Objective

As a Digital Forensic Analyst at Proforce Intelligence, you are tasked with performing a forensic investigation on a seized Android smartphone suspected of being involved in a corporate data breach. Your goal is to create a forensic image of the device and analyze it to extract critical information, including the mobile network, last contacted numbers, and registered email accounts associated with the device. You must use Autopsy for analysis and follow forensically sound procedures to ensure the evidence is admissible in court.

Scenario

Proforce Intelligence has received an Android smartphone (Samsung Galaxy S21, Android 13) from a corporate client investigating a potential data breach by an employee named Alex Carter. The device is suspected to contain evidence of unauthorized communications and data exfiltration. The client has provided legal authorization to seize and analyze the device. The phone is unlocked, and you have physical access to it.

Your tasks are:

1. Create a forensic image of the Android device using an image extractor tool of your choice.
2. Analyze the image using Autopsy to extract:
    - The mobile network provider used by the device.
    - The last five contacted phone numbers (via calls or messages).
    - A list of email accounts registered on the device.
3. Document your process and findings in a forensic report suitable for presentation to the client and potential use in court.

Requirements

- **Imaging Tool**: Choose any forensic imaging tool (e.g., Cellebrite UFED, Magnet AXIOM, FTK Imager, or ADB with `dd` command) to create a forensic image of the Android device. Justify your choice.
- **Analysis Tool**: Use Autopsy (version 4.21.0 or later) for all analysis tasks.
- **Deliverables**:
    - A forensic report (in PDF format) detailing your methodology, tools used, steps taken, findings, and chain of custody.
    - Screenshots or exported data from Autopsy showing the extracted information (mobile network, last contacted numbers, and registered email accounts).
    - A hash value (MD5 or SHA-1) of the forensic image to verify integrity.
- **Constraints**:
    - Ensure all actions are forensically sound (e.g., use write-blockers or read-only methods to prevent data alteration).
    - Maintain a documented chain of custody.
    - The report must be clear, concise, and suitable for both technical and non-technical audiences.

Task Instructions

Step 1: Forensic Imaging

1. **Select an Imaging Tool**: Choose a tool to create a forensic image of the Android device. Examples include:
    - **Cellebrite UFED**: For physical or logical acquisition.
    - **Magnet AXIOM**: For logical or full file system extraction.
    - **ADB with `dd` Command**: For manual imaging on rooted or unlocked devices (e.g., `adb shell dd if=/dev/block/mmcblk0 of=/sdcard/image.img`).
    - **FTK Imager**: If imaging an SD card or external storage.
2. **Create the Image**:
    - Connect the Android device to a forensic workstation using a write-blocker or enable USB debugging for read-only access.

- Perform a logical acquisition (to capture user data like contacts, messages, and emails) or a full file system/physical acquisition (to include system files and deleted data).
- Calculate and record the hash value (MD5 or SHA-1) of the image to verify integrity.

3. **Document the Process**:
   - Note the tool used, acquisition method (logical/physical), date, time, and any challenges encountered (e.g., encryption or locked partitions).
   - Record the chain of custody, including who handled the device, when, and where it was stored.

Step 2: Analysis with Autopsy

1. **Set Up Autopsy**:
   - Download and install Autopsy (version 4.21.0 or later) from autopsy.com if not already installed.
   - Create a new case in Autopsy, providing a case name (e.g., "Carter_Android_Investigation_2025") and investigator details (your name).
2. **Add the Forensic Image**:
   - Select "Disk Image" as the data source type and import the forensic image created in Step 1.
   - Configure ingest modules to include:
     - **File Type Identification**: To detect relevant file types (e.g., SQLite databases for contacts and messages).
     - **Keyword Search**: To search for email-related terms (e.g., "@gmail.com", "@outlook.com").
     - **Recent Activity**: To identify call logs and messages.
     - **Android Analyzer**: To extract Android-specific artifacts (e.g., contacts, SMS, and email accounts).
3. **Extract Required Information**:
   - **Mobile Network Provider**:
     - Look for SIM card data or network configuration files (e.g., `/system/etc/apns-conf.xml`) to identify the mobile network provider (e.g., MTN, GLO, AIRTEL)
   - **Last Contacted Numbers**:
     - Filter for call logs (`mmssms.db` or `calllog.db`) and SMS/MMS messages to identify the last five contacted phone numbers.
     - Note timestamps and whether the contact was via call or message.
   - **Registered Email Accounts**:
     - Use **Keyword Search** to find email addresses in files like `/data/data/com.google.android.gm/` (Gmail) or `/data/data/com.microsoft.outlook/` (Outlook).
     - Look for SQLite databases (e.g., `accounts.db`) containing email account details.
4. **Validate Findings**:
   - Cross-check extracted data with raw files in the image (e.g., manually inspect SQLite databases using Autopsy's file explorer).
   - Ensure timestamps and data integrity align with the investigation timeline.

Step 3: Forensic Report

Create a comprehensive forensic report in PDF format that includes:

1. **Introduction**:
   - Case background (e.g., corporate data breach involving Alex Carter or any naming of your choice).
   - Purpose of the investigation (extract mobile network, last contacted numbers, and email accounts).
2. **Methodology**:
   - Tools used (imaging tool and Autopsy).
   - Steps for imaging (e.g., acquisition method, hash verification).
   - Steps for analysis (e.g., ingest modules used, data extraction process).
3. **Findings**:
   - **Mobile Network Provider**: State the provider (e.g., "The device is registered to MTN").

    - **Last Contacted Numbers**: List the last five contacted numbers with details (e.g., phone number, date/time, call/SMS).
    - **Registered Email Accounts**: List all email accounts found (e.g., "alex.carter@gmail.com", "acarter@company.com").
    - Include screenshots or exported data from Autopsy to support findings. (**OPTIONAL**)
4. **Conclusion**:
    - Summarize key findings and their relevance to the investigation.
    - Note any limitations (e.g., encrypted partitions, inaccessible data).
5. **Technical Notes**:
    - Include the hash value of the forensic image.
    - Mention any challenges (e.g., partial data access due to Android 13 security).

Submission Guidelines

- Submit the forensic report as a PDF file named `Forensic_Report_<name_of_choice>_Android.pdf`.
- Email the deliverables to olioxxayo@gmail.com or precious@proforceintelligence.com by the specified deadline.

Evaluation Criteria

- **Accuracy**: Correct identification of the mobile network, last contacted numbers, and email accounts.
- **Forensic Soundness**: Adherence to chain of custody, use of write-blockers, and hash verification.
- **Report Quality**: Clarity, structure, and suitability for technical and non-technical audiences.
- **Tool Proficiency**: Effective use of the imaging tool and Autopsy for analysis.
- **Documentation**: Thoroughness in documenting methodology and findings.

Notes

- If you cannot access a physical Android device for imaging, simulate the task by downloading a sample Android disk image from a reputable source (e.g., dftt.sourceforge.net) and document that it's a simulation for the purpose of this task.
- Ensure Autopsy is configured to process Android-specific artifacts (e.g., enable the Android Analyzer module).
- If you encounter issues with encrypted partitions or locked data, note these in the report as limitations and suggest alternative approaches (e.g., requesting user credentials or using advanced tools like Cellebrite Premium).

Resources

- Autopsy Official Website: https://www.autopsy.com/
- Autopsy Documentation: http://sleuthkit.org/autopsy/docs/
- Sample Memory Images for Testing: http://dftt.sourceforge.net/
- Android Forensic Techniques: ResearchGate Article on Android Data Extraction

Good luck, and demonstrate your expertise as a Digital Forensic Analyst at Proforce Intelligence!