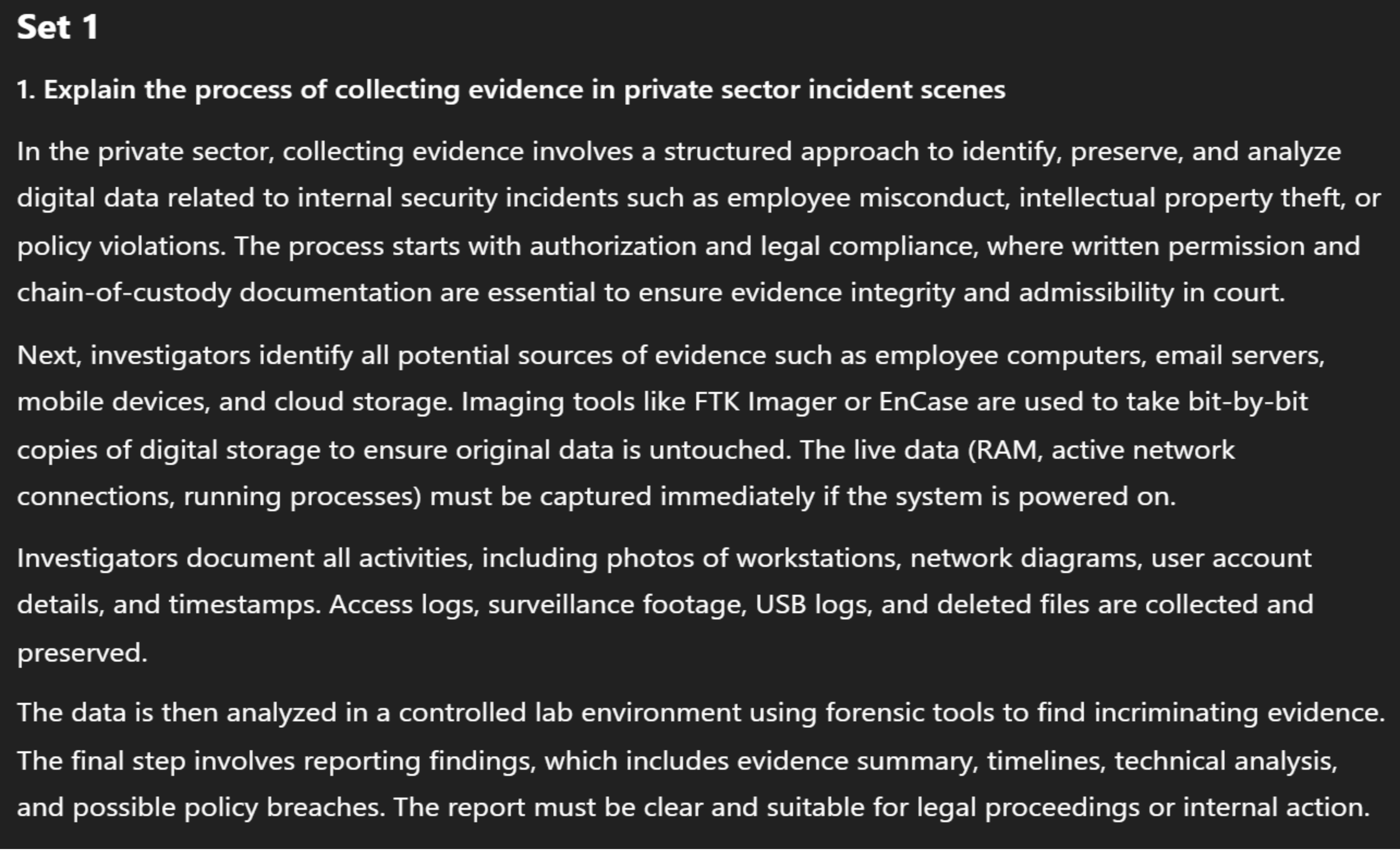


Set 1

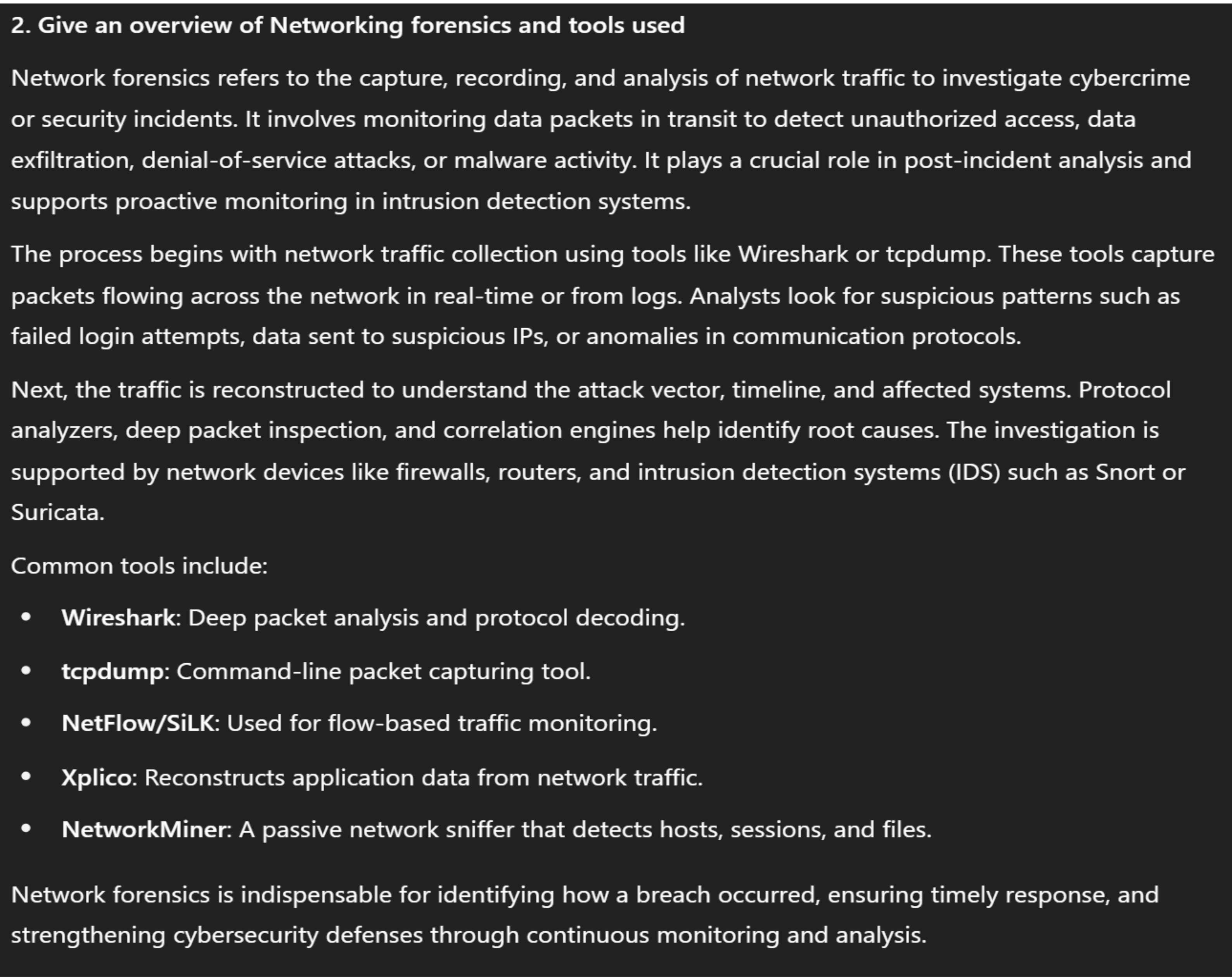
1. Explain the process of collecting evidence in private sector incident scenes

In the private sector, collecting evidence involves a structured approach to identify, preserve, and analyze digital data related to internal security incidents such as employee misconduct, intellectual property theft, or policy violations. The process starts with authorization and legal compliance, where written permission and chain-of-custody documentation are essential to ensure evidence integrity and admissibility in court.

Next, investigators identify all potential sources of evidence such as employee computers, email servers, mobile devices, and cloud storage. Imaging tools like FTK Imager or EnCase are used to take bit-by-bit copies of digital storage to ensure original data is untouched. The live data (RAM, active network connections, running processes) must be captured immediately if the system is powered on.

Investigators document all activities, including photos of workstations, network diagrams, user account details, and timestamps. Access logs, surveillance footage, USB logs, and deleted files are collected and preserved.

The data is then analyzed in a controlled lab environment using forensic tools to find incriminating evidence. The final step involves reporting findings, which includes evidence summary, timelines, technical analysis, and possible policy breaches. The report must be clear and suitable for legal proceedings or internal action.



2. Give an overview of Networking forensics and tools used

Network forensics refers to the capture, recording, and analysis of network traffic to investigate cybercrime or security incidents. It involves monitoring data packets in transit to detect unauthorized access, data exfiltration, denial-of-service attacks, or malware activity. It plays a crucial role in post-incident analysis and supports proactive monitoring in intrusion detection systems.

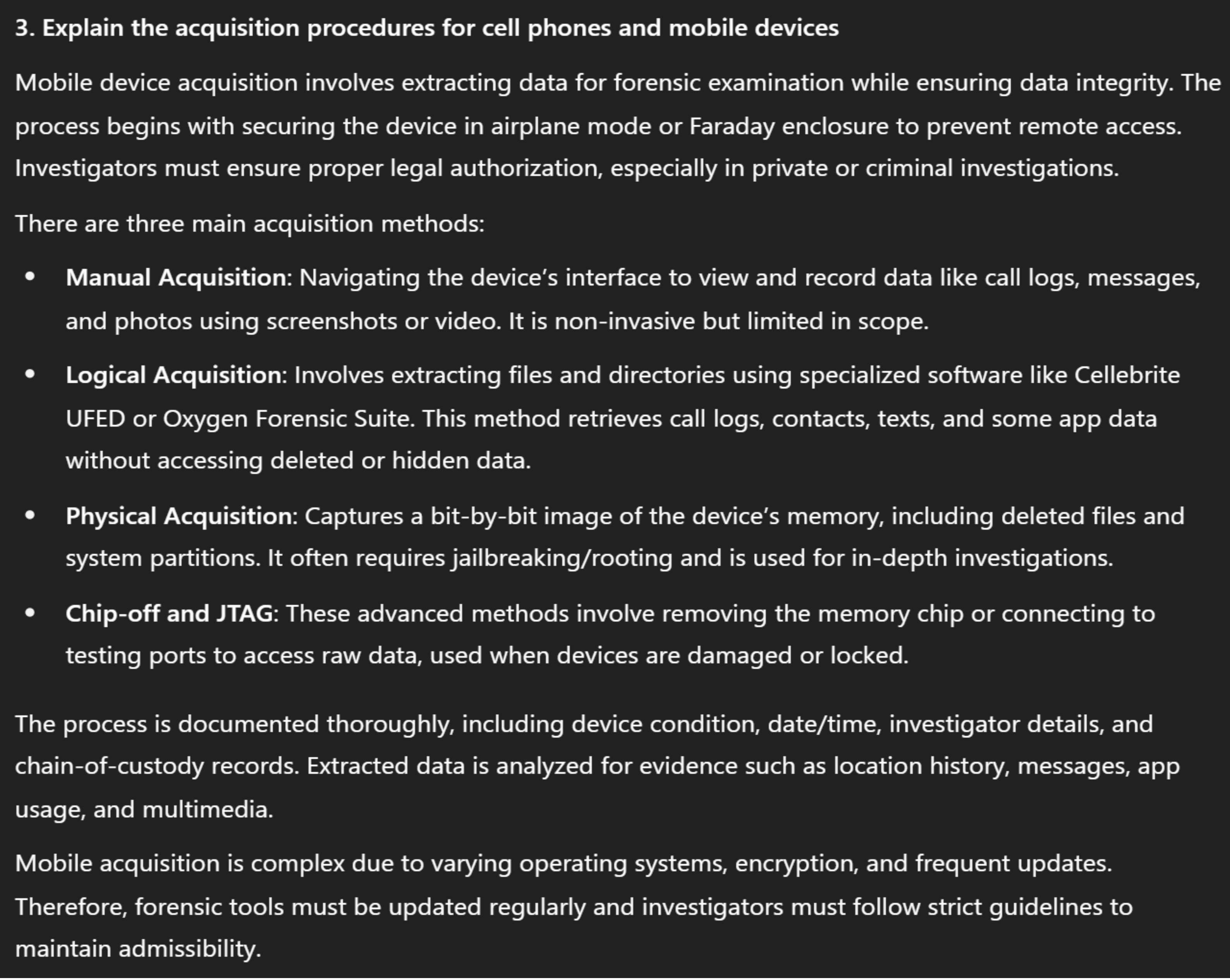
The process begins with network traffic collection using tools like Wireshark or tcpdump. These tools capture packets flowing across the network in real-time or from logs. Analysts look for suspicious patterns such as failed login attempts, data sent to suspicious IPs, or anomalies in communication protocols.

Next, the traffic is reconstructed to understand the attack vector, timeline, and affected systems. Protocol analyzers, deep packet inspection, and correlation engines help identify root causes. The investigation is supported by network devices like firewalls, routers, and intrusion detection systems (IDS) such as Snort or Suricata.

Common tools include:

- **Wireshark**: Deep packet analysis and protocol decoding.
- **tcpdump**: Command-line packet capturing tool.
- **NetFlow/SiLK**: Used for flow-based traffic monitoring.
- **Xplico**: Reconstructs application data from network traffic.
- **NetworkMiner**: A passive network sniffer that detects hosts, sessions, and files.

Network forensics is indispensable for identifying how a breach occurred, ensuring timely response, and strengthening cybersecurity defenses through continuous monitoring and analysis.



3. Explain the acquisition procedures for cell phones and mobile devices

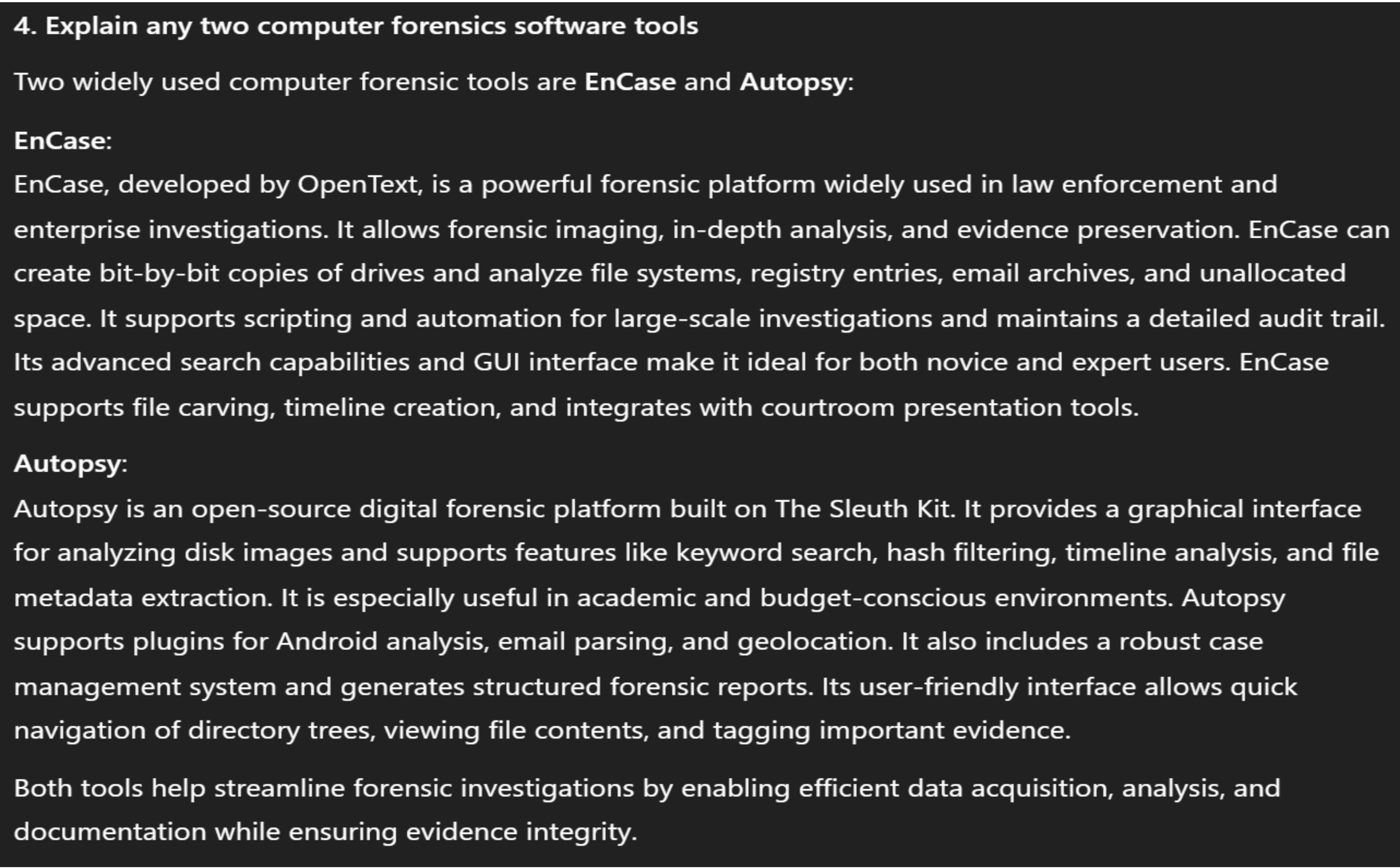
Mobile device acquisition involves extracting data for forensic examination while ensuring data integrity. The process begins with securing the device in airplane mode or Faraday enclosure to prevent remote access. Investigators must ensure proper legal authorization, especially in private or criminal investigations.

There are three main acquisition methods:

- **Manual Acquisition**: Navigating the device's interface to view and record data like call logs, messages, and photos using screenshots or video. It is non-invasive but limited in scope.
- **Logical Acquisition**: Involves extracting files and directories using specialized software like Cellebrite UFED or Oxygen Forensic Suite. This method retrieves call logs, contacts, texts, and some app data without accessing deleted or hidden data.
- **Physical Acquisition**: Captures a bit-by-bit image of the device's memory, including deleted files and system partitions. It often requires jailbreaking/rooting and is used for in-depth investigations.
- **Chip-off and JTAG**: These advanced methods involve removing the memory chip or connecting to testing ports to access raw data, used when devices are damaged or locked.

The process is documented thoroughly, including device condition, date/time, investigator details, and chain-of-custody records. Extracted data is analyzed for evidence such as location history, messages, app usage, and multimedia.

Mobile acquisition is complex due to varying operating systems, encryption, and frequent updates. Therefore, forensic tools must be updated regularly and investigators must follow strict guidelines to maintain admissibility.



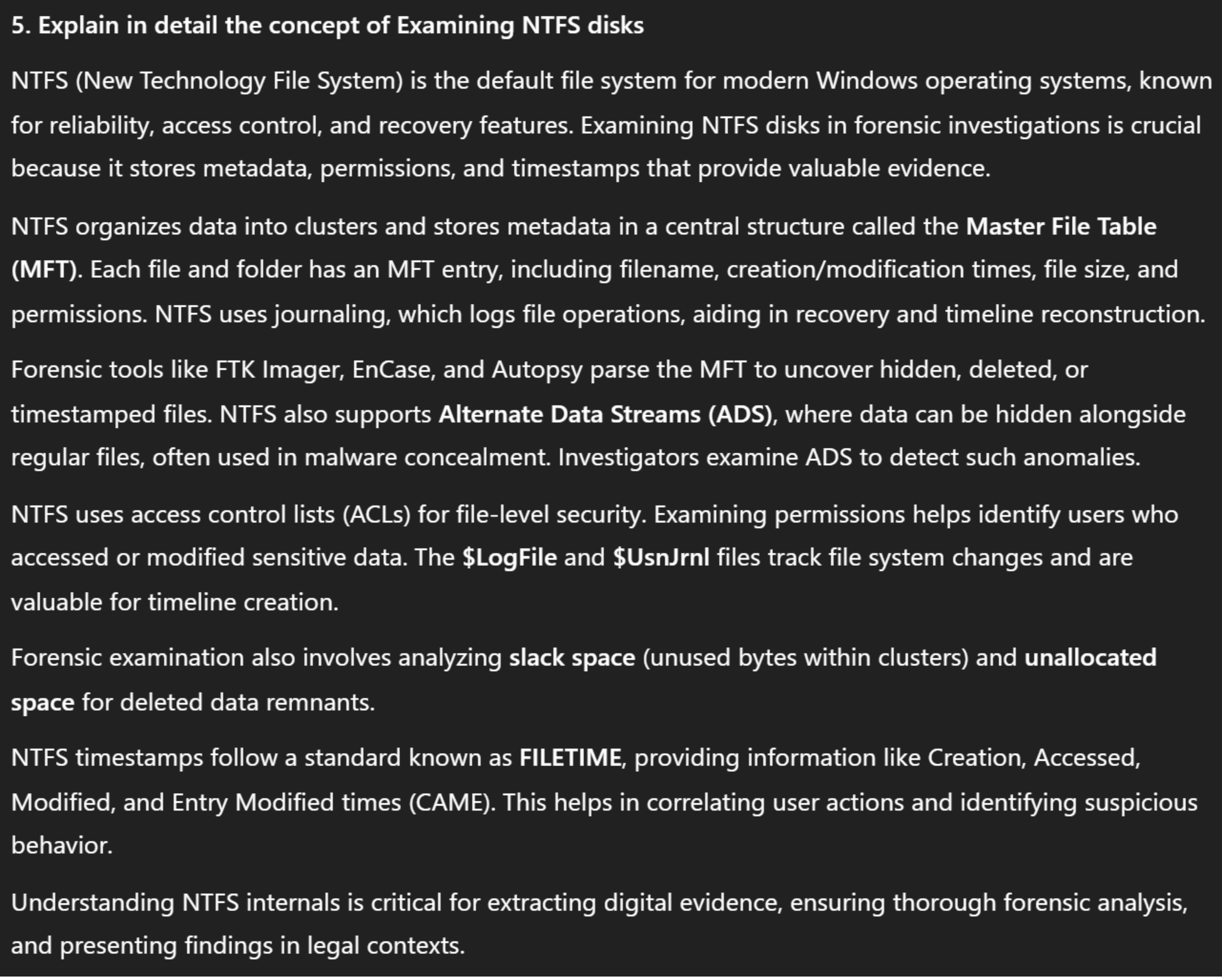
4. Explain any two computer forensics software tools

Two widely used computer forensic tools are **EnCase** and **Autopsy**:

EnCase:
EnCase, developed by OpenText, is a powerful forensic platform widely used in law enforcement and enterprise investigations. It allows forensic imaging, in-depth analysis, and evidence preservation. EnCase can create bit-by-bit copies of drives and analyze file systems, registry entries, email archives, and unallocated space. It supports scripting and automation for large-scale investigations and maintains a detailed audit trail. Its advanced search capabilities and GUI interface make it ideal for both novice and expert users. EnCase supports file carving, timeline creation, and integrates with courtroom presentation tools.

Autopsy:
Autopsy is an open-source digital forensic platform built on The Sleuth Kit. It provides a graphical interface for analyzing disk images and supports features like keyword search, hash filtering, timeline analysis, and file metadata extraction. It is especially useful in academic and budget-conscious environments. Autopsy supports plugins for Android analysis, email parsing, and geolocation. It also includes a robust case management system and generates structured forensic reports. Its user-friendly interface allows quick navigation of directory trees, viewing file contents, and tagging important evidence.

Both tools help streamline forensic investigations by enabling efficient data acquisition, analysis, and documentation while ensuring evidence integrity.



5. Explain in detail the concept of Examining NTFS disks

NTFS (New Technology File System) is the default file system for modern Windows operating systems, known for reliability, access control, and recovery features. Examining NTFS disks in forensic investigations is crucial because it stores metadata, permissions, and timestamps that provide valuable evidence.

NTFS organizes data into clusters and stores metadata in a central structure called the **Master File Table (MFT)**. Each file and folder has an MFT entry, including filename, creation/modification times, file size, and permissions. NTFS uses journaling, which logs file operations, aiding in recovery and timeline reconstruction.

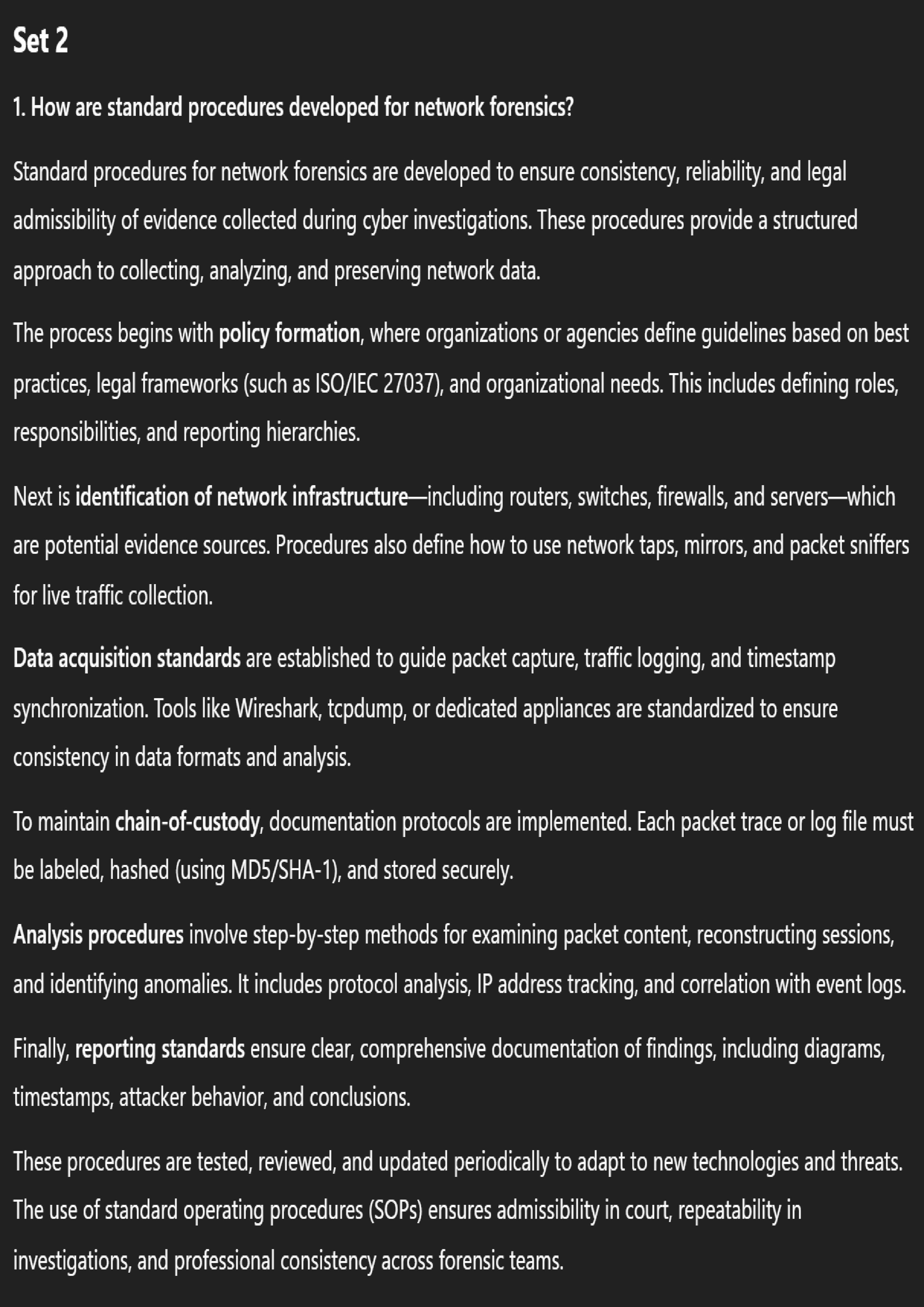
Forensic tools like FTK Imager, EnCase, and Autopsy parse the MFT to uncover hidden, deleted, or timestamped files. NTFS also supports **Alternate Data Streams (ADS)**, where data can be hidden alongside regular files, often used in malware concealment. Investigators examine ADS to detect such anomalies.

NTFS uses access control lists (ACLs) for file-level security. Examining permissions helps identify users who accessed or modified sensitive data. The **$LogFile** and **$UsnJrnl** files track file system changes and are valuable for timeline creation.

Forensic examination also involves analyzing **slack space** (unused bytes within clusters) and **unallocated space** for deleted data remnants.

NTFS timestamps follow a standard known as **FILETIME**, providing information like Creation, Accessed, Modified, and Entry Modified times (CAME). This helps in correlating user actions and identifying suspicious behavior.

Understanding NTFS internals is critical for extracting digital evidence, ensuring thorough forensic analysis, and presenting findings in legal contexts.



Set 2

1. How are standard procedures developed for network forensics?

Standard procedures for network forensics are developed to ensure consistency, reliability, and legal admissibility of evidence collected during cyber investigations. These procedures provide a structured approach to collecting, analyzing, and preserving network data.

The process begins with **policy formation**, where organizations or agencies define guidelines based on best practices, legal frameworks (such as ISO/IEC 27037), and organizational needs. This includes defining roles, responsibilities, and reporting hierarchies.

Next is **identification of network infrastructure**—including routers, switches, firewalls, and servers—which are potential evidence sources. Procedures also define how to use network taps, mirrors, and packet sniffers for live traffic collection.

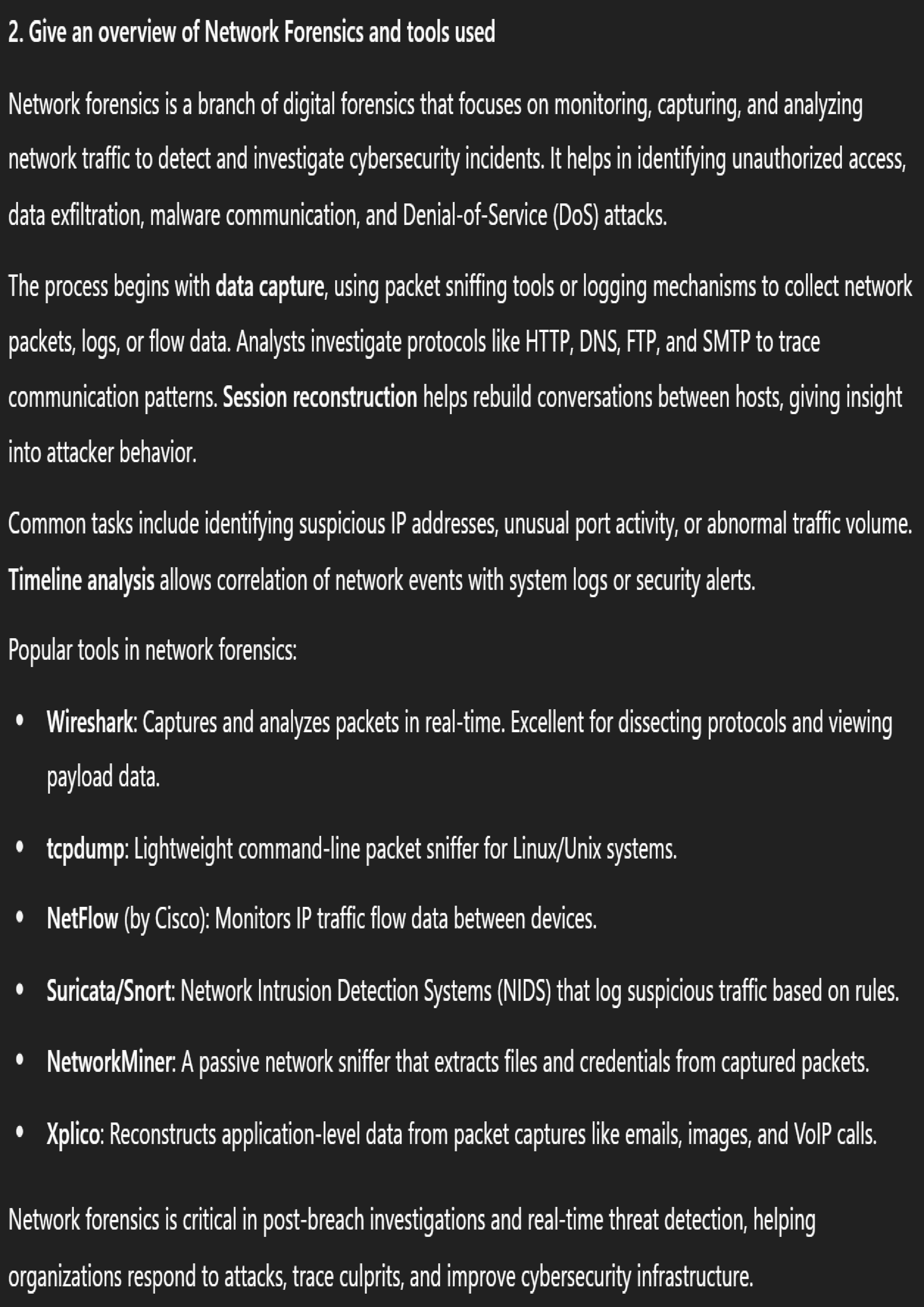
Data acquisition standards are established to guide packet capture, traffic logging, and timestamp synchronization. Tools like Wireshark, tcpdump, or dedicated appliances are standardized to ensure consistency in data formats and analysis.

To maintain **chain-of-custody**, documentation protocols are implemented. Each packet trace or log file must be labeled, hashed (using MD5/SHA-1), and stored securely.

Analysis procedures involve step-by-step methods for examining packet content, reconstructing sessions, and identifying anomalies. It includes protocol analysis, IP address tracking, and correlation with event logs.

Finally, **reporting standards** ensure clear, comprehensive documentation of findings, including diagrams, timestamps, attacker behavior, and conclusions.

These procedures are tested, reviewed, and updated periodically to adapt to new technologies and threats. The use of standard operating procedures (SOPs) ensures admissibility in court, repeatability in investigations, and professional consistency across forensic teams.



2. Give an overview of Network Forensics and tools used

Network forensics is a branch of digital forensics that focuses on monitoring, capturing, and analyzing network traffic to detect and investigate cybersecurity incidents. It helps in identifying unauthorized access, data exfiltration, malware communication, and Denial-of-Service (DoS) attacks.

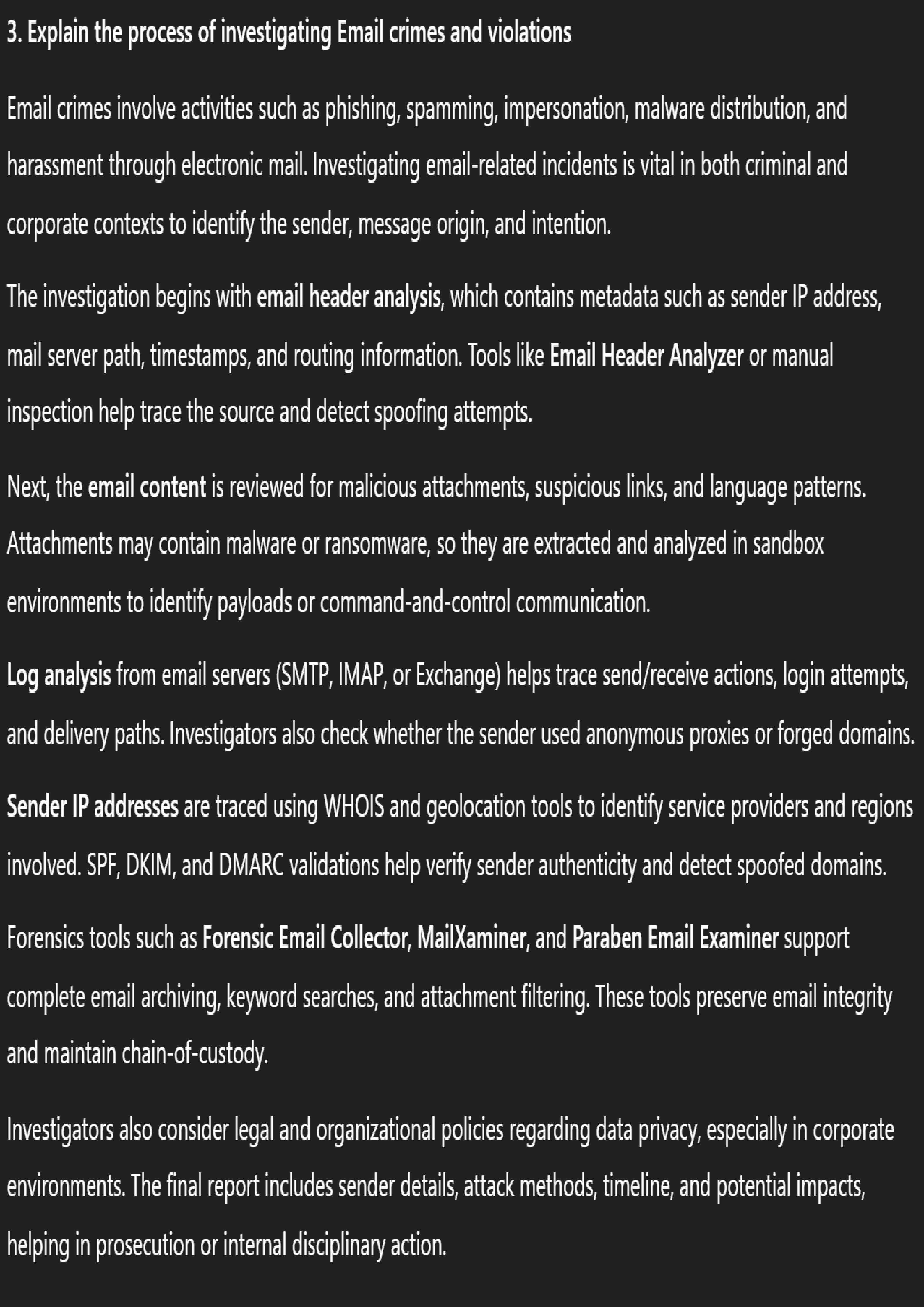
The process begins with **data capture**, using packet sniffing tools or logging mechanisms to collect network packets, logs, or flow data. Analysts investigate protocols like HTTP, DNS, FTP, and SMTP to trace communication patterns. **Session reconstruction** helps rebuild conversations between hosts, giving insight into attacker behavior.

Common tasks include identifying suspicious IP addresses, unusual port activity, or abnormal traffic volume. **Timeline analysis** allows correlation of network events with system logs or security alerts.

Popular tools in network forensics:

- **Wireshark**: Captures and analyzes packets in real-time. Excellent for dissecting protocols and viewing payload data.
- **tcpdump**: Lightweight command-line packet sniffer for Linux/Unix systems.
- **NetFlow** (by Cisco): Monitors IP traffic flow data between devices.
- **Suricata/Snort**: Network Intrusion Detection Systems (NIDS) that log suspicious traffic based on rules.
- **NetworkMiner**: A passive network sniffer that extracts files and credentials from captured packets.
- **Xplico**: Reconstructs application-level data from packet captures like emails, images, and VoIP calls.

Network forensics is critical in post-breach investigations and real-time threat detection, helping organizations respond to attacks, trace culprits, and improve cybersecurity infrastructure.



3. Explain the process of investigating Email crimes and violations

Email crimes involve activities such as phishing, spamming, impersonation, malware distribution, and harassment through electronic mail. Investigating email-related incidents is vital in both criminal and corporate contexts to identify the sender, message origin, and intention.

The investigation begins with **email header analysis**, which contains metadata such as sender IP address, mail server path, timestamps, and routing information. Tools like **Email Header Analyzer** or manual inspection help trace the source and detect spoofing attempts.

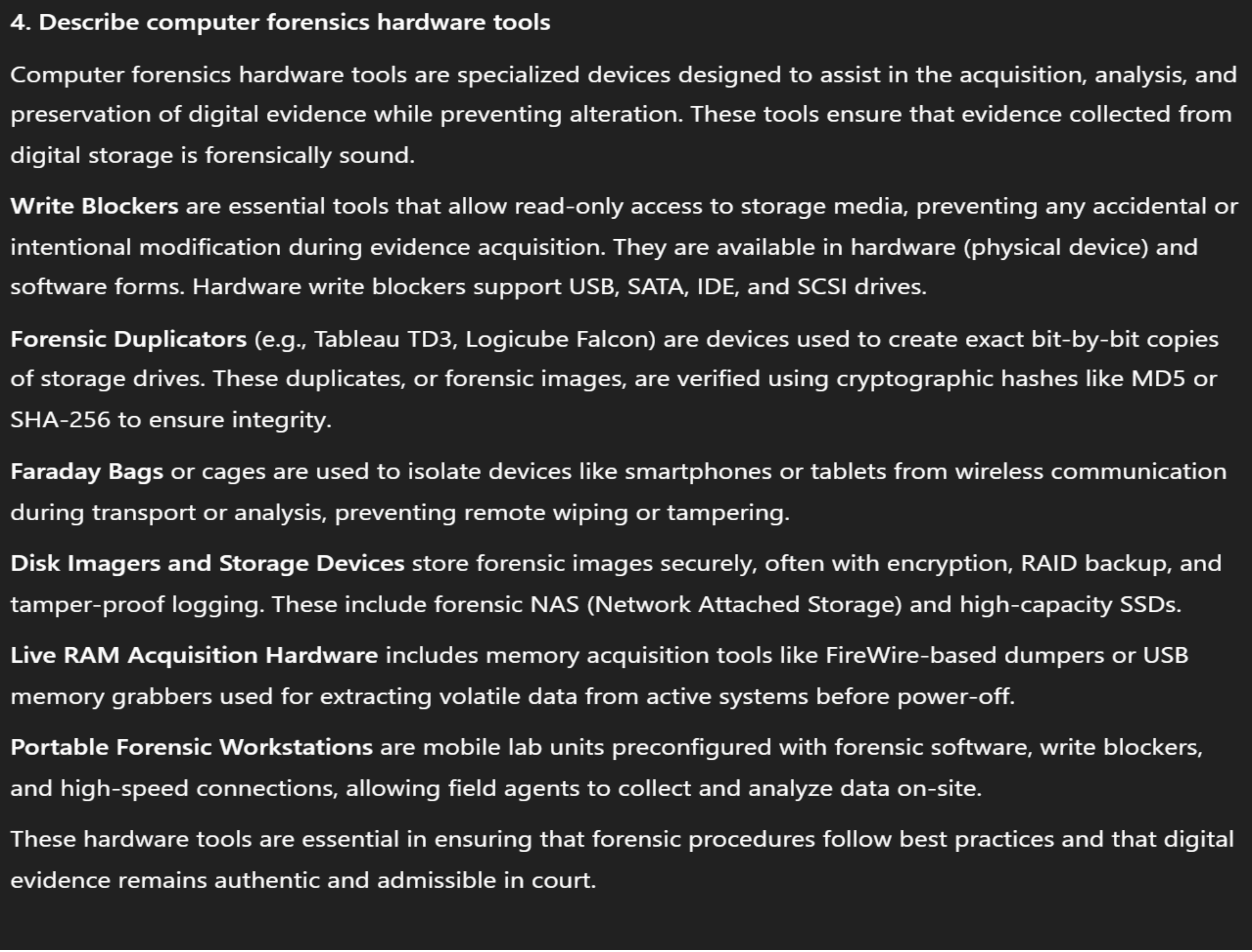
Next, the **email content** is reviewed for malicious attachments, suspicious links, and language patterns. Attachments may contain malware or ransomware, so they are extracted and analyzed in sandbox environments to identify payloads or command-and-control communication.

Log analysis from email servers (SMTP, IMAP, or Exchange) helps trace send/receive actions, login attempts, and delivery paths. Investigators also check whether the sender used anonymous proxies or forged domains.

Sender IP addresses are traced using WHOIS and geolocation tools to identify service providers and regions involved. SPF, DKIM, and DMARC validations help verify sender authenticity and detect spoofed domains.

Forensics tools such as **Forensic Email Collector**, **MailXaminer**, and **Paraben Email Examiner** support complete email archiving, keyword searches, and attachment filtering. These tools preserve email integrity and maintain chain-of-custody.

Investigators also consider legal and organizational policies regarding data privacy, especially in corporate environments. The final report includes sender details, attack methods, timeline, and potential impacts, helping in prosecution or internal disciplinary action.



4. Describe computer forensics hardware tools

Computer forensics hardware tools are specialized devices designed to assist in the acquisition, analysis, and preservation of digital evidence while preventing alteration. These tools ensure that evidence collected from digital storage is forensically sound.

Write Blockers are essential tools that allow read-only access to storage media, preventing any accidental or intentional modification during evidence acquisition. They are available in hardware (physical device) and software forms. Hardware write blockers support USB, SATA, IDE, and SCSI drives.

Forensic Duplicators (e.g., Tableau TD3, Logicube Falcon) are devices used to create exact bit-by-bit copies of storage drives. These duplicates, or forensic images, are verified using cryptographic hashes like MD5 or SHA-256 to ensure integrity.

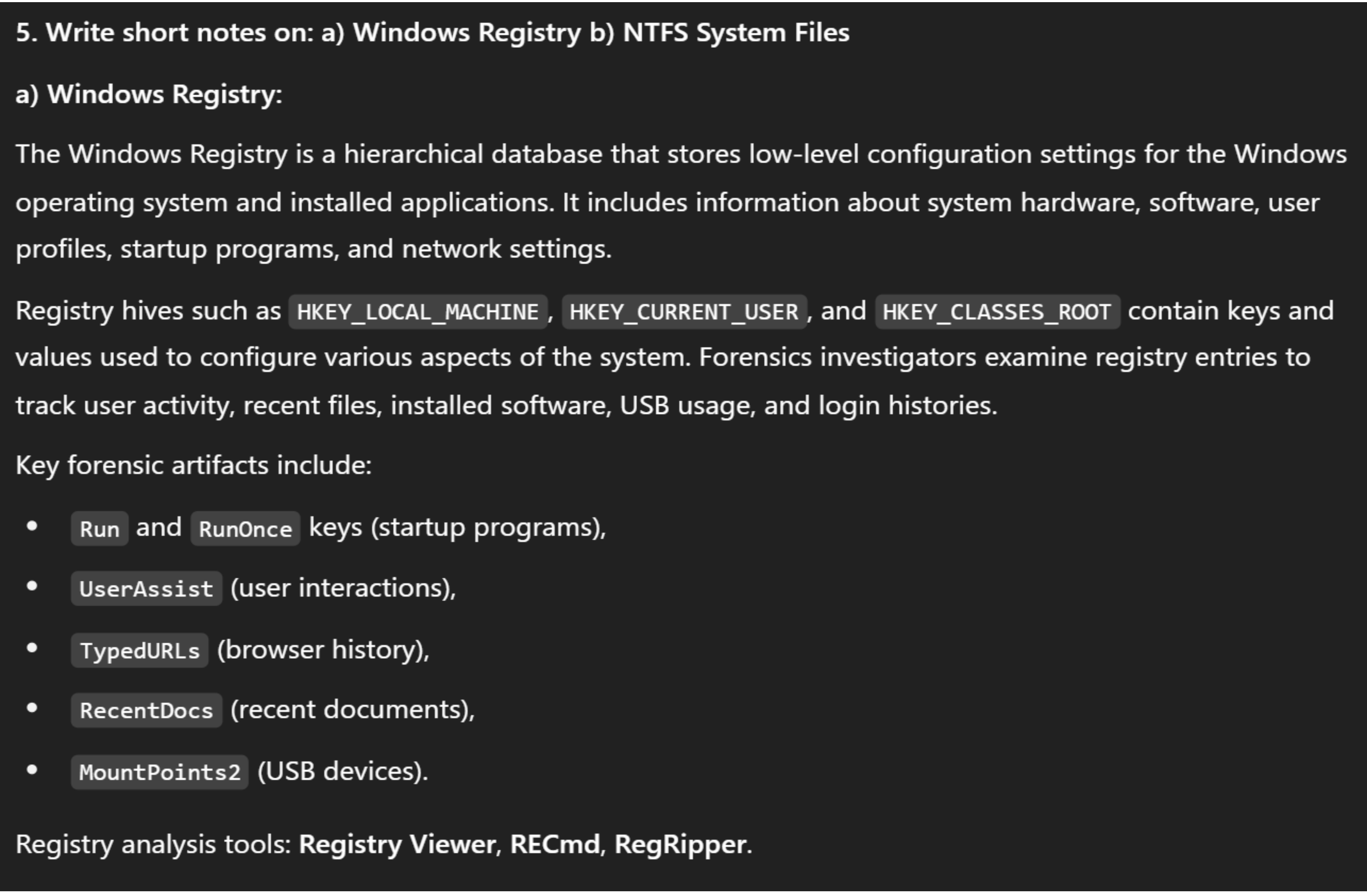
Faraday Bags or cages are used to isolate devices like smartphones or tablets from wireless communication during transport or analysis, preventing remote wiping or tampering.

Disk Imagers and Storage Devices store forensic images securely, often with encryption, RAID backup, and tamper-proof logging. These include forensic NAS (Network Attached Storage) and high-capacity SSDs.

Live RAM Acquisition Hardware includes memory acquisition tools like FireWire-based dumpers or USB memory grabbers used for extracting volatile data from active systems before power-off.

Portable Forensic Workstations are mobile lab units preconfigured with forensic software, write blockers, and high-speed connections, allowing field agents to collect and analyze data on-site.

These hardware tools are essential in ensuring that forensic procedures follow best practices and that digital evidence remains authentic and admissible in court.



5. Write short notes on: a) Windows Registry b) NTFS System Files

a) Windows Registry:

The Windows Registry is a hierarchical database that stores low-level configuration settings for the Windows operating system and installed applications. It includes information about system hardware, software, user profiles, startup programs, and network settings.

Registry hives such as `HKEY_LOCAL_MACHINE`, `HKEY_CURRENT_USER`, and `HKEY_CLASSES_ROOT` contain keys and values used to configure various aspects of the system. Forensics investigators examine registry entries to track user activity, recent files, installed software, USB usage, and login histories.

Key forensic artifacts include:

- `Run` and `RunOnce` keys (startup programs),
- `UserAssist` (user interactions),
- `TypedURLs` (browser history),
- `RecentDocs` (recent documents),
- `MountPoints2` (USB devices).

Registry analysis tools: **Registry Viewer, RECmd, RegRipper**.