FACULTY OF ENGINEERING & TECHNOLOGY (Co-Ed), SHARNBASVA UNIVERSITY KALABURAGI

ABOUT US

We believe and we Provide "Smart Security for Smart People" We are a team of enthusiastic people aspiring to be India's best cyber security service providers.

We are a dedicated cybersecurity company led by Certified Ethical Hackers and skilled Penetration Testers, specializing in VAPT, Network Audits, and global compliance (ISO, PCI DSS, GDPR, NIST). Our mission is to deliver tailored, proactive security solutions that empower businesses to operate safely in today's evolving threat landscape.

Beyond protection, we focus on awareness offering cybersecurity workshops, and training to foster a strong security culture. With a deep commitment to privacy, integrity, and personalized service, we protect what matters most your trust and your data.

SERVICES

- ✓ VAPT (Vulnerability Assessment & Penetration Testing),
- ✓ Network Infrastructure Audit
- ✓ IS/IT/EDP Audits for Banks
- ✓ IRDAI Audits
- ✓ CSCRF Audits
- ✓ Compliance Audit
    - ISO Audits – ISO 27001, ISO 9001, ISO 42001, ISO 2100, etc,.
    - PCI DSS
    - GDPR
    - NIST Framework
- ✓ Cybersecurity Workshops, Trainings, Internship and Awareness programs to the public and corporates.
- ✓ Trained around 17,000 students/ professionals

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

FACULTY OF ENGINEERING & TECHNOLOGY (Co-Ed),
SHARNBASVA UNIVERSITY KALABURAGI

LAB EXPERIMENTS LIST

01. Perform OSINT and footprinting on a target domain (whois, DNS, Google dorks) and produce an asset list.

02. Scan lab hosts for open ports/services (Nmap) and produce a vulnerability-priority sheet with remediation suggestions.

03. Demonstration of password vulnerability Tools: Hashcat, John the Ripper

04. Master the Fundamentals of Digital Forensics and Evidence Collection using Autopsy

05. Exploit SQL injection in an intentionally vulnerable web app (DVWA/OWASP Juice Shop) and document PoC and fixes.

06. Capture network traffic (Wireshark) for given scenarios, identify suspicious flows, and suggest detection rules.

07. Embed/extract hidden data in files (image/audio/doc) and evaluate detectability and forensic hints.

08. Analyze a provided memory dump using Volatility to identify processes, network connections, and possible malicious artifacts.

09. Create a forensic image (FTK Imager/dd), verify integrity (hashes), and recover deleted files via carving.

10 . Apply the IR lifecycle to a simulated incident (ransomware or data exfiltration), produce timeline, containment steps and incident report.

Experiment-1

OSINT and Footprinting on a target domain

Objective

To understand and perform OSINT and footprinting techniques on a target domain using publicly available tools and resources in order to identify domain details, IP addresses, subdomains, DNS records, email information, technologies used, and potential security exposures—without interacting directly with the target system.

Theory Overview

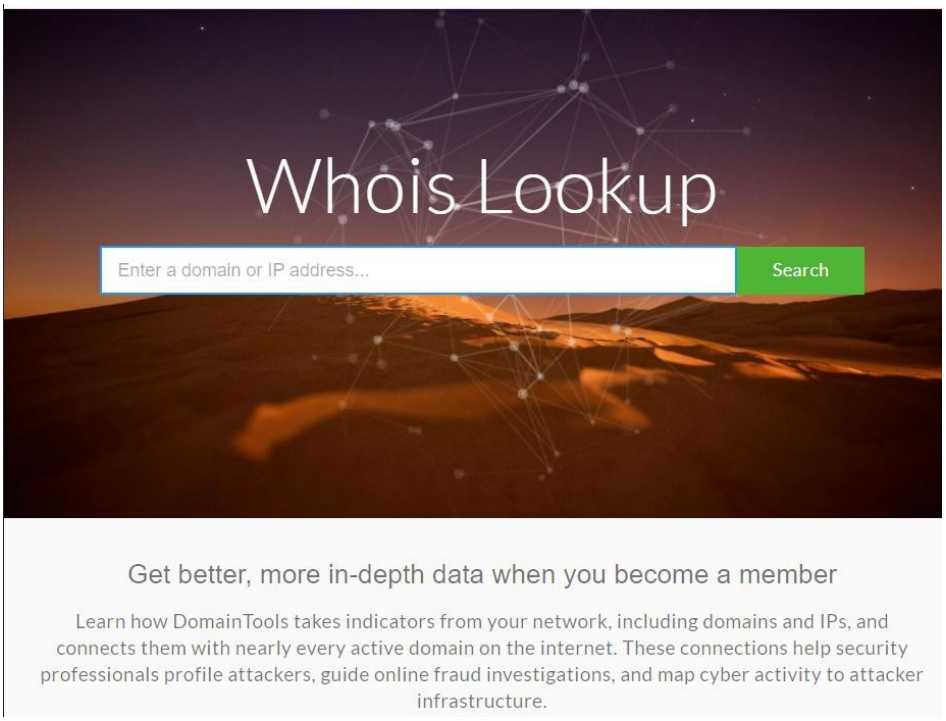
OSINT (Open-Source Intelligence) is the process of collecting information from publicly available resources.

Footprinting is the first phase of ethical hacking, where attackers or security professionals gather preliminary information about a target.

Whois Domain tool

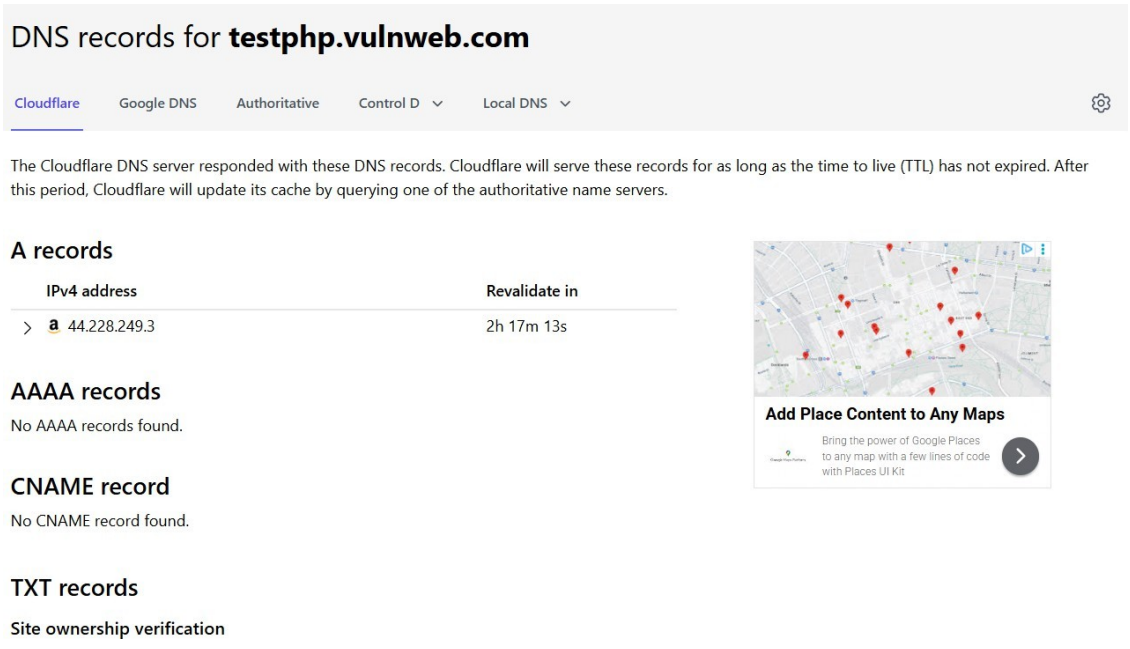
- Research domain ownership with Whois Lookup: Get ownership info, IP address history, rank, traffic, SEO & more.

FACULTY OF ENGINEERING & TECHNOLOGY (Co-Ed), SHARNBASVA UNIVERSITY KALABURAGI



DNS LOOKUP TOOL

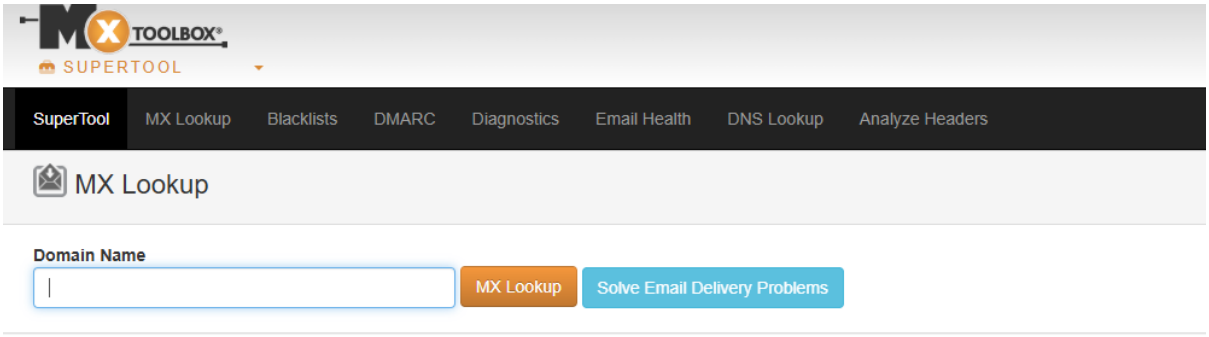
- A DNS Footprinting Tool is used to collect detailed information about a target domain using its DNS (Domain Name System) data.
- It helps ethical hackers or security analysts understand how a domain and its network are structured.



DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

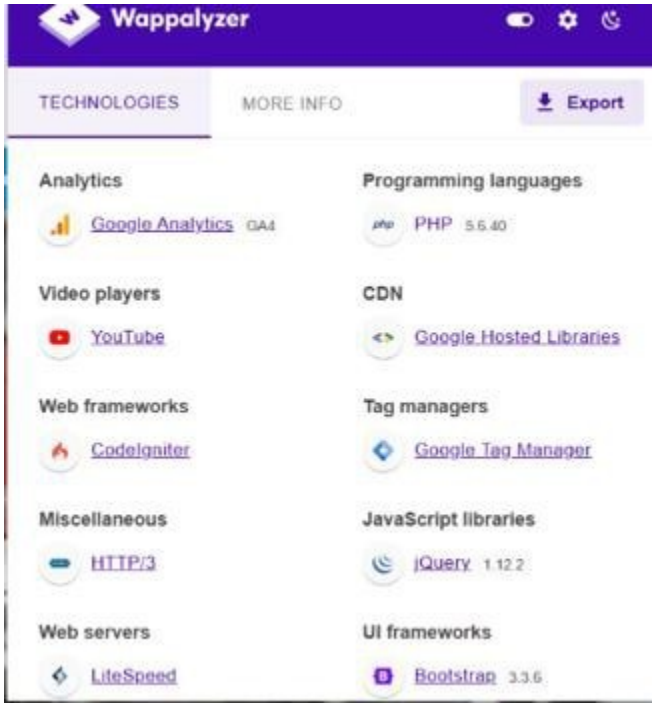
MX TOOLBOX

- MX Toolbox is a free online tool used to check and analyze DNS (Domain Name System) and email (mail server) settings.
- It helps you look up, test, and troubleshoot your domain's mail, DNS, and network records.



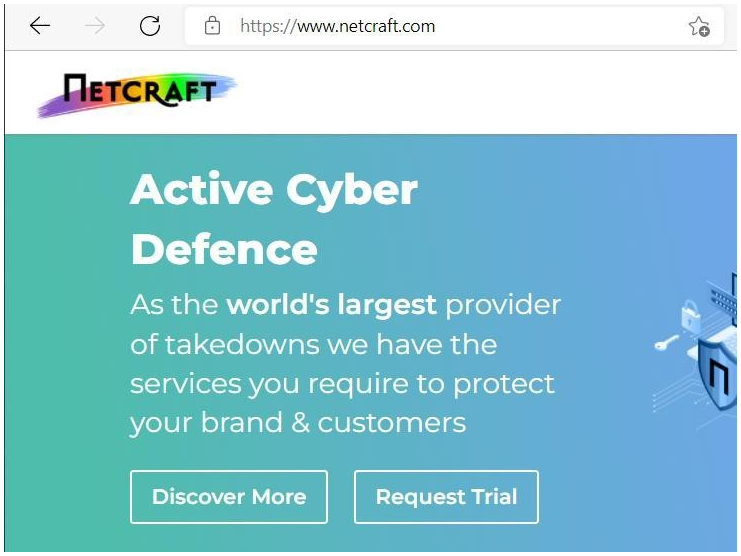
Wappalyzer

- Wappalyzer is a tool that identifies the technologies used by a website.
- It tells you what software, programming languages, frameworks, and tools a website is built with.



Netcraft

- Use our family of Netcraft extensions to ensure you don't get tricked by criminals. It's backed by our malicious site feeds that protect billions of people around the world from phishing, malware and other cybercrime activities.



Experiment 2:

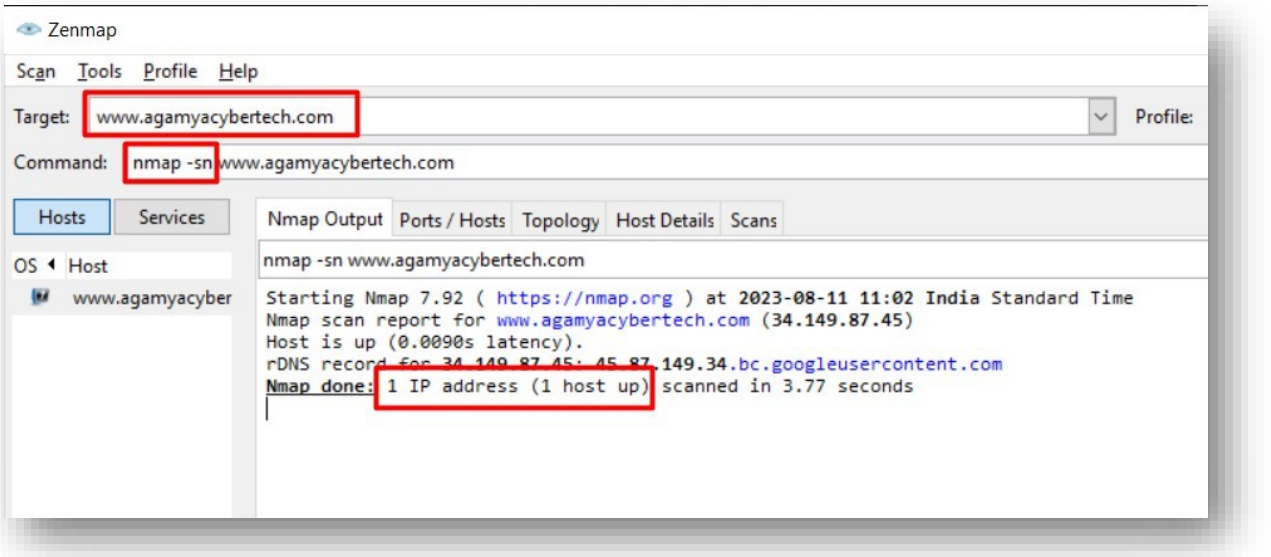
Scan lab hosts for open ports/services (Nmap) and produces a vulnerability-priority sheet with remediation suggestions.

Nmap (Network Mapper) is an open-source tool used for network discovery and security auditing. to scan networks and identify devices, services, open ports, and other network characteristics.

Basic Nmap Commands:

Simple Ping Scan (-sn)

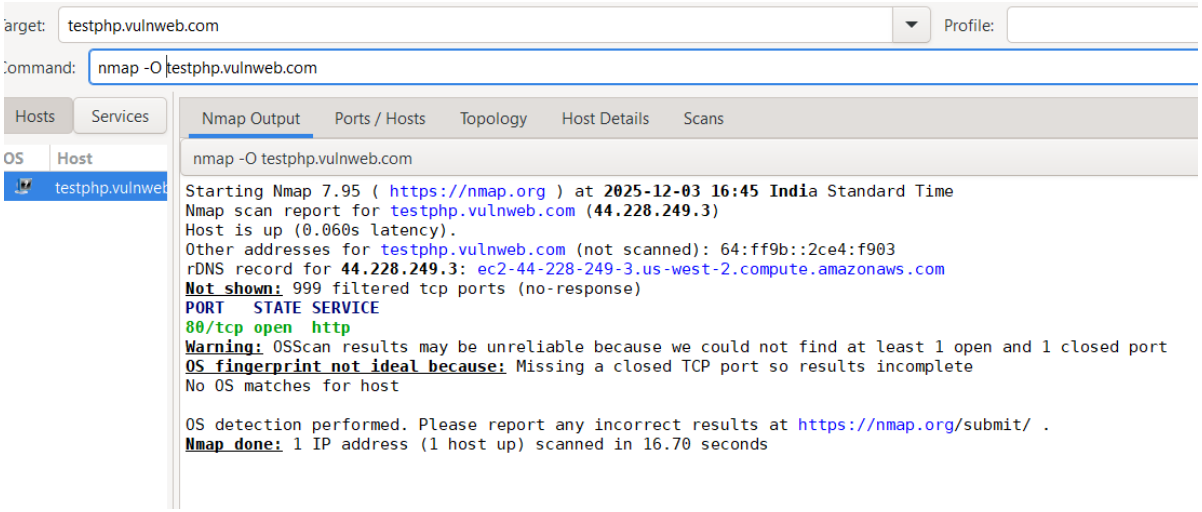
To check which hosts are up in a network range. It sends ICMP (Internet Control Message Protocol) Echo Request packets (essentially "pings") to the target IPs to check whether they respond, without scanning the ports. This type of scan is commonly used to detect which devices are currently active on a network.



OS Detection(-O)

To detect the operating system of a target.

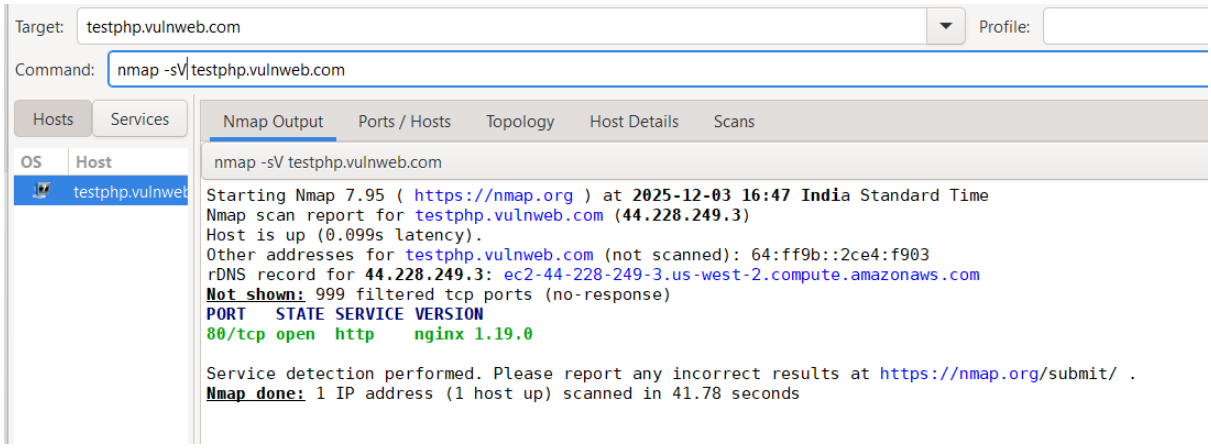
Nmap sends specially crafted packets to the target and analyzes how the system responds to these packets. Each operating system has a unique way of handling network requests, and these differences are known as "fingerprints." By matching the responses with known OS signatures, Nmap can identify the target's OS.



Service Version Detection(-sV):

To detect the versions of services running on open ports.

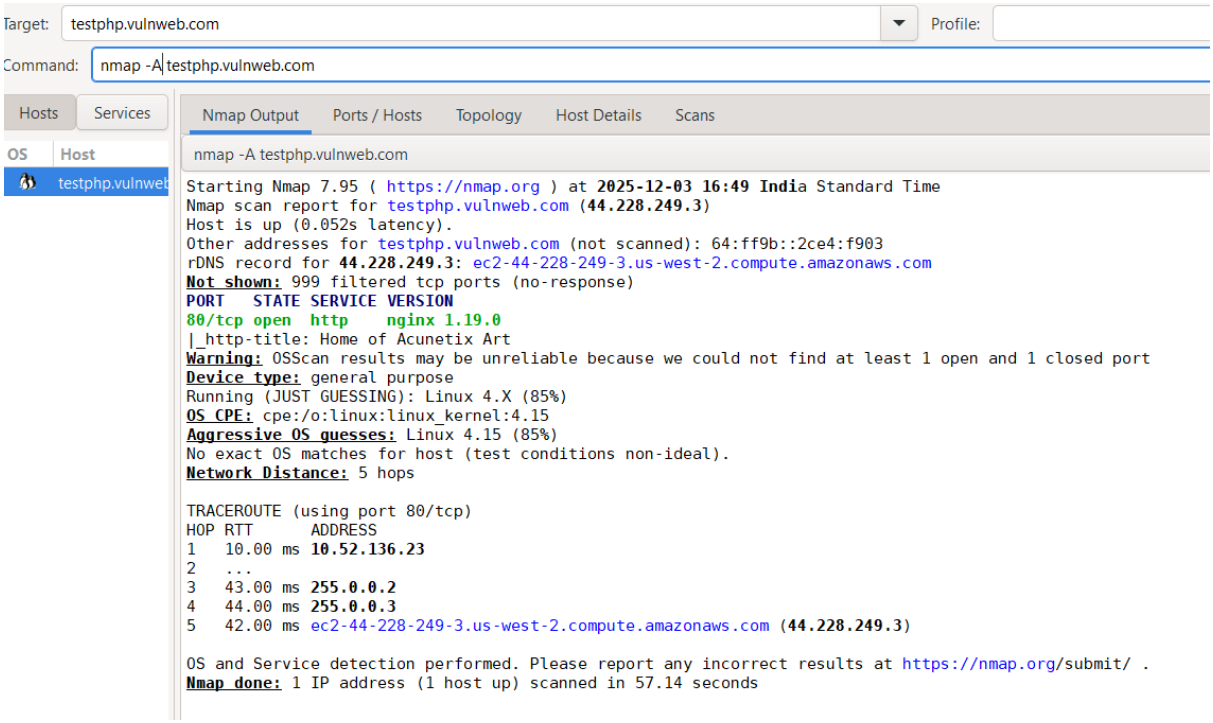
By knowing the specific version of a service, you can identify potential vulnerabilities associated with that version.



Aggressive Scan(-A):

This includes host discovery, port scanning, version detection, OS detection, and script scanning.

Scan in Nmap is a scan type that combines multiple useful scanning techniques togather a comprehensive set of information about a target host. It uses a variety of probes and techniques to provide insights into the target's open ports, services, operating system, and potential vulnerabilities.

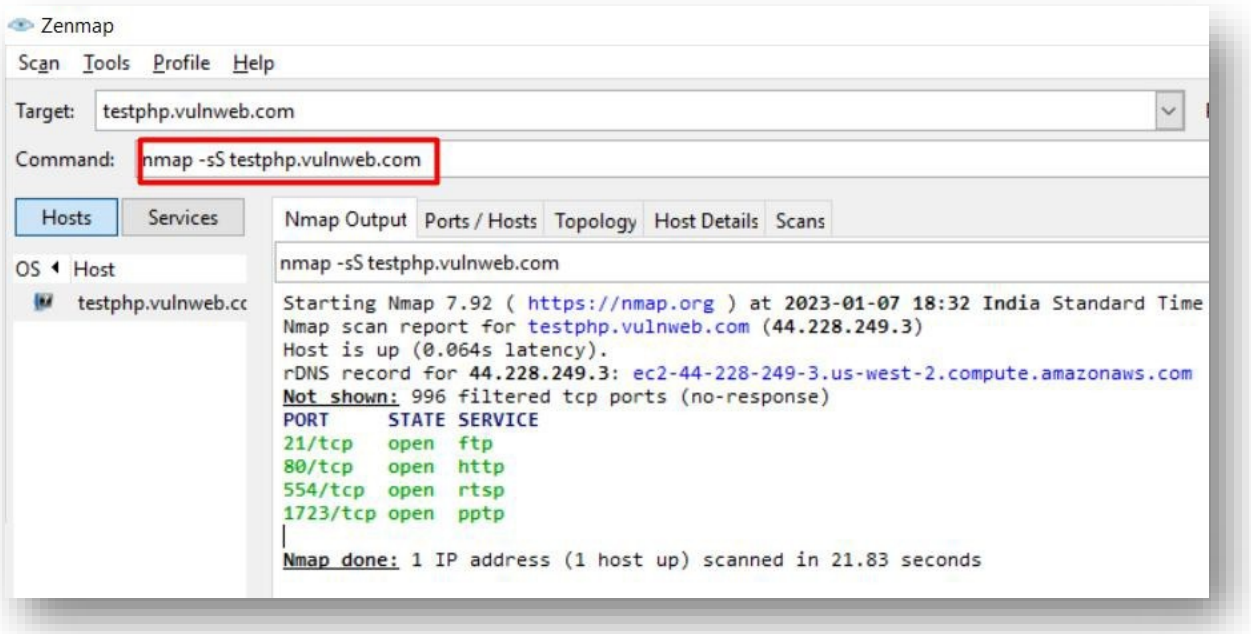


SYN Scan(-sS):

An SYN Scan (-sS) in Nmap is one of the most popular and commonly used port scanning techniques. It is often referred to as a half-open scan because it only sends a SYN packet to the target (which is the first step of the TCP handshake) and then waits for a response. The connection is never fully established, which makes this scan stealthy and fast.

- SYN Packet Sent: Nmap sends a SYN packet (connection request) to the target port.
- Response from Target:
  - SYN-ACK: If the port is open, the target responds with a SYN-ACK packet, indicating that it is willing to establish a connection.
  - RST (Reset): If the port is closed, the target responds with an RST packet, indicating the connection is refused.

No Final ACK: Nmap does not send the final ACK to complete the handshake. Instead, it simply waits for the response. This is why it is called a "half-open" scan — because the full handshake is never completed.

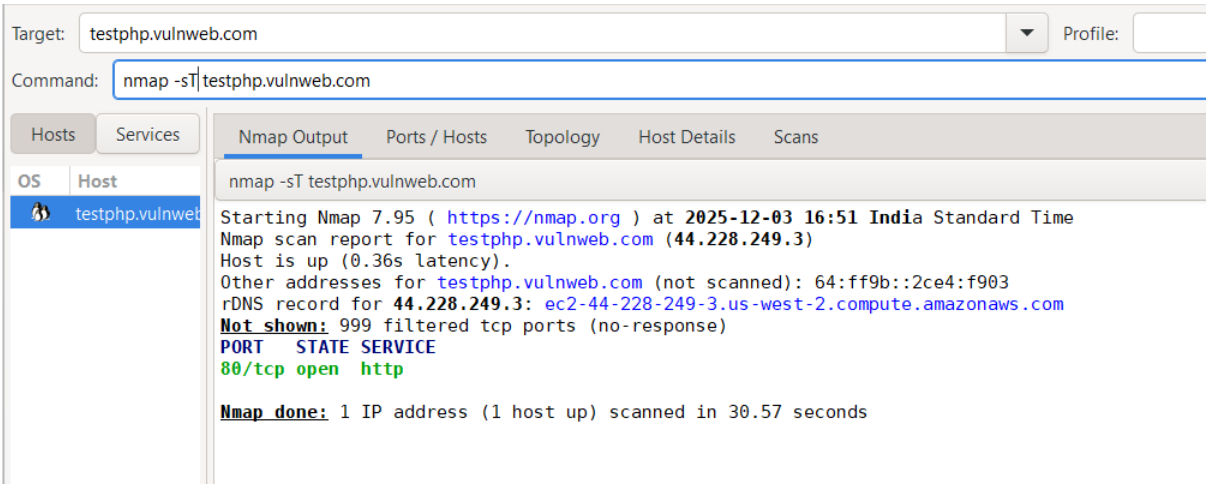


TCP Connect Scan(-sT):

A TCP Connect Scan (-sT) is a basic port scanning technique in Nmap where Nmap attempts to establish a full TCP connection with the target system to determine whether a port is open or closed. Unlike the SYN Scan (-sS), which only sends a SYN packet and does not complete the handshake, the TCP Connect Scan completes the full TCP handshake, making it more detectable but simpler to execute.

How TCP Connect Scan Works:

1. Send SYN Packet: Nmap sends a SYN (synchronize) packet to the target port to initiate the TCP handshake.
2. Receive SYN-ACK: If the port is open, the target system responds with a SYN-ACK packet (indicating the port is open and willing to accept a connection).
3. Complete the Handshake: Since the TCP Connect scan is not a half-open scan, Nmap completes the full handshake by sending an ACK packet to the target. The connection is established and immediately closed after the response.
4. Receive RST (Reset): If the port is closed, the target responds with an RST (reset) packet to indicate that no connection can be made.

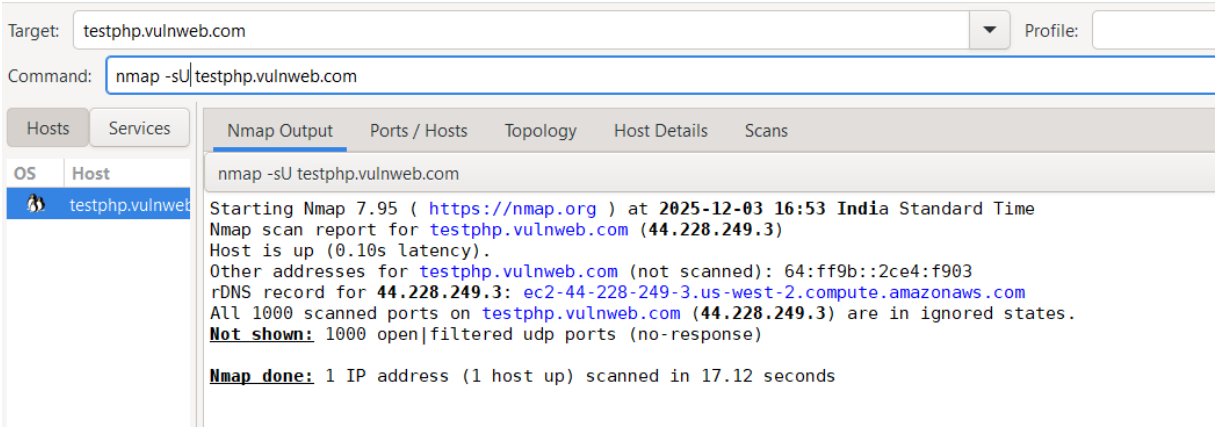


UDP Scan(-sU)

An UDP Scan (-sU) in Nmap is used to detect open UDP ports on a target system. Unlike the more common TCP port scanning techniques (such as SYN or Connect scans), which establish a connection via the TCP protocol, UDP scanning involves probing ports using the User Datagram Protocol (UDP), which is connectionless and does not rely on the same handshake process that TCP does.

How UDP Scan Works:

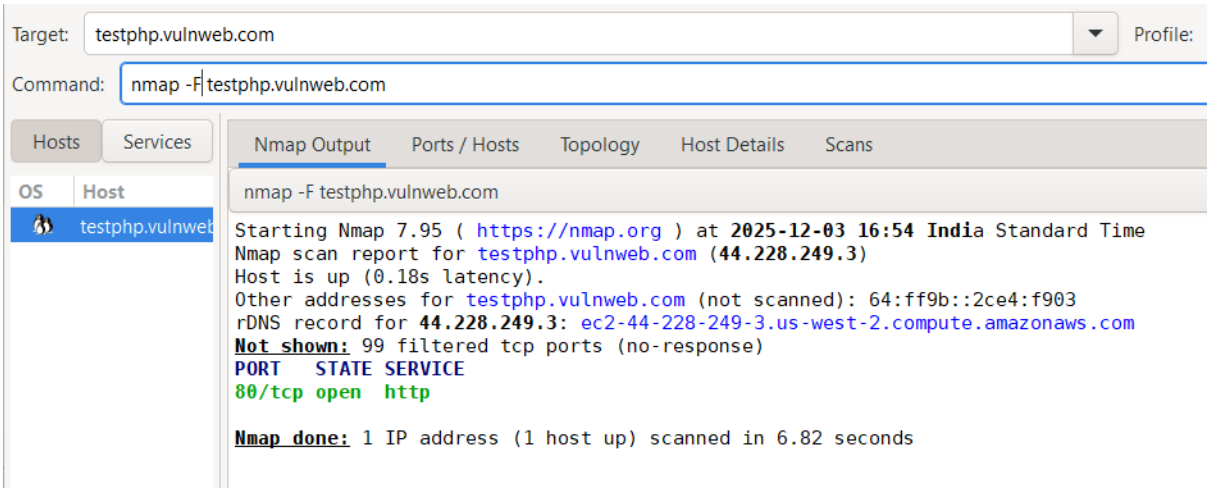
1. Send UDP Packet: Nmap sends a UDP packet to the target port. Because UDP is connectionless, no connection is established, and Nmap simply sends data to the port.
2. Receive Response:
    - No Response: If the port is open or filtered, there may be no response (since UDP does not confirm receipt or status). In some cases, firewalls or filters may block the probe, leading to no response.
    - ICMP Port Unreachable: If the port is closed, the target typically responds with an ICMP Port Unreachable message.
3. Timing and Delays: UDP scans can be slower than TCP scans because of the lack of immediate response. UDP packets may also be dropped by intermediate firewalls or network devices, which can cause a delay in results.



Fast Scan(-F)

The -F option in Nmap is used to enable a Fast Scan. This option tells Nmap to scan only the most commonly used ports instead of scanning all ports. It is typically used when you want to conduct a quicker scan and are primarily interested in finding open ports in the most commonly used ranges, rather than performing a full scan of all 65,535 ports.

When you use the-F option, Nmap will



Experiment 3

Demonstration of password vulnerability

John the Ripper password cracker

John the Ripper is a fast password cracker, currently available for many flavors of Unix, macOS, Windows, DOS, BeOS, and OpenVMS (the latter requires a contributed patch). Its primary purpose is to detect weak Unix passwords. Besides several crypt(3) password hash types most commonly found on various Unix flavors, supported out of the box are Kerberos/AFS and Windows LM hashes, as well as DES-based tripcodes, plus hundreds of additional hashes and ciphers in "-jumbo" versions.

How to install.

Install John from the Linux sudo

apt update

sudo apt install john

```
┌──(root㉿kali)-[/home/kali]
└─# sudo apt install john
john is already the newest version (1.9.0-Jumbo-1+git20211102-0kali10).
john set to manually installed.
The following packages were automatically installed and are no longer required:
  amass-common             libdisplay-info2       libjs-jquery-ui     libplacebo349
  gir1.2-girepository-2.0  libgdal37              libjs-underscore    libportmidi0
  libarmadillo14           libgeos3.14.0          libmongoc-1.0-0t64  librav1e0.7
  libbluray2               libgirepository-1.0-1  libnet1             libsqlcipher1
  libbson-1.0-0t64         libinstpatch-1.0-2     libobjc-14-dev      libtheoradec1
Use 'sudo apt autoremove' to remove them.
```

How to use.

To run John, you need to supply it with some password files and optionally specify a cracking mode, like this, using the default order of modes and assuming that "passwd" is a copy of your password file:

john passwd

or, to restrict it to the wordlist mode only, but permitting the use of word mangling rules: john--

wordlist=password.lst--rules passwd

Cracked passwords will be printed to the terminal and saved in the file called $JOHN/john.pot (in the documentation and in the configuration file for John, "$JOHN" refers to John's "home directory"; which directory it really is depends on how you installed John). The $JOHN/john.pot file is also used to not load password hashes that you already cracked when you run John the next time.

To retrieve the cracked passwords, run:

john--show passwd

While cracking, you can press any key for status, or 'q' or Ctrl-C to abort the session saving its state to a file ($JOHN/john.rec by default). If you press Ctrl-C for a second time before John had a chance to complete handling of your first Ctrl-C, John will abort immediately without saving. By default, the state is also saved every 10 minutes to permit for recovery in case of a crash.

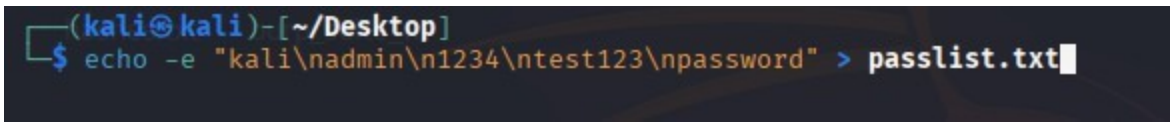
To continue an interrupted session, run:

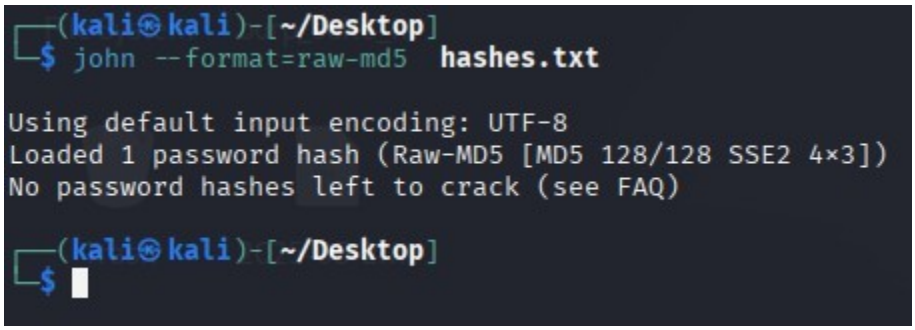
john--restore

Create a Password Wordlist Using echo

In this step, you will create a simple password wordlist file that john the ripper will use during brute-force testing. The file will contain multiple possible passwords, each on its own line.

echo-e "kali\nadmin\n1234\ntest123\npassword" > passlist.txt





In this step we are trying to crack password hash values which was stored in the hasesh.txt

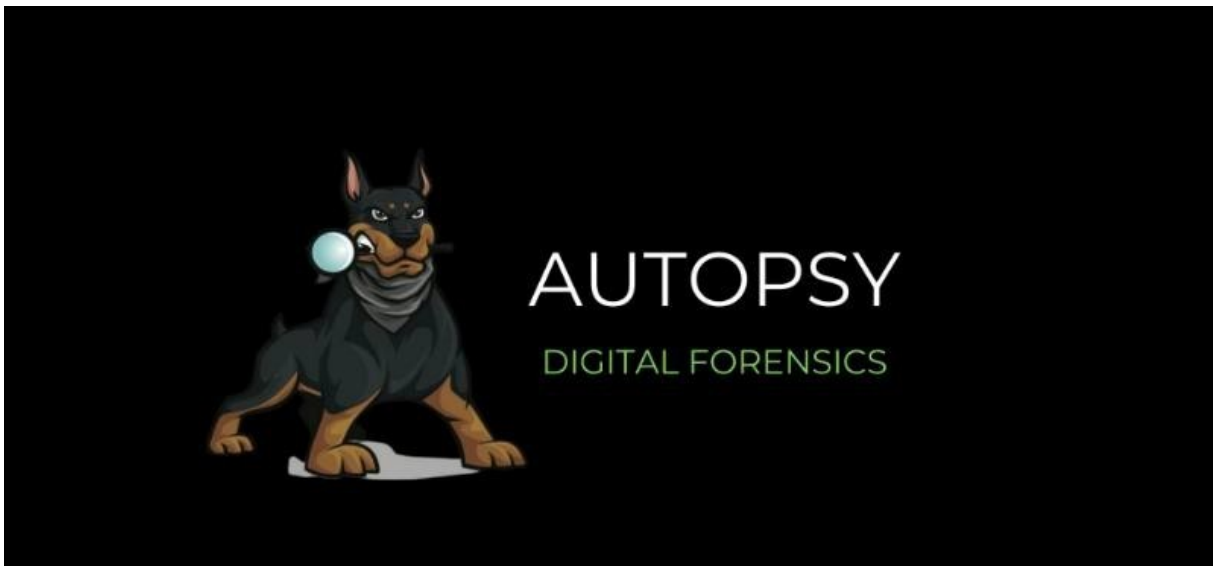
The password is: “password”, the password hash value is cracked successfully.

Experiment 4

Master the Fundamentals of Digital Forensics and Evidence Collection using Autopsy

An autopsy is an end-to-end open-source computer or digital forensics platform. It relates to the graphical interface of the Sleuth Kit and other computer forensic tools. It was built by Basis Technology with various essential features that can be used in commercial forensic tools.

It is used in different fields like law, military, corporate investigation, enforcement, etc. It can also be beneficial for personal use of individuals.



Autopsy helps forensic expert to:

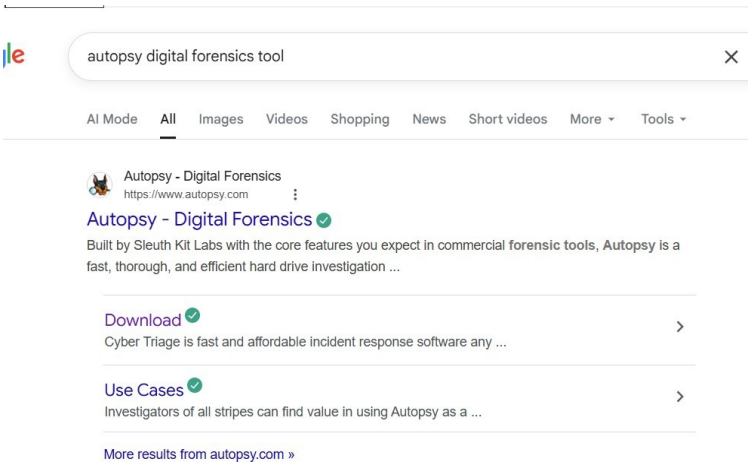
1. Create and Examine Forensic Images
   - Supports E01, E02, DD, RAW, AFF etc.
   - Ensures no changes are made to original evidence.
2. Recover Deleted Files
   - Finds deleted documents, photos, videos that are still present in unallocated space.
3. File System Analysis
   - Reads NTFS, FAT, exFAT, EXT, and other file systems.
   - Shows metadata (timestamps, permissions, file paths).
4. Keyword Searching

- Search for specific words, names, phone numbers, or patterns using keyword lists or regex.

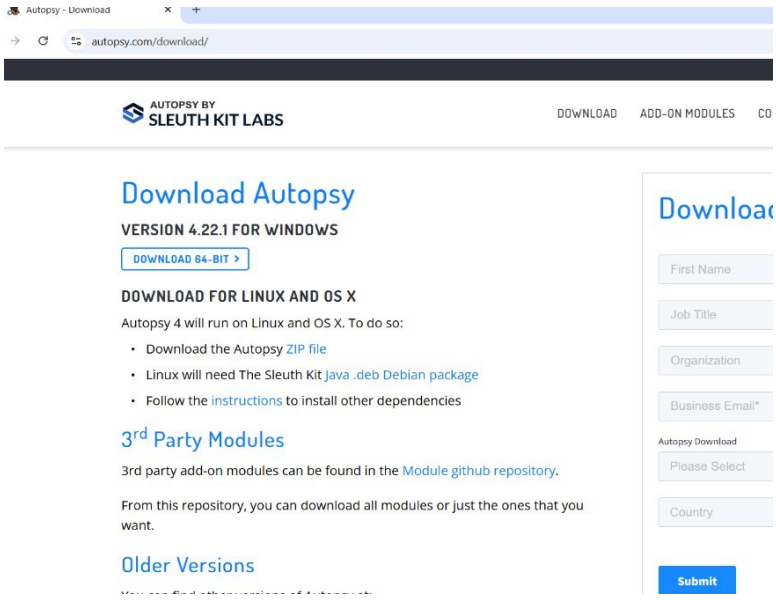
5. Timeline Analysis
   - Helps reconstruct events:
     - When files were created/deleted
     - Login times
     - Browsing history
     - Program execution
6. Browser History Analysis
   - Extracts browsing history from Chrome, Firefox, Edge.
   - Shows cookies, downloads, bookmarks.
7. Email Analysis
   - Reads PST, OST, MBOX, and other formats.
   - Extracts emails, attachments, timestamps.
8. Hash Filtering
   - Compares file hashes against databases:
     - Known Good (NSRL)
     - Known Bad (malware or illegal content)
9. Media & Artifact Extraction
   - Extracts:
     - Images
     - Videos
     - Thumbnails
     - EXIF data
     - Chat app artifacts (Skype, WhatsApp backups, etc.)
10. Reporting
    - Generates detailed HTML, PDF, or Excel reports for court.

How to install Autopsy?

Step 1 : Download the Autopsy from official website. As shown below



Step 2: Click on windows with the Windows Architecture of 64-bit.



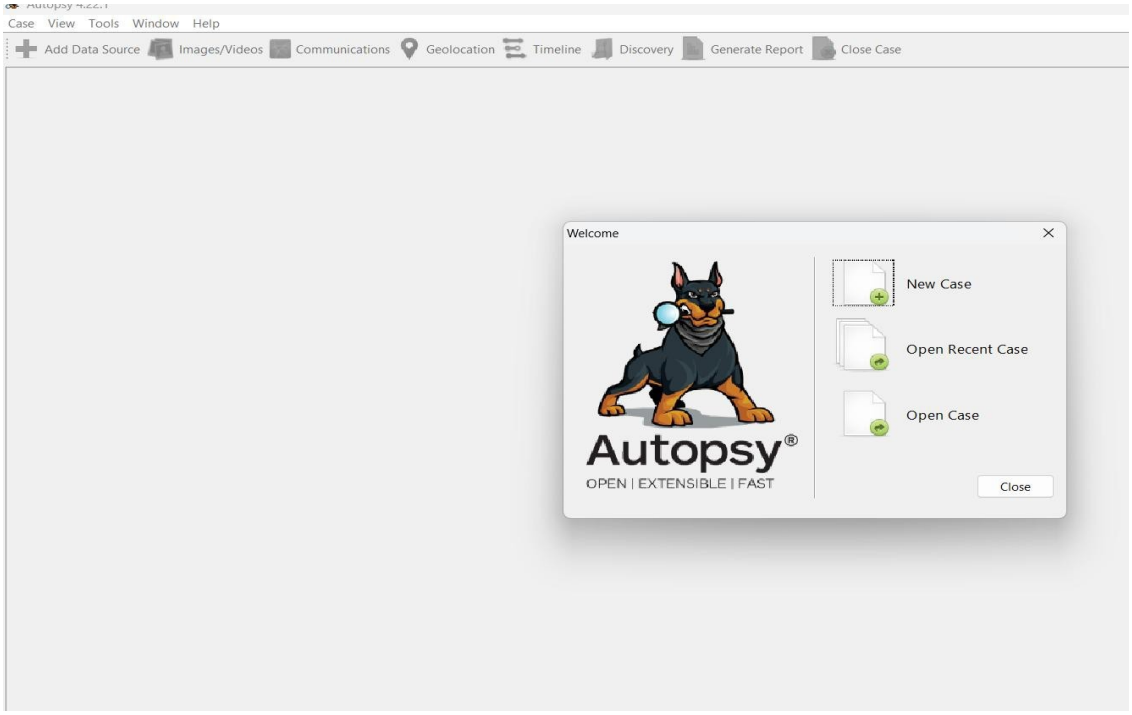
Step 3: If you get a Windows prompt, click yes.

Step 4: Click through the dialog boxes until you click a button that says Finish.

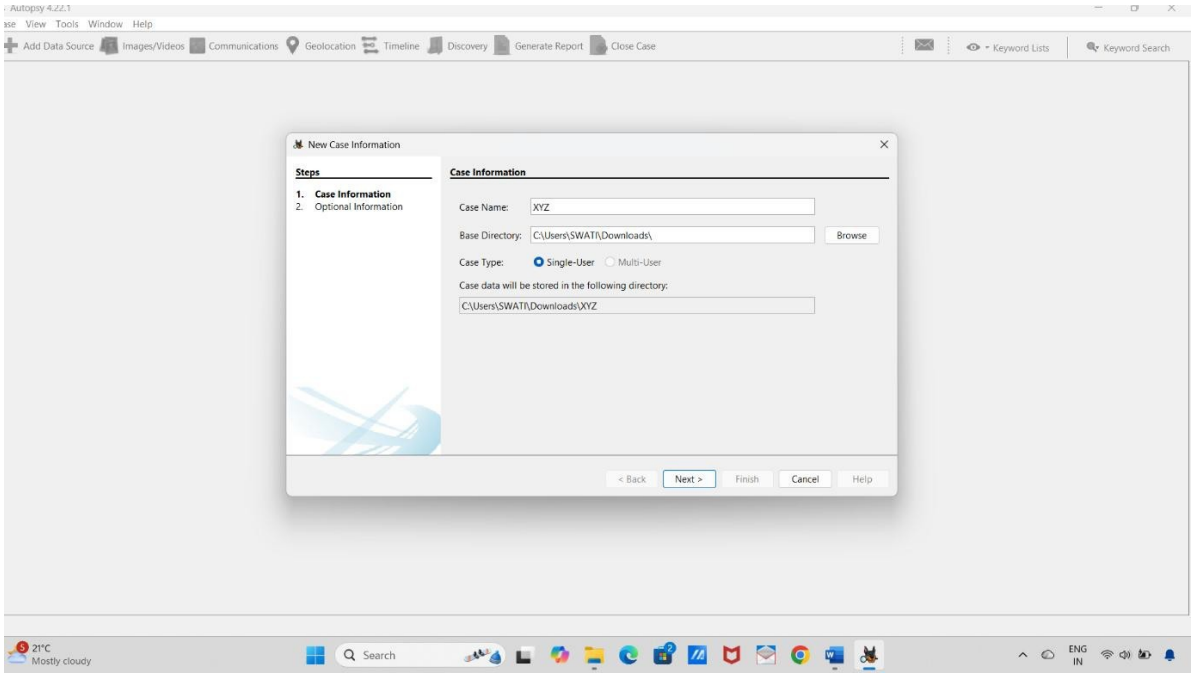
Step 5: Autopsy should be installed now.

How to use Autopsy for digital investigation? Step

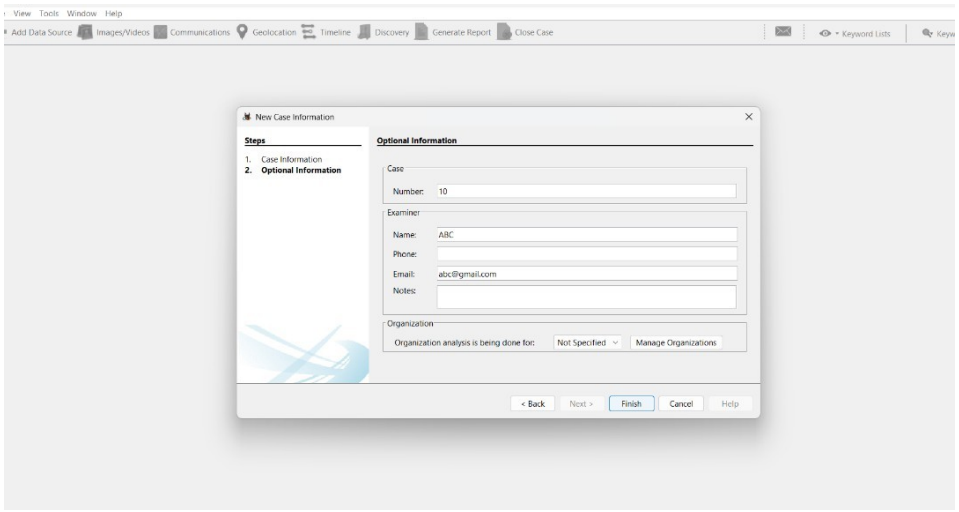
1: Run Autopsy and select new case.



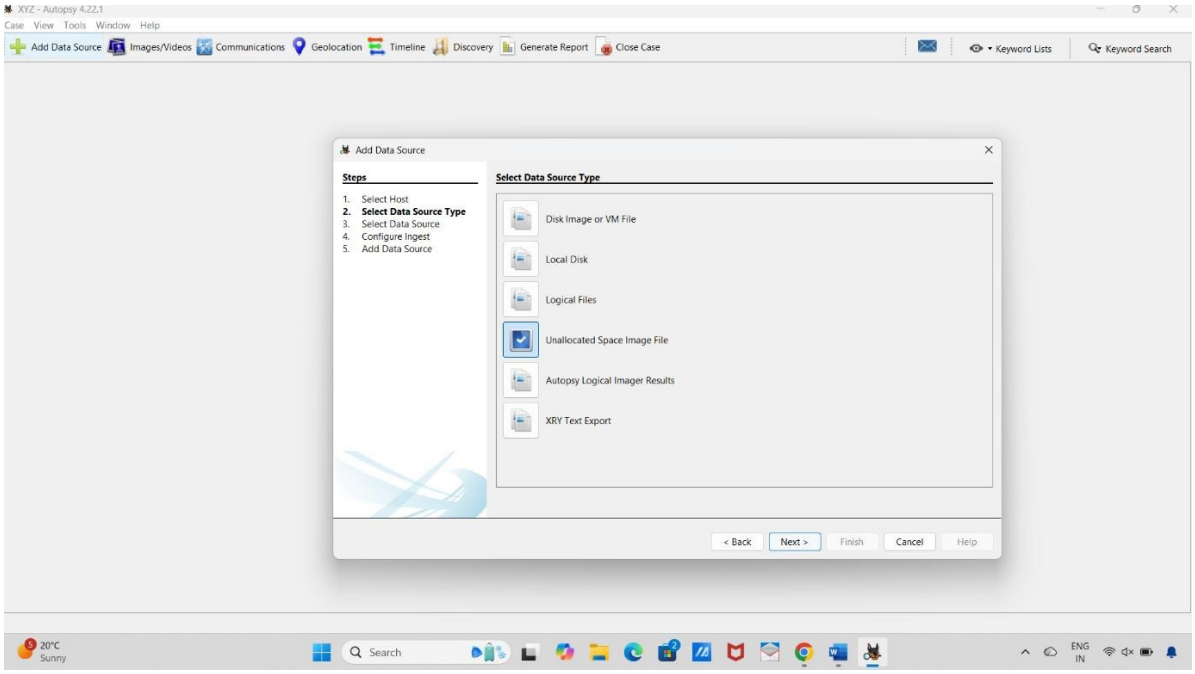
Step 2: Provide the case name and the directory to store the case file. Click on Next.



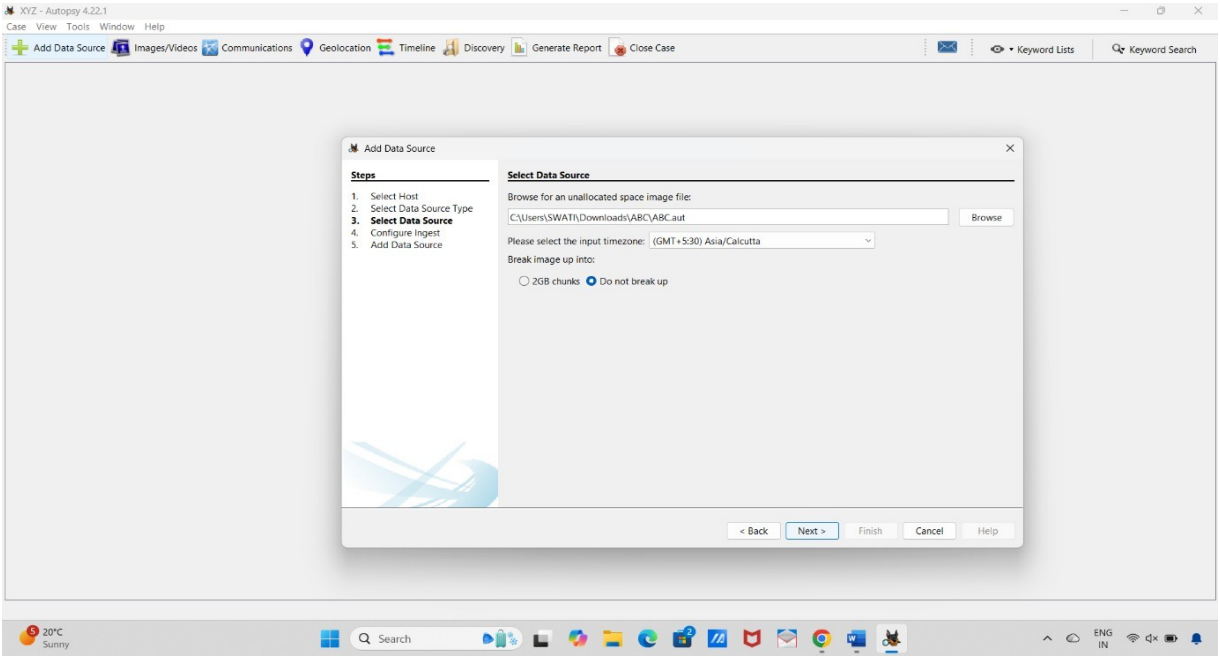
Step 3: Add case Number and Examiner's details, then click on Finish.



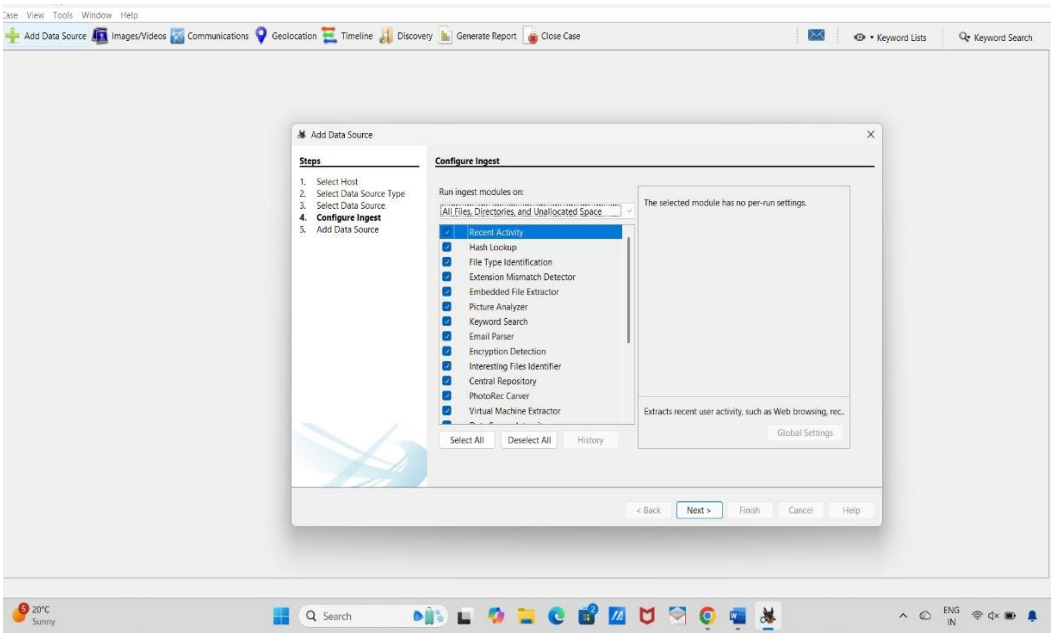
Step 4: Choose the required data source type, in this case Unallocated Slack image file click on Next.



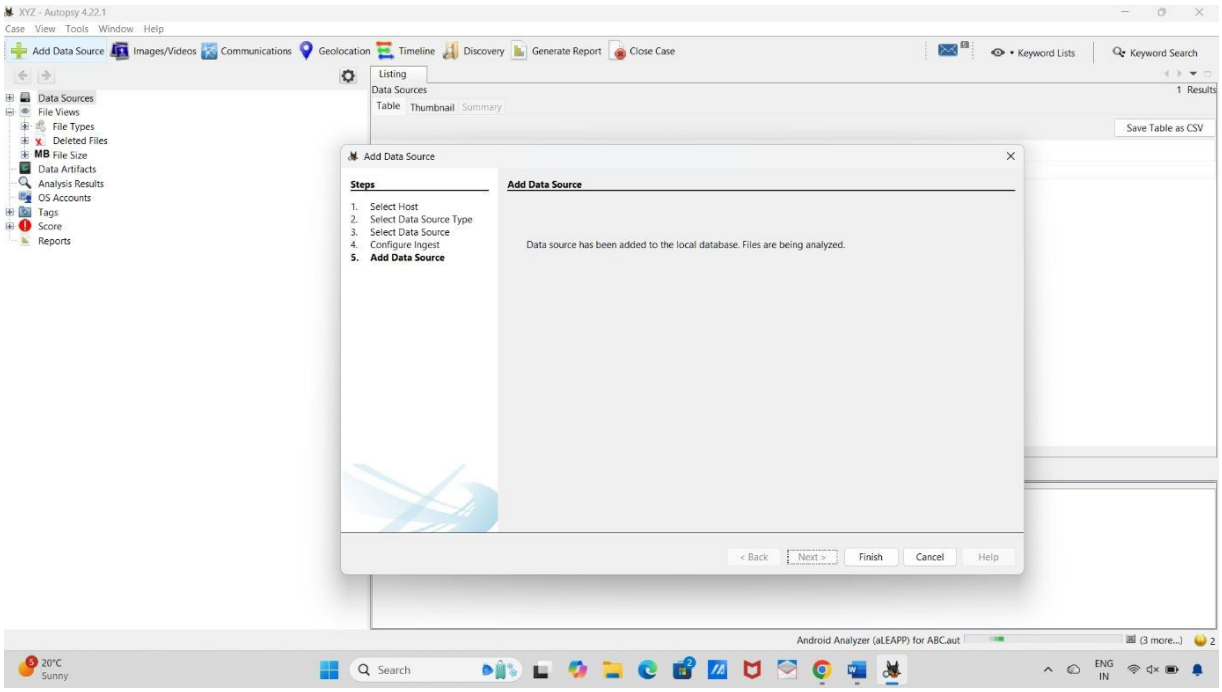
Step 5: Give path of the data source and click on Next.



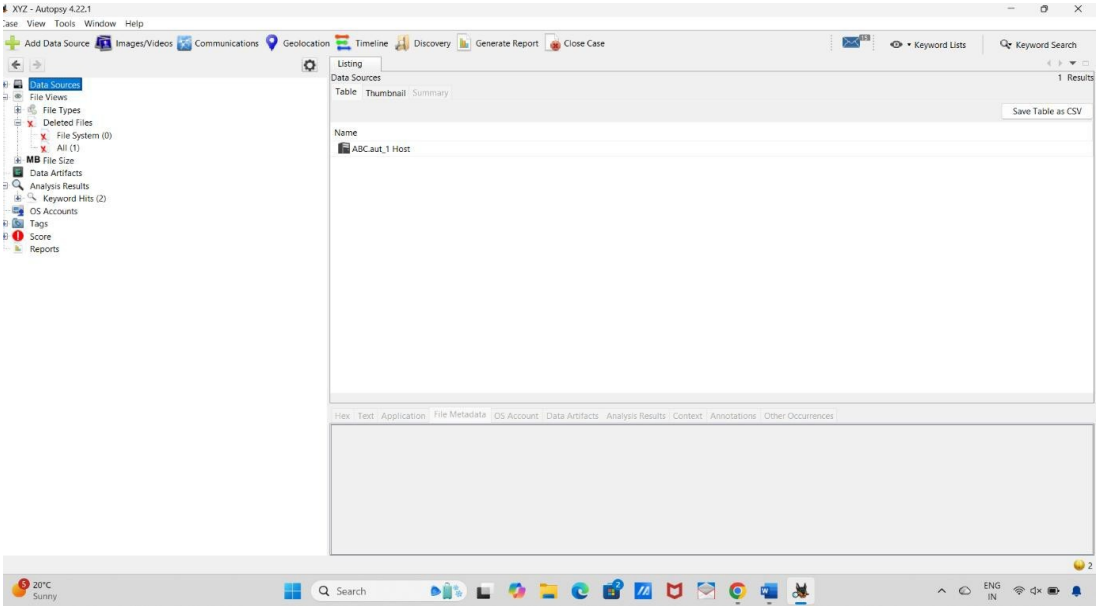
Step 6: Select the required modules and click on Next.



Step 7: After the data source has been added, click on Finish.



Step 8: You reach here once all the modules have been ingested. You can proceed for the investigation.



Experiment 5

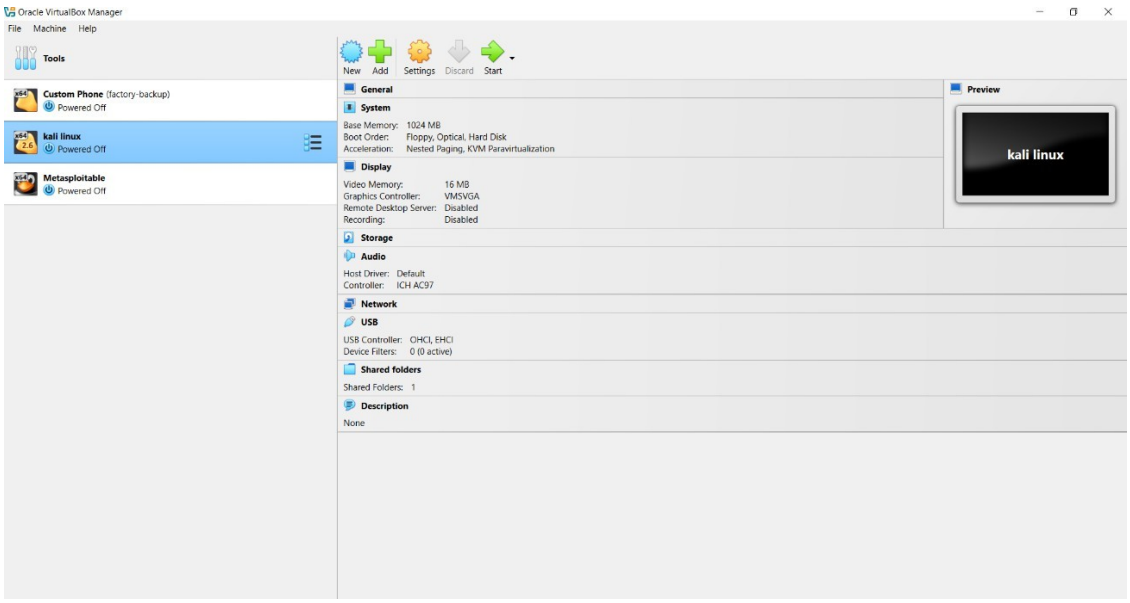
Exploit SQL Injection in an intentionally vulnerable web app (DVWA/OWAPS Juice shop) and document POC Fixes

Objectives

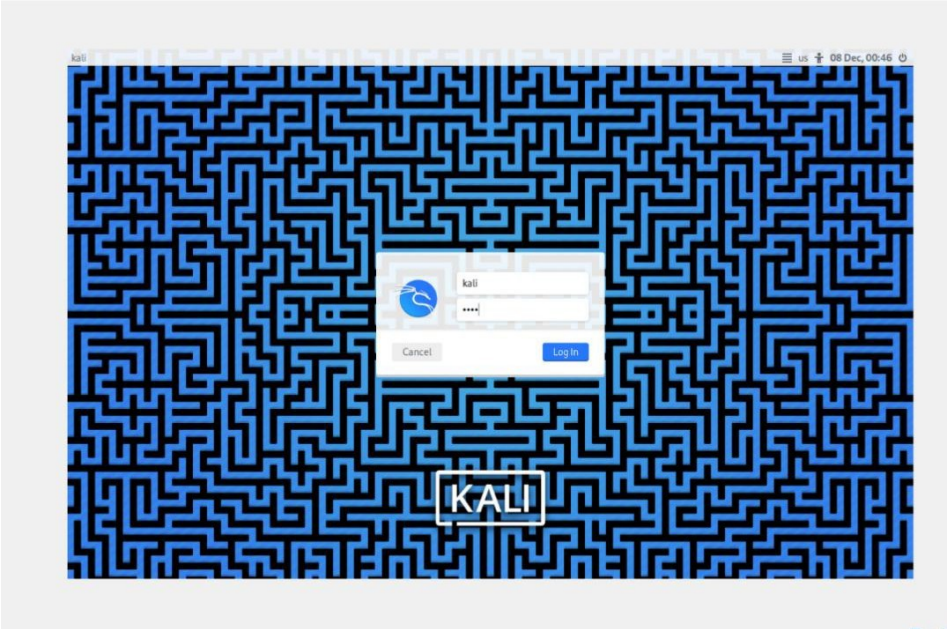
- To explain what DVWA is as a deliberately vulnerable web application designed for security training.
- To describe the purpose of DVWA, which is to provide a safe environment for practicing web vulnerability testing, understanding attacks, and learning secure coding techniques.
- To provide an overview of DVWA, including its features, security levels, and the various built-in vulnerabilities it offers for hands-on learning.

Overview of DVWA

DVWA (Damn Vulnerable Web Application) is a PHP/MySQL-based web application intentionally designed to be insecure. It includes multiple common web vulnerabilities—such as SQL Injection, XSS, CSRF, File Inclusion, and Command Injection—built into the system for training purposes. DVWA allows users to switch between different security levels (Low, Medium, High, Impossible) to practice exploiting vulnerabilities and then understand how they can be mitigated. It is widely used by students, developers, and security professionals to learn penetration testing, secure coding, and vulnerability analysis in a safe and controlled environment.



Select the instance and click the Start button in the top menu.

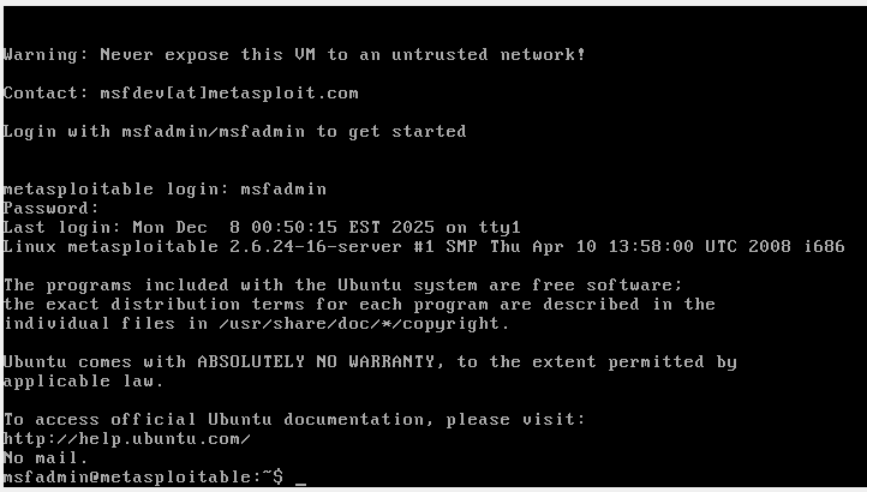


Login using default credentials:

Username: kali

Password: kali

Select the Metasploitable2 machine and click the Start button located in the top menu



Login using default credentials

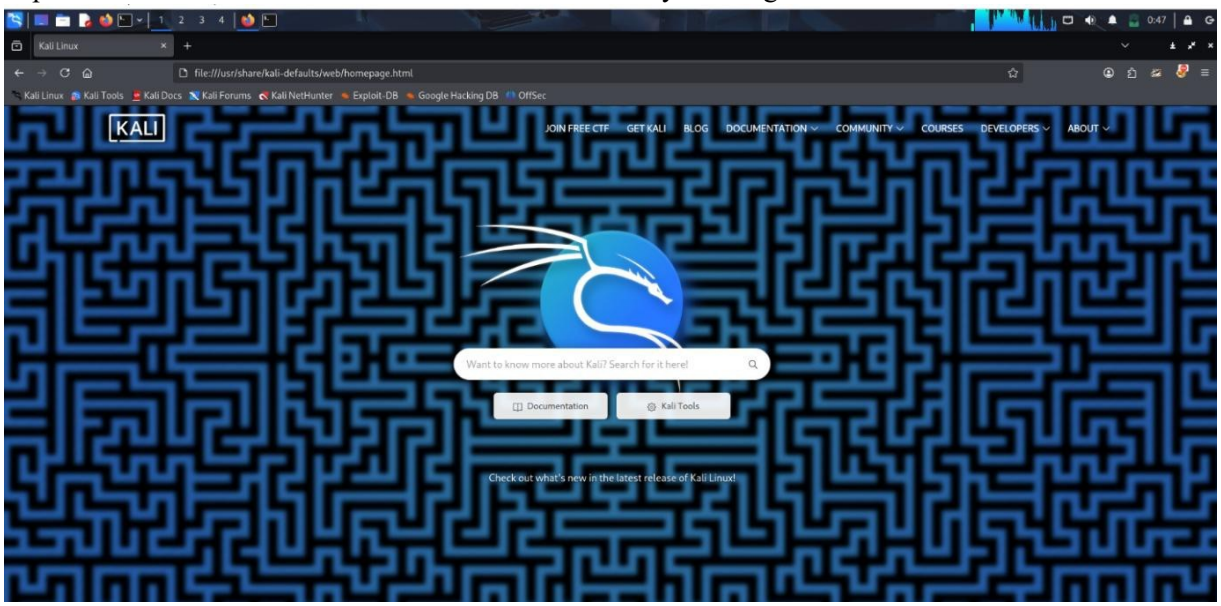
Username: msfadmin

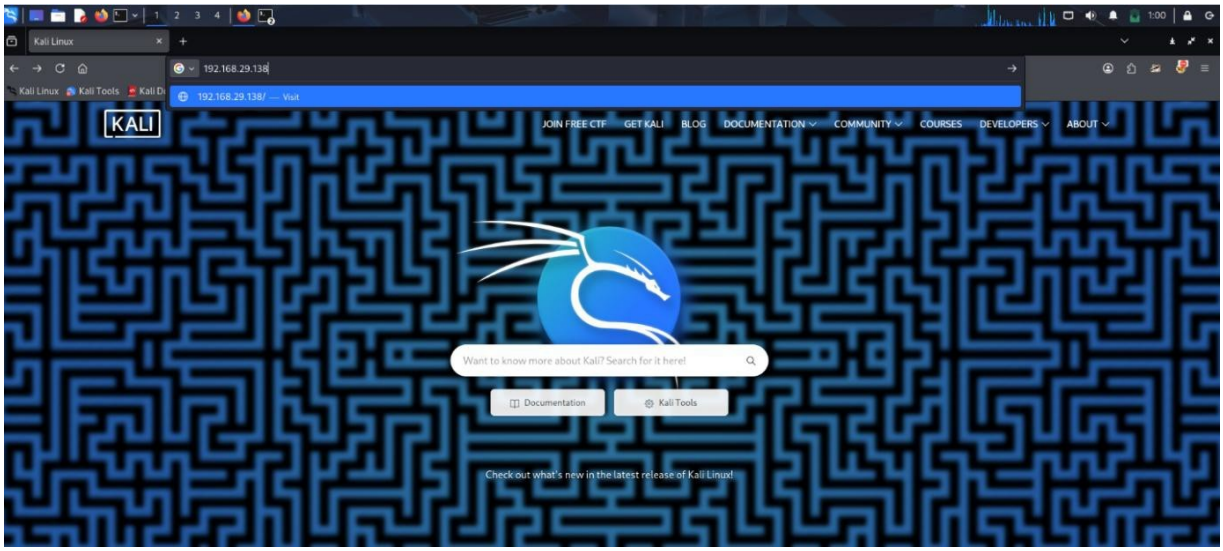
Password: msfadmin

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:52:6d:2d
          inet addr:192.168.29.139  Bcast:192.168.29.255  Mask:255.255.255.0
          inet6 addr: 2405:201:d00d:623c:a00:27ff:fe52:6d2d/64 Scope:Global
          inet6 addr: fe80::a00:27ff:fe52:6d2d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:162 errors:0 dropped:0 overruns:0 frame:0
          TX packets:70 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:19258 (18.8 KB)  TX bytes:7368 (7.1 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:101 errors:0 dropped:0 overruns:0 frame:0
          TX packets:101 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:23573 (23.0 KB)  TX bytes:23573 (23.0 KB)

msfadmin@metasploitable:~$ _
```

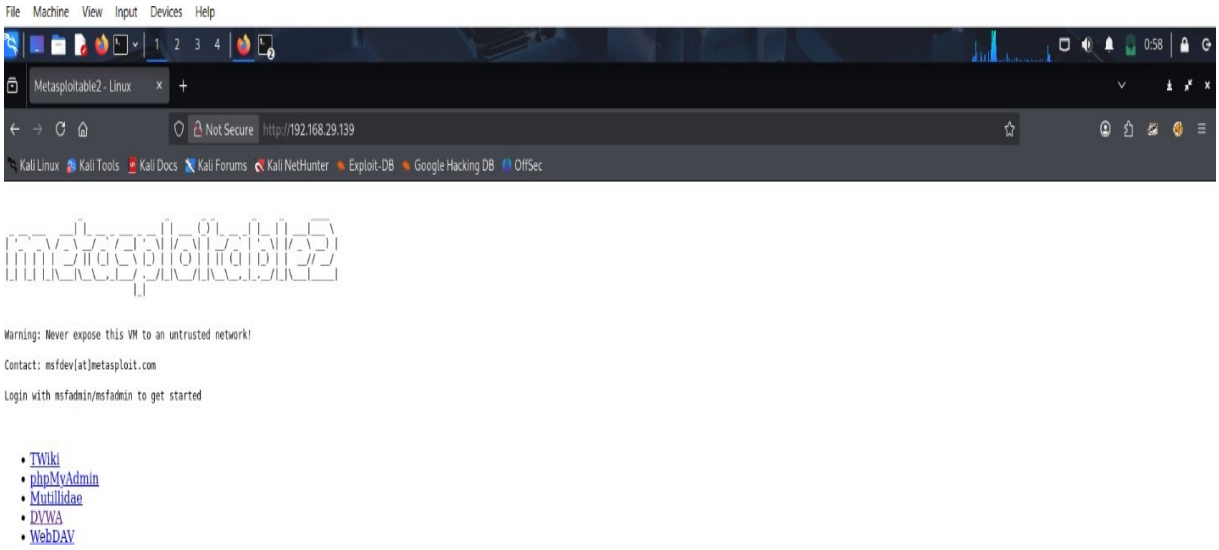
To check IP Address, enter command ifconfig

Open Kali Linux and launch the Firefox web browser by clicking on its icon





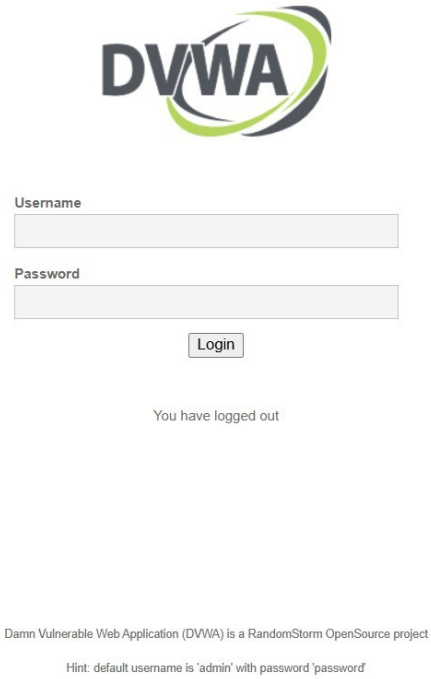
In the browser's search bar, enter the IP address



Click on the DVWA link to open the application

DVWA

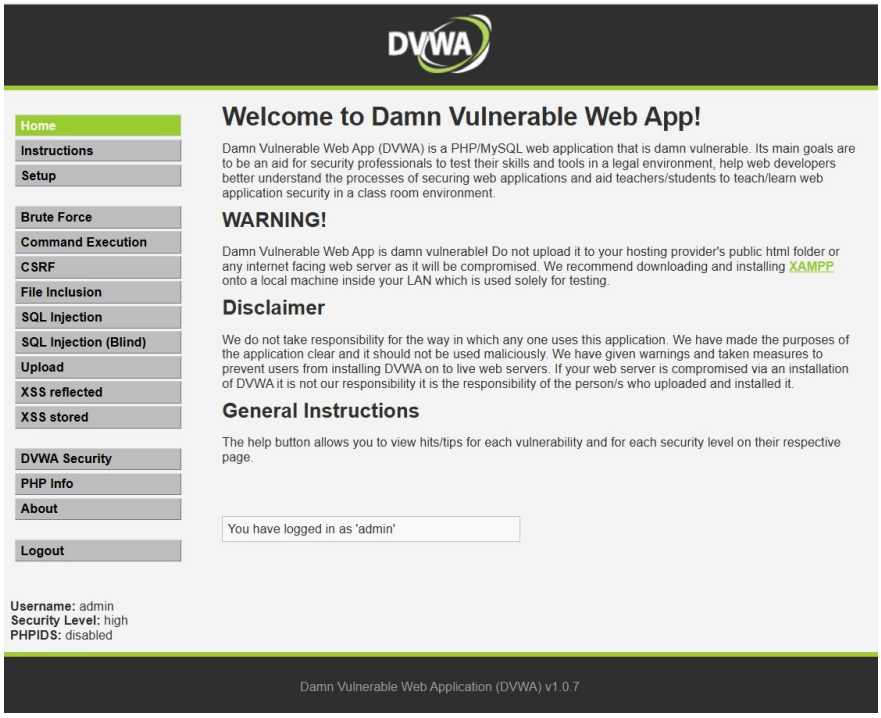
DVWA stands for Damn Vulnerable Web Application, a PHP/MySQL web application designed to help security professionals and enthusiasts learn about web application security. It's a deliberately insecure platform, making it an excellent tool for practicing and understanding common web vulnerabilities and how to mitigate them.



Log in using default credentials (admin/password).

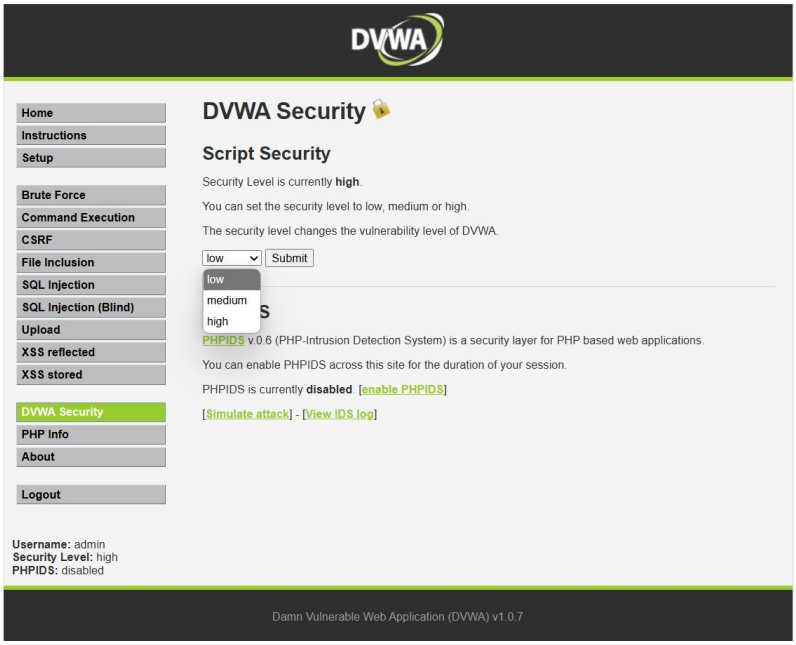
1. Vulnerabilities Included:

- SQL Injection
- Cross-Site Scripting (XSS)
- Cross-Site Request Forgery (CSRF)
- File Inclusion
- Command Injection
- Brute Force
- Insecure File Upload
- Security Misconfigurations.



2. Difficulty Levels: DVWA allows users to adjust the security level (Low, Medium, High, and Impossible) to simulate different scenarios and challenges.

Go to the "DVWA Security" tab and set the security level to Low.



SQL Injection

SQL Injection is a web application vulnerability that occurs when an attacker is able to insert or “inject” malicious SQL commands into a query that the application sends to its database. This happens when user input is not properly validated or sanitized.

Objective:

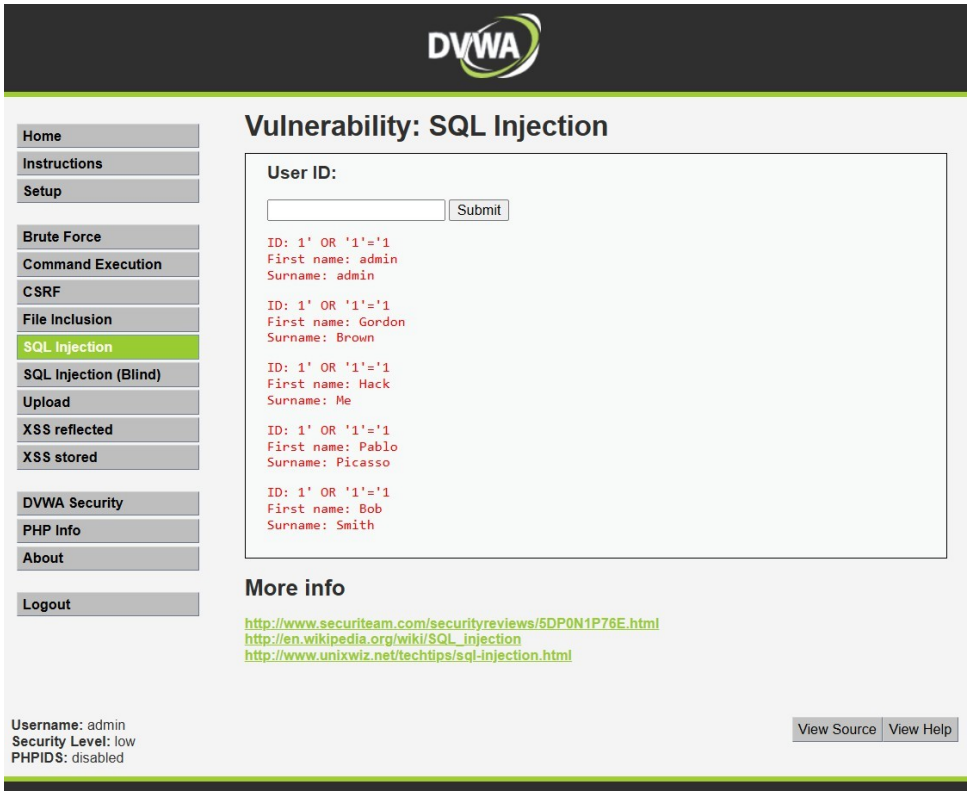
Extract sensitive data from the database by injecting malicious SQL queries.

Steps:

1.Navigate to the SQL Injection module.

2. Enter ' OR '1'='1 in the input field for "User ID" and click Submit.

This query bypasses authentication and retrieves all user data.



Experiment 6

Capture network traffic (Wireshark) for given scenarios, identify suspicious flows, and suggest detection rules.

Wireshark

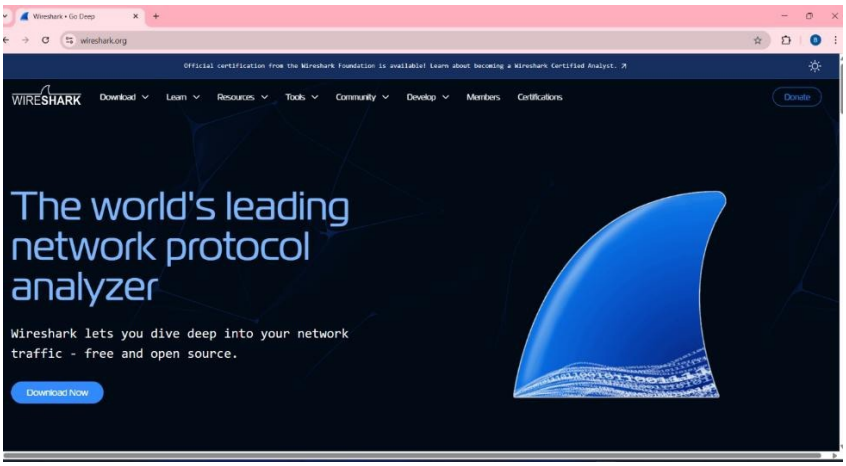
Wireshark is a powerful open-source network protocol analyzer used for network troubleshooting, analysis, and cybersecurity. It captures and inspects packets in real time, allowing users to see what's happening at a granular level in their network

Key Features of Wireshark:

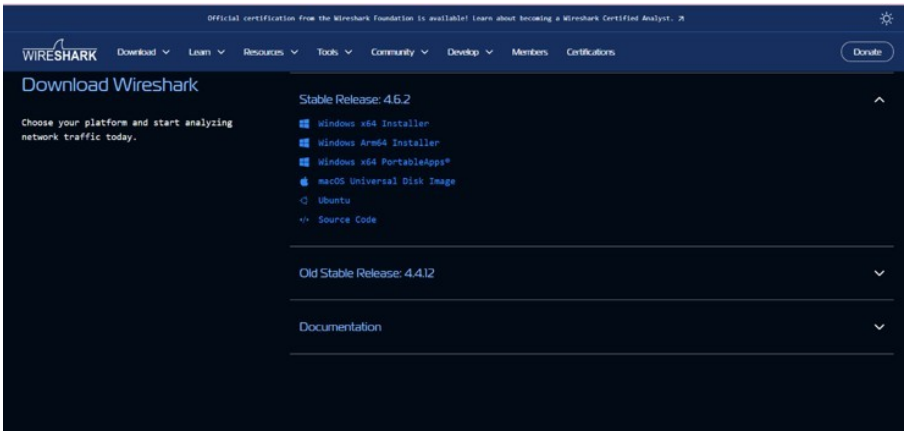
- Packet Capture: Captures network traffic from various interfaces.
- Deep Packet Inspection: Examines individual packets for detailed analysis.
- Protocol Analysis: Supports hundreds of network protocols (TCP, UDP, HTTP, DNS, etc.).
- Filtering & Searching: Apply display filters to find specific packets.
- Live & Offline Analysis: Capture live traffic or analyze saved .pcap files.

Install Wireshark

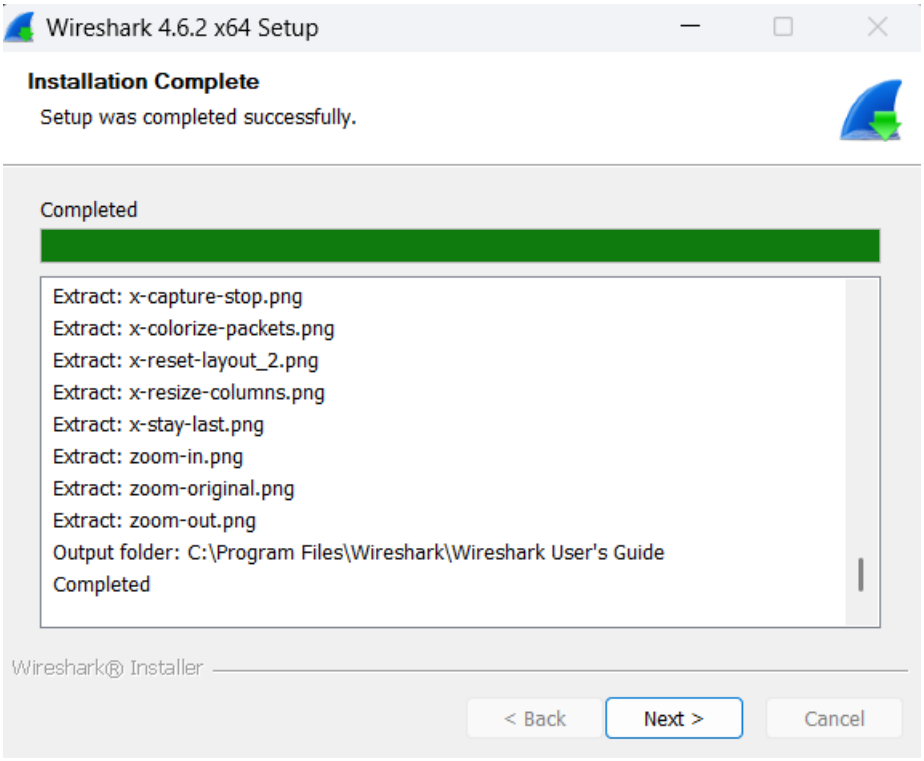
1. Step 1: Go to the official download page: https://www.wireshark.org/download.html



2. Download the Windows (64-bit) installer.



3. During setup, make sure to install Npcap (required for packet capturing).
4. Complete the installation and launch Wireshark.



When you launch Wireshark, you will see:

- A list of available network interfaces
- Your recent capture files
- The main toolbar and filter bar

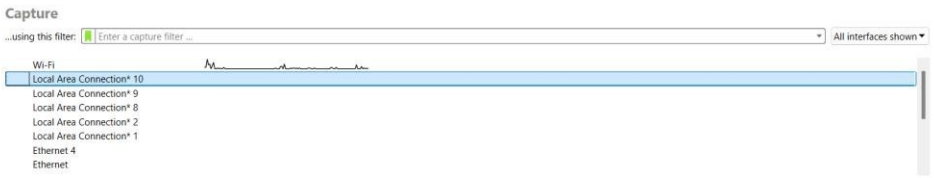
From here, you can select a network interface and start capturing packets immediately.

Choosing the Right Network Interface

Before you can start capturing packets, you need to choose the correct network interface. Wireshark will display all available interfaces on your system, and each one represents a different network connection.

The most common interfaces you will see include:

- Wi-Fi – Use this if you are connected to the internet wirelessly.
- Ethernet – Use this if your computer is connected via a network cable.
- VPN adapters – These appear when you are connected to a VPN.
- Virtual machine adapters – Created by software like VMware, VirtualBox, or Hyper-V.
- Loopback – Used for internal traffic on your computer; generally for advanced testing.



Start Capturing Packets (The Basics)

Once you have selected the correct network interface, you can begin capturing packets. This is the core function of Wireshark and the first step in analyzing network traffic.

How to start a packet capture:

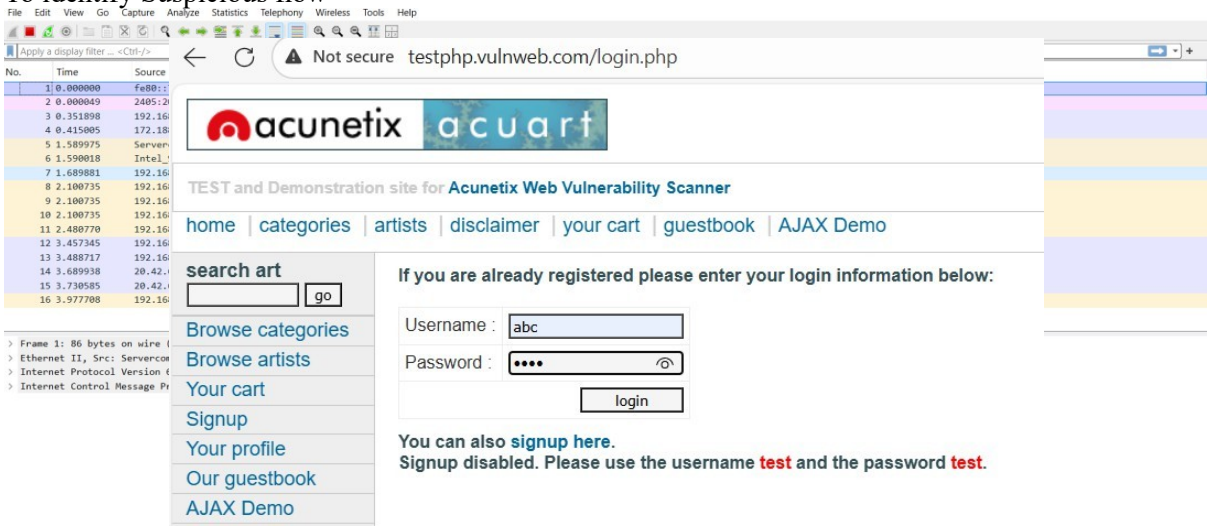
1. Select your network interface from the list.
2. Click the blue shark fin icon (Start Capturing Packets).
3. Packets will immediately begin scrolling in real time.
4. When you want to stop capturing, click the red square button (Stop).
5. To save your capture, go to File → Save As and save it as a .pcapng file.

Wireshark displays each packet in a new row, showing details such as the source, destination, protocol, and additional information.
Understanding the packet list columns:

- No. – The packet number in the capture sequence.
- Time – When the packet was captured.
- Source – The device sending the packet.
- Destination – The device receiving the packet.
- Protocol – The protocol used (TCP, UDP, DNS, HTTP, etc.).
- Length – Size of the packet.
- Info – A summary of what the packet contains.

At this stage, your packet capture is running and you are ready to begin analyzing the data.

To identify Suspicious flow



Open an Unsecure Website:

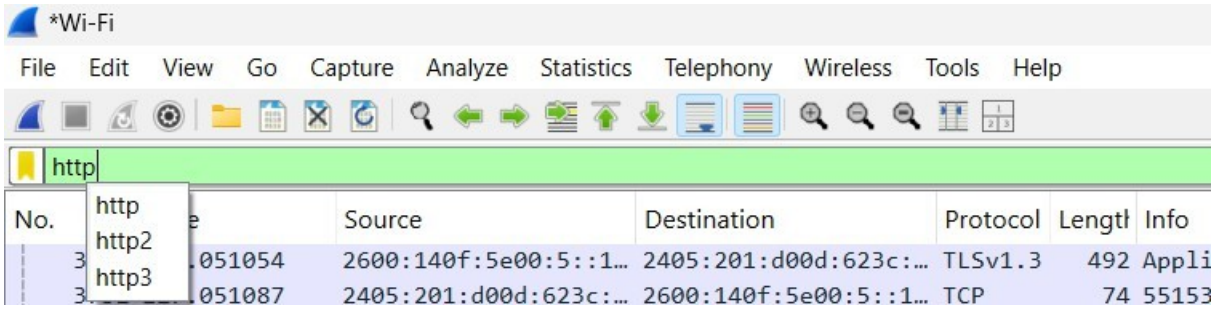
Login in to the website using random credentials like

Username: abc

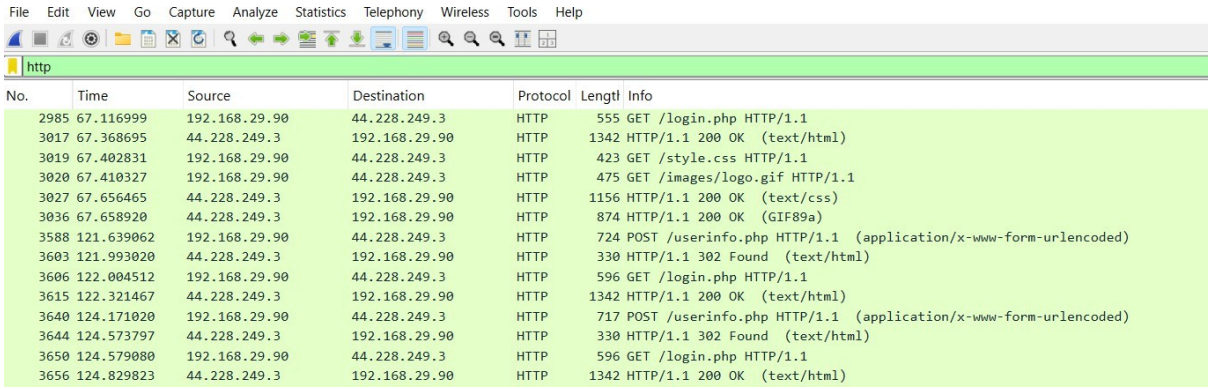
Password: 1234

Open Wireshark this login activity has been captured

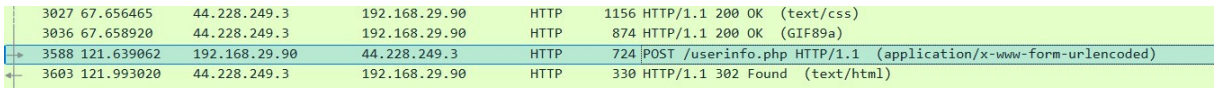
Use display filter and apply filter like http to filter out just the http packets.



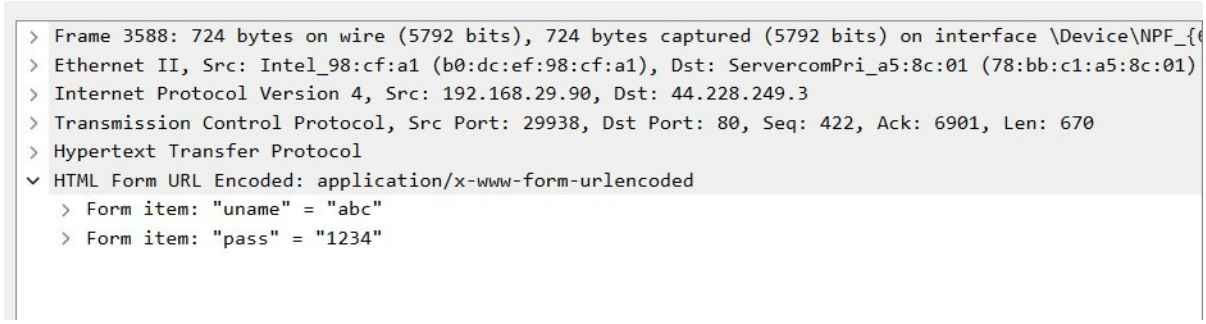
After applying the filter only http filters will get displayed



Click and open the packet which has the post method as shown in the image below



Double click to open the packet to analyze you will get the login credentials in a plan text format which attacker can view easily



Experiment 7

Embed /extract hidden data in files (image/audio/doc) and evaluate detectability and forensic hints.

Objectives

- Understand data hiding and steganography concepts
- Analyze carrier files for hidden content
- Extract embedded data using forensic utilities
- Evaluate detectability using statistical and structural indicators
- Identify forensic traces useful for investigations

Theory Overview

Steganography is the practice of concealing data within another file such that the existence of the hidden data is not apparent. Unlike encryption, steganography hides existence, not just content.

Common hiding areas:

- Least Significant Bits (LSB)
- Metadata sections
- Embedded objects
- Appended data after EOF
- Invisible Unicode characters

Steganography:

Steganography is the technique of hiding secret information inside ordinary files—such as images, audio, or text—so that the hidden data is not noticeable to anyone.

StegOnline Tool:

StegOnline is a web-based steganography analysis tool that lets you upload an image and inspect it using features like bit-plane viewing, LSB analysis, and PNG chunk inspection to detect or extract hidden data.

Tool: https://www.georgeom.net/StegOnline/upload

Preparation

1. Choose a set of test images ("cover images"). This could include PNGs, JPEGs, or other common formats. Keep a clean original copy for comparison.
2. (Optional / educational) Prepare a small text payload (e.g., secret.txt) or a small black-and-white image to embed via LSB — only if you intend to test embedding vs detection.
3. Make sure your browser is updated; open the StegOnline site (the "Upload" page).

Embedding (for controlled lab experiments)

1. Open StegOnline, upload your cover image via the "Upload" interface.
2. Navigate to the Embed page / UI panel. StegOnline allows embedding data using LSB techniques — you can select which bit-planes (e.g. LSB = bit 0, or bit 1, etc.), and which color channels (R, G, B, A) to embed in.
3. Provide the data you want to embed (text or an image). Configure options (bit-pattern, channels).
4. Perform the embedding; then download / save the resulting "stego image."
5. Keep both the original (cover) and the stego images for comparison.

Extraction & Inspection (using StegOnline)

You can use StegOnline to attempt to extract hidden data (if any exists), or at least inspect potential anomalies / bit-level artifacts.

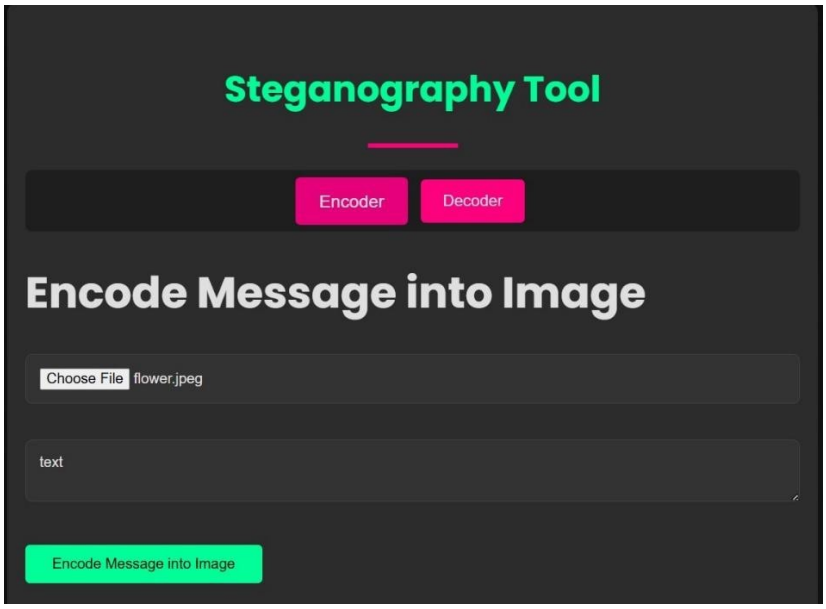
1. Upload the suspect image to StegOnline (via "Upload").
2. Use the Bit-plane browsing panel: view the image per-bitplane (for each channel: R, G, B, A) — this can reveal hidden patterns, text, or images embedded in low-order bits.
3. Use the Extract LSB data function: set the bit-pattern / channels (same as embedding, if known). If hidden data was embedded, this should recover it.

4. Use PNG chunk / metadata inspection (if image is PNG): StegOnline shows chunk info (e.g. IHDR, IDAT, ancillary chunks) — anomalies here can hint at manipulations.
5. Use String-extraction (if supported) — StegOnline may reveal plain ASCII/UTF strings hidden in image data

Steganography tool

Navigate to the website: https://iicsf.com/steganography-online/

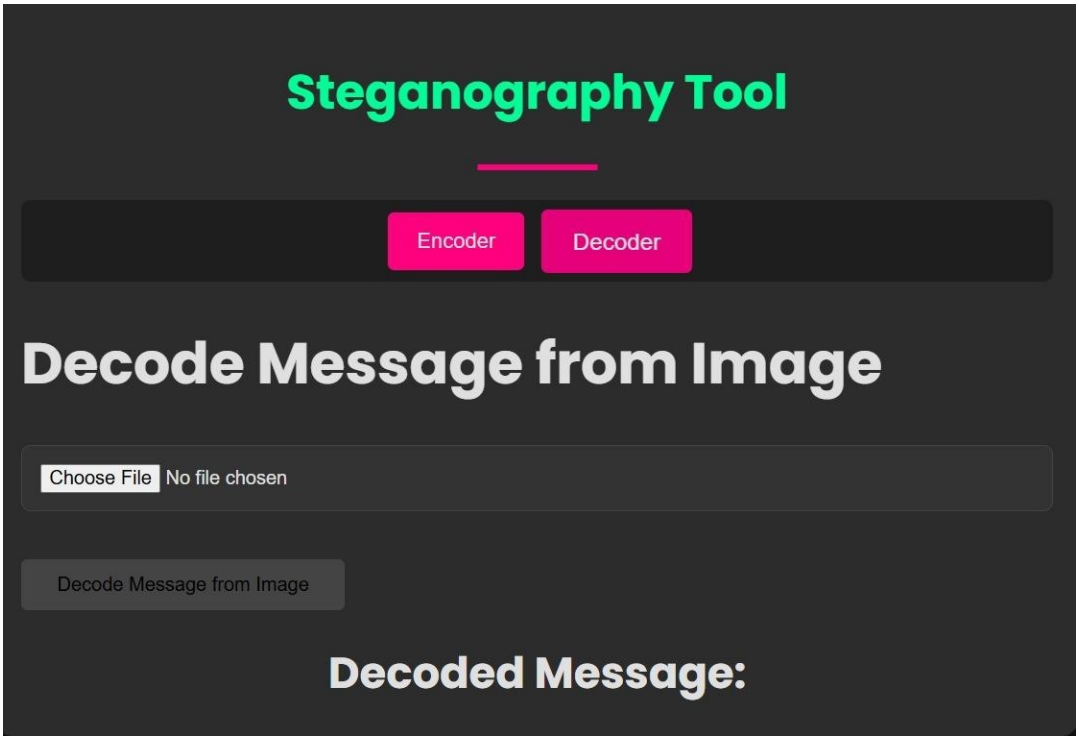
Select the image file to be used as the carrier, and specify the content that you wish to conceal within the image.



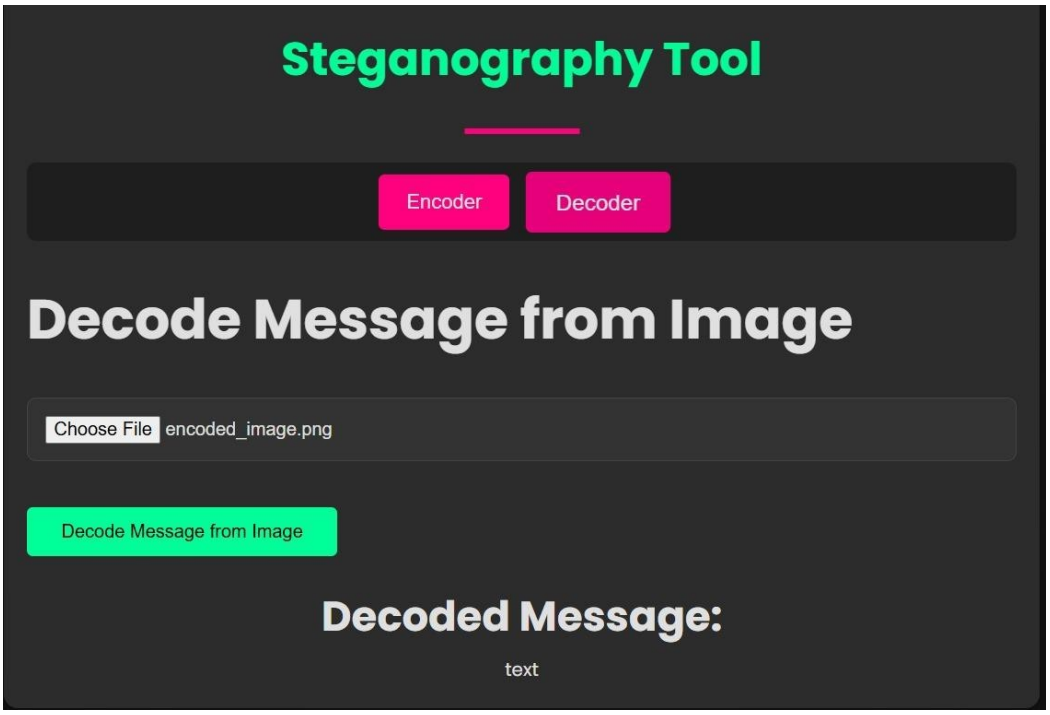
Click on the “Encode Message into Image” option to upload the selected image.

Once the image is uploaded, an output image containing the encoded message will be generated. Save this image for future use.

To retrieve the hidden message, select the “Decode” option:



Select the image file that contains the hidden data and click on “Decode Message from Image”. The encoded message embedded in the file will then be successfully extracted.



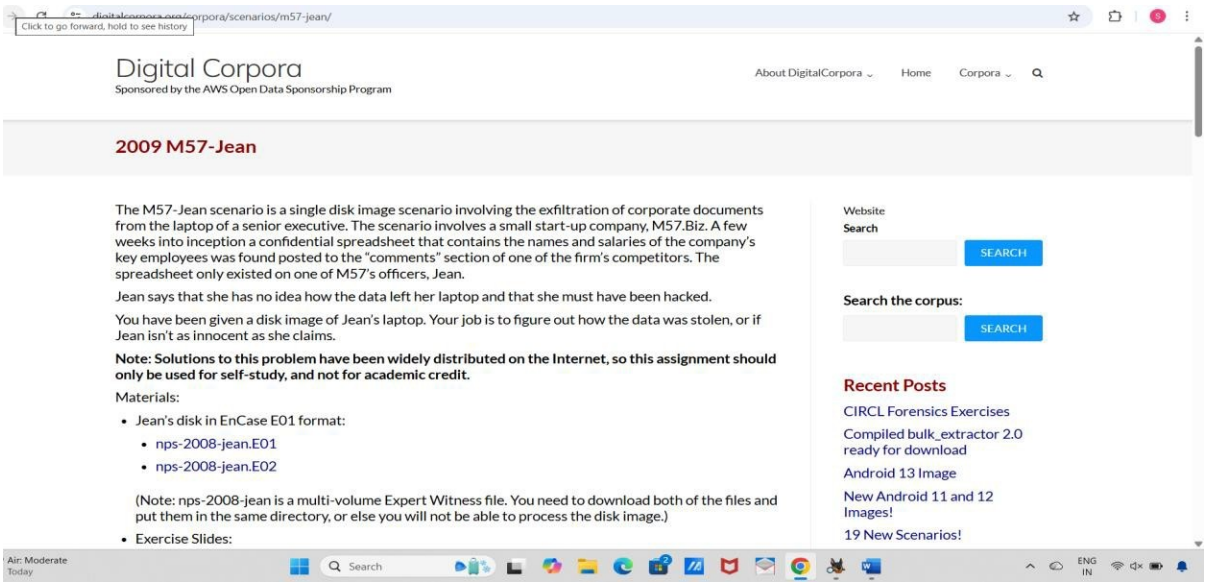
Experiment 8

Analyze a provided memory dump using Volatility to identify processes, network connections, and possible malicious artifacts.

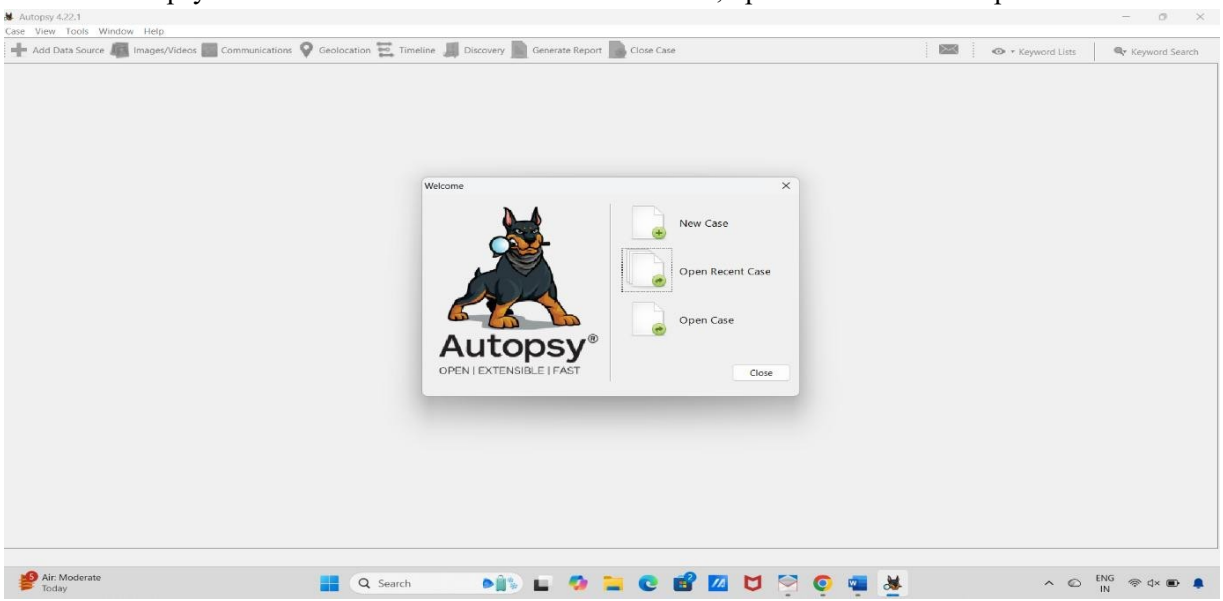
Case Analysis

Now, we will see how we can use Autopsy for investigating a hard drive. For that, we will go through a scenario most of us come across while studying digital forensics, and that is the scenario of 2009 M57-Jean.

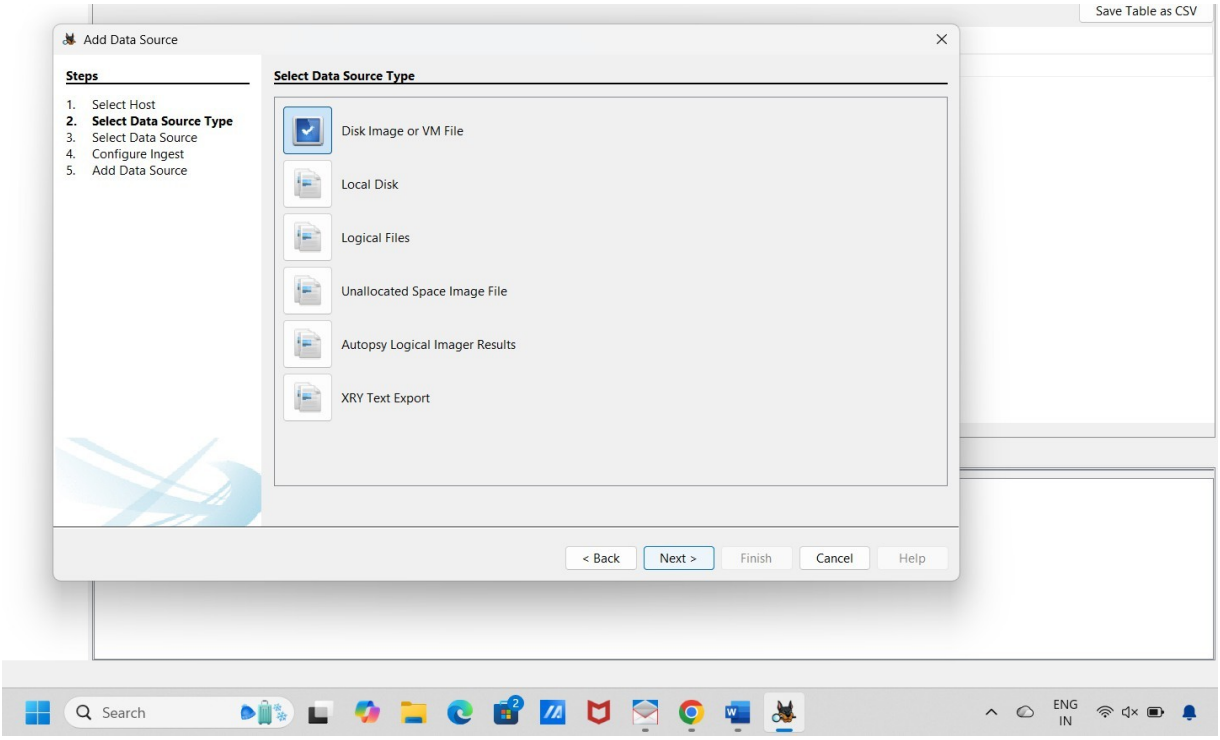
The image displays the complete scenario:



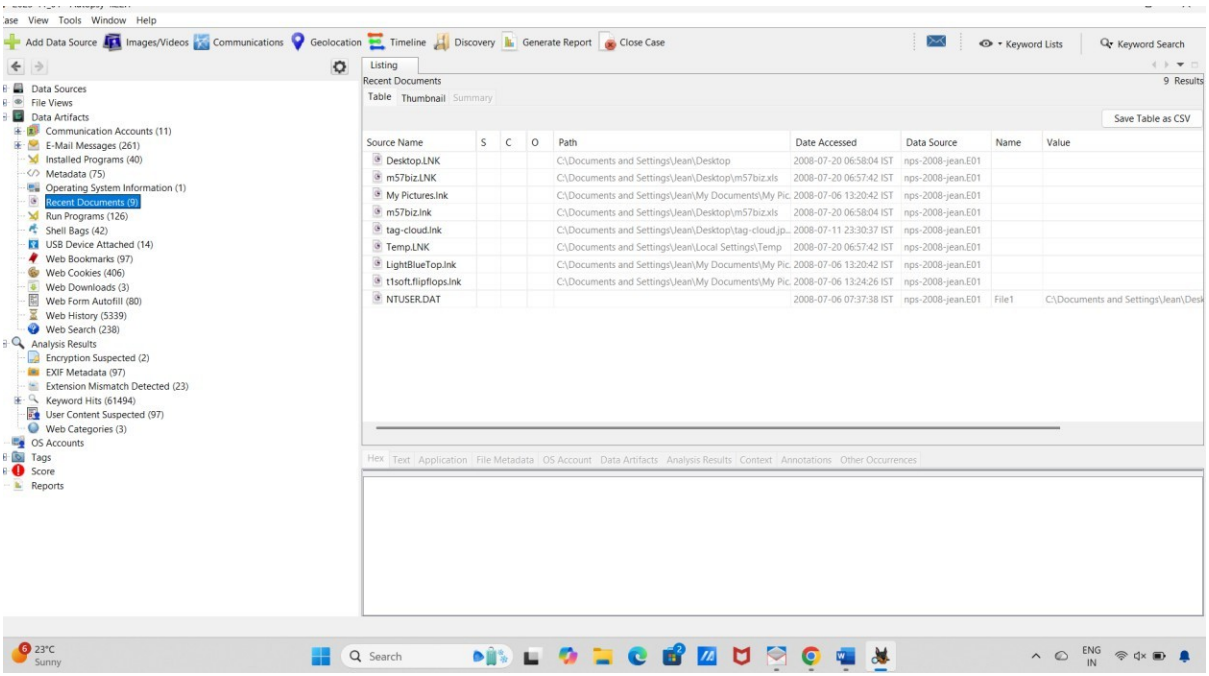
Start the Autopsy software and choose between the new case, open Recent Case or open case



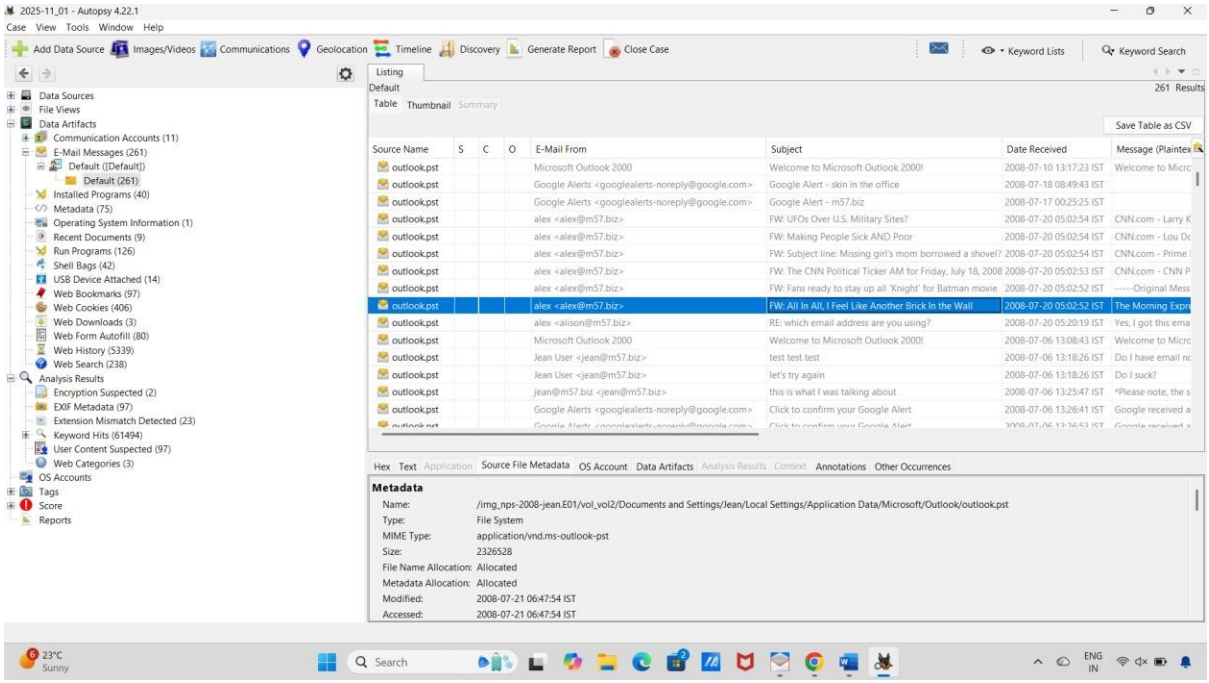
Enter the case information like the case number and location it, is to be saved in (if it's new case). The case number and examiner details may also enter.



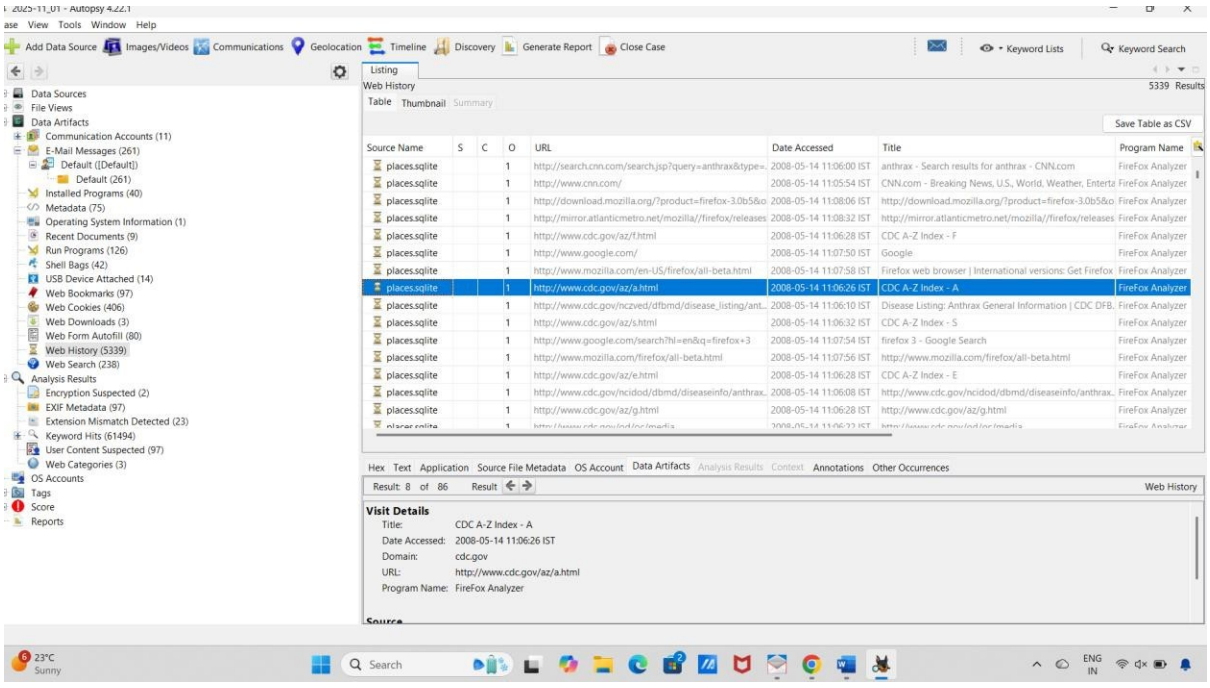
The ingested file nps-2008-jean.E01 and nps-2008-jean.E02 can be viewed



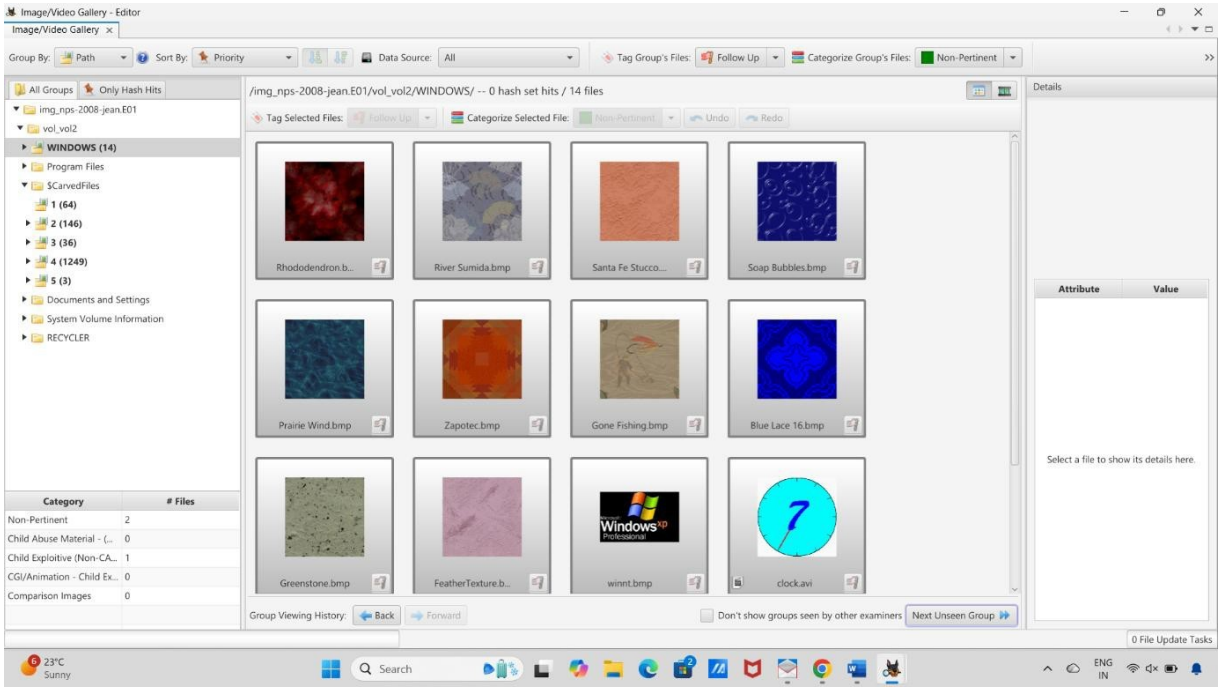
The mail from and to along with subject and meta data can be viewed.



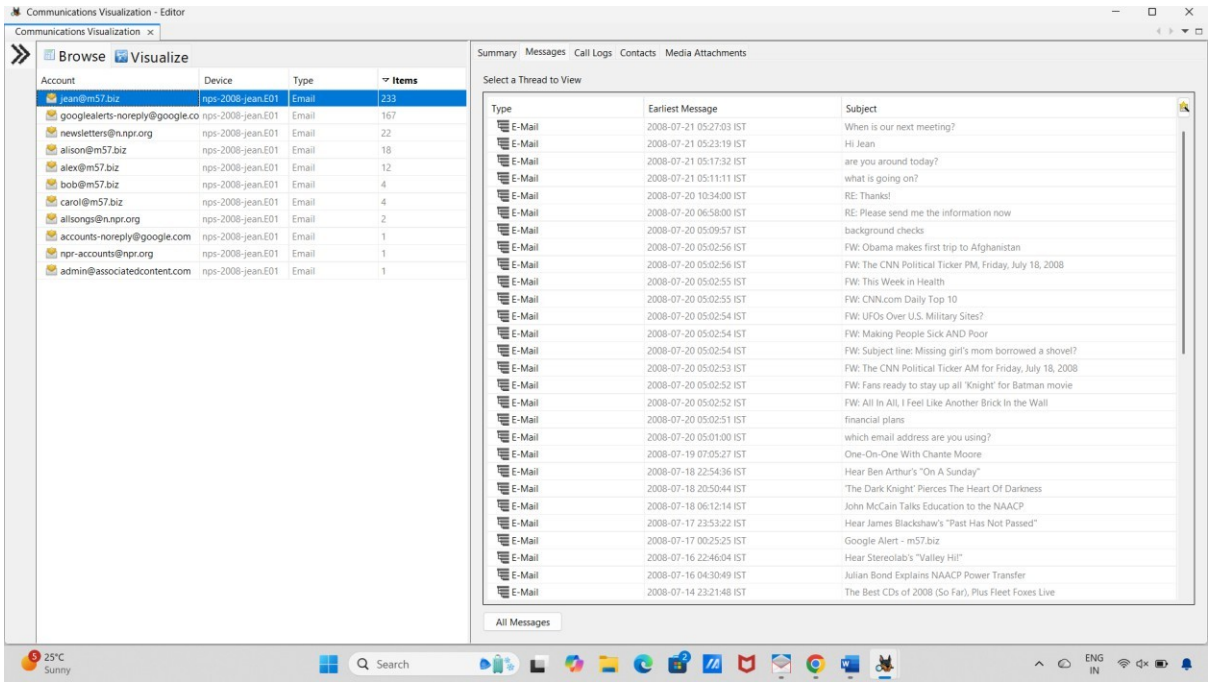
The web History can be viewed.



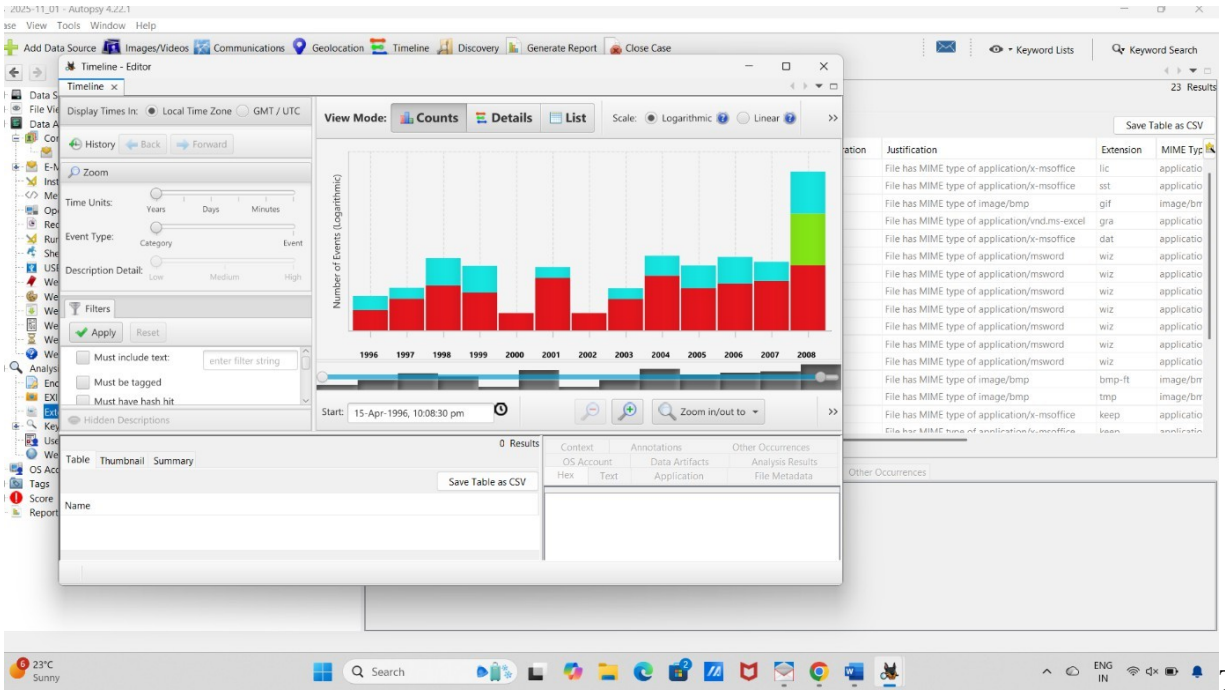
The image and video can be viewed.



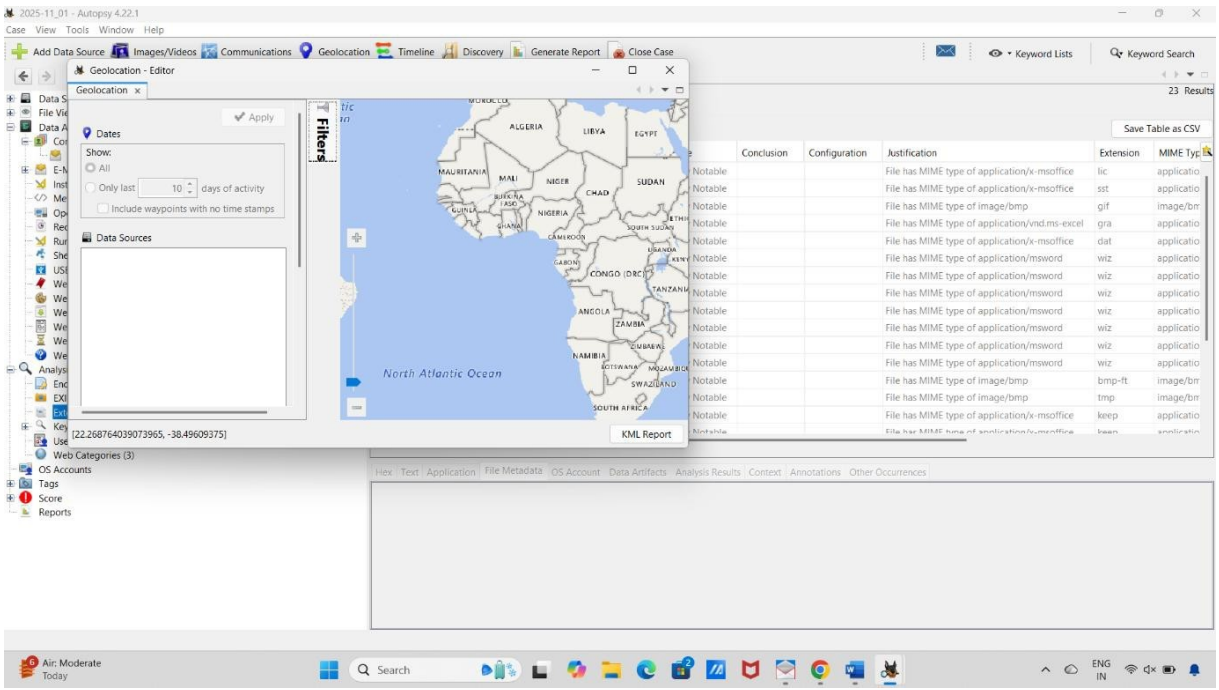
The direct way to look for the communication can be viewed here.



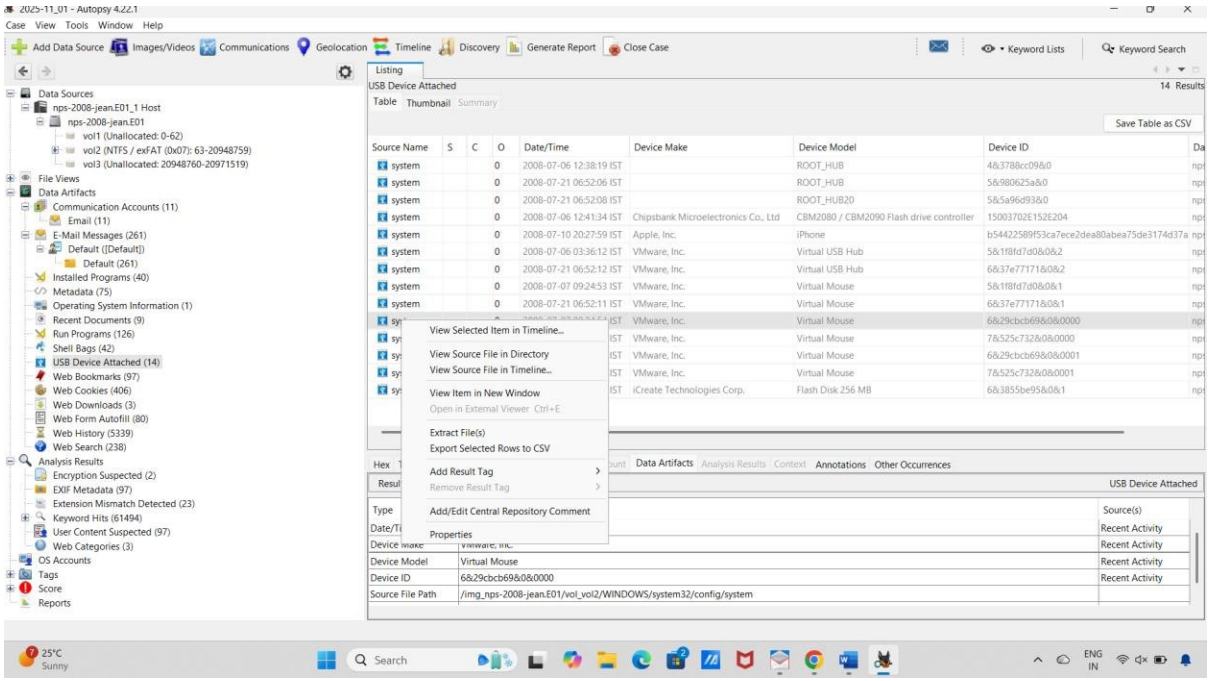
The Graphs can be made to understand the time line.



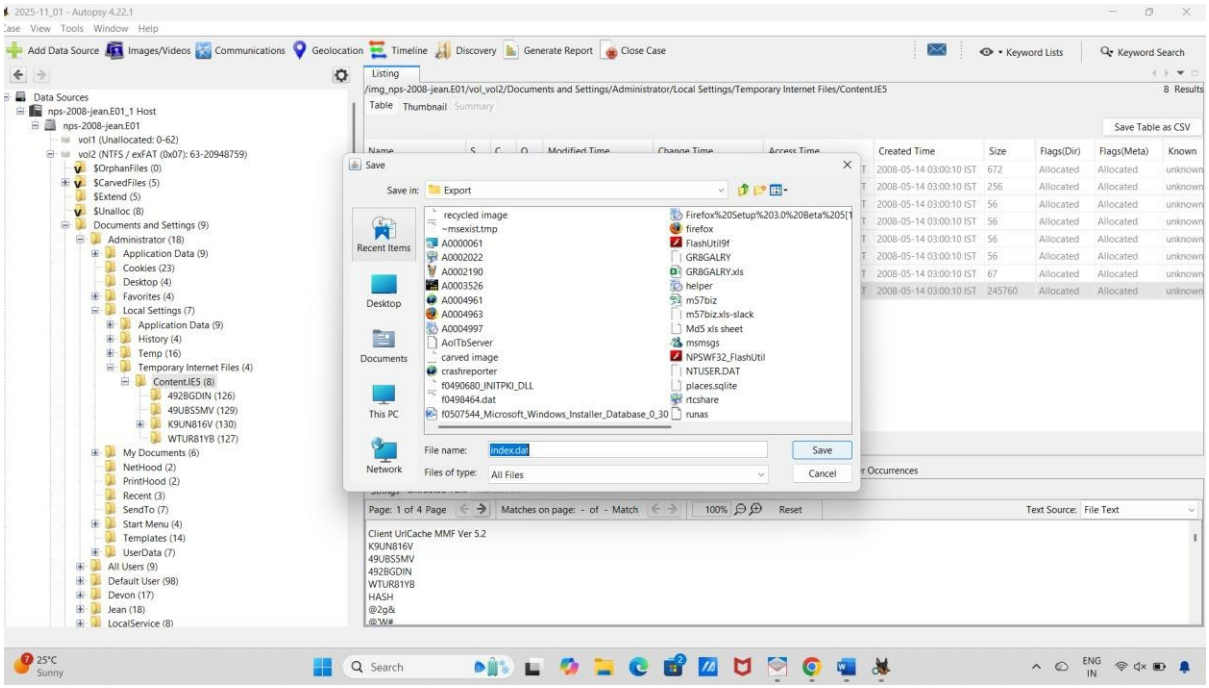
The Geo location can be viewed if necessary.



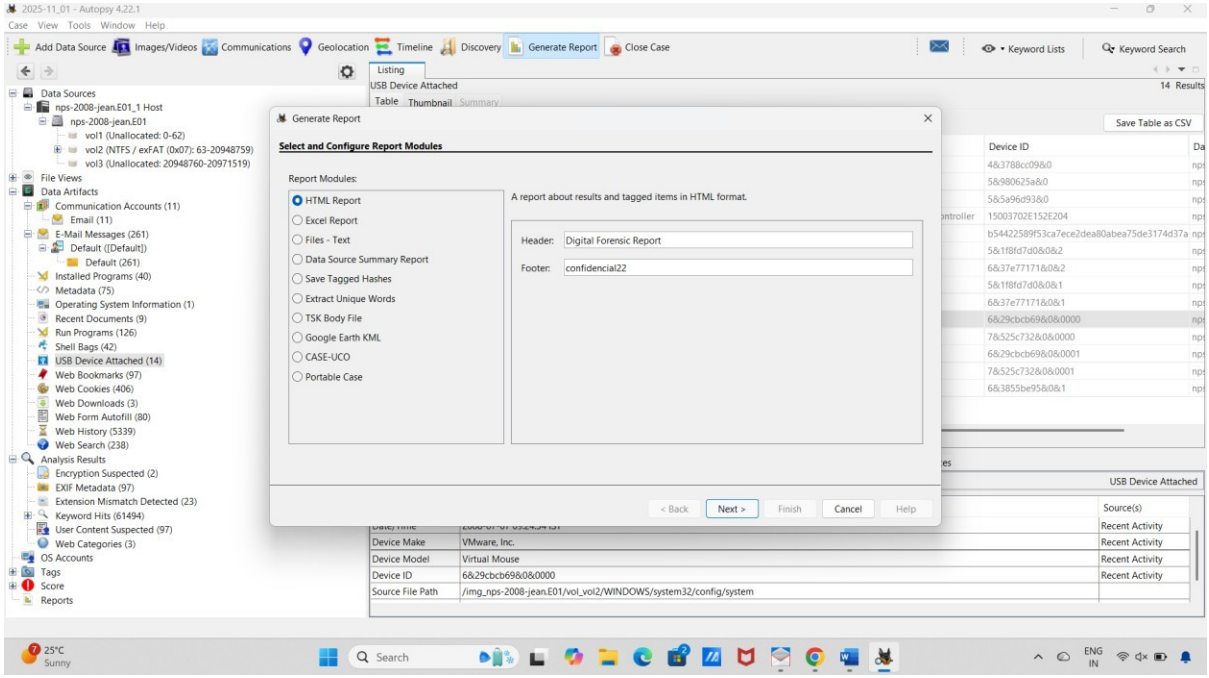
Right click on the file which need to be Extracted. Then click on the extract file option.



Click on Generate Report option then choose the format for Report.



Save the extracted file in on folder for further analysis.



Click on Generate Report option then choose the format for Report.

Experiment 9

Create a Forensic Image (FTK Imager/dd) ,verify integrity (hashes),and recover deleted files via carving

FTK Imager

It is a forensic tool used to create the exact copies of digital storage devices such as USB, Hard drive and memory card without any altering.

It is also used for file recovery (including deleted files), and viewing of file systems, ensuring data integrity through hashing for legal purposes. It's crucial for preserving evidence in corporate security, eDiscovery, and criminal investigations.

Installation on Windows Step 1: Go to the website

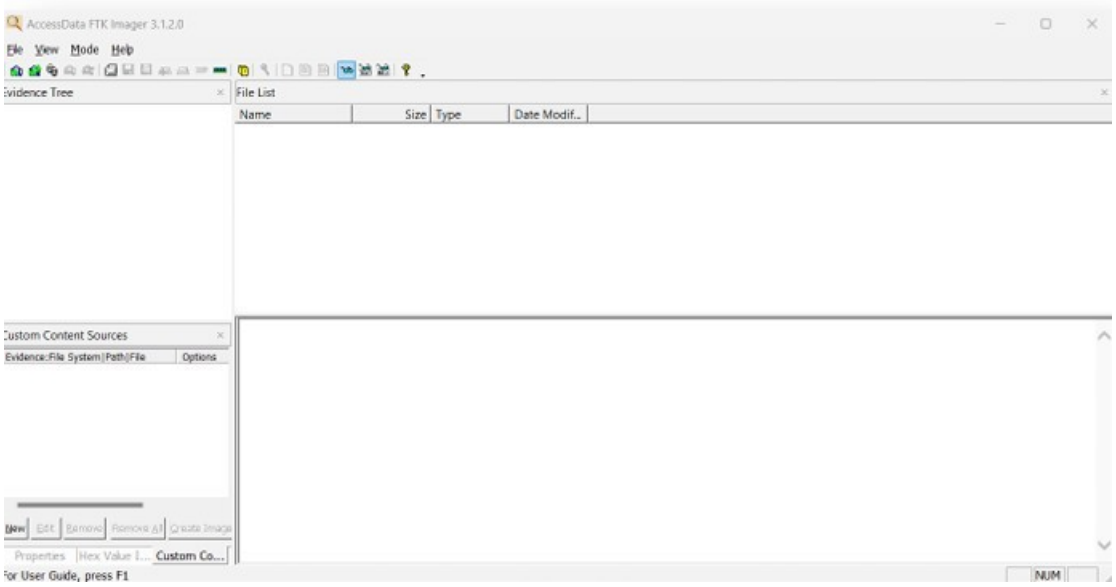
https://accessdata-ftk-imager.software.informer.com/

and click Download.. Now go to the file location and run the application.

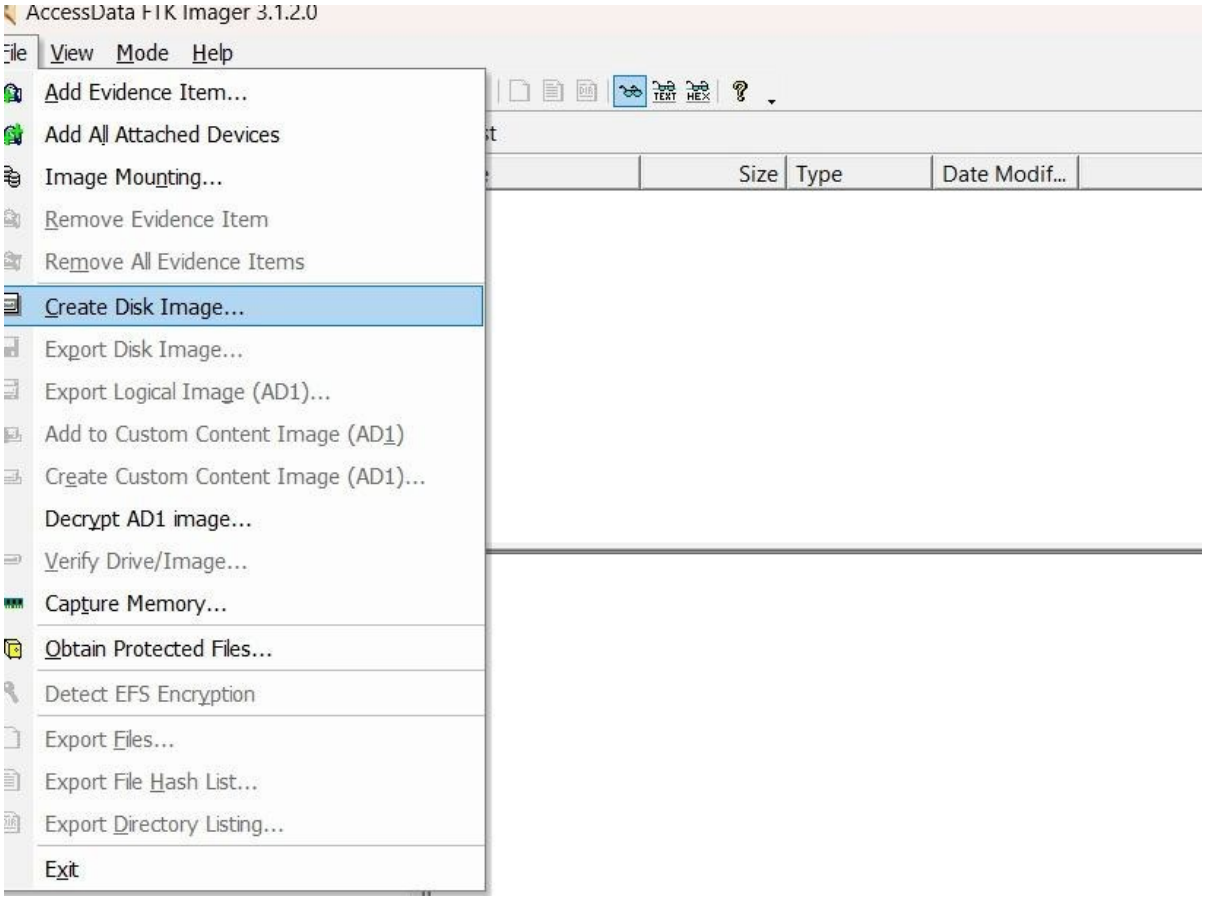
Step 2: Click on the next button.

Step 3: Click on install.

Step 4: Click on finish and Open the AccessData FTK Imager.

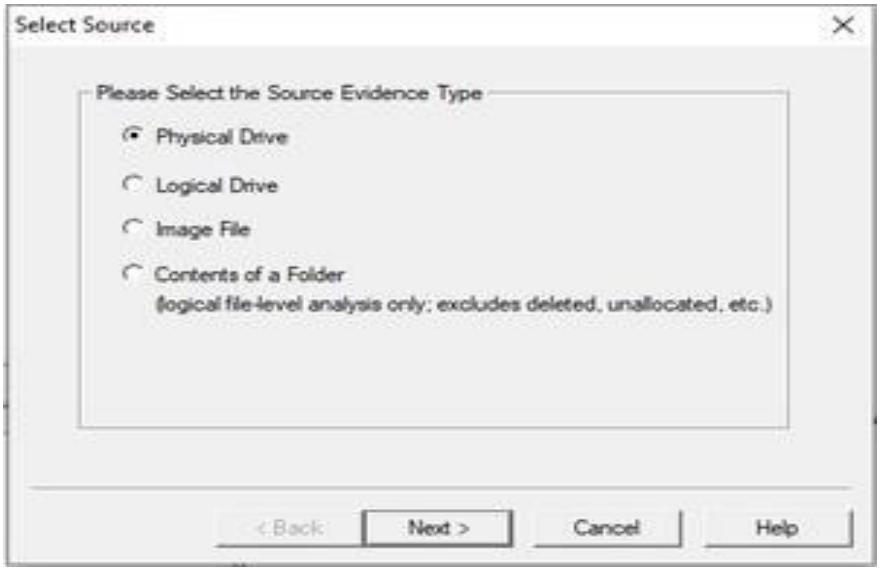


Step 5: In the menu navigation bar, you need to click on the File tab which will give you a drop-down, like given in the image below, just click on the first one that says, Add Evidence Item.



Step 6: After that, there will be a pop-up window that will ask you to *Select the Source of the Evidence.* If you have connected a physical hard drive to the laptop/computer you are using to make

the forensic image, then you will select the *Physical Drive* here. Click on Next. Now, Select the Physical Drive that you would like to use. Please make sure that you are selecting the right drive, or you will waste your time exporting a forensic image of your own OS drive.



- Click the Add button for the Image Destination.
- Select the Type of Forensic Image you would like to export.
- After that, you will have to enter information regarding the case now. You can either leave them blank or keep it general, this part is totally upon you.
- Next, you will need to *Choose the Destination* that you would like to export the forensic image and N*ame the Image.*

Lastly, you will need to wait for the Forensic Image to be created and then verified. The speed of creating the forensic image will vary based on your hardware. Once both have occurred, you have your forensic images ready.

Experiment 10

Apply the IR lifecycle to a simulated incident (ransomware or data exfiltration), produce timeline, containment steps and incident report

1. Basic Information

   Incident Title:

   Incident ID / Case Number:

   Date & Time Reported:

   Date & Time Detected:

   Reported By (Name/Department):

   Incident Handler/Responder:

   Severity Level: (Low / Medium / High / Critical)

2. Brief Description

   A short summary of what happened, how it was detected, and which systems/users were affected.

3. Timeline of Event

4. Affected Assets

List all affected:

   a. Devices / Systems

   b. User accounts

   c. Applications

d. Network segments

e. Data types (PII, credentials, financial data)

5. Evidence Collected
    a. Logs (system, application, network logs)
    b. Disk images / memory captures
    c. Screenshots
    d. Network captures (pcap files)
    e. Artifacts (malware samples, suspicious files)

(Include hash values and chain of custody if needed.)

6. Actions Taken
    a. Containment:
    b. Eradication:
    c. Recovery:

7. Impact Assessment
    a. Data loss or corruption
    b. Operational impact
    c. Financial loss (if known)
    d. Legal/regulatory implications
    e. Reputation risk

8. Recommendations
    a. Security improvements
    b. Policy updates
    c. Awareness training
    d. Patch management suggestions
    e. Additional monitoring tools

9. Conclusion
    a. A concise summary confirming:
    b. Whether the threat is fully removed
    c. Current system status
    d. Risk of recurrence
    e. Overall lessons learned

Example:

A web server receives a huge number of fake requests from a single IP address. Because of the overload, the web server becomes slow and stops responding to real users. Legitimate customers cannot access the website until the attack traffic is blocked.

Type: Flooding attack

Method: Sending continuous HTTP requests Impact:

Website goes offline for 30 minutes

INCIDENT RESPONSE REPORT – DoS Attack

1. Incident Details

- Incident Title: DoS Attack on Company Web Server
- Incident ID: IR-2025-DOSEX01
- Date & Time Detected: 08 December 2025, 14:10 hrs
- Reported By: Network Monitoring System (NMS)
- Handled By: Cybersecurity Incident Response Team (CIRT)
- Severity: High

2. Brief Description of Incident

On 08 December 2025, the company's main web server experienced a sudden spike in incoming HTTP GET requests originating from a single suspicious IP address. The requests rapidly

increased to several thousand per minute, overwhelming the server's processing capacity.

As a result, the website became slow, then unresponsive to legitimate users. This was identified as a Denial of Service (DoS) flooding attack.

3. Timeline of Event

Time	Event
14:10	NMS alerts unusual HTTP traffic spike
14:12	Server response time increases drastically
14:15	Website becomes unavailable for real users
14:18	CIRT begins investigation
14:20	Traffic traced to a single IP (203.184.22.91)
14:22	Temporary firewall block placed on attacking IP
14:25	Traffic reduces, server stabilizes
14:35	Services fully restored
15:00	Post-incident analysis initiated

4. Affected Assets

- Web Server: Apache Web Server hosted on Linux
- Services Impacted:
  - Public website
  - Customer login portal
- Users Affected: All website visitors during the attack window

- Data Impact: No data breach detected; only service disruption

5. Evidence Collected

- Apache access logs
- Show repeated GET requests from IP 203.184.22.91
- Firewall logs
- System performance metrics (CPU spike to 98%)
- Screenshot of NMS showing traffic surge
- Network packet capture (pcap file) confirming repeated identical requests

5. Analysis & Findings (Root Cause)

- The attacker performed an HTTP GET Flood DoS attack by repeatedly hitting the website's root page.
- Attack came from a single external IP, not a botnet (so not DDoS).
- No signs of malware or internal compromise.
- The server became overloaded due to:
  - High request rate
  - Limited rate-limiting rules
  - No WAF (Web Application Firewall) in place
- Final Root Cause:

  Server resources were exhausted due to high-volume fake traffic from one IP.

6. Actions Taken

Containment

- Blocked attacking IP using firewall (UFW/iptables)
- Disabled access to server temporarily for troubleshooting
- Enabled emergency rate limiting

Eradication

- Terminated long-waiting connections
- Cleared server cache
- Restarted Apache service to remove stalled processes

Recovery

- Restored normal traffic routes
- Verified service health and load capacity
- Website made live again by 14:35 hrs
- Monitored for additional 2 hours (no further anomalies)

7. Impact Assessment

- Service Downtime: 20 minutes
- Financial Loss: Minimal (short service outage)
- Customer Impact: Users unable to access website temporarily
- Data Integrity: No data loss or unauthorized access
- Reputation Impact: Low,

8. Recommendations

- Implement rate limiting on web server
- Set up Web Application Firewall (WAF)
- Use traffic filtering rules for repeated abnormal requests
- Enable Auto-Block for suspicious IPs
- Improve server capacity and load balancing
- Continuous monitoring using IDS/IPS
- Configure alert thresholds for unusual HTTP request spikes

9. Conclusion

The DoS attack was a single-IP flooding attack that caused temporary service unavailability.The incident was contained, eradicated, and resolved quickly with no data compromise.

Preventive measures are recommended to avoid recurrence and strengthen the organization’s incident readiness.

This laboratory manual presented a structured and comprehensive set of ten experiments designed to strengthen foundational and applied competencies in cybersecurity and digital forensics. Each experiment introduced core theoretical concepts followed by practical, tool-based implementation, enabling learners to bridge the gap between academic knowledge and real-world application.

Through systematic engagement with established security tools and methodologies—such as OSINT frameworks, Nmap scanning techniques, password-cracking utilities, forensic platforms like Autopsy and FTK Imager, Wireshark network analysis, steganography detection, and incident response procedures—students developed essential analytical and technical skills required for modern cybersecurity practice. The exercises provided exposure to threat identification, vulnerability exploitation, evidence acquisition, data recovery, and structured incident handling.

Collectively, these experiments fostered critical thinking, methodological rigor, and a deeper understanding of the cybersecurity landscape. By completing this series, learners are better prepared to assess system vulnerabilities, investigate security events, and implement effective defensive measures. The practical experience gained through this manual contributes significantly to the development of competent, ethically responsible cybersecurity professionals capable of addressing contemporary security challenges.