INDUSTRY BASED PROJECT REPORT

Supervised by

Dr. Imran Mahmud

Professor & Head

Department of Software Engineering

Daffodil International University

Submitted By

Md. Tanbir

ID: 212-35-728

Department of Software Engineering

Daffodil International University

Approval

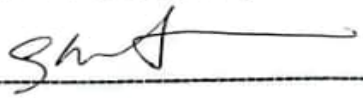
APPROVAL

This thesis is titled on "**Industry Based Project**", submitted by **Md. Tanbir (ID: 212-35-728)** to the Department of Software Engineering, Daffodil International University has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of Bachelor of Science in Software Engineering and approval as to its style and contents.

BOARD OF EXAMINERS

Chairman

Dr. Imran Mahmud
Professor & Head
Department of Software Engineering
Faculty of Science and Information Technology
Daffodil International University

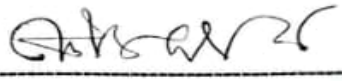


Internal Examiner 1

Md Shohel Arman
Assistant Professor
Department of Software Engineering
Faculty of Science and Information Technology
Daffodil International University

Internal Examiner 2

Md. Rajib Mia
Lecturer (Senior Scale)
Department of Software Engineering
Faculty of Science and Information Technology
Daffodil International University

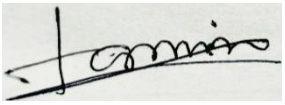


External Examiner

Md Habibur Rahman
Associate Professor
Department of Computer Science and Engineering
Islamic University, Bangladesh

DECLARATION

I hereby declare that; this internship has been done by me under the supervision of **Dr. Imran Mahmud, Professor & Head, Department of Software Engineering, Faculty of Science and Information Technology, Daffodil International University.** I also declare that neither this internship nor any part of this report has been submitted elsewhere for the award of any degree or diploma.



Md. Tanbir
ID: 212-35-728
Department of Software Engineering
Daffodil International University

Certified by

Dr. Imran Mahmud
Professor & Head
Department of Software Engineering
Faculty of Science and Information Technology
Daffodil International University

ACKNOWLEDGMENT

First, I want to give the Almighty Allah my sincere gratitude and thanks for enabling us to successfully finish the final year internship with Allah's help.

I would like to express my deepest gratitude to my parents, who have always been a tremendous source of inspiration and unwavering support. I owe my achievements today to their tireless dedication and hard work.

The first thing I want to do is thank Dr. Imran Mahmud, Professor & Head inthe Department of Software Engineering at Daffodil International University in Dhaka, from the bottom of my heart for his unflinching advice. His inspiration, guidance, and direction have giventhis work a strong foundation throughout the internship and report-writing process. His contributions to the development of the concepts explored in this study have greatly aided in the completion of this work.

I would also like to extend my sincere thanks to Md Tanvir Hasan Joha MD Backdoor Private Limited, for his unwavering support and encouragement throughout my journey.

Special thanks go to my internship supervisor Tahsina Sadia Meem, Forensic Analyst Backdoor Private Limited for his unwavering support andvaluable guidance during my internship.

Finally, I am grateful to my classmates and friends and All faculty Members in SWE for their collaboration, suggestions, and encouragement during this journey. Their support, whether big or small, has meant a lot to me.

ABSTRACT

This internship report outlines the professional experience gained at Backdoor Private Limited, a prominent cybersecurity firm specializing in Vulnerability Assessment and Penetration Testing (VAPT), Digital Forensics, and Security Operations Center (SOC) monitoring. During the internship, key contributions included conducting VAPT to identify and mitigate system vulnerabilities, assisting in digital forensic investigations to analyze cyber incidents, and supporting SOC monitoring to detect and respond to real-time threats. Hands-on experience with industry-standard tools, such as forensic software, and penetration testing frameworks, enhanced technical proficiency in cybersecurity operations. Collaboration with experienced professionals provided critical insights into proactive threat mitigation and robust security practices. This internship strengthened expertise in VAPT, digital forensics, and SOC operations while emphasizing the importance of adaptability and vigilance in safeguarding against evolving cyber threats

Table of Contents

Table Of Figure

CHAPTER 1: INTRODUCTION

1.1 Internship Overview

During my internship at Backdoor Private Limited, a top cybersecurity firm, I gained practical experience in Vulnerability Assessment and Penetration Testing (VAPT), Digital Forensics, and Security Operations Center (SOC) monitoring. My main tasks included running vulnerability scans and penetration tests to find system weaknesses, helping with digital forensic investigations to gather evidence from cyber incidents, and supporting SOC operations by monitoring network traffic for possible threats using SIEM platforms. I worked closely with experienced professionals and used tools like forensic software and penetration testing frameworks to improve system security. This experience deepened my understanding of proactive cybersecurity measures, sharpened my technical skills, and showed me the importance of flexibility and teamwork in tackling changing cyber threats. It prepared me for future challenges in the cybersecurity field.

1.2 Internship Purpose

The goal of my internship at Backdoor Private Limited was to gain practical experience in cybersecurity, especially in Vulnerability Assessment and Penetration Testing (VAPT), Digital Forensics, and Security Operations Center (SOC) monitoring. The internship aimed to improve my technical skills by using industry-standard tools and methods while working on real projects that strengthen security. It allowed me to work with experienced professionals and learn about proactive threat detection, incident response, and forensic analysis. Additionally, the internship helped me understand changing cyber threats and the need for flexibility in applying effective security measures. This experience prepared me for a career in cybersecurity.

1.2.1 Background

Backdoor Private Limited is a renowned cybersecurity firm specializing in delivering advanced security solutions, including Vulnerability Assessment and Penetration Testing (VAPT), Digital Forensics, and Security Operations Center (SOC) monitoring. The company serves a diverse clientele, addressing the growing need for robust cybersecurity in an increasingly digital world. My internship at Backdoor Private Limited was undertaken as part of an academic or professional development program to bridge theoretical knowledge with practical application in cybersecurity. With a foundational understanding of cybersecurity principles from prior coursework or self-study, I sought to immerse myself in real-world scenarios, leveraging the company's expertise and cutting-edge tools to deepen my skills in threat detection, forensic analysis, and

security operations. The internship was designed to provide exposure to industry practices, enhance technical proficiency, and foster a proactive approach to mitigating cyber risks in a dynamic threat landscape.

1.2.2 Benefits of Internship

Participating in an internship at Backdoor Private Limited offered numerous benefits that significantly contributed to my professional and personal growth in the cybersecurity field. Firstly, it provided hands-on experience with industry-standard tools and practices in Vulnerability Assessment and Penetration Testing (VAPT), Digital Forensics, and Security Operations Center (SOC) monitoring, allowing me to apply theoretical knowledge to real-world scenarios. Working alongside seasoned professionals enhanced my technical skills, forensic software, and penetration testing frameworks. The internship also fostered critical thinking and problem-solving abilities by exposing me to complex cyber threats and incident response strategies. Additionally, it offered valuable networking opportunities, enabling me to build connections with experts in the field. This experience improved my understanding of proactive cybersecurity measures, boosted my confidence in handling practical challenges, and prepared me for a successful career by aligning my skills with industry demands.

1.2.3 Goal

The main goal of my internship at Backdoor Private Limited was to gain hands-on experience and improve my skills in the cybersecurity field. By working on real-world projects, I wanted to connect my theoretical knowledge with practical use, building skills in proactive threat detection, incident response, and forensic analysis. I also aimed to develop adaptability, teamwork, and a strong grasp of changing cybersecurity challenges. This experience prepared me with the technical and professional background needed for a successful career in cybersecurity.

1.2.4 Scheduled

The internship at Backdoor Private Limited spanned from April 6, 2025, to June 6, 2024, lasting a total of three month. The standard office hours were from 10:00 AM to 6:00 PM, Sturday Friday, unless otherwise specified by the company. During this period, I engaged in various cybersecurity tasks, including Vulnerability Assessment and Penetration Testing (VAPT), Digital Forensics, and Security Operations Center (SOC) monitoring, aligning my work schedule with the company's operational hours to maximize productivity and collaboration with the team

CHAPTER 2: COMPANY OVERVIEW

2.1 Organization Profile

Backdoor Private Ltd is a premier Cybersecurity and IT solution firm Headquartered in Bangladesh, delivering cutting-edge digital protection. As a trusted partner of global Cybersecurity leaders, wee integrate world class technology with local expertise to safeguard organization against evaluation threats. Our certified team specializes in proactive threats detection, compliance, and resilience-building, serving governments enterprises and critical infrastructure sectors.

2.2 Vision of Organization:

To be a leader in Digital Security and make Backdoor a brand of trust by meeting each client requirement with highest accuracy confidentiality and transparency.

2.3 Mission of Organization:

To provided best-in-class information security expertise and customer-centric solutions to our customers. Along with strengthening client's digital security, educate them and enable them to remain safe in first-changing threat landscape.

2.4 Company Client:

- Modhumoti Bank Ltd
- Spectra Engineering Ltd.
- BSCL
- ICT Division
- Enhancing Digital Government and Economy
- Police Bureau of Investigation
- Anti-Terrorism Unit
- RAB Bangladesh
- BD Link Communication

CHAPTER 3: INTERNSHIP LEARNING

3.1 Internship Learning Outcome:

During my internship at Backdoor Private Limited as a Technical Executive, I gained practical experience in cybersecurity and IT. This experience helped me connect what I learned in theory with real-world applications. I became skilled in using tools like Nmap, Oxygen Forensic, Autopsy, FTK Imager, Nessus, OpenVAS, and Zenmap for network scanning, digital forensics, and vulnerability assessment. This improved my knowledge of host discovery, port scanning, data recovery, and threat detection. The internship also sharpened my teamwork, communication, and problem-solving skills in real IT situations, such as implementing system updates and tracking defects. Working with industry experts and handling live projects boosted my ability to apply IT principles, enhanced my SWOT analysis, and prepared me to face the challenges of the job market with confidence.

3.2 Learning to Internship:

3.2.1 Nmap Tools:

Description: Nmap (Network Mapper) is a flexible, open-source tool for exploring networks, auditing security, and gathering information. Cybersecurity experts use it a lot to find weaknesses and map out networks. It lets you find hosts using methods like ping scans (-sn) and list scans (-sL). It uses scan types like TCP SYN (-sS), TCP Connect (-sT), and UDP (-sU) to find open ports and running services.It also has stealthy scans like Null (-sN), FIN (-sF), and Xmas (-sX) that keep people from seeing what's going on.You can use your own Lua scripts with the scripting engine in Nmap (-sC or--script) to do things like find security holes and list services. There are also ways to get around firewalls and intrusion detection systems, like packet fragmentation (-f), decoy scanning (-D), and spoofing the source IP or MAC address. This is a great way to test network security and get into systems.

Nmap Tolls Using in Real life:

3.2.1.1 Host Discovery:

1.

- Command / option: **-sL: List Scan**
- Full Command: **nmap -sL 192.168.1.0/24 [Example IP address]**
- Description: This option performs a list scan, which simply lists the targets to scan without actually sending any packets to them.

- **Screenshot:**

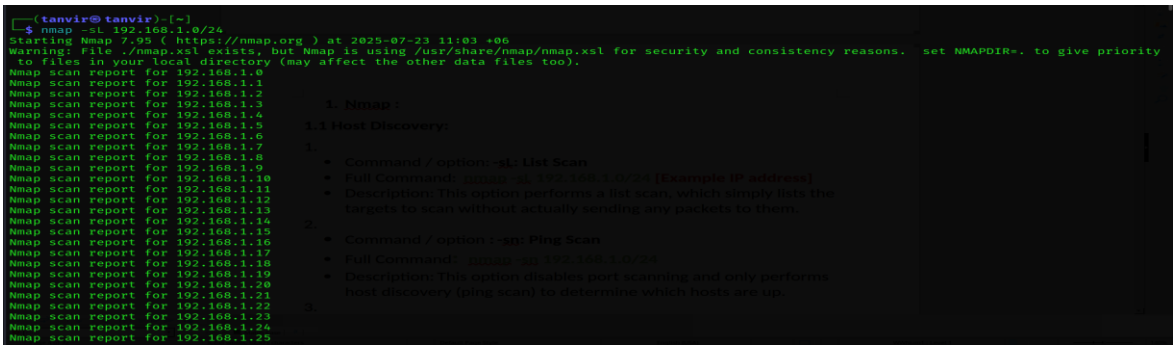


Figure 1

- **I did work:** we scan the company network found the all ip address in the company

2.

- Command / option: **-sn: Ping Scan**
- Full Command: **nmap -sn 192.168.1.0/24**
- Description: This option disables port scanning and only performs host discovery ping scan to determine which hosts are up.
- Screenshot:

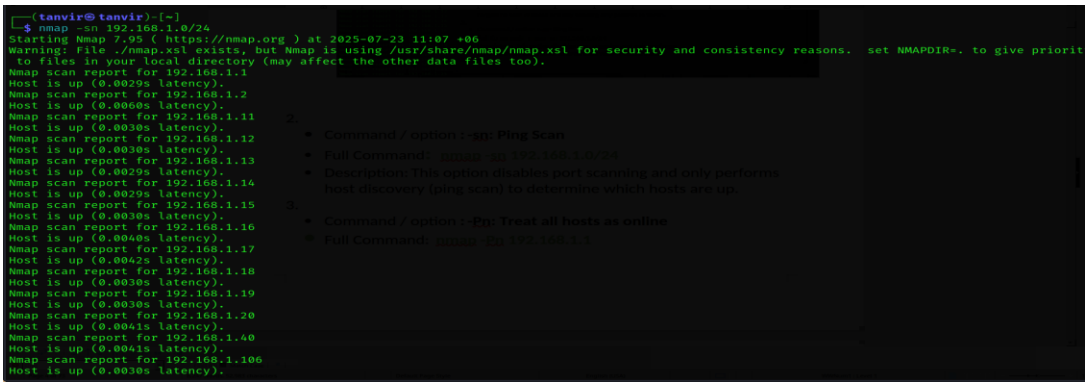


Figure 2

- **I did work:** we play the command in the company network. we found all live host in our company

3.

- Command / option: **-Pn: Treat all hosts as online**
- Full Command: **nmap -Pn 192.168.1.1**
- Description: This option skips host discovery and treats all specified hosts as online, which can be useful if you know the hosts are up but want to avoid pinging them.

- Screenshot:

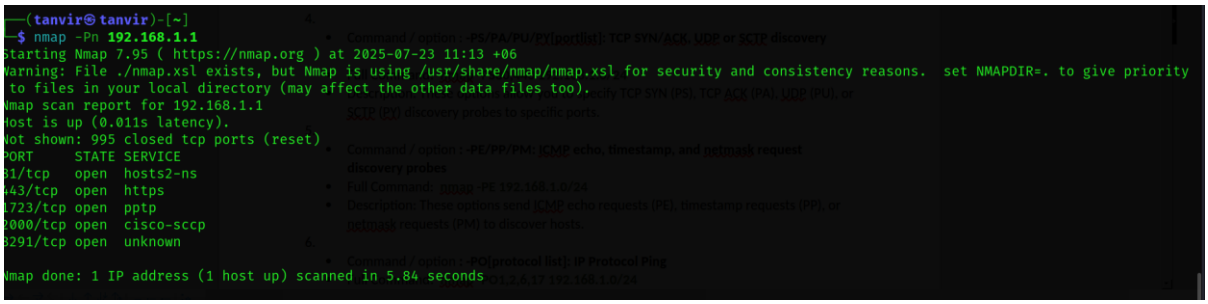
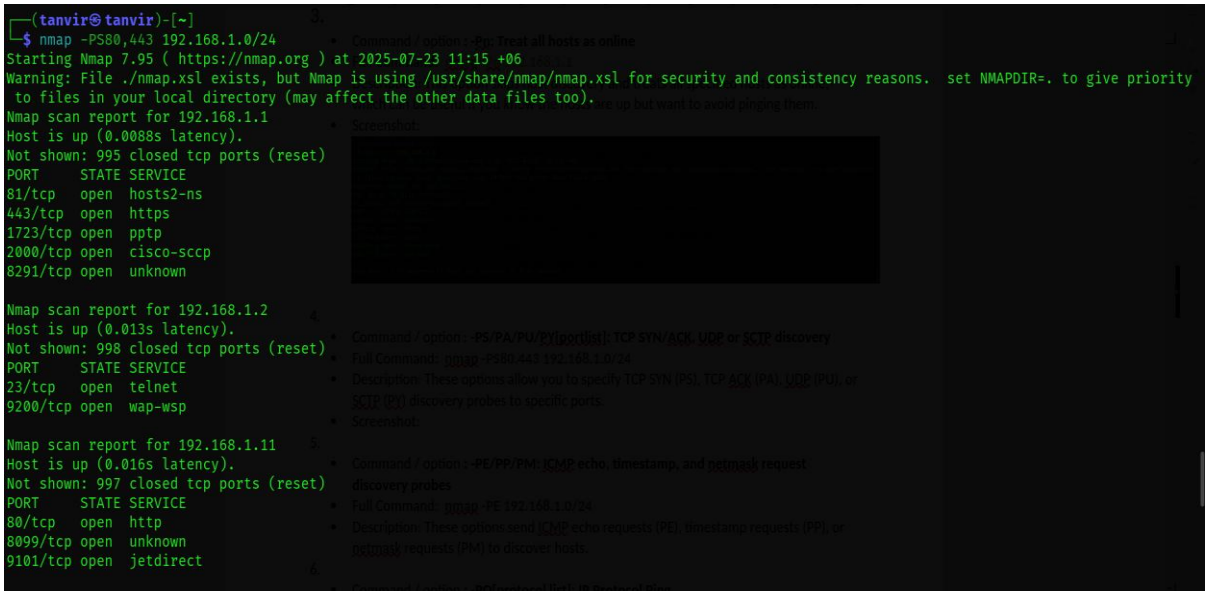


Figure 3

- **I did work:** scan the network find the whole host live without ping. we scan one host found many ports are open (https, hosts2-ns, pptp,cisco-sccp) here is no tcp port open.

4.

- Command / option: **-PS/PA/PU/PY [portlist]: TCP SYN/ACK, UDP or SCTP discovery**
- Full Command**:** **nmap -PS80,443 192.168.1.0/24**
- Description: These options allow you to specify TCP SYN, TCP ACK, UDP, or SCTP discovery probes to specific ports.
- Screenshot:



- **I did work:** We scan without 80 & 443 port in this network and find open all port and service in the network.

5.

- Command / option: **-PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes**
- Full Command: **nmap -PE 192.168.1.0/24**

- Description: These options send ICMP echo requests (PE), timestamp requests (PP), or netmask requests (PM) to discover hosts.
- Screenshot:

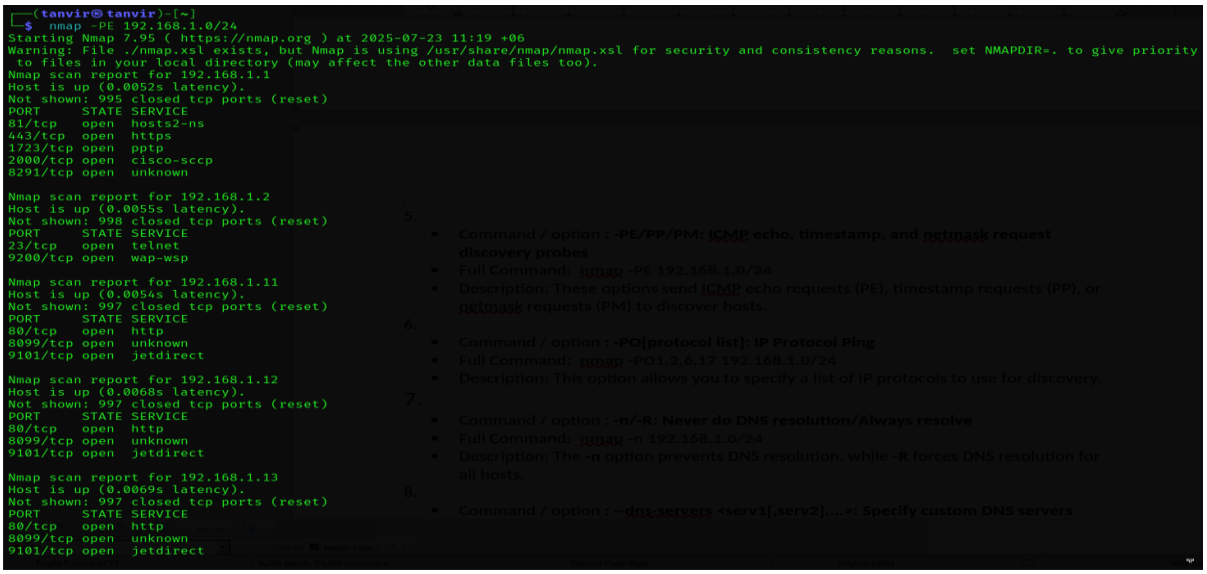


Figure 5

- **I did work:** The scan will create a list of hosts that respond to ICMP Echo Requests, showing they are online.

6.

- Command / option: **-PO [protocol list]: IP Protocol Ping**
- Full Command**:** **nmap -PO1,2,6,17 192.168.1.0/24**
- Description: This option allows you to specify a list of IP protocols to use for discovery.
- Screenshot:

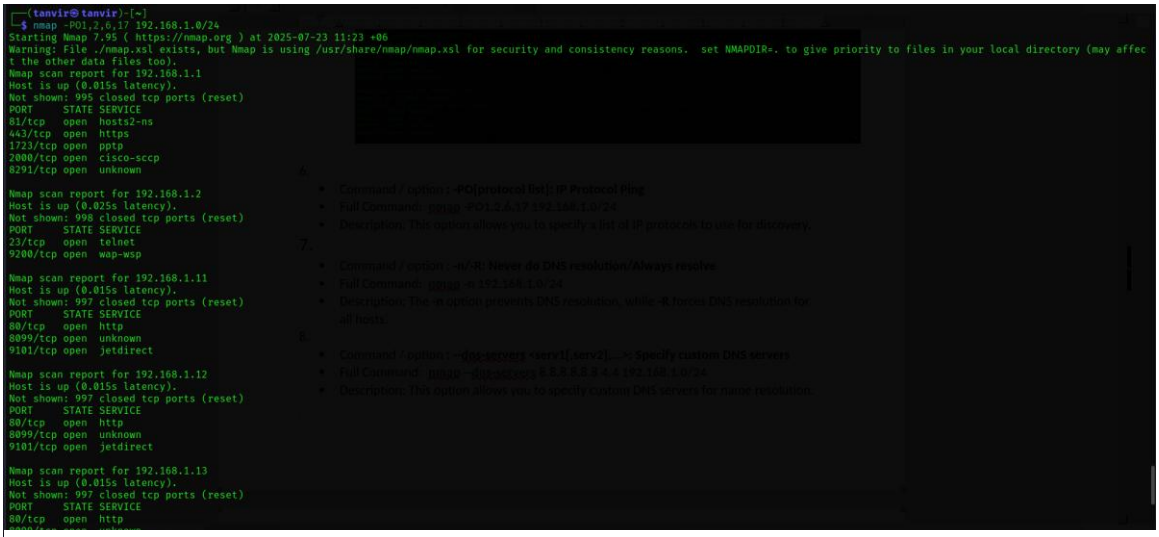


Figure 6

- **I did work:**

7.

- Command / option: **-n/-R: Never do DNS resolution/Always resolve**
- Full Command: **nmap -n 192.168.1.0/24**
- Description: The **-n** option prevents DNS resolution, while **-R** forces DNS resolution for all hosts.
- Screenshot:

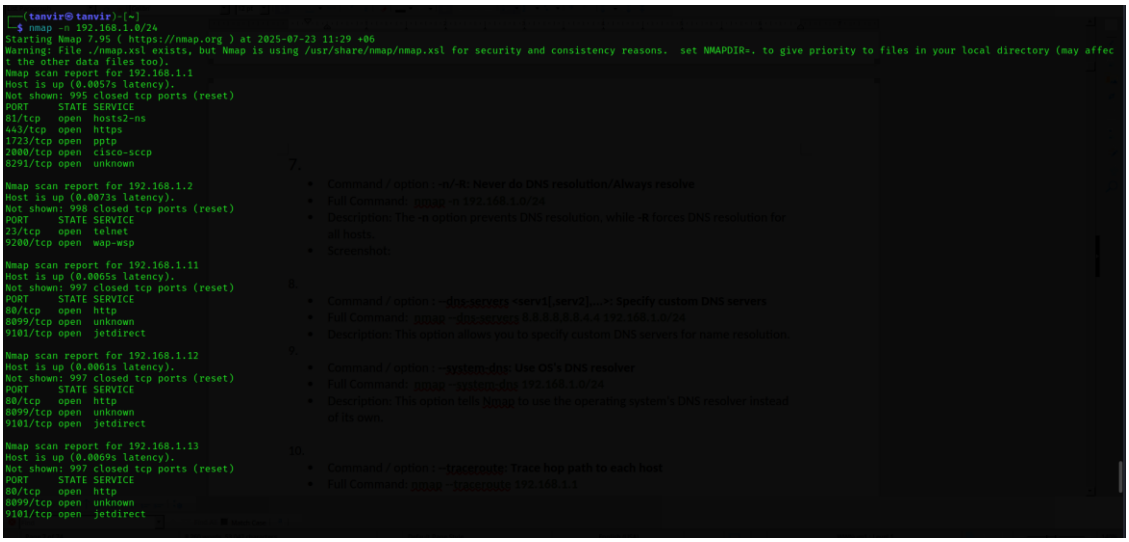


Figure 7

- **I did work:** The scan shows active hosts along with details like latency. It doesn't check for open ports or services unless you specify additional options.

8.

- Command / option: **--dns-servers <serv1[,serv2],...>: Specify custom DNS servers**
- Full Command**:** **nmap --dns-servers 8.8.8.8,8.8.4.4 192.168.1.0/24**
- Description: This option allows you to specify custom DNS servers for name resolution.
- Screenshot:

9.

- Command / option: **--system-dns: Use OS's DNS resolver**
- Full Command**:** **nmap --system-dns 192.168.1.0/24**
- Description: This option tells Nmap to use the operating system's DNS resolver instead of its own.
- Screenshot:

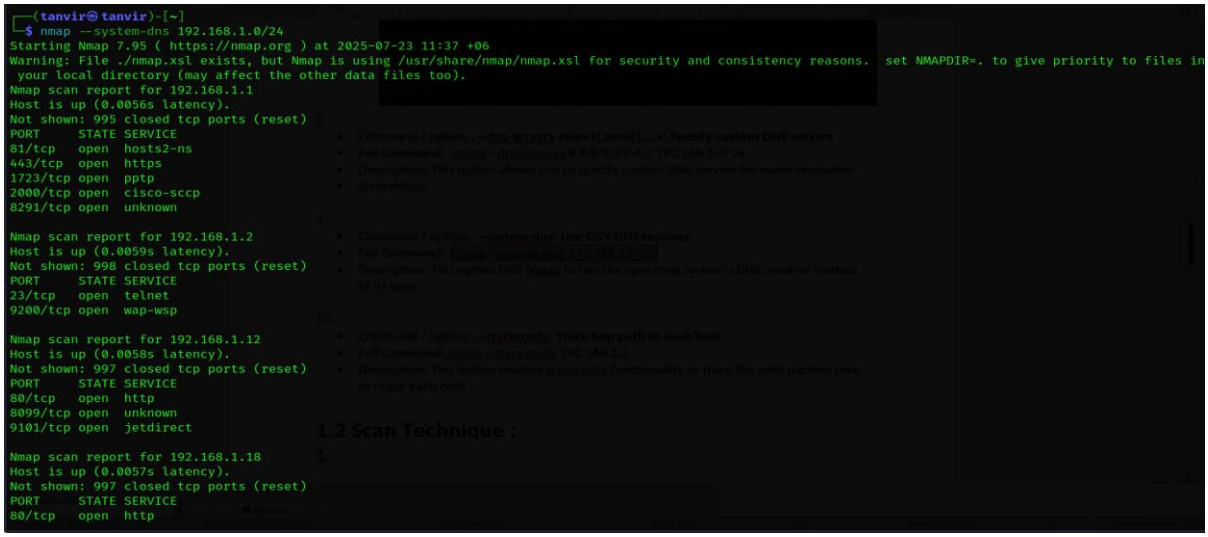


Figure 8

- **I did work:** The scan finds active devices on the network and tries to resolve their hostnames using the systems DNS resolver. This helps map a local network with useful hostnames. In some cases, it is faster than the default Nmap DNS resolution, but it relies on the systems DNS settings.

10.

- Command / option: **--traceroute: Trace hop path to each host**
- Full Command: **nmap --traceroute 192.168.1.1**
- Description: This option enables traceroute functionality to trace the path packets take to reach each host.
- Screenshot:

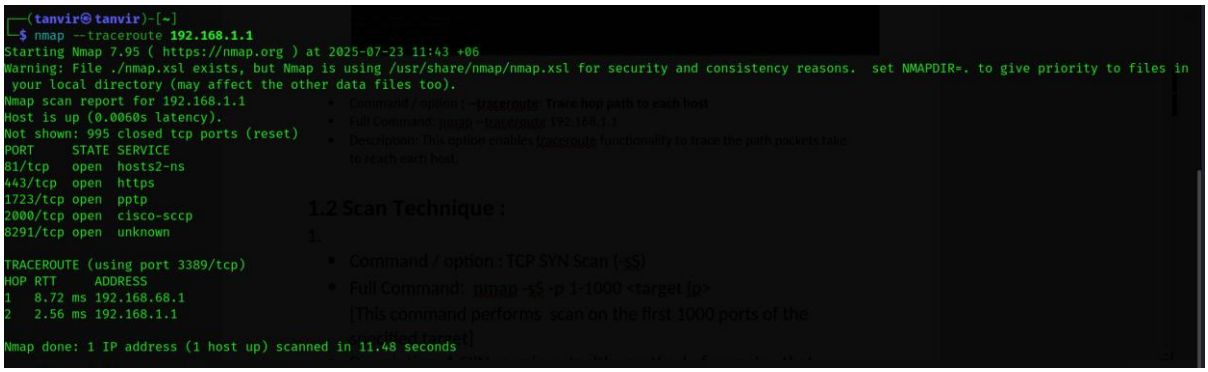


Figure 9

- **I did work:** The scan checks if 192.168.1.1 is active and shows the network path to it. Because 192.168.1.1 is on our network, the traceroute can only reveal one hop, which is the target itself, unless it goes through other devices.

3.2.1.2 Scan Technique:

1.

- Command / option: TCP SYN Scan (-sS)
- Full Command: **nmap -sS -p 1-1000 <target ip>**
- Description: A SYN scan is a stealthy method of scanning that sends SYN packets to target ports. If a SYN-ACK response is received, the port is open; if an RST is received, the port is closed. This method is less likely to be logged by the target system.
- Screenshot:

Figure 10

- **I did work:** This scan for SYN scan. it sends packet to port on 192.168.68.127. if one port receive response on SYN ACK means this port are open this scan find 21 ports are open. there are 999 ports are sending RST means this port are closed**.**

2.

- Command / option: **TCP Connect Scan (-sT)**
- Full Command: **nmap -sT -p 1-1000 <target ip>**
- Description: A TCP connect scan establishes a full TCP connection using the operating system's networking functions. It is more easily detected than a SYN scan but is useful when SYN scan is not possible.

- Screenshot:

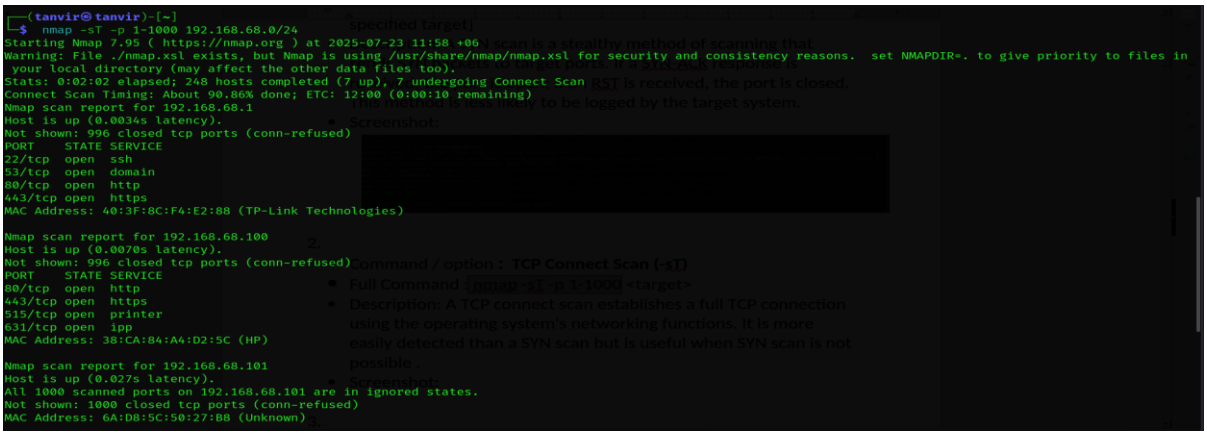


Figure 11

- **I did work:** This scan find TCP port are open and closed. We found the all-hosts TCP port and port number and whis service is running in port.

3.

- Command / option: **TCP ACK Scan (-sA)**
- Full Command: **nmap -sA -p 1-1000 <target ip>**
- Description: An ACK scan sends ACK packets to the target ports to determine whether they are filtered or unfiltered. It can help in mapping firewall rules.
- Screenshot:

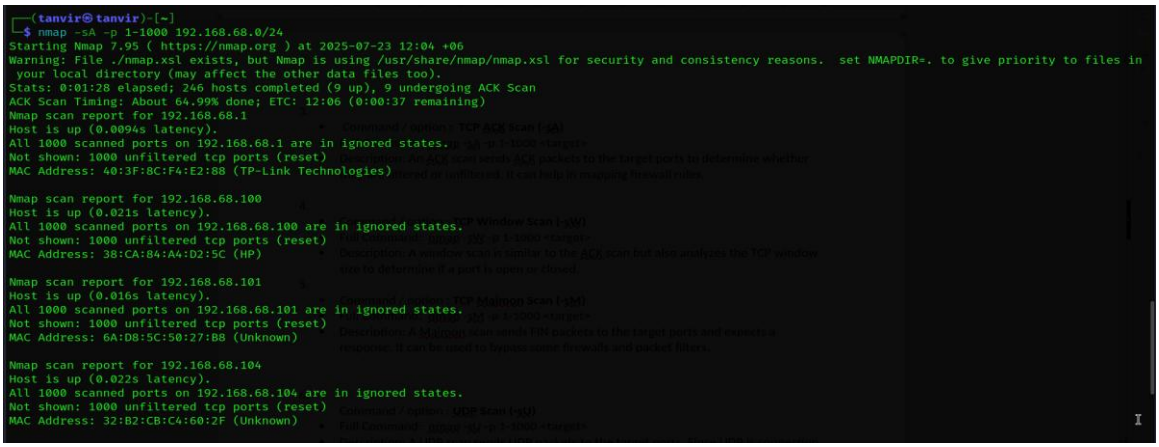


Figure 12

- **I did work:** The scan maps firewall rules for ports 1 to 1000 across the subnet. It identifies which ports are accessible (unfiltered) or blocked (filtered). This tool is useful for reviewing firewall settings or finding devices with specific port access without making a full connection.

4.

- Command / option: **UDP Scan (-sU)**

- Full Command: **nmap -sU -p 1-1000 <target ip >**
- Description: A UDP scan sends UDP packets to the target ports. Since UDP is connection less, it can be more challenging to determine the state of the ports open, closed, or filtered.
- **Screenshot:**

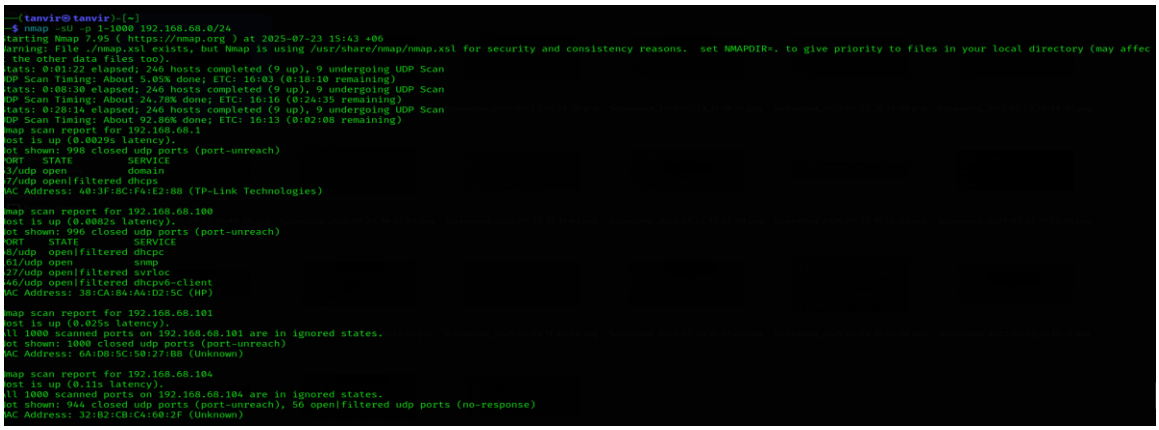


Figure 13

- **I did work:** The scan identifies active hosts and checks which UDP ports (1 to 1000) are open or accessible. This helps to discover services such as DNS that use UDP. UDP scans take longer than TCP scans because UDP does not establish a connection. Firewalls or missing responses can also make the results difficult to interpret.

3.2.1.3 Script Scan:

- Command / option: **-sC or --script=default**
- Full Command: **nmap -sC <target>**
- Description: This option runs the default set of scripts that come with Nmap. These scripts are generally safe and useful for gathering information about the target.

- Command / option: **--script=<Lua scripts>**
- Full Command**:** **nmap --script=http-title,ftp-anon <target>**
- Description: This option allows you to specify a comma-separated list of Lua scripts, script files, or script categories to run.

- Command / option: **--script-help=<Lua scripts>**
- Full Command: **nmap --script-help=http-title**

- Description: This option shows help information about the specified scripts or script categories.

3.2.1.4 Scanning Port:

1. Scanning Specific Ports

- Command / option: **-p**
- Full Command**:** **nmap -p 22 192.168.1.1/24**
- Description: Scans only port 22 (SSH) on the target 192.168.68.0/24
- Screenshot:

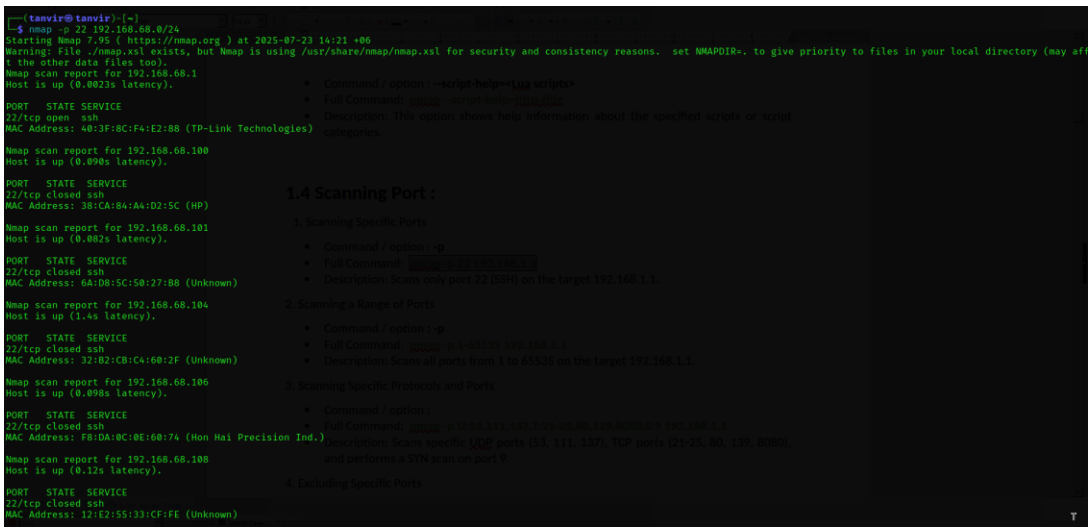


Figure 14

- **I did work:** This command scanning for 22 no port in 192.168.68.0/24 ip and find whis host are open and 22 no port is open and service are running.

2. Scanning a Range of Ports

- Command / option: **-p**
- Full Command: **nmap -p 1-65535 192.168.1.1**
- Description: Scans all ports from 1 to 65535 on the target 192.168.68.0/24
- **screenshot:**

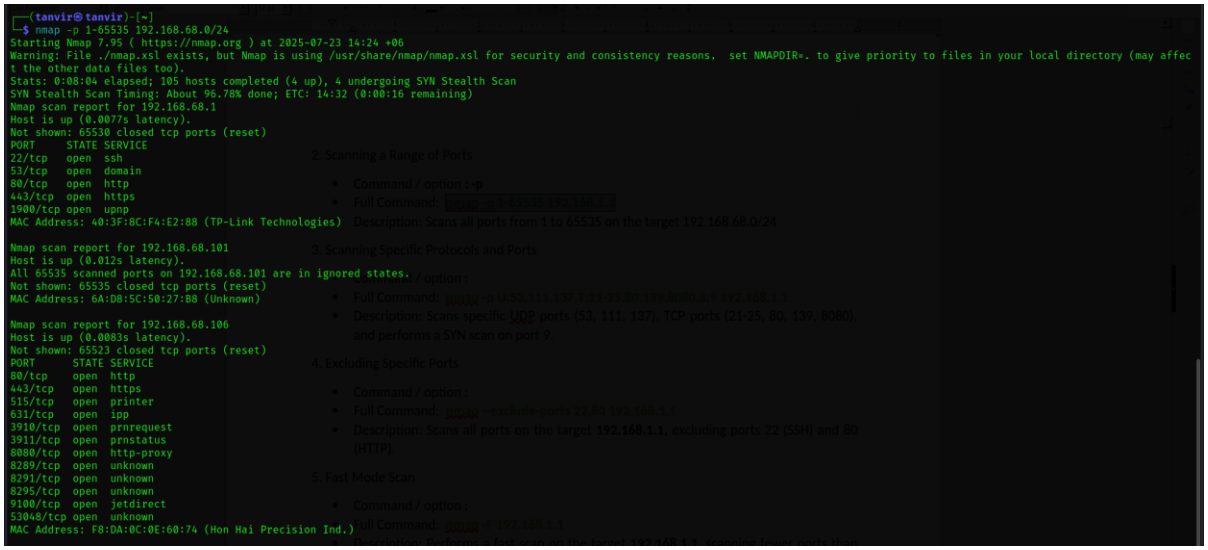


Figure 15

- **I did work:** We scan the network and all ip and check 1-65535 port is open or closed. we find some ports are open and some service is running

3. Scanning Specific Protocols and Ports

- Command / option:
- Full Command: **nmap -p U:53,111,137, T:21-25,80,139,8080, S:9 192.168.68.0/24**
- Description: Scans specific UDP ports (53, 111, 137), TCP ports (21-25, 80, 139, 8080), and performs a SYN scan on port 9.
- Screenshot:

Figure 16

- **I did work:** We scan specific UDP port and TCP port and SYN 9 no port**.** we found some TCP port to open and some TCP port are closed. Some services are running [eg: ftp,ssh http,https] are common service.

4. Excluding Specific Ports

- Command / option: nmap --exclude-ports
- Full Command: **nmap --exclude-ports 22,80 192.168.68.0/24**
- Description: Scans all ports on the target **192.168.1.1,** excluding ports 22 (SSH) and 80 (HTTP).

- Screenshot:

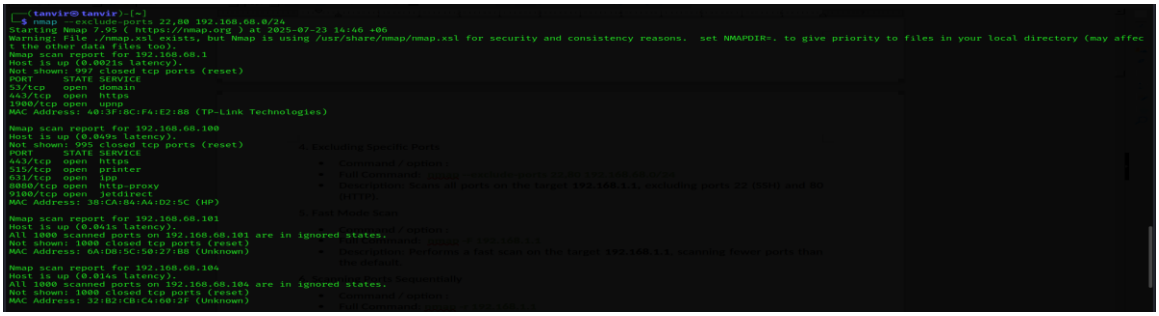


Figure 17

- **I did work:** The scan detects active hosts and checks the default set of ports for services (minus 22 and 80), which is useful for mapping a network while avoiding specific services like SSH or web servers. Excluding ports can reduce scan time or avoid triggering alerts on sensitive services.

5. Fast Mode Scan

- Command / option: nmap -F first scan
- Full Command: **nmap -F 192.168.68.0/24**
- Description: Performs a fast scan on the target **192.168.68.0/24**, scanning fewer ports than the default.
- Screenshot:

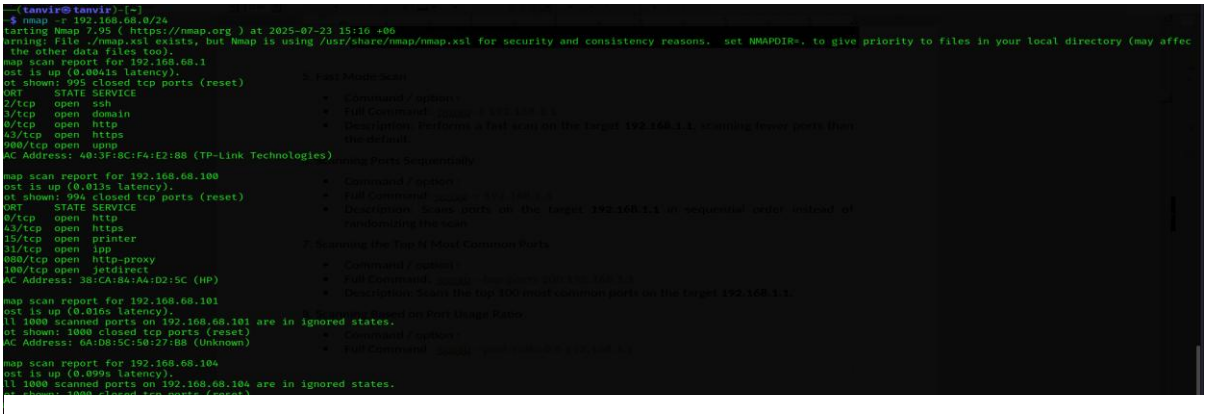


Figure 18

- **I did work:**

  The scan quickly finds active devices and their most frequently used open TCP ports. This is great for quickly looking at key services on a network. It's not as thorough as a full port scan, but it's fast.

6. Scanning Ports Sequentially

- Command / option: nmap -r scan port sequentially
- Full Command: **nmap -r 192.168.68.0/24**
- Description: Scans ports on the target **192.168.68.0/24** in sequential order instead of randomizing the scan
- Screenshot:

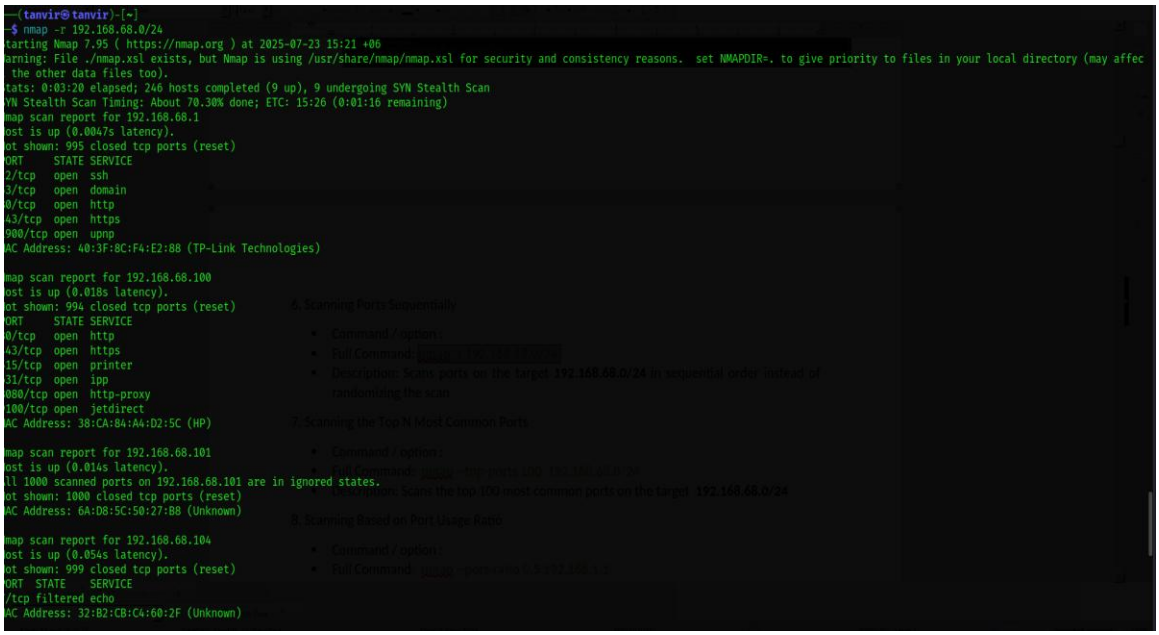


Figure 19

- **I did work:** The scan finds active devices on the subnet and their open TCP ports, focusing on the top 1000 ports. It scans these ports one after another. This helps map network services such as web servers or SSH that use predictable port orders for specific situations.

7. Scanning the Top N Most Common Ports

- Command / option:
- Full Command: **nmap --top-ports 100 192.168.68.0/24**
- Description: Scans the top 100 most common ports on the target **192.168.68.0/24**
- screenshot:

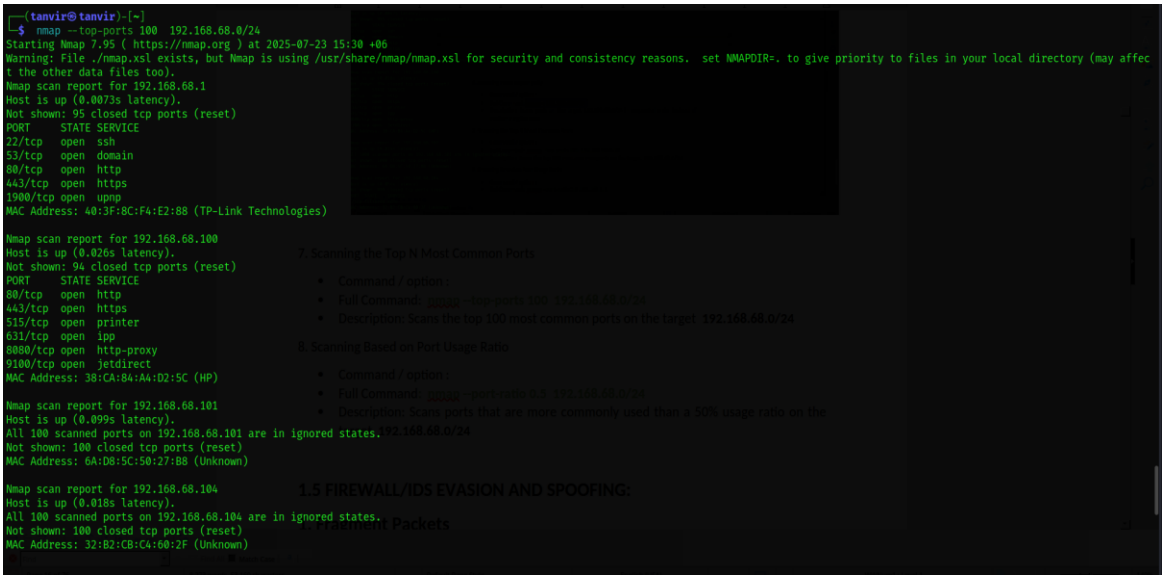


Figure 20

- **I did work: This scan find top 100 ports open and service is running in this port .**

8. Scanning Based on Port Usage Ratio

- Command / option:
- Full Command**:** **nmap --port-ratio 0.5 192.168.68.0/24**
- Description: Scans ports that are more commonly used than a 50% usage ratio on the target **192.168.68.0/24**
- Screenshot:

Figure 21

3.3Whois Command:

Description: Whois is a command-line tool used to query databases and retrieve information about domain names, IP addresses, and Autonomous System Numbers (ASNs). It provides important details for network reconnaissance and cybersecurity analysis. I used Whois to gather data such as registrar details, registration dates, name servers, and contact information for domains (ex: whois google.com). The tool offers options like specifying custom Whois servers (ex: whois -h whois.ripe.net 193.0.6.135) or querying specific ports (ex: whois -h whois.verisign-grs.com -p 43 example.com) for focused lookups. Whois was invaluable for identifying domain and network ownership. It helped with the early stages of security assessments and penetration testing by providing useful information about target infrastructures.

Command: whois [options] [domain|IP|ASN]

Common WHOIS Command Options provide this table

Option	Example	Description
Basic	whois example.com	Queries the default WHOIS server for domain info.
-h <host>	whois -h whois.verisign-grs.com example.com	Manually specify the WHOIS server to query.
-p <port>	whois -h whois.verisign-grs.com -p 43 example.com	Specifies a custom port (default is 43).
--verbose	whois --verbose example.com	Outputs detailed debug/connection info.
--help	whois --help	Displays help information for the command.

3.3.1 Example WHOIS Lookups

- **Domain Name Lookup**
- Example: whois google.com
- Description; Retrieves registrar, registration dates, name servers, contact info.
- **IP Address Lookup**
- Example; whois 8.8.8.
- Description Displays the network owner, ASN, CIDR range (usually from ARIN, RIPE, etc.).
- **Specify WHOIS Server**
- Ex: whois -h whois.ripe.net 193.0.6.135
- Description: Queries RIPE (European registry) directly for an IP.
- **Lookup Using Custom Port**
- Example: whois -h whois.verisign-grs.com -p 43 example.com
- Description: Uses a specific port for the WHOIS server.
- **ASN Lookup**
- Example: whois AS15169
- Description Shows owner and routing info for the Autonomous System.

3.4 Fierce

Description: Fierce is made to find hostnames and non-contiguous IP space that match designated domains. It can assist penetration testers and security experts in learning more about a target domain, which is essential for locating possible attack points. Through DNS queries, the tool can find subdomains that might not be publicly listed but could be useful for future exploitation.

Command: fierce --domain [target-domain]

Example: fierce --domain google.com

Scan Screenshot:

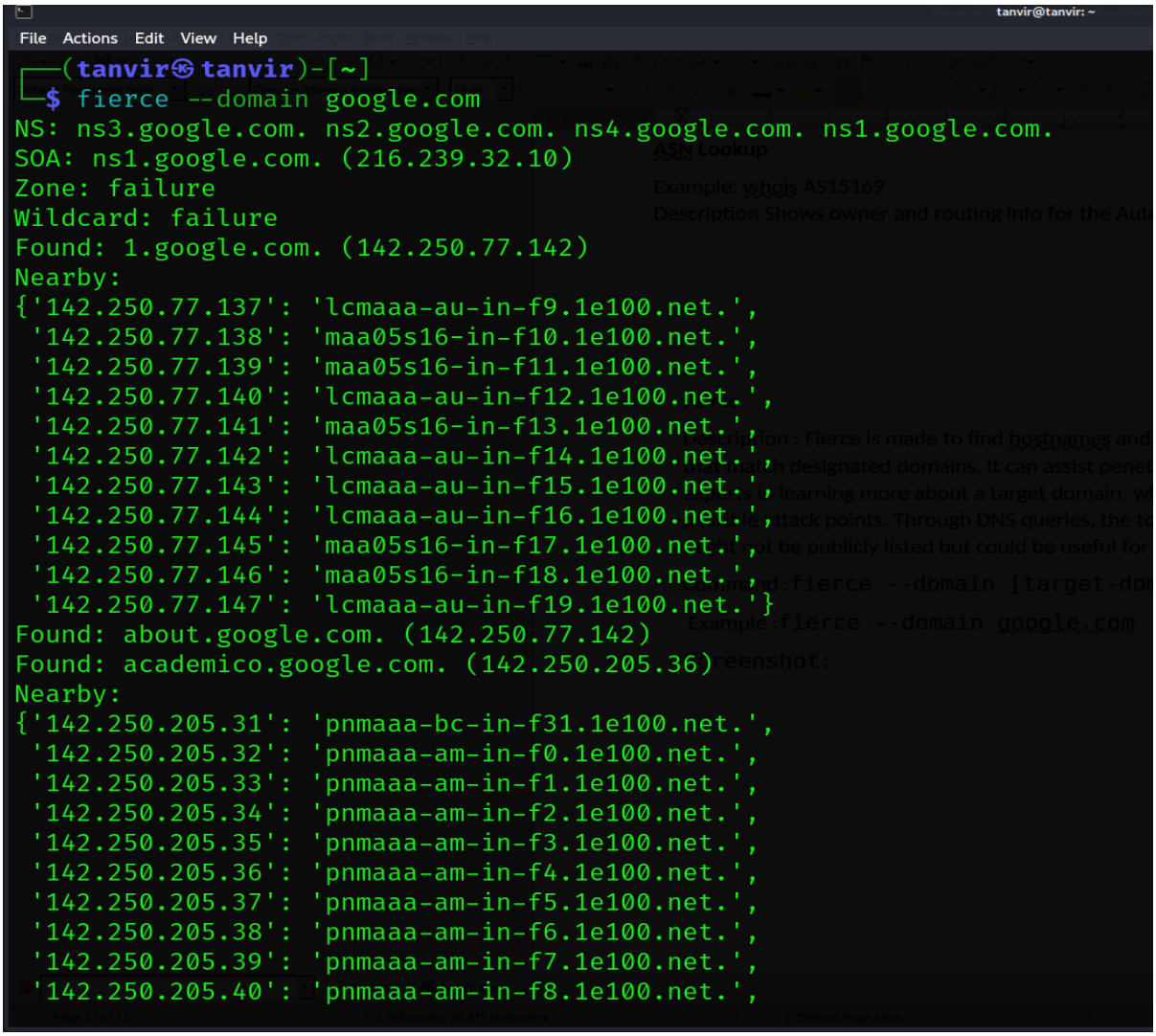


Figure 22

- **I did work:** The command outlines the DNS structure of google.com. It identifies subdomains and IP addresses that could be potential attack points or reveal network information. We found many ip address and DNS service for google.com

3.5 Dnsenum

Description: This command will gather information about the `example.com` domain, including its DNS records, subdomains, and other relevant data.

Command: **dnsenum example.com**

Example: **dnsenum backdoor.com.bd**

Scan Screenshot:

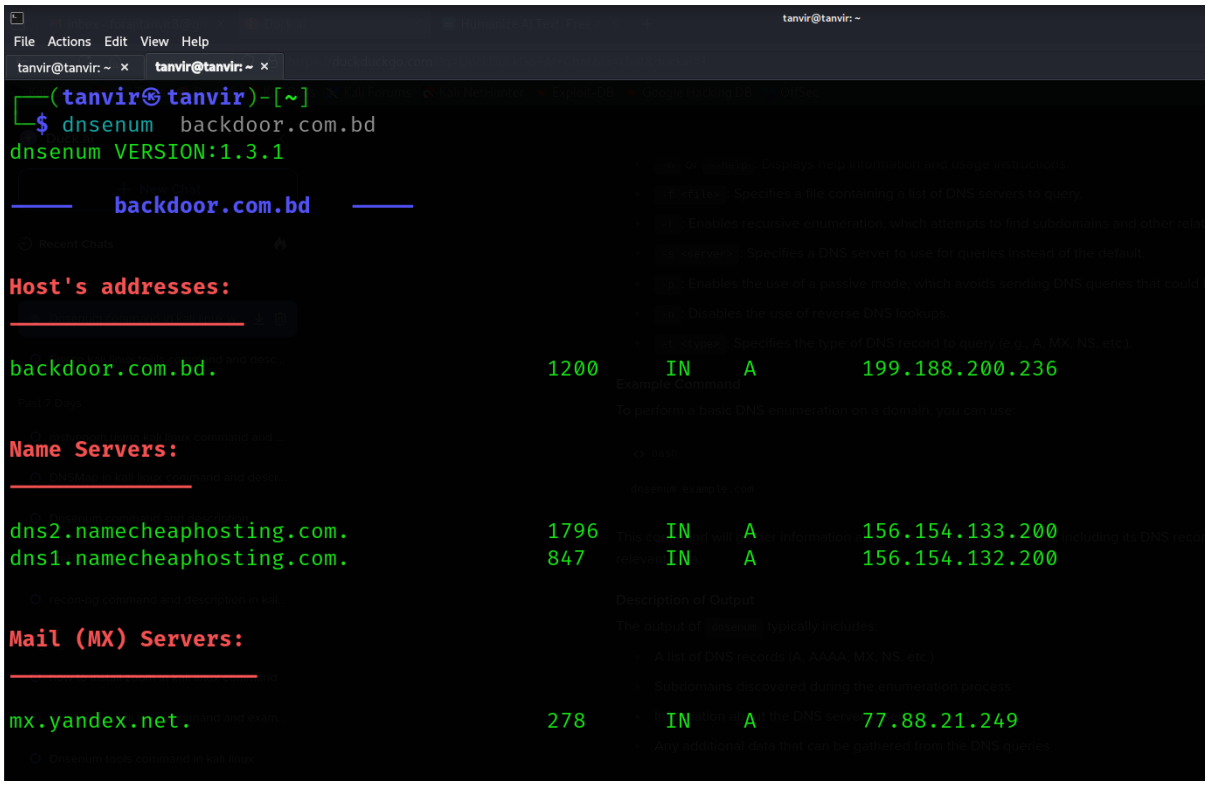


Figure 23

- **I did work:** The command collects DNS-related information about backdoor.com.bd, revealing subdomains, servers. we found backdoor.com.bd hosts server ,DNS server aand Mail server ,

3.6 DnsMap

Description: During the information-gathering phase of an infrastructure security assessment, penetration testers and security professionals can use **DNSMap**, an open-source network reconnaissance tool, to identify subdomains associated with a target domain. First released in 2006 and inspired by Paul Craig's fictional story *"The Thief No One Saw"*, DNSMap is designed to systematically uncover hidden or overlooked subdomains. It accomplishes this by utilising brute-force and dictionary-based methods to query DNS servers. A built-in wordlist of about 1,000 common Spanish and English words, including "ns1," "firewall," and "smtp," is part of the tool. For more focused scans, users can also provide their own unique wordlists. To improve the efficacy of scanning, DNSMap provides a number of sophisticated features. These include limiting false positives by filtering particular IP addresses, preventing detection by modifying query delays, and storing output in human-readable or CSV formats. The tool additionally includes a script called dnsmap-bulk.sh for large-scale operations, which enables effective bulk scanning of numerous targets.

Command: dnsmap example.com

Example: dnsmap backdoor.com.bd

Scan Screenshot:

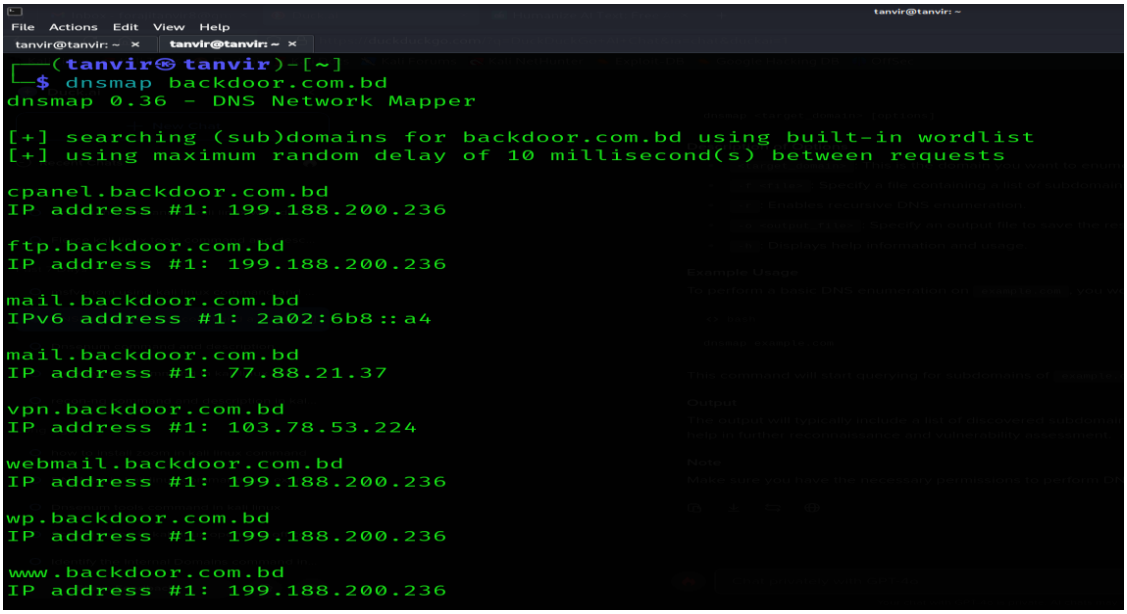


Figure 24

- **I did work:** The command identifies valid subdomains of backdoor.com.bd by brute-forcing, helping map the domain's attack surface or network presence. We found ftb server, web mail, mail server and server ip address.

3.7 Spiderfoot

Description: An effective open-source intelligence (OSINT) automation tool is SpiderFoot. By collecting and evaluating information from more than 200 public sources, such as DNS records, Whois, IP addresses, email addresses, social media, and threat intelligence services like Shodan and HaveIBeenPwned, it facilitates reconnaissance. During my internship at Backdoor Private Limited, I made use of SpiderFoot. It gathers data about targets, like domains, hostnames, or subnets, automatically. It makes use of more than 200 modules that facilitate data correlation, domain footprinting, and active and passive scanning. Its command-line options and web-based interface are simple to use. For a user-friendly experience, for instance, you can use commands like `python3 sf.py -l 127.0.0.1:5001`. Additionally, the tool provides customisable scan profiles, including Passive, Investigate, and Footprint. Its adaptability is further enhanced by API integrations and export choices, such as CSV, JSON, and GEXF. SpiderFoot is able to detect relationships between entities, vulnerabilities, and data leaks. This makes it valuable for offensive penetration testing and defensive security assessments. However, its performance depends on the availability of API keys for premium data sources and enough system resources for large scans.

Command: **spiderfoot -l 127.0.0.1:5001**

Screenshot:

Command in terminal:

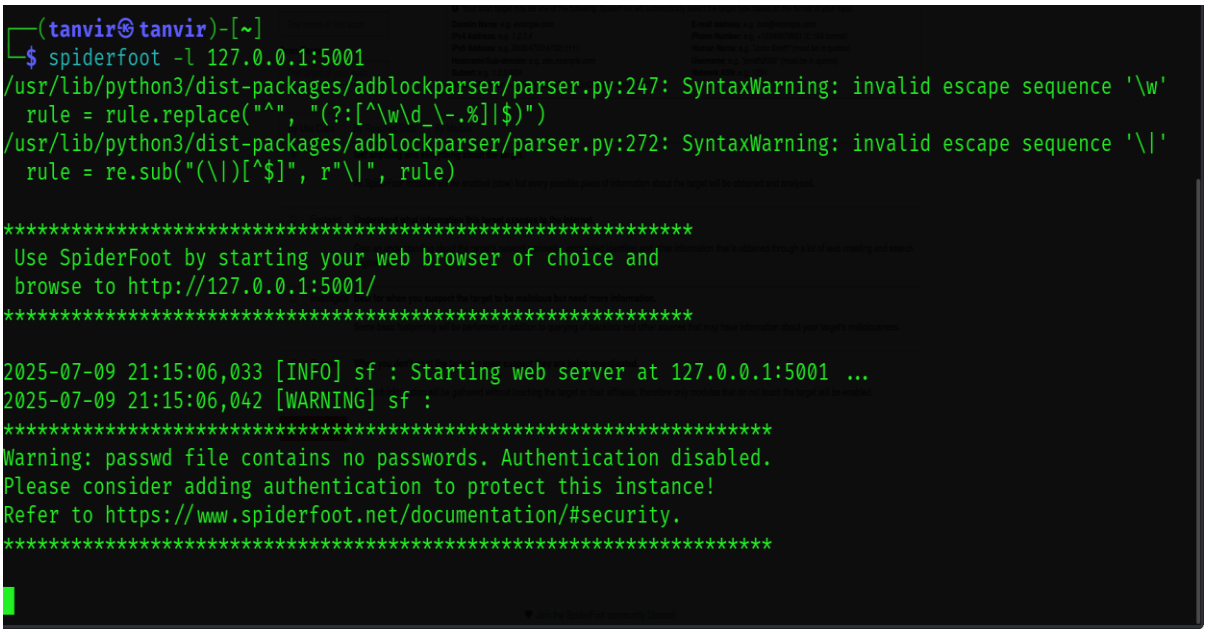


Figure 25

open web browser:

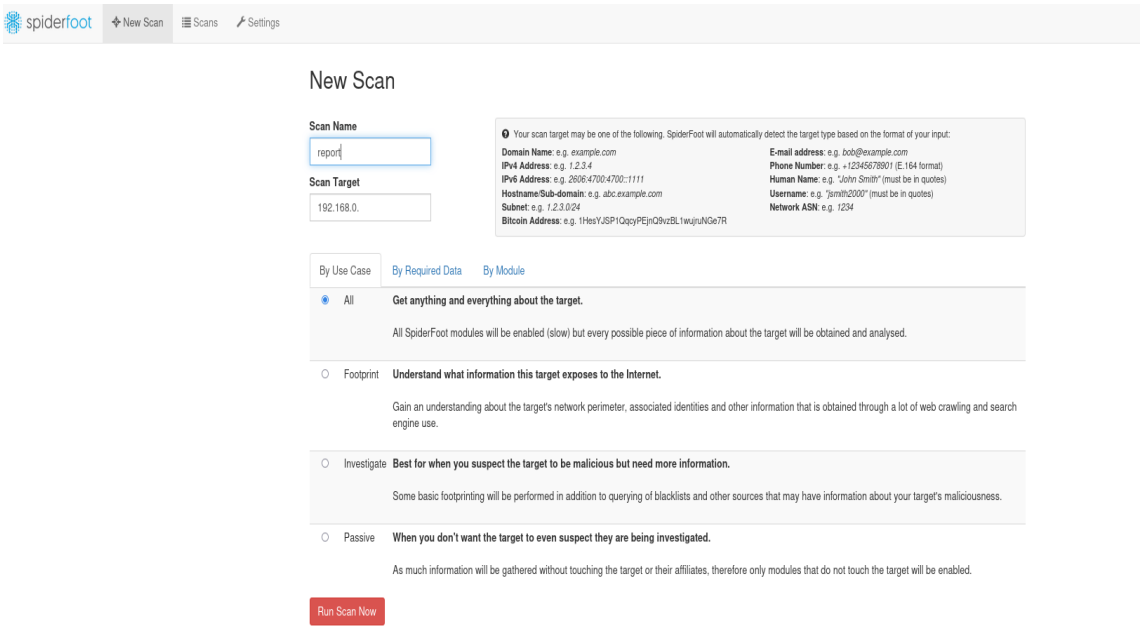


Figure 26

3.8 Nessus Tools:

Description: Nessus is a leading vulnerability scanner by Tenable, which can find security vulnerabilities in databases, applications, systems, and networks. When employed in Kali Linux, it enhances penetration testing by conducting extensive vulnerability analysis through its intuitive web interface and dense plugin set. The process involves the downloading and installation of the Nessus Debian package, bootstrapping the service, and setting up scans using the web interface (referenced at https://localhost:8834), and targets and scan policies. Nessus scans for vulnerabilities, misconfigurations, and compliance issues and reports with detailed information including severity ratings, remediation information, and exportable formats like HTML or PDF. Key highlights are an extensive, well-maintained plugin database, scan templates that can be customized, web application scanning, compliance checking, as well as Kali toolset integration, which makes it perfect for security experts. Frequent plugin updates and strategic target selection make it effective in managing vulnerabilities, but it calls for a separate Kali installation for smooth operation

3.8.1 Work Process of Nessus on Kali Linux

- **Open Nessus in this terminal:**
- **Open In browser:** https://localhost:11127 (any local browser)

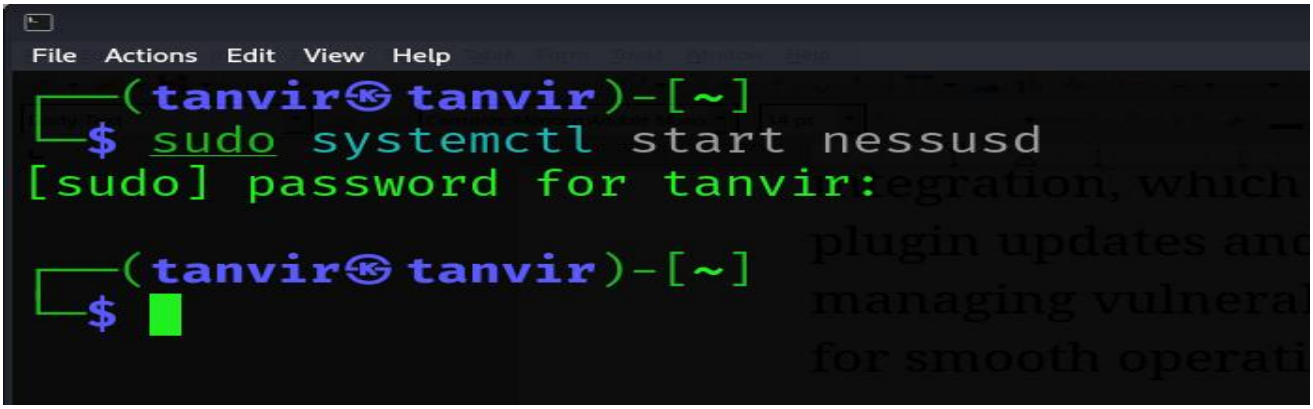


Figure 27

- **I did work:** We command in terminal and run Nessusd

- **Log in interface:**

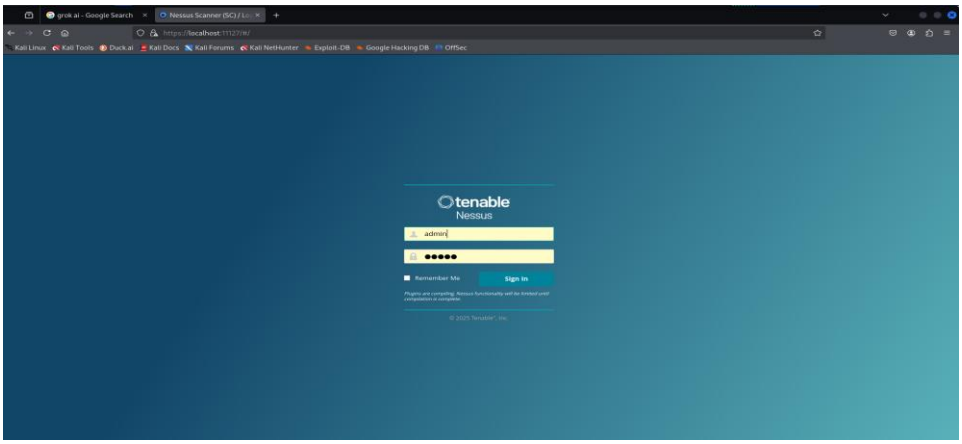


Figure 28

- **I did work: We login nessusd website use Username & Password**
- **Plugin the software:**

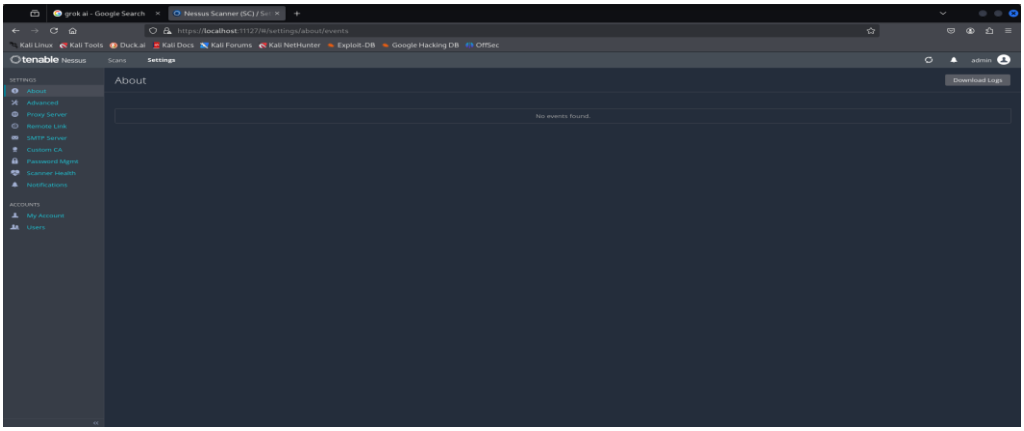


Figure 29

- **I did work: Plugin all service in nessusd**

- **Nessus Home page:**

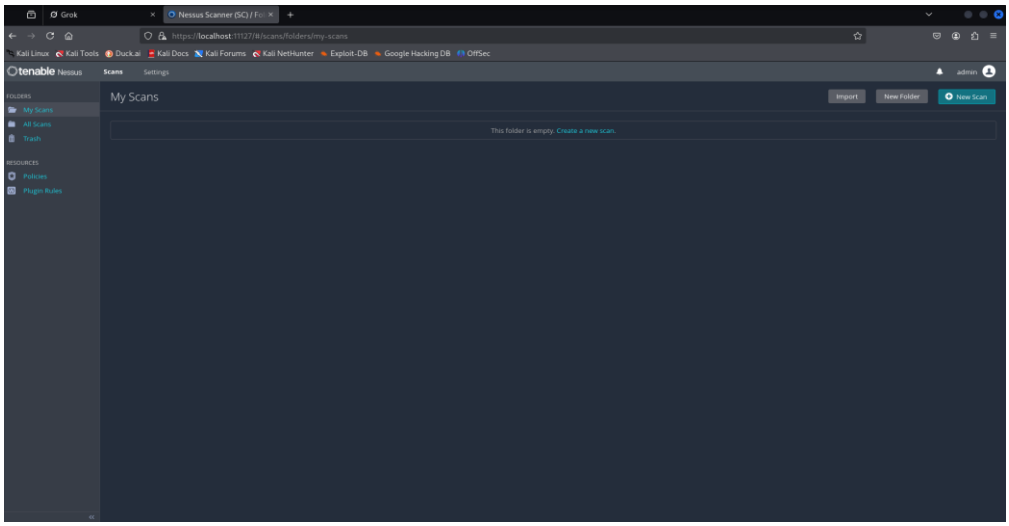


Figure 30

- **Scan Templates:**

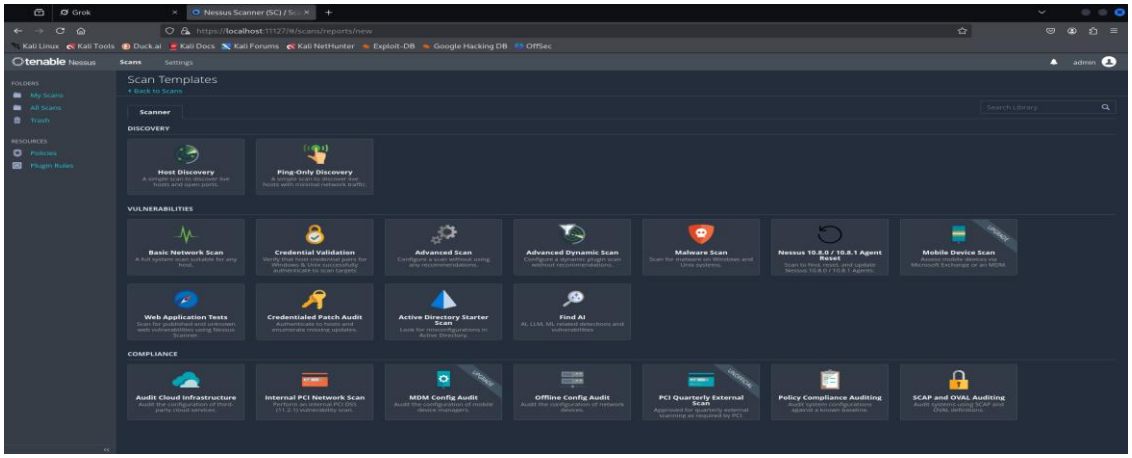


Figure 31

- **New Scan for Host Discovery:**

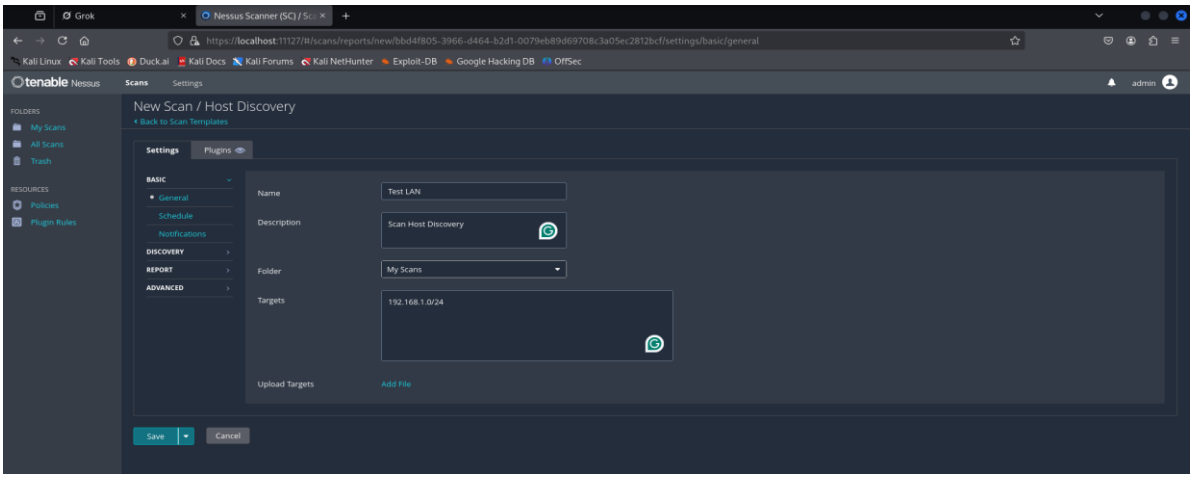


Figure 32

- **I did work: We start new scan for host discovery. We setup scan technique**
- **Save Scan**

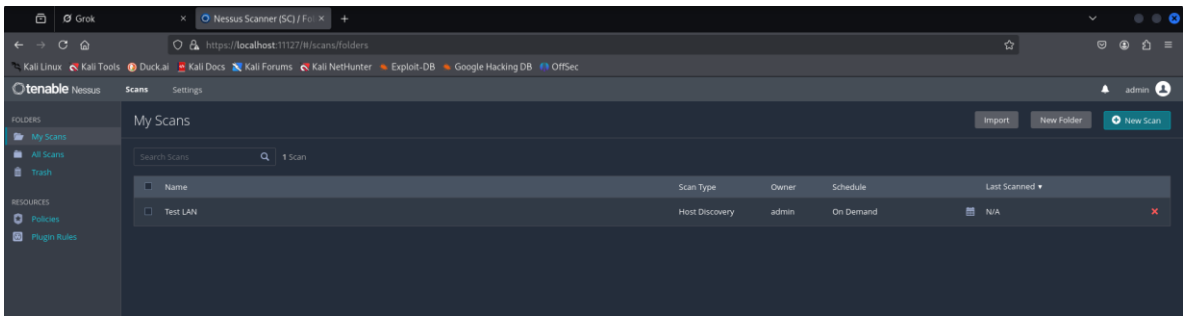


Figure 33

- **I did work: Save the scan for scanning host discovery**
- **Lunch the Scanning:**

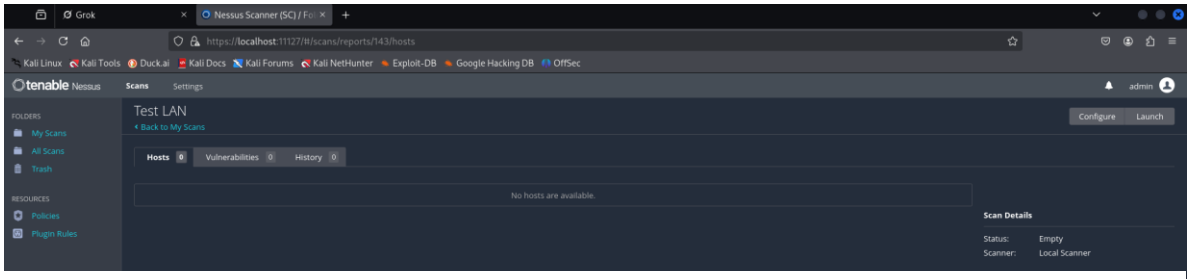


Figure 34

- **I did work: Lunch the host discovery scanning**

- **Start Scanning:**

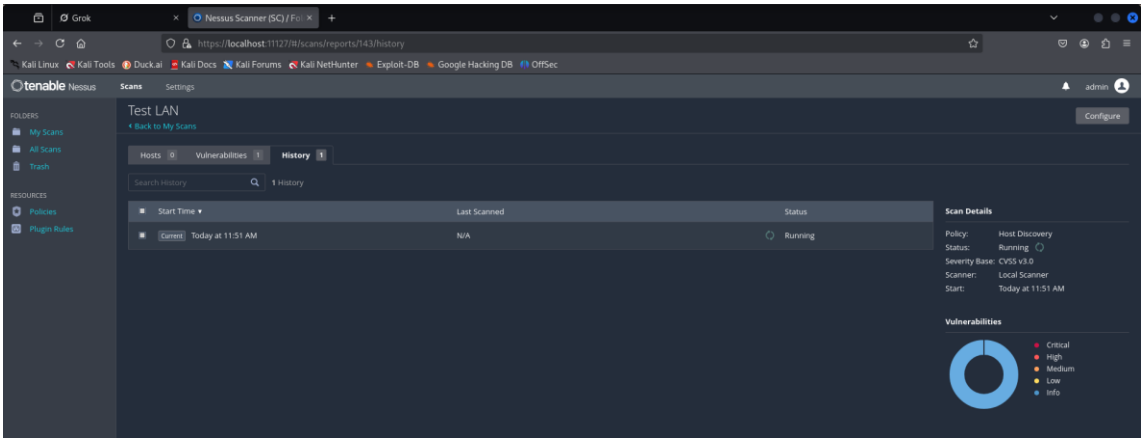


Figure 35

- **Scanning Complete:**

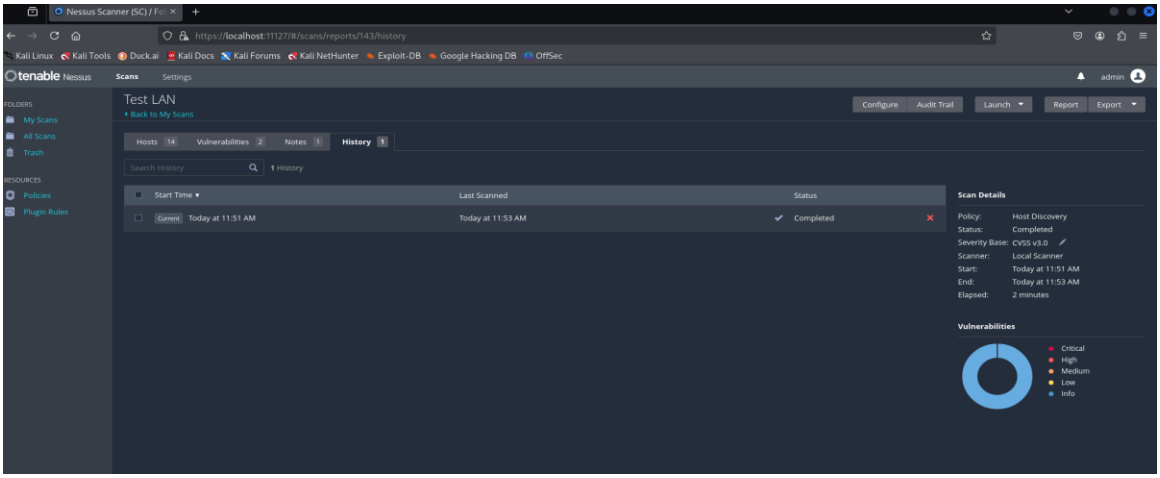


Figure 36

- **Host Discovery after scanning:**

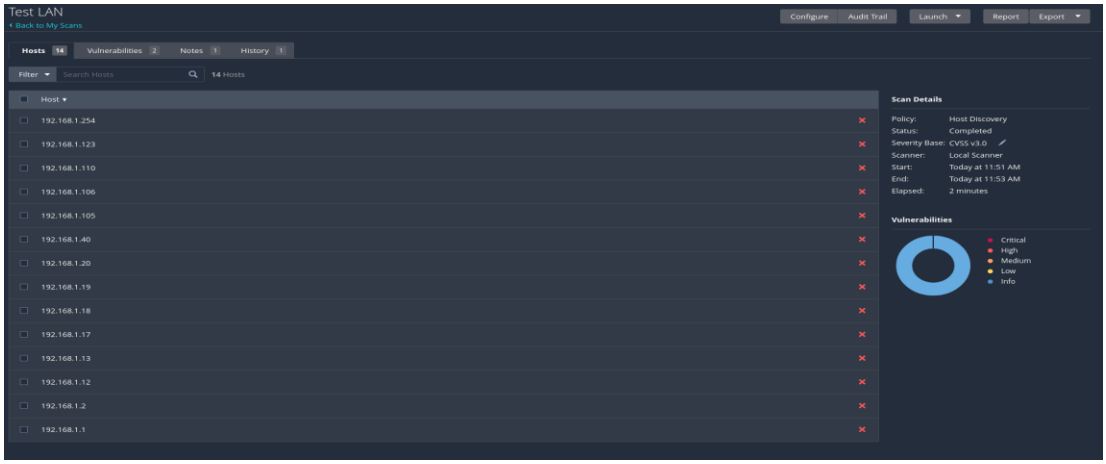


Figure 37

- **Venerability Find After scanning:**

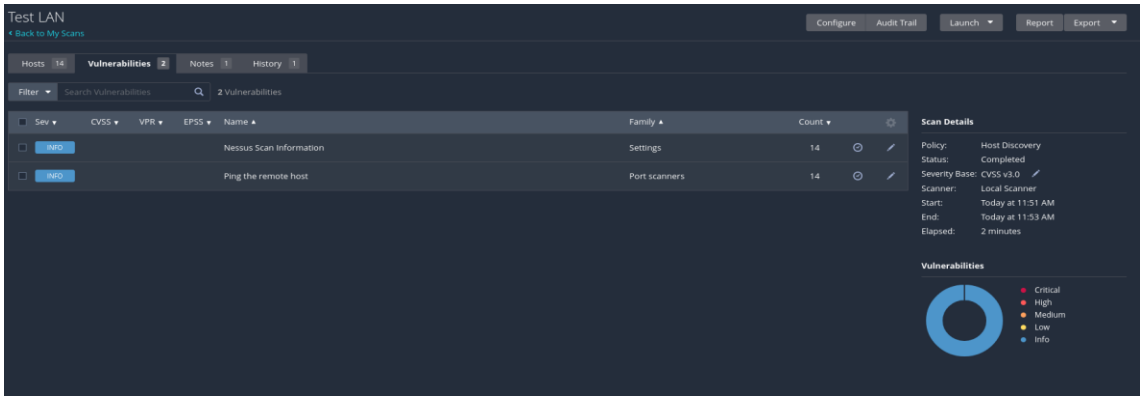


Figure 38

- **Generate Scanning:**

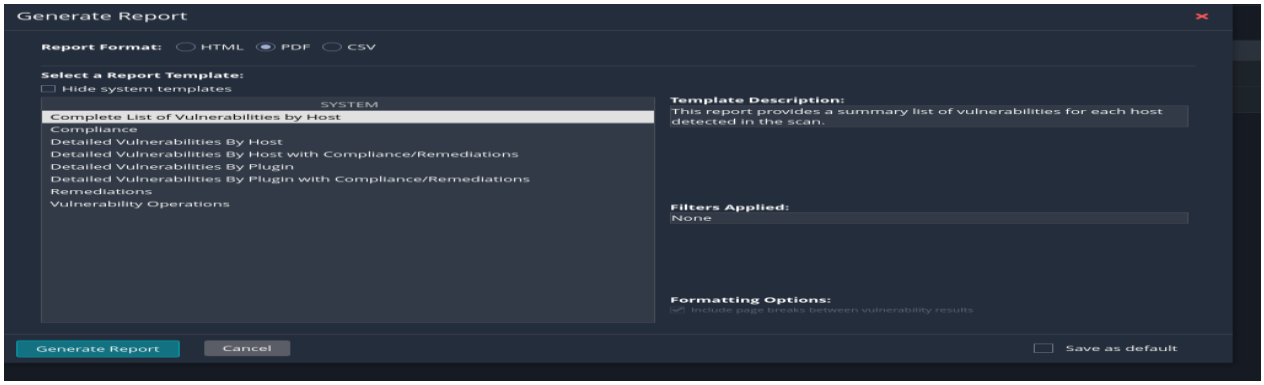


Figure 39

3.9 OpenVAS:

Description: OpenVAS (Open Vulnerability Assessment System), now known as Greenbone Vulnerability Manager (GVM), is a powerful open-source vulnerability manager and scanner that is pre-installed in Kali Linux, one of the most popular distributions for security professionals and penetration testers. It utilizes a large database of over 50,000 Network Vulnerability Tests (NVTs) to identify and detect vulnerabilities in networks, servers, applications, and endpoints, which are regularly updated to counter new threats. OpenVAS offers capabilities for both authenticated and unauthenticated testing across high- and low-level network protocols, industrial protocols, and custom vulnerability tests, making it a versatile tool for cybersecurity assessments. It provides detailed reports based on severity (low, medium, high) according to the Common Vulnerability Scoring System (CVSS) and is capable of tuning for large scans. It features a web-based tool, the Greenbone Security Assistant, which can be accessed through a browser at https://localhost:9392, allowing users to scan, manage tasks, and analyze results through an easy-to-use interface. OpenVAS is resource-intensive, requiring sufficient RAM and CPU resources, making it ideal for penetration testers and businesses looking for a cost-effective open-source solution for vulnerability management.

3.9.1 Work Process:

- **Open OpenVAS in Terminal:**
- **Command:** "sudo gvm-start"

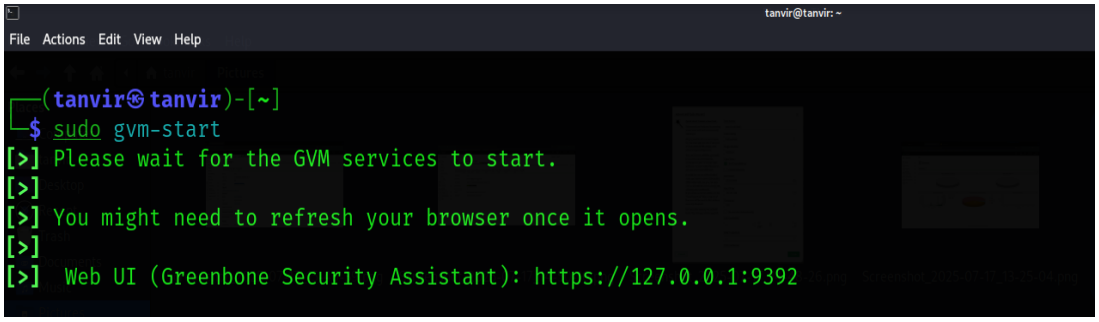


Figure 40

- **Open a browser :** open this link https://localhost:9392
- **Open Greenbone Security Login page:** log in Greenbone Security username & password

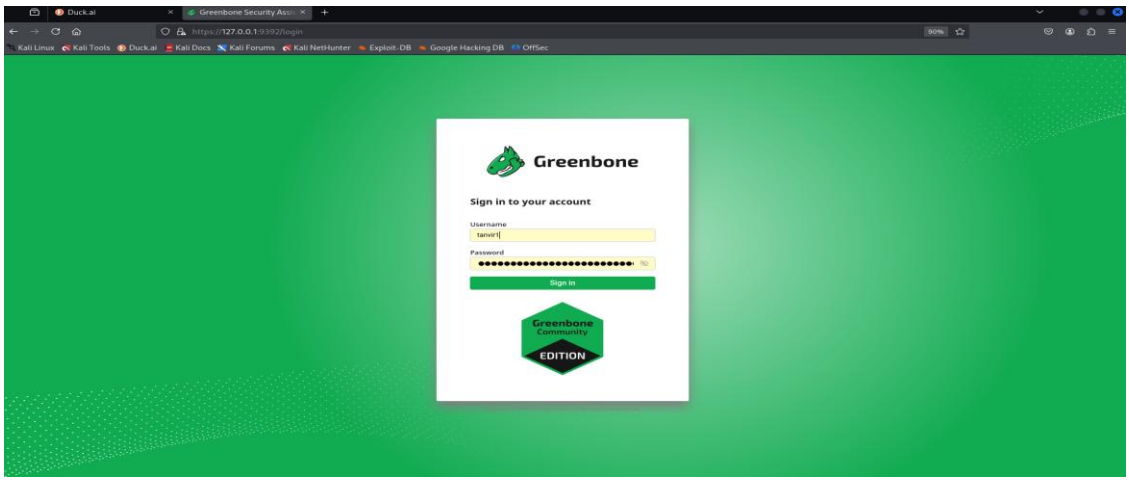


Figure 41

- **Open Dashboard:**

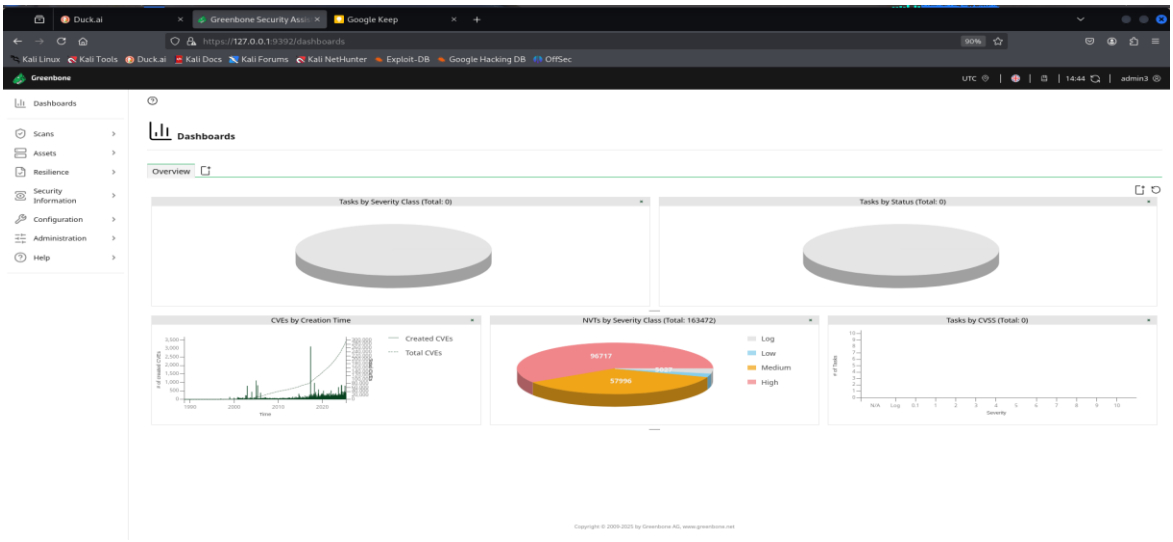


Figure 42

- **Scan Task :**

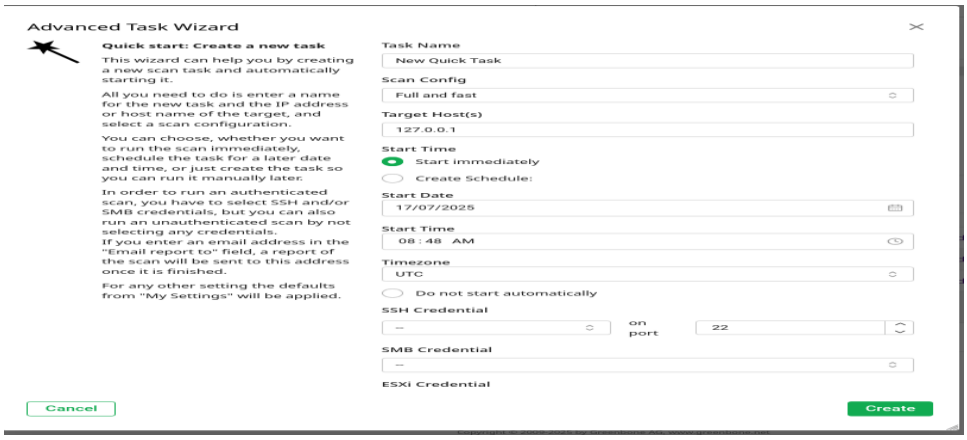


Figure 43

- **Lunch the scanning:**

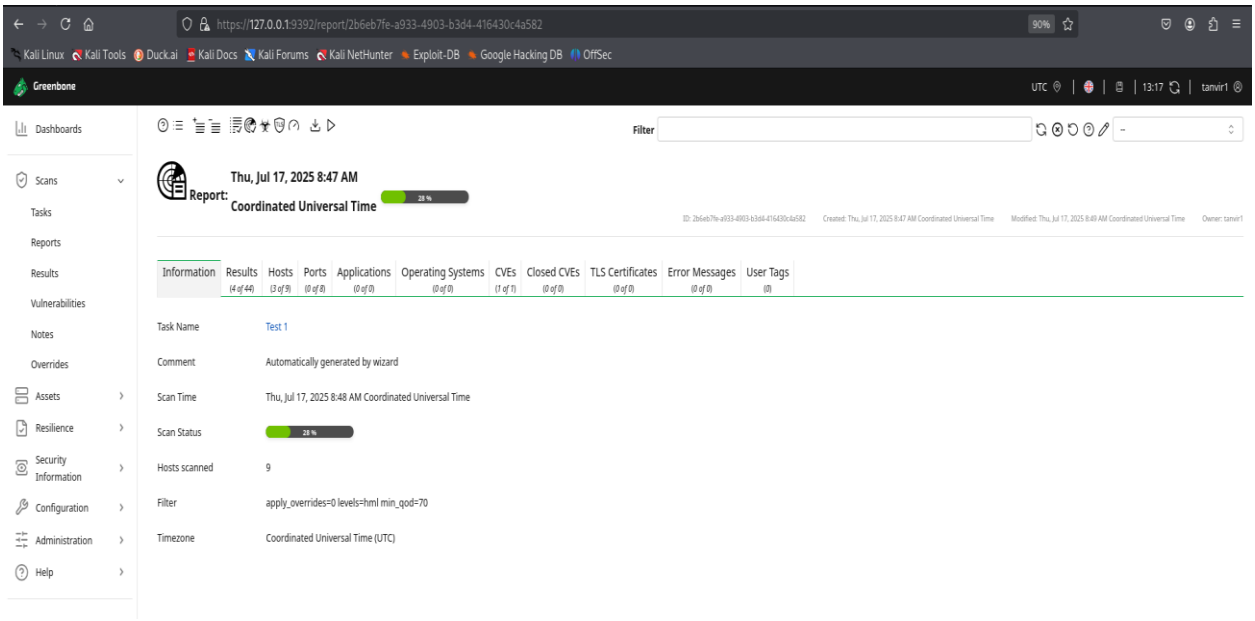


Figure 44

- **Complete Scanning:**

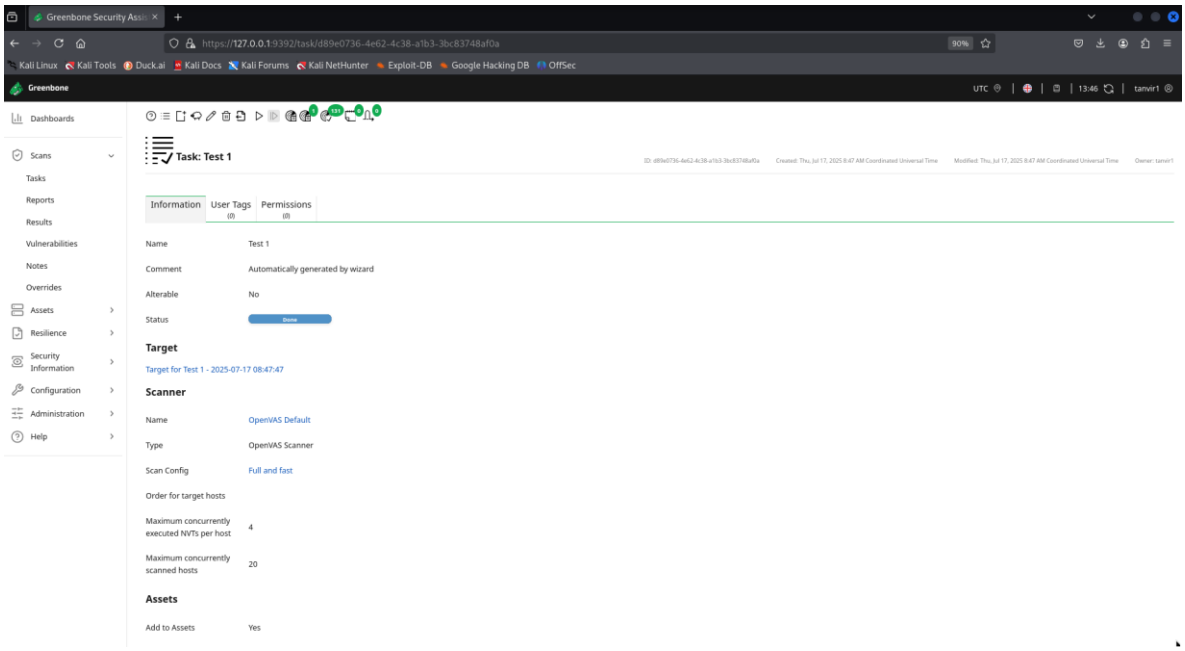


Figure 45

- **Stop Openvas in Terminal: " sudo systemctl stop gvmd "**

Figure 46

3.10 Zenmap

Description: The Nmap Security Scanner's official graphical user interface (GUI) is called Zenmap. This is an effective open-source tool for network exploration and security audits. It is compatible with Linux, Windows, and macOS, among other platforms. Nmap's command-line functionality is made simpler with Zenmap. While still offering sophisticated tools for seasoned users, this makes it simpler for novices to use. To locate hosts, open ports, services, and operating systems, users can perform network scans. Additionally, they can save their frequently used scans as profiles for easy access at a later time. A command creator for creating Nmap commands, a topology map for displaying network connections, and a searchable database for keeping and comparing scan results are all features of Zenmap's user-friendly interface. Zenmap is well-liked by network administrators and cybersecurity specialists for tasks like penetration testing and vendorability assessments because it provides comprehensive insights into network configurations and issues.

3.10.1 Work Process:

- **open Zenmap**
- **Zenmap home page:**

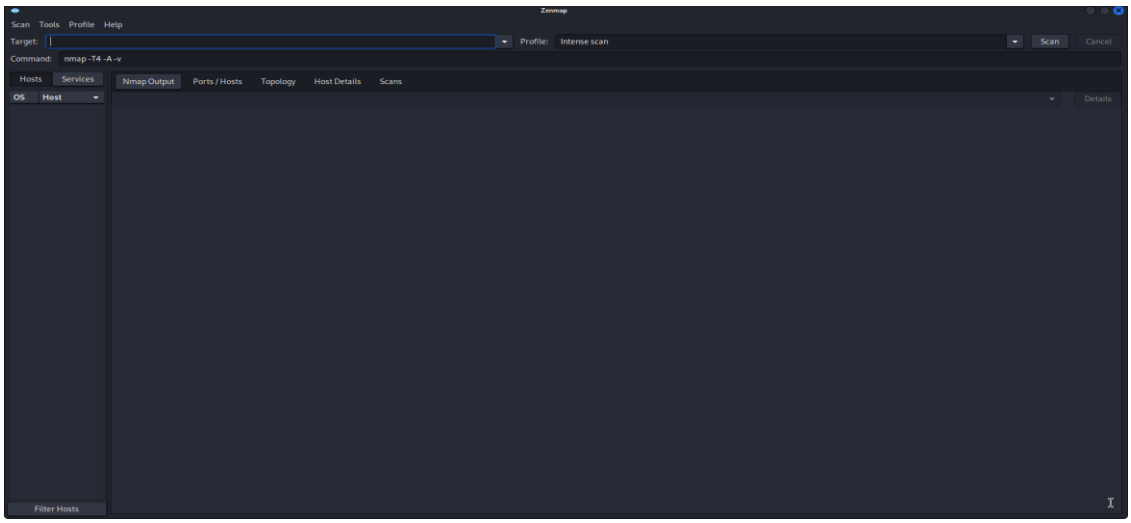


Figure 47

- **Set target ip and press scan:**

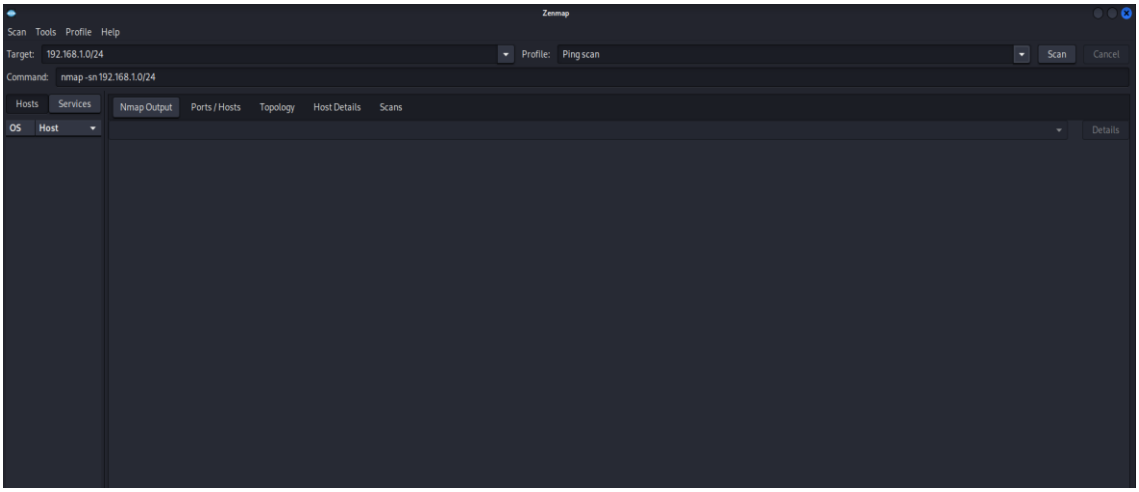


Figure 48

- **Complete scanning:**

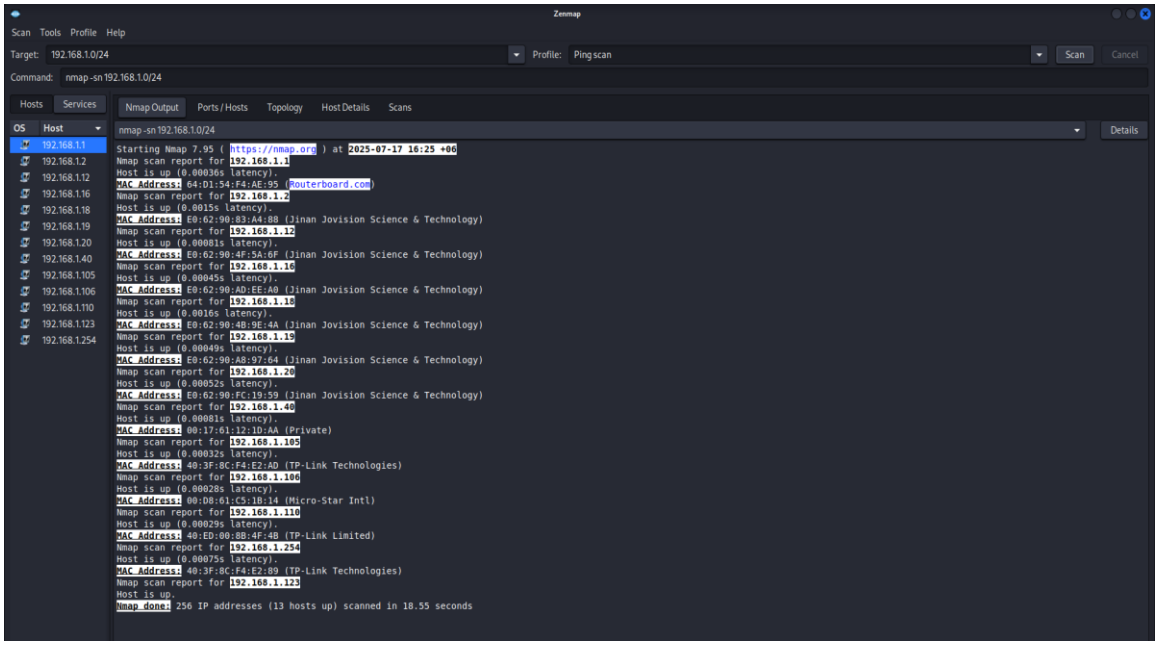


Figure 49

Digital Forensic

3.11 Oxygen Forensic

Description: Oxygen Forensic is a company that specializes in digital forensics and mobile data extraction. Their software solutions are widely used by law enforcement agencies, government institutions, and private organizations to recover and analyze data from mobile devices, cloud services, and other digital sources.

3.11.1 Key Features:

1. **Multi-Platform Support**: Oxygen Forensic works with many devices, including smartphones, tablets, and IoT devices on different operating systems like Android and iOS.
2. **App Data Recovery**: The software can pull data from popular apps, including social media, messaging, and email clients.
3. **Decryption Capabilities**: It can handle encrypted data, which lets forensic experts access information that might otherwise be hard to get.
4. **User-Friendly Interface**: Forensic analysts can easily navigate and use the software thanks to its intuitive design .
5. **Keyword and Content Search**: Users can locate particular keywords or phrases in the extracted data with the aid of the robust search function.
6. **Decryption and Password Recovery**: It enables access to encrypted data by decrypting data and recovering passwords.
7. **Evidence Management**: To ensure secure storage and convenient access for upcoming requirements, the software comes with tools for managing and preserving digital evidence.
8. **Reporting and Documentation**: It produces thorough reports that provide an overview of findings and include visual aids such as graphs and charts to clearly convey data for legal purposes.

3.11.2 Work Process:

► **Data Acquisition**:

- **Physical Extraction**: This entails obtaining a comprehensive picture of the storage on the device. This makes it possible to recover data and deleted files.
- **Logical Extraction**: This technique only extracts the device's accessible data. Contacts, messages, and app data are all included.
- **Cloud Extraction**: Data saved on cloud services connected to the device can be accessed by Oxygen Forensics tools. This includes Google Drive or iCloud backups.

► **Data Analysis**:

- **Data Visualization:** Graphic display of information to find patterns and relationships.
- **Keyword Search:** Looking for specific words in the extracted data.
- **Timeline Analysis:** Making timelines of events from timestamps in the data.

► **Reporting**:

- After the analysis, users may generate comprehensive reports that provide an overview of the findings. To clearly convey the data, these reports may contain graphs, charts, and other visual aids.

► **Evidence Management**:

- The software helps manage and store digital evidence, ensuring it is stored securely and can be accessed if needed for legal proceedings.

3.11.3 Work Process Screenshot:

- Open Oxygen Forensic
- **Oxygen Forensic Home page:**

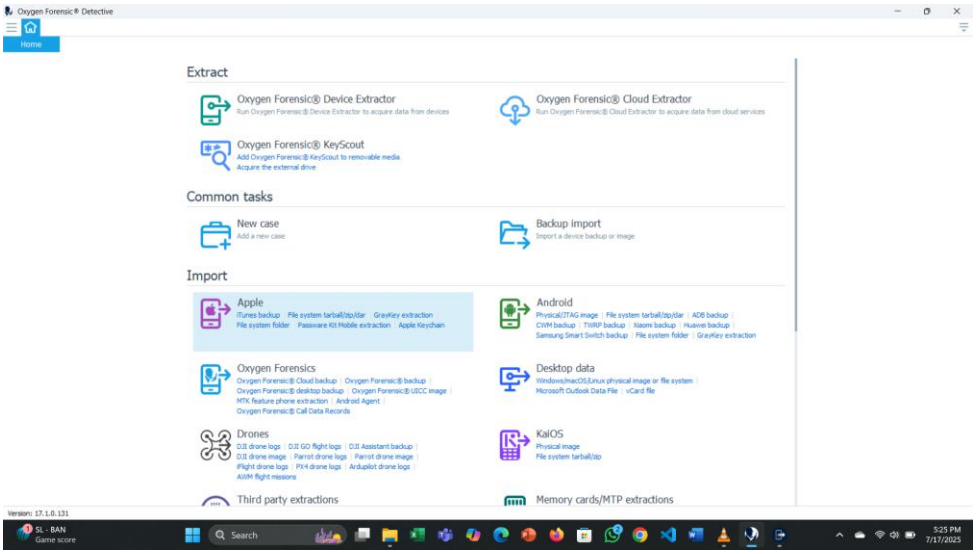


Figure 50

- **Device Connect option:**

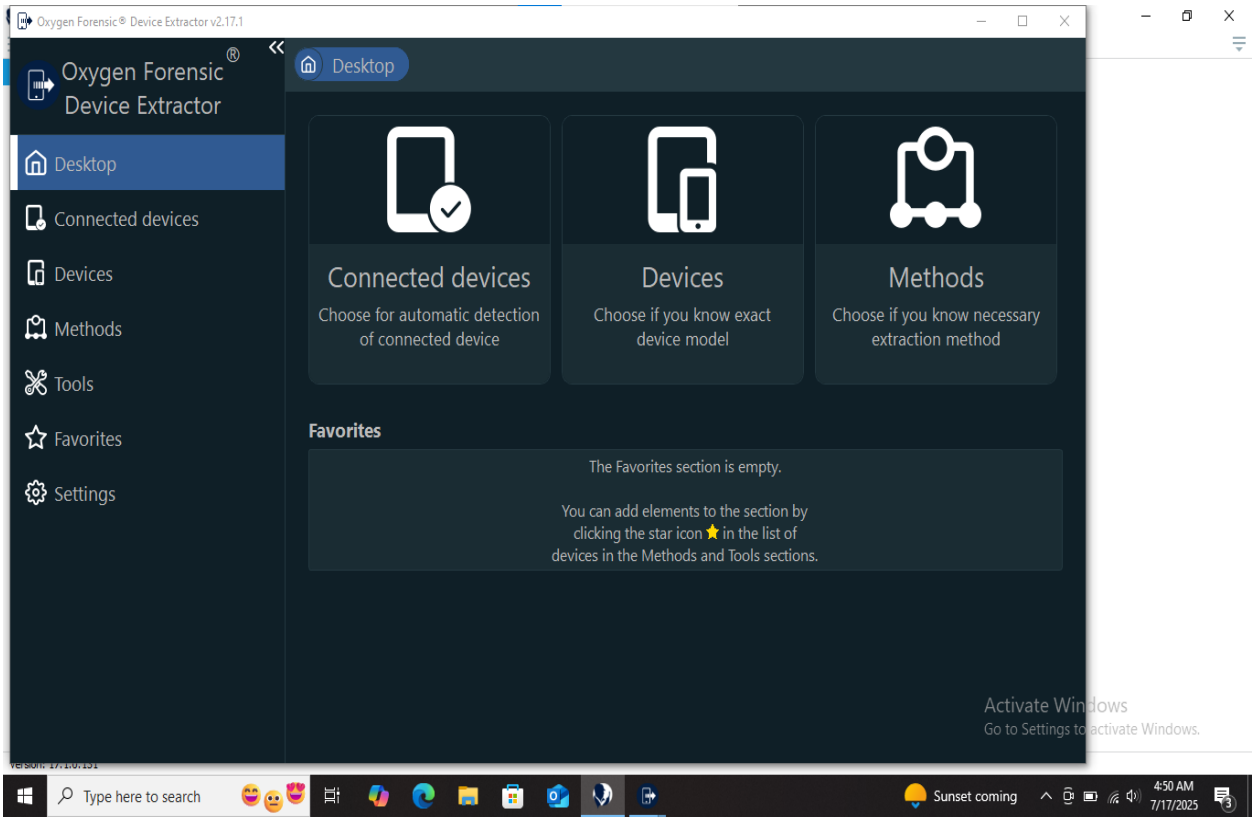


Figure 51

- **Connect device:**

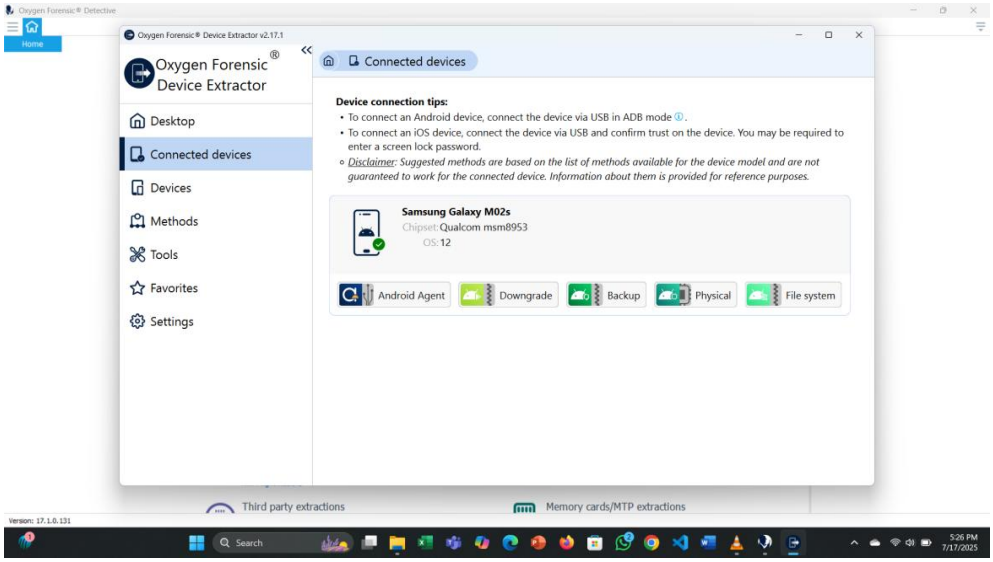


Figure 52

- **Select file system:**

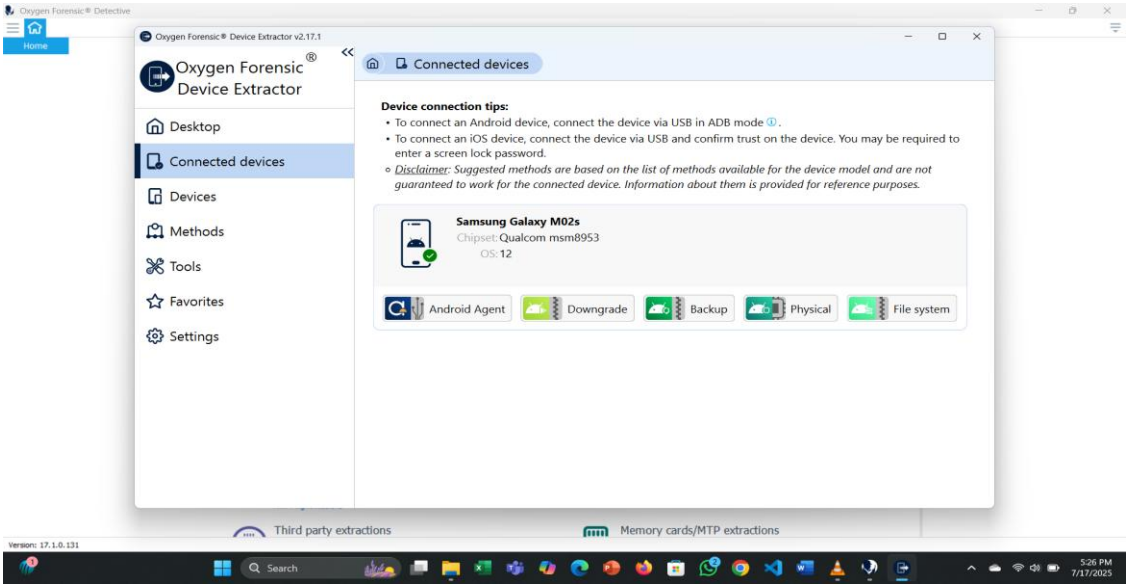


Figure 53

- **Find the Vulnerability: Exploit the vulnerabilities and root access this device.**

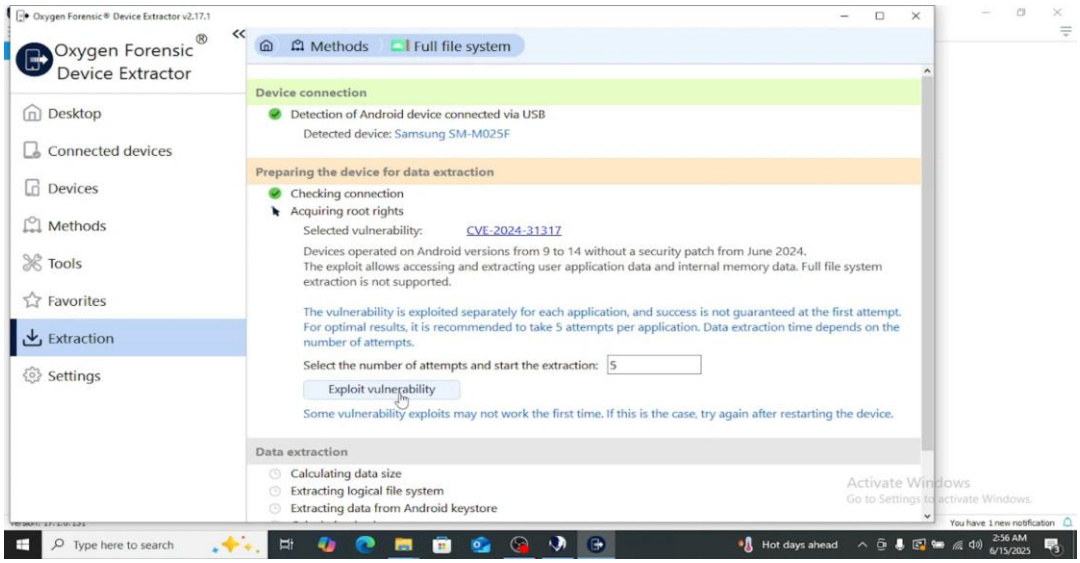


Figure 54

- **Import Android system :**

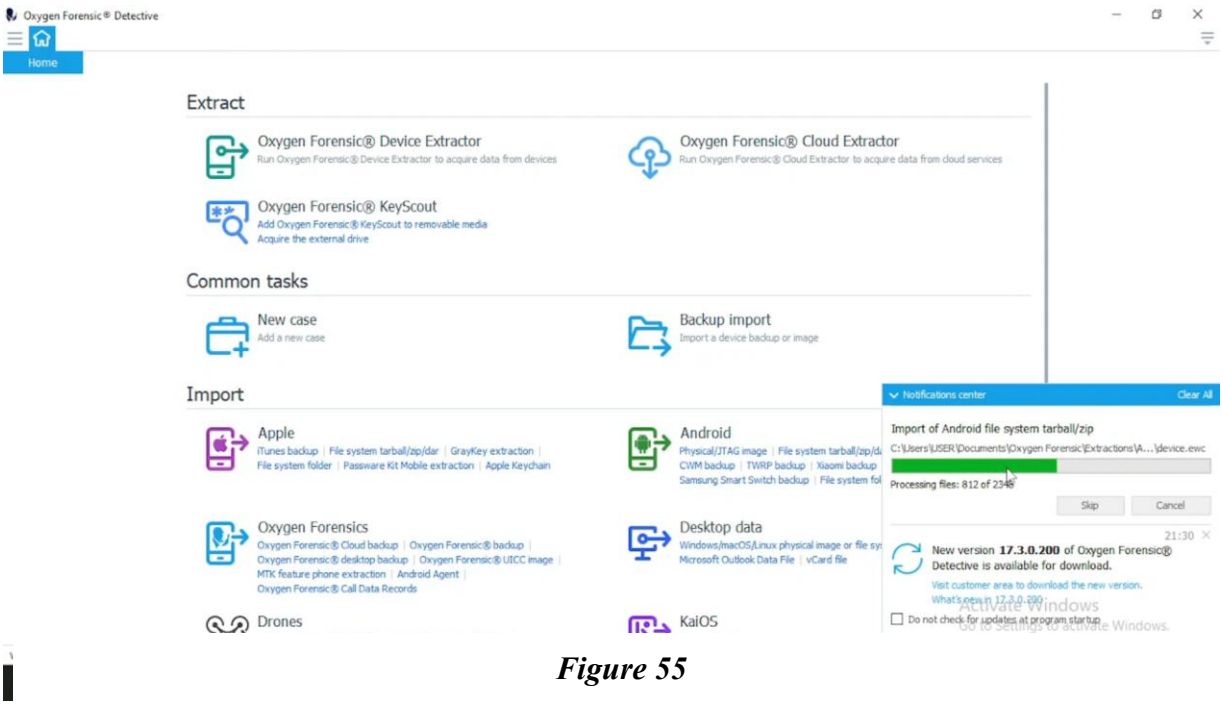


Figure 55

- **Import Backup file:**

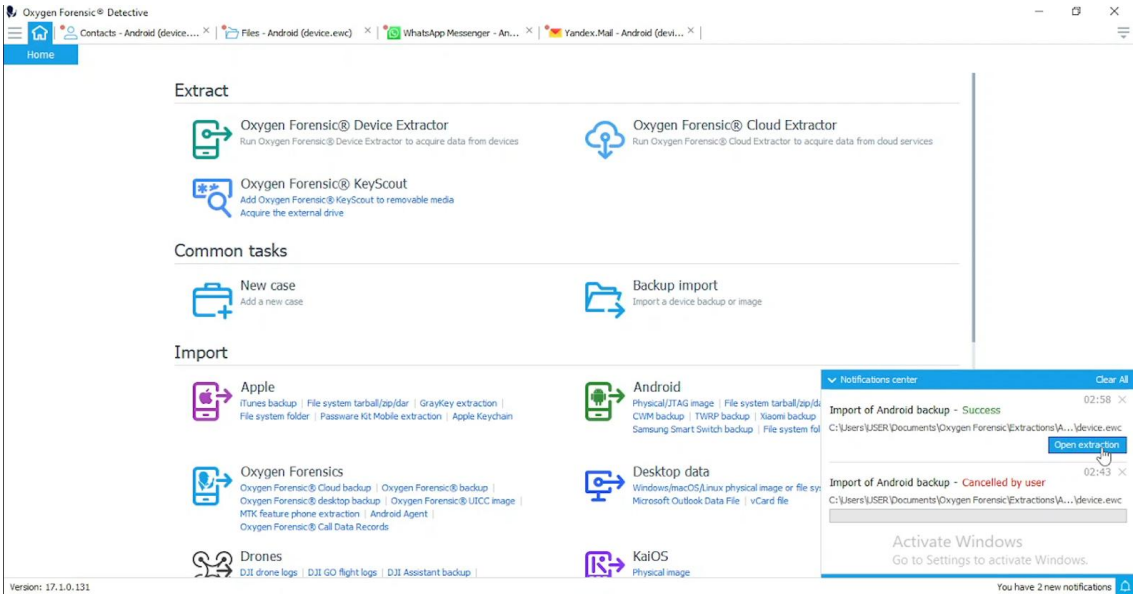


Figure 56

- **Recover file this Android system:**

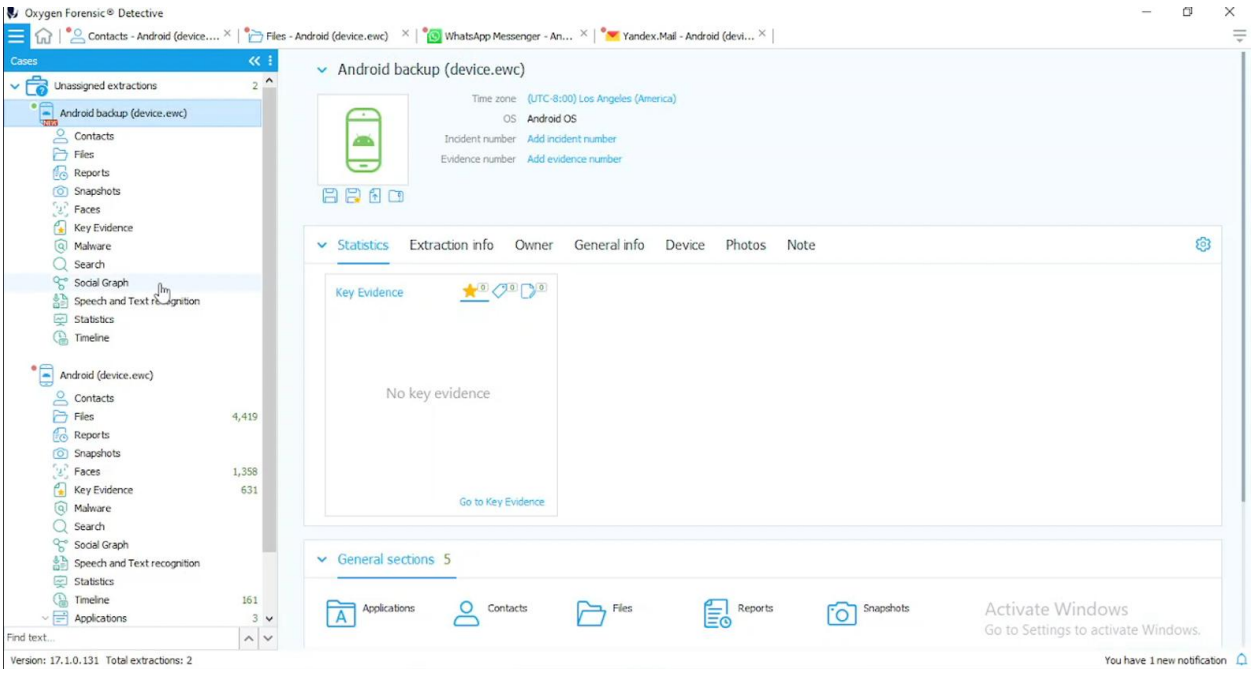


Figure 57

- **Malware Scanning this Android system:**

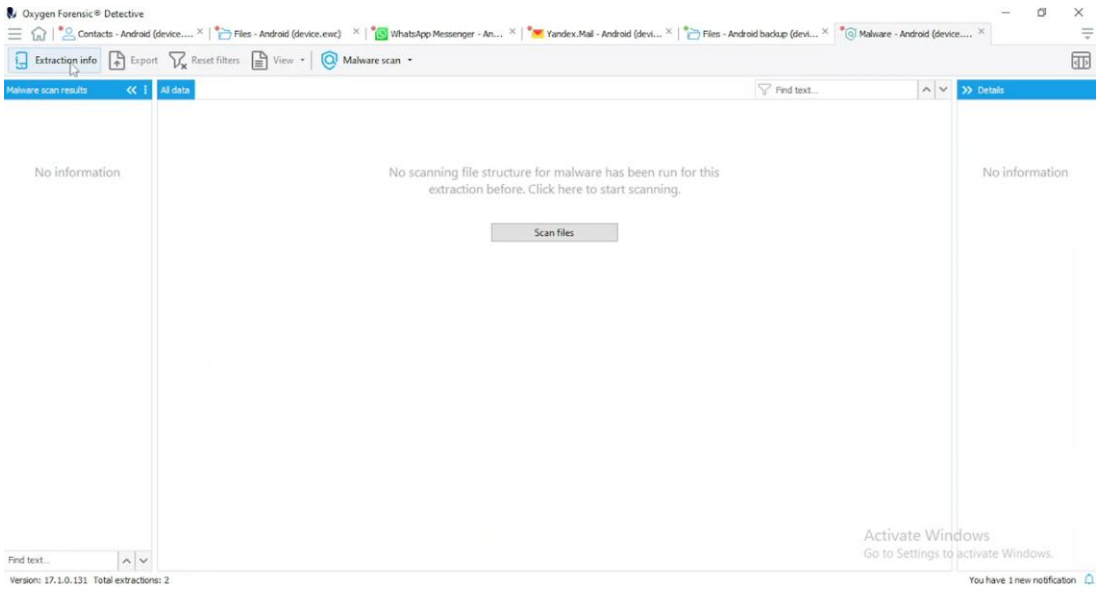


Figure 58

3.12 Autopsy:

Description: Autopsy is an easy-to-use, flexible tool that forensic investigators use to recover and analyze data from digital devices. It works with multiple file systems, manages different data sources, and offers features like file recovery, keyword searching, timeline analysis, and reporting. Law enforcement, cybersecurity, and incident response professionals widely use it for tasks such as recovering evidence, analyzing malware, and conducting criminal investigations.

3.12.1 Key Features of Autopsy:

► **Graphical User Interface (GUI)**

- **Description:** Autopsy has a simple, browser-like interface that makes complex forensic tasks easier. Even people who are not skilled with the command line can use it comfortably. It organizes data into browsable views, like file trees and timelines. It uses The Sleuth Kit for low-level analysis.
- **Benefit:** It simplifies workflows, lowers the learning curve, and improves usability for investigators.

► **Ingest Modules**

- **Description:** Modular plugins that automatically process data sources to collect artifacts.

 Hash Lookup: Compares files with known hash databases to find malicious or noteworthy files.

- **File Type Identification:** Identifies files by type, such as images or documents, for targeted analysis.
- **Keyword Search:** Finds user-specified terms or patterns within files, including unallocated space.
- **Email Analysis:** Extracts and parses email artifacts from file formats like PST or MBOX.
- **Web Artifacts:** Extracts browser history, cookies, and downloads from popular browsers.
- **Exif Data Extraction:** Extracts metadata from images and videos.

- **Benefit:** Automates evidence extraction and saves time while ensuring thorough analysis.

► File System Analysis:

- **Description:** There are several file systems supported ,and browsing of file structures, deleted files, as well as unallocated space is allowed. It extracts file metadata, such as creation/modification times, and reconstructs file fragments.
- **Benefit:** Enables detailed examination of storage media, necessary for retrieving lost or hidden information

► Timeline Analysis

- **Description:** Produces a timeline representation of file system activity in order to replicate user activity or incident timelines. Events can be filtered on date, file type, or source.
- **Benefit:** It helps investigators connect events and set patterns, such as opening or deleting a file.

► Hash-Based File Verification:

- **Description:** Computes and verifies file integrity using hash algorithms (MD5, SHA-1, SHA-256). Ensures the original evidence remains unaltered during analysis and matches known files against hash databases.
- **Benefit:** Maintains chain of custody and supports forensic admissibility in legal proceedings.

► Deleted File Recovery

- **Description:** Recovers deleted files and file fragments from unallocated space or partially overwritten data using file system metadata and carving.
- **Benefit:** Restores critical evidence that has been intentionally hidden or accidentally deleted.

► Reporting Tools

- **Description:** Generates reports that can be customized to include findings, labeled evidence, timelines, and investigator notes in formats like HTML, PDF, or Excel. Reports can include screenshots, file details, and metadata.
- **Benefit:** Facilitates good communication of results for legal, law enforcement, or client consumption.

► Open-Source and Community Support

- **Description:** All are free to use, with an active contributing community delivering updates, plugins, and documentation. Regular releases ensure compatibility with new file systems and forensic challenges.
- **Benefit:** Affordable and adaptable with a rich pool of community-based resources.

3.12.2 Work Process:

► Create a New Case

- **Description:** Begin by launching Autopsy and creating a new case to keep track of all the evidence, logs, and reports. You specify a case name, an optional case files storage directory, and optional data like the investigator name or case number. Autopsy populates a case database with all analysis results.
- **Purpose:** Provides a systematic setting for the investigation such that all the data is referenced to a case for traceability and structuring.
- **How It Works:** Inside Autopsy, click "New Case," enter the required information, and save. The case folder is created on the disk, and Autopsy sets up a database for metadata and results storage.

► Add a Data Source

- **Description:** Select the data source to investigate, for instance, a disk image (RAW), a logical drive, a mobile dump device, or a memory dump. Autopsy is compatible with multiple file systems. You specify the source location and optionally verify its hash (MD5/SHA-256) to ensure integrity.

- **Purpose:** Specifies the evidence to be processed, making sure Autopsy handles the right information and maintains its original form.
- **How It Works:** In the "Add Data Source" wizard, choose the source type, go to the file or device, and accept. Autopsy transforms the file system into a usable analysis format without modifying the original data.

► Configure Ingest Modules

- **Description:** Choose and configure ingest modules to automatically extract artifacts from the data source. These modules run during data processing and include:

 Hash Lookup: Compares file hashes against databases (e.g., NSRL) to identify known files (e.g., malware or contraband).

 File Type Identification: Sorts files by type (e.g., images, videos, documents) for targeted review.

 Keyword Search: Searches for user-defined terms or patterns (including regex) in files and unallocated space.

 Email Analysis: Extracts emails and attachments from formats like PST or MBOX.

 Web Artifacts: Collects browser history, cookies, and downloads from browsers like Chrome or Firefox.

 Exif Data Extraction: Pulls metadata (e.g., timestamps, GPS) from images and videos.

 Recent Activity: Identifies recent user actions, such as USB connections or file access.You can customize module settings, such as enabling specific hash databases or defining keyword lists.

 Purpose: Automates evidence extraction, reducing manual effort and ensuring comprehensive analysis.

- **How It Works:** In the “Ingest Modules” section, choose the modules you want. Configure their settings, such as uploading a keyword list. Then, start the ingest process. The modules run in the background, and you can see the progress.

► Process the Data Source (Ingest)

- **Description:** Autopsy processes the data source by parsing the file system, recovering deleted files, and running the selected ingest modules. It extracts metadata, artifacts, and file content, and it writes findings

to the case database. Hash values are computed to provide data integrity, and the original evidence is not modified. It is a time-intensive step, depending on the data size and the complexity of the modules.

- **Purpose:** Converts raw data into structured, queryable output to enable efficient analysis.
- **How It Works:** After modules are configured, click "Finish" to start ingestion. Autopsy ingests the data source, with progress bars for each module. Users can pause or prioritize tasks as needed.

► Analyze Results

- **Description:** Once ingestion is complete, explore the results using Autopsy's interface. Key analysis features include:
- **File View:** Browse files by directory, type, or status (deleted, allocated).
- **Timeline View:** Visualize file system events (creation, modification) chronologically to reconstruct activities.
- **Keyword Hits:** Review matches for search terms or patterns, including context from files or unallocated space.
- **Web Artifacts:** Examine browser history, downloads, or cookies organized by browser.
- **Email Artifacts:** View extracted emails, attachments, and metadata.
- **Tagging/Bookmarking:** Flag important files or artifacts for quick reference, with customization tags (Evidence). Filters and search tools help narrow down results, and relationships (email threads or file access patterns) can be visualized.
- **Purpose:** Enables investigators to identify, correlate, and interpret evidence to build a case or answer investigative questions.
- **How It Works:** Use the left-hand tree view to navigate data categories (File Types, Results). Click on items to view details, preview content, or export files. Use filters or sorting options to focus on specific data.

► Recover Deleted Files

- **Description:** Autopsy retrieves deleted files or file fragments from unallocated space using file system metadata or by using data carving techniques. The recovered files are shown in the "Deleted Files" view, with details like original path or partial content.

- **Purpose:** Retrieves vital evidence that has been intentionally deleted, incriminating documents or images.
- **How It Works:** During scanning, the "File Recovery" module identifies deleted files. Navigate to the "Deleted Files" node in the interface to review and export recoverable files.

► Generate Reports

- **Description:** Create detailed reports consolidating findings, such as tagged evidence, timelines, keyword hits, and file metadata. Autopsy supports different formats (HTML, PDF) and allows for customization. Reports can focus on specific artifacts or present a basic case synopsis.
- **Purpose:** Documents the investigation for legal proceedings, client reports, or team collaboration.
- **How It Works:** Navigate to the "Reports" menu, select a report type, and choose what data to report. Configure options, execute the report, and save or export.

3.12.3 Limitation:

► Processing Time for Large Datasets

- **Description**: Analyzing Big data sources, such as multi-terabyte disk images, can be time-consuming, especially when multiple ingest modules (keyword search, hash lookup) are enabled. The processing speed depends on system resources and the complexity of the analysis.
- **Impact**: Delays investigations when time is critical, requiring investigators to prioritize modules or use high-performance hardware to mitigate.

► Resource Intensive

- **Description:** Autopsy uses high system resources (CPU, RAM, disk space) to handle large data sets or run numerous ingest modules concurrently. Low-end systems can become sluggish or crash when under heavy loads.
- **Impact:** Users will need high-end hardware (multi-core processors, 16+ GB RAM) for efficient analysis, which will be cost-prohibitive for smaller agencies or individual researchers.

► Learning Curve for Advanced Features

- **Description:** Even if Autopsy's GUI is simple to work with, more advanced features like custom plugins, regex search, or timeline analysis require forensic experience and training. New users may struggle with complex configurations or interpreting results.
- **Impact:** May possibly require training or experience of digital forensics principles, limiting accessibility to beginners or non-specialists.

► Limited Mobile Device Support

- **Description:** Autopsy supports mobile device dumps (Android or iOS backups), but its native mobile device analysis features are not as robust as those of dedicated tools like Oxygen or Mobile Forensic . It may struggle with encrypted or proprietary mobile formats.
- **Impact:** Examiners may need additional tools for complete mobile forensics, which increases expense or workflow complexity.

► Dependence on File System Support

- **Description:** Autopsy supports common file systems, but may have partial or no support for rare, proprietary, or recently introduced file systems. Unsupported formats may interrupt analysis.
- **Effect:** Users may need to use other tools or convert data sources into appropriate formats, which complicates the process.

► Incomplete Deleted File Recovery

- **Description:** Although Autopsy is able to recover files deleted from file system metadata or data curving, recovery may not be complete, especially when data is overwritten or fragmented. This will work depending on the file system and deletion method.
- **Impact:** Critical evidence may be recoverable, potentially affecting the outcome of the case.

► Limited Real-Time Analysis

- **Description:** Autopsy is designed for post-mortem analysis of static data sources (disk images) and not for live system or real-time forensics. It lacks the capabilities for analyzing running systems or volatile memory in real time.
- **Impact:** Investigators require different tools (volatile memory forensics) to analyze live systems, which complicates incident response.

► Reporting Customization Restrictions

- **Description:** Although Autopsy supports report customization (HTML, PDF, Excel), the reporting interface is extremely flexible, not challenging with limited formatting choices or the integration of complex visualizations.
- **Impact:** For legal or professional presentations, increased workload may require manual post-processing of reports.

► Community-Driven Support

- **Description:** An open-source tool, Autopsy has community support rather than specialized commercial support. New features may have incomplete documentation, and bug fixes or updates are based on community contributions.
- **Impact:** Users are slow to get solutions or must go to community forums, which are less reliable than commercial tool support.

3.12.4 Work Process Screenshot Step by Step:

- Open Autopsy Tool in Windows and create a new case for a new case

- **Create a new case Details**

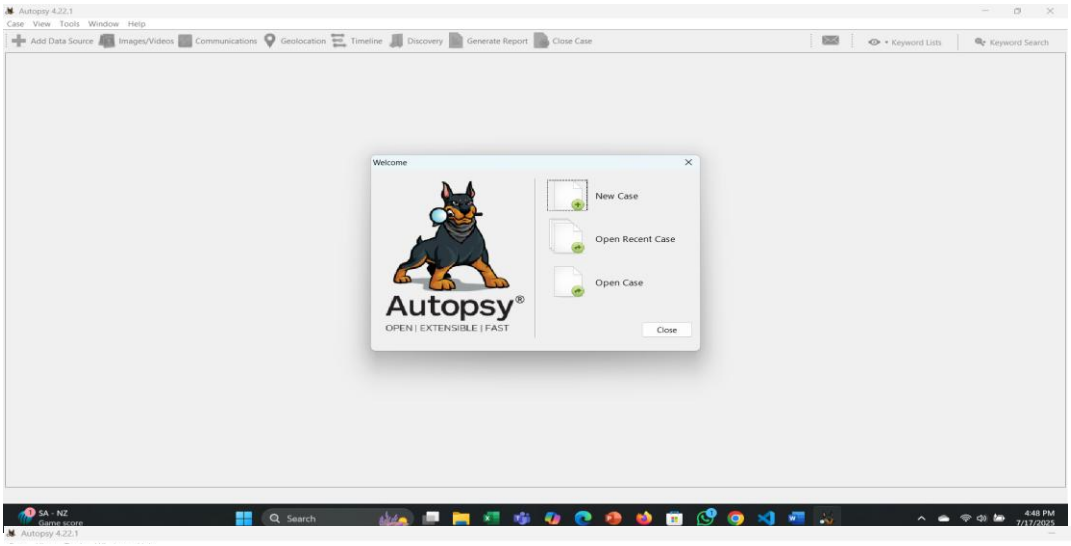


Figure 59

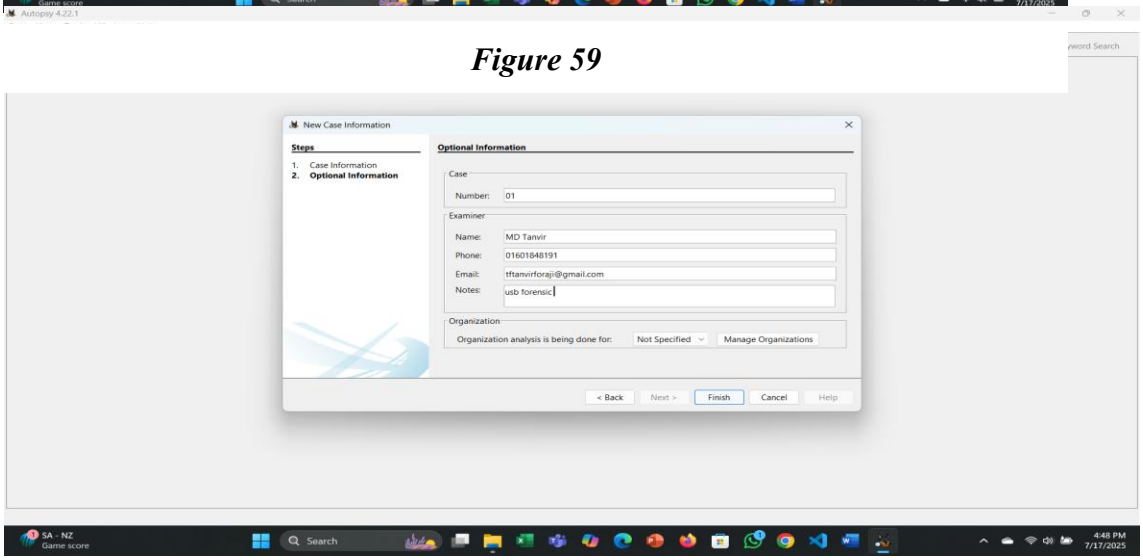


Figure 60

- **Select host**

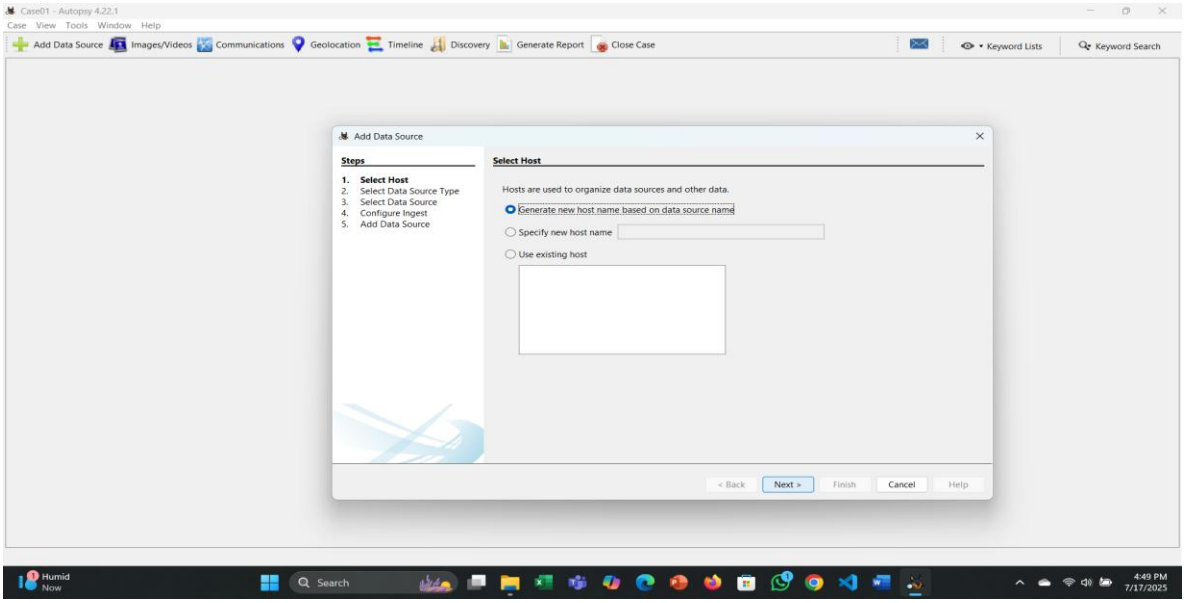


Figure 61

- **Select Data source:**

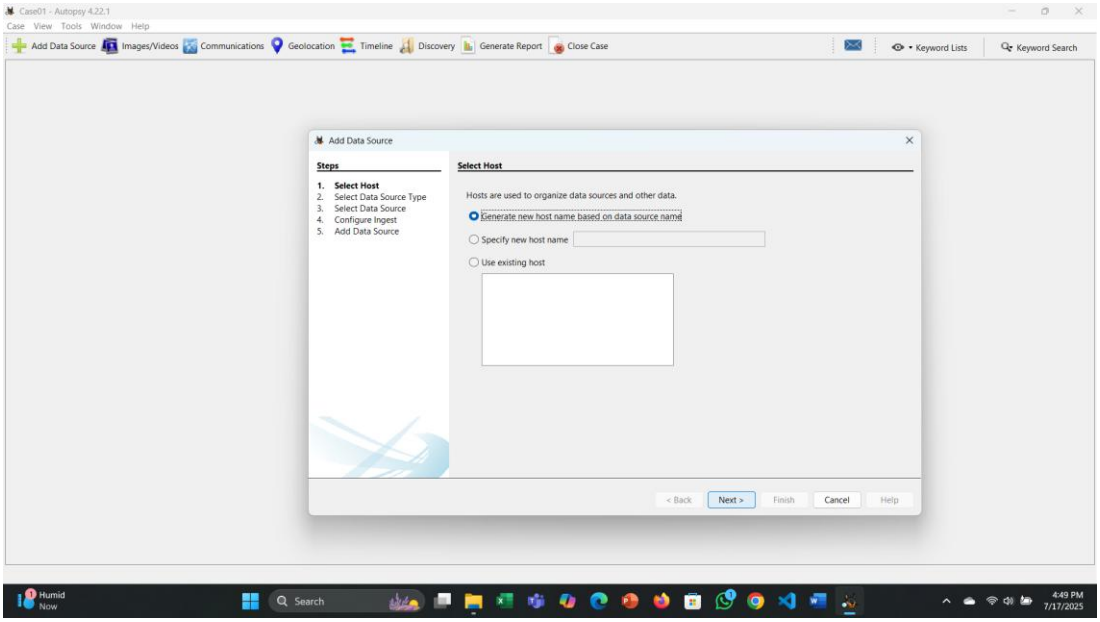


Figure 62

- **Select Data source:**

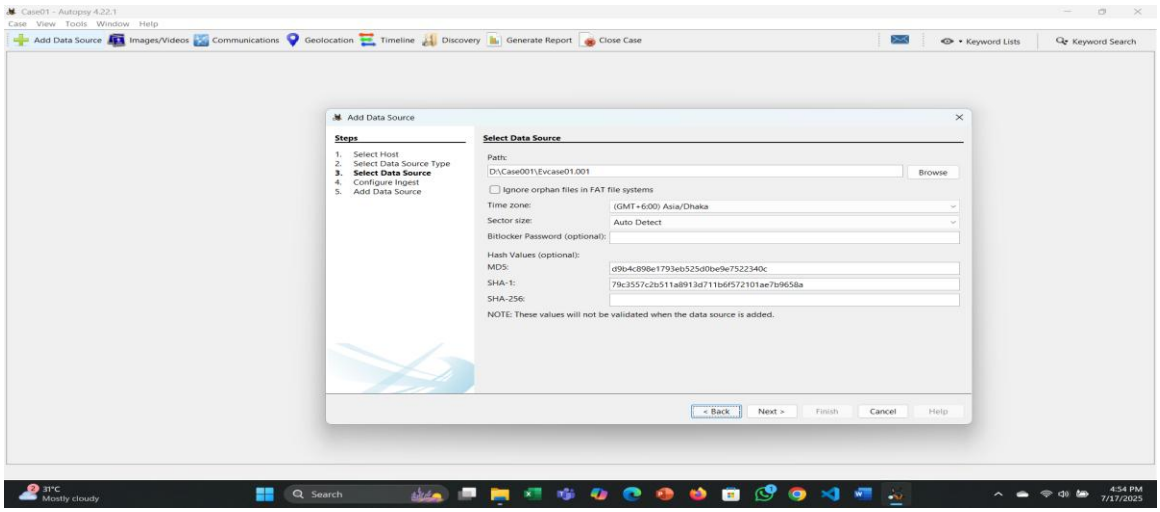


Figure 63

- **Configuration Ingest**

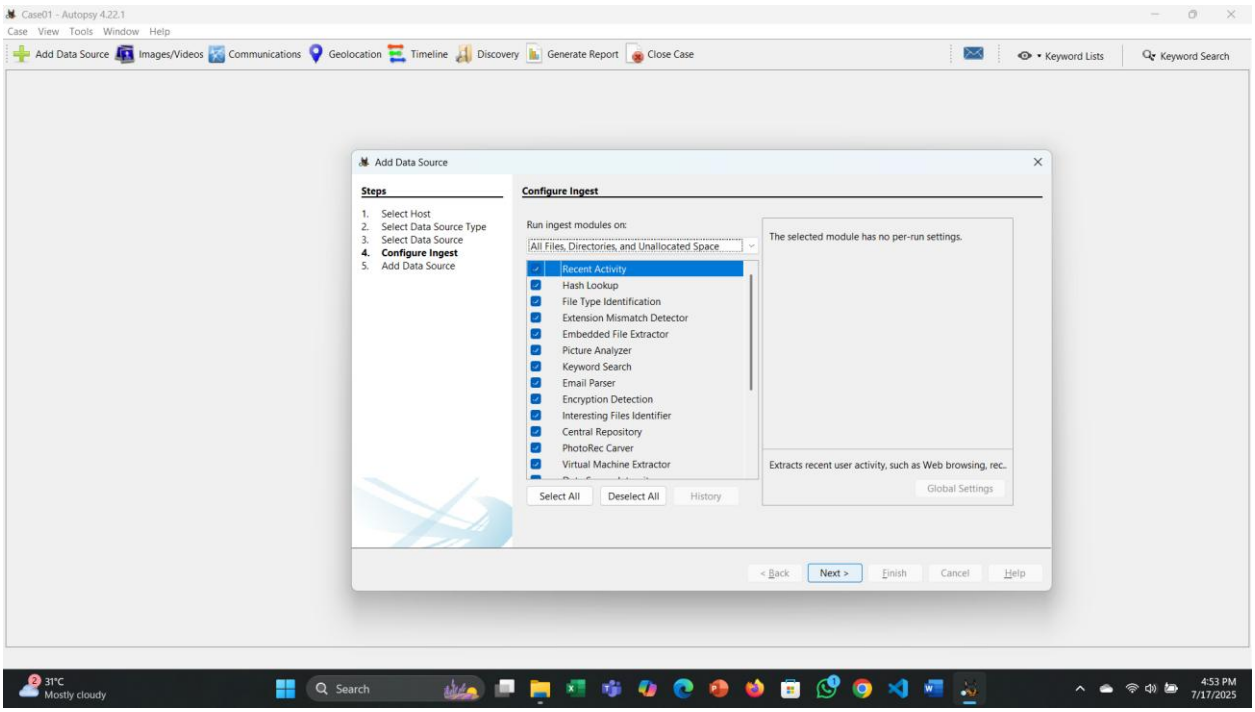


Figure 64

- **Creating this case to forensic to identify the evidence**

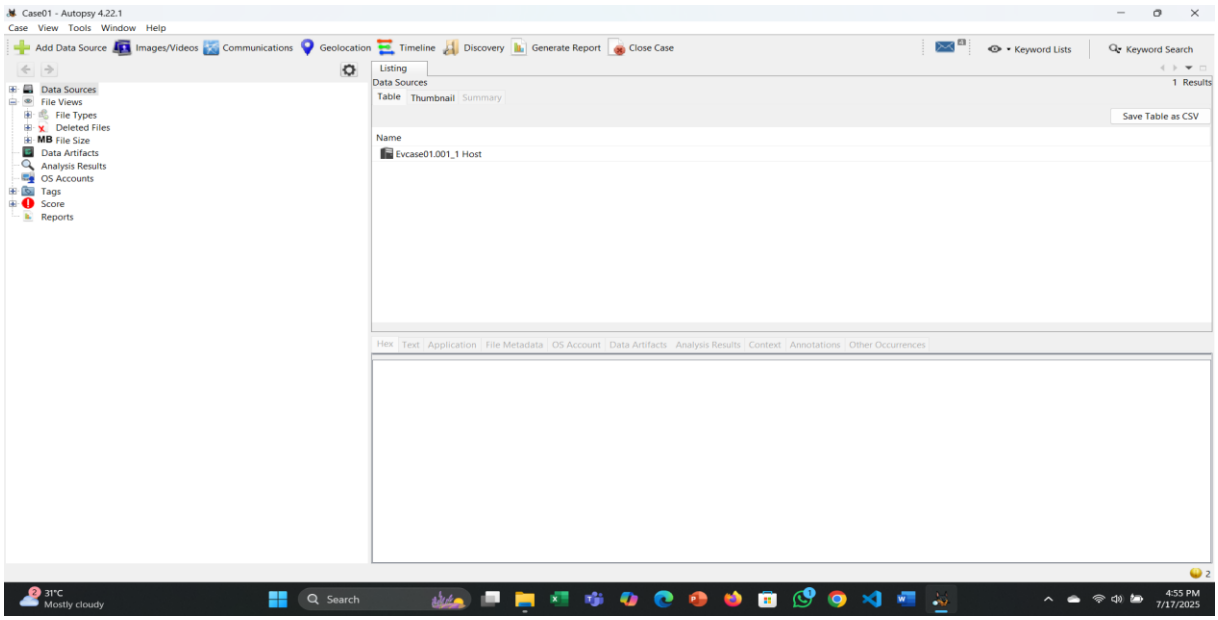


Figure 65

3.13

FTK imager:

Description: FTK Imager is a popular digital forensics tool created by Access Data. It helps with data preview, imaging, and analysis in forensic investigations. Users can make forensic images of computer hard drives, storage devices, and other digital media without changing the original data. This keeps the evidence intact using write-blocking methods. The tool is compatible with a variety of image formats, including DD, E01, and AFF. In a forensically sound manner, it enables examiners to view and extract data, including deleted files, file systems, and partitions. Features such as memory capture, hash verification (MD5, SHA-1), and the ability to export files and folders for further analysis are all included in the user-friendly FTK Imager. It is crucial to the process of digital forensics because law enforcement, cybersecurity professionals, and forensic analysts frequently use it to collect and store digital evidence for court cases.

3.13.1 Work Process:

► **Case Creation and Setup**:

- Investigators create a new case in FTK, defining parameters such as case number, evidence number, and examiner details.
- FTK Imager is often used to acquire forensic images before analysis in FTK. It can be launched from a forensic workstation or run from a USB drive on a live system.

► Data Acquisition:

- **Disk Imaging:** FTK Imager makes exact copies of storage devices, including hard drives, SSDs, USB drives, or memory cards, without changing the original evidence. Supported formats are DD/raw, E01 (EnCase), and AFF (Advanced Forensic Format).
- **Source Selection:** Users select the source (physical drive, logical drive, or existing image file) and specify a destination for the image
- **Hash Verification:** FTK Imager calculates MD5, SHA-1, or SHA-256 hash values to verify the integrity of the image against the original source
- **Live RAM Acquirement:** FTK Imager captures volatile memory data, including running processes, network connections, and encryption keys, which is critical for analyzing live systems.
- **Previewing Data:** Before imaging, FTK Imager allows investigators to preview files, folders, or deleted data to determine what to include in the image.

► Data Processing and Indexing:

- FTK uses a centralized database to pre-process and index information, enabling rapid search and analysis.
- Data is categorized, and artifacts like emails, documents, and multimedia are parsed automatically.
- FTK's database-driven approach ensures stability, preventing crashes common in memory-based tools

► Analysis:

- **File examination:** FTK Imager allows investigators to explore forensic images, view file structures, extract metadata, and recover deleted files through data mining
- **Comprehensive Analysis:** FTK provides advanced tools for analyzing emails (parsing for keywords, headers, or IP addresses), decrypting files, cracking passwords, and visualizing data relationships through timelines or cluster graphs.

- **Keyword Search and Filtering:** FTK supports regular expression search and advanced filtering to quickly identify specific evidence.
- **Mobile and Database Forensics:** FTK can ingest mobile extractions and perform database analysis, extracting data from apps like WhatsApp or Telegram.
- **Visualization:** FTK offers visual tools such as timelines, pie charts, and cluster graphs to highlight data relationships.

► Reporting and Collaboration:

- FTK produces customizable reports summarizing results, which can be exported for court or stakeholder review.
- FTK Web Viewer allows real-time access to case files for associates, supporting multi-case searches.
- FTK Enterprise and FTK Central enable remote endpoint collection and collaborative analysis in large-scale investigations.

► Documentation and Chain of Custody:

- FTK Imager logs all actions, including hash reports, to maintain a defensible chain of custody.
- FTK ensures that all processes adhere to court-recognized, legal standards for the admissibility of evidence

3.13.2 Key Features of FTK Imager:

► FTK Imager:

- **Forensic Imaging:** Creates bit-for-bit copies of storage media in formats such as E01, DD/raw, and AFF, preserving all data, including deleted files and unallocated space.
- **Hash calculation and verification:** Supports MD5, SHA-1, and SHA-256 to ensure data integrity.
- **Live RAM Analysis:** Captures volatile memory for insight into running processes, network connections, and encryption keys.
- **Data Carving:** Recovers deleted or fragmented files from forensic images

- **File Analysis:** Allows to preview and extract files, metadata and hidden or deleted content without changing the original evidence
- **Portability:** Can be run from a USB drive for live system imaging.
- **User-friendly interface:** accessible to both novice and experienced investigators
- **Free Availability:** FTK Imager is free to download and use indefinitely.

► FTK Forensic Toolkit:

- **Advanced Data Recovery:** Recovers data from encrypted or deleted files with precise algorithms
- **Comprehensive Analytics:** Handles large datasets, multiple file types, and mobile extractions with tools for email analysis, registry parsing, and database forensics.
- **Decryption and Password Cracking:** Decrypts files and recovers passwords for over 100 applications.
- **Distributed processing:** Uses multi-core CPU and four processing workers for fast data processing.
- **Visualization Tools:** Provides timelines, cluster graphs and pie charts for data interpretation.
- **Malware Detection:** Integrates Cerberus for automated malware triage and threat scoring.
- **Explicit Image Identification:** Automatically identifies pornographic images using a trained library of 30,000 images, which assists CSAM investigations.
- **OCR Engine:** Converts images to text with multiple language support, reducing OCR time by up to 30%
- **Integration:** Works seamlessly with third-party tools for mobile extraction and other forensic platforms
- **Scalability:** FTK Enterprise and FTK Central support large-scale, collaborative investigations with remote data collection
- **Extensive file system support:** Analyzes DMG, Ext4, exFAT, VxFS, VHD, YAFFS and more across Windows, macOS, Linux, and Unix.

3.13.3 Limitations of FTK and FTK Imager

► FTK Imager Limitations:

- **Limited analysis functionality:** While excellent for imaging, FTK Imager lacks the advanced analysis functionality of the full FTK suite, such as in-depth email parsing or visualization features. Testers must use FTK or other tools for detailed analysis.
- **Windows installation only:** FTK Imager cannot be installed on Linux or macOS systems, although it can image devices from these operating systems. This limits its deployment in non-Windows environments.
- **Compatibility issues:** May struggle with newer file systems or encryption methods, users should stay updated with the latest version to ensure compatibility
- **Live Imaging Impact:** Performing live imaging, especially RAM acquisition, can impact system performance and requires sufficient resources to avoid disruption.
- **No Mobile Data Extraction:** FTK Imager cannot directly extract data from mobile devices, requiring integration with third-party tools for mobile forensics

► FTK Forensic Toolkit Limitations:

- **High hardware requirements:** FTK's performance, especially with distributed processing, demands powerful hardware, which can be a bottleneck for small organizations.
- **Cost:** Unlike FTK Imager, FTK requires a license after a trial period and pricing details are not publicly disclosed, making it expensive for some users.
- **Learning curve:** Despite its intuitive interface, effective use of FTK's advanced features requires significant training, especially for non-technical users.
- **No native mobile extraction:** FTK relies on third-party tools for mobile data extraction, adding complexity to the workflow.

- **No Timeline View:** FTK does not have a dedicated timeline view, which can hinder chronological analysis of events compared to tools like Magnet AXIOM.
- **Separate Registry Viewer:** Registry analysis requires a separate program (Registry Viewer), which can disrupt workflow compared to integrated solutions.
- **Hashing Vulnerabilities:** Traditional hashes such as MD5 and SHA-1 used by FTK have a theoretical collision risk which could raise suspicions in legal proceedings, although this is rare with modern storage sizes.
- **Slow Startup:** Some users complain that FTK is slow to start up, which can affect the performance of time-sensitive investigations.

3.13.4 **Work process** screenshot:

- **Open FTK imager:**

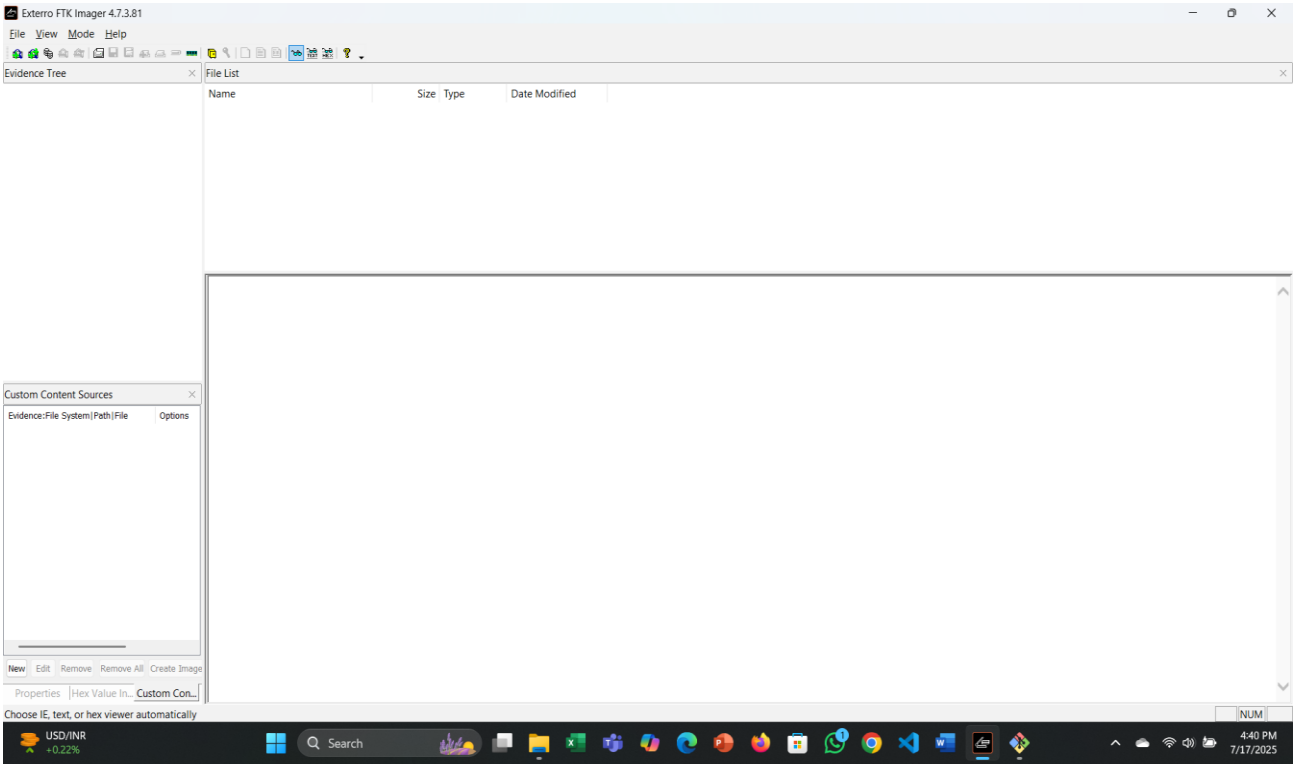


Figure 66

- **Create Disk image**

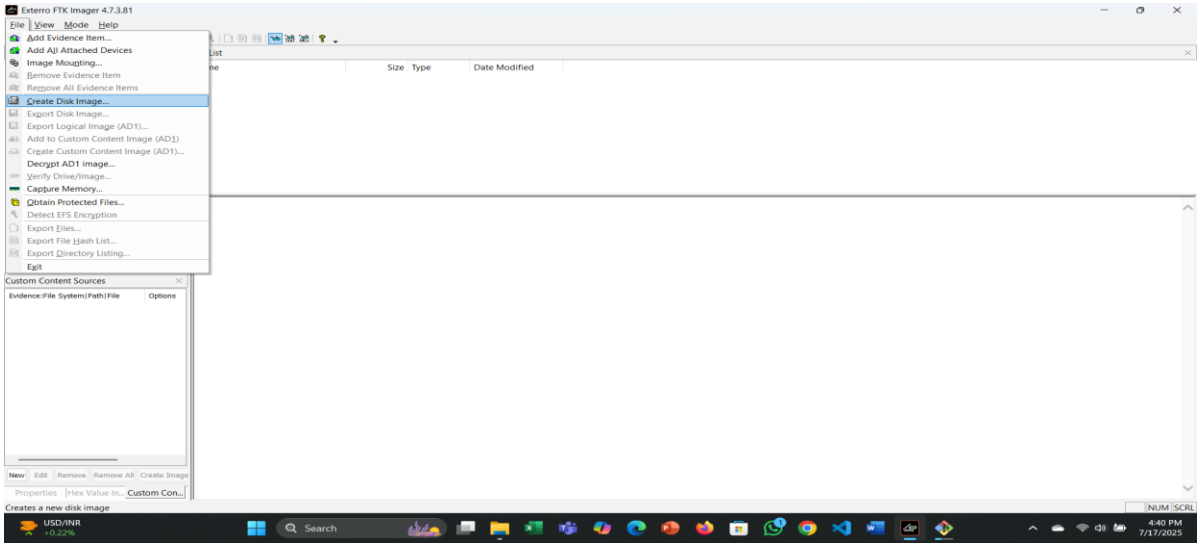


Figure 67

- **Select Source Evidence type**

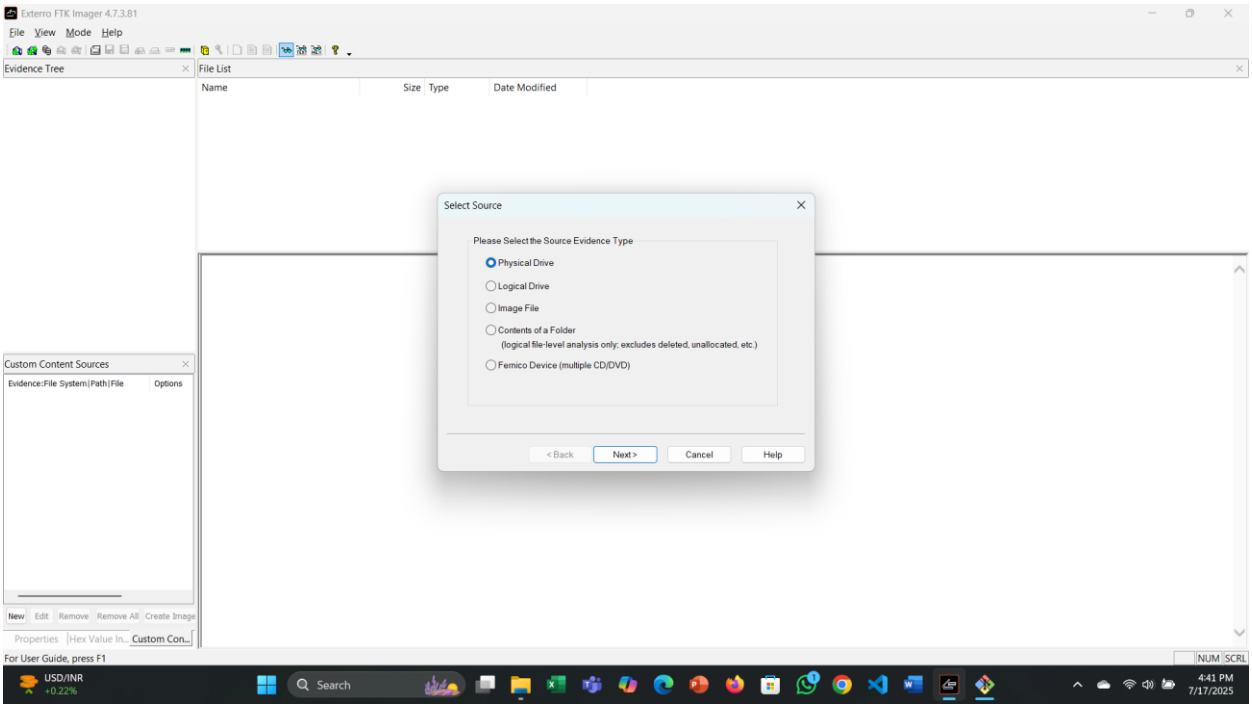


Figure 68

- **Select source of Drive**

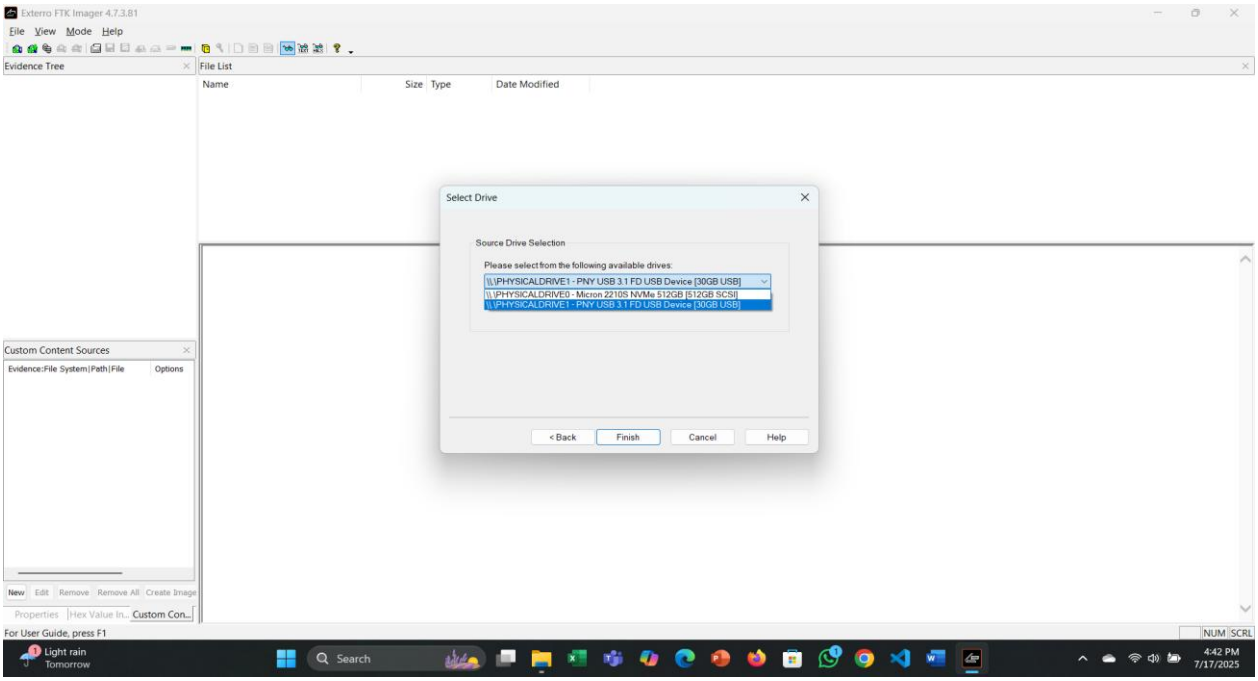


Figure 69

- **Select source of image file**

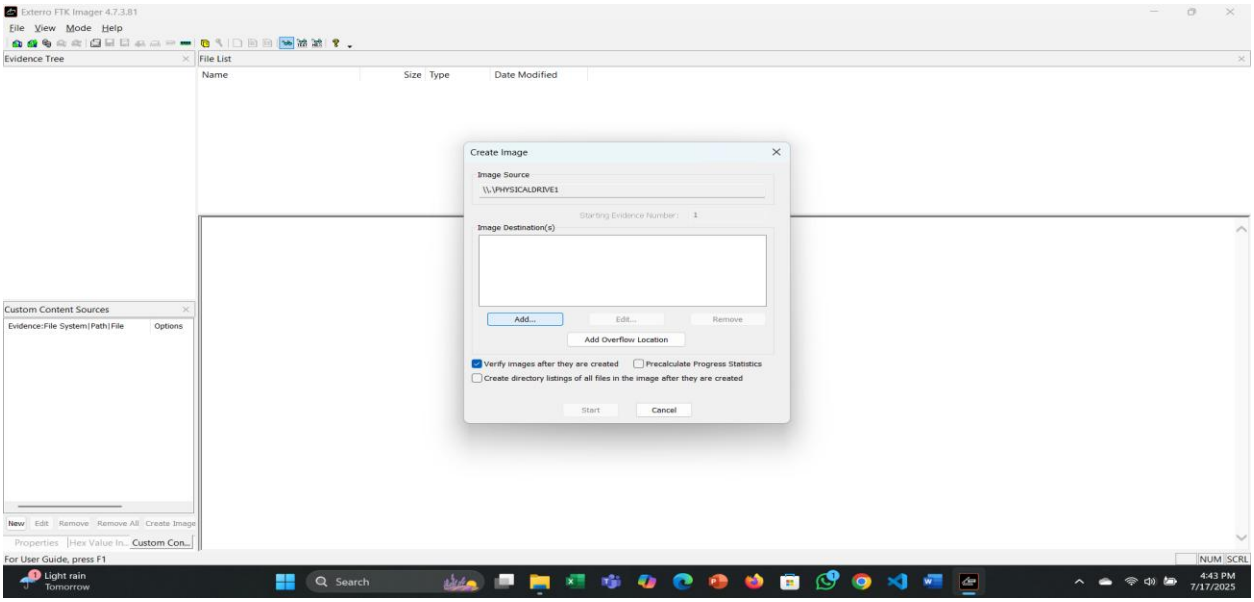


Figure 70

- **Select the Destination Image type:**

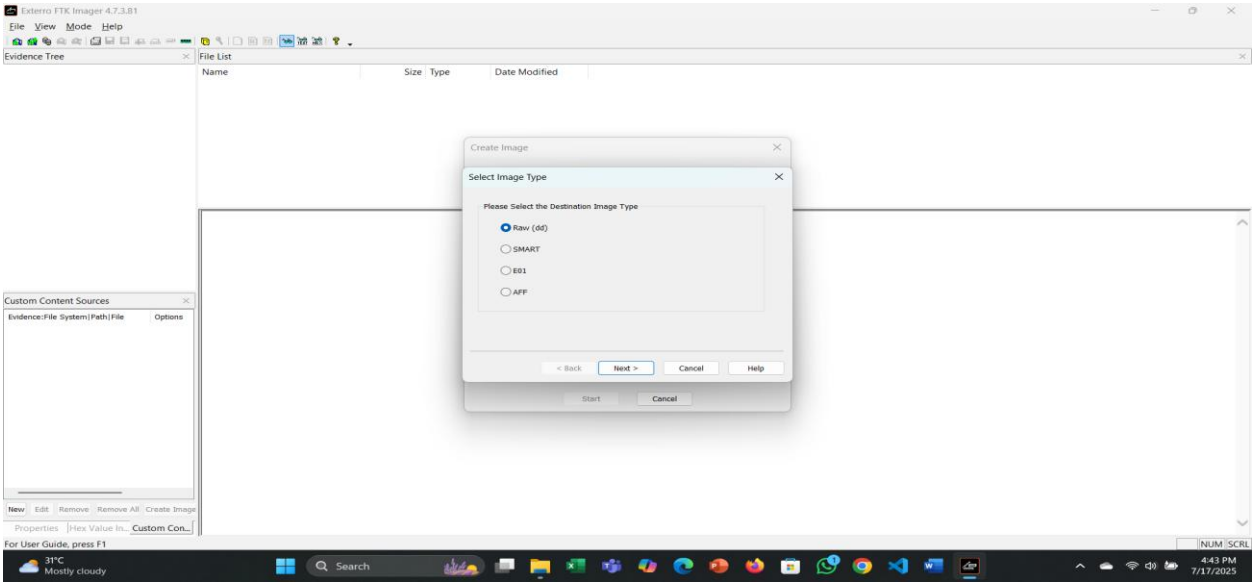


Figure 71

- **Select evidence Item information and examiner name**

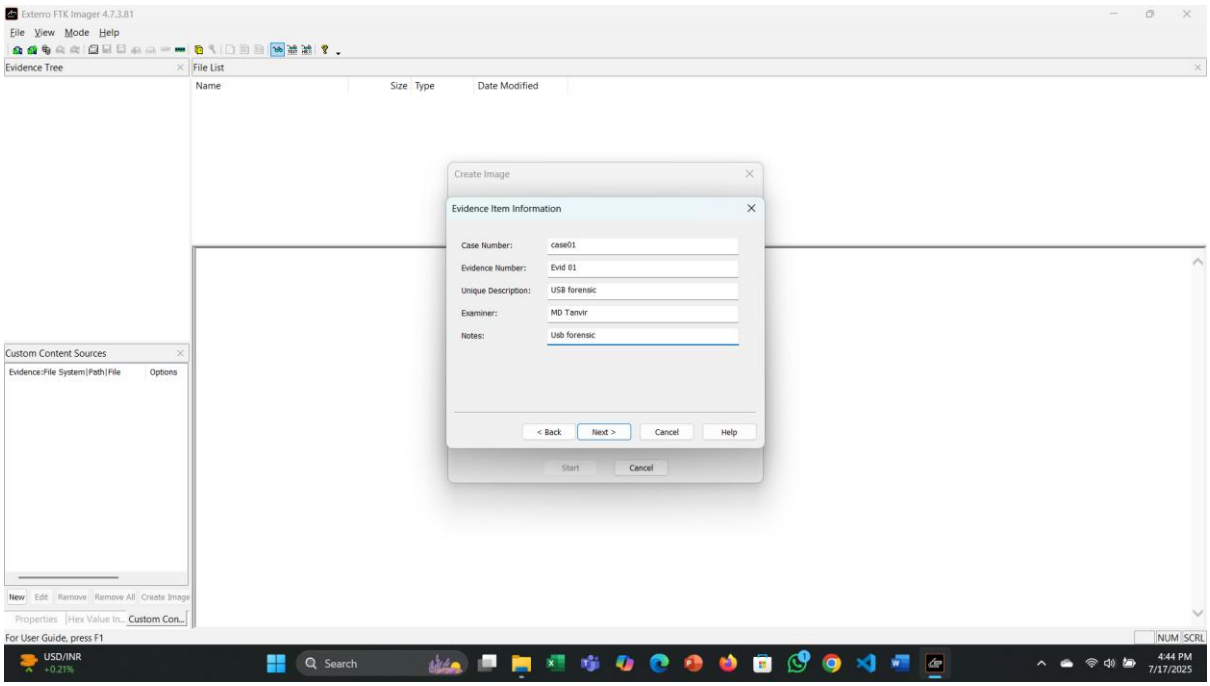


Figure 72

- **Select image Destination and select folder. image Fragmentation size selects.**

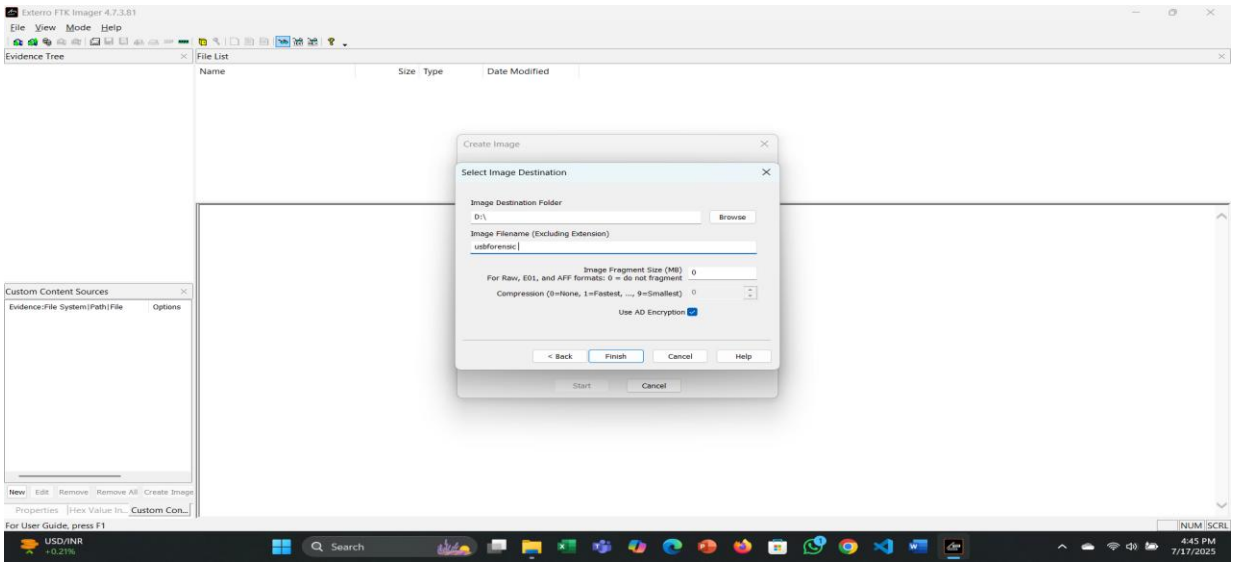


Figure 73

- **Start Creating the Image for evidence disk**

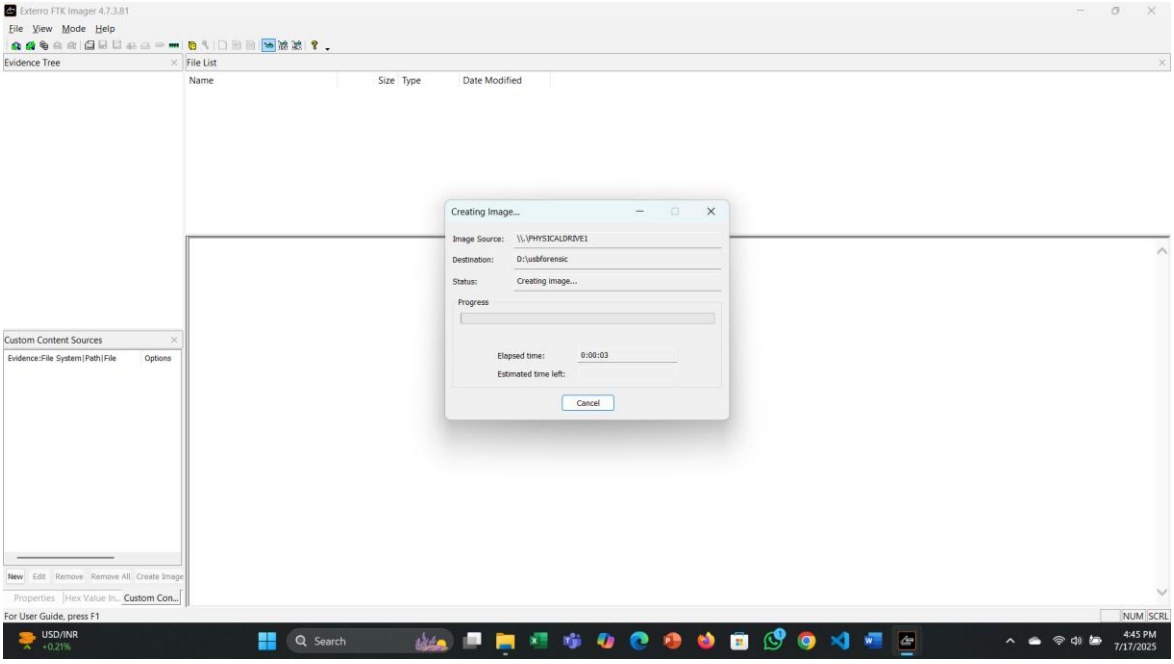


Figure 74

CHAPTER 4: INTERNSHIP SUMMARY

4.1 Overview:

The internship at Backdoor Private Limited, a leading cybersecurity and IT solutions firm in Bangladesh, offered a solid platform to connect theoretical IT knowledge with real-world experience as a Technical Executive. Under the guidance of Tahsina Sadia Meem, a Forensic Analyst, and Shuvo Sarkar, a SOC Analyst, I participated in hands-on projects that improved my skills in cybersecurity and digital forensics. The main goal was to use IT principles in practical situations, like system updates, defect tracking, and network security tasks, while also building teamwork, professional communication, and problem-solving skills. The internship required the use of various tools, including Nmap, Whois, SpiderFoot, Oxygen Forensic, Autopsy, FTK Imager, Nessus, OpenVAS, Zenmap, Fierce, Dnsenum, and DnsMap, for network reconnaissance, vulnerability scanning, and digital forensics. These tasks deepened my knowledge of host discovery, port scanning, data recovery, and threat detection, equipping me to face the challenges of the IT job market with practical skills and confidence. Backdoor Private Limited's emphasis on proactive threat detection and client-focused solutions, along with its team-oriented work environment, offered a strong foundation for my growth in the cybersecurity field.

4.2 Achievement:

During my internship at Backdoor Private Limited as a Technical Executive, I achieved significant milestones that enhanced my cybersecurity and IT expertise. I successfully applied theoretical knowledge to practical scenarios, mastering the use of tools like Nmap, Whois, SpiderFoot, Oxygen Forensic, Autopsy, FTK Imager, Nessus, OpenVAS, Zenmap, Fierce, Dnsenum, and DnsMap for tasks such as host discovery, port scanning, vulnerability assessment, and digital forensics. I contributed to live projects by implementing system updates, maintaining local computers, and tracking defects, which improved system efficiency and security. My hands-on experience with network reconnaissance and forensic analysis, including data recovery and evidence management, strengthened my technical proficiency. Additionally, as demonstrated by my cooperation with industry experts and adherence to corporate policies, I developed crucial soft skills like effective teamwork, professional email communication, and problem-solving under real-world constraints. These accomplishments, along with the advice of supervisors Tahsina Sadia Meem and Shuvo Sarkar, equipped me to confidently and competently handle the challenges of the modern IT job market.

4.3 Limitations of Internship:

The internship at Backdoor Private Limited offered useful hands-on experience in cybersecurity and digital forensics, but it faced several challenges that affected how much I could learn. The law on penetration testing was one of the main problems. I missed out on crucial offensive security skills because of this restriction, which prevented me from using programmes like Nmap, Nessus, or OpenVAS to simulate actual cyberattacks. I also couldn't run essential scripts, such as advanced Nmap scripts or custom modules of SpiderFoot. This likely happened because of company policies aimed at preventing network disruptions. As a result, I couldn't explore automated vulnerability detection and advanced remediation strategies. Relying on certain tools created additional problems. For example, Autopsy was slow with large datasets, FTK Imager lacked mobile data extraction, and OpenVAS had a complicated setup that could be made worse by limited hardware resources. The internship mainly focused on specific tasks like system updates and error tracking. This, along with the steep learning curve for tools like Nessus and Oxygen Forensics, limited my chances to engage in broader areas of IT, such as running independent projects or working with cloud security. These challenges

together reduced the opportunities for hands-on cybersecurity training, but the basic skills I developed in network scanning and forensics are still valuable.

4.4 Future Of the Internship:

My future career in cybersecurity and IT will be significantly enhanced by my internship as a Technical Executive at Backdoor Private Limited. By gaining hands-on experience with industry-standard tools, I have gained practical skills in network reconnaissance, digital forensics, and vulnerability assessment, which have established me as a competitive candidate for roles such as cybersecurity analyst, penetration tester, or forensic investigator. The ability to apply theoretical IT knowledge to real-world tasks such as system updates, error tracking, and data recovery has strengthened my problem-solving abilities and understanding of professional workflows, preparing me to tackle complex challenges in the IT job market. Additionally, the internship has enhanced essential soft skills, including teamwork, professional communication, and adherence to corporate policies, which are crucial for collaboration in a high-level environment.

4.5 Conclusion Of This Internship:

Finally, my internship at Backdoor Pvt Ltd as a technical executive was a life-changing opportunity that helped me close the gap between my theoretical understanding of IT and my real-world experience in digital forensics and cybersecurity. I improved my technical skills and prepared for a cybersecurity role by gaining practical experience with tools such as Nmap, Whois, SpiderFoot, Oxygen Forensic, Autopsy, FTK Imager, Nessus, OpenVAS, Zenmap, Fierce, Dnsenum, and DnsMap. These tools helped me in network reconnaissance, vulnerability assessment, and data recovery. The internship promoted crucial soft skills like teamwork, professional communication, and problem-solving under real-world constraints, despite restrictions like a ban on penetration testing and limitations on running critical scripts that prevented exposure to aggressive security and advanced automation. Working on real projects at a top cybersecurity company and being in a supportive environment under the direction of supervisors Tahsina Sadia Meem and Shuvo Sarkar formed a solid basis for future professional development. With the confidence and abilities I gained from these experiences, I was able to pursue advanced certifications and make a valuable contribution to the expanding field of digital security.

Key Word:
cybersecurity, vulnerability assessment, penetration testing, VAPT, digital forensics, Security Operations Center, SOC, network reconnaissance, threat detection, incident response, Nmap, Whois, SpiderFoot, Oxygen Forensic, Autopsy, FTK Imager, Nessus, OpenVAS, Zenmap, Fierce, Dnsenum, DnsMap, host discovery, port scanning, data recovery, forensic analysis, SIEM platforms, network security, system updates, defect tracking, malware detection, evidence management, data acquisition, keyword search, timeline analysis, hash verification, subdomain enumeration, DNS queries, proactive security, teamwork, professional communication, problem-solving, industry-standard tools, compliance, threat landscape, data visualization, reporting, file system analysis, live RAM capture, client-focused solutions, scan techniques, TCP SYN scan, TCP connect scan, UDP scan, script scan, port exclusion, fast scan, sequential scanning, top ports, port ratio, DNS resolution, traceroute, ICMP probes, Lua scripts, firewall evasion, domain lookup, IP lookup, ASN lookup, OSINT automation, vulnerability scanning, Greenbone Security Assistant, Network Vulnerability Tests, NVTs, forensic imaging, data carving, hash algorithms, MD5, SHA-1, SHA-256, mobile forensics, cloud extraction, email analysis, web artifacts, Exif data, file type identification, deleted file recovery, chain of custody, report customization, Kali Linux, network mapping, penetration testing frameworks, cyber threats, soft skills, system resources, data integrity, forensic workstation, client organizations, real-world projects, and career preparation

CHAPTER 5: REFERENCE

- **Nmap Tools:** https://www.kali.org/tools/nmap/
- **Whois :** https://www.kali.org/tools/whois/
- **Fierce:** https://www.kali.org/tools/fierce/
- **Dnsenum :** https://www.kali.org/tools/dnsenum/
- **DnsMap:** https://www.kali.org/tools/dnsmap/
- **Spiderfoot:** https://www.kali.org/tools/spiderfoot/
- **Nessus :** https://www.tenable.com/ , https://localhost:11127
- **Openvas:** https://www.openvas.org/index.html , https://localhost:9392
- **Zenmap:** https://nmap.org/zenmap/
- **FTK imager:** https://www.exterro.com/digital-forensics-software/ftk-imager
- **Autopsy:** https://www.autopsy.com/
- **Oxygen forensic**: https://digitalintelligence.com/store/products/oxygen-forensic-detective

CHAPTER 6: APPOINTMENT LATER

BACKDOOR
IN SEARCH OF ROOTS

Flat- 9(B), House-30, Road-42,
Gulshan-02, Dhaka 1212, Bangladesh.
www.backdoor.com.bd
info@backdoor.com.bd
+880 2 4881216-9

Ref: BPL/APML/001/25

Date: 25.02.2025

MD.Tanbir
Address: Daffodil International University
Phone: 01601848191
E-mail: tanbir35-728@diu.edu.bd

Subject: **Internship (Cyber Security) in Backdoor Private Ltd.**

Dear Tanbir,

Backdoor Private Ltd. is pleased to appoint you as an intern (Technology Department). Your internship shall be for a period of three (03) months effective from 6th April, 2025 under the following terms and conditions:

1. You will report to respective Tahsina Sadia Meem, Technical Executive of Backdoor Private Ltd. and will work under her guidance and supervision.
2. Your working hours will be 10:00 AM to 6:00 PM from Saturday to Thursday. You may need to work extensive office hours if required.
3. You will conduct yourself in a manner that is not prejudicial to the company's interest. You have to follow all the standard practices of the company according to its policies.
4. During the period, you might be allowed a maximum of 3 (three) days leave for emergency purposes, subject to the approval of your team leader.
5. You will be assigned on the departments as per the internship plan, and upon completion of the internship period, you are required to submit a report on your completed assignment to the technical department or Technical Executive Tahsina Sadia Meem.
6. You will be given a remuneration of BDT-5000/- only per month.

We look forward to working with you in the coming days.

Thank you,

General Manager (GM)
Backdoor Private Ltd.

I, MD.Tanbir, confirm acceptance of your offer of employment based on the terms and conditions contained here in above which have read and understood.

Signed: tanbir Date: 06-04-2025

Head Office: 17/B/3, Monipuripara (2nd Floor), Shangshad Avenue, Dhaka-1215, Bangladesh

CHAPTER 7: ACHIVEMENT

CERTIFICATE

OF TRAINER

MD Tanbir

Your expert guidance and active involvement as a trainer in the **"হাতে-কলমে ডিজিটাল ফরেনসিক প্রশিক্ষণ"** program, organised by the Cyber Security Centre of Daffodil International University in collaboration with Savar and Ashulia Thana police under the Police Headquarters, is deeply appreciated. Wishing you ongoing success in your endeavours.

Rubaiyat Islam

Dr.Rubaiyat islam
Director
Cyber Security Centre, DIU

Dr. Imran Mahmud
Professor & Head
Department of Software Engineering, DIU

CHAPTER 8: Plagiarism Report

212-35-728

ORIGINALITY REPORT

7%	6%	1%	4%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Daffodil International University Student Paper	2%
2	idoc.pub Internet Source	1%
3	aristininja.com Internet Source	1%
4	Submitted to Southern New Hampshire University - Continuing Education Student Paper	1%
5	www.coursehero.com Internet Source	<1%
6	Submitted to Colorado Technical University Online Student Paper	<1%
7	www.diskinternals.com Internet Source	<1%
8	Submitted to Capella University Student Paper	<1%
	tecadmin.net	

CHAPTER 8: Account Clearance