DSA CYBER SECURITY SQUAD 1 BUREAU OF INVESTIGATION

For Education Purposes Only Cyber Crime Investigation Dept.

Project by

Onatoye Olanrewaju

To create a professional investigation report for your DSA cybersecurity project

2025

Investigation Report: Android Forensic Image Analysis

Case Overview

Case Number: Dsa 2025 case 1

Investigator: Onatoye Olanrewaju

Date: July 3, 2025

Device Details: Android device specifics (model, OS version, etc.)

Image Details: URL of the Android forensic image analyzed (https;//github.com/akobe ajibolu/android image.git)

Executive Summary

Provide a brief overview of the investigation, including the purpose, scope, and key findings.

Methodology

Autopsy is an effective digital forensics tool designed to quickly and accurately analyze and examine digital data. Autopsy provides a user-friendly interface and a full set of tools to extract, display, and analyze data from diverse sources, whether for a cybercrime investigation, incident response, or a routine review of digital devices. Digital forensic experts worldwide rely on this open-source program to provide important insights that aid in resolving challenging cases and the discovery of covert digital traces.

The model of tools Used: **Autopsy 4.22.1**

Analysis Techniques: I extracted the android image using autopsy to reveal the data and information for investigation purpose

Findings

I hereby Present the results of the autopsy analysis, including relevant data extracted, such as:

```
*.gz filter=lfs diff=lfs merge=lfs -text
```

```
------------------------------METADATA------------------------------
```

Metadata

Name:	/img_Android_Image-main (1).zip
Type:	Raw Single
Size:	1719
MD5:	b1b4d8be398bfe531dbc0b40110457dc
SHA1:	9f2a4d33956bdc11a77c9c0265289e7cfe7aee51
SHA-256:	ac4c0bfb3b4639954211097e0660ef9473acaa6d7fc0fcca4e3ee2530e71514e
Sector Size:	512
Time Zone:	Africa/Lagos
Acquisition Details:	Unknown
Device ID:	b36d5e72-e87f-4adf-b301-054434ac4391
Internal ID:	1
Local Path:	C:\Users\Dell\Desktop\Android_Image-main (1).zip

File System Analysis: recovered files, folder structures, and file attributes

```
version https://git-lfs.github.com/spec/v1
oid sha256:4e17d75a0b9f39c0e0eb5aa32c227234dec75665d0da851b5aae452664a998e3
size 395835699
```

------------------------------METADATA------------------------------

Timeline Analysis: chronological sequence of events

~~~~
# Android Forensics Learning Image
This repository contains an **Android Forensics Image** designed for
educational purposes. The image simulates a realistic scenario where digital
evidence can be analyzed to uncover incriminating activities. It is ideal for
students, educators, and professionals in the fields of digital forensics and
cybersecurity to practice investigative techniques.
## Features
The forensics image includes the following types of simulated evidence:
- **Phone Numbers**: Contacts linked to suspicious activities.
- **Text Messages**: Conversations containing fraudulent discussions.
- **Cryptocurrency Wallet Address**: Evidence of transactions potentially
tied to internet fraud.
- **Other Artifacts**: Additional incriminating data to support investigative
workflows.
## Use Cases
This image is specifically crafted for:
1. **Digital Forensics Training**: Hands-on practice in identifying and
analyzing digital evidence.
2. **Cybersecurity Awareness**: Understanding the implications of poor
digital hygiene.
3. **Mock Investigations**: Simulating real-world scenarios for learning
purposes.
## Disclaimer
This image is **strictly for educational purposes** and must not be used for
unethical or illegal activities. All data is fictional and created to provide
a realistic learning experience.
## Getting Started
1. Clone this repository:
   ```bash
   git clone https://github.com/Akobe-Ajibolu/Android_Image.git
   ```
2. Extract the Android image:
  - Use a suitable extraction tool such as `tar` or `7z`.
  - Extract the image into a folder for easy access.
3. Analyze the image using Autopsy:
  - Open Autopsy and create a new case.
  - Add the extracted image as a data source.
  - Begin investigating the evidence using Autopsy's analysis tools.
~~~~

Conclusion

Metadata

Name:	/img_Android_Image-main (1).zip/$CarvedFiles/1/f0000000_Android_Image_main.zip/Android_Image-main/README.md
Type:	Derived
MIME Type:	text/x-web-markdown
Size:	1820
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2024-11-15 11:14:50 WAT
Accessed:	0000-00-00 00:00:00
Created:	0000-00-00 00:00:00
Changed:	0000-00-00 00:00:00
MD5:	485d0fc3e7519d7d50ce4dfaa2c037b4
SHA-256:	e2c8baab1cedd863fba6f8554c0119fccc05ba96f5d782c4ad4486fb0a365bcc
Hash Lookup Results:	UNKNOWN
Internal ID:	8

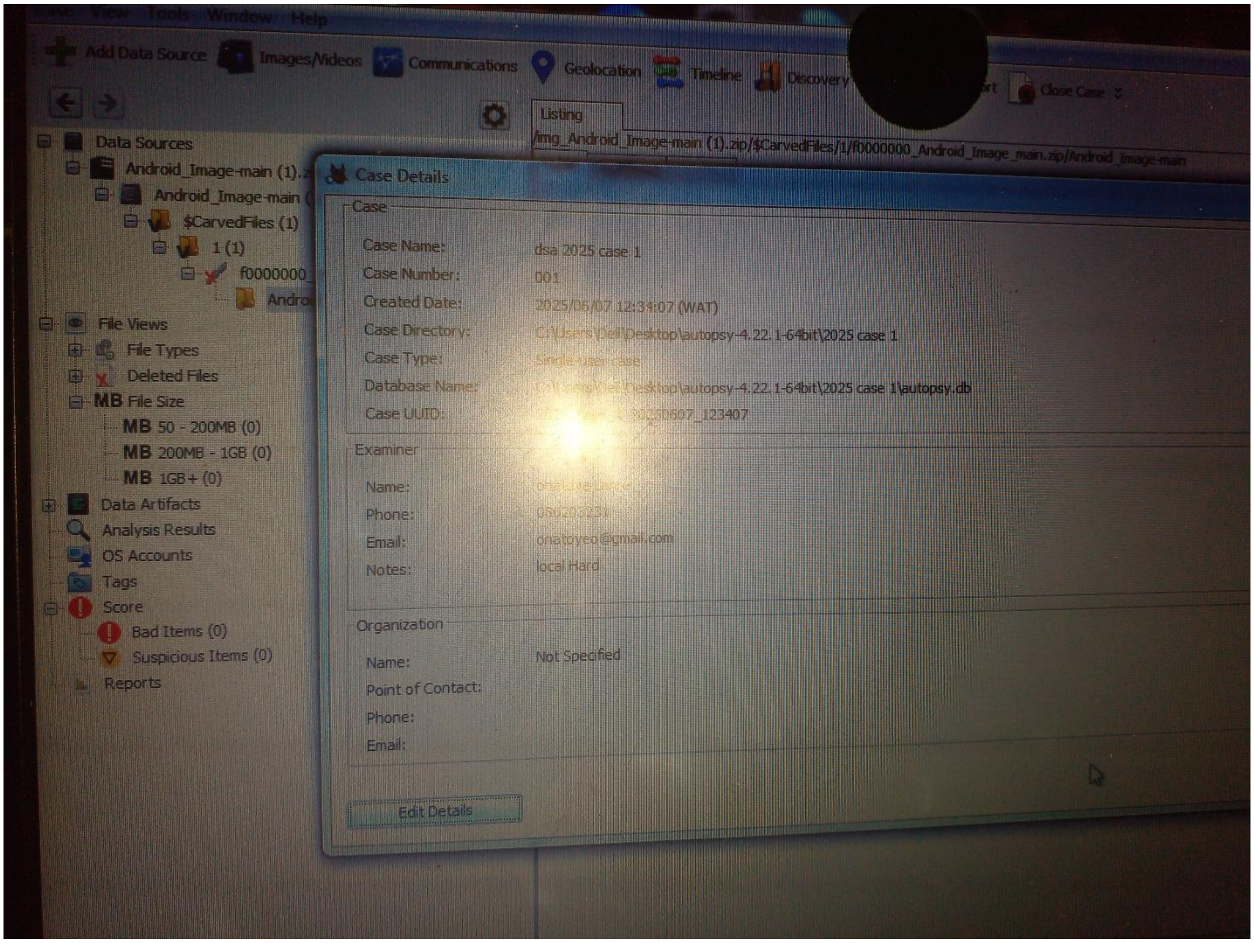
Recommendations

There is need for further collaboration with SOC and telecommunication network to track the time and extract soft copy of communication channel.

Appendices

Raw Data: extracted data in its original form

Screenshots: images of relevant data or analysis results



/img_Android_Image-main (1).zip/$CarvedFiles/1/f0000000_Android_Image_main.zip/Android_Image-main

Case Details

Case

Case Name: dsa 2025 case 1

Case Number: 001

Created Date: 2025/06/07 12:34:07 (WAT)

Case Directory: C:\Users\Dell\Desktop\autopsy-4.22.1-64bit\2025 case 1

Case Type: Single-user case

Database Name: C:\Users\Dell\Desktop\autopsy-4.22.1-64bit\2025 case 1\autopsy.db

Case UUID: [illegible] 20250607_123407

Examiner

Name: [illegible]

Phone: [illegible]

Email: onatoyeo@gmail.com

Notes: local Hard

Organization

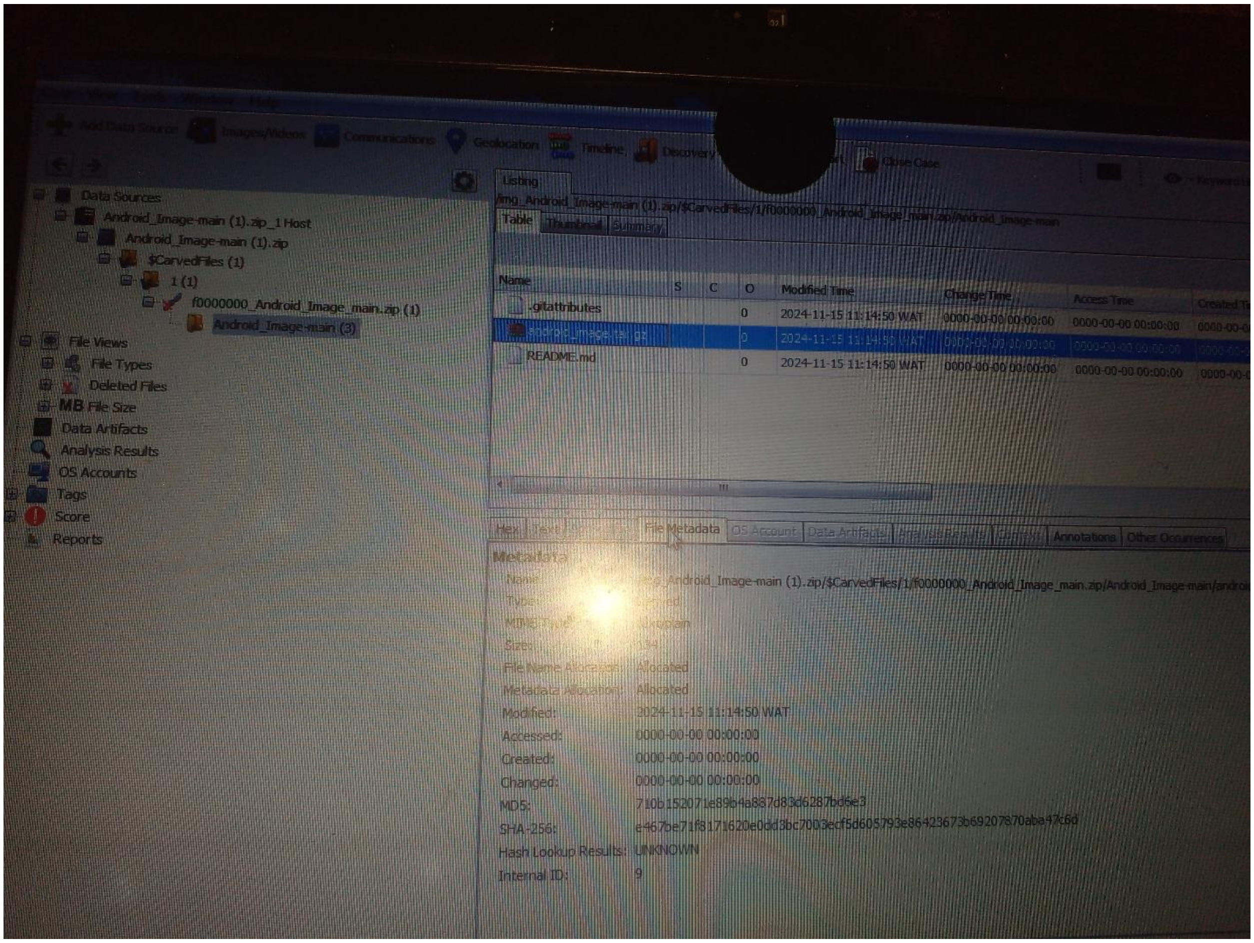
Name: Not Specified

Point of Contact:

Phone:

Email:

Autopsy Case file details

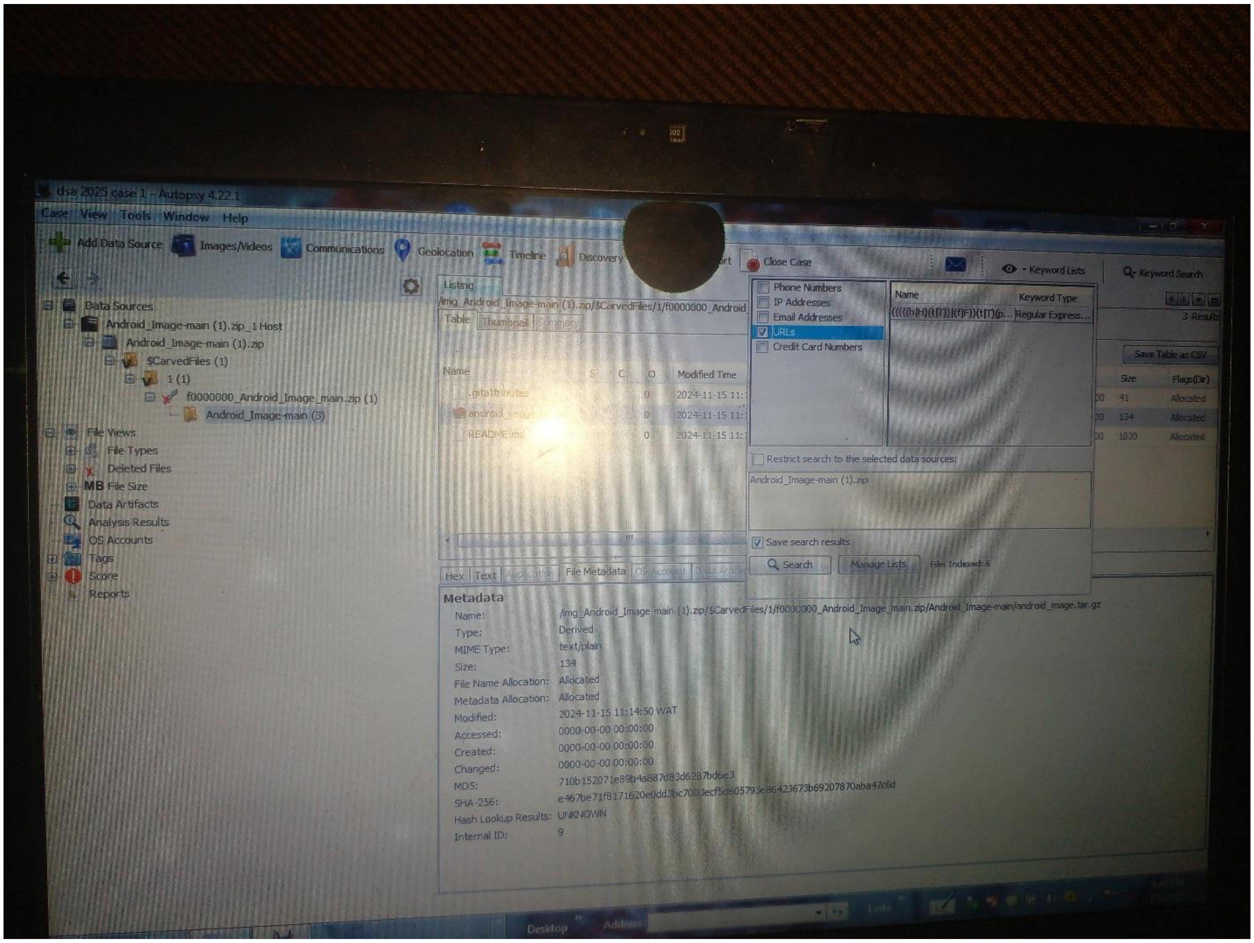


/img_Android_Image-main (1).zip/$CarvedFiles/1/f0000000_Android_Image_main.zip/Android_Image-main

Name	S	C	O	Modified Time	Change Time	Access Time	Created Ti
.gitattributes			0	2024-11-15 11:14:50 WAT	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-0
android_image.tar.gz			0	2024-11-15 11:14:50 WAT	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-0
README.md			0	2024-11-15 11:14:50 WAT	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-0

Metadata

Name:	/img_Android_Image-main (1).zip/$CarvedFiles/1/f0000000_Android_Image_main.zip/Android_Image-main/androi
Type:	Derived
MIME Type:	text/plain
Size:	134
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2024-11-15 11:14:50 WAT
Accessed:	0000-00-00 00:00:00
Created:	0000-00-00 00:00:00
Changed:	0000-00-00 00:00:00
MD5:	710b152071e89b4a887d83d6287bd6e3
SHA-256:	e467be71f8171620e0dd3bc7003ecf5d605793e86423673b69207870aba47c6d
Hash Lookup Results:	UNKNOWN
Internal ID:	9



/img_Android_Image-main (1).zip/$CarvedFiles/1/f0000000_Android

Name	S	C	O	Modified Time	Size	Flags(Dir)
.gitattributes			0	2024-11-15 11:1	41	Allocated
android_image.tar.gz			0	2024-11-15 11:1	134	Allocated
README.md			0	2024-11-15 11:1	1820	Allocated

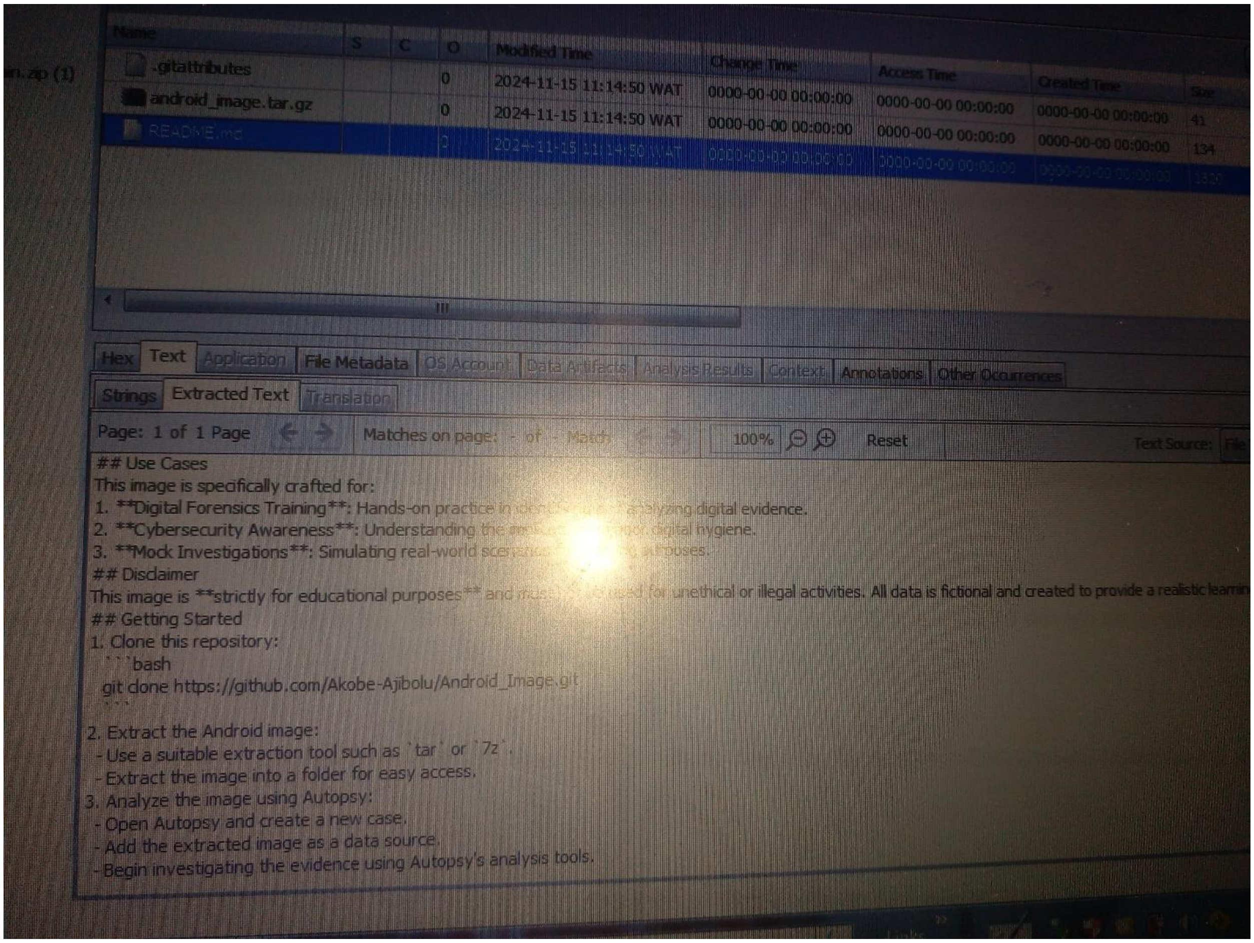
Name	Keyword Type
((((h|H)(t|T))|(f|F))(t|T)(p...	Regular Express...

Android_Image-main (1).zip

Metadata

Name: /img_Android_Image-main (1).zip/$CarvedFiles/1/f0000000_Android_Image_main.zip/Android_Image-main/android_image.tar.gz
Type: Derived
MIME Type: text/plain
Size: 134
File Name Allocation: Allocated
Metadata Allocation: Allocated
Modified: 2024-11-15 11:14:50 WAT
Accessed: 0000-00-00 00:00:00
Created: 0000-00-00 00:00:00
Changed: 0000-00-00 00:00:00
MD5: 710b152071e89b4a887d83d6287bd6e3
SHA-256: e467be71f8171620e0dd3bc7003ecf5d605793e86423673b69207870aba47c6d
Hash Lookup Results: UNKNOWN
Internal ID: 9

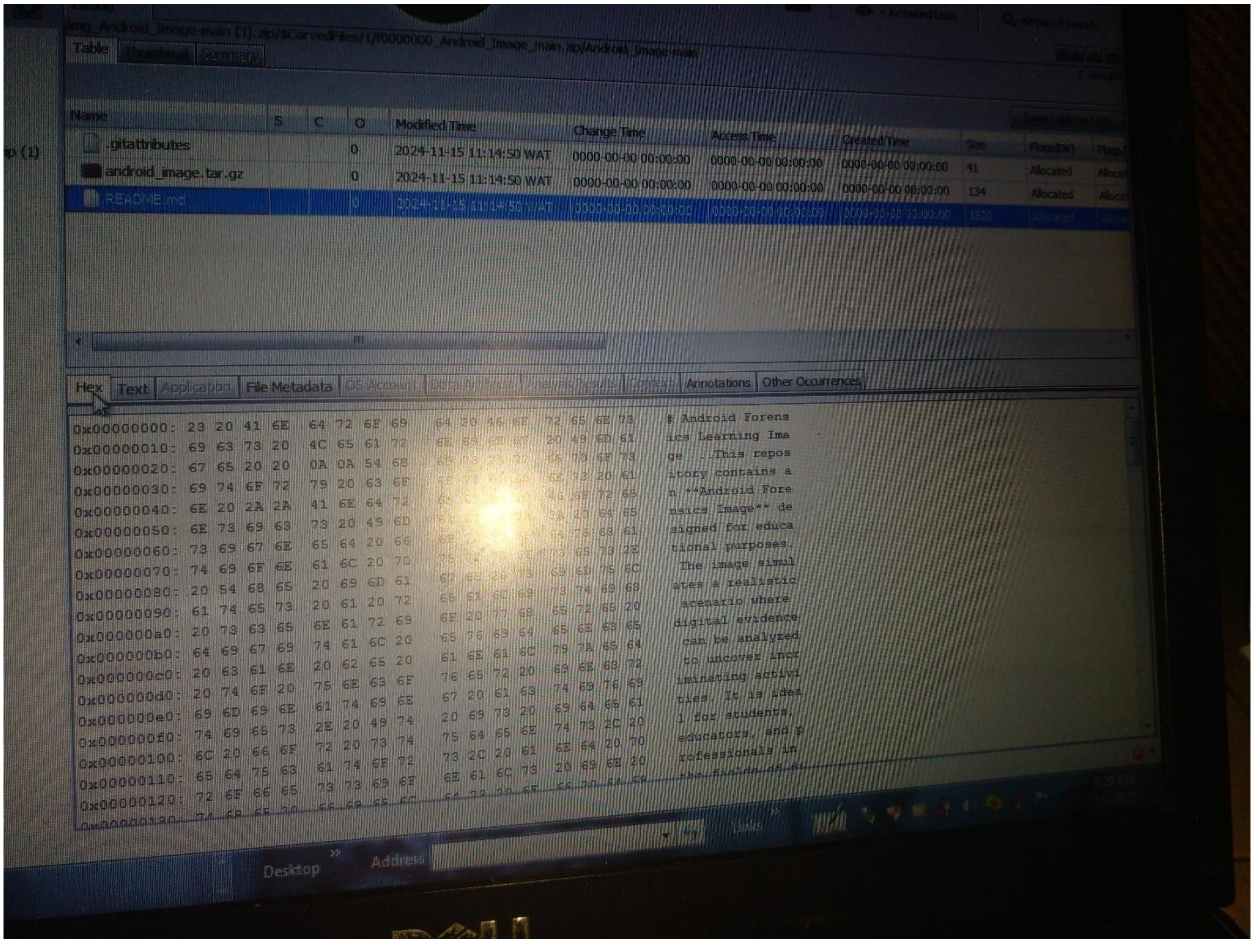
Metadata of forensic image



Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size
.gitattributes			0	2024-11-15 11:14:50 WAT	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	41
android_image.tar.gz			0	2024-11-15 11:14:50 WAT	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	134
README.md			0	2024-11-15 11:14:50 WAT	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1820

~~~
## Use Cases
This image is specifically crafted for:
1. **Digital Forensics Training**: Hands-on practice in [illegible] analyzing digital evidence.
2. **Cybersecurity Awareness**: Understanding the [illegible] or digital hygiene.
3. **Mock Investigations**: Simulating real-world scenarios [illegible] purposes.
## Disclaimer
This image is **strictly for educational purposes** and must [illegible] used for unethical or illegal activities. All data is fictional and created to provide a realistic learnin
## Getting Started
1. Clone this repository:
   ```bash
   git clone https://github.com/Akobe-Ajibolu/Android_Image.git
   ```
2. Extract the Android image:
 - Use a suitable extraction tool such as `tar` or `7z`.
 - Extract the image into a folder for easy access.
3. Analyze the image using Autopsy:
 - Open Autopsy and create a new case.
 - Add the extracted image as a data source.
 - Begin investigating the evidence using Autopsy's analysis tools.
~~~

Extracted text of forensic image

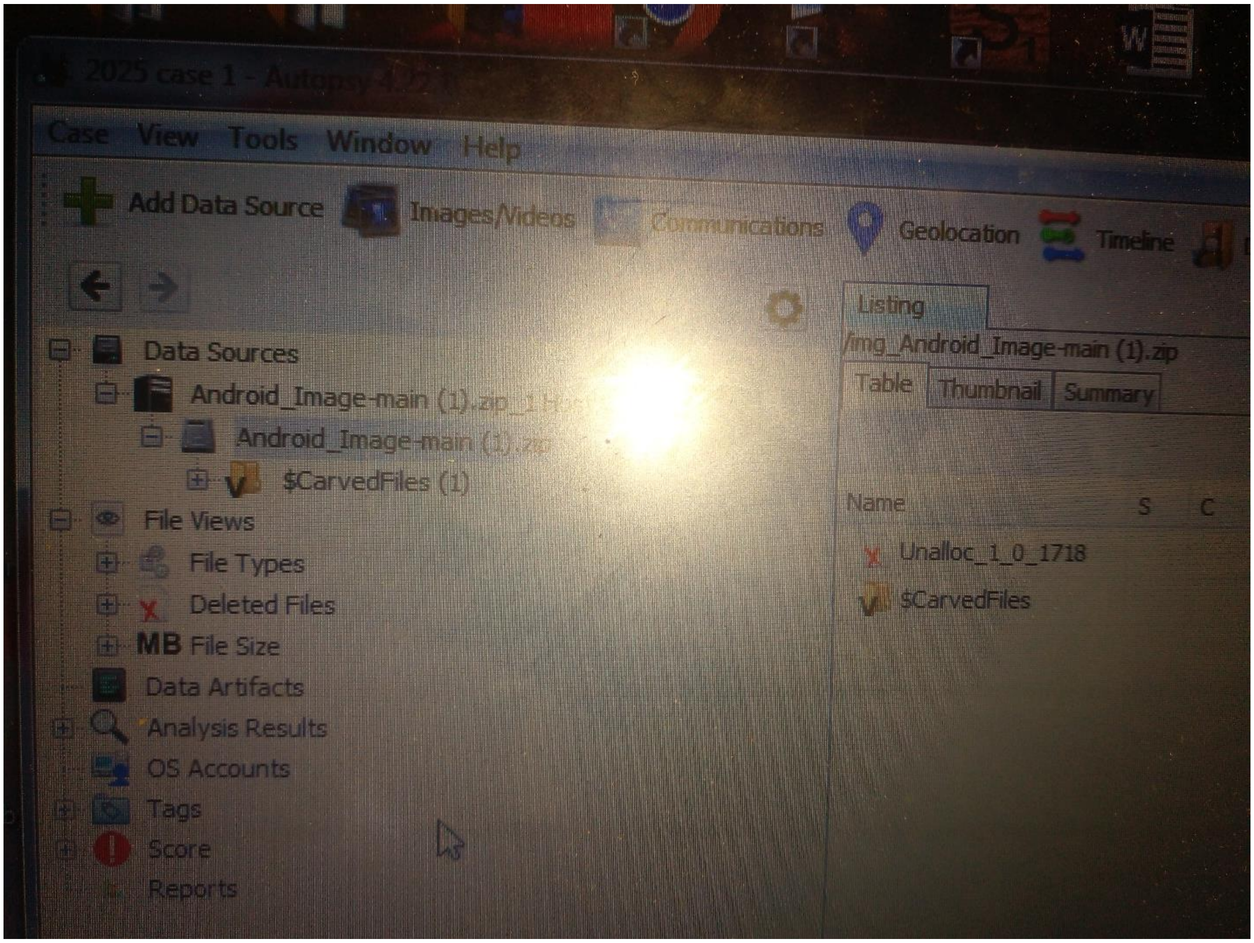


img_Android_Image-main (1).zip/$CarvedFiles/1/f0000000_Android_Image_main.zip/Android_Image-main

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags
.gitattributes			0	2024-11-15 11:14:50 WAT	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	41	Allocated	Allocat
android_image.tar.gz			0	2024-11-15 11:14:50 WAT	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	134	Allocated	Allocat
README.md			0	2024-11-15 11:14:50 WAT	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1820	Allocated	Allocat

```
0x00000000: 23 20 41 6E  64 72 6F 69  64 20 46 6F  72 65 6E 73   # Android Forens
0x00000010: 69 63 73 20  4C 65 61 72  6E 69 6E 67  20 49 6D 61   ics Learning Ima
0x00000020: 67 65 20 20  0A 0A 54 68  69 73 20 72  65 70 6F 73   ge  ..This repos
0x00000030: 69 74 6F 72  79 20 63 6F  6E 74 61 69  6E 73 20 61   itory contains a
0x00000040: 6E 20 2A 2A  41 6E 64 72  6F 69 64 20  46 6F 72 65   n **Android Fore
0x00000050: 6E 73 69 63  73 20 49 6D  61 67 65 2A  2A 20 64 65   nsics Image** de
0x00000060: 73 69 67 6E  65 64 20 66  6F 72 20 65  64 75 63 61   signed for educa
0x00000070: 74 69 6F 6E  61 6C 20 70  75 72 70 6F  73 65 73 2E   tional purposes.
0x00000080: 20 54 68 65  20 69 6D 61  67 65 20 73  69 6D 75 6C    The image simul
0x00000090: 61 74 65 73  20 61 20 72  65 61 6C 69  73 74 69 63   ates a realistic
0x000000a0: 20 73 63 65  6E 61 72 69  6F 20 77 68  65 72 65 20    scenario where 
0x000000b0: 64 69 67 69  74 61 6C 20  65 76 69 64  65 6E 63 65   digital evidence
0x000000c0: 20 63 61 6E  20 62 65 20  61 6E 61 6C  79 7A 65 64    can be analyzed
0x000000d0: 20 74 6F 20  75 6E 63 6F  76 65 72 20  69 6E 63 72    to uncover incr
0x000000e0: 69 6D 69 6E  61 74 69 6E  67 20 61 63  74 69 76 69   iminating activi
0x000000f0: 74 69 65 73  2E 20 49 74  20 69 73 20  69 64 65 61   ties. It is idea
0x00000100: 6C 20 66 6F  72 20 73 74  75 64 65 6E  74 73 2C 20   l for students, 
0x00000110: 65 64 75 63  61 74 6F 72  73 2C 20 61  6E 64 20 70   educators, and p
0x00000120: 72 6F 66 65  73 73 69 6F  6E 61 6C 73  20 69 6E 20   rofessionals in 
```

Fore



References: list of sources cited in the report