DIGITAL FORENSIC ANALYSIS OF THE PROVIDED ANDROID IMAGE

FOR THE

FINAL CAPSTONE PROJECT – DSA/CYBERSECURIY/2025

Peter Chukwuebuka Uzoukwu
DSA-Cyber security Student
cyberpeter6@gmail.com
+2347041543306

Digital Forensics Investigation Report

Case Title: Forensic analysis of the Android image
Case Number: DSA-CYBERSECURITY-2025
Date of Investigation: June 20-29, 2025
Investigator Name: Peter Chukwuebuka Uzoukwu, Cyber Security Student (DSA)
Client: INCUBATOR HUB (DIGITAL SKILL-UP AFRICA – DSA)

1. INTRODUCTION

This report outlines the findings of an investigation into a series of cybercrimes. These crimes involved fraudulent emails, unsolicited phone calls, and fake online investment websites, all designed to unlawfully steal personal information and financial assets from unsuspecting people.

The investigation shows that beginning on or around March 17, 2024, and continuing through that month within Nigeria, the suspect intentionally created a fraudulent investment platform. This was done to deceive victims into putting money into a non-existent business. It was also discovered that the suspect has a long history of committing similar cybercrimes involving email, phone, and investment scams.

This document serves to support a criminal complaint and an arrest warrant for SAMUEL JACKSON LIVISTONE, who also uses the names "SAM" and "Sammy." He is being charged with violating Nigeria's Cybercrime laws for conspiring to commit fraud through a fake online investment platform.

The facts in this report are based on my personal work on this case, my review of related documents, my professional training and experience, and information provided by other agents, law enforcement personnel, and witnesses. The report's goal is to demonstrate that there is enough probable cause to issue the complaint and arrest warrant, and it does not contain every detail of the government's investigation. Unless otherwise noted, all conversations are reported in summary, and all dates and monetary values are approximate.

2. SCOPE OF THE INVESTIGATION

- Extract and document:
- SMS messages, call logs, contact lists
- Application usage history
- Files, images, browser history, crypto wallets, deleted content
- Generate a comprehensive Forensics Investigation Report including:
- Methodology and tools used
- Screenshots and findings
- Conclusion and professional recommendations

3. METHODOLOGY AND TOOLS USED

3.1 Methodology

The investigation followed the standard digital forensic process:

- **Identification** – Determining potential sources of evidence.
- **Preservation** – Acquiring forensic images and archiving in a safe storage device to maintain evidence integrity.
- **Analysis** – Examining SMS messages, call logs, contact list, application usage history, files, images, browser history, crypto wallet, deleted contents.
- **Documentation** – Recording findings and maintaining chain-of-custody.
- **Presentation** – Creating a detailed report with conclusions and recommendations.

3.2 Tools Used

Tool	Purpose
• Autopsy/Sleuth Kit imaging.	File system analysis, keyword search, and

4. EVIDENCE SUMMARY AND FINDINGS

4.1 Devices Investigated

Device	Description	Serial No.	Acquisition Date
• Android Image	Provided Android Image	Android Image.tar.gz	June 22, 2025, 12am

5. FINDINGS

SAMUEL JACKSON LIVISTONE, a Nigerian citizen living in Nigeria, is believed to fund his lavish lifestyle through criminal activities. Our investigation identifies him as a leader within an international criminal network responsible for cybercrimes and fraudulent activities, including Business Email Compromise (BEC) schemes. This network targets victims globally, with the goal of stealing hundreds of millions of dollars. LIVISTONE, also known as "SAMMY," executed these frauds and laundered the proceeds with multiple partners, including two individuals referred to as Coconspirator 1 and Coconspirator 2.

This report highlights several fraudulent operations involving SAMMY. Evidence from messages on SAMMY's Android phone shows that he, along with Coconspirator 1 and Coconspirator 2, successfully defrauded victims of thousands of dollars and other currencies. Furthermore, separate communications between SAMMY and Coconspirator 1 reveal a conspiracy to launder significantly larger amounts—tens and sometimes hundreds of millions of dollars—which were the profits from other cybercrimes and intrusions.

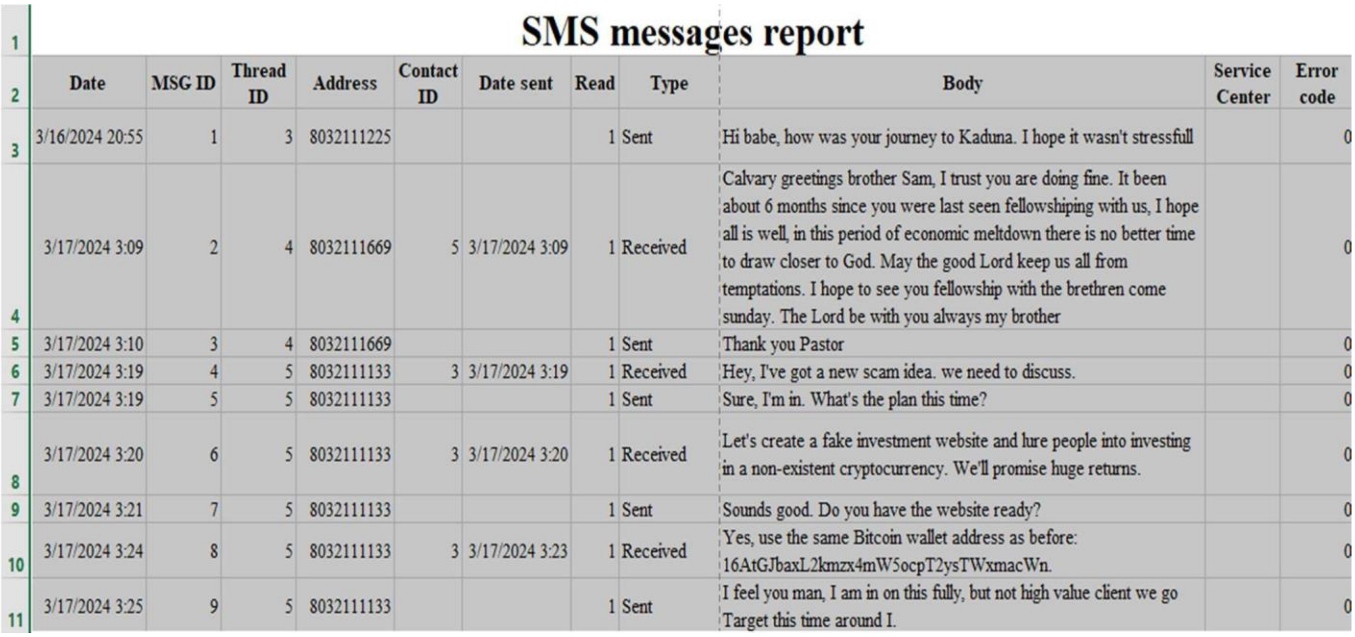
Analysis of the Android phone and online accounts of Coconspirator 1 showed that he was responsible for managing "money mule" teams for various scams. This analysis also confirmed that Coconspirator 1 used the Nigerian phone number +2348032111669 (referred to as "Phone Number 1") to discuss multiple fraudulent schemes and money laundering activities. Further investigation has established that "Phone Number 1" was one of the numbers used by SAMMY during 2024 and 2025.

This connection is confirmed by the contents of Coconspirator 1's Android phone, which listed Phone Number 1 (+2348032111669) under the contact name "Sam." The phone also held a URL (https://apyeth.gifts/) for a fraudulent website associated with "Sam's" co-conspirators. A search of the device uncovered messaging conversations between Coconspirator 1 and "Sam" (using Phone Number 1) discussing their criminal operations.

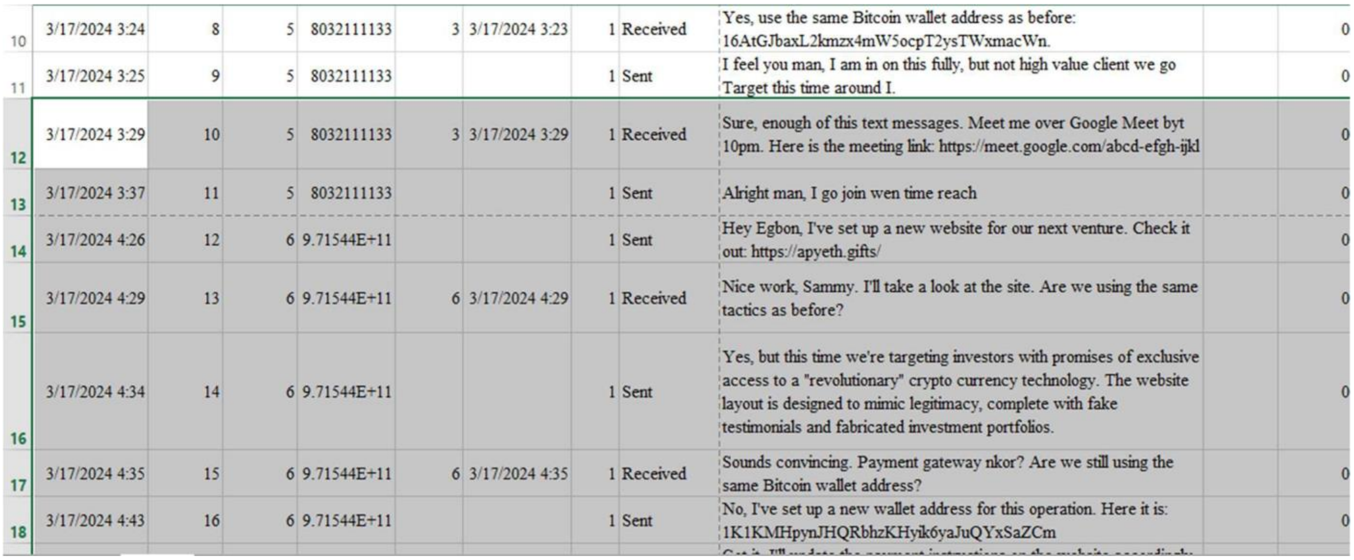
6. SCREENSHOTS (EVIDENCE OF CRIME COMMITTED)

Below are excerpt/screenshot of evidence (Exhibit A) from his Android Phone with his co- conspirator (Conspirator 1 & 2);

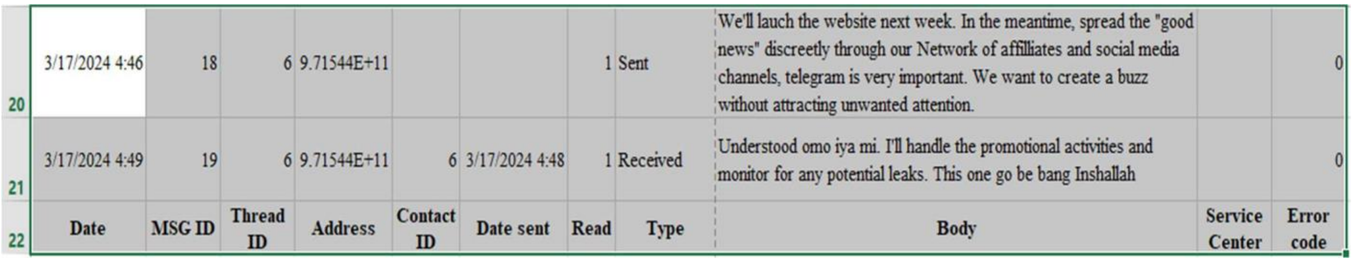
(A) SMS messages



1	SMS messages report										
2	Date	MSG ID	Thread ID	Address	Contact ID	Date sent	Read	Type	Body	Service Center	Error code
3	3/16/2024 20:55	1	3	8032111225			1	Sent	Hi babe, how was your journey to Kaduna. I hope it wasn't stressfull		0
4	3/17/2024 3:09	2	4	8032111669	5	3/17/2024 3:09	1	Received	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		0
5	3/17/2024 3:10	3	4	8032111669			1	Sent	Thank you Pastor		0
6	3/17/2024 3:19	4	5	8032111133	3	3/17/2024 3:19	1	Received	Hey, I've got a new scam idea. we need to discuss.		0
7	3/17/2024 3:19	5	5	8032111133			1	Sent	Sure, I'm in. What's the plan this time?		0
8	3/17/2024 3:20	6	5	8032111133	3	3/17/2024 3:20	1	Received	Let's create a fake investment website and lure people into investing in a non-existent cryptocurrency. We'll promise huge returns.		0
9	3/17/2024 3:21	7	5	8032111133			1	Sent	Sounds good. Do you have the website ready?		0
10	3/17/2024 3:24	8	5	8032111133	3	3/17/2024 3:23	1	Received	Yes, use the same Bitcoin wallet address as before: 16AtGJbaxL2kmzx4mW5ocpT2ysTWxmacWn.		0
11	3/17/2024 3:25	9	5	8032111133			1	Sent	I feel you man, I am in on this fully, but not high value client we go Target this time around I.		0

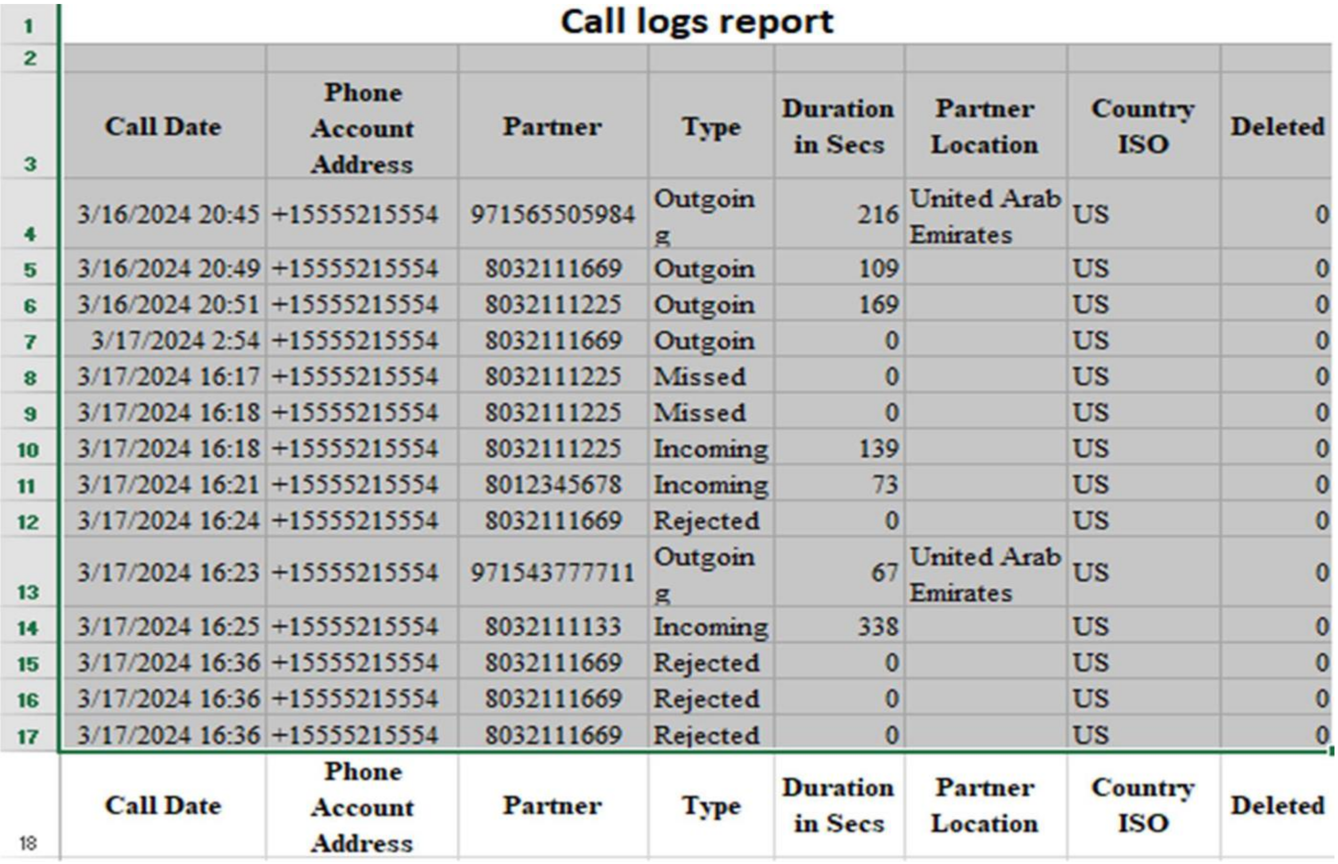


10	3/17/2024 3:24	8	5	8032111133	3	3/17/2024 3:23	1	Received	Yes, use the same Bitcoin wallet address as before: 16AtGJbaxL2kmzx4mW5ocpT2ysTWxmacWn.		0
11	3/17/2024 3:25	9	5	8032111133			1	Sent	I feel you man, I am in on this fully, but not high value client we go Target this time around I.		0
12	3/17/2024 3:29	10	5	8032111133	3	3/17/2024 3:29	1	Received	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		0
13	3/17/2024 3:37	11	5	8032111133			1	Sent	Alright man, I go join wen time reach		0
14	3/17/2024 4:26	12	6	9.71544E+11			1	Sent	Hey Egbon, I've set up a new website for our next venture. Check it out: https://apyeth.gifts/		0
15	3/17/2024 4:29	13	6	9.71544E+11	6	3/17/2024 4:29	1	Received	Nice work, Sammy. I'll take a look at the site. Are we using the same tactics as before?		0
16	3/17/2024 4:34	14	6	9.71544E+11			1	Sent	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.		0
17	3/17/2024 4:35	15	6	9.71544E+11	6	3/17/2024 4:35	1	Received	Sounds convincing. Payment gateway nkor? Are we still using the same Bitcoin wallet address?		0
18	3/17/2024 4:43	16	6	9.71544E+11			1	Sent	No, I've set up a new wallet address for this operation. Here it is: 1K1KMHpynJHQRbhzKHyik6yaJuQYxSaZCm		0



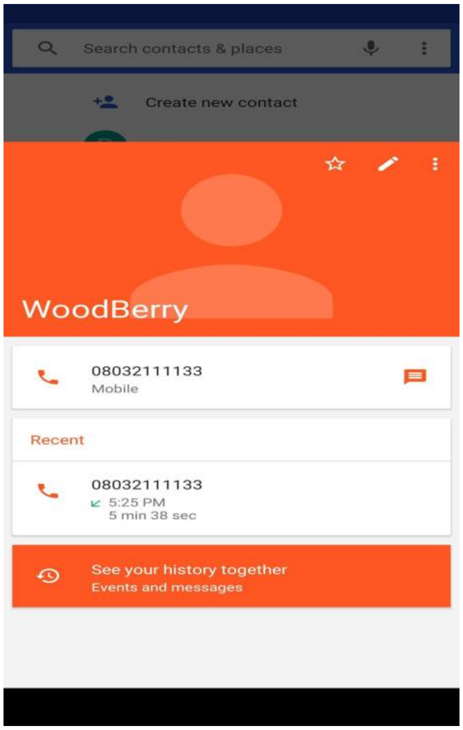
20	3/17/2024 4:46	18	6	9.71544E+11			1	Sent	We'll lauch the website next week. In the meantime, spread the "good news" discreetly through our Network of affilliates and social media channels, telegram is very important. We want to create a buzz without attracting unwanted attention.		0
21	3/17/2024 4:49	19	6	9.71544E+11	6	3/17/2024 4:48	1	Received	Understood omo iya mi. I'll handle the promotional activities and monitor for any potential leaks. This one go be bang Inshallah		0
22	Date	MSG ID	Thread ID	Address	Contact ID	Date sent	Read	Type	Body	Service Center	Error code

(B) **Call logs**



Call logs report

	Call Date	Phone Account Address	Partner	Type	Duration in Secs	Partner Location	Country ISO	Deleted
4	3/16/2024 20:45	+15555215554	971565505984	Outgoing	216	United Arab Emirates	US	0
5	3/16/2024 20:49	+15555215554	8032111669	Outgoin	109		US	0
6	3/16/2024 20:51	+15555215554	8032111225	Outgoin	169		US	0
7	3/17/2024 2:54	+15555215554	8032111669	Outgoin	0		US	0
8	3/17/2024 16:17	+15555215554	8032111225	Missed	0		US	0
9	3/17/2024 16:18	+15555215554	8032111225	Missed	0		US	0
10	3/17/2024 16:18	+15555215554	8032111225	Incoming	139		US	0
11	3/17/2024 16:21	+15555215554	8012345678	Incoming	73		US	0
12	3/17/2024 16:24	+15555215554	8032111669	Rejected	0		US	0
13	3/17/2024 16:23	+15555215554	971543777711	Outgoing	67	United Arab Emirates	US	0
14	3/17/2024 16:25	+15555215554	8032111133	Incoming	338		US	0
15	3/17/2024 16:36	+15555215554	8032111669	Rejected	0		US	0
16	3/17/2024 16:36	+15555215554	8032111669	Rejected	0		US	0
17	3/17/2024 16:36	+15555215554	8032111669	Rejected	0		US	0
18	Call Date	Phone Account Address	Partner	Type	Duration in Secs	Partner Location	Country ISO	Deleted



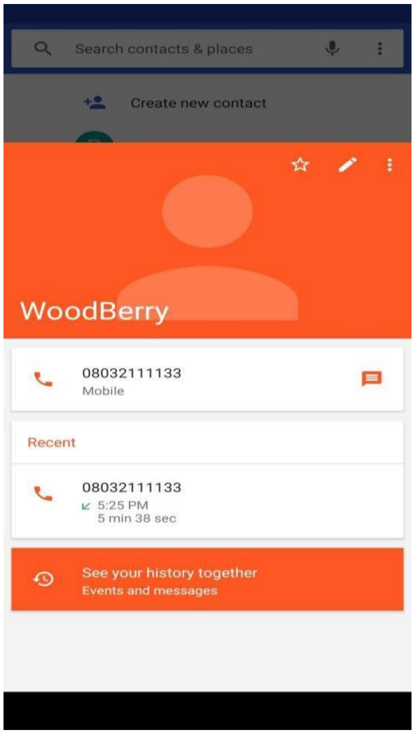
WoodBerry

08032111133
Mobile

Recent

08032111133
5:25 PM
5 min 38 sec

See your history together
Events and messages



WoodBerry

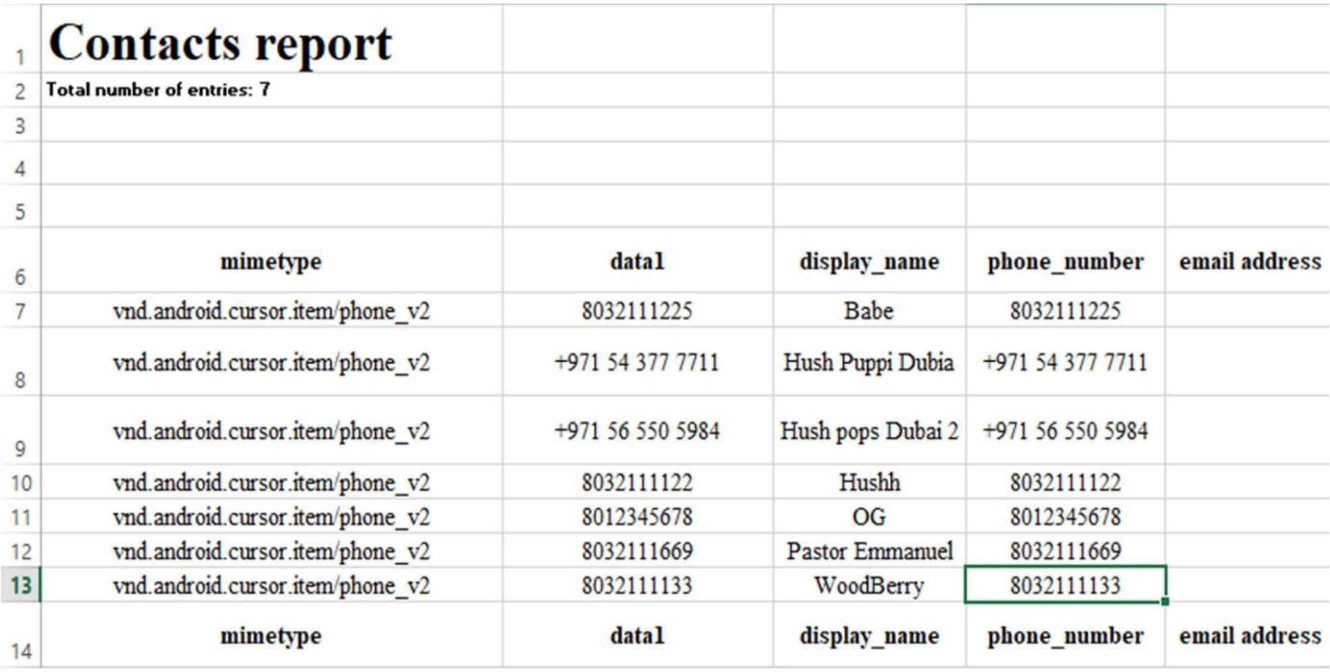
08032111133
Mobile

Recent

08032111133
5:25 PM
5 min 38 sec

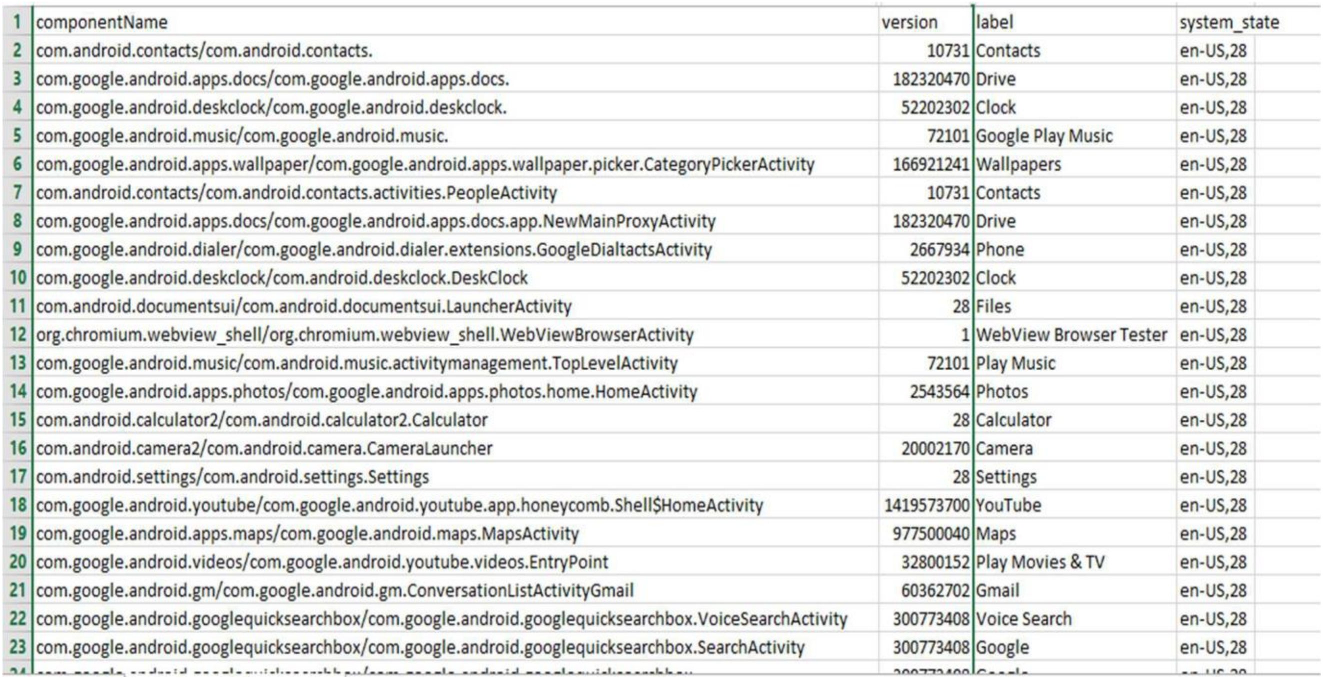
See your history together
Events and messages

(C) **Contact lists**

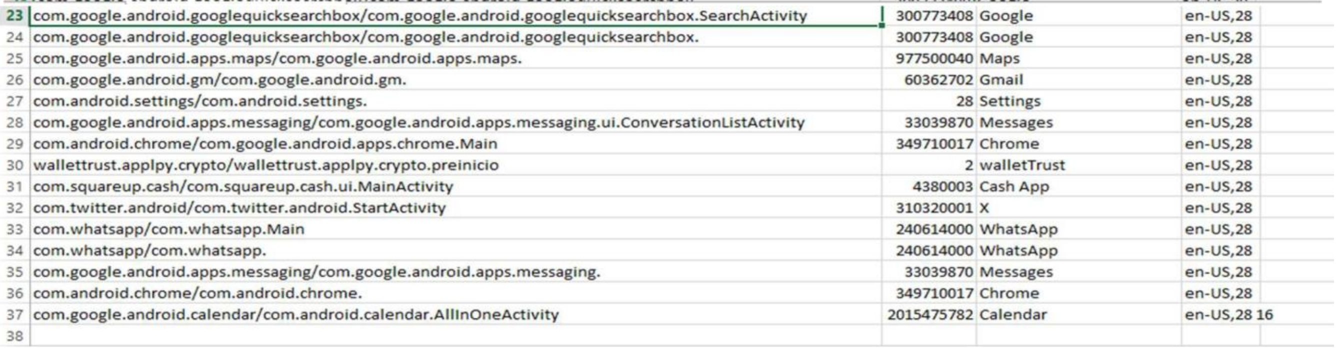


1	**Contacts report**				
2	**Total number of entries: 7**				
3					
4					
5					
6	**mimetype**	**data1**	**display_name**	**phone_number**	**email address**
7	vnd.android.cursor.item/phone_v2	8032111225	Babe	8032111225	
8	vnd.android.cursor.item/phone_v2	+971 54 377 7711	Hush Puppi Dubia	+971 54 377 7711	
9	vnd.android.cursor.item/phone_v2	+971 56 550 5984	Hush pops Dubai 2	+971 56 550 5984	
10	vnd.android.cursor.item/phone_v2	8032111122	Hushh	8032111122	
11	vnd.android.cursor.item/phone_v2	8012345678	OG	8012345678	
12	vnd.android.cursor.item/phone_v2	8032111669	Pastor Emmanuel	8032111669	
13	vnd.android.cursor.item/phone_v2	8032111133	WoodBerry	8032111133	
14	**mimetype**	**data1**	**display_name**	**phone_number**	**email address**

(D) **Application usage history**

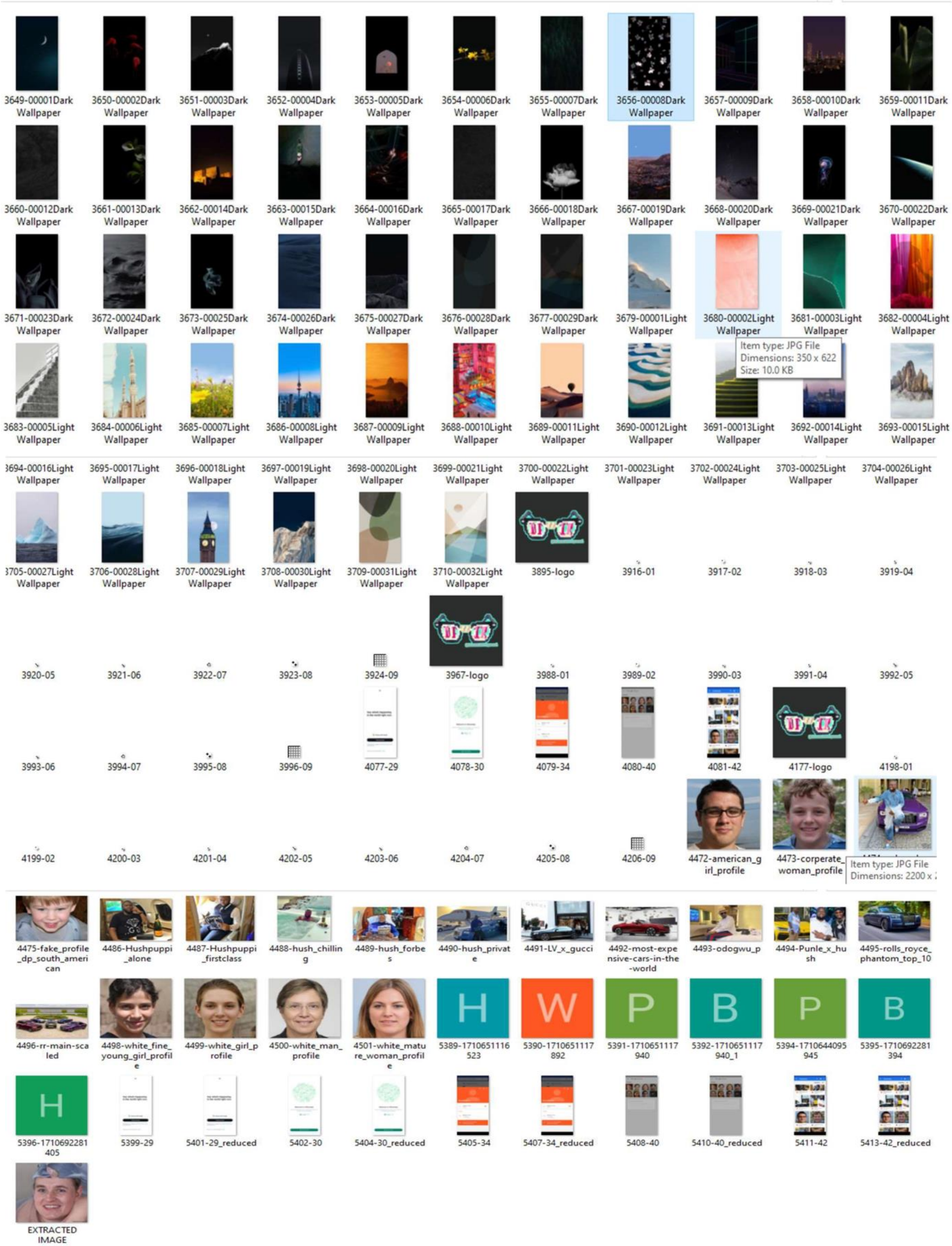


1	componentName	version	label	system_state
2	com.android.contacts/com.android.contacts.	10731	Contacts	en-US,28
3	com.google.android.apps.docs/com.google.android.apps.docs.	182320470	Drive	en-US,28
4	com.google.android.deskclock/com.google.android.deskclock.	52202302	Clock	en-US,28
5	com.google.android.music/com.google.android.music.	72101	Google Play Music	en-US,28
6	com.google.android.apps.wallpaper/com.google.android.apps.wallpaper.picker.CategoryPickerActivity	166921241	Wallpapers	en-US,28
7	com.android.contacts/com.android.contacts.activities.PeopleActivity	10731	Contacts	en-US,28
8	com.google.android.apps.docs/com.google.android.apps.docs.app.NewMainProxyActivity	182320470	Drive	en-US,28
9	com.google.android.dialer/com.google.android.dialer.extensions.GoogleDialtactsActivity	2667934	Phone	en-US,28
10	com.google.android.deskclock/com.android.deskclock.DeskClock	52202302	Clock	en-US,28
11	com.android.documentsui/com.android.documentsui.LauncherActivity	28	Files	en-US,28
12	org.chromium.webview_shell/org.chromium.webview_shell.WebViewBrowserActivity	1	WebView Browser Tester	en-US,28
13	com.google.android.music/com.android.music.activitymanagement.TopLevelActivity	72101	Play Music	en-US,28
14	com.google.android.apps.photos/com.google.android.apps.photos.home.HomeActivity	2543564	Photos	en-US,28
15	com.android.calculator2/com.android.calculator2.Calculator	28	Calculator	en-US,28
16	com.android.camera2/com.android.camera.CameraLauncher	20002170	Camera	en-US,28
17	com.android.settings/com.android.settings.Settings	28	Settings	en-US,28
18	com.google.android.youtube/com.google.android.youtube.app.honeycomb.Shell$HomeActivity	1419573700	YouTube	en-US,28
19	com.google.android.apps.maps/com.google.android.maps.MapsActivity	977500040	Maps	en-US,28
20	com.google.android.videos/com.google.android.youtube.videos.EntryPoint	32800152	Play Movies & TV	en-US,28
21	com.google.android.gm/com.google.android.gm.ConversationListActivityGmail	60362702	Gmail	en-US,28
22	com.google.android.googlequicksearchbox/com.google.android.googlequicksearchbox.VoiceSearchActivity	300773408	Voice Search	en-US,28
23	com.google.android.googlequicksearchbox/com.google.android.googlequicksearchbox.SearchActivity	300773408	Google	en-US,28



23	com.google.android.googlequicksearchbox/com.google.android.googlequicksearchbox.SearchActivity	300773408	Google	en-US,28	
24	com.google.android.googlequicksearchbox/com.google.android.googlequicksearchbox.	300773408	Google	en-US,28	
25	com.google.android.apps.maps/com.google.android.apps.maps.	977500040	Maps	en-US,28	
26	com.google.android.gm/com.google.android.gm.	60362702	Gmail	en-US,28	
27	com.android.settings/com.android.settings.	28	Settings	en-US,28	
28	com.google.android.apps.messaging/com.google.android.apps.messaging.ui.ConversationListActivity	33039870	Messages	en-US,28	
29	com.android.chrome/com.google.android.apps.chrome.Main	349710017	Chrome	en-US,28	
30	wallettrust.applpy.crypto/wallettrust.applpy.crypto.preinicio	2	walletTrust	en-US,28	
31	com.squareup.cash/com.squareup.cash.ui.MainActivity	4380003	Cash App	en-US,28	
32	com.twitter.android/com.twitter.android.StartActivity	310320001	X	en-US,28	
33	com.whatsapp/com.whatsapp.Main	240614000	WhatsApp	en-US,28	
34	com.whatsapp/com.whatsapp.	240614000	WhatsApp	en-US,28	
35	com.google.android.apps.messaging/com.google.android.apps.messaging.	33039870	Messages	en-US,28	
36	com.android.chrome/com.android.chrome.	349710017	Chrome	en-US,28	
37	com.google.android.calendar/com.android.calendar.AllInOneActivity	2015475782	Calendar	en-US,28	16
38					

(E) Images



3649-00001Dark Wallpaper
3650-00002Dark Wallpaper
3651-00003Dark Wallpaper
3652-00004Dark Wallpaper
3653-00005Dark Wallpaper
3654-00006Dark Wallpaper
3655-00007Dark Wallpaper
3656-00008Dark Wallpaper
3657-00009Dark Wallpaper
3658-00010Dark Wallpaper
3659-00011Dark Wallpaper

3660-00012Dark Wallpaper
3661-00013Dark Wallpaper
3662-00014Dark Wallpaper
3663-00015Dark Wallpaper
3664-00016Dark Wallpaper
3665-00017Dark Wallpaper
3666-00018Dark Wallpaper
3667-00019Dark Wallpaper
3668-00020Dark Wallpaper
3669-00021Dark Wallpaper
3670-00022Dark Wallpaper

3671-00023Dark Wallpaper
3672-00024Dark Wallpaper
3673-00025Dark Wallpaper
3674-00026Dark Wallpaper
3675-00027Dark Wallpaper
3676-00028Dark Wallpaper
3677-00029Dark Wallpaper
3679-00001Light Wallpaper
3680-00002Light Wallpaper
3681-00003Light Wallpaper
3682-00004Light Wallpaper

Item type: JPG File
Dimensions: 350 x 622
Size: 10.0 KB

3683-00005Light Wallpaper
3684-00006Light Wallpaper
3685-00007Light Wallpaper
3686-00008Light Wallpaper
3687-00009Light Wallpaper
3688-00010Light Wallpaper
3689-00011Light Wallpaper
3690-00012Light Wallpaper
3691-00013Light Wallpaper
3692-00014Light Wallpaper
3693-00015Light Wallpaper

3694-00016Light Wallpaper
3695-00017Light Wallpaper
3696-00018Light Wallpaper
3697-00019Light Wallpaper
3698-00020Light Wallpaper
3699-00021Light Wallpaper
3700-00022Light Wallpaper
3701-00023Light Wallpaper
3702-00024Light Wallpaper
3703-00025Light Wallpaper
3704-00026Light Wallpaper

3705-00027Light Wallpaper
3706-00028Light Wallpaper
3707-00029Light Wallpaper
3708-00030Light Wallpaper
3709-00031Light Wallpaper
3710-00032Light Wallpaper
3895-logo
3916-01
3917-02
3918-03
3919-04

3920-05
3921-06
3922-07
3923-08
3924-09
3967-logo
3988-01
3989-02
3990-03
3991-04
3992-05

3993-06
3994-07
3995-08
3996-09
4077-29
4078-30
4079-34
4080-40
4081-42
4177-logo
4198-01

4199-02
4200-03
4201-04
4202-05
4203-06
4204-07
4205-08
4206-09
4472-american_girl_profile
4473-corperate_woman_profile

Item type: JPG File
Dimensions: 2200 x

4475-fake_profile_dp_south_american
4486-Hushpuppi_alone
4487-Hushpuppi_firstclass
4488-hush_chilling
4489-hush_forbes
4490-hush_private
4491-LV_x_gucci
4492-most-expensive-cars-in-the-world
4493-odogwu_p
4494-Punle_x_hush
4495-rolls_royce_phantom_top_10

4496-rr-main-scaled
4498-white_fine_young_girl_profile
4499-white_girl_profile
4500-white_man_profile
4501-white_mature_woman_profile
5389-1710651116523
5390-1710651117892
5391-1710651117940
5392-1710651117940_1
5394-1710644095945
5395-1710692281394

5396-1710692281405
5399-29
5401-29_reduced
5402-30
5404-30_reduced
5405-34
5407-34_reduced
5408-40
5410-40_reduced
5411-42
5413-42_reduced

EXTRACTED IMAGE

(F) **Crypto wallets**

Based on my review of data from the suspect's Android phone and from a Bitcoin online Wallet account connected to that phone;
1K1KMHpynJHQRbhzKHyik6yaJuQYxSaZCm

7. PROFESSIONAL RECOMMENDATION BASED ON ANDROID IMAGE ANALYSIS

Based on a forensic analysis of a cybercrime suspect's Android phone, the following summary and recommendations are provided.

Summary of Forensic Findings

A forensic review of the suspect's Android device was conducted using Autopsy software to uncover evidence of fraudulent online investment activities. The analysis yielded several key findings:

- **Malicious Applications:** A link to a fraudulent investment website (https://apyeth.gifts/) was discovered within the phone's message logs.
- **Browser and Chat History:** Cryptocurrency wallet addresses found in chat messages and web browser history were identified as being connected to previously reported scams.
- **Data Tampering:** The analysis indicated that the user had intentionally attempted to delete data from the device.

Recommended Actions

1. Expand the Current Investigation

- The recovered cryptocurrency wallet addresses and application details should be checked against international fraud databases, such as Scamwatch and Chainalysis.
- Investigators should correlate the device's chat records and call logs with existing victim reports to identify potential co-conspirators and other associated devices.

2. Develop Defenses Against the Fraudulent App

- Collaborate with mobile security vendors or national cyber-response units (CERTs) to create a unique digital "fingerprint" for the malicious investment app (based on its package name, hash, or certificate).
- This signature should be shared with mobile antivirus companies and official app stores to ensure the app is automatically detected and blocked in the future.

3. Strengthen Legal and Collaborative Efforts

- The evidence gathered should be submitted to specialized financial cybercrime units.
- This evidence should be used to request legal subpoenas for transaction data from cryptocurrency exchanges associated with the recovered wallet addresses.

4. Issue a Public Advisory

- Use the details of this case to create a public fraud alert warning people about fake investment applications that impersonate legitimate platforms.
- This alert should include redacted screenshots of the fraudulent app and scam messages to help the public identify these threats.

5. Advocate for Stronger Industry-Wide Security

- Push for financial institutions and mobile platform providers to implement more rigorous vetting and digital signature verification for investment-related apps.
- Promote collaboration between law enforcement, mobile operating systems (like Google), and telecom companies to better detect and block high-risk behaviors, such as the side-loading of unverified applications.

8. CONCLUSION

The forensic investigation confirms that the suspect, SAMMY, who has a history of conducting online scams using various identities and social media profiles, was preparing to launch a new, sophisticated fake investment scheme. He reportedly considered this new scam to be unique due to the specific audience it was designed to target.

Furthermore, the investigation reveals that SAMMY has significant connections to well-known and successful cybercriminals, such as "Hushpuppi" and "Woodberry." It is also clear that SAMMY was not working in isolation, but rather as part of a group of co-conspirators to carry out these online frauds.

The evidence recovered from the suspect's Android device offers direct digital proof of his criminal intent and actions, covering everything from the development of fake investment apps to his communications with victims. This evidence is crucial for a criminal prosecution and also serves as a valuable resource for improving broader cybersecurity and mobile fraud-prevention efforts.

In summary, this incident exposes critical security gaps in cyberspace. The fact that criminals like SAMMY continue to operate is a clear signal that more aggressive and robust protection of the digital domain and its users is required. An immediate response to remedy the current situation, along with long-term strategic enhancements, is necessary to minimize the risk of similar events and restore trust among stakeholders.