1. What is the Role of Digital Evidence Acquisition in Forensics?

Answer: Digital evidence acquisition is the process of copying data from an electronic device in a manner that ensures the integrity of the evidence. The two main types of acquisition are:

- **Static Acquisition**: Captures data when the system is turned off, preventing alterations.
- **Live Acquisition**: Captures volatile data while the system is running, which is useful for encrypted drives or active systems.
  The goal is to create a bit-by-bit copy of the storage device, ensuring that no data is lost or altered during the investigation(FCL-ppt-3).

---

2. Explain the Process of Forensic Duplication and its Importance.

Answer: **Forensic duplication**, also known as **bit stream imaging**, is the process of creating an exact replica of data from storage devices like hard drives, USBs, or mobile phones. This process is essential because it allows investigators to work on a copy of the evidence while preserving the original data intact. There are two types of copying methods:

- **Logical Backup**: Copies files and directories but not deleted or hidden data.
- **Bit Stream Imaging**: Copies all sectors, including deleted files and slack space, providing a complete forensic image .

---

3. Describe the Importance of Validation and Verification in Digital Forensics.

Answer: **Validation and Verification** ensure that the tools and methods used in forensic investigations produce accurate and reliable results. Validation confirms that a tool works as intended, while verification proves that the output matches the original evidence. This is often done by calculating hash values like **MD5** or **SHA-1**. Tools like **FTK** and **EnCase** support validation by calculating hash sets during data acquisition .

---

4. What are the Key Features of the Advanced Forensic Format (AFF)?

Answer: The **Advanced Forensic Format (AFF)** is an open-source acquisition format developed to improve forensic investigation processes. Key features include:

- **Compression support** for large data sets.
- **No size restrictions**, allowing large-scale investigations.
- **Extensibility and metadata storage** for additional evidence information. AFF is widely used because it allows vendors to freely implement and extend the format across different platforms .

5. How is Mobile Forensics Conducted and What are its Challenges?

Answer: **Mobile device forensics** involves extracting data from devices like smartphones, GPS units, and tablets. Common data includes call logs, SMS messages, multimedia files, and GPS data. However, challenges in mobile forensics arise due to:

- **Diverse operating systems** and storage formats.
- **Frequent hardware updates** and encryption, making standardization difficult. Tools like **UFED** and **XRY** are widely used to retrieve data from these devices (FCL-ppt-3).

---

6. Explain the Role of Network and Wireless Forensics.

Answer:

- **Network Forensics** focuses on monitoring and analyzing network traffic to collect evidence for intrusion detection and cybercrime investigations. Since network traffic is volatile and transient, network forensics often requires real-time monitoring.
- **Wireless Forensics** deals with the collection and analysis of data transmitted over wireless networks. It includes methods for analyzing both plain data and **VoIP** (Voice-over-IP) conversations .

---

7. What is the Function of a Write-Blocker in Forensics?

Answer: A **write-blocker** is a tool used to prevent any changes to data on a storage device during forensic analysis. There are two types:

- **Hardware Write-Blockers**: Prevent the operating system from writing data to a connected drive.
- **Software Write-Blockers**: Run on the system and prevent any write operations on specified drives. Write-blockers are essential for ensuring that the original data remains unaltered, maintaining its admissibility in court .

---

8. Discuss the Importance of Hashing in Digital Forensics.

Answer: **Hashing** is the process of generating a fixed-length string (hash value) from data, ensuring data integrity. Common hash algorithms include **MD5** and **SHA-1**. Hashing is critical in forensics to verify that evidence has not been tampered with. Investigators compare hash values of original and copied data to ensure they are identical, proving that the copy is an exact replica .

---

9. What is Data Carving, and How is it Used in Forensics?

Answer: **Data carving** is a forensic technique used to recover files based on file signatures rather than file system metadata. This is particularly useful for recovering deleted or fragmented files. Tools scan the raw data on a storage device, reassembling files that are no longer listed in the file directory. Data carving is widely used in cases where file systems are corrupted or intentionally tampered with .

---

10. How is Memory Forensics Different from Traditional Disk Forensics?

Answer: **Memory forensics** involves capturing and analyzing data stored in a computer's **RAM** (Random Access Memory). Unlike disk forensics, which deals with static data, memory forensics focuses on **volatile data** that exists only while the system is running, such as running processes, open network connections, and encryption keys. Memory dumps are captured using specialized tools to preserve evidence of active sessions .