1

COMPUTER FORENSIC

Unit Structure

1.0 OBJECTIVE

This chapter would make you understand the following concept:

- Standard Procedure for computer forensic
- Bit Stream copy or forensic copy
- Procedures for Corporate High-Tech Investigations
- Data Acquisition
- Computer forensic Tools

1.1 INTRODUCTION TO COMPUTER FORENSIC:

- Computer forensics involves obtaining and analyzing digital information for use as evidence in civil, criminal, or administrative cases.
- The Fourth Amendment to the U.S. Constitution (and each state's constitution) protects everyone'sright to be secure in their person, residence, and property from search and seizure.
- Similarly, computer forensics differs from data recovery, which involves recovering data from a computer that was deleted by mistake or lost during a power surge.
- There are two kinds of evidence: inculpatory (in criminal cases, the expression is "incriminating") and exculpatory (in which the suspect might be cleared).
- Investigators often examine a computer disk not knowing whether it contains evidence.

1.2 STANDARD PROCEDURE

The standard procedure for conducting computer forensicsinvolves the following major five tasks:

1. Preparing a Computer Investigation
2. Takinga systematic approach
3. procedure for corporate High-Tech investigation
4. Conducting an investigation
5. Completing the case

1.2.1 Preparing a Computer Investigation

- A computer forensics professional's role is to gather evidence from a suspect's computer.
- Upon discovering evidence that a crime or policy violation has been committed, you begin preparing an investigation.
- In this process, the suspect's computer is investigated and the evidence is preserved.
- The first step inconducting an investigation is to follow a standard procedure.
- By approaching each case systematically, you can evaluate the evidencecarefully and document the chain of evidence, or chain of custody, which is the routetheevidence takes from the time you find it until the case is closed or goes to court.
- There can be two types of casesthat you might be investigating - one involving a **computer crime** and anotherinvolving a **company policy violation**.
- Computers and computer components are often found by law enforcement officers as they investigate crimes.
- The lead detective on the case wants you to examine the computer to find and organize datathat could be evidence of a crime.
- Companies regularlyestablish policies for employee use of computers.
- Company time can be wasted when employees surf the Internet, send personal e-mail, or use company computers during work hours.
- Computer forensics specialists are often hired to investigate policy violations because lost time can cost companies millions of dollars.

1.2.2 Taking a Systematic Approach

When preparing a case, you can apply standard systems analysis steps, explained in the following list, to problem-solving.

- **Make an initial assessment about the type of case you are investigating**—assess the type of case you are handling by talking to those involved and asking questions. Have law enforcement (police) or company security officers already seized the computer, disks, and other components? Do you need to visit an office or another location? Was the computer used to commit a crime, or does it contain evidence about another crime?

- **Determine a preliminary design or approach to the case**—Outline the general steps you need to follow to investigate the case. If the suspect is an employee and you need to acquire his or her system, determine whether you can seize the computer during work hours or have to wait until evening or weekend hours. If you're preparing a criminal case, determine what information law enforcement officers have already gathered.

- **Create a detailed checklist**—Refine the general outline by creating a detailed checklist of steps and an estimated amount of time for each step. This outline helps you stay on track during the investigation.

- **Determine the resources you need**—Based on the OS of the computer you're investigating, list the software you plan to use for the investigation, noting any other software or tools you might need.

- **Obtain and copy an evidence drive**—In some cases, you might be seizing multiple computers along with Zip disks, Jaz drives, CDs, USB drives, PDAs, and other removable media. Make a forensic copy of the disk.

- **Identify the risks**—List the problems you normally expect in the type of case you're handling. This list is known as a standard risk assessment. For example, if the suspect seems knowledgeable about computers, he or she might have set up a logon scheme that shuts down the computer or overwrites data on the hard disk when someone tries to change the logon password.

- **Mitigate or minimize the risks**—identify how you can minimize the risks. For example, if you are working with a computer on which the suspect has likely password protected the hard drive, you can make multiple copies of the original media before starting. Then if you destroy a copy during the process of retrieving information from the disk, you have additional copies.

- **Test the design**—Review the decisions you've made and the steps you've completed. If you have already copied the original media, a standard part of testing the design involves comparing hash values ensure that you copied the original media correctly.

- **Analyze and recover the digital evidence**—using the software tools and other resources you've gathered, and making sure you've addressed any risks and obstacles, examine the disk to find digital evidence.

- **Investigate the data you recover**—View the information recovered from the disk, including existing files, deleted files, and e-mail, and organize the files to help prove the suspect's guilt or innocence.
- **Complete the case report**—Write a complete report detailing what you did and what you found.
- **Critique the case**—Self-evaluation is an essential part of professional growth. After you complete a case, review it to identify successful decisions and actions and determine how you could have improved your performance.

1.2.2.1 Assessing the Case

In the company-policy violation case, you have been asked to investigate Raju. Daya from the IT Department seize all of Raju's storage media that might contain information about his whereabouts. After talking to Raju's co-workers, Daya learned that Raju has been conducting a personal business on the side using company computers. Therefore, the focus of the case has changed from a missing person to a possible employee abuse of corporate resources.

You can begin assessing the company policy violation case as follows:

- **Situation**— for eg: Employee abuse case.
- **Nature of the case**—Side business conducted on the employer's computer.
- **Specifics of the case**—The employee is reportedly conducting a side business on his employer's computer that involves registering domain names for clients and setting up their Web sites at local ISPs. Co-workers have complained that he has been spending too much time on his own business and not performing his assigned work duties. Company policy states that all company-owned computing assets are subject to inspection by company management at any time. Employees have no expectation of privacy when operating company computer systems.
- **Type of evidence**—Small-capacity USB drive.
- **Operating system**—Microsoft Windows XP.
- **Known disk format**—FAT16.
- **Location of evidence**—One USB drive recovered from the employee's assigned computer.

1.2.2.2 Planning Your Investigation

As soon as you have identified the requirements of the Domain Name case, you can plan your approach. You have already determined the kind

of evidence you need; now you can identify the specific steps to gather the evidence, establish a chain of custody, and perform the forensic analysis.

Most of these steps are listed below:

1. Acquire the USB drive from Raju's manager.
2. Complete an evidence form and establish a chain of custody.
3. Transport the evidence to your computer forensics lab.
4. Place the evidence in an approved secure container.
5. Prepare your forensic workstation.
6. Retrieve the evidence from the secure container.
7. Make a forensic copy of the evidence drive (in this case, the USB drive).
8. Return the evidence drive to the secure container.
9. Process the copied evidence drive with your computer forensics tools.

To document the evidence, you record details about the media, including who recovered the evidence and when and who possessed it and when. Use an **evidence custody form**, also called a **chain-of-evidence form**, which helps you document what has and has not been done with the original evidence and forensic copies of the evidence.

An evidence custody form usually contains the following information:

- **Case number**: Number the organization assigns when an investigation is initiated.

Figure:1.1 A sample multi-evidence form used in a corporate environment

Corporation X
Security Investigations
This form is to be used for one to ten pieces of evidence

Case No.:		Investigating Organization:	
Investigator:			
Nature of Case:			
Location where evidence was obtained:			

Description of evidence:	Vendor Name	Model No./Serial No.
Item #1		
Item #2		
Item #3		
Item #4		
Item #5		
Item #6		
Item #7		
Item #8		
Item #9		
Item #10		

Evidence Recovered by:		Date & Time:	
Evidence Placed in Locker:		Date & Time:	

Item #	Evidence Processed by	Disposition of Evidence	Date/Time
			Page __ of ___

- **Investigating organization:** The name of the organization. In large corporations with global facilities, several organizations might be conducting investigations in different geographic areas.
- **Investigator:** The name of the investigator assigned to the case. If many investigators are assigned, specify the lead investigator's name.
- **Nature of case:** A short description of the case. For example, in the corporate environment, it might be "Data recovery for corporate litigation" or "Employee policy violation case."
- **Location evidence was obtained:** The exact location where the evidence was collected. If we're using multi-evidence forms, a new form should be created for each location.
- **Description of evidence:** A list of the evidence items, such as "hard drive, 20 GB" or "one USB drive, 128 MB." On a multi-evidence form, write a description for each item of evidence we acquire.
- **Vendor name:** The name of the manufacturer of the computer evidence.
- **Model number or serial number:** List the model number or serial number (if available) of the computer component. Many computer components, including hard drives, memory chips, and expansion slot cards, have model numbers but not serial numbers.
- **Evidence recovered by:** The name of the investigator who recovered the evidence. The chain of custody for evidence starts with this information. The person placing his or her name on this line is responsible for preserving, transporting, and securing the evidence.
- **Date and time:** The date and time the evidence was taken into custody. This information establishes exactly when the chain of custody starts.
- **Evidence placed in locker:** Specifies which approved secure container is used to store evidence and when the evidence was placed in the container.
- **Item #/Evidence processed by/Disposition of evidence/Date/Time:** When we or another authorized investigator retrieves evidence from the evidence locker for processing and analysis, list the item number and the name, and then describe what was done to the evidence.
- **Page:** The forms used to catalog all evidence for each location should have page numbers. List the page number, and indicate the total number of pages for this group of evidence.

A single-evidence form, which lists only one piece of evidence per page. This form gives more flexibility in tracking separate pieces of evidence for

the chain-of-custody log. It also has more space for descriptions, which is helpful when finalizing the investigation and creating a case report. With this form, we can accurately account for what was done to the evidence and what was found. Use evidence forms as a reference for all actions taken during the investigative analysis.

1.2.2.3 Securing Your Evidence

1. Large evidence bags, tape, tags, and labels can be used to secure and catalog evidence in large computer components.
2. When gathering products to secure your computer evidence, make sure they are safe and effective to use on computer components. Be cautious when handling any computer component to avoid damaging the component or coming into contact with static electricity, which can destroy digital data.
3. For this reason, make sure you use anti- static bags when collecting computer evidence.
4. Consider using an antistatic pad with an attached wrist strap, too. Both help prevent damage to computer evidence.
5. Be sure to place computer evidence in a well-padded container. Padding prevents damage to the evidence as you transport it to your secure evidence locker, evidence room, or computer lab.
6. Securing evidence often requires building secure containers. If the computer component is large and contained in its own casing, such as a CPU cabinet, you can use evidence tape to seal all openings on the cabinet.
7. As a standard practice, you should write your initials on the tape before applying it to the evidence.
8. When collecting computer evidence, make sure you have a safe environment for transporting and storing it until a secure evidence container is available.

1.2.3 Procedures for Corporate High-Tech Investigations

- A high-tech investigation requires formal procedures and informal checklists to cover all important issues.
- These procedures are necessary to ensure that correct techniques are used in an investigation.
- Use informal checklists to be certain that all evidence is collected and processed properly.

1.2.3.1 Employee Termination Cases

- Investigations for termination cases usually involve employee abuse of corporate assets.

- Incidents that create an unfriendly work environment, such as viewing pornography in the workplace and sending inappropriate e-mail messages, are the main types of cases investigated.
- Consult the organization's general counsel and Human Resources Department for specific directions on how to handle these investigations.
- The following sections provide a summary of key points to consider when investigating that could result in the termination of an employee.

1.2.3.2 Internet Abuse Investigations

In order to investigate Internet abuse, you will need the following information:

- The organization's Internet proxy server logs.
- Suspect computer's IP address obtained from your organization's network administrator.
- Suspect computer's disk drive.
- Your preferred computer forensics analysis tool.

Following are the steps to follow when investigating Internet abuse:

1. Use the standard forensic analysis techniques and procedures.
2. Using tools such as Data Lifter or Forensic Toolkit's Internet keyword search option, extract all Web page URL information.
3. Contact the network firewall administrator and request a proxy server log, if it's available, of the suspect computer's network device name or IP address for the dates of interest. Confirm with your organization's network administrator that these logs are maintained and that the time to live (TTL) is set for IP addresses assigned through Dynamic Host Configuration Protocol (DHCP).
4. Compare the data recovered from forensic analysis to the proxy server log data to confirm that they match.
5. If the URL data matches the proxy server log and the forensic disk examination, continue analyzing the suspect computer's drive data, and collect any relevant downloaded inappropriate pictures or Web pages that support the allegation. If there are no matches between the proxy server logs, and the forensic examination shows no contributing evidence, report that the allegation is unsubstantiated.

Before investigating an Internet abuse case, it is important to know your state or country's privacy laws.

1.2.3.3 E-mail Abuse Investigations

E-mail investigations typically include spam, inappropriate and offensive message content, and harassment or threats.

Organizations must define a policy for e-mail records, just as they do for other computer evidence data.

The followings are the list that is needed for investigating e-mail abuse case:

- An electronic copy of the offending e-mail that contains message header data; consult with your e-mail server administrator
- If available, e-mail server log records; consult with your e-mail server administrator to see whether they are available
- For e-mail systems that store users' messages on a central server, access to the server; consult with your e-mail server administrator
- For e-mail systems that store users' messages on a computer as an Outlook .pst or .ost file, for example, access to the computer so that you can perform a forensic analysis on it
- Your preferred computer forensics analysis tool, such as Forensic Toolkit or ProDiscover

The recommended procedure for e-mail investigations are as follows:

1. **For computer-based e-mail data files**, such as Outlook .pst or .ost files, use the standard forensic analysis techniques and procedures for the drive examination.
2. **For server-based e-mail data files**, contact the e-mail server administrator and obtain an electronic copy of the suspect and victim's e-mail folder or data.
3. **For Web-based e-mailinvestigations**, such as Hotmail or Gmail, use tools such as Forensic Toolkit's Internet keyword search option to extract all related e-mail address information.
4. **Examine header data** of all messages of interest to the investigation.

1.2.3.4 Attorney-Client Privilege Investigations

- When conducting a computer forensics analysis under attorney-client privilege (ACP) rules for an attorney, you must keep all findings confidential.
- The attorney you're working for is the final authority over the investigation.
- For investigations of this nature, attorneys typically request that you extract all data from drives.

- It is your responsibility to obey with the attorney's directions.
- Drives can contain large amounts of data, so the attorney will want to know everything of interest on them.
- Many attorneys like to have printouts of the data you have recovered, but printouts can present problems when you have log files with several thousand pages of data or CAD drawing programs that can be read only by proprietary programs.

The following list are the basic steps for conducting an ACP case:

1. **Request a memorandum from the attorney** directing to start the investigation. The memorandum must state that the investigation is privileged communication and list the name and any other associates' names assigned to the case.
2. **Request a list of keywords** of interest to the investigation.
3. After we have received the memorandum, initiate the investigation and analysis. Any findings we made before receiving the memorandum are subject to discovery by the opposing attorney.
4. For drive examinations, **make two bit-stream images of the drive** using a different tool for each image, such as Encase for the first and ProDiscover or SafeBack for the second. If we have large enough storage drives, make each bit-stream image uncompressed so that if it becomes corrupt, we can still examine uncorrupted areas with the preferred forensic analysis tool.
5. If possible, **compare hash values on all files on the original and re-created disks**. Typically, attorneys want to view all data, even if it's not relevant to the case. Many GUI forensics tools perform this task during bitstream imaging of the drive.
6. Methodically **examine every portion of the drive** (both allocated and unallocated data areas) and extract all data.
7. **Run keyword searches** on allocated and unallocated disk space. Follow up the search results to determine whether the search results contain information that supports the case.
8. For Windows OSs, use special tools to analyze and extract data from the Registry, such as AccessData Registry Viewer or a Registry viewer program. Use the Edit, Find menu option in Registry Editor, for example, to search for keywords of interest to the investigation.
9. For binary files such as CAD drawings, locate the correct program and, if possible, make printouts of the binary file content. If the files are too large, load the specialty program on a separate workstation with the recovered binary files so that the attorney can view them.

10. For unallocated data (file slack space or free space) recovery, use a tool that removes or replaces nonprintable data, such as X-Ways Forensics Specialist Gather Text function.

11. Consolidate all recovered data from the evidence bit-stream image into well-organized folders and subfolders. Store the recovered data output, using a logical and easy-to-follow storage method for the attorney or paralegal.

1.2.3.5 Media Leak Investigations

The following are the guidelines for media leak investigations:

- Examine e-mail, both the organization's e-mail servers and private e-mail accounts (Hotmail, Yahoo!, Gmail, and so on), on company-owned computers.
- Examine Internet message boards, and search the Internet for any information about the company or product. Use Internet search engines to run keyword searches related to the company, product, or leaked information.
- Examine proxy server logs to check for log activities that might show use of free e-mail services, such as Gmail. Trace back to the specific workstations where these messages originated and perform a forensic analysis on the drives to help determine what was communicated.
- Examine known suspects' workstations, perform computer forensics examinations on persons of interest, and develop other leads on possible associates.
- Examine all company phone records for any calls to known media organizations.

The following list outlines steps to take for media leaks:

1. Interview management privately to get a list of employees who have direct knowledge of the sensitive data.
2. Identify the media source that published the information.
3. Review company phone records to see who might have had contact with the news service.
4. Obtain a list of keywords related to the media leak.
5. Perform keyword searches on proxy and e-mail servers.
6. Discreetly conduct forensic disk acquisitions and analysis of employees of interest.
7. From the forensic disk examinations, analyze all e-mail correspondence and trace any sensitive messages to other people who haven't been listed as having direct knowledge of the sensitive data.

8. Expand the discreet forensic disk acquisition and analysis for any new persons of interest.

9. Consolidate and review the findings periodically to see whether new clues can be discovered.

10. Report findings to management routinely, and discuss how much further to continue the investigation.

1.2.3.6 Industrial Espionage Investigations

The following list shows staff that we may need when planning an industrial espionage investigation:

- The computing investigator who is responsible for disk forensic examinations
- The technology specialist who is knowledgeable about the suspected compromised technical data
- The network specialist who can perform log analysis and set up network monitors to trap network communication of possible suspects
- The threat assessment specialist (typically an attorney) who is familiar with federal and state laws and regulations related to ITAR or EAR and industrial espionage

The following are the guidelines when initiating an international espionage investigation:

- Determine whether this investigation involves a possible industrial espionage incident, and then determine whether it falls under ITAR or EAR.
- Consult with corporate attorneys and upper management if the investigations must be conducted discreetly.
- Determine what information is needed to substantiate the allegation of industrial espionage.
- Generate a list of keywords for disk forensics and network monitoring.
- List and collect resources needed for the investigation.
- Determine the goal and scope of the investigation; consult with management and the company's attorneys on how much work we should do.
- Initiate the investigation after approval from management, and make regular reports of activities and findings.

The following are planning considerations for industrial espionage investigations:

- Examine all e-mail of suspected employees, both company-provided e-mail and free Web-based services.
- Search Internet newsgroups or message boards for any postings related to the incident.
- Initiate physical surveillance with cameras on people or things of interest to the investigation.
- If available, examine all facility physical access logs for sensitive areas, which might include secure areas where smart badges or video surveillance recordings are used.
- If there's a suspect, determine his or her location in relation to the vulnerable asset that was compromised.
- Study the suspect's work habits.
- Collect all incoming and outgoing phone logs to see whether any unique or unusual places were called.

1.2.4 Conducting an Investigation

Start by gathering the resources you identified in your investigation plan. You need the following items:

- Original storage media
- Evidence custody form
- Evidence container for the storage media, such as an evidence bag
- Bit-stream imaging tool; in this case, the ProDiscover Basic acquisition utility
- Forensic workstation to copy and examine the evidence
- Secure evidence locker, cabinet, or safe

1.2.5 Completing the Case

- After analyzing the disk, you can retrieve deleted files, e-mail, and items that have been purposefully hidden.
- Now that you have retrieved and analyzed the evidence, you need to write the final report.
- When you write your report, state what you did and what you found. The report you generated in ProDiscover gives you an account of the steps you took. As part of your final report, include the ProDiscover report file to document your work.

- A computing investigation should produce the same results if you repeat the steps taken. This capability is referred to as repeatable findings and without it, your work product has no value as evidence.
- Keep a written journal of everything you do. Your notes can be used in court.
- Basic report writing involves answering the six Ws: **who, what, when, where, why, and how.**
- Your organization might have templates to use when writing reports. You must describe your analysis' findings in your report based on the needs and requirements of your organization.

1.3 INCIDENT VERIFICATION AND SYSTEM IDENTIFICATION (SECURING A COMPUTER INCIDENT OR CRIME SCENE)

- Investigators secure an incident or crime scene to preserve the evidence and to keep information about the incident or crime confidential. Information made public could risk the investigation.
- If you're in charge of securing a computer incident or crime scene, use yellow barrier tape to prevent bystanders from accidentally entering the scene.
- Use police officers or security guards to prevent others from entering the scene. Legal authority for a corporate incident scene includes trespassing violations; for a crime scene, it includes obstructing justice or failing to comply with a police officer.
- Access to the scene should be restricted to only those people who have a specific reason to be there.
- Typically, incidents or crime scenes are secured in order to extend control beyond the immediate area of the incident.
- Using this technique, you avoid omitting parts of the scene that may be important.
- For major crime scenes, computer investigators are not usually responsible for defining a scene's security perimeter.
- As part of these cases, other specialists and detectives collect physical evidence and record the scene.
- For incidents primarily involving computers, the computers can be a crime scene within a crime scene, containing evidence to be processed.
- Evidence is commonly lost or corrupted because of professional curiosity, which involves police officers and other professionals who aren't part of the crime scene processing team.

- Their presence could contaminate the scene directly or indirectly.
- Always remember that **professional curiosity** can destroy or corrupt evidence, including digital evidence.
- When working at an incident or crime scene, be aware of what you're doing and what you have touched, physically or virtually.

For example, during one homicide investigation, the lead detective collected a good latent fingerprint from the crime scene. He compared it with the victim's fingerprints and those of others who knew the victim. He couldn't find a fingerprint matching the latent fingerprint from the scene. The detective suspected he had the murderer's fingerprint and kept it on file for several years until his police department purchased an Automated Fingerprint Identification Systems (AFIS) computer. During acceptance testing, the software vendor processed sample fingerprints to see how quickly and accurately the system could match fingerprints in the database. The detective asked the acceptance testing team to run the fingerprint he found at the homicide scene. He believed the suspect's fingerprints were in the AFIS database. The acceptance testing team complied and within minutes, AFIS found a near-perfect match of the latent fingerprint: It belonged to the detective.

1.4 RECOVERY OF ERASED AND DAMAGED DATA (DATA ACQUISITION)

- Data acquisition means recovering or acquiring data from electronic media.
- Data might be erased or it may damage in the electronic media.
- Data acquisition is the process of copying data.
- For computer forensics, Data Acquisition is the task of collecting digital evidence from electronic media.
- There are **two types of data acquisition: static acquisitions and live acquisitions**.
- Typically, a **static acquisition** is done on a computer seized during a police raid.
- If the computer has an encrypted drive, a **live acquisition** is done if the password or pass-phrase is available—meaning the computer is powered on and has been logged on to by the suspect.

1.4.1 Data Encryption and Compression

- The future of data acquisitions is shifting toward live acquisitions because of the use of disk encryption with newer operating systems (OSs).

- Digital investigations are increasingly concerned with collecting any data that is active in a suspect's computer RAM, in addition to encryption concerns.
- The processes and data integrity requirements for static and live acquisitions are the same.
- Live acquisitions are not capable of repeatable processes, which are essential for collecting digital evidence.
- With static acquisitions, if we have preserved the original media, making a second static acquisition should produce the same results.
- The data on the original disk is not altered, no matter how many times an acquisition is done.
- Making a second live acquisition while a computer is running collects new data as OS changes dynamically.
- The goal when acquiring data for a static acquisition is to preserve the digital evidence.
- Many times, we have only one chance to create a reliable copy of disk evidence with a data acquisition tool.Furthermore, failures do occur, so we need to learn several acquisition methods and tools.
- We should always search for newer and better tools to ensure the integrity of the forensics acquisitions.

1.4.2 Storage Formats for Digital Evidence

- The data acquired by a computer forensics acquisition tool is stored as an image file in one of **three formats**.
- Two formats are open source and the third is proprietary.
- Many computer forensics acquisition tools create a disk-to-image file in an older open-source format, known as raw, as well as their own proprietary format.
- The new open-source format, Advanced Forensic Format (AFF), is starting to gain recognition from computer forensics examiners.

1. Raw Format:

- Examiners performed a bit-by-bit copy from one disk to another disk the same size or larger.
- As a practical way to preserve digital evidence, vendors (and some OS utilities, such as the Linux/UNIX dd command) made it possible to write bit-stream data to files.

- This copy technique creates simple sequential flat files of a suspect drive or data set. The output of these flat files is referred to as a raw format.
- This format has unique advantages and disadvantages to consider when selecting an acquisition format.

Advantages: -

1. Fast data transfers

2. Capability to ignore minor data read errors on the source drive.

Disadvantage: -

1. It requires as much storage space as the original disk or data set.

2. some raw format tools, typically freeware versions, might not collect marginal (bad) sectors on the source drive, meaning they have a low threshold of retry reads on weak media spots on a drive.

Several commercial acquisition tools can produce raw format acquisitions and typically provide a validation check by using Cyclic Redundancy Check (CRC-32), Message Digest 5 (MD5), and Secure Hash Algorithm (SHA-1 or newer) hashing functions.

2. Proprietary Formats:

- Proprietary formats typically offer several features that complement the vendor's analysis tool, such as the following: -

1. The option to compress or not compress image files of a suspect drive, thus saving space on the target drive.

2. The capability to split an image into smaller segmented files for archiving purposes, such as to CDs or DVDs, with data integrity checks integrated into each segment.

3. The capability to integrate metadata into the image file, such as date and time of the acquisition, hash value (for self-authentication) of the original disk or medium, investigator or examiner name, and comments or case details.

The disadvantage of proprietary format acquisitions is:-

1. The inability to share an image between different vendors' computer forensics analysis tools.

2. File size limitation for each segmented volume.

3. Advanced Forensic Format:

- **Dr. Simson L. Garfinkel** from Basis Technology Corporation have developed a new open source acquisition format called **Advanced Forensic Format (AFF).**

- This format has the following design goals: -

1. Creating compressed or uncompressed image files
2. No size restriction for disk-to-image files
3. Providing space in the image file or segmented files for metadata
4. Simple design with extensibility
5. Open source for multiple computing platforms and OSs
6. Offer internal consistency checks for self-authentication

- File extensions include. afd for segmented image files and .afm for AFF metadata.
- Because AFF is open source, computer forensics vendors will have no implementation restrictions on this format.

1.4.3 Determining the Best Acquisition Method

There are two types of acquisitions: static acquisitions and live acquisitions.

- Typically, a static acquisition is done on a computer seized during a police raid, for example.
- If the computer has an encrypted drive, a live acquisition is done if the password or passphrase is available—meaning the computer is powered on and has been logged on to by the suspect.
- Static acquisitions are always the preferred way to collect digital evidence.
- In some situations, Static Acquisition are limited, such as an encrypted drive readable only while the computer is powered on or a networked computer.
- For both types of acquisitions, data can be collected with four methods:

1. creating a disk-to- image file,
2. creating a disk-to-disk copy,
3. creating a logical disk-to-disk or disk-to-data file,
4. creating a sparse copy of a folder or file.

- Creating a **disk-to-image file** is the most common method and offers the most flexibility for the investigation. With this method, we can make one or many copies of a suspect drive.
- These copies are bit-for-bit replications of the original drive.

- Sometimes we cannot make a disk-to-image file because of hardware or software errors or incompatibilities. This problem is more common when we have to acquire older drives.
- For these drives, we may have to create a **disk-to-disk copy** of the suspect drive.
- Several imaging tools can copy data exactly from an older disk to a newer disk. By using these programs, the target disk's geometry can be adjusted (its cylinder, head, and track configurations) to match the original suspect disk.
- Collecting evidence from a large drive can take several hours. If time is limited, consider using a **logical acquisition or sparse acquisition** data copy method.
- A **logical acquisition** captures only specific files of interest to the case or specific types of files.
- A **sparse acquisition** is similar but also collects remains of unallocated (deleted) data. This method is used only when we don't need to examine the entire drive.
- In electronic discovery for the purpose of process, a logical acquisition is becoming the preferred method, especially with large data storage systems.
- To determine which acquisition method to use for an investigation, consider the size of the source (suspect)disk.
- If the source disk is very large, such as 500 GB or more, make sure we have a target disk that can store a disk-to-image file of the large disk.
- If we do not have a target disk of comparable size, review alternatives for reducing the size of data to create a verifiable copy of the suspect drive.
- When working with large drives, an alternative is using tape backup systems. Snap-Back and SafeBack have special software drivers designed to write data from a suspect drive to a tape backup system through standard PCI SCSI cards.
- The advantage of this type of acquisition is that there's no limit to the size of data that can be acquired.
- The one big disadvantage, especially with microprocessor systems, is that it can be slow and time consuming.

1.4.4 Contingency Planning for Image Acquisitions

- As we are working with electronic data, we need to take precautions to ensure its security.

- We should also make contingency plans in situation software or hardware doesn't work or we encounter a failure during an acquisition.
- The most common and time-consuming technique for preserving evidence is creating a duplicate of your disk-to-image file. Many computer investigators do not make duplicates of their evidence because they don't have enough time or resources to make a second image. However, if the first copy does not work correctly, having a duplicate is worth the effort and resources. Be sure you take steps to lessen the risk of failure in your investigation.
- As a standard practice, make at least two images of the digital evidence you collect.
- If you have more than one imaging tool, make the first copy with one tool and the second copy with the other tool.
- Many acquisition tools do not copy data in the host protected area (HPA) of a disk drive. For these situations, consider using a hardware acquisition tool that can access the drive at the BIOS level.
- As part of your contingency planning, you must be prepared to deal with encrypted drives.

1.4.5 Using Acquisition Tools

- Many computer forensics software vendors have developed acquisition tools that run in Windows.
- These tools make acquiring evidence from a suspect drive more convenient, especially when we use them with hot-swappable devices, such as USB-2, FireWire 1394A and 1394B, or SATA, to connect disks to the workstation.
- Some of them are listed below:

1. Windows XP Write-Protection with USB Devices:

- When Microsoft updated Windows XP with Service Pack 2 (SP2), a new feature was added to the Registry: The USB write-protection feature blocks any writing to USB devices.
- On your acquisition workstation, simply connect the suspect drive to the USB external drive or connector after we've modified the Windows Registry to enable write-protection.
- To update the Registry, we need to perform three tasks.

1. First, back up the Registry in case something fails while we're modifying it.
2. Second, modify the Registry with the write protection feature.

3. Third, create two desktop icons to automate switching between enabling and disabling writes to the USB device.

2. Acquiring Data with a Linux Boot CD:

- The Linux OS has many features that are applicable to computer forensics, especially data acquisitions.
- Physical access for the purpose of reading data can be done on a connected media device, such as a disk drive, a USB drive, or other storage devices.
- In Windows OSs and newer Linux kernels, when we connect a drive via USB, FireWire, external SATA, or even internal PATA or SATA controllers, both OSs automatically mount and access the drive.
- In static acquisitions, this automatic access corrupts the integrity of evidence. When acquiring data with Windows, we must use a write-blocking device or Registry utility.
- With a correctly configured Linux OS, such as a forensic Linux Live CD, media are not accessed automatically, which eliminates the need for a write-blocker.
- If we need to acquire a USB drive that does not have a write-lock switch, use one of the forensic Linux Live CDs to access the device.

3. Capturing an Image with ProDiscover Basic:

- ProDiscover automates many acquisition functions, unlike current Linux tools.
- Because USB drives are typically small, a single image file can be acquired with no need to segment it.
- Before acquiring data directly from a suspect drive with ProDiscover Basic, always use a hardware write-blocker device or the write protection method for USB-connected drives.

4. Capturing an Image with AccessData FTK Imager:

- FTK Imager is a Windows data acquisition program that's included with a licensed copy of AccessData Forensic Toolkit.
- FTK Imager is designed for viewing evidence disks and disk-to-image files created from other proprietary formats.
- FTK Imager can read AccessData .ad1, Expert Witness (EnCase) .e01, SafeBack, SMART .s01, and raw format files.
- FTK Imager can make disk-to-image copies of evidence drives and enables we to acquire an evidence drive from a logical partition level or a physical drive level.

- We can also define the size of each disk-to-image file volume, allowing we to segment the image into one or many split volumes.

5. SnapBackDatArrest:

- SnapBackDatArrest from Columbia Data Products is an older forensics acquisition program that runs from a true MS-DOS boot floppy disk.
- It can make an image of an evidence drive in three ways: disk to SCSI drive (magnetic tape or Jaz disk), disk to network drive, and disk to disk.
- SnapBackDatArrest provides network drivers so that we can boot from a forensic boot floppy disk and access a remote network server's drive.

6. NTI SafeBack:

- SafeBack, another reliable MS-DOS acquisition tool, is small enough to fit on a forensic boot floppy disk.It performs an SHA-256 calculation for each sector copied to ensure data integrity.
- During the acquisition, SafeBack creates a log file of all transactions it performs. The log file includes a comment field where we can identify the investigation and data you collect.
- SafeBack does the following:

a) Creates image files

b) Copies from a suspect drive to an image on a tape drive

c) Copies from a suspect drive to a target drive by using a parallel port laplink cable

d) Copies a partition to an image file

e) Compresses image files to reduce the number of volume segments

7. DIBS USA RAID:

- DIBS USA has developed Rapid Action Imaging Device (RAID) to make forensically sound disk copies.
- DIBS USA RAID is a portable computer system designed to make disk-to-disk images.
- The copied disk can then be attached to a write-blocker device connected to a forensic workstation for analysis.

8. ILook Investigator IXimager:

- IXimager runs from a bootable floppy disk or CD. It's a standalone proprietary format acquisition tool designed to work only with ILook Investigator.
- It can acquire single drives and RAID drives. It supports IDE (PATA), SCSI, USB, and FireWire devices.
- The IXimager proprietary format can be converted to a raw format if other analysis tools are used.
- IXimager has three format options:

a) IDIF—A compressed format

b) IRBF—A raw format

c) IEIF—An encrypted format for added security

9. ASRData SMART:

- ASRData SMART is a Linux forensics analysis tool that can make image files of a suspect drive.
- SMART can produce proprietary or raw format images and includes the following capabilities:

a) Robust data reading of bad sectors on drives

b) Mounting suspect drives in write-protected mode

c) Mounting target drives, including NTFS drives, in read/write mode

d) Optional compression schemes to speed up acquisition or reduce the amount of storage needed for acquired digital evidence

10. Australian Department of DefencePyFlag:

- The Australian Department of Defence created the PyFlag tool.
- Intended as a network forensics analysis tool, PyFlag can create proprietary format Expert Witness image files and uses sgzip and gzip in Linux.

1.4.6 Validating Data Acquisitions

- Validating digital evidence requires using a hashing algorithm utility, which is designed to create a binary or hexadecimal number that represents the uniqueness of a data set, such as a file or disk drive.
- This unique number is referred to as a "digital fingerprint." Because hash values are unique, if two files have the same hash values, they are identical, even if they have different filenames.

- The following sections discuss how to perform validation with some currently available acquisition programs:

1. Linux Validation Methods:

- Linux and UNIX are rich in commands and functions. The two Linux shell commands, dd and dcfldd, have several options that can be combined with other commands to validate data.
- The dcfldd command has additional options that validate data collected from an acquisition.
- Validating acquired data with the dd command requires using other shell commands.
- Current distributions of Linux include two hashing algorithm utilities: md5sum and sha1-sum. Both utilities can compute hashes of a single file, multiple files, individual or multiple disk partitions,or an entire disk drive.

2. Windows Validation Methods:

- Windows has no built-in hashing algorithm tools for computer forensics.
- However, many Windows third-party programs do provide a variety of built-in tools.
- These third-party programs range from hexadecimal editors, such as X-Ways WinHex or Breakpoint Software Hex Workshop, to computer forensics programs, such as ProDiscover, EnCase, and FTK.
- Each program has its own validation technique used with acquisition data in its proprietary format.
- For example, ProDiscover's .eve files contain metadata in the acquisition file or segmented files,including the hash value for the suspect drive or partition.
- Image data loaded into Pro-Discover is hashed and then compared to the hash value in the stored metadata.
- If the hashes do not match, ProDiscover notifies us that the acquisition is corrupt and can't be considered reliable evidence. This function is called Auto Verify Image Checksum.

1.4.7 Using Remote Network Acquisition Tools

- Recent improvements in computer forensics tools include the capability to acquire disk data or data fragments (sparse or logical) remotely.
- With this feature, we can connect to a suspect computer remotely via a network connection and copy data from it.

- Remote acquisition tools vary in configurations and capabilities. Some require manual intervention on remote suspect computers to initiate the data copy.
- Others can acquire data secretly through an encrypted link by pushing a remote access program to the suspect's computer.
- From an investigation perspective, being able to connect to a suspect's computer remotely to perform an acquisition has tremendous appeal.
- It minimizes the chances of a suspect discovering that an investigation is taking place.
- Most remote acquisitions have to be done as live acquisitions, not static acquisitions.

The following are some of the Remote Acquisition Tools

1. Remote Acquisition with ProDiscover:

- Two versions of ProDiscover can perform remote acquisitions: ProDiscover Investigator and ProDiscover Incident Response.
- When connected to a remote computer, both tools use the ProDiscover acquisition method.
- After the connection is established, the remote computer is displayed in the Capture Image dialog box.
- ProDiscover Investigator is designed to capture data from a suspect's computer while the user is operating it, which is a live acquisition.
- ProDiscover Incident Response is designed to be integrated as a network intrusion analysis tool.

2. Remote Acquisition with EnCase Enterprise:

- EnCase Enterprise is set up with an Examiner workstation and a Secure Authentication for EnCase(SAFE) workstation. Acquisition and analysis are conducted on the Examiner workstation.
- The SAFE workstation provides secure encrypted authentication for the Examiner workstation and the suspect's system.
- The remote access program in EnCase Enterprise is Servlet, a passive utility installed on the suspect computer. Servlet connects the suspect computer to the Examiner and SAFE workstations.
- A unique feature is that Servlet can run in stealth mode on the suspect computer.

3. Remote Acquisition with R-Tools R-Studio:

- The R-Tools suite of software is designed for data recovery.

- As part of this recovery capability, the R-Studio network edition can remotely access networked computer systems. Its remote connection uses Triple Data Encryption Standard (3DES) encryption.
- Data acquired with R-Studio network edition creates raw format acquisitions, and it's capable of recovering the following file systems:

- FAT12, FAT16, FAT32
- NTFS, NTFS5
- Ext2FS, Ext3FS
- UFS1, USF2

4. Remote Acquisition with WetStoneLiveWire:

- WetStone'sLiveWire tool can connect remotely to a networked computer and perform a live acquisition of all connected drives.
- LiveWire's acquisition file format is raw (.dd).
- In addition to being able to copy disk data, LiveWire can capture RAM data from remote systems.

5. Remote Acquisition with F-Response:

- F-Response is a vendor-neutral specialty remote access utility designed to work with any computer forensics program.
- When installed on a remote computer, it sets up a security read-only connection that allows the computer forensics examiner to access it.
- With F-Response, examiners can access remote drives at the physical level and view raw data.
- After the F-Response connection has been set up, any computer forensics acquisition tool can be used to collect digital evidence.

6. Remote Acquisition with Runtime Software:

- Runtime Software offers several compact shareware programs for data recovery. For remote acquisitions, Runtime has created these utilities:

- DiskExplorer for FAT
- DiskExplorer for NTFS
- HDHOST

- Runtime has designed its tools to be file system specific, so DiskExplorer versions for both FAT and NTFS are available.

- HDHOST is a remote access program that allows communication between two computers.
- The connection is established between systems by using the DiskExplorer program corresponding to the suspect (remote) computer's drives.

1.5 DISK IMAGING AND PRESERVATION(UNDERSTANDING BIT-STREAM COPIES)

A bit-stream copy is a bit-by-bit copy (also known as a sector copy) of the original drive or storage medium and is an exact duplicate.

- The more exact the copy, the better chance we have of retrieving the evidence we need from the disk. This process is usually referred to as "acquiring an image" or "making an image" of a suspect drive.
- A bit-stream copy is different from a simple backup copy of a disk.
- Backup software can only copy or compress files that are stored in a folder or are of a known file type.
- Backup software cannot copy deleted files and e-mails or recover file fragments.
- A bit-stream image is the file containing the bit-stream copy of all data on a disk or disk partition.
- For simplicity, it is usually referred to as an "image," "image save," or "image file." Some manufacturers also refer to it as a forensic copy.
- To create an exact image of an evidence disk, copying the image to a target disk that's identical to the evidence disk is preferable.
- The target disk's manufacturer and model, in general, should be the same as the original disk's manufacturer and model.
- If the target disk is identical to the original, the size in bytes and sectors of both disks should also be the same.
- Some image acquisition tools can accommodate a target disk that's a different size than the original.
- Older computer forensics tools designed for MS-DOS work only on a copied disk.
- Current GUI tools can work on both a disk drive and copied data sets that many manufacturers refer to as "image saves."

1.6 AUTOMATED SEARCH TECHNIQUE

- A computer forensic examination is aimed at finding facts, and through these facts they attempt to recreate the truth of an event.

- An automated system can do what it was intended to do without the help of someone.

- By using Automated Search Techniques, you can find out whether certain types of objects exist in the collected information, such as hacking tools or pictures of certain types.

- There are two types of Automated Search Techniques: Manual Browsing and Automated Browsing.

Manual Browsing

- By using Manual Browsing, the Forensic Analyst browses the gathered data and selects the objects of his or her preference.

- This browsing is done with the help of a Watcher tool.
- A human-readable format is produced by decoding an object of data, such as file, and returning the result.

- In many investigations, manual browsing takes a lot of time and effort since there is a huge amount of information to collect.

Automated Browsing

- In an automated search procedure, the results of a search procedure are fully automated and can be accessed directly from the automated files of another party.

- The various types of automated Searchesare: Keyword Search, Regular Expression Search, Approximate Matching Search, Custom Searches, Search of Modifications.

1. Keyword Search –Keyword search consists of specific keywords

2. Regular Expression Search –The regular expression (Regex) is a powerful method of searching data in text files for patterns that are known.

3. Approximate Matching Search –It uses Matching algorithm.

4. Custom Searches –**This tool uses** Heuristic procedure to find full names of people in gathered information/data.

5. Search of Modifications –This is used for data objects that have been modified since specified instant in past.

1.7 FORENSIC SOFTWARE(COMPUTER FORENSIC TOOLS)

- Computer forensic tools helps us to acquire data from the computer.

- Computer forensics tools are constantly being developed, updated, patched, and revised.

1.7.1 Types of Computer Forensic Tools

- Computer forensics tools are divided into two major categories: hardware forensic tools and software forensic tools.

Hardware Forensics Tools:

- Hardware forensics tools range from simple, single purpose components to complete computer systems and servers.
- Single-purpose components can be devices, such as the ACARD AEC-7720WP Ultra-Wide SCSI-to-IDE Bridge, which is designed to write-block an IDE drive connected to a SCSI cable.
- Some examples of complete systems are Digital Intelligence F.R.E.D. systems, DIBS Advanced Forensic Workstations, and Forensic Computers Forensic Examination Stations and portable units.
- Under Hardware Forensic Tools we have to understand the concept of **Forensic Workstation and Write blocker.**

1. Forensic Workstations

- Many computer vendors offer a wide range of forensic workstations that we can tailor to meet yourinvestigation needs. The more diverse investigation environment, the more options we need.
- In general, forensic workstations can be divided into the following categories:

a) Stationary workstation—A tower with several bays and many peripheral devices

b) Portable workstation—A laptop computer with a built-in LCD monitor and almost as many baysand peripherals as a stationary workstation

c) Lightweight workstation—Usually a laptop computer built into a carrying case with a smallselection of peripheral options

2. Write-Blocker:-

- Write-blockers protect evidence disks by preventing data from being written to them.
- Software and hardware write-blockers perform the same function but in a different fashion.

- Software write-blockers, such as PDBlock from Digital Intelligence, typically run in a shell mode.

- PDBlock can run only in a true DOS mode, however, not in a Windows MS-DOS shell.

- With hardware write-blockers, we can connect the evidence drive to workstation and start the OS asusual. Hardware write-blockers are ideal for GUI forensics tools.

- They prevent Windows or Linux from writing data to the blocked drive. Hardware write-blockers actnas a bridge between the suspect drive and the forensic workstation.

- In the Windows environment, when a write-blocker is installed on an attached drive, the drive appearsas any other attached disk.
- When we copy data to the blocked drive or write updates to a file with Word, Windows shows that thedata copy is successful.

- However, the write-blocker actually discards the written data—in other words, data is written to null.

- When we restart the workstation and examine the blocked drive, we won't see the data or files youcopied to it previously.

- Most of the write-blockers enables to remove and reconnect drives without having to shut down theworkstation, which saves time in processing the evidence drive.

Software Forensics Tools:

- Software forensics tools are grouped into command-line applications and GUI applications.

- Some tools are specialized to perform one task, such as SafeBack, a command-line disk acquisition tool from New Technologies, Inc. (NTI).

- Other tools are designed to perform many different tasks. For example, Technology Pathways ProDiscover, X-Ways Forensics, Guidance Software EnCase, and AccessData FTK are GUI tools designed to perform most computer forensics acquisition and analysis functions.

- Software forensics tools are commonly used to copy data from a suspect's drive to an image file.

- Many GUI acquisition tools can read all structures in an image file as though the image were the original drive.

- Many analysis tools, such as ProDiscover, EnCase, FTK, X-Ways Forensics, ILook, and others, have the capability to analyse image files.
- Computer forensic Software tool can be divided into two type: command-line and GUI tools

1) command-line Forensic Tool

- The first tools that analysed and extracted data from floppy disks and hard disks were MS-DOS tools for IBM PC file systems.
- One of the first MS-DOS tools used for computer investigations was Norton DiskEdit.
- This tool used manual processes that required investigators to spend considerable time on a typical 500 MB drive.
- One advantage of using command-line tools for an investigation is that they require few system resources because they're designed to run in minimal configurations.
- Most tools fit on bootable media (floppy disk, USB drive, CD, or DVD).
- Conducting an initial inquiry or a complete investigation with bootable media can save time and effort.
- Most tools also produce a text report small enough to fit on a floppy disk.
- Some command-line forensics tools are created specifically for DOS/Windows platforms; others are created for Macintosh and UNIX/Linux.
- Because there are many different versions of UNIX and Linux, these OSs are often referred to as *nix platforms.

UNIX/Linux Forensics Tools:-

- The *nix platforms have long been the primary command-line OSs, but typical end users haven't used them widely.
- However, with GUIs now available with *nix platforms, these OSs are becoming more popular with home and corporate end users. Following are some *nix tools for Forensics Analysis:

SMART:

- SMART is designed to be installed on numerous Linux versions.

- We can analyse a variety of file systems with SMART; for a list of file systems or to download an evaluation ISO image for SMART and SMART Linux.

- SMART includes several plug-in utilities. This modular approach makes it possible to upgrade SMART components easily and quickly.

- SMART can also take advantage of multithreading capabilities in OSs and hardware, a feature lackingin other forensics utilities.

- Another useful option in SMART is the hex viewer. Hex values are color-coded to make it easier tosee where a file begins and ends.

Helix:

- Helix can load it on a live Windows system, and it loads as a bootable Linux OS from a cold boot. ItsWindows component is used for live acquisitions.
- During corporate investigations, often we need to retrieve RAM and other data, such as the suspect'suser profile, from a workstation or server that can't be seized or turned off.

- This data is extracted while the system is running and captured in its state at the time of extraction.

BackTrack:

- BackTrack is another Linux Live CD used by many security professionals and forensics investigators.

- It includes a variety of tools and has an easy-to-use KDE interface.

- Autopsy and Sleuth Kit are included with the BackTrack tools as well as Foremost, dcfldd, Pasco,MemFetch, and MBoxGrep.

Autopsy and Sleuth Kit:

- Sleuth Kit is a Linux forensics tool, and Autopsy is the GUI browser interface for accessing Sleuth Kit's tools.

- The Sleuth Kit is a collection of command line tools and a C library that allows you to analysediskimages and recover files from them.

- Autopsy is an easy to use, GUI-based program that allows to efficiently analyse hard drives and smartphones.

- It has a plug-in architecture that allows to find add-on modules or develop custom modules in Java orPython.

Knoppix-STD:

- Knoppix Security Tools Distribution (STD) is a collection of tools for configuring security measures,including computer and network forensics.

- Like Helix, Knoppix-STD is a Linux bootable CD. If we shut down Windows and reboot with theKnoppix-STD disc in the CD/DVD drive, system boots into Linux.

2) GUI Forensics Tools

- Several software vendors have introduced forensics tools that work in Windows. Because GUIforensics tools don't require the same understanding of MS-DOS and file systems as command-linetools, they can simplify computer forensics investigations.

- Most GUI tools are put together as suites of tools. For example, Technology Pathways, AccessData,and Guidance Software.
- GUI tools have several advantages, such as ease of use, the capability to perform multiple tasks, andno requirement to learn older OSs.

- Their disadvantages range from excessive resource requirements and producing inconsistent resultsbecause of the type of OS used, such as Windows Vista 32-bit or 64-bit systems.

1.7.2 Tasks performed by Computer Forensic tools.

- All computer forensics tools, both hardware and software, perform specific functions. These functions are grouped into five major categories:

1. Acquisition

- Acquisition, the first task in computer forensics investigations, is making a copy of the original drive.

- This procedure preserves the original drive to make sure it doesn't become corrupt and damage the digital evidence.

- Sub-functions in the acquisition category include the following:

a) Physical data copy

b) Logical data copy

c) Data acquisition format

d) Command-line acquisition

e) GUI acquisition

f) Remote acquisition

g) Verification

2. Validation and discrimination

Two issues in dealing with computer evidence are critical.

- First is ensuring the integrity of data being copied—the validation process.
- Second is the discrimination of data, which involves sorting and searching through all investigationdata. The process of validating data is what allows discrimination of data.
- Many forensics software vendors offer three methods for discriminating data values.
- These are the sub-functions of the validation and discrimination function:

a) Hashing
b) Filtering
c) Analysing file headers

3. Extraction:

- The extraction function is the recovery task in a computing investigation and is the most challenging of all tasks to master.
- Recovering data is the first step in analysing an investigation's data.
- The following sub-functions of extraction are used in investigations:

a) Data viewing
b) Keyword searching
c) Decompressing
d) Carving
e) Decrypting
f) Bookmarking

4. Reconstruction:

- The purpose of having a reconstruction feature in a forensics tool is to re-create a suspect drive to showwhat happened during a crime or an incident.
- Another reason for duplicating a suspect drive is to create a copy for other computer investigators, whomight need a fully functional copy of the drive so that they can perform their own acquisition, test, andanalysis of the evidence.
- These are the sub-functions of reconstruction:

a. Disk-to-disk copy

b. Image-to-disk copy

c. Partition-to-partition copy

d. Image-to-partition copy

5. Reporting:

- To complete a forensics disk analysis and examination, we need to create a report.

- Before Windows forensics tools were available, this process required copying data from a suspectdrive and extracting the digital evidence manually.

- The investigator then copied the evidence to a separate program, such as a word processor, to create areport.
- Windows forensics tools can produce electronic reports in a variety of formats, such as word processing documents, HTML Web pages, or Acrobat PDF files.

- These are the sub-functions of the reporting function:

a) Log reports
b) Report generator

1.8 SUMMARY

- When planning a case, take into account the nature of the case, instructions from therequester, what additional tools and expertise you might need, and how you willacquire the evidence.

- Computer forensics involves obtaining and analyzing digital information for use as evidence in civil, criminal, or administrative cases.

- To document the evidence, you record details about the media, including who recovered the evidence and when and who possessed it and when.

- A bit-stream copy is a bit-by-bit duplicate of the original disk. You should use theduplicate, whenever possible, when analyzing evidence.

- Evidence custody form is a printed form indicating who has signed out and been in physicalpossession of evidence.

- Forensic copy is another name for a bit-stream image.

- Evidence bags is a Nonstatic bags used to transport removable media, hard drives, and othercomputer components.

- Forensics data acquisitions are stored in three different formats: raw, proprietary, andAFF. Most proprietary formats and AFF store metadata about the acquired data inthe image file.
- The four methods of acquiring data for forensics analysis are disk-to-image file, disk-to-disk copy, logical disk-to-disk or disk-to-data file, or sparse data copy of a folder or file.
- Acquisition is the process of creating a duplicate image of data; one of the five requiredfunctions of computer forensics tools.
- The five functions required for computer forensics tools are acquisition, validationand discrimination, extraction, reconstruction, and reporting.

1.9 QUESTIONS

1. Define Computer Forensics.
2. List standard systems analysis steps to be applied when preparing a for forensic investigation case.
3. In the company-policy violation case, what are some initial assessments you should make for a computer investigation?
4. What in an evidence custody form? What information does it contain?
5. What are the different acquisition tools in forensics? Explain.

1.10 REFERENCES

- Guide to Computer Forensics and Investigations Fourth EditionbyBillNelsonAmeliaPhillipsChristopherSteuart.
- Guide To Computer Forensics And Investigations (usermanual.wiki)

2

NETWORK, CELL PHONE AND MOBILE DEVICE FORENSIC

Unit Structure

2.0 OBJECTIVE

This chapter would make you understand the following concept:

- Network Forensic
- Standard procedure for Network Forensic
- Cell phone and mobile device forensic

2.1 INTRODUCTION

- Some of the jobs for network administrators involve network forensics.
- Network forensics is different from network security because it deals with tracking down the source and results of an intrusion or attack event, not preventing intrusions or attacks.
- Live acquisitions are becoming more common because they can provide insight into how attackers can access a network.
- Mobile phone can also be considered an important media through which wealth of information can be collected.

2.2 NETWORK FORENSIC AND TRACKING NETWORK TRAFFIC

- Network forensics is the process of collecting and analyzing raw network data and tracking network traffic systematically to determine how an attack was carried out or how an event occurred on a network.
- Because network attacks are increasing, there is an increasing demand for skilled technicians to focus on this field.
- Labor forecasts predict a shortfall of 50,000 network forensics specialists in law enforcement, legal firms, corporations, and universities.
- When intruders get into a network, they leave a trail behind them. If we are able to spot variations in network traffic, we can track intrusions, so knowing your network's typical traffic patterns is important.
- For example, the primary ISP in Windhoek, Namibia, has peak hours of use between 6 a.m. and 6 p.m. because most people in that city have Internet access only at work. If a usage spike occurred during the night, the network administrator on duty would recognize it as unusual activity and could take steps to investigate it.
- Network forensics can also help to determine whether a network is truly under attack or a user has accidentally installed an untested patch or custom program.
- A lot of time and resources can be wasted determining that a bug in a custom program or an untested open-source program caused the "attack."

- Network forensics can be defined as the sniffing, recording, acquisition and analysis of the network traffic and event log in order to investigate a network security incidence.

- After an attack or intrusion, network forensics examiners must follow standard procedures for obtaining data.

- Network administrators want to find compromised machines and get them offline as quickly as possible so downtime is minimized.

- To ensure that all compromised systems have been found and to identify attack methods in an effort to prevent them from occurring again, standard procedures must be followed.

2.2.1 Securing Network

- Network forensics is used to determine how a security breach occurred; however, steps must be taken to harden networks before a security breach happens, particularly with recent increases in network attacks, viruses, and other security incidents.

- To determine how a security breach occurred, Network forensics is used. However, steps need to be taken to harden networks before a security breach happens, particularly with recent increases in network attacks, viruses, and other security incidents.

- Hardening includes a variety of tasks which sets up layers of protection to hide the most valuable data at the innermost part of the network.

- The National Security Agency (NSA) developed a similar approach, called the defense in depth (DiD) strategy.

- DiD has three modes of protection:
  1. People
  2. Technology
  3. Operations

- If one mode of protection fails, the others can be used to stop the attack.
- Listing **people** as a mode of protection means organizations must hire well-qualified people and treat them well so that they have no reason to seek revenge.

- In addition, organizations should make sure employees are trained satisfactorily in security procedures and are familiar with the organization's security policy.

- Physical and personnel security measures are included in this mode of protection.

- The **technology mode** includes choosing a strong network architecture and using tested tools, such as intrusion detection systems (IDSs) and firewalls.

- Penetration testing and risk assessment can also improve network security.

- Technology mode of protection requires the implementation of systems that allow thorough and rapid analysis of security breaches.

- Finally, the **operations mode** addresses day-to-day operations. The updating of security patches, antivirus software, and operating systems, as well as the monitoring and assessment of disaster recovery procedures, fall under this category.

2.2.2 Reviewing Network Logs

- Network logs record traffic that is coming in and out of a network.

- Network servers, routers, firewalls, andother network devices record the activities and events that move through them.

- Running Tcpdumpprogram is a common way of examining network traffic, which canproduce hundreds or thousands of lines of records.

TCP log from 2010-12-17:15:06:33 to 2010-12-17:15:06:34.

Tue Dec 15 15:06:33 2010; TCP; eth0; 1296 bytes; from

204.146.114.10:1916 to 156.26.62.201:126

Tue Dec 15 15:06:33 2010; TCP; eth0; 625 bytes; from

192.168.114.30:289 to 188.226.173.122:13

Tue Dec 15 15:06:33 2010; TCP; eth0; 2401 bytes; from

192.168.5.41:529 to 188.226.173.122:31

Tue Dec 15 15:06:33 2010; TCP; eth0; 1296 bytes; from

206.199.79.28:1280 to 10.253.170.210:168;first packet

END

- The first line of the output is simply the header.

- The format of rest of the lines is time;protocol; interface; size; source and destination addresses.

- In the above Example Time is Tue Dec 15 15:06:33 2010;protocol is TCP; interface is eth0; Size is 1296 bytes; source is 204.146.114.10:1916 and the destination is 156.26.62.201:126.

2.2.3 Performing Live Acquisitions

- Live acquisitions are especially helpful when you are dealing with active network intrusions or attacks, or when you suspect employees are accessing network areas they should not.

- In addition, information in RAM is lost after you turn off a suspect system. However, after you do a live acquisition, information on the system has changed because your actions affect RAM and running processes, which also means the information can't be reproduced.

- Therefore, live acquisitions don't follow typical forensics procedures. The problem investigators face is the order of volatility (OOV) that means how long a piece of information lasts on a system.

- Data such as RAM and running processes might exist for only milliseconds but other data, such as files storedon the hard drive, might last for years.

- The following steps show the general procedure for a live acquisition, although investigators differ onexact steps:

1. Create or download a bootable forensic CD, and test it before using it on a suspect drive.

2. If the suspect system is on the network and we can access it remotely, add the appropriate networkforensics tools to the workstation. If not, insert the bootable forensics CD in the suspect system.

3. Make sure we keep a log of all the actions; documenting the actions and reasons for these actions iscritical.

4. A network drive is ideal as a place to send the information we collect.If we don't have one available, connect a USB thumb drive to the suspect system for collecting data. Besure to note this step in the log.

5. Next, copy the physical memory (RAM). Microsoft has built-in tools for this task, or we can useavailable freeware tools, such as memfetch and BackTrack.
6. The next step varies, depending on the incident we're investigating. With an intrusion, for example, wemight want to see whether a rootkit is present by using a tool such as RootKit Revealer.We can also access the system's firmware to see whether it has changed, create an image of the drive overthe network, or shut the system down and make a static acquisition later.

7. Be sure to get a forensically sound digital hash value of all files that recover during the live acquisitionto make sure they aren't altered later.

2.2.4 Standard Procedures for Network Forensics

- Network forensics is a lengthy, tedious process, and the trail can quickly disappear.

- A standard procedure that is used in network forensics is as follows:

1. Always use a standard installation image for systems on a network. This image is not a bit-stream image but an image containing all the standard applications used. You should also have the MD5 and SHA-1 hash values of all application and OS files.

2. When an intrusion event happens, make sure the vulnerability has been fixed to prevent other attacks from taking advantage of the opening.

3. Attempt to retrieve all volatile data, such as RAM and running processes, by doing a live acquisition before turning the system off.

4. Acquire the compromised drive and make a forensic image of it.

5. Compare files on the forensic image to the original installation image. Compare hash values of common files, such as Win.exe and standard DLLs, and ascertain whether they have changed.

1.2.5 Network Tools

- A variety of tools are available for network administrators to perform remote shutdowns, monitor device use, and more.

- For examining Windows productsSysinternalscan be used which is a collection of free tools. They were created by Mark Russinovich and Bryce Cogswell and acquired by Microsoft.

- The following are the list of powerful Windows tools available at Sysinternals:

- **RegMon** – It shows all Registry data in real time.

- **Process Explorer**– It shows what files, Registry keys, and dynamic link libraries (DLLs)are loaded at a specific time.
- **Handle**- It shows what files are open and which processes are using these files.

- **Filemon** -It shows file system activity.

- PsTools is a suite which was created by Sysinternals.It includes the following tools:

- **PsExec**— It runs processes remotely

- **PsGetSid**— It displays the security identifier (SID) of a computer or user

- **PsKill**— It kills processes by name or process ID

- **PsList**— It lists detailed information about processes
- **PsLoggedOn**— It displays who is logged on locally
- **PsPasswd**— It allows you to change account passwords
- **PsService**— It enables you to view and control services
- **PsShutdown**— It shuts down and optionally restarts a computer
- **PsSuspend**— It allows you to suspend processes

- These tools help you monitor your network efficiently and thoroughly.
- A few of the Knoppix-STD tools for Unix/Linux include the following:

- **dcfldd**—It is a U.S. DOD computer forensics lab version of the dd command
- **memfetch**— It forces a memory dump
- **photorec**— It retrieves files from a digital camera
- **snort**— It is a popular IDS(Intrusion Detection System) that performs packet capture and analysis in real time
- **oinkmaster**— It helps to manage snort rules so that you can specify what items to ignore as regulartraffic and what items should raise alarms
- **john**—The latest version of John the Ripper, a password cracker
- **chntpw**—Enables to reset passwords on a Windows computer, including the administratorpassword
- **tcpdump and ethereal**—Packet sniffers

2.2.6 Using Packet Sniffers:

- Packet sniffers are devices and/or software placed on a network to monitor traffic.
- Most network administrators use sniffers for increasing security and tracking bottlenecks.
- On TCP/IP networks, sniffers examine packets, hence the term "packet sniffers." Most packet snifferswork at Layer 2 or 3 of the OSI model.
- Some sniffers capture packets, some analyze them, and some do both.

- Theorganization needs to have policies about network sniffing to fulfil with the new federal laws on digitalevidence.

- Most tools can read anything captured in **Pcap** (packet capture) format. **(Libpcap** is the version forUNIX/Linux, and **Winpcap** is the version for Windows.)

- You can use Tcpslice to extract information from large Libpcap files; just specify the time frame you want to examine.It is also capable of combining files.

- Network traffic recorded in Libpcap format can be replayed with a suite of tools called Tcpreplay; we use this information to test IDSs, switches, and routers.

- Tcpdstat generates Libpcap statistics close to real time, breaking packets down by protocol, so we can get a quick overview of network traffic, including average and maximum transfer rates.

- **Etherape**is a tool for viewing network traffic graphically.

- Another GUI tool,**Netdude**, was designed as an easy-to-use interface for inspecting and analysing largeTcpdump files.

- **Argus** is a session data probe, collector, and analysis tool. This real-time flow monitor can be used forsecurity, accounting, and network management.

1.2.7 Examining the Honeynet Project

- The Honeynet Project was developed to make information widely available in an attempt to prevent Internet and network attackers.

- The objectives of this project is to create awareness, give information, and tools.
- Making people and organizations aware that threats exist and they may be targeted is the first step in Honeynet Project.

- The second part of the service is to provide information about how to protect against these threats, including how attackers communicate and what tactics they employ.

- Finally, for people who wantto do their own research, the Honeynet Project offers tools and methods.

- A recent major threat is distributed denial-of-service (DDoS) attacks.

- There may be traces of a DDoS attack on other organizations' networks besides yours and your ISP's.

- InDDoS attacks, hundreds or even thousands of machines can be used.
- These machines are known as zombies because they have innocently become part of the attack.
- In the initial stages of DDoS attacks, the main concerns were the high financial costs and the lengthy tracking process.
- Zero-day attacks is another major threat.
- The goal of attackers is to exploit weaknesses in networks and operating systems before patches are available.
- Since vendors are unaware of these vulnerabilities, they haven't developed and released patches.
- The purpose of penetration testers is to find undiscovered vulnerabilities in networks and predict where the next onslaught of network attacks will originate.
- The Honeynet Project was built as a resource to help network administrators to deal withDDoS and other attacks.
- It involves installing honeypots and honeywalls at various locationsin the world.
- Honeypots are computers that copycat other machines on your network, but contain no valuable information. Their purpose is to lure attackers to your network.
- In this way, you can take the honeypot offline and not affect therunning of your network.
- Honeywalls are computers set up to monitor what is happening tohoneypots on your network and record what attackers are doing.
- Currently, the evidence produced by Honeywallscannot be used in court, but it cansurely be used todetermine howcriminals are breaking in and create better safeguards for networks.

2.3 MOBILE DEVICE FORENSICS

- There are great challenges in the field of cell phone and mobile device forensics due to the rapid changes it undergoes.
- The thought of losing your cell phone is terrifying because we store a tremendous amount of information on our phones.

- The following items might be stored on mobile,depending on your phone's model:
  - Incoming, outgoing, and missed calls
  - Text and Short Message Service (SMS) messages
  - E-mail
  - Instant messaging (IM) logs
  - Web pages
  - Pictures
  - Personal calendars
  - Address books
  - Music files
  - Voice recordings

- Many people store more information on their cell phones as compared to their computers, and with this variety of information, restoring together the facts of a case is possible.

- Many countries allow cell phones to access bank accounts and transfer funds from one phone to another.

- One of the most versatile devices ever invented is this handheld device.

- Despite the usefulness of these devices in providing clues for investigations, investigating cell phones and mobile devices is one of the most challenging tasks in digital forensics.

- n spite of the fact that many cell phones use similar storage schemes, there is no single standard for how and where messages are stored.

2.3.1 Mobile Phone Basics

- Till the end of 2008, there have been three generations of mobile phones: analog, digital personal communications service (PCS), and third-generation (3G).
- 3G offers increased bandwidth as compared to the other technologies:

- For pedestrian use 384 Kbps is offered.

- In a moving vehicle 128 Kbps is offered.

- 2 Mbps is for fixed locations, such as office buildings.

- With 3G's rapid adoption around the world, illicit activities-such as identity theft, child pornography, and bank fraud-are expected to increase rapidly.

- Sprint Nextel introduced the fourth-generation (4G) network in the year 2009.

- The list of digital networks that are used in the mobile phone industry are given below:

Digital Network	
Digital Network	Description
Code Division Multiple Access (CDMA)	Developed during World War II, this technology was patented by Qualcomm after the war. It uses the full radio frequency spectrum to define channels. For example Sprint and Verizon use CDMA networks.
Global System for Mobile Communications (GSM)	This is also a common digital network.It is used by AT&Tand T-Mobile and is the standard in Europe and Asia.
Time Division Multiple Access (TDMA)	This digital network uses the technique of dividing a radio frequency into time slots. GSM networks use this technique. It also refers to a specific cellular network standard covered by Interim Standard (IS) 136.
Integrated Digital Enhanced Network (iDEN)	This is Motorola protocol which combines several services such as data transmission, into one network.
Digital Advanced Mobile Phone Service (D-AMPS)	This network is a digital version of the original analogstandard for cell phones.
Enhanced Data GSM Environment (EDGE)	This is again a digital network that is faster version of GSM, is designed todeliver data.
Orthogonal Frequency Division Multiplexing (OFDM)	This technology for 4G networks uses energy more efficientlythan 3G networks and is more resistant to interference.

2.3.2Technologies used by 4G network

4G networks can use the following technologies:

1. **Orthogonal Frequency Division Multiplexing (OFDM):**By dividing radio waves over different frequencies using Orthogonal Frequency Division Multiplexing (OFDM), power is more efficiently used and interference is reduced.

2. **Mobile WiMAX:** This technology uses the IEEE 802.16e standard and Orthogonal Frequency Division Multiple Access (OFDMA) and isbelieved to support transmission speeds of 12Mbps.

3. **Ultra Mobile Broadband (UTMS):**It is also known as CDMA2000 EV-DO, this technology is expected tobe used by CDMA network providers to switch to 4G and support transmission speeds of 100 Mbps.

4. **Multiple Input Multiple Output (MIMO):** This technology was developed by Airgo and acquired byQualcomm, is expected to support transmission speeds of 312 Mbps.

5. **Long Term Evolution (LTE):** This technology, designed for GSM and UMTS technology, is expectedto support 45 Mbps to 144 Mbps transmission speeds.

2.3.3Communication of the cells

- Mostly, geographical areas are divided into cells like honeycombs.

- The three main components thatare used forcommunication with these cells are as follows:

1. Base transceiver station (BTS)—this component is Consist of radio transceiver equipment that defines cells and communicates with mobile phones. It is sometimes referred to as a cell phone tower, although the tower is only one part of the BTS equipment.

2. Base station controller (BSC)—This combination of hardware and software manages BTSs and assigns channels by connecting to the mobile switching center.

3. Mobile switching center (MSC)—This component connects calls by routing digital packets for the network and relies on a database to support subscribers. This central database contains account data, location data, and other key information needed during an investigation. If you have to retrieve information from a carrier's central database, you usually need a warrant or subpoena.

2.3.4 Inside Mobile Devices

- Mobile devices can be a simple phones to small computers which is also called smart phones.

- The hardware consists of a microprocessor, ROM, RAM, a digital signal processor, a radio module, amicrophone and speaker, hardware interfaces (such as keypads, cameras, and GPS devices), and an LCDdisplay.

- Many of the devices have removable memory cards, and Bluetooth and Wi-Fi are now included in some mobile devices,too.

- Basically, phones store system data in electronically erasable programmable read-only memory(EEPROM), which enables service providers to reprogram phones without having to access memory chipsphysically.

- Many users take advantage of this capability by reprogramming their phones to add features or switch to different service providers.

SIM Cards:-

- Subscriber identity module (SIM) cards are found most commonly in GSM devices and consist of amicroprocessor and 16 KB to 4 MB EEPROM.

- There are also high-capacity, high-density, super, and mega SIM cards that boast as high as 1 GBEEPROM.

- SIM cards are similar to standard memory cards, except the connectors are aligned differently.

- GSM refers to mobile phones as “mobile stations” and divides a station into two parts: the SIM card and the mobile equipment (ME), which is the remainder of the phone.

- The SIM card is necessary for the ME to work and serves these additional purposes:-

a) Identifies the subscriber to the network
b) Stores personal information
c) Stores address books and messages
d) Stores service-related information

2.3.5 Acquisition Procedures for Cell Phones and Mobile Devices

- The cell phones and mobile devicesshould followproper search and seizureprocedure. This procedure is as important as procedure for computer.

- The main worries with mobile devices are loss of power and synchronization with PCs.

- Since mobile devices have volatile memory, it is crucial that they don't lose power before youretrieve RAM data.

- Determine whether the device is on or offat the investigation scene.

- If it is off, leave it off, but find the recharger and attach it as soon as possible.

- Notethis step in your log.

- If the device is on then check the battery's current charge level on the LCD display.

- Immediately disconnect any mobile device attached to a PC via a cable or cradle/docking station. This step helps to prevent synchronization that may occur automatically on a set schedule and overwrite data on the device.

- When you are back in the forensics lab, you need to consider what can be retrieved. It is very important to know where information is stored. You should check these four areas for information:

1. The internal memory
2. The SIM cards
3. Any removable or external memory cards
4. The system server

- According to wiretap laws, checking system servers requires a search warrant or subpoena, so you need one if you want to check voicemail.

- Information from the service provider to determine where the suspect or victim was at the time of a call, to access backups of address books, and more.

- You can retrieve information from a SIM card also. The information that can be retrieved from SIM Card are:

1. Service-related data, such as identifiers for the SIM card and subscriber
2. Call data, such as numbers dialed
3. Message information
4. Location information

2.3.6 Sim File Structure

- The file system for a SIM card is a hierarchical structure (see Figure 2.3.7).

- This filestructure begins with the root of the system (MF). The next level consists of directory files(DF), and under them are files containing elementary data (EF).

- In Figure 2.3.7, the EFs underthe GSM and DCS1800 DFs contain network data on different frequency bands of operation.

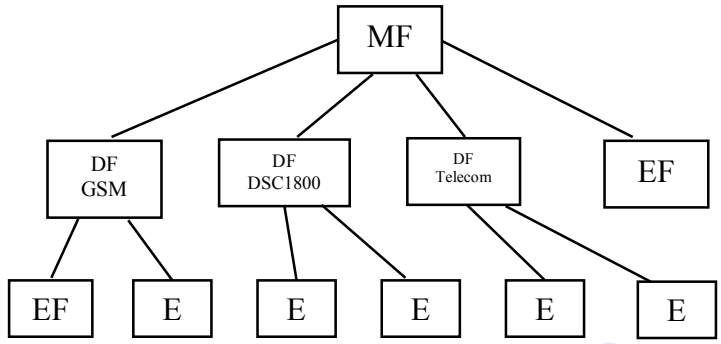

Figure: 2.3.7 SIM File Structure

- The EFs under the Telecom DF contain service-related data.

2.3.7 Mobile Forensics Tools

- **Paraben Software**, a leader in mobile forensics software, poses several tools, including Device Seizure that is used to acquire data from a variety of phone models.

- Paraben also has the Device Seizure Toolbox containing assorted cables, a SIM card reader, and otherequipment for mobile device investigations.

- **DataPilot**has alikecollection of cables that can interface with Nokia, Motorola, Ericsson, Samsung,Audiovox, Sanyo, and others.

- BitPim is another popular tool that is used to view data on many CDMA phones, including LG, Samsung,Sanyo, and others. It offers versions for Windows, Linux, and Mac OS X.
- By default BitPim stores files in My Documents\BitPim, so when we start a new case, make sure we movethese files to another location first so that they are not overwritten.

- A new tool, BitPim Cleaner by Mobile Forensics, Inc., moves these files. MFI is a new vendor of mobileforensics software and offers several affordable products as well as training.

- Cellebrite UFED Forensic System works with cell phones and PDAs. This kit comes with several cables,includes handset support for phones from outside the United States, and handles multiple languages.

- MOBILedit! is a forensics software tool containing a built-in write-blocker.

- It can connect to phones directly via Bluetooth, irDA, or a cable and can read SIM cards by using a SIM reader. It's also notable for being very user friendly.

- Another tool is SIMCon used to image files on a GSM/3G SIM or USIM card, including stored numbersand text messages.

2.4 SUMMARY

- Network forensics is the process of collecting and analyzing raw network data andsystematically tracking network traffic to discover how an attack took place.

- Live acquisitions are necessary to retrieve volatile data, such as RAM and running processes.

- By tracking network logs, you can get to know the normal traffic patterns on your network.

- It is possible for network tools to monitor traffic on a network, but they can also be used by intruders to attack from within a network.

- layered network defense strategy is an approach that is used to harden network which sets up several network layers to place the most valuable data at the innermost part of the network.

- Order of volatility (OOV) is aterm that refers to how long an item on a network lasts. RAM and running processes might last only milliseconds and items stored on hard drives can last for years.

- Distributed denial-of-service (DDoS) attacks is a type of DoS attack in which other onlinemachines are used, without the owners' knowledge, to launch an attack.

- Honeypot is a computer or network set up to lure an attacker.

- Honeystickis aHoneypot and Honeywall combined on a bootable memory stick.

- Honeywalls is an Intrusion prevention and monitoring systems that track what attackers do onhoneypots.

- People store huge amount of information on cell phones, including calls, text messages, picture and music files, address books, and more. These files can give you a lot of information when investigating cases.

- The three generations of mobile phones are: analog, digital personal communications service (PCS), and third-generation (3G).
- The next generation of mobile phones is 4G technology.

2.5 QUESTION

1. What are network forensics? Explain the 3 modes of protection in DiD Strategy.
2. What is Live Acquisition? How is it performed?
3. What is the standard procedure used for network forensics?
4. List the different network tools and explain any two.
5. State and explain different types of digital networks.
6. What are different Mobile Forensic tools? Explain.
7. Explain SIM File structure.

2.6 REFERENCES

- Guide to Computer Forensics and Investigations Fourth Edition by Bill Nelson Amelia Phillips Christopher Steuart.
- https://usermanual.wiki/Pdf/Guide20to20Computer20Forensics20and20Investigations.93483670/help

3

INTERNET FORENSIC

Unit Structure

3.0 OBJECTIVES

- To understand the several practices involved in internet forensic
- To get familiar with the threats involved in world wide web
- To acquaint with the hacking and various illegal access
- To understand the concept of domain name ownership investigation

3.1 INTRODUCTION

The examination of illegal activity that has taken place online. It examines the history of browsers, the scripts and header messages used by Web servers, and the origins, contents, patterns, and transmission routes of emails and Web pages. It is the use of scientific approaches in investigations of online crimes, fraud, and abuse.

Different types of Internet forensics:

Types of computer forensics

- Database forensics: The examination of information contained in databases, both data and related metadata
- Email forensics
- Malware forensics
- Memory forensics
- Mobile forensics
- Network forensics

3.2 WORLD WIDE WEB THREATS

3.2.1 Web threats definition

Web-based threats, also known as online threats, are a subset of cybersecurity hazards that could result in an unfavorable internet-based event or action.

End-user vulnerabilities, online service operators, developers, or the web services themselves are all sources of web risks. Regardless of motive or origin, digital threats can have negative effects on both people and organizations.

This phrase often refers to network-based dangers in the following categories, but is not restricted to them:

- Private network threats: Threats to private networks affect the smaller networks connected to the larger international internet. Home Wi-Fi or Ethernet networks, business intranets, and national intranets are some common examples.
- Host threats: Certain network host devices are affected by host threats. Corporate endpoints and personal gadgets like cell phones, tablets, and desktop PCs are frequently referred to as hosts.
- Web server threats: Threats to dedicated hardware and software used to support online infrastructure and services have an impact on web servers.

3.2.2 What are web threats?

Threats from the internet put users and computer systems at risk of harm. This category includes a wide range of risks, including well-known perils like phishing and computer infections. Other dangers, such as offline data theft, can be categorized with this group as well.

Online hazards are not just restricted to online behavior; they also eventually cause harm by using the internet. Although not all online threats are generated with intent, many do one of the following things:

- Denial of access: blocking access to computer systems and/or network services.
- Acquisition of access: unwelcome or unauthorized access to a personal computer or network services.
- The use of computer and/or network services without authorization or consent.
- Exposing critical government information and private information without authorization, such as images and login details.
- Unauthorized or undesirable alterations to network services or computers.

The range of web threats has greatly expanded in recent years. Smart gadgets and high-speed mobile networks have made it possible for malware, fraud, and other issues to have an always-connected vector. Moreover, consumer security knowledge has lagged behind online usage in areas like communications and productivity via the Internet of Things (IoT).

The web will remain rapidly growing as an appealing attack option for malevolent parties as we continue to rely more heavily on it for daily activities. The top concerns that continue to pose new hazards to privacy and security are convenience and a lack of caution when using the internet.

Despite the fact that computer-based targets are more often than not the intended audience, cyber threats ultimately have an impact on humans.

3.2.3 How do web threats work?

When a web threat situation occurs, a number of factors come into play that raise concerns.

There are a few fundamental elements to any web attack, specifically:

1. Threat motives provide an intentional threat agent with a reason or objective for harming others. Some danger agents may lack motivation because they act unintentionally or independently.

2. Threat agents are anything or anyone that has the potential to cause harm, with the internet acting both as a threat vector and as a potential target.

3. Any flaw in human nature, in technological systems, or in other resources that could result in a negative incidence or exploit is a vulnerability.

4. The adverse effects of a threat agent acting on one or more vulnerabilities are known as threat outcomes.

A threat to computer systems transforms into an attack as these elements interact. Threatening behavior may be motivated by any of the following: finance, information, surveillance, retaliation, sabotage, and more.

Often, threat agents are persons who want to do harm. By extension, an agent might be anything that is persuaded to work in the interests of the primary threat agent. However, some threat agents completely operate without human involvement, such as destructive natural events.

The types of threat agents include:

- **Non-human agents:** Examples include malicious code (viruses, malware, worms, scripts), natural disasters (weather, geological), utility failure (electrical, telecom), technology failure (hardware, software), and physical hazards (heat, water, impact).

- **Intentional human agents:** Based on malicious intent. Can be internal (employees, contractors, family, friends, acquaintances) and external (professional and amateur hackers, nation-state actors and agencies, competitor corporations)

- **Accidental human agents:** Based on human error. Similar to intentional threats, this type can include internal and external agents.

- **Negligence-based human agents:** Based on careless behaviors or safety oversights. Again, this category can also include internal and external agents.

Points of weakness where someone or something can be controlled are known as vulnerabilities. Vulnerabilities can be viewed as both a threat to the web and a problem that makes further threats possible. This area often has some kind of technological or human weakness that can enable system access, abuse, or destruction.

Threat outcomes may result in the disclosure of private information, user deception, disruption of computer use, or the seizure of access privileges. Online dangers frequently have the following effects, although not only those.

- **Reputation damage:** Loss of trust from clients and partners, search engine blacklisting, humiliation, defamation, etc.

- **Operations disruption:** Operational downtime, access denial to web-based services such as blogs or message boards, etc.

- **Theft:** Financial, identity, sensitive consumer data, etc.

Almost any operating system (OS) or application vulnerability can be exploited by cybercriminals to launch an attack. The majority of cybercriminals, however, will create web threats that specifically target some of the most popular operating systems and programmes, such as:

- **Java:** Because Java is installed on over 3 billion devices (that are running under various operating systems) exploits can be created to target specific Java vulnerabilities on several different platforms/operating systems.

- **Adobe Reader:** Although many attacks have targeted Adobe Reader, Adobe has implemented tools to protect the program against exploit activity. However, Adobe Reader is still a common target.

- **Windows and Internet Explorer:** Active exploits still target vulnerabilities that were detected as far back as 2010 – including MS10-042 in Windows Help and Support Center, and MS04-028, which is associated with incorrect handling of JPEG files.

- **Android:** Cybercriminals use exploits to gain root privileges. Then, they can achieve almost complete control over the targeted device.

3.2.4 How to spot web threats?

Despite the limitless variety of web-based hazards, several common characteristics of web threats can be identified. Yet, recognizing a cyber threat necessitates having a keen eye for minute things.

Web infrastructure gear is obviously vulnerable to some hazards, such heat and water. Others need serious attention, whereas those are simpler to spot. You should exercise the utmost caution while receiving digital messages and surfing websites.

The following advice will help you:

- **Grammar:** Malicious actors may not always carefully craft their messages or web content when assembling an attack. Look for typos, odd punctuation, and unusual phrasing.

- **URLs:** Harmful links can be masked under decoy anchor text — the visible text that's displayed. You can hover over a link to inspect its true destination.

- **Poor quality images**: The use of low-resolution or unofficial images may indicate a malicious webpage or message.

3.2.5 Types of web security threats

As was already mentioned, most web dangers involve both technological and human manipulation. Be aware that many web risks overlap with one another, and several might happen at the same time. The following list could contain some of the most typical web hazards.

1) **Social engineering:** Social engineering entails tricking consumers into acting against their own interests without realizing it. These threats typically include deceiving users by winning their trust. Such user manipulation may take the following forms:

- **Phishing:** impersonating trustworthy organizations or individuals in order to obtain personal information from them.

- **Watering hole attacks:** Using well-known websites to trick consumers into endangering themselves.

- **Network spoofing:** False access points that impersonate trustworthy ones.

2) **Malicious code:** includes malicious software and harmful scripts, which are lines of computer code used to create or exploit security holes. Malicious code is the technical aspect of web threats, whereas social engineering is the human aspect. These dangers may consist of, but not be limited to:

- **Injection attacks:** Attacks known as "injection" include inserting malicious code into reputable websites and applications. SQL Injection and Cross-Site Scripting are two examples (XSS).

- **Botnet:** A network of comparable "zombies" where a user device is taken over for remote, automated use. They are employed to quicken malware attacks, spam operations, and other activities.

- **Spyware:** Tracking software that keeps tabs on user activity on a computer device is known as spyware. Keyloggers are among the most prevalent examples.

- **Computer worms:** Programs that execute, replicate, and spread on their own without the assistance of a related software.

3) **Exploits:** Exploits are deliberate abuses of weaknesses that could result in an unfavorable event.

- **Brute force attacks:** Attempts to bypass security "gates" and weaknesses manually or automatically. Usually, this entails creating every password conceivable for a private account.

- **Spoofing:** Disguising one's true identity in order to influence reliable computer systems. Cache poisoning, DNS spoofing, and IP spoofing are a few examples.

4) **Cybercrime:** Any illicit activity carried out using computer systems is referred to as cybercrime. These dangers frequently carry out their schemes online.

- **Cyberbullying:** The psychological abuse of victims through threatening behavior.

- Private information is made public when it is disclosed without authorization. Examples include emails that are leaked, private images, and large corporate data leaks.

- **Cyber libel:** Also referred to as online defamation, involves harming the reputations of people or organizations. This can be accomplished through misinformation or disinformation (the purposeful dissemination of false information) (mistaken distribution of inaccurate information).

- **Advanced Persistent Threats (APTs):** Bad actors acquire access to a private network and establish ongoing access as part of APTs. To take advantage of weaknesses and acquire access, they mix social engineering, malicious software, and other threats.

3.3 HACKING AND ILLEGAL ACCESS

Illegal access, often known as hacking, refers to unauthorized attempts to get over a network's or information system's security measures. It is the most well-known and widespread type of cybercrime. In India, the term "hacking" has the broadest legal scope. Hacking also requires mens rea, or knowledge or purpose to cause unjust loss or damage, like other criminal offences do.

Theft of secured data and the disclosure of sensitive information as a result of organized hackers who are more profit-driven have prompted both businesses and individuals to take up cyber security. According to current trends, anyone may become a hacker, and hacking is largely made easy by free tools disguising themselves as network utilities and being made available online. A hacker is a person who specializes in working with the security protocols for computer and network systems in the field of data security.

Hackers' most recent and prevalent targets in current trends are mobile and smart phones. There are indications that because there are so many more mobile phones than PCs, these attacks on smart phones have been considerably more prevalent than those against computers or laptops.

Spotting the difference:

Hacking is the term for improperly accessing a computer system to gain unauthorized access.

Unauthorized access can be defined as employing standard access methods to obtain access to a computer system without permission.

To further distinguish the two, consider the following example:

Unauthorized access occurs when you use a friend's Facebook account after they failed to log out. Although though it's quite simple and doesn't take a lot of technical knowledge, hacking involves infecting their PC with keylogging software that collects their login information and then logging into their account.

3.4 OBSCENE AND INCIDENT TRANSMISSION

Obscene, indecent, and profane material cannot be broadcast on radio or television, according to federal law. That should sound obvious enough, but depending on who you ask, defining what obscene, indecent, and profane mean might be challenging.

I know it when I see it, Justice Potter Stewart famously penned in the Supreme Court's landmark 1964 ruling on obscenity and pornography. The FCC's standards are still impacted by that case today, and the laws are enforced in response to public complaints about airing unacceptable information.

In other words, you can inform the FCC and ask us to look into anything if you "know it when you see it" and find it unpleasant.

- **Deciding what's obscene, indecent or profane**

Each sort of material is defined specifically:

- The First Amendment does not provide any protection for offensive material. The Supreme Court created a three-part standard for content to be deemed obscene: It must be racially insulting, depict or describe sexual behavior in a way that is "patently objectionable," and generally lack serious literary, aesthetic, political, or scientific significance.

- Indecent content, which does not pass the three-prong standard for obscenity, depicts sexual or excretory organs or actions in a way that is obviously offensive.

- Profane language is defined as being "grossly offensive" and is seen as a public nuisance.

The specifics of the content, the time of day it was broadcast, and the environment in which it occurred are all factors that affect how the FCC rules apply.

Obscene material cannot be broadcast at any time of day without breaking the law. When there is a reasonable possibility that minors may be in the audience, indecent and profane content is not permitted on broadcast TV and radio between the hours of 6 a.m. and 10 p.m.

- **What about cable, satellite TV and satellite radio?**

Obscenity is not permitted on broadcast, cable, or satellite TV or radio since it is not protected by the First Amendment. But, because cable, satellite TV, and satellite radio are subscription services, the same restrictions on decency and profanity do not apply to them.

- **Implementing the laws**

Obscenity, indecency, and profanity regulations are often enforced by starting with public complaints that FCC personnel examine for potential infractions. A station's license may be revoked, a fine imposed, or a caution or admonition issued by the FCC if an investigation is necessary and it is determined that the station is breaking one of its rules.

- **What if I have feedback or issues regarding a particular broadcast?**

Any feedback or issues with a particular broadcast should be addressed to the stations and networks concerned.

- **What details should I provide in a complaint to the FCC about profanity, vulgarity, or obscenity?**

Please provide the following details before registering a complaint:

- The broadcast's date and time.
- The station's call sign, channel, and/or frequency.
- Details on what was said or shown during the broadcast.

For the purpose of examining the context of objectionable language, images, or scenarios and identifying potential rule infractions, detailed complaints are helpful. When possible, it is also beneficial (though not necessary) to provide a tape or transcript of a broadcast. Nevertheless, any supporting materials you submit become part of the FCC's records and might not be returned.

3.5 DOMAIN NAME OWNERSHIP INVESTIGATION

Your website's name is its domain name. A domain name is used as a means of identifying a firm as Internet commerce grows. Because so many businesses now do business or promote online, domain names have grown in value and are subject to dispute frequently.

The use of another person's trademark as a domain name is typically seen as trademark infringement and may be protected under trademark law.

3.5.1 Who is the domain owner?

Whoever first registered the website address with a recognized registrar, such Domain.com, owns the domain name. That person must pay registration fees and keep all of their contact information current in order to preserve ownership.

A person acquires ownership of a domain name once they have legitimately registered it and provided all necessary personal data to a recognized registrar. They are the sole owners of that domain name and are free to sell it whenever they want. If the owner chooses, they may transfer domain name ownership to a new user.

3.5.2 Length of domain ownership

The typical duration of domain ownership is two years. But, you may register a domain name for up to 10 years, depending on the extensions. Those who don't want to sign a multi-year contract can also choose renewal.

The annual charge that domain owners must pay varies depending on the Top level domain (TLD) they have selected. Since 2000, Domain.com has provided some of the lowest TLD renewal and registration prices available.

3.5.3 Why look up a domain owner?

There are numerous reasons for someone to search for a domain owner. It frequently occurs because the owner has knowledge of the domain and website that no one else does. It's also typical for domain owners to do their own searches to ensure that the internet representation of their website is accurate.

Other justifications for a domain owner search include:

- **Make a purchase:** The majority of the time, a person who is seeking up the owner of a domain name is wanting to buy it. There are hundreds of millions of registered names, and for many people and companies, their perfect domain name has already been taken. Sometimes buying an existing domain simply requires getting in touch with the owner and working out a deal. It's frequently much more difficult, but it all depends on who owns the domain name, any plans they might have for the website, and how amenable they are to negotiations.

- **Inquire about goods or services:** On occasion, a website might not offer all the information required to understand its goods or services. In situations like these, the domain holder might be able to fill in the blanks or respond to inquiries that the website might not be able to address.

- **Check for authenticity:** It's critical to confirm that a website is precisely what it purports to be before transacting business through it. The internet is rife with false information, and it's shockingly simple for websites to purposefully or unintentionally mislead themselves. A website's legitimacy can be confirmed by looking up the domain owner, which can give parties looking to conduct financial transactions some piece of mind. Similar to this, knowing whether a website is legitimate will make it simpler to believe any information that may be provided.

- **Report a technical issue:** If there are no obvious ways to report a website's malfunction, getting in touch with the owner directly can be helpful. Being invested in the website's maintenance, the owner is frequently appreciative of being made aware of a problem.

- **Verify your own information:** If you own a domain, it's critical to ensure that search results for your website accurately reflect it. With hundreds of millions of domains registered, information errors are all but certain. By keeping your personal information current, you can make it easier for prospective purchasers to contact you if you choose to sell your domain in the future.

3.5.4 Finding a domain name owner

There are a few techniques to determine who owns a website if you know the domain name. Searching WHOIS databases is typically the most straightforward method of locating a domain name owner. There are various different methods for finding the owner of a domain name if a WHOIS search is unsuccessful.

WHOIS databases

These are completely free, publicly accessible search engines that list practically all websites and domain names. In order to gather all the data on the acquisition, resale, and transfer of domain names, WHOIS services collaborate with registrars like Domain.com.

WHOIS services and ICANN

There are numerous WHOIS databases, and the Internet Corporation for Assigned Names and Numbers coordinates them all (ICANN). A nonprofit organisation called ICANN is responsible for maintaining and protecting domain names, websites, and other internet namespaces. They have coordinated a central registry that compiles all registered domains since 1998.

3.5.5 Other methods for searching domain ownership

Before giving up, try a few other research techniques if your attempt to locate a domain name owner through the WHOIS databases does not yield the expected results.

Carefully inspect the website

The website itself may be able to provide contact information, even if the domain name owner has concealed their information in the WHOIS database. Look for links that say "contact information" or something similar as you scroll down the page, paying close attention to the top and bottom of the page. Even if it doesn't put you in touch with the owner directly, they might be able to direct you to someone who can.

Social media

Check every single social media account connected to the website or domain name you are investigating. Think of tools like Instagram, Twitter, Facebook, and LinkedIn. Once more, search for any mention of "contact information" or email addresses that may be present.

3.6 SUMMARY

The use of scientific techniques in criminal investigations is known as forensics. With the sole objective of solving a riddle, it is a distinct discipline of study that incorporates knowledge from all branches of science, including entomology, genetics, geology, and mathematics. The general people is extremely fascinated by it. Millions of us are familiar with how luminol may be used to reveal bloodstains in the bath and how rifling marks on a bullet can identify a murder weapon thanks to television dramas.

The field of computer forensics investigates how computers are used to commit crimes. The information on a hard disc may be vitally important in situations involving child pornography, identity theft, blackmail, and accounting fraud. Disk analysis and email tracking are now typical methods used by law enforcement agencies all over the world.

The focus is shifted from a specific system to the entire Internet through internet forensics. Finding illicit conduct and the persons responsible for it becomes extremely difficult with a single global, enormous network. The credit card information of a victim in Germany can be stolen by a con artist in the United States using a web server in Korea.

Regrettably, the fundamental protocols that control Internet traffic were not created to deal with issues like spam, viruses, and other such issues. Verifying the origin of a message or the owner of a website can be challenging, if not impossible. The little things become significant in situations like this. The organization of files on a website or the method used to fake email headers can function similarly to a fingerprint at a physical crime scene.

3.7 LIST OF REFERENCES

1] Guide to computer forensics and investigations, Bill Nelson, Amelia Philips and Christopher Steuart, course technology,5th Edition,2015.

2] Incident Response and computer forensics, Kevin Mandia, Chris Prosise, Tata McGrawHill,2nd Edition,2003.

3.8 UNIT END EXERCISES

1) What do you mean by World Wide Web Threats?
2) Define Web threats.
3) What are web threats?
4) How do web threats work?
5) How to spot web threats?
6) What are the types of web security threats?
7) Explain: Hacking and Illegal access.
8) Describe the Obscene and Incident transmission.
9) What is Domain Name Ownership Investigation?
10) Who is a domain owner?
11) What is the length of domain ownership?
12) Why look up a domain owner?
13) How to find a domain name owner? Illustrate other methods for searching domain ownership.

4

E-MAIL, MESSENGER, SOCIAL-MEDIA AND BROWSER FORENSICS

Unit Structure

4.0 OBJECTIVES

- Discuss the functions of the client and server in email and the tasks involved in investigating e-mail crimes and violations
- Identify some of the available forensic tools
- Describe the utilization of social media forensics
- Discuss how to investigate browser forensics

4.1 INTRODUCTION

This chapter describes how to track, recover, and analyze emails using disc editors and general-purpose forensics tools for email investigations. Email is a popular form of communication, and different email

applications have different methods for storing and tracking email. Some require their own folders and data files on the local machine and are installed separately from the OS. Some avoid installing any new software on the client machine by making use of already installed software, including Web browsers. Also, a lot of people use social media platforms like Twitter, Facebook, and LinkedIn to interact. This chapter demonstrates the interactions between email clients and servers as well as their respective email programs.Also, a summary of the legal concerns influencing discussions on social media is provided. Also, we have taken into consideration the browse forensics.

4.2 E-MAIL FORENSICS

Emails have become the most common method for business communication, document transfers, and transactions on computers and mobile devices as a result of the prevalence of the internet. With its emergence, email security mechanisms have also been put in place to lessen illicit activity like ransomware, phishing emails, and business email compromise. The need to study individual emails and extract data from them for legal purposes, such as civil lawsuits and legally supported criminal investigations, does arise. This is the use case for email forensics.

The term "email forensics" means exactly what it says. the forensically sound study of emails and their contents to establish their authenticity, source, date, time, true sender, and recipients. The purpose of this is to make digital evidence that can be used in criminal or civil proceedings admissible.

4.2.1 e-mail analysis

A subset of digital forensics called email forensics concentrates on the forensic examination of email in order to gather digital evidence for cyberattacks and other cyber events. It includes a thorough forensic study of a number of email-related elements, including Message-IDs, transmission paths, attached files and documents, IP addresses of servers and machines, etc.

The following methods are employed by email forensic specialists to evaluate emails and examine the digital evidence:

1. Examination of Email Headers

Email headers contain crucial data, such as the sender and recipient's names, the servers and other devices the message has passed through, etc. Figure 1 highlights a few of the crucial email header fields.

Figure 1: Sample e-mail header

Investigators and forensics specialists are assisted in the email inquiry by the crucial information in email headers. For example, the Delivered-To field includes the email address of the receiver, and the Received-By field includes:

- IP address of the most recent SMTP server accessed.
- It's SMTP ID.
- the moment the email was received, both in time and date.

Similar information, including the IP address and hostname of the sender, is provided in the Received: from field. Once more, such details can be useful in catching the offender and gathering proof.

2. Email Server Analysis

To determine an email's source, email servers are inspected. For instance, associated ISP or Proxy servers are checked if an email is removed from a client application, the senders, or the recipients, as they frequently save copies of emails after delivery. Moreover, servers keep records that can be examined to determine the computer's address where the email originated.

It is important to note that major Internet Service Providers (ISPs) often archive the logs for the Hypertext Transfer Protocol (HTTP) and Simple Mail Transfer Protocol (SMTP). If a log is preserved, it may be difficult and time-consuming to find pertinent emails using decompression and extraction methods. It is therefore best to review the logs as soon as you can.

3. Examining Devices on Networks

Sometimes, server logs are not accessible. This may occur for a variety of reasons, including when servers are not set up to keep logs or when an ISP won't provide the log files. In such a case, investigators can look for an email message's origins in the logs kept by network devices like switches, firewalls, and routers.

4. Fingerprints of the Sender Mailer

Email communications also include X-headers in addition to common headers like Subject and To. They can be used to identify the email client program, such as Outlook or Opera Mail, and are frequently added for spam filter information, authentication results, etc. Moreover, the original sender, or the IP address of the sender's machine, can be identified using the x-originating-IP header.

5. Message-IDs

A distinctive identifier called Message-ID aids in the global forensic analysis of emails. It is made up of a lengthy string of letters and numbers that ends with the Fully Qualified Domain Name (FQDN). The client software used to send emails, such as Mail User Agents (MUA) or Mail Transfer Agents, generates message IDs (MTA). A Message-ID is composed of two components. There are two parts: one before @ and one after @. Information like the message's timestamp is included in the message-first ID's portion. This information contains the time stamp for the message's transmission. Information pertaining to FQDN is contained in the second section of the message-ID.

6. Identifiers for embedded software

The email programme that a sender uses occasionally enables the inclusion of extra details about the message and any associated files. For instance, it appears as a Transport Neutral Encapsulation Format (TNEF) or custom header in Multipurpose Internet Mail Extensions (MIME) content. These portions can be thoroughly analysed to provide important information about the sender, such as the MAC address, Windows login username, PST file name, and more.

7. Use of Bait

When a suspect or cybercriminal's whereabouts are unknown, an email investigation approach called the bait tactic is employed. In this scenario, the investigators email the suspect with a http: “<img src>” tag. The investigators' PC serves as the image source. The HTTP server that hosts the image logs the IP address of the machine when the suspect views the email in a log entry. The IP address might be used by the detectives to find the suspect. Suspects may sometimes use a proxy server to hide their identify as a preventative step. In that scenario, the proxy server's IP address is noted. Yet, the suspect can be located by looking through the proxy server's log.

The investigator can send an email with one of the following contents if the log is not available either:

- with an Active X object on an HTML page.
- a Java applet that has been embedded and is set up to run on the recipient's computer.

Both of these have the ability to capture the suspect's computer's IP address and transmit it to the investigators' email.

8. Forensics of bulk emails

Huge mailbox collections are frequently looked at, studied, and utilized as proof in court. Hence, working with enormous mails is often required of legal practitioners. The majority of email client programmes, including Outlook and Gmail, have a dashboard with a number of useful features. But, if you solely use keywords in the interface, you might not achieve the desired outcomes.

When emails are presented as case-related evidence, the date and time are two email properties that are seen to be essential. However, hackers may tamper with these characteristics, and emails can be falsified just like physical papers. Also, since an email doesn't travel directly from the recipient to the sender, accurately calculating its real course is a challenging task.

9. The value of utilizing the hashing algorithm

The two most important hashing algorithms utilized by experts in digital forensics are MD5 and SHA1. In email forensics investigations, the employment of the MD5 and SHA1 hashing algorithms is normal procedure. These algorithms make it possible for forensic investigators to safeguard digital evidence from the time it is collected until it is presented in court. Hash values are crucial because throughout an inquiry, electronic documents are shared with legal experts and other parties. Hence, it is essential to make sure that everyone has identical copies of the files.

4.2.3 e-mail spoofing

What is email-spoofing?

In email spoofing, an attacker conceals their identity by using an email header to pass as a trusted sender. (An email header is a piece of code that includes information about the sender, recipient, and tracking information.)

While email spoofing is a particular strategy that involves falsifying email header data, attackers might employ alternative strategies to achieve the same effects. Attackers might, for instance, design an email domain that closely resembles the legitimate sender's domain in the hopes that receivers won't spot the mistake. Using the domain "@1egitimatecompany.com" rather than "@legitimatecompany.com" is one illustration. To disguise themselves as a sender, attackers may also

alter the display name. For instance, they can send malicious emails from "LegitimateCEOName@gmail.com" rather than

LegitimateCEOName@legitimatecompany.com.

Successful email spoofing attempts will appear as legal domains, such as cloudflare.com, as opposed to a misspelt domain (janeexecutive@ jan3scompany.com) or an address not connected to the domain at all (janetherealceo@gmail.com). This is the fundamental distinction between these tactics. The specific subject of this post will be emails with forged headers.

The more general category of domain spoofing includes email spoofing. Attackers will try to impersonate a website name (or email address) in domain spoofing, usually as part of phishing assaults. Beyond email, domain spoofing can be used to make phoney websites or false adverts.

How does email-spoofing work?

Attackers fake the fields that email recipients may view using scripts. These fields, which contain the "from" and "reply-to" addresses, are located in the email header. Here is an illustration of how these fields may appear in a hoax email:

- From: “Legitimate Sender” email@legitimatecompany.com
- Reply-to: email@legitimatecompany.com

Because the email transmission technology Simple Mail Transfer Protocol (SMTP) lacks an internal mechanism for verifying email addresses, it is possible to forge these fields. In actuality, the SMTP envelope and the header of an email both contain the sender's and recipient's email addresses. The recipient's viewable fields are included in the email header. Yet, the data that servers utilize to deliver an email to the proper address is contained in the SMTP envelope. Nevertheless, these fields are not necessary for a successful email transmission. Email spoofing is simple since the SMTP envelope never verifies the header and the recipient cannot view the contents of the envelope.

Because a faked email appears to be from a trustworthy sender, recipients might be persuaded to click on harmful links, divulge sensitive information, or carry out other acts they wouldn't normally do. Due to this, phishing scams frequently employ email spoofing.

Attackers may occasionally employ other strategies to increase the legitimacy of a faked email domain. A company's logo, branded artwork, and other design components can be copied, or words and language might be used that seem appropriate for the imitation business.

How to protect against email-spoofing

Some actions can be taken by email recipients to guard against email spoofing:

- Beware of messages that demand quick or urgent action: Recipients should be careful of any unexpected or unsolicited emails that request sensitive information, money, or other urgent action. For instance, it would be suspect if an application suddenly asked you to update your login details.

- Examine email headers: Some email applications provide a method for seeing an email's header. In Gmail, for instance, selecting "Show original" on a certain email will display the email header. To find the "Received" portion, locate the header's "Received" section. The email is probably faked if a domain other than the one in the "From" address appears.

- Use software that detects fake messages: By requiring authentication for receiving emails, anti-spam software can prevent spoofing efforts.

  In order to stop attackers from sending messages from their domain, domain owners can also take action. Organizations can achieve this by setting up Domain Name System (DNS) records just for authentication. They consist of:

- Sender Policy Framework (SPF) records: SPF records list the servers that are permitted to send emails from a specific domain. In this manner, a fictitious email address connected to a domain would not appear on the SPF record and would fail authentication.

- DKIM records: DomainKeys Identified Mail (DKIM) records use two cryptographic keys: one public and one privatefor authentication. The DKIM record contains the public key, and the DKIM header is digitally signed using the private key. False emails from a domain with a DKIM record won't pass authentication since they aren't signed with the right cryptographic keys.

- Domain-based Message Authentication Reporting and Conformance (DMARC) records: DMARC records contain DMARC policies that instruct email servers what to do following an SPF and DKIM record check. Based on these tests, domain owners can establish policies that determine whether to restrict, permit, or send messages. These records offer further defense against email spoofing since DMARC standards compare against other authentication policies and let domain owners establish more precise constraints.

By integrating phishing and malware protection, security directors can also take action at the organizational level to shield staff members from email spoofing.

4.2.4 Laws against e-mail Crime

Every action and response that takes place online is subject to legal and technological considerations. The phrase "cyberlaw" refers to the legal problems that arise in cyberspace. It is an integration of many laws to

handle and address these problems and difficulties that people on the web daily present.

There is currently no comprehensive legislation to address cybercrime anywhere in the world because it is a field that is still evolving towards specialization. Nonetheless, the Government of India has the Information Technology Act,2000 in place to control dangerous online actions that infringe an internet user's rights. There are situations when it may be discovered that the IPC & IT Act's sections that punish such conduct overlap.

Penalties against cybercrime

Data theft, virus transmission into a system, hacking, data destruction, and blocking access to the network to a legitimate person are all punishable under sections 43 and 66 of the IT Act with a maximum sentence of three years in prison or a fine of Rs. 5 lacs, whichever is greater. Data theft is also punishable under Sections 378 and 424 of the IPC, with maximum sentences of 3 years in jail, a fine, or both, and 2 years in prison, a fine, or both, respectively. According to Section 426 of the IPC, it is illegal to deny access to a legitimate person or harm a computer system and is punishable by up to three months in prison, a fine, or both.

Under Section 65 of the IT Act, tampering with computer source material is a criminal offence. Infractions of privacy are punishable under Section 66E. According to the law, anyone who takes, publishes, or distributes a picture of someone's private parts without getting their permission has violated their right to privacy and faces up to three years in prison, a fine of up to 2 lacs or both.

Cyberterrorism is a key topic that is addressed by Section 66F, and it is punishable. It lists the actions that constitute cyber terrorism, such as denying access, breaking into a network, or sending a virus or malware that could potentially kill or injure someone. All of these actions are done with the intention of endangering the integrity, sovereignty, unity, and security of India or inspiring fear in the country's citizens.

Receiving stolen computer resources or equipment dishonestly is an infraction that is covered under Section 66B of the IT Act and Section 411 of the IPC. According to Section 66C of the IT Act, anyone found guilty of using another person's identity credentials for fraud or dishonest behavior faces up to three years in prison and a sentence of Rupees three lakhs in fines. According to Section 66D of the IT Act, utilizing a computer resource to impersonate someone else is considered cheating. Equivalent provisions are provided for these offences in Sections 419, 463, 465, and 468 of the IPC.By failing to implement and maintain a reasonable and rigorous method to protect the sensitive data of any person in their control, corporations are subject to penalties under the IT Act in addition to individuals. Such a body corporate is responsible for making restitution to the party who incurred harm as a result of the corporation's carelessness.

The IT Act also gives the Central Government the authority to direct the blocking of public access to any information on a computer resource or intermediary if it deems it necessary in the interest of the State, in addition to the provisions for punishment. Such information can also be intercepted, decrypted, or monitored.

4.3 MESSENGER FORENSICS: YAHOO MESSENGER

This section investigated the MSN Messenger forensic artefacts found on a suspect's computer to make contact between that individual and his victims. The investigations covered in this section concentrate on Yahoo Messenger 7.0 and look at the methods for using it to identify comparable objects.

Although it has undergone significant change over the years, Yahoo Messenger began as a one-to-one instant chat system created and distributed by Yahoo in 1998. The business started off as a sort of student hobby in April 1994 as an Internet directory service, but over time it developed into the most popular website on the Internet.

Yahoo provides users with a variety of chat rooms, as well as the option to create and manage "Yahoo Groups" in order to manage mailing lists, share files, trade messages, and other functions. Yahoo also functions as an Internet search engine and chat platform.

Updates for Yahoo Messenger are frequent, in part because security holes are patched, but more recently also because the communications protocol supporting the product is changed in an effort to thwart the efforts of software developers producing third-party programmes (like Trillian) to handle Yahoo "chat."

In contrast to MSN Messenger, Yahoo Messenger makes use of data files to keep a range of data about how its features, particularly file transfers and connections, were used. They provide much more room for conventional computer forensics than MSN Messenger and are helpful in determining connections made between one party and another.

4.4 SOCIAL MEDIA FORENSICS:FORENSICS TOOLS FOR SOCIAL MEDIA INVESTIGATIONS

Although software for social media forensics is being created, there are currently few tools accessible.In addition, there are several uncertainties around the application of the data gathered by these technologies in arbitration or court. Investigators frequently encounter the issue of discovering information unrelated to a case, and occasionally it necessitates stopping to get a different warrant or subpoena, such as when looking into a fraud allegation and discovering evidence of corporate espionage.It may also be necessary to obtain the consent of the individuals whose information is being analyzed before using social media forensics tools.

Several OSN solutions employ specialized Web crawlers to find data, however they are inefficient since it takes too long to find the data. Nonetheless, there are some useful software programmes on the market right now. There are many tools available from the Afentis Forensics group, including Facebook Forensics, YouTube Forensics, Twitter Forensics, and LinkedIn Forensics (http://afentis.com/expert-witness/forensic-software/). For instance, Facebook Forensics allows you to download a person's whole profile.Another tool, X1 Social Discovery (www.x1.com/products/x1_social_discovery/), can be used in two modes in Facebook: a credentialed user account (which requires the username and password of the person under investigation) and a public account (created to examine the publicly accessible posts of people or groups). Moreover, X1 offers Twitter and YouTube facilities. Researchers also developed an open-source tool to target Facebook accounts (Huber, Mulazzani, et al., "Social Snapshots: Digital Forensics for Online Social Networks," ACSAC '11, Proceedings of the 27th Annual Computer Security Applications Conference, December 2011). This technology, which is not yet distributed, was used to collect screenshots of public material with Facebook users' permission.

4.5 BROWSER FORENSICS

Browser forensics is mostly used to examine a computer's browser history and general web activity in order to look for any suspicious activity or content access. In order to obtain accurate information on a targeted system, this also refers to tracking website traffic and analyzing server-generated LOG files.

4.5.1 Cookie Storage and Analysis

What is storage for cookies?

A website you visit will place information known as cookies on your computer. Although each cookie in certain browsers is a little file, all cookies are kept in a single file in Firefox's profile folder.

If you're curious about "where cookies are stored," the answer is straightforward: your web browser will store them locally to remember the "name-value pair" that uniquely identifies you. The web browser sends that information to the web server in the form of a cookie if the user visits that website again in the future.

How are cookie data analyzed?

How does Chrome verify cookies?

- Open the developer console by selecting Inspect with the right-click menu.
- Go to the console's Apps tab.
- Under the Storage section, widen the dropdown for Cookies. To view the cookie details, choose the website under Cookies.

4.5.2 Analyzing Cache and temporary internet files

Windows Internet Explorer and MSN Explorer save webpage content in the Temporary Internet Files (or cache) folder on the computer's hard drive for easy access.

How to locate temporary internet files?

This section describes how to view a list of the temporary internet files (stored cache data) that your browser keeps. These files are bits of information that speed up the loading of frequently visited websites. A mobile device like a smartphone or a tablet cannot see temporary internet files.

Method 1: Finding Cache Files on Mac

Open your Mac's Finder. Click the blue smiling face icon on the bottom-left to open your Finder.

- Make sure the menu bar on the top-left says "Finder."

2: **Hold down the Alt or ⌥ Option key on your keyboard.** This will allow you to reveal the **Library** folder on the **Go** menu.

3: **Click the Go tab on the menu bar.** While holding down the **alt (option)** key, click the **Go** at the top of your screen. It will open a drop-down menu.

4: **Click Library on the menu.** This will open your user library folder.

- The Library option only shows up when you press down the **alt (option)** key.

5: **Double-click the Caches folder.** You can find all the internet cache stored on your computer here.

6: **Find and double-click the "com.apple.safari" folder.** You can find different types of Safari browsing cache in this folder.

- If you're using another web browser, look for your browser's software company here. For example, look for "Google" if you're using Chrome, and "Mozilla" for Firefox.

7: **Double-click the "fsCachedData" folder.** You can find your Safari browsing cache data files here.

Method 2: Finding Cache Files on Windows

1: **Open your Start menu.** Click the Start menu icon on the lower-left corner, or press the ⊞ Win key on your keyboard.

- Alternatively, you can open the search or Cortana from your menu bar.

2: **Type Show hidden files and folders into the menu search.** Your file and folder settings will show up at the top of the search results.

3: **Click the Show hidden files and folders option in the search results.** This will open your Folder Options window.

4: **Select "Show hidden files, folders, and drives" in the Advanced Settings box.** When this option is selected, you can view and browse all hidden and system folders on your computer.

5: **Click the Apply button.** You can now view and open hidden folders.

6: **Open the This PC or My Computer app.** This app looks like a desktop computer icon. You can find it on your Start menu or on your desktop

7: **Double-click your main drive.** This is the hard drive where your Windows system is set up.

- This drive is usually named **Local Disk** and/or the **C:** drive.

8: **Double-click the "Users" folder.** You can find a list of all the users saved on your computer here.

9: **Double-click your user folder.** Your user folder is named by your user name. You can find your user files here.

10: **Double-click the "App Data" folder.** This is a hidden folder so it looks like a transparent folder icon in your user folder.

11: **Double-click the "Local" folder.**

12: **Find and double-click the "Microsoft" folder in Local.** You can find your Internet Explorer or Microsoft Edge cache in this folder.

- If you're using a different web browser, look for your browser's software company here. For example, look for "Google" if you're using Chrome, and "Mozilla" for Firefox.

13: **Find and double-click the "Windows" folder in Microsoft.**

14: **Find and double-click the "Caches" folder.** You can view all your Internet Explorer or Edge browsing cache in this folder.

4.5.3 Web browsing activity reconstruction

One area of computer forensics that is becoming more and more vital is web browser forensics. This is due to the fact that evidence pertaining to an individual's Internet usage may be relevant in a growing number of criminal and civil proceedings. In this section, Pasco and Galleta, two open-source programs, are used to reconstruct web browsing behavior. These programs are used to examine cookie and index.dat files.

Electronic evidence has frequently influenced the results of high-profile civil lawsuits and criminal investigations over the past few years. These cases have involved everything from proving employee misconduct leading to termination of employment under unfavorable circumstances to proving intellectual property theft and insider trading that violates SEC regulations. Investigating a suspect's web usage is a critical stage in computer forensics. This data may be helpful for a variety of purposes, including looking into a company's policy violation and looking for corporate espionage and federal offences.

Examining a suspect's web browsing history could provide critical clues to solving a case since criminal, corporate or civil investigations involving illegal or improper web usage usually requires expert analysis of the information stored by a web browser as a result of a suspect's Internet activity. Many people browse the Internet each day using common web browsers such as Microsoft Internet Explorer, Mozilla Firefox, Netscape Navigator, Opera and Safari with Internet Explorer being by far the most common of these browsers.So, it is typically pertinent to analyze the information in Internet Explorer into a human readable format during forensic analysis. Two open-source tools used to rebuild a person's web usage patterns are Pasco and Galleta. Both Pasco and Galleta are designed to run on a variety of operating systems, including Windows (through Cygwin), Mac OS X, Linux, and BSD.

- **Pasco**

Keith J. Jones, a Principal Computer Forensic Consultant at Foundstone, Inc., created Pasco, an Internet Explorer activity forensic analysis tool. One of the guiding principles of computer forensics is that all analysis procedures must be thoroughly documented, reproducible, and have an acceptable margin of error because many significant files in Microsoft Windows have undocumented structures. There are currently few open-source techniques and resources that forensic investigators can use to analyze the data stored in exclusive Microsoft files.

The reconstruction of a subject's online behavior is necessary for many computer crime investigations. To look through the information in Internet Explorer's cache files, the program Pascoa Latin word for "browse"was created. The basis of Pasco's investigation is based on the information in an index.dat file being parsed and the output being produced in a field-delimited format so that it may be loaded into a spreadsheet tool. Pasco was designed to run on a variety of operating systems, including Windows (through Cygwin), Mac OS X, Linux, and BSD.

- **Galleta**

Keith J. Jones, a Principal Computer Forensic Consultant at Foundstone, Inc., also created Galleta, an Internet Explorer cookie forensic analysis tool. Since reconstructing a subject's Internet Explorer cookie files is a common requirement in computer crime investigations, Galleta examines the structure of the data included in the cookie files. Galleta, which is Spanish for "cookie," was created to automate this process. The inspection methodology of Galleta is built around parsing the data in Cookie files and producing the results in a field-delimited format that can be loaded in a spreadsheet tool. Galleta is designed to run on a variety of operating systems, including Windows (through Cygwin), Mac OS X, Linux, and BSD.

4.6 SUMMARY

Phishing, pharming, and spoofing scam techniques are employed by email fraudsters. Users are frequently lured to websites or asked for sensitive information in phishing emails. Phishing emails link visitors to websites that impersonate real companies or official government websites where they ask for personal information about the victims. A client/server architecture is the distribution of email messages from a single central server to linked client computers used in both intranet and Internet e-mail settings. Email services are offered by the server using server email software. Email programmes, often known as e-mail clients, are used by client computers to connect to the email server to send and retrieve emails.

Unsettling components are appearing on the dark web as a result of technology's ongoing progress. Clever people are misusing their abilities and abusing the internet for bad activities and occasionally financial gain. Thus, cyber law is a current necessity. Because of the enormous difficulty in navigating the cyberspace, some activities take place in an unregulated, legal limbo. So, there is still a long way to go until India has a broad and all-encompassing law for cybercrimes.

4.7 LIST OF REFERENCES

1) Guide to computer forensics and investigations, Bill Nelson, Amelia Philips and Christopher Steuart, course technology,5th Edition,2015.

2) Incident Response and computer forensics, Kevin Mandia, Chris Prosise, Tata McGrawHill,2nd Edition,2003.

4.8 UNIT END EXERCISES

1) Explain e-mail analysis.

2) Describe e-mail spoofing.

3) Discuss on laws against e-mail Crime.

4) Write a note on: Messenger Forensics: Yahoo Messenger.

5) Explain Social Media Forensics: Forensics Tools for Social Media Investigations.

6) Write a note on Browser Forensics.

7) What do you mean by Cookie Storage and Analysis?

8) Explain the concept of Analyzing Cache and temporary internet files.

9) Describe the Web browsing activity reconstruction.

5

INVESTIGATION, EVIDENCE PRESENTATION AND LEGAL ASPECTS OF DIGITAL FORENSICS

Unit Structure

5.0 OBJECTIVE

- The objective of this chapter is to make learners understand the principles and practices of presenting digital evidence in court proceedings. Digital forensics deals with the collection, preservation, analysis, and presentation of electronic evidence, which can be used in a court of law.
- To learn how to collect and preserve digital evidence in a manner that is legally admissible. This involves understanding the legal requirements for digital evidence, as well as the rules of evidence and court procedures.
- Additionally, studying these aspects of digital forensics can also help learners to understand how to present digital evidence in a clear and convincing manner in court. This includes preparing reports and presenting evidence in a manner that is understandable to judges and juries.
- Overall, it is essential for learners to understand how professionals working in the field of digital forensics, as well as for legal professionals need to use digital evidence in court proceedings.

5.1 INTRODUCTION

Cyber forensics is the practice of gathering, scrutinizing, interpreting, documenting, and demonstrating electronic evidence related to computers. It involves analyzing data from a system or device to create physical evidence that can be presented in court. The examination process entails making a digital or soft copy of the system's storage, with the ultimate goal of determining who is responsible for a security breach. The investigation is conducted on a software copy to prevent any harm to the system. In today's technological era, cyber forensics is a crucial and essential factor.

5.2 WHAT IS DIGITAL FORENSICS?

- Digital forensics is a subfield of forensic science that deals with the recovery and analysis of data found in digital devices relating to cybercrime. Originally used as a synonym for computer forensics, the term has now broadened to encompass the investigation of any device capable of storing digital data.

- Digital forensics is also a relatively new and dynamic field of forensic investigation that utilizes various techniques to gather, validate, identify, analyze, interpret, document, and present digital evidence for use in civil, administrative, and criminal proceedings.

- Digital evidence can be used as evidence in a legal case. For digital evidence to be considered admissible in a court of law, it must adhere to a specific set of rules and standards

- Although the first computer crime was reported in 1978 and legislation such as the Florida computers act followed, it was not until the 1990s that digital forensics became a recognized term. It wasn't until the early 21st century that national policies on digital forensics emerged.

- The process of digital forensics involves identifying, preserving, analyzing, and documenting digital evidence, which is then presented in a court of law when required.

5.2.1 What is Evidence?

- The term "evidence" comes from the Latin word ēvidēnt-, which means "apparent" or "obvious." This word is commonly used in legal contexts and dramas, as evidence is required to establish a connection between a person and a crime or crime scene.

- Evidence is employed in various forms to demonstrate that a statement or assertion is valid, such as when we say that the chocolate marks on your face and the crumbs on the table are proof that you consumed the remaining brownies.

5.2.2 What is Digital Evidence?

- Digital evidence refers to information and data that are relevant to an investigation and are either stored on, received or transmitted by electronic devices.

- It can be collected by securing and examining electronic devices. This type of evidence is similar to latent evidence such as fingerprints or DNA, as it is often hidden or not readily apparent.

- Unlike physical evidence, digital evidence can easily cross jurisdictional borders and can be quickly altered, damaged or destroyed with minimal effort. Additionally, digital evidence can be time-sensitive, meaning that it may lose its evidential value if not collected and analyzed promptly.

- Although credit card fraud and child pornography are two examples of electronic crimes that are frequently associated with digital evidence, this technology has other uses as well. Today, a variety of crimes are prosecuted using digital evidence. For instance, a suspect's email or mobile phone records may contain important information about the suspect's motives, their participation in a crime, and their relationships with other suspects.

- Law enforcement agencies are integrating the practice of computer forensics, which involves collecting and analyzing digital evidence, in order to combat e-crime and gather relevant evidence for all types of crimes. The challenge for

law enforcement agencies lies in the need to provide training to officers on how to properly collect digital evidence, while also keeping pace with the constantly evolving technologies, such as computer operating systems.

5.2.3 Issues Need to be Considered When Evaluating Digital Evidence?

- Evidence is physical proof that can support a fact.

- Digital evidence, on the other hand, refers to evidence in electronic form, which can take various forms and come from different sources, such as computers, smartphones, and other electronic devices. Before collecting digital evidence, a digital forensics examiner must have the legal authority to do so.

- The **sensitive** nature of the evidence presents one of the main challenges in digital forensic investigation since its value might be lost if it is not properly gathered, stored, and protected. Digital evidence's **fragility** can change depending on the type of data and how volatile it is. Evidence must fulfill specific requirements in order to be admitted in court, including appropriate collection, relevancy, authenticity, and dependability.

5.2.4 Why Collect Evidence?

- Collecting evidence serves several important purposes, including:

1. **Future Prevention:** By collecting and analyzing evidence from a security incident, organizations can gain insights into how the attack occurred and identify vulnerabilities in their systems or processes. This information can be used to prevent similar incidents from happening in the future.

2. **Accountability and Justice:** Collecting evidence is crucial for identifying the individuals or groups responsible for the attack and holding them accountable for their actions. This can involve working with law enforcement agencies to prosecute perpetrators and seek justice for victims.

3. **Learning and Improvement:** The analysis of evidence can also provide valuable insights into how security incidents

occur, what techniques are being used by attackers, and how to improve security measures to better protect against future attacks. This information can be shared with other organizations to help prevent similar incidents from occurring in their systems.

- Overall, collecting evidence is essential for understanding the nature of security incidents, holding individuals accountable for their actions, and preventing future attacks.

5.3 AUTHORIZATION TO COLLECT EVIDENCE

- In digital forensics, the authorization to collect evidence depends on the specific circumstances and jurisdiction. Generally, law enforcement officers and digital forensic investigators must follow the applicable laws and regulations that govern the collection and use of digital evidence.

- Before seizing and searching digital devices or data, law enforcement officials frequently need a judge's warrant, which they can get from a variety of sources. The warrant must be supported by probable cause and set forth the precise items or information that will be gathered. In rare situations, such as when there is a threat to the public's safety or a risk that evidence would be lost, law enforcement officials may also be permitted to gather digital evidence without a warrant.

- In addition to legal requirements, digital forensic investigators must also adhere to ethical and professional standards. They should obtain the consent of the device owner before conducting a forensic examination and should respect the privacy of individuals whose data is being collected.

- Overall, the authorization to collect evidence in digital forensics depends on the laws and regulations in the relevant jurisdiction, as well as ethical and professional standards. It is important for digital forensic investigators to be aware of the legal and ethical considerations when collecting and handling digital evidence.

5.4 ACQUISITION OF EVIDENCE

- Acquiring evidence in digital forensics involves collecting data from digital devices or storage media, such as computers, smartphones, hard drives, and other electronic devices.

- The process of acquiring digital evidence can be complex and requires a high level of technical skill and knowledge. Here are some of the key steps involved in the acquisition of evidence in digital forensics:

1. **Identification:** The first step is to identify the digital devices or storage media that may contain relevant evidence. This may involve examining a suspect's computer or mobile device, as well as any other devices that may be relevant to the investigation.

2. **Preservation:** The next step after identifying the pertinent devices is to preserve the data stored there in order to prevent its inadvertent, deliberate, or unintentional deletion or modification. This might entail making a forensic duplicate of the device, which is a clone of the data bit-for-bit.

3. **Collection:** Data can be gathered and examined after it has been kept. This could entail employing specialised software to look for particular data kinds, such emails, documents, or photographs.

4. **Analysis:** The collected data is analyzed to determine whether it contains evidence that is relevant to the investigation. This may involve examining metadata, file headers, and other data to reconstruct a timeline of events.

5. **Presentation:** Finally, the results of the analysis are presented in a clear and understandable format, such as a written report or a presentation to a court or other legal authority.

- Collecting digital evidence requires adherence to strict standards and protocols to uphold the credibility of the evidence and uphold the rights of all parties involved in the

investigation. It is imperative to ensure that the evidence gathered is admissible in court and immune to challenges based on tampering or other irregularities.

5.4.1 General Procedure

- **Identification of Evidence:** It is crucial to distinguish between pertinent evidence and useless irrelevant material.

- **Evidence Preservation:** The evidence must be safeguarded and kept in a condition that closely resembles its original state.
- **Analysis of the Evidence**: To analyse the evidence, one must have a thorough understanding of the issue and employ powerful tools.

- **Presentation of the Evidence**: Effective presentation of the evidence is essential, and it should be done in a way that non-experts can understand it.

5.4.2 Collecting and Archiving

- **Logs:-**After developing a strategy and identifying the evidence to collect, it is important to establish a system for collecting and archiving data. This includes setting up system logging functions to track activity and storing these logs securely with regular backups. Logs and messages can be utilised to track down any damage inflicted by intruders.

- **Monitoring:-** In addition, monitoring activity can help gather statistics, detect irregular behavior, and trace the source of attacks. Any unusual activity or unknown users should be closely inspected. To be transparent, it is recommended to display a disclaimer when users log on that outlines the monitoring being conducted. This helps to establish a level of transparency and trust with users.

5.4.3 Methods of Evidence Acquisition

- There are several methods of evidence acquisition in digital forensics, including:

1. **Disk Imaging:** This is a technique of creating a forensic copy of digital media that bit-by-bit copies exactly the original data. This method serves two purposes: to protect

data preservation and to stop any alterations or changes to the original data during the acquisition stage.

2. **Live Acquisition:** This method involves collecting data from a running computer or other electronic device. Live acquisition is used to collect volatile data that is lost when the device is shut down or restarted. It is important to note that live acquisition may alter or modify the data on the device.

3. **Network Forensics:** This method involves capturing and analyzing network traffic, such as email messages or instant messaging conversations. Network forensics can be used to identify potential sources of attacks and to gather evidence that is stored on remote systems.

4. **Memory Forensics:** This method involves analyzing the volatile memory of a running computer or other electronic device. Memory forensics can be used to recover data that has been deleted or to identify malicious code that is running in memory.

5. **Mobile Forensics:** This method calls for the extraction and analysis of data from portable electronics like smartphones, smartwatches and tablets. Mobile forensics is used to retrieve a variety of data types, including call records, deleted text messages, and other relevant data that can be used in an inquiry.

- Depending on the type of digital media and the needs of the inquiry, it's crucial to select the right acquisition method. Additionally, all methods of acquisition must be used in a way that protects the validity of the evidence and follows stringent policies and procedures..

5.4.4 Volatile Data

- In digital forensics, "volatile data" refers to data that is stored in temporary or volatile memory, such as RAM (Random Access Memory), cache, or registers. Unlike data stored on hard drives or other non-volatile storage media, volatile data is not preserved when a computer or device is shut down or loses power.

- Examples of volatile data that can be useful in digital forensics investigations include information about running processes, open network connections, and data stored in memory that has not yet been written to disk.

- Because volatile data is not preserved when a computer is shut down, it is important for digital forensics investigators to collect this data as quickly as possible after a system is seized. This is typically done using specialized software tools that can capture and preserve volatile data without altering or contaminating the original data.

- Therefore, volatile data is very important in digital forensics investigations since it can provide vital details on the state of a system at the time of an incident. Volatile data must be gathered and analysed using specialised equipment, knowledge, and a thorough grasp of the hazards and constraints associated with doing so.

5.4.5 Acquisition of Live Data

- Live Data Acquisition entails obtaining volatile information from digital devices such as the registry, cache, and RAM via their standard interfaces. Because of its dynamic nature and rapid change, this data must be gathered in real time by investigators.

- Live data capture, however, comes with some dangers. Since the data is not write-protected, even routine operations like browsing files or turning on a computer run the risk of altering or erasing the available evidence. Furthermore, it can be difficult to manage contamination because some tools and commands have the potential to modify file access dates and times, make use of shared libraries or DLLs, or even launch malware. A forced reboot could, in the worst instance, result in the loss of all volatile data. Therefore, when performing live data acquisition, investigators need to be cautious.

- Collecting volatile information can provide valuable insights into the security incident, such as a logical timeline, network connections, command history, running processes,

connected devices, and user login details. This information can be used to better understand the incident and potentially identify the attacker.

- Collecting live data in digital forensics requires a careful and methodical approach to avoid modifying or damaging the data being collected. Here are some general steps to follow when collecting live data in digital forensics.

1. **Obtain the necessary legal authority:** Before collecting live data, it is important to obtain the necessary legal authority to do so. This could involve obtaining a search warrant or other legal authorization to collect the data.

2. **Identify the relevant data sources:** Determine what data sources need to be collected. This could include devices such as computers, servers, mobile devices, or network devices. It is important to have a clear understanding of the systems and devices involved before attempting to collect live data.

3. **Document the system:** Create a detailed inventory of the system being collected. This should include information such as the system configuration, software installed, and network connections.

4. **Use forensically sound methods:** Collect the data using forensically sound techniques, such as making a clone of the device's memory or hard drive bit-for-bit. It is of the utmost importance to employ procedures and tools that do not alter the data being gathered.

5. **Monitor the system:** During the data collection process, monitor the system to ensure that it remains in a stable and secure state. This may involve using tools to monitor system activity or running commands to check for any changes to the system.

6. **Analyze the data:** Once the information has been gathered, it can be analysed to determine the system actions. To find any pertinent evidence, this may entail looking through system logs, network traffic, or application data.

- So remember, digital forensics live data collection demands a meticulous and rigorous technique. To make sure that the data is admissible in court if necessary, it is crucial to apply forensically sound methodologies and document the collecting process.

5.4.6 How to Collect Volatile Evidence Without Destroying it?

- To collect volatile evidence from a running computer system without destroying potential evidence, investigators should follow these basic steps:

1. Keep meticulous records of every action taken on the live system.
2. Take screenshots of the system to record its current condition.
3. Determine the operating system that is installed on the suspected device.
4. The date and time presented by the system should be noted down along with the current local time.
5. Take the RAM data out of the computer and put it on an external drive.
6. Check to see if file or entire disc encryption is being used.
7. Obtain additional volatile operating system data and store it on a removable storage medium.
8. Decide on the best strategy for seizing any hardware and any other data on the hard disc that might be useful as proof.
9. Create a thorough report outlining all the steps done and the results of the investigation..

5.5 DUPLICATION AND PRESERVATION OF EVIDENCE

- Digital evidence are prone to tampering that is they can be copied and altered, which raises questions about its legitimacy and integrity. In order to ensure the dependability and admissibility of digital evidence in a court of law, it is essential to follow the right duplication and preservation methods. By adhering to these processes, the digital evidence's dependability and credibility can be upheld, increasing its value as a piece of legal evidence.

1. **Duplication:** It is essential to use a forensically sound technique that ensures an exact reproduction of the original

evidence when reproducing digital evidence. To do this, a bit-for-bit copy must be created, making sure to include all data, even hidden and deleted files. The copy should be created using a write-blocking device in order to preserve the integrity of the original evidence. During the copying process, this device stops any alterations to the original evidence. The duplicating digital evidence's accuracy and dependability can be maintained by following these procedures.

2. **Preservation:** Digital evidence must also be properly preserved to ensure that it remains unchanged and uncorrupted. This requires maintaining the evidence in a safe and regulated setting with appropriate temperature and humidity control, such as a locked evidence room with restricted access.. Additionally, the evidence should be stored in a format that is compatible with future analysis and should be regularly backed up to prevent loss or corruption.

- Maintaining a chain of custody for the digital evidence is as crucial to following correct duplication and preservation processes. From the time the evidence is gathered until it is presented in court, its location and ownership must always be documented. By following proper procedures for duplication, preservation, and chain of custody, digital evidence can be used with confidence in legal proceedings.

5.5.1 How to Preserve Digital Crime Scene

- The computer investigator must take into account the operating system and apps that are already installed on the computer in addition to worries about the computer owner installing harmful processes and gadgets.

- While typical storage locations like spreadsheet, database, and word processing files make it simple to find evidence, there is also a chance that evidence may also be present in **file slack, deleted files, and the Windows swap file**. Such data is frequently **fragmented**, making it simple for ordinary operations like computer booting or Windows operation to erase such evidence.

- Windows may create new files and access old ones as part of its routine operations when it starts. This operation has the potential to change or destroy previously stored data in the Windows swap file as well as overwrite wiped files.

- **Preserving the digital crime scene** is crucial for any investigation to be successful. Here are some **general steps** to follow to preserve a digital crime scene:

1. Secure the area: First, secure the physical environment to prevent anyone from accessing the scene and tampering with evidence.

2. Document the scene: Take photographs and detailed notes of the scene, including the location and condition of any devices, networks, or other relevant items.

3. Make a copy: Create a forensic image of all digital media at the scene, including hard drives, mobile devices, and other storage devices. This will ensure that the original evidence is not altered in any way.

4. Analyze the image: Use **specialized forensic software** to analyze the image and search for any evidence that may be relevant to the investigation.

5. Preserve the evidence: Store the digital evidence in a secure location to ensure that it is not lost or damaged.

6. Chain of custody: Keep a **strict chain of custody**, documenting who has handled the evidence and when.

7. Follow best practices: Follow best practices for evidence collection and preservation, such as using **write-blockers** to prevent the alteration of the original data and avoiding using the devices for any purpose other than the investigation.

- By taking these actions, investigators may protect the digital crime scene, guaranteeing that the evidence will be accepted in court and be useful in bringing the offender to justice.

5.6 AUTHENTICATION OF THE EVIDENCES

- Authentication of digital evidence in digital forensics involves verifying the integrity and authenticity of the digital evidence collected during an investigation. The following are some of the steps that are typically taken to authenticate digital evidence:

1. **Documentation:** All evidence collected must be documented, including the chain of custody, to ensure that it can be traced back to its source.

2. **Preservation:** During the gathering and analysis process, it is crucial to preserve the validity of the evidence. It is essential to avoid any evidence manipulation or change. In order to accomplish this, the evidence must be kept in a safe and regulated setting, preventing unauthorised access or modifications. The integrity of the evidence can be preserved, keeping its dependability and credibility for forensic and legal purposes, by putting in place the necessary security measures.

3. **Verification:** The authenticity of digital evidence can be verified by analyzing the metadata, file properties, and file signatures. This involves checking the dates and times of the creation, modification, and access to the file, as well as the source of the file.

4. **Hashing:** A cryptographic hash function can be used to generate a unique value for the digital evidence, which can be compared with a known value to confirm its authenticity.

5. **Validation:** The validation of digital evidence involves ensuring that it has not been tampered with or altered during the collection and analysis process.

6. **Documentation:** All steps taken to authenticate digital evidence must be meticulously documented in order to ensure transparency and the possibility of process verification if necessary. A thorough record of the steps taken, the tools used, and the methods used during the authentication process is provided by proper documentation. This documentation is used as a guide and makes it possible

for others to examine and confirm the legitimacy of the digital evidence. The integrity and reliability of the authentication process can be ensured by maintaining thorough and open documentation.

- By these actions, digital forensic investigators can ensure that the digital evidence they collect is authentic and admissible in court.

5.7 ANALYSIS OF EVIDENCE

- Forensic analysis is a process of examining digital evidence to establish facts and draw conclusions about what happened during an incident

- During the analysis , forensic examiners piece together all relevant data from the request and answer questions such as who, what, when, where, and how as it is important to extract evidence by carefully interpreting the acquired information using appropriate methodologies and standards.

- They determine the origin and creator of each item, as well as its significance to the case.

- Instead of using the original media, the examiner should work with a copy or image of it, and they may utilise extra tools to recover deleted files or other important data. However, these tools must be validated for accuracy and reliability. The examiner typically approaches evidence extraction by looking for either something they don't know within something they do know, or by looking for something they know within unstructured data using carving techniques.

- Once evidence is found, it is assembled to reconstruct events and provide factual information, such as identifying the attack scenario, attacker identity, or location. If there are multiple sources of evidence, it is aggregated and correlated to provide a more complete picture of the events. This information is then provided to the requestor.

- Creating a timeline of events is often helpful in providing a clear understanding of the sequence of activities. Examiners

record all their findings in the "Analysis Results List," which fulfills the forensic request.

- Additionally, any new leads or sources of data that emerge during this phase are added to the appropriate lists and may be examined further.

5.7.1 Preparation for Forensic Analysis

- Preparing for forensic analysis of evidence involves several steps to ensure the accuracy and reliability of the analysis. Here are some steps that can be followed:

1. **Documentation:** Proper documentation of the evidence before and during analysis is essential. This involves keeping records of the date and time the evidence was gathered, the source, the chain of custody, and any modifications that were made to the evidence.

2. **Preservation:** To ensure that the evidence is not contaminated or damaged, it should be properly preserved. This can be achieved by keeping the evidence in a safe or other secure location where it is shielded from the weather, dampness, or any other physical harm.

3. **Preparation of the analysis environment:** A controlled environment should be prepared for the analysis, such as a laboratory, where the evidence can be analyzed without any interference or contamination. The laboratory should be equipped with appropriate hardware, software, and other tools required for the analysis.

4. **Verification of Tools:** Verification of the tools to be used in the analysis is important, to ensure that the tools are reliable, and that they do not damage the evidence or interfere with the results. This can be done by conducting a test on a sample data set or through vendor validation or certification.

5. **Analysis plan:** An analysis plan should be developed before the actual analysis. This plan should include a step-by-step procedure for the analysis, the tools to be used, the data to be analyzed, and the expected outcomes.

6. **Expertise and training:** The personnel who perform the analysis should have the required expertise and training in the field of forensic analysis. This ensures that the analysis is conducted in a scientific and unbiased manner.

7. **Quality control and assurance:** A quality control and assurance process should be implemented to ensure that the analysis is conducted accurately, consistently, and in accordance with the forensic standards.

- These procedures can successfully protect the validity of the forensic study and the integrity of the available evidence.

5.7.2 FORENSIC DUPLICATION

- A hard drive, USB drive, or memory card are examples of storage devices that can be duplicated for forensic purposes. This process is also known as disc imaging or bit-by-bit imaging. All of the data, metadata, and related information that were present on the original storage device at the time of duplication are included in this duplicate, which acts as an exact counterpart of the original.

- In digital forensics, forensic duplication is essential because it enables investigators to work with a copy of the original data while protecting the integrity of the evidence and the original device. It gives detectives the freedom to analyse the replica without tampering with or harming the original data. This minimises the chance of undermining the original data's evidentiary value and ensures that any investigative operations or analysis may be carried out in a controlled manner.

- A sector-by-sector clone of the original storage device is often made using specialised software during the forensic duplication process. This process ensures that every bit of data, including deleted files and hidden data, is included in the duplicate. The duplicate is typically stored on a separate device or in a secure location to ensure its integrity and chain of custody.

- Once the forensic duplicate has been created, it can be used to perform a variety of forensic tasks, including data

recovery, analysis, and investigation. It can also be used in legal proceedings as evidence. To make sure that the data is not affected or altered in any way when working with forensic duplicates, it is crucial to adhere to established forensic protocols.

5.7.3 Restoring Forensic Duplicate

- Making a bit-by-bit copy or image of a storage device, like a hard disk or memory card, and utilising that copy to restore the original data in a way that is forensically sound and can be used for further analysis constitutes the process of restoring a forensic duplicate. The process of restoring a forensic duplicate involves several steps:

1. **Verification:** Make sure the forensic duplicate is an identical replica of the original storage device by verifying it.

2. **Extraction:** Extract the relevant data from the forensic duplicate, such as files or other data that may be of interest in an investigation.

3. **Analysis:** Analyze the data to determine if there is any evidence of wrongdoing or to identify potential suspects.

4. **Reporting:** Report the findings to the relevant parties, such as law enforcement or a court of law.

- When recovering a forensic copy, it's crucial to follow the right forensic procedures to make sure that the data is not destroyed or altered in any way, which could jeopardise the validity of the investigation. This may involve using specialized software or tools, as well as adhering to specific protocols and guidelines established by the forensic community.

5.7.4 Recovering Previously Deleted Files

- Recovering previously deleted files for forensic analysis of evidence can be a complex and sensitive process that requires specialized tools and expertise. The following are some typical actions that might be taken during the process:

1. **Secure the device:** Before attempting to recover any deleted files, it's important to secure the device or storage media containing the data. A bit-by-bit copy of the storage medium or the creation of a forensic image of the device may be required for this. By doing this, it is made possible for the original data to be saved and analysed in a forensically sound manner.

2. **Use specialized forensic software:** There are many tools available that can help recover deleted files, but forensic investigators often use specialized software that can analyze the storage media at a low level to find and recover data that may not be accessible using traditional file recovery methods. Some common tools used in digital forensics include **EnCase, Forensic Toolkit (FTK), and AccessData.**

3. **Analyze the recovered data:** Once the deleted files have been recovered, forensic investigators will typically analyze the data to determine its relevance to the case at hand. This may involve examining metadata such as timestamps and file properties, looking for signs of tampering or attempts to conceal data, or searching for specific keywords or patterns.

4. **Document the process:** Throughout the recovery and analysis process, it's important to document all steps taken and any findings or observations made. This ensures that the analysis is transparent and defensible if the evidence is used in court.

- It's important to remember that the likelihood of successful file recovery is influenced by a variety of variables, such as how recently the data were deleted, if the storage medium was damaged or overwritten, and the strength of the encryption or other security mechanisms in use. Therefore, we need to work with a qualified digital forensic expert who can advise on the feasibility of recovering deleted files in a given case.

5.7.5 Tools and Techniques to Recover Deleted Data

- Deleted data recovery is a crucial aspect of digital forensics, which involves the process of recovering lost, hidden, or

deleted data from electronic devices. Here are some common tools and techniques used in digital forensics for deleted data recovery:

1. **Data Recovery Software:** A variety of electronic devices, including hard drives, memory cards, USB drives, and other digital storage devices, can have their lost or erased data recovered using data recovery software. Some popular data recovery software includes Recuva, EaseUS, TestDisk, and PhotoRec.

2. **Disk Imaging:** Disk imaging is a technique used to create a complete copy of a storage device, including deleted and hidden data. This image can then be analyzed using data recovery software or other forensic tools. This technique is helpful in preserving the data in a forensically sound manner.

3. **File Carving:** By examining the unprocessed data on the storage media, the file carving technique can be utilised to recover deleted files. File carving software identifies file headers and footers to determine the boundaries of the deleted file and extract the relevant data.

4. **Hex Editor:** A Hex editor is a tool that allows forensic analysts to view and edit binary data on a storage device. This tool is particularly helpful when trying to recover data that has been overwritten or corrupted.

5. **Live Forensics:** Live forensics involves analyzing a system while it is still running to collect volatile data such as network connections, running processes, and open files. This technique is useful when trying to recover data that may have been deleted after a system was shut down.

6. **Write-Blocking:** Write-blocking tools are used to prevent any changes from being made to the storage device while data is being recovered. This technique is essential in ensuring the data is forensically sound and can be used as evidence in legal proceedings.

- Overall, digital forensics experts use a combination of tools and techniques to recover deleted data from electronic

devices. It is essential to use the proper techniques and tools to ensure that the recovered data is forensically sound and can be used in court if necessary.

5.8 REPORTING ON THE FINDINGS

- A key responsibility in digital forensics is to analyze lawfully seized digital device content and present their findings in a report, which may support ongoing investigations. In this process, the device in question is completely examined, its contents are carefully examined, and a technical report is produced. The technical report has a number of uses, including intelligence collection and evaluating the device's potential value as evidence. A thorough examination of the device will reveal important insights that can be used to gather intelligence and assess the device's value and significance as potential evidence in the inquiry.

- This preliminary report may potentially pave the way for the hiring of additional, thorough forensic investigators. Therefore, the ability to write a technical report should be regarded as a necessary skill for all practitioners of digital forensics. Hence, a forensic report is an essential element in a digital forensics case, as it provides an objective and detailed account of the analysis and findings of the digital evidence. This report serves as a primary means of communication between the digital forensics practitioner and the stakeholders involved in the case, such as law enforcement, legal professionals, or corporate security personnel.

- The forensic report is also critical because it presents the evidence in a clear and understandable way, which enables stakeholders to make informed decisions about the case. The report provides an accurate account of the digital evidence examined, the methods used, the conclusions reached, and the potential implications of the findings. This information is crucial for supporting legal proceedings, identifying leads for further investigation, or informing a course of action.

- A well-written forensic report is also essential for establishing the credibility of the digital forensics

practitioner and the evidence presented. It can demonstrate that the analysis was conducted in an objective and systematic way, following accepted digital forensics best practices and industry standards. In general, the outcome of a case depends heavily on the forensic report, which is an essential part of the digital forensics process.

5.8.1 Goals of A Forensic Report

- The goals of a forensic report are to present an accurate and impartial assessment of evidence and to help investigators, attorneys, and other interested parties to understand the facts of a case. A well-written forensic report must be based on an in-depth and objective study of the evidence that is available and should concisely state the forensic expert's findings, conclusions, and views.

- The specific goals of a forensic report may vary depending on the nature of the case and the intended audience, but some common objectives include:

1. **Providing an objective analysis of the evidence:** A forensic report should present an unbiased assessment of the evidence and provide a clear and concise explanation of the findings.

2. **Supporting legal proceedings:** The writing of forensic reports should be appropriate for the legal viewers, which includes judges, jurors, and lawyers, as they are frequently utilised in court proceedings.

3. **Assisting in investigations:** Forensic reports can be helpful in guiding further investigations, particularly when new information arises.

4. **Providing expert testimony:** Forensic experts may be called upon to provide testimony in court, and the forensic report can serve as a foundation for this testimony.

5. **Enhancing understanding:** A well-written forensic report can help investigators, attorneys, and other parties to better understand the case and the evidence.

- A forensic report's main goal is to present an accurate and unbiased examination of the available evidence. This report has a number of uses, including aiding in court cases and helping interested parties understand the specifics of a case's facts. The forensic report is essential in allowing informed decision-making and guaranteeing a fair and just resolution of the issue at hand by providing an objective and accurate analysis of the facts.

5.8.2 Guidelines for Forensic Report

- In order to ensure that a forensic report is accurate, understandable, and comprehensive, it is crucial to adhere to a few rules when creating one. The following general recommendations for producing a forensic report:

1. **Follow a clear and consistent structure:** Your report should have a clear and consistent structure, with a clear introduction, body, and conclusion. Use headings and subheadings to organize your report and make it easy to navigate.

2. **Be objective and unbiased:** Your report should be objective and unbiased, presenting the facts and evidence in a clear and neutral manner. Avoid making assumptions or drawing conclusions that are not supported by the evidence.

3. **Use clear and concise language:** Avoid using technical jargon or other terms that can be challenging for non-specialists to understand by using plain, simple language. For a clear and simple presentation of information, use tables, graphs, and bullet points.

4. **Use appropriate formatting:** Use appropriate formatting to make your report easy to read and navigate. Use a readable font size and style, and use appropriate spacing, margins, and indentation.

5. **Document your sources:** Document all sources of information and evidence used in your report, including the methodology used to gather the evidence. This will allow others to replicate your findings and validate your conclusions.

6. **Use proper grammar, punctuation, and spelling:** Use proper grammar, punctuation, and spelling to ensure that your report is professional and easy to read. Proofread your report carefully to ensure that it is free of errors.

7. **Include a conclusion:** Your report should include a clear and concise conclusion that summarizes your findings and any recommendations or conclusions that can be drawn from the evidence.

- Overall, a forensic report should be clear, objective, and complete, and should follow established guidelines for report writing in order to ensure that it is accurate and admissible in court.

5.8.3 Template for Digital Forensic Report

- Here is a basic template for a digital forensic report:

1. Executive Summary :-

a. A brief overview of the investigation and the findings.
b. A summary of the key issues or findings.
c. Recommendations for further actions, if necessary.

2. Introduction:-

a. A statement of purpose outlining the scope of the investigation.
b. Identification of the parties involved in the investigation.
c. A description of the forensic tools and techniques used in the investigation

3. Background Information:-

a. A description of the digital evidence collected.
b. A summary of the system and network configurations.
c. A timeline of relevant events leading up to the investigation

4. Findings:-

a. A detailed description of the digital evidence collected.
b. Analysis of the evidence collected, including relevant metadata.
c. Identification of any gaps or inconsistencies in the evidence.
d. Conclusions drawn from the analysis of the evidence.

5. Supporting Details :-

a. In the Supporting Details section, important findings are in-depthly analysed. This section explains **"How we found conclusions outlined in Relevant Findings?".**
b. It includes a list of important files with their full paths, the outcomes of string searches, the number of files reviewed, the number of emails/URLs reviewed, and any other pertinent information.
c. In this section, we place a greater emphasis on technical depth. Since it conveys much more than written texts, it also includes charts, tables, and illustrations. Numerous subsections are also included to achieve the goals outlined.

6. Investigative Leads

a. Investigative Leads carry out tasks that can aid in learning more details about the matter being investigated.
b. If there is still time, the investigators complete all duties that are still unfinished in order to gather further data.
c. For law enforcement, the Investigative Lead section is absolutely essential.
d. This section offers additional tasks for gathering the data required to advance the case. For instance, determining whether any firewall logs date back far enough in time to accurately depict any attacks that may have occurred.

7. Additional Subsections :

a. Depending on the demands and particular needs of the client, a forensic report may have extra subsections. In specific cases, the following subsections can offer insightful information:

i. Attacker Methodology: This section provides a summary of the techniques the attacker used, assisting readers in comprehending the nature and particulars of the attacks. In circumstances involving computer infiltration, it is very important.
ii. User Applications –The details in this part centres on the pertinent applications that were installed on the examined media. It can be useful to understand the programmes that are already installed on the system because they might be relevant to the case.
iii. Internet Activity – The Internet Activity or Web Browsing History part offers the user's web browsing history connected to the material that has been analysed. This data

can provide insight into user intentions, the downloading of potentially harmful tools, online searches, and the use of programmes intended to remove evidence or perform secure deletion.

8. Conclusion:-

a. A summary of the key findings.
b. Recommendations for further actions, if necessary.

9. Appendix

a. Detailed technical information, if relevant.
b. Copies of relevant documents, if necessary.
c. Supporting evidence, if appropriate

- It's important to note that the exact content and format of a digital forensic report may vary depending on the specific case and the requirements of the audience. It is recommended to consult with legal counsel and follow any applicable guidelines or standards in creating a digital forensic report.

5.9 TESTIMONY

- Preparing for testimony as a forensic expert requires careful consideration of the facts of the case and the requirements of the legal system. Here are some steps you can take to prepare for testimony as a forensic expert:

1. **Review the case materials:** Start by going over all the case-related materials, such as witness testimonies, police records, forensic reports, and any other pertinent documents. Make sure you are familiar with the case's facts and the disputed points.

2. **Conduct a thorough analysis:** Conduct a thorough analysis of the evidence in the case, using your expertise to evaluate the strengths and weaknesses of each piece of evidence. Make sure you can explain your analysis in a clear and concise manner.

3. **Identify potential challenges to your analysis:** Anticipate any challenges to your analysis that may arise during cross-examination. Think about the different ways that the

opposing side may try to discredit your analysis and be prepared to respond.

4. **Practice your testimony:** Practice your testimony so that you are comfortable and confident when you are on the stand. Work with a colleague or mentor to go through potential questions and answers, and refine your presentation to make it as clear and persuasive as possible.

5. **Be objective and impartial:** As a forensic expert, it is important that you remain objective and impartial in your analysis and testimony. Stick to the facts and avoid making assumptions or speculations that are not supported by the evidence.

6. **Understand the legal standards:** Make sure you understand the legal standards that apply to the case, including the burden of proof and the elements of any relevant crimes or causes of action. Be prepared to explain how your analysis supports or undermines the legal standards at issue.

7. **Be respectful and professional:** Finally, be respectful and professional throughout the process. Remember that you are there to assist the court in reaching a just and fair resolution, and that your role as a forensic expert is critical to that process.

5.9.1 Consulting Expert or Expert Witness

- A consulting expert or expert witness in digital forensics is typically someone who has specialized knowledge and expertise in the collection, preservation, analysis, and presentation of digital evidence in legal proceedings. They may be called upon to provide expert testimony in court, or to provide consultation services to attorneys, law enforcement agencies, or other organizations.

- Before giving testimony, expert witnesses are questioned about their knowledge and skills. Expert witnesses are different from traditional witnesses because experts can offer opinions about matters in their fields. For example, a

digital forensics expert can offer opinions on computers and digital evidence.

- It may be necessary to ask expert witnesses to clarify complex issues for non-expert members. A digital forensics specialist might be asked, for instance, to explain digital concepts to persons who aren't professionals in the field.

- Expert witnesses have many requirements, but perhaps the most important quality is honesty. Expert witnesses must provide honest testimony, even if it contradicts the argument of those who are paying the witnesses' fees. Expert witnesses must also inform the court if they believe they are not qualified to provide an expert analysis of a particular question before the court.

- Depending on the details of the case and the requirements of the client, a consulting expert's or expert witness's involvement in digital forensics may change. Some of the tasks that they may be asked to perform include:

1. Conducting forensic analysis of digital devices or data.
2. Examining and interpreting digital evidence.
3. Preparing written reports and presenting findings in court.
4. Providing technical expertise and advice to legal teams.
5. Educating attorneys, judges, and juries on the technical aspects of digital forensics.

- Consulting experts and expert witnesses in digital forensics must possess a deep understanding of computer systems, networks, and software, as well as knowledge of the legal and regulatory requirements related to digital evidence. They must also be able to communicate complex technical information to non-technical audiences in a clear and understandable way.

- The basis for the expert witness report and testimony is a computer forensic expert examination and assessment. In today's complex world of data breaches and charges of inadequate cybersecurity, the expert's job is even more crucial. To mitigate the disastrous effects of a data leak,

businesses of all sizes must integrate cybersecurity into their core operations.

- Lack of comprehensive incident or data breach response strategies can cause significant financial loss and reputational harm.

- In broad terms, a consulting expert's or expert witness's job in digital forensics is to support and advise legal teams and other groups participating in court cases involving digital evidence.

5.9.2 Preparing to Deal With News Media as Expert Witness

- You might be required to speak with the media as a witness in a digital forensics case. This can be an opportunity to raise awareness about the importance of digital forensics and your role in the legal process. However, it is essential to prepare yourself and your messaging to ensure that your interactions with the media are effective and do not compromise the case.

- Here are some tips for preparing to deal with the news media as an expert witness:

  - **Understand the case and your role:** Before engaging with the media, it is critical to have a clear understanding of the case and your role as an expert witness. This will help you to provide accurate and relevant information to the media and avoid making statements that could harm the case.

  - **Prepare your messaging:** Develop key messages that you want to convey to the media. Keep your messaging clear, concise, and relevant to the case. Avoid using jargon and technical language that may confuse or alienate your audience.

  - **Anticipate questions:** Try to anticipate the questions that the media may ask and prepare responses in advance. Practice delivering your responses with confidence and clarity.

- **Stick to the facts:** Stick to the facts and avoid speculating or making predictions. If you are not sure about something, it is better to admit that you don't know rather than providing incorrect or misleading information.

- **Be aware of legal restrictions:** Be aware of any legal restrictions that may limit what you can say to the media. It is important to respect the legal process and not say anything that could prejudice the case.

- **Remain calm and composed**: Dealing with the media can be stressful, but it is essential to remain calm and composed. Speak clearly, maintain eye contact, and avoid appearing defensive or argumentative.

- By paying attention to these pointers, you may get ready to interact with the media as a qualified witness in a digital forensics case.

5.10 SUMMARY

- In order to ensure that digital evidence is admissible in judicial proceedings, digital forensics investigations necessitate a well-organized and systematic approach to evidence presentation.

- Digital forensics investigations should present evidence in accordance with accepted best practises, which include accurate documenting of all actions taken, the preservation of original evidence, and the fabrication of forensic copies for analysis.

- Maintaining the integrity of the evidence and making sure it stays clean throughout the inquiry are crucial.

- Digital forensics practitioners must be mindful of legal aspects that may impact their investigations, including privacy laws, data protection laws, and laws that govern the admissibility of digital evidence in court.

- Practitioners should be familiar with relevant legislation and case law in their jurisdiction to ensure that their

investigations and evidence presentation comply with legal requirements.

- To present digital evidence in a legal setting, it is essential to prepare a well-written forensic report that provides an objective and detailed account of the analysis and findings. The report should follow established guidelines, which include a clear description of the evidence examined, the methods used, the conclusions reached, and the potential implications of the findings.

- In general, the presenting of evidence in digital forensics investigations calls for meticulous planning, adherence to best practises, and a complete comprehension of the legal considerations that influence the admissibility of digital evidence in legal proceedings.

5.11 REFERENCES

1. Guide to computer forensics and investigations, Bill Nelson, Amelia Philips and Christopher Steuart, course technology,5th Edition,2015.
2. Incident Response and computer forensics, Kevin Mandia, Chris Prosise, Tata McGrawHill,2nd Edition,2003.
3. https://www.magnetforensics.com/resources/reporting-findings-at-a-technical-level-in-digital-forensics-a-guide-to-reporting/
4. https://www.eccouncil.org/what-is-digital-forensics/
5. https://www.bluevoyant.com/knowledge-center/understanding-digital-forensics-process-techniques-and-tools
6. https://www.guru99.com/digital-forensics.html
7. https://flylib.com/
8. https://enigmaforensics.com/
9. https://info-savvy.com/
10. https://es.slideshare.net/
11. https://www.eccouncil.org/
12. https://mu.ac.in/
13. https://www.igi-global.com/
14. "Advances in Digital Forensics II" Springer Science and Business Media LLC, 2006
15. AAlvine Boaye Belle, Yixi Zhao. "Evidence-Based Software Engineering: A Checklist-Based Approach to

Assess the Abstracts of Reviews Self-Identifying as Systematic Reviews
16. https://www.coursehero.com/
17. https://accsaglobal.org/

5.12 UNIT END EXERCISE

1. Do a case study on qualified forensic duplicate.
2. Do a self study by creating a forensic duplicate and a qualified forensic duplicate of a hard drive.
3. Try to recover deleted file on windows

5.13 QUESTIONS

1. Write a short note on Evidence
2. Write a short note on Authorization to collect evidence
3. Explain meaning of authentication of evidence
4. What are the steps for forensic analysis?
5. What are the goals of a report?
6. Explain template for forensic report?
7. Explain how to prepare a testimony

❖❖❖❖

6

INTRODUCTION TO LEGAL ASPECTS OF DIGITAL FORENSICS

Unit Structure

6.0 OBJECTIVES

- Understanding the legal and regulatory frameworks governing digital forensics and the admissibility of digital evidence in court.
- Understanding the legal requirements for the collection, preservation, and analysis of digital evidence.
- Understanding the legal and ethical considerations associated with digital forensics, such as privacy, data protection, and chain of custody.
- Developing an understanding of how digital evidence is presented in court and the legal requirements for its admissibility.
- Understanding the role of digital forensic experts in legal proceedings and their ethical obligations to the court.

6.1 INTRODUCTION

- The legal aspects of digital forensics is to understand the legal and regulatory frameworks governing the collection, analysis, and presentation of digital evidence in a court of law. Digital forensics involves the extraction, preservation, and analysis of digital evidence for use in legal proceedings. However, the use of digital evidence in court is subject to legal scrutiny and regulations, and digital forensic experts must comply with these regulations to ensure that the evidence is admissible in court.
- The legal aspects of digital forensics cover various areas, including search and seizure, privacy, data protection, chain of custody, and admissibility of evidence. Digital forensic experts must understand

these legal aspects to conduct investigations and provide evidence that is acceptable in a court of law. Understanding the legal requirements for digital forensics is essential for ensuring that the evidence is admissible and the investigation is conducted within the legal framework.

- The legal aspects of digital forensics are important for investigating and presenting digital evidence in a court of law. In India, the legal framework for digital forensics is primarily governed by the Information Technology Act, 2000 (IT Act).

- The IT Act provides legal recognition for electronic documents and digital signatures and defines cyber crimes and penalties for such offenses. It also outlines the procedures for the collection, preservation, and analysis of digital evidence in a court of law.

- Under the IT Act, digital forensic evidence is admissible in court if it is collected in accordance with the prescribed legal procedures. The Act also specifies the qualifications and responsibilities of digital forensic experts, who must be certified and qualified to carry out forensic investigations.

- The IT Act also addresses privacy concerns related to the collection and use of digital evidence. It mandates that digital evidence must be collected and analyzed in a manner that preserves the privacy of the individuals involved. It also includes provisions for the protection of personal data and the confidentiality of sensitive information.

- Moreover, the IT Act also empowers law enforcement agencies and courts to issue orders for the production of electronic records and digital evidence. Failure to comply with such orders may lead to penalties, including imprisonment or fines.

6.2 LAWS AND REGULATIONS

- Laws and regulations are rules or guidelines that are established by a government, organization, or authority to ensure compliance with certain standards, promote safety, maintain order, protect individual rights, and prevent harm to individuals or society as a whole.

- Laws are typically created and enforced by governments at the national, state or local level. They are legally binding and carry the force of the state behind them. Laws are enforced through the legal system, which can involve courts, police, and other government agencies.

- Regulations, on the other hand, are rules established by organizations or authorities to govern specific areas or industries. For example, regulatory bodies like INTERPOL which is an international organization that facilitates cooperation among law enforcement

agencies from different countries to combat cybercrime. It provides a platform for exchanging information and intelligence to help identify, locate, and apprehend cyber criminals. Regulations are typically enforced by the organizations or authorities that established them and may also involve government agencies in some cases.

- Laws and regulations are critical in ensuring the safety and well-being of individuals and society as a whole by providing clear guidelines for behavior and consequences for non-compliance.

- Cybercrime is a global problem that affects individuals, businesses, and governments. Various countries have enacted laws and regulations to combat cybercrime and regulate digital forensics. Here are some examples of laws and regulations for cybercrime and digital forensics from different countries:

  - **The United States:** The United States has several laws and regulations that govern cybercrime and digital forensics. These include the Computer Fraud and Abuse Act, the Electronic Communications Privacy Act, the Cybersecurity Information Sharing Act, and the Federal Rules of Evidence. These laws regulate cybercrime and the collection, preservation, and analysis of digital evidence.

  - **The United Kingdom:** The United Kingdom has the Computer Misuse Act, which criminalizes unauthorized access to computer systems and the modification of data. The UK also has the Police and Criminal Evidence Act, which governs the collection and admissibility of digital evidence in court.

  - **India:** As mentioned earlier, the Information Technology Act, 2000 (IT Act) governs cybercrime and digital forensics in India. The Act defines cybercrime and prescribes penalties for such offenses. It also outlines the procedures for the collection, preservation, and analysis of digital evidence in a court of law.

  - **European Union:** The European Union has the General Data Protection Regulation (GDPR), which regulates the collection and processing of personal data by organizations. The EU also has the Network and Information Systems (NIS) Directive, which requires organizations to report security incidents and cyber attacks to competent authorities.

  - **Australia:** Australia has the Cybercrime Act, which criminalizes cybercrime, including hacking, identity theft, and online fraud. The country also has the Telecommunications (Interception and Access) Act, which regulates the interception of electronic communications for law enforcement purposes.

- These are just a few examples of the laws and regulations for cybercrime and digital forensics in different countries. The legal

framework for cybercrime and digital forensics varies from country to country, but they all aim to prevent cybercrime, protect personal data, and ensure the admissibility of digital evidence in court.

6.2.1 LAWS AND REGULATION INDIA

- India's legal framework for cybercrime and digital forensics aims to prevent cybercrime, protect personal data, and ensure the admissibility of digital evidence in court. The government and law enforcement agencies are continuously updating their policies and regulations to keep pace with the evolving landscape of cyber threats.

- India has a complex legal system that includes civil, criminal, and regulatory laws. Here's a brief overview of each:

  - **Civil law:** Civil law in India governs private disputes between individuals, organizations, or entities. The Indian civil law is mainly based on the Indian Contract Act, 1872, the Specific Relief Act, 1963, the Transfer of Property Act, 1882, and the Hindu Marriage Act, 1955, among others. The Indian civil law covers matters such as property disputes, divorce and marriage laws, contracts, torts, inheritance, and more.

  - **Criminal law:** Criminal law in India deals with the prosecution of individuals or entities that commit crimes. The Indian Penal Code, 1860, is the primary statute that governs criminal law in India. It outlines the crimes and their respective punishments, such as theft, murder, rape, assault, and other offenses.

  - **Regulatory law:** Regulatory law in India governs specific industries and sectors to ensure that they follow the necessary regulations, standards, and guidelines. The regulatory authorities ensure that businesses and organizations comply with rules and guidelines in their respective industries. For instance, the Securities and Exchange Board of India (SEBI) regulates the securities market, while the Telecom Regulatory Authority of India (TRAI) oversees the telecommunications sector.

- Additionally, India has various specialized laws that cover specific areas such as labor law, intellectual property law, environmental law, and taxation. These laws aim to ensure that businesses and individuals follow the necessary regulations, policies, and guidelines for their respective industries.

- The Indian legal system is constantly evolving and changing. The judiciary, government, and regulatory authorities are always updating and amending these laws to keep up with the changing social, economic, and technological landscape in India.

6.2.2 IMPORTANT CODE

1. **The Indian Penal Code (IPC):** The IPC is a criminal code that covers various offenses such as murder, theft, fraud, and sexual offenses. It also includes provisions for criminal acts such as cybercrime, forgery, and defamation.

2. **The Code of Criminal Procedure (CrPC):** The CrPC is a procedural law that provides guidelines for the conduct of criminal proceedings in India. It covers various aspects such as the arrest of suspects, the search of premises, and the admissibility of evidence in court.

3. **The Civil Procedure Code (CPC):** The CPC is a procedural law that governs civil cases such as property disputes, contract disputes, and family law matters. It provides guidelines for filing cases, evidence collection, and the conduct of trials in civil cases.

6.2.3 IMPORTANTS OF LAWS AND REGULATIONS

- Digital forensics is the process of collecting, analyzing, and preserving digital evidence to investigate and prevent cybercrime. The importance of laws and regulations in digital forensics cannot be overstated. Here are some reasons why laws and regulations are essential in digital forensics:

  - **Legal Admissibility:** In digital forensics, it is important that the evidence collected is legally admissible in court. Laws and regulations provide guidelines for the collection, preservation, and analysis of digital evidence to ensure that it is legally valid and admissible in court.

  - **Protecting Digital Evidence:** Laws and regulations provide a framework for protecting digital evidence from tampering, destruction, or unauthorized access. They ensure that digital evidence is collected and stored in a manner that preserves its integrity and authenticity.

  - **Standardization:** Laws and regulations provide a standardized approach to digital forensics. They ensure that digital evidence is collected, preserved, and analyzed in a consistent and repeatable manner. This is important because it ensures that evidence is reliable, and the investigation can be repeated if necessary.

  - **Privacy and Security:** Laws and regulations provide guidelines for protecting the privacy and security of digital evidence. They ensure that digital evidence is collected and analyzed in a manner that respects the privacy rights of individuals and protects sensitive data from unauthorized access.

  - **Deterrence:** Laws and regulations play a crucial role in deterring cybercrime. They provide clear and severe penalties for cybercrime,

which acts as a deterrent to potential offenders. This helps to prevent cybercrime and protect individuals and organizations from harm.

- Laws and regulations are essential in digital forensics to ensure that evidence is legally admissible, protected from tampering, collected in a standardized manner, and analyzed in a way that respects privacy and security. They also play a crucial role in deterring cybercrime and protecting individuals and organizations from harm.

6.2.4 REGULATORY BODIES FOR CYBER CRIME

- There are several regulatory bodies that are involved in combating cybercrime at the international, national, and regional levels. Some of these bodies include:

- **International Criminal Police Organization (INTERPOL):** INTERPOL is an international organization that facilitates cooperation among law enforcement agencies from different countries to combat cybercrime. It provides a platform for exchanging information and intelligence to help identify, locate, and apprehend cyber criminals.

- **United States Department of Justice (DOJ):** The DOJ is the primary law enforcement agency in the United States and has a dedicated Cybercrime Unit that investigates and prosecutes cybercriminals operating within the US and abroad. The DOJ also works closely with other international law enforcement agencies to combat cybercrime.
  \
- **European Union Agency for Cybersecurity (ENISA):** ENISA is an agency of the European Union that provides expertise and support to EU member states in the area of cybersecurity. It assists in the development of cybersecurity policies, regulations, and standards across the European Union.

- **Federal Bureau of Investigation (FBI):** The FBI is the principal investigative arm of the US Department of Justice and is responsible for investigating cybercrimes that fall under federal jurisdiction, including those that involve national security and critical infrastructure.

- **Computer Emergency Response Team (CERT):** CERTs are organizations that specialize in cybersecurity incident response, providing services such as vulnerability assessments, incident management, and threat intelligence. They operate in many countries and often work closely with law enforcement agencies to combat cybercrime.

- These are just a few examples of regulatory bodies that are involved in combating cybercrime. There are many other organizations, both public and private, that play a role in fighting cybercrime and ensuring cybersecurity.

6.2.5 REGULATORY BODIES FOR CYBER CRIME INDIA

- In India, there are several regulatory bodies that play a key role in combating cybercrime and ensuring cybersecurity. Some of these bodies include:

  - **National Cyber Security Coordinator:** The National Cyber Security Coordinator (NCSC) is responsible for implementing India's cybersecurity strategy and coordinating cybersecurity efforts across government agencies, industry, and academia. The NCSC is also responsible for setting up and managing the National Cyber Coordination Centre (NCCC), which serves as a hub for monitoring and responding to cybersecurity threats in India.

  - **National Technical Research Organisation:** The National Technical Research Organisation (NTRO) is a technical intelligence agency that is responsible for collecting and analyzing electronic intelligence in India. The NTRO plays a key role in detecting and responding to cyber threats that pose a threat to national security.

  - **Computer Emergency Response Team:** The Indian Computer Emergency Response Team (CERT-In) is the national agency responsible for responding to cybersecurity incidents and managing vulnerabilities in the country's cyberspace. CERT-In works closely with other government agencies, industry partners, and international organizations to prevent and mitigate cyber attacks.

  - **Reserve Bank of India:** The Reserve Bank of India (RBI) is responsible for regulating the banking and financial sector in India, including ensuring the security and integrity of digital payments and financial transactions. The RBI has set up various regulations and guidelines to ensure cybersecurity in the financial sector and prevent cyber fraud.

  - **Ministry of Electronics and Information Technology:** The Ministry of Electronics and Information Technology (MeitY) is responsible for formulating policies and programs for the development of the electronics and IT industry in India. MeitY has launched various initiatives to promote cybersecurity and develop a secure and resilient cyberspace in the country.

- These are some of the key regulatory bodies in India that are involved in combating cybercrime and ensuring cybersecurity. Other regulatory bodies and law enforcement agencies, such as the Cyber Crime Investigation Cell (CCIC) and the Central Bureau of Investigation (CBI), also play important roles in addressing cybercrime in India.

6.2.6 LEVELS OF LAW

- In India, the legal system consists of multiple levels, including the following:

  - **Local Law:** Local laws refer to laws made by local or municipal bodies that govern specific regions or areas within a state. For example, laws made by municipal corporations, panchayats, or town councils.

  - **State Law:** Each state in India has its own set of laws and regulations that govern activities within the state. State laws cover areas such as education, agriculture, public health, and policing, among others.

  - **Federal Law:** Federal laws are enacted by the central government of India and are applicable throughout the country. These laws include the Indian Constitution, the Indian Penal Code, and the Code of Criminal Procedure, among others.

  - **International Law:** International law refers to laws and agreements between different countries or international organizations. India is a signatory to various international conventions and treaties, including the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, among others. International law can also have an impact on Indian domestic laws, particularly when it comes to issues such as extradition, international trade, and human rights.

6.2.7 LEVELS OF CULPABILITY

- Culpability refers to the degree of responsibility or blameworthiness a person holds for a particular action or omission. The levels of culpability can be categorized into different degrees based on the nature and severity of the action or omission. In general, there are four levels of culpability recognized by law:

  - **Intentional:** Intentional culpability is the highest degree of culpability and involves an individual knowingly and deliberately committing a wrongful act. It is also called "willful" or "knowing" culpability. For example, intentionally committing murder or theft.

  - **Reckless:** Reckless culpability refers to when an individual is aware that their actions or omissions create a substantial and unjustifiable risk, but they go ahead and take the risk anyway. It is also called "heedless" or "conscious disregard" culpability. For example, driving a car at a very high speed on a crowded street, knowing that it might cause an accident.

  - **Negligent:** Negligent culpability involves a person's failure to exercise reasonable care and caution, which results in harm to others. Negligent culpability may arise from an omission or failure to act, or from an act

that falls below the standard of care expected of a reasonable person. For example, a doctor failing to provide appropriate medical care to a patient, resulting in harm or death.

- **Strict liability:** Strict liability culpability is the lowest degree of culpability and holds an individual liable for a harmful act or omission, even if they did not have any intent to cause harm, nor were they negligent or reckless in their actions. For example, a company being held strictly liable for producing and selling a defective product that causes harm to consumers.

- The different degrees of culpability have different legal consequences, and the severity of the punishment increases with the level of culpability.

6.2.7 LEVEL AND BURDEN OF PROOF CIVIL VERSUS CRIMINAL CASES

- In both civil and criminal cases, there are different levels and burdens of proof that must be met to reach a verdict. However, the levels and burdens of proof in civil cases and criminal cases differ.

- **Civil Cases:** In civil cases, the burden of proof is generally "preponderance of the evidence," which means that the plaintiff must prove that it is more likely than not that the defendant committed the wrongdoing. This is a lower standard than in criminal cases. The plaintiff is the one who has the burden of proof, and they must present evidence and convince the court that their version of the events is more likely true than not.

- **Criminal Cases**: In criminal cases, the burden of proof is much higher, and the standard is "beyond a reasonable doubt." The prosecution has the burden of proving the defendant's guilt beyond a reasonable doubt, which is a much higher standard than in civil cases. Beyond a reasonable doubt means that the evidence presented is so strong and convincing that there can be no other reasonable explanation for the defendant's actions. This is to ensure that an innocent person is not convicted of a crime.

- **Level of Proof:** The level of proof in civil cases is lower than in criminal cases. In civil cases, the plaintiff must prove their case by a preponderance of the evidence, whereas, in criminal cases, the prosecution must prove their case beyond a reasonable doubt. This difference in the level of proof is because the consequences of a criminal conviction can be severe, including imprisonment, fines, and loss of civil rights, whereas, in civil cases, the consequences are generally limited to compensation or damages.

- To conclude, the level and burden of proof in civil cases and criminal cases differ significantly. The burden of proof in civil cases is

generally "preponderance of the evidence," while in criminal cases, the burden of proof is "beyond a reasonable doubt." The level of proof in civil cases is lower than in criminal cases, as the consequences of a criminal conviction are severe.

6.3 INFORMATION TECHNOLOGY ACT

- The Information Technology Act, 2000 also Known as an IT Act is an act proposed by the Indian Parliament reported on **17th October 2000,** to provide legal recognition for electronic commerce and electronic transactions in India. This Information Technology Act is based on the United Nations Model law on Electronic Commerce 1996 **(UNCITRAL Model)** which was suggested by the General Assembly of United Nations by a resolution dated on 30th January, 1997.

- The Act was amended in 2008 to align it with the United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce.

- The IT Act 2000 contains provisions for various cyber crimes such as unauthorized access to computer systems, hacking, spreading of viruses, cyber terrorism, cyber stalking, identity theft, and phishing. The Act also provides for the establishment of the Cyber Appellate Tribunal to deal with appeals against any order passed by an adjudicating officer under the Act.

- The IT Act 2000 also contains provisions related to digital signatures and electronic documents, making them legally admissible in courts. It also provides for the establishment of the Controller of Certifying Authorities (CCA) to regulate the issuance of digital signatures.

- The Act also deals with issues related to online content, providing for the removal of objectionable material from the internet and imposing penalties for the publication of sexually explicit material. However, these provisions have been subject to criticism for their potential impact on freedom of speech and expression.

- Overall, the IT Act 2000 is an important law that aims to provide a legal framework for electronic transactions and cyber security in India. It has been amended over the years to keep up with the changing technology landscape and address emerging cyber threats.

- The main objective of this act is to carry lawful and trustworthy electronic, digital and online transactions and alleviate or reduce cybercrimes. The IT Act has 13 chapters and 90 sections. The last four sections that starts from ‘section 91 – section 94’, deals with the revisions to the Indian Penal Code 1860.

- The IT Act, 2000 has two schedules:
  - First Schedule – Deals with documents to which the Act shall not apply.
  - Second Schedule – Deals with electronic signature or electronic authentication method.

6.3.1 FEATURES OF IT ACT 2000

- The Information Technology (IT) Act 2000 is an Indian law that provides a legal framework for electronic transactions and cyber security in India. Some of the key features of the IT Act 2000 are:
  - **Legal recognition of electronic transactions:** The Act provides legal recognition for electronic contracts, digital signatures, and other electronic transactions.
  - **Electronic authentication:** The Act allows the use of digital signatures and electronic authentication methods to verify the authenticity of electronic documents and transactions.
  - **Cyber offences and punishments:** The Act provides for the punishment of several cyber offences, including hacking, spreading of computer viruses, unauthorized access to computer systems, cyber terrorism, and identity theft.
  - **Establishment of Controller of Certifying Authorities (CCA):** The Act provides for the establishment of the CCA, which is responsible for regulating the issuance of digital signatures in India.
  - **Establishment of Cyber Appellate Tribunal:** The Act provides for the establishment of the Cyber Appellate Tribunal, which is responsible for hearing appeals against orders passed by the Controller of Certifying Authorities and Adjudicating Officers.
  - **Adjudicating Officers:** The Act provides for the appointment of Adjudicating Officers to adjudicate any contravention of the Act.
  - **Penalties:** The Act provides for the imposition of fines and imprisonment for contraventions of the Act, with fines ranging from Rs. 1 lakh to Rs. 10 lakhs and imprisonment ranging from six months to three years.
- Overall, the IT Act 2000 is an important law that aims to provide a legal framework for electronic transactions and cyber security in India. It has been amended over the years to keep up with the changing technology landscape and address emerging cyber threats.

6.3.2 SOME OFFENCES AND PUNISHMENTS UNDER IT ACT

- The Information Technology (IT) Act 2000, as amended in 2008, contains provisions for various cyber crimes and their corresponding punishments. Some of the offences and punishments under the Act are:

  - **Tampering with computer source documents:** Any person who knowingly or intentionally conceals, destroys or alters any computer source code or any other computer data, with the intention of causing damage or harm to another person, can be punished with imprisonment of up to three years, or a fine of up to two lakh rupees, or both.

  - **Hacking:** Any person who gains unauthorized access to a computer system, computer network or computer resource, can be punished with imprisonment of up to three years, or a fine of up to two lakh rupees, or both.

  - **Publishing or transmitting obscene material in electronic form:** Any person who publishes or transmits any material containing sexually explicit act or conduct in electronic form can be punished with imprisonment of up to five years, or a fine of up to ten lakh rupees, or both.

  - **Identity theft:** Any person who impersonates someone else by using their identity information, with the intention of causing damage or harm to that person, can be punished with imprisonment of up to three years, or a fine of up to one lakh rupees, or both.

  - **Cyber terrorism:** Any person who commits any act of cyber terrorism, which includes accessing or attempting to access a computer resource with the intention of threatening the unity, integrity, security or sovereignty of India, can be punished with imprisonment for life.

  - **Publishing false digital signature certificates:** Any person who publishes a false digital signature certificate can be punished with imprisonment of up to two years, or a fine of up to one lakh rupees, or both.

- These are just some of the offences and corresponding punishments under the IT Act 2000. The Act also provides for the appointment of an adjudicating officer to adjudicate any contravention of the Act, and the establishment of the Cyber Appellate Tribunal to hear appeals against the orders of the adjudicating officer.

- Sections and Punishments under Information Technology Act, 2000 are as follows :

SECTION	PUNISHMENT
Section 43	This section of IT Act, 2000 states that any act of destroying, altering or stealing computer system/network or deleting data with malicious intentions without authorization from owner of the computer is liable for the payment to be made to owner as compensation for damages.
Section 43A	This section of IT Act, 2000 states that any corporate body dealing with sensitive information that fails to implement reasonable security practices causing loss of other person will also liable as convict for compensation to the affected party.
Section 66	Hacking of a Computer System with malicious intentions like fraud will be punished with 3 years imprisonment or the fine of Rs.5,00,000 or both.
Section 66 B, C, D	Fraud or dishonesty using or transmitting information or identity theft is punishable with 3 years imprisonment or Rs. 1,00,000 fine or both.
Section 66 E	This Section is for Violation of privacy by transmitting image or private area is punishable with 3 years imprisonment or 2,00,000 fine or both.
Section 66 F	This Section is on Cyber Terrorism affecting unity, integrity, security, sovereignty of India through digital medium is liable for life imprisonment.
Section 67	This section states publishing obscene information or pornography or transmission of obscene content in public is liable for imprisonment up to 5 years or fine of Rs. 10,00,000 or both.
Section 67A	This section states publishing images containing sexual acts. Imprisonment up to seven years, or/and with fine up to Rs. 1,000,000
Section 67B	Transmitting material depicting children, including nude or sexually explicit pictures of a child. shall be punished on first conviction with imprisonment of

	either description for a term which may extend to five years and with a fine which may extend to Rupees ten lakh and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to Rupees ten lakh:
Section 67C	This section states failure to maintain records. Imprisonment up to three years, or/and with fine.
Section 68	This section states failure/refusal to comply with orders. Imprisonment up to 2 years, or/and with fine up to Rs. 100,000
Section 69	Failure/refusal to decrypt data. Imprisonment up to seven years and possible fine.
Section 70	Securing access or attempting to secure access to a protected system. Imprisonment up to ten years, or/and with fine.
Section 71	This section states about Misrepresentation. Imprisonment up to 2 years, or/and with fine up to Rs. 100,000
Section 72	This section states about breach of confidentiality and privacy Imprisonment up to 2 years, or/and with fine up to Rs. 100,000
Section 72A	This section states that disclosure of information in breach of lawful contract. Imprisonment up to 3 years, or/and with fine up to Rs. 500,000
Section 73	Publishing electronic signature certificate false in certain particulars. Imprisonment up to 2 years, or/and with fine up to Rs. 100,000
Section 74	Publication for fraudulent purpose. Imprisonment up to 2 years, or/and with fine up to Rs. 100,000

6.3.3 Key Featutres of Amendments it Act 2008

- The Information Technology (IT) Act 2000 was amended in 2008 to address emerging cyber threats and keep up with the changing technology landscape. Some of the key features of the IT Act 2008 amendment are:

  - **Data protection:** The amendment introduced new provisions related to data protection and privacy, which require companies to implement reasonable security practices to protect sensitive personal data. It also provides for the punishment of those who access, download, or extract personal data without the consent of the owner.

  - **Cyber terrorism:** The amendment introduced new provisions to address cyber terrorism, including the use of the internet to threaten the unity, integrity, security or sovereignty of India. The punishment for such offences was increased to imprisonment for life.

  - **E-commerce:** The amendment provides legal recognition to electronic contracts and transactions, including electronic signatures, and facilitates e-commerce by introducing provisions related to electronic payment systems, digital signatures, and certification authorities.

  - **Cyber offences and punishments:** The amendment added new cyber offences, including sending offensive or menacing messages, and providing assistance in committing cyber crimes. It also increased the punishment for several cyber offences, including hacking, tampering with computer source documents, and publishing sexually explicit material online.

  - **Establishment of Cyber Appellate Tribunal:** The amendment provided for the establishment of the Cyber Appellate Tribunal to hear appeals against orders passed by the Controller of Certifying Authorities and Adjudicating Officers.

  - **Removal of objectionable content:** The amendment introduced new provisions related to the removal of objectionable content from the internet, and provides for the punishment of those who fail to comply with such orders.

- Overall, the IT Act 2008 amendment was a significant step towards strengthening the legal framework for electronic transactions and cyber security in India. It provided a much-needed update to the IT Act 2000, which was enacted in a different era of technology and cyber threats.

6.4 GIVING EVIDENCE IN COURT

- Giving evidence in court is crucial due to several reasons. Foremost, it is an important part of the justice system. In order to determine the

truth of a matter and make a fair decision, judges and juries need to hear evidence from witnesses who were present at the relevant events.

- Secondly, giving evidence in court allows individuals to hold others accountable for their actions. By providing testimony, witnesses can help establish the facts of a case and help to ensure that those responsible for any wrongdoing are held accountable.

- Thirdly, giving evidence in court can be an opportunity for individuals to seek justice for themselves or others who have been wronged. For example, a victim of a crime can provide evidence to help ensure that the perpetrator is convicted and punished.

- Finally, giving evidence in court can help to prevent future harm. By providing testimony, witnesses can help to establish facts that can be used to develop new laws or regulations that protect individuals from harm but giving evidence in court can be a daunting task. Here are some points to help you prepare for giving evidence in court:

  - **Understand the case:** Make sure you understand the details of the case and what you will be asked to testify about. Review any documents or other evidence that you have that relate to the case.

  - **Speak with the attorney:** If you are a witness for one of the parties, speak with their attorney before the trial. They can explain what to expect during the trial and help you prepare for your testimony.

  - **Tell the truth:** It is crucial to tell the truth when giving evidence in court. Giving false evidence is a serious offence and can lead to criminal charges.

  - **Be clear and concise:** When giving evidence, speak clearly and concisely, and avoid rambling or going off-topic. Answer only the questions you are asked, and avoid volunteering additional information.

  - **Listen carefully:** Listen carefully to the questions you are asked, and take your time when answering. If you do not understand a question, ask for clarification.

  - **Dress appropriately:** Dress in a professional manner, as you would for a job interview. Avoid wearing anything that could be seen as distracting or offensive.

  - **Be respectful:** Show respect for the court and the judge. Address the judge as "Your Honor" and be polite to everyone in the courtroom.

  - **Practice:** If you are feeling nervous, practice your testimony beforehand. Ask a friend or family member to act as the attorney and ask you questions.

- Remember, giving evidence in court is an important responsibility. By following these tips, you can help ensure that you give an accurate and helpful testimony.

6.4.1 Testifying in Court

- In 2009, the U.S. Supreme Court issued a ruling in the case of Melendez-Diaz v. Massachusetts that granted defendants the right to cross-examine forensic laboratory analysts in criminal cases. Prior to this ruling, analysts could submit reports of forensic findings without appearing in court. However, the Melendez-Diaz decision stated that a laboratory report cannot be used as evidence without live testimony. This means that forensic scientists who perform laboratory testing for the prosecution must now be available for testimony in court under the Confrontation Clause of the Sixth Amendment.

- This ruling has significant implications for the forensic and legal communities, as experts must now be prepared to testify in court regarding their findings. Preparing for expert testimony is essential, as it can be a daunting task

- Testifying in cyber crime cases can be a complex and challenging task, as these cases often involve technical details that may be difficult for non-experts to understand. Here are some tips to help you prepare for testifying evidence in a cyber crime case:

  - **Understand the evidence:** As a witness, it is important to understand the evidence that you will be testifying about. This may include digital evidence such as computer files, emails, or other electronic data.

  - **Review the evidence:** Review the evidence carefully before the trial, and be sure to note any important details or information that may be relevant to the case. Keep a copy of the evidence with you so you can refer to it during your testimony.

  - **Speak with the attorney:** If you are a witness for one of the parties, speak with their attorney before the trial. They can explain what to expect during the trial and help you prepare for your testimony. Be sure to discuss any concerns or questions you may have.

  - **Be clear and concise:** When giving evidence, speak clearly and concisely, and avoid using technical jargon or acronyms that may not be familiar to the judge or jury. Explain any technical terms or concepts that are necessary to understand your testimony.

  - **Stick to the facts:** Stick to the facts of the case and avoid speculating or offering opinions that are not based on the evidence. Only testify about what you know or have experienced firsthand.

- **Be prepared for cross-examination:** The opposing attorney may try to challenge your testimony or the evidence you present. Be prepared to answer difficult questions and remain calm and composed.

- **Be respectful:** Show respect for the court and the judge. Address the judge as "Your Honor" and be polite to everyone in the courtroom.

- Overall, testifying evidence in a cyber crime case can be challenging, but by understanding the evidence, reviewing it carefully, and being prepared to explain technical terms, you can help ensure that your testimony is accurate and helpful to the case.

6.4.2 INTRODUCTION TO TRIAL PROCESS

- The trial process is a fundamental part of the legal system in which a case is presented in a court of law to determine guilt or innocence, liability or non-liability, or other legal issues. The trial process generally consists of several stages, including pre-trial proceedings, jury selection, opening statements, presentation of evidence, witness testimony, closing arguments, and the verdict.

- During pre-trial proceedings, the parties involved in the case may file motions and engage in discovery, which involves the exchange of information between the parties. Jury selection, also known as voir dire, is the process of choosing a jury from a pool of potential jurors. The selection process typically involves questioning by the attorneys and the judge.

- The trial begins with opening statements, in which the parties outline their case and the evidence they plan to present. The presentation of evidence is a critical part of the trial process, and the parties must comply with strict rules of evidence. Witnesses may be called to testify, and evidence may be presented in the form of documents, photographs, or physical objects.

- Once all the evidence has been presented, the attorneys give their closing arguments, summarizing the evidence and making their case for why their client should prevail. The judge then instructs the jury on the law and the standard for determining guilt or liability.

- The jury then deliberates and returns a verdict, which may be a finding of guilt or liability, a finding of innocence or non-liability, or a hung jury, in which the jury cannot reach a unanimous verdict. The trial process is a complex and often lengthy process, and the outcome can have a significant impact on the lives of those involved.

6.4.3 TRIAL PROCESS WITH RESPECT TO DIGITAL FORENSICS

- The trial process for digital forensics involves the following steps:

  - **Collection:** The first step in the digital forensics trial process is the collection of electronic evidence. This evidence can come from a variety of sources, such as computer hard drives, mobile devices, or network servers.
  - **Analysis:** Once the evidence is collected, it must be analyzed to determine its relevance to the case. This analysis can include identifying key data points, reconstructing events, and examining files and other data.

  - **Preservation:** After the evidence is analyzed, it must be preserved in a manner that ensures its authenticity and admissibility in court. This can involve making copies of the data or storing it in a secure location.

  - **Presentation:** During the trial, the digital evidence is presented to the judge or jury in a way that is easy to understand and relevant to the case. This may involve testimony from digital forensics experts, as well as the use of visual aids such as diagrams or timelines.

  - **Cross-examination:** The opposing side may challenge the authenticity or accuracy of the digital evidence, and the digital forensics expert may be subject to cross-examination. The expert must be prepared to defend their findings and explain their methods.

  - **Admissibility:** The judge will ultimately decide whether the digital evidence is admissible in court. The evidence must be relevant, reliable, and obtained legally in order to be admissible.

- The digital forensics trial process can be complex, as it involves technical knowledge and the ability to present complex data in a way that is easily understood. However, it is an important part of the legal process, as digital evidence can be crucial in many criminal and civil cases.

6.4.4 Testifying as an Evidentiary Witness

- Testifying as an evidentiary witness involves providing information in court under oath that is relevant to a legal proceeding. Evidentiary witnesses are individuals who have firsthand knowledge of the facts of the case, and their testimony is intended to assist the trier of fact, such as a judge or jury, in determining the truth of the matter at issue

- When testifying as a witness, you can give only facts, not opinion.

- For an example, as an IT professional and working network administrator, you may find yourself called upon to testify as a victim

or a witness (i.e., a representative of a company whose network is victimized) in a computer-related crime.

- If you are called to testify as an evidentiary witness, there are a few things you should keep in mind. First, you will be asked to take an oath or affirmation to tell the truth, and it is important to take this seriously. You should also be prepared to answer questions truthfully, to the best of your ability, and without withholding or distorting any relevant information.

- It is also important to be respectful and professional while testifying. You should dress appropriately, speak clearly, and remain calm and composed, even if you are faced with aggressive questioning. You should also listen carefully to the questions being asked, and if you do not understand a question, ask for clarification.

- During your testimony, you may be asked to provide specific details about events or conversations you witnessed or participated in. It is important to be as clear and concise as possible when providing this information, and to avoid speculation or guessing.

- Finally, it is important to remember that your role as an evidentiary witness is to provide factual information, rather than to argue or advocate for a particular outcome. Your testimony may be critical in determining the outcome of a case, and it is important to take this responsibility seriously and to provide accurate and truthful information to the court.

6.4.5 TESTIFYING AS AN EXPERT WITNESS

- Testifying as an expert witness in a cyber crime case involves providing specialized knowledge and expertise related to the technical aspects of the case. As an expert witness in a cyber crime case, you may be asked to explain complex technical concepts, interpret data, and provide an opinion on the actions of the parties involved.

- If you are called to testify as an expert witness in a cyber crime case, there are several things you should keep in mind. First, you should ensure that you have a deep understanding of the subject matter and are fully prepared to answer questions related to the case. This may involve reviewing relevant documents and evidence, conducting additional research, and working closely with the legal team to prepare for trial.

- You should also be prepared to explain technical concepts in simple and understandable terms. Many jurors may not have a technical background, and it is important to communicate your expertise in a way that is accessible and easily understood by a non-technical audience.

- You should be prepared to explain the methodology of your investigation, the tools and techniques you used, and the evidence you discovered. This may involve describing your analysis of computer systems, networks, and digital storage devices, as well as your retrieval of deleted or encrypted data. You should also be prepared to explain your findings and the conclusions you drew from the evidence. This may involve explaining how you linked digital evidence to a specific individual or incident, or how you determined the presence of malware or other malicious activity.

- During your testimony, you may be asked to provide your opinion on the actions of the parties involved in the cyber crime case. It is important to ensure that your opinions are based on solid technical evidence and that you can support your opinions with clear and convincing arguments.

- You should also be prepared to defend your investigation against cross-examination by opposing counsel. This may involve explaining the limitations and potential sources of error in your investigation, as well as your adherence to professional standards and guidelines.

- In addition, it is important to maintain objectivity and independence in your role as an expert witness. Your duty is to the court, and it is essential that you provide unbiased and impartial testimony based on your technical expertise and the facts of the case.

- Finally, as with any witness, it is important to remain respectful and professional during your testimony. You should dress appropriately, speak clearly, and remain calm and composed, even if faced with aggressive questioning. By following these guidelines, you can provide valuable technical expertise to help the court make an informed decision in the cyber crime case.

6.4.6 QUALIFYING AS AN EXPERT

- Qualifying as an expert in a case involves being recognized by the court as having specialized knowledge or expertise in a particular field that is relevant to the case. Experts are often called upon to provide testimony or opinion to help the court better understand complex issues or technical information.

- To qualify as an expert, you must demonstrate to the court that you have the necessary knowledge and expertise in the relevant field. This may involve providing a detailed explanation of your education, training, and professional experience, as well as any certifications or licenses that you hold.

- In addition, you must demonstrate to the court that your knowledge and expertise are relevant to the case at hand. This may involve explaining how your expertise relates to the facts of the case, and how

you can assist the court in understanding technical or complex information that may be relevant to the case.

- To qualify as an expert, you may also be required to demonstrate your objectivity and independence. This may involve disclosing any financial or personal interest you have in the outcome of the case, and demonstrating that your opinions are based on sound, scientific or professional principles, rather than personal bias.

- Once you have demonstrated your expertise and relevance to the case, the court will make a determination as to whether you qualify as an expert. If the court agrees that you are qualified, you will be allowed to provide testimony or opinion in the case.

- In conclusion, qualifying as an expert in a case involves demonstrating to the court that you have the necessary knowledge, expertise, and objectivity to provide testimony or opinion on technical or complex issues relevant to the case. By doing so, you can provide valuable assistance to the court in making an informed decision.

6.4.7 EMPLOYING EXPERTS

- Employing an expert for cases can be a crucial step in building a strong legal case, especially in cases that involve complex technical or scientific issues. An expert can provide specialized knowledge and experience that can help to clarify complex issues and support or refute claims made by the opposing side.

- When employing an expert for a case, there are several important considerations to keep in mind. These include:

  - **Expertise:** The expert you choose should have expertise in the specific area that is relevant to your case. This may involve knowledge of a particular industry, technology, or scientific field, as well as the ability to interpret and analyze technical data and evidence.

  - **Qualifications:** The expert you choose should have the necessary qualifications and experience to support their opinions and testimony in court. This may involve having specific certifications or degrees, as well as a proven track record of success in their field.

  - **Objectivity:** It is important that the expert you choose is objective and unbiased in their analysis and opinions. This may involve ensuring that the expert has no financial or personal interest in the outcome of the case, and that their opinions are based on scientific or professional principles, rather than personal bias.

  - **Communication:** The expert you choose should be able to communicate complex technical or scientific concepts in a way that is easily understandable to non-experts, such as jurors or judges. This

may involve having strong written and verbal communication skills, as well as the ability to provide clear and convincing testimony in court.

- **Cost:** Employing an expert can be expensive, and it is important to consider the cost of hiring an expert when building your legal case. You may want to discuss the cost of hiring an expert with your legal team, and determine if the benefits of having an expert on your side outweigh the cost.

- In conclusion, employing an expert for cases can be an important step in building a strong legal case, especially in cases that involve complex technical or scientific issues. By considering the above factors, you can choose an expert who has the necessary expertise, qualifications, objectivity, communication skills, and cost-effectiveness to support your case in court.

6.4.8 Giving Direct Testimony

- Giving direct testimony typically refers to the act of providing firsthand information or evidence in a legal proceeding or a court of law. Direct testimony involves providing factual statements and observations about an event, situation, or circumstance based on one's personal knowledge or experience.

- Direct testimony is typically given in response to questions posed by an attorney during a trial, and it is intended to help the court or jury make an informed decision based on the facts of the case. It is important for witnesses giving direct testimony to be honest, accurate, and objective in their statements.

- To give effective direct testimony, witnesses should speak clearly, answer questions directly, and avoid speculation or conjecture. They should also remain calm and composed, even under cross-examination by opposing counsel. The goal of direct testimony is to provide a clear and accurate account of the relevant facts, and to help the court or jury reach a fair and just verdict.

6.4.9 Cross Examination

- Cross examination is a legal process in which an attorney questions a witness who has already given testimony in a court proceeding. Cross examination typically occurs after direct examination, which is when an attorney questions their own witness. During cross examination, the opposing attorney has the opportunity to question the witness in order to challenge or undermine their testimony.

- The purpose of cross examination is to test the credibility of the witness, to clarify any inconsistencies in their testimony, and to elicit additional information that may support the opposing party's case. Cross examination is an important part of the adversarial system, as it

allows each side to challenge the evidence and arguments presented by the other.

- During cross examination, the attorney may ask leading questions, which are designed to elicit a specific answer from the witness. The attorney may also attempt to impeach the witness, which means to challenge the witness's credibility by pointing out inconsistencies or contradictions in their testimony.

- It is important to note that cross examination must be conducted in a respectful and professional manner, and that attorneys are bound by ethical rules that prohibit them from asking certain types of questions or engaging in certain types of behavior. The judge has the authority to intervene if the questioning becomes overly aggressive or unfair.

- Therefore, cross examination is a crucial component of a legal proceeding, as it allows each side to challenge the evidence and arguments presented by the other. It can be an intense and often dramatic process, but it is designed to ensure that the truth is revealed and justice is served.

6.5 CYBER CRIME

6.5.1 Cyber Crime

- Cybercrime refers to criminal activities that are committed with the help of internet, computer networks, or other digital technologies. This can include a wide range of illegal activities, such as hacking, identity theft, cyber stalking, online fraud, copyright infringement, and the distribution of viruses and other malware.

- Cybercrime is a growing problem around the world, and it can have serious consequences for individuals, businesses, and governments. Some cybercrimes can cause financial loss, damage to reputation, or even physical harm. In addition, cybercriminals often operate across borders, making it difficult for law enforcement to track them down and bring them to justice..

- Some of the most common forms of cybercrime in India include phishing, hacking, identity theft, online fraud, cyberbullying, and the distribution of malware. Cybercriminals often target individuals and businesses that are not adequately protected, including small and medium-sized enterprises (SMEs) and individual users who are not aware of the risks associated with using the internet.

- To combat cybercrime, governments, law enforcement agencies, and cybersecurity experts work together to develop and implement strategies to prevent and investigate these crimes. This may include measures such as cybersecurity education and awareness campaigns,

increased regulation of online activities, and the development of new technologies to detect and prevent cyber attacks.

6.5.2 CYBER CRIME TYPES IN INDIA

- Cybercrime is a growing problem in India, as the country's rapid development in information technology has created new opportunities for criminals to exploit the internet and other digital technologies.

- Some of the most common types of cybercrime in India include:

  - **Online financial fraud:** This includes activities such as phishing, credit card fraud, and identity theft.

  - **Social media abuse:** This includes harassment, defamation, and the spread of fake news.

  - **Cyberstalking:** This involves using the internet to harass or threaten someone.

  - **Hacking:** This includes unauthorized access to computer systems, websites, or other digital assets.

  - **Online child sexual abuse:** This includes activities such as grooming, sextortion, and the distribution of child pornography.

  - **Identity theft:** Identity theft is a type of cyber crime where the perpetrator steals the victim's personal information, such as their social security number or credit card details, and uses it for fraudulent purposes. In 2021, a group of hackers stole the personal information of millions of users of the job-seeking website, LinkedIn.

  - **Phishing:** A phishing attack is a type of cyber crime where the attacker sends emails or messages pretending to be a legitimate organization or person to trick the victim into providing sensitive information, such as login credentials, credit card details, or other personal information. In 2020, a group of hackers launched a phishing attack on the World Health Organization (WHO) amid the COVID-19 pandemic.

  - **Ransomware:** Ransomware is a type of malware that encrypts a victim's files, rendering them inaccessible, and then demands a ransom payment in exchange for the decryption key. In 2021, the Colonial Pipeline, a major fuel pipeline in the United States, was hit by a ransomware attack that disrupted the fuel supply to the East Coast of the US. In 2022 AIIMS(All India Institute of Medical Science) was also shaken by this kind of attack.

- These are just a few examples of cyber crime cases. As technology continues to evolve, it is likely that cyber crime will continue to be a growing threat to individuals and organizations around the world.

- The Indian government has taken steps to address cybercrime by enacting laws such as the Information Technology Act, 2000, which provides a legal framework for dealing with cyber offenses. The act defines various cybercrimes and specifies punishments for those found guilty of committing them.

- The government has established several agencies and initiatives, including the Cyber Crime Investigation Cell (CCIC), the National Cyber Security Policy, and the Indian Computer Emergency Response Team (CERT-In). These organizations work to identify and investigate cybercrime, as well as to educate the public about the risks associated with using digital technologies.

- The Indian police have also set up specialized units such as the Cyber Crime Investigation Cell and Cyber Crime Police Stations to investigate and prosecute cybercrime cases. However, cybercrime remains a complex and challenging area for law enforcement, as it often involves criminals operating across international borders and using sophisticated technologies to cover their tracks.

- To protect themselves from cybercrime, individuals and organizations in India are advised to take steps such as using strong passwords, avoiding suspicious links and downloads, and keeping their software and operating systems up to date. Additionally, reporting any cybercrime incidents to the appropriate authorities can help to prevent further damage and bring criminals to justice.

6.5.3CYBER CRIME CASE STUDIES

➢ **CASE STUDY 1:-**

- India has witnessed several high-profile cyber crime cases in recent years. Here's a case study of a major cyber crime incident that took place in India:

- In 2016, India's second-largest bank, Punjab National Bank (PNB), fell victim to a massive fraud involving fake letters of credit (LoCs). The scam, which was estimated to be worth over $2 billion, was carried out by two employees of the bank, who had colluded with a diamond merchant and a few other firms.

- The fraudsters had used a sophisticated malware to hack into the bank's core banking system and create fake LoCs, which they then used to obtain credit from other banks. The fraud had been going on for several years, and it was only discovered when one of the banks

that had extended credit to the diamond merchant requested payment from PNB.

- The incident exposed serious lapses in the bank's security systems and led to a sharp decline in the bank's share prices. The Reserve Bank of India (RBI) also imposed a penalty on the bank for its failure to detect the fraud.

- The PNB fraud is a classic example of a cyber crime that involves a combination of technology and human collusion. The incident highlights the need for strong cybersecurity measures and effective risk management practices to prevent and detect cyber attacks. The PNB case also led to increased scrutiny of the banking sector in India, with the RBI taking several steps to improve the security and resilience of the country's financial system.

➢ **CASE STUDY 2**

- One of the biggest cyber crimes in India is the 2016 attack on the National Payment Corporation of India (NPCI), which is the organization that oversees digital payments in the country.

- The attack, which took place in July 2016, involved the theft of over 3.2 million debit card details from several banks in India, including State Bank of India, ICICI Bank, HDFC Bank, and Axis Bank. The stolen card details were used to carry out fraudulent transactions, which resulted in losses of over Rs 1.3 crore (approximately $170,000) for the affected banks.

- The attack was initially believed to have been carried out by an international cyber crime group, but later investigations revealed that the attack was the work of a local gang that had ties to Pakistan. The attackers had managed to install malware on the systems of several banks, which enabled them to access and steal the card details.

- The NPCI and the affected banks quickly took measures to contain the damage and prevent further losses. The incident highlighted the growing threat of cyber attacks on India's financial sector and the need for stronger cybersecurity measures to prevent such attacks in the future.

- The NPCI attack is one of the biggest cyber crimes in India in terms of the scale of the attack and the financial losses suffered by the affected banks. The incident also underscores the importance of cybersecurity for India's digital economy, which is growing rapidly as more and more people in the country adopt digital payment systems.

CASE STUDY 3:- Shreya Singhal v. UOI[7]

- In the instant case, the validity of Section 66A of the IT Act was challenged before the Supreme Court.

- **Facts:** Two women were arrested under Section 66A of the IT Act after they posted allegedly offensive and objectionable comments on Facebook concerning the complete shutdown of Mumbai after the demise of a political leader. Section 66A of the IT Act provides punishment if any person using a computer resource or communication, such information which is offensive, false, or causes annoyance, inconvenience, danger, insult, hatred, injury, or ill will.

- The women, in response to the arrest, filed a petition challenging the constitutionality of Section 66A of the IT Act on the ground that it is violative of the freedom of speech and expression.

- **Decision:** The Supreme Court based its decision on three concepts namely: discussion, advocacy, and incitement. It observed that mere discussion or even advocacy of a cause, no matter how unpopular, is at the heart of the freedom of speech and expression. It was found that Section 66A was capable of restricting all forms of communication and it contained no distinction between mere advocacy or discussion on a particular cause which is offensive to some and incitement by such words leading to a causal connection to public disorder, security, health, and so on.

➢ **CASE STUDY 4:- Christian Louboutin SAS Vs Nakul Bajaj & ORS (2018) 253 DLT 728**

- Background Facts A luxury shoe company filed a lawsuit seeking an injunction against an e-commerce portal for facilitating trademark infringement with a seller of counterfeit goods.

- Issue Whether the defendant is permitted to utilise the plaintiff's logos, marks, and images, which are protected under Section 79 of the Information Technology Act?

- Decision The defendant is more than an intermediary, according to the Court, because the website has complete control over the products supplied through its platform.

- It recognises and promotes third-party vendors to market their wares. The Court also stated that an e-commerce platform's active participation would insulate it from the rights granted to intermediaries under Section 79 of the IT Act.

➢ CASE STUDY 5 :- RANSOMEWARE ATTACK AIIMS

- India's top public health institute, All India Institute of Medical Sciences (AIIMS), Delhi came under heavy ransomware attack, crippling routine health service affecting thousands of patients.

- The cyber-attack comes within a month after AIIMS announced that it would go paperless from January 1, 2023, and be fully digitised by April 2023.

- According to the media reports, the AIIMS management stated that a ransomware had "affected outpatient and inpatient digital hospital services, including smart lab, billing, report generation, appointment scheduling". The attack is believed to be a possible ransomware attack where the criminals who hacked into the system were reportedly asking for a ransom payment, though this has been denied by Delhi Police.

- Of the 100 servers — 40 physical and 60 virtual — five physical servers were infiltrated by the hackers. The damage could have been far worse but was contained. Data in the servers was successfully retrieved,
- Ransomware is essentially a kind of malicious software where the perpetrator is able to gain illegal access to the victim's data and ask for a ransom to restore access to the data for the victim.

- Due to the 10-day long cyber attack, AIIMS Delhi had to switch to manual management of emergency and other allied health services.

- The Indian Computer Emergency Response Team (CERT-IN) in its India Ransomware Report 2022 stated that there is a 51-percent increase in the number of ransomware attacks across multiple sectors including critical infrastructure.

More about AIIMS cyber attack:

1. **Halting access:** The organisation's critical data is encrypted so that they cannot access files, databases, or applications stored on the main and backup servers of the hospital.

2. **Ransom demand:** The attackers have made an undisclosed demand to be sought in cryptocurrency in exchange for a key that would decrypt the data.

3. **Multi-agency investigation:** The extent and threat of the attack is so much that multiple agencies like Delhi Police, the Centre's Computer Emergency Response Team (CERT-In), the Ministry of Home Affairs, and even the National Investigation Agency have joined the probe.

4. **Contingency plan:** Meanwhile, AIIMS Delhi has decided to get four new servers from the Defence Research and Development Organisation (DRDO) to be used on an immediate basis to provide e-hospital facility for patients.

6.5.4 Safeguards Available in India Against Cyber Threats

- Information Technology Act, 2000 (Amended in 2008): It is the main law for dealing with cybercrime and digital commerce in India.

- **National Critical Information Infrastructure Protection Centre (NCIIPC):** It was created under Section 70A of IT Act 2000 to protect the nation's critical information infrastructure.

- **CERT-In (Cyber Emergency Response Team):** It is National Nodal Agency for Cyber Security and is operational since 2004.

- **National Cyber Security Policy, 2013:** The policy provides the vision and strategic direction to protect the national cyberspace.

- **Cyber Swachhta Kendra:** It helps users to analyse and keep their systems free of various viruses, bots/ malware, Trojans etc.

- Cyber Surakshit Bharat: It was launched in 2018 to spread awareness about cybercrime and building capacity for safety measures for Chief Information Security Officers and frontline IT staff across all government departments.

6.6 SUMMARY

- Cybercrime refers to criminal activities that are committed using digital technologies, such as computers, the internet, and mobile devices. The rise of cybercrime has led to the development of laws and regulations aimed at preventing and punishing these activities.

- Laws and regulations provide a legal framework for addressing cyber crime, protecting personal data, and promoting cyber security. They often include provisions for punishing cyber criminals, regulating companies that handle sensitive data, and promoting information sharing among organizations to prevent cyber threats. The laws and regulations related to cyber crime are constantly evolving to keep up with the changing technology landscape and emerging cyber threats.

- In recent years, laws and regulations related to technology and the internet have become increasingly important, as more and more activities take place online. These include laws related to cyber crime, data protection, and online privacy.

- The IT Act 2000 is an important law that aims to provide a legal framework for electronic transactions and cyber security in India. It

has been amended over the years to keep up with the changing technology landscape and address emerging cyber threats.

- The laws related to cybercrime and data privacy are complex and rapidly evolving. It is important for individuals and businesses to stay informed about these laws and to take steps to protect themselves from cyber threats.

- Giving evidence and testimony in court can be a daunting and challenging experience. However, it is a critical part of the justice system, and it is important for witnesses to understand their rights and responsibilities when called upon to testify. Witnesses must also answer questions to the best of their knowledge and recollection, and must not withhold any relevant information. It is important for witnesses to be well-prepared when giving evidence in court. This includes reviewing any relevant documents or materials, practicing their testimony, and being aware of the procedures and protocols that are followed in court.

6.7 REFERENCES

1. The Information Technology Act, Author: S.R. Bhansali.
2. Internet Law, Author: Rodney D. Ryder
3. Information Technology Law and Practice, Author: Vakul Sharma.
4. International Journal of Law and Information Technology.
5. Indian Journal of Law [Manupatra].
6. https://www.computerhope.com/jargon/c/cyber-law.htm.
7. (2013) 12 SCC 73.
8. https://www.lawyersclubindia.com/articles/landmark-judgments-on-cyber-law-14025.asp.
9. https://en.wikipedia.org/wiki/IT_law.
10. https://www.meity.gov.in/content/cyber-laws.
11. https://www.crime-scene-investigator.net/testifying-in-court-as-a-forensic-expert.html

6.8 UNIT END EXERCISE

1. Do a case study on vicarious liability.
2. Do a case study on Federal Laws

6.9 QUESTIONS

1. Write a short note on Laws and Regulations.
2. Write difference between the criminal and the civil cases.
3. Explain Information Technology Act
4. Explain the sections and punishment of IT Act
5. Explain Giving evidence in court>