DIGITAL FORENSIC INVESTIGATION REPORT

1. INTRODUCTION

This report presents the findings from a forensic analysis conducted on a digital Android image file, provided for educational purposes. The objective was to recover and analyze various digital artifacts such as SMS messages, call logs, browsing history, installed applications, deleted content, crypto wallet, images, contact lists and other user data to simulate a real-world mobile forensic investigation.

1.1. Case Details

- **Case Name:** DSA ANDROID FORENSIC INVESTIGATION PROJECT 2025
- **Case Number:** 123456AB
- **Examiner Name:** Helen Emem Ekanem
- **Examiner Phone:** 08033954410
- **Examiner Email:** helenekanem23@gmail.com
- **Notes:** Helen's android image forensic analysis

2. METHODOLOGY & TOOLS USED

Tool: Autopsy 4.22.1
Platform: Windows
Image File Analyzed: android_image.tar
Analysis Steps:

- Initiated a new case in Autopsy, providing case information and examiner details (as seen in **Case Name** and **Screenshot: Case Information**).
- Selected host option to "Generate new host name based on data source name" (as seen in screenshots: **Host Selection** and **Add Data Source - Select Host**).
- Added the android_image.tar as a data source (as seen in **Data Source Added**).
- Configured ingest modules, initially reviewing available options (as seen in **Screenshot named: Configure Ingest 1**) and then ensuring "Android Analyzer" was selected for comprehensive data extraction (as seen in **Screenshot: Configure Ingest**).
- Parsed and categorized artifacts via Autopsy's Built (as seen in **Screenshot: Data Artifacts Summary**).
- Examined individual components: messages, call logs, web activity, installed apps, cookies, deleted files, and images.
- Collected screenshots and documented significant artifacts.

3. ARTIFACTS RECOVERED

3.1. SMS Messages

Total Messages Found: 25 (as seen in **Screenshot: Messages Overview 1&2**)

- **Message 1:** "Calvary greetings brother Sam, I trust you are doing fine. It's 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 timeto 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" (Date: 2024-03-17 03:09:45 WAT, Phone Number: c8148deb-7ada-4bb9-aecb-55763dc8a631) - *Message 1.png*.
- **Message 2:** "Hey, I've got a new scam idea, we need to discuss." (Date: 2024-03-17 03:19:10 WAT, Phone Number: c8148deb-7ada-4bb9-aecb-55763dc8a631) – *See Message 2: Screenshot 23*
- **Message 3:** "Let's create a fake investment website and lure people into investing in a non-existent cryptocurrency. We'll promise huge returns." (Date: 2024-03-17 03:20:44 WAT, Phone Number: c8148deb-7ada-4bb9-aecb-55763dc8a631) - *Message 3.png: Screenshot 24*
- **Message 4:** "Yes, use the same Bitcoin wallet address as before: 16AG1bAVJkrmz4W5ovpCS7TywsTWMacWN." (Date: 2024-03-17 03:23:45 WAT, Phone Number: c8148deb-7ada-4bb9-aecb-55763dc8a631) - *See Message 4.png and Screenshot 25*
- **Message 5:** "Sure, enough of these text messages. Meet me over Google Meet byt 10pm. Here is the meeting link: https://meet.google.com/abcd-efgh-ijkl" (Date: 2024-03-17 03:29:45 WAT, Phone Number: c8148deb-7ada-4bb9-aecb-55763dc8a631) - *See Message 5.png*
- **Message 6:** "Nice work, Sammy. I'll take a look at the site. Are we using the same tactics as before?" (Date: 2024-03-17 04:29:40 WAT, Phone Number: +971543777711) - *See Message 6.png: Screenshot 27*
- **Message 7:** "Sounds convincing. Payment gateway nko? Are we still using the old one?" (Date: 2024-03-17 04:46:40 WAT, Phone Number: c8148deb-7ada-4bb9-aecb-55763dc8a631) - *See Message 7.png*
- **Message 8:** "Got it. I'll update the payment instructions on the website. Make sure the 'returns' look very attractive." (Date: 2024-03-17 04:48:57 WAT, Phone Number: c8148deb-7ada-4bb9-aecb-55763dc8a631) - *See Message 8.png*
- **Message 9:** "Understood omo iya mi. I'll handle the promotional activities and monitor for any potential leaks. This one go be bang Inshallah" (Date: 2024-03-17

04:48:57 WAT, Phone Number: +971543777711) - *See Message 9.png*

- **Message 10:** "Hi babe, how was your journey to Kaduna. I hope it wasn't stressfull!" (Date: 2024-03-16 21:05:46 WAT, from: 016a6d69-7d6f-4818-a524-d190646f18f8, to 08032111225) – *See Message 10*
- **Message 11:** "Thank you Pastor" (Date: 2024-03-17 04:10:17 WAT, from: 016a6d69-7d6f-4818-a524-d190646f18f8, to: 08032111669) - *See Screenshot 46: Message 11 and Screenshot 54: Message 11 (New) and Screenshot 62: Message 11 (Final)*
- **Message 12:** "Sure, I'm in. What's the plan this time?" (Date: 2024-03-17 04:19:54 WAT, from: 016a6d69-7d6f-4818-a524-d190646f18f8, to 08032111133) - *See Screenshot 47: Message 12*
- **Message 13:** "Sounds good. Do you have the website ready?" (Date: 2024-03-17 04:21:08 WAT, from: 016a6d69-7d6f-4818-a524-d190646f18f8, to 08032111133) - *See Screenshot 63: Messages 13*
- **Message 14:** "I feel you man, I am in on this fully, but not high value client we go Target this time around L." (Date: 2024-03-17 04:25:38 WAT, from: 016a6d69-7d6f-4818-a524-d190646f18f8, to: 08032111133) - *See Screenshot 48: Message 14*
- **Message 15:** "Alright man, I go join wen time reach" (Date: 2024-03-17 04:37:29 WAT, from: 016a6d69-7d6f-4818-a524-d190646f18f8, to: 08032111133) - *See Screenshot 49: Message 15*
- **Message 16:** "Hey Egbon, I've set up a new website for our next venture. Check it out: https://apyeth.gifts/" (Date: 2024-03-17 05:26:00 WAT, From: 016a6d69-7d6f-4818-a524-d190646f18f8, To: +971543777711) - *See Screenshot 50: Message 16*
- **Message 17:** "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." (Date: 2024-03-17 05:34:40 WAT, from: 016a6d69-7d6f-4818-a524-d190646f18f8, to +971543777711) - *See Screenshot 64: Message 17*
- **Message 18:** "No, I've set up a new wallet address for this operation. Here it is: 1K1KMHpyhH0RBh3QHyabJyaQ2VvSaZCm" (Date: 2024-03-17 05:43:19 WAT, from: 016a6d69-7d6f-4818-a524-d190646f18f8, to +971543777711) - *See Screenshot 65: Message 18*
- **Message 19:** "We'll launch 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." (Date: 2024-03-17 05:46:00 WAT, From: 016a6d69-7d6f-4818-a524-d190646f18f8, to: +971543777711) - *See Screenshot 66: Message 19.*

- **Note:** Some messages were repeated on the message log making it a total of 28 messages.

3.2. Call Logs

Total Calls Recovered: 14 (as seen in Data Artifacts 1.png, Screenshot 12: Data Artifacts Summary, Screenshot 34: Data Artifacts Overview and Screenshot 40: Data Artifacts Overview (Updated))
Notable Findings: (as seen in Call Logs 1.png, Call Log 1.png, Call Log 2.png, and Screenshot 35: Call Logs under Artifacts)

- Call +97156509084 on 2024-03-16 20:45:54 WAT
- Call 08032111669 on 2024-03-16 20:50:49 WAT
- Call 08032111225 on 2024-03-16 20:51:59 WAT
- Call 08032111669 on 2024-03-17 02:54:56 WAT
- Call 08032111225 on 2024-03-17 16:17:36 WAT
- Call 08032111225 on 2024-03-17 16:18:04 WAT
- Call 08032111225 on 2024-03-17 16:18:22 WAT
- Call 08012345678 on 2024-03-17 16:21:46 WAT
- Call 08032111225 on 2024-03-17 16:24:09 WAT
- Call +971543777711 on 2024-03-17 16:25:34 WAT
- Call 08032111133 on 2024-03-17 16:26:20 WAT
- Call 08032111669 on 2024-03-17 16:36:15 WAT
- Call 08032111669 on 2024-03-17 16:36:21 WAT
- Call 08032111669 on 2024-03-17 16:36:28 WAT

3.3. Communication Accounts

Accounts Found: 21 (as seen in **Screenshot 40: Data Artifacts Overview (Updated)**)

- **Device IDs:** cd148deb-7ada-4bb9-aecb-55763dc8a631 (as seen in **Device 1.png** and **Screenshot 14: Device Communication Account**), 016a6d69-7d6f-4818-a524-d190646f18f8 (from contacts2.db and mmssms.db) - *See Screenshot 42: Devices and Screenshot 52: Devices (New)*
- **Phone Numbers:** 18 total (as seen in **Screenshot 51: Phones**)
  - 08032111225 (Source: contacts2.db)
  - +971543777711 (Source: contacts2.db)
  - 08032111122 (Source: contacts2.db)

  - 08012345678 (Source: contacts2.db)
  - 08032111669 (Source: contacts2.db)
  - 08032111225 (Source: mmssms.db)
  - 08032111669 (Source: mmssms.db)
  - 08032111133 (Source: mmssms.db)
  - +1555315554 (Source: LogicalFileSet1)
  - +97156509084 (Source: LogicalFileSet1)
  - 08032111669 (Source: LogicalFileSet1)
  - 08032111225 (Source: LogicalFileSet1)
  - 08012345678 (Source: LogicalFileSet1)
  - +971543777711 (Source: LogicalFileSet1)
  - 08032111133 (Source: LogicalFileSet1)

3.4. Web Browser History

Total Records: 12 (as seen in Data Artifacts 1.png, Screenshot 12: Data Artifacts Summary, and Screenshot 34: Data Artifacts Overview and Screenshot 40: Data Artifacts Overview (Updated))
Notable Findings: (as seen in Screenshot 2: Browser History Findings and Web History 8.png)

1. **Search Term:** "how to know if efcc is tracking you"
   - **Accessed:** 2024-03-17 03:49:04 WAT
   - **Source:** Google Search
   - **URL:** https://www.google.com/search?client=ms-unknown...
2. **Visited:** Nairaland forum post titled 'Scared Of Being Arrested By EFCC'
   - **Accessed:** 2024-03-17 03:47:51 WAT
   - **URL:** https://www.nairaland.com/9982372/scared-being-arr...
3. **Visited:** Page discussing investment scams
   - **Accessed:** 2024-03-17 03:40:47 WAT
   - **URL:** https://www.google.com/url?q=https://businessday.n...
4. **Visited:** "7 fake cryptocurrency investment platforms..."
   - **Accessed:** 2024-03-17 03:40:55 WAT
   - **URL:** https://businessday.ng/technology/article/here-are-7...
5. **Search Term:** "how to avoid being caught by EFCC"
   - **Accessed:** 2024-03-17 03:42:06 WAT
   - **Source:** Google Search
   - **URL:** https://www.google.com/search?q=how+to+avoid+...
6. **Visited:** "EFCC Devices Discreet Means Of Tracking Yahoo Boys..."
   - **Accessed:** 2024-03-17 03:48:51 WAT
   - **URL:** https://www.google.com/url?q=https://www.nairalan...

3.5. Web Cookies

Cookies Found: 207 (as seen in **Data Artifacts 1.png**, **Screenshot 12: Data Artifacts Summary**, and **Screenshot 34: Data Artifacts Overview** and **Screenshot 40: Data Artifacts Overview (Updated)**)

3.6. Web Searches

Searches Found: 4 (as seen in Data Artifacts 1.png, Screenshot 12: Data Artifacts Summary, Web Search.png, and Screenshot 31: Web Search Details and Screenshot 40: Data Artifacts Overview (Updated))
Notable Findings:

1. "new and latest investment scam format" - Accessed: 2024-03-17 03:39:59 WAT (Source: https://www.google.com/search?q=google.com, Comment: Chrome Search Terms)
2. "how to avoid being caught by the EFCC" - Accessed: 2024-03-17 03:42:06 WAT (Source: https://www.google.com/search?q=google.com, Comment: Chrome Search Terms)
3. ""create new bit" "create new bitcoin"" - Accessed: 2024-03-17 04:38:00 WAT (Source: Google Quick Search)
4. ""create new bit" "create new bitcoin"" - Accessed: 2024-03-17 04:38:00 WAT (Source: Google Quick Search)

3.7. Installed Programs

Total Applications Identified: 5 (as seen in **Data Artifacts 1.png**, **Installed Programs 1.png**, **Phone.png**, and **Screenshot 17: Installed Programs List** and **Screenshot 40: Data Artifacts Overview (Updated)**)

- com.google.android.youtube (YouTube)
- com.squareup.cash (Cash App)
- com.twitter.android (Twitter)
- com.whatsapp (WhatsApp)
- wallettrust.appley.crypto (Cryptocurrency Wallet App)

3.8. Deleted Files

Deleted Files Recovered: Metadata present, no content files visible (as seen in **Screenshot 3: Deleted Files Metadata**, **deleted files 1.png**, and **Screenshot 13: Deleted Files View**). File types by extension were also identified (as seen in **File by Extension 1.png**, **File Type 1.png, Screenshot 15: File Types by Extension**, and **Screenshot 16: File Types Overview**).

3.9. Images

Total Images Found: 19 (as seen in Image 7.jpg and Screenshot 28: Image 1.png)
Notable Findings:

- Several wallpapers (e.g., dark-themed thumbnails) (as seen in **Screenshot 28: Image 1.png**)
- odogmu_jp.jpg (a person in a hat sitting on a bed) (as seen in **Image 7.jpg**)
- hushpuppi_firstclass.jpg (a person holding a Forbes magazine in what appears to be a first-class cabin) (as seen in **Image 5.jpg** and **Screenshot 29: Image 5.jpg**)
- hush_forbes.jpeg (another image of a person holding a Forbes magazine) (as seen in **Image 6.jpg** and **Screenshot 30: Image 6.jpg**)

3.10. Archives

Total Archives Found: 1 (as seen in **Screenshot 33: Archives by File Extension**)

- android_image.tar (Size: 712965024, Location: /LogicalFileSet)

3.11. Contacts

Total Contacts Found: 7 (as seen in Screenshot 40: Data Artifacts Overview (Updated) and Screenshot 41: Contact Lists)
Notable Findings:

- Babe: 08032111225
- Hush Puppi Dubia: +971 54 377 7711
- Hush pops Dubai 2: +971 56 390 5984
- Hushh: 08032111225
- OG: 08012345678
- Pastor Emmanuel: 08032111669
- WoodBerry: 08032111133

3.12. Keyword Hits

Total Keyword Hits Found: 528 (as seen in Screenshot 40: Data Artifacts Overview (Updated) and Screenshot 43: Keyword Hints)
Notable Findings:

- Single Literal Keyword Search: 0
- Single Regular Expression Search: 0
- Email Addresses: 528

3.13. Score

Total Score Items: 81 Suspicious Items (as seen in Screenshot 55: Score Overview and Screenshot 56: Suspicious Items No. 1, Screenshot 57: Suspicious Items No 2, Screenshot 58: Suspicious Items No.3, Screenshot 59: Suspicious Items No.4)

Notable Findings:

- **Bad Items:** 0
- **Suspicious Items:** 81, including various system files, application-related files (e.g., base.apk, base.odex for com.squareup.cash, com.twitter.android, com.whatsapp, wallettrust.appley.crypto), and other miscellaneous files.

4. KEY FINDINGS

- **Suspicious Searches:** The device user was concerned about government surveillance, as evidenced by searches like "how to know if efcc is tracking you" and "how to avoid being caught by EFCC". There are also searches related to creating new cryptocurrency.
- **Active Communication Activity:** A significant number of SMS messages (33 total), call logs (14 total), cookies (207 total), and communication accounts (21 total) point to regular communication. The communication accounts include multiple phone numbers and device IDs, with a total of 18 phone numbers identified.
- **Web Activity Shows Behavioral Insight:** The user browsed forums related to fear of arrest and investment scams. This, combined with the suspicious searches, suggests potential involvement in or concern about illicit activities.
- **SMS Messages Indicate Scam Activity:** Several SMS messages explicitly discuss creating a "fake investment website" to "lure people into investing in a non-existent cryptocurrency" and handling "promotional activities" for this scheme. From the findings, it must be noted that WoodBerry, who is Sam's partner, initiated the scam idea as seen in the screenshot titled Message 1. One of the messages mentions "monitoring for any potential leaks." The messages also reveal a Bitcoin wallet address and a Google Meet link, indicating active coordination. New messages further detail conversations related to travel, plans, and a new website for a "next venture" (https://apyeth.gifts/), and explicitly mention targeting investors with "revolutionary" crypto currency technology and setting up a new wallet address for the operation.
- **Presence of Cryptocurrency Wallet App:** The discovery of wallettrust.appley.crypto directly contradicts the initial assessment of "No Direct Evidence of Cryptocurrency Wallets." This strongly suggests the user has a cryptocurrency wallet installed on the device, which is highly relevant to the suspected scam activity.
- **Image Artifacts Provide Context:** The recovered images, particularly those featuring a person holding a Forbes magazine (potentially "Hushpuppi" given the

filenames), could be significant for identifying the user or associating them with a public persona, especially if the individual is known for illicit financial activities.

- **Detailed Contact List:** The presence of a detailed contact list with names like "Hush Puppi Dubia" and "WoodBerry" further strengthens the potential link to individuals known for financial crimes.
- **Numerous Email Addresses in Keyword Hits:** The high number of email addresses found in keyword hits (528) suggest extensive online communication or data related to email accounts, which could be a rich source of further evidence.
- **Suspicious Items Identified:** Autopsy flagged 81 suspicious items, including various application and system files, which warrant further investigation to determine their nature and relevance to any illicit activities.

5. CONCLUSION

The forensic analysis of android_image.tar revealed significant user activity including web searches, call history, SMS messages, installed applications, images, contacts, keyword hits, and suspicious items. The browser history, in particular, suggested anxiety regarding potential monitoring or criminal investigation. Crucially, the recovered SMS messages provide direct evidence of planning and executing a cryptocurrency investment scam, including details about a Bitcoin wallet, meeting coordination, and a new website (https://apyeth.gifts/). The discovery of the wallettrust.appley.crypto application further strengthens the evidence of involvement in fraudulent activities related to cryptocurrency. The presence of specific images and a detailed contact list, potentially linked to known public figures involved in financial crimes, adds another layer of contextual information that warrants further investigation. The numerous email addresses found also indicate a broad scope of digital communication. The identification of suspicious items by Autopsy further highlights areas requiring deeper analysis.

6. RECOMMENDATIONS

- **Corroborate with SIM/Network Data:** To trace call logs and messaging patterns, cross-reference with SIM card and network provider data.
- **Keyword Search of Recovered Messages:** Conduct a more extensive keyword search of all recovered messages for sensitive phrases (e.g., 'EFCC', 'scam', 'Bitcoin', 'investment', 'crypto', 'payment gateway', 'returns', 'Google Meet', 'apyeth.gifts').
- **Export Full Browser and App Logs:** Export and analyze full browser history and

application logs for deeper behavioral profiling and to uncover any hidden or encrypted data.

- **Apply Mobile-Specific Parsing Tools:** Utilize advanced mobile forensic tools like Cellebrite or MOBILedit for more comprehensive app data extraction, especially for inaccessible app data.
- **Hash and Archive Image Securely:** Ensure the forensic image is hashed and archived securely to maintain its integrity for future re-analysis or presentation in legal proceedings.
- **Investigate Bitcoin Wallet Address:** The Bitcoin wallet address found in the SMS messages should be investigated further to trace transactions and associated entities.
- **Investigate Google Meet Link:** The Google Meet link should be investigated for any associated calendar entries or participant information, if possible.
- **Forensic Analysis of Cryptocurrency Wallet App:** A dedicated forensic analysis of the wallettrust.appley.crypto application data should be performed to extract wallet details, transaction history, and any associated accounts.
- **Image Analysis and Identification:** Further analyze the recovered images, especially those with identifiable individuals or specific filenames (e.g., "hushpuppi"), to confirm identities and potential links to known individuals or ongoing investigations.
- **Contact List Cross-Referencing:** Cross-reference the recovered contact list with known associates or individuals of interest in related investigations.
- **Email Address Analysis:** Analyze the 528 identified email addresses for patterns, communication, and potential links to other accounts or activities.
- **Website Investigation:** Investigate the newly discovered website https://apyeth.gifts/ for its content, registration details, and any associated infrastructure.
- **Suspicious Items Analysis:** Conduct a detailed analysis of the 81 flagged suspicious items to determine their nature, origin, and potential malicious intent or relevance to the suspected illicit activities.

7. APPENDIX: SCREENSHOTS

Overview of Autopsy Interface

[Overview of Autopsy Interface] (uploaded: Logical File Set 1.png-5945fa42-65d9-4c04-986c-f8232fa25b03)

Browser History Findings

[Browser History Findings] (uploaded: Web History 0.png-81b72877-3365-4fb1-8926-1154052032c1)

Deleted Files Metadata

[Deleted Files Metadata] (uploaded: File View 1.png-ff83242e-5983-4eec-96dd-bd1ca0497b6c)

Message 4

[Message 4] (uploaded: Message 4.png-72a47e89-7e76-4901-b49c-b0fc64c34aa7)

Message 5

[Message 5] (uploaded: Message 5.png-6fce8c6d-c99b-4fc5-9229-e1fbf430ec96)

Message 6

[Message 6] (uploaded: Message 6.png-6fa35ba2-e9ef-42a0-a4c3-8655affd42cb)

Message 7

[Message 7] (uploaded: Message 7.png-c2f16076-cb64-4200-9891-b8f06e7845b7)

Messages Overview 1&2

[Messages Overview 1&2] (uploaded: Messages 0.png-6806865b-ed81-4320-976f-8adf7d203bf8)

Web History Detail

[Web History Detail] (uploaded: Web History 8.png-3f336a67-76ca-4111-b840-2dfe5c2ca861)

Data Source Added

[Data Source Added] (uploaded: Data Source 1.png-62306392-c2e2-4d9e-8a94-1c6f696ef202)

Configure Ingest

[Configure Ingest] (uploaded: Configuration Ingest 2.png-b21c8a68-5545-4485-b785-beba6135a46d)

Data Artifacts Summary

[Data Artifacts Summary] (uploaded: Data Artifacts 1.png-4c885469-6f13-4326-968f-4e31ab115894)

Deleted Files View

[Deleted Files View] (uploaded: deleted files 1.png-cab08114-01ec-4b27-9b49-115e331e70bc)

Device Communication Account

[Device Communication Account] (uploaded: Device 1.png-9b73b1a0-3c69-4a10-bd88-b69bd8ac5e35)

File Types by Extension

[File Types by Extension] (uploaded: File by Extension 1.png-5ae2cf68-e2d7-42d7-9b33-48463c9649ef)

File Types Overview

[File Types Overview] (uploaded: File Type 1.png-571304df-4344-41a5-bf2a-dd81cb393d90)

Installed Programs List

[Installed Programs List] (uploaded: Installed Programs 1.png-bfc5255d-b1b5-4b83-b0d9-2d490694d74d)

Case Name

[Case Name] (uploaded: Case Name.png-f0bb7dde-4cf0-450d-a3b7-c89f9c97ccba)

Case Information

[Case Information] (uploaded: Case Information.png-077e8f1b-070a-4bb9-9be2-1e02085a4182)

Configure Ingest 1

[Configure Ingest 1] (uploaded: configuration Ingest 1.png-ef688d60-e98f-4b1e-a9de-e84650da89cf)

Host Selection

[Host Selection] (uploaded: Host Selection.png-eee48112-3eb6-443f-a016-

e95bf8bd4f79)

Message 1

[Message1] (uploaded: Message 1.png-d6504db4-618c-4f69-8447-ad6131a4b708)

Message 2

[Message 2] (uploaded: Message 2.png-94b109ed-1963-451b-905d-900b130398a7)

Message 3

[Message 3] (uploaded: Message 3.png-468fbc05-c4e0-4d08-a406-f8195d5d3b12)

Message 4

[Message 4] (uploaded: Message 4.png-a18eaeb4-f8cb-47d5-ba0b-455ffd45d10e)

Message 5

[Message 5] (uploaded: Message 5.png-5e0982cf-910b-4a1f-a687-2557d805fb63)

Message 6

[Message 6] (uploaded: Message 6.png-dcad6fd2-ef15-4ae4-88b0-d948b20977ff)

Image 1.png

[Image 1.png] (uploaded: Image 1.png-8c438b1f-f360-4b8f-8edc-222e63a44049)

Image 5.jpg

[Image 5.jpg] (uploaded: Image 5.jpg-d465874d-5bd5-4de8-b5a0-4fd3dcbeeff3)

Image 6.jpg

[Image 6.jpg] (uploaded: Image 6.jpg-78d25ee8-1627-4690-a112-b7ad596bcea0)

Web Search Details

[Web Search Details] (uploaded: Web Search.png-1e066f31-ac79-41b9-9649-5214f83bd38b)

Add Data Source

[Add Data Source - Select Host] (uploaded: Add Data Source 1.png-254bcd18-cf79-4db4-b850-1a82ba773074)

Archives by File Extension

[Archives by File Extension] (uploaded: Archives by File Extension.png-3c8f65ad-18b8-4738-b2c2-6c4a84ed3bd9)

Call Logs under Artifacts

[Call Logs under Artifacts] (uploaded: Call Logs under Artifacts.png-06b73091-943f-455a-8bbc-b3ae32e3b83d)

Case Information (New)

[Case Information] (uploaded: Case Information.png-e05ad25b-bc60-4bc4-b054-ea1830ca756d)

Call Log 1 Detail

[Call Log 1 Detail] (uploaded: Call Log 1.png-67136f03-c064-4d69-b0fb-aec686bbe8ed)

Call Log 2 Detail

[Call Log 2 Detail] (uploaded: Log 2.png-f147a7b9-09b5-42dd-af7e-6d64927e8f87)

Call Logs List

[Call Logs List] (uploaded: Call Logs 1.png-3b6ada18-3a2b-44bc-a4f7-ce1a7baca6bc)

Data Artifacts Overview

Contact Lists

[Contact Lists] (uploaded: Contact lists.png-44b307e0-5e69-42b0-89c0-6bb5d83cd857)

Devices

Keyword Hints

[Keyword Hints] (uploaded: Keyword Hints.png-f97e7016-a7d0-4827-b28c-ce36130d326d)

Message 10

[Message 10] (uploaded: Message 10.png-38ec65e5-449e-46c3-b8cd-

65f71e058c39)

Message 11

[Message 11] (uploaded: Message 11.png-6c2c9e85-bfbd-44f4-b381-4231a4aaa107)

Message 12

[Message 12] (uploaded: Message 12.png-0fff519e-a454-4366-90d0-bf91f7340ae7)

Message 14

[Message 14] (uploaded: Message 14.png-a2629e98-04d9-4534-b00f-5f1b10bcfe40)

Message 15

[Message 15] (uploaded: Message 15.png-6ad692eb-418e-485a-a128-0cef07a7de10)

Message 16

[Message 16] (uploaded: Message 16.png-ce69ed36-26d7-4447-bfcf-4c4b4763d925)

Suspicious Items No. 1

[Suspicious Items No. 1] (uploaded: Suspicious Items No. 1.png-d40483ec-e9c9-41f1-9049-640a600336e9)

Suspicious Items No 2

[Suspicious Items No 2] (uploaded: Suspicious Items No 2.png-acc0b24e-d173-49e6-8a25-e484666a91f9)

Suspicious Items No.3

[Suspicious Items No.3] (uploaded: Suspicious Items No.3.png-6e925643-0bf4-40ef-9dba-d0af0e75765a)

Suspicious Items No.4

[Suspicious Items No.4] (uploaded: Suspicious Items No.4.png-85ad7e44-19f5-4e5f-9a51-7644be9dd07a)

Messages 13

[Messages 13] (uploaded: Messages 13.png-7510007c-79a6-460b-b364-34c40c2

Message 18

[Message 18] (uploaded: Message 18.png-b5294404-d263-4ee7-a374-1f625662b91b)

Message 19

[Message 19] (uploaded: Message 19.png-58e20e10-9f75-4021-b1cf-817169dc1b97)