

## #Computer Forensics Fundamentals

**\*Computer Forensics:**-Computer forensics, also referred to as computer forensic analysis, electronic discovery, electronic evidence discovery, digital discovery, data recovery, data discovery, computer analysis, and computer examination, is the process of examining computer media (hard disks, diskettes, tapes, etc.) for evidence.

-In other words, computer forensics is the collection, preservation, analysis, and presentation of computer-related evidence.

-Computer evidence can be useful in criminal cases, civil disputes, and human resources/employment proceedings.

-Computer forensics is primarily used for two separate purposes, investigation and data recovery.

-Computer forensics is the face of modern investigations.

-When a crime is committed and an investigation is started, one of the more common places to look for clues is the computer or cell phone of a suspect.

-This is where a computer forensics professional enters the picture.

-When a suspect has been identified and their personal computer or cell phone taken into evidence, a computer forensics professional goes searching for data that is relevant to the investigation.

-Aside from working to collect evidence, computer forensics professionals can also work in data recovery.

-When it comes to data recovery, forensics professionals can take broken hard drives, crashed servers and other compromised devices and retrieve the data that was previously lost.

**\*Use of Computer Forensics in Law Enforcement** (9 marks) :-If there is a computer on the premises of a crime scene, the chances are very good that there is valuable evidence on that computer.

-If the computer and its contents are examined (even if very briefly) by anyone other than a trained and experienced computer forensics specialist, the usefulness and credibility of that evidence will be lost.

-Computer forensics tools and techniques have proven to be a valuable resource for law enforcement in the identification of leads and in the processing of computer-related evidence.



-Computer forensics tools and techniques have become important resources for use in internal investigations, civil lawsuits, and computer security risk management.

-Law enforcement and military agencies have been involved in processing computer evidence for years.

-This are the Use of Computer Forensics in Law Enforcement they are;

- **Recovering deleted files** such as documents, graphics, and photos.
- **Searching unallocated space** on the hard drive, places where an abundance of data often resides.
- **Tracing artifacts**, those tidbits of data left behind by the operating system.  
-Our experts know how to find these artifacts and, more importantly, they know how to evaluate the value of the information they find.
- **Processing hidden files** — files that are not visible or accessible to the user — that contain past usage information.  
-Often, this process requires reconstructing and analyzing the date codes for each file and determining when each file was created, last modified, last accessed and when deleted.
- **Running a string-search** for e-mail, when no e-mail client is obvious.

**\*Steps taken by Computer Forensics Specialists (5 marks )**:-The computer forensics specialist should take several careful steps to identify and attempt to retrieve possible evidence that may exist on a subject's computer system.

-This are the Steps taken by Computer Forensics Specialists they are;

1. **Protect**:- the subject computer system during the forensic examination from any possible alteration, damage, data corruption, or virus introduction.
2. **Discover**:- all files on the subject system. This includes existing normal files, deleted yet remaining files, hidden files, password-protected files, and encrypted files.
3. **Recover**:- all (or as much as possible) of discovered deleted files.
4. **Reveal**:- (to the greatest extent possible) the contents of hidden files as well as temporary or swap files used by both the application programs and the operating system.
5. **Access**:- the contents of protected or encrypted files.
6. **Analyze**:- all possibly relevant data found in special (and typically inaccessible) areas of a disk.
7. **Print out**:- an overall analysis of the subject computer system, as well as a listing of all possibly relevant files and discovered file data.
8. **Provide an opinion of the system layout**:- the file structures discovered; any discovered data and authorship information; any attempts to hide, delete, protect,



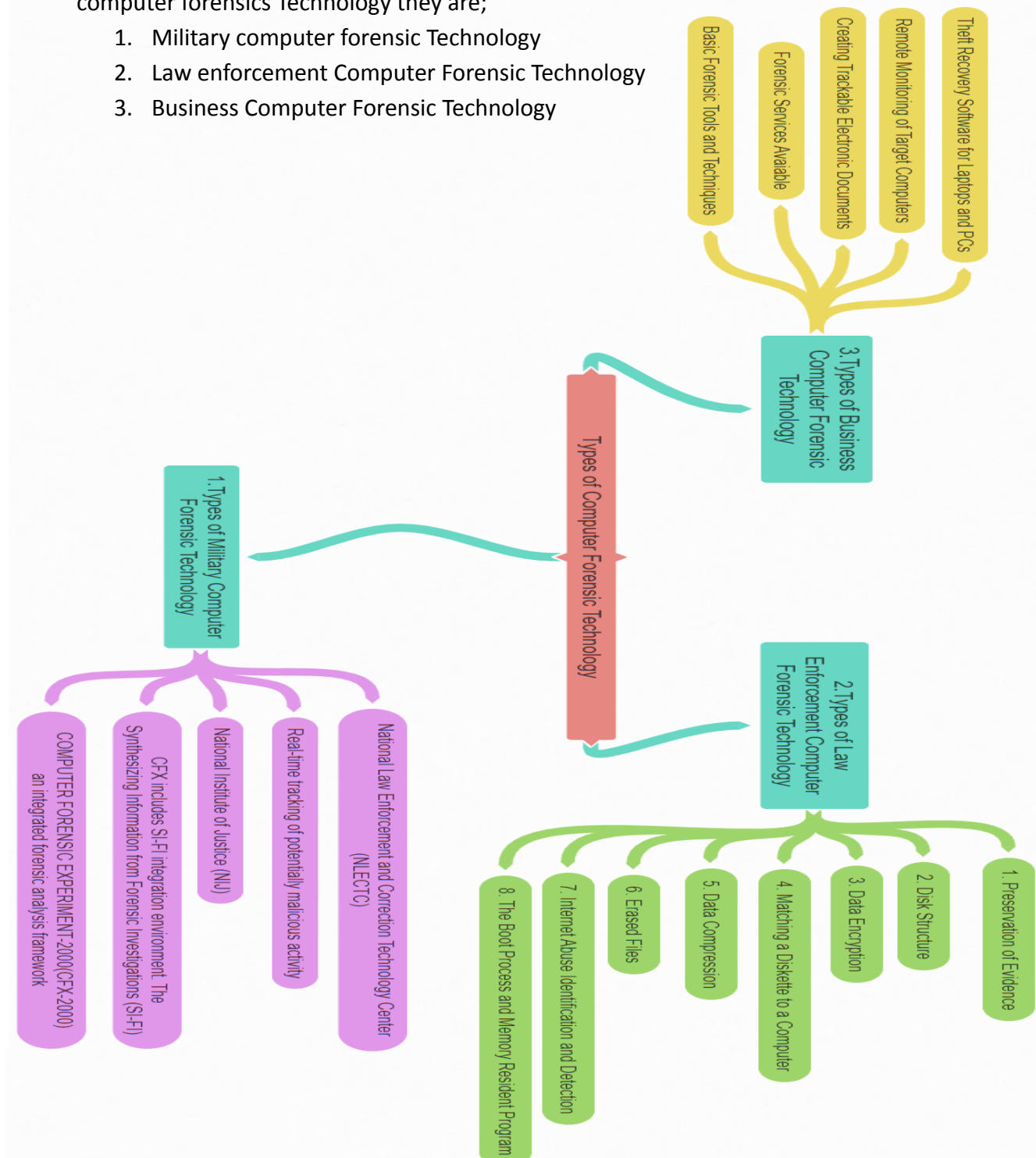
and encrypt information; and anything else that has been discovered and appears to be relevant to the overall computer system examination.

9. **Provide expert consultation:-** and/or testimony, as required.

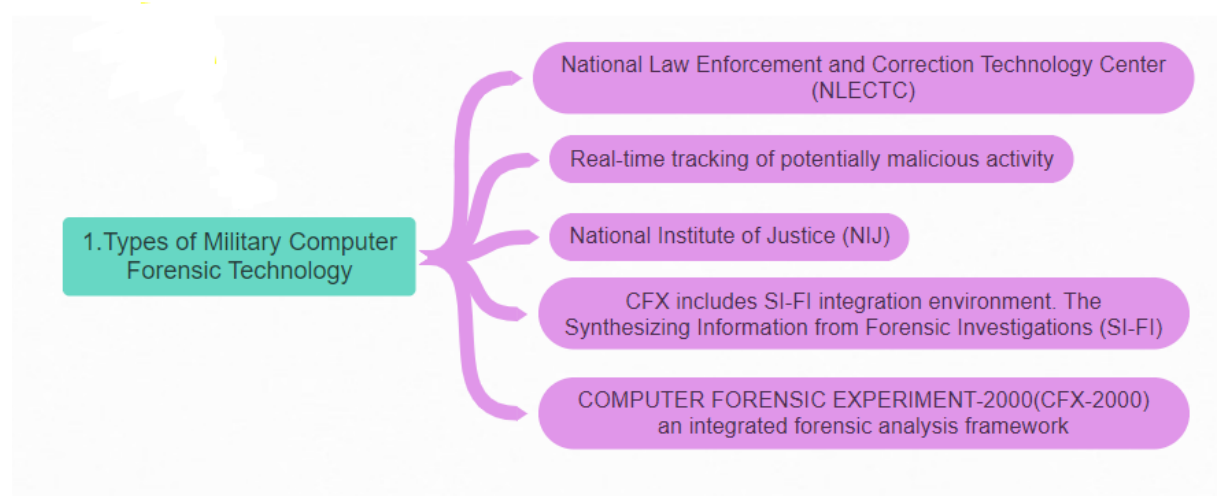
**\* Scientific method in Computer Forensic Analysis:-**

**#Types of Computer Forensic Technology** (9mark):-There are 3 types of computer forensics Technology they are;

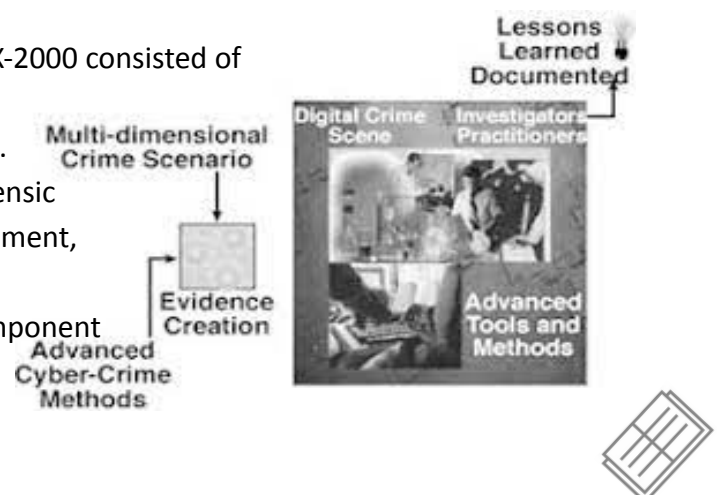
1. Military computer forensic Technology
2. Law enforcement Computer Forensic Technology
3. Business Computer Forensic Technology



1. **Types of Military computer forensic Technology**: -Key objectives of cyber forensics include rapid discovery of evidence, estimation of potential impact of the malicious activity on the victim, and assessment (evaluating) of the intent and identity of the criminal.
  - Real-time tracking of potentially malicious activity is especially difficult.
  - when relevant data has been purposefully altered, removed, or buried in order to avoid being discovered.
  - so, the **National Law Enforcement and Corrections Technology Centre (NLECTC)** works with **criminal justice professionals** to find a technology.

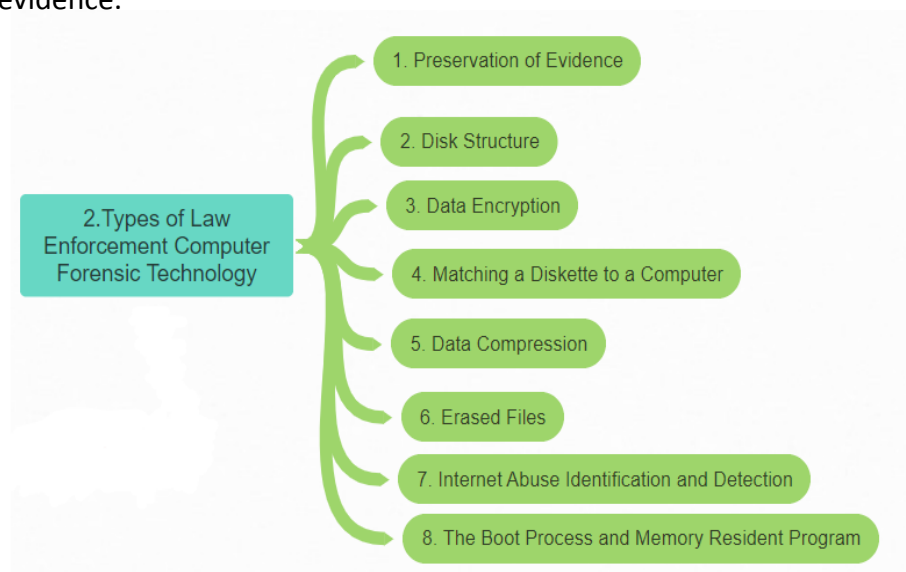


- The result of their partnership they form **Computer Forensics Experiment 2000 (CFX-2000)**.
- And conduct a experiment having a realistic cyber crime scenario specifically designed to exercise and show the value of the technology used.
- The central hypothesis of CFX-2000 is possible to accurately determine the motives, intent, targets, sophistication, identity, and location of cyber criminals and cyber terrorists.
- The NLECTC assembled a diverse group of computer crime investigators from DoD and federal, state, and local law enforcement to participate in the CFX-2000 exercise hosted by the New York State Police's Forensic Investigative Center in Albany, New York.
- The cyber forensic tools involved in CFX-2000 consisted of **commercial off the-shelf software** and **directorate-sponsored R&D prototypes**.
- The Synthesizing Information from Forensic Investigations (**SI-FI**) integration environment, developed under contract by WetStone Technologies, Inc. [2], was the main component Of the technology.



- SI-FI** supports the collection, examination, and analysis processes in a cyber forensic investigation.
- The SI-FI prototype uses digital evidence bags (DEBs), which are secure and tamper proof containers used to store digital evidence.
- The CFX-2000 results confirmed that the assumption was mostly accurate and that it is easy to determine the identity and purpose of cybercriminals.
- In order to be ready for any kind of cyber attacks and investigations, researchers must maintain a strong focus on the study and development of cyber forensic technologies as electronic technology continues to grow quickly.

2. **Types of Law enforcement Computer Forensic Technology**:-Computer forensics tools and techniques have become important resources for use in internal investigations, civil lawsuits, and computer security risk management.
- Law enforcement and military agencies have been using computer evidence for years.
  - Computer forensics tools and techniques have proven to be a valuable resource for law enforcement in the identification of leads and in the processing of computer related evidence.



→**Computer Evidence Processing Procedures**:-Processing procedures and methodologies should fit to federal computer evidence processing standards.

- A. **Preservation of Evidence**:-Computer evidence is fragile and can be changed or deleted by a variety of events.



- Computer evidence can be useful in criminal cases, civil disputes, and human resources/ employment proceedings.
- Black box** computer forensics software tools are good for some basic investigation tasks, but they do not offer a full computer forensics solution.
- SafeBack software overcomes some of the evidence weaknesses of black box computer forensics approaches.
- SafeBack technology has become a worldwide standard in making **mirror image backups** since 1990.
- (SafeBack is used to create mirror-image (bit-stream) backup files of hard disks or to make a mirror-image copy of an entire hard disk drive or partition.SafeBack image files cannot be altered or modified )

Q)What is mirror backup?

-A mirror backup is an exact copy of the selected folders and files from the source being backed up.

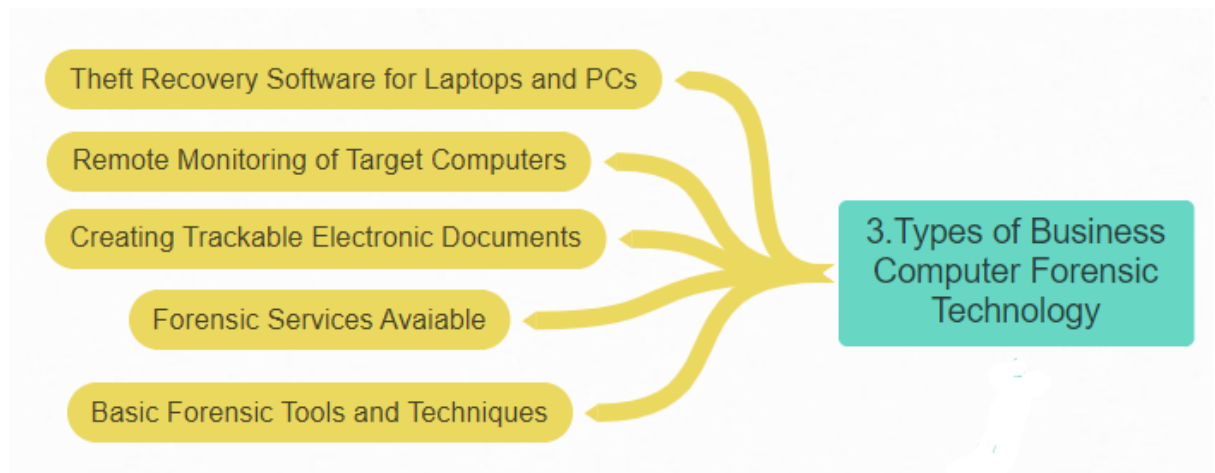
-Mirror backups are unique in that when you delete a file from the source, that file will eventually be deleted on the mirror backup.

- B. **Disk Structure**:-Computer forensic experts must understand how computer hard disks and floppy diskettes are structured .
  - And where the computer evidence can exist in different layers of the disk's structure.
  - They should also demonstrate their knowledge of how to modify the structure and hide data in deep places on floppy diskettes and hard disk drives.
- C. **Data Encryption**:-Computer forensic experts should become familiar with the use of software to crack security connected with the different file structures.
- D. **Matching a Diskette to a Computer**:-[google](#)
- E. **Data Compression**:-Computer forensic experts should become familiar with how compression works and how compression programs can be used to hide and mask sensitive data.
  - And also learn how password-protected compressed files can be broken.
- F. **Erased Files**:-Computer forensic experts should become familiar with how previously erased files can be recovered by using DOS programs and by manually using data- recovery technique & familiar with cluster chaining.
- G. **Internet Abuse Identification and Detection**:-Computer forensic experts should become familiar with how to use specialized software to identify a targeted computer that has been used on the Internet.
  - This process will focus on the data that the computer user probably doesn't realize exists (file slack, unallocated file space, and Windows swap files).




- H. **The Boot Process and Memory Resident Programs:**-Computer forensic experts should become familiar with how the operating system can be modified to change data and destroy data.  
-For example, this technology could be to secretly record business leaders using their keyboards.

3. **Types of Business Computer Forensic Technology:**- This are types of business computer forensics technology.



- A. **Remote monitoring of target computers:**-Data Interception by Remote Transmission (**DIRT**) is a powerful remote control monitoring tool that allows quiet monitoring of all activity on one or more target computers simultaneously from a remote command center.  
-No physical access is necessary.  
-Application also allows agents to remotely seize and secure digital evidence prior to physically entering suspect premises.  
Or  
-Moreover, agents can use this application to remotely capture or seize and store digital evidence before physically visiting a suspect location.



- B. **Creating trackable electronic documents:**-There are so many powerful intrusion  detection tools .  
-Binary Audit Identification Transfer (BAIT) is one of a powerful intrusion detection tool that allows users to create trackable electronic documents.



- BAIT identifies (including their location) unauthorized intruders who access, download, and view these tagged documents.
- BAIT also allows security personnel to trace the chain of custody and chain of command of all who possess the stolen electronic documents.

**C. Theft recovery software for laptops and PCs:**-If your PC or laptop is stolen, is it smart enough to tell you where it is?

-According to a recent FBI report, 98% of stolen computers are never recovered. According to Safeware Insurance, 1,201,000 PCs and laptops were stolen in 2002 and 2003, costing owners \$7.8 billion dollars [9]. According to a recent joint ComputerSecurity Institute/FBI survey, 72% of the Fortune 1000 companies experienced laptop theft [9].

→What is the Real Cost of a Stolen Laptop or PC?

-When you lose your wallet, the last thing you think of is how much it is going to cost to replace your wallet.

-The same is true when equipment (especially a computer) is stolen.

- The price of the replacement hardware.
- The price of replacing the software.
- The cost of recreating data. If possible at all, do you keep perfect back-ups?
- The cost of lost production time or instruction time.
- The loss of customer goodwill (lost faxes, delayed correspondence or billings, problems answering questions and accessing data).
- The cost of reporting and investigating the theft, filing police reports and insurance claims.
- The cost of increased insurance.
- Types of Computer Forensics Technology
- The cost of processing and ordering replacements, cutting a check, and the like.
- If a thief is ever caught, the cost of time involved in prosecution .

-**PC PhoneHome** is a software application that will track and locate a lost or stolen PC or laptop any-where in the world.

It is easy to install.

-It is also completely transparent to the user.

-If your PC PhoneHome-protected computer is lost or stolen, all you need to do is make a report to the local police and call CD's 24-hour command center.

-CD's recovery specialists will assist local law enforcement in the recovery of your property.





D. **Basic forensic tools and techniques:-** explain cheyandaaa

E. **Forensic services available** (3 marks) :-this are the Forensic services available they are;

- Lost password and file recovery
- Location and retrieval of deleted and hidden files
- File and email decryption
- Email supervision and authentication
- Threatening email traced to source
- Identification of Internet activity
- Computer usage policy and supervision
- Remote PC and network monitoring
- Tracking and location of stolen electronic files
- Honeypot sting operations
- Location and identity of unauthorized software users
- Theft recovery software for laptops and PCs
- Investigative and security software creation
- Protection from hackers and viruses.

**#Types of Computer Forensic System** (9 mark):- Following are the types of computer forensic system.

1. Internet security systems
2. Intrusion detection systems
3. Firewall security systems
4. Biometric security systems
5. Network disaster recovery systems
6. Public key infrastructure security systems
7. Wireless network security systems

1. **Internet security systems** (9 mark):-Talking about internet and network security is something that many managers and executives fear doing.
  - They believe that talking about their security procedures and guidelines will make their businesses more open to intrusion.
  - Because of this lack of communication, some executives are not completely aware of the numerous security technology advancements and developments that allow businesses to securely take full advantage of the benefits and capabilities of the Internet and intranets.
  - Ironically, Internet security can provide a more secure solution, as well as one that is faster and less expensive than traditional solutions to security problems of employees photocopying proprietary information, faxing or mailing purchase orders, or placing orders by phone.



→**Internet Security System Principles and Architecture**:-The First step of formulating a corporate Internet security strategy involves **crafting a high-level management policy statement that provides an organization's security framework and context.**

-The Internet security procedures that are required to protect a company's systems, networks, transactions, and data must be specified in this policy.

-The next step is to start a systematic analysis of the assets of an organization, determining the value of information, or the possible damage to reputation when it is disclosed and possible risks.

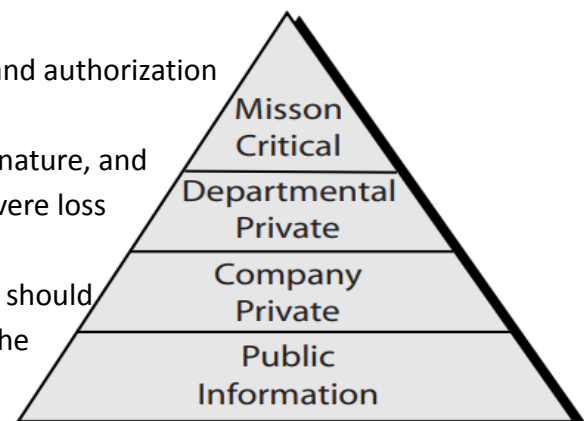
-This step is no more difficult than the risk management that a corporation is already facing every day.

-Most businesses already have clearly established what information is valuable, who should have access to it, and who has responsibility for protecting it, as the Internet security hierarchy in Figure shown below.

-Information such as trade secrets, vault and authorization codes, and lock and key

Information e clearly of a **mission critical** nature, and their accidental disclosure could cause severe loss to a business or operation.

- In addition to Internet security,attention should be given to physical security (restricting the use of modems and removable media and controlling access to devices) also.



**FIGURE 3.1** Internet security hierarchy.

-**Departmental information** is typically data that is private to a particular department, such as payroll information in finance and medical records in personnel.

-**Company private information** varies from company to company but typically consists of information that should only be disclosed to employees and partners of a company, such as policy and procedure manuals.

-**Public information** is information such as product information, brochures, and catalogs that needs to be freely available to anyone.

-Customers and other interested parties are frequently given access to this information over the Internet.

-Implementing an Internet security policy has its price.

-The more security desired, the greater the cost required to provide it.

-The cost of providing security increases with the required level of protection.



2. **Intrusion detection systems** (9 mark):-IDS observes network traffic for malicious transactions and sends immediate alerts when it is observed.

-It is software that checks a network or system for malicious activities or policy violations.

-Each illegal activity or violation is often recorded either centrally using a SIEM system or notified to an administration.

-IDS monitors a network or system for malicious activity and protects a computer network from unauthorized access.

-The intrusion detector task is to build a predictive model (i.e. a classifier) capable of distinguishing between 'bad connections' (intrusion/attacks) and 'good (normal) connections'.



→**Classification of Intrusion Detection System/types of IDS:-** There are five types of IDS: network-based, host-based, protocol-based, application protocol-based and hybrid.

-The two most common types of IDS are: (e randu ennam matram just onnu explain cheythal mathi)

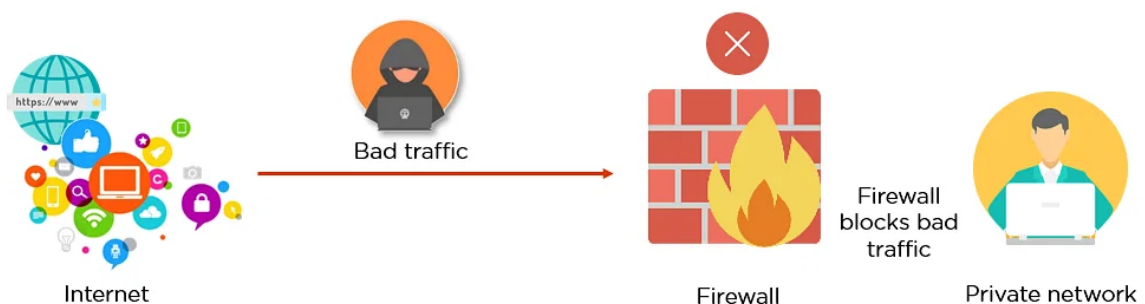
- Network Intrusion Detection System (NIDS):-It is a system that analyze incoming traffic.
  - Once an attack is identified or abnormal behavior is observed, the alert can be sent to the administrator.
- Host Intrusion Detection System (HIDS):-It is a system that monitors important operating system (OS) files.

→**Detection Method of IDS:-**

- Signature-based Method:-It detects the attacks on the basis of the specific patterns such as the number of bytes or a number of 1s or the number of 0s in the network traffic.
  - It also detects the already known malicious instruction sequence that is used by the malware.
  - The detected patterns in the IDS are known as signatures.
  - Signature-based IDS can easily detect the attacks whose pattern (signature) already exists in the system but it is quite difficult to detect new malware attacks as their pattern (signature) is not known.
- Anomaly-based Method:-It was introduced to detect unknown malware attacks as new malware is developed rapidly.
  - In anomaly-based IDS there is the use of machine learning to create a trustful activity model and anything coming is compared with that model and it is declared suspicious if it is not found in the model.



3. **Firewall security systems** (9 mark):-A Firewall is a network security device that monitors and filters incoming and outgoing network traffic based on an organization's security policies.
- A firewall is essentially the barrier that sits between a private internal network and the public Internet.
  - A firewall's main purpose is to allow non-threatening traffic in and to keep dangerous traffic out.
  - A firewall is a cybersecurity tool that filters network traffic and helps users block malicious software from accessing it.



→**Types of Firewalls**:- following are the types of firewalls

- **Packet filtering**:-Packet filtering firewall is used to control network access by monitoring outgoing and incoming packets and allowing them to pass or stop based on source and destination IP address, protocols, and ports.
  - Packet firewalls treat each packet in isolation.
  - They have no ability to tell whether a packet is part of an existing stream of traffic.
  - Only It can allow or deny the packets based on unique packet headers.
  - Packet filtering firewall maintains a filtering table that decides whether the packet will be forwarded or discarded.
- **Proxy service**:-A proxy server firewall caches, filters, logs, and controls requests from devices to keep networks secure and prevent access to unauthorized parties and cyberattacks.
  - A proxy server is often considered part of a firewall, which prevents unauthorized access and connections.
  - The proxy is more of a mediator that establishes connections between users and networks.
- **Stateful inspection**:-Stateful firewalls are able to determine the **connection state of packet**, unlike Packet filtering firewall, which makes it more efficient.



- Next Generation Firewall (NGFW):-Next Generation Firewalls are being deployed to stop modern security breaches like advance malware attacks and application-layer attacks.
  - It consists of **Deep Packet Inspection** which is used to protect the network from these modern threats.

→**Advantages of using Firewall**:-This are the main advantages of firewall.

- Protection from unauthorized access
- Prevention of malware and other threats
- Control of network access
- Monitoring of network activity
- Enhanced privacy
- Policy enforcement
- Controlled access to the site.

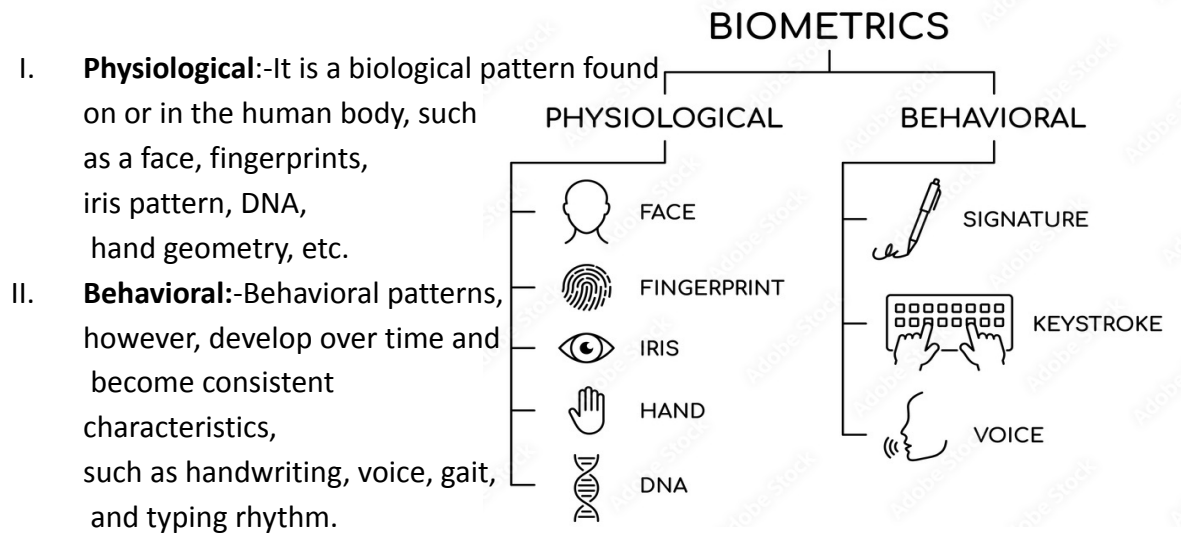
4. **Biometric security systems**(9 mark):-It is a technology that extracts information out of biological or behavioral patterns of a person to recognize a particular person.
- It currently uses most is physical access control like fingerprint recognition because of its lower price.
  - Biometric system is subjected to many malicious attacks which can be performed by various forms of threats.
  - Malicious attacks on a biometric machine are a security concern and degrade the system's performances.
  - Biometric system has various limitations like spoof attacks, noisy sensor data, interclass variations, and interclass similarity, etc.
  - The high attacks are relevant to any biometric system which is to be analyzed, and countermeasures are to be taken while designing the biometric system.
  - The different attacks in biometrics systems are as follow:
    - Fake Biometric
    - Spoofing the Feature set
    - Template Tampering Attack
    - Trojan horse attack etc..

→**Biometric Authentication**:-It is a way to verify ,beyond a doubt,that a person is who they say they are.

- It perform this verification by checking biological or behavioral characteristics.
- For example Facial Recognition,Voice Recognition,DNA Matching,Retina Scanning etc



→**Types of Biometric System**:-Physiological and Behavioural Biometric Identification are the two primary forms of Biometric Identification.



5. **Network disaster recovery systems**(3 mark):-Modern organizations have to operate on a 24/7 basis in order to stay competitive in the market.

-It is important to create a disaster recovery (DR) plan so as to ensure that your business can continue to operate even during a DR event.

-However, a lot of companies forget how important network disaster recovery is while creating DR plans.

-A network disaster recovery plan includes a set of procedures required to effectively respond to a disaster that affects a network and causes disturbance.

-The main purpose of network disaster recovery is to ensure that business services can be delivered to customers even if there was a network connectivity issue.

-However, disasters come in different forms and sizes, which makes it hard to predict what their impact would be, which network components would be affected, and how many resources would be required to restore network connectivity.

→**Possible Causes of Network Failures**:-Various factors can lead to network failure. They are;

- **Hardware failure**:- Network equipment such as routers, switches, modems, gateways, or any other device can fail and, as a result, affect the performance of all other devices connected to them.
- **Cascading failure**:- A single network consists of multiple routers, nodes, or switches.



-One of those network components might become overloaded and stop working, which can trigger a cascade of failures within a single network.

- **Issues with the internet connection:-** Failure to set up an internet connection can cause problems with network connectivity and interrupt data transfer.
- **Human errors:-** Sometimes, network connectivity problems might be the result of mistakes made by employees when working with network equipment or manually configuring network components.
- **Network attacks:-** Network services can get disrupted after a cyber-attack, whose aim is to prevent the organization from delivering its services, forcing it to shut down.
- **Natural or man-made disaster:-** Disasters of any type can significantly damage or even destroy your production center and virtual infrastructure, thus causing significant business losses.

-Network Disaster Recovery Plan So Important because an organization cannot function properly if one of its system components stops working.

-Without network services, a company cannot properly execute its business operations and move data within the infrastructure.

-Network disaster recovery can be a challenging task because even a single error can disrupt the entire DR process.

6. **Public key infrastructure security systems (PKI):-** PKI (or Public Key Infrastructure) is the framework of encryption and cybersecurity that protects communications between the server (your website) and the client (the users).

-PKI is essential in building a trusted and secure business environment by being able to verify and exchange data between various servers and users.

-The most distinct feature of Public Key Infrastructure (PKI) is that it uses a pair of keys to achieve the security service.

-The key pair is the comprises of **private key and public key**.

7. **Wireless network security systems:-** Wireless security is the protection of wireless networks, devices and data from unwanted access and breaches.

-It involves a variety of strategies and practices designed to preserve it.

-It is a subset of network security that adds protection for a wireless computer network.

-Without sufficient security measures, unauthorized users can easily gain access to a wireless network, steal sensitive data, and disrupt network operations.

-To prevent unwanted access and protect data in transit, wireless connections must be secured with strong authentication procedures, encryption protocols, access control rules, intrusion detection and prevention systems, and other security measures.



- By securing wireless connections, your organization's data is protected and you maintain the trust of customers and partners.
  - The first and one of the most important step toward securing a wireless network ,Is the encrypt the wireless network by giving a proper password otherwise anyone can access it.
  - Enable Access control rules to determine which people or devices are permitted to connect to the network and what degree or level of access they have.
  - Securing the physical components of the wireless network (routers, access points, and other devices), so that no one can access and tamper with them.
  - Updating router's firmware is a good move towards a secure wireless network.
  - Firmware update fix know bugs and provide security updates.
- 





## Module-2

### **#Data Recovery:-**computers systems may crash.

- Files may be accidentally deleted.
- Disks may accidentally be formatted.
- Computer viruses may corrupt files.
- Files may be accidentally overwritten.
- Others may try to destroy your files.
- All of these can lead to the loss of your critical data.
- You may think it's lost forever, However, in order to recover your data, you should use the most recent tools and techniques to recover it.
- In many cases, the data cannot be found using the limited software tools available to most users.
- But the advanced tools should allow us to find your files and restore them.

**\*Data recovery defined:-**Data recovery is the process in which highly trained engineers evaluate and extract data from damaged media and return it in its original format.

- In data recovery it is possible to retrieve files that have been deleted and passwords that have been forgotten or to recover entire hard drives that have been physically damaged.
- Perhaps your information has been subjected to a virus attack, suffered damage from smoke or fire, or your drive has been immersed in water—the data recovery experts can recover it.

### **Q) Data backup and Recovery process (9 marks)** 📌

**\*Data backup and Recovery** (9 marks) :-Backup and recovery describes the process of creating and storing copies of data that can be used to protect organizations against data loss.

- Recovery from a backup typically involves restoring the data to the original location, or to an alternate location where it can be used in place of the lost or damaged data.
- A proper backup copy is stored in a separate system or medium, such as tape etc
- The purpose of the backup is to create a copy of data that can be recovered in the event of a primary data failure.
- Primary data failures can be the result of hardware or software failure, data corruption, or a human-caused event, such as a malicious attack (virus or malware), or accidental deletion of data.
- Backup copies allow data to be restored.
- Storing the copy of the data on separate medium is to protect against primary data loss or corruption.



- This additional medium can be as simple as an external drive or USB stick, or something larger, such as a disk storage system, cloud storage container, or tape drive.
- The alternate medium can be in the same location as the primary data or at a remote location.
- The key difference between backup and recovery is that the backup process is how you save and protect your production data and safely store it away so you have it for a later time.
- Recovery is the process whereby you retrieve and restore that backup data to your production systems to avoid downtime.

→**Backup Obstacles:**-The following are obstacles to backing up applications:

1. Backup window
2. Network bandwidth
3. Lack of resources

1. **Backup window:**-A backup window is the time slot when it is most suitable to back up data, applications or a system.

-It is a predefined/pre scheduled time when the backup software is permitted to start the backup process on a system.

Or

-The backup window is the period of time when backups can be run.

-The backup window is generally timed to occur during nonproduction periods when network bandwidth and CPU utilization are low.

2. **Network bandwidth:**-Many companies now have more data to protect than can be transported.

-If a network cannot handle the impact of transporting hundreds of gigabytes of data over a short period of time, then the organization's backup plan is unworking.

3. **Lack of resources:**-Many companies fail to make appropriate investments in data protection until it is too late.

**\*The role of Backup in Data Recovery:**-There are many factors that affect back-up.

-For example:

- **Storage costs are decreasing:**-With the development of **disc drive technologies**,The cost of primary (online) storage has fallen dramatically over the past several years and continues to do.
  - This has a huge impact on backup.
  - A users become more addicted to having immediate access to more and more information online.
  - Because the time required to restore data from secondary media is found to be unacceptable.
- **Systems have to be online continuously:**-Seven/twenty-four (7 × 24) operations have become the normal in many of today's businesses.



-Because systems must be continuously online, the difficult situation is that you can no longer take files offline long enough to perform backup.

- **The role of backup has changed:**-It's no longer just about restoring data.  
-The role of backup now includes the responsibility for recovering user errors and ensuring that good data has been saved and can quickly be restored.

**\*The Data Recovery Solution:**-Data Recovery is the process of restoring data from damaged, failed, corrupted, or inaccessible secondary storage media when it cannot be accessed normally.

-Data recovery only implies over the data written on the device.

-If you are trying to recover unwritten data, data recovery techniques may not work eventually.

-Following are the solutions for data recovery.

- **Building Recovery Toolkit:**-It is always better to save the data from losing rather than performing recovery measures.  
-Although, you can install free recovery tools to recover up to approximately 2 GB of data and purchase tools if data exceeds the limit.
- **Using High-Performance Backup – CDP:**-Continuous Data Protection (CDP), also known as continuous backup, is a system that regularly backs up data on a computer system.  
-CDP allows you to restore your data.
- **Direct attached storage:** Virtual and physical servers can be added as backup repositories.

**\* Hiding and Recovering Hidden Data:**-Data hiding is the process of changing or manipulating a file in order to hide information.

-Data-hiding techniques include hiding the entire portion, changing file extensions, setting file attributes to hidden, bit-shifting, using encryption, and setting up password protection.

#### →Data hiding benefits

- Ensures the privacy of sensitive data in cyberspace.
- Prevents unauthorized access to private information.
- reduces the possibility of cyberattacks and data breaches.
- creates safe routes for communication
- Protects property rights and digital assets.

→**Reason for Hiding Data:**-There are many reasons why an individual would want to hide their information for criminal and non-criminal purpose.

-some of the reasons for hiding data are as follows:

- Due to the level of secrecy
- Due to privacy
- Due to confidentiality
- To hide proof of fraud activities



- For hide malicious codes

→ **Data-hiding Techniques** (9 marks):-

**1. File manipulation**

- Filenames and extensions

**2. Disk manipulation**

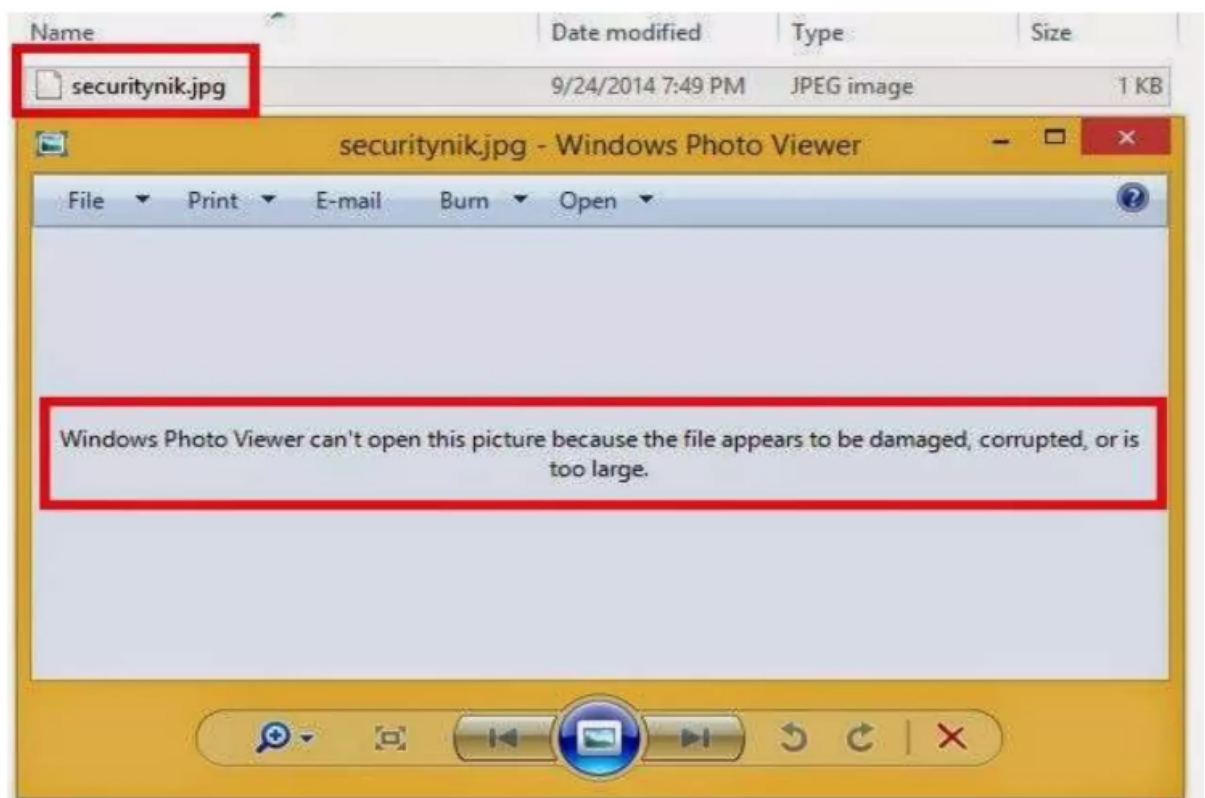
- Hidden partitions
- Bad clusters

**3. Encryption**

- Bit shifting
- Steganography

**1. File manipulation**

- **Filenames and extensions:-**For example we have a file with an extension of .jpg.
  - The objective is to open this file.
  - But when we opened it we saw this type of error.



- As we can be seen above, we encountered an error.
- Now, a typical user may say this file is corrupt and thus probably delete the file and move on.
- While that may be acceptable for the regular user, a forensics analyst would need to dig a little deeper.



- By help of a tool we can find the extension of the file.
- and change the extension from .jpg to that particular extension.
- The file extension can be changed by either renaming the file in "Windows Explorer" or in the command prompt.

## 2. Disk manipulation

- **Hidden partitions** :-A hidden partition does not have a drive letter and it cannot be seen in Windows Explorer, thus operating systems cannot access it.
  - Files in hidden partition are not lost, but they cannot be accessed in normal method.
  - We can create a partition and then hide it using a disk editor.
  - We can get access to hidden partitions using tools such as: GDisk, PartitionMagic, System Commander, and LILO.
  - hidden partitions are also a prime location for storing evidence files and other files of interest.
- **Bad clusters** :-This method is more common in FAT file systems.
  - This technique involves using a disk editor, such as **Norton DiskEdit**, to mark good clusters as bad clusters.
  - The OS then considers these clusters unusable.
  - The only way they can be accessed from the OS is by changing them to good clusters with a disk editor.
  - To mark a good cluster as bad using Norton Disk Edit, we type the letter B in the **FAT entry** corresponding to that cluster.

## 3. Encryption

- **Bit shifting** :-Bit-shifting is an old technique that shifts bit patterns to alter byte values of data and makes files look like binary executable code.
  - A well-known technique for hiding data is shifting bit patterns to alter the byte values of data.
  - Bit-shifting changes data from readable code to data that looks like binary executable code.
- **Steganography** :-It refers to hiding information within other data or media, such as images, audio files, or videos.
  - Since hackers cannot assume the specific embedding method, they cannot detect the hidden data.
  - It is a technique which hides the information in such a way that no third person other than the receiver knows that there is a secret message hidden inside the information that is transferred.
  - This are the Types of Steganography
    - Text steganography:- Text steganography conceals a secret message inside a piece of text
    - Image steganography:- In image steganography, secret information is encoded within a digital image.



- Video steganography
- Audio steganography:-One simple form of audio steganography is “backmasking,” in which secret messages are played backwards on a track (requiring the listener to play the entire track backwards).
- Network steganography:-network steganography is a clever digital steganography technique that hides information inside network traffic.

→**Recovering hidden data**:-Hidden data, also known as metadata, is information that is embedded within a file or document that is not immediately visible to the user.

-There are several ways to identify hidden data within a file or document.

-One of the simplest methods is to use a specialized software program designed to scan for and extract metadata.

-These programs can quickly scan a file or document and identify any hidden data that may be present.

-Another method for identifying hidden data is to manually examine the file or document.

-This can be done by opening the file in a text editor or word processor and examining the file's properties.

-Many text editors and word processors have built-in tools that allow users to view and edit metadata, making it easy to identify hidden data.

-In addition to software and manual methods, there are also online tools and websites that can be used to identify hidden data.

-These tools can be used to scan a file or document and extract any hidden data that may be present.

These tools can be especially useful for identifying hidden data in large collections of files or documents.

-By using specialized software, manual examination, and online tools, it is possible to quickly and easily identify any hidden data that may be present.

-This information can then be used for a variety of purposes, including forensic analysis and data recovery.

**#Evidence Collection**:-Even in the best of situations, gathering evidence may be challenging, but when that evidence is electronic, an investigator faces some extra complexities.

-The reasons for collecting evidence are:

- **Future Prevention**:-You will never be able to prevent someone else from doing it in the future if you don't know what went wrong.  
-Similar to leaving your door's lock unfixed after someone breaks in.



- **Responsibility**:-There are two responsible parties after an attack: the attacker and the victim.
  - The attacker is responsible for the damage done, and the only way to bring him to justice is with good evidence to prove his actions.
  - The victim, on the other hand, has a responsibility to the community.
  - Information gathered after the attack can be examined and used by others to prevent further attacks.

**\*Collection options**:-Once a attack has been detected, you have two options:

1. **pull the system off the network and begin collecting evidence** or
2. **leave it online and attempt to monitor the intruder.**

-Both have their pros and cons.

-In the case of monitoring, you may accidentally alert the intruder while monitoring and cause him to wipe his tracks and it destroying evidence as he goes.

-If you disconnect the system from the network, you may find that you have insufficient evidence or, worse, that the attacker left a dead man and it destroys any evidence once the system detects that its offline.

**\*Types of Evidence** :-Before you start collecting evidence, it is important to know the different types of evidence categories.

-Without taking these into consideration, you may find that the evidence you've spent several weeks and quite a bit of money collecting is useless.

**-Any evidence that can stand alone and doesn't depend on other sources is considered real evidence.**

- **Real Evidence**:- Any evidence that can stand alone and doesn't depend on other sources is considered real evidence.
  - These pieces of evidence involve physical or real evidence such as flash drives, hard drives, documents, etc.
  - an eyewitness can also be considered as real evidence.
- **Testimonial Evidence**:-Testimonial evidence is any evidence supplied by a witness.
  - As long as the witness can be considered trustworthy, testimonial evidence can be almost as powerful as real evidence.
  - Word processor documents written by a witness may be considered testimonial—as long as the author is willing to state that he wrote it.
- **Hearsay**:-Hearsay is any evidence presented by a person who was not a direct witness.
  - Word processor documents written by someone without direct knowledge of the incident are hearsay.
  - Hearsay is generally Unacceptable in court and should be avoided.



- **Digital Evidence:**-It includes any kind of digital file from an electronic source.  
-This may be an email, text messages, instant messages, files, and documents extracted from hard drives, electronic financial transactions, audio files, and video files.

**\*Rules of evidence** (9 marks):-There are five rules for collecting electronic evidence they are ;

1. **Admissible:**-Admissible is the most basic rule.  
-The evidence must be able to be used in court.  
-otherwise It is the same as not gathering the evidence in the first place if this rule is broken.
2. **Authentic:**- You must be able to show that the evidence relates to the incident in a relevant way.
3. **Complete:**-It's not enough to collect evidence that just shows one side of the incident.  
-You collect not only evidence that can prove the attacker's actions, but also evidence that could prove their innocence.  
-For example, if you can show that the attacker was online at the time of the occurrence, you also need to show who else was online and why you believe they weren't responsible
4. **Reliable:**-The evidence you collect must be reliable.  
-Your evidence collection and analysis procedures must not cast doubt on the evidence's authenticity and veracity.  
Or  
-The methods you use for gathering and analysing evidence must not raise questions about its authenticity or reliability.
5. **Believable:**-The evidence you present should be clearly understandable and believable to a jury.  
-The presentation should be in a understandable form to the jury.

-Using the previous five rules, you can derive some basic do's and don'ts:

- Minimize handling and corruption of original data:-Once you've created a master copy of the original data, don't touch it or the original.  
-Any alterations made to the originals will have an impact on the results of any study performed later on copies.
- Account for any changes and keep detailed logs of your actions:-Sometimes evidence alteration is unavoidable.  
-In these cases, it is absolutely essential that the **nature, extent, and reasons** for the changes be documented.





- Comply with the five rules of evidence:-The five rules are there for a reason.  
-If you don't follow them, you are probably wasting your time and money.  
-Following these rules is essential to guaranteeing successful evidence collection.
- Do not exceed your knowledge:-If you don't understand what you are doing, Any modifications you make are not changeable and you can't describe what exactly you did.  
-If you ever find yourself "out of your depth," either go and learn more before continuing (if time is available) or find someone who knows the territory.
- Be prepared to testify:- If you're not willing to testify to the evidence you have collected, you might as well stop before you start.
- Work fast:-The faster you work, the less likely the data is going to change.  
-Volatile evidence may vanish entirely if you don't collect it in time.  
-This is not to say that you should rush.  
-You must still collect accurate data
- Proceed from volatile to persistent evidence:-Always try to collect the most volatile evidence first.
- Don't shut down before collecting evidence:-You should never, ever shutdown a system before you collect the evidence.  
-Not only do you lose any volatile evidence, but also the attacker may have trojaned the startup and shutdown scripts, plug-and-play devices may alter the system configuration, and temporary file systems may be wiped out.
- Don't run any programs on the affected system :-The attacker may have left trojaned programs and libraries on the system; you may accidentally trigger something that could change or destroy the evidence you're looking for.  
-Any programs you use should be on **read-only media**.

**\*General procedure** :-When collecting and analyzing evidence, there is a general four-step procedure to follow they are;

1. **Identification of Evidence**:-You must be able to distinguish between evidence and junk data.  
-For this purpose, you should know **what the data is, where it is located, and how it is stored**.  
-Once this is done, you will be able to work out the best way to retrieve and store any evidence you find.
2. **Preservation of Evidence**:-The evidence you find must be preserved as close as possible to its original state.  
-Any changes made during this phase must be documented and justified.



3. **Analysis of Evidence**:-The stored evidence must be analyzed to extract the relevant information and recreate the chain of events.
  - Analysis requires in-depth knowledge of what you are looking for and how to get it.
  - Always be sure that the person or people who are analyzing the evidence are fully qualified to do so.
4. **Presentation of Evidence**:-The manner of presentation is important, and it must be Understandable for everyone.

**\*Collection and Archiving**:- identified the evidence that needs to be collected, it's time to start the actual process of capturing the data.  
-Storage of that data is also important.

- **Logs and Logging**:-You should run some kind of system logging function.
  - It is important to keep these logs secure and to back them up periodically.
  - Messages and logs from programs can be used to show what damage an attacker did.
- **Monitoring**:-By monitoring we can gather statistics, watch out for irregular, and trace where an attacker is coming from and what he is doing.
  - Unusual activity or the sudden appearance of an unknown user.
  - Monitoring logs show you important information you might have missed and you can see them separately.

**\*Methods of collection** :-There are two basic forms of collection:

- **freezing the scene** and
- **honeypotting**.

-The two aren't mutually exclusive.

-You can collect frozen information after or during any honeypotting.

1. **freezing the scene** :-Freezing the scene involves taking a snapshot of the system in its **compromised state**.
  - Make sure the programs and utilities used to collect the data are also collected and stored on the same medium as the data.
  - All data collected should have a **cryptographic message digest** created ,and those digests should be compared to the originals for verification.
2. **honeypotting**:-Honeypotting is the process of creating a replica system and drawing the attacker into it for further monitoring.
  - so he can be monitored without (much) further damage.
  - The placement of misleading information and the attacker's response to it is a good method for determining the attacker's motives.
  - You must make sure that any data on the system related to the attacker's detection and actions is either removed or encrypted.
  - otherwise they can cover their tracks by destroying it.



**\*Artifacts:**-Whenever a system is compromised, there is almost always something left behind by the attacker—be it

- code fragments,
- trojaned programs,
- running processes, or
- sniffer log files.

-These are known as artifacts.

-They are one of the important things you should collect, but you must be careful.

-You should never attempt to analyze an artifact on the compromised system.

-Artifacts are capable of anything, and you want to make sure their effects are controlled.

-Artifacts may be difficult to find.

-Analysis of artifacts to finding other systems that the attacker (or his tools) has compromised.

**\*Collection steps:**- following are the collection steps:

- Find the evidence.
- Find the relevant data.
- Create an order of volatility.
- Remove external avenues of change.
- Collect the evidence.
- Document everything

1. **Find the evidence:**-Determine where the evidence you are looking for is stored.

-Use a checklist.

-Not only does it help you to collect evidence, but it also can be used to double-check that everything you are looking for is there.

2. **Find the relevant data:**-Once you've found the evidence, you must figure out what part of it is relevant to the case.

- Don't spend hours collecting information that is obviously useless.

3. **Create an order of volatility:**-The order of volatility for your system is a good guide and makes sure you don't lose a lot of uncorrupted evidence.

4. **Remove external avenues of change:**-It is essential that you avoid modification to the original data.

-Preventing anyone from tampering with the evidence.

5. **Collect the evidence:**-You can now start to collect the evidence using the appropriate tools for the job.

6. **Document everything:**-Your collection procedures may be questioned later, so it is important that you document everything you do.

-Timestamps, digital signatures, and signed statements are all important.



-Don't leave anything out.

**\*Controlling contamination** (3) :-Once the data has been collected, it must be protected from contamination.

-Originals should never be used in forensic examination; verified duplicates should be used.

-This not only ensures that the original data remains clean, but also enables examiners to try more dangerous, potentially data-corrupting tests.

-A good way of ensuring that data remains uncorrupted is to keep a chain of custody.

-This is a detailed list of what was done with the original copies once they were collected.

-Remember that this will be questioned later on, so document everything (who found the data, when and where it was transported [and how], who had access to it, and what they did with it).

-But it is necessary to prove your case.

- Analysis:-Once the data has been successfully collected, it must be analyzed the evidence you wish to present and attempt to reconstruct what actually happened.

-As always, you must make sure that you fully document everything you do.

- Time:-To reconstruct the events that cause to your system being corrupted.

-And create a timeline.

-This can be particularly difficult when it comes to computers.

-**Clock drift, delayed reporting, and differing time zones** can create confusion.

-One thing to remember is to never, ever change the clock on an affected system.

- Forensic Analysis of Back-ups:-When analyzing backups, it is best to have a dedicated host for the job.

-This examination host should be secure, clean and isolated from any network.

-You don't want it tampered with while you work.

**\*Reconstructing the attack**:-After collecting the data.

-And attempt to reconstruct the chain of events leading to and following the attacker's break-in.

-All of the evidence we have obtained has to be connected.

-Include all of the evidence we've found when reconstructing the attack no matter how small it is.



## #Conducting Digital Investigation

→ **steps for conducting a complete and qualified digital investigation are** (3 marks):-

1. **Preparation**:-creating a strategy for carrying out an effective digital investigation and obtaining materials and resources in support of it.
2. **Survey/Identification**:-The identification process mainly includes things like what evidence is present, where it is stored, and lastly, how it is stored.  
-During this stage, it is essential to document the evidence, where it is stored, and the format in which it is stored.
3. **Preservation**:-In this phase, data is isolated, secured, and preserved.  
-It includes preventing people from using the digital device so that digital evidence is not tampered with.
4. **Examination and Analysis**:-Examination is the process of Identifying relevant information and finding more related hints from this information.  
-In Analysis, All relevant digital data is examined during this stage, and the most relevant parts are analyzed and extracted.  
-This relevant information is converted into a format one can use to present to the stakeholders or the court.
5. **Presentation**:-The investigator plays the role of a presenter and provides graphs, reports, and visual aids for the further investigation process.

**\*Digital investigation process models** (9 marks) :-Following are the different types of Digital investigation process models.

- **Physical Model** :-A computer under investigation may be viewed as a subset of the actual crime scene.  
-Physical evidence may exist around a server that was attached by an employee and evidence might be found in a home computer that is being used illegally.  
-Furthermore, the end goal of most digital investigation is to identify a person who is responsible.  
-and therefore There must be a connection between the digital and physical investigations.



-Phases of digital and physical investigations in digital investigation process model.

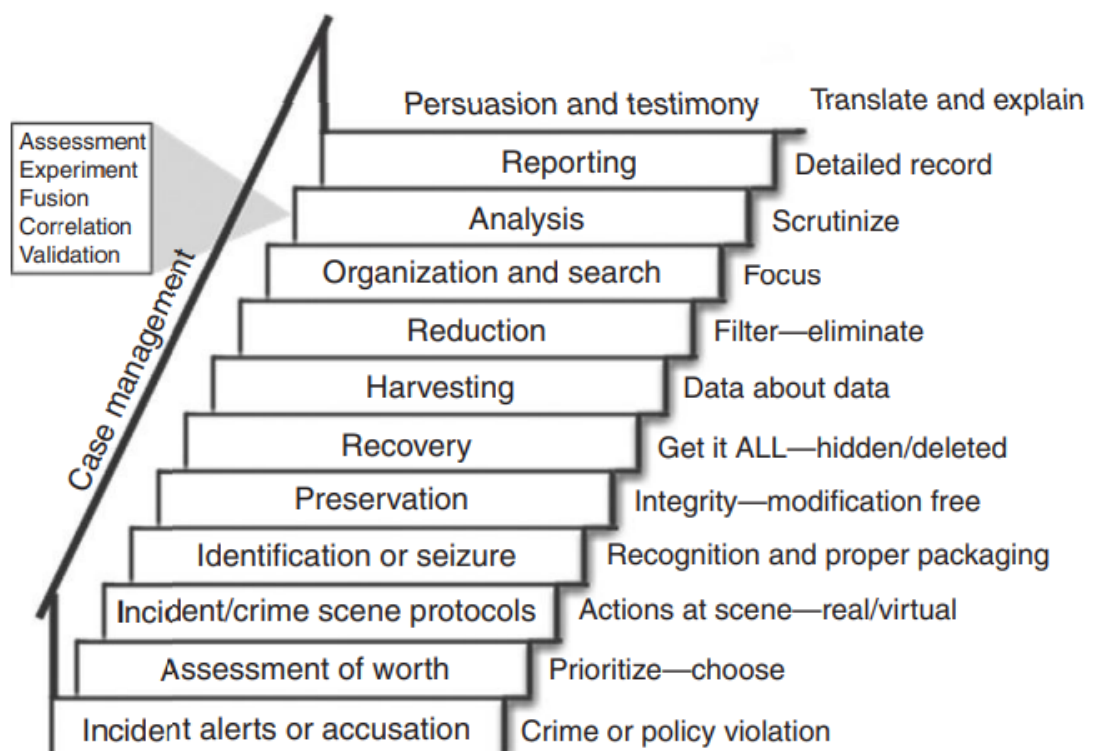
	Phase Goals (Physical)	Phase Goals (Digital)
Crime scene preservation	Securing entrances and exits and preventing physical changes to evidence	Preventing changes in potential digital evidence, including network isolation, collecting volatile data, and copying entire digital environment
Crime scene survey	Walking through scene, identifying obvious and fragile physical evidence	Identification of obvious evidence by searching in digital evidence (typically in lab)
Crime scene documentation	Photographs, sketches, maps of evidence, and crime scene	Photographs of digital devices and individuated descriptions of digital devices
Crime scene search and collection	In-depth search for physical evidence	Analysis of system for nonobvious evidence (typically in lab)
Crime scene reconstruction	Developing theories based on analysis results and testing against evidence	

- **Staircase Model** :-it provides a practical and orderly approach to conducting an effective digital investigation .

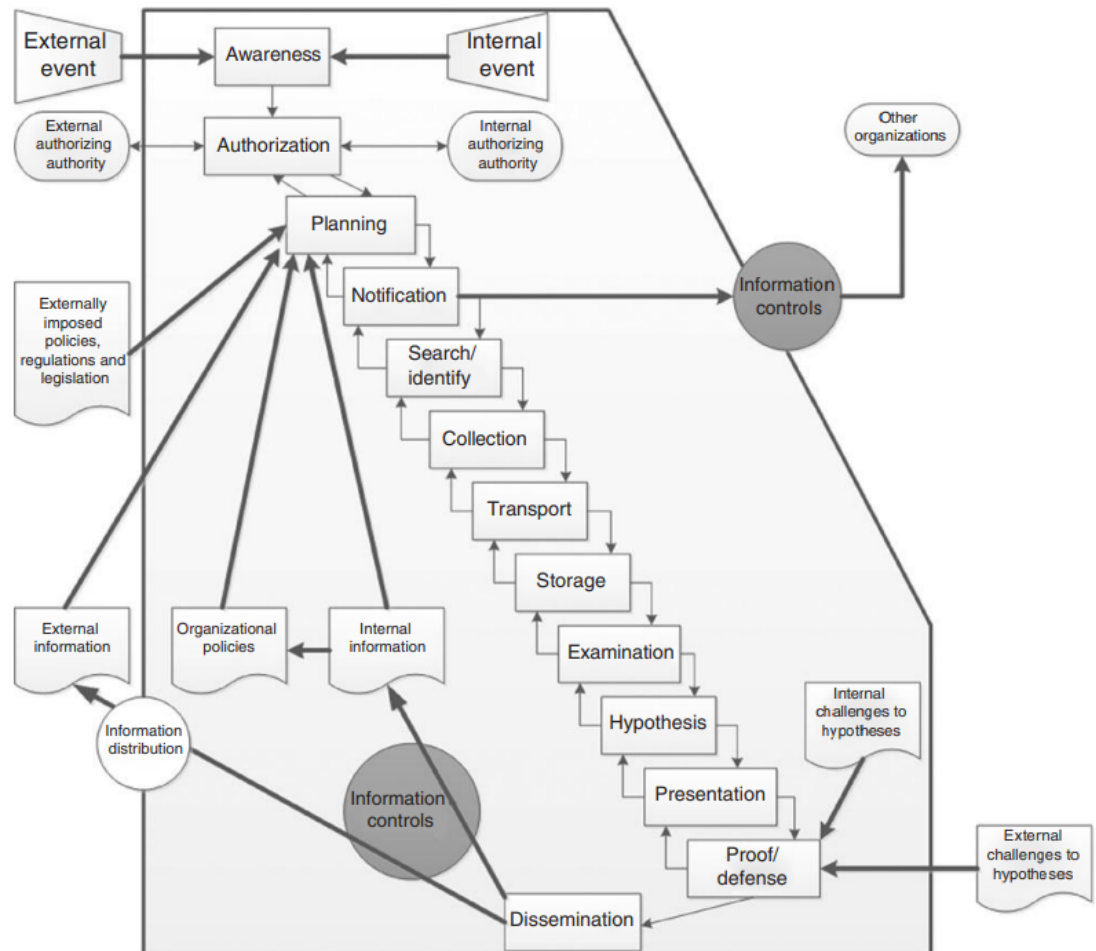
-Digital investigators, forensic examiners, and attorneys work

together to scale these steps from bottom to top in an orderly manner.

-This model can be represented as;



- **Evidence Flow Model** :-This model covers nontechnical parts of a digital inquiry, such as authorization, notification, proof/defense, and evidence transportation evidence.  
-The main goal of this model is to completely describe the flow of information in a digital investigation, as soon as digital detectives are alerted until the investigation reaches its conclusion.



- One weakness of this model is that it ignore certain steps that are present in other models such as the return or destruction of evidence at the end of an investigation.
- Furthermore, the terms used to describe each step are not clearly defined, making it difficult to compare with other models.
- because It ignore the preservation step present in other models because it is not considered necessary or because it is treated as part of the collection process.
- A further limitation of this model is that it does not define basic requirement or goals of each step in an investigation.

- **Subphase Model** :-The top-level steps used in this model are preparation, incident response, data collection, data analysis, findings presentation, and incident conclusion.  
-The three goal-based subphases of the analysis process are survey, extract, and examine.



- following are the goal for file system analysis:

- Reduce the amount of data to analyze.
- Determine the skill level of the suspect.
- Recover deleted files.
- Find relevant hidden data.
- Determine chronology of file activity.
- Recover relevant **ASCII** data.
- Recover relevant **non-ASCII** data.
- Find out about past non-email activities on the Internet.
- Recover relevant e-mail and attachments
- Recover relevant “personal organizer” data  
(e.g., calendar, address books, etc.)
- Recover printed documents.
- Identify relevant software applications and configurations
- Find evidence of unauthorized system modification (e.g., Trojan applications)

-The analysis of digital evidence is more commonly viewed as a separate process.

-To assist investigators in carrying out each step correctly, the idea of objectives-based subphases might be used to an existing high-level investigation process model rather than trying to create new terminology or modify the high-level procedures.

- **Roles and Responsibilities Model** :-By offering a framework of roles and responsibilities in digital investigations, the **FORZA model** reaches an even higher level of abstraction.

-The goal of this framework is to address not just the technical aspects of a digital investigation but also the legal and managerial issues.

- Fundamentally, the FORZA model defines eight roles and six fundamental questions that each role must handle in an investigation: **who, what, how, when, where, and why**.

**\*Scaffolding for digital investigations** (9 marks):-When comparing the process models , There are number of differences that are not explained in the terminology or how the investigative process has been examined.

-These differences, which include authorization and transportation, might be of different viewpoint, and are related to non investigative occurrences.

-Although such occurrences and activities are not central to digital investigations.

-They provide necessary scaffolding to help build a solid case.

-This scaffolding also includes accusation/alert, threshold considerations, and case management.





-Scaffolding focuses on 6 aspects they are:

1. **Accusation or Incident Alert** :-In This step a signal formed by an alarm from an intrusion detection system,a system administrator reviewing firewall logs, or some combination of indicators from multiple security sensors installed on networks and hosts.
  - Then an accusation or automated incident alert is present , it is necessary to consider the source and reliability of the information.
  - If someone reports harassment because of continuously inappropriate messages showing up on their screen, it's possible that they are dealing with a computer virus or worm.
  - An warning from an intrusion detection system might simply be a false alarm, it could represent an attempt or it might be a failed attack.
  - Therefore, it is necessary to weigh the strengths, weaknesses, and other known factors related to the sources .
  - In addition, analyzing an accusation or alert thoroughly, some initial facts must be gathered because it is necessary before launching a full-blown investigation.
2. **Authorization** :- Before approaching digital evidence, it is important to be certain that the search is not going to violate any laws.
  - Because there are strict privacy laws protecting certain forms of digital evidence like stored e-mail.
  - If laws are violated, the evidence can be weakened or suppressed.
  - Because errors in this step can put the entire investigation at risk.
  - Requesting authorization is the best way to stay on the side of safety.
3. **Threshold Consideration** :- investigative activities are usually busy with multiple cases or having high priority duties that required more attention.
  - digital investigators must establish thresholds in order to prioritize cases and make decisions about how to allocate resources.
  - Threshold considerations vary for each investigation based on their environment.
  - In civil, business, and military operations, suspicious activity will be investigated but **policy, regulations, and continuity of operations** may be the primary concern.
4. **Transportation** :- Moving evidence from the crime scene to the forensic laboratory or from one laboratory to another contains a significant amount of threats, because it can cause loss from confidentiality to destruction of evidence.
  - One should keep in mind that rarely gets a second chance to re-collect evidence that has been lost.
  - When organising the transfer of evidence, investigators have to take care of the evidence.
  - And make evidence copies and share it with other experts.



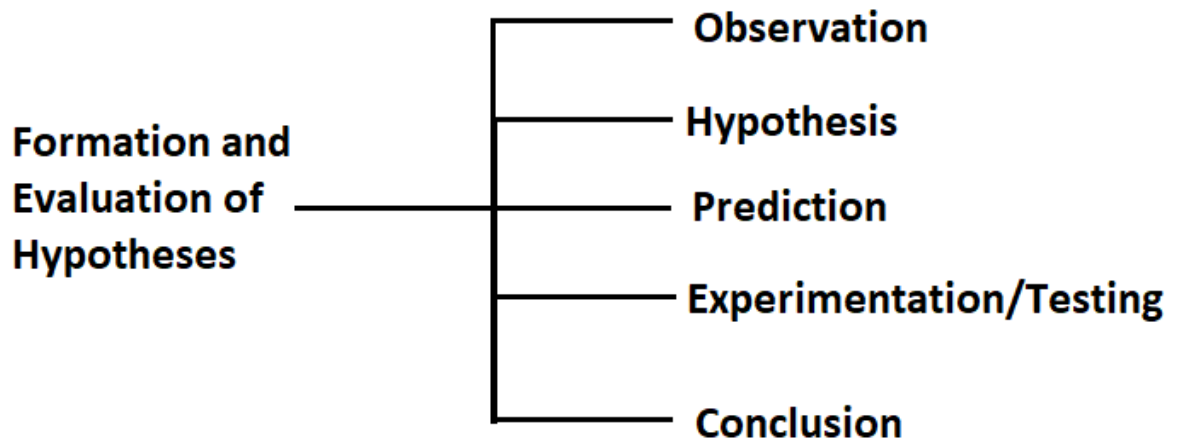
5. **Verification** :- Reviewing the information gathered in the survey phase for mistakes or mistakes can be avoid.
  - Evaluation of the correctness and completeness of obtained data as well as documentation for its integrity.
  - It is also necessary to verify that the results of forensic examination and analysis are correct.
  - verification include **hash comparison, comparing results of multiple tools, checking data at a low level, and peer review.**
6. **Case Management** :-Case management plays a vital role in digital investigations, connecting all of the activities and results together.
  - The purpose of effective case management is to ensure that a digital investigation proceeds smoothly and that all relevant information resulting from each step of the process is captured, documented, and connected together to create a clear and compelling picture of the incident.
  - The success of a digital investigation is heavily dependent on case management.
  - Without efficient case management **methods and supporting tools**, investigative opportunities may be missed,digital evidence may be overlooked or lost, and important information may not be uncovered.

**\*Applying scientific method in Digital investigations** :-The process models that define each step of an investigation can be useful for certain purposes, such as developing procedures.

- But they are too complex and strict to be followed in every investigation.
- All steps of the investigative process are frequently combined and After gaining a greater understanding of the case, a digital investigator might need to go back and review certain procedures.
- Preparation is needed at every step of an investigation.
- In addition, while identifying all potential sources of digital evidence, it may be necessary to preserve certain items immediately before volatile data are lost.
- The scientific method provide a simple, flexible methodology.
- The scientific method begins with **fact gathering and validation**, and gives to **hypothesis formation and experimentation/ testing** , for searching for evidence.

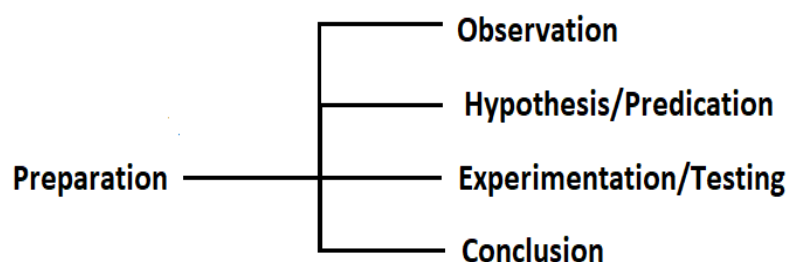
1. **Formation and Evaluation of Hypotheses**:-At each stage of the investigative process a digital investigator is trying to get answers for specific questions and accomplish certain goals relating to the case.
  - These questions and goals will drive the overall digital investigation process.
  - Therefore, it is important for digital investigators to have a robust and repeatable methods within each step to help them accomplish the goals and questions that are necessary to solve the case.





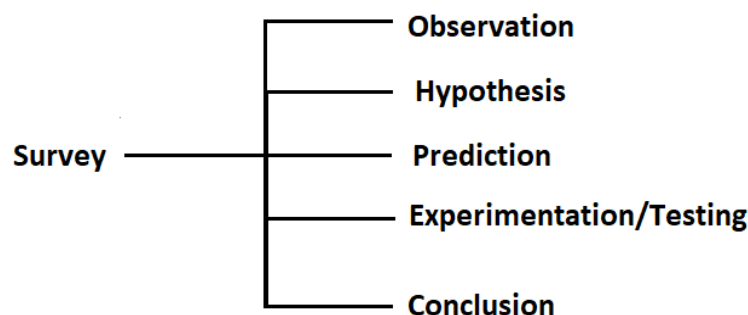
- Observation :- One or more events (incident) will occur, that cause suspicion and that lead you to start an investigation.
  - Digital investigators will use these details as a starting point for their investigation.
  - For Example, a user may have seen that, after visiting a certain website, their web browser crashed and an antivirus warning was immediately generated.
- Hypothesis :-Based on the current facts of the incident,Digital investigators will develop a hypothesis (theory) on what may have happened.
- Prediction :-Based on the hypothesis, digital investigators will then predict the possible location of the evidence related to the event.
- Experimentation/Testing :- Digital investigators will then analyze the available evidence to test the hypothesis, looking for the presence of the predicted artifacts.
- Conclusion :-Digital investigators will then form a conclusion based upon the results of their findings.
  - A digital investigator may have found that the evidence supports the hypothesis or there were not enough findings to generate a conclusion.

2. **Preparation**:-The general aim of preparing for a digital investigation is to create a plan to perform an effective digital investigation.
  - And get the staff and resources that are required.
  - When preparing to execute a search warrant,Digital investigators will create a plan where exactly to look and what are the expected evidence items to find.
  - An example of applying the scientific method to preparation for the preservation step of a digital investigation is provided here:



- Observation:-gathering information about the crime scene in order to estimate the quantity and kind of computer equipment that have been used, and whether full disk encryption is in use.
  - Interviewing persons who are familiar with the area to be searched might be part of this step.
  - Covert surveillance may be necessary for this observation procedure in situations where inside information is not easily accessible.
- Hypothesis/Predication:-Based on the information gathered about the crime scene,
  - digital investigators will form theories about the types of computer systems and internal components such as hard drive capacity and its interface.
- Experimentation/Testing:-It may be possible to test some predictions about what will or will not be found at the crime scene.
- Conclusions:-The outcome of this process should be a strong plan for preserving evidence at the crime scene.
  - For some cases ,Digital investigators must also get ready to process digital evidence while on the scene.
  - Digital investigators are not allowed to gather information from every computer system, thus in order to determine which systems are relevant to the research, some on scene keyword searches on multiple computers must be done.

3. **Survey**:-With a plan prepared from the preparation step, The digital investigators can easily recognize digital evidence at the crime scene.
- The aim of the process is to find all potential sources of evidence.

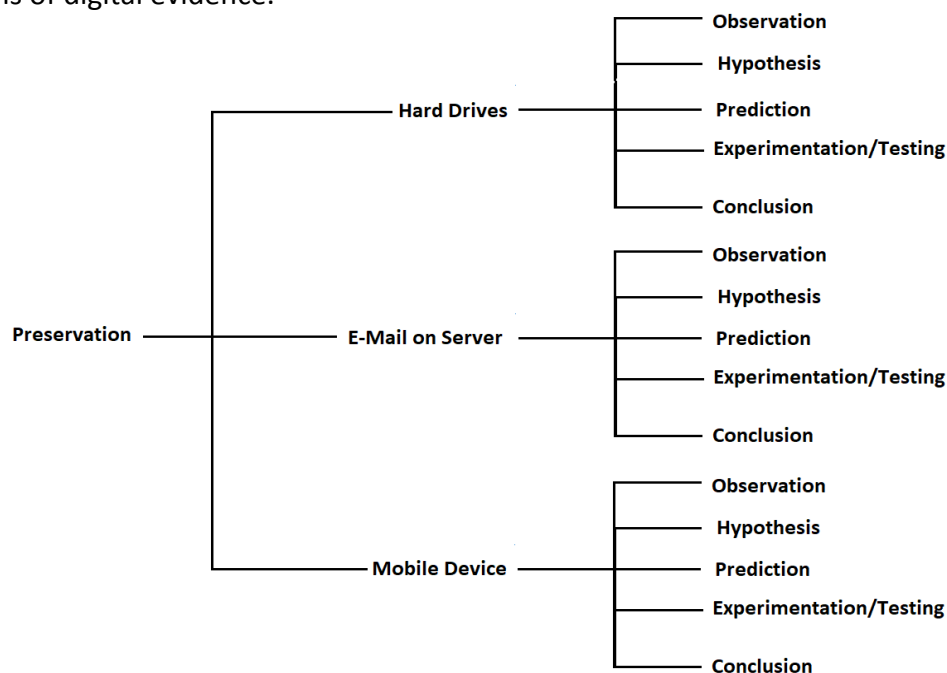


- Observation:-To uncover unexpected items as well as the expected ones, an in-depth investigation of the crime scene should be conducted.
- Hypothesis:-Theories should be developed about why certain expected items are not present, and why certain unexpected items were found.



- Prediction:- contain an Ideas about where missing items may be found.
  - And Determine which items may contain relevant data.
  - When large quantities of computers or removable media are involved, it may be necessary to develop theories about which ones do and do not contain relevant digital evidence.
- Experimentation/Testing:-When digital investigators believe that certain items are not relevant to the case, some experimentation and testing is needed to confirm it.
- Conclusions:-Based on the available information,There is a high level of confidence that every important source of digital evidence that has been preserved and identified.

4. **Preservation**:-investigators must make sure that potentially volatile items are collected or obtain it in their current state.
- Take proper actions to ensure the integrity of evidence, physical and digital.
  - The accuracy and reliability as well as professional acceptance may be questioned by opposing counsel.
  - In digital forensics, the preservation step is where digital forensics begins.
  - The output of this stage is usually a set of duplicate copies of all sources of digital data.
  - This output provides investigators with two categories they are;
    - First, the original material is documented and stored in a proper environmentally controlled location, in an unmodified state.
    - Second, an exact duplicate of the original material is created that will be analyzed as the investigation continues.
  - Consider examples of the scientific process applied to the preservation of common forms of digital evidence.



### ➤ Hard Drives

- Observation :-A hard drive has a SATA interface with a certain number of sectors documented on the label.
- Hypothesis :-A complete and accurate duplicate of the hard drive can be obtained without altering the original.
- Prediction :-The duplicate will have the same hash value as the original hard drive.
- Experimentation/Testing :- Comparing the hash value of the forensic duplicate with that of the original hard drive confirms that they are the same.
  - However, when comparing the size of the forensic duplicate with the capacity of the hard drive shows an imbalance.
  - And we need to examine the disk to find the imbalance.
- Conclusions :- There is a high level of confidence that all of the data on the hard drive was accurately duplicated.

### ➤ E-Mail on Server

- Observation :- E-mail is stored on a server, including 30 days of deleted messages.
- Hypothesis :-With the least amount of damage to the server, mails belonging to the people who are in the search can be extracted to generate an exact and full duplicate of all relevant emails.
- Prediction :-The resulting copies of mailboxes will contain all relevant e-mail.
- Experimentation/Testing :- To be sure that mails removed in the last 30 days were not captured by the search technique, more testing is required to find messages that were deleted over 30 days before.
- Conclusions :- There is a high degree of confidence that all available e-mail, including deleted items, was accurately with minimal disruption to the server.

### ➤ Mobile Device

- Observation :-Mobile device has a digital camera that can take photographs and videos
- Hypothesis :-A complete and accurate duplicate of photographs and videos on the mobile device can be obtained with minimal alteration of the original device.
- Prediction :-All the photos and videos will be captured in the forensic investigation.



- Experimentation/Testing :-The data obtained from the mobile device contain two photographs and one video, whereas a manual examination of the device shows many more photographs and videos were not obtained.  
-Further testing is needed to capture multimedia stored outside of the default storage folder.
- Conclusions :- There is a high level of confidence that complete and accurate duplicates of all the photographs and videos were captured from the mobile device and removable storage card .

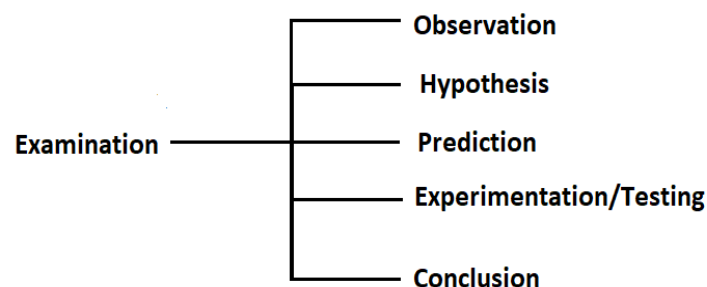
5. **Examination**:-Forensic examination is the process of extracting and viewing information from the evidence, and making it available for analysis.

-Forensic examination of digital evidence is generally one of the most resource intensive and time-consuming steps in a digital investigation.

-To produce useful results in a timely manner we use a three levels of forensic examination they are;

- ★ **survey/triage forensic inspections**:-Targeted review of all available media to determine which items contain the most useful evidence and require additional processing.
- ★ **preliminary forensic examination**:-items identified during survey/triage as containing the most useful evidence.  
-It quickly gives the detectives the evidence they need to conduct interviews and generate leads.
- ★ **in-depth forensic examination**:-For full forensic examination of items that require deep investigation to gain a more complete understanding of the crime.

-The scientific method applied during the forensic examination process is provided here.



- Observation :- A hard drive contains documents that are relevant to the Investigation.
- Hypothesis :- All documents are stored in Microsoft Office formats, predominantly Word and Excel.



- Prediction :- Extracting all documents will result in for analysis.
- Experimentation/Testing :- other file types in the hard drive which was compressed (.ZIP files) contain many documents that were not extracted originally.
  - Further examination finds relevant documents in unsearchable formats, including PDF etc.
- Conclusions :-There is a high level of confidence that the production of documents obtained from the hard drive are complete and accurate.

6. **Analysis:-**The forensic analysis process is in-separable from the scientific method.

-forensic analysis is the application of the scientific method and It contain critical questions for an investigation like who, what, where, when, how, and why.

-This step involves the detailed study of data identified, preserved, and examined throughout the digital investigation.

-Following are the subcategories of analysis ;

- Observation :-Digital data items that may be viewed or read by humans have visible content and reconstructed context.
  - That content and context of digital evidence may contain information that is used to reconstruct events relating to the offense and to determine factors such as means, motivation, and opportunity.
- Hypothesis :- Develop a theory to explain digital evidence.
- Prediction :- Based upon the hypothesis, digital investigators will then predict where they believe the trace of that event will be located.
- Experimentation/Testing :- Determine whether or not digital evidence is compatible with the working theory.
  - Eventually, experimentation leads to falsification or general acceptance.
- Conclusions :- There is a high level of confidence that all of the data has been analysed.

7. **Reporting and testimony:-**To provide a transparent view of the investigative process, final reports should contain important details from each step, including reference to protocols followed.

- and methods used to seize, document, collect, preserve, recover, reconstruct, organize, and search key evidence.

-The majority of the report generally leading to conclusion and descriptions of the supporting evidence.

-Writing a conclusion without providing an in-depth summary of the investigation and supporting evidence is not appropriate.





## #Computer Basics for Digital Investigators

**\*Basic Operation of Computers** (9 marks) :-Each time a computer is turned on, it must connected with its internal components and the peripheral world.

-This start-up process is called the **boot process**.

-Because it is a process of switching on the computer and starting the operating system.

-The boot process has three basic stages:

1. **Central processing unit (CPU) reset,**
2. **Power-on self-test (POST),**
3. **Disk boot.**

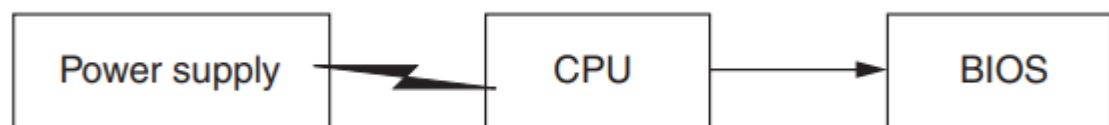
- **central processing unit (CPU) :-** The CPU is the core of any computer.

-Everything depends on the CPU's ability to process instructions that it receives.

-So, the first stage in the boot process is to get the CPU started—reset—with an electrical pulse.

-This pulse is usually generated when the power switch or button.

-Once the CPU is reset, it starts the computer's basic input and output system (BIOS)



- **Basic Input and Output System (BIOS) :-** The BIOS deals with the basic movement of data around the computer.

-Every program run on a computer uses the BIOS to communicate with the CPU.

-Some BIOS programs allow an individual to set a password, and then, until the password is typed in, the BIOS will not run and the computer will not Function.

- **POST and CMOS Configuration Tool:-** The BIOS contains a program called the POST that tests the fundamental components of the computer.

-When the CPU first activates the BIOS, the POST program is initiated.

-For the safe, the first test verifies the integrity of the CPU.

-Then The rest of the POST verifies that all of the computer's components are functioning properly, including the disk drives, monitor, RAM, and keyboard.

-After the BIOS is activated and before the POST is complete, Intel-based computers allow the user to open the complementary metal oxide silicon (CMOS) configuration tool at this stage.

-Computers use CMOS RAM chips to retain the date, time, hard drive parameters, and other configuration details while the computer's main power



is off.

-A small battery powers the CMOS chip.

- **Disk Boot** :- A boot disk is a removable data storage medium used to load and boot an operating system.

-One of the most common uses of a boot disk is to start the computer when the operating on the internal hard drive does not load. Generally, a boot disk contains a full-scale operating system.

-A boot disk may also be referred to as a bootable diskette, startup disk, bootable disk or bootable rescue disk.

-A boot disk could be any of several different types of media, including a CD-ROM, a DVD-ROM, a flash drive, an external Firewire hard drive, or a floppy disk.

**\*Representation of Data** (9) :-All digital data are basically combinations of ones and zeros, commonly called **bits**.

-Data Representation refers to the form in which data is stored, processed, and transmitted.

-In order to store the data in digital format, we can use any device like computers, smartphones, and iPads.

-**Digitization** is a type of process in which we convert information like photos, music, number, text into digital data.

-Electronic devices are used to manipulate these types of data.

-The binary digits or bits are used to show the digital data, which is represented by 0 and 1.

-The main use of binary digit is that it can store the information or data in the form of 0s and 1s.

Characters	ASCII Value
A - Z	65 - 90
a - z	97 - 122
0 - 9	48 - 57
Special Symbol	0 - 47, 58 - 64, 91 - 96, 123 - 127

→**File Formats and Carving**:-A file format is a standard way of storing data on a computer file.

-There are multiple types of file formats present which can be used to store and retrieve data efficiently.

-For example , a graphics file format such as JPEG has a completely different structure from Microsoft Word Documents.



-The headers and footers for some common file types are listed below

File Type	Header	Footer
JPEG	Usually FF D8 FF E0 or FF D8 FF E1 and sometimes FF D8 FF E3	FF D9
GIF	47 49 46 38 37 61 or 47 49 46 38 39 61	00 3B
Microsoft Office	D0 CF 11 E0 A1 B1 1A E1	N/A

-The common headers in a JPEG image, Word document, and other file types are often referred to as file signatures.

-And can be used to locate and restore portions of deleted files.

-The process of searching for a certain file signature and attempting to extract the associated data is called “carving”.

Or

-Extracting data (file) out of undifferentiated blocks (raw data) is called carving.

-Identifying and recovering files based on analysis of file formats is known as file carving.

-In Cyber Forensics, carving is a helpful technique in finding hidden or deleted files from digital media.

## \*Storage Media

→**Storage Media** :-A storage device is a kind of hardware, which is also known as storage, storage medium, digital storage, or storage media that has the ability to store information either temporarily or permanently.

-It can be used either internally or externally to a computer system.

-For any computing device, a storage device is one of the core components that is available in several structures and sizes on the basis of requirements and functionalities.

-A computer would be considered a dumb terminal without a storage device.

-It cannot store or hold any type of information or settings if it has no storage device.

-Although your computer can run without storage media.

-Example of storage media are;

★ Floppy Disk: Floppy Disk is also known as a floppy diskette.

-It is generally used on a personal computer to store data externally.

-A Floppy disk is made up of a **plastic cartridge** and secured with a protective case.

-Nowadays floppy disk is replaced by new and effective storage devices like USB, etc.

★ Hard Disk: Hard Disk is a storage device (HDD) that stores and retrieves data using magnetic storage.

-It is a non-volatile storage device that can be modified or deleted n number of times without any problem.

-Non-volatile means the data retains when the computer shuts down.



-Its main components include a read/write actuator arm, head actuator, read/write head, spindle, and platter.

-The disk is divided into tracks.

-Each track is further divided into sectors.

-The point to be noted here is that outer tracks are bigger in size than the inner tracks but they contain the same number of sectors and have equal storage capacity.

-The Read-Write head that performs all the read and writes operations on the disk.

-Most basic hard drives are made up of numerous disk platters, which are circular disks composed of aluminum, glass, or ceramic that are arranged around a spindle inside a sealed chamber.

-The platter is rotated by a motor attached to the spindle.

-The chamber also contains the read/write heads, which use a magnetic head to record information to and from tracks on the platters.

-The disks are additionally covered in a thin magnetic coating.

-The platters rotate at up to 15,000 rotations per minute by the motor.

-A second motor regulates the location of the read and write heads.

-Most computers and laptops have HDDs as their secondary storage device.

-It is actually a set of stacked disks.

-The read-write speed of HDDs is not so fast but decent.

-It ranges from a few GBs to a few and more TB.

★ Pen Drive: It is also known as a USB flash drive that includes flash memory with an integrated USB interface.

-We can directly connect these devices to our computers and laptops and read/write data into them in a much faster and more efficient way.

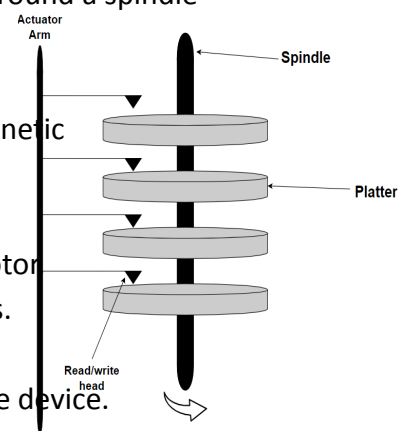
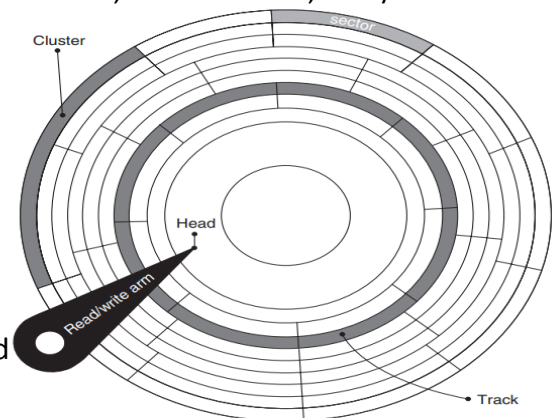
-These devices are very portable. It ranges from 1GB to 256GB generally.

★ CD: It is known as Compact Disc.

-It contains tracks and sectors on its surface to store data.

-It is made up of polycarbonate plastic and is circular in shape.

-CD can store data up to 700MB.



**\*File Systems** :- A file system defines how files are named, stored, and retrieved from a storage device.

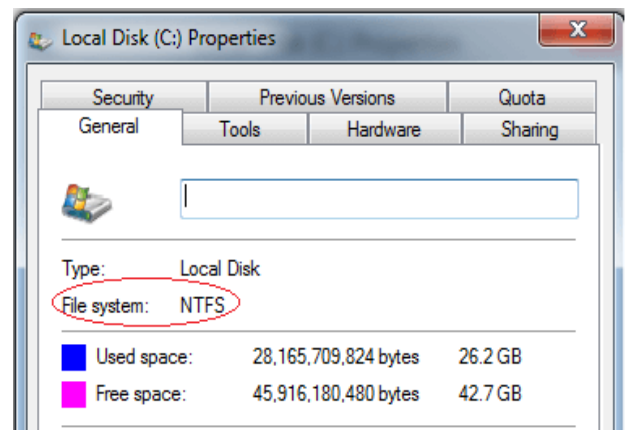
-Every time you open a file on your computer or smart device, your operating system uses its file system internally to load it from the storage device.

-There are various file systems with Windows, NTFS is the most common in modern times.

-It would be impossible for a file with the same name to exist and also impossible to remove installed programs.

-The examples of file systems are given below:

- **FAT:** FAT is a type of file system, which is developed for hard drives.
  - it helps to manage files on Microsoft operating systems.
  - FAT is not used by later versions of Microsoft Windows like Windows XP, Vista, 7, and 10 as they use NTFS.
  - The FAT8, FAT12, FAT32, FAT16 are all the different types of FAT.



- **NTFS (New Technology File System):** A modern file system used by Windows.
  - It supports features such as file and folder permissions, compression, and encryption.
- **GFS:** A GFS is a file system, which stands for Global File System.
  - It has the ability to make enable multiple computers to act as an integrated machine.
  - When the physical distance of two or more computers is high, and they are unable to send files directly with each other, a GFS file system makes them capable of sharing a group of files directly.
- **ext (Extended File System):** A file system commonly used on Linux and Unix-based operating systems.
- **HFS (Hierarchical File System):** A file system used by macOS.

**\*Dealing with Password Protection and Encryption** (9 marks) :-Two of the greatest difficulty that investigators face today are password protection and encryption.

-Dealing with password protection can be the easier task.

-A variety of tools are available for obtaining or guessing passwords on different file types.

-Two of the most powerful password recovery programs currently available are;

- **Password Recovery Toolkit (PRTK)**
- **DNA from Access Data.**

-The PRTK can recover passwords from many file types and is useful for dealing with encrypted data.



- Encryption is a general term for encoding information.
- Theoretical, encryption locks data with a key and only people with the appropriate key can unlock the data.
- Encryption can be broken using specialized knowledge and equipment.
- But, in many cases, it is not possible to expect the required resources to break encryption.
- Encryption is a process by which a readable digital object (plaintext) is converted into an unreadable digital object (ciphertext) using a mathematical function.
- However, there are simple, keyless encoding systems.
- For Example , **ROT13** is a simple code that substitutes each letter in the plaintext message with the letter that is 13 letters farther along in the alphabet .
- So, a becomes n, b becomes o, etc.
- ROT13 is commonly used in news to mask potentially offensive content and allowing the reader to decrypt the message.
- Another reason to use ROT13 is to disorder the email addresses in a message to make it more difficult for Internet spammers to reap the addresses.



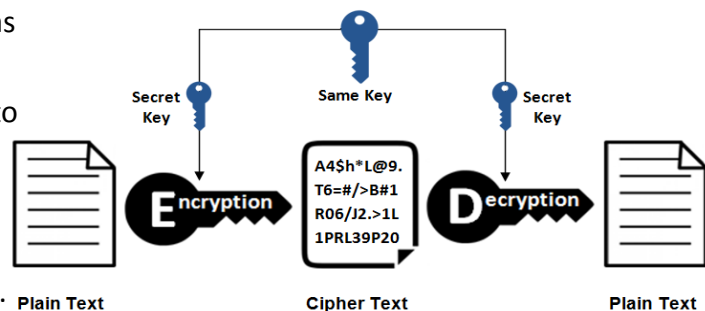
→**Private Key Encryption** :-Private key encryption is a straightforward.

- The same key that is used to encrypt a message is also used to decrypt it.
- Without the key, it is very difficult to unlock the data. **Symmetric Encryption**

-Private key cryptography also known as **symmetric-key cryptography**.

- Private key encryption is widely used to secure communications over the Internet.

-because it ensures that only the intended person can read the message.



-One of the biggest limitations is key distribution.

-Since the same key is used for encryption and decryption, both the sender and receiver must have the key.

-This can be difficult to achieve, especially when communicating with multiple parties.

-To overcome this limitation, public key cryptography was developed.

-Public key cryptography, also known as **asymmetric key cryptography**, uses two keys (public and private) to encrypt and decrypt data.

-The public key is used for encryption and the private key is used for decryption.

-It allows users to communicate securely without sharing keys.



→ **Public Key Encryption** :- public-key Encryption, also known as **asymmetric-key cryptography**.

-Public key cryptography uses both public key and private key in order to encrypt and decrypt data.

-The public key can be distributed commonly but the private key can not be shared with anyone.

- **Public Key**: Public keys are designed to be public.

-They can be freely given to everyone or posted on the internet.

-By using the public key, one can encrypt the plain text message into the cipher text.

-In simple words, one can say that a public key is used for closing the lock.

- **Private Key**: The private key is totally opposite of the public key.

-The private key is always kept secret and never shared.

-Using this key we decrypt cipher text messages into plain text.

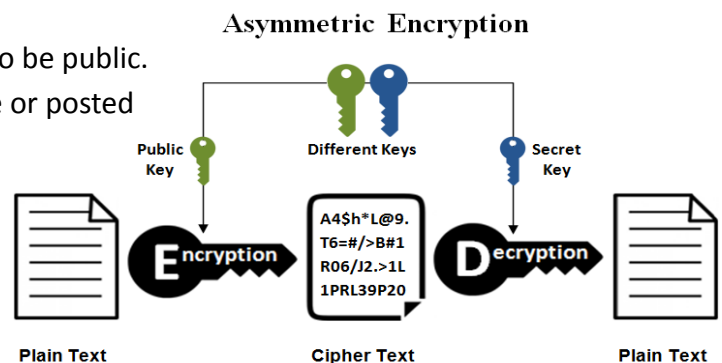
-In simple words, one can say that the private key is used for opening the lock.

-In symmetric-key cryptography, a single key is used to encrypt and decrypt the message.

-Here, the possibility of data loss or unauthorized access to data is high.

-To overcome the unauthorized access of data and data sent securely without any loss, we use public-key cryptography.

-Public-key cryptography is more secure than symmetric-key cryptography because the public key uses two keys to encrypt and decrypt the data.



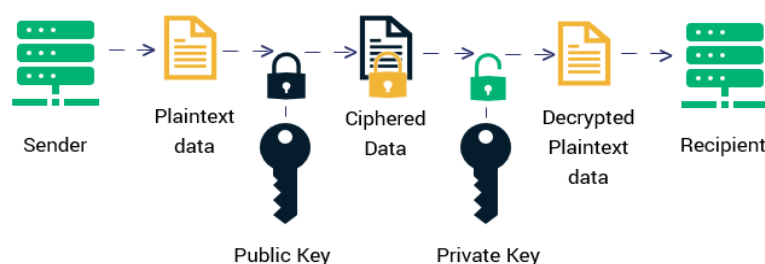
→ **Email Encryption** :- Email encryption involves encrypting the content of email messages in order to protect potentially sensitive information from being read by anyone other than intended person.

-Hackers use email to target victims and steal data, such as personal information like names, addresses, and login credentials, then commit crimes like identity theft or identity fraud.

-When sending an email with sensitive information, you can use encryption.

-Email encryption refers to plain text being converted into scrambled cipher text.

-The email can then only be read by the recipient that has the private key that will be used to decode the email.



**\*Log files** <sup>(3)</sup> :-Log files are a historical record of everything and anything that happens within a system, including events such as transactions, errors and intrusions.

-With proper log file tracking, businesses can either avoid errors within their operating systems.

-Smart log tracking reduces downtime and minimizes the risk of lost data.

-In the world of cybersecurity, log files are texts that provide security information about a system.

-The information includes IP address of the system, network address, computer name, and login data.

-Login data includes log in username, date and time of previous login and current login status.

-Security log files assist the system administrator to identify and detect any unauthorized login attempts.

-With information from the log files, the administrator is able to improve the security of the system.

-Log files are useful in post-error investigations.

-By using log files, you are able to determine the causes of a certain error or security breach.

-Additionally, you will be able to determine if the error was purposeful or accidental depending on the number of attempts to breach the security infrastructure.

-Log file allows you to control access to a particular resource.

-You can determine which systems can access resources such as printers, etc.

-Numerous attempts to breach your network security as recorded in the log files is an indication that you require a highly secure infrastructure.





## Module - 4

**#Cyber Crime** (9 marks) :- Cybercrime or a computer-oriented crime is a crime that includes a computer and a network.

- The computer may have been used in the operation of a crime or it may be the target.
- Cybercrime is the use of a computer as a weapon for committing crimes such as committing fraud, identity theft, or breaching privacy.
- Cybercrime may threaten a person or a nation's security and financial health.
- Any offenses committed against individuals or groups of individuals to harm the reputation or cause physical or mental trauma through electronic means can be defined as Cybercrime.
- Cybercrime can be carried out by individuals or organizations.
- Some cybercriminals are organized, use advanced techniques and are highly technically skilled.
- Others are Hackers with no experience.

→ **Roles of computer in cyber crime** :- Computers serve a major role in Cyber crime.

- This cybercrime is performed by a knowledgeable computer user who is usually referred to as a "**hacker**", who illegally browses or steals a company's information or a piece of individual private information and uses this information for malicious activity.
- In some cases, The attacker can destroy and corrupt data files.
- The role of a computer in the crime may vary depending upon the activity that a person does.
- For Example, a person may steal the details and misuse them on one hand, and on the other hand, a terrorist may use the information to do violent activities and some persons may steal financial information for trading purposes and so on.
- But all these activities can be done by a computer only.
- There are several examples of crime that use computers they are as follows:
  - **Malware creation**: The process of creating malware like viruses etc.
  - **Cybersquatting**: It is a process of gaining personal information and trying to resell them.
  - **Harvesting**: Here, hackers usually steal a person's private information from an account and use it for illegal activities.
  - **Wiretapping**: Here, the hacker connects a device to a phone line and tries to listen to the conversations.
- Thus a computer plays a role in criminal activity.

→ **Categories of cyber crimes**:-There are three major categories of cyber crimes:

1. **Crimes Against People / individual** :- These crimes include cyber harassment and stalking, distribution of child pornography, credit card fraud, human trafficking, spoofing, identity theft, and online libel or slander.



2. **Crime Against Institution** :- The main target here is institution.  
-Usually, this type of crime is done by teams of criminals including malware attacks and denial of service attacks.
3. **Crimes Against Government / states**:-When a cybercrime is committed against the government, it is considered an attack on that nation's independence.  
-Cybercrimes against the government include hacking, accessing confidential information, cyber warfare, cyber terrorism, and pirated software.

→**Prevention of Cyber Crime** :-Below are some points by means of which we can prevent cyber crime:

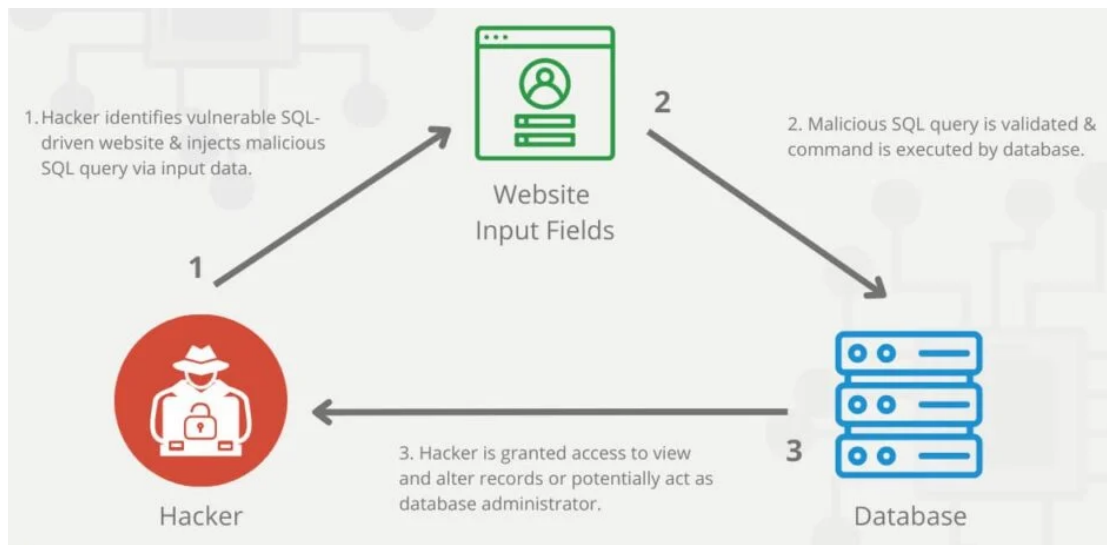
- **Use strong password**:-Maintain different password and username combinations for each account.  
-Weak passwords can be easily cracked using certain attacking methods like Brute force attack, Rainbow table attack etc,  
-So make them complex.  
-That means combination of letters, numbers and special characters.
- **Use trusted antivirus in devices** :-Always use trustworthy and highly advanced antivirus software in mobile and personal computers.  
-This leads to the prevention of different virus attack on devices.
- **Keep social media private**:-Always keep your social media accounts data privacy only to your friends.
- **Use secure network**:-Public Wi-Fi are vulnerable.  
-Avoid conducting financial or corporate transactions on these networks.
- **Never open attachments in spam emails**:-A computer gets infected by malware attacks from an email.  
-So , Never open an attachment from a sender you do not know.

**# Crime Types**:-Any criminal activity carried out over the internet is referred to as cybercrime.

-Given below are the types of cyber crime ;

- \***SQL Injections** (9 marks) :-A SQL injection attack is carried out by an attacker who "injects" malicious SQL code into the application's input data.  
-SQL injection allows the attacker to read, change, or delete sensitive data as well as execute administrative operations on the database.  
-SQL injection is a code injection technique that might destroy your database.  
-SQL injection is one of the most common web hacking techniques.  
-SQL injection is the placement of malicious code in SQL statements, via web page input.





- For Example Suppose we have an application based on student records. Any student can view only his or her own records by entering a unique and private student ID.
- The student enters the following in the input field: as student id = 12222345 or 1=1.

#### Query:

```
SELECT * from STUDENT where  
STUDENT-ID == 12222345 or 1 = 1
```

- Now, this 1=1 will return all records student.
- So basically, all the student data is compromised.
- Now the malicious user can also delete the student records in a similar fashion.
- the malicious can use the '=' operator in a clever manner to retrieve private and secure user information.
- Attackers simply add 1=1 in the username and password query that way attacker can get into the account without knowing the username or password.

#### Query:

```
Select * from User where  
(Username = "" or 1=1) AND  
(Password="" or 1=1).
```

- Impact of SQL Injection** :-The hacker can retrieve all the user data present in the database such as user details, credit card information, and social security numbers, and can also gain access to protected areas like the administrator portal.
- It is also possible to delete user data from the tables.



### →Preventing SQL Injection

- Restricting access privileges of users and defining how much amount of data any outsider can access from the database.
  - Basically, users should not be granted permission to access everything in the database.
- Error messages –these should not reveal sensitive information and where exactly an error occurred.
  - Simple custom error messages such as “Sorry, we are experiencing technical errors.
  - The technical team has been contacted.
  - Please try again later” can be used instead of display the SQL statements that caused the error.

-Some of the other methods used to prevent SQL Injection are:

- Password hashing
- Web application firewall
- Purchase better software
- Always update and use patches
- Continuously monitor SQL statements and database

→**Detecting SQL Injection**:-Most of the time, SQLi vulnerabilities are easy to identify and relatively easy to fix, before an attack can ever occur.

-follow the step for identifying Sql injection (SQLi)

- Submit the single quotation mark character ( ' ) and look for errors and anomalies.
- Submit some SQL syntax to evaluate the original value of each entry point, looking for differences in the application’s responses.
- Use Boolean search conditions (OR 1=1 and OR 1=2) to identify differences in the responses from the application.

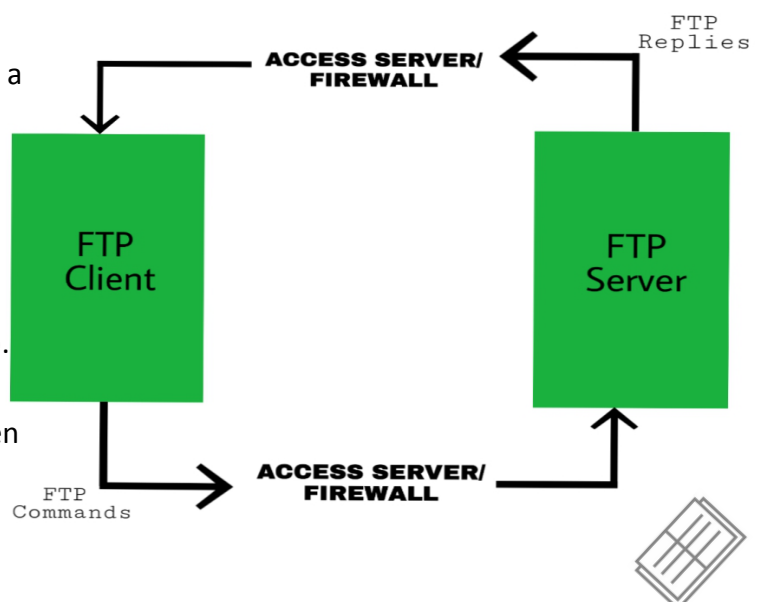
\* **Theft of FTP password** :-The primary purpose of an FTP server is to allow users to upload and download files.

-An FTP server is a computer that has a file transfer protocol (FTP) address.

-And its purpose is to receive an FTP connection.

-FTP is a protocol used to transfer files via the internet between a server (sender) and a client (receiver).

-it is a common solution used to facilitate remote data sharing between computers.



- Theft of FTP password refers to the un-authorized access of a user's FTP (File Transfer Protocol) login details, which includes both the username and password.
- This type of cyber attack can occur in various ways, such as phishing emails, malware infections, or brute-force attacks that guess passwords.
- Once an attacker has stolen an FTP password, they can access the victim's FTP server and potentially steal sensitive data or modify files without authorization.
- This can have serious consequences for individuals, organizations, and businesses that rely on FTP for file sharing and storage.

-Following are the method to Theft a FTP password;

- **Method 1: Crack Using Hydra :-** Hydra is often the tool of choice.  
-It can perform rapid dictionary attacks against more than 50 protocols, including telnet, FTP, HTTP, HTTPS, SMB, several databases, and much more.
- **Method Two: Crack Using Patator :-** Patator is a multipurpose brute-forcer. It is quite useful for making brute force attacks on many ports such as FTP, HTTP, SMB etc.

-Any password hacking attempt is successful only because of predictable password combinations.

-Firewalls and IPS are great when increasing the protection of your assets over the network.

-monthly password changes and random password audits across systems to ensure weak passwords are not in use.

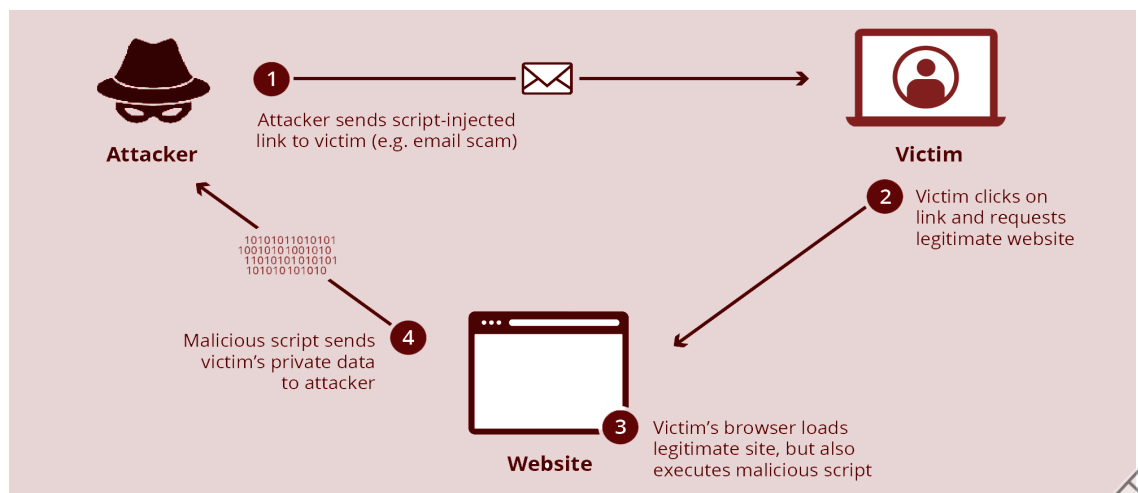
**\*Cross-site scripting (9 mark) :-** Cross-site scripting (XSS) is used, where the attacker attaches code in a website.

-That will execute when the victim loads the website.

-That malicious code can be inserted in several ways.

-Most popularly, it is either added to the end of a url or posted directly onto a page that displays user-generated content.

-cross-site scripting is a client-side code injection attack.



-JavaScript cross-site scripting attacks are popular because JavaScript has access to some sensitive data that can be used for identity theft and other malicious purposes.  
-For example, JavaScript has access to cookies\*, and an attacker could use an XSS attack to steal a user's cookies and impersonate them online.

-A typical cross-site scripting attack flow is as follows:

- The victim loads a webpage and the malicious code copies the user's cookies
- The code then sends an HTTP request to an attacker's webserver with the stolen cookies in the body of the request.
- The attacker can then use those cookies to access bank account numbers or other sensitive data.

→**Types of cross-site scripting** :- The two most popular types of cross-site scripting attacks are;

➤ Reflected cross-site scripting :-This is the most commonly seen cross-site scripting attack.

-With a reflected attack, malicious code is added onto the end of the url of a website.

-When the victim loads this link in their web browser, the browser will execute the code injected into the url.

-The attacker usually tricks the victim into clicking on the link.

-For example, a user might receive a legitimate-looking email that claims to come from their bank.

-The email will ask them to take some action on the bank's website, and provide a link.

-The link may end up looking something like this:

**`http://legitamite-bank.com/index.php?user=<script>here is some bad code!</script>`**

-Although the first part of the url looks safe and contains the domain of a trusted website, the code injected onto the end of the url can be malicious.

➤ Persistent cross-site scripting :-This happens on sites that let users post content that other users will see, such as a comments form or social media site,

-for example. If the site doesn't properly validate the inputs for user-generated content, an attacker can insert code that other users' browsers will execute when the page loads.

-For example an attacker might go to an online chatting site might put something like this in their profile:



***"Hi! My name is Dave, I enjoy long walks on the beach and  
<script>malicious code here</script>"***

-Any user that tries to access Dave's profile will become a victim to Dave's persistent cross-site scripting attack.

→**prevent cross-site scripting**

- **If possible, avoiding HTML in inputs** - One very effective way to avoid persistent cross-site scripting attacks is to prevent users from posting HTML into form inputs.
- **Sanitizing data** - Sanitizing data is similar to validation, but it happens after the data has already been posted to the web server, yet still before it is displayed to another user.
  - There are several online tools that can sanitize HTML and filter out any malicious code injections.
- **Taking cookie security measures** - Web applications can also set special rules for their cookie handling that can help in cookie-theft via cross-site scripting attacks.

**\*Viruses** :-viruses are unwanted software programs or pieces of code that interfere with the functioning of the computer.

- They spread through contaminated files, data, and insecure networks.
- Once it enters your system, it spread from one program to another program and from one infected computer to another computer.
- There are many antiviruses, which are programs that can help you protect your machine from viruses.
- It scans your system and cleans the viruses detected during the scan.
- Some of the popular antiviruses include Avast, Quickheal, McAfee, Kaspersky, etc.

**\*Worms**:-Worms are similar to a virus but it does not modify the program.

- It replicates itself more and more to cause slow down the computer system.
- Worms can be controlled by remote.
- The main objective of worms is to eat the system resources.

**Q)Difference between Virus and Worms (3 marks)?**

Virus	Worm
<ul style="list-style-type: none"><li>• The virus is the malicious code which will destroy the functioning of the computer system and transfer from one to another system.</li></ul>	<ul style="list-style-type: none"><li>• The malicious program that will copy itself and spread from one system of the computer to another through a network is called a worm.</li></ul>
<ul style="list-style-type: none"><li>• The virus is created by human action.</li></ul>	<ul style="list-style-type: none"><li>• The creation of a worm doesn't need human action.</li></ul>
<ul style="list-style-type: none"><li>• The speed of spreading the virus is slow.</li></ul>	<ul style="list-style-type: none"><li>• The speed of spreading of worms is fast.</li></ul>
<ul style="list-style-type: none"><li>• The host is needed for spreading the virus.</li></ul>	<ul style="list-style-type: none"><li>• No host is needed for spreading the virus.</li></ul>



Removing  
Malware

Antivirus, formatting

Virus removal tool, formatting

Protect the  
System using

Antivirus software

Antivirus, firewall

\* **Logical bombs** :-A logic bomb is a type of malware that contains malicious code that is secretly added to software.

-It is triggered at a specific event and used to destroying a system by clearing hard drives, deleting files, or corrupting data.

-An event can be a specific date or time leading up to the launch of an infected software application or the deletion of a specific record from a system.

-In order to maximize damage before being noticed, logic bombs are mainly used with **trojan horses, worms, and viruses**.

-The primary objective of logic bombs is to reformat a hard drive, modify or corrupt data, and remove important files from the system.

-The attacks caused by a logic bomb can be huge level.

- There are multiple examples of logic bombs that describe how they have wiped some organizations and servers of major financial institutions.

-use multiple layers of cybersecurity to protect yourself against logic bombs and not depend only on any antivirus software.

-Antivirus software may not be able to catch all instances of malware; however, it is absolutely powerful to protect against malware as well as logic bombs.

-As Logic bombs are triggered at a particular time; hence, they do not execute their malicious code immediately.

-That's why antivirus software may be unable to handle.

- Also, getting backup of your business's data regularly is the best idea to protect against logic bombs, even if you are using multiple layers of cybersecurity.

\* **E-mail bombing** :-An e-mail bomb is the sending of a huge number of e-mails to one system or person.

-with the goal of overflowing the mailbox and overwhelming the mail server.

-An e-mail bomb is a type of **denial-of-service attack**.

-People who send e-mail bombs have malicious intent, i.e., they intend to do harm.

-Along with hackers, e-mail bombers are a danger and nuisance for online people, businesses, and other entities.





-There are two main types of e-mail bombs

1. **Denial-of-service (DOS) attack**:-In this type of bomb, the attacker sends a massive number of emails to one address.  
-The system floods, resulting in a denial-of-service, i.e., the system crashes.
2. **Mass subscriptions**:-The attacker automatically subscribes someone, i.e., the victim, to many electronic mailing lists.  
-Each mailing list sends many messages regularly.  
-Subsequently, there is a flood of mail hitting the victim's email account virtually all the time.

**\*DoS attack** (9 marks) :-A denial-of-service (DoS) attack is a type of cyber attack in which a malicious actor aims to a computer or other device unavailable to its users by interrupting the device's normal functioning.

-Their purpose is to disrupt an organization's network operations by denying access to its users.

-For example, if a bank website can handle 10 people a second by clicking the Login button, an attacker only has to send 10 fake requests per second to make it so no users can log in.

-The most famous DoS technique is **the Ping of Death**.

-The Ping of Death attack works by generating and sending special network messages that cause problems for systems that receive them.

-DoS attacks typically fall in 2 categories:

1. Buffer overflow attacks:- It is a kind of attack where a computer can run out of RAM, hard disc space, or CPU time due to a memory buffer overflow.  
-This type of abuse frequently leads to lazy behavior, system crashes, or other server behaviors, resulting in denial-of-service.
2. Flood attacks :-Flood attacks occur when the system receives too much traffic , causing them to slow down and eventually stop.

-The primary focus of a DoS attack is to overflow the capacity of a targeted machine, that resulting in denial-of-service.

-Some of the consequences of I DoS attack may include:

- A DoS attack can make a website or service unavailable to users, causing lost revenue and damage to customer relationships.
- Sites may remain online during a DoS attack.  
-They may become slow or unresponsive, making it difficult or impossible for users to interact.
- The aftermath of a DoS attack can be expensive.  
-Extensive damage can be done to the target.
- A successful DoS attack can damage a company's reputation, and can cause data breaches.



-Detecting a DoS attacks early can minimizing its impact.

-A DoS attack can be detected by any of the following signs:

- Abnormally high traffic
- Slow or unresponsive servers
- High server utilization
- Unusual traffic patterns
- Unusual traffic sources

→**Preventing a DoS attack** can be challenging, but there are several effective techniques:

- **Network segmentation** - Segmenting networks into smaller, more manageable pieces, can limit the impact of a DoS attack.
- **IP blocking** - Blocking traffic from known or suspected malicious sources can prevent DoS traffic from reaching its target.
- **Rate limiting** - Limiting the rate of traffic to reach a server or resource can prevent a DoS attack from overwhelming it.

**\*Spamming**:-Spam describes large numbers of unwanted messages sent via email, instant chatting, social media, or text messages.

-It often contains promotional or advertising information and may also contain phishing, malware-spreading, or fake links or attachments.

-Spam's main goal is to efficiently reach a large number of recipients to make money or collect personal data.

-Spam is typically considered an irritation and can risk people's and organizations' security.

→**Types of Spam**

- Email Spam: This type of spam is sent through email.  
-Cybercriminals send phishing emails that appear to be from legitimate sources, but contain malicious links or requests for personal information.
- Instant Messaging Spam: Instant messaging spam is sent through messaging platforms such as WhatsApp & Telegram.  
-They often contain tempting offers such as job openings, contests or lottery wins that are too good to be true.
- Social Media Spam: There are several types of social media spam, like fake profiles, fake likes, spam comments, & malicious links that can trick users into downloading malware.
- SMS Spam: This type of spam messages are sent in bulk to mobile phones.  
-They may contain fake lottery wins, offers for free stuff or requests to click a link that will download malware to the phone.
- Voice Call Spam: Cybercriminals use robocalls to make calls to mobile or landline phones to promote products, spread scams or demand payments.



→**Prevention from Spamming** (3 mark) :-Spam, or unsolicited messages, can be a real headache for many people.

-They often end up in our email inbox & can be anything from annoying advertisements to phishing scams.

-However, with the right precautions, you can protect yourself from spam & avoid falling victim to cyber threats.

1. **Use Spam Filters** :-Many email providers have built-in spam filters that can help to block unwanted messages.
  - These filters analyze incoming emails based on their content & headers & determine whether they are spam or not.
  - They work by using algorithms that identify spam based on patterns, such as specific keywords or phrases that spammers often use.
2. **Be Cautious with Your Email Address** :-Unwanted messages can be easily sent to you by spammers via your email address.
  - To prevent this, be cautious with your email address.
  - Only share it with people you trust & avoid posting it on social media or public forums.
3. **Avoid Clicking on Suspicious Links** :-Spam emails often contain links that can lead to malicious websites or fraudulent pages.
  - Consequently, you should avoid clicking these links and if it looks suspicious, delete the message immediately..
4. **Unsubscribe** :-If you're receiving unwanted messages from legitimate companies, you can typically unsubscribe from their mailing list.
  - You will no longer receive emails from them after you do this.
5. **Installing Cybersecurity Software** :-To further protect yourself from spam & other cyber threats, consider installing cybersecurity software on your device.
  - This software can help to detect & block spam messages, while also providing additional layers of protection against malware & phishing scams.
6. **Report Spam** :-Most email services have a "report spam" feature that allows you to Report unwanted messages.
  - Reporting spam can help your email service provider to improve its spam filters & protect other users from similar messages.

**\*Web jacking**:-when attackers illegally gain control of an organisation's or individual's website is known as Web Jacking.

-The hackers implant a fake website, which, when you open it, takes you to another fraudulent website, where the attackers try to extract sensitive information.

-This crucial data can range from simple account passwords to credit card details.



-How to be safe from web jacking attack method

- First of all do not enter sensitive data in any link sent to you.
- Check the URL
- Just because the address looks Ok, don't assume this is a legitimate site.
- Read company name carefully, is it right or wrong.
- check that there is http protocol or https, if http then do not enter your data.
- If you are not sure, site is real or fake, enter a wrong username and password.
- Use a browser with anti-phishing detection.

**\* Identity theft and Credit card fraud** (3 marks) :-Identity Theft also called Identity Fraud is a crime that is being committed by a huge number nowadays.

-Identity theft happens when someone steals your personal information to commit fraud.

-This theft is committed in many ways by gathering personal information such as transactional information of another person to make transactions.

-There are various types of identity threats but some common ones are :

1. Criminal Identity Theft
2. Senior Identity Theft
3. Medical Identity Theft
4. Tax Identity Theft
5. Social Security Identity Theft
6. Financial Identity Theft

→**Steps Of Prevention From Identity Theft**:-Following are some methods by which you can enhance your security for identity thefts;

- Use Strong Passwords and do not share your PIN with anyone on or off the phone.
- Secure all your devices with a password.
- Don't install random software from the internet.
- Don't post sensitive information over social media.
- While entering passwords at payment gateway ensure its authenticity.
- Keep a practice of changing your PIN and password regularly.
- Do not disclose your information over phone.
- While traveling do not disclose personal information with strangers.
- Do not make all the personal information on your social media accounts public.
- Do not fill personal data on the website that claims to offer benefits in return.

-Credit card fraud is a type of cybercrime or financial crime where a fraudster gains access to sensitive information regarding your credit card.

-Such sensitive information includes your credit card number, PIN, CVV, and other similar details needed to use the card to make a purchase.

-Credit card fraud has become an increasingly common problem in the digital age.



-While credit card companies and banks are working hard to improve their security measures and prevent fraud, there are still several steps that you can take to protect your personal information and avoid falling victim to credit card fraud.

-Below are some important pointers to keep in mind.

- **Keep your credit card details secure:** The most effective way to prevent credit card fraud is by keeping your credit card details secure.
  - Avoid sharing your credit card number, CVV code, and other sensitive information with anyone .
- **Regularly check your account statements:** It is important to regularly check your account statements for any unauthorised transactions.
  - If you spot any transactions that you don't recognise, contact your bank, or credit card company immediately.
- **Avoid using public Wi-Fi:** Public Wi-Fi networks are not secure, and cybercriminals can easily intercept the data that you transmit over these networks.
- **Always use secure websites:** When making any online transactions, always make sure that the website is secure and has a valid SSL certificate.
  - You should also avoid clicking on any links in emails or messages that ask you to provide your credit card details.
- **Report suspicious activity immediately:** If you suspect any fraudulent activity on your account, report it immediately.
  - Most banks and credit card companies have a 24-hour helpline that you can call for any assistance.
- **Get a card protection plan:** Another way in which you can save yourself against financial losses due to credit card fraud, is by buying a card protection plan.

**\*Data diddling (3 marks ):**-Data diddling, or data manipulation, is a type of computer-based fraud in which data is altered or changed to cause harm, gain an advantage, or hide fraudulent activities.

-This can be done by changing data values, modifying data fields, deleting data, or adding data to a database or computer system.

-when a person intentionally enters wrong information into a computer, system, or document.

-It is used when businesses and individuals want to hide part of their profits for tax avoidanc.

-It could also be used to do the opposite — make the number of sales to make it look like the business has more customers than it really does.

-This is done to get a better loan proposal from the bank.

-If a business owner wants to bring their opponent down, they can also use this technique to cause damage to someone's company or its reputation.

-Data diddling can be performed by manually entering the data or remotely by hacking the system or using malware to automatically change input data.



**\*Salami attacks** (9 marks):-A salami attack is a type of cybercrime that involves the theft of small amounts of money from a large number of accounts, often over a long period of time.

-the thief is able to steal small amounts of money from many accounts without being noticed.

-These attacks can be difficult to detect and can have serious consequences for individuals and organizations.

-The goal of this type of attack is to steal small amounts of money from each account over a long period of time, in order to avoid detection.

-It was first salami been seen, when a group of programmers in the former Soviet Union was caught stealing small amounts of money from the government by manipulating financial transactions.

—>**Types of Salami attacks:**

**1. Salami Slicing:**-Salami Slicing occurs when the attackers/hacker get customer information, like Bank/credit card details.

-and other similar sort of detail by using an online database.

-the attacker/hacker deduct an small amount of cash from each account.

-these amounts add up to an large amount of cash and this can be often invisibly to deduct it.

-Most people do not report the deduction, often due to the small amount involved.

-For example, suppose an attacker withdraws ₹0.01 (1 paise) from each bank account.

-Nobody will notice such a minor amount.

-However, a large sum is produced when one paise is deducted from each account holder at that bank.

**2. Penny Shaving :-**A penny-shaving attack is similar to a salami-slicing attack, but it involves the manipulation of financial transactions in order to steal small amounts of money from a single account over a long period of time.

→**How to Spot a Salami Attack:**-A salami attack is a type of financial fraud where small amounts of money are stolen over a long period of time, which adds up to a significant amount of money.

-Here are some ways to spot a salami attack:

- **Monitor your bank statements regularly:** Keep a close eye on your bank statements and transactions, and check them frequently to identify any unauthorized transactions.
- **Look for small deductions:** Watch out for small deductions or transactions you don't recognize, as these can indicate a salami attack.



- **Check your credit report:** Keep an eye on your credit report for any unauthorized accounts or inquiries.  
-If you see something suspicious, take action immediately.
- **Set up alerts:** Most banks offer alert services that notify you of any unusual activity on your account.  
-You can set up alerts for transactions over a certain amount or for any changes to your account.
- **Keep your passwords secure:** Always use strong and unique passwords for your financial accounts and never share them with anyone.

→**Prevention From Salami attack** :- Users are needed to check their account weekly transactions and month-to-month bank statements to shield their bank accounts from salami attack.

-If you have got any issues with any strange charges on your account, contact your bank.  
-Financial institutions, such as banks, should also update their security so that the attacker does not become familiar with how the framework is designed.

**\*Phishing** :-Phishing is a type of cybersecurity attack.

- malicious actors send messages pretending to be a trusted person or entity.  
-Phishing messages manipulate a user, causing them to perform actions like installing a malicious file, clicking a malicious link, or disclose sensitive information.

**\*Cyber stalking** (3 marks ):-Cyberstalking is a crime committed when someone uses the internet and other technologies to harass or stalk another person online.

-it can include gossip, false accusations, teasing, and even extreme threats.

-The three most common types of cyber stalking are as follows:

1. **Email stalking:** This type of stalking involves the sender sending hateful, obscene, or threatening emails to the recipient.  
-Sometimes the attacker may also include viruses and spam in the email.
2. **Internet stalking:** This type of stalking occurs when an individual spreads rumors or tracks victims on the internet.
3. **Computer stalking:** This type of stalking occurs when an individual hacks into a victim's computer and takes control of it.



-Some of the common examples of cyberstalking are:

- Making rude, offensive, or suggestive online comments
- Sending the target threatening, controlling, or lewd messages or emails.
- Making a fake social media profile to follow the victim.
- Gaining access to the victim's online accounts



- Posting or publishing photos of the victim.
- Attempting to obtain photographs of the victim
- Tracking the victim's online movements using tracking devices.

**\*Spoofing** :-In cybersecurity, 'spoofing' is when fraudsters pretend to be someone or something else to win a person's trust.

-The motivation is usually to gain access to systems, steal data, steal money, or spread malware.

-Spoofing can apply to emails, phone calls and websites, or it can be more technical, such as **IP spoofing, Address Resolution Protocol (ARP) spoofing or Domain Name System (DNS) server.**

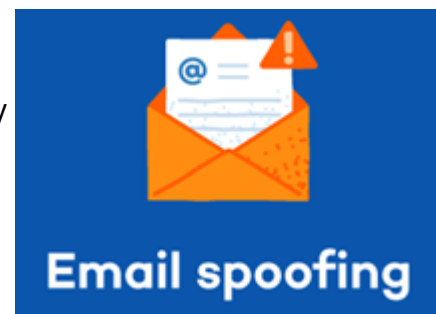
-Typically, spoofing attacks use trusted connections by pretending to be someone or something the victim is familiar with.

-A successful spoofing attack can have serious consequences.

-An attacker may be able to steal sensitive personal or company information, harvest information for use in a future attack or fraud attempt, spread malware through malicious links or attachments.

#### →Types of Spoofing Attacks

- Email spoofing :-the most widely-used attacks.
  - User receiving an emails from a friend or an authority figure asking us to do something.
  - Most of the time, we can easily determine that someone is trying to trick (or phish) us.
  - But, sometimes, those emails are pretty convincing.



- IP Spoofing :-IP address spoofing hides the true identity and location of the computer or mobile device used by the cyber criminal.
  - the cyber criminal aims to hide their location from the recipient.
  - This approach can be used with email or website spoofing to add more legitimacy to the attack.
  - hackers and scammers alter the header details to hide their original identity.



- Caller ID Spoofing :-Caller ID spoofing is a common tactic that uses a phone number that appears to come from your area code.
  - We are all more likely to answer a call when we see it is a local number.
  - The cyber criminal may pretend to be a police officer.
  - Because the caller ID looks authentic, the victim is convinced to pay fines that don't exist and provide confidential information, all under the threat of being arrested.





- **Website Spoofing** :-Website spoofing uses a fake website that looks legitimate.  
-A spoofed website looks exactly like the actual website—the logo, branding, colors, layout, domain name, and contact details are all the same.  
-It's challenging to identify a spoofed website without closely inspecting the domain name.



- **DNS Spoofing** :-Domain Name Server or DNS spoofing allows cyber criminals to redirect traffic from the intended legitimate IP address to a faked IP address.



### →Ways To Spot Spoofing

- **In Website Spoofing**
  - If the padlock is missing from the website address bar, the website is not secure and is likely spoofed.
  - The URL uses HTTP and not HTTPS.
  - Spelling errors, broken links, suspicious contact us information, and missing social media badges can all be indicators that the website has been spoofed.
  - Website addresses containing the name of the spoofed domain are not the official domain.
- **In Email Spoofing**
  - Spelling errors or an incorrect domain name in the sender's email address indicate a spoofed email.
  - Email language urges you to act quickly, transfer money, or provide confidential information.
  - Spelling errors, poor grammar, and unfamiliar language can indicate the email isn't originating from a genuine source.
  - Attachments and an email message that urges you to download the attachment.
- **In Caller ID, Text Message, or SMS Spoofing**
  - If the phone number displays without brackets () or dashes -. For example, 4567893543.
  - The caller ID is your phone number or looks very similar (e.g., one digit may differ).
  - The phone number or caller's name are hidden.



## ->Prevent Spoofing

✓ Dos	✗ Don'ts
<ul style="list-style-type: none"><li>• Turn on your spam filter</li><li>• Check for poor grammar</li><li>• Hover over the URL before clicking</li><li>• Confirm information with the source</li><li>• Set up two-factor authentication</li><li>• Download cybersecurity software</li></ul>	<ul style="list-style-type: none"><li>• Click on unfamiliar downloads</li><li>• Answer calls or emails from unrecognized senders</li><li>• Give out your personal information to unfamiliar sources</li><li>• Use the same password across multiple logins</li></ul>

**\*Pornography** :- Cyber Pornography means the publishing, distributing or designing pornography by using cyberspace.

-The technology has its pros and cons and cyber pornography is the result of the advancement of technology.

-With the easy availability of the Internet, people can now view thousands of porn on their mobile or laptops, they even have access to upload pornographic content online.

-Pornography has been around for centuries, but with the advent of the internet, it has become more accessible than ever before.

-Unfortunately, this increased accessibility has also led to an increase in cybercrime related to pornography.

-Many surveys reveal that a person who is addicted to pornography has a change in attitude towards himself and his family.

-One of the most serious forms of pornography-related cybercrime is child pornography.

-Another form of pornography-related cybercrime is revenge porn.

-Sharing photos or videos without the permission of the person in the photos or videos.

-Finally, pornography-related cybercrime can also include addiction.

-Studies have shown that pornography can be addictive, and that it can have a negative impact on mental health and relationships.

-In conclusion, pornography-related cybercrime is a serious and growing problem.



**\* Defamation:-** Defamation is the act of publishing false or incorrect statements about an individual or organization on the internet.

-It can include statements made on social media, forums, blogs, or any other online platform.

-defamation can cause significant harm to the reputation of the person or organization and can lead to loss of business, financial damages, and emotional distress.

-If someone or an organisation has been defamed online, they have two options for pursuing justice:

- Either file a civil lawsuit for damages or
- File a complaint with the cybercrime police.

-The remedies available include an court order to stop the publication of defamatory material, removal of defamatory content from the internet, and financial penalties.

**\*Computer vandalism /Cyber vandalism :-**Cyber vandalism is the purposeful, malicious destruction of digital property.

-It usually targets websites and other tech products, but it can also be used to threaten individuals or institutions.

-Cyber vandals use all sorts of tools to deface websites, delete files, take over user accounts, or send spam and viruses.

-It is similar to traditional vandalism in the physical world, where people or groups deface, alter, or damage digital property to create disaster or send a message.

→**Types of Cyber Vandalism**

- **Identity Theft:** The act of taking a person's personal information, such as their bank information, to engage in fraud or other illegal actions is known as identity theft.
- **Phishing Attack:** Phishing is a technique to mislead people into disclosing their personal data, including passwords or credit card details.
- **Website Vandalism:** Website vandalism refers to online vandalism that alters a website's appearance and content, frequently for political or ideological reasons.  
-The purpose of this modification is to prevent the websites from operating normally and to send a message.

→**Impact of Cyber Vandalism are;**

- Financial Loss
- National Security Threats
- Privacy Violations
- Infrastructure Damage

**\*Cyber terrorism :-**Cyber terrorism (also known as digital terrorism) is defined as troublemaking attacks by recognised terrorist organisations against computer systems with the intent of generating alarm, panic etc.

-The internet can be used by terrorists to finance their operations, train other terrorists, and plan terror attacks.



- cyber terrorism used to hack the government or private servers to access sensitive information or even take money for terror activities.

-Types of cyber terrorism attacks

- Phishing
- Ransomware:-Ransomware is malicious software that locks victims out of their computer files and blocks other resources, releasing them only after the victims pay a ransom, typically in the form of a cryptocurrency such as Bitcoin.
- Data breaches:-A data breach [External link:open\\_in\\_new](#) occurs when an attacker gains unauthorized access to a person's or organization's information.

→**Example of Cyber terrorism**

- Hacking into computer systems.
- Introducing viruses to vulnerable networks.
- Website Defacing.
- Denial-of-Service (DoS) attacks.
- Terroristic threats made via email

**\*Cyber warfare** :-Cyber warfare is usually defined as a cyber attack or series of attacks that target a country.

-for example, computer viruses or denial-of-service attacks.

-The objective is to weaken the target country by compromising its core systems.

→ **Goal of cyber warfare**

- **Stealing sensitive information:** It is used to steal sensitive information such as intellectual property, military secrets, or financial data.
- **Undermining national security:** Cyber attacks can be used to undermine national security by disrupting military operations, stealing classified information, or compromising sensitive systems.
- **Undermining democratic processes:** Cyber attacks can be used to interfere with democratic processes by spreading disinformation, manipulating election results, or spreading sensitive data related to political processes.

**# Hacking** :-Hackers are computer experts that use advanced programming skills to neutralize security protocols and gain access to devices or networks.

-Hackers also take advantage of weaknesses in network security to gain access.

-One example of computer hacking is the use of a password cracking technique to gain access to a computer system.

-The process of gaining illegal access to a computer system, or a group of computer systems, is known as hacking.

-This is accomplished by cracking the passwords and codes that grant access to systems.



-Hacking in cyber security refers to the misuse of devices like computers, smartphones, tablets, and networks to cause damage to or corrupt systems, gather information on users, steal data and documents, or disrupt data-related activity.

-Hackers use a variety of techniques to achieve their aims. Some of the most common methods include:

- Hacking passwords
- Infecting devices with malware
- Exploiting insecure wireless networks
- Gaining backdoor access

-Once they have gained access to your data or devices, they can:

- Steal your money and open credit card and bank accounts in your name
- Destroy your credit rating
- Make purchases on your behalf
- Use and abuse your Social Security number
- Sell your information to others who will use it for malicious purposes
- Delete or damage important files on your computer
- Obtain sensitive personal information and share it, or threaten to share it, publicly

→**Types of Hackers**:-following are the types of hackers

1. **Black Hat Hackers** :- These types of hackers, often known as **crackers**.

-And always have a malicious motive and gain illegal access to computer networks and websites.

-Their goal is to make money by stealing secret organizational data, stealing funds from online bank accounts, violating privacy rights to benefit criminal organizations, and so on.

-Black hat hackers use their technique skill to harm others.

-Their goal is to gain unauthorized access to networks and systems, they attack to steal data, spread malware causing damage to systems.

-Black hat hackers are also referred to as **malicious hackers, unethical hackers, and crackers**.

2. **White Hat Hackers/Ethical Hackers** :- White hat hackers (sometimes referred to as ethical hackers) are opposites of black hat hackers.

-They employ their technical knowledge to defend against malicious hackers.

-White hats are employed by businesses and government agencies as data security analysts, researchers, security specialists, etc.

-White hat hackers, with the permission of the system owner and with good motives, use the same hacking tactics that the black hackers use.

-They can work as contractors, freelancers, or in-house for the companies.

-They assist their customers in resolving security flaws before they are exploited by criminal hackers.

-Also known as **ethical hacking**.



3. **Grey Hat Hackers** :-Grey hat hackers sit somewhere between the black and the white hat hackers.
- They aim to break rules and ethics, unlike black hat hackers, but they don't do so with the intention of hurting people or making money.
  - Their actions are typically carried out for the common good.
  - grey hat hackers uncover weaknesses such as vulnerabilities, Instead of completely using them, they report them.
  - But grey hat hackers may demand payment in exchange for providing full details of what they uncovered.

#### →Hacking prevention

- Use strong passwords
- Be vigilant against phishing
- Keep your devices and software up to date
- Stay away from unwanted websites.
- Only download software from reputable sources. Before downloading free software or file-sharing applications, give them a thorough examination.
- Don't access personal or financial data with public Wi-Fi
- Use a good quality antivirus.

\* **Malwares** (9 marks) :-Malware, short for malicious software, refers to any intrusive software developed by cybercriminals (often called hackers) to steal data and damage or destroy computers and computer systems.

-Examples of common malware include **viruses, worms, Trojan viruses, spyware, adware, and ransomware.**

-The goal of malware is to cause damage and steal information or financial benefit.

-There are billions of malware attacks every year, and malware infections can happen on any device or operating system. Windows, Mac, iOS, and Android systems can all fall victim.

#### →Types of Malware

-Malware can be designed to achieve a variety of goals in various ways.

-Some of the most common types of malware include:

1. **Adware** :- Adware is malicious software used to collect data on your computer usage and provide appropriate advertisements to you.
  - While adware is not always dangerous, in some cases adware can cause issues for your system.
  - Adware can redirect your browser to unsafe sites, and it can even contain Trojan horses and spyware.
  - Additionally, significant levels of adware can slow down your system noticeably.
  - Because not all adware is malicious, it is important to have protection that constantly and scans these programs.



2. **Spyware** :- Spyware is malicious software that runs secretly on a computer and reports back to a remote user.
  - Rather than simply disrupting a device's operations, spyware targets sensitive information and can grant remote access to predators.
  - Spyware is often used to steal financial or personal information.
3. **Virus** :- front ill unde 🙌
4. **Worms** :- front ill unde 🙌
5. **Trojan virus** :It is one of the most dangerous malware types.
  - Trojan viruses are addressed as helpful software programs.
  - But once the user downloads it, the Trojan virus can gain access to sensitive data and then modify, block, or delete the data.
  - This can be extremely harmful to the performance of the device.
  - Trojans can be used to steal financial information or install other forms of malware, often ransomware.
6. **Ransomware**:-Ransomware is malicious software that gains access to sensitive information within a system, encrypts that information so that the user cannot access it, and then demands a financial payout for the data to be released.
  - By clicking an unknown link, the user downloads the ransomware.
  - The attacker proceeds to encrypt specific information that can only be opened by a mathematical key they know.
  - When the attacker receives payment, the data is unlocked.

-Follow these three easy steps to remove malware from your device.

1. Download and install a good cybersecurity program.
2. Run a scan using your new program.
3. Change all your passwords.



Join for more MCA short note : [https://t.me/mgu\\_mca\\_shortnote](https://t.me/mgu_mca_shortnote)



**@MGU\_MCA\_SHORTNOTE**