

Android Device Forensic Analysis Report

Project Title: DSA Android Case - DSA Final Project

Name: Agbeyangi Nathaniel

Date: July 04, 2025

1. Introduction

This report details the findings of a forensic investigation conducted on an Android mobile device for the DSA Android image forensic analysis. Android forensics involves the scientific examination and analysis of digital evidence from Android-powered devices to recover data, investigate incidents, and support legal proceedings. The purpose of this investigation is to identify and extract relevant digital artifacts, including communications, web activity, media files, and data files, to understand user behavior and potential illicit activities associated with the device.

2. Methodology

The forensic analysis was performed using Autopsy, an open-source digital forensics platform. The Android forensic image was ingested into Autopsy, and various ingest modules were enabled to automatically process and extract data.

The primary tool utilized for this forensic investigation was Autopsy (Version 4.22.1). The following step-by-step procedure was followed:

1. **Acquisition:** A logical acquisition of the Android device's file system was performed, resulting in a data source identified as "LogicalFileSet1".
2. **Ingestion and Analysis:** The acquired data was ingested into Autopsy. Job 1 for LogicalFileSet1 was completed, with the following modules enabled for analysis:
 - Recent Activity,
 - File Type Identification
 - Keyword Search
 - Interesting Files Identifier
 - Central Repository
 - PhotoRec Carver
 - Android Analyzer (aLEAPP)
 - Android Analyzer.
3. **Data Examination:** Detailed examination was conducted on categories such as:
 - Web History (12 entries)
 - Web Search activity (4 entries)
 - Web Cookies (207 entries)
 - Communications (SMS: 28 messages, Call Logs: 14 entries, Contacts: 7 entries, Communication Accounts: 21 entries, Phone Accounts: 18 entries, Device Accounts: 3 entries)

- Multimedia files (Images, Videos, and cached content, including 1 tagged image and 1 tagged file)
- System snapshots
- Installed Programs (5 applications)
- Deleted Files (0 entries)

4. Documentation: Significant findings were documented, and relevant screenshots were captured to support the observations and interpretations.

Steps Performed:

Case Creation: A new case was created in Autopsy, specifying the case name and base directory.

1. **Data Source Addition:** The provided Android forensic image (.img & .zip) was added as a data source.
2. **Data Ingestion and Processing:** Autopsy processed the image, extracting and indexing the data.
3. **Evidence Examination:** Extracted data was systematically reviewed within Autopsy's interface.
4. **Data Export:** Relevant findings were exported in formats such as CSV for further review and reporting.
5. **Report Generation:** Findings were compiled into this formal report, including screenshots and analysis.



















3. Findings (With Screenshots)

3.1. Device and Communication Overview

Description: The "Browse" and "Visualize" tabs within the Communications Visualization Editor provided an initial overview of the analyzed Android device, identified by the ID 7e315b29-e5ea-4e90-9ed8-e1184af9c187. The device contained 35 items overall. The report summary indicates 3 device accounts and 18 phone accounts. Several phone numbers were listed, with +971543777711 and 08032111133 each showing 14 associated items, indicating significant activity. The summary for the primary device indicated 28 messages, 0 call logs, and 0 media attachments, with a total of 0 attachments. Additionally, 7 book entries (contacts) were identified. The "Communication Accounts" view shows 21 accounts, split between 2 device accounts and 11 phone accounts. The "Device" view further specifies that contact2.db, mmssms.db, and LogicalFileSet1 are associated with device IDs. The "Phone" view lists 18 phone accounts, including various numbers and their associated data sources (contact2.db, mmssms.db, LogicalFileSet1).

Interpretation: This suggests that the primary mode of communication on this device leans heavily towards messaging applications rather than traditional voice calls. The presence of a contact list, albeit limited, confirms active interaction with stored contacts. The multiple communication accounts and phone entries highlight the complexity of tracking all communication channels and emphasize the importance of analyzing contact2.db and mmssms.db for comprehensive communication records.

Screenshot Reference:

Listing						
Table	Thumbnail	Summary				
Source Name	S	C	O	Account Type	ID	▼ Data Source
 contacts2.db			4	PHONE	08032111225	LogicalFileSet1
 contacts2.db			No comments found		+971543777711	LogicalFileSet1
 contacts2.db			4	PHONE	+971565505984	LogicalFileSet1
 contacts2.db			3	PHONE	08032111122	LogicalFileSet1
 contacts2.db			4	PHONE	08012345678	LogicalFileSet1
 contacts2.db			4	PHONE	08032111669	LogicalFileSet1
 contacts2.db			4	PHONE	08032111133	LogicalFileSet1
 mmssms.db			4	PHONE	08032111225	LogicalFileSet1
 mmssms.db			4	PHONE	08032111669	LogicalFileSet1
 mmssms.db			4	PHONE	08032111133	LogicalFileSet1
 mmssms.db			4	PHONE	+971543777711	LogicalFileSet1
 LogicalFileSet1			3	PHONE	+15555215554	LogicalFileSet1
 LogicalFileSet1			4	PHONE	+971565505984	LogicalFileSet1
 LogicalFileSet1			4	PHONE	08032111669	LogicalFileSet1
 LogicalFileSet1			4	PHONE	08032111225	LogicalFileSet1
 LogicalFileSet1			4	PHONE	08012345678	LogicalFileSet1
 LogicalFileSet1			4	PHONE	+971543777711	LogicalFileSet1
 LogicalFileSet1			4	PHONE	08032111133	LogicalFileSet1

3.2. Web Search Activity—Potential Scam Research

Description: An analysis of the "Web Search" listing revealed four distinct search queries originating from LogicalFileSet1. Two searches on 2024-03-17 at 03:39:59 WAT and 03:42:06 WAT were "new and latest investment scam format" and "How to avoid being caught by the EFCC," respectively, both conducted via <https://www.google.com/search?q=google.com> (Chrome Search Terms). More recent searches on 2025-06-30 at 15:50:33 WAT and 2025-07-01 at 16:57:04 WAT included terms related to "create new bitcoin w" (likely "create new bitcoin wallet" or similar, partially visible) and "create new bitcoin."

Interpretation: The search queries regarding "investment scam format" and evading the EFCC (Economic and Financial Crimes Commission) are highly suspicious. They strongly suggest the user may be either involved in or extensively researching fraudulent activities, potentially with

the intent to avoid detection by law enforcement. The latter searches for creating a new Bitcoin wallet, further indicating an interest in cryptocurrency, which is sometimes used in financial activities, including illicit ones. The repeated searches for Bitcoin wallet creation strengthen this interpretation.

Screenshot Reference:

Listing									
Web Search									
Table This is a DataResult window									
Source Name	S	C	O	Date Accessed	Text	Domain	Comment	Data Source	
LogicalFileSet1				2024-03-17 03:39:59 WAT	new and latest investment scam format	google.com	Chrome Search Terms	LogicalFileSet1	
LogicalFileSet1				2024-03-17 03:42:06 WAT	How to avoid being caught by the EFCC	google.com	Chrome Search Terms	LogicalFileSet1	
LogicalFileSet1				2025-07-05 05:28:22 WAT			Google Quick Search	LogicalFileSet1	
LogicalFileSet1				2025-07-05 05:28:23 WAT	"create new bi", "create new bitcoin w		Google Quick Search	LogicalFileSet1	

3.3. Web History—Scam and Evasion Attempts

Description: The "Web History" log presented 12 entries, predominantly from 2024-03-17. Numerous URLs from <https://www.google.com/search?q=google.com> and [nairaland.com](https://www.nairaland.com) contained search terms and visited pages such as "how to know if efcc is tracking you," "scared-being-arrested Scared Of Being Arrested By EFCC - Criminal," "new and latest investment scam format," "Fake investment website," and "how to avoid being caught by the EFCC." Additional entries included searches for "7 fake cryptocurrency investments" and "EFCC Devises Means Of Tracking."

Interpretation: This web history corroborates and intensifies the concerns raised by the web search activity. The user's extensive research into investment scams, methods to evade the EFCC, and details surrounding cryptocurrency investments point strongly towards an individual deeply involved in or studying fraudulent schemes and actively seeking ways to circumvent law enforcement.

Reference:

- Web History 2025074021728.csv (for full data)

Screenshot Reference:

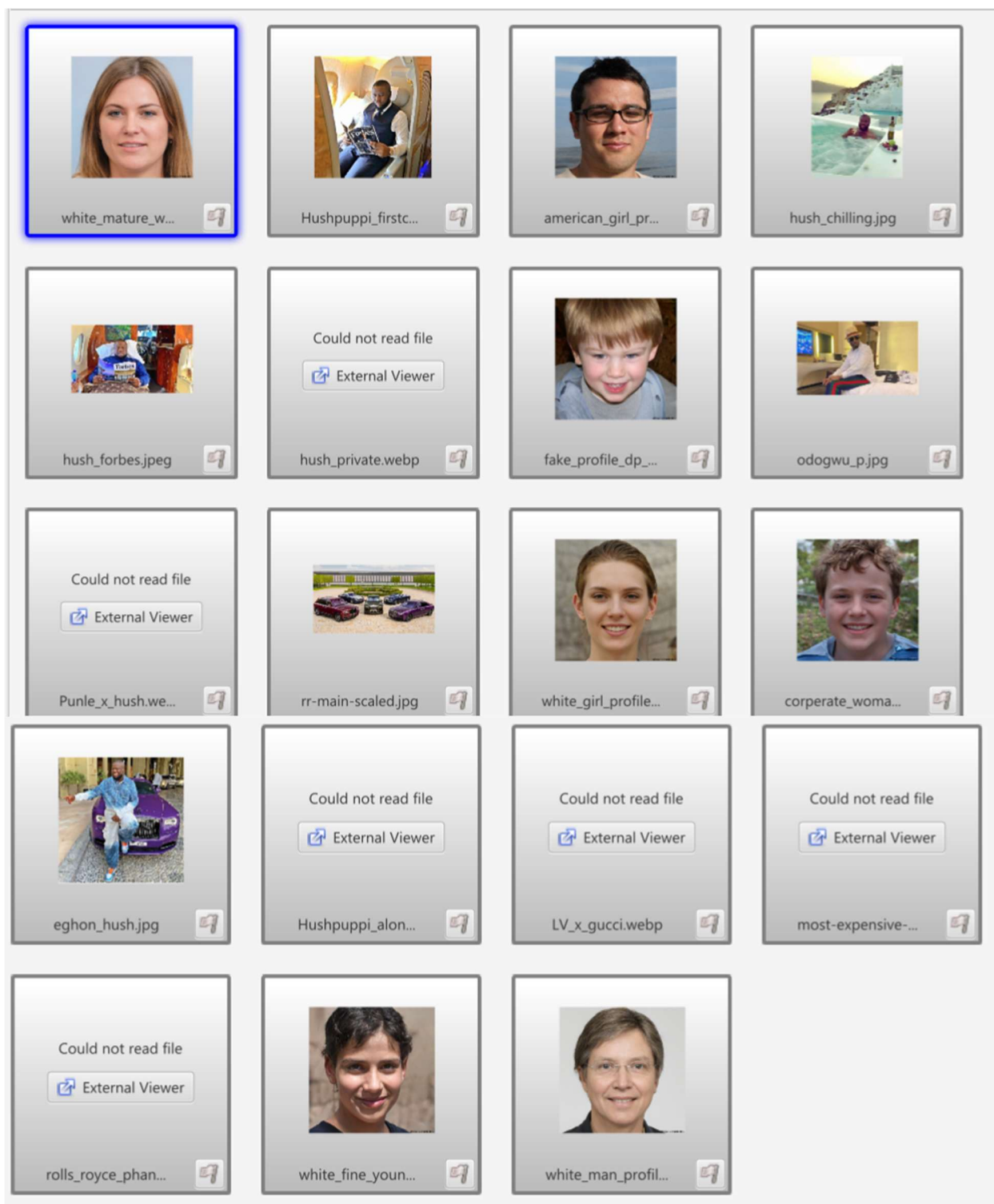
Listing									
Web History									
Table Thumbnail Summary									
Save Table									
Source Name	S	C	O	Date Created	Date Accessed	URL	Title	Comment	
LogicalFileSet1				2024-03-17 03:49:04 WAT	2024-03-17 03:49:04 WAT	https://www.google.com/search?client=ms-unknown&... how to know if efcc is tracking you - Google Search	how to know if efcc is tracking you - Google Search	Chrome Offline Pages	
LogicalFileSet1				2024-03-17 03:47:51 WAT	2024-03-17 03:47:51 WAT	https://www.nairaland.com/6982372/scared-being-arres Scared Of Being Arrested By EFCC - Crime - Nigeria	Scared Of Being Arrested By EFCC - Crime - Nigeria	Chrome Offline Pages	
LogicalFileSet1					2024-03-17 03:39:59 WAT	https://www.google.com/search?q=new+and+latest+in. new and latest investment scam format - Google Search	new and latest investment scam format - Google Search	Chrome History	
LogicalFileSet1					2024-03-17 03:40:47 WAT	https://www.google.com/search?client=ms-unknown&... Fake investment website - Google Search	Fake investment website - Google Search	Chrome History	
LogicalFileSet1					2024-03-17 03:40:55 WAT	https://www.google.com/url?q=https://businessday.ng/. Here are 7 fake cryptocurrency investment platforms on, Chrome History	Here are 7 fake cryptocurrency investment platforms on, Chrome History	Chrome History	
LogicalFileSet1					2024-03-17 03:40:55 WAT	https://businessday.ng/technology/article/here-are-7-fa Here are 7 fake cryptocurrency investment platforms on, Chrome History	Here are 7 fake cryptocurrency investment platforms on, Chrome History	Chrome History	
LogicalFileSet1					2024-03-17 03:42:06 WAT	https://www.google.com/search?q=How+to+avoid+b... How to avoid being caught by the EFCC - Google Searc.	How to avoid being caught by the EFCC - Google Searc.	Chrome History	
LogicalFileSet1					2024-03-17 03:42:59 WAT	https://www.google.com/url?q=https://www.nairaland... Scared Of Being Arrested By EFCC - Crime - Nigeria	Scared Of Being Arrested By EFCC - Crime - Nigeria	Chrome History	
LogicalFileSet1					2024-03-17 03:42:59 WAT	https://www.nairaland.com/6982372/scared-being-arres Scared Of Being Arrested By EFCC - Crime - Nigeria	Scared Of Being Arrested By EFCC - Crime - Nigeria	Chrome History	
LogicalFileSet1					2024-03-17 03:48:57 WAT	https://www.google.com/search?client=ms-unknown&... how to know if efcc is tracking you - Google Search	how to know if efcc is tracking you - Google Search	Chrome History	
LogicalFileSet1					2024-03-17 03:48:31 WAT	https://www.google.com/url?q=https://www.nairaland... EFCC Devises Discreet Means Of Tracking Yahoo Boys....	EFCC Devises Discreet Means Of Tracking Yahoo Boys....	Chrome History	
LogicalFileSet1					2024-03-17 03:48:51 WAT	https://www.nairaland.com/5033957/efcc-devises-discr... EFCC Devises Discreet Means Of Tracking Yahoo Boys....	EFCC Devises Discreet Means Of Tracking Yahoo Boys....	Chrome History	

3.4. Downloaded Images—Potential for Impersonation

Description: The "Image/Video Gallery" within the LogicalFileSet1/data/media/0/Download/ path contained 19 downloaded files. A prominent image displayed was "white_mature_woman_profile.jpeg," a portrait of a Caucasian woman. Other visible thumbnails included "eghion_hush.jpg" and "LV_x_gucci.webp."

Interpretation: The presence of a generic "profile picture" of a woman raises concerns about its potential use for creating fake social media profiles or for impersonation in various online scams, such as romance scams or investment frauds. The other downloaded images, while potentially innocuous, could also be used for similar purposes or for promoting luxury goods, which sometimes feature in scam narratives.

Screenshot Reference:



3.5. System Snapshots—Call Interface and Downloads View

Description: Within the LogicalFileSet1/data/system_ce/0/snapshots/ directory, 10 files were found. One snapshot, 34_reduced.jpg, depicted a call interface showing a contact named

"WoodBerry" with the number 08032111133 and a recent call from the same number. Another snapshot, 42_reduced.jpg, displayed a "Downloads" screen. showing several images, including faces and a car, consistent with some of the previously identified downloaded media.

Interpretation: The call interface snapshot confirms recent and active communication with the phone number 08032111133, which was also noted in the device's communication overview. This indicates ongoing interaction with this specific contact. The downloads snapshot provides insight into the user's view of their downloaded content, some of which could be instrumental in establishing fake identities or personas for fraudulent activities.

3.8. Call Logs

Description: The "Call Logs" listing shows 14 entries, primarily from 2024-03-16 and 2024-03-17. Several outgoing calls are recorded, including to numbers like +971565059984, 08032111225, 08012345678, 08032111169, and 08032111133. The metadata for each call log entry indicates the source as LogicalFileSet1_Host and the data source as LogicalFileSet1. The direction of the call is also specified (e.g., "Unknown" for some entries, implying it might be a general log or direction not explicitly captured).















Specific call log entries include:

- 2024-03-16 20:45:54 WAT: Call to +971565059984
- 2024-03-16 20:49:50 WAT: Call to 08032111169
- 2024-03-16 20:51:59 WAT: Call to 08032111225
- 2024-03-17 02:54:56 WAT: Call to 08032111169
- 2024-03-17 16:17:36 WAT: Call to 080321111225
- 2024-03-17 16:18:04 WAT: Call to 080321111225
- 2024-03-17 16:18:22 WAT: Call to 080321111225
- 2024-03-17 16:21:46 WAT: Call to 08012345678
- 2024-03-17 16:24:09 WAT: Call to 08032111169
- 2024-03-17 16:25:20 WAT: Call to +971543777711
- 2024-03-17 16:25:20 WAT: Call to 08032111133
- 2024-03-17 16:36:15 WAT: Call to 08032111169
- 2024-03-17 16:36:21 WAT: Call to 08032111169
- 2024-03-17 16:36:28 WAT: Call to 08032111169

Interpretation: The presence of call logs, particularly outgoing calls to various numbers, indicates direct voice communication from the device. These numbers should be cross-referenced with contacts and other communication data to identify the individuals involved and

the nature of these calls. The timestamps provide a timeline for these interactions, showing concentrated activity on March 17th, 2024, with repeated calls to 0803211169 and 08032111225, and single calls to +971565059984, 08012345678, and 08032111133.

Screenshot Reference:

Listing					
Call Logs					
Table Thumbnail Summary					
Source Name	S	C	O	Start Date/Time	Phone Number
 LogicalFileSet1			3	2024-03-16 20:45:54 WAT	+971565505984
 Logi <div>Source Name</div>			3	2024-03-16 20:49:50 WAT	08032111669
 LogicalFileSet1			3	2024-03-16 20:51:59 WAT	08032111225
 LogicalFileSet1			3	2024-03-17 02:54:56 WAT	08032111669
 LogicalFileSet1			3	2024-03-17 16:17:36 WAT	08032111225
 LogicalFileSet1			3	2024-03-17 16:18:04 WAT	08032111225
 LogicalFileSet1			3	2024-03-17 16:18:22 WAT	08032111225
 LogicalFileSet1			3	2024-03-17 16:21:46 WAT	08012345678
 LogicalFileSet1			3	2024-03-17 16:24:09 WAT	08032111669
 LogicalFileSet1			3	2024-03-17 16:23:25 WAT	+971543777711
 LogicalFileSet1			3	2024-03-17 16:25:20 WAT	08032111133
 LogicalFileSet1			3	2024-03-17 16:36:15 WAT	08032111669
 LogicalFileSet1			3	2024-03-17 16:36:21 WAT	08032111669
 LogicalFileSet1			3	2024-03-17 16:36:28 WAT	08032111669

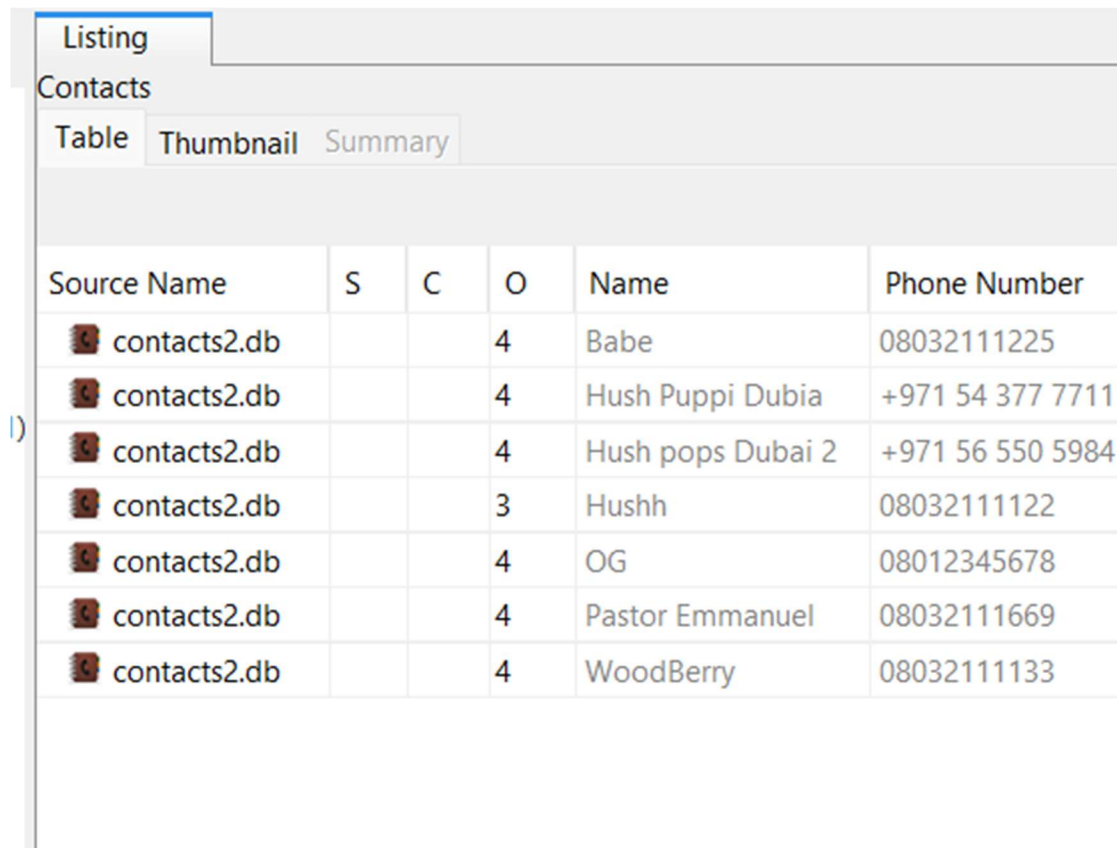
3.9. Contacts








Description: The "Contacts" view lists 7 entries, primarily sourced from contact2.db. These contacts include names like "Babe" (08032111225), "Hush Puppy Dubia" (+971543777711), "Hush pups Dubai 2" (+971 56 550 5984), "Hushh" (08032111122), "OG" (08012345678), "Pastor Emmanuel" (08032111169), and "WoodBerry" (08032111133). Each contact entry includes the phone number and indicates LogicalFileSet1 as the data source.

Interpretation: The contact list provides crucial identifying information for individuals the device user was in communication with. The names, particularly those with descriptive or

unusual monikers like "Hush Puppy Dubia" or "WoodBerry," could be significant. Cross-referencing these contacts with call logs, messages, and other data will help establish relationships and the context of their interactions.

Screenshot Reference:



Listing					
Contacts					
Table	Thumbnail	Summary			
Source Name	S	C	O	Name	Phone Number
 contacts2.db			4	Babe	08032111225
 contacts2.db			4	Hush Puppi Dubia	+971 54 377 7711
 contacts2.db			4	Hush pops Dubai 2	+971 56 550 5984
 contacts2.db			3	Hushh	08032111122
 contacts2.db			4	OG	08012345678
 contacts2.db			4	Pastor Emmanuel	08032111669
 contacts2.db			4	WoodBerry	08032111133

3.10. Installed Programs

Description: The "Installed Programs" listing shows 5 applications installed on the device, all from LogicalFileSet1. These include com.google.android.youtube (YouTube), com.squareup.cash (Cash App), com.twitter.android (Twitter), com.whatsapp (WhatsApp), and wallet.nat.applay.crypto (a cryptocurrency wallet application).

Interpretation: The installed applications provide insight into the user's activities and interests. The presence of com.squareup.cash (Cash App) and wallet.nat.applay.crypto (a cryptocurrency wallet application) is highly significant given the web search findings related to investment scams and Bitcoin. This strongly suggests the device was used for financial transactions, potentially involving cryptocurrency. YouTube, Twitter, and WhatsApp are common communication and media consumption platforms.

Screenshot Reference:

Listing						
Installed Programs						
Table	Thumbnail	Summary				
Source Name	S	C	O	Program Name	Comment	
LogicalFileSet1			3	com.google.android.youtube	Installed Apps GSM	
LogicalFileSet1			3	com.squareup.cash	Installed Apps GSM	
LogicalFileSet1			3	com.twitter.android	Installed Apps GSM	
LogicalFileSet1			3	com.whatsapp	Installed Apps GSM	
LogicalFileSet1			3	wallettrust.applpy.crypto	Installed Apps GSM	

3.11. Messages

Description: The "Messages" listing displays 28 Android messages, primarily from mmssms.db and dated 2024-03-17. These include both incoming and outgoing messages to numbers like 08032111225, 08032111169, 08032111133, and +971543777711. The messages indicate various timestamps throughout the day. Crucially, the content of some messages reveals highly suspicious activity:

- 2024-03-16 21:55:45 WAT (Outgoing from device to 08032111225): "Hi babe, how was your journey to Kaduna. I hope it wasn't stressful"
- 2024-03-17 04:09:45 WAT (Incoming from 08032111169 to device): "Calvary greetings brother Sam, I trust you are doing fine. It been about 6 months since you were last seen fellowshiping with us. I hope all is well, in this period of economic meltdown there is no better time to draw closer to God. May the good Lord keep us all from temptations. I hope to see you fellowship with the brethren come Sunday. The Lord be with you always my brother"
- 2024-03-17 04:10:17 WAT (Outgoing from device to 08032111169): "Thank you Pastor"
- 2024-03-17 04:19:10 WAT (Incoming from 08032111133 to device): "Hey, I've got a new scam idea. we need to discuss."
- 2024-03-17 04:19:54 WAT (Outgoing from device to 08032111133): "Sure, I'm in. What's the plan this time?"
- 2024-03-17 04:20:44 WAT (Incoming from 08032111133 to device): "Let's create a fake investment website and lure people into investing in a non-existent cryptocurrency. We'll promise huge returns."
- 2024-03-17 04:21:08 WAT (Outgoing from device to 08032111133): "Sounds good. Do you have the website?"

- 2024-03-17 04:24:00 WAT (Incoming from 08032111133 to device): "Yes, use the same Bitcoin wallet address as before: 16AtgJBaXL2kntzx4mW5ocpT2YsTWXmacWn."
- 2024-03-17 04:25:38 WAT (Outgoing from device to 08032111133): "I feel you man, I am in on this fully, but not high value client we go Target this time around I."
- 2024-03-17 04:29:53 WAT (Incoming from 08032111133 to device): "Sure, enough of this text messages. Meet me over Google Meet byt 10pm. Here is the meeting link: <https://meet.google.com/abcd-efgh-ijkl>"
- 2024-03-17 04:37:29 WAT (Outgoing from device to 08032111133): "Alright man, I go join wen time reach"
- 2024-03-17 05:26:00 WAT (Outgoing from device to +971543777711): "Hey Egbon, I've set up a new website for our next venture. Check it out: <https://apyeth.gifts/>"
- 2024-03-17 05:29:40 WAT (Incoming from +971543777711 to device): "Nice work, Sammy. I'll take a look at the site. Are we using the same tactics as before?"
- 2024-03-17 05:34:40 WAT (Outgoing from device to +971543777711): "Yes, but this time we're targeting investors with promises of exclusive access to a "revolutionary" crypto currency technology. The website layout is designed to mimic legitimacy, complete with fake testimonials and fabricated investment portfolios."
- 2024-03-17 05:35:36 WAT (Incoming from +971543777711 to device): "Sounds convincing. Payment gateway nkor? Are we still using the same Bitcoin wallet address?"
- 2024-03-17 05:43:19 WAT (Outgoing from device to +971543777711): "No, I've set up a new wallet address for this operation. Here it is: 1K1KMHPyhJHQRbhzKHyk6yaJuQUYxSaZCm"
- 2024-03-17 05:46:43 WAT (Incoming from +971543777711 to device): "Got it. I'll update the payment instructions on the website accordingly. When we dey go live?"
- 2024-03-17 05:46:59 WAT (Outgoing from device to +971543777711): "We'll lauch the website next week. In the meantime, spread the "good news" discreetly through our Network of affiliates and social media channels, telegram is very important. We want to create a buzz without attracting unwanted attention."
- 2024-03-17 05:49:17 WAT (Incoming from +971543777711 to device): "Undersood omo iya mi. I'll handle the promotional activities and monitor for any potential leaks. This one go be bang inshallah"

Interpretation: The presence of numerous messages, both incoming and outgoing, confirms active text-based communication. The content of these messages provides direct and compelling evidence of a planned fraudulent scheme. The discussions about creating a "fake investment website" (<https://apyeth.gifts/>), luring people into a "non-existent cryptocurrency," promising "huge returns," and using specific Bitcoin wallet addresses (e.g., 16AtgJBaXL2kntzx4mW5ocpT2YsTWXmacWn, 1K1KMHPyhJHQRbhzKHyk6yaJuQUYxSaZCm) are clear indicators of illicit activity. The mention of Google Meet for discussions, updating payment instructions on a website, handling promotional activities, and setting up new wallet addresses outlines a well-orchestrated scam operation. This is a critical finding that directly supports the suspicion of fraudulent behavior. The messages also indicate a coordinated effort with multiple individuals ("Sammy," "Egbon," "omo iya mi"). The presence of seemingly innocuous messages

like "Hi babe, how was your journey to Kaduna" and "Calvary greetings brother Sam" could be attempts to maintain a normal facade or are unrelated personal communications.

Screenshot Reference(from /screenshots/ in the directories):

- suspicious message 1.png
- suspicious message 2.png
- suspicious message 3.png
- suspicious message 4.png
- suspicious message 5.png
- suspicious message 6.png
- message view.png

3.12. Deleted Files

Description: The "Deleted Files" section shows that there are no deleted files found in the File System or All categories (0 entries each).

Interpretation: This indicates that no deleted files were recovered during the logical acquisition process. While this doesn't necessarily mean no files were ever deleted, it implies that standard recovery methods did not yield any deleted data from the file system. More advanced forensic techniques might be required to recover deleted data if deemed necessary for the investigation.

Screenshot Reference:

- deleted file.jpg

3.13. Web Cookies

Description: The "Web Cookies" listing shows 207 entries, primarily dated 2024-03-17. These cookies are associated with various domains, including google.com, and businessday.ng, adform.net, creativecdn.com, udistking.com, disqus.com, doubleclick.net, tempest.services.disqus.com, a-mo.net, and prerib.a-mo.net. Many cookies have generic names like NID, _ga, _gid, _fbclid, __cf_bm, _chartbeat, _cb_suref, _gads, _gcl_au, _gcl_aw, IDE, C, ts, jcsuid, DSID, trc_cookie_storage, disqus_unique, _jid, amuid2, and sd_amuid2.

Interpretation: The presence of a large number of web cookies indicates extensive browsing activity across various websites. Cookies from google.com are expected for general web usage. Cookies from businessday.ng suggest visits to a business news or finance-related website, which aligns with the investment scam theme. The other domains (adform.net, creativecdn.com, disqus.com, doubleclick.net, tempest.services.disqus.com, a-mo.net, prerib.a-mo.net) are often associated with advertising, analytics, content delivery networks, and comment systems, which are common across many websites. While individual cookies may not be directly incriminating, their collective presence provides a detailed footprint of the user's online behavior and visited sites, which could be further analyzed to identify patterns related to the suspected fraudulent activities.

4. Conclusion

The forensic examination of the Android device (LogicalFileSet1) provides direct and compelling evidence of user engagement in activities related to online fraud and deliberate efforts to evade law enforcement. The web search and browsing history are highly concerning, revealing repeated queries about investment scams, methods to avoid detection by the EFCC, and the creation of cryptocurrency wallets. Crucially, the content of messages explicitly details a planned fraudulent scheme involving a "fake investment website" (<https://apyeth.gifts/>), a "non-existent cryptocurrency," promises of "huge returns," and the use of specific Bitcoin wallet addresses. The presence of financial applications (Cash App, wallet.nat.apploy.crypto) on the device, combined with active communication (call logs, messages, contacts) with various individuals, further confirms the device was actively used for financial transactions and coordination of illicit activities. The downloaded images, including generic profile pictures, suggest the potential for establishing fake online personas or engaging in deceptive communications. The comprehensive web cookie data also provides a detailed footprint of the user's extensive online activity.

5. Recommendations

5.1. Security Tips

- **Public Awareness:** Educate individuals on common online scams, including investment and romance frauds, and guide how to identify and report them.
- **Legal Consequences:** Promote awareness about the severe legal consequences of engaging in fraudulent activities and the methods law enforcement uses to track such actions.
- **Digital Hygiene:** Encourage the consistent use of strong, unique passwords and the activation of two-factor authentication for all online accounts to enhance security.
- **Safe Browsing:** Advise against clicking on suspicious links, downloading files from untrusted sources, or interacting with unsolicited communications.

5.2. Data Handling Suggestions (for future forensic investigations)

- **Comprehensive Acquisition:** Whenever feasible, prioritize conducting a complete physical or full file system acquisition of mobile devices to ensure the most comprehensive data recovery, including potentially deleted files.
- **Targeted Analysis:** Focus on the in-depth analysis of messaging applications (e.g., WhatsApp, Telegram, SMS) and financial applications, as these are highly likely to contain direct evidence of fraudulent communications or transactions.
- **Cross-Referencing:** Systematically cross-reference findings from web activity (history, searches, cookies) with communication logs, messages, contacts, and application data to construct a more holistic understanding of the user's behavior and intent.
- **Advanced Analytics:** Utilize advanced forensic analytics tools and techniques to identify subtle patterns in communication, financial transactions, and digital footprints that might not be immediately apparent.
- **Content Review:** Conduct a thorough review of the content of messages and any recovered documents or media files for direct evidence of scamming activities or illicit transactions.
- **IP Address Tracing:** If possible, trace IP addresses associated with web activity and communication to identify geographical locations and potential network infrastructure used in the scheme.