Digital and Cyber Forensics: A Contemporary Evolution in Forensic Sciences

11

Sameer Saharan and Bhuvnesh Yadav

Abstract

Digitalization has a revolutionary impact on human society as it has provided easy access to information and increased interpersonal connectivity, ease of data storage, and businesses. Most of the personal, financial, and official transactions are now conducted digitally. The security of the online/offline data becomes a necessity as these data are now more prone to cyberattacks and breach of information. Criminals are taking advantages of any loophole in the security of these data, and that has resulted in skyrocketed cybercrimes. Both preventive and responsive measures are required to nullify the cyber or digital crimes. The conventional forensic investigations are not sufficient to investigate such crimes, and therefore, new contemporary branch of forensic evolved, that is, utilizing principles of forensic investigation for the digital data. This chapter will explain the development and role of digital and cyber forensics in cybercrime investigations. The chapter also focuses on the processes and techniques involved in prevention and investigation of cybercrimes.

Keywords

Digital forensics · Cyber forensics · Cybercrimes · Data acquisition

S. Saharan · B. Yadav (✉)
Department of Chemistry, Biochemistry and Forensic Science, Amity School of Applied Sciences, Amity University Haryana, Gurugram, Haryana, India

J. Singh, N. R. Sharma (eds.), *Crime Scene Management within Forensic Science*,
https://doi.org/10.1007/978-981-16-6683-4_11

11.1 Introduction

With advancement of the digital technology, computers have become ubiquitous as a processing and controlling device. The information that was processed manually and preserved as record on paper has been gradually shifted to the digital processing. Personal profile, business transactions, processes, and technical details are now stored in computers. Easy access to high- speed Internet, easy operation, and worldwide connectivity have shown efflorescence in the digital processing of data. The information which was initially stored and authenticated by the signatures and thumbprints on the security documents is now identified and authenticated by digital signatures. As the moon has a dark side, so is with the digital world. The information which is being created, stored, and transferred by digital means have security threat. The breach of cyber privacy can lead to significant loss of valuable information that can be misused by the hackers, resulting in significant financial and professional setback to the industries and persons. The misuse of digital platform increased manifolds in the last decade, resulting in cybercrimes like leakage of personal information, ransomwares, defamation, riots, and threats to national security. In 2020, nearly 445 million cyberattacks were reported which was double of the previous year. It shows the necessity of tracing cyber criminals [1]. Cybercrime cannot be prevented by traditional methods of crime investigations; therefore, new approach, i.e., cyber forensics, came into existence developed which works on the digital footprint of web search history, messages, emails, documents, etc. Cyber forensics is based on the retrieval of the entire information by following these digital footprints [2]. Locard's exchange principle also applies in digital and cyber forensics. Just as criminals leave fingerprints, blood, hair, etc. on the crime scene, here, also, criminals leave their traces in the form of registry keys and log files, which can be tracked with the help of some tools in digital and cyber forensics [3]. Digital and cyber forensics has gradually attained its position as that of other branches of forensic science like fingerprint, toxicology, biology, etc.

11.1.1 Digital Forensics and Cyber Forensics

Until the late 1990s, digital forensics was referred to as "computer forensics." The terms "digital forensics" and "cyber forensics" are used interchangeably; however, there is a minor difference between these two terms. Digital forensics deals with all digital electronic devices, e.g., cell phone, digital networks, hard drives, flash drives, digital cameras, electronic files such as image file, and email [4]. Technically, digital forensics is the science of identifying, extracting, analyzing, and presenting digital evidence stored in digital devices, whereas cyber forensics is the process of gathering and documenting evidence from a computer to the computing device in a manner that can be shown to a court using investigation and analysis technique. Digital and cyber forensics have the same goal, i.e., to determine whether a tool was used for illegal purposes (illegal data breach by hacking computers) or not and, if yes, then to trace the culprit. Digital forensics is not only confined to retrieval of data

but also playing highly significant role in data breach analysis. The following are the subgroups of digital forensics that deal with different digital devices [5]:

(a) Computer forensics (deals with computers, its embedded systems, and static memory).
(b) Mobile device forensics (deals with data recovery from smartphones/mobile devices).
(c) Forensic data analysis (deals with tracking online transactions).
(d) Network forensics (deals with monitoring and analysis of network traffic for collection of evidence).

11.1.2 History of Digital Forensics

The demand for computer forensics came into existence with the beginning of the information age/digital era, which was characterized by greater information production, transmission, consumption, and reliance. In the mid-twentieth century, modern computers were largely owned and operated by huge firms, such as universities and government agencies. Theft of computers and computer components was the major focus of standard computer crime investigations. Such crimes were easily solved by the conventional forensic strategies of trace evidence collection and analysis. With introduction of personal computers in the mid-1970s, old crimes with new tactics arose, and computer crimes were no longer limited to computer or component theft. Newer methods of computer crimes were evolved, particularly for financial crimes (fraud, embezzlement), majority of which were done by persons who have access to private information about the corporation's operations [6].

By the late 1970s, computer crimes became a major concern for national and international firms, and issue was raised in the conference held in France (1976) entitled "Council of Europe Conference on Criminological Aspects of Economic Crime." Many types of cybercrimes were described during that conference. The Federal Computer Systems Protection Act of 1977 was introduced as the first federal cybercrime law in the United States. Though the act was not accepted, it was recognized for drawing attention to the importance of cybercrime law [7].

The digital revolution initiated in the 1980s, when IBM offered PCs for the general population. These systems were quite powerful, but they only had a few programs. The FBI Magnetic Media Program (1984), which later known as Computer Analysis Response Team (CART), was the first known effort to tackle cybercrime. Subsequently, Electronic Crimes Special Agent Program (ECSAP), Seized Computer Evidence Recovery Specialists (SCERS), and Defense Computer Forensic Laboratory (DCFL) came into existence. Access Data was founded in 1987 and is widely regarded as a pioneer in the field of cyber forensics. FBI hosted the International Conference on Computer Evidence (IOCE) in 1993 and 1995, which was attended by delegates from 26 countries, and a jointly decision was taken about sharing experiences and aid regarding cybercrime. The G8 countries assigned the

task of creating international guidelines, protocols, and procedures for digital evidence to IOCE in 1998 [6, 8].

The Scientific Working Group on Digital Evidence (SWGDE) was constituted with law enforcement officers, forensic laboratory scientists, and employees from private companies who collaborated to produce cross-disciplinary digital evidence guidelines which were published as "Best Practices for Computer Forensics" in 2002. At the Budapest Convention on Cybercrime (2004), an international treaty was formed that recognized crimes perpetrated on computer systems and networks via the Internet, such as copyright infringement, child pornography, and fraud [9].

In 2005, ISO released the General Guidelines for Testing and Calibration Laboratories (ISO 17025). Cyber forensic tools quickly gained attraction; EnCase by Guidance Software and FTK by Access Data led the commercial tools category, achieving significant success and legal acceptability [8].

In 2006, US Courts approved the new Rules of Civil Procedure that classified digital information as a new type of evidence and established a mandatory method for dealing with digital evidence, known as electronic discovery or "eDiscovery." In 2007, the FBI stated in Congressional testimony that its Computer Analysis and Response Team (CART) analyzed over 2.5 petabytes of evidence. The Forensic Science Education Programs Accreditation Commission (FEPAC) and American Society of Testing Materials (ASTM) are stepping toward accrediting US academic programs in digital forensics [6].

After all those efforts, digital forensics is growing with the advancement of technology. There are new and advanced tools in the market which make tasks very easy.

11.1.3 Digital Forensics Standards and Guidelines

The following are the most common organizations which play an important role in digital forensics.

11.1.3.1 National Institute of Standards and Technology (NIST)

NIST was established in 1901 and is working under the Department of Commerce (USA). NIST provides measures to support the simplest to the most complex human-made products. NIST's technology, measurements, and standards are used in a wide range of products and services throughout the world. There are three major digital forensic projects at the NIST which are supported by the US Department of Justice, law enforcement, and other sponsoring organizations [10]. These projects are:

(a) National Software Reference Library (NSRL).
(b) Computer Forensic Tool Testing (CFTT).
(c) Computer Forensic Reference Data Sets (CFRDS).

11.1.3.2 National Institute of Justice (NIJ)

This institute is working as the research, development, and evaluation wing of the US Department of Justice. Its goal is to use science to improve our understanding of crime and justice concerns [11].

11.1.3.3 International Organization on Computer Evidence (IOCE)

The major task of IOCE is to develop international standards for the exchange and recovery of electronic evidence. IOCE has established working groups in Canada, Europe, the United Kingdom, and the United States in response to the G-8 Communique and Action Plans of 1997. IOCE presented the following five main principles at the International Hi-Tech Crime and Forensics Conference (1999) [9]:

(a) Any actions made after seizing digital evidence should not change the evidence.
(b) When accessing original digital evidence, a person must be forensically qualified.
(c) All activities involving the seizure, access, storage, or transfer of digital evidence must be adequately documented, preserved, and available for review.
(d) During the time that digital evidence is in their possession, an individual is liable for any activities performed with regard to it.
(e) These standards must be followed by every agency in charge of seizing, accessing, storing, or transferring digital evidence.

11.1.3.4 American Society of Crime Laboratory Directors (ASCLD)

It is a nonprofit organization of forensic science managers and crime laboratory directors. The organization's goal is to promote professional interests while also assisting in the development of laboratory management ideas and procedures. It is the only accrediting body dedicated solely to laboratories that conduct criminal justice testing [12].

11.1.3.5 ISO SC 27 CS1

This contains generic security and privacy approaches, techniques, and guidelines, such as [13]:

(a) Methodology for gathering security requirements.
(b) Information and ICT security management, including information security management systems, security procedures, and security controls and services.
(c) Cryptographic and other security measures, such as those that secure information accountability, availability, integrity, and secrecy.
(d) Support documents for security administration, including terminology, standards, and methods for registering security components.
(e) Identity management, biometrics, and privacy security aspects.
(f) In the field of information security management systems, there are standards for conformance assessment, accreditation, and auditing.
(g) Criteria and methodology for evaluating security.

11.1.4 Glossary Used in Digital and Cyber Forensics

To get familiar with the concepts of digital forensics, the following terminologies are frequently used [14]:

- Acquisition: In digital forensics, data acquisition refers to the techniques for collecting digital information, including cloning and copying evidence from any electronic source. It means developing a forensic image from digital devices that can store electronic data, such as servers, tablets, CD-ROMs, gaming consoles, portable hard drives, hard drives, thumb drives, and other computer technologies.
- ACPO guidelines: ACPO (Association of Chief Police Officers) has developed a set of computer-based evidence guidelines. It provides a set of four key principles:
  - There must be no actions taken that alter data stored on a digital device that may later be used as evidence in court.
  - If accessing original stored data on a digital device is required, you must be both capable and able to justify your acts, as well as the effect they may have on any digital evidence used in court.
  - Both steps taken and applied to the digital proof must be recorded and maintained safely and securely. If another forensic expert reviews the procedures, the conclusion must be the same.
  - The investigation's lead investigator is ultimately responsible for ensuring that these guidelines are followed.
- Active data: The data we can actually see is known as active data. Data files, applications, and operating system files are included under this category.
- Ambient data: The information on a device that is not viewed or used as part of routine operations is referred to as ambient data. It is created accidentally, as a by-product of other tasks, and serves no particular purpose.
- Archival data: Archival data is often compressed and stored on another medium, such as tape or CD. Such information is normally not readily accessible to the user and must be recovered from archival media before it can be accessed.
- ASCII: ASCII (American Standard Code for Information Interchange) is a character encoding standard for electronic communication. Computers, telecommunications equipment, and other devices all use ASCII codes to represent text.
- Audit trail: An audit trail is a security-relevant historical record, collection of records, and/or destination and source of records that provide documentary evidence of the chronology of activities that have affected a particular action, process, occurrence, or system at any given time.
- Backdoor: A backdoor is method by which any users (authorized/unauthorized) can bypass usual security protocols and gain high-level user access to a computer, network, or computer program.
- Backdoor Trojan: Backdoor Trojans are malicious software programs that allow unauthorized access to a computer in order to set up a remote attack. Remote

attackers may use a compromised computer to submit commands or gain complete control.

- Backup: Backup is the copy of computer data stored on a hard drive to protect against accidental loss or corruption.
- Backup server: A backup server is a server that allows you to back up your data, files, applications, and databases. It can be locally based or a remote backup server, and it offers both hardware and software features for managing and recovering your backups.
- Backup media: Backup media refers to the storage media used for backup electronic data, such as discs, disc drives, and tapes.
- Bit: A bit, or binary digit, is a basic unit of information or the smallest unit of data in computers and digital communications. Each bit is represented by a 1 or a 0.
- Cache: Cache is a temporary storage area that helps web pages, browsers, and apps load faster.
- Compressed file: Any file containing one or more files or directories that are smaller than their original file size is referred to as a compressed file. These files allow for faster downloading and more data to be stored on a removable device.
- Cookies: Cookies are text files that include small amounts of data, such as a login and password, and are used to identify your computer when you access the network. HTTP cookies are used to identify and improve the web browsing experience of users.
- Corrupt file: A file that has been corrupted. When a problem occurs during the saving process, a file becomes corrupted.
- Cyberattack: The theft, alteration, or destruction of a specific target using digital devices, computer networks, or technology-dependent companies. Attacks are carried out by distributing malicious software, creating bogus websites, or gaining unauthorized access, and they frequently result in extensive destruction.
- Dark web: The dark web is a decentralized network of websites that tries to keep users as anonymous as possible by routing all of their communications through several servers and encrypting them at every stage.
- Deep web: Parts of the Internet that are not fully accessible through typical search engines like Google, Yahoo, and Bing are referred to as the deep web.
- Deduplication: Deduplication is a method of reducing storage capacity requirements by eliminating redundant copies of data.
- Digital forensics: The use of investigative and analytical procedures to identify, preserve, extract, and document digital evidence in a way that is suitable for court presentation.
- Directory: A list of files stored on a hard disc or other media that is organized hierarchically is called directory. The root directory is the topmost directory.
- Disk mirroring: Disk mirroring is a method of protecting a computer system from data loss and other potential losses caused by disc failures. The data is replicated using this method by writing it to two or more identical hard drives, all of which are attached to a single disc controller board. If one of the mirrored hard drives fails, the data can be recovered from the others.

- Encryption: Encryption is the process of converting data into a secret code that hides the true meaning of the data.
- File carving: The technique of retrieving files that have been deleted but not totally erased from a digital device. It operates by scanning and reassembling the raw bytes of a hard disk.
- File server: In a computer network, a file server is a central server instance that allows linked clients to utilize the server's storage capacities.
- File signature: A file signature is information that is used to identify or validate a file's contents.
- File slack: File slack is the unallocated space on a hard drive where a file is kept. Because each cluster on a drive has a storage threshold and files are of varying sizes, this space remains empty or unused.
- Forensic image: A forensic image is a type of copy of original evidence that has all of the data found in the original but wrapped in a forensic file format that prevents tampering.
- Hash value: A hash value is the result of a calculation (hash algorithm) on a string of text, an electronic file, or the contents of an entire hard drive.
- Hash match: The hash match operator performs a variety of logical operations, all of which employ an in-memory hash table to locate matching data. Hash match can be used with a single or two inputs due to its versatility. The *build input* is the initial input, which is shown on top of a graphical execution plan. The *probe input* is a second input that is optional.
- Insider threat: An insider threat to an organization's security comes from former or present employee, contractor, or third party. Sabotage, theft, fraud, access rights abuse, and espionage are all examples of common insider threats.
- Imaging tools: A storage medium can be imaged using either forensic software or hardware. There are both free and commercial solutions that can help with the procedure. The most significant characteristics to check for when selecting a tool are the speed with which it can conduct an image and its reliability.
- ISO 9001 certification: An organization that meets the certification requirements regularly offers products or services that fulfil customer and regulatory standards.
- Keylogger: Keyloggers are a sort of monitoring software that records a user's keystrokes. These keystroke loggers, one of the oldest types of cyber threat, record the information you type into a website or application and send it to a third party.
- Keyword match: A keyword match is a typical approach used in computer forensics and electronic discovery to find and identify every instance of a particular word or phrase on a computer or other media, even if the word or phrase appears in unallocated space or deleted files.
- Live analysis: The process of analyzing digital media in real time rather than turning it off and sending it to a lab. This strategy frequently proves to be the most effective means of capturing evidence since it decreases the chance of information being tampered with and allows for more retrieval of volatile data.
- LNK files: LNK files (also known as labels or Windows shortcut files) are files that are created automatically by Windows operating system whenever a user

opens a file. The operating system uses these files to ensure quick access to a certain file. Furthermore, some of these files can be written by users to help them with their tasks.

- Log file: A log file is a computer-generated data file that contains information about usage patterns, activities, and operations within an operating system, application, server, or another device.
- Master file table (MFT): One of the most significant files in the NTFS (New Technology File System) file system is the Master File Table (MFT). It keeps a record of all files on a volume, including their location in the directory, physical location on the drive, and file metadata.
- Metadata: The data embedded within a file that describes the document's characteristics. Although some metadata may be seen by the user, such as modification dates and file sizes, other hidden or embedded information requires the assistance of a technical expert to locate.
- Network: A network is a collection of computers, servers, mainframes, network devices, peripherals, and other devices that are connected to allow data to be shared.
- New Technology File System (NTFS): The Windows NT operating system uses the New Technology File System to efficiently store, organize, and find files on a hard disk.
- Outsider threat: A threat to an organization's security that originates from the outside, such as a cybercriminal, hacktivist, or competition-sponsored attacker. Economic gain, corporate espionage, and social or political change are all common reasons for an outside attack.
- Program: A program is a computer software that can be executed. It's similar to a script, but it's usually much bigger and doesn't need a scripting engine to run. A program, on the other hand, is made up of compiled code that can be run straight from the operating system of a computer.
- Registry hives: A hive is a logical group of keys, subkeys, and values in the registry that is accompanied by a collection of supporting files loaded into memory, when the operating system is started or a user logs in. When a new user connects to a computer, a new hive with a distinct file for the user profile is created. This is called the user profile hive.
- Shadow volume: Shadow volume is a feature of the Microsoft Windows operating system. It enables Windows users to create manual and automated backup copies of their computer data and volumes. Even if such files or volumes are in use, this feature is available.
- Software: Software is a collection of programs that are designed to execute a specific task. A program is a group of instructions designed to address a specific problem.
- Steganography: Steganography is the art of concealing a secret message within a non-secret object. Many forms of steganography nowadays involve hiding a secret piece of text within a photograph. Alternatively, you may hide a secret message or script inside a Word or Excel document.

- System integrity: Methods for ensuring that data on a computer is genuine, correct, and protected from unauthorized user alteration.
- TOR (The Onion Router): An open-source privacy network that allows users to surf the Internet anonymously.
- Window registry: A swap file is a section of the hard drive dedicated to temporary data storage. The swap file is used by Windows to increase performance. A computer's primary memory, or RAM, is used to store data for present activities, but the swap file acts as additional memory that can be utilized to store additional data.
- Write blocker: A write blocker is a device that allows data to be read from a hard disc without changing the data on the disc. On the hard drive, the device allows a read command but not a write command to be executed. The examiner can use a built-in write blocker in most imaging tools while imaging a hard disc. While software tools or changes to the Windows registry can achieve write blocking, hardware methods will be favored in digital forensic laboratories.

11.1.5 Electronic Evidence

Digital forensics focuses on collection of data from electronic evidence, its transformation into useful information, and delivering the findings to the court. The IT Act and its amendments are based on the model law on electronic commerce established by the United Nations Commission on International Trade Law. The Information Technology Act of 2000, related amendments to the Evidence Act of 1872, and the Indian Penal Code of 1860 established the concept of electronic evidence. According to Section 2(1)(t) of the Information Technology Act, 2000, "electronic record" means data, record or data generated, image or sound stored, received or sent in an electronic form or microfilm or computer-generated micro fiche [15–17].

So, electronic evidence is the data that is manipulated, stored, or communicated by any man-made device, computer, or computer system, or transmitted through a communication system, and that has the ability to make either party's factual account more or less reasonable than it would be without the evidence. In short, electronic evidence is the data or information that exists in digital format and utilized in a court of law to "prove" or "expose the truth" about a crime.

11.1.5.1 Challenges with Electronic Evidence

Unlike other evidence (DNA, fingerprint, blood, etc.), the process is very challenging in case of digital evidence due to the fact that [18]:

- The data may be dispersed across numerous physical locations, even countries.
- Data can be easily and very quickly transferred across jurisdictional borders.
- The data is highly volatile, meaning it can be readily changed, rewritten, damaged, or destroyed with a single keystroke.
- It is possible to copy the data without causing it to degrade.

- Electronic evidence has a short lifespan before it is considered useless, unlike any other type of forensic evidence.

11.1.5.2 Guidelines for Electronic Evidence

The following guidelines must be followed when dealing with electronic evidence [19]:

(a) It is necessary to gather electronic evidence in a lawful manner.
(b) Before handling electronic evidence, the staff involved must undergo the relevant training program.
(c) Any changes made to the electronic evidence must not affect the data. If access to the original data or changes to the system settings are required, only authorized personnel should be able to do so, and those personnel must be able to justify their actions.
(d) If possible, any activity that requires accessing or changing the original data should be recorded and witnessed by another practitioner.
(e) All acts made while dealing with electronic evidence must be documented and kept on file so that they can be audited. Those actions should be repeatable by an independent third party with the same effects.

11.1.6 Forensic Investigation Process

The purpose of a digital forensic investigation is to learn everything there is to know about an incident. It entails locating and assessing digital evidence relevant to the case. The basic processes of investigation are followed by digital forensic experts; the complexities of these processes vary depending on the model of the organization in charge of the inquiry [2]. In the digital forensic laboratory, electronic evidence analysis usually involves four phases (Fig. 11.1).

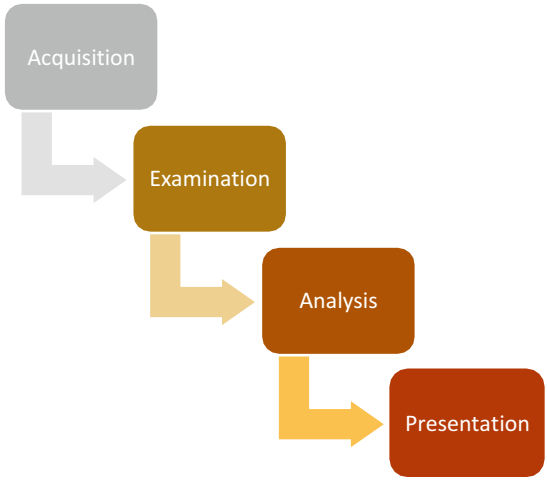

Fig. 11.1 Processing of digital evidence during digital forensics investigation

The chain of custody of the evidence must be updated anytime it changes hands throughout the procedure, and its integrity must be always maintained. The examination and analysis steps might be repeated until the work meets the requirements of the case. Although it is widely assumed that conducting digital forensics work in the laboratory requires these four phases, not all cases will require all four. In some circumstances, the acquisition step can be bypassed entirely to undertake triage during the examination step. For example, when there are enormous quantities of data, conducting acquisition on each evidence item may not be possible. The detail explanation of these four phases is as follows:

11.1.6.1 Acquisition

The process of generating a forensic copy of electronic evidence (exhibit) such as a hard drive, USB drive, or server in the form of an image file/s is known as acquisition or data acquisition. The image file/s will then be used to analyze the evidence in the next stage of the process. The acquisition is conducted to protect the electronic evidence's integrity. It is to make an exact copy of the data without altering the electronic evidence's content in any manner. The acquisition of electronic evidence must be done in a forensically suitable way. Typically, data is obtained by capturing volatile data from a running computer during a search or by obtaining a storage device from a seized computer, or at any other point during an inquiry. Data and information saved in electronic form are intangible, making them easier to manipulate and alter than traditional forms of proof. As a result, having a defined and tested acquisition procedure is critical [2, 5, 20].

Both the exhibit's hash value and the image file must be recorded once an image file has been created. The image file is hashed to ensure that the content of the exhibit is identical. In digital forensics, hashing algorithms like Sha-256 are employed. The hash-generating capability is available in most forensic software and hardware.

Unless circumstances prevent examiners from doing so, examination and analysis must be done on a forensic copy of the original evidence. This is critical to protect the evidence's integrity. The forensic copy of the electronic evidence must be preserved elsewhere, not on the evidence itself. To avoid being confused up with the original evidence or forensic copies from other instances, the forensic copy must be carefully labelled. As a result, before receiving cases, the digital forensic laboratory must prepare certain storage medium.

This chapter demonstrates how to perform a digital forensic investigation and analysis on computer.

Levels of Data Acquisition

There are two levels of data acquisition [2, 21]:

- **Physical data acquisition:** Physical data acquisition includes all raw data. At this level of acquisition, all data on the disc will be copied, including the partition scheme, partitioned area, and un-partitioned space. Because it includes deleted files and unallocated clusters, the Examiner frequently chooses this level of data acquisition of the entire drive.

- **Logical data acquisition:** Logical data acquisition only includes a subset of raw data. On the disc level, logical data acquisition copies only a logical partitioned area. When dealing with encryption, logical data acquisition of unlocked data is recommended over physical data acquisition of encrypted data. The examiner must first decide on the exhibit's state before making a copy.

Types of Acquisition

- **Live acquisition:** Live acquisition is performed on a live system. A live system is one that is up and running and in which data is constantly being processed, allowing information to be changed. Switching a live system off may result in the loss of volatile data, such as data saved in the cloud, encrypted data, ongoing processes, network linked, and mounted file systems, due to the substantial evidentiary value that can be discovered in a live system. The level of volatility in a system's data varies. If the machine is turned off or rebooted, these data will be lost. When collecting live data, the examiner should start with the most volatile data. The order of typical levels of volatility, from most to least volatile, is as follows: Memory, Swap File, Network Processes, System Processes, and File System Information. Live acquisition is also used in two situations: (i) when a system is business critical and cannot be shut down and (ii) when volatile data is more significant than erased data.
  - **Dead acquisition:** Dead acquisition is carried out on a dead system. A dead system is one that is not in use; it is switched off and has no power. Volatile data in temporary storage regions on a computer, such as RAM memory, ongoing processes, cache, or current application dialogues, will no longer be accessible after the machine is dead. Dead acquisition is a simple procedure that is usually carried out automatically using forensic equipment. If feasible, remove the hard disc from the computer before connecting it to the equipment. In some circumstances, dead acquisition cannot be used to recover netbook PCs or devices with soldered solid-state drive storage. In such circumstances, other extraction methods, such as starting the system with a live CD/USB, should be considered. When erased data is more important than volatile data, a dead acquisition is performed.

    After then, the examiner must decide whether to clone the exhibit or generate an image. The data is copied bit by bit from one storage medium to another by the clone. The image, on the other hand, moves data from one storage media to another, bit by bit, producing an image file. After that, the file can be saved on another medium. The latter method is more typically employed because the image file can then be read by most forensic software and processed for forensic analysis. Cloning is frequently utilized in simulations.

Imaging Formats

Raw and E01 (EnCase Evidence File) are two of the most prevalent image file formats. In a raw file, these formats store all data from the original medium. E01

contains physical bitstream copy stored in a single/multiple files enriched with metadata. Expert Witness Format (EWF) and Advanced Forensic Format (AFF) are two other formats that are used for analysis. They have characteristics such as:

- Compression of data.
- Encryption of data.
- Error checks.
- Case metadata.
- Hash sums.
- Splitting the image in chunks.

In addition, several forensic software systems have their own proprietary picture formats with similar features. It is recommended to choose an image format that is supported by most of the forensic software. A few digital forensic laboratories utilize distinct forensic software; thus, if the examiner selects a unique image file format, the image file may not be opened.

Process of Acquisition

The common process for conducting data acquisition can be divided in the following four steps [21]:

(a) **Identify storage media:** Before handing over, the examiner must provide a compatible storage media with sufficient data size. The examiner may need to prepare many storage media to store the image file if the exhibit is substantial.
(b) **Imaging the exhibit:** Before imaging the exhibit, make sure it is connected to a write blocker for protecting its integrity. This function is available in most forensic software. The image file is subsequently saved to the storage media that has been prepared. Use a standard labelling format to protect the storage media and the image file by hashing all the evidence with SHA256. The examiner should be aware that utilizing a write-blocking approach does not prevent data modifications on a solid-state drive or flash media with a controller chip. The controller will begin reorganizing data on the flash chips as soon as it is connected to a power supply. Even when connected to a write-blocking device, the controller performs tasks such as wear-leveling, write-amplification, and trash collection. At present time, the only technique to generate a proper forensic copy of the flash media is to use a lot of resources. This is accomplished by unsoldering the chip(s) from the circuit board and, if possible, reassembling the data in the proper order.
(c) **Verify exhibit and image file:** After creating the image file, the examiner must verify that it can be opened with forensic software and that the hash values of the exhibit and the image file match.
(d) **Documentation:** In the case notes, the final stage in examining and analyzing the computer is to document the procedure, including the tools used, hash values, date and time, and the examiner's initials. The flow chart of the process of acquisition is shown in Fig. 11.2.

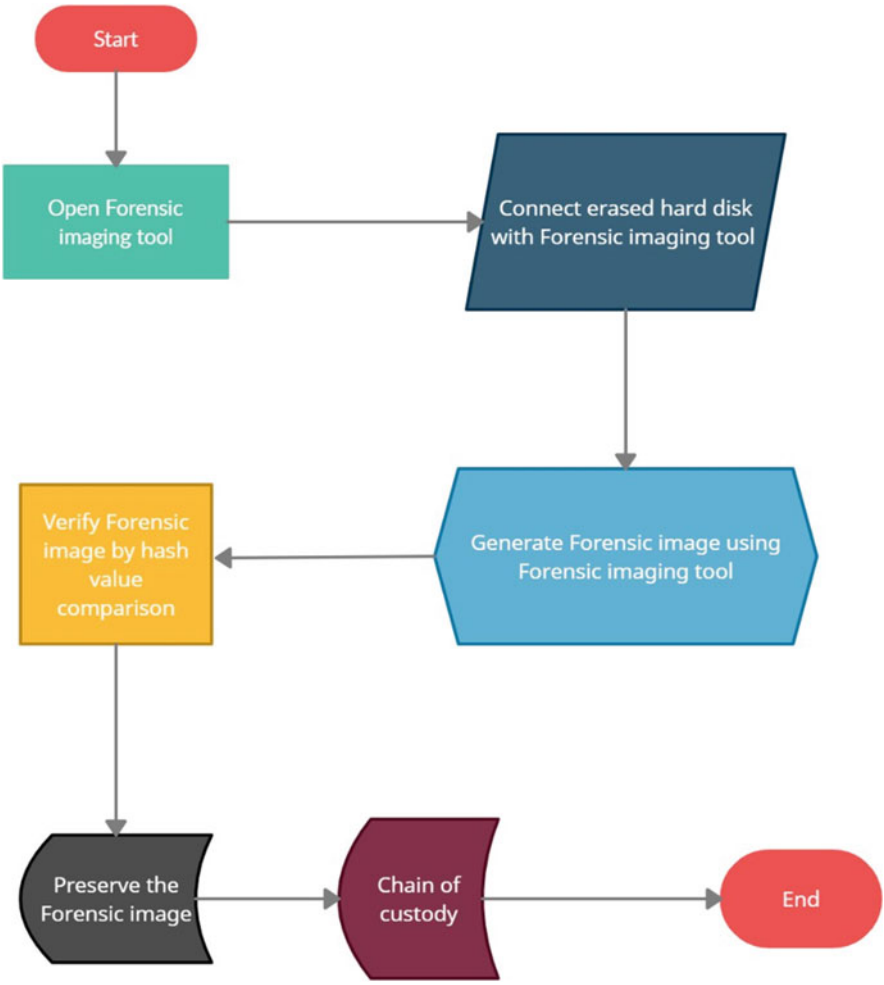

Fig. 11.2 Process of acquisition

11.1.6.2 Examination

Wherever feasible, original evidence should not be examined. The examiner must always work on the evidence's forensic copy (image file). If this is necessary, data access must be restricted using a write blocker. Examiners may need to perform the examination in an isolated or pre-set environment in some cases, for example, using a database system or game software to run the simulation. Examiners can accomplish this by encapsulating the case in a functional container using virtualization technology. When the examination is over, the examiner can use a recognized image, or a feature provided by the operating system to restore the workstation to its prior condition [2, 21].

Triage

The process of prioritizing cases, exhibits, or data for analytic procedures based on their relevance to the case is known as triage. Cases, exhibits, or data will be analyzed in order of importance, from most important to least important, based on the results of triage. It's likely that some won't be examined at all since they're irrelevant to the matter under investigation. Triage is carried out to deal with problems such as:

- There are a large number of exhibits or large amounts of data that must be analyzed in a short period of time.
- Exhibits can no longer be stored owing to legal difficulties.
- It is a high-priority case with imminent outcomes, such as when physical damage or death is a possibility.

Though the triaging is beneficial, it cannot be used for a comprehensive exam. Automated processing, such as that provided by forensic software or the application of self-written programs to exhibits or data, is used to conduct triage. Triage remains a viable option for dealing with a situation that cannot be resolved in any other way. There is a lot of software available that performs triage functions, some of which is commercial and some of which is open source. Triage can be performed while the exhibit is still operational or by booting the exhibit utilizing forensic bootable media. The examiner then enters keywords and runs the system before picking and storing pertinent files on removable storage media. There is a chance that this automated data analysis will just look at subsets of data, leaving out some crucial information. This drawback must be conveyed to the investigator, prosecutor, and court, who are the deciding authorities to proceed with the triaging procedure or not.

Methods for Computer Examinations

A computer can be examined using a variety of methodologies and procedures. Some tasks require a high level of expertise, while others, such as running an automated process, need only a basic level of expertise. The examiner can employ a variety of forensic software. Some software can recover passwords, correlate data among electronic evidence, and execute keyword searches, depending on the software capacity.

(a) **Examination on Dead System**
The following information must be considered while examining a dead system:
- Active files, deleted files, file slack, partition slack, disk slack, and shadow files.
- Device artefacts—operating system files, file registry, file metadata, encrypted files, log files, and database files.
- Browsing history, e-mail, social media, and peer-to-peer file sharing.

(b) **Examination on Live System**
The following information should be considered when examining a live system:

- Random access memory (RAM).
- Running processes.
- Network connections.
- System settings.
- Storage media.
- Cloud services.

  Examination of a live system on any of the above data may be undertaken depending on the case request.

(c) **Automated Processing**

Automated processing is frequently carried out employing forensic software's readily available features. The examiner normally determines the scope of automated processing which can be applied to other similar investigations. Running a hash comparison on images in a child pornography case is an example. The following are typical automated processing actions and sequences:

(i) Extraction of data from the operating system and users.
(ii) Mount containers, for example, ZIP, RAR, and encrypted containers.
(iii) Extract and analyze objects like emails and web history.
(iv) Analysis of signatures.
(v) Recover files and folders that have been erased.
(vi) Carve specific file types.
(vii) Recover deleted partitions.
(viii) These analytical approaches may be utilized depending on the case request:
  - Optical Character Recognition (OCR) of PDF files.
  - Create thumbnails for simple viewing.
  - Extract photos from videos.
  - Skin-tone detection for films.
  - Hash comparison.
(ix) Logs from the operating system are examined.

Data Recovery

Data recovery is the process of recovering data that has been deleted, corrupted, hidden, or lost from storage medium. The storage medium may be damaged, corrupted, or formatted, rendering data inaccessible. As a result, data recovery also entails the process of repairing the storage media so that data can be recovered. Data recovery can be divided into two categories: logical recovery and physical recovery. When storage media is accessible but the data is formatted, corrupted, buried, or lost, logical recovery is used. Typically, forensic software is used in the recovery procedure. When the storage media are inaccessible due to mechanical or technological breakdown, physical recovery is performed. The recovery process is time-consuming and requires specialized knowledge. Physical recovery in some situations requires the use of a special room. When repairing a cable in a USB thumb drive, for example, a soldering equipment is required. Because the cost is

significant and a highly experienced examiner is necessary to do the activities, not many digital forensic laboratories can afford to create a physical rehab facility.

Filtering

Applying filters to an image file before analyzing it can assist the examiner by limiting the quantity of data he or she must look at and analyze. Hash sets are commonly used in filtering strategies to either filter out known operating systems or application files (whitelisting) or to explicitly search for hash matches inside databases of known illicit content (blacklisting). When only specific types of findings are relevant to the case, filtering can be used. Signature analysis can be used to filter files based on size, date, owner, and a variety of other attributes found in the metadata. Most commercial forensic software includes this filtering feature. The process of examination is shown in Fig. 11.3.

11.1.6.3 Analysis

Categories of Digital Traces

A criminal who commits a crime by computer will leave traces at a "digital crime scene," just as he or she would leave physical traces at a crime scene. Some of these traces can be configured to be discovered by the examiner, while others can be made to be hidden [2, 21]. There are two types of traces:

(a) **Discoverable:** Artefacts that are automatically saved on the computer. Even if a suspect tries to hide his/her tracks, the chances of uncovering such traces are high. Some of the discoverable traces are:
- Slack space.
- Unallocated space.
- MFT entries.
- RAM.

(b) **Non-discoverable**: Artefacts that can be set up such that they aren't saved on the computer. For example, a web browser that allows the user to disable or wipe download history. Some of the undiscoverable traces:
- Thumb caches.
- Most recently used lists.
- Log files.
- Browser histories.
- Browser caches.
- Most used programs.
- Form data.
- Pagefile.sys.
- Hiberfil.sys.
- Volume shadow copies.
- Download history.

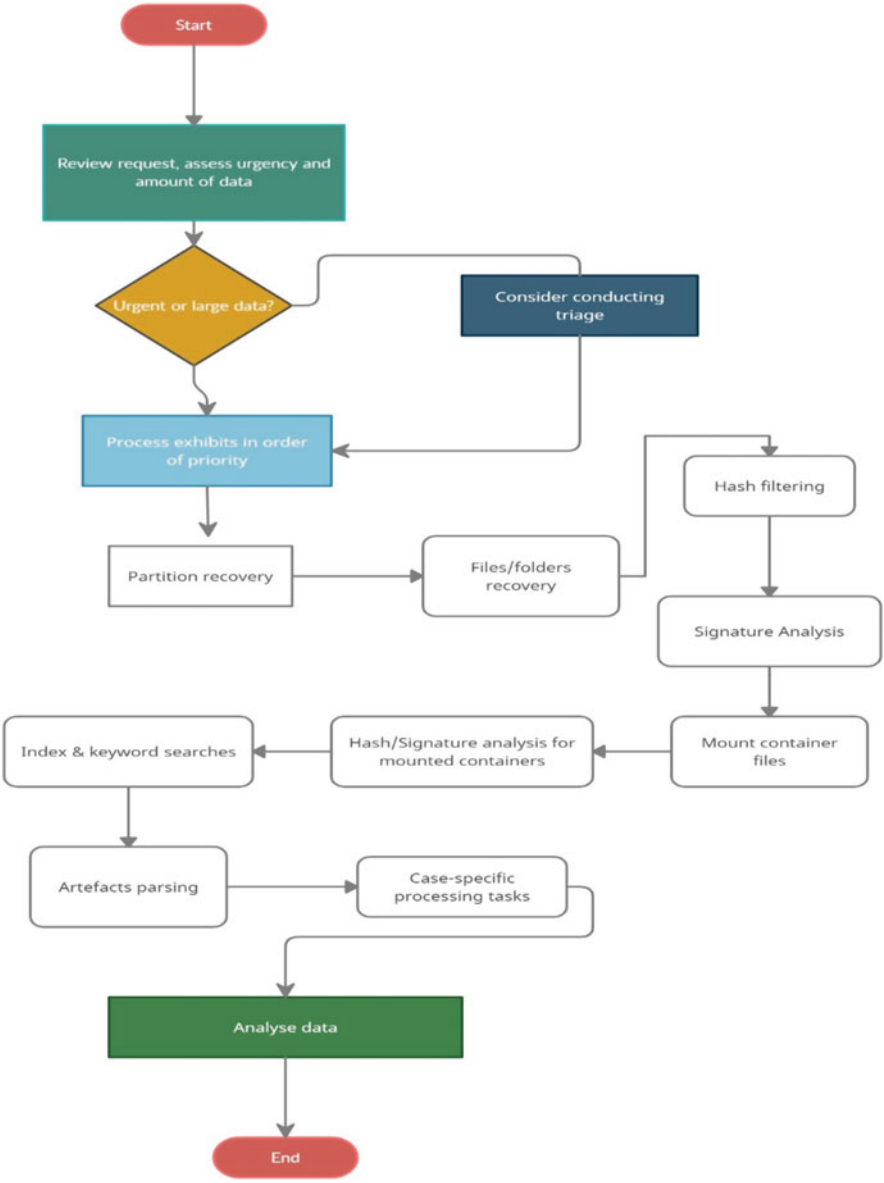

Fig. 11.3 Process of examination [21]

Procedure for Different Traces

The sort of data and information that must be taken from a computer is determined by the case. For example, data/information taken from a computer in a fraud case is often in the form of spreadsheets, emails, and office documents. Pictures, movies,

and communication messages are examples of possibly connected data/information in a child-abuse case.

The following sections explain in detail the types of data that can be extracted from a computer.

(a) emails: email analysis, which usually involves mail applications like Outlook, Thunderbird, and Mail, as well as webmail accounts. Different forms of artefacts will be produced by different mail clients. Personal folder files, such as PST, OST, and PAB, are used by Outlook to hold evidence. Inbox files are used by Thunderbird to store messages. Although forensic software usually need these files, it does not always retrieve all messages. As some forensic tools are unable to recover deleted communications from personal folder files, a data recovery approach may be required.
(b) Office documents: Filtering the files of interest is usually done after file signature analysis. To ensure that the file header and extension are the same, file signature analysis compares the two. If they don't match, the document header or extension may have been changed to disguise the information. Using a keyword search to filter files is necessary. Both processes are usually performed automatically by most forensic software. It is recommended for the examiner to refer the requester for content analysis after similar documents have been located. This is to ensure that the document being extracted is relevant to the case under investigation. When the requester confirms the documents, the examiner can go deeper into the document, its metadata, and who created it, as well as determine whether it was delivered or received on the computer.
(c) Pictures and videos: To undertake image and video analysis, the examiner must first have a clear understanding of what the requester is looking for. If searching for identical photographs is required, the requester must provide the examiner with the required photos. If the files have known hashes, the requester may need to provide the hashes to the examiner, or the examiner may be able to use a list of hashes from established databases. If it involves a specific segment of a video, the requester must provide its distinguishing characteristics. One example is extracting all motorcycle-related images from a video. The most common starting point for image analysis is signature analysis. The examiner can then use the thumbnail view to filter through the images in the gallery. A hash comparison can be used to find a set of known photographs in a case, such as a child abuse case or stolen blueprints. Some forensic software includes a capability that detects comparable pictures. The retrieved images can then be displayed in a gallery format. The examiner should consider extracting the metadata of photos and video files if the location or production details of those media are essential. Metadata are collections of data that describe and provide information about other data, such as GPS coordinates, creation date and time, and the equipment used to acquire the image. It is impossible for the examiner to go through thousands of photos and videos to find one specific video or picture file in some exhibits. The most efficient method is to extract all images and then send them to the requester. After the examiner has found the

relevant photos/videos, he/she can undertake further analysis to extract further useful information, such as GPS coordinates and creation or modification data.

(d) Internet browser: Internet browsers are of evidential value in many cases. They typically contain the following artefacts:
- Website visit history.
- Local cache/temporary Internet files.
- Bookmarks/favorites.
- Session's information.
- Cookies.
- Saved usernames and passwords.
- Entries from form fields.
- Internet keyword searches.

Analyzing browser artefacts can be useful for determining purpose or intent; for example, search engine phrases can be used to prove intent. Google Chrome, Microsoft Internet Explorer, Mozilla Firefox, and Apple Safari are all popular browsers. They all save data in the user's home directory. All other browsers use SQLite databases to store the artefacts stated above, except for Microsoft browsers. Browser analysis is available in most online forensic applications. However, due to rapidly growing technology, some forensic software may take some time to refresh its database due to frequent updates to particular browsers. As most browsers nowadays deal with SQLite databases, the examiner can manually analyze the artefact using free SQLite database browsers.

(e) Software: When a software needs to be examined, it almost always requires the extraction and comprehension of its artefacts. Communication software (e.g., WhatsApp and Skype), steganography software (e.g., OpenStego), password safes (e.g., KeePass), file sharing software (e.g., uTorrent), and cryptocurrency software (e.g., cryptocurrency wallets) are all examples of such software. Although there are no standard techniques for analyzing all software artefacts due to their diversity, it is generally done by conducting information gathering on the software artefacts from credible and reputable sources. A simulation can then be used to confirm the findings.

(f) User activity: The computer operating system tracks user activity at many different places. For example:
- Power on and shutdown.
- Software settings.
- Most recently used files lists.
- Device use.
- User logins.
- Wi-Fi connections.
- Preferred programs.
- Setup of user environment.
- Frequently accessed files.

This user activity can be analyzed to have a better knowledge of the user's behavior and even to prove evidential behaviors. The relics are stored in

various locations depending on the operating system. Most artefacts in Microsoft Windows are saved in the Registry, Event Logs, and Jump Lists. The artefacts are saved in the Library and log folders on OS X systems, whereas the majority of the data is stored in the user home folder, or the "/etc" or "/var" directories on Linux systems.

(g) Log file: Analyzing log files is critical, especially in times of system attacks. The examiner should not only retrieve allocated log files but also traces of deleted/unallocated log files. For log file analysis, specialized software are available. The premise of such an analysis is to look for specific phrases, unusual patterns, or logs that fall within a specific time window.

(h) Encryption: The majority of recent operating systems have built-in encryption capabilities. The user can easily enable full disc encryption for a system drive. Before the exhibit is transferred to a digital forensic laboratory, it is recommended that the passwords or encryption keys be acquired at the crime scene using live data forensics. Other passwords can also be extracted from the disc if possible. These passwords and their variants can be used to build a dictionary that can be used to launch a password cracking assault. Traditional law enforcement activities, such as obtaining physical evidence, such as written passcodes, keys, or recovery strings, should also be carried out to locate passcodes.

(i) Computer memory (RAM): The memory dump can be analyzed in the digital forensic laboratory if the computer memory was captured while the seized computer was still functioning. Understanding the memory architectures of various operating systems to analyze the memory dump necessitates a high level of technical knowledge and specialized software. Volatility and Rekall are two examples of this, both of which are freely available on the Internet. The following are examples of artefacts that can be retrieved from memory dumps:
- Running processes, including their memory.
- Process information (e.g., handles).
- Encryption keys.
- Opened files.
- Usernames, passwords.
- Unsaved documents.

Virtualization

When it comes to virtualization, a picture is worth a thousand words. The examiner can see the operating system environment of an exhibit in the same way that the suspect has viewed it. Finding evidence inside a virtual computer can be quicker and more expressive than reassembling data traces from an image file. Viewing pirated gaming software is one example. When mounting an image, use write-protected or read-only parameters with a write cache so that the virtual operating system can write log files without compromising the image's integrity.

Process of Handling Mass Data

Some instances involve many machines and a large amount of data. To complete the task quickly, separation of forensic analysis from the content analysis is required. Examiners focus on forensic analysis activities such as exhibit recovery, parsing, mounting, and processing, while investigators with case-specific knowledge perform content analysis. To ensure smooth functioning, the examiners and investigators may need to create and apply correct methods for handling and examining extracted files.

11.1.6.4 Presentation

The presentation phase means compiling findings and presenting them to stakeholders in a clear and intelligible manner. The examiner must compile the findings and results into a forensic report once the analysis step is complete. Judges, prosecutors, and all parties involved should be able to grasp the examiner's explanations and translations of sophisticated technical circumstances. They may also be asked to analyze the data and provide an opinion on their significance. When a significant number of exhibits are analyzed, the examiner may find it difficult to convey the findings to the investigative team. It is suggested that analytic tools be used to make it easier to link digital evidence with other data from the inquiry [2, 21].

Admissibility of Electronic Evidence

The requirements for electronic evidence admissibility may range from one jurisdiction to the next. When examining electronic evidence for trial, the examiner should examine the following criteria:

(i) Authenticity: The evidence must establish facts in a form that cannot be contested and must be indicative of the original situation.
(ii) Completeness: Any examination of the facts, or any opinion based on it, must tell the complete scenario, and not be skewed to fit a more favorable or desired viewpoint.
(iii) Reliability: Nothing about the collection and subsequent handling of the material should raise any doubts about its legitimacy or validity.
(iv) Convincing: The evidence must be convincing in terms of the facts it depicts, and it must be able to persuade the stakeholder in court of the truth.
(v) Proportionality: The procedures employed to acquire evidence must be fair and proportionate to the purposes of justice: the prejudice caused to any party's rights must not outweigh the evidence's probative value.

Report Writing

A forensic report must be written in simple, straightforward language. The outcome must be correctly summarized, as well as provide a clear response to the requester's case request. All technical details should be put in the appendix section rather than being included in the main content. This is to make it easier for laymen to grasp the report. The examiner must also avoid making any statements that cannot be supported by evidence. In the statement "The suspect tampered with File A," for

example, “File A located in Computer B has been changed” would be an appropriate sentence.

It can be difficult for the examiner to communicate the conclusions in the report due to the complexity of the case. Visual aids and visual representations, such as animation, slides, images, and live demonstrations, are effective ways to improve comprehension.

Expert Witness

In some jurisdictions, submitting a forensic report in place of the examiner attending the court session is adequate in court. In other jurisdictions, however, the examiner is required to appear in court and offer his or her expert testimony in connection with the case. An expert witness is a person who, via education, training, talent, or experience, possesses specialized knowledge and expertise that goes beyond that of the average individual. Others may rely on the witness’ specialized (scientific, technical, or other) opinion concerning evidence or a fact within the field of his or her skill, referred to as the expert opinion, because his or her knowledge is sufficient. In some countries, the trial judge determines expert status in each case, and the person is only an expert in that case. In some jurisdictions, the legal institution appoints an expert, who is then responsible for any case that falls within his or her area of knowledge. The rights and responsibilities of an expert witness vary by country. Examiners must be well versed in their jurisdiction’s legislation, court procedures, and role, as well as their rights and responsibilities.

11.1.7 Digital Forensic Tools

With gradual development of cyber forensic, various digital forensics tools have been developed for countering and analyzing cyber threats. Few top digital forensic tools are listed below.

11.1.7.1 Forensic Tool Kit (FTK)

A comprehensive computer forensics tool which is compatible with Windows, Linux, and macOS. It brings together all the most common forensic tools in one spot for investigators. It has features for email analysis, file decryption, data carving, data visualization, web viewer, Cerberus, and optical character recognition [22].

11.1.7.2 Autopsy Kit

It is an open-source forensic tool which is compatible with Windows, Linux, and macOS. Autopsy examines disc images, local discs, or a local file folder. Autopsy examines disc images, local discs, or a local file folder. It supports raw or E01 formats and can work on features like Keyword search, graphical interface, extraction of camera and geolocation from a .jpeg file, registry analysis, email analysis, hash set filtering, strings from unallocated space and unknown file types, Android support, and web artifacts [23].

11.1.7.3 Volatility

The Sleuth Kit focuses on the hard disc, but it's not the only place on a computer where forensic data and artifacts might be kept. Important forensic data might be kept in RAM, which must be acquired swiftly and carefully in order to be forensically valid and helpful [24].

It is also open-source tool and compatible with Windows, Linux, and macOS. It can examine raw dumps, crash dumps, VMware dumps (.vmem), virtual box dumps, and a variety of other types of dumps.

11.1.7.4 Registry Recon

The Windows registry serves as a configuration store for the Windows operating system and the apps that run on it. The registry is one of the most popular places where malware deploys persistence methods, and these applications can store several different data in it. Registry Recon is a commercial application for reconstructing Windows registries from forensic images. It also has the capacity to reconstruct deleted parts of the registry using unallocated memory space analysis [25].

11.1.7.5 Cellebrite UFED

With the growing relevance of mobile forensics, acquiring a mobile-focused forensics solution could be beneficial. Cellebrite UFED is recognized as the most advanced commercial mobile forensics tool available. It works on a variety of platforms (not only mobile devices) and has exclusive mobile device analysis methodologies and tools. It provides for physical as well as advanced logical acquisition and passwords for devices. It enables the examiner to open a password-protected encrypted raw disc image file [26].

11.1.7.6 Wireshark

Although many forensics tools concentrate on the endpoint, it is not the only source of information in a forensics investigation. The majority of cyberattacks take place over the network, and network traffic captures can aid in the detection of malware as well as provide access to data that has been deleted or overwritten on the endpoint [27].

Wireshark is the most popular and commonly used tool for network traffic analysis. Wireshark is a free and open-source network traffic analyzer that includes dissectors for a variety of network traffic types, a simple and easy-to-use GUI for traffic analysis, and a lot of capability behind the hood. It can either capture live traffic or ingest network capture files for analysis.

11.1.8 Applications of Digital and Cyber Forensics

There are many challenges fronting digital and cyber forensics in the present scenario. These challenges are because of easy availability of hacking tools and significant use of the Internet. The investigation is complicated by the large amount

of stored data. There are many advantages of cyber and digital forensics, and a few are enlisted as follows:

- It helps in protecting the integrity of computer system.
- It aids in the development and presentation of evidence in court, which may result in the criminal's punishment.
- It assists businesses in retrieving critical data if their computer systems or networks are attacked.
- It locates cyber criminals from all around the world with ease.
- It aids in the protection of the funds and time of an organization.
- It allows to extract, evaluate, and analyze factual evidence to show cyber criminal behavior in court.

However, the digital evidence analyzed by cyber forensic experts have limitations also which are listed below:

- In court, it must be proven that that no tampering has occurred to the digital evidence.
- The expense of creating and storing digital data is exceedingly high.
- Judges and lawyers must have a broad understanding of computers.
- If the digital forensic tool utilized does not meet the required criteria, the evidence may be rejected by the court of law.
- Due to the investigating officer's lack of technical understanding, the desired outcome may not be achieved.

11.2 Conclusion

The digital forensics have emerged as a contemporary science in the past few years. As the exponential growth in Internet use has increased cybercrimes manyfold, it is essential to develop new investigative tools to counter the cyberattacks. Hackers have their own ways to breach the data which can be threat to privacy, personal data, financial, and security. Both preventive and responsive measures are required to counter such attacks. Therefore, advanced technological development of cyber forensics is essential. It is the fastest growing field of forensic science as newer techniques are being introduced. However, the validation and authentication of these techniques are essential for their admissibility in courts. Therefore, digital forensic guidelines and technology should be so strong that digital evidence can be relied upon and courts cannot dismiss digital evidence in the absence of any other evidence.

References

1. Help next Security 445 million attacks detected since the beginning of 2020. https://www.helpnetsecurity.com/2020/04/29/2020-attack-rate/. Accessed 26 May 2021
2. A basic guide for the management and procedures of a digital forensics laboratory. Retrieved 26 May, 2021 from https://webcache.googleusercontent.com/search?q=cache:mpnsToyghiIJ:https://rm.coe.int/glacy-dfl-guide-version-aug-2017-v8/16809ebf68+&cd=1&hl=en&ct=clnk&gl=in 3. SI110: Computer forensics. https://www.usna.edu/Users/cs/wcbrown/courses/si110AY13S/lec/l30/lec.html
3. SI110: Computer forensics. https://www.usna.edu/Users/cs/wcbrown/courses/si110AY13S/lec/l30/lec.html
4. Casey E (2011) Digital evidence and computer crime: forensic science, computers, and the internet. Academic Press
5. Digital forensics: References – OpenLearn – Open University. open.edu/openlearn/science-maths-technology/digitalforensics/content-section-4.3
6. Pollitt M (2010) A history of digital forensics. In: IFIP International conference on digital forensics, Springer, Heidelberg, pp 3–15
7. Whitcomb CM (2002) An historical perspective of digital evidence: a forensic scientist's view. Int J Digit Evid 1(1):7–15
8. Parasram SVN (2020) Digital forensics with Kali Linux. Packt Publishing
9. Digital evidence: standards and principles, by SWGDE and IOCE. https://archives.fbi.gov/archives/aboutus/lab/forensic-science-communications/fsc/april2000/swgde.htm
10. National Institute of Standards and Technology Retrieved 25 May, 2021 from https://www.nist.gov/about-nist
11. National Institute of Justice Retrieved 25 May, 2021 from https://nij.ojp.gov/about/national-institute-justice-mission-and-guiding-principles
12. ASCLD Home. https://www.ascld.org/
13. ISO/IEC JTC 1/SC 27 – Information security, cybersecurity and privacy protection (1989). www.iso.org/committee/45306.html
14. Computer forensic glossary Retrieved 26 May, 2021 from https://burgessforensics.com/computer-forensicsglossary/
15. Duggal P (2001) Cyberlaw in India: The information technology act 2000 – Some perspectives – Media, telecoms, IT, entertainment – India. https://www.mondaq.com/india/it-and-internet/13430/cyberlaw-in-india-the-information-technologyact-2000%2D%2Dsome-perspectives
16. The Indian Evidence Act 1872. https://indiankanoon.org/doc/1953529/
17. India Code: Indian Penal Code 1860. https://www.indiacode.nic.in/handle/123456789/2263?locale=en
18. Kramer XE (2018) Challenges of electronic taking of evidence: old problems in a new guise and new problems in disguise. II Conferencia Internacional & XXVI Jornadas Iberoamericanas de Derecho Procesal IIDP & IAPL, La Prueba en el Proceso/Evidence in the process Atelier 391–410
19. Nelson SD, Olson BA, Simek JW (2006) The electronic evidence and discovery handbook: Forms, checklists, and guidelines
20. Barbara JJ (ed) (2007) Handbook of digital and multimedia forensic evidence. Springer Science & Business Media
21. Interpol global guidelines for digital forensic laboratories. https://www.interpol.int/en/content/download/13501/file/INTERPOL_DFL_GlobalGuidelinesDigitalForensicsLaboratory.pdf
22. Forensic Toolkit (FTK)® AccessData, https://accessdata.com/products-services/forensic-toolkit-ftk#
23. Autopsy Law Enforcement. https://www.autopsy.com/use-case/law-enforcement/

24. FAQ Volatilityfoundation. https://www.volatilityfoundation.org/faq
25. Registry Recon – Forensic Focus. https://www.forensicfocus.com/reviews/registry-recon/
26. Cellebrite UFED IOS – Cellebrite. https://www.cellebrite.com/en/ufed-unlock-iphone-x/?utm_source=adwords&utm_medium=Paid-Search&utm_campaign=702076&utm_content=ufed-unlock-iphonex&gclid=CjwKCAjwwqaGBhBKEiwAMk-FtDpvaiJLBfYbmLpI_2pD9un71BJbyd3E4GrLYOaTciMM59ZdnbOxIBoC5_EQAvD_BwE
27. Wireshark. Go Deep. https://www.wireshark.org/