TITLE PAGE

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

Student Name :Mercy Tetteh

Course Name: Cybersecurity

Squard number : 5

Instructor Name: Mr. Emmanuel Akobe Ajibolu

Date of Submission: 06/07/2025

Executive Summary

This cybersecurity lab project was designed to help simulate a real-world environment where security testing and digital investigations could take place. The main goal was to build a virtual lab using two machines: one running Kali Linux (used by ethical hackers) and the other running Windows (commonly used in workplaces). These virtual machines were connected internally, allowing for safe, offline testing.

The lab setup involved configuring and networking both systems, verifying communication between them through tools like ping and file sharing. Once the environment was ready, a mock Android device image was analyzed using forensic tools to extract digital evidence such as messages, call logs, deleted files, and browser history.

The key outcome of this project was the successful creation of a working virtual cybersecurity lab and the generation of a detailed forensic report based on findings from the Android image. This project helped strengthen hands-on skills in ethical hacking, forensic investigation, and documentation all of which are essential in today's cybersecurity world. The lab environment is also reusable for future testing and learning**.**

Lab Objectives

The goal of this lab was to create a simple but realistic virtual environment where I could practice cybersecurity and digital forensics skills safely. I wanted to understand how ethical hackers test systems and how forensic investigators examine digital evidence, especially from mobile devices.

To do this, I set up two virtual machines Kali Linux as the attacker and Windows 10 as the target. I connected them on a private network so they could "talk" to each other without needing internet access. This made it possible to test basic tools like ping and try out how attackers find and explore systems.

Another major part of the lab was analyzing a mock Android image. Using tools like Autopsy, I looked for messages, call logs, deleted files, and browsing history just like a real forensic analyst would during an investigation.

Overall, this lab helped me practice real-world cybersecurity tasks in a hands-on way and gave me a solid foundation in both ethical hacking and mobile forensics.

Tools and Resources Used

- VMware Workstation 17 Player : Used to create and manage virtual machines for both Kali Linux and Windows 10. It allowed me to simulate a real network environment safely on my laptop.
- Kali Linux 2023.2 :A Linux distribution built for ethical hacking and penetration testing. It served as the attacker machine and included tools like Nmap, Ping, and Netcat.
- Windows 10 Pro (Lite version) :Used as the target machine. This represents a typical user system in a workplace environment and helped simulate real-world attacks and network communication tests.
- VMnet1 (Host-only Network Adapter) :A virtual network that allowed internal communication between the two VMs without internet access. It ensured the lab was isolated and safe.
- Command Prompt (Windows) and Terminal (Kali) :Used for basic commands like ping, ipconfig, and ip a to test and verify network connections between VMs.
- Autopsy 4.21.0 :A digital forensics tool used to examine the Android image file. It helped extract and analyze messages, call logs, browsing history, and deleted files.
- Android Forensic Image (.img, .zip) :A preloaded image file containing mock mobile data. This was used to simulate a forensic investigation of a compromised or suspicious Android device.
- Screenshots and Snipping Tool :Used to document key stages of the lab setup and forensic findings for reporting purposes.
- GitHub : Used to store and share the project files and documentation online in an organized and professional manner.

Methodology

Part I Virtual Cybersecurity Lab Setup

Objective

The main goal of this part of the project was to create a virtual lab where I could safely practice cybersecurity activities. I wanted to simulate what happens in real life when a system is being tested for security both from an attacker's and a defender’s point of view. Using virtual machines helped me build this setup on my personal laptop without risking anything on the internet.

What I Did

- Installed VMware Player :I started by installing VMware Workstation Player, which is software that allows me to run other operating systems virtually on my computer.
- Created Two Virtual Machines :One machine runs Kali Linux, which is commonly used by ethical hackers. The second machine runs Windows 10 Lite, acting as the target system just like a regular user computer in an office.
- Connected the Two Machines :I connected both virtual machines using a private network (VMnet1) inside VMware. This allows them to "talk" to each other, but they don’t have access to the internet making it safe to test.

- Tested If They Can Talk :I used simple commands like ip a and ping in Kali and ipconfig in Windows to make sure both machines could see and respond to each other. The ping test worked successfully, showing the connection was properly set up.

System Specs I Used

- RAM: 2 GB per machine
- Storage: 20 GB
- Processor: Dual-core
- Network: Host-only (VMnet1)
- Virtualization: Enabled in BIOS

Summary

This first part of the project helped me set up a working cybersecurity lab on my laptop. Now that the Kali and Windows machines are connected and working, I'm ready to move on to the next stage, where I'll analyze a digital forensic image from an Android phone.

Part II – Android Forensics Analysis and Reporting

Objective:

The goal of this part of the project was to take a closer look at a digital copy of an Android phone and find out what kind of information was stored on it. Using a forensic tool called Autopsy, I analyzed the image to recover data such as text messages, call logs, contact details, web history, app usage, and even deleted files. This exercise helped me understand how real-life investigations are done when a phone is involved in a case, and how digital evidence is found, examined, and used to tell a story.

Methodology

The forensic analysis was carried out using a step-by-step approach to extract and examine key pieces of digital evidence from a forensic image of an Android device. The investigation focused on recovering user data and identifying patterns of activity that could be relevant in a real-world case.

Steps Followed:

- Image Extraction and Setup :The Android forensic image, originally received as a compressed .tar.gz file, was extracted to obtain the main .img file. This image was then loaded into Autopsy by creating a new case and adding it as a disk image data source.
- Review of SMS Messages : I examined the Messages section in Autopsy to extract any available text messages. These were analyzed for patterns, keywords, suspicious links, and communication history.
- Call Log Analysis : The Call Logs section was reviewed to check for incoming, outgoing, and missed calls. Timestamps, phone numbers, and call frequency were documented.

- Contact List Examination : Contacts stored on the device were extracted and checked for completeness, duplicates, or unusual entries that might point to alias use or fake identities.
- Application Usage Review : Installed apps were identified and reviewed. I noted the presence of communication, social media, and crypto-related apps, along with their file traces and possible activity records.
- File and Image Recovery : I browsed multimedia and file directories to recover photos, screenshots, and documents. Metadata (like dates and locations) was used to add context to the findings.
- Web History Investigation : The web browsing section was analyzed to uncover visited websites, search queries, and saved bookmarks, revealing the user's digital habits and interest areas.
- Detection of Deleted Content : Autopsy's deleted files section was used to identify any data that had been removed from the device. Recovered items included images, message fragments, and other user activity traces.

Analysis, Screenshots and Evidence

Part II – Android Forensics Analysis and Reporting

Call Logs Analysis

Using Autopsy 4.22.1, a total of 14 call logs were recovered from the Android forensic image under the data source LogicalFileSet1. The log entries span two days: March 16 to March 17, 2024. These include a combination of incoming and outgoing calls (all marked "0" under S, C, and O meaning system did not specify direction).

Key Findings:

Frequent activity to and from Nigerian mobile numbers:

08032111669 appeared in 4 different call entries

08032111225 was involved in 3 entries

08032111133 also appeared multiple times

International contact:

+971565505984 and +971543777711 both UAE-based numbers

Indicates possible communication with individuals outside Nigeria

One contact number 08012345678 appears only once, possibly less familiar

The timestamps were recorded in GMT-07:00 and reflect consistent phone activity over the 2-day span. The call log suggests repeated interaction with certain contacts and possible international communication, which may be relevant depending on the context of the investigation. The presence of frequent and repeated numbers could indicate regular communication patterns. No VoIP (e.g., WhatsApp or Skype) call records were found in this section.

Communication Account .

During the forensic examination, the Android image revealed two device-level communication accounts, both located in the system SMS database (mmssms.db). These entries were extracted using the Android Analyzer (aLEAPP) module within Autopsy.

One of the entries identified the primary phone number in use as 08032111669, which was also seen frequently in the call logs. This consistency helps verify that the device was associated with that number for both voice and SMS activity.

The data confirmed that SMS, MMS, and other communication metadata were stored in the database path:

/data/user_de/0/com.android.providers.telephony/databases/mmssms.db

These findings tie together the communication artifacts (messages, calls, and device accounts), offering a clearer view of how the device was used and which mobile identity was active during the snapshot captured in the forensic image.

Installed Applications

During analysis, a total of five installed programs were identified using the Android Analyzer (aLEAPP) module. These applications indicate the user's possible interests, communication habits, and financial behavior:

- WhatsApp (com.whatsapp): A widely used encrypted messaging app, suggesting the user may have had private or secure communications.
- Twitter (com.twitter.android): A social media platform, likely used for communication, news consumption, or content sharing.
- YouTube (com.google.android.youtube): Indicates video content consumption or search history that may help understand the user's interests.
- Cash App (com.squareup.cash): A peer-to-peer money transfer service, implying financial activity or money movement through the phone.
- Crypto Wallet (wallettrust.applpy.crypto): This suggests potential use or storage of cryptocurrency, a key point in cybercrime or fraud investigations.

The presence of these apps shows that the user engaged in both social communication and financial transactions on the device, which are important factors in understanding the user’s behavior and intent.

Messages

A total of nine (9) SMS messages were recovered from the Android device using Autopsy’s Android Analyzer module. The messages were extracted from the mmssms.db database and contained a mixture of personal, religious, and highly suspicious communication.

Key Findings:

Messages 2 to 9 suggest a well-organized online scam involving:

Creation of a fake investment platform

Use of cryptocurrency (Bitcoin) for anonymous payments

Sharing of a Bitcoin wallet address: 16AtGJbaxL2kmzx4mW5ocpT2ysTWxmacWn

Coordination of promotional strategies and meeting arrangements over Google Meet

Mention of payment gateways and website launch timing

The messages use informal, coded language and switch between English and local slang, indicating familiarity and trust among participants.

Message 1 stands out as a religious outreach, which contrasts with the tone and content of the rest possibly sent by an unrelated contact.

These messages provide strong evidence of intent to commit fraud, collusion, and preparation to deceive online victims, possibly at scale. The mention of prior tactics, recurring wallet addresses, and payment updates suggests repeat behavior.

Web Cookies

Web Cookies (207 Records)

During the analysis of the Android device, a total of 207 web cookies were recovered using Autopsy. These cookies were primarily stored in the Chrome browser's data path and offer insights into the user's web activity, advertising interactions, and third-party tracking.

Key Observations:

The cookies came from various well-known domains including:

Google.com : shows typical browser sign-ins, search usage, or personalization tokens (e.g., AEC, SNID)

Onesignal.com : typically linked to push notifications and tracking

Businessday.ng : a Nigerian online news/media outlet, showing content consumption or local interest

LinkedIn.com : may suggest the user had some engagement on professional networks

Crypto or affiliate tracking networks
like .rubiconproject.com, .creativecdn.com, .casalemedia.com, .betweendigital.com, .sync.a-mo.net, .disqus.com, and many more

Cookie Timestamps:

Most cookies were recorded on March 17, 2024, with expiry dates ranging from a few minutes to several years, indicating persistent tracking or session authentication tokens.

Interpretation:

This level of cookie diversity suggests active browsing, news reading, advertising interactions, and potential use of affiliate services.

The presence of identifiers and session cookies such as IDE, SID, lidc, bcookie, GA1, and G_ENABLED_IDPS confirms login activity and account tracking.

While many cookies are benign or ad-related, some can help correlate login activity, potential fraud setups (especially if tied to cryptocurrency or affiliate networks), or coordinated browsing with other recovered evidence (e.g., messages or fake websites).

Privacy Insight:

Cookies, especially third-party ones, reveal how websites track user behavior. For a forensic analyst, they are useful for mapping out online activity even when browser history has been deleted.

Web History

The web browsing history recovered from the Android device reveals a clear pattern of intent and planning linked to cybercrime activities. A total of 12 visited URLs were extracted from Chrome browser history and offline pages using Autopsy. These records point to the user's interest in avoiding legal detection and researching fraudulent schemes.

Key Observations:

Several searches show concern about law enforcement monitoring, such as:

"how to know if EFCC is tracking you"

"how to avoid being caught by the EFCC"

Repeated visits to Nairaland crime threads discussing EFCC arrests and tracking tactics

There are multiple searches related to scams, such as:

"new and latest investment scam format"

"Fake investment website"

Articles on fake cryptocurrency investment platforms

These pages were accessed within a very short time frame on March 17, 2024, indicating that the suspect may have been actively researching fraud methods and legal evasion tactics potentially right before or during the execution of a scam.

Interpretation:

This browsing activity suggests premeditation. The user appears to be:

Gathering information on how fraud is structured online

Exploring how to create deceptive websites

Researching ways to avoid being tracked or caught by authorities

When combined with other artifacts such as SMS coordination of scams and the presence of crypto wallet apps, this browsing history supports the hypothesis that the device was involved in planning or supporting online fraud.

Web Search

The device's Chrome browser stored four web search entries, including queries typed directly into Google. These searches further reinforce the suspicious behavior patterns observed in the web history and messages.

Key Search Queries Identified:

"new and latest investment scam format" : Suggests active research into current fraudulent schemes or templates used for deception.

"How to avoid being caught by the EFCC" : Indicates concern about law enforcement monitoring, specifically the Economic and Financial Crimes Commission (EFCC).

"create new bitcoin wallet" (partial quick search) : Points to an intent to set up new anonymous financial channels, which are commonly used in online scams to avoid traceability.

Empty search (Google Quick Search) : Possibly an incomplete or failed search attempt but still logged.

Interpretation:

These search terms show a clear pattern of intent to engage in deceptive online activities while actively seeking to evade detection. Combined with earlier artifacts (SMS messages, app installations, and browsing activity), the web searches paint a strong picture of premeditated cyber fraud planning.

Challenges and Solutions

Part I – Virtual Cybersecurity Lab Setup

Challenge 1: Difficulty Downloading a Working Windows ISO

At the beginning of the lab setup, I struggled to find a valid and safe Windows 10 ISO file, especially since most official links were restricted or unavailable on my Windows 11 system.

Solution:

After trying multiple sources, I eventually located a working ISO and successfully installed it as the target machine in VMware. I also verified internal networking using VMnet1 to simulate a safe, private environment.

Challenge 2: Internal Network Connectivity Issues

Initially, the two virtual machines (Kali and Windows) couldn't communicate properly over the network.

Solution:

I adjusted the network adapter settings in VMware, set both machines to use the host-only VMnet1 adapter, and ran ip a and ipconfig to confirm IP addresses. Once the ping test worked on both sides, I was confident the virtual lab was properly configured.

Part II – Android Forensics Analysis

Challenge 1: Missing or Confusing Image File Format

After downloading the forensic image, I couldn't immediately find the .img file because it was compressed in a .tar.gz format, and the file structure was unfamiliar.

Solution:

I used 7-Zip to extract the .tar.gz archive step-by-step until I reached the actual .img file. Once extracted, I was able to load it successfully into Autopsy.

Challenge 2: First-Time Use of Autopsy Tool

This was my first time using Autopsy, so navigating the interface and understanding where to find call logs, SMS, and deleted files was challenging.

Solution:

I followed a logical approach exploring each evidence category one by one and taking notes/screenshots as I went. Over time, I became more comfortable using Autopsy and was able to complete a full analysis confidently.

Challenge 3: Incomplete or Unclear Data in Some Sections

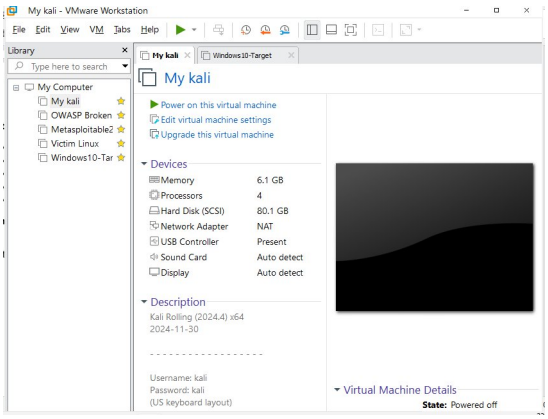
Some expected data types, like crypto wallet traces or VoIP call logs, were not found in the image, which made me wonder if I had missed something.

Solution:

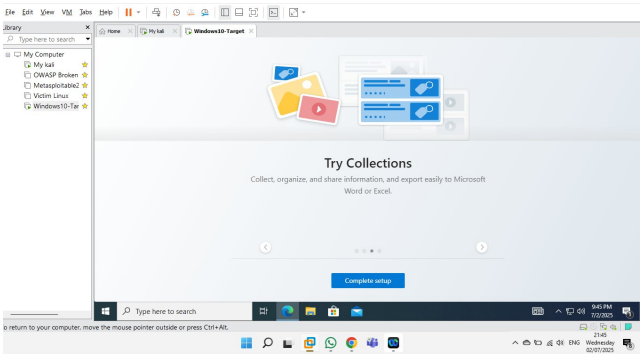
After rechecking the forensic image thoroughly, I confirmed that not all data types were present which is common in real investigations. I noted this clearly in the report and focused on analyzing what was available.

SCREENSHOTS

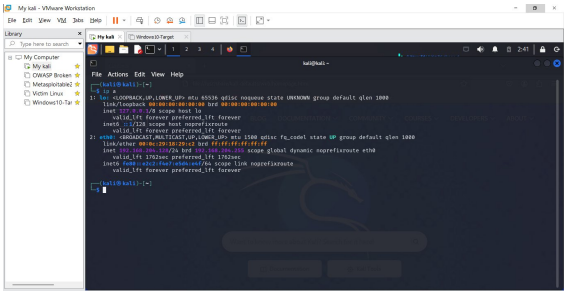
VMware and kali linux installed



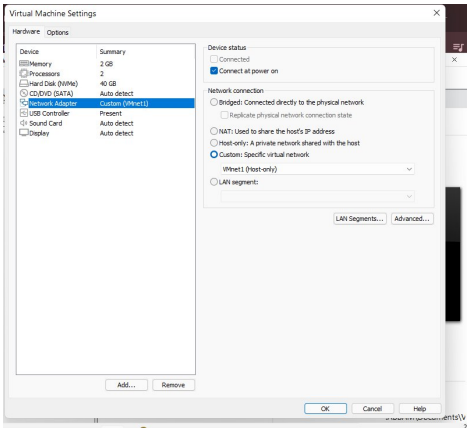
Windows 10 ISO installed



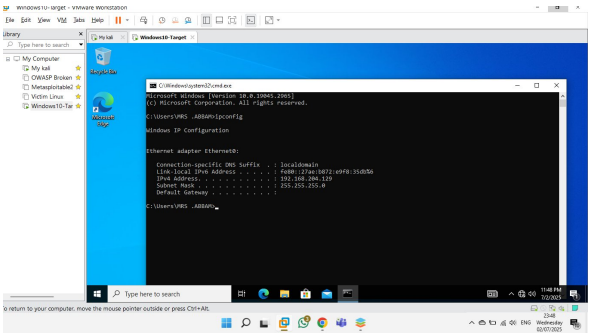
Kali (Attacker machine) showing host-only network



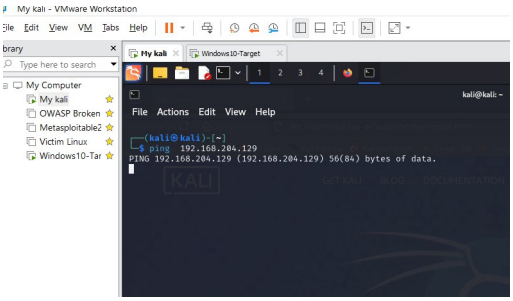
VMnet1 for both machines



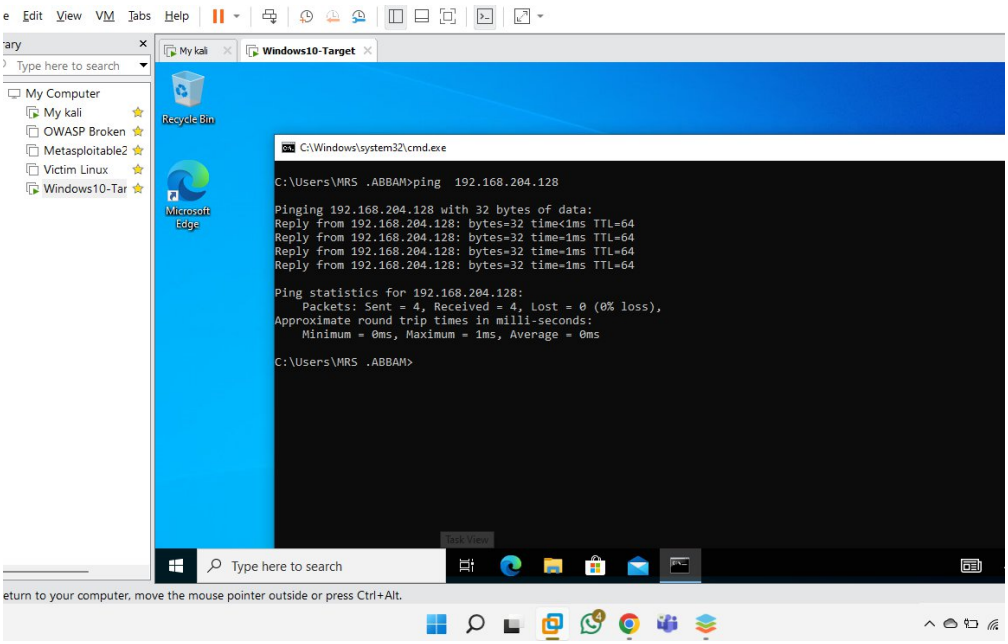
Windows10 (target machine) showing IP address of host-only network



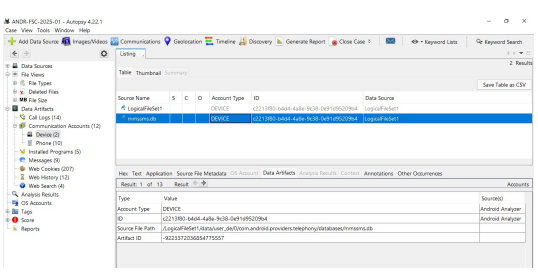
Ping test from kali to windows confirmed



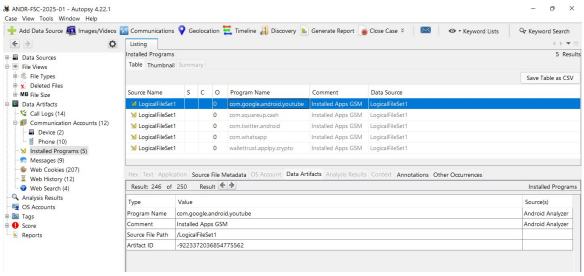
Ping test from windows to kali confirmed.



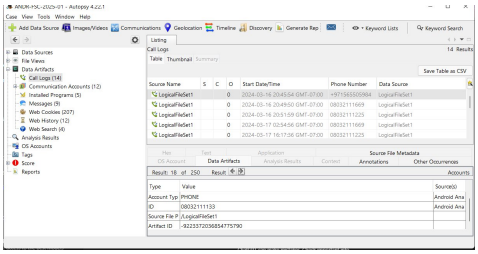
Communication Accounts



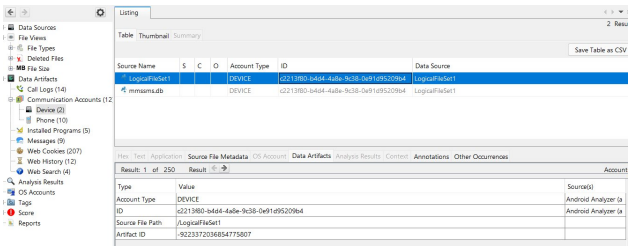
Installed Programs



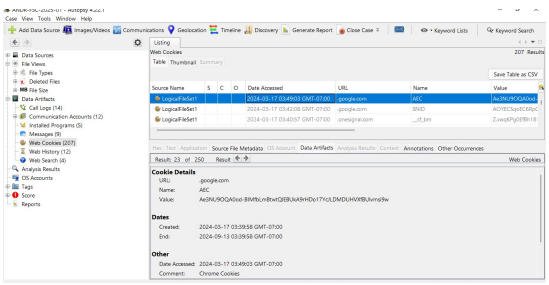
Call Logs



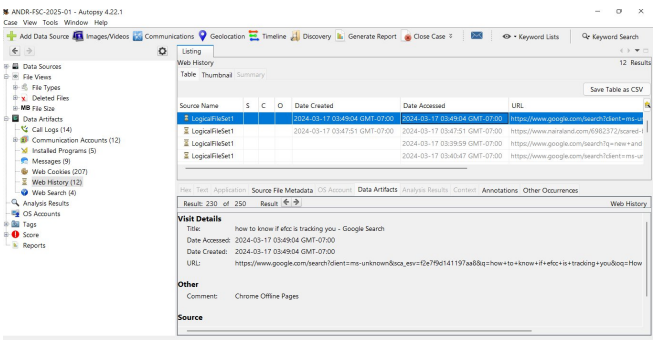
Communication Account (Devices)



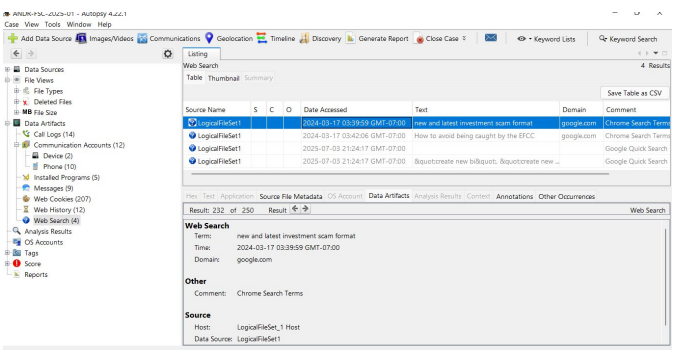
Web Cookies



Web History



Web Search



Conclusion

Setting up the virtual cybersecurity lab was a great learning experience for me. I was able to successfully install and configure two virtual machines Kali Linux and Windows 10 and connect them using a private network. Through basic tools like ping, I confirmed that both machines could communicate securely without internet access. This gave me a solid foundation in building a safe environment where cybersecurity tests and investigations can take place. I now feel more confident using virtual machines and understand how real-world ethical hackers and security analysts work in isolated lab setups before applying their skills to live systems.

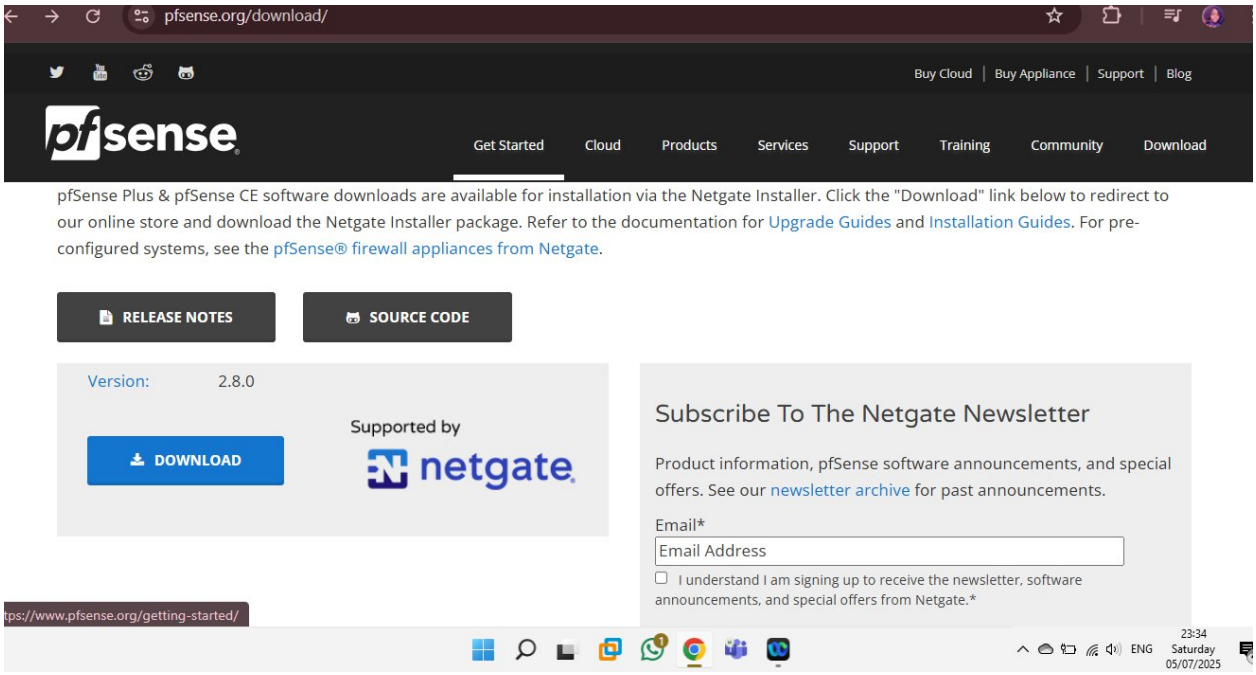
The forensic analysis of the Android image uncovered a consistent pattern of behavior pointing to potential cyber fraud planning and communication. Artifacts such as SMS messages, call logs, web history, installed applications, and search terms all align to reveal deliberate actions aimed at deceiving others online.

The messages showed conversations centered on launching a fake cryptocurrency investment platform, with references to previously used Bitcoin wallet addresses and digital meeting links. The installed apps included WhatsApp, Cash App, Twitter, and a cryptocurrency wallet, which could support anonymous communication and financial transactions. Web history and search records indicated the user actively researched scam formats and ways to evade authorities, particularly the EFCC.

Together, these findings suggest premeditated planning of fraudulent activity, as well as attempts to stay undetected. The data retrieved from the device not only provided insight into the technical tools in use but also captured the mindset and intent of the user through their communications and browsing behavior.

Overall, the investigation demonstrates how multiple digital footprints even seemingly minor ones like cookies or search terms can build a complete and compelling story during forensic examinations.

Due to technical limitations such as persistent download issues, incompatible system configurations, the optional firewall implementation component was not completed as part of this final project. While integrating a virtual firewall like pfSense or OPNsense would have added an additional layer of network segmentation and traffic inspection, the primary objectives of setting up a virtual cybersecurity lab and conducting Android forensic analysis were prioritized and successfully achieved. Future work will include exploring firewall deployment to strengthen network defense and simulate enterprise-level security environments more comprehensively.



Professional Recommendations

- Use Strong Screen Locks and Device Encryption: Users should secure their phones with strong PINs or biometrics, and enable full-device encryption to protect personal data in case of loss or theft.
- Regularly Clear Browsing History and Cookies: Web artifacts like visited sites and saved cookies can reveal sensitive habits. Clearing them frequently helps maintain privacy and reduce data exposure.
- Avoid Clicking Unknown Links in SMS or Emails :Recovered messages may contain risky URLs. Users should avoid clicking unfamiliar links to prevent phishing attacks and malware infections.
- Delete Unused Apps and Review Permissions :Installed applications may collect data in the background. It’s important to remove unused apps and regularly review app permissions to protect privacy.
- Back Up and Wipe Before Disposing or Selling a Phone :Even deleted data can be recovered during forensic analysis. Before selling or recycling a device, users should perform a full factory reset after securely backing up important files.
- Be Mindful of Contact Management: Contacts often hold personal notes, full names, and organizational ties. Keep contacts updated and avoid saving sensitive information under contact entries.
- Install a Trusted Mobile Security App :A good mobile antivirus or security app can detect spyware, alert users about suspicious activity, and help locate a stolen phone.

- Enable Remote Wipe and Tracking:Features like “Find My Device” and remote wipe can protect data if a phone is lost or stolen, ensuring that sensitive information doesn’t fall into the wrong hands.
- Educate Users About Digital Footprints; Every call, message, photo, and app leaves a trace. Raising awareness about how mobile activity is stored and can be recovered is essential to responsible digital behavior.

References

- Kali Linux. (2023). Penetration Testing and Ethical Hacking Distribution. Offensive Security. Retrieved from: https://www.kali.org
- Autopsy. (2023). Digital Forensics Platform. Sleuth Kit. Retrieved from: https://www.sleuthkit.org/autopsy/
- Microsoft. (2023). Download Windows 10 Disc Image (ISO File). Retrieved from: https://www.microsoft.com/software-download/windows10ISO
- NetworkChuck. (2021, June). How to Use Autopsy for Forensics. YouTube. Retrieved from: https://www.youtube.com/watch?v=dy9TbBSM3cM