Digital SkillUp Africa Final Capstone Project in Cybersecurity

Project Title: Building a Virtual Cybersecurity Laboratory and Conducting Android Forensics Investigations

Part Number: TWO

Part Title: Android Forensics Analysis and Reporting

Student Name: ONAEKO, Emmanuel Oladipupo

Email: eonaeko778@gmail.com

DIGITAL FORSENIC INVESTIGATION REPORT

CASE AGAINST: SAM

CASE NO: DSA_RE_0021

REPORT COMPLIED BY EMMANUEL ONAEKO (DIGITAL SKILLUP AFRICA FORSENIC INVESTIGATOR)

DIGITAL SKILLUP AFRICA FINANCIAL CRIME COMMISSION (DFCC)

Date report compiled: 5th July, 2025

DECLARATION OF INTENT AND AFFIDAVIT

The Contents of this report of an investigation undertaken by me, and I hereby confirm that:

1. The investigation was conducted following the financial and criminal laws of Nigeria and the guidelines of digital forensic investigation.
2. The Software and hardware used to support this investigation were prepared and used in a manner designed to assure the forensic integrity of both the process and its outcomes
3. The opinions presented at the end of the report are based solely on the evidence found

I, **ONAEKO EMMANUEL OLADIPUPO**, being duly sworn, declare and state as follows that evidences submitted were properly identified, investigated, evaluated and preserved and shall be used as submitted to the court and attempted as evidence to prove innocence or guilt of the Defendant.

INTRODUCTION

This report is submitted for the purpose of presenting relevant and admissible digital evidence that establishes the motive, behavioural patterns, and intent underlying the fraudulent activities attributed to the individual identified by the alias **“SAM”**, the owner of the analysed Android device.

All findings contained herein fall within the scope of my professional competence and forensic expertise. I, ***Emmanuel Onaeko***, the appointed investigator, affirm that this report does not extend into matters beyond my domain of specialisation and is prepared following standard investigative and evidentiary procedures.

EXECUTIVE SUMMARY

A substantial segment of the Nigerian population has recently fallen victim to a sophisticated fraudulent scheme involving a counterfeit cryptocurrency investment platform. This platform exploited various digital channels to lure individuals with the promise of exceptionally high returns on investment. Victims were instructed to make payments with the assurance of receiving profits within two weeks. However, upon the due date, access to the platform was abruptly terminated, and the perpetrators absconded with the funds, sparking widespread public outrage.

In response to the growing number of complaints, the **Digital Skillup Africa Financial Crimes Commission (DFCC)** initiated a formal investigation. This led to the arrest of a prime suspect, identified as **“SAM”**, and the lawful retrieval of his Android mobile device under a duly authorised search warrant, executed during a high-compliance operation.

I, **Emmanuel Onaeko**, was appointed as the digital forensic examiner and lead investigator in this matter. My role was to conduct a forensic reconstruction and analysis of the seized device to extract and preserve potential digital evidence. This report details the findings of that investigation, including critical communication threads, digital footprints, and the identification of known accomplices: **“Woodberry”** and **“Hushpuppi.”** These findings form the basis of the case *Digital Skillup Africa Financial Crimes Commission (DFCC) v. SAM*

TOOLS USED

- 7-Zip: This is a free and open-source file archiver software used to compress and decompress files, and it was used to extract the Android image of the suspect to prepare it for analysis
- Autospy: This is a powerful, open-source digital forensics platform used for conducting in-depth investigations on digital devices such as computers, mobile phones, and storage media, and it was used primarily as a tool for digital forensics to extract the evidence, which is now presented
- Virtual Environment: This forensics was conducted in an isolated environment of Windows 10 on a virtual block to preserve the integrity of the submitted evidence
- Snipping Tool: This was used primarily to snip and capture evidence

METHODOLOGY

The section details the process carried out towards proper evidence analysis.

Virtual Environment Setup

The virtual environment was set up on VirtualBox, leveraging the Windows 10 operating system, after which Autopsy was installed to cover the digital forensics activity.

Integrity Check of Android image

The Android image was first hashed at the place of the recipients to verify that there was no change in the image. The hash was compared with the hash of the Android image at the point of starting the investigation to ensure that it had notbeen been tampered with

Case Initialisation in Autopsy:

The case was launched and initiated on Autopsy by documenting the Case Name, Case Number, Examiner name and was enabled for the structured storage of all analysis, artefacts, and logs generated during the case investigation.

Android Image Setup

The Android image was then extracted using 7-Zip and then properly imported as a case study file on Autopsy, and it was ensured that it was properly imported to ensure

proper configuration and to preserve the integrity of the findings of the investigation.

Identification and Labelling of Evidence

After proper setup, the possible sources of evidence were first sighted before anything was out, possible sources identified were SMS messages, images, call logs, browser history, contact lists, application usage activity and each of this evidence was gathered and properly labelled.

Forensic Examination

The case was systematically investigated to reveal various findings that were adopted as evidence for the allegation of a scam.

Overview of analysis

1. File System Overview

- File system: Logical file

2. User Data Recovered

- Contacts: 7 contacts found
- SMS/MMS: 28 text messages recovered
- Call Logs: 14 unique call entries

3. Web Artefacts

- Web cookies found: 207
- Web History: 12
- Web search: 4

4. Media Metadata (EXIF)

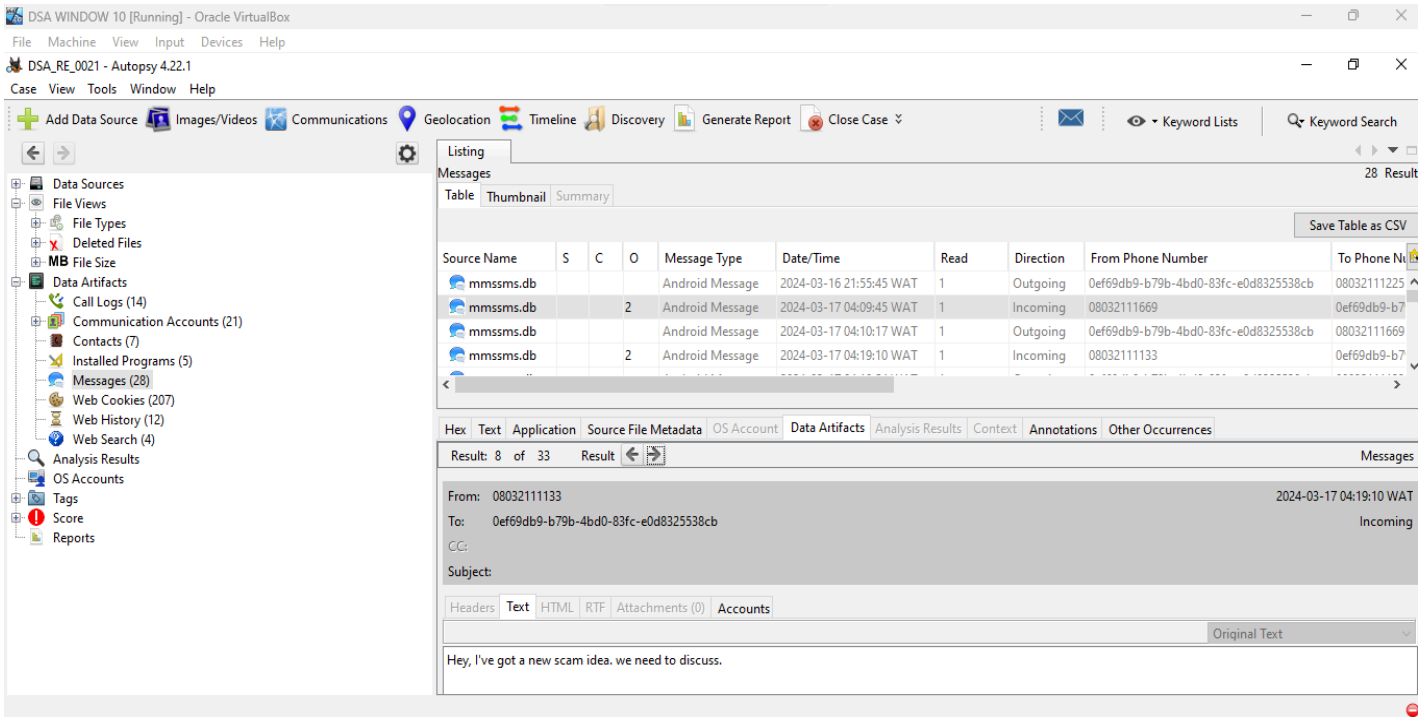
- 19 key images found
- Camera app used: Android default
- No videos found

5. Deleted Files: Nil

EVIDENCE AND FINDINGS

In alignment with the investigative objectives, our focus was directed toward the acquisition and analysis of digital evidence relevant to the suspect's activities. This included identifying the suspect's affiliations, uncovering potentially incriminating content, and extracting other evidentiary material that may substantiate the allegations and serve as admissible proof in the present case.

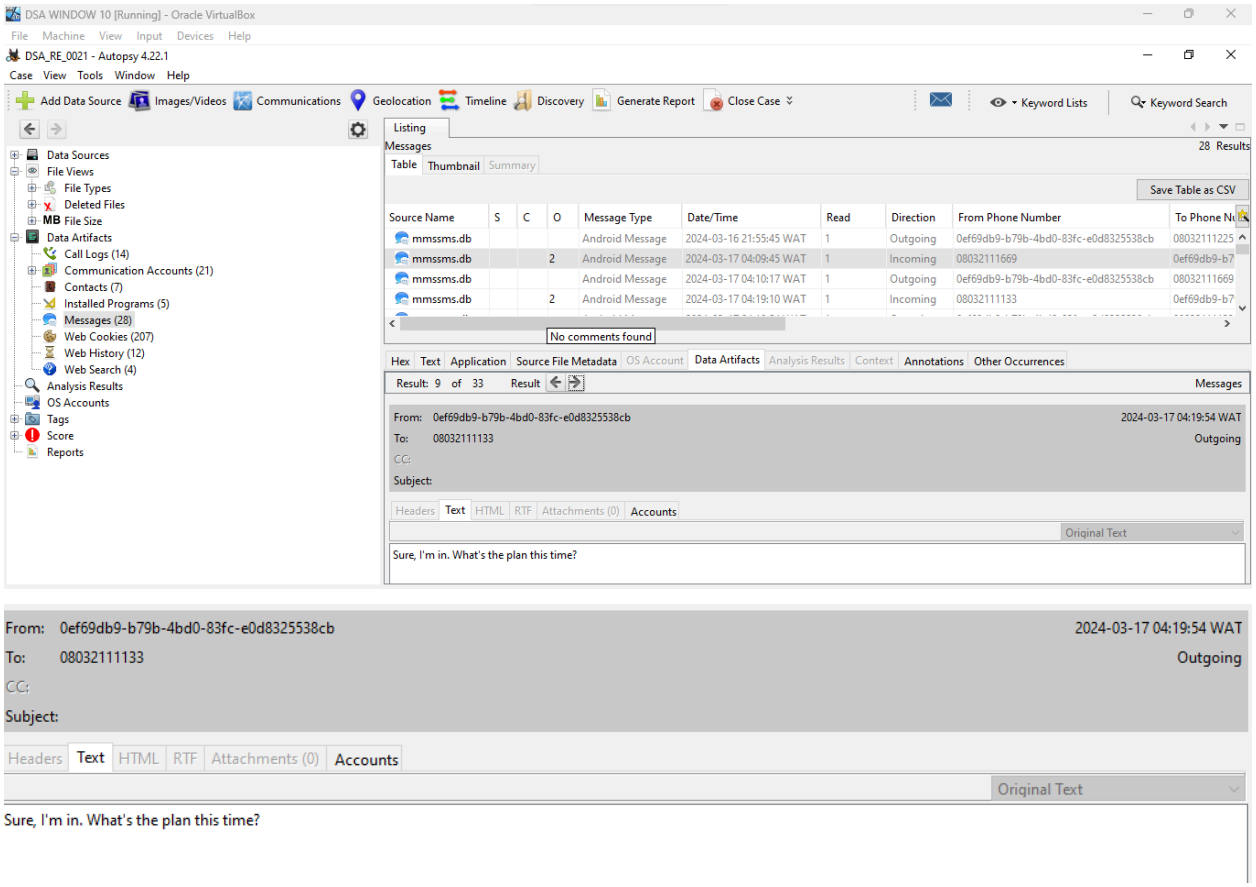
EXHIBIT 1: THE MESSAGE TO START A NEW SCAM



This picture gives evidence of a message initiated to **"SAM"** on **17th March 2024** at exactly **04:10 PM** with the statement *"Hey, I 've got a new scam idea, we need to*

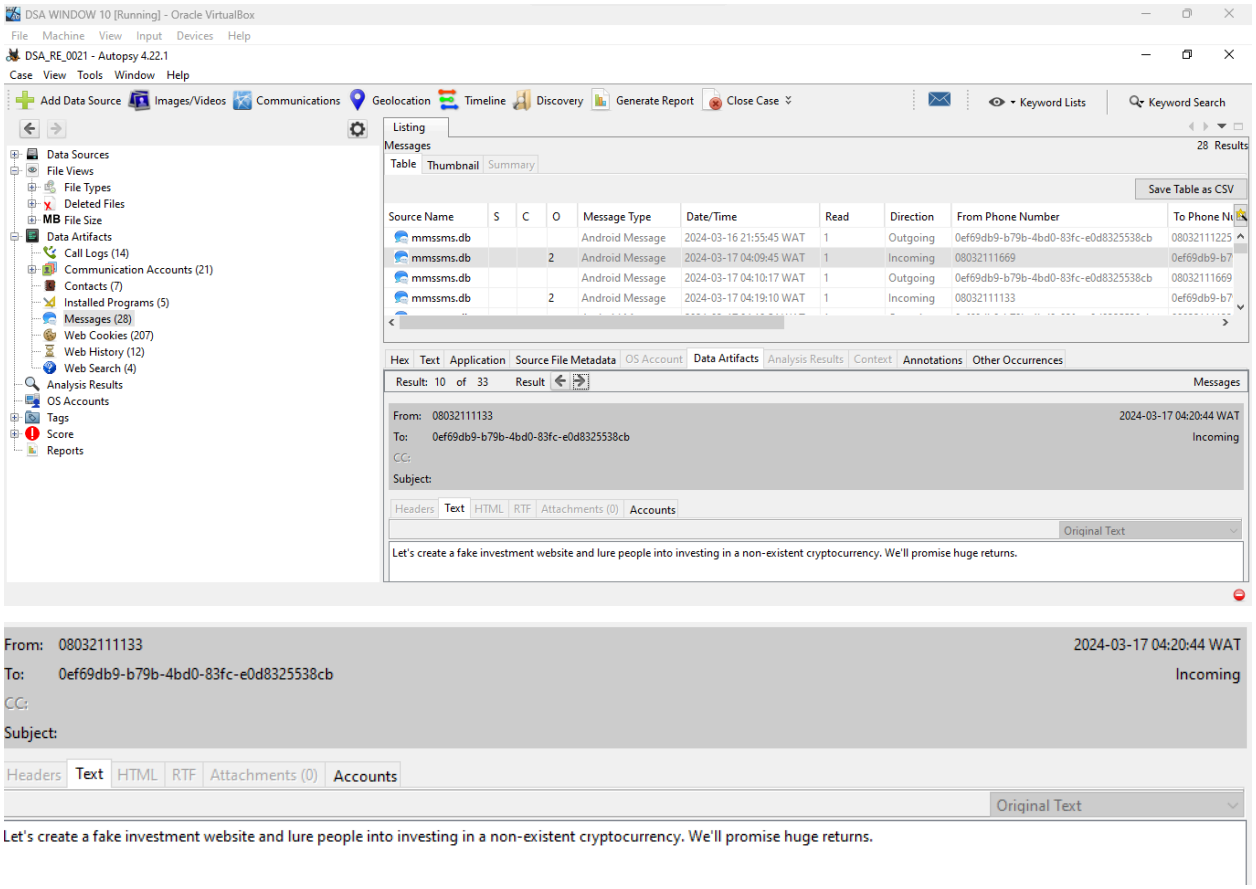
discuss", which I regard as the message initiation process to start a new scam to elude with people's money.

EXHIBIT 2: SAM REPLY



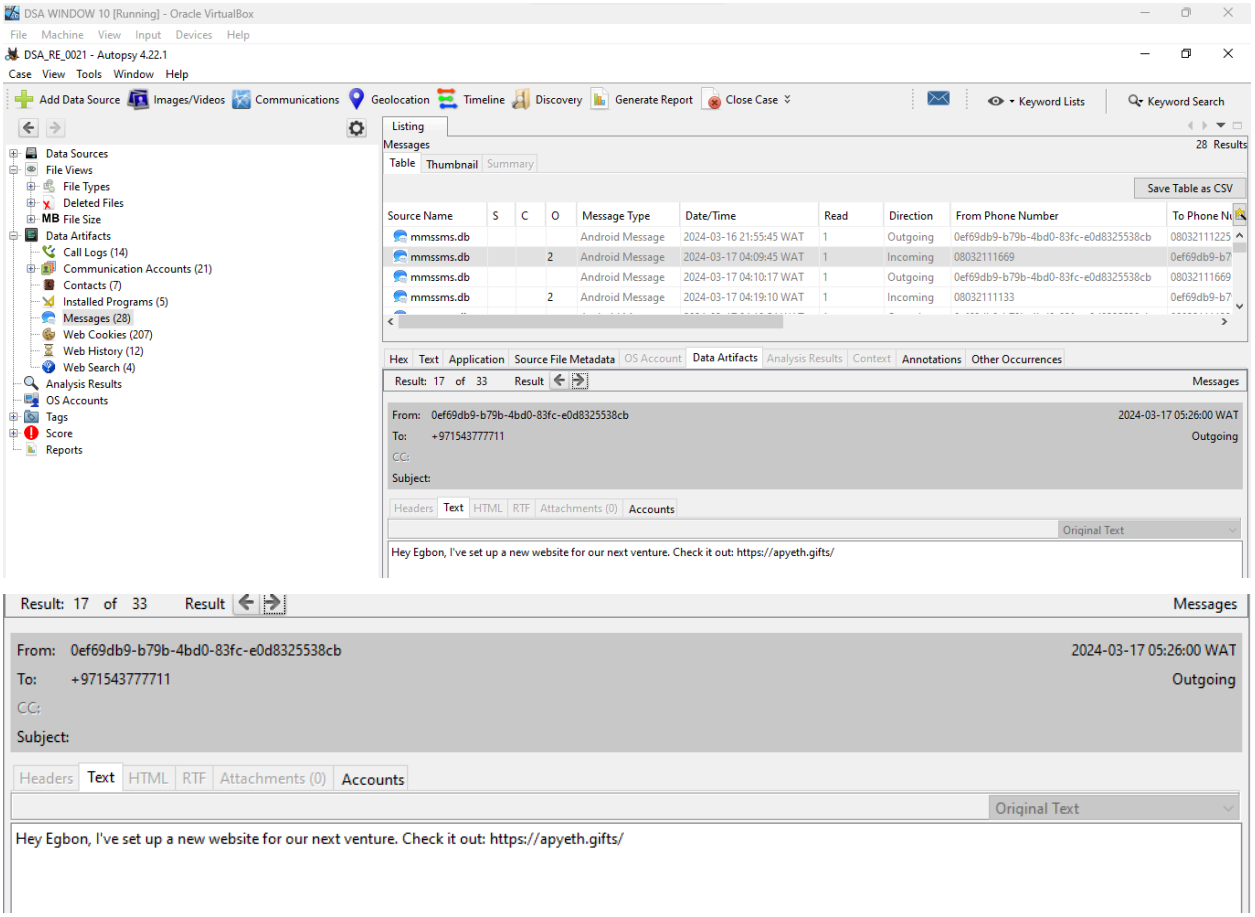
We observed that SAM would reply with so much excitement to know how the scam would go with a reply of ***"Sure, I'm I in. What's the plan this time?"*** This doesn't just show excitement, but also gives insight that they are behind some other scam initiatives previously

EXHIBIT 3: Message Initiation on starting the scam website



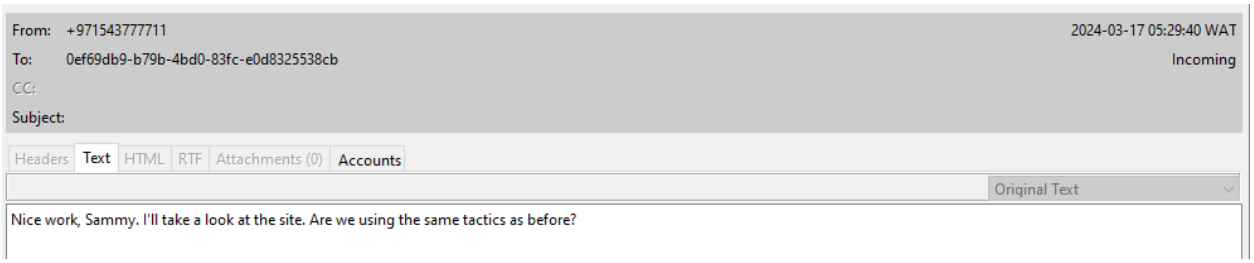
A message was sent to further say that *"they should create a fake website and lure people into investing in a non-existent cryptocurrency and we'll promise huge returns'* which was sent on **17th March, 2025,** from *"08032111133,* which is a woodberry number to **"SAM"**

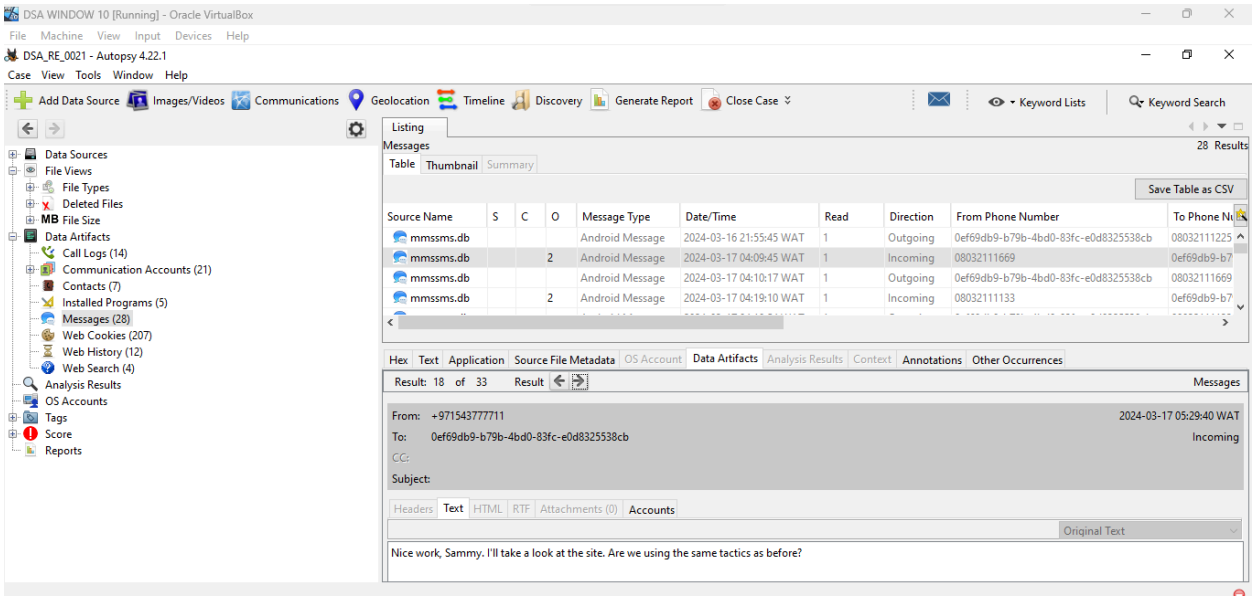
EXHIBIT 4:MESSAGE TO FOREIGN NUMBER BY SAM



"SAM" would send a message to the *+9715437777711,* which was identified as *HUSHPUPPI,* saying, *"Hey Egbon, I've set up a new website for our next venture. Check it out: https://apeyeth.gifts/*

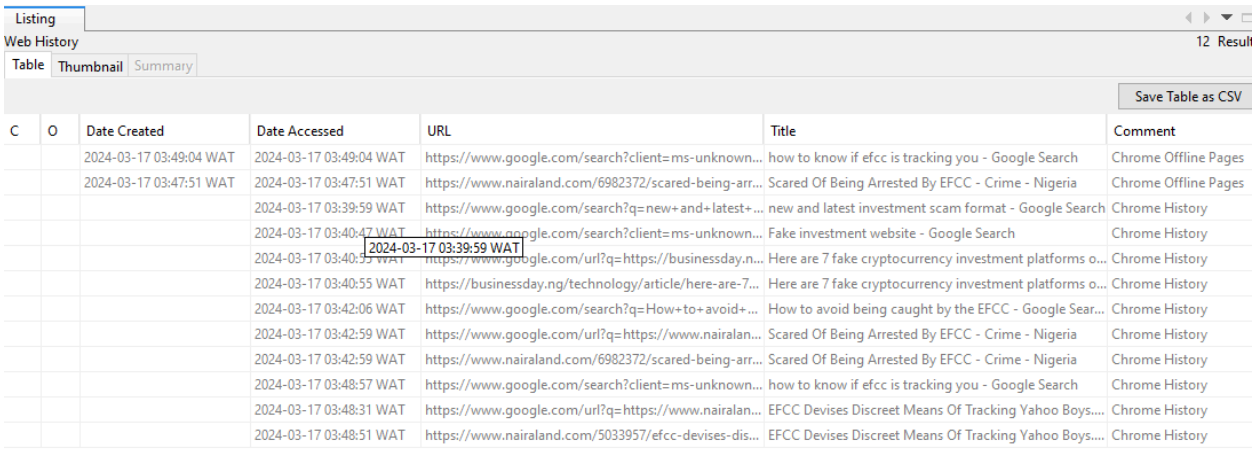
EXHIBIT 5: Foreign Number Reply to SAM





“SAM” also got this reply from the foreign number, highlighting that *it is a nice work, and they should use the same tactics as before*

EXHIBIT 6:WEB HISTORY



The website's history from **“SAM”** phone is rather incriminating, as it shows someone who is trying to evade the law with history such as *“ EFCC Devise Discreet Means of Tracking Yahoo Boys”, “Scared of Being Arrested by EFCC”,* among other searches that are not appropriate.

EXHIBIT 7: WEB SEARCH

Date Accessed	Text	Domain
2024-03-17 03:39:59 WAT	new and latest investment scam format	google.com
2024-03-17 03:42:06 WAT	How to avoid being caught by the EFCC	google.com
2025-07-06 15:17:35 WAT		
2025-07-06 15:17:36 WAT	"create new bi", "create new bitcoin...	

“SAM” web searches on the internet also see the evidence that he is planning a scam with search from *17th March 2024* at about *03:39:59 WAT* being *“ new and latest investment scam format”* and further searches indicating a plan to subvert the hand of the law with a message on *6th July 2025* showing that web search on *“ create new bitcoin wallet”*

EXHIBIT 8: INSTALLED PROGRAMS

Installed Programs

Program Name	Install Date/Time	Comment
com.google.android.youtube		Installed Apps GSM
com.squareup.cash		Installed Apps GSM
com.twitter.android		Installed Apps GSM
com.whatsapp		Installed Apps GSM
wallettrust.applpy.crypto		Installed Apps GSM

:

This shows the app that **“SAM”** had installed on his phone, which is *SquareUp. cash* and *wallettrust* are suspect and may have been used to aid transactions performed, and this application was never authorised to perform in Nigeria, so apart from committing fraud, **“SAM”** has also breached the regulatory operations of Nigeria

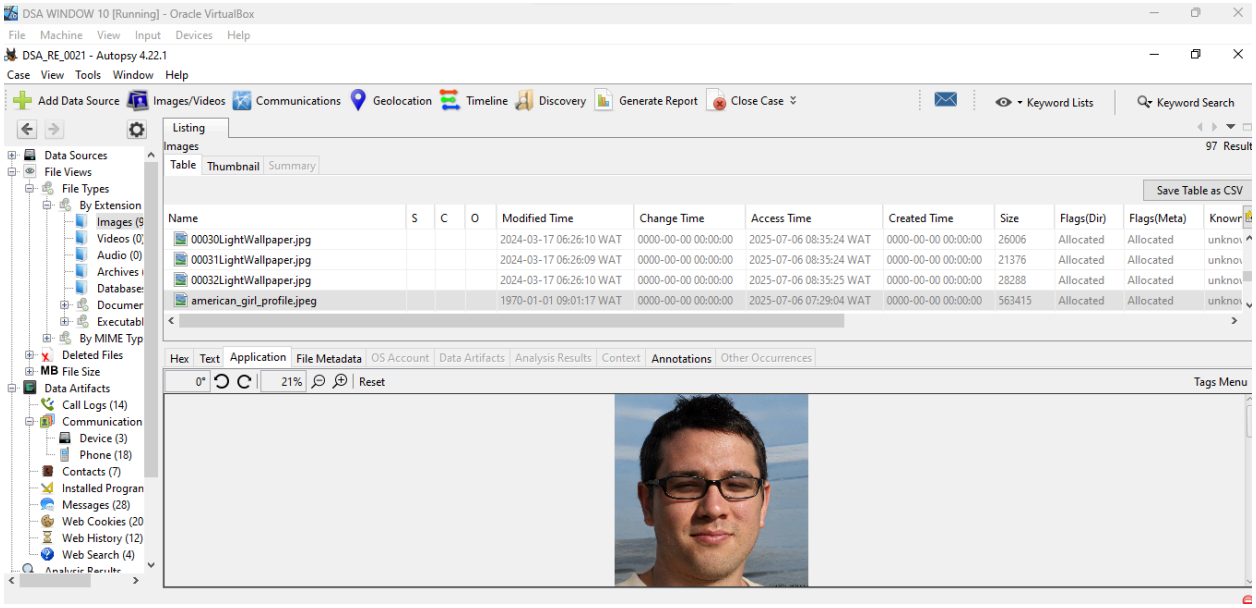
EXHIBIT 9: SUSPICIOUS CALL TO FOREIGN NUMBER “+15555215554”

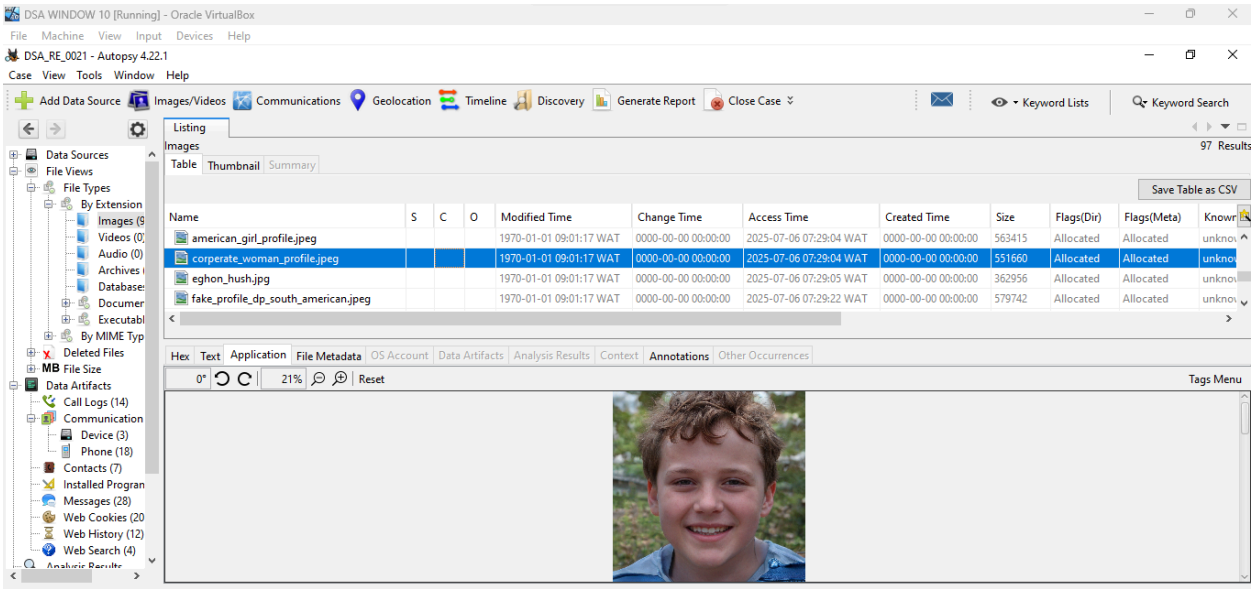
Call Logs

Person Name	From Phone Number	To Phone Number	Date/Time	Direction	Phone Number
			2024-03-16 20:45:54 WAT		+15555215554
			2024-03-16 20:49:50 WAT		+15555215554
			2024-03-16 20:51:59 WAT		+15555215554
			2024-03-17 02:54:56 WAT		+15555215554
			2024-03-17 16:17:36 WAT		+15555215554
			2024-03-17 16:18:04 WAT		+15555215554
			2024-03-17 16:18:22 WAT		+15555215554
			2024-03-17 16:21:46 WAT		+15555215554
			2024-03-17 16:23:25 WAT		+15555215554
			2024-03-17 16:24:09 WAT		+15555215554
			2024-03-17 16:25:20 WAT		+15555215554
			2024-03-17 16:36:15 WAT		+15555215554
			2024-03-17 16:36:21 WAT		+15555215554
			2024-03-17 16:36:28 WAT		+15555215554

We would notice a suspect call **"SAM"** made to *"+15555215554"* which we would later identify as *"HUSHPUPPI"*, who is currently facing litigation in the US for fraud, so that gives us a clue that they were in collusion to scam people.

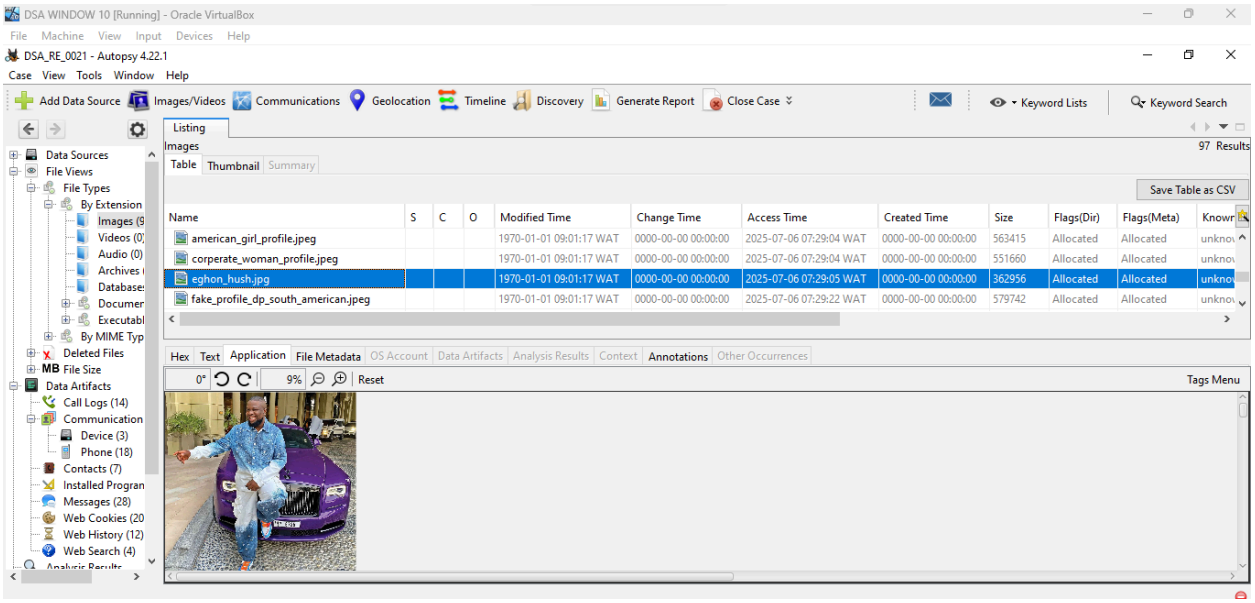
EXHIBIT 10:SUSCEPT IMAGES WITH SUSCEPT FILENAME





We would find suspect pictures in the Android Image, with a Suspect filename, suggesting that these are images they use when performing social engineering on their victims.

EXHIBIT 11: FLASHY IMAGES OF HUSHPUPPI



We would find incriminating pictures of one of his accomplices and mentors: **HUSHPUPPI**, who is currently facing allegations of financial fraud in the US, and it also has a suspect filename with *"Egbon_Hush"*

EXHIBIT 12: TOTAL MESSAGES THAT WE RECOVERED FROM THE SAME PHONE

Subject
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
Hey, I've got a new scam idea. we need to discuss.
Let's create a fake investment website and lure people into investing in a non-existent cryptocurrency. We'll promise huge returns.
Yes, use the same Bitcoin wallet address as before: 16AtGJbaxL2kmzx4mW5ocpT2ysTWxmacWn.
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
Nice work, Sammy. I'll take a look at the site. Are we using the same tactics as before?
Sounds convincing. Payment gateway nkor? Are we still using the same Bitcoin wallet address?
Got it. I'll update the payment instructions on the website accordingly. When we dey go live?
Understood omo iya mi. I'll handle the promotional activities and monitor for any potential leaks. This one go be bang Inshallah
Hi babe, how was your journey to Kaduna. I hope it wasn't stressfull
Thank you Pastor
Sure, I'm in. What's the plan this time?
Sounds good. Do you have the website ready?
I feel you man, I am in on this fully, but not high value client we go Target this time around I.
Alright man, I go join wen time reach
Hey Egbon, I've set up a new website for our next venture. Check it out: https://apyeth.gifts/
Yes, but this time we're targeting investors with promises of exclusive access to a "revolutionary" crypto currency technology. The website layout is desi
No, I've set up a new wallet address for this operation. Here it is: 1K1KMHpynJHQRbhzKHyik6yaJuQYxSaZCm
We'll lauch the website next week. In the meantime, spread the "good news" discreetly through our Network of affillliates and social media channels, tele
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

Hi babe, how was your journey to Kaduna. I hope it wasn't stressfull
Thank you Pastor
Sure, I'm in. What's the plan this time?
Sounds good. Do you have the website ready?
I feel you man, I am in on this fully, but not high value client we go Target this time around I.
Alright man, I go join wen time reach
Hey Egbon, I've set up a new website for our next venture. Check it out: https://apyeth.gifts/
Yes, but this time we're targeting investors with promises of exclusive access to a "revolutionary" crypto currency technology. The website layout is desi
No, I've set up a new wallet address for this operation. Here it is: 1K1KMHpynJHQRbhzKHyik6yaJuQYxSaZCm
We'll lauch the website next week. In the meantime, spread the "good news" discreetly through our Network of affillliates and social media channels, tele
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
Hey, I've got a new scam idea. we need to discuss.
Let's create a fake investment website and lure people into investing in a non-existent cryptocurrency. We'll promise huge returns.
Yes, use the same Bitcoin wallet address as before: 16AtGJbaxL2kmzx4mW5ocpT2ysTWxmacWn.
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
Nice work, Sammy. I'll take a look at the site. Are we using the same tactics as before?
Sounds convincing. Payment gateway nkor? Are we still using the same Bitcoin wallet address?
Got it. I'll update the payment instructions on the website accordingly. When we dey go live?
Understood omo iya mi. I'll handle the promotional activities and monitor for any potential leaks. This one go be bang Inshallah

These images show the messages that **"SAM**" sent from **17th March 2024** at about **04:09:45** to **17th March 2024** at about **04:48:57,** which shows a series of incriminating messages from **"WOODBERRY"** with phone number **"08032111133"** and **"HUSHPUPPI"** with phone number "**+971543777711"**

SUMMARY AND CONCLUSIONS

Following a thorough forensic examination of the extracted Android device image, we successfully recovered significant digital evidence that is both **incriminating** and

legally admissible in a court of law. The analysis was conducted in accordance with established forensic standards and chain-of-custody procedures, ensuring the **integrity and reliability** of all findings.

In light of the evidence obtained, I strongly recommend that the material be critically examined by the prosecuting authority and that this case be pursued with **utmost diligence, transparency, and adherence to due process**. Given the widespread impact of the fraudulent scheme, many Nigerian citizens are anticipating a fair resolution that could potentially aid in the **recovery of misappropriated funds** and restore public trust.

Additionally, I recommend that this case be leveraged as part of a **national cybersecurity and digital fraud awareness initiative**. Educating the public on how such scams operate could significantly help in preventing future occurrences and strengthening overall cyber resilience across the country.

Thank you

_____

ONAEKO EMMANUEL OLADIPUPO

Date: July 4th, 2025