Question Bank - Cyber Forensics

Unit 1

Q1. What are the steps taken to apply a systematic approach to an investigation? Elaborate.

Ans.

The systematic approach to an investigation in Cyber Forensics typically involves the following steps:

- Identification
    - Identifying what evidence is present, where it is stored, how it is stored (in which format).
    - Electronic devices can be personal computers, Mobile phones, PDAs, etc.
- Preservation
    - Data is isolated, secured, and preserved.
    - It includes prohibiting unauthorized personnel from using the digital device so that digital evidence, mistakenly or purposely, is not tampered with and making a copy of the original evidence.
- Analysis
    - Forensic lab personnel reconstruct fragments of data and draw conclusions based on evidence.
- Documentation
    - A record of all the visible data is created.
    - It helps in recreating and reviewing the crime scene.
    - All the findings from the investigations are documented.
- Presentation
    - All the documented findings are produced in a court of law for further investigations.
- Procedure
    - The procedure starts with identifying the devices used and collecting the preliminary evidence on the crime scene.
    - Then the court warrant is obtained for the seizures of the evidence which leads to the seizure of the evidence.
    - The evidence is then transported to the forensics lab for further investigations and the procedure of transportation of the evidence from the crime scene to labs is called chain of custody.
    - The evidence is then copied for analysis and the original evidence is kept safe because analysis is always done on the copied evidence and not the original evidence.
    - The analysis is then done on the copied evidence for suspicious activities and accordingly the findings are documented in a non technical tone.
    - The documented findings are then presented in the court of law for further investigation

Q2. Define “Image Acquisition”. Write a note on whole disk encryption.

Ans.

- Image acquisition refers to the process of creating a digital image of a physical storage device or a logical drive for forensic analysis.
- In cyber forensics, image acquisition plays a crucial role in extracting information from the digital evidence without altering it.
- Whole Disk Encryption
    1. Whole disk encryption is a technique used to protect the data stored on a storage device by encrypting the entire disk, including the operating system and installed applications.
    2. In cyber forensics, this technique poses a challenge for investigators because they need to access the data in an unencrypted form to perform their analysis.
    3. It works by automatically converting data on a hard drive into a format that can't be understood by anyone who doesn't have the key to undo the conversion.
    4. Specifically, the hard drive is converted from a readable plaintext to a ciphertext that isn't readable unless it's converted back to plaintext with a key.
    5. Without the proper authentication key, even if the hard drive is removed and placed in another machine, the data remains inaccessible.
    6. To overcome this challenge, investigators can use a technique called live imaging, where they create a copy of the disk while the operating system is running.
    7. This technique requires investigators to have the encryption key to access the data.
    8. Another approach to tackle whole disk encryption is to use a cold boot attack.
    9. In this technique, the investigator forcibly shuts down the computer and tries to extract the encryption key from the computer's memory.
    10. This technique works because the memory chips retain the data for a few seconds even after the power is removed.
    11. In conclusion, whole disk encryption is an effective technique but presents a challenge for cyber forensic investigators.
    12. The use of a live imaging technique or a cold boot attack can help overcome this challenge and extract the required information for the investigation.

Q3. What are the tasks performed by computer forensics tools? Explain.

Ans.

All computer forensics tools, both hardware and software, perform specific functions.

These functions are grouped into five major categories:

1. Acquisition
    a. Acquisition, the first task in computer forensics investigations, is making a copy of the original drive.
    b. This procedure preserves the original drive to make sure it doesn't become corrupt and damage the digital evidence.
    c. Sub-functions in the acquisition category include the following:
        i. Physical data copy
        ii. Logical data copy
        iii. Data acquisition format
        iv. Command-line acquisition
        v. GUI acquisition
        vi. Remote acquisition
        vii. Verification

2. Validation and discrimination
    a. Two issues in dealing with computer evidence are critical.
    b. First is ensuring the integrity of data being copied - the validation process.
    c. Second is the discrimination of data, which involves sorting and searching through all investigation data.
    d. The process of validating data is what allows discrimination of data.
    e. Many forensics software vendors offer three methods for discriminating data values.
    f. These are the sub-functions of the validation and discrimination function:
        i. Hashing
        ii. Filtering
        iii. Analyzing file headers.

3. Extraction
    a. The extraction function is the recovery task in a computing investigation and is the most challenging of all tasks to master.
    b. Recovering data is the first step in analyzing an investigation's data.
    c. The following sub-functions of extraction are used in investigations:
        i. Data viewing
        ii. Keyword searching
        iii. Decompressing
        iv. Decrypting
        v. Bookmarking

4. Reconstruction
    a. 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.
    b. 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.
    c. These are the sub-functions of reconstruction:
        i. Disk-to-disk copy
        ii. Image-to-disk copy
        iii. Partition-to-partition copy
        iv. Image-to-partition copy

5. Reporting
    a. To complete a forensics disk analysis and examination, we need to create a report.
    b. Before Windows forensics tools were available, this process required copying data from a suspect drive and extracting the digital evidence manually.
    c. The investigator then copied the evidence to a separate program, such as a word processor, to create a report.
    d. Windows forensics tools can produce electronic reports in a variety of formats, such as word processing documents, HTML Web pages, or Acrobat PDF files.
    e. These are the sub-functions of the reporting function:
        i. Log reports
        ii. Report generator

Q4. Explain in brief the need of computer forensics software tools.

Ans.

1. Computer forensics software tools are necessary for conducting digital investigations and analyzing digital evidence.
2. With the increasing use of technology in everyday life, there is a growing need for tools that can extract and analyze digital evidence from various devices such as computers, smartphones, and other digital storage media.
3. Computer forensics software tools are specifically designed to help investigators collect, preserve, and analyze digital evidence.
4. These tools can help investigators retrieve deleted files, analyze internet browsing history, recover encrypted data, and identify malicious software or other digital threats.
5. These tools can assist investigators in building a timeline of events, tracking changes made to files, and identifying potential sources of digital evidence.
6. The use of computer forensics software tools is essential in modern-day investigations, particularly in cases involving cybercrime, intellectual property theft, and fraud.
7. These tools provide investigators with the ability to examine digital evidence thoroughly and efficiently, helping to build a stronger case and increase the chances of a successful prosecution.
8. Cybercrime Investigations:
    a. Cybercrime is a growing concern worldwide, and computer forensics software tools are essential in investigating these types of crimes.
    b. These tools can help identify sources of malware, track down cybercriminals, and recover data that has been stolen or encrypted.
    c. For example, software tools like EnCase, FTK, and X-Ways Forensics are commonly used in cybercrime investigations.
9. Fraud Investigations:
    a. Fraud investigations often involve digital evidence, and computer forensics software tools are essential in analyzing this evidence.
    b. These tools can help identify fraudulent transactions, recover deleted data, and analyze financial records.
    c. For example, software tools like Nuix, Autopsy, and Paladin are commonly used in fraud investigations.

Q11. Describe how to validate data acquisitions.

Ans.

Validating data acquisition involves ensuring that the data collected is accurate, complete, and reliable.
Here are some steps to follow to validate data acquisition:

- Define the data acquisition process:
    - Start by clearly defining the data acquisition process, including the data sources, collection methods, and expected outcomes.
- Determine data accuracy:
    - Check the accuracy of the data collected.
    - This involves comparing the collected data against known or expected values.
    - If the data is inaccurate, investigate the reason for the discrepancy and take appropriate corrective action.
- Check data completeness:
    - Ensure that all the required data has been collected.
    - This can be achieved by cross-checking the collected data against the list of required data elements.
- Ensure data reliability:
    - Verify that the data collection methods used are reliable and consistent.
    - For instance, if the data is collected using sensors or other measuring instruments, verify that the instruments are calibrated and functioning correctly.
- Perform data quality checks:
    - Apply data quality checks, such as checking for data consistency, outliers, and missing values.
    - Use statistical methods to identify any anomalies and ensure that they are resolved appropriately.
- Validate data with stakeholders:
    - Consult with stakeholders to validate the data collected.
    - This involves reviewing the data with the stakeholders to ensure that it is accurate, complete, and relevant to their needs.
- Document data acquisition validation:
    - Document the data acquisition validation process, including the methods used, the results obtained, and any corrective actions taken.

Q17. Describe how to conduct an investigation.
Ans.
To Conduct Forensic Investigation there are four common steps to follow

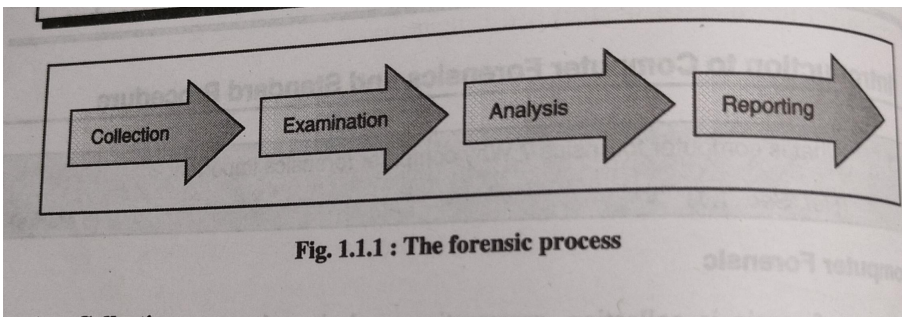


Fig. 1.1.1 : The forensic process

- Collection
    - This is the first phase in the forensic process.

    - In this phase data is identified, labeled and recorded and gathering the data and physical evidence related to the incident being invested is done. Simultaneously integrity of the chain of custody is also preserved.
- Examination
    - In this phase from the collected data identify and extract the pertinent information, using proper forensic tools and techniques and also maintain integrity of the evidence.

- Analysis
    - In this phase results of the examination phase are analyzed.
    - From the analysis useful answers to the questions are generated which are presented in the previous phases.
    - Most probably the case gets solved in this phase.
- Reporting
    - In the reporting phase the results of the analysis are done, which contains
    - The information pertinent to the case.
    - Actions that have been accomplished are left to be performed.
    - Moves left to be performed.
    - Advocated enhancements to processes and tools.

OR

To conduct an investigation in cyber forensics, the following steps need to be taken:

- Identify and secure the evidence:
    - The first step is to identify the device or system that has been subject to the cyber incident and secure it.
    - The evidence needs to be secured in a way that maintains its integrity.
- Preserve the evidence:
    - The evidence should be preserved to avoid contamination or damage.
    - This includes identifying the physical location of the device, being aware of any external influences that may have affected it (such as power outages) and using appropriate tools and techniques to preserve the data.
- Analyze the evidence:
    - Once the evidence has been secured and preserved, it needs to be analyzed.
    - This involves examining the data to identify any evidence of a cyber incident.
    - The analysis may include data recovery, decryption, and searching for metadata.
- Determine the scope:
    - Once the evidence has been analyzed, the scope of the incident needs to be determined.
    - This involves identifying who was behind the incident and what actions were taken.
    - It is important to determine whether the scope of the incident extends beyond the identified device.
- Report and communicate:
    - Once the investigation is complete, a report needs to be prepared.
    - This report should include a summary of the incident, the evidence that was found, and the implications of the incident.
    - It is important to communicate the report and its findings to the relevant stakeholders.

- Take appropriate action:
    - The final step is to take appropriate action based on the findings of the investigation.
    - This could include legal action, implementing new security measures, or updating policies and procedures.

Overall, conducting an investigation in cyber forensics requires a methodical approach to ensure the preservation of evidence, accurate analysis, and appropriate action based on the findings.

Q21. Describe the importance of network forensics
Ans.

- Network forensics is the process of capturing, recording, and analyzing network traffic to identify and investigate security incidents or other network-related issues.
- It is an essential aspect of computer forensics and is crucial in detecting and responding to security breaches and other network-related incidents.
- Here are some key reasons why network forensics is important:
    - Detecting Network Threats:
        - Network forensics provides visibility into network traffic, allowing security analysts to detect and investigate potential security threats.
        - By analyzing network traffic patterns, it is possible to identify suspicious activity, such as data exfiltration, unauthorized access attempts, and malware infections.
    - Incident Response:
        - Network forensics is an essential component of incident response, providing a detailed record of events leading up to and during a security incident.
        - This information is invaluable in determining the scope and impact of an incident, identifying the source of the attack, and developing an effective response plan.
    - Compliance and Auditing:
        - Many organizations are required to comply with industry-specific regulations and standards that mandate the use of network forensics tools.
        - By implementing network forensics solutions, organizations can monitor and analyze network activity to ensure compliance with these requirements and provide auditors with the necessary evidence of compliance.
    - Preventing Future Attacks:
        - By analyzing network traffic and identifying security threats, network forensics can help organizations identify vulnerabilities and weaknesses in their network infrastructure.
        - This information can be used to develop and implement security measures to prevent future attacks.

Q19. Write a note on data encryption and compression.
Ans.
Data Encryption and Compression

- According to recent research figures, last year more than 15-million different malware files were detected with nearly 300 000 new malware samples being recorded every day.
- Against this backdrop, data file encryption techniques are evolving rapidly to protect information stored on tablets and PCs from theft and unintentional data loss.
- Data encryption is the ciphering or scrambling of data.
- The only way to decipher or unscramble it is via a deciphering mechanism.
- This can be in the form of a key, long passcode, portable radio frequency identification (RFID) chip, or a combination of these and other techniques.
- Data encryption is a strongly advised method of not only securing tablets and PCs, but also network- attached devices and the often-critical information they contain.
- More specifically, data encryption is growing increasingly popular in today's approach to email security with "clientless' methods pioneered by industry leaders who are setting the standard for effectiveness and also for ease of setup and customization to suit diverse requirements and environments.

The importance of encryption

- Encryption is being accepted as a fundamental element of data protection and the overall threat protection landscape.
- In this light, are three key reasons why businesses need to consider encryption.
    - The first is protection for sensitive data against hacking and data breaches.
    - The second is to safeguard against unintended information disclosure through accidental exposure of critical data.
    - Thirdly, the migration to cloud-based services presents a security issue, and encryption is able to assist companies to protect data that may be vulnerable in this scenario. In order for encryption to be effective, it has to be easy to manage, transparent to users, and able to work with multiple platforms and file types.
    - There is a fourth and most important reason for the adoption of data encryption solutions: Encryption helps companies comply with new legislation requirements mitigating potentially large fines. In the European Union (EU) the General Data Protection Regulation (GDPR) recently came into effect. It mandates all companies holding customer or employee data to secure the data or face severe financial penalties of up to 4% of annual worldwide revenue.
- Legislation confirms that encryption is accepted as one of the best - if not the best - security measures available.
- Data compression techniques can complement data encryption in a comprehensive data security application.
- They are often key components of commonly deployed cybercrime tightening regimes. Data compression removes redundant character strings in a Tile leaving the compressed Tile with a more uniform distribution of characters.
- However, the use of compression algorithms should depend on operational constraints. For example, if an organization has storage or bandwidth challenges and there isa need to compress data, many specialists advise that it should be compressed first then encrypted.
- Until recently, compressing encrypted text was not advised as the cryptogram is, in essence, a random series of bytes that do not compress well.

- However, newer data storage methods efficiently couple data compression with encryption in simultaneous compression/encryption schemes that can help limit the performance penalty that certain data compression algorithms present.

OR

- A few criminals are becoming smarter.
- So data-hiding techniques which include encryption and steganography.
- The evidence of criminal activity is placed in such a way where traditional search methods cannot find it.
- Encryption Scrambling data, for example an e-mail message, so that it cannot be readable to the interceptor.
- Many publically available programs permit the user to create virtual encrypted disks which are opened by selected key.
- It is not possible to read the encrypted data without the key.
- When you encrypt a file, only contents of the file get encrypted but the name of the file, size and the timestamps are unencrypted. It is possible to build the parts of the content of the file from other locations, such as swap file, temporary files, and deleted, unencrypted copies.
- In computer forensics, many encryption programs with extra functions makes the investigation difficult.
- Few functions include use of a key file, plausible deniability, and full-volume encryption.
- Steganography
    - It is nothing but hiding a message into a larger file, typically in a photographic image or sound file.
    - Steganography has the capability of disrupting the forensic process when used correctly.
    - In computer forensics to preserve the data evidence MD5 is used for data integrity and cryptcat is used to encrypt the data which is transferred via net.
- Data Compression
    - Many computer users use compression tools like WinZip, Alzip and WinRAR.
    - These are the widely used compression tools and support many compressed formats.
    - These tools are mainly used for archiving purposes.
    - The DEFLATE algorithm is the main compression algorithm for WinZip and Alzip. WinRAR uses a modified version of this DEFLATE algorithm.
    - For example, zip, gz and alz are extensions of the given compression algorithms which use the DEFLATE data compression algorithm.
    - The dual algorithm for decompression is known as INFLATE.
    - Since the DEFLATE and INFLATE algorithms are common among compression utilities these are used for damaged compressed file recovery methodology.

      OR

Data Encryption

- Encryption is a method of transforming data with the intention of keeping it a secret.
- Encryption uses an algorithm called a cipher to encrypt data and it can be decrypted only using a special key.

- Encrypted information is known as ciphertext and the process of obtaining the original information (plaintext) from the ciphertext is known as decryption.
- Encryption is specially required when communicating over an untrusted medium such as the internet, where information needs to be protected from other third parties.
- Modern encryption methods focus on developing encryption algorithms (ciphers) that are hard to break by an adversary due to the computational hardness (therefore could not be broken by a practical means).
- Two of the widely used encryption methods are Symmetric key encryption and Public-key encryption.
- In Symmetric key encryption, both the sender and the receiver share the same key used to encrypt the data.
- In Public-key encryption, two different but mathematically related keys are used.

Data Compression

- Data compression is a method of transforming data with the intention of reducing its size.
- This is useful because it allows saving resources like storage space and bandwidth (when transferring data).
- It uses an encoding method that will reduce the amount of bits used to store the data than the original representation.
- When using compressed data, they need to be decompressed first.
- When designing a data compression scheme, one has to consider important factors such as the level of compression required, amount of distortion introduced by the compression scheme and the computational and hardware resources required to compress and decompress data.
- Especially, when it comes to video decompression, special hardware will be required to decompress the stream fast enough so that the viewing is not disturbed.
- With video, decompressing beforehand would not be an option since it will require a large storage space.

Unit 2

Q5. Describe some common peer-to-peer networks or applications.

Ans.

Peer-to-peer (P2P) networks are a type of network architecture where all nodes in the network act as both clients and servers.

In P2P networks, each node can initiate and respond to requests for data or services, and there is no centralized server or hierarchy of nodes.

This model allows for distributed computer communication and has been a vital part of many file-sharing networks over the years.

Here are some common examples of P2P networks or applications:

1. **BitTorrent:**
   - ➢ BitTorrent is a popular P2P file-sharing protocol used to distribute large files over the internet.
   - ➢ It allows users to share files with other users in a decentralized manner, where each user acts as a source and a receiver of the data.
   - ➢ The BitTorrent protocol breaks up large files into smaller pieces, which are then distributed among multiple users, making it faster and more efficient than traditional file-sharing methods.
2. **Skype:**
   - ➢ Skype is a popular P2P communication application that allows users to make voice and video calls over the internet.
   - ➢ Skype uses a hybrid P2P architecture, where some of the data is sent directly between users, while other data is routed through centralized servers.
3. **Bitcoin:**
   - ➢ Bitcoin is a digital cryptocurrency that uses a decentralized P2P network to facilitate transactions.
   - ➢ Transactions are verified and recorded on a distributed ledger called the blockchain, which is maintained by a network of nodes.
4. **Napster:**
   - ➢ Napster was one of the first P2P file-sharing applications, allowing users to share music files over the internet.
   - ➢ It was shut down in 2001 due to copyright infringement issues.
5. **Gnutella:**
   - ➢ Gnutella is a decentralized P2P file-sharing network that allows users to share files without the need for a centralized server.
   - ➢ It uses a distributed hash table (DHT) to locate files and nodes in the network.

Q6. Write a note on "The Examination and Analysis Phases" in Internet forensics.

Ans.

1. The examination and analysis phases are critical steps in the process of conducting Internet forensics investigations.

2. These phases involve the collection and analysis of digital evidence from various sources, including network traffic, internet service provider (ISP) logs, and user devices.
3. Here's a brief overview of these two phases:
    a. Examination Phase:
        i. The examination phase involves the identification, acquisition, and preservation of digital evidence related to the investigation.
        ii. This includes collecting data from ISP logs, network traffic captures, and user devices such as computers, smartphones, and tablets.
        iii. The collected data is then stored in a secure location to ensure its integrity and authenticity.
    b. Analysis Phase:
        i. The analysis phase involves the examination and interpretation of the collected data to determine the sequence of events that occurred and identify the parties involved.
        ii. This phase includes a variety of techniques, including data mining, network analysis, and forensic analysis of individual devices.
        iii. During this phase, investigators use specialized tools and software to analyze the collected data, identify patterns, and reconstruct events.
4. The examination and analysis phases are crucial to the success of Internet forensics investigations.
5. They help investigators identify and collect relevant digital evidence, preserve it in a secure manner, and analyze it to reconstruct the sequence of events leading up to a particular incident.
6. By conducting a thorough examination and analysis, investigators can identify the parties responsible for the incident, develop a timeline of events, and provide evidence that can be used in court to prosecute the offenders.

Q7. Elaborate: Collection Phase - Local Acquisition.

Ans.

1. The lines between computer and Internet forensics blur when it comes to local acquisition.
2. 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.
3. 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.
4. Artifacts are generated from the use of the Internet through a web browser, email correspondence and instant messaging.
5. There are three types of traces: history, cache, and cookies
    a. BrowserHistory:
        - The browser history contains all the URLs you have either typed into the address bar.
        - 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 a 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.

b. BrowserCache:

- ➢ Most 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.
- ➢ As it saves network traffic and reduces response time, pleasing both the user and the server.

c. BrowserCookies:

- ➢ Many third-party services have specialized in brokering advertisement between advertisers and content providers, with an increasing focus on targeted advertising.
- ➢ 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).

Or

- Local acquisition in cyber forensics refers to the process of acquiring digital evidence from a computer or device that is physically located at the incident scene.
- This type of acquisition is often conducted by law enforcement agencies or forensic investigators who need to collect evidence for use in criminal investigations or legal proceedings.
- The process of local acquisition typically involves removing the hard drive or other storage media from the device and connecting it to a write-blocker, which is a hardware device that prevents any changes from being made to the data on the storage media.
- Once the storage media is connected to the write-blocker, it can then be imaged using a variety of forensic tools and techniques.

- This process involves creating an image or copy of the digital storage media, such as a hard drive, solid-state drive, or flash drive, and analyzing the contents of the image to identify evidence of criminal activity.
- The goal of local acquisition is to identify and preserve all potential sources of evidence, including deleted files, internet history, and system logs, which may be critical to an investigation.
- It is important to note that local acquisition should only be undertaken by experienced professionals who are trained in cyber forensics and understand the proper procedures for collecting and preserving digital evidence.
- Improper acquisition methods or mishandling of evidence can lead to the evidence being compromised or invalidated, which could have serious consequences for the investigation or legal proceedings.
- Proper documentation and chain of custody procedures should also be followed to ensure that the collected evidence is admissible in court.
- Ultimately, the goal of local acquisition in cyber forensics is to provide accurate and reliable digital evidence that can be used to support criminal investigations and prosecution.

Q8. Elaborate: Collection Phase - Network Acquisition.

Ans.

1. The collection phase of digital forensics investigations involves the identification, acquisition, and preservation of digital evidence.
2. In the context of network forensics, the collection phase involves the acquisition of data from various sources, including network devices, network traffic, and logs.
3. Network acquisition is a critical part of the collection phase and involves the capture and preservation of network traffic data for analysis.

<u>Process of Network Acquisition in Collection Phase:</u>

1. **Identify Data Sources:**
    a. The first step in the network acquisition phase is to identify the data sources that are relevant to the investigation.
    b. This may include data from network devices, such as routers and switches, as well as network traffic data from various sources, such as network taps, packet sniffers, and intrusion detection systems.
2. **Select Acquisition Methods:**
    a. Once the relevant data sources have been identified, the next step is to select the appropriate acquisition methods.
    b. Network acquisition methods may include packet capture, network taps, or port mirroring, depending on the specific requirements of the investigation.
3. **Capture Network Traffic:**
    a. The next step is to capture network traffic data using the selected acquisition methods.
    b. Packet capture tools such as Wireshark or tcpdump are commonly used to capture network traffic data.
    c. The data is typically captured in a file format, such as PCAP or PCAPNG.
4. **Preserve Data Integrity:**
    a. After capturing network traffic data, it's important to preserve its integrity and authenticity.

b. This involves securely storing the data and ensuring that it's not tampered with in any way.
c. The captured data should be stored in a secure location and protected from unauthorized access.

5. **Analyze Data:**
    a. Once the network traffic data has been captured and preserved, the analysis phase can begin.
    b. During this phase, network forensics tools are used to analyze the captured data to identify suspicious activity or security breaches.

Q9. Elaborate: Collection Phase - Remote Acquisition.

Ans.

1. Recent improvements in computer forensics tools include the capability to acquire disk data or data fragments (sparse or logical) remotely.
2. With this feature, we can connect to a suspect computer remotely via a network connection and copy data from it.
3. Remote acquisition tools vary in configurations and capabilities. Some require manual intervention on remote suspect computers to initiate the data copy.
4. Others can acquire data surreptitiously through an encrypted link by pushing a remote access program to the suspect's computer.
5. From an investigation perspective, being able to connect to a suspect's computer remotely to perform an acquisition has tremendous appeal.
6. It minimizes the chances of a suspect discovering that an investigation is taking place.
7. Most remote acquisitions have to be done as live acquisitions, not static acquisitions.
8. The following section describes how to perform remote acquisitions in ProDiscover:
    a. Remote Acquisition with ProDiscover:
        i. Two versions of ProDiscover can perform remote acquisitions: ProDiscover Investigator and ProDiscover Incident Response.
        ii. When connected to a remote computer, both tools use the ProDiscover acquisition method.
        iii. After the connection is established, the remote computer is displayed in the Capture Image dialog box.
        iv. ProDiscover Investigator is designed to capture data from a suspect's computer while the user is operating it, which is a live acquisition.
        v. ProDiscover Incident Response is designed to be integrated as a network intrusion analysis tool.
    b. Remote Acquisition with EnCase Enterprise:
        i. EnCase Enterprise is set up with an Examiner workstation and a Secure Authentication for EnCase (SAFE) workstation.
        ii. Acquisition and analysis are conducted on the Examiner workstation.
        iii. The SAFE workstation provides secure encrypted authentication for the Examiner workstation and the suspect's system.
        iv. The remote access program in EnCase Enterprise is Servlet, a passive utility installed on the suspect computer.
        v. Servlet connects the suspect computer to the Examiner and SAFE workstations.

vi. A unique feature is that Servlet can run in stealth mode on the suspect computer.

c. Remote Acquisition with R-Tools R-Studio:
   i. The R-Tools suite of software is designed for data recovery.
   ii. As part of this recovery capability, the R-Studio network edition can remotely access networked computer systems.
   iii. Its remote connection uses Triple Data Encryption Standard (3DES) encryption.
   iv. Data acquired with R-Studio network edition creates raw format acquisitions, and it's capable of recovering the following file systems:
      1. FAT12, FAT16, FAT32
      2. NTFS, NTFS5
      3. Ext2FS, Ext3FS
      4. UFS1, USF2

d. Remote Acquisition with WetStone LiveWire:
   i. 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.
   ii. LiveWire's acquisition file format is raw (.dd).
   iii. In addition to being able to copy disk data, LiveWire can capture RAM data from remote systems.

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

f. Remote Acquisition with Runtime Software:
   i. Runtime Software offers several compact shareware programs for data recovery.
   ii. For remote acquisitions, Runtime has created these utilities:
      1. DiskExplorer for FAT
      2. DiskExplorer for NTFS
      3. HDHOST
   iii. Runtime has designed its tools to be file system specific, so DiskExplorer versions for both FAT and NTFS are available.
   iv. HDHOST is a remote access program that allows communication between two computers.
   v. The connection is established between systems by using the DiskExplorer program corresponding to the suspect (remote) computer's drives.

Q10. Write a note on the following:
a. World Wide Web Threats
Ans:

- There are many forms of intrusion and attacks.
- As compared to internal threats, external threats get the most attention.
- Attackers may or may not have computer knowledge and skills to launch an attack.
- The hackers learn the details of the computer system by performing attacks.
- To access the system illegally they try to get the user credentials
- Few of the attacks are unintentional which happens because of lack of knowledge.
- Attacks can be done without gaining entry to the network or system.
- However, as with any technology, the Web is also susceptible to various threats that can compromise the security, privacy, and integrity of users and organizations
- Here are some common World Wide Web threats:
    - Malware: Malware is malicious software that is designed to infect computers and steal sensitive information.
    - Phishing: Phishing is a type of cyber attack that involves sending fraudulent emails or creating fake websites to trick users into disclosing sensitive information such as usernames, passwords, and credit card numbers.
    - Denial of Service (DoS) Attacks: DoS attacks are designed to disrupt the normal functioning of a website or web application by overwhelming it with traffic.
    - SQL Injection: SQL injection is a type of attack in which an attacker injects malicious SQL code into a web application, potentially allowing them to access or manipulate sensitive data stored in a database.

Q13. Explain the role of e-mail in investigations.
Ans.

- Email 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 email to see whether it's authentic.
- Typically, phishing emails 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 email to solicit victims, thus saving postage costs of international mail.
- Unlike newer, more sophisticated phishing email 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.

Q14. 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 email 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 email 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 email messages.
- Regardless of the OS or e-mail program, users access their email based on permissions the email 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 email.
- Overall, an intranet email 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 email 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 email accounts, and usernames tend to follow a naming convention that the email 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 email services, such as Google, Hotmail, or Yahoo!, owns the email server and accepts everyone who signs up for the service by providing a username and password.
- Email companies also provide their own servers and administrators.
- After users sign up, they can access their email from any computer connected to the Internet.

Q16. Explain the use of e-mail server logs.

Ans :

- Email server logs are a valuable source of information in digital forensics investigations, as they provide a record of all incoming and outgoing email messages on an email server.
- Email server logs can be used to investigate a range of security incidents, including email-based attacks, data breaches, and intellectual property theft.
- Here are some of the ways in which email server logs can be used:
    - Detecting Suspicious Activity:
        - Email server logs can be used to identify suspicious activity, such as the sending or receiving of large volumes of emails, emails with

suspicious attachments or links, and emails sent from unauthorized IP addresses or domains.

- Tracing Email Paths:
  - Email server logs can be used to trace the path of an email message, identifying the sender, recipient, and any intermediate email servers that the message passed through.
- Identifying User Activity:
  - Email server logs can be used to identify the activity of individual users on the email system, including the sending and receiving of email messages, login times, and IP addresses used.
- Investigating Data Leakage:
  - Email server logs can be used to investigate data leakage incidents, such as the unauthorized sending of sensitive information via email, by identifying the sender, recipient, and contents of the email message.
- Conducting Forensic Analysis:
  - Email server logs can be used as evidence in digital forensics investigations, providing a record of email-based activity that can be analyzed to identify potential security breaches or cyber attacks.

Q20. What are the ways of finding people on social media?
Ans :
There are several ways to find people on social media, including:
Search Engines: Using a search engine, such as Google or Bing, can be an effective way to find people on social media. Simply enter the person's name and other relevant details, such as their location or employer, and the search engine will provide links to their social media profiles.
Social Media Search: Many social media platforms, such as Facebook, Twitter, and LinkedIn, have built-in search features that allow users to search for other users based on their name, location, or other criteria.
Email and Phone Number Search: Some social media platforms, such as Facebook and LinkedIn, allow users to search for other users based on their email address or phone number. This can be a useful way to find people who may not have a visible social media profile.
People Search Engines: There are also specialized people search engines, such as Spokeo and Pipl, that allow users to search for people based on their name, address, phone number, or email address. These search engines can often provide more comprehensive results than traditional search engines.
Reverse Image Search: If you have a photo of the person you are trying to find, you can use a reverse image search engine, such as Google Images, to search for other instances of that photo online. This can help you identify other social media profiles or websites associated with that person.

Q21. Write in brief about location data.
Ans :

1. Location data is a type of digital data that is generated by electronic devices and services that use GPS, Wi-Fi, cellular networks, and other location-based technologies to track and record the location of a user.
2. This data is often used for a range of purposes, including mapping, navigation, and location-based advertising.
3. Location data can be collected by a variety of sources, including smartphones, fitness trackers, smartwatches, and vehicles. It can be used to create a detailed picture of an individual's movements and activities over time, including their home and work locations, travel patterns, and daily routines.
4. The collection and use of location data has raised concerns about privacy and security.
5. Location data can be used to track individuals without their knowledge or consent, and can reveal sensitive information about their personal lives, such as their religious beliefs, political affiliations, and health status.
6. Governments and law enforcement agencies may also use location data in investigations and surveillance activities.
7. In some cases, location data has been used as evidence in criminal cases.
8. To protect their privacy, individuals can take steps to limit the collection and use of their location data. This includes disabling location services on their devices, using privacy-focused search engines and apps, and being mindful of the data they share online.
9. Companies that collect and use location data are required to comply with privacy laws and regulations, and must take steps to protect the data they collect.

Q25. Write a note on Web Cache.
Ans.

- 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.
- 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 don't necessarily refresh the web page.

Q26. Write a note on messenger forensics.
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.
- This evidence 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 using the built-in registry editor for Windows.

Unit 3

Q1. Describe how to prepare for computer investigations and explain the difference between law enforcement agencies and corporate investigations.
Ans.
Preparing for computer investigations involves several essential steps to ensure a thorough and effective investigation.
These steps include:

- Establish an investigation team: The first step is to form a team of experts, including legal counsel, computer forensic experts, and investigators.
- Secure the evidence: It's essential to secure the electronic devices and evidence from any further damage or loss.
- Identify the scope and objectives: The investigation team must define the scope, objectives, and protocols for the investigation.
- Collect data: The team must collect data from relevant sources, such as servers, hard drives, email messages, databases, and network logs.
- Analyze the data: After collecting data, it needs to be analyzed for potential evidence of wrongdoing.
- Document the investigation: The investigation team must document their findings and maintain the chain of custody.

The difference between law enforcement agencies and corporate investigations lies in their objectives, scope, and authority. Law enforcement investigations are typically criminal investigations conducted by law enforcement agencies to gather evidence of criminal activity, which may result in prosecution. In contrast, corporate investigations are conducted by a private organization to determine whether misconduct has occurred within the company, and to identify risks and vulnerabilities for the company. While law enforcement agencies have extensive resources, such as forensic labs and arrest authority, corporate investigations often rely on the expertise of third-party investigators and technical specialists. Additionally, law enforcement investigations are typically focused on criminal charges, while corporate investigations are more oriented towards resolving internal disputes and taking corrective action.

Q4. List the steps in preparing for an evidence search.
Ans.

Obtain a warrant or consent:

- Before beginning any evidence search, you must have legal authorization to conduct it.
- This can be in the form of a warrant obtained through a court order or consent given by the owner or authorized user of the device.

Assemble the team:

- Identify the members of the team who will be involved in the search, including the lead investigator, forensic analysts, and technical support staff.

Secure the device:

- Ensure that the device is properly secured to prevent any further changes to the data.
- This may require disconnecting it from the internet, disabling any automatic software updates, and physically securing the device.

Document the device:

- Take detailed notes of all hardware and software components, including their version numbers and any unique identifiers.
- Also, document their current state, including whether they are on or off, encrypted, or password-protected.

Create a forensic image:

- Make an exact copy of the data on the device using a specialized software or hardware tool.
- This will preserve the data in its original state and allow it to be analyzed without altering or modifying the original data.

Analyze the forensic image:

- Analyze the forensic image using various tools and techniques to identify any evidence related to the case.
- This may involve searching for specific file types, examining the registry for traces of user activity, or analyzing network traffic logs.

Document the findings:

- Document all findings, including the location of the evidence, its significance, and any potential challenges or limitations.
- This information may be used to support legal proceedings or to aid in further investigations.

Present the findings:

- Present the evidence and findings to the relevant parties, such as law enforcement, legal counsel, or other stakeholders.
- Ensuring that all findings are accurate and clearly documented is critical to effectively presenting evidence in court.

Q7. List procedures for storing digital evidence.

Ans.

Secure the Scene:

- Before any digital evidence can be collected, the scene must be secured so that no data is lost or tampered with.

Document the Scene:

- Take photographs, video, and notes to document the digital environment.
- The documentation should include every device and networked resource that could potentially be involved in the investigation.

Identify Digital Evidence:

- Identify all digital devices that may contain evidence.
- This includes computers, mobile devices, servers, and external storage media.

Collect Digital Evidence:

- Make a bit-for-bit copy of the digital evidence that is to be examined.
- This involves taking an image or copy of the entire hard drive or storage media.

Analyze Digital Evidence:

- Once the evidence has been copied, it can be analyzed using digital forensic tools to recover deleted files, locate hidden files, and find any remnants of deleted information.

Secure and preserve the Chain of Custody:

- Maintain proper documentation of the chain of custody for any digital evidence.
- This ensures that the evidence is admissible in a court of law.

Present Evidence in Court:

- Digital evidence must be presented properly in court with a detailed explanation of the procedures used for storage and analysis.

Retain Digital Evidence:

- Retain digital evidence for future reference and use in case of any appeals.
- It is important to have an established retention policy in place to determine how long digital evidence should be kept.

Q9. Explain the importance of reports.

Ans.

Reports play a crucial role in cyber forensics as they provide detailed documentation of the investigation process and findings, which are essential in both legal and non-legal settings. Below are the reasons why reports are important.

- Legal evidence:
    - Reports contain comprehensive details about the evidence collected and analyzed during the investigation process, which can be presented in court as legal evidence.
    - Reports provide an authoritative source of evidence for the prosecution to establish a strong case against the accused.
- Transparency:
    - Reports are a transparent record of the investigative procedure that can be used to show the investigative steps taken, analysis methodology used, and the accuracy and validity of the results obtained.
    - Additionally, it provides a trail that can be traced and audited in case an independent third party wants to review the findings.
- Decision-making:
    - In the absence of a proper report, it can be challenging to make an informed decision based on findings.
    - A report makes it easier for stakeholders to make informed decisions and provides a basis for recommendations and actions.
- Documentation:
    - Reports provide an official record of the cybercrime investigation, which is important for compliance purposes.
    - Documentation helps in analyzing the security breaches and identifying the root causes for future prevention.

- Knowledge sharing and collaboration:
    - Reports can be used to share knowledge and insights with colleagues, stakeholders, and security professionals.
    - This can help in professional growth, developing best practices, and enhancing collaboration among teams.
- Continuous improvement:
    - Reports document the investigation techniques, process, and outcome.
    - These insights can be used to identify areas of improvement, update policies, and improve training.
- Clarity of information:
    - Reports provide a clear, concise, and accurate picture of the investigation findings.
    - This helps in easy decision-making processes and reduces the chances of misunderstandings.
- Protection of data:
    - Reports are a protected document that ensures the data collected in the investigation process is confidential, secure, and not tampered with.
    - This is of utmost importance in cyber forensic investigations as data is integral for the investigation process.

Q11. Explain how to use forensics tools to generate reports.
Ans.

- Identification of relevant tools:
    - The first step in generating reports in cyber forensics is identifying the relevant tools that can extract the required information from digital devices or networks.
    - Forensic tools like FTK Imager, Autopsy, EnCase, Sleuth Kit, etc., can be used to extract digital evidence from various sources.
- Gathering digital evidence:
    - Once the tools are identified, the next step is to use them to gather digital evidence from the targeted devices or network.
    - The digital evidence includes artefacts like files, emails, chat logs, network traffic, system logs, etc.
- Analyzing the evidence:
    - Once the evidence is extracted, it needs to be analyzed to find patterns and identify potential culprits.
    - Analysis of the digital evidence involves using various forensic techniques like timeline analysis, keyword searching, data carving, hashing, etc.
- Creating reports:
    - After analyzing the evidence, the final step is to create a report based on the findings.
    - The report should be organized and structured, highlighting the key findings and outlining any anomalies.
    - It should be presented in a clear and concise manner so that it can be easily understood by non-technical stakeholders.
- Including chain of custody:
    - It's important to ensure that the chain of custody is maintained throughout the forensic investigation process.

    - The chain of custody is a record of the physical possession of evidence and any changes that have been made to it.
    - The chain of custody should be included in the report as evidence of the integrity of the digital evidence.
- Including screenshot:
    - Along with the detailed description of the findings, it is important to attach various screenshots to the report.
    - It provides clear evidence and detail about the identified artifacts, processes, and findings.
- Including proper time stamps:
    - In most cases, the digital evidence will have a creation or modified time stamp.
    - Including this in the report provides a detailed timeline of when and how certain events took place.
- Including recommendations:
    - Lastly, the report should include recommendations for remediation, prevention, and mitigation strategies.
    - These recommendations will help the stakeholders to take appropriate action against identified threats and aids in improving the security posture of the organization.

Q12. Explain guidelines for giving testimony as a technical/scientific or expert witness
Ans.
As a technical/scientific or expert witness in cyber forensics, one must follow certain guidelines while giving testimony in court.
These guidelines are:

- Provide an unbiased and impartial expert opinion:
    - The expert witness must ensure that the testimony provided is based on facts and evidence rather than personal beliefs or opinions.
- Maintain objectivity:
    - The expert witness must remain objective throughout the testimony and avoid taking sides or being influenced by the interests of the prosecution or defense.
- Clearly state the qualifications:
    - The expert witness must clearly state his/her qualifications, expertise, training, and experience in the field of cyber forensics.
- Clearly explain methodology:
    - The expert witness must explain the methodology used to analyze the evidence and arrive at conclusions.
- Use understandable language:
    - The expert witness must use language that is easily understandable to the jury and avoid technical jargon or confusing language.
- Avoid making assumptions:
    - The expert witness must avoid making assumptions or speculations and rely only on facts and evidence.
- Be prepared to defend the findings:
    - The expert witness must be prepared to defend his/her findings and opinions under cross-examination by the opposing counsel.

- Be truthful:
    - The expert witness must be truthful and accurate in their testimony, avoiding exaggerations or misrepresentations of the evidence or analysis.

New Question

Q1)Why is computer forensics imp?
Ans:
Computer forensic is collection, preservation, analysis and presentation of computer- related evidence. It determines the past actions that have taken place on a computer system using computer forensic techniques. Computer forensics is the process of methodically examining computer media (hard disks, diskettes, tapes, etc.) for evidence.

Why Is Computer Forensics Important?

1. A few criminals are becoming smarter. So data-hiding techniques include steganography. The evidence of criminal activity is placed in such a way where traditional search methods cannot find it.

- Encryption: Scrambling data, for example an e-mail message, so that it cannot be readable to the interceptor.

- Steganography: It is nothing but hiding a message into a larger file, typically in a photographic image or sound file.

2. Computer forensics isn't just about "detective work" - searching for and trying to find information. Computer forensics is also worried with:

- Sensitive data handling responsibly and confidentially.
- Taking precautions to not nullify findings by corrupting data.
- Taking precautions to make certain the integrity of the information.
- Staying within the regulation and guidelines of evidence.

Q 2) Explain computer forensics process steps
Ans:
Digital forensics is a branch of forensic science that focuses on digital devices and cybercrime. Through a process of identifying, preserving, analyzing and documenting digital evidence, forensic investigators recover and investigate information to aid in the conviction of criminals. Collection.
To Conduct Forensic Investigation there are four common steps to follow

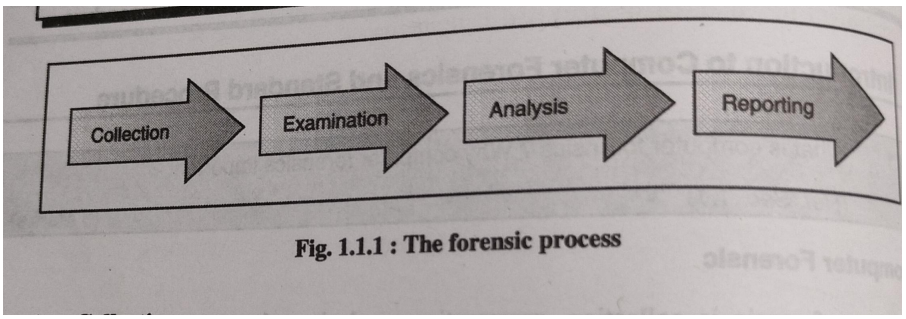


Fig. 1.1.1 : The forensic process

- Collection
  - This is the first phase in the forensic process.
  - In this phase data is identified, labeled and recorded and gathering the data and physical evidence related to the incident being invested is done. Simultaneously integrity of the chain of custody is also preserved.
- Examination
  - In this phase from the collected data identify and extract the pertinent information, using proper forensic tools and techniques and also maintain integrity of the evidence.

- Analysis
  - In this phase results of the examination phase are analyzed.
  - From the analysis useful answers to the questions are generated which are presented in the previous phases.
  - Most probably the case gets solved in this phase.
- Reporting
  - In the reporting phase the results of the analysis are done, which contains
  - The information pertinent to the case.
  - Actions that have been accomplished are left to be performed.
  - Moves left to be performed.
  - Advocated enhancements to processes and tools.
  -

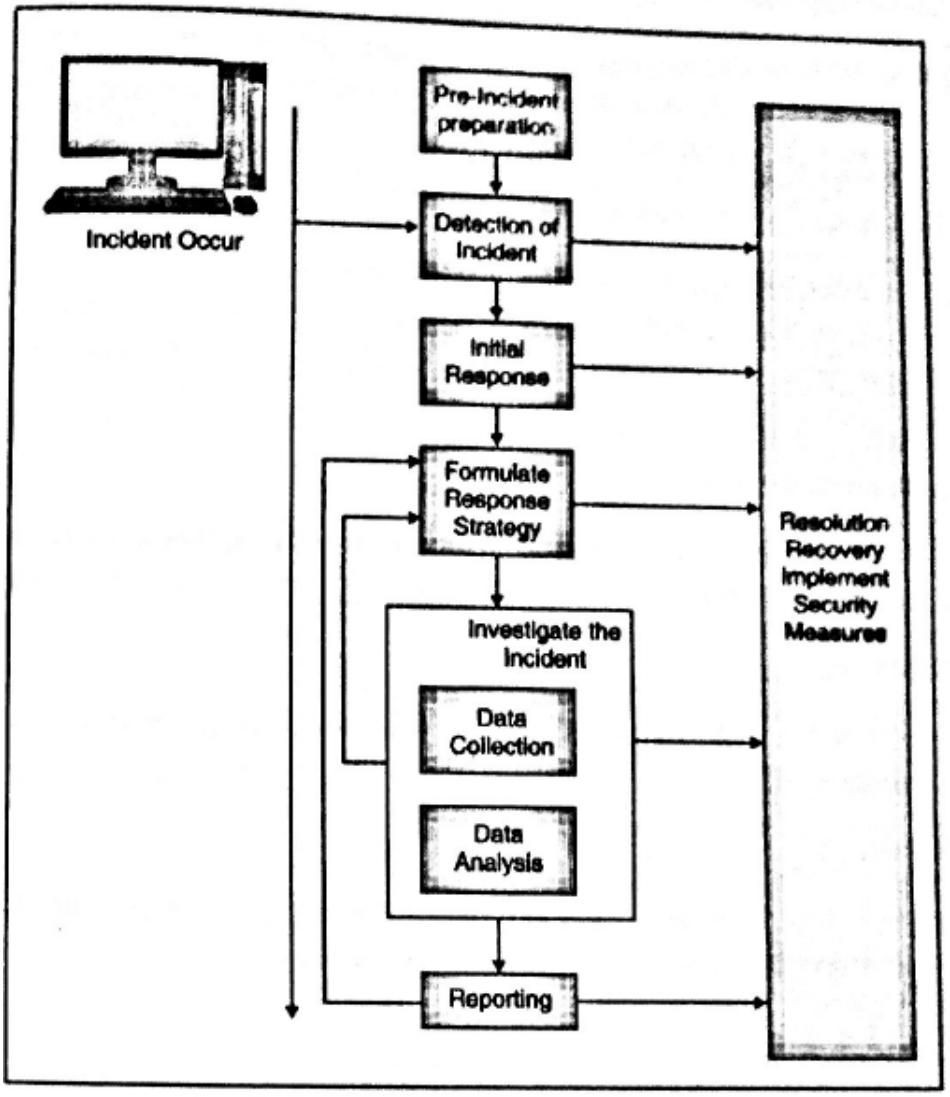
Q 3) What is the incident & goal of the incident?
Ans :
Computer security Incident is any unlawful, unauthorized, or unsuitable activity that includes a computer system or a computer network. Such an activity can incorporate any of the following events:
1. Theft of trade secrets.
2. Email spam or harassment.
3.Embezzlement
4. Unauthorized or unlawful intrusions into computing systems.
5. Denial-of-service (DoS) attacks.
6. Extortion.
7. Any unlawful action when the evidence of such action may be stored on computer media for example fraud, threats, and traditional crimes.
8. Possession or dissemination of child pornography.

Goals of Incident Response:

The goals of the Incident response are as follows:

1. To prevent a disconnected, no cohesive response.
2. Confirms or dispels whether an incident happened.
3. Promotes gathering of accurate information.
4. Establishes controls for proper retrieval and handling of evidence.
5. Protects privacy rights established by law and policy.
6. Minimizes damage to business and network operations.
7. Allows for criminal or civil action against culprits.
8. Provides accurate reports and useful recommendations.
9. Provides quick detection and containment.
10. Minimizes exposure and compromise of proprietary data.
11. Protects your organization's reputation and assets.
12. Educates senior management.
13. Promotes quick detection and/or prevention of such incidents in the future.

Q 4)Explain incidence response.
Ans :
Computer security incidents are often complicated,multifaceted troubles like complex engineering problem.Black box approach is used to solve the incident problem.In the approach divide the larger problem of incident resolution into components and less than input and output of each component.



In our methodology ,there are seven important components of incident response:

- Pre-incident preparation

  In this phase actions are taken to prepare the organization and the CSIRT before incidents occur.

- Detection of incidents

  In this phase potential computer security incidents are identified.

- Initial response

  In this phase an initial investigation is performed. The basic details surrounding the incident are recorded. The incident response team is assembled and individuals who need to know about the incident are notified.

- Formulate response strategy

  In this phase best response is determined and the management approval is taken based on the results of all the known facts. What types of civil, criminal,

administrative, or other actions are appropriate to take are determined, based on the conclusions obtained from the investigation. on

- . Investigate the incident

  In this phase thorough collection of data. To determine what happened, when it happened, who did it, and how it can be prevented in the future is reviewed from the collected data.

- Reporting

  In this phase information is accurately reported about the investigation in a manner useful to decision makers.

- Resolution

  In this phase security measures are employed. For any problem procedural changes record lessons learned, and develop long-term fixes are identified.

Q 5)What is disk imaging?
Ans:

- Disk Imaging makes a large compressed file of your drive. You can restore this data to drive. Image file is large in size and maximum people store it to external drives or file shares. The disk imaging software creates the exact copy of the hard disk. The forensic image consists of Deleted files, system files, slack space and executables.

- A disk imaging/ duplication is a file that contains every bit of information from the source, in a raw bit stream format. A 5GB hard drive would result in a 5GB forensic duplicate. No data is stored within the file, except in the case where errors occurred in a read

- extra operation from the original. When this occurs, a placeholder is put where the bad data would have been. A forensic duplicate may be compressed after the duplication process. The tools that create a forensic image are:

1. Unix dd command
2. dfeldd (U.S. Department of Defense (DoD) Computer Forensics Lab version of the dd command).
3. open-source Open Data Duplicator (ODD) e.g. FTK imager

1. Qualified Forensic Duplicate

-CA A qualified forensic duplicate is a file that contains every bit of information from the source, but may be stored in an altered or changed form. Two examples of altered paperwork are in-band hashes and Empty Quarter compression.

2.Restored Image

A restored image is what you get when you restore a forensic duplicate or a qualified forensic duplicate to another storage medium. The restoration process is more complicated than it sounds.

3.Mirror image

A mirror image is created from hardware that does a bit-by-bit copy from one hard drive to another. Hardware solutions are very fast, pushing the theoretical maximum data rate of the IDE or SCSI interfaces.

Q 6) How deleted files recover on windows sys
Ans :
Many times you want to clear the unallocated space on a restored forensic image in order to undelete or recover as many files or file fragments as possible. You also want to recover the evidence which was deleted by the attacker.

In this section, we are going to study different ways to obtain files, for all intents and purposes, suspects would believe they no longer exist. As you probably know, deleted files are not truly deleted, they are merely marked for deletion.

For example, when a file or directory is deleted from a FAT file system, the first letter of its filename is set to the sigma character (O), or, in hex, 0xES. This means that these files will remain intact until new data has overwritten the physical area where these deleted files are located on the hard drive.

Special tools can find these "intact" deleted files and recover them for review. After a file has been marked for deletion, each hard drive I/O could overwrite the data you want to

recover. To recover the file on windows system we use following tools:

1. Windows based tools: Encase, FTK

2 Linux tools: Fatback, TASK, and Foremost

1. Windows-Based Tools to Recover Files on FAT File Systems EnCase and FTK are the tools of the windows system for recovering files on FAT

filesystems. Both EnCase and FTK have this capability built-in, and they automatically recover any files they can.

2. Linux Tools to Recover Files on FAT File Systems

Three Linux utilities that can recover data: Fatback, TASK, and Foremost.

Q 7)Explain techniques used to recover crashed or damaged data.
Ans :

In computer forensics it is necessary to recover information that is erased, deleted and damaged. Users, companies/organizations, and government Agencies use data recovery for different reasons. Data recovery is an important part of Computer forensic.

Techniques used to recover erased or damaged data:

- Cyber forensics is the practice of collecting, analyzing, and preserving digital evidence in order to investigate cybercrime. One of the key challenges in cyber forensics is recovering crashed or damaged data, which can occur due to a variety of reasons such as hardware failure, software bugs, malicious attacks, or accidental deletion. In order to recover such data, cyber forensic experts employ a variety of techniques, some of which are outlined below:

- Disk Imaging: One of the first steps in data recovery is to create a bit-by-bit copy of the affected disk or storage device. This is known as disk imaging, and it ensures that the original data is not modified or overwritten during the recovery process. Once the disk image is created, various tools can be used to analyze and recover the data from the image.

- File Carving: File carving is a technique used to recover files that have been deleted or damaged beyond repair. This technique involves searching for specific patterns in the disk image and extracting any files that match those patterns. File carving can be a time-consuming process, but it can often recover files that would be otherwise lost.

- Data Recovery Software: There are a variety of data recovery software tools available that can help recover data from damaged or corrupted storage devices. These tools use various algorithms to analyze the disk image and identify recoverable data. Some examples of data recovery software include Recuva, EaseUS Data Recovery, and Stellar Data Recovery.

- Forensic Analysis: If the data recovery techniques described above fail to recover the necessary data, forensic analysis may be required. This involves a detailed examination of the disk image in order to identify any traces of the lost or damaged data. Forensic analysis can be time-consuming and requires specialized knowledge and tools.

- RAID Reconstruction: In cases where the damaged data is stored on a RAID system, RAID reconstruction may be necessary. This involves rebuilding the RAID array using the remaining disks and specialized software. Once the array is rebuilt, data recovery techniques can be used to recover any missing or damaged data.

Q 8)Different networks forensic tools.

Network forensics is capture, recording and analysis of network packets in order to determine the source of network security attacks. The major goal of network forensics is to collect evidence. It tries to analyze network traffic data, which is collected from different sites and different network equipment, such as firewalls and IDS. In addition, it monitors on the

network to detect attacks and analyze the nature of attackers. Network forensics is also the process of detecting intrusion patterns, focusing on attacker activity.

NIKSUN

NIKSUN NetDetector is a full-featured appliance for network security monitoring built on NIKSUN'S award-winning NikOS architecture. It is the only security monitoring appliance that integrates signature-based IDS functionality with statistical anomaly detection, analytics and deep forensics with full-application reconstruction and packet level decodes. Recognized as the industry's best security monitoring and forensics appliance to safeguard against increasingly sophisticated cyber-attacks.

NETSCOUT

Netscout Arbor Spectrum addresses these challenges by serving as a force multiplier for the security team, regardless of their size and expertise levels. Not only does it provide unprecedented visibility into network activity and quickly surface high-priority issues, it enables security teams to detect and investigate incidents in a far more efficient and complete fashion.

LOGRYTHM

LogRhythm Network Monitor When attackers compromise the perimeter or are operating from within, you need to know. Evidence of intruders and insider threats lies within network communications. Detect network-based threats with real-time network monitoring and big data analytics

SAVVIUS

Savvius vigil automates the collection of network traffic needed for security investigations, both reducing the likelihood of a breach, minimizing their impact. Even breaches not discovered for months can be effectively investigated using Vigil. Savvius Vigil, which integrates with all leading IDS/IPS systems, includes Omnipeek, award-winning network forensics software.

PACKETSLED

PacketSled automates incident response by fusing business context, AI, entity enrichment and detection with network visibility. Used for real-time analysis and response, PacketSled's platform leverages continuous stream monitoring and retrospection to provide network forensics and security analytics

Q 9)Concept of live acquisition

Ans :

Live acquisitions are mainly useful when you are dealing with active network attacks or

intrusions or you have doubt that employees are accessing network areas that they should not have to access. Live acquisitions is performed before the system go offline and it has also become

necessity as attack may left footprint or evidence only in running processes or RAM; for

For instance, there is some malware which disappears when the system is restarted. The information in RAM gets lost when the suspect's system is turned off. After the live acquisition, there is change in the information on the system

Information because your actions have affected the RAM and the running processes, so, the information cannot be produced again. As a result, live acquisitions don't follow typical forensics procedures.

The following is the general procedure given for live acquisition, the steps are:

1. Create/download a bootable forensic CD, before using it on the suspected drive.

If the suspected system is on your network and you can access it remotely, add the

suitable forensic tools to your computer. Otherwise insert the bootable forensics CD in the suspected system.

2. Ensure that you are keeping the log of all of your actions. Documenting the actions and reasons for these actions is important.

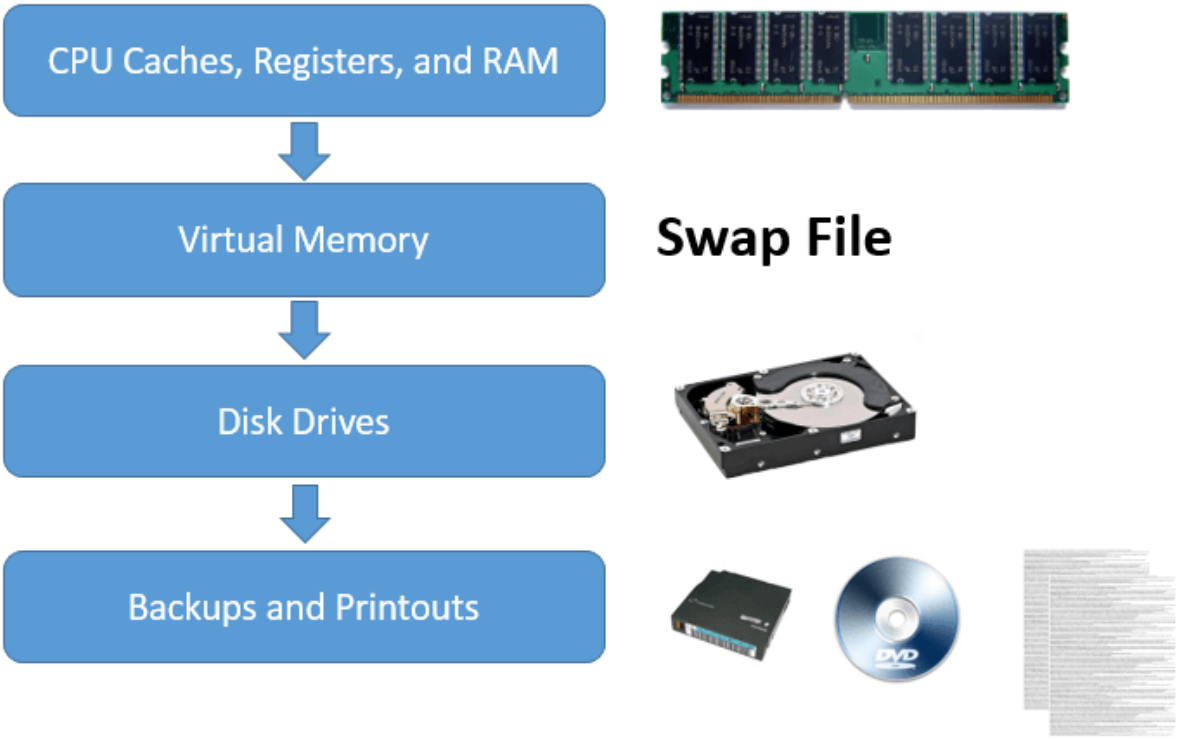
3. A network drive is perfect as a place to send the data you gather. In the event that you don't have one accessible, interface a USB thumb drive to the suspect system for gathering information. Ensure that you have noted this step in your log.

4. Now copy the physical memory (RAM).

5. The next step depends on the incident you are investigating. For example, if you want to shut down the system and make the static acquisition later, you want to know whether a rootkit is present by using a tool such as RootKit Revealer; You may also want to access the firmware to check if it is changed or not.
6. Be confident that you will get the forensically sound digital hash value of all files you have recovered in the live acquisition to ensure that they are not modified later

Q 10)Order of volatility.
Ans:

- In forensics, order of volatility refers to the order in which you should collect evidence.
- Highly volatile data is easily lost, such as data in memory when you turn off a computer.
- Less volatile data, such as printouts, is relatively permanent and the least volatile.



- According to the Internet Engineering Task Force (IETF), the Order of Volatility is as follows:
    - Registers, Cache
        - The contents of CPU cache and registers are extremely volatile, since they are changing all of the time.
        - Literally, nanoseconds make the difference here.
        - An examiner needs to get to the cache and register immediately and extract that evidence before it is lost.
    - Routing Table, ARP Cache, Process Table, Kernel Statistics, Memory
        - Some of these items, like the routing table and the process table, have data located on network devices.
        - In other words, that data can change quickly while the system is in operation, so evidence must be gathered quickly.
        - Also, kernel statistics are moving back and forth between cache and main memory, which make them highly volatile
        - Finally, the information located on random access memory (RAM) can be lost if there is a power spike or if power goes out, Clearly, that information must be obtained quickly.
    - Temporary File Systems
        - Even though the contents of temporary file systems have the potential to become an important part of future legal proceedings, the volatility concern is not as high here.
        - Temporary file systems usually stick around for awhile.\
    - Disk
        - Even though we think that the data we place on a disk will be around forever, that is not always the case.
        - However, the likelihood that data on a disk cannot be extracted is very low.

- Remote Logging and Monitoring Data that is Relevant to the System in Question
  - The potential for remote logging and monitoring data to change is much higher than data on a hard drive, but the information is not as vital.
  - So, even though the volatility of the data is higher here, we still want that hard drive data first.
- Physical Configuration, Network Topology, and Archival Media
  - Here we have items that are either not that vital in terms of the data or are not at all volatile.
  - The physical configuration and network topology is information that could help an investigation, but is likely not going to have a tremendous impact.
  - Finally, archived data is usually going to be located on a DVD or tape, so it isn't going anywhere anytime soon. It is great digital evidence to gather, but it is not volatile.

Q 11)Standard procedure used in network forensics.
Ans :
Network forensics is a long and tiresome process. A standard procedure is used in network forensics is as follows:

1. Every time use the standard installation image for systems on a network. This image is not a bit-stream image but an image containing all the standard applications used. For all the applications and OS files you should have the MD5 and SHA-1 hash values.

2.In case, an intrusion incident occurs, ensure the vulnerability has been fixed to avoid other attacks from taking advantage of the opening.

3. Try to recover all the volatile data by performing the live acquisition before the system turns off, for example, RAM and running processes.
4. Acquire and make the forensic image of the compromised drive.

5. Perform the comparison between files on a forensic image and the original installation image. Also compare the common files hash values, such as Win.exe and standard DLLS, and find out whether they have been altered..

Q 12)Digital network for mobile phones

Q 13)STM card -Explain

Q 14)Explain Mobile forensics.

Q 15) Explain Internet forensis

Q 16) Explain pre intrusion attack / activities.

Q 17)Explain password tracking techniques.

Q 18) Explain Trojan, Virus, Worms.

Q 20)Explain internet forensics

Q 21) Explain mail forensics

Q 22)Steps involved in e-mail analysis

Q 23) Explain Can spam act.

The CAN-SPAM Act, a law that sets the rules for commercial email, establishes requirements for commercial messages, gives recipients the right to have you stop emailing them, and spells out tough penalties for violations.

Despite its name, the CAN-SPAM Act doesn't make a difference just to mass email. It covers every single business message, which the law characterizes as "any electronic mail message the basic role of which is the business ad or advancement of a business item or administration," including email that advances content on business sites.

- The law makes no special case for business-to-business email. That implies all email - for instance, a message to previous clients declaring another product offering - must obey the rules to the law.

Q 24) Explain browser forensics

Q 25)Cookie storage and analysis.

Q 26)What is evidence? & different types of evidence

The evidence is any information of supporting value, that means which proves something or helps to prove something relevant to the case.

The digital evidence consists of the data on a computer, images audio and video files. It is a data and information of value to an investigation that is stored on an electronic device,

received or transmitted by an electronic machine.

You can acquire the evidence when data or electronic machines are seized /in custody and secured for the examination. Examples of evidence are a fingerprint, DNA, files on system etc.

The problems in acquiring digital evidence are

(a) Digital Evidences can be easily modified, damaged or destroyed.

(b) Digital Evidences are time sensitive

The types of evidence are

Real evidence:

Real evidence are something that one can carry into a courtroom and show it in front of the jury. Real evidence is the most powerful evidence. This evidence typically "speaks for itself."

2. Documentary evidence:

The evidence which is in the written form is nothing but the documentary evidence. For example server logs, email, database document etc. Documentary evidence might be faked via a professional pc user and therefore must be authenticated to be admissible in a courtroom. Continually produce the original document, do not use the copy.

3.Testimonial evidence
Testimonial evidence is nothing but the statement of a witness, underneath oath
either in court or by deposition. This sort of evidence normally helps or validates alternative types.

4. Demonstrative evidence:

Demonstrative evidence recreates or explains the different evidence. Demonstrative evidence does not "talk for itself" and is used to demonstrate and make clear previous points. This sort of evidence is maximum helpful in explaining technical topics to non-technical audiences.

Q 27)Steps in preparing for evidence search