DSA final project.

FINAL PROJECT PROPOSAL
Title: Building a Virtual Cybersecurity Laboratory and Conducting Android Forensics..

Virtual Lab for Cyber Security

OLUWASEUN OJO
DSA-Cyber security Student
joshseuntoin117@gmail.com
+2348135388280

In today’s rapidly evolving threat landscape, hands-on experience is critical for understanding cybersecurity principles, from penetration testing to digital forensics. This project documents the creation of a **virtual cybersecurity laboratory**, designed to simulate real-world attack and defense scenarios in a safe, controlled environment

Running virtual machine
21/5/2024 - 19/6/2024

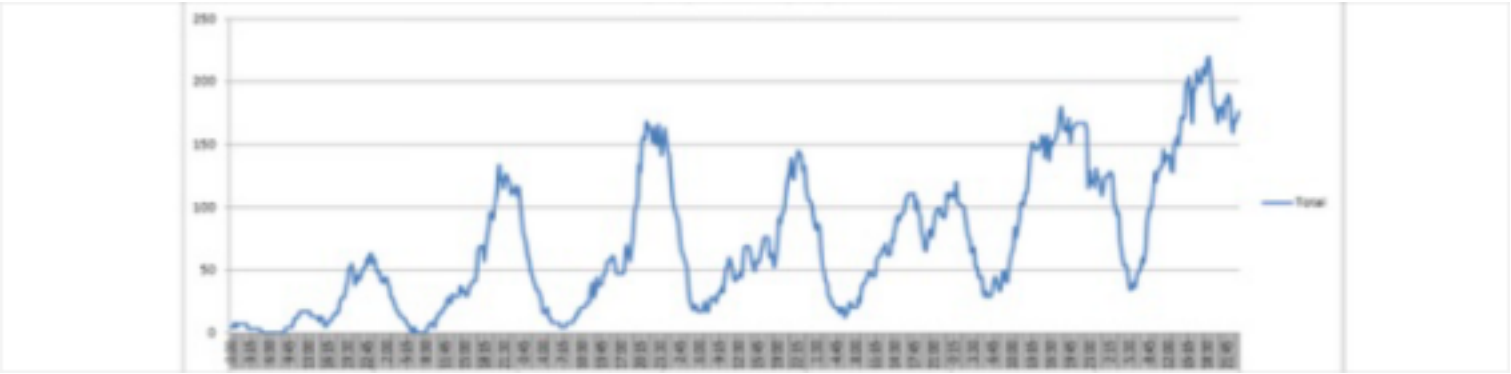


Fig1 Virtual Machines Running

An operating system image, preconfigured for labs and equipped with security tools, can run as a virtual machine. Students remotely access the virtual lab environment, load a preconfigured operating system image, run it as a virtual machine, complete a lab assignment

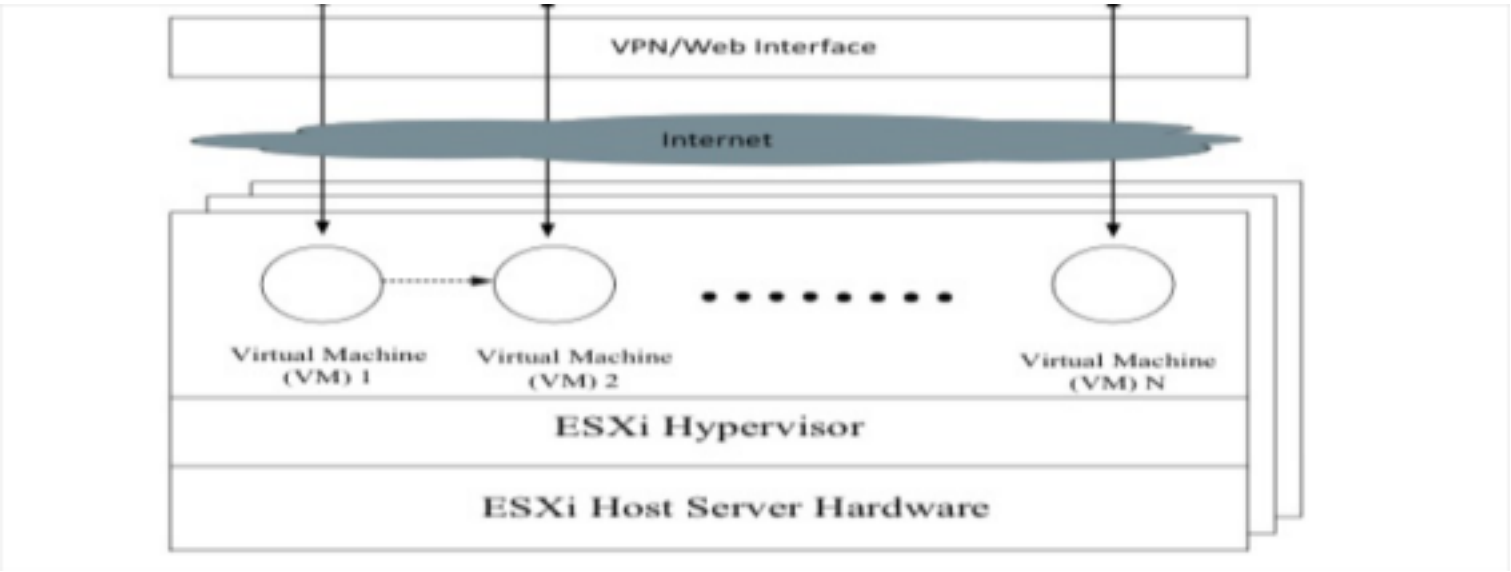


Fig2
Virtual Lab Platform without Network Boundary

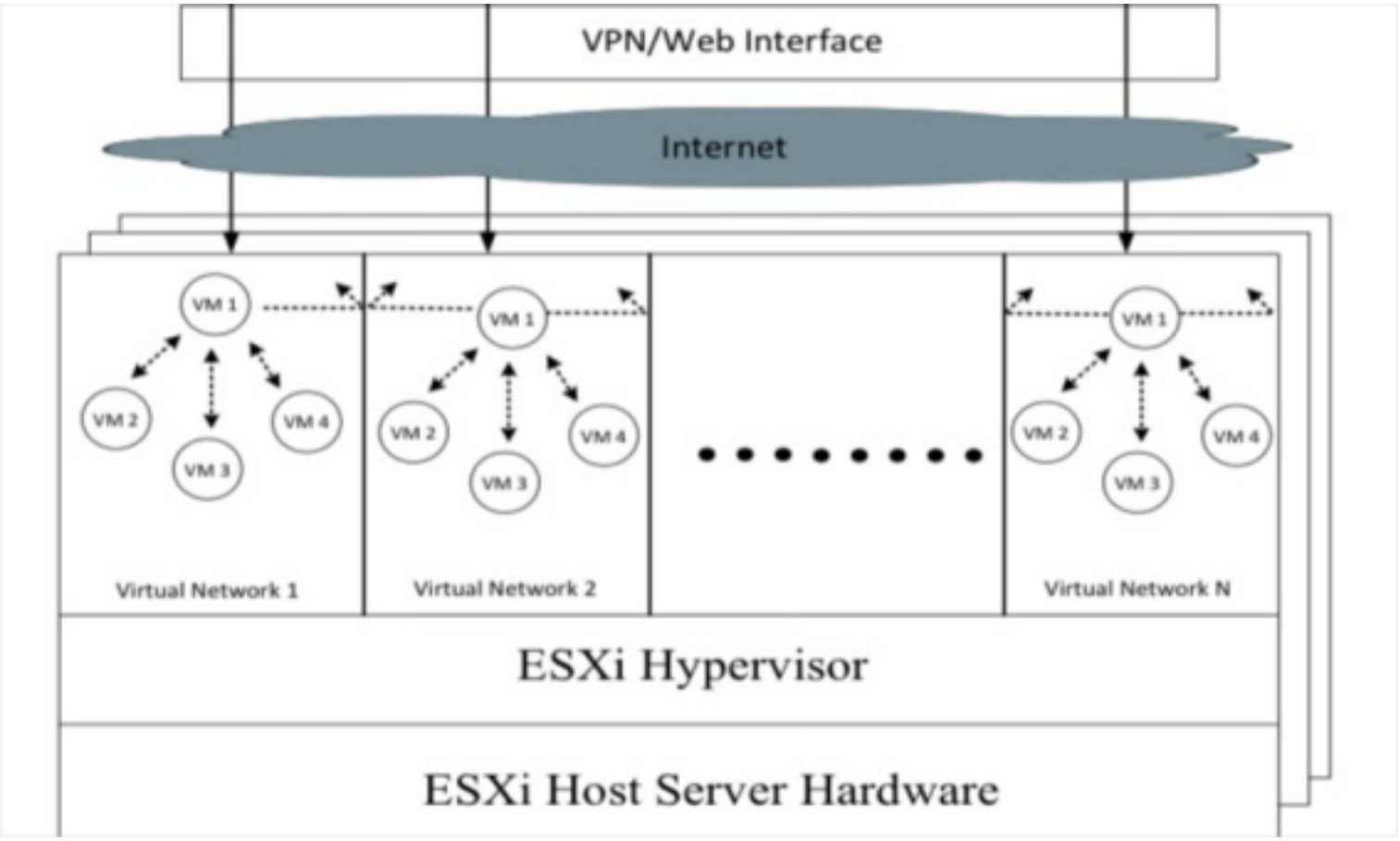


Fig 3: Virtual Lab Platform with Network Boundary.

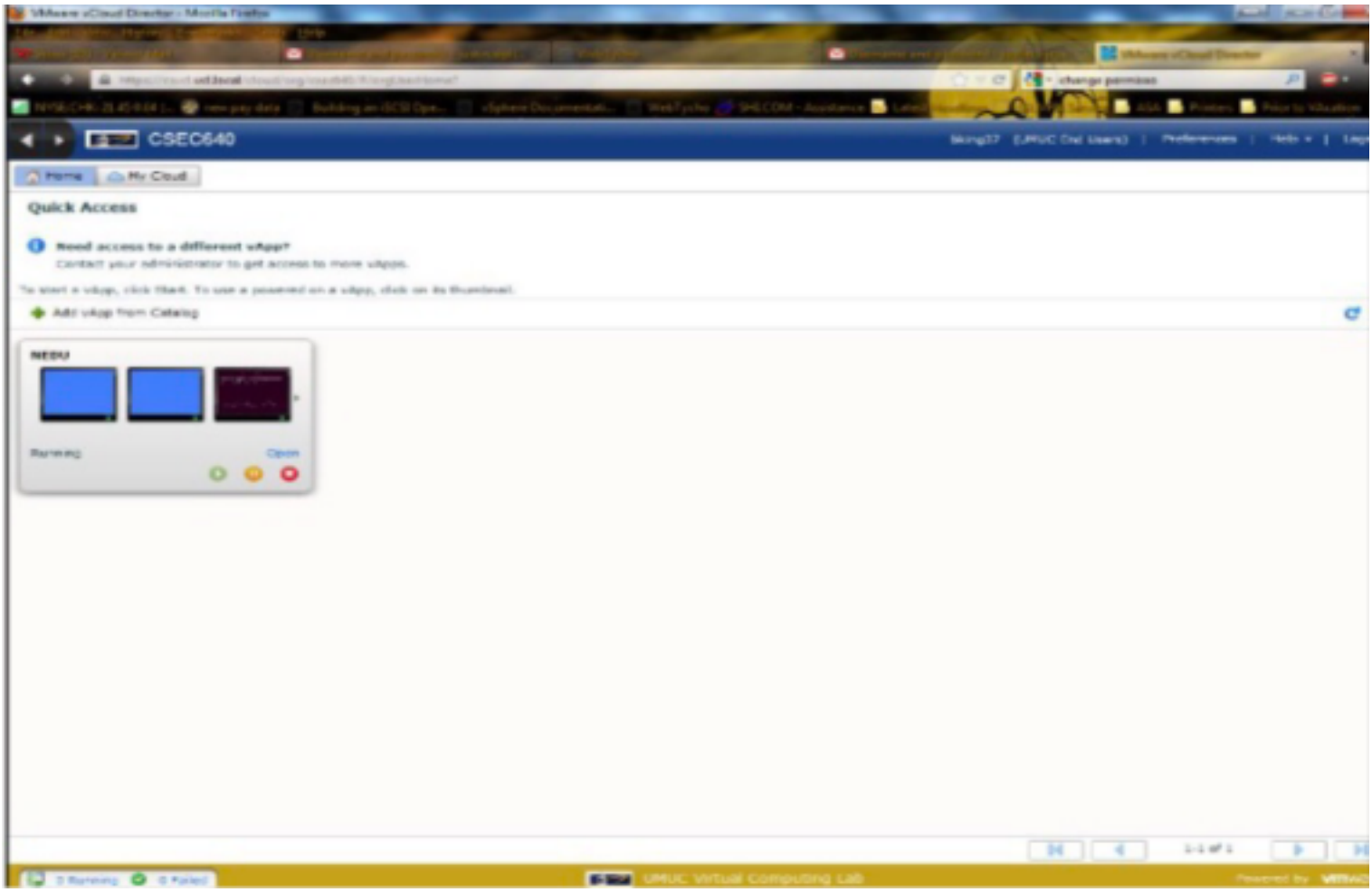


Fig4: Loading a Set of Virtual Machines (V2-Window Server, V3-Linux, and V4- Linux) via web interface. The MENU panel shows three consoles for V1, V2, and V3.

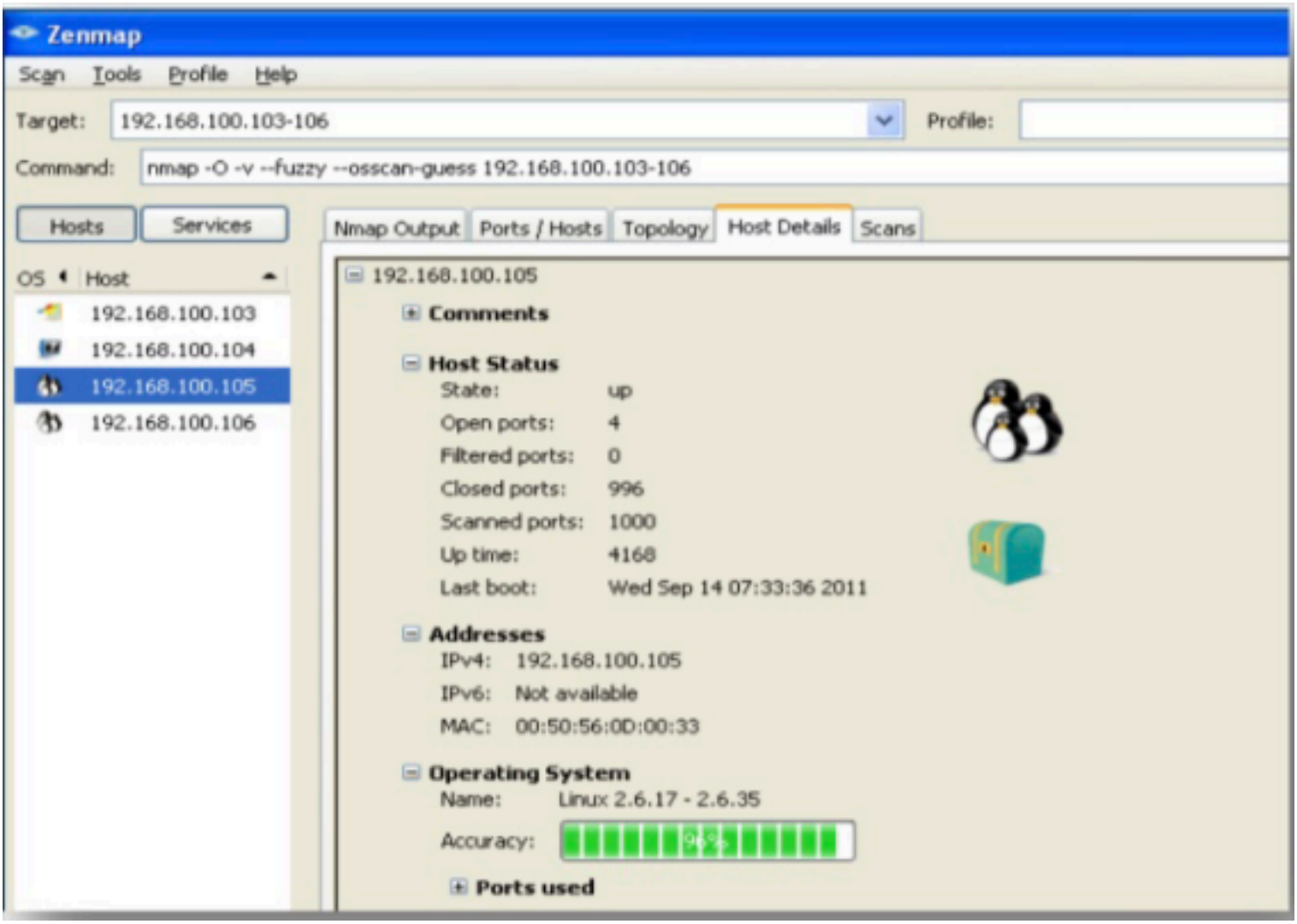


Fig 5: Nmap - Successful OS Guess Detection (with osscan-guess filter).

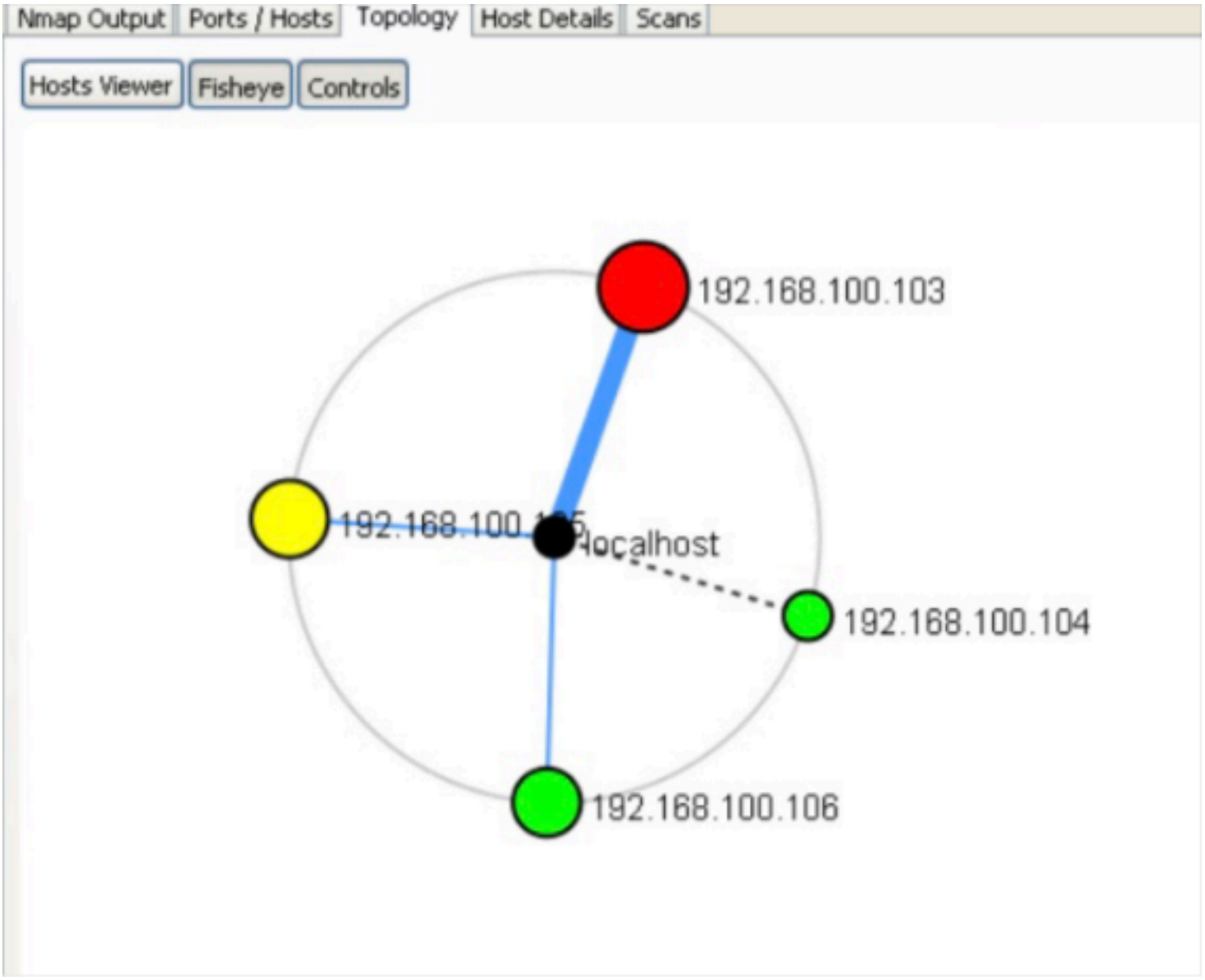


Fig 6: Nmap - Sample Topology Diagram of the Virtual Network.

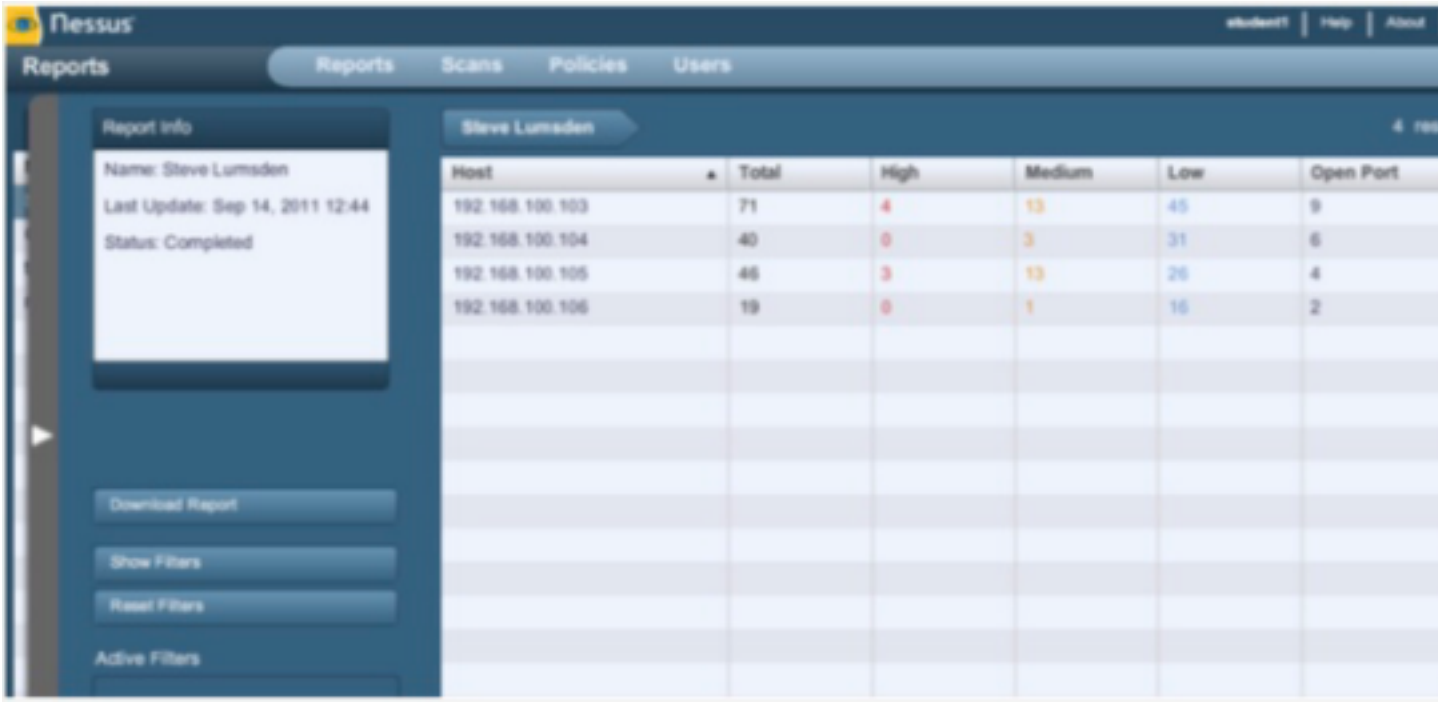


Fig 7: Sample Nessus Report Scan Result from UMUC Virtual Lab.

Hybrid Approach with Dedicated Test Servers

As reported the major downside with UMUC's current virtual cyber lab configuration is performance degradation experienced by users when a number of concurrent users reaches a certain threshold point. This is primarily due to the large number VMs running on each ESXi server, which maximizes CUP and memory usage of the ESXi servers. For instance, for the vulnerability scanning lab, 100 concurrent students mean 400 VMs since four dedicated VMs are assigned to each student. Thus, one way to avoid the serious performance slowdown is to reduce

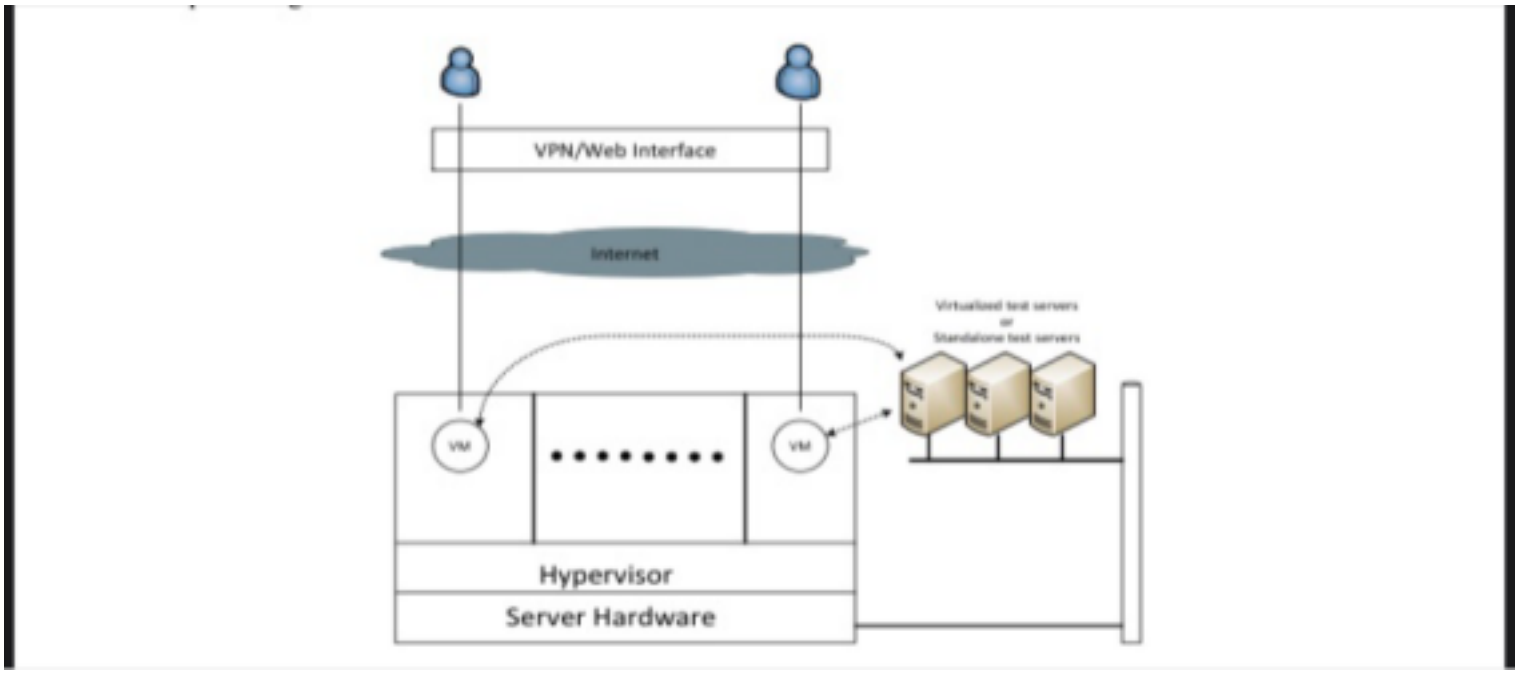


Figure 8: Hybrid Approach: VM Host Servers with Dedicated Standalone Servers.

Desktop Virtualization Approach for Cyber Lab

of Virtual Lab Solutions for Online Cyber Security

APPENDIX A

In this appendix, we show two xml configuration files, which were used to create virtual networks in our KVM, test server. These two xml configuration files were read by libvirt (KVM toolkit) to create two virtual segments.

```
<network>
  <name>net1</name>
  <uuid>5156cb69-58dd-3fd4-a643-13f1dd859327</uuid>
  <forward mode='nat'/>
  <bridge name='virbr1' stp='on' delay='0' />
  <mac address='52:54:00:F4:87:D9'/>
  <ip address='192.168.100.1' netmask='255.255.255.0'>
    <dhcp>
      <range start='192.168.100.128' end='192.168.100.254' />
    </dhcp>
  </ip>
</network>
```

DIGITAL FORENSIC ANALYSIS OF THE PROVIDED ANDROID IMAGE
FOR THE
FINAL CAPSTONE PROJECT – DSA/CYBERSECURIY/2025

OLUWASEUN OJO
DSA-Cyber security Student
joshseuntoin117@gmail.com
+2348135388280

Digital Forensics Investigation Report
Case Title: Forensic analysis of the Android image
Case Number: DSA-CYBERSECURITY-2025
Date of Investigation: June 19-29, 2025
Investigator Name: Oluwaseun Ojo Cyber Security Student (DSA) Client: INCUBATOR HUB (DIGITAL SKILL-UP AFRICA – DSA)

1. INTRODUCTION

This report documents the outcome of a formal investigation into a series of cyber-enabled

fraudulent activities, specifically involving the use of deceptive email correspondence, unsolicited telephone communications, and fictitious online investment platforms, conducted with the intent to unlawfully obtain personal information and misappropriate financial assets from unsuspecting individuals.

Beginning no later than March 17th, 2024 at about 04:19:10 WAT and continuing through at least the month of March, 2024, in the county of Nigeria, the suspect conspired to launch a fake investment platform to lure suspecting victims into investing in a non-existing business venture. From investigation, the suspect, has a long history of cybercrime, through email, telephone and fake investment scams.

This report is made in support of a criminal complaint against, and arrest warrant for, DONALD JACKSON LIVISTONE , also known as (“aka”) “DON,” aka “Sammy”, for violation of the Cybercrime criminal code law of the Federal Republic of Nigeria (Conspiracy to engage in Cybercrime/Scam through fake online Investment platform).

The facts set forth in this report are based upon my personal involvement in this investigation, my review of reports and other documents related to this investigation, my training and experience, and information obtained from other agents, law enforcement officers, and witnesses. This report is intended to show merely that there is sufficient probable cause for the requested complaint and arrest warrant, and does not purport to set forth all of my knowledge of the government’s

investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this report are related in substance and in part only. Unless specifically indicated otherwise, all dates set forth below are “on or about” the dates indicated, and all amounts or sums 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

4. EVIDENCE SUMMARY AND FINDINGS

4.1 Devices Investigated

Device Description Serial No. Android Image Provided Android Image Android Image.tar.gz 5. FINDINGS

Acquisition Date

June 22, 2025, 12am

Tool Purpose

- Autopsy/ SleuthKit File system analysis, keyword search, and imaging.

Donald JACKSON LIVISTONE is a Nigerian national living in Nigeria. My investigation has revealed that Don finances his opulent lifestyle through crime, and that he is one of the leaders of a transnational network that facilitates computer intrusions, fraudulent schemes (including BEC schemes), targeting victims around the world in schemes designed to steal hundreds of millions of dollars. Don participated in these fraudulent schemes and money laundering in coordination with multiple co-conspirators, including the persons referred to herein as Coconspirator 1 and Coconspirator

This report discusses several fraudulent schemes involving Don. First, messages found on the Android phone of Donald reflect that Don, Coconspirator 1, and Coconspirator 2, with others, committed fraud/scam that defrauded victims of thousands of money in dollars and other currencies.

Other communications between Donald(Don) and Coconspirator 1 indicate that, in addition to these schemes,Donald(Don) and Co-conspirator 1 conspired to launder tens, and at times

hundreds, of millions of dollars that were proceeds of other fraudulent schemes and computer intrusions, including a fraudulent scheme.

Analysis of Coconspirator 1's Android and other online accounts showed that Coconspirator 1 operated and tasked money mule crews for a number of fraudulent schemes, Analysis also showed that Coconspirator 1 communicated with the Nigerian phone number +2348032111669 ("Phone Number 1") about multiple fraudulent schemes and money laundering. As described below, Phone Number 1 was one of the phone numbers DONAD (DON) used during 2024 and 2025.

Coconspirator 1's Android phone listed Phone Number 1 (+2348032111669) with the contact name "DON." The phone also contained a URL for a website set up by "Sam's" co- conspirator; https://apyeth.gifts/

Searches of Phone Number 1 and the contact name "DON" in Coconspirator 1's Android phone revealed messaging conversations between "DON," using Phone Number 1, and Coconspirator 1.

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

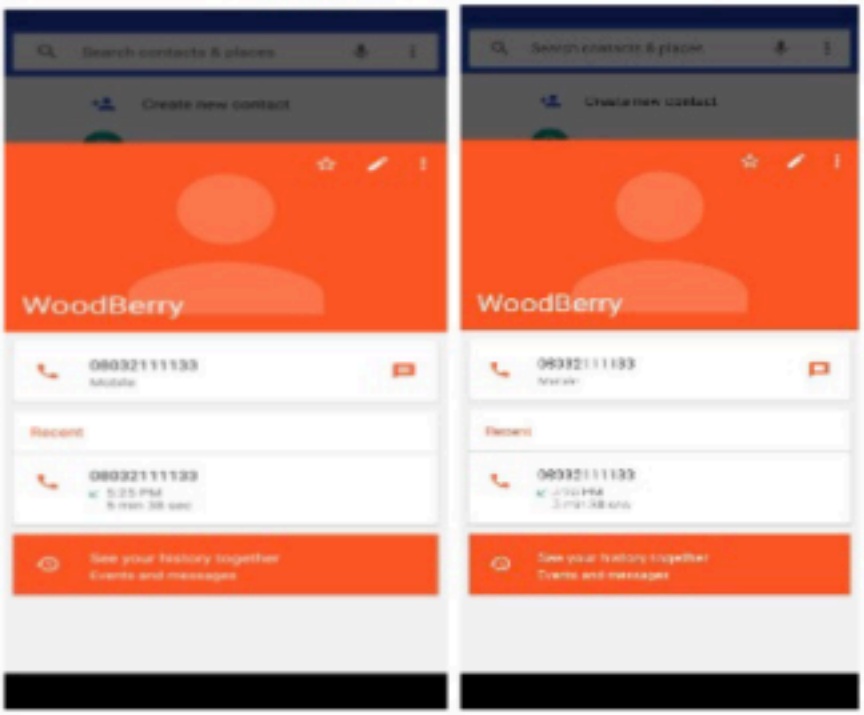
SMS messages report

	Date	MSG ID	Thread ID	Address	Contact ID	Date sent	Read	Type	Body	Service Center	Error code
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 16AtGJbaxL2kmzn4mW5ocpT2ysTWsmacWn.		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 16AtGJbaxL2kmzn4mW5ocpT2ysTWsmacWn.		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: 1K1KMHpyuJHQRbhzKHyltbyaJsQYxSaZCm		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 affiliates 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 oma 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
3/16/2024 20:45	+15555215554	971565505984	Outgoing	216	United Arab Emirates	US	0
3/16/2024 20:49	+15555215554	8032111669	Outgoing	109		US	0
3/16/2024 20:51	+15555215554	8032111225	Outgoing	169		US	0
3/17/2024 2:54	+15555215554	8032111669	Outgoing	0		US	0
3/17/2024 16:17	+15555215554	8032111225	Missed	0		US	0
3/17/2024 16:18	+15555215554	8032111225	Missed	0		US	0
3/17/2024 16:18	+15555215554	8032111225	Incoming	139		US	0
3/17/2024 16:21	+15555215554	8012345678	Incoming	73		US	0
3/17/2024 16:24	+15555215554	8032111669	Rejected	0		US	0
3/17/2024 16:23	+15555215554	971543777711	Outgoing	67	United Arab Emirates	US	0
3/17/2024 16:25	+15555215554	8032111133	Incoming	338		US	0
3/17/2024 16:36	+15555215554	8032111669	Rejected	0		US	0
3/17/2024 16:36	+15555215554	8032111669	Rejected	0		US	0
3/17/2024 16:36	+15555215554	8032111669	Rejected	0		US	0
Call Date	Phone Account Address	Partner	Type	Duration in Secs	Partner Location	Country ISO	Deleted



(C) Contact lists

(C) **Contact lists**

Contacts report

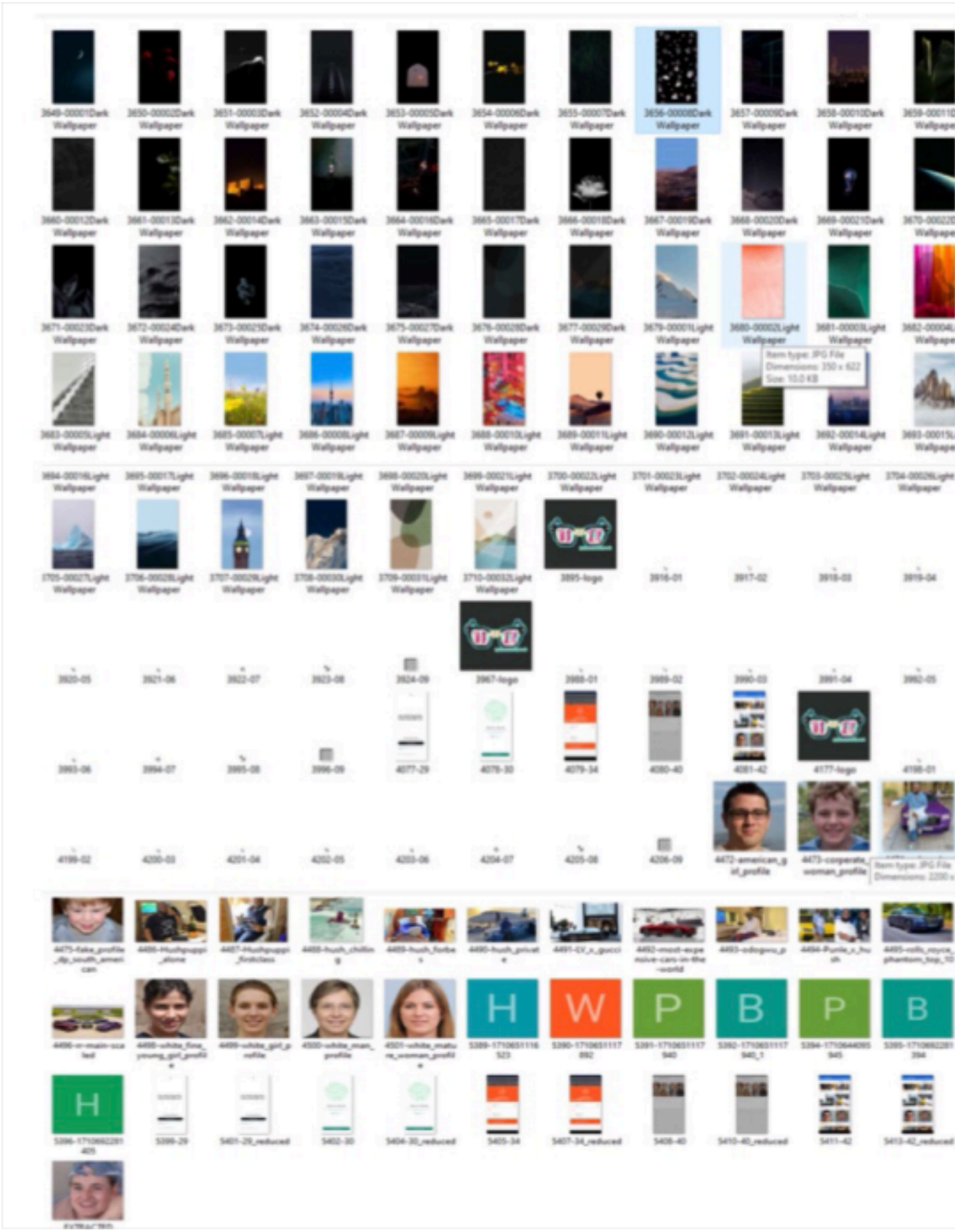
Total number of entries: 7

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	310120001	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) 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
Recommendation: Enhance Mobile Device Security Protocols and Implement Mobile Device Management (MDM)
Context from Analysis:
A forensic analysis was conducted on the provided Android image belonging to a cybercrime suspect, using Autopsy. The investigation focused on uncovering digital evidence related to fraudulent online investment schemes. The following findings were extracted from the device image:

- App Artifacts and Side-loaded APKs:
- A fake investment URL (https://apyeth.gifts/), was recovered from the message log.
  Browser History and Chat Evidence:
- Cryptocurrency wallet addresses found in message log history and browser sessions matched addresses reported in previous scam reports.
- System Artifacts and Intentional Data Deletion:

Actionable Recommendations:

- Preserve and Expand Investigation through Multi-Device Correlation:
  Cross-reference recovered wallet addresses and app signatures with international fraud databases (e.g., Scamwatch, Chainalysis).
- Correlate chat records and call logs with known victim reports and initiate digital attribution to other devices or co-conspirators.
- Develop Custom Signatures for Fraudulent App Detection:

Work with mobile security vendors or CERT units to fingerprint the malicious investment app (e.g., package name, icon hash, certificate).

- Distribute to mobile AV engines and app stores for broader protection and future automatic detection.
- Strengthen Legal and Investigative Collaboration:

- Submit recovered evidence to financial cybercrime units and request subpoenas for cryptocurrency exchange data tied to recovered wallet addresses.

Public Advisory on Emerging Mobile Fraud Trends:

- Use this case as a foundation to publish a fraud alert for the public about fake investment apps that mimic legitimate platforms.
- Include screenshots of the fraudulent app and scam messages (redacted for privacy) in outreach campaigns or press releases.
- Encourage Financial Institutions and Mobile Platforms to Improve App Vetting:
  - Advocate for stricter vetting and digital signature verification of investment apps.
  - Recommend collaboration between law enforcement and mobile platforms (Google, telecoms) to detect and block high-risk side-loading behavior.

8. CONCLUSION

The forensic investigation confirms that an Donald, who is known for operating regular online scam with different names and online social media accounts, was planning to launch another fraudulent online fake investment scam, which according to him, was going to be one of its kind. Because of the audience he was targeting in his new online fake investment scam.

The investigation also shows that “Donald” was highly connect with well-known successful internet fraudsters, the likes of “Hushpuppi” and “Woodberry”. Also, the investigation shows that “Donald” was not acting alone, as he had other conspirators working together in achieving these online scam schemes.

The findings from the suspect’s Android device provide direct digital evidence of fraudulent intent and execution—ranging from the development and deployment of fake investment apps to communication with victims. This evidence not only supports criminal prosecution but also presents an opportunity for broader cyber security and fraud-prevention efforts targeting the mobile ecosystem.

In summary, this incident highlights several critical gaps, this incident indicates several critical gap in the security of the cyber space. That individuals like “Donald” still exist out there, calls for a more robust and aggressive protection of the cyber space and the citizens by extension. Immediate remediation and long-term strategic improvements are necessary to mitigate the risks of recurrence and to restore stakeholder trust.