Unit 1: Digital Evidence and Processes involved in Digital Forensics

1

UNIT STRUCTURE

1.1 LEARING OBJECTIVES

After going through this chapter, you should be able to understand:

- Challenges in cyber forensics
- Principles in evidence management
- Role of First Responder

1.2 INTRODUCTION

The field of cyber forensics is still in its infancy stage as it possesses a strong need for direction and definition. Areas of speciality within a professional environment, certifications, and/or curriculum development are still questioned. With the continued need to standardize parts of the field, methodologies need to be created that will allow for uniformity and direction. To date, huge volumes of data, heterogeneous information and communication technologies, and borderless cyberinfrastructure create new challenges for security experts and law enforcement agencies investigating cybercrimes.[43] The future of digital forensics is explored, with an emphasis on these challenges and the advancements needed to effectively protect modern societies and pursue cybercriminals. Today the technology in cyber forensic is utilizing the application of scientific methods and technics to recover data from electronic and digital media. The increase in the growth of computer and the Internet use has changed the human behaviour and ways of communication, this growth in technology has given rise to the rise in cybercrime which is now sophisticated and difficult to trace, investigate, and prosecute of criminals without reliable and accurate data collection.[44]

1.3 DIGITAL EVIDENCE

Digital evidence or electronic evidence is any probative information stored or transmitted in digital form that a party to a court case may use at trial. Before accepting digital evidence a court will determine if the evidence is relevant, whether it is authentic if it is hearsay and whether a copy is acceptable or the original is required. The digital evidence is used to establish a credible link between the attacked, victim, and the crime scene. Some of the information stored in the victim's system is based on the IP address, system log-in & remote log-in details, browsing the history, log files, emails, images etc.

1.4 LOCARD'S PRINCIPLE

[43] ORGANIZING RESEARCH AND DEVELOPMENT IN CYBER FORENSICS <https://docs.lib.purdue.edu/cgi/viewcontent.cgi?article=1075&context=techmasters>

[44] Adelstein F (2006) Live forensics: diagnosing your system without killing it first. Commun ACM 49(2):63–66

Wherever a criminal, steps, whatever he touches, whatever he leaves, even unconsciously, will serve as a silent witness against him. Not only his fingerprints or his footprints but his hair, the fibers from his clothes, the glass he breaks, the tool mark he leaves, the paint he scratches, the blood or semen he deposits or collects. All of these and more, bear mute witness against him. This is evidence that does not forget. It is not confused by the excitement of the moment. It is not absent because human witnesses are. It is factual evidence. Physical evidence cannot be wrong, it cannot perjure itself, it cannot be wholly absent. Only human failure to find it, study and understand it, can diminish its value. Digital evidence is usually not in a format that is directly readable by a human. Therefore it requires some additional steps to convert it into a human-readable form in the form of writing. Digital evidences must follow the requirements of the Best Evidence Rule.[45]

1.5 BEST EVIDENCE RULE

The Best Evidence Rule, which has been established to deter any alteration of evidence, either intentionally or unintentionally, states that the court prefers the original evidence at the trial rather than a copy, but will accept a duplicate under these conditions:

- The original was lost or destroyed by fire, flood, or other acts of God. This has included such things as careless employees or cleaning staff.
- The original was destroyed in the normal course of business.
- The original is in possession of a third party who is beyond the court's subpoena power.

This rule has been relaxed to allow duplicates unless there is a genuine question as to the original's authenticity, or admission of the duplicate would, under the circumstances, be unfair.[46]

1.6 CHARACTERISTICS OF DIGITAL EVIDENCE

The following are the essential characteristics of digital evidence:-

[45] Rahayu, S. & Robiah, Y. & Sahib, Shahrin. (2008). Mapping Process of Digital Forensic Investigation Framework. 8

[46] Hewling, Moniphia & Sant, Paul. (2012). Digital Forensics: An integrated approach

- ***Admissibility***

It must be in conformity with common law and legislative rules. There must be a relationship between the evidence and the fact being proved. Digital evidence is often ruled inadmissible by courts because it was obtained without authorization. In most jurisdictions, a warrant is required to seize and investigate digital devices. In a digital investigation this can present problems where, for example, evidence of other crimes are identified while investigating another.[47]

- ***Reliability***

The evidence must be from undisputed origin

- ***Completeness***

The evidence should prove the culprit's actions and help to reach a conclusion.

- ***Convincing to Judges***

The evidence must be convincing and understandable by the judges.

- ***Authentication***

The evidence must be real and related to the incident. Courts largely concerned themselves with the reliability of such digital evidence. The investigator must be able to prove to the authenticity of the digital evidence by explaining:

- The reliability of the computer equipment.
- The manner in which the basic data was initially entered.
- The measures taken to ensure the accuracy of the data as entered.
- The method of storing the data and the precautions are taken to prevent its loss.
- The reliability of the computer programs used to process the data, and
- The measures taken to verify the accuracy of the program.

1.7 TYPES OF INVESTIGATION

There are four main types of investigation performed by digital forensics specialists.

[47] Carrier B. D., Spafford E, (2004) "An event based Digital forensics Investigation Framework" Center for Education and Research in Information Assurance and Security

a) Criminal Forensics

Criminal forensics is the largest form of digital forensics and falling under the remit of law enforcement (or private contractors working for them). Criminal forensics is usually a part of a wider investigation conducted by law enforcement and other specialists with reports being intended to facilitate that investigation and, ultimately, to be entered as expert evidence before the court. Focus is on forensically sound data extraction and producing report/evidence in simple terms that a layman will understand.

b) Intelligence gathering

Intelligence gathering is a type of investigation associated with crime, but in relation to providing intelligence to help track, stop or identify criminal activity. Unless the evidence is later to be used before the court of law, forensic soundness is less of a concern in this form of investigation, instead speed can be a common requirement.

c) Electronic discovery (eDiscovery)

Electronic discovery or eDiscovery is similar to ***"Criminal Forensics"*** but in relation to civil law. Although functionally identical to its criminal counterpart, eDiscovery has specific legal limitations and restrictions, usually in relation to the scope of any investigation. Privacy laws (for example, the right of employees not to have personal conversation intercepted) and human rights legislation often affect electronic discovery.

d) Intrusion Investigation

The final form of investigation is different from the above-mentioned three types of investigation. Intrusion investigation is instigated as a response to a network intrusion, for example, a hacker trying to steal corporate secrets. The investigation focuses on identifying the entry point for such attacks, the scope of access and mitigating the hacker's activities. Intrusion investigation often occurs ***"live"*** (i.e. in real-time) and leans heavily on the discipline of network forensics.

1.8 CHALLENGES IN DIGITAL FORENSICS IN PRESENT ERA

Digital forensics is facing a crisis. Hard-won capabilities are in jeopardy of being diminished or even lost as the result of advances and fundamental changes in the computer industry:

- The growing size of storage devices means that there is frequently insufficient time to create a forensic image of a subject device or to process all of the data once it is found.
- The increasing prevalence of embedded flash storage and the proliferation of hardware interfaces means that storage devices can no longer be readily removed or imaged.
- The proliferation of operating systems and file formats is dramatically increasing the requirements and complexity of data exploitation tools and the cost of tool development.[48]
- Whereas cases were previously limited to the analysis of a single device, increasingly cases require the analysis of multiple devices followed by the correlation of the found evidence.
- Pervasive encryption means that even when data can be recovered, it frequently cannot be processed.
- Use of the ***"cloud"*** for remote processing and storage, and to split a single data structure into elements, means that frequently data or code cannot even be found.
- Malware that different programmed information to persistent storage necessitates the need for expensive RAM forensics.
- Legal challenges increasingly limit the scope of forensic investigations.

These problems are most obvious to examiners faced with cell phones and other mobile computing platforms. It is vital for forensics examiners to be able to extract data from cell phones in a principled manner, as mobile phones are a primary tool of criminals and terrorists. But there is no standard way to extract information from cell phones. In recent years there has been substantial interest in RAM-based forensics to defeat encryption and to find malware that is not written to persistent storage. RAM forensics can capture the current state of a machine in a way that is not possible using disk analysis alone. But RAM Digital Forensics tools are dramatically more difficult to create than disk tools. Unlike information written to disk, which is stored with the intention that it will be read back in the future possibly by different programmed information in RAM is only intended to be read by the running program. As a result, there is less reason for programmers to document data structures or conserve data layout from one version of

[48] Brill AE, Pollitt M (2006) The evolution of computer forensic best practices: an update on programs and publications. Journal of Digital Forensic Practice, 1:3–11

a program to another. Both factors greatly complicate the task of the tool developer, which increases tool cost and limits functionality.

1.9 PROCESSES INVOLVED IN DIGITAL FORENSICS

The digital forensics process involves the following five levels of investigation:-

a) Identification of the Digital Evidence

This step involves the identification of any digital evidence which might be present at the crime scene. This can involve computers, pen drives, hard disks or any other electronic device that can store digital data. Also, it needs to be taken care of that the processes followed when the computer is found in on or off state are different.

b) Acquisition of the Identified Evidence

This step comes after the identification step as after the evidence has been identified it needs to be acquired in the most appropriate manner such that the integrity of the data stored in the evidence remains intact. The sub-steps followed during this part of the investigation can be seizing the crime scene, forensically acquiring the data stored in the found devices for further investigation. The two sources of evidence: ***volatile and non-volatile data*** have different methods of acquisition. In the case of volatile data, the order in which the data is collected is of utmost importance. One suggested order can be network connections, ARP cache, login session, running processes, open files and the contents of RAM. Meanwhile, in case of non-volatile data i.e. from hard-disk the bitstream image can be done using three strategies: using a hardware device such as write blocker where the system is taken offline and the hard drive is removed, using a forensic tool Helix which is used to boot the system or using a live system acquisition which can be done either locally or remotely in case of encrypted systems that cannot be taken offline or are only accessible remotely.[49]

c) Preservation of the acquired evidence

The evidence acquired should be kept in such a way that it remains the same even after the investigation process has been completed as it was first acquired. This is done via a well-

[49] Carrier, B, & Spafford, E H (2004) An Event-based Digital Forensic Investigation Framework. Proceedings of Digital Forensics Research Workshop. Baltimore, MD

defined process known as the chain of custody which ensures that the evidence remains protected from the unintended alterations. In order to achieve this, read-only copies are made by the practitioners or experts to work upon whereas, the original evidence is kept in a secured location.

d) Examination and Analysis stage

This is the most crucial step of any investigative procedure as it is the strongest as well as the most vulnerable part where any minor mistake can lead up to the evidence's ineffectiveness to be presented in the court of law. Examining the evidence involves the step of categorizing the digital evidence and the tools which would be used to analyse that evidence. For instance, a received email can include multiple information regarding the source's email address, metadata as well as the data which can be used to find the IP address of the sender's workstation. One important advice which needs to be taken care of at this stage of analysis involves the difference in the data generated from different devices. For instance, the data and the metadata generated from an image and an email would be different. Evidence's correctness and authenticity to be presented in the court of law totally depends upon the expert's experience and skill.

e) Presentation or Documentation of Evidence

This is the last stage of the investigation procedure which includes the process of presenting a report or documentation on what type of evidence was obtained, the description about the experts who worked upon the evidence, the methods followed and the tools used in a specific format. The report can also include the protocols and legal policies followed. It should be presented in the most understandable way stating its findings to be very accurate.

1.10 ROLE OF FIRST RESPONDER

The first responder is the person who first accesses the victim's computer. He must be prepared well to collect the evidence for the crime scene in a manner that is accepted by the court.[50] Therefore, the availability of trusted digital forensics toolkit is necessary for the first responder. Some of the important steps in preparing the first responder's toolkit are:

a) Create a forensics tool testbed

[50] Casey, E (2004) Digital Evidence and Computer Crime (2 ed) Elsevier Academic Press

The testbed should be created from the trusted source and functionality of the testbed should be checked in advance before using them in the field. Some of the guidelines are:

- Identify the appropriate OS type your organization is using, based on which the testbed is created. An organization may have a verity of OS deployed in its network. For example, it may have Linux based servers and Windows and Mac-based PC/Laptop. In that case, one has to create multiple testbeds for each OS type.
- Disinfect the testbed from the availability of any data on the machine. Preferably use a new/fresh machine. In case, a new machine is not available to use wiping tools to wipe out any data from the machine.[51]
- Install the OS and all the necessary software to conduct the forensic investigation.
- Ensure that the OS and all the programmes installed in the testbed are updated to the latest version. If any patch is required for the successful operation of the system, the same should also be installed.
- Compute Hash to ensure the integrity of the file system.

b) Document the Forensics tool testbed

It includes the following:-

- Name, type and version of OS.
- Details of the types of various applications/software installed in the testbed along with the details of the upgrades and patches.
- Details of various types of hardware installed in the testbed.
- Details pertaining to hash and checksum of the testbed.

c) Document the summary of the forensic tools

For every tool that is acquired for the testbed, the following information is documented for easy reference and record.

- Details about the source from where the software was brought. In case it's a freeware, mention the site/source from where the tool was downloaded.

[51] K.Rogers, M., Goldman, J., Mislan, R, Wedge, T, & Debrota, S (2006) Computer Forensics Field Triage Process Model. Proceedings of Conference on Digital Forensics, Security and Law, (pp 27-40)

- Detailed description about the purpose, working and compatibility of the tool with OS and other software.
- Details of tool dependencies and the system effects which include the details about the required system access levels by the user to run a tool and the details of shared libraries.

d) Test the tools

Now the tools selected and installed are tested in the testbed and its performance and output is examined.

1.11 LET'S SUM UP

In this chapter, we have studied digital evidence and its characteristics along with the best evidence rule. Finally, we also studied the challenges faced in digital forensics in the present era and the processes involved in digital forensics.

1.12 FURTHER READING

- Rahayu, S. & Robiah, Y. & Sahib, Shahrin. (2008). Mapping Process of Digital Forensic Investigation Framework. 8.
- Adams, Richard & Hobbs, Val & Mann, Graham. (2014). Journal of Digital Forensics, Security & Law. Journal of Digital Forensics, Security & Law. 8. 25-48.
- Hamidovic, Haris & Salkic, Hadzib. (2016). THE BASIC STEPS OF DIGITAL EVIDENCE HANDLING PROCESS. International Journal of information and communication technologies. 2.
- Prasad, Ajay & Pandey, Jeetendra. (2016). Digital Forensics.

1.13 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. What is Locard's Principle?

Wherever a criminal, steps, whatever he touches, whatever he leaves, even unconsciously, will serve as a silent witness against him. Not only his fingerprints or his footprints but his hair, the fibers from his clothes, the glass he breaks, the tool mark he leaves, the paint he scratches, the blood or semen he deposits or collects. All of these and more, bear mute witness against him. This is evidence that does not forget. It is not confused by the excitement of the

moment. It is not absent because human witnesses are. It is factual evidence. Physical evidence cannot be wrong, it cannot perjure itself, it cannot be wholly absent. Only human failure to find it, study and understand it, can diminish its value. Digital evidence is usually not in a format that is directly readable by a human. Therefore it requires some additional steps to convert it into a human-readable form in the form of writing.

2. What are the different types of investigation?

There are four main types of investigation performed by digital forensics specialists.

a) Criminal Forensics

Criminal forensics is the largest form of digital forensics and falling under the remit of law enforcement (or private contractors working for them). Criminal forensics is usually a part of a wider investigation conducted by law enforcement and other specialists with reports being intended to facilitate that investigation and, ultimately, to be entered as expert evidence before the court. Focus is on forensically sound data extraction and producing report/evidence in simple terms that a layman will understand.

b) Intelligence gathering

Intelligence gathering is a type of investigation associated with crime, but in relation to providing intelligence to help track, stop or identify criminal activity. Unless the evidence is later to be used before the court of law, forensic soundness is less of a concern in this form of investigation, instead of speed can be a common requirement.

c) Electronic discovery (eDiscovery)

Electronic discovery or eDiscovery is similar to ***"Criminal Forensics"*** but in relation to civil law. Although functionally identical to its criminal counterpart, eDiscovery has specific legal limitations and restrictions, usually in relation to the scope of any investigation. Privacy laws (for example, the right of employees not to have personal conversation intercepted) and human rights legislation often affect electronic discovery.

d) Intrusion Investigation

The final form of investigation is different from the above-mentioned three types of investigation. Intrusion investigation is instigated as a response to a network intrusion, for example, a hacker trying to steal corporate secrets. The investigation focuses on identifying

the entry point for such attacks, the scope of access and mitigating the hacker's activities. Intrusion investigation often occurs ***"live"*** (i.e. in real-time) and leans heavily on the discipline of network forensics.

3. What is Best Evidence Rule?

The Best Evidence Rule, which has been established to deter any alteration of evidence, either intentionally or unintentionally, states that the court prefers the original evidence at the trial rather than a copy, but will accept a duplicate under these conditions:

- The original was lost or destroyed by fire, flood, or other acts of God. This has included such things as careless employees or cleaning staff.
- The original was destroyed in the normal course of business.
- The original is in possession of a third party who is beyond the court's subpoena power.

This rule has been relaxed to allow duplicates unless there is a genuine question as to the original's authenticity, or admission of the duplicate would, under the circumstances, be unfair.

1.14 ACTIVITY

Explain the challenges and the process involved in digital forensics along with the Role of the First Responder and the important steps in preparing the toolkit? (1000-1500 words)