Practical – 4

Aim :- Implementation of MITM- attack using wireshark / network sniffers.

Wireshark or Ettercap

We'll need a client machine as well whose network traffic we will spoof and sniff to get cleartext submission of passwords from certain vulnerable websites.

Ettercap is GUI based tool built into Kali so need to download and install anything, so let's get started doing a MiTM attack with Ettercap.

Step #1: Start ettercap

Let's view the help file for ettercap by typing;

kali > ettercap -h

```
root@kali:~# ettercap -h

ettercap 0.8.0 copyright 2001-2013 Ettercap Development Team


Usage: ettercap [OPTIONS] [TARGET1] [TARGET2]

TARGET is in the format MAC/IP/PORTs (see the man for further detail)

Sniffing and Attack options:
  -M, --mitm <METHOD:ARGS>    perform a mitm attack
  -o, --only-mitm             don't sniff, only perform the mitm attack
  -b, --broadcast             sniff packets destined to broadcast
  -B, --bridge <IFACE>        use bridged sniff (needs 2 ifaces)
  -p, --nopromisc             do not put the iface in promisc mode
  -S, --nosslmitm             do not forge SSL certificates
  -u, --unoffensive           do not forward packets
  -r, --read <file>           read data from pcapfile <file>
  -f, --pcapfilter <string>   set the pcap filter <string>
  -R, --reversed              use reversed TARGET matching
  -t, --proto <proto>         sniff only this proto (default is all)
      --certificate <file>    certificate file to use for SSL MiTM
      --private-key <file>    private key file to use for SSL MiTM

User Interface Type:
  -T, --text                  use text only GUI
      -q, --quiet                 do not display packet contents
      -s, --script <CMD>          issue these commands to the GUI
  -C, --curses                use curses GUI
  -D, --daemon                daemonize ettercap (no GUI)
  -G, --gtk                   use GTK+ GUI
```

As you can see, ettercap has a significant help file for running it from a command line, but the only thing we need from here is the switch to run it in graphical mode. In the bottom line of the screenshot (not the bottom line of the actual help file as I have truncated it in the interest of space), you can see the -G switch. This after the command ettercap will launch the ettercap GUI.

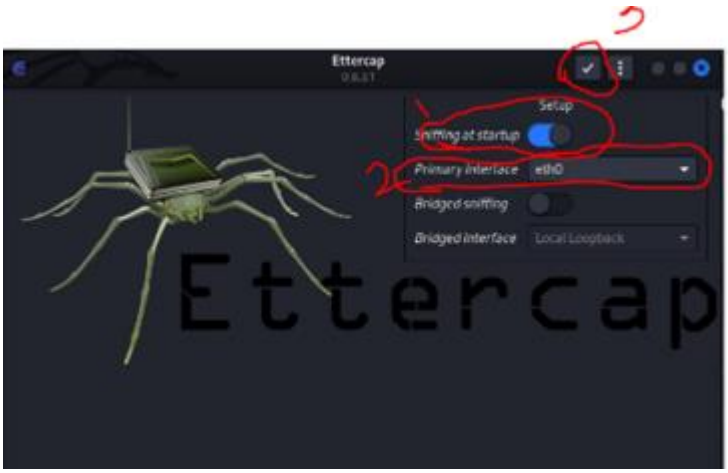
kali > ettercap -G

When we do, the ettercap GUI will start as seen below.

The first step in launching our MiTM attach is to start sniffing. Go to pulldown menu that says "Sniff" and click on "Sniffing at startup".

When we do that, it asking us what interface we want to use and defaults to eth0.

Then click on TICK mark

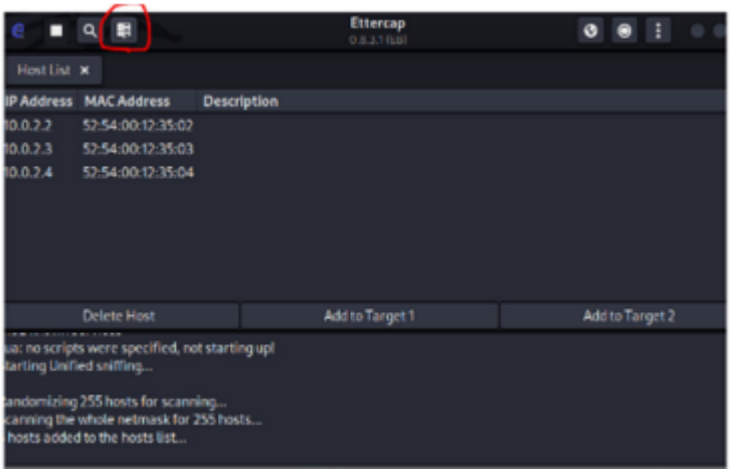


When we click "OK", ettercap launches it sniffing and loads its plugins.

Our next step to find the hosts on the network.

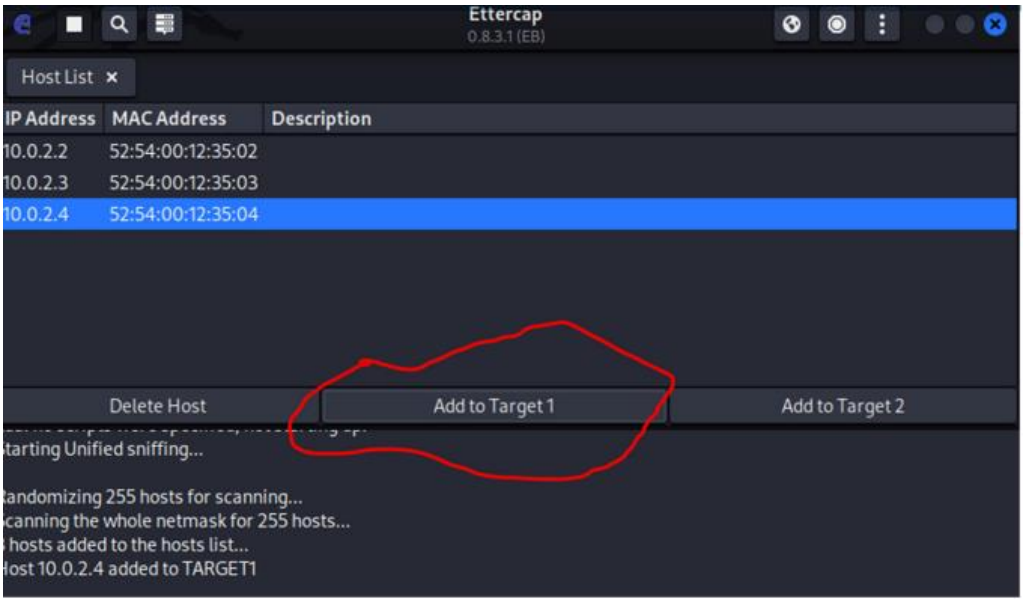
Click on the "Hosts" tab and you will see a menu that includes "Scan for Hosts". Click on it and ettercap will begin scanning the network for hosts.

Now, using that same "Hosts" tab, click on "Hosts List". This will display all the hosts that ettercap has discovered on your network as seen in the screenshot below.

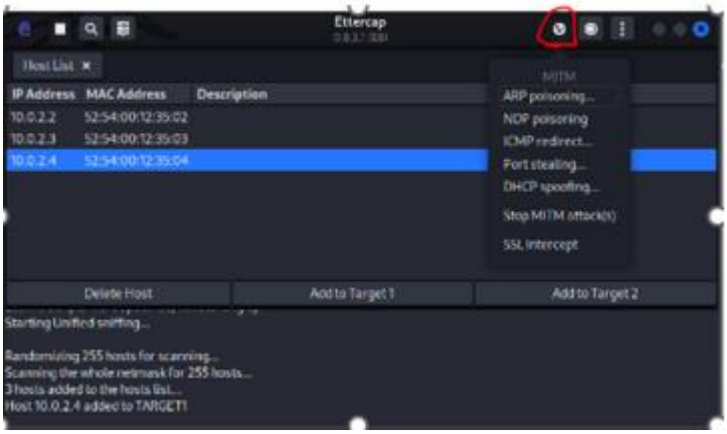


Now, select one of the hosts that will be the target of this attack in the window by clicking on it and then click on "Add to Target 1" at the bottom of the window. When you do so, ettercap will add that host as the first target in our MiTM attack as seen in the screenshot below.

Next, select the second host in this attack and then click "Add to Target 2".

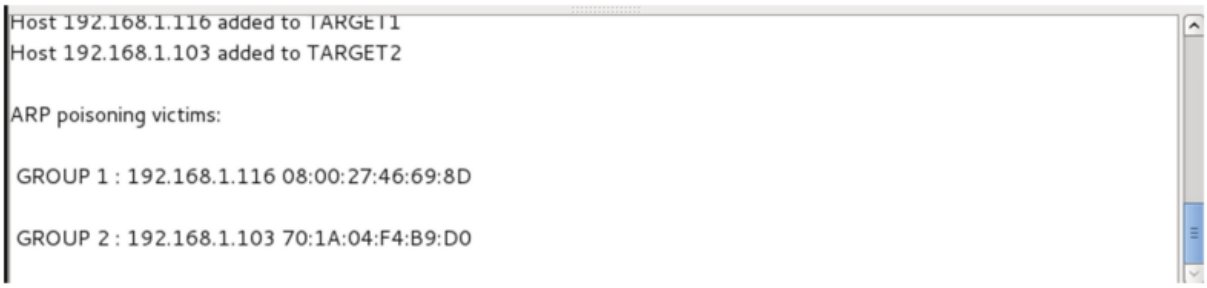


Finally, go to the menu above and click on MITM tab and the drop down menu will have a selection called "ARP Poisoning" as seen in the screenshot below.



Select it and it will open a pop window like below. Select "Sniff remote connections". When we press OK, ettercap will begin ARP poisoning and you will see ettercap respond in its main windows with the message below.

Now, we have successfully placed ourselves between the two targets systems and all their traffic must flow through us. This is where the fun begins as we can now delete, manipulate, impersonate and view all their traffic.



NOW open any browser on target IP address system and open any HTTP websites of LOGIN PAGE type your id and password then it will show output in ettercap output panel.

WIRESHARK:-

A basic setup is complete and victim network traffic will now pass through the attacker machine. To listen to these packets, we will use Wireshark (To know about the basics of Wireshark, read our article here)

- Open up a new terminal and type wireshark. Go to the interface which is capturing all the data flow (here eth0) and start the capture.

- Filter out packets according to what you are looking for. For the purpose of this demo, the user is logging in to a vulnerable website DVWA which uses HTTP instead of the secure version HTTPS. Filter protocol as http and search for required data. Disclaimer: This tutorial is purely intended for educational purposes and should not be misused.

- Right click on the packet and follow TCP stream to open up the data contained within. We can clearly obtain the login credentials of the user, that is the username and password.

MITM is one of the classic hacks and on a LAN connection, ARP spoofing is much preferred. Today there have been various measures to prevent such an attack by use of HTTPS, use of VPN and, strong WEP/WAP encryption on access points.

Practical – 10

Aim :- Implementation of Cyber Forensicstoolsfor Disk Imaging, Data acquisition, Data extraction and Data Analysis and recovery.

1. **FTK Imager (Data acquisition and Disk Imaging)**

SCOPE:

The Scope of practical acquisition of digital evidence can encompass a wide range of methods and devices. Common areas are: Hard Drives, USB, Mobile Devices, Network Forensics, Live system etc.

REQUIREMENTS:

The requirements are Hardware and Devices, FTK imager software, Forensics workstations, sample data, Documentation Templates etc.

THEORY:

Data Acquisition:

¬ The gathering and recovery of sensitive data during a digital forensic investigation is known as data acquisition and collecting and preserving electronic evidence from various sources.

¬ Digital forensic analysts need to know how to access, recover, and restore that data as well as how to protect it for future management. This involves producinga forensic image from digital devices and other computer technologies.

¬ The data acquisition process involves several steps: Identification, Preservation, collection, Verification, Documentation.

Disk Imaging:

Disk imaging, also known as forensic imaging or disk cloning, is a crucial process indigital forensics for cybersecurity. It involves creating a bit-for-bit copy or snapshot of an entire storage device, suchas ahard drive, solid-state drive (SSD), or any other media, to preserve its contents for analysis and investigation. The purpose of disk imaging is to obtain an exact replica of the original storage device, including not only the visible files and folders but also the hidden and deleteddata.

Types of Disk Imaging:

¬ Logical Imaging: Logical imaging, also known as file-level imaging or logical acquisition, involves creating an image or snapshot of the logical structure of a storage device, such as a file system or a partition. This type of imaging captures the files and directories stored on the disk, along with their metadata and attributes, without including unallocated space or low-level disk structures.

¬ Physical Imaging: Physical imaging, also known as bit-for-bit imaging or sectorlevel imaging, is a comprehensive process that involves creating an exact copyof the entire storage device, including all sectors, regardless of whether they are allocated or unallocated. This type of imaging captures not

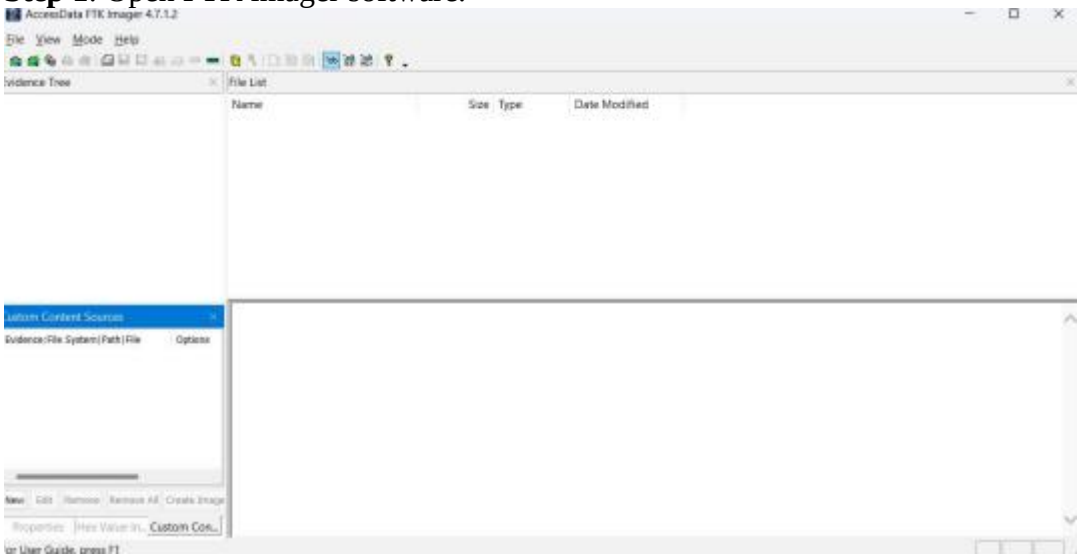
only the visible files and folders but also the hidden data, deleted files, slack space, and all other datapresent on the disk.

¬ Forensic Significance of Imaging:

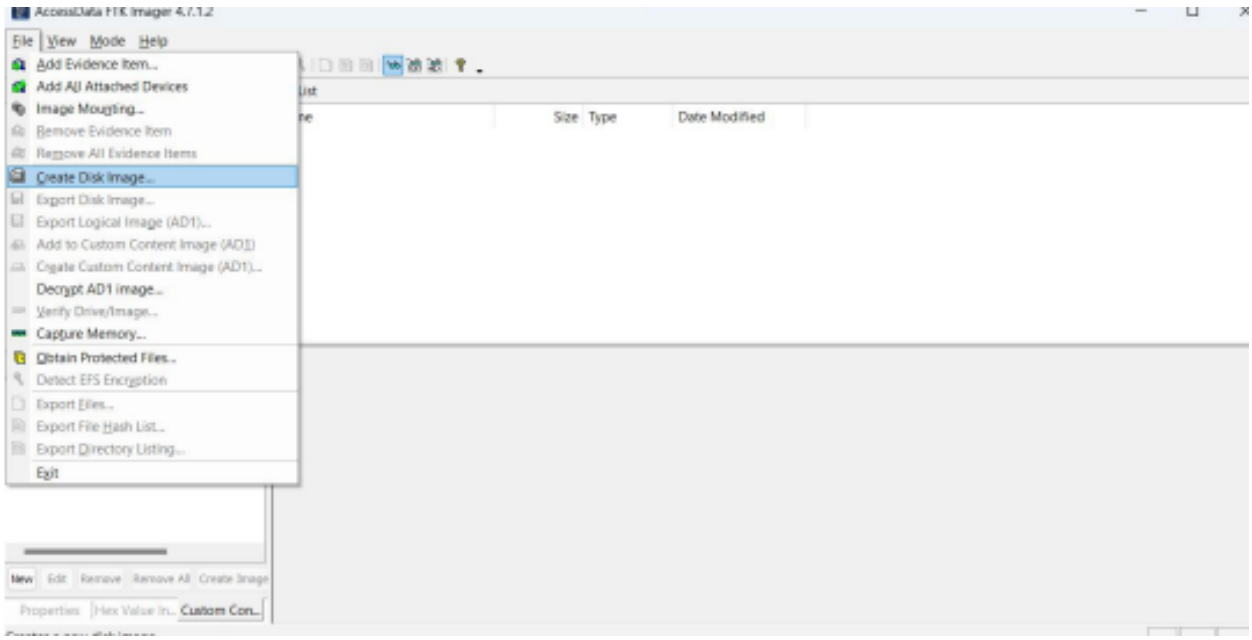
¬ Forensic imaging prevents the loss of original data. These imaging tools and techniques are the only way to ensure that electronic data can be successfullyadmitted as evidence in a court or legal proceeding.

EXAMINATION:

Step 1: Open FTK imager software.

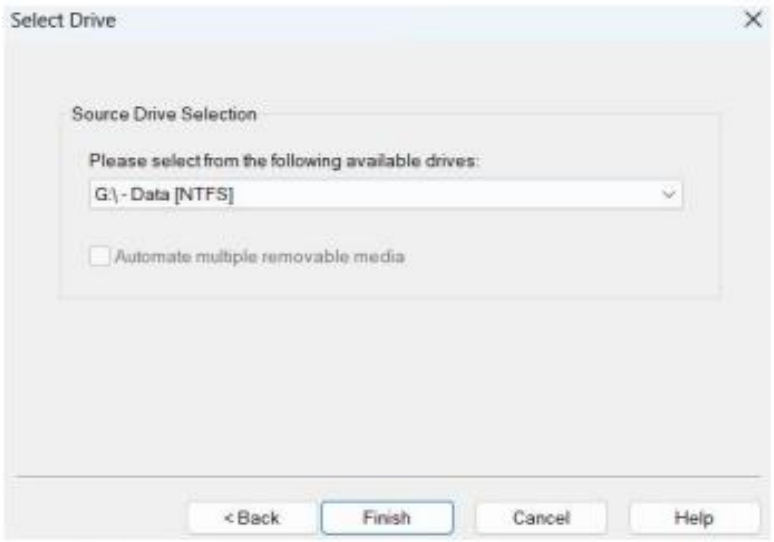


Step 2: Now go to the file option - > choose Create Disk Image

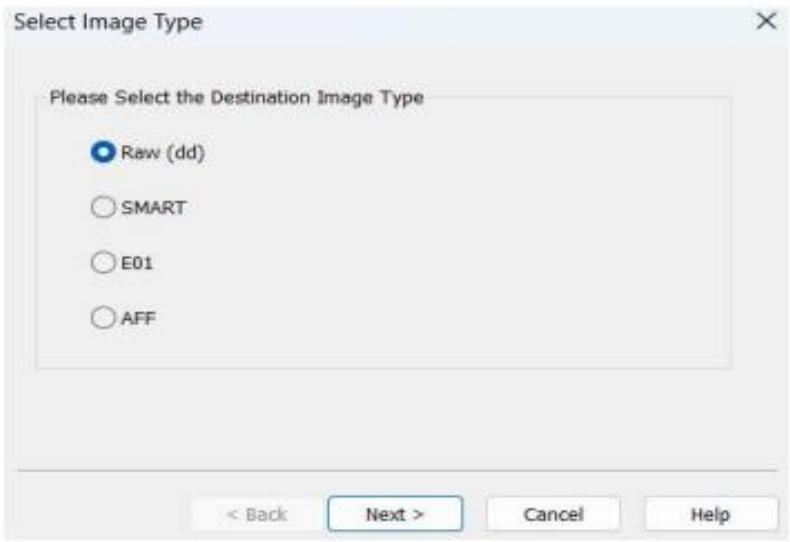


Step 3: After clicking Create Disk image -> select the source of evidence type like Logical Drive, then click next option.

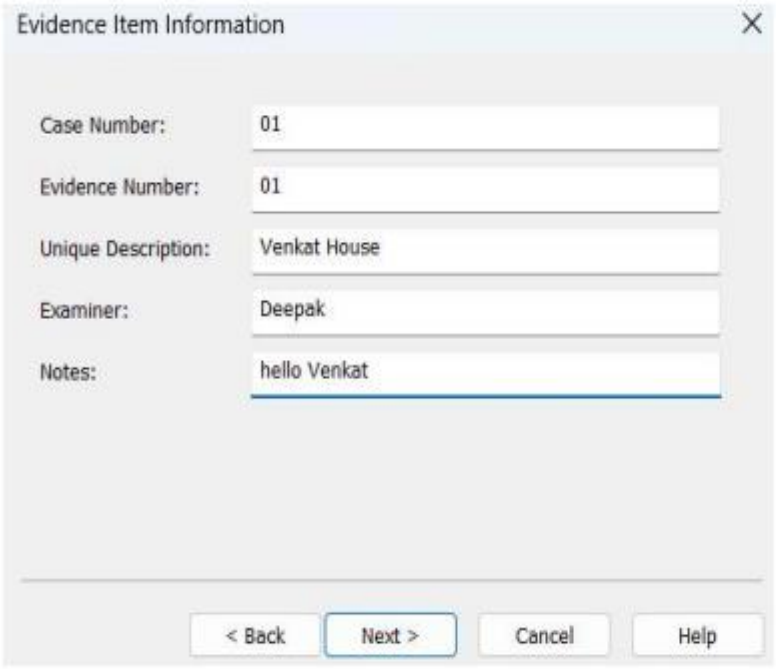
Step 4: Now select source drive path and then press the finish button.



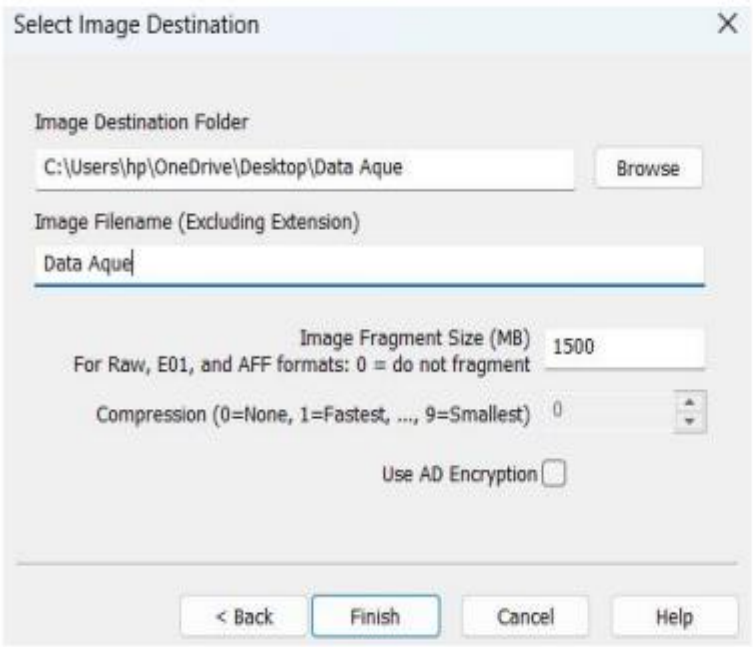
Step 5: Choose destination image type (Raw(dd)) -> Next.



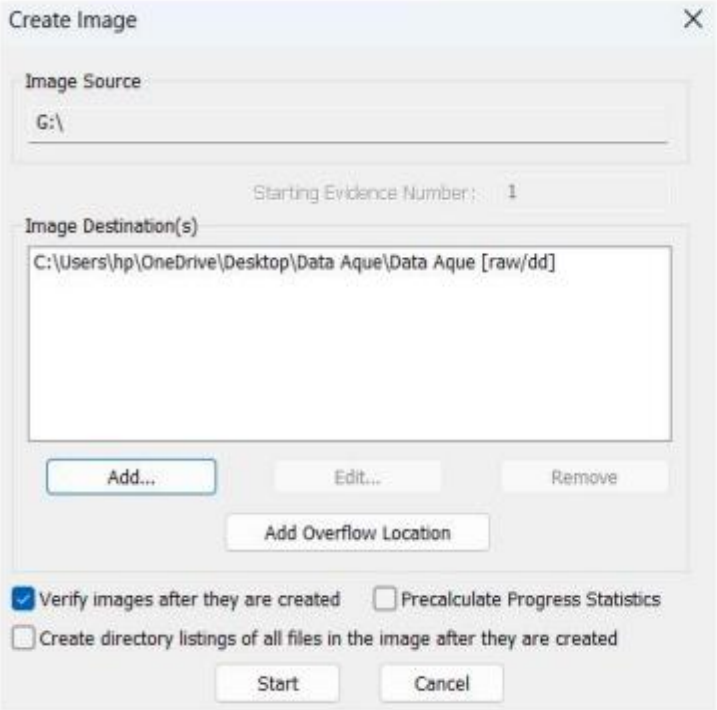
Step 6: Now fill the form of Evidence item information.



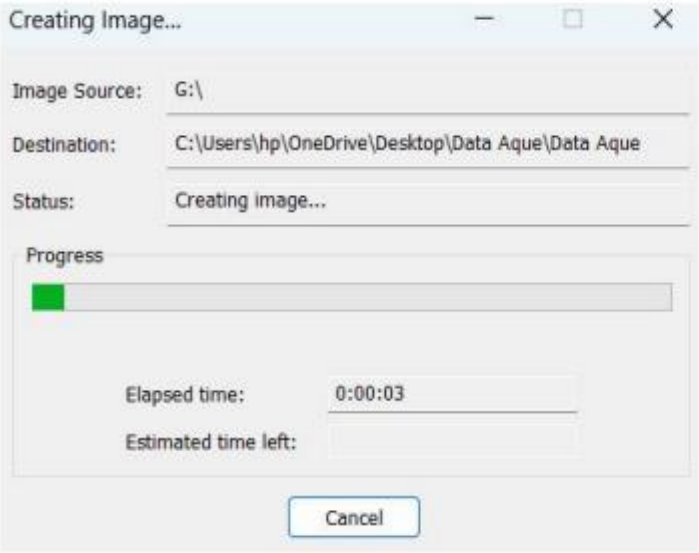
Step 7: After filling the information -> select image destination, enter Image filename and Image fragment size then click the finish button.



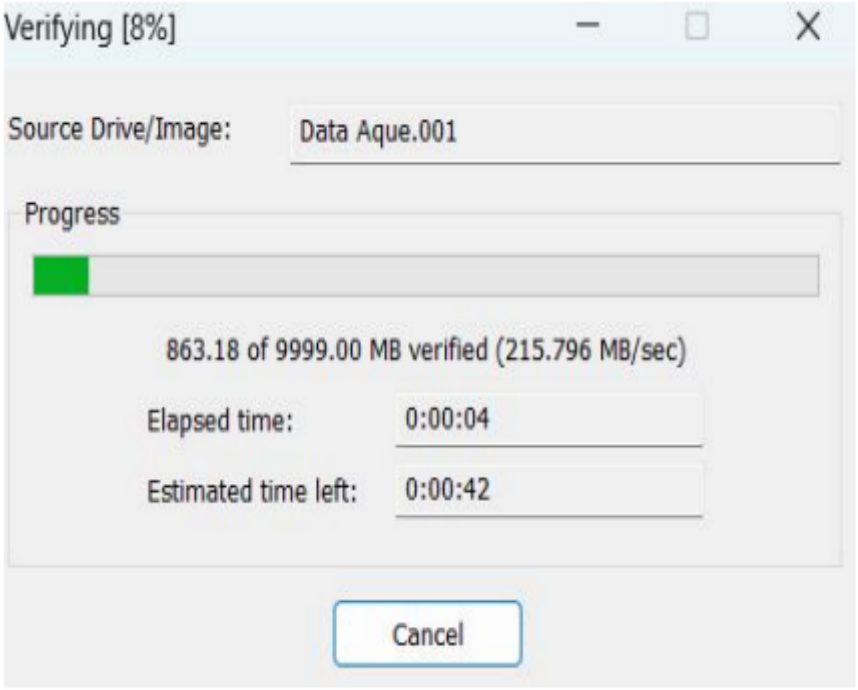
Step 8: After all the processes now, click in the checkbox of verify images after they are created -> start.



Step 9: Progress for creating image.



Step 10: Verifying the source drive/image.



Step 11: Verify result of source drive/image form of hash values.

OBSERVATION:

```
Created By AccessData® FTK® Imager 4.7.1.2

Case Information:
Acquired using: ADI4.7.1.2
Case Number: 01
Evidence Number: 01
Unique description: Venkat House
Examiner: Deepak
Notes: hello Venkat

------------------------------------------------------------

Information for C:\Users\hp\OneDrive\Desktop\Data Aque\Data Aque:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Logical
[Drive Geometry]
 Bytes per Sector: 512
 Sector Count: 20,477,952
[Physical Drive Information]
 Removable drive: False
 Source data size: 9999 MB
 Sector count:    20477952
[Computed Hashes]
 MD5 checksum:    a8b13d1099105de415d7b795374ef1aa
 SHA1 checksum:   b473b690eff93531639142ee301187a8a0947d81

Image Information:
 Acquisition started:   Wed Jun 28 13:00:17 2023
 Acquisition finished:  Wed Jun 28 13:01:01 2023
 Segment list:
  C:\Users\hp\OneDrive\Desktop\Data Aque\Data Aque.001
  C:\Users\hp\OneDrive\Desktop\Data Aque\Data Aque.002
  C:\Users\hp\OneDrive\Desktop\Data Aque\Data Aque.003
  C:\Users\hp\OneDrive\Desktop\Data Aque\Data Aque.004
  C:\Users\hp\OneDrive\Desktop\Data Aque\Data Aque.005
  C:\Users\hp\OneDrive\Desktop\Data Aque\Data Aque.006
  C:\Users\hp\OneDrive\Desktop\Data Aque\Data Aque.007

Image Verification Results:
 Verification started:  Wed Jun 28 13:01:01 2023
 Verification finished: Wed Jun 28 13:01:40 2023
 MD5 checksum:    a8b13d1099105de415d7b795374ef1aa : verified
 SHA1 checksum:   b473b690eff93531639142ee301187a8a0947d81 : verified
```

2. Autopsy (Data Extraction, Data Analysis and Data Recovery)

Z

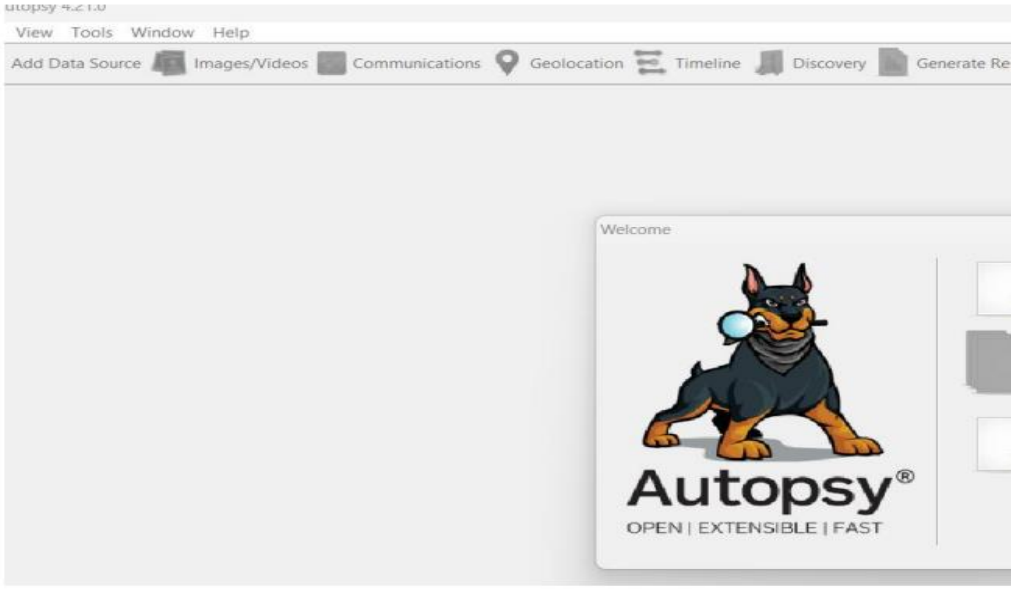
¬ Autopsy is a digital forensics platform and graphical interface to The Sleuth Kit and other digital
¬ forensics tools. It is used by law enforcement, military, and corporate examiners to investigate what
¬ happened on a computer. You can even use it to recover photos fromyour camera's memory card.
¬ Basically, the autopsy is a free open-source tool that supports a wide range of other digital forensics
¬ modules and tools. The tool is largely maintained by Basis Technology Corp. With the assistance of
¬ programmers from the community. The Autopsy is computer software that makes it simpler to deploy
¬ many of the open-source programs and plugins used in The Sleuth Kit.

Features of Autopsy

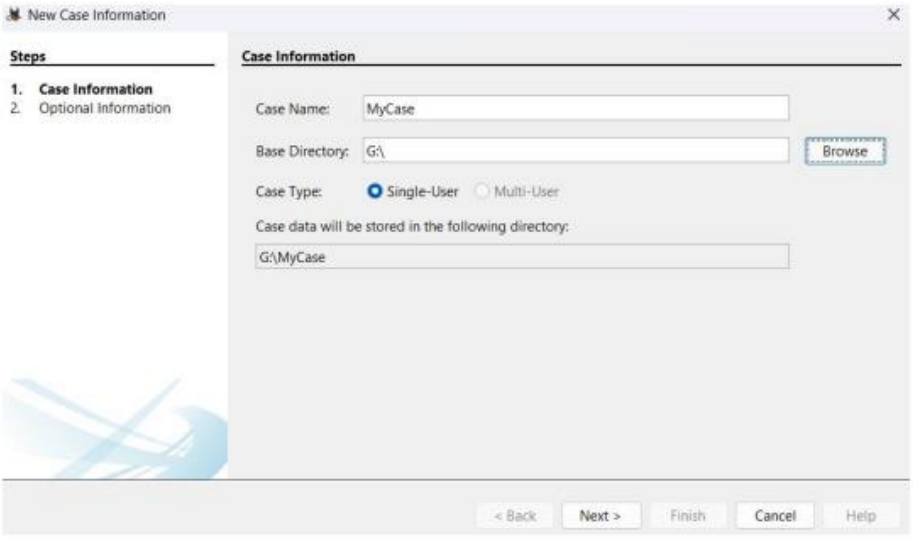
¬ Timeline Analysis:- Displays system events in a graphical interface to help identify activity.
¬ Keyword Search: Text extraction and index searched modules enable you to findfiles that
¬ mention specific terms and find regular expression patterns.
¬ Web Artifacts-: Extracts web activity from common browsers to help identifyuser activity.
¬ Registry Analysis:-Uses Reg Ripper to identify recently accessed documents andUSB devices.
¬ Email Analysis: Parses MBOX format messages, such as Thunderbird.
¬ EXIF: Extracts geo location and camera information from JPEG files.
¬ Robust File System Analysis: Support for common file systems, including NTFS,
¬ FAT12/FAT16/FAT32/ExFAT, HFS+, ISO9660 (CD-ROM), Ext2/Ext3/Ext4, Yaffs2
¬ Unicode Strings Extraction: Extracts strings from unallocated space and unknownfile types in many languages
¬ File Type Detection based on signatures and extension mismatch detection. Interesting Files Module will flag files and folders based on name and path.
¬ Android Support: Extracts data from SMS, call logs, contacts, Tango, Words withFriends, and more.
¬ Multi-User Cases: Collaborate with fellow examiners on large cases.
¬ LNK File Analysis:- Identifies shortcuts and accessed documents

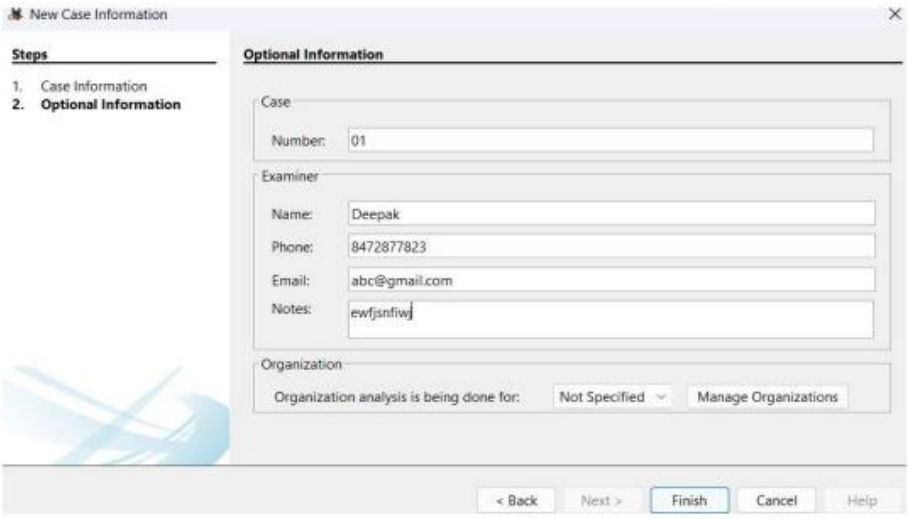
EXAMINATION:

Step 1: Download and setup the installation process of Autopsy tool. Open it.

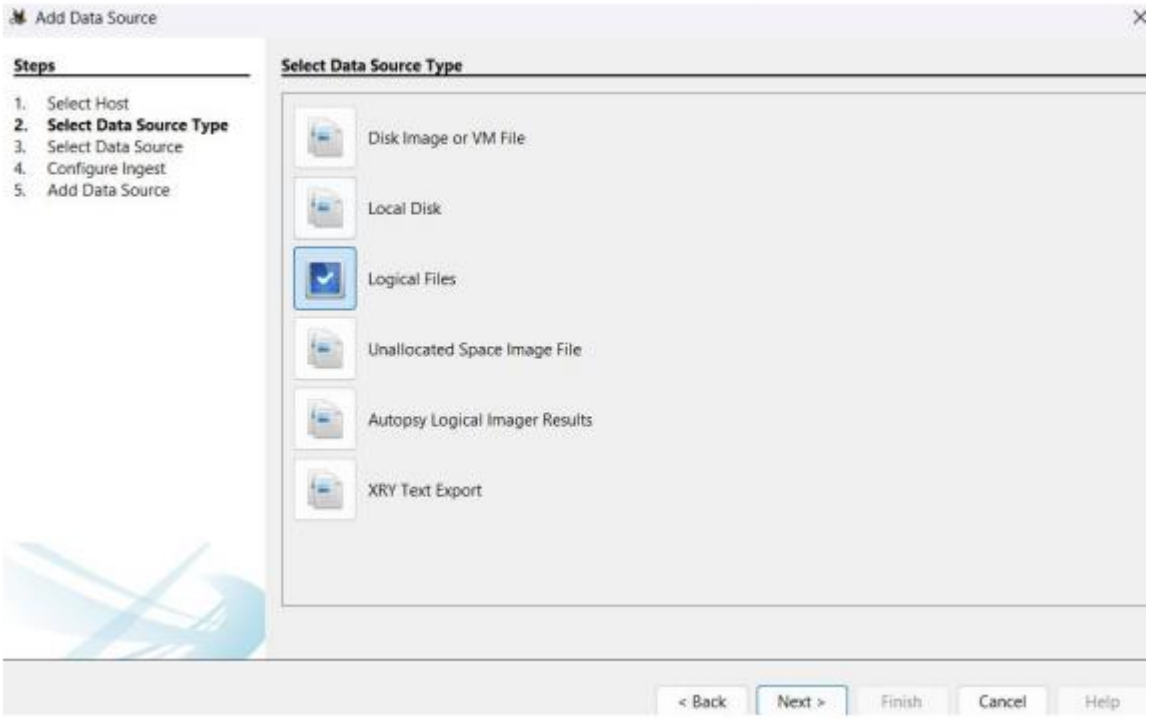


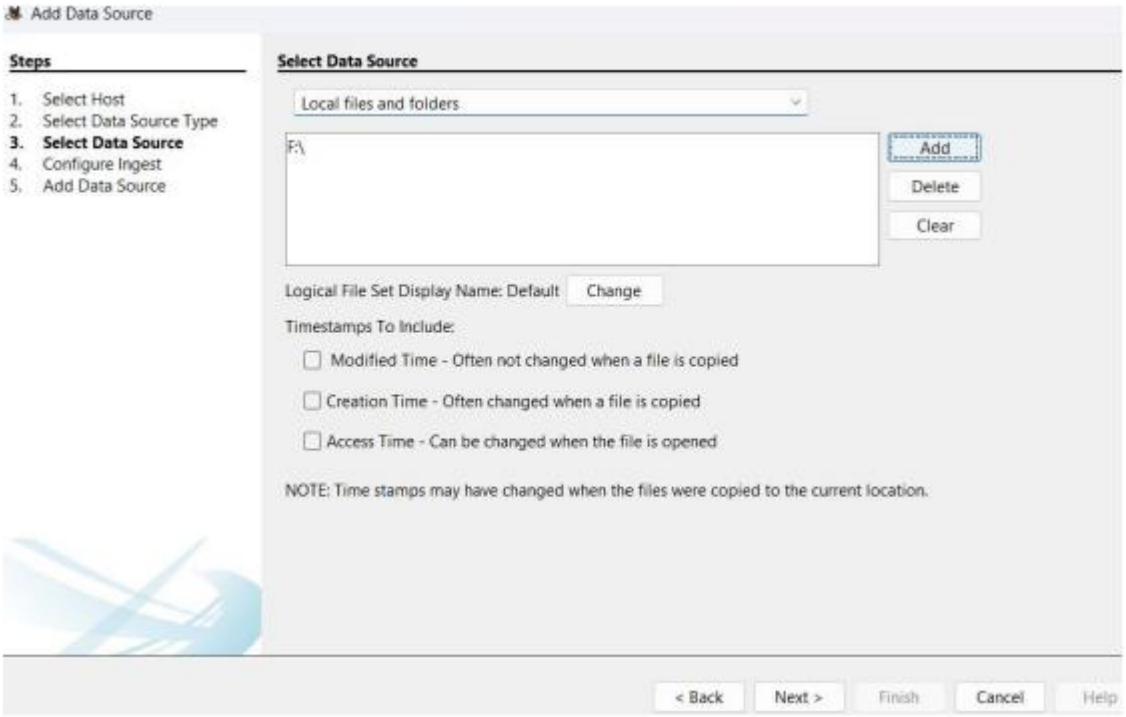
Step 2: Create a case file – Open Autopsy and click New Case > enter a case name and choose a directory.

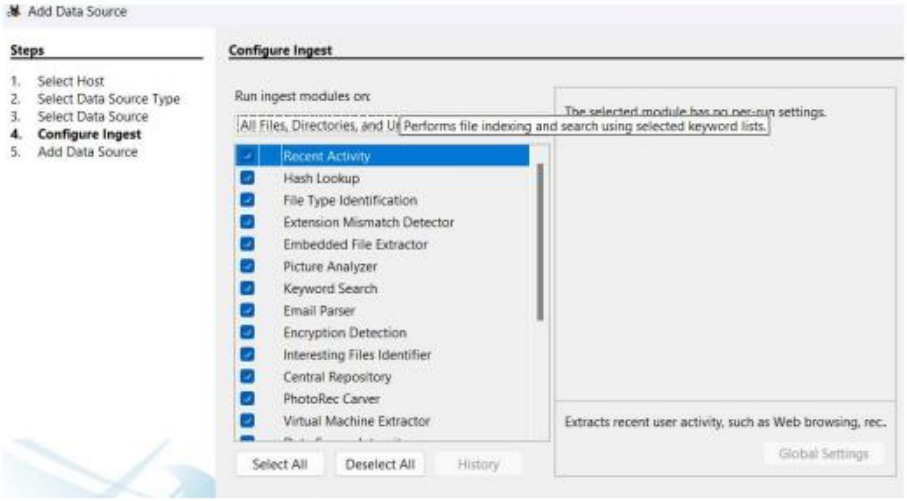




Step 3: Select data source – Now, add the data source windows pops up > select Logical disk from the drop-down list > choose the targeted drive image.

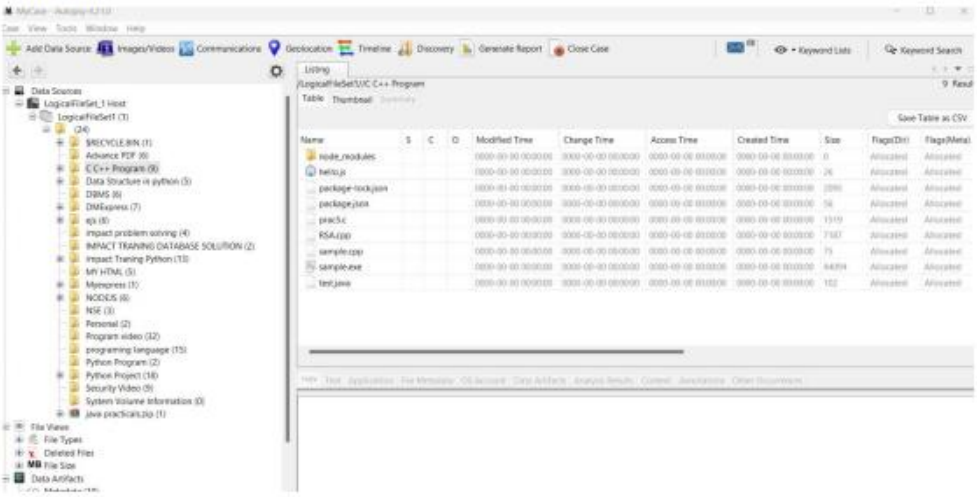

Add Data Source
Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source
Select Data Source Type
Disk Image or VM File
Local Disk
Logical Files
Unallocated Space Image File
Autopsy Logical Imager Results
XRY Text Export
< Back
Next >
Finish
Cancel
Help


Add Data Source
Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source
Select Data Source
Local files and folders
F:\
Add
Delete
Clear
Logical File Set Display Name: Default
Change
Timestamps To Include:
Modified Time - Often not changed when a file is copied
Creation Time - Often changed when a file is copied
Access Time - Can be changed when the file is opened
NOTE: Time stamps may have changed when the files were copied to the current location.
< Back
Next >
Finish
Cancel
Help



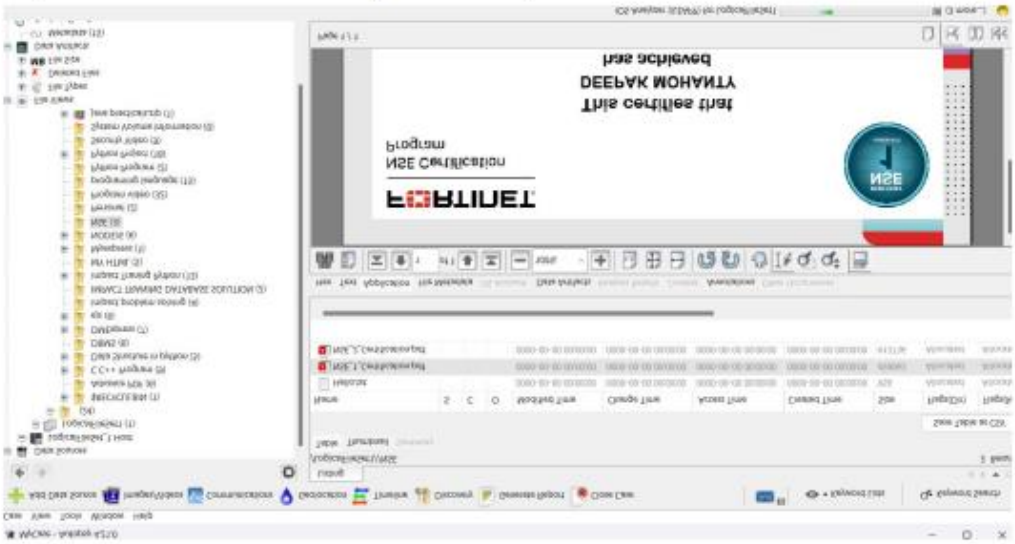
Step 4: Click next to proceed.

Step 5: Wait for the analysis to complete, and the data will be displayed in different categories.



OBSERVATION:

Data Restoration – Open the folder of the files, Right-click on it to restore and select export. Choose a location to export the data , click save.



Practical – 8

Aim :- Implementation of OS hardening and RAM dump analysisto collect the Artifacts and other Information.

RAM dumps

A memory dump is the process of taking all information content in RAM and writing it to a storage drive as a memory dump file (*.RAW format).

Volatile memory, or RAM, is used to store data currently used by a running process: whether it is a user application or a system service. This type of memory is much quicker than a regular hard drive but unlike files permanently stored on a drive (unless deleted), data from RAM may disappear instantly. At the same time, it may store data crucial for your case, including passwords in raw format without encryption or encoding, decrypted data otherwise kept encrypted on a drive, decryption keys for various services, apps and WDE, remote sessions data, chats in social networks, malware code, cryptocurrency transactions, various system info such as loaded registry branches, and so on. This is why it is not argued that capturing RAM contents must be one of the first steps in seizing a running computer or laptop.

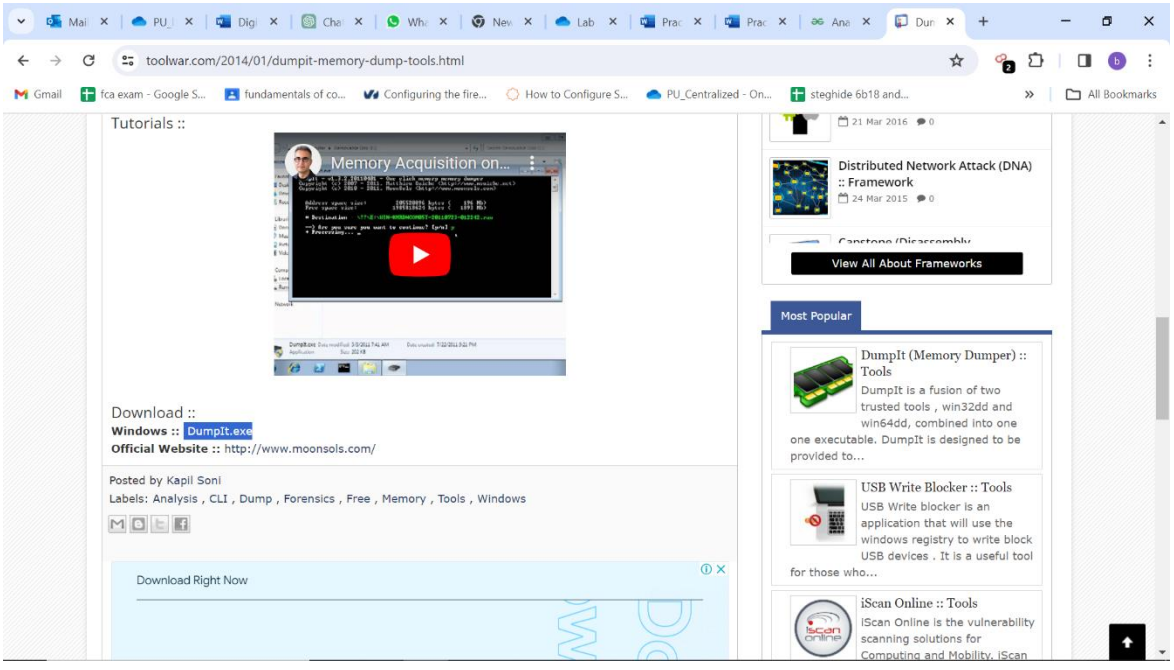
There are various tools that can be used for memory dump. Some of them are:

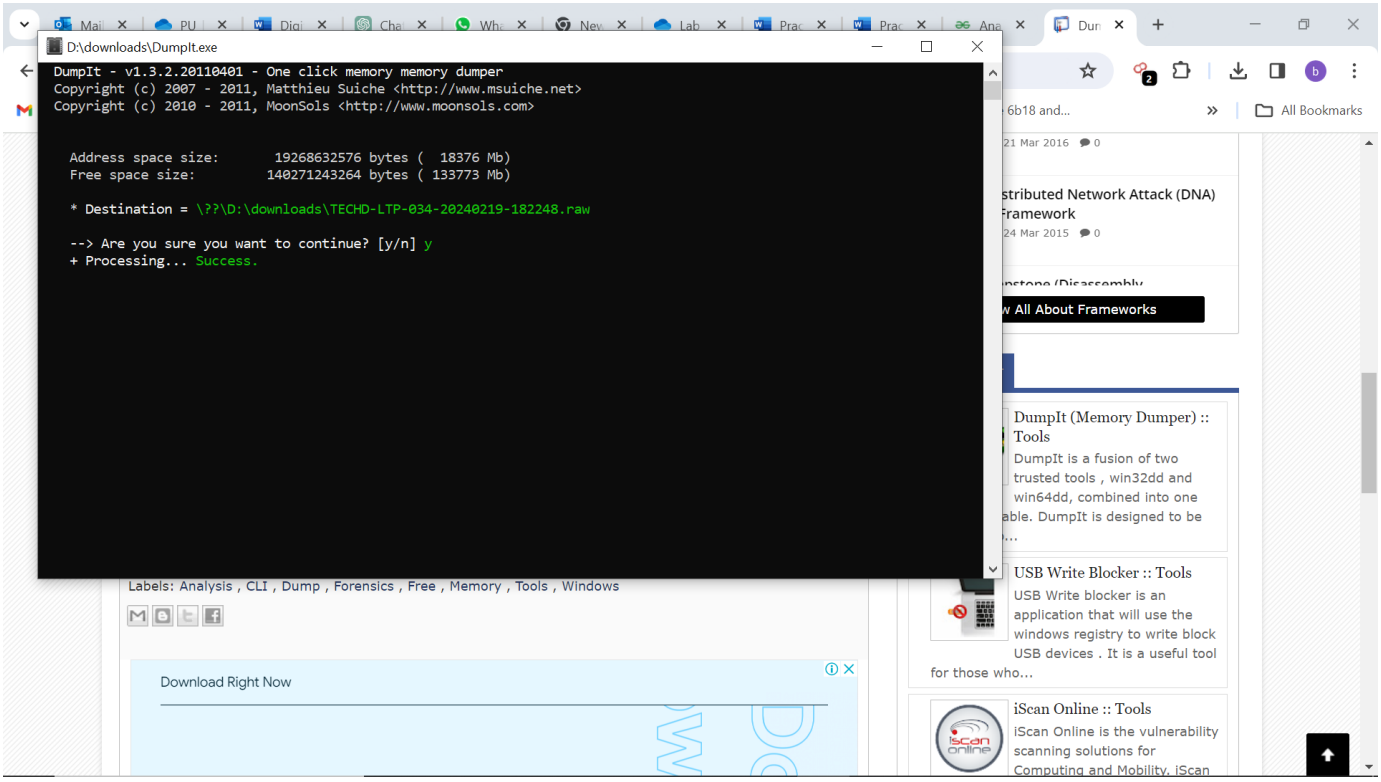
1. Autopsy
2. Dump-IT

Procedure

Creating RAM dump using Dump-IT

1. Download **DumpIT** tool from toolwar website
2. Open Dump-IT.exe





Autopsy performs operations onto disk images which can be created using tools like FTK Imager. Here an already created image is used. You may download Autopsy from here and the disk image used in this article from here.

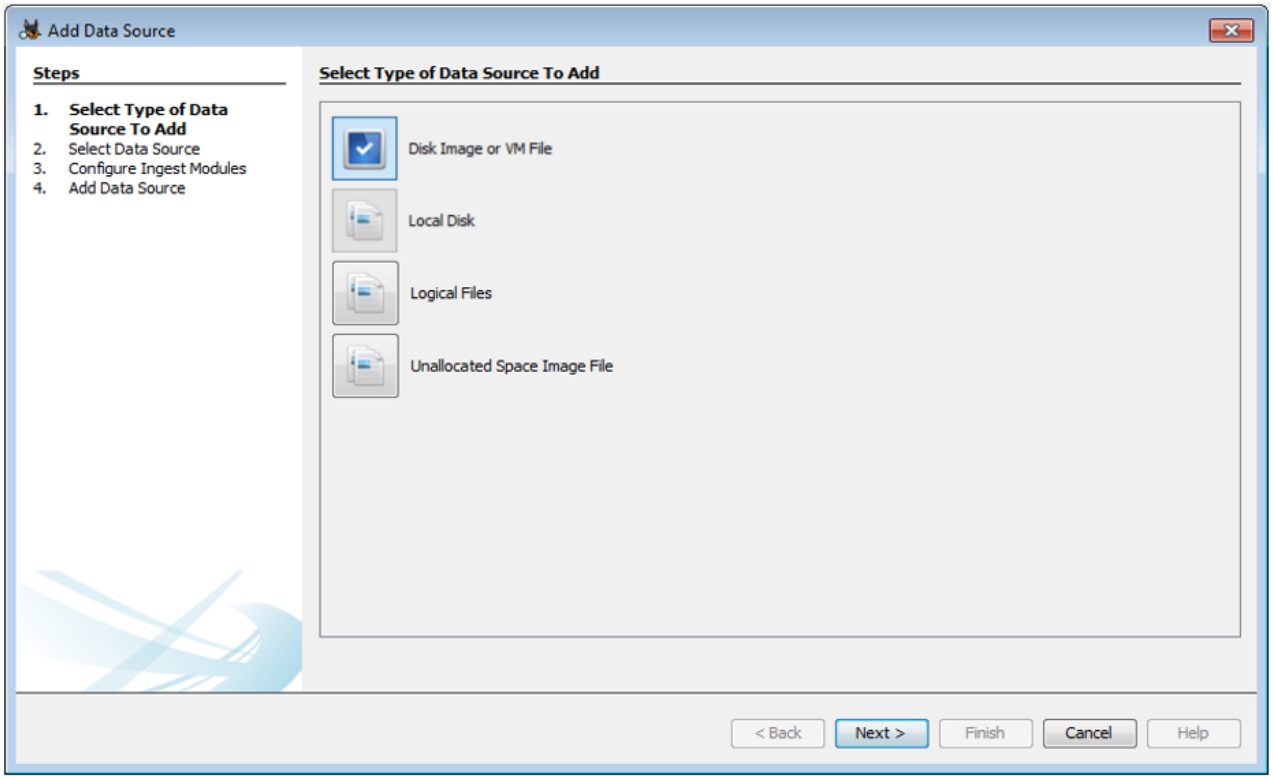
1. Getting Started

Open Autopsy and create a new case

Click on **Finish** after completing both the steps.

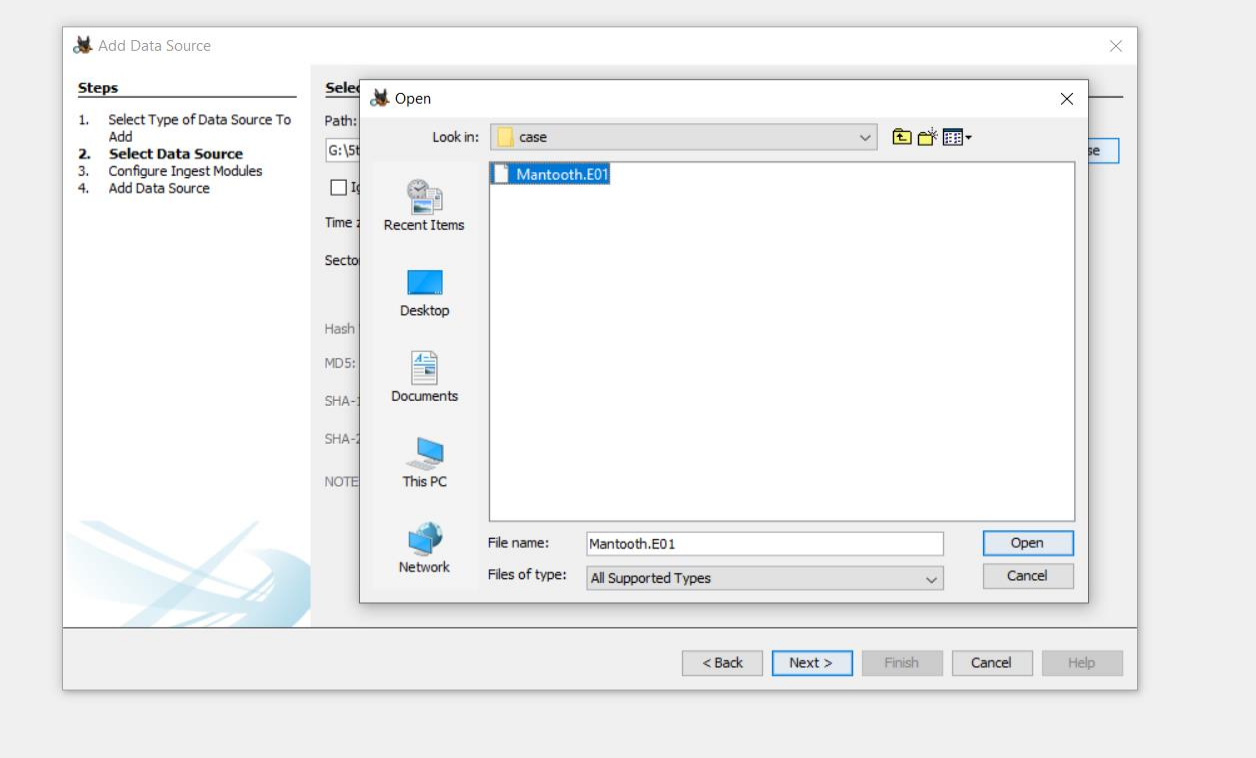
2. Add a data source.

Select the appropriate data source type.

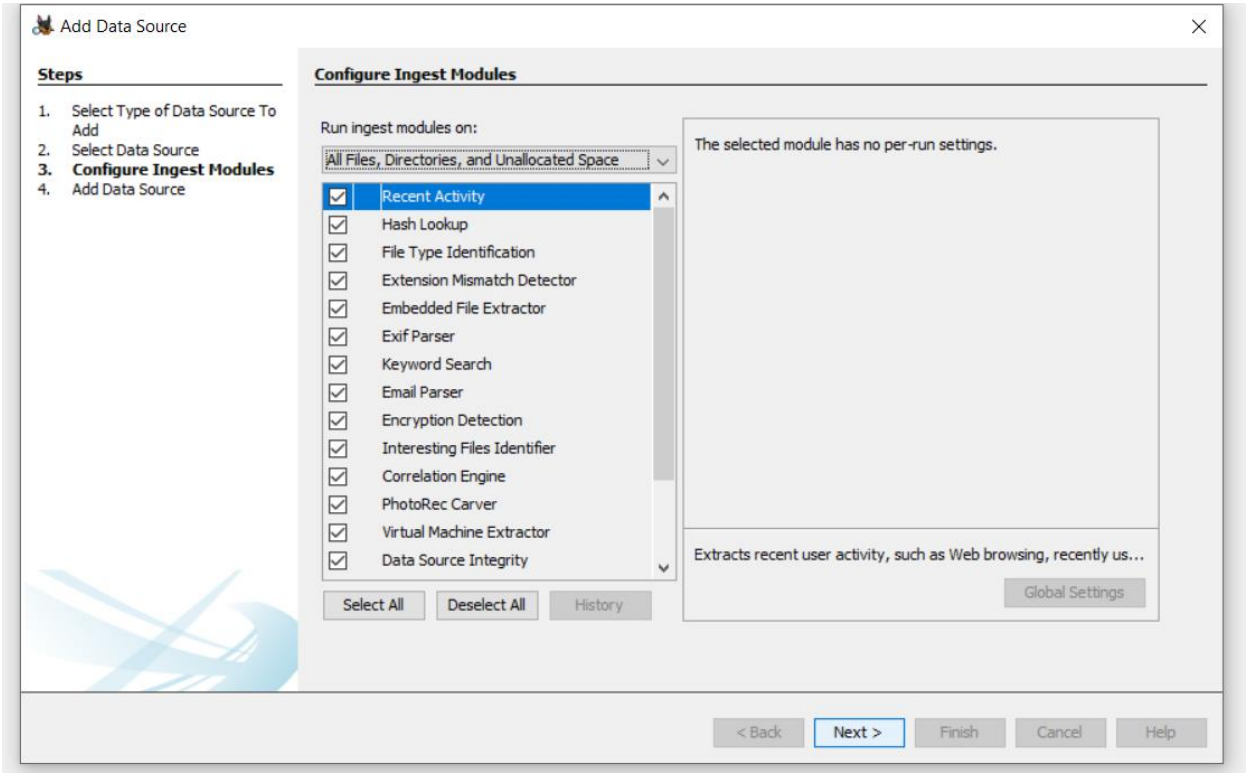


- **Disk Image or VM file:** Includes images that are an exact copy of a hard drive or media card, or a virtual machine image.
- **Local Disk:** Includes Hard disk, Pen drive, memory card, etc.
- Logical Files. : Includes local folders or files.
- **Unallocated Space Image File**: Includes files that do not contain a file system but need to run through ingest.

The data source used here is a disk image. Add the data source destination.



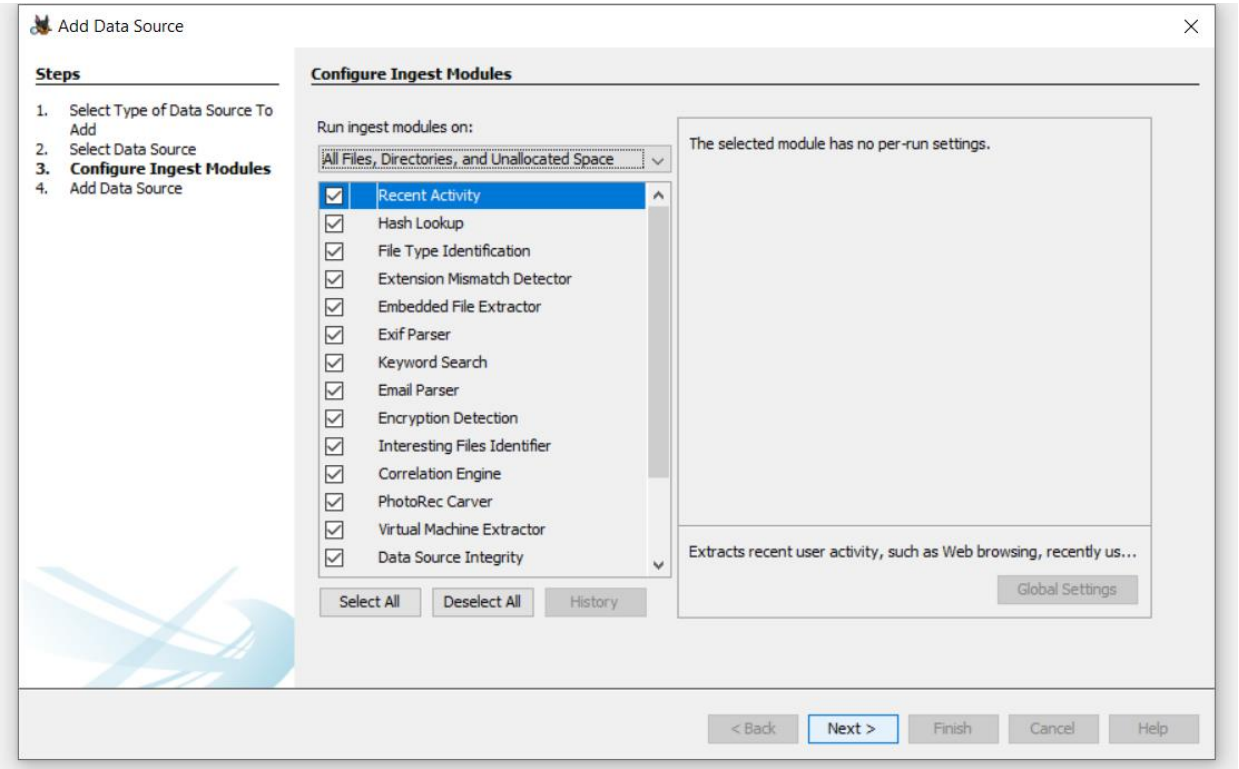
Configure ingest modules.



The ingest modules determine factors for which the data in the data source is to be analyzed. Here is a brief overview of each of them.

- **Recent Activity**: Discover the recent operations performed on the disk, for example, the files that were last viewed.
- **Hash Lookup**: Identify files using hash values.

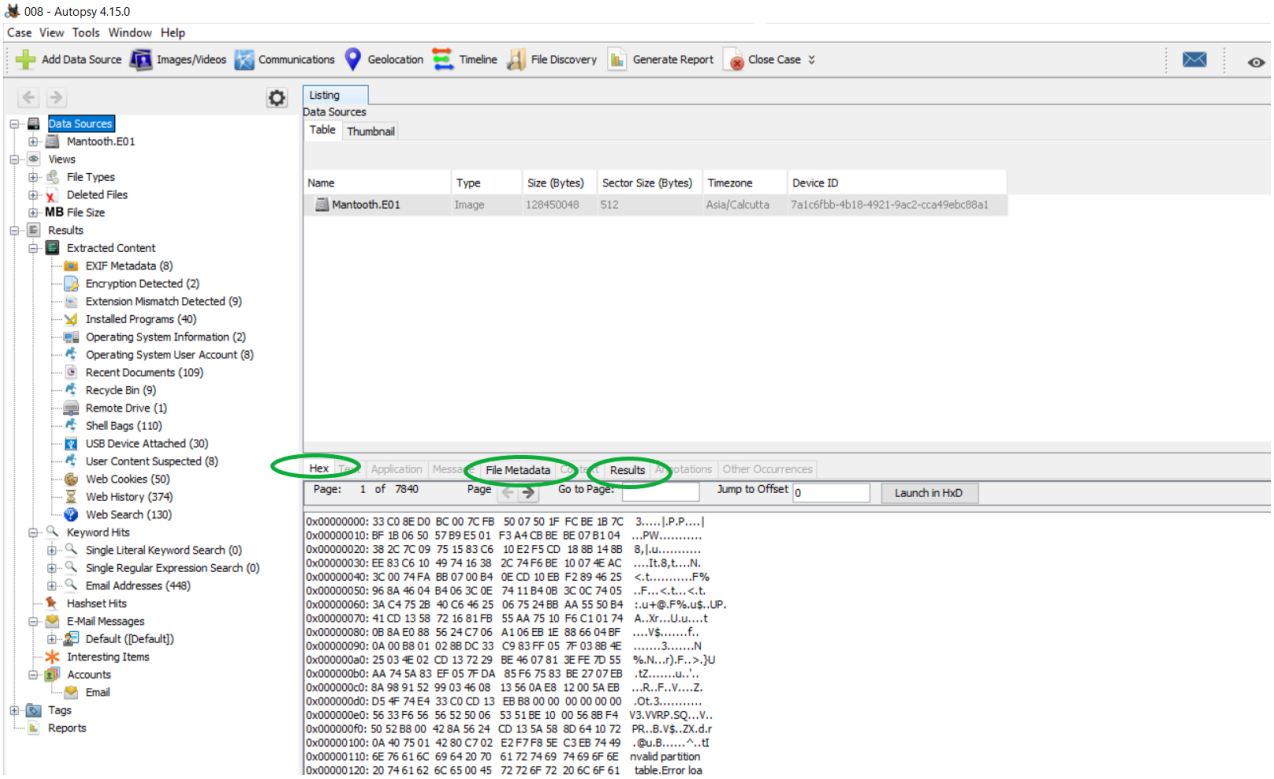
- **File Type Identification:** Identify files based on their internal signatures rather than just file. extensions.
- **Extension Mismatch Detector:** Identify files whose extensions are tampered with/changed possibly to hide evidence.
- **Embedded File Extractor: It** extracts embedded files such as .zip, .rar, etc. and uses the derived file for analysis. Another example could be a PNG image saved inside a doc to make it appear as a document and thus hide crucial information.
- **EXIF (Exchangeable Image File Format) Parser:** It is used to retrieve metadata about the files, for example, date of creation, geolocation, etc.
- **Keyword Search:** Search for a particular keyword/pattern in the data source.
- **Email Parser:** If the disk holds any form of email database, for example, pst/ost files of outlook then information from these files can be extracted using an email parser.
- **Encryption Detection:** Detects and identifies encrypted / password-protected files.
- **Interesting File Identifier:** Let's set custom rules regarding the filtering of data. Examiner is notified when results pertaining to these rules are found.
- **Correlation Engine:** Allows saving properties in and then retrieved from the central repository. It helps in displaying correlated properties.
- **PhotoRec Carver:** Recover files, photos, etc. from the unallocated space.
- **Virtual Machine Extractor:** Extract and analyze any Virtual machine found on the data source.
- **Data Source Integrity:** Calculates the hash values and stores them in the database in case they aren't already present. Otherwise, it will verify the hash values associated with the database.
- **Plaso:** Extract timestamp for various types of files.
- **Android Analyzer:** Analyze SQLite and other files retrieved from an Android device.



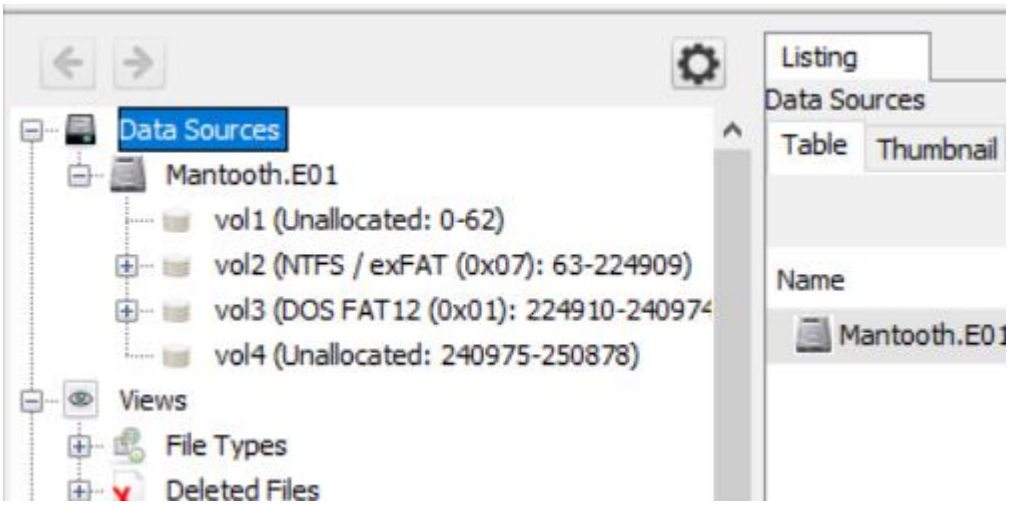
Select all that will serve the purpose of your investigation and click Next. Once the data source is added, click Finish. It will take some buffer time to extract and analyze the data depending upon the size of the Data Source.

3. Exploring the data source:

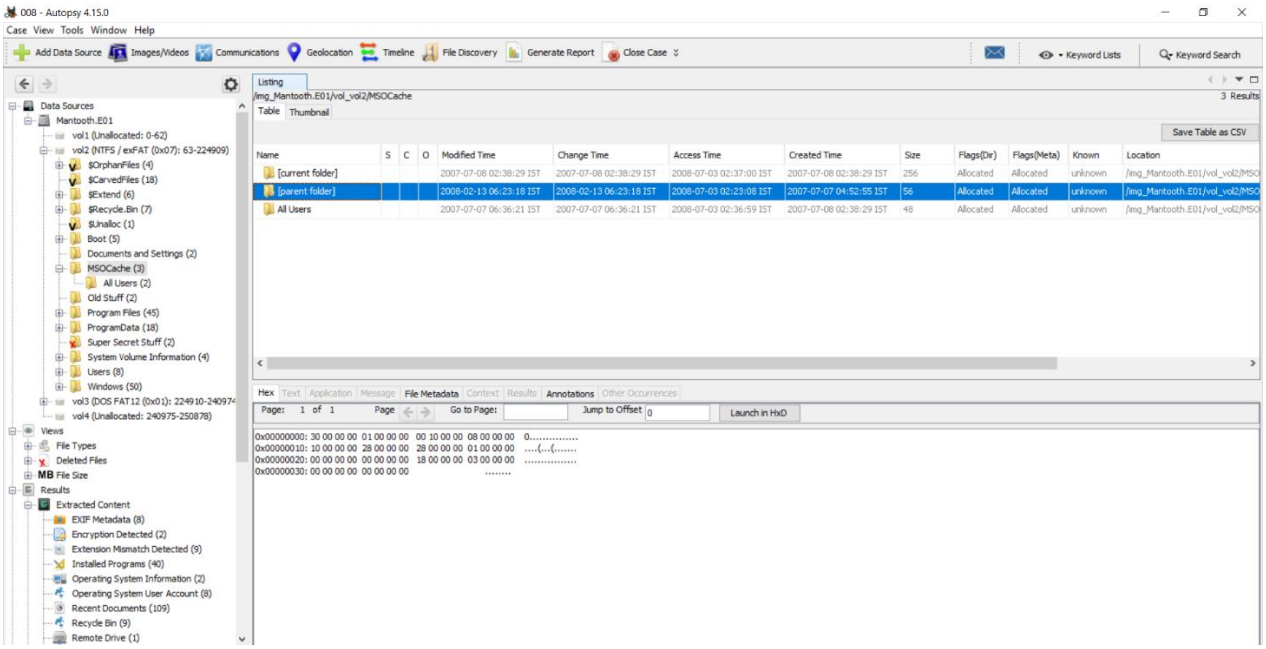
The Data Source information: Here the basic metadata is shown. A detailed analysis is displayed in the bottom section. These details can be extracted in the form of Hex values, Results, File Metadata, etc.



The disk image is then broken down based upon its volume partitions.

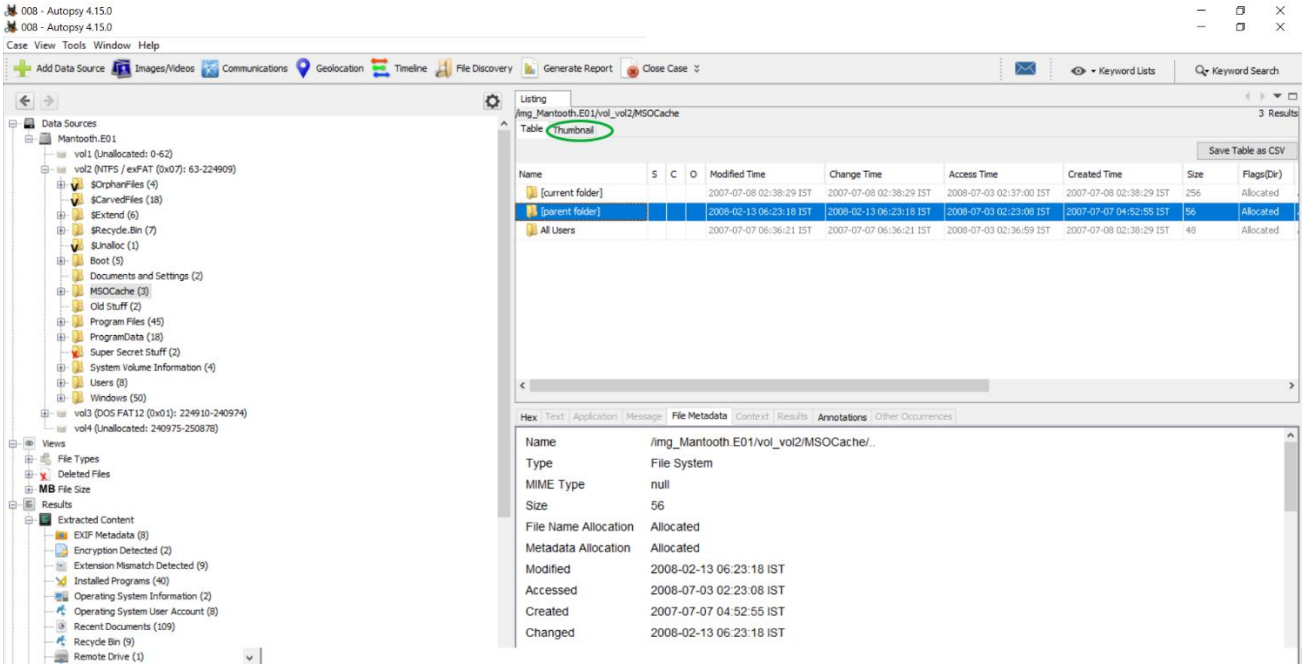


Each volume can be browsed for its contents, results for which are displayed in the section at the bottom. For example, the content shown below belongs to Data Sources -> Mantooth.E01 -> MSOCache-> [Parent Folder].

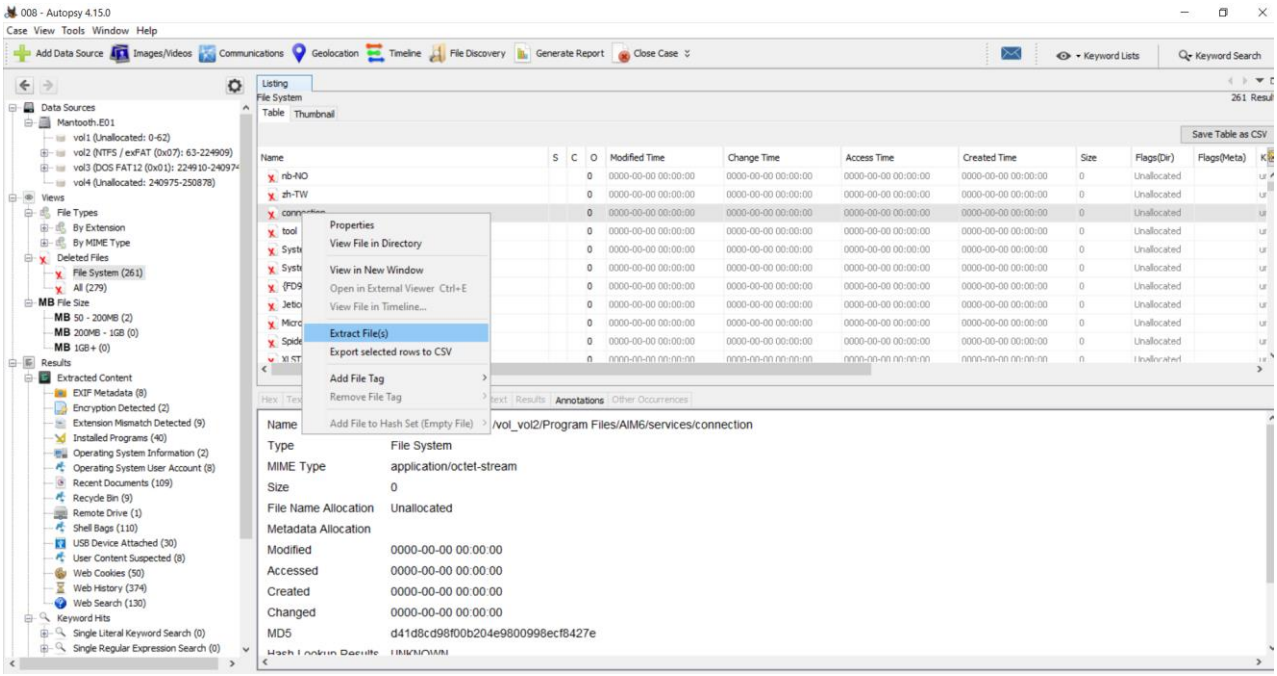


Views (Determines the factor of file classification)

- **File Type**: Here the files are categorized based upon their type. The classification can be done either on the basis of file.extension or MIME type. While both of these provide a hint about how to deal with a file, file extensions are commonly used by the OS to decide what program shall be used to open a file and MIME types are used by the browser to decide about how to present the data (or by the server on how to interpret the data received). Files displayed here also include the deleted files.



- **Deleted Files:** Here information about the files that were specifically deleted can be found. These deleted files can be recovered as well: Right-click on the file to be recovered -> click on Extract File(s). -> Save the file in an appropriate destination.



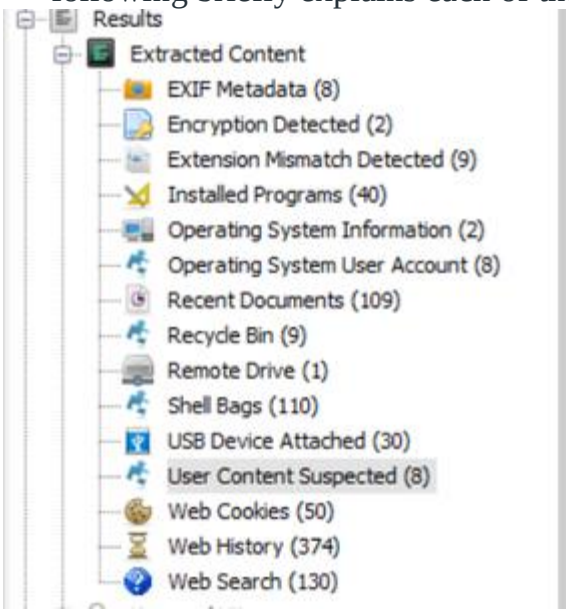
- **MB Size Files:** Here files are classified based upon their size. The range starts from 50MB. This enables the examiner to determine exclusively large files.

Note: It is usually advised to not scan or extract any suspected files/ disks such as payload files, etc. in the main system, rather scan them in safe environments such as a virtual machine, and then extract the data, as they hold the possibility of being corrupt and may infect the examiner's system with viruses.

Results:

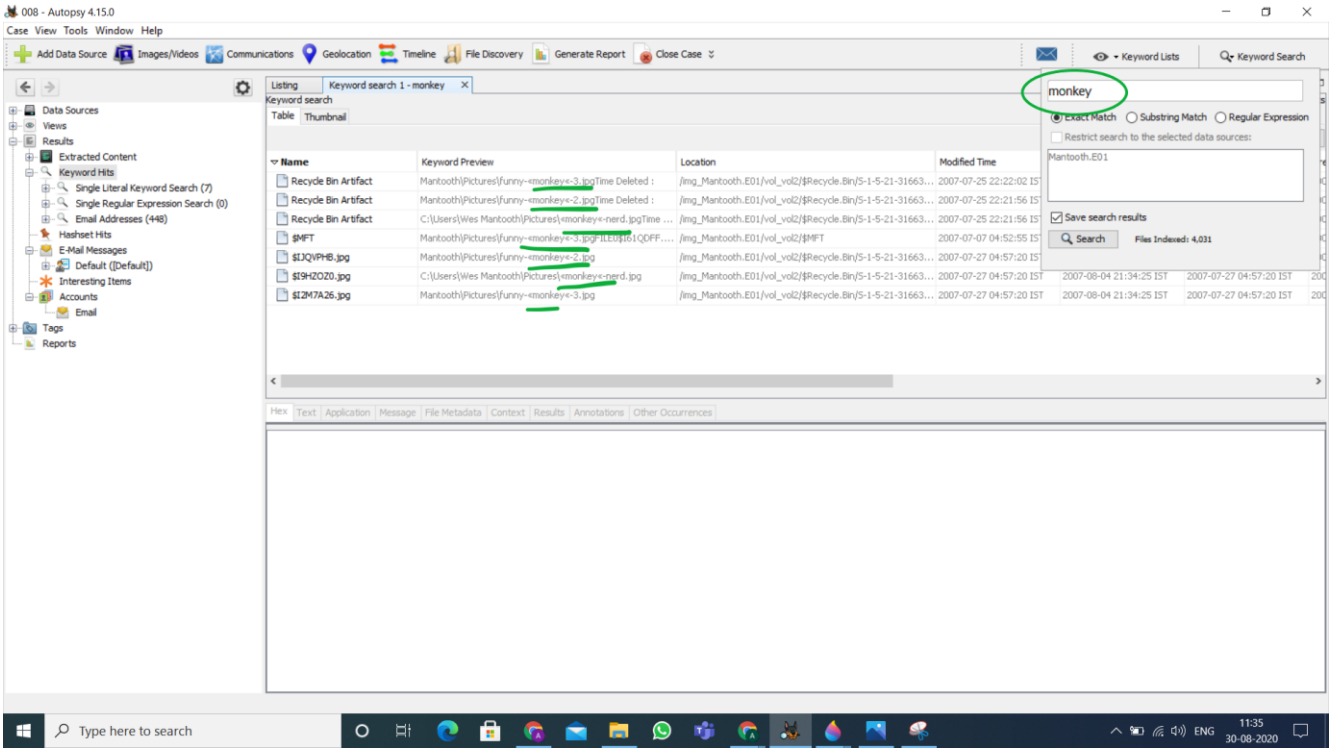
All the extracted data is viewed in ***Views/ Data Source***. In ***Results***, we get the information about this data.

- **Extracted Content:** Each Extracted Content displayed below can be further explored. The following briefly explains each of them.



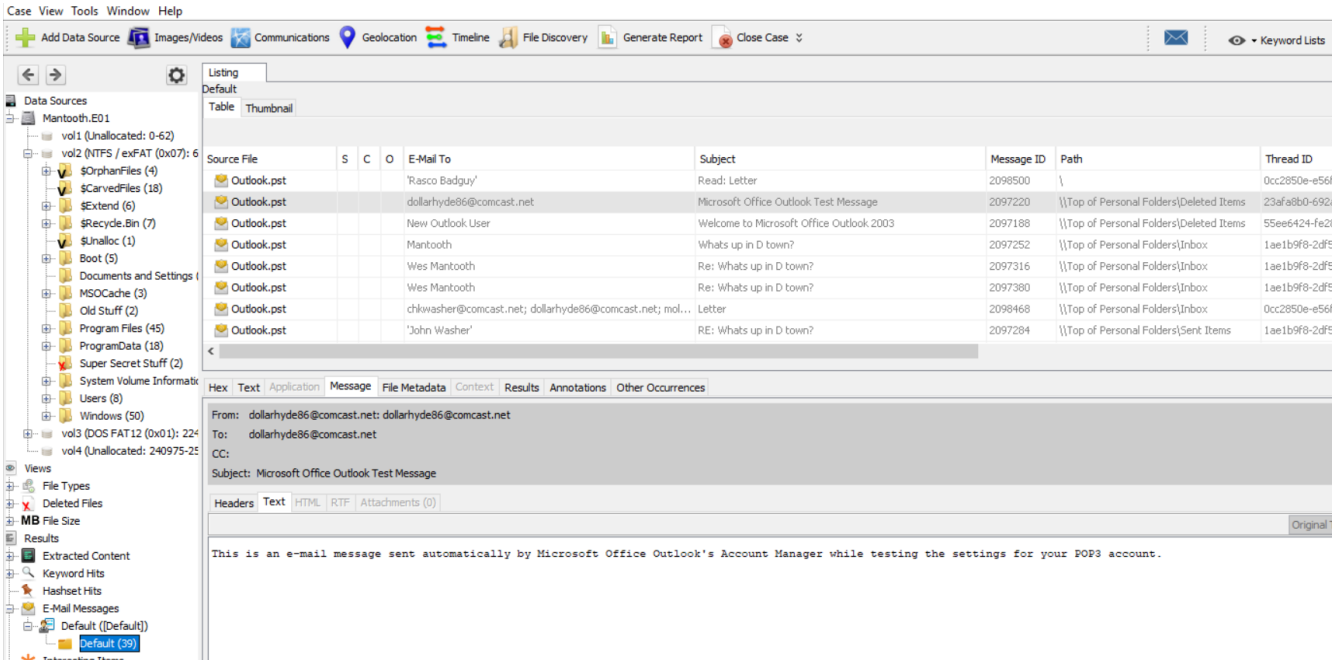
- **EXIF Metadata:** It contains all the .jpg images that have EXIF Metadata associated with them, this Metadata can be analyzed further.
- **Encryption Detection:** It detects files that are password protected/ encrypted.

- **Extension Mismatch Detection:** As explained above, it Identifies the files whose extensions do not match their MIME types and thus they may be suspicious.
- **Installed Programs:** It gives details about the software used by the user. This information is extracted with the help of the Software Registry hive.
- **Operating System Information:** It gives information about the OS with the help of the Windows Registry hive and the Software Registry hive.
- **Operating System User Account:** It lists information about all the user accounts, for example, accounts belonging to the device are extracted from the Software Hive and the accounts associated with the Internet Explorer using index.data files.
- **Recent documents:** Lists all the documents that were accessed nearby the time the disk image was captured.
- **Recycle Bin:** Files that are temporarily stored on the system before being permanently deleted are visible here.
- **Remote Drive:** Shows information about all the remote drives accessed using the system.
- **Shell bags:** A shell bag is a set of registry keys that stores details about a folder being viewed, such as its position, icon, and size. All the Shell bags from the system can be viewed here.
- **USB Device attached:** All the information about the external devices attached to the system is displayed here. This data is extracted from Windows Registry which is actually a maintained database about all the activities taking place on the system.
- **Web Cookies:** Cookies saves the user information from the sites and thus provide a lot of information about the user's online activities.
- **Web History:** All the details about the browser history is shown here.
- **Web Searches:** Details about the web searches made are displayed here.
- **Keyword Hits:** Here specific keywords can be looked for in the image of the disk. Multiple data sources can be selected for the lookup. The search can be restricted to Exact match, Substring match and Regular expression, for example, emails/ IP Addresses, etc.

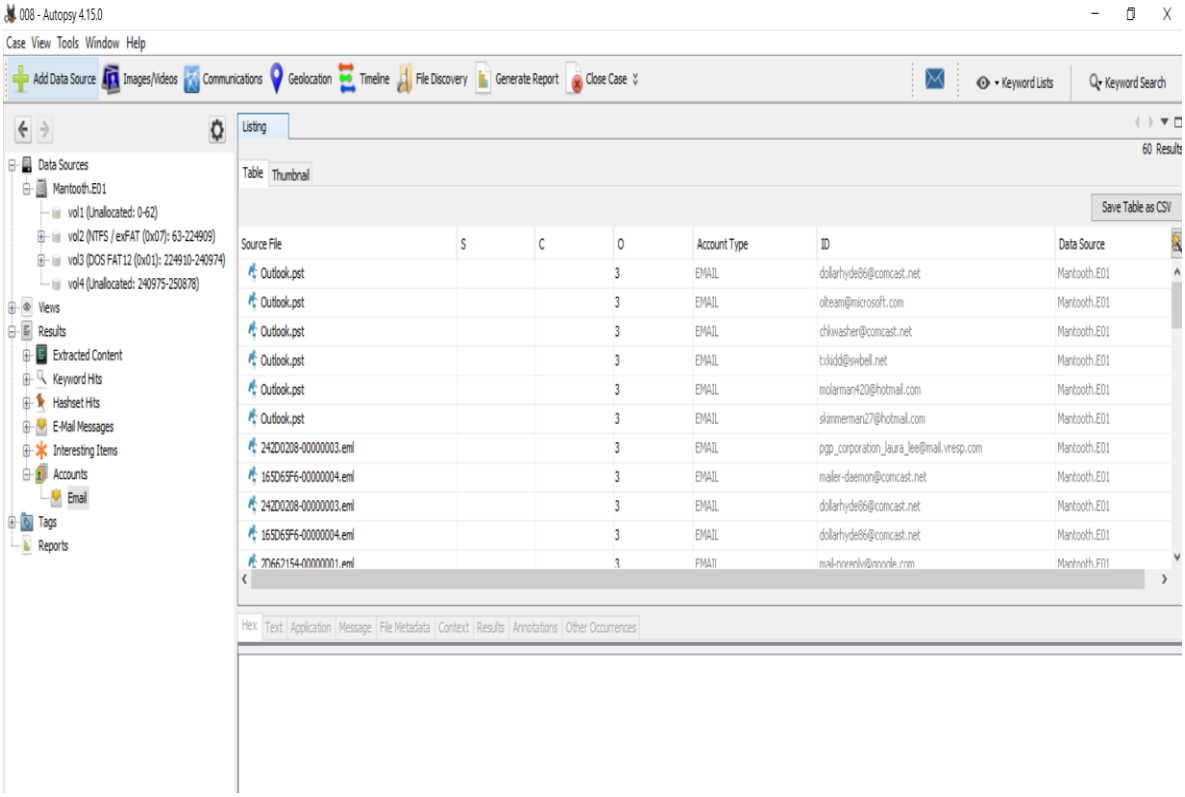


- **HashSet Hits:** Here the search can be made using hash values.

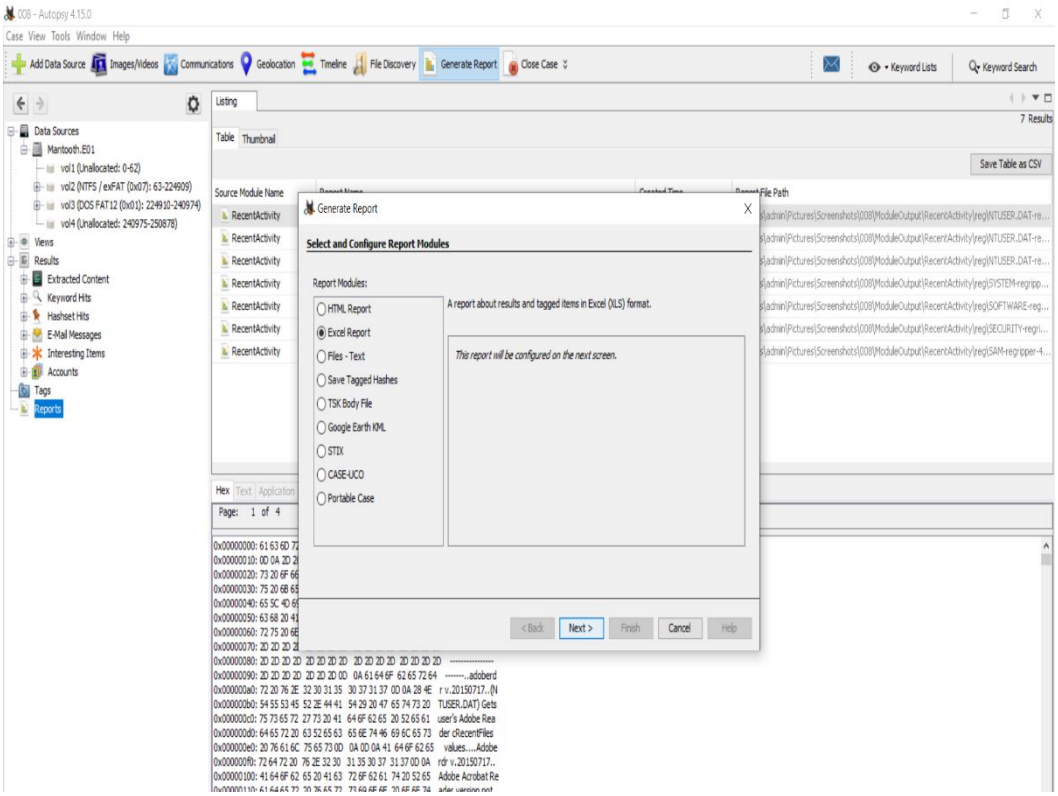
- **E-mail Messages:** Here all the *outlook.pst* files can be explored.

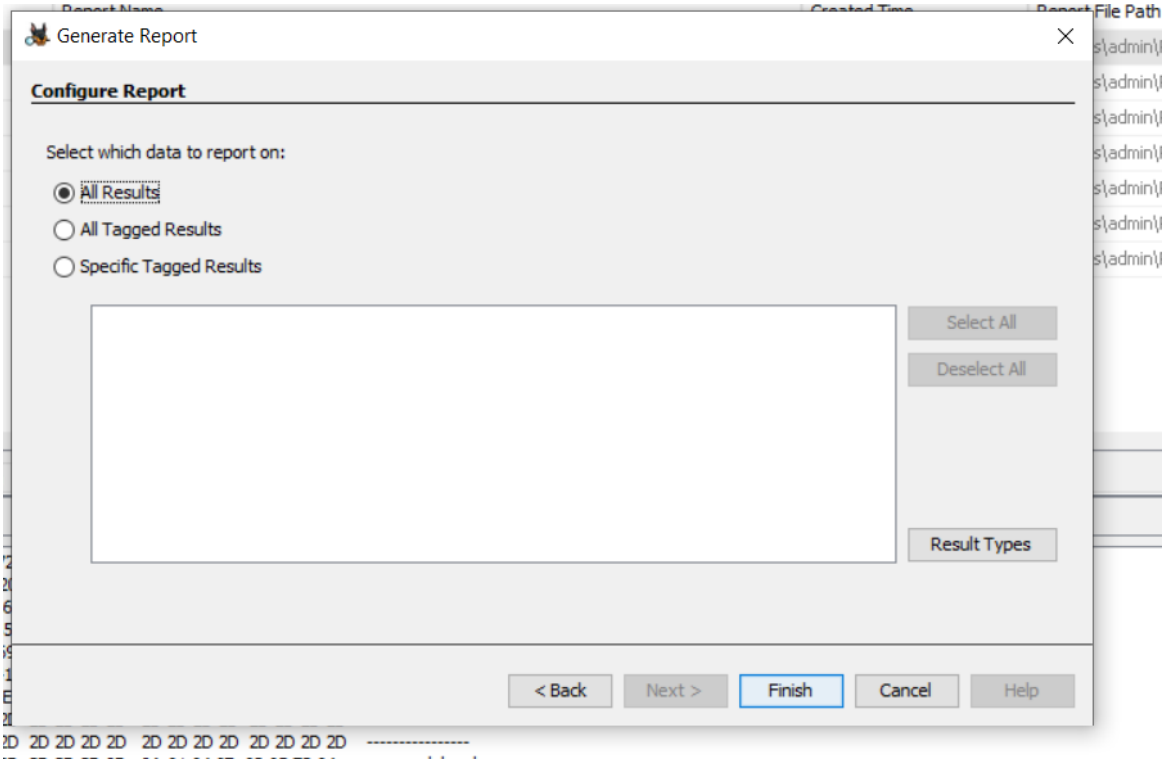


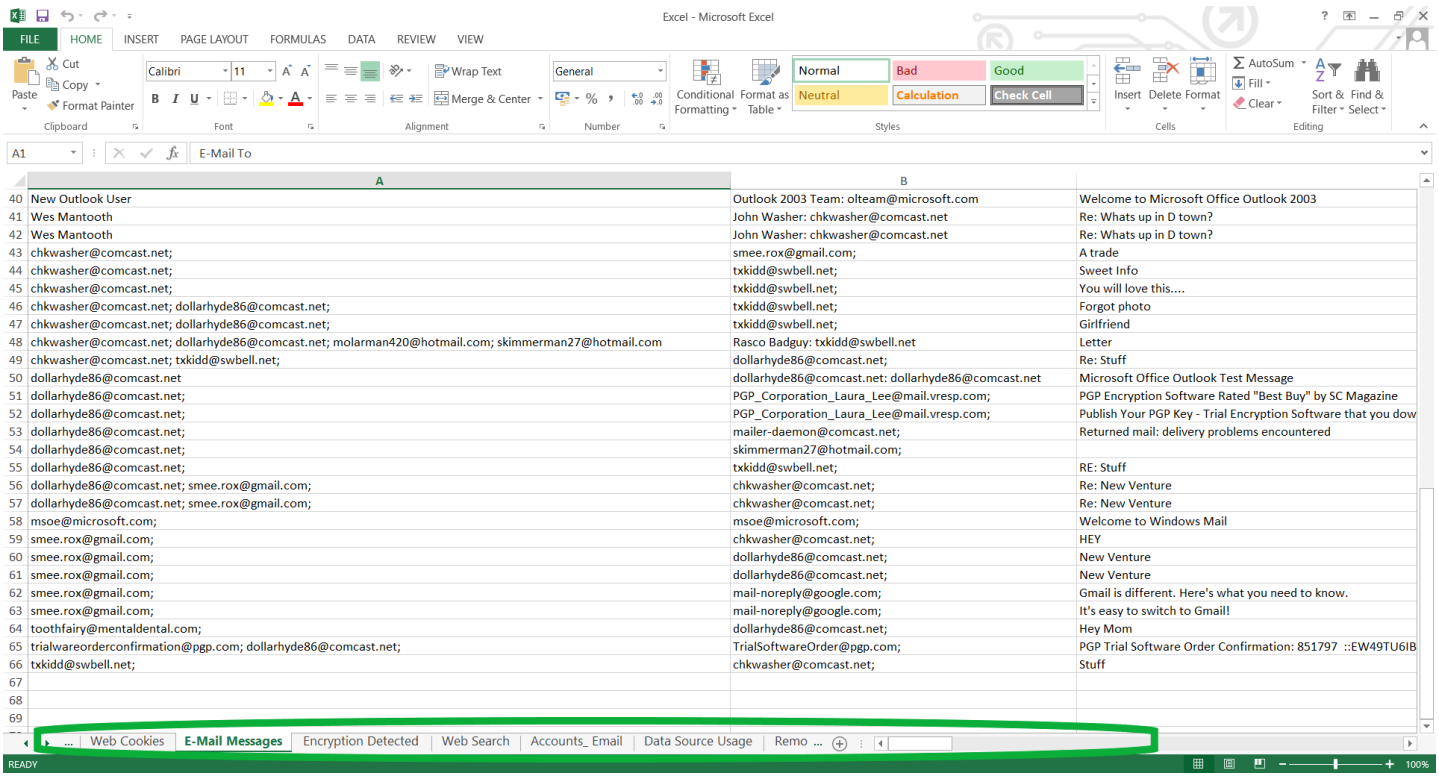
- **Interesting Items:** As discussed before, these are the file results based upon the custom rules set by the examiner.
- **Accounts:** Here all the details regarding the accounts present on the disk are shown. This disk has the following EMAIL accounts.



- **Reports:** Reports about the entire analysis of the data source can be generated and exported in many formats.

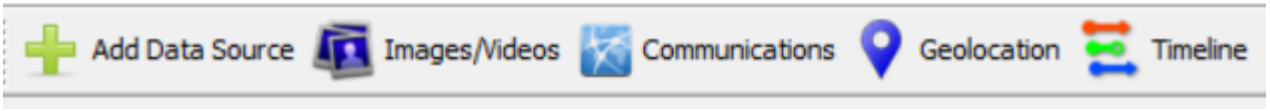

Generate Report
Select and Configure Report Modules
Report Modules:
HTML Report
Excel Report
Files - Text
Save Tagged Hashes
TSK Body File
Google Earth KML
STIX
CASE-UCO
Portable Case
A report about results and tagged items in Excel (XLS) format.
This report will be configured on the next screen.
< Back
Next >
Finish
Cancel
Help


Generate Report
Configure Report
Select which data to report on:
All Results
All Tagged Results
Specific Tagged Results
Select All
Deselect All
Result Types
< Back
Next >
Finish
Cancel
Help

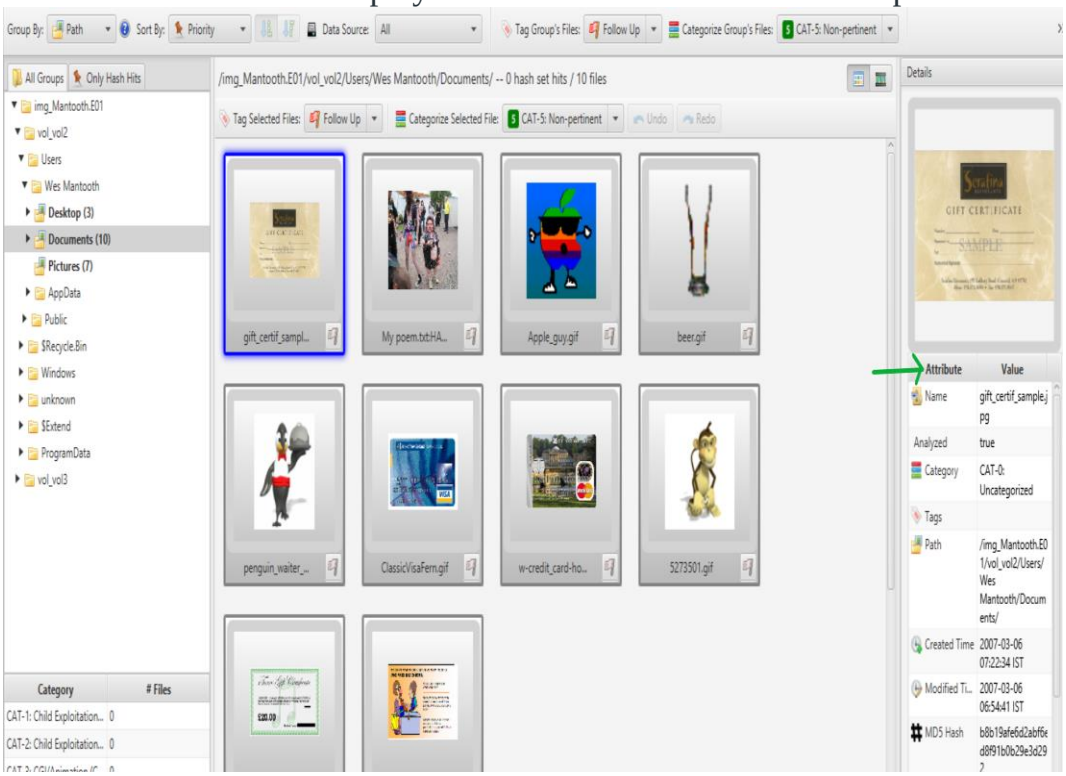


	A	B	
40	New Outlook User	Outlook 2003 Team: olteam@microsoft.com	Welcome to Microsoft Office Outlook 2003
41	Wes Mantooth	John Washer: chkwasher@comcast.net	Re: Whats up in D town?
42	Wes Mantooth	John Washer: chkwasher@comcast.net	Re: Whats up in D town?
43	chkwasher@comcast.net;	smee.rox@gmail.com;	A trade
44	chkwasher@comcast.net;	txkidd@swbell.net;	Sweet Info
45	chkwasher@comcast.net;	txkidd@swbell.net;	You will love this....
46	chkwasher@comcast.net; dollarhyde86@comcast.net;	txkidd@swbell.net;	Forgot photo
47	chkwasher@comcast.net; dollarhyde86@comcast.net;	txkidd@swbell.net;	Girlfriend
48	chkwasher@comcast.net; dollarhyde86@comcast.net; molarman420@hotmail.com; skimmerman27@hotmail.com	Rasco Badguy: txkidd@swbell.net	Letter
49	chkwasher@comcast.net; txkidd@swbell.net;	dollarhyde86@comcast.net;	Re: Stuff
50	dollarhyde86@comcast.net	dollarhyde86@comcast.net: dollarhyde86@comcast.net	Microsoft Office Outlook Test Message
51	dollarhyde86@comcast.net;	PGP_Corporation_Laura_Lee@mail.vresp.com;	PGP Encryption Software Rated "Best Buy" by SC Magazine
52	dollarhyde86@comcast.net;	PGP_Corporation_Laura_Lee@mail.vresp.com;	Publish Your PGP Key - Trial Encryption Software that you dow
53	dollarhyde86@comcast.net;	mailer-daemon@comcast.net;	Returned mail: delivery problems encountered
54	dollarhyde86@comcast.net;	skimmerman27@hotmail.com;	
55	dollarhyde86@comcast.net;	txkidd@swbell.net;	RE: Stuff
56	dollarhyde86@comcast.net; smee.rox@gmail.com;	chkwasher@comcast.net;	Re: New Venture
57	dollarhyde86@comcast.net; smee.rox@gmail.com;	chkwasher@comcast.net;	Re: New Venture
58	msoe@microsoft.com;	msoe@microsoft.com;	Welcome to Windows Mail
59	smee.rox@gmail.com;	chkwasher@comcast.net;	HEY
60	smee.rox@gmail.com;	dollarhyde86@comcast.net;	New Venture
61	smee.rox@gmail.com;	dollarhyde86@comcast.net;	New Venture
62	smee.rox@gmail.com;	mail-noreply@google.com;	Gmail is different. Here's what you need to know.
63	smee.rox@gmail.com;	mail-noreply@google.com;	It's easy to switch to Gmail!
64	toothfairy@mentaldental.com;	dollarhyde86@comcast.net;	Hey Mom
65	trialwareorderconfirmation@pgp.com; dollarhyde86@comcast.net;	TrialSoftwareOrder@pgp.com;	PGP Trial Software Order Confirmation: 851797 ::EW49TU6IB
66	txkidd@swbell.net;	chkwasher@comcast.net;	Stuff
67			
68			
69			

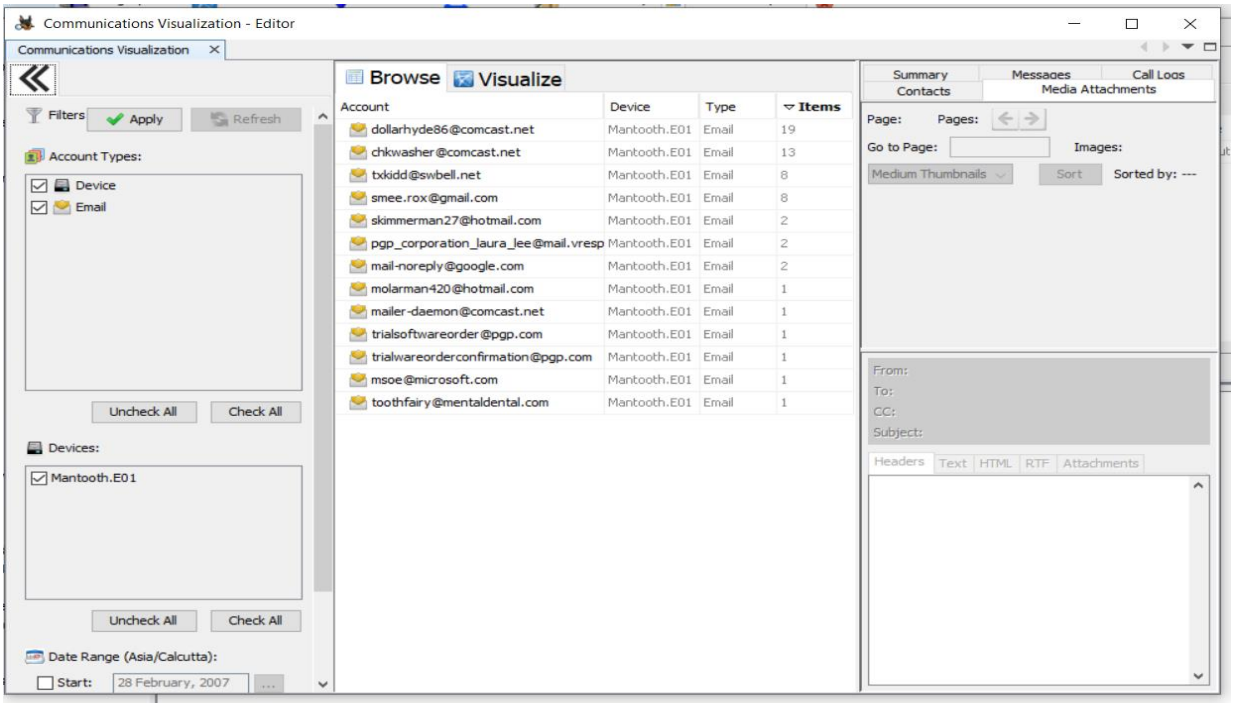
Additional Features:



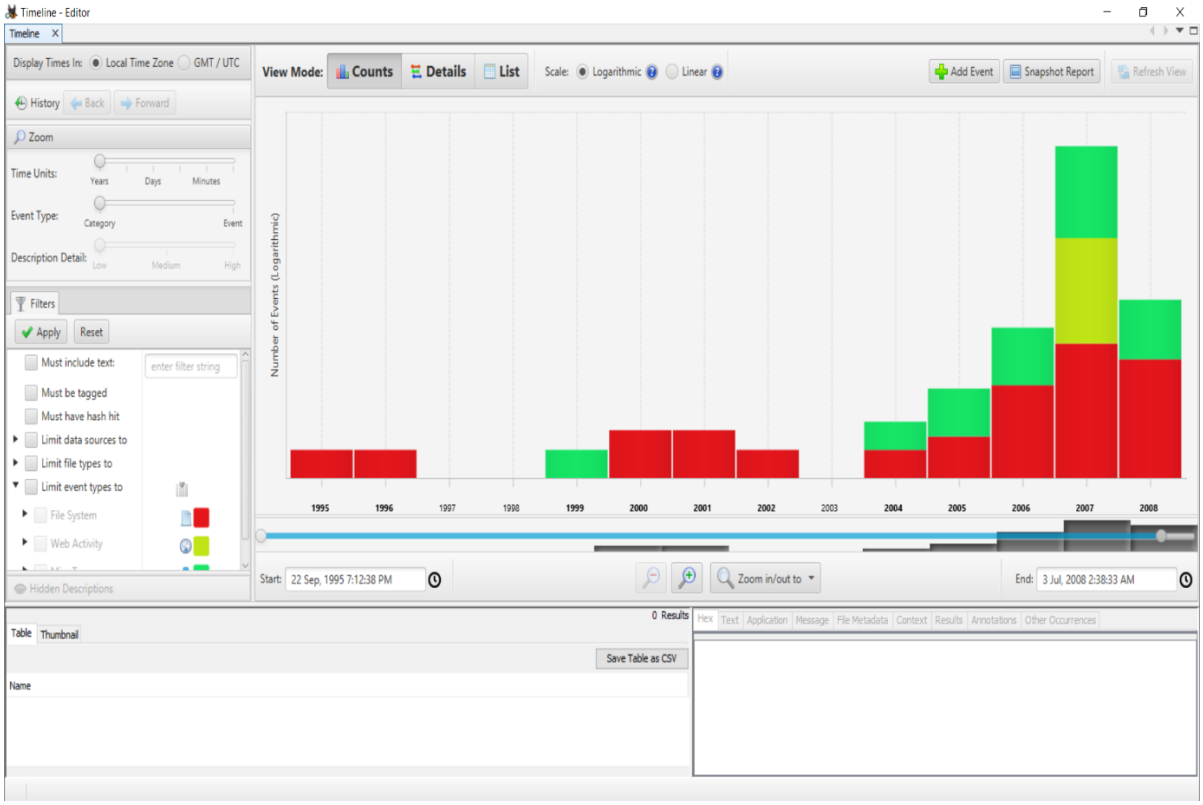
- **Add a Data Source:** Each case can hold multiple Data Sources.
- **Images/Videos:** Images/ Videos in the data source can be viewed in Gallery View. The information here is displayed in the form of attribute-value pairs.



- **Communications:** All the communications made using the source device are displayed here. This device had communications only in the form of emails.



- **Geolocation:** This window displays the artifacts that have longitude and latitude attributes as waypoints on a map. Here the data source has no waypoints.
- **Timeline:** Information about when the computer was used or what events took place before or after a given event can be found, this greatly helps in investigating events near about a particular time.



- Almost all the basic features and how actually Autopsy works have been discussed in this article. However, it is always recommended to go through different sample data sources to explore even more

Practical – 9

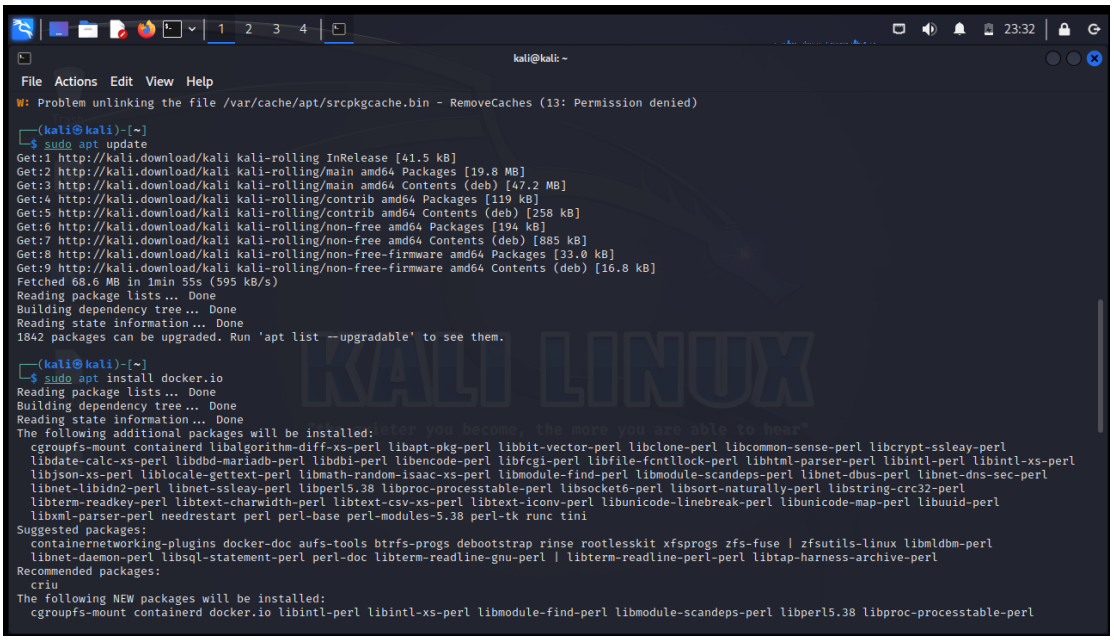
Aim :- Implementation of Mobile Audit and generate the report of the existing Artifacts.

1. Update APT:

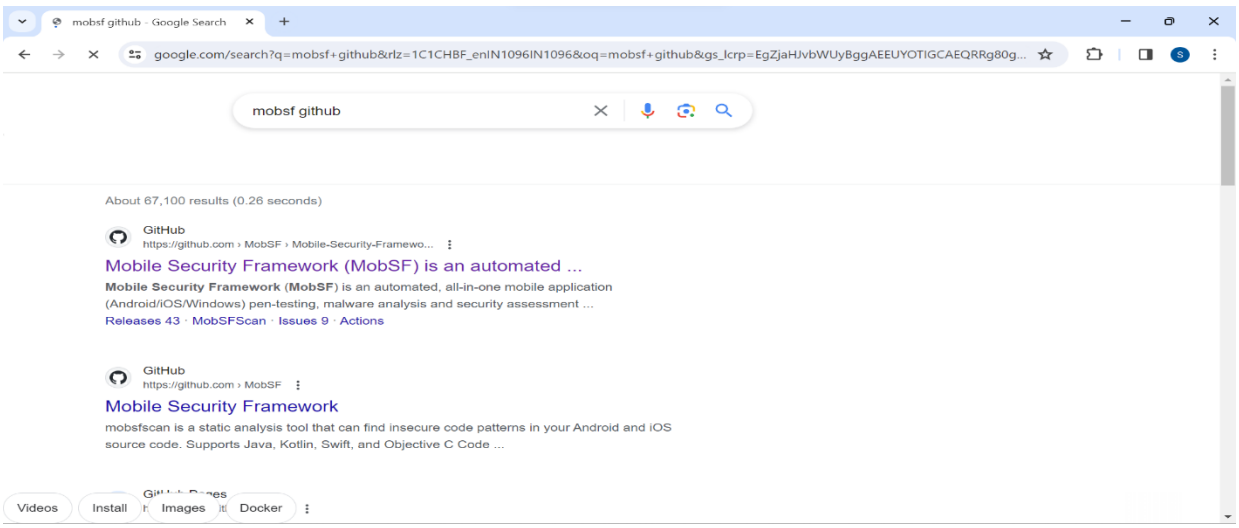
sudo apt update

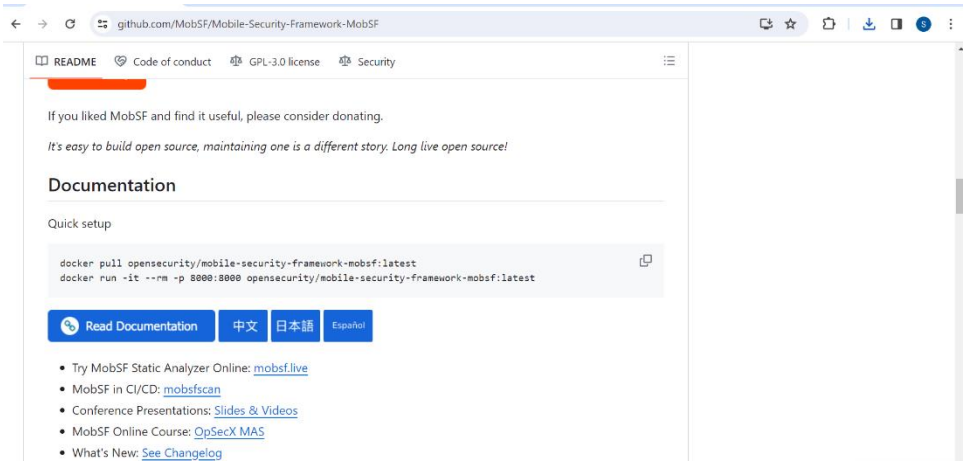
2. Install docker:

sudo apt install docker.io



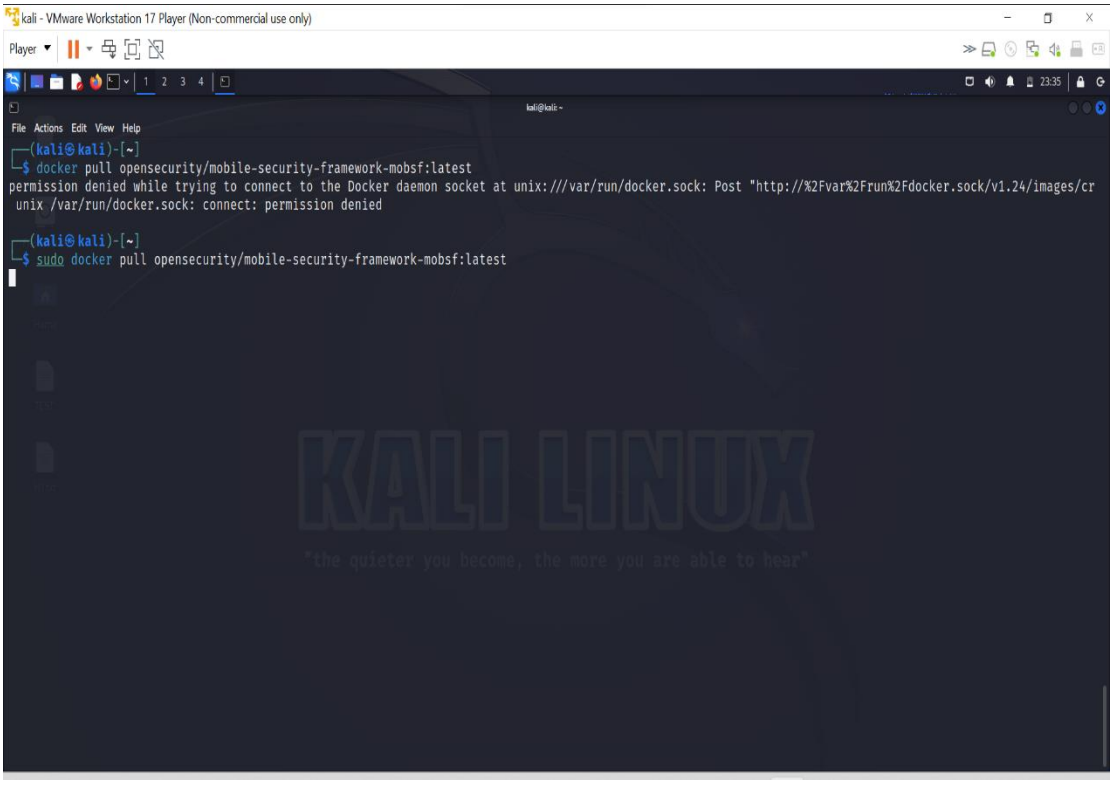
3. Search mobsf github on your web browser.



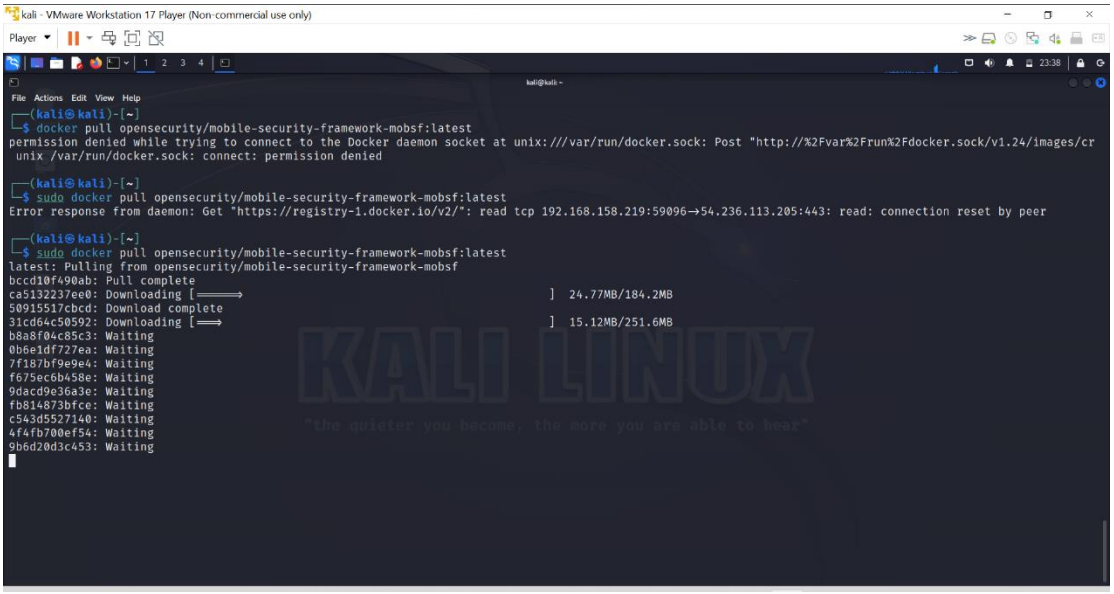


Next, download MobSF Docker image from https://hub.docker.com/r/opensecurity/mobile-security-framework-mobsf/ with the following command:

docker pull opensecurity/mobile-security-framework-mobsf:latest



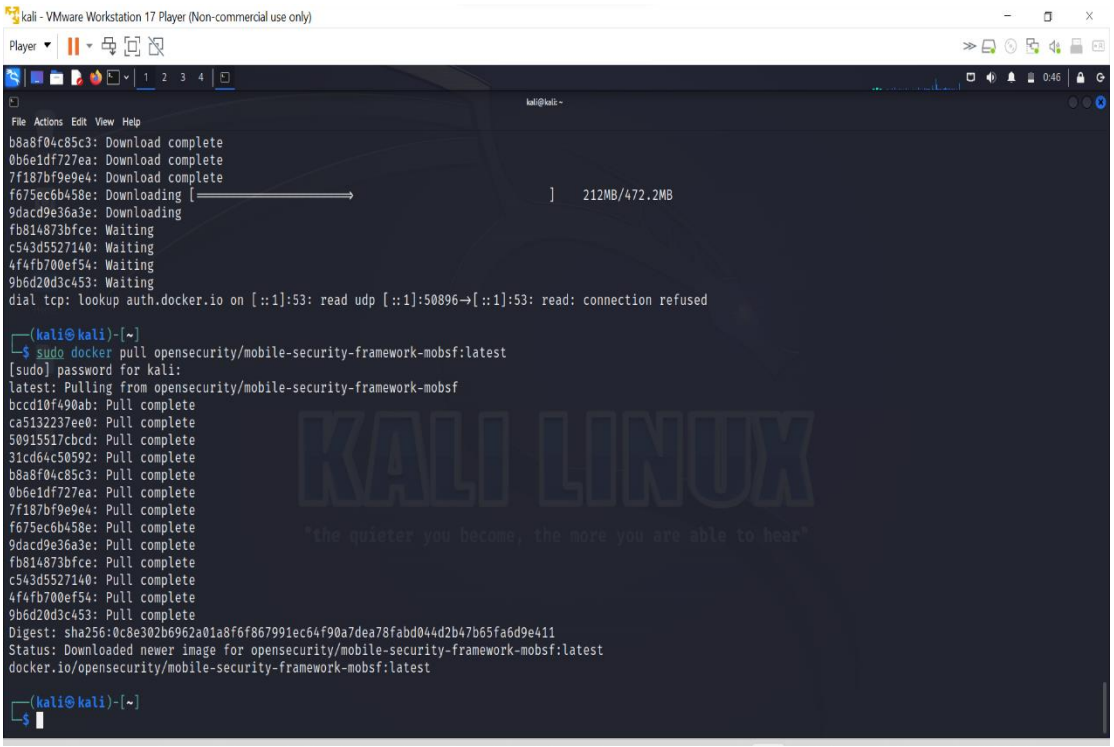
Once you issue the command, you would notice the following output on your console:

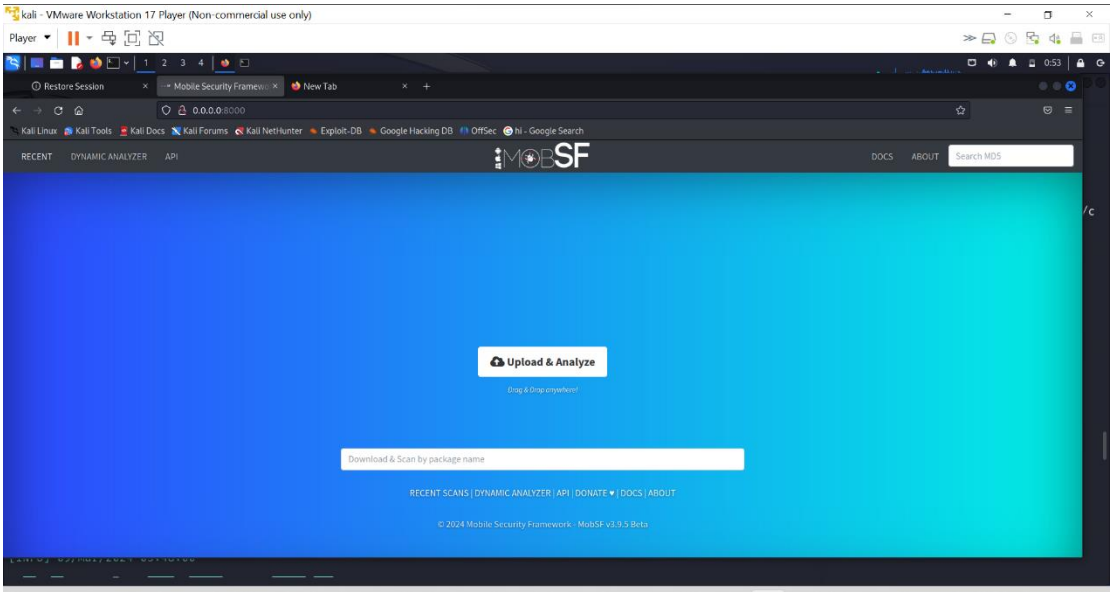


This signifies that the docker image for MobSF is being downloaded. Once completed, the following message will appear:

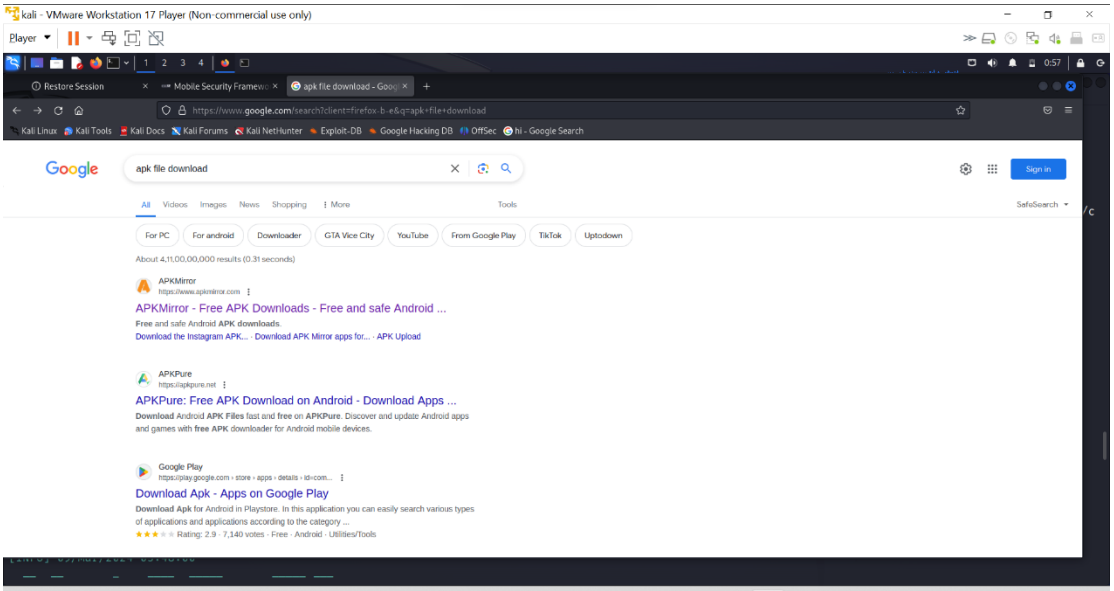
Now that the docker image is downloaded, the image can be run with the following command:

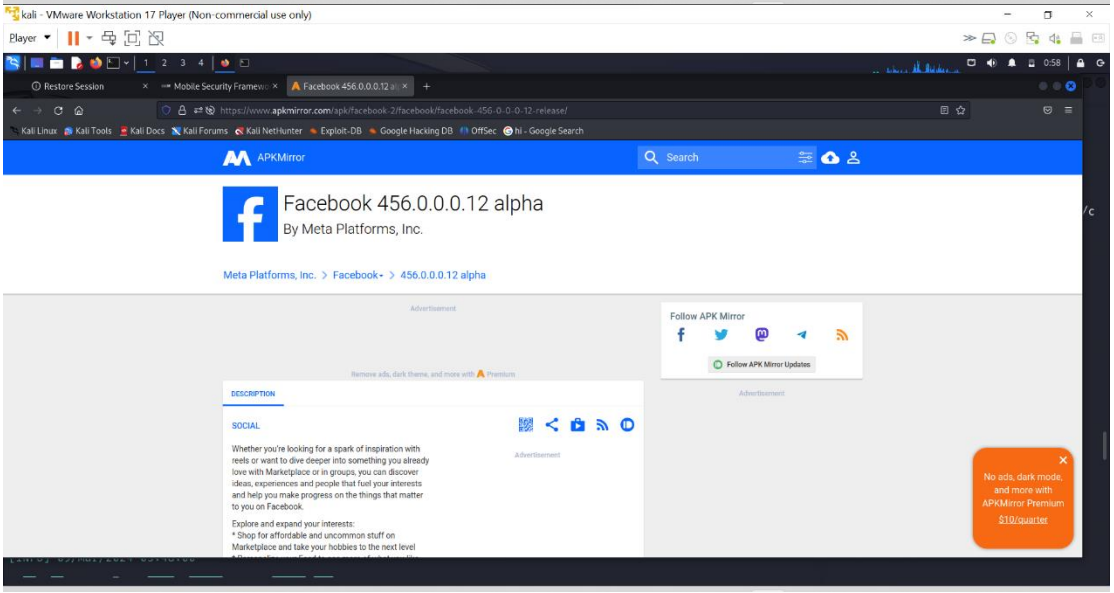
docker run -it -p 8000:8000 opensecurity/mobile-security-framework-mobsf

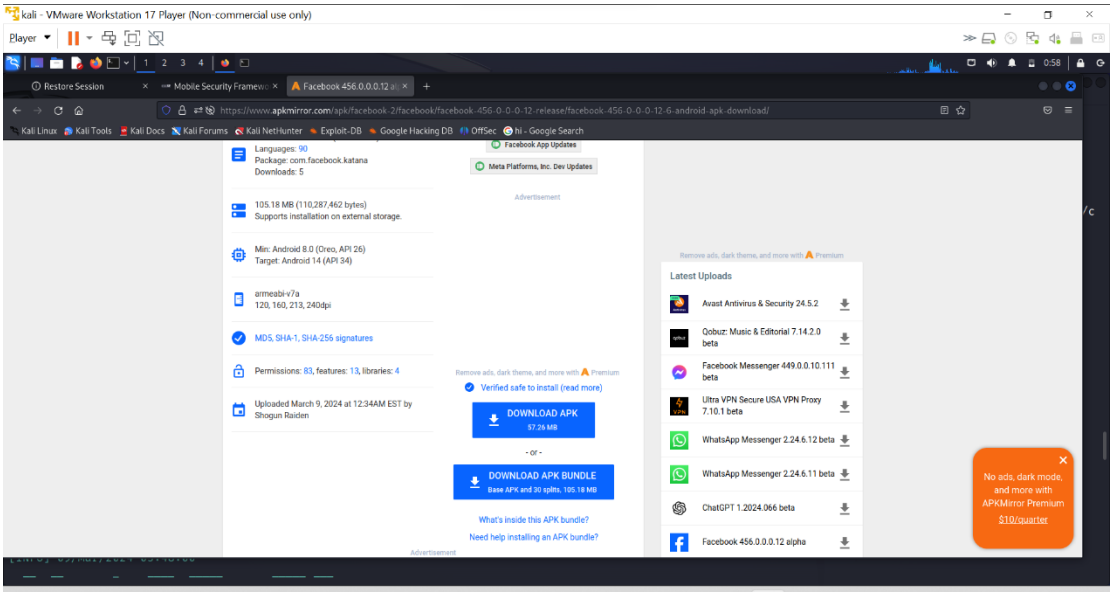


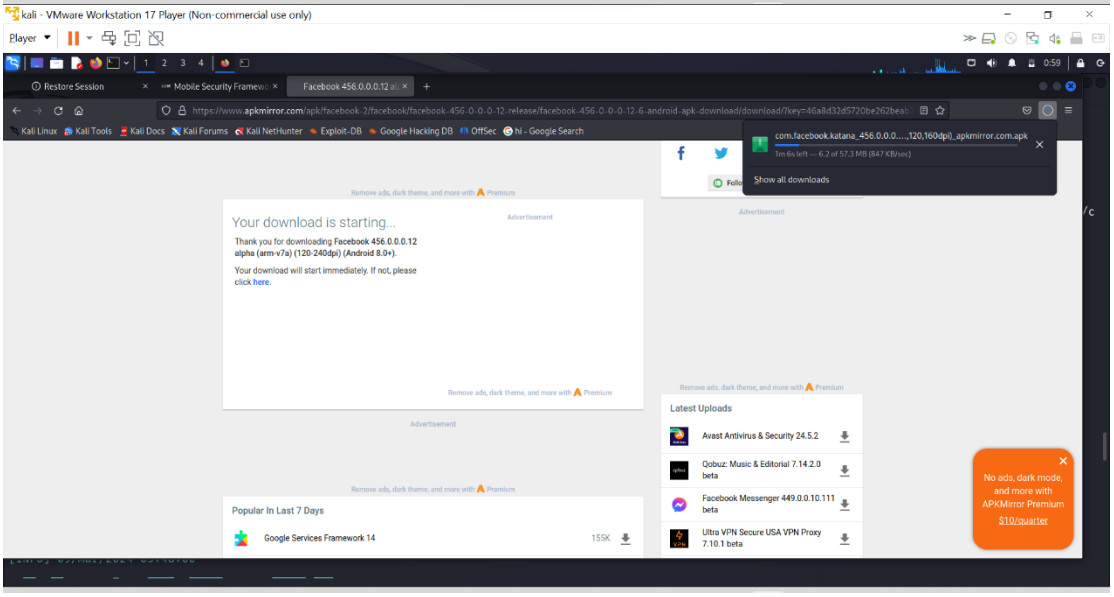


For our testing, we take Facebook Lite's APK file.

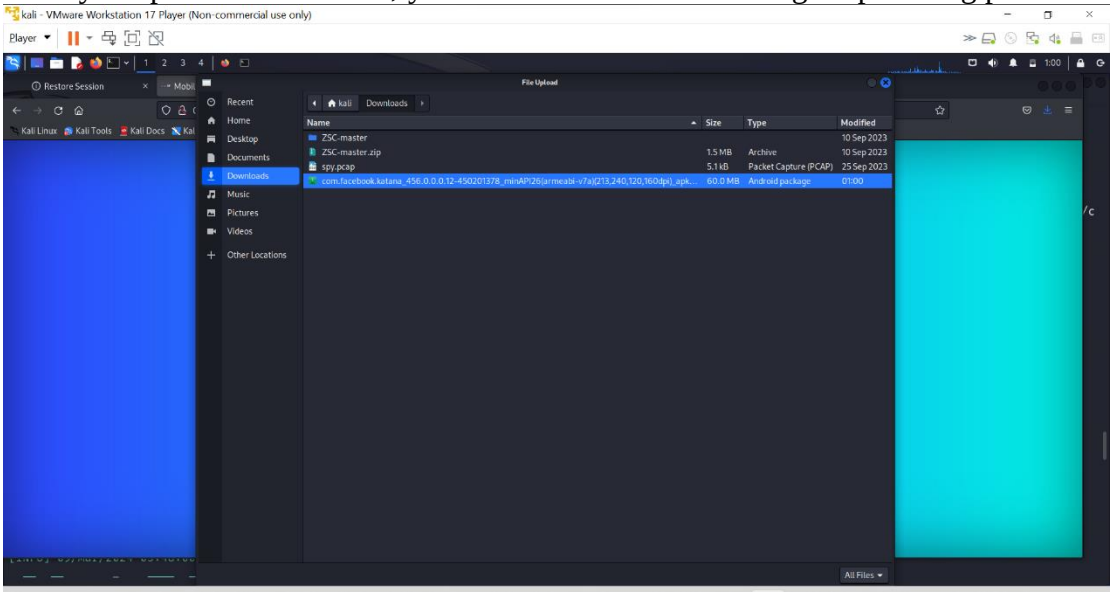


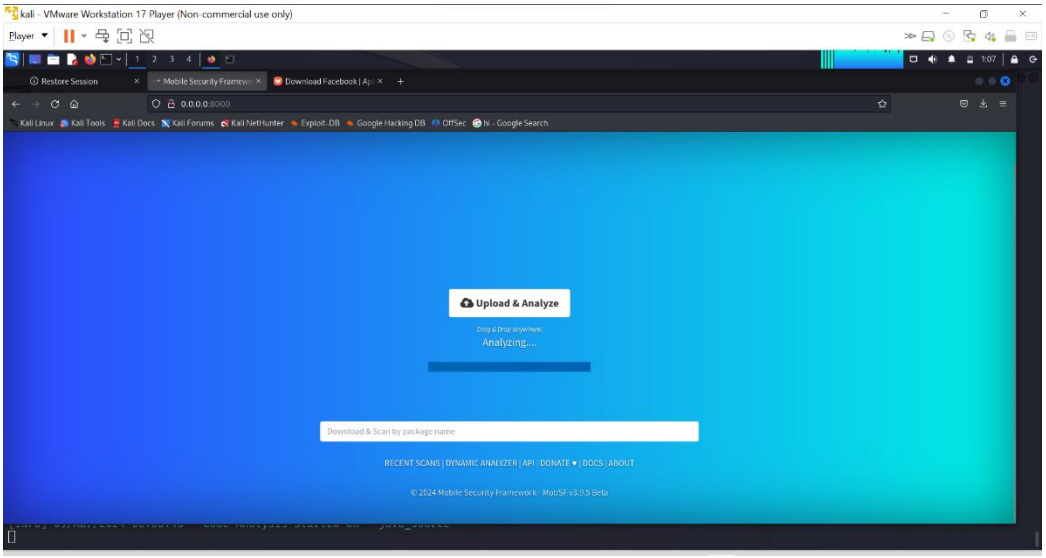




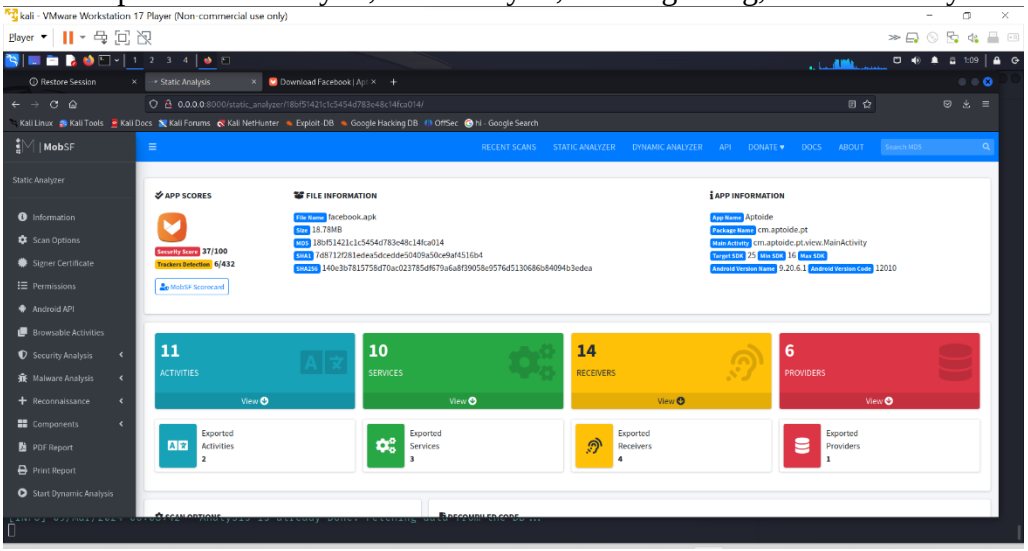


Once you upload the APK file, you would notice the following output being printed on our terminal:

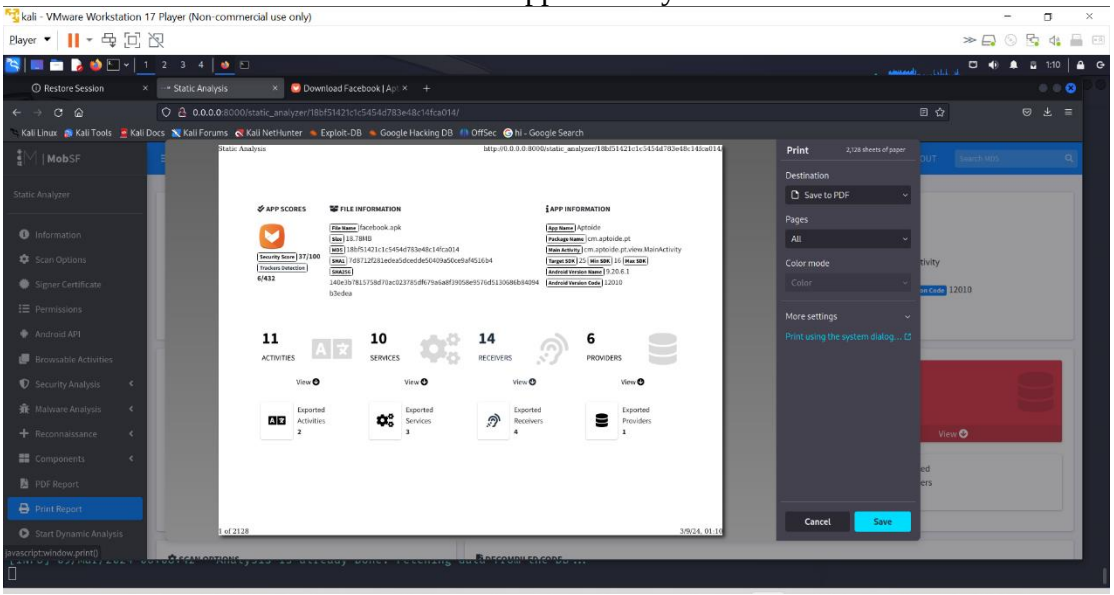




Once the analysis is complete, the browser will show assessment details, such as application description, Android permission analysis, code analysis, CVSS grading, malware analysis etc.



You also notice a brief overview of the application you have reviewed. You can also the report for same.



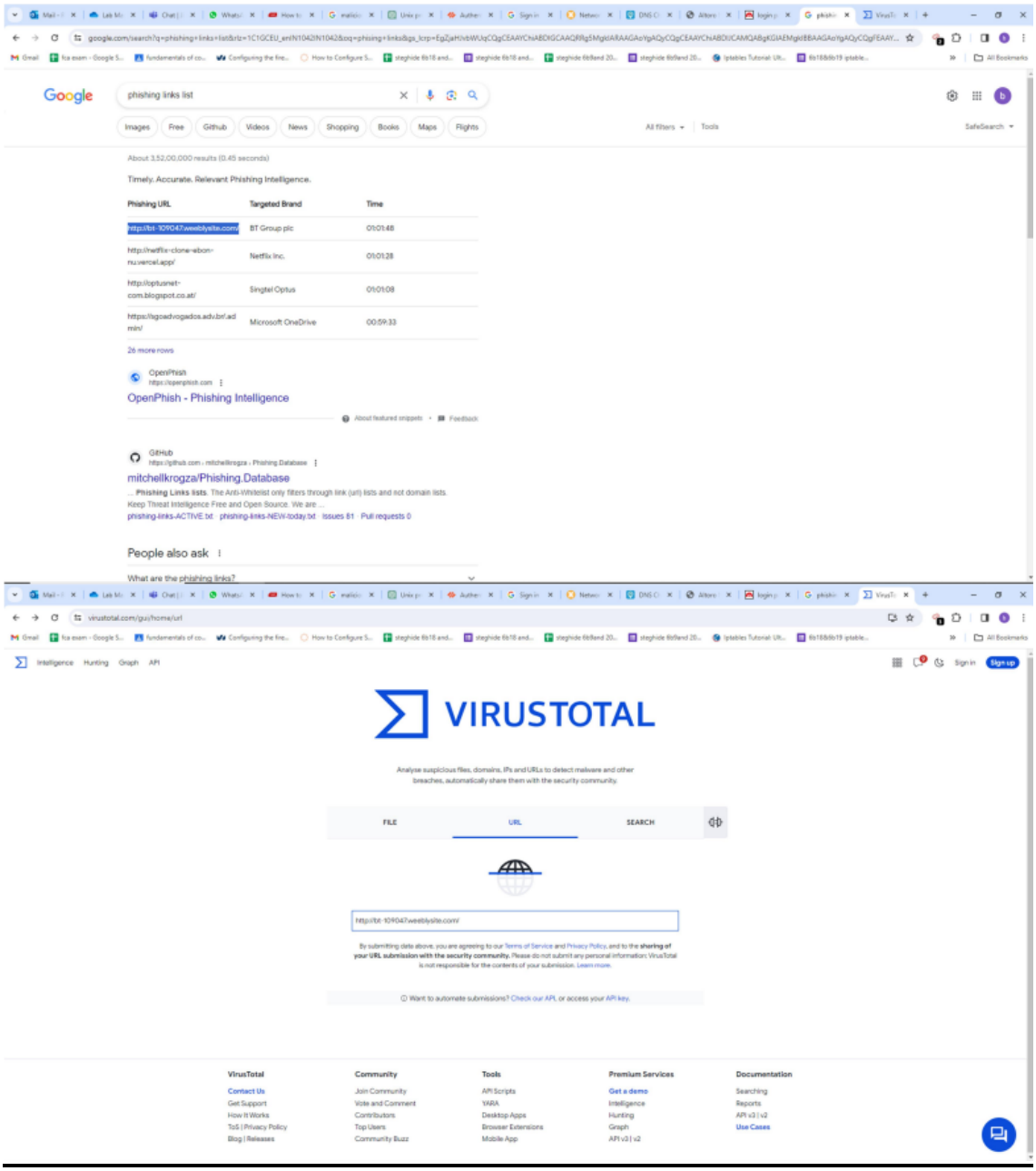
Practical – 7

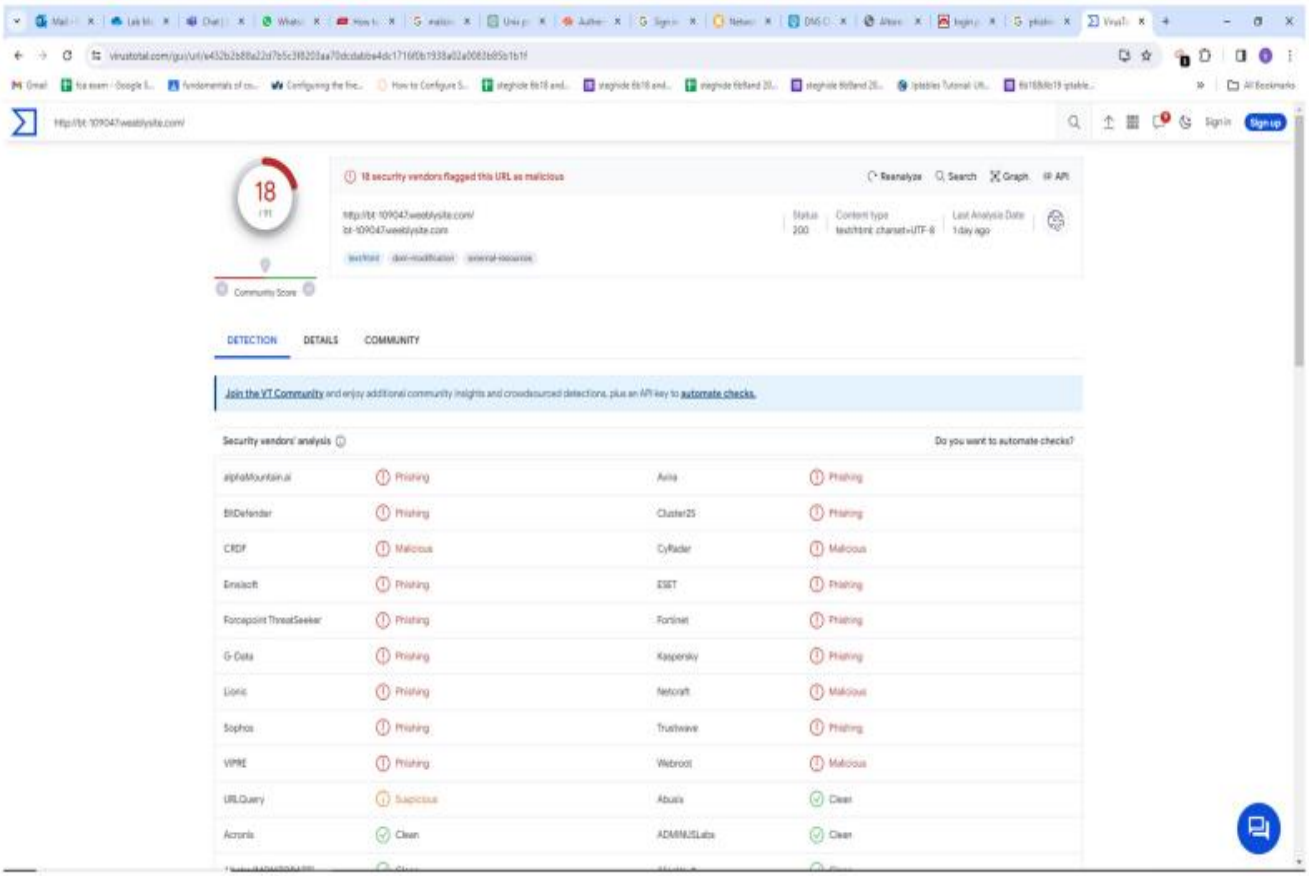
Aim :- Implementation of IT Audit, malware analysis and Vulnerability assessment and generate the report.

Objective: To know how to find vulnerabilities by using NESSUS

Requirements: Laptop, Kali linux, Nessusd pakage in kali

Malware analysis





NESSUS:

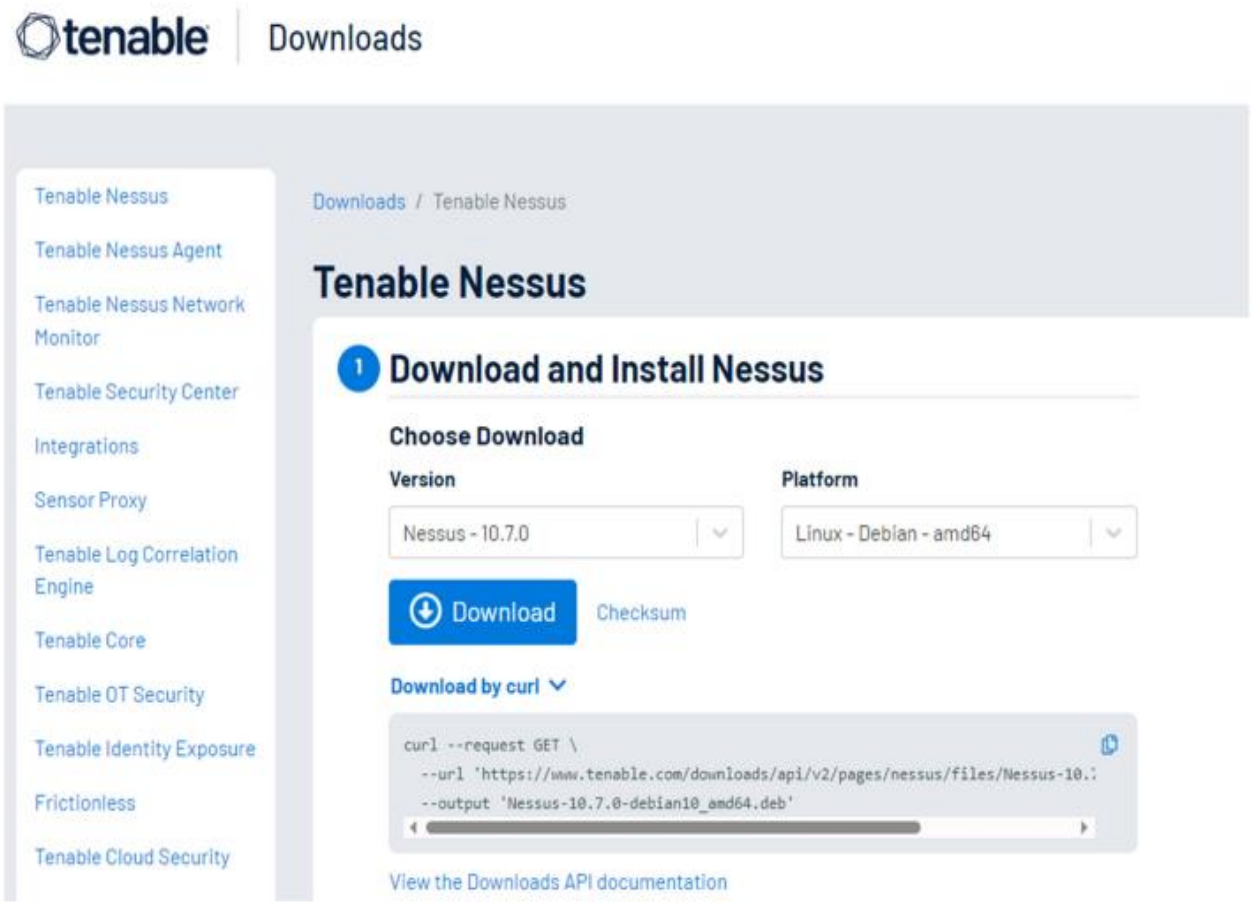
Nessus, developed by Tenable Inc, is a widely-used open-source vulnerability scanner. It offers a paid subscription, Nessus Professional, as well as a free version, Nessus Essentials, which is limited to 16 IP addresses per scanner.

Nessus provides a range of services, including vulnerability assessments, network scans, web scans, asset discovery, and more, to aid security professionals, penetration testers, and other cybersecurity enthusiasts in proactively identifying and mitigating vulnerabilities in their networks.

How to install a Nessus in kali
Unlike many security tools, Nessus doesn't come installed on Kali Linux. But it is very easy to download and install.

Follow these steps to install Nessus on your Kali:

1. Download the Nessus package for Debian on the Nessus website and make sure you set the Platform to **Linux-Debian-amd64**.



2. When it's finished downloading, open your Linux terminal and navigate to the location you downloaded the Nessus file to.

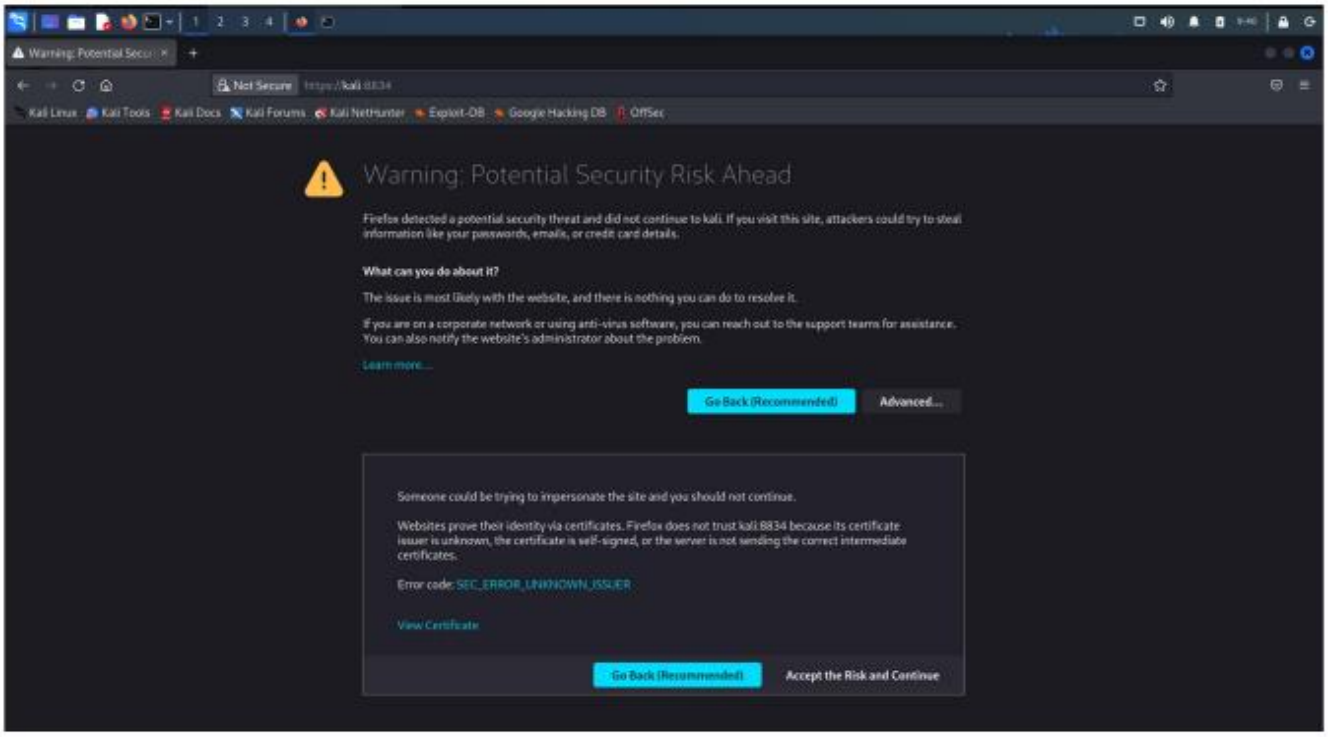
Install Nessus using this command:

```
dpkg -i Nessus-10.7.0-debian10_amd64.deb
Selecting previously unselected package nessus.
(Reading database ... 399450 files and directories currently installed.)
Preparing to unpack Nessus-10.7.0-debian10_amd64.deb ...
Unpacking nessus (10.7.0) ...
Setting up nessus (10.7.0) ...
HMAC : (Module_Integrity) : Pass
SHA1 : (KAT_Digest) : Pass
SHA2 : (KAT_Digest) : Pass
SHA3 : (KAT_Digest) : Pass
TDES : (KAT_Cipher) : Pass
AES_GCM : (KAT_Cipher) : Pass
AES_ECB_Decrypt : (KAT_Cipher) : Pass
RSA : (KAT_Signature) : RNG : (Continuous_RNG_Test) : Pass
Pass
ECDSA : (PCT_Signature) : Pass
ECDSA : (PCT_Signature) : Pass
DSA : (PCT_Signature) : Pass
TLS13_KDF_EXTRACT : (KAT_KDF) : Pass
TLS13_KDF_EXPAND : (KAT_KDF) : Pass
TLS12_PRF : (KAT_KDF) : Pass
PBKDF2 : (KAT_KDF) : Pass
SSHKDF : (KAT_KDF) : Pass
KBKDF : (KAT_KDF) : Pass
```

Start the Nessus service with this command:

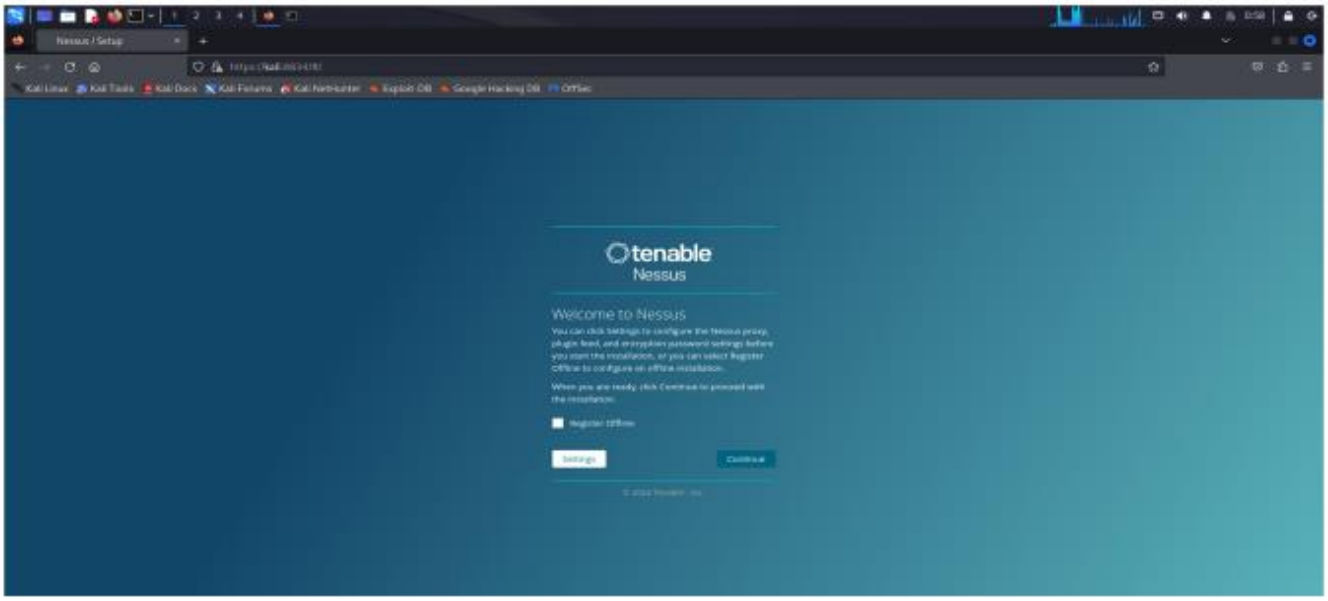
```
File Actions Edit View Help
systemctl start nessusd.service

systemctl status nessusd.service
● nessusd.service - The Nessus Vulnerability Scanner
     Loaded: loaded (/lib/systemd/system/nessusd.service; disabled; preset: disabled)
     Active: active (running) since Sat 2024-02-10 00:56:06 EST; 13s ago
   Main PID: 7753 (nessus-service)
      Tasks: 14 (limit: 2260)
     Memory: 114.4M
        CPU: 12.710s
     CGroup: /system.slice/nessusd.service
             ├─7753 /opt/nessus/sbin/nessus-service -q
             └─7754 nessusd -q

Feb 10 00:56:06 kali systemd[1]: Started nessusd.service - The Nessus Vulnerability Scanner.
Feb 10 00:56:08 kali nessus-service[7754]: Cached 0 plugin libs in 1msec
Feb 10 00:56:08 kali nessus-service[7754]: Cached 0 plugin libs in 0msec
```

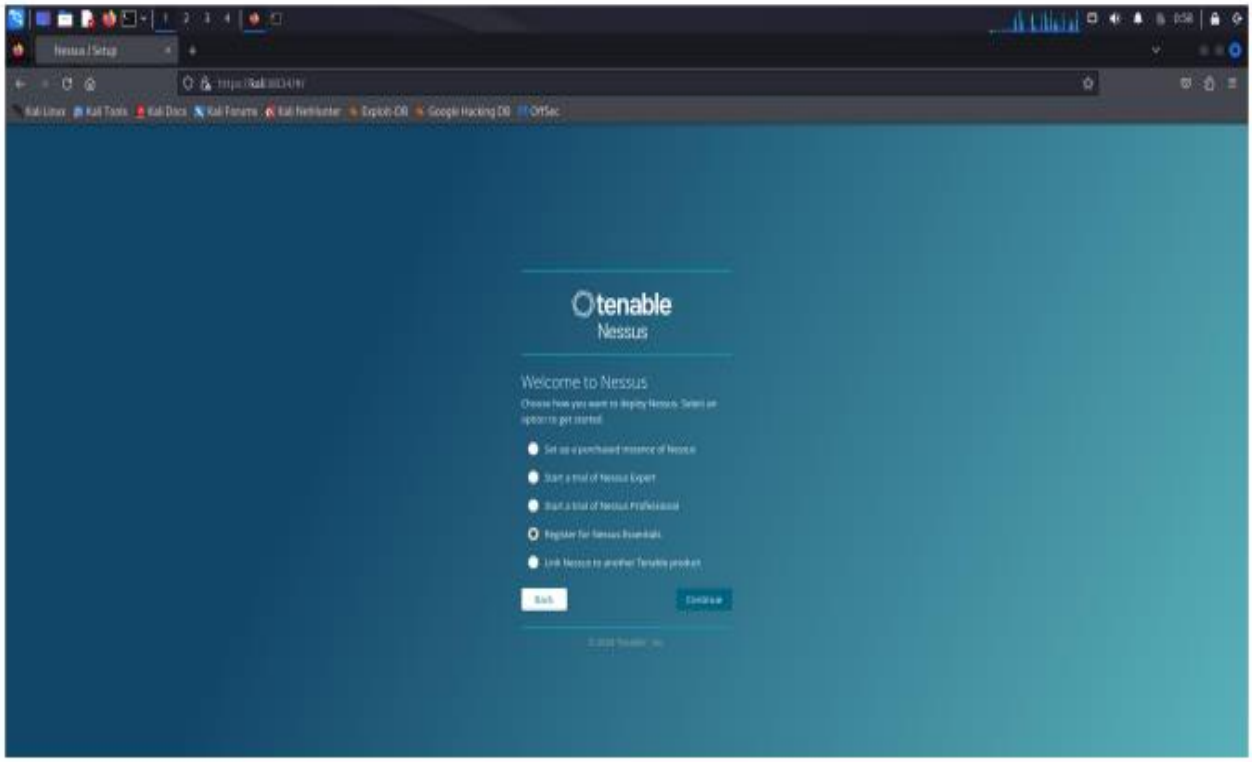
On your browser, go to **https://kali:8834/**. It would show a warning page.



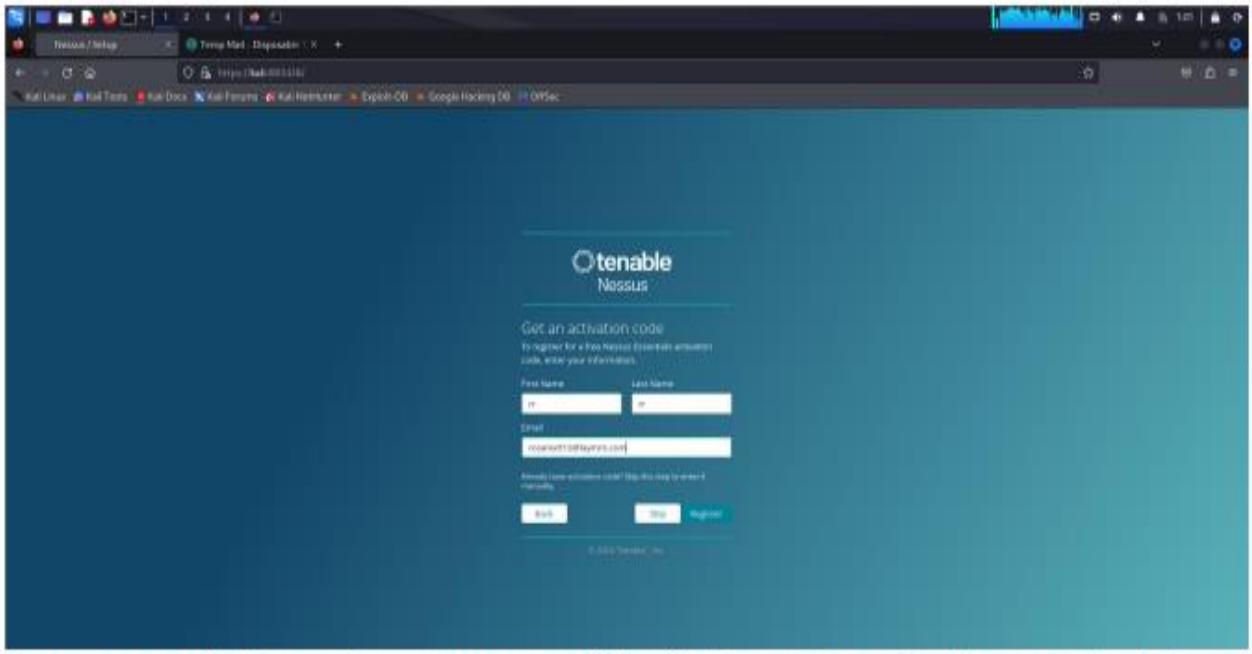
Click on Advanced. Then, click on Accept Risk and Continue.

7. Choose the Nessus Product you prefer. If you want the free version of Nessus, click on **Register Nessus Essentials.**

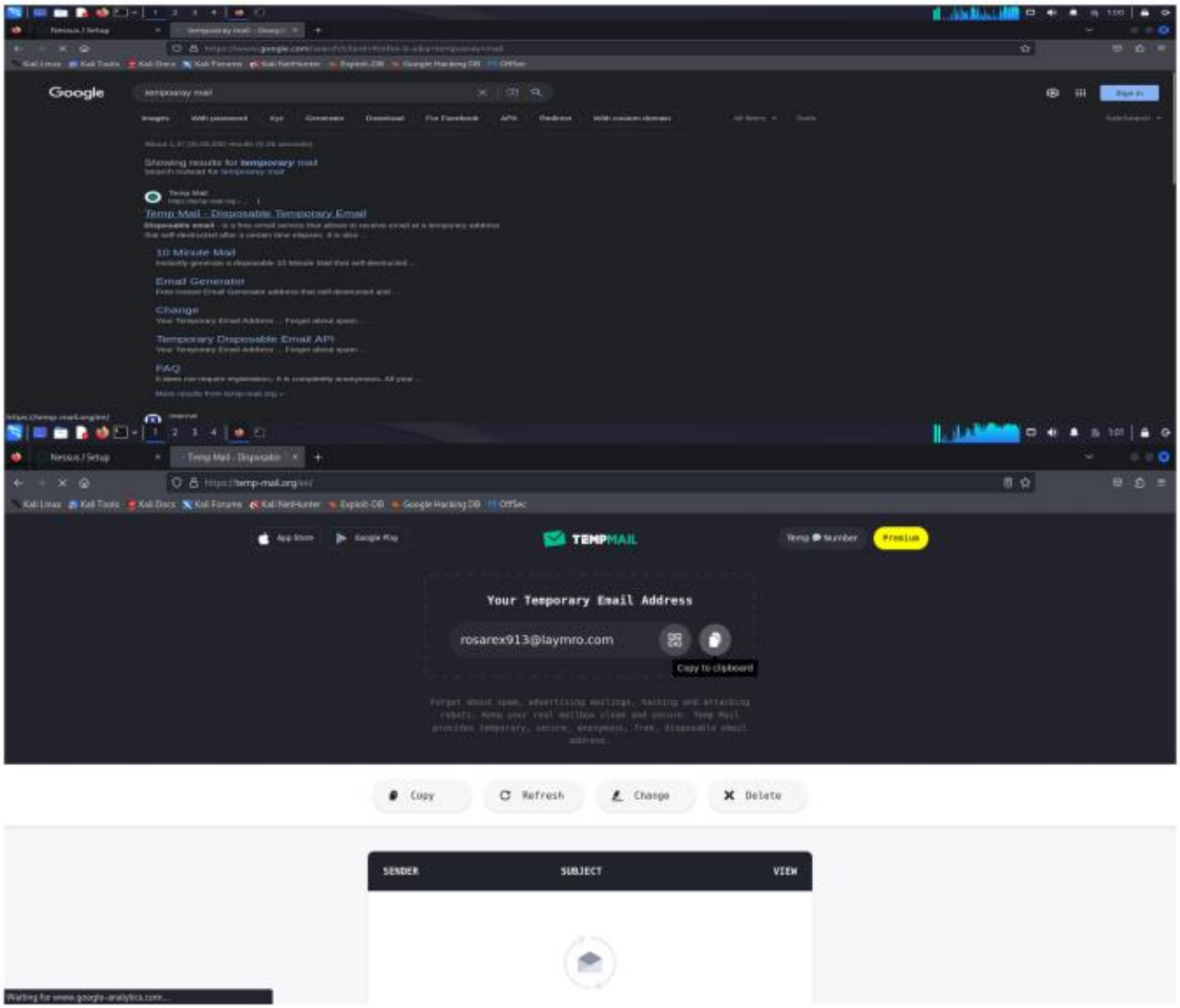




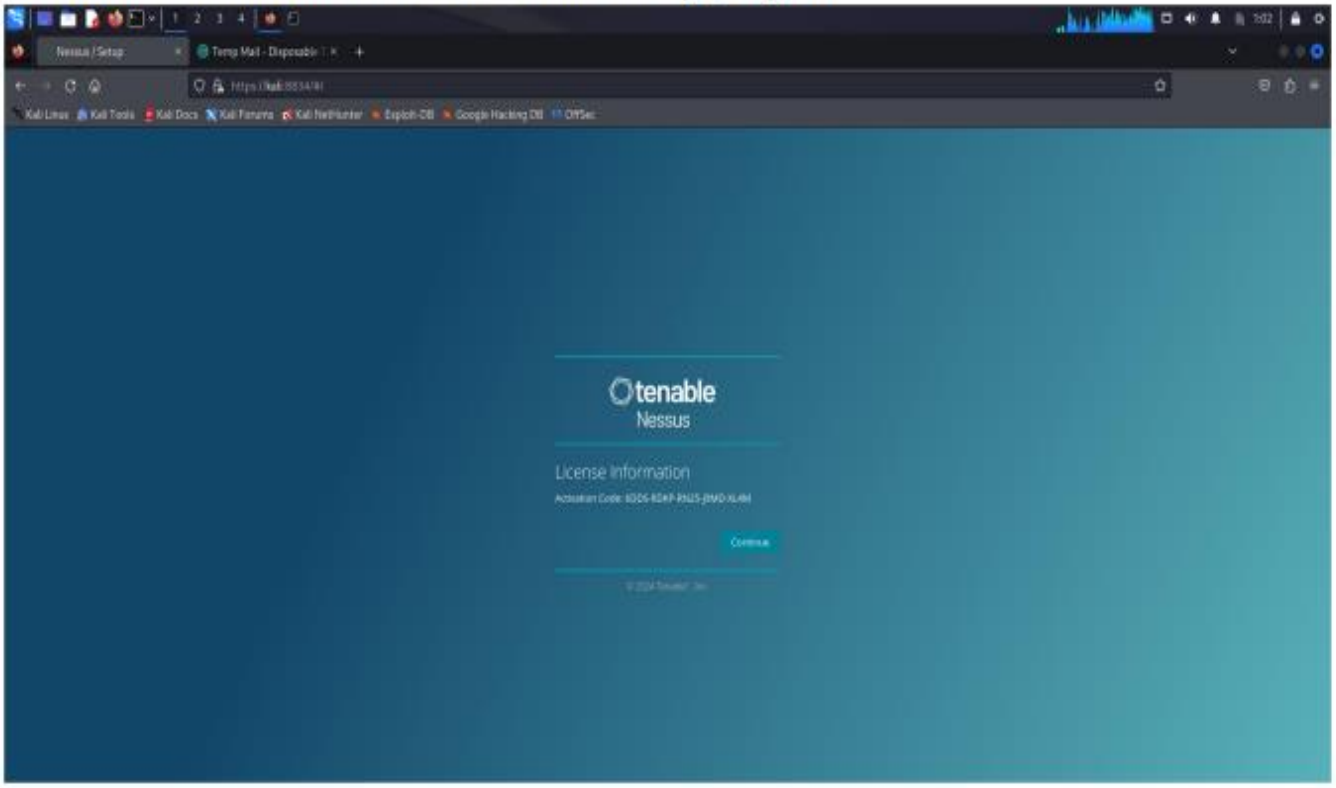
Enter your name and email address to receive an activation code by email. Paste the activation code into the space provided and choose a username and password.

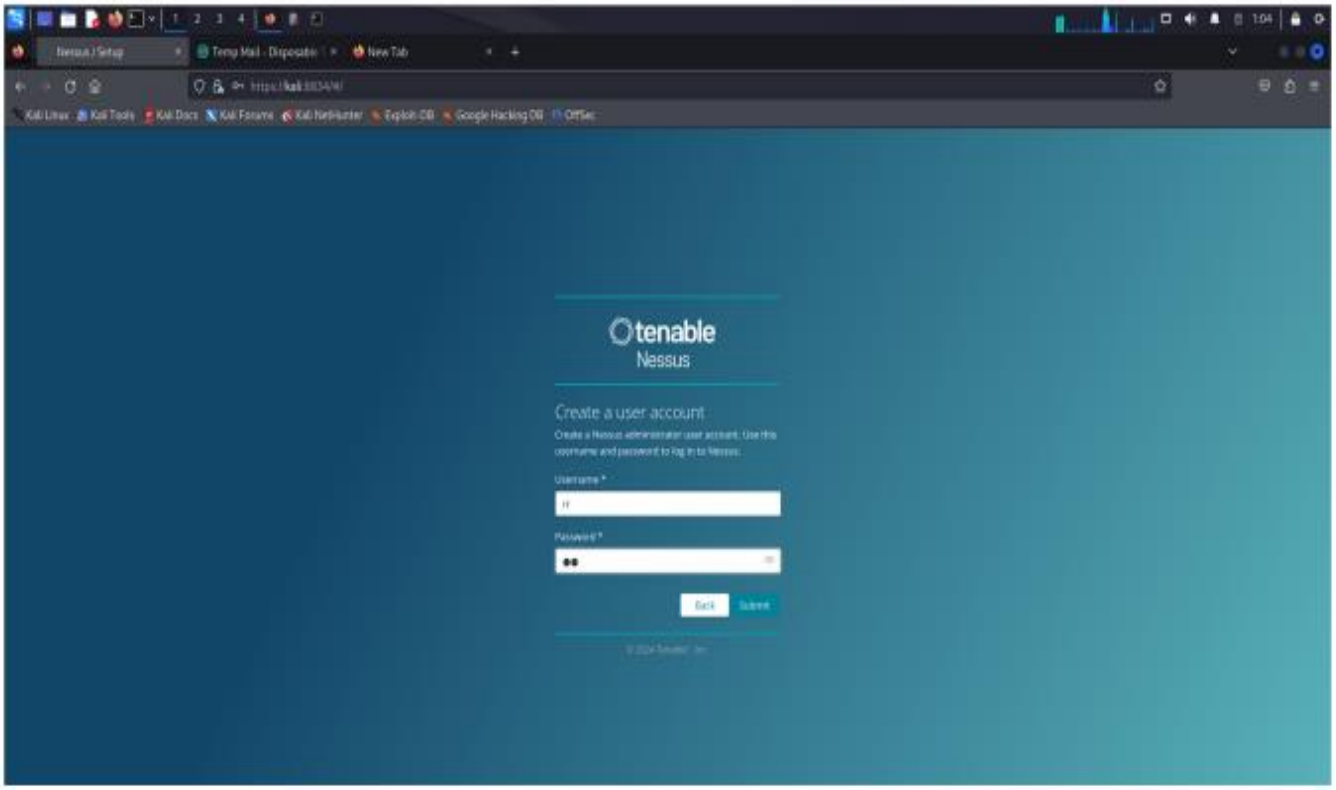


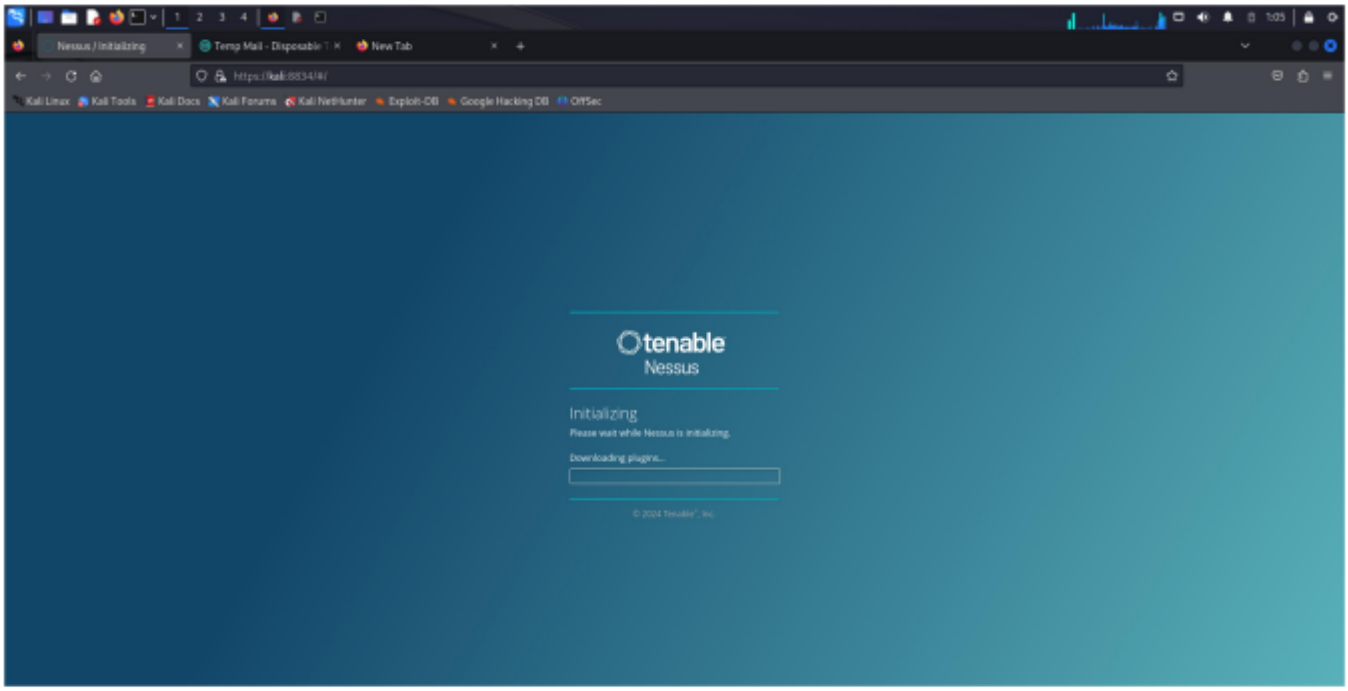
You can use emailaddress as temporary you can visit online temporary email address examples below

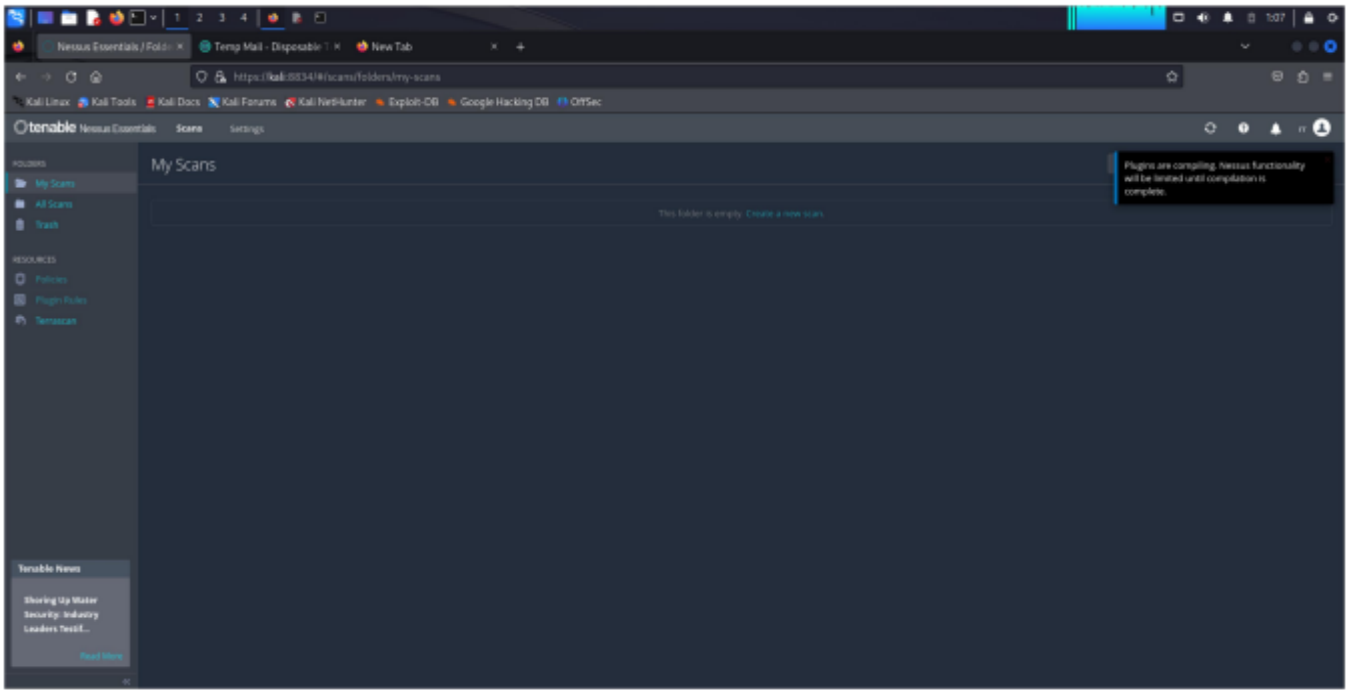

Google
temporary mail
Temp Mail - Disposable Temporary Email
10 Minute Mail
Email Generator
Change
Temporary Disposable Email API
FAQ
TEMPMAIL
Your Temporary Email Address
rosarex913@laymro.com
Copy to clipboard
Copy
Refresh
Change
Delete
SENDER
SUBJECT
VIEW

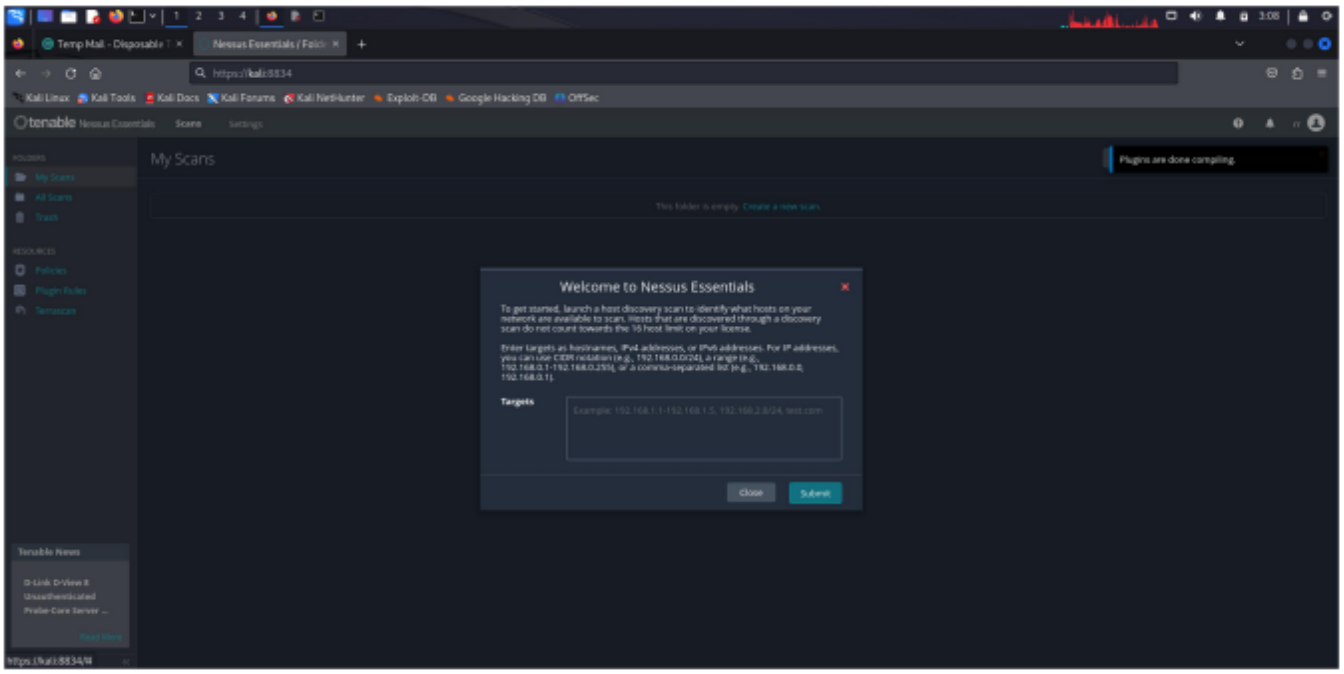
Allow Nessus to download the necessary plugins.



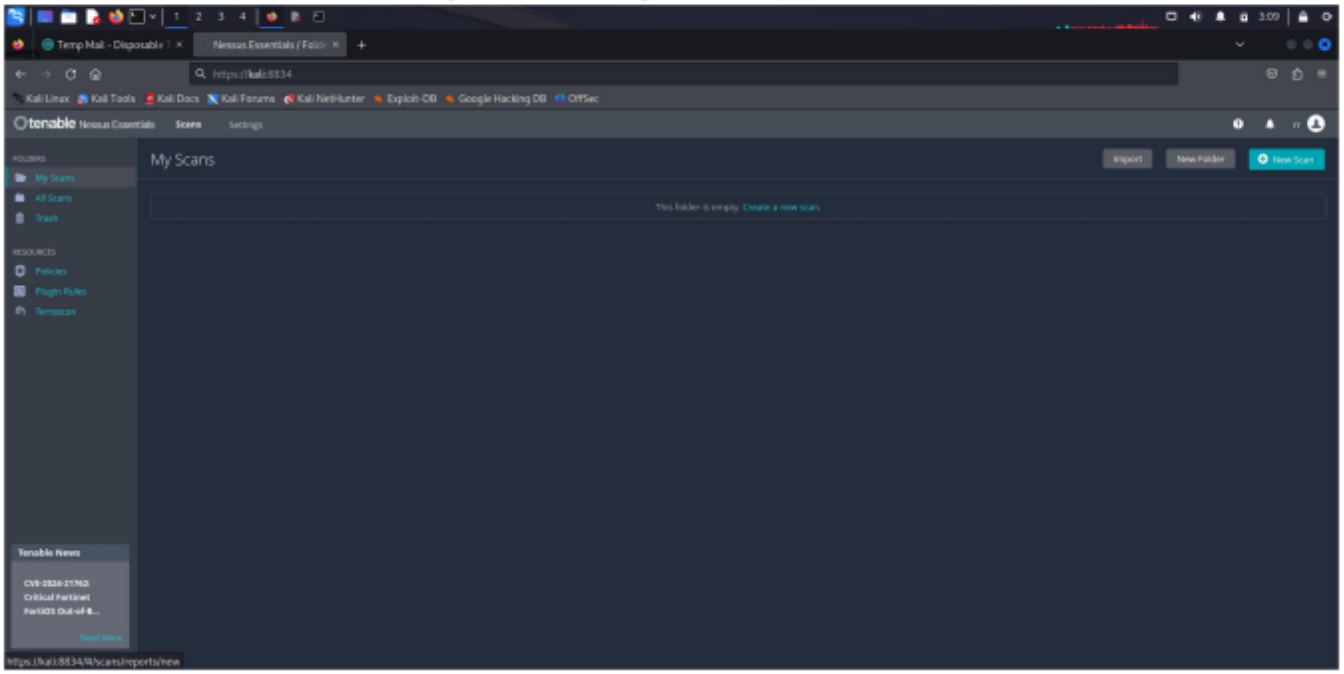



tenable
Nessus
Initializing
Please wait while Nessus is initializing.
Downloading plugins...

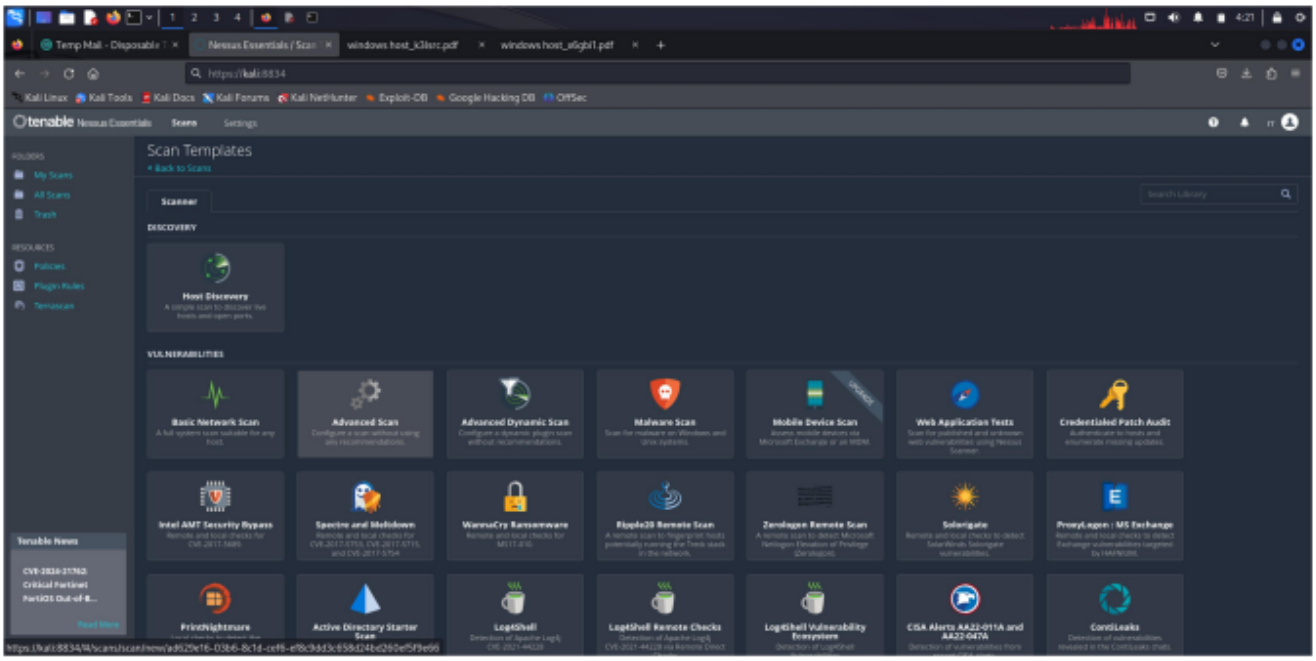

My Scans
Plugins are compiling. Nessus functionality will be limited until compilation is complete.



Click on **New Scan** to begin scanning for vulnerabilities

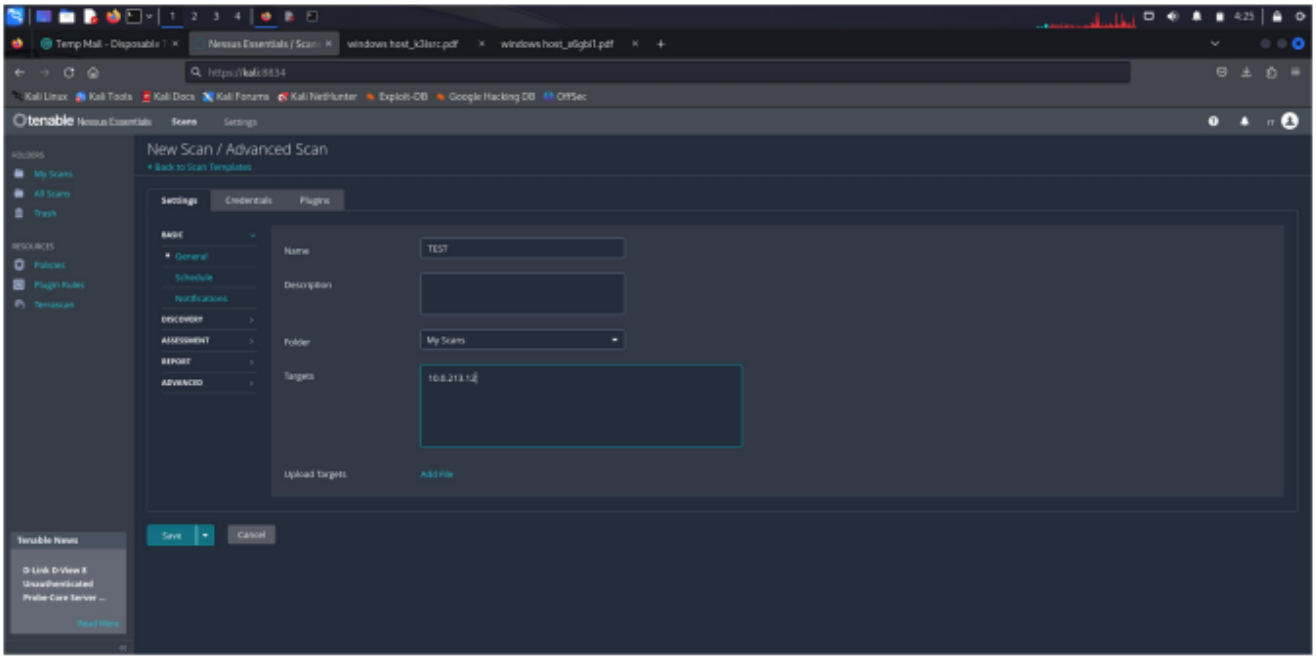


Click on Advance scan



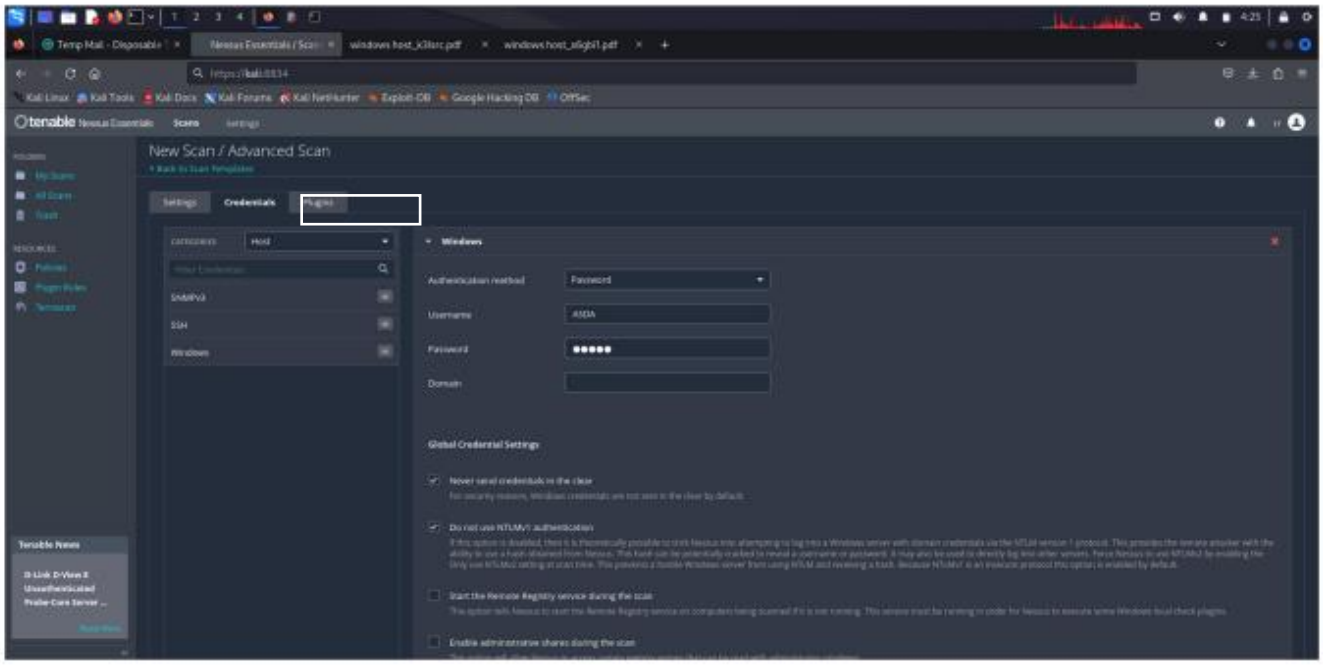
Give name for scaning (e.g test,windows scan..etc)

Give the ip address of your windows that you want to scan for vulnerabilities in Target box shown in the below

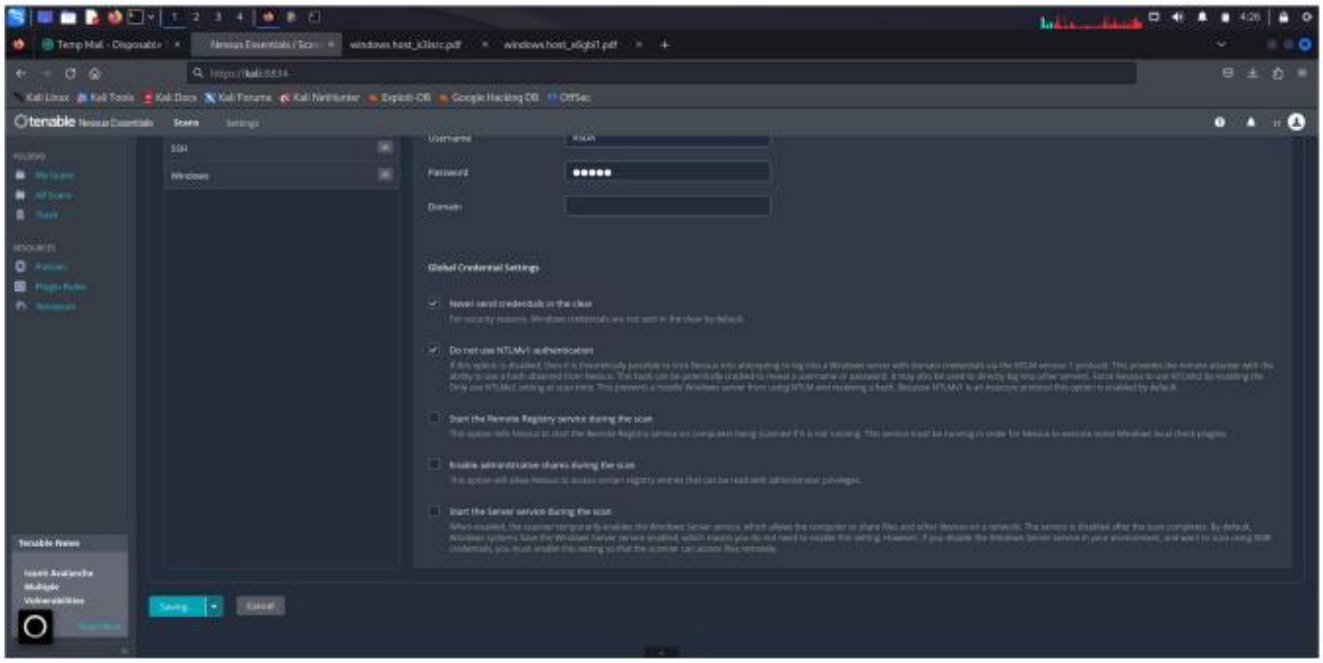


Give the credentials of your windows like username and password if you known (OPTIONAL).

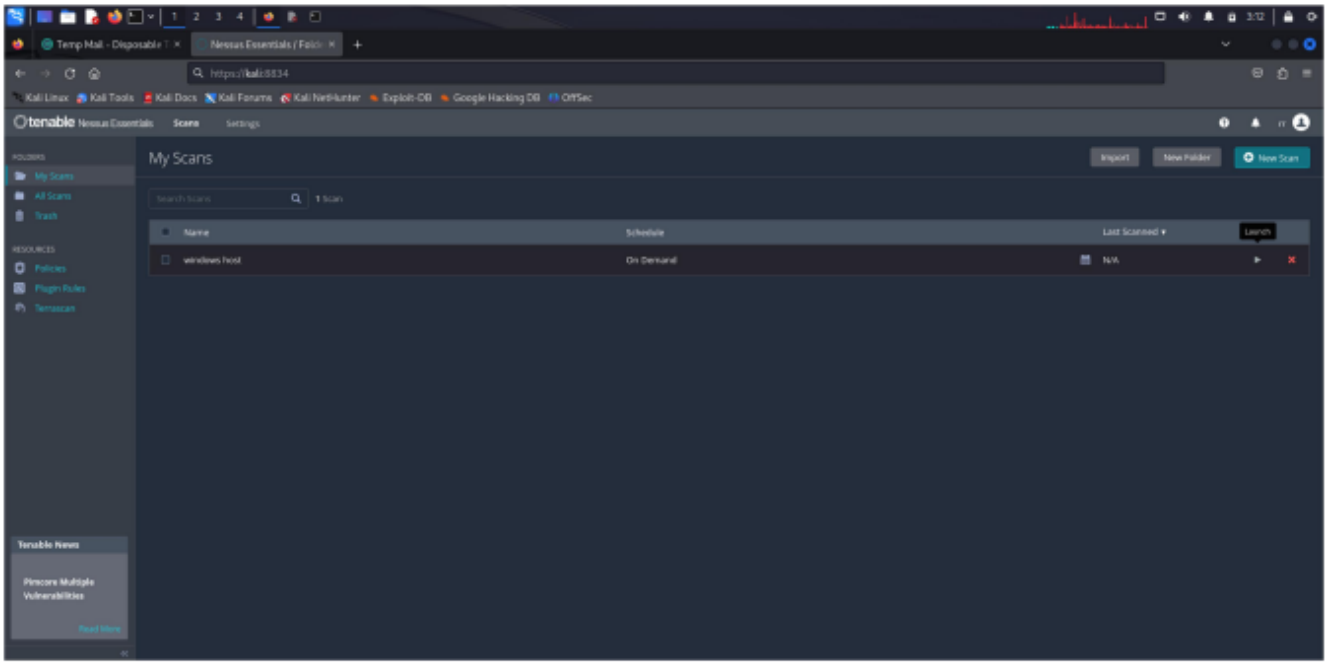
NOTE:- Use of giving credential it will help you scan more into your system.



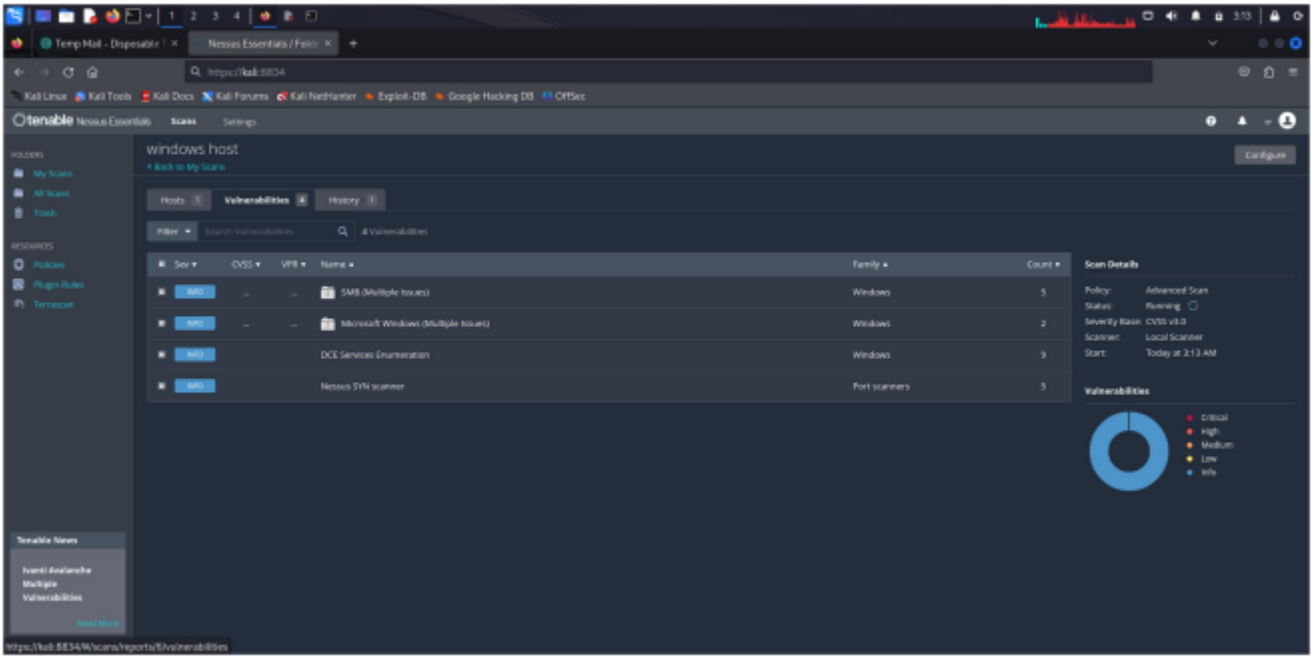
Go down and save the Progress

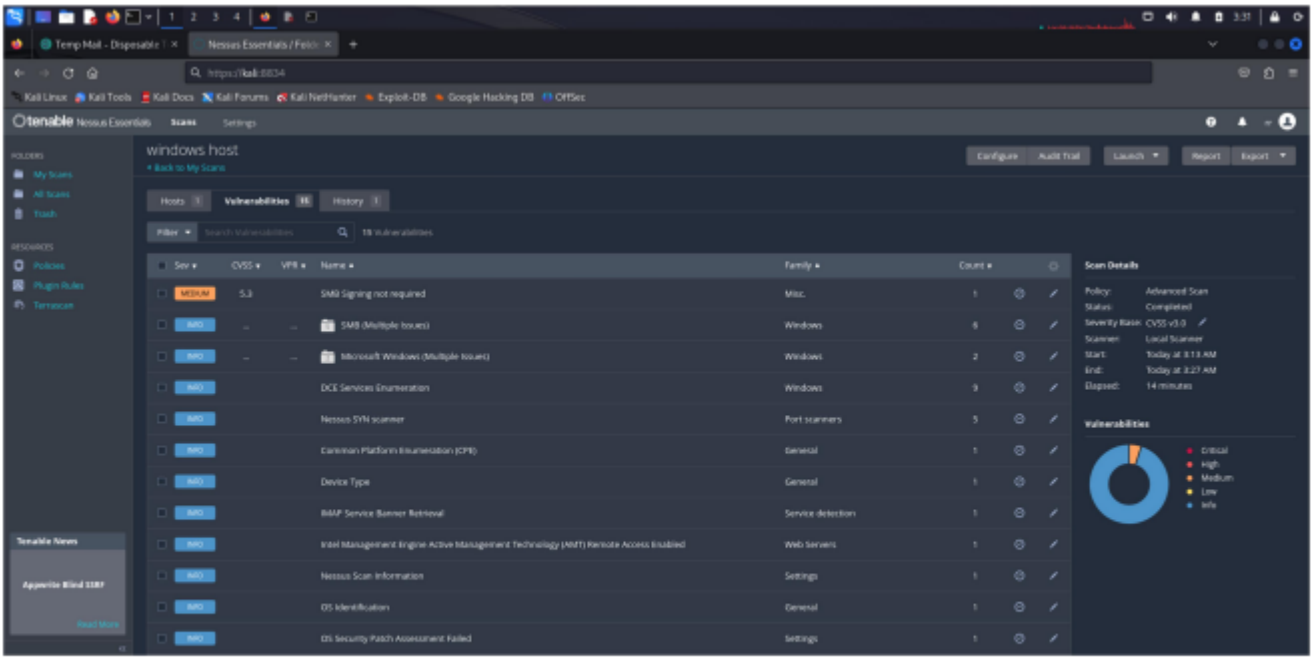


Click on launch

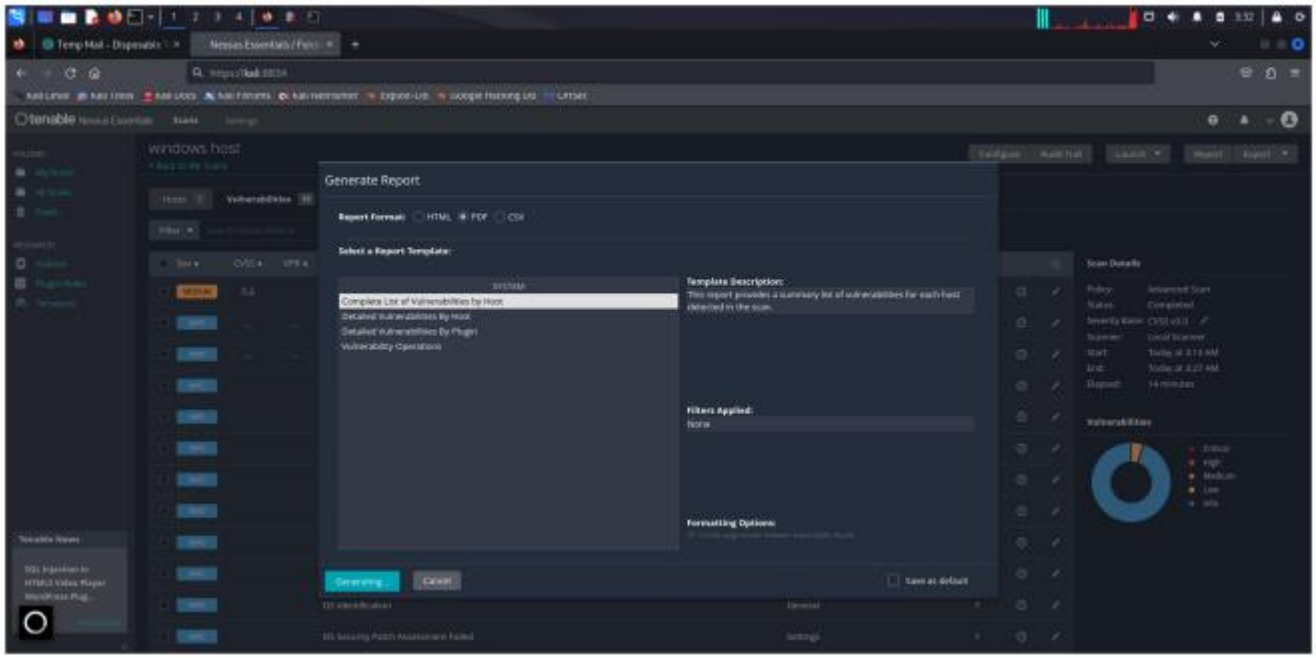


Wait for Some time to get the Output.





ON RIGHT SIDE CLICK ON REPORT TO GENERATE THE ENTIRE REPORT OF YOUR SYSTEM VULNERABILITY


Generate Report
Report Format:
HTML
PDF
CSV
Select a Report Template:
Complete List of Vulnerabilities by Host
Detailed Vulnerabilities By Host
Detailed Vulnerabilities By Plugin
Vulnerability Operations
Template Description:
Filters Applied:
None
Formatting Options:
Generating...
Cancel
Save as default

Practical – 6

Aim :- Implementation to identify web vulnerabilities, using OWASP project.

Theory :-

Introducing ZAP:-

Zed Attack Proxy (ZAP) is a free, open-source penetration testing tool being maintained under the umbrella of the Open Web Application Security Project (OWASP). ZAP is designed specifically for testing web applications and is both flexible and extensible. At its core, ZAP is what is known as a "man-in-the-middle proxy." It stands between the tester's browser and the web application so that it can intercept and inspect messages sent between browser and web application, modify the contents if needed, and then forward those packets on to the destination. It can be used as a stand-alone application, and as a daemon process.

If there is another network proxy already in use, as in many corporate environments, ZAP can be configured to connect to that proxy.

ZAP provides functionality for a range of skill levels – from developers, to testers new to security testing, to security testing specialists. ZAP has versions for each major OS and Docker, so you are not tied to a single OS. Additional functionality is freely available from a variety of add-ons in the ZAP Marketplace, accessible from within the ZAP client. Because ZAP is open-source, the source code can be examined to see exactly how the functionality is implemented. Anyone can volunteer to work on ZAP, fix bugs, add features, create pull requests to pull fixes into the project, and author add-ons to support specialized situations.

Install and Configure ZAP

ZAP has installers for Windows, Linux, and Mac OS/X. There are also Docker images available on the download site listed below.

Install ZAP The first thing to do is install ZAP on the system you intend to perform pentesting on. Download the appropriate installer from ZAP's download location at https://www.zaproxy.org/download/ and execute the installer.

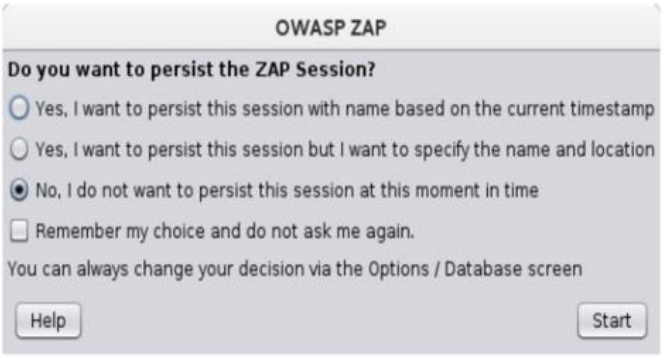
Note that ZAP requires Java 8+ in order to run. The Mac OS/X installer includes an appropriate version of Java but you must install Java 8+ separately for Windows, Linux, and Cross-Platform versions. The Docker versions do not require you to install Java.

Once the installation is complete, launch ZAP and read the license terms. Click Agree if you accept the terms, and ZAP will finish installing, then ZAP will automatically start.

Persisting a Session When you first start ZAP, you will be asked if you want to persist the ZAP session. By default, ZAP sessions are always recorded to disk in a HSQLDB database with a default name and location.

If you do not persist the session, those files are deleted when you exit ZAP.

If you choose to persist a session, the session information will be saved in the local database so you can access it later, and you will be able to provide custom names and locations for saving the files.



For now, select No, I do not want to persist this session at this moment in time, then click Start. The ZAP sessions will not be persisted for now.

ZAP Desktop UI:
The ZAP Desktop UI is composed of the following elements:
1**. Menu Bar** – Provides access to many of the automated and manual tools.

2. **Toolbar** – Includes buttons which provide easy access to most commonly used features.

3. **Tree Window** – Displays the Sites tree and the Scripts tree.

4. **Workspace Window** – Displays requests, responses, and scripts and allows you to edit them.

5. **Information Window** – Displays details of the automated and manual tools.

6. **Footer** – Displays a summary of the alerts found and the status of the main automated tools.

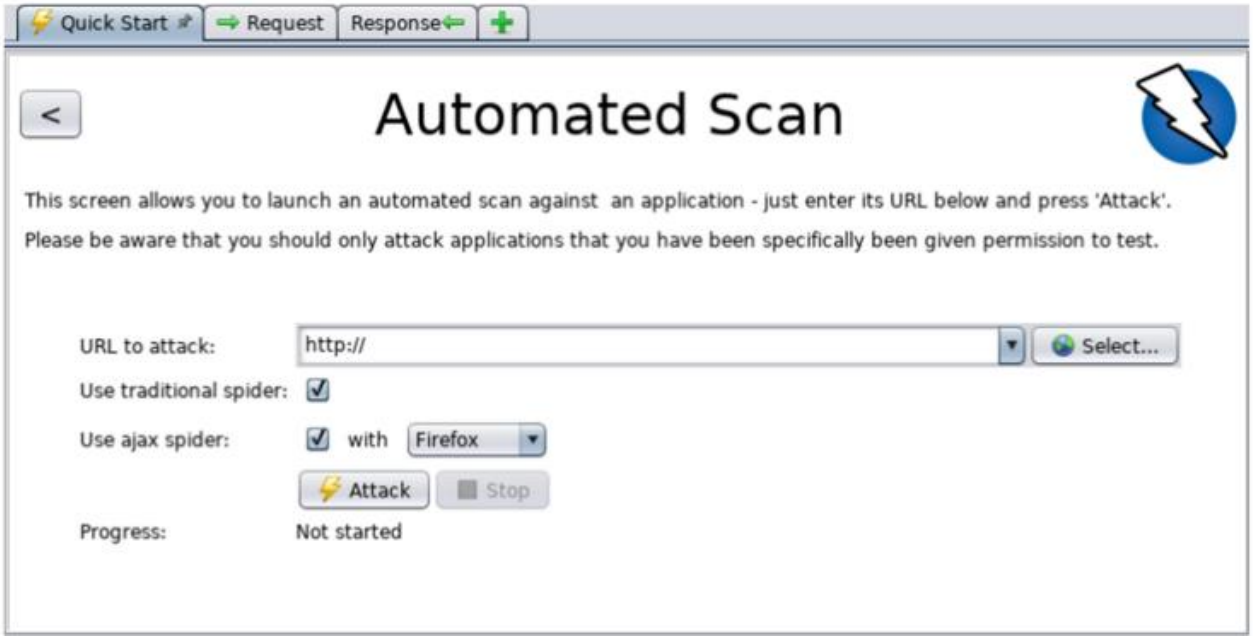
Running an Automated Scan
The easiest way to start using ZAP is via the Quick Start tab. Quick Start is a ZAP add-on that is included automatically when you installed ZAP. To run a Quick Start Automated Scan :

1. Start ZAP and click the Quick Start tab of the Workspace Window.

2. Click the large Automated Scan button.

3. In the URL to attack text box, enter the full URL of the web application you want to attack.

4. Click the Attack button.



- ZAP will proceed to crawl the web application with its spider and passively scan each page it finds. Then ZAP will use the active scanner to attack all of the discovered pages, functionality, and parameters.

- ZAP provides 2 spiders for crawling web applications, you can use either or both of them from this screen.

- The traditional ZAP spider which discovers links by examining the HTML in responses from the web application. This spider is fast, but it is not always effective when exploring an AJAX web application that generates links using JavaScript.

- For AJAX applications, ZAP's AJAX spider is likely to be more effective. This spider explores the web application by invoking browsers which then follow the links that have been generated. The AJAX spider is slower than the traditional spider and requires additional configuration for use in a "headless" environment.

- ZAP will passively scan all of the requests and responses proxied through it. So far ZAP has only carried out passive scans of your web application. Passive scanning does not change responses in any way and is considered safe. Scanning is also performed in a background thread to not slow down exploration.

- Passive scanning is good at finding some vulnerabilities and as a way to get a feel for the basic security state of a web application and locate where more investigation may be warranted. Active scanning, however, attempts to find other vulnerabilities by using known attacks against the selected targets.

- Active scanning is a real attack on those targets and can put the targets at risk, so do not use active scanning against targets you do not have permission to test.

See Explored Pages

To examine a tree view of the explored pages, click the Sites tab in the Tree Window. You can expand the nodes to see the individual URLs accessed.

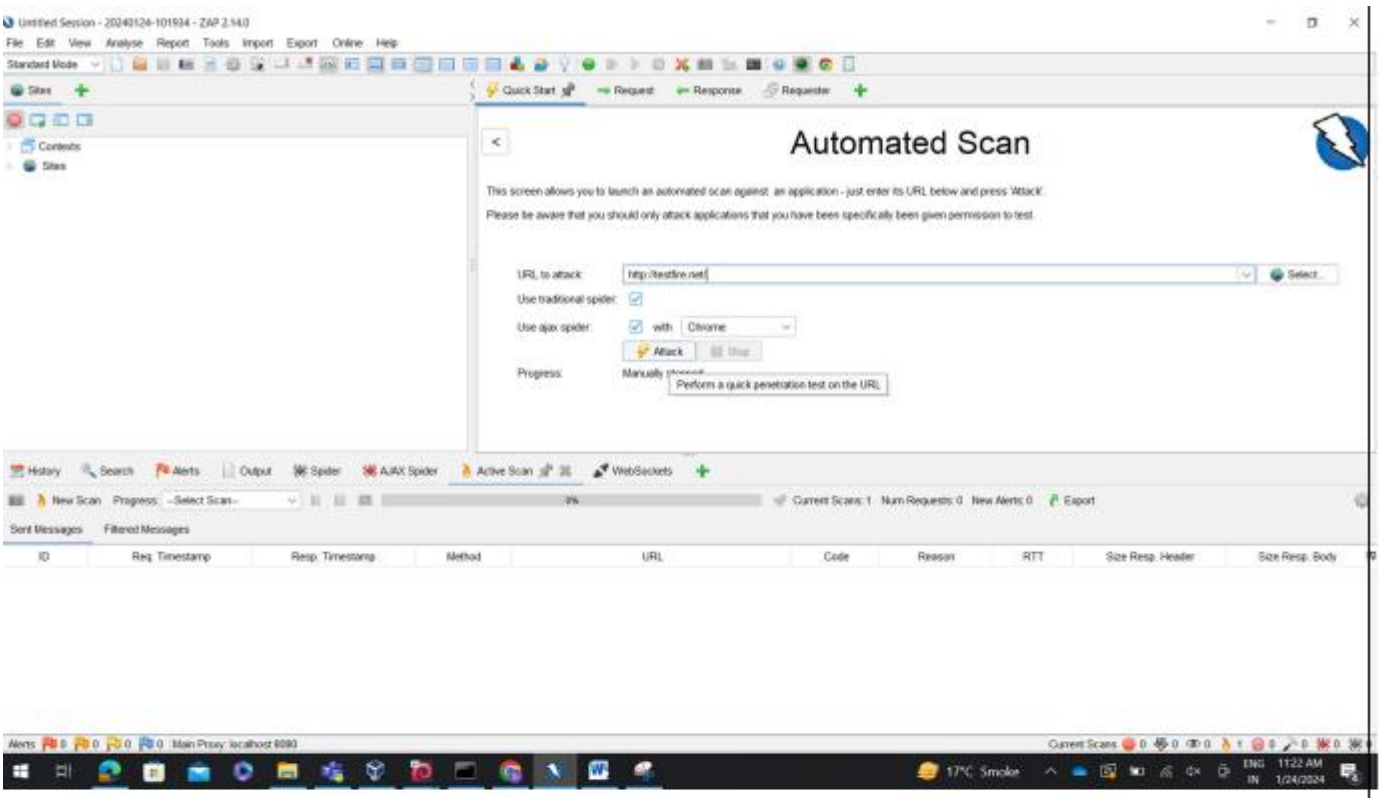
View Alerts and Alert Details

The left-hand side of the Footer contains a count of the Alerts found during your test, broken out into risk categories. These risk categories are:

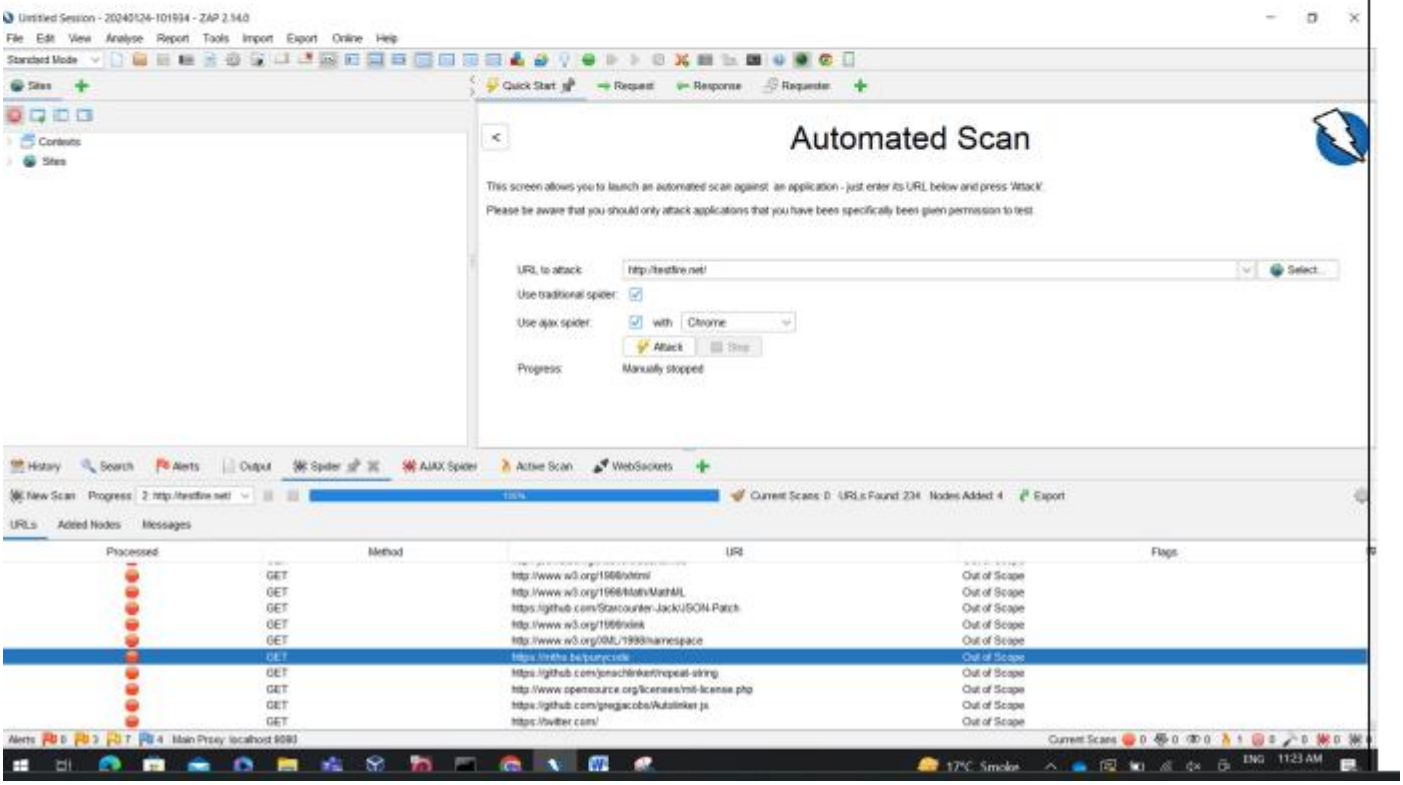
To view the alerts created during your test:

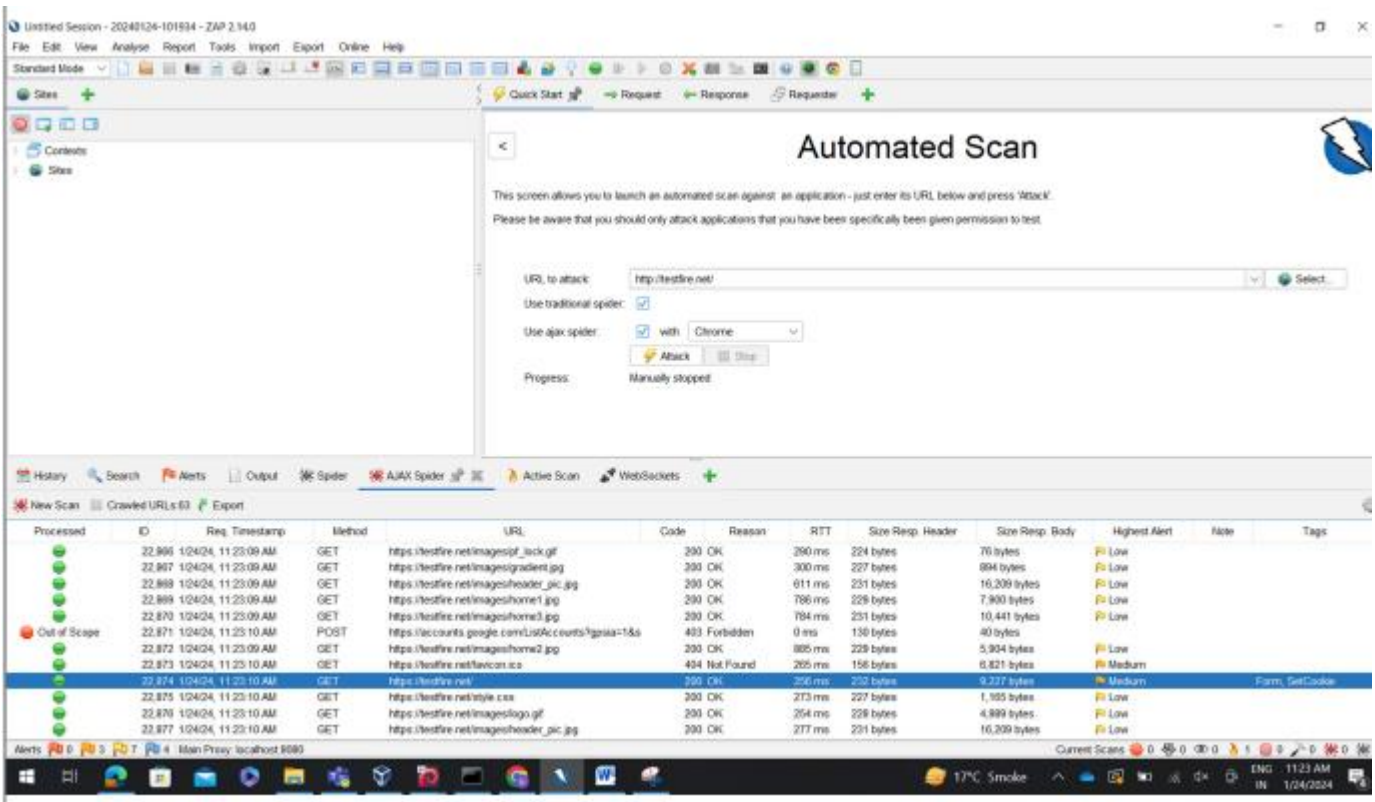
1. Click the Alerts tab in the Information Window.
2. Click each alert displayed in that window to display the URL and the vulnerability detected in the right side of the Information Window.
3. In the Workspace Windows, click the Response tab to see the contents of the header and body of the response. The part of the response that generated the alert will be highlighted.

Here are the Outputs of a Sample bank website follow the images below step by step



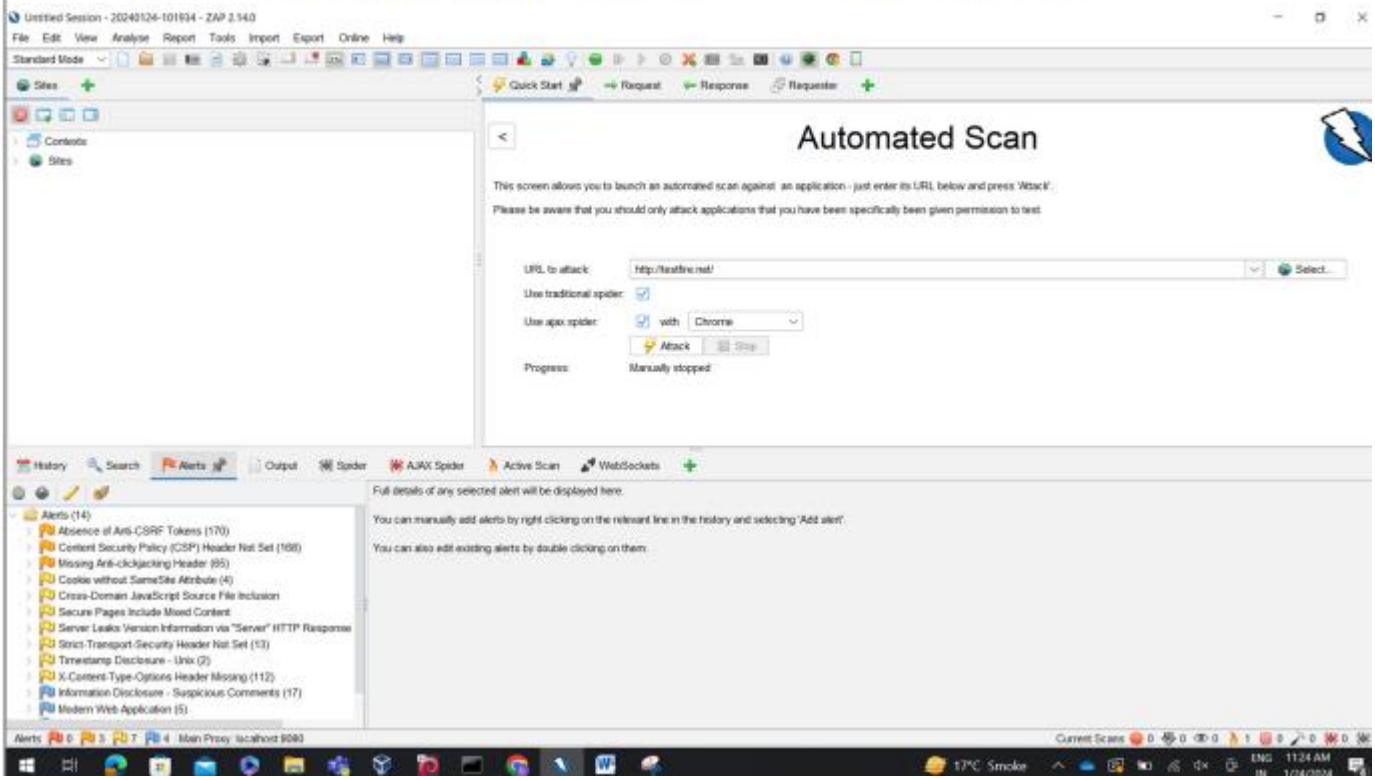
CLICK ON ATTACK BUTTON

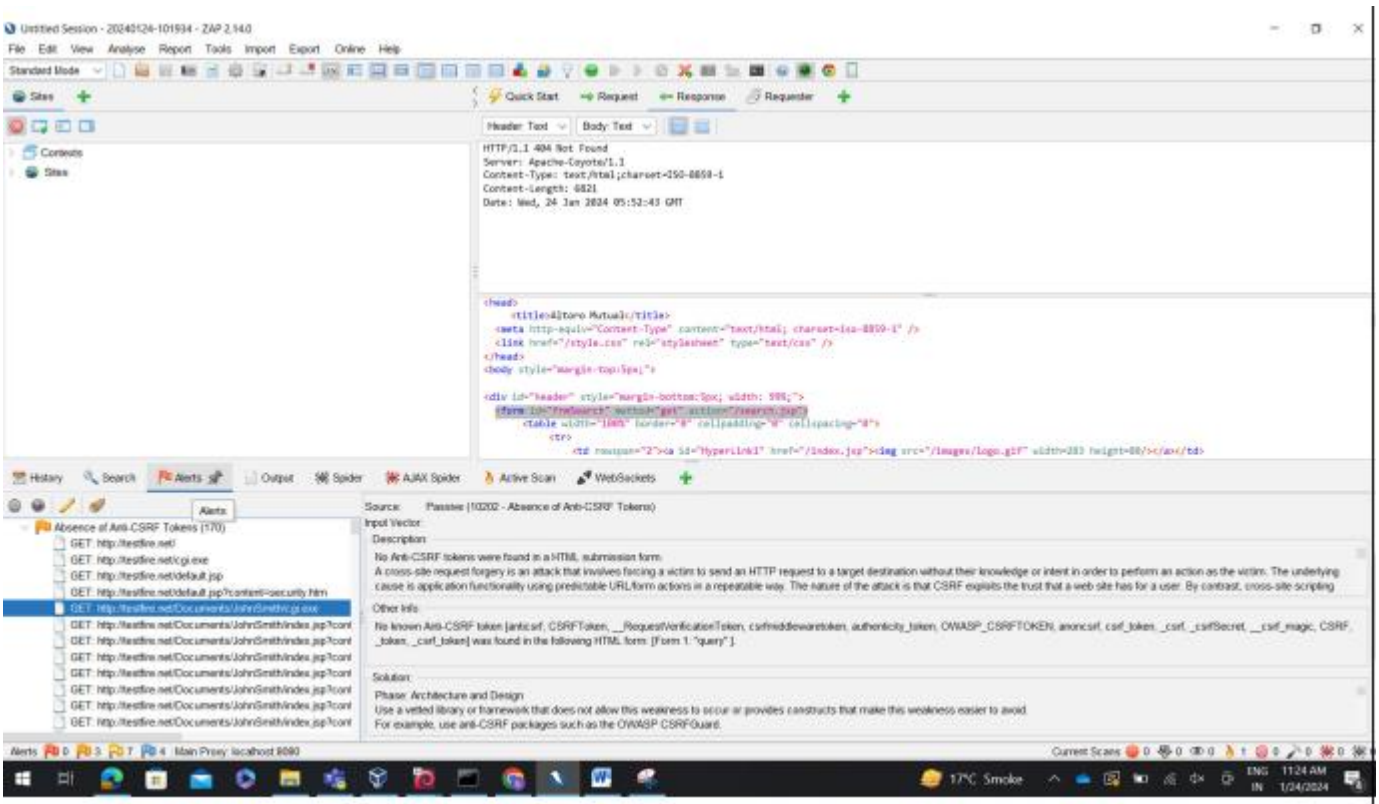




CHECK THE OUTPUT OF BELOW DASHBORD IN IMAGE

CLICK ON ALERT OPTION TO CHECK VULNERABLITIES IN BELOW IMAGE





SELECT ANY LINK CHECK THAT DESCRIPTION ABOUT VULNERABILITY