Mobile Device Forensic Analysis Report

Date: 28/06/2025

Investigator: Agent Charles Mordi

Tools Used:

- Autopsy - File carving, timeline, deleted data recovery

2. Summary of Key Findings

[Mobile] Communication & Messaging

a. SMS/MMS

Data Source: mmssms.db

Total Messages Recovered: 346 (Inbox + Sent)

Example Message:

From: +2348012345678

Date: 2024-10-22 13:22

Body: "Meet me at the drop-off zone by 5."

Extended Analysis:

Some messages suggest fraudulent activity and crypto scams, mentioning fake investment websites, crypto wallets, and wallet addresses.

Example Extract (Redacted):

#	Phone Number	Date & Time (UTC)	Message Body (Excerpt)
4	08032111133	2024-10-22 18:19:10	"Hey, I've got a new scam idea..."
8	08032111133	2024-10-22 18:24:00	"Use the same Bitcoin wallet address as before..."
16	+971543777711	2024-10-22 20:03:19	"New wallet address for this operation..."

b. Call Logs

Data Source: calllog.db

Total Entries: 122

Incoming: 48, Outgoing: 53, Missed: 21

Example:

Number: +2348099998888

Date: 2024-11-03 09:45

Duration: 02:15 min

Type: Outgoing

c. Contacts

Data Source: contacts2.db

Total Contacts Recovered: 187

Included names, numbers, and emails

d. WhatsApp

Databases Extracted: msgstore.db, wa.db

Messages: 1,202 across 13 chats

Media: 145 images, 23 videos

Deleted messages partially recovered

Example:

Contact: "Boss Kelvin"

Date: 2025-01-05 08:55

Message: "The documents are ready. PDF sent."

[Web] Browsing & Search Activity

a. Chrome History

Source: Chrome app data folder

Total URLs Visited: 523

Notable domains: binance.com, coinmarketcap.com, nairaland.com

Example visit:

URL: https://www.binance.com/en/trade/BTC_USDT

Timestamp: 2025-02-13 18:11

b. Firefox History

Sessions and cookies recovered

Focus on crypto/wallet sites

c. Google Search Queries

Extracted from Google service logs

Searches include:

"how to reset trust wallet seed"

"metamask transaction stuck"

"how to recover deleted WhatsApp messages android"

d. YouTube Activity

Watched videos log recovered

Examples:

"How to send BNB from Trust Wallet"

"Forensics 101: How to trace crypto wallets"

[Media] Media & Storage

a. Photos & Videos

Total items recovered: 632

Folders: /DCIM/, /Pictures/, /WhatsApp/Media/

EXIF Data: 92 photos geotagged (Lagos, Abuja)

Timestamps aligned with messaging data

b. Downloads

Notable files: ID_scan_1.pdf, wallet_seed_note.txt (flagged sensitive)

c. Screenshots

Binance transaction history

Trust Wallet balances

QR codes for wallet recovery

[Crypto] Cryptocurrency & Financial Apps

a. MetaMask

Folder: /data/data/io.metamask/

Artifacts: Encrypted keystore files

Memory dump analysis revealed private key fragments

b. Trust Wallet

Folder: /data/data/com.wallet.crypto.trustapp/

Partial seed phrase recovered

Login traces from mobile and Wi-Fi

c. Coinbase

App data and account tokens found

Correlated with browsing and email logs

d. Binance

Frequent visits and app usage

Suspicious artifacts such as API keys and app modding indicators

3. Technical Analysis Notes

Timestamps converted from Unix epoch (milliseconds) to UTC.

Cross-referenced SQLite databases for contacts, SMS, call logs.

Thread IDs used to group messages by conversation.

EXIF metadata confirms GPS data and timestamps.

File carving with Autopsy and Bulk Extractor revealed deleted and hidden data.

4. Conclusion

The forensic analysis reveals deliberate use of the device for cryptocurrency-related activities, including potential scams. Attempts to hide or delete data were partially overcome by recovery techniques. Communications and media provide strong evidence of fraudulent schemes.

Recommendation: Forward findings to cybercrime and financial crime units for further blockchain transaction analysis and suspect profiling.

Report Compiled By:

Agent Charles Mordi

Digital Forensics Investigator

Date: 28/06/2025