing PowerShell module, which can automate the majority of Windows activities. It is planned to develop a suitable front-end that will enable framework users to synthesize forensic photos not only via command line but also via graphical interface.

The ForTrace framework contains multiple modules that users can mix to simulate a variety of scenarios. Using a range of Windows-internal processes and apps, this enables it to generate realistic data at scale. During and after the execution of a user-scripted scenario, it simultaneously gathers volatile network traffic and memory data. These considerations must also take into account main memory and network traces in addition to persistent storage.

2.8. Interpretation and reporting

Identifying, collecting, analysing, and presenting digital evidence to legal decision-makers often requires expert knowledge. Results of digital forensics investigations are documented in reports and disseminated to the public. Legal decision-making bodies often have little to no knowledge of or insight into the processes that have led to the digital evidence. The use of technology with secret source code and functions, often referred to as "black box" technology, has been the subject of debate within the digital forensic community. What is considered a fact depends on the epistemological perspective, which is different in law vs science.

Facts should be understood as statements that are generally made and accepted as a matter of routine practice and convention and involve little to no active interpretation from the expert. There will always be a degree of uncertainty associated with an opinion, and to facilitate a fair assessment of evidence, uncertainty should be disseminated clearly and understandably. A task common between digital evidence and other forensic disciplines concerns evaluation which has been seen to be related to the Bayesian model of probability and inference. According to this model, trace evaluation should be performed relative to at least two competing claims as a "strength of evidence" approach. The use of likelihood ratio in forensic science is, however, still debated.

Due to the rapid and significant changes in information technology, developing and maintaining databases for digital forensic traces would be an impossible task. The current study aims to provide more knowledge about digital forensic examiners' practice when they interpret, evaluate, and present digital evidence in their reports [264]. Putting forensic capabilities in the hands of individuals without enough scientific understanding and advising support may cause more difficulties than it solves. Some digital forensic practitioners wrongly believe that they are just reporting what they witness and are unaware of the inherent judgments and judgements in digital investigations. It is difficult to discern between purposeful and accidental obfuscation in the absence of a normative method for evaluating digital evidence in light of competing hypotheses. The formal foundation for the scientific interpretation of evidence used by other forensic disciplines is unknown to digital forensic practitioners. A practitioner may draw a conclusion based on the output of a commercial tool, a practitioner could evaluate the results of numerous tools, and a practitioner could undertake case-specific experiments [265].

Each of the practitioners may claim to be doing a digital forensic examination, but the results could vary significantly. Practitioners of digital forensics have the rare chance to employ an approach that has evolved over the previous century. Globally, policymakers are reacting to the demand for a normative approach to appraising forensic evidence. This decisive war will be lost if the digital forensics community fails to respond quickly to this issue.

2.8.1. Opinion

Sunde (2021) examined the ways in which digital forensic examiners form their opinions. Digital forensic examiners from eight different countries participated in a quasi-experiment. They were tasked with analysing an evidence file obtained from the project Digital Corpora. Context had a significant effect on the observations of traces, but no biasing effect was found on interpretations or conclusions. It is therefore considered unlikely that the contextual information has impacted the content that was analysed here. It has been proposed that there are three types of forensic science opinions: investigative, preliminary and fully evaluative.

Due to the conditioning information provided, it was expected that the digital forensic examiners would perceive the task as a part of the investigation phase. The task description did not explicitly address offence level issues, but its nature did not exclude opinions addressing such issues.

The analysis procedure for exploring digital forensic reporting practices was threefold. First, a procedure for quantitative contents analysis of conclusion types and level of issues according to Hierarchy of Issues is elaborated. Second, the procedure for the quantitative content analysis of content concerning the credibility of the reported results is outlined. Third, the quiz-style content analysis of certainty descriptors from the conclusions is described. Examples of coding categories are provided under the respective sections.

The digital forensic experiment scenario suggested that they were in an early phase of the investigation, it was expected that opinions would be articulated as either investigative opinions or preliminary evaluative opinions. The observed conclusions types in digital forensic reports were Categorical conclusion and Strength of support, with an even distribution between the two conclusion types. The strength of support conclusion type is used to describe to what degree the result supports a proposition or hypothesis. Categorical conclusions have been criticized since they imply absolute certainty or a greater level of certainty than is warranted. The use of Bayesian methods such as likelihood ratio in forensic evaluation has been recommended in guidelines for the digital forensic discipline.

All strength of support conclusions in the digital forensic reports referred to a single hypothesis/explanation. The conclusion type has similarities with what is referred to as posterior probabilities. Deciding on a posterior probability involves evaluating the evidence in light of the hypothesis while considering the prior probability. A prior probability is the probability of the evidence before considering the hypothesis. Digital forensics reports should exercise transparency about the prior probabilities.

There are some risks with the strength of support approach used in digital forensic reports that should be highlighted. When presented in relation to a single hypothesis, the conclusion may be perceived as the probability that the hypothesis is true, known as the prosecutor's fallacy or the fallacy of transposed conditions. If the evidence is presented relative to a proposition or a set of competing hypotheses, the chance of misconceptions would be reduced.

Digital forensic conclusions were analysed for which level within the hierarchy of issues they addressed. A trace is defined as "any modification, subsequently observable, resulting from an event". The activity level issues would be concerned with linking activities or events to a trace, e.g., creating a file, deleting a log, downloading an image, sending an email, or executing a program. Within forensic science in general, the offence level is considered outside the domain of scientists. The high proportion of activity and offence level issues in digital forensic conclusions observed in the current study suggests that digital forensic may deviate from other forensic science disciplines in this respect. It is relevant to explore in future studies to what degree the results are representative for digital forensic reports in real casework. A broader knowledge base may facilitate a normative discussion about how, when, and by whom (which expertise) digital evidence should be examined and evaluated.

The content analysis of the digital forensic reports suggests that important information for assessing the credibility of the result was often absent or inadequately described. A description of tool(s) used was found in 70% of the reports, but only 57.5% were specific and included version numbers. 70% included the time zone abbreviation, although only 15% explained how it should be understood in contrast to local time. A digital forensic report is written for someone else and usually for someone with low-level technical knowledge. Explanation of the terminology used in the report is crucial for understanding what is presented.

It is therefore alarming that only 15% of the digital forensic reports included such explanations. The very low proportion of digital forensic examiners conveying this information is a cause for concern. There were substantial deficiencies concerning method descriptions, statements about reliability/validity of methods or tools, and explicating that the conclusion was an opinion. A detailed method description is important for verification and peer review purposes but was provided in only 17.5% of the digital forensic reports. Due to rapid technology development, no tool can be trusted to perform perfectly over time and should be tested regularly. Information about whether there are known errors associated with the tool is vital for assessing the credibility of the result.

The analysis of digital forensic reports shows that uncertainty was articulated with a wide variety of expressions. Some expressions may have similarities with descriptors used in established frameworks for evaluative reporting, for example, "is very probable" and "highly probable". However, none of the reports referred to an established framework of expressions, which would provide more clarity in understanding these expressions' probative value.

Digital forensic examiners mainly tend to use two opinion types in their reports: Categorical conclusion and strength of support. The main finding in the report content analysis is that there seem to be several deficiencies in the reporting practices. Vital information is missing, presented vaguely, or even erroneously. Standards such as the Certainty scale or Digital Evidence Certainty Descriptors are not known or implemented sufficiently. The study suggests a higher likelihood of observing descriptions of limitations and methods (vague) in digital forensic reports compared to reports from the forensic science disciplines included here. It also shows a higher proportion of forensic science reports that included reasoning or justification of the conclusion and explicated that the conclusion was an opinion. There seems to be a high risk of erroneous or misleading results presented in digital forensics reports, suggesting a need to increase the quality of such reports. When considering the lack of balanced conclusions among the digital forensic examiners (none were presented in relation to multiple hypotheses), and the deficiencies found in the content analysis, there are serious concerns about the accuracy of these reports.

2.8.2. Preliminary opinions

Globally, misinterpretation of digital evidence is an increasing concern, prompting some nations to address the issue at the national level. It is vital to standardise the formation and expression of evaluations based on digital evidence. Recent efforts to establish a uniform approach in forensic science have centred on assessing forensic observations in light of conflicting hypotheses. Practitioners of digital forensics should be able to present their opinions in a manner that is clear, comprehensive, accurate, and consistent. There is a large gap between merely technical discoveries and completely evaluative judgements when competing proposals are presented in a legal arena [266].

The approach should reflect the fact that digital evidence is employed in a wide range of investigations, not just in criminal and civil cases. In terms of scientific interpretation, forensic professionals should focus on assessing the reliability of evidence in light of hypotheses. Focusing on the probability of a hypothesis increases the possibility of confirmation bias and the inclusion of material outside the forensic practitioner's area of expertise. Digital forensics is a young subfield of forensic science, and research in this area is in its infancy. It is sometimes necessary and fair to make decisions without a completely evaluated probability ratio.

This paper offers a modification of the C-Scale for expressing such evidence value expressions for evaluation. It includes a database of cases involving digital evidence tampering that can be used to support the assignment of probabilities.

A forensic practitioner explains the meaning and importance of observed digital evidence to factfinders during an evidential investigation. As an investigation continues, a forensic practitioner may be requested to do a preliminary examination of forensic observations without being given an alternative on behalf of a defendant. There is no standard procedure for generating and evaluating hypotheses and forming early evaluations of each hypothesis. In other instances, forensic experts are tasked with determining if digital data kept on a smartphone has been tampered with. Formally articulating the probabilities of predicted observations at this point of investigation provides insight into the reasoning process of the forensic practitioner and reduces the possibility of bias.

For example, a man is accused of stealing his employer's client contact list by transmitting it over his smartphone from his work account to his personal account. A forensic expert obtained information from the man's smartphone, but the expected texts are not present. Using another forensic tool, the fragments of deleted communications, including one with an attachment named "customers," are recovered, but the attachment's content is not. The majority of file recovery operations require an estimate of the data allotted to the file, necessitating the application of fundamental forensic science procedures such as authentication, classification, and evaluation. A digital forensics programme offers a non-allocated file named "contact.xlsx" as recovered with accompanying metadata, but additional verification is required to determine whether the related data on disc is the original file content.

The recovered data is incompatible with the file's metadata and name. Additional investigation reveals that the file's previously allotted disc space is now filled with zeroes. In light of these Second Phase observations, the forensic expert assigns the following evidence strength levels to each hypothesis. The forensic analysis of temporal data was compatible with the deletion of data prior to a certain date. However, the forensic examiner discovered several temporal anomalies that cast doubt on the deletion's timing.

Backdating on computers typically results in temporal anomalies, such as out-of-order system log entries. The forensic expert believes that the system was retroactively updated, but cannot determine whether this was the result of a person or a system error.

2.8.2.1. Expressing evaluations with precision and consistency.

Some forensic practitioners continue to employ verbal categorical categories that can be used both positively and negatively: Possibly, Probably, Very Probably, and Almost certainly. The major issue with these scales is that they improperly express the probability of a proposition that lacks a logical basis. To standardise qualitative terminology used to report evaluative judgements across forensic specialities, a different verbal scale matched with probability ratios has been proposed. Initially, the C-Scale was proposed in a categorical format, which introduced the problem of cliff edge effects. In light of an explanatory hypothesis, a forensic practitioner may have difficulties selecting whether to assign a C-Value of C4 or C5 to digital evidence.

On this scale, digital forensic practitioners can compare their evaluations in reference to C-Values. A forensic practitioner is aware that new observations may arise in the future, necessitating a revision of the evaluation. When assigning C-Values, the forensic practitioner is aware that additional content recovery procedures may uncover additional pertinent data. The C-Scale is designed to evaluate the strength of digital evidence observed in light of a hypothesis, not the probability of such a hypothesis. For example, interpreting geolocation data to answer the forensic question “Was the smartphone’s owner present at this location at this time?” needs a combined review of location, time, and identity.

2.8.2.1.1. C- value verbal level

- C0 – Erroneous/incorrect
  - o Evidence contradicts established fact
- C1 – Extremely weak evidence
  - o o The evidence is highly dubious
- C2 – Very weak evidence
  - o There is only one source of evidence that is easily manipulated
- C3 – Weak evidence
  - o The source(s) of evidence are harder to manipulate, but there is not enough evidence to reach a clear conclusion or there are unexplained contradictions in the observed evidence in light of the hypothesis
- C4 – Strong evidence
  - o Multiple, independent sources that are harder to tamper with
- C5 – Very strong evidence
  - o Evidence from several, independent sources that is harder to manipulate (very strong harmonious observations in light of the hypothesis)
- C6 – Extremely strong evidence
  - o The evidence is unquestionable and tamper-proof.

2.8.2.2. Developing datasets to facilitate digital evidence evaluation. A proof-of-concept database is being constructed based on a repository of cases involving various sorts of interference in digital crime scenes, such as mass deletion, reformatting, disc wiping, backdating, and concealing. The database has a standard structure and is being transformed to the Cyberinvestigation Analysis Standard Expression format (CASE - case-ontology.org). The current dataset is small, anonymized to protect privacy, and the ground truth is uncertain in certain instances.

In forensic science, establishing ground truth can be difficult, especially when digital evidence has been disguised or deleted. In the example cited, for two of three deletion entries, it was determined that digital evidence was erased. However, this conclusion was equivocal and may have been the result of evidence deletion. Depending on the sort of crime, digital forensic observations may have a varied meaning or relevance. For instance, the deletion of files holding incriminating evidence in a child pornography case cannot normally be compared to computer breach situations. Such discrepancies must be considered when building datasets to enable digital evidence appraisal.

Fact-finders and decision-makers rely on evaluative judgements when weighing various explanations for the evidence and selecting the most persuasive account of an offence. There is a need for consistency in the formulation and expression of preliminary evaluation views by digital forensic practitioners. By following a logical procedure, forensic practitioners can attain greater consistency and openness (Investigative Process Following Scientific Reasoning). The C-Scale is a valuable instrument for expressing preliminary thoughts on digital evidence in any form of investigation in a way that can be understood by non-technical and non-specialist fact-finders and decision-makers. It provides a framework for reasoning and assessing observed evidence, as well as a consistent method for expressing evaluations in terms of evidence strength. It is anticipated that this will contribute to more transparent forensic findings and alert all parties to further questions.

2.8.3. Argumentation

Frequently, forensic investigators must collect vast quantities of data from a variety of seized devices, internet forums, and/or cloud storage. Tools give reconstruction capabilities that are limited to their particular domain, such as chronological analysis of file metadata or relational analysis of who communicated with whom. Human investigators must determine how various forms of evidence are rationally related. The Digital Forensics community is undoubtedly at a crossroads in terms of how it reports case information. In many circumstances, even while factual material may be confirmed, it is difficult to quantify regions of doubt regarding a user’s digital actions. The third guide intends to expand the forensic practitioners’ “thinking toolkit” by introducing two graphical tools for inferential reasoning [267].

Forensic scientists are always making inferences. They link evidence to proof, generate new hypotheses, identify future steps, and draw conclusions.

Logical inferences are a “thinking toolbox” of several forms: deduction, induction, abduction.

- Deduction helps reach a conclusion based on available facts. Deduction requires that valid premises lead to a conclusion. The same conclusion must always hold, even if more premises are added. This logic is rarely used in forensics. Mathematical theorems can lead to “logically robust” inferences.
- Forensics largely uses induction. It facilitates reasoning under uncertainty and producing probabilistic, defensible, and ampliative conclusions (establishing generalisable new knowledge or theories based on case specific knowledge). Conclusions are seldom certain. Setting a baseline determines allowable uncertainty. The standard of proof in civil law is “under the balance of probability” (i.e., more probable than not), but in criminal law it is “beyond reasonable doubt".
- In addition to induction, forensics practitioners can use abduction. Falsification—questioning “how” or “what if'—enables theories to be formed and tested.

Common-sense inferences combine all the reasoning above. Generalizations, presumptions, assumptions, tale filling-gaps, and beliefs are typically implicit and unexpressed. These “rarely undergo systematic critical investigation".

2.8.3.1. Toulmin’ structured argumentation. A claim (C) is the proposition one wishes to prove true or untrue. It can be a conclusion, a decision, an expert’s view, a hypothesis, or a case statement, for example. A ground (G) might be collected evidence, a fact, a piece of information, created data, a scientific discovery, a legal precedent, or an observation. A warrant (W) is an inference that links a ground to a claim; it is a bridge-statement. A rebuttal (R) is a counterargument that undermines the credibility of a claim.

Structured argumentation has been used for many reasons with the objective of subjecting knowledge and assumptions that lead to a conclusion to systematic, critical examination. It has been used to construct safety cases and dependability cases, to trace and justify software design decisions, to instil trust in software development, and to reveal risk/mitigation threads for risk assessment. Toulmin’s argumentation model clarifies what is being evaluated in a much more precise manner. It was employed by Pasquale et al. in the context of forensic preparedness for event response. Wigmore charting generates a graphic accompanied by a key list like a legend.

Different sorts of evidence may be related by directed lines and a set of eight symbols. Roberts and Aitken suggest that several interrelated charts may end up nested. Inferences' logical structure is revealed by modified Wigmorean analysis, most likely the Toulmin scheme. The Digital Forensics community has not yet made substantial strides in the development and acceptance of procedures for determining digital evidence uncertainty.

2.8.3.2Case. Studies

1. Digital forensic experts analysed an advanced-fee fraud case involving a criminal group that targeted the elderly in the United Kingdom and the United States. The investigation included hundreds of victim interviews, a number of search and seizure activities, and a large number of financial transactions.

   There are several claims:

1. Suspect 'X' lifestyle not compliant with declared income.
2. Suspect 'X' had contact with victims.
3. Suspect 'X' had possession of fraudulent information.
4. Suspect 'X' had access to resources to facilitate fraud.
5. Suspect 'X' operated a money laundering scheme.

Three warrants (Warrants 1, 2, and 3) connect the claim to Ground 1, as they link victims to mobile phones and SIM cards recovered by law enforcement. The first instance demonstrates how structured argumentation can be used to recreate a large case logically, exceeding the function of case management tools. The primary argument for claim 2 is presented with the claim, grounds, warrants, and supporting evidence. Rebuttals 2–4 may be sufficient to contradict Rebuttal 1 and restore faith in the first assertion.

2. Case two presents a fundamental Claim, namely that suspect 'X' murdered victim 'Y,' which may be refuted by an assessment of relevant digital evidence sources. Unacknowledged rebuttals pose a potential risk to the validity of any conclusions or hypotheses obtained from a research. Rebuttals must be responded to with a counterargument or by acknowledging the original rebuttal's potential validity. When possible, warrants should be supported with testing and validation methods to bolster their evidentiary weight.
3. Case three gives an analysis of a fictitious sexual assault scenario involving the finding of an image of the alleged victim on the phone of the suspect. This case illustrates the evolution of an initial argument, followed by the presentation of eight counterarguments. The counterargument to one rebuttal is expanded as a whole argument based on the fact that the victim acknowledged their presence in the photograph. The fourth and fifth rebuttals are also counterarguments to the initial assertion and pose a challenge to the practitioner. Warrant 4 and the supporting forensic study (Backing 3) corroborate the photo's validity and the presence of the victim.

   Consent is not a defence for some behaviours, but for the purposes of this hypothetical case, it is considered that it could be. Here, the surrounding circumstances of the case, particularly those indicated in Ground 4 and Warrant 5 – proof of the suspect and victims' interactions and relationship, can support a refutation of this.

Structured argumentation is intended to assist a scenario's logical formulation. It provides a clear knowledge of what a practitioner has done, why process work has been performed, and the significance of this work in a given context. A systematic argumentation methodology helps both technical and legal peer assessment. Structured argumentation could be considered a technique for quality management because it facilitates more access to investigative procedures for the purposes of review. It could also aid juries in their interpretation of the evidence, enabling them to determine where there is a strong argument and where there are weak points that could be countered.

Structured reasoning at different levels of abstraction may be used for a variety of objectives, including documenting the outcomes of a research. Validating argumentation in digital forensics investigations requires persuasiveness, soundness, and completeness. Convincingness pertain to whether or not the argumentation is persuasive enough to convince the audience that the result reached is reasonable. One risk practitioners may face is becoming ensnared in exhaustively examining every theoretical possibility in terms of argument and counterargument and their refinement. Structured argumentation may be viewed as an expense if advantages are not deemed to outweigh problems, i.e. if digital forensics practitioners do not endorse it.

It can, however, become a very useful tool for supporting practitioners throughout their embedded investigations and case management. The approach does not require any specialised background (theoretical or mathematical) and is based on the unconscious conclusions that forensic practitioners already make.

2.8.4. Evaluating automated decisions

Increasing information volume, variety, velocity, dispersion, and complexity are overwhelming forensic scientists, crime analysts, and security experts. There is an urgent need for automated solutions that integrate scientific concepts and procedures in order to answer forensic queries. Massive amounts of data can be sifted through more effectively and efficiently with the assistance of automated technologies. There is a possibility that forensic practitioners will not recognise the output of an automated instrument as an inference requiring review [268].

Reviewing source code provides some clarity and comprehension if the forensic practitioner is familiar with Python. Additionally, the output of an automated system such as Plaso must be reviewed in light of the question of interest. Numerous automated tools are ambiguous regarding their applicability and provide little assistance to forensic practitioners in evaluating outputs critically. This paper presents design requirements for automated systems that enable forensic analysis, including examination of alternatives and evidence weight assignment support. This work compiles a list of existing terms and meanings related to the evaluation of automated systems and the decision-making process that ensues.

It examines technologies used for face comparison on identification documents/passports, fingerprints and shoemarks in criminal investigations, and digital evidence for any form of enquiry. Results should be specific enough to evaluate if a system is suitable for a particular forensic topic. Expert systems solve problems using a knowledge base that contains a number of facts and an inference engine that applies logical rules. A system is able to apply codified information and/or statistically acquired knowledge to case-specific facts. In both circumstances, the performance of the system may be evaluated using known data.

2.8.4.1. Different levels of evaluation. Multiple degrees of review are possible for automated systems, including performance evaluation, understandability evaluation, and forensic evaluation. Common system measures include accuracy, precision, recall, and F1-score. Traditional file carving tools and systems that target portions of partially overwritten files require different performance measures. The F-score combines accuracy and recall to facilitate the comparison of systems. The F1-score is better suited to evaluating performance when the classes are unequal.

Multiple metrics can be used to determine how near the algorithm's output is to the truth. A fundamental understanding of statistics is required to comprehend these performance measurements. A performance review will assist forensic professionals in determining whether or not the system is truly fitted to the forensic issue. However, when conducting forensic analysis, it is also vital to assess the system's output.

Forensic practitioners require a method for analysing the factors and characteristics that contributed to this result.

Such insights facilitate comprehension, explicability, and openness. For sophisticated and opaque box systems, it is required to incorporate another mechanism to enhance system comprehension. For instance, LIME enables users to comprehend how the characteristics affect the outcome by running the system numerous times, each time "hiding" a feature to determine how it influences the outcomes. DeepLift is also used to determine which elements of a deep learning system are crucial.

Evaluation of understandability is an integral component of contemporary automated systems. It seeks to determine whether or not the system is comprehensible or gives sufficient explanations. Forensic practitioners must eventually assign a (relative) probability to observed data in light of a working hypothesis and in comparison to competing hypotheses. In general, the phrase "proposition" is favoured, whereas "hypothesis" is employed throughout a study. In this context, the evidence is the automated system's output. Changing the hypothesis can affect the evaluation's outcomes.

Automatic technologies employed in forensic analysis offer limited aid in evaluating the uncertainty underlying a particular output. Contextual data and general knowledge might be explicitly incorporated into either the automated system or the evaluation processes, but they could also be considered during the decision-making process. There are three decisions that can be supported by the readings of outputs from an automated system by a forensic practitioner.

1. Performance evaluation helps forensic practitioners decide whether to use an automated system.
2. Understandability evaluation helps forensic practitioners decide the validity of an automated system's output.
3. Forensic evaluation supports a forensic practitioner's judgement about the weight of evidence in light of presented propositions and is conveyed to those involved in a case to help them decide with confidence (e.g., investigator, attorney, judge)

In contrast, automated decision making is complicated by the reporting forms that are simplest for non-specialists to comprehend are hardest to defend intellectually and experimentally. Simply declaring that a statement is true (or incorrect) may appear straightforward and comprehensible, but it lacks the needed transparency.

2.8.4.2. The advantages and disadvantages of approaches. With the inclusion of labels like "User clicked a link" and "User reloaded the website," digital traces can be represented as event-like data. It is simple to confuse these sorts of digital evidence with the accompanying activities. To decrease the danger of misinterpretation, it is essential to explicitly distinguish between a trace and the (possible) activity it indicates. A forensic practitioner with understanding of Python programming can examine the source code of a given outcome to comprehend its reasoning. The output of an automated system like Plaso must be reviewed in light of the investigation's focus question.

Additional study may be necessary to determine whether the interpretation is accurate, or there may be alternative explanations for a particular digital footprint. Depending on the data being analysed, the performance of a carving tool can vary considerably. The classification of a group of bytes as related material is not necessarily explained by automated algorithms for salvaging renderable content. When content is partially erased or unrelated fragments have been erroneously mixed, forensic practitioners are able to detect these anomalies without difficulty. Detailed audit logs can provide some information, but there is a need for more sophisticated methods that aid practitioners in comprehending certain outputs.

The calculation of the 'trace-vs.-reference' score and its form (similarity score or distance score, range of values, etc.) differ between systems. For instance, the OpenFace toolkit generates distance scores with a value between 0 and 1 for each comparison. The Idemia MorphoFace Investigate system provides similarity scores ranging from 0 to 50,000, which change as photographs are removed or added to the dataset. The result of forensic facial recognition tasks (1-vs-N) is a list of scores associated with potential candidates. The operator examines the score list and sorts potential hits, effectively making a judgement based on understandability, so as to use this information to infer about the continuing investigation.

This method is completely automated and requires no human input. The use of Levenshtein distance to determine the close similarity of usernames within email addresses is understandable to a technical analyst, but may not be to a non-technical user of system. A user would comprehend the approximate level of resemblance between the two email addresses, as well as the fact that the link was formed via email addresses rather than any other type of trace. In one case, fraudsters impersonating AirBnB send emails to apartment-seeking victims. The forensic analysis clearly supports the conclusion that the addresses were created by the same individual and that the two incidents represent a sequence of crimes. This demonstrates how, given the identical output of an automated system, various conclusions and decisions can be formed when knowledge and context are taken into account.

2.8.4.3. Developing automated evaluation support systems. Accountability, dependability, transparency, and scientific reasoning should form the basis of such automated systems. The performance evaluation must include a description of the data used for training and/or testing. Strong communication exists between the system's developer and the users who must comprehend and implement the results. The tradeoff between comprehensibility and completeness in comprehensibility presents ethical issues. For a non-technical individual to comprehend how the system functions, one may be inclined to oversimplify the explanations.

This may be especially true in the legal system, where individuals favour reliable institutions and unambiguous solutions. Unanswered is the extent to which a system supporting forensic analysis can automate the entire process of hypothesis selection, knowledge and context consideration, and evaluation. Using an automated system to help forensic analysis might pose numerous problems regarding dependability and decision-making. It is suggested to formalise the three evaluation levels for such systems. The evaluation results should be specific enough to identify whether or not the system is suitable for a particular application.

In addition to supporting contextual analysis, the system should maintain the context of the information at each level. The purpose of understandability evaluation is to assist a forensic practitioner in determining if a certain output from an automated system is incorrect/invalid and should be rejected, or whether it is appropriate for forensic evaluation. This paper provides some advice on how to build such systems, but numerous obstacles remain. It is impossible to provide a comprehensive list of all conceivable systems and recommendations for each.

2.8.5. Certainty descriptors

The veracity of all forensic scientific evidence has been and will continue to be scrutinised. The manner in which the forensic practitioner characterises their evidence in terms of "weight/reliability/likelihood or uncertainty" is one of the primary areas of concern. There appears to be a trend in forensic science towards the requirement of more quantitative approaches for describing findings. The Digital Forensics practitioner must compare the outcomes of a given examination to a list of suspect conditions and provide a cogent explanation of what they believe occurred. While many other traditional forensic science fields are urged to quantify the weight of their evidence, Digital forensics rarely does so [269].

Digital Forensics expert witnesses are generally at liberty to express the manner of their findings as they see fit. In doing so, it is possible that alternative definitions and quantifications of dependability will emerge, which may threaten the consistency of legal decision-making. There have previously been calls for help to bolster the creation of techniques to evaluate the correctness, dependability, and 'uncertainty' of forensic analysis outcomes. As opposed to the expert, who can present evidence based on their competence, the evidential, sometimes known as a "technical witness," will provide details about the case facts and digital scenario. Both present evidence that depicts the digital events that have transpired in a certain instance, but their ability to remark differs significantly.

Regardless of the role in which a practitioner is functioning (the acquisition of expert witness status varies different jurisdictions), they must ensure that they accurately explain their evidence. Due to the nature of digital evidence and investigations of this type, there is concern that it may not be possible to develop a scientific mechanism for measuring digital evidence. The development of any evidence weighting system must capture and weight the practitioner's perception of the evidence's significance. This requires the formalised use of subjective opinion, a challenging undertaking. If practitioners were asked to estimate the credibility of specific hypotheses regarding specific digital scenarios, it is almost probable that they would hold divergent opinions.

The area of Digital Forensics lacks a database of results or case characteristics that can be examined to determine the association between various sorts of digital occurrences. In an ideal situation, a digital footprint is the product of a single activity. In actuality, though, numerous actions may be responsible for a specific piece of digital evidence.

If evidence suggests that two actions could have been implemented on a system, it becomes necessary to identify any definitive digital traces that can be used to determine which action has been done. In the course of a Digital Forensics investigation, digital forensics practitioners must handle three "categories" of uncertainty. These include:

- uncertainty regarding the description of data
- uncertainty regarding data-related actions; and
- uncertainty regarding actions linked to a suspect.

Digital Forensics examiners are currently unable to weight their evidence using accepted robust scientific methodologies. This work posits that a more practical solution is to unify the language practitioners use to communicate certainty in their findings. The Digital Evidence Certainty Descriptors framework consists of six descriptors that should cover all possible digital circumstances. Digital Evidence Certainty Descriptors provides six descriptors that are not concerned with measuring uncertainty but rather with identifying when uncertainty exists in a set of findings. This is intended to ensure that practitioners use uniform terminology when describing the presence of ambiguity in an examination. In an effort to avoid informal or imprecise techniques of description, it also aims to standardise the language used to describe evidence.

2.8.6. The digital evidence certainty descriptors

- To call a scenario "conclusive," a practitioner needs 100% proof. In this scenario, an act can cause a collection of repercussions. The genuine meaning of fact precludes any alternative explanation. Thus, "conclusive fact" should only be used in such scenarios and not to describe cases where other hypotheses may exist. When using "conclusive fact" as an evidence descriptor, practitioners should be cautious because it involves a thorough evaluation of all possible hypotheses about a scenario and their rigors testing and refutation, leaving just one outcome.
- Persuasive digital evidence supports the concept, but it is not conclusive. The practitioner's interpretation of a digital event cannot be proven, but all system actions are consistent with known, accepted, and documented device functionality. Digital data cannot prove a hypothesis, but it cannot disprove it. The practitioner's description is supported by all data about a system, but other external causes may have caused it.
- A practitioner can describe digital evidence as "conceivable" with the lowest assurance. Where digital data partially supports a hypothesis but one or more fundamental requisites are absent to fully validate the scenario, "conceivable" is applicable. Due of the available digital content, the theory remains possible. However, competing hypotheses remain valid. "Conceivable" and "Insufficient Information" may be used together.
- If there isn't enough digital information to prove a series of dubious acts, apply the "Insufficient Information" label. This descriptor does not rule out any suspected behaviours, but the practitioner lacks adequate knowledge to confirm them. Insufficient information may be feasible.
- "Implausible" should be used to indicate a probable event with no evidence. "Implausible" denotes an event that would require external elements that are both absent and unobserved. An occurrence is "implausible" if it lacks the essentials to support a hypothesis. Such requirements would be present during the technology's normal operation.
- "Impossible" describes digital events that cannot occur given the current scenario and technology under consideration. Due to technological diversity and undocumented functionality, this descriptor should be used with caution. The "Impossible" description is used to describe the scenario where two conventional hard drives are suspected of exchanging digital data via physical contact.

3. Conclusion

The review covered the period 2019–2022 during which there has substantial development in the field of digital forensics.

Some of the broad observations from the review that require further attention include the difficulty in explaining why a machine came up with a particular answer; and bias remains a concern, especially in the context of artificial intelligence because human biases might be replicated by machine learning systems. However, digital forensics, which is increasingly being referred to as digital forensic science, has reached a threshold of maturity as computer science and forensic science.

Extensive research has been conducted on Darknet markets, including investigations into the times of day when users are most active and the effects of closing market places, which were found to have relatively little of an effect on users. The use of cryptocurrencies remained the preferred method of payment for purchases made on darknet markets. Open source intelligence, such as the subreddit r/darknet on Reddit, which has over 203,000 registered members, is a good resource for gaining insight and intelligence regarding Darknet markets. The terms "newbie," "noob," "new," "beginner," and "n00b" are among the most common search terms, along with "security" and "DarkNet markets payments." Bitcoin, which has been around for a while, and Monero are currently the two cryptocurrencies with the most widespread use (provides greater anonymity). The transparency of Bitcoin transactions, which includes specifics such as the number of BTC that were exchanged and the exact time at which the transaction took place, is one of the advantages of Bitcoin from an investigative point of view.

There was a broadening of the consensus that the Daubert standard is applicable to cases involving digital evidence. As a consequence of this, there was an appreciation that the majority of the tools used are private or proprietary commercial solutions that do not have any stated error rates. The practitioners' risk homoeostasis of what is acceptable for the conceptions of "rigour" and "process" has evolved as a result. Manufacturers of tools are still having trouble keeping up with the rapidly advancing technological landscape.

The use of on-scene decryption and the categorisation of photos taken at the crime scene were the primary focuses of digital forensics at the scene of the crime. The method of conducting a digital forensic investigation focused on new forms of technology, such as solid state drives, as well as reevaluating the digital forensic procedure. Memory forensics is considered increasingly significant, with particular emphasis placed on finding solutions for desktop operating systems, encryption, crash dumps, hibernation files, debuggers, and virtualization by means of hypervisors that generate and execute virtual computers.

An examination of file systems, in particular well-known systems such as Windows, as well as an investigation of potential future file systems such as Google Fuschia; and distributed file systems. The topic of anti-forensics was discussed in a number of works, with particular attention paid to the distinction between accidental and intentional tampering as well as the efficacy of erasure techniques.

Within the realm of devices and systems, the primary concentration of cloud forensics was placed on the difficulties associated with conducting a forensic investigation of cloud computing systems as outlined by NIST as well as the various possible solutions, such as "forensic by design." When it comes to dealing with forensic investigation of Internet of Things systems, the field is just getting its feet wet. A number of the authors considered not just the more conventional approaches to analysis, but also the more recent method of electromagnetic side-channel analysis. The field of digital forensics for motor vehicles is becoming increasingly significant. The "Internet of vehicles ecosystem," the "digital identification of motor vehicles," and the "digital forensic analysis of motor vehicle collisions" are some of the topics that fall under this category of research. It was mentioned that there is one common tool that is offered for sale in the market for conducting digital forensics on motor vehicles.

Apps and social media were combined as a subject for discussion because there is a growing overlap between the two fields. The functionality of messaging app vendors is evolving to encompass larger social media services such as publishing channels and news channels. Using evidence found on social media sites is one way that behavioural science is beginning to use digital forensic approaches. It has been discovered that criminal profiling and sentiment analysis might potentially be deduced from posts made on social media.

A small sample of the digital evidence in legal proceedings and the cybercrime and data governance issues occupying the minds of the justice system and political leaders in several jurisdictions was discussed.

The question "Is artificial intelligence the answer to the issues found in digital forensics?" was asked. "Is artificial intelligence the answer?" There were presentations of papers on a wide variety of technologies made within the field of machine learning. Several aspects of digital forensics, such as file classification, were improved with the use of AI. Deep learning is an alternative to traditional machine learning that has been researched by a number of authors. Deep learning refers to the use of neural networks with multiple layers for the purpose of tuning machines to do certain tasks. The discovery of possible data sources for digital evidence, the collection and acquisition of evidence, as well as its interpretation, all involved the application of deep learning. In addition to this, it was used in evidence analysis tasks such as clustering and classification; determining the relationship status between the evidence, the suspect, and the victim; and estimating the weight, validity, reliability, and inferences. Several problems have been discovered in the application of artificial intelligence to digital forensics. These problems include the requirement for AI that is explicable, as well as the fact that the results of AI are presented in such a way that reinforces the infallibility bias that has already been verified.

In the areas of management and quality, some new problems were discovered, and several of the previously discovered problems were given more attention. The reliability of software was called into serious doubt after it was shown that most software has between one and one hundred defects for every thousand lines of code, with the top one percent of programmers producing an average of eleven defects for every thousand lines. The idea of zero-trust digital forensics, in which every part of an examination is presumed to be untrustworthy unless it is demonstrated to be confirmed, was presented. This idea has to be investigated in greater depth.

There have been multiple suggestions made regarding the administration of digital forensics, particularly within government entities that deal with law enforcement. Among the many suggestions is the appointment of a Forensic Advisor as well as the development of a decision-support framework for first responders.

In the process of conducting digital forensics, there was an increased emphasis placed on the human elements involved. It was discovered that bias can have a negative effect on the integrity of the process, which is an issue that has been identified to have a substantial impact on other forensic disciplines. In addition, the practise of digital forensics has room for improvement in the areas of peer review processes, credentialing of examiners, assurance of technical reliability, and tool validation.

In closing, I'd like to elaborate on a point that I mentioned in the overview that came before this one. There are a small number of the included articles that are in disagreement with my thoughts as the reviewer. These publications have been included because they do make a positive contribution to the overall body of knowledge in the area, and the field benefits from having a variety of perspectives. In a nutshell, the primary reason for my opinion is that the author(s) has/have paid insufficient regard to the forum in which the output of the digital forensics process is ultimately assessed and in which decisions are made. The arena in which the facts are determined and from which crucial feedback is supplied to both the field and the practitioners is the court of law. The various actors within the justice system perform several roles including customer, client, victim, stakeholder, witness etc. The capacity of the expert to accurately express that information in a manner that is understandable and with an appropriate weighting is sometimes given insufficient attention, despite the fact that testimony in both written and spoken versions might be technically accurate. It is the court that makes a decision based on the presented evidence and it is the responsibility of the expert to: 1) ensure that evidence is accurate, reliable and understandable; 2) accept the findings as a form of feedback and evaluation of the digital forensic science proffered to the court. I have high hopes that individuals and groups who are going to keep working in this industry, whether in academic or operational capacities, will keep this in mind as they move forwards with their projects.

References

[1] E. Casey, Editorial: interrelations between digital investigation and forensic science, Digit. Invest. 28 (2019) A1–A2.

[2] E. Casey, Maturation of digital forensics, Digit. Invest. 29 (2019) A1–A2.

[3] M. Brunt, Police Infiltrate Encrypted System, Arrest Hundred 'leading Secret Criminal Lives', and Seize £54m, Sky News, 2020. Retrieved from, https://news.sky.com/story/operation-venetic-police-catch-hundreds-suspected-of-leading-secret-criminal-lives-by-cracking-codes-12019558.

[4] Sky News, EncroChat: what It Is, Who Was Running It, and How Did Criminals Get Their Encrypted Phones?, Retrieved from, 2020, https://news.sky.com/story/encrochat-what-it-is-who-was-running-it-and-how-did-criminals-get-their-encrypted-phones-12019678.

[5] J. Cox, How Police Secretly Took Over a Global Phone Network for Organised Crime, Vice, 2020. Retrieved from, https://www.vice.com/en_us/article/3aza95/how-police-took-over-encrochat-hacked.

[6] Europol/Eurojust, Dismantling of an Encrypted Network Sends Shock Waves through Organised Crime Groups across Europe, Joint press release, 2020. Retrieved from, https://www.europol.europa.eu/newsroom/news/dismantling-of-encrypted-network-sends-shockwaves-through-organised-crime-groups-across-europe.

[7] A. Maurushat, A. Bello, B. Bragg, Artificial intelligence enabled cyber fraud: a detailed look into payment diversion fraud and ransomware, Indian J. Law Technol. 15 (2) (2019) 261–299.

[8] B. Nikkel, Fintech forensics: criminal investigation and digital evidence in financial technologies, Forensic Sci. Int. Digit. Invest. 33 (2020), 200908.

[9] S.M. Ho, D. Kao, M.-J. Chiu-Huang, W. Li, C.-J. Lai, Detecting cyberbullying hotspots on Twitter: a predictive analytics approach, in: Forensic Science International: Digital Investigation, DFRWS 2020 EU – Proceedings of the Seventh Annual DFRWS Europe, vol. 32, 2020, 300906.

[10] C. Ngejane, J. Eloff, T. Sefara, V. Marivate, Digital forensics supported by machine learning for the detection of online sexual predatory chats, Forensic Sci. Int.: Digit. Invest. 36 (2021), 301109.

[11] A. Maurushat, A. Bello, B. Bragg, Artificial intelligence enabled cyber fraud: a detailed look into payment diversion fraud and ransomware, Indian J. Law Technol. 15 (2) (2019) 261–299.

[12] N. Karie, V. Kebande, H.S. Venter, Diverging deep learning cognitive computing techniques into cyber forensics, Forensic Sci. Int. Synergy 1 (2019) 61–67.

[13] A. Alrajhi, A survey of artificial intelligence techniques for cybersecurity improvement, Int. J. Cyber-Secur. Digital Forensics 9 (1) (2020) 34–41.

[14] R.M. Mohammad, M. Alqahtani, A comparison of machine learning techniques for file system forensics analysis, J. Inf. Secur. Appl. 46 (2019) 53–61.

[15] N. Karie, V. Kebande, H.S. Venter, Diverging deep learning cognitive computing techniques into cyber forensics, Forensic Sci. Int. Synergy 1 (2019) 61–67.

[16] Z. Bruce, Editorial: deep learning, bias and turnaround time, Forensic Sci. Int. Digit. Invest. 39 (2021), 301318.

[17] R. Segate, Cognitive bias, privacy rights, and digital evidence in international criminal proceedings: demystifying the double-edged ai revolution, Int. Crim. Law Rev. 21 (2) (2021) 242–279.

[18] P. Anderson, Z. Zuo, L. Yang, Y. Qu, An intelligent online grooming detection system using AI technologies, in: 2019 IEEE International Conference on Fuzzy Systems, (FUZZ-IEEE), 2019.

[19] J. Sester, D. Hayes, M. Scanlon, N.-A. Le-Khac, A comparative study of support vector machine and neural networks for file type identification using n-gram analysis, Forensic Sci. Int. Digit. Invest. 36 (2021), 301121.

[20] A. Alrajhi, A survey of artificial intelligence techniques for cybersecurity improvement, Int. J. Cyber-Secur. Digit. Forensics 9 (1) (2020) 34–41.

[21] S. Alam, Applying natural language processing for detecting malicious patterns in Android applications, Forensic Sci. Int. Digit. Invest. 39 (2021), 301270.

[22] M. Hirano, R. Hodota, R. Kobayashi, RanSAP: an open dataset of ransomware storage access patterns for training machine learning models, Forensic Sci. Int. Digit. Invest. 40 (2022), 301314.

[23] S. Poudyal, D. Dasgupta, Z. Akhtar, K. Gupta, A multi-level ransomware detection framework using Natural Language Processing and Machine Learning, in: Paper Delivered at International Conference in Malicious and Unwanted Software (MALCON 2019), Nantucket, Massachusetts, USA, 2019.

[24] In the Tor Network, Users' Messages are Routed through a Series of Relays that Obscure the Identity of the User and the Websites that They Access.

[25] Y. Tsuchita, N. Hiramoto, Dark web in the dark: investigating when transactions take place on cryptomarkets, Forensic Sci. Int. Digit. Invest. 36 (2021) 1–16, 301093.

[26] Operation Onymous, A Joint Operation Including 16 European Countries, Coordinated by the European Cybercrime Centre (Europol), the U.S. Federal Bureau of Investigation, the U.S. Immigration and Customs Enforcement, the U.S. Homeland Security Investigations and Eurojust, Took Down Several Darknet Marketplaces, 2017. Retrieved from, https://www.europol.europa.eu/media-press/newsroom/news/global-action-against-dark-markets-tor-network.

[27] Wallet Explorer. Found at https://www.walletexplorer.com/(last accessed 7 January 2022).

[28] N. Hiramoto, Y. Tsuchiya, Measuring darl web marketplaces via Bitcoin transactions: from birth to independence, Forensic Sci. Int.: Digit. Invest. 35 (2020), 301086.

[29] K. Bahamazava, R. Nanda, The shift of DarkNet illegal drug trade preferences in cryptocurrency: the question of traceability and deterrence, Forensic Sci. Int.: Digit. Invest. 40 (2022), 301377.

[30] M. Lusetti, L. Salsi, A. Dallatana, A blockchain based solution for the custody of digital files in forensic medicine, Digit. Invest. 35 (2020), 301017.

[31] G. Macia-Fernandez, J.A. Gomez-Hernandez, M. Robles, P. Garcia-Teodoro, Blockchain-based forensic system for collection and preservation of network service evidences, Digit. Invest. 28 (2019) S141.

[32] D. Orr, Cryptocurrency: its Impact and Forensic Worth. To be Published in Encyclopaedia of Forensic Sciences, third ed., Elsevier, 2022.

[33] X. Burri, E. Casey, T. Bolle, D.-O. Jaquet-Chiffelle, Chronological independently verifiable chain of custody ledger using blockchain technology, Forensic Sci. Int.: Digit. Invest. 33 (2020), 300976.

[34] D.-O. Jacquet-Chiffelle, E. Casey, J. Bourquenoud, Tamperproof timestamped provenance ledger using blockchain technology, Forensic Sci. Int.: Digit. Invest. 33 (2020), 300977.

[35] D. Billard, Tainted digital evidence and privacy protection in blockchain-based systems, Forensic Sci. Int.: Digit. Invest. 32 (2020), 300911.

[36] T. Thomas, T. Edwards, I. Baggili, BlockQuery: toward forensically sound cryptocurrency investigation, Forensic Sci. Int.: Digit. Invest. 40 (2022), 301340.

[37] S. Chen, C. Zhao, L. Huang, Yuan, M. Liu, Study and implementation on the application of blockchain in electronic evidence generation, Forensic Sci. Int.: Digit. Invest. 35 (2021), 301001.

[38] B.C.A. Petroni, R.F. Goncalves, P.S. de A. Ignacio, J.Z. Reis, G.J.D.U. Matins, Smart contracts applied to a functional architecture for storage and maintenance of digital chain of custody using blockchain, Forensic Sci. Int.: Digit. Invest. 34 (2020), 300985.

[39] IBM Blockchain, Smart Contract Defined, 2022. Retrieved from, https://www.ibm.com/topics/smart-contracts. (Accessed 15 January 2022).

[40] X. Zhang, J. Grannis, I. Baggili, N. Beeebe, Frameup: an incriminatory attack on Storj: a peer to peer blockchain enabled distributed storage system, Digit. Invest. 29 (2019) 28–42.

[41] Y. Tsuchia, N. Hiramoto, Dark web in the dark: investigating when transactions take place on cryptomarkets, Forensic Sci. Int.: Digit. Invest. 36 (2021), 301093.

[42] N. Hiramoto, Y. Tsuchiya, Measuring dark web marketplaces via Bitcoin transactions: from birth to independence, Forensic Sci. Int.: Digit. Invest. 35 (2020), 301086.

[43] T. Thomas, M. Piscitelli, I. Shavrov, I. Baggili, Memory FORESHADOW: memory FOREnSics of HArDware CryptOcurrency wallets – a tool and visualization framework, Forensic Sci. Int.: Digit. Invest. 33 (2020), 301002.

[44] M. Frowis, T. Gottschalk, B. Haslhofer, C. Ruckert, P. Pesch, Safeguarding the evidential value of forensic cryptocurrency investigations, Forensic Sci. Int.: Digit. Invest. 33 (2020), 200902.

[45] S. Castell, Authored by AI- Here be crypto dragons: it's all about the evidence, Solicitors' J. 162 (2019) 42–45.

[46] W. Koerhuis, T. Kechadi, N.-A. Le-Khac, Forensic analysis of privacy-oriented cryptocurrencies, Forensic Sci. Int. 33 (2020), 200891.

[47] S. Dyson, W. Buchanan, L. Bell, Scenario-based creation and digital investigation of Ethereum ERC20 tokens, Forensic Sci. Int.: Digit. Invest. 32 (2020), 200894.

[48] A. Jones, S. Vidalis, Rethinking digital forensics, Ann. Emerg. Technol. Comput. 3 (2) (2019) 42–53.

[49] E. OliveiraJr, A. Zorzo, C. Neu, Towards a conceptual model for promoting digital forensics experiments, Forensic Sci. Int.: Digit. Invest. 35 (2021), 301014.

[50] J. Schneider, H.-P. Deifel, S. Milius, F. Freiling, Unifying metadata-based storage reconstruction and carving with LAYR, Forensic Sci. Int.: Digit. Invest. 33 (2020), 301006.

[51] M. Kumar, Solid state drive forensics analysis – challenges and recommendations, Concurrency Comput. Pract. Ex. 33 (24) (2021), e6442.

[52] J. Abraham, R. Ng, M. Morelato, M. Tahtouh, C. Roux, Automatically classifying crime scene images using machine learning methodologies, Forensic Sci. Int.: Digit. Invest. 39 (2021), 301273.

[53] J. Bang, J. Park, S. Lee, Visio: an empirical framework for examiners to accessing password-protected resources for on-the-scene digital investigations, Forensic Sci. Int.: Digit. Invest. 40 (2022), 301376.

[54] C. Hassenfeldt, J. Jacques, I. Baggili, Exploring the learning efficacy of digital forensics concepts and bagging & tagging of digital devices in immersive virtual reality, Forensic Sci. Int.: Digit. Invest. 33 (2020), 301011.

[55] G. Horsman, Contemporaneous notes for digital forensic examinations, Forensic Sci. Int.: Digit. Invest. 37 (2021), 301173.

[56] G. Horsman, Conducting a 'manual examination' of a device as part of a digital investigation, Forensic Sci. Int.: Digit. Invest. 40 (2022), 301331.

[57] D. Palmbach, F. Breitinger, Artifacts for detecting timestamp manipulation in NTFS on Windows and their reliability, Forensic Sci. Int.: Digit. Invest. 32S (2020) S1–S9. DFRWS 2020 EU – Proceedings of the Seventh Annual DFRWS Europe.

[58] A. Thierry, T. Muller, A systemic approach to understanding MACB timestamps on Unix-like systems, Forensic Sci. Int.: Digit. Invest. 40 (2022), 301338.

[59] H. Kim, I. Kim, K. Kim, AIBFT: artificial intelligence browser forensic toolkit, Forensic Sci. Int.: Digit. Invest. 36 (2021), 301091.

[60] R. Yakota, Y. Hawai, K. Tsuchiya, D. Imoto, M. Hirabayashi, N. Akiba, H. Kakuda, K. Tanabe, M. Honma, K. Kurosaw, A revisited visual-based geolocalization framework for forensic investigation support tools, Forensic Sci. Int.: Digit. Invest. 35 (2020), 301088.

[61] C. Galbraith, P. Smyth, H. Stern, Statistical methods for the forensic analysis of geolocated event data, Forensic Sci. Int.: Digit. Invest. 33 (2020), 301009.

[62] S. Ge, M. Xu, T. Qiao, N. Zheng, A novel file carving algorithm for docker container logs recorded by json-file logging driver, Forensic Sci. Int.: Digit. Invest. 39 (2021), 301272.

[63] M. Martin-Perez, R. Rodrigues, F. Breitinger, Forensic Sci. Int. Digit. Invest. 36 (2021), 301120.

[64] F. Amato, A. Castiglione, Cozzolino, F. Narducci, A semantic-based methodology for digital forensic analysis, J. Parallel Distr. Comput. 138 (2020) 172–177.

[65] D. Closser, E. Bou-Harb, A live digital forensics approach for quantum mechanical computers, Forensic Sci. Int.: Digit. Invest. 40 (2022), 301341.

[66] G. Horsman, Defining principles for preserving privacy in digital forensic examinations, Forensic Sci. Int.: Digit. Invest. 40 (2022), 301350.

[67] M. Seyyar, Z. Geradts, Privacy impact assessment in large-scale digital forensic examinations, Forensic Sci. Int. 33 (2020), 200906.

[68] G. Horsman, N. Sunde, Part 2: the phase-oriented advice and review structure (PARS) for digital forensic investigations, Forensic Sci. Int.: Digit. Invest. 36 (2021), 301074.

[69] E. Kouokam, A. Dirik, PRNU-based source device attribution for YouTube videos, Digit. Invest. 29 (2019) 91–100.

[70] D. Cunha, E. Silva, J. Lambert, R. Ribeiro, Peritus Framework: towards multimedia evidence analysis uniformization in Brazilian distributed forensic model, Forensic Sci. Int.: Digit. Invest. 35 (2021), 301089.

[71] P. Mullan, C. Riess, F. Freiling, Towards openset forensic source grouping on JPEG header information, Forensic Sci. Int.: Digit. Invest. 32 (2020), 300916.

[72] F. Ahmed, F. Khelifi, A. Lawgaly, A. Bouridane, A machine learning-based approach for picture acquisition timeslot prediction using defective pixels, Forensic Sci. Int. 39 (2021), 301311.

[73] T. Latzo, R. Palutke, F. Freiling, A universal taxonomy and survey of forensic memory acquisition techniques, Digit. Invest. 28 (2019) 56–69.

[74] F. Block, A. Dewald, Windows. Memory forensics: detecting (un)intentionally hidden injected code by examining page table entries, Digit. Invest. 29 (2019) S3–S12.

[75] T. Latzo, R. Palutke, F. Freiling, A universal taxonomy and survey of forensic memory acquisition techniques, Digit. Invest. 28 (2019) 56–69.

[76] J. Stuttgen, M. Cohen, Anti-forensic resilient memory acquisition, Digit. Invest. 10 (2013) S105–S119.

[77] R. Yehuda, E. Shlingbaum, Y. Gershfeld, S. Tayouri, N. Zaidenberg, Hypervisor memory acquisition for ARM, Forensic Sci. Int.: Digit. Invest. 37 (2021), 301106.

[78] S. Davies, R. Macfarlane, W. Buchanan, Evaluation of live forensic techniques in ransomware attack mitigation, Forensic Sci. Int.: Digit. Invest. 33 (2020), 300979.

[79] D. Uroz, R. Rodriguez, Characteristics and detectability of Windows auto-start extensibility pints in memory forensics, Digit. Invest. 28 (2019) S95–S104.

[80] F. Block, A. Dewald, Windows. Memory forensics: detecting (un)intentionally hidden injected code by examining page table entries, Digit. Invest. 29 (2019) S3–S12.

[81] D. Uroz, R. Rodriguez, On challenges in verifying trusted executable files in memory, Forensic Sci. Int.: Digit. Invest. 32 (2020), 300917.

[82] T. Latzo, J. Brost, F. Freiling, BMCLeech: introducing stealthy memory forensics to, BMC. Forensic Sci. Int.: Digit. Invest. 32 (2020), 300919.

[83] C. Yucel, A. Koltuksuc, Imaging and evaluating the memory access for malware, Forensic Sci. Int.: Digit. Invest. 32 (2020), 200903.

[84] N. Naik, P. Jenkins, N. Savage, L. Yang, T. Boongoen, N. Iam-On, Fuzzy-import hashing: a static analysis technique for malware detection, Forensic Sci. Int.: Digit. Invest. 37 (2021), 301139.

[85] T. Groß, M. Busch, T. Müller, Forensic Sci. Int.: Digit. Evid. 36 (2021), 301113.

[86] A. Case, R. Maggio, M. Manna, G. Richard, Memory analysis of macOS page queues, Forensic Sci. Int.: Digit. Invest. 33 (2020), 301004.

[87] P. Casey, R. Lindsay-Decusati, I. Baggili, F. Breitinger, Inception: virtual space in memory space in real space – memory forensics of immersive reality in the HTC Vive. Digital Investigation, in: DFRWS 2019 USA – Proceedings of the Nineteenth Annual DFRWS USA, vol. 29, 2019, pp. S13–S21.

[88] P. Casey, R. Lindsay-Decusati, I. Baggili, F. Breitinger, Inception: virtual space in memory space in real space – memory forensics of immersive reality in the HTC Vive. Digital Investigation, in: DFRWS 2019 USA – Proceedings of the Nineteenth Annual DFRWS USA, vol. 29, 2019, pp. S13–S21.

[89] F. Tofflani, A. Oliveri, M. Graziano, J. Zhou, The vidence beyond the wall: memory forensic in SGX environments, Forensic Sci. Int.: Digit. Invest. 39 (2021), 301313.

[90] L. Sikos, Packet analysis for network forensics: a comprehensive survey, Forensic Sci. Int.: Digit. Invest. 32 (2020), 200892.

[91] J. Pluskal, F. Breitinger, O. Rysavy, Netfox detective: a novel open-source network forensics analysis tool, Forensic Sci. Int.: Digit. Invest. 35 (2020), 301019.

[92] S. Sentanoe, H. Reiser, SSHkex: leveraging virtual machine introspection for extracting SSH keys and decrypting SSH network traffic, Forensic Sci. Int.: Digit. Invest. 40 (2022), 301337.

[93] M. Karresand, S. Axelsson, G. Dyrkolbotn, Using NTFS cluster allocation behaviour to find the location of the user, Digit. Invest. 29 (2019). DFRWS 2019 USA – Proceedings of the Nineteenth Annual DFRWS USA, S51-S60.

[94] J.-N. Hilgert, M. Lambertz, M. Rybalka, R. Schell, Syntactical carving of PNGs and automated generation of reproducible datasets, Digit. Invest. 29 (2019) S22–S30.

[95] K. Odogwu, P. Gladyshev, B. Habibnia, PNG data detector for DECA, Forensic Sci. Int.: Digit. Invest. 32 (2020), 300910.

[96] J.-N. Hilgert, M. Lambertz, M. Rybalka, R. Schell, Syntactical carving of PNGs and automated generation of reproducible datasets, Digit. Invest. 29 (2019) S22–S30.

[97] M. Karresand, S. Axelsson, G. Dyrkolbotn, Using NTFS cluster allocation behaviour to find the location of the user, Digit. Invest. 29 (2019). DFRWS 2019 USA – Proceedings of the Nineteenth Annual DFRWS USA, S51-S60.

[98] R. Nordvik, K. Porter, F. Toolan, S. Axelsson, K. Franke, Generic metadata time carving, Forensic Sci. Int.: Digit. Invest. 33 (2020), 301005.

[99] F. Faust, A. Thierry, T. Muller, F. Freiling, Selective imaging of file system data on live systems, Forensic Sci. Int.: Digit. Invest. 36 (2021), 301115.

[100] J. Choi, J. Park, S. Lee, Forensic exploration on windows file history, Forensic Sci. Int.: Digit. Invest. 26 (2021), 301134.

[101] M. Karresand, G. Dyrkolbotn, S. Axelsson, An empirical study of the NTFS cluster allocation behaviour over time, Forensic Sci. Int.: Digit. Invest. 33 (2020), 301008.

[102] E. Casey, Digital stratigraphy: contextual analysis of file system traces in forensic science, J. Forensic Sci. 63 (45) (2018) 1383–1391.

[103] j. Oh, S. Lee, H. Hwang, NTFS Data Tracker: tracking file data history based on $LogFile, Forensic Sci. Int.: Digit. Invest. 39 (2021), 301309.

[104] M. Um, J. Han, S. Lee, File fingerprinting of the ZIP format for identifying and tracking provenance, Forensic Sci. Int. 39 (2021), 301271.

[105] P. Prade, T. Gros, A. Dewald, Forensic analysis of the resilient file system (resilient file system) version 3.4, Forensic Sci. Int.: Digit. Invest. 32 (2020), 300915.

[106] M. Jarrett, S. Morris, Purple dawn: dead disk forensics on Google's Fuchsia operating system, Forensic Sci. Int.: Digit. Invest. 39 (2021), 301269.

[107] E. Harshany, R. Benton, D. Bourrie, W. Glisson, Big data forensics: Hadoop 3.2.0 reconstruction, Forensic Sci. Int. Digit. Invest. 32 (2020), 300909. DFRWS 2020 EU – Proceedings of the Seventh Annual DFRWS Europe.

[108] R. Mohammad, M. Alquhtani, A comparison of machine learning techniques for file system analysis, J. Inf. Secur. Appl. 46 (2019) 53–61.

[109] R. Nordvik, R. Stoykova, K. Franke, S. Axelsson, Reliability validation for file system interpretation, Forensic Sci. Int.: Digit. Invest. 37 (2021), 301174.

[110] M. Park, O. Yi, J. Kim, A methodology for the decryption of encrypted smartphone backup data on android platform: a case study on the latest Samsung smartphone backup system, Forensic Sci. Int.: Digit. Invest. (2020), 301026.

[111] S. Kang, G. Kim, M. Park, J. Kim, Methods for decrypting the data encrypted by the latest Samsung smartphone backup programs in Windows and macOS, Forensic Sci. Int.: Digit. Invest. 39 (2021), 301310.

[112] A. Kanta, I. Coisel, M. Scanlon, A survey exploring open source intelligence for smarter password cracking, Forensic Sci. Int.: Digit. Invest. 35 (2020), 301075.

[113] P. McLaren, G. Russell, W. Buchanan, Z. Tan, Decrypting live SSH traffic in virtual environments, Digit. Invest. 29 (2019) 109–117.

[114] S. Lanagan, K.-K. Choo, On the need for AI to triage encrypted data containers in U.S. law enforcement applications, Forensic Sci. Int.: Digit. Invest. 38 (2021), 301217.

[115] J. Schneider, J. Wolf, F. Freiling, Tampering with digital evidence is hard: the case of main memory images, Forensic Sci. Int.: Digit. Invest. 32 (2020), 300924.

[116] G. Horsman, D. Errickson, When nothing may be evidence of something: anti-forensics and digital toolmarks, Sci. Justice 59 (2019) 565–572.

[117] W. Bhat, A. AlZahrani, M. Wani, Can computer forensic tools be trusted in digital investigations? Sci. Justice 61 (2021) 198–203.

[118] National Institute of Standards and Technology, NIST Special Publication 800-88, Revision 1, Guidelines for Media Sanitization, 2014. Retrieved from, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf.

[119] A. Jones, I. Afrifa, An evaluation of data erasing tools, J. Digit. Forensic. Secur. Law 15 (1) (2020) 1–20.

[120] J. Schneider, J. Wolf, F. Freiling, Tampering with digital evidence is hard: the case of main memory images, Forensic Sci. Int.: Digit. Invest. 32 (2020). DFRWS 2020 EU – Proceedings of the Seventh Annual DFRWS Europe, pp300924.

[121] J. Schneider, L. Dusel, B. Lorch, J. Drafz, F. Freiling, Prudent design principles for digital tampering experiments, Forensic Sci. Int.: Digit. Invest. 40 (2022), 301334.

[122] G. Horsman, D. Errickson, When nothing may be evidence of something: anti-forensics and digital toolmarks, Sci. Justice 59 (2019) 565–572.

[123] G. Horsman, The challenge of identifying historic 'private browsing' sessions on suspect devices, Forensic Sci. Int.: Digit. Invest. 34 (2020), 300980.

[124] R. Palutle, F. Block, P. Reichenberger, D. Stripeika, Hiding process memory via anti-forensic techniques, Forensic Sci. Int.: Digit. Invest. 33 (2020), 301012.

[125] D. Mothi, H. Janicke, I. Wagner, A novel principle, to validate digital forensic models, Forensic Sci. Int.: Digit. Invest. 33 (2020), 200904.

[126] S. Hasanabadi, A. Lashkari, A. Ghorbani, A game-theoretic approach for forensic investigators against rootkits, Forensic Sci. Int.: Digit. Invest. 33 (2020), 200909.

[127] S. Hasanabadi, A. Lashkari, A. Ghorbani, A survey and research challenges of anti-forensics: evaluation of game-theoretic models in simulation of forensics agents' behaviour, Forensic Sci. Int.: Digit. Invest. 35 (2020), 301024.

[128] M. Herman, M. Iorga, A. Salim, R. Jackson, M. Hurst, R. Leo, R. Lee, N. Landreville, A. Mishra, Y. Wang, R. Sardinas, NIST Cloud Computing Forensic Science Challenges. NISTIR 8006, National Institute of Standards and Technology. U.S. Department of Commerce, 2020.

[129] B. Manral, G. Somani, K.-K. Choo, M. Conti, M. Gaur, A systematic review on cloud forensics challenges, solutions, and future directions, ACM Comput. Surv. 56 (6) (2019) 124, 124:28.

[130] M. Herman, M. Iorga, A. Salim, R. Jackson, M. Hurst, R. Leo, R. Lee, N. Landreville, A. Mishra, Y. Wang, R. Sardinas, NIST Cloud Computing Forensic Science Challenges. NISTIR 8006, National Institute of Standards and Technology. U.S. Department of Commerce, 2020.

[131] G. Horsman, What's in the Cloud? – an examination of the impact of cloud storage usage on the browser cache, J. Digit. Forensic. Secur. Law 15 (1) (2020) 1–16.

[132] A. Akilal, M.-T. Kechadi, An improved forensic-by-design framework for cloud computing with systems engineering standard compliance, Forensic Sci. Int.: Digit. Invest. 40 (2022), 301315.

[133] NIST, NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management, Technical Report, National Institute of Standards and Technology, 2020. Retrieved from, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf.

[134] N. Dalezios, S. Shiales, N. Kolokotronis, B. Ghita, Digital forensics cloud log unification: implementing cloud auditing data federation in Apache CloudStack, J. Inf. Secur. Appl. 54 (2020), 102555.

[135] X. Zhang, J. Grannis, I. Baggili, N. Beebe, Frameup: an incriminatory attack on Storj: a peer to peer blockchain enabled distributed storage system, Digit. Invest. 29 (2019) 28–42.

[136] P. Lutta, M. Sedky, M. Hassan, U. Jayawickrama, B. Bastaki, The complexity of internet of things forensics: a state-of-the-art review, Forensic Sci. Int.: Digit. Invest. 38 (2021), 301210.

[137] X. Zhang, O. Upton, N.L. Beebe, K.-K.R. Choo, IoT botnet forensics: a comprehensive digital forensic case study on Mirai botnet servers, Forensic Sci. Int.: Digit. Invest. 32 (2020), 300926.

[138] S. Torabi, E. Bou-Hard, C. Assi, M. Debbabi, A scalable platform for enabling the forensic investigation of exploited IoT devices and their generated unsolicited activities, Forensic Sci. Int.: Digit. Invest. 32 (2020), 300922.

[139] Y. Shin, H. Kim, S. Kim, D. Yoo, W. Jo, T. Shon, Certificate injection-based encrypted traffic forensic in AI speaker ecosystem, Forensic Sci. Int.: Digit. Invest. 33 (2020), 301010.

[140] P. Lutta, M. Sedky, M. Hassan, U. Jayawickrama, B. Bastaki, The complexity of internet of things forensics: a state-of-the-art review, Forensic Sci. Int.: Digit. Invest. 38 (2021), 301210.

[141] P. Lutta, M. Sedky, M. Hassan, U. Jayawickrama, B. Bastaki, The complexity of internet of things forensics: a state-of-the-art review, Forensic Sci. Int.: Digit. Invest. 38 (2021), 301210.

[142] J.-P. Sandvik, K. Franke, H. Abie, A. Arnes, Quantifying data volatility for IoT forensics with examples from Contiki S, Forensic Sci. Int.: Digit. Invest. 2022 (2022), 301343.

[143] J. Castelo Gomez, J. Carillo Mondejar, J. Roldan Gomez, J. Martinez Martinez, Developing an IoT forensic methodology. A concept proposa, Forensic Sci. Int.: Digit. Evid. 36 (2021), 301114.

[144] T. Heckman, T. Souvignet, D. Sauveron, D. Naccache, Medical equipment used for forensic data extraction: a low-cost solution for forensic laboratories not provided with expensive diagnostic or advanced repair equipment, Forensic Sci. Int.: Digit. Invest. 36 (2021), 301092.

[145] V. Paxson, Bro: a system for detecting network intruders in real-time, Comput. Network. 31 (23–24) (1999) 2435–2463.

[146] M. Roesch, et al., Snort: lightweight intrusion detection for networks, Lisa 99 (1999) 229–238.

[147] M. Pour, E. Bou-Hard, K. Varma, N. Neshenko, D. Pados, K.-K. Choo, Comprehending the IoT cyber threat landscape: a dimensionality reduction technique to infer and characterise Internet-scale IoT probing campaigns, Digit. Invest. 28 (2019) S40–S49.

[148] Y. Tok, C. Wang, S. Chattopadhyay, Stitcher: correlating digital forensic evidence on internet-of-things devices, Forensic Sci. Int. Digit. Invest. 35 (2021), 301071.

[149] P. Agbedanu, A. Jurcut, BLOFF: A Blockchain-based Forensic Model in IoT. Published in Revolutionary Applications of Blockchain-Enabled Privacy and Access Control, IGI Global, 2021. Retrieved from, https://arxiv.org/pdf/2103.08442.pdf.

[150] A. Sayakkara, N.-A. Le-Khac, M. Scanlon, A survey of electromagnetic side-channel attacks and discussion on their case-progressing potential for digital forensics, Digit. Invest. 29 (2019) 43–54.

[151] A. Sayakkara, N.-A. Le-Khac, M. Scanlon, EMvidence: a framework for digital evidence acquisition from IoT devices through electromagnetic side-channel analysis, Forensic Sci. Int.: Digit. Invest. 32 (2020), 300907.

[152] Sakakkara, A., Le-Khac, N-A. and Scanlon, M. Leveraging electromagnetic side-channel analysis for the investigation of IoT devices. Digit. Invest.: DFRWS 2019 USA – Proceedings of the Nineteenth Annual DFRWS USA, 29, S94-S103.

[153] Q. Le, L. Miralles-Pechuan, A. Sayakkara, N.-A. Le-Khac, M. Scanlon, Identifying Internet of Things software activities using deep learning-based electromagnetic side-channel analysis, Forensic Sci. Int.: Digit. Invest. 39 (2021), 301308.

[154] A. Sayakkara, N.-A. Le-Khac, M. Scanlon, Facilitating electromagnetic side-channel analysis for IoT investigation: evaluating the EMvidence framework, Forensic Sci. Int.: Digit. Invest. 33 (2020), 301003.

[155] J. van Zandwijk, A. Boztas, The phone reveals your motion: digital traces of walking, driving and other movements on iPhones, Forensic Sci. Int.: Digit. Invest. 37 (2021), 301170.

[156] E. Casey, D.-O. Jacquet-Chiffelle, H. Spicheger, E. Ryser, Structuring the evaluation of location-related mobile device evidence, Forensic Sci. Int.: Digit. Invest. 32 (2020), 300928.

[157] M. Tart, I. Brodie, N. Patrick-Gleed, B. Edwards, K. Weeks, R. Moore, R. Haseler, Cell site analysis: use and reliability of survey methods, Digit. Invest. 38 (2021), 301222.

[158] M. Tart, S. Pope, D. Baldwin, R. Bird, Cell site analysis: roles and interpretation, Sci. Justice 59 (2019) 558–564.

[159] D. Kim, S. Lee, Study of identifying and managing the potential evidence for effective Android forensics, Forensic Sci. Int.: Digit. Invest. 33 (2020), 200897.

[160] Y. Zhang, B. Li, Y. Sun, Android encryption database forensic analysis based on static analysis, in: CSAE 2020: Proceedings of the 4th International Conference on Computer Science and Application Engineering, 2020.

[161] G. Kim, M. Park, J. Kim, A study on LG content lock and data acquisition from apps based on content lock function, Forensic Sci. Int.: Digit. Invest. 39 (2021), 301284.

[162] J. Gregoria, B. Alarcos, A. Gardel, Forensic analysis of Nucleus RTOS and MTK smartwatches, Digit. Invest. 29 (2019) 55–66.

[163] A. Fukami, K. Nishimura, Forensic analysis of water damaged mobile devices, Digit. Invest. 29 (2019) S71–S79.

[164] K. Gomez Buquerin, C. Corbett, H.-J. Hof, Forensic Sci. Int.: Digit. Invest. 36 (2021), 301111.

[165] K. Dolos, C. Meyer, A. Attenberger, J. Steinberger, Driver identification using in-vehicle digital data in the forensic context of a hit and run accident, Forensic Sci. Int.: Digit. Invest. 35 (2020), 301090.

[166] R. Rak, D. Kopencova, M. Felcan, Digital vehicle identity – digital VIN in forensic and technical practice, Forensic Sci. Int.: Digit. Invest. 39 (2021), 301307.

[167] K. Malinova, G. Kasanicky, J. Podhorsky, Usagae of digital evidence in the technical analysis of traffic collisions, in: 14th International Scientific Conference on Sustainable, Modern and Safe Transport. in: Transport Research Procedia, vol. 55, 2021, pp. 1737–1744.

[168] T. Holt, D. Dolliver, Exploring digital evidence recognition among front-line law enforcement officers at fatal crash scenes, Forensic Sci. Int.: Digit. Invest. 37 (2021), 301167.

[169] C. Alexakos, C. Katsini, K. Votis, A. Lalas, D. Tzorvaras, D. Serpanos, Enabling digital forensics readiness in Internet of Vehicles, in: 23rd EURO Working Group on Transportation Meeting, EWGT 2020, 16-18 September 2020, Paphos, Cyprus. in: Transportation Research Procedia, vol. 52, 2021, pp. 339–346.

[170] K. Gomez Buquerin, C. Corbett, H.-J. Hof, Forensic Sci. Int.: Digit. Invest. 36 (2021), 301111.

[171] N. Park, W. Lee, S. Lim, J. Byun, G.-H. Na, I.-Y. Jeon, Energy-based linear CM audio recovery method of impaired MP4 file stored in dashboard camera memory, Forensic Sci. Int.: Digit. Invest. 39 (2021), 301274.

[172] Pessolano, G., Read, H., Sutherland, I. and Xynos, K. Forensic analysis of the Nintendo 3DS NAND. Digit. Invest., 29, S61-S70.

[173] Barr-Smith, F., Farrant, T., Leonard-Lagarde, B., Rigby, D., Rigby, S. and Subley-Calder, F. Dead man's switch: forensic autopsy of the Nintendo Switch. Forensic Sci. Int.: Digit. Invest., 36, 301110.

[174] Y. Fang, C. Zhao, C. Huang, L. Liu, SankeyVis: visualizing active relationship from emails based on multiple dimensions and topic classification methods, Forensic Sci. Int.: Digit. Invest. 35 (2021), 300981.

[175] M. Bin Azhar, R. Cox, A. Chamberlain, Forensic investigations of popular ephemeral messaging application on Android and iOS platforms, Int. J. Adv. Secur. 13 (1&2) (2020) 41–53.

[176] J. Son, Y. Kim, D. Oh, K. Kim, Forensic analysis of instant messengers: decrypt signal, Wicky and Threema, Forensic Sci. Int.: Digit. Invest. 40 (2022), 301347.

[177] P. Fernandez-Alvarez, R. Rodrguez, Extraction and analysis of retrievable memory artifacts from Windows Telegram Desktop application, Forensic Sci. Int.: Digit. Invest. 40 (2022), 301341.

[178] G. Kim, M. Park, S. Lee, Y. Park, I. Lee, A study on the decryption methods of telegram X and BBM-Enterprise databases in mobile and PC, Forensic Sci. Int.: Digit. Invest. 35 (2020), 300998.

[179] s. Shin, G. Kim, S. Kim, J. Kim, Forensic analysis of note and journal applications, Forensic Sci. Int.: Digit. Invest. 40 (2022), 301355.

[180] R. Matthews, K. Lovell, M. Sorell, Ghost protocol – snapchat as a method of surveillance, Forensic Sci. Int.: Digit. Invest. 36 (2021), 301112.

[181] X. Zhang, F. Breitinger, E. Kuechinger, S. O'Shaughnessy, Android application forensics: a survey of abfuscation, obfuscation detection and deobfuscation techniques and their impact on investigations, Forensic Sci. Int.: Digit. Evid. 39 (2021), 301285.

[182] A. Mahr, M. Cichon, S. Mateo, C. Grajda, I. Baggili, Zooming into the pandemic! A forensic analysis of the Zoom application, Forensic Sci. Int.: Digit. Invest. 36 (2021), 301107.

[183] M. Nicoletti, M. Bernaschi, Forensic analysis of microsoft skype for business, Digit. Invest. 29 (2019) 159–179.

[184] S. Kim, G. Kim, S. Shin, B. Youn, J. Song, I. Lee, J. Kim, Methods for recovering deleted data from the realm database: case study on Minitalk and Xabber, Forensic Sci. Int.: Digit. Invest. 40 (2022), 301353.

[185] A. Akinbi, E. Ojie, Forensic analysis of open-cource XMPP multi-client social networking apps on iOS devices, Forensic Sci. Int.: Digit. Invest. 36 (2021), 301122.

[186] G. Schipper, R. Seelt, N.-A. Le-Khac, Forensic analysis of Matrix protocol and Riot.im application, Forensic Sci. Int.: Digit. Invest. 36 (2021), 301118.

[187] G. Kim, S. Kim, M. Park, Y. Park, I. Lee, J. Kim, Forensic analysis of instant messaging apps: decrypt Wickr and private text messaging data, Forensic Sci. Int.: Digit. Invest. 37 (2021), 301138.

[188] G. Dorai, S. Aggarwal, N. Patel, C. Powell, VIDE – Vault app identification and extraction systems for iOS devices, Forensic Sci. Int.: Digit. Invest. 33 (2020), 301007.

[189] N. Mutawa, Bryce, V. Franqueira, A. Marrington, J. Read, Behavioural Digital Forensics Model: embedding behavioural analysis into the investigation of digital crimes, Digit. Invest. 28 (2019) 70–82.

[190] N. Mutawa, Bryce, V. Franqueira, A. Marrington, J. Read, Behavioural Digital Forensics Model: embedding behavioural analysis into the investigation of digital crimes, Digit. Invest. 28 (2019) 70–82.

[191] R. Rouhi, F. Bertini, D. Montesi, User profiles' image clustering for digital investigation, Forensic Sci. Int.: Digit. Invest. 38 (2021), 301171.

[192] N. Zubair, A. Ayub, H. Yoo, I. Ahmed, PEM: remote forensic acquisition of PLC memory in industrial control systems, Forensic Sci. Int.: Digit. Invest. 40 (2022), 3013376.

[193] S. Qasim, J. Smith, I. Ahmed, Control logic forensics framework using built-in decompiler of engineering software in industrial control systems, Forensic Sci. Int.: Digit. Invest. 33 (2020), 301013.

[194] J. Shin, H. Choi, J. Seo, A study on command block collection and restoration techniques through detection of project file manipulation on engineering workstation detection of project file manipulation on engineering workstation of industrial control system, Forensic Sci. Int.: Digit. Invest. 40 (2022), 301354.

[195] E. Karafili, L. Wang, E. Lupu, An argumentation-based reasoner to assist digital investigation and attribution of cyber-attacks, in: Forensic Science International: Digital Investigation, 32S, DFRWS 2020 EU – Proceedings of the Seventh Annual DFRWS Europe, 2020, pp. S1–S9.

[196] P. Sommer, Evidence from hacking: a few tiresome problems, Forensic Sci. Int.: Digit. Invest. 40 (2022), 301333.

[197] M. Steinbach, S. Zenglein, K. Brandl, Phishing detection on hidden tor services, Forensic Sci. Int.: Digit. Invest. 36 (2021), 301117.

[198] O. Ribaux, T. Souvignet, Hello are you available?" Dealing with online frauds and the role of forensic science, Forensic Sci. Int.: Digit. Invest. 33 (2020), 300978.

[199] S. Davies, R. Macfarlane, W. Buchanan, NapierOne: a modern mixed file data set alternative to Govdoc1, Forensic Sci. Int.: Digit. Invest. 40 (2022), 301330.

[200] B. Manral, G. Somani, Establishing forensics capabilities in the presence of superuser insider threats, Forenic Sci. Int.: Digit. Invest. 38 (2021), 301263.

[201] T. Grivna, J. Drapal, Attacks on the confidentiality, intengrity and availability of data and computer systems in the criminal case law of the Czech Republic, Digit. Invest. 28 (2019) 1–13.

[202] M. Kavazovic, D. Pajevic, M. Lucic-Catic, P. Puharic, Digital evidence handling in practice of police agencies in b&h, Crim. Justice Issues J. Crim. Justice, Criminol. Secur. Stud. (5) (2019) 351–388, 2019.

[203] D. Ennin, R. Mensah, Cybercrime in Ghana and the reaction of the law, J. Law, Policy Glob. 84 (2019) 36–45.

[204] T. Krishnakumar, Law enforcement access to data in India: considering the past, present, and future of section 91 of the code of criminal procedure, 1973, Indian J. Law Technol. 15 (1) (2019) 67–101.

[205] D. Kusuma Wardani, S. Soewondo, Judhariksawan, A. Magassing, Electronic evidence in criminal procedural law, J. Law, Policy Glob. 104 (2020) 1–5.

[206] J. Kancauskiene, Computer forensics and electronic evidence in criminal legal proceedings: Lithuania's experience, Digit. Evid. Electron. Signature Law Rev. 16 (2019) 11–24.

[207] P. Kahle, Cyber violence against women and girls in Nepal, Kathmandu School Law Rev. 7 (1) (2019) 85–99.

[208] F. Eboibi, I. Mac-Barango, Law and judicial application of digital forensic science in Nigeria, J. Law, Policy Glob. 96 (2020) 61–75.

[209] F. Gozukara, Challenges and possible severe legal consequences of application users information from CNG-Logs, Forensic Sci. Int.: Digit. Invest. 39 (2021), 301312.

[210] J. Riekkinen, Electronic evidence in criminal procedure: on the effects of ICT and the development towards the network society on the life-cycle of evidence, Digit. Evid. Electron. Signature Law Rev. 16 (2019) 6–10.

[211] A. Maurushat, A. Bello, B. Bragg, Artificial intelligence enabled cyber fraud: a detailed look into payment diversion fraud and ransomware, Indian J. Law Technol. 15 (2) (2019) 261–299.

[212] D. Send, S. Mason, Artificial intelligence and evidence, Singapore Acad. Law J. 33 (Special Issue) (2021) 241–279.

[213] A. Flynn, Physical fruits vs. digital fruits: why patane should not apply to the contents of digital devices, Univ. Illinois J. Law Technol. Pol. (1) (2021) 1–34, 2021.

[214] M. Noval, Digital evidence in criminal cases before the U.S. Courts of Appeal: trends and issues for consideration, J. Digit. Forensic. Secur. Law 14 (4) (2020) 1–42.

[215] Decision No 50. Haskova District Court, Civil Division, II appellate civil panel, Bulgaria; civil procedure code; formation of contract; electronic evidence; exchanges via social networking website; proof, Digit. Evid. Electron. Signature Law Rev. 16 (2019) 57–59.

[216] K. Ruseva, Commentary, Digit. Evid. Electron. Signature Law Rev. 16 (2019) 60.

[217] Hangzhou Huatai Yimai Culture Media Co., Ltd, V. Shenzhen Daotong Technology Development Co., Ltd, Zhe 0192 civial case, first court No. 81. Hangzhou internet court of the People's Republic of China, 27 June 2018 (2018), Digit. Evid. Electron. Signature Law Rev. 16 (2019) 61–70.

[218] Case TlnRnKo 09.01.2017, 1-15-9051, Tallin Circuit Court (9 January 2017). Estonia; VAT on property; admissibility of evidence collected by surveillance; digital evidence guidelines; continuity of evidence (also known as chain of custody); MD5 hash – whether sufficient to prove evidence not altered; status of opinion of external expert (a lawyer), Digit. Evid. Electron. Signature Law Rev. 16 (2019) 71–89.

[219] P. Sokol, L. Rozenfeldova, K. Lucivjanska, J. Harasta, IP addresses in the context of digital evidence in the criminal and civil case law of the Slovak Replublic, Forensic Sci. Int.: Digit. Invest. 32 (2020), 300918.

[220] National Police Chiefs' Council, Digital Forensic Science Strategy, 2020. Retrieved from, https://www.npcc.police.uk/Digital%20Forensic%20Science%20Strategy%202020.pdf.

[221] G. Horsman, Defining 'service levels' for digital forensic science organisations, Forensic Sci. Int.: Digit. Invest. 38 (2021), 301178.

[222] F. Bankole, A. Taiwo, I. Claims, An extended digital forensic readiness and maturity model, Forensic Sci. Int.: Digit. Invest. 40 (2022) 301348I.

[223] Not Reproduced Here.

[224] G. Horsman, Decision support for first responders and digital device prioritisation, Forensic Sci. Int.: Digit. Invest. 38 (2021), 301219.

[225] H. van Beek, J. van den Bos, A. Boztas, E. van Eijk, R. Schramp, M. Ugen, Digital forensics as a service: stepping up the game, Forensic Sci. Int.: Digit. Invest. 35 (2020), 301021.

[226] E. Casey, Editorial – crisis or opportunity? Forensic Sci. Int.: Digit. Invest. 32 (2020), 30091.

[227] Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, as Amended by Protocols Nos. 11 and 14, 4 November 1950, Article 6 - Right to a Fair Trial.

[228] N. Sunde, Strategies for safeguarding examiner objectivity and evidence reliability during digital forensic investigations, Forensic Sci. Int.: Digit. Invest. 40 (2022), 301317.

[229] G. Horsman, Formalising investigative decision making in digital forensics: proposing the digital evidence reporting and decision support (DERDS) framework, Digit. Invest. 28 (2019) 146–151.

[230] G. Horsman, Part 1:quality assurance mechanisms for digital forensic investigations: introducing the Verification of Digital Evidence framework, Forensic Sci. Int.: Rep. 2 (2020), 100038.

[231] G. Horsman, Part 2:- quality assurance mechanisms for digital forensic investigations: knowledge sharing and the Capsule of Evidence (CODE), Forensic Sci. Int.: Rep. 2 (2020), 100035.

[232] C. Neale, I. Kennedy, B. Proce, Y. Yu, B. Nuseieibeh, The case for zero trust digital forensics, Forensic Sci. Int.: Digit. Invest. 40 (2022), 301352.

[233] N. Sunde, I. Dror, A hierarchy of expert performance (HEP) applied to digital forensics: reliability and bias ability in digital forensics decision making, Forensic Sci. Int.: Digit. Invest. 37 (2021), 301175.

[234] N. Sunde, Strategies for safeguarding examiner objectivity and evidence reliability during digital forensic investigations, Forensic Sci. Int. Digit. Invest. 40 (2022), 301317.

[235] N. Sunde, I. Dror, A hierarchy of expert performance (Hierarchy of Expert Performance) applied to digital forensics: reliability and bias ability in digital forensics decision making, Forensic Sci. Int.: Digit. Invest. 37 (2021), 301175.

[236] G. Horsman, N. Sunde, Part 1: the need for peer review in digital forensics, Forensic Sci. Int.: Digit. Invest. 35 (2020), 301062.

[237] G. Horsman, Formalising investigative decision making in digital forensics: proposing the digital evidence reporting and decision support (DERDS) framework, Digit. Invest. 28 (2019) 146–151.

[238] D. Mothi, H. Janicke, I. Wagner, A novel principle to validate digital forensic models, Forensic Sci. Int.: Digit. Invest. 33 (2020), 200904.

[239] G. Horsman, Part 1:quality assurance mechanisms for digital forensic investigations: introducing the Verification of Digital Evidence framework, Forensic Sci. Int.: Rep. 2 (2020), 100038.

[240] E. Ryser, H. Spichiger, E. Casey, Structured decision making in investigations involving digital and multimedia evidence, Forensic Sci. Int.: Digit. Invest. 34 (2020), 301015.

[241] G. Horsman, Part 2:- quality assurance mechanisms for digital forensic investigations: knowledge sharing and the Capsule of Evidence (CODE), Forensic Sci. Int.: Rep. 2 (2020), 100035.

[242] N. Zahadat, Digital forensics, a need for credentials and standards, J. Digit. Forensic. Secur. Law 14 (1) (2019) 4–14, 2019.

[243] Editor's note – This Is not Strictly True. A Standard for Accreditation to ISO 17025 for Forensic Science Laboratories, Including Provisions for Digital Evidence, Is Available in Many Countries Including in Developed Economies. ISO 17025 Addresses the Requirements of a "Profession" Described Earlier by the Author and Additional Requirements. However, for Various Reasons, Many Agencies Choose not to Adopt the Standard..

[244] Forensic Science Regulator, Codes of Practice and Conduct: for Forensic Science Providers and Practitioners in the Criminal Justice System, FSR-C-100, Issue 7, 2021.

[245] Forensic Science Regulator, Codes of Practice and Conduct, Appendix: Digital Forensics Services, FST-C-107, Issue 2, 2020.

[246] R. Stoykova, Digital evidence: unaddressed threats to fairness and the presumption of innocence, Comput. Law Secur. Rep. 42 (2021), 105575.

[247] v Barberà, Spain, § 78; also, Capeau v. Belgium, no. 42914/98, 2005, p. 25.

[248] J. Jackson, S. Summers, The Internationalisation of Criminal Evidence: beyond the Common Law and Civil Law Traditions, Cambridge University Press, 2012.

[249] G. Tully, N. Cohen, D. Compton, G. Davies, R. Isbell, T. Watson, Forensic Sci. Int.: Digit. Invest. 32 (2020), 200905.

[250] A. Marshall, The unwanted effects of imprecise language in forensic science, Forensic Sci. Int.: Digit. Invest. 40 (2022), 301349.

[251] G. Horsman, Opinion: does the field of digital forensics have a consistency problem? Forensic Sci. Int.: Digit. Invest. 33 (2020), 300970.

[252] E. Casey, Strengthening trust: integration of digital investigation and forensic science, Forensic Sci. Int.: Digit. Invest. 33 (2020), 301000.

[253] C. Neale, I. Kennedy, B. Proce, Y. Yu, B. Nuseieibeh, The case for zero trust digital forensics, Forensic Sci. Int.: Digit. Invest. 40 (2022), 301352.

[254] E. Casey, The chequered past and risky future of digital forensics, Aust. J. Forensic Sci. 63 (2018) 1383–1391.

[255] P. Reedy, Interpol review of digital evidence, Forensic Sci. Int.: Synergy 2 (2020) 489–520.

[256] N. Hughes, U. Karabiyik, Towards reliable digital forensic investigations through measurement science, WIREs Forensic Sci. 2 (2020) e1367.

[257] P. Ladkin, B. Littlewood, H. Thimbleby, M. Thomas, The Law Commission presumption concerning the dependability of computer evidence, Digit. Evid. Electron. Signature Law 17 (2020) 1–14.

[258] R. Stoykova, S. Anderson, K. Franke, S. Axelsson, Reliability assessment of digital forensic investigations in the Norwegian police, Forensic Sci. Int.: Digit. Invest. 40 (2022), 301351.

[259] Forensic Science Regulator, Forensic Science Regulator Guidance: Method Validation in Digital Forensics, FSR-G-218, Issue 2, 2020.

[260] A. Marshall, Digital forensic tool verification: an evaluation of options for establishing trustworthiness, Forensic Sci. Int.: Digit. Invest. 38 (2021), 301181.

[261] T. Wu, F. Breitinger, S. O'Shaughnessy, Digital forensic tools: recent advances and enhancing the status quo, Forensic Sci. Int.: Digit. Invest. 34 (2020), 300999.

[262] A. Marshall, Digital forensic tool verification: an evaluation of options for establishing trustworthiness, Forensic Sci. Int.: Digit. Invest. 38 (2021), 301181.

[263] T. Gobel, S. Maltan, J. Turr, H. Baier, F. Mann, ForTrace – a holistic forensic data set synthesis framework, Forensic Sci. Int.: Digit. Invest. 40 (2022), 301344.

[264] N. Sunde, What does a digital forensics opinion look like? A comparative study of digital forensics and forensic science reporting practices, Sci. Justice 61 (2021) 586–596.

[265] E. Casey, Editorial: the epic story of scientific interpretation in digital investigations, Forensic Sci. Int.: Digit. Invest. 34 (2020), 301063.

[266] E. Casey, Standardization of forming and expressing preliminary evaluative opinions on digital evidence, Forensic Sci. Int.: Digit. Evid. 32 (2020), 200888.

[267] V. Franqueira, G. Horsman, Towards sound forensic arguments: structured argumentation applied to digital forensics practice, Forensic Sci. Int.: Digit. Invest. 32 (2020), 300923.

[268] T. Bolle, E. Casey, M. Jacquet, The role of evaluations in reaching decisions using automated systems supporting forensic analysis, Forensic Sci. Int.: Digit. Invest. 34 (2020), 301016.

[269] G. Horsman, Digital evidence certainty descriptors, Forensic Sci. Int.: Digit. Invest. 32 (2020), 200896.