DIGITAL FORENSICS

Digital evidence handling procedures

1. Identification

Digital evidence is presented in physical and logical form. The physical form refers to the construction and resultant appearance, in the form of a physical component or digital device that contains potential digital evidence. The logical form of the digital evidence refers to the format of data and its storage location and address within the digital device, such as a hard drive.
The identification process involves the search for, recognition and documentation of potential digital evidence at an incident scene. The identification process should identify digital storage media and processing devices that may contain potential digital evidence relevant to the occurred incident. This stage also includes a triage process to prioritize the evidence collection based on their volatility. The volatility of the data should be identified to ensure the correct order of the collection and acquisition processes to minimize the damage to the potential digital evidence and to obtain the best evidence. In addition, the process should identify the possibility of hidden potential digital evidence.
First responders or digital evidence examiners should be aware that not all digital storage media can be easily identified and located, for example cloud computing, NAS and SAN; all add a virtual component to the identification process. First responders or digital evidence examiners should systematically carry out a thorough search for items that may contain digital evidence. Different types of digital devices that may contain potential digital evidence can easily be overlooked, disguised or co-mingled amongst other irrelevant material.

2. Collection

Once the digital devices that may contain potential digital evidence are identified, first responders or digital evidence examiners should decide whether to collect or acquire during the next step. There are a number of decision factors for this. The choice needs to be balanced with the circumstances.
Collection is a step in the digital evidence handling process where devices that potentially contain digital evidence are removed to a laboratory or another controlled environment for later acquisition and analysis. Potential digital evidence can exist in two conditions: when a system is powered on or when the system is powered off.
Different approaches and tools are required for this process, depending on the condition.
The collection step involves the gathering of physical devices that may contain potential digital evidence from its original location and documenting all the collected items and the

steps involved. All items collected should be properly recorded and packaged prior to transportation. It is important for first responders or digital evidence examiners to collect any material that might relate to the potential digital evidence (e.g. paper with passwords noted down, cradles and power connectors for embedded system devices). Potential digital evidence may be tampered with or easily spoiled if reasonable care is not applied. There is a variety of reliable collection methods. First responders or digital evidence examiners should adopt the best possible collection method based on the situation, cost and time, and document the decision for using a particular method.

Removal of digital storage media is not always recommended and first responders or digital evidence examiners should be sure they are trained and knowledgeable to know and recognize when it is allowable to do so. Besides, there are some circumstances when it is impractical to collect digital devices. First responders or digital evidence examiners should consider the following circumstances, but is not limited to only these :

- If there is no legal entitlement to collect the digital device;
- If there is an obligation to use other methods (e.g. to avoid interrupting a business);
- If first responders or digital evidence examiners wants to capture the method of operation of a suspect during abuse of a system;
- If the collection or acquisition should take place covertly, if considered legal by the jurisdiction;
- If it is a mission-critical digital device that cannot tolerate any downtime;
- If it contains volatile data that should be acquired immediately in order to avoid any loss of data due to interruption of power supply;
- If the physical size of the digital device is too big, such as a server at a data centre or RAID system;
- If it is a safety-critical digital device that would endanger life if stopped;
- If it is a business-critical digital device that also services innocent parties; and
- If it contains encrypted volume or data which requires recovery of password or key within the volatile memory.

3. Acquisition

The acquisition process involves producing an image of potential digital evidence or digital device that may contain a potential digital device and documenting the methods and steps used. There are a variety of reliable and validated acquisition methods and tools. First responders or digital evidence examiners should adopt a suitable acquisition method based on the situation, cost and time, and document the decision for using a particular method or tool appropriately.

First responders or digital evidence examiners should use the appropriate method and be able to justify the selection of that method. The acquisition method used should produce an image copy of the digital evidence or digital devices that may contain potential digital evidence. Both the original copy and the image copy should be verified with a proven verification function (proven accurate at that point in time) that is acceptable to the person who will use the evidence. Both copies should produce the same hash values and the image copy be verified as a bitwise copy of the original digital evidence. There will be instances where the verification process cannot be performed, for example when acquiring a running system, the original copy contains error sectors, or the acquisition time period is limited. In such instances, first responders or digital evidence examiners should use the best possible method available and be able to justify and defend the selection of the method. If the imaging cannot be verified, then this needs to be documented and justified. If necessary, the acquisition method used should be able to obtain the allocated and unallocated space.

There may be instances in which an image copy of a source disk may not be feasible, such as when the source is too large. In these instances, a first responders or digital evidence examiners may perform a logical acquisition. This acquisition type targets only specific data types, directory or locations for acquisition. This generally takes place on a file and partition level. This method will only copy the active files and non-file-based allocated space on the digital storage media and will not copy deleted files or unallocated space. Other instances where this method can be useful are if they are mission-critical systems that cannot be shutdown. Besides, when the data to be collected contains personal data, some jurisdictions require that the seals on the data should be done in presence of the owner of the data.

4. **Preservation**

Potential digital evidence should be preserved to ensure its usefulness for investigating incidents and to protect the integrity of the evidence. The preservation process involves the safeguarding of potential digital evidence and digital devices that may contain potential digital evidence from tampering or spoliation. The preservation process should be initiated and maintained throughout the digital evidence handling steps starting from the identification of the digital devices that may contain potential digital evidence. In the best-case scenario, there should be no spoliation to the data itself or any metadata associated with it (e.g. date and time-stamps). First responders or digital evidence examiners should be able to demonstrate that the evidence has not been modified since it was identified, collected or acquired.

In some cases, the confidentiality of digital evidence is a requirement, either a business requirement or a legal requirement (e.g. privacy). The digital evidence should be preserved in a manner that ensures the confidentiality of the data.

5. **Examination**

In-depth systematic search of evidence relating to the suspected crime needs to be done prior to performing a full analysis. This focuses on identifying and locating potential evidence, possibly within unconventional locations. The result (output) of the work in this stage of the investigative process is the smallest set of digital information that has the highest potential for containing data of probative value, and detailed documentation for analysis.

6. Analysis

This step involves the detailed scrutiny of data identified by the preceding activities. The techniques employed here will tend to involve review and study of specific, internal attributes of the data. Analysis determines significance, reconstructs fragments of data and draws conclusions based on evidence found. It may take several iterations of examination and analysis to support a crime theory. The distinction of analysis is that it may not require high technical skills to perform and thus more people can work on this case.

7. Reporting

To provide a transparent view of the investigative process, final reports should contain important details from each step, including References to protocols followed and methods used to seize, document, collect, preserve, recover, reconstruct, organize, and search key evidence. The majority of the report generally deals with the analysis leading to each conclusion and descriptions of the supporting evidence. No conclusion should be written without a thorough description of the supporting evidence and analysis. Also, a report can exhibit the investigator or examiner's objectivity by describing any alternative theories that were eliminated because they were contradicted or unsupported by evidence.

8. Persuasion and Testimony

In some cases, it is necessary to present the findings outlined in a report and address related questions before decision makers can reach a conclusion. A significant amount of effort is required to prepare for questioning and to convey technical issues in a clear manner. Therefore, this step in the process includes techniques and methods used to help the analyst and/or domain expert translate technological and engineering detail into understandable narrative for discussion with decision makers.

9. Returning evidence

Ensuring physical and digital property is returned to the proper owner as well as determining how and what criminal evidence must be removed. Again not an explicit forensics step, however any model that seizes evidence rarely addresses this aspect.

Device Forensics

A branch of computer forensics, deals with gathering digital evidence available in different types of devices such as mobile phones, PDA, iPod, printers, scanners, camera, fax machines, etc. The normal computer forensic procedure is inadequate to identify and collect the evidence from these devices. In order to collect evidence in such devices and to ensure its admissibility in a court of law, sound forensic techniques and a systematic approach are needed. Device forensics is the solution to the issue. It includes the following divisions.

Computer Forensics : Computer Forensics is a scientific method of investigation and analysis in order to gather evidence from digital devices or computer networks and components which is suitable for presentation in a court of law or legal body. It involves performing a structured investigation while maintaining a documented chain of evidence to find out exactly what happened on a computer and who was responsible for it.

TYPES :

- **Disk Forensics**: It deals with extracting raw data from the primary or secondary storage of the device by searching active, modified, or deleted files.
- **Network Forensics**: It is a sub-branch of Computer Forensics that involves monitoring and analyzing the computer network traffic.
- **Database Forensics**: It deals with the study and examination of databases and their related metadata.
- **Malware Forensics**: It deals with the identification of suspicious code and studying viruses, worms, etc.
- **Email Forensics**: It deals with emails and their recovery and analysis, including deleted emails, calendars, and contacts.
- **Memory Forensics**: Deals with collecting data from system memory (system registers, cache, RAM) in raw form and then analyzing it for further investigation.
- **Mobile Phone Forensics**: It mainly deals with the examination and analysis of phones and smartphones and helps to retrieve contacts, call logs, incoming, and outgoing SMS, etc., and other data present in it.

Some Tools used for Investigation:

Tools for Laptop or PC –

- **COFEE –** A suite of tools for Windows developed by Microsoft.
- **The Coroner's Toolkit –** A suite of programs for Unix analysis.
- **The Sleuth Kit –** A library of tools for both Unix and Windows.

Tools for Memory:

- Volatility
- WindowsSCOPE

Tools for Mobile Device :

- MicroSystemation XRY/XACT

APPLICATIONS

- Intellectual Property theft
- Industrial espionage
- Employment disputes
- Fraud investigations
- Misuse of the Internet and email in the workplace
- Forgeries related matters
- Bankruptcy investigations
- Issues concerned the regulatory compliance

Advantages of Computer Forensics :

- To produce evidence in the court, which can lead to the punishment of the culprit.
- It helps the companies gather important information on their computer systems or networks potentially being compromised.
- Efficiently tracks down cyber criminals from anywhere in the world.
- Helps to protect the organization's money and valuable time.
- Allows to extract, process, and interpret the factual evidence, so it proves the cybercriminal action's in the court.

Disadvantages of Computer Forensics :

- Before the digital evidence is accepted into court it must be proved that it is not tampered with.
- Producing and keeping electronic records safe is expensive.
- Legal practitioners must have extensive computer knowledge.
- Need to produce authentic and convincing evidence.
- If the tool used for digital forensics is not according to specified standards, then in a court of law, the evidence can be disapproved by justice.

- A lack of technical knowledge by the investigating officer might not offer the desired result.

Mobile Forensics : Mobile forensics, a subtype of digital forensics, is concerned with retrieving data from an electronic source. The recovery of evidence from mobile devices such as smartphones and tablets is the focus of mobile forensics. Because individuals rely on mobile devices for so much of their data sending, receiving, and searching, it is reasonable to assume that these devices hold a significant quantity of evidence that investigators may utilize.
Mobile devices may store a wide range of information, including phone records and text messages, as well as online search history and location data. We frequently associate mobile forensics with law enforcement, but they are not the only ones who may depend on evidence obtained from a mobile device.

Uses of Mobile Forensics:

The military uses mobile devices to gather intelligence when planning military operations or terrorist attacks. A corporation may use mobile evidence if it fears its intellectual property is being stolen or an employee is committing fraud. Businesses have been known to track employees' personal usage of business devices in order to uncover evidence of illegal activity. Law enforcement, on the other hand, may be able to take advantage of mobile forensics by using electronic discovery to gather evidence in cases ranging from identity theft to homicide.

Principles of Mobile Forensics:

The purpose of mobile forensics is to extract digital evidence or relevant data from a mobile device while maintaining forensic integrity. To accomplish so, the mobile forensic technique must develop precise standards for securely seizing, isolating, transferring, preserving for investigation, and certifying digital evidence originating from mobile devices.
The process of mobile forensics is usually comparable to that of other fields of digital forensics. However, it is important to note that the mobile forensics process has its own unique characteristics that must be taken into account. The use of proper methods and guidelines is a must if the investigation of mobile devices is to give positive findings.

Memory forensics (sometimes referred to as memory analysis) refers to the analysis of volatile data in a computer's memory dump. Information security professionals conduct memory forensics to investigate and identify attacks or malicious behaviors that do not leave easily detectable tracks on hard drive data.

What is Volatile Data?

Volatile data is the data stored in temporary memory on a computer while it is running. When a computer is powered off, volatile data is lost almost immediately. Volatile data resides in a computer's short term memory storage and can include data like browsing history, chat messages, and clipboard contents. If, for example, you were working on a document in Word or Pages that you had not yet saved to your hard drive or another non-volatile memory source, then you would lose your work if your computer lost power before it was saved.

What is in a Memory Dump?

A memory dump (also known as a core dump or system dump) is a snapshot capture of computer memory data from a specific instant. A memory dump can contain valuable forensics data about the state of the system before an incident such as a crash or security compromise. Memory dumps contain RAM data that can be used to identify the cause of an incident and other key details about what happened.

The Importance of Memory Forensics

Memory forensics can provide unique insights into runtime system activity, including open network connections and recently executed commands or processes. In many cases, critical data pertaining to attacks or threats will exist solely in system memory – examples include network connections, account credentials, chat messages, encryption keys, running processes, injected code fragments, and internet history which is non-cacheable. Any program – malicious or otherwise – must be loaded in memory in order to execute, making memory forensics critical for identifying otherwise obfuscated attacks.

As attack methods become increasingly sophisticated, memory forensics tools and skills are in high demand for security professionals today. Many network-based security solutions like firewalls and antivirus tools are unable to detect malware written directly into a computer's physical memory or RAM. Security teams should look to memory forensics tools and specialists to protect invaluable business intelligence and data from stealthy attacks such as fileless, in-memory malware or RAM scrapers.

Memory Forensics Tools

Traditional network and endpoint security software has some difficulty identifying malware written directly in your system's RAM. Traditional security systems typically analyze input sources like network, email, CD/DVD, USB drives, and keyboards, yet lack the ability to analyze volatile data that is stored in memory. These systems are viable options for protecting against malware in ROM, BIOS, network storage, and external hard drives. However, your data in execution might still be at risk due to attacks that upload malware to memory locations reserved for authorized programs. The most sophisticated enterprise security systems now come with memory forensics and behavioral analysis capabilities which can identify malware, rootkits, and zero days in your system's physical memory.

Memory forensics tools also provide invaluable threat intelligence that can be gathered from your system's physical memory. Physical memory artifacts include the following:

- Usernames and Passwords: Information users input to access their accounts can be stored on your system's physical memory.
- Decrypted Programs: Any encrypted malicious file that gets executed will have to decrypt itself in order to run. This threat intelligence is valuable for identifying and attributing threats.
- Open Clipboard or Window Contents: This may include information that has been copied or pasted, instant messenger or chat sessions, form field entries, and email contents.

While this is in no way an exhaustive list, it does demonstrate the importance of solutions that incorporate memory forensics capabilities into their offerings. There are also a range of commercial and open source tools designed solely for conducting memory forensics. The decision of whether to use a dedicated memory forensics tool versus a full suite security solution that provides memory forensics capabilities – as well as the decision of whether to use commercial software or open source tools – depends on the business and its security needs.

Network Forensics :

Network forensics is a subcategory of digital forensics that essentially deals with the examination of the network and its traffic going across a network that is suspected to be involved in malicious activities, and its investigation for example a network that is spreading malware for stealing credentials or for the purpose analyzing the cyber-attacks. As the internet grew cybercrimes also grew along with it and so did the significance of network forensics, with the development and acceptance of network-based services such as the World Wide Web, e-mails, and others.

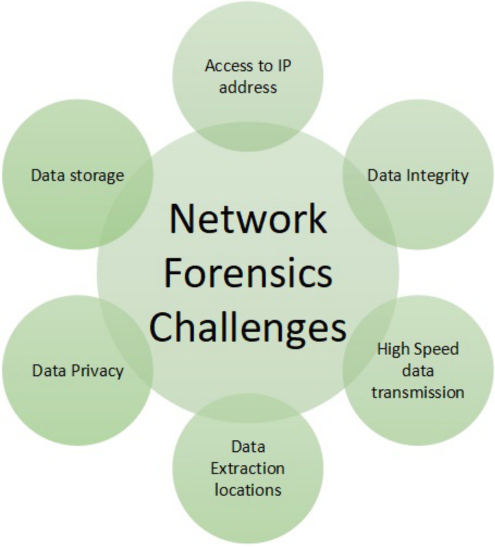
With the help of network forensics, the entire data can be retrieved including messages, file transfers, e-mails, and web browsing history, and reconstructed to expose the original transaction. It is also possible that the payload in the uppermost layer packet might wind up on the disc, but the envelopes used for delivering it are only captured in network traffic. Hence, the network protocol data that enclose each dialog is often very valuable.

For identifying the attacks investigators must understand the network protocols and applications such as web protocols, Email protocols, Network protocols, file transfer protocols, etc.

Investigators use network forensics to examine network traffic data gathered from the networks that are involved or suspected of being involved in cyber-crime or any type of cyber-attack. After that, the experts will look for data that points in the direction of any file manipulation, human communication, etc. With the help of network forensics, generally, investigators and cybercrime experts can track down all the communications and establish timelines based on network events logs logged by the NCS.

Challenges in Network Forensics:

- The biggest challenge is to manage the data generated during the process.
- Intrinsic anonymity of the IP.
- Address Spoofing.


Access to IP address
Data storage
Data Integrity
Network Forensics Challenges
Data Privacy
High Speed data transmission
Data Extraction locations

Advantages:

- Network forensics helps in identifying security threats and vulnerabilities.
- It analyzes and monitors network performance demands.
- Network forensics helps in reducing downtime.
- Network resources can be used in a better way by reporting and better planning.

- It helps in a detailed network search for any trace of evidence left on the network.

Disadvantage:

- The only disadvantage of network forensics is that It is difficult to implement.

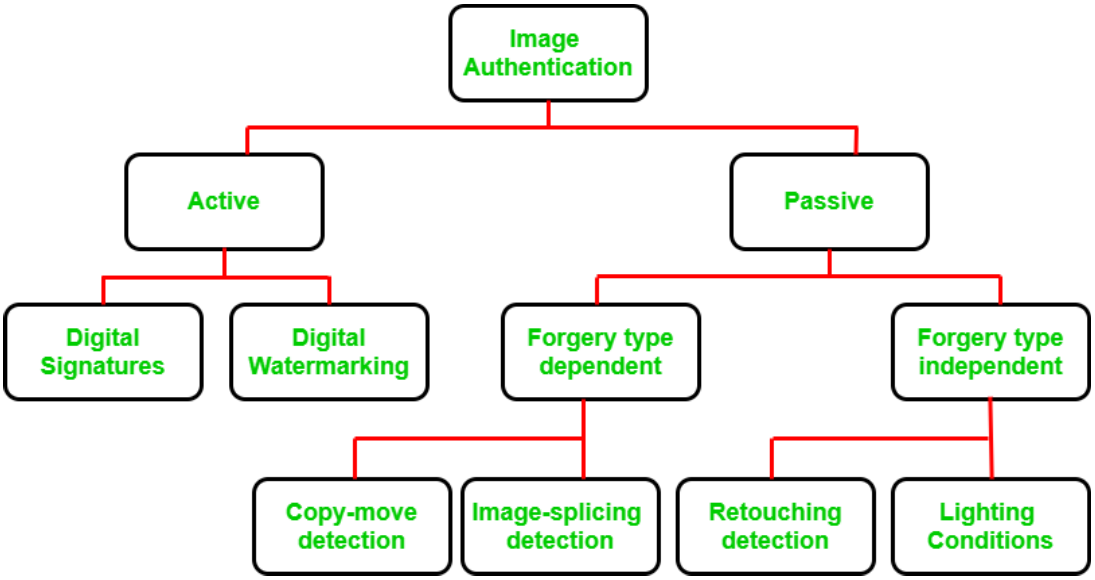
Multimedia Forensics

When applied to the field of multimedia, digital forensics started to face challenges, as multimedia is content that uses a mix of audio, video, images, text. Thanks to the wide adoption of mobile devices, cheaper storage, high bandwidth, online users are generating a humongous amount of data. This growth has pushed digital multimedia in the forefront. The amount of data is so massive that it has surpassed the capabilities of the forensic experts to effectively analyze and process the data. Multimedia forensics has now become an integral part of Cyber Forensics. Multimedia forensics involves the set of techniques used for the analysis of multimedia signals like audio, video, images. It aims to:

- Reveal the history of digital content.
- Identifying the acquisition device that produced the data.
- Validating the integrity of the contents.
- Retrieving information from multimedia signals.

What are the approaches to Multimedia Authentication?

Internet content is not only limited to text form, it comes in a lot of different varieties, so the forensic approaches developed to analyze them must also vary in scope. The goal here is to analyze images, text, audio, video, in order to generate a piece of logical Forensic evidence. Multimedia Forensics divides its efforts between 2 main approaches – ***Active Image Authentication*** and ***Passive Image Authentication***.



Active Image Authentication:
In this technique, a known authentication code is embedded in the image at the time of image generation or sent with the image for accessing its integrity at the receiving end. Verifying this code authenticates the originality of the image. Active Authentication is further classified into 2 categories: Digital Watermarking and Digital Signatures.

Drawbacks of Active image authentication:

- The authentication code needs to be embedded in the image at the time of recording using special equipment thus prior information about the image becomes indispensable.
- This approach requires a digital watermark or a digital signature to be created precisely when the image is recorded, which limits its ability to handle specially equipped digital devices.
- As the majority of the images on the Internet, today don't have a watermark or a digital signature, which has forced this image authentication method to consider additional techniques – **Digital Watermarking:** In this technique a digital watermark is embedded into the image at the time of either image acquisition or in the processing stage. **Digital Signatures:** Digital signatures embed some secondary information that is usually obtained from the image, at the acquisition end into the image.

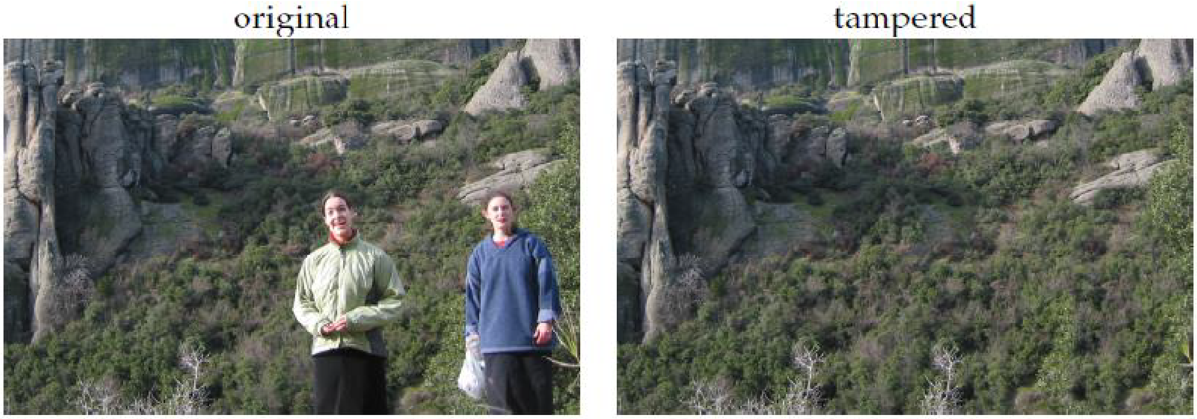
Passive Image Authentication:
Passive authentication also known as image forensics uses the only image with no prior information for accessing the integrity of the image. Passive authentication works on the

assumption that even though tampering with the image may not leave any visual trace, they are likely to alter the underlying statistics. This means that digital forgeries may disturb the underlying properties of the image, quality of the image, even though no physical clue has been left behind. Passive techniques are further classified into ***Forgery-type dependent*** and ***Forgery-type independent techniques***.

Forgery-type dependent –

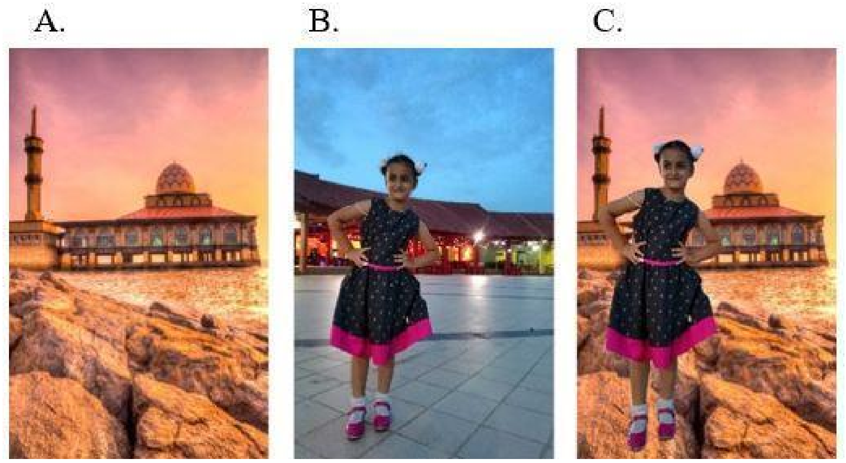
These are designed to detect only certain types of forgeries like copy-move and image-splicing which are dependent on the type of forgery carried out on the image. It is further classified into 2 categories: ***Copy-move detection*** and ***Image-splicing detection***.

1. Copy-move detection: Copy-move is the most popular photo tampering technique because of the ease with which it can be carried out. It involves copying some regions in the image and moving the same to some other region in the image. Since the copied region belongs to the same image so the dynamic range and color remain compatible with the rest of the image. In copy-move detection post-processing operations like blurring are used to decrease the effect of border irregularities between the two images.



2. Image-splicing detection: The Image-splicing method involves merging 2 or more images, changing the original image significantly to create a forged image. Please note when merging images with differing backgrounds, it becomes difficult to make the border and boundaries indiscernible. Image-splicing detection is a challenging task involving the following techniques:

- Composite regions are investigated by a variety of methods.
- The presence of abrupt changes between different regions that are combined to create a composite image and their backgrounds, provide valuable traces to detect splicing in the image under consideration.



Forgery-type independent –

These methods detect forgeries independent of forgery type but based on artifact traces left during the process of re-sampling and due to lighting inconsistencies. It is further classified into 2 categories: **1. Retouching detection:** This method is most commonly used for commercial and aesthetic applications. Retouching is mostly carried out to enhance or reduce the image features or to create a convincing composition of 2 images that requires rotation, resizing, or stretching of one of the images. Image retouching detection is done using the following techniques:

- Find the blurring, enhancements, or color changes and illumination changes in the forged image.
- Retouching Detection is easy if the original image is available however blind detection is a challenging task.

What are Digital Fingerprints?

Cryptographic tools and access control mechanisms ensure the safe delivery of multimedia content across the Internet. But this protection ends as soon as the content is delivered to the end-user and safely decrypted. Digital Fingerprinting has emerged to cater to this post-delivery by identifying the end-users who have authorized access to plaintext but use it for unauthorized purposes. Digital Fingerprinting process involves investigators to trace the illegal usage of multimedia content through a unique identifying information known as "Fingerprint" that is embedded in the content before distribution. Youtube is using this technology to scan files and match the digital fingerprints they find against a database of copyrighted material to see if any intellectual property is being violated. Digital Fingerprints are technically coded strings of binary digits generated by mathematical algorithms, they are as unique as the analog fingerprints of a person. The more images and videos continue to flood the Internet, the more difficult it becomes to protect the information through forensic investigations. As online multimedia content grows, it becomes important for the users and creators to understand the legal boundary of the virtual world.

Anti Forensics

Anti-forensic aims to make investigations on digital media more difficult and therefore more expensive. It is usually possible to distinguish anti-forensic techniques into specific categories, each of which is specifically designed to attack one or more steps that analysts will perform during their activities. All forensic analysts, whether from private or public laboratories such as the police, take specific steps during each stage of analyzing a new case.

Knowledge of these steps, generally summarized as “Identification”, “Acquisition”, “Analysis” and “Reporting”, is the first step to better understanding the benefits and limitations of each anti-forensic technique. As in many other areas of information security, a good level of security is achieved through a stratified problem-solving model. This means that challenging just one of these steps by investigators often does not produce the desired result. Moreover, an expert analyst will at best still be able to demonstrate that he was able to deal with some evidence, even without knowing the content of that evidence.

These are the general anti-forensic categories discussed in this document:

- Data hiding, obfuscation, and encryption
- Trail Blackout
- Falsification of data
- Overwriting data/metadata:
- Data deletion and physical destruction
- Encryption
- Online anonymity

HIDING DATA IN FILE SYSTEM STRUCTURES

Data hiding is one of the anti-forensic techniques that attackers use to create inaccessible knowledge. Exhaustive NTFS-based disks contain unhealthy clusters during the data file as BadClus, and also the MFT eight entry represents these bad clusters. BadClus could be a sparse file that allows attackers to cover an unlimited amount of information further because it contains a large number of clusters for BadClus that cover a lot of information.

TRAIL BLACKOUT

Trail Obfuscation is one of many anti-forensic techniques that attackers use to mislead, complicate, disorient, divert and/or distract the rhetorical investigative method. the method includes completely different techniques and tools such as:

- Wood cleaners
- Spoofing
- Misinformation
- Bouncing spine
- Zombie accounts
- Trojan commands

In this method, attackers delete or modify the information of some vital files to confuse the incident responders. They modify header data and various roles using file extensions. Timestamping, which is part of the Metasploit Framework, is one every path obfuscation tool that attackers use to switch, modify, and delete date and time information and make it useless for transforming incident responses.

DATA FALSIFICATION

The term forgery usually describes a message-related attack against a cryptographic digital signature scheme. This is an attack that tries to produce a digital signature for a message without having access to the private signing key of the relevant signer.

OVERWRITING DATA/METADATA

Intruders use various programs to write information to the storage device, making it difficult or impossible to recover. These programs will record information, metadata, or each to prevent a forensic investigation method. Rewriting programs adds 4 modes:

- Overwrite the entire media
- Overwrite individual files
- Overwrite deleted files on media
- Overwriting information will be done using disk sanitization

METADATA REWRITE:

Metadata refers to data that stores details about the knowledge. It plays a vital role within society. Its forensic investigation method by providing details such as the time of creation, the names of the systems used to create and modify it, the name of the author, the time and date of modification, and the names of the users who modified the UN Agency file, and various details. Incident responders will create a timeline of the attackers' actions by arranging the file's timestamps and various details in a ranked order.

DATA DELETION AND PHYSICAL DISPOSAL:

While anyone can delete data, it takes an experienced professional to actually destroy data. The goal of data destruction is to completely get rid of any trace of data so that it is no longer accessible. This goal can be achieved in several different ways, including physical destruction, degaussing, and overwriting.

ENCRYPTION

Encryption is a method of translating information into a secret code so that only licensed personnel can access it. It is effective due to information security. To browse an encrypted file, users need a secret key or countersign that can overwrite the file. Therefore, most attackers use the encryption technique as the most effective anti-forensic technique. Data encryption is one commonly used technique to defeat the rhetorical investigation method and involves encoding codes, files, folders, and typically complete exhaustive drives. The intruders use robust coding algorithms to encrypt the information about the price of the investigation, which makes this information almost indistinct even if the key is not selected. Some algorithms deflect investigative processes by applying special functions as well as by using a key file, full-volume encryption, and plausible deniability.

ENCRYPTED NETWORK PROTOCOLS

Attackers use encrypted network protocols to protect the identification of network traffic in addition to its content from the forensic examination. Few cryptographic encapsulation protocols like SSL and SSH will only protect the content of the traffic. However, to protect against traffic analysis, attackers should also anonymize themselves whenever possible. Attackers use virtual routers, such as Onion routing, which provide multiple layers of protection. Onion routing is a technique used for covert network communication. This network encapsulates messages in layers of encryption, similar to the layers of an onion, and uses a worldwide voluntary network of routers to anonymize the delivery and destination of communications. This makes tracking this type of communication and assigning it to a van for incident responders incredibly difficult.

BUFFER OVERFLOW AGAINST FORENSIC TOOLS

In a buffer overflow exploit, attackers use the buffer overflow as input to a remote system to inject and execute code in the address house of a running program, successfully modifying the behavior of the victim program. Attackers typically use buffer overflows to gain access to a remote system once they transfer the attack tools, which are stored on the target computer's hard drive.

ONLINE ANONYMITY

The best way to be online anonymity is using incognito mode or TOR Browser

DETECTION OF ACTIVITIES OF FORENSIC TOOLS

Attackers are fully prepared for the PC forensics tools used by responders to search for and analyze evidence from the "victim's computer or network." Therefore, they try to include rhetorical tools and programs to identify methods in the system or malware they use. These programs act intelligently and change the behavior of CFT detective work.

Forensic Report Writing and Expert Testimony

Forensics is the application of science to investigations, more particularly criminal investigations. The result of these forensic-related investigations is detailed in a forensic report. These reports are often used for several purposes, including billing, affidavits, and as proof of what was found or not found. These reports are very important to a case. The expert opinions and reports to various courts in India and abroad.

Basic components of a forensic report include articulating a referral question, and sources of information, presenting relevant data and then giving an expert opinion without being biased, grammatically correct text, and avoiding jargon, opinions, and data should be linked or related. A forensic report is usually related to or about the subject and not for the subject. This forensic report proves useful in court proceedings and can also influence the decision of the court.

Section 45 of the Indian Evidence Act allows the expert to give opinions and reports to the court in India. As per Section 45 of the Indian Evidence Act 1872- When the Court has to form an opinion upon a point of foreign law or science or art, or as to the identity of handwriting or finger impressions, the opinions upon that point of persons specially skilled in such foreign law, science or art, or in questions as to the identity of handwriting or finger impressions are relevant facts. Such persons are called experts. Further as per Section 46 of the Indian Evidence Act 1872 – it is stated that facts, not otherwise relevant, are relevant if they support or are inconsistent with the opinions of experts when such opinions are relevant.

Thus the ingredients of section 45 and section 46 highlight that:

1. The court when necessary will place its faith in the skills of persons who have technical knowledge of the facts concerned.
2. The court will rely on the bonafide statement of proof given by the expert concluded based on scientific techniques.
3. The evidence considered irrelevant would be given relevance in the eyes of law if they are consistent with the opinion of experts.

Purpose of Forensic Reports

The forensic report is frequently the primary work product of a forensic evaluation. A forensic report is intended to inform and influence the court about an assessment subject, specifically about the subject's psychological functioning and behavior. The forensic evaluator must be aware of the purpose of the report and direct the narrative accordingly.

One of the main purposes of the forensic report can be said to be to apply psychological knowledge to understand and help in answering the legal question or issue raised. This happens because judges and lawyers usually do not possess the in-depth knowledge related to forensic science that might be required to arrive at certain decisions. In such cases opinions from experts might prove to be useful in decision-making for courts. Such testimonies provided by the experts are critical in legal issues.

The forensic reports can have testimonies or opinions of the experts regarding the insanity of an individual which to a great extent determines whether the accused is guilty or not. It can help in determining whether the parent is fit for custody of a child in juvenile custody cases. In criminal matters, it can help in understanding the behavior of the criminal. These are some of the ways in which forensic reports serve their purpose in the judicial system.

Who is the client/customer?

The forensic report is of assistance to people like judges, lawyers, and investigating institutions to name a few. Forensic reports and expert opinion help the judges in decision-making in the court of law. Forensic knowledge can be useful in concluding legal matters. Attorneys can request an individual assessment if they feel such a report will be favorable to their client's case. They can use expert opinion to put forward their case under Section 45 of the Indian Evidence Act. A forensic report is subjected to scrutiny by both the lawyers (i.e. the defendants and appellants) and also by the judge. The forensic report also proves to be useful in conducting a successful investigation as it can help in linking evidence of the crime with the criminal.

General Structure of a Forensic Report

- **Title of the Examination report-** It means whether it is toxicological/handwriting opinion/ballistics etc. with a proper legal section of the evidence act of that particular country or region.
- Name and address of the laboratory with the contact information like telephone, mobile, fax, and email.
- Affiliation of the laboratory showing its legal entity and accreditation status. In case you are a freelancer, all credentials with your expertise and experience must be mentioned on the letterhead of the report or at the end of the report.
- Unique ID No. of the report with the date (if applicable)

- Name of the customer (client/attorney/individual) with reference letter number and date (assignment letter)
- Case Enquiry/ DD/ FIR no. ………date …………u/s……….Police Station, under which court (if applicable)
- Mode of receipt of material (evidence/specimens): Through messenger or by post / by mail
- Sampling Method; How the sampling done by the IO/ Investigator/ Forensic Expert
- Reference to the Test Method(s); Reference to lab procedure manual/ books/published standard method- used in the examination, or sometimes to the previous cases solved or convicted.
- Condition of Parcels/Test samples and seals; eg. Received. One sealed/ unsealed ..parcel. The seals were intact and tallied with the specimen seal as per the forwarding authority letter.
- Description of Specimens/Parcels/Samples/Exhibits etc.
- Methodology of Examination
- Result of Examination & Opinion
- Signature or examining officer along with seal.

Main Components of a Forensic Report

Understanding the Referral Question

It is important to identify the referral question. Identifying it will help the evaluator in understanding the purpose of the report; what question specifically he is supposed to answer and where his role comes in. Referral questions will also help the expert in focusing on only the subject and not dwell on unwanted topics. It will limit the contents of the report. It will make the report clear, unambiguous, and understandable.

Documenting the Notification Process

This part is mainly concerned with informing the examinee on how the information collected will be used. It deals with the confidentiality of the report. How the examinee was informed about the purpose of the evaluation; how the consent was obtained and whether the examinee understood the nature of the evaluation.

Providing the Factual Basis for an Expert Opinion

The sources of information received by the examiner have to be listed. This will help in maintaining the reliability and accountability of the report. This will also ensure clarity and transparency. The report should only have information that is relevant to the issue. This section may also contain the ‘past history’ or ‘relevant history’ of the person being examined if it proves useful for the issue.

Clinical Conclusions and Expert Opinions

The expert provides his or her opinion after presenting all the relevant data. The data forms the basis or foundation of the opinion. The reasoning has to be provided by the expert for arriving at a particular opinion. Basically, the expert in the end addresses the question by giving his opinion with the help of all the relevant data cited. The data provides for a logical and orderly explanation of the opinions and interpretations.

Acceptable Report Length

Short-length Reports: These reports are approximately three pages long. These reports are essentially the conclusion section of a report, without preceding data, along with recommendations.

Standard Report: These reports are around two to ten pages long. This type of report would include background history, test results, and conclusions. This is the ideal type of report length.

Comprehensive Report: This report can be up to 30 pages. Such types of reports should typically not be used unless the referring party asks so.

Do's and Don'ts

- Do determine the structure of your report beforehand according to your case.
- Do answer the referral question clearly.
- Don't use too technical language, flowery language, and lengthy wordy sentences.
- Do write the report keeping in mind the targeted audience.
- Do avoid grammatical errors and jargon.
- Don't put needless information in the report. Try to answer the referral question only.
- Do consider the length of the report by asking the party for guidance.
- Do report relevant sources in the report and include all the data related to the referral question.
- The test conducted should be comprehensible by the court and the test should be valid and reliable.
- Don't rely on only one source of data.

Difference between Forensic Report and Clinical Report

The purpose of both the clinical report and forensic report is different. The purpose of the former is for a diagnostic clarification or a treatment. Whereas a forensic report is intended to be useful in decision-making in courts. It intends to provide information on a legal issue and generally influences the decision of the court. The impact of both the reports also differs to a large extent. Forensic reports have more lasting repercussions than clinical reports. Clinical reports influence the treatment to be carried out or provide additional information for the treatment. A forensic report influences the judgement of a case. Also, the content of both the reports varies to a great extent. The method of acquiring data is different for both. A forensic report caters to a larger audience than a clinical report. Also since the forensic report may be subjected to a court of law it has to be backed by more reasoning. Thus, it requires more substantiated evidence and opinions backed by reason than a clinical report.

Recommendations

- The legal standard, legal purpose, or forensic purpose for the report should be stated clearly.
- The report should be organized in a logical sequence so that it is understandable to the targeted audience. The information should also be provided in a logical sequence so that conclusions and opinions are followed by the data based upon which the conclusion was arrived at.
- Also, there should be no communication gap between the professionals indulged in a particular report writing. Cooperation and proper communication between professionals will always lead to better results.
- Unnecessary delays should be avoided.
- Speculation and guesswork should also be avoided.
- The language used should be precise and objective. Biasness should be avoided.
- An executive summary can be provided when reports are long. Also, the usage of topic headings to break up the report will make it easier to read.

Standards and best practices in Digital Forensics

There are two subsets of standards and best practice guides:

- Those with a closer link with ISO standards (above the time axis),
- Those without a link or with a very loose link with ISO standards (below the time axis).

The first subset is more about quality assurance and the second is more about technical/legal/judicial processes. Most standards and best practice guides in the second subset (as covered in this chapter) are made by US bodies, which is mainly due to the leading roles of three key US bodies, National Institute of Standards and Technology (NIST) and two SWGs (Scientific Working Groups), in the digital forensics field. This partitioning has its root in the fact that ISO standards are more about quality assurance procedures, so standards and best practice guides more related to technical/legal/judicial procedures are less dependent on ISO standards. While ISO standards are the most important ones among all digital forensics standards, the IAAC forensic-readiness guide is the most comprehensive non-standard guide and also the most recent as its latest edition was published in November 2013. The UK ACPO (Association of Chief Police Officers) 'Good Practice Guide' is probably the most cited non-standard guide, which can be explained by its long history since the 1990s.

All the standards and best practice guides in detail according to the following content-based grouping:

- Electronic evidence and digital forensics
- Multimedia evidence and multimedia forensics
- Digital forensics laboratory accreditation
- General quality assurance (management)
- Training, education and certification

ISO Standards

A number of ISO standards are important in the field of digital forensics:

- ISO/IEC 27037:2012 'Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence' (2012)
- ISO/IEC 27035:2011 'Information technology – Security techniques – Information security incident management' (2011)
- ISO/IEC 17025:2005 'General requirements for the competence of testing and calibration laboratories' (2005)
- ISO/IEC 17020:2002 'General criteria for the operation of various types of bodies performing inspection' (2002)
- ISO/IEC 27001:2013 'Information technology – Security techniques – Information security management systems – Requirements' (2013b)
- ISO/IEC 27002:2013 'Information technology – Security techniques – Code of practice for information security management' (2013a)
- ISO 9001:2008 'Quality management systems – Requirements' (2008)

There are also several other new standards that have not been officially published but are in the final stage of being finalized:

- ISO/IEC 27041 'Information technology – Security techniques – Guidelines on assuring suitability and adequacy of incident investigative methods' (2014a): DIS (draft international standard) as of April 2014
- ISO/IEC 27042 'Information technology – Security techniques – Guidelines for the analysis and interpretation of digital evidence' (2014b): DIS (draft international standard) as of April 2014

- ISO/IEC 27043 ‘Information technology – Security techniques – Incident investigation principles and processes’ (2014c): FDIS (final draft international standard) as of September 2014
- ISO/IEC 30121 ‘System and software engineering – Information technology – Governance of digital forensic risk framework’ (2014d): FDIS (final draft international standard) as of September 2014

Other International/Regional Standards and Guides

There are some other international/regional standards and best practice guides, although some of them (i.e. those made by ASTM International) appear to be more geared to the US digital forensics community. For regional standards and best practice guides we focused mainly on European ones.

- ASTM International Standards4: –
  - ASTM E2678-09 ‘Guide for Education and Training in Computer Forensics’ (2009)
  - ASTM E2763-10 ‘Standard Practice for Computer Forensics Guide’ (2010)
  - ASTM E2825-12 ‘Standard Guide for Forensic Digital Image Processing’ (2012)
- A best practice guide from the IETF (Internet Engineering Task Force): RFC 3227 ‘Guidelines for Evidence Collection and Archiving’ (2002)
- International best practice guides:
  - ILAC-G19:2002 ‘Guidelines for Forensic Science Laboratories’ (2002)
  - ILAC-G19:08/2014 ‘Guidelines for Forensic Science Laboratories’ (2014)
  - IOCE (International Organization on Computer Evidence) ‘Guidelines for Best Practice in the Forensic Examination of Digital Technology’ (2002a)
  - IOCE ‘Training Standards and Knowledge Skills and Abilities’ (2002b)
- European best practice guides:
  - ENFSI (European Network of Forensic Science Institutions) ‘Guidelines for Best Practice in the Forensic Examination of Digital Technology’ Version 6.0 (2009)
  - ENFSI Forensic Speech and Audio Analysis Working Group (FSAAWG) ‘Best Practice Guidelines for ENF Analysis in Forensic Authentication of Digital Evidence’ (2009)

Digital Forensics Best Practices

Forensic examiners adhere to specific standards and rules for conducting examinations that are designed to insure that the original evidence is not altered while in their custody, and to insure that their evidence is later admissible in court. Most best practices and policies are written with those goals in mind.

- Whenever possible, do not examine the original media. Write, protect the original, copy it, and examine only the copy.
- Use write blocking technology to preserve the original while it is being copied.
- Computer forensic examiners must meet minimum proficiency standards.
- Examination results should be reviewed by a supervisor and peer reviewed on a regular schedule.
- All hardware and software should be tested to insure they produce accurate and reliable results.
- Forensic examiners must observe the highest ethical standards.
- Forensic examiners must remain objective at all times.
- Forensic examiners must strictly observe all legal restrictions on their examinations.

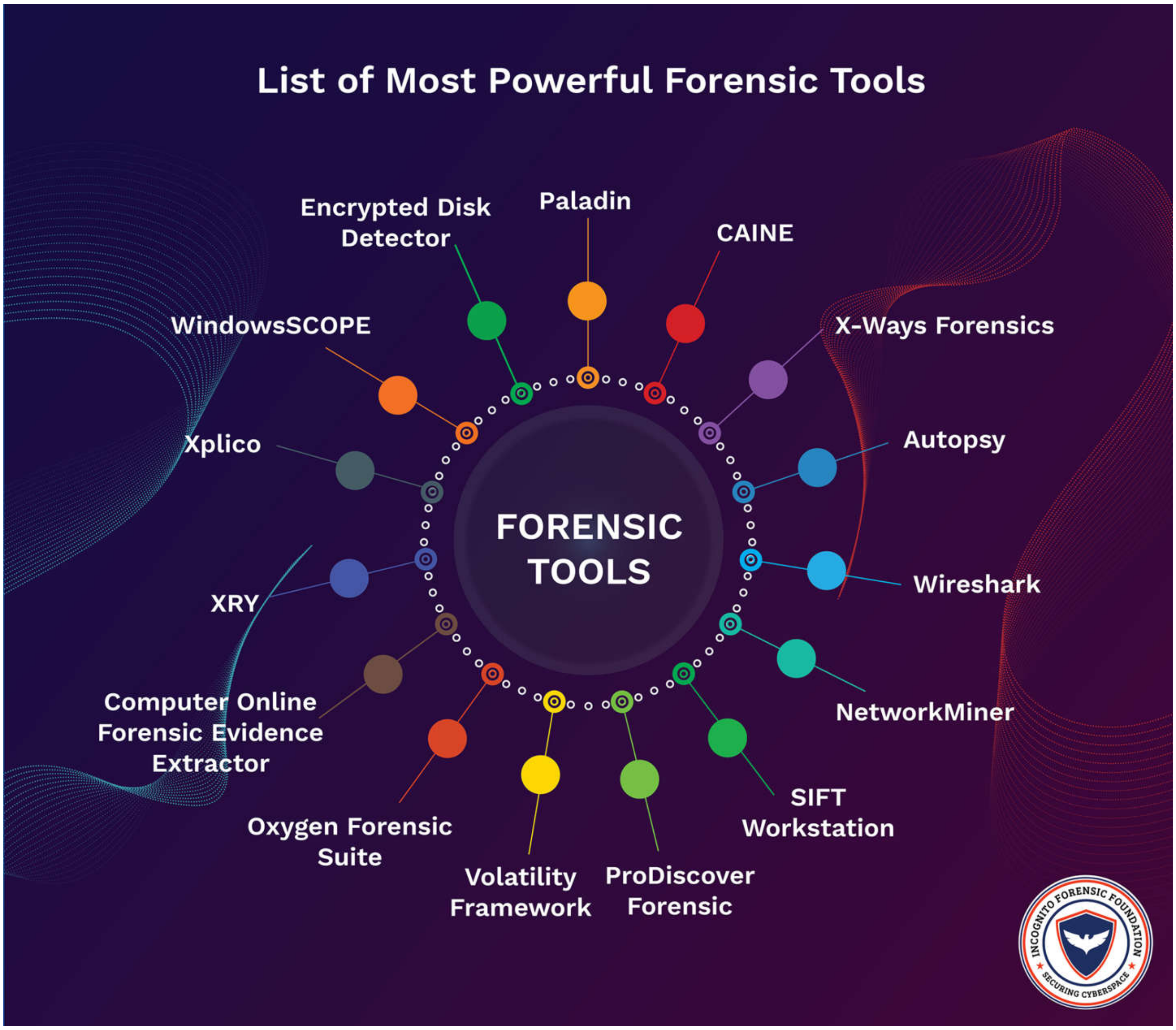
How law enforcement agencies and industry use digital forensics tools

The most common use of digital forensics is to support or refute a hypothesis in a criminal or civil court:

- **Criminal cases**: Involving the investigation of any unlawful activity by cybercriminals. These cases are usually carried out by law enforcement agencies and digital forensic examiners.
- **Civil cases**: Involving the protection of rights and property of individuals or contractual disputes between commercial entities were a form of digital forensics called electronic discovery (eDiscovery).

Digital forensics experts are also hired by the private sector as part of cybersecurity and information security teams to identify the cause of data breaches, data leaks, cyber attacks, and other cyber threats.

Digital forensic analysis may also be part of incident response to help recover or identify any sensitive data or personally identifiable information (PII) that was lost or stolen in a cybercrime.



List of Most Powerful Forensic Tools

FORENSIC TOOLS

- Paladin
- CAINE
- X-Ways Forensics
- Autopsy
- Wireshark
- NetworkMiner
- SIFT Workstation
- ProDiscover Forensic
- Volatility Framework
- Oxygen Forensic Suite
- Computer Online Forensic Evidence Extractor
- XRY
- Xplico
- WindowsSCOPE
- Encrypted Disk Detector