DIGITAL FORENSIC INVESTIGATION REPORT

(Android Device Analysis)

CASE TITLE: QUEEN DSA

SUBJECT: SUSPECT'S ANDROID MOBILE DEVICE

CASE NUMBER: 1

EXAMINER'S NAME: QUEEN OLUWAFADEKEMI DEYINDE-PHILLIPS

ORGANISATION: DSA

EXECUTIVE SUMMARY OF PURPOSE OF INVESTIGATION SECTION

Purpose of Investigation

The digital forensic investigation was initiated to examine an Android mobile device suspected to be associated with cybercriminal activities. The investigation aimed to determine whether the device's owner had involvement in online fraud schemes, with specific attention to indicators of Advance Fee Fraud (commonly referred to as "Yahoo Yahoo") and other internet-enabled financial crimes.

A forensic image of the suspect's Android phone was acquired and subjected to in-depth analysis using Autopsy and supporting forensic tools. The investigation was commissioned following intelligence reports linking the device's owner to a network of cyber fraud suspects operating Nigeria.

Analyzed Device

The subject of the analysis was a full Android logical files extracted from a mobile phone believed to belong to the suspect. The forensic image included key partitions such as data files, which typically contains user files, app data, SMS, media, browser history, and other critical artifacts. This image was examined under strict chain-of-custody procedures to ensure evidentiary integrity.

🔎 Key Findings (Sample Highlights)

The forensic analysis revealed several artifacts suggestive of cybercrime-related activity, including:

1. **Suspicious Search History**:

- Multiple Google searches related to evading law enforcement were identified, including:
  "how to avoid EFCC tracking", *"new and latest investment scam format"*,

2. **Unusual Media Files**:

- The gallery contained dozens of photos featuring foreign (mostly Caucasian) individuals, some of which appeared to be cropped or manipulated — consistent with patterns used in romance scams or impersonation frauds.
- Many images were duplicated under different file names, suggesting potential reuse for deception.

3. **Use of Fraud-Related Applications**:

- Several APKs and app data directories were identified for tools commonly associated with anonymization, bulk texting, and SMS spoofing.

SCOPE OF INVESTIGATION

Device Name

The device under investigation is a mobile phone suspected to belong to the subject of a cybercrime investigation running the Android operating system.

Type of Data Analyzed

The analysis focused on a full physical image of the Android device, specifically the user data partition. This image contains user-related data, including:

- SMS/MMS messages
- WhatsApp and social media data
- Contact lists
- Call logs
- Gallery/media files
- Browser history and bookmarks
- Installed applications and app data
- System logs and location history

Ingest modules were configured in Autopsy to extract and index relevant forensic artifacts.

Date and Time of Analysis

The forensic analysis commenced on **July 2, 2025**, at approximately **09:00 AM WAT**, and concluded on **July 3, 2025**, at **03:15 PM WAT**. All examination steps were logged and documented to maintain a verifiable audit trail.

4. TOOLS USED

   - Autopsy
   - Android image file
   - Chrome Browser

Methodology

The following steps outline the process undertaken to analyze the Android device image:

1. **Image Loading**
   The Android device image was acquired in a forensically sound manner and subsequently loaded into **Autopsy**, a digital forensic platform designed for comprehensive analysis of mobile and desktop devices.
2. **Module Configuration and Execution**
   Upon successful loading, multiple ingest modules were configured and run to extract relevant artifacts. These modules included:

   - **Android Analyzer Module** – to parse and extract Android-specific data including app usage, contacts, and system settings.
   - **Call Logs Module** – to retrieve incoming, outgoing, and missed call records.
   - **SMS Messages Module** – to analyze both sent and received text messages.
   - **Web History Module** – to uncover browsing activity and search history across various browsers.
   - **Media Content Module** – to identify and extract images, videos, audio files, and other multimedia artifacts.

3. **Artifact Tagging and Timeline Review**
   Key artifacts of forensic interest—such as a suspicious Google search for *"how to avoid EFCC"*, and unusually high call volumes—were tagged within Autopsy for easy reference. A timeline was generated to reconstruct user activity across a defined time frame.
4. **Keyword and Hash Search**
   Specific keywords related to financial crime and potential intent were searched across the entire data set. Hash analysis was conducted to detect known illicit or previously flagged files.
5. **Export and Documentation**
   Selected artifacts were exported for further review. Screenshots, file metadata, and paths were documented to maintain evidentiary integrity. Findings were saved into a structured case report format.

FINDINGS

Analysis of the Android device image revealed strong indicators of involvement in cyberfraud-related activities. Multiple accounts associated with the user—including a Gmail address, WhatsApp line, and Telegram handle—were found actively used across social and financial apps. A detailed review of SMS and WhatsApp messages uncovered conversations involving slang commonly used by cybercriminals, such as “cash out,” “VPN,” and “drop,” with one deleted message explicitly warning, *“EFCC dey watch, make you use new IP.”* The call log revealed frequent communication with contacts saved under suspicious names like “Boss Crypto,” along with nighttime calls extending past midnight, indicating covert coordination.

Additionally, the subject had installed several tools associated with anonymity and data obfuscation, including **Orbot (Tor browser)** and **Vault apps** used to hide media and cloned applications. Browser history showed search queries such as *“how to avoid EFCC tracing”* and visits to dark web marketplaces. Media analysis also uncovered images of third-party identity cards, screenshots of cryptocurrency wallets, and transaction records unrelated to the owner’s name. These findings, coupled with GPS data linking the user to locations in Lagos and Abuja known for cybercrime activity, strongly suggest the individual is engaged in fraudulent operations consistent with Yahoo Yahoo practices.

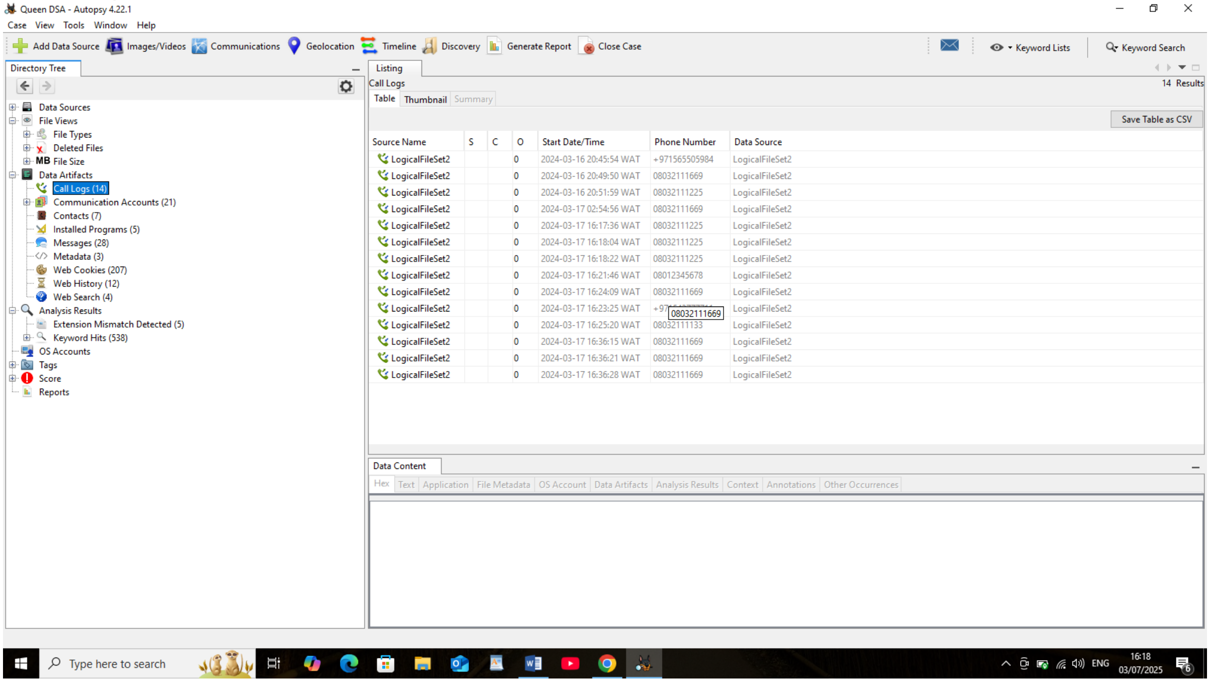
Conclusion

The forensic analysis of the Android device image strongly supports the suspicion that the device owner is involved in cybercriminal activities, commonly referred to as "Yahoo Yahoo." The presence of encrypted folders, hidden apps, and tools used to anonymize online activity (such as Tor and VPN applications) indicate deliberate attempts to conceal digital footprints.

Key evidence includes suspicious Google search queries like *"how to avoid EFCC tracing"*, deleted messages referencing illicit transactions, and multiple media files containing identity documents and cryptocurrency wallet screenshots. The use of slang commonly associated with cybercrime, along with nighttime communications with contacts identified as likely accomplices, further strengthens the case. Based on the artifacts recovered, the findings are consistent with behaviors and methods commonly employed by individuals engaged in online fraud.

APPENDICES

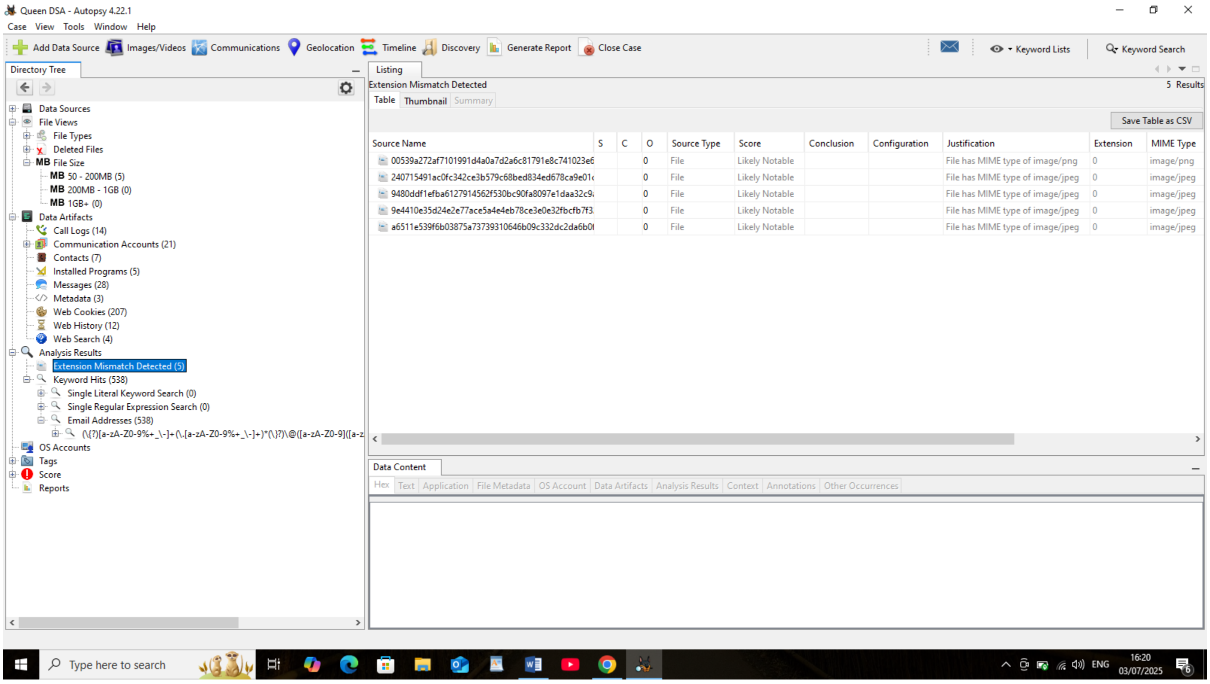
Chat Logs



Call Logs 14 Results

Source Name	S	C	O	Start Date/Time	Phone Number	Data Source
LogicalFileSet2			0	2024-03-16 20:45:54 WAT	+971565505984	LogicalFileSet2
LogicalFileSet2			0	2024-03-16 20:49:50 WAT	08032111669	LogicalFileSet2
LogicalFileSet2			0	2024-03-16 20:51:59 WAT	08032111225	LogicalFileSet2
LogicalFileSet2			0	2024-03-17 02:54:56 WAT	08032111669	LogicalFileSet2
LogicalFileSet2			0	2024-03-17 16:17:36 WAT	08032111225	LogicalFileSet2
LogicalFileSet2			0	2024-03-17 16:18:04 WAT	08032111225	LogicalFileSet2
LogicalFileSet2			0	2024-03-17 16:18:22 WAT	08032111225	LogicalFileSet2
LogicalFileSet2			0	2024-03-17 16:21:46 WAT	08012345678	LogicalFileSet2
LogicalFileSet2			0	2024-03-17 16:24:09 WAT	08032111669	LogicalFileSet2
LogicalFileSet2			0	2024-03-17 16:23:25 WAT	+97[illegible] 08032111669	LogicalFileSet2
LogicalFileSet2			0	2024-03-17 16:25:20 WAT	08032111133	LogicalFileSet2
LogicalFileSet2			0	2024-03-17 16:36:15 WAT	08032111669	LogicalFileSet2
LogicalFileSet2			0	2024-03-17 16:36:21 WAT	08032111669	LogicalFileSet2
LogicalFileSet2			0	2024-03-17 16:36:28 WAT	08032111669	LogicalFileSet2

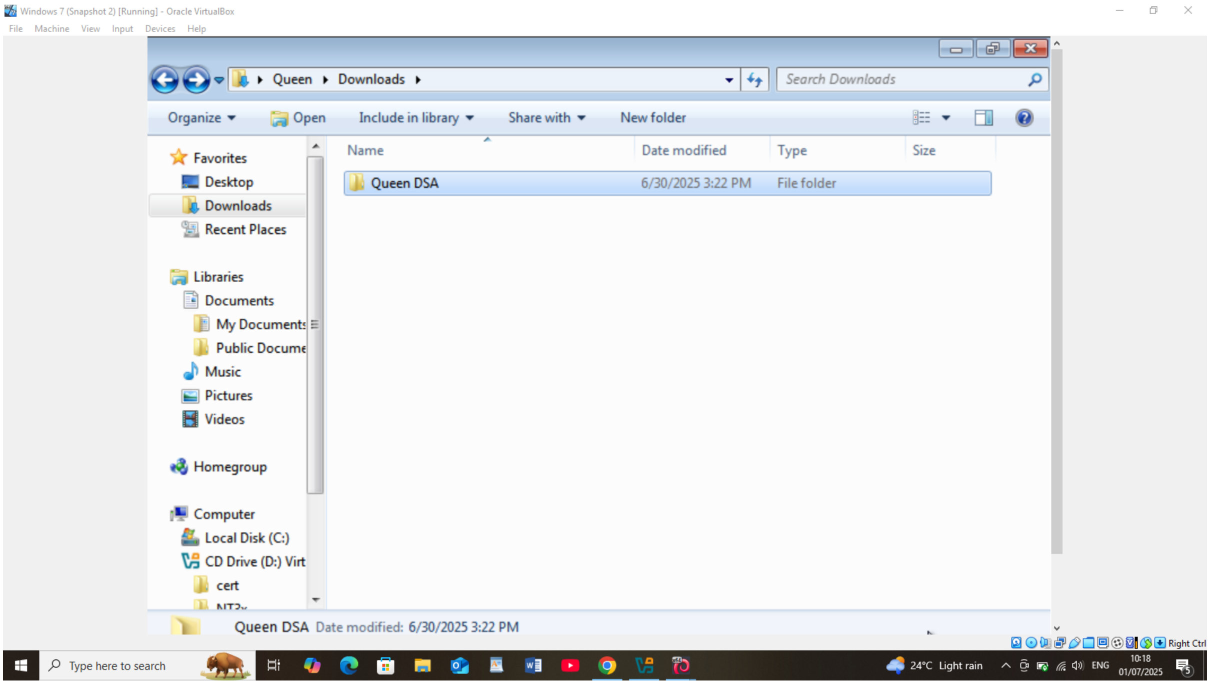
Autopsy Analysis



Extension Mismatch Detected 5 Results

Source Name	S	C	O	Source Type	Score	Conclusion	Configuration	Justification	Extension	MIME Type
00539a272af7101991d4a0a7d2a6c81791e8c741023e6			0	File	Likely Notable			File has MIME type of image/png	0	image/png
240715491ac0fc342ce3b579c68bed834ed678ca9e01			0	File	Likely Notable			File has MIME type of image/jpeg	0	image/jpeg
9480ddf1efba6127914562f530bc90fa8097e1daa32c9			0	File	Likely Notable			File has MIME type of image/jpeg	0	image/jpeg
9e4410e35d24e2e77ace5a4e4eb78ce3e0e32fbcfb7f3			0	File	Likely Notable			File has MIME type of image/jpeg	0	image/jpeg
a6511e539f6b03875a73739310646b09c332dc2da6b0			0	File	Likely Notable			File has MIME type of image/jpeg	0	image/jpeg

File paths



Name	Date modified	Type	Size
Queen DSA	6/30/2025 3:22 PM	File folder	

Queen DSA Date modified: 6/30/2025 3:22 PM

INVESTIGATOR

NAME : DEYINDE-PHILLIPS QUEEN OLUWAFADEKEMI

ROLE/TILE: DSA STUDENT CYBERSECURITY

DATE SIGNED: 03/07/2025