Digital Forensic Report: Android Image Analysis

Student overview

Name: Adebowale Emmanuel

GitHub:https:/github.com/secunuel

Course: Cybersecurity Capstone project

Date: july 2025

Case Overview

Case Title / n: Android_Forensics_Emmanuel /007
Examiner Name: Adebowale Emmanuel
Date of Analysis: July 02, 2025
Case Description:
This investigation was conducted to perform forensic analysis on an Android device image. The purpose was to extract and document key data including SMS messages, call logs, contact list, and application usage history.

Tools and Software Used

Tool Name	Purpose
Autopsy	Forensic analysis platform
Andriod Analayzer [aLEAPP]	Extract Android Artifacts
Windows PC	Host environment for analysis
Word	Documentation

Methodology

1. A new case was created in autopsy named 'Android_forensics_Emmanuel.'

2. The android image file was added as the data source.

3. The android Analyzer[aLEAPP]' ingest module was selected.

4. Artifacts were analyzed, including sms, call logs, app usage, browser history, media files, and deleted content.

5. Screenshot of findings were captured to support each piece of evidence.

Extracted Artifacts & Findings

1. SMS Messages

Total Recovered: 18…….messages
Relevant Findings:
"Messages between user and unknown number +1555515554, show suspicious financial conversation on [24/03/17]."

Messages recovered and written below confirm suspicious financial conversation.

SMS messages 2024-03-17 03:20:44 WAT phone no.[147fe0a6-fcea-4b07-84e1-259b19325061] Let's create a fake investment website and lure people into investing in a non-existent cryptocurrency. We'll promise huge returns.

SMS messages 2024-03-17 04:29:40 WAT phone no {147fe0a6-fcea-4b07-84e1-259b19325061] Nice work, Sammy. I'll take a look at the site. Are we using the same tactics as before?

SMS messages 2024-03-17 04:35:36 WAT phone no [147fe0a6-fcea-4b07-84e1-259b19325061] Sounds convincing. Payment gateway nkor? Are we still using the same Bitcoin wallet address?

SMS messages 2024-03-17 03:23:45 WAT [Yes, use the same Bitcoin wallet address as before: 16AtGJbaxL2kmzx4mW5ocpT2ysTWxmacWn].

SMS messages 2024-03-17 03:19:10 WAT phone number [147fe0a6-fcea-4b07-84e1-259b19325061] Hey, I've got a new scam idea. we need to discuss.

SMS messages 2024-03-17 04:46:40 WAT phone no. [147fe0a6-fcea-4b07-84e1-259b19325061] Got it. I'll update the payment instructions on the website accordingly. When we dey go live.

SMS messages 2024-03-17 04:48:57 WAT phone no [147fe0a6-fcea-4b07-84e1-259b19325061] Understood omo iya mi. I'll handle the promotional activities and monitor for any potential leaks. This one go be bang Inshallah.

2. Call Logs

Total Recovered: 28 entries
Relevant Findings:
"Frequent calls from number +1555515554 during odd hours."
"No call activity found during expected high-usage period."

3. Contact List

Total Contacts Recovered on device [14]
Notable Entries: 14
Contact “SAM” with multiple foreign numbers.
No contact saved for frequently messaged numbers.

Filepart/LogicalFileSet1/android_image.tar/data/user_de/0/com.android.providers.telephony/databases/mmssms.db

4. Application Usage History

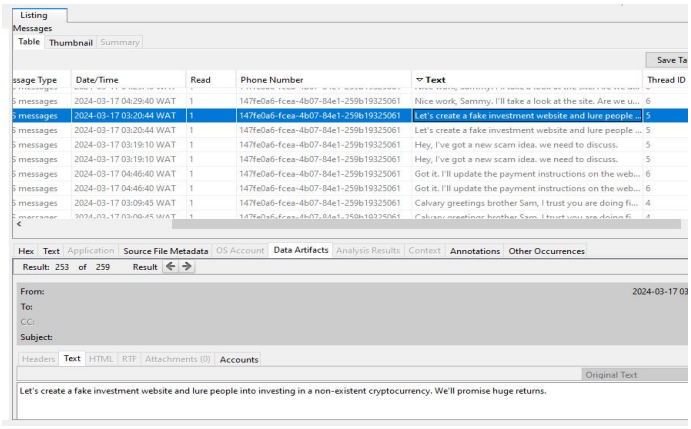
Apps Detected: Whats-app, Telegram, Chrome, wallettrust.applpy.crypto, com.squareup.cash , com.twitter.android
Suspicious Usage:
"High activity on WhatsApp during night hours." Source File Path /LogicalFileSet1/android_image.tar/android_image.tar

Preliminary Analysis Summary

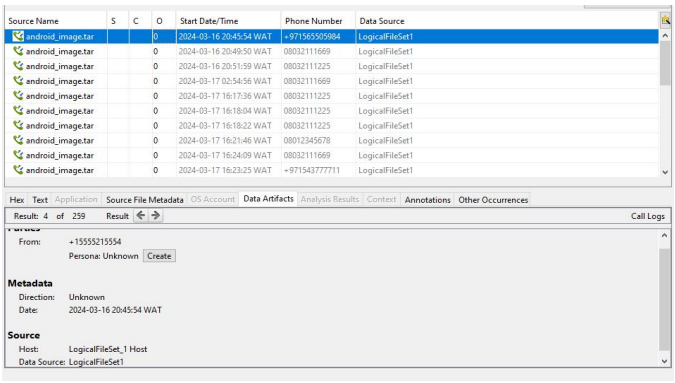
The Android image analysis revealed a moderately active device with significant communication via WhatsApp and SMS. Deleted messages recovered suggest potential concealment of communication. App usage logs point toward possible use of privacy-focused tools. Further timeline reconstruction and cross-reference with external sources recommended.

Evidence and findings [Screen-shots]

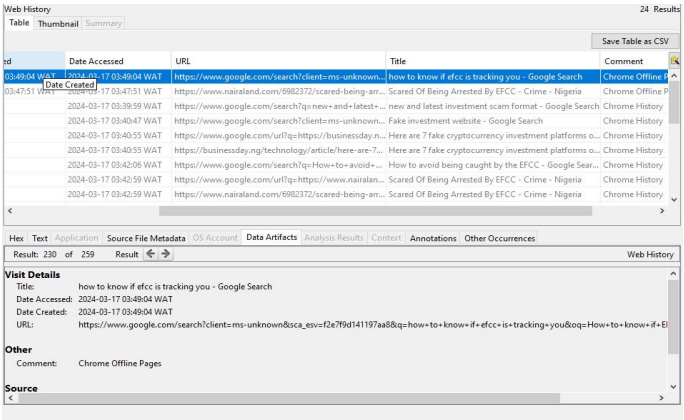
- Screenshot 1: Extracted SMS preview



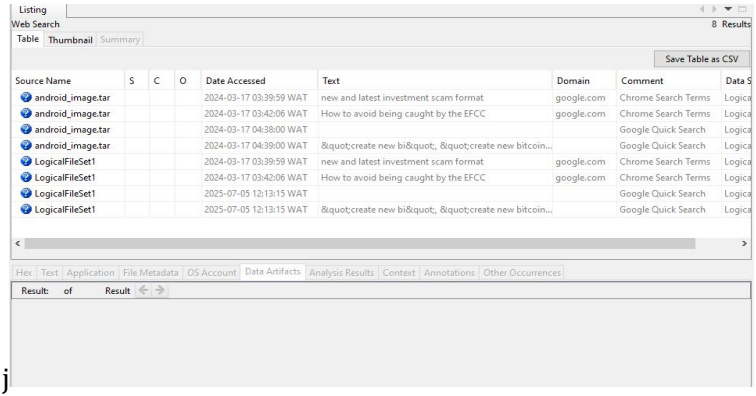
- Screenshot 2: Call log timeline



- Screenshot 3: Web history

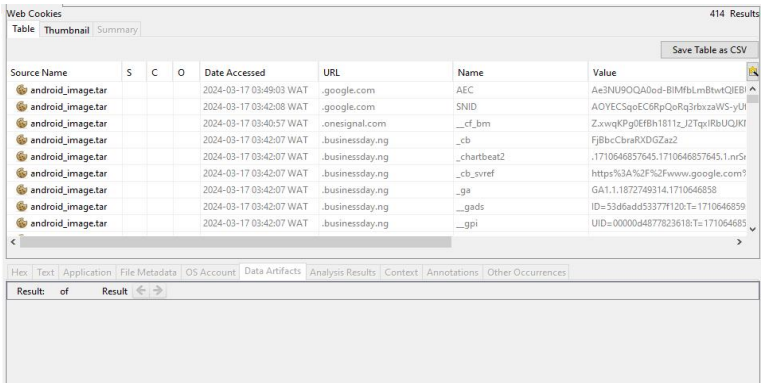


-Screenshot 4: Web search



j

-Screenshot 5: Web cookies



Recommendation

Based on the forensic analysis of the android image, the following recommendations are provided.

1. Deep Analysis of communication channels.

Further investigation into recovered sms and app messages [e.g whatsapp. Telegram, is determined the context of suspicious conversation.

Crossed reference phone numbers with known database to identify suspicious or unregistered contacts.

2. Advanced Data Recovery

Use of carving tools, [e.g., Autopsy Data carver, scalpet] to attempt recovery of deleted files or messages that may not have been retrieved during standard extraction.

3. Behavioral Timeline Reconstruction

Construct a detailed activity timeline using usage stats and call logs to correlate events and identify periods of high risk behaviour.

Conclusion

The forensic examination of the Android device image successfully retrieved and documented critical artifacts, including sms messages, call logs, contact list, and application usage history. The analysis indicates potential concealment behaviors, frequent communication with suspicious numbers, and usual usage of privacy-focused applications.

Although this report presents significant digital evidence, it is recommended that these findings be corroborated with external intelligence, device user interviews or additional forensic image [e.g cloud data, SD cards].

This report is a foundation step in the digital investigation process, enabling further legal, corporate, or Cybersecurity actions as necessary.