2 Introduction to Digital Forensics and Digital Evidences

LEARNING OBJECTIVES

After reading this chapter, you will be able to:

- Understand the concept of digital forensic and its effect on the digital world.
- Interpret and apply various digital forensic process models.
- Understand the rules and regulations in digital forensics.
- Understand the concept of digital evidences and its role.
- Apply evidence-handling procedure to both obtained validated evidence.
- Identify the different challenges in evidence handling.

It requires a very unusual mind to undertake the analysis of the obvious.

— Alfred North Whitehead

2.1 Introduction to Digital Forensic

Forensic science is a well-established science that plays a critical role in criminal justice systems. The origin of the word "forensic" can be traced back to the Latin word "forensis", which means open court. Forensic science is often referred to as forensics. Forensic science is applied in both criminal and civil actions. Therefore, effectively forensics means legal or related to courts.

Digital forensics is also referred to as digital forensic science, a branch of computer forensic science that includes the restoration and inspection of material detected in digital devices, often in relation to a cybercrime. Information and Communications Technology (ICT) working environments face the challenge of prolonged computer use for activities that are not work-related. User activity portrayals may consist of browsing the Internet for one's own purpose and utilizing online search engines for work-related information. However, browsing sessions are not specific to only the above-mentioned activities.

With the emergence of ICT, there have been simultaneous advancements in social networking, mobile technology, cloud computing, and storage solutions that have increased the information flow within organizations. This has weakened the security of organizational data. The increasing activity in ICT-focused environments has also led to an increase in the misuse of computer and network. A common employee can use simple password cracking tools to gain access to managerial account information, for fraud and theft of company resources as many open source tools are available to perform illegal activities.

Scanned by CamScanner

Increased computer and network misuse have led to an increase in computer-related investigations. A typical investigation includes certain hypothesis or observable phenomenon that is verified by some proof. These developments in investigation have led to auditing being the key in answering questions related to user activity and cybercrime.

The field of digital forensics has made some rapid developments over the past few years due to the advancement in tools and systems that allow ordinary computer users to be more proficient in performing difficult audit tasks. Many literature and internet searches are available that guide a trivial and easy tutorial user on how to perform simple tasks aimed at gaining access to any computer. This has enabled the ordinary computer user to access all types of information, such as copied music, pornography, confidential documents, illegal software and so on. Thus, there is an increased demand in computer security mechanisms in an effort to control such activities and a growing need for forensic tools to gather accurate digital evidence. According to Beebe, the lack of digital forensic standardization and process results in limited prosecution that is not acceptable in the court of law.

Numerous forensic tools are freely available, creating a misconception among the common man that anyone can conduct a computer forensic investigation. The forensic tools used have various features that facilitate digital forensic investigations (DFIs). In a court of law, the process followed in gathering the digital evidence and the digital evidence itself is important. Unfortunately, the court proceedings focus on scrutinizing the validity of the process followed in evidence handling before considering its value.

Numerous procedures have been proposed for the collection of digital forensic evidence. Committees such as the Digital Forensic Research Workshop Group (DFRWS) and the American Society of Digital Forensics and e Discovery (ASDFED) have proposed processes to be followed in the collection of digital evidence. From this, it follows that there is no standard forensic process in place that can be followed by digital forensic investigators. It would be a serious mistake for a forensic investigator to ignore the procedure of evidence collection in cases where the evidence aids in proving the case and leaves no doubt in the minds of those having to decide on the matter. Where evidence is presented without proof of thorough procedure, the defence may question the forensic procedure followed to collect the digital evidence. The famous American court case of Simpson is an example where the forensic process was scrutinized by the defence. In this case, the crime scene evidence was collected. However, a robust evidence collection process was not followed, hence, the evidence was invalidated by the defence. Tools such as Encase have been accepted as a reliable solution in computer crime investigations. Both the process followed when using Encase and the resulting digital evidence have been accepted as reliable. Other tools have also been used successfully, such as FTK and Sleuth Kit. Some are commercially available while others are open source. Many of these tools have been validated and accepted as reliable by the American judiciary. However, the evidence collection process and the digital evidence presentation are vital in any successful prosecution.

Digital forensics can be defined as follows:

> Digital Forensic is a series of steps to uncover and analyze electronic data through scientific method. The major goal of the process is to duplicate original data and preserve original evidence then performing the series of the investigation by collecting, identifying and validating the digital information for the purpose of reconstructing past events.

2.2 Need of Digital Forensic

Computer forensics is the process of using the latest knowledge of science and technology with computer sciences to collect, analyze, and present proofs to the criminals or civil courts. Network administrator and security staff administer and manage networks and information systems should have complete knowledge of computer forensics. The meaning of the word "forensics" is "to bring to the court".

Scanned by CamScanner

It is necessary for network administrator and security staff of networked organizations to practice computer forensics and should have knowledge of laws, because rate of cyber crimes is increasing greatly.

If your network is attacked and intruder is caught, then good knowledge about computer forensics will help to provide evidence and prosecute the case in the court.

There are many risks if you practice computer forensics badly. If you do not take it in account, then vital evidence might be destroyed. New laws are being developed to protect customers' data; but, if certain kind of data is not properly protected, then many liabilities can be assigned to the organization. As organizations are increasing in number and the risk of hackers and contractors is also increasing, so they have developed their own security systems. Organizations have developed security devices for their network like intrusions detection systems (IDS), proxies, firewalls which report on the security status of network of an organization. So, technically, the major goal of computer forensics is to recognize, gather, protect and examine data in such a way that protects the integrity of the collected evidence to use it efficiently and effectively in a case.

2.3 Rules of Computer/Digital Forensic

While performing a DFI, the investigator should go by the following rules:

Rule 1. An examination should never be performed on the original media.

Rule 2. A copy is made onto forensically sterile media. New media should always be used if available.

Rule 3. The copy of the evidence must be an exact, bit-by-bit copy (Sometimes referred to as a bit-stream copy).

Rule 4. The computer and the data on it must be protected during the acquisition of the media to ensure that the data is not modified (Use a write blocking device when possible).

Rule 5. The examination must be conducted in such a way as to prevent any modification of the evidence.

Rule 6. The chain of the custody of all evidence must be clearly maintained to provide an audit log of whom might have accessed the evidence and at what time.

2.4 Types of Digital Forensics

Digital forensics is a constantly evolving scientific field with many subdisciplines. Some of these subdisciplines are as follows:

1. **Computer Forensics** – the identification, preservation, collection, analysis and reporting on evidence found on computers, laptops, and storage media in support of investigations and legal proceedings. The purpose of computer forensics is to obtain evidence from various computer systems, storage mediums, or electronic documents. Throughout the course of our investigations, we can obtain a wide range of information, including system and file transfer logs; internet browsing history; email and text communication logs; hidden, deleted, temporary, and password-protected files; sensitive documents and spreadsheets; and many more.
2. **Network Forensics** – the monitoring, capture, storing, and analysis of network activities or events in order to discover the source of security attacks, intrusions or other problem incidents, that is, worms, virus, or malware attacks, abnormal network traffic and security breaches. The purpose of network forensics is to monitor and analyze computer network traffic, including LAN/WAN and internet traffic, with the aim of gathering information, collecting evidence, or detecting and determining the extent of intrusions and the amount of compromised data.

Scanned by CamScanner

3. **Mobile Devices Forensics** – the recovery of electronic evidence from mobile phones, smartphones, SIM cards, PDAs, GPS devices, tablets, and game consoles. Mobile device forensics involves the recovery of digital evidence or data from mobile devices. This can include call and communications data, such as call logs, test messages, and in-app communication via WhatsApp, WeChat, etc., as well as location information via inbuilt GPS or cell site logs.
4. **Digital Image Forensics** – the extraction and analysis of digitally acquired photographic images to validate their authenticity by recovering the metadata of the image file to ascertain its history.
5. **Digital Video/Audio Forensics** – the collection, analysis, and evaluation of sound and video recordings. The science is the establishment of authenticity as to whether a recording is original and whether it has been tampered with, either maliciously or accidentally.
6. Memory forensics – the recovery of evidence from the RAM of a running computer, also called **live acquisition**.

In practice, there are exceptions to blur this classification, because the grouping by the provider is dictated by staff skill sets, contractual requirements, lab space, etc. For example:

1. Tablets or smart phones without SIM cards could be considered computers.
2. Memory cards (and other removable storage media) are often found in smart phones and tablets, so they could be considered under mobile forensics or computer forensics.
3. Tablets with keyboards could be considered laptops and fit under computer or mobile forensics.

The science of digital forensics has a seemingly limitless future and as technology advances, the field will continue to expand as new types of digital data are created by new devices logging people's activity. Although digital forensics began outside the mainstream of forensic science, it is now fully absorbed and recognized as a branch of forensic science.

2.5 Ethical Issues

"Ethics" is derived from the ancient Greek word *ethikos*, meaning "moral, showing moral character". Ethics in digital forensics field can be defined as a set of moral principles that regulate the use of computers; some common drawbacks of computer forensics include intellectual property resources, privacy concerns, and the impact of computers on the society. To effectively spot ethical problems, an examiner must be familiar with the law and professional norms governing the cyber forensics discipline, and this familiarity is one of several presumptions incorporated into the code of ethics.

With this perspective in mind, ethical decision-making in digital forensics work comprises of one or more of the following:

1. Honesty toward the investigation.
2. Prudence means carefully handling the digital evidences.
3. Compliance with the law and professional norms.

2.5.1 General Ethics Norms for Investigator in Digital Forensic Field

Computer forensics is an integral part of the widely expanding field of digital forensics, as with any investigative field there comes a time when ethical issues will arise. During the research in the digital forensic field, ethics or rights comes first.

Hence, before starting the investigation in the digital forensic field, the investigator should satisfy the following points.

Scanned by CamScanner

1. Should contribute to the society and human being.
2. Should avoid harm to others.
3. Should be honest and trustworthy.
4. Should be fair and take action not to discriminate.
5. Should honor property rights, including copyrights and patents.
6. Should give proper credit to intellectual property.
7. Should respect the privacy of others.
8. Should honor confidentiality.

2.5.2 *Unethical Norms for Digital Forensic Investigation*

The investigator should not:

1. Uphold any relevant evidence.
2. Declare any confidential matters or knowledge learned in an investigation without an order from a court of competent jurisdiction or without the client's consent.
3. Express an opinion on the guilt or innocence belonging to any party.
4. Engage or involve in any kind of unethical or illegal conduct.
5. Deliberately or knowingly undertake an assignment beyond his or her capability.
6. Distort or falsify education, training or credentials.
7. Display bias or prejudice in findings or observations.
8. Exceed or outpace authorization in conducting examinations.

2.6 Digital Forensic Investigations

Digital investigations, DFIs, forensic examination, and forensic investigations have been used to describe an investigation where a digital device forms part of the incident. For the purposes of this study, the term "digital forensic investigation" (DFI) is used. The terms will, however, be used interchangeably in this section to reflect the opinions of other authors. The successful outcome of a DFI is the presentation of digital evidence. A DFI is conducted by an appropriately certified investigator.

A DFI is thus a special type of investigation wherever scientific procedures and techniques used can permit the results, that is, the digital proof, to be allowable in a court of law. The results of a DFI should have a legal basis. Proof cannot be directly read, and a few tools are employed to look at the state of the information. One in every tool to watch the state of digital knowledge is indirect knowledge observation. This is similar to being told concerning one thing rather than seeing it for you, formally referred to as rumour within the rules of proof. The burden you attribute to the evidentiary worth relies on the extent to which the tool is trustworthy.

Digital forensic investigation or DFI is a special type of investigation where the scientific procedures and techniques used will be allowed to view the results – digital evidence – to be admissible in a court of law.

2.7 Introduction to Digital Evidences

The field of computer security includes events that provide a successful courtroom experience, which are both worthwhile and satisfactory. Investigation of a computer security incident leads to a legal proceeding, such as court proceeding, where the digital evidence and documents obtained are likely used as *exhibits* in the trial.

Scanned by CamScanner

To meet the requirements of the judging body and to withstand or face any challenges, it is essential to follow the evidence-handling procedures. Also, it is necessary to ensure that the evidence-handling procedures chosen are not difficult to implement at your organization as this can sometimes become an overhead for an organization. In this chapter, we will discuss the collection, handling, and storage of information in an appropriate manner. We will also explain the effective and efficient evidence-handling procedures along with the guidelines for implementing these procedures in your organizations.

While investigating a computer security incident, we are sometimes unsure and indecisive whether an item (viz., a chip, floppy disk, etc.) should be considered as an evidence or an attachment or an addendum. Relevant evidence is defined as "An information which has a positive impact on the action occurred, such as the information supporting an incident."

Digital evidence is any information or data of value to an investigation that is stored on, received by, or transmitted by an electronic device. Text messages, emails, pictures and videos, and internet searches are some of the most common types of digital evidence.

Evidence can be stated as *any information that can be confident or trusted* and can prove something related to a case in trial, that is, indicating that a certain substance or condition is present. It is safe to use such information as evidence during an investigation. Many materials or objects can help us prove our case, such as document, electronic media, electronic files, printouts, or other objects obtained during an investigation (Fig. 2.1). They can be treated as evidence or proof and handled according to your organization's evidence-handling process.

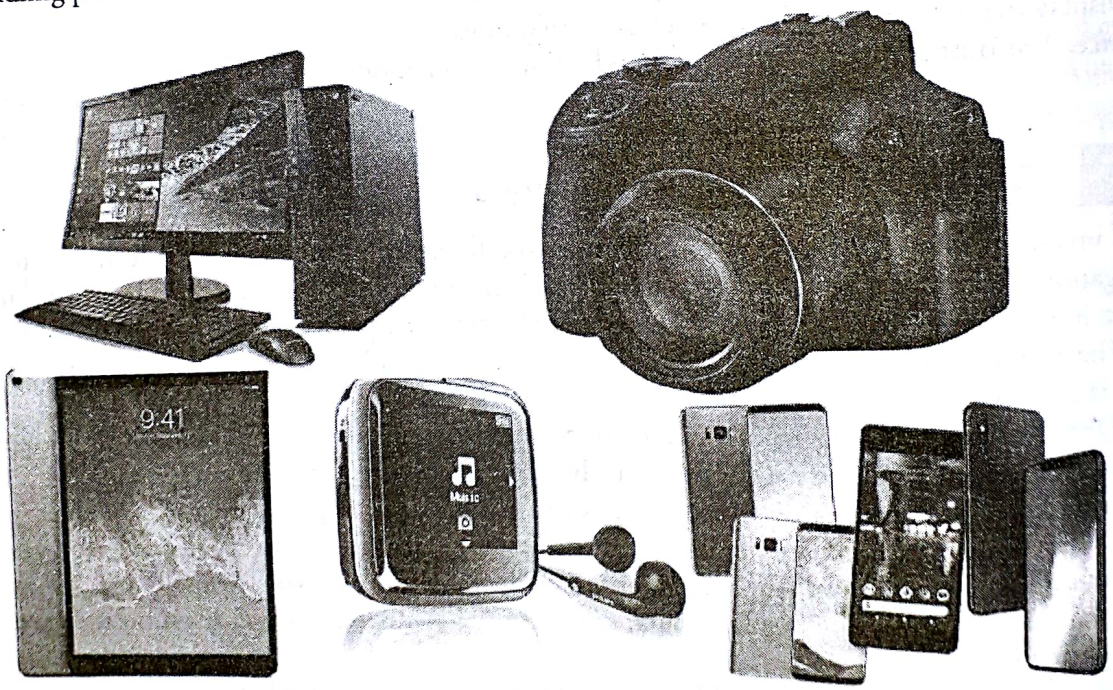

Figure 2.1 Examples of digital devices.

2.7.1 The Best Evidence Rule

The best evidence rule is that the original or true writing or recording must be confessed in court to prove its contents without any expectations. In the best evidence rule, an original copy of the document is considered as superior evidence. One of the rules states that if an evidence is readable by sight or reflects the data

Scanned by CamScanner

accurately, such as any printout or data stored in a computer or similar devices or any other output, it is considered as "original". It states that multiple copies of electronic files may be a part of the "original" or equivalent to the "original". The collected electronic evidence is mostly transferred to different media. Hence, many computer security professionals are dependent on this rule.

We define *best evidence* as the most complete copy or a copy which includes all necessary parts of evidence, which is closely related to the original evidence. One of the best evidences is having the original evidence media. Let us say a client has a copy of the original evidence media. Then, it is considered as the best evidence. We treat forensic duplication by considering it as the best evidence. Therefore, when we say "best evidence", it refers to the evidence we have in our power.

2.7.2 Original Evidence

Sometimes the procedure adopted to deal with a situation or case takes it outside the control of the client/victim. We also assume that a case with proper diligence or a case with persistent work will end up in a judicial proceeding, and we will handle the evidences accordingly. If criminal or civil proceedings (proceedings other than criminal proceeding in a court) are a possibility, then we often persistently push the client/victim to allow us to handover all the original evidences, since we have evidence-handling procedures in place.

For our purpose, we define *original evidence* as the truth or real(original) copy of the evidence media which is given by a client/victim. We define best incidence as the most complete copy, which includes all the necessary parts of the evidence that are closely related to the original evidence. It is also called as duplication of evidence media. There should be an evidence protector which will store either the best evidence or original evidence for every investigation in the evidence safe.

2.8 Rules of Digital Evidence

Rule of evidence is also called as *law of evidence.* It surrounds the rules and legal principles that govern all the proof of facts. This rule helps us to determine what evidence must or must not be considered by a trier of fact. The rule of evidence is also concerned with the amount, quality, and type of proof which helps us to prove in a litigation. The rules may vary according to the criminal court, civil court, etc. The rules must be:

1. **Admissible:** The evidence must be usable in the court.
2. **Authentic:** The evidence should act positively to an incident.
3. **Complete:** A proof that covers all perspectives.
4. **Reliable:** There ought to be no doubt about the reality of the specialist's decision.
5. **Believable:** The evidence should be understandable and believable to the jury.

Rule 103: Rule of evidence

1. Maintaining a claim of error.
2. No renewal of objection or proof.
3. Aim an offer of proof.
4. Plain error taken as notice.

Evidence collection should always be performed to ensure that it will withstand legal proceedings. Key criteria for handling such evidence are outlined as follows:

1. The proper protocol should be followed for acquisition of the evidence irrespective of whether it physical or digital. Gentle handling should be exercised for those situations where the device may be damaged (e.g., dropped or wet).

Scanned by CamScanner

2. Special handling may be required for some situations. For example, when the device is actively destroying data through disk formatting, it may need to be shut down immediately to preserve the evidence. On the other hand, in some situations, it would not be appropriate to shut down the device so that the digital forensics expert can examine the device's temporary memory.
3. All artifacts, physical and/or digital should be collected, retained, and transferred using a preserved chain of custody.
4. All materials should be date and time stamped, identifying who collected the evidence and the location it is being transported to after initial collection.
5. Proper logs should be maintained when transferring possession.
6. When storing evidence, suitable access controls should be implemented and tracked to certify the evidence has only been accessed by authorized individual.

2.9 Characteristics of Digital Evidence

This section provides a few hints of the essence and characteristics of digital evidence. These characteristics can help and challenge investigators during an investigation.

2.9.1 *Locard's Exchange Principle*

According to Edmond Locard's principle, when two items make contact, there will be an interchange. The Locard principle is often cited in forensic sciences and is relevant in digital forensics investigations.

When an incident takes place, a criminal will leave a hint evidence at the scene and remove a hint evidence from the scene. This alteration is known as the Locard exchange principle. Many methods have been suggested in conventional forensic sciences to strongly prosecute criminals. Techniques used consist of blood analysis, DNA matching, and fingerprint verification. These techniques are used to certify the existence of a suspected person at a physical scene. Based on this principle, Culley suggests that where there is a communication with a computer system, clues will be left.

2.9.2 *Digital Stream of Bits*

Cohen refers to digital evidence as a bag of bits, which in turn can be arranged in arrays to display the information. The information in continuous bits will rarely make sense, and tools are needed to show these structures logically so that it is readable.

The circumstances in which digital evidence are found also helps the investigator during the inspection. Metadata is used to portray data more specifically and is helpful in determining the background of digital evidence.

2.10 Types of Evidence

There are many types of evidence, each with their own specific or unique characteristics. Some of the major types of evidence are as follows:

1. Illustrative evidence
2. Electronic evidence
3. Documented evidence

Scanned by CamScanner

4. Explainable evidence
5. Substantial evidence
6. Testimonial

2.10.1 Illustrative Evidence

Illustrative evidence is also called as demonstrative evidence. It is generally a representation of an object which is a common form of proof. For example, photographs, videos, sound recordings, X-rays, maps, drawing, graphs, charts, simulations, sculptures, and models.

2.10.2 Electronic Evidence

Electronic evidence is nothing but digital evidence. As we know, the use of digital evidence in trials has greatly increased. The evidences or proof that can be obtained from an electronic source is called as *digital evidence* (viz., emails, hard drives, word-processing documents, instant message logs, ATM transactions, cell phone logs, etc.)

2.10.3 Documented Evidence

Documented evidence is similar to demonstrative evidence. However, in documentary evidence, the proof is presented in writing (viz., contracts, wills, invoices, etc.). It can include any number of medias. Such documentation can be recorded and stored (viz., photographs, recordings, films, printed emails, etc.).

2.10.4 Explainable Evidence (Exculpatory)

This type of evidence is typically used in criminal cases in which it supports the dependent, either partially or totally removing their guilt in the case. It is also referred to as *exculpatory evidence*.

2.10.5 Substantial Evidence

A proof that is introduced in the form of a physical object, whether whole or in part, is referred to as *substantial evidence*. It is also called as *physical evidence*. Such evidence might consist of dried blood, fingerprints, and DNA samples, casts of footprints, or tires at the scene of crime.

2.10.6 Testimonial

It is a kind of evidence spoken by a spectator under oath, or written evidence given under oath by an official declaration, that is, affidavit. This is one of the common forms of evidence in the system.

2.11 Challenges in Evidence Handling

While responding to a computer security incident, a failure to adequately document is one of the most common mistakes made by computer security professionals. Analytical data might never be collected, critical data may be lost, or data's origin and meaning may become unknown. As there are many evidences collected, the evidence collected based on technical complexity is the fact that the properly retrieved evidence requires a paper trial. Such documentations give an impression of having a certain quality against the natural instincts of the technical practical knowledge of individuals, who often investigate computer security incidents.

Scanned by CamScanner

The challenges faced in evidence handling must be properly understood by all investigators. Investigators should also understand how to meet these challenges. Therefore, it is essential for every organization to have formal evidence-handling procedures that support computer security investigation. The most difficult task for an evidence handler is to authenticate the collected evidence at the judicial proceeding. Maintaining the chain of custody is also necessary. You must have both power and skill to validate your evidence.

2.11.1 Authentication of Evidence

The laws of many state jurisdictions define data as "*written-works*" and "*record-keeping*". Before introducing them as evidence, documents and recorded material must be authenticated.

The evidences that are collected by any person/investigator should be collected using authenticate methods and techniques because during court proceedings these will become major evidences to prove the crime. In other words, for providing a piece of evidence of the testimony, it is necessary to have an authenticated evidence by a spectator who has a personal knowledge to its origin.

For an evidence to be admissible, it is necessary that it should be authenticated, otherwise the information cannot be presented to the judging body. The matter of record is that the evidence collected by any person should meet the demand of authentication. The evidences collected must have some sort of internal documentation that records the manner of collected information.

2.11.2 Chain of Custody

Maintaining the chain of custody means that the evidences collected should not be accessed by any unauthorized individual and must be stored in a tamper-proof manner. For each item obtained, there must be a complete chain of custody record. Chain of custody is nothing but the requirement that you may be able to trace the location of evidence from the moment it was collected to the moment it was presented in a judicial proceeding (Fig. 2.2).

Figure 2.2 Digital evidence should be 100% authentic.

To meet the requirements of chain of custody (Fig. 2.3), evidences are stored in a secure place by police departments and federal law enforcement agencies, which have a property departments. As per the experts and law enforcement officers, evidences are "checked-out" whenever they need to be reviewed and "checked-in" whenever they are returned back to storage.

Scanned by CamScanner

The challenge of chain of custody requirements in any organization is maintaining positive control (the evidence which you owned or have must be kept in your sight at all times) of all the collected best evidence until the evidences are carried or shipped to evidence custodians for proper storage. As evidences should not be accessible to anyone other than the appointed evidence custodian, the best evidence of your organization must be stored within a safe or storage room. "Evidence safe" is nothing but the storage area. The evidence custodians must control all the access to the evidence safe.

CHAIN OF CUSTODY

Received From: _____
Received By: _____
Date: _____ Time: _____ am/pm

Received From: _____
Received By: _____
Date: _____ Time: _____ am/pm

Received From: _____
Received By: _____
Date: _____ Time: _____ am/pm

Received From: _____
Received By: _____
Date: _____ Time: _____ am/pm

Received From: _____
Received By: _____
Date: _____ Time: _____ am/pm

Received From: _____
Received By: _____
Date: _____ Time: _____ am/pm

Figure 2.3 Chain of custody.

2.11.3 *Evidence Validation*

The challenge is to ensure that providing or obtaining the data that you have collected is similar to the data provided or presented in the court. Several years pass between the collection of evidence and the production of evidence at a judiciary proceeding, which is very common. To meet the challenge of validation, it is necessary to ensure that the original media matches the forensic duplication by using MD5 hashes. The evidence for every file is nothing but the MD5 hash values that are generated for every file that contributes to the case.

The verify function within the Encase application can be used while duplicating a hard drive with Encase. To perform a forensic duplication using dd, you must record a MD5 hash for both the original evidence media and binary files or the files which compose the forensic duplication.

Note: Evidence collection calculated by MD5 after 6 months may not be helpful. MD5 hashes should be performed when the evidence is obtained.

Scanned by CamScanner

Summary

In this chapter, we discussed numerous digital forensic models and highlighted the phases in each model. Each DFPM uses particular series of phases. In digital forensic field, there are many forensic approaches which can be used by the investigator to investigate the cases. Digital evidences can be found in the form of information from computer documents, emails, instant messages, internet history, or text from various electronic devices, and it is very effective. Computer is treated as a primary source of evidence in almost all cases. Digital evidence plays a vital role in digital forensic investigation.

Key Terms

- **Acquisition:** The process of creating a duplicate copy of digital media for the purpose of examining it.
- **Computational forensics:** Computational forensics are digital forensics with the use of artificial intelligence.
- **Digital media:** Used within the fields to refer to the physical medium (viz., a hard drive) or data-storage device.
- **E-discovery or Discovery:** A common acronym for electronic discovery.
- **Exhibit:** Digital media seized for investigation is usually referred to as an "exhibit".
- **Hashing:** Within the field, "hashing" refers to the use of hash functions (e.g., CRC, SHA1 or MD5) to verify that an "image" is identical to the source media.
- **Image:** A duplicate copy of some digital media created as part of the forensic process.
- **Imaging:** Synonym of "acquisition".
- **Live analysis:** Analysis of a piece of digital media from within itself; often used to acquire data from RAM where this would be lost upon shutting down the device.
- **Slack space:** The unused space at the end of a file in a file system that uses fixed-size clusters (if the file is smaller than the fixed block size, then the unused space is simply left). Often contains deleted information from previous uses of the block.
- **Steganography:** The word steganography comes from the Greek name "steganos" (hidden or secret) and "graphy" (writing or drawing) and literally means hidden writing. Steganography uses techniques to communicate information in a way that is hidden.
- **Verification:** A term used to refer to the hashing of both source media and acquired image to verify the accuracy of the copy.
- **Hacking:** Modifying a computer in a way which was not originally intended to benefit the hacker's goals.
- **Denial-of-service attack:** An attempt to prevent legitimate users of a computer system from having access to that system's information or services.
- **Metadata:** Data about data. It can be embedded within files or stored externally in a separate file and may contain information about the file's author, format, creation date, and so on.
- **Write blocker:** A hardware device or software application which prevents any data from being modified or added to the storage medium being examined.
- **Bit copy:** "Bit" is a contraction of the term "binary digit" and is the fundamental unit of computing. A bit copy refers to a sequential copy of every bit on a storage medium, which includes areas of the medium "invisible" to the user.
- **RAM:** Random Access Memory. RAM is a computer's temporary workspace and is volatile, which means its contents are lost when the computer is powered off.
- **Key-logging:** The recording of keyboard input giving the ability to read a user's typed passwords, emails, and other confidential information.
- **Data:** Information in analog or digital form that can be transmitted or processed.
- **Data extraction:** A process that identifies and recovers information that may not be immediately apparent.

Scanned by CamScanner

- **Encryption:** A procedure that converts plain text into symbols to prevent anyone but the intended recipient from understanding the message.
- **File format:** The structure by which data is organized in a file.
- **Forensic wipe:** A verifiable procedure for sanitizing a defined area of digital media by overwriting each byte with a known value; this process prevents cross-contamination of data.
- **Hash or hash value:** Numerical values that represent a string of text (search term), generated by hashing functions (algorithms). Hash values are used to query large sums of data such as databases or hard drives for specific terms. In forensics, hash values are also used to substantiate the integrity of digital evidence and/or for inclusion and exclusion comparisons against known value sets.
- **Log file:** A record of actions, events, and related data.
- **Media:** Objects on which data can be stored. Includes hard drives, thumb drives, CD/DVD, floppy discs, SIM cards from mobile devices, memory cards for cameras, etc.
- **Metadata:** Data, frequently embedded within a file, that describes a file or directory, and can include the locations where the content is stored, dates and times, application-specific information, and permissions (e.g., email headers and website source code contain metadata).
- **Partition:** User-defined section of electronic media. Partitions can be used to separate and hide information on a hard drive.
- **Source code:** The instructions written in a programming language used to build a computer program.
- **Work copy:** A copy or duplicate of a recording or data that can be used for subsequent processing and/or analysis. It is also called an image.
- **Write block/write protect:** Hardware and/or software methods of preventing modification of content on a media storage unit such as a CD or thumb drive.
- **Acquisition of digital evidence:** Acquisition of digital evidence begins when information and/or physical items are collected or stored for examination. The term "evidence" implies that the collection of evidence is recognized by the courts. The process of collecting is also assumed to be a legal process and is appropriate for rules of evidence in that locality. A data object or physical item only becomes evidence when so deemed by a law enforcement official or designee.
- **Data objects:** Objects or information of potential probative value that are associated with physical items. Data objects may occur in different formats without altering the original information.
- **Digital Evidence:** Information of probative value stored or transmitted in digital form.
- **Physical items:** Items on which data objects or information may be stored and/or through which data objects are transferred.
- **Original digital evidence:** Physical items and data objects associated with such items at the time of acquisition or seizure.
- **Duplicate digital evidence:** An accurate digital reproduction of all data objects contained on an original physical item.
- **Copy:** An accurate reproduction of information contained on an original physical item, independent of the original physical item.

Review Questions

1. What is digital forensics?
2. Explain the process of digital forensics.
3. What ethical issues are involved in the digital forensic process?
4. Explain the history of digital forensic field.
5. What is an evidence-handling procedure?
6. What are the challenges in evidence handling?
7. What is digital evidence?
8. Explain the various types of evidence. Explain the rules of evidence.
9. Describe the term *metadata*.

Scanned by CamScanner