LAB ASSIGNMENT - 01

1 AIM

Study of Computer Forensics and different tools used for forensic investigation at least 7.

2 Tools used for Forensic Investigation:

2.1 Autopsy:

(a) It is an open-source digital forensics platform used for analyzing and investigating hard drives and smartphones.

(b) Features:

i. User-friendly graphical interface.

ii. File analysis, keyword search, and timeline analysis.

iii. Support for various file systems and disk image formats.

iv. Integration with external plugins for extended functionality.

2.2 Wireshark:

(a) Wireshark is a popular network protocol analyzer that allows users to capture and inspect data on a network in real-time.

(b) Features:

i. Live packet capturing and offline analysis.

ii. Deep inspection of hundreds of protocols.

iii. Rich display filters for precise analysis.

iv. Cross-platform support (Windows, macOS, Linux).

2.3 ProDiscover:

(a) ProDiscover is a commercial digital forensics tool designed for computer and network investigations.

(b) Features:

i. Disk imaging and analysis.

ii. Email and file recovery.

iii. Advanced search capabilities.

iv. Timeline analysis for reconstructing events.

2.4 FTK Imager:

(a) FTK Imager is a forensic imaging tool used for acquiring and analyzing digital evidence.

(b) Features:

i. Create forensic images of disks and drives.

ii. View and analyze file systems and deleted files.

iii. Simple and intuitive user interface.

iv. Supports various image formats.

2.5 EnCase:

(a) EnCase is a widely used digital forensics tool that provides a range of features for evidence collection and analysis.

(b) Features:

i. Disk imaging and forensic analysis.

ii. Supports a wide range of file systems.

iii. Powerful keyword and index searches.

iv. Timeline analysis and reporting capabilities.

2.6 CAINE:

(a) CAINE (Computer Aided Investigative Environment) is an open source digital forensics platform which provides a user friendly environment for computer investigations.

(b) Features:

i. Integrated tools for data acquisition and analysis.

ii. Live boot capability without modifying the host system.

iii. Automated tools for imaging, file analysis, and searches.

iv. Open-source and cross-platform (Linux).

2.7 SIFT Workstation:

(a) SIFT (SANS Investigative Forensic Toolkit) Workstation is an open-source forensic toolkit maintained by SANS.

(b) Features:

i. Collection of various forensic tools and utilities.

ii. Pre-configured environment for forensic analysis

iii. Linux-based, providing flexibility and extensibility.

iv. Focus on digital evidence examination and analysis.

2.8 Sleuth Kit:

(a) The Sleuth Kit is an open-source digital forensics toolkit that provides command-line tools for analyzing disk images.

(b) Features:

i. File system analysis for various formats.

ii. In-depth file and metadata examination.

iii. Support for various hashing algorithms.

iv. Portable and cross-platform.

LAB ASSIGNMENT - 02

1 AIM

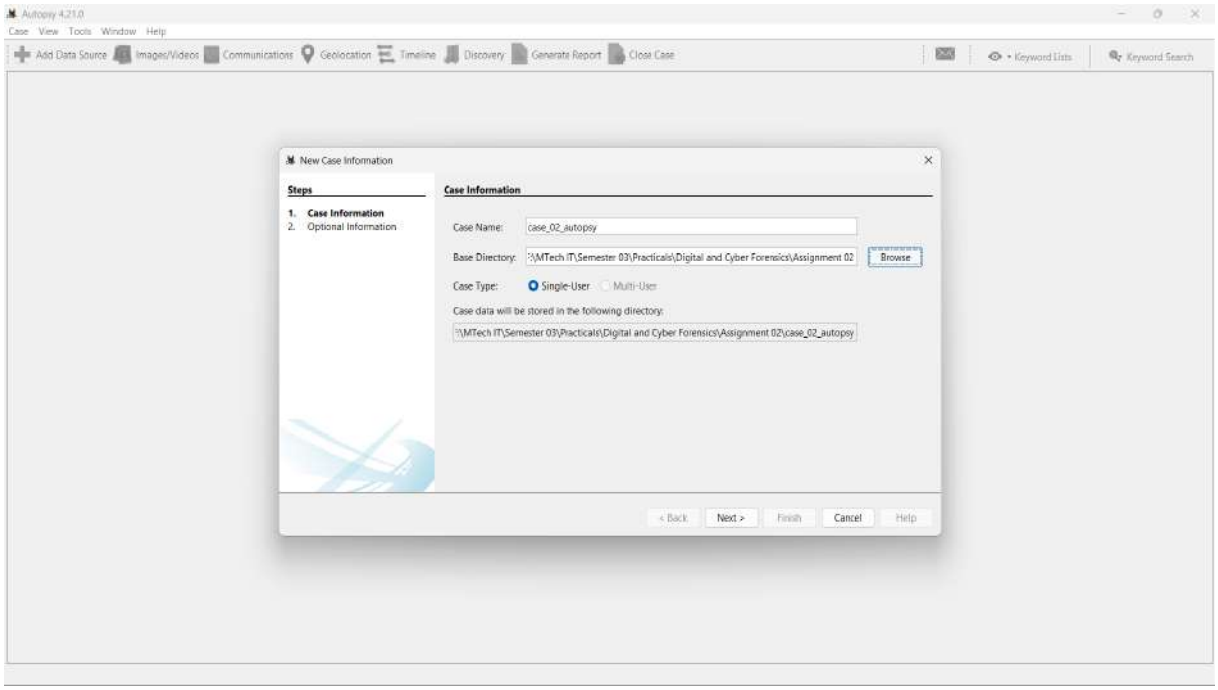
Perform to make the forensic image of the storage drive (Using ProDiscover, AccessData FTK Imager, and Autopsy)

2 Different tools used for Forensic Investigation

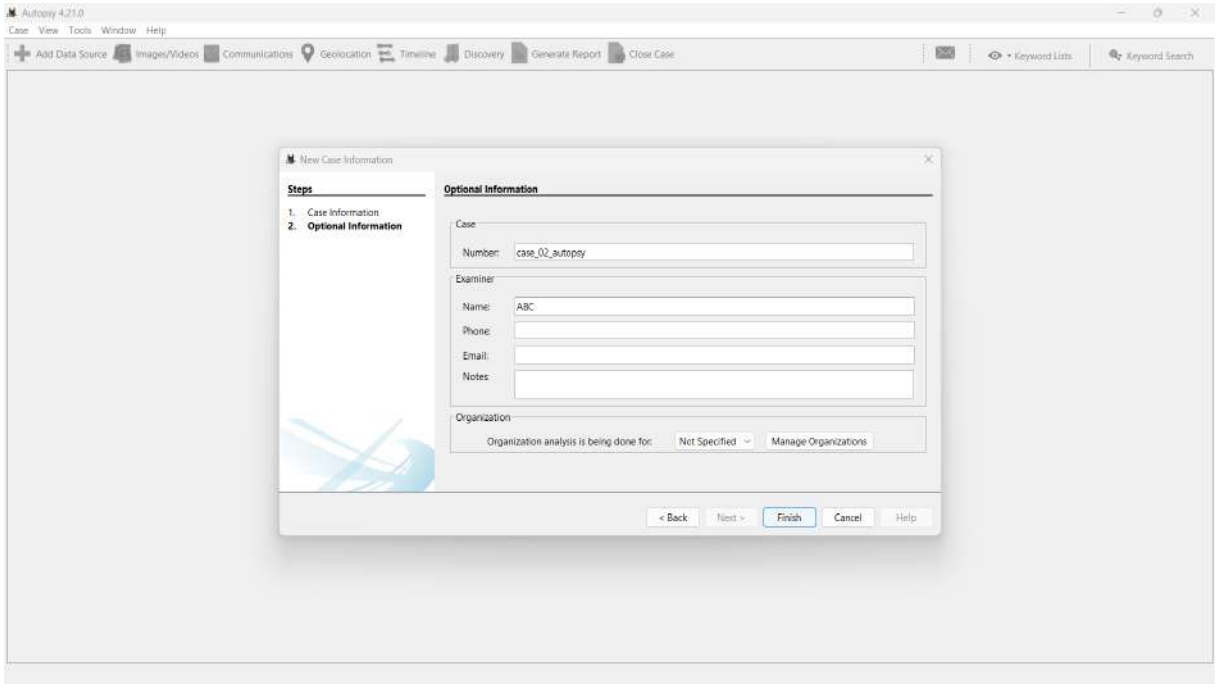
2.1 Perform using Autopsy

Steps to make forensic image using Autopsy are as follows: -

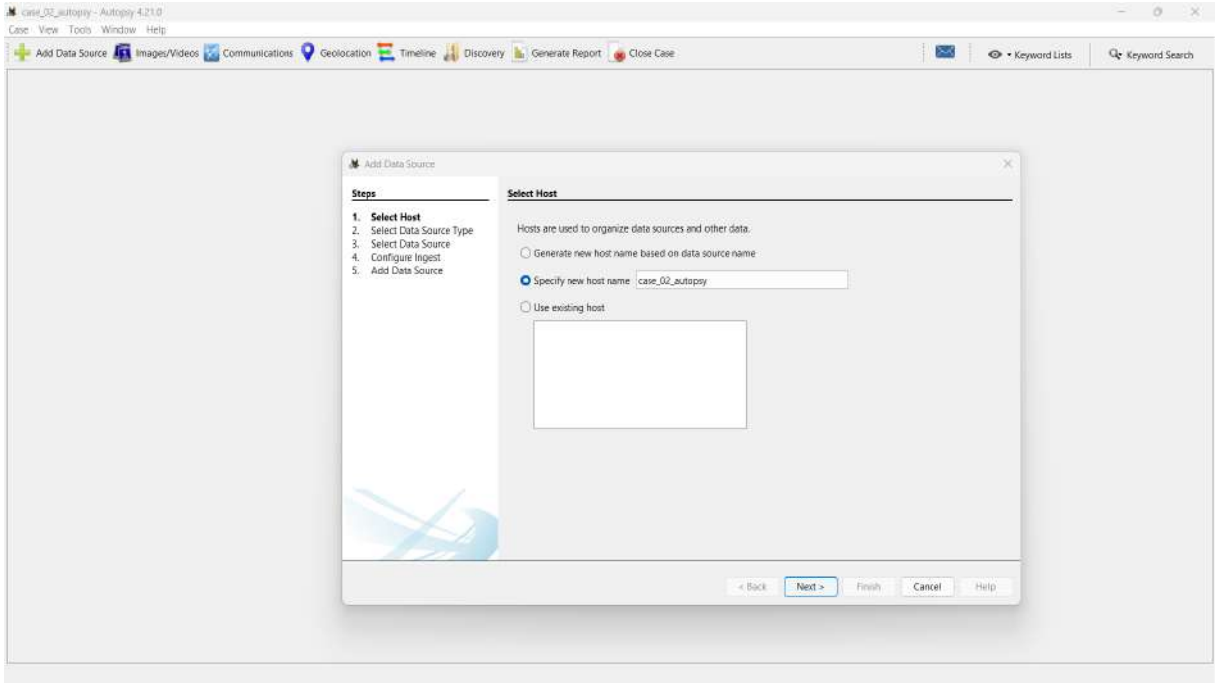
1. Start Autopsy for Windows.
2. In Autopsy's main window, click the Create New Case button. In the New Case Information window, enter case_02_autopsy in the Case Name text box, and click Browse next to the Base Directory text box. Navigate to and click your work folder. Make sure the Single-user option button is selected for Case Type, and then click Next.



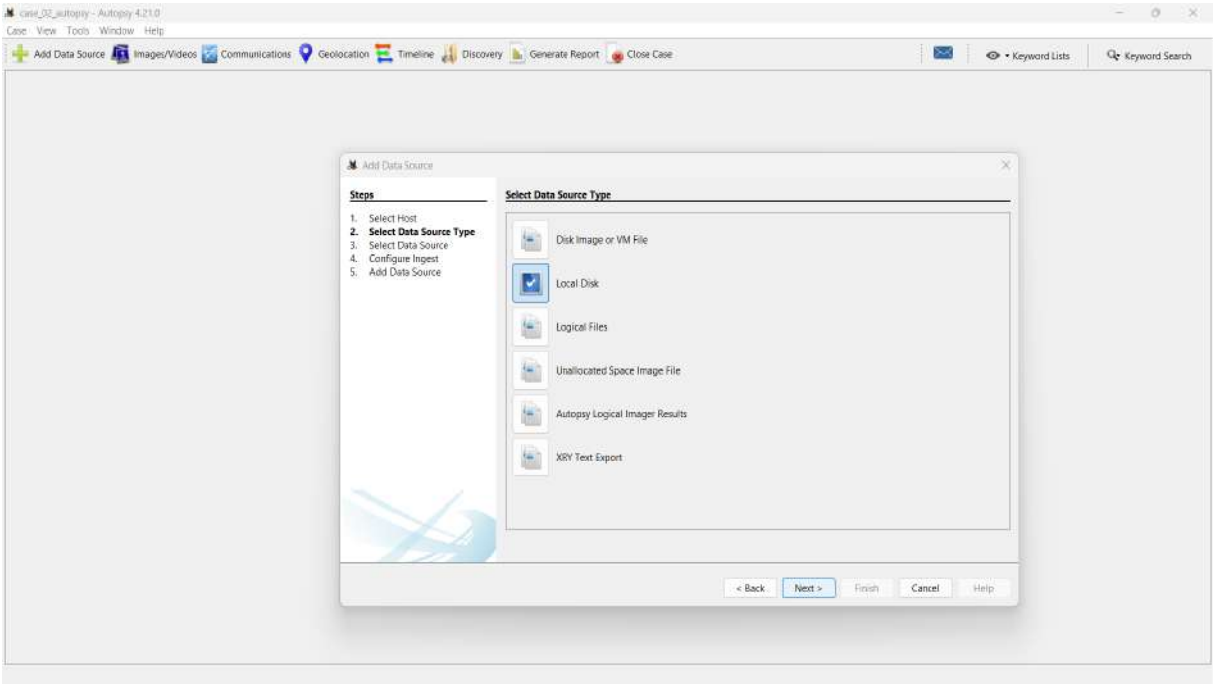
3. In the Additional Information window, type case_02_autopsy in the Case Number text box and your name in the Examiner text box, and then click Finish to start the Add Data Source Wizard.



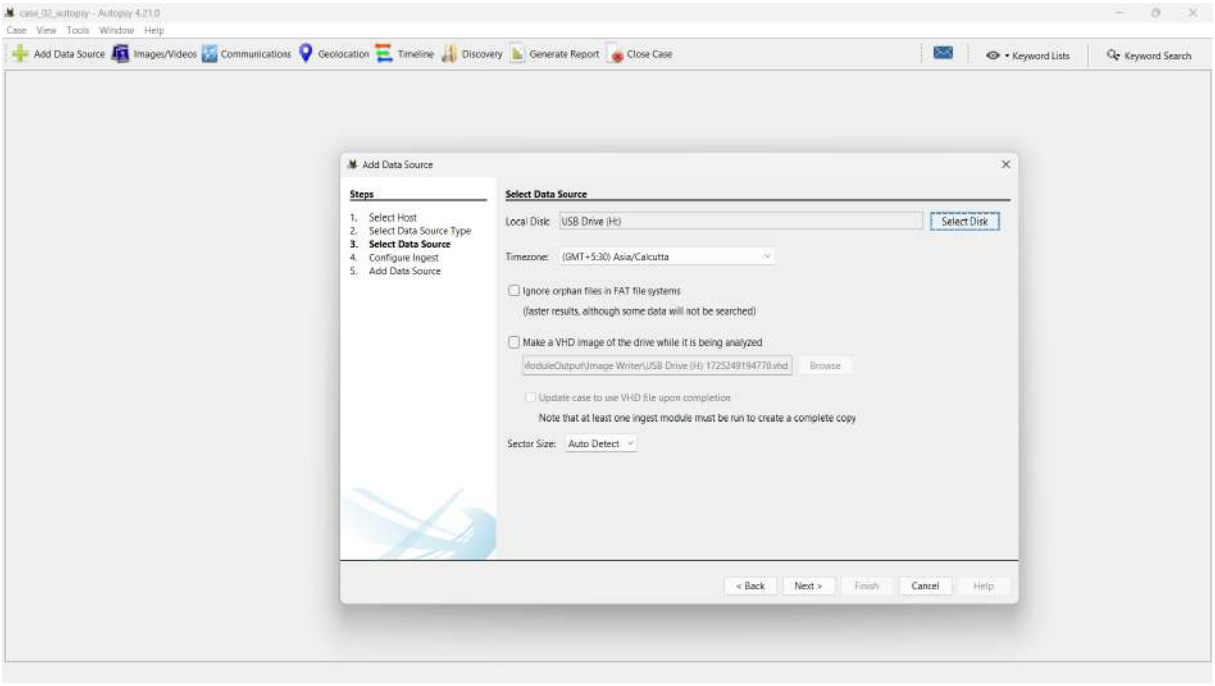
4. In the Add data source window, specify the new host name as case_02_autopsy, and click on Next.



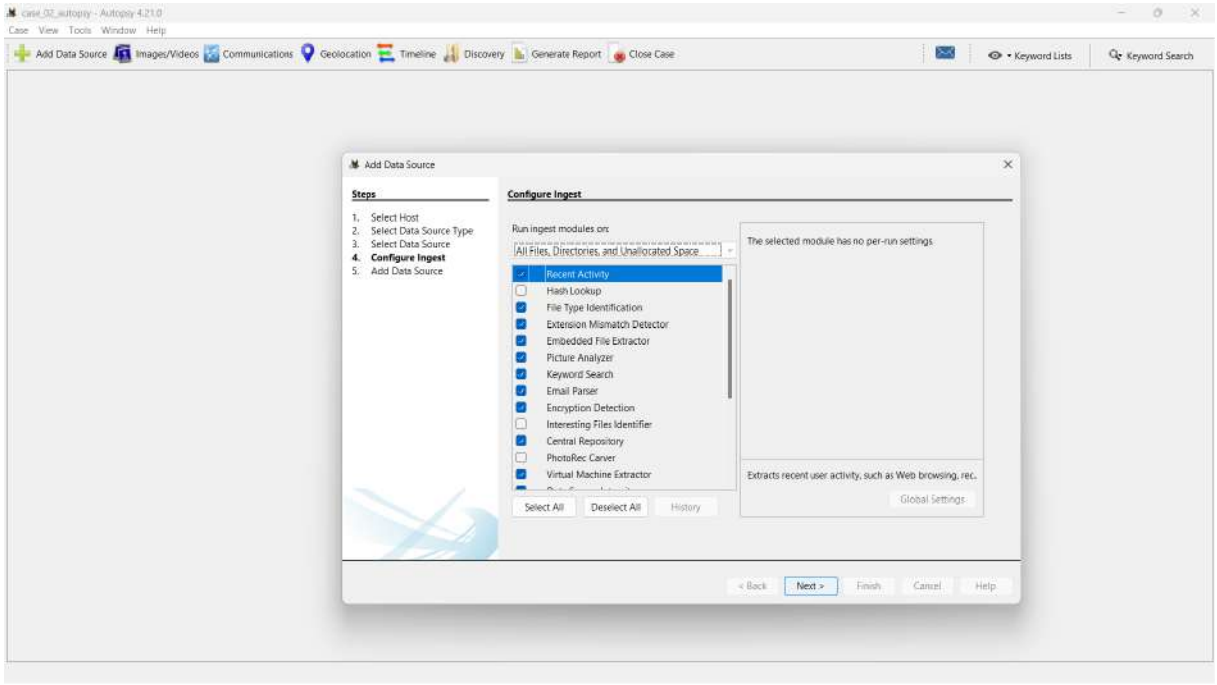
5. In the Select Data Source Type, click ”Local Disk” and click on Next.



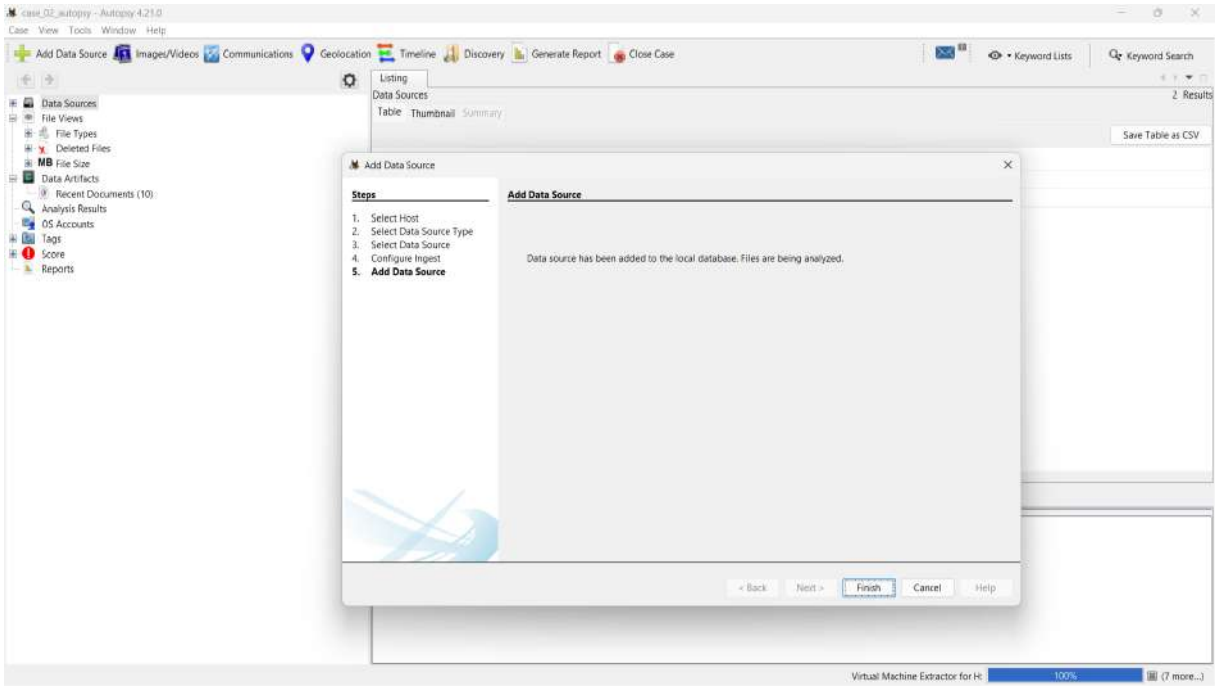
6. Select the Disk as given in the screenshot and click on Next.



7. Next, select the settings in the configure ingest module window, and then click on Next.



8. Now, click on Finish.

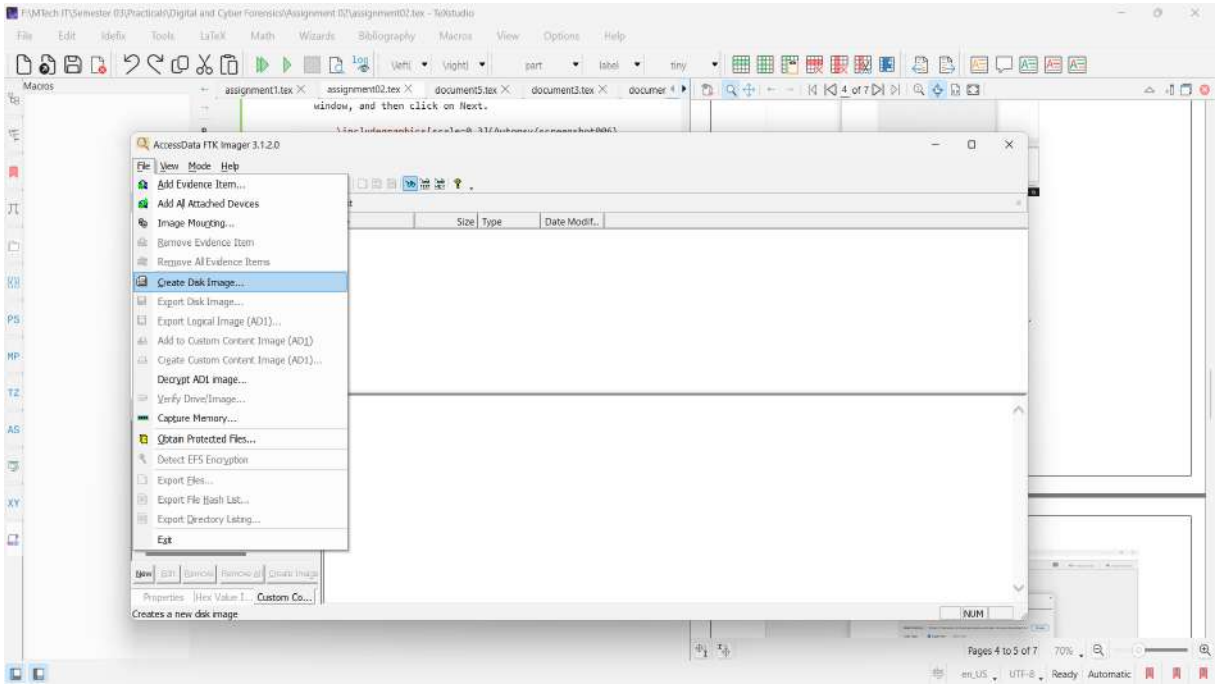


2.2 Perform using AccessData FTK Imager

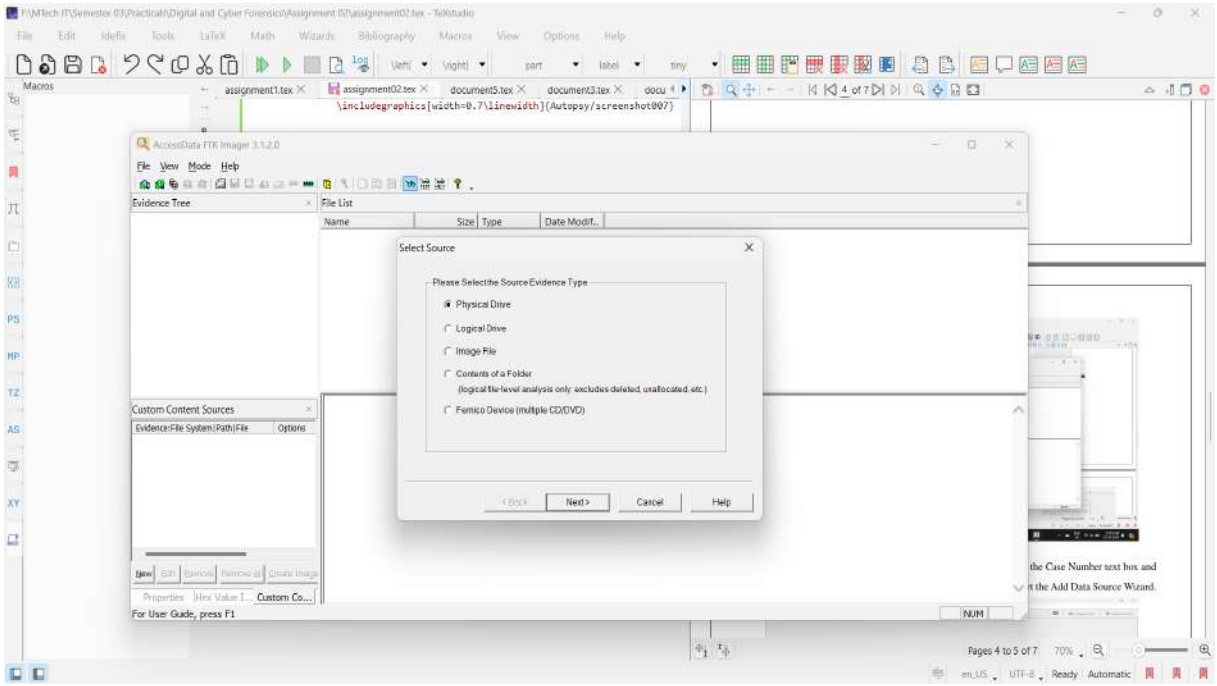
Steps to make forensic image using AccessData FTK Imager are as follows: -

1. Start AccessData FTK Imager for Windows.

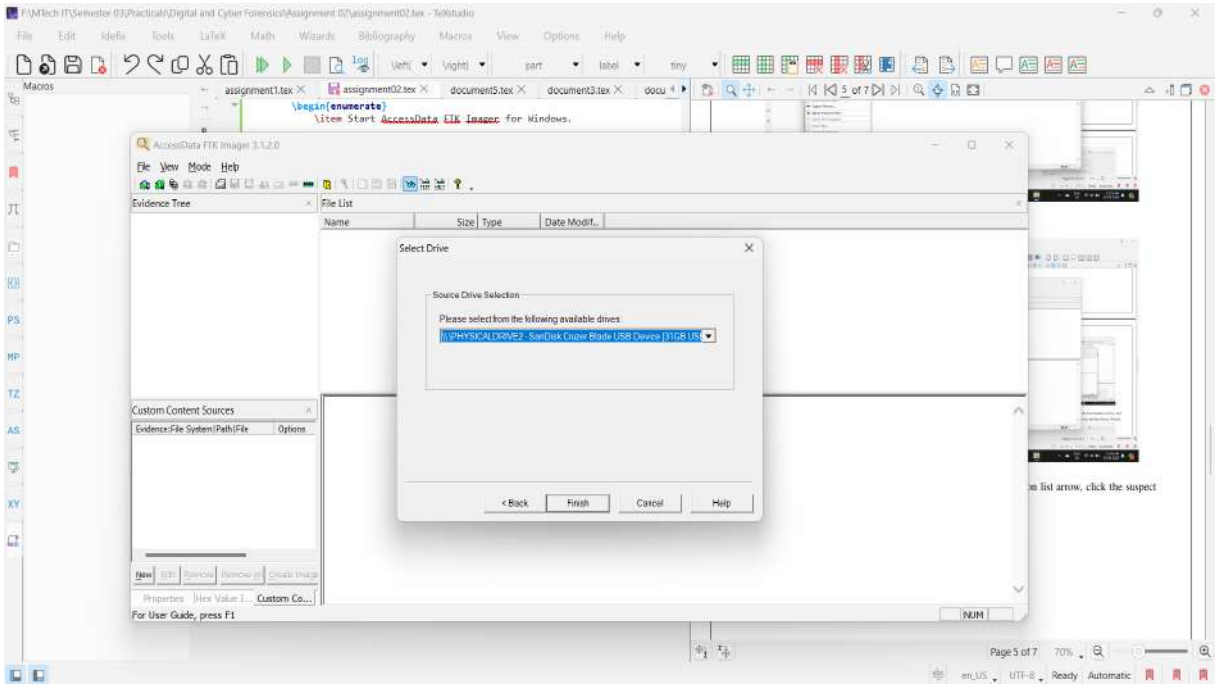
2. In AccessData FTK Imager, click on File → Create Disk Image.



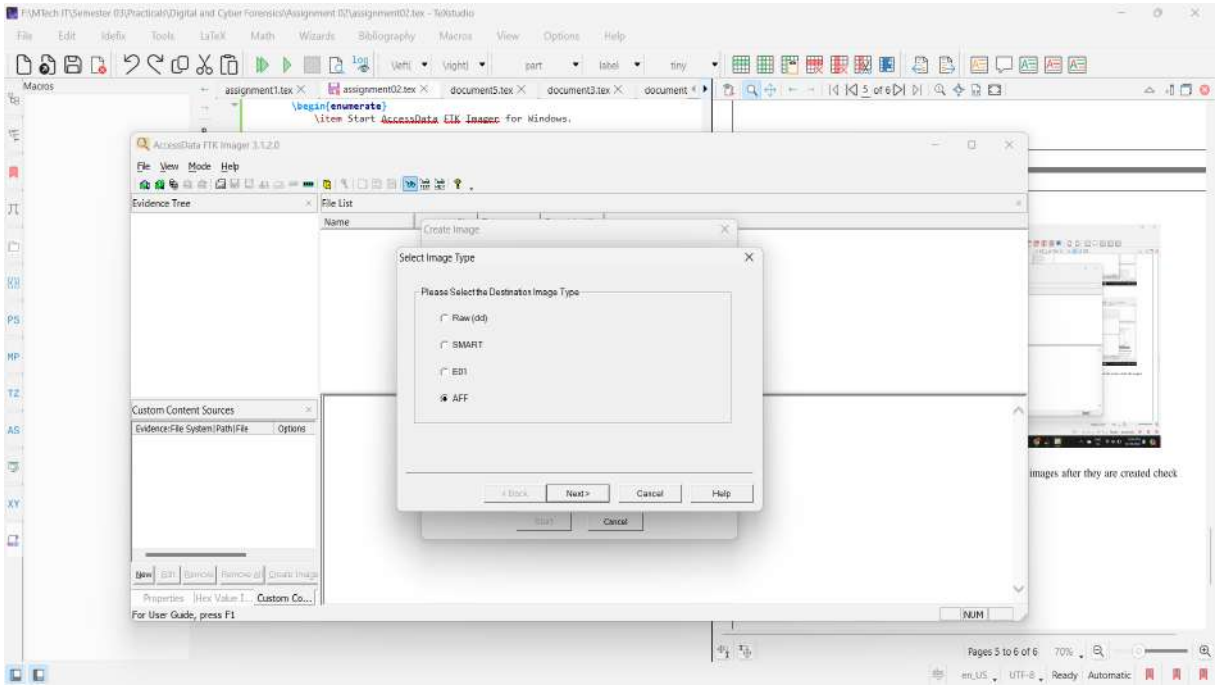
3. Click on Physical Drive and click on Next.



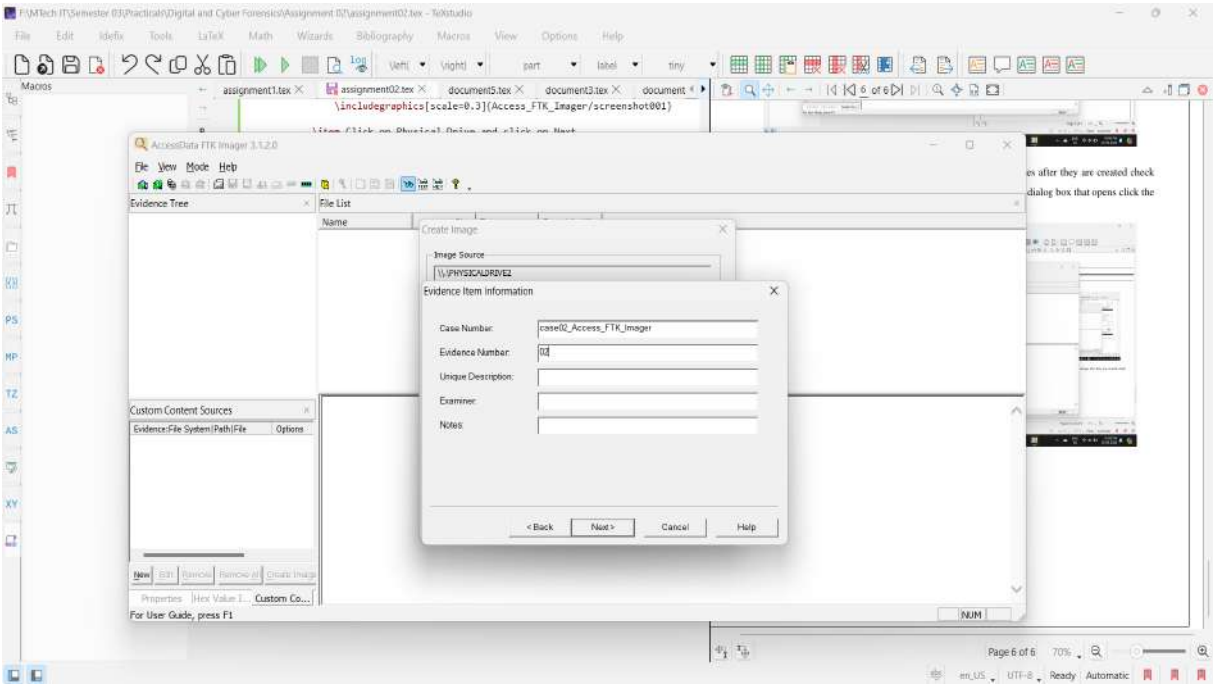
4. In the Select Drive dialog box, click the Source Drive Selection list arrow, click the suspect drive, and then click Finish.



5. In the Create Image dialog box, click to select the Verify images after they are created check box, if necessary, and then click Add. In the Select Image Type dialog box that opens click the AFF option button, if necessary, and then click Next.

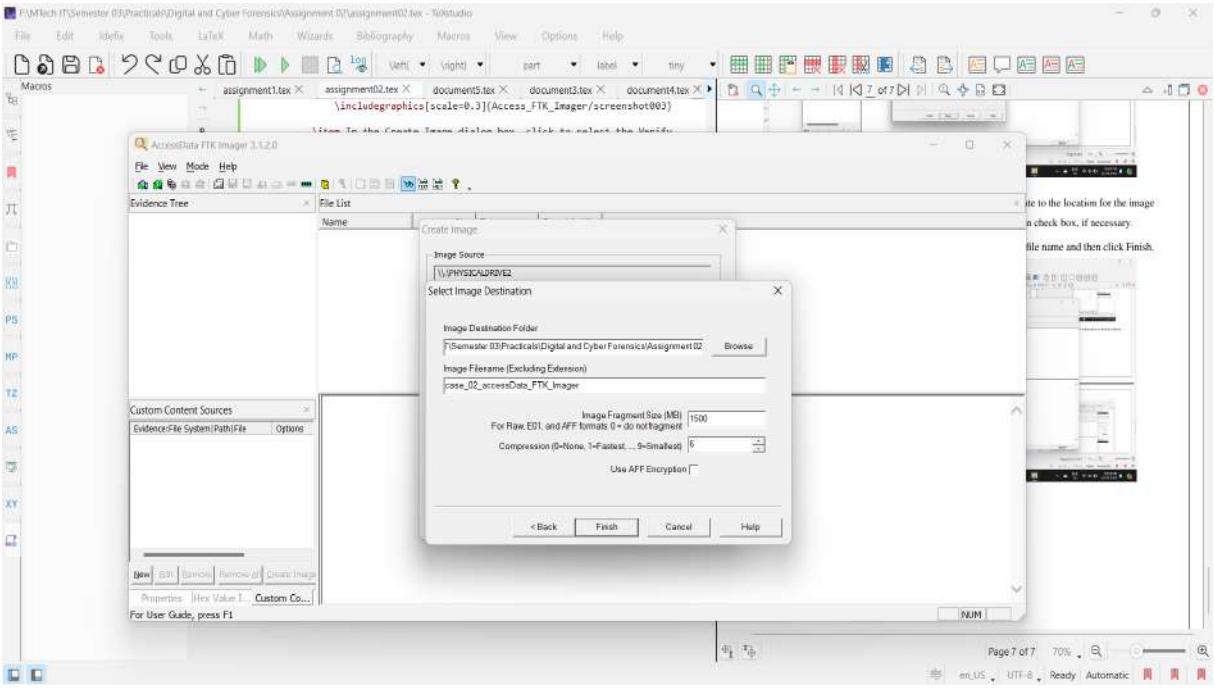


6. In the Evidence Item Information dialog box, complete the case information as shown in below figure, and then click Next.

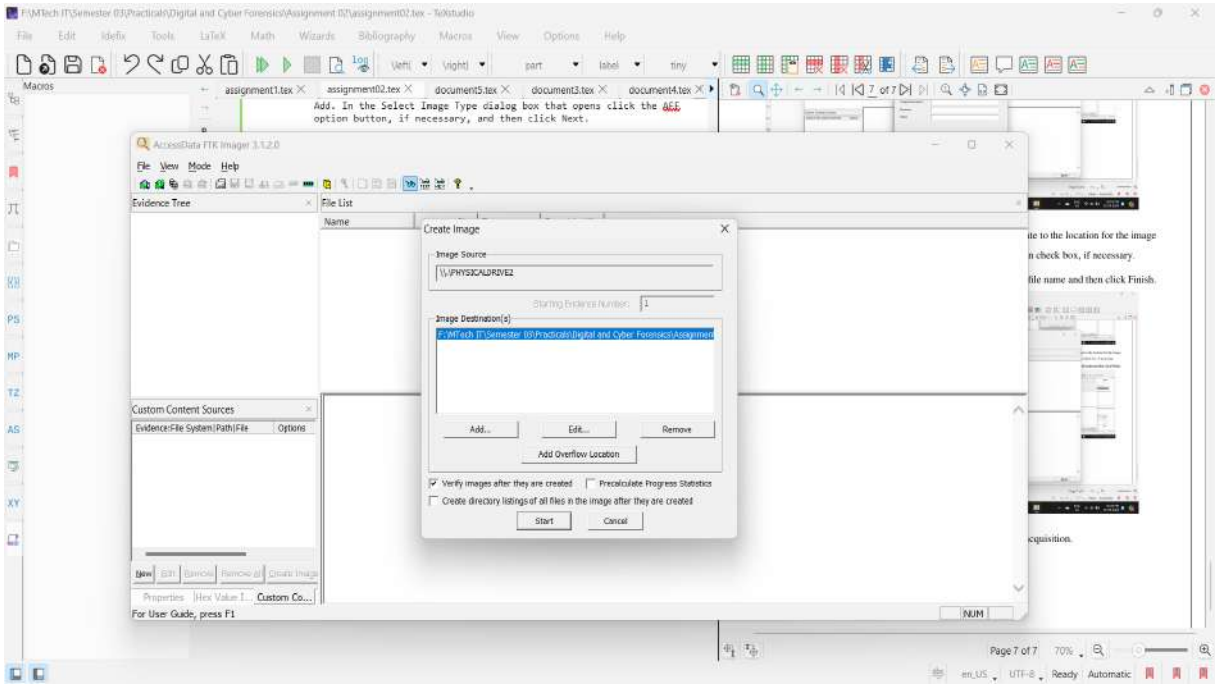


7. In the Select Image Destination dialog box click Browse, navigate to the location for the image file (your work folder), and click to clear the Use AD Encryption check box, if necessary.

   In the Image Filename (Excluding Extension) text box, type the file name and then click Finish.



8. Next, in the Create Image dialog box, click Start to initiate the acquisition.



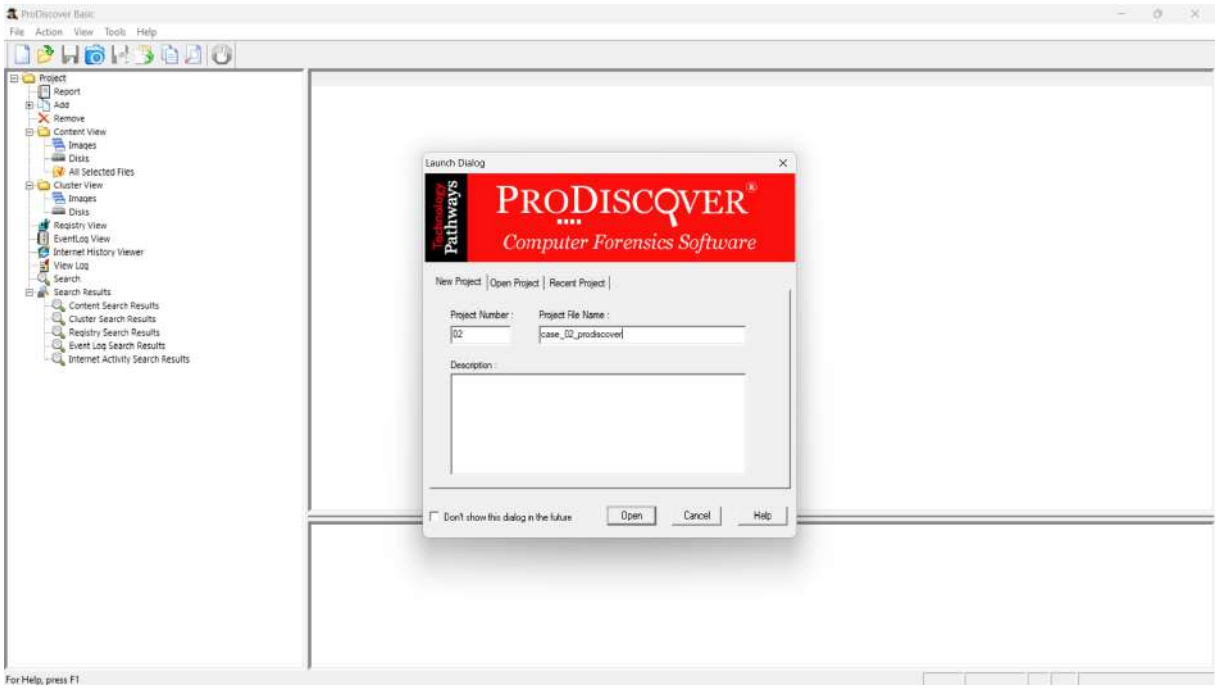
9. When FTK Imager finishes the acquisition, review the information in the Drive/Image Verify Results dialog box, and then click Close. Click Close again in the Creating Image dialog box.

2.3 Perform using ProDiscover

Steps to make forensic image using ProDiscover are as follows: -

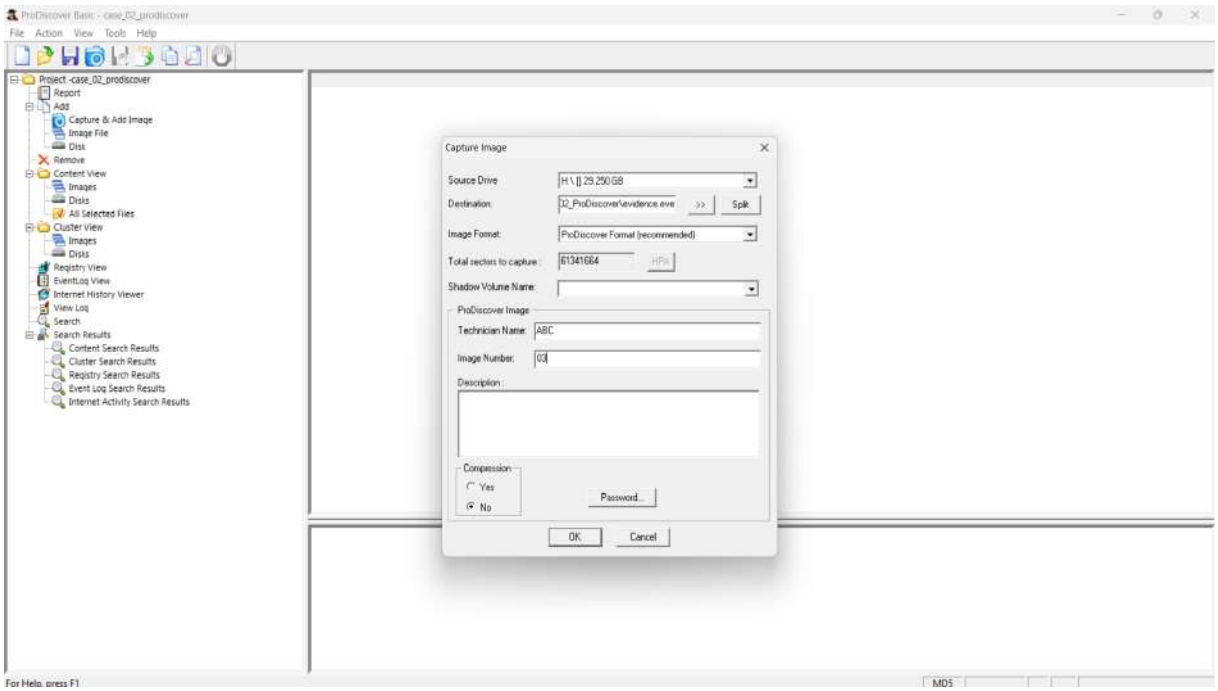
1. Start ProDiscover for Windows.

2. Next, under ”New Project” section, type the Project Number and Project File Number, and then click on Open.



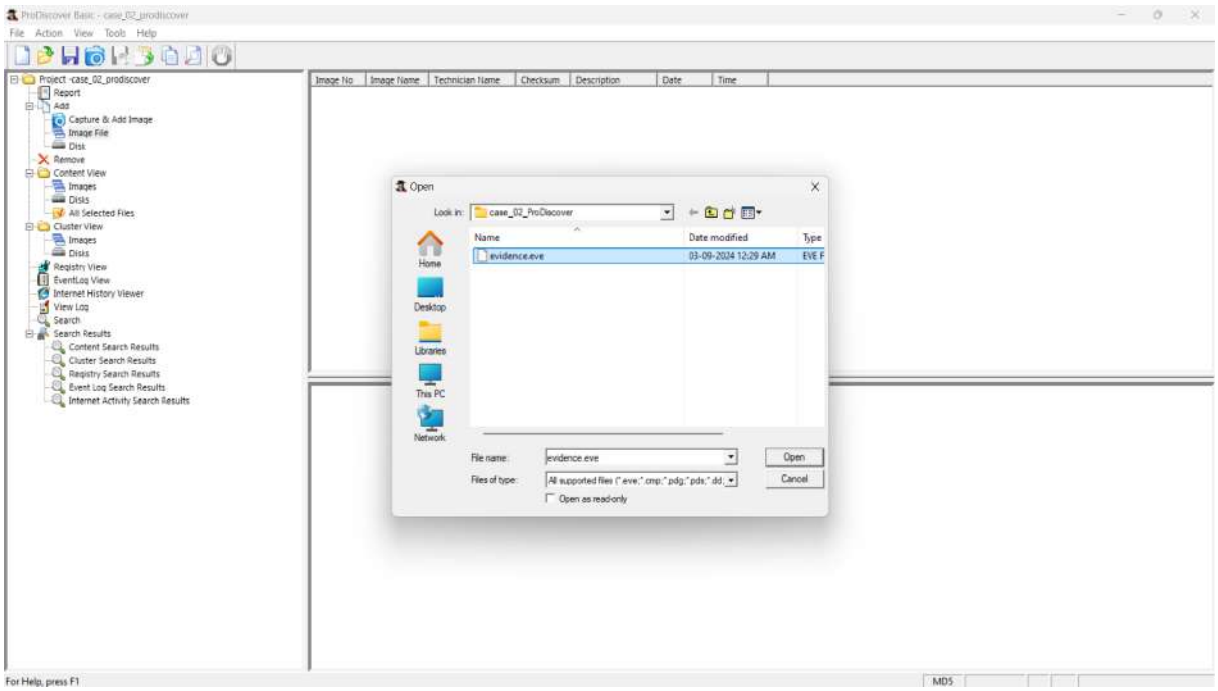
3. Click on Action → Capture Image

4. In the Capture Image, select the Source Drive and the destination you want to save at. Then, click on OK.



5. Image capture is complete.

6. Now, mount the image by clicking on Add → Image File, and then select the .eve file. Then, click on Open.



7. Now the steps are complete.

LAB ASSIGNMENT - 03

1 AIM

To Recover a Deleted File using Forensic Tools (FTK Imager, Autopsy, ProDiscover).

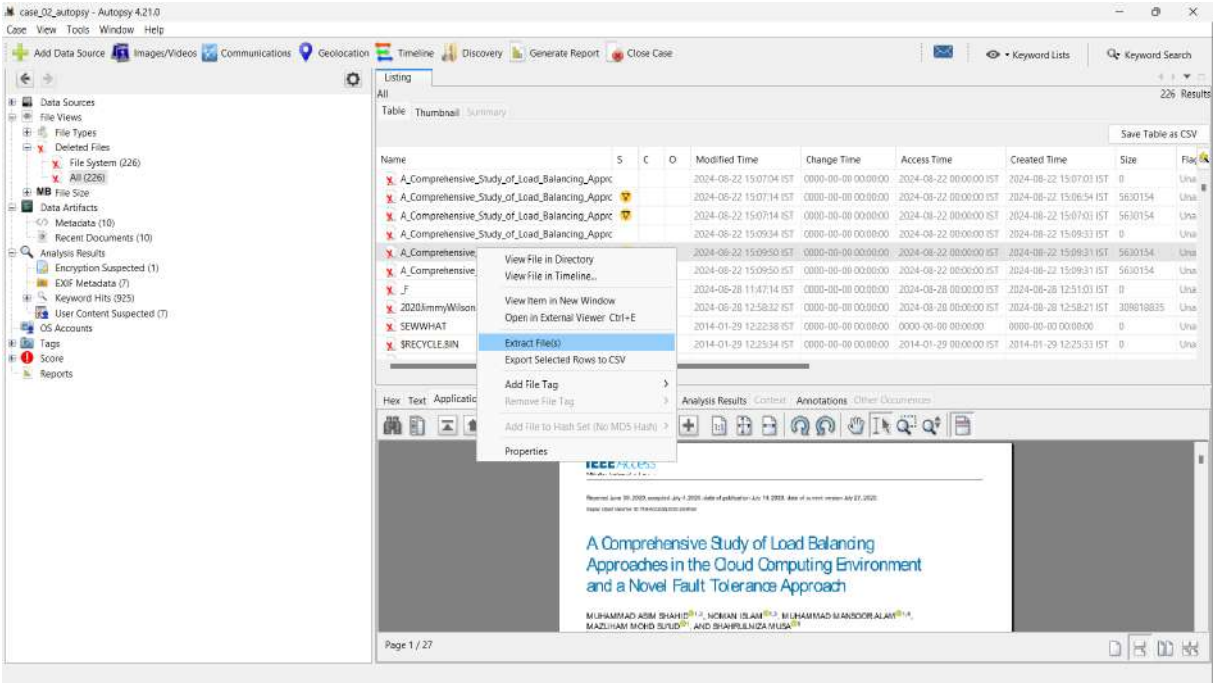
2 Different tools used for Forensic Investigation

2.1 Perform using Autopsy

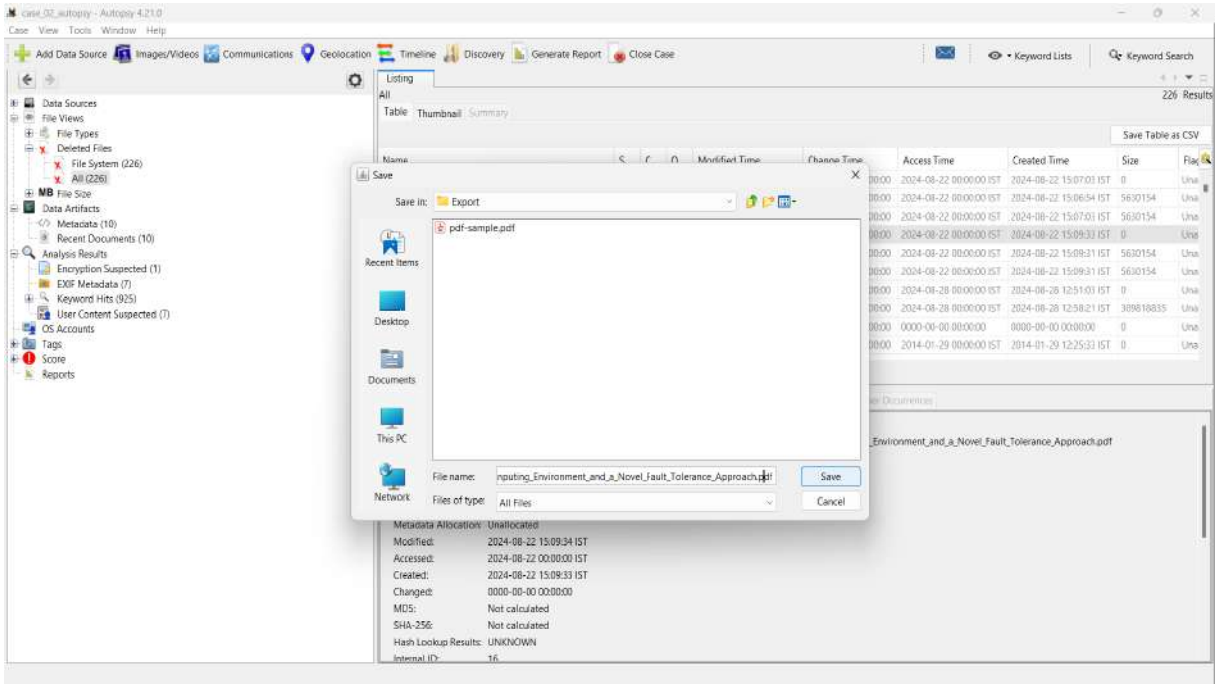
Steps to recover deleted files using Autopsy are as follows: -

1. Start Autopsy for Windows.

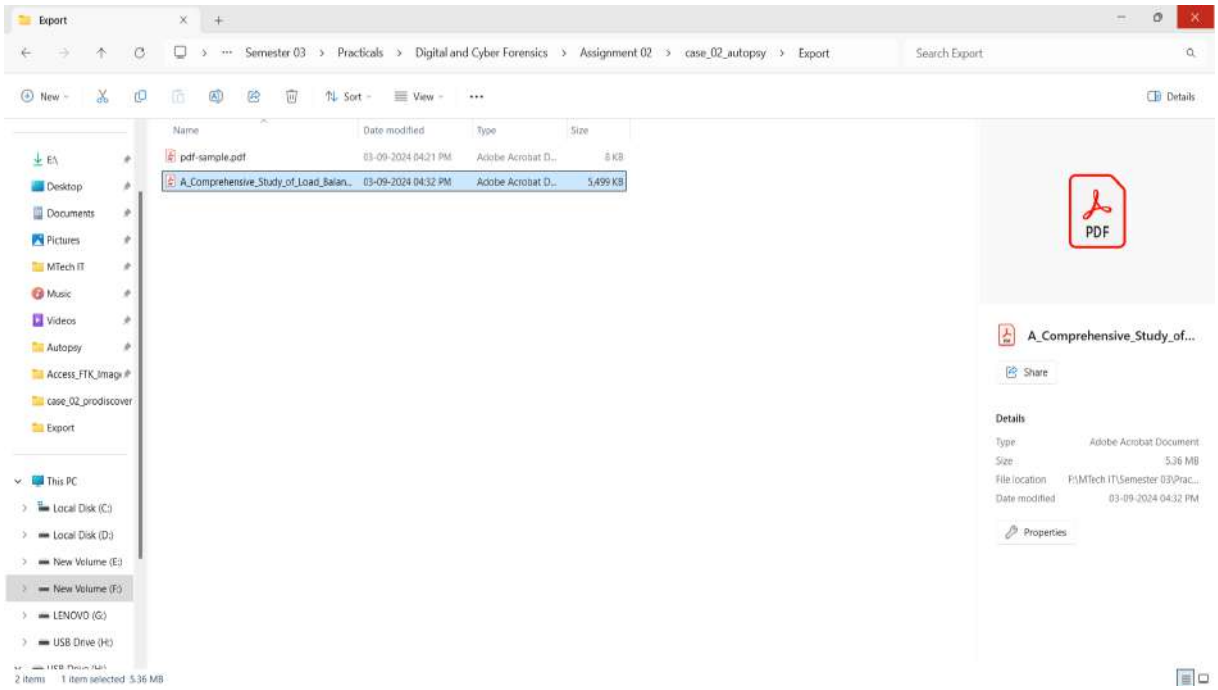
2. Select the file you want to recover. Right-Click on the file → Extract File(s).



3. Select the directory where you want to save it, and then click on Save.



4. The file is now recovered as in the screenshot provided

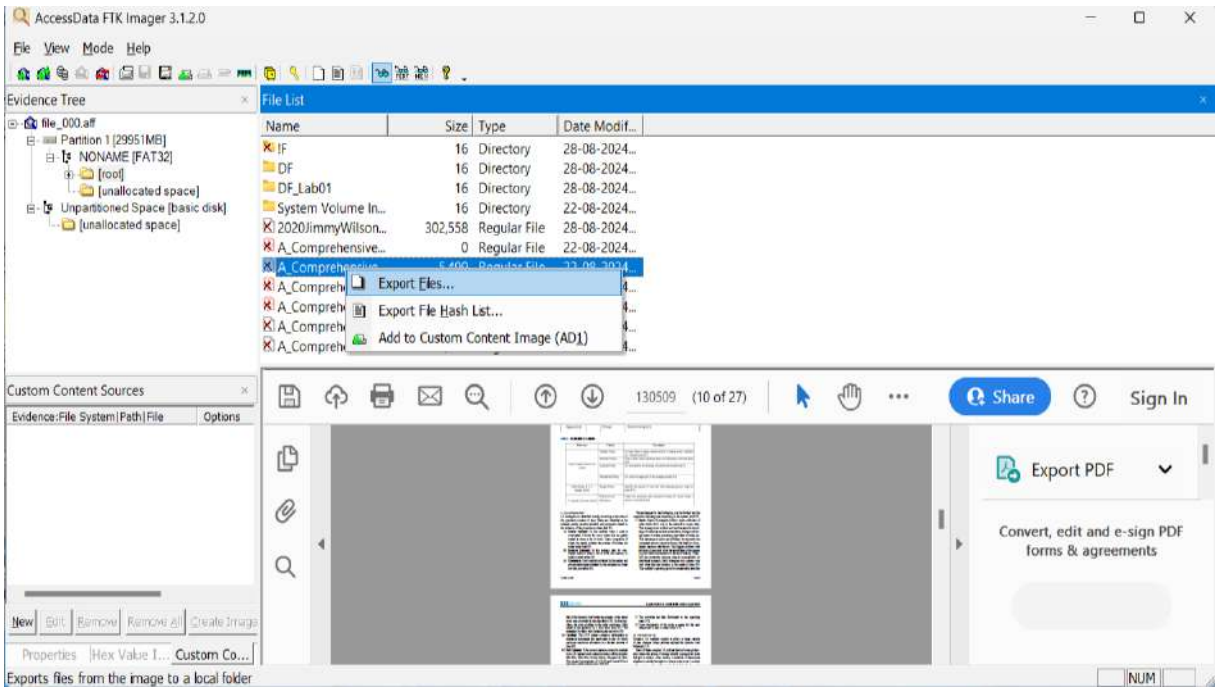


2.2 Perform using AccessData FTK Imager

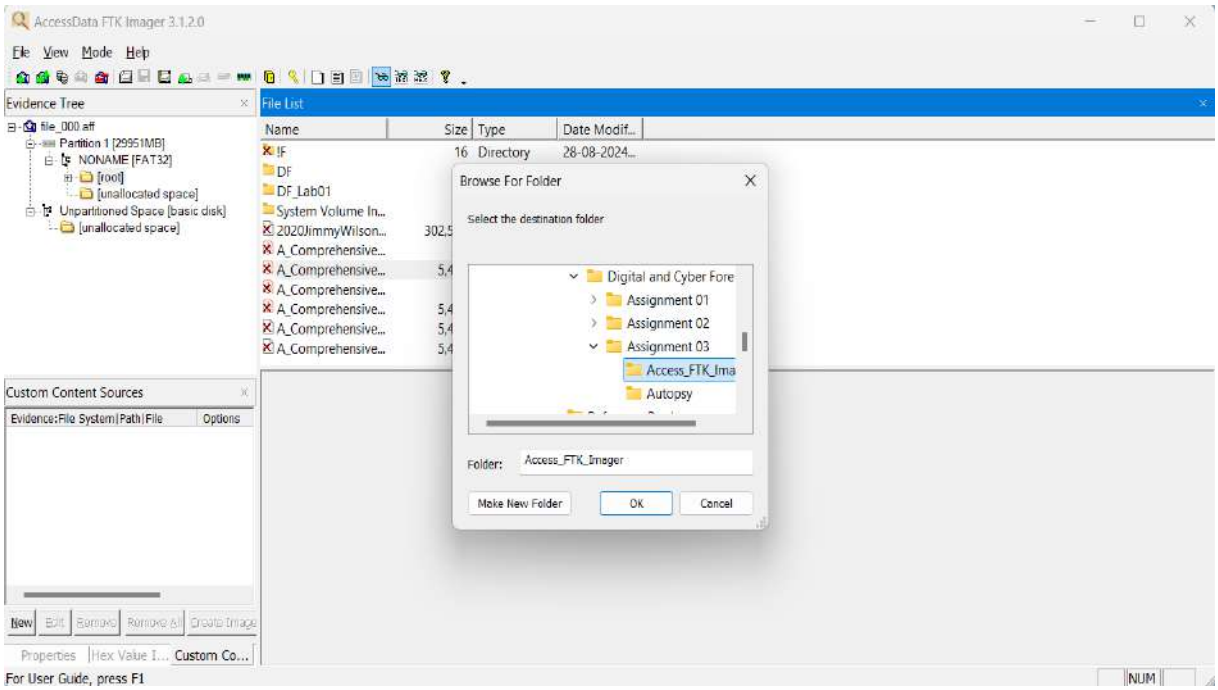
Steps to recover deleted files using AccessData FTK Imager are as follows: -

1. Start AccessData FTK Imager for Windows.

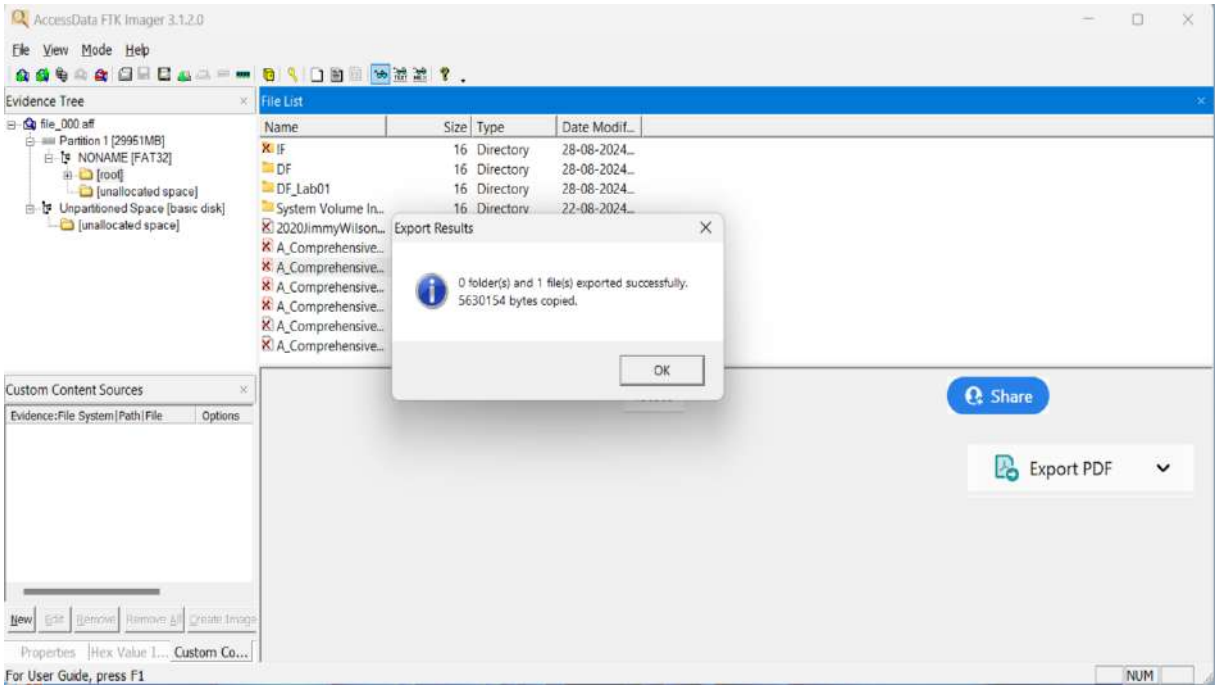
2. Select the file you want to recover. Right-Click on the file → Export File.



3. Select the Destination Folder you want to save and click OK.



4. The file is exported/saved successfully.



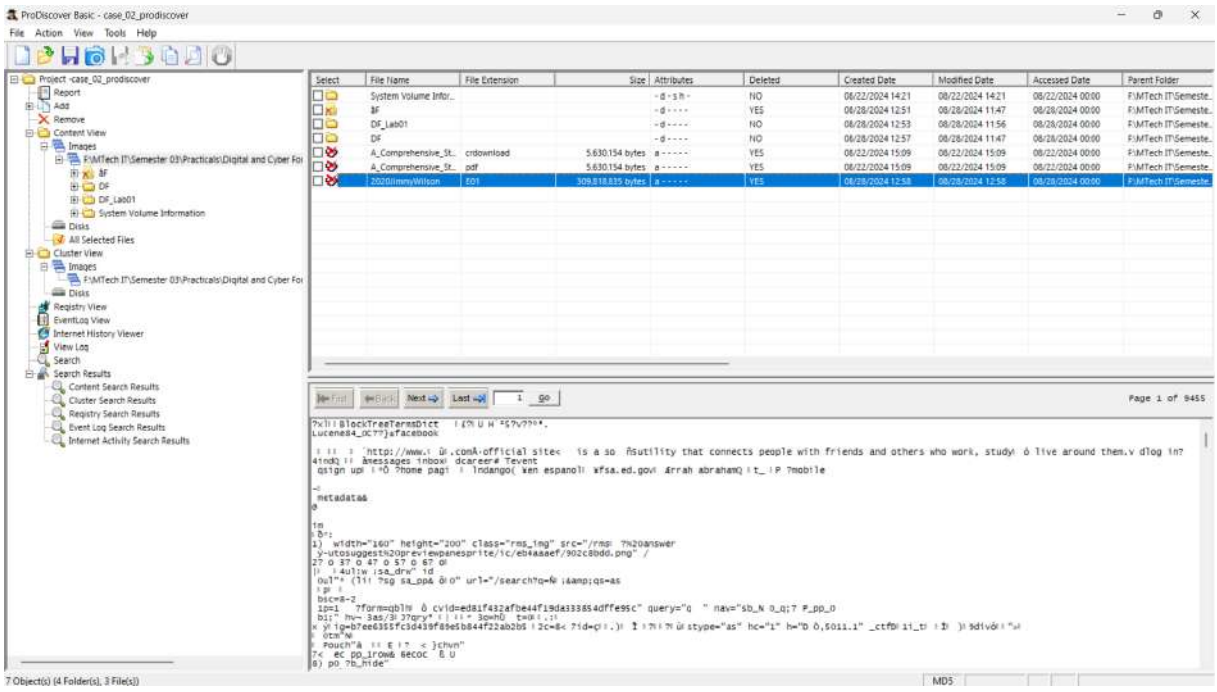
2.3 Perform using ProDiscover

Steps to recover deleted files using ProDiscover are as follows: -

1. Start ProDiscover for Windows.

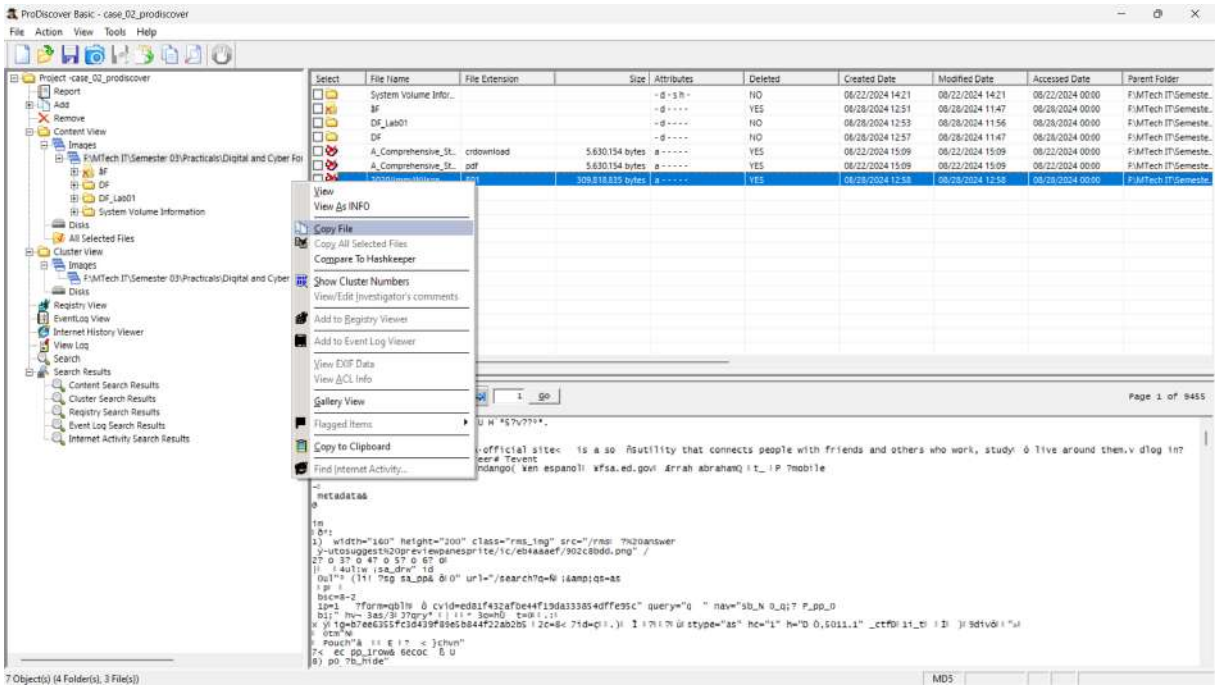
2. Open the project from which you want to recover the files from.

3. Select a file to recover from the work area.

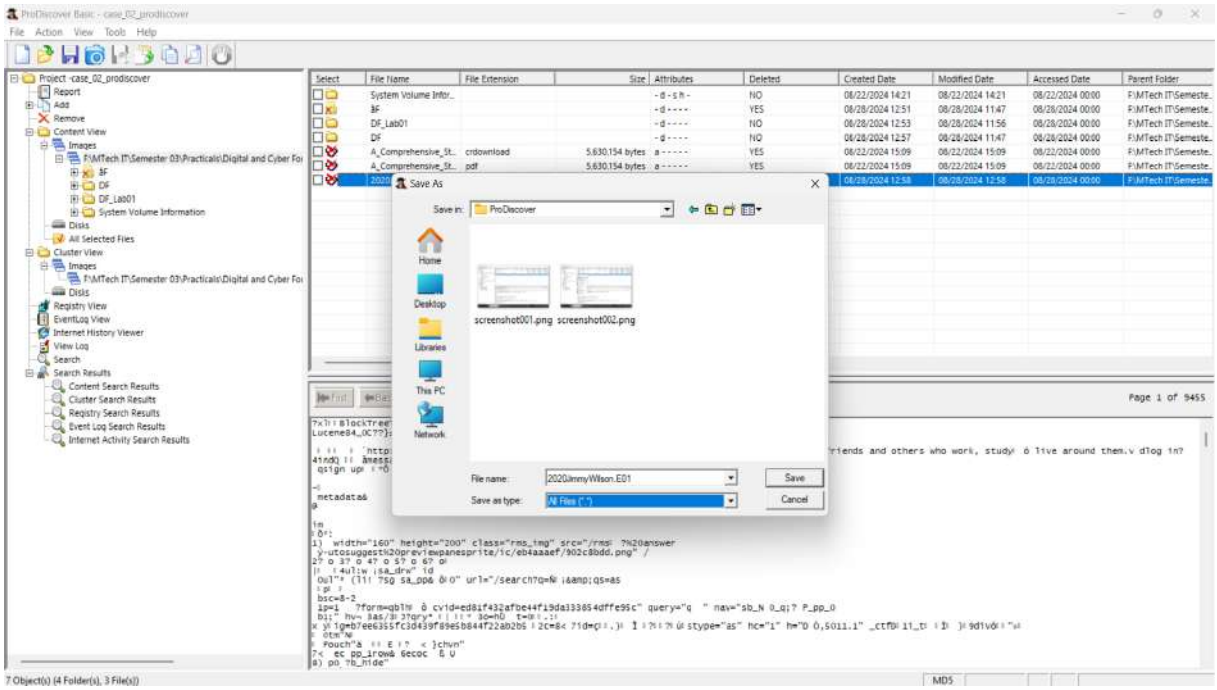


4. Right click on a file that you want to create a copy of the file.

5. ProDiscover a pop-up dialog with the choice to View or Recover the selected file. Select ”Copy File”.



6. Enter the desired location and file name to save the file as in the ”Save As” dialog box that appears and click ”Save”.



7. The file has been recovered.

LAB ASSIGNMENT - 04

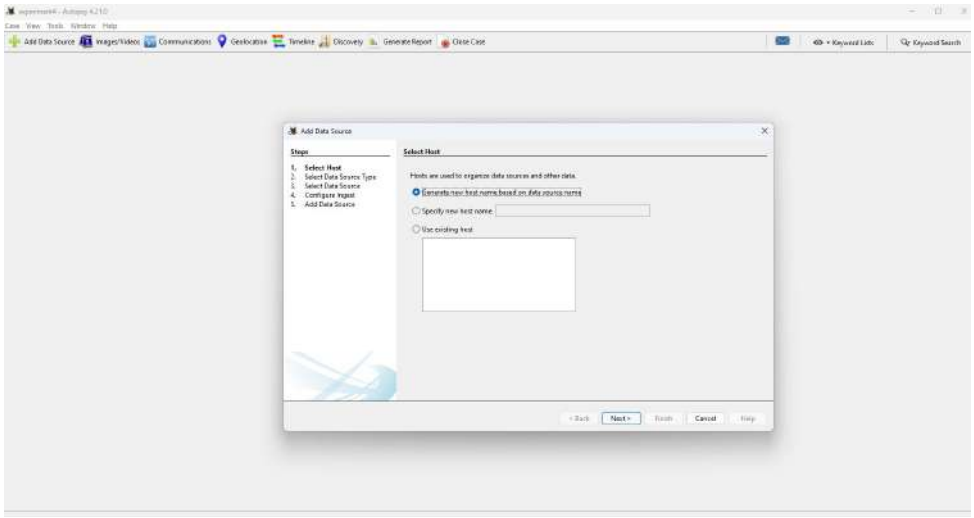
1 AIM

To Find Last Connected USB from a Suspected Drive or Image (using Autopsy).

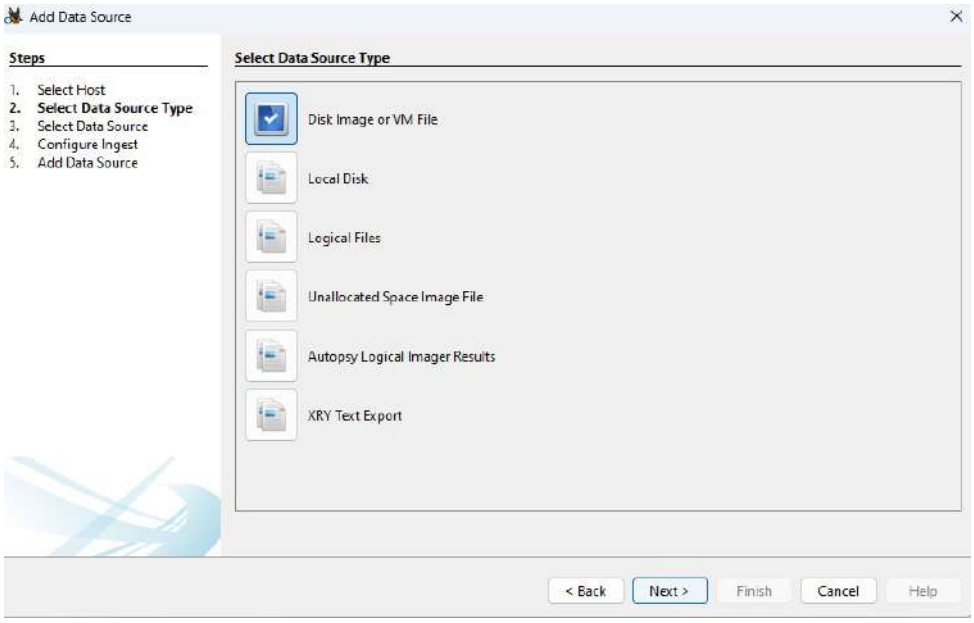
2 Steps to find last connected USB from a suspected drive or image using autopsy

Steps to find last connected USB from a suspected drive or image using autopsy are as follows :-

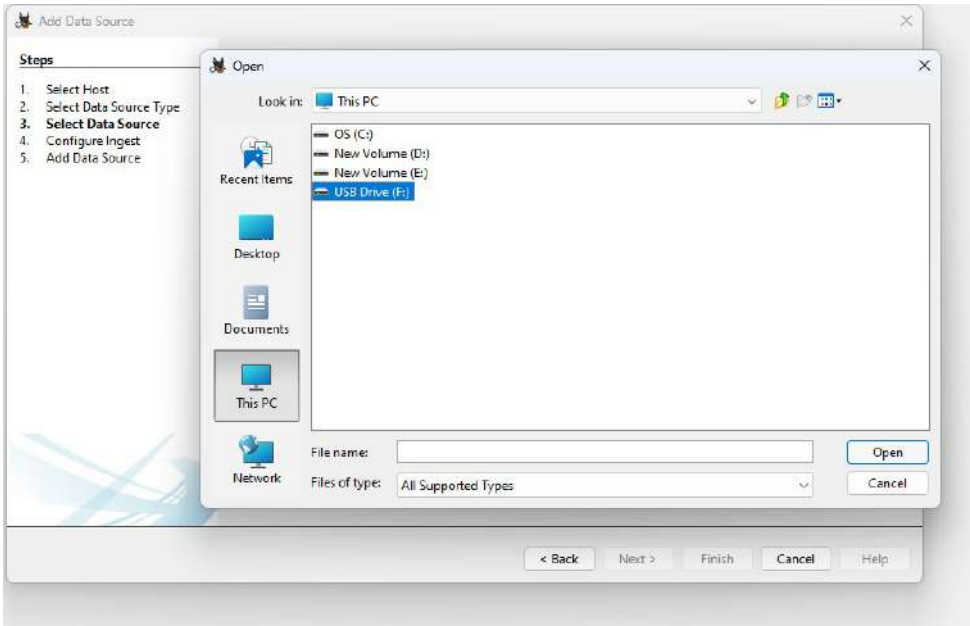
1. Run Autopsy software as Administrator. Create a new case and click on “Add Data Source”.



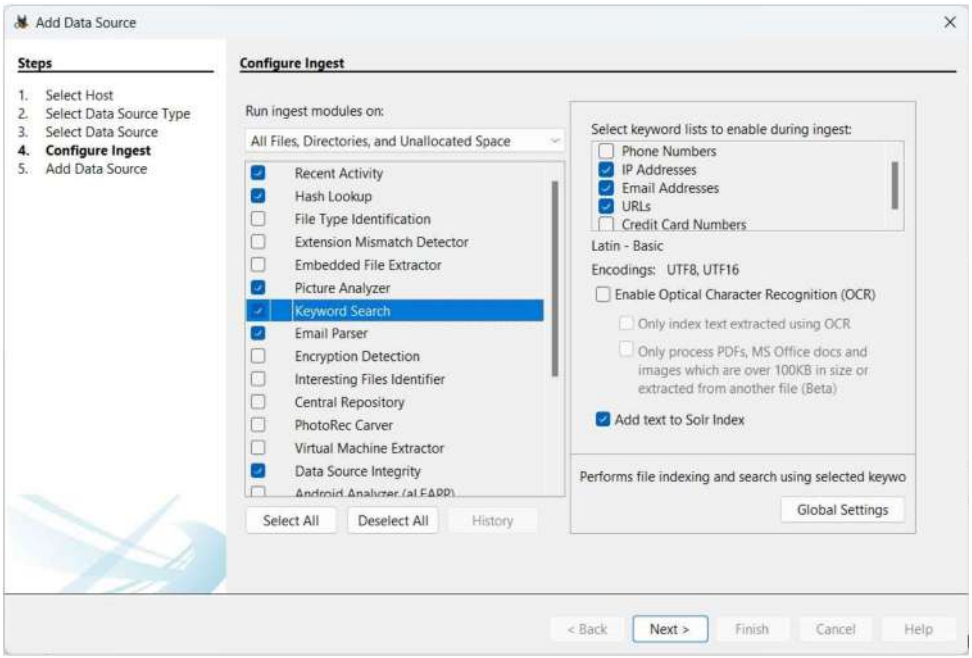
2. Select “Disk Image or VM File” and click Next.



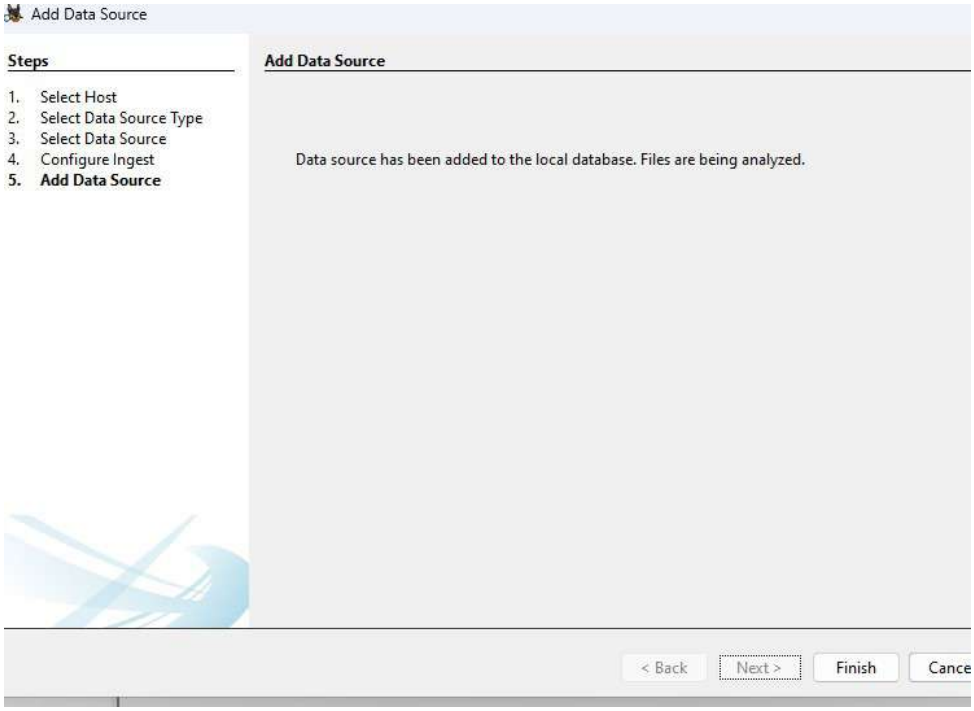
3. Browse the path and select the Disk Image (nps-2009-domexusers.E01) and click next.



4. Select the ingest modules shown below.

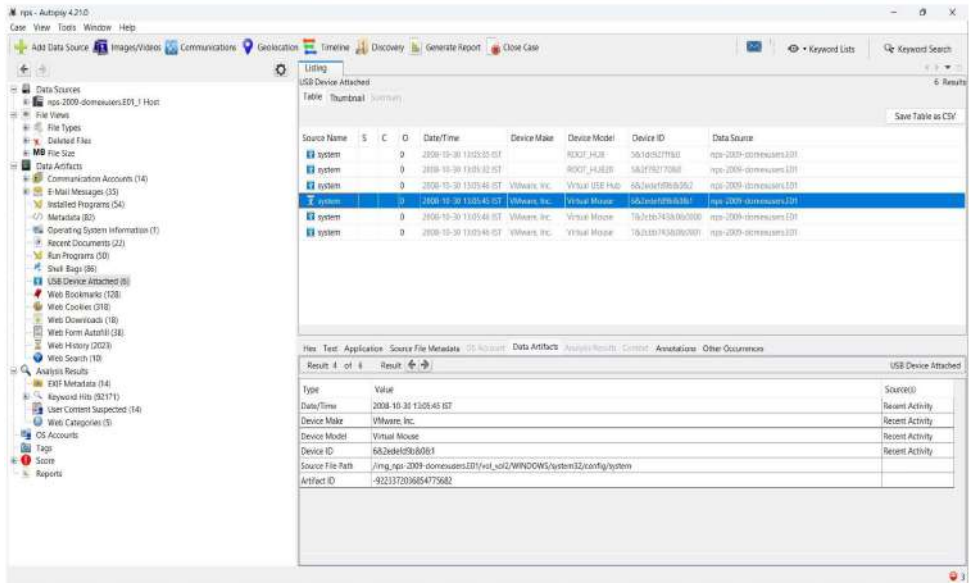


5. After the data source has been added, click Finish.



6. Now wait till the processing completes (in the bottom right of the window).

7. Under the “Data Artifacts” option, click on “USB Device Attached”.



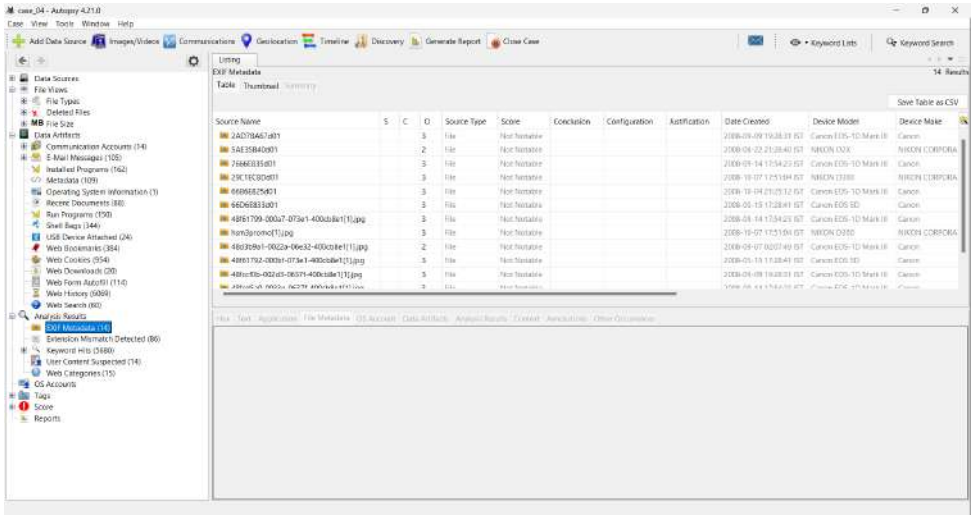
LAB ASSIGNMENT - 05

1 AIM

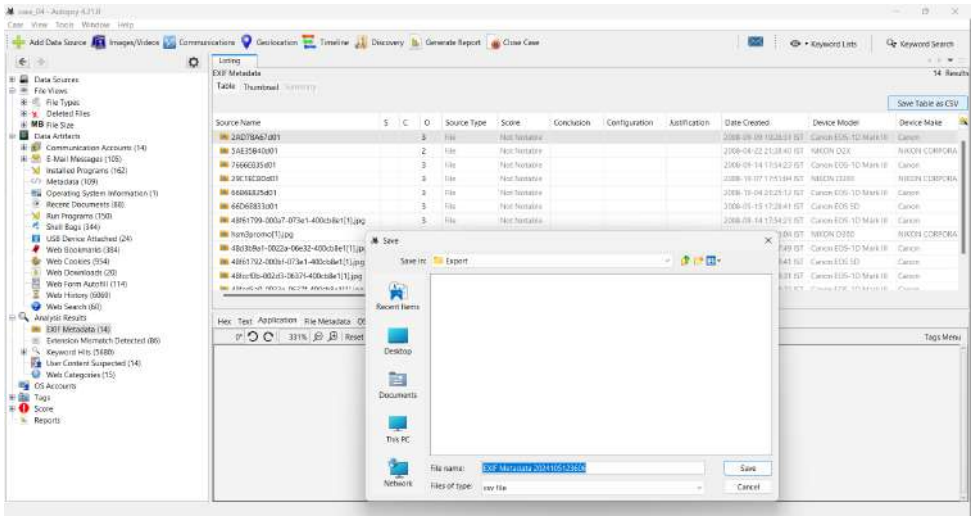
Extract Exchangeable image file format (EXIF) Data from Image Files (Using Autopsy).

2 Steps to extract EXIF Data from Image files.

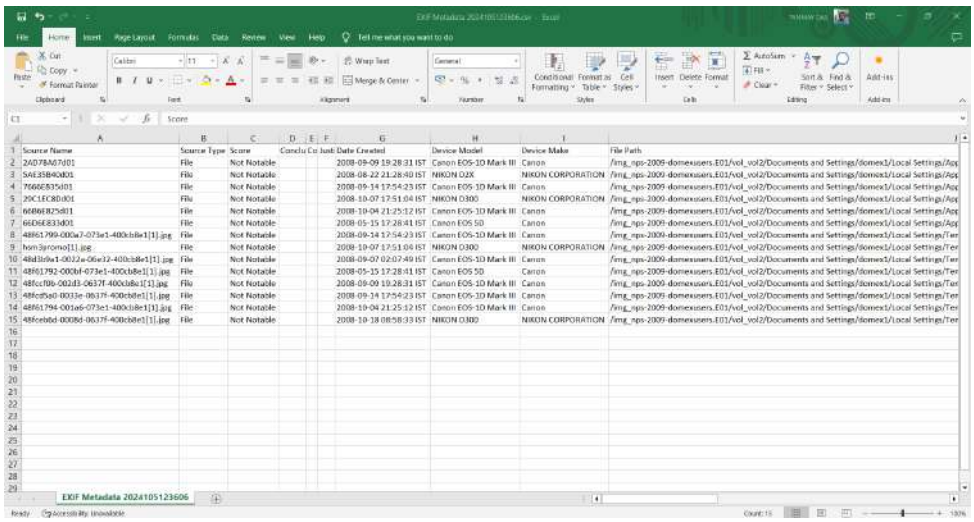
1. Select the ”EXIF Metadata” in the ”Analysis Results” section as provided in the screenshot.



2. Select the ”Save Table as CSV” button. Select the folder where you want to save the file, and the click on Save.



3. Open the CSV file. You will see the details of the image files as in the below screenshot.



Source Name	Source Type	Score	Conclu Co	Justi	Date Created	Device Model	Device Make	File Path
2A07BA67d01	File	Not Notable			2008-09-09 19:28:31 IST	Canon EOS-1D Mark III	Canon	/img_nps-2009-domexusers.E01/vol_vol2/Documents and Settings/domex1/Local Settings/Apj
5AE35B40d01	File	Not Notable			2008-08-22 21:28:40 IST	NIKON D2X	NIKON CORPORATION	/img_nps-2009-domexusers.E01/vol_vol2/Documents and Settings/domex1/Local Settings/Apj
7666E835d01	File	Not Notable			2008-09-14 17:54:23 IST	Canon EOS-1D Mark III	Canon	/img_nps-2009-domexusers.E01/vol_vol2/Documents and Settings/domex1/Local Settings/Apj
29C1EC80d01	File	Not Notable			2008-10-07 17:51:04 IST	NIKON D300	NIKON CORPORATION	/img_nps-2009-domexusers.E01/vol_vol2/Documents and Settings/domex1/Local Settings/Apj
6686E825d01	File	Not Notable			2008-10-04 21:25:12 IST	Canon EOS-1D Mark III	Canon	/img_nps-2009-domexusers.E01/vol_vol2/Documents and Settings/domex1/Local Settings/Apj
66D6E833d01	File	Not Notable			2008-05-15 17:28:41 IST	Canon EOS 5D	Canon	/img_nps-2009-domexusers.E01/vol_vol2/Documents and Settings/domex1/Local Settings/Apj
48861799-000a7-073e1-400cb8e1[1].jpg	File	Not Notable			2008-09-14 17:54:23 IST	Canon EOS-1D Mark III	Canon	/img_nps-2009-domexusers.E01/vol_vol2/Documents and Settings/domex1/Local Settings/Tem
hom3jeromo[1].jpg	File	Not Notable			2008-10-07 17:51:04 IST	NIKON D300	NIKON CORPORATION	/img_nps-2009-domexusers.E01/vol_vol2/Documents and Settings/domex1/Local Settings/Tem
48d1b9e1-0022a-06e12-400cb8e1[1].jpg	File	Not Notable			2008-09-07 02:07:49 IST	Canon EOS-1D Mark III	Canon	/img_nps-2009-domexusers.E01/vol_vol2/Documents and Settings/domex1/Local Settings/Tem
48861792-000bf-073e1-400cb8e1[1].jpg	File	Not Notable			2008-05-15 17:28:41 IST	Canon EOS 5D	Canon	/img_nps-2009-domexusers.E01/vol_vol2/Documents and Settings/domex1/Local Settings/Tem
48fccf0b-002d3-0637f-400cb8e1[1].jpg	File	Not Notable			2008-09-09 19:28:31 IST	Canon EOS-1D Mark III	Canon	/img_nps-2009-domexusers.E01/vol_vol2/Documents and Settings/domex1/Local Settings/Tem
48fcd5a0-0033e-0637f-400cb8e1[1].jpg	File	Not Notable			2008-09-14 17:54:23 IST	Canon EOS-1D Mark III	Canon	/img_nps-2009-domexusers.E01/vol_vol2/Documents and Settings/domex1/Local Settings/Tem
48861794-001a6-073e1-400cb8e1[1].jpg	File	Not Notable			2008-10-04 21:25:12 IST	Canon EOS-1D Mark III	Canon	/img_nps-2009-domexusers.E01/vol_vol2/Documents and Settings/domex1/Local Settings/Tem
48fceb8d-0008d-0637f-400cb8e1[1].jpg	File	Not Notable			2008-10-18 08:58:33 IST	NIKON D300	NIKON CORPORATION	/img_nps-2009-domexusers.E01/vol_vol2/Documents and Settings/domex1/Local Settings/Tem

LAB ASSIGNMENT - 06

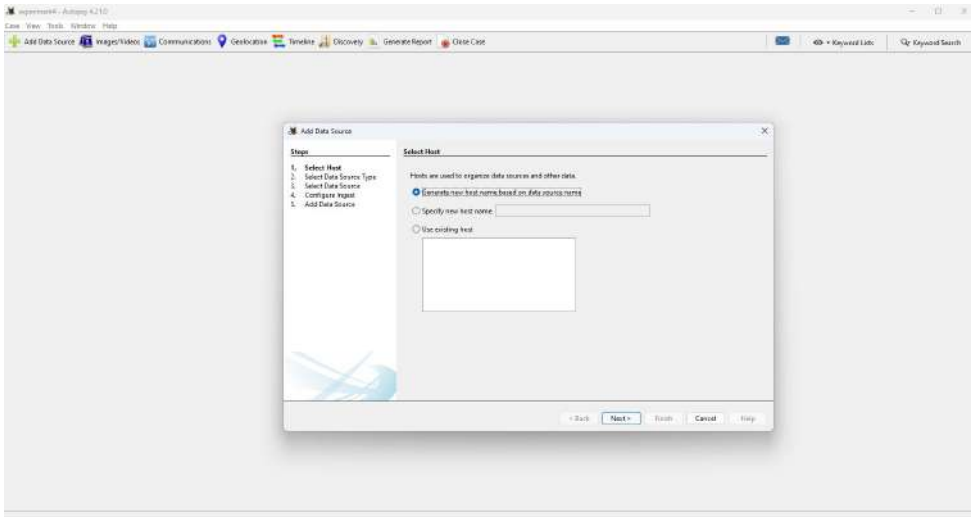
1 AIM

To collect the Email Evidence from a Suspected Drive or Image (using Autopsy).

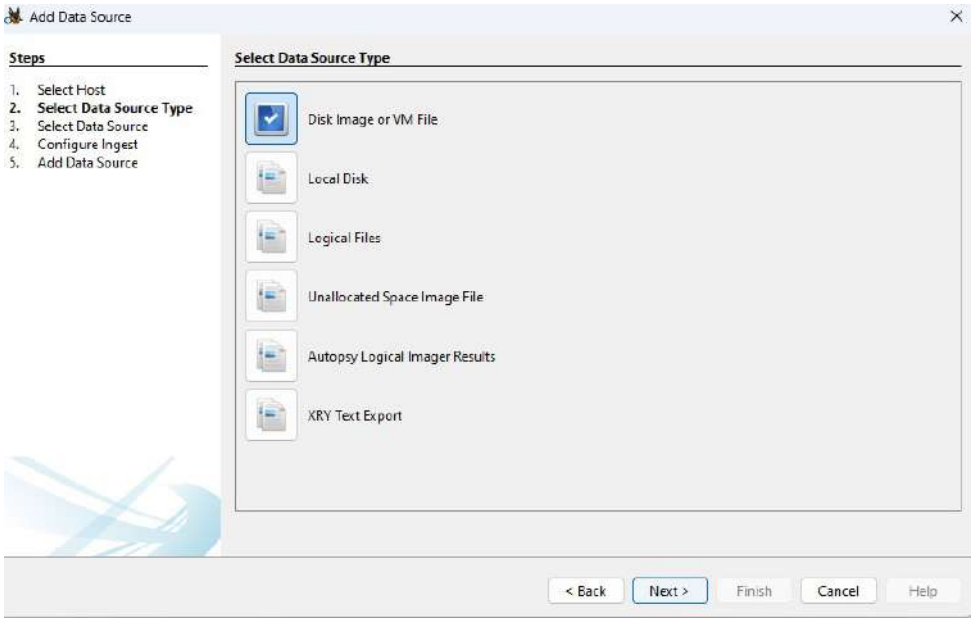
2 Steps to collect the Email Evidence from a Suspected Drive or Image (using Autopsy).

Steps to collect the Email Evidence from a Suspected Drive or Image (using Autopsy).are as follows :-

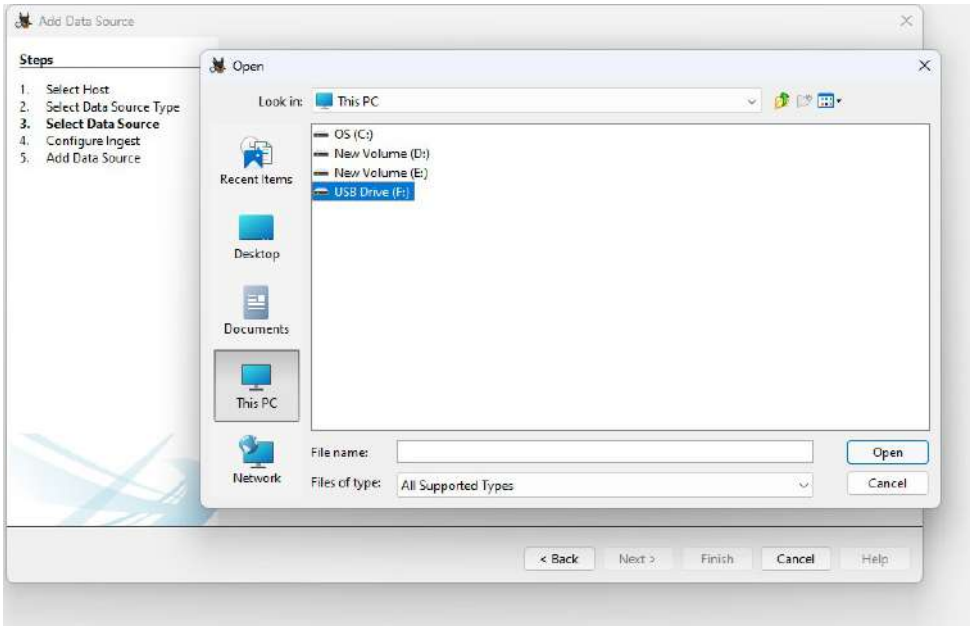
1. Run Autopsy software as Administrator. Create a new case and click on “Add Data Source”.



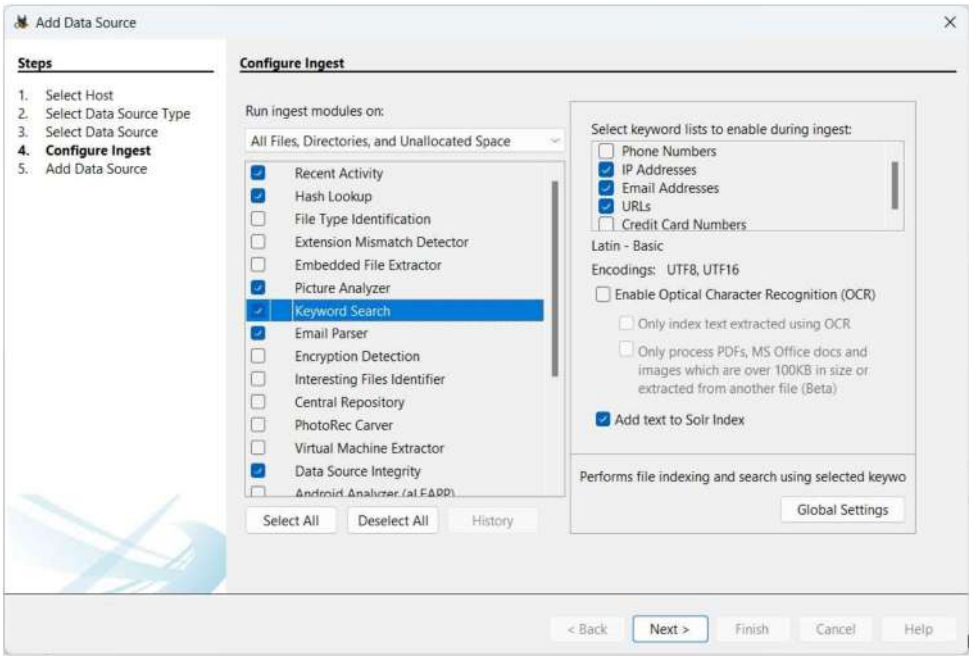
2. Select “Disk Image or VM File” and click Next.



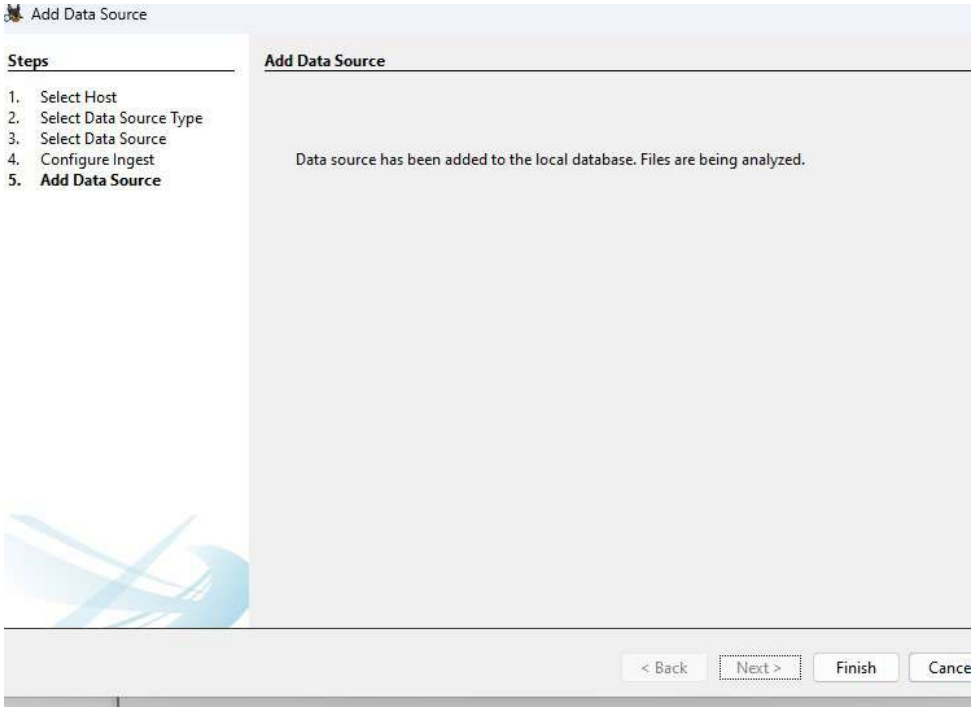
3. Browse the path and select the Disk Image (nps-2009-domexusers.E01) and click next.



4. Select the ingest modules shown below.

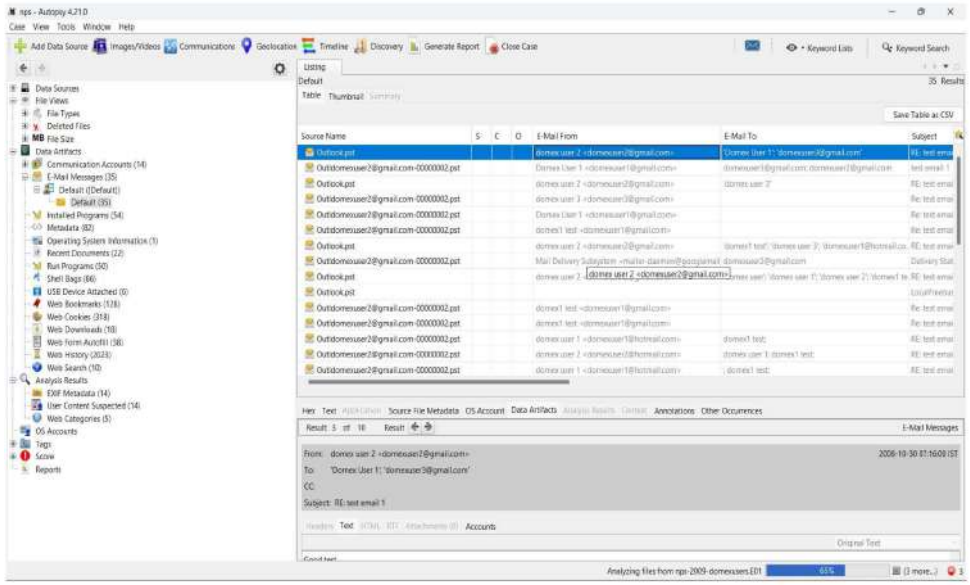


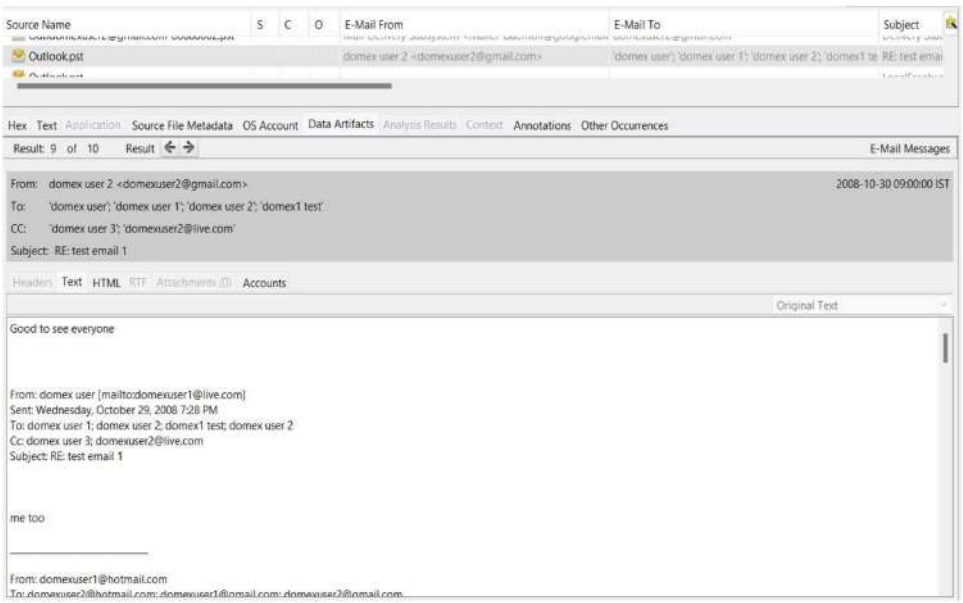
5. After the data source has been added, click Finish.

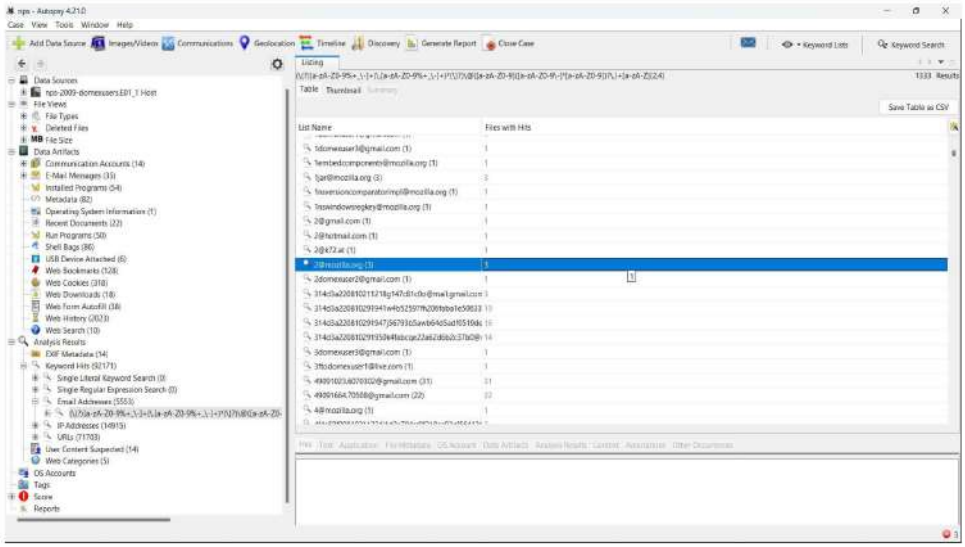


6. Now wait till the processing completes (in the bottom right of the window).

7. Under the "Data Artifacts" option, expand E-Mail Messages as shown below.




Source Name
S
C
O
E-Mail From
E-Mail To
Subject
Outlook.pst
domex user 2 <domexuser2@gmail.com>
'domex user'; 'domex user 1'; 'domex user 2'; 'domex1 te
RE: test emai
Hex
Text
Application
Source File Metadata
OS Account
Data Artifacts
Analysis Results
Context
Annotations
Other Occurrences
Result: 9 of 10
Result
E-Mail Messages
From: domex user 2 <domexuser2@gmail.com>
2008-10-30 09:00:00 IST
To: 'domex user'; 'domex user 1'; 'domex user 2'; 'domex1 test'
CC: 'domex user 3'; 'domexuser2@live.com'
Subject: RE: test email 1
Headers
Text
HTML
RTF
Attachments (0)
Accounts
Original Text
Good to see everyone
From: domex user [mailto:domexuser1@live.com]
Sent: Wednesday, October 29, 2008 7:28 PM
To: domex user 1; domex user 2; domex1 test; domex user 2
Cc: domex user 3; domexuser2@live.com
Subject: RE: test email 1
me too
From: domexuser1@hotmail.com


Case
View
Tools
Window
Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
Listing
Table
Thumbnail
Save Table as CSV
List Name
Files with Hits
Data Sources
File Views
Data Artifacts
Analysis Results
OS Accounts
Tags
Score
Reports

LAB ASSIGNMENT - 07

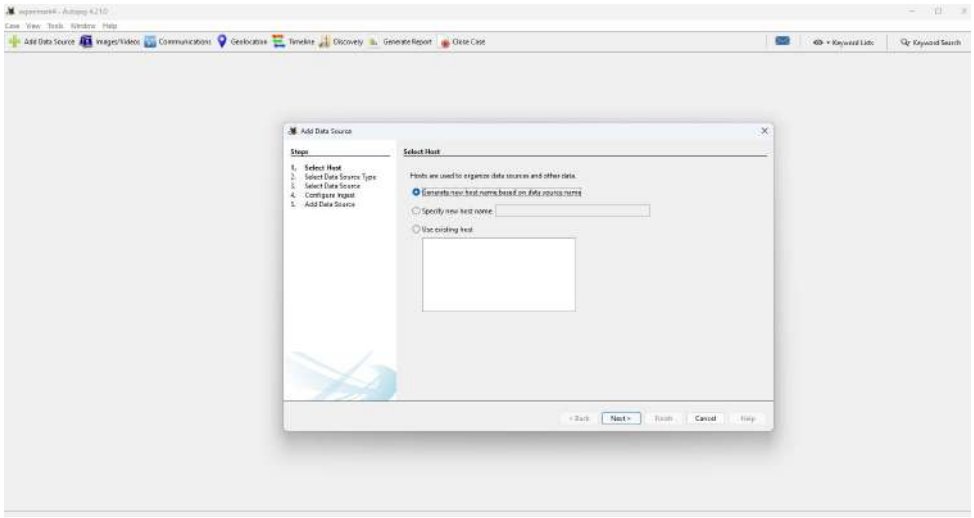
1 AIM

To Extract Browser Artifacts from a Suspected Drive or Image (using Autopsy).

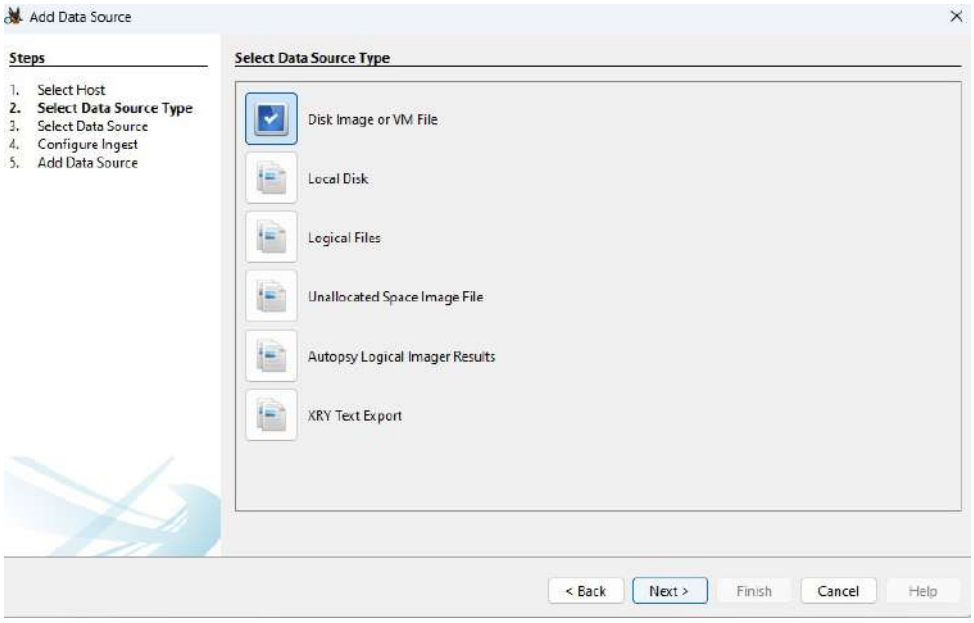
2 Steps to Extract Browser Artifacts from a Suspected Drive or Image (using Autopsy).

Steps to Extract Browser Artifacts from a Suspected Drive or Image (using Autopsy) are as follows :-

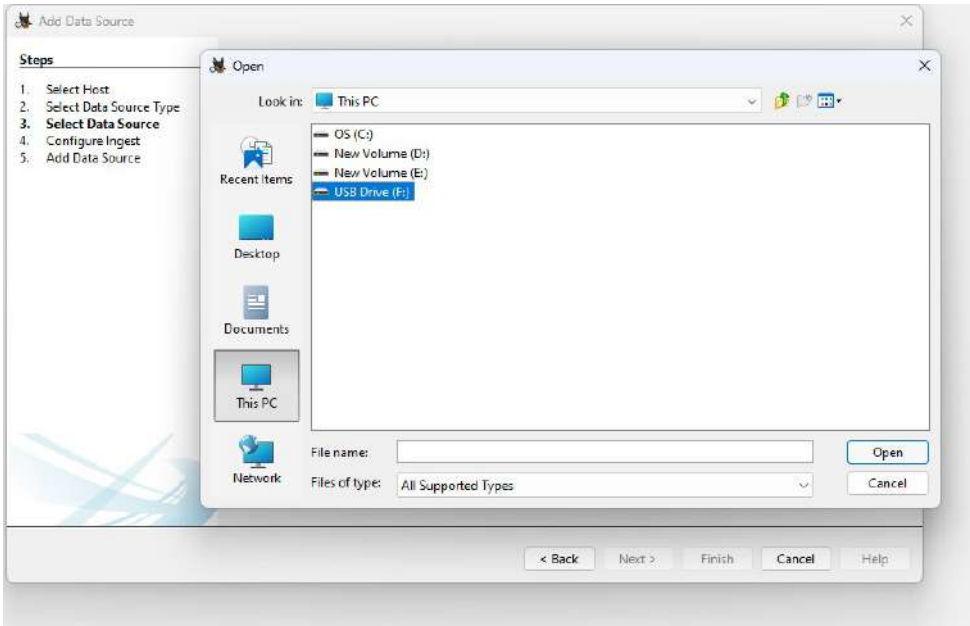
1. Run Autopsy software as Administrator. Create a new case and click on “Add Data Source”.



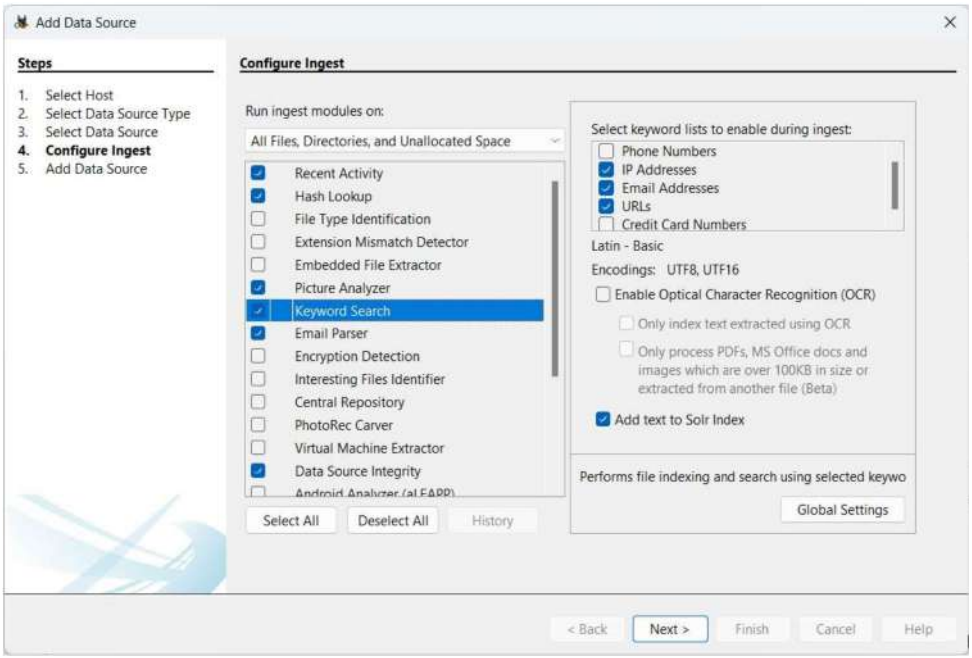
2. Select “Disk Image or VM File” and click Next.



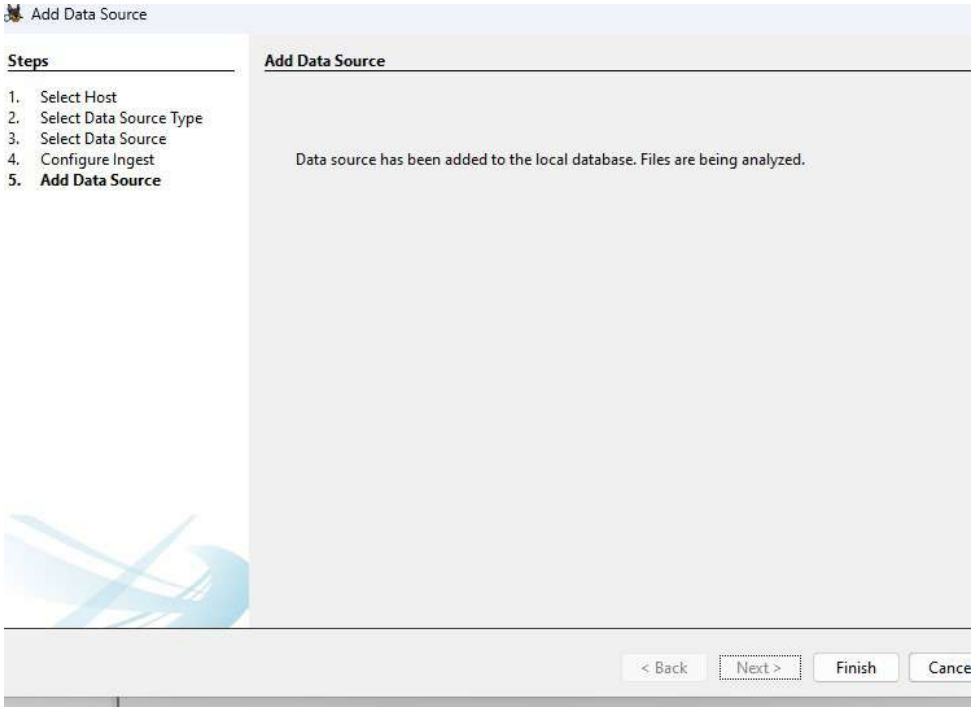
3. Browse the path and select the Disk Image (nps-2009-domexusers.E01) and click next.



4. Select the ingest modules shown below.

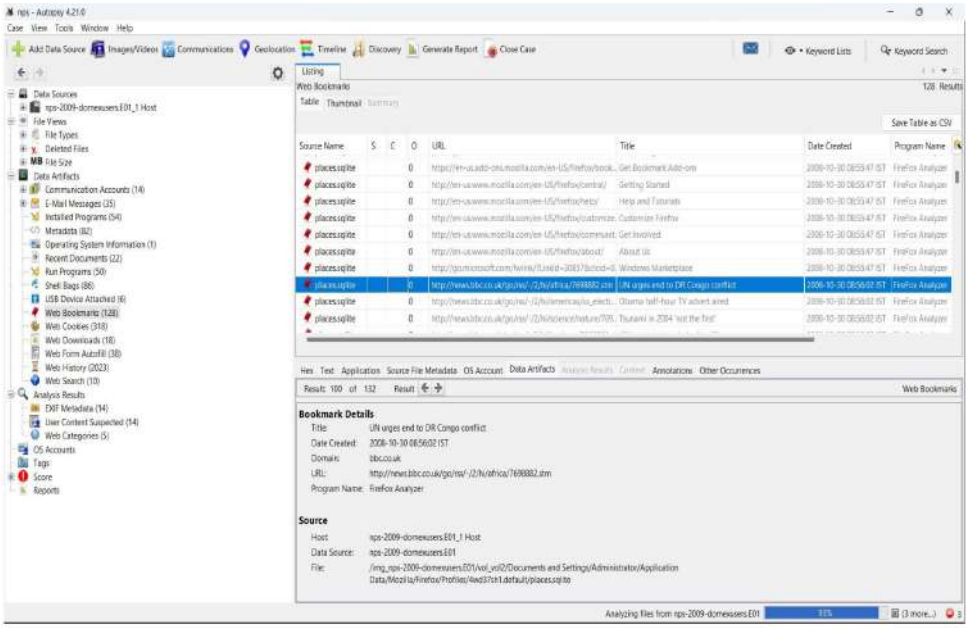


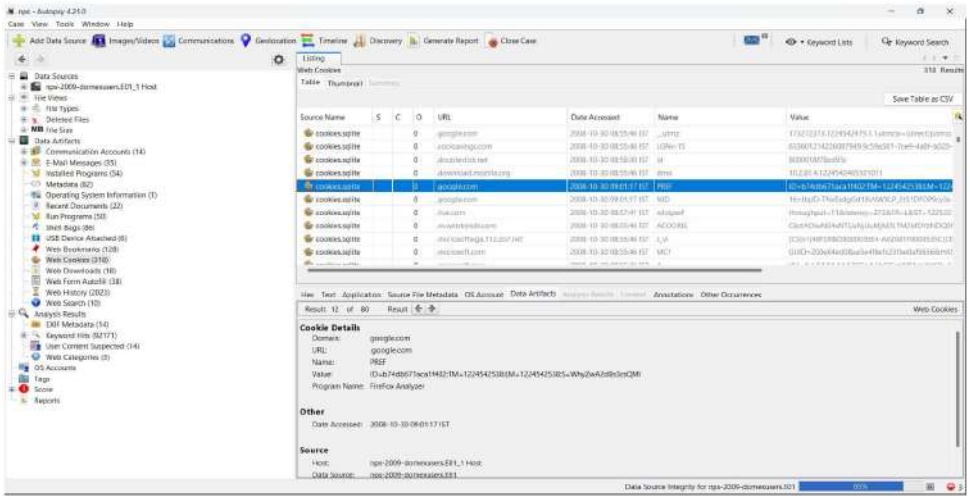
5. After the data source has been added, click Finish.

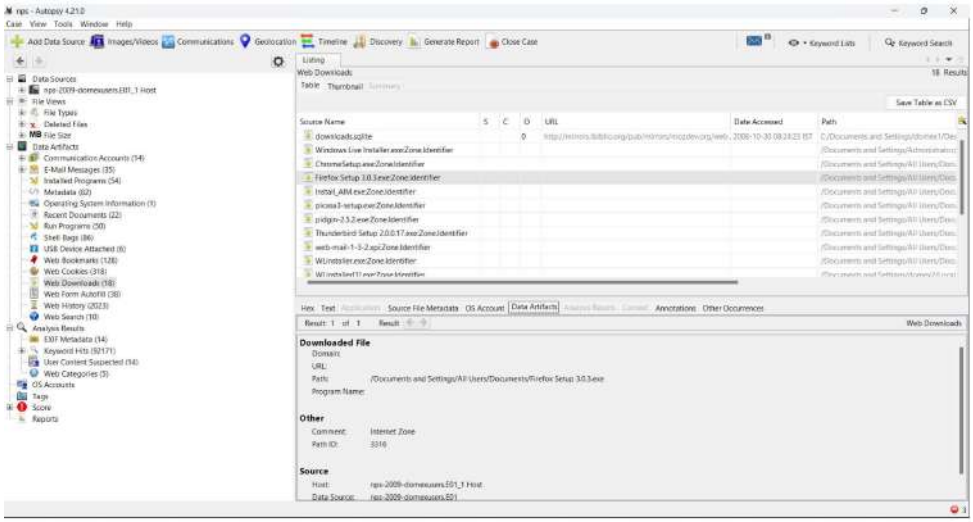


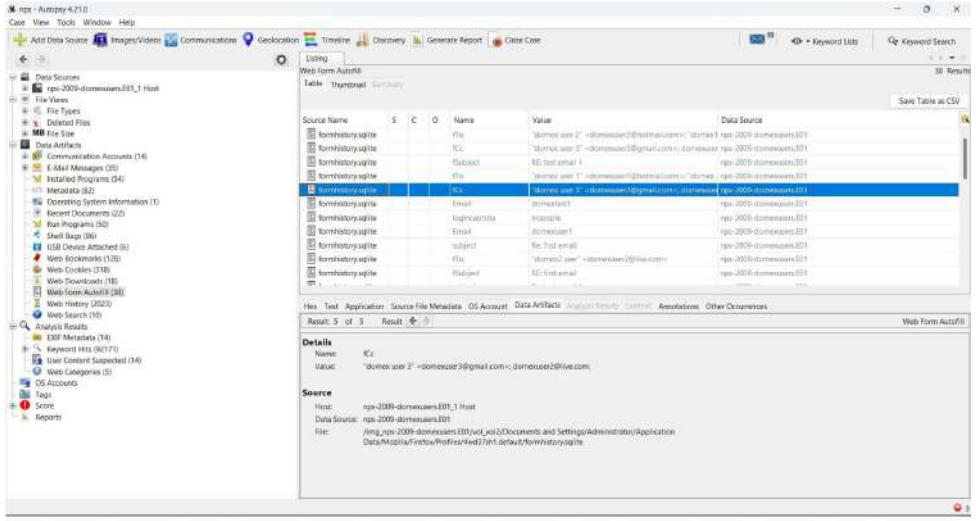
6. Now wait till the processing completes (in the bottom right of the window).

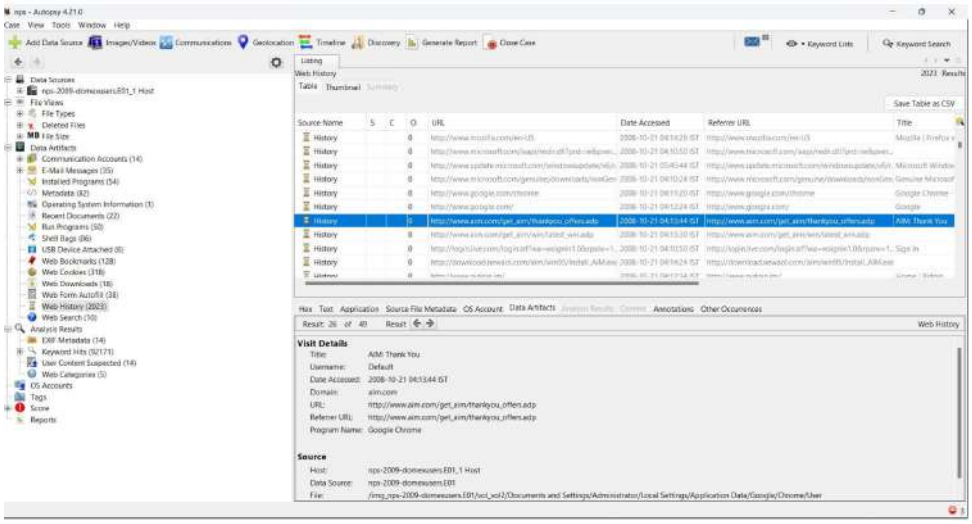
7. Under the "Data Artifacts" option, expand E-Mail Messages as shown below.

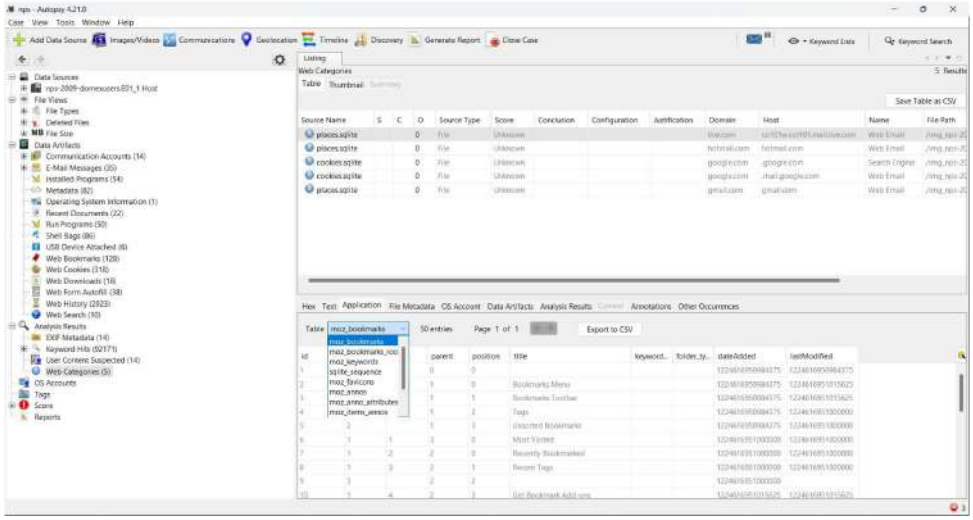












LAB ASSIGNMENT - 08

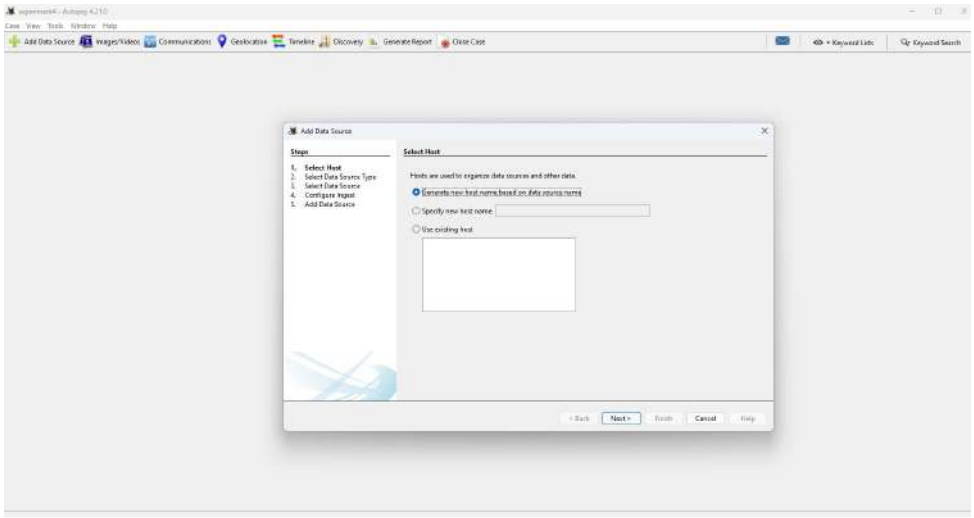
1 AIM

Perform a full live forensics case investigation using Autopsy.

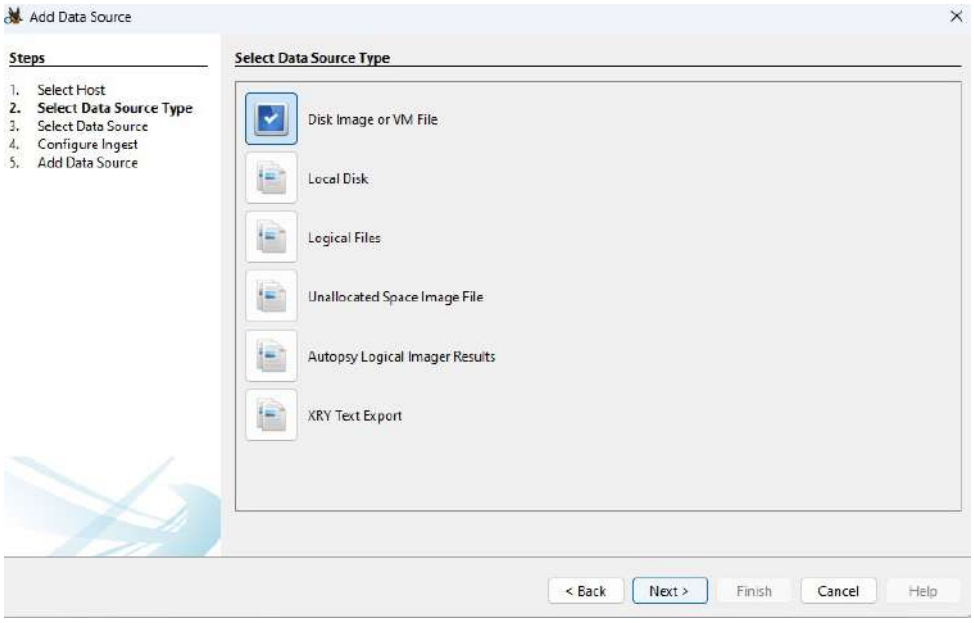
2 Steps to perform a full live forensics case investigation using Autopsy.

Steps to perform a full live forensics case investigation using autopsy are as follows :-

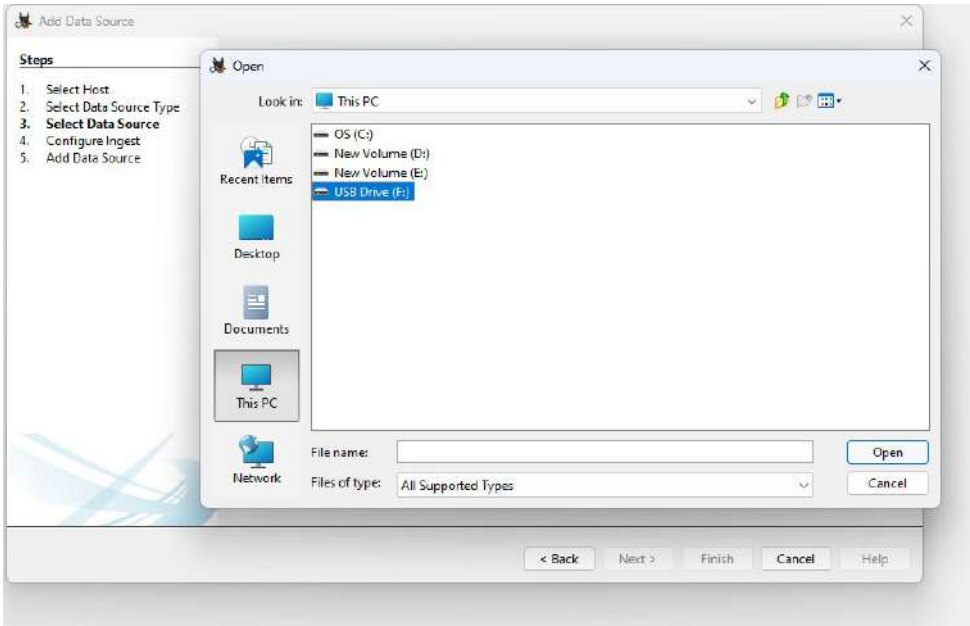
1. Run Autopsy software as Administrator. Create a new case and click on “Add Data Source”.



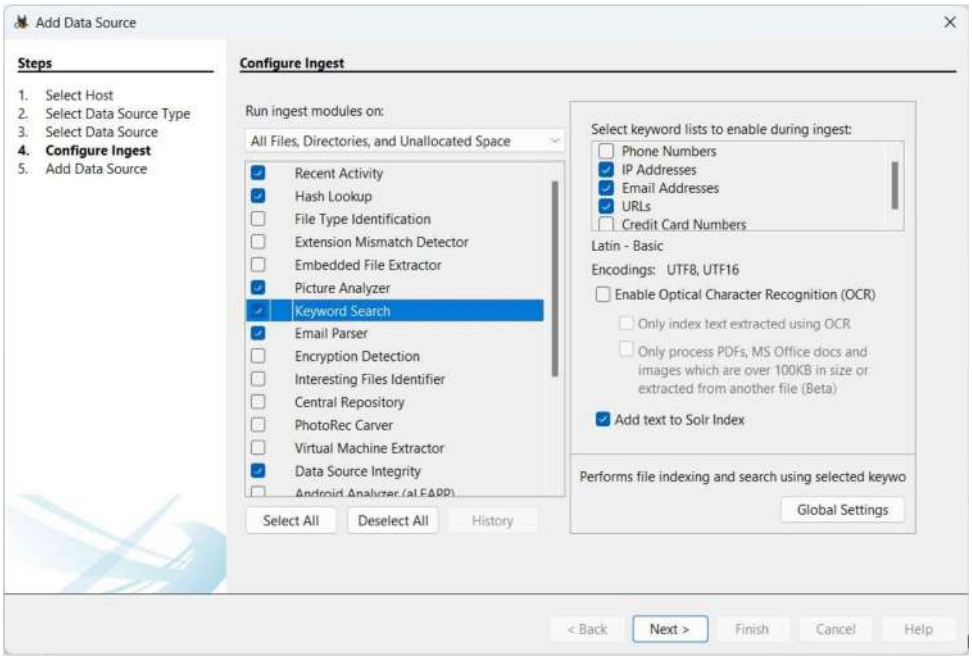
2. Select “Disk Image or VM File” and click Next.



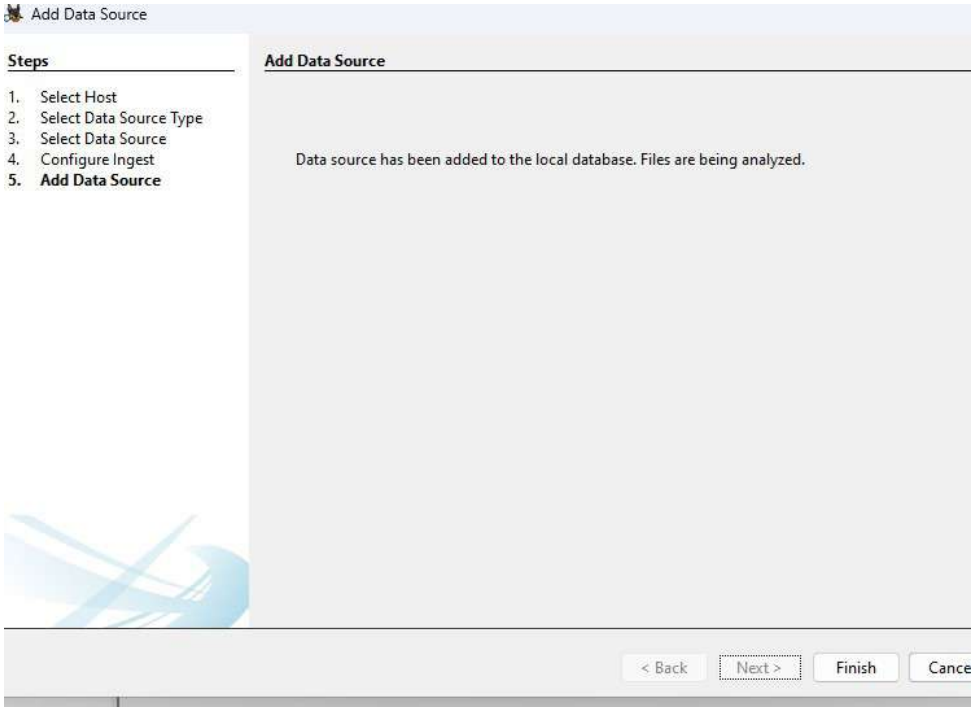
3. Browse the path and select the Disk Image (nps-2009-domexusers.E01) and click next.



4. Select the ingest modules shown below.

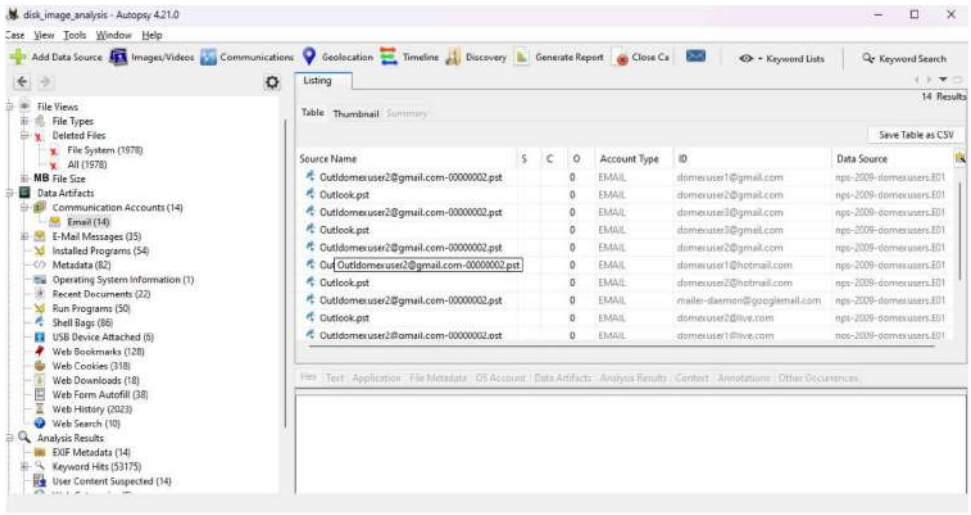


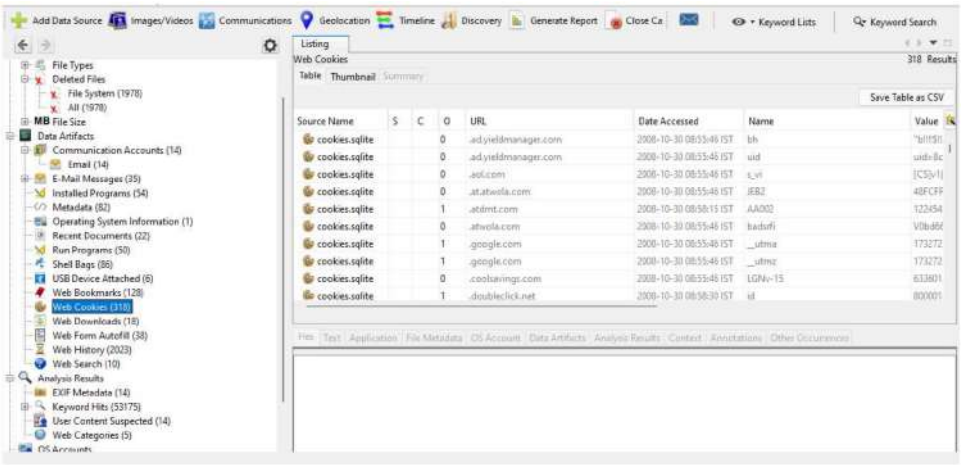
5. After the data source has been added, click Finish.

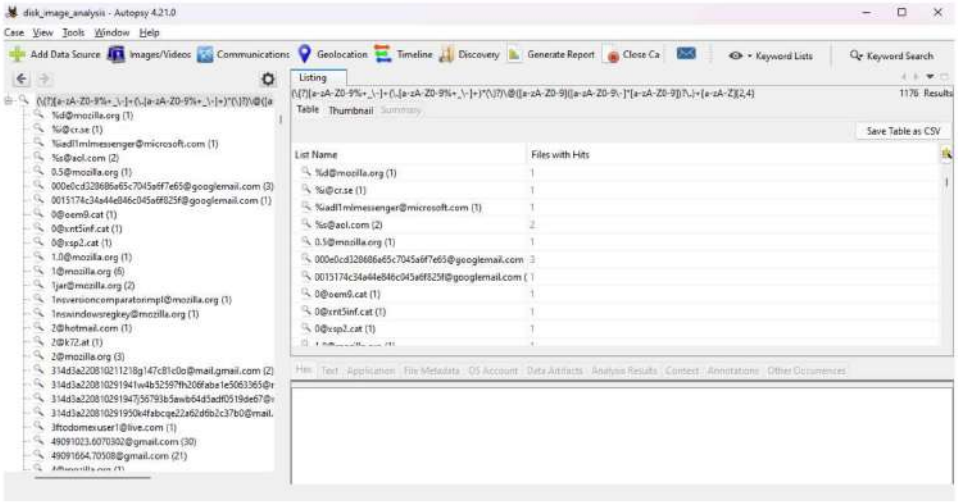


6. Now wait till the processing completes (in the bottom right of the window).

7. Explore the various tabs on right side to investigate the files.




Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Ca
Keyword Lists
Keyword Search
Listing
Web Cookies
318 Results
Table
Thumbnail
Summary
Save Table as CSV
Source Name
S
C
O
URL
Date Accessed
Name
Value
cookies.sqlite
2008-10-30 08:55:46 IST
2008-10-30 08:56:15 IST
File Types
Deleted Files
File System (1978)
All (1978)
MB File Size
Data Artifacts
Communication Accounts (14)
Email (14)
E-Mail Messages (35)
Installed Programs (54)
Metadata (82)
Operating System Information (1)
Recent Documents (22)
Run Programs (50)
Shell Bags (86)
USB Device Attached (6)
Web Bookmarks (128)
Web Cookies (318)
Web Downloads (18)
Web Form Autofill (38)
Web History (2023)
Web Search (10)
Analysis Results
EXIF Metadata (14)
Keyword Hits (53175)
User Content Suspected (14)
Web Categories (5)
OS Accounts


disk_image_analysis - Autopsy 4.21.0
Case
View
Tools
Window
Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Ca
Keyword Lists
Keyword Search
Listing
1176 Results
Table
Thumbnail
Summary
Save Table as CSV
List Name
Files with Hits
%d@mozilla.org (1)
%i@cr.se (1)
%iadl1mlmessenger@microsoft.com (1)
%s@aol.com (2)
0.5@mozilla.org (1)
000e0cd328686a65c7045a6f7e65@googlemail.com (3)
0015174c34a44e846c045a6f825f@googlemail.com (1)
0@oem9.cat (1)
0@xnt5inf.cat (1)
0@xsp2.cat (1)
1.0@mozilla.org (1)
1@mozilla.org (6)
1jar@mozilla.org (2)
1nswindowsregkey@mozilla.org (1)
2@hotmail.com (1)
2@k72.at (1)
2@mozilla.org (3)
3ftodomexuser1@live.com (1)
49091023.6070302@gmail.com (30)
49091664.70508@gmail.com (21)

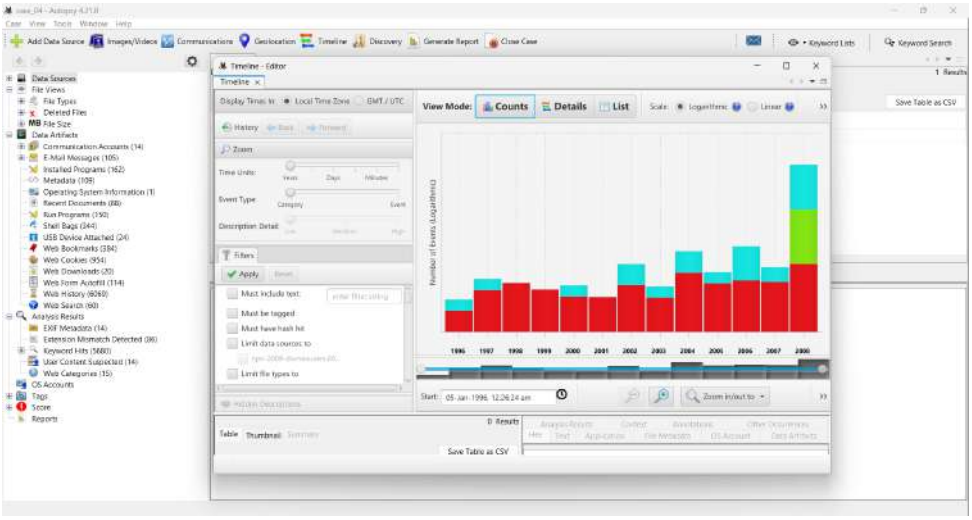
LAB ASSIGNMENT - 09

1 AIM

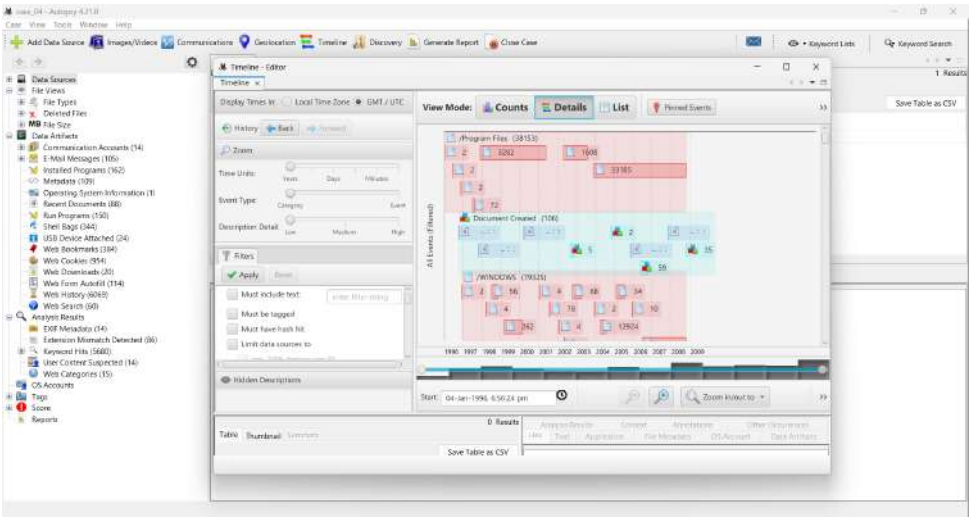
Generate a Timeline and Discovery of a given Forensic Image and generate its compatible report (using Autopsy).

2 Steps to generate the Timeline of a Forensic Image

1. Click on Timeline at the top. The screen will be displayed as follows.

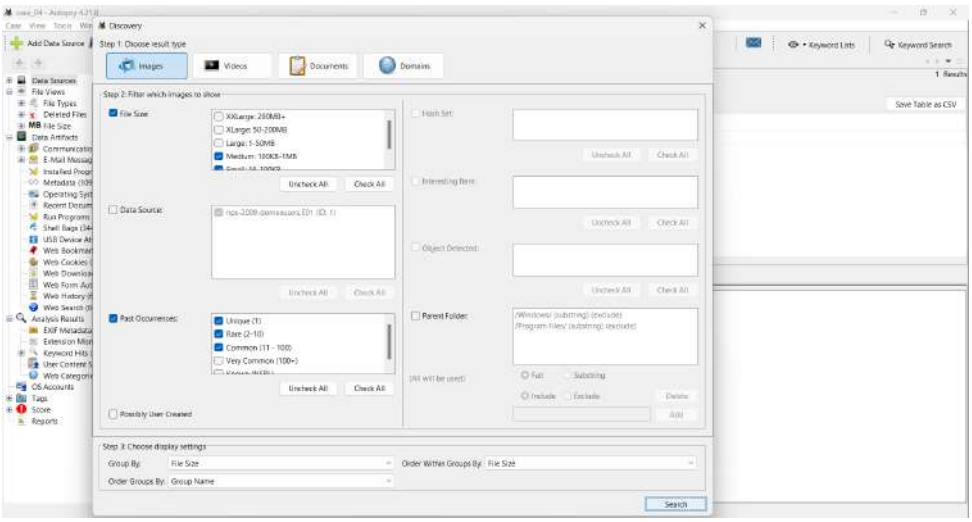


2. Next, click on the ”Details” button, It will display the number of events created in the respective years.



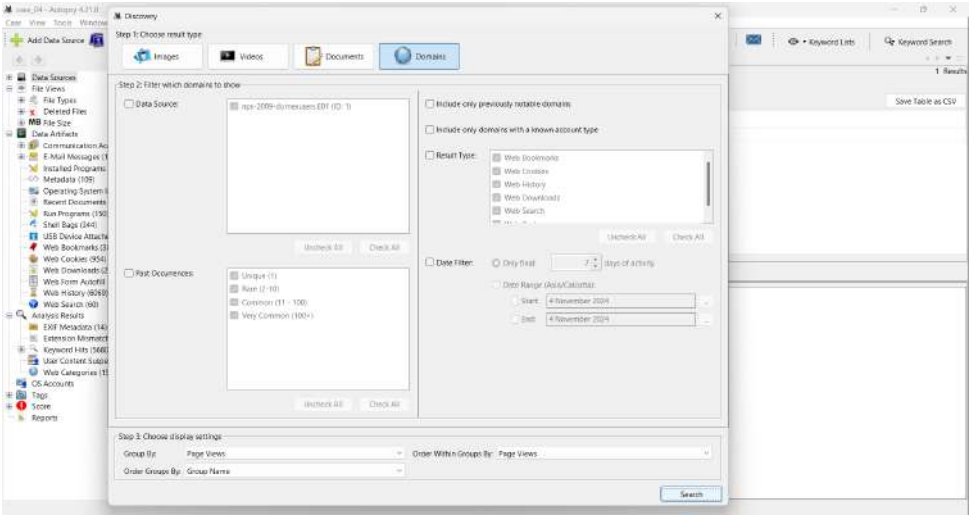
3 Steps to generate the Discovery of the Forensic Image

1. Click on the ”Discovery” at the top. The screen will be displayed as follows.

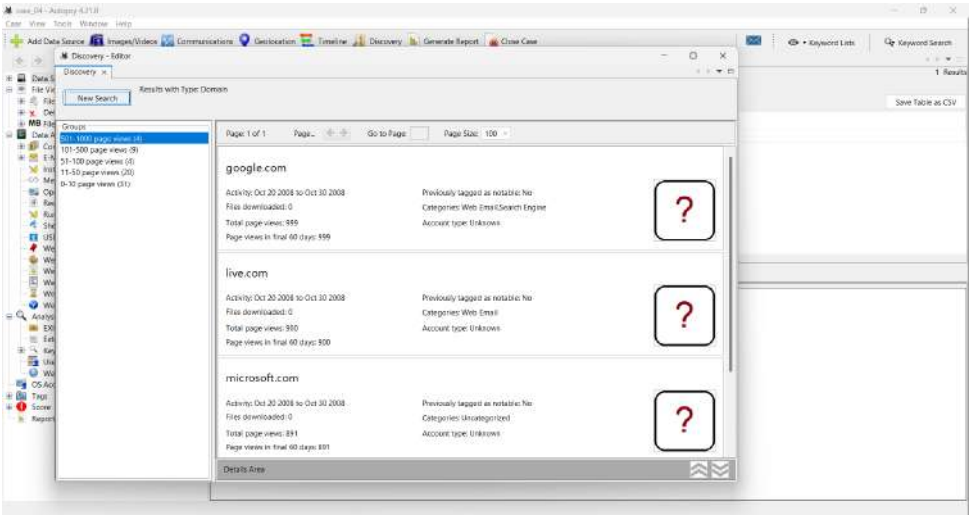


2. Next, filter which images, videos, documents or domains you want to show and then click on Search. It will show all these accordingly.

   Lets check for Domains, for example.



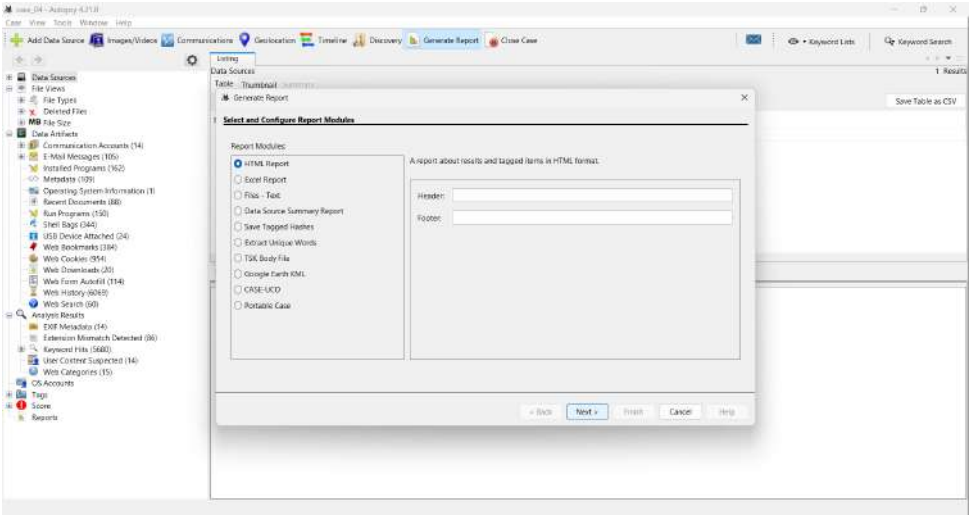
   You can filter out either manually or can keep the default filters as it is. Now, clicking on Search will generate the following results.



Similarly, we can do for others as well.

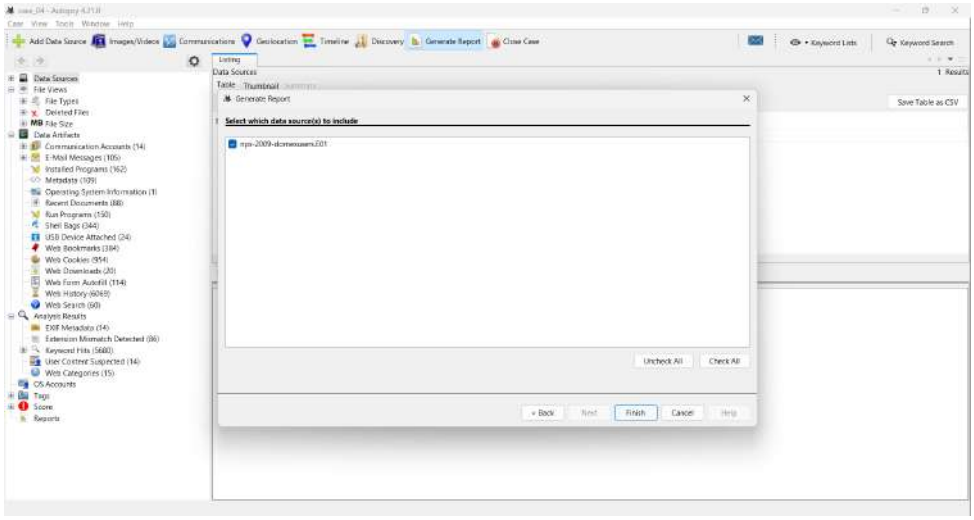
4 Steps to generate the report of the Forensic Image

1. Click on the ”Generate Report” at the top. The screen will be displayed as follows.

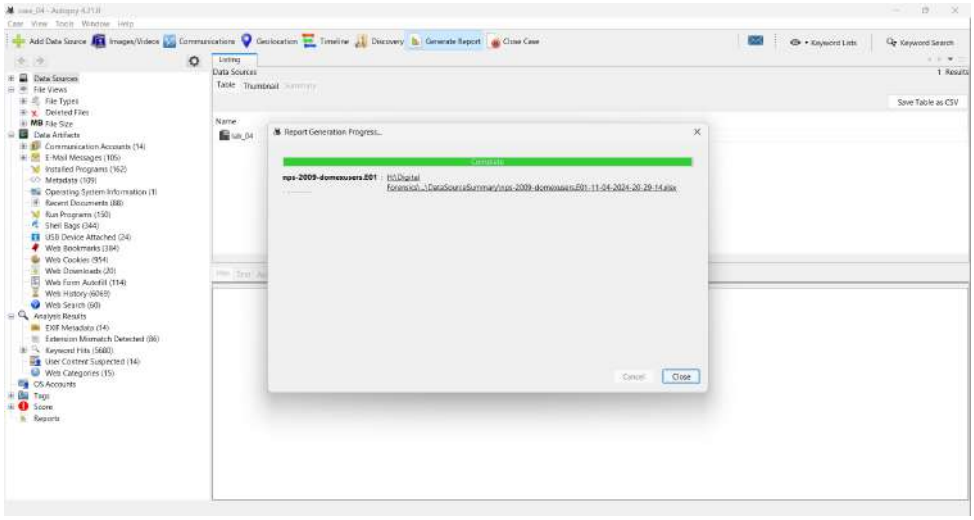


2. Select the ”Data Source Summary Report” and then click Next.

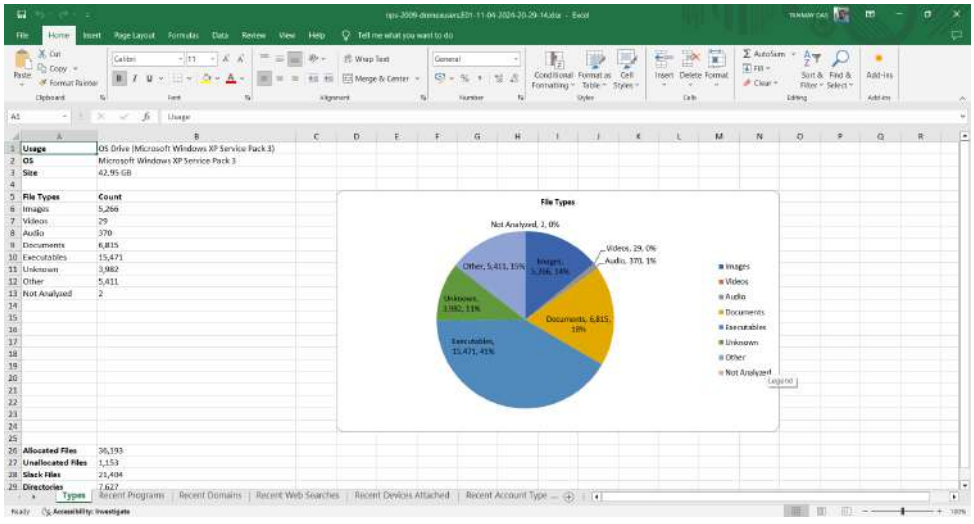
3. Select the data source you want to include and click on ”Finish”.



4. The Report is now generated. Click on Close.



5. The report is viewed as shown below.



LAB ASSIGNMENT - 10

1 AIM

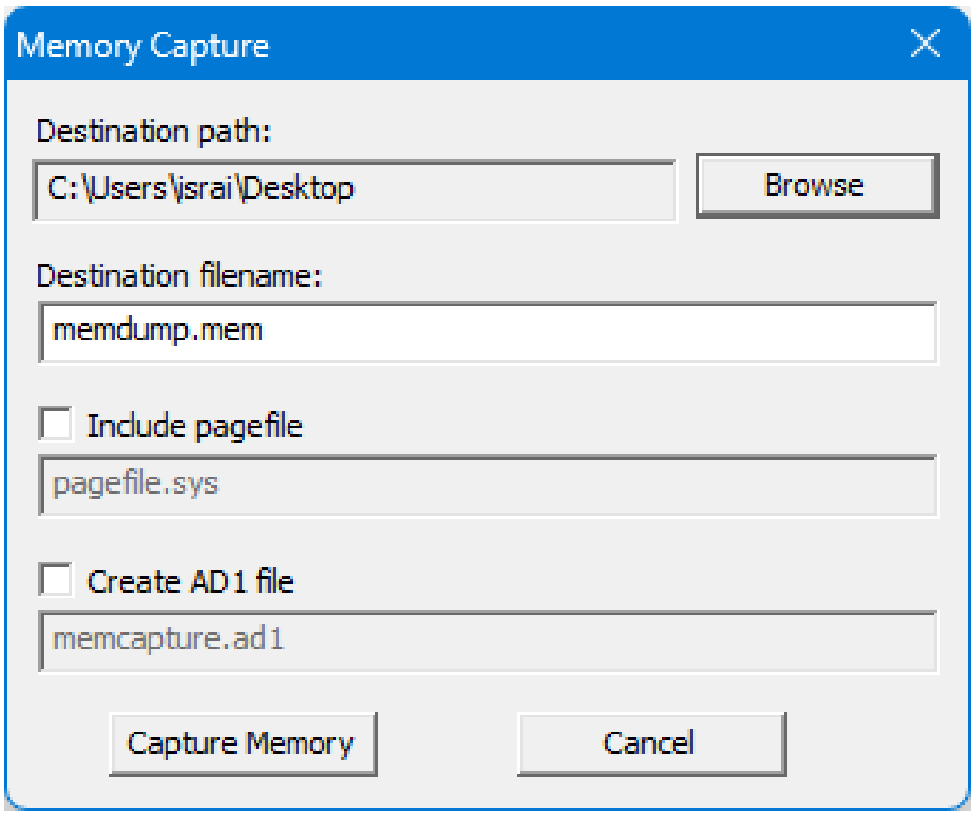
Perform Live Acquisition (RAM) for Order of Volatile (using FTK Imager).

2 Steps to perform Live Acquisition (RAM) for Order of Volatile (using FTK Imager).

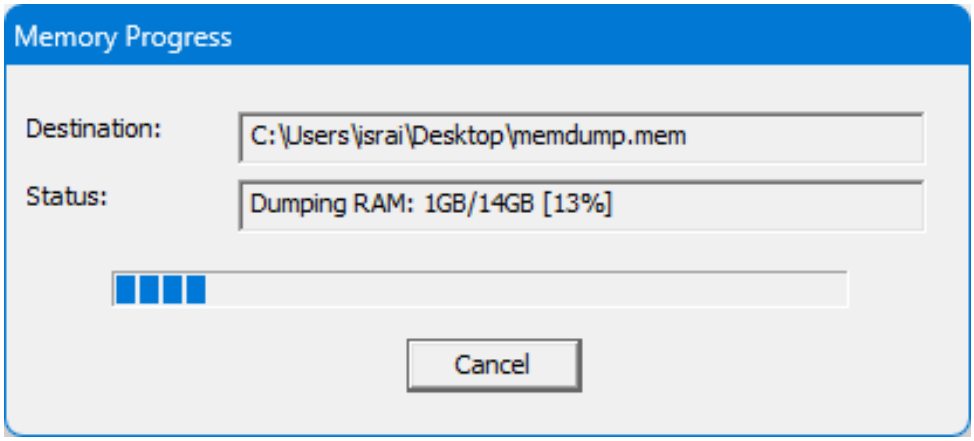
Steps to perform Live Acquisition (RAM) for Order of Volatile (using FTK Imager)are as follows :-

1. Open FTK imager and select capture RAM.

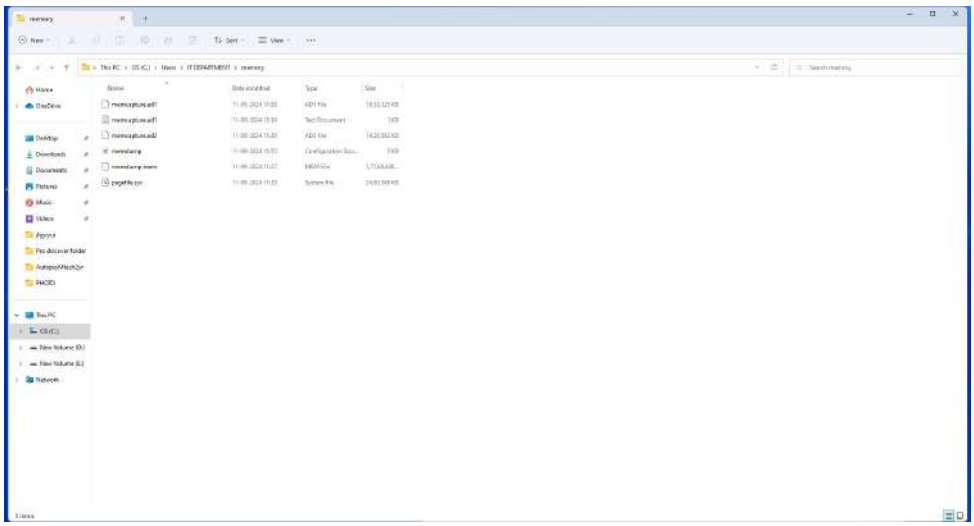
2. Select Destination where the files are to be stored



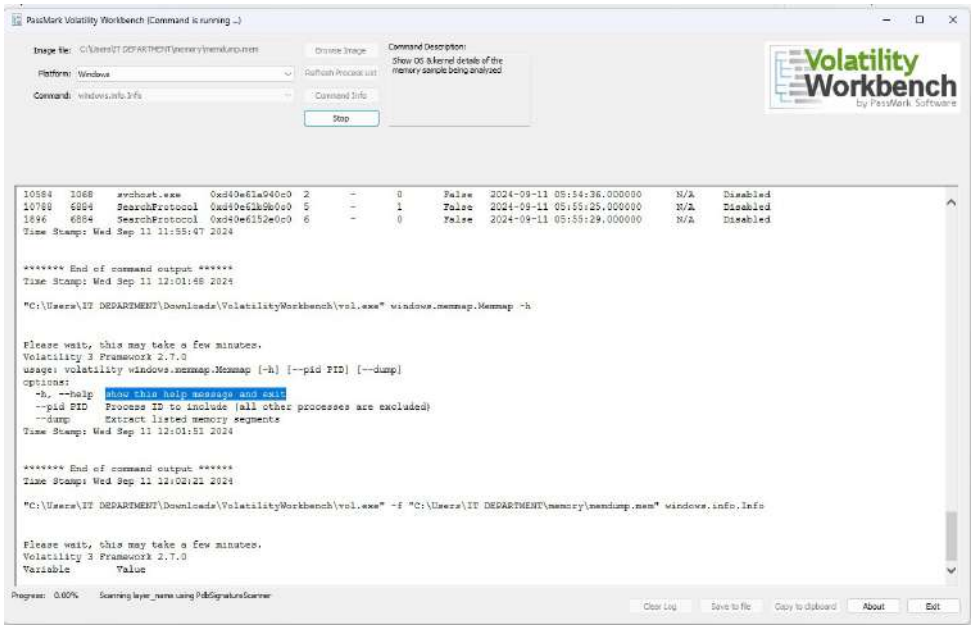
3. Capturing memory



4. Files in drive that are created by memory capture.



5. Add these files to Volatility Workbench and analyze.



3 Analyzing Volatile Memory:

1. Extracting Information with Volatility:
   - Open a terminal or command prompt.
   - Navigate to the directory where Volatility is installed.

2. Determine the Profile:
   - Use the imageinfo command to determine the profile of the memory dump.

3. Analyze Memory:
   - Use Volatility plugins to extract information.

- Examples of commands include :

    - pslist: Lists running processes.
    - pstree: Displays process listing as a tree.
    - netscan: Shows network connections.
    - cmdscan: Scans for command history.
    - filescan: Scans for file objects.
    - dumpfiles: Extracts specific file objects.
    - dillist: Lists loaded DLLs.
    - malfind: Looks for suspicious injected code.
    - hashdump: Dumps password hashes.
    - hivelist: Lists registry hives.

4. Interpret Results:
    - Analyze the output for evidence related to the investigation.
5. Document Findings:
    - Document all findings carefully for legal and investigative purposes.

LAB ASSIGNMENT - 11

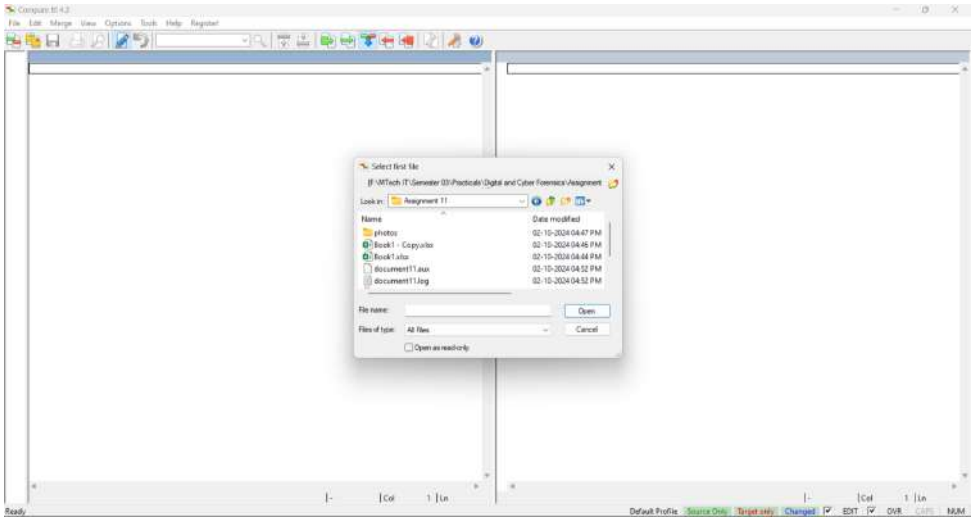
1 AIM

Compare two files for forensic investigation (Using Compare IT!) and identify changes in the hex structure of the files.

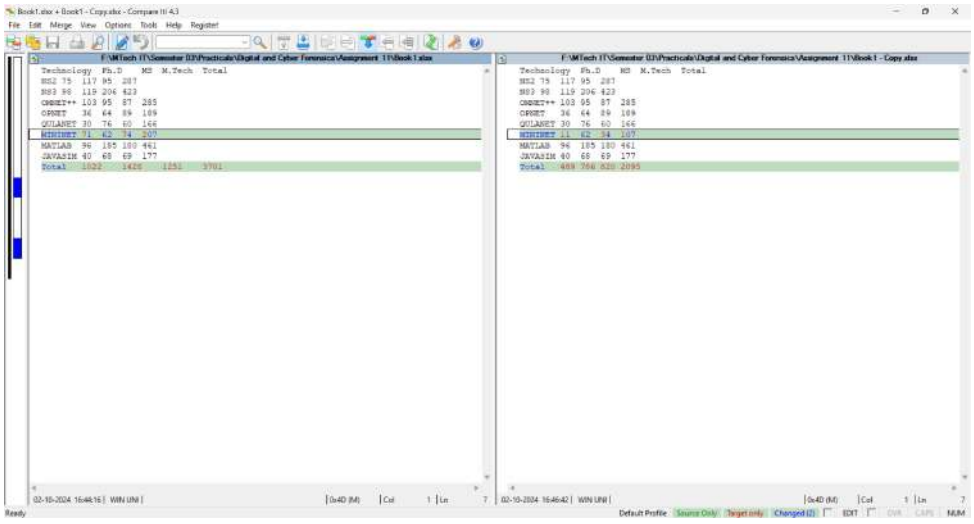
2 Steps to compare two files using Compare It!

Steps to to compare two files using Compare It! are as follows: -

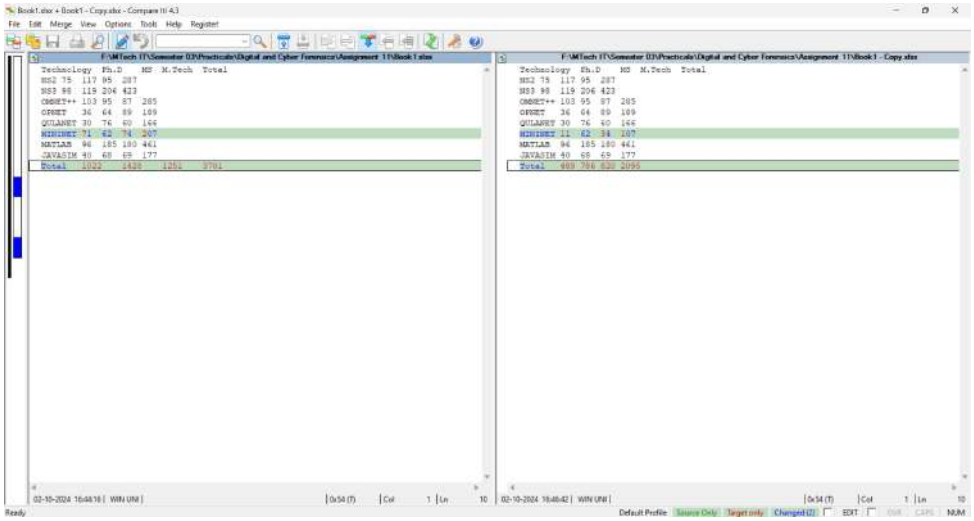
1. Click on Compare It Tool, It will show a window to select the files to be compared.
2. First select the first file and click on open and then select the second file and click on open.



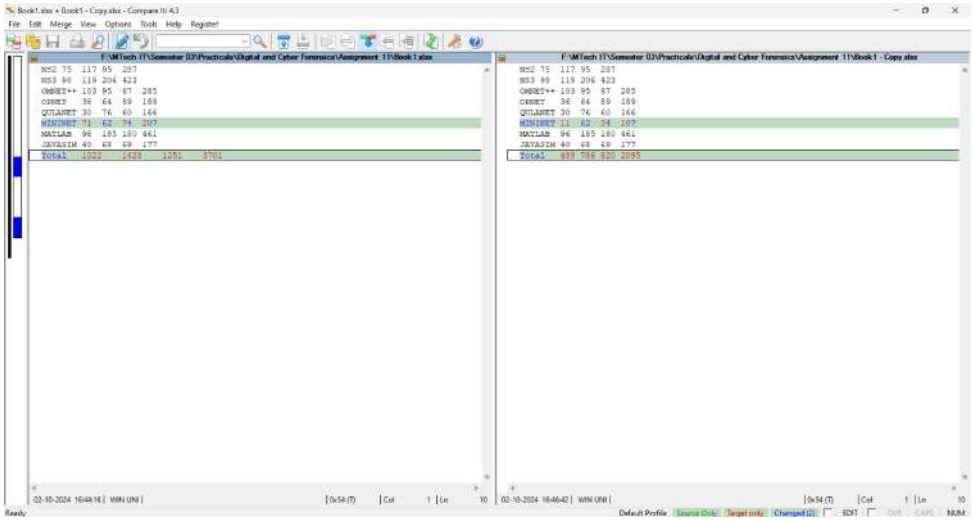
3. Now it will show us the changes in the highlighted bar.



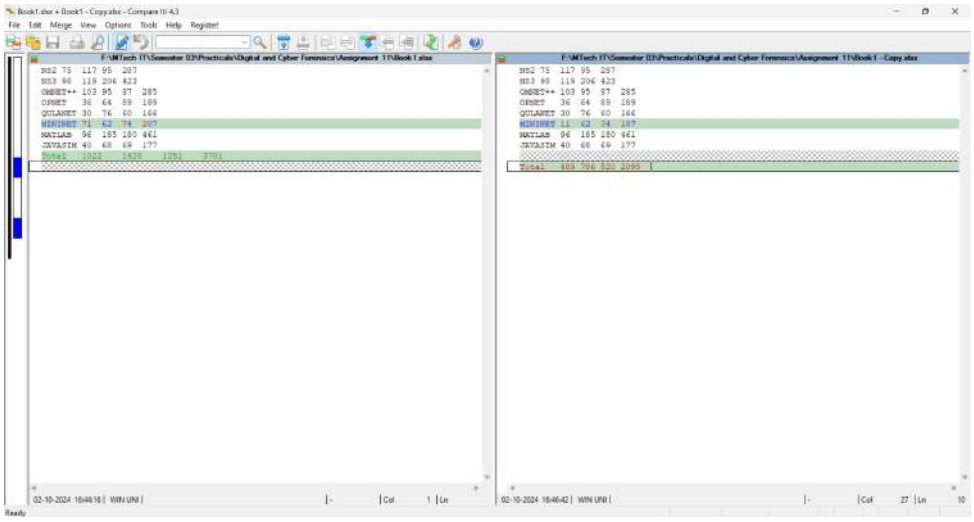
4. Now click on View and select Next Diff and it will show the next change.



5. Now click on view and select changes only. It will show all the changes simultaneously.



6. Now click on Merge and Select Separate Option.It will separate the changed lines.



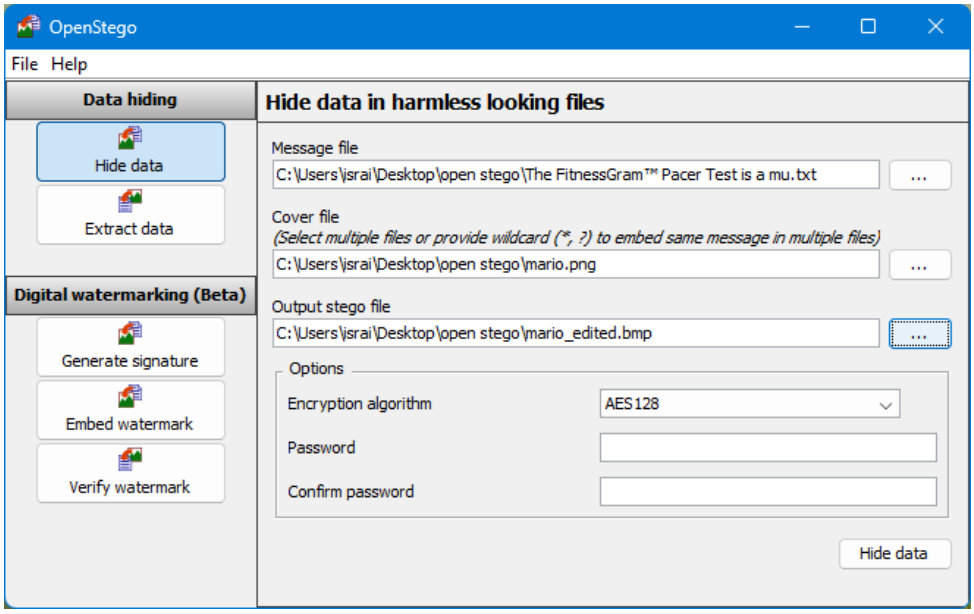
LAB ASSIGNMENT -12

1 AIM

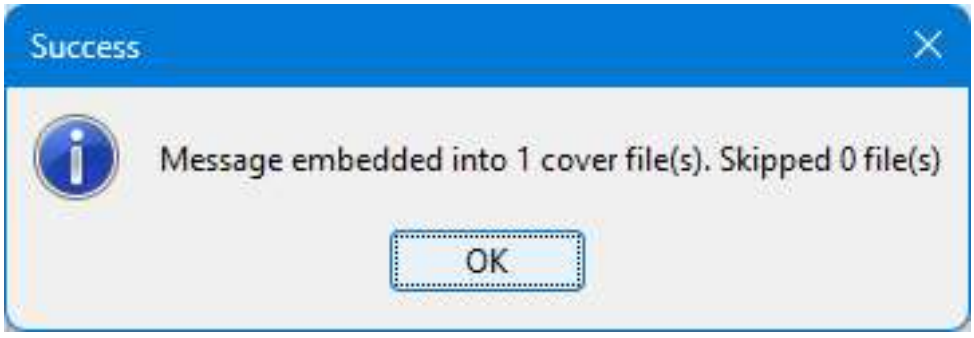
Use OpenStego software to perform data hiding, data extracting and digital watermarking. Also, the steps for hiding any file behind an image should be studied using Command Prompt (CMD). Use Compare IT! Software for further analysis.

2 Steps to perform to perform data hiding, data extracting and digital watermarking. Also, the steps for hiding any file

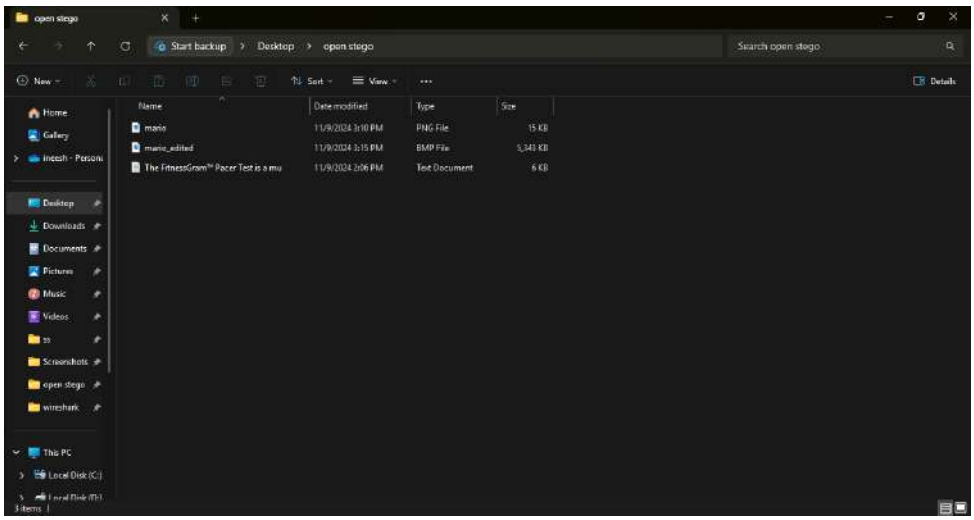
1. Crete a text file and choose an image and add the path to the output file.



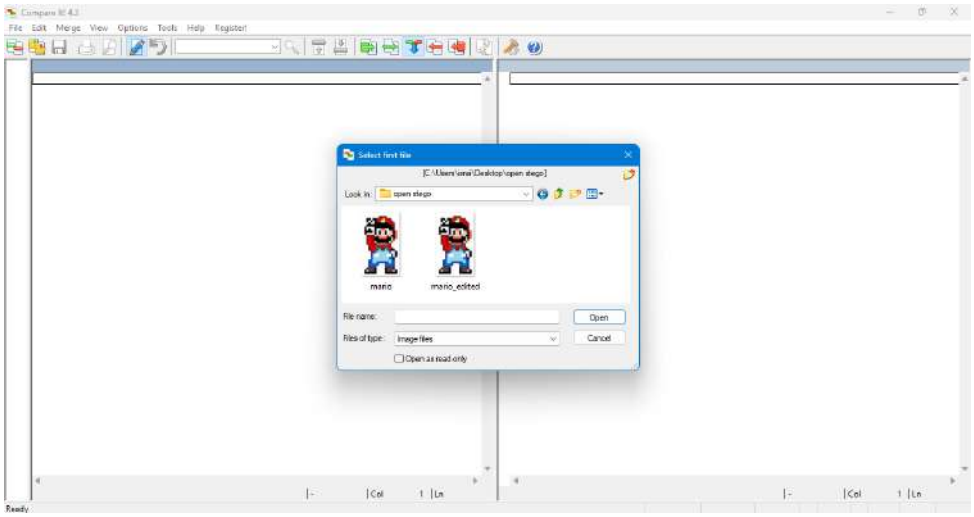
2. After that we get the following prompt.



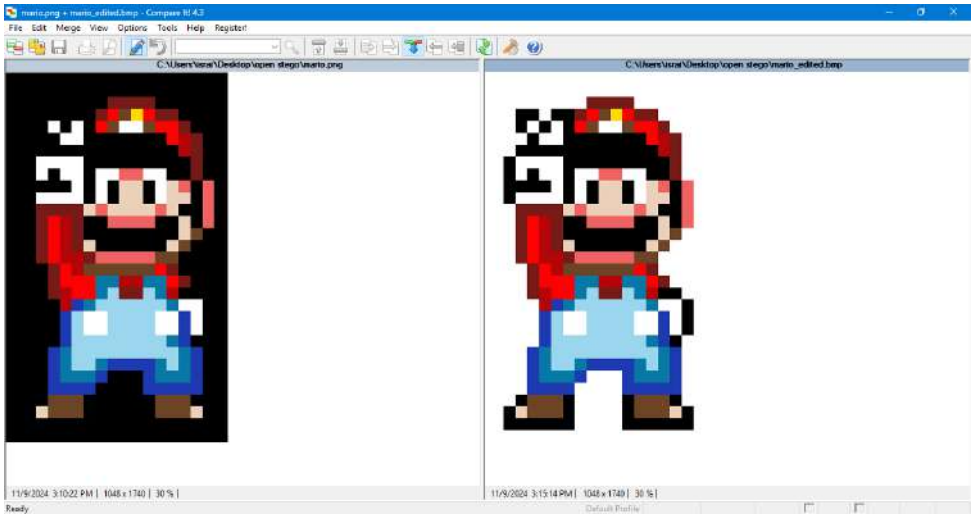
3. The output file name is - Mario-edited.



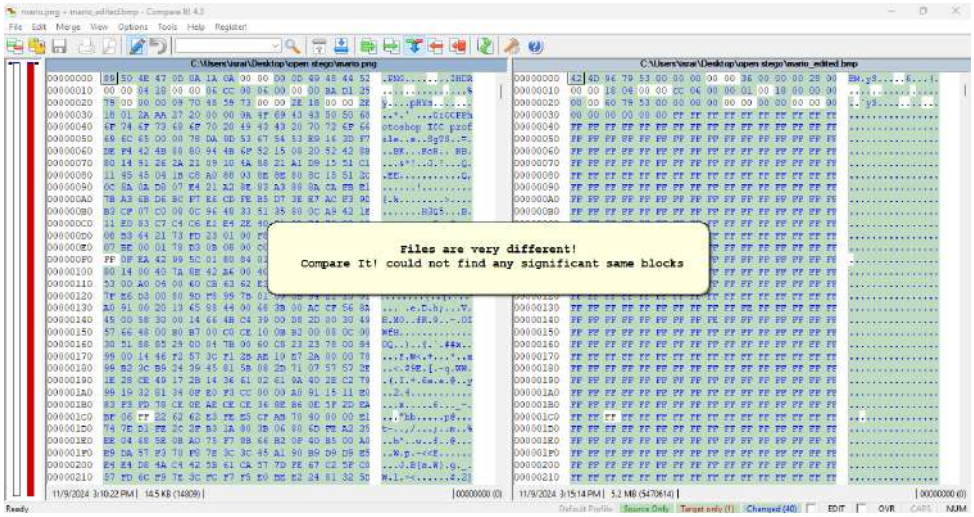
4. Now we use Compare It! choose the original and the edited files.



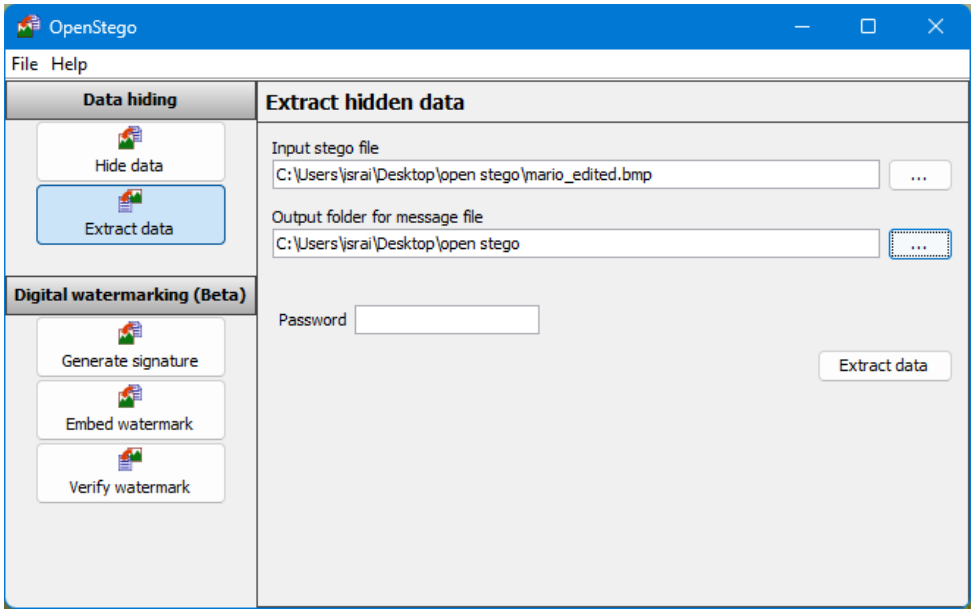
5. Left image - Original, Right - Edited.



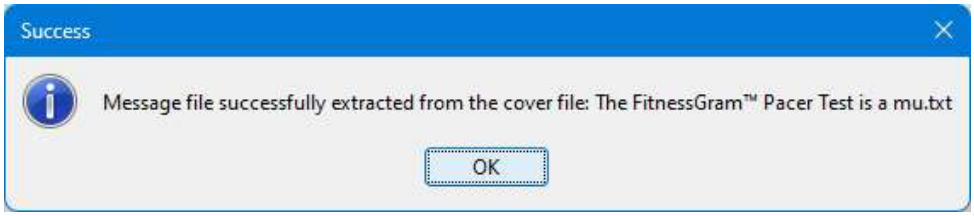
6. As we can see Compare It! successfully distinguishes between the files.



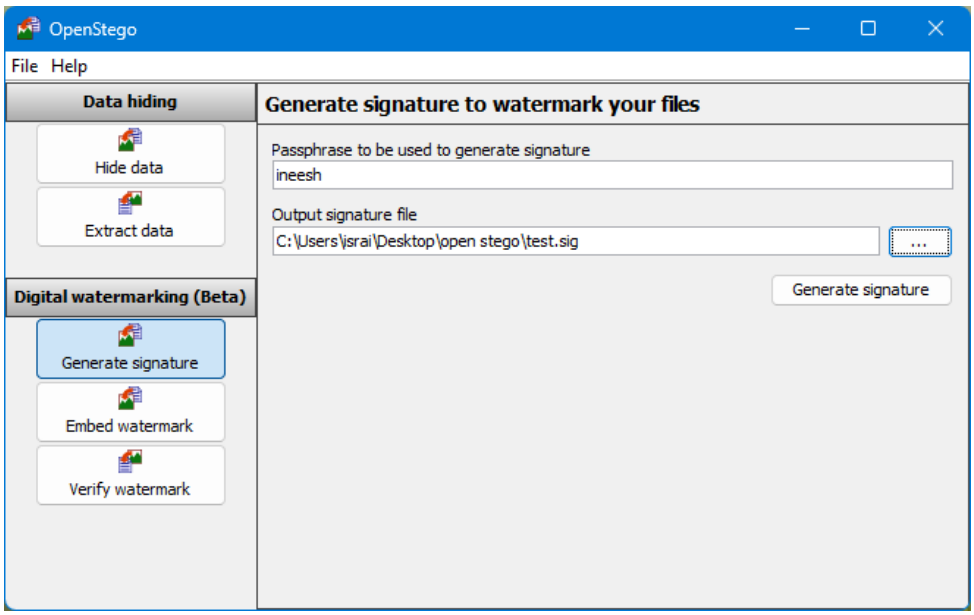
7. For extracting data form an stego image we have to provide - 1. the setego file 2. the output for the txt found in the image.



8. We get the prompt of the file generated/ recoverred form the image.

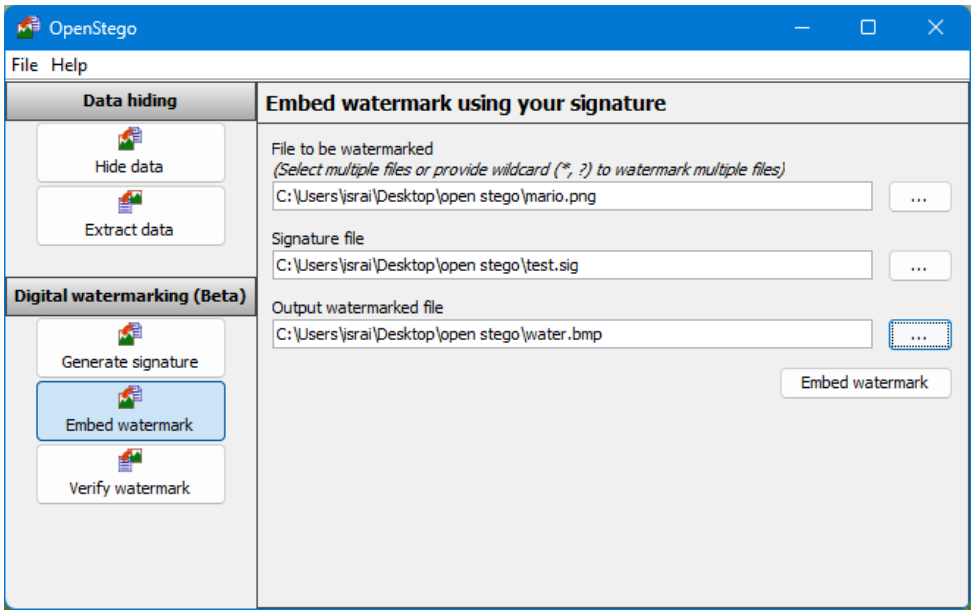


9. For Digital Watermarking we have to give a passphrase and the output path.

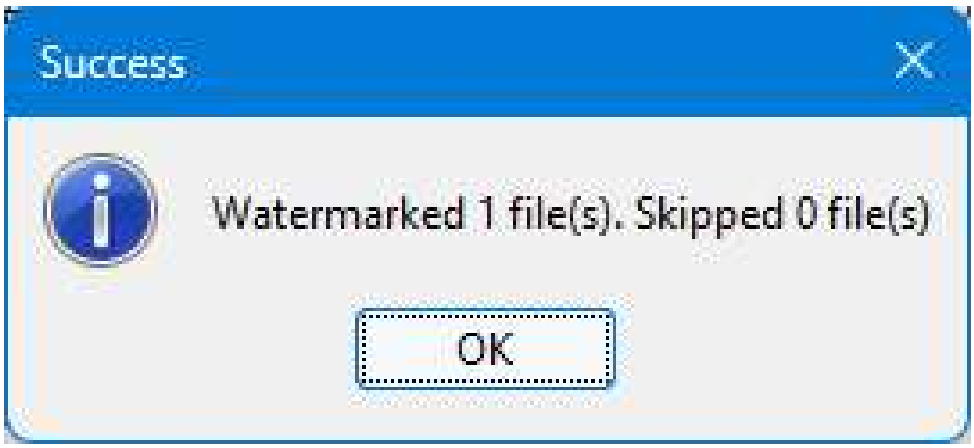


10. Prompt of signature successfully created.

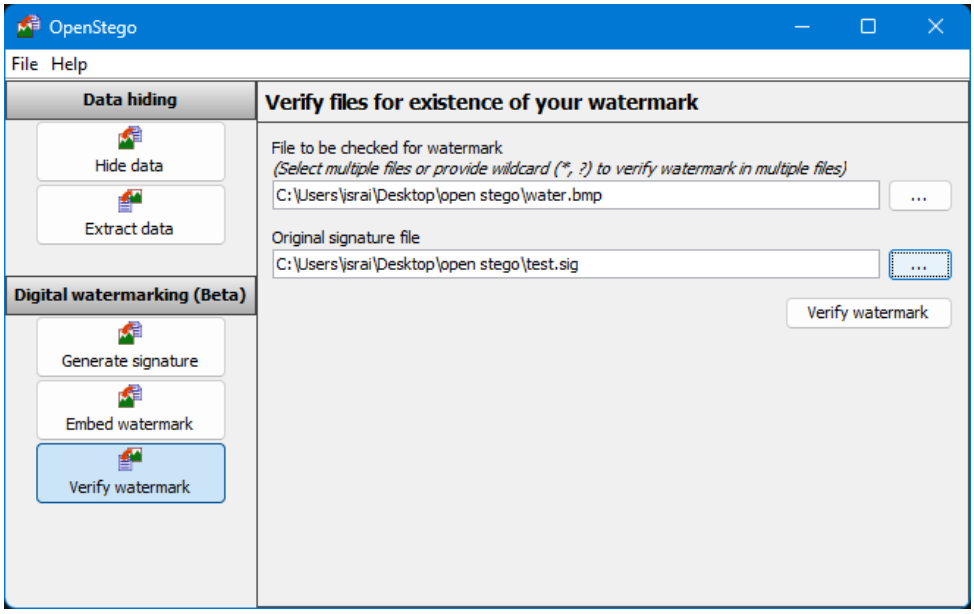
11. To embed watermark in an image we have to insert our generated signature to the image file which we want and give an output path.



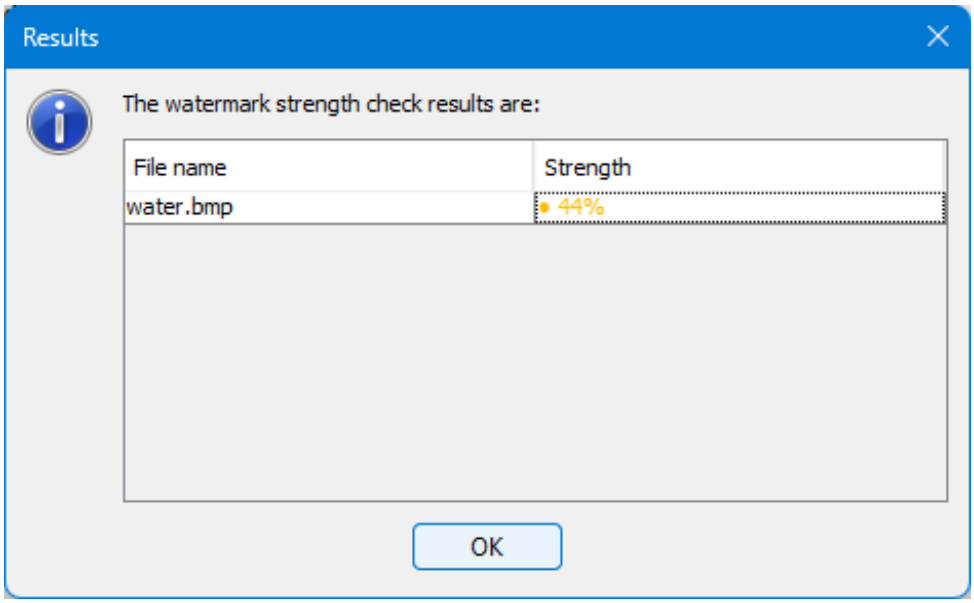
12. Prompt for successful generation of watermark image.



13. For verification we check using the watermarked image and the signature generated before.



14. Checks for the signature strength.



LAB ASSIGNMENT - 13

1 AIM

Study the John the Ripper tool for password cracking.

2 Theory

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

JtR supports several common encryption technologies out-of-the-box for UNIX and Windows-based systems. (ed. Mac is UNIX based). JtR autodetects the encryption on the hashed data and compares it against a large plain-text file that contains popular passwords, hashing each password, and then stopping it when it finds a match.

Simple.

In our Live Cyber Attack demo, the Varonis IR team demonstrates how to steal a hashed password, use JtR to find the true password, and use it to log into an administrative account. That is a very common use case for JtR!

JtR also includes its own wordlists of common passwords for 20+ languages. These wordlists provide JtR with thousands of possible passwords from which it can generate the corresponding hash values to make a high-value guess of the target password. Since most people choose easy-to-remember passwords, JtR is often very effective even with its out-of-the-box wordlists.

3 Practicals: Cracking Password with John the Ripper Tool

1. First, create a zip file and protect it with a password to simulate a cracking scenario.
    - Filename: `ss.zip`
2. On a Linux machine, use John the Ripper to crack the password for accessing the file. Commands used in this process include:
    (a) Creation of a file and adding text: “this is a test to check for encryption”

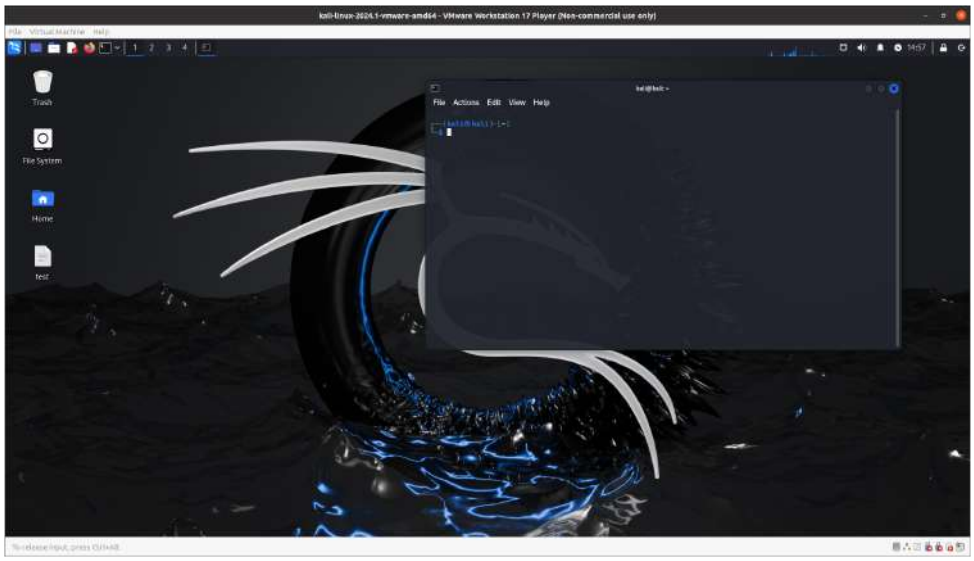
(b) `gpg --symmetric --cipher-algo AES256 /home/kali/Desktop/test`

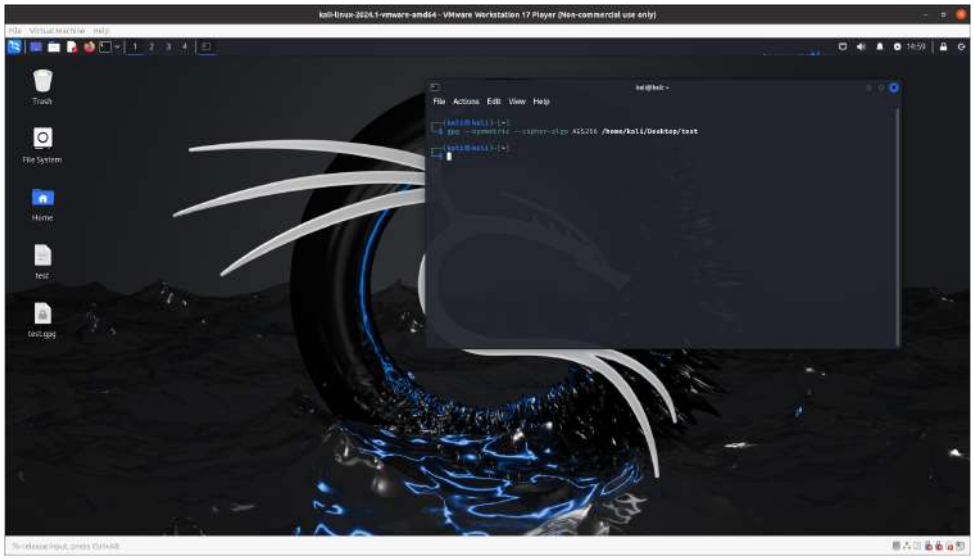
(c) `gpg2john /home/kali/Desktop/test.gpg > hash.txt`

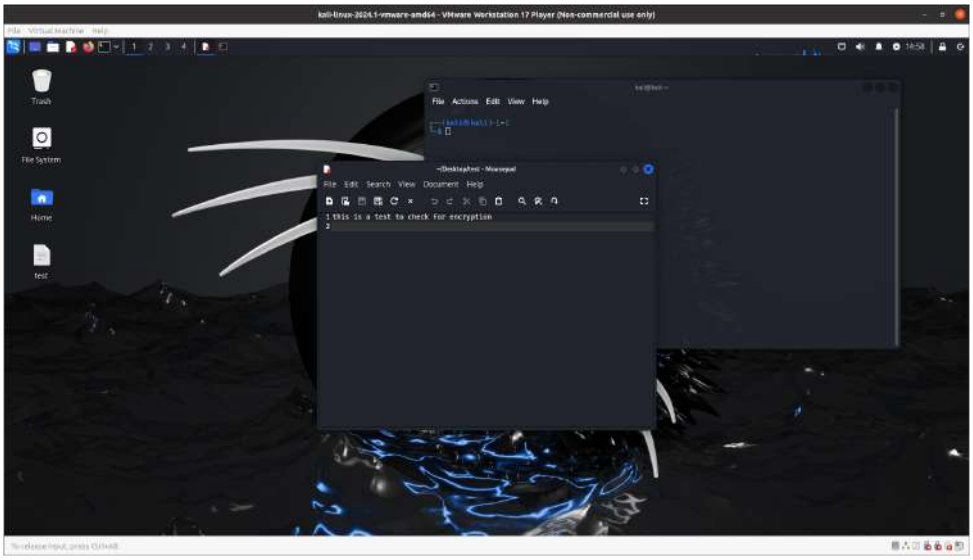
(d) `john hash.txt`

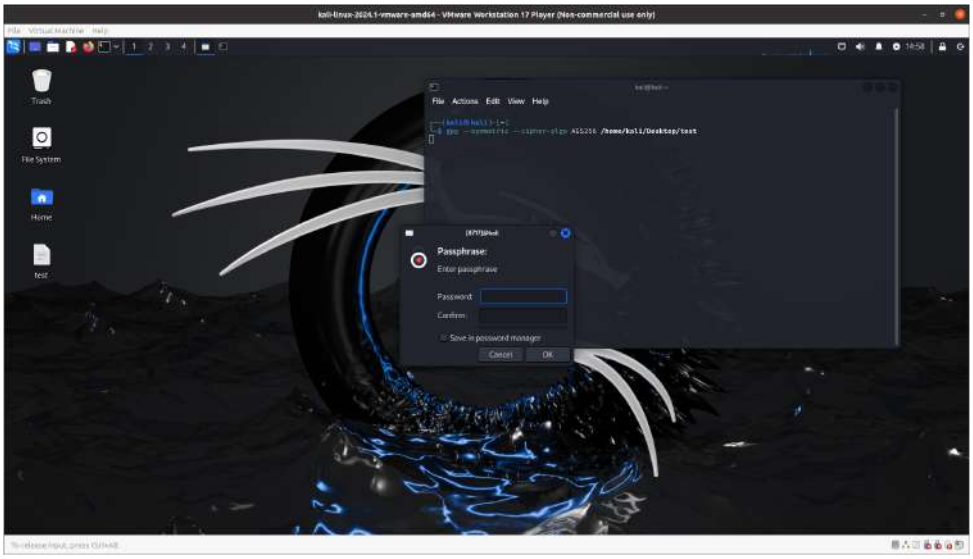
(e) `gpg --decrypt /home/kali/Desktop/test.gpg`

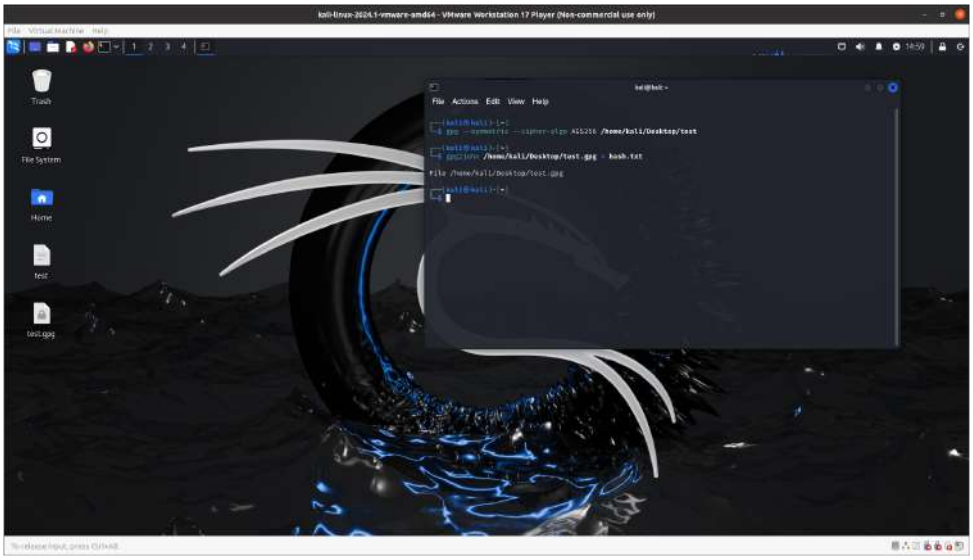
3. Images to illustrate each step:



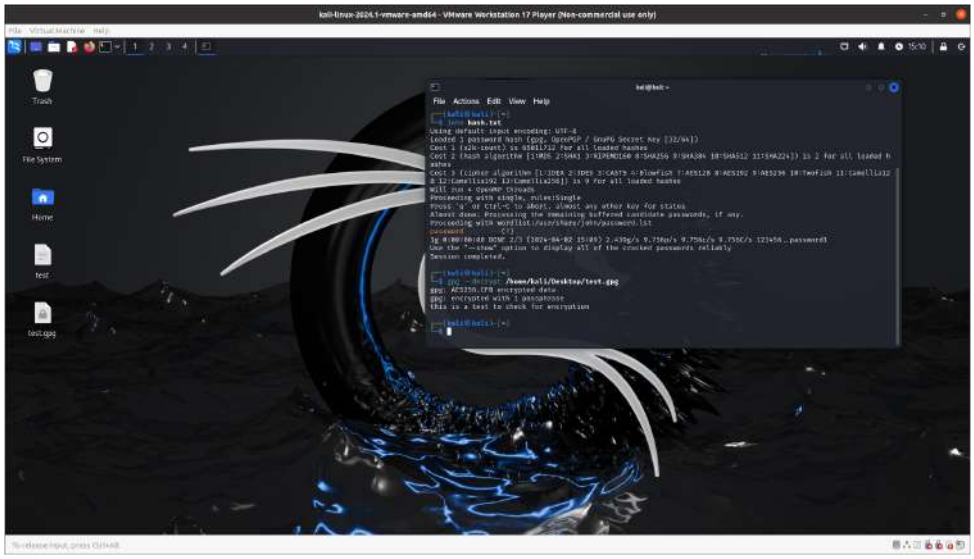



kali-linux-2024.1-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Trash
File System
Home
test
File Edit Search View Document Help
1 this is a test to check for encryption


kali-linux-2024.1-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Trash
File System
Home
test
Passphrase:
Enter passphrase
Password:
Confirm:
Save in password manager
Cancel
OK


kali-linux-2024.1-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Trash
File System
Home
test
test.gpg


kali-linux-2024.1-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
File Virtual Machine Help
Trash
File System
Home
test
test.gpg
kali@kali: ~
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ gpg -c /home/kali/Desktop/test.gpg > hash.txt
File /home/kali/Desktop/test.gpg
┌──(kali㉿kali)-[~]
└─$ john hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (gpg, OpenPGP / GnuPG Secret Key [32/64])
Cost 1 (iter-count) is 65011712 for all loaded hashes
Cost 2 (hash algorithm [1:MD5 2:SHA1 3:RIPEMD160 8:SHA256 9:SHA384 10:SHA512 11:SHA224]) is 2 for all loaded hashes
Cost 3 (cipher algorithm [1:IDEA 2:3DES 3:CAST5 4:Blowfish 7:AES128 8:AES192 9:AES256 10:Twofish 11:Camellia128 12:Camellia192 13:Camellia256]) is 9 for all loaded hashes
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
password   (?)
1g 0:00:00:00 DONE 2/3 (2024-04-02 15:09) 2.439g/s 9.756p/s 9.756c/s 123456..password1
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
┌──(kali㉿kali)-[~]
└─$


kali-linux-2024.1-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
File Virtual Machine Help
Trash
File System
Home
test
test.gpg
kali@kali: ~
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ john hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (gpg, OpenPGP / GnuPG Secret Key [32/64])
Cost 1 (iter-count) is 65011712 for all loaded hashes
Cost 2 (hash algorithm [1:MD5 2:SHA1 3:RIPEMD160 8:SHA256 9:SHA384 10:SHA512 11:SHA224]) is 2 for all loaded hashes
Cost 3 (cipher algorithm [1:IDEA 2:3DES 3:CAST5 4:Blowfish 7:AES128 8:AES192 9:AES256 10:Twofish 11:Camellia128 12:Camellia192 13:Camellia256]) is 9 for all loaded hashes
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
password   (?)
1g 0:00:00:00 DONE 2/3 (2024-04-02 15:09) 2.439g/s 9.756p/s 9.756c/s 123456..password1
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
┌──(kali㉿kali)-[~]
└─$ gpg -c /home/kali/Desktop/test.gpg
gpg: AES256.CFB encrypted data
gpg: encrypted with 1 passphrase
this is a test to check for encryption
┌──(kali㉿kali)-[~]
└─$

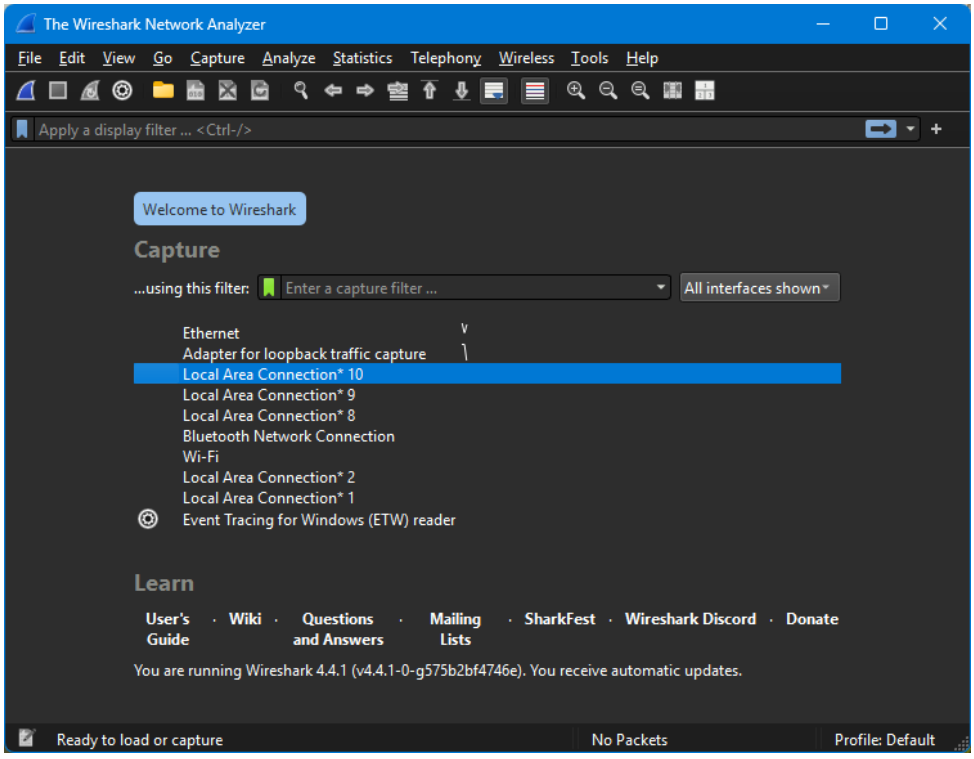
LAB ASSIGNMENT -14

1 AIM

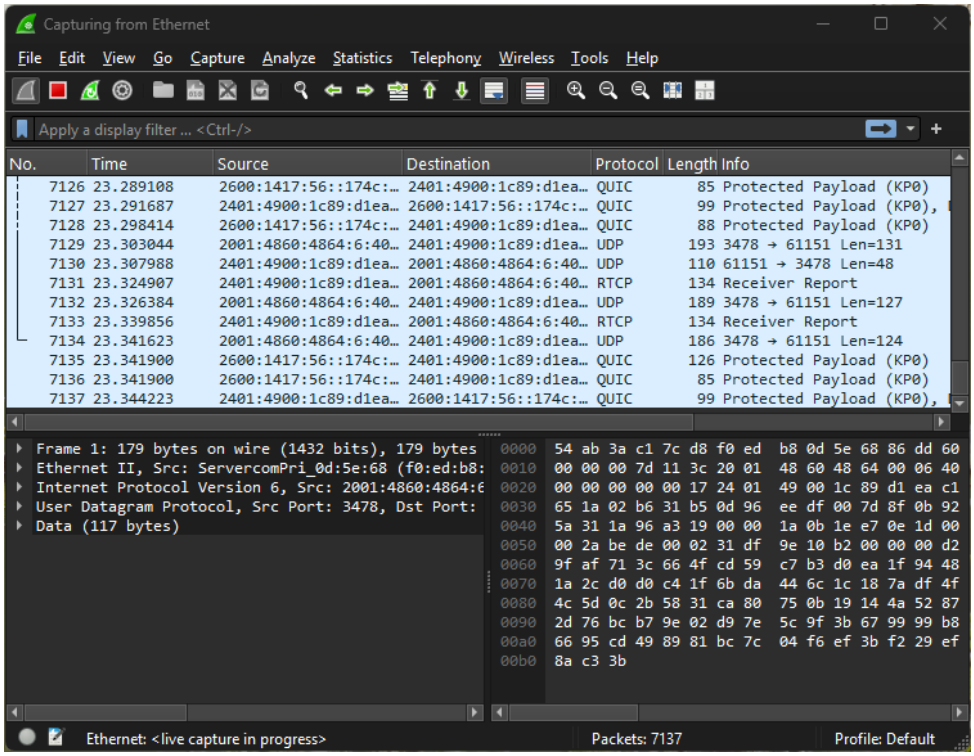
Study the WIRESHARK tool for Network forensics. Analyze the live capturing packets. Also, perform a packet analysis on given pcap files.

2 Steps to perform logical file examination of a given android mobile forensic image

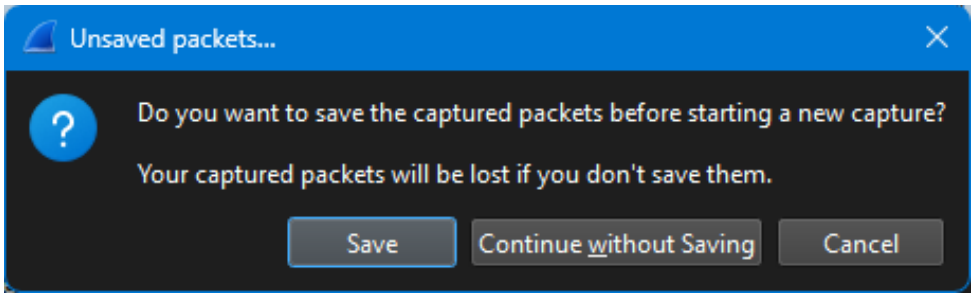
1. Select which network to capture the packets from.



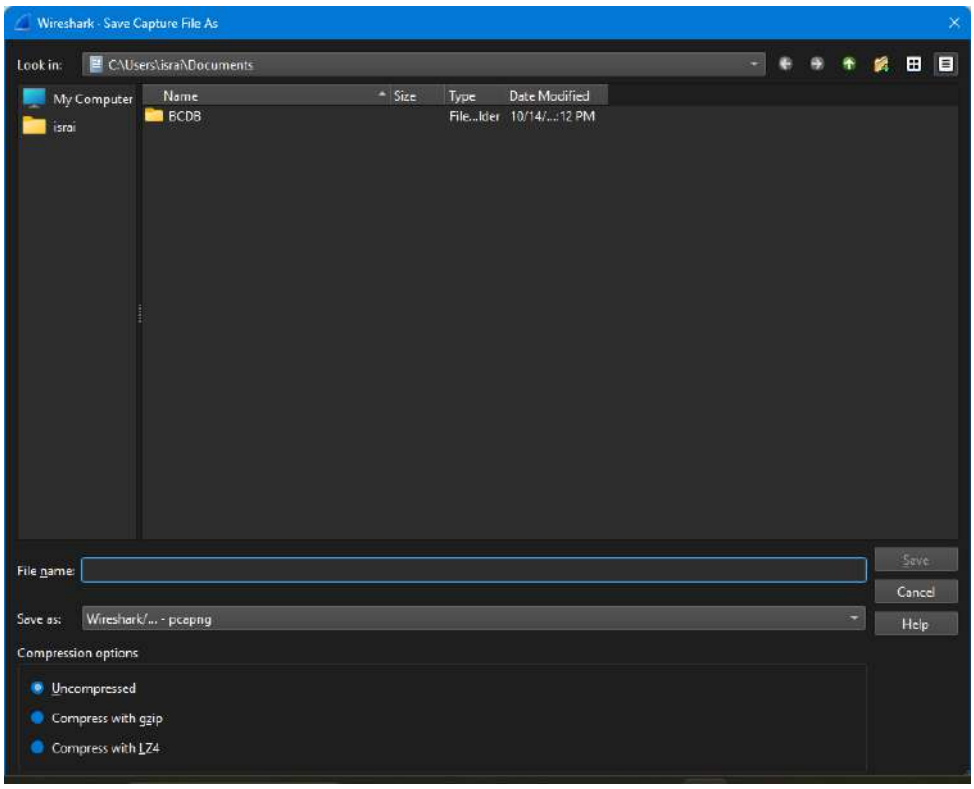
2. Capture the following packets for analysis.



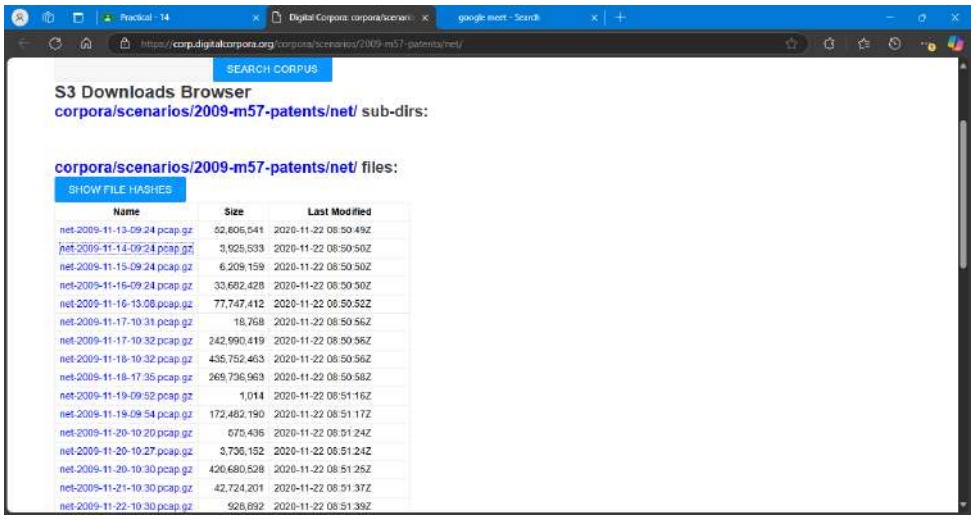
3. Save the captured packets.



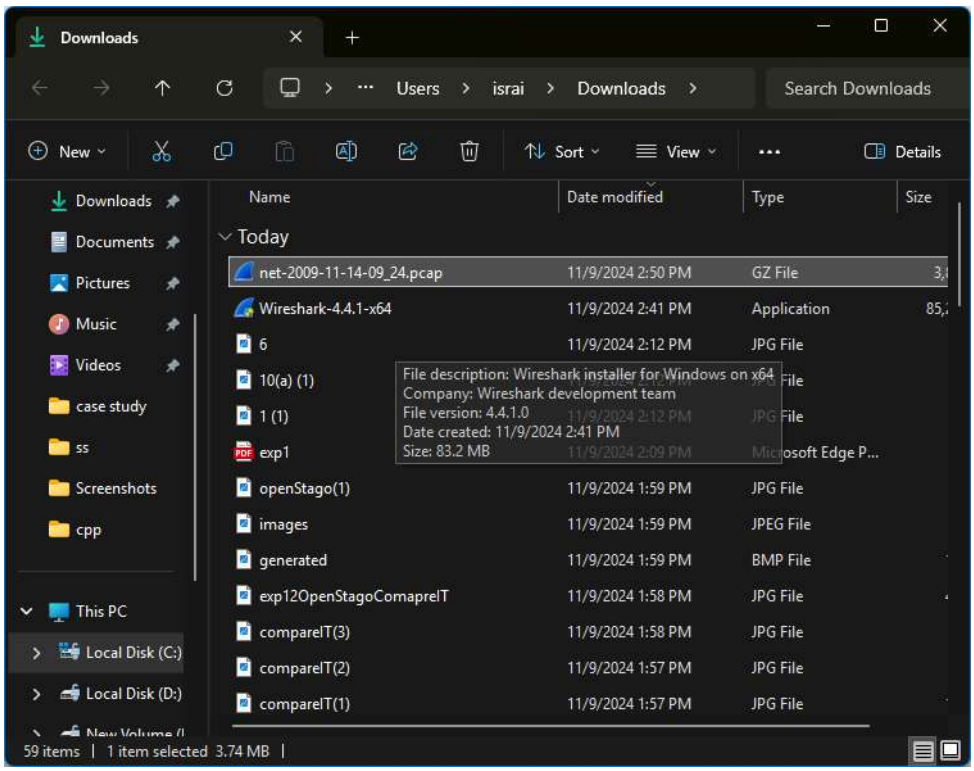
4. Save at a location.This completes the real time packet analysis.



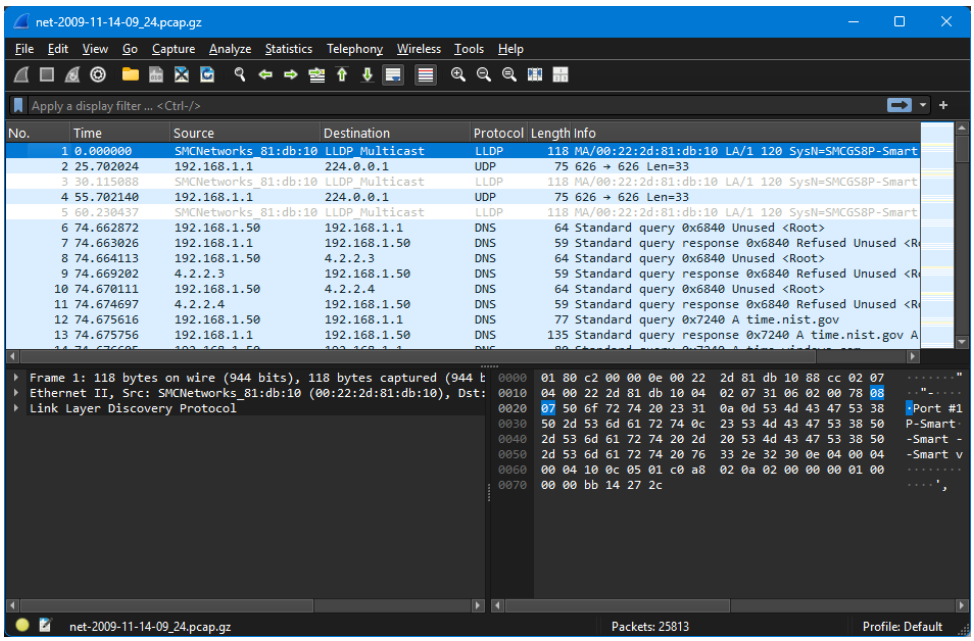
5. For analysis of Pcap files first download the necessary file.



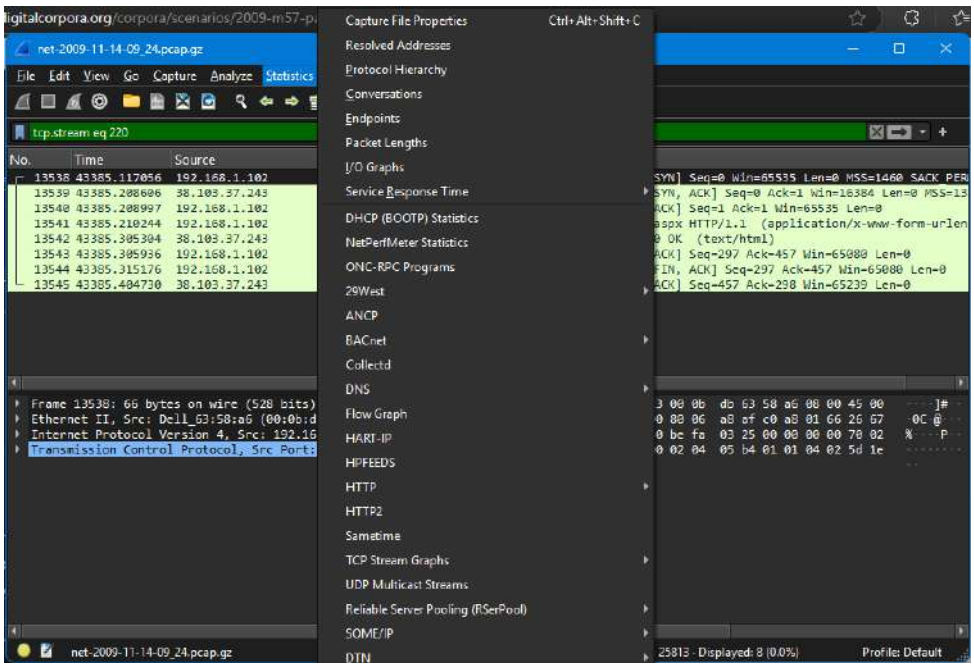
6. After downloading open the Pcap file with Wireshark



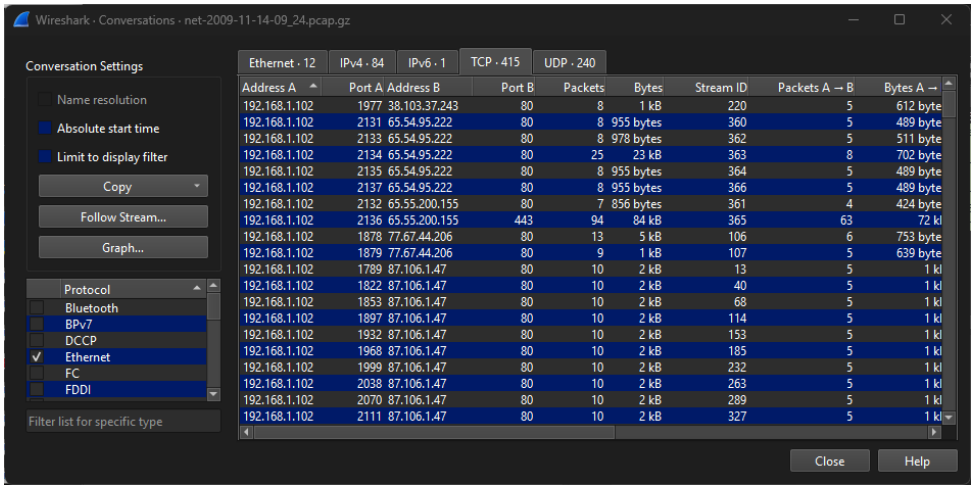
7. After opening the Pcap file, check all the packets.



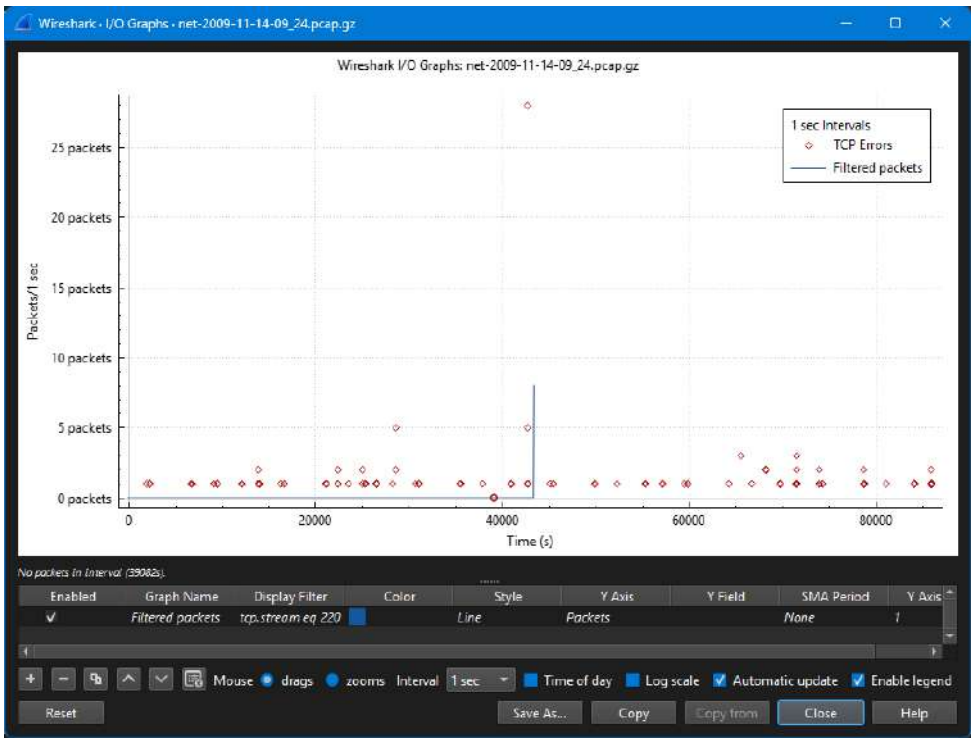
8. Select the Statistics tab for analysis.



9. Conversion between different ports.



10. Graph about the I/O Graph.


Wireshark · I/O Graphs · net-2009-11-14-09_24.pcap.gz
Wireshark I/O Graphs: net-2009-11-14-09_24.pcap.gz
1 sec Intervals
TCP Errors
Filtered packets
25 packets
20 packets
15 packets
10 packets
5 packets
0 packets
Packets/1 sec
0
20000
40000
60000
80000
Time (s)
No packets in Interval (39082s).
Enabled
Graph Name
Display Filter
Color
Style
Y Axis
Y Field
SMA Period
Y Axis
Filtered packets
tcp.stream eq 220
Line
Packets
None
1
Mouse
drags
zooms
Interval
1 sec
Time of day
Log scale
Automatic update
Enable legend
Reset
Save As...
Copy
Copy from
Close
Help

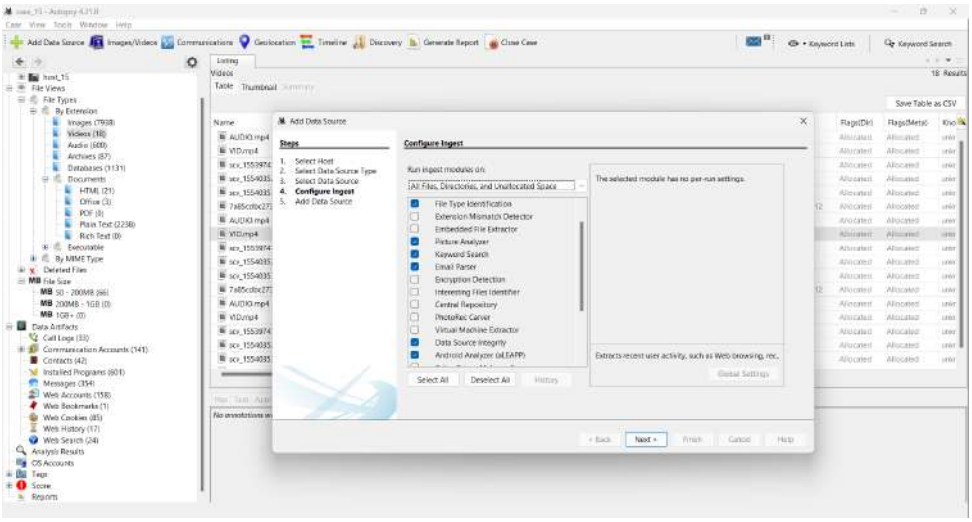
LAB ASSIGNMENT - 15

1 AIM

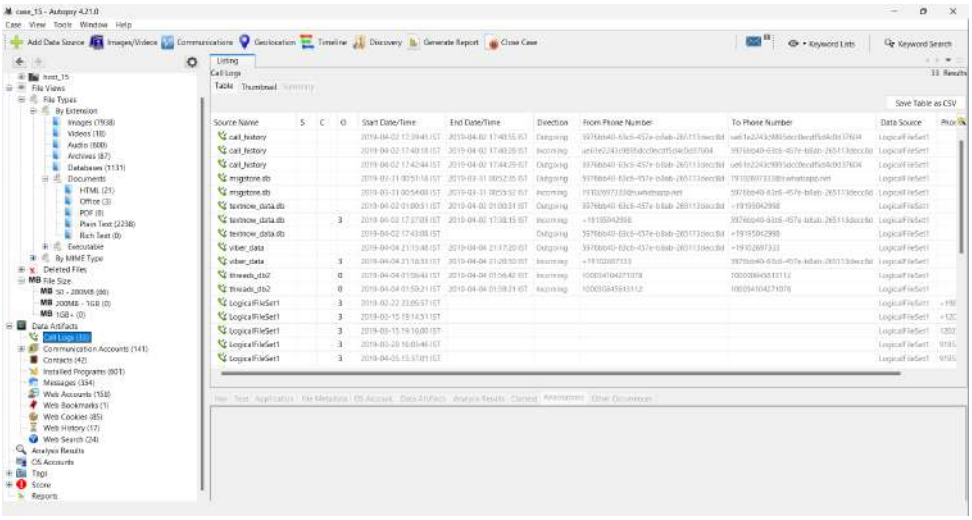
Perform a logical file examination of a given Android mobile forensic image using Autopsy (aleapp + relevant parsers).

2 Steps to perform the logical file examination of a given Android mobile forensic image

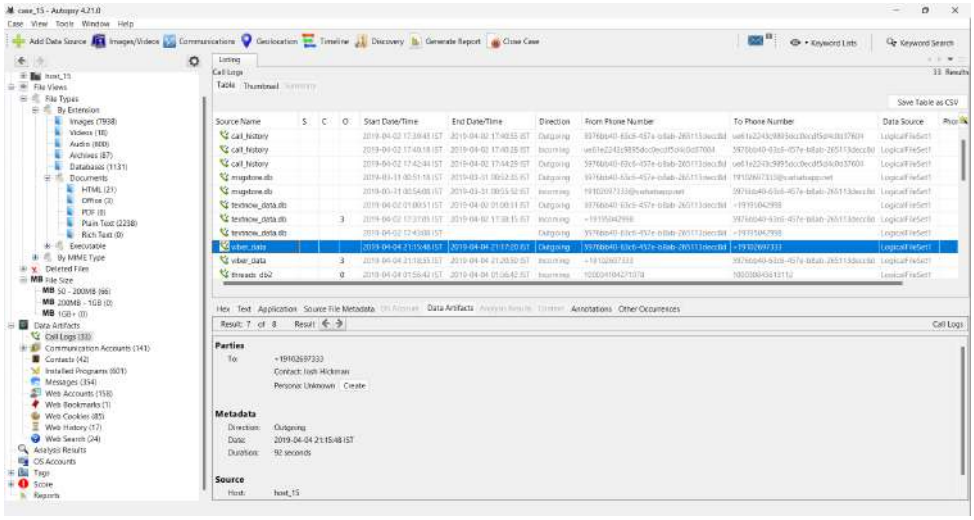
1. While creating a forensic image of a given android mobile,select the required ingest modules as provided in the screenshot.



2. If you want to see the list of call logs,click on call logs. It will display all the call logs as provided in the screenshot.



3. If you want to see a particular call log,click on any of the call log. You will be able to see the information related to that call log.



LAB ASSIGNMENT - 16

1 AIM

Study the SANS workstation environment and perform digital acquisition on a digital drive.

2 Steps to perform the digital acquisition of the Digital Drive using SANS workstation

1. Mount the Drive in a Read-Only Mode:

   Open a terminal in your SIFT workstation.

   List all connected storage devices using: sudo fdisk -l

   Identify the target drive (e.g., /dev/sdb).

2. Create a Forensic Image of the Drive:

   - Use dcfldd to create a forensic image:

     sudo dcfldd if=/dev/sdb of=/path/to/output/image.dd hash=md5,sha256

     hashlog=/path/to/output/image.hash.log

   - Explanation of flags:

     if=/dev/sdb: Specifies the input drive.

     of=/path/to/output/image.dd: Specifies the output image file.

     hash=md5,sha256: Computes MD5 and SHA-256 hashes.

     hashlog=/path/to/output/image.hash.log: Saves hashes in a log file.

3. Verify the Integrity of the Image

   - Compare hashes of the original drive and forensic image to confirm integrity.

   - Use md5sum and sha256sum commands:

     md5sum /path/to/output/image.dd

     sha256sum /path/to/output/image.dd

   - Compare these hashes to those in image.hash.log.

4. Document the Process

    - Document each step, noting drive details, acquisition time, and hash values.

    - This is essential for the chain of custody and validation of evidence integrity.

5. Analyze the Forensic Image

    - Proceed with forensic analysis on the SIFT workstation using tools like Autopsy, The Sleuth Kit, or bulk_extractor.