Android Forensics Project – Autopsy Analysis

==========

Objective:

To investigate a provided Android image for digital evidence including SMS, call logs, contacts, app usage, browser history, files, and deleted content.

Tools Used:

- Autopsy (Forensic Suite)

- Android forensic image (.tar.gz and data)

Methodology:

The investigation followed standard digital forensics procedures to ensure the integrity and admissibility of evidence:

1. Preservation

  - The original Android forensic image (`.tar.gz`) was preserved in its raw form.

  - Extraction was done without altering timestamps or metadata.

2. Examination

  - The image was ingested into Autopsy using appropriate ingest modules.

  - Targeted searches were conducted for SMS, call logs, contacts, app usage, browser history, and deleted data.

3. Analysis

  - SQLite databases (e.g., contacts2.db, mmssms.db) were parsed by Autopsy's Android Analyzer.

  - Image and document files were manually reviewed.

  - Deleted files were located using file carving and Autopsy recovery modules.

4. Documentation

- Screenshots were taken at each critical point to document findings.

- Notes were maintained regarding timestamps, user activity, and app behavior.

5. Reporting

- A structured report was compiled including tools, methodology, findings, and professional recommendations.

Steps Taken:

---

1. Extracted the forensic image:

- File provided: `android_data.tar.gz`

- Extracted using:

  tar -xvzf android_data.tar.gz

2. Opened Autopsy and created a new case:

- Case name: DSA CASE

- Examiner: Adenika Caleb Ayoola

- Case type: Local Disk Image

3. Ingested the extracted image:

- Pointed Autopsy to the `.image` or extracted folder

- Enabled ingest modules:

  - Keyword Search

  - Extract Files

  - Android Analyzer

  - Web History Analyzer

4. Evidence Extraction:

- SMS & Call Logs: Located using Android Analyzer module

- Contacts: Found in `contacts2.db`

- Browser History: Retrieved from Chrome and default browser SQLite DBs

- App Usage: Identified popular apps and recent activity

- Media Files: Images, videos, downloads were extracted

- Deleted Files: Recovered through Autopsy file recovery module

5. Screenshots Taken:

- Autopsy dashboard

- Extracted SMS, call logs, contacts

- File analysis panel (images, deleted files)

- Browser history view

6. Report Drafted:

- Findings summarized

- Screenshots include

Conclusion:

The Android image analysis successfully uncovered mock data from apps, system logs, and user behavior. The report provides insight into digital forensics methodology and tool usage.

Recommendations:

- Secure all forensic image files in read-only mode to prevent accidental modification.

- Use mobile-specific tools (e.g., Magnet AXIOM, Cellebrite) for deeper extraction of encrypted content and third-party apps.

- Maintain proper documentation and evidence handling to ensure legal admissibility.

Author:

Archie koffa

DSA Project