ANDROID MOBILE FORENSICS INVESTIGATION: ARTIFACT EXTRACTION AND ANALYSIS

CYBER SECURITY CAPSTONE PROJECT

REPORT ADDRESSED TO: INSTRUCTOR

PREPARED BY EUNICE ALAO

CASE NUMBER: 007

EVIDENCE FILENAME: ANDROID_IMAGE.DD

JULY 18, 2025

THE INCUBATOR HUB

Introduction

This report presents a digital forensic analysis of a provided Android device image. The objective was to simulate a real-world mobile investigation by extracting and examining key artifacts such as SMS messages, call logs, contacts, browser history, application data, and deleted content. The investigation aimed to uncover user activity patterns and potential digital evidence that may be relevant to a legal or security-related inquiry.

Tools Used

1. Autopsy
2. 7-zip File Manager

Methodology

To begin the forensic investigation, the provided Android image file was first extracted using 7-Zip, a reliable open-source utility for handling compressed archives. Once the image was successfully extracted, Autopsy, a digital forensics platform was used to analyze the contents of the image.

A new case was created in Autopsy, and the extracted image file was added as the primary data source. The platform automatically indexed the file system and parsed key artifact categories including communications (SMS, call logs, contacts), web activity, images, application data, and deleted content. Each artifact was then reviewed manually within the Autopsy interface, and relevant findings were documented through screenshots and notes for inclusion in this report.

Findings

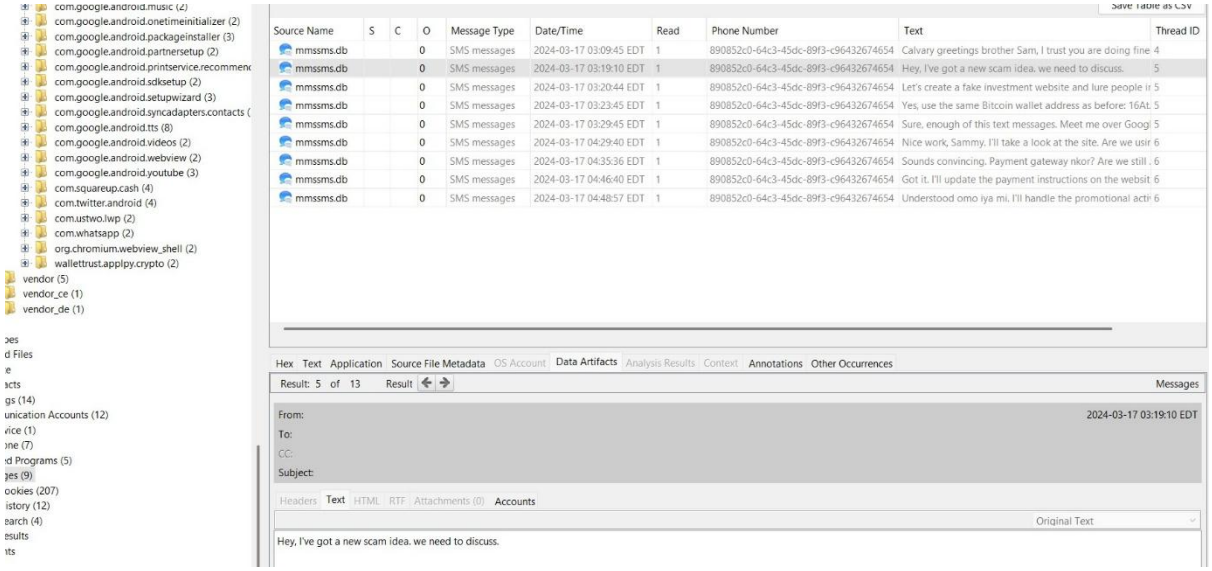
SMS and Call Log Analysis

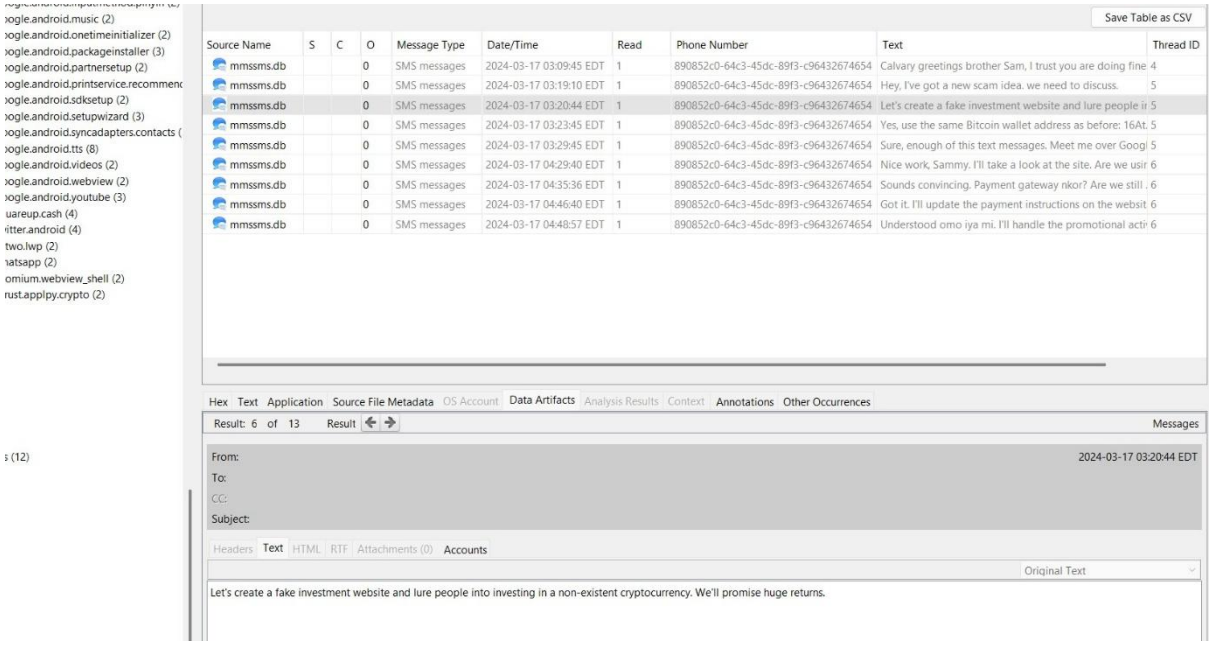
A total of 8 SMS messages were recovered during the forensic analysis of the Android image. These messages revealed an ongoing fraudulent planning and collaboration. These involved discussions around creating a fake investment platform, soliciting victims using false promises, and transacting through cryptocurrency to avoid traceability. Notable artifacts include:

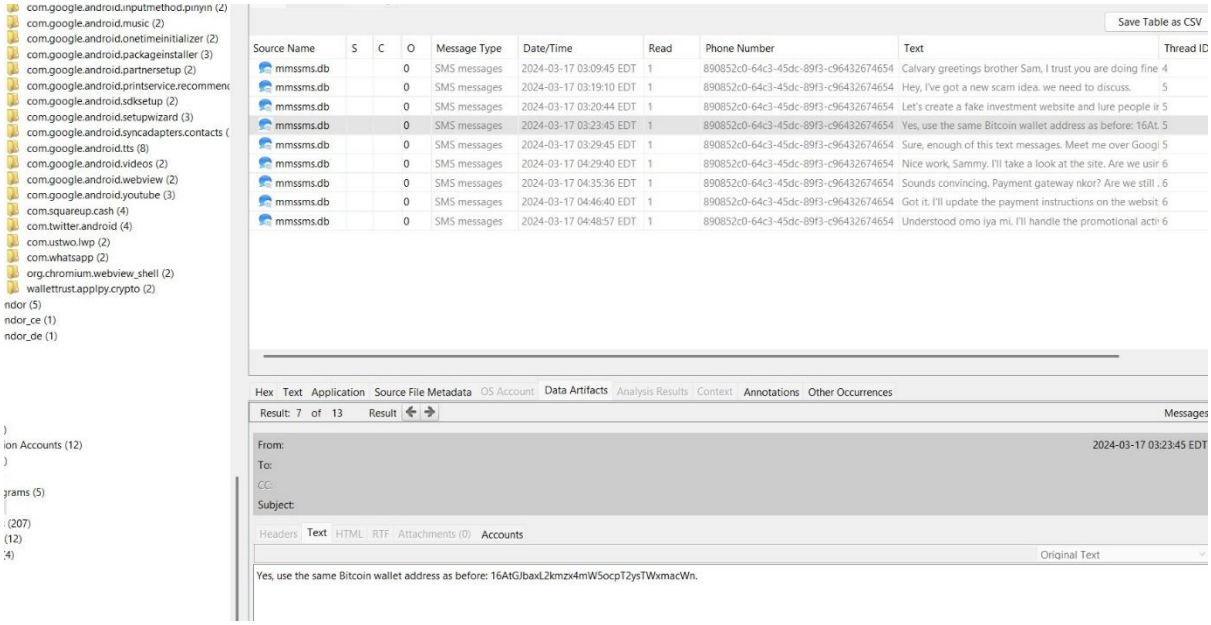
- A proposal for a scam involving fake cryptocurrency investments
- Reference to a previously used Bitcoin wallet address: 16AtGJbaxL2kmzx4mW5ocpT2ysTWxmacWn

- Operational terms such as “promotional activities,” “payment gateway,” and “when we dey go live?” clearly point to premeditated cybercrime.
- Use of code-switching (mix of English and informal language), indicating familiarity and possible attempt at concealment.

Screenshots of some of the message threads were taken to document the artifacts.







The call log artifact contained records of 14 outgoing calls made to 7 unique phone numbers. Due to the nature of the associated SMS messages, it is plausible that some or all these contacts were linked to the planning or execution of the suspected fraudulent scheme. Each call log entry included a call ID.

Application Usage History

Analysis of the installed applications on the Android image revealed the presence and usage of several high-interest apps, suggesting the device owner's behavioural and digital footprint. Notably, the following applications were identified: YouTube, twitter, WhatsApp, Square up cash app, and Trust wallet.

The presence of these applications, particularly Cash App and Trust Wallet, in conjunction with SMS messages discussing a fake investment scam, indicates deliberate use of crypto-fintech tools to conceal financial trails. Combined with communication apps like WhatsApp and Twitter, the device likely served as a hub for both planning and executing digital fraud.

Browser History Analysis

The suspect's browser history reveals a pattern of visits and searches that suggest an intent to engage in fraudulent online activities and a concern about law enforcement tracking. Key websites accessed include:

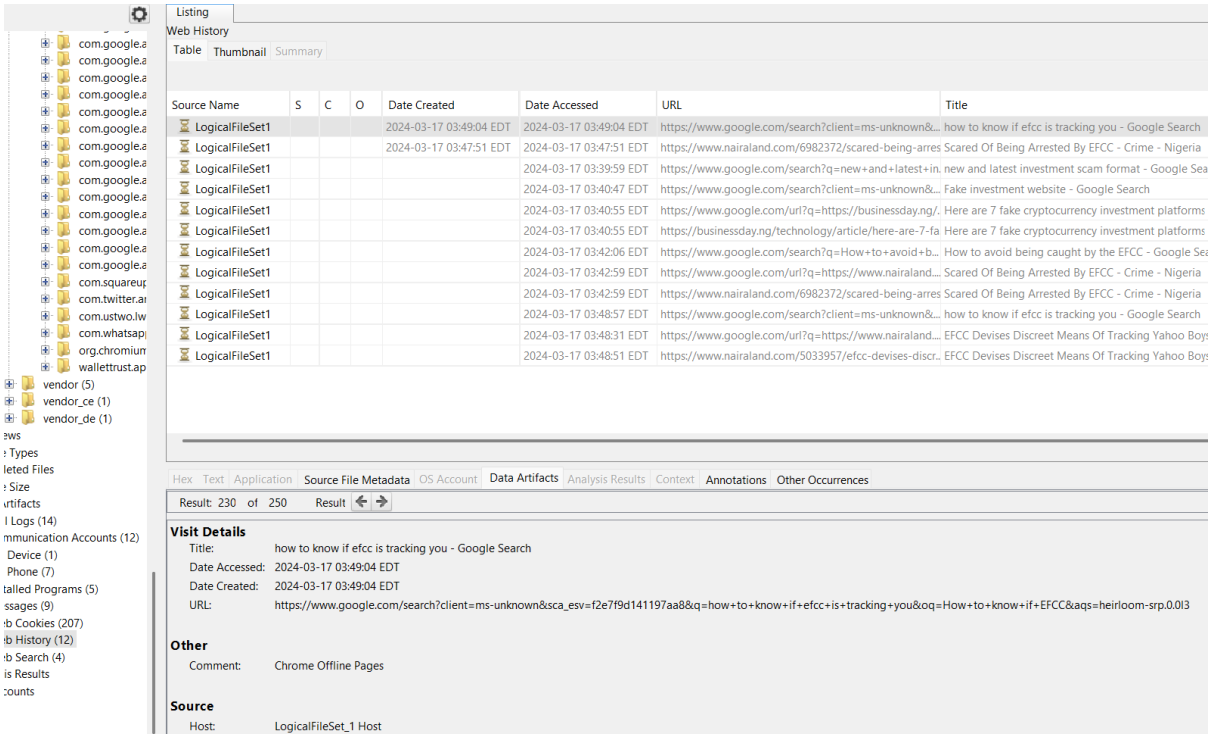
- Google – Used for multiple search queries.

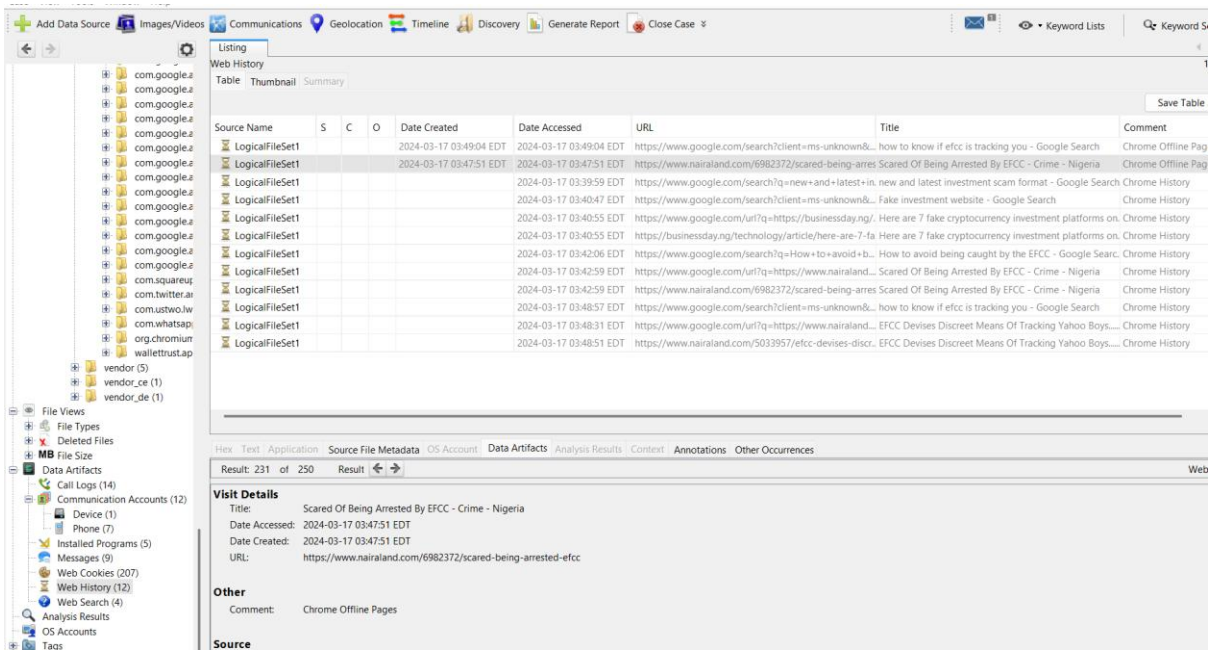
- Naira land – A popular Nigerian online forum, potentially used to gather information or connect with others.

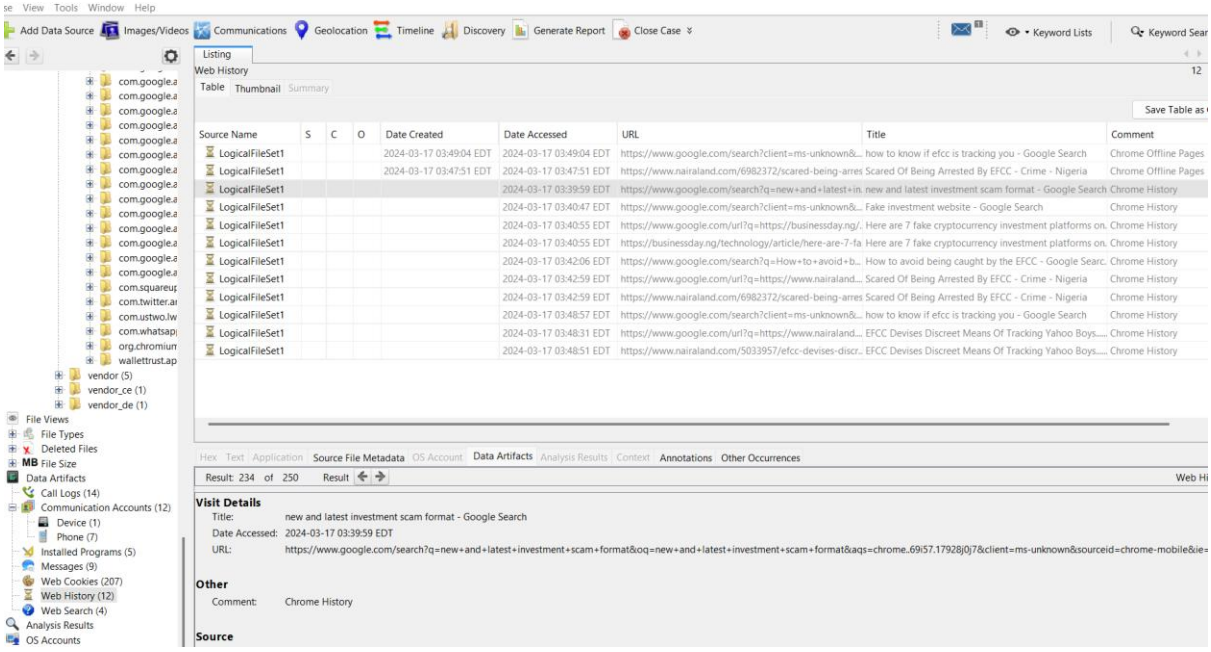
Notable search queries include:

- Scared of being arrested by EFCC
- How to know if EFCC is tracking you
- New and latest investment scam format
- Fake investment website
- Fake cryptocurrency investment platforms

The pattern supports the likelihood that the individual was researching ways to evade detection while developing or executing online fraud tactics.







Conclusion and Recommendations

Conclusion

The forensic examination of the Android device image revealed compelling evidence suggestive of coordinated fraudulent activity which involved planning and potentially executing cyber-enabled financial fraud.

Recommendation

1. Deeper Dive into Cryptocurrency Transactions
2. Cross-reference findings with law enforcement databases
3. Secure all extracted data and logs for legal proceedings, ensuring the integrity of evidence for prosecution