

# 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\_Emanuel /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\_Emanuel.'
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

Listing

Messages

TableThumbnailSummary

Save To

Message Type	Date/Time	Read	Phone Number	Text	Thread ID
Message	2024-03-17 04:29:40 WAT	1	1479e0a6-fcea-4b07-84e1-259b19325061	Nice work, Sammy. I'll take a look at the site. Are we u...	6
Message	2024-03-17 03:20:44 WAT	1	1479e0a6-fcea-4b07-84e1-259b19325061	Let's create a fake investment website and lure people ...	5
Message	2024-03-17 03:20:44 WAT	1	1479e0a6-fcea-4b07-84e1-259b19325061	Let's create a fake investment website and lure people ...	5
Message	2024-03-17 03:19:10 WAT	1	1479e0a6-fcea-4b07-84e1-259b19325061	Hey, I've got a new scam idea. we need to discuss.	5
Message	2024-03-17 04:46:40 WAT	1	1479e0a6-fcea-4b07-84e1-259b19325061	Got it. I'll update the payment instructions on the web...	6
Message	2024-03-17 04:46:40 WAT	1	1479e0a6-fcea-4b07-84e1-259b19325061	Got it. I'll update the payment instructions on the web...	6
Message	2024-03-17 03:09:45 WAT	1	1479e0a6-fcea-4b07-84e1-259b19325061	Calvary greetings brother Sam, I trust you are doing fl...	4
Message	2024-03-17 03:09:45 WAT	1	1479e0a6-fcea-4b07-84e1-259b19325061	Calvary greetings brother Sam, I trust you are doing fl...	4

HexTextApplicationSource File MetadataOS AccountData ArtifactsAnalysis ResultsContextAnnotationsOther Occurrences

Result: 253 of 259Result

From:2024-03-17 03:09:45 WAT

To:

CC:

Subject:

HeadersTextHTMLRTFAttachments (0)Accounts

Original Text

Let's create a fake investment website and lure people into investing in a non-existent cryptocurrency. We'll promise huge returns.

- 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	+71855529904	LogicalFileSet1
android_image.tar			0	2024-03-16 20:46:50 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 16:28:23 WAT	+971543777711	LogicalFileSet1

Hex
Test
Application
Source File Metadata
OS Account
Data Artifacts
Analysis Results
Context
Annotations
Other Occurrences

Result: 4 of 259
Result

From: +15555215554
Person: Unknown
Create

### Metadata

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

### Source

Host: LogicalFileSet1 Host  
Data Source: LogicalFileSet1

Call Log

- Screenshot 3: Web history

Web History

Table Thumbnail Summary

24 Results

Save Table as CSV

id	Date Accessed	URL	Title	Comment
03-49-04 WAT	Created: 2024-03-17 03:49:04 WAT	https://www.google.com/search/client=ms-unknown	how to know if efc is tracking you - Google Search	Chrome Offline
03-47-31 WAT	Date Created: 17-03-25:51 WAT	https://www.nairaland.com/6982372/scared-being-arti	Scared Of Being Arrested By EFCC - Crime - Nigeria	Chrome History
	2024-03-17 03:39:59 WAT	https://www.google.com/search?q=nev-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-arti	Scared Of Being Arrested By EFCC - Crime - Nigeria	Chrome History

Hex Text Application Source File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Result: 230 of 259 Results

Web History

Visit Details

Title	how to know if efc 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&sa_svs=79d41917aa8&q=how-to+know-if+efcc-is-tracking-you&oeqHow-to+know-if+Ef

Other

Comment: Chrome Offline Pages

Source

-Screenshot 4: Web search

Listing

Web Search

8 Results

TableThumbnailSummary

Save Table as CSV

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

HexTextApplicationFile MetadataOS AccountData ArtifactsAnalysis ResultsContextAnnotationsOther Occurrences

Result of Result

-Screenshot 5: Web cookies

Web Cookies

414 Results

TableThumbnailSummary

Save Table as CSV

Source Name	S	C	O	Date Accessed	URL	Name	Value
android_image.tar				2024-03-17 03:49:03 WAT	.google.com	AEC	Ae3NU90QA0od-BIMfBlmBtwitQIEB
android_image.tar				2024-03-17 03:42:08 WAT	.google.com	SNID	AOYECsqoEC6RpQoRiq3rbizaWS-yUl
android_image.tar				2024-03-17 03:40:57 WAT	.onesignal.com	__cf_bm	Z.xwqKPgEFBh1811z_J2TqrIRbUQJKI
android_image.tar				2024-03-17 03:42:07 WAT	.businessday.ng	__cb	FJBbcCbraRXDGZax2
android_image.tar				2024-03-17 03:42:07 WAT	.businessday.ng	__chartbeat2	.1710646857645.1710646857645.1.nvS
android_image.tar				2024-03-17 03:42:07 WAT	.businessday.ng	__cb_vref	https%3A%2F%2Fwww.google.com%3F
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=53d6add533779120T=1710646859
android_image.tar				2024-03-17 03:42:07 WAT	.businessday.ng	__gpi	UID=000004877823618T=171064685

HexTextApplicationFile MetadataOS AccountData ArtifactsAnalysis ResultsContextAnnotationsOther Occurrences

Result of Result

## **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.