

**MERU UNIVERSITY OF SCIENCE AND TECHNOLOGY**

**DEPARTMENT OF COMPUTER SCIENCE**

**BACHELOR OF SCIENCE IN COMPUTER SECURITY AND FORENSICS**

**CT206/104336/20**

**JAPHETH MUUSYA KASINYA**

**CCF 3457: NETWORK FORENSICS INVESTIGATIONS**

**TERM PAPER**

**BACKGROUND**

[Digital forensics](https://www.bluevoyant.com/services/digital-forensics) is the practice of identifying, acquiring, and analyzing electronic evidence. Today almost all criminal activity has a digital forensics element, and digital forensics experts provide critical assistance to police investigations. Digital forensic data is commonly used in court proceedings.

Forensic science is a multidisciplinary subject that uses scientific concepts and procedures to investigate crimes, evaluate evidence, and provide expert testimony in judicial cases. This concept is anchored by Locard's principle which states that when a perpetrator commits a crime, they inevitably bring something into the crimescene and leave with something from it (Byard et al., 2015). Digital forensics, commonly known as computer forensics, is a field of forensic science that investigates, analyzes, and recovers digital evidence from electronic devices and digital media. Therefore, network forensics focuses on monitoring, collecting, analyzing, and reconstructing network events in order to detect security incidents, intrusions, or other suspicious activity in a networked environment. Investigations in network forensics involve use of systematic procedures and tools that aid in finding evidential data or information in the networks.

**LITERATURE REVIEW**

**2.1 Digital forensics**

This forensic science field involves acquiring, preserving, retrieving, and presenting data that has been processed electronically and stored on computer media (Robles, 2020).

**2.1.1 Overview on forensics**

Forensics, originating from the Latin term "forensis" meaning "of the forum" or "public," has grown from its roots in ancient civilizations to become a sophisticated and diverse science. Its origins can be traced back to ancient civilizations like the Egyptians, who used primitive methods of fingerprinting and autopsy. The use of forensic evidence in court procedures gained traction during the Middle Ages when forensic science began in the late nineteenth century, with the concepts of forensic investigation and the interchange of trace evidence between crime sites and suspects (Wolstenholme et al., 2021). Today, forensic science consists of several processes, including evidence gathering, analysis, interpretation, and presentation. These steps entail a methodical investigation of physical, biological, and digital evidence utilizing specialized techniques and technology to discover facts, reconstruct events, and provide expert testimony in judicial processes.

**2.1.2 Forensics Basics and Criminalities**

Forensic analysis includes a variety of disciplines, including forensic biology (DNA analysis, bloodstain pattern analysis), forensic chemistry (drug analysis, toxicology), forensic anthropology (human remains identification), forensic odontology (dental analysis), forensic pathology (autopsy), and digital forensics. They play critical responsibilities in assisting law enforcement in solving crimes, determining guilt or innocence, and ensuring justice is served. Criminal offenses are illegal activities or behaviors that break societal standards and regulations. Criminal investigations use forensic evidence to identify and prosecute individuals who have committed crimes ranging from theft and assault to homicide, cybercrime, and terrorism. Investigators can use forensic techniques and approaches to find evidence, determine motives and timelines, link individuals to crime scenes, and ultimately bring offenders to justice.

**2.1.3 Advanced Topics in Computer and Network Forensics**

These topics dive deeper into specialized fields and new developments in the industry, dealing with progressively difficult problems and cutting-edge cyberthreats.

Network traffic analysis entails using advanced techniques such as deep packet inspection and machine learning to detect and mitigate network-based attacks and data exfiltration.

Memory Forensics examines volatile memory to retrieve information about ongoing programs, network connections, and malware artifacts, which is critical for detecting advanced cyber threats(Ec-Council, 2009).

Mobile device forensics is the process of extracting data from smartphones, wearables, and other devices in order to find evidence of criminal activity, conversations, and digital transactions.

Cloud forensics is evaluating digital evidence stored in cloud environments while resolving issues such as data sovereignty, isolation, and access control.

Malware analysis is the study of malicious software to better understand its behavior, dissemination mechanisms, and potential indicators of compromise, which helps with threat identification and mitigation (Ec-Council, 2009).

Automating tools and procedures for real-time security issue detection, analysis, and reaction can improve the effectiveness and scalability of cyber protection. This is known as incident response automation (Sivaprasad, 2017).

Expertise in cryptography and blockchain analytics is necessary for Blockchain Forensics, which tracks cryptocurrency transactions and smart contracts to uncover financial crime or money laundering operations.

**2.2 Forensic Modeling and Principles Forensic**

By simulating and analyzing forensic scenarios using mathematical, statistical, or computational tools, Forensic modeling helps with evidence interpretation and event reconstruction. These models can be used to replicate crime scenes, simulate directions, calculate the time of death, or forecast how forensic evidence would behave in certain scenarios.

The term "Principles of Forensic Science" refers to the basic ideas and procedures that underpin forensic investigations. These include the significance of context in interpreting evidence, the necessity of impartiality, objectivity, and integrity in forensic analysis, Locard's Exchange Principle (every contact leaves a trace), the necessity of upholding chain of custody, and the application of validated methods and protocols (Rogers et al., 2006). These principles and guidelines guarantee that evidence is gathered, examined, and interpreted truthfully and ethically in the interest of justice and the truth.

**2.2.1 Duplication Forensics Analytics**

The field of duplication forensics analytics focuses on finding and examining duplicate data in digital storage media, including file systems, disk images, and memory dumps. By exposing patterns of file replication, manipulation, or illegal copying, it assists investigators in locating duplicate files, folders, or data clusters. Reconstructing timelines of events is aided by duplicate forensics analytics, which evaluates the integrity of digital evidence and tracks the origin and dissemination of data (Mandia & Prosise, 2003). Advanced methods improve forensic investigations by detecting patterns and abnormalities through statistical analysis, machine learning, and data mining.

**2.2.2 File Carving**

With the help of file carving, forensic experts can retrieve data and files from fragmented or raw disk images without depending on the metadata of the file system. File carving comes very handy in digital forensics when trying to recover lost or corrupted files, reassembling evidence from compromised systems, or extracting particular file types (such documents, photos, or videos) from disk dumps or images. It involves finding file signatures or headers which, regardless of a file's location or fragmentation, indicates its beginning and end and examines the storage medium's binary content (Richard et al., 2007). Sophisticated file carving techniques increase the precision and effectiveness of file recovery from raw data by utilizing heuristics, pattern recognition algorithms, and file signature databases.

**2.2.3 Digital forensics techniques**

### Reverse Steganography

Cybercriminals use steganography to hide data inside digital files, messages, or data streams. Reverse steganography involves analyzing the data hashing found in a specific file. When inspected in a digital file or image, hidden information may not look suspicious. However, hidden information does change the underlying has or string of data representing the image.

### Stochastic Forensics

Stochastic forensics helps analyze and reconstruct digital activity that does not generate digital artifacts.

### Cross-drive Analysis

Cross-drive analysis, also known as anomaly detection, helps find similarities to provide context for the investigation.

### Live Analysis

Live analysis occurs in the operating system while the device or computer is running. It involves using system tools that find, analyze, and extract volatile data, typically stored in RAM or cache.

### Deleted File Recovery

Deleted file recovery, also known as data carving or file carving, is a technique that helps recover deleted files. It involves searching a computer system and memory for fragments of files that were partially deleted in one location while leaving traces elsewhere on the inspected machine.

**2.2.4 Mobile Device Forensics**

The practice of removing and examining digital evidence from smartphones, tablets, and other mobile devices in order to find proof of criminal conduct or security breaches is known as mobile device forensics. A few examples of useful tools are Autopsy, Magnet AXIOM, Oxygen Forensic Detective, Cellebrite UFED, and XRY. Using specialized tools and techniques, mobile device forensics involves extracting data such as call logs, text messages, emails, photos, and app activity data (Reiber, 2018). This field is essential to investigations since it helps with legal proceedings and offers insights into event timelines.

**2.2.5 Network Surveillance and Accountability**

While accountability guarantees conformity to legal and ethical norms, network surveillance monitors network traffic and communications to identify security threats and policy infractions (Ma et al., 2020). It uses methods to spot unusual activity and safeguard private data, such as intrusion detection and packet capture. Using audit trails and access controls to assure the legal and moral use of surveillance technologies, effective surveillance techniques strikes a balance between security requirements and privacy rights.

**2.2.6 Network attack Traceback and Attribution**

The process of tracking down the sources and attackers of assaults on networks is called network attack attribution and traceback. While attribution seeks to place specific individuals or organizations at fault for the attack, traceback refers to locating the attack vector through network architecture (Joshi & Pilli, 2016). Not only do these methods assess network logs, traffic patterns, and system metadata, but they also acquire evidence such as digital footprints and virus signatures. Traceback and attribution are crucial for identifying efficient cybersecurity techniques and apprehending offenders, notwithstanding their difficulty.

**2.2.7 Multimedia Forensics**

In order to determine authenticity, integrity, and origin, multimedia forensics analyzes and investigates digital multimedia content, including pictures, videos, and audio recordings. This field uses a variety of methods and instruments, such as image analysis, video forensics, and audio verification, to search digital artifacts for indications of alteration, tampering, or fraud (“Multimedia Forensics,” 2022). In criminal investigations, court cases, and digital media authentication, multimedia forensic analysis is essential to maintaining the validity and admissibility of multimedia evidence. A good example of a case study is the Jackie Maribe and Joey court case in Kenya.

**2.2.8 Multicast Fingerprinting**

In the context of multimedia distribution via networks, multicast fingerprinting is a technology used for copyright enforcement and digital content protection. According to Luh and Kundur (2005), content owners can track and identify illicit copies or redistribution by inserting unique identifiers, sometimes known as "fingerprints," into multimedia content prior to distribution. Though invisible to the human sight or ear, these fingerprints can be identified and decoded with the use of specialist software and algorithms. This helps to enforce copyright protection and discourage piracy.

**2.3 Intrusion and Online Frauds Detection**

Intrusion and online fraud detection are essential cybersecurity procedures that use a variety of methods to find and stop fraudulent activity and unauthorized access attempts on networks. These systems examine user behavior patterns and network traffic using techniques like anomaly detection and machine learning algorithms in order to quickly identify potentially harmful or suspicious conduct. Intrusion detection systems (IDS) and fraud detection systems (FDS) are designed to quickly detect and respond to security problems by continually monitoring system activity and network traffic(Peters, 2013). This helps protect against data breaches, financial losses, and damage to one's reputation.

**2.3.1 Steganography and Steganalysis**

Steganography is the art of concealing confidential information in digital media, while steganalysis is the science of finding such information(Kruse & Heiser, n.d.). Information can be subtly hidden from casual observers within text, audio files, or photographs using steganography. Steganalysis methods are used to detect these covert communications by examining minute changes or trends in the carrier medium. These methods include statistical analysis and machine learning. Steganography and steganalysis play a continuous game of cat and mouse in cybersecurity, with steganography being used to hide sensitive data and steganalysis being used to identify and neutralize such threats.

**2.4 Anonymity, Pseudonymity and P3P**

The Platform for Privacy Preferences Project, or P3P, is a protocol created by the World Wide Web Consortium (W3C) that improves transparency and privacy protection in online interactions by allowing websites to express their privacy policies in a machine-readable format and giving users easy access to understand and control over how websites collect and use their personal information(Federrath, 2003).When someone hides their identity to safeguard their privacy or evade responsibility, they are said to be anonymous. This can happen in a variety of situations, including online interactions and transactions. It can be done by adopting a false name or alias in place of one's true identity. Pseudonymity, on the other hand, enables people to preserve some degree of anonymity while remaining traceable in a particular setting. Social media and other platforms frequently let users set up pseudonymous profiles, which lets them communicate with people while hiding their real identity.

**2.5 Cyber Law**

Cyberlaw refers to the set of legal rules and guidelines that control how people use the internet, digital devices, and engage in online activities. It is sometimes referred to as information technology law or internet law (Grabowski & Robinson, 2021). A vast array of legal concerns are covered, such as online expression, digital commerce, cybersecurity, data privacy, and intellectual property rights. In addition to rules unique to different countries and sectors of the economy, cyber law includes both national and international legal frameworks. Assuring the safety of people, businesses, and governments in the digital era, it is vital in forming the legal framework of cyberspace.

**2.6 Security and Privacy Policies and Guidelines**

Documents outlining an organization's policies, methods, and best practices for managing security risks and protecting sensitive data are known as security and privacy policies and guidelines (Peltier, 2016). Numerous subjects are usually covered by these rules, including incident response, encryption, data protection, access control, and regulatory compliance. Some of the significant ones can be classified to Broadly Applicable Laws and Regulations and Industry-Specific Guidelines and Requirements. Some of the most common include:

* Sarbanes-Oxley Act (SOX) ensures financial transparency and accountability within corporations.
* Payment Card Industry Data Security Standard (PCI DSS) protects payment card data and transactions.
* Payment Service Directive, revised (PSD2) regulates payment services in the European Union.
* Gramm-Leach-Bliley Act (GLBA) addresses financial institutions’ privacy practices.
* Children’s Online Privacy Protection Act (COPPA). Safeguards children’s online privacy.
* Health Insurance Portability and Accountability Act (HIPAA) which focuses on healthcare data security and privacy.
* The National Institute of Standards and Technology (NIST) offers cybersecurity frameworks and recommendations, such as the NIST Cybersecurity Framework and Special Publication 800 series, that are specifically designed for use by government agencies and contractors.
* The Family Educational Rights and Privacy Act (FERPA) limits access to personally identifiable information and ensures confidentiality for student education records kept by educational institutions.
* Retail enterprises are subject to privacy rules under the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) with relation to the gathering, use, and safeguarding of consumer data, including consent management and data subject rights.

**2.7 Case studies and Ethical Issues**

Cybersecurity case studies provide insights into issues and best practices by illuminating real-world incidents and ethical dilemmas faced by professionals and organizations. These instances, which include privacy issues and data breaches, offer important insights toward comprehending and reducing cybersecurity threats(Macnish & Van Der Ham, 2020). Making informed decisions on cybersecurity requires careful consideration of ethical issues, such as responsible disclosure and privacy concerns.

**2.8 Court Testimony**

Delivering expert testimony in court on cybercrimes and security breaches is a part of the cybersecurity court testimony process. Cybersecurity specialists can be asked to appraise digital artifacts, provide jurors with technical evidence, and clarify difficult legal terms. The types of security breaches, the efficacy of security precautions, and attacker identification are a few examples of topics that might be discussed. To assist stakeholders in appreciating the value of digital evidence and assisting them in reaching decisions, experts must persuade others with their technical knowledge. Finding accountability, calculating damages, and obtaining justice in court are all dependent on the testimony of witnesses in cybersecurity matters (Easttom, 2021).

**2.9 Report Writing Skills**

* conciseness and clarity. Make sure your writing is simple to understand and free of needless terminology.
* Make sure your introduction, methodology, findings, and conclusions are all well described and organized in a logical manner.
* Adjust the report to the background, degree of knowledge, and interests of the audience.
* Provide accurate citations and substantiate claims and conclusions with reliable data.
* neutrality. When presenting data and analysis, be objective and try to keep your personal prejudices to a minimum.
* Correctness and Wholeness. Make sure you cover the subject matter accurately and completely, covering all pertinent areas.
* Graphical Support. To improve understanding, include pertinent and professionally made images, such as tables, charts, and graphs.
* expert demonstration. For a professional final output, pay attention to font, layout, and proofreading.

**CONCLUSION**

Eventually, all the above topics provide a clear overview and posture of Digital forensics and more precisely Network forensics. The paper first describes the field of digital forensics and the principles used to achieve Network forensics in a systematic and ethical manner. Specific topics like duplication forensics analysis, Cyber forensics tools and Network attack traceback and attribution show some of the processes undertaken in the network forensics procedure. Also, the topics Cyber law and Security and privacy policies point out the policies and standards that need to be complied with to ensure that user data is secured and their privacy is achieved to prevent breaches of Confidentiality, Integrity and Availability of information and information systems. Lastly, the paper addresses the importance of court testimony by an expert witness after network forensics and provides some report writing skills that can provide a comprehensive report on the incident and procedure ie. Network forensics processes.

Although this paper covers most common topics in Network forensics due to scope retention, the knowledge revolving around network forensics and computer forensics at large is enormous. Network forensic investigations professionals should ensure a code of ethics and professionalism to ensure admissibility of evidence in court in an understandable manner even for the non-technical personnel like the jury. Thisway, it will be possible to achieve justice in criminal cases involving digital forensics.

**REFERENCES**

Byard, R. W., James, H., Berketa, J., & Heath, K. (2015). Locard’s principle of exchange, dental examination and fragments of skin. *Journal of Forensic Sciences*, *61*(2), 545–547.<https://doi.org/10.1111/1556-4029.12964>

Robles, F. (2020). DIGITAL FORENSICS. *Uazuay*.<https://www.academia.edu/42251806/DIGITAL_FORENSICS>

Wolstenholme, R., Jickells, S., & Forbes, S. (2021). *Analytical techniques in forensic science*. John Wiley & Sons

Ec-Council. (2009). *Computer Forensics: Investigating network intrusions and cyber crime*. <https://www.amazon.com/Computer-Forensics-Investigating-Intrusions-EC-Council/dp/1435483529>

Sivaprasad, A. (2017). Secured Proactive Network Forensic framework. *2017 International Conference on Current Trends in Computer, Electrical, Electronics and Communication (CTCEEC)*. <https://doi.org/10.1109/ctceec.2017.8455003>

Rogers, M., Goldman, J. E., Mislan, R., Wedge, T., & Debrota, S. (2006). Computer Forensics Field Triage Process model. *The Journal of Digital Forensics, Security and Law*. <https://doi.org/10.15394/jdfsl.2006.1004>

Mandia, K., & Prosise, C. (2003). *Incident Response & Computer Forensics, 2nd ed.* McGraw Hill Professional.

Richard, G. G., Roussev, V., & Marziale, L. (2007). In-Place File Carving. *IFIP*, 217–230. <https://doi.org/10.1007/978-0-387-73742-3_15>

Vashishth, T. (2023). *Cyber forensics up and running: A hands-on guide to digital forensics tools and technique (English Edition)*. BPB Publications.

Reiber, L. (2018). *Mobile Forensic Investigations: A Guide to Evidence Collection, Analysis, and Presentation, second edition*. McGraw Hill Professional.

Ma, Y., Wu, Y., & Ge, J. (2020). *Accountability and privacy in network security*. Springer Nature.

Joshi, R. C., & Pilli, E. S. (2016). Network Forensic Attribution. In *Computer communications and networks* (pp. 131–142). <https://doi.org/10.1007/978-1-4471-7299-4_7>

Multimedia Forensics. (2022). In *Advances in computer vision and pattern recognition*. <https://doi.org/10.1007/978-981-16-7621-5>

Luh, W., & Kundur, D. (2005). New paradigms for effective multicasting and fingerprinting of entertainment media. *IEEE Communications Magazine*, *43*(6), 77–84. <https://doi.org/10.1109/mcom.2005.1452834>

Peters, C. A. (2013). *Intrusion and fraud detection using multiple machine learning algorithms*.

Kruse, W. G., II, & Heiser, J. G. (n.d.). *Computer Forensics: Incident Response Essentials*. Pearson Education.

Federrath, H. (2003). *Designing privacy enhancing technologies: International Workshop on Design Issues in Anonymity and Unobservability, Berkeley, CA, USA, July 25-26, 2000. Proceedings*. Springer.

Grabowski, M., & Robinson, E. P. (2021). *Cyber Law and Ethics: Regulation of the Connected World*. Routledge.

Peltier, T. R. (2016). *Information Security policies, procedures, and standards: Guidelines for Effective Information Security Management*. CRC Press.

Macnish, K., & Van Der Ham, J. (2020). Ethics in cybersecurity research and practice. *Technology in Society*, *63*, 101382. <https://doi.org/10.1016/j.techsoc.2020.101382>

Easttom, C. (2021). *Digital forensics, investigation, and response*. Jones & Bartlett Learning.

Multimedia Forensics. (2022). In H. T. Sencar, L. Verdoliva, & N. Memon (Eds.), *Advances in Computer Vision and Pattern Recognition*. Springer Singapore. https://doi.org/10.1007/978-981-16-7621-5

*What is Multimedia Forensic | IGI Global*. (n.d.). Www.igi-Global.com. Retrieved February 10, 2024, from https://www.igi-global.com/dictionary/multimedia-forensic-techniques-acquisition-device/19588