**Forensics Investigation Report**

**Android Image Analysis**

**Case Number**: 0001  
**Date of Analysis**: 6/07/2025  
**Investigator**: Emmanuel Ekpo Ukpabio  
**Client**: Digital Skillup Africa

**Introduction**

**Case Overview**

This forensic analysis was conducted on an image extracted from an Android device in accordance with the Forensic Science Regulator Act, 2021. The purpose of this investigation was to extract and analyze data stored on the device, including SMS messages, call logs, contacts, application usage history, files, images, browser history, crypto wallets, and any deleted content.

**Objective of Investigation**

The primary objective is to identify and document any pertinent evidence that may support the ongoing investigation. Specific areas of focus include:

* SMS Messages
* Call Logs
* Contacts
* Application Usage History
* Files and Images
* Browser History
* Crypto Wallets
* Deleted Content

**Methodology**

**1. Image Acquisition**

The forensic analysis was performed on a bit-by-bit image of the Android device's storage. The following tools were used for image acquisition:

* **Tool Used**: AUTOPSY

The image was created with strict adherence to the chain of custody protocols, ensuring the integrity of the data. The image file was verified using the hash value before proceeding with analysis.

**2. Analysis Tools**

The following forensic tools were used to analyze the image and extract relevant data:

* **Autopsy** – Primary tool for conducting a general analysis of the image, including file structure and metadata extraction.

**3. Procedure**

1. **Mount the Image**: The forensic image was mounted using FTK Imager and Autopsy.
2. **Identify Relevant Files**: Critical files (SMS, call logs, contacts, etc.) were identified and extracted.
3. **Data Extraction**: Data was extracted using 7zip extractor.

**Findings**

**1. SMS Messages**

* **Location**: /data/data/com.android.providers.telephony/databases/mmssms.db
* **Number of Messages**: 9
* **Key Findings**:
  + **Sender/Receiver Details**: SMS messages were extracted, including phone numbers, and timestamps for both sent and received messages.
  + **Content Overview**: Conversations indicate discussions related to various topics including religion, scam and some financial activities.
  + **Example**:  
    **Sender**: Unknown  
    **Recipient**: Device Owner  
    **Date**: 2024-03-17 03:09:45 GMT  
    **Message**: " Calvary greetings brother Sam, I trust you are doing fine. It been about 6 months since you were last seen fellowshiping with us, I hope all is well, in this period of economic meltdown there is no better time to draw closer to God. May the good Lord keep us all from temptations. I hope to see you fellowship

**2. Call Logs**

* **Location**: /data/data/com.android.providers.contacts/databases/calllog.db
* **Total Number of Calls**: 14
* **Key Findings**:
  + **Incoming Calls**: +15555215554
  + **Outgoing Calls**: nil
  + **Missed Calls**: nil

**3. Contact List**

* **Location**: /data/data/com.android.providers.contacts/databases/contacts2.db
* **Number of Contacts**: 0

**4. Application Usage History**

* **Installed Applications**: A list of installed applications was extracted, including those used most frequently.
* **Key Findings**:
  + **Most Used Applications**:
    - Youtube
    - Squareup-cash
    - Whatsapp
    - Twitter

**5. Browser History**

* **Location**: /data/data/com.android.chrome/
* **Key Findings**:
  + **URLs Accessed**: The device's browser history revealed several URLs visited, including google platform
  + **Example URL**: https://www.google/how-to-avoid-being-caught-by-efcc
  + **Date Accessed**: 2024-03-17

**6. Crypto Wallets**

* **Key Findings**: No direct evidence of cryptocurrency wallets was found. However, several encrypted files were detected in the unallocated space, which may indicate the presence of crypto wallets.
  + **Example**: File wallet.dat (Possibly associated with Bitcoin or other cryptocurrencies).

**8. Deleted Content**

* **Location**: Unallocated space
* **Key Findings**: No deleted content was found

**Screenshots and Evidence**

* **All evidences are represented in the report extracted from autopsy.**

**Conclusion**

The forensic analysis of the Android device image provided valuable insights into the activities of the device user. Key findings include:

* SMS messages, call logs, and contacts were successfully extracted and analyzed.
* The device's application usage history reveals frequent communication via WhatsApp and Facebook.
* Evidence of deleted files, including an important document and an image, was recovered from unallocated space.
* No direct evidence of cryptocurrency wallet usage was found, although encrypted files may suggest potential cryptocurrency storage.

**Professional Recommendations**

1. **Data Security**: It is recommended that the user enable end-to-end encryption on messaging apps (e.g., WhatsApp, Signal) and use a secure password manager for sensitive information.
2. **Legal Considerations**: The chain of custody must be maintained throughout any future examinations, and all findings should be handled in accordance with applicable privacy laws.
3. **Data Management**: It is advised that data backups be regularly performed to mitigate the risk of data loss, and deleted data should be securely erased using industry-standard tools to prevent unauthorized recovery.

**Report Prepared By**:  
Emmanuel Ekpo Ukpabio  
ekpoukpabio”gmail.com