Practical: 1

Aim: File System Analysis using The SleuthKit (Autospy).

Theory

Sleuth Kit is a collection of command line tools and a C library that allows you to analyze disk images and recover files from them. It is used behind the scenes in Autopsy and many other opensource forensics tools.

There are multiple techniques that could be used to perform the analysis on the files, listed below are the techniques that could be used.

img_stat: It displays the details associated with the image files.

fls: It displays files and directory in a disk image

fsstat: It displays general details of a file system.

istat: It displays details of a meta-data structure (i.e. inode).

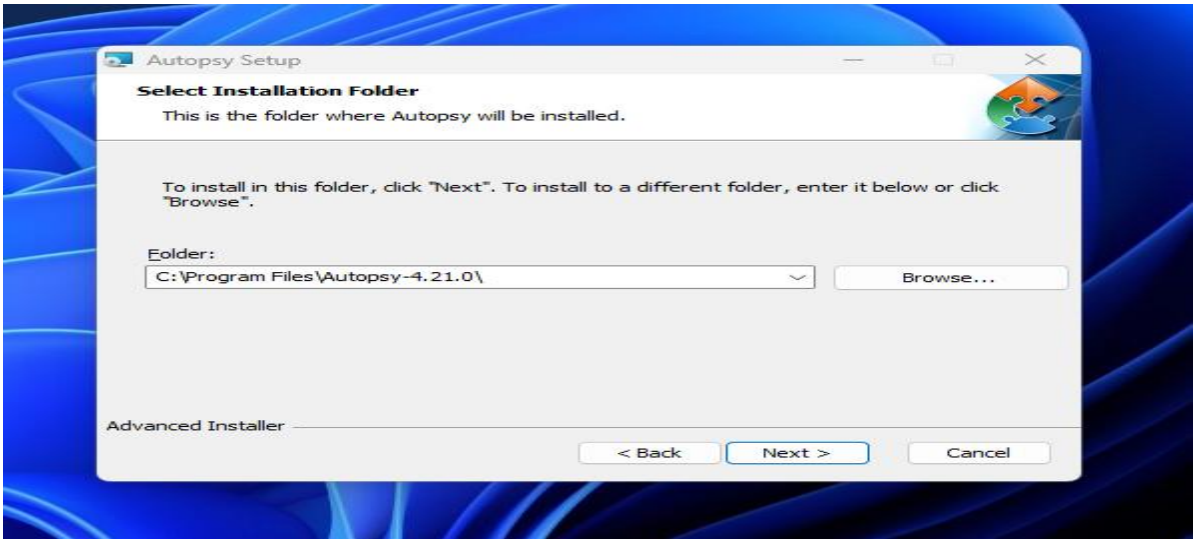
Autopsy: It is a digital forensics platform and graphical interface to the Sleuth Kit and other digital forensics too

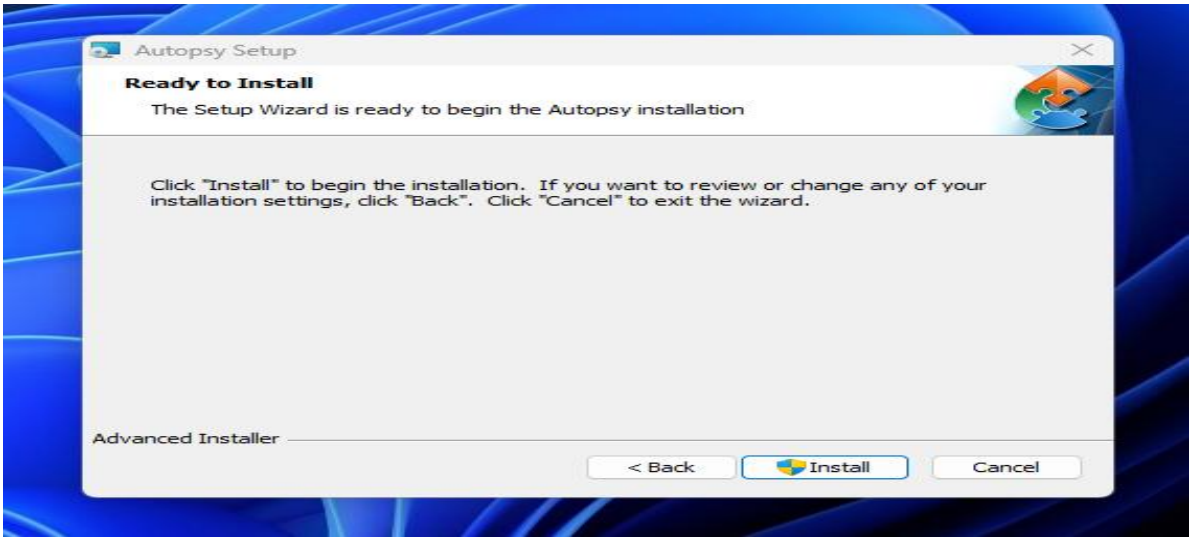
Autopsy is a digital forensics platform and graphical interface to The Sleuth Kit® and other digital forensics tools. It is used by law enforcement, military, and corporate examiners to investigate what happened on a computer. You can even use it to recover photos from your camera's memory card.

Autopsy is an easy to use, GUI-based program that allows you to efficiently analyze hard drives and smart phones. It has a plug-in architecture that allows you to find add-on modules or develop custom modules in Java or Python.

Easy to Use

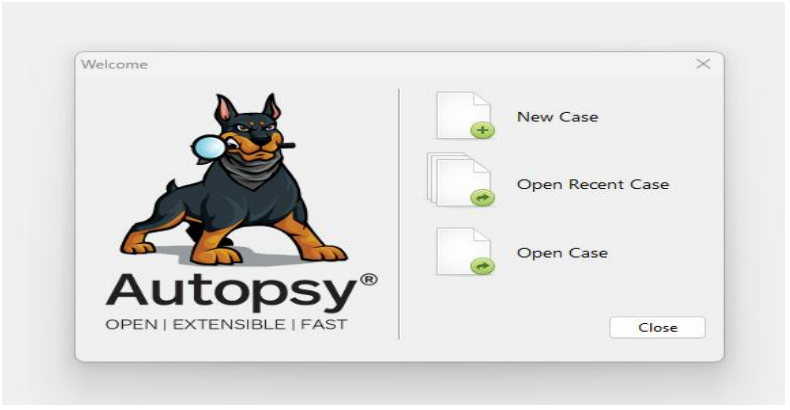
Autopsy was designed to be intuitive out of the box. Installation is easy and wizards guide you through every step. All results are found in a single tree



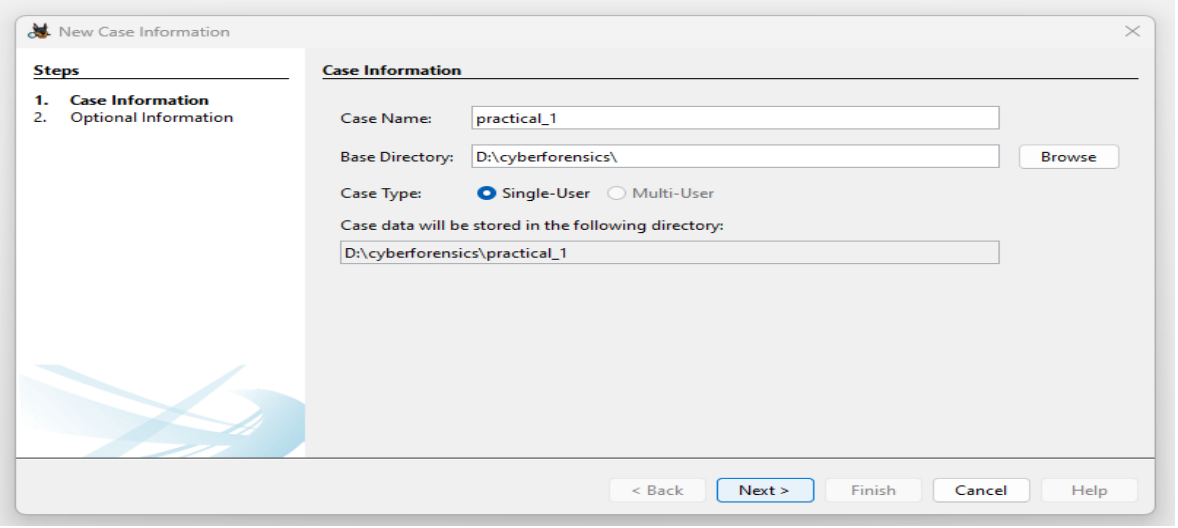


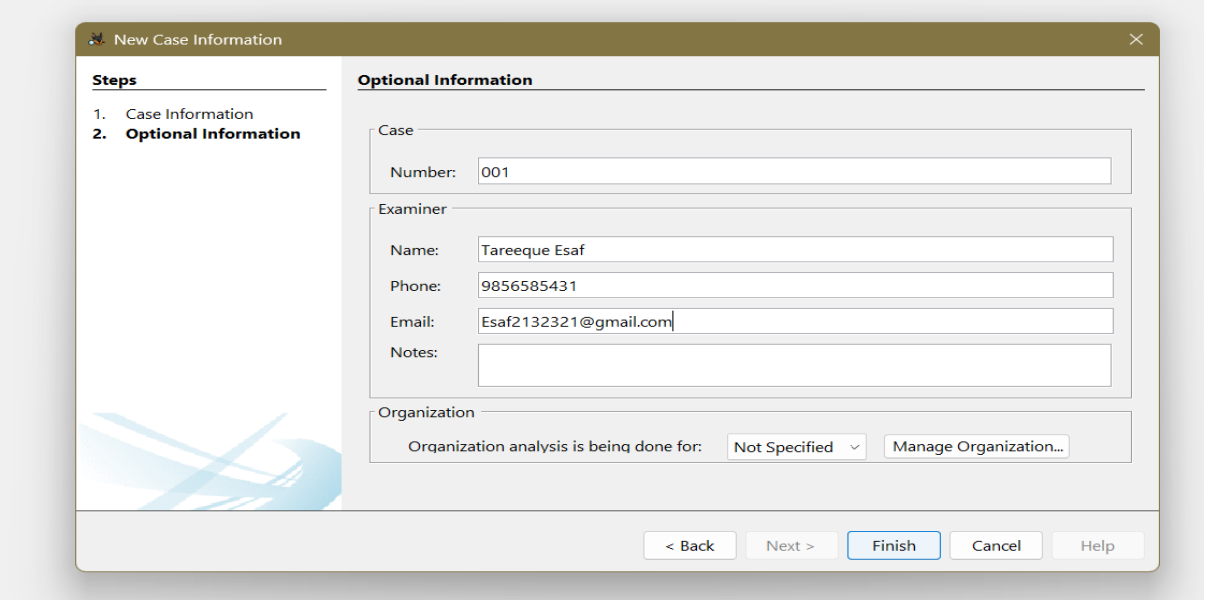
Step 1- Start a New Case

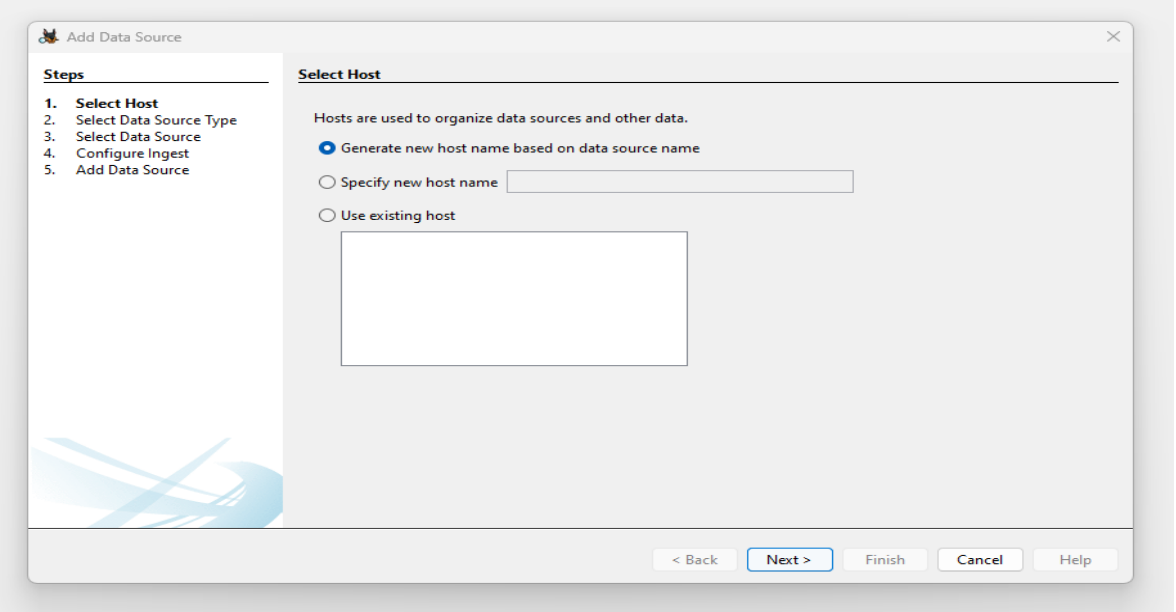
Click New Case. This will add a new case folder to the system and allow you to begin adding evidence. To begin, click New Case.



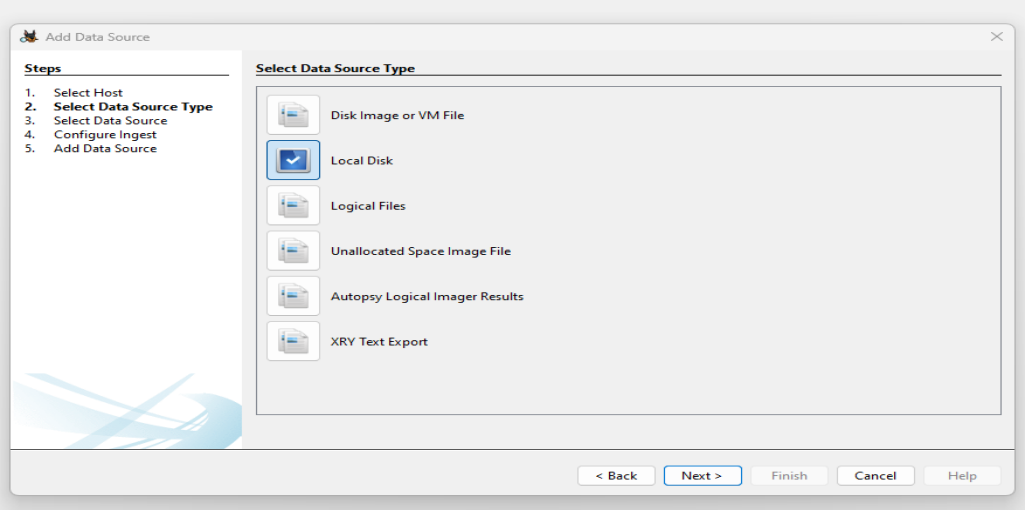
Step 2-Enter the Case Details

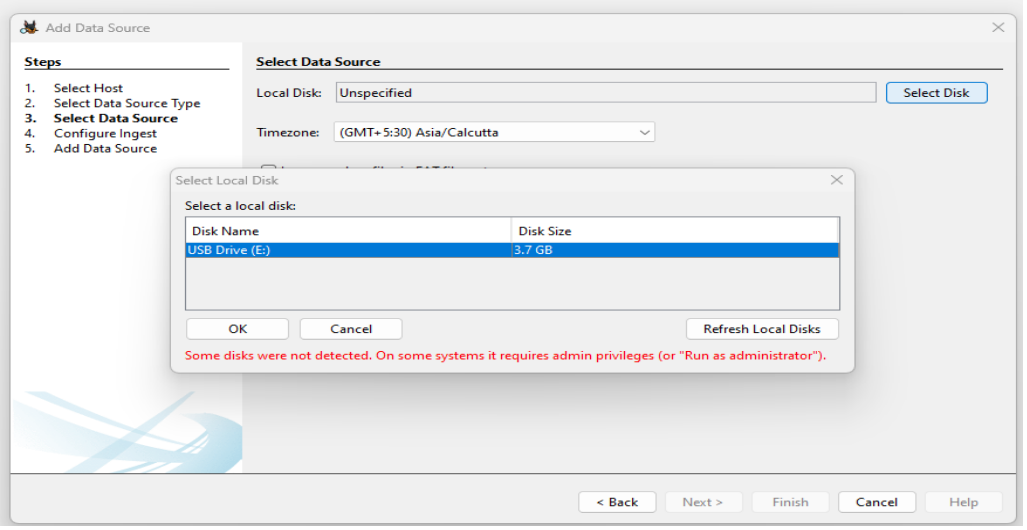


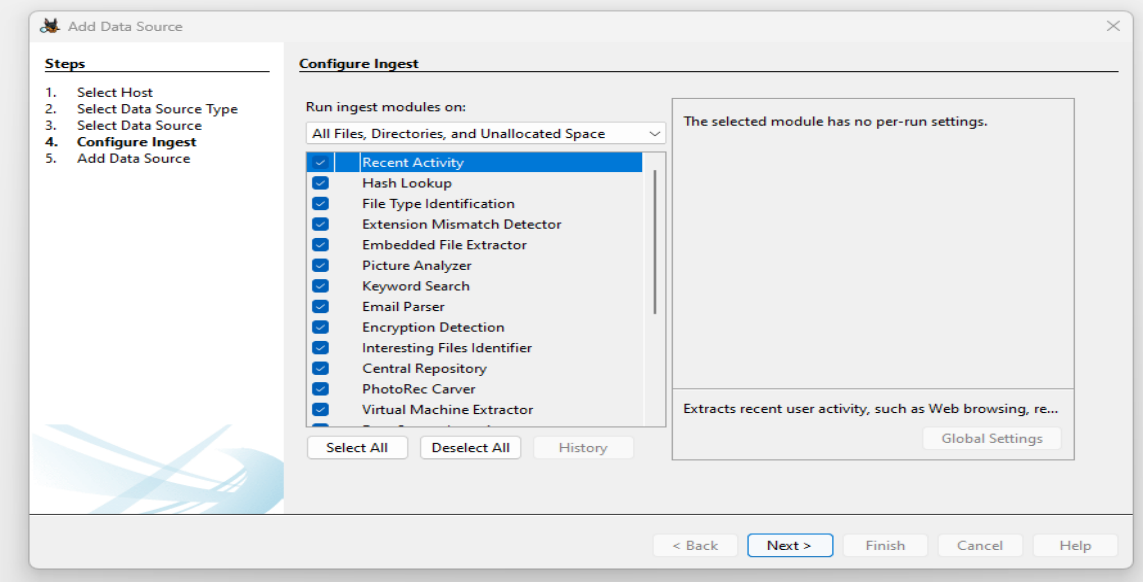




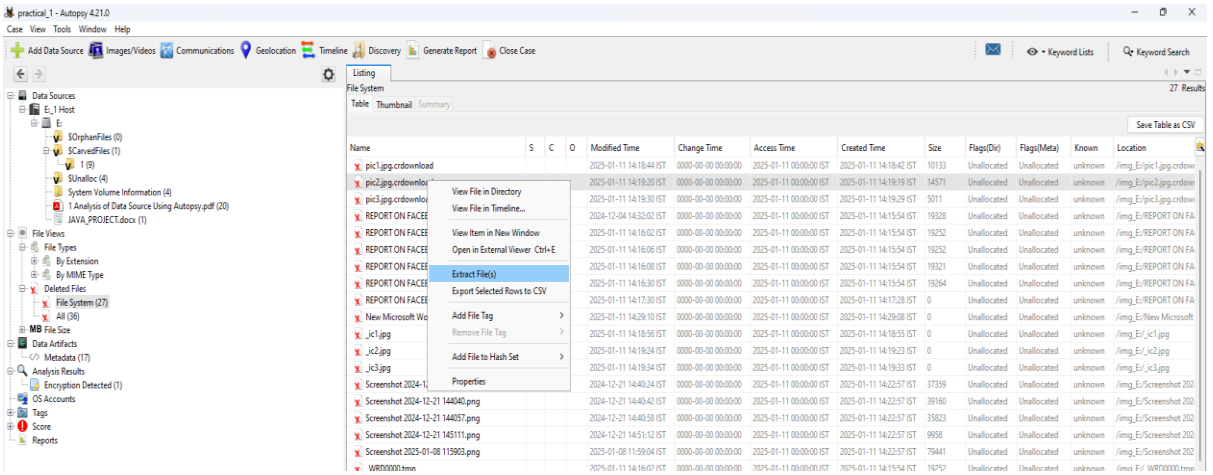
Step 3 -Choose the path

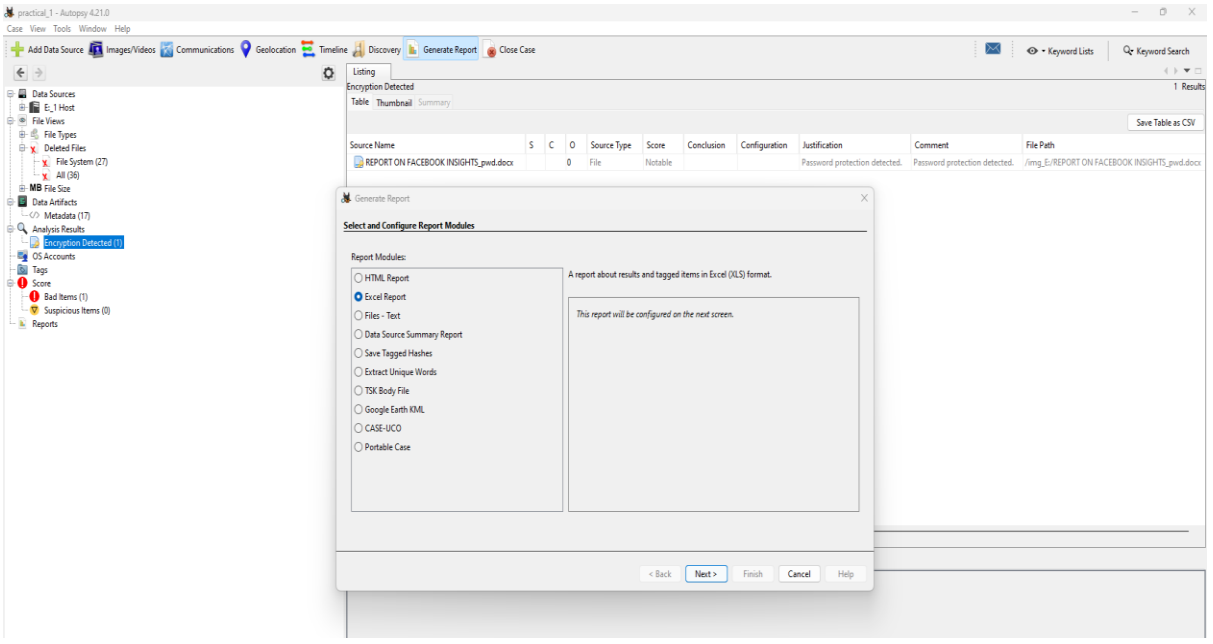


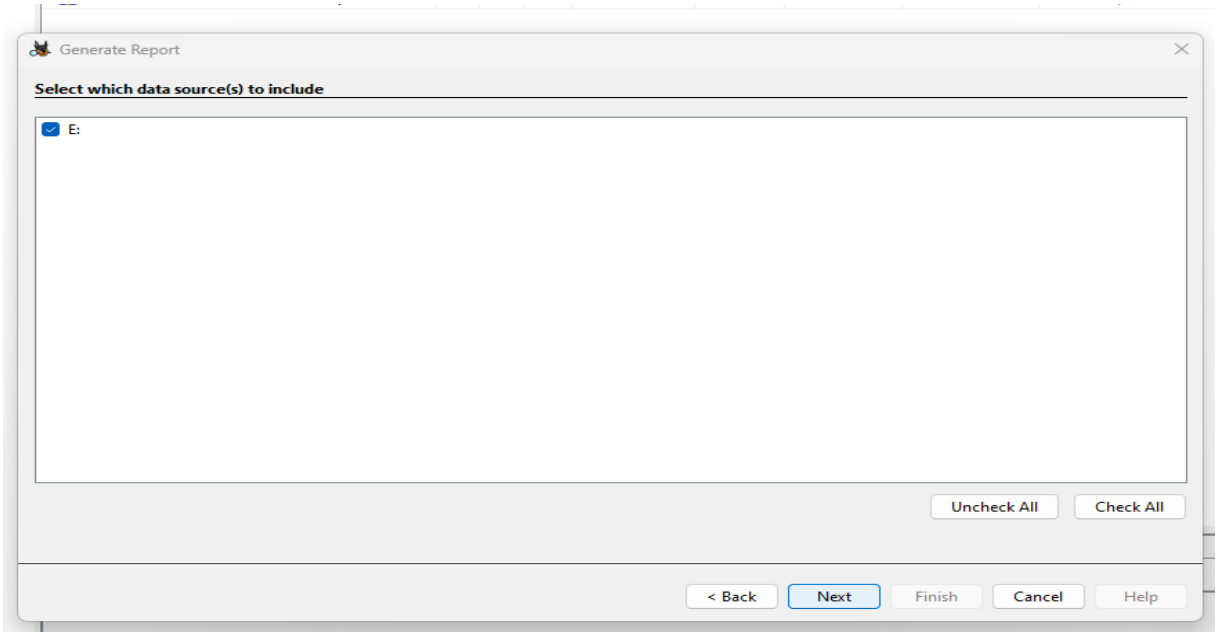


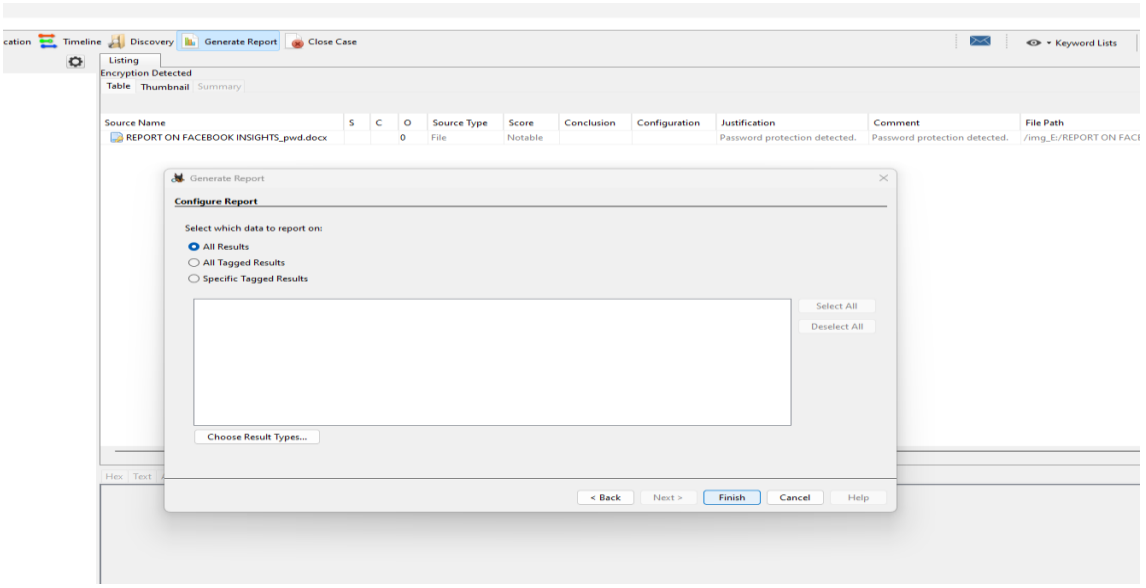


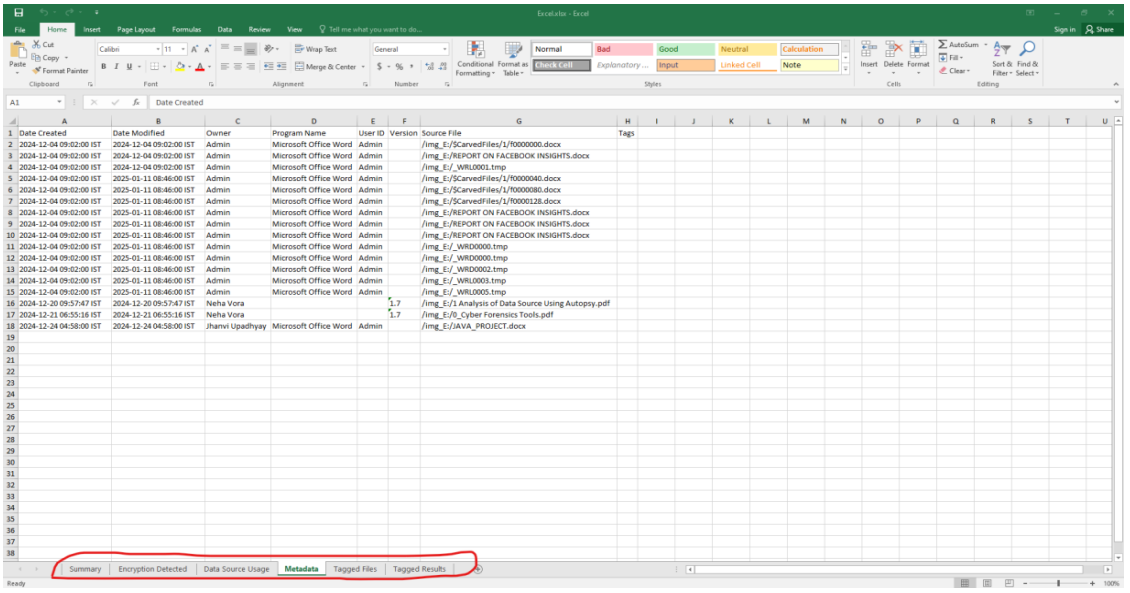
Step 4 -Retrieve the classified files








Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Listing
Encryption Detected
Table
Thumbnail
Summary
Source Name
S
C
O
Source Type
Score
Conclusion
Configuration
Justification
Comment
File Path
REPORT ON FACEBOOK INSIGHTS_pwd.docx
0
File
Notable
Password protection detected.
Password protection detected.
/img_E:/REPORT ON FACE
Generate Report
Configure Report
Select which data to report on:
All Results
All Tagged Results
Specific Tagged Results
Select All
Deselect All
Choose Result Types...
Hex
Text
< Back
Next >
Finish
Cancel
Help


Date Created
Summary
Encryption Detected
Data Source Usage
Metadata
Tagged Files
Tagged Results

Practical: 2

Aim: Explore Windows forensic tools (OS Forensics).

Theory

OS Forensics extract forensic data from computers, quicker and easier than ever.

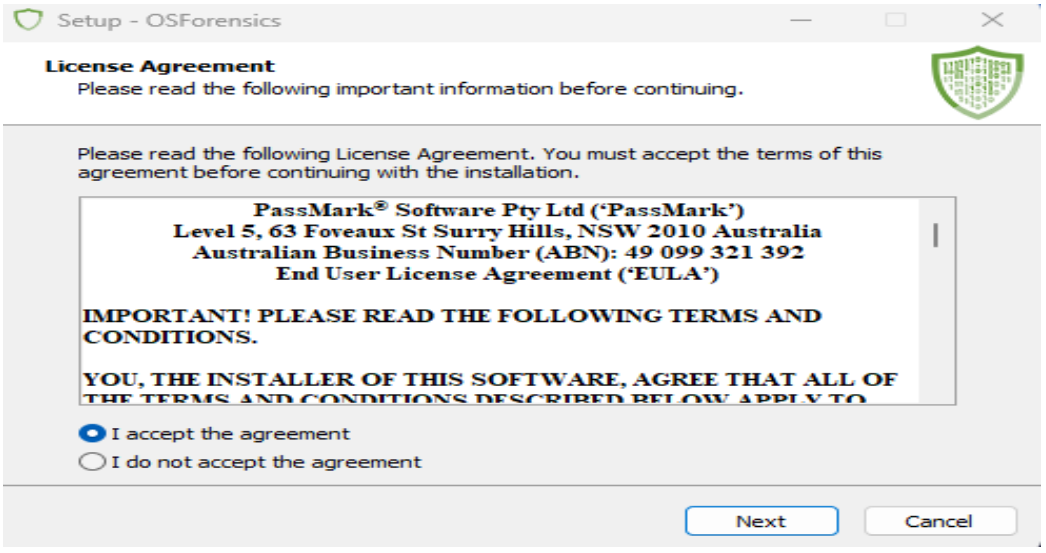
The professional and bootable editions of OS Forensics have many features not available in the free edition, including:

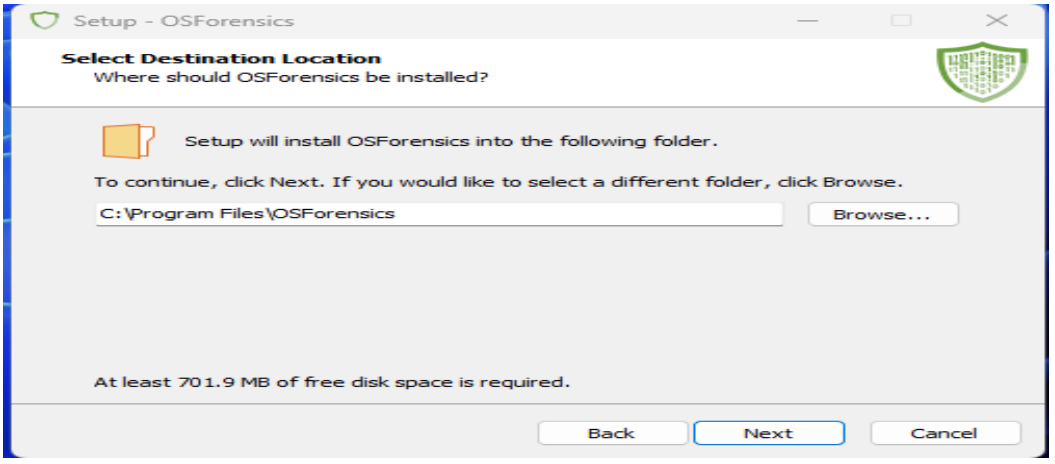
- Import and export of hash sets.
- Customizable system information gathering.
- No limits on the number of cases being managed through OS Forensics.
- Restoration of multiple deleted files in one operation.
- List and search for alternate file streams.
- Sort image files by color.
- Disk indexing and searching not restricted to a fixed number of files.
- No watermark on web captures.
- Multi-core acceleration for file decryption.
- Customizable System Information Gathering.
- View NTFS directory $I30 entries to identify potential hidden/deleted files.

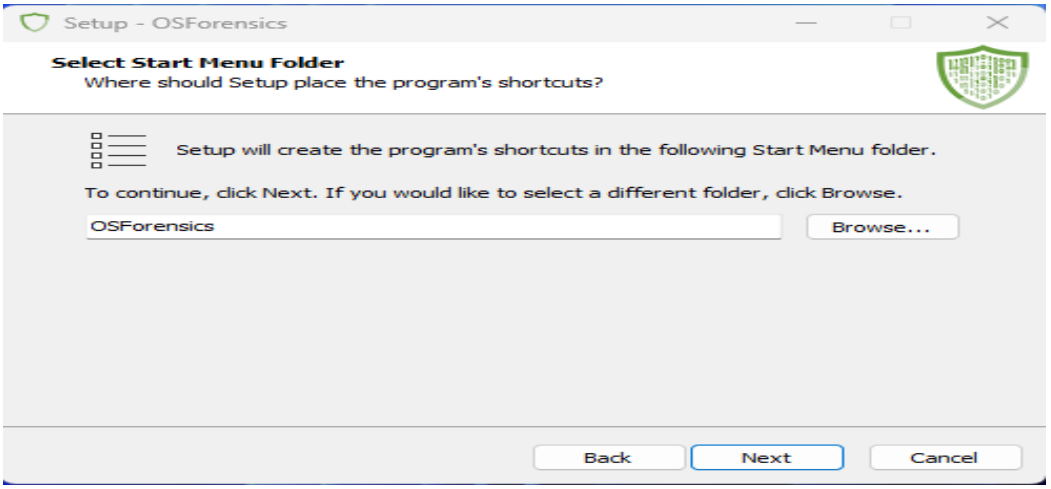
Code/Demo & Output/Steps:

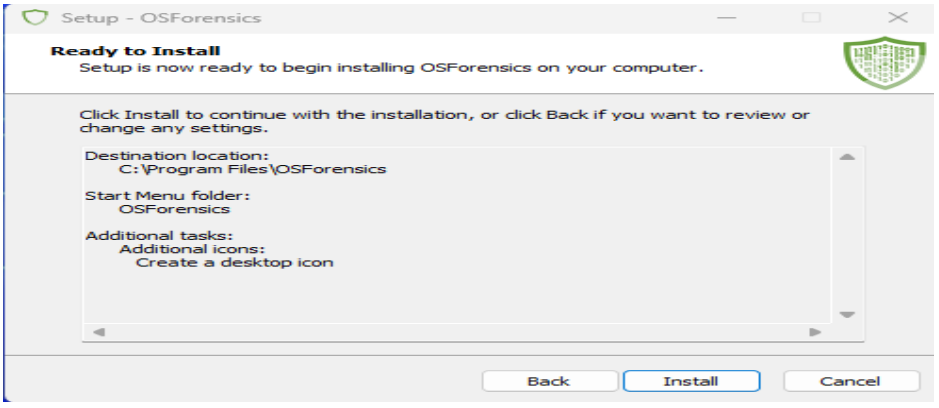
Go to: https://www.osforensics.com/download.html

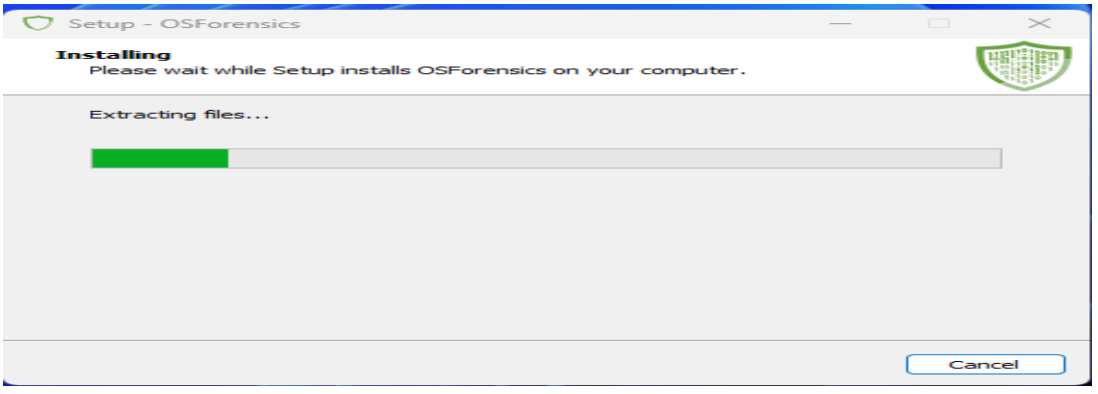
Installing OS Forensics tool

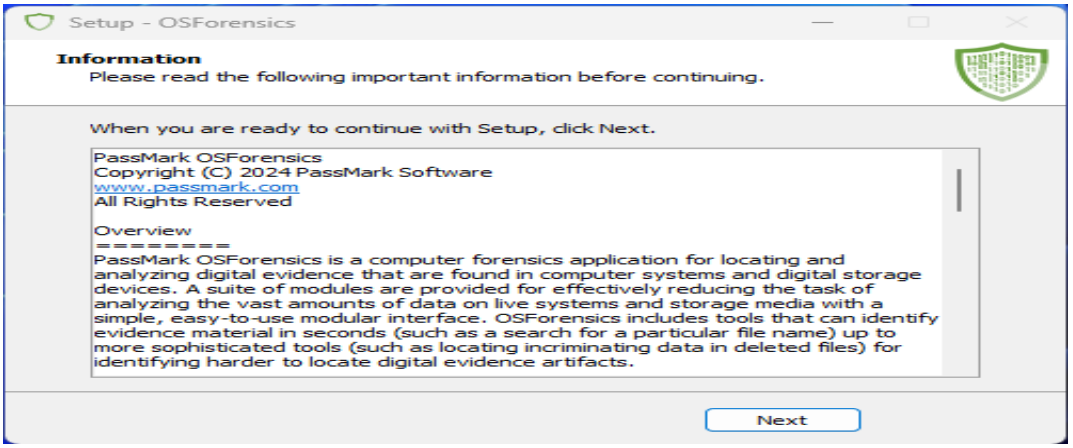


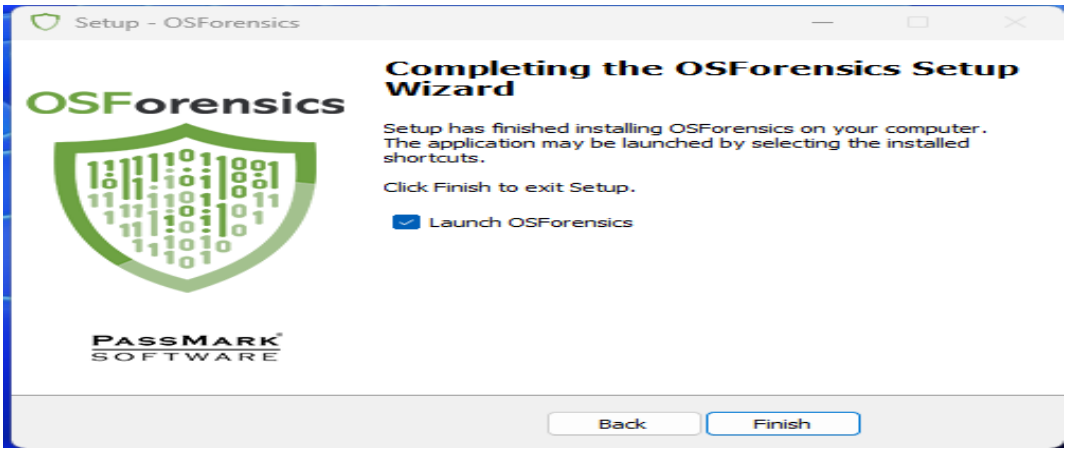

Setup - OSForensics
Select Destination Location
Where should OSForensics be installed?
Setup will install OSForensics into the following folder.
To continue, click Next. If you would like to select a different folder, click Browse.
C:\Program Files\OSForensics
Browse...
At least 701.9 MB of free disk space is required.
Back
Next
Cancel


Setup - OSForensics
Select Start Menu Folder
Where should Setup place the program's shortcuts?
Setup will create the program's shortcuts in the following Start Menu folder.
To continue, click Next. If you would like to select a different folder, click Browse.
OSForensics
Browse...
Back
Next
Cancel

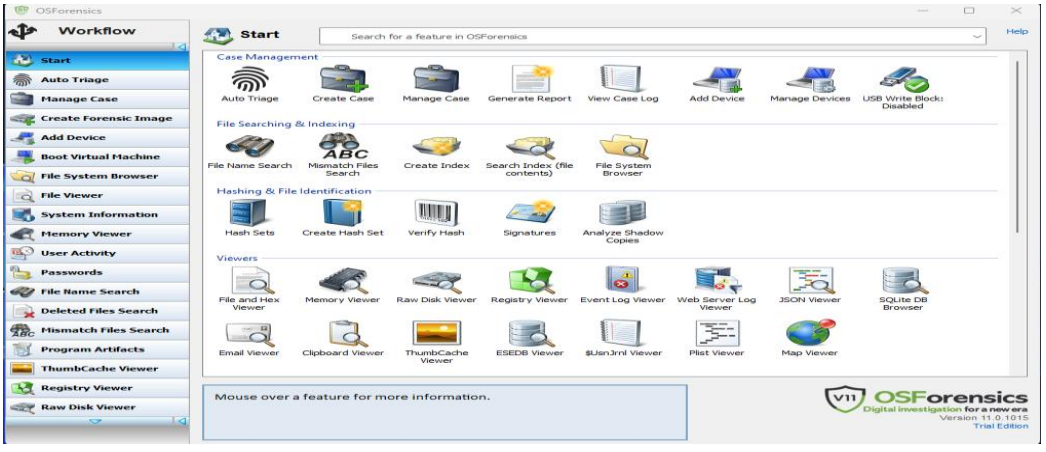

Setup - OSForensics
Ready to Install
Setup is now ready to begin installing OSForensics on your computer.
Click Install to continue with the installation, or click Back if you want to review or change any settings.
Destination location:
C:\Program Files\OSForensics
Start Menu folder:
OSForensics
Additional tasks:
Additional icons:
Create a desktop icon
Back
Install
Cancel


Setup - OSForensics
Installing
Please wait while Setup installs OSForensics on your computer.
Extracting files...
Cancel


Setup - OSForensics
Information
Please read the following important information before continuing.
When you are ready to continue with Setup, click Next.
PassMark OSForensics
Copyright (C) 2024 PassMark Software
www.passmark.com
All Rights Reserved
Overview
PassMark OSForensics is a computer forensics application for locating and analyzing digital evidence that are found in computer systems and digital storage devices. A suite of modules are provided for effectively reducing the task of analyzing the vast amounts of data on live systems and storage media with a simple, easy-to-use modular interface. OSForensics includes tools that can identify evidence material in seconds (such as a search for a particular file name) up to more sophisticated tools (such as locating incriminating data in deleted files) for identifying harder to locate digital evidence artifacts.
Next


Setup - OSForensics
OSForensics
PASSMARK SOFTWARE
Completing the OSForensics Setup Wizard
Setup has finished installing OSForensics on your computer. The application may be launched by selecting the installed shortcuts.
Click Finish to exit Setup.
Launch OSForensics
Back
Finish


OSForensics
Workflow
Start
Auto Triage
Manage Case
Create Forensic Image
Add Device
Boot Virtual Machine
File System Browser
File Viewer
System Information
Memory Viewer
User Activity
Passwords
File Name Search
Deleted Files Search
Mismatch Files Search
Program Artifacts
ThumbCache Viewer
Registry Viewer
Raw Disk Viewer
PassMark® Software
OSForensics
PassMark Software
www.osforensics.com
Unlicensed trial
Click on Continue for your 30day evaluation (30 Days left)
Continue Using Trial Version
Upgrade to Professional Version
Exit


OSForensics
Workflow
Start
Search for a feature in OSForensics
Help
Case Management
Auto Triage
Create Case
Manage Case
Generate Report
View Case Log
Add Device
Manage Devices
USB Write Block: Disabled
File Searching & Indexing
File Name Search
Mismatch Files Search
Create Index
Search Index (file contents)
File System Browser
Hashing & File Identification
Hash Sets
Create Hash Set
Verify Hash
Signatures
Analyze Shadow Copies
Viewers
File and Hex Viewer
Memory Viewer
Raw Disk Viewer
Registry Viewer
Event Log Viewer
Web Server Log Viewer
JSON Viewer
SQLite DB Browser
Email Viewer
Clipboard Viewer
ThumbCache Viewer
ESEDB Viewer
$UsnJrnl Viewer
Plist Viewer
Map Viewer
Mouse over a feature for more information.
OSForensics
Digital investigation for a new era
Version 11.0.1015
Trial Edition

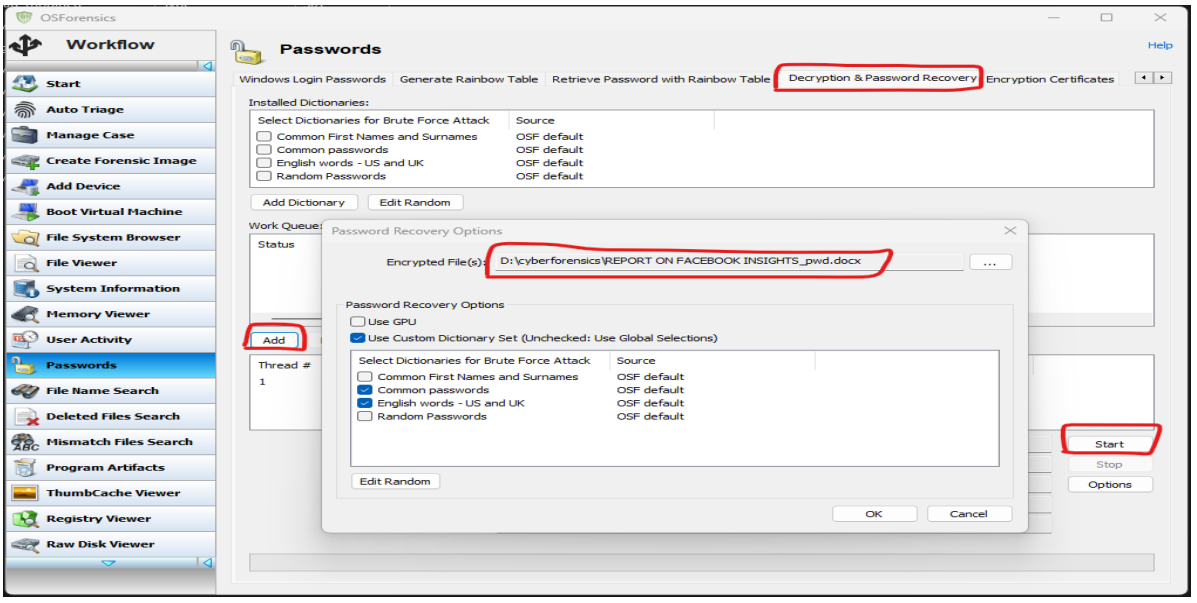
After Successfully installing OS Forensics this kind of interface should be display on your system. OS Forensics supports two methods of gaining access to encrypted office documents.

The first method is for older documents that use 40bit encryption (old XLS, DOC & PDF files).For these documents is it possible to try all possible keys to decrypt the document, with the output being an unencrypted file.

By using this tool we crack password protected files by simply importing the file

Select

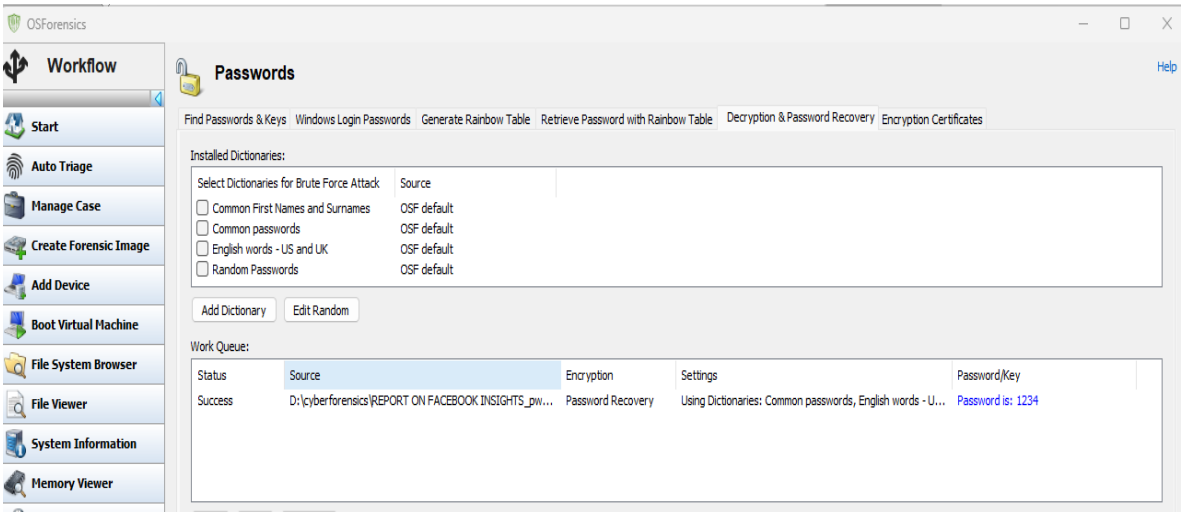
1.Password -> Decryption & Password recovery



This tool having some preloaded decrypted password file by using unique combination of alpha-numeric. Password combination it is encrypting password protected files.

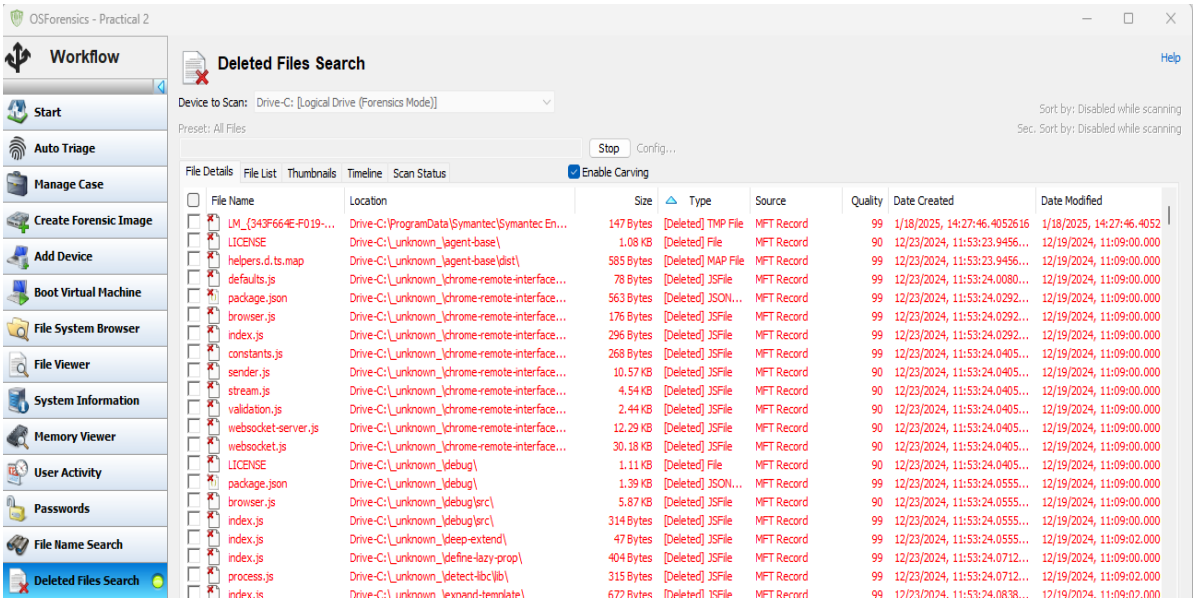
Add -> Select password Protected file -> select predefine password libraries -> Start

Password is Display in this Prompt

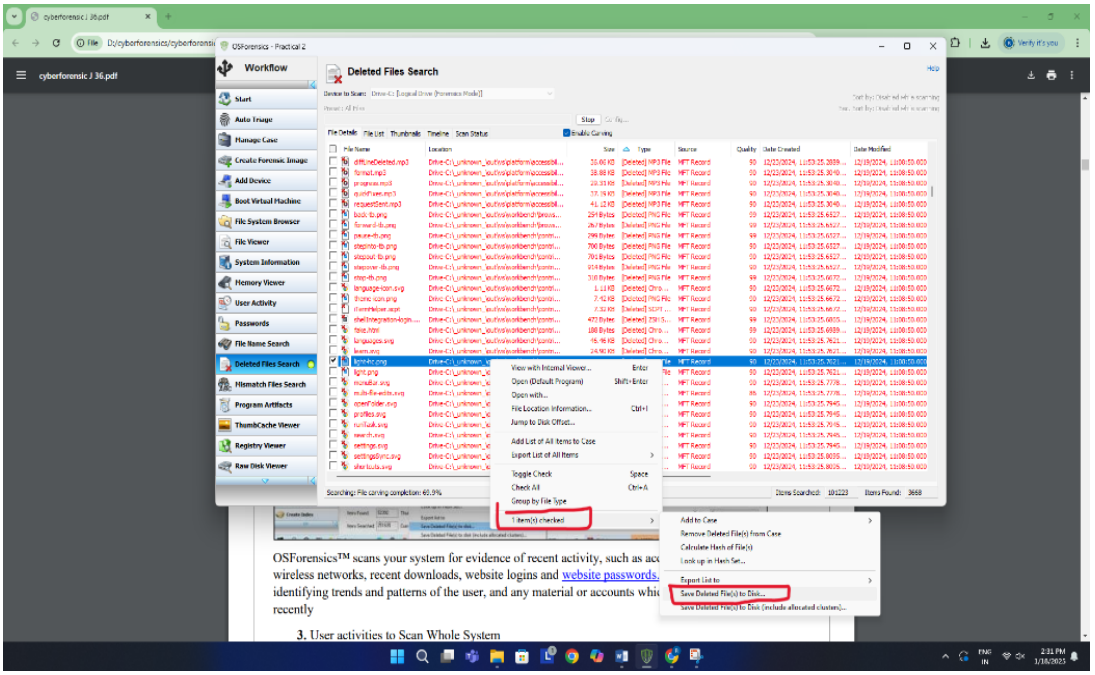


2.Deleted File Search

Select Deleted File Search -> Select Device Drive -> Search



Select the file that wants to recover by simply right click Checked item -> Save Delete Files on Disk and Select the Folder

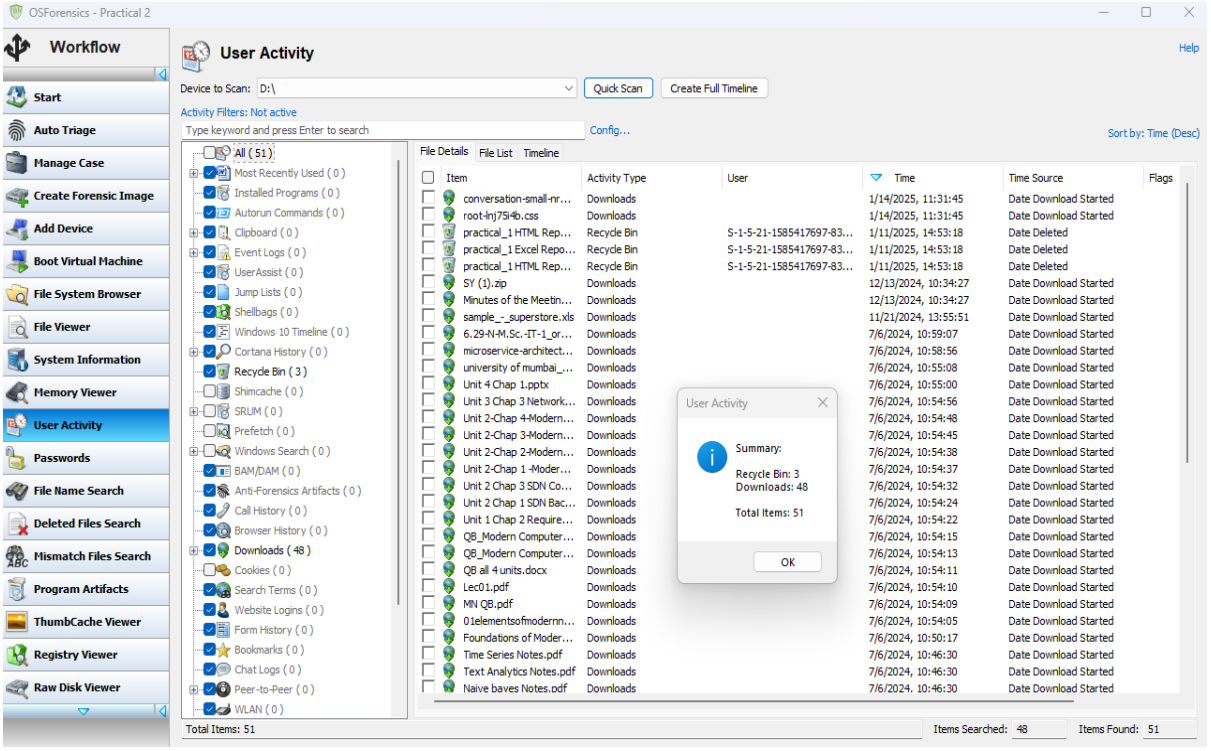


OS Forensics scans your system for evidence of recent activity, such as accessed websites, USB drives, wireless networks, recent downloads, website logins and website passwords. This is especially useful for identifying trends and patterns of the user, and any material or accounts which have been accessed recently

3.User activities to Scan Whole System

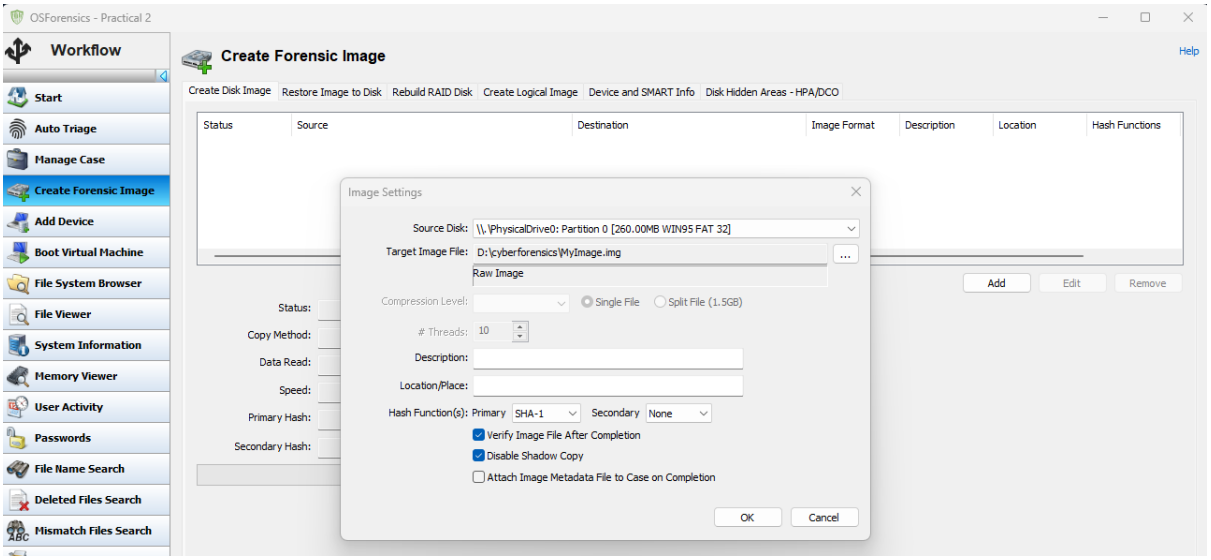
Select User Activity -> Select the Drive -> click on scan.

Multiple user activities are shown in detailed manner.



4.Create a bit-by-bit copy of a drive using OS Forensics in a forensic way. It is use to acquire image of the whole drive.

Select forensics imaging -> select the target image file -> ok



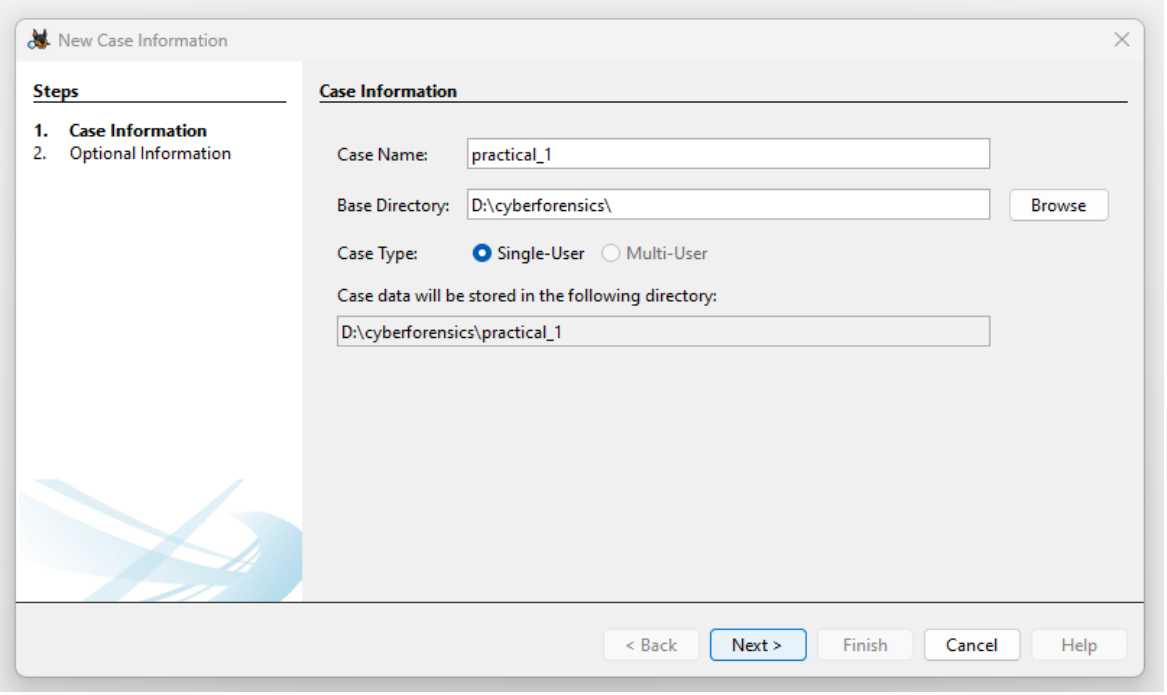
Practical: 3

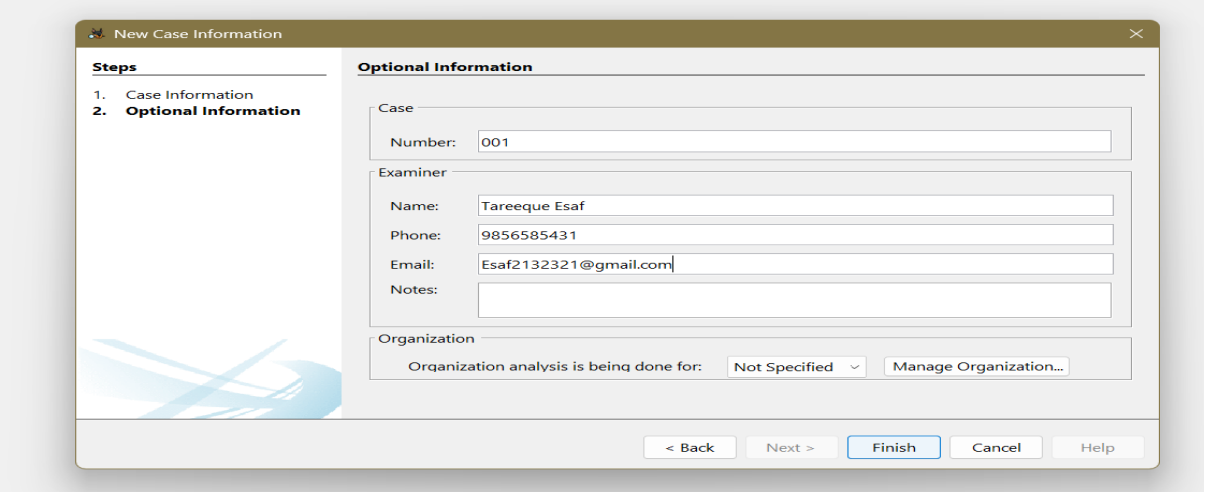
Aim: Using Forensic Tool Kit (FTK) & Writing report using FTK (Access Data FTK).

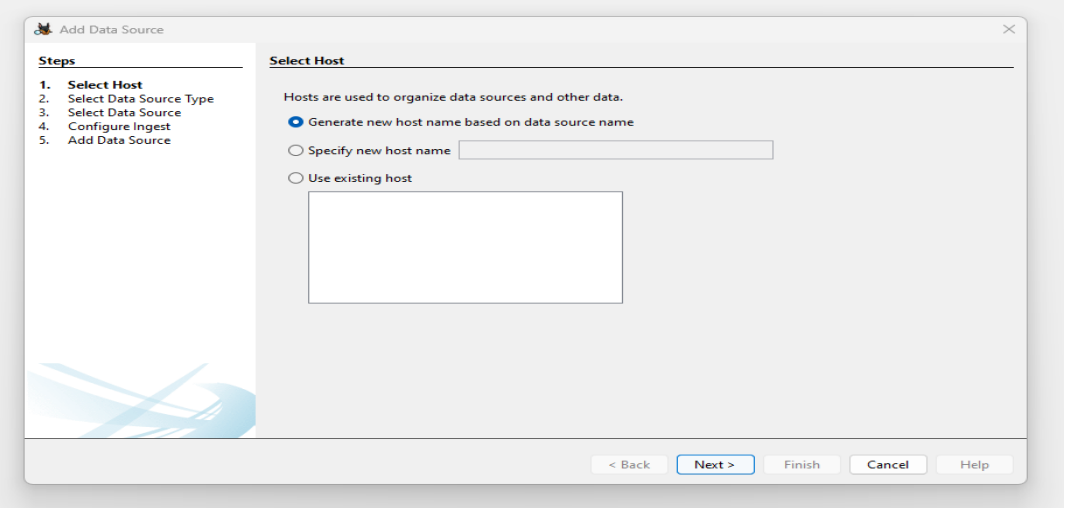
Step 1-Start a New Case

Click New Case. This will add a new case folder to the system and allow you to begin adding evidence. To begin, click New Case.

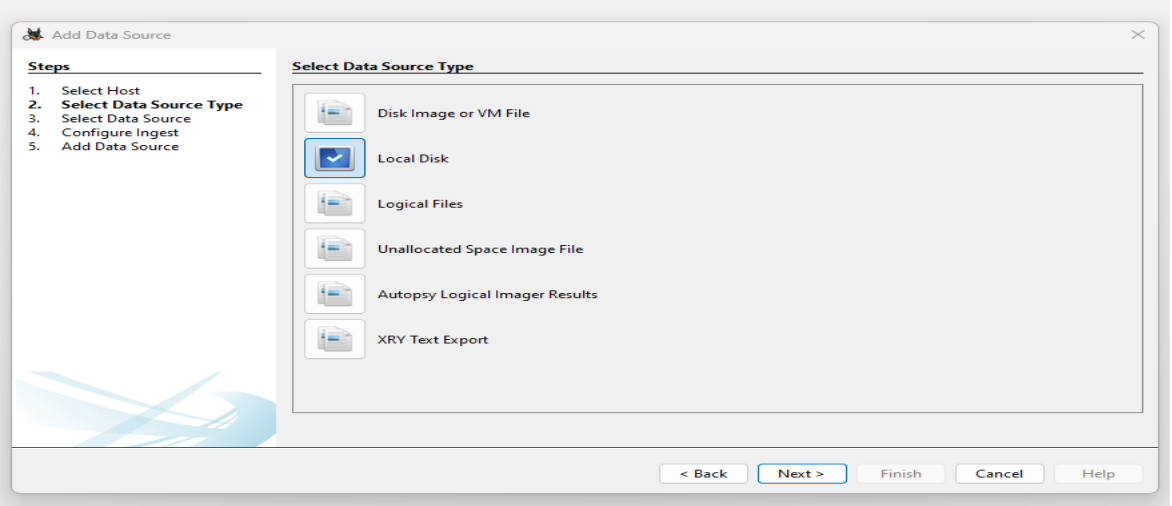
Step 2 -Enter the Case Details

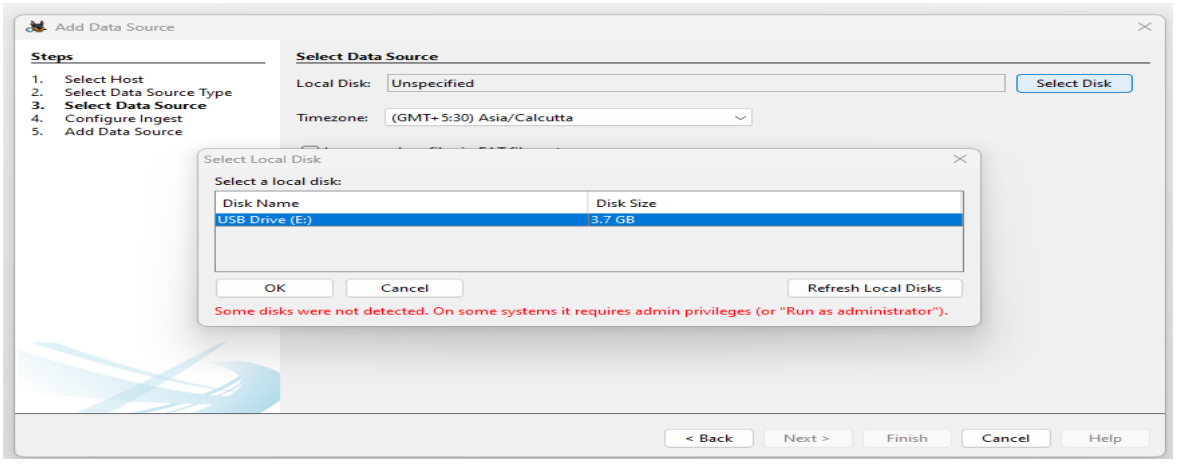


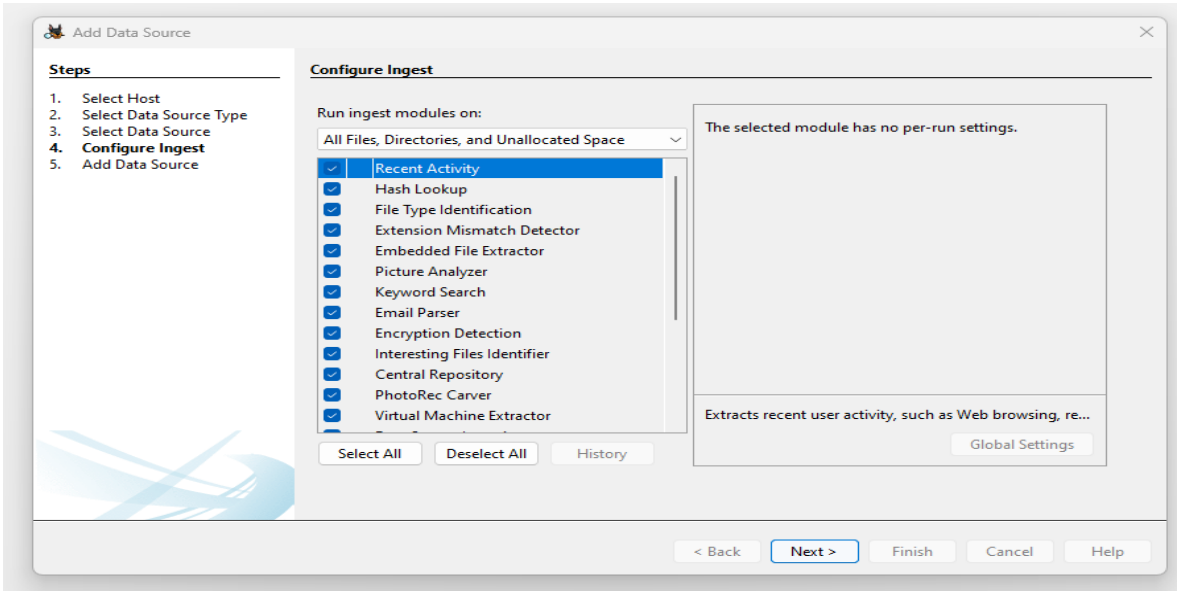




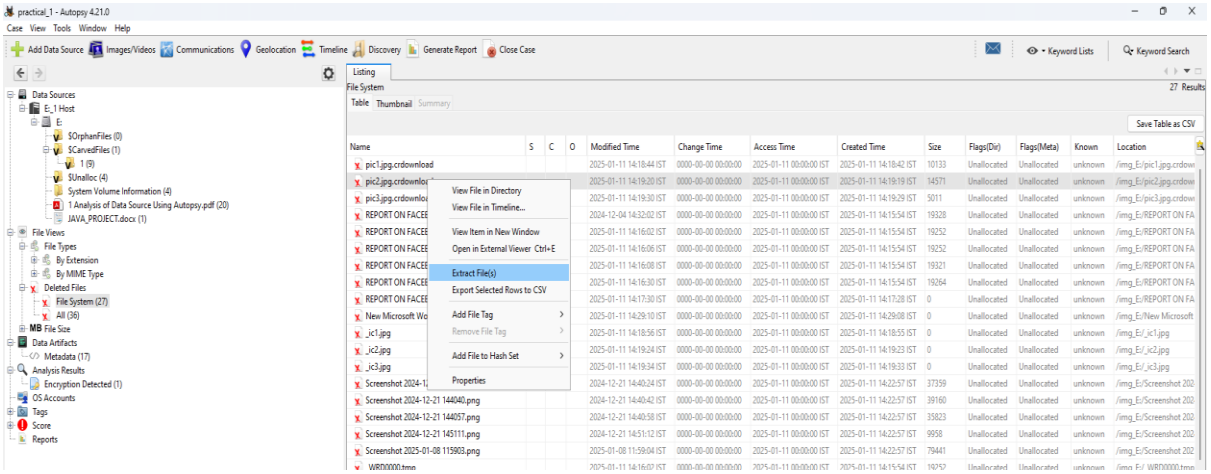
Step 3 -Choose the path

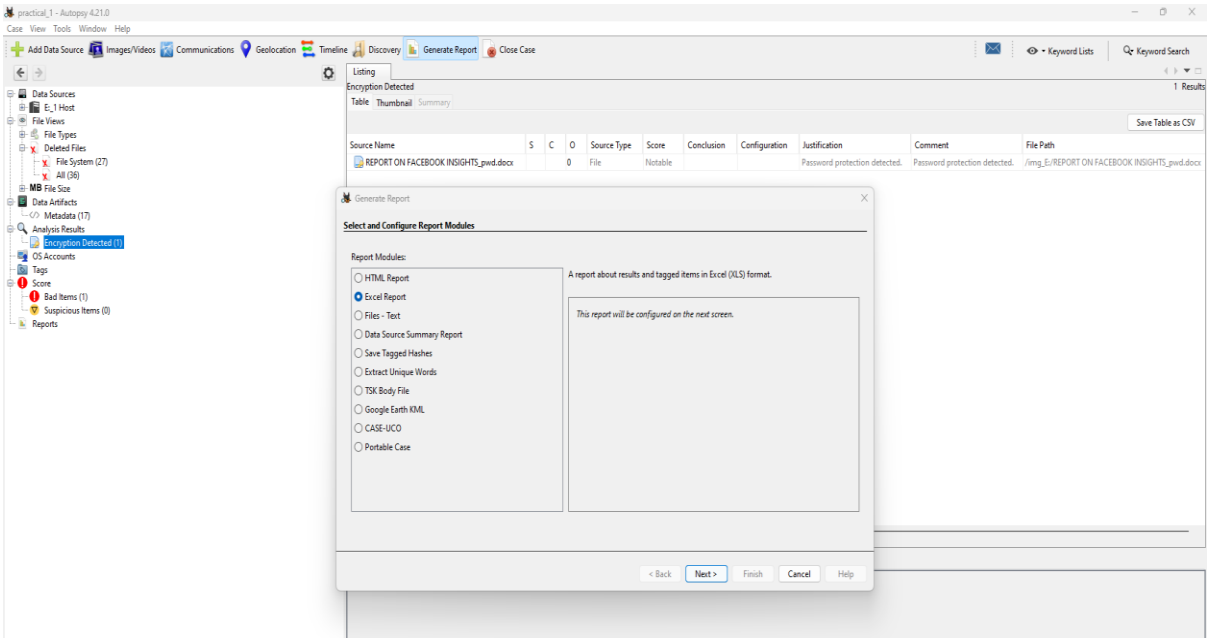


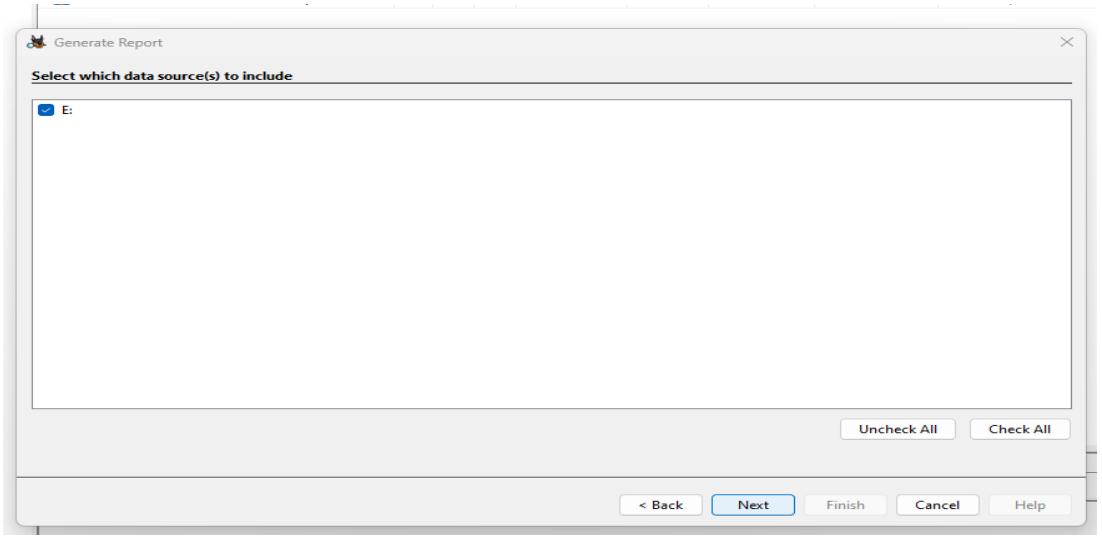


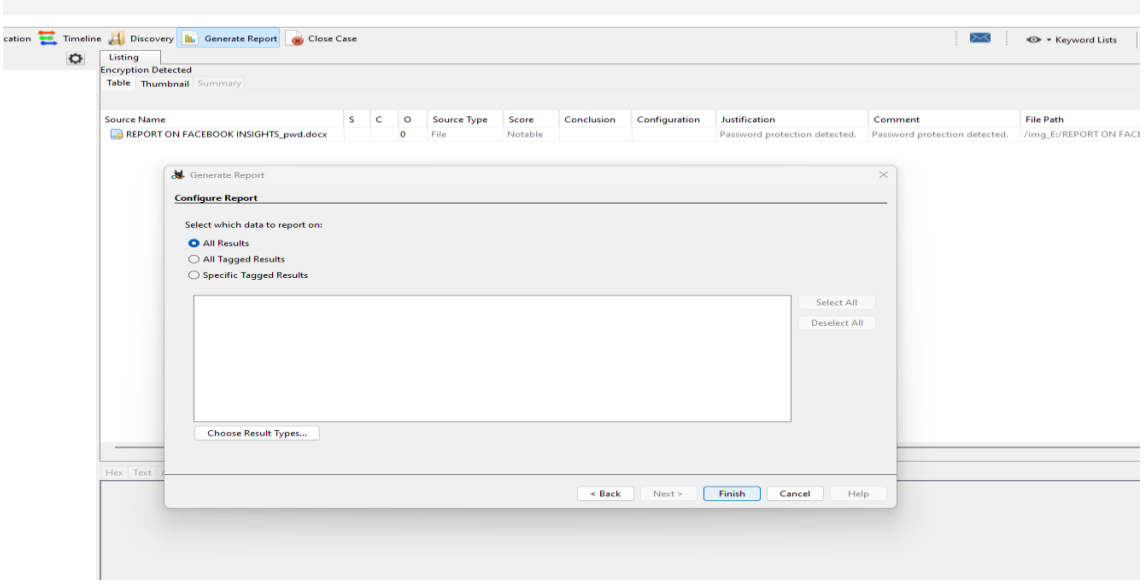


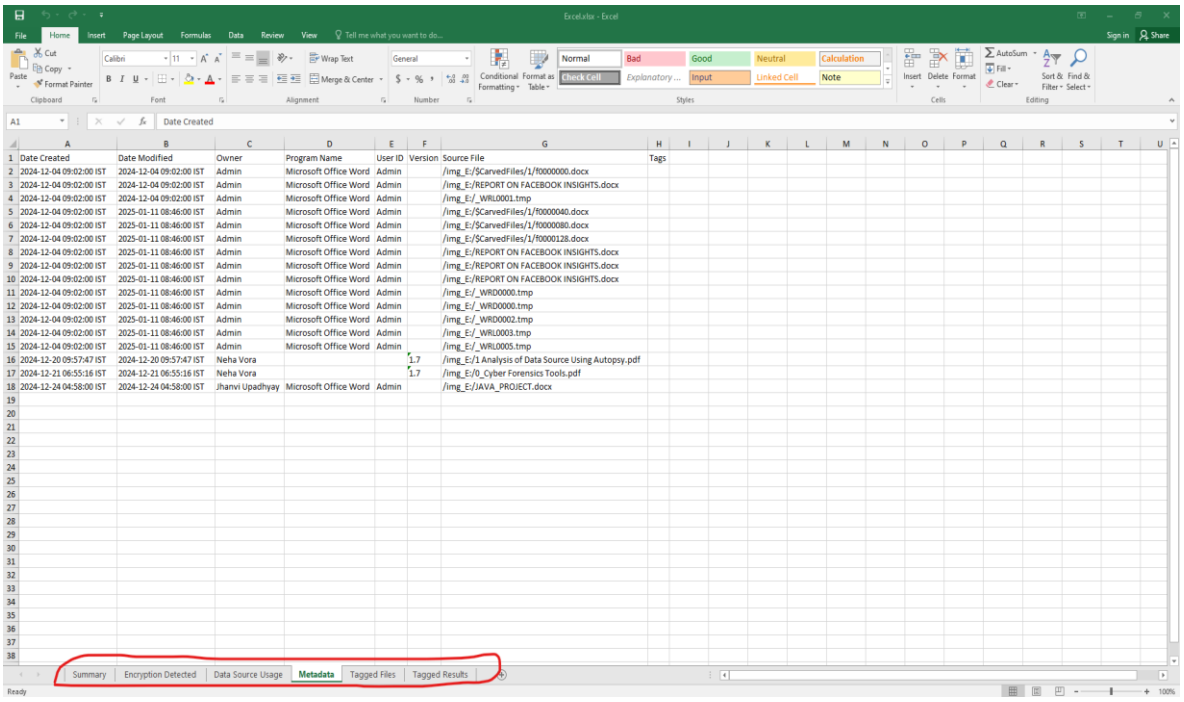
Step 4 -Retrieve the classified files




practical_1 - Autopsy 4.21.0
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
Data Sources
E_1 Host
File Views
File Types
Deleted Files
File System (27)
All (36)
MB File Size
Data Artifacts
Metadata (17)
Analysis Results
Encryption Detected (1)
OS Accounts
Tags
Score
Bad Items (1)
Suspicious Items (0)
Reports
Listing
Encryption Detected
1 Results
Table
Thumbnail
Summary
Save Table as CSV
Source Name
S
C
O
Source Type
Score
Conclusion
Configuration
Justification
Comment
File Path
REPORT ON FACEBOOK INSIGHTS_pwd.docx
0
File
Notable
Password protection detected.
Password protection detected.
/img_E:/REPORT ON FACEBOOK INSIGHTS_pwd.docx
Generate Report
Select and Configure Report Modules
Report Modules:
HTML Report
Excel Report
Files - Text
Data Source Summary Report
Save Tagged Hashes
Extract Unique Words
TSK Body File
Google Earth KML
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
Select which data source(s) to include
E:
Uncheck All
Check All
< Back
Next
Finish
Cancel
Help

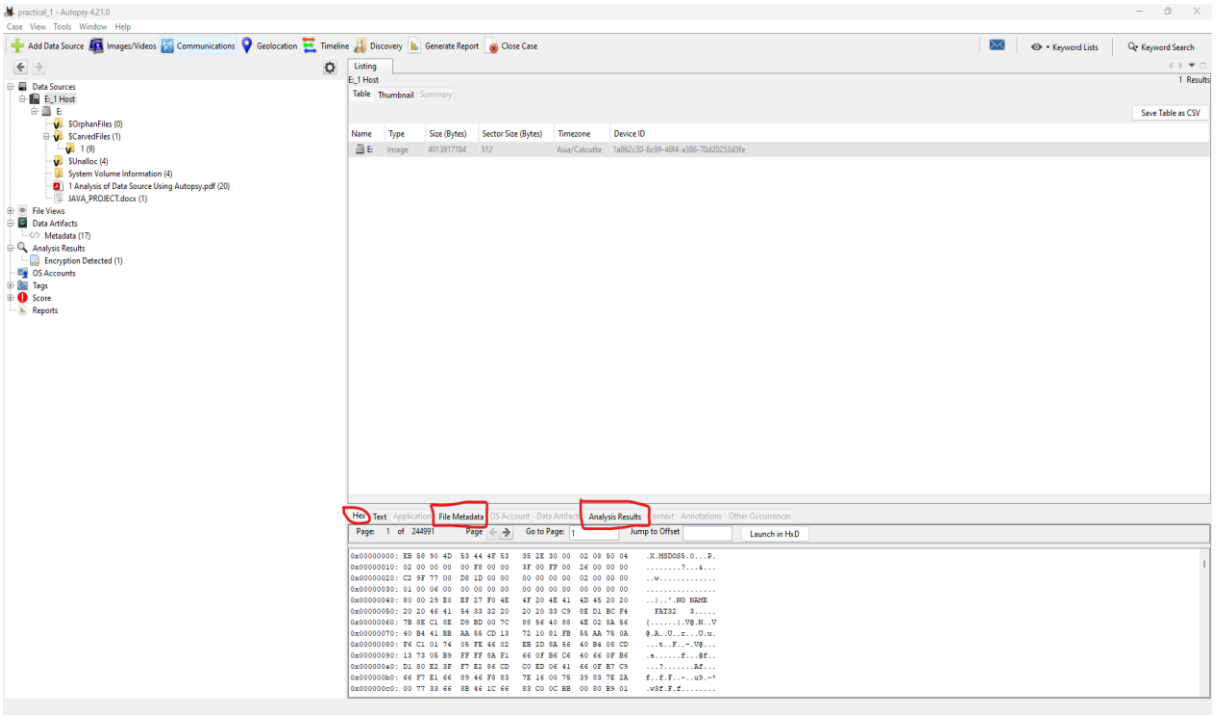

Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Listing
Encryption Detected
Table
Thumbnail
Summary
Source Name
S
C
O
Source Type
Score
Conclusion
Configuration
Justification
Comment
File Path
REPORT ON FACEBOOK INSIGHTS_pwd.docx
0
File
Notable
Password protection detected.
Password protection detected.
Generate Report
Configure Report
Select which data to report on:
All Results
All Tagged Results
Specific Tagged Results
Select All
Deselect All
Choose Result Types...
< Back
Next >
Finish
Cancel
Help



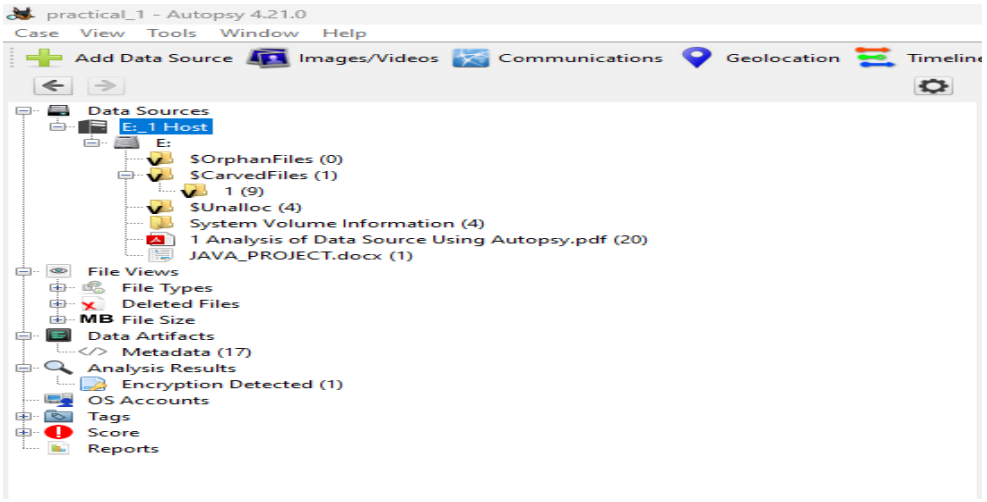
3. Exploring the data source:

The Data Source information: Here the basic metadata is shown. A detailed analysis is displayed in

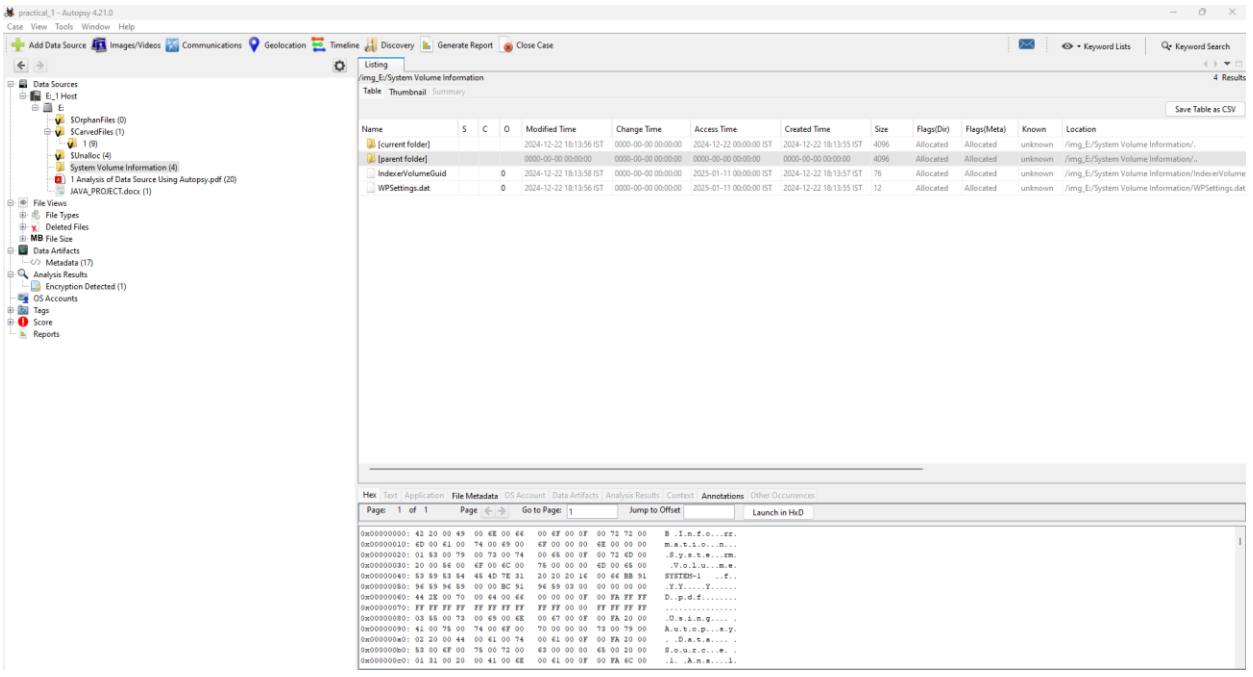
the bottom section. These details can be extracted in the form of Hex values, Results, File Metadata, etc.



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

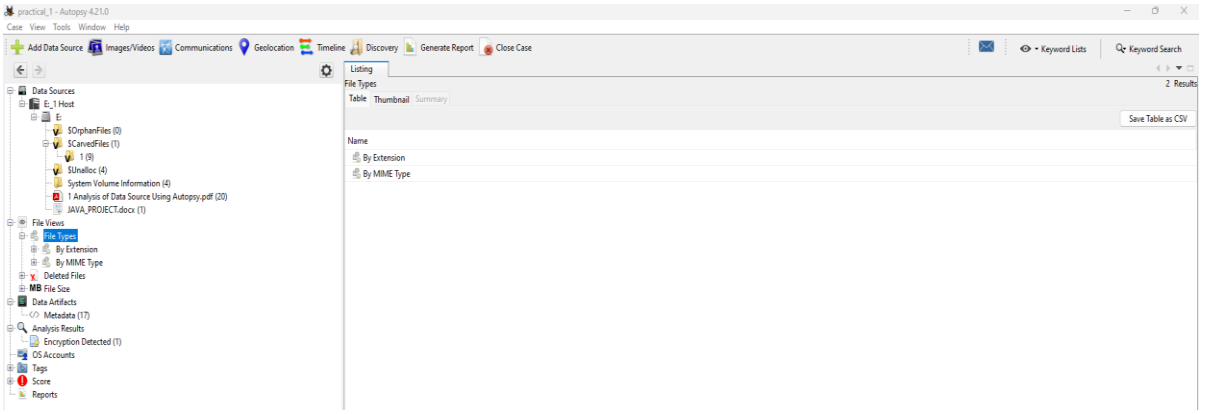


Each volume can be browsed for its contents, results for which are displayed in the section at the bottom. For example, the content shown below belongs to Data Sources -> System Volume Information (4) -> [Parent Folder].



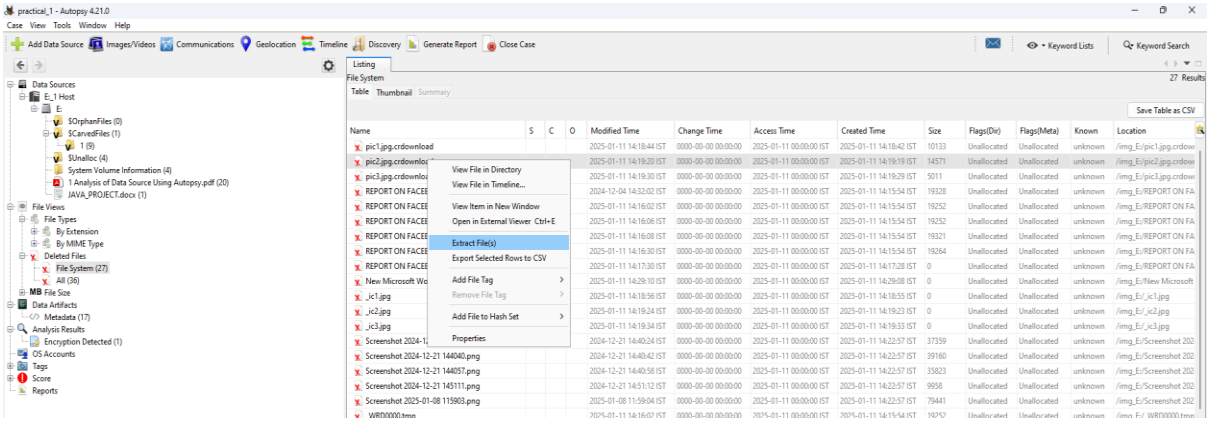
Views (Determines the factor of file classification)

• **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.

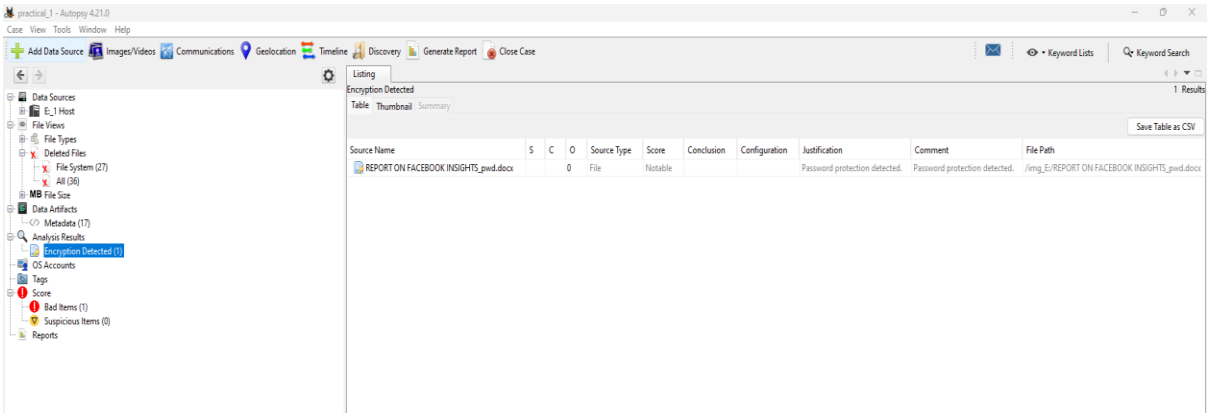
Results:

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.

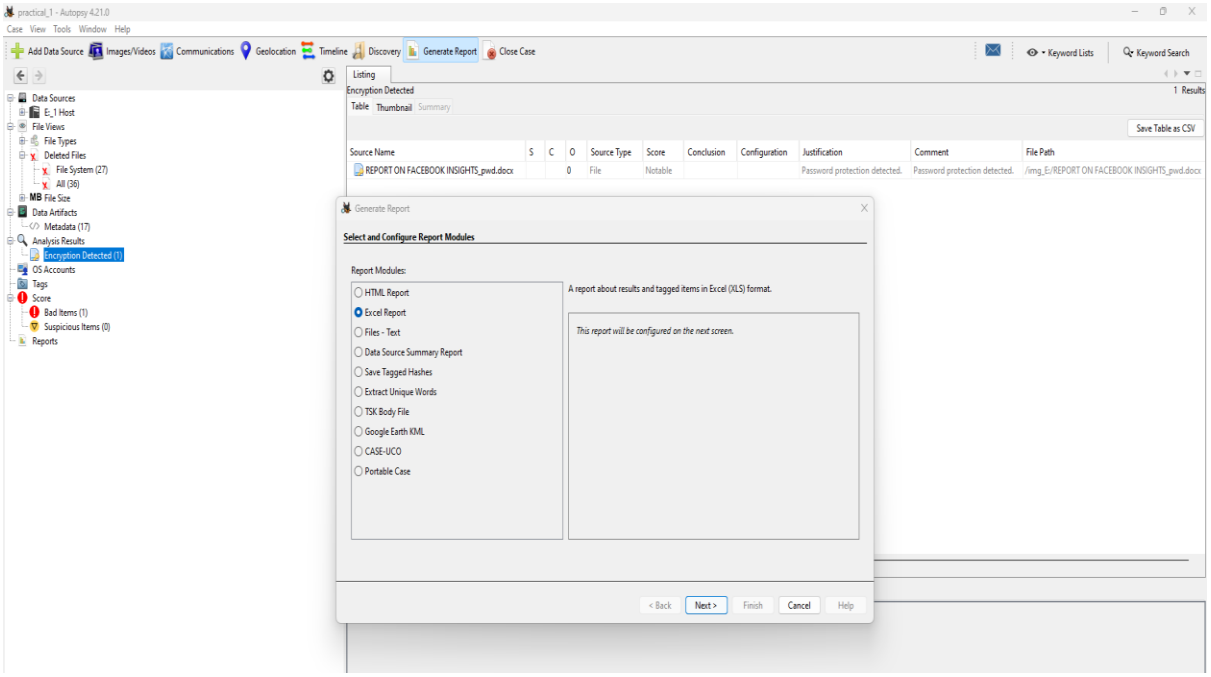
• **HashSet Hits:** Here the search can be made using hash values.

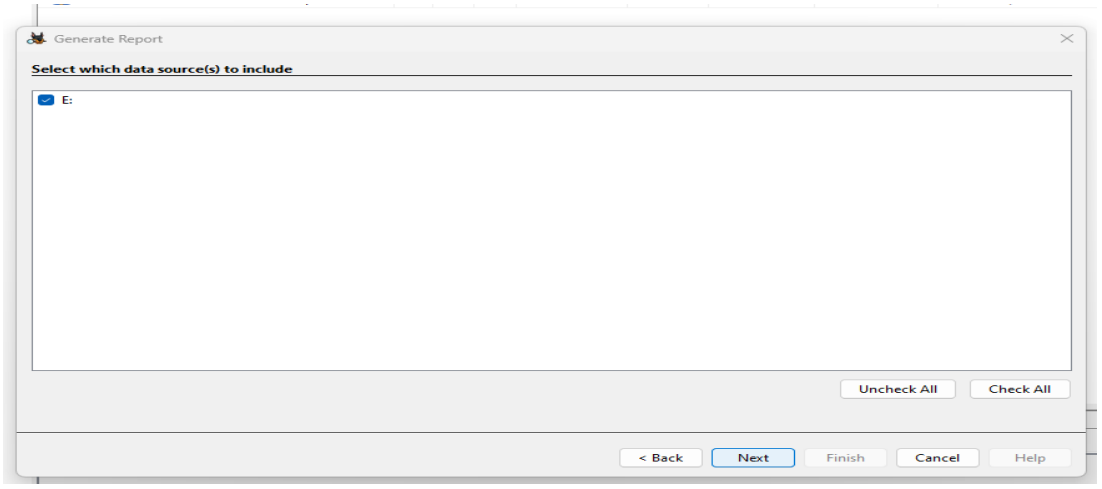
• **E-mail Messages:** Here all the outlook.pst files can be explored.

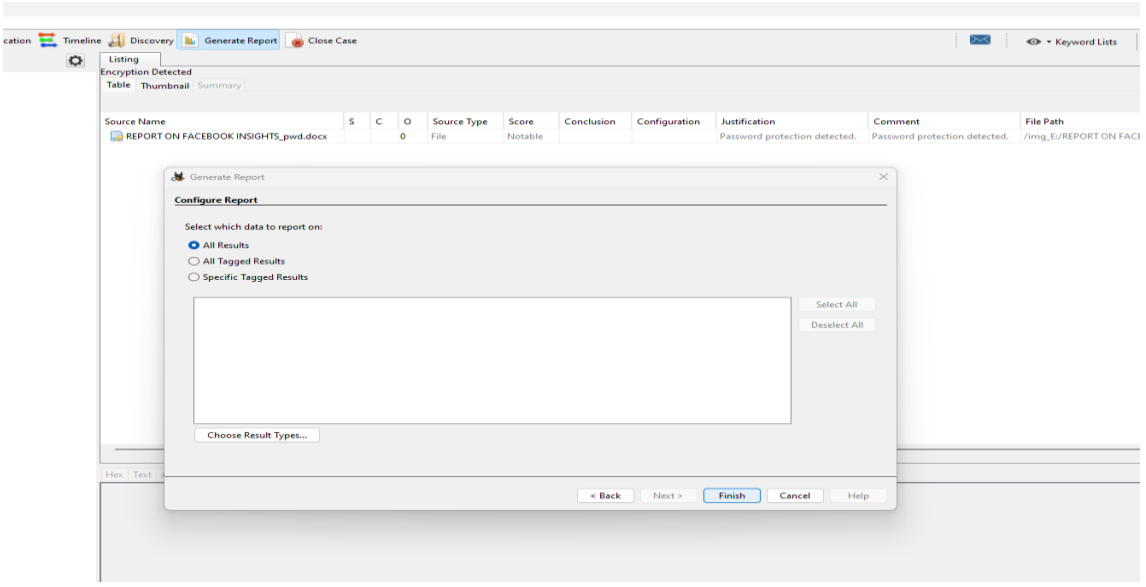
• **Interesting Items:** As discussed before, these are the file results based upon the custom rules set by the examiner.

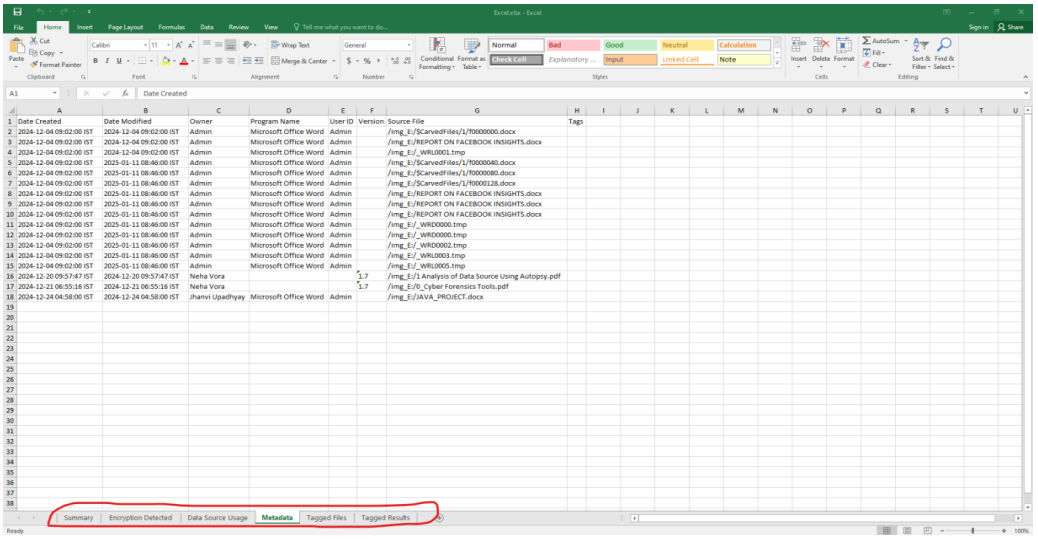
• **Accounts:** Here all the details regarding the accounts present on the disk are shown. This disk has the following EMAIL accounts.

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

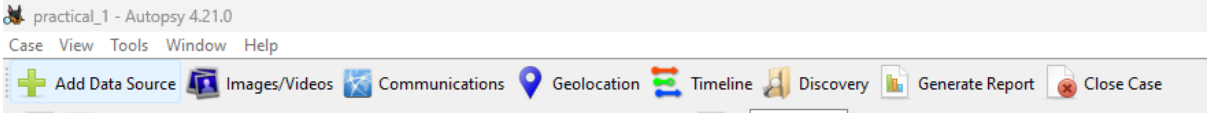






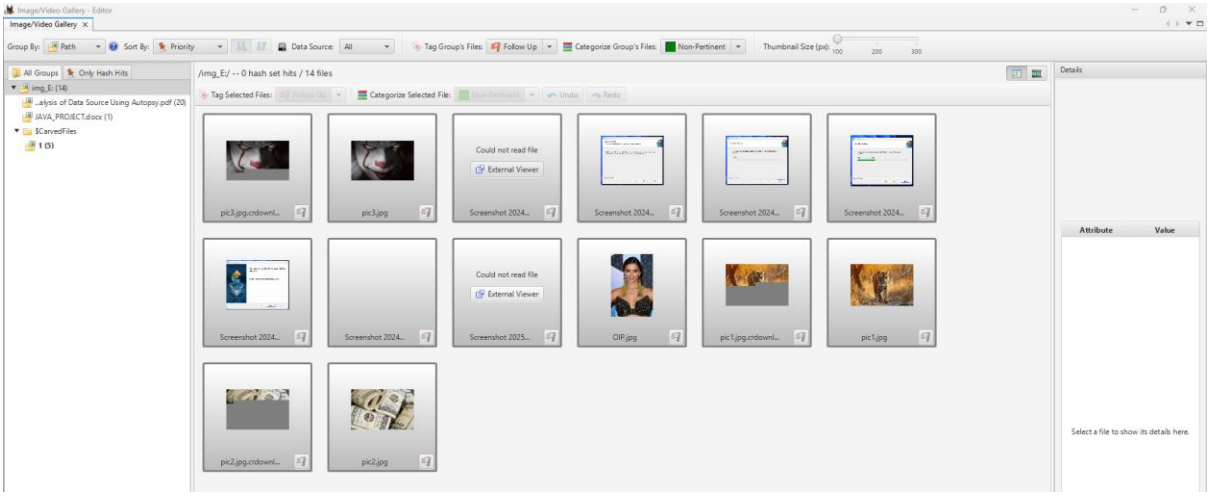


Additional Features:



• **Add a Data Source:** Each case can hold multiple Data Sources.

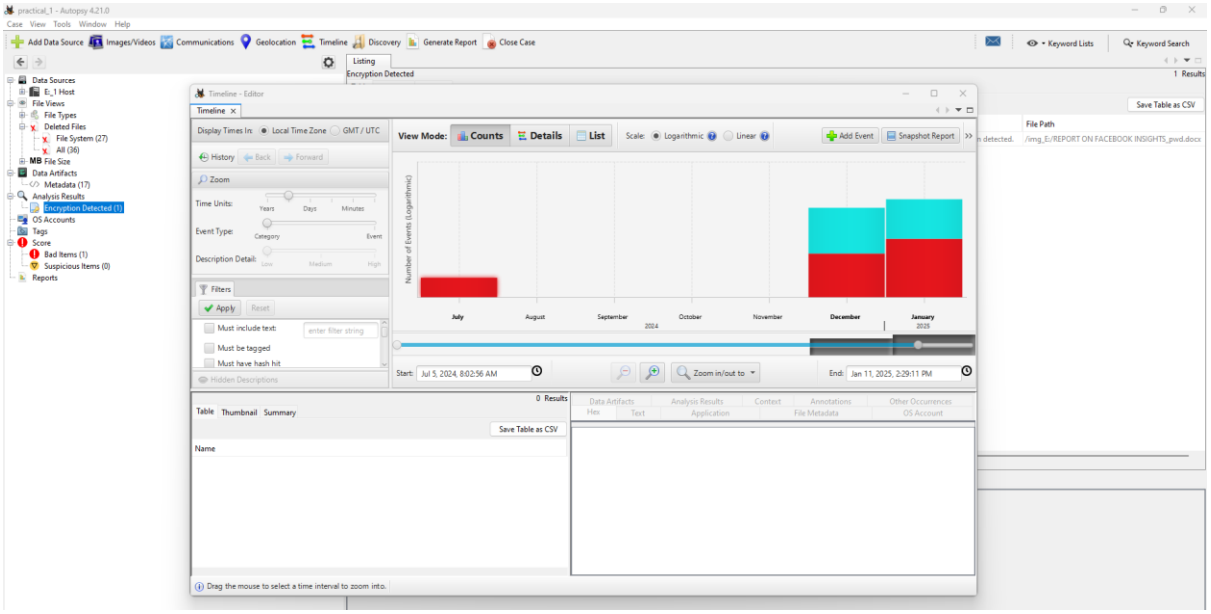
• **Images/Videos:** Images/ Videos in the data source can be viewed in Gallery View. The information here is displayed in the form of attribute-value pairs.



• **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.



Practical: 4

Aim: (A) Creating a Forensic Image using FTK Imager

Theory

A Forensic Image is most often needed to verify the integrity of the image after an acquisition ofa Hard Drive has occurred. This is usually performed by law enforcement for court because, aftera forensic image has been created, its integrity can be checked to verify that it has not been tampered with. The image is an identical copy of all the drive structures and contents.

Need for a Forensic Image

In today's world of crime, many cases have been solved by using this technique, as evidence apart from what is available through an operating system, has been found using this technique, as incriminating data might have deleted to prevent discovery during the investigation. Unless that data is overwritten and deleted securely, it can be recovered.

One of the advantages includes the prevention of the loss of critical files.

When you suspect a custodian of deleting or altering files. A complete forensic image will, to a certain extent, allow you to recover deleted files. It can also potentially be used to identify files that have been renamed or hidden.

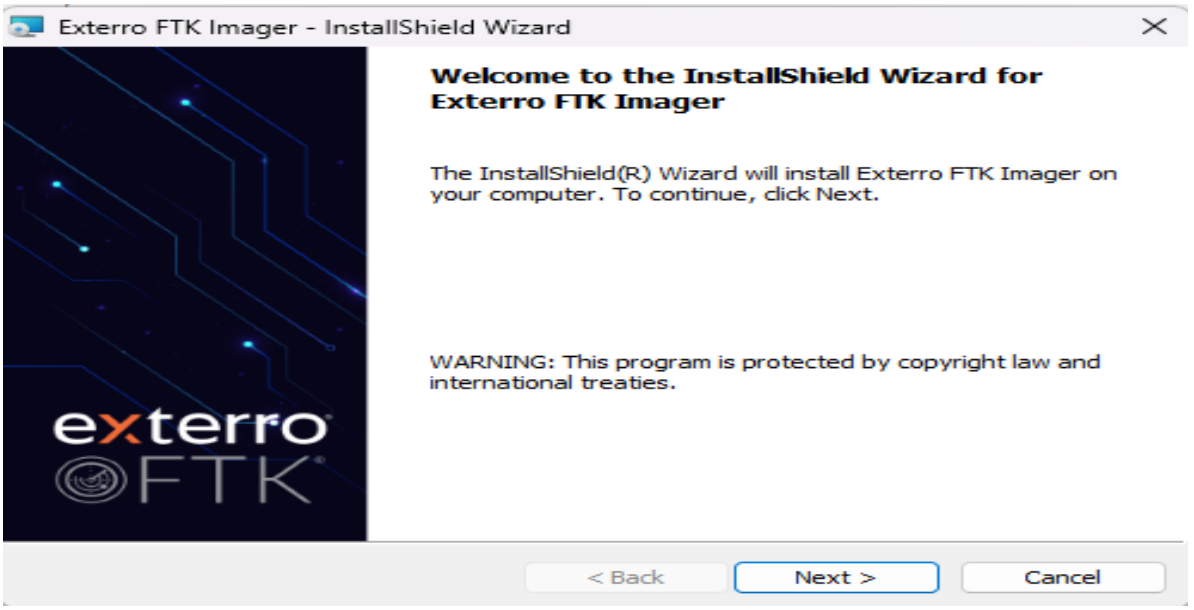
What Is FTK Imager?

FTK Imager is a tool for creating disk images and is absolutely free to use. It was developed by The Access Data Group. It is a tool that helps to preview data and for imaging.

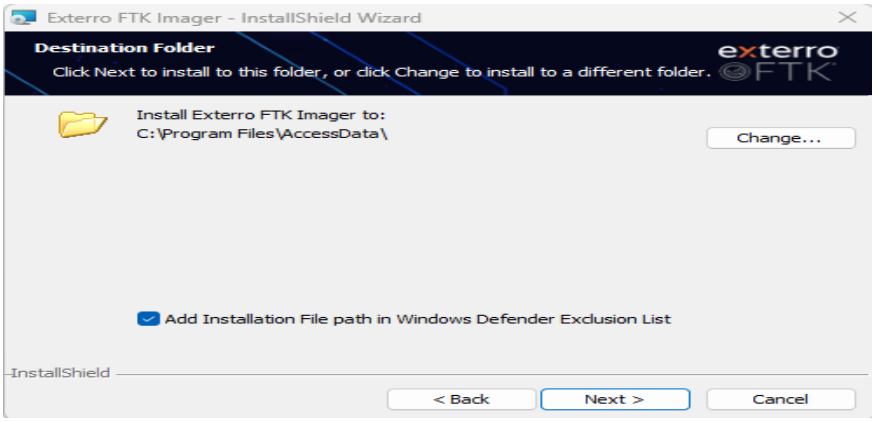
With FTK Imager, you can:

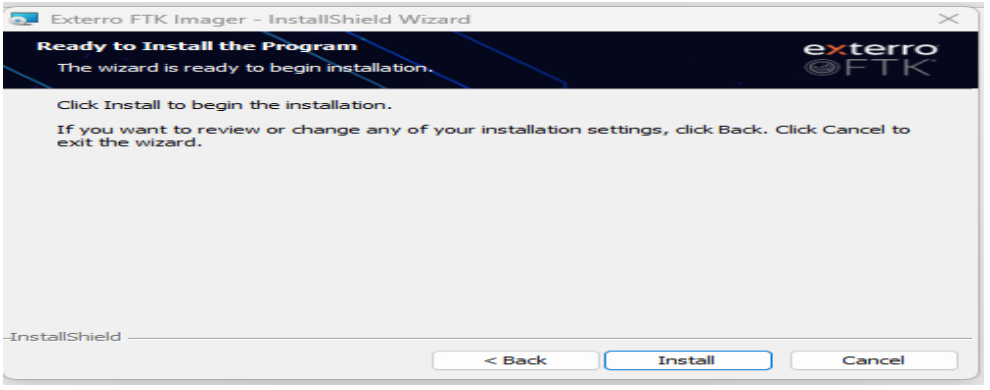
Create forensic images or perfect copies of local hard drives, floppy and Zip disks, DVDs, folders, individual files, etc. without making changes to the original evidence. Preview files and folders on local hard drives, network drives, floppy diskettes, Zip disks, CDs, and DVDs.

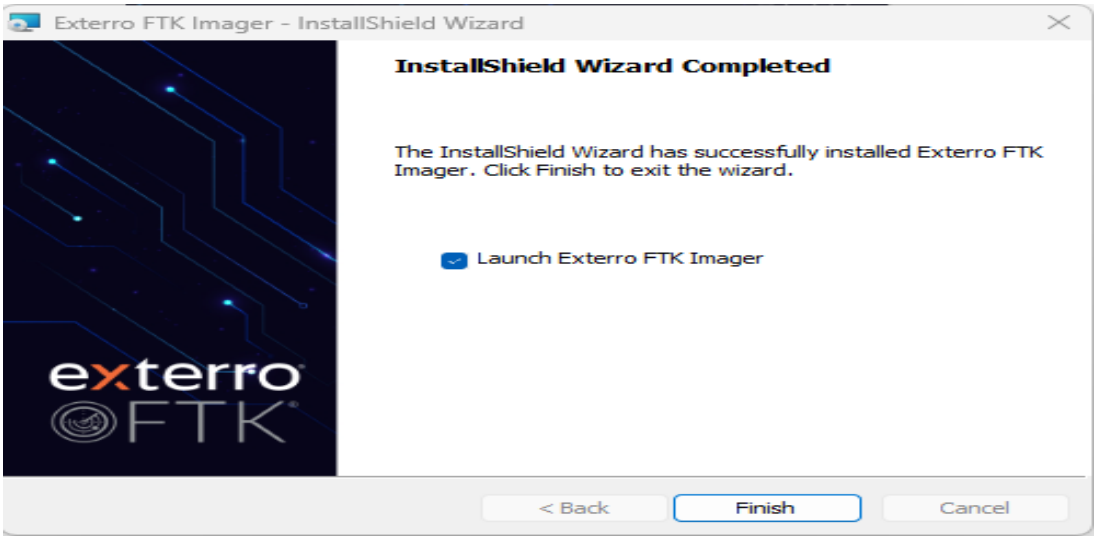
Step 1: Installing FTK Imager



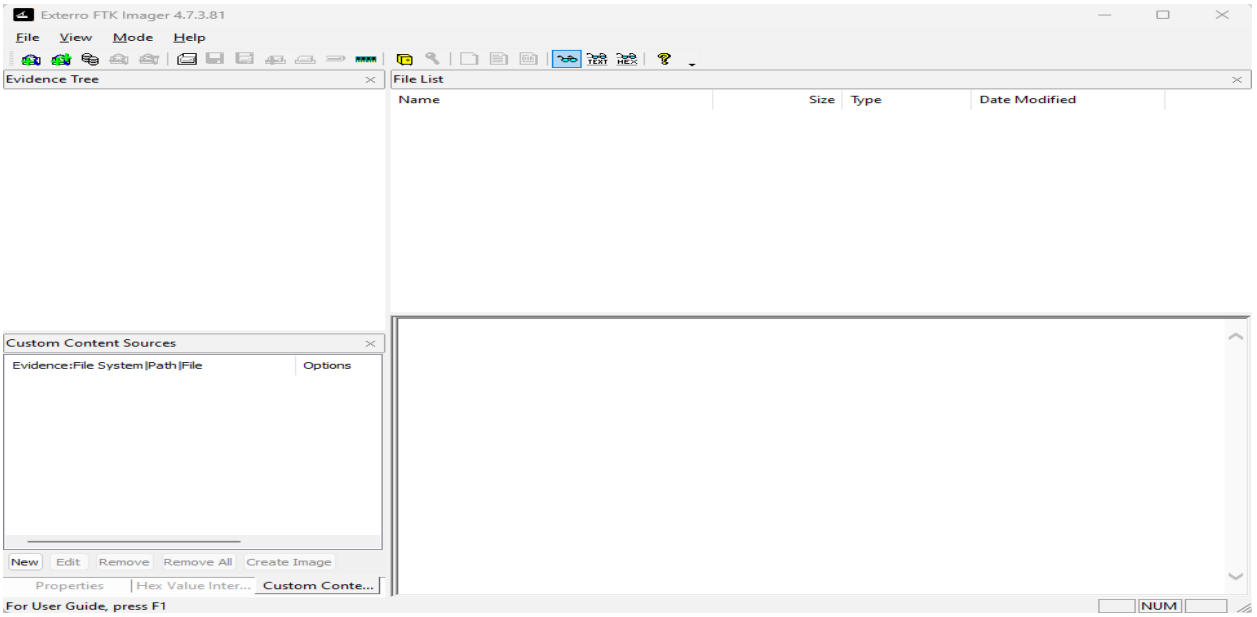

Exterro FTK Imager - InstallShield Wizard
License Agreement
Please read the following license agreement carefully.
exterro FTK
END-USER LICENSE AGREEMENT FOR EXTERRO SOFTWARE
IMPORTANT - READ CAREFULLY
This End-User License Agreement ("EULA") is a legal agreement
I accept the terms in the license agreement
I do not accept the terms in the license agreement
Print
InstallShield
< Back
Next >
Cancel


Exterro FTK Imager - InstallShield Wizard
Destination Folder
Click Next to install to this folder, or click Change to install to a different folder.
exterro FTK
Install Exterro FTK Imager to:
C:\Program Files\AccessData\
Change...
Add Installation File path in Windows Defender Exclusion List
InstallShield
< Back
Next >
Cancel

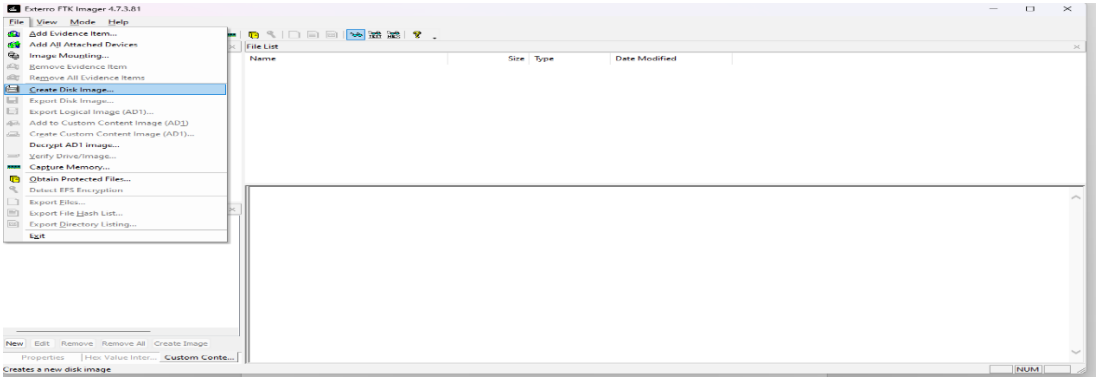

Exterro FTK Imager - InstallShield Wizard
Ready to Install the Program
The wizard is ready to begin installation.
exterro FTK
Click Install to begin the installation.
If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.
InstallShield
< Back
Install
Cancel


Exterro FTK Imager - InstallShield Wizard
exterro FTK
InstallShield Wizard Completed
The InstallShield Wizard has successfully installed Exterro FTK Imager. Click Finish to exit the wizard.
Launch Exterro FTK Imager
< Back
Finish
Cancel

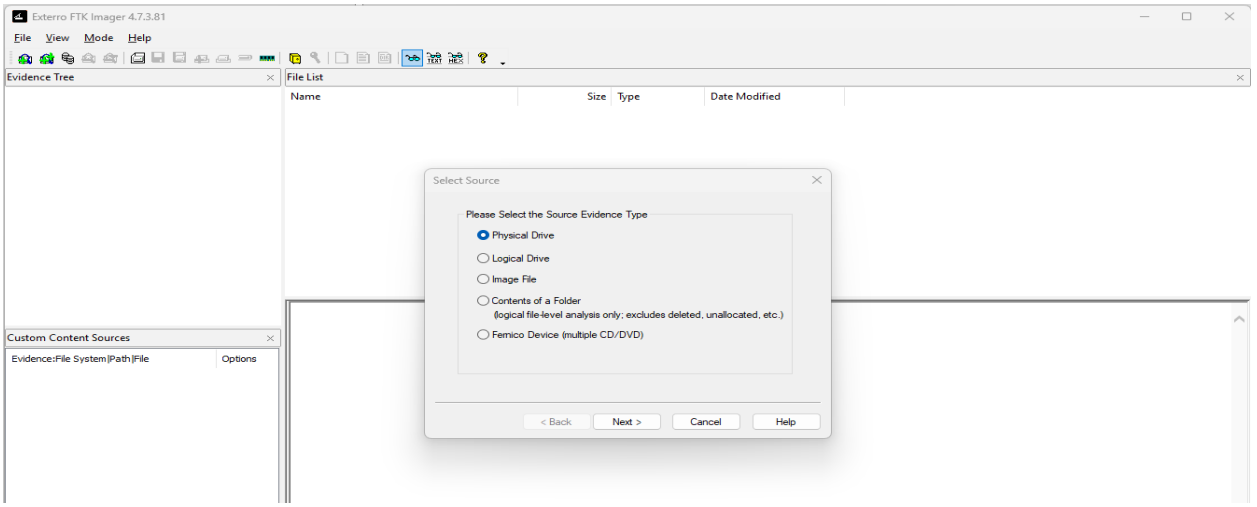
Step 2: Open the Access Data FTK Imager.



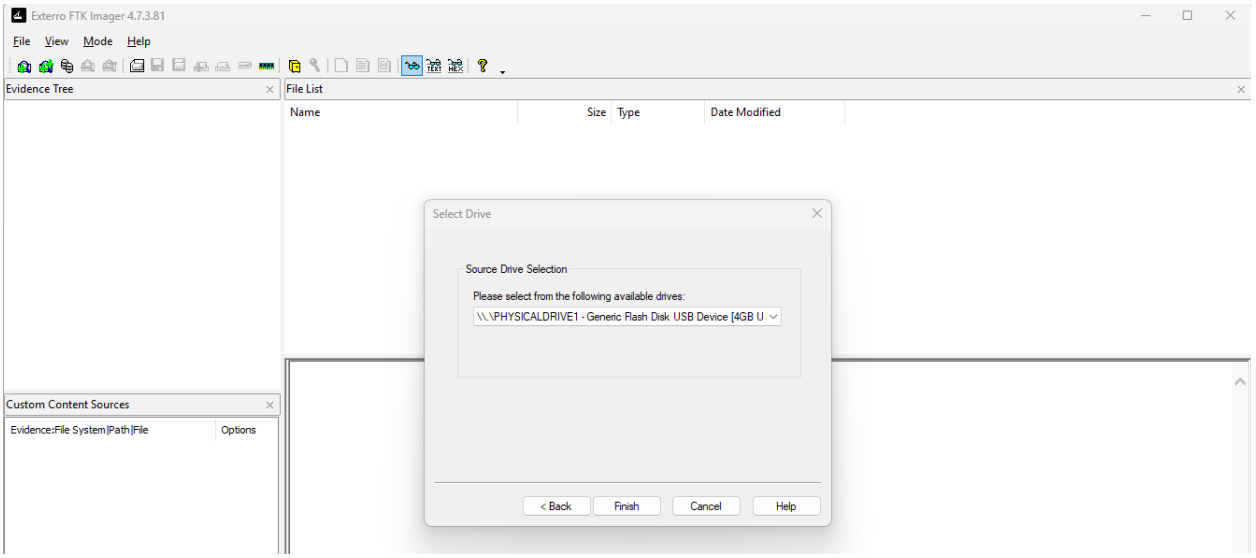
Step 3: Click File, and then Create Disk Image, or click the button on the tool bar.



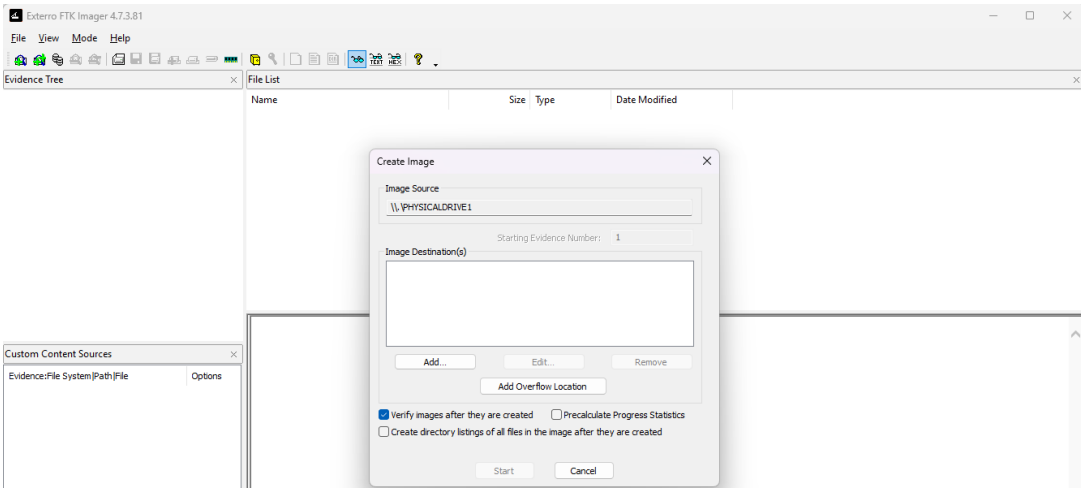
Step 4: Select the source evidence type you want to make an image of and click Next.

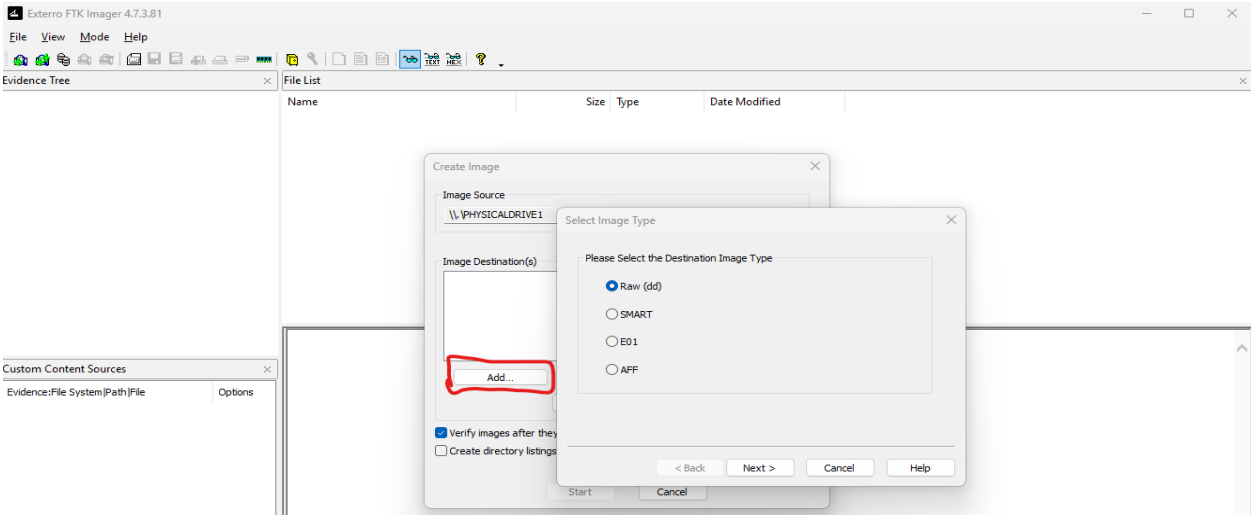


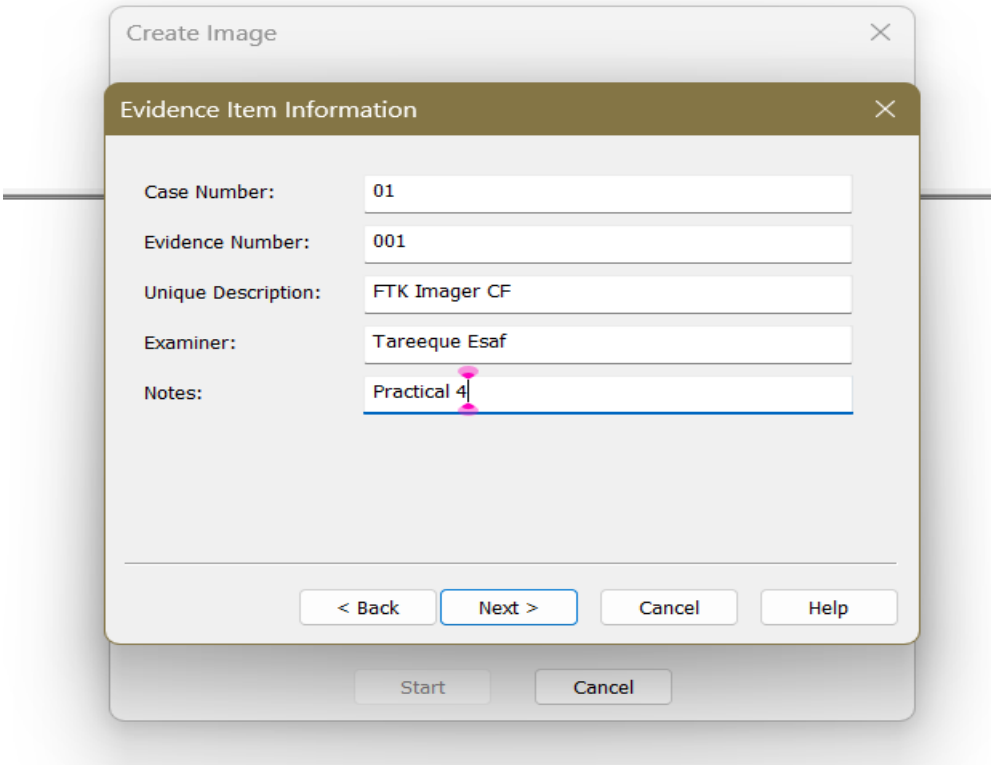
Step 5: Select the source evidence file with path.



Step 6: Click on “add” to add image destination

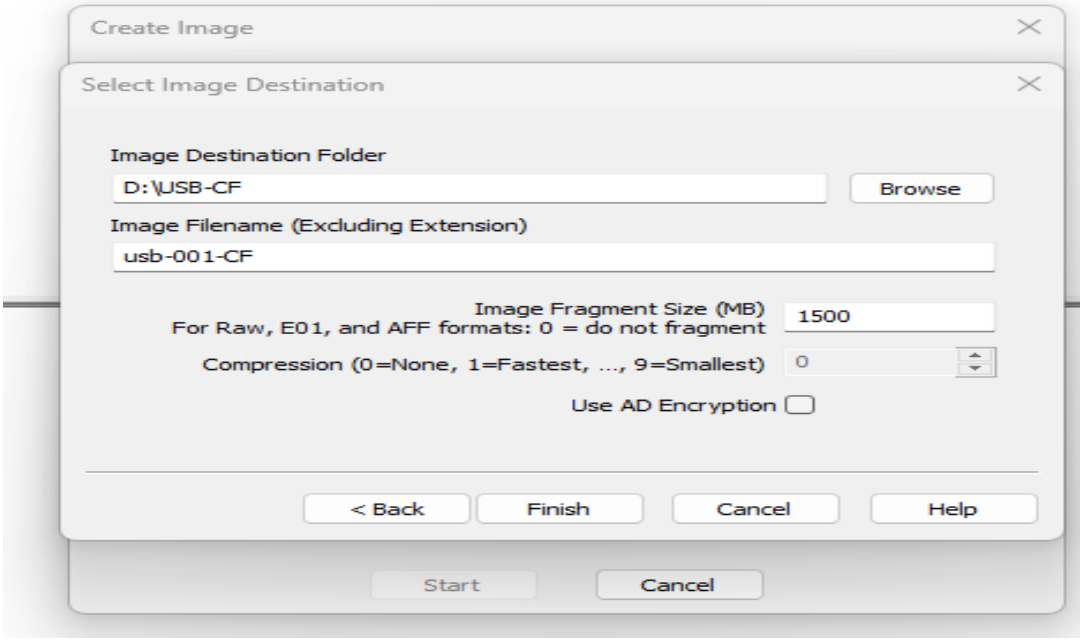


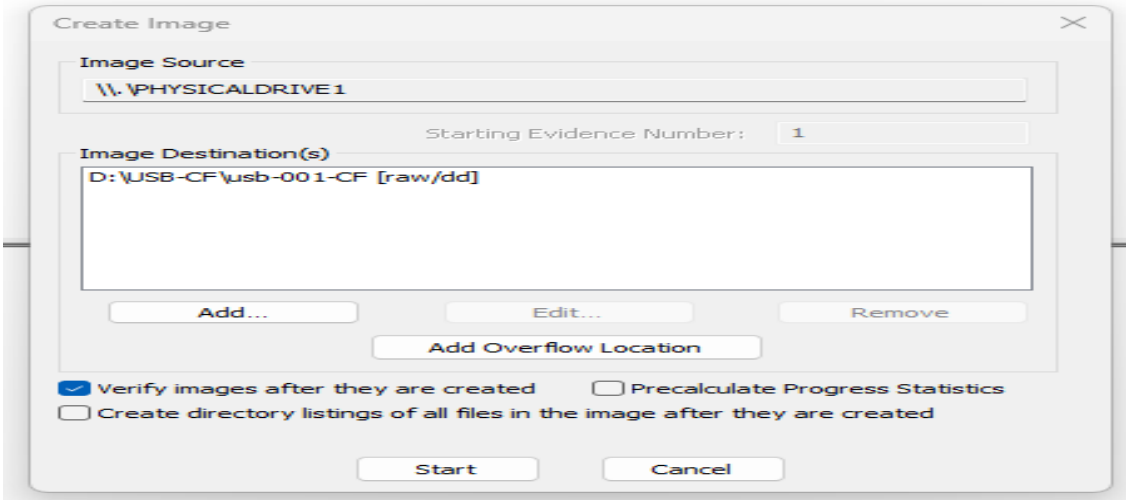




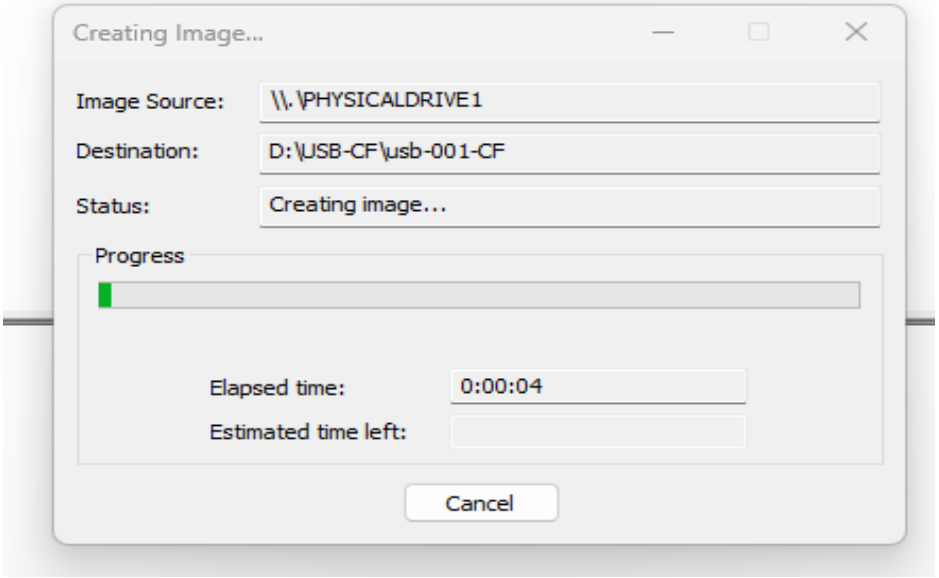
In the Image Destination Folder field, type the location path where you want to save the image file, or click **Browse** to find to the desired location.

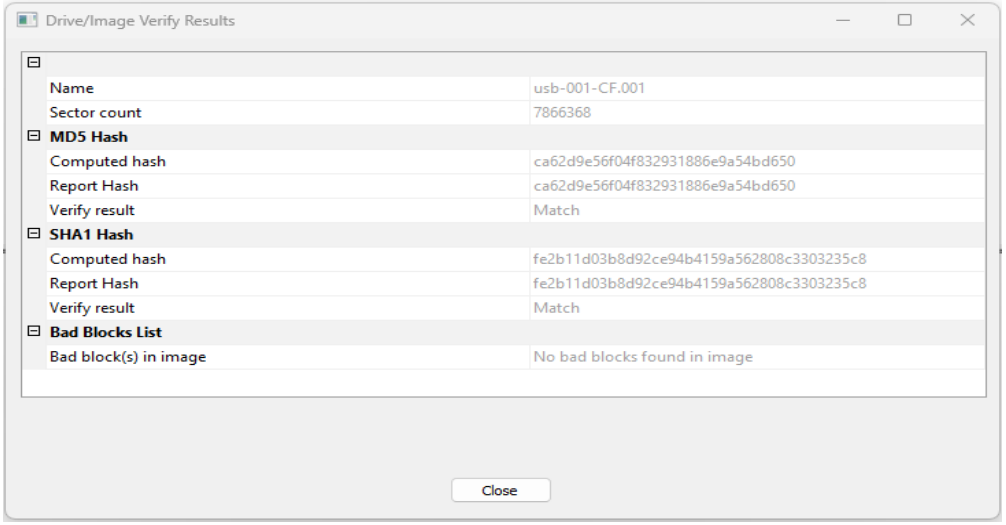
Note: If the destination folder you select is on a drive that does not have sufficient free space to store the entire image file, FTK Imager prompts for a new destination folder when all available space has been used in the first location. In the Image Filename field, specify a name for the image file but do not specify a file extension.





Step 7: After adding the image destination path click on finish and start the image processing.

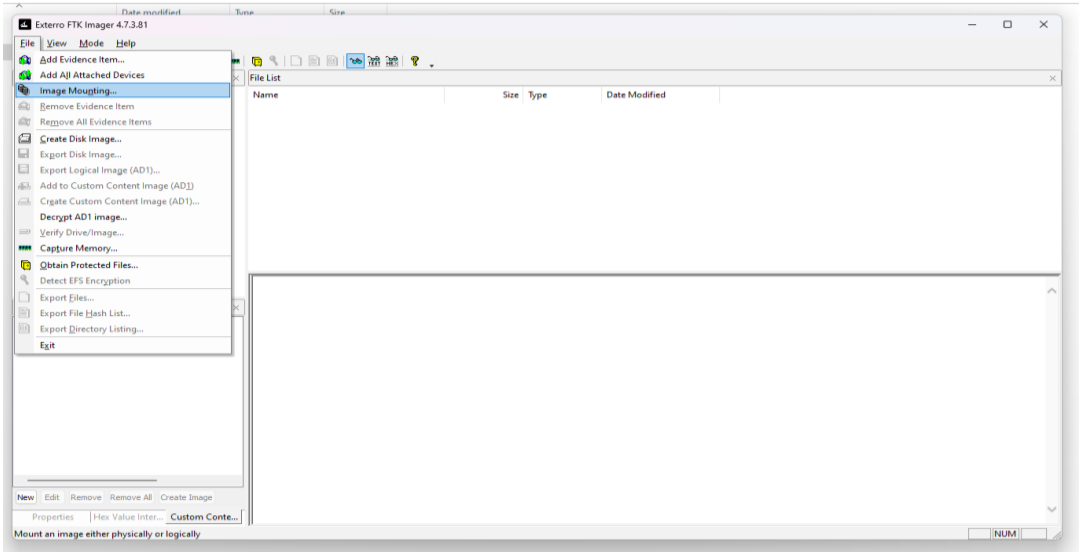


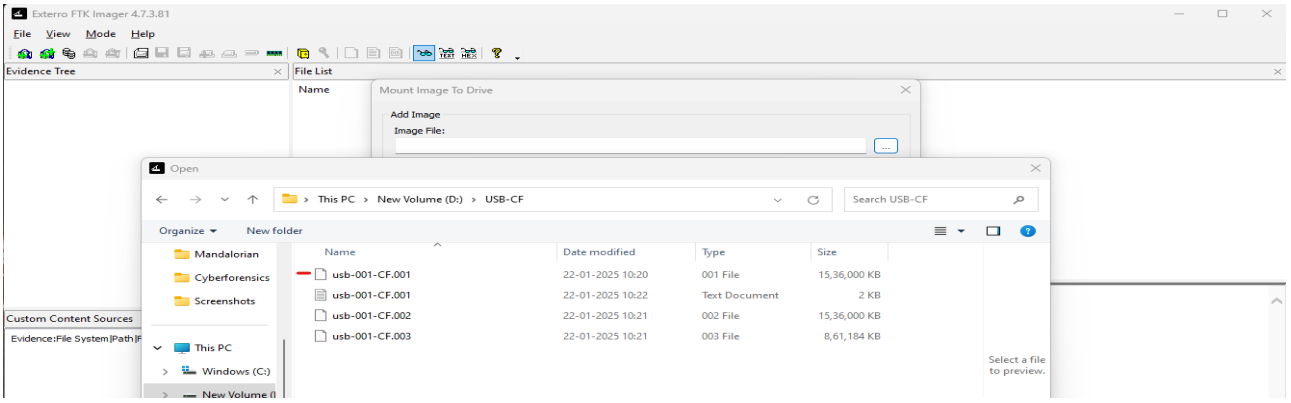


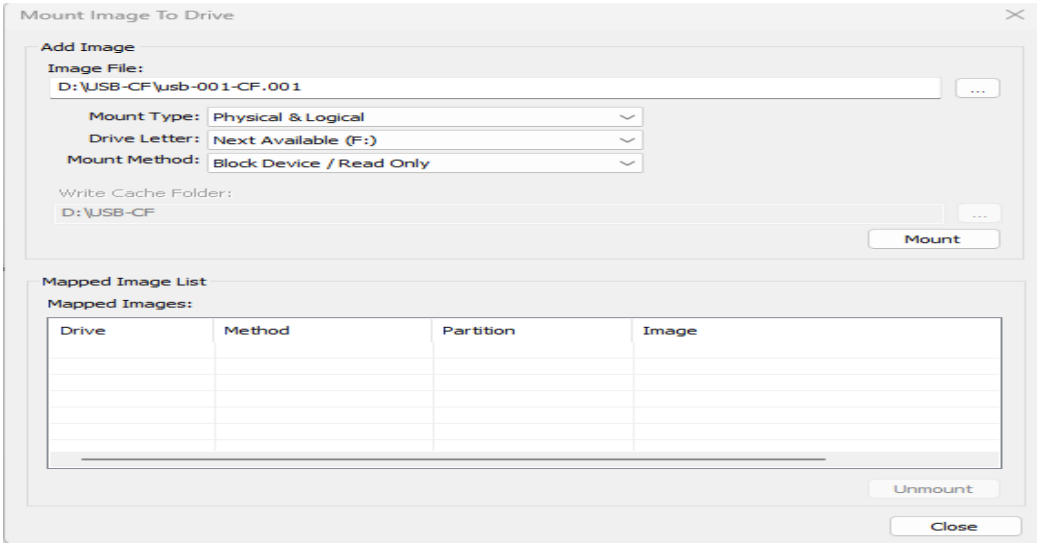
Step 8: After the images are successfully created, click Image Summary to view detailed file information, including MD5 and SHA1 checksums.

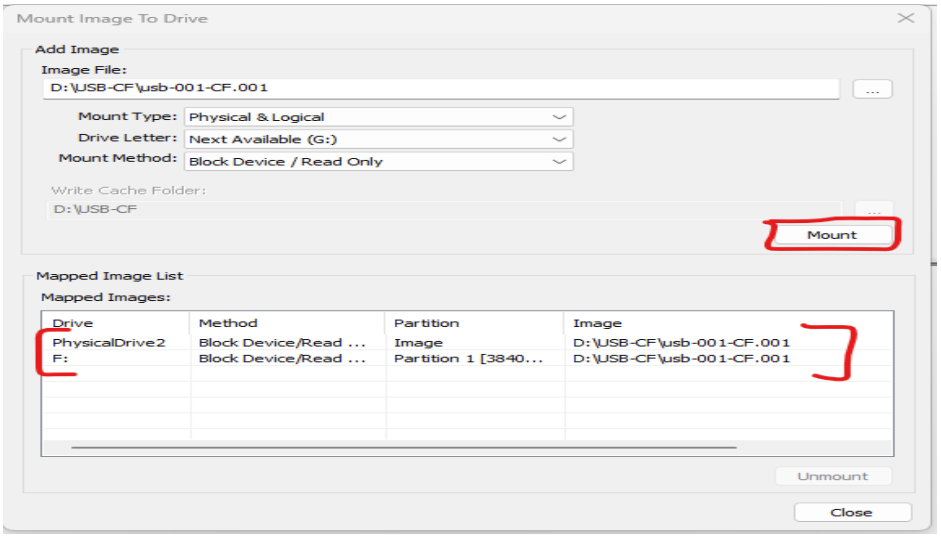
```
Created By Exterro® FTK® Imager 4.7.3.81

Case Information:
Acquired using: ADI4.7.3.81
Case Number: 001
Evidence Number: 001-2025
Unique description: FTK Imager CF
Examiner: Viraj Joshi
Notes: Practical 4

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

Information for D:\USB-CF\usb-001-CF:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 489
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 7,866,368
[Physical Drive Information]
 Drive Model: Generic Flash Disk USB Device
 Drive Serial Number: 0
 Drive Interface Type: USB
 Removable drive: True
 Source data size: 3841 MB
 Sector count:    7866368
[Computed Hashes]
 MD5 checksum:    ca62d9e56f04f832931886e9a54bd650
 SHA1 checksum:   fe2b11d03b8d92ce94b4159a562808c3303235c8

Image Information:
 Acquisition started:   Wed Jan 22 10:19:00 2025
 Acquisition finished:  Wed Jan 22 10:21:54 2025
 Segment list:
  D:\USB-CF\usb-001-CF.001
  D:\USB-CF\usb-001-CF.002
  D:\USB-CF\usb-001-CF.003
 COMPUTED HASH :  ca62d9e56f04f832931886e9a54bd650
 COMPUTED HASH :  fe2b11d03b8d92ce94b4159a562808c3303235c8

Image Verification Results:
 Verification started:  Wed Jan 22 10:21:54 2025
 Verification finished: Wed Jan 22 10:22:03 2025
 MD5 checksum:    ca62d9e56f04f832931886e9a54bd650 : verified
 SHA1 checksum:   fe2b11d03b8d92ce94b4159a562808c3303235c8 : verified
```

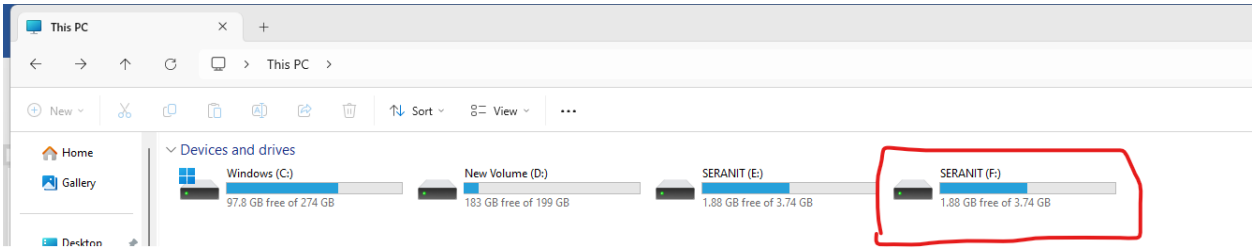
Step 9: Image mounting



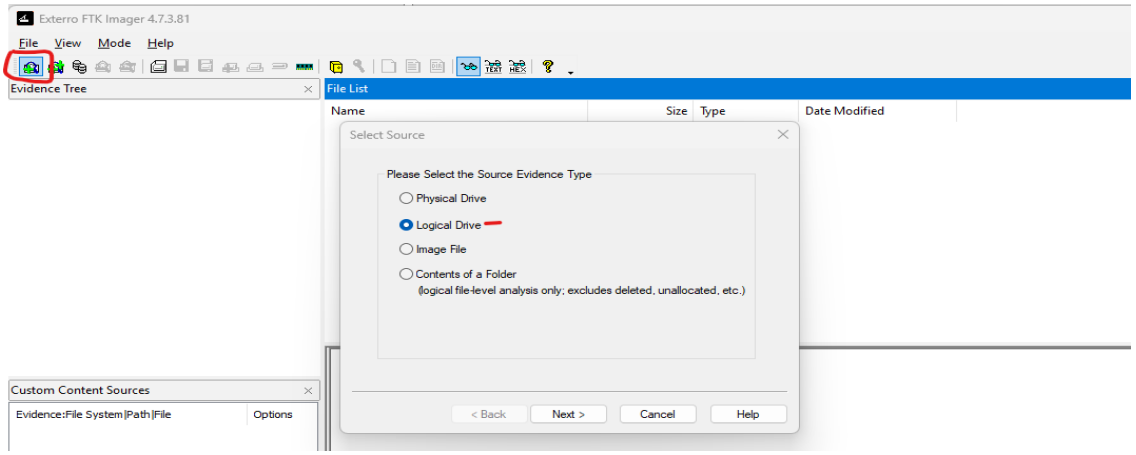


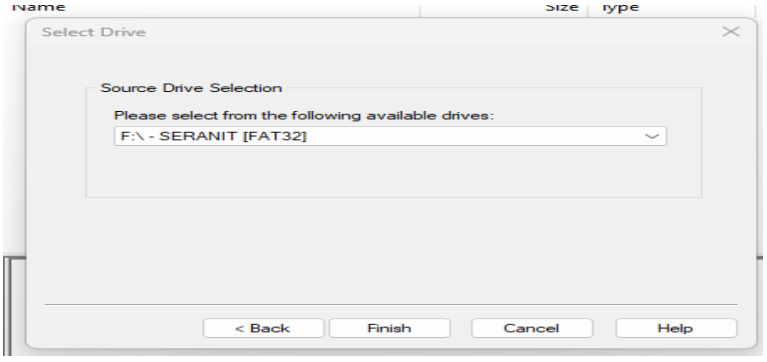


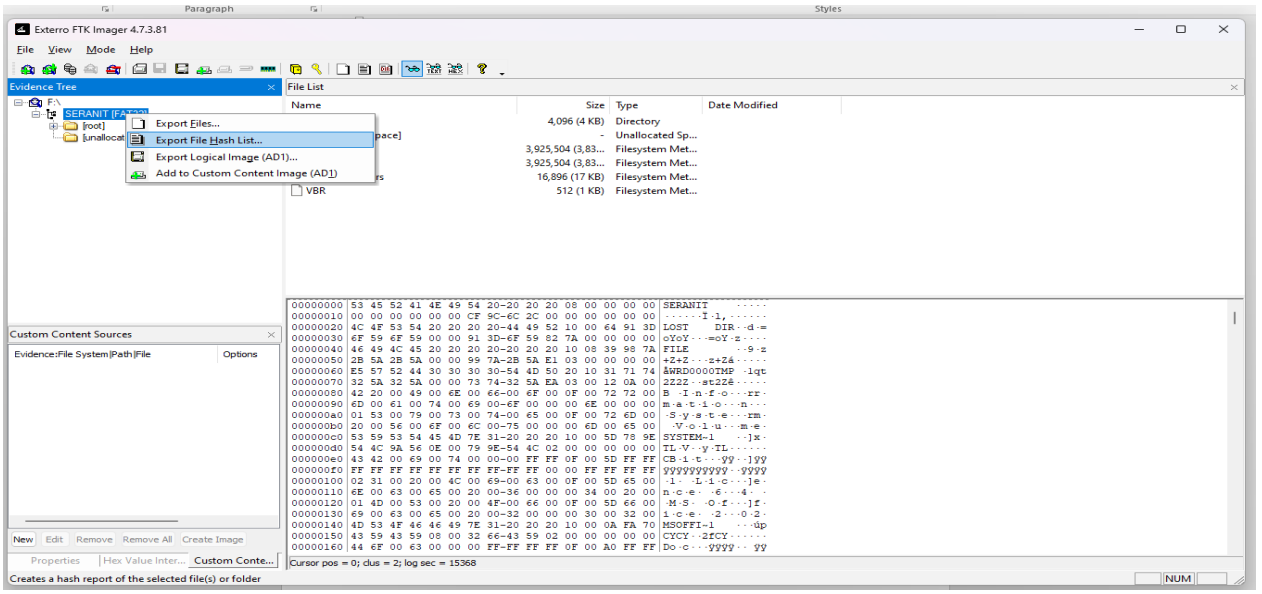


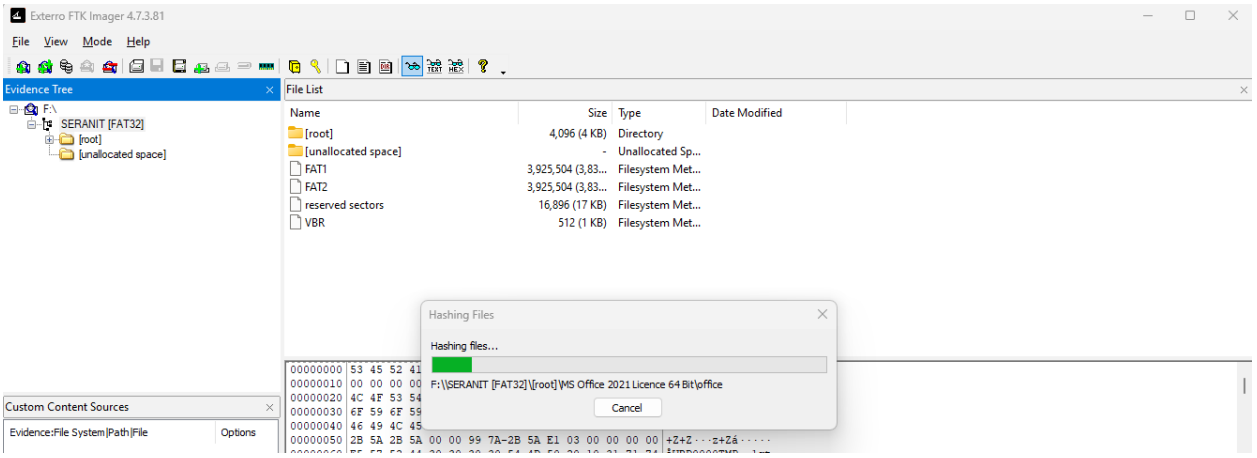


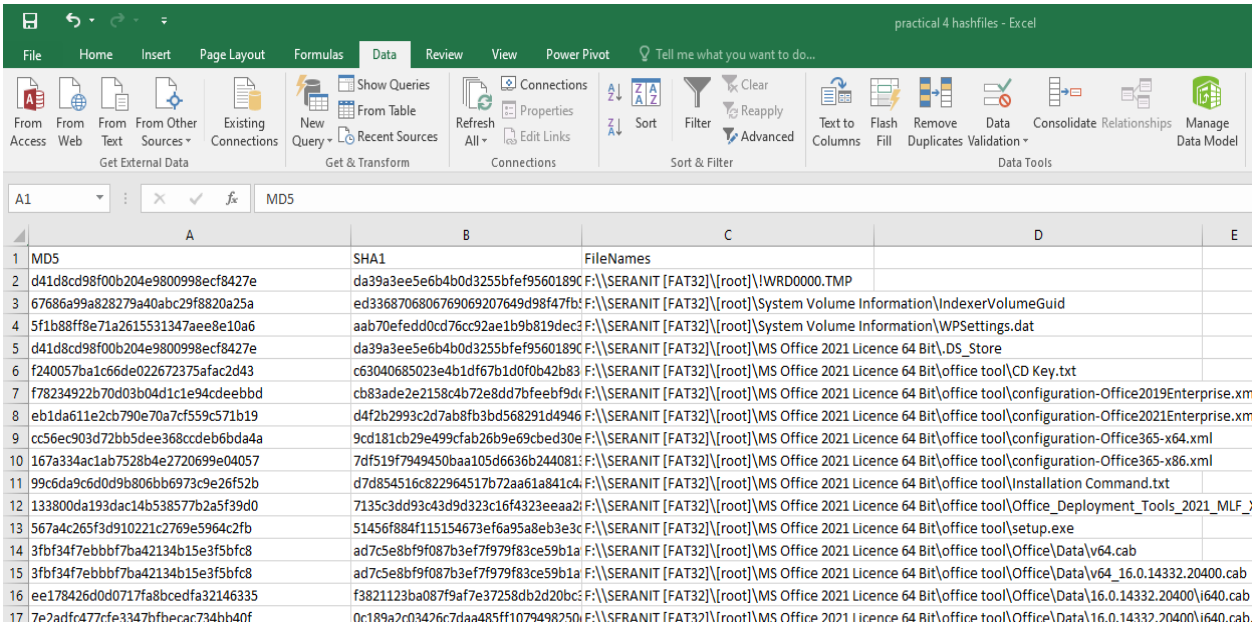
Step 10: Now select the source evidence type as Logical disk







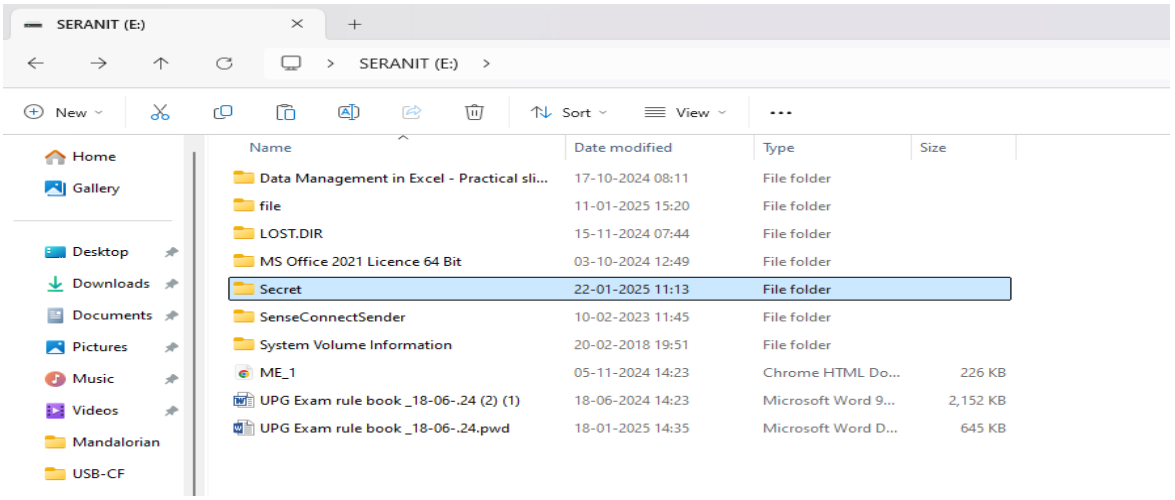




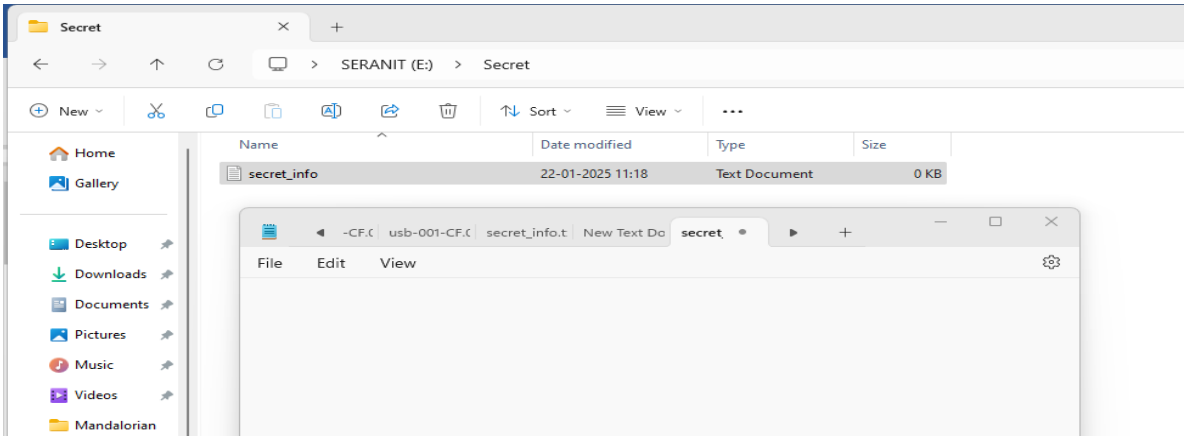
	A	B	C	D	E
1	MD5	SHA1	FileNames		
2	d41d8cd98f00b204e9800998ecf8427e	da39a3ee5e6b4b0d3255bfef95601890	F:\\SERANIT [FAT32]\[root]\!WRD0000.TMP		
3	67686a99a828279a40abc29f8820a25a	ed3368706806769069207649d98f47fb5	F:\\SERANIT [FAT32]\[root]\System Volume Information\IndexerVolumeGuid		
4	5f1b88ff8e71a2615531347aee8e10a6	aab70efedd0cd76cc92ae1b9b819dec3	F:\\SERANIT [FAT32]\[root]\System Volume Information\WPSettings.dat		
5	d41d8cd98f00b204e9800998ecf8427e	da39a3ee5e6b4b0d3255bfef95601890	F:\\SERANIT [FAT32]\[root]\MS Office 2021 Licence 64 Bit\.DS_Store		
6	f240057ba1c66de022672375afac2d43	c63040685023e4b1df67b1d0f0b42b83	F:\\SERANIT [FAT32]\[root]\MS Office 2021 Licence 64 Bit\office tool\CD Key.txt		
7	f78234922b70d03b04d1c1e94cdeebbd	cb83ade2e2158c4b72e8dd7bfeebf9d6	F:\\SERANIT [FAT32]\[root]\MS Office 2021 Licence 64 Bit\office tool\configuration-Office2019Enterprise.xm		
8	eb1da611e2cb790e70a7cf559c571b19	d4f2b2993c2d7ab8fb3bd568291d4946	F:\\SERANIT [FAT32]\[root]\MS Office 2021 Licence 64 Bit\office tool\configuration-Office2021Enterprise.xm		
9	cc56ec903d72bb5dee368ccdeb6bda4a	9cd181cb29e499cfab26b9e69cbed30e	F:\\SERANIT [FAT32]\[root]\MS Office 2021 Licence 64 Bit\office tool\configuration-Office365-x64.xml		
10	167a334ac1ab7528b4e2720699e04057	7df519f7949450baa105d6636b244081	F:\\SERANIT [FAT32]\[root]\MS Office 2021 Licence 64 Bit\office tool\configuration-Office365-x86.xml		
11	99c6da9c6d0d9b806bb6973c9e26f52b	d7d854516c822964517b72aa61a841c4	F:\\SERANIT [FAT32]\[root]\MS Office 2021 Licence 64 Bit\office tool\Installation Command.txt		
12	133800da193dac14b538577b2a5f39d0	7135c3dd93c43d9d323c16f4323eeaa2	F:\\SERANIT [FAT32]\[root]\MS Office 2021 Licence 64 Bit\office tool\Office_Deployment_Tools_2021_MLF_		
13	567a4c265f3d910221c2769e5964c2fb	51456f884f115154673ef6a95a8eb3e3c	F:\\SERANIT [FAT32]\[root]\MS Office 2021 Licence 64 Bit\office tool\setup.exe		
14	3fbf34f7ebbbf7ba42134b15e3f5bfc8	ad7c5e8bf9f087b3ef7f979f83ce59b1a	F:\\SERANIT [FAT32]\[root]\MS Office 2021 Licence 64 Bit\office tool\Office\Data\v64.cab		
15	3fbf34f7ebbbf7ba42134b15e3f5bfc8	ad7c5e8bf9f087b3ef7f979f83ce59b1a	F:\\SERANIT [FAT32]\[root]\MS Office 2021 Licence 64 Bit\office tool\Office\Data\v64_16.0.14332.20400.cab		
16	ee178426d0d0717fa8bcedfa32146335	f3821123ba087f9af7e37258db2d20bc3	F:\\SERANIT [FAT32]\[root]\MS Office 2021 Licence 64 Bit\office tool\Office\Data\16.0.14332.20400\i640.cab		
17	7e2adfc477cfe3347bfbecac734bb40f	0c189a2c03426c7daa485ff1079498250	F:\\SERANIT [FAT32]\[root]\MS Office 2021 Licence 64 Bit\office tool\Office\Data\16.0.14332.20400\i640.cab		

B) Encryption detection using FTK imager

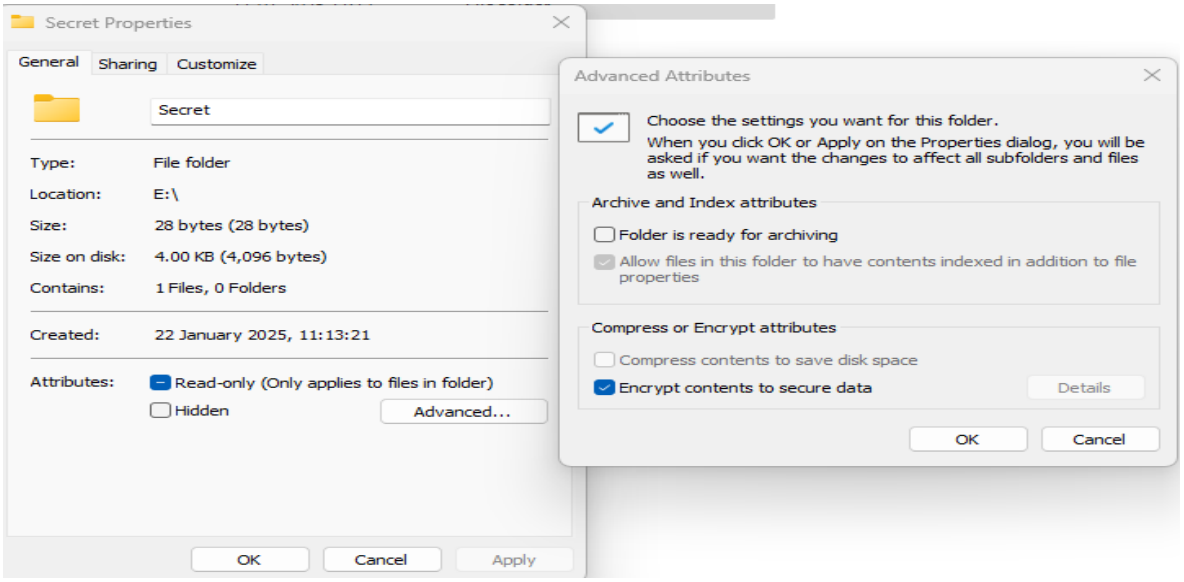
Step 1: Create a folder name Secret

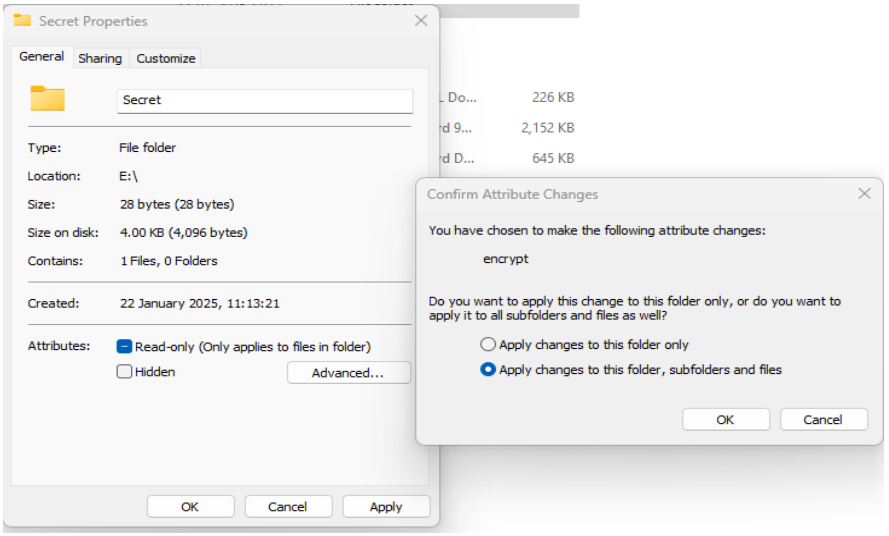


Step 2: Create a textfile

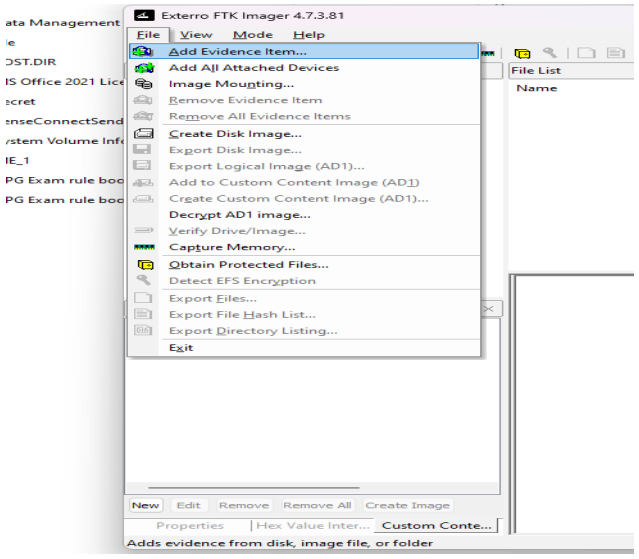


Step 3: Go to properties, select advanced and click on Encrypt content to secure data

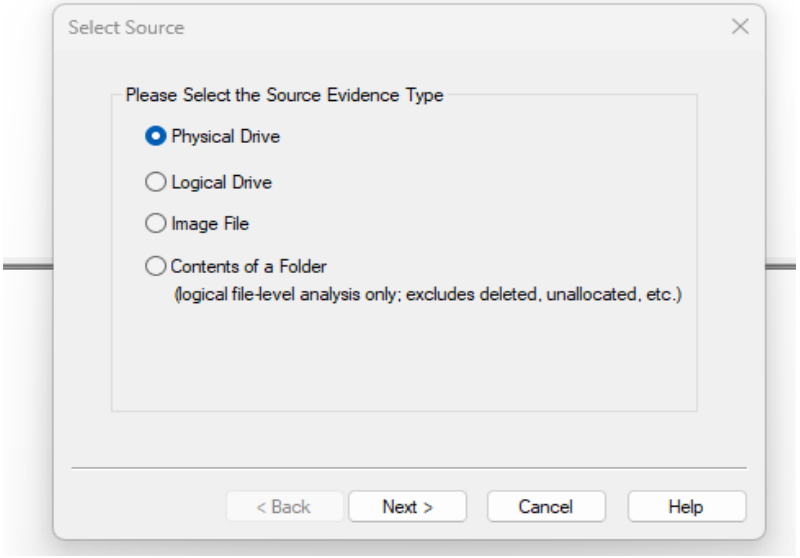




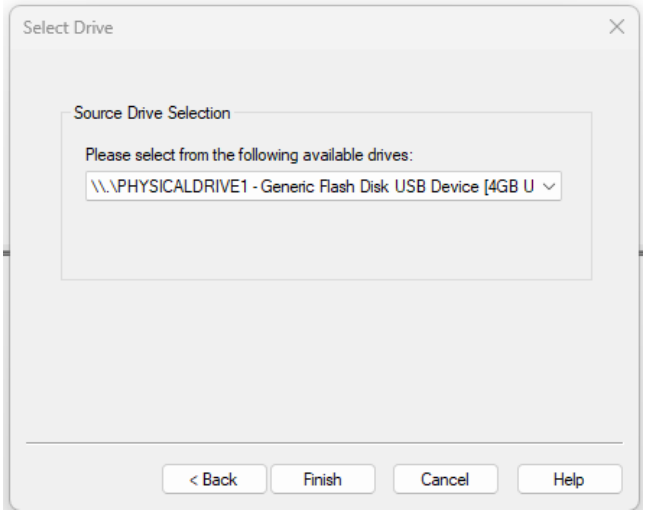
Step 4: Now open FTK Imager



Step 5: Add the physical drive



Step 6: Select your USB



Practical: 5

Aim: (A)Web Attack Detection Problem Statement: Detecting web attack on the data packets.

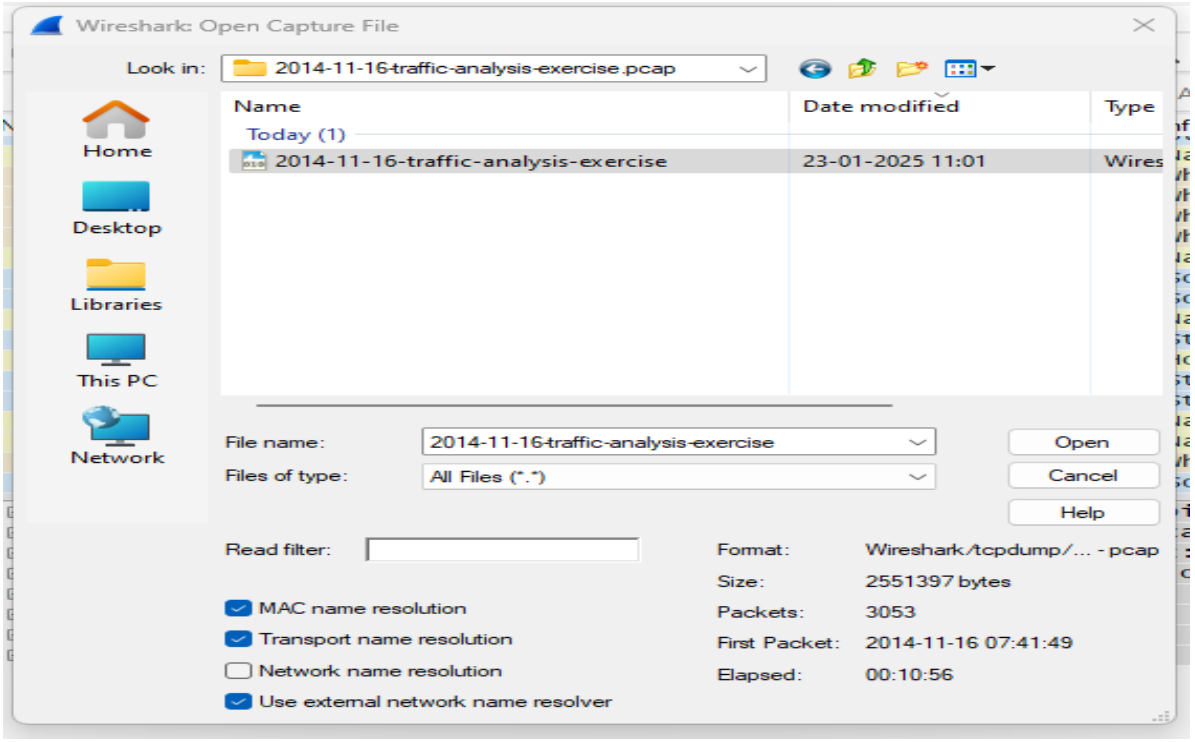
Theory

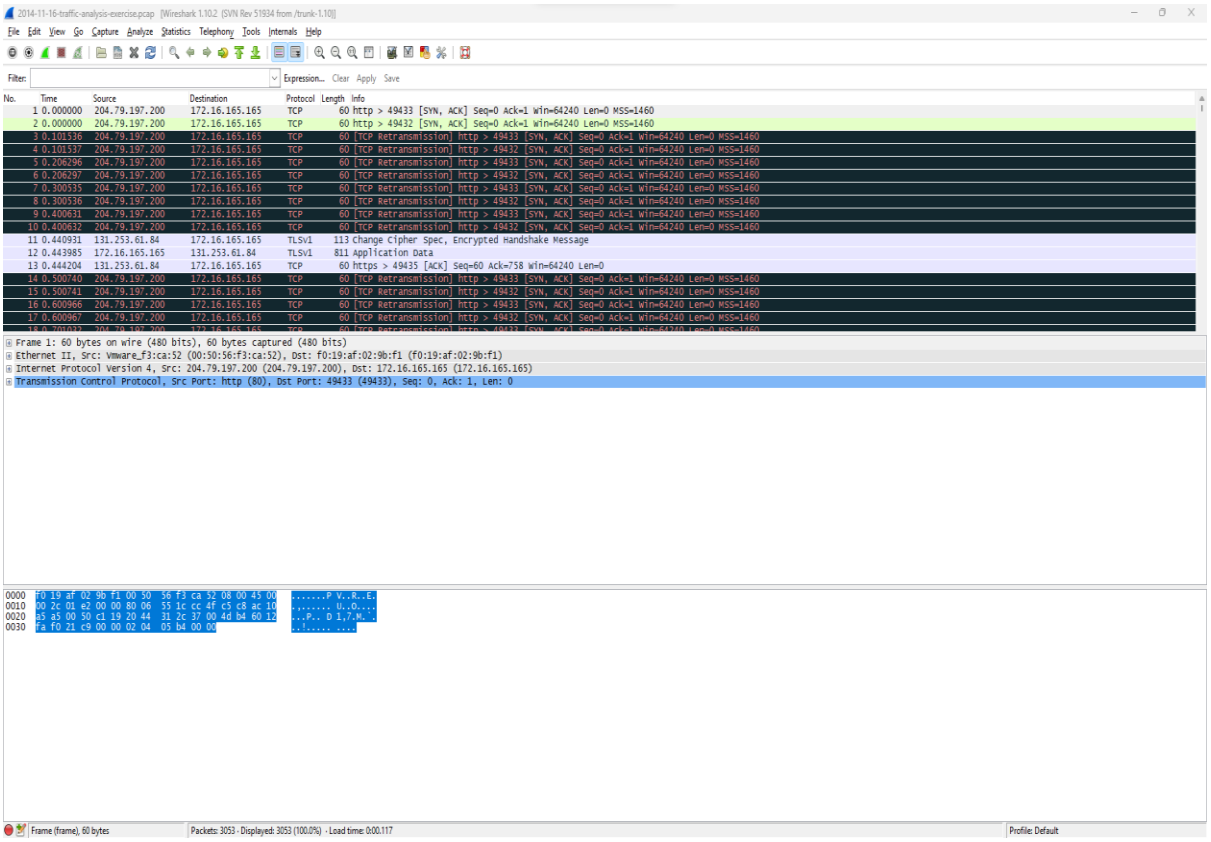
Wireshark is a packet sniffer and analysis tool. It captures network traffic on the local networkand stores that data for offline analysis. Wireshark captures network traffic from Ethernet, Bluetooth, Wireless (IEEE.802.11), Token Ring, Frame Relay connections, and more. Wireshark allows you to filter the log either before the capture starts or during analysis, so youcan narrow down and zero into what you are looking for in the network trace

Steps: Here we have used Sample Packets for Detection form https://www.malware-traffic-analysis.net/

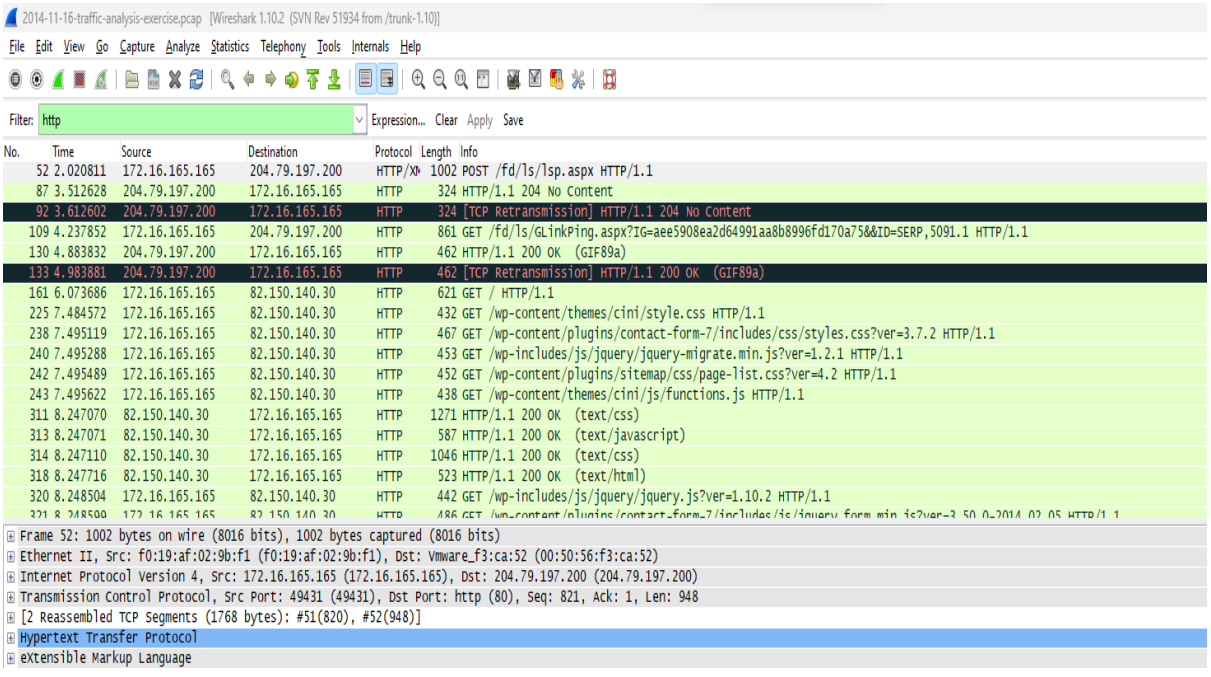
- **2014-12-15 -- Traffic analysis exercise - 1 pcap, 3 Windows hosts, and 1 EK.**
- **2014-12-08 -- Traffic analysis exercise - Questions about EK traffic.**
- **2014-12-04 -- Traffic analysis exercise - Questions about EK traffic.**
- **2014-11-23 -- Traffic analysis exercise - Questions about EK traffic.**
- **2014-11-16 -- Traffic analysis exercise - Questions about EK traffic.**

Choose the file. Enter password: infected_20141116

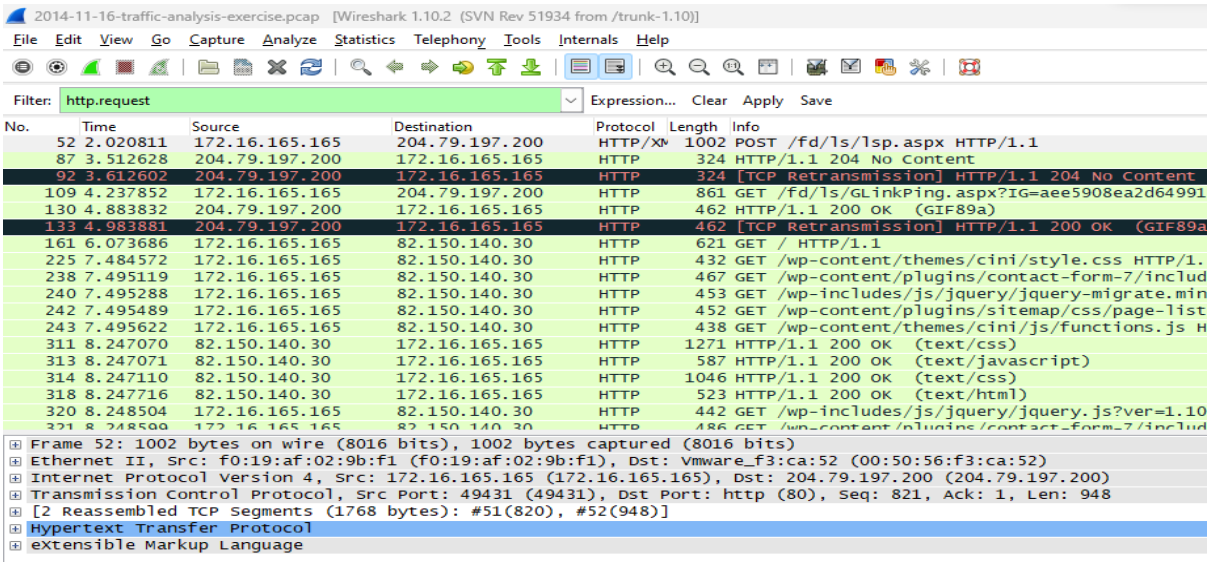




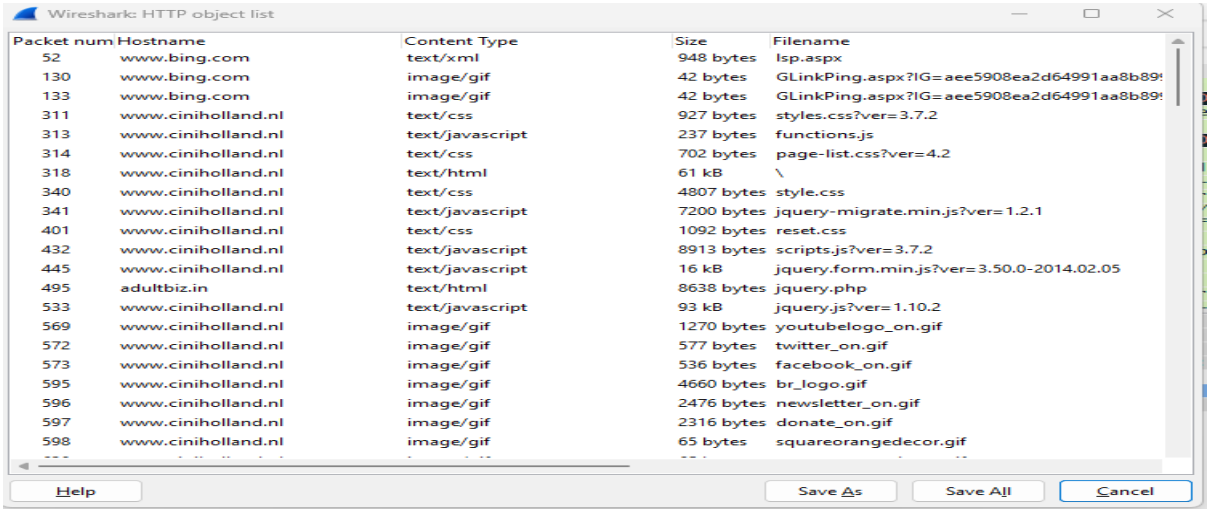
We have filter the packets. Now only http packets are only been displayed.



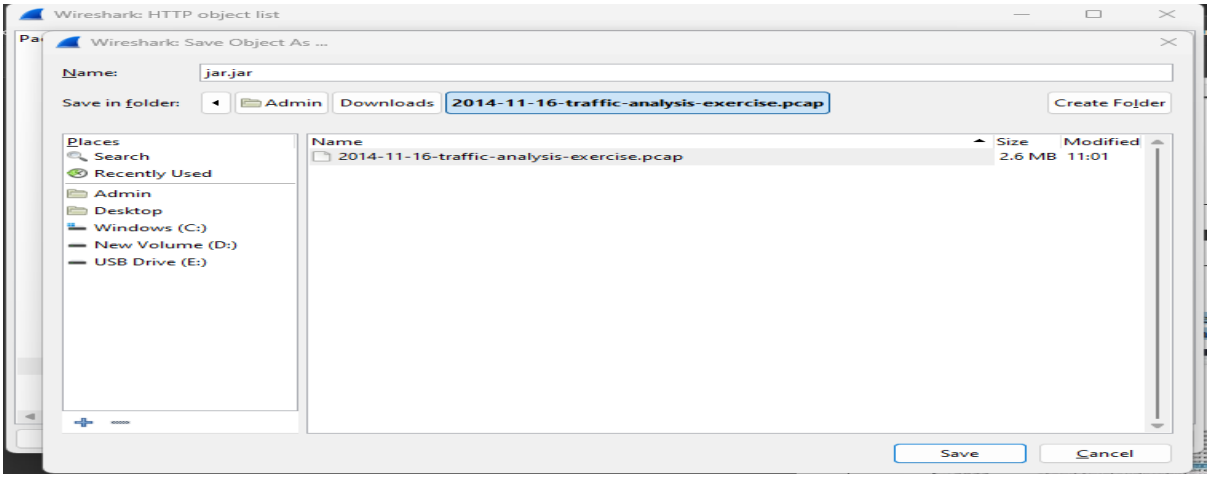
Narrow down the search to http.request which will show only the GET/POST requests



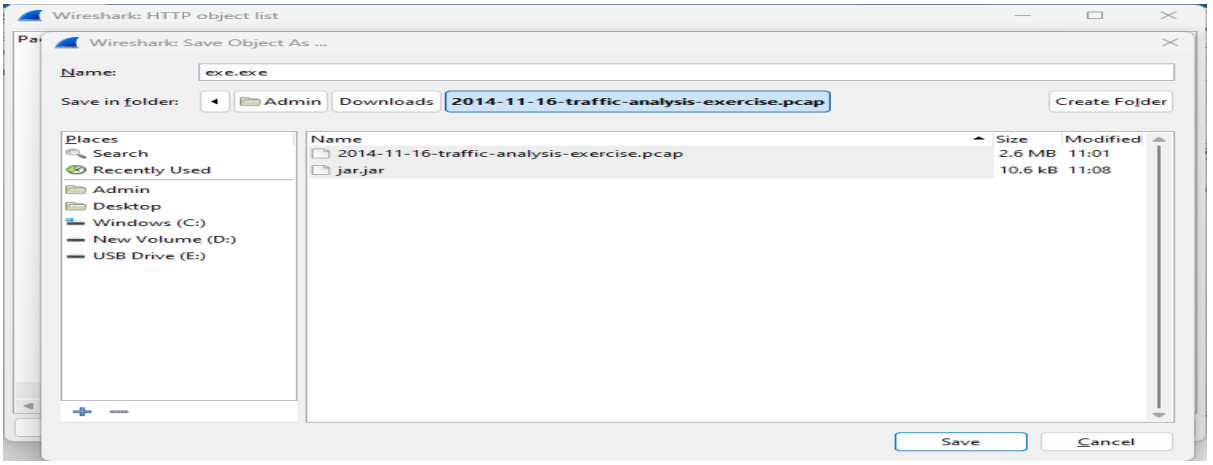
Now go to File -> Export Objects -> HTTP You will get a Window like this Here you will see all the HTTP objects which are downloaded in this Packet



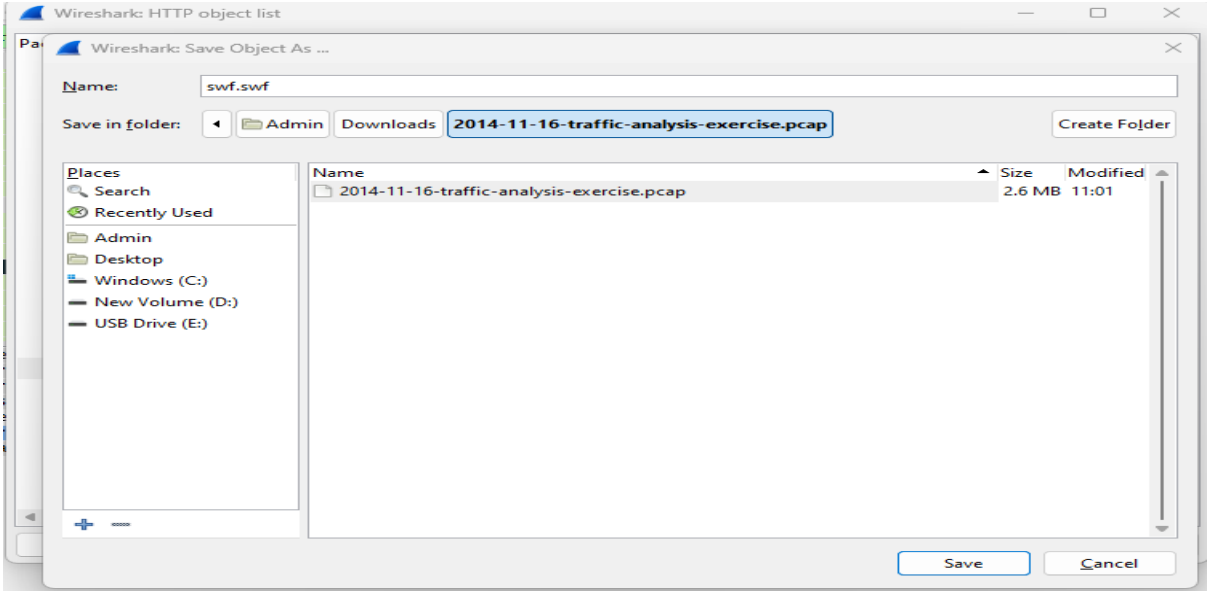
Will see from above objects weather the file is affected or not by selecting the file to detect the virus Select the java file and click on save. Save the file with extension .jar



Similarly select other two files and save it one by oneExtension .exe

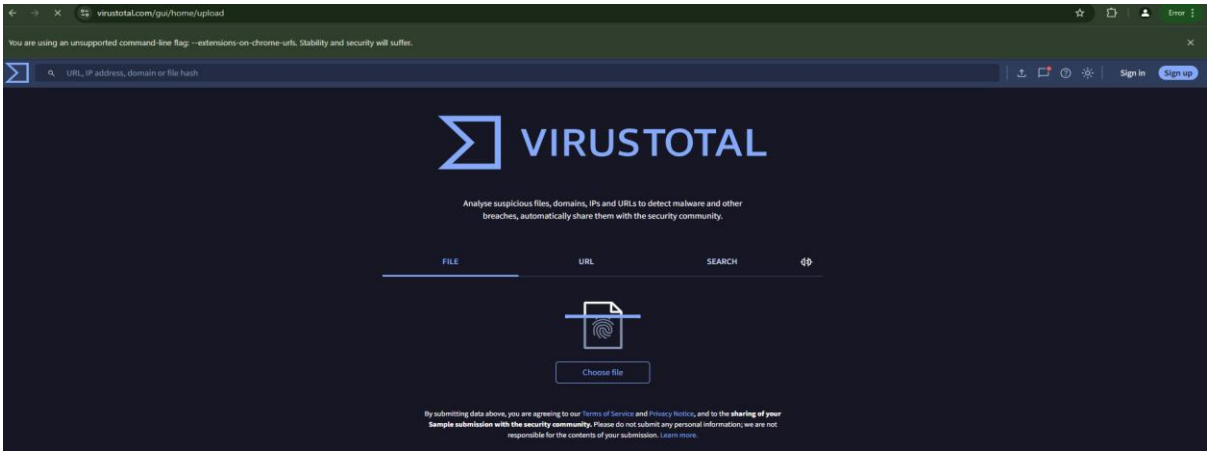


Extension .swf

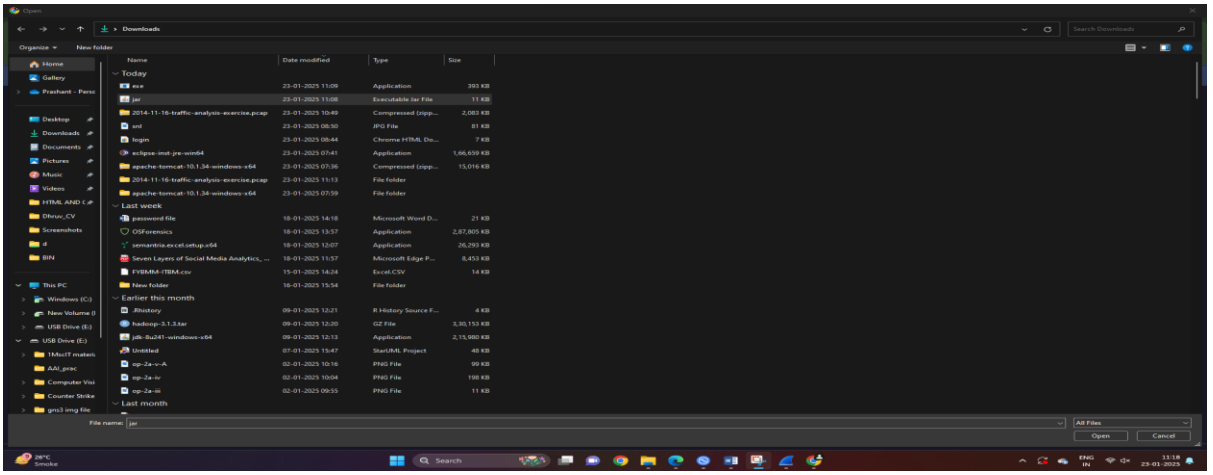


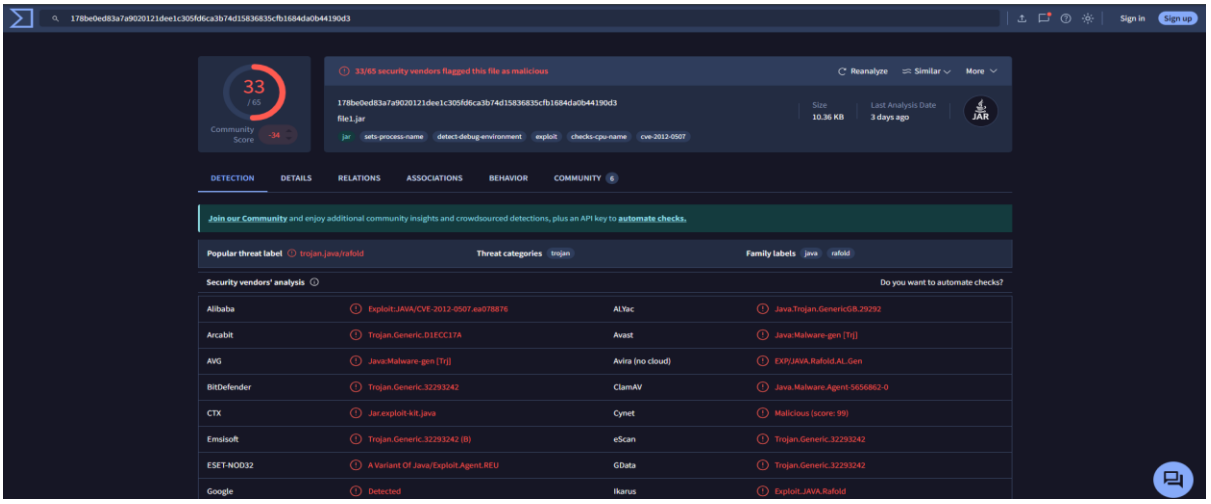
When you are looking for malware, use content and application type of file. So, here we have used java, executable and shockwave flash files. All files are saved in the system.

Go to browser and open virustotal.com

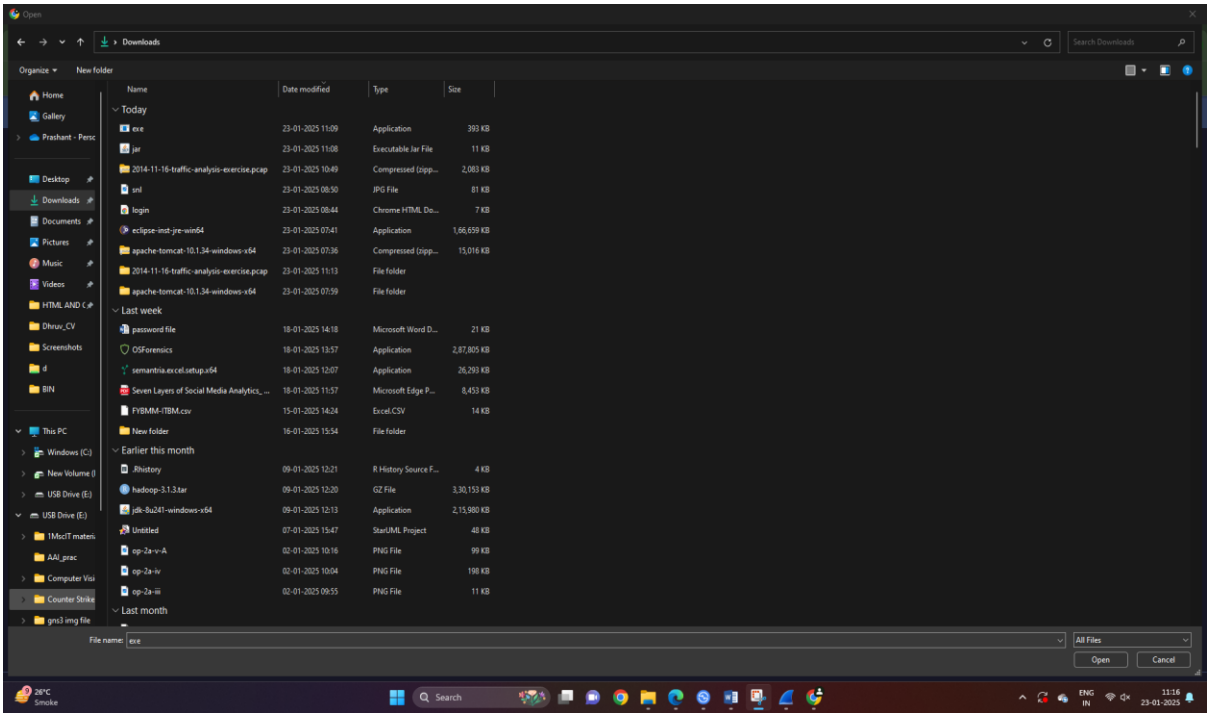


Click on choose file select the .jar file which was saved earlier

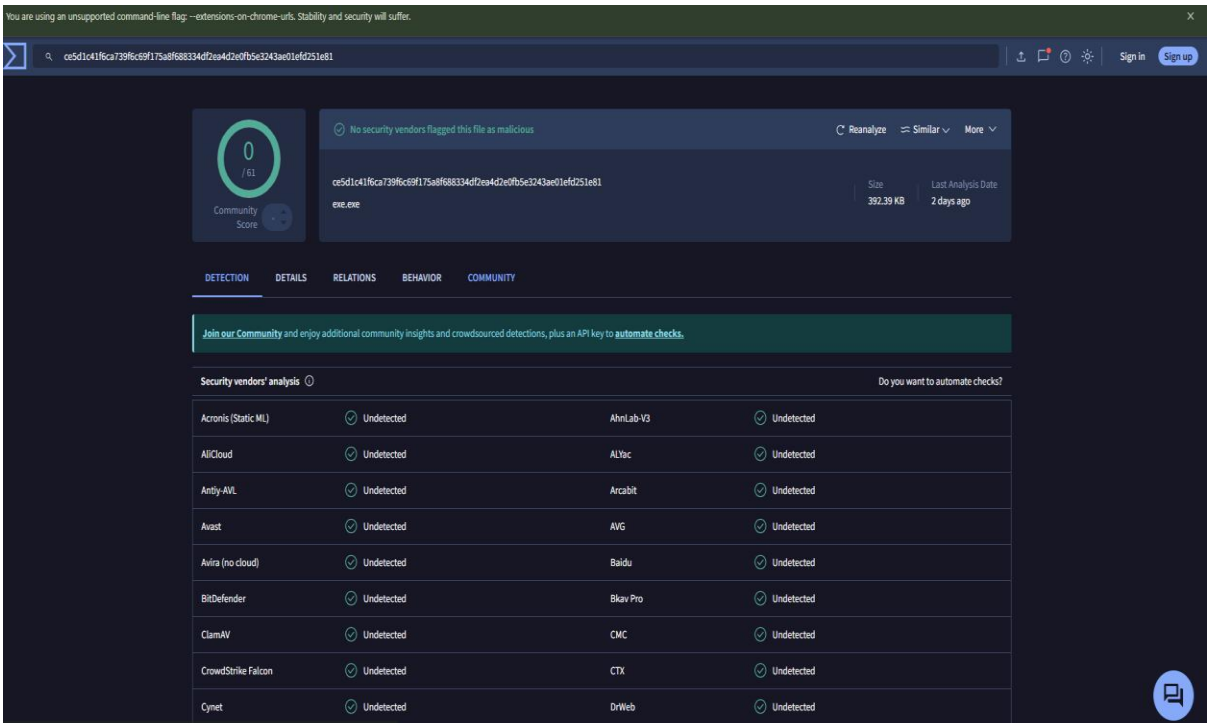




Click on choose file select the .exe file which was saved earlier



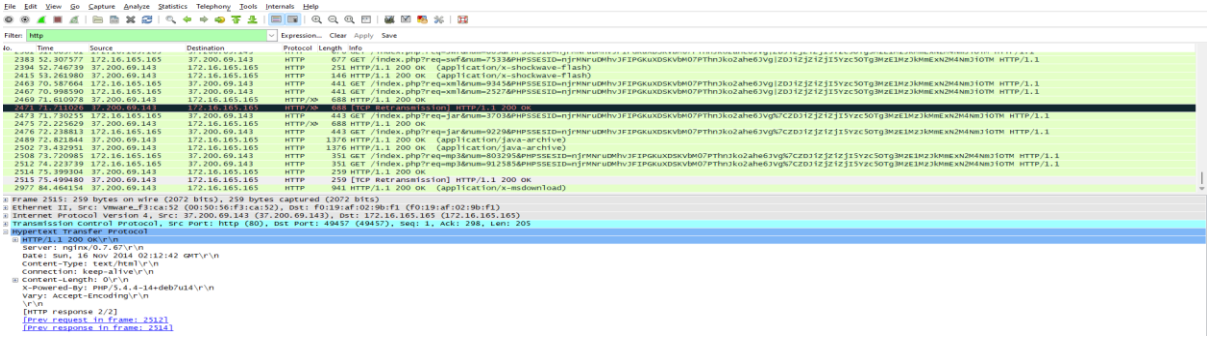
Click on open Virus total will calculate the hash value of the file and then detects whether the files is malicious or not. Here the malicious attack has been detected. It is infected file.



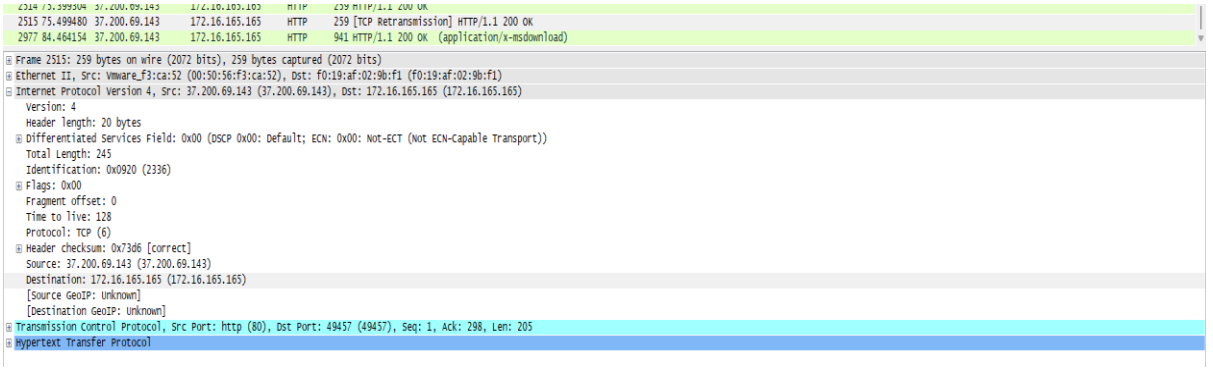
.swf file is infected

To know other details about the detected malware.What is the url of infected site?

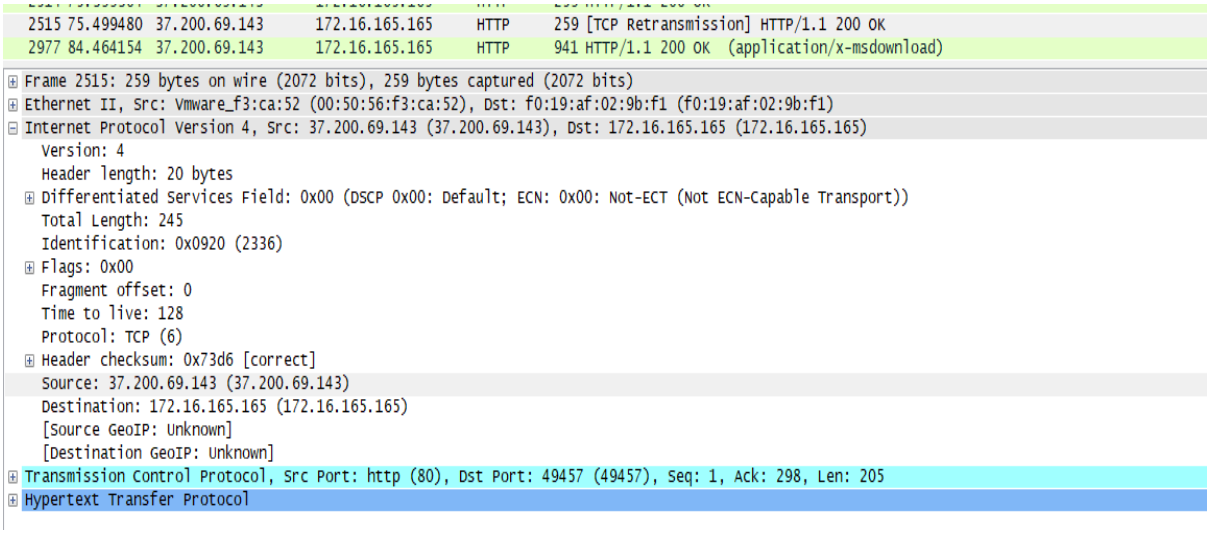
Select the packet and view the detail information



What is the IP address of infected website?



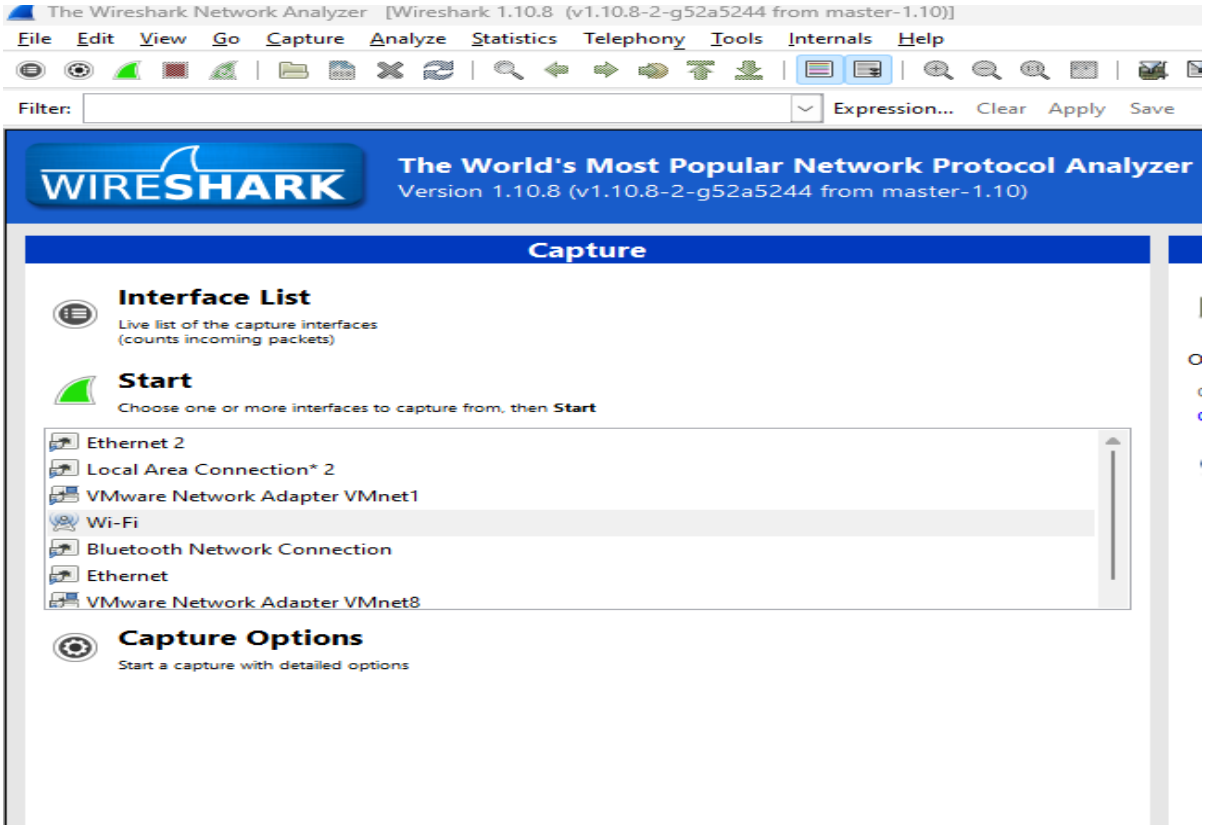
What is the IP address of infected machine?



B. Traffic Capturing and Analysis.

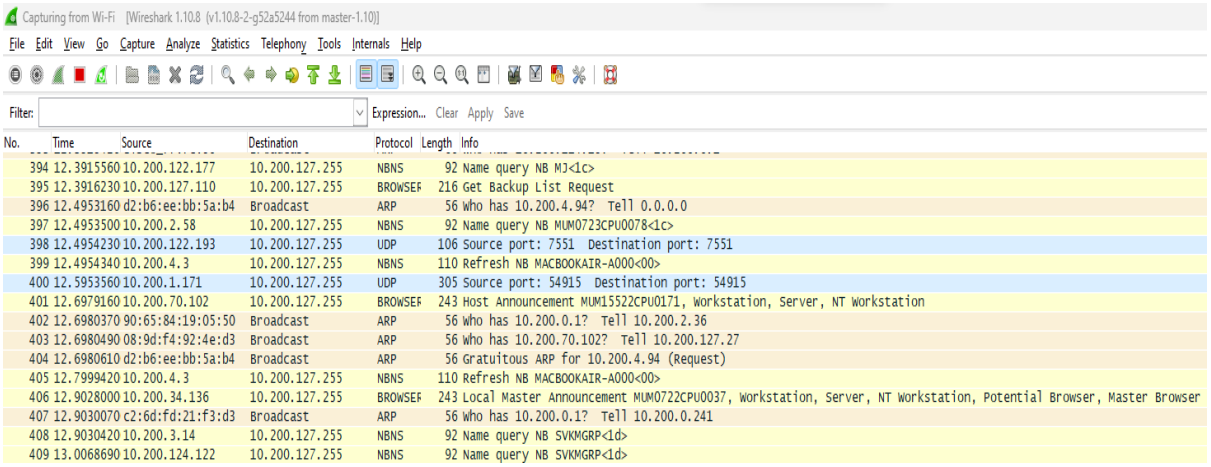
Capturing Packets

Capture traffic on your wireless network, click your wireless interface. You can configure advanced features by clicking Capture > Options, but this isn't necessary for now.



As soon as you single-click on your network interface's name, you can see how the packets are working in real time. Wireshark will capture all the packets going in and out of our systems.

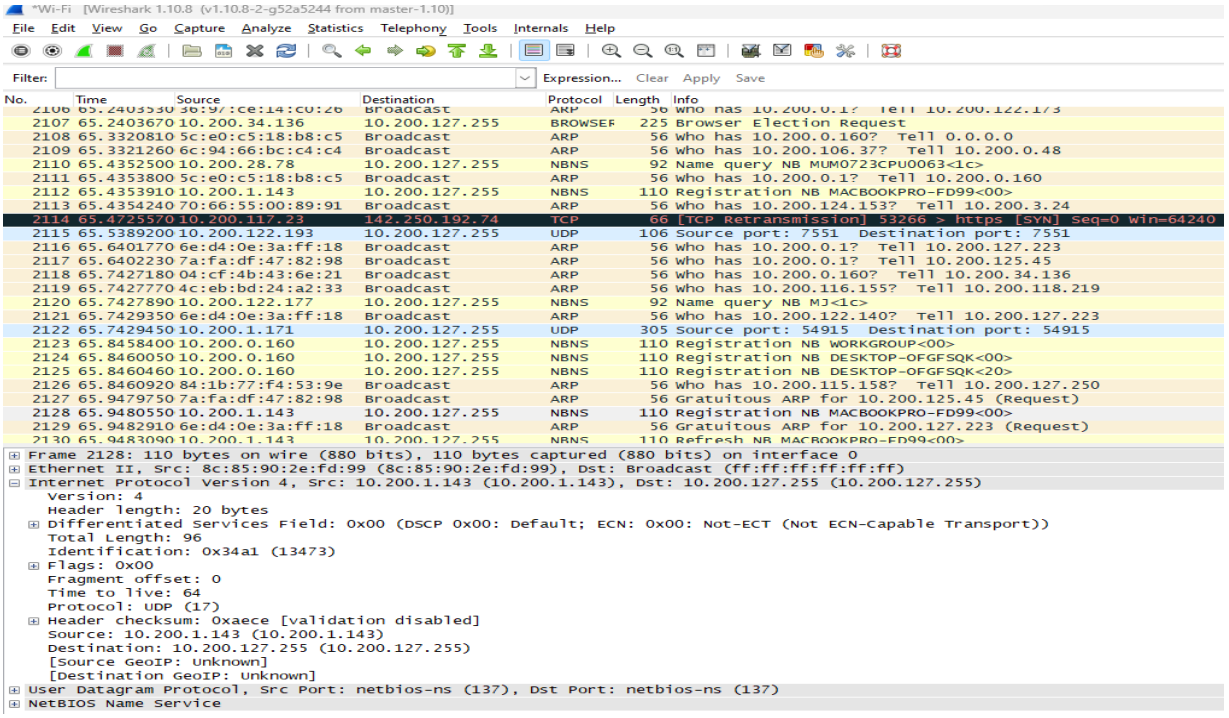
Promiscuous mode is the mode in which you can see all the packets from other systems on the network and not only the packets send or received from your network adapter. Promiscuous mode is enabled by default.



The red box button "STOP" on the top left side of the window can be clicked to stop the capturing of traffic on the network.

Analyse the Capture Data

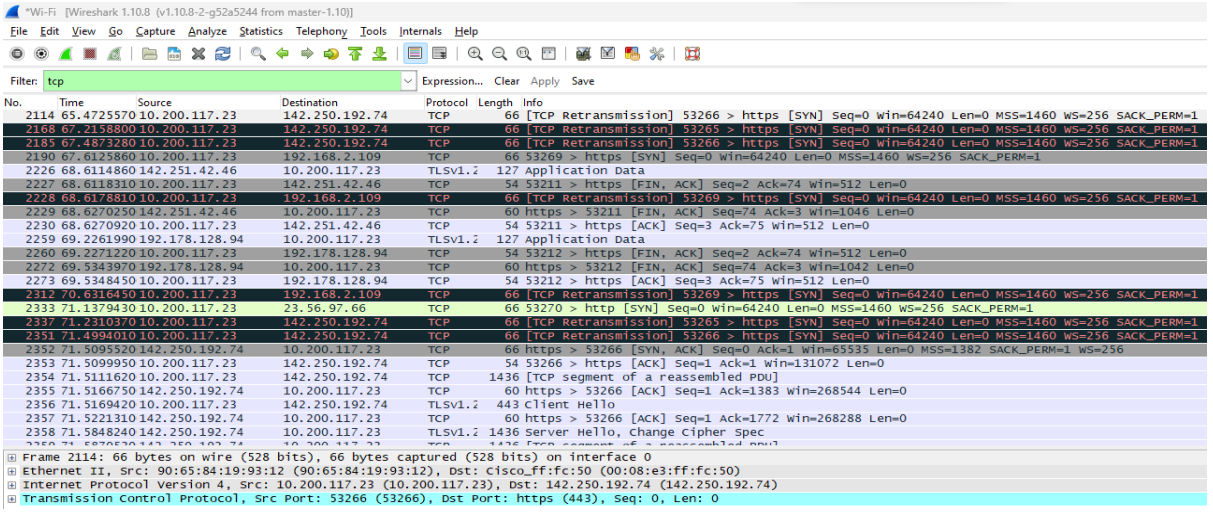
First of all, click on a packet and select it. Now, you can scroll down to view all its details.



To Analyse the captured packets different filters commands are used:

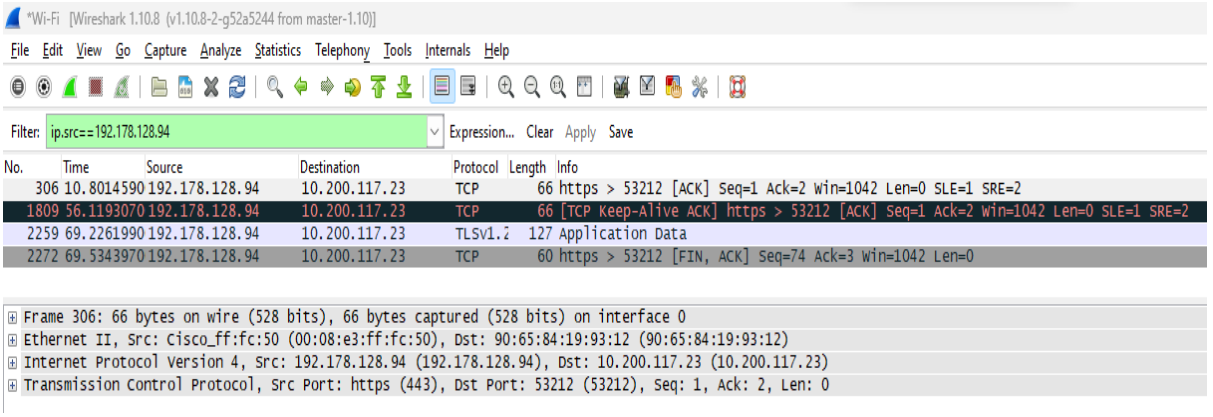
1.Display packets which are using TCP protocol

tcp



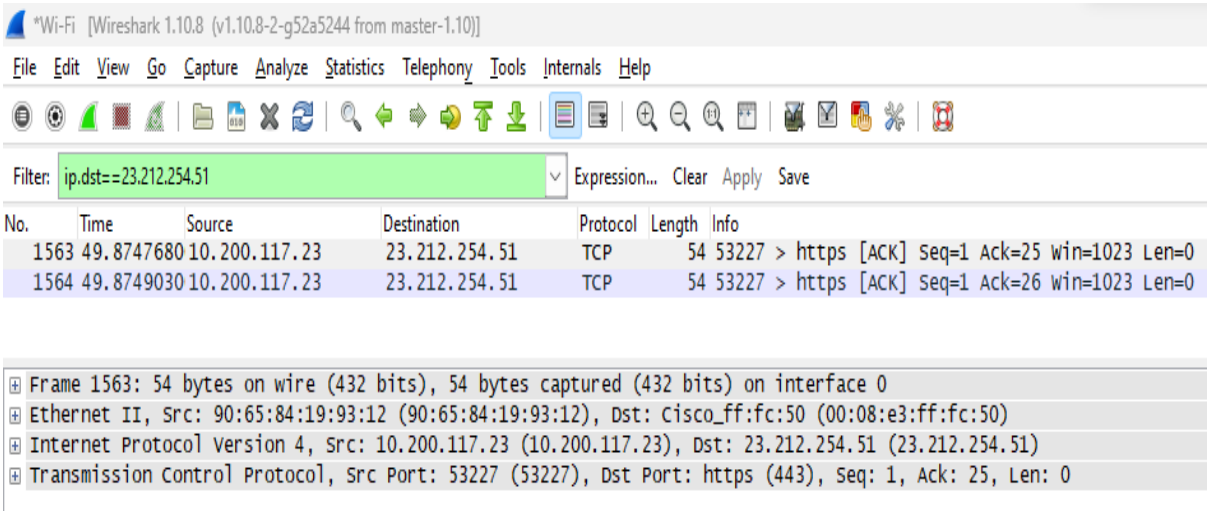
2.Display packets which are coming from specific IP-address

ip.src == 192.178.128.94



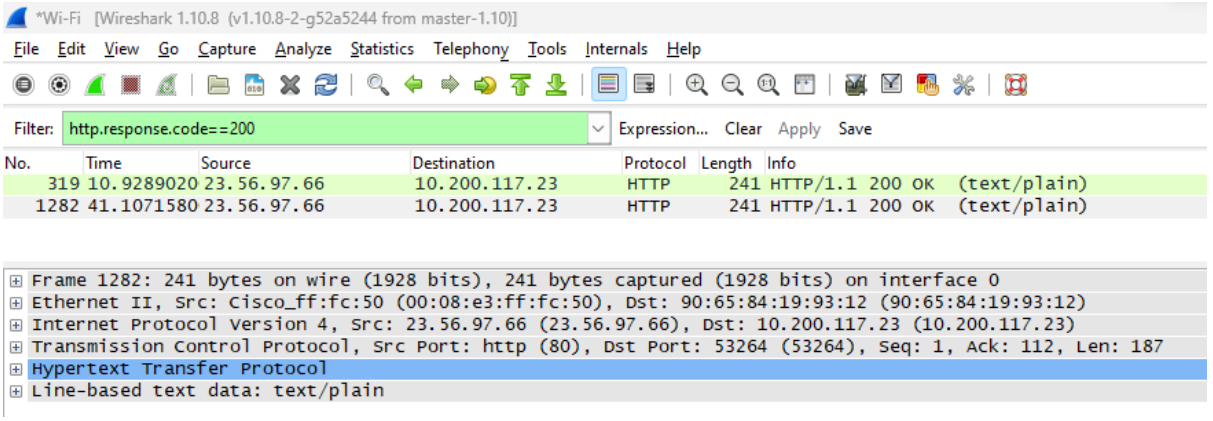
3.Display packets which are having specific IP-address destination

ip.dst == 23.212.254.51



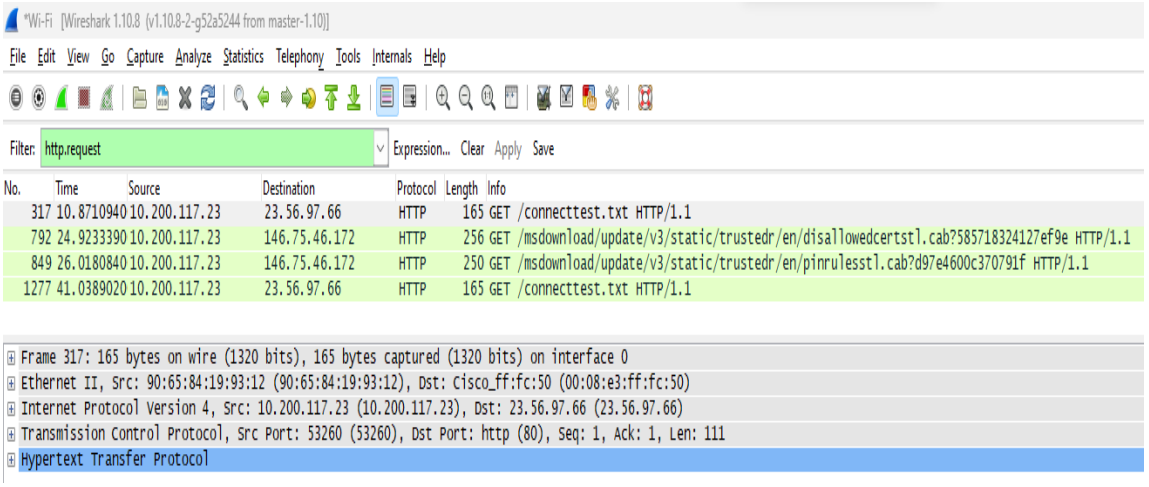
4.Display packets having no error connecting to server □

http.response.code==200



5.Display packets which are using http request

http.request



C. Perform Network Forensic Analysis tool using NetworkMiner.

Theory:

Network Miner is an open source Network Forensic Analysis Tool (NFAT) for Windows (but also works in Linux / Mac OS X / FreeBSD). Network Miner can be used as a passive network sniffer/packet capturing tool in order to detect operating systems, sessions, hostnames, open ports etc. without putting any traffic on the network. Network Miner can also parse PCAP files for off-line analysis and to regenerate/reassemble transmitted files and certificates from PCAP files.

Network Miner makes it easy to perform advanced Network Traffic Analysis (NTA) by providing extracted artifacts in an intuitive user interface. The way data is presented not only makes the analysis simpler, it also saves valuable time for the analyst or forensic investigator.

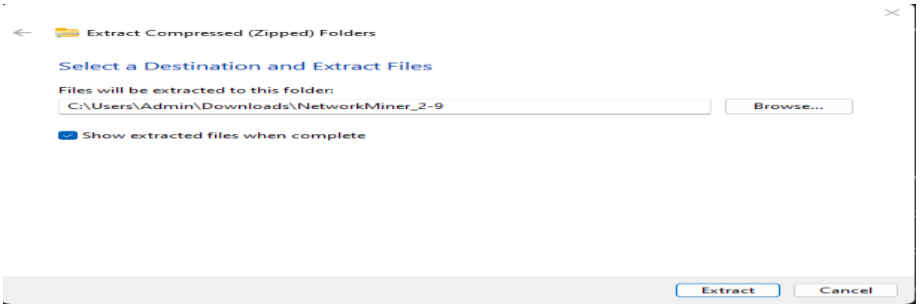
Step 1: Download Network miner from https://www.netresec.com/?page=NetworkMiner

JSON-LD		✓
Configurable file output directory		✓
Configurable time zone (UTC, local or custom)		✓
Geo IP localization (***)		✓
DNS Whitelisting (****)		✓
Advanced OS fingerprinting		✓
Web browser tracing (video tutorial)		✓
Online ad and tracker detection		✓
Host coloring support		✓
Command line scripting support		✓ NetworkMinerCLI
Price	Free	$ 1300 USD
	Download NetworkMiner (free edition)	Buy NetworkMiner Professional

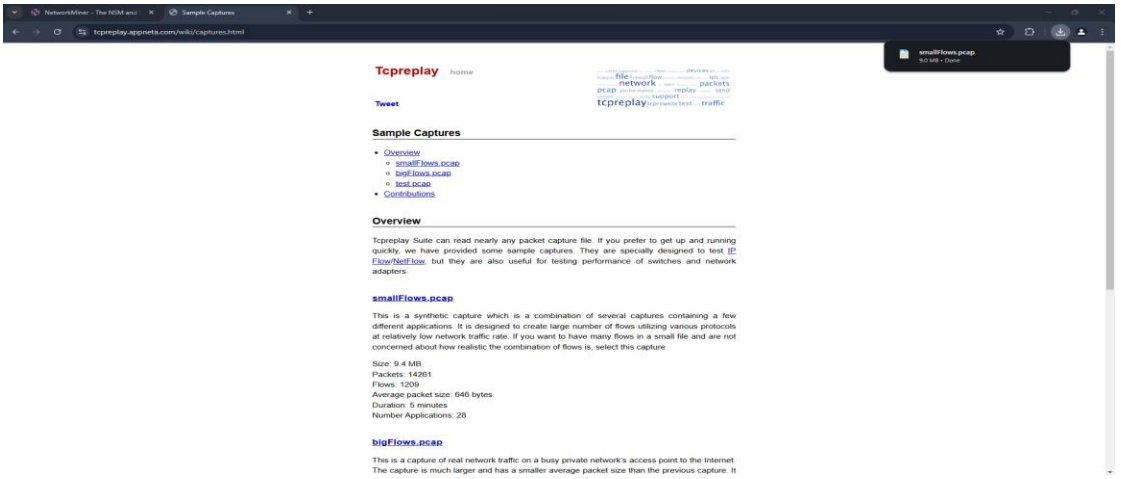
** Fingerprinting of Operating Systems (OS) is performed by using databases from Satori and p0f*
*** Identified protocols include: DNS, FTP, HTTP, HTTP2, IRC, Meterpreter, NetBIOS NameService, NetBios SessionService, Socks, Spotify's Server Protocol, SSH, SSL, TDS (MS-SQL) and TPKT*
**** This product includes GeoLite data created by MaxMind, available from maxmind.com*
***** Domain names in the DNS tab are checked against the Alexa top 1,000,000 sites*

Step 2: Extract the file from zip file contents in download folder. Open C drive- Program Files and Create a new folder- networkminer2. Copy all folder contents in this folder.

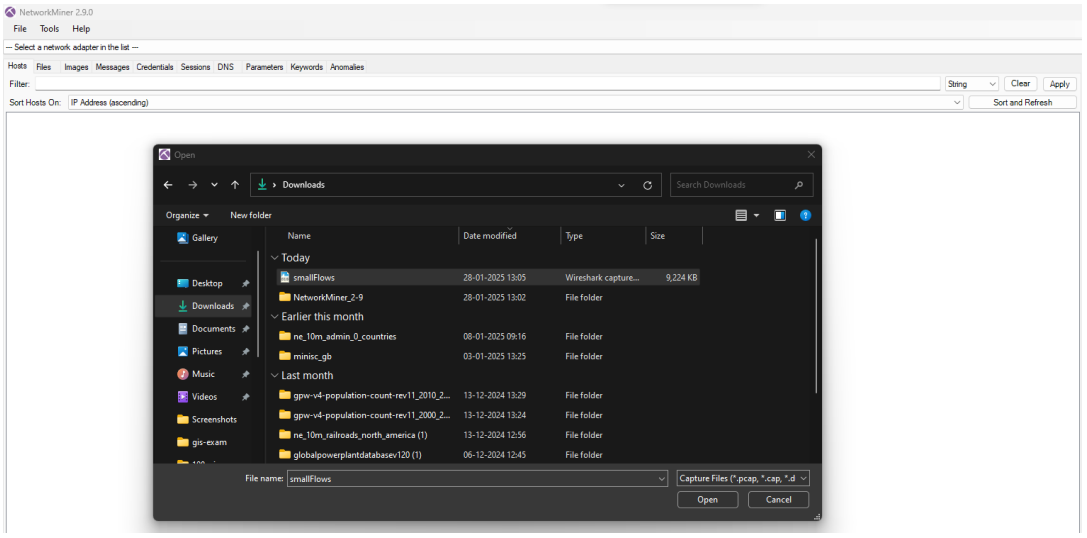
Step 3: Run the Application.exe file from the folder to Open Network Miner.



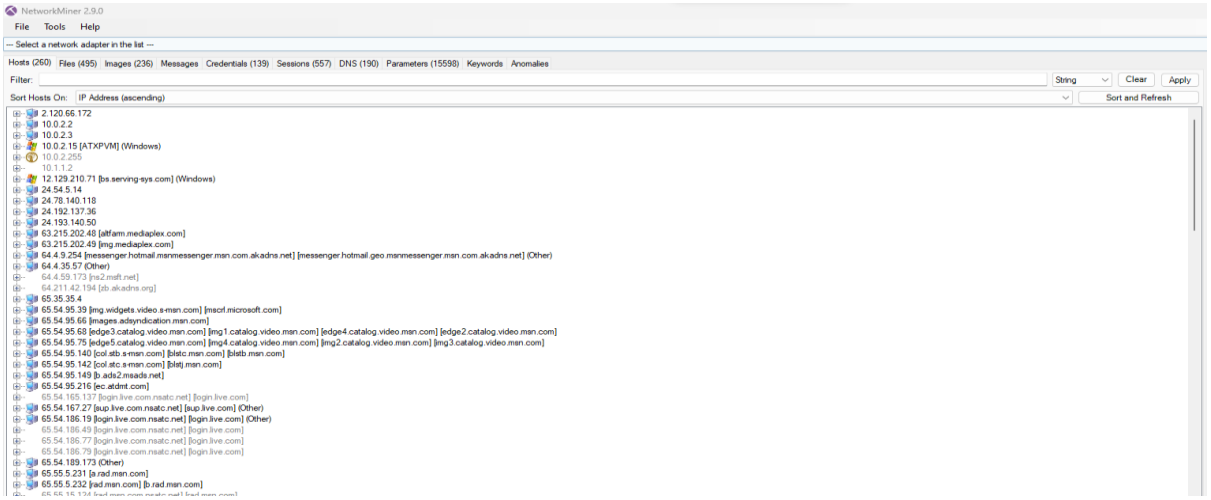
Step 4: Download pcap file from the URL mentioned in the screenshot below https://tcpreplay.appneta.com/wiki/captures.html



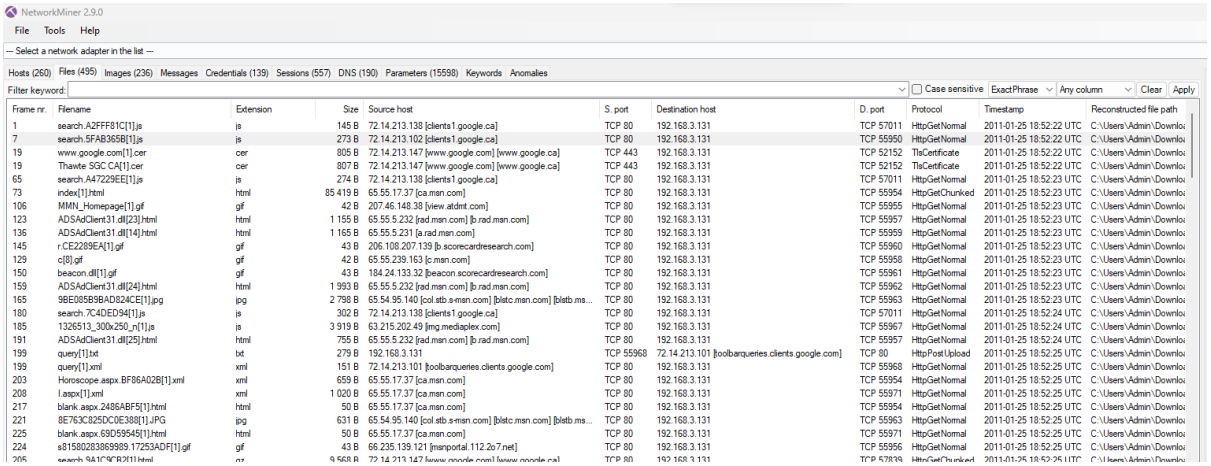
Step 5: Open this pcap file in Network Miner. Network Miner-> File-> Open-> Select pcap file.



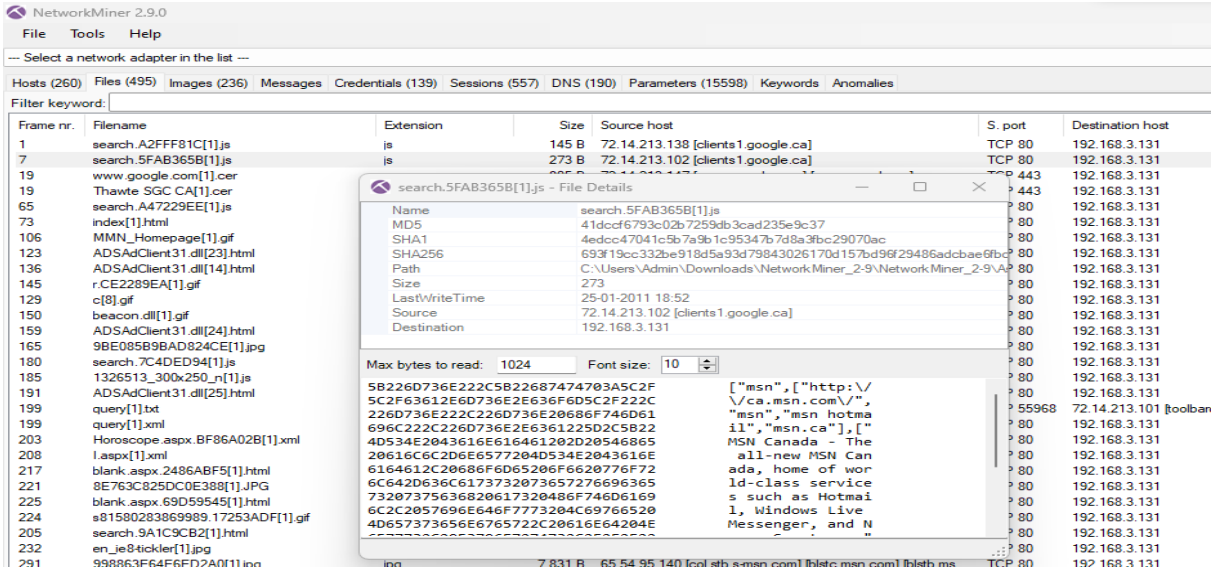
Step 6: In the hosts tab, you can see all the host that were engaged while recording the pcap files. These pcap files could be from a recorded session of Wireshark.



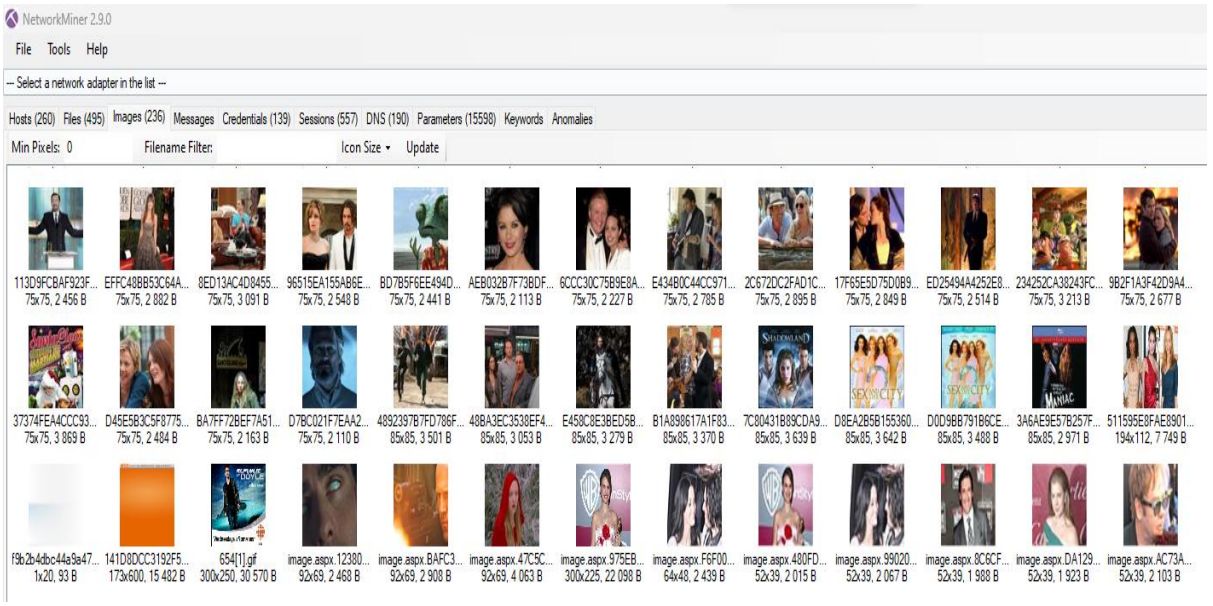
Step 7: Open files tab to view all the files that were recorded during the pcap session.



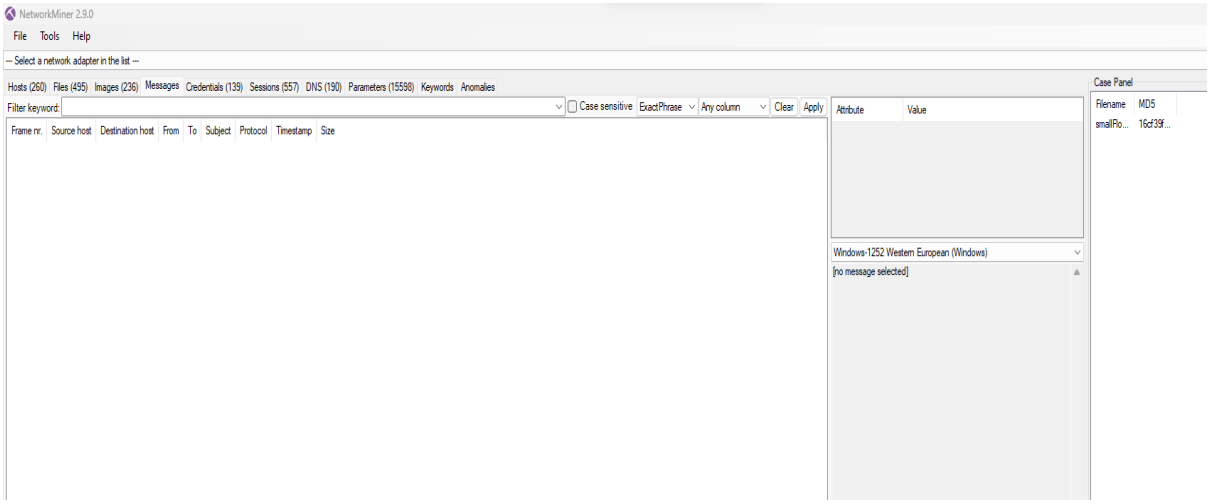
Step 8: Right click select file details



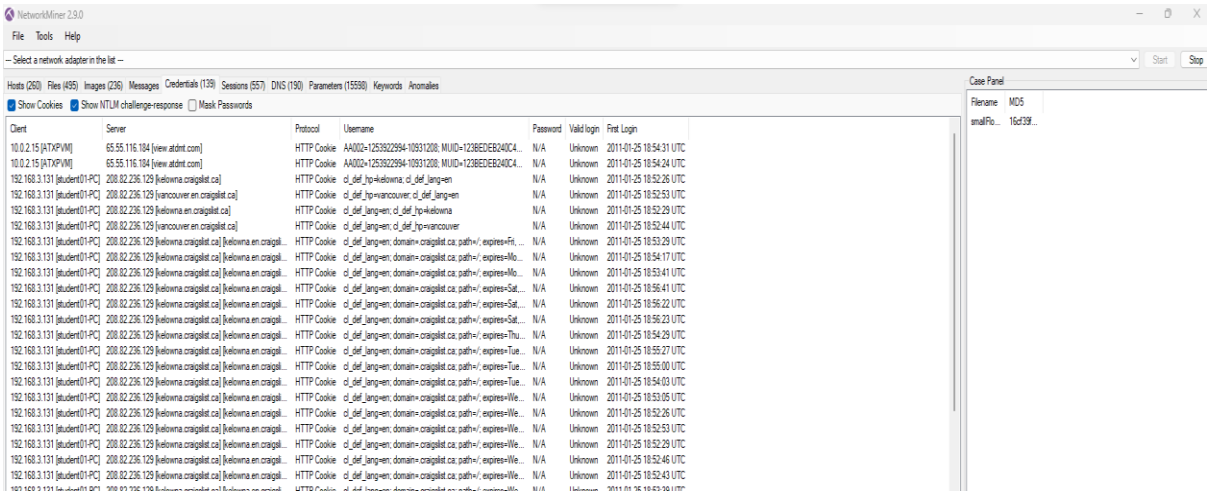
Step 9: You can view all image below



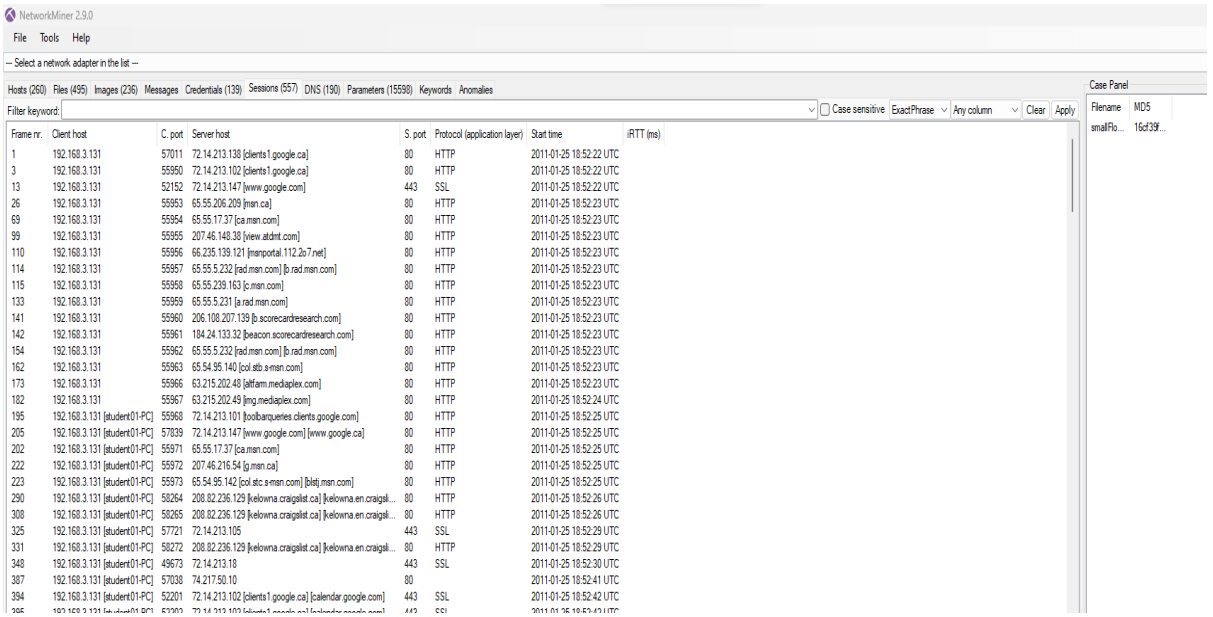
Step 10: You can view all messages below



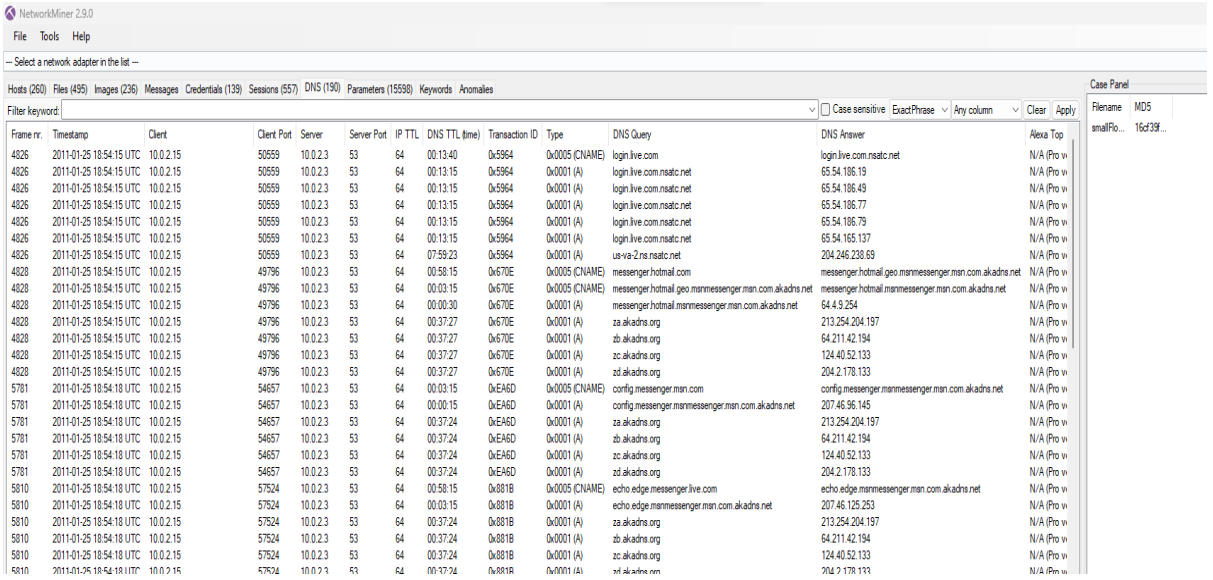
Step 11: You can view all credentials below



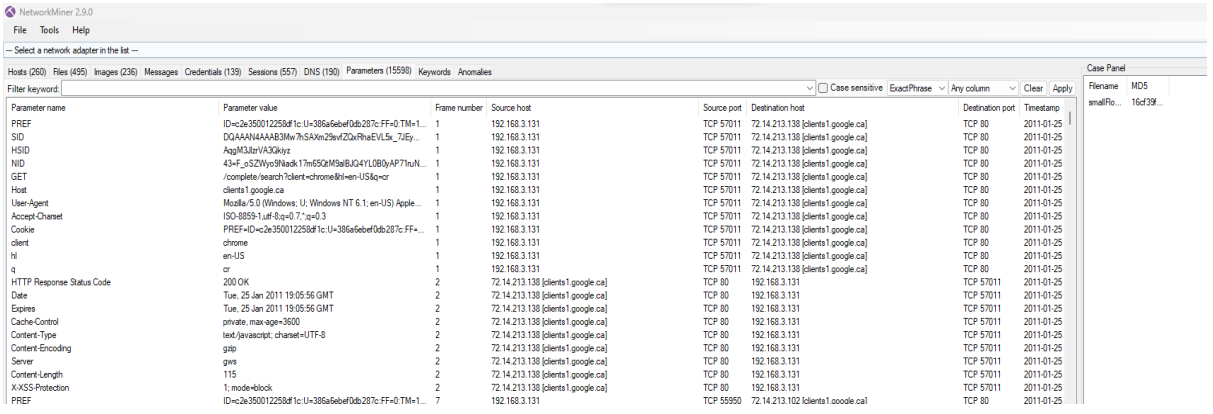
Step 12: You can view all sessions below



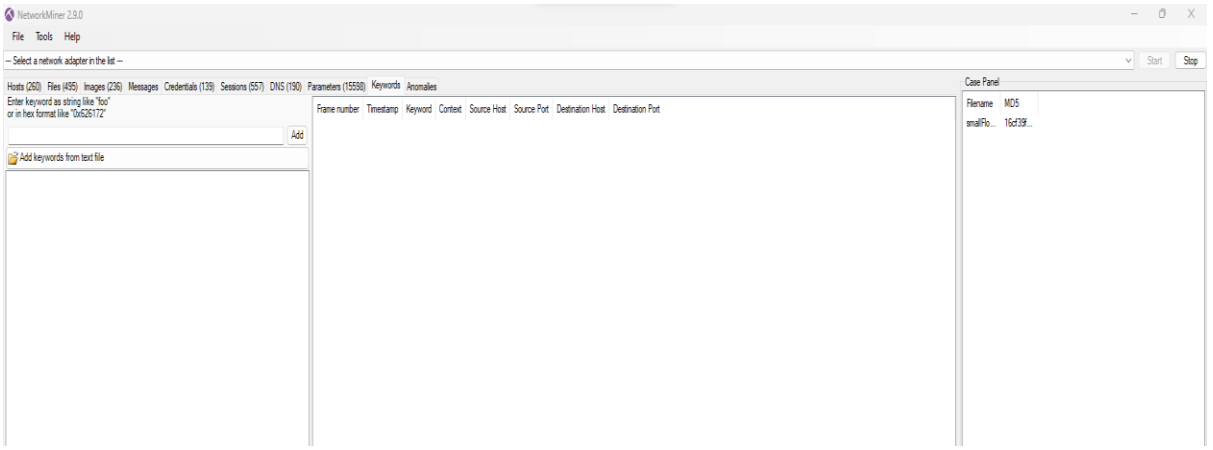
Step 13: You can view all DNS below



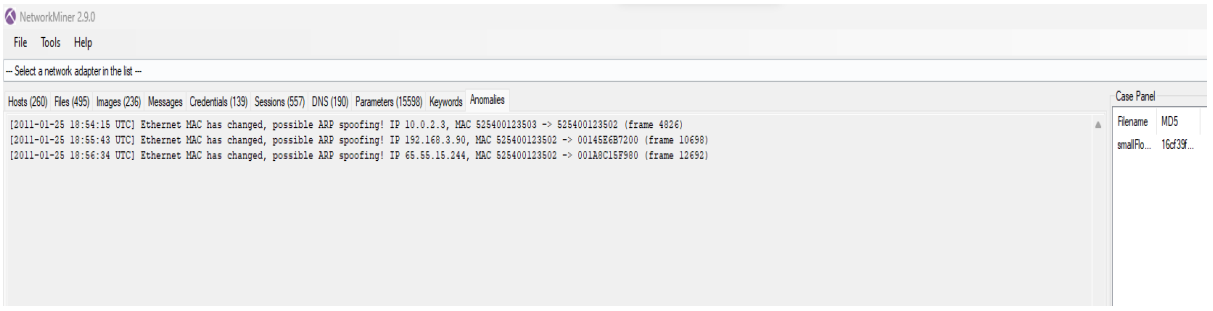
Step 14: You can view all parameters below



Step 15: You can view all keywords below



Step 16: You can view any anomalies below



Practical: 6

Aim: A) Dump Memory contents using PMdump

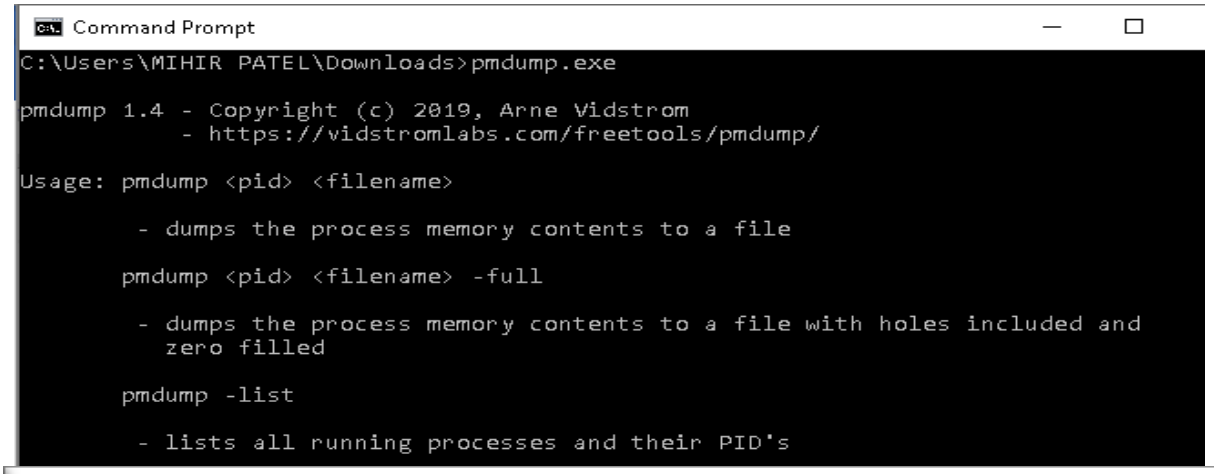
Theory

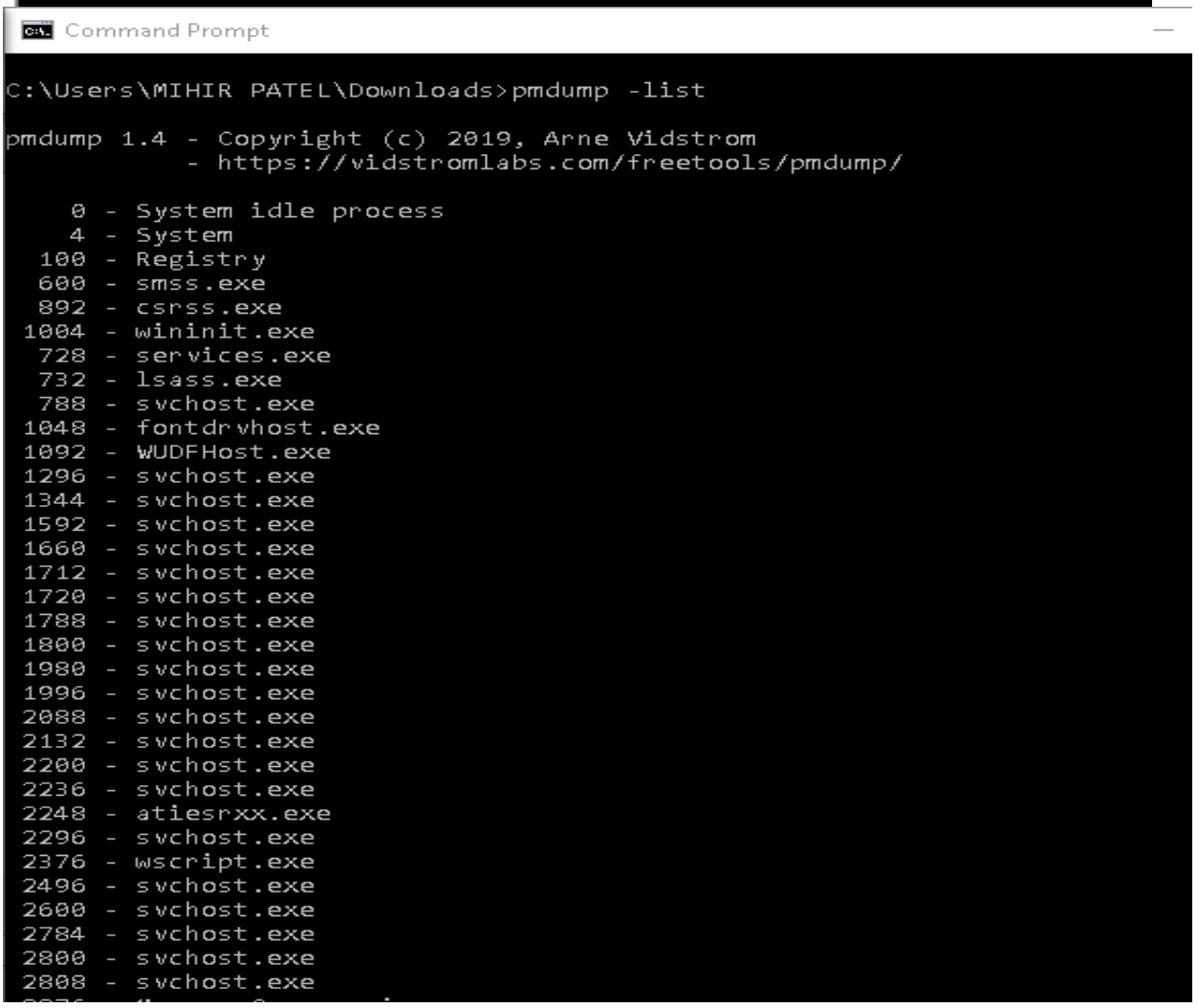
A large number of applications can fall prey to this security vulnerability and get their user's passwords hacked - web browsers, email clients, instant messengers, etc. fall in this category. The main idea behind the hack is that while the application is running, we should be able to dump its entire memory to file, without having to stop or tamper with the application in any way. Pmdump makes this possible very easily by allowing us to select the running applicationwhose memory we want to dump. Download a copy of the Pmdump programs and Strings program beforehand. Also, we shall use the demo application MemPass.exe to show the vulnerability. The application is a very simple piece of code which takes the user input, clearsthe screen, and pauses its execution. We will first run MemPass.exe, input a password, then switch to Pmdump and dump the process memory into a file. Finally, we will use the strings program to retrieve the password from this file.

STEP 1: Run mempass.exe, it asks for a password, We have to enter the password and pressEnter

After Pressing Enter, mempass clears the screen and pauses there as seen in the below screen

Step 2: Open a new terminal and Run pmdump.exe program.





Step 3: Pmdump allows us to list all the programs which are currently Running using thecommand pmdump -list, as shown in Below snapshot, mempass has PID- 8808

Step 4: Now Run pmdump command and give thePID of mempass i.e 8808 as input and giveFilename i.e pass.txt in which it can dump the entire memory of mempass program

```
C:\Users\MIHIR PATEL\Downloads>pmdump 8808 pass.txt

pmdump 1.4 - Copyright (c) 2019, Arne Vidstrom
           - https://vidstromlabs.com/freetools/pmdump/
```

Step 5: pass.txt file gets created and it has some Garbled Characters.

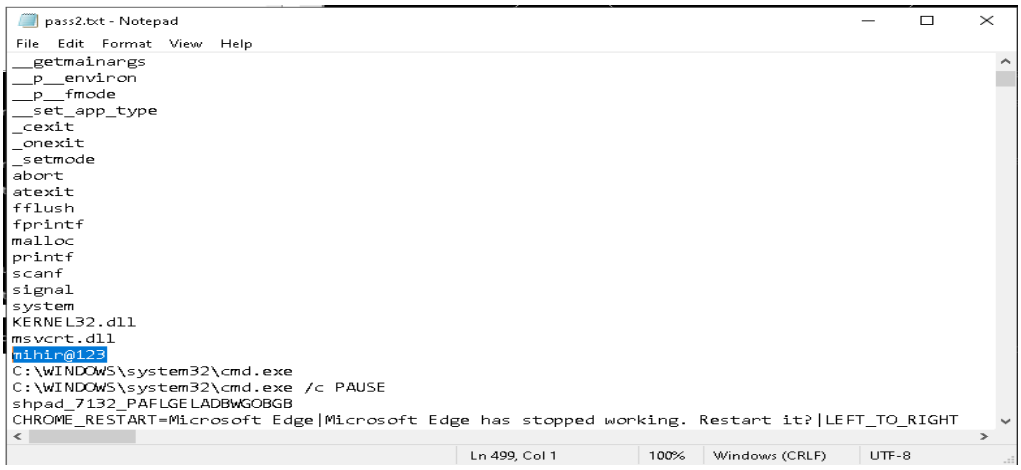
Step 6: Now we Run the Strings Program

```
C:\Users\MIHIR PATEL\Downloads>strings.exe

Strings v2.53 - Search for ANSI and Unicode strings in binary images.
Copyright (C) 1999-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

usage: strings.exe [-a] [-f offset] [-b bytes] [-n length] [-o] [-s] [-u] <file or
directory>
-a      Ascii-only search (Unicode and Ascii is default)
-b      Bytes of file to scan
-f      File offset at which to start scanning.
-o      Print offset in file string was located
-n      Minimum string length (default is 3)
-s      Recurse subdirectories
-u      Unicode-only search (Unicode and Ascii is default)
-nobanner
        Do not display the startup banner and copyright message.
```

```
C:\Users\MIHIR PATEL\Downloads>strings.exe -a -n 5 -nobanner pass.txt > pass2.txt
```

Here we need to give -a for ASCII only and then it also asks for minimum string length forwhich we give-n 5 and -nobanner for quiet,then we give the input file pass.txt and output file as pass2.txt

Step 7: All the Strings are Printed in pass2.txt which also includes our Password in unencryptedFormat



Practical: 7

Aim: Using Data Acquisition Tools [ProDiscover]

Theory

ProDiscover Forensics is a comprehensive digital forensics software that empowers investigators to capture key evidence from computer systems. ProDiscover has capabilities to handle all aspects of an in- depth forensic investigation to collect, preserve, filter, and analyse evidence.

Data Acquisition Tools:

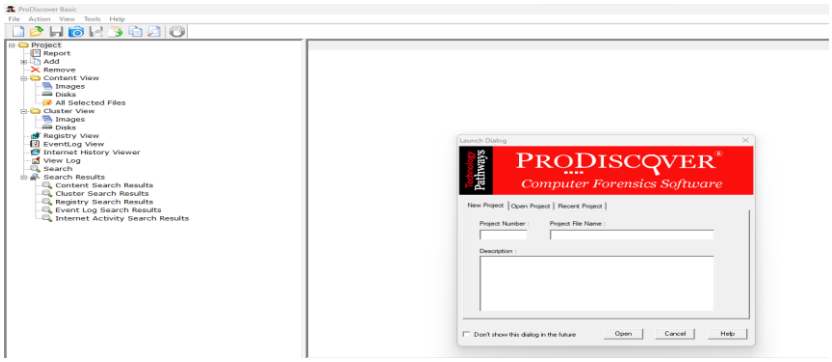
USB WRITE BLOCKER + FTK Imager

•USB Write Blocker enables you to activate or deactivate the write protection for

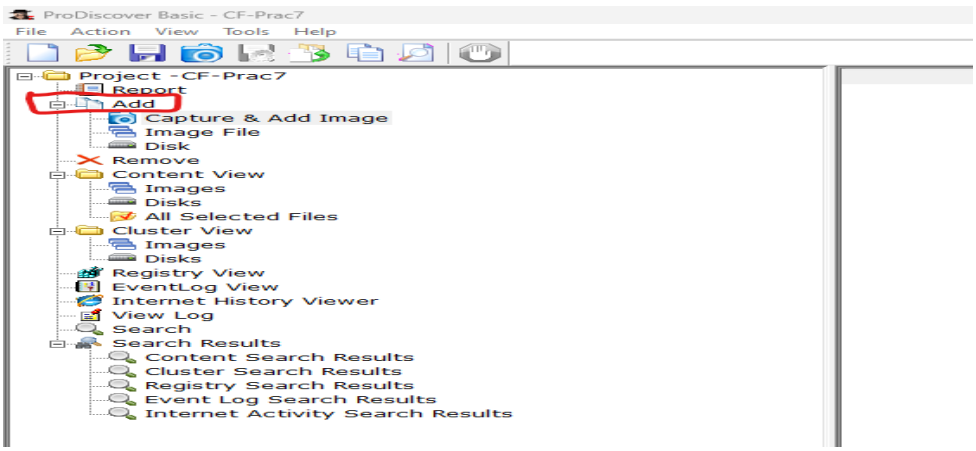
your USB portable devices with just a few clicks. With USB Write Blocker, you will beable to restrict the access of others to your important documents and prevent unwanted, accidental modifications that might cause data loss.

•Forensic Toolkit, or FTK, is a computer forensics software made by Access Data. Itscans a hard drive looking for various information.

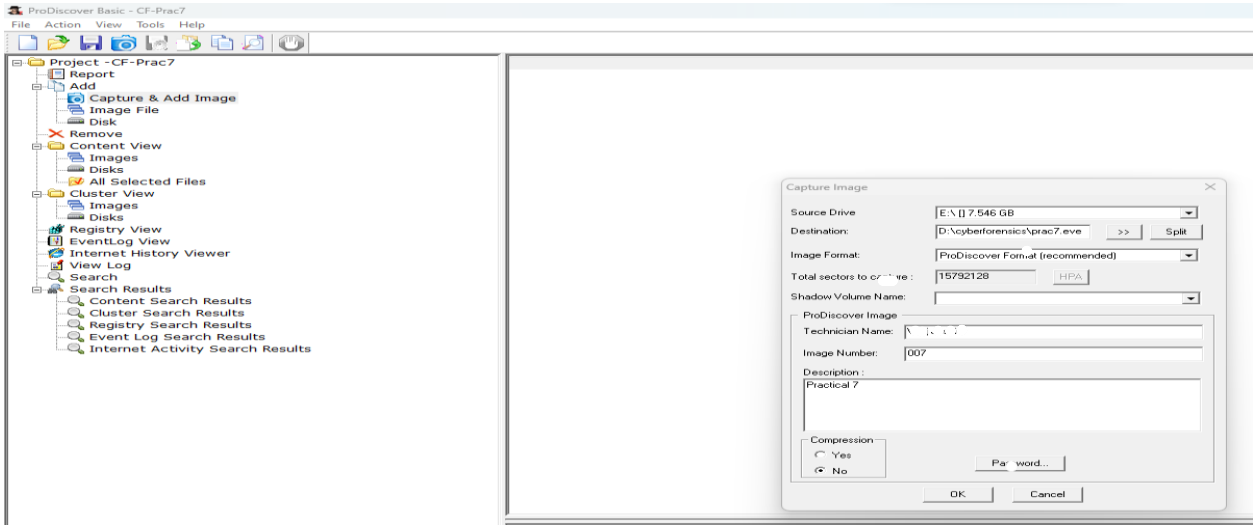
Step 1: Open ProDiscover Basic and start with new project.



Step 2: The new created project appears on the left side – Go on add and select Capture andAdd Image

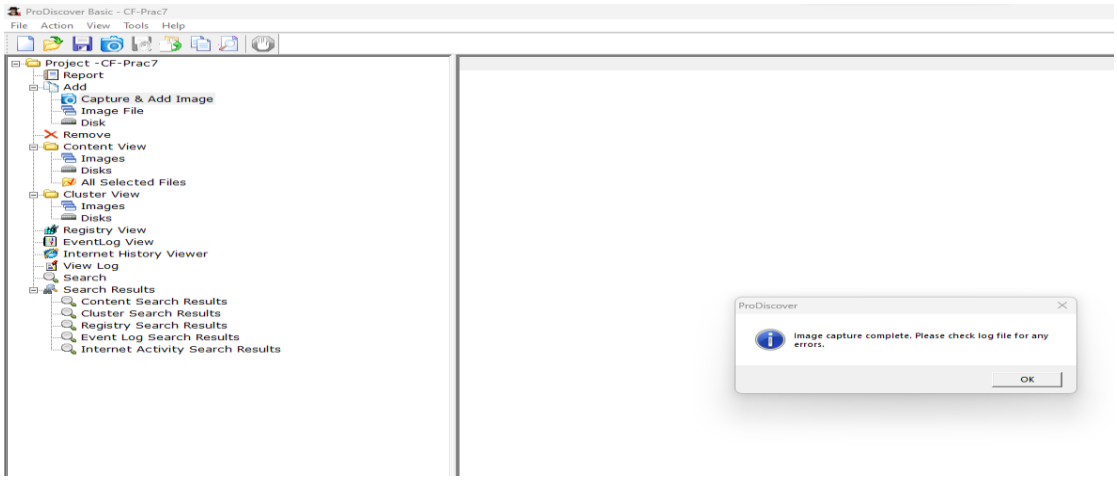


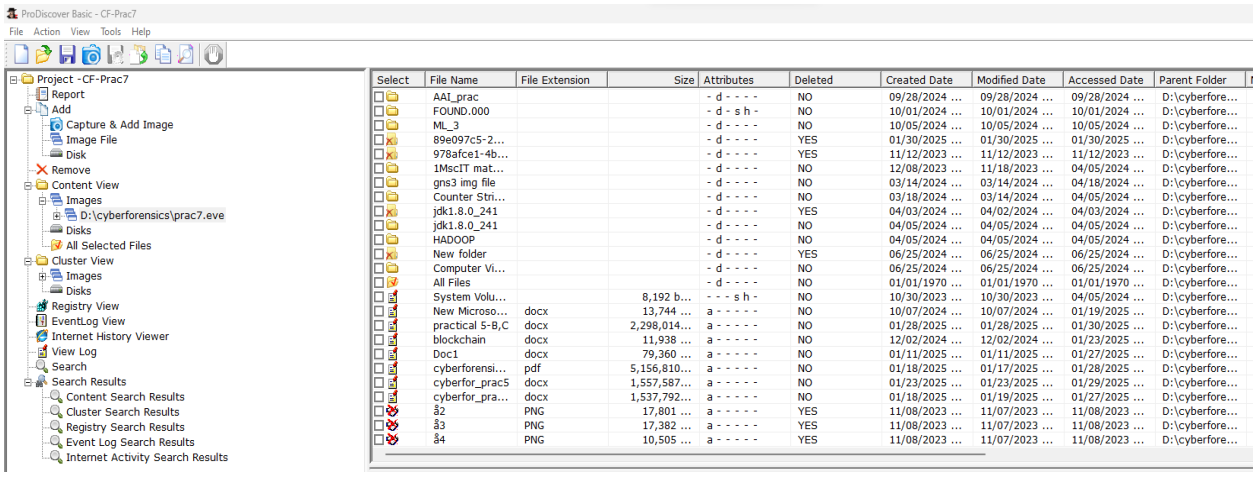
Step 3: Select your Source Drive file from the drop down, select Destination path and add Technician Name, Image Number and Description. Click on ok



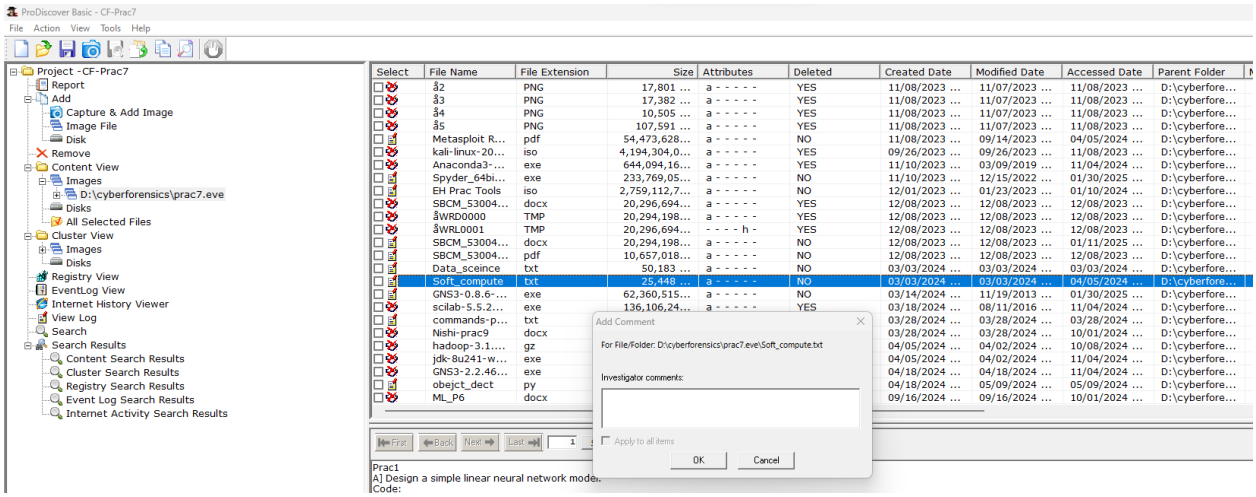
Step 4: The image capturing will start processing.

Step 5: The image has been captured. Click on Ok

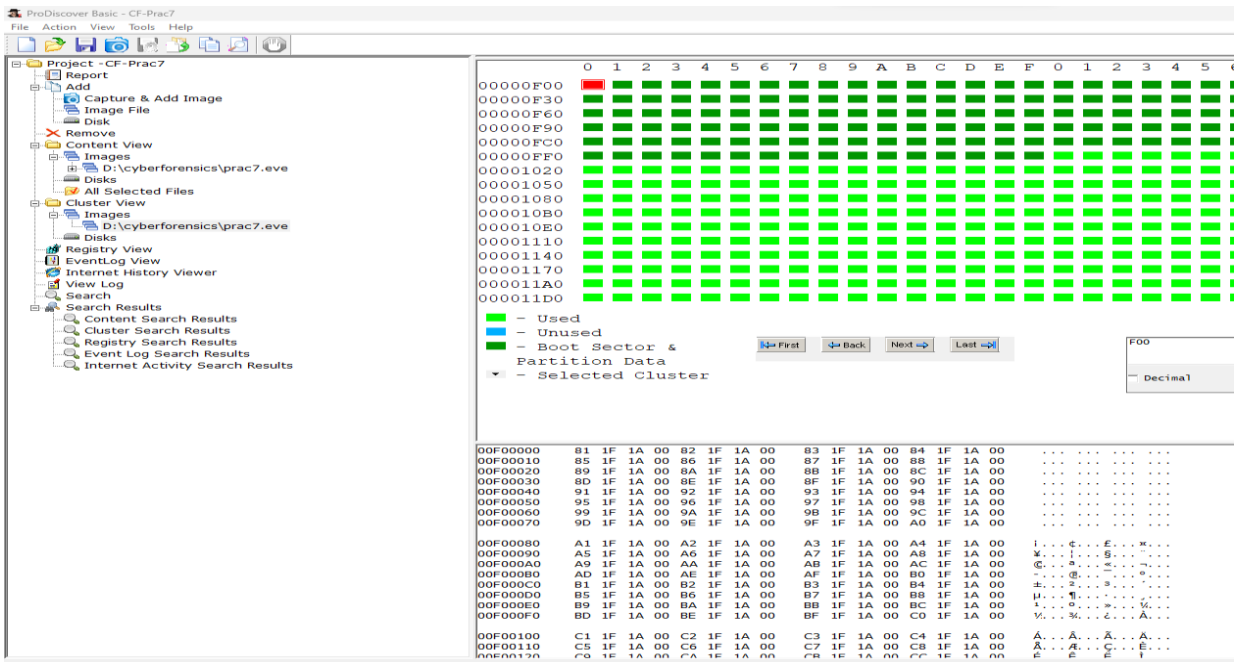




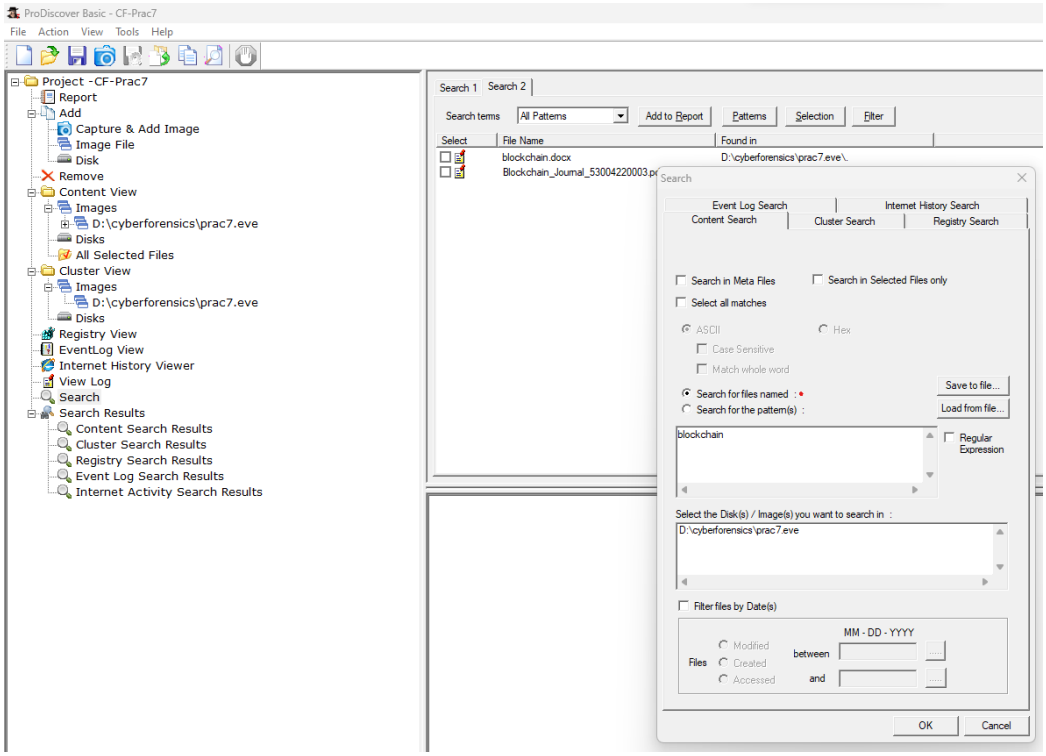
Step 7: Click on any of the file and type a comment.



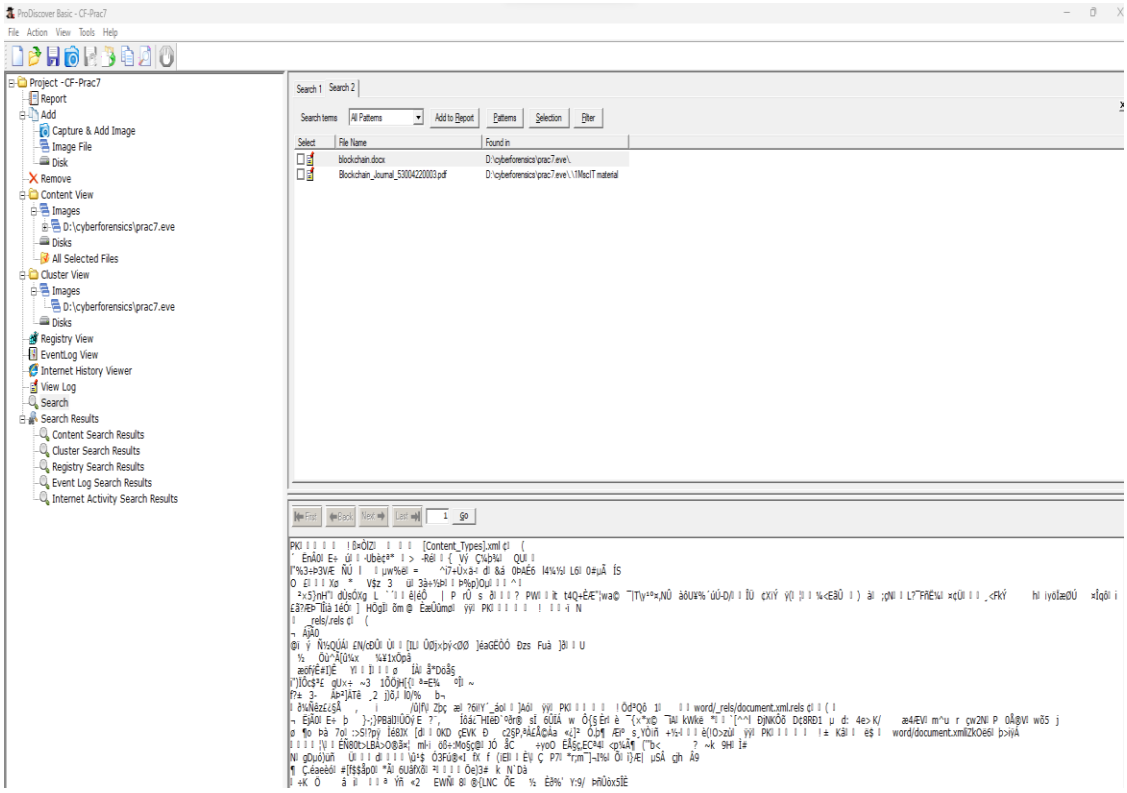
Step 8: To see the cluster view, click on cluster view tab on the left side panel.



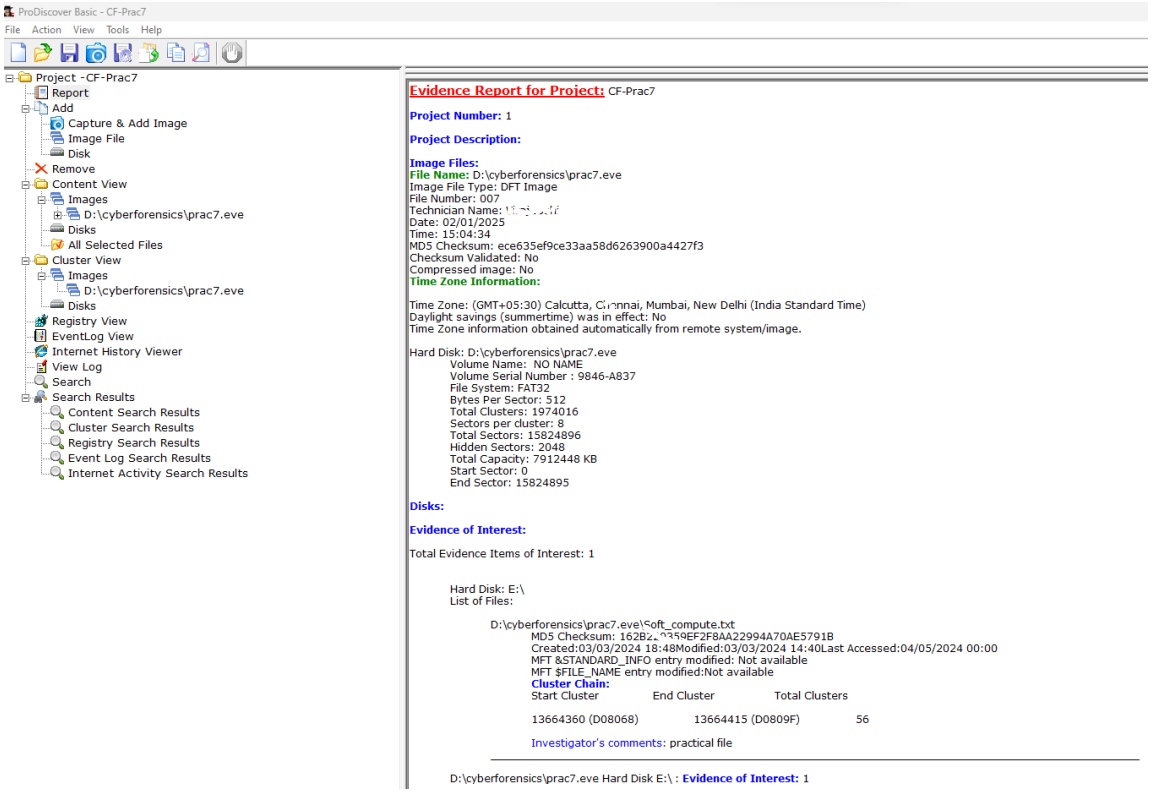
Step 9: For Keyword Search, Click on the Search option on left side of panel and Enter the filename to be searched in the image created.

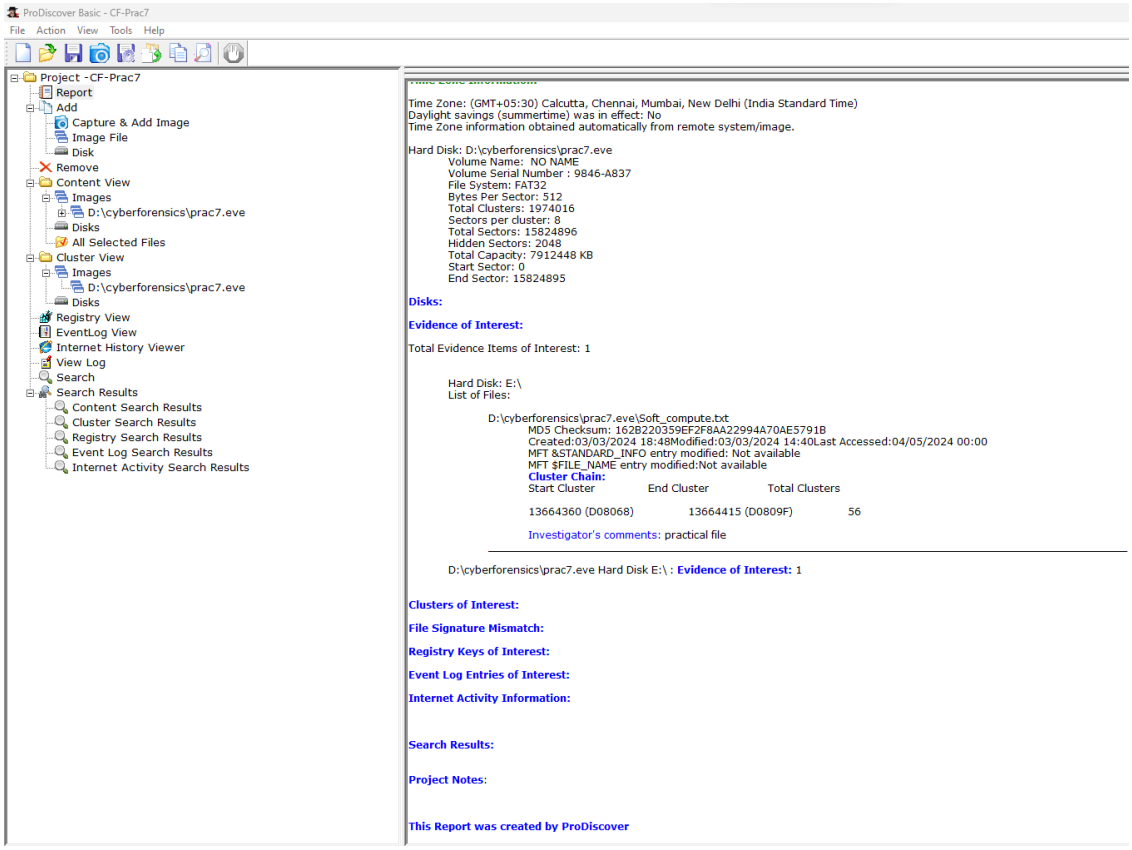


Step 10: The following is the Output of the keyword search.



Step 11: Click on View – Report This will show entire gist of report done in the project.





Practical: 8

Aim: Using Steganography tool (S-Tool)

Theory

Steganography is one of the oldest technique used to hide data in a image, hide image into imageand hide data in a video/audio etc.You can easily hide any kind of video/audio/text/message/image into each other.

Best Tools to Perform Steganography:

There are many software available that offer steganography. Some offer normal steganography but a few offer encryption before hiding the data. These are the steganography tools which are available for free:

•Stegosuite is a free steganography tool which is written in Java. With Stegosuite you can easily hide confidential information in image files.

•Steg hide is an open source Steganography software that lets you hide a secret file in image or audio file.

•Xiao Steganography is a free software that can be used to hide data in BMP images or inWAV files.

•SSuit Picsel is another free portable application to hide text inside an image file but ittakes a different approach when compared to other tools.

•OpenPuff is a professional steganographic tool where you can store files in image,audio, video or flash files

Install the latest version of this tool Lauch stegosuite using below command

In order to encrypt an image file with a confidential file, first, you need to load the image file through the File menu.

Select a file in BMP, GIF, JPG or PNG format from the file browser and then click the OK button. The image file will be loaded in the main Stegosuite window.

You can do the following three tasks through this window:

●Enter a secret message along with the file(s) you want to embed.

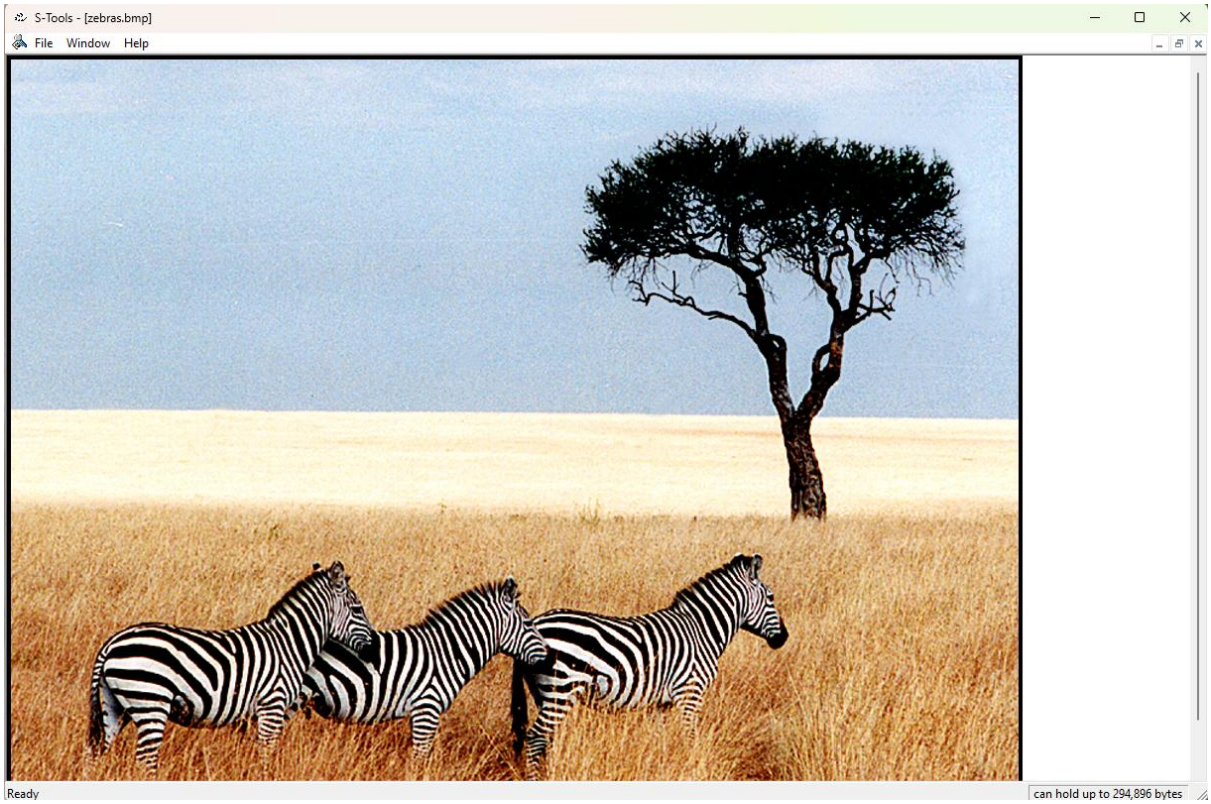
●Right-click and then add a confidential file in the “embedded files” area.

●Enter a password that will be used while extracting the embedded files and a secret message, later from the image.

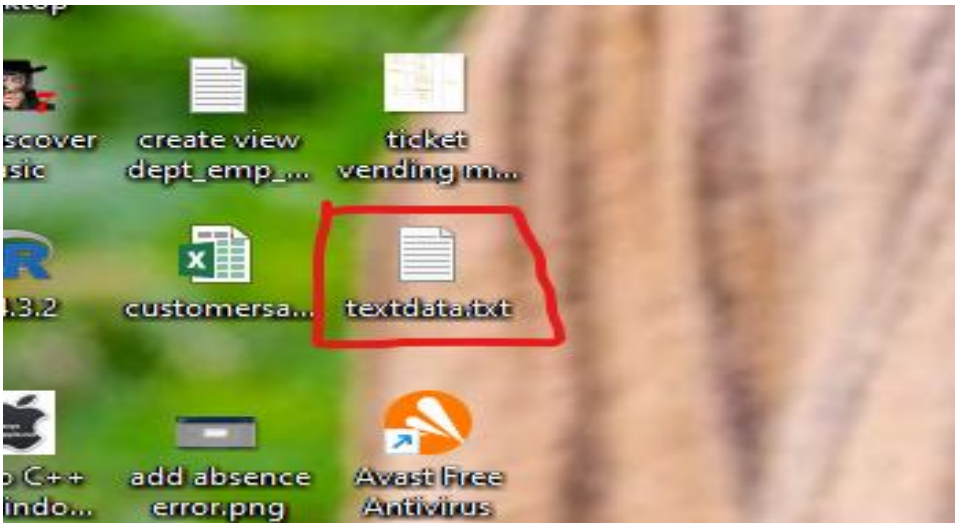
In order to extract the original confidential file from the image file it was embedded into, you can right- click the image file from the file browser and select “Open With Other Application from the menu and then select Stegosuite from the Select Application list as follows:

Or you can open the Stegosuite application and load an embedded image file from the File menu. Once the file is loaded, simply provide the password and click the Extract button after which, the original confidential file will be extracted back to your system.

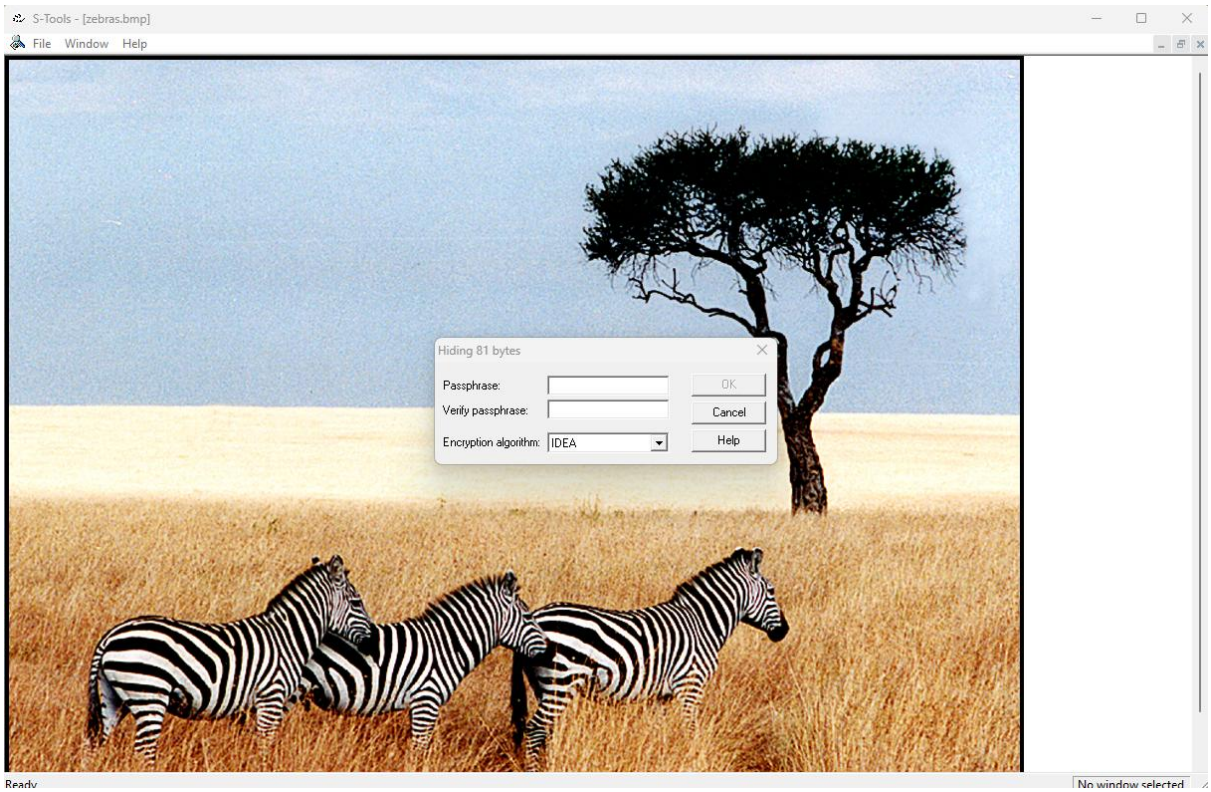
Step 1: Download S-tool using giving link https://www.cs.vu.nl/~ast/books/mos2/zebras.html-> then drag and drop the Zebra.bmp image



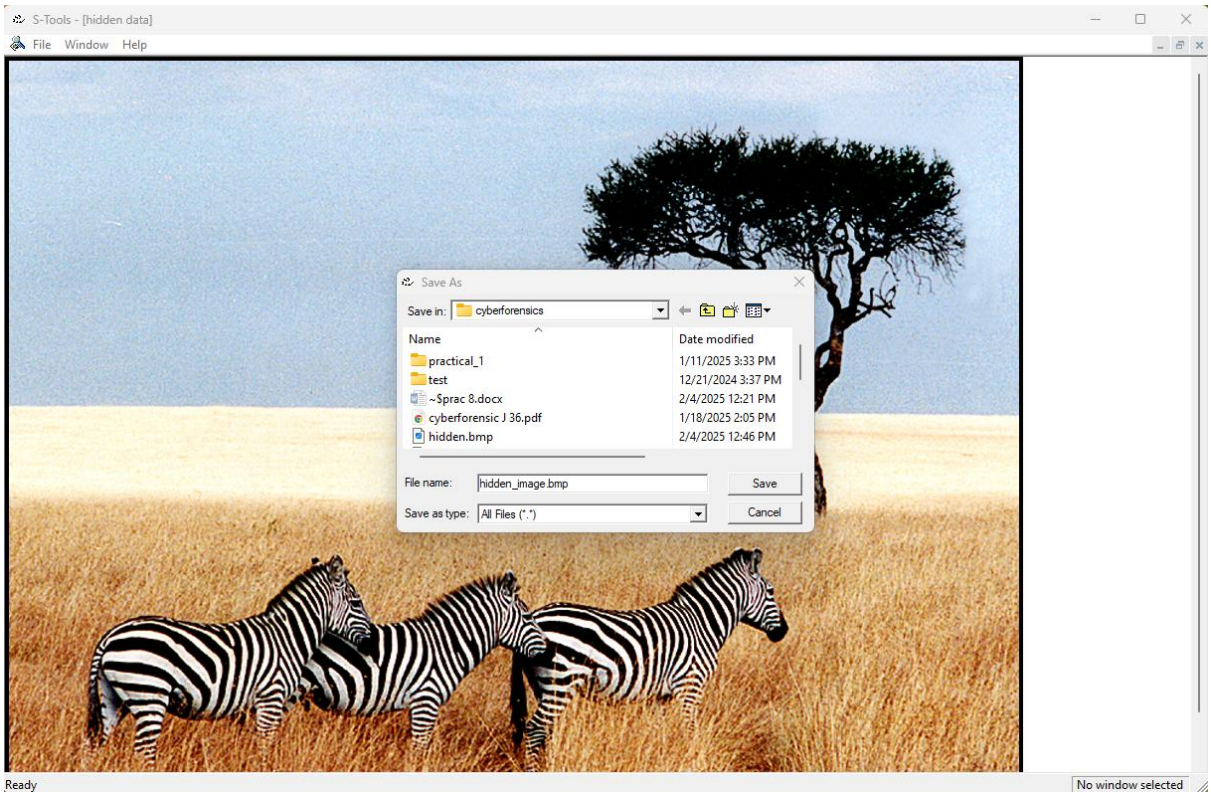
Step 2: Create a new text document-> Type anything inside it and save it



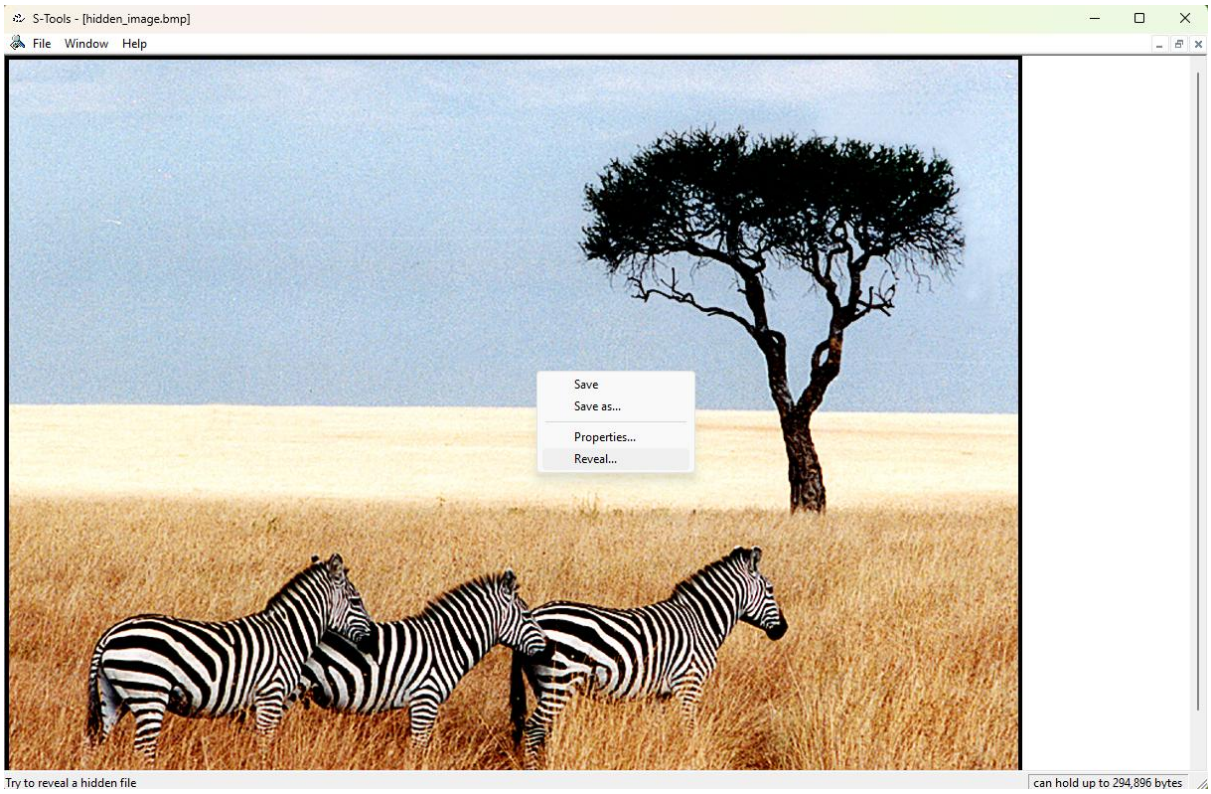
Step 3: Now drag and drop the text file on the image-> enter the password



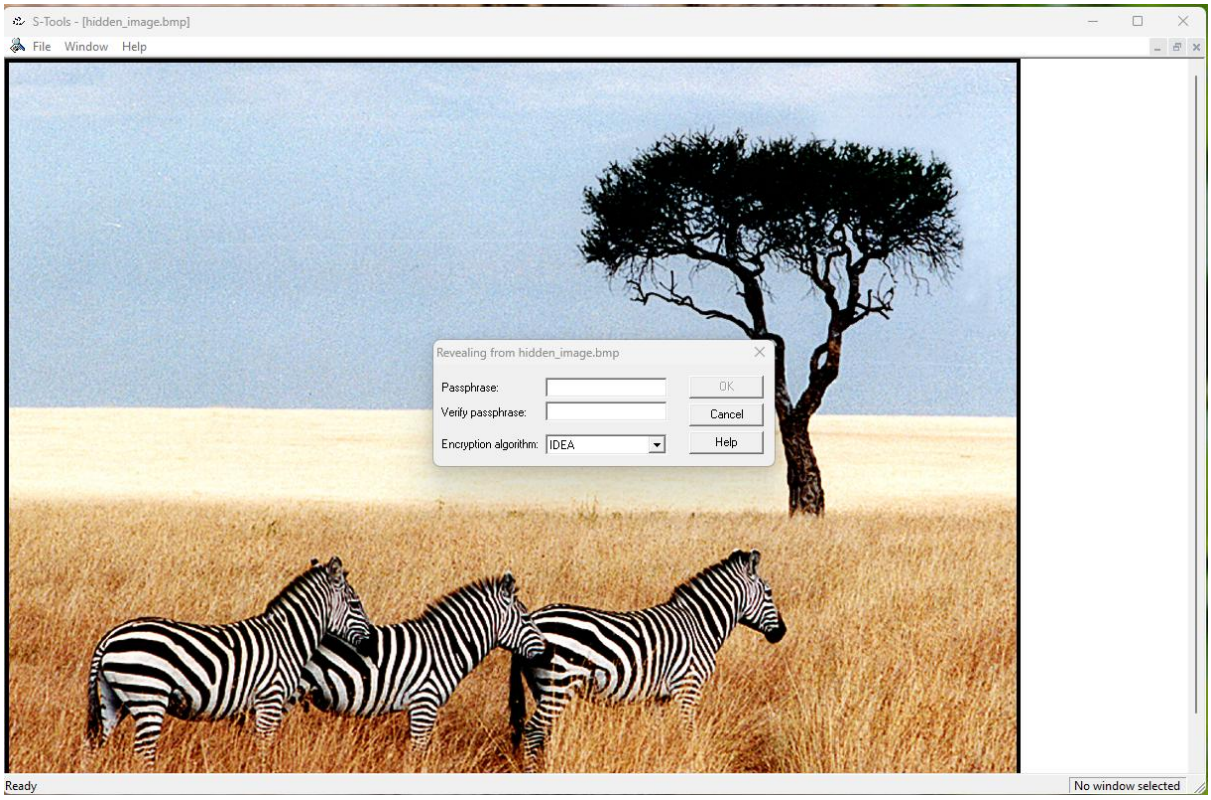
Step 4: Now save the file

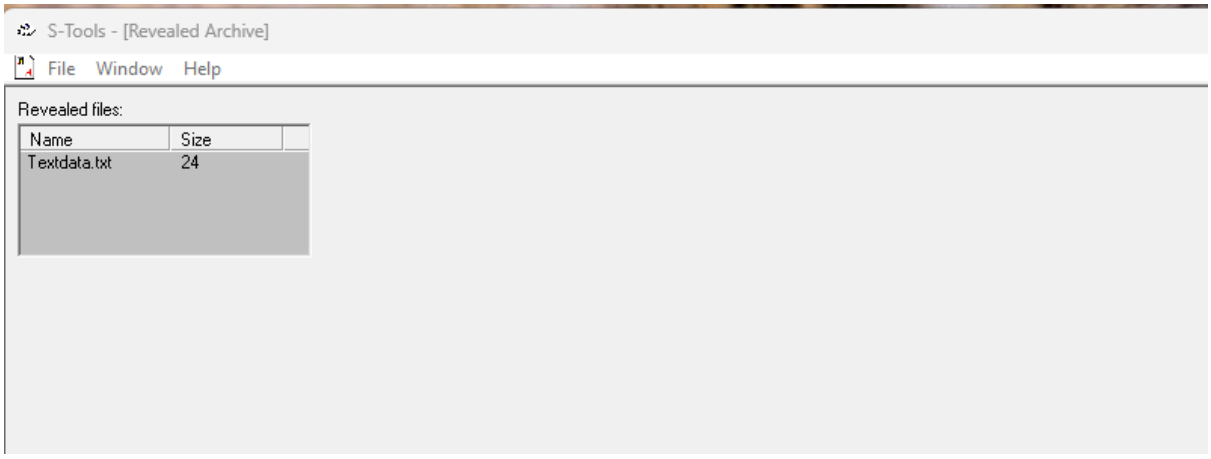


Step 5: Open saved image -> right click on it-> Revel…

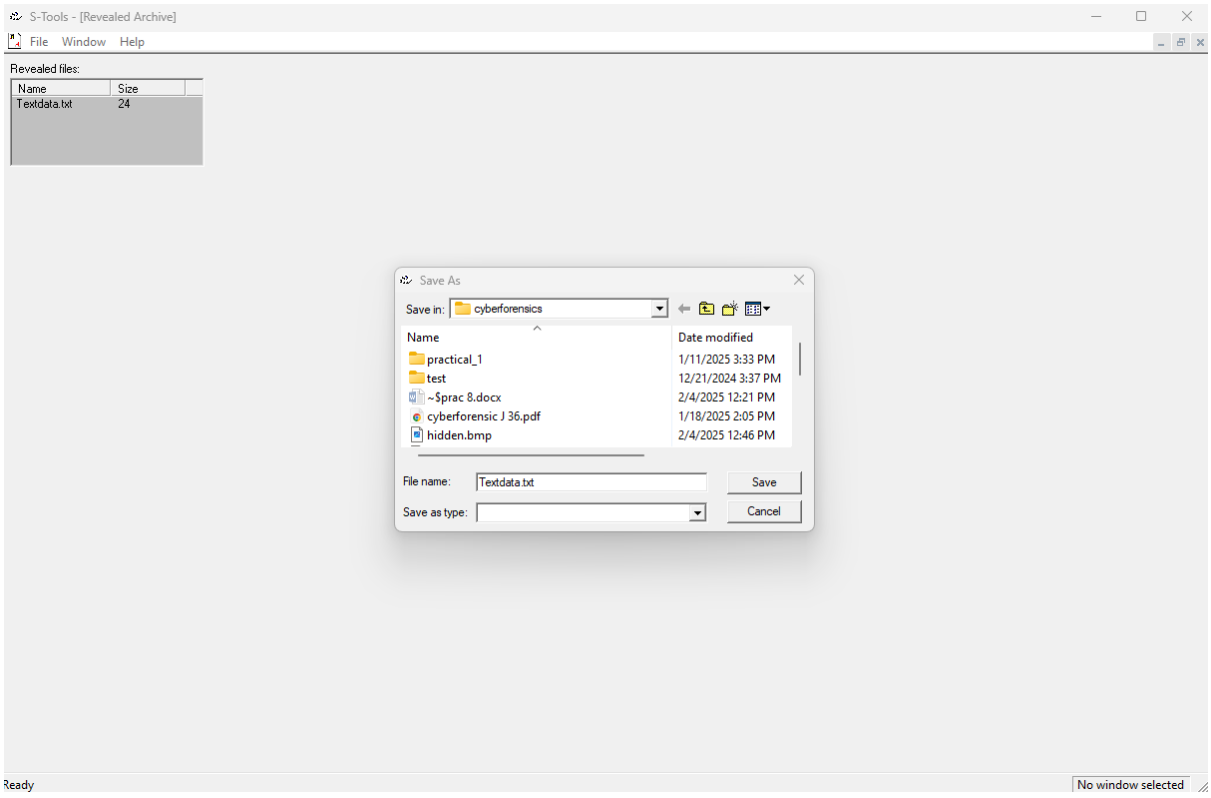


Step 6: Enter the password that you have created





Step 7: Now save the Text file (TextData) file



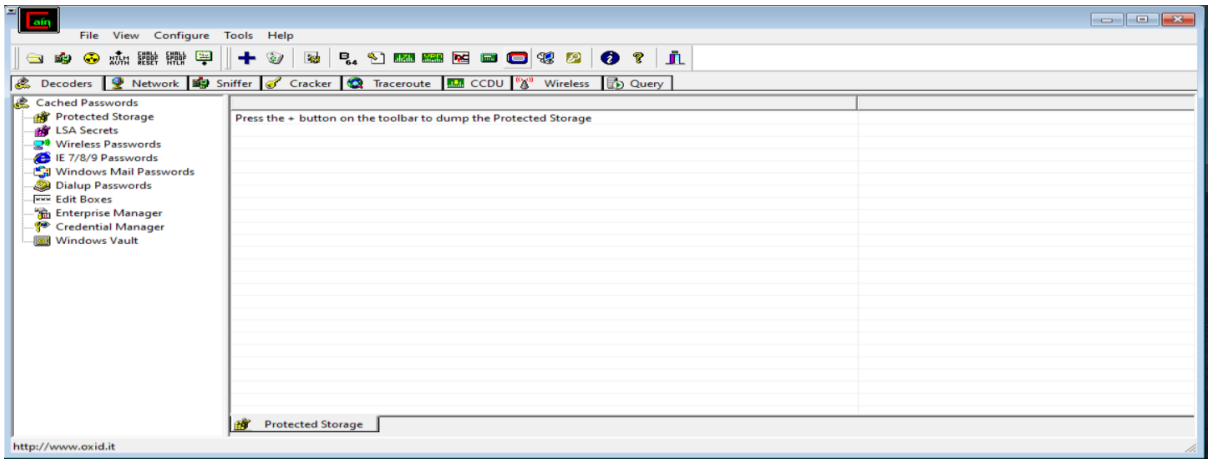
Practical: 9

Aim: (A) Performing Password Cracking [Cain & Abel].

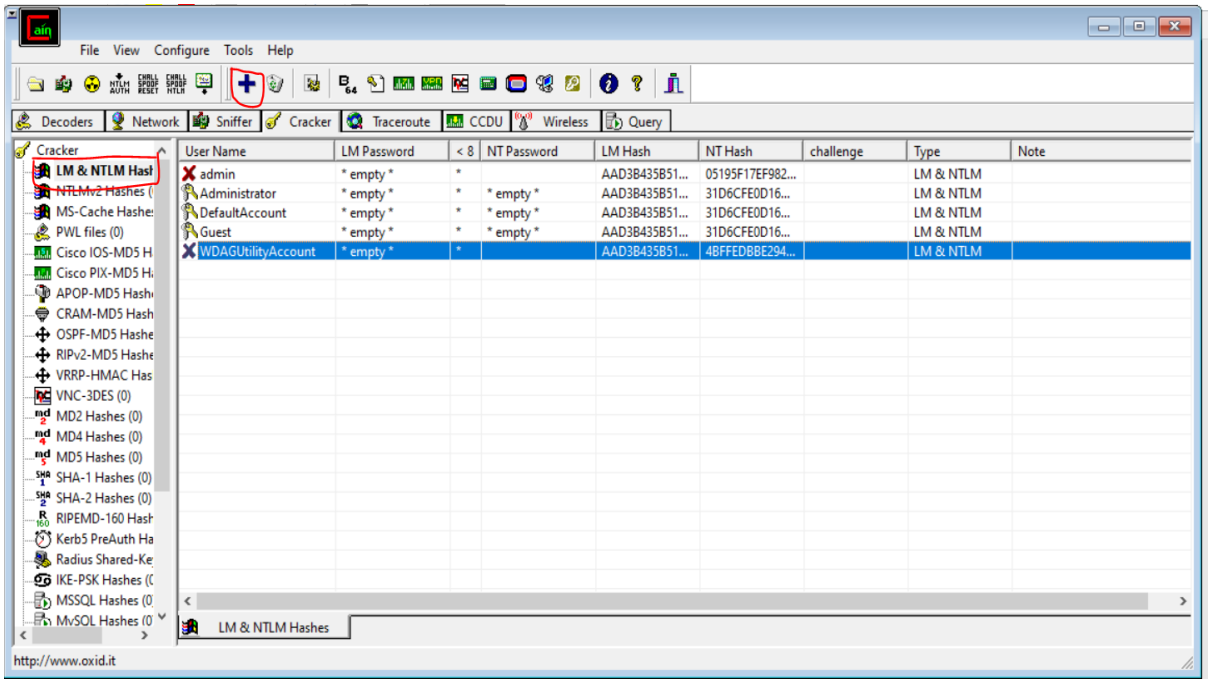
Theory

Cain & Abel is a tool that will be quite useful for network administrators, teachers, professional penetration testers, security consultants/professionals, forensic staff and security software vendors.

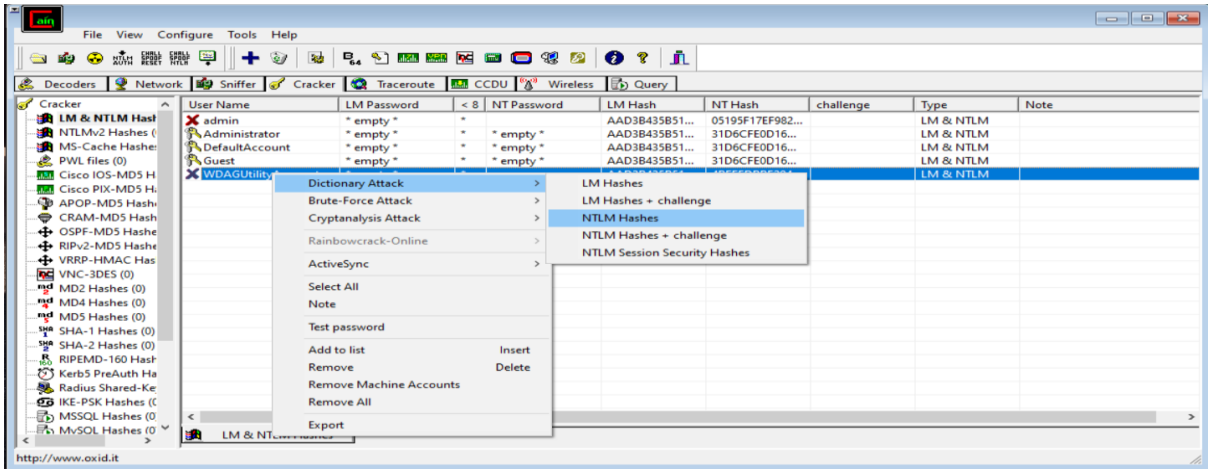
Step1:Download Cain n able software using the given link http://www.oxid.it/downloads/ca_setup.exe Now it's time to speak about the cracker tab,the most important feature of Cain.When Cain captures some LM and NTLM hashes or any kind of passwords for any supported protocols, Cain sends them automatically to the Cracker tab. We will import a local SAMfile just for demonstration purposes to illustrate this point. Here is how to import the SAMfile

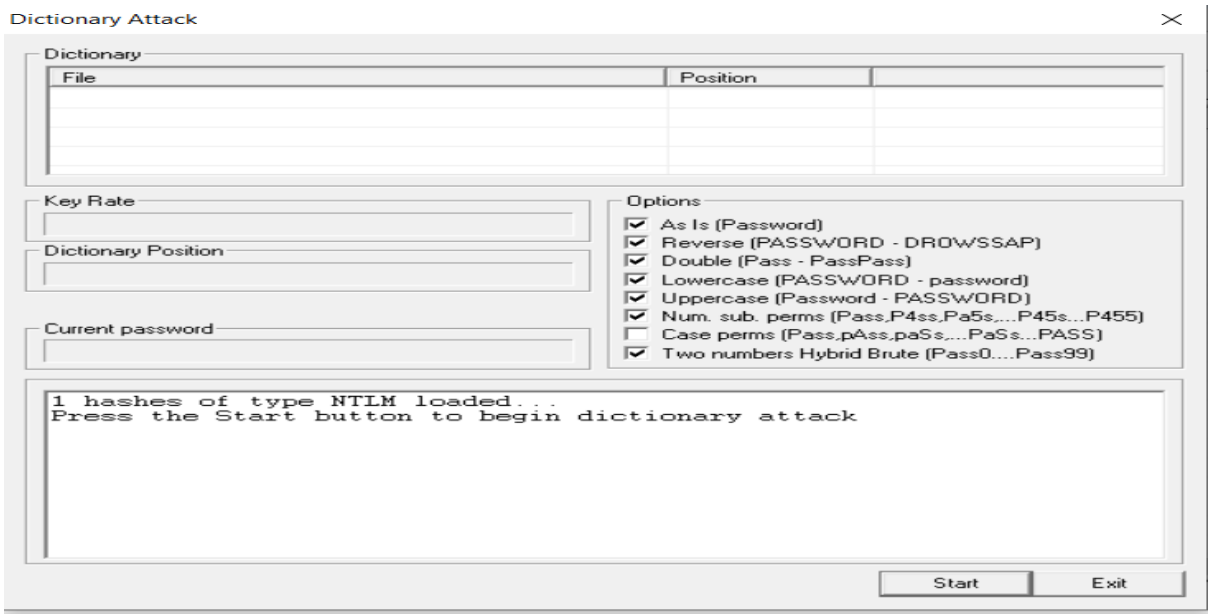


Step 2: Click on Craker-> then plus icon-> then LM & NTLM head

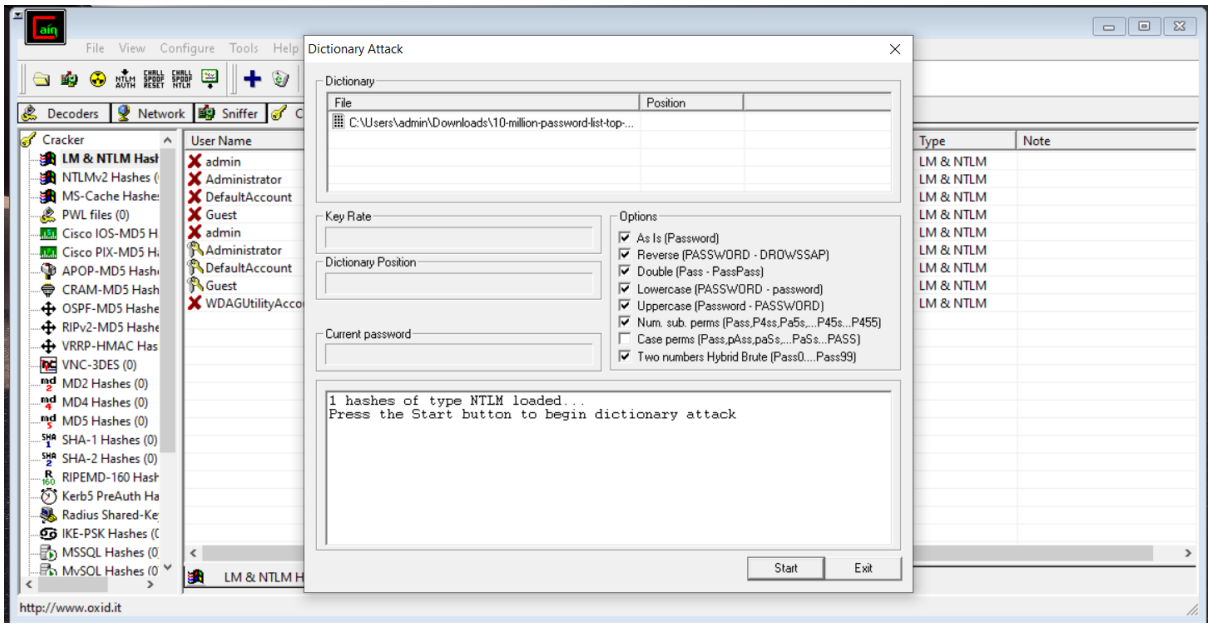


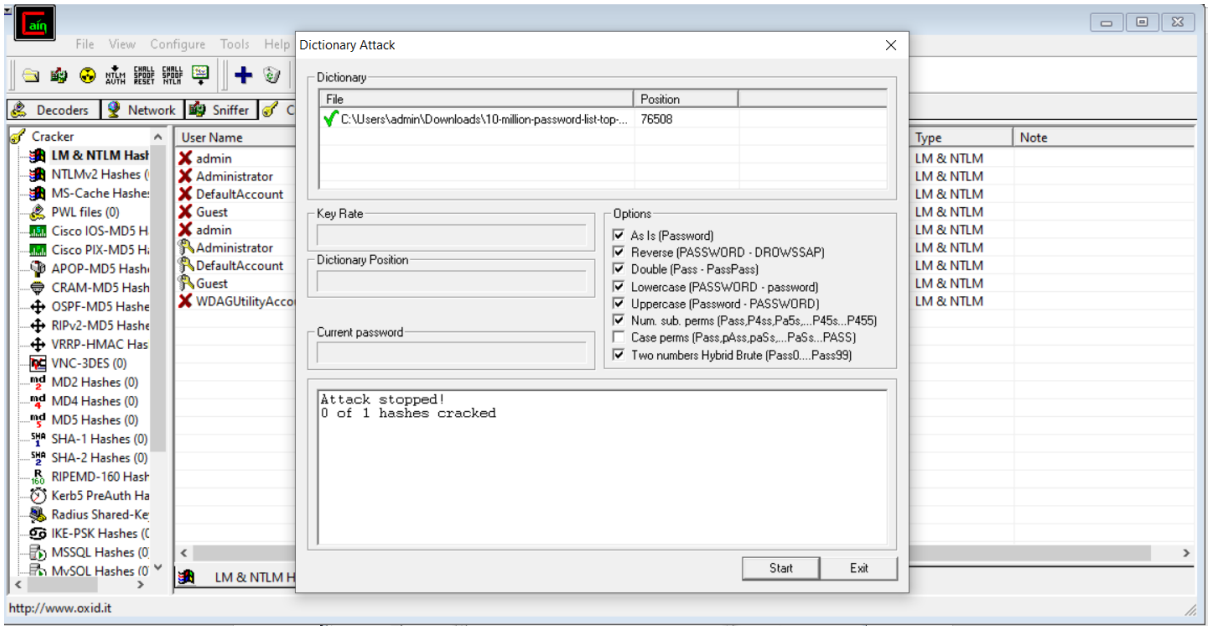
Step 3: Now right click on WDAG





Step 4: Choose a file 10-million passwords.txt (you will get on github)-> click on start




Dictionary Attack
Dictionary
File
Position
C:\Users\admin\Downloads\10-million-password-list-top-...
76508
Key Rate
Dictionary Position
Current password
Options
As Is (Password)
Reverse (PASSWORD - DROWSSAP)
Double (Pass - PassPass)
Lowercase (PASSWORD - password)
Uppercase (Password - PASSWORD)
Num. sub. perms (Pass,P4ss,Pa5s,...P45s...P455)
Case perms (Pass,pAss,paSs,...PaSs...PASS)
Two numbers Hybrid Brute (Pass0....Pass99)
Attack stopped!
0 of 1 hashes cracked
Start
Exit
Cracker
User Name
Type
Note
admin
Administrator
DefaultAccount
Guest
WDAGUtilityAcco
LM & NTLM
http://www.oxid.it

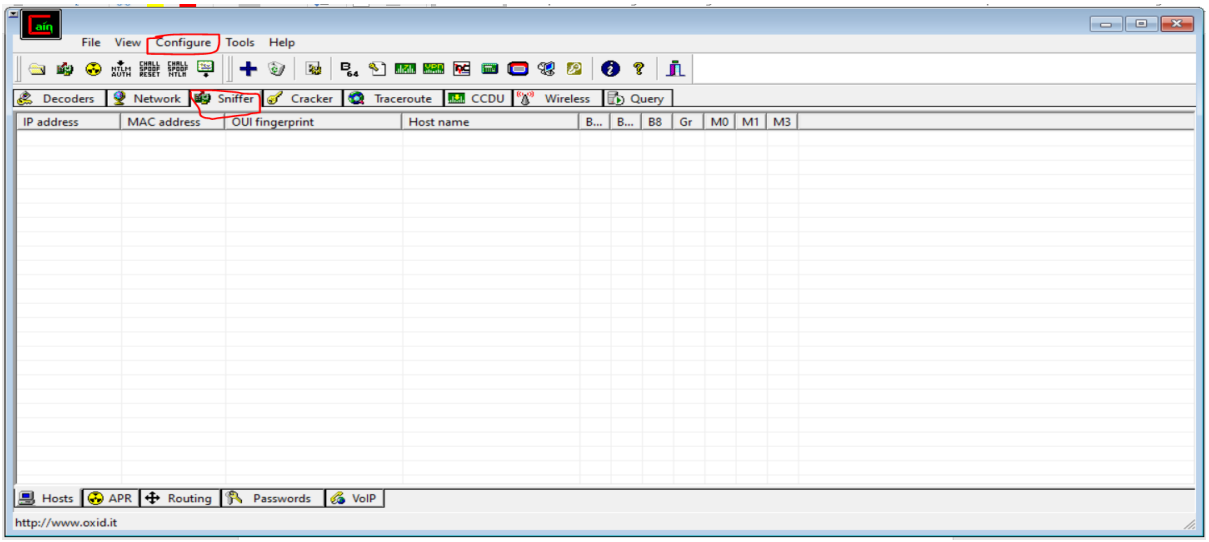
B) Performing Sniffing [Cain & Abel].

Theory

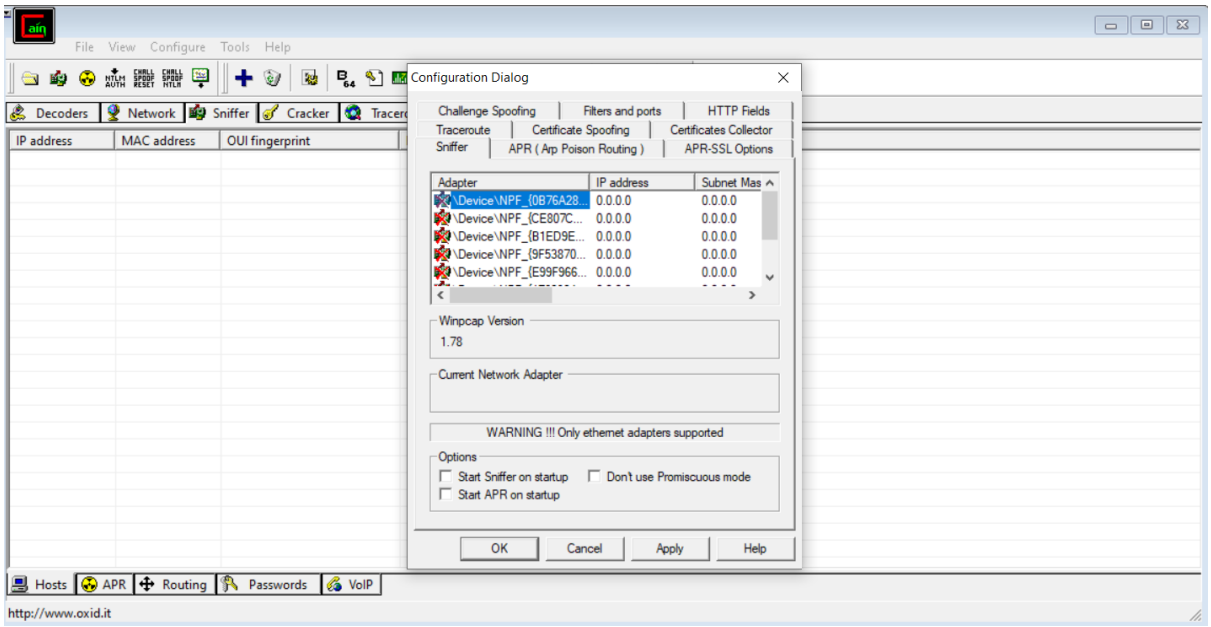
Sniffing:

A packet analyser (also known as a network analyser, protocol analyser or packet sniffer, or for particular types of networks, an Ethernet sniffer or wireless sniffer) is a computer program or a piece of computer hardware that can intercept and log traffic passing over a digital network or part of a network. As data streams flow across the network, the sniffer captures each packet and,if needed, decodes the packet's raw data, showing the values of various fields in the packet, andanalyses its content according to the appropriate RFC or other specifications.

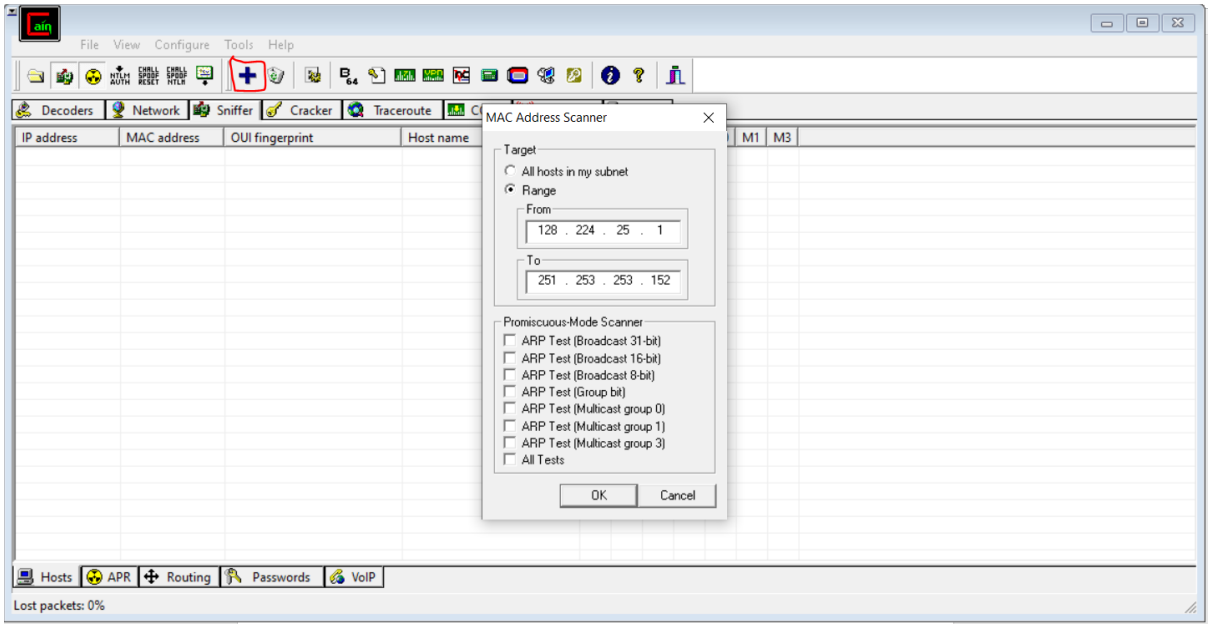
Step 1: Go to -> Sniffer Tab and click Configure in the main menu to configure your packet listening adapter.



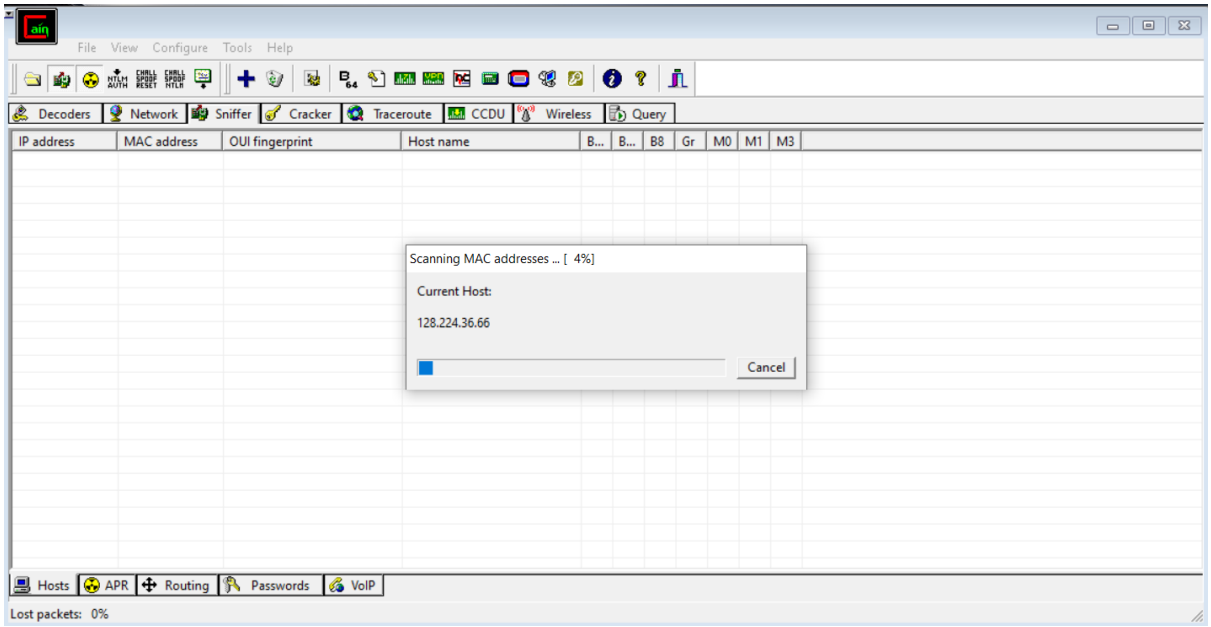
Step 2: Select the appropriate network adapter for your network that you want to sniff the packets forplain-text passwords. And Click Ok



Step 3: This is very interesting step. Now we need to select the router`s IP address and click ok. This means that we want to listen to every packet that is sent to router. If we select any other IP address in our LAN network then we can listen to only that particular HOST on the network.



Step 4: After Scanning Mac Address. You will finally get the Output.



Practical: 10

Aim: A) Scan Registry using RegScanner.

Theory

RegScanner is a small and lightweight system utility, which allows you to scan the Registry, findthe desired Registry values that match the specified search criteria and then displays them in a list.

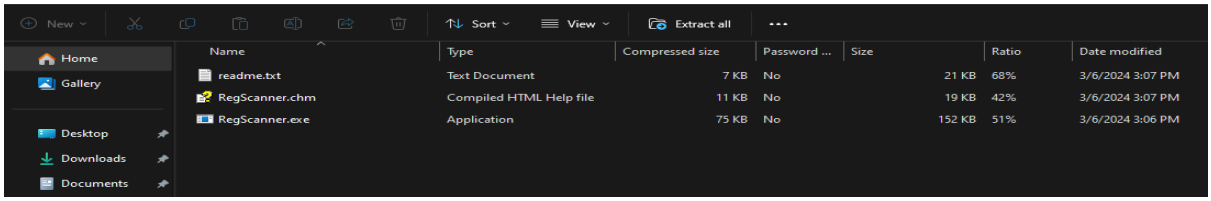
I.Problem Statement

A registry scanner or registry cleaner is third-party software for Microsoft Windows that searchesfor registry items that are redundant or no longer needed, then removes or resolves them. The objective is to help the system work more efficiently by "cleaning" it of these superfluous registryentries.

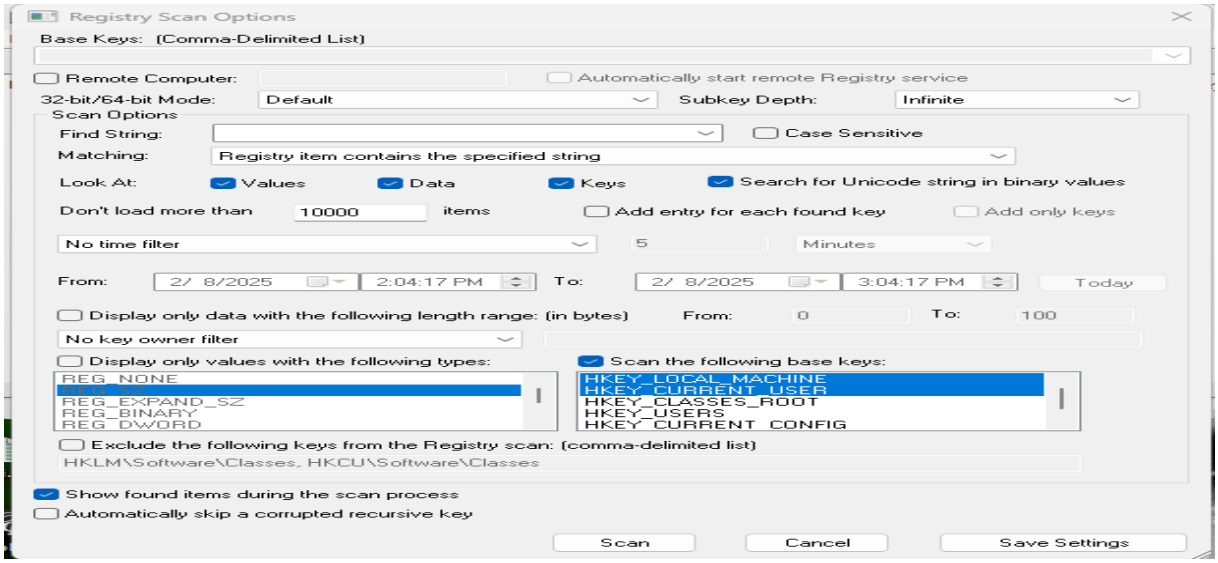
II.Literature/Theory

Some Registry cleaners make no distinction as to the severity of the errors, and many that do may erroneously categorize errors as "critical" with little basis to support it.[1] Removing or changing certain Registry data can prevent the system from starting, or cause application errorsand crashes

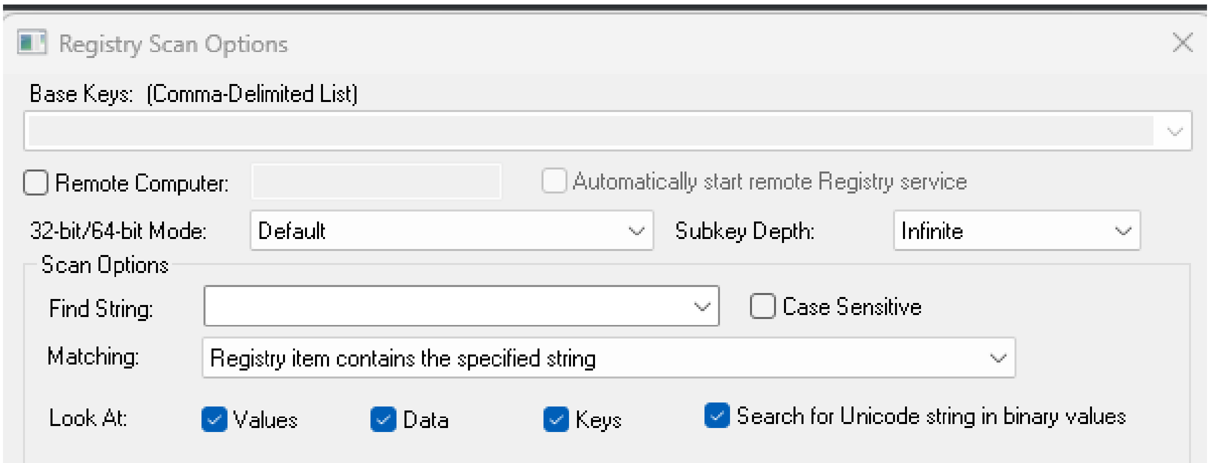
Step 1: Install RegScanner > Double click on RegScanner .exe file to run the application.



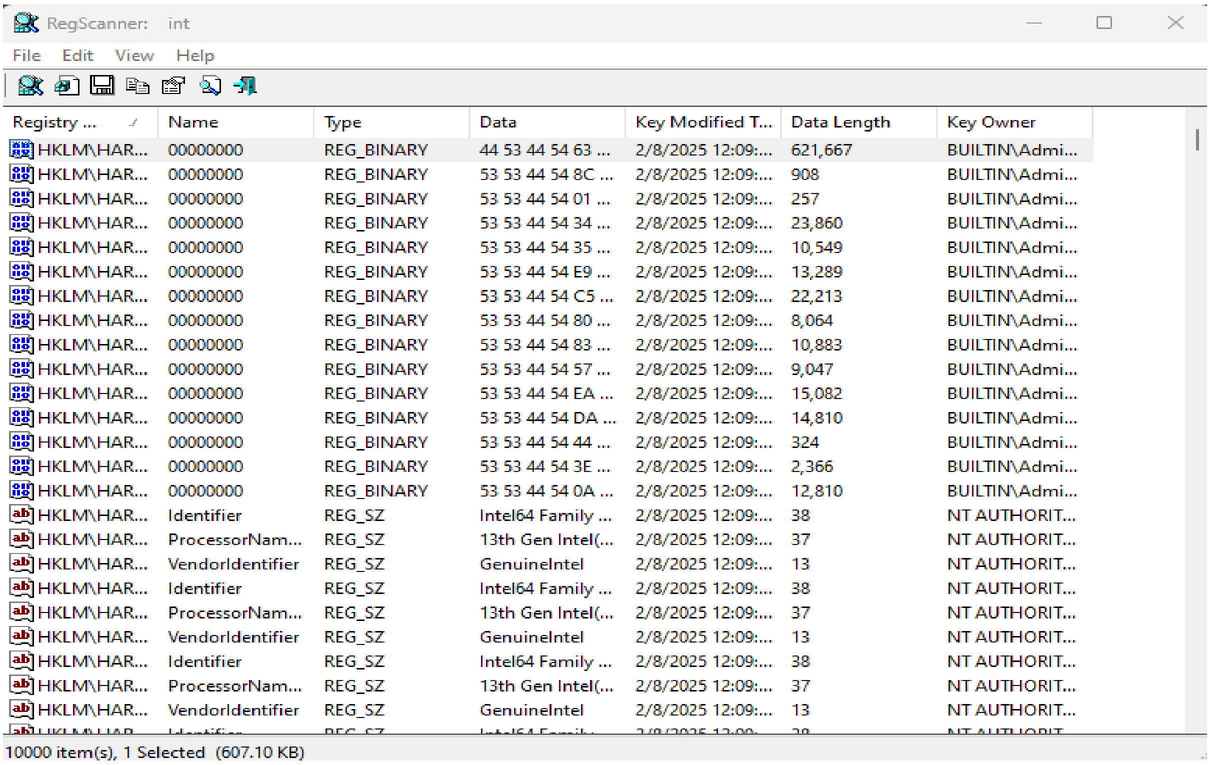
Step 2: Quickly scan your registry and you can also search for the specific values with RegScanner.. You can select to scan the base keys



Step 3: In Matching drop-down > Select Registry item contains the specified string -> Type(int)

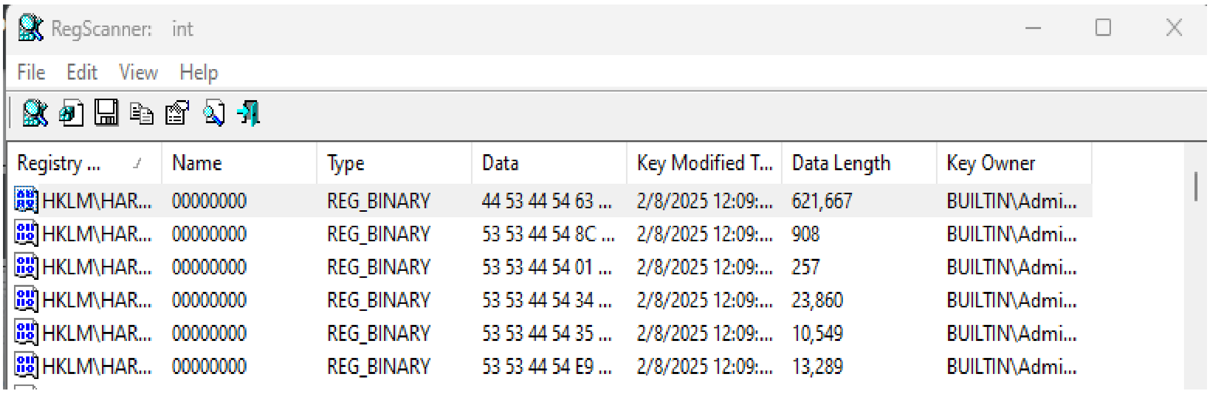


Step 4: Scan Result / Output:



Registry ...	Name	Type	Data	Key Modified T...	Data Length	Key Owner
HKLM\HAR...	00000000	REG_BINARY	44 53 44 54 63 ...	2/8/2025 12:09:...	621,667	BUILTIN\Admi...
HKLM\HAR...	00000000	REG_BINARY	53 53 44 54 8C ...	2/8/2025 12:09:...	908	BUILTIN\Admi...
HKLM\HAR...	00000000	REG_BINARY	53 53 44 54 01 ...	2/8/2025 12:09:...	257	BUILTIN\Admi...
HKLM\HAR...	00000000	REG_BINARY	53 53 44 54 34 ...	2/8/2025 12:09:...	23,860	BUILTIN\Admi...
HKLM\HAR...	00000000	REG_BINARY	53 53 44 54 35 ...	2/8/2025 12:09:...	10,549	BUILTIN\Admi...
HKLM\HAR...	00000000	REG_BINARY	53 53 44 54 E9 ...	2/8/2025 12:09:...	13,289	BUILTIN\Admi...
HKLM\HAR...	00000000	REG_BINARY	53 53 44 54 C5 ...	2/8/2025 12:09:...	22,213	BUILTIN\Admi...
HKLM\HAR...	00000000	REG_BINARY	53 53 44 54 80 ...	2/8/2025 12:09:...	8,064	BUILTIN\Admi...
HKLM\HAR...	00000000	REG_BINARY	53 53 44 54 83 ...	2/8/2025 12:09:...	10,883	BUILTIN\Admi...
HKLM\HAR...	00000000	REG_BINARY	53 53 44 54 57 ...	2/8/2025 12:09:...	9,047	BUILTIN\Admi...
HKLM\HAR...	00000000	REG_BINARY	53 53 44 54 EA ...	2/8/2025 12:09:...	15,082	BUILTIN\Admi...
HKLM\HAR...	00000000	REG_BINARY	53 53 44 54 DA ...	2/8/2025 12:09:...	14,810	BUILTIN\Admi...
HKLM\HAR...	00000000	REG_BINARY	53 53 44 54 44 ...	2/8/2025 12:09:...	324	BUILTIN\Admi...
HKLM\HAR...	00000000	REG_BINARY	53 53 44 54 3E ...	2/8/2025 12:09:...	2,366	BUILTIN\Admi...
HKLM\HAR...	00000000	REG_BINARY	53 53 44 54 0A ...	2/8/2025 12:09:...	12,810	BUILTIN\Admi...
HKLM\HAR...	Identifier	REG_SZ	Intel64 Family ...	2/8/2025 12:09:...	38	NT AUTHORIT...
HKLM\HAR...	ProcessorNam...	REG_SZ	13th Gen Intel(...	2/8/2025 12:09:...	37	NT AUTHORIT...
HKLM\HAR...	VendorIdentifier	REG_SZ	GenuineIntel	2/8/2025 12:09:...	13	NT AUTHORIT...
HKLM\HAR...	Identifier	REG_SZ	Intel64 Family ...	2/8/2025 12:09:...	38	NT AUTHORIT...
HKLM\HAR...	ProcessorNam...	REG_SZ	13th Gen Intel(...	2/8/2025 12:09:...	37	NT AUTHORIT...
HKLM\HAR...	VendorIdentifier	REG_SZ	GenuineIntel	2/8/2025 12:09:...	13	NT AUTHORIT...
HKLM\HAR...	Identifier	REG_SZ	Intel64 Family ...	2/8/2025 12:09:...	38	NT AUTHORIT...
HKLM\HAR...	ProcessorNam...	REG_SZ	13th Gen Intel(...	2/8/2025 12:09:...	37	NT AUTHORIT...
HKLM\HAR...	VendorIdentifier	REG_SZ	GenuineIntel	2/8/2025 12:09:...	13	NT AUTHORIT...

10000 item(s), 1 Selected (607.10 KB)



Registry ...	Name	Type	Data	Key Modified T...	Data Length	Key Owner
HKLM\HAR...	00000000	REG_BINARY	44 53 44 54 63 ...	2/8/2025 12:09:...	621,667	BUILTIN\Admi...
HKLM\HAR...	00000000	REG_BINARY	53 53 44 54 8C ...	2/8/2025 12:09:...	908	BUILTIN\Admi...
HKLM\HAR...	00000000	REG_BINARY	53 53 44 54 01 ...	2/8/2025 12:09:...	257	BUILTIN\Admi...
HKLM\HAR...	00000000	REG_BINARY	53 53 44 54 34 ...	2/8/2025 12:09:...	23,860	BUILTIN\Admi...
HKLM\HAR...	00000000	REG_BINARY	53 53 44 54 35 ...	2/8/2025 12:09:...	10,549	BUILTIN\Admi...
HKLM\HAR...	00000000	REG_BINARY	53 53 44 54 E9 ...	2/8/2025 12:09:...	13,289	BUILTIN\Admi...

B) Study Registry Viewer tool (Alien Registry Viewer).

Theory

I.Title

Alien Registry Viewer allows you to explore registry files, search for specific key names and values, export registry data into a. REG or text file and bookmark registry keys as favorites. As well as the above mentioned files, Windows uses hidden files with the same names and extensions.

II.Problem Statement

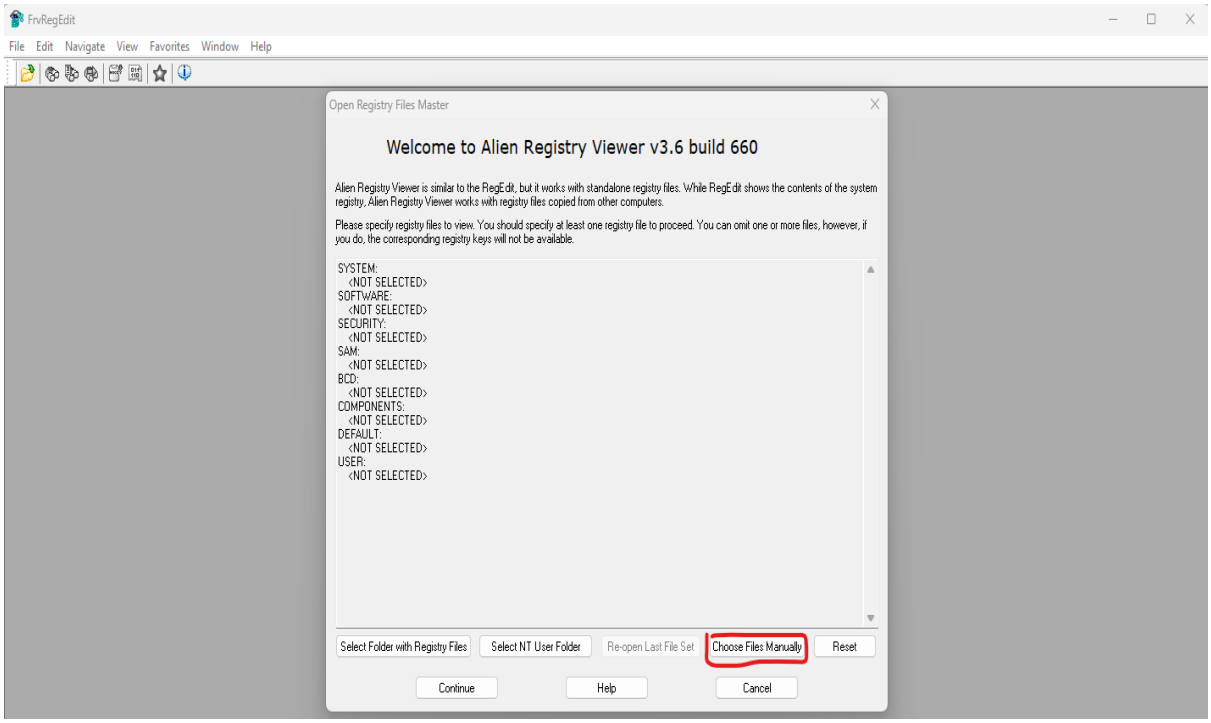
Registry Viewer allows you to view the protected storage of a registry. Passwords, usernames, and other information can be stored in the secured storage, which is not accessible using the Windows Registry Editor. Registry Viewer comes with a number of tools for retrieving and reporting vital registry data.

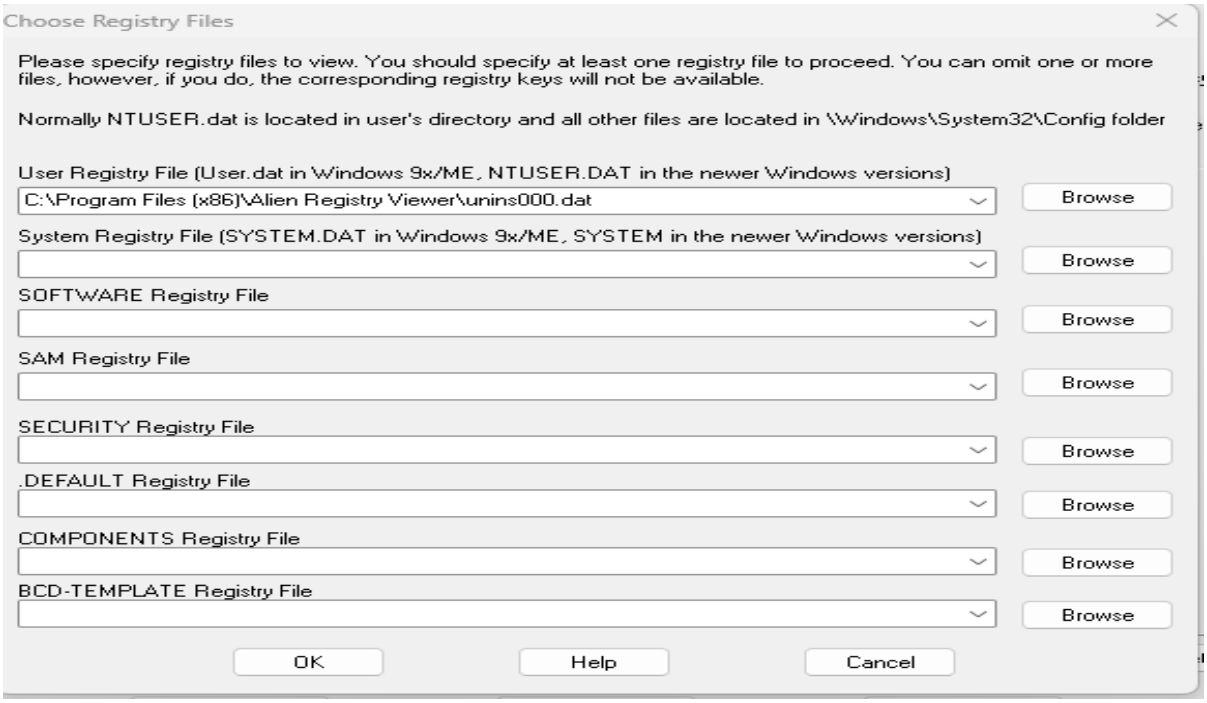
III.Literature/Theory

Alien Registry Viewer is similar to the RegEdit application included into Windows, but unlike RegEdit, it works with standalone registry files. The current version of Alien Registry Viewer works in the read-only mode, i.e. you can view but you cannot edit registry files.

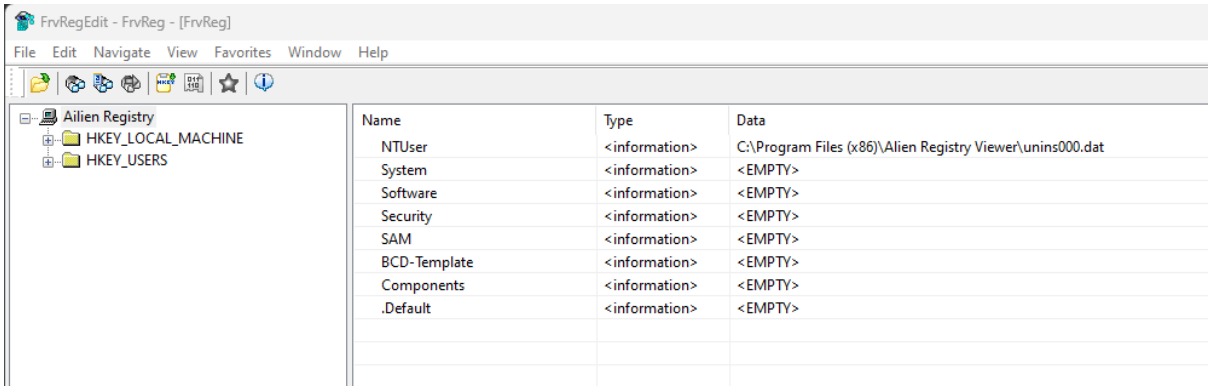
Step 1: Install the Alien registry viewer by double clicking on the .exe file.-> The following window would appear.Click on Next.

Step 2: After installation the following window would appear.





Step 3: Click on HKEY_CLASSES_ROOT HKEY_CURRENT_USER…. etc



Step 4: Press CTRL + F. The following dialog box will appear.in Find what textbox type .pdf > Click Find Next.