Practice Questions:

**Question 1:**

You are investigating a suspect involved in a cyberstalking case. The physical image of their Android device reveals the use of secure messaging apps and cloud sync features (e.g., Telegram, Signal, Google Drive, MEGA). The device was factory reset prior to seizure, but you also have access to a companion laptop (Windows 11) used by the suspect.

**a)** Describe the approach you would take to correlate artifacts between the phone and laptop to recover deleted communications.  
**b)** What evidence sources on the laptop could help retrieve synced or cached cloud data? Mention at least two tools you would use and justify their application.  
**c)** How would you handle encrypted or zero-access containers (e.g., .enc files, VeraCrypt volumes) discovered on either device? Outline methods for key recovery or decryption attempts.

**Question 2:**

During a corporate espionage investigation, you acquire an Android device with a multi-user setup and multiple secure folder apps (e.g., Samsung Secure Folder, Shelter, and hidden vault apps). The main user profile appears clean, but logs show recent switching between user profiles.

**a)** Explain how you would identify hidden or alternate user profiles and locate secure folder containers.  
**b)** What forensic techniques can reveal or extract data from within such secure environments, even if partially encrypted or obfuscated?  
**c)** If timestamps and file metadata are manipulated to mislead investigators, what cross-validation strategies would you use to identify anomalies or reconstruct the true sequence of events?

**Question 3:**

In a digital financial fraud case, you acquire a rooted Android device. The device shows traces of tampering: modified system files, altered timestamps, presence of Xposed Framework modules, and signs of app reinstallation and data injection into messaging apps.

**a)** Describe how you would detect signs of app data manipulation and differentiate between genuine and injected content.  
**b)** What types of artifacts or log sources can help validate if a message or transaction was truly sent/received by the user? Provide two specific examples.  
**c)** Identify two Xposed modules or root-based tools commonly used for spoofing or data hiding. Explain how you would detect and counter their effects during analysis.

**Question 4:** You have acquired a physical image of a suspect’s Android device in connection with an organized fraud case. The device has several encrypted messaging and banking apps. The suspect is known to use privacy-focused applications (e.g., cleaning tools, app lockers, file shredders) regularly.

Preliminary analysis shows:

* Most chat histories, call logs, and media files from key apps are missing.
* Logs indicate recent use of a third-party cleaning app.
* Some remnants of SQLite databases and app cache folders were found in unallocated space.

You suspect that data was intentionally wiped shortly before device seizure.

1. Describe the forensic techniques you would use to recover deleted artifacts. What indicators would help you identify app-specific residuals?
2. How would you reconstruct a user activity timeline by correlating recovered timestamps from app caches, logs, and system-level artifacts (e.g., logcat, usage stats, system logs)? Provide examples of at least two types of artifacts you would rely on.
3. What specific anti-forensics features might third-party cleaning or privacy apps implement? For each, explain one method or tool that can detect or bypass these features to support evidence recovery.
4. Assume you recovered a partially overwritten msgstore.db (WhatsApp database) and obfuscated image files. Explain how you would attempt to:

* Reconstruct conversation fragments from the incomplete database.
* Match obfuscated media files to app activity or message references.
* Validate the integrity of any reconstructed communication.

**Question 5:**

You are examining an Android device seized in a human trafficking case. The suspect used anonymous communication apps and had multiple social media accounts. While most content has been deleted, you discover residual metadata (e.g., EXIF data, thumbnail caches, autofill records) and some partially deleted app databases.

1. How would you use metadata and system-level artifacts to infer user behavior and social connections? Give at least two types of metadata you would correlate.
2. What techniques can help map recovered media (even without full content) to time, location, or communication context?
3. Describe how tools like Autopsy, or Magnet AXIOM can assist in visually reconstructing a narrative from fragmented data.

**Question 6:**

In a suspected case of espionage, a seized Android device shows signs of persistent malware, covert data exfiltration channels, and rooted access. Unusual network activity, including DNS tunneling and encrypted outbound traffic to unknown servers, is noted in logs.

a) What forensic methods would you use to trace malware activity and identify data exfiltration routes on the device?

b) Explain how to extract and analyze network logs or PCAP files generated on the device. What indicators would you look for in covert channels like DNS tunneling?

c) How would you differentiate between system-level modifications made by the user and those introduced by malware? Support your answer with two types of forensic evidence.