Forensic Examination of a Supplied Android Image

Capstone Project – DSA/Cybersecurity – 2025

Presented by:

Abioye Emmanuel Abiodun

Cybersecurity Student, DSA Program
Email: eabioye54@gmail.com
Phone: +234 813 215 4665

Digital Forensics Investigation Report
Case Title: Android Image Forensic Examination
Case ID: DSA-CYBERSECURITY-2025
Investigation Period: June 23– June 30, 2025
Investigator: Abioye Emmanuel Abiodun, Cybersecurity Student (DSA)
Client: Incubator Hub – Digital Skill-Up Africa (DSA)

1. INTRODUCTION

This report presents the findings of a digital forensic investigation into a cyber fraud case involving deceptive emails, unsolicited calls, and a fake online investment platform aimed at stealing personal and financial information from victims.

The fraudulent activities began around March 17, 2024, in Nigeria, and continued throughout the month. The suspect, **Samuel Jackson Livistone**, also known as "Sam" or "Sammy," is believed to have created a fictitious investment scheme to trick victims into funding a non-existent business. He has a known history of involvement in similar cybercrimes.

The investigation supports a criminal complaint and arrest warrant for Samuel Jackson Livistone under Nigeria's Cybercrime Act, for conspiracy to commit online fraud.

The report is based on the investigator's direct involvement, review of related documents, professional experience, and information from other officers and witnesses. It aims to establish probable cause, not to detail the entire case. Dates and figures mentioned are approximate unless stated otherwise.

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

3.1 Methodology The investigation followed the standard digital forensic process:

 Evidence Identification: Locate possible sources of digital evidence.

 Preservation: Secure and store forensic copies to protect data integrity.

 Analysis: Examine data such as messages, call logs, contacts, app usage, files, images, browser activity, crypto wallets, and deleted content.

 Documentation: Record findings and maintain a clear chain of custody.

 Reporting: Compile a comprehensive report with conclusions and actionable recommendations.

3.2 Tools Used & Tool Purpose

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

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 24, 2025, 12am

5. FINDINGS

The investigation identified **Samuel Jackson Livistone**, also known as "Sam" or "Sammy," as a Nigerian national residing in Nigeria and a key figure in a global cybercriminal network. Evidence shows that Sammy funds his lavish lifestyle through criminal activities, including computer intrusions and various fraudulent operations—such as Business Email Compromise (BEC) schemes—targeting victims worldwide. These scams are estimated to involve the theft and laundering of millions of dollars.

Messages retrieved from Sammy's Android phone indicate his direct involvement, along with **Coconspirator 1** and **Coconspirator 2**, in fraud schemes that defrauded victims of substantial sums in both U.S. dollars and other currencies. Further communications confirm that Sammy and Coconspirator 1 conspired to launder large amounts of money obtained through these schemes.

Forensic analysis of Coconspirator 1's Android phone and online accounts revealed that they managed money mule networks used in fraudulent operations. The same device contained communications with Nigerian phone number **+2348032111669**, identified as one of Sammy's numbers, saved under the contact name **"Sam"**. Additionally, the phone included a web link (**https://apyeth.gifts/**), associated with Sammy's fraudulent activities.

Messaging logs between "Sam" (using the above number) and Coconspirator 1 further confirmed their coordination in multiple scams and money laundering schemes during 2024 and 2025.

6. SCREENSHOTS (EVIDENCE OF CRIME COMMITTED)

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

(A) SMS messages

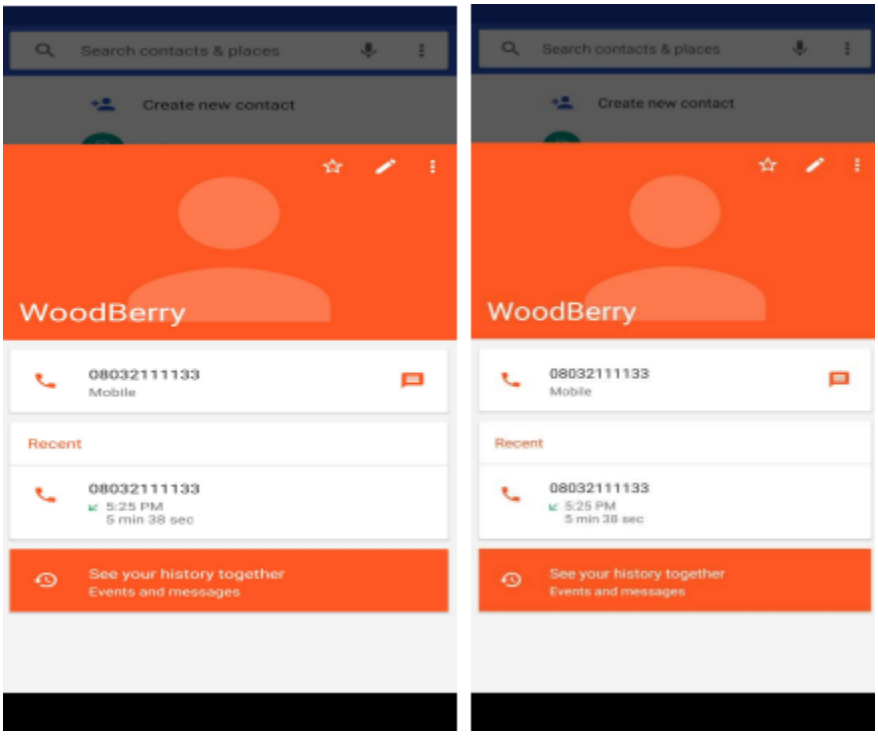
SMS messages report

Date	MSG ID	Thread ID	Address	Contact ID	Date sent	Read	Type	Body	Service Center	Error code
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
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
3/17/2024 3:10	3	4	8032111669			1	Sent	Thank you Pastor		0
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
3/17/2024 3:19	5	5	8032111133			1	Sent	Sure, I'm in. What's the plan this time?		0
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
3/17/2024 3:21	7	5	8032111133			1	Sent	Sounds good. Do you have the website ready?		0
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
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
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
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
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
3/17/2024 3:37	11	5	8032111133			1	Sent	Alright man, I go join wen time reach		0
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
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
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

(B) Call logs

SMS messages report

Date	MSG ID	Thread ID	Address	Contact ID	Date sent	Read	Type	Body	Service Center	Error code
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
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
3/17/2024 3:10	3	4	8032111669			1	Sent	Thank you Pastor		0
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
3/17/2024 3:19	5	5	8032111133			1	Sent	Sure, I'm in. What's the plan this time?		0
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
3/17/2024 3:21	7	5	8032111133			1	Sent	Sounds good. Do you have the website ready?		0
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
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
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
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
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
3/17/2024 3:37	11	5	8032111133			1	Sent	Alright man, I go join wen time reach		0
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
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
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



(C) Contact lists

Contacts report

Total number of entries: 7

mimetype	data1	display_name	phone_number	email address
vnd.android.cursor.item/phone_v2	8032111225	Babe	8032111225	
vnd.android.cursor.item/phone_v2	+971 54 377 7711	Hush Puppi Dubia	+971 54 377 7711	
vnd.android.cursor.item/phone_v2	+971 56 550 5984	Hush pops Dubai 2	+971 56 550 5984	
vnd.android.cursor.item/phone_v2	8032111122	Hushh	8032111122	
vnd.android.cursor.item/phone_v2	8012345678	OG	8012345678	
vnd.android.cursor.item/phone_v2	8032111669	Pastor Emmanuel	8032111669	
vnd.android.cursor.item/phone_v2	8032111133	WoodBerry	8032111133	
mimetype	data1	display_name	phone_number	email address

(D)Application usage history

componentName	version	label	system_state
com.android.contacts/com.android.contacts.	10731	Contacts	en-US,28
com.google.android.apps.docs/com.google.android.apps.docs.	182320470	Drive	en-US,28
com.google.android.deskclock/com.google.android.deskclock.	52202302	Clock	en-US,28
com.google.android.music/com.google.android.music.	72101	Google Play Music	en-US,28
com.google.android.apps.wallpaper/com.google.android.apps.wallpaper.picker.CategoryPickerActivity	166921241	Wallpapers	en-US,28
com.android.contacts/com.android.contacts.activities.PeopleActivity	10731	Contacts	en-US,28
com.google.android.apps.docs/com.google.android.apps.docs.app.NewMainProxyActivity	182320470	Drive	en-US,28
com.google.android.dialer/com.google.android.dialer.extensions.GoogleDialtactsActivity	2667934	Phone	en-US,28
com.google.android.deskclock/com.android.deskclock.DeskClock	52202302	Clock	en-US,28
com.android.documentsui/com.android.documentsui.LauncherActivity	28	Files	en-US,28
org.chromium.webview_shell/org.chromium.webview_shell.WebViewBrowserActivity	1	WebView Browser Tester	en-US,28
com.google.android.music/com.android.music.activitymanagement.TopLevelActivity	72101	Play Music	en-US,28
com.google.android.apps.photos/com.google.android.apps.photos.home.HomeActivity	2543564	Photos	en-US,28
com.android.calculator2/com.android.calculator2.Calculator	28	Calculator	en-US,28
com.android.camera2/com.android.camera.CameraLauncher	20002170	Camera	en-US,28
com.android.settings/com.android.settings.Settings	28	Settings	en-US,28
com.google.android.youtube/com.google.android.youtube.app.honeycomb.Shell$HomeActivity	1419573700	YouTube	en-US,28
com.google.android.apps.maps/com.google.android.maps.MapsActivity	977500040	Maps	en-US,28
com.google.android.videos/com.google.android.youtube.videos.EntryPoint	32800152	Play Movies & TV	en-US,28
com.google.android.gm/com.google.android.gm.ConversationListActivityGmail	60362702	Gmail	en-US,28
com.google.android.googlequicksearchbox/com.google.android.googlequicksearchbox.VoiceSearchActivity	300773408	Voice Search	en-US,28
com.google.android.googlequicksearchbox/com.google.android.googlequicksearchbox.SearchActivity	300773408	Google	en-US,28
com.google.android.googlequicksearchbox/com.google.android.googlequicksearchbox.SearchActivity	300773408	Google	en-US,28
com.google.android.googlequicksearchbox/com.google.android.googlequicksearchbox.	300773408	Google	en-US,28
com.google.android.apps.maps/com.google.android.apps.maps.	977500040	Maps	en-US,28
com.google.android.gm/com.google.android.gm.	60362702	Gmail	en-US,28
com.android.settings/com.android.settings.	28	Settings	en-US,28
com.google.android.apps.messaging/com.google.android.apps.messaging.ui.ConversationListActivity	33039870	Messages	en-US,28
com.android.chrome/com.google.android.apps.chrome.Main	349710017	Chrome	en-US,28
wallettrust.applpy.crypto/wallettrust.applpy.crypto.preinicio	2	walletTrust	en-US,28
com.squareup.cash/com.squareup.cash.ui.MainActivity	4380003	Cash App	en-US,28
com.twitter.android/com.twitter.android.StartActivity	310320001	X	en-US,28
com.whatsapp/com.whatsapp.Main	240614000	WhatsApp	en-US,28
com.whatsapp/com.whatsapp.	240614000	WhatsApp	en-US,28
com.google.android.apps.messaging/com.google.android.apps.messaging.	33039870	Messages	en-US,28
com.android.chrome/com.android.chrome.	349710017	Chrome	en-US,28
com.google.android.calendar/com.android.calendar.AllInOneActivity	2015475782	Calendar	en-US,28 16

E. IMAGES

(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

Recommendation:

Enhance Mobile Device Security Protocols and Implement Mobile Device Management (MDM)

Context from Forensic Analysis

A forensic examination of the suspect's Android device was conducted using **Autopsy**, focusing on evidence related to **fraudulent online investment schemes**. Key findings from the analysis include:

- **Application Evidence:** Presence of suspicious app artifacts and side-loaded APKs.
- **Fraudulent URL:** A fake investment link (**https://apyeth.gifts/**) was found in the message logs.
- **Cryptocurrency Evidence:** Wallet addresses recovered from chats and browser history matched those in known scam databases.
- **System Behavior:** Indicators of intentional data deletion and system manipulation were also observed.

Actionable Recommendations

1. **Expand the Investigation Across Devices:**
    - Link wallet addresses and app data to international fraud databases (e.g., Chainalysis, Scamwatch).
    - Match chat and call records with known victim reports to identify other involved devices or individuals.
2. **Detect Fraudulent Apps Proactively:**
    - Collaborate with mobile security teams or CERT units to create detection signatures for the fake investment app (e.g., package ID, icon, certificate).
    - Share these signatures with antivirus engines and app platforms for wider prevention.
3. **Enhance Legal and Law Enforcement Collaboration:**
    - Forward key evidence to financial cybercrime units.
    - Request subpoenas for transaction details from crypto exchanges linked to recovered wallet addresses.

Public Advisory

1. **Raise Public Awareness:**

- Use this case to issue alerts about fake investment apps that imitate legitimate platforms.
- Share redacted screenshots of the scam app and messages in public campaigns or media releases.

2. **Promote Stronger App Security Measures:**
   - Urge financial institutions and mobile platforms to enforce stricter app vetting and signature checks.
   - Recommend collaboration between law enforcement, Google, and telecom providers to identify and block risky side-loaded apps.

8. Conclusion

The forensic investigation confirms that **"Sammy"**, a known online scammer using multiple aliases and social media profiles, was planning to launch a new, large-scale fake investment scam. Evidence also links him to notorious cybercriminals like *Hushpuppi* and *Woodberry*, and shows he was working with other co-conspirators.

Digital evidence recovered from his Android device confirms his direct involvement in fraudulent activities, including fake app development, victim communication, and scam coordination.

These findings support legal action and highlight broader cybersecurity concerns—particularly vulnerabilities in the mobile ecosystem. This case underscores the urgent need for stronger cybersecurity measures and sustained efforts to protect users and prevent future cyber fraud.