CMSGu2015-02

National Computer Board

Mauritian Computer Emergency Response Team

Enhancing Cyber Security in Mauritius

Good Code of Practice on Digital Forensics

CERT-MU

National Computer Board
Mauritius

Version 1.0

May 2015

Issue No. 2

Table of Contents

DISCLAIMER: *This guideline is provided "as is" for informational purposes only. Information in this guideline, including references, is subject to change without notice. The products mentioned herein are the trademarks of their respective owners.*

1.0 Introduction

1.1 Purpose and Scope

The purpose of this guideline is to aid computer forensic investigators, law enforcement agencies and other stakeholders involved in digital forensics investigation in understanding the principles for the collection, preservation, analysis and reporting of evidence in a way which is admissible to a court of law.

1.2 Audience

The target audience for this document includes incident handlers, cybercrime staff, legal officers and any other group of people involved computer forensics investigations.

1.3 Document Structure

This document is organised into the following sections:

Section 1 contains the document's content, the targeted audience and the document's structure.

Section 2 presents a brief overview on digital forensics.

Section 3 states the different roles in evidence collection and incident handling.

Section 4 explains the need for professional ethics in digital forensics.

Section 5 illustrates the principles of electronic evidence gathering.

Section 6 concludes the document.

Section 7 contains a list of references that have been used in this document.

2.0 Brief Overview on Digital Forensics

Digital forensics, also known as computer and network forensics, has many definitions. Most commonly, it is considered the application of science to the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data.

Regardless of the situation, the forensic process comprises the following basic phases:

- **Collection & Preservation**

  The first phase in the process is to identify, label, record, and acquire data from the possible sources of relevant data, while following guidelines and procedures that preserve the integrity of the data. Collection is typically performed in a timely manner because of the likelihood of losing dynamic data such as current network connections, as well as losing data from battery-powered devices (e.g., cell phones, PDAs).

- **Examination**

  Examinations involve forensically processing large amounts of collected data using a combination of automated and manual methods to assess and extract data of particular interest, while preserving the integrity of the data.

- **Analysis**

  The next phase of the process is to analyze the results of the examination, using legally justifiable methods and techniques, to derive useful information that addresses the questions that were the impetus for performing the collection and examination.

- **Reporting**

  The final phase is reporting the results of the analysis, which may include describing the actions used, explaining how tools and procedures were selected, determining what other actions need to be performed (e.g., forensic examination of additional data sources, securing identified vulnerabilities, improving existing security controls), and providing recommendations for improvement to policies, guidelines, procedures, tools, and other aspects of the forensic process. The formality of the reporting step varies greatly depending on the situation.

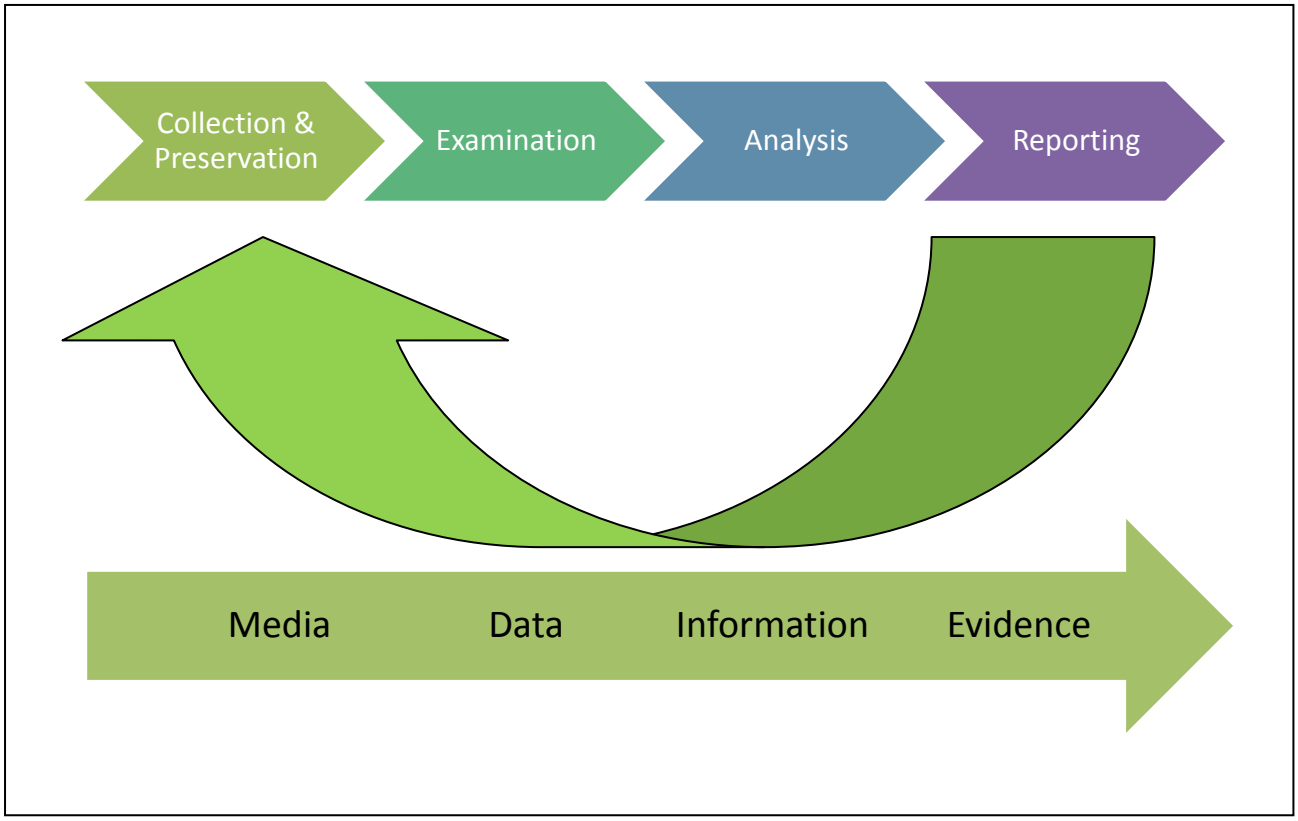

Figure 1 The Forensic Process

3.0 Different roles in evidence collection and incident handling

3.1 Forensic Staffing

Practically every organization needs to have some capability to perform computer and network forensics. Without such a capability, an organization will have difficulty determining what events have occurred within its systems and networks, such as exposures of protected, sensitive data. Although the extent of this need varies, the primary users of forensic tools and techniques within an organization usually can be divided into the following groups:

- **Investigators/Police**
  Investigators are most often from the Mauritius Police Force in Mauritius and they are responsible for investigating allegations of misconduct. The Police use many forensic techniques and tools.

- **Incident Handlers**
  This group responds to a variety of computer security incidents, such as unauthorized data access, inappropriate system usage, malicious code infections, and denial of service attacks. Incident handlers typically use a wide variety of forensic techniques and tools during their investigations. In Mauritius, the CERT-MU is responsible for the abovementioned tasks at the National level.

- **Law Enforcement Officials**
  Legal advisors are also part of the criminal investigation. They are responsible for providing legal advice on the prosecution process and on the forensic report to ensure that it is permissible in a court of law.

- **IT Professionals**
  This group includes technical support staff and system, network, and security administrators. They use a small number of forensic techniques and tools specific to their area of expertise during their routine work (e.g., monitoring, troubleshooting, data recovery).

3.2 Interactions with Other Teams

It is not feasible for any one person to be well-versed in every technology (including all software) used within an organization; therefore, individuals performing forensic actions should be able to reach out to other teams and individuals within their organization as needed for additional assistance. For example, an incident involving a particular database server might be handled more efficiently if the database administrator were available to provide background information, answer technical questions, and provide database documentation and other reference material. Organizations should ensure that IT professionals throughout the organization, especially incident handlers and other first responders to incidents, understand their roles and responsibilities for forensics, receive ongoing training and education on forensic.related policies, guidelines, and procedures, and are prepared to cooperate with and assist others when the technologies that they are responsible for are part of an incident or other event.

In addition to IT professionals and incident handlers, others within an organization may also need to participate in forensic activities in a less technical capacity. Examples include management, legal advisors, human resources personnel, auditors, and physical security staff. Management is responsible for supporting forensic capabilities, reviewing and approving forensic policy, and approving certain forensic actions (e.g., taking a mission-critical system off-line for 6 hours to collect data from its hard drives). Legal advisors should carefully review all forensic policy and high-level guidelines and procedures, and they can provide additional guidance when needed to ensure that forensic actions are performed lawfully. The human resources department can provide assistance in dealing with employee relations and the handling of internal incidents. Auditors can help determine the economic impact of an incident, including the cost of forensic activity. Physical security staff can assist in gaining access to and physically securing evidence. Although these teams often do not play a prominent role in the forensic process, the services that these teams provide can be beneficial.

To facilitate inter-team communications, each team should designate one or more points of contact. These individuals are responsible for knowing the expertise of each team member and directing inquiries for assistance to the appropriate person. Organizations should maintain a list of contacts that the appropriate teams can reference as needed. The list should include both standard (e.g., office phone) and emergency (e.g., cell phone) contact methods.

4.0 The Need for professional ethics in Digital Forensics

The relatively recent and rapid evolution of computers and information systems has resulted in unique capabilities to store, retrieve, and process information. In recent years, new fields of expertise, such as "ethical hacking" and cloud forensics have emerged, all of which have added to the "huge demand" for highly educated specialists in the discipline of digital forensics.

Likewise, the capabilities made possible by the evolution of computers and information systems have given rise to new controversies regarding boundaries and obligations, intellectual property rights, privacy rights, diplomatic relations and military affairs, critical infrastructure, and the public welfare. Although some controversies can be anticipated and prospectively addressed by contract, the remainder, whether fresh or familiar, are to be resolved in civilized societies by the courts of law.

However, both civil and criminal laws have failed to keep pace with technological and societal trends boosted by technological advances. Even where the law may seem certain, pursuing a judicial remedy is costly and burdensome. Consequently, certifying organizations have adopted a code of professional ethics to provide examiners with the framework necessary to avoid or mitigate liabilities likely to require judicial remedies or likely to bring disgrace to the organization.

Codes of ethics serve other important interests, including presenting an image of prestige and credibility for the organization and the profession, eliminating unfair competition and fostering cooperation among professionals

One way to define codes of ethics may be to suggest what the code of ethics is not. First and foremost, it should not be considered as an aspiring commonplace, nor should it be an estimate of or a substitute for the law. Rather, the code of ethics is designed to establish a minimum standard of acceptable conduct for all reasonably foreseeable activities within the profession. Such activities include: representations of one's skills and expertise; research; interactions with clients, supervisors, government authorities, judicial officers, and attorneys; collection, preservation, and analysis of evidence; testing (*i.e.*, validation of hardware and software tools), consultation (advising); report writing; testifying; mentoring; teaching; and continuing education.

Furthermore, digital forensics involves recognizing, classifying, and managing ethical dilemmas, respecting boundaries, and honoring obligations. In light of the wide range of digital forensics activities, one other thing to say the code is not is an exhaustive list of prohibited behaviors or of permissible behaviors.

Although codes of ethics maybe somewhat prescriptive, prohibitive, or a combination of both, they are intended to provide guidance for reasonable persons acting in good faith. What this means is that not every proper behavior can feasibly be enumerated (and if every conceivable prohibited behavior was attempted to be enumerated, the improper ones omitted might be construed as permissible loopholes). Therefore, codes of ethics typically are purposefully broad and vague. This differs significantly from the criminal law, which must be written such that a reasonable person of ordinary intelligence would understand what conduct is prohibited. And, although codes of ethics do not enumerate every possible prohibited act, they often do prescribe proper behavior in hortatory terms, and are otherwise presumptive: Examiners are presumed to possess good moral character and *de minimus* experience and training regarding, among other things: separation of duties; the criminal law applicable to digital forensics investigations; intellectual property law (*e.g.*, trade secrets and copyright), the duty of reasonable care; the duties of loyalty, independence, and confidentiality; and contractual obligations.

Although the code is not law, conduct in violation thereof is likely to harm others, and may expose the examiner to criminal liability, sanctions by a court, damages liabilities in a civil suit, or other adverse consequences. Moreover, conduct or ethical decision-making that clearly falls outside the code of ethics may be the examiner's ruination, because reputation is the examiner's most important asset. Thus, no less important than competence is compliance with the code, which in turn demands consistent, informed ethical decision-making.

5.0 Principles of electronic evidence gathering

When gathering any form of evidence, including digital evidence, it is of paramount importance that appropriate procedures and guidelines are strictly followed and adhered to.

While laws regarding admissibility of evidence differ between countries, using these more practical principles is considered to be a good basic guideline as they are accepted internationally. This does not mean that by applying only these guidelines the evidence gathered will be admissible in court.

The *Electronic evidence guide - A basic guide for police officers, prosecutors and judges,* developed within the framework of the European Union and the Council of Europe joint project (CyberCrime@IPA project), for example, identifies five principles that establish a basis for all dealings with electronic evidence.

- Principle 1 – Data Integrity
- Principle 2 – Audit Trail
- Principle 3 – Specialist Support
- Principle 4 – Appropriate Training
- Principle 5 – Legality

A brief explanation of these five principles is given below.

As a first responder it is important to find out which principles or rules are applicable to you. It is advisable that CERTS get in touch with law enforcement representatives prior to engaging in evidence gathering activities and to familiarize themselves with the applicable rules. In most cases these will be very similar to the principles mentioned above. There may be specific legal requirements, depending on the jurisdiction of the proposed activity.

- **Data Integrity**

  The integrity of digital evidence must be maintained at all stages. From all the principles this is probably the most important one. As the integrity of the evidence is of utmost importance, it is vital that the integrity requirement of the evidence is the main driver and should be the most important factor in deciding what to do (and what not do).

  Digital data is volatile, and the ease with which digital media can be modified implies that documenting a chain of custody is extremely important to establish

the authenticity of evidence. In addition, all examination processes must be documented so that if needed, they can be replicated. The evidential integrity and authenticity of digital evidence can be demonstrated by using hash checksum or Cyclic Redundancy Check (CRC), which is used during the acquisition stage as a method of checking for errors in the evidence file. However, nowadays we can consider that those methods are not sufficient anymore. Therefore it is considered better to use a one-way hash algorithm such as MD5 or SHA-1. This way it is possible to determine if changes have occurred to digital evidence at any point of an investigation. As both MD5 and SHA-1 algorithms are now considered to be relatively weak it is recommended to use stronger algorithms such as SHA-2. In some circumstances it is necessary that data on a computer that is still running has to be accessed. Special precautions should be taken to minimise the impact on the data and this should be done, as said, only exceptionally and only by competent personnel to perform this operation and able to "explain the relevance and the implications of their actions".

When the evidence cannot be collected without altering it, gathering steps must be very well documented and you have to be able to tell exactly what tools were used, what they did to the system and which changes they produced. This is for example important when performing a memory dump[27]. Such a memory dump cannot be done without incurring at least some modification of the memory. But in many cases it is much more valuable to have the data from volatile memory even if altered than not have it at all. The first responder must however be able to testify later which steps he/she took and to explain any alteration to the evidence that was not avoidable.

- **Audit trail**

  An audit trail (often referred to as chain of custody or chain of evidence) is the process of preserving the integrity of the digital evidence. "Documentation permeates all steps of investigative process but is particularly important in the digital evidence seizure step. It is necessary to record details of each piece of seized evidence to help to establish its authenticity and initiate the chain of custody." Indeed, an "audit trail or other record of all processes applied to digital

evidence should be created and preserved. An independent third party should be able to examine those actions and achieve the same result."

It is of vital importance that any digital exhibit can be tracked from the moment when it was seized at the crime scene all the way to the courtroom, as well as anywhere else in between such as laboratories or storages. To demonstrate that a robust chain of custody or audit log was maintained details of the evidence and how it was handled, by whom as well as everything that has happened to it needs to be recorded at every step of the investigation.

It is important to stress how such details can be crucial. It is better to note down too many details than recording too few details about the actions taken. It is, for example, advisable to note down which keystrokes were entered and which mouse movements have been made rather than just to write down in generic terms that "a forensic backup has been performed."

- **Specialist support**

  Specialist support needs to be requested as soon as possible when evidence gathering raises some specific (technical issues) and the first responders in charge of the evidence collection is not familiar with the issue or its implications.

  As there are so many different systems and technical situations, it is almost impossible for a digital forensics expert to have the specific know-how on how to deal with all these sorts of electronic evidence. This is why it is so crucial to call in the right specialists – either internal from the team or from external - when necessary and to have the right equipment ready for them to perform their tasks.

- **Appropriate training**

  Proper training is a very important prerequisite for the success of the search and seizure of electronic evidence. Appropriate and constant training should be provided to all first responders dealing with digital forensic, especially when they are expected to deal specifically with 'live' computer and access original data.

- **Legality**

The person in charge of the investigation has overall responsibility for ensuring that the law and the principles of digital evidence are adhered to.

Legal guidance for the practitioner varies depending on the jurisdiction in which they reside. Further, a distinction must be made between legislative documents and guidance and principles provided by relevant governing bodies within the forensic industry.

5.1 Collecting Evidence

5.1.1 Arriving at the scene

Upon arrival at a (potential) crime scene, it is vital that the first responder establishes his surroundings, identifying key evidential areas of the scene and any individuals who are involved in the suspected offence. If the first responder is not the first person at the scene, they should seek to establish contact with those persons who attended the crime scene first. Upon doing so, they can establish the potential location of digital devices and any interaction which has occurred between suspects at the scene.

Prior to entering the scene, health and safety requirements should be established. It is crucial to identify threats which remain, either in the form of personnel still present at the scene, along with environmental factors. The safety of the first responder and other officials at the scene is paramount and steps should be taken to ensure they are not placed in danger.

It also is best practice to never go alone to unknown locations (like home user apartments, a customer's offices, etc.). When doing this as support for a client like for example a bank, someone from the client institution should accompany the first responder. In some cases it might be necessary to explain to the representative of the constituent or client what exactly will be done (e.g. trying to confirm that there is malware on the system) and, even more importantly, what will not be done. It can be useful to ask this person what (s)he has been doing and if he (s)he has noticed strange behaviour of the system. This information can lead to clues on the necessary next steps.

Upon entering the scene the first responder should maintain contemporaneous notes of their actions. The first responder should have access to guidelines from his/her employer or from the body that requested the evidence gathering on how to do this.

To supplement written notes, a first responder should utilise a digital camera or video recording device in order to create accurate depictions of the scene.
Records should include but are not limited to:

- Time and date which the scene was entered
- Floor plan of the scene documenting the location of devices and surrounding objects
- Personnel present in the scene
- Photographs of the scene upon entering
- Photographs of all digital exhibits *in situ*

All digital evidence should be identified and secured and no unauthorised individuals should interact with the devices. First responders should also attempt to ascertain as much information from the constituent. Password login information, network topology (both physical and virtual), users of the computer systems, Internet connections and security provisions could all provide useful guidance during an examination of the exhibit. It is important to note that first responders should not deal with suspects.

5.1.2 Evidence Collection

As mentioned, in many cases the first responder might be required to collect evidence in the premises of a client (e.g. a bank, company or a private individual's home). As analysing this data is in most cases quite time-consuming, it often will make sense to produce a mirror of the systems and analyse the images in the lab and not on site.

It is recommended that the first responder has a flow chart at hand on how to proceed in different cases. It is vital that this flow chart covers almost all possible cases. Important questions in this tree would be:

- Is the computer running?
- Is the computer networked?
- Do you want to preserve volatile data?
- Is there full-disk encryption applied?
- Is the console unlocked?

5.1.3 Memory forensics

Although forensic analysis of volatile memory is out of the scope of this document as it is quite complex, it is important for the first responder to understand that sometimes the data or evidence you're looking for is only in the physical memory. In such cases a shutdown to create a forensic image of the discs will cause that data to be lost or changed. Data within physical memory that might be evidentially relevant could among other things be application processes, open files and registry handles, network information, passwords and cryptographic keys, unencrypted content, hidden data and possibly malicious code.

Data within physical memory is constantly changing and is not structured in the same way that in file systems of for example hard drives and is therefore much more difficult to predict and parse into meaningful data as a result. Hard disks have a strict pre-defined structure where analysts know where to look for certain structures and data types on a specific kind of file system. Memory can be allocated and de-allocated to different areas depending on what memory is already being used.

In many occasions passwords and configuration files reside (in decrypted form) in the memory, but can only be found on disk in encrypted form. When investigating a possible malware infection, for instance, it might be useful to know which network connections were made. Removing a computer system from the network will terminate these connections which could possibly be very important to know.

As storage becomes cheaper and cheaper we often encounter cases where the hard drive space would take weeks to analyse as the amount of data is enormous. In these cases an appropriate and targeted memory search could give the desired results fairly quickly.

There are a number of tools that can be used to dump physical memory for different platforms and where possible the tool should be run from an external device such as a USB thumb drive, and the memory dump itself should be saved to an external hard drive as well. A note worth remembering is that when a USB device is inserted into a PC it will leave information behind and unavoidably alter the system. In a Windows for example this would be creating entries in the Registry for the USB device being used.

5.2 Sources of evidence

There are numerous sources of digital evidence and each requires a different process for gathering that evidence as well as different tools and methods for capturing it. It is not just the personal computer, laptop, mobile phone or Internet that provides sources of digital evidence, any piece of digital technology that processes or stores digital data could be used to commit a crime. The device and information it contains may store relevant digital evidence for proving or disproving a suspected offence.

It is vital that responders are able to identify and correctly seize potential sources of digital evidence. An example of the types of digital devices encountered by a digital forensic practitioner include, but are not limited to the following:

- Computers – such as Personal Computers (PC's), laptops, servers or even game consoles
- Storage devices – Compact Discs, Digitally Verstaile Discs, removeable data storage drives (USB thumb drives) and memory cards
- Handheld devices - mobile (smart) phones, digital cameras, satelite navigation systems
- Network devices like hubs, switches, routers and wireless access points

There is an important difference between volatile and non-volatile data. Volatile data is data that is lost when the device is not powered on. A typical example of this would be the random-access memory (RAM) storage in a PC. Nowadays personal computers have gigabytes of volatile storage so the data in the RAM is becoming more and more important. When gathering evidence, this should be taken into account as just simply disconnecting a system from power might destroy evidence stored in volatile storage. Doing a memory dump is necessary at this stage in many cases.

5.3 Digital forensics tools and commands

Over the last decade, the number of crimes that involve computers has grown, spurring an increase in companies and products that aim to assist law enforcement in using computer-based evidence to determine the who, what, where, when, and how for crimes. As a result, computer and network forensics has evolved to assure proper presentation of computer crime evidentiary data into court. Forensic tools and techniques are most often thought of in the context of criminal investigations and computer security incident handling used to respond to

an event by investigating suspect systems, gathering and preserving evidence, reconstructing events, and assessing the current state of an event. However, forensic tools and techniques are also useful for many other types of tasks, such as the following:

- **Operational Troubleshooting**

  Many forensic tools and techniques can be applied to troubleshooting operational issues, such as finding the virtual and physical location of a host with an incorrect network configuration, resolving a functional problem with an application, and recording and reviewing the current OS and application configuration settings for a host.

- **Log Monitoring**

  Various tools and techniques can assist in log monitoring, such as analyzing log entries and correlating log entries across multiple systems. This can assist in incident handling, identifying policy violations, auditing, and other efforts.

- **Data Recovery**

  There are dozens of tools that can recover lost data from systems, including data that has been accidentally or purposely deleted or otherwise modified. The amount of data that can be recovered varies on a case-by-case basis.

- **Data Acquisition**

  Some organizations use forensics tools to acquire data from hosts that are being redeployed or retired. For example, when a user leaves an organization, the data from the user.s workstation can be acquired and stored in case it is needed in the future. The workstation.s media can then be sanitized to remove all of the original user.s data.

- **Due Diligence/Regulatory Compliance**

  Existing and emerging regulations require many organizations to protect sensitive information and maintain certain records for audit purposes. Also, when protected information is exposed to other parties, organizations may be required to notify other agencies or impacted individuals. Forensics can help organizations exercise due diligence and comply with such requirements.

The typical tools used by law enforcement and the private sector to carry out digital forensic investigations are often close-sourced and expensive commercial packages. Examples are ENCASE and FTK. During the 1980s and the beginning of the 1990s, most digital forensic investigations were carried out using non-specialist tools. From then on, specialised software and hardware was created that allowed digital forensics investigations to take place without modifying data and media. The move from 'live analysis' to the use of these tools boosted the capabilities of digital forensics enormously.

However, forensic investigations should not be restricted to only these tools. Investigators should make use of Windows and Linux commands available online for better results. Experimenting with these tools in a test environment and on test data is a very good way for knowing the strength of the respective tools. Various disk images and memory dumps that can be used to train and experiment can be found online. It is important that investigators have good command of their tools and that they have the functionalities of these commands always in the back of their minds.

5.4 Evidence Examination

The investigation process itself involves the interpretation of the raw data and the reconstruction of events. This examination should be conducted on the data acquired and not on the original evidence. Although this examination is in most cases out of the scope for most CERTs, it is important that first responders have a good knowledge of what could be done with the evidence. Also, in some cases it could be that law enforcement asks for assistance to CERTs with regards to the examination.

5.4.1 Extraction

The examination and identification of evidence is dependent upon the type of crime which is being analysed. Evidential files can come in many forms, ranging from proprietary operating systems files to Internet browser artefacts. There are many techniques used to target this evidence which include but are not limited to:

- **Hashing**

- Hashes are a unique string used to identify a file and ensure it has not been tampered with since its gathering.

- **Keyword searching**
  - Keyword searching is the process of location strings of information.
  - Often utilised in forensics to highlight files which may contain particular text which would indicate that they are evidential.
  - Can significantly cut down the time it takes to complete an investigation.

- **File signatures**
  - Each type of file mains a series of bytes at the beginning which identifies its type. This must be queried against the extension it has - if they match then the file is what it says it is.

- **Known evidential locations**
  - Specific areas of a system can be analysed to identify known relevant files.
    - Registry for MRU lists, Typed URLs etc.
    - Recent folder for records of recently accessed files.
    - Often specific Malware samples can be identified by specific files or other changes visible to the analyst

- **File carving**
  - Files have a file signature or string of bytes at the beginning which identifies the starting point of the file - often this is termed as the file header
  - Files often also maintain a 'file footer'. Similar to the header, this is a unique set of bytes at the end of the file.
  - All data between the header and footer is relevant to that particular file and the process of collection of this data from unallocated areas of the disk is known file carving.

- **Mounting of compound files**
  - Files with an internal file structure or set of files storage within it.
  - Examples include, .zip, .rar

- **File system containers**
    - Often interesting data is stored in file system containers or images which may require a password to mount. If a system is shut down access to mounted devices may no longer be possible due to missing passwords. Some file containers cannot be recognized as such. Thus due care is needed analysing a live system.

5.4.2 Analysis

Once the data is extracted it can be analysed. Although the analysis of evidence is out of scope of this report, we quickly want to touch upon this topic.

One example of this analysis is the evidence from the Internet-based activities. This can take multiple forms depending on the user's choice of application for accessing Internet-based content.

Typically a user will browse the Internet using an Internet browser application, like Chrome, Internet Explorer, and FireFox.

A user visits a website by either typing in the URL (universal resource locator) for the webpage or searching for it via a search engine (e.g. Google). These actions leave behind traces known as Internet History (IH). IH is often stored in system files belonging to the web browser; however each browser maintains its own unique structure for maintaining its IH. Internet Explorer maintains IH in index.dat files, Firefox maintains SQLite database files. An analysis of IH can often reveal where a user has been whilst browsing the Internet, the time and date these actions were carried out and how often a user visits a particular site. Many browsers have the ability to delete their IH; however, even after this action has been carried out it is often possible to recover these recovered from deleted portions of the hard drive.

Another important source of information depicting Internet usage is the Internet cache and temporary Internet Files (TIF). The Internet cache is a feature of most browsers, designed to improve the user's experience whilst browsing the website by speeding up the process of rendering webpages. Every time a user visits a webpage it is downloaded to the local machine. The next time the user visits this website, the webpage can be re-built quicker by using the locally downloaded elements as opposed to downloading the website content again.

This provides significant benefit to the forensic analyst as the cache maintains a record of webpages, which the user has visited which could include pictures and videos hosted on the webpage itself.

Furthermore browsers store cookies containing a plethora of information. It also should be noted, that many browsers create backups of history files which may be recovered.

Modern web browsers can operate in so called ‘incognito’ or ‘private’ mode. No information is saved then. In most of these cases preserving live evidence is the only way to go.

During the analysis it is extremely important to have the overall timeline (a list with timestamps, sources, names and descriptions of the findings). Timelines are for identifying at what point in time a certain activity has occurred on a system. They are mostly used for data reduction as well as for the identification of changes that have occurred on a certain system over time. Many forensic tools now have integrated options for timeline searches. Timelines are very powerful in the field of digital forensics but they also bring a lot of complexity with them. There can be a mismatch between BIOS and System Clock settings, settings from multiple users or even systems, etc.

One point that can lead to confusion and must be considered by the analyst is the time on the system. What time zone the system was running in. How much time was the system off from the real time? The time of some evidence is recorded in local system time. Other time stamps are recorded in UTC time. All time stamps must hence be ‘normalized’ to get an accurate picture.

5.5 Presentation of evidence and reporting

- **Presentation**

  A report must be written in a way that is suitable for a non-technical audience and digital evidence needs to be presented in a clear and accurate manner, which clearly identifies the significance of the actual evidence to the investigation.

- **Verification**

The report should focus on and verify that the evidence being presented is authentic, reliable and admissible and it should be sufficiently detailed so that an independent third party could replicate the conclusions.

- **Forensic Examination**

  To support the report writing process a forensic examination requires detailed notes to be taken contemporaneously.

- **Conclusions**

  The investigator should clearly state what forensic tools were used in the investigation to assist any reviewer in understanding the results and conclusions being made.

Before formally submitting a written report or presenting any results from an investigation, the investigator should validate these results. It is considered best practice to verify the evidence and the best way to verify your results is by running a second reliable forensic tool, or by manually checking the evidences original location and confirming it matches the original results.

When a digital forensic investigator presents the findings it is often beneficial to state clearly in the report how the evidence was handled and analysed to demonstrate and verify the chain of custody and also all of the investigative processes that were carried out on the evidence.

However, the format of the report depends on the initial requirements on the investigation. It should, if possible, be agreed on beforehand.

6.0 Conclusion

Digital forensics or computer forensics involves many steps such as evidence collection, preservation, analysis and reporting. It is crucial that the data collected at a crime scene remains untampered so that the result obtained after full examination is not biased. The result is then presented in the form of a report in a court of law for final judgement. Not only are principles for electronic evidence gathering important, but also professional ethics.

7.0 References

- **www.enisa.europa.eu**
- **www.acpo.police.uk**
- **www.7safe.com**
- **www.csrc.nist.gov**