

## Practical: 1

**Aim:** File System Analysis using The SleuthKit (Autopsy).

### 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

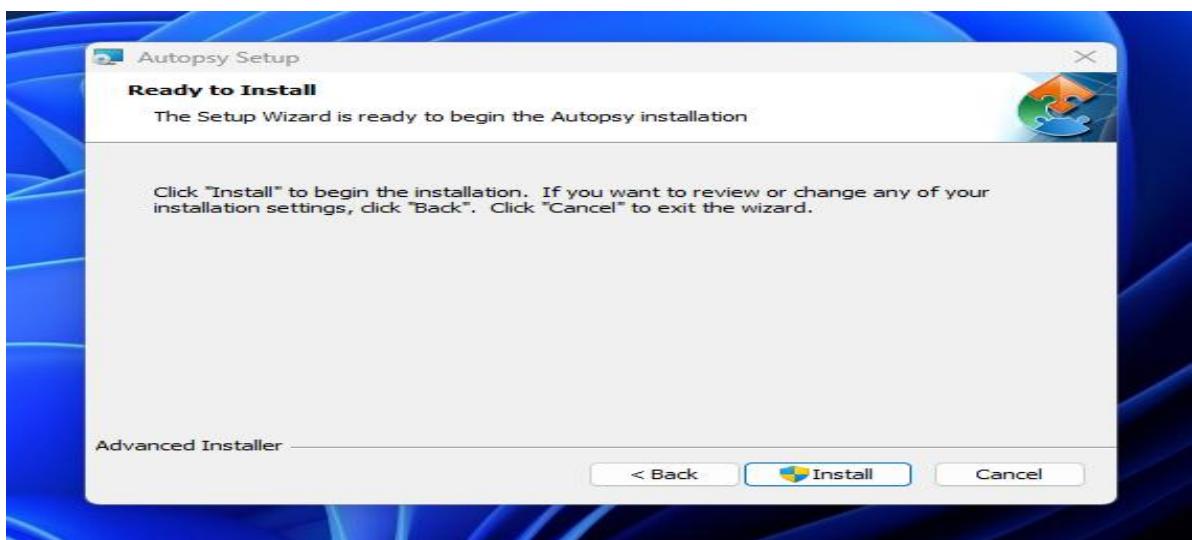
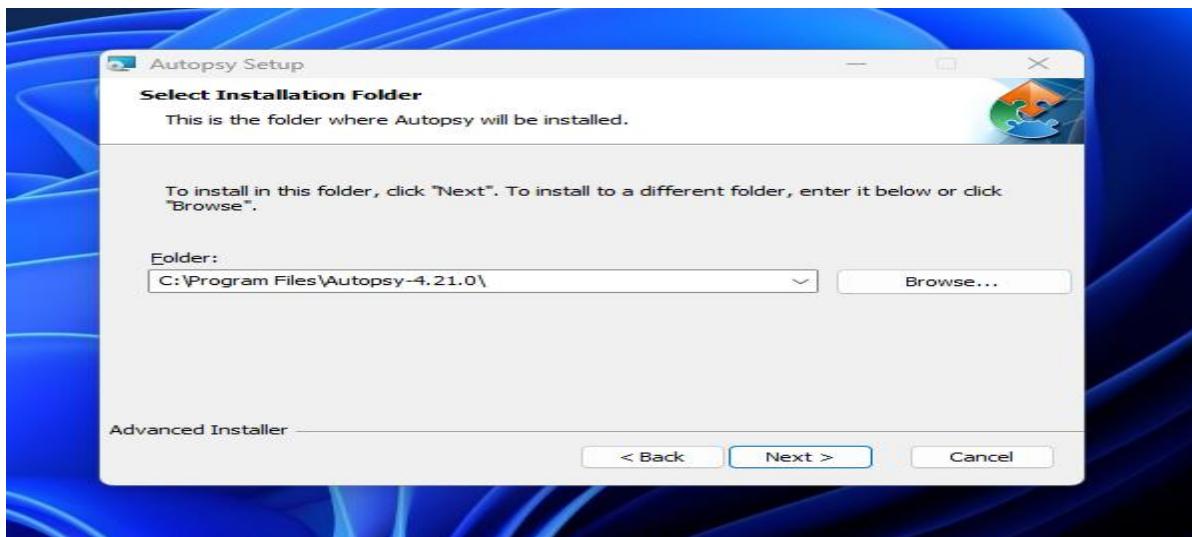
Autopsy is a digital forensics platform and graphical interface to The Sleuth Kit® and other digital forensics tools. It is used by law enforcement, military, and corporate examiners to investigate what happened on a computer. You can even use it to recover photos from your camera's memory card.

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

New Case Information

**Steps**

1. Case Information
2. Optional Information

**Case Information**

Case Name: practical\_1

Base Directory: D:\cyberforensics\

Case Type:  Single-User  Multi-User

Case data will be stored in the following directory:  
D:\cyberforensics\practical\_1

< Back  Finish Cancel Help

New Case Information

**Steps**

1. Case Information
2. **Optional Information**

**Optional Information**

Case

Number: 001

Examiner

Name: Tareeq Esaf

Phone: 9856585431

Email: Esaf2132321@gmail.com

Notes:

Organization

Organization analysis is being done for: Not Specified

< Back  Finish Cancel Help

Add Data Source

**Steps**

1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source

**Select Host**

Hosts are used to organize data sources and other data.

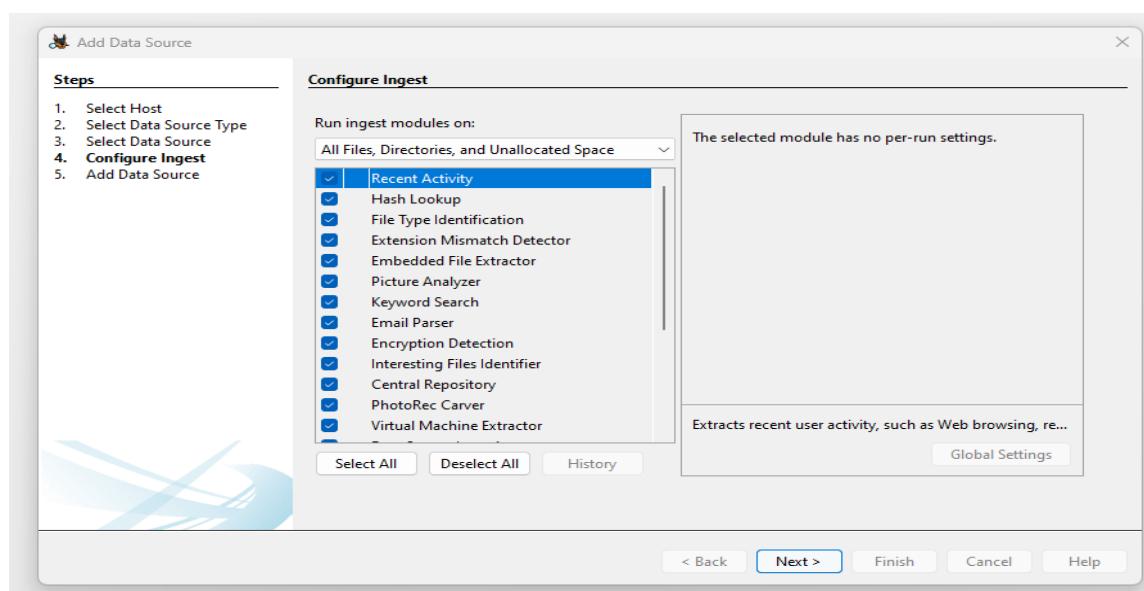
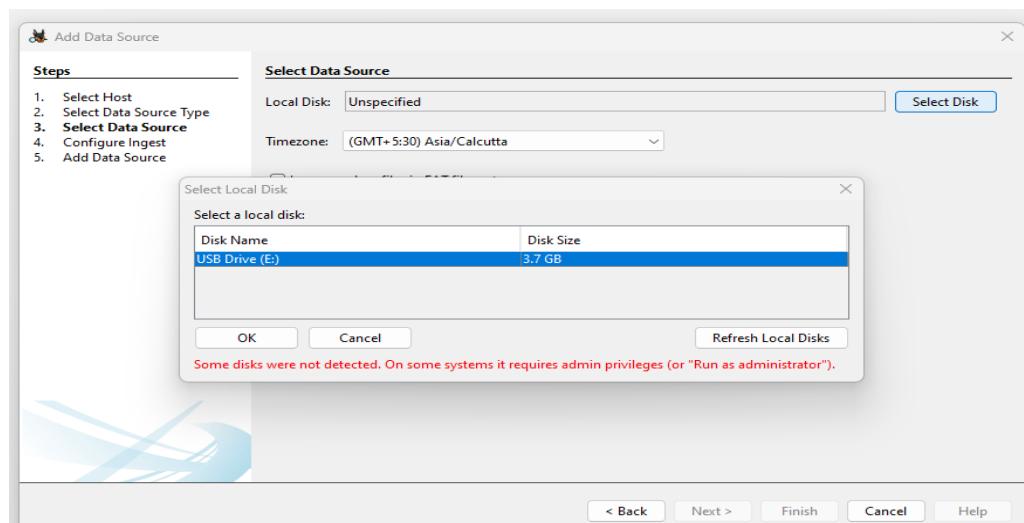
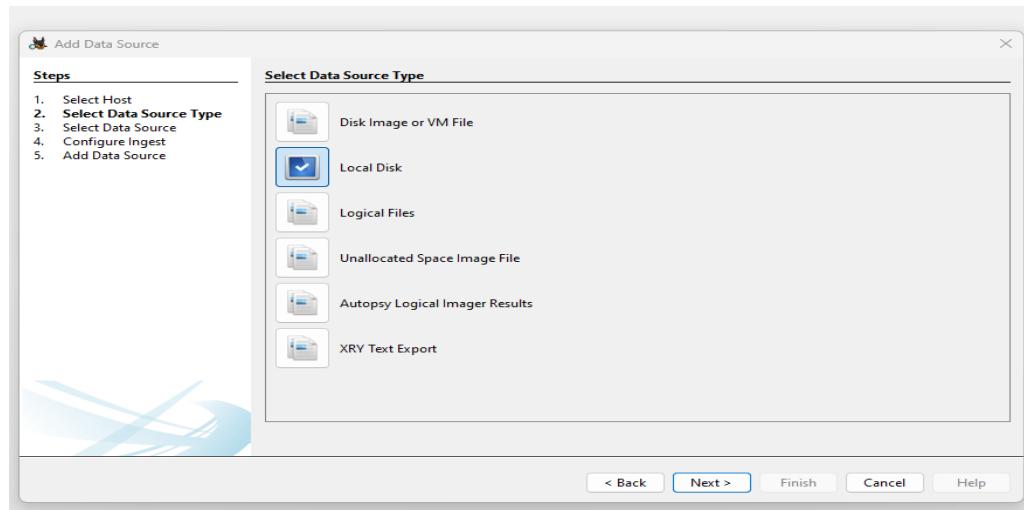
Generate new host name based on data source name

Specify new host name

Use existing host

< Back  Finish Cancel Help

### Step 3 -Choose the path



## Step 4 -Retrieve the classified files

Screenshot of Autopsy 4.21.0 showing the listing of files from the E:\ Host data source. A context menu is open over several files, with 'Extract File(s)' highlighted.

| Name                               | S | C | O | Modified Time           | Change Time         | Access Time             | Created Time            | Size  | Flags(Dir)  | Flags(Meta) | Known   | Location                |
|------------------------------------|---|---|---|-------------------------|---------------------|-------------------------|-------------------------|-------|-------------|-------------|---------|-------------------------|
| pic1.jpg.crdownload                |   |   |   | 2023-01-11 14:18:44 IST | 0000-00-00 00:00:00 | 2025-01-11 00:00:00 IST | 2025-01-11 14:18:42 IST | 10133 | Unallocated | Unallocated | unknown | /img_E:/pic1.jpg.crdown |
| pic2.jpg.crdownload                |   |   |   | 2025-01-11 14:19:20 IST | 0000-00-00 00:00:00 | 2025-01-11 00:00:00 IST | 2025-01-11 14:19:19 IST | 14571 | Unallocated | Unallocated | unknown | /img_E:/pic2.jpg.crdown |
| pic3.jpg.crdownload                |   |   |   | 2025-01-11 14:19:30 IST | 0000-00-00 00:00:00 | 2025-01-11 00:00:00 IST | 2025-01-11 14:19:29 IST | 5011  | Unallocated | Unallocated | unknown | /img_E:/pic3.jpg.crdown |
| REPORT ON FACE                     |   |   |   | 2024-12-04 14:32:02 IST | 0000-00-00 00:00:00 | 2025-01-11 00:00:00 IST | 2025-01-11 14:15:45 IST | 19328 | Unallocated | Unallocated | unknown | /img_E:/REPORT ON FA    |
| REPORT ON FACE                     |   |   |   | 2025-01-11 14:16:08 IST | 0000-00-00 00:00:00 | 2025-01-11 00:00:00 IST | 2025-01-11 14:15:54 IST | 19252 | Unallocated | Unallocated | unknown | /img_E:/REPORT ON FA    |
| REPORT ON FACE                     |   |   |   | 2025-01-11 14:16:08 IST | 0000-00-00 00:00:00 | 2025-01-11 00:00:00 IST | 2025-01-11 14:15:54 IST | 19252 | Unallocated | Unallocated | unknown | /img_E:/REPORT ON FA    |
| REPORT ON FACE                     |   |   |   | 2025-01-11 14:16:30 IST | 0000-00-00 00:00:00 | 2025-01-11 00:00:00 IST | 2025-01-11 14:15:54 IST | 19264 | Unallocated | Unallocated | unknown | /img_E:/REPORT ON FA    |
| REPORT ON FACE                     |   |   |   | 2025-01-11 14:17:30 IST | 0000-00-00 00:00:00 | 2025-01-11 00:00:00 IST | 2025-01-11 14:17:28 IST | 0     | Unallocated | Unallocated | unknown | /img_E:/REPORT ON FA    |
| New Microsoft Wo                   |   |   |   | 2023-01-11 14:16:02 IST | 0000-00-00 00:00:00 | 2025-01-11 00:00:00 IST | 2025-01-11 14:15:54 IST | 19252 | Unallocated | Unallocated | unknown | /img_E:/New Microsoft   |
| j1.jpg                             |   |   |   | 2025-01-11 14:16:56 IST | 0000-00-00 00:00:00 | 2025-01-11 00:00:00 IST | 2025-01-11 14:16:55 IST | 0     | Unallocated | Unallocated | unknown | /img_E:/j1.jpg          |
| j2.jpg                             |   |   |   | 2025-01-11 14:16:56 IST | 0000-00-00 00:00:00 | 2025-01-11 00:00:00 IST | 2025-01-11 14:16:54 IST | 0     | Unallocated | Unallocated | unknown | /img_E:/j2.jpg          |
| j3.jpg                             |   |   |   | 2025-01-11 14:16:54 IST | 0000-00-00 00:00:00 | 2025-01-11 00:00:00 IST | 2025-01-11 14:16:53 IST | 0     | Unallocated | Unallocated | unknown | /img_E:/j3.jpg          |
| Screenshot 2024-1                  |   |   |   | 2024-12-21 14:40:24 IST | 0000-00-00 00:00:00 | 2025-01-11 00:00:00 IST | 2025-01-11 14:22:57 IST | 37359 | Unallocated | Unallocated | unknown | /img_E:/Screenshot 202  |
| Screenshot 2024-12-21 14:40:40.png |   |   |   | 2024-12-21 14:40:42 IST | 0000-00-00 00:00:00 | 2025-01-11 00:00:00 IST | 2025-01-11 14:22:58 IST | 39160 | Unallocated | Unallocated | unknown | /img_E:/Screenshot 202  |
| Screenshot 2024-12-21 14:40:57.png |   |   |   | 2024-12-21 14:40:58 IST | 0000-00-00 00:00:00 | 2025-01-11 00:00:00 IST | 2025-01-11 14:22:57 IST | 35823 | Unallocated | Unallocated | unknown | /img_E:/Screenshot 202  |
| Screenshot 2024-12-21 14:51:12 IST |   |   |   | 2024-12-21 14:51:12 IST | 0000-00-00 00:00:00 | 2025-01-11 00:00:00 IST | 2025-01-11 14:22:57 IST | 9958  | Unallocated | Unallocated | unknown | /img_E:/Screenshot 202  |
| Screenshot 2025-01-08 11:59:04 IST |   |   |   | 2025-01-08 11:59:04 IST | 0000-00-00 00:00:00 | 2025-01-11 00:00:00 IST | 2025-01-11 14:22:57 IST | 79441 | Unallocated | Unallocated | unknown | /img_E:/Screenshot 202  |
| Screenshot 2025-01-08 11:59:03.png |   |   |   | 2025-01-08 11:59:03 IST | 0000-00-00 00:00:00 | 2025-01-11 00:00:00 IST | 2025-01-11 14:22:57 IST | 79441 | Unallocated | Unallocated | unknown | /img_E:/Screenshot 202  |
| WRN00001.mmn                       |   |   |   | 2025-01-11 14:16:07 IST | 0000-00-00 00:00:00 | 2025-01-11 00:00:00 IST | 2025-01-11 14:15:54 IST | 10757 | Unallocated | Unallocated | unknown | /mnis F:/WRN00001.mmn   |

Screenshot of Autopsy 4.21.0 showing the 'Encryption Detected' section. A context menu is open over a file named 'REPORT ON FACEBOOK INSIGHTS\_pwd.docx', with 'Add File Tag' highlighted.

| Source Name                          | S | C | O | Source Type | Score | Conclusion | Configuration | Justification | Comment                       | File Path                                    |
|--------------------------------------|---|---|---|-------------|-------|------------|---------------|---------------|-------------------------------|--|
| REPORT ON FACEBOOK INSIGHTS_pwd.docx |   |   |   | File        | 0     | Notable    |               |               | Password protection detected. | /img_E:/REPORT ON FACEBOOK INSIGHTS_gwd.docx |

Generate Report dialog box:

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 KMZ
- 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

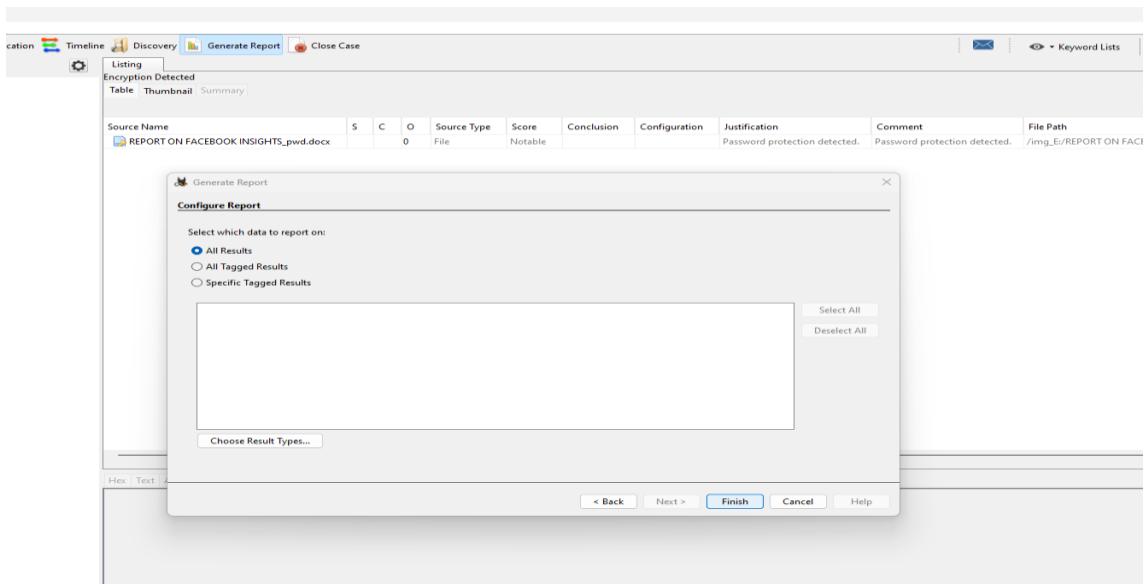
Generate Report dialog box:

Select which data source(s) to include

E:

Uncheck All    Check All

< Back    Next >    Finish    Cancel    Help



Excel file - Excel

| A  | B                       | C                          | D               | E                     | F       | G       | H                                       | I    | J | K | L | M | N | O | P | Q | R | S | T | U |
|----|-------------------------|----------------------------|-----------------|-----------------------|---------|---------|---|------|---|---|---|---|---|---|---|---|---|---|---|---|
| 1  | Date Created            | Date Modified              | Owner           | Program Name          | User ID | Version | Source File                             | Tags |   |   |   |   |   |   |   |   |   |   |   |   |
| 2  | 2024-12-04 09:02:00 IST | 2024-12-04 09:02:00 IST    | Admin           | Microsoft Office Word | Admin   |         | /img_E/3Carvedfiles/1/f0000000.docx     |      |   |   |   |   |   |   |   |   |   |   |   |   |
| 3  | 2024-12-04 09:02:00 IST | 2024-12-04 09:02:00 IST    | Admin           | Microsoft Office Word | Admin   |         | /img_E/REPORT ON FACEBOOK INSIGHTS.docx |      |   |   |   |   |   |   |   |   |   |   |   |   |
| 4  | 2024-12-04 09:02:00 IST | 2024-12-04 09:02:00 IST    | Admin           | Microsoft Office Word | Admin   |         | /img_E/_WRL000000.tmp                   |      |   |   |   |   |   |   |   |   |   |   |   |   |
| 5  | 2024-12-04 09:02:00 IST | 2024-12-04 11:08:46:00 IST | Admin           | Microsoft Office Word | Admin   |         | /img_E/_WRL000000.docx                  |      |   |   |   |   |   |   |   |   |   |   |   |   |
| 6  | 2024-12-04 09:02:00 IST | 2024-12-04 09:02:00 IST    | Admin           | Microsoft Office Word | Admin   |         | /img_E/_WRL000000.tmp                   |      |   |   |   |   |   |   |   |   |   |   |   |   |
| 7  | 2024-12-04 09:02:00 IST | 2024-12-04 09:02:00 IST    | Admin           | Microsoft Office Word | Admin   |         | /img_E/_WRL000000.docx                  |      |   |   |   |   |   |   |   |   |   |   |   |   |
| 8  | 2024-12-04 09:02:00 IST | 2024-12-04 09:02:00 IST    | Admin           | Microsoft Office Word | Admin   |         | /img_E/_WRL000000.tmp                   |      |   |   |   |   |   |   |   |   |   |   |   |   |
| 9  | 2024-12-04 09:02:00 IST | 2024-12-04 09:02:00 IST    | Admin           | Microsoft Office Word | Admin   |         | /img_E/_WRL000000.docx                  |      |   |   |   |   |   |   |   |   |   |   |   |   |
| 10 | 2024-12-04 09:02:00 IST | 2024-12-04 09:02:00 IST    | Admin           | Microsoft Office Word | Admin   |         | /img_E/_WRL000000.tmp                   |      |   |   |   |   |   |   |   |   |   |   |   |   |
| 11 | 2024-12-04 09:02:00 IST | 2024-12-04 09:02:00 IST    | Admin           | Microsoft Office Word | Admin   |         | /img_E/_WRL000000.docx                  |      |   |   |   |   |   |   |   |   |   |   |   |   |
| 12 | 2024-12-04 09:02:00 IST | 2024-12-04 09:02:00 IST    | Admin           | Microsoft Office Word | Admin   |         | /img_E/_WRL000000.tmp                   |      |   |   |   |   |   |   |   |   |   |   |   |   |
| 13 | 2024-12-04 09:02:00 IST | 2024-12-04 09:02:00 IST    | Admin           | Microsoft Office Word | Admin   |         | /img_E/_WRL000000.docx                  |      |   |   |   |   |   |   |   |   |   |   |   |   |
| 14 | 2024-12-04 09:02:00 IST | 2024-12-04 09:02:00 IST    | Admin           | Microsoft Office Word | Admin   |         | /img_E/_WRL000000.tmp                   |      |   |   |   |   |   |   |   |   |   |   |   |   |
| 15 | 2024-12-04 09:02:00 IST | 2024-12-04 09:02:00 IST    | Admin           | Microsoft Office Word | Admin   |         | /img_E/_WRL000000.docx                  |      |   |   |   |   |   |   |   |   |   |   |   |   |
| 16 | 2024-12-20 09:57:47 IST | 2024-12-20 09:57:47 IST    | Neha Vora       |                       |         |         |   |      |   |   |   |   |   |   |   |   |   |   |   |   |
| 17 | 2024-12-21 06:55:18 IST | 2024-12-21 06:55:18 IST    | Neha Vora       |                       |         |         |   |      |   |   |   |   |   |   |   |   |   |   |   |   |
| 18 | 2024-12-24 04:58:00 IST | 2024-12-24 04:58:00 IST    | Jhanvi Upadhyay | Microsoft Office Word | Admin   |         | /img_E/_JAVA_PROJECT.docx               |      |   |   |   |   |   |   |   |   |   |   |   |   |
| 19 |                         |                            |                 |                       |         |         |   |      |   |   |   |   |   |   |   |   |   |   |   |   |
| 20 |                         |                            |                 |                       |         |         |   |      |   |   |   |   |   |   |   |   |   |   |   |   |
| 21 |                         |                            |                 |                       |         |         |   |      |   |   |   |   |   |   |   |   |   |   |   |   |
| 22 |                         |                            |                 |                       |         |         |   |      |   |   |   |   |   |   |   |   |   |   |   |   |
| 23 |                         |                            |                 |                       |         |         |   |      |   |   |   |   |   |   |   |   |   |   |   |   |
| 24 |                         |                            |                 |                       |         |         |   |      |   |   |   |   |   |   |   |   |   |   |   |   |
| 25 |                         |                            |                 |                       |         |         |   |      |   |   |   |   |   |   |   |   |   |   |   |   |
| 26 |                         |                            |                 |                       |         |         |   |      |   |   |   |   |   |   |   |   |   |   |   |   |
| 27 |                         |                            |                 |                       |         |         |   |      |   |   |   |   |   |   |   |   |   |   |   |   |
| 28 |                         |                            |                 |                       |         |         |   |      |   |   |   |   |   |   |   |   |   |   |   |   |
| 29 |                         |                            |                 |                       |         |         |   |      |   |   |   |   |   |   |   |   |   |   |   |   |
| 30 |                         |                            |                 |                       |         |         |   |      |   |   |   |   |   |   |   |   |   |   |   |   |
| 31 |                         |                            |                 |                       |         |         |   |      |   |   |   |   |   |   |   |   |   |   |   |   |
| 32 |                         |                            |                 |                       |         |         |   |      |   |   |   |   |   |   |   |   |   |   |   |   |
| 33 |                         |                            |                 |                       |         |         |   |      |   |   |   |   |   |   |   |   |   |   |   |   |
| 34 |                         |                            |                 |                       |         |         |   |      |   |   |   |   |   |   |   |   |   |   |   |   |
| 35 |                         |                            |                 |                       |         |         |   |      |   |   |   |   |   |   |   |   |   |   |   |   |
| 36 |                         |                            |                 |                       |         |         |   |      |   |   |   |   |   |   |   |   |   |   |   |   |
| 37 |                         |                            |                 |                       |         |         |   |      |   |   |   |   |   |   |   |   |   |   |   |   |
| 38 |                         |                            |                 |                       |         |         |   |      |   |   |   |   |   |   |   |   |   |   |   |   |

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.

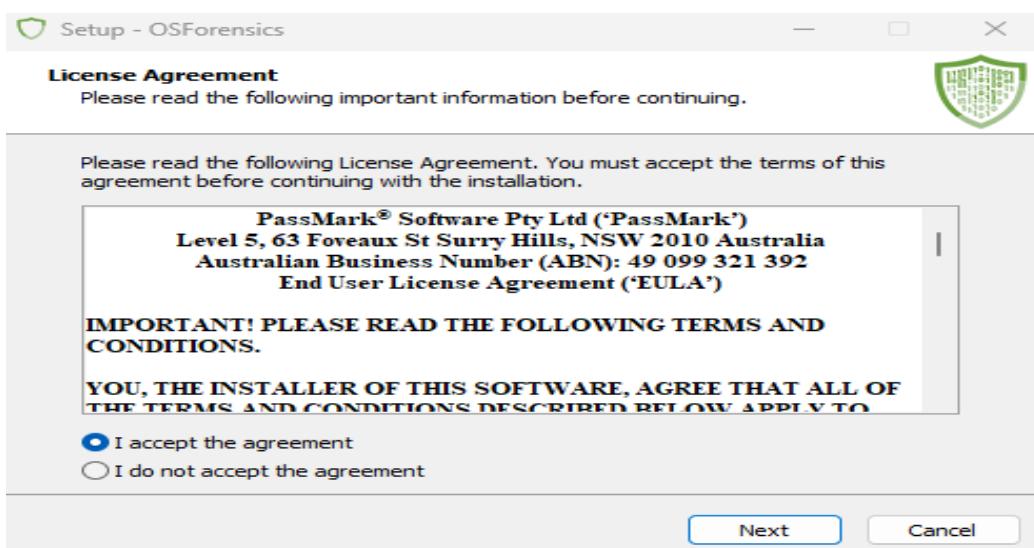
The professional and bootable editions of OS Forensics have many features not available in the free edition, including:

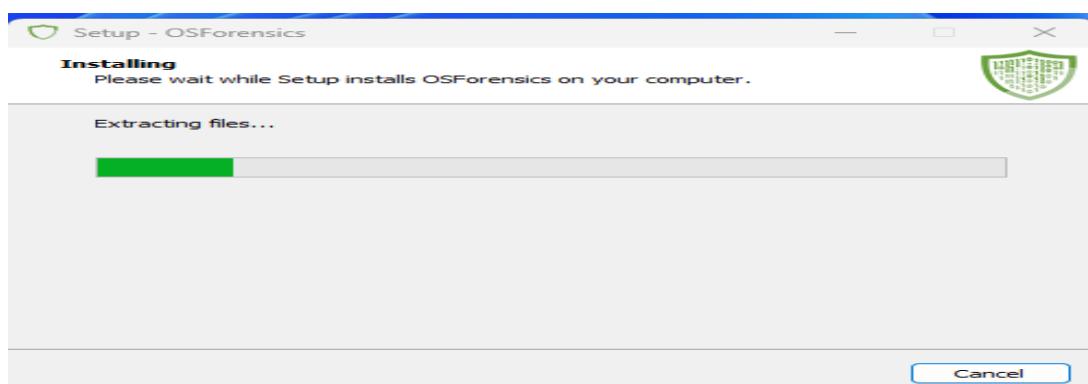
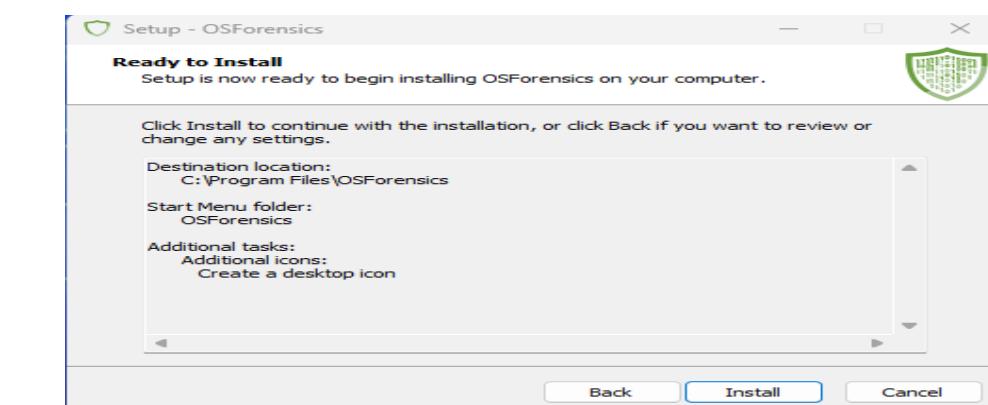
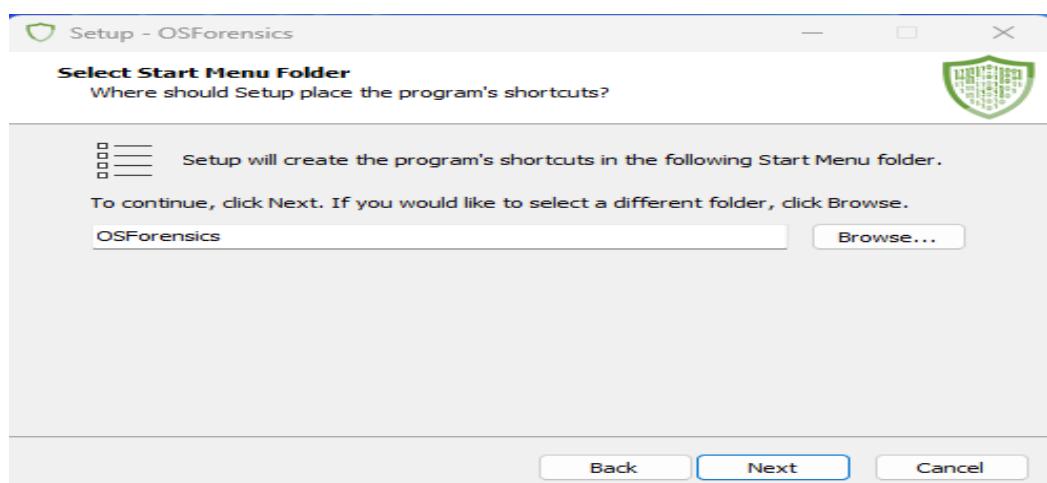
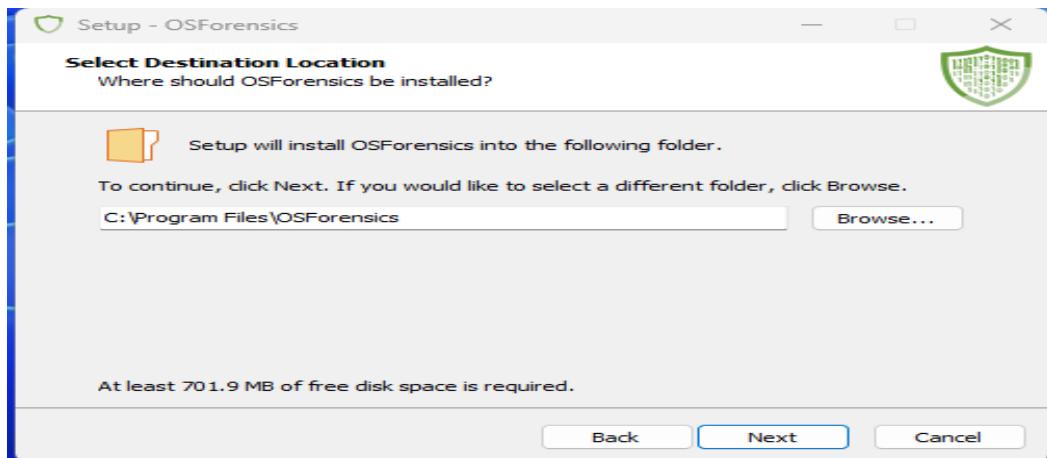
- Import and export of hash sets.
- Customizable system information gathering.
- No limits on the number of cases being managed through OS Forensics.
- Restoration of multiple deleted files in one operation.
- List and search for alternate file streams.
- Sort image files by color.
- Disk indexing and 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.

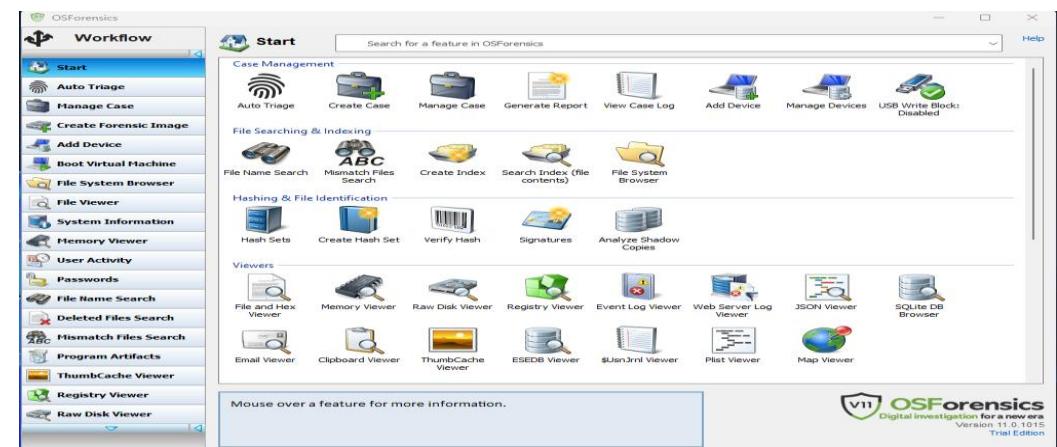
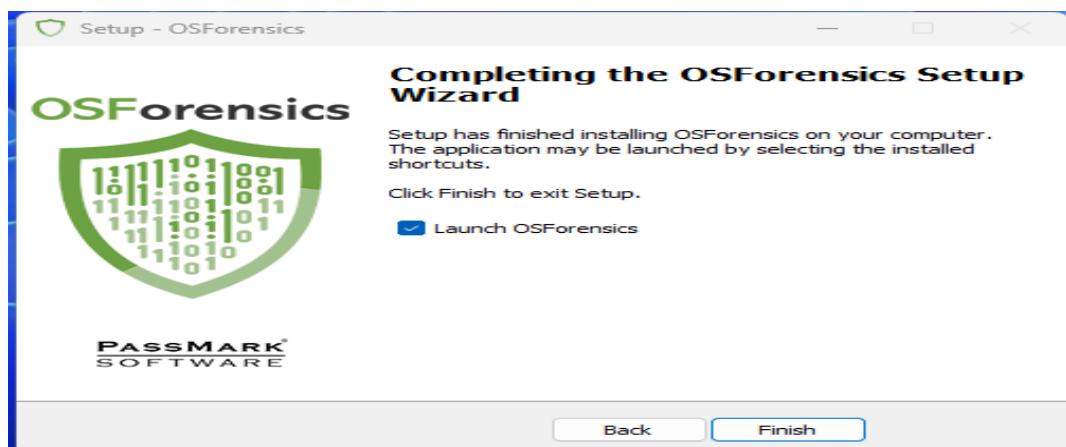
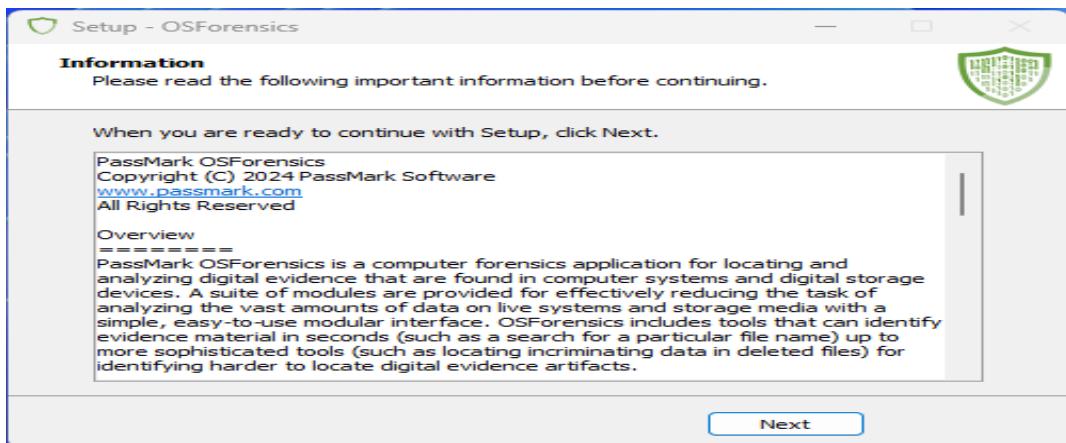
### Code/Demo & Output/Steps:

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

### Installing OS Forensics tool







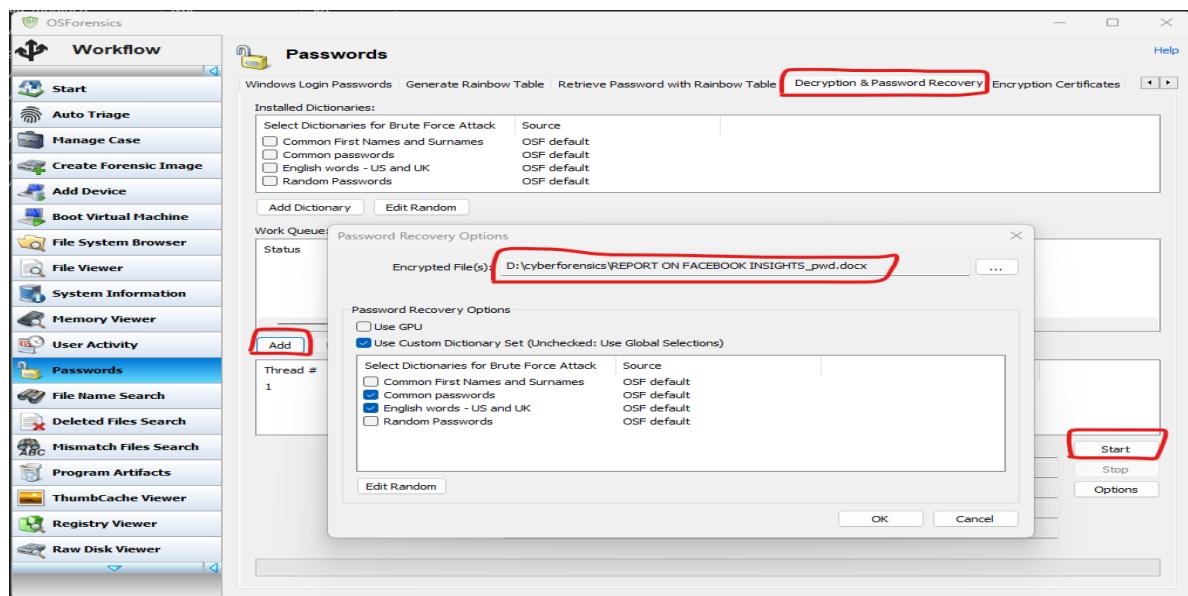
After Successfully installing OS Forensics this kind of interface should be display on your system. OS Forensics supports two methods of gaining access to encrypted office documents.

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

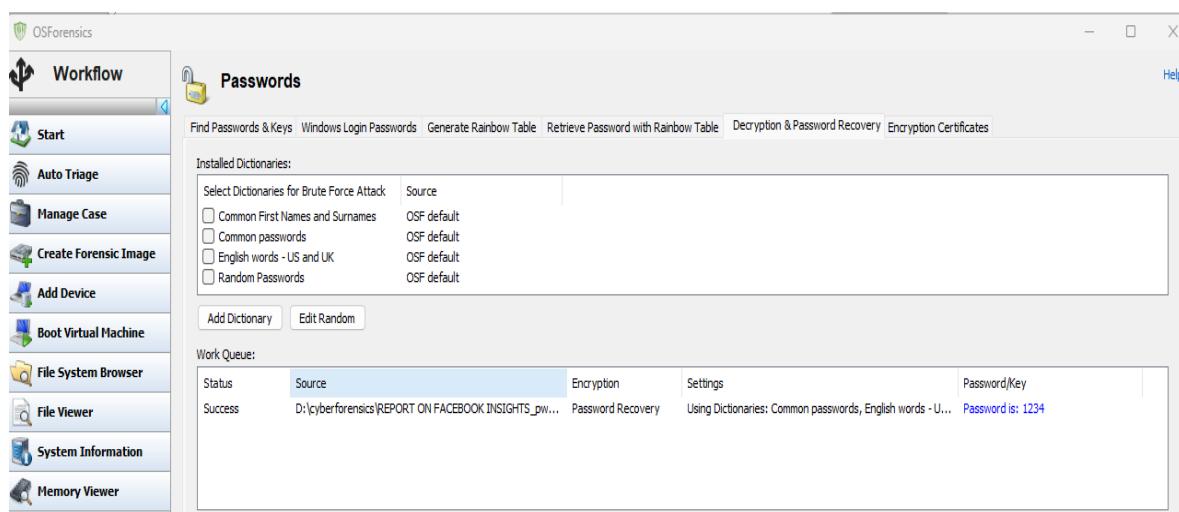
## 1.Password -> Decryption & Password recovery



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

Add -> Select password Protected file -> select predefined 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

OSForensics™ scans your system for evidence of recent activity, such as active wireless networks, recent downloads, website logins and [website passwords](#), identifying trends and patterns of the user, and any material or accounts which recently

**3. User activities to Scan Whole System**

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.

| Item                      | Activity Type | User                      | Time                 | Time Source           | Flags |
|---------------------------|---------------|---------------------------|----------------------|-----------------------|-------|
| conversation-small-nr...  | Downloads     | S-1-5-21-1585417697-83... | 1/14/2025, 11:31:45  | Date Download Started |       |
| root\In754b.css           | Downloads     | S-1-5-21-1585417697-83... | 1/14/2025, 11:31:45  | Date Download Started |       |
| practical_1HTML Repo...   | Recycle Bin   | S-1-5-21-1585417697-83... | 1/11/2025, 14:53:18  | Date Deleted          |       |
| practical_1Excel Repo...  | Recycle Bin   | S-1-5-21-1585417697-83... | 1/11/2025, 14:53:18  | Date Deleted          |       |
| SY (1).zip                | Downloads     |                           | 12/13/2024, 10:34:27 | Date Download Started |       |
| Minutes of the Meetin...  | Downloads     |                           | 12/13/2024, 10:34:27 | Date Download Started |       |
| sample__superstore.xls    | Downloads     |                           | 11/21/2024, 13:55:51 | Date Download Started |       |
| 6.29-N-M.Sc-IT-1_0...     | Downloads     |                           | 7/6/2024, 10:59:07   | Date Download Started |       |
| microservice-architect... | Downloads     |                           | 7/6/2024, 10:58:56   | Date Download Started |       |
| university of mumbai_...  | Downloads     |                           | 7/6/2024, 10:55:08   | Date Download Started |       |
| Unit 4 Chap 1.pptx        | Downloads     |                           | 7/6/2024, 10:55:00   | Date Download Started |       |
| Unit 3 Chap 3 Number...   | Downloads     |                           | 7/6/2024, 10:54:56   | Date Download Started |       |
| Unit 2 Chap 4-Modern...   | Downloads     |                           | 7/6/2024, 10:54:48   | Date Download Started |       |
| Unit 2 Chap 3-Modern...   | Downloads     |                           | 7/6/2024, 10:54:45   | Date Download Started |       |
| Unit 2 Chap 2-Modern...   | Downloads     |                           | 7/6/2024, 10:54:38   | Date Download Started |       |
| Unit 2 Chap 1-Modem...    | Downloads     |                           | 7/6/2024, 10:54:37   | Date Download Started |       |
| Unit 2 Chap 3 SDN Co...   | Downloads     |                           | 7/6/2024, 10:54:32   | Date Download Started |       |
| Unit 2 Chap 1 SDN Bac...  | Downloads     |                           | 7/6/2024, 10:54:24   | Date Download Started |       |
| Unit 1 Chap 2 Require...  | Downloads     |                           | 7/6/2024, 10:54:22   | Date Download Started |       |
| Q8_Modern Computer...     | Downloads     |                           | 7/6/2024, 10:54:15   | Date Download Started |       |
| Q8_Modern Computer...     | Downloads     |                           | 7/6/2024, 10:54:13   | Date Download Started |       |
| Q8 all 4 units.docx       | Downloads     |                           | 7/6/2024, 10:54:11   | Date Download Started |       |
| Lec01.pdf                 | Downloads     |                           | 7/6/2024, 10:54:10   | Date Download Started |       |
| MN Q8.pdf                 | Downloads     |                           | 7/6/2024, 10:54:09   | Date Download Started |       |
| 01elements of modern...   | Downloads     |                           | 7/6/2024, 10:54:05   | Date Download Started |       |
| Foundations of Moder...   | Downloads     |                           | 7/6/2024, 10:50:17   | Date Download Started |       |
| Time Series Notes.pdf     | Downloads     |                           | 7/6/2024, 10:46:30   | Date Download Started |       |
| Text Analytics Notes.pdf  | Downloads     |                           | 7/6/2024, 10:46:30   | Date Download Started |       |
| Naive baves Notes.pdf     | Downloads     |                           | 7/6/2024, 10:46:30   | Date Download Started |       |

### 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

A screenshot of the 'New Case Information' dialog box. On the left, a sidebar titled 'Steps' shows '1. Case Information' and '2. Optional Information'. The main area is titled 'Case Information'. It contains fields for 'Case Name' (set to 'practical\_1'), 'Base Directory' (set to 'D:\cyberforensics\'), 'Case Type' (with 'Single-User' selected), and a note that 'Case data will be stored in the following directory: D:\cyberforensics\practical\_1'. At the bottom are buttons for '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'.

**New Case Information**

**Steps**

1. Case Information
2. **Optional Information**

**Optional Information**

**Case**

Number: 001

**Examiner**

Name: Tareeq Esaf  
Phone: 9856585431  
Email: Esaf2132321@gmail.com  
Notes:

**Organization**

Organization analysis is being done for: Not Specified Manage Organization...

< Back Next > **Finish** Cancel Help

**Add Data Source**

**Steps**

1. **Select Host**
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source

**Select Host**

Hosts are used to organize data sources and other data.

Generate new host name based on data source name  
 Specify new host name   
 Use existing host

< Back **Next >** Finish Cancel Help

### Step 3 -Choose the path

**Add Data Source**

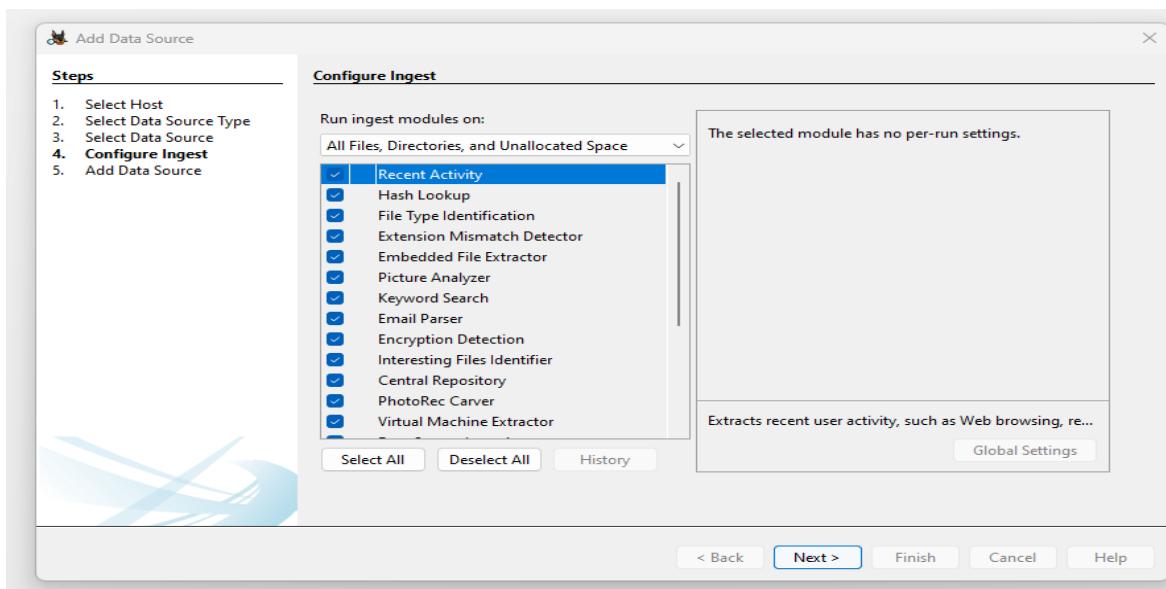
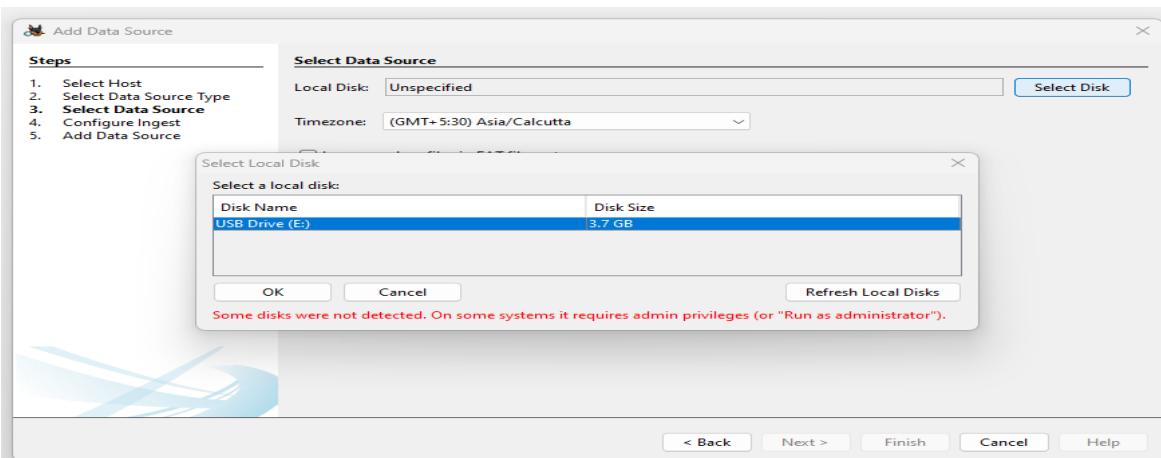
**Steps**

1. Select Host
2. **Select Data Source Type**
3. Select Data Source
4. Configure Ingest
5. Add Data Source

**Select Data Source Type**

- Disk Image or VM File
- Local Disk
- Logical Files
- Unallocated Space Image File
- Autopsy Logical Imager Results
- XRY Text Export

< Back **Next >** Finish Cancel Help



## Step 4 -Retrieve the classified files

| Name                             | S | C | O | Modified Time           | Change Time         | Access Time             | Created Time            | Size  | Flags(Dir)  | Flags(Meta) | Known   | Location                |
|----------------------------------|---|---|---|-------------------------|---------------------|-------------------------|-------------------------|-------|-------------|-------------|---------|-------------------------|
| pic1.jpg.crdownload              |   |   |   | 2023-01-11 14:18:44 IST | 0000-00-00 00:00:00 | 2023-01-11 00:00:00 IST | 2023-01-11 14:18:42 IST | 10133 | Unallocated | Unallocated | unknown | /img_E:/pic1.jpg.crdown |
| pic1.jpg.crdownload              |   |   |   | 2023-01-11 14:19:20 IST | 0000-00-00 00:00:00 | 2023-01-11 00:00:00 IST | 2023-01-11 14:19:19 IST | 14571 | Unallocated | Unallocated | unknown | /img_E:/pic1.jpg.crdown |
| pic1.jpg.crdownload              |   |   |   | 2023-01-11 14:19:30 IST | 0000-00-00 00:00:00 | 2023-01-11 00:00:00 IST | 2023-01-11 14:19:29 IST | 5011  | Unallocated | Unallocated | unknown | /img_E:/pic1.jpg.crdown |
| REPORT ON FACE                   |   |   |   | 2024-12-04 14:59:03 IST | 0000-00-00 00:00:00 | 2025-01-11 00:00:00 IST | 2023-01-11 14:55:15 IST | 9328  | Unallocated | Unallocated | unknown | /img_E:/REPORT ON FA    |
| REPORT ON FACE                   |   |   |   | 2023-01-11 14:16:02 IST | 0000-00-00 00:00:00 | 2023-01-11 00:00:00 IST | 2023-01-11 14:15:54 IST | 1932  | Unallocated | Unallocated | unknown | /img_E:/REPORT ON FA    |
| REPORT ON FACE                   |   |   |   | 2023-01-11 14:16:08 IST | 0000-00-00 00:00:00 | 2023-01-11 00:00:00 IST | 2023-01-11 14:15:54 IST | 19252 | Unallocated | Unallocated | unknown | /img_E:/REPORT ON FA    |
| REPORT ON FACE                   |   |   |   | 2023-01-11 14:16:08 IST | 0000-00-00 00:00:00 | 2023-01-11 00:00:00 IST | 2023-01-11 14:15:54 IST | 19321 | Unallocated | Unallocated | unknown | /img_E:/REPORT ON FA    |
| REPORT ON FACE                   |   |   |   | 2023-01-11 14:16:30 IST | 0000-00-00 00:00:00 | 2023-01-11 00:00:00 IST | 2023-01-11 14:15:54 IST | 19264 | Unallocated | Unallocated | unknown | /img_E:/REPORT ON FA    |
| REPORT ON FACE                   |   |   |   | 2023-01-11 14:17:30 IST | 0000-00-00 00:00:00 | 2023-01-11 00:00:00 IST | 2023-01-11 14:17:28 IST | 0     | Unallocated | Unallocated | unknown | /img_E:/REPORT ON FA    |
| REPORT ON FACE                   |   |   |   | 2023-01-11 14:29:10 IST | 0000-00-00 00:00:00 | 2023-01-11 00:00:00 IST | 2025-01-11 14:29:08 IST | 0     | Unallocated | Unallocated | unknown | /img_E:/New Microsoft   |
| New Microsoft Wo                 |   |   |   | 2023-01-11 14:18:56 IST | 0000-00-00 00:00:00 | 2023-01-11 00:00:00 IST | 2023-01-11 14:18:55 IST | 0     | Unallocated | Unallocated | unknown | /img_E:/New Microsoft   |
| iC1.jpg                          |   |   |   | 2023-01-11 14:18:56 IST | 0000-00-00 00:00:00 | 2023-01-11 00:00:00 IST | 2023-01-11 14:18:55 IST | 0     | Unallocated | Unallocated | unknown | /img_E:/iC1.jpg         |
| iC1.jpg                          |   |   |   | 2023-01-11 14:18:56 IST | 0000-00-00 00:00:00 | 2023-01-11 00:00:00 IST | 2023-01-11 14:18:55 IST | 0     | Unallocated | Unallocated | unknown | /img_E:/iC1.jpg         |
| Screenshot 2024-1-               |   |   |   | 2024-12-21 14:40:24 IST | 0000-00-00 00:00:00 | 2023-01-11 00:00:00 IST | 2023-01-11 14:25:57 IST | 37359 | Unallocated | Unallocated | unknown | /img_E:/Screenshot 202  |
| Screenshot 2024-12-21 144040.png |   |   |   | 2024-12-21 14:40:42 IST | 0000-00-00 00:00:00 | 2023-01-11 00:00:00 IST | 2025-01-11 14:25:57 IST | 39160 | Unallocated | Unallocated | unknown | /img_E:/Screenshot 202  |
| Screenshot 2024-12-21 144059.png |   |   |   | 2024-12-21 14:40:59 IST | 0000-00-00 00:00:00 | 2023-01-11 00:00:00 IST | 2023-01-11 14:25:57 IST | 35823 | Unallocated | Unallocated | unknown | /img_E:/Screenshot 202  |
| Screenshot 2024-12-21 145111.png |   |   |   | 2024-12-21 14:51:12 IST | 0000-00-00 00:00:00 | 2023-01-11 00:00:00 IST | 2023-01-11 14:25:57 IST | 9958  | Unallocated | Unallocated | unknown | /img_E:/Screenshot 202  |
| Screenshot 2025-01-08 150904.PNG |   |   |   | 2025-01-08 15:09:04 IST | 0000-00-00 00:00:00 | 2023-01-11 00:00:00 IST | 2023-01-11 14:25:57 IST | 79441 | Unallocated | Unallocated | unknown | /img_E:/Screenshot 202  |
| WRN00001.mnn                     |   |   |   | 2025-01-11 14:16:02 IST | 0000-00-00 00:00:00 | 2025-01-11 00:00:00 IST | 2025-01-11 14:15:54 IST | 19739 | Unallocated | Unallocated | unknown | /img_F:/WRN00001.mnn    |

practical\_1 - Autopsy 4.21.0

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

**Listing** Encryption Detected Table Thumbnail Summary

Source Name: REPORT ON FACEBOOK INSIGHTS.pwd.docx S: 0 C: 0 O: 0 Source Type: File Score: Notable Conclusion: Configuration: Justification: Comment: Password protection detected. File Path: /img\_E/REPORT ON FACEBOOK INSIGHTS.pwd.docx

Save Table as CSV Keyword Lists 1 Results

**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

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

**Listing** Encryption Detected Table Thumbnail Summary

Source Name: REPORT ON FACEBOOK INSIGHTS.pwd.docx S: 0 C: 0 O: 0 Source Type: File Score: Notable Conclusion: Configuration: Justification: Password protection detected. Comment: Password protection detected. File Path: /img\_E/REPORT ON FACI

**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

| A  | B                       | C                       | D               | E                     | F       | G  | H           | I | J | K | L | M | N | O | P | Q | R | S | T | U |
|----|-------------------------|-------------------------|-----------------|-----------------------|---------|--|-------------|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1  | Date Created            | Date Modified           | Owner           | Program Name          | User ID | Version  | Source File |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 2  | 2024-12-04 09:02:00 IST | 2024-12-04 09:02:00 IST | Admin           | Microsoft Office Word | Admin   | /img_E/ScavengedFiles/1/00000000.docx              |             |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 3  | 2024-12-04 09:02:00 IST | 2024-12-04 09:02:00 IST | Admin           | Microsoft Office Word | Admin   | /img_E/REPORT ON FACEBOOK INSIGHTS.docx            |             |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 4  | 2024-12-04 09:02:00 IST | 2024-12-04 09:02:00 IST | Admin           | Microsoft Office Word | Admin   | /img_E/_WRLD0001.tmp                               |             |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 5  | 2024-12-04 09:02:00 IST | 2023-01-11 08:46:00 IST | Admin           | Microsoft Office Word | Admin   | /img_E/ScavengedFiles/1/0000040.docx               |             |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 6  | 2024-12-04 09:02:00 IST | 2023-01-11 08:46:00 IST | Admin           | Microsoft Office Word | Admin   | /img_E/ScavengedFiles/1/0000080.docx               |             |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 7  | 2024-12-04 09:02:00 IST | 2023-01-11 08:46:00 IST | Admin           | Microsoft Office Word | Admin   | /img_E/ScavengedFiles/1/0000128.docx               |             |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 8  | 2024-12-04 09:02:00 IST | 2023-01-11 08:46:00 IST | Admin           | Microsoft Office Word | Admin   | /img_E/REPORT ON FACEBOOK INSIGHTS.docx            |             |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 9  | 2024-12-04 09:02:00 IST | 2023-01-11 08:46:00 IST | Admin           | Microsoft Office Word | Admin   | /img_E/REPORT ON FACEBOOK INSIGHTS.docx            |             |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 10 | 2024-12-04 09:02:00 IST | 2023-01-11 08:46:00 IST | Admin           | Microsoft Office Word | Admin   | /img_E/REPORT ON FACEBOOK INSIGHTS.docx            |             |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 11 | 2024-12-04 09:02:00 IST | 2023-01-11 08:46:00 IST | Admin           | Microsoft Office Word | Admin   | /img_E/_WRLD0002.tmp                               |             |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 12 | 2024-12-04 09:02:00 IST | 2023-01-11 08:46:00 IST | Admin           | Microsoft Office Word | Admin   | /img_E/_WRLD0003.tmp                               |             |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 13 | 2024-12-04 09:02:00 IST | 2023-01-11 08:46:00 IST | Admin           | Microsoft Office Word | Admin   | /img_E/_WRLD0002.tmp                               |             |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 14 | 2024-12-04 09:02:00 IST | 2023-01-11 08:46:00 IST | Admin           | Microsoft Office Word | Admin   | /img_E/_WRLD0003.tmp                               |             |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 15 | 2024-12-04 09:02:00 IST | 2023-01-11 08:46:00 IST | Admin           | Microsoft Office Word | Admin   | /img_E/_WRLD0005.tmp                               |             |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 16 | 2024-12-20 09:57:47 IST | 2024-12-20 09:57:47 IST | Neha Vora       |                       |         | /img_E/1 Analysis of Data Source Using Autopsy.pdf |             |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 17 | 2024-12-21 09:55:16 IST | 2024-12-21 09:55:16 IST | Neha Vora       |                       |         | /img_E/2 Cyber Forensics Tools.pdf                 |             |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 18 | 2024-12-24 04:58:00 IST | 2024-12-24 04:58:00 IST | Jhanvi Upadhyay | Microsoft Office Word | Admin   | /img_E/3 JAVA_PROJECT.docx                         |             |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 19 |                         |                         |                 |                       |         |  |             |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 20 |                         |                         |                 |                       |         |  |             |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 21 |                         |                         |                 |                       |         |  |             |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 22 |                         |                         |                 |                       |         |  |             |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 23 |                         |                         |                 |                       |         |  |             |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 24 |                         |                         |                 |                       |         |  |             |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 25 |                         |                         |                 |                       |         |  |             |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 26 |                         |                         |                 |                       |         |  |             |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 27 |                         |                         |                 |                       |         |  |             |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 28 |                         |                         |                 |                       |         |  |             |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 29 |                         |                         |                 |                       |         |  |             |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 30 |                         |                         |                 |                       |         |  |             |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 31 |                         |                         |                 |                       |         |  |             |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 32 |                         |                         |                 |                       |         |  |             |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 33 |                         |                         |                 |                       |         |  |             |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 34 |                         |                         |                 |                       |         |  |             |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 35 |                         |                         |                 |                       |         |  |             |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 36 |                         |                         |                 |                       |         |  |             |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 37 |                         |                         |                 |                       |         |  |             |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 38 |                         |                         |                 |                       |         |  |             |   |   |   |   |   |   |   |   |   |   |   |   |   |

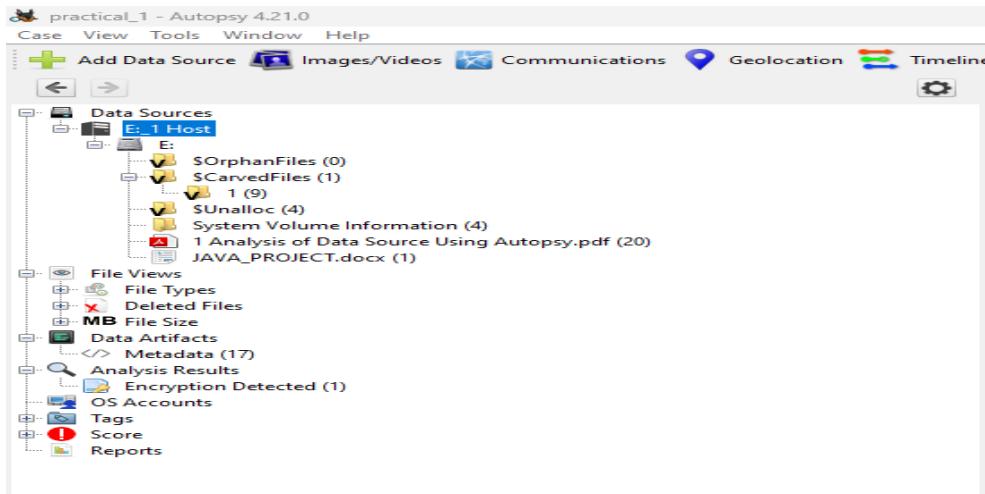
### 3. Exploring the data source:

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.

| Name      | Type       | Size (Bytes) | Sector Size (Bytes) | Timezone      | Device ID                            |
|-----------|------------|--------------|---------------------|---------------|--------------------------------------|
| E:\ Image | 4013917184 | 512          |                     | Asia/Calcutta | 1a8f2c30-8c99-4664-a386-70d20253d3fe |

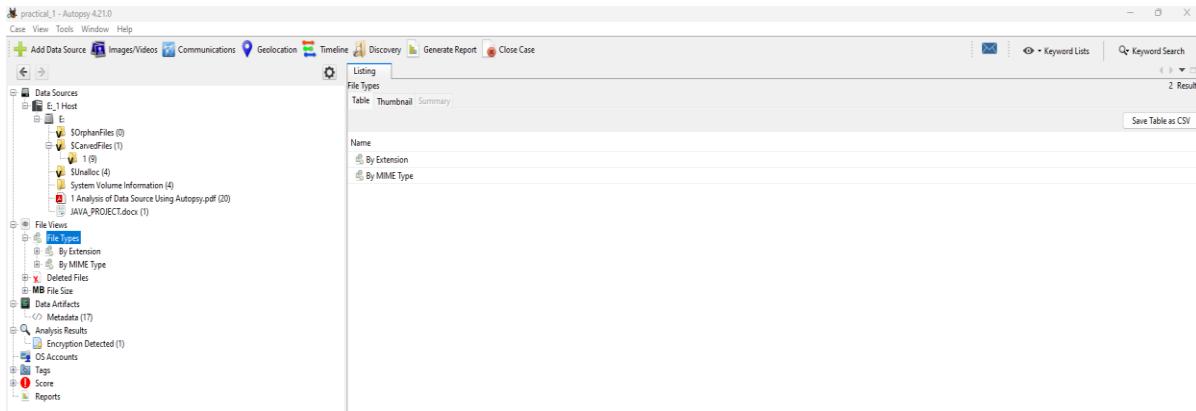
The disk image is then broken down based upon its partitions.



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.

| Name                             | S | C | O | Modified Time           | Change Time         | Access Time             | Created Time            | Size  | Flags(Dir)  | Flags(Meta) | Known   | Location              |
|----------------------------------|---|---|---|-------------------------|---------------------|-------------------------|-------------------------|-------|-------------|-------------|---------|-----------------------|
| pic1.jpg.crdownload              |   |   |   | 2025-01-11 14:18:44 IST | 0000-00-00 00:00:00 | 2025-01-11 00:00:00 IST | 2025-01-11 14:18:42 IST | 10133 | Unallocated | Unallocated | unknown | /img_E/pic1.jpg.crdow |
| pic1.jpg.crdownload0             |   |   |   | 2025-01-11 14:18:30 IST | 0000-00-00 00:00:00 | 2025-01-11 00:00:00 IST | 2025-01-11 14:18:29 IST | 14571 | Unallocated | Unallocated | unknown | /img_E/pic1.jpg.crdow |
| pic1.jpg.crdownload1             |   |   |   | 2025-01-11 14:18:30 IST | 0000-00-00 00:00:00 | 2025-01-11 00:00:00 IST | 2025-01-11 14:18:29 IST | 5011  | Unallocated | Unallocated | unknown | /img_E/pic1.jpg.crdow |
| REPORT ON FA CEE                 |   |   |   | 2024-12-04 14:23:02 IST | 0000-00-00 00:00:00 | 2024-01-11 00:00:00 IST | 2024-01-11 14:18:54 IST | 19238 | Unallocated | Unallocated | unknown | /img_E/REPORT ON FA   |
| REPORT ON FACE                   |   |   |   | 2025-01-11 14:18:02 IST | 0000-00-00 00:00:00 | 2025-01-11 00:00:00 IST | 2025-01-11 14:18:54 IST | 19352 | Unallocated | Unallocated | unknown | /img_E/REPORT ON FA   |
| REPORT ON FACE                   |   |   |   | 2025-01-11 14:18:08 IST | 0000-00-00 00:00:00 | 2025-01-11 00:00:00 IST | 2025-01-11 14:18:54 IST | 19252 | Unallocated | Unallocated | unknown | /img_E/REPORT ON FA   |
| REPORT ON FACE                   |   |   |   | 2025-01-11 14:18:08 IST | 0000-00-00 00:00:00 | 2025-01-11 00:00:00 IST | 2025-01-11 14:18:54 IST | 19321 | Unallocated | Unallocated | unknown | /img_E/REPORT ON FA   |
| REPORT ON FACE                   |   |   |   | 2025-01-11 14:18:30 IST | 0000-00-00 00:00:00 | 2025-01-11 00:00:00 IST | 2025-01-11 14:18:54 IST | 19264 | Unallocated | Unallocated | unknown | /img_E/REPORT ON FA   |
| New Microsoft Wo                 |   |   |   | 2025-01-11 14:17:30 IST | 0000-00-00 00:00:00 | 2025-01-11 00:00:00 IST | 2025-01-11 14:17:29 IST | 0     | Unallocated | Unallocated | unknown | /img_E/New Microsoft  |
| j1c1.jpg                         |   |   |   | 2025-01-11 14:18:56 IST | 0000-00-00 00:00:00 | 2025-01-11 00:00:00 IST | 2025-01-11 14:18:55 IST | 0     | Unallocated | Unallocated | unknown | /img_E/j1c1.jpg       |
| j1c1.jpg                         |   |   |   | 2025-01-11 14:18:56 IST | 0000-00-00 00:00:00 | 2025-01-11 00:00:00 IST | 2025-01-11 14:18:53 IST | 0     | Unallocated | Unallocated | unknown | /img_E/j1c1.jpg       |
| j1c1.jpg                         |   |   |   | 2025-01-11 14:18:56 IST | 0000-00-00 00:00:00 | 2025-01-11 00:00:00 IST | 2025-01-11 14:18:53 IST | 0     | Unallocated | Unallocated | unknown | /img_E/j1c1.jpg       |
| Screenshot 2024-1-               |   |   |   | 2025-01-11 14:18:24 IST | 0000-00-00 00:00:00 | 2025-01-11 00:00:00 IST | 2025-01-11 14:18:23 IST | 0     | Unallocated | Unallocated | unknown | /img_E/Screenshot 202 |
| Screenshot 2024-12-21 14040.png  |   |   |   | 2025-01-11 14:18:34 IST | 0000-00-00 00:00:00 | 2025-01-11 00:00:00 IST | 2025-01-11 14:18:33 IST | 0     | Unallocated | Unallocated | unknown | /img_E/Screenshot 202 |
| Screenshot 2024-12-21 140407.png |   |   |   | 2024-12-21 14:04:02 IST | 0000-00-00 00:00:00 | 2025-01-11 00:00:00 IST | 2025-01-11 14:22:57 IST | 37359 | Unallocated | Unallocated | unknown | /img_E/Screenshot 202 |
| Screenshot 2024-12-21 140538.png |   |   |   | 2024-12-21 14:04:02 IST | 0000-00-00 00:00:00 | 2025-01-11 00:00:00 IST | 2025-01-11 14:22:57 IST | 35823 | Unallocated | Unallocated | unknown | /img_E/Screenshot 202 |
| Screenshot 2024-12-21 145111.png |   |   |   | 2024-12-21 14:51:12 IST | 0000-00-00 00:00:00 | 2025-01-11 00:00:00 IST | 2025-01-11 14:22:57 IST | 9958  | Unallocated | Unallocated | unknown | /img_E/Screenshot 202 |
| Screenshot 2024-01-08 115903.png |   |   |   | 2025-01-08 11:59:04 IST | 0000-00-00 00:00:00 | 2025-01-11 00:00:00 IST | 2025-01-11 14:22:57 IST | 79441 | Unallocated | Unallocated | unknown | /img_E/Screenshot 202 |
| WR000000ms                       |   |   |   | 2025-01-11 14:18:07 IST | 0000-00-00 00:00:00 | 2025-01-11 00:00:00 IST | 2025-01-11 14:18:04 IST | 10130 | Unallocated | Unallocated | unknown | /img_E/WR000000ms     |

- **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.

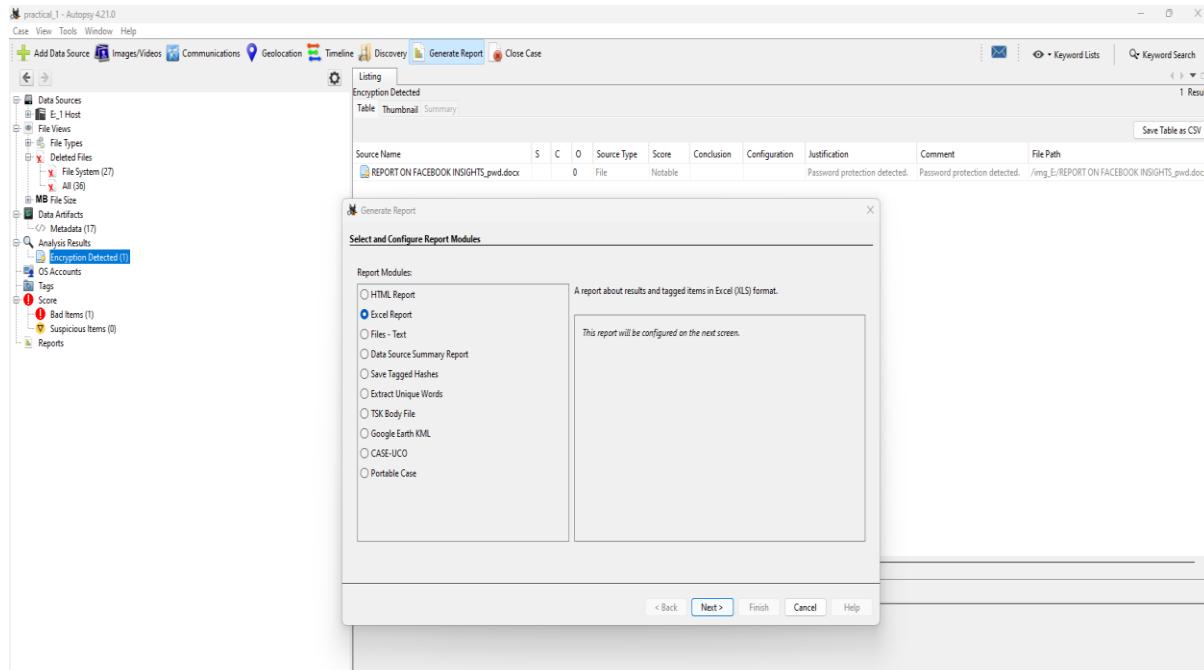
- **EXIF Metadata:** It contains all the .jpg images that have EXIF Metadata associated with them, this Metadata can be analyzed further.

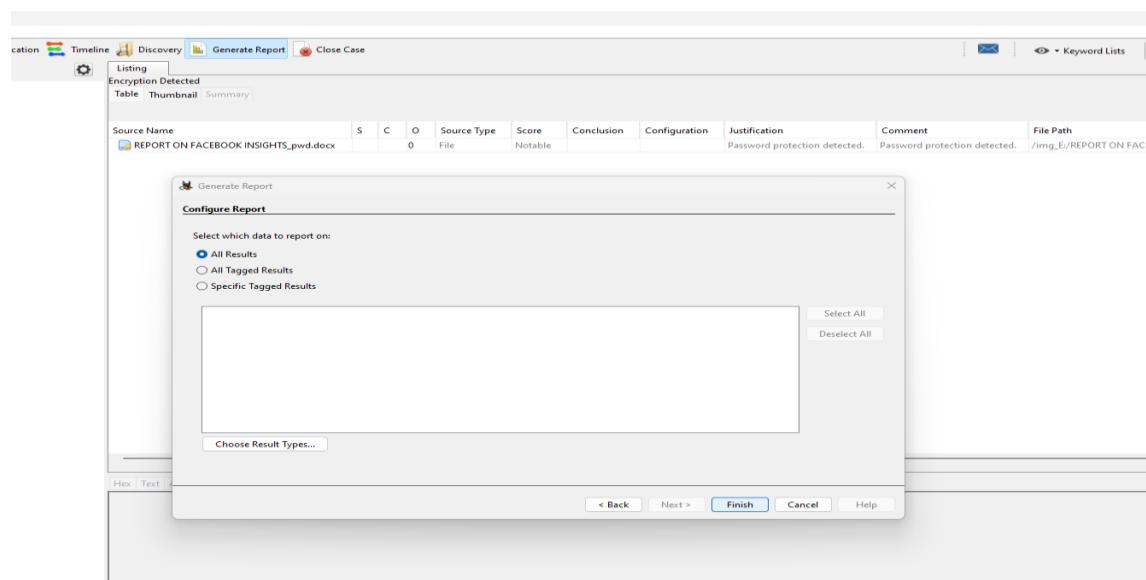
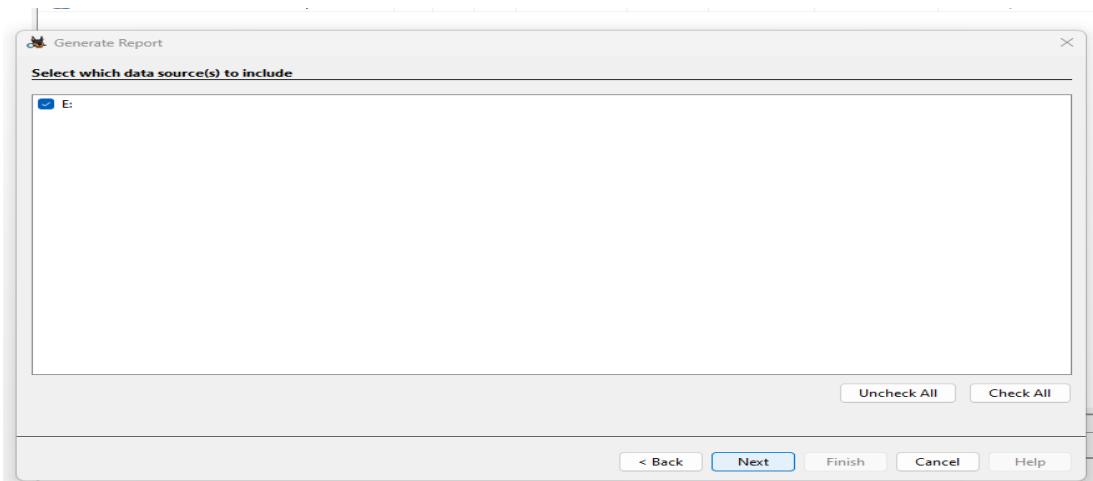
- **Encryption Detection:** It detects files that are password protected/ encrypted.

| 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 |

- **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.

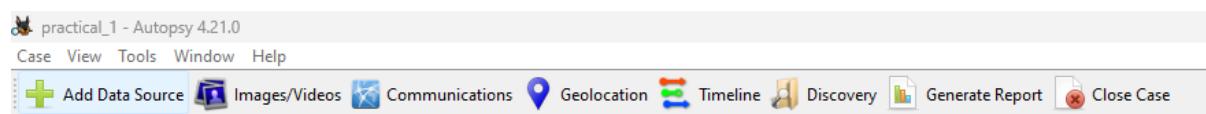




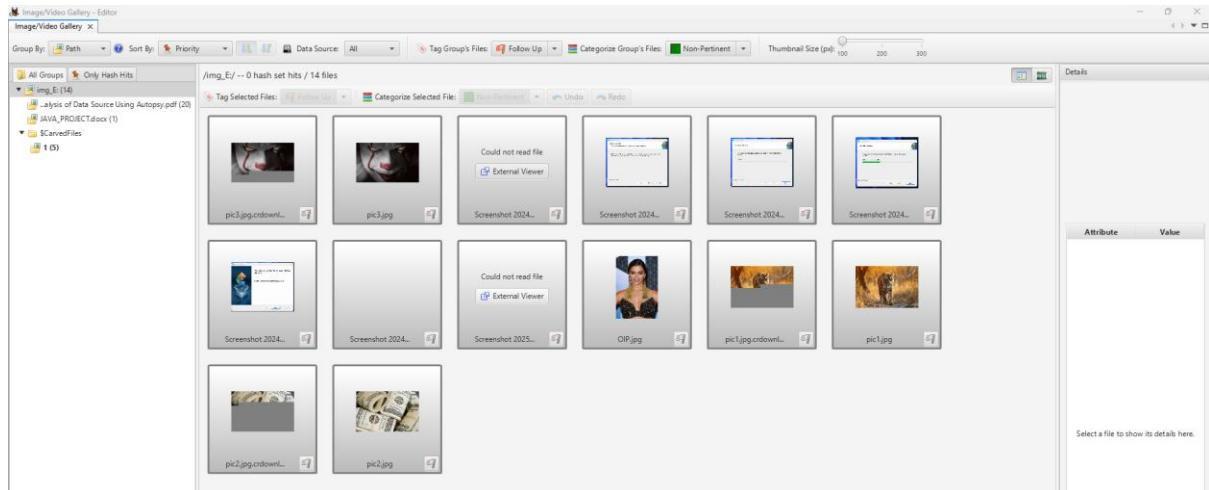
Excel.xlsx - Excel

|    | A                       | B                       | C               | D                     | E       | F   | G           | H    | I | J | K | L | M | N | O | P | Q | R | S | T | U |
|----|-------------------------|-------------------------|-----------------|-----------------------|---------|---|-------------|------|---|---|---|---|---|---|---|---|---|---|---|---|---|
|    | Date Created            | Date Modified           | Owner           | Program Name          | User ID | Version   | Source File | Tags |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 1  | 2024-12-04 09:02:00 IST | 2024-12-04 09:02:00 IST | Admin           | Microsoft Office Word | Admin   | /img_E/_CarvedFiles/1/f0000000.docx               |             |      |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 2  | 2024-12-04 09:02:00 IST | 2024-12-04 09:02:00 IST | Admin           | Microsoft Office Word | Admin   | /img_E/_REPORT ON FACEBOOK INSIGHTS.docx          |             |      |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 3  | 2024-12-04 09:02:00 IST | 2024-12-04 09:02:00 IST | Admin           | Microsoft Office Word | Admin   | /img_E/_WR00001.ms                                |             |      |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 4  | 2024-12-04 09:02:00 IST | 2024-12-04 09:02:00 IST | Admin           | Microsoft Office Word | Admin   | /img_E/_WR00002.ms                                |             |      |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 5  | 2024-12-04 09:02:00 IST | 2024-12-11 08:46:00 IST | Admin           | Microsoft Office Word | Admin   | /img_E/_CarvedFiles/1/f0000040.docx               |             |      |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 6  | 2024-12-04 09:02:00 IST | 2024-12-11 08:46:00 IST | Admin           | Microsoft Office Word | Admin   | /img_E/_CarvedFiles/1/f0000080.docx               |             |      |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 7  | 2024-12-04 09:02:00 IST | 2024-12-11 08:46:00 IST | Admin           | Microsoft Office Word | Admin   | /img_E/_CarvedFiles/1/f0000128.docx               |             |      |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 8  | 2024-12-04 09:02:00 IST | 2024-12-11 08:46:00 IST | Admin           | Microsoft Office Word | Admin   | /img_E/_REPORT ON FACEBOOK INSIGHTS.docx          |             |      |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 9  | 2024-12-04 09:02:00 IST | 2024-12-11 08:46:00 IST | Admin           | Microsoft Office Word | Admin   | /img_E/_REPORT ON FACEBOOK INSIGHTS.docx          |             |      |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 10 | 2024-12-04 09:02:00 IST | 2024-12-11 08:46:00 IST | Admin           | Microsoft Office Word | Admin   | /img_E/_WR00001.ms                                |             |      |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 11 | 2024-12-04 09:02:00 IST | 2024-12-11 08:46:00 IST | Admin           | Microsoft Office Word | Admin   | /img_E/_WR00002.ms                                |             |      |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 12 | 2024-12-04 09:02:00 IST | 2024-12-11 08:46:00 IST | Admin           | Microsoft Office Word | Admin   | /img_E/_WR00003.ms                                |             |      |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 13 | 2024-12-04 09:02:00 IST | 2024-12-11 08:46:00 IST | Admin           | Microsoft Office Word | Admin   | /img_E/_WR00004.ms                                |             |      |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 14 | 2024-12-04 09:02:00 IST | 2024-12-11 08:46:00 IST | Admin           | Microsoft Office Word | Admin   | /img_E/_WR00005.ms                                |             |      |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 15 | 2024-12-04 09:02:00 IST | 2024-12-11 08:46:00 IST | Admin           | Microsoft Office Word | Admin   | /img_E/_WR00006.ms                                |             |      |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 16 | 2024-12-20 09:57:47 IST | 2024-12-20 09:57:47 IST | Neha Vora       | Microsoft Office Word | Admin   | /img_E/_Analysis of Data Source Using Autopsy.pdf |             |      |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 17 | 2024-12-21 06:55:16 IST | 2024-12-21 06:55:16 IST | Neha Vora       | Microsoft Office Word | Admin   | /img_E/_Cyber Forensics Tools.pdf                 |             |      |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 18 | 2024-12-24 04:58:00 IST | 2024-12-24 04:58:00 IST | Jhanvi Upadhyay | Microsoft Office Word | Admin   | /img_E/_JAVA_PROJECT.docx                         |             |      |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 19 |                         |                         |                 |                       |         |   |             |      |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 20 |                         |                         |                 |                       |         |   |             |      |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 21 |                         |                         |                 |                       |         |   |             |      |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 22 |                         |                         |                 |                       |         |   |             |      |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 23 |                         |                         |                 |                       |         |   |             |      |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 24 |                         |                         |                 |                       |         |   |             |      |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 25 |                         |                         |                 |                       |         |   |             |      |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 26 |                         |                         |                 |                       |         |   |             |      |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 27 |                         |                         |                 |                       |         |   |             |      |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 28 |                         |                         |                 |                       |         |   |             |      |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 29 |                         |                         |                 |                       |         |   |             |      |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 30 |                         |                         |                 |                       |         |   |             |      |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 31 |                         |                         |                 |                       |         |   |             |      |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 32 |                         |                         |                 |                       |         |   |             |      |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 33 |                         |                         |                 |                       |         |   |             |      |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 34 |                         |                         |                 |                       |         |   |             |      |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 35 |                         |                         |                 |                       |         |   |             |      |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 36 |                         |                         |                 |                       |         |   |             |      |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 37 |                         |                         |                 |                       |         |   |             |      |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 38 |                         |                         |                 |                       |         |   |             |      |   |   |   |   |   |   |   |   |   |   |   |   |   |

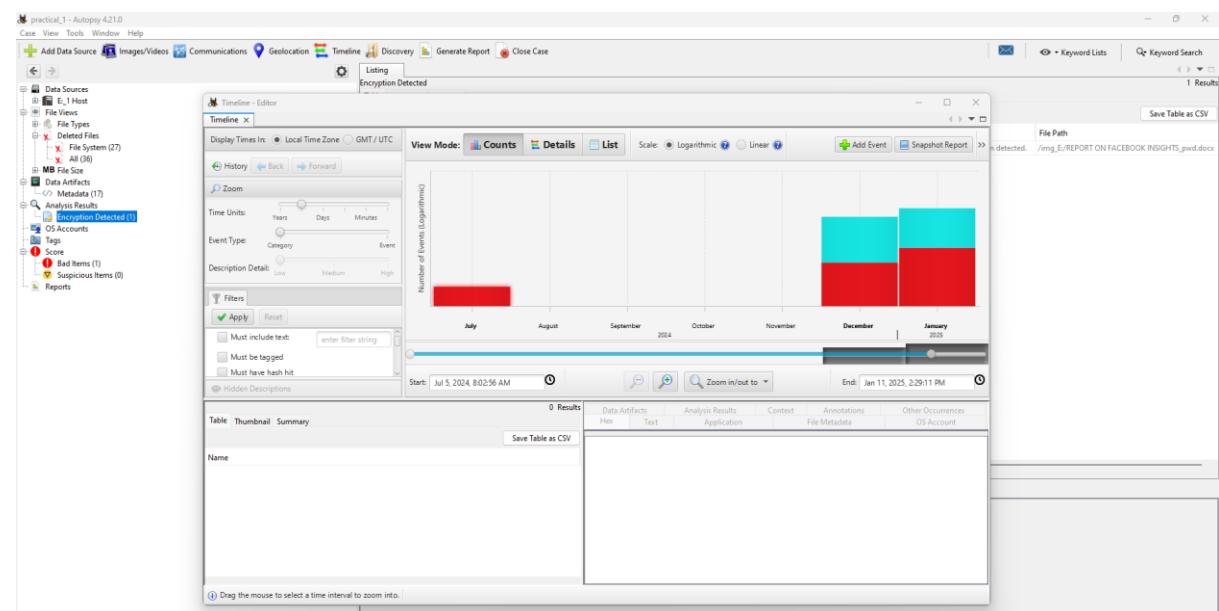
## Additional Features:



- **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 of a Hard Drive has occurred. This is usually performed by law enforcement for court because, after a 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.

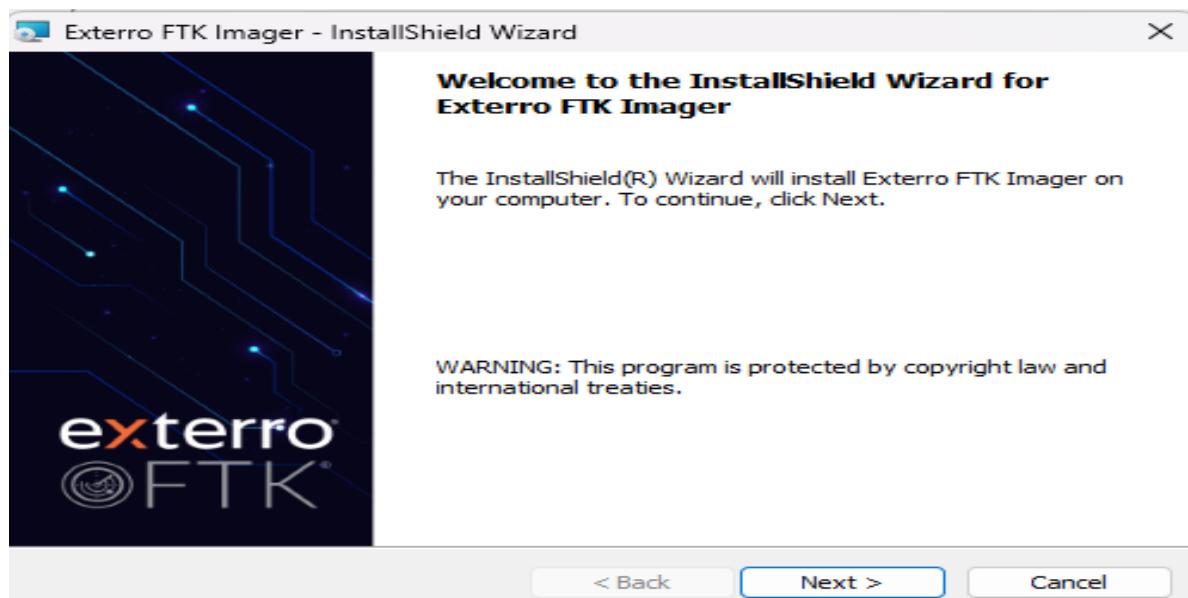
#### What Is FTK Imager?

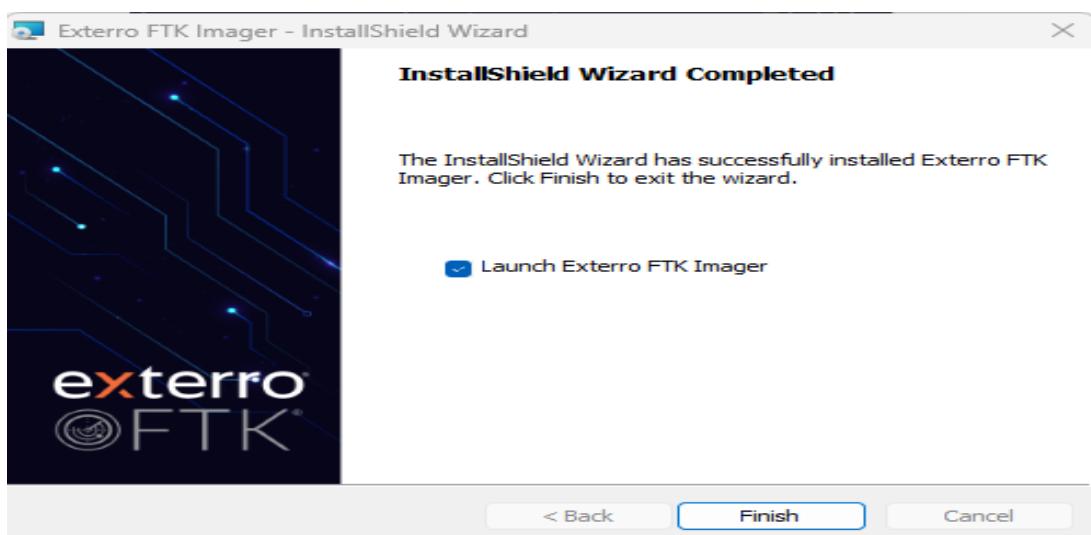
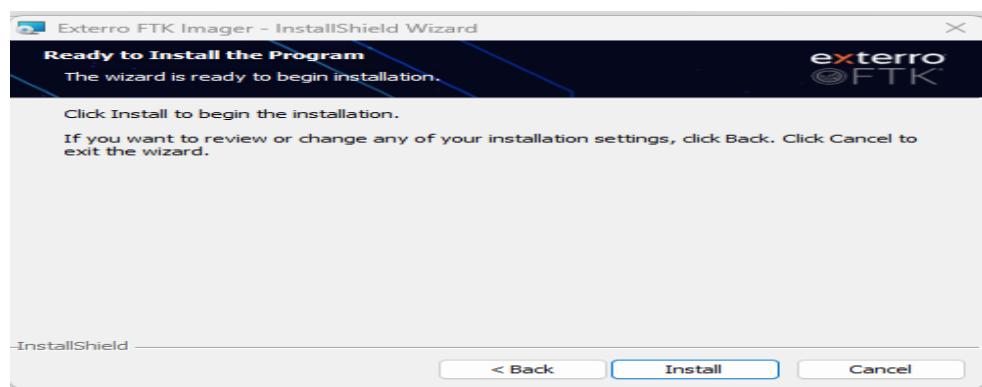
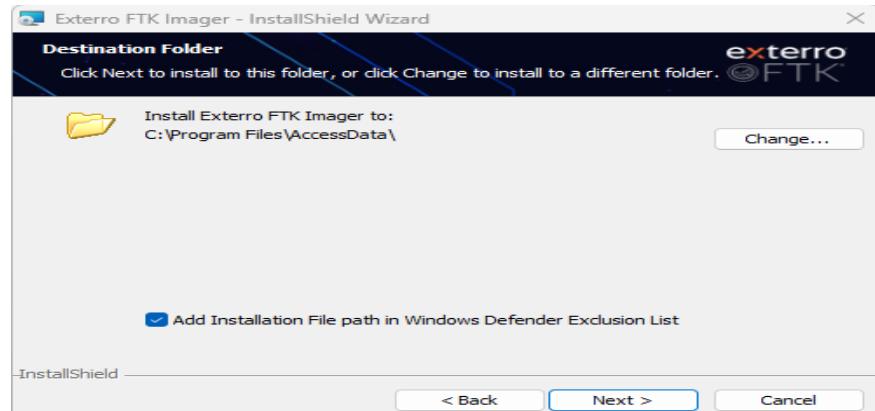
FTK Imager is a tool for creating disk images and is absolutely free to use. It was developed by The Access Data Group. It is a tool that helps to preview data and for imaging.

With FTK Imager, you can:

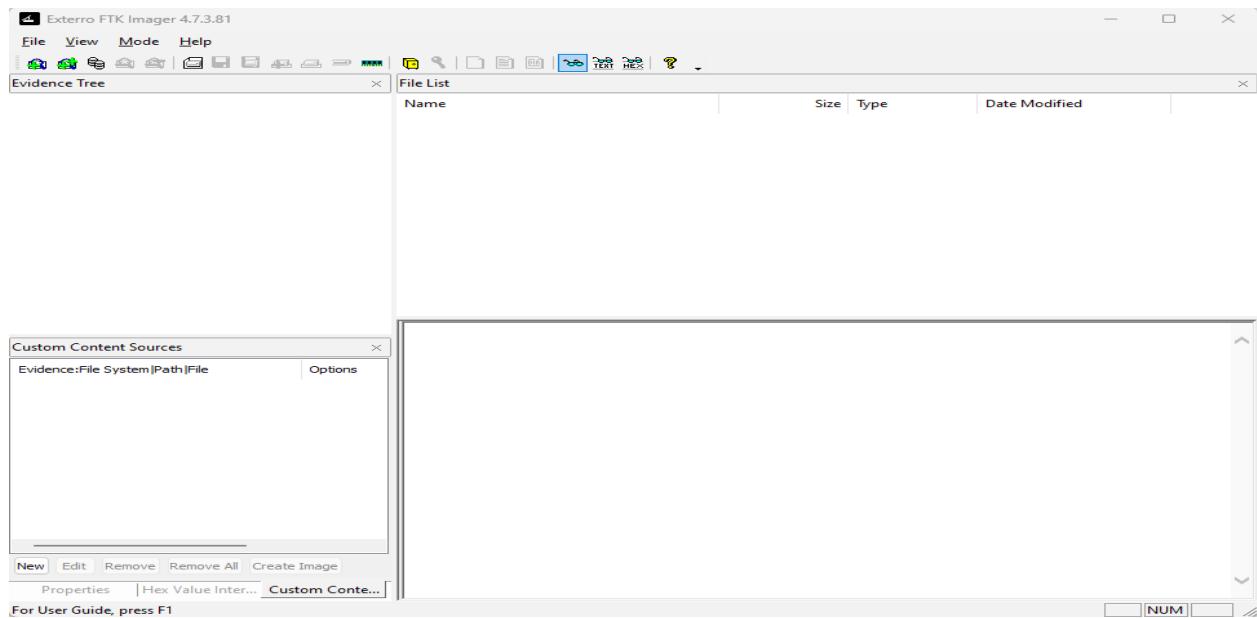
Create forensic images or perfect copies of local hard drives, floppy and Zip disks, DVDs, folders, individual files, etc. without making changes to the original evidence. Preview files and folders on local hard drives, network drives, floppy diskettes, Zip disks, CDs, and DVDs.

#### Step 1: Installing FTK Imager

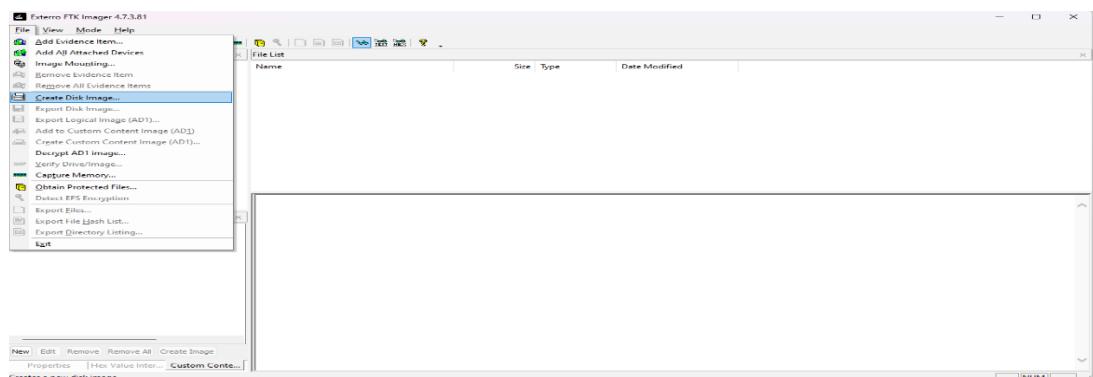




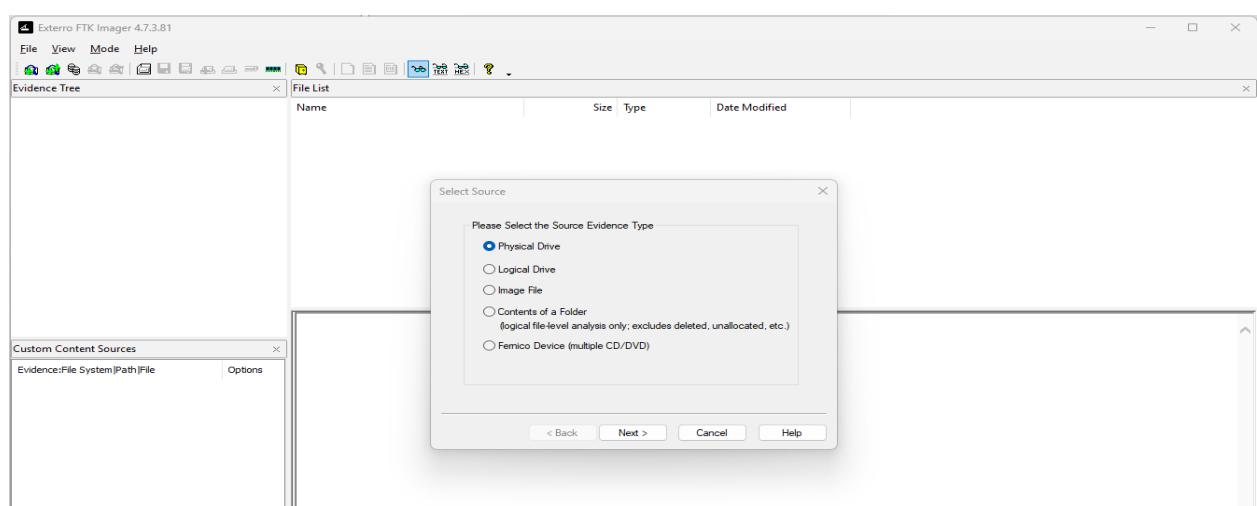
## Step 2: Open the Access Data FTK Imager.



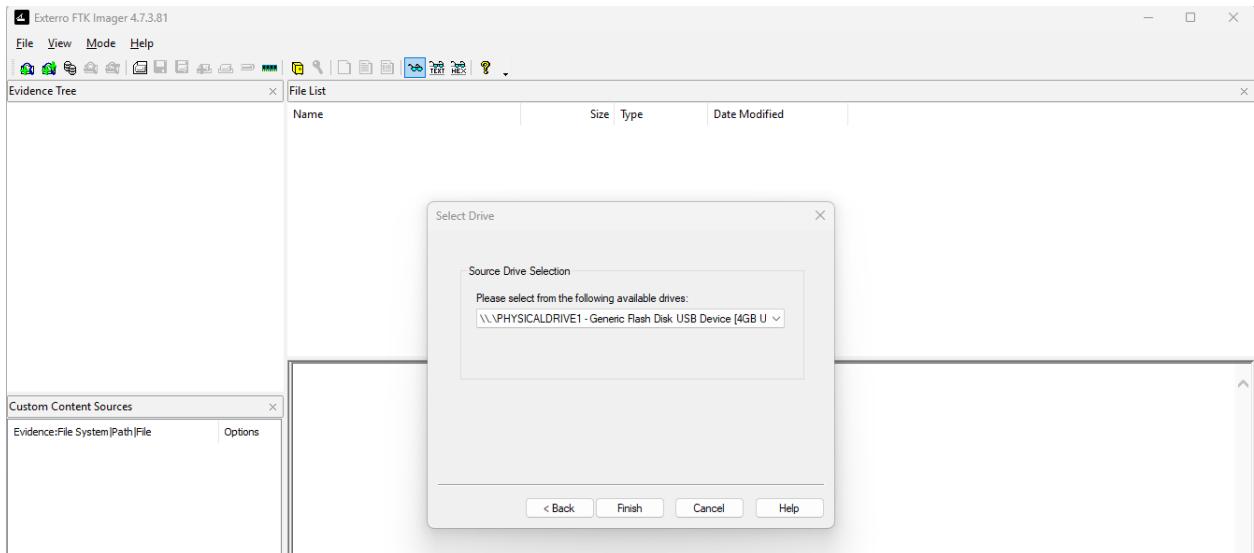
## Step 3: Click File, and then Create Disk Image, or click the button on the tool bar.



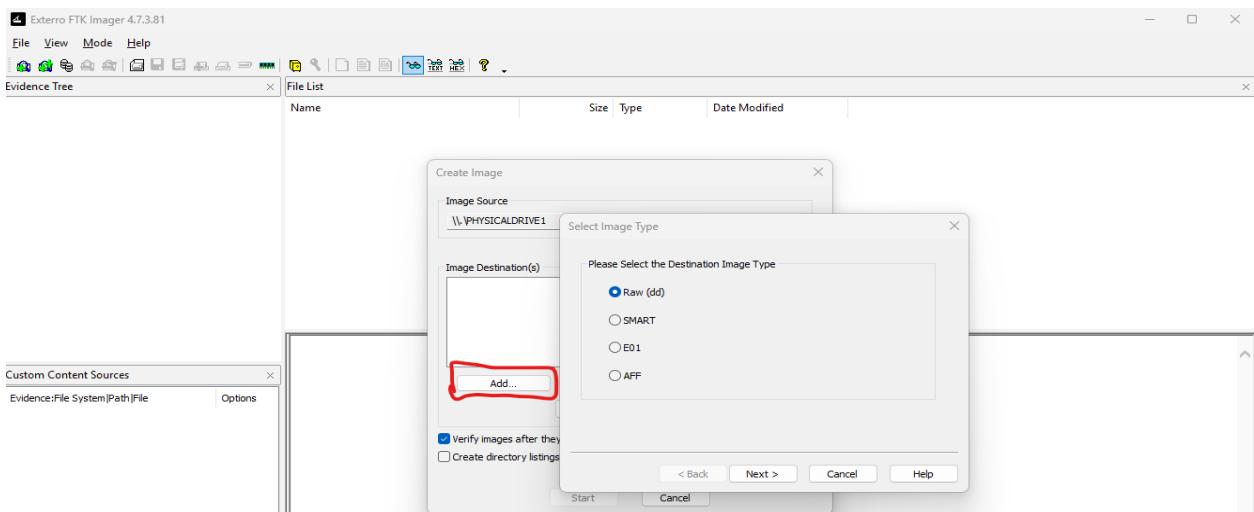
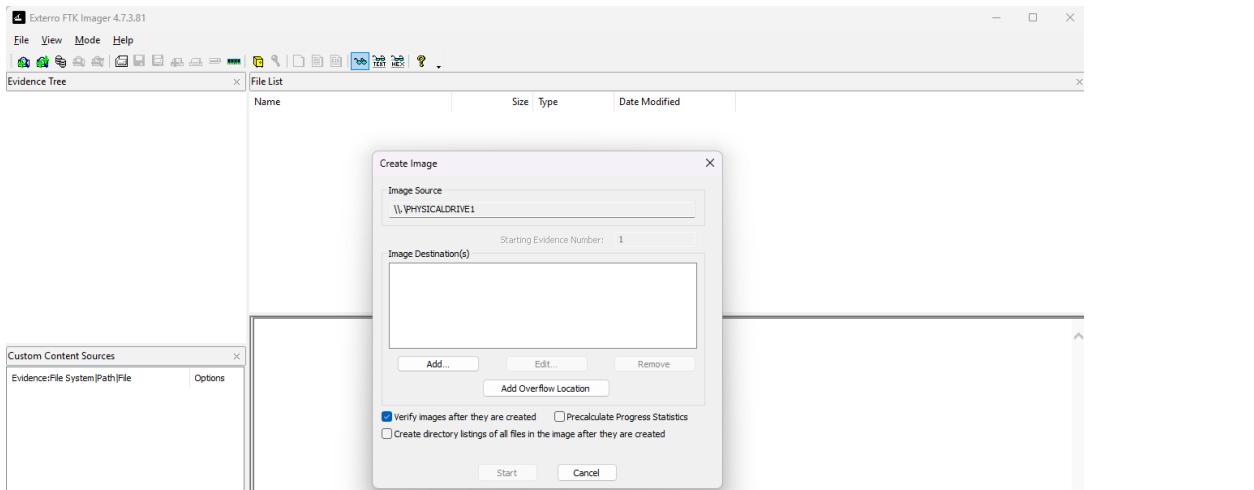
## Step 4: Select the source evidence type you want to make an image of and click Next.

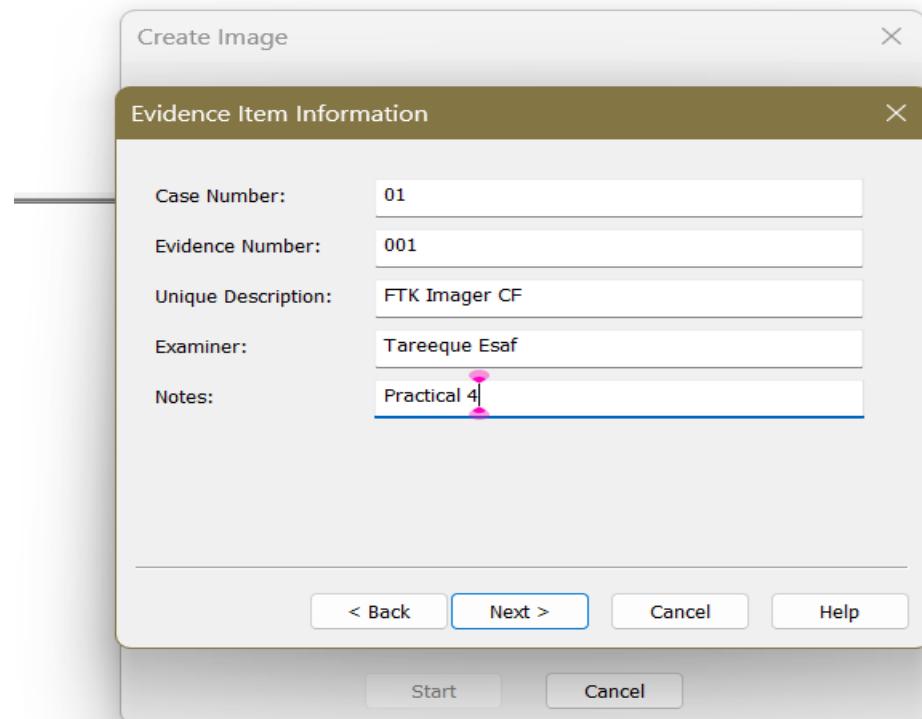


## Step 5: Select the source evidence file with path.



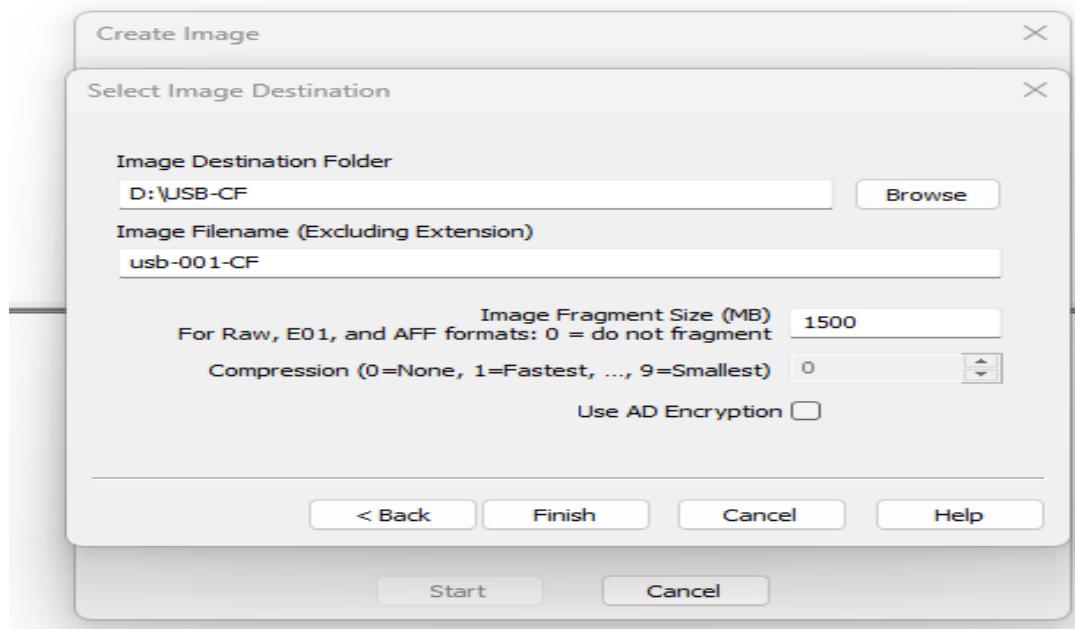
## Step 6: Click on “add” to add image destination

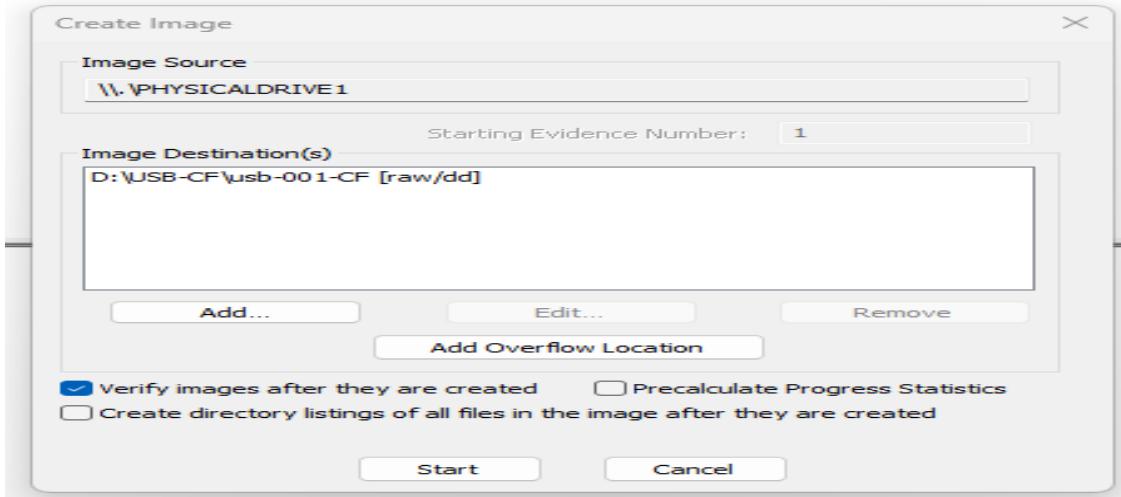




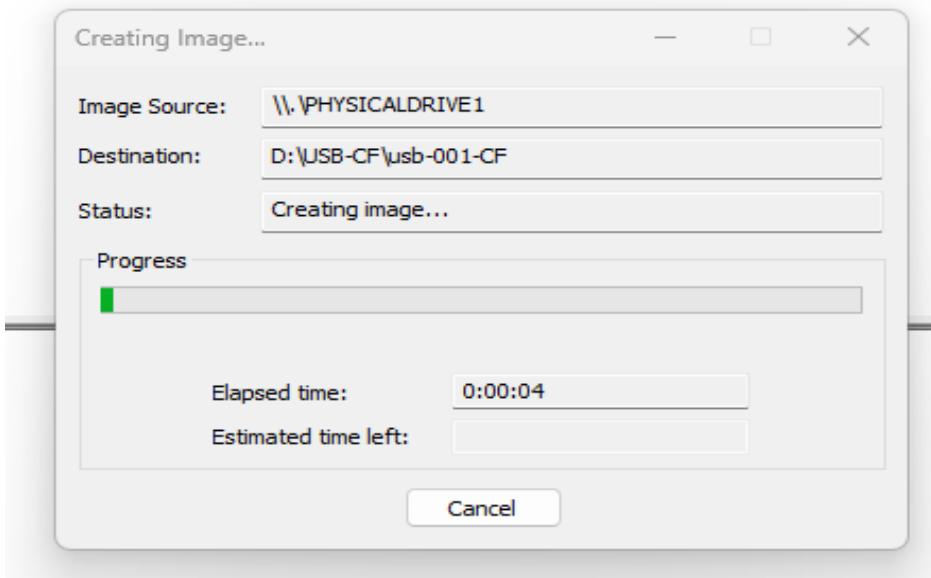
In the Image Destination Folder field, type the location path where you want to save the image file, or click **Browse** to find to the desired location.

**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.



| Drive/Image Verify Results |  |
|----------------------------|--|
| Name                       | usb-001-CF.001                           |
| Sector count               | 7866368                                  |
| MD5 Hash                   |  |
| Computed hash              | ca62d9e56f04f832931886e9a54bd650         |
| Report Hash                | ca62d9e56f04f832931886e9a54bd650         |
| Verify result              | Match                                    |
| SHA1 Hash                  |  |
| Computed hash              | fe2b11d03b8d92ce94b4159a562808c3303235c8 |
| Report Hash                | fe2b11d03b8d92ce94b4159a562808c3303235c8 |
| Verify result              | Match                                    |
| Bad Blocks List            |  |
| Bad block(s) in image      | No bad blocks found in image             |

**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

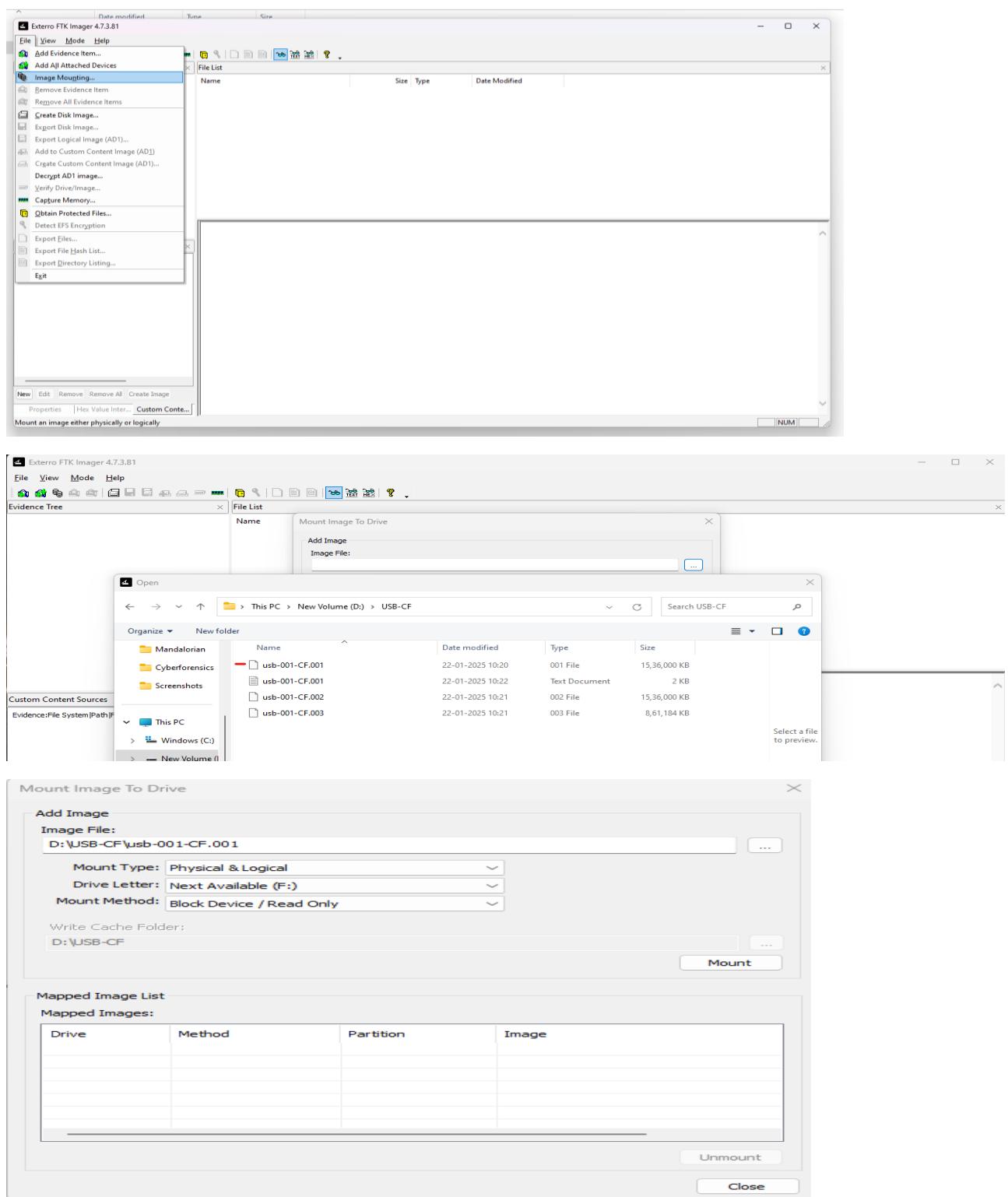
-----
Information for D:\USB-CF\usb-001-CF:

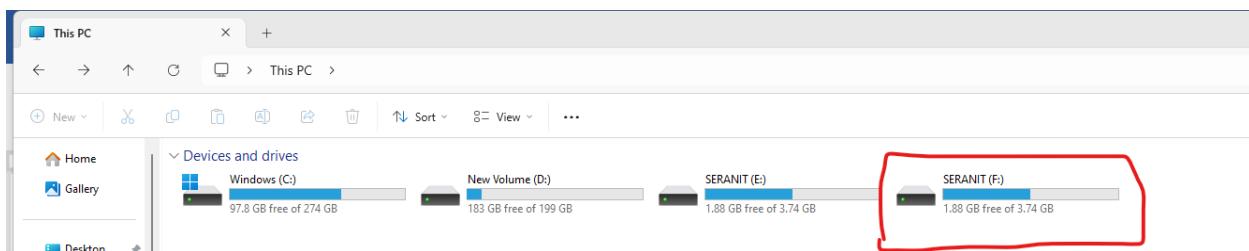
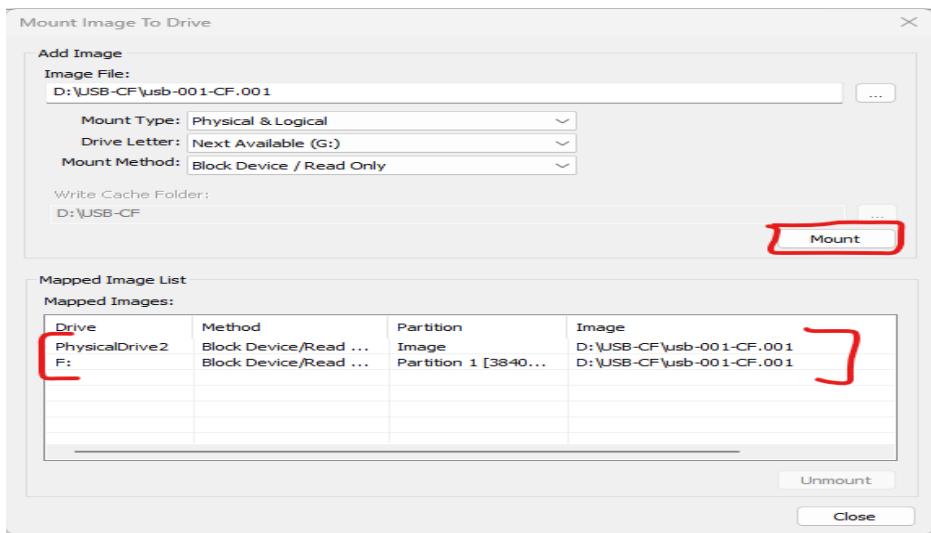
Physical Evidentiary Item (Source) Information:
[Device Info]
Source Type: Physical
[Drive Geometry]
Cylinders: 489
Tracks per Cylinder: 255
Sectors per Track: 63
Bytes per Sector: 512
Sector Count: 7,866,368
[Physical Drive Information]
Drive Model: Generic Flash Disk USB Device
Drive Serial Number: 00
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

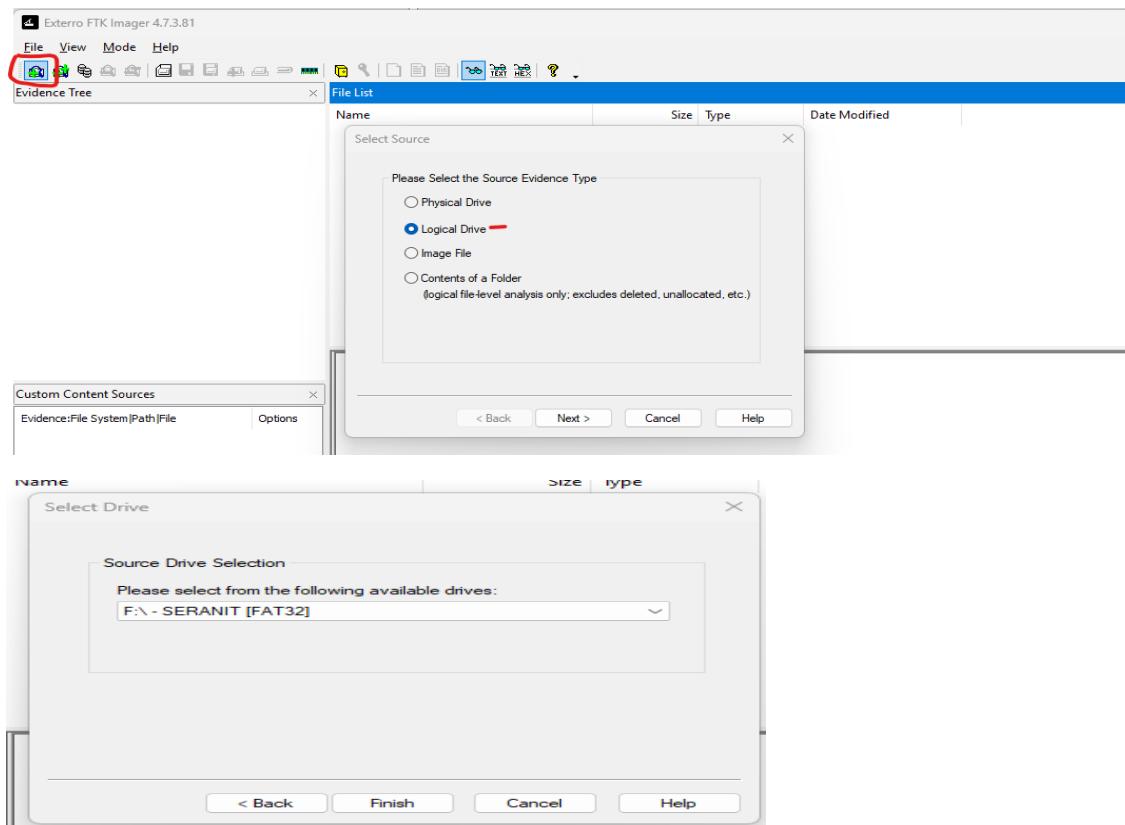
Image Verification Results:
Verification started: Wed Jan 22 10:21:54 2025
Verification finished: Wed Jan 22 10:22:03 2025
MD5 checksum: ca62d9e56f04f832931886e9a54bd650 : verified
SHA1 checksum: fe2b11d03b8d92ce94b4159a562808c3303235c8 : verified
```

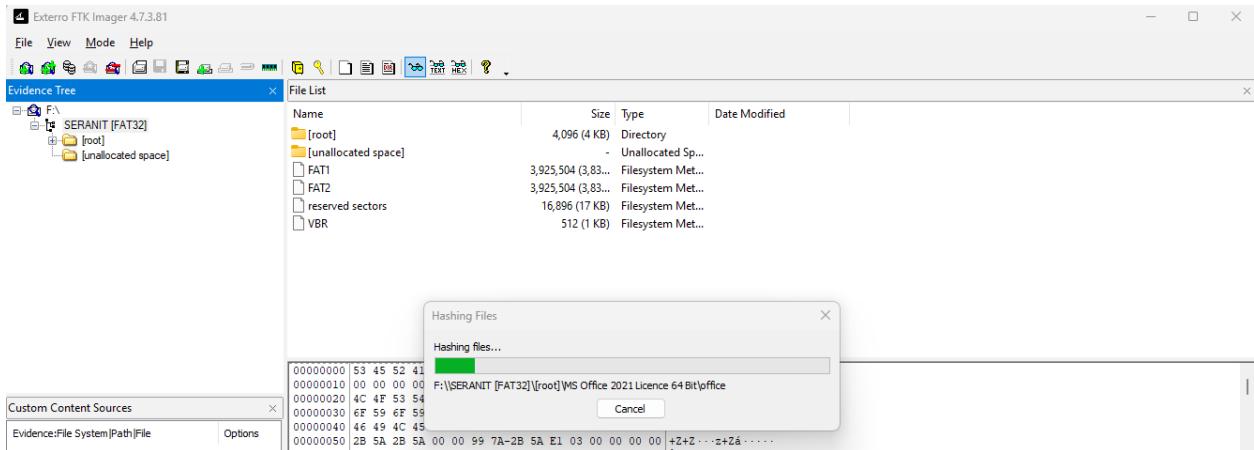
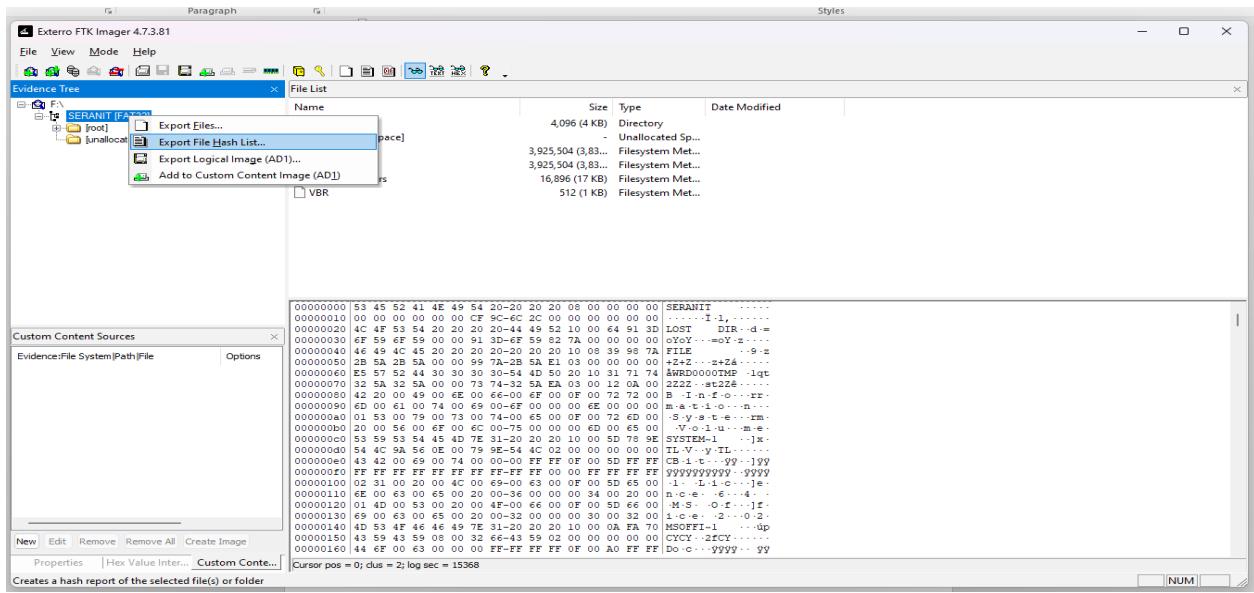
## Step 9: Image mounting





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



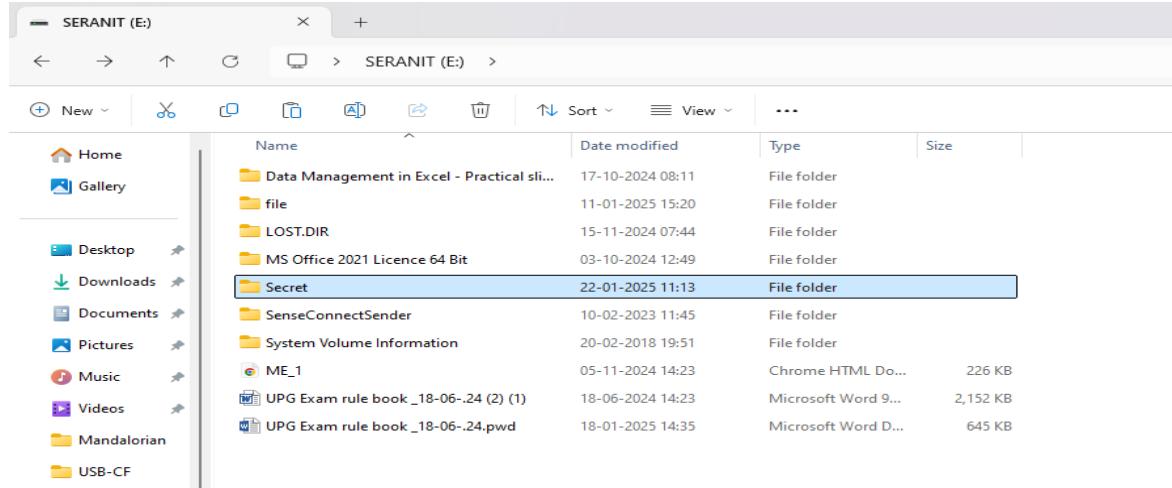


practical 4 hashfiles - Excel

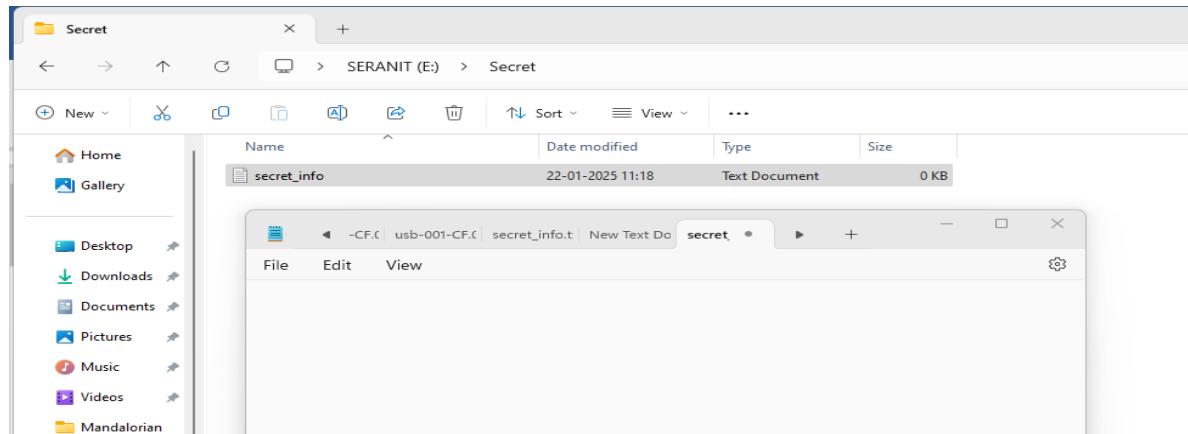
|    | A                                 | B                                 | C  | D | E |
|----|-----------------------------------|-----------------------------------|--|---|---|
| 1  | MD5                               | SHA1                              | FileNames  |   |   |
| 2  | d41d8cd98f00b204e9800998ecf8427e  | da39a3ee5e6b4b0d3255bfef9560189C  | F:\SERANIT [FAT32]\[root]\!WRD0000.TMP   |   |   |
| 3  | 67686a99a828279a40abc29f8820a25a  | ed3368706806769069207649d98f47fb  | F:\SERANIT [FAT32]\[root]\System Volume Information\IndexerVolumeGuid  |   |   |
| 4  | 5f1b88ff8e71a2615531347aae8e10a6  | aab70fedfd0cd76cc92ae19b9819dec3  | F:\SERANIT [FAT32]\[root]\System Volume Information\WPSettings.dat   |   |   |
| 5  | d41d8cd98f00b204e9800998ecf8427e  | da39a3ee5e6b4b0d3255bfef9560189C  | F:\SERANIT [FAT32]\[root]\MS Office 2021 Licence 64 Bit\DS_Store   |   |   |
| 6  | f240057ba1c66de022672375faac2d43  | c63040685023e41df67b1d0f042b83    | F:\SERANIT [FAT32]\[root]\MS Office 2021 Licence 64 Bit\office tool\CD Key.txt                               |   |   |
| 7  | f78234922b70d03b04d1c1e94cdeebbd  | cb83ade2e2158c4b72e8dd7bfeefb9d   | F:\SERANIT [FAT32]\[root]\MS Office 2021 Licence 64 Bit\office tool\configuration-Office2019Enterprise.xml   |   |   |
| 8  | e1b1da611e2cb790e70a7cf595c71b19  | d4f2b2993c2d7ab8f3bd568291d4946   | F:\SERANIT [FAT32]\[root]\MS Office 2021 Licence 64 Bit\office tool\configuration-Office2021Enterprise.xml   |   |   |
| 9  | cc56ec903d72bb5dee368ccdeb6bd4a   | 9cd181cb29e499cfa826b9e69cbcd30e  | 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  | d7d854516c822964517b72aa1841c4    | F:\SERANIT [FAT32]\[root]\MS Office 2021 Licence 64 Bit\office tool\Installation Command.txt                 |   |   |
| 12 | 133800da193da14b538577b2a5f39d0   | 7135c3dd9c43d9d323c16f4323eeaa2   | F:\SERANIT [FAT32]\[root]\MS Office 2021 Licence 64 Bit\office tool\Office_Deployment_Tools_2021_MLF_        |   |   |
| 13 | 5674a4c265f3d910221c2769e5964c2fb | 51456f884f1151546736f6a5a8eb3e3c  | F:\SERANIT [FAT32]\[root]\MS Office 2021 Licence 64 Bit\office tool\setup.exe                                |   |   |
| 14 | 3fbf34f7ebbbf7ba42134b15e3f5bf8   | ad7c5e8bf9f087b3ef7f979f83ce59b1a | F:\SERANIT [FAT32]\[root]\MS Office 2021 Licence 64 Bit\office tool\Office\Data\v64.cab                      |   |   |
| 15 | 3fbf34f7ebbbf7ba42134b15e3f5bf8   | ad7c5e8bf9f087b3ef7f979f83ce59b1a | F:\SERANIT [FAT32]\[root]\MS Office 2021 Licence 64 Bit\office tool\Office\Data\v64_16.0.14332.20400.cab     |   |   |
| 16 | ee178426d0d0717fa8bcdfa32146335   | f3821123ba087f9af7e37258d2d20bc   | F:\SERANIT [FAT32]\[root]\MS Office 2021 Licence 64 Bit\office tool\Office\Data\v64.16.0.14332.20400\640.cab |   |   |
| 17 | 7e2adfc477cfe1347bf7fecac734hh40f | 0c189a2r03426c7daa485ff1079498250 | F:\SERANIT [FAT32]\[root]\MS Office 2021 Licence 64 Bit\office tool\Office\Data\v64.16.0.14332.20400\640.cab |   |   |

## B) Encryption detection using FTK imager

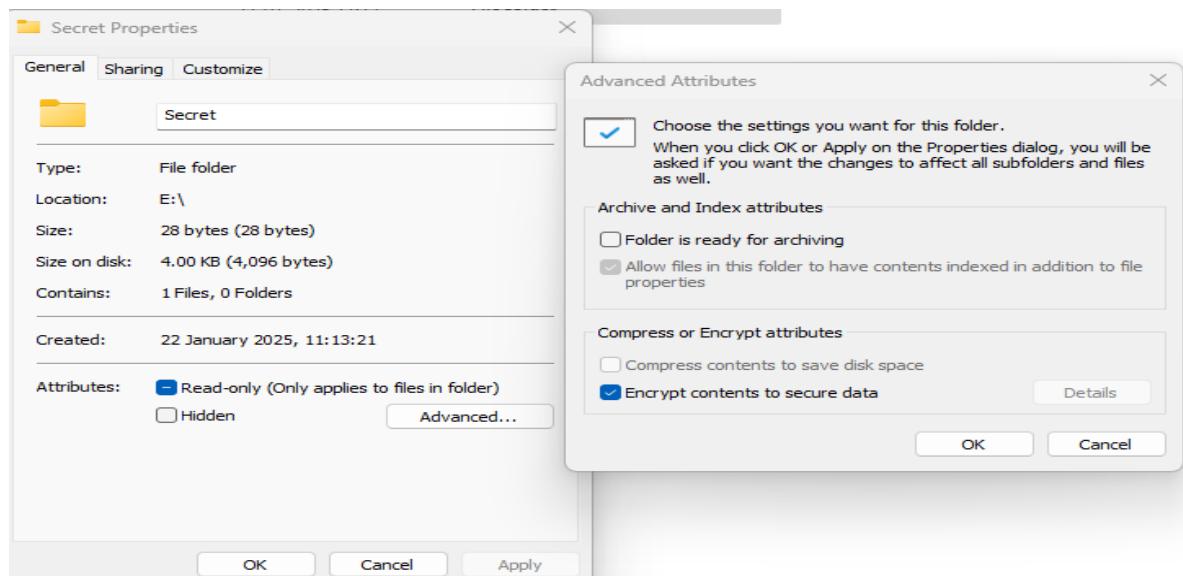
### Step 1: Create a folder name Secret

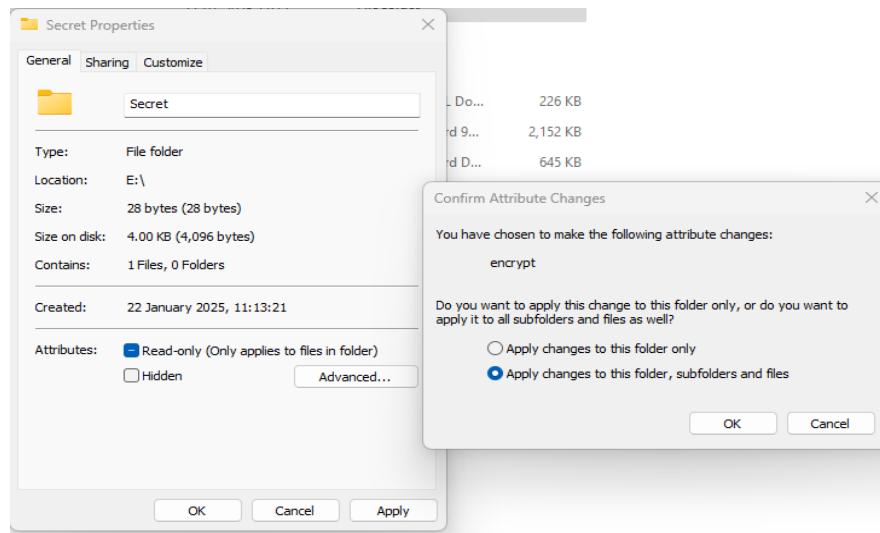


### Step 2: Create a textfile

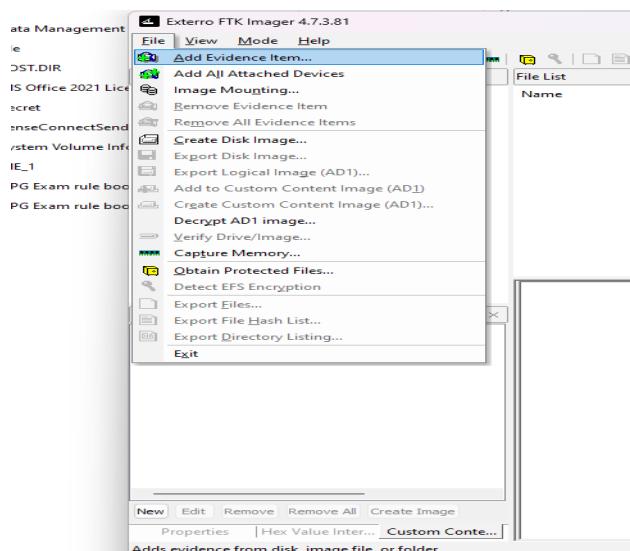


### Step 3: Go to properties, select advanced and click on Encrypt content to secure data

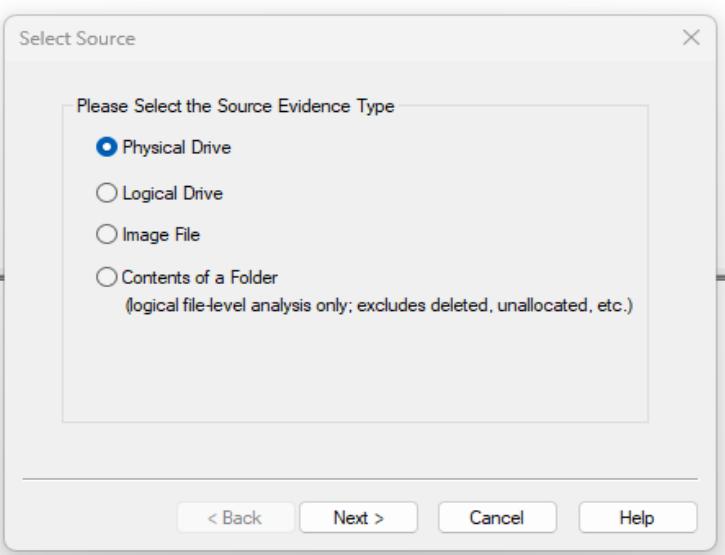




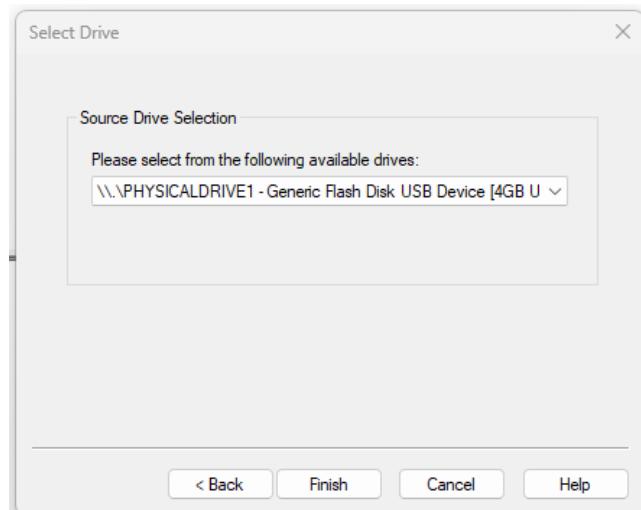
#### Step 4: Now open FTK Imager



#### 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.**

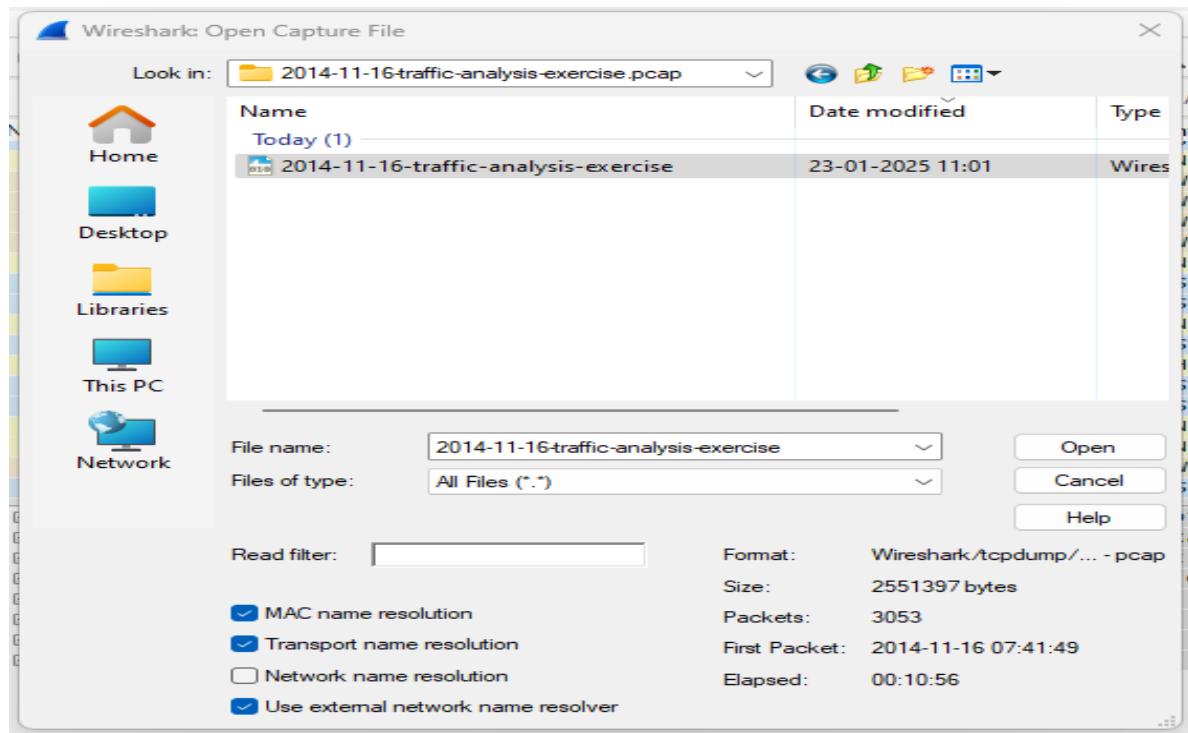
### Theory

Wireshark is a packet sniffer and analysis tool. It captures network traffic on the local network and 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 you can 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



The screenshot shows the Wireshark interface with the following details:

- Frame List:** Shows 3053 frames captured, starting from frame 1. Frame 1 is highlighted.
- Frame Details:** Displays the structure of frame 1, which is a TCP SYN packet. It includes fields like Time, Source, Destination, Protocol, Length, Info, and a hex dump.
- Hex View:** Provides a detailed hex dump of the selected frame, showing bytes 00000 to 00030.
- Source Code:** Shows the C code for the application layer of the selected frame.
- Statistics:** Shows various network statistics for the session.

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

The screenshot shows the Wireshark interface with the following details:

- File Menu:** File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Tools, Internals, Help.
- Toolbar:** Includes icons for file operations, capture, analyze, and search.
- Filter Bar:** Set to "http".
- Table View:** Shows a list of network frames with columns: No., Time, Source, Destination, Protocol, Length, and Info. The list includes various HTTP requests and responses, some with status codes like 200 OK or 304 Not Modified.
- Frame Details:** Frame 52 is selected, showing the following details:
  - Frame:** 52: 1002 bytes on wire (8016 bits), 1002 bytes captured (8016 bits)
  - Ethernet II:** Src: f0:19:af:02:9b:f1 (f0:19:af:02:9b:f1), Dst: VMware\_f3:ca:f5 (00:50:56:f3:ca:f5)
  - Internet Protocol Version 4:** Src: 172.16.165.165 (172.16.165.165), Dst: 204.79.197.200 (204.79.197.200)
  - Transmission Control Protocol:** Src Port: 49431 (49431), Dst Port: http (80), Seq: 821, Ack: 1, Len: 948
  - Content:** [2 Resassembled TCP Segments (1768 bytes): #51(820), #52(948)]
  - Protocol:** Hypertext Transfer Protocol
  - Language:** extensible Markup Language

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

Wireshark 1.10.2 (SVN Rev 51934 from /trunk-1.10) [2014-11-16-traffic-analysis-exercise.pcap]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: http.request

| No. | Time       | Source         | Destination    | Protocol | Length | Info   |
|-----|------------|----------------|----------------|----------|--------|--|
| 52  | 2.020811   | 172.16.165.165 | 204.79.197.200 | HTTP/TCP | 1002   | 1002 POST /fd/ls/lsp.aspx HTTP/1.1                       |
| 87  | 3.512628   | 204.79.197.200 | 172.16.165.165 | HTTP     | 324    | 324 HTTP/1.1 204 No Content                              |
| 92  | 3.612602   | 204.79.197.200 | 172.16.165.165 | HTTP     | 324    | [TCP Retransmission] HTTP/1.1 204 No Content             |
| 109 | 4.237852   | 172.16.165.165 | 204.79.197.200 | HTTP     | 861    | 861 GET /fd/ls/GLinkPing.aspx?IG=aee5908ea2d64991aa8b89! |
| 130 | 4.883832   | 204.79.197.200 | 172.16.165.165 | HTTP     | 462    | 462 HTTP/1.1 200 OK (GIF89a)                             |
| 133 | 4.983881   | 204.79.197.200 | 172.16.165.165 | HTTP     | 462    | [TCP Retransmission] HTTP/1.1 200 OK (GIF89a)            |
| 161 | 6.073686   | 172.16.165.165 | 82.150.140.30  | HTTP     | 621    | 621 GET / HTTP/1.1                                       |
| 225 | 7.484572   | 172.16.165.165 | 82.150.140.30  | HTTP     | 432    | 432 GET /wp-content/themes/cini/style.css HTTP/1.1       |
| 238 | 7.495119   | 172.16.165.165 | 82.150.140.30  | HTTP     | 467    | 467 GET /wp-content/plugins/contact-form-7/include       |
| 240 | 7.495288   | 172.16.165.165 | 82.150.140.30  | HTTP     | 453    | 453 GET /wp-includes/js/jquery/jquery-migrate.min.js     |
| 242 | 7.495489   | 172.16.165.165 | 82.150.140.30  | HTTP     | 452    | 452 GET /wp-content/plugins/sitemap/css/page-list        |
| 243 | 7.495622   | 172.16.165.165 | 82.150.140.30  | HTTP     | 438    | 438 GET /wp-content/themes/cini/js/functions.js          |
| 311 | 8.247070   | 82.150.140.30  | 172.16.165.165 | HTTP     | 1271   | 1271 HTTP/1.1 200 OK (text/css)                          |
| 313 | 8.247071   | 82.150.140.30  | 172.16.165.165 | HTTP     | 587    | 587 HTTP/1.1 200 OK (text/javascript)                    |
| 314 | 8.247110   | 82.150.140.30  | 172.16.165.165 | HTTP     | 1046   | 1046 HTTP/1.1 200 OK (text/css)                          |
| 318 | 8.247716   | 82.150.140.30  | 172.16.165.165 | HTTP     | 523    | 523 HTTP/1.1 200 OK (text/html)                          |
| 320 | 8.248504   | 172.16.165.165 | 82.150.140.30  | HTTP     | 442    | 442 GET /wp-includes/js/jquery/jquery.js?ver=1.10        |
| 291 | R 8.248500 | 172.16.165.165 | 82.150.140.30  | HTTP     | 484    | 484 GET /wp-content/themes/cini/include/func             |

Frame 52: 1002 bytes on wire (8016 bits), 1002 bytes captured (8016 bits)  
 Ethernet II, Src: F0:19:af:02:9b:f1 (f0:19:af:02:9b:f1), Dst: VMware-f3:ca:52 (00:50:56:f3:ca:52)  
 Internet Protocol Version 4, Src: 172.16.165.165 (172.16.165.165), Dst: 204.79.197.200 (204.79.197.200)  
 Transmission Control Protocol, Src Port: 49431 (49431), Dst Port: http (80), Seq: 821, Ack: 1, Len: 948  
 [2 Reassembled TCP Segments (1768 bytes): #51(820), #52(948)]  
 Hypertext Transfer Protocol  
 extensible Markup Language

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

| Packet num | Hostname           | Content Type    | Size       | Filename                                  |
|------------|--------------------|-----------------|------------|---|
| 52         | www.bing.com       | text/xml        | 948 bytes  | Isp.aspx                                  |
| 130        | www.bing.com       | image/gif       | 42 bytes   | GLinkPing.aspx?IG=aee5908ea2d64991aa8b89! |
| 133        | www.bing.com       | image/gif       | 42 bytes   | GLinkPing.aspx?IG=aee5908ea2d64991aa8b89! |
| 311        | www.cinlholland.nl | text/css        | 927 bytes  | styles.css?ver=3.7.2                      |
| 313        | www.cinlholland.nl | text/javascript | 237 bytes  | functions.js                              |
| 314        | www.cinlholland.nl | text/css        | 702 bytes  | page-list.css?ver=4.2                     |
| 318        | www.cinlholland.nl | text/html       | 61 kB      | \   |
| 340        | www.cinlholland.nl | text/css        | 4807 bytes | style.css                                 |
| 341        | www.cinlholland.nl | text/javascript | 7200 bytes | jquery-migrate.min.js?ver=1.2.1           |
| 401        | www.cinlholland.nl | text/css        | 1092 bytes | reset.css                                 |
| 432        | www.cinlholland.nl | text/javascript | 8913 bytes | scripts.js?ver=3.7.2                      |
| 445        | www.cinlholland.nl | text/javascript | 16 kB      | jquery.form.min.js?ver=3.50.0-2014.02.05  |
| 495        | adultbiz.in        | text/html       | 8638 bytes | jquery.php                                |
| 533        | www.cinlholland.nl | text/javascript | 93 kB      | jquery.js?ver=1.10.2                      |
| 569        | www.cinlholland.nl | image/gif       | 1270 bytes | youtubelogo_on.gif                        |
| 572        | www.cinlholland.nl | image/gif       | 577 bytes  | twitter_on.gif                            |
| 573        | www.cinlholland.nl | image/gif       | 536 bytes  | facebook_on.gif                           |
| 595        | www.cinlholland.nl | image/gif       | 4660 bytes | br_logo.gif                               |
| 596        | www.cinlholland.nl | image/gif       | 2476 bytes | newsletter_on.gif                         |
| 597        | www.cinlholland.nl | image/gif       | 2316 bytes | donate_on.gif                             |
| 598        | www.cinlholland.nl | image/gif       | 65 bytes   | squareorangedecor.gif                     |

Help Save As Save All Cancel

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

Wireshark: Save Object As ...

Name: jar.jar

Save in folder: Downloads

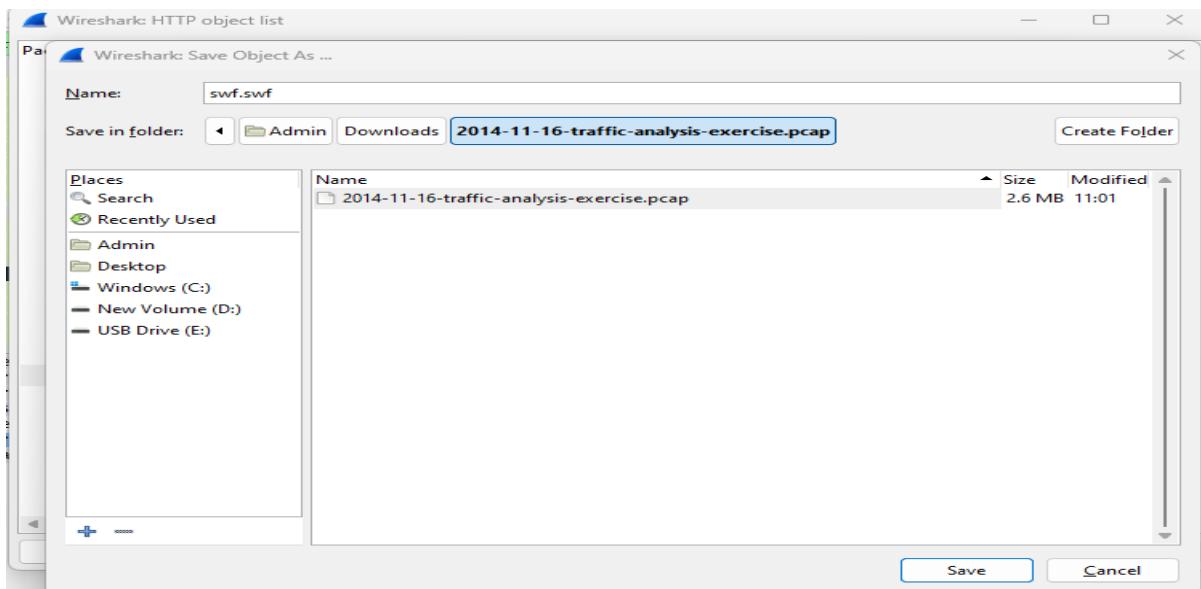
Places

Save

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



Extension .swf

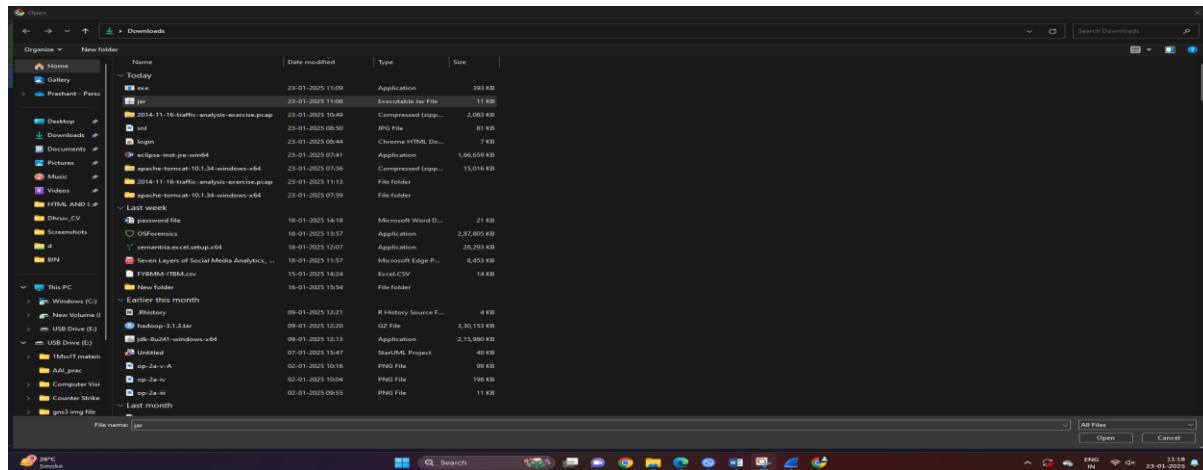


When you are looking for malware, use content and application type of file. So, here we have used java, executable and shockwave flash files. All files are saved in the system.

Go to browser and open virustotal.com

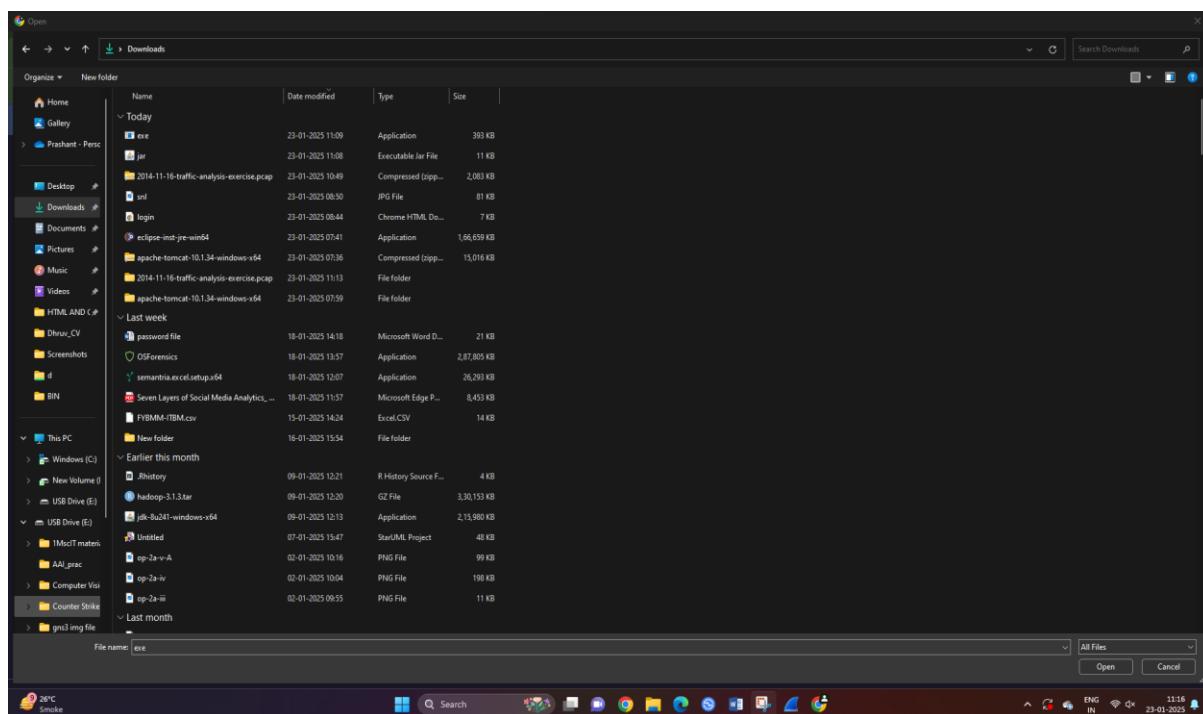
A screenshot of the VirusTotal website. The URL is 'virustotal.com/gui/home/upload'. The page features the 'VIRUSTOTAL' logo and a large input field for file upload. Below the input field is a 'Choose file' button. A note at the bottom states: 'By submitting data above, you are agreeing to our Terms of Service and Privacy Notice, and to the sharing of your sample submission with the security community. Please do not submit any personal information; we are not responsible for the contents of your submission. Learn more.' The 'FILE' tab is selected.

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



A screenshot of a VirusShare analysis page. At the top, it shows a 'Community Score' of 33/65. Below that, the file name is listed as '178be0ed63a7a9020121dee1c305fd6ca3b74d15836835cfb1684da0b44190d3 file.jar'. The threat category is 'trojan'. Vendor detections include Alibaba, Arcabit, AVG, BitDefender, CTX, Emissor, ESET-NOD32, and Google. The page also features a 'Join our Community' button and a 'Do you want to automate checks?' section.

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.**

| Security vendor's analysis | Do you want to automate checks? |
|----------------------------|---------------------------------|
| Acronis (Static ML)        | Undetected                      |
| AllCloud                   | Undetected                      |
| Anti-AVL                   | Undetected                      |
| Avast                      | Undetected                      |
| Avira (no cloud)           | Undetected                      |
| BitDefender                | Undetected                      |
| ClamAV                     | Undetected                      |
| CrowdStrike Falcon         | Undetected                      |
| Cynet                      | Undetected                      |
| AhnLab-V3                  | Undetected                      |
| ALYac                      | Undetected                      |
| Arcabit                    | Undetected                      |
| AVG                        | Undetected                      |
| Baidu                      | Undetected                      |
| Bkav Pro                   | Undetected                      |
| CMC                        | Undetected                      |
| CTX                        | Undetected                      |
| DrWeb                      | Undetected                      |

**.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**

```

HTTP/1.1 404 Not Found
Date: Sun, 16 Nov 2014 02:12:42 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
Content-Length: 0
Server: Apache/2.2.22 (Ubuntu)
Vary: Accept-Encoding
HTTP/1.1 404 Not Found
[HTTP response 2/2]
HTTP/1.1 404 Not Found
[HTTP response 3/3]
HTTP/1.1 404 Not Found
[HTTP response 4/4]

```

**What is the IP address of infected website?**

```

HTTP/1.1 404 Not Found
Date: Sun, 16 Nov 2014 02:12:42 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
Content-Length: 0
Server: Apache/2.2.22 (Ubuntu)
Vary: Accept-Encoding
HTTP/1.1 404 Not Found
[HTTP response 2/2]
HTTP/1.1 404 Not Found
[HTTP response 3/3]
HTTP/1.1 404 Not Found
[HTTP response 4/4]

```

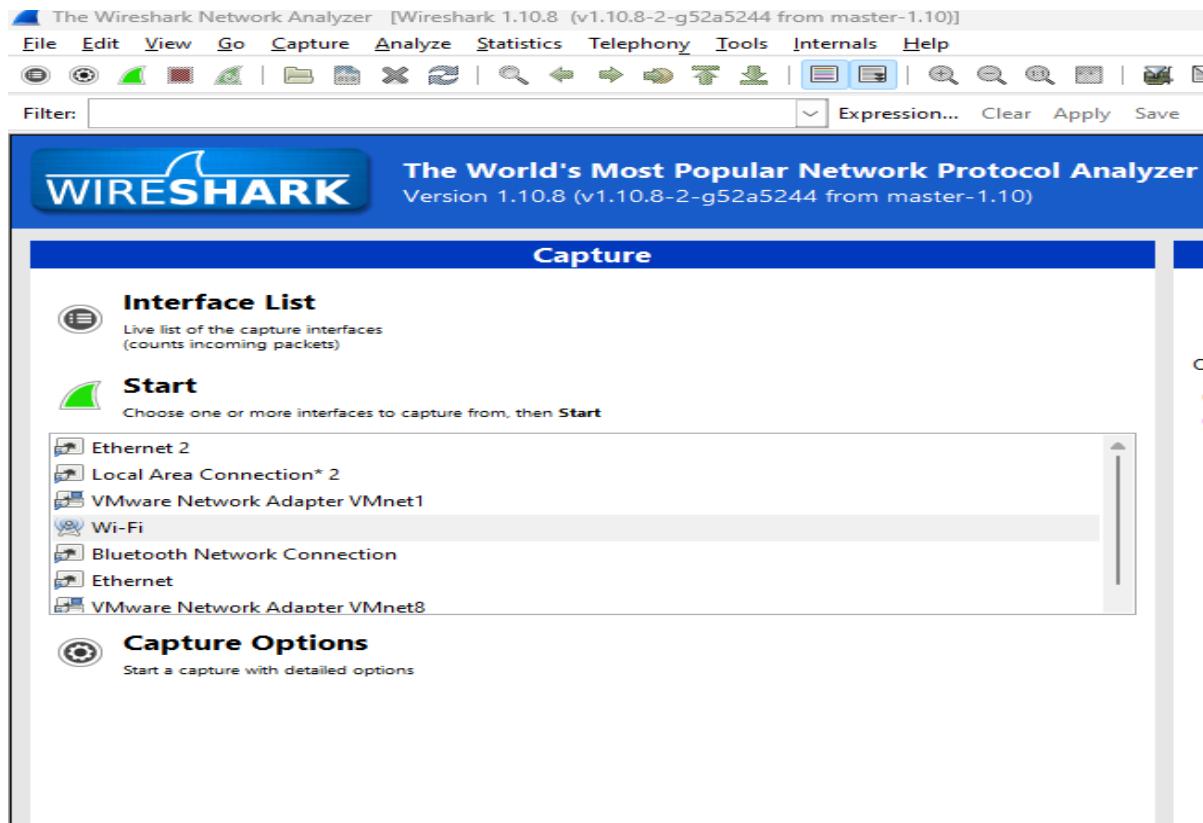
## What is the IP address of infected machine?

|  |                |      |  |
|--|----------------|------|--|
| 2515 75.499480 37.200.69.143   | 172.16.165.165 | HTTP | 259 [TCP Retransmission] HTTP/1.1 200 OK       |
| 2977 84.464154 37.200.69.143   | 172.16.165.165 | HTTP | 941 HTTP/1.1 200 OK (application/x-msdownload) |
| ⊕ Frame 2515: 259 bytes on wire (2072 bits), 259 bytes captured (2072 bits)                                |                |      |  |
| ⊕ Ethernet II, Src: VMware_f3:ca:52 (00:50:56:f3:ca:52), Dst: f0:19:af:02:9b:f1 (f0:19:af:02:9b:f1)        |                |      |  |
| ⊕ Internet Protocol Version 4, Src: 37.200.69.143 (37.200.69.143), Dst: 172.16.165.165 (172.16.165.165)    |                |      |  |
| Version: 4   |                |      |  |
| Header length: 20 bytes  |                |      |  |
| ⊕ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport)) |                |      |  |
| Total Length: 245  |                |      |  |
| Identification: 0x0920 (2336)  |                |      |  |
| ⊕ Flags: 0x00  |                |      |  |
| Fragment offset: 0   |                |      |  |
| Time to live: 128  |                |      |  |
| Protocol: TCP (6)  |                |      |  |
| ⊕ Header checksum: 0x73d6 [correct]  |                |      |  |
| Source: 37.200.69.143 (37.200.69.143)  |                |      |  |
| Destination: 172.16.165.165 (172.16.165.165)   |                |      |  |
| [Source GeoIP: Unknown]  |                |      |  |
| [Destination GeoIP: Unknown]   |                |      |  |
| ⊕ Transmission Control Protocol, Src Port: http (80), Dst Port: 49457 (49457), Seq: 1, Ack: 298, Len: 205  |                |      |  |
| ⊕ Hypertext Transfer Protocol  |                |      |  |

## 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.

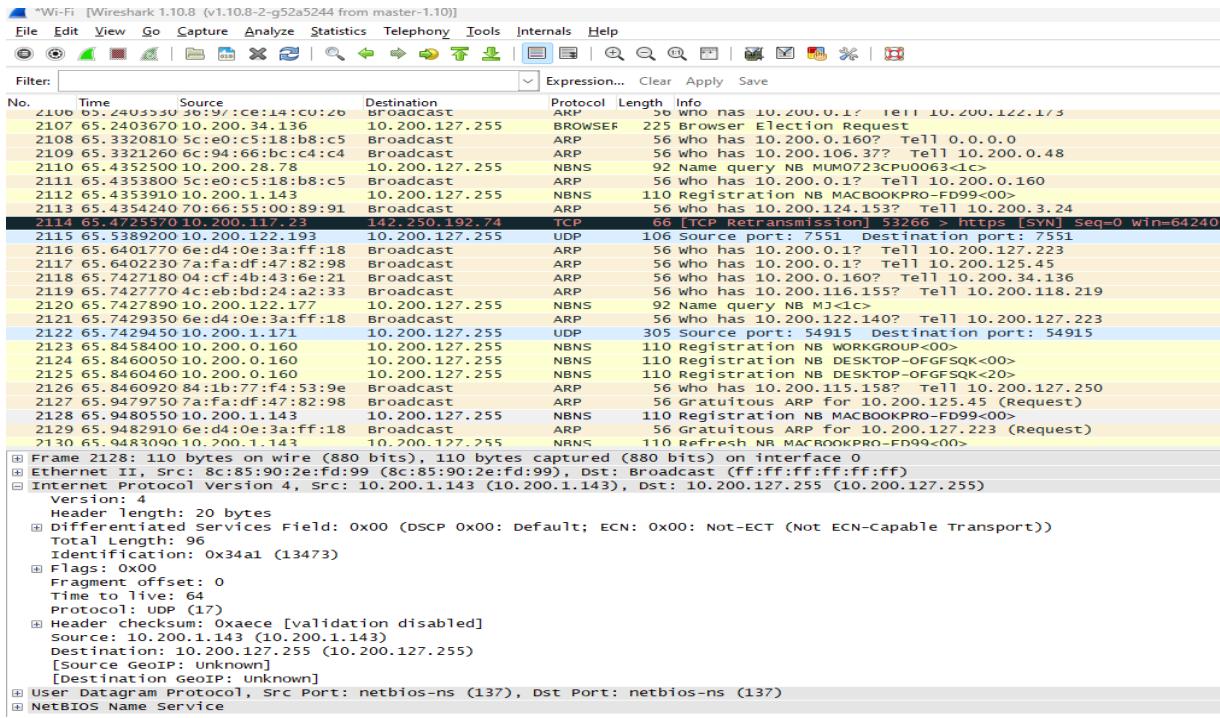
Promiscuous mode is the mode in which you can see all the packets from other systems on the network and not only the packets send or received from your network adapter. Promiscuous mode is enabled by default.

| No. | Time       | Source            | Destination    | Protocol | Length | Info   |
|-----|------------|-------------------|----------------|----------|--------|--|
| 394 | 12.3915560 | 10.200.122.177    | 10.200.127.255 | NBNS     | 92     | Name query NB M3<1c>   |
| 395 | 12.3916230 | 10.200.127.110    | 10.200.127.255 | BROWSEF  | 216    | Get Backup List Request  |
| 396 | 12.4953160 | d2:b6:ee:bb:5a:b4 | Broadcast      | ARP      | 56     | Who has 10.200.4.94? Tell 0.0.0.0  |
| 397 | 12.4953500 | 10.200.2.58       | 10.200.127.255 | NBNS     | 92     | Name query NB MUM0723CPU0078<1c>   |
| 398 | 12.4954230 | 10.200.122.193    | 10.200.127.255 | UDP      | 106    | Source port: 7551 Destination port: 7551   |
| 399 | 12.4954340 | 10.200.4.3        | 10.200.127.255 | NBNS     | 110    | Refresh NB MACBOOKAIR-A000<0>  |
| 400 | 12.5953560 | 10.200.1.171      | 10.200.127.255 | UDP      | 305    | Source port: 54915 Destination port: 54915   |
| 401 | 12.6979160 | 10.200.70.102     | 10.200.127.255 | BROWSEF  | 243    | Host Announcement MUM1532CPU0171, workstation, Server, NT Workstation  |
| 402 | 12.6980370 | 90:65:84:19:05:50 | Broadcast      | ARP      | 56     | Who has 10.200.0.17? Tell 10.200.2.36  |
| 403 | 12.6980490 | 08:9d:f4:92:4e:d3 | Broadcast      | ARP      | 56     | Who has 10.200.70.102? Tell 10.200.127.27  |
| 404 | 12.6980610 | d2:b6:ee:bb:5a:b4 | Broadcast      | ARP      | 56     | Gratuitous ARP for 10.200.4.94 (Request)   |
| 405 | 12.7999420 | 10.200.4.3        | 10.200.127.255 | NBNS     | 110    | Refresh NB MACBOOKAIR-A000<0>  |
| 406 | 12.9028000 | 10.200.34.136     | 10.200.127.255 | BROWSEF  | 243    | Local Master Announcement MUM0722CPU0037, workstation, Server, NT Workstation, Potential Browser, Master Browser |
| 407 | 12.9030070 | c2:6d:fd:21:f3:d3 | Broadcast      | ARP      | 56     | Who has 10.200.0.1? Tell 10.200.0.241  |
| 408 | 12.9030420 | 10.200.3.14       | 10.200.127.255 | NBNS     | 92     | Name query NB SVKMGRP<1d>  |
| 409 | 13.0068690 | 10.200.124.122    | 10.200.127.255 | NBNS     | 92     | Name query NB SVKMGRP<1d>  |

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.



Wi-Fi [Wireshark 1.10.8 (v1.10.8-2-g52a5244 from master-1.10)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

| No.  | Time                                | Source         | Destination | Protocol | Length | Info   |
|------|-------------------------------------|----------------|-------------|----------|--------|--|
| 2106 | 03:24:03:35:00:39:ce:14:c0:26       | broadcast      |             | ARP      | 60     | who has 10.200.0.1? Tell 10.200.122.173                  |
| 2107 | 05:24:03:67:10:200,34:136           | 10.200.127.255 |             | BROWSER  | 225    | Browser Election Request                                 |
| 2108 | 05:33:20:81:00:5c:e0:c5:18:b8:c5    | broadcast      |             | ARP      | 56     | who has 10.200.0.160? Tell 0.0.0.0                       |
| 2109 | 05:33:21:26:06:c4:94:66:bc:c4:c4    | broadcast      |             | ARP      | 56     | who has 10.200.106.37? Tell 10.200.0.48                  |
| 2110 | 05:43:52:50:00:10,200,28:78         | 10.200.127.255 |             | NBNS     | 92     | Name query NB MLMQ0723CPU0063<lc>                        |
| 2111 | 05:43:53:80:00:5c:e0:c5:18:b8:c5    | broadcast      |             | ARP      | 56     | who has 10.200.0.1? Tell 10.200.0.160                    |
| 2112 | 05:43:53:91:10:200,1.143            | 10.200.127.255 |             | NBNS     | 110    | Registration NB MACBOOKPRO-FD99<00>                      |
| 2113 | 05:43:54:24:70:66:55:00:89:91       | broadcast      |             | ARP      | 56     | who has 10.200.124.153? Tell 10.200.3.24                 |
| 2114 | 05:47:25:57:10,200,117,23           | 142.250.192.74 |             | TCP      | 66     | [TCP Retransmission] 53266 > https [SYN] Seq=0 win=64240 |
| 2115 | 05:53:89:20:10,200,122,193          | 10.200.127.255 |             | UDP      | 106    | Source port: 7551 Destination port: 7551                 |
| 2116 | 05:64:01:77:00,200,117,23           | 142.250.192.74 |             | ARP      | 56     | who has 10.200.0.1? Tell 10.200.127.223                  |
| 2117 | 05:64:02:23:00,74:fa:df:47:82:98    | broadcast      |             | ARP      | 56     | who has 10.200.0.1? Tell 10.200.125.45                   |
| 2118 | 05:65:74:27:77:00,4:c:f:bd:24:a2:33 | broadcast      |             | ARP      | 56     | who has 10.200.0.160? Tell 10.200.34.136                 |
| 2119 | 05:65:74:27:77:00,4:c:f:bd:24:a2:33 | broadcast      |             | ARP      | 56     | who has 10.200.116.155? Tell 10.200.118.219              |
| 2120 | 05:65:74:27:77:00,4:c:f:bd:24:a2:33 | 10.200.127.255 |             | NBNS     | 92     | Name query NB MJ<lc>                                     |
| 2121 | 05:65:74:29:35:00,6:d4:0e:3a:ff:18  | broadcast      |             | ARP      | 56     | who has 10.200.122.140? Tell 10.200.127.223              |
| 2122 | 05:65:74:29:45:10,200,1,171         | 10.200.127.255 |             | UDP      | 305    | Source port: 54915 Destination port: 54915               |
| 2123 | 05:65:84:58:00:10,200,0,160         | 10.200.127.255 |             | NBNS     | 110    | Registration NB WORKGROUP<00>                            |
| 2124 | 05:65:84:60:00:50:10,200,0,160      | 10.200.127.255 |             | NBNS     | 110    | Registration NB DESKTOP-OFGFSOK<00>                      |
| 2125 | 05:65:84:60:04:60:10,200,0,160      | 10.200.127.255 |             | NBNS     | 110    | Registration NB DESKTOP-OFGFSOK<00>                      |
| 2126 | 05:65:84:60:92:00,84:1b:77:f4:53:98 | broadcast      |             | ARP      | 56     | who has 10.200.115.158? Tell 10.200.127.250              |
| 2127 | 05:65:94:79:75:00,74:fa:df:47:82:98 | broadcast      |             | ARP      | 56     | Gratuitous ARP For 10.200.125.45 (Request)               |
| 2128 | 05:65:94:80:55:10,200,1,143         | 10.200.127.255 |             | NBNS     | 110    | Registration NB MACBOOKPRO-FD99<00>                      |
| 2129 | 05:65:94:82:91:00,6:d4:0e:3a:ff:18  | broadcast      |             | ARP      | 56     | Gratuitous ARP For 10.200.127.223 (Request)              |
| 2130 | 05:65:94:83:09:00,10,200,1,143      | 10.200.127.255 |             | NRNS     | 110    | Refresh Ns MACBOOKPRO-FD99<00>                           |

Frame 2128: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface 0

Ethernet II, Src: 8c:85:90:2e:fd:99 (8c:85:90:2e:fd:99), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

Internet Protocol Version 4, Src: 10.200.1.143 (10.200.1.143), Dst: 10.200.127.255 (10.200.127.255)

Version: 4

Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))

Total Length: 96

Identification: 0x34a1 (13473)

Flags: 0x00

Fragment offset: 0

Time to live: 64

Protocol: UDP (17)

Header checksum: 0xaece [validation disabled]

Source: 10.200.1.143 (10.200.1.143)

Destination: 10.200.127.255 (10.200.127.255)

[Source GeoIP: Unknown]

[Destination GeoIP: Unknown]

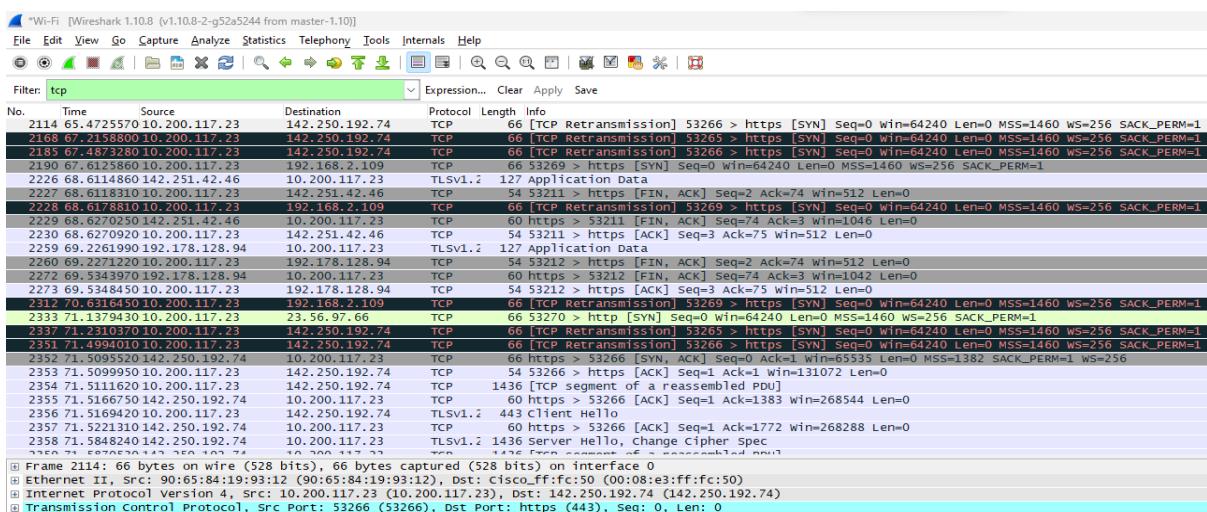
User Datagram Protocol, Src Port: netbios-ns (137), Dst Port: netbios-ns (137)

NetBIOS Name Service

To Analyse the captured packets different filters commands are used:

### 1. Display packets which are using TCP protocol

tcp



Wi-Fi [Wireshark 1.10.8 (v1.10.8-2-g52a5244 from master-1.10)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: tcp Expression... Clear Apply Save

| No.  | Time                             | Source         | Destination | Protocol | Length | Info   |
|------|----------------------------------|----------------|-------------|----------|--------|--|
| 2114 | 05:47:25:57:10,200,117,23        | 142.250.192.74 |             | TCP      | 66     | [TCP Retransmission] 53266 > https [SYN] Seq=0 win=64240 Len=0 MSS=1460 ws=256 SACK_PERM=1 |
| 2168 | 05:53:89:20,10,200,117,23        | 142.250.192.74 |             | TCP      | 66     | [TCP Retransmission] 53265 > https [SYN] Seq=0 win=64240 Len=0 MSS=1460 ws=256 SACK_PERM=1 |
| 2185 | 05:67:48:73:28:10,200,117,23     | 142.250.192.74 |             | TCP      | 66     | [TCP Retransmission] 53266 > https [SYN] Seq=0 win=64240 Len=0 MSS=1460 ws=256 SACK_PERM=1 |
| 2190 | 05:65:23:86:00,10,200,117,23     | 192.168.2.109  |             | TCP      | 66     | 53269 > https [SYN] Seq=0 win=64240 Len=0 MSS=1460 ws=256 SACK_PERM=1                      |
| 2226 | 05:61:14:86:00,142,251,42,46     | 10,200,117,23  |             | TLSv1.2  | 127    | Application Data   |
| 2227 | 05:68:13:23:10,200,117,23        | 142.251.42.46  |             | TCP      | 54     | 53211 > https [FIN, ACK] Seq=2 Ack=74 win=512 Len=0  |
| 2228 | 05:61:78:80:10,200,117,23        | 192.168.2.109  |             | TCP      | 66     | [TCP Retransmission] 53269 > https [SYN] Seq=0 win=64240 Len=0 MSS=1460 ws=256 SACK_PERM=1 |
| 2229 | 05:68:27:02:50,142,251,42,46     | 10,200,117,23  |             | TCP      | 60     | https > 53211 [FIN, ACK] Seq=74 Ack=3 win=1046 Len=0                                       |
| 2230 | 05:62:70:92:10,200,117,23        | 142.251.42,46  |             | TCP      | 54     | 53211 > https [ACK] Seq=3 Ack=75 win=512 Len=0   |
| 2259 | 05:69:22:61:99:00,192,178,28,94  | 10,200,117,23  |             | TLSv1.2  | 127    | Application Data   |
| 2260 | 05:69:22:71:22:10,200,117,23     | 192.178.128,94 |             | TCP      | 54     | 53212 > https [FIN, ACK] Seq=2 Ack=74 win=512 Len=0  |
| 2272 | 05:69:53:43:97:10,192,178,28,94  | 10,200,117,23  |             | TCP      | 60     | https > 53212 [FIN, ACK] Seq=74 Ack=3 win=1042 Len=0                                       |
| 2273 | 05:69:54:84:50:10,200,117,23     | 192.178.128,94 |             | TCP      | 54     | 53212 > https [ACK] Seq=3 Ack=75 win=512 Len=0   |
| 2332 | 05:70:61:64:50:10,200,117,23     | 192.168.2.109  |             | TCP      | 66     | [TCP Retransmission] 53269 > https [SYN] Seq=0 win=64240 Len=0 MSS=1460 ws=256 SACK_PERM=1 |
| 2333 | 05:71:13:79:40:10,200,117,23     | 23.56.97.66    |             | TCP      | 66     | 53270 > http [SYN] Seq=0 win=64240 Len=0 MSS=1460 ws=256 SACK_PERM=1                       |
| 2337 | 05:71:23:10:37:10,200,117,23     | 142.250.192.74 |             | TCP      | 66     | [TCP Retransmission] 53265 > https [SYN] Seq=0 win=64240 Len=0 MSS=1460 ws=256 SACK_PERM=1 |
| 2351 | 05:71:49:94:01:10,200,117,23     | 142.250.192.74 |             | TCP      | 66     | [TCP Retransmission] 53266 > https [SYN] Seq=0 win=64240 Len=0 MSS=1460 ws=256 SACK_PERM=1 |
| 2352 | 05:71:50:95:52:10,200,117,23     | 142.250.192.74 |             | TCP      | 66     | https > 53266 [SYN, ACK] Seq=0 Ack=1 win=65535 Len=0 MSS=1382 SACK_PERM=1 ws=256           |
| 2353 | 05:71:50:99:50:10,200,117,23     | 142.250.192.74 |             | TCP      | 54     | 53266 > https [ACK] Seq=1 Ack=1 win=131072 Len=0   |
| 2354 | 05:71:51:11:62:10,200,117,23     | 142.250.192.74 |             | TCP      | 1436   | [TCP segment of a reassembled PDU]   |
| 2355 | 05:71:51:66:75:10,200,117,23     | 10,200,117,23  |             | TCP      | 60     | https > 53266 [ACK] Seq=1 Ack=1383 win=268544 Len=0  |
| 2356 | 05:71:51:69:42:10,200,117,23     | 142.250.192.74 |             | TLSv1.2  | 443    | Client Hello   |
| 2357 | 05:71:52:21:31:10,142,250,192,74 | 10,200,117,23  |             | TCP      | 60     | https > 53266 [ACK] Seq=1 Ack=1772 win=268288 Len=0  |
| 2358 | 05:71:58:48:24:10,200,117,23     | 10,200,117,23  |             | TLSv1.2  | 1436   | Server Hello, Change Cipher Spec   |
| 2359 | 05:71:58:55:20:10,200,117,23     | 10,200,117,23  |             | TCP      | 1436   | [TCP segment of a reassembled PDU]   |

Frame 2114: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0

Ethernet II, Src: Cisco\_ff:fc:50 (00:08:e3:ff:fc:50)

Internet Protocol Version 4, Src: 10.0.65.84:19:93:12 (90:65:84:19:93:12), Dst: Cisco\_ff:fc:50 (00:08:e3:ff:fc:50)

Transmission Control Protocol, Src Port: 53266 (53266), Dst Port: https (443), Seq: 0, Len: 0

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

ip.src == 192.178.128.94

The Wireshark interface shows a list of network frames. The filter bar at the top is set to "ip.src==192.178.128.94". The packet list table has columns: No., Time, Source, Destination, Protocol, Length, and Info. The following packets are listed:

| No.  | Time       | Source         | Destination   | Protocol | Length | Info  |
|------|------------|----------------|---------------|----------|--------|---|
| 306  | 10.8014590 | 192.178.128.94 | 10.200.117.23 | TCP      | 66     | https > 53212 [ACK] Seq=1 Ack=2 Win=1042 Len=0 SLE=1 SRE=2                      |
| 1809 | 56.1193070 | 192.178.128.94 | 10.200.117.23 | TCP      | 66     | [TCP Keep-Alive ACK] https > 53212 [ACK] Seq=1 Ack=2 Win=1042 Len=0 SLE=1 SRE=2 |
| 2259 | 69.2261990 | 192.178.128.94 | 10.200.117.23 | TLSV1.2  | 127    | Application Data  |
| 2272 | 69.5343970 | 192.178.128.94 | 10.200.117.23 | TCP      | 60     | https > 53212 [FIN, ACK] Seq=74 Ack=3 Win=1042 Len=0                            |

Details pane below the packet list shows:

- Frame 306: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
- Ethernet II, Src: Cisco\_ff:fc:50 (00:08:e3:ff:fc:50), Dst: 90:65:84:19:93:12 (90:65:84:19:93:12)
- Internet Protocol Version 4, Src: 192.178.128.94 (192.178.128.94), Dst: 10.200.117.23 (10.200.117.23)
- Transmission Control Protocol, Src Port: https (443), Dst Port: 53212 (53212), Seq: 1, Ack: 2, Len: 0

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

ip.dst == 23.212.254.51

The Wireshark interface shows a list of network frames. The filter bar at the top is set to "ip.dst==23.212.254.51". The packet list table has columns: No., Time, Source, Destination, Protocol, Length, and Info. The following packets are listed:

| No.  | Time       | Source        | Destination   | Protocol | Length | Info  |
|------|------------|---------------|---------------|----------|--------|---|
| 1563 | 49.8747680 | 10.200.117.23 | 23.212.254.51 | TCP      | 54     | 53227 > https [ACK] Seq=1 Ack=25 Win=1023 Len=0 |
| 1564 | 49.8749030 | 10.200.117.23 | 23.212.254.51 | TCP      | 54     | 53227 > https [ACK] Seq=1 Ack=26 Win=1023 Len=0 |

Details pane below the packet list shows:

- Frame 1563: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
- Ethernet II, Src: 90:65:84:19:93:12 (90:65:84:19:93:12), Dst: Cisco\_ff:fc:50 (00:08:e3:ff:fc:50)
- Internet Protocol Version 4, Src: 10.200.117.23 (10.200.117.23), Dst: 23.212.254.51 (23.212.254.51)
- Transmission Control Protocol, Src Port: 53227 (53227), Dst Port: https (443), seq: 1, Ack: 25, Len: 0

## 4. Display packets having no error connecting to server □

http.response.code==200

The Wireshark interface shows a list of network frames. The filter bar at the top is set to "http.response.code==200". The packet list table has columns: No., Time, Source, Destination, Protocol, Length, and Info. The following packets are listed:

| No.  | Time       | Source      | Destination   | Protocol | Length | Info                         |
|------|------------|-------------|---------------|----------|--------|------------------------------|
| 319  | 10.9289020 | 23.56.97.66 | 10.200.117.23 | HTTP     | 241    | HTTP/1.1 200 OK (text/plain) |
| 1282 | 41.1071580 | 23.56.97.66 | 10.200.117.23 | HTTP     | 241    | HTTP/1.1 200 OK (text/plain) |

Details pane below the packet list shows:

- Frame 1282: 241 bytes on wire (1928 bits), 241 bytes captured (1928 bits) on interface 0
- Ethernet II, Src: Cisco\_ff:fc:50 (00:08:e3:ff:fc:50), Dst: 90:65:84:19:93:12 (90:65:84:19:93:12)
- Internet Protocol Version 4, Src: 23.56.97.66 (23.56.97.66), Dst: 10.200.117.23 (10.200.117.23)
- Transmission Control Protocol, Src Port: http (80), Dst Port: 53264 (53264), Seq: 1, Ack: 112, Len: 187
- Hypertext Transfer Protocol
- Line-based text data: text/plain

## 5. Display packets which are using http request

### http.request

| No.  | Time       | Source        | Destination   | Protocol | Length | Info   |
|------|------------|---------------|---------------|----------|--------|--|
| 317  | 10.8710940 | 10.200.117.23 | 23.56.97.66   | HTTP     | 165    | GET /connecttest.txt HTTP/1.1  |
| 792  | 24.9233390 | 10.200.117.23 | 146.75.46.172 | HTTP     | 256    | GET /msdownload/update/v3/static/trustedr/en/disallowedcertst1.cab?585718324127ef9e HTTP/1.1 |
| 849  | 26.0180840 | 10.200.117.23 | 146.75.46.172 | HTTP     | 250    | GET /msdownload/update/v3/static/trustedr/en/pinrulesst1.cab?d97e4600c370791f HTTP/1.1       |
| 1277 | 41.0389020 | 10.200.117.23 | 23.56.97.66   | HTTP     | 165    | GET /connecttest.txt HTTP/1.1  |

Frame 317: 165 bytes on wire (1320 bits), 165 bytes captured (1320 bits) on interface 0  
Ethernet II, Src: Cisco\_(90:65:84:19:93:12) (00:08:e3:ff:fc:50), Dst: Cisco\_ff:fc:50 (00:08:e3:ff:fc:50)  
Internet Protocol Version 4, Src: 10.200.117.23 (10.200.117.23), Dst: 23.56.97.66 (23.56.97.66)  
Transmission Control Protocol, Src Port: 53260 (53260), Dst Port: http (80), Seq: 1, Ack: 1, Len: 111  
Hypertext Transfer Protocol

## 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>**

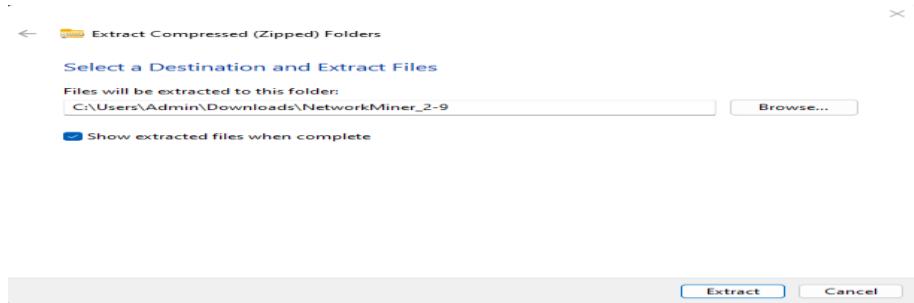
The screenshot shows the Netresec website with the following details:

- Header:** Experts in network security monitoring and network forensics
- Navigation:** NETRESEC | Products | Training | Resources | Blog | About Netresec
- Breadcrumbs:** NETRESEC » Products » NetworkMiner
- Title:** NetworkMiner
- Description:** NetworkMiner is an [open source](#) network forensics tool that extracts artifacts, such as files, images, emails and passwords, from captured network traffic in PCAP files. NetworkMiner can also be used to capture live network traffic by sniffing a network interface. Detailed information about each IP address in the analyzed network traffic is aggregated to a network host inventory, which can be used for passive asset discovery as well as to get an overview of which devices that are communicating. NetworkMiner is primarily designed to run in Windows, but can also be used in [Linux](#).
- Image:** A large purple circle with a white 'X' through it.
- Software Preview:** Shows the NetworkMiner 2.7.3 application window with a list of hosts (192.168.0.1, 192.168.0.2 (Linux), 192.168.0.50) and various tabs like Anomalies, Hosts (179), Files (287), Images (8), Messages, Credentials (4), Sessions (242), DNS (1497), Parameters (4074), Keywords.
- Features Table:**

| Feature                                       | Status            |
|---|-------------------|
| 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
- Buttons:** Download NetworkMiner (free edition) / Buy NetworkMiner Professional
- Footnotes:**
  - \* 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.**

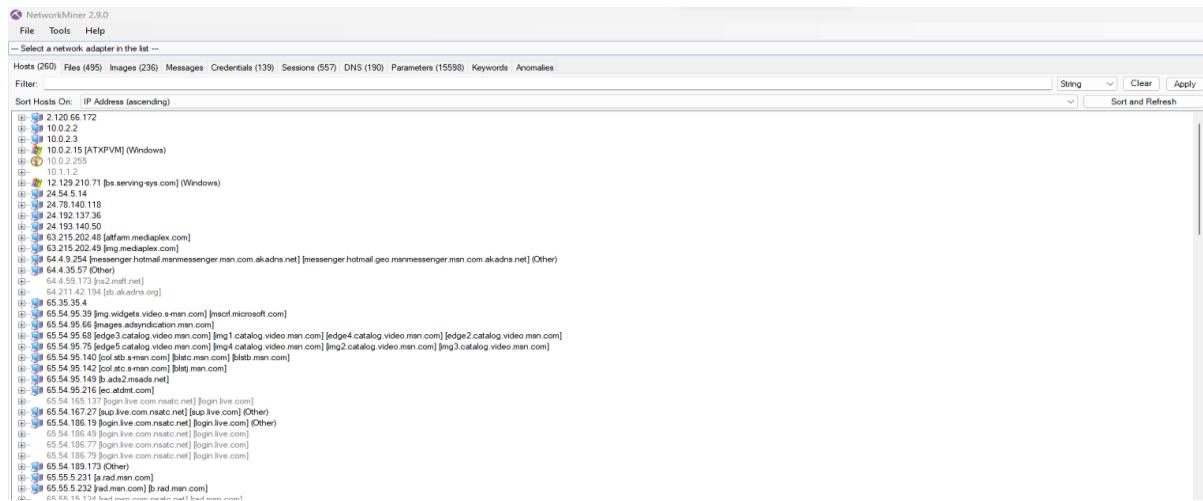
**Step 3: Run the Application.exe file from the folder to Open Network Miner.**



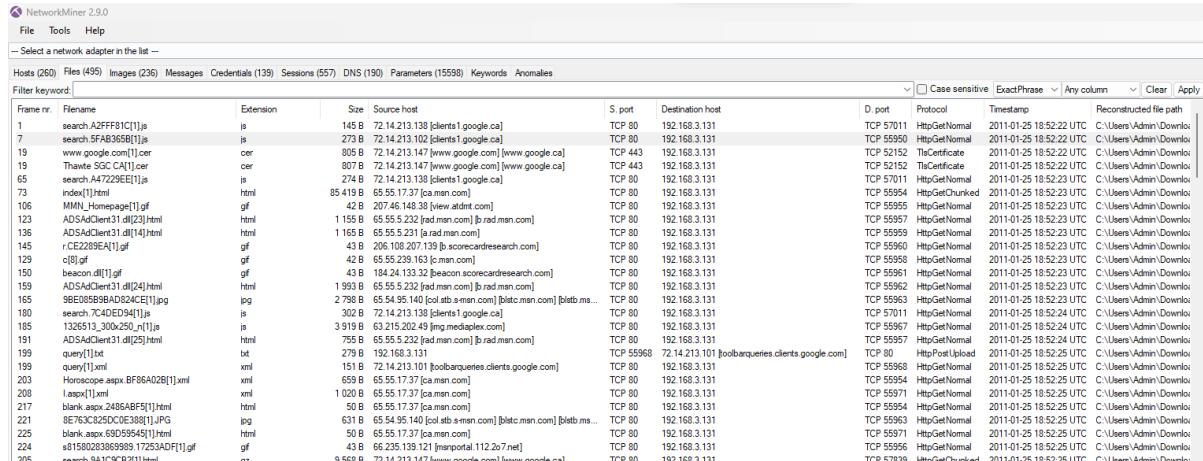
**Step 4: Download pcap file from the URL mentioned in the screenshot below**  
<https://tcpreplay.appneta.com/wiki/captures.html>

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

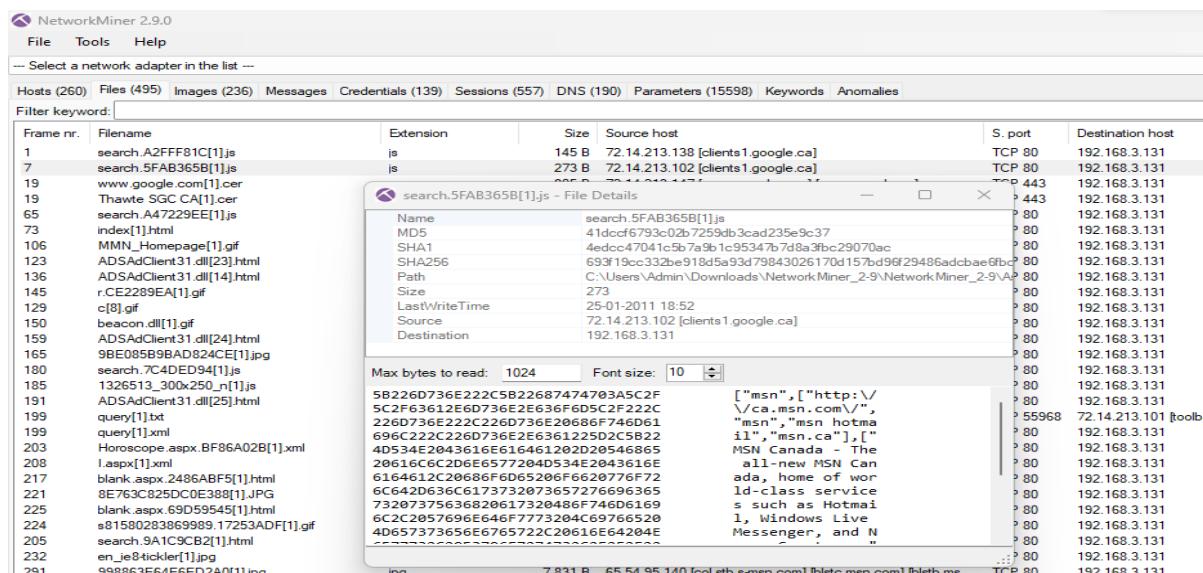
**Step 6:** In the hosts tab, you can see all the host that were engaged while recording the pcap files. These pcap files could be from a recorded session of Wireshark.



**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

NetworkMiner 2.9.0

File Tools Help

– Select a network adapter in the list –

Hosts (260) Files (495) Images (236) Messages Credentials (139) Sessions (557) DNS (190) Parameters (15598) Keywords Anomalies

Min Pixels: 0    Filename Filter:    Icon Size:    Update

|                                     |                                     |                                       |                                       |                                       |  |                                       |                                       |                                       |                                       |                                       |                                       |                                       |
|-------------------------------------|-------------------------------------|---------------------------------------|---------------------------------------|---------------------------------------|--|---------------------------------------|---------------------------------------|---------------------------------------|---------------------------------------|---------------------------------------|---------------------------------------|---------------------------------------|
| 113D9FCBAF932F...<br>75x75, 2 456 B | EFFC48BB53C64A...<br>75x75, 2 882 B | 8ED134AC4D845...<br>75x75, 3 091 B    | 96515EA155A96E...<br>75x75, 2 548 B   | BD795FEE494D...<br>75x75, 2 441 B     | AEB03287F73BDF...<br>75x75, 2 113 B      | 6CCC30C75B9E8A...<br>75x75, 2 227 B   | E434B0C44CC971...<br>75x75, 2 785 B   | 2C672DC2FAD1C...<br>75x75, 2 895 B    | 7F65E5D75D0B9...<br>75x75, 2 849 B    | ED25494A4252E8...<br>75x75, 2 514 B   | 234252CA38249F...<br>75x75, 3 213 B   | 982F1A3F42D944...<br>75x75, 2 677 B   |
| 37374FFEA4CC93...<br>75x75, 3 869 B | D45E5B3C5F8775...<br>75x75, 2 484 B | B47F72BEF7A51...<br>75x75, 2 163 B    | D7BC021F7EAA2...<br>75x75, 2 110 B    | 4892397B7FD786F...<br>85x85, 3 501 B  | 488A3EC3638EF4...<br>85x85, 3 053 B      | E458C8E3BED5B...<br>85x85, 3 279 B    | B1A898617A1F83...<br>85x85, 3 370 B   | 7C80431B89CD49...<br>85x85, 3 639 B   | D8EA26B155360...<br>85x85, 3 642 B    | D0D98B791B8CE...<br>85x85, 3 488 B    | 3A6AE95E78257F...<br>85x85, 2 971 B   | 511595E8FAE8901...<br>194x127, 7749 B |
| f962b4dbc44a9e...<br>1x20, 93 B     | 654[1].g...<br>300x250, 30 570 B    | image.aspx.12380...<br>92x69, 2 468 B | image.aspx.BAFC3...<br>92x69, 2 908 B | image.aspx.47C5C...<br>92x69, 4 063 B | image.aspx.975EB...<br>300x225, 22 098 B | image.aspx.F6F00...<br>64x48, 2 439 B | image.aspx.480FD...<br>52x39, 2 015 B | image.aspx.99020...<br>52x39, 2 067 B | image.aspx.3C6CF...<br>52x39, 1 988 B | image.aspx.DA129...<br>52x39, 1 923 B | image.aspx.AC73A...<br>52x39, 2 103 B |                                       |

## Step 10: You can view all messages below

NetworkMiner 2.9.0

File Tools Help

– Select a network adapter in the list –

Hosts (260) Files (495) Images (236) Messages Credentials (139) Sessions (557) DNS (190) Parameters (15598) Keywords Anomalies

Filter keyword:  Case sensitive:  ExactPhrase:  Any column:  Clear:  Apply:

| Frame nr. | Source host | Destination host | From | To | Subject | Protocol | Timestamp | Size | Case Panel   |
|-----------|-------------|------------------|------|----|---------|----------|-----------|------|--|
|           |             |                  |      |    |         |          |           |      | Case Panel   |
|           |             |                  |      |    |         |          |           |      | Filename: MD5<br>smallFo... 16cf39f...                           |
|           |             |                  |      |    |         |          |           |      | Windows-1252 Western European (Windows)<br>[no message selected] |

## Step 11: You can view all credentials below

NetworkMiner 2.9.0

File Tools Help

– Select a network adapter in the list –

Hosts (260) Files (495) Images (236) Message Credentials (139) Sessions (557) DNS (190) Parameters (15598) Keywords Anomalies

Show Cookies  Show NTLM challenge-response  Mask Passwords

| Client                       | Server                                   | Protocol    | Username  | Password | Valid login | First Login             |
|------------------------------|--|-------------|---|----------|-------------|-------------------------|
| 10.0.2.15 [ATXPVM]           | 65.55.116.104 [www.atbnt.com]            | HTTP Cookie | AA002+125392294-10931208; MUID=1238EDB2404...         | N/A      | Unknown     | 2011-01-25 18:54:31 UTC |
| 10.0.2.15 [ATXPVM]           | 65.55.116.104 [www.atbnt.com]            | HTTP Cookie | AA002+125392294-10931208; MUID=1238EDB2404...         | N/A      | Unknown     | 2011-01-25 18:54:24 UTC |
| 192.168.3.131 [studentD1-PC] | 208.82.236.129 [kelowna.en.craiglist.ca] | HTTP Cookie | cl_def_hp_kelowna.cl_def_langen                       | N/A      | Unknown     | 2011-01-25 18:52:26 UTC |
| 192.168.3.131 [studentD1-PC] | 208.82.236.129 [kelowna.en.craiglist.ca] | HTTP Cookie | cl_def_hp_vancouver.cl_def_langen                     | N/A      | Unknown     | 2011-01-25 18:52:53 UTC |
| 192.168.3.131 [studentD1-PC] | 208.82.236.129 [kelowna.en.craiglist.ca] | HTTP Cookie | cl_def_langen.cl_def_hp_vancouver                     | N/A      | Unknown     | 2011-01-25 18:52:29 UTC |
| 192.168.3.131 [studentD1-PC] | 208.82.236.129 [kelowna.en.craiglist.ca] | HTTP Cookie | cl_def_langen.cl_def_hp_vancouver                     | N/A      | Unknown     | 2011-01-25 18:52:44 UTC |
| 192.168.3.131 [studentD1-PC] | 208.82.236.129 [kelowna.en.craiglist.ca] | HTTP Cookie | cl_def_langen.domain_craiglist.ca.path=/expressFr...  | N/A      | Unknown     | 2011-01-25 18:53:20 UTC |
| 192.168.3.131 [studentD1-PC] | 208.82.236.129 [kelowna.en.craiglist.ca] | HTTP Cookie | cl_def_langen.domain_craiglist.ca.path=/expressMo...  | N/A      | Unknown     | 2011-01-25 18:54:17 UTC |
| 192.168.3.131 [studentD1-PC] | 208.82.236.129 [kelowna.en.craiglist.ca] | HTTP Cookie | cl_def_langen.domain_craiglist.ca.path=/expressMo...  | N/A      | Unknown     | 2011-01-25 18:53:41 UTC |
| 192.168.3.131 [studentD1-PC] | 208.82.236.129 [kelowna.en.craiglist.ca] | HTTP Cookie | cl_def_langen.domain_craiglist.ca.path=/expressSa...  | N/A      | Unknown     | 2011-01-25 18:54:41 UTC |
| 192.168.3.131 [studentD1-PC] | 208.82.236.129 [kelowna.en.craiglist.ca] | HTTP Cookie | cl_def_langen.domain_craiglist.ca.path=/expressSa...  | N/A      | Unknown     | 2011-01-25 18:52:22 UTC |
| 192.168.3.131 [studentD1-PC] | 208.82.236.129 [kelowna.en.craiglist.ca] | HTTP Cookie | cl_def_langen.domain_craiglist.ca.path=/expressSa...  | N/A      | Unknown     | 2011-01-25 18:52:23 UTC |
| 192.168.3.131 [studentD1-PC] | 208.82.236.129 [kelowna.en.craiglist.ca] | HTTP Cookie | cl_def_langen.domain_craiglist.ca.path=/expressThu... | N/A      | Unknown     | 2011-01-25 18:54:29 UTC |
| 192.168.3.131 [studentD1-PC] | 208.82.236.129 [kelowna.en.craiglist.ca] | HTTP Cookie | cl_def_langen.domain_craiglist.ca.path=/expressTue... | N/A      | Unknown     | 2011-01-25 18:55:27 UTC |
| 192.168.3.131 [studentD1-PC] | 208.82.236.129 [kelowna.en.craiglist.ca] | HTTP Cookie | cl_def_langen.domain_craiglist.ca.path=/expressTue... | N/A      | Unknown     | 2011-01-25 18:55:00 UTC |
| 192.168.3.131 [studentD1-PC] | 208.82.236.129 [kelowna.en.craiglist.ca] | HTTP Cookie | cl_def_langen.domain_craiglist.ca.path=/expressTue... | N/A      | Unknown     | 2011-01-25 18:54:03 UTC |
| 192.168.3.131 [studentD1-PC] | 208.82.236.129 [kelowna.en.craiglist.ca] | HTTP Cookie | cl_def_langen.domain_craiglist.ca.path=/expressWe...  | N/A      | Unknown     | 2011-01-25 18:53:06 UTC |
| 192.168.3.131 [studentD1-PC] | 208.82.236.129 [kelowna.en.craiglist.ca] | HTTP Cookie | cl_def_langen.domain_craiglist.ca.path=/expressWe...  | N/A      | Unknown     | 2011-01-25 18:52:26 UTC |
| 192.168.3.131 [studentD1-PC] | 208.82.236.129 [kelowna.en.craiglist.ca] | HTTP Cookie | cl_def_langen.domain_craiglist.ca.path=/expressWe...  | N/A      | Unknown     | 2011-01-25 18:52:53 UTC |
| 192.168.3.131 [studentD1-PC] | 208.82.236.129 [kelowna.en.craiglist.ca] | HTTP Cookie | cl_def_langen.domain_craiglist.ca.path=/expressWe...  | N/A      | Unknown     | 2011-01-25 18:52:29 UTC |
| 192.168.3.131 [studentD1-PC] | 208.82.236.129 [kelowna.en.craiglist.ca] | HTTP Cookie | cl_def_langen.domain_craiglist.ca.path=/expressWe...  | N/A      | Unknown     | 2011-01-25 18:52:46 UTC |
| 192.168.3.131 [studentD1-PC] | 208.82.236.129 [kelowna.en.craiglist.ca] | HTTP Cookie | cl_def_langen.domain_craiglist.ca.path=/expressWe...  | N/A      | Unknown     | 2011-01-25 18:52:43 UTC |

## Step 12: You can view all sessions below

| Case Panel |                              |         |   |         |                              |                         |          |  |
|------------|------------------------------|---------|---|---------|------------------------------|-------------------------|----------|--|
| Frame nr.  | Client host                  | C. port | Server host   | S. port | Protocol (application layer) | Start time              | RTT (ms) |  |
| 1          | 192.168.3.131                | 57011   | 72.14.213.133 [clients1.google.ca]                        | 80      | HTTP                         | 2011-01-25 18:52:22 UTC |          |  |
| 3          | 192.168.3.131                | 55950   | 72.14.213.102 [clients1.google.ca]                        | 80      | HTTP                         | 2011-01-25 18:52:22 UTC |          |  |
| 13         | 192.168.3.131                | 52152   | 72.14.213.147 [www.google.com]                            | 443     | SSL                          | 2011-01-25 18:52:22 UTC |          |  |
| 26         | 192.168.3.131                | 55953   | 65.55.206.209 [mns.ca]                                    | 80      | HTTP                         | 2011-01-25 18:52:23 UTC |          |  |
| 69         | 192.168.3.131                | 55954   | 65.55.17.37 [ca.msn.com]                                  | 80      | HTTP                         | 2011-01-25 18:52:23 UTC |          |  |
| 99         | 192.168.3.131                | 55955   | 207.46.148.38 [view.admn.com]                             | 80      | HTTP                         | 2011-01-25 18:52:23 UTC |          |  |
| 110        | 192.168.3.131                | 55956   | 66.235.139.121 [imperialt112.com.7.net]                   | 80      | HTTP                         | 2011-01-25 18:52:23 UTC |          |  |
| 114        | 192.168.3.131                | 55957   | 65.55.5.232 [ad.msn.com] [b.rad.msn.com]                  | 80      | HTTP                         | 2011-01-25 18:52:23 UTC |          |  |
| 115        | 192.168.3.131                | 55958   | 65.55.239.163 [c.msn.com]                                 | 80      | HTTP                         | 2011-01-25 18:52:23 UTC |          |  |
| 133        | 192.168.3.131                | 55959   | 65.55.5.231 [d.msn.com]                                   | 80      | HTTP                         | 2011-01-25 18:52:23 UTC |          |  |
| 141        | 192.168.3.131                | 55960   | 206.108.207.139 [b.scorecardresearch.com]                 | 80      | HTTP                         | 2011-01-25 18:52:23 UTC |          |  |
| 142        | 192.168.3.131                | 55961   | 184.24.133.32 [beacon.scorecardresearch.com]              | 80      | HTTP                         | 2011-01-25 18:52:23 UTC |          |  |
| 154        | 192.168.3.131                | 55962   | 65.55.5.232 [rad.msn.com] [b.rad.msn.com]                 | 80      | HTTP                         | 2011-01-25 18:52:23 UTC |          |  |
| 162        | 192.168.3.131                | 55963   | 65.54.95.140 [col.atb.s-msn.com]                          | 80      | HTTP                         | 2011-01-25 18:52:23 UTC |          |  |
| 173        | 192.168.3.131                | 55966   | 63.215.202.48 [atfarm.medialux.com]                       | 80      | HTTP                         | 2011-01-25 18:52:23 UTC |          |  |
| 182        | 192.168.3.131                | 55967   | 63.215.202.49 [img.medialux.com]                          | 80      | HTTP                         | 2011-01-25 18:52:24 UTC |          |  |
| 195        | 192.168.3.131 [student01-PC] | 55968   | 72.14.213.101 [bookazines.clients.google.com]             | 80      | HTTP                         | 2011-01-25 18:52:25 UTC |          |  |
| 205        | 192.168.3.131 [student01-PC] | 57839   | 72.14.213.147 [www.google.com] [www.google.ca]            | 80      | HTTP                         | 2011-01-25 18:52:25 UTC |          |  |
| 202        | 192.168.3.131 [student01-PC] | 55971   | 65.55.17.37 [ca.msn.com]                                  | 80      | HTTP                         | 2011-01-25 18:52:25 UTC |          |  |
| 222        | 192.168.3.131 [student01-PC] | 55972   | 207.46.16.54 [g.msn.ca]                                   | 80      | HTTP                         | 2011-01-25 18:52:25 UTC |          |  |
| 223        | 192.168.3.131 [student01-PC] | 55973   | 65.54.95.142 [col.stc.s-msn.com] [btej.msn.com]           | 80      | HTTP                         | 2011-01-25 18:52:25 UTC |          |  |
| 290        | 192.168.3.131 [student01-PC] | 58284   | 208.82.236.129 [kelowna.craggit.ca] [kelowna.in.craig...] | 80      | HTTP                         | 2011-01-25 18:52:26 UTC |          |  |
| 308        | 192.168.3.131 [student01-PC] | 58285   | 208.82.236.129 [kelowna.craggit.ca] [kelowna.in.craig...] | 80      | HTTP                         | 2011-01-25 18:52:26 UTC |          |  |
| 325        | 192.168.3.131 [student01-PC] | 57721   | 72.14.213.105   | 443     | SSL                          | 2011-01-25 18:52:26 UTC |          |  |
| 331        | 192.168.3.131 [student01-PC] | 58272   | 208.82.236.129 [kelowna.craggit.ca] [kelowna.in.craig...] | 80      | HTTP                         | 2011-01-25 18:52:26 UTC |          |  |
| 346        | 192.168.3.131 [student01-PC] | 49673   | 72.14.213.18  | 443     | SSL                          | 2011-01-25 18:52:30 UTC |          |  |
| 387        | 192.168.3.131 [student01-PC] | 57038   | 74.217.50.10  | 80      | HTTP                         | 2011-01-25 18:52:41 UTC |          |  |
| 394        | 192.168.3.131 [student01-PC] | 52201   | 72.14.213.102 [clients1.google.ca] [calendar.google.com]  | 443     | SSL                          | 2011-01-25 18:52:42 UTC |          |  |
| 395        | 192.168.3.131 [student01-PC] | 57721   | 72.14.213.101   | 443     | SSL                          | 2011-01-25 18:52:42 UTC |          |  |

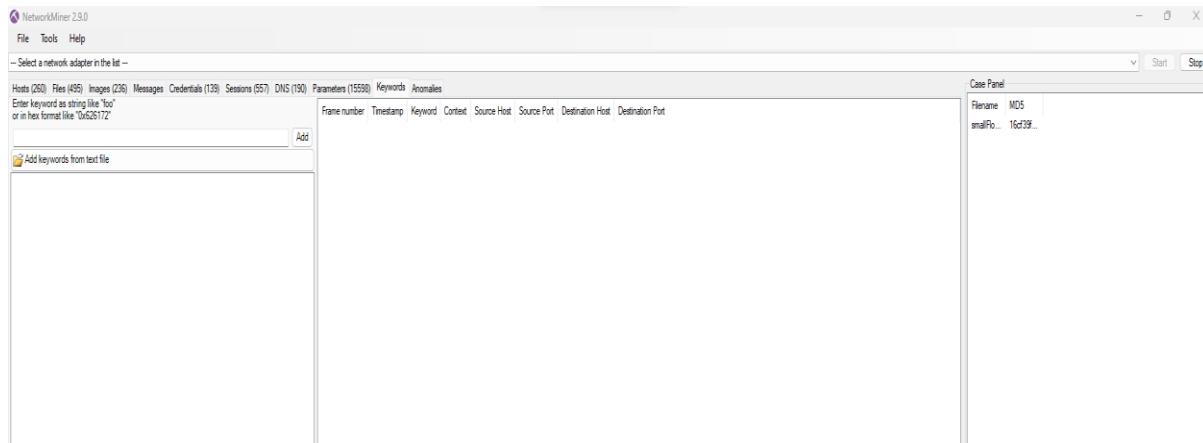
## Step 13: You can view all DNS below

| Case Panel |                         |           |             |               |             |          |                |   |
|------------|-------------------------|-----------|-------------|---------------|-------------|----------|----------------|---|
| Frame nr.  | Timestamp               | Client    | Client Port | Server        | Server Port | IP TTL   | DNS TTL (time) | Transaction ID  |
| 4262       | 2011-01-25 18:54:15 UTC | 10.0.2.15 | 50559       | 72.14.213.131 | 80          | 00:13:40 | 0:5964         | 0x0005 (CNAME) login.live.com                                     |
| 4265       | 2011-01-25 18:54:15 UTC | 10.0.2.15 | 50559       | 72.14.213.131 | 80          | 00:13:15 | 0:5964         | 0x0001 (A) login.live.com.nsac.net                                |
| 4266       | 2011-01-25 18:54:15 UTC | 10.0.2.15 | 50559       | 72.14.213.131 | 80          | 00:13:15 | 0:5964         | 0x0001 (A) login.live.com.nsac.net                                |
| 4268       | 2011-01-25 18:54:15 UTC | 10.0.2.15 | 50559       | 72.14.213.131 | 80          | 00:13:15 | 0:5964         | 0x0001 (A) login.live.com.nsac.net                                |
| 4269       | 2011-01-25 18:54:15 UTC | 10.0.2.15 | 50559       | 72.14.213.131 | 80          | 00:13:15 | 0:5964         | 0x0001 (A) login.live.com.nsac.net                                |
| 4270       | 2011-01-25 18:54:15 UTC | 10.0.2.15 | 50559       | 72.14.213.131 | 80          | 00:13:15 | 0:5964         | 0x0001 (A) login.live.com.nsac.net                                |
| 4272       | 2011-01-25 18:54:15 UTC | 10.0.2.15 | 50796       | 72.14.213.18  | 443         | 00:03:15 | 0:5964         | 0x0001 (A) us-vs-2.msac.net                                       |
| 4273       | 2011-01-25 18:54:15 UTC | 10.0.2.15 | 49796       | 72.14.213.105 | 443         | 00:03:15 | 0:6706         | 0x0005 (CNAME) messenger.hotmail.geo.messenger.msn.com.akadns.net |
| 4274       | 2011-01-25 18:54:15 UTC | 10.0.2.15 | 49796       | 72.14.213.105 | 443         | 00:03:15 | 0:6706         | messenger.hotmail.geo.messenger.msn.com.akadns.net                |
| 4275       | 2011-01-25 18:54:15 UTC | 10.0.2.15 | 49796       | 72.14.213.105 | 443         | 00:03:15 | 0:6706         | 0x0001 (A) messenger.hotmail.geo.messenger.msn.com.akadns.net     |
| 4276       | 2011-01-25 18:54:15 UTC | 10.0.2.15 | 49796       | 72.14.213.105 | 443         | 00:03:15 | 0:6706         | 64.9.254  |
| 4277       | 2011-01-25 18:54:15 UTC | 10.0.2.15 | 49796       | 72.14.213.105 | 443         | 00:03:15 | 0:6706         | za.akadns.org   |
| 4278       | 2011-01-25 18:54:15 UTC | 10.0.2.15 | 49796       | 72.14.213.105 | 443         | 00:03:15 | 0:6706         | 64.211.42.194   |
| 4279       | 2011-01-25 18:54:15 UTC | 10.0.2.15 | 49796       | 72.14.213.105 | 443         | 00:03:15 | 0:6706         | 124.40.52.133   |
| 4280       | 2011-01-25 18:54:15 UTC | 10.0.2.15 | 49796       | 72.14.213.105 | 443         | 00:03:15 | 0:6706         | 204.217.8.133   |
| 5781       | 2011-01-25 18:54:18 UTC | 10.0.2.15 | 54657       | 72.14.213.131 | 80          | 00:03:15 | 0:6460         | config.messenger.msn.com  |
| 5781       | 2011-01-25 18:54:18 UTC | 10.0.2.15 | 54657       | 72.14.213.131 | 80          | 00:03:15 | 0:6460         | config.messenger.msn.com.akadns.net                               |
| 5781       | 2011-01-25 18:54:18 UTC | 10.0.2.15 | 54657       | 72.14.213.131 | 80          | 00:03:15 | 0:6460         | 207.45.96.145   |
| 5781       | 2011-01-25 18:54:18 UTC | 10.0.2.15 | 54657       | 72.14.213.131 | 80          | 00:03:15 | 0:6460         | za.akadns.org   |
| 5781       | 2011-01-25 18:54:18 UTC | 10.0.2.15 | 54657       | 72.14.213.131 | 80          | 00:03:15 | 0:6460         | 213.254.204.197   |
| 5781       | 2011-01-25 18:54:18 UTC | 10.0.2.15 | 54657       | 72.14.213.131 | 80          | 00:03:15 | 0:6460         | 64.211.42.194   |
| 5781       | 2011-01-25 18:54:18 UTC | 10.0.2.15 | 54657       | 72.14.213.131 | 80          | 00:03:15 | 0:6460         | 124.40.52.133   |
| 5781       | 2011-01-25 18:54:18 UTC | 10.0.2.15 | 54657       | 72.14.213.131 | 80          | 00:03:15 | 0:6460         | 204.217.8.133   |
| 5810       | 2011-01-25 18:54:18 UTC | 10.0.2.15 | 57524       | 72.14.213.131 | 80          | 00:03:15 | 0:8918         | 0x0005 (CNAME) echo.edge.messenger.live.com                       |
| 5810       | 2011-01-25 18:54:18 UTC | 10.0.2.15 | 57524       | 72.14.213.131 | 80          | 00:03:15 | 0:8918         | echo.edge.messenger.msn.com.akadns.net                            |
| 5810       | 2011-01-25 18:54:18 UTC | 10.0.2.15 | 57524       | 72.14.213.131 | 80          | 00:03:15 | 0:8918         | 207.45.125.253  |
| 5810       | 2011-01-25 18:54:18 UTC | 10.0.2.15 | 57524       | 72.14.213.131 | 80          | 00:03:15 | 0:8918         | za.akadns.org   |
| 5810       | 2011-01-25 18:54:18 UTC | 10.0.2.15 | 57524       | 72.14.213.131 | 80          | 00:03:15 | 0:8918         | 64.211.42.194   |
| 5810       | 2011-01-25 18:54:18 UTC | 10.0.2.15 | 57524       | 72.14.213.131 | 80          | 00:03:15 | 0:8918         | 124.40.52.133   |
| 5810       | 2011-01-25 18:54:18 UTC | 10.0.2.15 | 57524       | 72.14.213.131 | 80          | 00:03:15 | 0:8918         | N/A (Pro v)   |

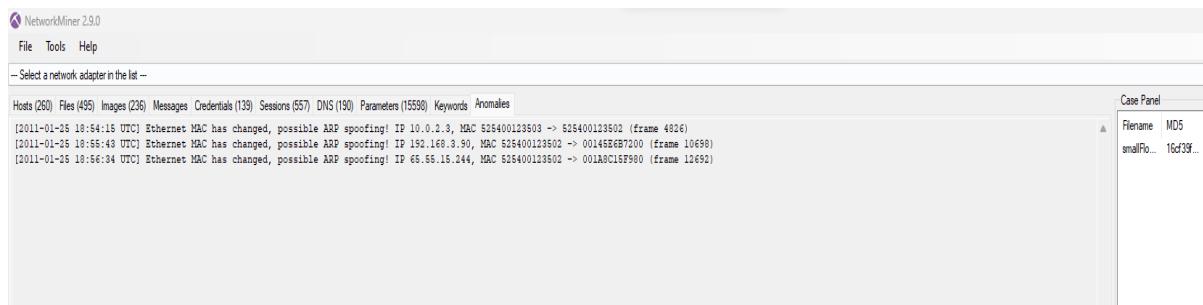
## Step 14: You can view all parameters below

| Case Panel                |  |               |                                    |             |                                    |                                    |            |            |
|---------------------------|--|---------------|------------------------------------|-------------|------------------------------------|------------------------------------|------------|------------|
| Parameter name            | Parameter value  | Frame number  | Source host                        | Source port | Destination host                   | Destination port                   | Timestamp  |            |
| PREF                      | 0 e2e350012258#f1c:U=38a6ebef0b:287c:FF=0:TM=...   | 1             | 192.168.3.131                      |             | TCP 57011                          | 72.14.213.138 [clients1.google.ca] | TCP 80     | 2011-01-25 |
| SID                       | DGAA4NAA4AB3M#7h5AXVn25vQ2RhsVLSw_7Ey...   | 1             | 192.168.3.131                      |             | TCP 57011                          | 72.14.213.138 [clients1.google.ca] | TCP 80     | 2011-01-25 |
| HSID                      | AgpM3drVtA03kzY  | 1             | 192.168.3.131                      |             | TCP 57011                          | 72.14.213.138 [clients1.google.ca] | TCP 80     | 2011-01-25 |
| NID                       | 43+o_pSZWyo5hNack17m65Qm59aBjQYL0b/APTu...   | 1             | 192.168.3.131                      |             | TCP 57011                          | 72.14.213.138 [clients1.google.ca] | TCP 80     | 2011-01-25 |
| GET                       | /complete/search?client=chrome&hl=en-US&cr...  | 1             | 192.168.3.131                      |             | TCP 57011                          | 72.14.213.138 [clients1.google.ca] | TCP 80     | 2011-01-25 |
| Host                      | clients1.google.ca   | 1             | 192.168.3.131                      |             | TCP 57011                          | 72.14.213.138 [clients1.google.ca] | TCP 80     | 2011-01-25 |
| User-Agent                | Mozilla/5.0 (Windows NT 6.1; en-US) AppleWebKit/535.2 (KHTML, like Gecko) Chrome/19.0.1084.57 Safari/535.2 | 1             | 192.168.3.131                      |             | TCP 57011                          | 72.14.213.138 [clients1.google.ca] | TCP 80     | 2011-01-25 |
| Accept-Charset            | ISO-8859-1;utf-8;q=0.7,*;q=0.3   | 1             | 192.168.3.131                      |             | TCP 57011                          | 72.14.213.138 [clients1.google.ca] | TCP 80     | 2011-01-25 |
| Cookie                    |  | 1             | 192.168.3.131                      |             | TCP 57011                          | 72.14.213.138 [clients1.google.ca] | TCP 80     | 2011-01-25 |
| client                    | chrome   | 1             | 192.168.3.131                      |             | TCP 57011                          | 72.14.213.138 [clients1.google.ca] | TCP 80     | 2011-01-25 |
| en-US                     | 1  | 192.168.3.131 |                                    |             | TCP 57011                          | 72.14.213.138 [clients1.google.ca] | TCP 80     | 2011-01-25 |
| or                        | 1  | 192.168.3.131 |                                    |             | TCP 57011                          | 72.14.213.138 [clients1.google.ca] | TCP 80     | 2011-01-25 |
| HTTP Response Status Code | 200 OK   | 2             | 72.14.213.138 [clients1.google.ca] | TCP 80      | 192.168.3.131                      | TCP 80                             | 2011-01-25 |            |
| Date                      | Tue, 25 Jan 2011 09:56 GMT   | 2             | 72.14.213.138 [clients1.google.ca] | TCP 80      | 192.168.3.131                      | TCP 80                             | 2011-01-25 |            |
| Expires                   | Tue, 25 Jan 2011 09:56 GMT   | 2             | 72.14.213.138 [clients1.google.ca] | TCP 80      | 192.168.3.131                      | TCP 80                             | 2011-01-25 |            |
| Cache-Control             | private, max-age=3600  | 2             | 72.14.213.138 [clients1.google.ca] | TCP 80      | 192.168.3.131                      | TCP 80                             | 2011-01-25 |            |
| Content-Type              | text/javascript; charset=UTF-8   | 2             | 72.14.213.138 [clients1.google.ca] | TCP 80      | 192.168.3.131                      | TCP 80                             | 2011-01-25 |            |
| Content-Encoding          | gzip   | 2             | 72.14.213.138 [clients1.google.ca] | TCP 80      | 192.168.3.131                      | TCP 80                             | 2011-01-25 |            |
| Server                    | gws  | 2             | 72.14.213.138 [clients1.google.ca] | TCP 80      | 192.168.3.131                      | TCP 80                             | 2011-01-25 |            |
| Content-Length            | 115  | 2             | 72.14.213.138 [clients1.google.ca] | TCP 80      | 192.168.3.131                      | TCP 80                             | 2011-01-25 |            |
| X-XSS-Protection          | 1; mode=block  | 2             | 72.14.213.138 [clients1.google.ca] | TCP 80      | 192.168.3.131                      | TCP 80                             | 2011-01-25 |            |
| PREF                      | 0 e2e350012258#f1c:U=38a6ebef0b:287c:FF=0:TM=...   | 7             | 192.168.3.131                      | 55950       | 72.14.213.102 [clients1.google.ca] | TCP 80                             | 2011-01-25 |            |

## Step 15: You can view all keywords below



## Step 16: You can view any anomalies below



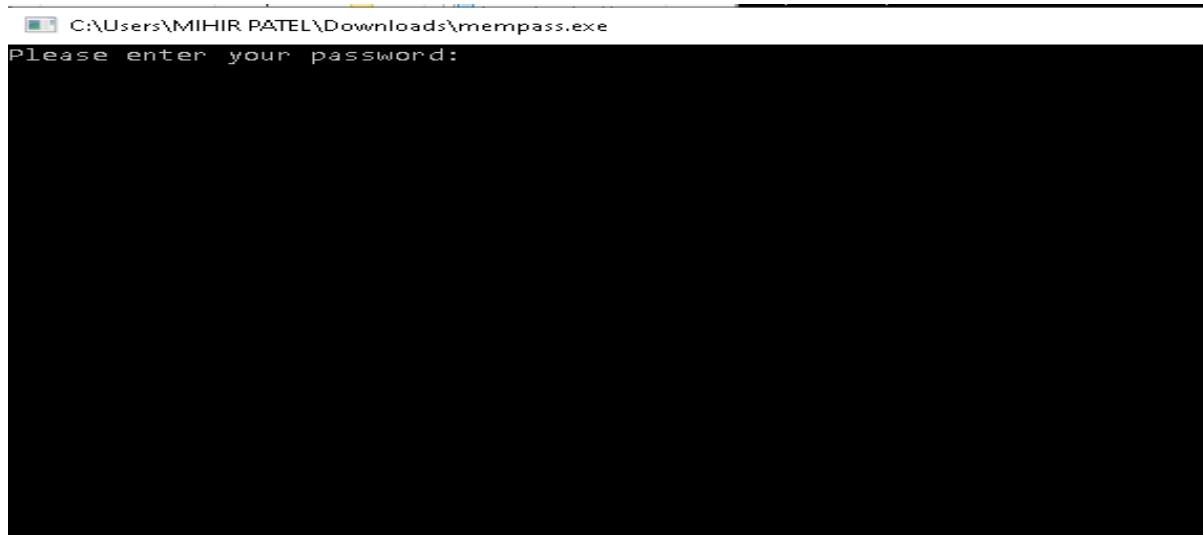
## Practical: 6

### 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 application whose 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, clears the 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 press Enter



#### 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.

```
C:\> Command Prompt
C:\Users\MIHIR PATEL\Downloads>pmdump.exe

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

Usage: pmdump <pid> <filename>
      - dumps the process memory contents to a file
      pmdump <pid> <filename> -full
      - dumps the process memory contents to a file with holes included and
        zero filled
      pmdump -list
      - lists all running processes and their PID's

C:\> Command Prompt
C:\Users\MIHIR PATEL\Downloads>pmdump -list

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

  0 - System idle process
  4 - System
 100 - Registry
 600 - smss.exe
 892 - csrss.exe
1004 - wininit.exe
 728 - services.exe
 732 - lsass.exe
 788 - svchost.exe
1048 - fontdrvhost.exe
1092 - WUDFHost.exe
1296 - svchost.exe
1344 - svchost.exe
1592 - svchost.exe
1660 - svchost.exe
1712 - svchost.exe
1720 - svchost.exe
1788 - svchost.exe
1800 - svchost.exe
1980 - svchost.exe
1996 - svchost.exe
2088 - svchost.exe
2132 - svchost.exe
2200 - svchost.exe
2236 - svchost.exe
2248 - atiesrxx.exe
2296 - svchost.exe
2376 - wscript.exe
2496 - svchost.exe
2600 - svchost.exe
2784 - svchost.exe
2800 - svchost.exe
2808 - svchost.exe
2876 - mempass.exe
```

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

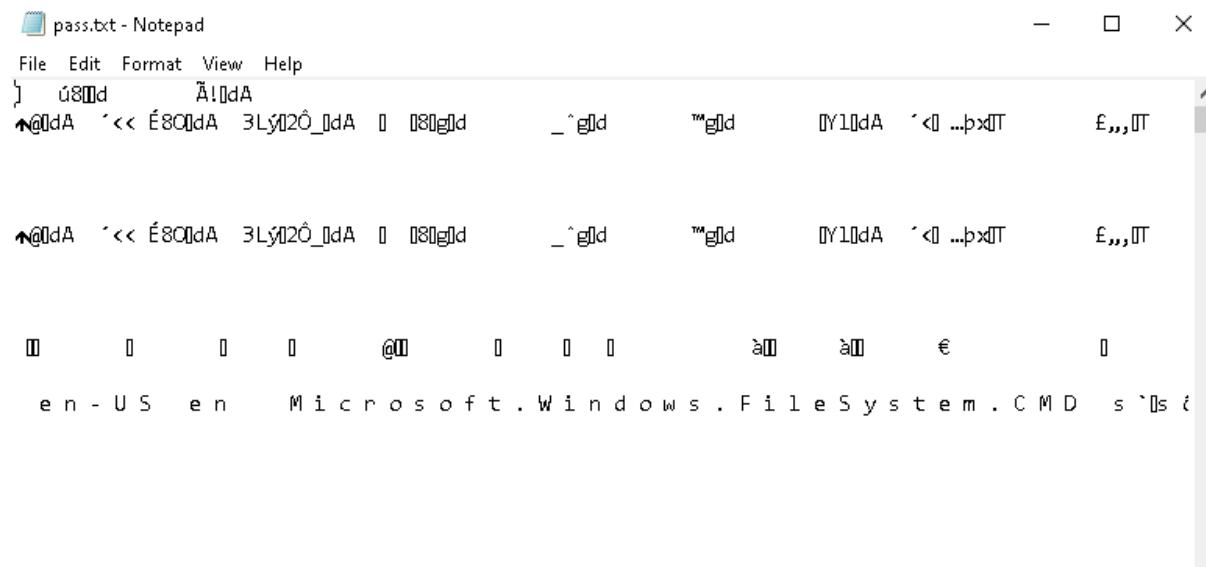


**Step 4: Now Run pmdump command and give thePID of mempass i.e 8808 as input and givefilename i.e pass.txt in which it can dump the entire memory of mempass program**

```
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

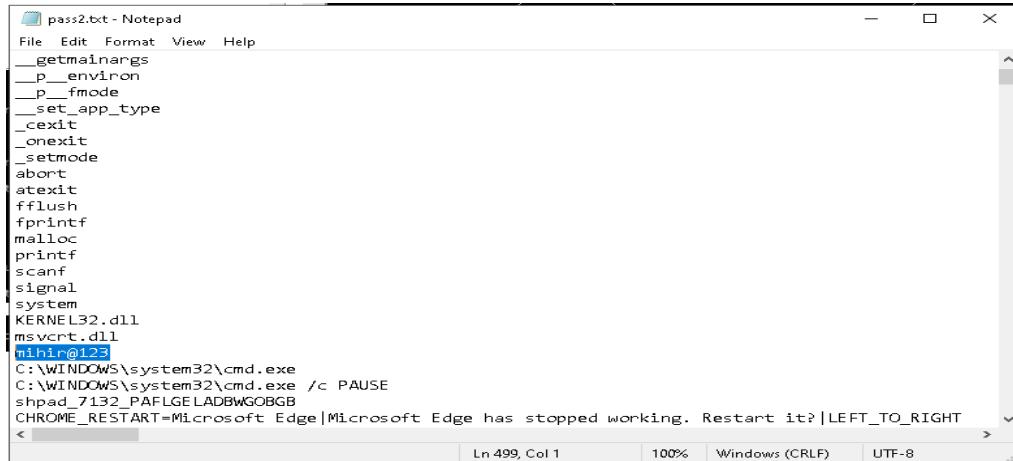
Strings v2.53 - Search for ANSI and Unicode strings in binary images.
Copyright (C) 1999-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

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 for which 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



The screenshot shows a Windows Notepad window titled "pass2.txt - Notepad". The window contains a list of strings extracted from the input file "pass.txt". The strings include system-related functions like \_getmainargs, \_\_P\_\_environ, \_\_P\_\_fmode, \_\_set\_app\_type, \_cexit, \_onexit, \_setmode, abort, atexit, fflush, fprintf, malloc, printf, scanf, signal, and system. It also lists DLL names like KERNEL32.dll and msvcrt.dll. A password, "mihir@123", is highlighted in blue. Below the strings, there is a command-line session showing the execution of cmd.exe and its pause operation. At the bottom of the window, there is a message from Microsoft Edge indicating a restart.

```
File Edit Format View Help
__getmainargs
__P__environ
__P__fmode
__set_app_type
_cexit
_onexit
_setmode
abort
atexit
fflush
fprintf
malloc
printf
scanf
signal
system
KERNEL32.dll
msvcrt.dll
mihir@123
C:\WINDOWS\system32\cmd.exe
C:\WINDOWS\system32\cmd.exe /c PAUSE
shpad_7132_PAFLGE LADBwGOBGB
CHROME_RESTART=Microsoft Edge|Microsoft Edge has stopped working. Restart it?|LEFT_TO_RIGHT
< Ln 499, Col 1 | 100% | Windows (CRLF) | UTF-8 >
```

## Practical: 7

### Aim: Using Data Acquisition Tools [ProDiscover]

#### Theory

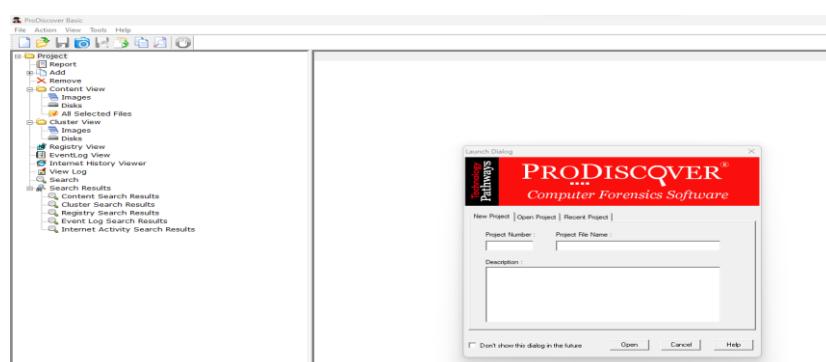
ProDiscover Forensics is a comprehensive digital forensics software that empowers investigators to capture key evidence from computer systems. ProDiscover has capabilities to handle all aspects of an in-depth forensic investigation to collect, preserve, filter, and analyse evidence.

#### Data Acquisition Tools:

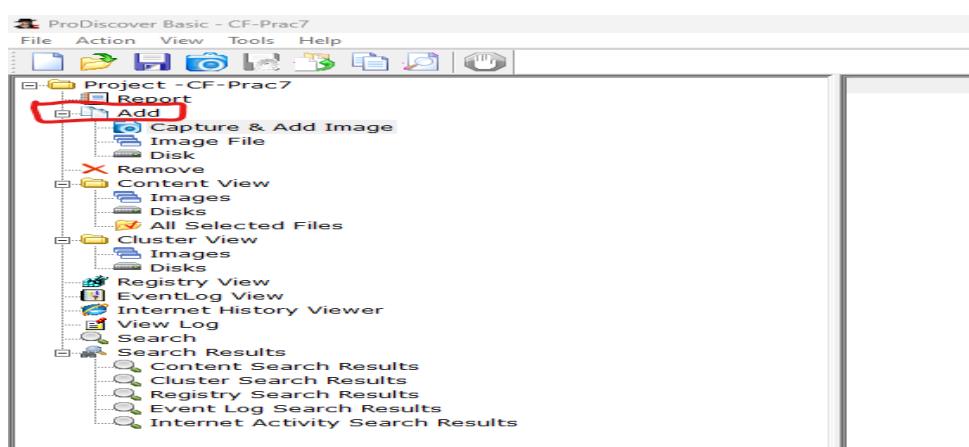
USB WRITE BLOCKER + FTK Imager

- 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 be able 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. It scans a hard drive looking for various information.

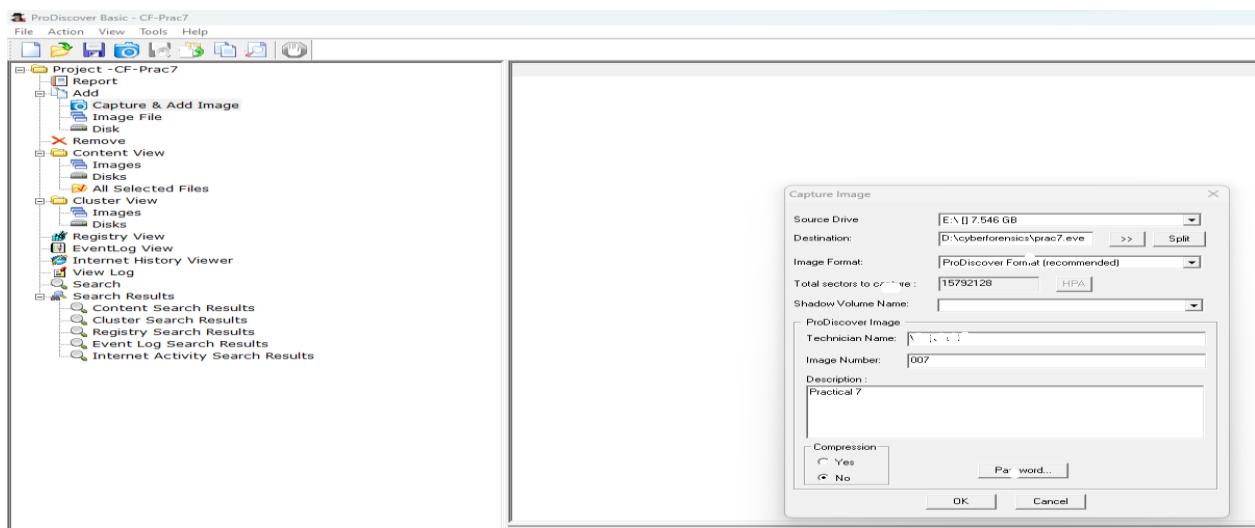
#### Step 1: Open ProDiscover Basic and start with new project.



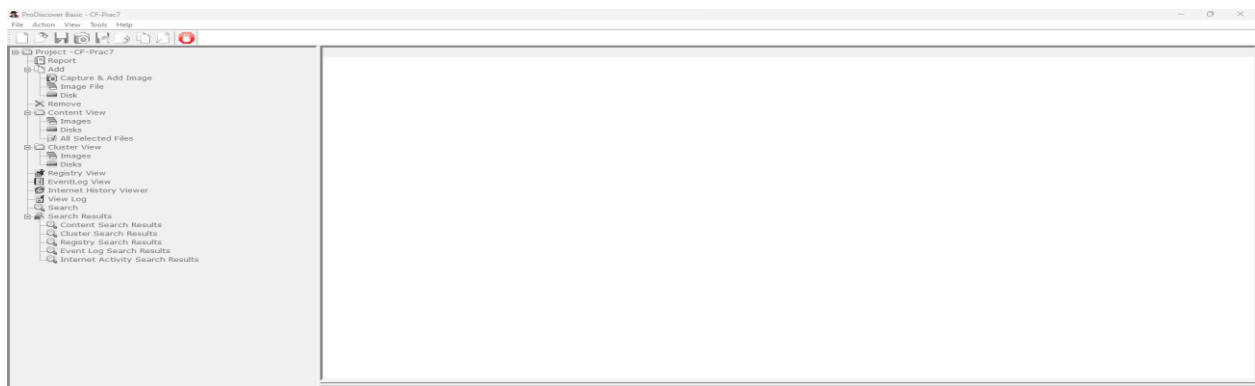
#### Step 2: The new created project appears on the left side – Go on add and select Capture and Add Image



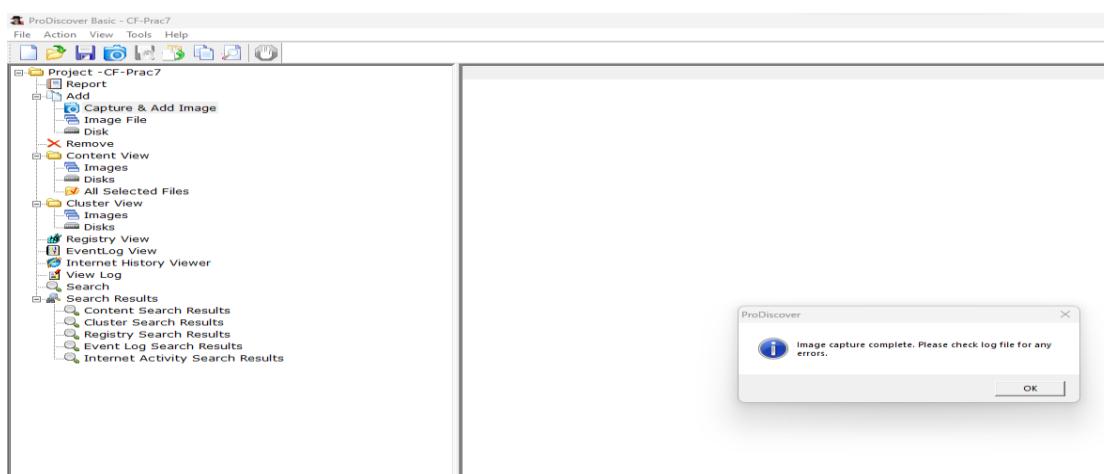
**Step 3: Select your Source Drive file from the drop down, select Destination path and add Technician Name, Image Number and Description. Click on ok**



**Step 4: The image capturing will start processing.**



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



| File Explorer View |                                  |                          |                  |                |               |             |         |                |                |                |                  |
|--------------------|----------------------------------|--------------------------|------------------|----------------|---------------|-------------|---------|----------------|----------------|----------------|------------------|
| File Path          |                                  | Select                   | File Name        | File Extension | Size          | Attributes  | Deleted | Created Date   | Modified Date  | Accessed Date  | Parent Folder    |
| Project - CF-Prac7 | Report                           | <input type="checkbox"/> | AII_prac         |                |               | - d - s h - | NO      | 09/28/2024 ... | 09/28/2024 ... | 09/28/2024 ... | D:\cyberforen... |
|                    | Add                              | <input type="checkbox"/> | FOUND.000        |                |               | - d - s h - | NO      | 10/01/2024 ... | 10/01/2024 ... | 10/01/2024 ... | D:\cyberforen... |
|                    | Capture & Add Image              | <input type="checkbox"/> | Ml_3             |                |               | - d - s h - | NO      | 10/05/2024 ... | 10/05/2024 ... | 10/05/2024 ... | D:\cyberforen... |
|                    | Image File                       | <input type="checkbox"/> | 89e097c5-2...    |                |               | - d - s h - | YES     | 01/30/2025 ... | 01/30/2025 ... | 01/30/2025 ... | D:\cyberforen... |
|                    | Disk                             | <input type="checkbox"/> | 978afce1-4b...   |                |               | - d - s h - | YES     | 11/12/2023 ... | 11/12/2023 ... | 11/12/2023 ... | D:\cyberforen... |
|                    | Remove                           | <input type="checkbox"/> | 1MscIT mat...    |                |               | - d - s h - | NO      | 12/08/2023 ... | 11/18/2023 ... | 04/05/2024 ... | D:\cyberforen... |
|                    | Content View                     | <input type="checkbox"/> | gnis3 img fil... |                |               | - d - s h - | NO      | 03/14/2024 ... | 03/14/2024 ... | 04/18/2024 ... | D:\cyberforen... |
|                    | Images                           | <input type="checkbox"/> | Counter Stri...  |                |               | - d - s h - | NO      | 03/18/2024 ... | 03/14/2024 ... | 04/18/2024 ... | D:\cyberforen... |
|                    | D:\cyberforensics\prac7.eve      | <input type="checkbox"/> | jdk1.8.0_241     |                |               | - d - s h - | YES     | 04/03/2024 ... | 04/02/2024 ... | 04/03/2024 ... | D:\cyberforen... |
|                    | Disk                             | <input type="checkbox"/> | jdk1.8.0_241     |                |               | - d - s h - | NO      | 04/05/2024 ... | 04/05/2024 ... | 04/05/2024 ... | D:\cyberforen... |
|                    | All Selected Files               | <input type="checkbox"/> | HADOOP           |                |               | - d - s h - | NO      | 04/05/2024 ... | 04/05/2024 ... | 04/05/2024 ... | D:\cyberforen... |
|                    | Cluster View                     | <input type="checkbox"/> | New folder       |                |               | - d - s h - | YES     | 06/25/2024 ... | 06/25/2024 ... | 06/25/2024 ... | D:\cyberforen... |
|                    | Images                           | <input type="checkbox"/> | Computer Vi...   |                |               | - d - s h - | NO      | 06/25/2024 ... | 06/25/2024 ... | 06/25/2024 ... | D:\cyberforen... |
|                    | Disk                             | <input type="checkbox"/> | All Files        |                |               | - d - s h - | NO      | 01/01/1970 ... | 01/01/1970 ... | 01/01/1970 ... | D:\cyberforen... |
|                    | Registry View                    | <input type="checkbox"/> | System Volu...   |                | 8,192 b...    | - d - s h - | NO      | 10/30/2023 ... | 10/30/2023 ... | 04/05/2024 ... | D:\cyberforen... |
|                    | EventLog View                    | <input type="checkbox"/> | New Microso...   | docx           | 13,744 ...    | a - - -     | NO      | 10/07/2024 ... | 10/07/2024 ... | 01/19/2025 ... | D:\cyberforen... |
|                    | Internet History Viewer          | <input type="checkbox"/> | practical S-B,C  | docx           | 2,298,014 ... | a - - -     | NO      | 01/28/2025 ... | 01/28/2025 ... | 01/30/2025 ... | D:\cyberforen... |
|                    | View Log                         | <input type="checkbox"/> | blockchain       | docx           | 11,938 ...    | a - - -     | NO      | 12/02/2024 ... | 12/02/2024 ... | 01/23/2025 ... | D:\cyberforen... |
|                    | Search                           | <input type="checkbox"/> | Doc1             | docx           | 79,360 ...    | a - - -     | NO      | 01/11/2025 ... | 01/11/2025 ... | 01/27/2025 ... | D:\cyberforen... |
|                    | Search Results                   | <input type="checkbox"/> | cyberforen...    | pdf            | 5,156,810 ... | a - - -     | NO      | 01/18/2025 ... | 01/17/2025 ... | 01/28/2025 ... | D:\cyberforen... |
|                    | Content Search Results           | <input type="checkbox"/> | cyberfor_prac5   | docx           | 1,557,587 ... | a - - -     | NO      | 01/23/2025 ... | 01/23/2025 ... | 01/29/2025 ... | D:\cyberforen... |
|                    | Cluster Search Results           | <input type="checkbox"/> | cyberfor_pra...  | docx           | 1,537,792 ... | a - - -     | NO      | 01/18/2025 ... | 01/19/2025 ... | 01/27/2025 ... | D:\cyberforen... |
|                    | Registry Search Results          | <input type="checkbox"/> | ä2               | PNG            | 17,801 ...    | a - - -     | YES     | 11/08/2023 ... | 11/07/2023 ... | 11/08/2023 ... | D:\cyberforen... |
|                    | Event Log Search Results         | <input type="checkbox"/> | ä3               | PNG            | 17,382 ...    | a - - -     | YES     | 11/08/2023 ... | 11/07/2023 ... | 11/08/2023 ... | D:\cyberforen... |
|                    | Internet Activity Search Results | <input type="checkbox"/> | ä4               | PNG            | 10,505 ...    | a - - -     | YES     | 11/09/2023 ... | 11/07/2023 ... | 11/08/2023 ... | D:\cyberforen... |

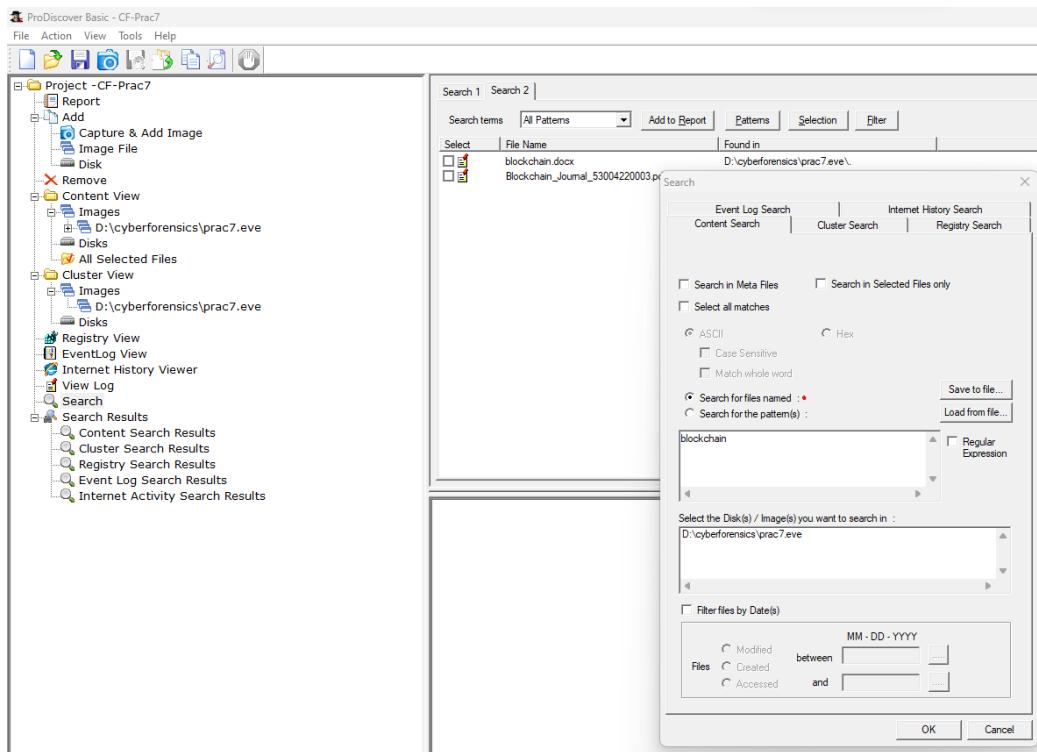
Step 7: Click on any of the file and type a comment.

| File                                | Action           | View           | Tools           | Help       |         |                |                |                |                   |
|-------------------------------------|------------------|----------------|-----------------|------------|---------|----------------|----------------|----------------|-------------------|
| File Explorer                       |                  |                |                 |            |         |                |                |                |                   |
| Project - CF-Prac7                  |                  |                |                 |            |         |                |                |                |                   |
| Select                              | File Name        | File Extension | Size            | Attributes | Deleted | Created Date   | Modified Date  | Accessed Date  | Parent Folder     |
| <input type="checkbox"/>            | à2               | PNG            | 17,801 ...      | a -----    | YES     | 11/08/2023 ... | 11/07/2023 ... | 11/08/2023 ... | D:\cyberforens... |
| <input type="checkbox"/>            | à3               | PNG            | 17,382 ...      | a -----    | YES     | 11/08/2023 ... | 11/07/2023 ... | 11/08/2023 ... | D:\cyberforen...  |
| <input type="checkbox"/>            | à4               | PNG            | 10,505 ...      | a -----    | YES     | 11/08/2023 ... | 11/07/2023 ... | 11/08/2023 ... | D:\cyberforen...  |
| <input type="checkbox"/>            | à5               | PNG            | 107,591 ...     | a -----    | YES     | 11/08/2023 ... | 11/07/2023 ... | 11/08/2023 ... | D:\cyberforen...  |
| <input type="checkbox"/>            | Metasploit R...  | pdf            | 54,473,628 ...  | a -----    | NO      | 11/08/2023 ... | 09/14/2023 ... | 04/05/2024 ... | D:\cyberforen...  |
| <input type="checkbox"/>            | kali-linux-20... | iso            | 4,194,304,0 ... | a -----    | YES     | 09/26/2023 ... | 09/23/2023 ... | 11/08/2023 ... | D:\cyberforen...  |
| <input type="checkbox"/>            | Anaconda3-20...  | exe            | 640,016,16 ...  | a -----    | YES     | 09/26/2023 ... | 09/23/2023 ... | 11/08/2023 ... | D:\cyberforen...  |
| <input type="checkbox"/>            | Sploit Prac T... | iso            | 233,769,0 ...   | a -----    | NO      | 11/10/2023 ... | 11/05/2023 ... | 01/30/2025 ... | D:\cyberforen...  |
| <input type="checkbox"/>            | SPCM_S3004...    | docx           | 2,759,117,7 ... | a -----    | NO      | 12/01/2023 ... | 01/23/2023 ... | 01/10/2024 ... | D:\cyberforen...  |
| <input type="checkbox"/>            | SPCM_S3004_...   | docx           | 20,296,694 ...  | a -----    | YES     | 12/08/2023 ... | 12/08/2023 ... | 12/08/2023 ... | D:\cyberforen...  |
| <input type="checkbox"/>            | àWR00001         | TMP            | 20,296,694 ...  | a -----    | YES     | 12/08/2023 ... | 12/08/2023 ... | 12/08/2023 ... | D:\cyberforen...  |
| <input type="checkbox"/>            | SPCM_S3004...    | docx           | 20,294,198 ...  | a -----    | NO      | 12/08/2023 ... | 12/08/2023 ... | 01/11/2025 ... | D:\cyberforen...  |
| <input type="checkbox"/>            | SPCM_S3004_...   | pdf            | 10,657,018 ...  | a -----    | NO      | 12/08/2023 ... | 12/08/2023 ... | 12/08/2023 ... | D:\cyberforen...  |
| <input type="checkbox"/>            | Data_sceince     | txt            | 50,183 ...      | a -----    | NO      | 03/03/2024 ... | 03/03/2024 ... | 03/03/2024 ... | D:\cyberforen...  |
| <input checked="" type="checkbox"/> | Soft_computer    | txt            | 25,448 ...      | a -----    | NO      | 03/03/2024 ... | 03/03/2024 ... | 04/05/2024 ... | D:\cyberforen...  |
| <input type="checkbox"/>            | GNS3-0.8.6...    | exe            | 62,360,151 ...  | a -----    | NO      | 03/14/2024 ... | 11/19/2019 ... | 01/30/2020 ... | D:\cyberforen...  |
| <input type="checkbox"/>            | scilab-5.5.2...  | exe            | 136,106,24 ...  | a -----    | YES     | 03/18/2024 ... | 08/11/2016 ... | 11/04/2024 ... | D:\cyberforen...  |
| <input type="checkbox"/>            | commands-p...    | txt            |                 |            |         | 03/28/2024 ... | 03/28/2024 ... | 03/28/2024 ... | D:\cyberforen...  |
| <input type="checkbox"/>            | Nishi-prac9      | docx           |                 |            |         | 03/28/2024 ... | 03/28/2024 ... | 10/01/2024 ... | D:\cyberforen...  |
| <input type="checkbox"/>            | hadoop-3.1...    | gz             |                 |            |         | 04/05/2024 ... | 04/02/2024 ... | 04/05/2024 ... | D:\cyberforen...  |
| <input type="checkbox"/>            | jdk-Bu241-w...   | exe            |                 |            |         | 04/05/2024 ... | 04/02/2024 ... | 11/04/2024 ... | D:\cyberforen...  |
| <input type="checkbox"/>            | GNS3-2.2.46...   | exe            |                 |            |         | 04/18/2024 ... | 04/18/2024 ... | 11/04/2024 ... | D:\cyberforen...  |
| <input type="checkbox"/>            | object_detec...  | py             |                 |            |         | 04/18/2024 ... | 05/09/2024 ... | 05/09/2024 ... | D:\cyberforen...  |
| <input type="checkbox"/>            | Ml_P6            | docx           |                 |            |         | 09/16/2024 ... | 09/16/2024 ... | 10/01/2024 ... | D:\cyberforen...  |

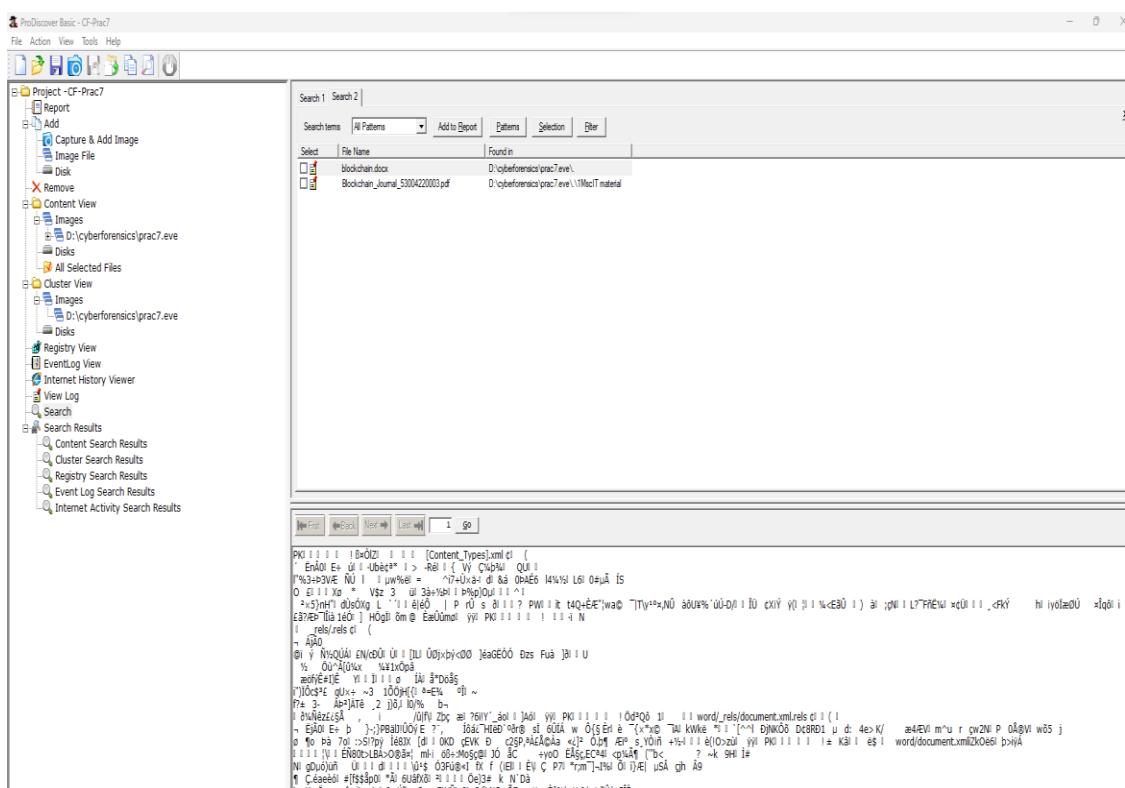
**Step 8: To see the cluster view, click on cluster view tab on the left side panel.**

The screenshot shows the ProDiscover Basic software interface. On the left, a tree view displays the project structure under 'Project - CF-Prac7'. The 'Report' section contains 'Capture & Add Image', 'Image File', and 'Disk'. The 'Remove' section has an 'X Remove' option. 'Content View' includes 'Images' (with a file named 'D:\cyberforensics\prac7.eve'), 'Disks', and 'All Selected Files'. 'Cluster View' includes 'Images' (with a file named 'D:\cyberforensics\prac7.eve') and 'Disks'. 'EventLog View', 'Internet History Viewer', and 'Log' sections are also present. 'Search' and 'Search Results' sections follow, with links to 'Content Search Results', 'Cluster Search Results', 'Registry Search Results', 'Event Log Search Results', and 'Internet Activity Search Results'. On the right, a large hex dump window shows a file starting with 'FOO'. The first byte is highlighted in red as 'Selected Cluster'. A legend below the dump defines colors: green for 'Used', blue for 'Unused', dark green for 'Boot Sector & Partition Data', and grey for 'Selected Cluster'. Navigation buttons for 'First', 'Back', 'Next', and 'Last' are at the bottom of the dump window.

**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.

ProDiscover Basic - CF-Prac7

File Action View Tools Help

Project - CF-Prac7

- Report
  - Add
    - Capture & Add Image
    - Image File
    - Disk
  - Remove
  - Content View
    - Images
      - D:\cyberforensics\prac7.eve
    - Disk
    - All Selected Files
  - Cluster View
    - Images
      - D:\cyberforensics\prac7.eve
    - Disk
  - Registry View
  - EventLog View
  - Internet History Viewer
  - View Log
  - Search
    - Content Search Results
    - Cluster Search Results
    - Registry Search Results
    - Event Log Search Results
    - Internet Activity Search Results

**Evidence Report for Project: CF-Prac7**

**Project Number:** 1

**Project Description:**

**Image Files:**

**File Name:** D:\cyberforensics\prac7.eve  
**Image File Type:** DFT Image  
**File Name Extension:** .eve  
**Technician Name:** 11.11.24  
**Date:** 02/01/2025  
**Time:** 15:04:34  
**MD5 Checksum:** ece635ef9ce33aa58d6263900a4427f3  
**Checksum Validated:** No  
**Compressed Image:** No

**Time Zone Information:**

Time Zone: (GMT+05:30) Calcutta, Chennai, Mumbai, New Delhi (India Standard Time)  
 Daylight savings (summertime) was in effect: No  
 Time Zone information obtained automatically from remote system/image.

**Hard Disk:** D:\cyberforensics\prac7.eve

Volume Name: NO NAME  
 Volume Serial Number : 9846-A837  
 File System: FAT32  
 Bytes Per Sector: 512  
 Total Clusters: 197316  
 Sectors per cluster: 8  
 Total Sectors: 15824896  
 Hidden Sectors: 2048  
 Total Capacity: 7912448 KB  
 Start Sector: 0  
 End Sector: 15824895

**Disks:**

**Evidence of Interest:**

Total Evidence Items of Interest: 1

Hard Disk: E:\  
 List of Files:

D:\cyberforensics\prac7.eve\soft\_comput.txt  
 MD5 Checksum: 162820359E7278A422994A70AE5791B  
 Created:03/03/2024 18:49Modified:03/03/2024 14:40Last Accessed:04/05/2024 00:00  
 MFT &STANDARD\_INFO entry modified: Not available  
 MFT \$FILE\_NAME entry modified:Not available

| Cluster Chain: | Start Cluster     | End Cluster       | Total Clusters |
|----------------|-------------------|-------------------|----------------|
|                | 13664360 (D08068) | 13664415 (D0809F) | 56             |

**Investigator's comments:** practical file

---

D:\cyberforensics\prac7.eve Hard Disk E:\ : **Evidence of Interest:** 1

ProDiscover Basic - CF-Prac7

File Action View Tools Help

Project - CF-Prac7

- Report
  - Add
    - Capture & Add Image
    - Image File
    - Disk
  - Remove
  - Content View
    - Images
      - D:\cyberforensics\prac7.eve
    - Disk
    - All Selected Files
  - Cluster View
    - Images
      - D:\cyberforensics\prac7.eve
    - Disk
  - Registry View
  - EventLog View
  - Internet History Viewer
  - View Log
  - Search
    - Content Search Results
    - Cluster Search Results
    - Registry Search Results
    - Event Log Search Results
    - Internet Activity Search Results

**Evidence Report for Project: CF-Prac7**

**Time Zone Information:**

Time Zone: (GMT+05:30) Calcutta, Chennai, Mumbai, New Delhi (India Standard Time)  
 Daylight savings (summertime) was in effect: No  
 Time Zone information obtained automatically from remote system/image.

**Hard Disk:** D:\cyberforensics\prac7.eve

Volume Name: NO NAME  
 Volume Serial Number : 9846-A837  
 File System: FAT32  
 Bytes Per Sector: 512  
 Total Clusters: 197316  
 Sectors per cluster: 8  
 Total Sectors: 15824896  
 Hidden Sectors: 2048  
 Total Capacity: 7912448 KB  
 Start Sector: 0  
 End Sector: 15824895

**Disks:**

**Evidence of Interest:**

Total Evidence Items of Interest: 1

Hard Disk: E:\  
 List of Files:

D:\cyberforensics\prac7.eve\soft\_comput.txt  
 MD5 Checksum: 162820359E7278A422994A70AE5791B  
 Created:03/03/2024 18:49Modified:03/03/2024 14:40Last Accessed:04/05/2024 00:00  
 MFT &STANDARD\_INFO entry modified: Not available  
 MFT \$FILE\_NAME entry modified:Not available

| Cluster Chain: | Start Cluster     | End Cluster       | Total Clusters |
|----------------|-------------------|-------------------|----------------|
|                | 13664360 (D08068) | 13664415 (D0809F) | 56             |

**Investigator's comments:** practical file

---

D:\cyberforensics\prac7.eve Hard Disk E:\ : **Evidence of Interest:** 1

**Clusters of Interest:**

**File Signature Mismatch:**

**Registry Keys of Interest:**

**Event Log Entries of Interest:**

**Internet Activity Information:**

---

**Search Results:**

**Project Notes:**

This Report was created by ProDiscover

## **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 image and 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 in WAV files.
- SSuit PicSel is another free portable application to hide text inside an image file but it takes 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.

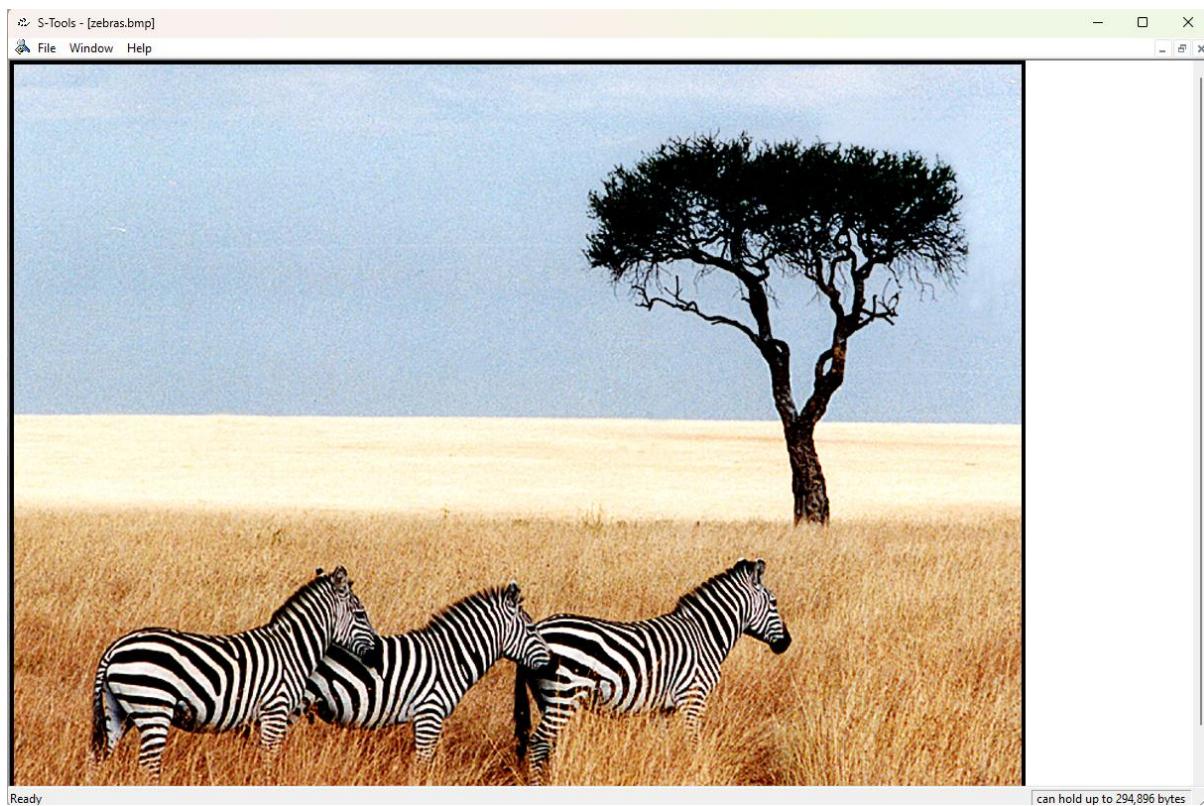
You can do the following three tasks through this window:

- 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.

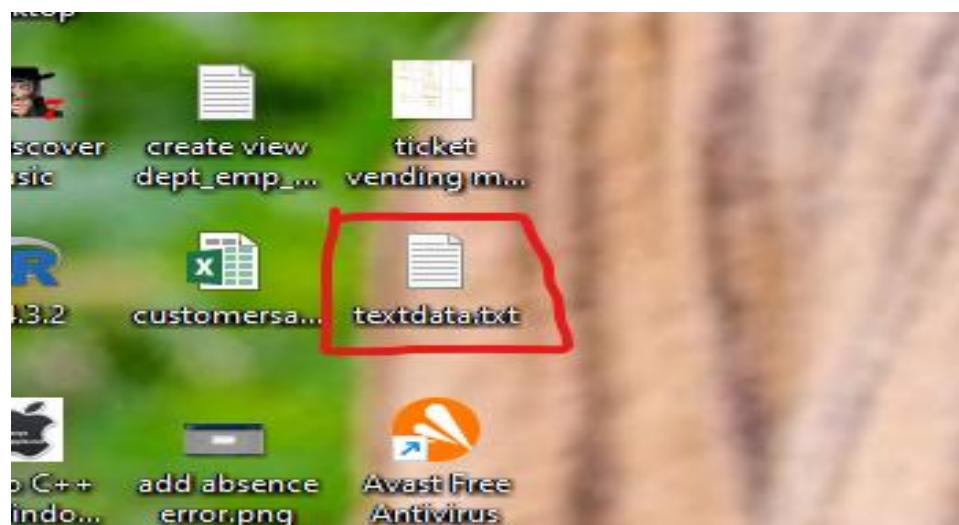
In order to extract the original confidential file from the image file it was embedded into, you can right- click the image file from the file browser and select “Open With Other Application” from the menu and then select Stegosuite from the Select Application list as follows:

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.

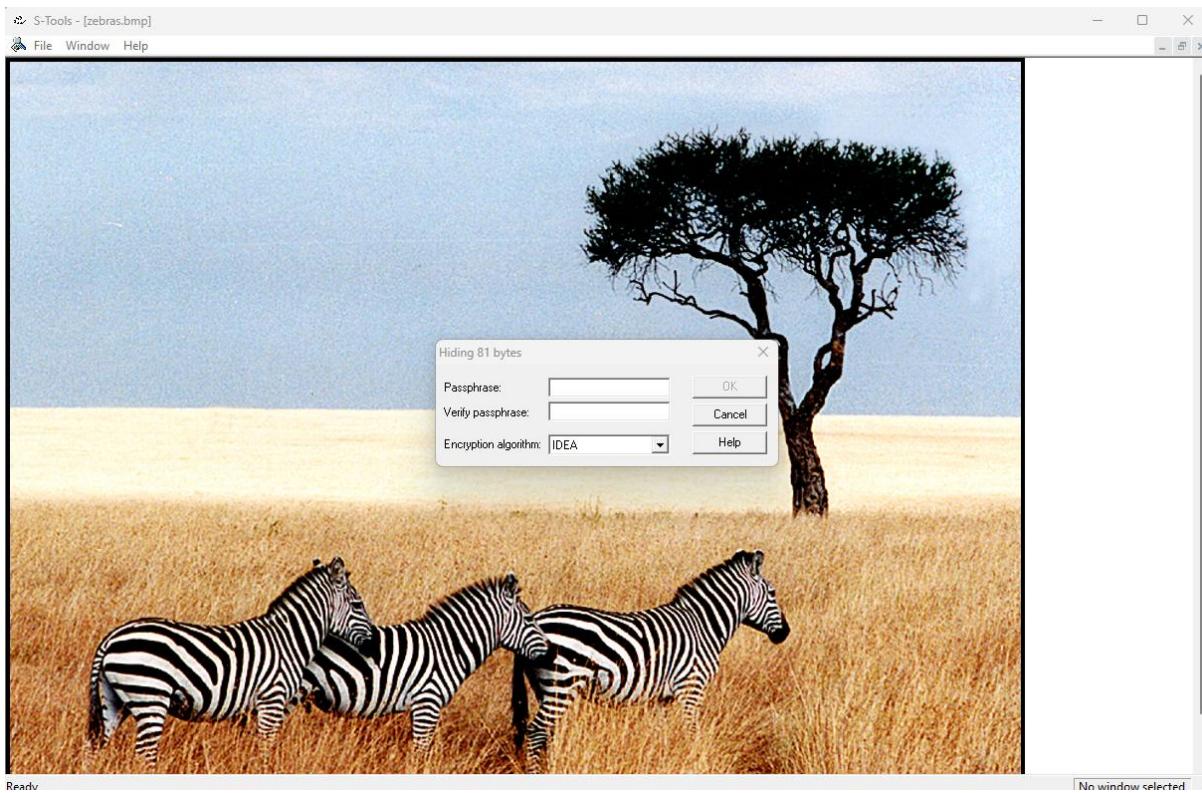
**Step 1: Download S-tool using giving link**  
<https://www.cs.vu.nl/~ast/books/mos2/zebras.html>-> then drag and drop the Zebra.bmp image



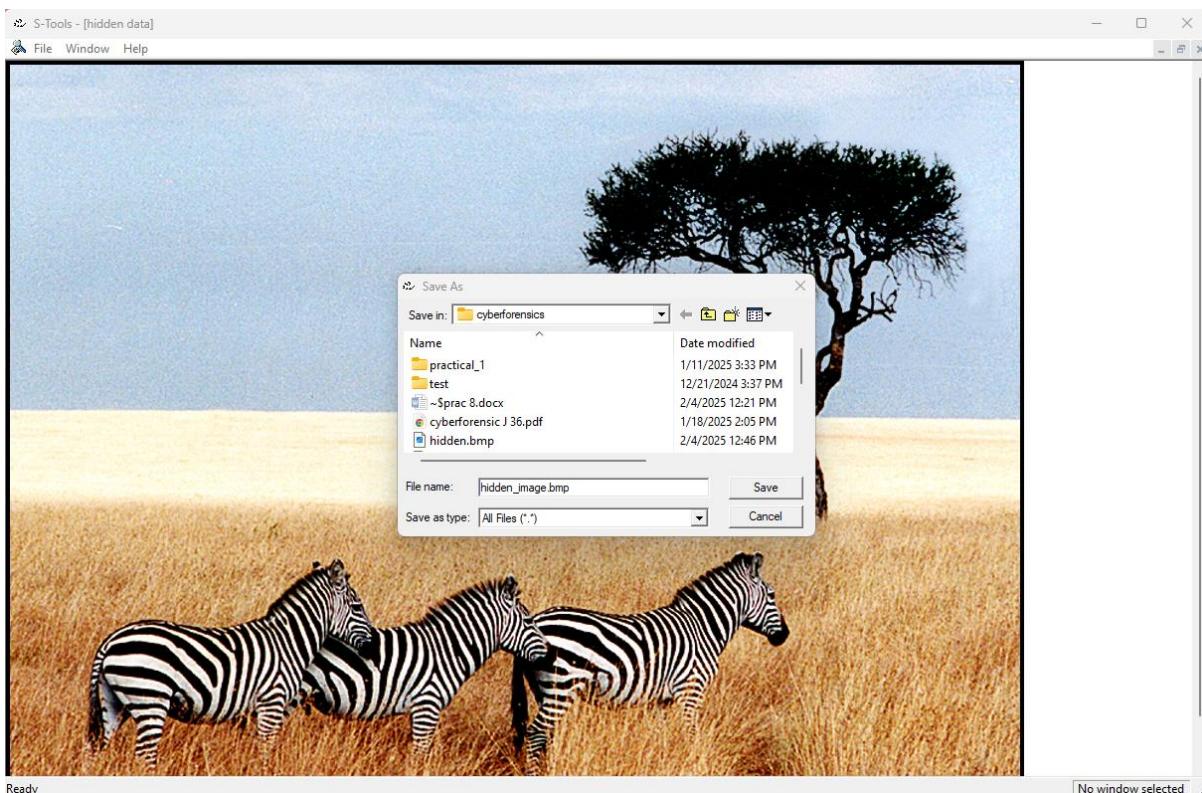
**Step 2: Create a new text document-> Type anything inside it and save it**



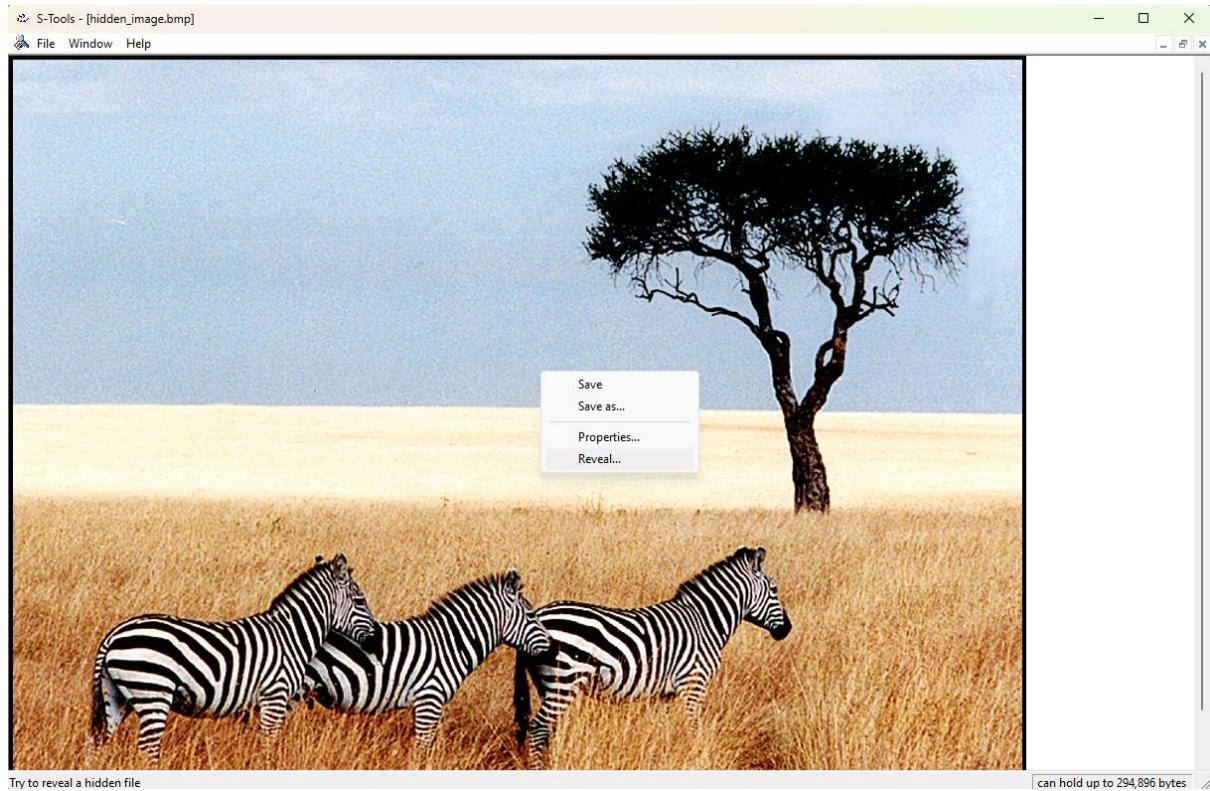
**Step 3: Now drag and drop the text file on the image-> enter the password**



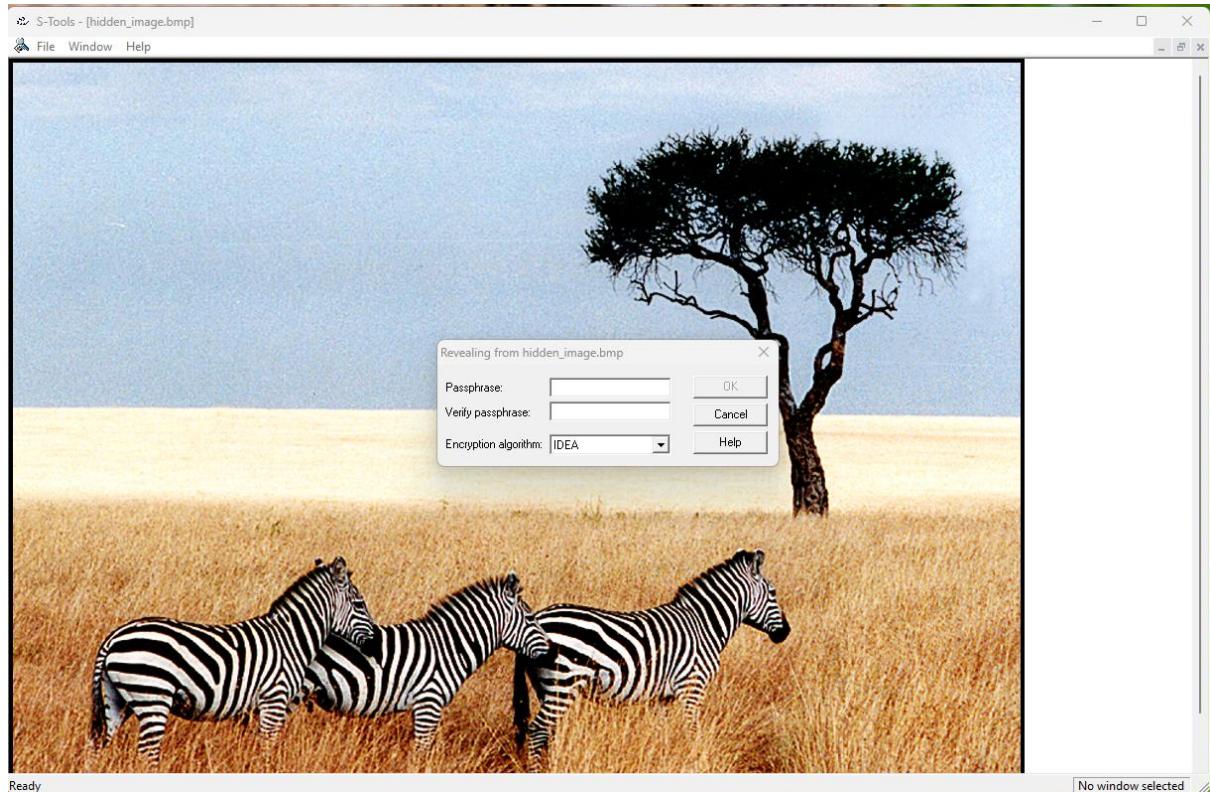
**Step 4: Now save the file**

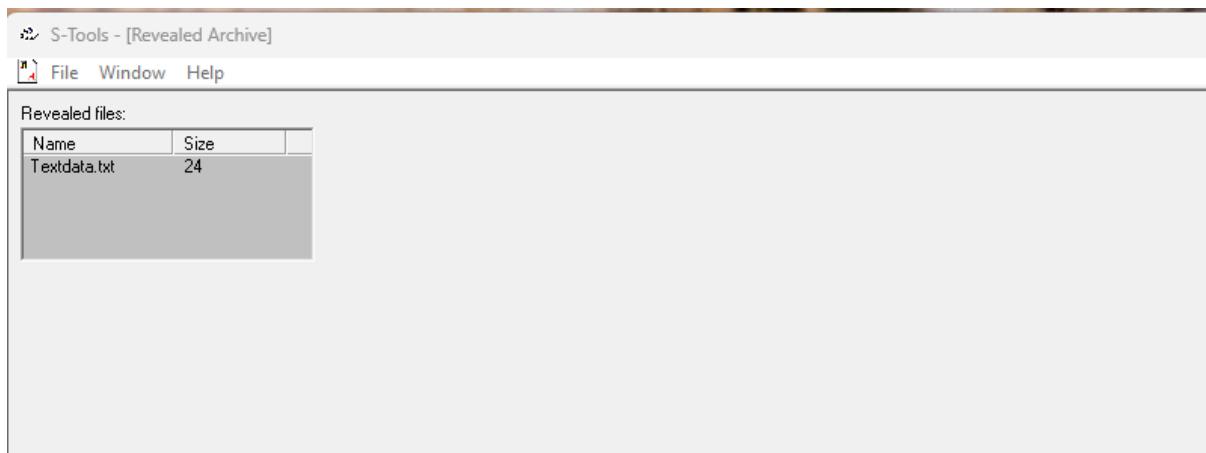


**Step 5: Open saved image -> right click on it-> Revel...**

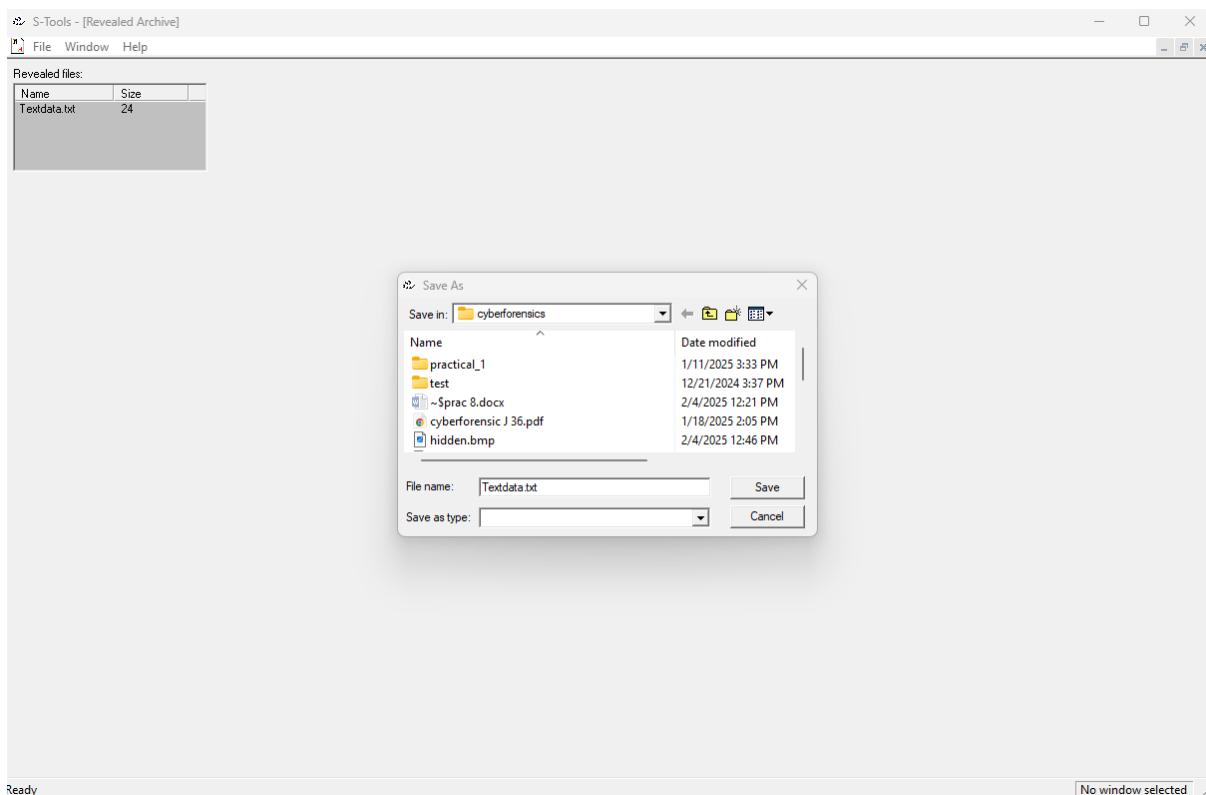


**Step 6: Enter the password that you have created**





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



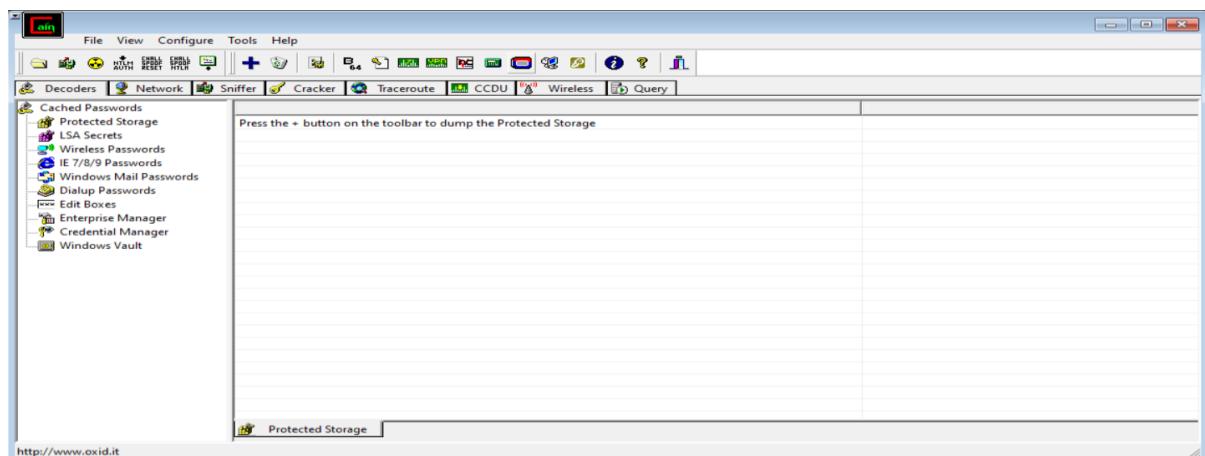
## Practical: 9

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

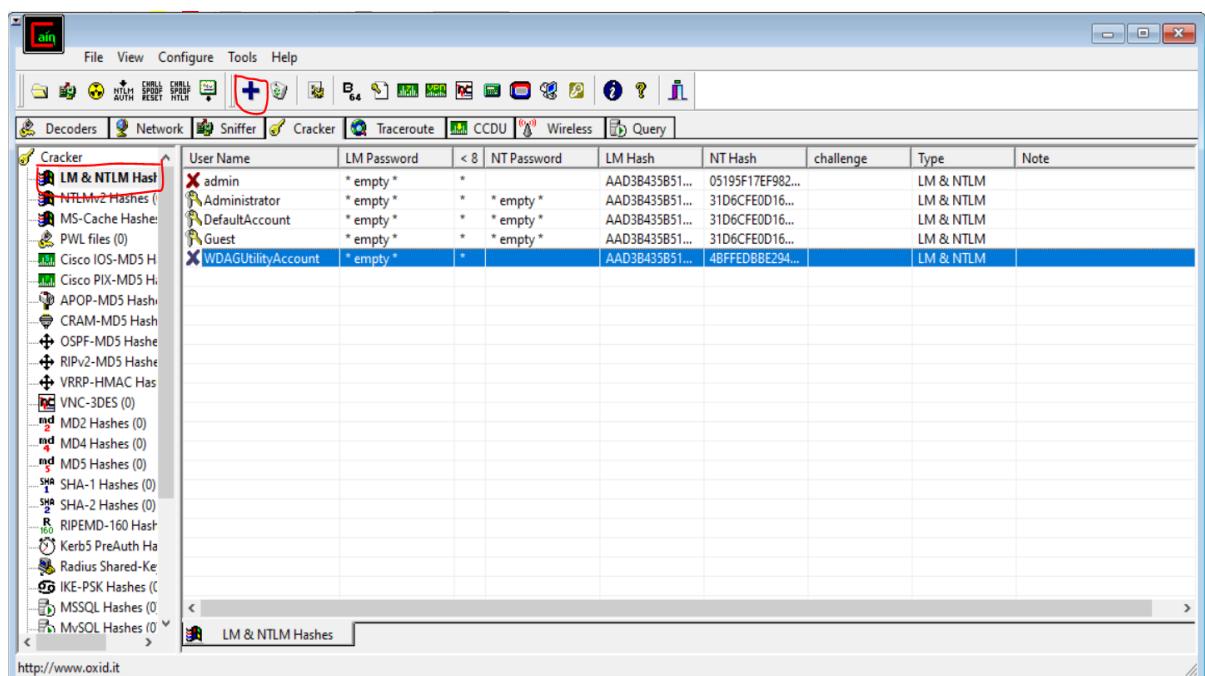
### Theory

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.

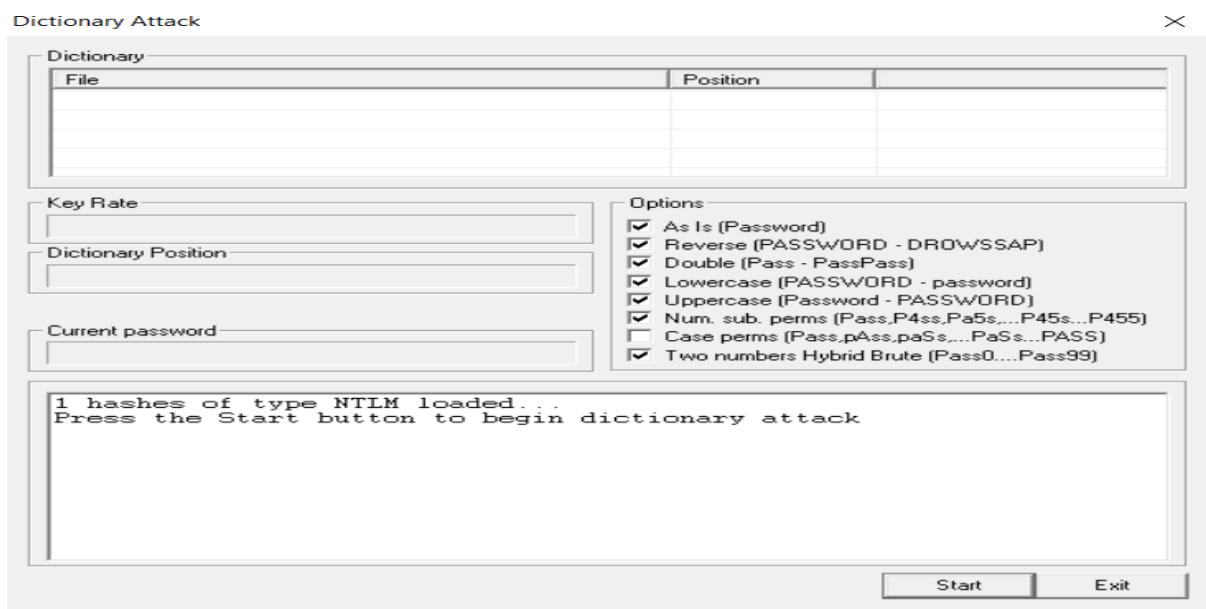
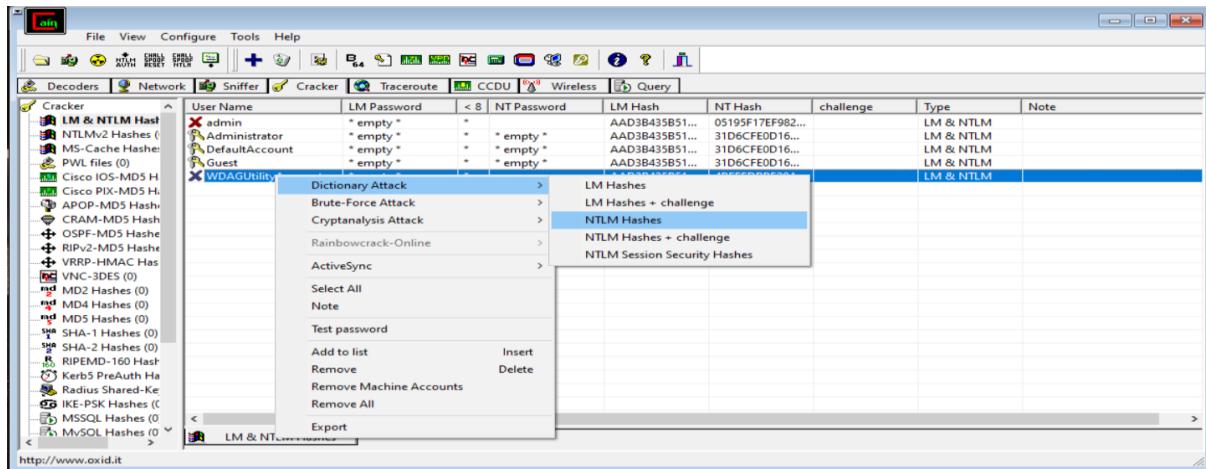
**Step1:** Download Cain n able software using the given link [http://www.oxid.it/downloads/ca\\_setup.exe](http://www.oxid.it/downloads/ca_setup.exe) Now it's time to speak about the cracker tab, the most important feature of Cain. When Cain captures some LM and NTLM hashes or any kind of passwords 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



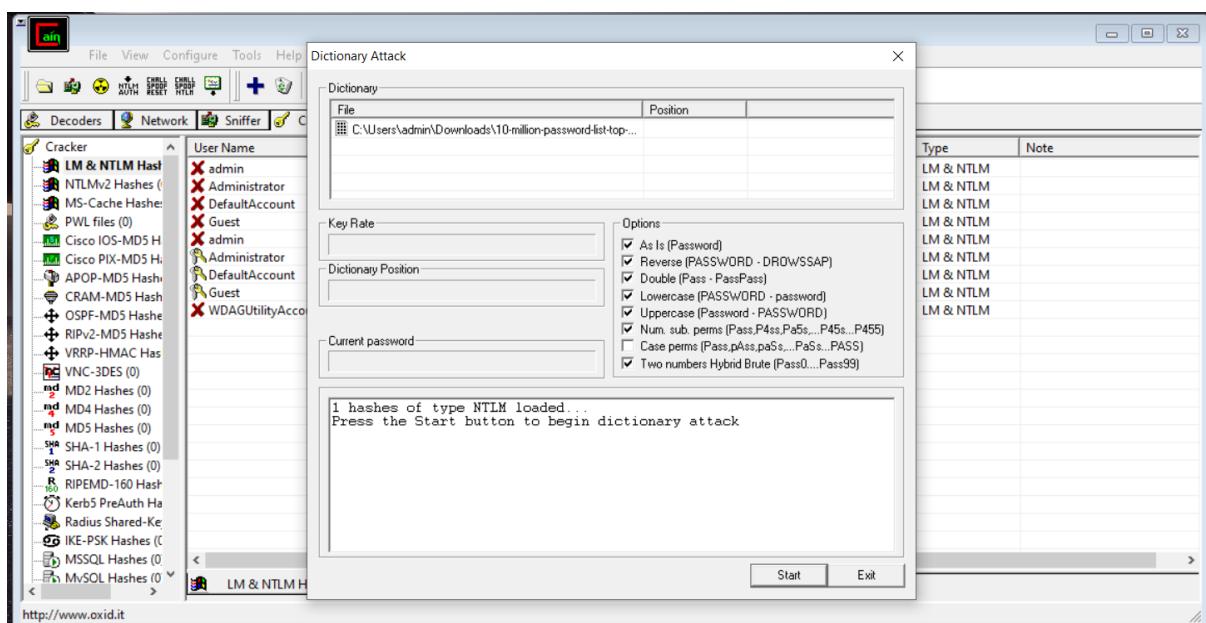
Step 2: Click on Craker-> then plus icon-> then LM & NTLM head

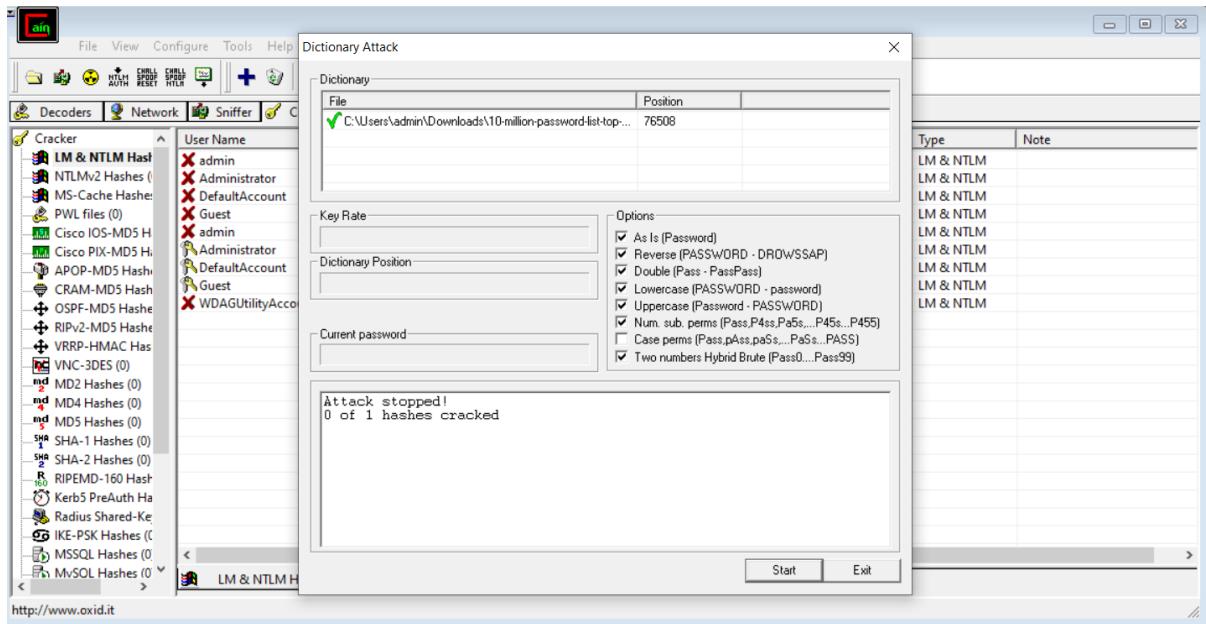


### Step 3: Now right click on WDAG



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





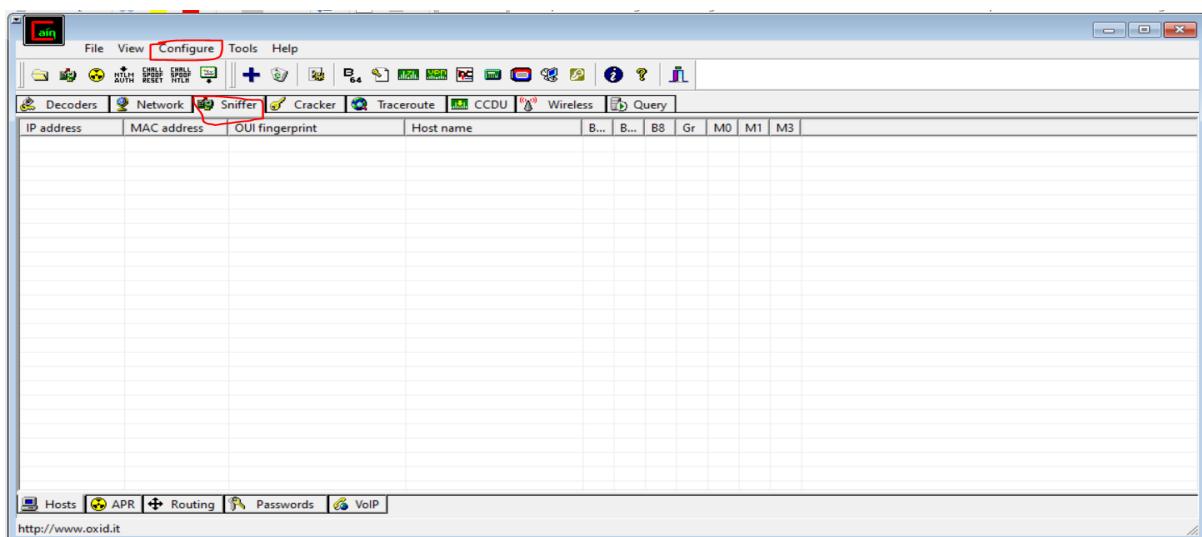
## B) Performing Sniffing [Cain & Abel].

### Theory

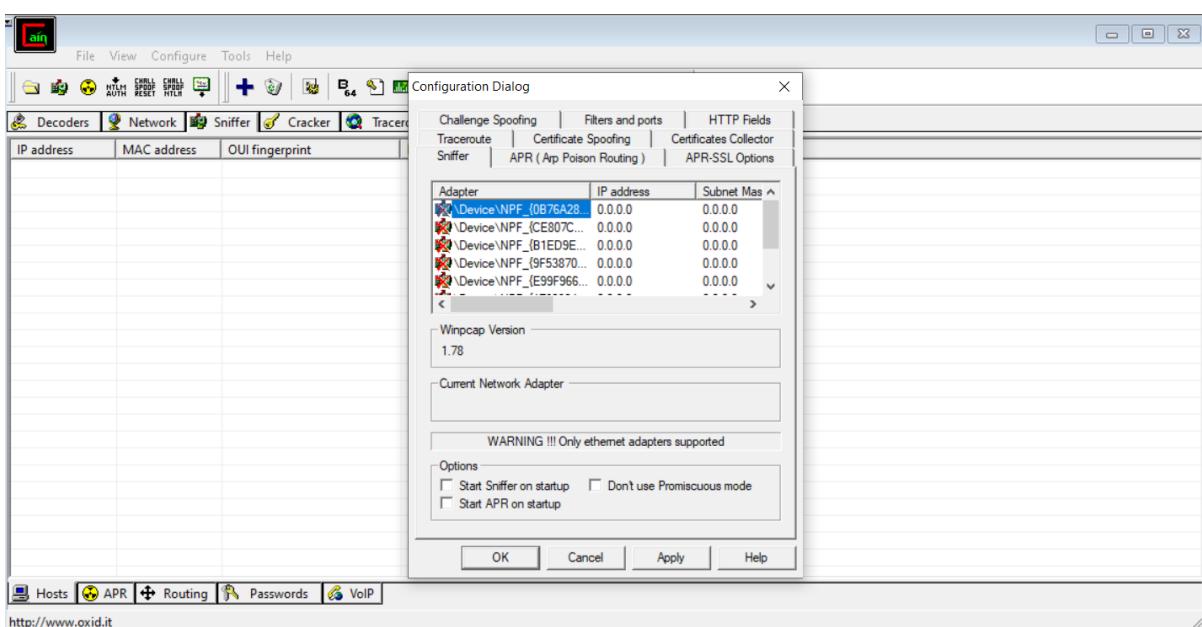
Sniffing:

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, and analyses its content according to the appropriate RFC or other specifications.

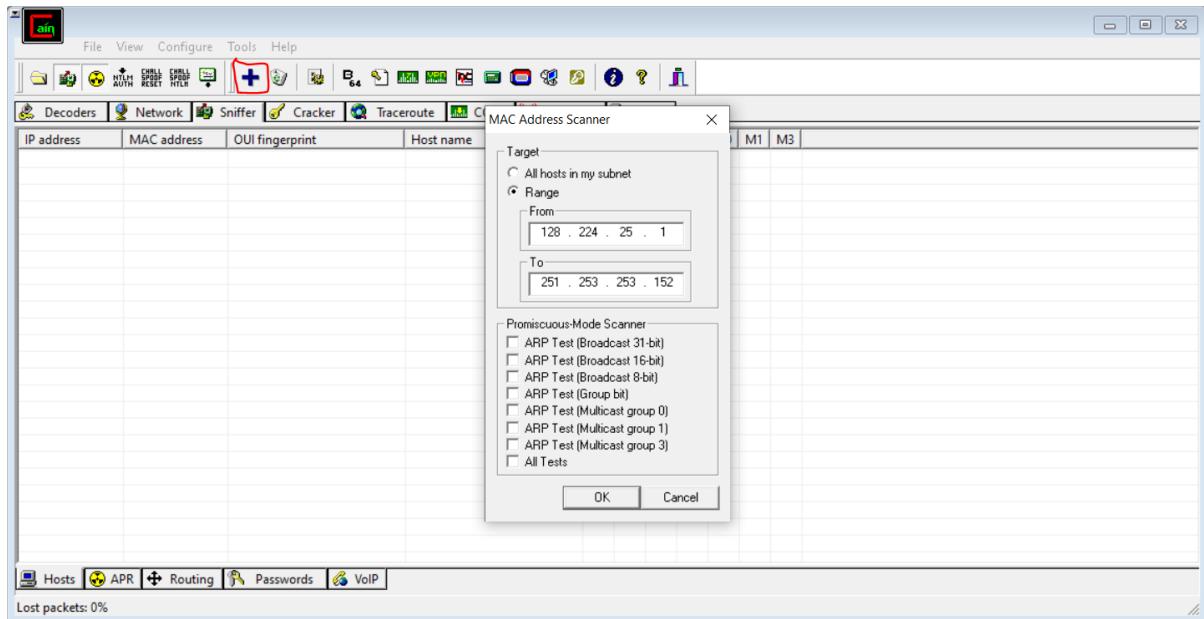
**Step 1: Go to -> Sniffer Tab and click Configure in the main menu to configure your packet listening adapter.**



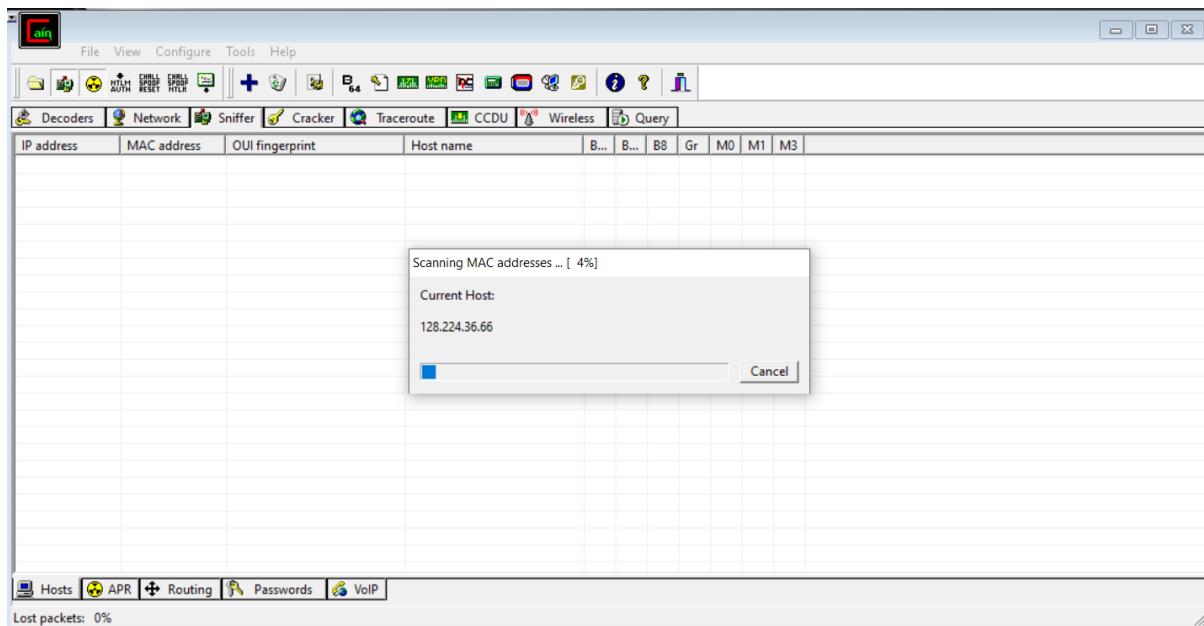
**Step 2: Select the appropriate network adapter for your network that you want to sniff the packets for plain-text passwords. And Click Ok**



**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, find the desired Registry values that match the specified search criteria and then displays them in a list.

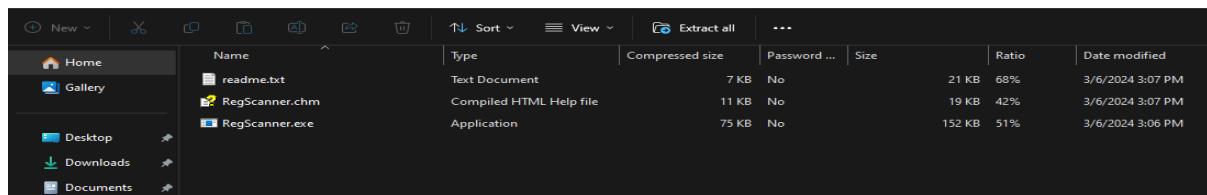
#### I. Problem Statement

A registry scanner or registry cleaner is third-party software for Microsoft Windows that searches for 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 registry entries.

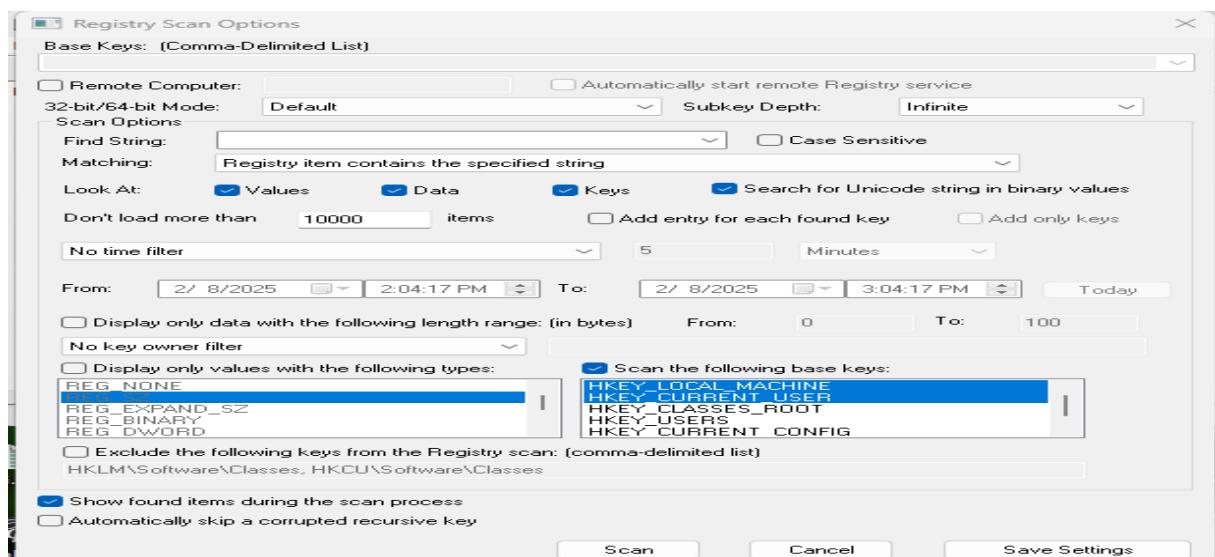
#### II. Literature/Theory

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 errors and crashes

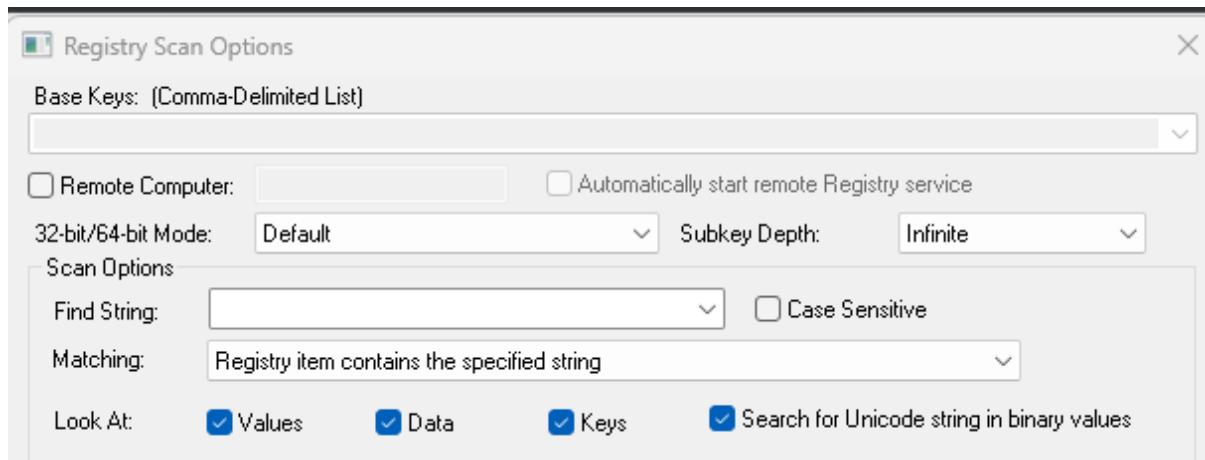
**Step 1: Install RegScanner > Double click on RegScanner .exe file to run the application.**



**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:**



The screenshot shows the RegScanner application interface. The title bar reads "RegScanner: int". The menu bar includes File, Edit, View, and Help. Below the menu is a toolbar with icons for search, refresh, and other functions. The main window displays a table of registry key information:

| 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\Admini... |
| HKLM\HAR...  | 00000000 | REG_BINARY | 53 53 44 54 8C ... | 2/8/2025 12:09:... | 908         | BUILTIN\Admini... |
| HKLM\HAR...  | 00000000 | REG_BINARY | 53 53 44 54 01 ... | 2/8/2025 12:09:... | 257         | BUILTIN\Admini... |
| HKLM\HAR...  | 00000000 | REG_BINARY | 53 53 44 54 34 ... | 2/8/2025 12:09:... | 23,860      | BUILTIN\Admini... |
| HKLM\HAR...  | 00000000 | REG_BINARY | 53 53 44 54 35 ... | 2/8/2025 12:09:... | 10,549      | BUILTIN\Admini... |
| HKLM\HAR...  | 00000000 | REG_BINARY | 53 53 44 54 E9 ... | 2/8/2025 12:09:... | 13,289      | BUILTIN\Admini... |

## 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

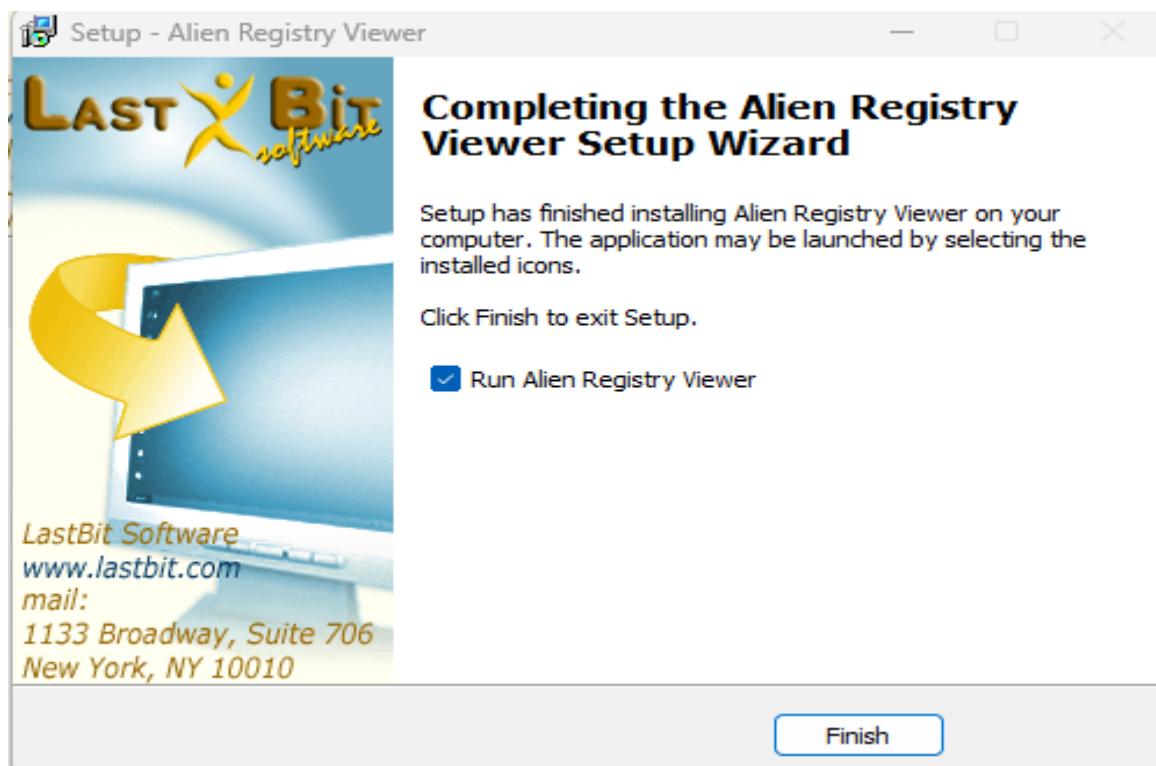
Registry Viewer allows you to view the protected storage of a registry. Passwords, usernames, and other information can be stored in the secured storage, which is not accessible using the Windows Registry Editor. Registry Viewer comes with a number of tools for retrieving and reporting vital registry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

#### III.Literature/Theory

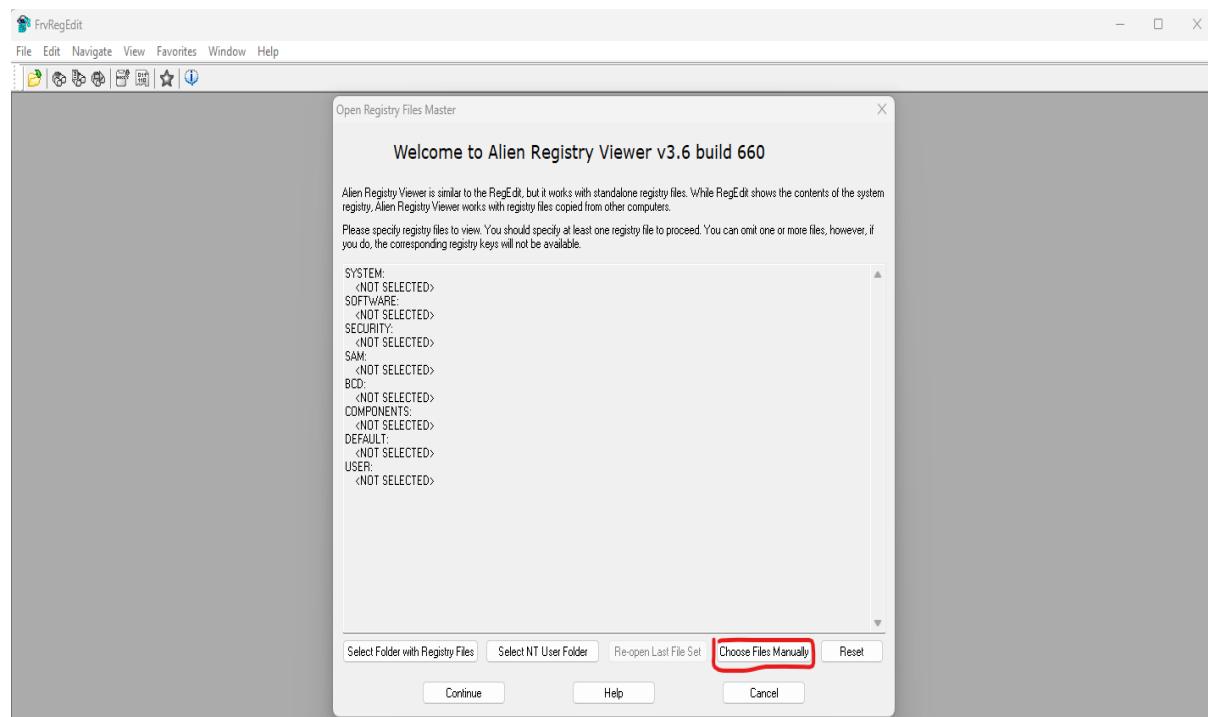
Alien Registry Viewer is similar to the RegEdit application included into Windows, but unlike RegEdit, it works with standalone registry files. The current version of Alien Registry Viewer works in the read-only mode, i.e. you can view but you cannot edit registry files.

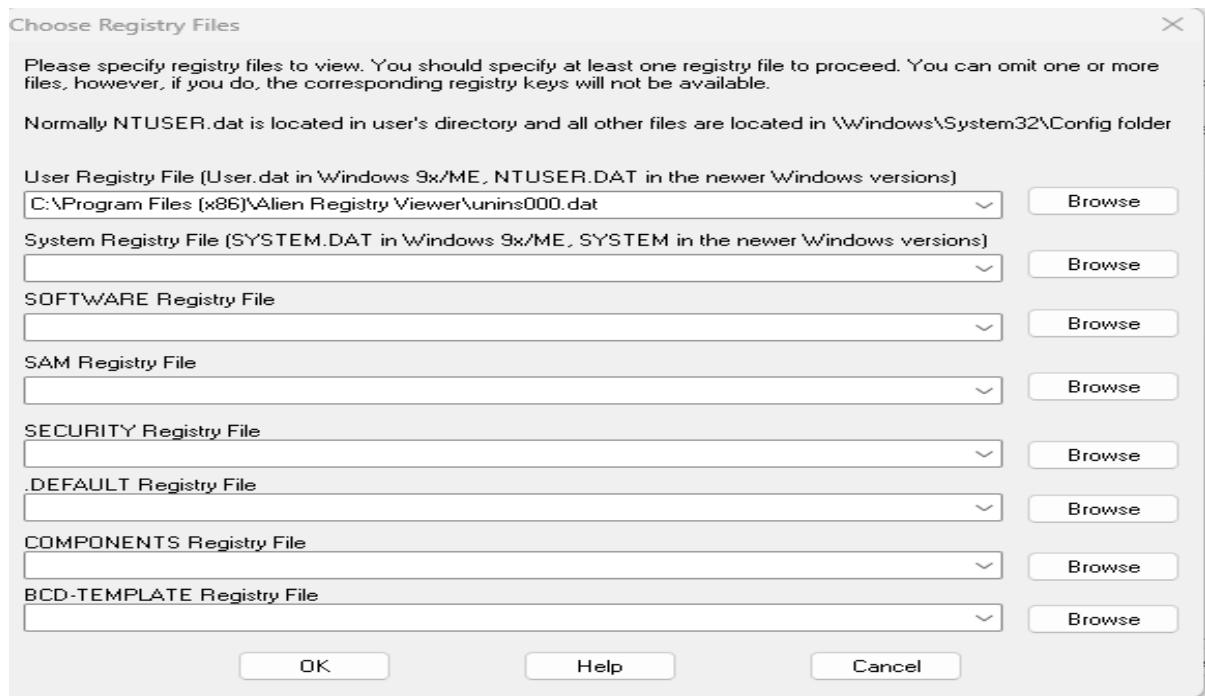
**Step 1: Install the Alien registry viewer by double clicking on the .exe file.-> The following window would appear.Click on Next.**



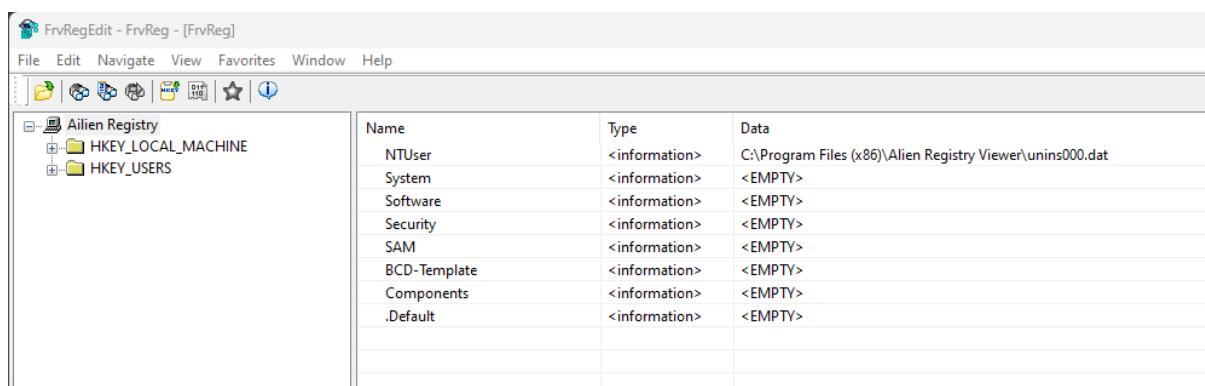


**Step 2: After installation the following window would appear.**





### 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.

