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.

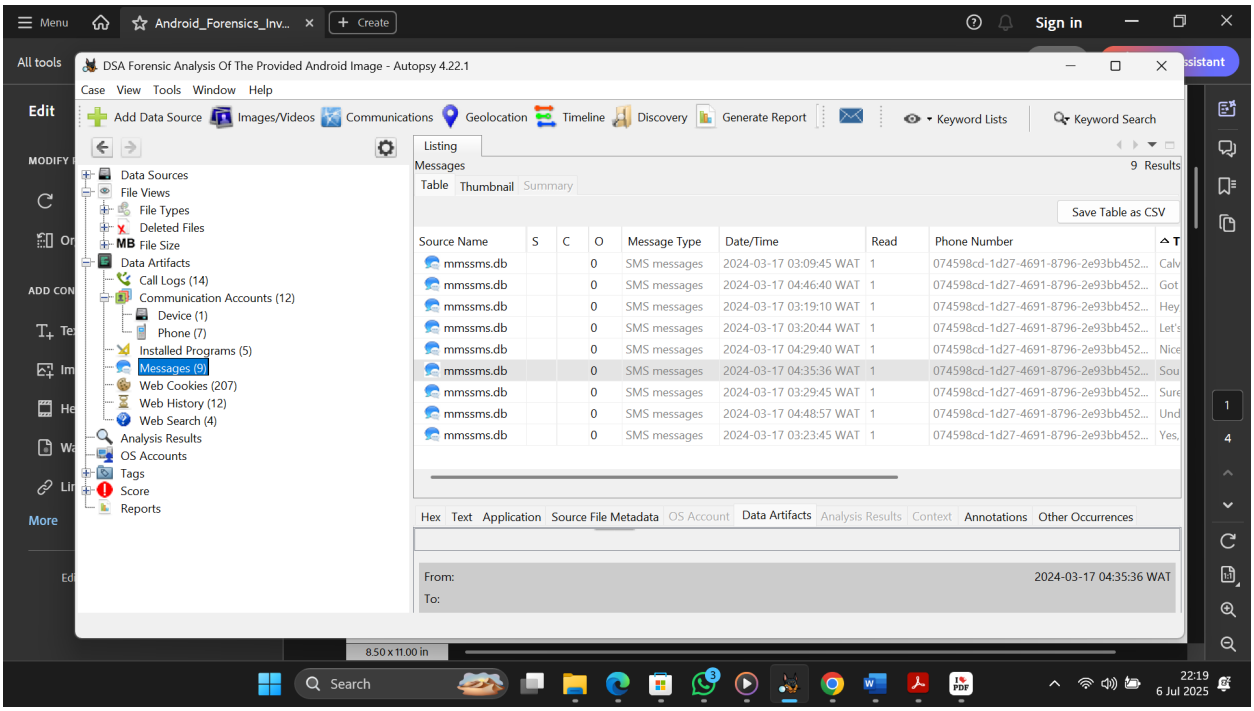
1.2 Forensic Tools Utilized

*Autopsy: Image analysis and reporting
* Android Image: Extract evidence

2. Findings

2.1 SMS Messages

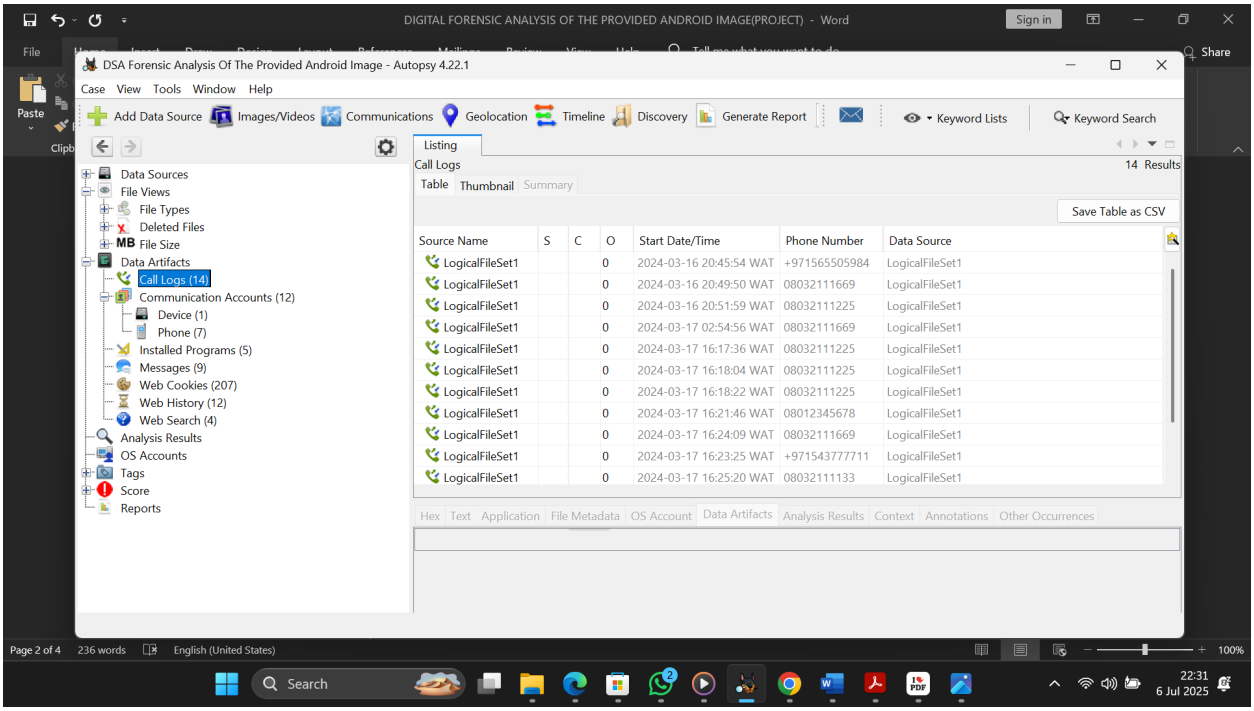
*Tool Used: Autopsy_Communications Tab
*Total Messages Recovered: 9
* Sender: 08032111133



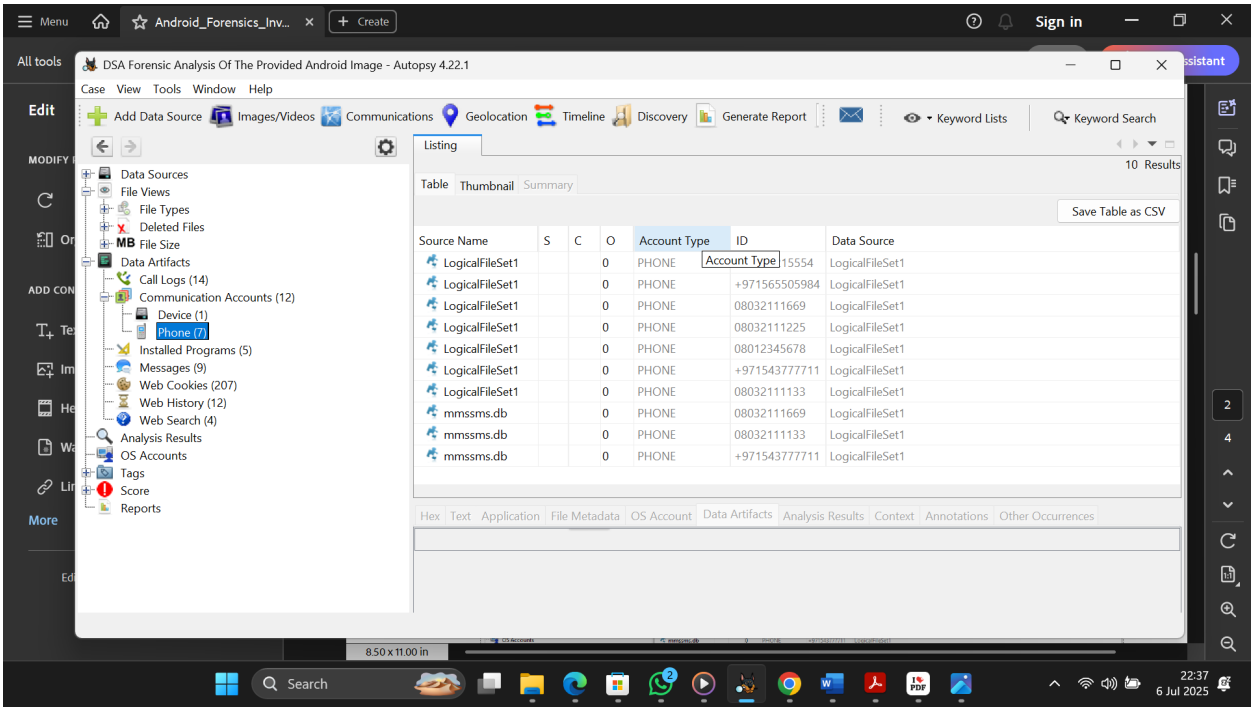
2.2 Call Logs

Total Entries: 14

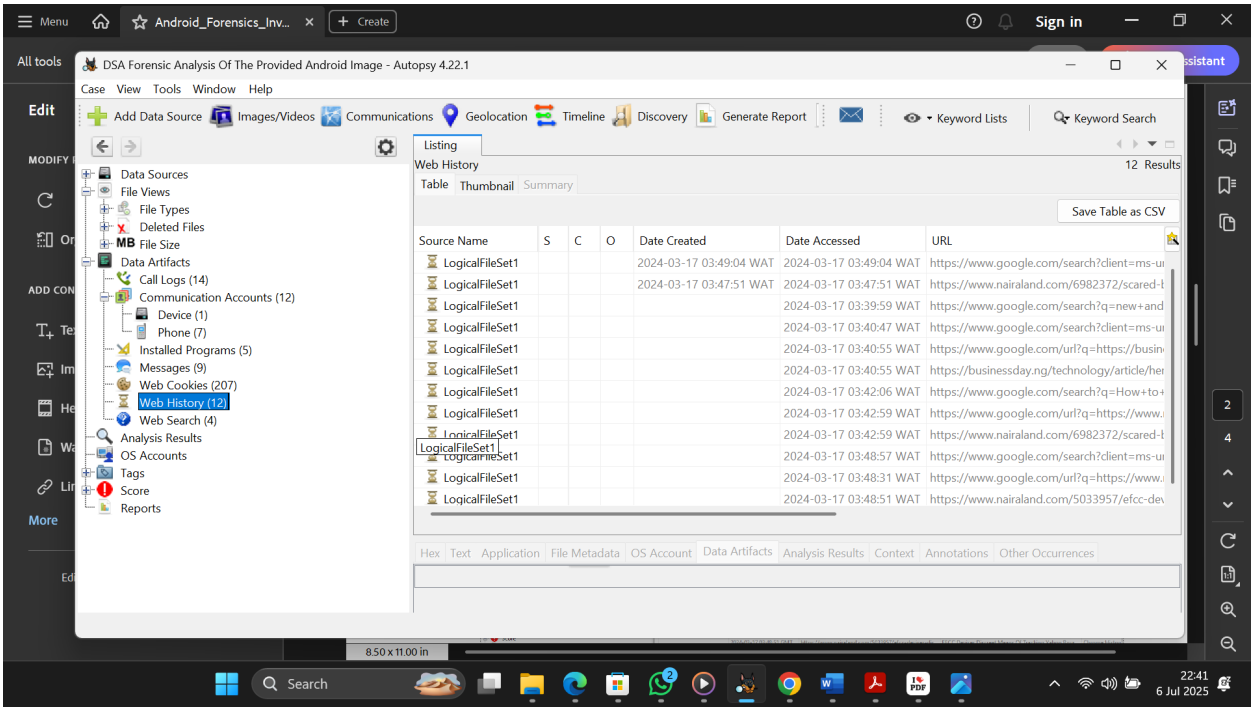
As shown below



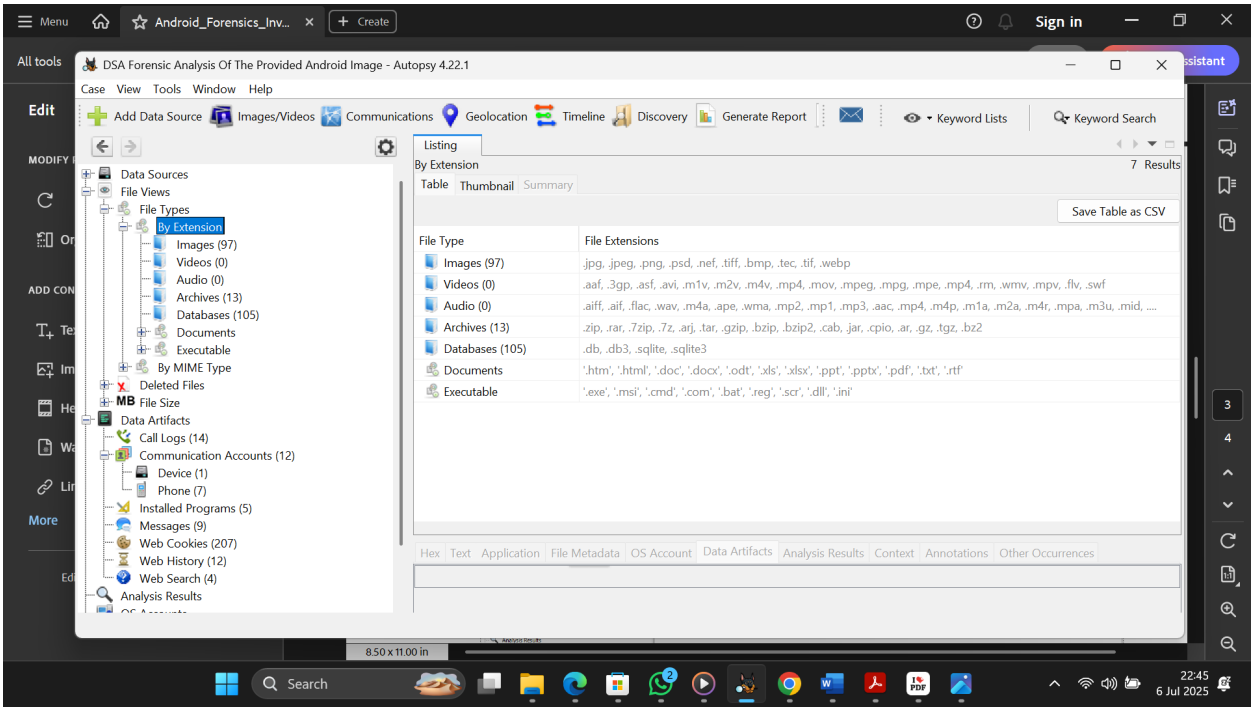
2.3 Phone Contact List

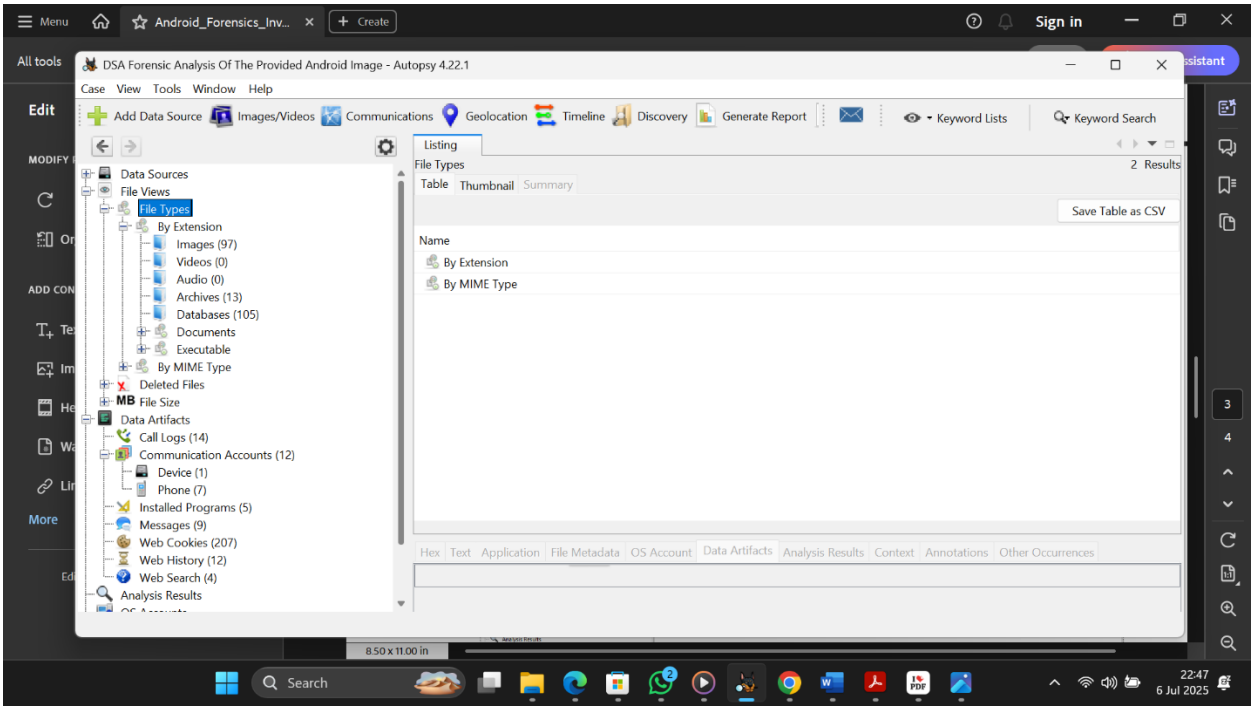


2.4 Application Usage/Web History



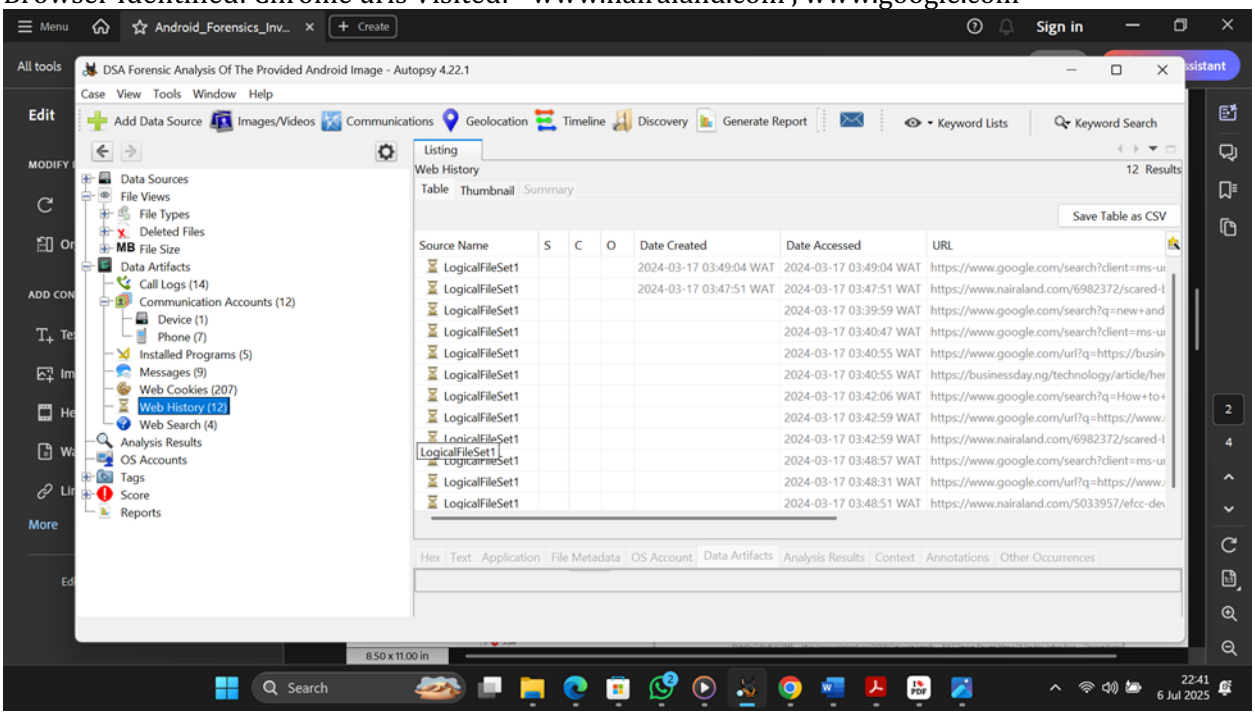
2.5 **User Files & Images**





2.6 Browser History

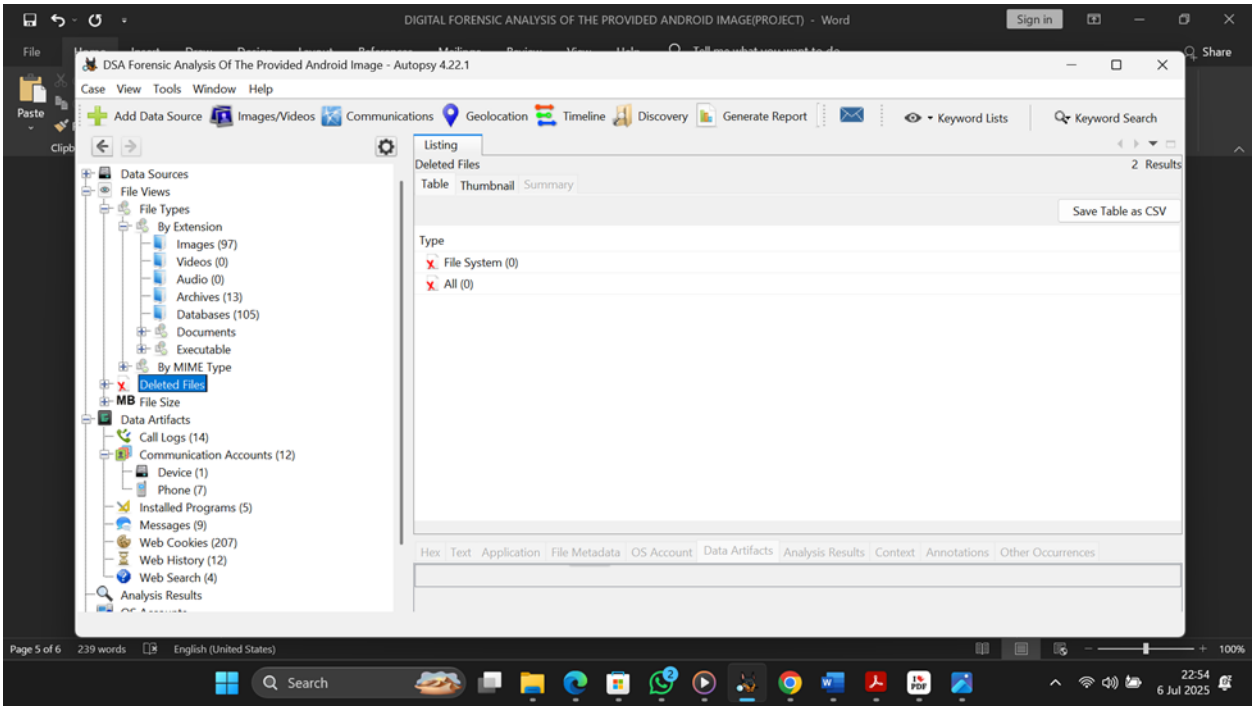
Browser Identified: Chrome urls Visited: - www.nairaland.com , www.google.com



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