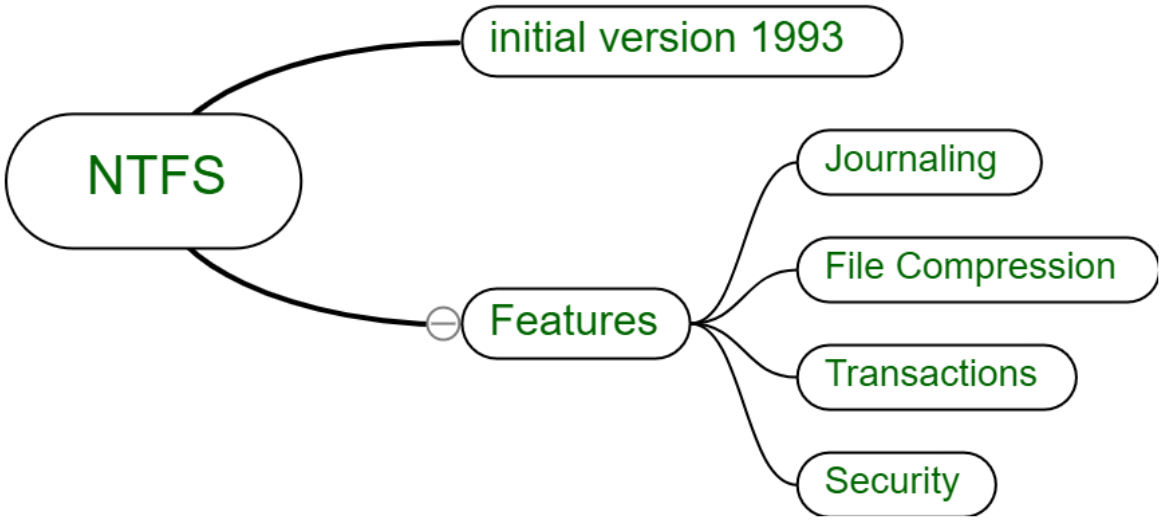
Digital Forensic Notes

Q1.Explain the NTFS file system in details?

Ans. NTFS stands for **New Technology File System** is a proprietary file system developed by Microsoft, started with the Windows NT 3.1 and many other such as Windows 2000, including Windows XP, Windows Server 2003, Windows 7, Windows 8. NTFS file system has many technical benefits over FAT (File Allocation Table) an improved version and HPFS (High Performance File System) an improved support for metadata.

NTFS (New Technology File System): Windows NT has come with a new file system called NTFS in 1993. This stands for New Technology File System. This was an enhanced and more advanced version of FAT systems. All Windows installation is done on NTFS, it first formats the storage in NFTS format and then install on it. Mostly NTFS is done on internal drives. This has no file size limits and no partition or volume limits. Theoretically up to 16 EiB size of a single file.



- **Journaling –** This technique records the metadata and its changes in the volume or partition.
- **Transactions –** This function enable files and folders to be recreated, renamed, deleted and many more without affecting others.

Characteristics of NTFS :

1. **Compatibility –**It supports compression of files and directories to optimize storage space.
2. **Scalability –**It introduced with improved performance, scalable in comparison to its precursor.
3. **Efficiency –**It utilizes the disk space efficiently by using smaller size of clusters.
4. **Attributes –**NTFS's attributes Read-only, hidden, system, archive, not content indexed, off-line, temporary, compressed.

Advantages of NTFS :

- Easily recovers file system and supports long file names.
- Provides users with local security by protecting files and directories.
- NTFS is a journaling file system.
- It supports spanning volumes spread across several physical drives.

- Support larger sized hard drives with increasing general performance of the drive .

Disadvantages of NTFS :

- NTFS performance does not decrease as FAT does.
- Removable devices such as Android smart phones, do not support NTFS.
- Doesn't include a system that guarantee file system performance.

Q2. Explain the Significance of the MFT?

Ans. Managed file transfer (MFT) is a technology platform that allows organizations to reliably exchange electronic data between systems and people, within and outside the enterprise, securely and in compliance with applicable regulations.

Benefits of managed file transfer

- **Data security:** High-profile data breaches and failed transfers can drastically impact a company's bottom line and reputation. MFT offers a preemptive security strategy with real-time monitoring, and validation security policies and controls to protect data in transit or at rest.
- **Data growth:** Data is everywhere, and companies face larger and more varied files than in the past. The number of users sharing files has grown as have the number of end-points and devices. And as files get larger, the time to move them over global distances becomes longer. MFT brings reliable, automated governance to the movement of files inside and outside the business and can accelerate big data movements around the globe.
- **Regulatory compliance:** Legislative and industry requirements, such as the Payment Card Industry Data Security Standards (PCI DSS), the Health Insurance Portability and Accountability Act (HIPPA), Basel II, Sarbanes-Oxley Act (SOX) and others, typically have stringent data security standards. Using a properly configured MFT system to encrypt, transmit, monitor and store sensitive data empowers organizations to meet security mandates.
- **Technology megatrends:** Moving files has become more complex with the adoption of transformational technologies. The growth of big data, cloud applications, artificial intelligence, data analytics and the Internet of Things (IoT) place a premium on the speed and bulk of file transfers. MFT offers advanced capabilities and support for multiple platforms, mobile devices, applications and other existing IT infrastructure.
- **Visibility:** Companies need to anticipate risk factors to mitigate damages. Operational visibility over file movements leads to proactive issue resolution, like failed transfers and improved compliance with SLA commitments.

Q3.Explain the mobile network structure in details?

Ans. **Mobile Network Structure**

A mobile network, like a bustling city, is a complex system with many interconnected components working seamlessly to keep you connected. To understand it fully, we need to dive into its layers, each playing a crucial role:

1. Cell Sites and Coverage:

- Imagine the city divided into neighborhoods, each served by a **cell site** (like a tower with antennas). These emit radio signals, creating "cells" of coverage.
- Different cell sizes exist: macro cells for wider areas, micro cells for dense urban areas, and femtocells for indoor coverage.
- Your phone constantly communicates with the strongest cell, ensuring seamless connection even as you move.

2. Base Station Subsystem (BSS):

- This layer manages communication directly with your phone. It consists of:

- **Base Transceiver Station (BTS):** The tower-mounted antenna transmitting and receiving signals.
- **Base Station Controller (BSC):** Coordinates multiple BTS, managing radio resources and handovers (switching between cells).

3. Network Switching Subsystem (NSS):

- The "brain" of the network, controlling calls, data, and subscriber information. It includes:
  - **Mobile Switching Center (MSC):** Routes calls, manages location updates, and interacts with other networks.
  - **Home Location Register (HLR):** Stores subscriber data like phone number and service profile.
  - **Visitor Location Register (VLR):** Temporary database for users roaming in another network area.
  - **Gateway Mobile Switching Center (GMSC):** Connects the mobile network to external networks like landlines.

4. Operation and Support System (OSS):

- Monitors and manages the entire network, ensuring smooth operation and troubleshooting issues.

5. Additional Layers:

- **Circuit Switched Network:** handles voice calls directly connecting callers.
- **Packet Switched Network:** handles data like internet traffic in smaller packets.
- **Mobile Data Networks:** like 3G, 4G, and 5G, provide varying data speeds and capabilities.

Understanding the Handover:

- As you move, your phone seamlessly switches between cells without dropping calls. This "handover" is orchestrated by the BSC and MSC, ensuring uninterrupted communication.

Q4.Explain in detail about IMAP?

Ans. **Internet Message Access Protocol (IMAP)** is an application layer protocol that operates as a contract for receiving emails from the mail server. It was designed by Mark Crispin in 1986 as a remote access mailbox protocol, the current version of IMAP is IMAP4. It is used as the most commonly used protocol for retrieving emails. This term is also known as Internet mail access protocol, Interactive mail access protocol, and Interim mail access protocol.

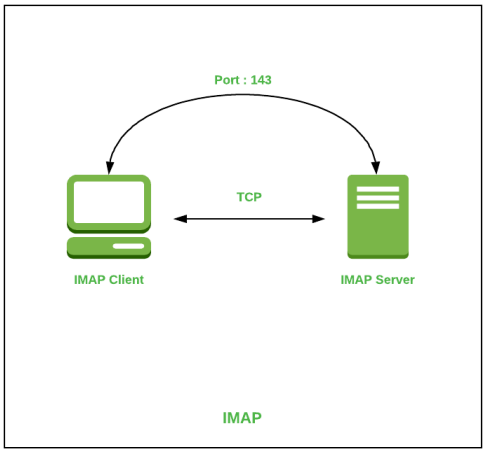
Features of IMAP :

- It is capable of managing multiple mailboxes and organizing them into various categories.
- Provides adding of message flags to keep track of which messages are being seen.
- It is capable of deciding whether to retrieve email from a mail server before downloading.
- It makes it easy to download media when multiple files are attached.

Working of IMAP :

IMAP follows Client-server Architecture and is the most commonly used email protocol. It is a combination of client and server process running on other computers that are connected through a network. This protocol resides over the TCP/IP protocol for communication. Once the communication is set up the server listens on port 143 by default which is non-encrypted. For the secure encrypted communication port, 993 is used.

Architecture of IMAP :



Advantages :

- It offers synchronization across all the maintained sessions by the user.
- It provides security over POP3 protocol as the email only exists on the IMAP server.
- Users have remote access to all the contents.
- It offers easy migration between the devices as it is synchronized by a centralized server.
- There is no need to physically allocate any storage to save contents.

Disadvantages :

- IMAP is complex to maintain.
- Emails of the user are only available when there is an internet connection.
- It is slower to load messages.
- Some emails don't support IMAP which makes it difficult to manage.
- Many browser-based solutions are unavailable due to not support of IMAP.

Q5. Explain the differences between steganography and cryptography?

Ans. 1. **Steganography:** Steganography is a method in which secret message is hidden in a cover media. Steganography means covered writing. Steganography is the idea to prevent secret information by creating the suspicion. Steganography is less popular than Cryptography. In steganography, structure of data is not usually altered. The forms of steganography are:

1. Text
2. Audio
3. Video
4. Images
5. Network or Protocol

2. Cryptography: Cryptography means secret writing. In cryptography, sender does not send message directly to the receiver, before sending information to the receiver information or plain text is converted into cipher text by using some encryption algorithm then send to the receiver and receiver decrypt the cipher text into plain text to read the original information. It is of two types:

1. Symmetric key cryptography
2. Asymmetric key cryptography

The difference between Steganography and Cryptography:

S.NO	Steganography	Cryptography

1.	**Steganography** means **covered writing.**	**Cryptography** means **secret writing.**
2.	Steganography is less popular than Cryptography.	While cryptography is more popular than Steganography.
3.	Attack's name in Steganography is **Steganalysis.**	While in cryptography, Attack's name is **Cryptanalysis.**
4.	In steganography, structure of data is not usually altered.	While in cryptography, structure of data is altered.
5.	Steganography supports **Confidentiality** and **Authentication** security principles.	While cryptography supports **Confidentiality** and **Authentication** security principles as well as **Data integrity** and **Non-repudiation**.
6.	In steganography, the fact that a secret communication is taking place is hidden.	While in cryptography only secret message is hidden.
7.	In steganography, not much mathematical transformations are involved.	Cryptography involves the use of number theory, mathematics etc. to modify data
8.	In Steganography the information is hidden.	In cryptography the information is transformed.
9.	Hidden information is not visible.	Transformed information is visible.
10.	Steganography Provides Confidentiality only.	Cryptography Provides Confidentiality, Integrity, Non-repudiation.
11.	Steganography doesn't have specific algorithms.	Cryptography have Various recognized and approved algorithms.
12.	The goal of steganography is to make the information invisible to anyone who doesn't know where to look or what to look for	The main goal of cryptography is to keep the contents of the message secret from unauthorized access.

Q6. Explain brute force cracking in detail?

Ans. A brute force attack is a hacking method that uses trial and error to crack passwords, login credentials, and encryption keys. It is a simple yet reliable tactic for gaining unauthorized access to individual accounts and organizations' systems and networks. The hacker tries multiple usernames and passwords, often using a computer to test a wide range of combinations, until they find the correct login information.

The name "brute force" comes from attackers using excessively forceful attempts to gain access to user accounts. Despite being an old cyberattack method, brute force attacks are tried and tested and remain a popular tactic with hackers.

Types of Brute Force Attacks

There are various types of brute force attack methods that allow attackers to gain unauthorized access and steal user data.

1. Simple Brute Force Attacks

A simple brute force attack occurs when a hacker attempts to guess a user's login credentials manually without using any software. This is typically through standard password combinations or personal identification number (PIN) codes.

These attacks are simple because many people still use weak passwords, such as "password123" or "1234," or practice poor password etiquette, such as using the same password for multiple websites. Passwords can also be guessed by hackers that do minimal reconnaissance work to crack an individual's potential password, such as the name of their favorite sports team.

2. Dictionary Attacks

A dictionary attack is a basic form of brute force hacking in which the attacker selects a target, then tests possible passwords against that individual's username. The attack method itself is not technically considered a brute force attack, but it can play an important role in a bad actor's password-cracking process.

The name "dictionary attack" comes from hackers running through dictionaries and amending words with special characters and numbers. This type of attack is typically time-consuming and has a low chance of success compared to newer, more effective attack methods.

3. Hybrid Brute Force Attacks

A hybrid brute force attack is when a hacker combines a dictionary attack method with a simple brute force attack. It begins with the hacker knowing a username, then carrying out a dictionary attack and simple brute force methods to discover an account login combination.

The attacker starts with a list of potential words, then experiments with character, letter, and number combinations to find the correct password. This approach allows hackers to discover passwords that combine common or popular words with numbers, years, or random characters, such as "SanDiego123" or "Rover2020."

4. Reverse Brute Force Attacks

A reverse brute force attack sees an attacker begin the process with a known password, which is typically discovered through a network breach. They use that password to search for a matching login credential using lists of millions of usernames. Attackers may also use a commonly used weak password, such as "Password123," to search through a database of usernames for a match.

5. Credential Stuffing

Credential stuffing preys on users' weak password etiquettes. Attackers collect username and password combinations they have stolen, which they then test on other websites to see if they can gain access to additional user accounts. This approach is successful if people use the same username and password combination or reuse passwords for various accounts and social media profiles.

Q7. What is First Response?

Ans. In digital forensics, the "first response" refers to the initial steps taken when an incident or potential breach is discovered. It involves the immediate actions by forensic investigators or incident response teams to secure the scene, preserve evidence, and prevent further damage or data loss. First response activities typically include isolating affected systems, securing physical and digital evidence, documenting the situation, and initiating procedures to maintain the integrity of potential evidence. This phase is crucial in ensuring that the investigation proceeds effectively and that valuable information is not compromised.

Q8. Describe SANS Forensics Methodology?

Ans. The SANS Forensics Methodology is a comprehensive approach to digital forensics, primarily focused on incident response and investigation. It typically involves the following key steps:

Identification: Recognize and understand potential security incidents or anomalies that may require investigation.

Preservation: Ensure the preservation of volatile data and the integrity of evidence during the investigation.

Collection: Gather relevant data from various sources, such as disk images, network captures, and log files.

Examination: Analyze collected data using forensic tools and techniques to uncover evidence and understand the scope of the incident.

Analysis: Piece together the information gathered to reconstruct events, identify patterns, and determine the extent of the compromise.

Documentation: Thoroughly document the entire investigation process, including methodologies, findings, and any actions taken.

Presentation: Communicate the results of the investigation to stakeholders, law enforcement, or other relevant parties.

Review: Evaluate the entire process to identify areas for improvement and enhance future incident response capabilities.

SANS, which stands for SysAdmin, Audit, Network, and Security, is an organization known for providing cybersecurity training and certifications, and its forensics methodology reflects best practices in the field.

Q9. Describe the use of bit locker during forensics investigation?

Ans. BitLocker, a disk encryption program in Windows, plays a crucial role in forensic investigations by securing data on drives. During an investigation, BitLocker can be both a challenge and a resource. Investigators may encounter encrypted drives, requiring proper authentication or recovery keys to access data. On the positive side, BitLocker helps protect sensitive information from unauthorized access. Investigators often need to employ decryption methods, utilizing recovery keys or passwords, to access and analyze the encrypted data, ensuring a comprehensive examination of digital evidence.

Q10. Explain the role of a forensic expert?

Ans. A forensic expert plays a crucial role in legal investigations by applying specialized knowledge to analyze and interpret evidence. Their responsibilities include collecting, preserving, and examining digital or physical evidence to uncover facts relevant to a case. Whether in computer forensics, DNA analysis, or other fields, forensic experts use scientific methods to draw conclusions and present findings in court. They must adhere to strict protocols to ensure the integrity of evidence, collaborating with law enforcement or legal professionals. The role demands expertise in their specific field, staying current with technological advancements, and providing objective, unbiased analysis to assist in the pursuit of justice.

Q11. How do you preserve evidence?

Ans. In digital forensics, preserving evidence involves taking steps to ensure the integrity and authenticity of digital data. Here's a concise guide:

Document the System: Record system details, including hardware, software, and network configurations.

Isolate the System: Disconnect the device from networks to prevent remote tampering. Use Faraday bags for mobile devices to block signals.

Power Down Safely: Power off the device properly to avoid altering its state. If possible, use write-blocking hardware to prevent any writes to the storage.

Label and Document Storage Media: Clearly label storage media, document its condition, and use write-blocking tools to access the data without altering it.

Create a Forensic Image: Make a bit-by-bit copy of the entire storage media. Hash the image to verify its integrity. Work with the forensic image to preserve the original evidence.

Maintain Chain of Custody: Document who handles the evidence, when, and for what purpose. This establishes a clear record of the evidence's journey.

Secure Storage: Store digital evidence in a secure environment, ensuring it is protected from physical damage, tampering, or unauthorized access.

Document Procedures: Clearly document the procedures followed during the preservation process, including any tools or software used.

Adhere to Legal Standards: Follow legal and jurisdictional standards for handling digital evidence. This may include obtaining proper authorization and ensuring the admissibility of evidence in court.

Q12. Define DOS attack?

Ans. A Denial-of-Service (DoS) attack is a malicious attempt to disrupt the normal functioning of a computer system, network, or service by overwhelming it with a flood of illegitimate requests or traffic. The goal is to make the target

resource unavailable to its intended users, causing a denial of service. DoS attacks can take various forms, including flooding networks with traffic, exploiting vulnerabilities to crash services, or exhausting system resources.

Q13. What is Sniffing?

Ans. Sniffing refers to the unauthorized interception of network traffic to capture and analyze data being transmitted. This activity is often conducted by attackers using "sniffers" or "packet sniffers," which are tools designed to monitor and collect data from a network. Sniffing can expose sensitive information such as usernames, passwords, and other confidential data if it's transmitted in an unencrypted form. It's a security concern, and network administrators use encryption protocols like HTTPS to mitigate the risk of data being easily intercepted during transmission.

Q14. Define Spoofing?

Ans. Spoofing in digital forensics refers to the act of deceiving or manipulating systems, processes, or data by presenting false or misleading information to make it appear authentic. This can involve various techniques and methods to impersonate a legitimate entity or alter the characteristics of data to mislead investigators or compromise the integrity of digital evidence.

Q15. Define First Response and First Responder?

Ans. **First Response**: The immediate actions and measures taken in reaction to an emergency or crisis situation. It involves the initial steps to assess, manage, and address the situation promptly.

First Responder: An individual, typically trained and equipped in emergency response, who arrives first at the scene of an incident. Examples include paramedics, police officers, and firefighters. Their role is crucial in providing immediate assistance and stabilizing the situation

Q16.What is Steganography?

Ans. Steganography is the technique of hiding data within an ordinary, nonsecret file or message to avoid detection; the hidden data is then extracted at its destination. Steganography use can be combined with encryption as an extra step for hiding or protecting data.

Q17. What is Cryptography?

Ans. Cryptography is the practice and study of techniques for securing communication and information from adversaries. It involves the use of mathematical algorithms to transform information into a format that is unintelligible to unauthorized individuals. The primary goal of cryptography is to provide confidentiality, integrity, and authenticity to data.

Q18. What is Rainbow Attack?

Ans. Rainbow Attack is a type of cryptographic attack on password hashes. It involves precomputing and storing the hashes of a large number of possible passwords in a table, known as a rainbow table. This table is then used to quickly reverse hashed passwords, exploiting the limited key space of most passwords and making it easier to find the original plaintext password. Rainbow attacks highlight the importance of using strong, unique passwords and employing additional security measures like salting to enhance password security.

Q19. Explain about Digital Signature? How does electronic Signature is differ from the Digital Signature?

Ans. A digital signature is a cryptographic technique that uses public-key infrastructure (PKI) to provide authentication, data integrity, and non-repudiation. It involves the use of a private key to sign a document and a corresponding public key to verify the signature. Digital signatures often come with encryption standards, making them more secure and less prone to tampering. They are authenticated using a digital signature certificate issued by licensed certifying authorities.

Feature	Digital signature	Electronic signature
Purpose	Used to protect the document	Used mainly to verify the document
Regulation and third parties' participation	A digital signature is authorized and regulated by certification authorities	It is usually not regulated
Use of cryptographic algorithms	A digital signature is created using cryptographic algorithms	Significantly less protected. No cryptographic algorithms are used
Verification	A digital signature can be verified. To obtain a digital signature, a person has to produce proof of identity	An electronic signature cannot be verified
Advantages	Preferred over an electronic signature because of its higher level of authenticity	Easy to use, but the degree of evidential value is lower
The intention of the signer	The signer is particularly concerned about the security of the document	The signer indicates the intention to agree to the contract terms and conditions
Visual mark	The "fingerprint" of the signature is embedded in a document signed using a digital certificate	An electronic signature is considered to be not only a handwritten signature but also a password, a PIN code, or any other expression of consent

Q20. What is the full form of SMTP ?What is the use of SMTP?

Ans. The full form of SMTP is the Simple Mail Transfer Protocol. It is a basic protocol for sending emails via servers between two computers on a TCP / IP network. It is part of the TCP / IP protocol application level, which makes it easy to deliver email messages to one or more recipients over the network.

Q21. What is Cyber Laws? How it is impacts on corporate?

Ans. Cyber laws, also known as cybersecurity laws or internet laws, are a set of legal regulations that govern online activities, data protection, and the use of digital technologies. These laws are designed to address various issues related to the internet, computer systems, and electronic information.

The impact of cyber laws on corporations is significant. Some key aspects include:

Data Protection and Privacy: Cyber laws often include regulations regarding the collection, storage, and processing of personal data. Compliance with these laws is crucial for corporations to protect customer privacy and avoid legal consequences.

Intellectual Property Protection: Cyber laws help safeguard intellectual property rights in the digital realm. Corporations need to respect and adhere to copyright, trademark, and patent laws to protect their own intellectual assets and avoid infringing on others'.

Cybersecurity Standards: Laws may establish cybersecurity standards that corporations must follow to protect their systems and data from cyber threats. Compliance with these standards helps mitigate the risk of cyberattacks.

E-Commerce Regulations: For businesses engaged in online transactions, cyber laws often govern electronic contracts, digital signatures, and consumer protection in e-commerce. Compliance ensures legal validity and trust in online business transactions.

Incident Response and Reporting: Cyber laws may require corporations to have incident response plans in place and to report certain types of cyber incidents promptly. This helps in addressing and mitigating the impact of cyber threats.

Employee Training and Awareness: Legal requirements related to cybersecurity often necessitate employee training and awareness programs within corporations. This is crucial for maintaining a secure digital environment.

Liability and Legal Consequences: Non-compliance with cyber laws can lead to legal consequences, including fines and penalties. Corporations need to be aware of and adhere to these laws to avoid financial and reputational damage.

Q22. Define RAID? What are the various types of RAID are there? Explain each of them?

Ans. RAID, which stands for Redundant Array of Independent Disks, is a storage technology that combines multiple physical drives into a single logical unit for data redundancy, performance improvement, or both.

There are several RAID levels, each with its own characteristics:

RAID 0 (Striping):

Description: Data is split across multiple drives for increased performance.

Advantages: Improved read/write speeds.

Disadvantages: No data redundancy; if one drive fails, all data is lost.

RAID 1 (Mirroring):

Description: Data is duplicated on two drives for redundancy.

Advantages: Data redundancy; if one drive fails, data is still available.

Disadvantages: Half of the total storage is used for redundancy.

RAID 5 (Striping with Parity):

Description: Data is striped across multiple drives with distributed parity for fault tolerance.

Advantages: Good balance between performance and redundancy.

Disadvantages: Reduced performance during a drive failure; rebuilding process can stress the system.

RAID 6 (Striping with Dual Parity):

Description: Similar to RAID 5, but with dual parity for increased fault tolerance.

Advantages: Can withstand the failure of two drives simultaneously.

Disadvantages: More complex and requires a minimum of four drives.

RAID 10 (Mirrored Striping):

Description: Combination of RAID 1 and RAID 0; data is mirrored and striped.

Advantages: High performance and redundancy.

Disadvantages: Requires a minimum of four drives; half of the total storage is used for redundancy.

RAID 50 (Striping with Distributed Parity and Mirroring):

Description: Combines RAID 5 and RAID 0; data is striped across RAID 5 arrays with a RAID 0 stripe.

Advantages: Improved performance and fault tolerance.

Disadvantages: Complex and requires a minimum of six drives.

RAID 60 (Striping with Dual Parity and Mirroring):

Description: Similar to RAID 50 but with dual parity for increased fault tolerance.

Advantages: Improved fault tolerance compared to RAID 50.

Disadvantages: Requires a minimum of eight drives.

Q23. What are the various components of Hard Disc Drives ?Explain each of them?

Ans. Hard Disk Drives (HDDs) consist of several components that work together to store and retrieve data:

Platters: These are circular, flat disks made of a magnetic material. Data is stored on the surface of these platters in the form of magnetic patterns.

Read/Write Heads: Positioned above and below each platter, these heads are responsible for reading and writing data. They move rapidly across the surface of the platters during operation.

Actuator Arm: The actuator arm holds the read/write heads and positions them over the desired track on the platter. Movement of the actuator arm is controlled by the actuator motor.

Actuator Motor: This motor moves the actuator arm, allowing precise positioning of the read/write heads. The speed and accuracy of this movement impact the overall performance of the HDD.

Spindle: The platters are attached to a spindle, and the spindle motor rotates them at a constant speed. The rotational speed, measured in revolutions per minute (RPM), affects the speed at which data can be accessed.

Controller Board (PCB): This board contains the electronics responsible for controlling the operation of the hard drive. It includes the firmware, which is a set of instructions that govern the drive's behavior.

Cache or Buffer: A small amount of high-speed volatile memory (RAM) is used as a buffer to temporarily store data being read or written. This helps improve overall system performance.

Connectors and Interface: HDDs have connectors and interfaces that allow them to be connected to the motherboard of a computer. Common interfaces include SATA and, in older systems, IDE (Integrated Drive Electronics).

Casing/Enclosure: The outer casing or enclosure protects the internal components from dust, moisture, and physical damage. It also helps dissipate heat generated during operation.

Q24. Explain Compact Disc and its type ?

Ans. A Compact Disc (CD) is a digital optical disc storage format used to store and play back audio, video, and other data.but later expanded to encompass data storage, including software and other multimedia content. CDs revolutionized the music industry and played a significant role in the transition from analog to digital audio. It typically has a diameter of 120 mm and can store up to 700 MB of data.

There are several types of CDs:

CD-DA (Compact Disc Digital Audio): The standard audio CD format used for music playback. It can hold up to 74 minutes of audio.

CD-ROM (Compact Disc Read-Only Memory): Designed for computer data storage. It is read-only and used for distributing software and multimedia applications.

CD-R (Compact Disc Recordable): Users can record data onto this type of CD, but the data cannot be erased or re-recorded once it's written.

CD-RW (Compact Disc Re-Writable): Unlike CD-R, CD-RW allows for multiple recording sessions and erasing of data, making it rewritable.

CD-ROM XA (Extended Architecture): An extension of CD-ROM that allows for mixed-mode data, combining audio and computer data on the same disc.

Video CD (VCD): A format for storing video content on a CD, providing a lower-quality alternative to DVDs.

Super Audio CD (SACD): An audio format providing higher audio quality than standard CDs, especially in terms of surround sound.

Photo CD: Developed by Kodak, it allows storage of digital photos on a CD for viewing on compatible devices.

Q25. Explain different categories of Computer forensic tools?

Ans. Computer forensic tools can be categorized based on their functionality and purpose:

Disk and File Analysis Tools:

Purpose: Examine and analyze data at the disk and file system level.
Examples: EnCase, FTK (Forensic Toolkit), Autopsy.

Network Forensic Tools:

Purpose: Monitor and analyze network traffic for evidence.
Examples: Wireshark, Network Miner, tcp dump.

Memory Forensic Tools:

Purpose: Extract and analyze volatile memory for evidence.
Examples: Volatility, Rekall, WinDbg.

Mobile Forensic Tools:

Purpose: Extract and analyze data from mobile devices.
Examples: Cellebrite, Oxygen Forensic Detective, XRY.

Database Forensic Tools:

Purpose: Investigate and analyze data stored in databases.
Examples: SQLiteSpy, DbVisualizer, Forensic Toolkit (FTK) Database.

Malware Analysis Tools:

Purpose: Analyze and dissect malicious software.
Examples: IDA Pro, OllyDbg, VirusTotal.

Forensic Imaging Tools:

Purpose: Create bit-for-bit copies of storage devices for analysis.
Examples: dd, FTK Imager, Win32 Disk Imager.

Steganography Detection Tools:

Purpose: Detect hidden information within files.
Examples: StegExpose, Stegdetect, Gargoyle.

Password Cracking Tools:

Purpose: Recover passwords to access protected files or systems.
Examples: John the Ripper, Hashcat, Cain and Abel.

Live Analysis Tools:

Purpose: Examine a system without altering its state.
Examples: Sysinternals Suite, Helix3 Pro.

Log Analysis Tools:

Purpose: Analyze system and application logs for evidence.
Examples: ELK Stack (Elasticsearch, Logstash, Kibana), Splunk.

Q26. What is IT Act 2000? When it was first time Amended?

Ans. The Information Technology Act, 2000 is an Indian legislation that provides legal recognition for electronic transactions and facilitates e-governance by recognizing electronic records and digital signatures. It was enacted on June 9, 2000, and came into force on October 17, 2000. The primary objectives of the IT Act, 2000 include regulating and promoting the secure and effective use of electronic records and facilitating electronic commerce.

The Information Technology (Amendment) Act, 2008 was introduced to address emerging challenges in the field of information technology and electronic transactions. It came into effect on October 27, 2009. The amendments focused on enhancing the legal framework to deal with issues such as cyber threats, data protection, and electronic governance. The amended act also introduced new offenses and increased penalties for certain cybercrimes.

Q27. What is Chain of Custody?

Ans. Chain of custody refers to the chronological documentation or paper trail that records the sequence of custody, control, transfer, analysis, and disposition of physical or electronic evidence. This process is crucial in legal and forensic contexts to ensure the integrity and admissibility of evidence in a court of law.

In various fields such as law enforcement, forensics, and legal proceedings, maintaining a clear chain of custody is essential to demonstrate that the evidence collected has not been tampered with, altered, or contaminated during its handling. This documentation typically includes details about who collected the evidence, when and where it was collected, who has had possession of it, and any changes or transfers of possession that occurred.

The chain of custody is designed to provide transparency and accountability, ensuring that the evidence presented in court is reliable and has not been compromised. It helps establish the authenticity of the evidence and enables the court to assess its credibility. If there are breaks in the chain of custody, it may raise doubts about the reliability of the evidence and could potentially affect its admissibility in legal proceedings.

Q28. What are different types of Hackers? Explain each of them.

Ans. A Hacker is a person who is intensely interested in the mysterious workings of any computer operating system. Hackers are most often programmers. They gather advanced knowledge of operating systems and programming languages and discover loopholes within systems and the reasons for such loopholes. There are generally 10-types of Hackers, they are:

White Hat Hackers: White hat hackers are the one who is authorized or the certified hackers who work for the government and organizations by performing penetration testing and identifying loopholes in their cybersecurity. They also ensure the protection from the malicious cyber crimes. They work under the rules and regulations provided by the government, that's why they are called Ethical hackers or Cybersecurity experts.

Black Hat Hackers: They are often called Crackers. Black Hat Hackers can gain the unauthorized access of your system and destroy your vital data. The method of attacking they use common hacking practices they have learned earlier. They are considered to be as criminals and can be easily identified because of their malicious actions.

Gray Hat Hackers: Gray hat hackers fall somewhere in the category between white hat and black hat hackers. They are not legally authorized hackers. They work with both good and bad intentions; they can use their skills for personal gain. It all depends upon the hacker. If a gray hat hacker uses his skill for his personal gains, he/she is considered as black hat hackers.

Script Kiddies: They are the most dangerous people in terms of hackers. A Script kiddie is an unskilled person who uses scripts or downloads tools available for hacking provided by other hackers. They attempt to attack computer systems and networks and deface websites. Their main purpose is to impress their friends and society. Generally, Script Kiddies are juveniles who are unskilled about hacking.

Green Hat Hackers: They are also amateurs in the world of hacking but they are bit different from script kiddies. They care about hacking and strive to become full-blown hackers. They are inspired by the hackers and ask them

few questions about. While hackers are answering their question they will listen to its novelty.

Blue Hat Hackers: They are much like the white hat hackers; they work for companies for security testing of their software right before the product launch. Blue hat hackers are outsourced by the company unlike white hat hackers which are employed by the (part of the) company.

Red Hat Hackers: They are also known as the eagle-eyed hackers. Like white hat hackers, red hat hackers also aims to halt the black hat hackers. There is a major difference in the way they operate. They become ruthless while dealing with malware actions of the black hat hackers. Red hat hacker will keep on attacking the hacker aggressively that the hacker may know it as well have to replace the whole system.

State/Nation Sponsored Hackers: State or Nation sponsored hackers are those who are appointed by the government to provide them cybersecurity and to gain confidential information from other countries to stay at the top or to avoid any kind of danger to the country. They are highly paid government workers.

Hacktivist: These are also called the online versions of the activists. Hacktivist is a hacker or a group of anonymous hackers who gain unauthorized access to government's computer files and networks for further social or political ends.

Malicious Insider or Whistleblower: A malicious insider or a whistleblower could be an employee of a company or a government agency with a grudge or a strategic employee who becomes aware of any illegal activities happening within the organization and can blackmail the organization for his/her personal gain.