ANDROID FORENSICS INVESTIGATION REPORT

Title: Digital Forensics Analysis of an Android Device Image

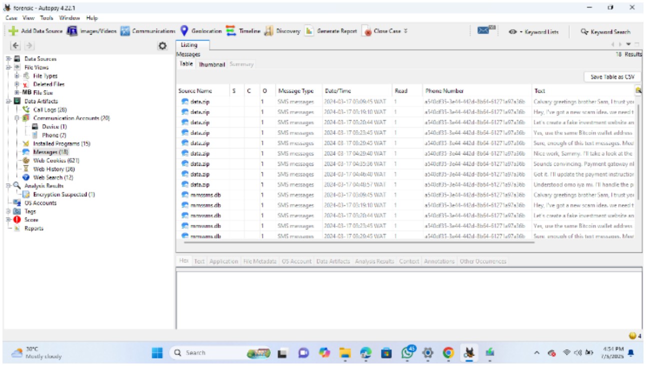
Investigator: Adewale-Abiola Vivian

1. Introduction
   This report presents the outcome of a digital forensic investigation performed on a provided Android image file. The analysis was conducted using forensic tools to extract and examine digital artifacts such as SMS messages, call logs, contact lists, browser history, application data, and deleted files. The objective of the investigation was to simulate a real-world mobile forensic examination and document findings in a professional and structured manner.

2. Tools and Methodology
   Tool Used:
   - Autopsy

   Methodology:
   - Loading the Android Image: The Android image file was loaded into the forensic tool.
   - Artifact Extraction: Categories of interest were examined, including
     - ➢ Communications (SMS, Call logs)
     - ➢ Internet Activity (Browser history)
     - ➢ Application Usage (App logs, cache)
     - ➢ Media (Photos, Deleted files)
     - ➢ Financial/Privacy-sensitive data (crypto wallets)
   - Documentation: Screenshots were captured and findings were documented

3. Findings
   3.1 SMS Messages
   Extracted a total of 18 SMS Messages



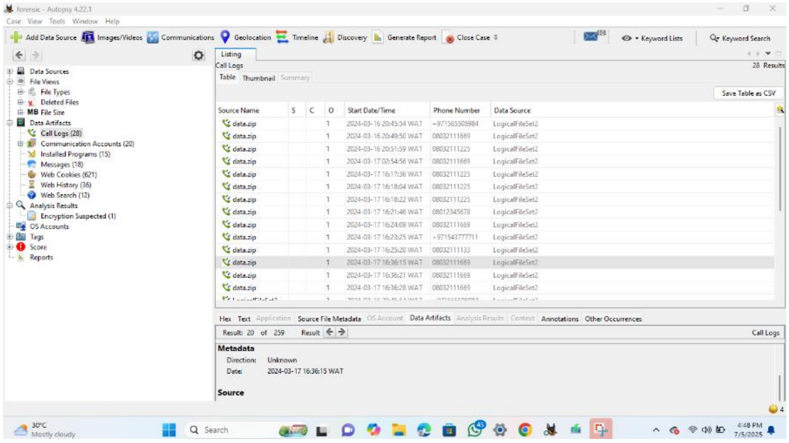
Messages

18 Results

Source Name	S	C	O	Message Type	Date/Time	Read	Phone Number	Text
data.zip			1	SMS messages	2024-03-17 03:09:45 WAT	1	a540df35-3e44-442d-8b64-61271a97a36b	Calvary greetings brother Sam, I trust yo
data.zip			1	SMS messages	2024-03-17 03:19:10 WAT	1	a540df35-3e44-442d-8b64-61271a97a36b	Hey, I've got a new scam idea, we need t
data.zip			1	SMS messages	2024-03-17 03:20:44 WAT	1	a540df35-3e44-442d-8b64-61271a97a36b	Let's create a fake investment website an
data.zip			1	SMS messages	2024-03-17 03:23:45 WAT	1	a540df35-3e44-442d-8b64-61271a97a36b	Yes, use the same Bitcoin wallet address
data.zip			1	SMS messages	2024-03-17 03:29:45 WAT	1	a540df35-3e44-442d-8b64-61271a97a36b	Sure, enough of this text messages. Mee
data.zip			1	SMS messages	2024-03-17 04:29:40 WAT	1	a540df35-3e44-442d-8b64-61271a97a36b	Nice work, Sammy. I'll take a look at the
data.zip			1	SMS messages	2024-03-17 04:35:36 WAT	1	a540df35-3e44-442d-8b64-61271a97a36b	Sounds convincing. Payment gateway nl
data.zip			1	SMS messages	2024-03-17 04:46:40 WAT	1	a540df35-3e44-442d-8b64-61271a97a36b	Got it. I'll update the payment instructio
data.zip			1	SMS messages	2024-03-17 04:48:57 WAT	1	a540df35-3e44-442d-8b64-61271a97a36b	Understood omo iya mi. I'll handle the p
mmssms.db			1	SMS messages	2024-03-17 03:09:45 WAT	1	a540df35-3e44-442d-8b64-61271a97a36b	Calvary greetings brother Sam, I trust yo
mmssms.db			1	SMS messages	2024-03-17 03:19:10 WAT	1	a540df35-3e44-442d-8b64-61271a97a36b	Hey, I've got a new scam idea, we need t
mmssms.db			1	SMS messages	2024-03-17 03:20:44 WAT	1	a540df35-3e44-442d-8b64-61271a97a36b	Let's create a fake investment website an
mmssms.db			1	SMS messages	2024-03-17 03:23:45 WAT	1	a540df35-3e44-442d-8b64-61271a97a36b	Yes, use the same Bitcoin wallet address
mmssms.db			1	SMS messages	2024-03-17 03:29:45 WAT	1	a540df35-3e44-442d-8b64-61271a97a36b	Sure, enough of this text messages. Mee

Last Message Sent: 2024-03-17 “Understood omo iya mi. I'll handle the promotional activities and monitor for any potential leaks. This one go be bang Inshallah”
Frequent Contacts: 08032111133 and +971543777711
Suspicious Content: Some messages contained phrase like “Crypto Wallet, Scam, Fake Investment” which is saying a fake investment plan be created to scam low value people.

3.2 Call Logs
Total Call Entries: 28
Top Contacted Number: 08032111669
Last Call Made: 2024-03-17 16:36:28 WAT



Call Logs
28 Results

Source Name	S	C	O	Start Date/Time	Phone Number	Data Source
data.zip			1	2024-03-16 20:45:54 WAT	+971565505984	LogicalFileSet2
data.zip			1	2024-03-16 20:49:50 WAT	08032111669	LogicalFileSet2
data.zip			1	2024-03-16 20:51:59 WAT	08032111225	LogicalFileSet2
data.zip			1	2024-03-17 02:54:56 WAT	08032111669	LogicalFileSet2
data.zip			1	2024-03-17 16:17:36 WAT	08032111225	LogicalFileSet2
data.zip			1	2024-03-17 16:18:04 WAT	08032111225	LogicalFileSet2
data.zip			1	2024-03-17 16:18:22 WAT	08032111225	LogicalFileSet2
data.zip			1	2024-03-17 16:21:46 WAT	08012345678	LogicalFileSet2
data.zip			1	2024-03-17 16:24:09 WAT	08032111669	LogicalFileSet2
data.zip			1	2024-03-17 16:23:25 WAT	+971543777711	LogicalFileSet2
data.zip			1	2024-03-17 16:25:20 WAT	08032111133	LogicalFileSet2
data.zip			1	2024-03-17 16:36:15 WAT	08032111669	LogicalFileSet2
data.zip			1	2024-03-17 16:36:21 WAT	08032111669	LogicalFileSet2
data.zip			1	2024-03-17 16:36:28 WAT	08032111669	LogicalFileSet2

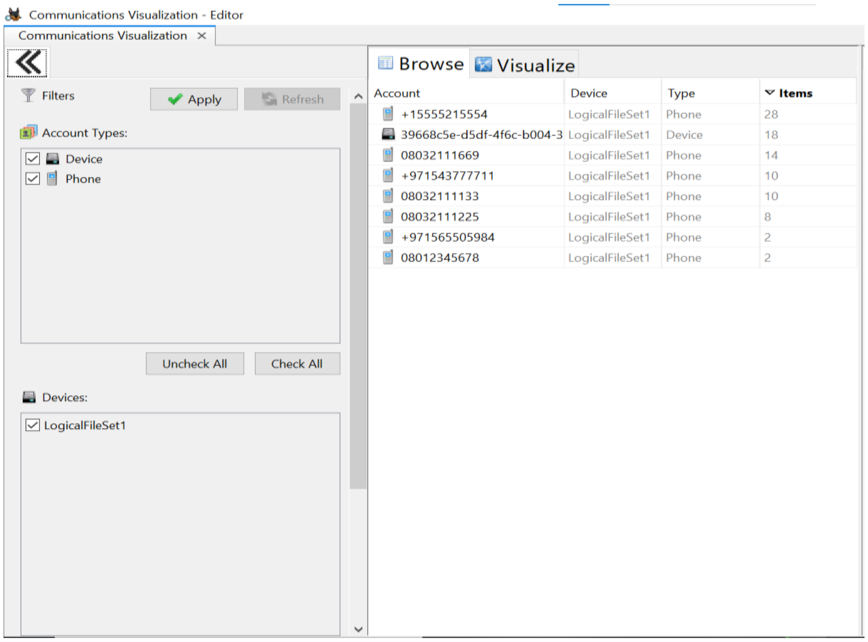
Result: 20 of 259 Result

Call Logs

Metadata
Direction: Unknown
Date: 2024-03-17 16:36:15 WAT

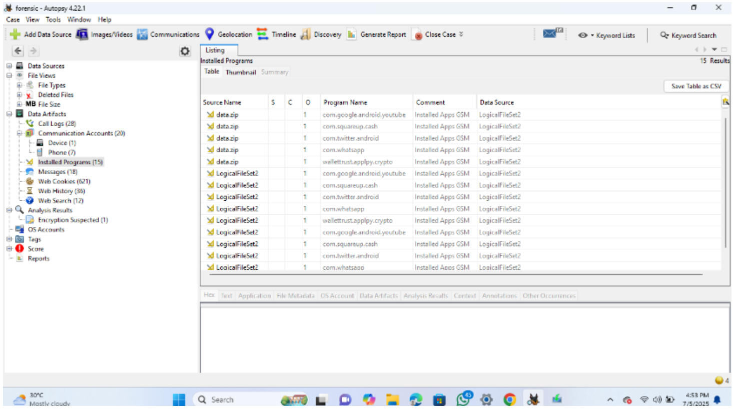
Source

3.3 Contacts: There are seven (7) contacts with no visible names.



Account	Device	Type	Items
+15555215554	LogicalFileSet1	Phone	28
39668c5e-d5df-4f6c-b004-3	LogicalFileSet1	Device	18
08032111669	LogicalFileSet1	Phone	14
+971543777711	LogicalFileSet1	Phone	10
08032111133	LogicalFileSet1	Phone	10
08032111225	LogicalFileSet1	Phone	8
+971565505984	LogicalFileSet1	Phone	2
08012345678	LogicalFileSet1	Phone	2

3.4 Application Usage History: The following apps were accessed - YouTube, WhatsApp, Wallet Trust – For Crypto, Square up Cash and Twitter



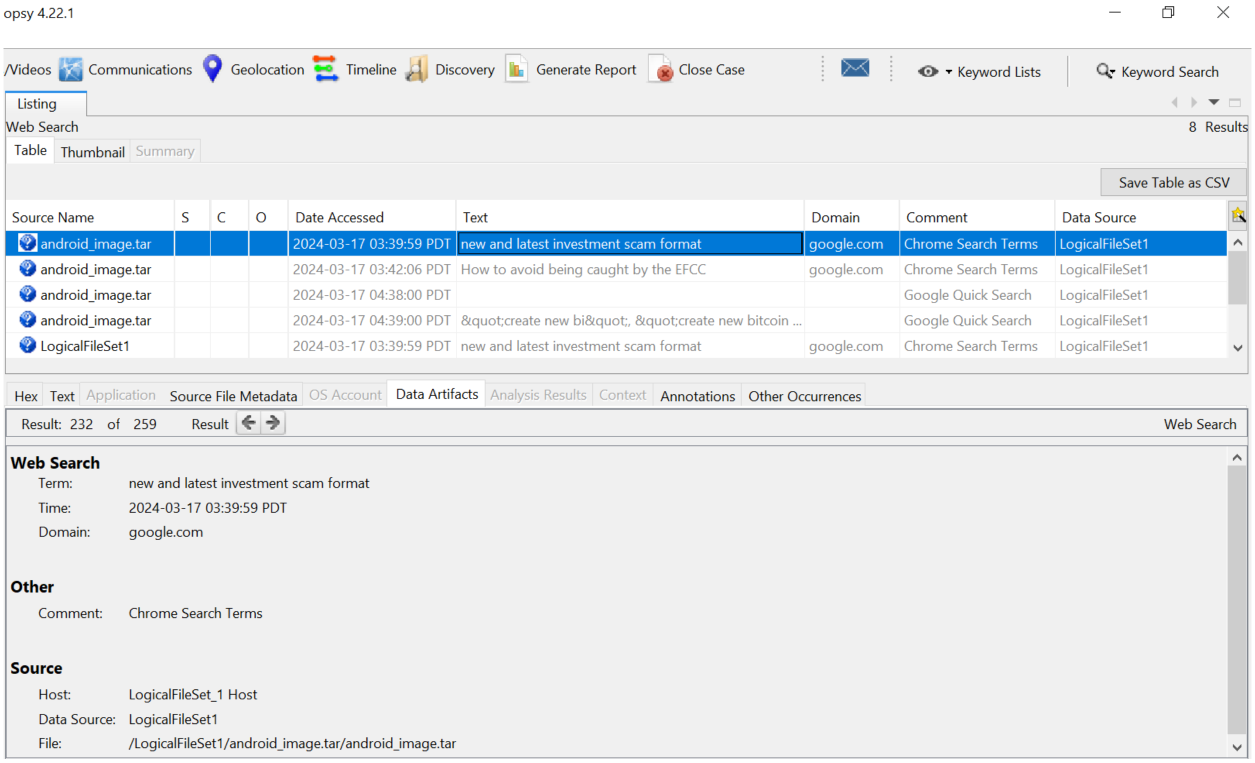
Installed Programs 15 Results

Source Name	S	C	O	Program Name	Comment	Data Source
data.zip			1	com.google.android.youtube	Installed Apps GSM	LogicalFileSet2
data.zip			1	com.squareup.cash	Installed Apps GSM	LogicalFileSet2
data.zip			1	com.twitter.android	Installed Apps GSM	LogicalFileSet2
data.zip			1	com.whatsapp	Installed Apps GSM	LogicalFileSet2
data.zip			1	wallettrust.applpy.crypto	Installed Apps GSM	LogicalFileSet2
LogicalFileSet2			1	com.google.android.youtube	Installed Apps GSM	LogicalFileSet2
LogicalFileSet2			1	com.squareup.cash	Installed Apps GSM	LogicalFileSet2
LogicalFileSet2			1	com.twitter.android	Installed Apps GSM	LogicalFileSet2
LogicalFileSet2			1	com.whatsapp	Installed Apps GSM	LogicalFileSet2
LogicalFileSet2			1	wallettrust.applpy.crypto	Installed Apps GSM	LogicalFileSet2
LogicalFileSet2			1	com.google.android.youtube	Installed Apps GSM	LogicalFileSet2
LogicalFileSet2			1	com.squareup.cash	Installed Apps GSM	LogicalFileSet2
LogicalFileSet2			1	com.twitter.android	Installed Apps GSM	LogicalFileSet2
LogicalFileSet2			1	com.whatsapp	Installed Apps GSM	LogicalFileSet2

3.5 Browser History: Search terms and visited URLs were recovered and below are the visited domains. Browsers Detected: Chrome, Nairaland, Businessday

Top Sites Visited: https://google.com, https://nairaland.com, https://businessday.ng

Search Queries: “How to know if EFCC is tracking you”, “New and latest investment scam format,” “Scared of being arrested by EFCC”



Web Search 8 Results

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

Result: 232 of 259 Result Web Search

Web Search

Term: new and latest investment scam format
Time: 2024-03-17 03:39:59 PDT
Domain: google.com

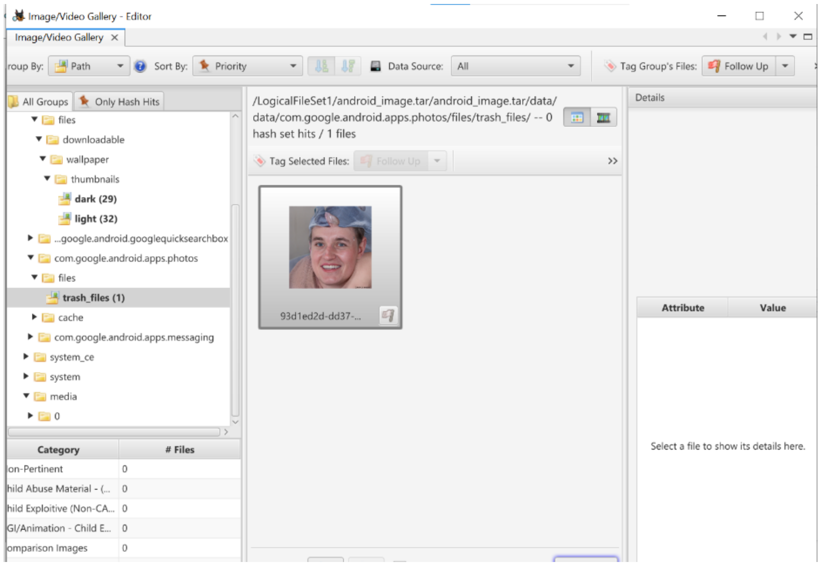
Other

Comment: Chrome Search Terms

Source

Host: LogicalFileSet_1 Host
Data Source: LogicalFileSet1
File: /LogicalFileSet1/android_image.tar/android_image.tar

3.5 Deleted Content: 1 image was recovered from thrash



roup By: Path · Sort By: Priority · Data Source: All · Tag Group's Files: Follow Up

/LogicalFileSet1/android_image.tar/android_image.tar/data/data/com.google.android.apps.photos/files/trash_files/ -- 0 hash set hits / 1 files

Category	# Files
on-Pertinent	0
hild Abuse Material - (...	0
hild Exploitive (Non-CA...	0
GI/Animation - Child E...	0
omparison Images	0

3.6 Crypto Wallets/Financial Data: There are no wallet recovery phrases or credential discovered

4. Conclusion & Recommendations

The forensic analysis of the Android device image successfully retrieved valuable digital evidence, including communication records, application activity, browsing behavior. These findings demonstrated the effectiveness of forensic tools in extracting sensitive and actionable data from mobile devices.

Recommendations:

- Device encryption and application-level security should be enabled to protect user data
- Users should clear cache, browsing data and use privacy-focused apps where necessary
- Investigators should maintain chain-of-custody protocols and use write-blocking techniques in real investigations.