UNIT III: DIGITAL EVIDENCE AND FIRST RESPONDER PROCEDURE

3.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- Know about the digital evidence and best evidence rule
- Understand Locard‘s principle
- Identify various types of digital evidence
- Learn digital evidence investigation procedure
- Prepare first responder toolkit
- Create a forensics tool testbed
- Document the forensics tool testbed and summary of the forensics tools
- Test the tools
- Recognise common mistakes of First Responder
- Identify various technical, administrative and legal issues of computer forensics
- Explain various types of investigations
- Classify techniques of digital forensics
- Understand volatile data
- Discover the importance of volatile data
- The list order of volatility of digital evidence

3.2 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. Some of the popular electronic devices which are potential digital evidence are HDD, CD/DVD media, backup tapes, USB drive, biometric scanner, digital camera, smartphone, smart card, PDA, etc.

The digital evidence is used to establish a credible link between the attacker, victim, and the crime scene. Some of the information stored in the victim‘s system can be potential digital evidence are IP address, system log-in & remote log-in details, browsing history, log files, emails, images, etc.

3.2.1 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 fibres 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. 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 evidence must follow the requirements of the Best Evidence Rule.

3.2.2 Best Evidence Rule

The best evidence rule, which had 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.

3.2.3 Characteristics of Digital Evidence

Following are essential characteristics of digital evidence:

- **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.
- **Reliability**: The evidence must be of indisputed 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 are 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 are taken to verify the accuracy of the program.

3.2.4 Stages in Digital Evidence Investigation Process

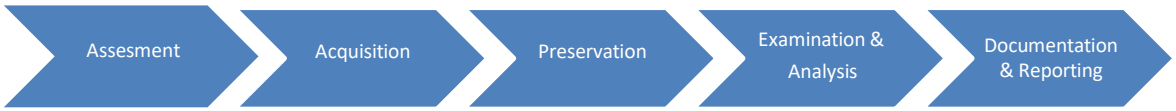

Figure 7: Stages in digital evidence investigation process

- **Assessment:** It is a key point of an investigation where the potentially relevant sources of information are identified. Without this stage, the chance to preserve and collect relevant material can be lost. This stage could also inform other activities including gathering information about possible passwords and attempts to attribute the sources to individuals as ownership of a device or a document can be a point of contention later on. In this phase, the investigator makes the assessment of the situation and consider many factors for making an assessment like whether the investigation is to be performed internally or an external agency is to be involved; Whether a search warrant is required. Also, some pre-search investigation needs to be performed like gathering information about the infrastructure and assets of the company; gathering information about the employees who are directly or indirectly involved with the case; gathering information about the security incident team and their key skills, etc. Also, the investigator needs to prepare and check the forensic investigation toolkit to conduct the investigation. He also needs to brief the investigating team about the search strategy; guidelines to be followed while investigation for eg. maintaining the logs of the events, chain of evidence and chain of custody. Chain of evidence is the process of documenting each and every step carried out during the investigation process to prove the authenticity of the digital evidence in the court.
- **Acquisition:** It is a process of gathering the data from wherever it resides. The most common collection approach is to create an image of a target device which can then be examined without altering the original exhibit. In a wider sense, this could also apply to aspects such as requesting and receiving communications data. Cloud storage is an increasing concern and whilst the forensic recovery of files stored remotely is possible, the subsequent analysis may require detailed knowledge of the application used. Complications can also arise from the data being held in a different jurisdiction. The goal of the investigator in this phase is to acquire the evidence in a forensically sound manner so that it is accepted by the court of law. It is good practice to record the physical attributes of every digital media like serial number, make, model, IP address and MAC address in case of network devices like NIC card, etc. and label them clearly so that they can easily be identified in the later course of action. It is also a sound practice

to gather information regarding the user login, password, etc. from the users and system administrators. Remember to use a forensically clean storage device to store the evidence. For making a copy of the digital evidence, use the bit-stream copy option, which acquires a bit-by-bit image of the original evidence and can be considered as equalized to original for the purpose of investigation. Don‘t forget to calculate checksum or hash value of the on original copy and duplicate copy. The same value of checksum and hash value will guarantee both the copies are technically the same for the purpose of investigation. It is important to note that logs from the servers, firewalls, routers, and stand-alone devices should also be recorded. Precautions regarding static electricity and magnetic fields should be taken while acquiring the digital evidence as it may alter data present in the digital devices. Therefore anti-static bags are used to store the digital evidence. The investigator must thoroughly examine the situation and if deemed essential, a further search warrant may be required to search third party data carriers like ISP. After the acquisition, the chain of custody, which the record of the history of the custody of the evidence is prepared and recorded.

- **Preservation:** Preserving the digital evidence is as important as acquiring it and the proper care must be taken to preserve the evidence so that data stored in digital storage devices can be used to investigate the case. It is advisable to take the photograph of the computer, cabling and the devices that are attached to the victim‘s computer, which are as important as a victim‘s computer. Also, label the seized cables along with the media. It is important to note that only forensically clean storage devices should be used to store the logs and other important digital information from the victim‘s system. Avoid dust, scratch, and exposure to a magnetic or electric field by using antistatic bags. Care must also be taken to save the digital evidence from exposure to wireless radiations by storing them in wireless hold bags. One must avoid the use of a USB drive or firmware drive as they change the state of the system. Intentional or accidental modification of data during the acquisition and preservation stage should be avoided and in case, it occurs, records the changes made in the system. Make the storage devices write-protect in order to accidentally overwrite the data. After bringing the digital media to the forensics lab, a proper chain of custody should be maintained and this evidence should be stored in a physically safe location with access control facility. Also, enough duplicate copies of the media should be made to carry out the investigation. *NEVER USE ORIGINAL MEDIA FOR CARRYING OUT INVESTIGATION*.
- **Examination and Analysis:** The purpose of the examination and analysis process is to make sense of the diverse digital data collected. A range of tools and techniques are used for this in an effort to ensure that as much data as possible is available for review. A lot of this data is of no relevance to the investigation but it may take considerable effort to get a good understanding of the relevance of material and to present it in an intelligible form. This data is examined and analysed to draw meaningful conclusions for the case. The first and the foremost thing to be kept in mind is the examination should be done by a trained person as mishandling of digital devices may corrupt the data. The examination requires the data to be extracted to the testbed for analysis. While examining, the goal of the investigator is to find out if files, folders, emails, partitions are

deleted and use recovery tools to restore them. Also, check if traces of data wiping software is present in the system so that special strategies could be used to recover data. If the files and documents are passwords protected then check whether the password for the same is available, else use password cracking software to crack the password and gain access to the files. The second important task after the examination is analysis. It is the process of putting the different pieces of evidence together to allow conclusions to be drawn and ideas tested. Some units have dedicated analytical support available which is a useful resource but many investigators don not have routine access to analysts so it can be helpful for the investigator to be able to conduct their own analysis. The primary information is gathered based on the interviews conducted with the witnesses at the crime site which is then used to frame the keywords to search the relevant document, files, etc. for investigation. The photographs, paper documents seized during the raid, etc are useful for analysis. The Investigator look for document properties, file signatures, browser history, chat history, emails, printer spools, cache files, registry files, timeframe, ownership information, etc. to find clues and missing link. Hash values are compared to find weather a duplicate or multiple copies of the file exist. If required, use decrypting software to decrypt the files if they are encrypted. The most important point in the analysis process is to keep the log of all the steps carried out during the examination & analysis phase including the details of keywords used, the list of search results returned using these keywords, searching methodology used while carrying out an investigation, etc.

- **Documentation and Reporting:** The examination and analysis can be conducted at a highly technical level but the information will ultimately need presenting to other individuals, either elsewhere in the investigation or the legal process, who are not so familiar with the detailed processes used and are more concerned with the usefulness of the information provided. Therefore documentation and reporting is a crucial part of the digital evidence investigation process. During this phase, a detailed report is performed which includes all the information related to the case like details of OS, software, versions, patched installed in the machine and a detailed note about the action taken during the forensic investigations along with the keywords searches, logs, cache, etc. It also documents any point that is contrary to the rules or to that which is normal or established. It also consists of the details of data analysing and the findings of the investigator.

3.3 FIRST RESPONDER TOOLKIT

The first responder is the person who first accesses the victim‘s computer. He must be prepared well to collect the pieces of evidence for the crime scene in a manner that is accepted by the court. 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:

1. Create a forensics tool testbed.
2. Document the forensics tool testbed.
3. Document the summery of the forensics tools.
4. Test the tools.

The above four steps are described in details in the following section.