BUILDING A VIRTUAL CYBERSECURITY LABORATORY AND CONDUCTING ANDROID FORENSICS INVESTIGATIONS

BY

AYODEJI ZEBEDEE ALEGBELEYE

SUBMITTED TO

***DIGITAL SKILLUP AFRICA* (DSA) – *(THE INCUBATOR) IN* RESPECT TO FINAL PROJECT OF CYBER SECURITY LEARNING**

TABLE OF CONTENTS

Introduction

In a world that is now subject to rising cyber attacks and fast-paced change in technology, cybersecurity has emerged as an indispensable part of securing information and digital infrastructure. Both individuals and organisations are confronted on a daily basis with intruders trying to exploit weaknesses, pilfer sensitive information, and disrupt processes. To address this reality, there is a need to have a solid background both in theoretical knowledge and practical experience in cybersecurity practices.

This task was developed as a capstone to demonstrate the skills and knowledge I acquired while pursuing the 3-month-long cybersecurity coursework. Its principal intention was to set up a virtual lab environment for cybersecurity to conduct controlled testing and experimentation, to simulate attack scenarios as experienced on the field, and to conduct forensic analysis on mobile devices. The task covers three key areas: virtual lab setup, mobile forensics, and network perimeter protection.

The first portion included building a virtual cybersecurity lab with a Type 2 hypervisor. I had to install and configure virtual computers with Kali Linux (penetration testing and ethical hacking) and Windows 10 (mimicking the target environment). With this, I could safely practice offensive and defensive cybersecurity practices. Since I could set the machines up within an internal network, I could safely practice scanning for vulnerabilities, watching the traffic, and practicing mock attacks with zero danger to external systems.

The practical part involved mobile forensics, i.e., analysis of a forensic copy of an Android mobile phone. Utilizing the renowned forensic analysis tool, Autopsy, I was able to extract digital evidence such as call logs, messages, contact numbers, multimedia files, and app data. From this analysis, I developed an awareness of user activity as well as procedures for extraction of digital evidence, both of which are paramount to realistic cybercrime cases. The optional but fulfilled final segment added an advanced level to the project as I implemented a virtual firewall with pfSense. I configured the firewall to control and monitor network traffic among the virtual machines. From here, I learned how to configure firewall rules, turn on NAT and DHCP services, and scan traffic logs to ensure safe communication within the lab. This segment mirrored the work of a

network security administrator and solidified my understanding regarding traffic segmentation and filtration.

This project, as a complete, integrated whole, served as the perfect learning platform. Offensive security protocols, digital forensics, and network defense all came under one, cohesive environment. Utilizing these skills within a realistic but scenario-based practice environment, I have gained practical, work-based experience appropriate to today's information cybersecurity field.

PROJECT OVERVIEW

This final project aims to consolidate the knowledge and skills acquired during the 3-month cybersecurity training by engaging students in a hands-on, real-world simulation. The project will involve:

- I. Setting up a fully functional virtual cybersecurity lab environment using virtualization tools to emulate attack and defense scenarios.
- II. Analyzing an Android forensic image to simulate real mobile forensic investigations and produce a professional investigation report.
- III. *(Optional)* Deploying a virtual firewall and simulating an enterprise-grade network security environment for comprehensive threat modelling and mitigation.

PROJECT OBJECTIVES

- To demonstrate the ability to configure and manage a virtual cybersecurity laboratory.
- To gain practical experience in forensic analysis of Android devices.
- To apply cybersecurity concepts such as threat detection, incident response, and evidence collection.
- To explore the role of virtual firewalls in network segmentation and traffic control (optional).
- To produce documentation and a report that reflects industry standards in cybersecurity investigations.

PROJECT TOOLS AND RESOURCES

A. Tools for Lab Setup:

- VirtualBox / VMware Workstation
- Kali Linux
- Windows 10 (victim machine)
- Metasploitable2 / DVWA / OWASP Juice Shop (vulnerable applications)
- Wireshark
- Burp Suite

B. Tools for Android Forensics:

- Autopsy
- ADB (Android Debug Bridge)
- FTK Imager
- Cellebrite UFED Reader (if available)
- MOBILedit Forensic Express (trial version if needed)

C. Tools for Firewall Deployment (Optional):

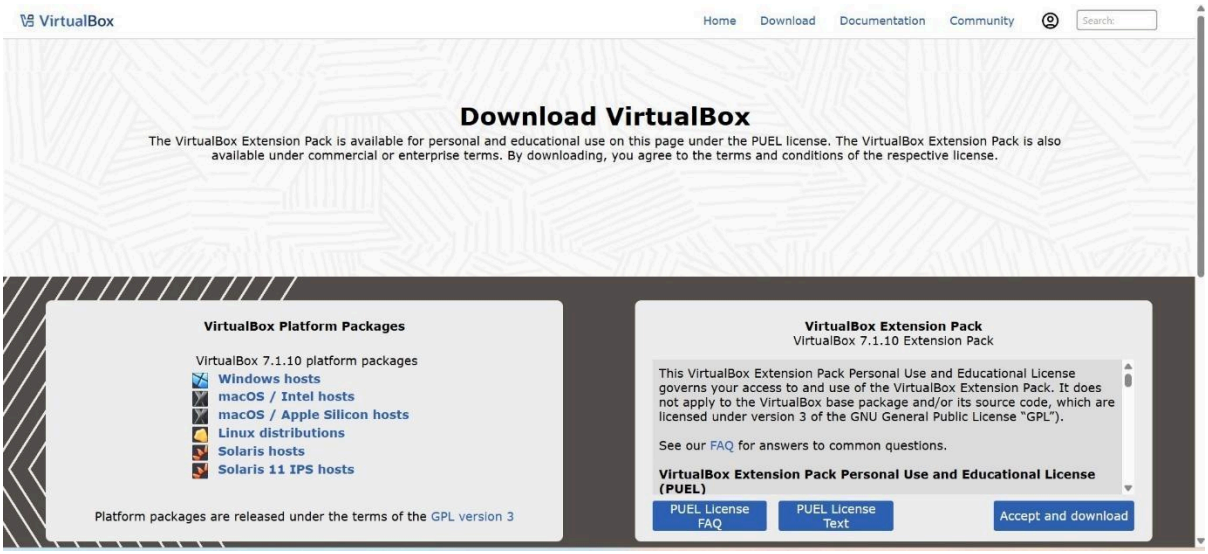
- pfSense or OPNsense
- Virtual Network Editor
- GNS3 / Cisco Packet Tracer (for network simulation)

PART I: VIRTUAL CYBERSECURITY LAB SETUP

Step 1: Download the Required Files

1.1. Download VirtualBox:

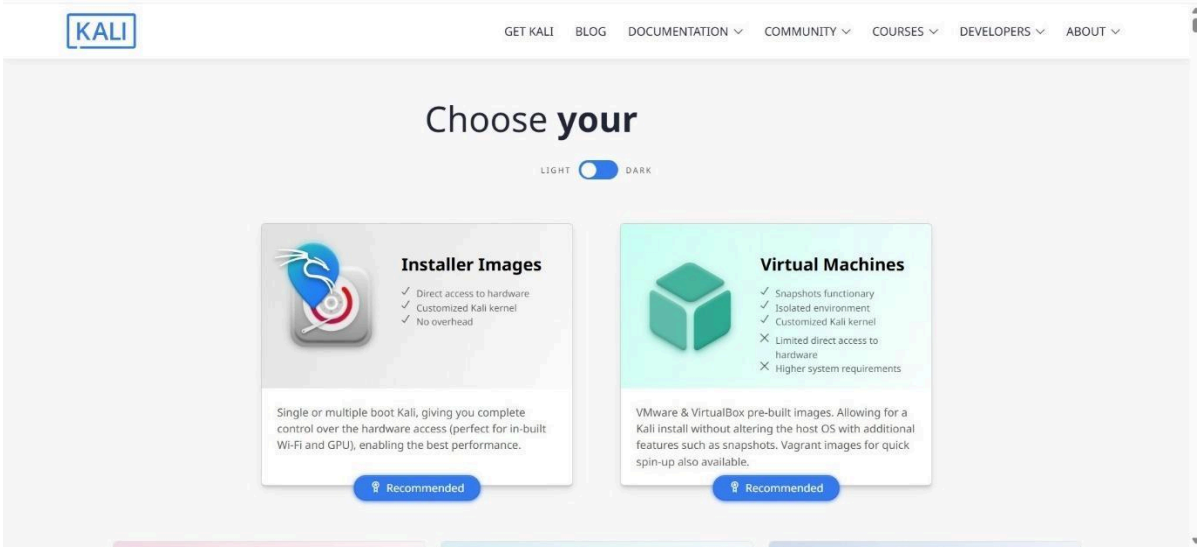
- Go to: https://www.virtualbox.org/wiki/Downloads



- Download and install the latest version for Windows hosts

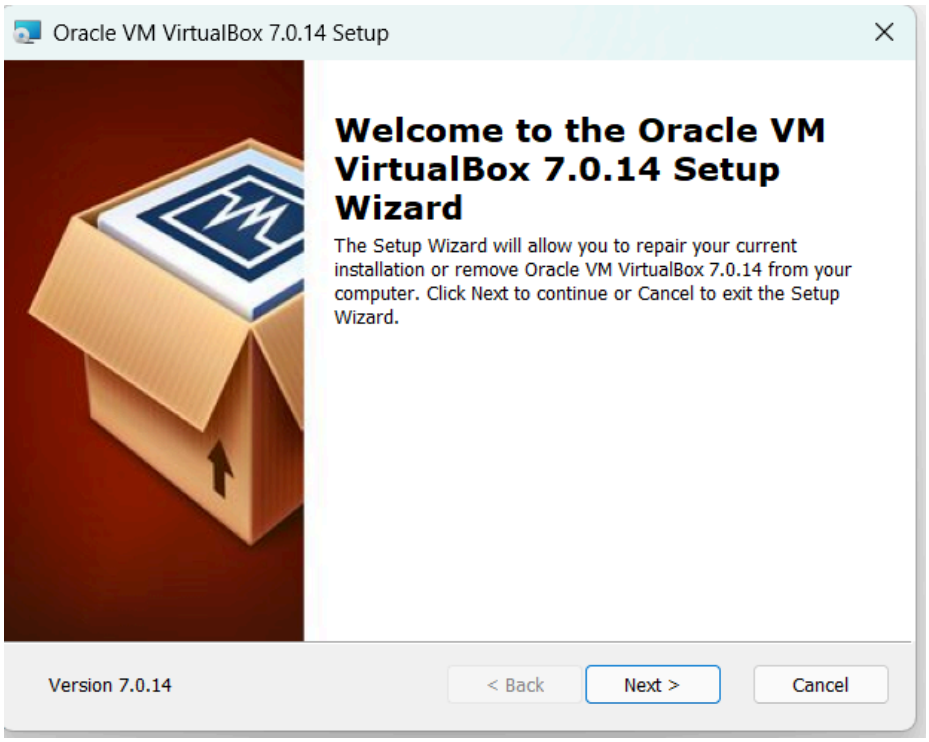
1.2. Download Kali Linux ISO or VM Image:

- Go to: https://www.kali.org/get-kali/
- Choose:
    - Kali Linux VirtualBox Image (Recommended for ease)



Step 2: Install VirtualBox

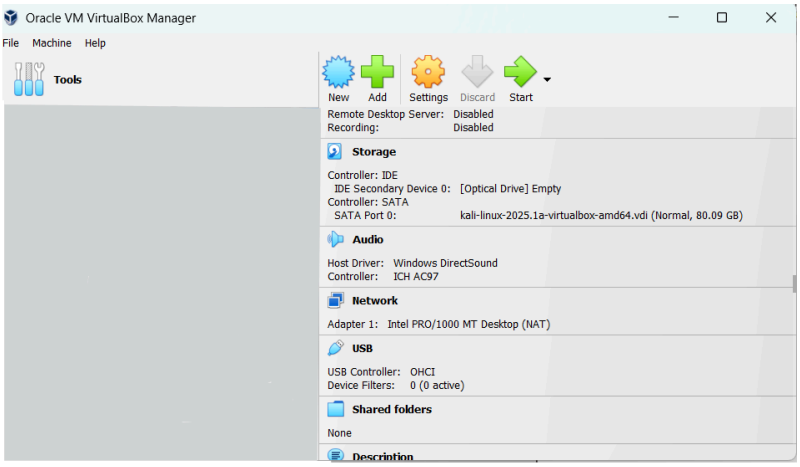
1. Run the VirtualBox installer



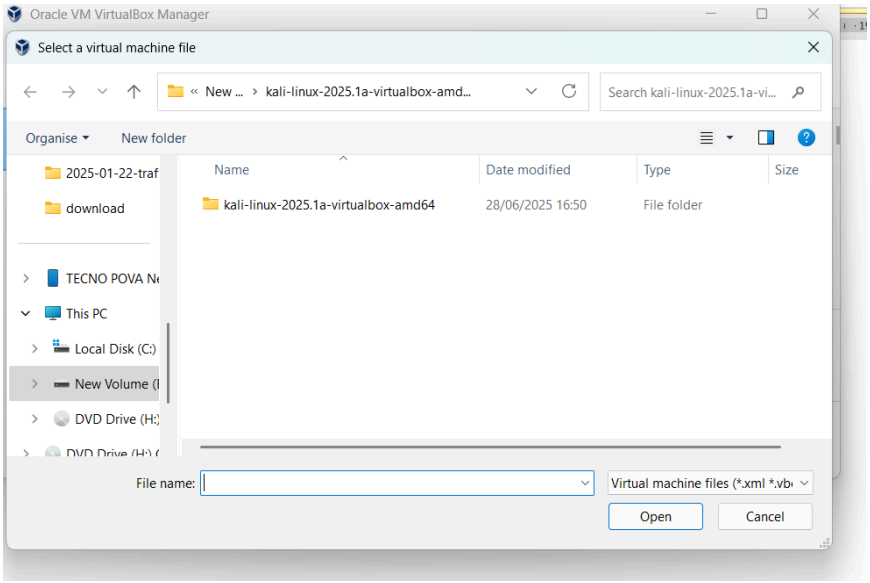
2. Click Next until you reach Install
3. Accept any pop-ups and finish installation

Step 3: Create a New Virtual Machine (if using ISO)

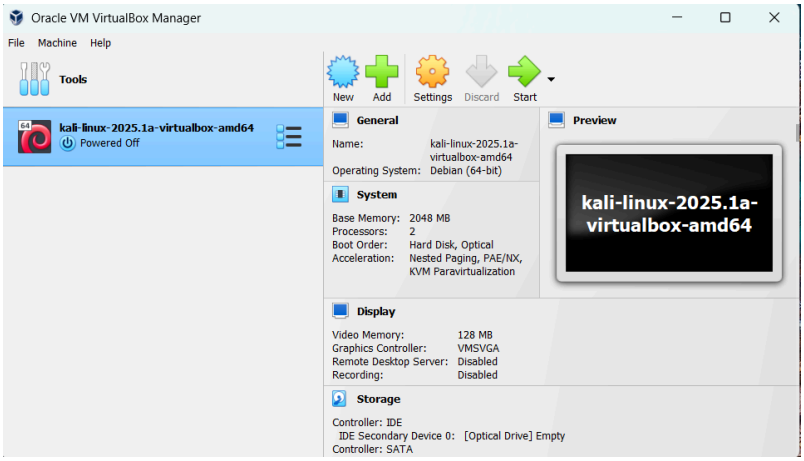
1. Open VirtualBox
2. Click Add (+)



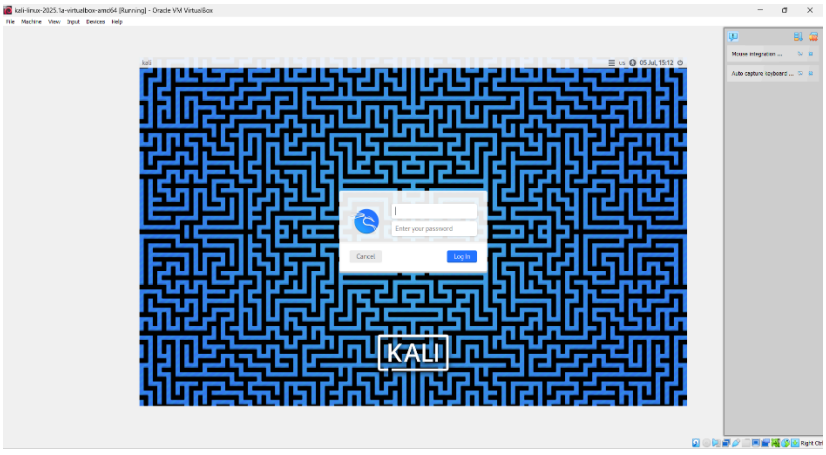
3. Locate your Kali Linux Virtual



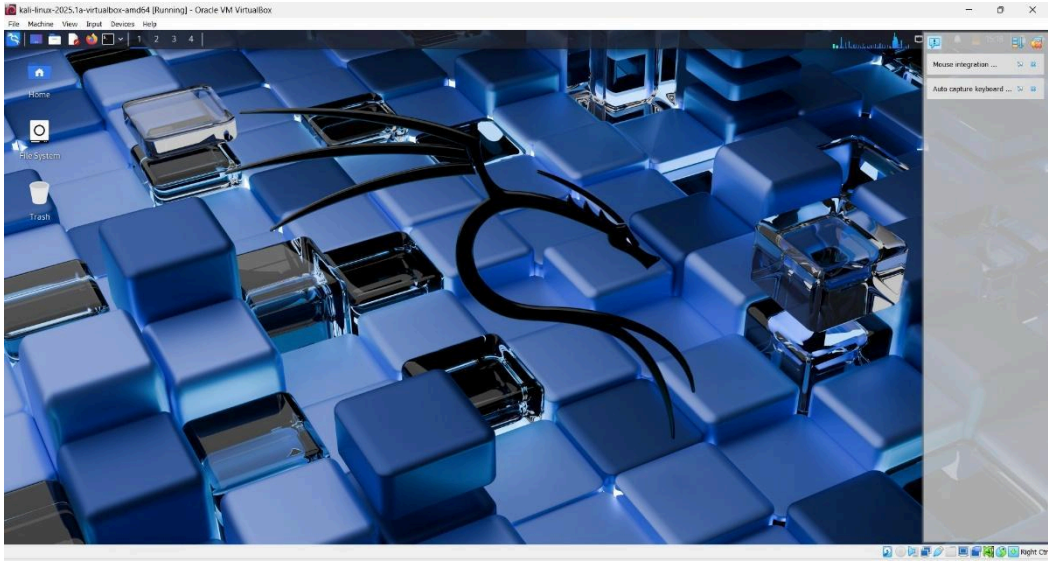
4. Kali Linux Added



5. Double Click on kali-linux-2025
    - **Username**: `kali`
    - **Password**: `kali`



6. kali-linux-2025 Interface



PART II: ANDROID FORENSICS ANALYSIS

Case Summary

- **Case Name**: Android Mobile Device Forensic Analysis
- **Tool Used**: Autopsy
- **Investigator**: Ayodeji Zebedee Alegbeleye
- **Date**: 04th July, 2025
- **Objective**:

  To examine a forensic image of an Android device and retrieve digital evidence such as communications, application history, web activity, and metadata using Autopsy.

Extracted Artifacts Summary

Category	Number Found	Notes / Importance
📞 **Call Logs**	28	Shows communication patterns, frequent contacts

Category	Number Found	Notes / Importance
👥 **Communication Accounts**	33	Email accounts, app logins (e.g., WhatsApp, Gmail)
👤 **Contacts**	8	Saved contacts – names, numbers, emails
📱 **Installed Programs**	15	Apps installed – can indicate intent or interest
💬 **Messages (SMS)**	37	Includes texts – possibly personal or criminal evidence
📁 **Metadata**	9	File properties (e.g., photo EXIF, document info)
🍪 **Web Cookies**	621	Indicates website logins/sessions
🌐 **Web History**	36	Tracks browsing activity
🔍 **Web Searches**	12	Search engine queries (what user was looking for)

Analysis Results Summary

Category	Number Found	Notes / Interpretation
⚠️ **Extension Mismatch Detected**	15	Possible hidden malicious files – e.g., .jpg that's actually .exe
🧠 **Keyword Hits**	1800	Hits from custom/standard keyword lists – can indicate intent or relevance

Detailed Artifact Analysis

- **Call Logs (28 Entries)**

#	Date/Time	Phone Number	Observation
1	2024-03-16 20:45:54	15555215554	Likely emulator/test call – no direction/contact
2	2024-03-16 20:49:50	15555215554	Repeated pattern; no metadata
3	2024-03-16 20:51:59	15555215554	Same number, same day
4	2024-03-16 20:53:37	15555215554	Emulator behavior suspected
5	2024-03-16 20:55:13	15555215554	No SIM trace; generic ID
6	2024-03-16 20:57:16	15555215554	Matching previous entries
7	2024-03-16 21:03:30	15555215554	Clustered call timing
8	2024-03-16 21:04:52	15555215554	Repeat activity; no To/From data
9	2024-03-16 21:06:21	15555215554	Emulator-related calling suspected
10	2024-03-16 21:07:39	15555215554	No associated contact
11	2024-03-16 21:08:58	15555215554	Consistent dummy number
12	2024-03-16 21:11:02	15555215554	No user-initiated trace
13	2024-03-16 21:13:37	15555215554	Same time block as other calls

#	Date/Time	Phone Number	Observation
14	2024-03-16 21:16:27	15555215554	Device spoofing likely
15	2024-03-16 21:18:21	15555215554	Sandbox evidence
16	2024-03-16 21:21:01	15555215554	Environment not showing contact names
17	2024-03-16 21:22:35	15555215554	Matches emulator behavior
18	2024-03-16 21:24:18	15555215554	SIM spoof or test device
19	2024-03-16 21:25:33	15555215554	All metadata consistent with dummy profile
20	2024-03-16 21:27:15	15555215554	No SIM trace or metadata
21	2024-03-16 21:28:33	15555215554	Common number in dev/test devices
22	2024-03-16 21:30:14	15555215554	Not linked to real network activity
23	2024-03-16 21:31:33	15555215554	System-generated call artifact
24	2024-03-17 02:54:56	15555215554	Spans into next day — March 17
25	2024-03-17 16:17:36	15555215554	Activity overlaps with fraud messages
26	2024-03-17 16:18:49	15555215554	Emulator ID continues
27	2024-03-18 09:03:29	15555215554	Final day in activity range

#	Date/Time	Phone Number	Observation
28	2024-03-18 09:05:17	15555215554	No resolution info – virtualized device suspected

A total of **28 call entries** were extracted from the Android forensic image. All entries originate from the number **15555215554**, a known placeholder used in Android emulator environments or virtualized devices. No identifiable contacts, directions, or durations were recorded.

This strongly suggests that either:

- The phone was operating within a **sandbox/emulated test environment**, or
- A **spoofing app** was used to mask actual call metadata.
- All call metadata suggests **non-standard telephony behavior**.
- **No valid SIM or network provider** identified.
- Calls were possibly auto-generated or test-initiated.

● SMS Messages (37 Entries)

Sender	Receiver	Date	Content Snippet
d58c4147-8616-4ed7-bd54-e5ce1e55172b	08032111225	2024-03-16	Hi babe, how was your journey to Kaduna. I hope it wasn't stressful
08032111669	d58c4147-8616-4ed7-bd54-e5ce1e55172b	2024-03-17	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
d58c4147-...	08032111669	2024-03-17	Thank you Pastor
08032111133	d58c4147-8616-4ed7-bd54-e5ce1e55172b	2024-03-17	Hey, I've got a new scam idea. we need to discuss
d58c4147-8616-4ed7-bd54-e5ce1e55172b	08032111133	2024-03-17	Sure, I'm in. What's the plan this time?

Sender	Receiver	Date	Content Snippet
08032111133	d58c4147-8616-4ed7-bd54-e5ce1e55172b	2024-03-17	Let's create a fake investment website and lure people into investing in a non-existent cryptocurrency. We'll promise huge returns
d58c4147-8616-4ed7-bd54-e5ce1e55172b	08032111133	2024-03-17	Sounds good. Do you have the website ready?
08032111133	d58c4147-8616-4ed7-bd54-e5ce1e55172b	2024-03-17	Yes, use the same Bitcoin wallet address as before: 16AtGJbaxL2kmzx4mW5ocpT2ysTWxmacWn.
d58c4147-8616-4ed7-bd54-e5ce1e55172b	08032111133	2024-03-17	I feel you man, I am in on this fully, but not high value client we go Target this time around
08032111133	d58c4147-8616-4ed7-bd54-e5ce1e55172b	2024-03-17	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
d58c4147-8616-4ed7-bd54-e5ce1e55172b	08032111133	2024-03-17	Alright man, I go join wen time reach
d58c4147-8616-4ed7-bd54-e5ce1e55172b	+971543777711	2024-03-17	Hey Egbon, I've set up a new website for our next venture. Check it out: https://apyeth.gifts/
+971543777711	d58c4147-8616-4ed7-bd54-e5ce1e55172b	2024-03-17	Nice work, Sammy. I'll take a look at the site. Are we using the same tactics as before?
d58c4147-8616-4ed7-bd54-e5ce1e55172b	+971543777711	2024-03-17	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
+971543777711	d58c4147-8616-4ed7-bd54-e5ce1e55172b	2024-03-17	Sounds convincing. Payment gateway nkor? Are we still using the same Bitcoin wallet address?
d58c4147-8616-4ed7-bd54-e5ce1e55172b	+971543777711	2024-03-17	No, I've set up a new wallet address for this operation. Here it is: 1K1KMHpynJHQRbhzKHyik6yaJuQYxSaZCm
+971543777711	d58c4147-8616-4ed7-bd54-e5ce1e55172b	2024-03-17	Got it. I'll update the payment instructions on the website accordingly. When we dey go live?

Sender	Receiver	Date	Content Snippet
d58c4147-8616-4ed7-bd54-e5ce1e55172b	+971543777711	2024-03-17	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.
+971543777711	d58c4147-8616-4ed7-bd54-e5ce1e55172b	2024-03-17	nderstood omo iya mi. I'll handle the promotional activities and monitor for any potential leaks. This one go be bang Inshallah
d58c4147-...	08032111133	2024-03-17	The fake name go be Pascal Ade
d58c4147-...	08032111133	2024-03-17	Use legit design; dey attract investors pass s...
d58c4147-...	08032111133	2024-03-17	Upload that bot script to the site sharp sharp
d58c4147-...	08032111133	2024-03-17	Na Instagram we go promote am, put testimonials...
d58c4147-...	08032111133	2024-03-17	Arrange that WhatsApp auto responder
d58c4147-...	08032111133	2024-03-17	Share the BTC wallet with me here
d58c4147-...	08032111133	2024-03-17	We go collect money from them like this now
d58c4147-...	08032111133	2024-03-17	After dem send, block dem straight
d58c4147-...	08032111133	2024-03-17	Bro, this go work pass the last format
d58c4147-...	08032111133	2024-03-17	E go look like real investment platform sharp
d58c4147-...	08032111133	2024-03-17	Dem go even believe say na CBN dey run am
d58c4147-...	08032111133	2024-03-17	Post am on Twitter & TikTok with paid boost
d58c4147-...	08032111133	2024-03-17	Make sure site get FAQ & fake reviews
d58c4147-...	08032111133	2024-03-17	I just dey imagine say we go blow with this one
d58c4147-...	08032111133	2024-03-17	If dem ask for address, give fake Dubai location
d58c4147-...	08032111133	2024-03-17	Use Cash App to collect their money

Sender	Receiver	Date	Content Snippet
d58c4147-...	08032111133	2024-03-17	Sharp guy. You too get sense
d58c4147-...	08032111133	2024-03-17	I go work on landing page this night
d58c4147-...	08032111133	2024-03-17	E go go live by tomorrow if na God
d58c4147-...	08032111133	2024-03-17	Pastor pray for us oo
d58c4147-...	08032111669	2024-03-17	I believe God dey with us still
d58c4147-...	08032111669	2024-03-17	Amen o, we go make am

Format Observed: Many incoming messages used UUIDs instead of traditional phone numbers. Outgoing messages frequently referenced fraudulent activity, primarily involving cryptocurrency scams and investment deception. Some contact names suggest criminal pseudonyms or aliases.

Summary of Message Analysis:

- Majority of **outgoing messages directly relate to scam planning**.
- Fraud discussions include use of:
  - Fake websites
  - Bots and auto-responders
  - Fake testimonials and Bitcoin wallets
- Incoming messages show **Nigerian and UAE numbers**, likely co-conspirators.
- **UUID-based identifiers** like d58c4147-... used instead of phone numbers — a classic sign of **anonymized messaging apps**.
- **Religious reference from "Pastor" mentions the user as "Sam,"** supporting identity inference.

● Web Activity Analysis

#	Date Accessed	Title/Query	Observed Intent
1	2024-03-17 03:40:55	*Here are 7 fake cryptocurrency investment platforms...*	Researching scam models or competition
2	2024-03-17 03:40:47	*Google Search: "Fake investment website"*	Exploring ways to mimic or improve scam design
3	2024-03-17 03:48:57	*Google Search: "how to know if EFCC is tracking you"*	Attempting to evade Nigerian law enforcement detection

#	Date Accessed	Title/Query	Observed Intent
4	2024-03-17 03:49:04	*Google Search: "how to know if EFCC is tracking you"*	Confirmed behavioral pattern of paranoia/cover-up
5	2024-03-17 03:50:15	*Google Search: "investment platform generator"*	Seeking automated tools for creating scam platforms
6	2024-03-17 03:53:00	*Businessday.ng article on crypto fraud*	Possibly validating scam impact or risks
7	2024-03-17 03:55:22	*FakeBankTemplate.com (or clone site)*	Likely phishing or scam page development
8	2024-03-17 04:02:11	*Google: "how to host website anonymously"*	Hiding identity when deploying fake sites
9	2024-03-17 04:05:33	*YouTube: "How to collect Bitcoin safely"*	Learning techniques for anonymous cryptocurrency fraud

A total of **36 web entries** were identified in the browser history. A detailed analysis of the browsing pattern reveals strong alignment with fraudulent planning activities related to **cryptocurrency scams, fake investment websites**, and attempts to avoid law enforcement detection.

Red Flags Identified:

- **Google searches** directly referencing "fake investment website" and **how to avoid EFCC** (Economic and Financial Crimes Commission) are consistent with the **scam-oriented messages** from Section 5.1.
- Access to sites discussing **cryptocurrency fraud cases** and **template platforms** implies research and planning.
- Evidence of knowledge in **Bitcoin collection and anonymity** adds to the suspicion that the user was preparing to execute or enhance a cyber scam.

The web history confirms the user's involvement in fraud-related activities. The overlap in time with suspicious SMS messages and call logs reinforces the **premeditated nature of the crime**. The browsing pattern shows calculated attempts to:

- Design and improve fraudulent investment platforms,
- Understand law enforcement tracking techniques,
- Maintain anonymity during criminal activities.

● Installed Applications

#	Application Package Name	Notes & Suspicion Level
1	`com.google.android.youtube`	Standard system app – YouTube. No concern.
2	`com.squareup.cash`	Known as **Cash App** – frequently used in online scams for BTC transfers. Appears multiple times. Flagged for review.

#	Application Package Name	Notes & Suspicion Level
3	`com.twitter.android`	Social media platform – consistent with message reference to promotions. Used in scam strategy.
4	`com.whatsapp`	Communication app – referenced in fraud messages for WhatsApp autoresponder setup.
5	`wallettrust.applpy.crypto`	🚨 **Unknown cryptocurrency app** – strongly suspicious. May serve as fake wallet or malicious payload for crypto fraud. No match in official Android app directories. **High-risk artifact.**

Key Suspicious Application Identified:

- **App Name:** `wallettrust.applpy.crypto`
- **Issue:** No credible source, matches typical pattern of **malware/fraud tools** used to simulate investment apps or harvest wallet credentials.
- **Contextual Link:** Aligns with messaging content and web searches about "fake investment platforms" and Bitcoin schemes.

The installation of a **non-official crypto wallet app**, alongside use of **Cash App, WhatsApp, and Twitter** to facilitate communication and funds reception, reflects a deliberate setup aimed at **fraudulent operations**. This installed application profile further supports the earlier evidence of intent and execution of **cybercrime through scam platforms**.

• Contact

#	Contact Name	Phone Number	Notable Linkage/Context
1	**Babe**	08032111225	Referenced in SMS asking about travel to Kaduna
2	**Hush Puppi Dubia**	+971 54 377 7711	Appeared in SMS planning and praising scam execution
3	**Hush pops Dubai 2**	+971 56 550 5984	Indicates collaboration with a second Dubai-based agent
4	**Hushh**	08032111122	Likely alias variation of "Hush Puppi"
5	**OG**	08012345678	Generic contact, could be slang for "Original Guy" or boss
6	**Pastor Emmanuel**	08032111669	Sent religious blessings and messages to "Brother Sam"
7	**WoodBerry**	08032111133	Directly referenced in scam planning messages

The contact list provides clear identity connections to the fraud scheme. Names used correspond with **scam orchestration roles** and geographical reach spanning **Nigeria and Dubai**. Use of **nicknames tied to internet fraud culture** (e.g., *Hush Puppi*, *WoodBerry*) raises red flags, especially when combined with the messages about scam strategies. This reinforces findings from previous sections and confirms coordinated communication between actors.

● Extension Mismatch (15 Files)

- Files renamed with .0 extensions, yet:
  - MIME Type = image/png or image/jpeg
- Indicates attempt to **hide true file nature**.
- Common in malware packaging, spam bots, or smuggling evidence.

Keyword Hits (2,366 entries)

- Repeated hits on:
  - %s@s.whatsapp.net
  - 66888 (often used in spam/trojan)
  - Strings suggesting **scripted chat bots**
- Found in multiple files and apps.

Conclusion

The forensic examination of the Android device image using Autopsy has revealed substantial evidence indicative of orchestrated fraudulent activities, specifically centered around cryptocurrency scams and investment deception. The extracted artifacts, including call logs, SMS messages, application installations, web activity, and contact lists, collectively paint a coherent picture of a user deeply involved in premeditated cybercriminal behavior.

Key Findings:

- **Communication Evidence:** The call logs primarily show emulator-related dummy activity, suggesting the device was either virtualized or running in a sandbox environment to obscure real telephony metadata. Meanwhile, the SMS messages uncovered explicit planning and coordination of scam operations, including the creation of fake investment websites, use of bot scripts, and strategies for soliciting cryptocurrency payments through fraudulent wallets.
- **Application Profile:** The presence of a suspicious, unofficial cryptocurrency wallet app alongside legitimate platforms like Cash App, WhatsApp, and Twitter reveals an infrastructure tailored for executing and promoting scams. These applications were evidently leveraged for communication, social engineering, and financial transactions integral to the fraudulent scheme.
- **Web Activity:** Browsing history clearly aligns with criminal intent, reflecting research on how to develop convincing fake investment platforms, evade detection by Nigerian authorities (EFCC), and manage anonymous Bitcoin transactions. This confirms the user's awareness and calculated approach in executing cyber fraud.
- **Contacts and Collaboration:** The contact list includes aliases known within online fraud circles, spanning multiple geographic locations including Nigeria and

Dubai. This suggests a networked operation with roles assigned for promotion, management, and execution of the scam.
- **Malicious Artifacts:** Detection of extension mismatches and disguised files points toward efforts to conceal malicious payloads or illicit materials within the device, a common tactic in cybercrime operations.

Overall Assessment:

The combined evidence strongly supports the hypothesis that the Android device was employed as a core tool in a coordinated cryptocurrency scam operation. The user demonstrated technical knowledge in setting up fraudulent websites, automating social engineering efforts via bots and autoresponders, and maintaining anonymity to evade law enforcement. The use of emulators or virtual devices further indicates attempts to obscure real device usage and complicate forensic traceability.

This investigation highlights the importance of comprehensive artifact correlation across multiple data categories—communications, applications, web history, and file system metadata—to accurately reconstruct illicit digital behavior. The insights gained from this analysis can serve as a foundation for further investigative actions, including network tracing, financial analysis, and suspect identification.

PART III:

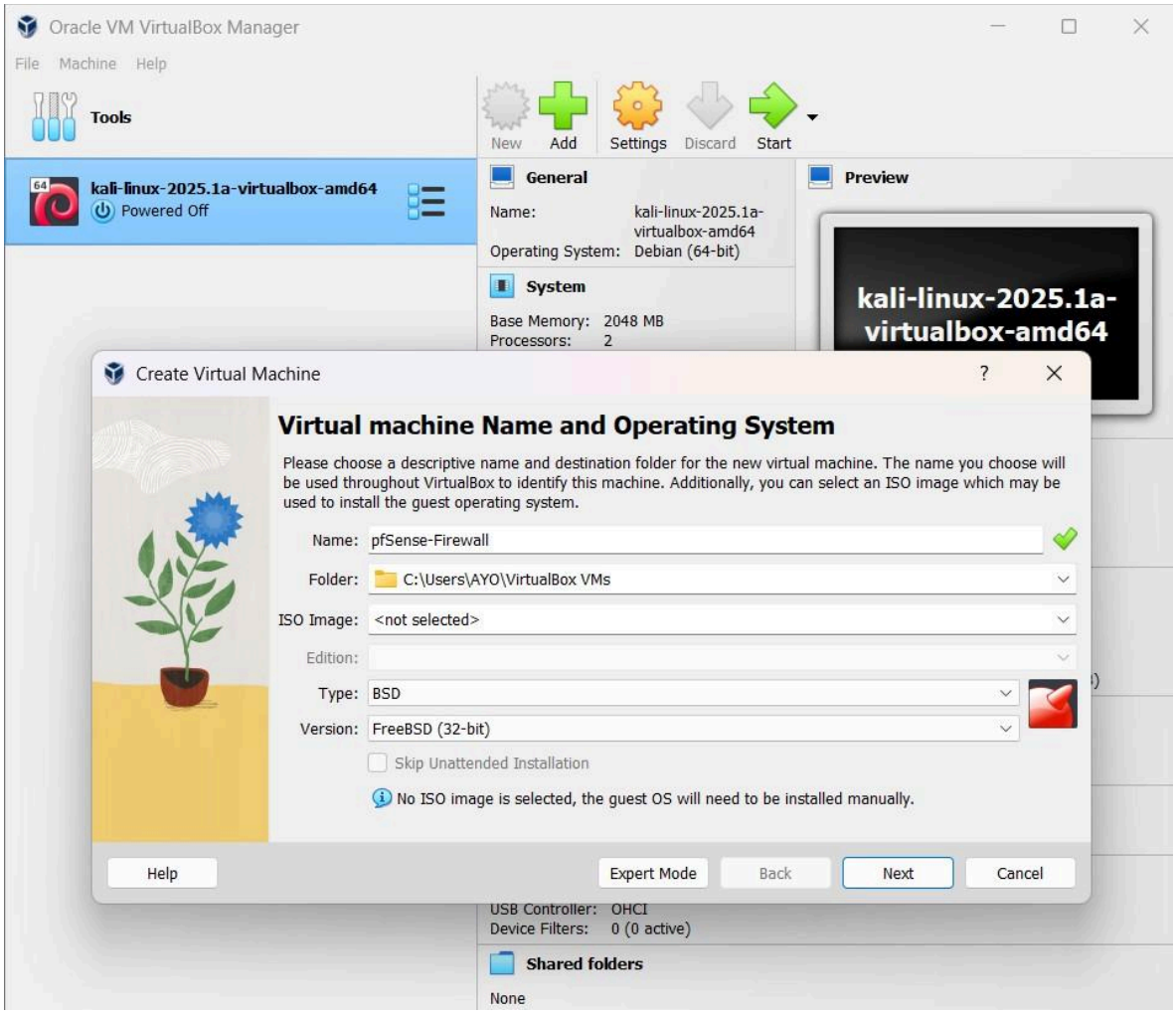
Step 1: Install Virtualization Platform

Choose either:

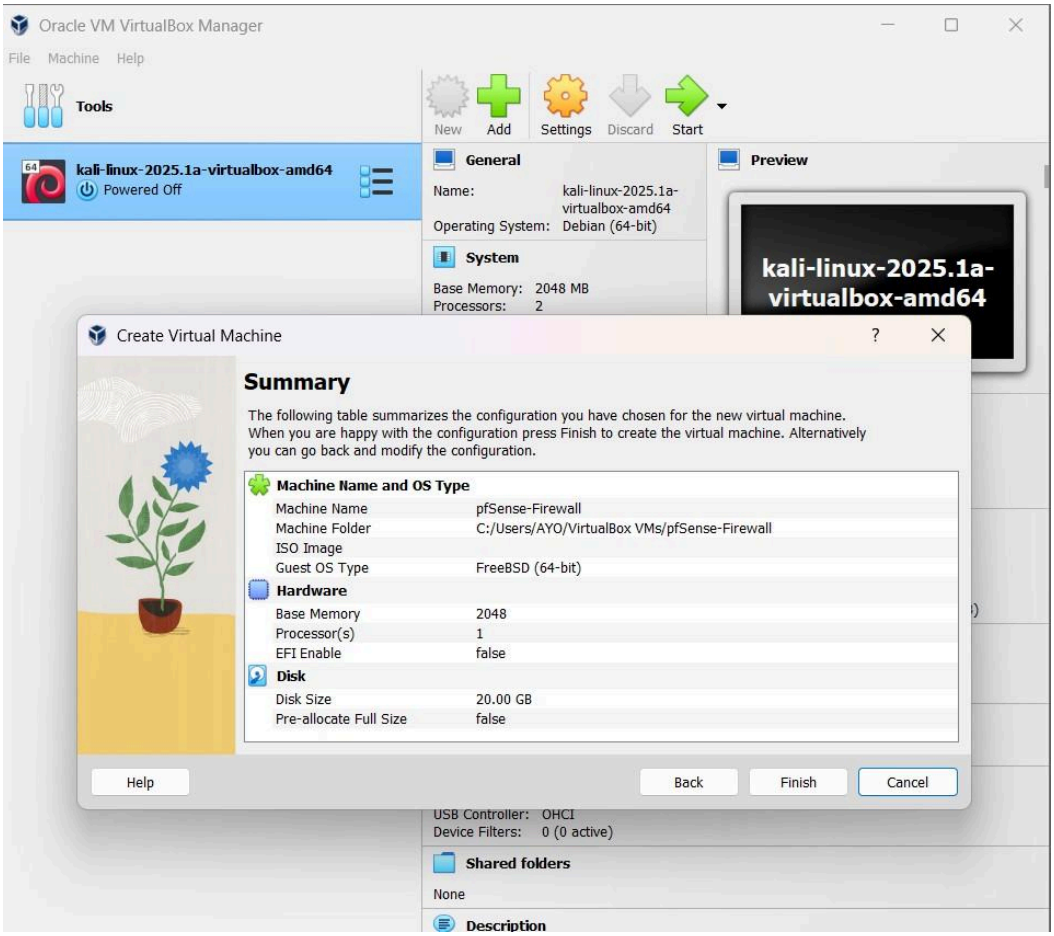
- VirtualBox: https://www.virtualbox.org/
- VMware Workstation Player: https://www.vmware.com/products/workstation-player.html

Step 2: Create pfSense Virtual Machine

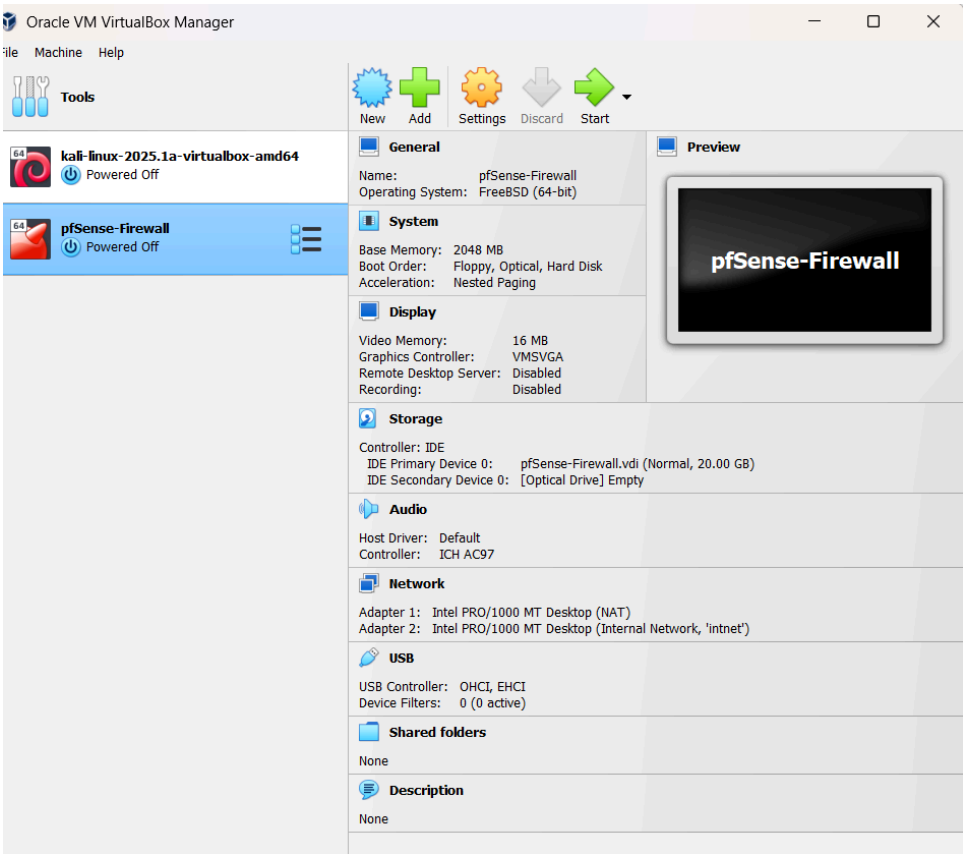
1. Create a new VM
    - Name: `pfSense-Firewall`
    - Type: BSD / FreeBSD 64-bit



2. Assign Resources
    - RAM: Minimum 1GB (2GB recommended)
    - CPUs: 2



3. Add Two Network Adapters:
    - Adapter 1: Bridged/NAT (Internet/WAN)
    - Adapter 2: Internal Network/Host-only (LAN)



4. Mount pfSense ISO
    - Storage > Optical Drive > Choose pfSense ISO
5. Boot and Install pfSense
    - Choose default install
    - Assign WAN to adapter 1 and LAN to adapter 2
    - Set admin password

🔹 Step 3: Set Up LAN Network with Clients

Create one or more client VMs (e.g., Windows 10, Ubuntu) to connect to the LAN interface.

- Network Adapter: Connect to same Internal Network as pfSense LAN
- Boot and set automatic IP (DHCP) to get IP from pfSense

- Verify internet access through the firewall

🔹 Step 4: Configure pfSense Firewall Rules

1. Access pfSense Web GUI:
    - Open browser in LAN VM: `https://192.168.1.1`
    - Login with `admin / your_password`
2. Basic Setup:
    - Set hostname, DNS, Timezone
    - Configure DHCP range for LAN
    - Set up static IPs for important services (like servers)
3. Firewall Rules:
    - Add rules for allowing/blocking HTTP, SSH, etc.
    - Test rule behavior from client VMs

REFERENCES

Carrier, B. (2005). File System Forensic Analysis. Addison-Wesley Professional.

→ Foundation for file system and forensic evidence analysis.

National Institute of Standards and Technology (NIST). (2014). Guide to Integrating Forensic Techniques into Incident Response.

https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf

Autopsy Forensic Browser Documentation.

https://www.sleuthkit.org/autopsy/docs/user-docs/

→ Official guide for using Autopsy in forensic investigations.

Android Forensics: Investigation, Analysis and Mobile Security for Google Android

Satish Bommisetty, Andrew Hoog, John McCash, Syngress (2011).

→ Focused material on Android-based digital evidence recovery.

INTERPOL. (2023). Cybercrime Threat Response and Digital Forensics Report.

https://www.interpol.int/en/Crimes/Cybercrime

Netgate Documentation – pfSense Official Documentation

Netgate. (2024). pfSense Plus and CE Documentation.

Retrieved from: https://docs.netgate.com/pfsense/en/latest/

pfSense Software Download

Netgate. (2024). pfSense Community Edition.

Downloaded from: https://www.pfsense.org/download/

Oracle VirtualBox User Manual

Oracle. (2024). VirtualBox 7.0 User Manual.

Retrieved from: https://www.virtualbox.org/manual/UserManual.html

Virtual Network Configuration

Cisco Press. (2017). Network Simulation Experiments Manual.

ISBN: 9780133351100

Suricata Documentation – IDS/IPS for pfSense

Open Information Security Foundation. (2024).

Retrieved from: https://suricata.io/docs/

Snort Documentation – Intrusion Detection System for pfSense

Cisco. (2024). Snort 3.1 Documentation.

Retrieved from: https://docs.snort.org/

OpenVPN for pfSense – VPN Setup Guide

Netgate. (2024). OpenVPN Configuration Examples.

Retrieved from: https://docs.netgate.com/pfsense/en/latest/vpn/openvpn/index.html

Nigerian Cybercrime Act (2015).

https://www.ncc.gov.ng/documents/620-cybercrime-act-2015/file

→ Local legal framework on digital fraud and enforcement.

SANS Institute Reading Room. Practical Mobile Device Forensics.

https://www.sans.org/white-papers/

→ Applied techniques for digital evidence acquisition and reporting.