

DIGITAL FORENSIC ANALYSIS OF DSA ANDROID IMAGE

Case Information

Case Title: Android Device Forensic Analysis

Investigator Name: Ashante Okosun

Case Number: 001

Date of Investigation: 6/07/2025

Device Type: Phone

Tools Used: Autopsy, Android Image

1. Methodology

1.1 Evidence Acquisition

Android forensic image received: [android_image.tar.gz]

Image mounted and analyzed using Autopsy and supporting forensic tools.

1.2 Forensic Tools Utilized

* Autopsy: Image analysis and reporting

* Android Image: Extract evidence

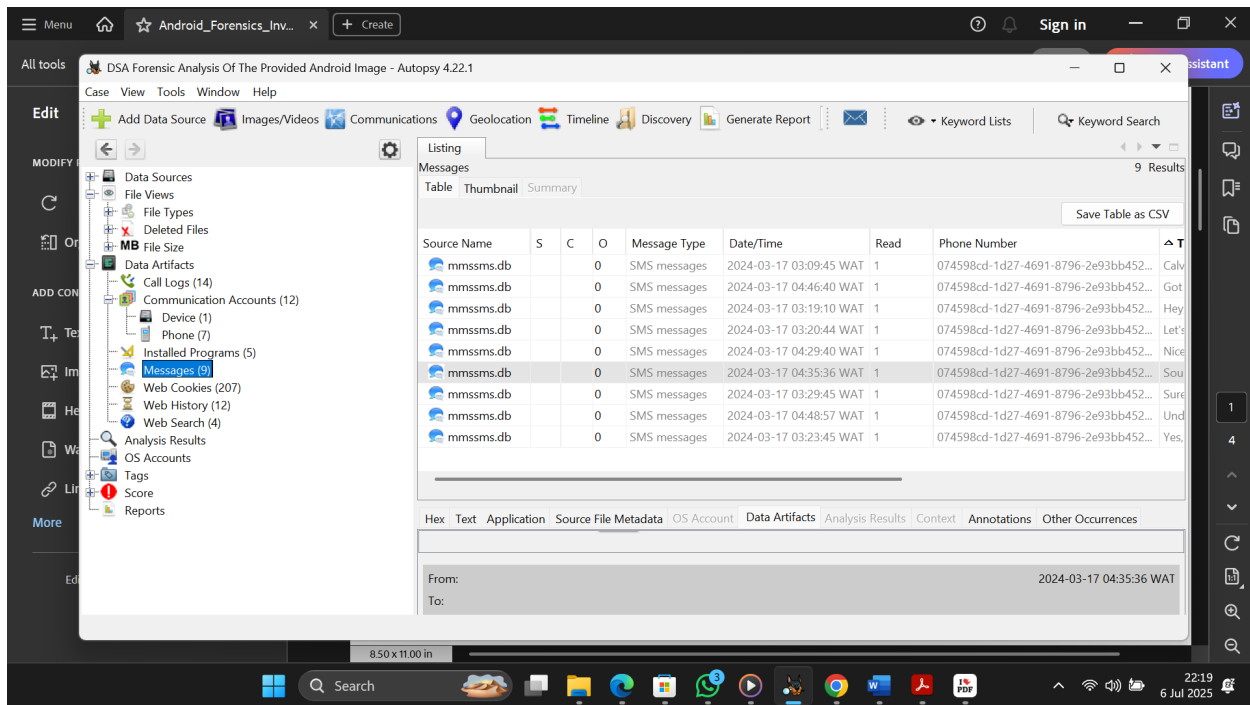
2. Findings

2.1 SMS Messages

* Tool Used: Autopsy_Communications Tab

* Total Messages Recovered: 9

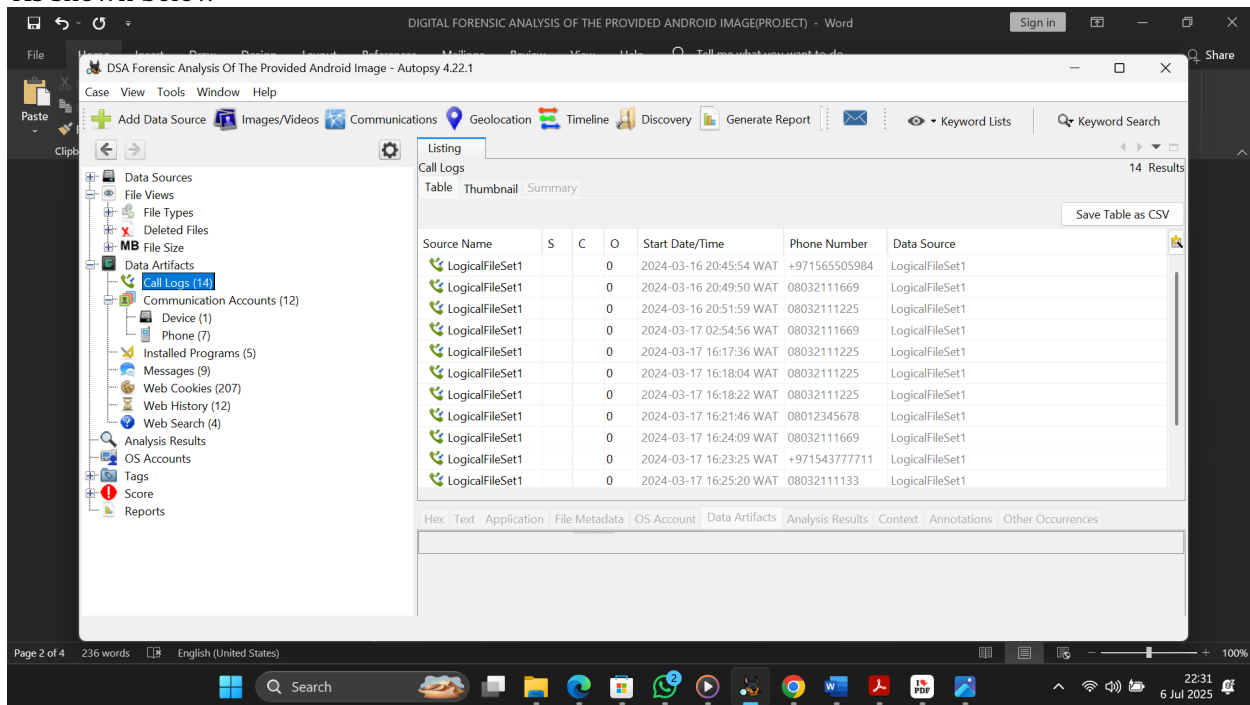
* Sender: 08032111133



2.2 Call Logs

Total Entries: 14

As shown below



2.3 Phone Contact List

The screenshot displays the Autopsy 4.22.1 interface. The left sidebar shows the 'Phone (7)' folder selected under 'Data Artifacts'. The main window shows a 'Listing' view with a table of 10 results. The table has columns for Source Name, S, C, O, Account Type, ID, and Data Source. The data is as follows:

Source Name	S	C	O	Account Type	ID	Data Source
LogicalFileSet1			0	PHONE	15554	LogicalFileSet1
LogicalFileSet1			0	PHONE	+971565505984	LogicalFileSet1
LogicalFileSet1			0	PHONE	08032111669	LogicalFileSet1
LogicalFileSet1			0	PHONE	08032111225	LogicalFileSet1
LogicalFileSet1			0	PHONE	08012345678	LogicalFileSet1
LogicalFileSet1			0	PHONE	+971543777711	LogicalFileSet1
LogicalFileSet1			0	PHONE	08032111133	LogicalFileSet1
mmssms.db			0	PHONE	08032111669	LogicalFileSet1
mmssms.db			0	PHONE	08032111133	LogicalFileSet1
mmssms.db			0	PHONE	+971543777711	LogicalFileSet1

2.4 Application Usage/Web History

The screenshot displays the Autopsy 4.22.1 interface. The left sidebar shows the 'Web History (12)' folder selected under 'Data Artifacts'. The main window shows a 'Listing' view with a table of 12 results. The table has columns for Source Name, S, C, O, Date Created, Date Accessed, and URL. The data is as follows:

Source Name	S	C	O	Date Created	Date Accessed	URL
LogicalFileSet1				2024-03-17 03:49:04 WAT	2024-03-17 03:49:04 WAT	https://www.google.com/search?client=ms-ur
LogicalFileSet1				2024-03-17 03:47:51 WAT	2024-03-17 03:47:51 WAT	https://www.nairaland.com/6982372/scared-l
LogicalFileSet1					2024-03-17 03:39:59 WAT	https://www.google.com/search?q=new+and
LogicalFileSet1					2024-03-17 03:40:47 WAT	https://www.google.com/search?client=ms-ur
LogicalFileSet1					2024-03-17 03:40:55 WAT	https://www.google.com/url?q=https://busin-
LogicalFileSet1					2024-03-17 03:40:55 WAT	https://businessday.ng/technology/article/he
LogicalFileSet1					2024-03-17 03:42:06 WAT	https://www.google.com/search?q=How+to+
LogicalFileSet1					2024-03-17 03:42:59 WAT	https://www.google.com/url?q=https://www.u
LogicalFileSet1					2024-03-17 03:42:59 WAT	https://www.nairaland.com/6982372/scared-l
LogicalFileSet1					2024-03-17 03:48:57 WAT	https://www.google.com/search?client=ms-ur
LogicalFileSet1					2024-03-17 03:48:31 WAT	https://www.google.com/url?q=https://www.u
LogicalFileSet1					2024-03-17 03:48:51 WAT	https://www.nairaland.com/5033957/efcc-de

2.5 User Files & Images

The screenshot shows the Autopsy 4.22.1 interface. The left sidebar displays a tree view of data sources, with 'File Types' expanded and 'By Extension' selected. The main pane shows a table of file types and their extensions.

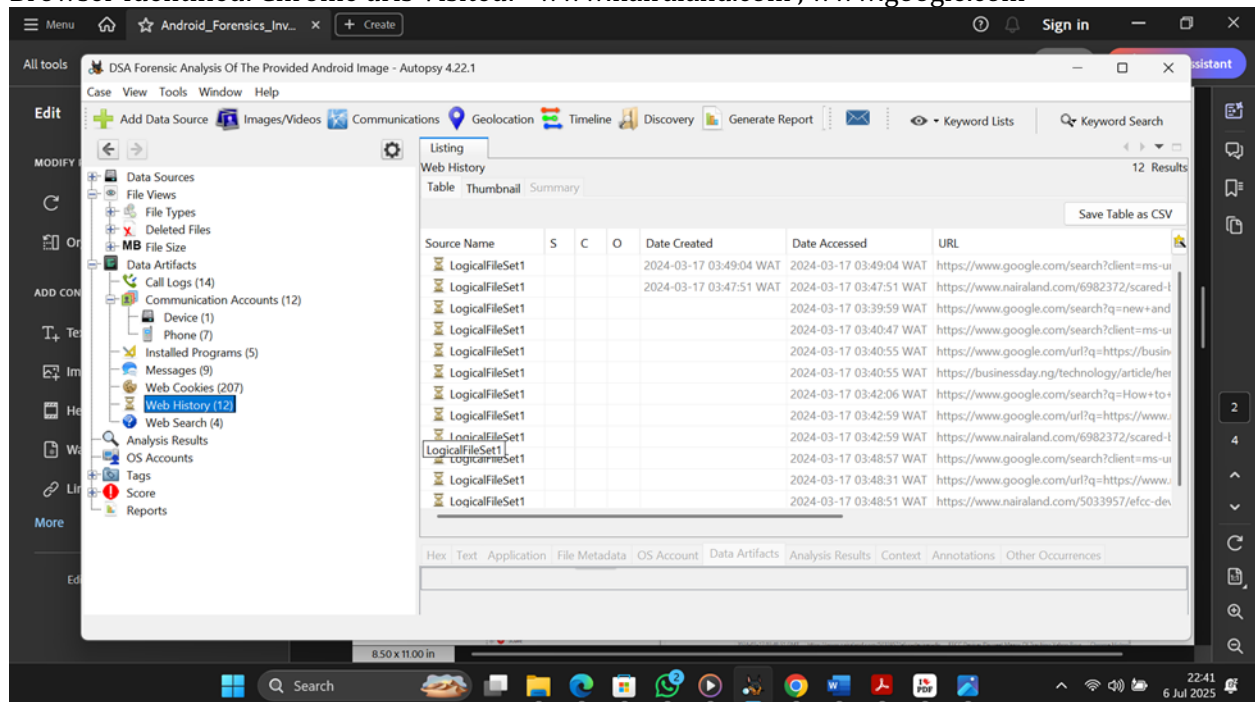
File Type	File Extensions
Images (97)	jpg, jpeg, .png, .psd, .nef, .tif, .bmp, .tec, .tif, .webp
Videos (0)	.aaf, .3gp, .asf, .avi, .m1v, .m2v, .m4v, .mp4, .mov, .mpeg, .mpg, .mpe, .mp4, .rm, .wmv, .mpv, .flv, .swf
Audio (0)	.aiff, .aif, .flac, .wav, .m4a, .ape, .wma, .mp2, .mp1, .mp3, .aac, .mp4, .m4p, .m1a, .m2a, .m4r, .mpa, .m3u, .mid, ...
Archives (13)	.zip, .rar, .7zip, .7z, .arj, .tar, .gzip, .bzip, .bzip2, .cab, .jar, .cpio, .ar, .gz, .tgz, .bz2
Databases (105)	.db, .db3, .sqlite, .sqlite3
Documents	.html, .htm, .doc, .docx, .odt, .xls, .xlsx, .ppt, .pptx, .pdf, .txt, .rtf
Executable	.exe, .msi, .cmd, .com, .bat, .reg, .scr, .dll, .lni

The screenshot shows the Autopsy 4.22.1 interface. The left sidebar displays a tree view of data sources, with 'File Types' expanded and 'By MIME Type' selected. The main pane shows a table of file types and their MIME types.

Name
By Extension
By MIME Type

2.6 Browser History

Browser Identified: Chrome urls Visited: - www.nairaland.com , www.google.com



2.7 Crypto Wallet Artifacts

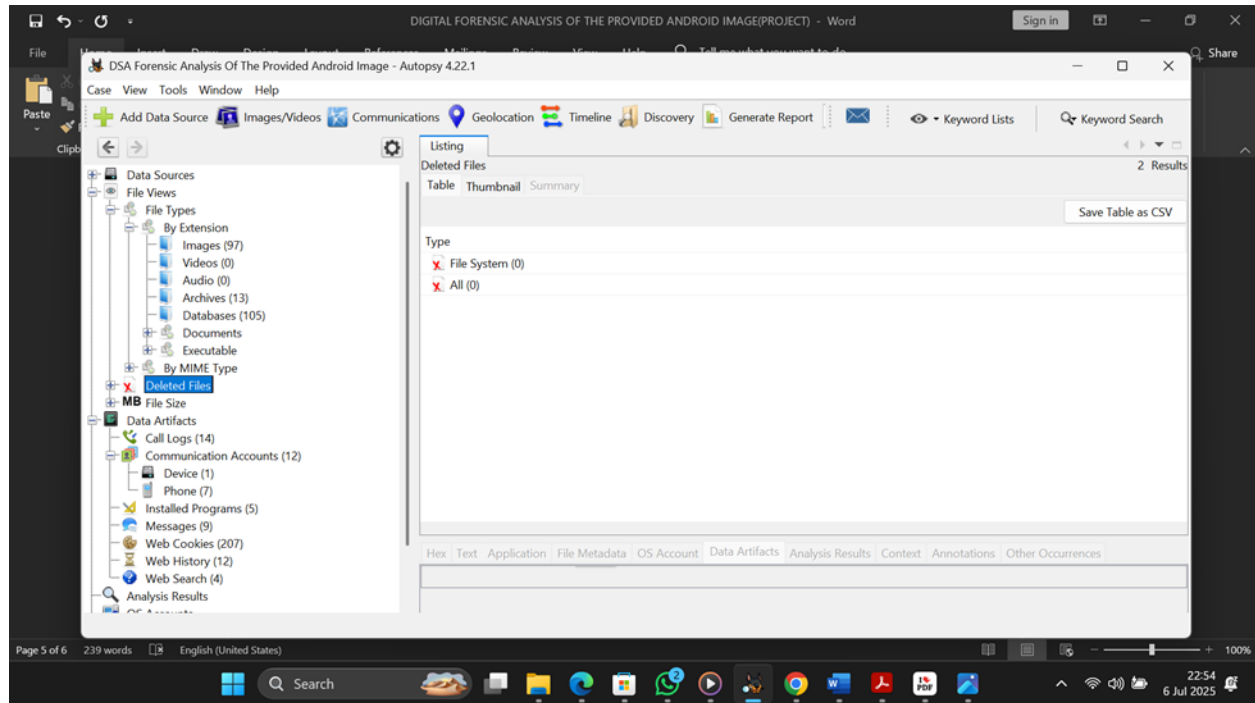
*Applications Found- Bitcoin wallet address: 16AtGJbaxL2kmzx4mW5ocpT2ysTWxmacWn.

*Location: messages

2.8 Deleted Content

Recovery Method: Carving with Autopsy

No deleted files



3. Conclusion

The forensic investigation of the provided Android image revealed key digital artifacts related to: - Communication logs (calls and SMS) - Application behavior and potential usage in illicit activities - Presence of cryptocurrency wallet applications - Images used for illicit behaviours

4. Professional Recommendations

- Preserve the original image for chain-of-custody integrity - Secure a warrant for decryption of app data - Cross-reference contacts with known persons of interest - Monitor transactions from recovered crypto wallet addresses - Consider deep analysis of cloud sync services (Google Drive, WhatsApp backups)

Ashante Okosun

DSA Cybersecurity Student

ashanteokosun@gmail.com

+2348027594783

