University Exam Paper Solution

Academic Year:

Year: -

Semester: -

Subject: -

Date of Exam: -

Name of Subject In charge: -

Signature of Subject In charge: -

_____
_____
_____

Head of the Department

Q. 1.

A) Explain Mobile forensics. What are various challenges in Mobile forensics.

ANS :

- **Mobile Forensics :**

➢ Mobile forensics is a branch of digital forensics related to the recovery of digital evidence from mobile devices.

➢ The mobile forensics process is broken into three main categories: seizure, acquisition, and examination/analysis.

➢ Forensic examiners face some challenges while seizing the mobile device as a source of evidence. At the crime scene, if the mobile device is found switched off, the examiner should place the device in a faraday bag to prevent changes should the device automatically power on.

➢ Faraday bags are specifically designed to isolate the phone from the network. If the phone is found switched on, switching it off has a lot of concerns attached to it. If the phone is locked by a PIN or password or encrypted, the examiner will be required to bypass the lock or determine the PIN to access the device.

➢ Mobile phones are dynamic systems that present a lot of challenges to the examiner in extracting and analysing digital evidence.

➢ The rapid increase in the number of different kinds of mobile phones from different manufacturers makes it difficult to develop a single process or tool to examine all types of devices.

➢ Mobile phones are continuously evolving as existing technologies progress and new technologies are introduced. Furthermore, each mobile is designed with a variety of embedded operating systems. Hence, special knowledge and skills are required from forensic experts to acquire and analyze the devices.

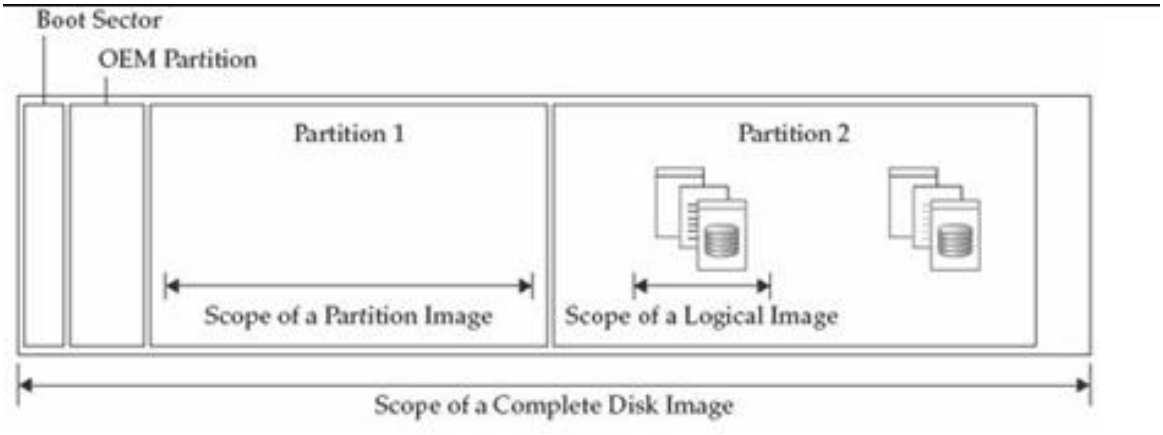
- **Challenges In Mobile Forensics :**
  - ➢ One of the biggest forensic challenges when it comes to the mobile platform is the fact that data can be accessed, stored, and synchronized across multiple devices.
  - ➢ As the data is volatile and can be quickly transformed or deleted remotely, more effort is required for the preservation of this data.

- Mobile forensics is different from computer forensics and presents unique challenges to forensic examiners which are :
    - Hardware Differences
    - Mobile OS
    - Mobile platform security features
    - Lack of resources
    - Generic state of the device
    - Anti forensic techniques
    - Dynamic nature of evidence
    - Accidental reset
    - Device ultration
    - Passcode recovery
    - Communication SHIELDING
    - Lack of availability tolls
    - Malicious programs on device
    - Legal issues

B) Explain forensic duplicate as Admissible Evidence

Ans:

- A duplicate is an accurate digital reproduction of all data objects contained on the original physical item and associated media. forensic duplication as an image of every accessible bit from the source medium.
- Also it is an accurate copy of data that is created with the goal of being admissible as evidence in legal proceedings.
- We can perform duplication with methods that are generally accepted in the forensic community in various image formats like :
    - Complete image,
    - Partition image ang
    - logical imgae.



- Every image has its purpose, and the investigation team ought to perceive when to use one image instead of the other. Most significantly, the team has to perceive the implications of that alternative.
- Though the whole disk image has the most desirable format as a result of its foremost comprehensive and captures the contents of the storage medium during a static state, technology, business priorities, availableness, and advantage may demand a special method.

C) What is evidence handling procedure?

Ans :

- **Evidence:**
- We can define evidence as any information of probative value, meaning it proves something or helps prove something relevant to the case. It is safest to treat any information of probative value that you obtain during an investigation as evidence
- **Evidence Handling Procedure:**
- When handling evidence during an investigation, you will generally adhere to the following procedures:

1.If examining the contents of a hard drive currently placed within a computer, record information about the computer system under examination.

2.Take digital photographs of the original system and/or media that is being duplicated.

3.Fill out an evidence tag for the original media or for the forensic duplication (whichever hard drive you will keep as best evidence and store in your evidence safe).

4.Label all media appropriately with an evidence label.

5.Store the best evidence copy of the evidence media in your evidence safe.

6.An evidence custodian enters a record of the best evidence into the evidence log. For each piece of best evidence, there will be a corresponding entry in the evidence log.

7.All examinations are performed on a forensic copy of the best evidence, called a working copy.

8.An evidence custodian ensures that backup copies of the best evidence are created. The evidence custodian will create tape backups once the principal investigator for the case states that the data will no longer be needed in an expeditious manner.

9.An evidence custodian ensures that all disposition dates are met. The dates of evidence disposition are assigned by the principal investigator.

10.An evidence custodian performs a monthly audit to ensure all of the best evidence is present, properly stored, and labeled.

D) What are the challenges in network forensics?

Ans :

- The Challenges faced in evidence handling must he properly understood by all investigators.
- Investigates should also understand how to meet these challenges.
- Therefore, it is essential for every organization to have formal evidence handling procedures that supports computer security investigation.
- The most difficult task for an evidence handler is to authenticate the collected evidence at the judicial proceeding. Maintaining thechain of custedy is also necessary. You must have both power and skill to validate your evidence.

  1. Authentication of Evidence :

  • The laws of many state jurisdictions define data as written-work and "record-keeping". Before introducingthem as evidence, documents and recorded material must be authenticated.

  • The evidences that are collected by any person/investigator should be collected using authenticate methods and techniques because during court proceedings these will become major evidence to prove the crime.

  • In other words, for providing a piece of evidence of the testimony, it is necessary to have an authenticated evidence by a spectator whe has a personal knowledge to its origin.

  • For an evidence to be admissible, it is necessary that it should be authenticated, otherwise the information cannot be presented to the judging body.

  • The matter of record is that the evidence collected by any peson should meet the demand of authentication.

  • The evidences collected must have some sort of internal documentation that records the

manner of collected information.

2. Chain of Custody :

• Maintaining the chain of custody means that the evidences collected should not be accessed by any unauthorized individual and must be stored in a tamper-proof manner.

• For each item obtained, there must be a complete chain of custody record.

• Chain of custody is nothing but the requirement that you may be able to trace the location of evidence from the moment i was collected to the moment it was presented in a judicial proceeding.

• To meet the requirements of chain of custody (as shown in fig), evidences are stored in a secure place by police departments and federal law enforcement agencies, which have a property departments.

• As per the experts and law enforcement officers, evidences are "checked-out" whenever they need to be reviewed and "checked-in" whenever they are returned back to storage.

• The challenge of chain of custody requirements in any organization is maintaining positive control (the evidence which you owned or have must be kept in your sight at all times) of all the collected best evidence until the evidences are carried or shipped to evidence custodians for proper storage.

• As evidences should not be accessible to anyone other than the appointed evidence custodian, the best evidence of your organization must be stored within a safe or storage room. "Evidence safe" is nothing but the storage area.

• The evidence custodians must control all the access to the evidence safe.

• Whenever team member wants to use or perform an experiment on evidance which is under custodian, the team members has to maintain the recipt of the evidence.

3. Evidence Validation :

• The challenge is to ensure that providing or obtaining the data that you have collected is similar to the data provided or presented in the court.

• Several years pass between the collection of evidence and the production of evidence at a judiciary proceeding, which is very common.

• To meet the challenge of validation, it is necesary to ensure that the original media matches the forensic duplication by using MD5 hashes.

• The evidence for every file is nothing but the MD5 hash values that are generated for every file that contributes to the case.

• Many tools like Encase are used in routine life for evidence validation. The verify function within the Encase application can be used while duplicating a hard drive with

Encase.

• To perform a forensic duplication using dd, you must record a MD5 hash for both the original evidence media and binary files or the files which compose the forensic duplication.

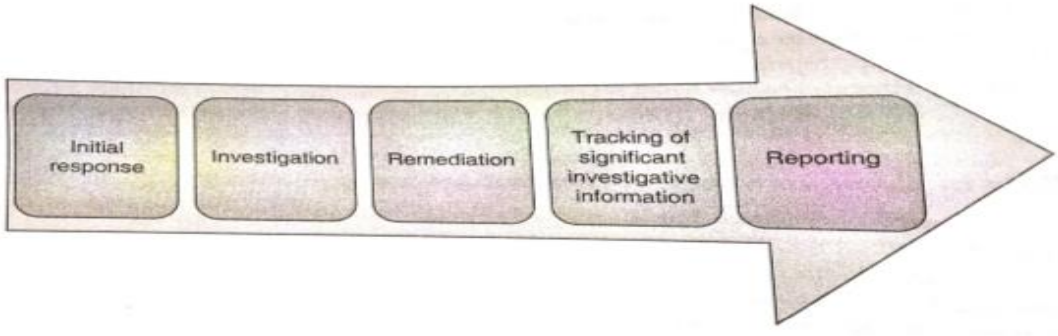
• Care should be taken that Evidence collection calculated by MD5 after 6 months may not be helpful. MD5 hashes should be performed when the evidence is obtained.

Q. 2 A) Explain Incident Response Process and its Methodology.

Ans :

- **Incident Response :**
  - Incident response is a term used to describe the process by which an organization handles a data breach or cyberattack, including the way the organization attempts to manage the consequences of the attack or breach (the "incident").
  - Ultimately, the goal is to effectively manage the incident so that the damage is limited and both recovery time and costs, as well as collateral damage such as brand reputation, are kept at a minimum.
- **IR Process :**
  - The basic incident process is composed with 5 phases :

    1. Initial Response
    2. Investigation
    3. Remediation
    4. Trcking of investigative Information
    5. Reporting



1. **Initial Response :**
   - Initial response includes the activities that respond to an incident like policies, tools, procedures, effective governance and communication plans.

- It also implies that the affected groups have instituted the control necessary to recover and continue operations after an incident is discovered.
- The main objective in this step include assembling the response team, reviewing network-based and other readily available data, determining the type of incident, and assessing the potential impact.
- The goal is to gather enough initial infortion to allow the team to determine the appropriate response.
- The team develops the formal incident response capability, where they create an incident response process defining the organizational structure with roles and responsibilities; where they create procedures with detailed guidance in order to respond to an incident; where they select the right people with the appropriate skill set; where they define the criteria to declare an incident; where they define the right tools to handle an incident; where the team defines what they are going to report; and to whom is the team going to communicate.
- This step is crucial to ensure response actions are known and coordinated. Good preparation will help them to limit the potential damage by ensuring quick and effective response actions.

2. Investigation :

- Investigation is the phase where team personnel determine the priority, scope, and root cause of the incident.
- This step is where the team verilfies if an occasion has occurred, supported events observation, indicators and search for deviations from traditional operations and for malicious acts or tries to and do damage.
- The protection mechanism in place can facilitate the team doing the identification.
- Incident handler team will use their experience to look at the signs and indicators.
- The observations might occure at network, host or at system level. It is where the team leverages the alerts and logs from routers, firewalls, IDS,Gateways and more.

3. Remidiation :

- It is the post incident repair of affected systems, communication and instructions to affected parties and analysis that confirms the threat has been contained.
- The determination of whether there are regulatory requirements for reporting the incident will be made at this stage.

- Apart from any formal reports, the post-mortem will be completed at this stage as it may impact the remidiation and interpretation of the incident.

4. Tracking investigative information :

- Usually We have found a handful of data points that are critical to any investigation. These items must be tracked as close to real time as possible, because team members will use them as the "ground truth" when it comes to the current status of the investigation.
- This data will also be the first thing that team members will reference when queries come in from management. The information may be :

  1. List of evidence collected: This should include the date and time of the collection and the source the data, whether it be an actual person or a server. Ensure that a chain of custody is maintained for each item. Keep the chain of custody with the item, and its presence in this list is an indicator to you that an item has been handled properly.

  2. List of affected systems: Track how and when the system was identified. Here "affected" includes systems that are suspected of a security compromise as well as those simply accessed by a suspicious account.

  3. List of any files of interest: This list usually contains only malicious software, but it may also contain data files or captured command output. Track the system the file was found on as well as the file system metadata.

  4. List of accessed and stolen data: This includes file names, content, and the date of suspected exposure.

  5. List of significant attacker activity: During examinations of live response or forensic data, we may discover significant activities, such as logins and malware execution. It Include the system affected and the date and time of the event.

  6. List of network-based IOCs: Track relevant IP addresses and domain names.

  7. List of host-based IOCs: Track any characteristic necessary to form a well-defined indicators.

  8. List of compromised accounts: Ensure you track the scope of the account's access, local or domain wide.

4. Reporting :

- All incident response activities will be documented to include artifacts obtained using methods consistent with chain of custody and confidentiality requirements.

- Incidents will be prioritized and ranked according to their potential to disclose restricted data. As an investigation progresses, that ranking may change, resulting in a greater or lesser prioritization of resources.
- Incidents will be reviewed post-mortem to assess whether the investigational process was successful and effective.
- Subsequent adjustments may be made to methods and procedures and by other participants to improve the incident response process.

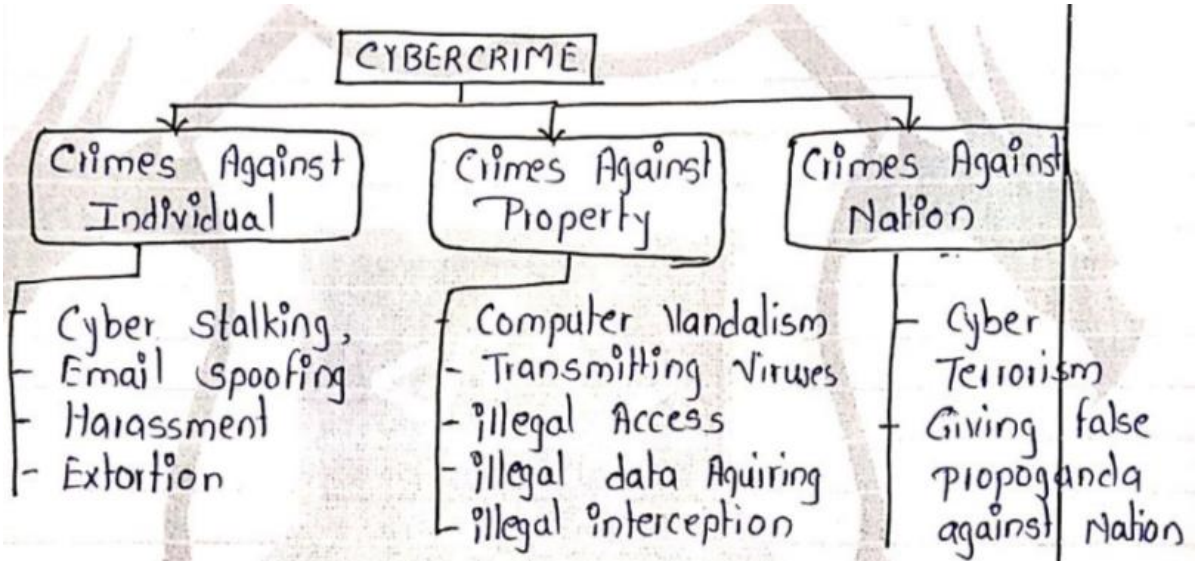
Q. 2 B) Compare active attacks vs Passive attacks. Classify the cybercrime and explain any one briefly.

Ans:

- **Active Attack Vs Passive Attack :**

Key	Active Attack	Passive Attack
Modification	In Active Attack, information is modified.	In Passive Attack, information remain unchanged.
Dangerous For	Active Attack is dangerous for Integrity as well as Availability.	Passive Attack is dangerous for Confidentiality.
Attention	Attention is to be paid on detection.	Attention is to be paid on prevention.
Impact on System	An Active Attack can damage the system.	A Passive Attack does not have any impact on the regular functioning of a system.
Victim	The victim gets informed in an active attack.	The victim does not get informed in a passive attack.
System Resources	System Resources can be changed in active attack.	System Resources are not changed in passive attack.

- **Classification of Cybercrime :**


CYBERCRIME
Crimes Against Individual
Crimes Against Property
Crimes Against Nation
Cyber Stalking,
Email Spoofing
Harassment
Extortion
Computer Vandalism
Transmitting Viruses
Illegal Access
Illegal data Aquiring
Illegal interception
Cyber Terrorism
Giving false propoganda against Nation

I CYBERCRIME AGAINST INDIVIDUAL :

↳ Crimes exclusively committed against persons include crimes such as spreading of child pornography, harassment of people by using a computer, cyber stalking, internet grooming, extortion, facebook stalking, credit card fraud etc.

↳ Basicaly the crimes which are harmful to an individual or human being are fall under this category.

↳ Some forms of cybercrimes may victimize individuals over internet, called as 'Cyber Nuisance'.

* Examples :

1) INTERNET GROOMING :

↳ Process of befriending children to perpetrate sexual crimes, abuse, or exploitation over the internet
- Groomers persuade young children to send sexually explicit images or have abuse conversations online.

2) CYBER STALKING :

↳ Refers to a crime that relies upon electronic communication for sending a fake, threatning emils / messages to follow & harras the victim.
- Cyber stalking occurs in many forms such as - harassing, embarrassing, humiliating, isolating or frightening the victim by following him/her online.
- It can happen via email (called email stalking), chat rooms & discussion forums
- Usually people who are not aware about rules of internet safety & inexperianced web users are prone to this attack.
- In Internet stalking, victim is harassed via internet by sending obscene content or a virus repeatedly through an email.
- Hence, Computer stalking is usage of computer skills to gain an unauthorized access to victim's computer & provide harmful actions towards victim.

Q. 3 A) Discuss basic security precautions to be taken to safeguard Laptops and wireless devices and what are the devices related to security issues?

Ans:

- **precautions to be taken to safeguard Laptops and wireless devices :**

1.Use a password :

An account password is an effective first line of defence, but only if you avoid choosing a commonly used - and therefore easily guessed - password. An analysis of passwords stolen from websites during recent security incidents reveals that the most common include "password", "123456", "abc123", "qwerty" and, bizarrely, "monkey".

2.Disable booting from CD or USB

It's easy to change or remove an account password using a free resetting program such as pogostick, or to guess a short one using a "bruteforce guessing" program such as Ophcrack.

But running these involves booting the computer from a CD or USB stick, so you can increase security by disabling the ability to boot from one of these devices. This can be done by altering the settings in your laptop's basic input/output system (BIOS) – the built-in software with generic code to control the machine – which can usually be accessed by pressing F1, F4, F10 or Del just after you switch it on.

To ensure that no-one can override these settings, password-protect the BIOS so that no more changes can be made to it without entering the password. This can also be configured in the BIOS settings.

3.Encrypt your hard drive

If your laptop is stolen from your car or hotel room there is usually nothing to stop the thief from removing your hard drive and attaching it to another computer. Doing this bypasses any account password protection and allows them to access your data easily.

The best way to prevent this is to encrypt your laptop's hard drives. Encrypted drives can only be accessed after the encryption key is supplied - usually in the form of a PIN, a password or by inserting a USB stick containing the key.

You can encrypt an entire drive using BitLocker, an encryption utility included with some versions of Windows Vista, Windows 7 and Windows 8. A free, open source alternative is TrueCrypt, which also works with Windows XP, Linux and OS X.

4.Use a virtual private network (VPN)

Publicly accessible networks, such as those offered in airports, conference centres and hotel rooms, present a particular security risk to laptop users. This is because hackers armed with free programs such as Cain and Abel, Wireshark or Ettercap can connect to the same networks and eavesdrop on emails or copy passwords as they pass over the network.

The best way to protect your data from interception by other network users is to encrypt it while it is in transit between your computer and your office network, using a company VPN.

If you don't have access to a company VPN, you can use one from service provider such as StreamVia or StrongVPN. This ensures your data is encrypted and protected from other users of the public local network.

5.Use secure email

Sometimes it can prove difficult to get a VPN connection working, so it's prudent to ensure that any email program, webmail system or cloud based email service that you use is configured to use a secure sockets layer (SSL) or transport layer security (TLS). This ensures that both your username and password, and the contents of your emails, are encrypted as they travel across the internet.

Webmail services like Gmail and cloud based services like Microsoft's Office 365 are configured in this way by default, but email offered by many internet service providers is not.

Q. 3 B) Explain Volatile Data Collection from Windows System.

Ans :

- Volatile data is the data that is usually stored in cache memory or RAM. This volatile data is not permanent this is temporary and this data can be lost if the power is lost i.e., when computer looses its connection.
- During any cyber crime attack, investigation process is held in this process data collection plays an important role but if the data is volatile then such type of data should be collected immediately.
- Volatile information can be collected remotely or onsite. If there are many number of systems to be collected then remotely is preferred rather than onsite.
- It is very important for the forensic investigation that immediate state of the computer is recorded so that the data does not lost as the volatile data will be lost quickly.
- If the volatile data is lost on the suspects computer if the power is shut down, Volatile information is not crucial but it leads to the investigation for the future purpose.
- To avoid this problem of storing volatile data on a computer we need to charge continuously so that the data isn’t lost. So that computer doesn’t loose data and forensic expert can check this data sometimes cache contains Web mail.
- This volatile data may contain crucial information.so this data is to be collected as soon as possible. This process is known “Live Forensics”.
- This may include several steps they are:

- Initially create response tool kit.
- Storing in this information which is obtained during initial response.
- Then obtain volatile data
- Then after that performing in in-depth live response.

CREATING A RESPONSE TOOLKIT :

◦ For an initial response, we need to plan your approach to obtain all the information without affecting any potential evidence. Because we will be issuing commands with administrator rights on the victim system, we need to be particularly careful not to de-stroy or alter the evidence.

◦ The best way to meet this goal is to prepare a complete response toolkit. Testing a toolkit for the first time in live investigation will be the biggest risk in the process of investigation.

◦ Hence before investigation the incident, the investigator tean used to preapare a response toolkit. Which is done by foolowing steps :

◦ Collecting the tools:

▪ In all incident responses, regardless of the type of incident, it is critical to use trusted

▪ commands. For responding to Windows, we maintain a CD or two floppy disks that contain a minimum of the tools mentioned below :

• cmd.exe : the command prompt for windows system

• PsLoggedOn: shows ll the users connected locallyy & remotely

• netstat: enumerates all listening ports and all current connections to those ports.

• Fport: shows all the processes that are open on TCP/IP ports.

• PS List : list out all running processes on target.

• Kill : A command that terminates a process

• arp : A system tool that shows the MAC addresses of systems that the target system has been communicating with, within the last minute.

- At a minimum, the following volatile data is collected prior to forensic duplication:
  - System date and time
  - A list of the users who are currently logged on
  - Time/date stamps for the entire file system
  - A list of currently running processes
  - A list of currently open sockets
  - The applications listening on open sockets
  - A list of the systems that have current or had recent connections to the system

Q. 4 A) What do you understand by social engineering? Give Classification.

Ans :

- **Social engineering** is a manipulation technique that exploits human error to obtain private information or valuable data. In cybercrime, the human hacking scams entice unsuspecting users **to disclose data, spread malware infections**, or give them access to **restricted systems**. Attacks can occur **online, in-person**, and by other interactions. **Social engineering** scams are based on how people think and act.
- Hackers try to exploit the user's knowledge. Thanks to technology's speed, many consumers and employees are not aware of specific threats such as drive-by downloads. Users cannot realize the value of personal data like **phone number**. Many users are unsure of how best to protect themselves and theirconfidential information.Social engineering attackers have two goals:
    - **Subversion: Interrupting** or **corrupting** data due to loss or inconvenience.
    - **Theft**: Obtaining valuable items such as **information, access**
- Every type of cybersecurity attack involves some social engineering. **For example**, **classic email** and **virus scams** are laden with social overtones
- Classification of social engineering :

A. Human-Based Social Engineering

- Human-based social engineering refers to person-to-person interaction to get the required/desired information. An example is calling the help desk and trying to find out a password.
- **1. Impersonating an employee or valid user:** "Impersonation" (e.g. posing oneself as an employee of the same organization) is perhaps the greatest technique used by social engineers to deceive people. Social engineers "take advantage" of the fact that most people are basically helpful, so it seems harmless to tell someone who appears to be lost where the computer room is located, or to let someone into the building who "forgot" his/her badge, etc, or pretending to be an employee or valid user on the system.
- **2. Posing as an important user:** The attacker pretends to be an important user - for example, a Chief Executive Officer (CEO) or high-level manager who needs immediate assistance to gain access to a system. The attacker uses intimidation so that a lower-level employee such as a help-desk worker will him/her in gaining access to the system. Most of the low-level employees will not ask any question to someone who appears to be in a position of authority.

- **3. Using a third person:** An attacker pretends to have permission from an authorized source to use a system. This trick is useful when the supposed authorized personnel is on vacation or cannot be contacted for verification.
- **4. Calling technical support:** Calling the technical support for assistance is a classic social engineering example. Help-desk and technical support personnel are trained to help users, which makes them good prey for social engineering attacks.
- **5. Shoulder surfing:** It is a technique of gathering information such as usernames and passwords by watching over a person's shoulder while he/she logs into the system, thereby helping an attacker to gain access to the system.
- **6. Dumpster diving:** It involves looking in the trash for information written on pieces of paper or computer printouts.

- **B. Computer-Based Social Engineering**
- Computer-based social engineering refers to an attempt, made to get the required/desired information by using computer software/Internet. For example, sending. a fake E-Mail to the user and asking him/her to re-enter a password in a web-page to confirm it.
- **1. Fake E-Mails:** The attacker sends fake E-Mails to numerous users in such that the user finds it as a legitimate mail. This activity is also called "Phishing". It is an attempt to entice the Internet users (netizens) to reveal their sensitive personal information, such as user-names, passwords and credit card details by impersonating as a trustworthy and legitimate organization and/or an individual. Banks, financial institutes and payment gateways are the common targets. Phishing is typically carried out through E-Mails or instant messaging and often directs users to enter details at a website, usually designed by the attacker with abiding the look and feel of the original website. Thus,Phishing is also an example of social engineering techniques used to fool netizens. The term "Phishing" has been evolved from the analogy that Internet scammers are using E-Mails lures to fish "Phishing" and financial data from the sea of Internet users (i.e., netizens).
- **2. E-Mail attachments:** E-Mail attachments are used to send malicious code to a victim's system, which will automatically (e.g., keylogger utility to capture passwords) get executed. Viruses, Trojans, and worms can be included cleverly into the attachments to entice a victim to open the attachment.

- **3. Pop-up windows**: Pop-up windows are also used, in a similar manner to E-Mail attachments. Pop-up windows with special offers or free stuff can encourage a unintentionally install malicious software.

Q. 4 B) Briefly explain types of digital evidence with example.

Ans :

- **Definition :**
  - *Digital evidence is any information or data of value to an investigation that is stored on, received by, or transmitted by an electronic device.* Text messages, emails, pictures and videos, and internet searches are some of the most common types of digital evidence.
  - Evidence can also be stated as any information that can be confident or trusted and can prove something related to a case in trial, that is, indicating that a certain substance or condition is present.
- **Types :**
  - There are many types of evidence, each with their specific or unique characteristics. Some of the major types of evidence are as follows :
    - Illustrative Evidence
    - Electronic evidence
    - Documented evidence
    - Explainable Evidence
    - Substantial Evidence
    - Testimonial

1. **Illustrative Evidence:**
   - Ilustrative evidence is also called as demonstrative evidence. It is generally a representation of an object which is a common form of proof.
   - For example, photographs, vidcos, sound recordings, X-rays, maps, drawing, charts, simulations, sculptures, and models.
2. **Electronic Evidence:**
   - Electronic evidence is nothing but digital evidence. As we know, the use of digital evidence in trials has greatly increased.

- The evidences or proof that can be obtained from an electronic source is called as digital evidence.
- For example emails, hard drives, word-processing documents, instant message logs, ATM transactions, cell phone logs, etc.

3. **Documented Evidence:**
   - Documented evidence is similar to demonstrative evidence. However, in documentary evidence, the proof is in writing. E,g, contracts, wills, invoices, etc. It can include any number of medias.
   - Such documentation can be recorded and stored.
   - For example, photographs, recordings, films, printed emails, etc.
4. **Explainable (Exculpatory) Evidence:**
   - This type of evidence is typically used in criminal cases in which it supports the dependent, either partially or totally removing their guilt in the case.
   - It is also referred to as exculpatory evidence.
5. **Substaintial Evidence:**
   - A proof that is introduced in the form of a physical object, whether whole or in part, is referred to as substantial evidence.
   - It is also called as physical evidence. Such evidence might consist of dried blood, fingerprints and DNA samples, casts of footprints, or tires at the scene of crime.
6. **Testimonial Evidence:**
   - It is a kind of evidence spoken by a spectator under oath, or written evidence given under oath by an official declaration, that is, affidavit.
   - This is one of the common forms of evidence in the system.

Q. 5 A) Explain process for collecting Network Based Evidence.

Ans :

- Network-based evidence collection is a crucial component of computer forensics investigations.
- Network-based evidence collection involves the collection of evidence from network traffic, network devices, and network infrastructure

I. Types of Network-based Evidence Collection

A. Passive Network-based Evidence Collection :

- Passive network-based evidence collection involves the collection of evidence from network traffic without actively affecting the network.Passive network-based evidence collection can provide information about network activity and potentially relevant evidence.

B. Active Network-based Evidence Collection

- Active network-based evidence collection involves the collection of evidence from network devices and infrastructure by actively interacting with the network.Active network-based evidence collection can provide more detailed information about network activity and potentially relevant evidence.
- Acquisition: To find or locate a specific evidence in a network environment can be a hard task. There are multiple sources of evidence commencing from the wireless access points to the web proxies to the central log servers which makes it often difficult to point out the exact location of an evidence. In certain cases, where we are still aware of a specific evidence and as to where it resides, obtaining an access to it can often become complex at times due to the political or technical reasons.
- Content: Apart from the filesystems, which are mainly designed to contain all the contents of files and their metadata, network devices may or may not store evidence with the level of granularity desired. The storage limit capacity of the network devices is often very limited. Most of the time, only the selected metadata about the data transfer or transaction is maintained as compared to entire records of the data that traversed the network.
- Storage: Secondary or persistent storage are usually not engaged as part of network devices. As a result of this consequence a device may not be able to survive a reset because the data contained in these network devices are unstable and uncertain.
- Privacy: Depending on the jurisdiction, legal issues could arise which may include personal privacy issues that are unique to network-based acquisition techniques.
- Seizure: Seizing of a hard drive can cause trouble and disruption to an individual or organization. However, a copy of the original hard drive can be constructed and deployed where the grave operations can continue with limited disturbance. Seizure done to a network device are most often way more disruptive. In the most serious cases, an entire network segment may be brought down perpetually. In most of the circumstances, investigators have the ability to minimize the impact on network operations.
- Admissibility: Filesystem-based evidence is being admitted consistently both in criminal and civil proceedings. As long as the filesystem-based evidence is relevant to the case, lawfully acquired & properly handle there is a clear precedent for validating or verifying the evidence and admitting it in court. In variance, the network forensics is one of the newest approaches to

digital investigations. Often there arise conflicting or even non-existing legal precedents for the admission of various types of network-based digital evidence. With time the network-based digital evidence may become more widespread and the case precedents will be set and standardized.

Q. 5 B) Explain various guidelines for digital forensic report writing along with its goals.

Ans :

➢ The Geberal principals or guidelines while writing an forensic report are :

1. **Document Investigative Steps Immediately and Clearly :**
   - Documenting investigative steps immediately requires discipline and organization, but it is essential to successful report writing.
   - Write everything down in a fashion that is understandable to you and others; do not use shorthand or shortcuts.
   - Such vague notations, incomplete scribbling, or unclear documentation will eventually lead to redundant efforts, forced translation of notes, confirmation of notes, and a failure to comprehend notes by yourself or others.
   - Writing something clearly and concisely at the moment you discover evidence (information of probative value) saves time and promotes accuracy.
   - We call this the “write it tight” philosophy. This can’t be emphasized enough, so it is worth repeating: Document as you go!
2. **Know the Goals of Your Analysis :**
   - Know what the goals of your examination are, before you begin your analysis. This fosters a focused report, which is what a client/consumer wants.
   - For law enforcement examin-ers, every crime has elements of proof.
   - Your report should unearth evidence that confirms or dispels these elements. The bottom line is that the more focused your reports are, the more effective they are.
3. **Organize Your Report :**
   - it is also called as Write “macro to micro.”
   - Organize your forensic report to start at the high level, and have the complexity of your report increase as your audience continues to read it.

- Include a table of contents for your longer reports. The table of contents enforces a logical approach to documenting your findings, and it helps the reader understand what your report accomplishes.

4. **Follow a Template :**
    - Follow a standardized report template. This makes your report writing scalable, establishes a repeatable standard, and saves time.
    - In practice, your report can be organized in many different fashions, but it needs to make sense.
5. **Use Consistent Identifiers :**
    - In a report, referring to an item in different ways—such as referring to the same computer as a system, PC, box, web server, victim system, and so on—can create confusion.
    - Developing a consistent, unwavering way to reference each item throughout your report is critical to eliminate such ambiguity or confusion.
    - It is a good idea to create a unique identifier or reference tag for each person, place, and thing (nouns) referred to repeatedly in your report. That label will identify the corresponding item for the remainder of the report.
6. **Use Attachments and Appendices :**
    - Use attachments or appendices to maintain the flow of your report. You do not want to interrupt your forensic report with 15 pages of source code right in the middle of your conclusions.
    - Any information, files, and file fragments that you cite in your report that are over a page long should be included as appendices or attachments. Then, you can include a brief reference to the appendix in the report.
    - For example, you might say, “A printout of the whois information is included as Appendix A.”
    - Some material is too big or simply impossible to provide in a printed format.
    - We simply burn a CD-ROM that contains all files that we cited in the report, and we append it as the last attachment in the report.
7. **Have Co-workers Read Your Reports :**
    - Employ other co-workers to read your forensic reports. This helps develop reports that are comprehensible to nontechnical personnel who have an impact on your incident response

strategy and resolution (such as Human Resources personnel, legal counsel, and business unit managers).

- Also, remember to write your reports at the appropriate level of the consumer of your report.

8. **Use MD5 Hashes :**

- Create and record the MD5 hashes of your evidence, whether it is an entire hard drive or specific files.
- Performing MD5 hashes for all evidence provides support to the claim that you are diligent and attentive to the special requirements of forensic examination.
- If your evidence is handled properly and remains tamper-proof, the MD5 hashes calculated for a given set of data will always remain the same.
- By recording these MD5 values, your audience becomes confident that you are handling the data in the appropriate manner.

9. **Include Metadata :**

- Record and include the metadata for every file or file fragment cited in your report. This metadata includes the time/date stamps, full path of the file (or physical location of the file fragments), the file size, and the file's MD5 sum.
- This identifying data will help to eliminate confusion and also to increase consumer confidence.

➢ **Goals for forensic report writing :**

➢ Report writing, like so many things in life, requires a documented process to ensure a repeatable standard is met by your organization.

➢ Investigative reports must be accurate, written in a timely manner, and understandable to your audience.

➢ They must meet the "golden standard" established by your organization.

➢ To write such a report, Computer forensic reports should achieve the following goals:

1. Accurately describe the details of an incident
2. Be understandable to decision-makers
3. Be able to withstand a barrage of legal scrutiny
4. Be unambiguous and not open to misinterpretation

5. Be easily referenced (using paragraph numbers for the report and Bates numbers for attached documents)
6. Contain all information required to explain your conclusions
7. Offer valid conclusions, opinions, or recommendations when needed
8. Be created in a timely manner

➢ Writing reports that meet these goals can be the most difficult challenge of performing incident response and computer forensics.

Q. 6 A) Tools used in network forensics

Ans :

1. **tcpdump**

   Tcpdump is a popular command line tool available for capturing and analyzing network traffic primarily on Unix based systems. Using tcpdump, we can capture the traffic and store the results in a file that is compatible with tools like Wireshark for further analysis. Tcpdump can either be used to do a quick packet capture for troubleshooting or for capturing traffic continuously in large volumes for future analysis**.**

2. **Wireshark**

   It would be a surprise if someone worked in the Cyber Security field and not heard of the tool Wireshark. Wireshark is an open-source tool available for capturing and analyzing traffic with support for applying filters using the graphical user interface. On the system, where Wireshark is running one can choose the interface on which traffic needs to be captured.

3. **Snort**

   Snort is one of the most popular network Intrusion Detection Systems available for free. There is a commercial version of Snort available, which is currently offered by Cisco. Snort is highly configurable, which allows the users to add custom plugins called preprocessors. In addition to it, it comes with a great set of output options. At its core, Snort provides alerts based on rulesets provided to it. The Snort administrator needs to feed the rules as the default installation doesn't come with any rules by default**.**

4. **Network Miner**

   According to the official website netresec.com, "NetworkMiner is an open source Network Forensic Analysis Tool (NFAT) for Windows (but also works in Linux / Mac OS X / FreeBSD). NetworkMiner can be used as a passive network sniffer/packet capturing tool in order to detect

operating systems, sessions, hostnames, open ports etc. without putting any traffic on the network. NetworkMiner can also parse PCAP files for off-line analysis and to regenerate/reassemble transmitted files and certificates from PCAP files.

NetworkMiner makes it easy to perform advanced Network Traffic Analysis (NTA) by providing extracted artifacts in an intuitive user interface. The way data is presented not only makes the analysis simpler, it also saves valuable time for the analyst or forensic investigator.

5. **NMAP :**One of the forensics tools for network scanning and auditing is Network Mapper (abbreviated NMAP). Its compatibility with practically all major operating systems, including Windows, Linux, Mac, and some less well-known ones like Solaris and HP-UX, is one of its main benefits.

Q. 6 B) Roles of CSIRT in handling incident

Ans:

- The role of the CSIRT is to serve as the first responder to computer security incidents within the Department and to perform vital functions in identifying, mitigating, reviewing, documenting, and reporting findings to management. The CSIRT coordinates with the Chief Technology Officer (CTO), but is accountable directly to the Secretary.
- The CSIRT will be responsible for the following activities:
    - Classifying Department security incidents

      (2) Meeting upon notification of a reported computer security incident dependent upon the incident severity level

      (3) Conducting a preliminary assessment to determine the root cause, source, nature and extent of damage of the suspected computer security incident with recommended responses as deemed appropriate

      (4) Selecting additional support members and subject matter experts as necessary for the reported incident

      (5) Maintaining confidentiality and need to know of information related to computer security incidents

      (6) Assisting with recovery efforts and providing reports to management

      (7) Performing and documenting all incidents and as appropriate include a root cause analysis and lessons learned

      (8) Reporting incidents to the Florida Digital Services and the Cybercrime Office

      (9) Maintaining awareness of, and implementing procedures for, an effective response to computer security incidents

      (10) Staying current on functional and security operations for the technologies

within their individual area of responsibility

(11) Receiving annual training on cybersecurity, threats, trends and best practices

Q. 6 C) Email tracing-internet Fraud

Ans:

- The term "internet fraud" generally covers cybercrime activity that takes place over the internet or on email, including crimes like identity theft, phishing, and other hacking activities designed to scam people out of money**.**
- Internet scams that target victims through online services account for millions of dollars worth of fraudulent activity every year. And the figures continue to increase as internet usage expands and cyber-criminal techniques become more sophisticated.

- Email-based phishing scams are among the most prevalent types of internet fraud, which continues to pose a serious threat to internet users and businesses.

- Statistics from Security Boulevard show that in 2020, 22% of all data breaches involved a phishing attack, and 95% of all attacks that targeted business networks were caused by spear phishing. Furthermore, 97% of users could not spot a sophisticated phishing email, 1.5 million new phishing sites were created every month, and 78% of users understand the risk of hyperlinks in emails but click them anyway.

- Email-based phishing scams are constantly evolving and range from simple attacks to more sneaky and complex threats that target specific individuals.

- Email phishing scams see cyber criminals masquerade as an individual that their victim either knows or would consider reputable. The attack aims to encourage people to click on a link that leads to a malicious or spoofed website designed to look like a legitimate website, or open an attachment that contains malicious content.

- The hacker first compromises a legitimate website or creates a fake website. They then acquire a list of email addresses to target and distribute an email message that aims to dupe people into clicking on a link to that website. When a victim clicks the link, they are taken to the spoofed website, which will either request a username and password or automatically download malware onto their device, which will steal data and login credential information. The hacker can use this data to access the user’s online accounts,

steal more data like credit card details, access corporate networks attached to the device, or commit wider identity fraud.

- Email phishing scam attackers will often express the need for urgency from their victims. This includes telling them that their online account or credit card is at risk, and they need to log in immediately to rectify the issue.