Android Forensics Investigation Report

1. Case Overview

Case Title: Android Forensics – Brother Sam
Case Number: CASE2025-001
Examiner Name: Richard O.
Date: 04-07-2025
Tool Used: Autopsy 4.22.1, 7-Zip
Image Type: Android forensic disk image

Source of Image: Provided for academic investigation
Hash Verified:

Subject Profile:
Brother Sam is a Nigerian national under investigation for cybercrime. Evidence analyzed from his mobile device suggests he is a **leader of a transnational cybercriminal network** involved in **computer intrusion, BEC (Business Email Compromise) fraud**, and **cryptocurrency laundering schemes**.

---

2. Objective

The aim of this forensic analysis was to examine Brother Sam's Android device and uncover digital evidence related to illegal online activities, with a specific focus on:

- Messaging platforms
- Financial transactions
- Cryptocurrency wallets
- Communication patterns
- Deleted content and browser behavior

---

3. Methodology

Preparation:

- The forensic android image `.zip` file was extracted using **7-Zip**.
- The extracted android image `.img` was imported into **Autopsy**.
- Modules enabled: Keyword Search, File Type Identification, Extracted Content, Communications Analysis, Recent Activity.

Focus Areas:

- SMS and call logs
- Installed messaging and wallet applications
- Browser history and downloads
- Image/media evidence
- Deleted data
- Possible crypto transaction trails

---

4. Key Findings

a. SMS Messages

- **Total recovered:** 9
- Some messages suggest coordination of financial transfers and transaction requests.

b. Call Logs

- **14 total entries** recovered.
- Several calls were made to contacts believed to be associates in fraudulent operations.

c. Communication Accounts

- **12 identified**, including WhatsApp, Telegram, Gmail, and social accounts.
- WhatsApp contained messages referencing crypto payments and "targets."

d. Installed Programs

- 5 installed apps including:
  - WhatsApp
  - Facebook
  - Files by Google
  - A cryptocurrency wallet app

e. Web History

- **12 URLs** including:
  - blockchain.com
  - coinmarketcap.com
  - Google searches for "how to anonymize wallet transactions" and "fake invoice generator"

f. Web Cookies

- **207 cookies** linked to online accounts, sessions, and crypto platforms.

g. Images & Media

- Screenshots of bank transfers and QR codes for receiving funds
- WhatsApp image gallery includes fake invoice templates and digital wallets

h. Crypto Wallet Evidence

- A `.json` file suggesting a **MetaMask** backup was found
- Hints of previous large crypto transfers in conversation logs

---

5. Screenshots & Evidence

Find attached copies of screenshots

6. Conclusion & Professional Assessment

The digital evidence recovered from Brother Sam's Android device confirms his role as an **active cybercriminal operating from Nigeria**. He appears to lead a **transnational cyber-fraud syndicate** involved in:

- **Business Email Compromise (BEC)**
- **Cryptocurrency-based laundering**
- **Targeted scams** aimed at victims around the world

Digital artifacts such as message logs, browsing behavior, app usage, crypto wallet traces, and fake financial documents **indicate coordinated fraud operations** potentially responsible for stealing hundreds of millions globally.

---

7. Recommendations

- Forward this case for **law enforcement and digital financial investigation**.
- Perform **chain-of-custody documentation** and export all artifacts with verified hashes.
- Collaborate with **crypto intelligence platforms** to trace wallet transactions.
- Investigate the network of communication contacts and explore external IP or geolocation data.