Unit 1: Basics of Forensic Concepts

1

UNIT STRUCTURE

1.1 LEARNING OBJECTIVES

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

- Evolution of Computer Forensics
- Scope of Cyber Forensics
- Investigation process

1.2 INTRODUCTION

The advancement of Information and Communication Technologies (ICT) opens new avenues and ways for cybercriminals to commit crime. The recent development in Information Communication Technology (ICT) has made tremendous changes in every aspect of our life. These changes have been clearly reflected in cyberspace-related areas.[1] Cybercrime describes a wide range of circumstances in which technology is involved in the commission of a crime. It presents numerous and constantly evolving challenges to government and law enforcement. Cybercrime is an umbrella term used to describe two distinct but closely related criminal activities i.e., ***Cyber-dependent and Cyber-enabled crimes.*** The former are offences that can only be committed by using a computer, computer networks, or another form of ICT. These acts include the spreading of viruses and other malicious software and distributed denial of service (DDoS) attacks. Cyber-dependent crimes are primarily acts directed against computers or network resources, although there may be secondary outcomes from the attacks, such as fraud and the latter, Cyber-enabled crimes, are traditional crimes that are increased in their scale or reach by the use of computers, computer networks or another form of ICT.

Computer forensics is the practice of collecting, analysing and reporting on digital data in a way that is legally admissible. It can be used in the detection and prevention of crime and in any dispute where evidence is stored digitally. It deals with the preservation, identification, extraction and documentation of computer evidence. Like many other forensic sciences, computer forensics involves the use of sophisticated technological tools and procedures that must be followed to guarantee the accuracy of the preservation of evidence and the accuracy of results concerning computer evidence processing. The use of specialized techniques for recovery, authentication, and analysis of computer data, typically of data which may have been deleted or destroyed.[2]

Digital forensics is the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating

[1] "Bridging the gap in Legislation, Investigation <https://vc.bridgew.edu/ijcic/vol2/iss1/5/>
[2] Cybercrime and Digital Forensics: Bridging the gap <https://vc.bridgew.edu/cgi/viewcontent.cgi?article=1014&context=ijcic>

or furthering the reconstruction of events found to be criminal; or helping to anticipate unauthorized actions shown to be disruptive to planned operations.

1.3 EVOLUTIONS OF COMPUTER FORENSICS

The field of Computer Forensics began to evolve more than 30 years ago. The field began in the United States, in large part, when law enforcement and military investigators started seeing criminals get technical. The fields of information security which focuses on protecting information and assets, and computer forensics, which focuses on the response of hi-tech offenses, started to intertwine. The history of forensic science dates back thousands of years. Fingerprinting was one of its first applications. The ancient Chinese used fingerprints to identify business documents. In 1892, a eugenicist named Sir Francis Galton established the first system for classifying fingerprints. Sir Edward Henry, the commissioner of the Metropolitan Police of London, developed his own system in 1896 based on the direction, flow, pattern and other characteristics in fingerprints.[3] The Henry Classification System became the standard for criminal fingerprinting techniques worldwide. The timeline of the evolution of computer forensics are as follows:-

YEAR	EVENT
1835	Scotland Yard's Henry Goddard became the first person to use physical analysis to connect a bullet to murder weapon. Later, a team of scientists at the Aerospace Corporation in California developed a method for detecting gunshot residue using scanning electron microscopes.
1836	James Marsh developed a chemical test to detect arsenic, which was used during the murder trial.
1892	Sir Francis Galton established the first system for classifying fingerprints.
1896	Sir Edward Henry, based on the direction, flow, pattern and other characteristics in

[3] Richard III GG, Roussev V Next-generation digital forensics. Communications of the ACM 2006 Feb 1;49(2):76-80

	fingerprints.
1920	American physician Calvin Goddard created the comparison microscope to help determine which bullets came from which shell casings.
1930	Karl Landsteiner won the Nobel Prize for classifying human blood into its various groups.
1970	Aerospace Corporation in California developed a method for detecting gunshot residue using scanning electron microscopes.
1984	FBI Magnetic Media program, which was later renamed to Computer Analysis and Response Team (CART), was created and it is believed to be the beginning of computer forensic.
1988	International Association of Computer Investigative Specialists (IACIS) was formed.
1995	International Organization on Computer Evidence (IOCE) was formed.
1997	G8 nations declared that "Law enforcement personnel must be trained and equipped to address high-tech crimes".
1998	- G8 appointed IICE to create international principles, guidelines and procedures relating to digital evidence. - 1st INTERPOL Forensic Science Symposium was held.
2000	First FBI Regional Computer Forensic Laboratory was established.

1.4 OBJECTIVES OF COMPUTER FORENSICS

The objectives of Computer forensics are to provide guidelines for:[4]

- Following the first responder procedure and access the victim's computer after the incident.

[4] Rogers MK, Seigfried K The future of computer forensics: a needs analysis survey Computers & Security. 2004 Feb 29;23(1):12-6

- Designing procedures at a suspected crime scene to ensure that the digital evidence obtained is not corrupted.
- Data acquisition and duplication.
- Recovering deleted files and deleted partitions from digital media to extract the evidence and validate them.
- Provide guidelines for analysing digital media to preserve evidence, analysing logs and deriving conclusions, investigate network traffics and logs to correlate events, investigate wireless and web attacks, tracking emails and investigate email crimes.
- Producing computer forensic report which provides complete report on computer forensic investigation process.
- Preserving the evidence by following the chain of custody.
- Employing the rigorous procedures necessary to have forensic results stand up to scrutiny in a court of law.
- Presenting digital forensics results in a court of law as an expert witness.

1.5 BASIC CONCEPT OF COMPUTER FORENSIC

Regardless of specific case or technology used, the concept of computer forensics is constant and consists of four basic steps which include:

- ***Preparation***

Preparation includes understanding local laws, legal issues and determination of tools and procedures to employ in carrying out computer forensics tasks. This step also includes understanding the assignment at hand, preparing the team, and checking equipment.

- ***Collection***

This involves on-site acquisition of digital evidence by making binding copy of hard drives and learning the unusual or evidence collection and taking the collected evidence to the laboratory where evidence acquisition is made. Another method of collection is live forensics when evidence is collected from powered-on computers.

- ***Examination and Analysis***

This is a key area of computer forensics and involves examination of data, internet artefacts, temporary files, spool files, shortcuts, keywords search and dealing with encryption.

- ***Reporting***

This involves a court expert report being made according to valid templates. The reports are written the way the judges and prosecutors understand it.[5]

1.6 USES OF COMPUTER FORENSICS

The uses of computer forensics include the following:

- Detecting a cybercrime.
- Solving an alleged criminal activity provided the medium used in perpetrating the crime is a digital device.
- Forestalling a crime from taking place.
- Computer forensics investigations are often used to refute or support a supposition during civil, criminal and corporate litigations.
- Computer forensics is used in the private sector by companies who are undergoing internal investigations into unauthorized technical and network transgressions.

Computer forensics is used in a variety of cases such as:-

- Intellectual Property Theft
- Industrial espionage
- Employment disputes
- Fraud investigations
- Forgeries
- Bankruptcy investigations
- Inappropriate email and internet use in the workplace
- Regulatory compliance

[5] Prasanthi, B. V. "Cyber Forensic Tools: A Review" International Journal of Engineering Trends and Technology (IJETT) 41.Number-5 (2016): 6

1.7 ETHICS TO BE FOLLOWED BY DIGITAL FORENSICS EXPERT

Digital Forensic expert is an investigator that investigates the digital evidence. The task of the Digital Investigator is very crucial as any information left can lead the case in a different situation.[6] So some ethics are expected to be followed by the Digital Investigator while conducting the investigation such as:

- The investigator should not delete or alter any evidence i.e., any proof related to the case should be kept at secure place and should not be damaged.
- Should protect the computer/digital devices against viruses viz-a-viz viruses should be removed so that they don't destroy any information.
- Keep a log of all work done.
- Keep any Client Attorney information that is gained confidential.

The role of Digital Investigator in a Forensic investigation of a crime is complicated which starts at the crime scene, continues into the computer labs for deep investigation, and ends in the court where the final judgment is done. There is no scope of negligence at all.

1.8 IMPLICATIONS OF DIGITAL FORENSICS

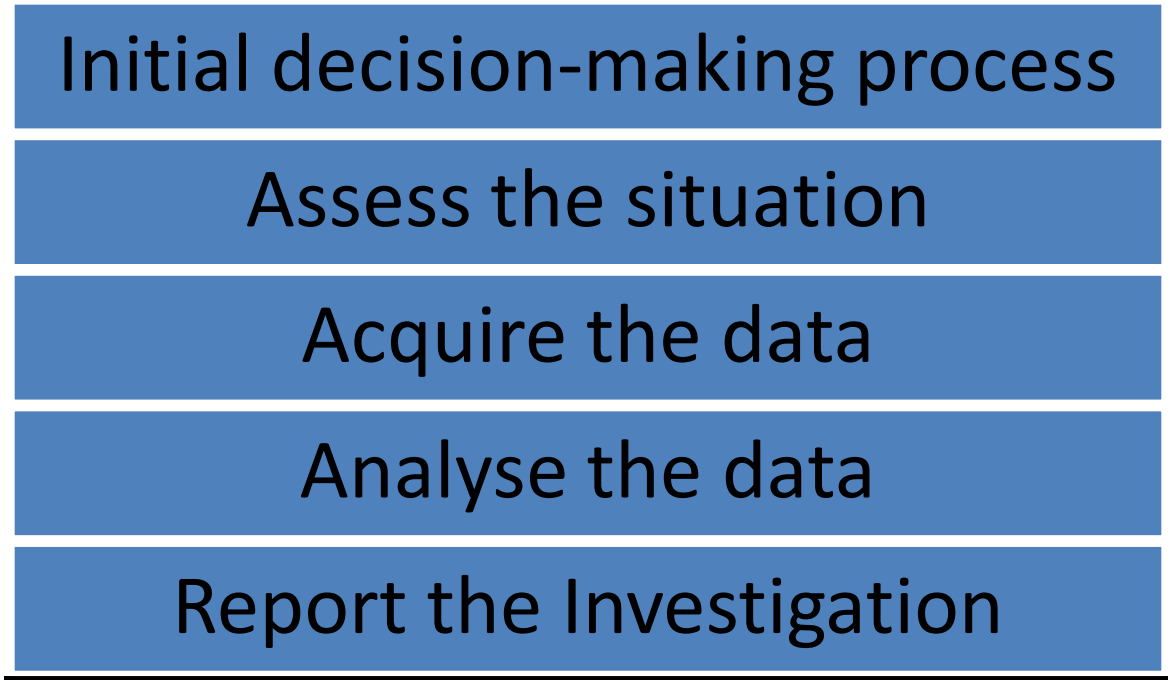
Digital forensics is commonly used in both criminal law and private investigation. Traditionally, it has been associated with criminal law, where the evidence is collected to support or oppose a hypothesis before the court of law. As with other areas of forensics, this is often a part of wider investigation spanning a number of disciplines. In some cases, the collected evidence is used as a form of intelligence gathering, used for other purposes than court proceedings.[7] As a result, intelligence gathering is sometimes held to a less strict forensic standard. In civil litigation or corporate matters, digital forensics forms part of the electronic discovery process. Forensic procedures are similar to those in criminal investigations, often with different legal requirements and limitations. Outside of the courts, digital forensics can form a part of internal corporate

[6] Sekar, Vyas, et al "Toward a framework for internet forensic analysis." ACM HotNets-III 2004

[7] Prasanthi, B V (2017). Cyber Forensic Science to Diagnose Digital Crimes- A study. International Journal of Computer Trends and Technology (IJCTT)

investigations. The main focus of digital forensics investigations is to recover objective evidence of criminal activity (termed actus reus in legal parlance). However, the diverse range of data held in digital devices can help with other areas of inquiry.

1.9 COMPUTER FORENSICS INVESTIGATION PROCESS



The investigation process of computer forensics are as follows:-

- **INITIAL DECISION-MAKING PROCESS**

  One must determine whether or not to involve law enforcement with the assistance of legal advisors. If the determination of law enforcement is needed, then the internal investigation must continue unless law enforcement officials advise otherwise. Depending on the type of incident being investigated, the primary concern should be to prevent further damage to the

organization by those person(s) who caused the incident. The investigation is important but is secondary to protecting the organization unless there are national security issues.[8]

- **ASSESS THE SITUATION**

The assessment of situation establishes the required resources for an internal investigation. There is a five-step process that must be followed which is as follows:-

a) Notify decision-makers and acquire authorization

To conduct a computer investigation, one must first need to obtain proper authorization unless existing policies and procedures provide incident response authorization. One must need to conduct a thorough assessment of the situation and define a course of action. The following are some of the best practices:

- If no written incident response policies and procedures exist, notify decision-makers and obtain written authorization from an authorized decision-maker to conduct the computer investigation.

- Document all actions you undertake that are related to this investigation. Ensure there is a complete and accurate documented summary of the events and decisions that occurred during the incident and the incident response. This documentation may ultimately be used in court to determine the course of action that was followed during the investigation.[9]

- Depending on the scope of the incident and absent any national security issues or life safety issues, the first priority is to protect the organization from further harm.

[8] Digital Forensics in Law Enforcement: A Needs Based Analysis of Indiana Agencies by Teri A. Cummins Flory (Purdue University),2016
[9] What Is Computer Forensics? (GUIDE) | Forensic Control <https://www.forensiccontrol.com/what-is-computer-forensics>

After the organization is secure, restoration of services (if needed) and the investigation of the incident are the next priorities.

Decisions made may be questioned as much as the evidence. Because computer evidence is complex, different investigations (such as those conducted by an opposing party) may make different decisions and reach different conclusions.

b) Review policies and laws

At the start of a computer investigation, it is important to understand the laws that might apply to the investigation as well as any internal organization policies that might exist. The following are the best practices:-

- Determine if you have the legal authority to conduct an investigation. Many organizations state in their policies and procedures that there is no expectation of privacy in the use of the organization's equipment, e-mail, Web services, telephone, or mail and that the company reserves the right as a condition of employment to monitor and search these resources. Such policies and procedures should be reviewed by the organization's legal advisors, and all employees, contractors, and visitors should be notified of their existence. If you are uncertain about your authority, contact your management, your legal advisors, or (if necessary) your local authorities.
- Consult with legal advisors to avoid potential issues from improper handling of the investigation.[10] These issues may include:

    - Compromising customers' personal data.
    - Violating any state or federal law, such as federal privacy rules.
    - Incurring criminal or civil liability for improper interception of electronic communications. Consider warning banners.

[10] Forensic Examination of Digital Evidence: A Guide for Law Enforcement

- Viewing sensitive or privileged information. Sensitive data that may compromise the confidentiality of customer information must only be made available as part of investigation-related documentation if it directly pertains to the investigation.

- Maintain digital copies of evidence, printouts of evidence, and the chain of custody for all evidence, in case of legal action. Preservation of the chain of custody is accomplished by having verifiable documentation that indicates who handled the evidence when they handled it, and the locations, dates, and times of where the evidence was stored. Secure storage of evidence is necessary, or custody cannot be verified.

c) Identify Investigation Team Members

Ideally, team members should be established before the team is needed for an actual investigation. It is important that investigation teams be structured appropriately and have appropriate skills. The following are the best practices for forming an investigation team:-

- Identify a person who understands how to conduct an investigation. Remember that the credibility and skills of the person performing the investigation are often scrutinized if a situation results in legal proceedings in a court of law.
- Identify team members and clarify the responsibilities of each team member.
- Assign one team member as the technical lead for the investigation. The technical lead usually has strong technical skills and is experienced in computer investigations. In investigations that involve suspected parties who are technically skilled, you might need to select investigation team members who are more skilled than the suspected parties.
- Keep the investigation team as small as possible to ensure confidentiality and to protect your organization against unwanted information leaks.
- Engage a trusted external investigation team if your organization does not have personnel with the necessary skills.

- Ensure that every team member has the necessary clearance and authorization to conduct their assigned tasks. This consideration is especially important if any third-party personnel, such as consultants, are involved in the investigation.[11]

d) Conduct a thorough assessment

Clearly documented assessment of the situation is required to prioritize your actions and justify the resources for the internal investigation. This assessment should define the current and potential business impact of the incident, identify affected infrastructure, and obtain as thorough an understanding as possible of the situation. This information will help you define an appropriate course of action. The following are the best practices to conduct a thorough assessment:-

- Use all available information to describe the situation, its potential severity, potentially affected parties, and (if available) the suspected party or parties.
- Identify the impact and sensitivity of the investigation on your organization. For example, assess whether it involves customer data, financial details, health care records, or company confidential information. Remember to evaluate its potential impact on public relations. This assessment will likely be beyond the expertise of IT and should be done in conjunction with management and legal advisors.
- Analyse the business impact of the incident throughout the investigation. List the number of hours required to recover from the incident, hours of downtime, cost of damaged equipment, loss of revenue, and value of trade secrets. Such an assessment should be realistic and not inflated. The actual costs of the incident will be determined at a later date.
- Analyse affected intangible resources, such as the future impact on reputation, customer relationships, and employee morale. Do not inflate the severity of the incident. This analysis is for informational purposes only to help understand the scope of the incident. The actual impact will be determined at a later date. This

[11] Barrett, Neil, Computer Forensics Jump Start: Computer Forensics Basics, Solomon, Sybex Printing, 2005

assessment will likely be beyond the expertise of IT and should be done in conjunction with management and legal advisors.

e) Prepare for Evidence Acquisition

A detailed document containing all information must provide a starting point for the next phase and for the final report preparation. In addition, understand that if the incident becomes more than just an internal investigation and requires court proceedings, it is possible that all processes used in gathering evidence might be used by an independent third party to try and achieve the same results. The document that provides detailed information about the situation and must include the following:-

- An initial estimate of the impact of the situation on the organization's business.
- A detailed network topology diagram that highlights affected computer systems and provides details about how those systems might be affected.
- Summaries of interviews with users and system administrators.
- Outcomes of any legal and third-party interactions.
- Reports and logs generated by tools used during the assessment phase.
- A proposed course of action.

- ACQUIRE THE DATA

Some computer investigation data is fragile, highly volatile, and can be easily modified or damaged. Therefore, one needs to ensure that the data is collected and preserved correctly prior to analysis. There is a three-step process that must be followed which is as follows:-

a) Build computer investigation toolkit

A toolkit might contain a laptop computer with appropriate software tools, operating systems and patches, application media, write-protected backup devices, blank media, basic networking equipment, and cables. Ideally, such a toolkit will be created in advance, and team members will be familiar with the tools before they have to conduct an investigation.

The following are the guidelines that needs to be followed when building and using a computer investigation toolkit:-

- Decide which tools you plan to use before you start the investigation. The toolkit will typically include dedicated computer forensics software, such as Sysinternals, Encase, The Forensic Toolkit (FTK), or ProDiscover.
- Ensure that you archive and preserve the tools. You might need a backup copy of the computer investigation tools and software that you use in the investigation to prove how you collected and analysed data.
- List each operating system that you will likely examine, and ensure you have the necessary tools for examining each of them.
- Include a tool to collect and analyse metadata.
- Include a tool for creating bit-to-bit and logical copies.
- Include tools to collect and examine volatile data, such as the system state.
- Include a tool to generate checksums and digital signatures on files and other data, such as the File Checksum Integrity Validator (FCIV) tool.
- If you need to collect physical evidence, include a digital camera in the toolkit.

b) Collect the data

Data collection of digital evidence can be performed either locally or over a network. Acquiring the data locally has the advantage of greater control over the computer(s) and data involved. However, it is not always feasible. Other factors, such as the secrecy of the investigation, the nature of the evidence that must be gathered, and the timeframe for the investigation will ultimately determine whether the evidence is collected locally or over the network.

c) Store and archive

When evidence is collected and ready for analysis, it is important to store and archive the evidence in a way that ensures its safety and integrity. The best practices for data storage and archival include the following:-

- Physically secure and store the evidence in a tamper-proof location.
- Ensure that no unauthorized person has access to the evidence, over the network or otherwise. Document who has physical and network access to the information.
- Protect storage equipment from magnetic fields. Use static control storage solutions to protect storage equipment from static electricity.
- Make at least two copies of the evidence you collected, and store one copy in a secure offsite location.
- Ensure that the evidence is physically secured as well as digitally secured.
- Clearly document the chain of custody of the evidence. Create a check-in / check-out list that includes information such as the name of the person examining the evidence, the exact date and time they check out the evidence, and the exact date and time they return it.

- **ANALYSE THE DATA**

There is a three step process to analyse the evidence that is gathered during the acquisition of data phase of an internal investigation.

a) Analyse network data

When network analysis is required, the following procedure is followed:-

- Examine network service logs for any events of interest. Typically, there will be large amounts of data, so you should focus on specific criteria for events of interest such as username, date and time, or the resource being accessed.
- Examine firewall, proxy server, intrusion detection system (IDS), and remote access service logs. Many of these logs contain information from monitored incoming and outgoing connections and include identifying information, such as IP address, time of the event, and authentication information.

- View any packet sniffer or network monitor logs for data that might help you determine the activities that took place over the network. In addition, determine whether connections you examine are encrypted-because you will not be able to read the contents of an encrypted session.

b) Analyse Host Data

Host data includes information about such components as the operating system and applications. The following procedure is used to analyse the copy of the host data obtained in the acquisition of the data phase.

- Identify what you are looking for. There will likely be a large amount of host data, and only a portion of that data might be relevant to the incident. Therefore, you should try to create search criteria for events of interest.
- Examine the operating system data, including clock drift information, and any data loaded into the host computer's memory to see if you can determine whether any malicious applications or processes are running or scheduled to run.
- Examine the running applications, processes, and network connections.

c) Analyse storage media

The following procedure is to be followed to extract and analyse data from the storage media collected:-

- Whenever possible, perform offline analysis on a bit-wise copy of the original evidence.
- Determine whether data encryption was used, such as the Encrypting File System (EFS) in Microsoft Windows. Several registry keys can be examined to determine whether EFS was ever used on the computer. If you suspect data encryption was used, then you need to determine whether or not you can actually recover and read the encrypted data.

- If necessary, uncompress any compressed files and archives. Although most forensic software can read compressed files from a disk image, you might need to uncompress archive files to examine all files on the media you are analysing.
- Create a diagram of the directory structure. It might be useful to graphically represent the structure of the directories and files on the storage media to effectively analyse the files.
- Identify files of interest.
- Examine the registry, the database that contains Windows configuration information, for information about the computer boot process, installed applications (including those loaded during startup), and login information such as username and logon domain.
- Study the metadata of files of interest, using tools such as Encase by Guidance Software, The Forensic Toolkit (FTK) by AccessData, or ProDiscover by Technology Pathways. File attributes such as timestamps can show the creation, last access, and last written times, which can often be helpful when investigating an incident.
- Use file viewers to view the content of the identified files, which allow you to scan and preview certain files without the original application that created them. This the approach protects files from accidental damage and is often more cost-effective than using the native application. Note that file viewers are specific to each type of file; if a viewer is not available, use the native application to examine the file.[12]

- **REPORT THE INVESTIGATION**

There is a two-step process to organize the information that you gather and the documentation that you create throughout a computer investigation.

a) Gather and Organize information

The following procedure is to be followed to gather and organize the required documentation for the final report.

[12] Legal Aspects of Digital Forensics by Daniel J. Ryan and Gal Shpantzer

- Gather all documentation and notes from the Assess, Acquire, and Analyse phases. Include any appropriate background information.
- Identify parts of the documentation that are relevant to the investigation.
- Identify facts to support the conclusions you will make in the report.
- Create a list of all evidence to be submitted with the report.
- List any conclusions you wish to make in your report.
- Organize and classify the information you gather to ensure that a clear and concise report is the result.

b) Write a report

The following list identifies recommended report sections and information that should be included:-

- Purpose of report
- Author of report
- Incident summary
- Evidence
- Details i.e., description of what evidence was analysed and the analysis methods that were used.
- Conclusion
- Supporting documents

1.10 LET'S SUM UP

In this chapter, we have studied the evolution of computer forensics along with the basic concepts and objectives of computer forensics. We also studied the uses and ethics that need to be followed by the digital forensics expert. Finally, we ended our discussion with the Computer Forensics Investigation process.

1.11 FURTHER READING

- P. Y. S. B. D. C. A. U. Bansal, "Cyber Forensics-The art of Decoding the Binary Digits," International Journal of Emerging Technology and advanced engineering, vol. 2.
- Rogers MK, Seigfried K. The future of computer forensics: a needs analysis survey. Computers Security 2004 Feb;23(1): 12-16.
- MansonD,CarlinA,Ramos S,GygerA,KaufmanM,TreicheltJ. Is the open way a better way? Digital Forensics using Open Source Tools. Proceedings of the 40th Hawaii International Conference on System Sciences, 2007.
- Karyda M, Mitrou L. Internet forensics: legal and technical issues. Second International Workshop on Digital Forensics and Incident Analysis (WDFIA), 2007.
- Garfinkel SL. Automating Disk Forensic Processing with SleuthKit, XML and Python, 2009. Fourth IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering. Conference at Berkeley, California, USA.

1.12 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. What are the objectives of computer forensics?

The objectives of Computer forensics are to provide guidelines for:

- Following the first responder procedure and access the victim's computer after incident.
- Designing procedures at a suspected crime scene to ensure that the digital evidence obtained is not corrupted.
- Data acquisition and duplication.
- Recovering deleted files and deleted partitions from digital media to extract the evidence and validate them.
- Provide guidelines for analysing digital media to preserve evidence, analysing logs and deriving conclusions, investigate network traffics and logs to correlate events, investigate wireless and web attacks, tracking emails and investigate email crimes.
- Producing computer forensic report which provides a complete report on computer forensic investigation process.
- Preserving the evidence by following the chain of custody.
- Employing the rigorous procedures necessary to have forensic results stand up to scrutiny in a court of law.
- Presenting digital forensics results in a court of law as an expert witness.

2. What are the uses of computer forensics?

The uses of computer forensics include the following:

- Detecting a cybercrime.
- Solving an alleged criminal activity provided the medium used in perpetrating the crime is a digital device.
- Forestalling a crime from taking place.
- Computer forensics investigations are often used to refute or support a supposition during civil, criminal and corporate litigations.
- Computer forensics is used in the private sector by companies who are undergoing internal investigations into unauthorized technical and network transgressions.

3. What are the implications of digital forensics?

Digital forensics is commonly used in both criminal law and private investigation. Traditionally, it has been associated with criminal law, where the evidence is collected to support or oppose a hypothesis before the court of law. As with other areas of forensics, this is often a part of wider investigation spanning a number of disciplines. In some cases, the collected evidence is used as a form of intelligence gathering, used for other purposes than court proceedings. As a result, intelligence gathering is sometimes held to a less strict forensic standard. In civil litigation or corporate matters, digital forensics forms part of the electronic discovery process. Forensic procedures are similar to those in criminal investigations, often with different legal requirements and limitations. Outside of the courts, digital forensics can form a part of internal corporate investigations. The main focus of digital forensics investigations is to recover objective evidence of criminal activity (termed actus reus in legal parlance). However, the diverse range of data held in digital devices can help with other areas of inquiry.

1.13 ACTIVITY

Explain the different phases of investigation process with the help of diagram? Explain it with an example. (1000-1500 words)