

## Answers to the Short Answer Questions

1. List any three private sector computer crimes.

- **Data Breaches**  
Unauthorized access to sensitive customer or company data, often to sell or misuse the information.
- **Intellectual Property Theft**  
Stealing copyrighted materials, patents, or trademarks from private-sector companies for personal or commercial gain.
- **Distributed Denial of Service (DDoS) Attacks**  
Overloading a company's servers with excessive traffic to disrupt operations or harm its reputation.
- **Financial Fraud**  
Hacking into company systems to manipulate financial records, steal funds, or execute unauthorized transactions.
- **Cyber Fraud**  
Deceptive practices, such as phishing or creating fake websites, to steal money or sensitive information from private companies or their clients.

2. Describe the different types of storage formats used for storing collected digital evidence.

- **Raw Format :** The raw format is a bit-for-bit, **uncompressed copy of the original data stored on a storage medium**. It captures all the data from the source device, **including the filesystem, unallocated space, and slack space, making it ideal for forensic analysis**.

The advantages of the raw format are fast data transfers and the capability to ignore minor data read errors on the source drive.

### **Characteristics:**

- ✓ Uncompressed:  
Data is stored without any compression, maintaining the exact original size.
- ✓ File Extensions:  
Typically saved with extensions like .dd, .img, or .raw.
- ✓ Simple Structure:  
No additional metadata is added, making the format straightforward to create and analyze.

- **Proprietary Formats :**

Proprietary formats are specialized file formats developed by specific forensic tools or software vendors. These formats often include features such as compression, encryption, and metadata storage, tailored to optimize forensic analysis and evidence preservation.

Characteristics:

- ✓ Tool-Specific:

Can only be fully utilized by the tools that created them (though some allow partial access via other tools).

- ✓ Feature-Rich:

Often include metadata about the imaging process, case details, and investigator notes.

- ✓ Compression and Encryption:

Reduce file size and enhance security while maintaining data integrity.

- **Advanced Forensic Format**

The Advanced Forensic Format (AFF) is an open, flexible, and extensible format designed for storing digital forensic images and associated metadata. It was developed to address the limitations of proprietary formats by offering a non-restrictive and feature-rich alternative.

Characteristics:

- ✓ Open Source:

Designed to be openly available and compatible with a wide range of forensic tools.

- ✓ Modular Design:

Stores data and metadata in separate, easily manageable sections.

- ✓ Support for Compression and Encryption:

Reduces storage size and ensures secure evidence storage.

### 3. Analyse how deleted data in solid state storage devices possess a challenge for investigation?

Deleted data in solid-state storage devices (SSDs) poses unique challenges for forensic investigations due to the underlying technology and mechanisms used in SSDs. The primary challenges are

- SSDs use **Wear-Leveling Algorithm** to distribute write and erase operations evenly across memory cells to extend device lifespan.  
This constant reshuffling of data complicates the recovery of deleted data, as previous data locations **might be overwritten or moved elsewhere.**
- SSDs often **overwrite blocks** as part of their operation due to limited storage cells per block. This makes overwritten data nearly impossible to retrieve.

- SSDs **do not have slack space** (unused portions of storage within allocated blocks) like HDDs do. The absence of slack space reduces the chance of finding remnants of deleted files.
- Many modern SSDs use hardware-based **encryption** to enhance data security. If encryption is enabled and keys are erased or inaccessible, the data becomes unreadable.
- **Limited Forensic Tools** in SSD. Investigators may need specialized tools or techniques that are not universally available or well-documented.
- SSDs require periodic power to retain their state, especially for data in the cache or volatile memory. A powered-off SSD may lose temporary or cached data, reducing recovery chances.

#### 4. What happens when someone empties the Recycle Bin in NTFS ?

When someone empties the Recycle Bin on a computer using the NTFS (New Technology File System), the files are not immediately or completely erased. Instead, the following processes occur:

- **Deletion of File References**  
Metadata Removal: NTFS removes the reference to the file in the Master File Table (MFT), which acts as an index for all files on the storage device.  
The file's entry in the MFT is marked as "available," indicating that the space previously occupied by the file can now be overwritten.  
Effect: The data itself remains on the disk, but the operating system no longer knows its location or recognizes the file as existing.
- **Space Marked as Free**  
Logical Deletion:  
The storage space occupied by the file is flagged as free space in the NTFS file system.  
Effect: New data can overwrite the space, but until that happens, the deleted data may be recoverable using specialized tools.

#### 5. What is a data fork and a resource fork?

- **Data Fork**  
The data fork is the part of the file that contains the **actual data or content of the file**, such as the text in a document, the pixels in an image, or the binary data in an executable file.

Characteristics:

- ✓ Stores the primary content or payload of the file.
- ✓ Similar to how files are stored in other file systems like NTFS or FAT.
- ✓ Universal and easily transferable to other file systems.

Examples:

For a text file: the data fork holds the actual text.

For an image: the data fork contains the image's pixel data.

- **Resource Fork**  
The resource fork is a separate part of the file that stores additional structured information, such as metadata, configuration settings, or graphical elements like icons, menus, and dialog boxes.

Characteristics:

- ✓ Designed to store resources in a structured way, making them easily accessible to applications.

- ✓ Includes items like application settings, localization strings, and UI elements.
- ✓ Specific to macOS systems and may not be supported when transferred to other file systems.

Examples:

For an application: the resource fork might include icons, strings for error messages, or layout information for dialog boxes.

For a document: the resource fork could include formatting information or preview icons.

## 6. How the forensics acquisition method in mobile differs from that in computer system?

The forensic acquisition methods for **mobile devices** and **computer systems** differ significantly due to variations in the devices' architecture, data storage, operating systems, and security mechanisms.

### ➤ Data Storage and Structure

Mobile devices typically use flash storage which differs from the storage methods used in computer systems. They may also include external storage media, such as SD cards. The data on mobile devices is often stored using file systems such as APFS (Apple File System) for iOS devices or ext4 for Android devices. Additionally, mobile devices frequently have built-in encryption and security mechanisms that protect the data.

On the other hand, computer systems use traditional storage devices such as HDDs (Hard Disk Drives) or SSDs (Solid-State Drives), which may be formatted with file systems like NTFS (Windows), HFS+ (macOS), or ext4 (Linux). While computers can also use encryption (e.g., BitLocker on Windows or FileVault on macOS), this is often optional and not universally applied. In general, computers tend to have less complex data protection measures compared to mobile devices, making it somewhat easier to acquire data from them.

### ➤ Physical vs. Logical Acquisition

For **mobile devices**, forensic acquisition can be broadly classified into **logical acquisition** and **physical acquisition** methods:

**Logical acquisition** involves extracting data that is accessible at the user level, such as contacts, text messages, media files, app data, and other user-generated content. This method is less invasive and faster, but it may not provide access to deeper or deleted data, which is often stored in areas not directly accessible by the operating system.

**Physical acquisition** involves creating a bit-by-bit copy of the device's storage, capturing all data, including deleted files and data from unallocated space. However, this method is often more intrusive and may require specialized tools, especially if the device is protected by strong security mechanisms or encryption.

In **computer systems**, both logical and physical acquisition are common practices:

**Logical acquisition** involves extracting files, system logs, application data, and other user-accessible content. This can be done relatively easily through standard forensic tools, such as **EnCase**, **FTK Imager**, or **X-Ways Forensics**.

**Physical acquisition** in computer systems is similar to mobile devices in that it involves creating a complete bit-level copy of the drive. However, physical acquisition on computers is usually more straightforward, as the file system and storage structure are often less complex compared to mobile devices. Tools like **FTK Imager** and **dd** (on Linux) can capture everything, including deleted files and unallocated disk space.

➤ **Data Protection and Encryption**

Mobile devices often come with **Full Disk Encryption (FDE)** enabled by default, making it more difficult to access the data stored on them. Forensic investigators may need to bypass these encryption mechanisms, which may require the **PIN/password** or a **specialized unlocking tool**.

In contrast, while computers can also be encrypted, encryption is not as widely applied as in mobile devices. Systems like **BitLocker** (Windows) provides disk encryption, but many users do not enable these features. Forensic investigators can typically gain access to computer data once the password or encryption key is obtained

➤ **Device Lock and Security Mechanisms**

Mobile devices generally employ more sophisticated security mechanisms than computers. In addition to **PINs**, **fingerprint authentication**, and **facial recognition**, many mobile devices have security features such as **remote wipe** and **device locking** via mobile device management (MDM) solutions. These mechanisms can complicate the acquisition of evidence, especially if the device is remotely wiped or locked before investigators can access it.

7. Define the DiD strategy for protection

The **Defense in Depth (DiD)** strategy is a multi-layered security approach designed to protect information, systems, and networks from a wide variety of threats. The idea behind DiD is to implement multiple layers of defense at different levels, so that if one layer is breached, other layers will still provide protection, reducing the overall risk of a security breach. It combines both preventive and detective controls to ensure a comprehensive and resilient security posture.

**Advantages of the DiD Strategy:**

- ✓ **Layered Security:** By implementing multiple layers of defense, DiD reduces the likelihood of a successful attack. Even if one layer is bypassed, attackers will face additional barriers.
- ✓ **Resilience:** DiD enhances resilience by ensuring that failure in one component does not compromise the entire system. It helps mitigate risks and ensures continuous operation.
- ✓ **Early Detection:** The strategy promotes the use of multiple tools for monitoring and detection, increasing the chances of early identification of security incidents, enabling quicker responses.

8. Explain different roles of a forensics examiner

A **forensic examiner** plays a crucial role in investigating digital crimes and incidents by collecting, analyzing, and preserving digital evidence in a manner that ensures its integrity for potential use in legal proceedings.

- ✓ **Evidence Collection**

One of the primary responsibilities of a forensic examiner is to **collect digital evidence** from various devices, including computers, smartphones, servers, network devices, and external storage media (e.g., USB drives, DVDs, etc.). **Chain of custody** must be maintained, which means that the examiner must document each step of evidence handling to ensure that it is admissible in court.

### ✓ Evidence Preservation

**Preserving the integrity of digital evidence** is a critical part of the forensic examiner's role. Evidence must be secured in a way that prevents accidental alterations or damage during the collection process. Forensic examiners use methods like **creating bit-by-bit copies** (images) of storage devices to avoid modifying original evidence. They also use tools to ensure that digital evidence is stored securely and can be referenced later without any changes.

### ✓ Data Recovery

Digital evidence often involves deleted or damaged data. A forensic examiner uses specialized tools and techniques to **recover deleted files**, even from devices where data has been intentionally erased or overwritten.

### ✓ Analysis of Digital Evidence

The forensic examiner conducts detailed **analysis** of the collected data to identify and extract relevant information. This involves reviewing file systems, examining metadata, and using forensic tools to uncover hidden or encrypted data.

### ✓ Creating Forensic Reports

After analysis, forensic examiners are responsible for **documenting their findings** in detailed forensic reports. These reports must be clear, concise, and based on objective facts. The reports may include:

- The methods used for evidence collection and analysis
- The findings and interpretations of the data
- Any anomalies or relevant data discovered during the examination

## 9. What are the different types of reports?

### ➤ Preliminary Report (Initial Report)

This is an early report created shortly after the initial investigation begins, often outlining the scope and nature of the investigation. It helps set the direction for further analysis and serves as a record of the actions taken during the early stages of the investigation.

### ➤ Formal report

A **formal report consisting of facts from your findings** in the context of digital forensics is typically referred to as a **Final Forensic Report** or **Forensic Analysis Report**. This

type of report presents an objective, fact-based summary of the investigative process, the evidence collected, and the conclusions drawn from the analysis.

➤ **Examination plan**

An **examination plan** for an attorney who has retained you as a forensic expert outlines the steps and processes you will follow during the forensic investigation to gather, preserve, analyze, and report evidence. This plan is designed to ensure that the attorney has a clear understanding of the investigative approach, the objectives of the examination, and the anticipated outcomes.

➤ **Expert Witness Report**

This report is typically produced when a forensic examiner is called upon to provide expert testimony in a court case. It includes detailed findings from the investigation, along with an expert analysis that can be used to support legal arguments.

➤ **Forensic Analysis Report**

This type of report focuses specifically on the detailed analysis of the data collected during the forensic examination. It is used to present the findings of the digital evidence in a clear and structured format.


➤ **Technical Report**


A technical report focuses on the technical aspects of the forensic examination. It is often highly detailed and aimed at other forensic experts, technical staff, or law enforcement personnel.

➤ **Final Report**

The final report is the comprehensive document that summarizes the entire forensic investigation. It includes all findings, conclusions, and interpretations of the data collected. This report is often used for legal purposes and may be presented in court as part of the legal proceedings.

10. Differentiate between soft link and hard link.

Aspect	Soft Link (Symbolic Link)	Hard Link
Definition	A soft link is a pointer or shortcut to the target file's location.	A hard link is a direct reference to the file's data on the disk.
Nature	Acts as a separate file containing the path to the target file.	Acts as an additional name for the same file data.
File Reference	Points to the file's path or location.	Points to the file's inode (the actual file content).
Cross-Partition Support	Can link to files across different file systems or partitions.	Cannot link across file systems or partitions.
Target Requirement	The target file must exist; otherwise, the soft link becomes a "broken"  .	Remains valid as long as the underlying file data exists, even if the original file is deleted.

File Size	Small, as it only stores the path to the target file.	No additional space used for file data; only a directory entry is added.
Deletion Behavior	If the target file is deleted, the soft link becomes invalid.	The hard link remains functional and retains the file data until all hard links are deleted.
Usage	Commonly used for shortcuts and symbolic references. 	Used for creating multiple references to the same file.