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 delected content.

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

Extracted Artifacts & Findings

1. SMS Messages

Total Recovered: 18…….messages
Relevant Findings:
- Example: "Messages between user and unknown number +234********* show suspicious financial conversation on [date]."
- Example: "Deleted messages recovered from mmssms.db via SQLite."

File Path: /data/data/com.android.providers.telephony/databases/mmssms.db

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

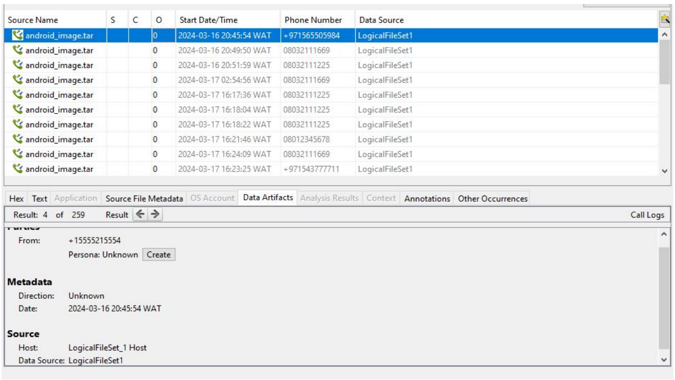
Apps Detected: Whats-app, Telegram, Chrome, wallettrust.applpy.crypto, com.squareup.cash , com.twitter.android
Suspicious Usage:
"High activity on WhatsApp during night hours." Source File Path /LogicalFileSet1/android_image.tar/android_image.tar

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



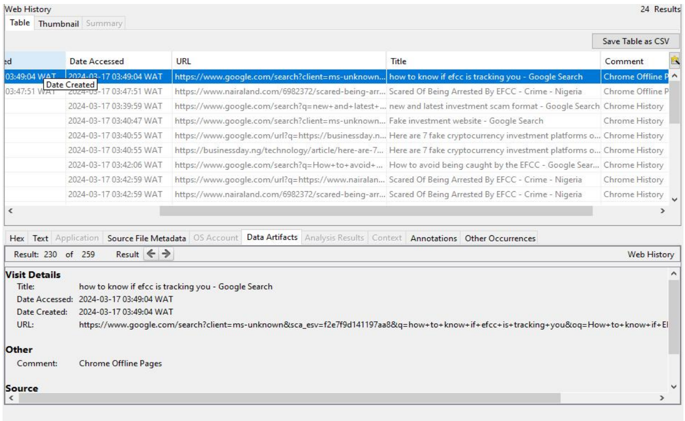
Source Name	S	C	O	Start Date/Time	Phone Number	Data Source
android_image.tar			0	2024-03-16 20:45:54 WAT	+971565505984	LogicalFileSet1
android_image.tar			0	2024-03-16 20:49:50 WAT	08032111669	LogicalFileSet1
android_image.tar			0	2024-03-16 20:51:59 WAT	08032111225	LogicalFileSet1
android_image.tar			0	2024-03-17 02:54:56 WAT	08032111669	LogicalFileSet1
android_image.tar			0	2024-03-17 16:17:36 WAT	08032111225	LogicalFileSet1
android_image.tar			0	2024-03-17 16:18:04 WAT	08032111225	LogicalFileSet1
android_image.tar			0	2024-03-17 16:18:22 WAT	08032111225	LogicalFileSet1
android_image.tar			0	2024-03-17 16:21:46 WAT	08012345678	LogicalFileSet1
android_image.tar			0	2024-03-17 16:24:09 WAT	08032111669	LogicalFileSet1
android_image.tar			0	2024-03-17 16:23:25 WAT	+971543777711	LogicalFileSet1

From: +15555215554
Persona: Unknown

Metadata
Direction: Unknown
Date: 2024-03-16 20:45:54 WAT

Source
Host: LogicalFileSet_1 Host
Data Source: LogicalFileSet1

- Screenshot 3: Web history



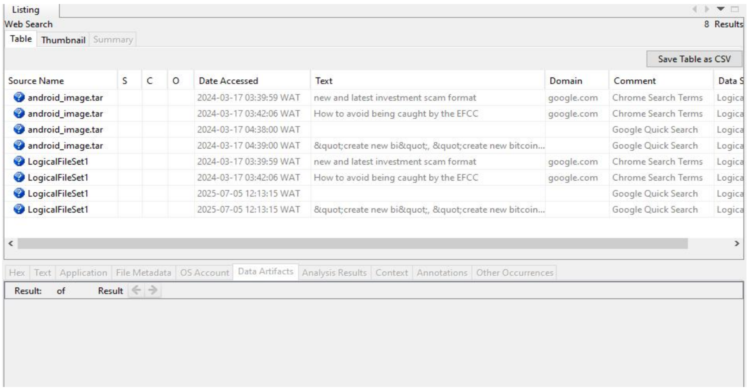
ed	Date Accessed	URL	Title	Comment
03:49:04 WAT	2024-03-17 03:49:04 WAT	https://www.google.com/search?client=ms-unknown...	how to know if efcc is tracking you - Google Search	Chrome Offline P
03:47:51 WAT	2024-03-17 03:47:51 WAT	https://www.nairaland.com/6982372/scared-being-arr...	Scared Of Being Arrested By EFCC - Crime - Nigeria	Chrome Offline P
	2024-03-17 03:39:59 WAT	https://www.google.com/search?q=new+and+latest+...	new and latest investment scam format - Google Search	Chrome History
	2024-03-17 03:40:47 WAT	https://www.google.com/search?client=ms-unknown...	Fake investment website - Google Search	Chrome History
	2024-03-17 03:40:55 WAT	https://www.google.com/url?q=https://businessday.n...	Here are 7 fake cryptocurrency investment platforms o...	Chrome History
	2024-03-17 03:40:55 WAT	https://businessday.ng/technology/article/here-are-7...	Here are 7 fake cryptocurrency investment platforms o...	Chrome History
	2024-03-17 03:42:06 WAT	https://www.google.com/search?q=How+to+avoid+...	How to avoid being caught by the EFCC - Google Sear...	Chrome History
	2024-03-17 03:42:59 WAT	https://www.google.com/url?q=https://www.nairalan...	Scared Of Being Arrested By EFCC - Crime - Nigeria	Chrome History
	2024-03-17 03:42:59 WAT	https://www.nairaland.com/6982372/scared-being-arr...	Scared Of Being Arrested By EFCC - Crime - Nigeria	Chrome History

Visit Details
Title: how to know if efcc is tracking you - Google Search
Date Accessed: 2024-03-17 03:49:04 WAT
Date Created: 2024-03-17 03:49:04 WAT
URL: https://www.google.com/search?client=ms-unknown&sca_esv=f2e7f9d141197aa8&q=how+to+know+if+efcc+is+tracking+you&oq=How+to+know+if+El

Other
Comment: Chrome Offline Pages

Source

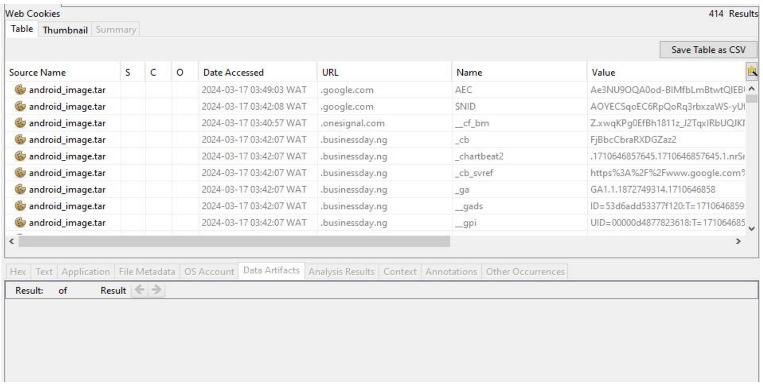
-Screenshot 4: Web search



Source Name	S	C	O	Date Accessed	Text	Domain	Comment	Data S
android_image.tar				2024-03-17 03:39:59 WAT	new and latest investment scam format	google.com	Chrome Search Terms	Logica
android_image.tar				2024-03-17 03:42:06 WAT	How to avoid being caught by the EFCC	google.com	Chrome Search Terms	Logica
android_image.tar				2024-03-17 04:38:00 WAT			Google Quick Search	Logica
android_image.tar				2024-03-17 04:39:00 WAT	&quot;create new bi&quot;, &quot;create new bitcoin...		Google Quick Search	Logica
LogicalFileSet1				2024-03-17 03:39:59 WAT	new and latest investment scam format	google.com	Chrome Search Terms	Logica
LogicalFileSet1				2024-03-17 03:42:06 WAT	How to avoid being caught by the EFCC	google.com	Chrome Search Terms	Logica
LogicalFileSet1				2025-07-05 12:13:15 WAT			Google Quick Search	Logica
LogicalFileSet1				2025-07-05 12:13:15 WAT	&quot;create new bi&quot;, &quot;create new bitcoin...		Google Quick Search	Logica

j

-Screenshot 5: Web cookies



Source Name	S	C	O	Date Accessed	URL	Name	Value
android_image.tar				2024-03-17 03:49:03 WAT	.google.com	AEC	Ae3NU9OQA0od-BIMfbLmBtwtQIEB
android_image.tar				2024-03-17 03:42:08 WAT	.google.com	SNID	AOYECSqoEC6RpQoRq3rbxzaWS-yU
android_image.tar				2024-03-17 03:40:57 WAT	.onesignal.com	__cf_bm	Z.xwqKPg0EfBh1811z_J2TqxIRbUQJKI
android_image.tar				2024-03-17 03:42:07 WAT	.businessday.ng	_cb	FjBbcCbraRXDGZaz2
android_image.tar				2024-03-17 03:42:07 WAT	.businessday.ng	_chartbeat2	.1710646857645.1710646857645.1.nrSı
android_image.tar				2024-03-17 03:42:07 WAT	.businessday.ng	_cb_svref	https%3A%2F%2Fwww.google.com%
android_image.tar				2024-03-17 03:42:07 WAT	.businessday.ng	_ga	GA1.1.1872749314.1710646858
android_image.tar				2024-03-17 03:42:07 WAT	.businessday.ng	__gads	ID=53d6add53377f120:T=1710646859
android_image.tar				2024-03-17 03:42:07 WAT	.businessday.ng	__gpi	UID=00000d4877823618:T=171064685

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 Andriod device image succefully 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.