DIGITAL FORENSIC

Practical File

Course Code : INITE22

Submitted By –

Name: Rohit Kumar

Roll no.: 2020UIN3322

Branch: ITNS

Semester: 6th

Academic Year: 2022-23

INDEX

SNO.	NAME	DATE	SIGNATURE
1	Study of Computer Forensics and different tools used for forensic investigation at least 7.		
2	Perform to make the forensic image of the storage drive (Using ProDiscover, AccessData FTK Imager, and Autopsy).		
3	To Recover a Deleted File using Forensic Tools (FTK Imager/Autopsy).		
4	To Recover a Deleted File using Forensic Tools (ProDiscover).		
5	To Collect the Email Evidence from a Suspected Drive or Image.		
6	How to Extract Browser Artifacts (Using Autopsy).		
7	Find Last Connected USB on your system - USB Forensics (Using Autopsy).		
8	Perform a full Live Forensics Case Investigation (Using Autopsy).		
9	Extract Exchangeable image file format (EXIF) Data from Image Files (Using Autopsy).		
10	Perform Live Forensics in the Volatile Memory (Using FTK Imager).		
11	Study the WIRESHARK tool for Network forensics.		
12	Comparison of two Files for forensics investigation (Using Compare IT!).		
13	To study the steps for hiding and to extract any file behind an image file/ Audio file using Command Prompt (CMD).		
14	Study the John the ripper framework for Examining the encrypted file.		

Practical - 1

Study of Computer Forensics and different tools used for forensic investigation

1. WIRESHARK

Wireshark is a powerful network protocol analyzer and forensic tool that is used to capture and analyze network traffic in real-time. It is commonly used by network administrators, security professionals, and forensic analysts to troubleshoot network problems, detect network intrusions, and investigate network-based crimes.Wireshark can be used in a real-time environment to open saved trace files from packet captures. An important feature is its capability to rebuild sessions.

Some of the key features of WIRESHARK include:

1.)Live capture and offline analysis: Wireshark can capture and analyze network traffic in real-time as well as analyze previously captured traffic stored in PCAP files.

2.)Deep inspection of hundreds of protocols: Wireshark can decode and analyze a wide range of protocols including TCP/IP, HTTP, FTP, DNS, and many others.

3.)Powerful display filters: Wireshark provides a wide range of filters that enable analysts to focus on specific packets of interest, including filters based on IP address, protocol type, and many other criteria.

4.)Customizable packet output: Wireshark enables users to customize how packets are displayed and presented to make it easier to identify and analyze the relevant information.

5.)VoIP analysis: Wireshark has built-in support for analyzing VoIP (Voice over IP) traffic, including the ability to decode SIP, RTP, and other VoIP protocols

2. ProDiscover Forensic

ProDiscover Forensic is a commercial digital forensic software tool developed by Technology Pathways. It is used by law enforcement, government agencies, and corporate organizations to acquire, analyze, and report on digital evidence. ProDiscover Forensic is known for its ability to extract and analyze data from a wide range of devices and file systems, including hard drives, mobile devices, cloud services, and other forms of digital storage media.

Some of the key features of ProDiscover Forensic include:

1)Mobile device support: ProDiscover Forensic includes tools for acquiring and analyzing data from mobile devices such as smartphones and tablets.

2)Cloud support: ProDiscover Forensic has the capability to acquire and analyze data from cloud services like Google Drive, OneDrive, and Dropbox.

3)File system support: ProDiscover Forensic supports a wide range of file systems, including NTFS, FAT, exFAT, ext2/3/4, HFS+, and APFS.

4)Reporting: ProDiscover Forensic includes a built-in reporting feature that allows examiners to create and export detailed reports of their findings.

5)Encryption support: ProDiscover Forensic has the ability to decrypt and analyze data stored on encrypted devices, even if the encryption key is unknown.

3. ENCASE

EnCase is a commercial digital forensic software tool used by law enforcement, government, and corporate examiners to acquire, analyze, and share forensic data. It is used to recover data from various devices such as hard drives, mobile phones, and other forms of digital storage media. It also includes features for analyzing and reporting on the collected data. It is developed by Guidance Software, Inc.

some of the key features include:

1)Data acquisition: EnCase allows for the acquisition of data from various sources, including hard drives, mobile phones, and other forms of digital storage media. It supports both logical and physical data acquisition, including the ability to create images of the acquired data.

2)Data analysis: EnCase includes advanced analytical tools that allow examiners to search, analyze, and report on collected data. It has a built-in keyword search function, hash filtering, and support for regular expressions. It also allows to create timeline, identify and extract artifacts such as emails, chats, instant messages, pictures and videos

3)File carving: EnCase can recover deleted files and fragmented data by "carving" it out of unallocated space on the hard drive.

4)File header and footer detection: EnCase can detect and extract files based on their header and footer signatures.

5)File system support: EnCase supports a wide range of file systems, including NTFS, FAT, exFAT, ext2/3/4, HFS+, and APFS.

4. FTK (FORENSIC TOOLKIT)

FTK (Forensic Toolkit) is a commercial digital forensic software tool developed by AccessData. It is widely used by law enforcement, government agencies, and corporate organizations to acquire, analyze, and report on digital evidence. FTK is known for its fast processing speeds and powerful analytical capabilities.

Some of the key features of FTK include:

1)Data acquisition: FTK allows for the acquisition of data from various sources, including hard drives, mobile phones, and other forms of digital storage media. It supports both logical and physical data acquisition, and can create images of the acquired data.

2)Data analysis: FTK includes advanced analytical tools that allow examiners to search, analyze, and report on collected data. It has a built-in keyword search function, hash filtering, and support for regular expressions.

3)File carving: FTK can recover deleted files and fragmented data by "carving" it out of unallocated space on the hard drive.

4)File header and footer detection: FTK can detect and extract files based on their header and footer signatures.

5)File system support: FTK supports a wide range of file systems, including NTFS, FAT, exFAT, ext2/3/4, HFS+, and APFS.

5. X-Ways Forensics

X-Ways Forensics is a commercial digital forensic software tool developed by X-Ways Software Technology AG. It is used by law enforcement, government agencies, and corporate organizations to acquire, analyze, and report on digital evidence. X-Ways Forensics is known for its user-friendly interface and powerful data analysis capabilities.

Some of the key features of X-Ways Forensics include:

1)Data acquisition: X-Ways Forensics allows for the acquisition of data from various sources, including hard drives, mobile phones, and other forms of digital storage media. It supports both logical and physical data acquisition, and can create images of the acquired data.

2)Data analysis: X-Ways Forensics includes advanced analytical tools that allow examiners to search, analyze, and report on collected data. It has a built-in keyword search function, hash filtering, and support for regular expressions.

3)File carving: X-Ways Forensics can recover deleted files and fragmented data by "carving" it out of unallocated space on the hard drive.

4)File header and footer detection: X-Ways Forensics can detect and extract files based on their header and footer signatures.

5)File system support: X-Ways Forensics supports a wide range of file systems, including NTFS, FAT, exFAT, ext2/3/4, HFS+, and APFS.

6. Xplico

Xplico is an open-source digital forensic software tool developed by the Xplico team. It is designed to extract and analyze data from network traffic and can be used to investigate various types of network-based crimes such as cyber attacks, data breaches, and theft of intellectual property. Xplico is able to extract and analyze data from a wide range of network protocols including HTTP, FTP, SMTP, and many others.

Some of the key features of Xplico include:

1)Network traffic analysis: Xplico is able to analyze network traffic, extract and decode various types of data such as email, instant messaging, and file transfer.

2)Protocol decoding: Xplico can decode a wide range of network protocols, including HTTP, FTP, SMTP, and many others.

3)Evidence visualization: Xplico includes a graphical user interface that allows investigators to visualize the extracted data, making it easier to identify patterns and anomalies.

4)Reporting: Xplico includes a built-in reporting feature that allows investigators to create and export detailed reports of their findings.

5)Open-source: Xplico is an open-source software, which means that the source code is publicly available for anyone to use, modify and distribute.

7. The Sleuth Kit (+Autopsy)

The Sleuth Kit (TSK) is a collection of open-source digital forensic tools developed by Brian Carrier. It is designed to be used as a command-line tool or in conjunction with Autopsy, a graphical user interface (GUI) for TSK. Together, TSK and Autopsy provide a comprehensive set of forensic tools for the acquisition, analysis, and reporting of digital evidence.

Some of the key features of TSK and Autopsy include:

1)Reporting: Autopsy includes a built-in reporting feature that allows examiners to create and export detailed reports of their findings.

2)Open-source: TSK and Autopsy are open-source software, which means that the source code is publicly available for anyone to use, modify, and distribute.

3)Scripting and automation: TSK allows to automate repetitive tasks, and enables to create custom scripts and plug-ins to perform complex tasks and analysis.

4)Multi-language support: Autopsy can extract and analyze data in various languages.

5)Advanced search capabilities: Autopsy allows to search multiple keywords, Boolean search, Exact and Fuzzy search, and search by hash values.

8. Oxygen Forensic Suite

Oxygen Forensic Suite is a commercial digital forensic software tool developed by Oxygen Forensics. It is used by law enforcement, government agencies, and corporate organizations to acquire, analyze, and report on digital evidence. Oxygen Forensic Suite is known for its ability to extract and analyze data from a wide range of devices and applications, including mobile devices, cloud services, and other forms of digital storage media.

Some of the key features of Oxygen Forensic Suite include:

1)Data acquisition: Oxygen Forensic Suite allows for the acquisition of data from various sources, including hard drives, mobile phones, and other forms of digital storage media. It supports both logical and physical data acquisition, and can create images of the acquired data.

2)Data analysis: Oxygen Forensic Suite includes advanced analytical tools that allow examiners to search, analyze, and report on collected data. It has a built-in keyword search function, hash filtering, and support for regular expressions.

3)Mobile device support: Oxygen Forensic Suite includes tools for acquiring and analyzing data from mobile devices such as smartphones and tablets, including the ability to extract data from the cloud services and third-party applications.

4)Cloud support: Oxygen Forensic Suite has the capability to acquire and analyze data from cloud services like Google Drive, OneDrive, and Dropbox.

5)Social Media and messengers support: Oxygen Forensic Suite can extract and analyze data from various social media and instant messaging applications, such as WhatsApp, Telegram, Facebook, Instagram, Snapchat, and many others.

9. BlackLight

BlackLight is a commercial digital forensic software tool developed by BlackBag Technologies. It is used by law enforcement, government agencies, and corporate organizations to acquire, analyze, and report on digital evidence. BlackLight is known for its ability to extract and analyze data from a wide range of devices and file systems, including hard drives, mobile devices, cloud services, and other forms of digital storage media.

Some of the key features of BlackLight include:

1)Data acquisition: BlackLight allows for the acquisition of data from various sources, including hard drives, mobile phones, and other forms of digital storage media. It supports both logical and physical data acquisition, and can create images of the acquired data.

2)Data analysis: BlackLight includes advanced analytical tools that allow examiners to search, analyze, and report on collected data. It has a built-in keyword search function, hash filtering, and support for regular expressions.

3)Mobile device support: BlackLight includes tools for acquiring and analyzing data from mobile devices such as smartphones and tablets.

4)Cloud support: BlackLight has the capability to acquire and analyze data from cloud services like Google Drive, OneDrive, and Dropbox.

5)File system support: BlackLight supports a wide range of file systems, including NTFS, FAT, exFAT, ext2/3/4, HFS+, and APFS.

10. Cellebrite UFED

Cellebrite UFED (Universal Forensic Extraction Device) is a commercial digital forensic software tool developed by Cellebrite. It is used by law enforcement, government agencies, and corporate organizations to acquire, analyze, and report on digital evidence from mobile devices, such as smartphones and tablets. UFED is known for its ability to extract and analyze data from a wide range of mobile devices, including both iOS and Android devices.

Some of the key features of Cellebrite UFED include:

1)Social Media and messengers support: UFED can extract and analyze data from various social media and instant messaging applications, such as WhatsApp, Telegram, Facebook, Instagram, Snapchat, and many others.

2)Reporting: UFED includes a built-in reporting feature that allows examiners to create and export detailed reports of their findings.

3)Encryption support: UFED has the ability to decrypt and analyze data stored on encrypted devices, even if the encryption key is unknown.

4)Advanced search capabilities: UFED allows to search multiple keywords, Boolean search, Exact and Fuzzy search, and search by hash values.

5)Scripting and automation: UFED allows to automate repetitive tasks, and enables to create custom scripts and plug-ins to perform complex tasks and analysis.

6)Mobile forensics lab in a box: UFED is portable and allows to perform forensics on site, without the need to bring the device to the lab

Practical - 2

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

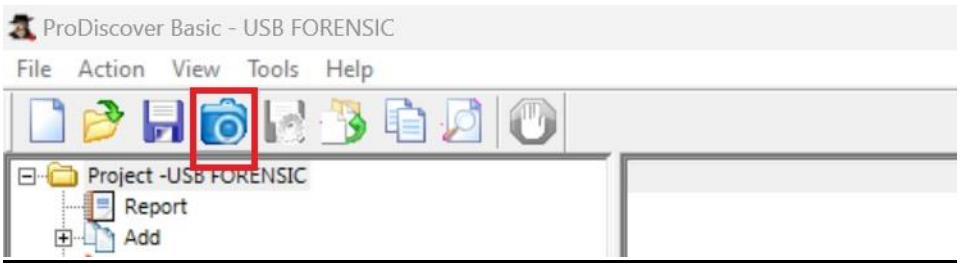
I.PRODISCOVER:

Procedure:

1.) Connect the storage device to the computer where ProDiscover is installed.

2.) Open ProDiscover Basic software and Enter Project Name,Number and description of it and then click on the “open” button.

3)Click on the " Capture Image " button located on the main toolbar.



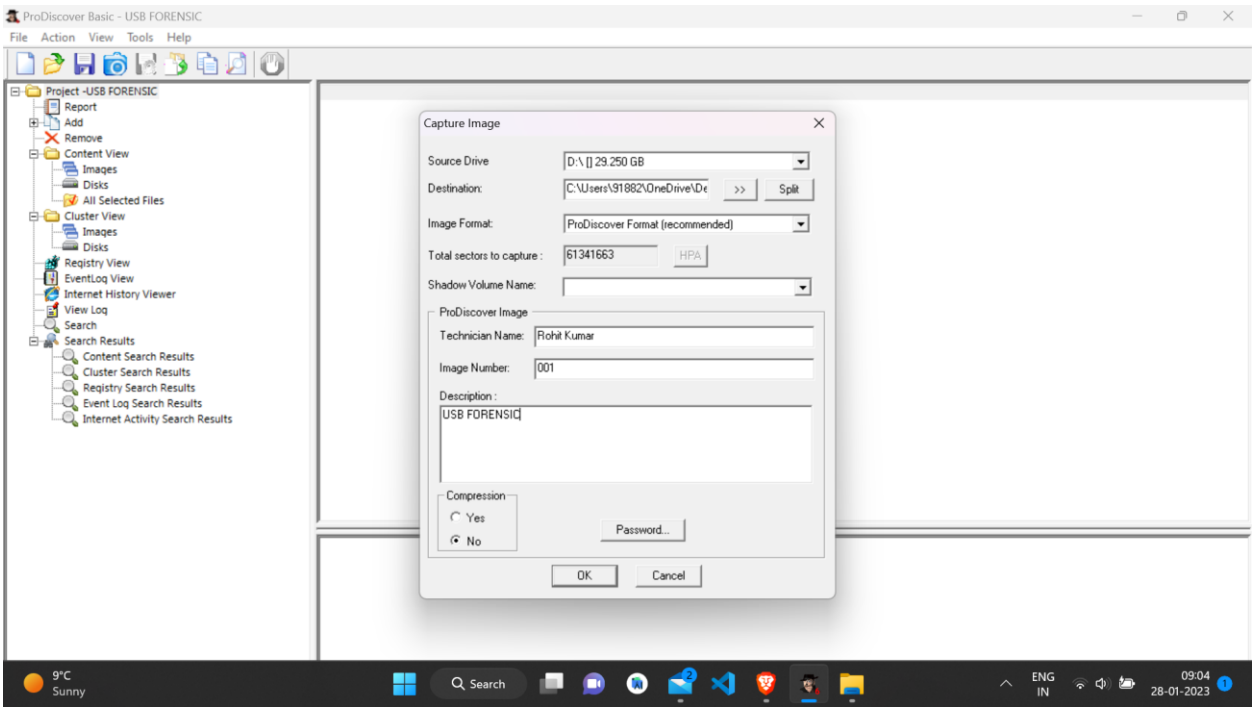
4) In the "Capture Image" window,

->Select the storage device that you want to image from the list of available devices.

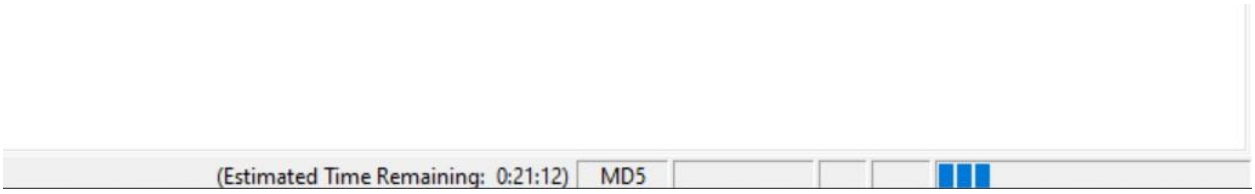
->Select the destination folder where you want to save the image file, and enter a name for the image file.

->Enter the Technician Name,Image Number and description

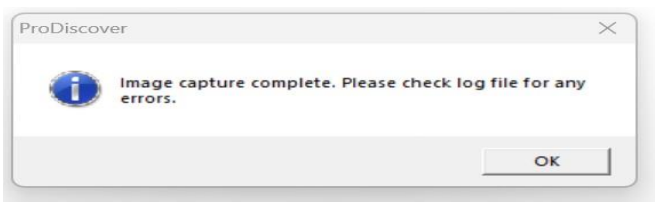
->Click the "ok" button to begin the imaging process.



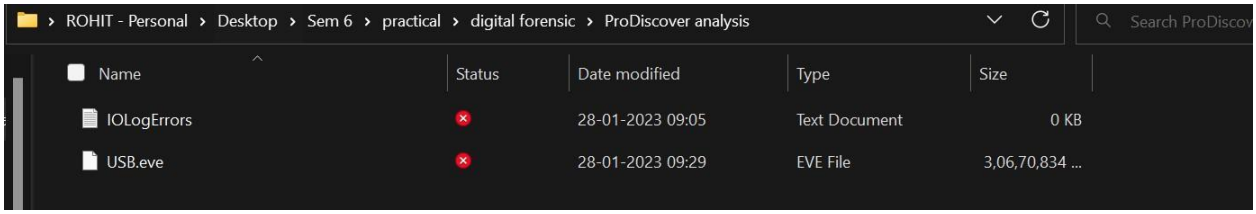
5) Monitor the Progress of the Imaging Process.When the imaging starts,a progress bar will be displayed in the bottom right corner.



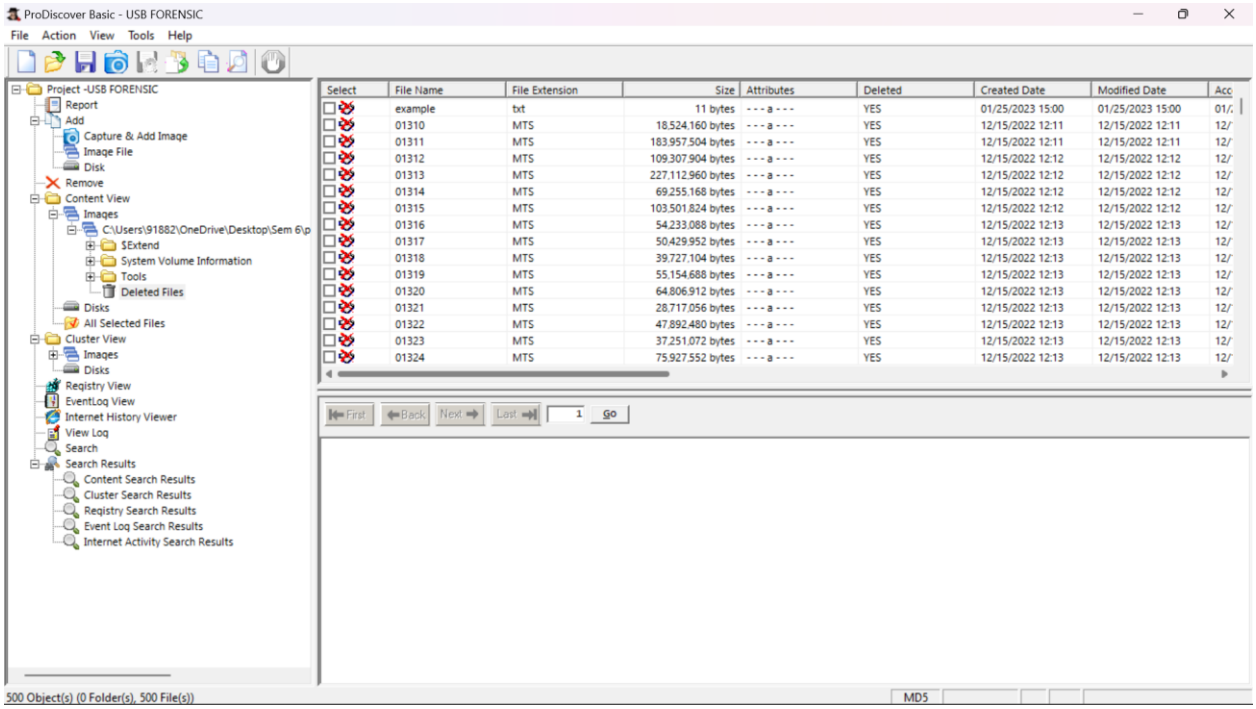
6) Once the imaging process is complete, it will show a pop up window of “image Capture Completed”.



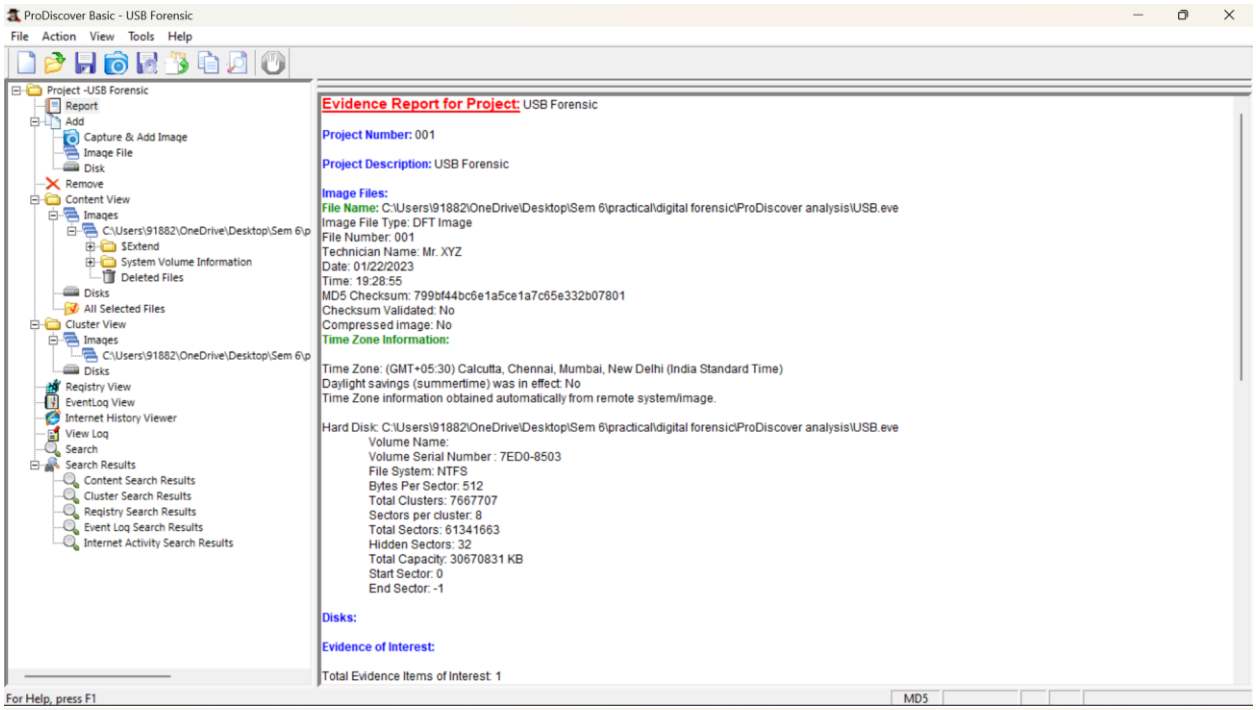
7)The image file is saved in the destination folder that you specified.

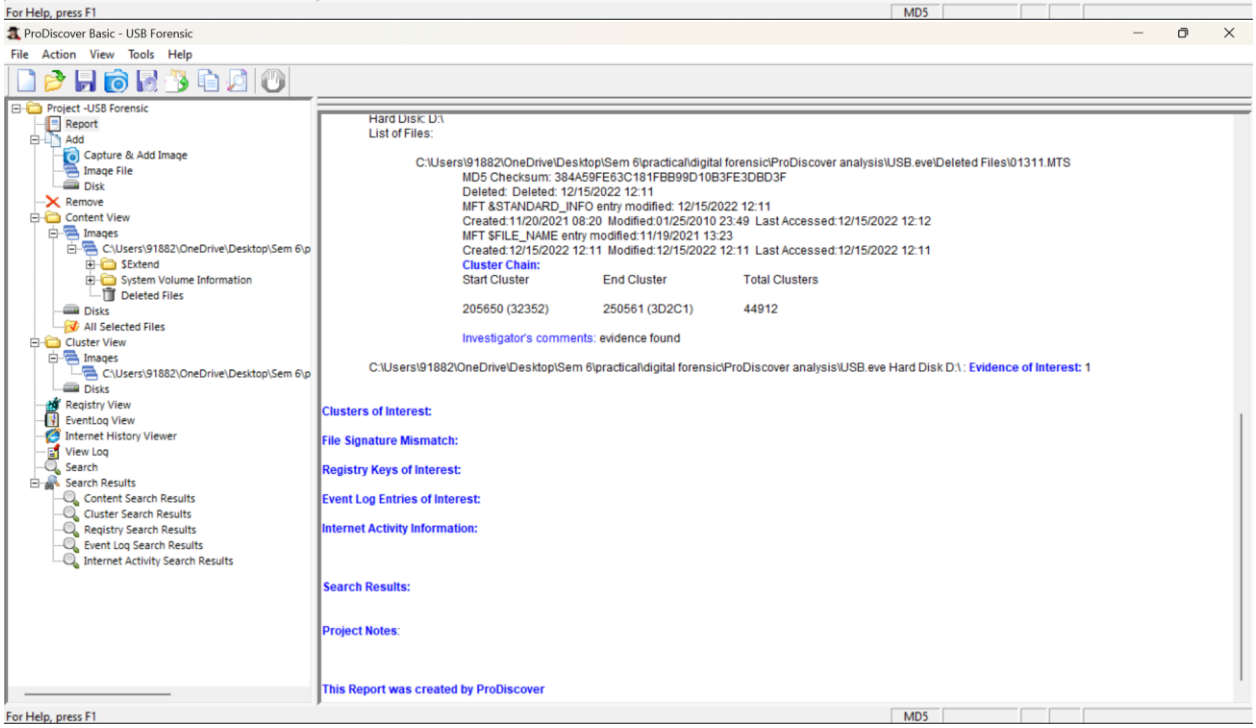


#Now, you can open your image file by clicking “add”->”image File”->then select the image file where you have stored and image will be open in the prodiscover software for analysis purpose and red cross marks which is shown in the software are the files which are deleted from the storage device



PRODISCOVER FORENSIC REPORT



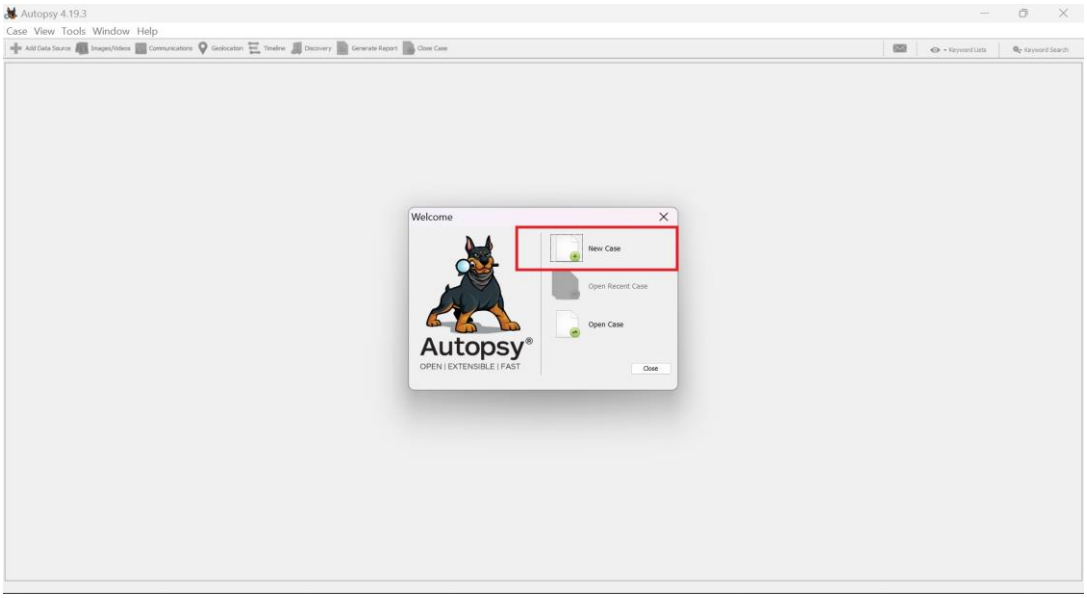


II.AUTOPSY:

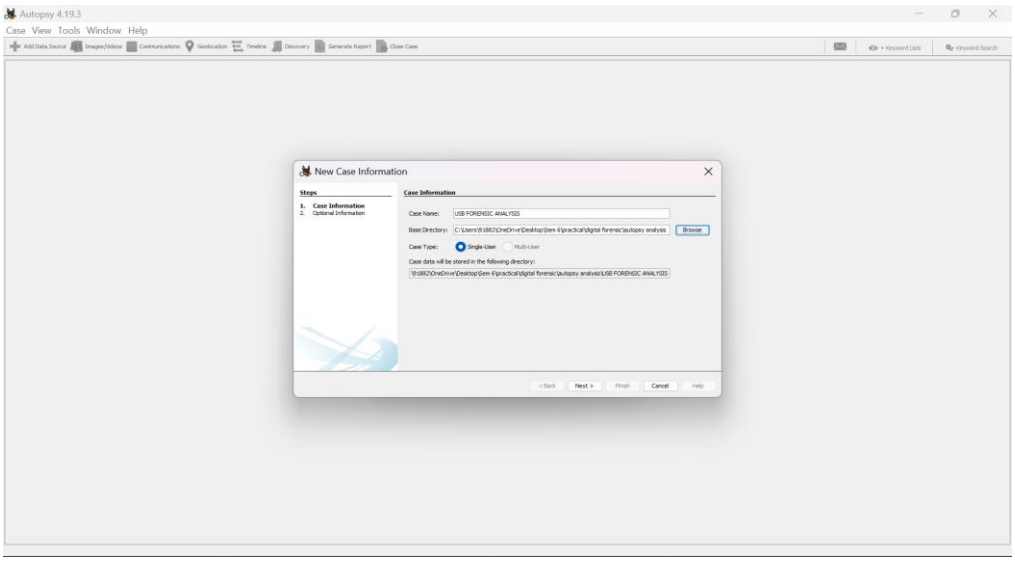
Procedure:

1.) Connect the storage device to the computer where Autopsy is installed.

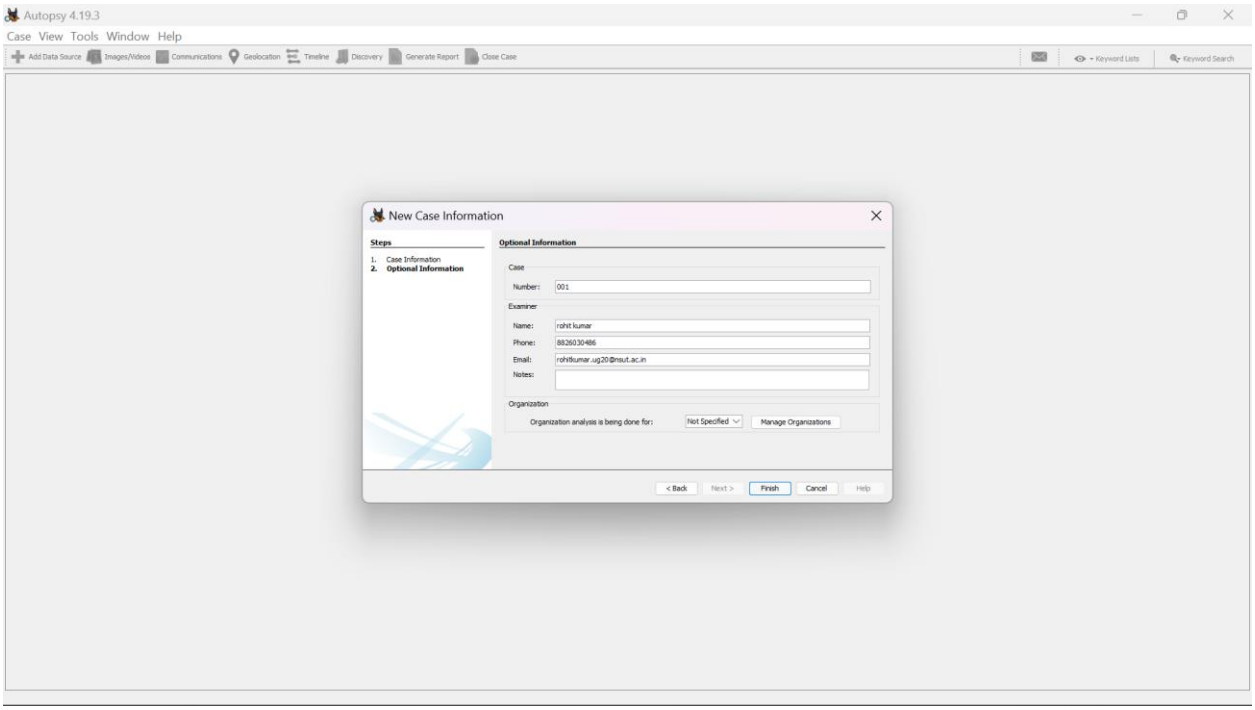
2.) Launch Autopsy, and click on the "New Case" button.



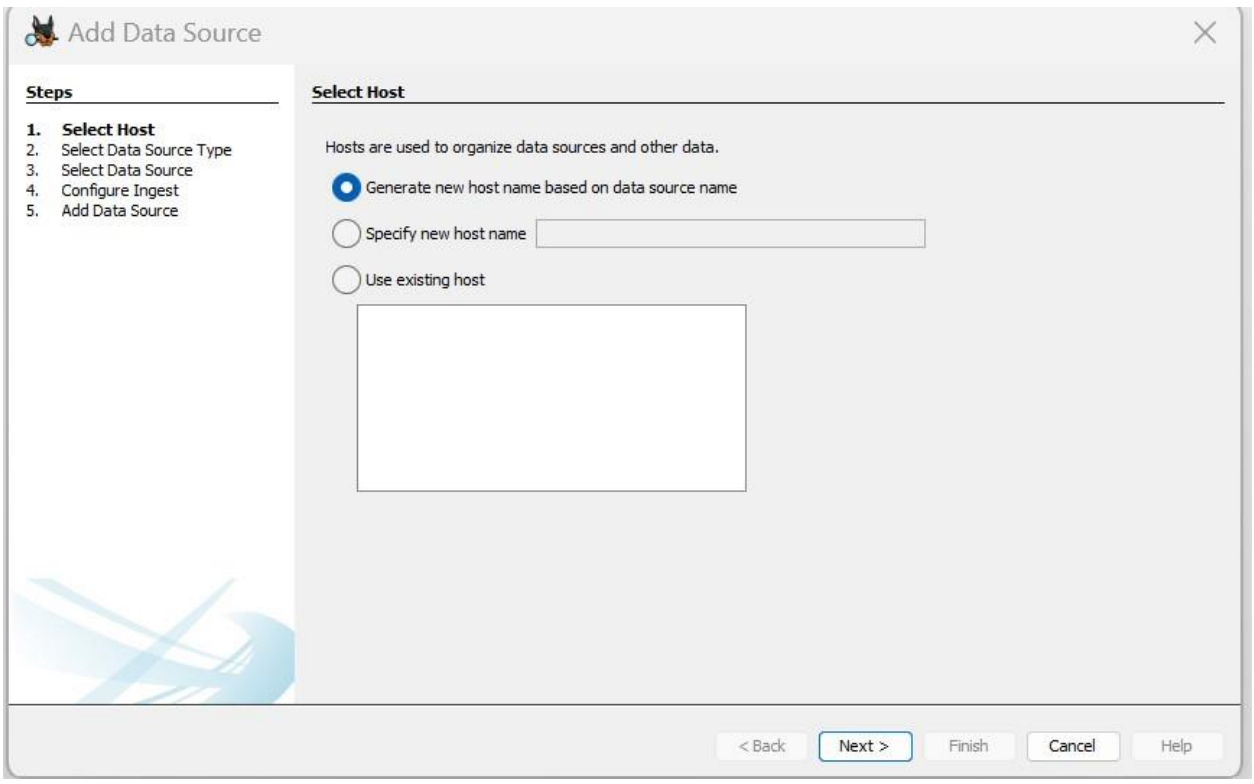
3) Enter Case Name and Base Directory where you want to store your Forensic image then click “Next”.



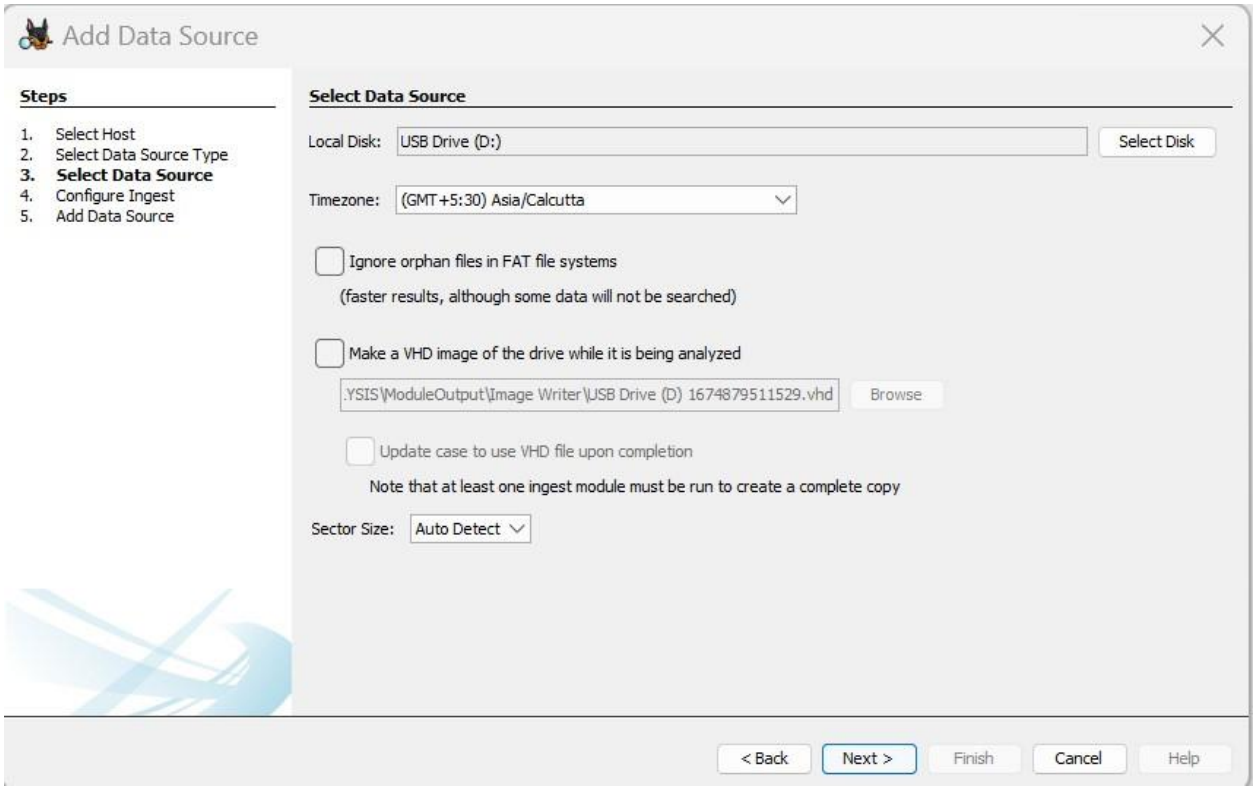
4) Now, Enter case number,and all other information and then click “Finish” Button



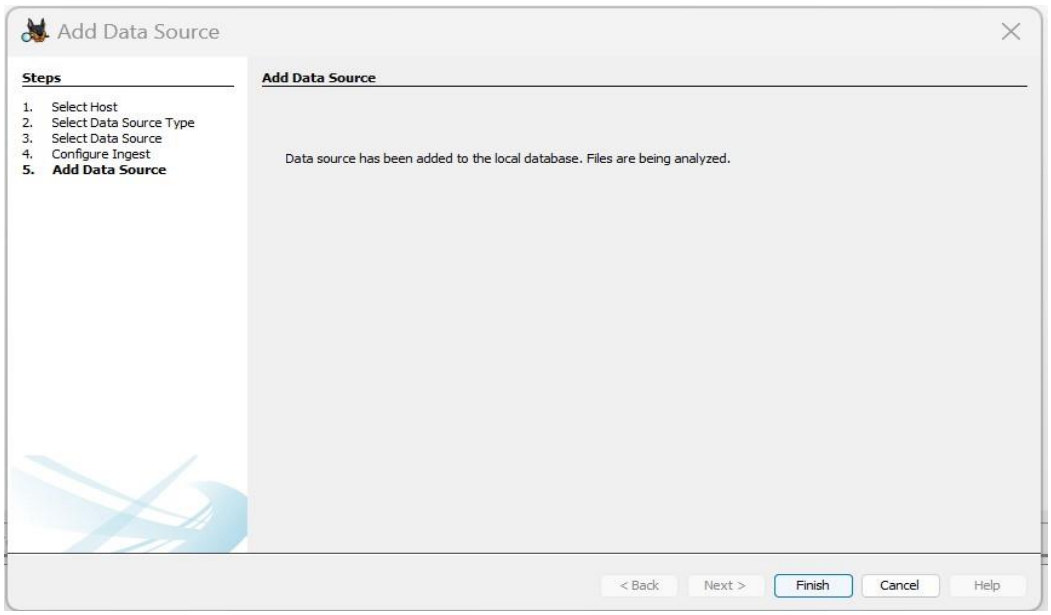
5) Now, in add data source window , select first option which is “Generate new host name”



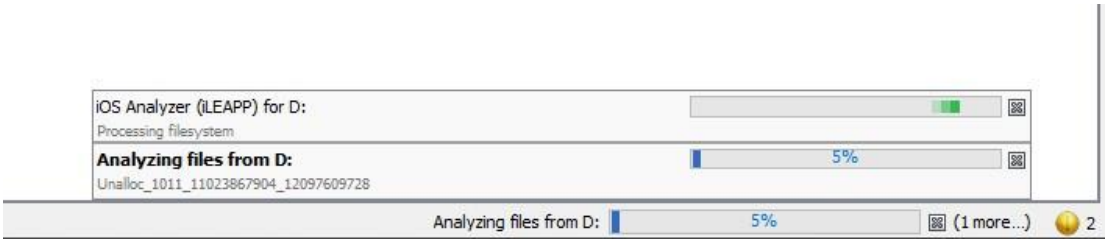
6)Then, Select “Local Disk” as data source type and then select the storage device by clicking “Select Disk” button then click “next” button.



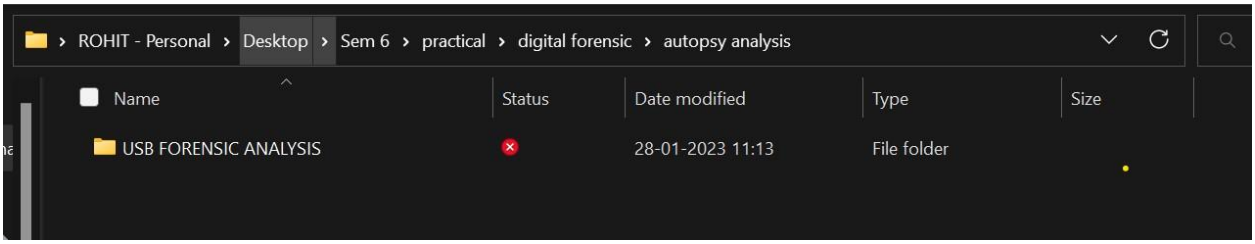
7)Now, it will show “Data source has been added” . click on finish button



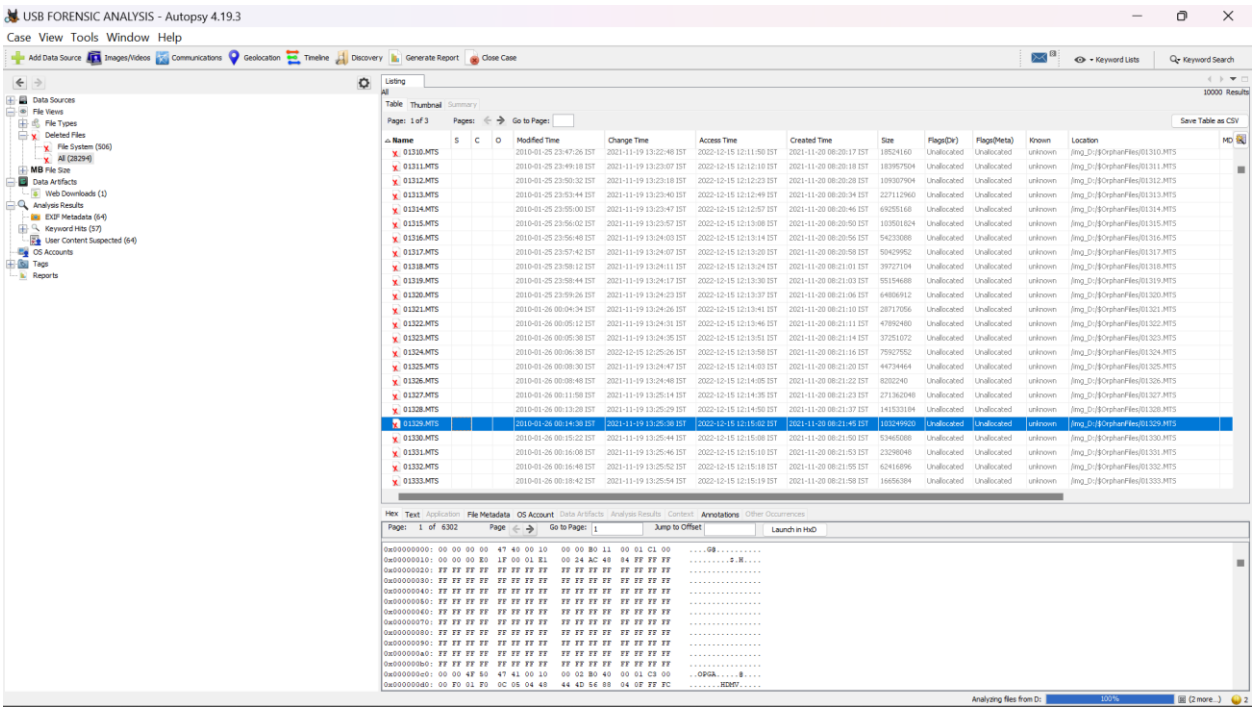
8)Now, it will start analyzing file of storage device and progress of it will be shown in the bottom left corner of the window.



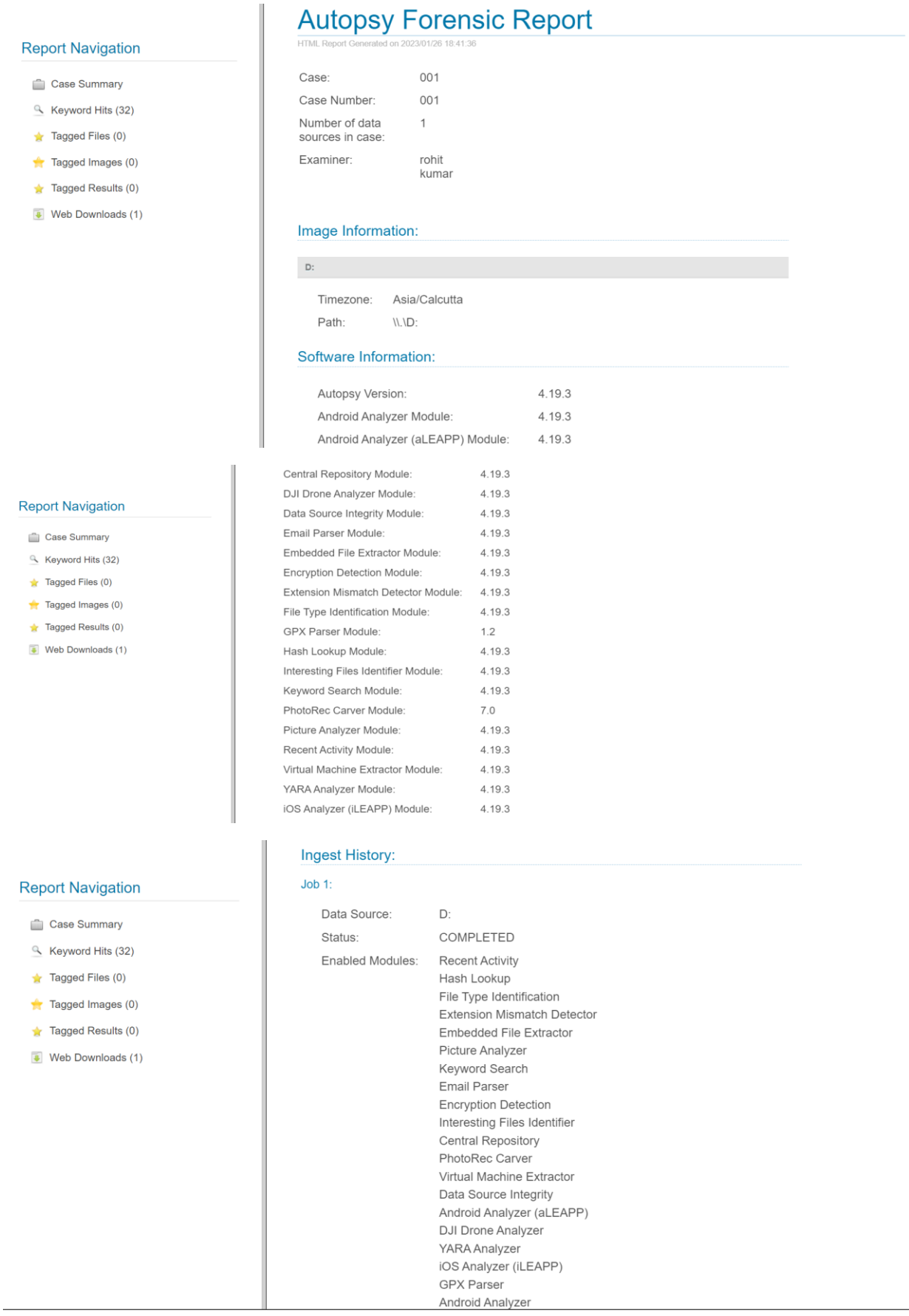
9)After the progress completed ,the image will be created on the destination folder and the image file will automatically be open in the autopsy software where you can analyzed the image file.



Now, you can see deleted files of storage device by clicking “Deleted Files” and the red cross marks files which are shown in the software are the deleted files .you can also preview the files by clicking on it



AUTOPSY FORENSIC REPORT



Report Navigation

- Case Summary
- Keyword Hits (32)
- Tagged Files (0)
- Tagged Images (0)
- Tagged Results (0)
- Web Downloads (1)

Autopsy Forensic Report

HTML Report Generated on 2023/01/26 18:41:36

Case:	001
Case Number:	001
Number of data sources in case:	1
Examiner:	rohit kumar

Image Information:

D:

Timezone:	Asia/Calcutta
Path:	\\.\D:

Software Information:

Autopsy Version:	4.19.3
Android Analyzer Module:	4.19.3
Android Analyzer (aLEAPP) Module:	4.19.3
Central Repository Module:	4.19.3
DJI Drone Analyzer Module:	4.19.3
Data Source Integrity Module:	4.19.3
Email Parser Module:	4.19.3
Embedded File Extractor Module:	4.19.3
Encryption Detection Module:	4.19.3
Extension Mismatch Detector Module:	4.19.3
File Type Identification Module:	4.19.3
GPX Parser Module:	1.2
Hash Lookup Module:	4.19.3
Interesting Files Identifier Module:	4.19.3
Keyword Search Module:	4.19.3
PhotoRec Carver Module:	7.0
Picture Analyzer Module:	4.19.3
Recent Activity Module:	4.19.3
Virtual Machine Extractor Module:	4.19.3
YARA Analyzer Module:	4.19.3
iOS Analyzer (iLEAPP) Module:	4.19.3

Report Navigation

- Case Summary
- Keyword Hits (32)
- Tagged Files (0)
- Tagged Images (0)
- Tagged Results (0)
- Web Downloads (1)

Ingest History:

Job 1:

Data Source:	D:
Status:	COMPLETED
Enabled Modules:	Recent Activity Hash Lookup File Type Identification Extension Mismatch Detector Embedded File Extractor Picture Analyzer Keyword Search Email Parser Encryption Detection Interesting Files Identifier Central Repository PhotoRec Carver Virtual Machine Extractor Data Source Integrity Android Analyzer (aLEAPP) DJI Drone Analyzer YARA Analyzer iOS Analyzer (iLEAPP) GPX Parser Android Analyzer

III.FTK Imager :

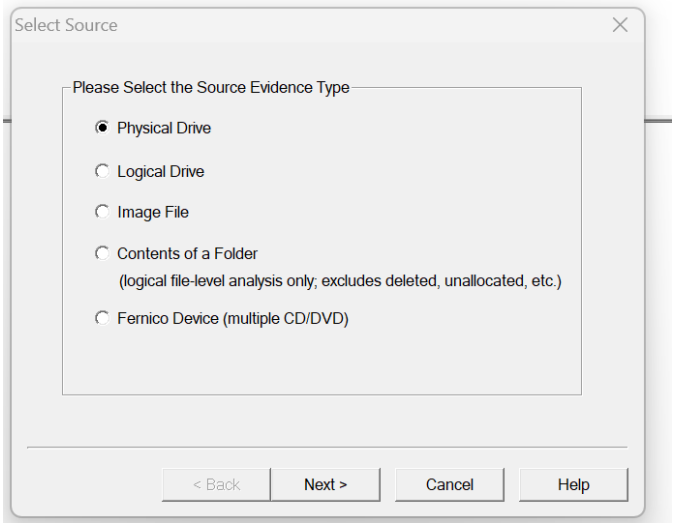
Procedure:

1.) Connect the storage device to the computer where Ftk imager is installed.

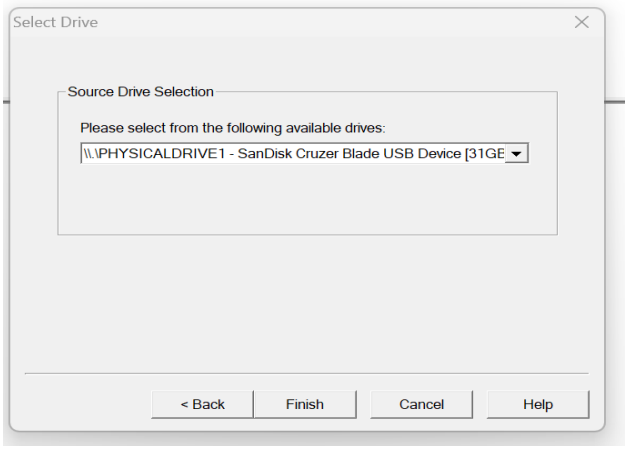
2.) Launch FTK Imager.

3.) From the "File" menu, select "Create Disk Image".

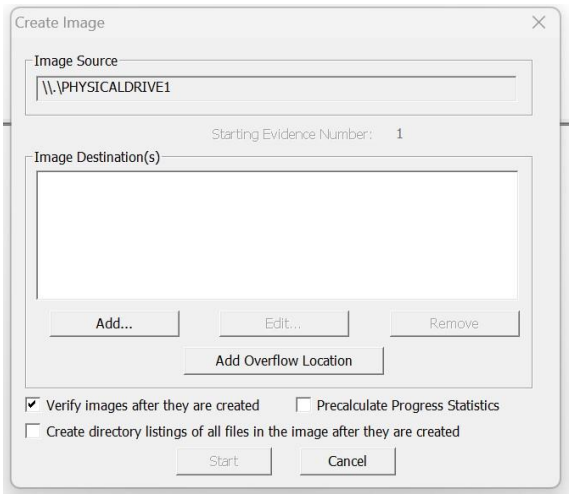
4)In the "Select Source" window, select the option to "Physical Drive"



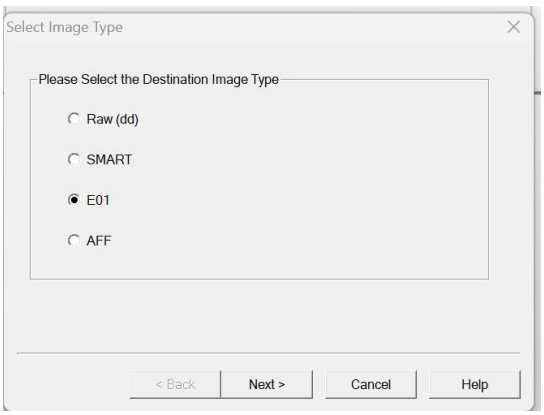
5)Then select the storage device that you want to image from the list of available devices and click Finish button.



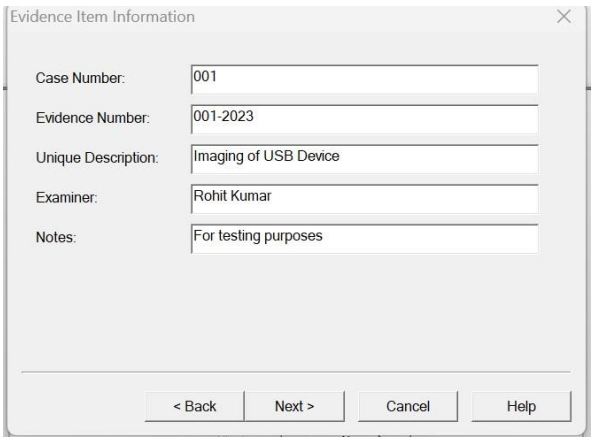
6)In Create Image Window ,Select a destination folder for the image file by clicking “add” button and It is important to select a destination folder with enough space to store the image file.



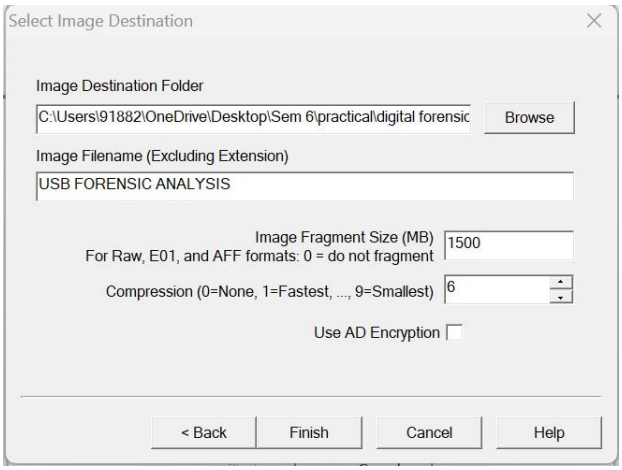
7)Select Destination Image Type and click Next



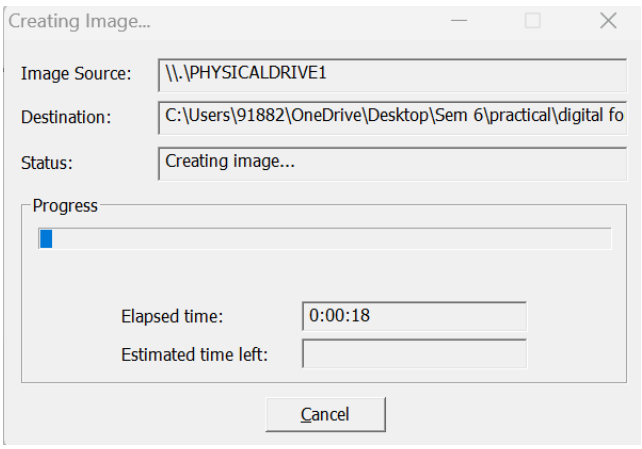
8)Enter all the required information in evidence item information window



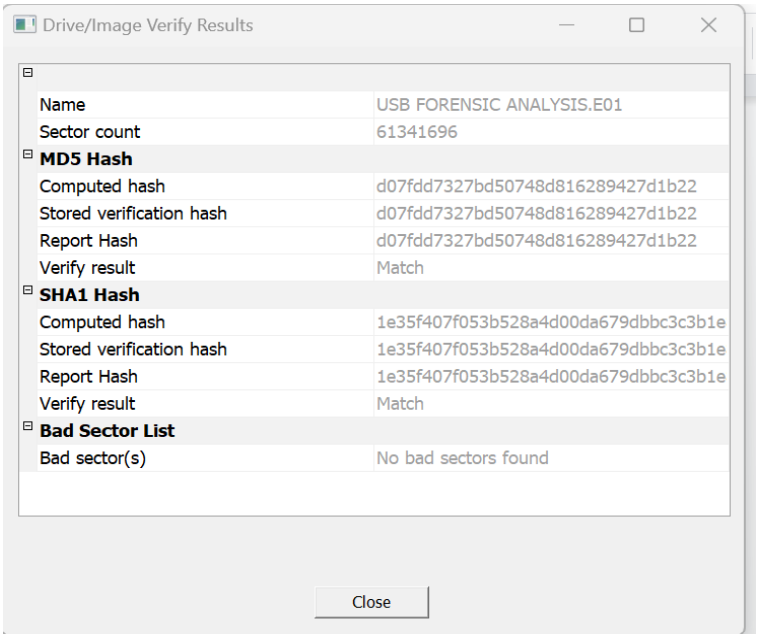
9)select destination and enter file name then click finish button.



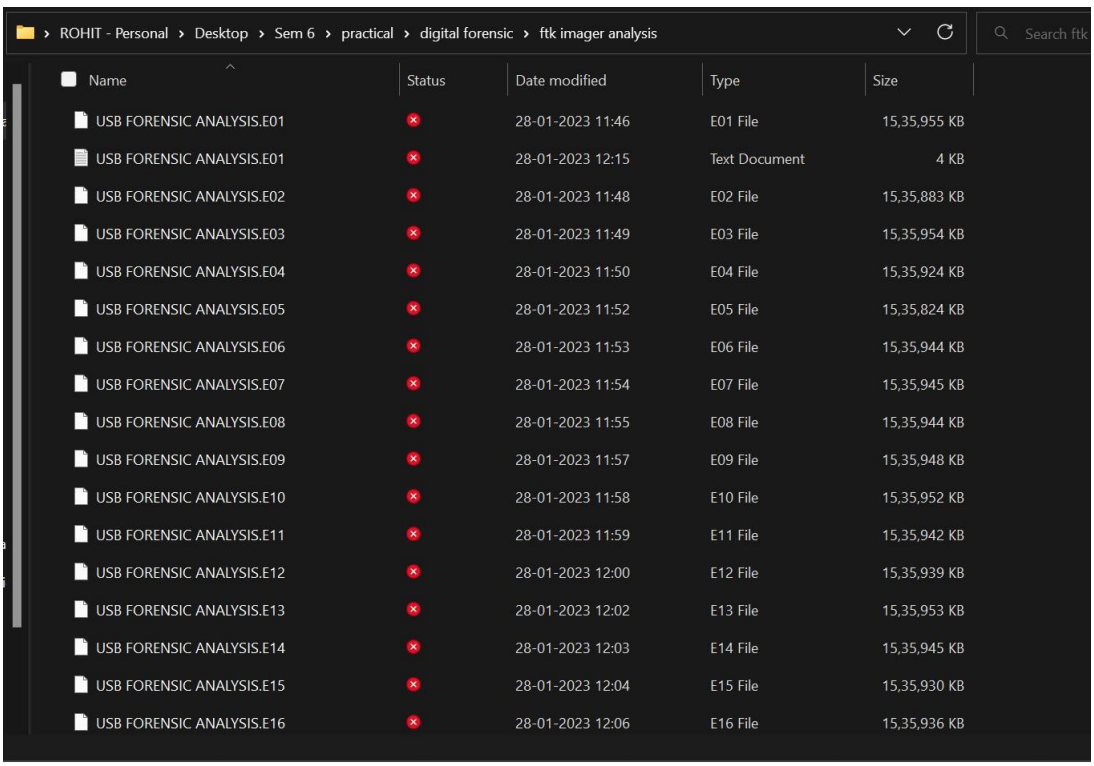
10)Click on the "start" button to start the imaging process.Monitor the progress of the imaging process in the "Creating Image" window. You can see the current status, estimated time remaining, and any errors that may occur..



11) Once the imaging process is complete, A “verify results” window will be opened which helps in verify the integrity of the image file.If the MD5 hash and sha-1 hash matches then it ensure that the image file is complete and uncorrupted.



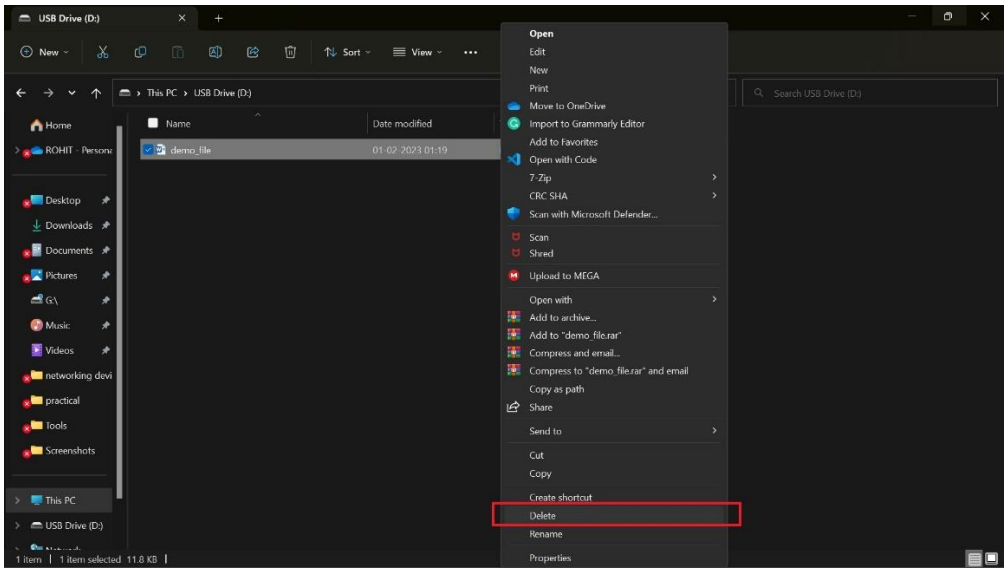
12)Lastly after the imaging process is completed the image file will be stored in the destination folder that you specify.

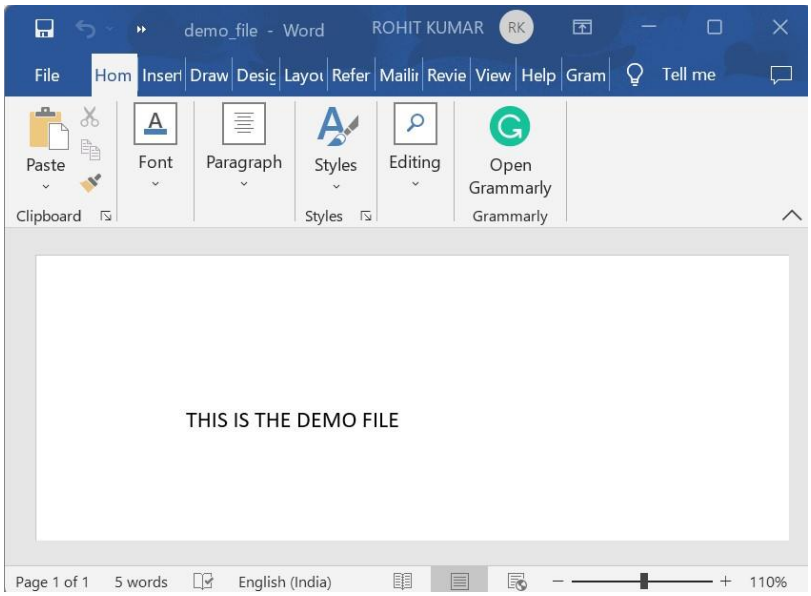


Practical - 3

Q). To Recover a Deleted file using Forensics Tools (FTK Imager/Autopsy)

THIS IS THE DEMO FILE WHICH I AM GOING TO DELETE AND RECOVERED IT USING AUTOPSY/FTK Imager



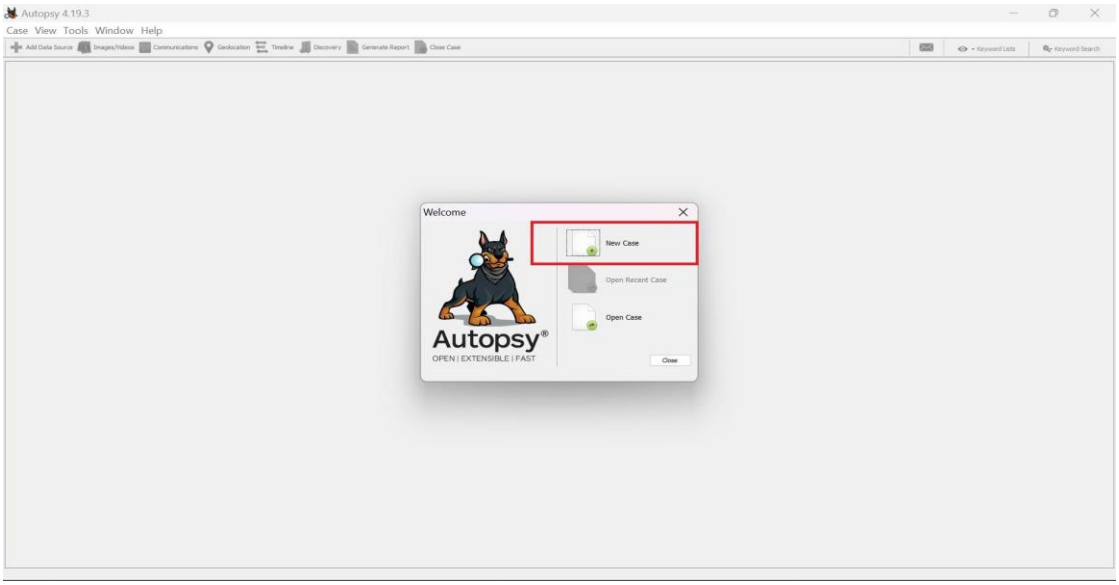


I.AUTOPSY:

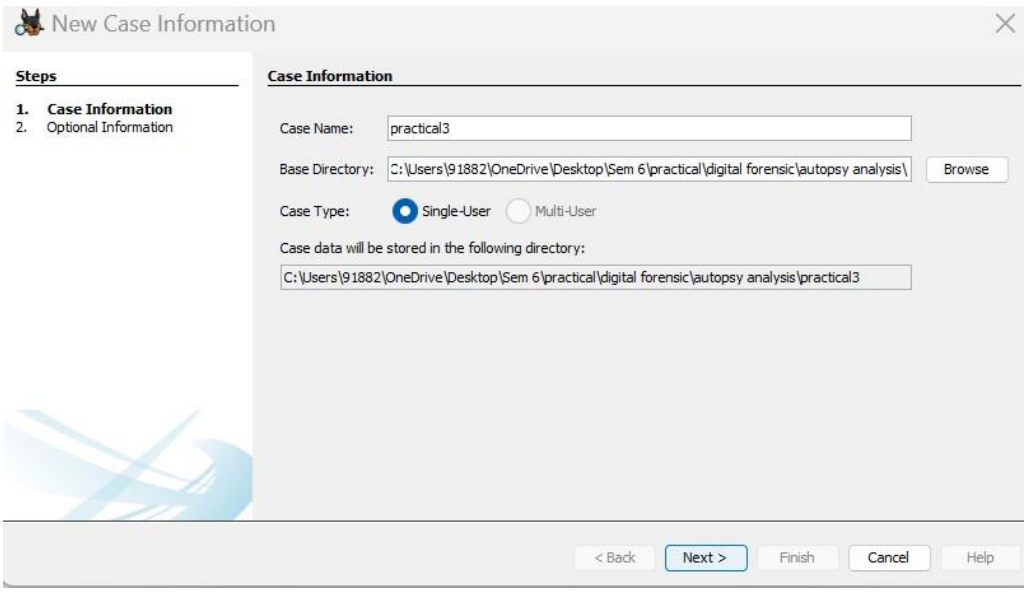
Procedure:

1.) Connect the storage device to the computer where Autopsy is installed.

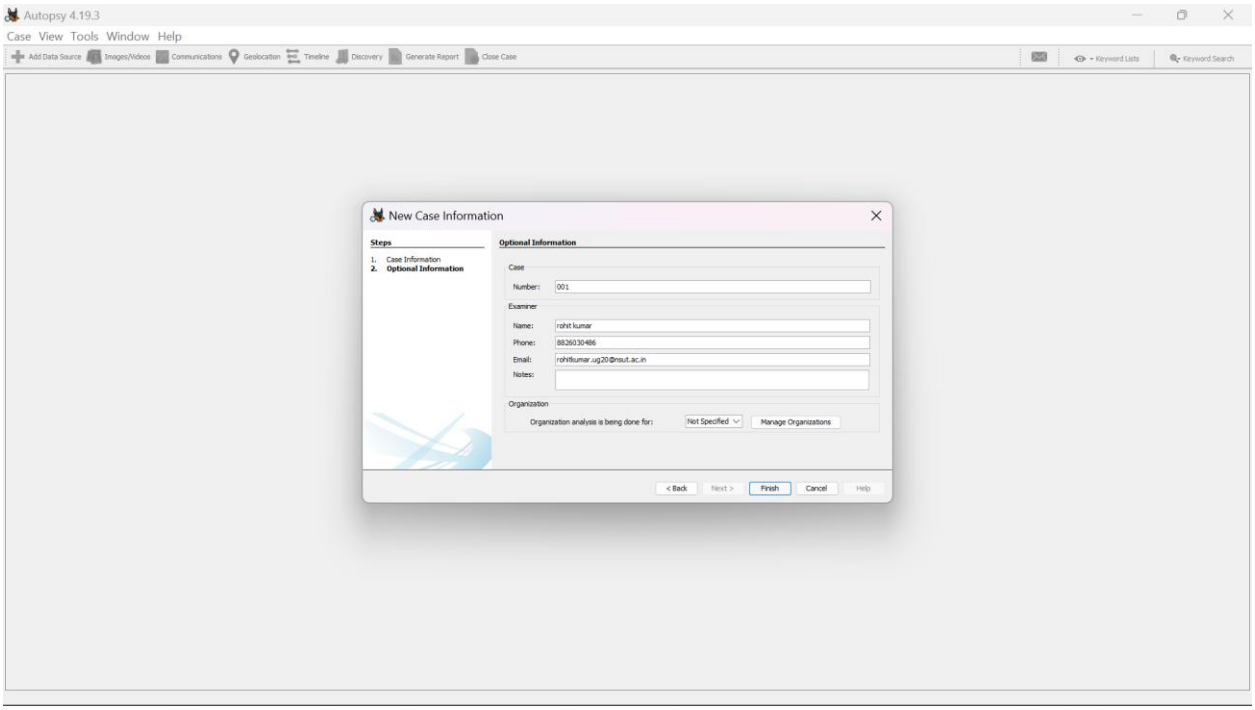
2.) Launch Autopsy, and click on the "New Case" button.



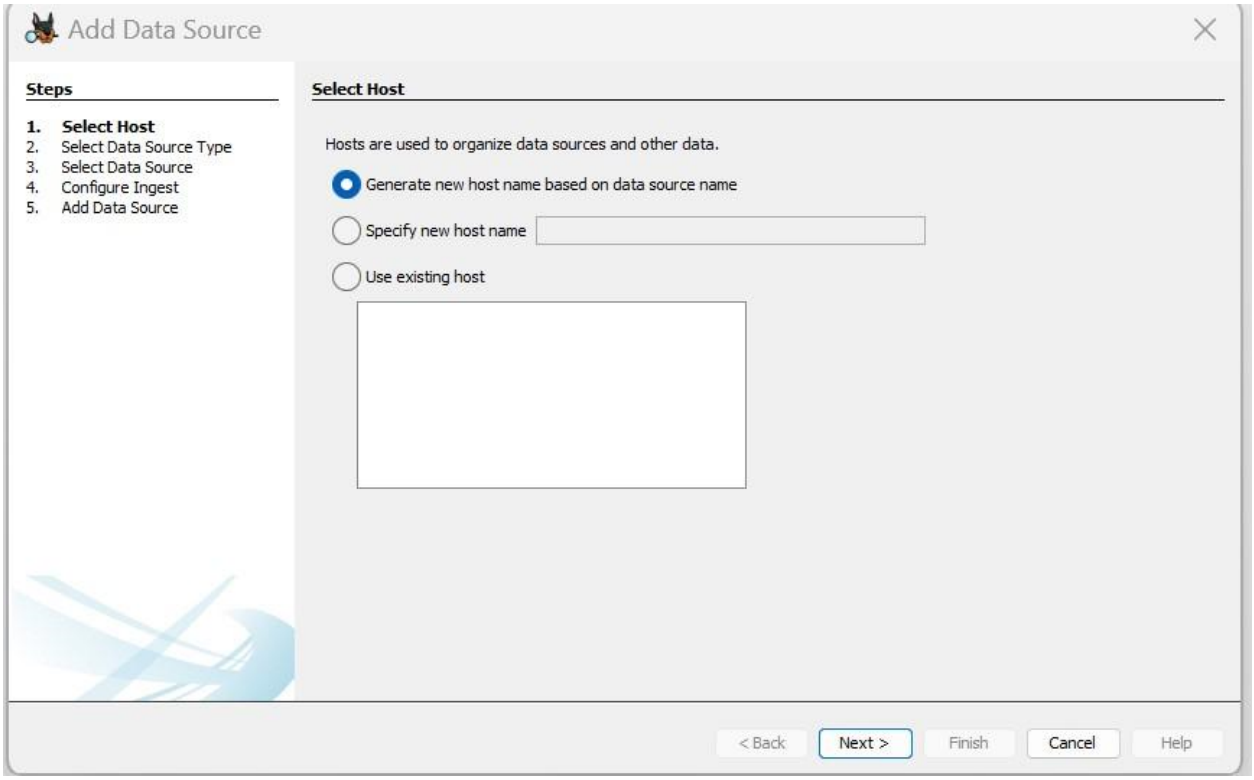
3) Enter Case Name and Base Directory where you want to store your Forensic image then click “Next”.



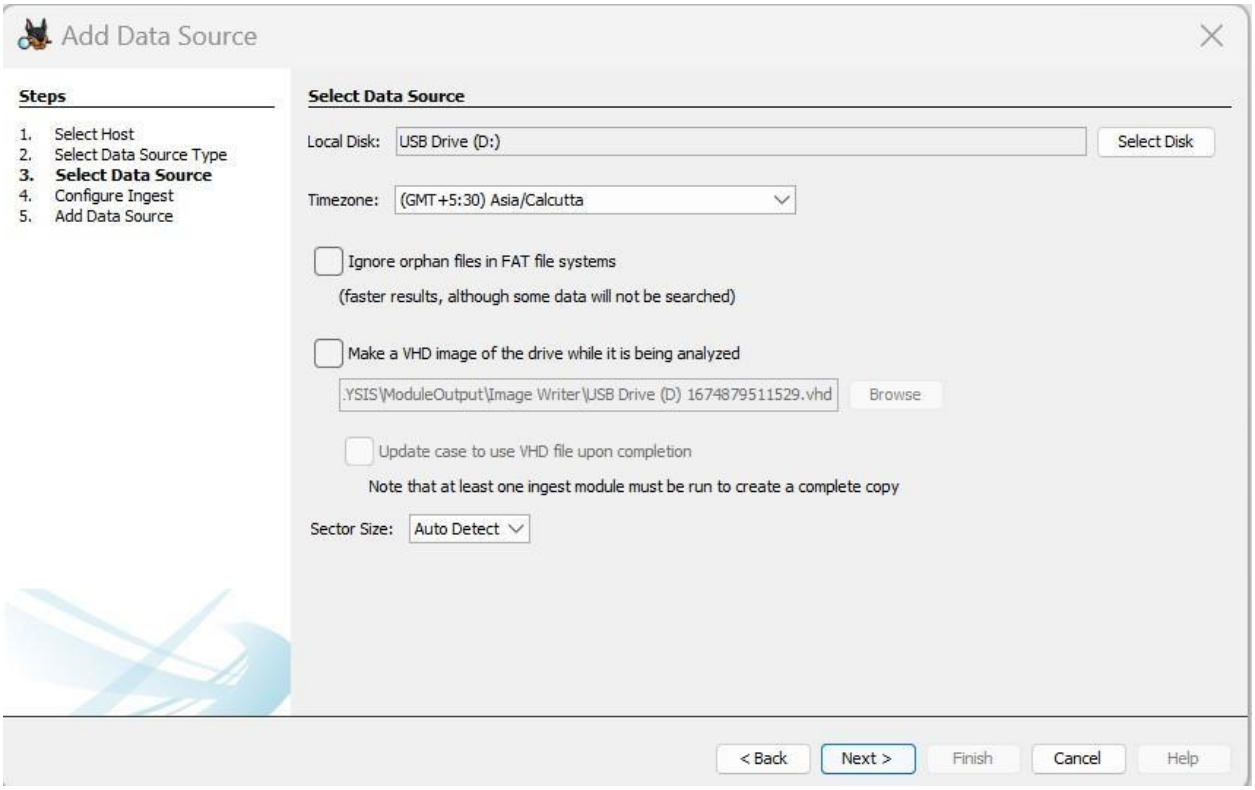
4) Now, Enter case number,and all other information and then click “Finish” Button



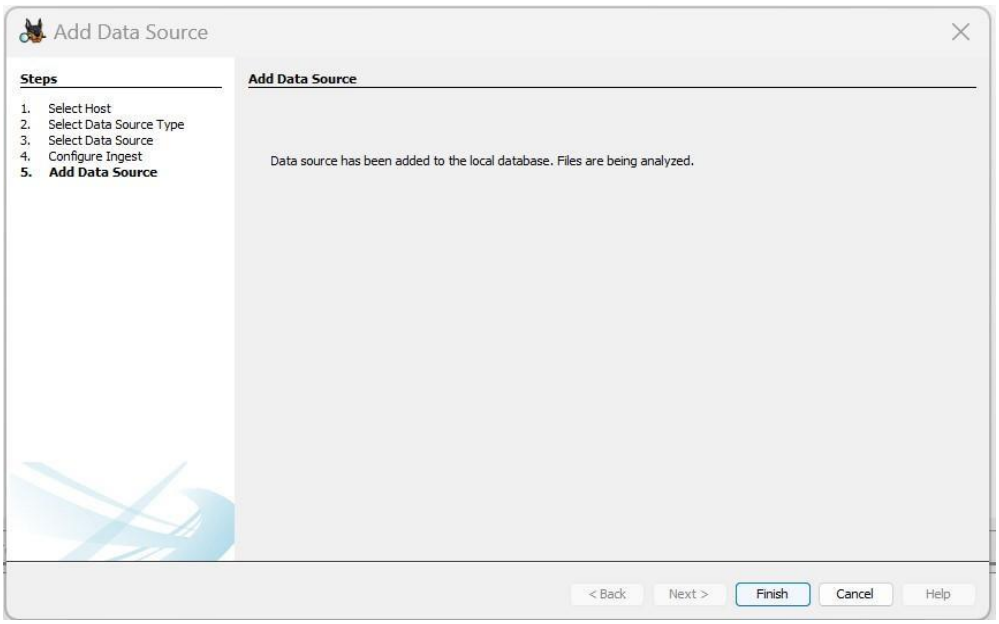
5) Now, in add data source window , select first option which is “Generate new host name”



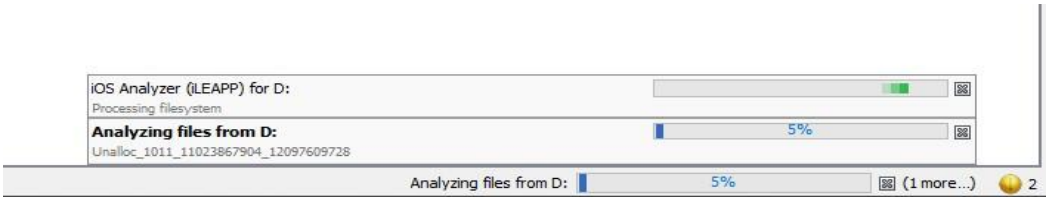
6)Then, Select “Local Disk” as data source type and then select the storage device by clicking “Select Disk” button then click “next” button.



7)Now, it will show “Data source has been added” . click on finish button

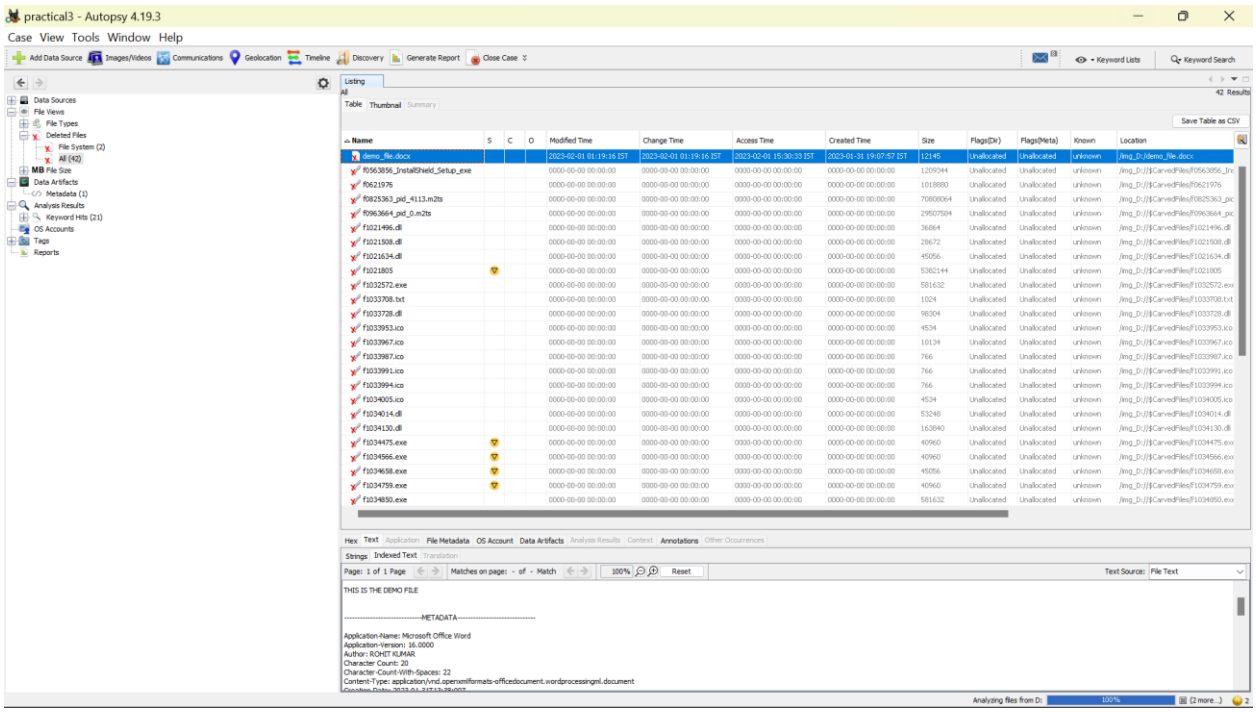


8)Now, it will start analyzing file of storage device and progress of it will be shown in the bottom left corner of the window.

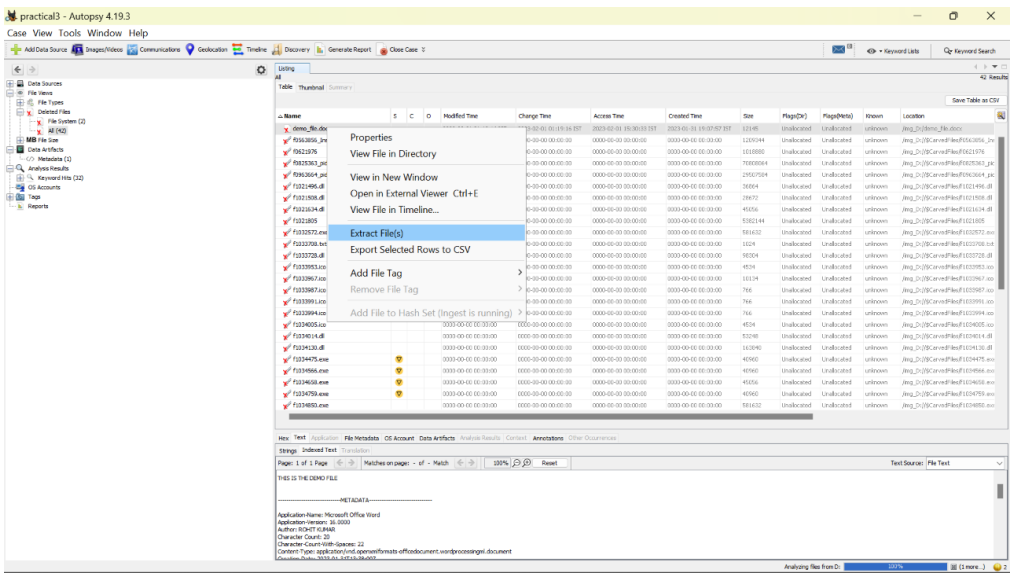


9)After the progress completed ,the image will be created on the destination folder and the image file will automatically be open in the autopsy software where you can analyzed the image file.

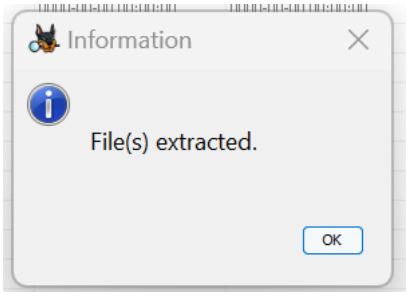
Now, you can see deleted files of storage device by clicking “Deleted Files” and the red cross marks files which are shown in the software are the deleted files .you can also preview the files by clicking on it.



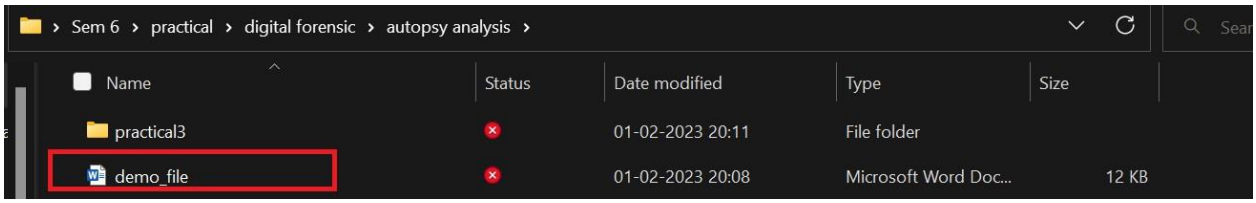
10)select the file which you want to recover and right click on it then select extract files then select the destination where you want to extract the file.In my case it is "demo" file which I have deleted.



11)After the file has been extracted it will show a pop up show of file extracted succesfully and file has been stored at destination folder



As you can see the demo file which I have deleted has been recovered



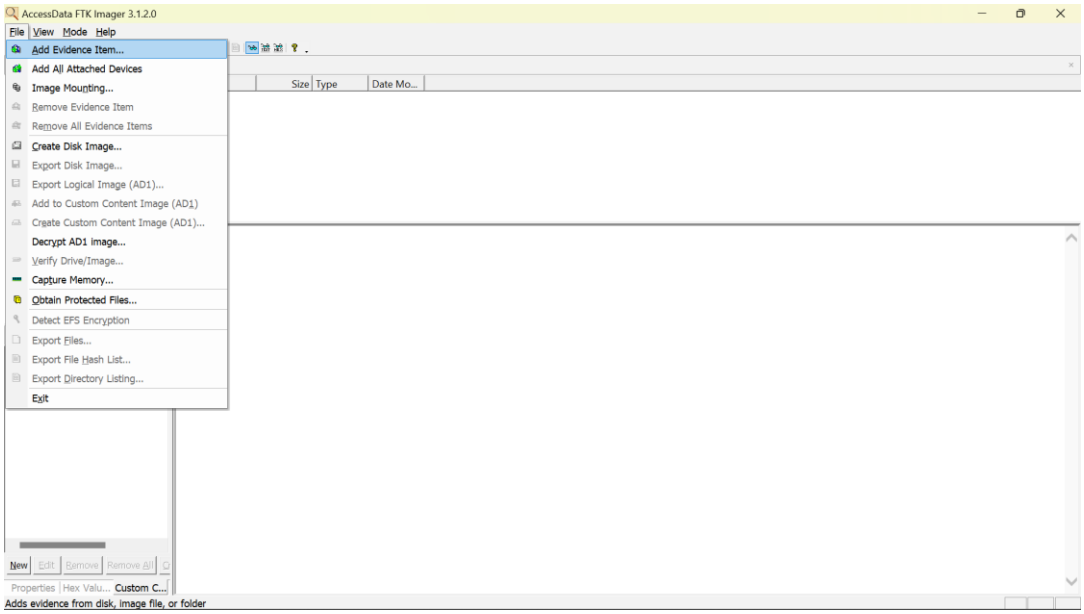
II.FTK Imager :

Procedure:

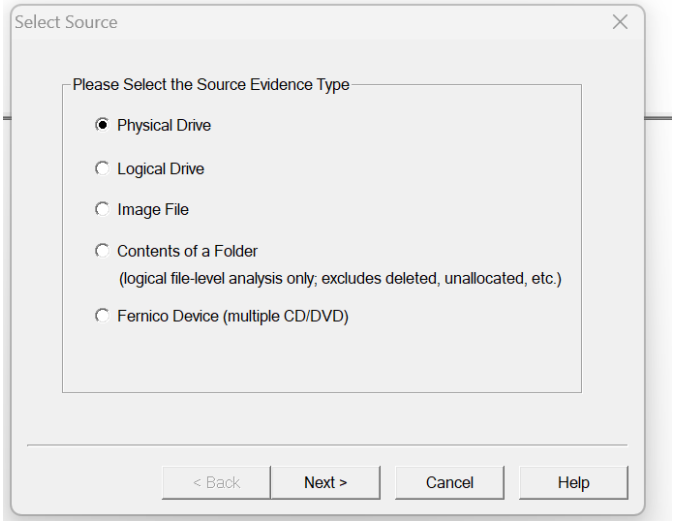
1.) Connect the storage device to the computer where Ftk imager is installed.

2.) Launch FTK Imager.

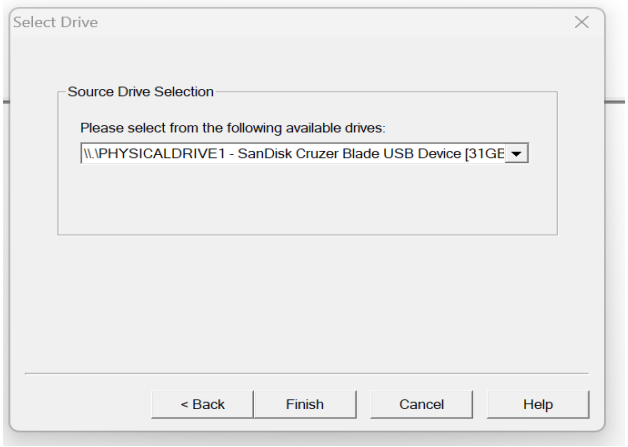
3.) From the "File" menu, select "Add Evidence Item".



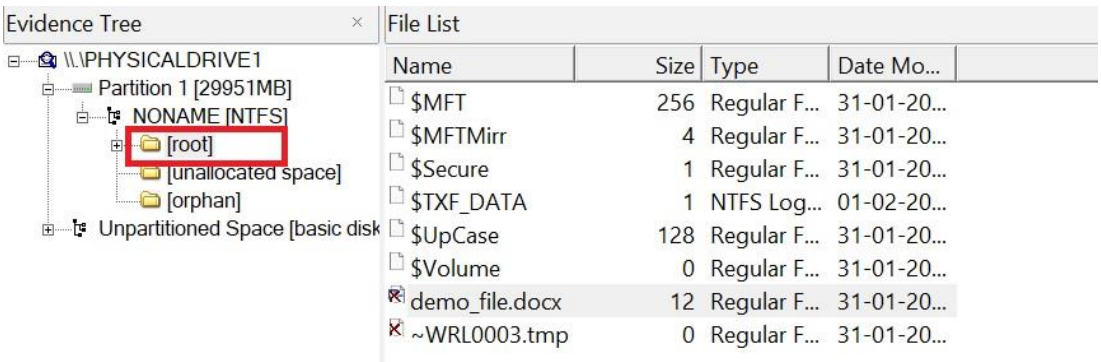
4)In the "Select Source" window, select the option to "Physical Drive"



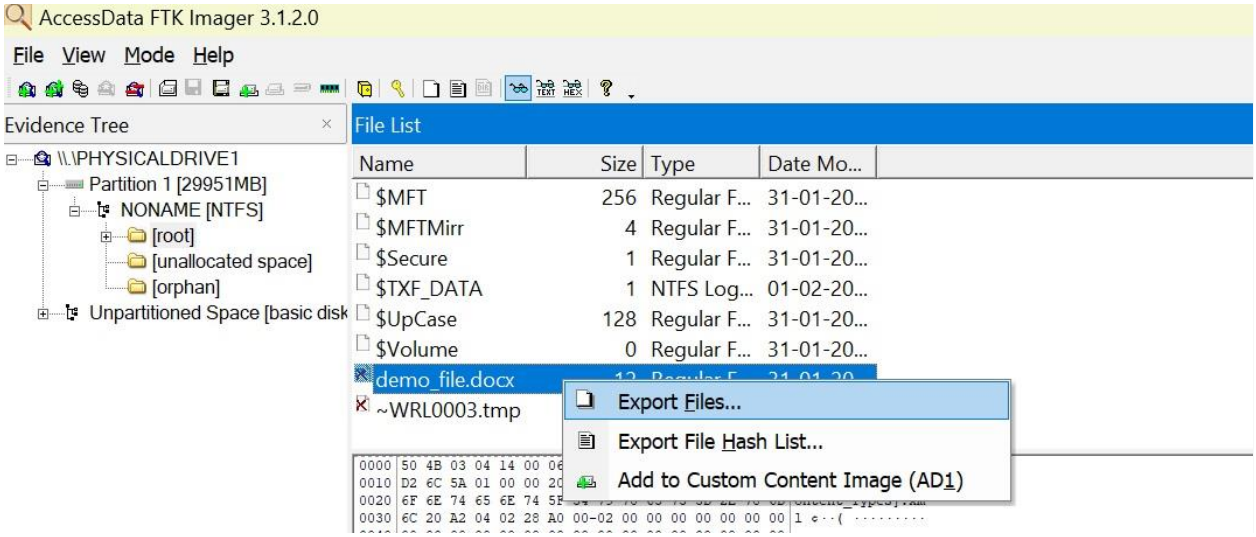
5)Then select the storage device that you want to image from the list of available devices and click Finish button.



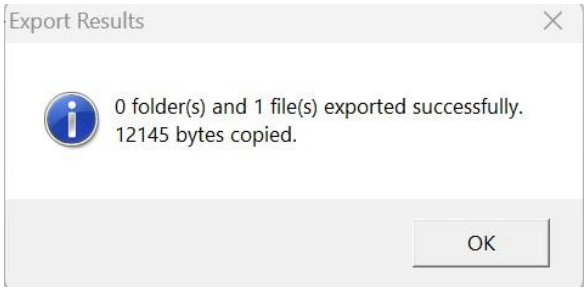
6)Now Expand Evidence Tree and select "root"



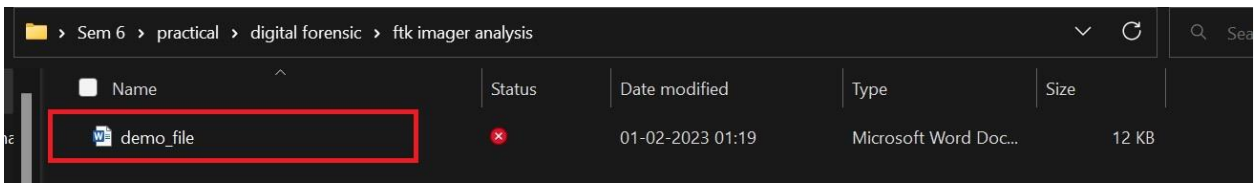
7)Now,select the file which you want to recover then right click on it and select "export files" and export this file on your desired location in my case it demo_file.docx which I have deleted.



8)After the file is exported it will show a pop up window of file extracted successfully and stored at destination location



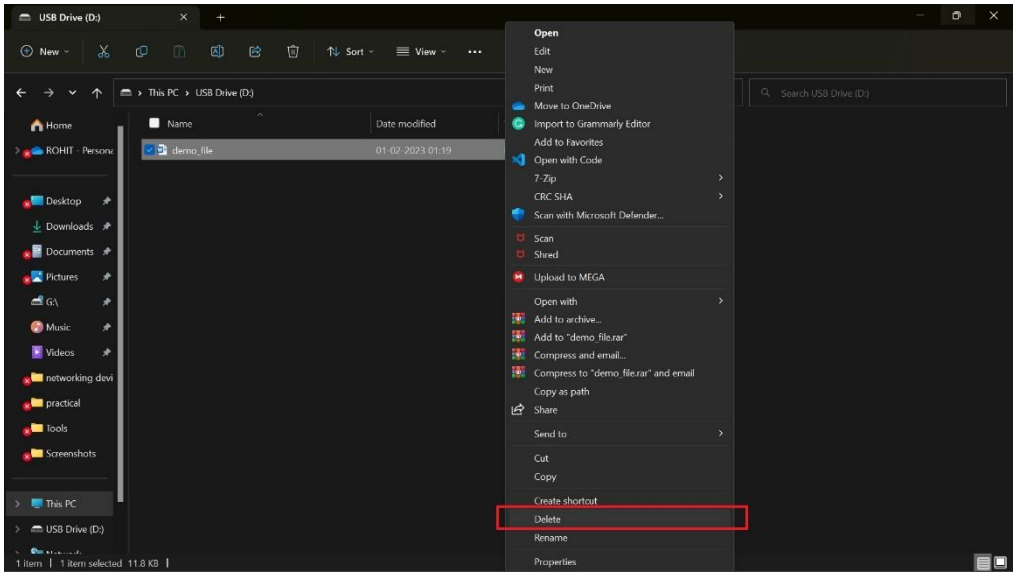
As you can see the demo file which I have deleted has been recovered

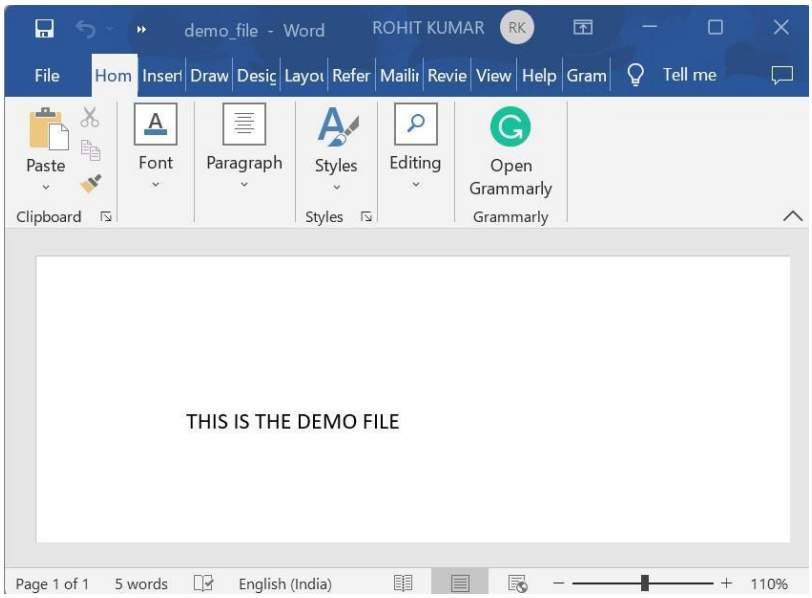


Practical - 4

Q). To recover a deleted file using Forensic Tools (ProDiscover)

THIS IS THE DEMO FILE WHICH I AM GOING TO DELETE AND RECOVERED IT USING ProDiscover





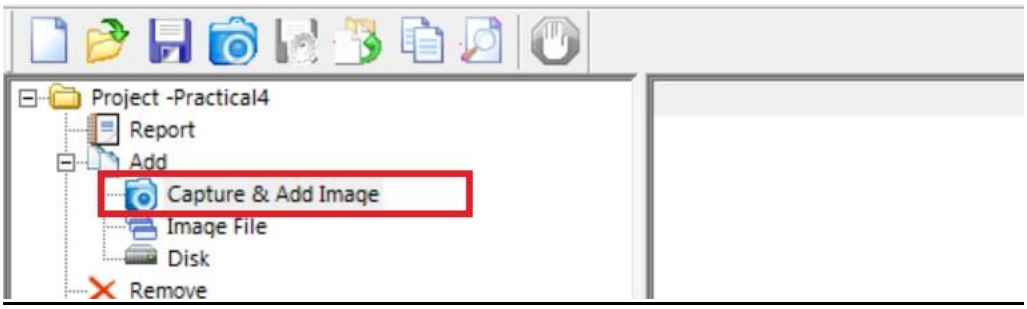
PRODISCOVER:

Procedure:

1.) Connect the storage device to the computer where ProDiscover is installed.

2.) Open ProDiscover Basic software and Enter Project Name,Number and description of it and then click on the “open” button.

3) Click on the " Capture & Add Image " button located on the main toolbar.



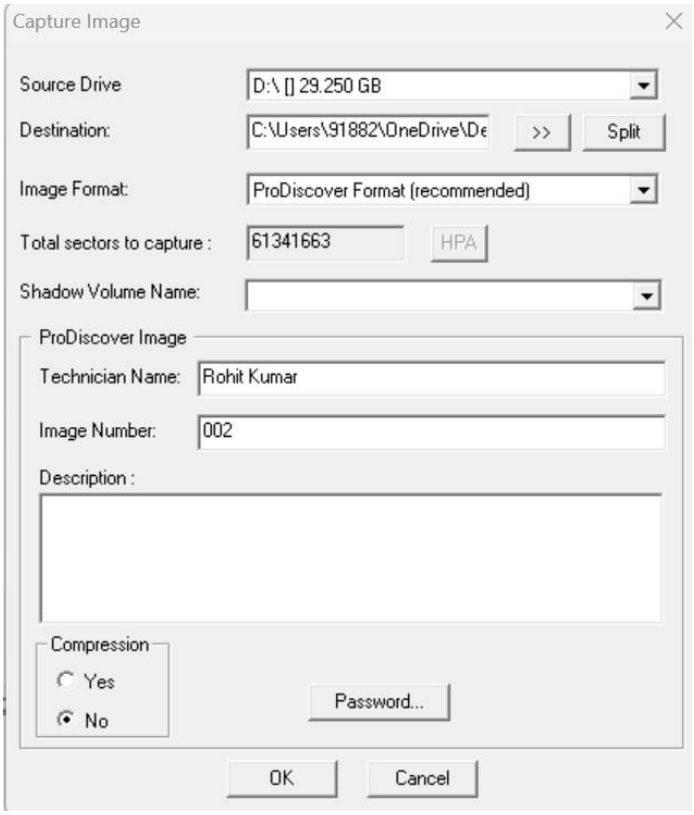
4) In the "Capture Image" window,

->Select the storage device that you want to image from the list of available devices.

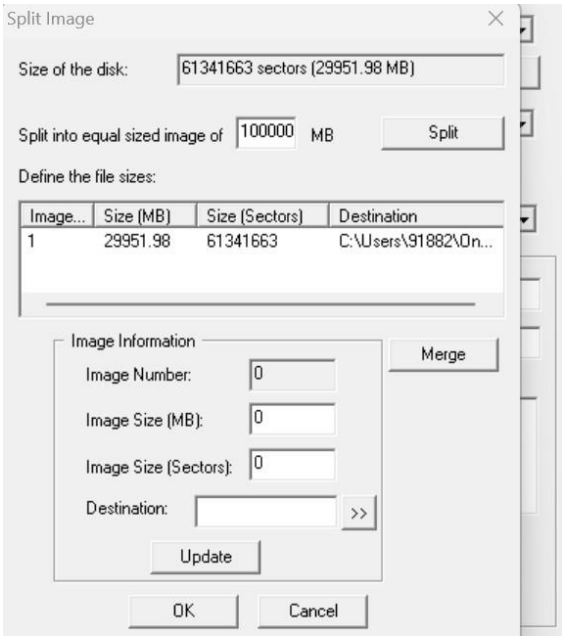
->Select the destination folder where you want to save the image file, and enter a name for the image file.

->Enter the Technician Name,Image Number and description

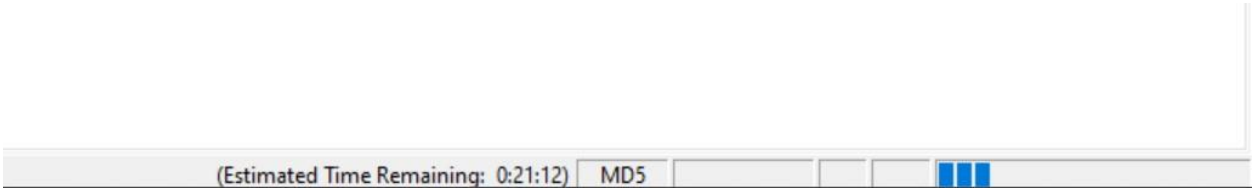
->Click the "ok" button to begin the imaging process.



Note:- if your storage device is bigger in size then you can break the large image file of it into smaller equal chunks by clicking "split" button and selecting the size for smaller size chunks



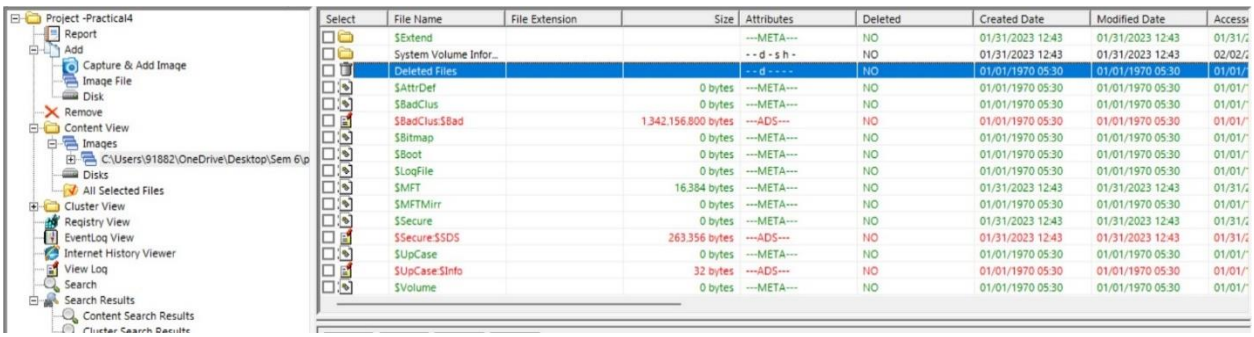
5) Monitor the Progress of the Imaging Process.When the imaging starts,a progressbar will be displayed in the bottom right corner.



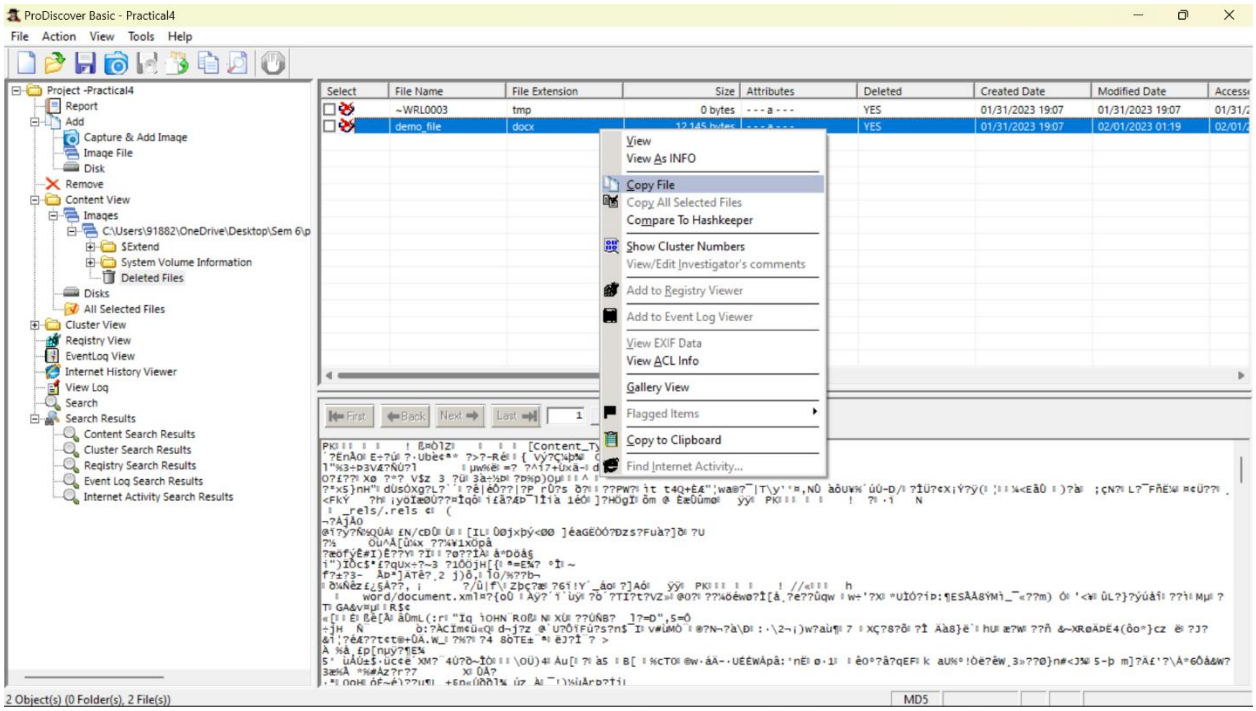
6) Once the imaging process is complete, it will show a pop up window of “image Capture Completed”.

7)The image file is saved in the destination folder that you specified.

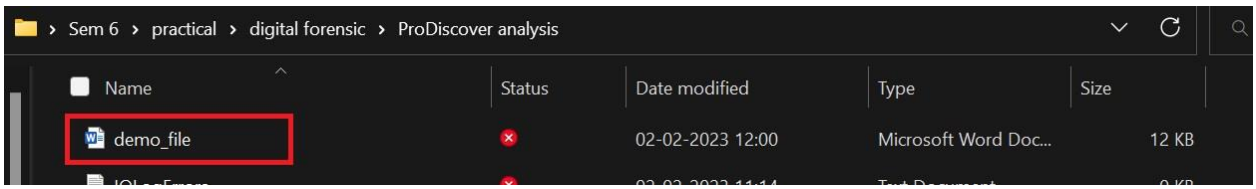
Now, you can open your image file by clicking “Content View”->”Images”->then select the image file where you have stored and image will be open in the prodiscover software for analysis purpose then select the "Deleted Files" which is shown below in the screenshot



8)The red cross marks states that this files are deleted. Now, select any file which you want to recover right click on it and select copy file then select the destination where you want to recover the file.



9)The Deleted File (demo_file.docx) has been recover to the location specified by the user



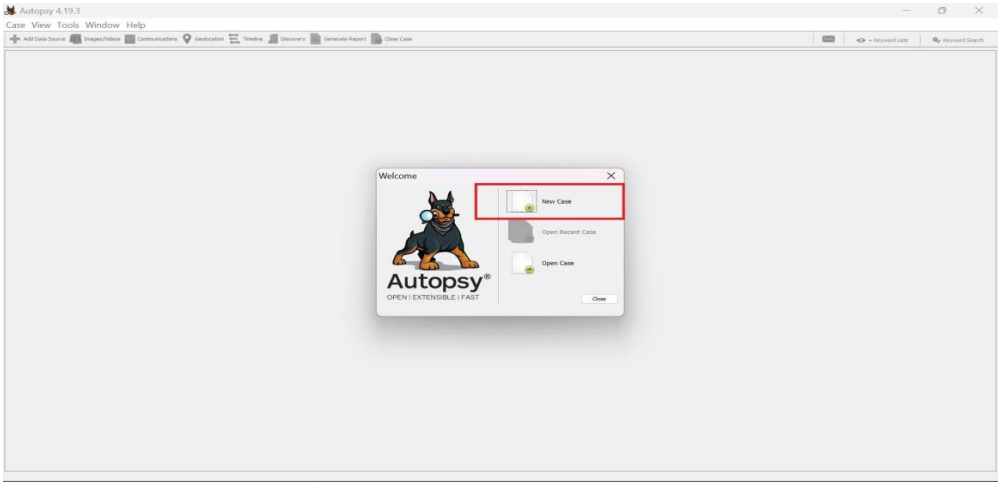
Practical - 5

Q). To Collect the Email Evidence from a Suspected Drive or Image.

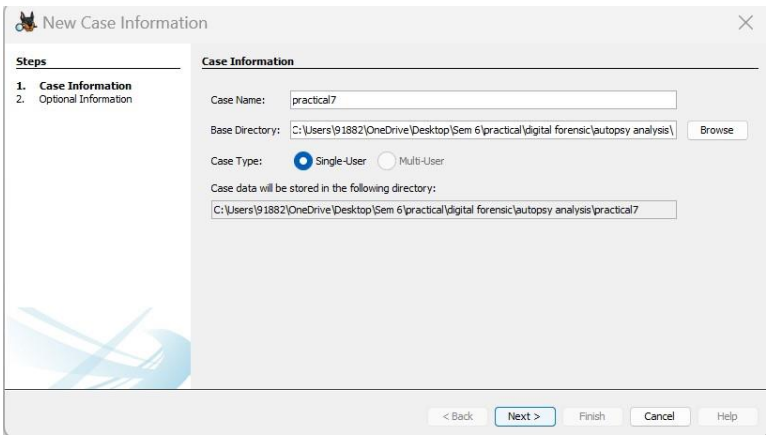
AUTOPSY:

Procedure:

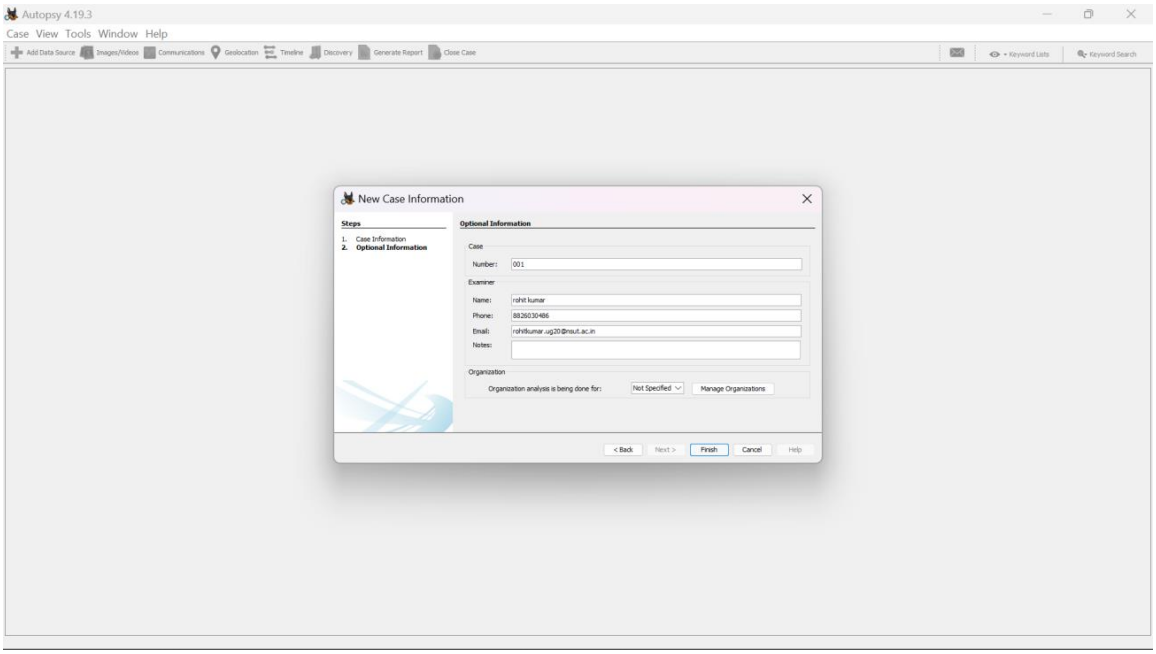
1.) Launch Autopsy, and click on the "New Case" button.



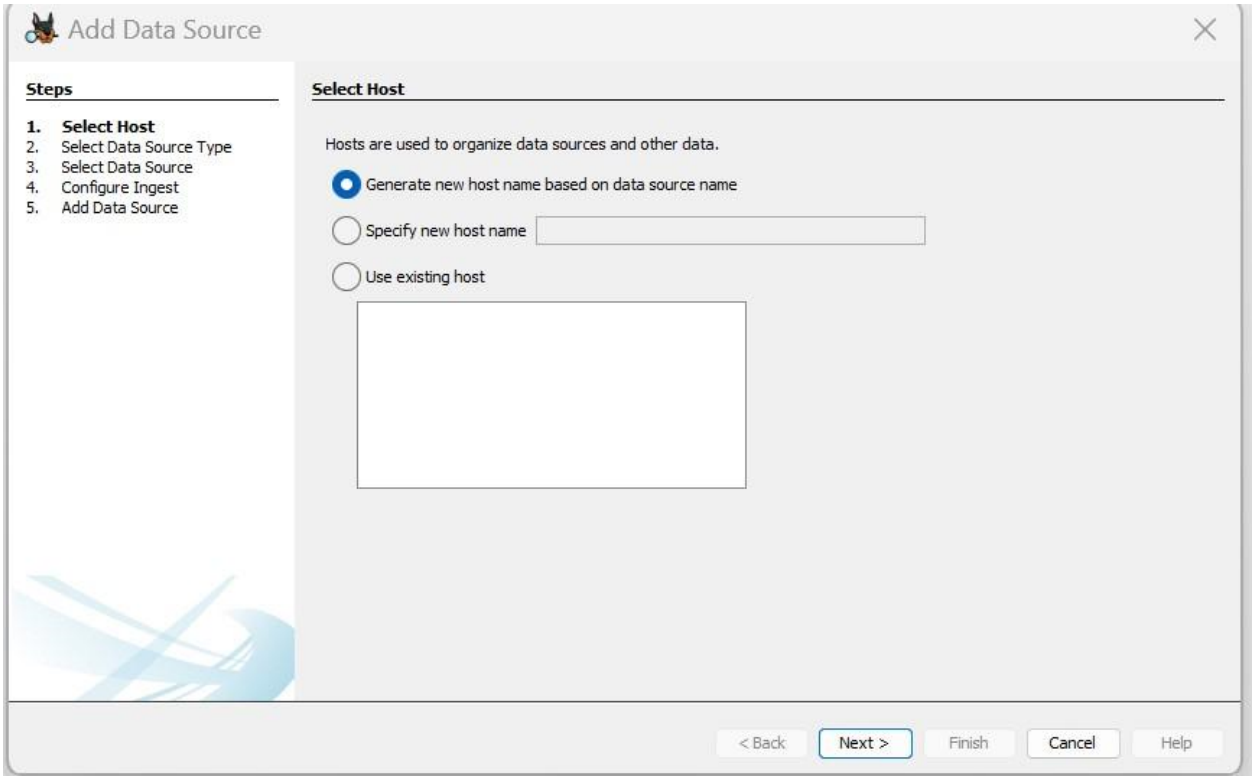
2) Enter Case Name and Base Directory where you want to store your Forensic image then click “Next”.



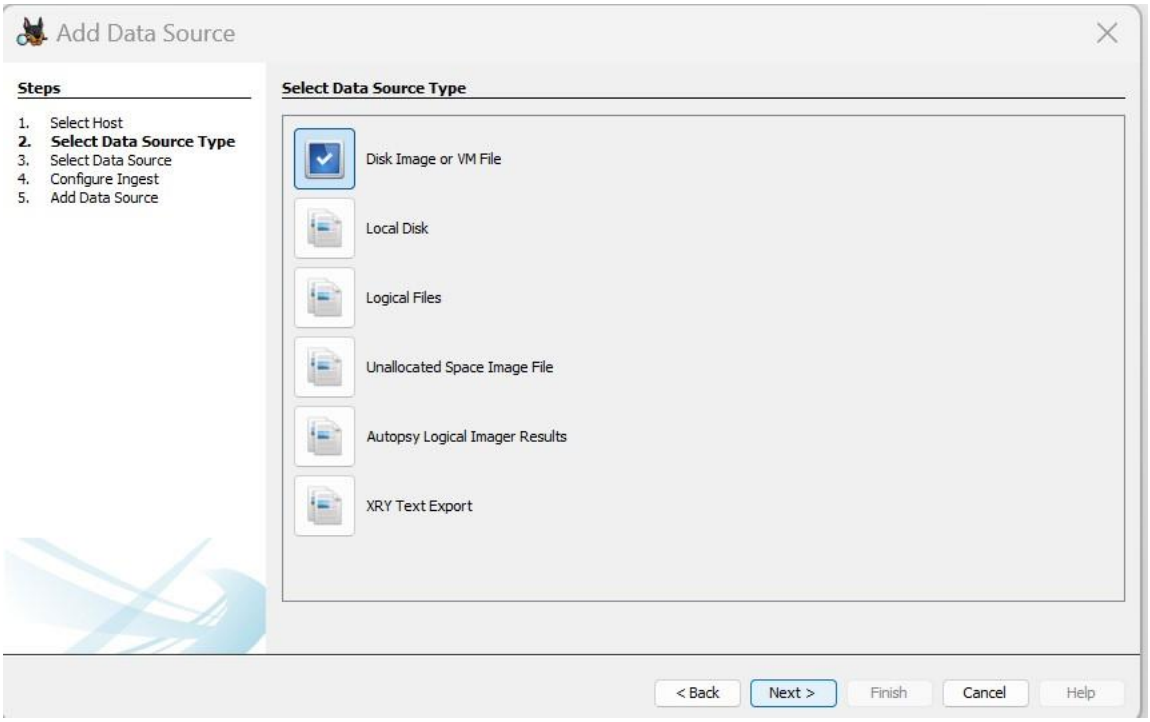
3) Now, Enter case number,and all other information and then click “Finish” Button



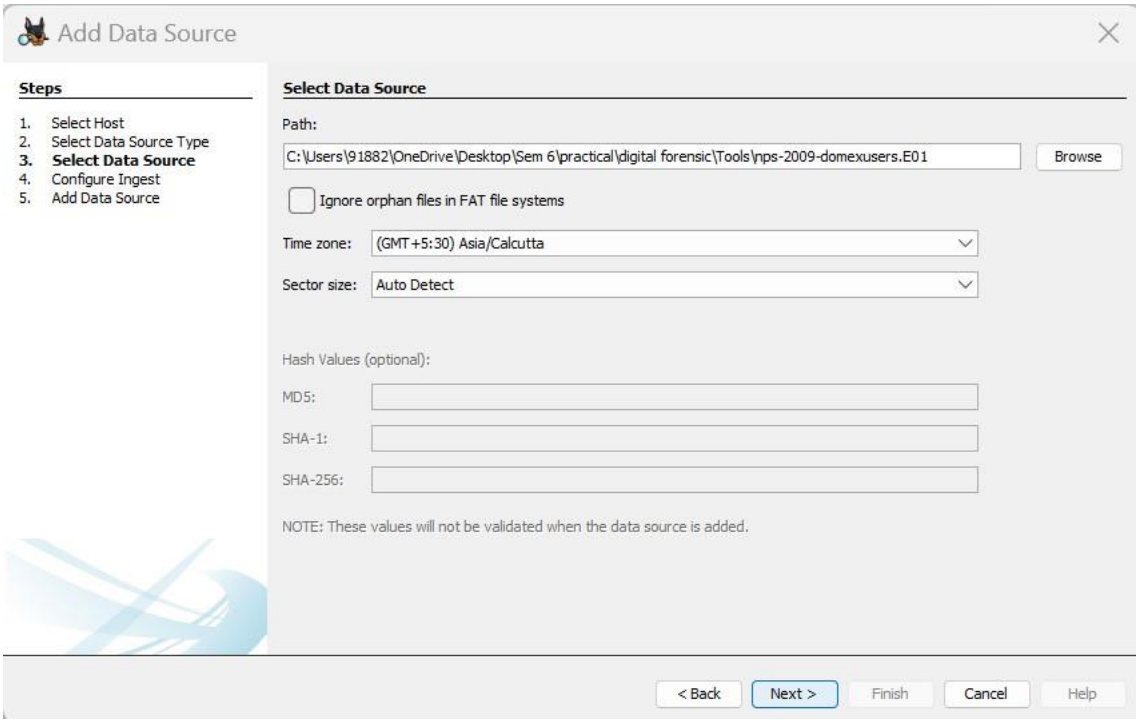
4)Then, in add data source window , select first option which is “Generate new host name”



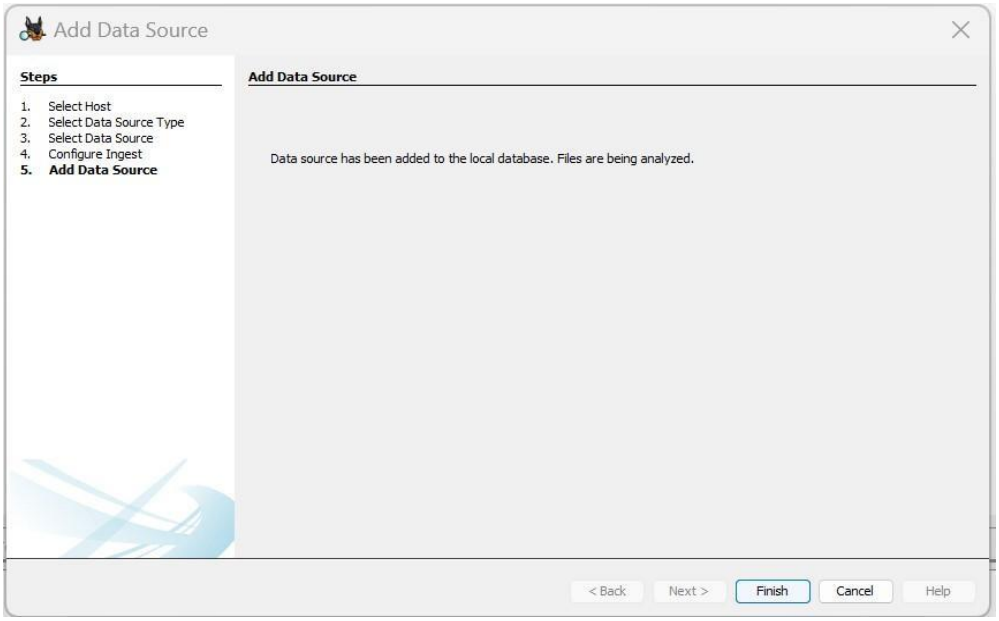
5)Then, Select “Disk Image or Vm File ” option. To analyze the image file of storage device



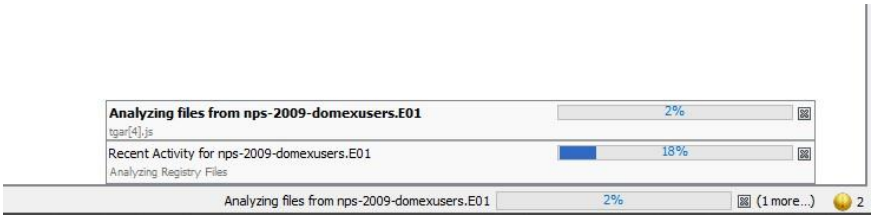
6)Now, in path section Enter the location of your image file then click Next button



7)Now, it will show “Data source has been added” . click on finish button



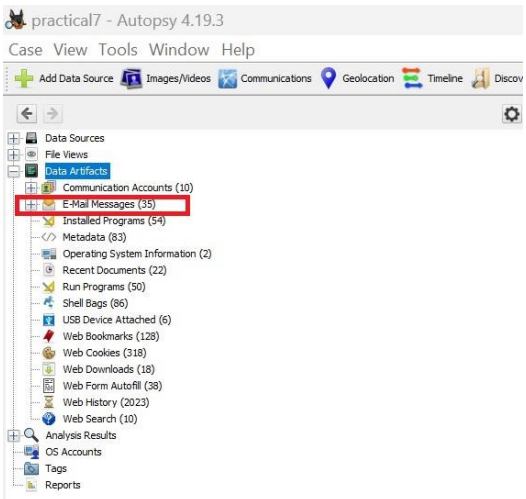
8)Then, it will start analyzing image file and progress of it will be shown in the bottom left corner of the window.



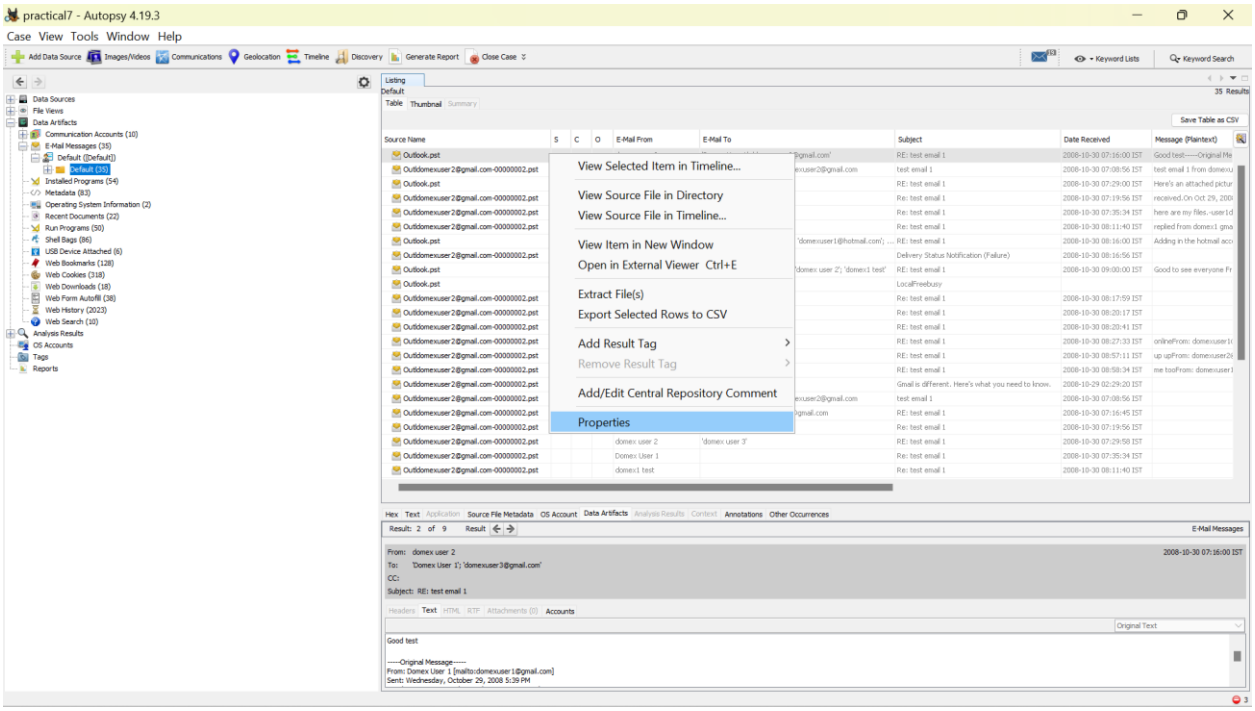
9)After the progress completed ,the image file will automatically be open in the autopsy software where you can analyzed the image file.

Now, On Tree View ,Under the "Data Artifacts " node , You can see "Email Message "

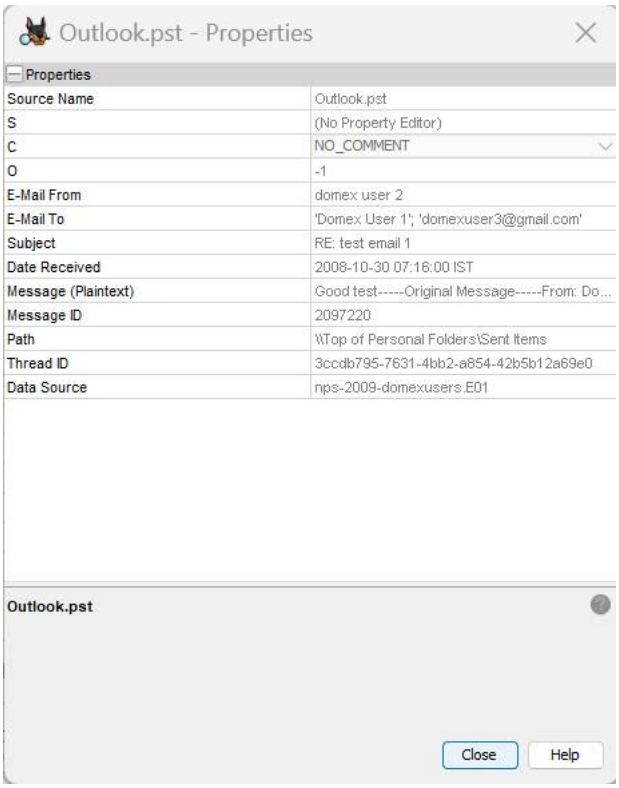
Section click on it.



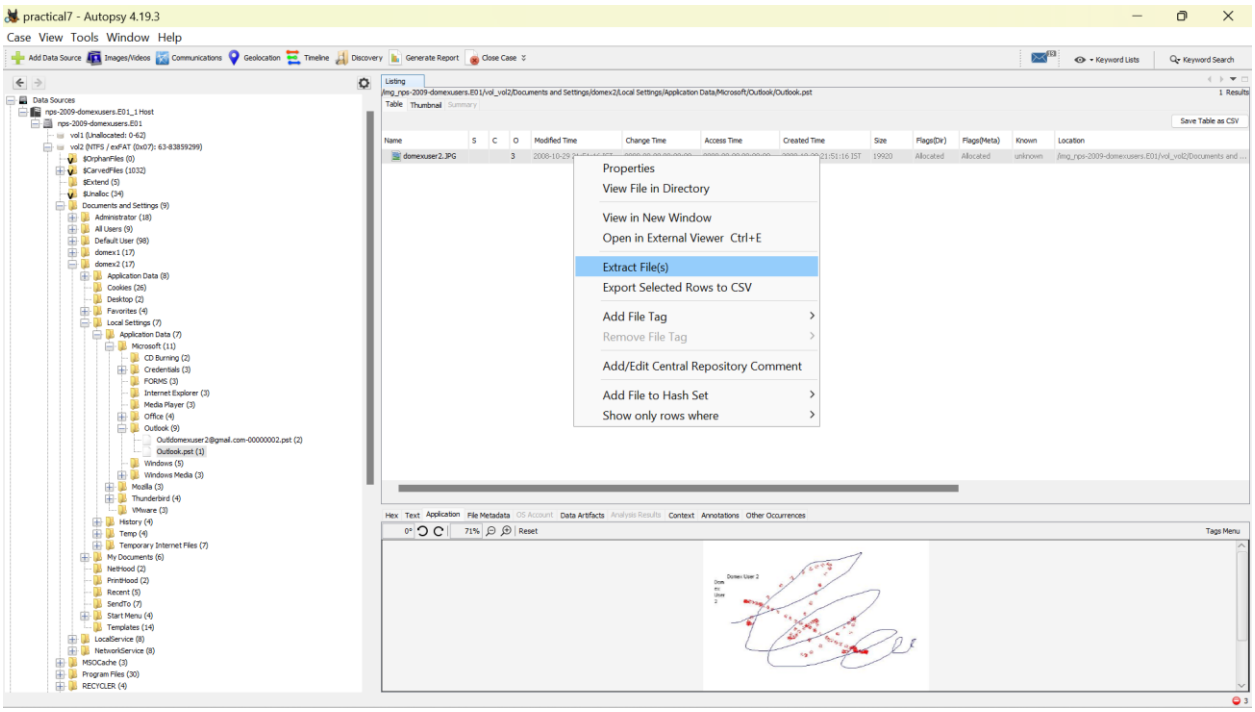
10) Then it will show us all the emails evidence. Now, click on any email then select "Properties" button.



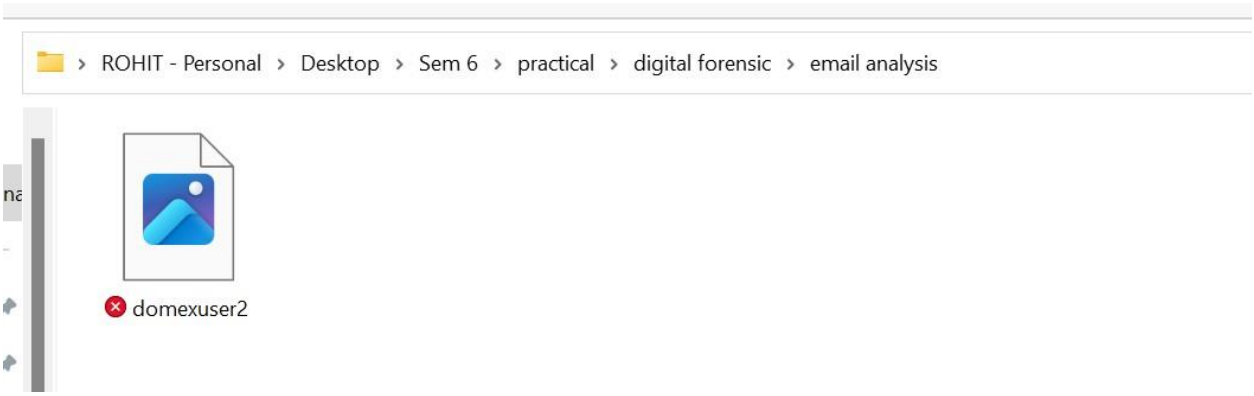
11) then a properties window will be opened. It contains all the information like sender,receipient ,subject and message of the mail.



12)You can also download the content of the mail by clicking on that mail then select that content and click on Extract file then save the content to the desired location . In my case the content is jpg file but the content can be anything like pdf , word file etc.



As you can see the content of the email has been store to the location defined by the user



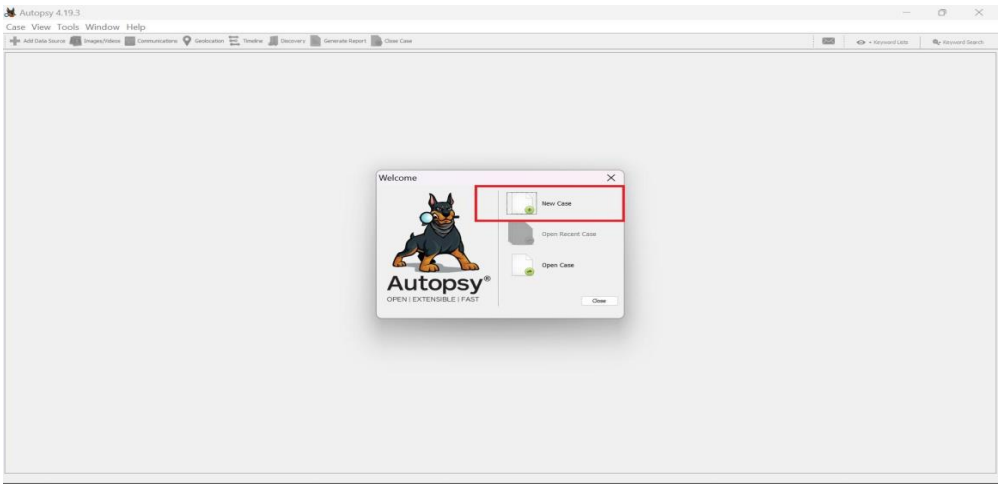
Practical - 6

Q). How to Extract Browsing Artifacts (Using Autopsy)

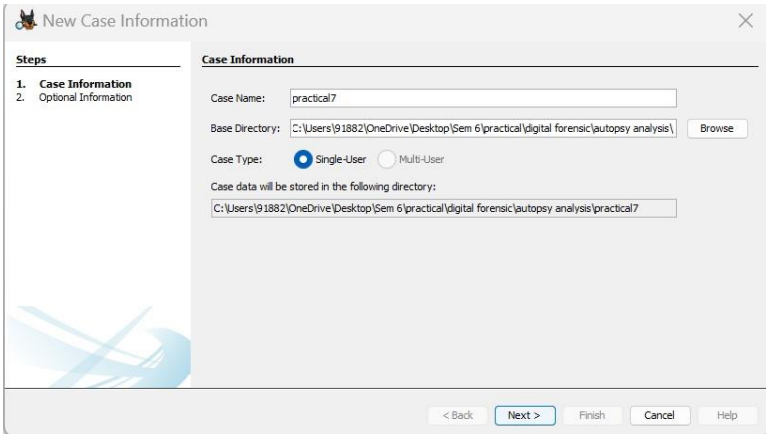
AUTOPSY:

Procedure:

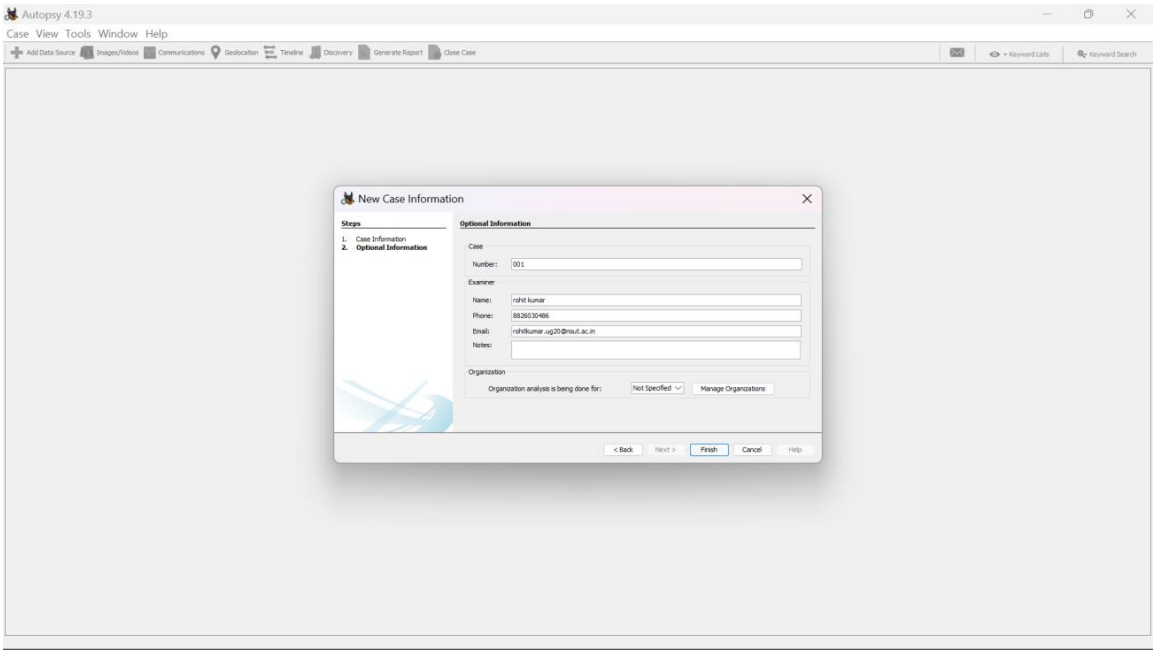
1.) Launch Autopsy, and click on the "New Case" button.



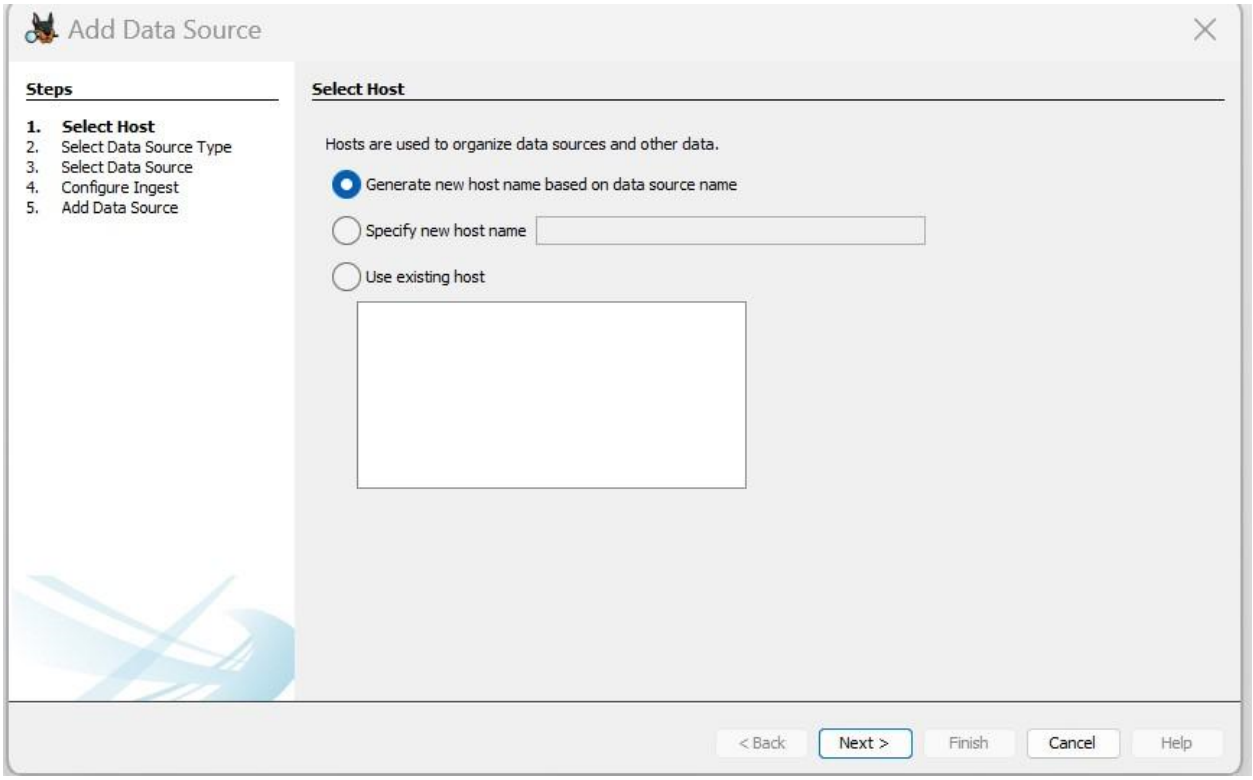
2) Enter Case Name and Base Directory where you want to store your Forensic image then click “Next”.



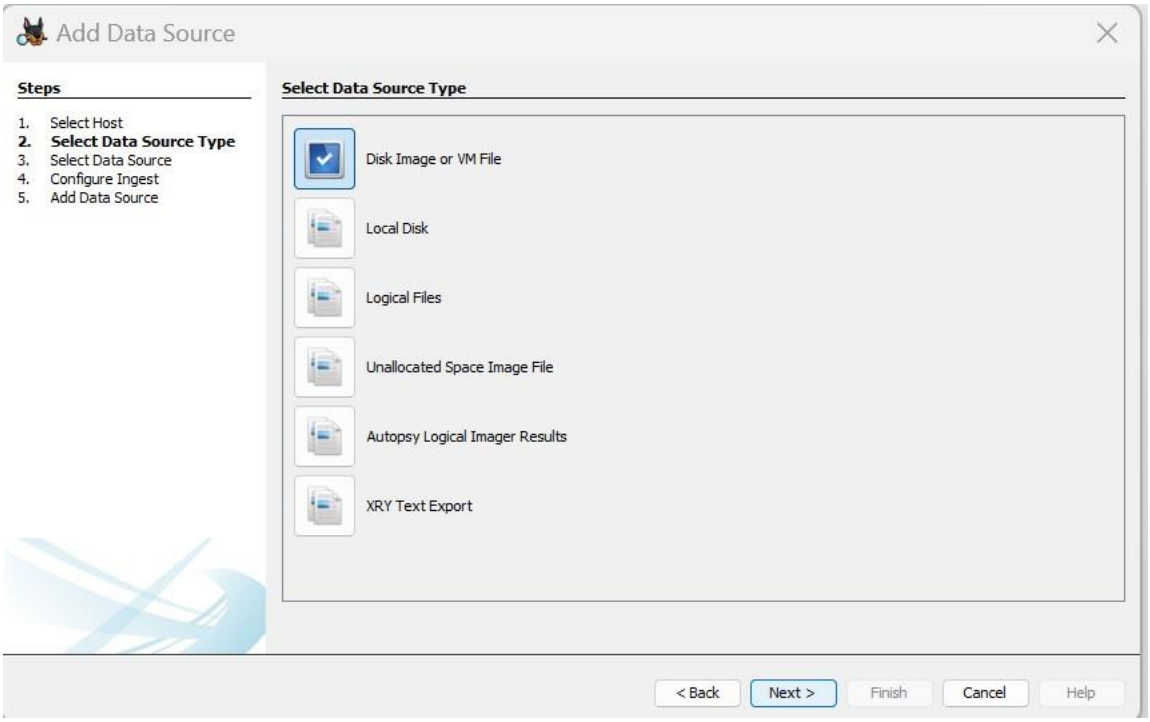
3) Now, Enter case number,and all other information and then click “Finish” Button



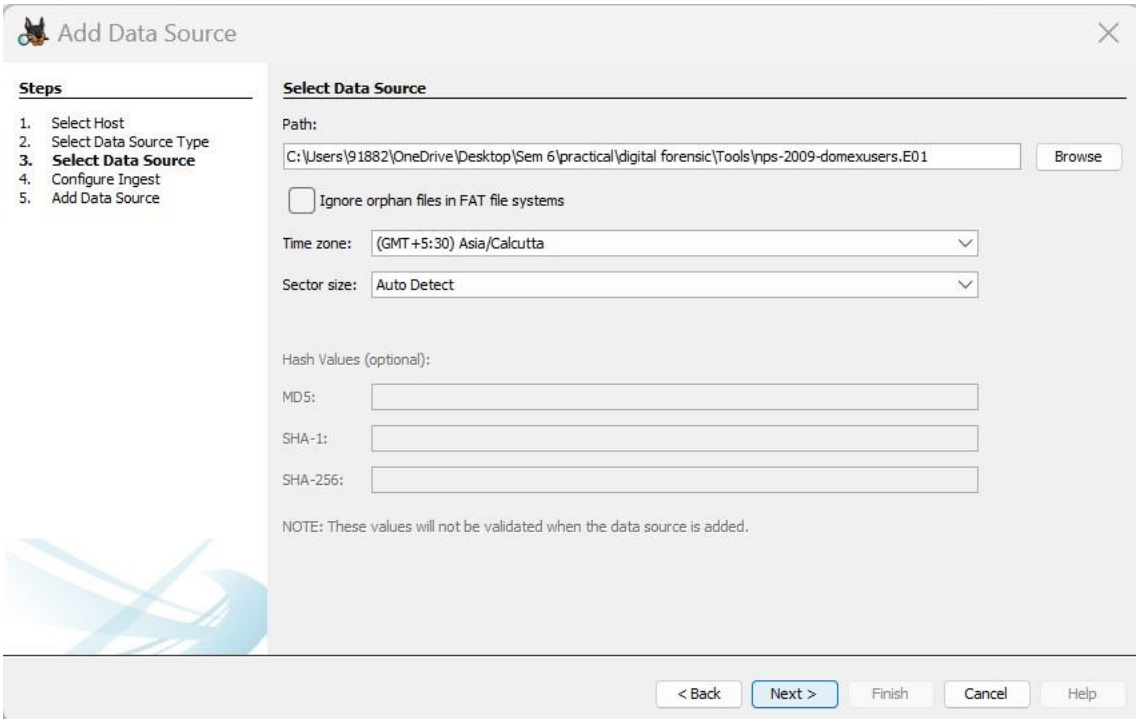
4)Then, in add data source window , select first option which is “Generate new host name”



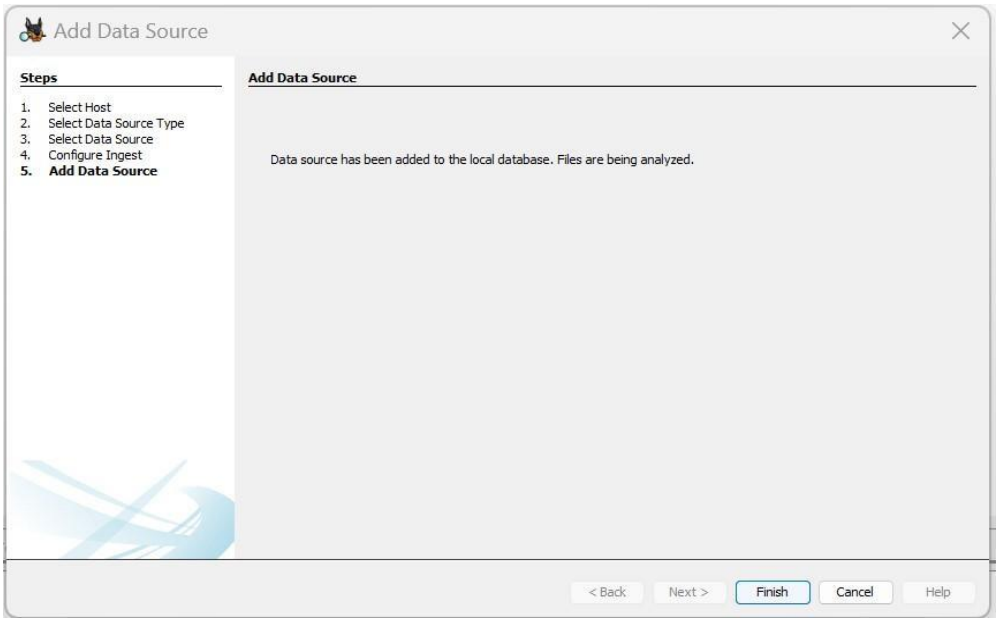
5)Then, Select “Disk Image or Vm File ” option. To analyze the image file of storage device



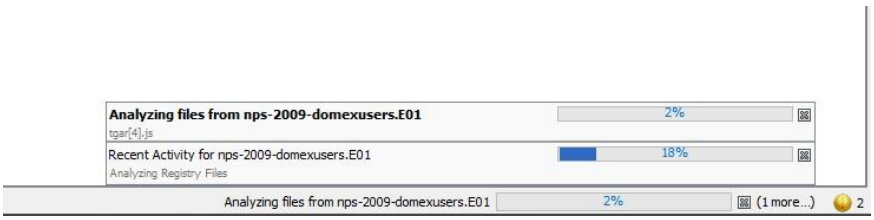
6)Now, in path section Enter the location of your image file then click Next button



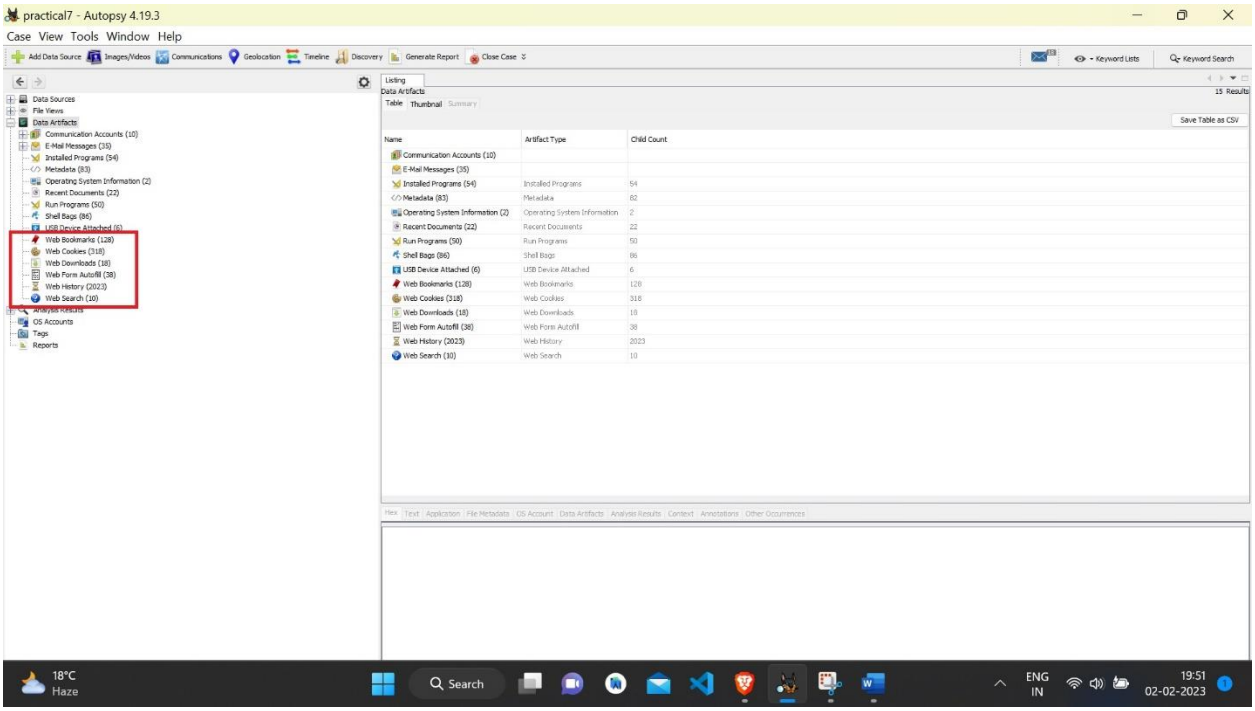
7)Now, it will show “Data source has been added” . click on finish button



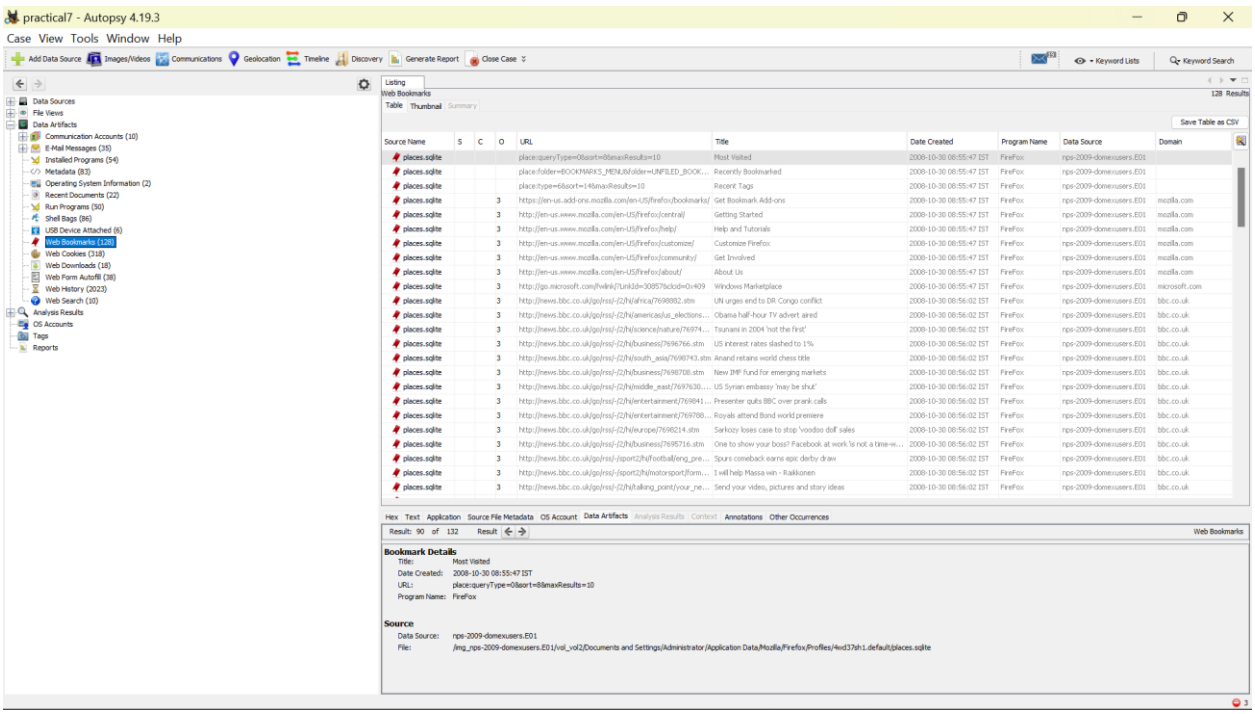
8)Then, it will start analyzing image file and progress of it will be shown in the bottom left corner of the window.



9)After the progress completed ,the image file will automatically be open in the autopsy software where you can analyzed the image file.Now, On Tree View ,Under the "Data Artifacts " node , You can see all the browsing aritfacts like web Bookmarks , History , downlaods and web search.

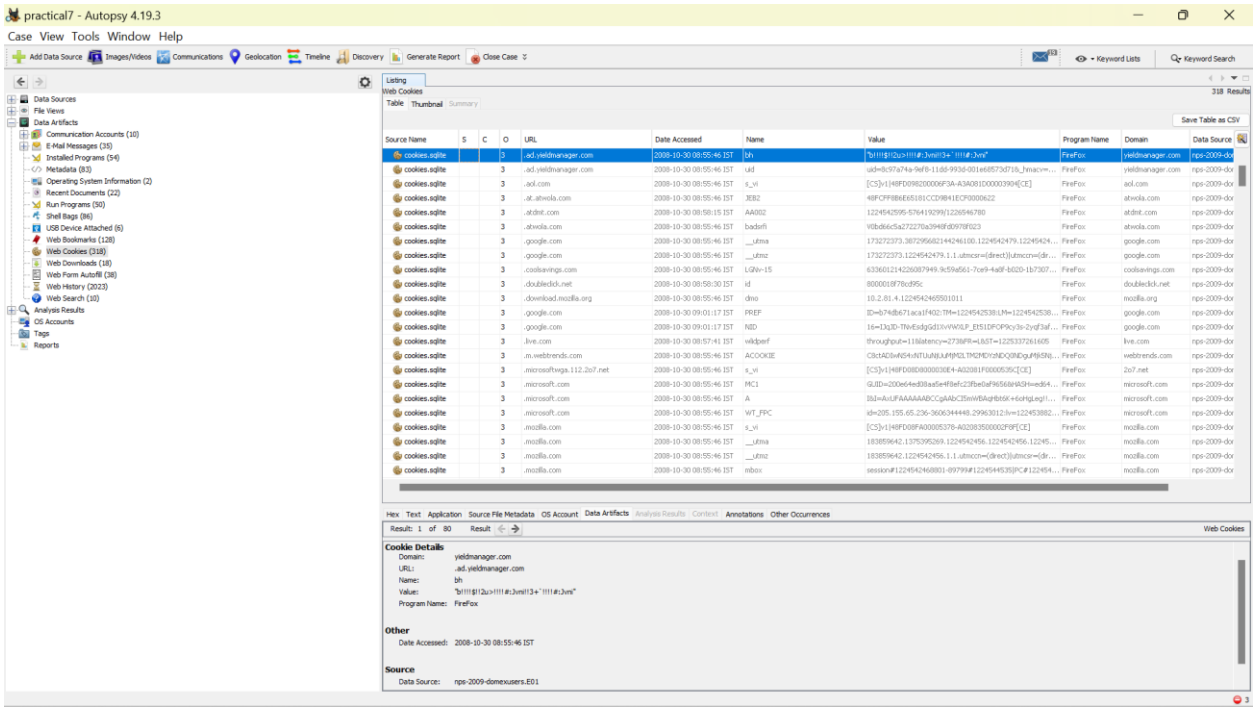


On clicking "Web Bookmarks" , it will show us all the bookmarks saved by the user along with their timestamp and url

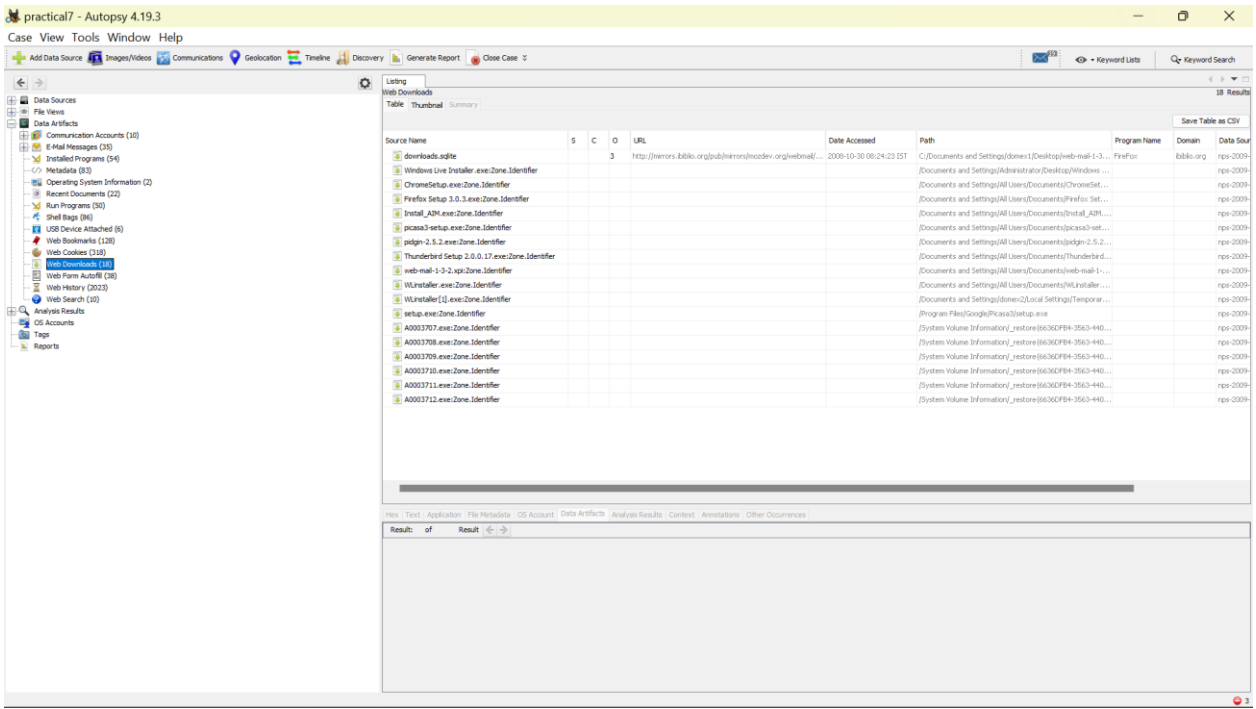


On clicking "Web Cookies " it will show us all the different websites user have visited.

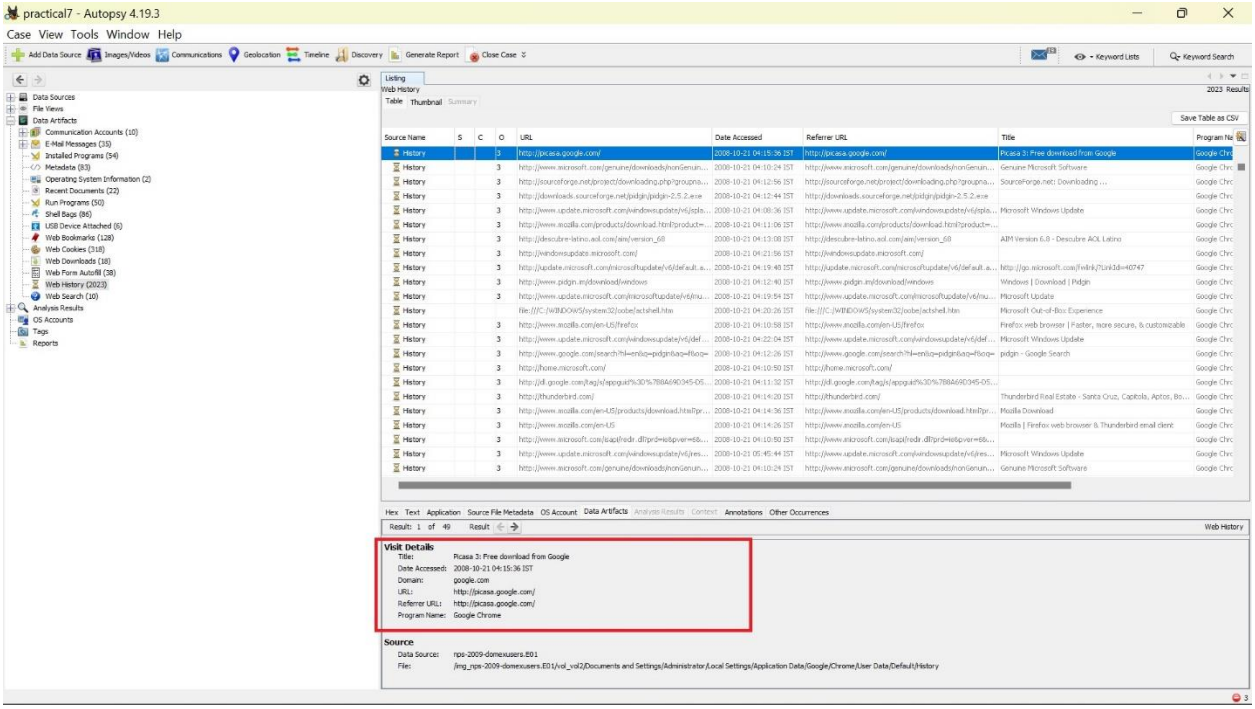
Cookies are used to tell the server that the user have returned to a particular website. And it also stores some information for quickly authentication the user.



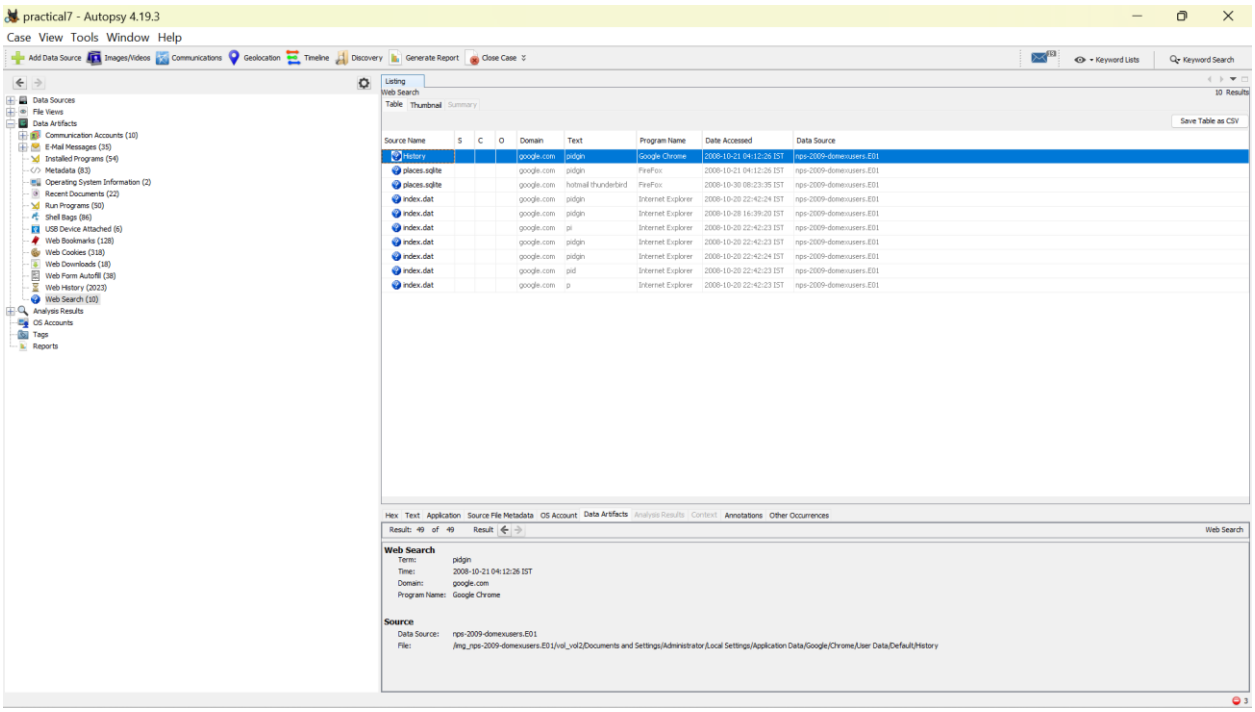
If user have downloaded something then the record of it will be stored in web downlaods section as in my case it is showing 18 downloads



In web History section , it will show the history of all the websites visited by the user along with their timestamp and their url and when you click on it ,it will show the visit details



In web search section , it shows us the different text search by the users.



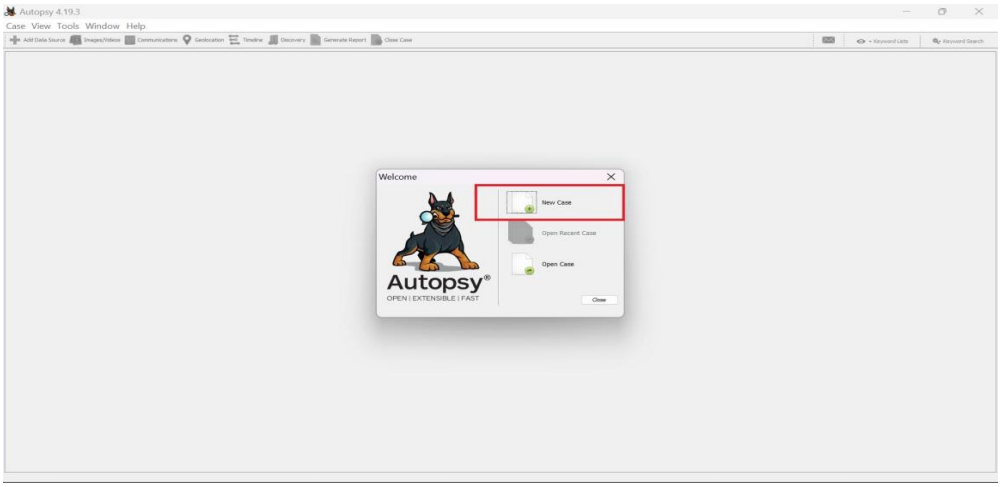
Practical - 7

Q). Find Last Connected USB on your system - USB Forensics (Using Autopsy)

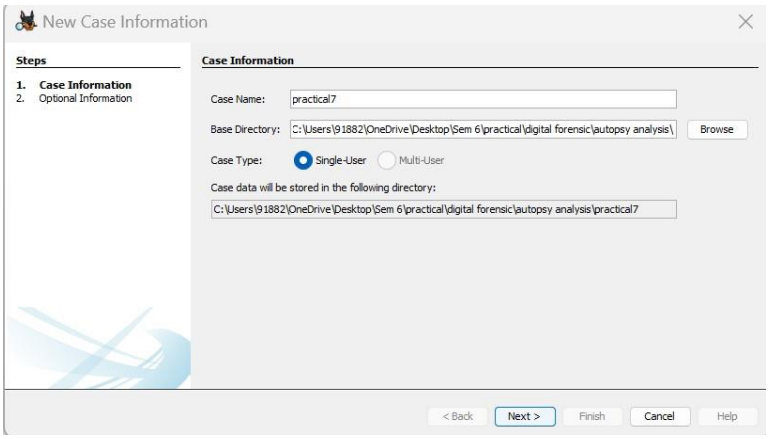
AUTOPSY:

Procedure:

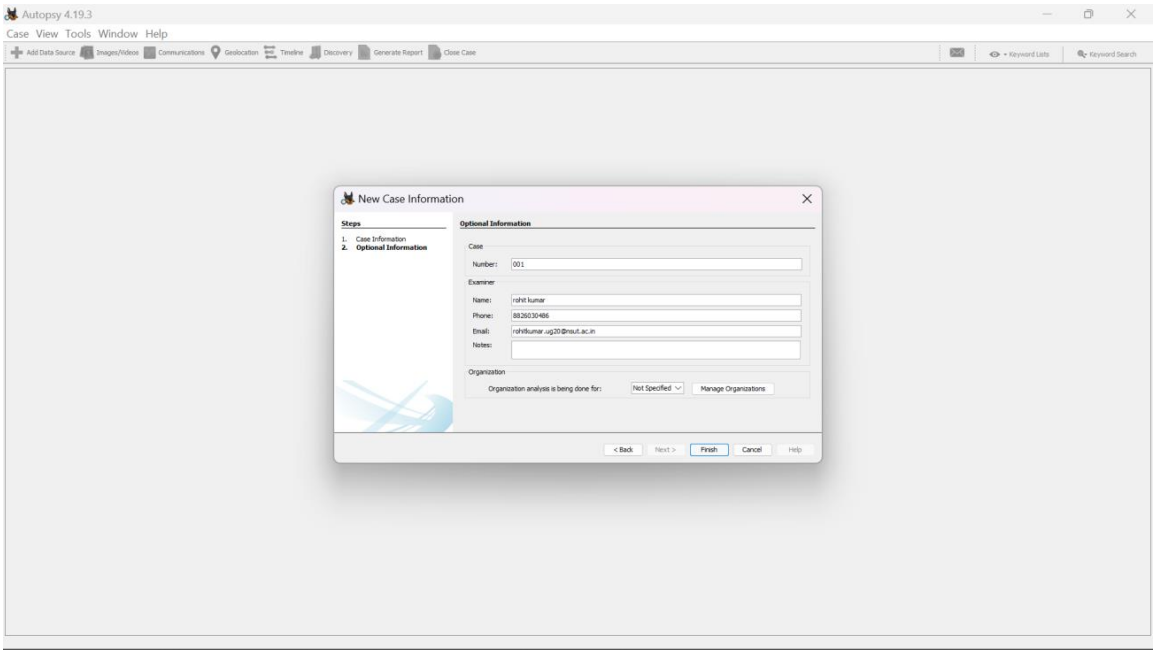
1.) Launch Autopsy, and click on the "New Case" button.



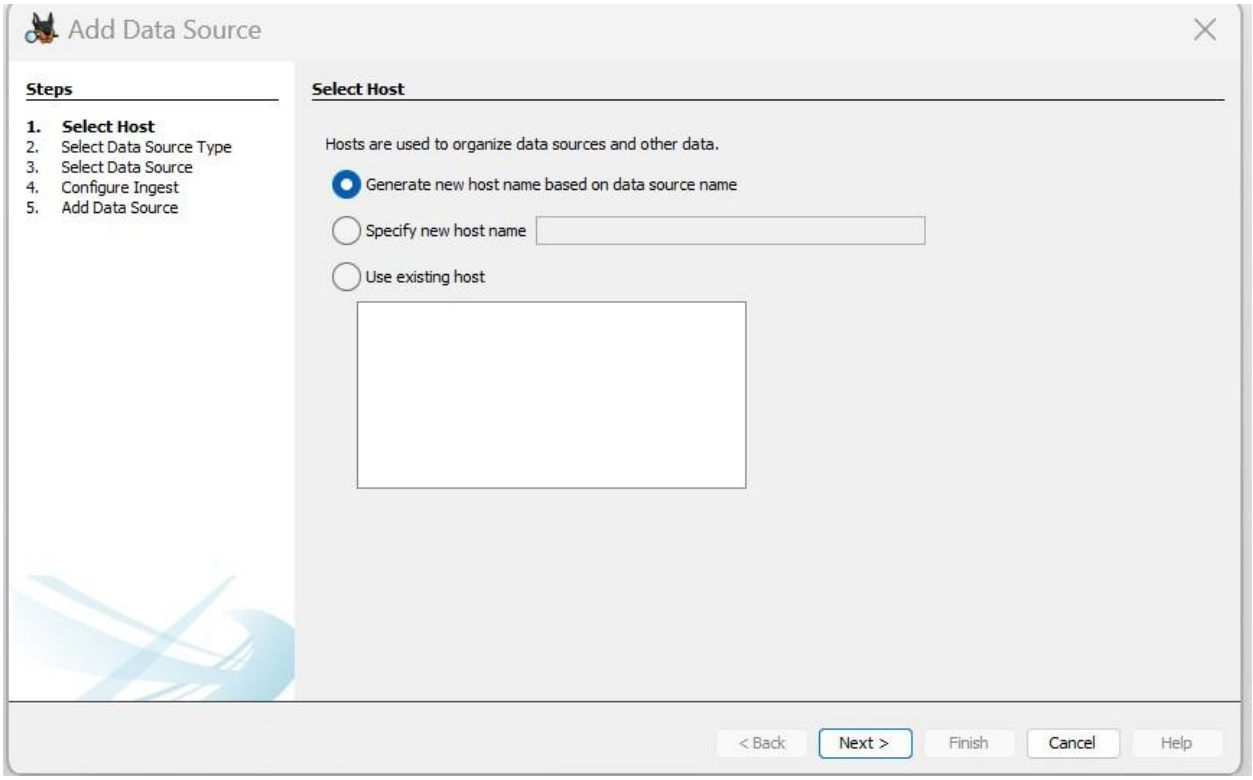
2) Enter Case Name and Base Directory where you want to store your Forensic image then click “Next”.



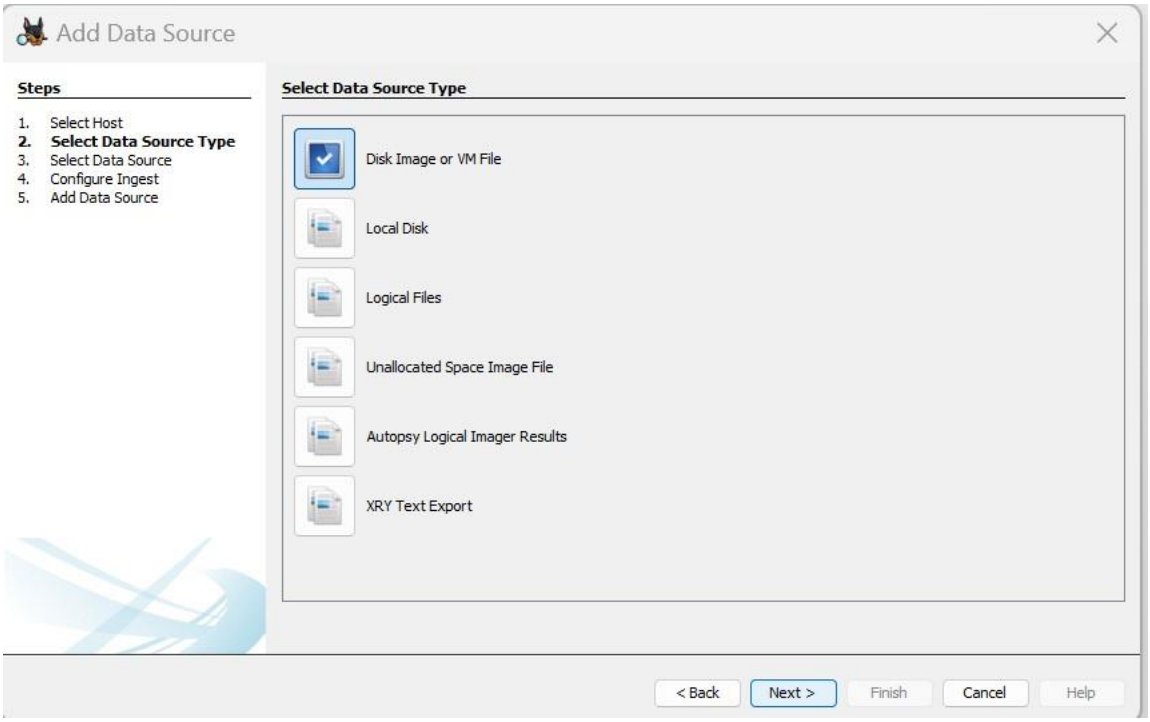
3) Now, Enter case number,and all other information and then click “Finish” Button



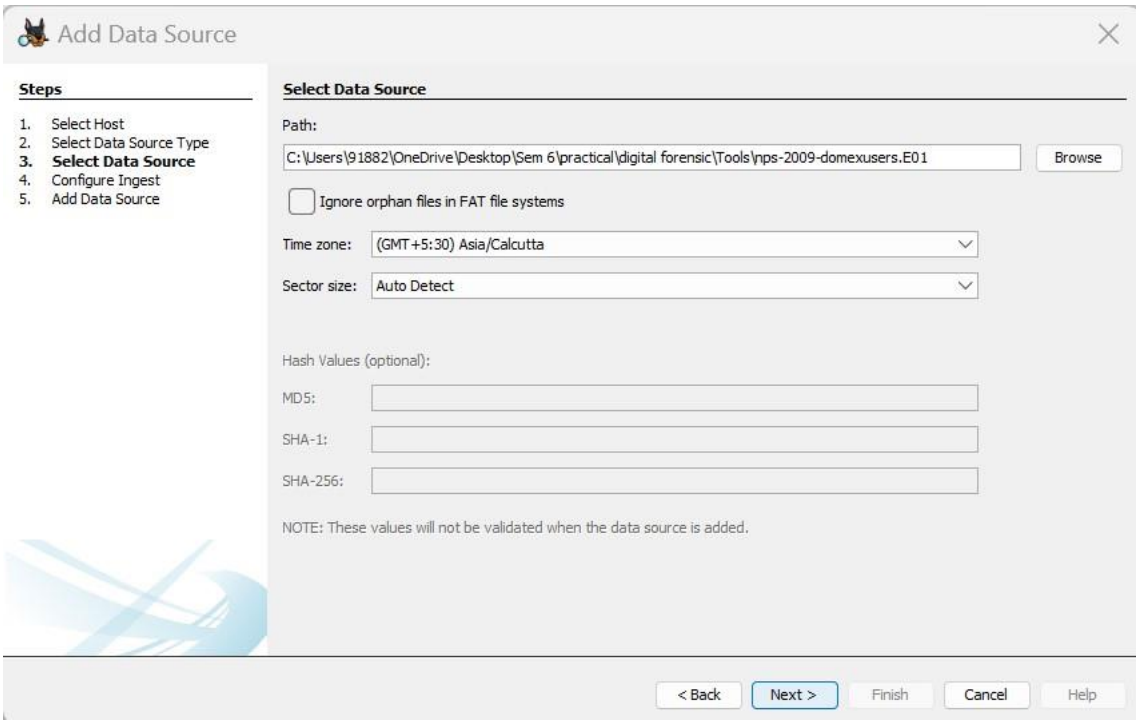
4)Then, in add data source window , select first option which is “Generate new host name”



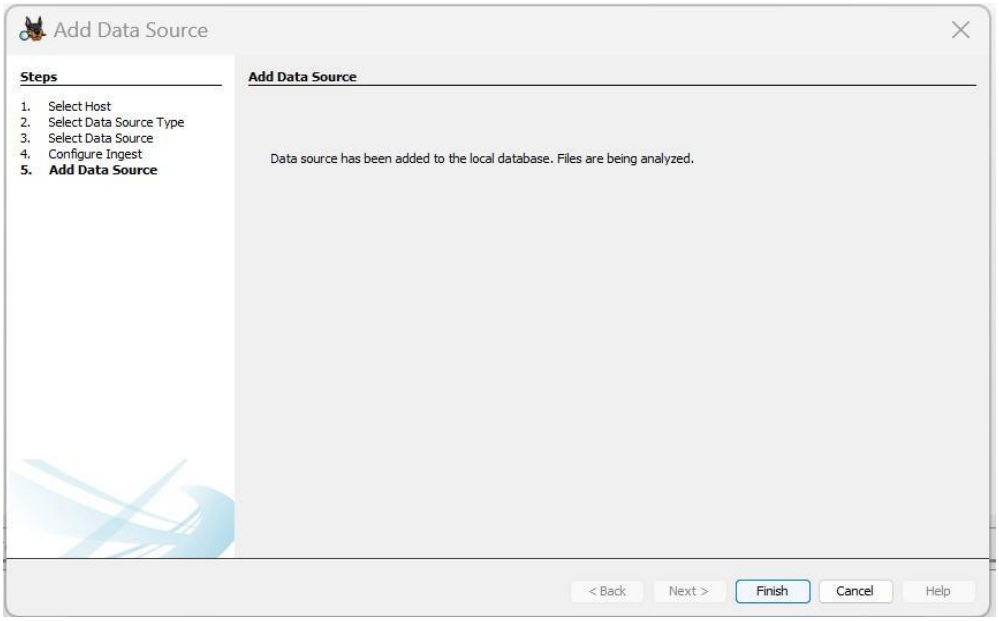
5)Then, Select “Disk Image or Vm File ” option. To analyze the image file of storage device



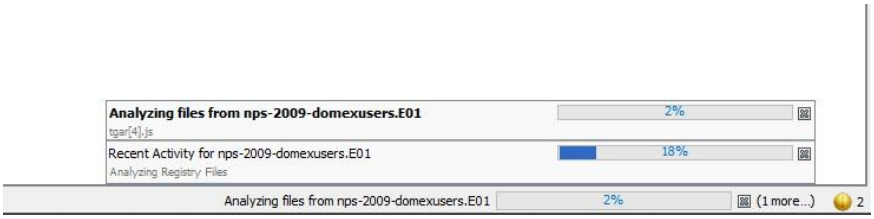
6)Now, in path section Enter the location of your image file then click Next button



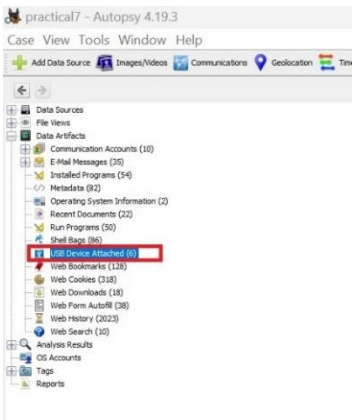
7)Now, it will show “Data source has been added” . click on finish button



8)Then, it will start analyzing image file and progress of it will be shown in the bottom left corner of the window.



9)After the progress completed ,the image file will automatically be open in the autopsy software where you can analyzed the image file.Now, On Tree View ,Under the "Data Artifacts " node , navigate to "USB device attached" to find all the devices connected to the system



10)On clicking , it will show us all the usb device attached to the system along with there timestamp ,device model and device id.

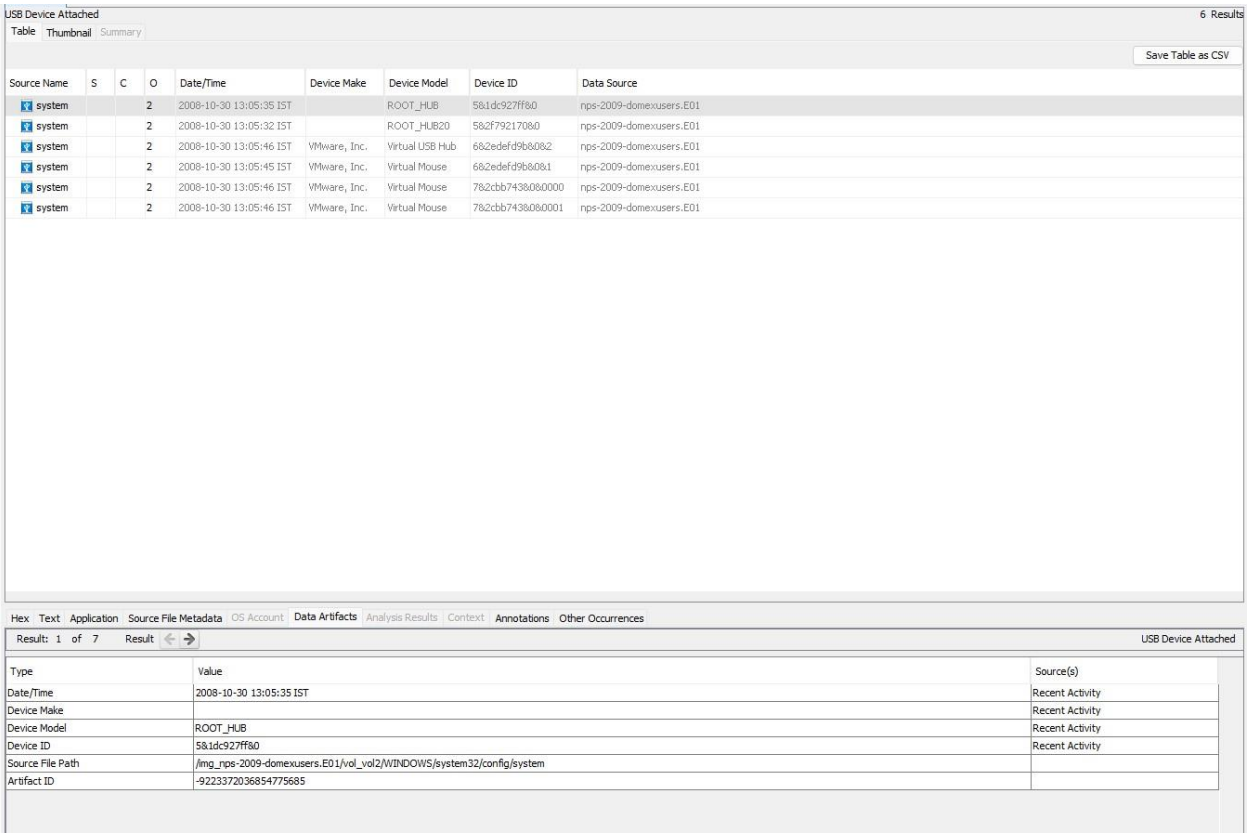
Listing

USB Device Attached

Table | Thumbnail | Summary

Source Name	S	C	O	Date/Time	Device Make	Device Model	Device ID	Data Source
system			2	2008-10-30 13:05:35 IST		ROOT_HUB	5&1dc927ff&0	nps-2009-domexusers.E01
system			2	2008-10-30 13:05:32 IST		ROOT_HUB20	5&2f792170&0	nps-2009-domexusers.E01
system			2	2008-10-30 13:05:46 IST	VMware, Inc.	Virtual USB Hub	6&2edefd9b&0&2	nps-2009-domexusers.E01
system			2	2008-10-30 13:05:45 IST	VMware, Inc.	Virtual Mouse	6&2edefd9b&0&1	nps-2009-domexusers.E01
system			2	2008-10-30 13:05:46 IST	VMware, Inc.	Virtual Mouse	7&2cbb7438&0&0000	nps-2009-domexusers.E01
system			2	2008-10-30 13:05:46 IST	VMware, Inc.	Virtual Mouse	7&2cbb7438&0&0001	nps-2009-domexusers.E01

11)On clicking any usb device it will show all the information about an usb device along with date/time when it was last connected



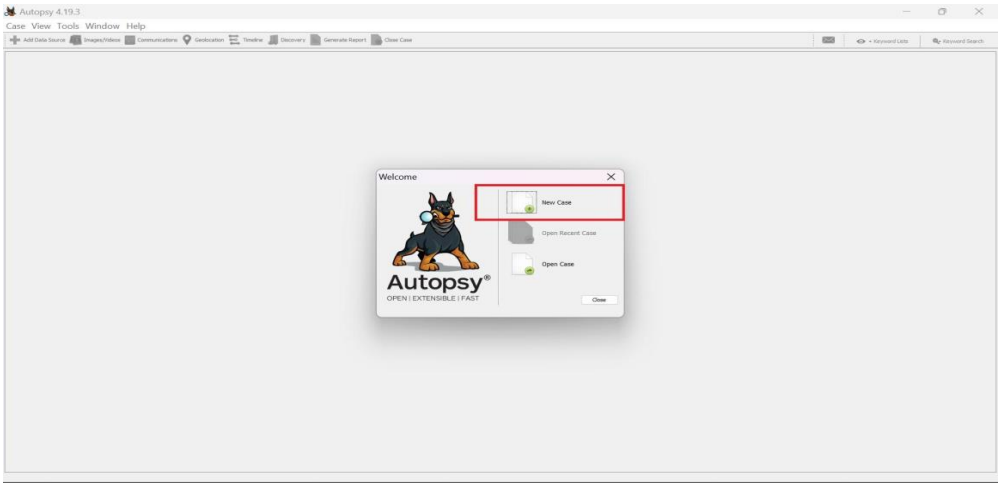
Practical - 8

Q). Perform a full Live Forensics Case Investigation (Using Autopsy)

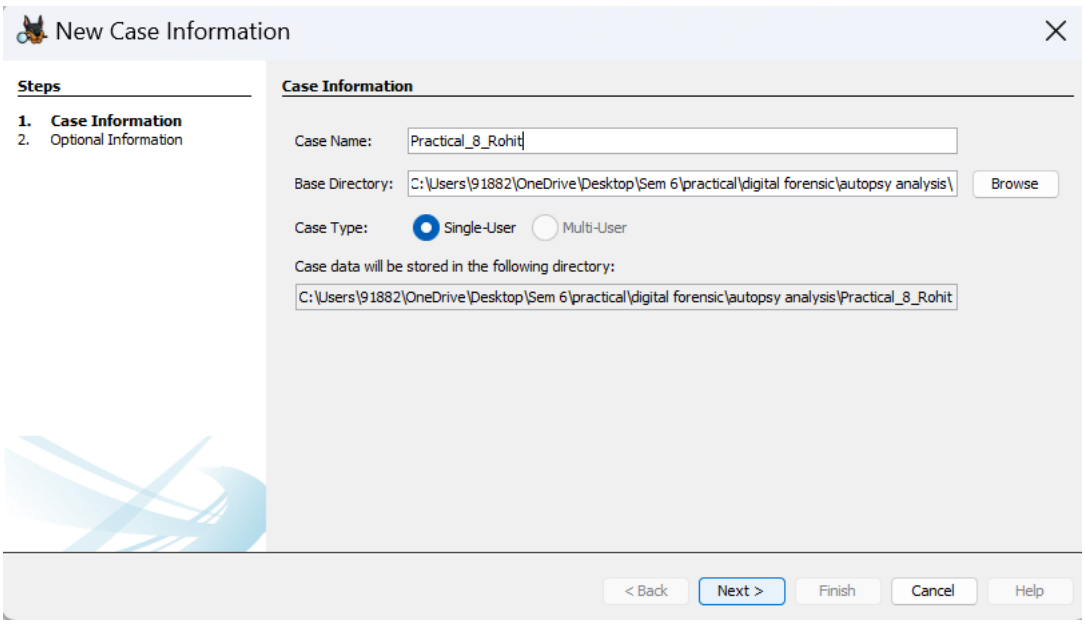
AUTOPSY:

Procedure:

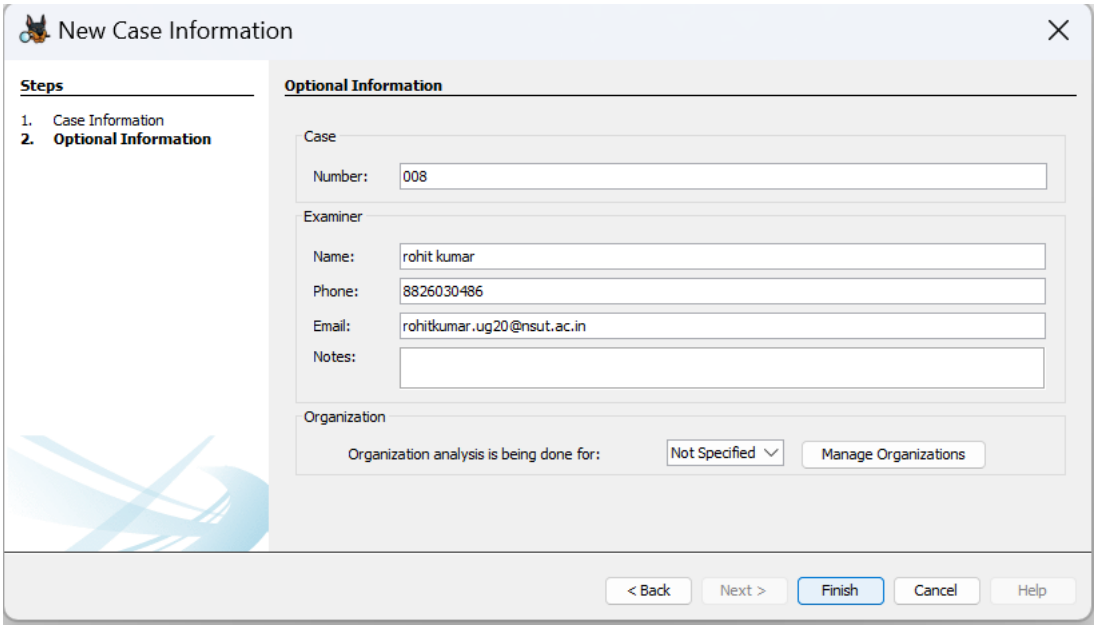
1.) Right click on autopsy icon then select "run as administrator" then click on "New Case Button".



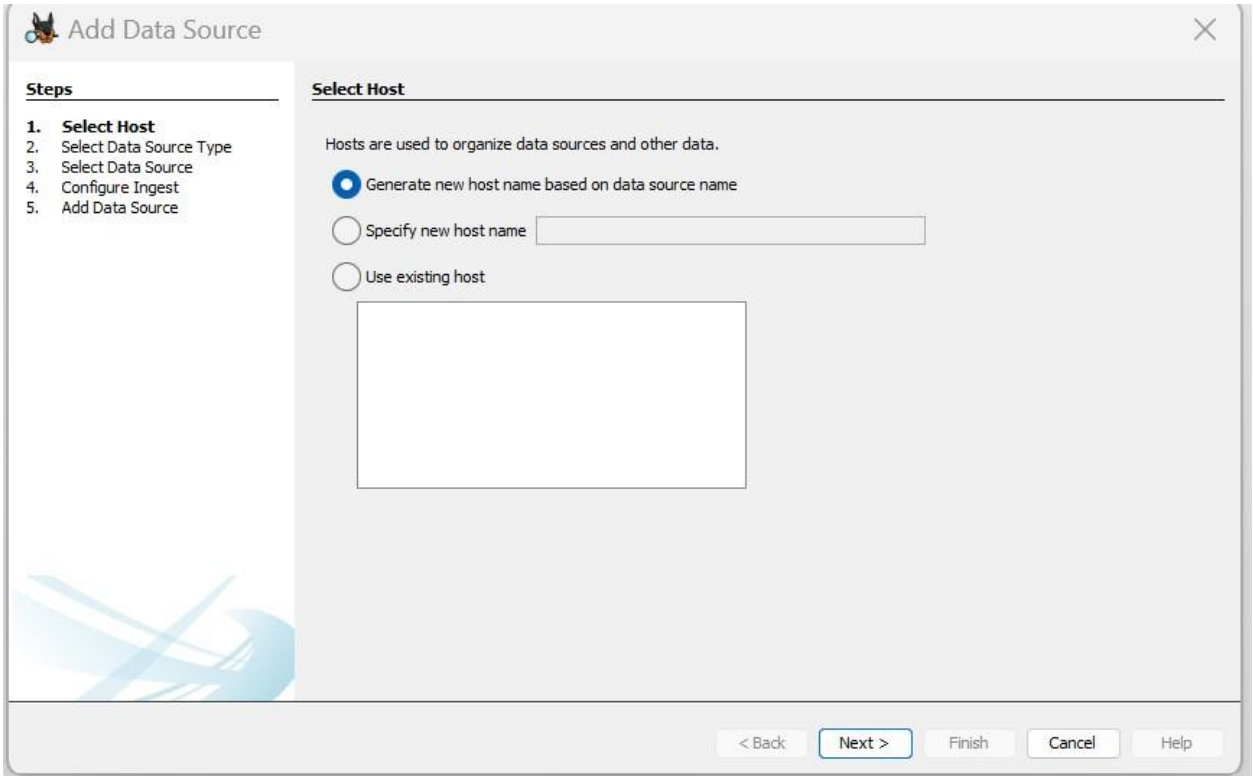
2) Enter Case Name and Base Directory where you want to store your Forensic image then click “Next”



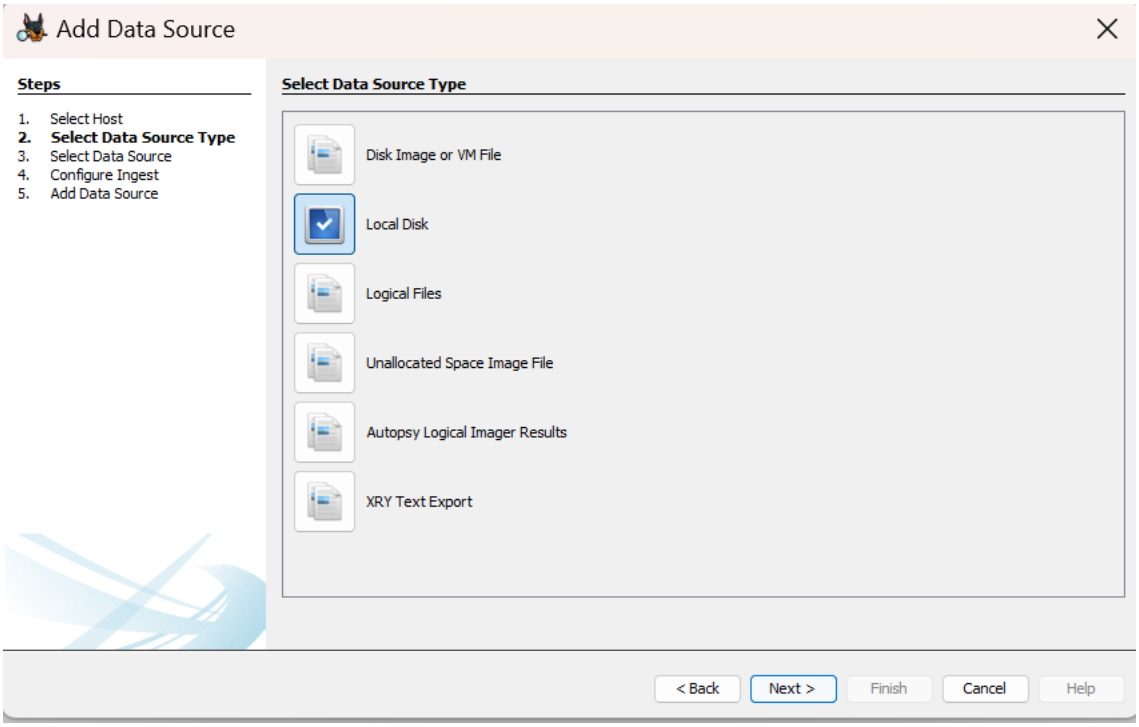
3) Now, Enter case number,and all other information and then click “Finish” Button



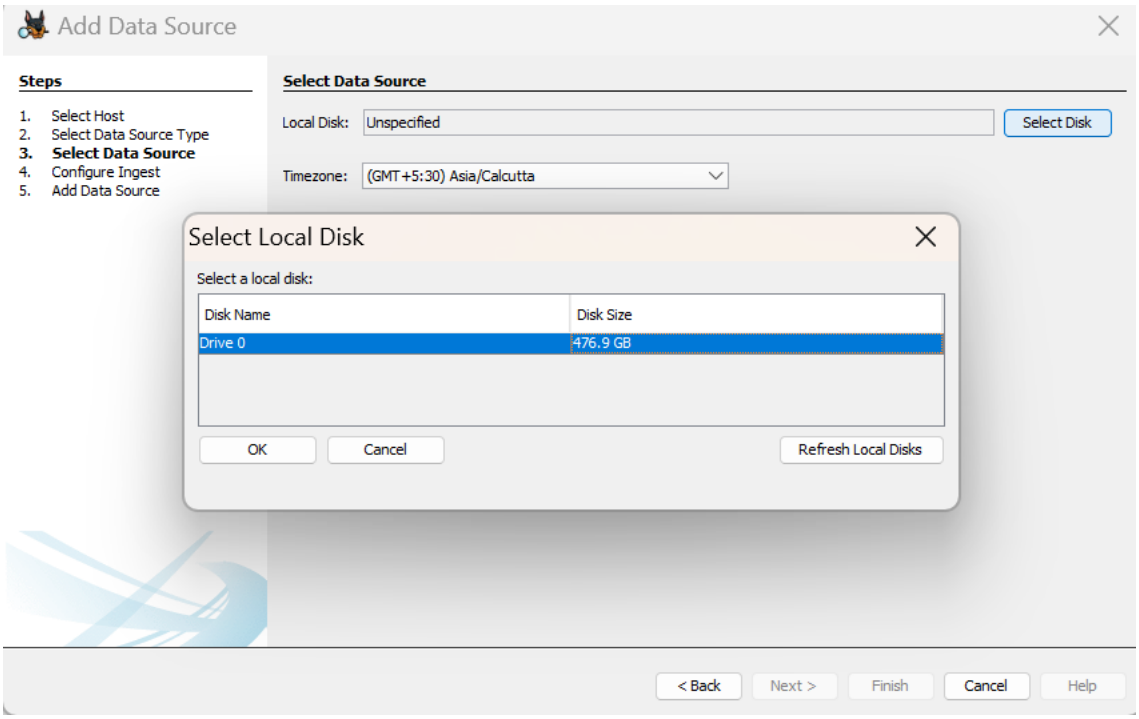
4)Then, in add data source window , select first option which is “Generate new host name”



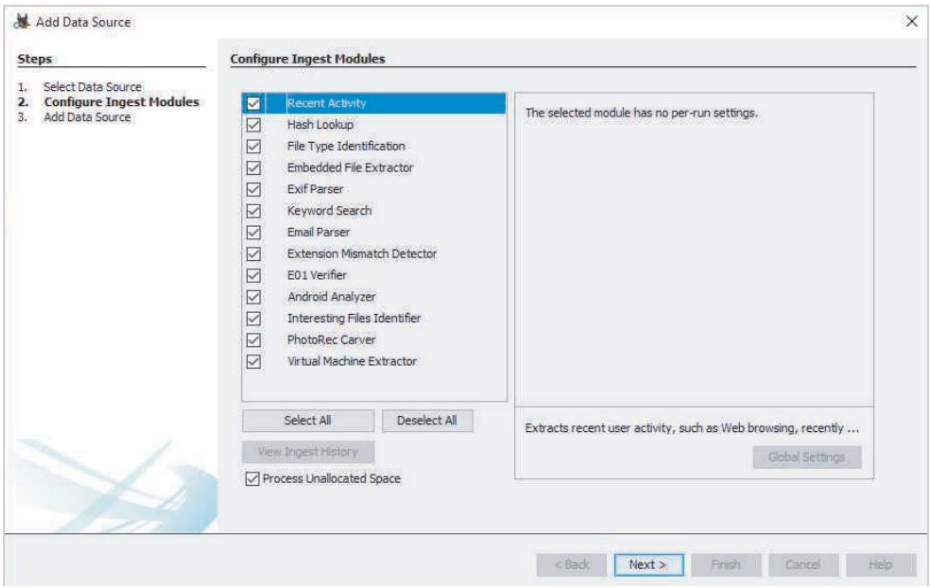
5)Then, Select “Local Disk” option. To Perform live forensic case investigation



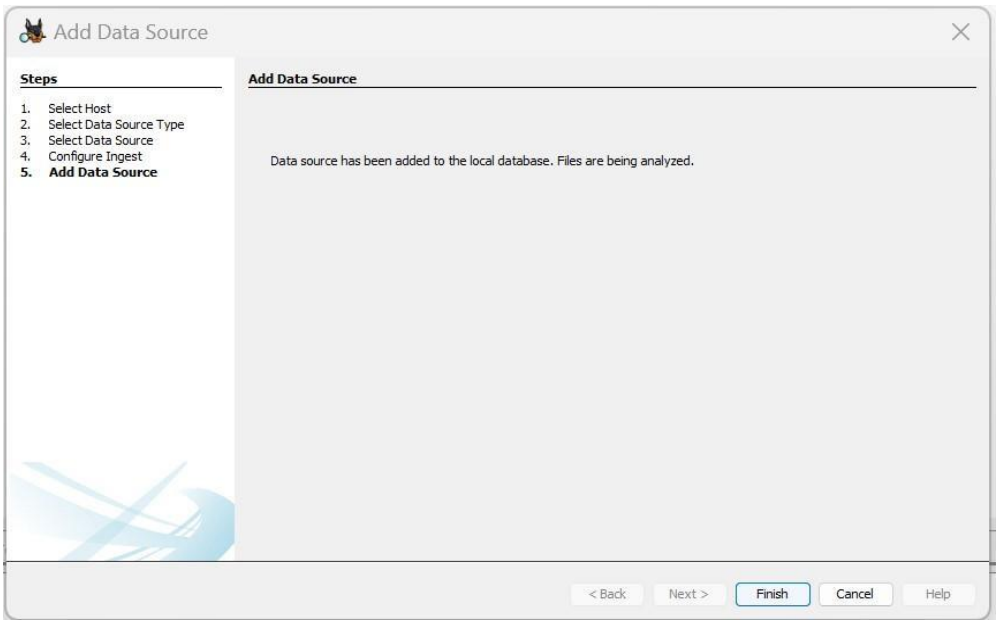
6)Now, In the Select Data Source window, click the "select disk" button. Then choose your storage disk to perform live forensic case investigation then click on "next" button



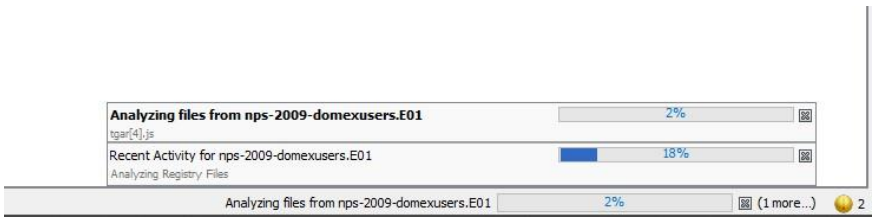
7) In the Configure Ingest Modules window, you can select what type of processing you want, such as a hash lookup or an Exif parser .Leave the default selections, click Next, and then click Finish.



8)Now, it will show “Data source has been added”. click on finish button



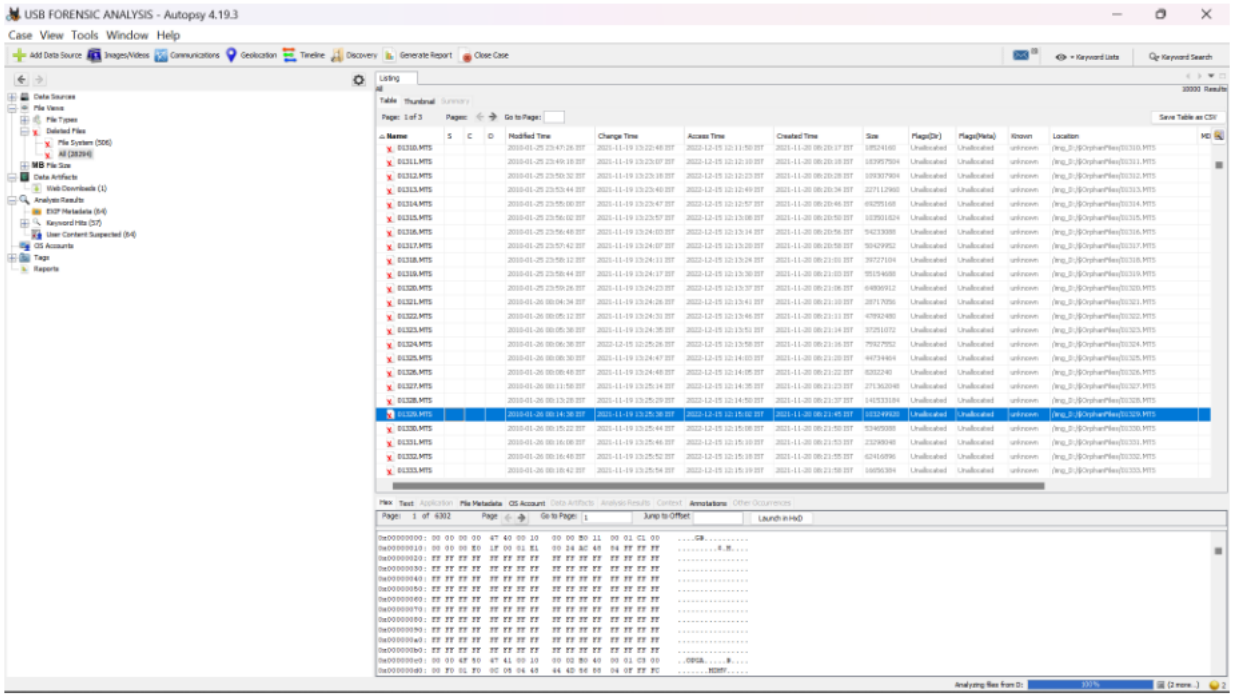
9)Then, it will start analyzing the file and progress of it will be shown in the bottom left corner of the window.



9)After the progress completed ,the image will automatically be open in the autopsy software where you can analyzed the file.

Now, you can see deleted files of storage device by clicking “Deleted Files” and the red cross marks files which are shown in the software are

the deleted files .you can also preview the files by clicking on it



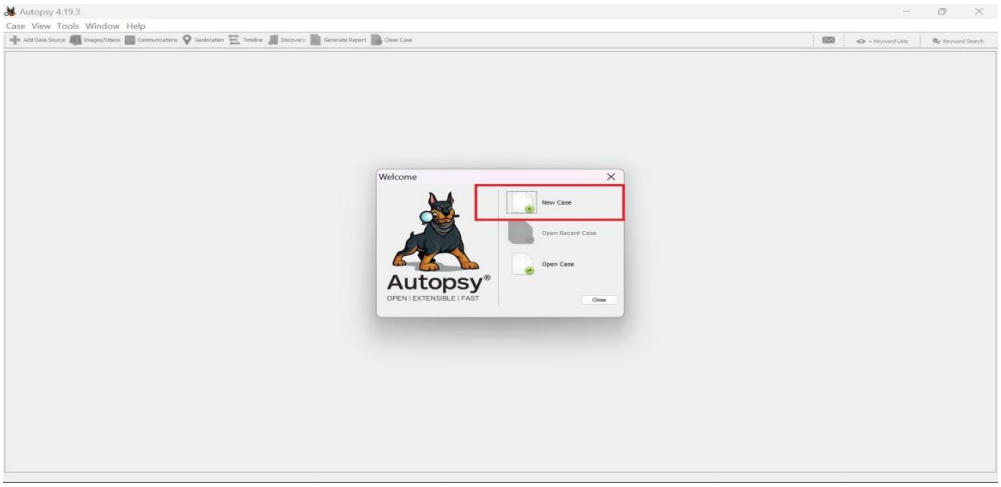
Practical - 9

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

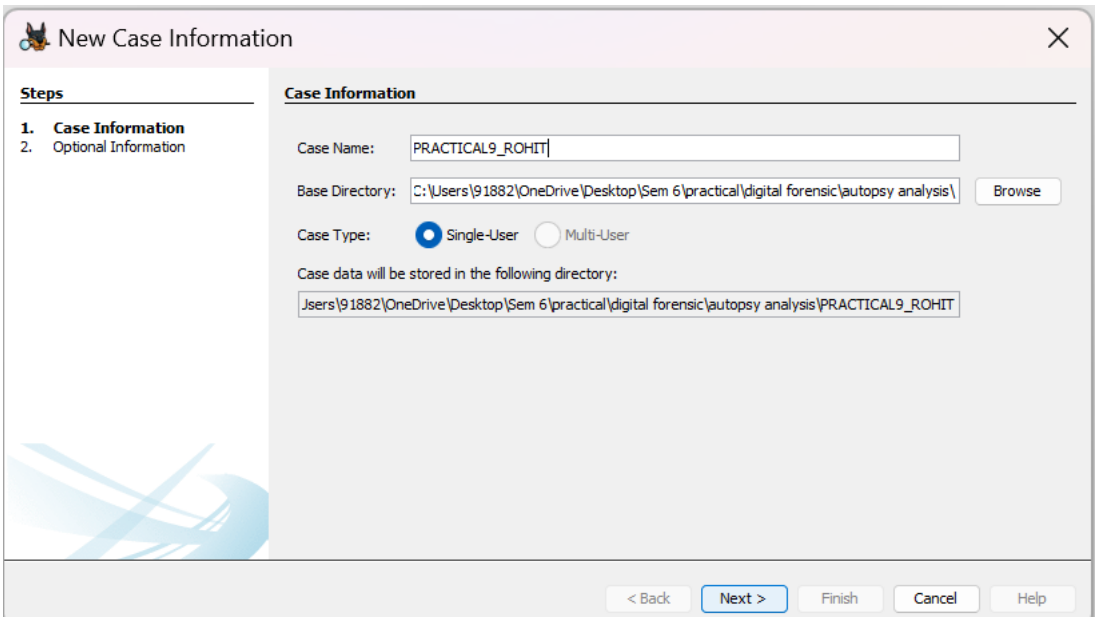
AUTOPSY:

Procedure:

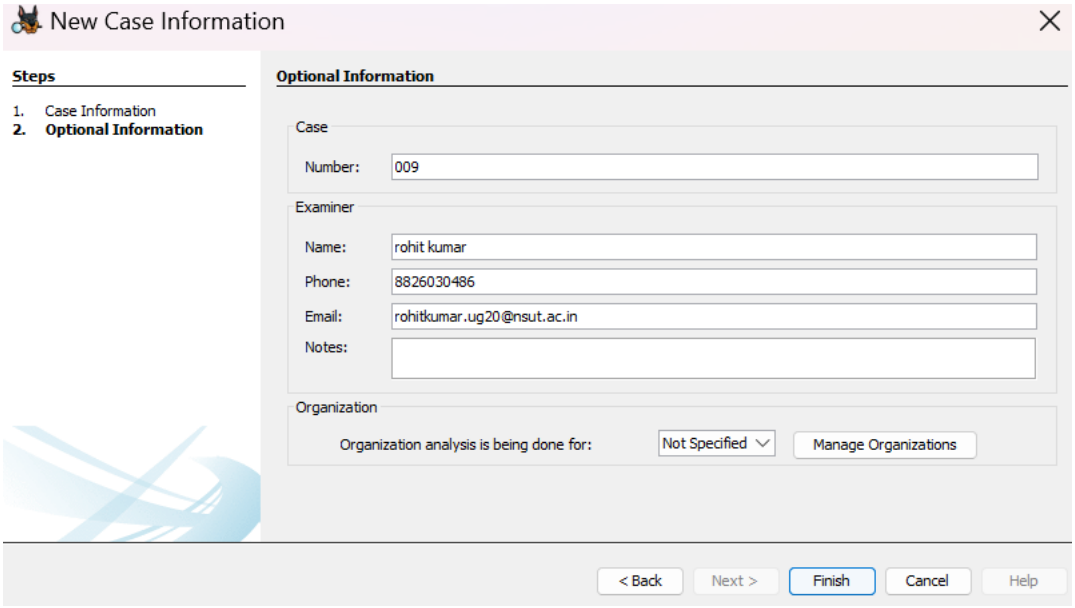
1.) Launch Autopsy, and click on the "New Case" button.



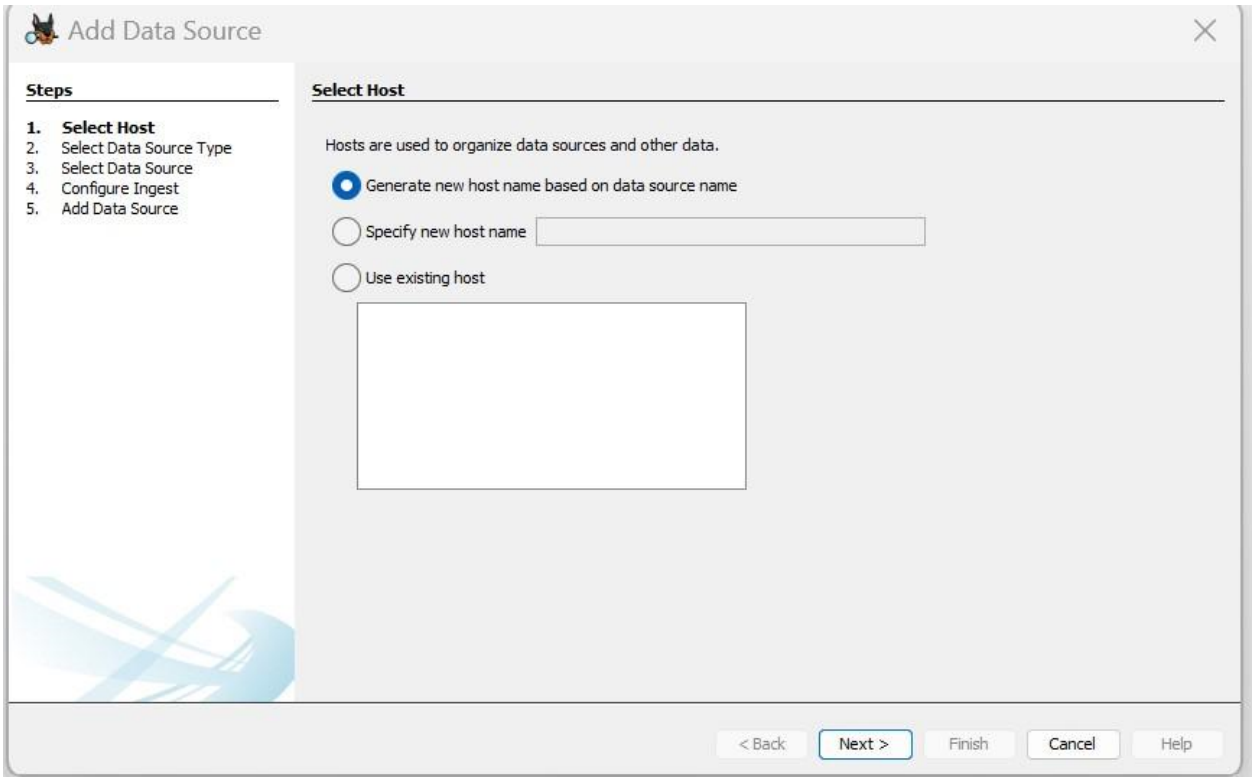
2) Enter Case Name and Base Directory where you want to store your Forensic image then click “Next”.



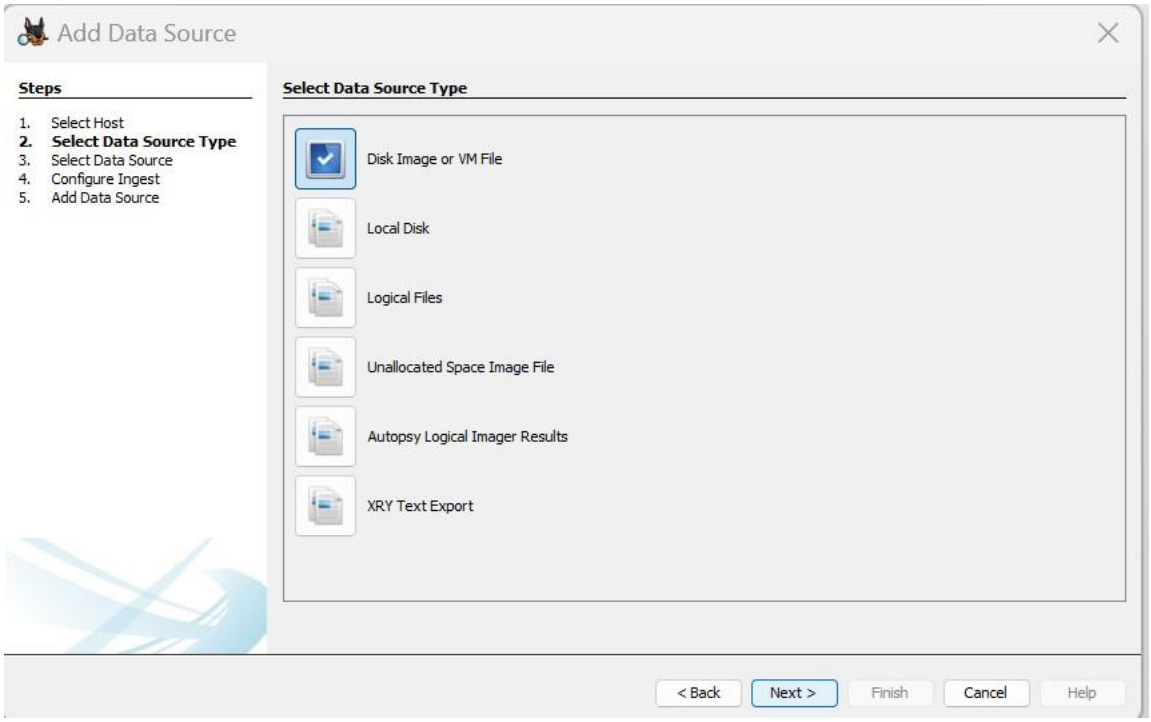
3) Now, Enter case number,and all other information and then click “Finish” Button



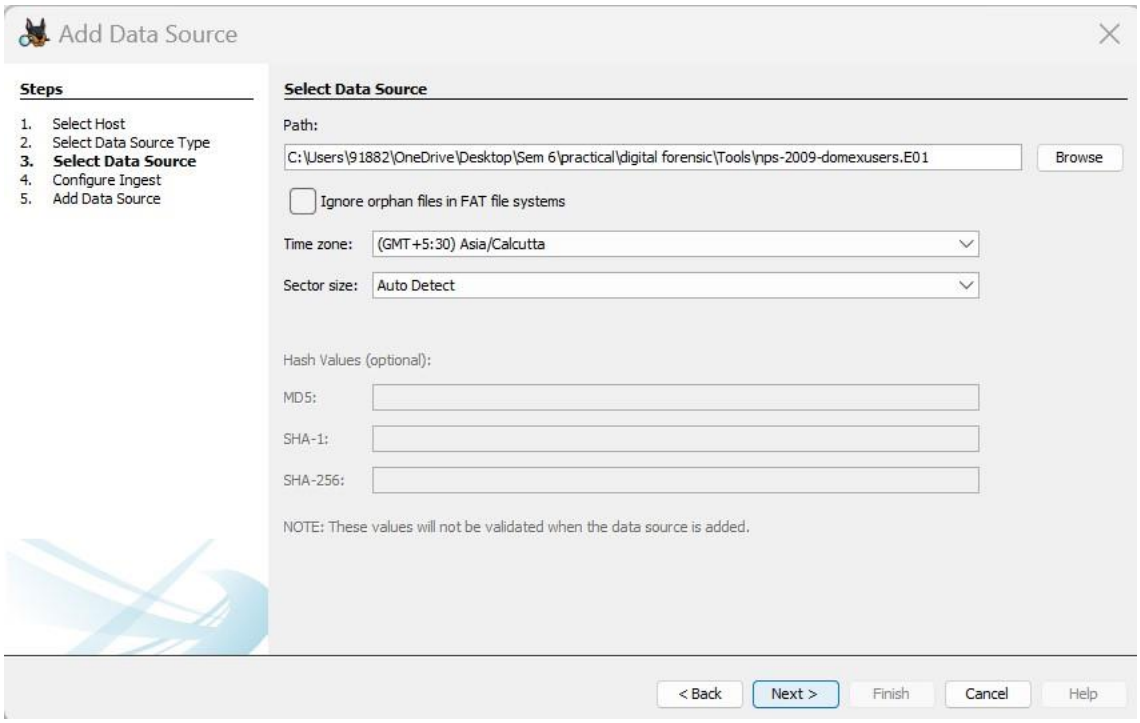
4)Then, in add data source window , select first option which is “Generate new host name”



5)Then, Select “Disk Image or Vm File ” option. To analyze the image file of storage device

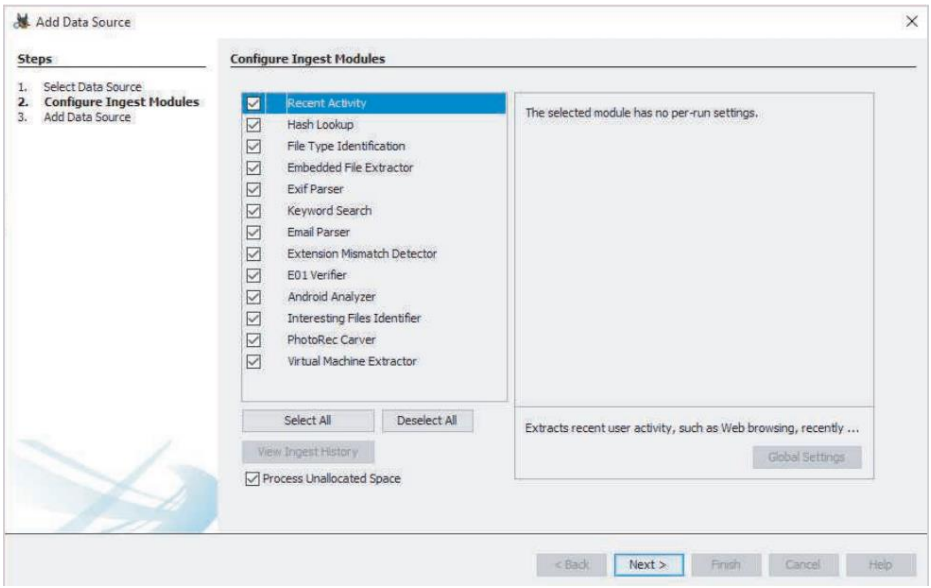


6)Now, In the Select Data Source window, click the Browse button next to the "Browse for an image file" text box, navigate to the location of your image file and click the that file, and then click Open. Click Next.

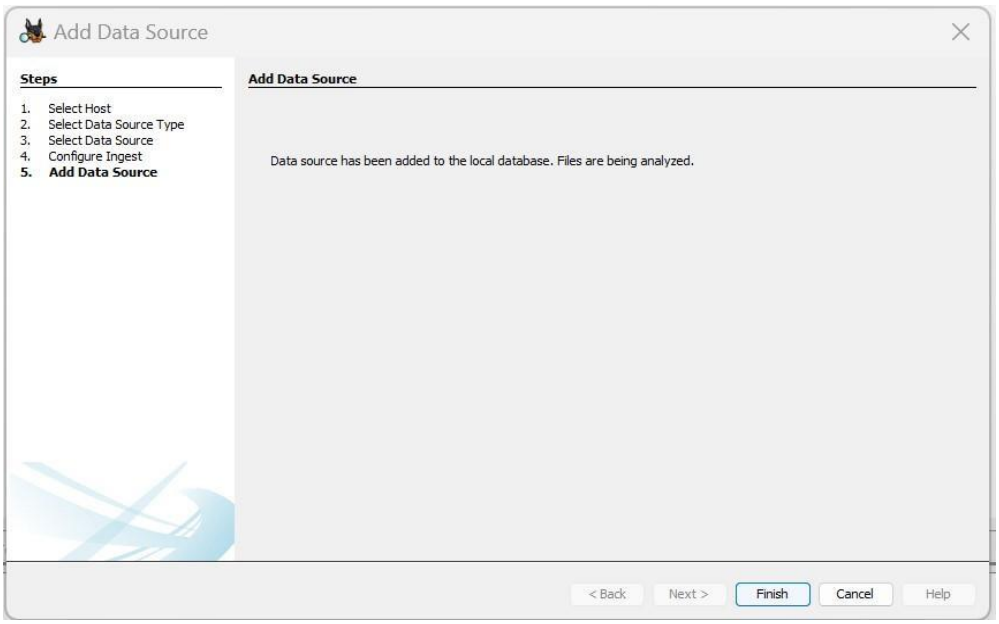


7) In the Configure Ingest Modules window, you can select what type of processing you want, such as a hash lookup or an Exif parser .Leave the default selections,click Next, and then click Finish.

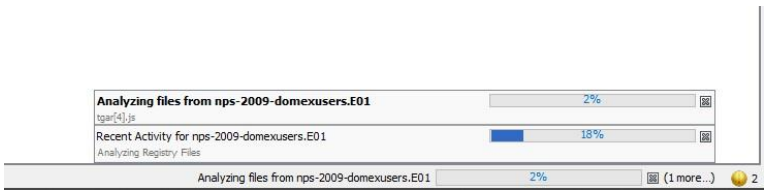
(NOTE:- MAKE SURE EXIF PARSER IS SELECTED TO EXTRACT EXIF DATA FROM IMAGE FILE)



8)Now, it will show “Data source has been added”. click on finish button

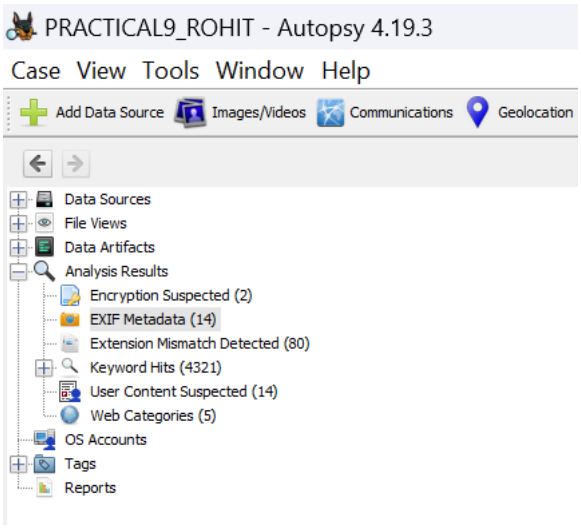


8)Then, it will start analyzing image file and progress of it will be shown in the bottom left corner of the window.

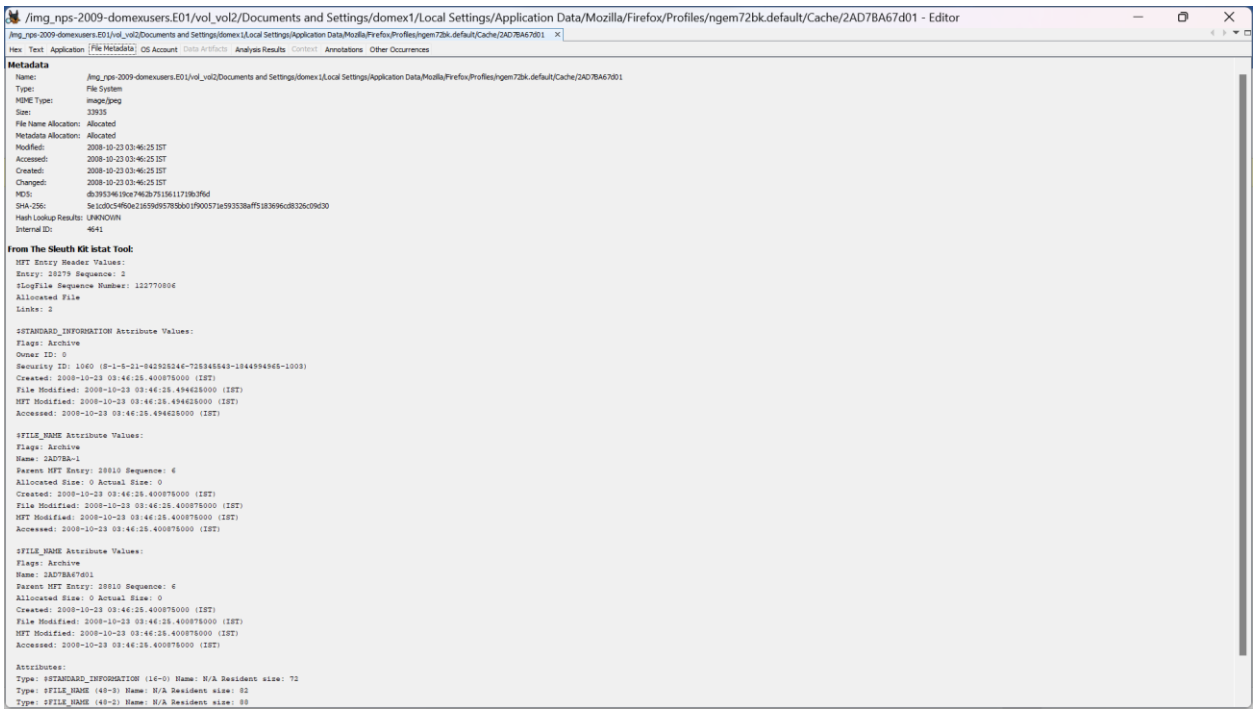


9)After the progress completed ,the image file will automatically be open in the autopsy software where you can analyzed the image file. Now,

On Tree View ,Under the "Analysis Result " node , navigate to "EXIF metadata"



10)On clicking , it will show us all EXIF metadata files. To view this file metadata,Right click on any file then click "View item in new window" then it will open new window then click "File metadata". Then it will dislplay the metdata of the file as shown below :



11)Lastly if you want to extract and save this EXIF metadata file .Right click on it and then click Extract File(s). In the Save dialog box, click Save to save the files in your desired location then exit autopsy.

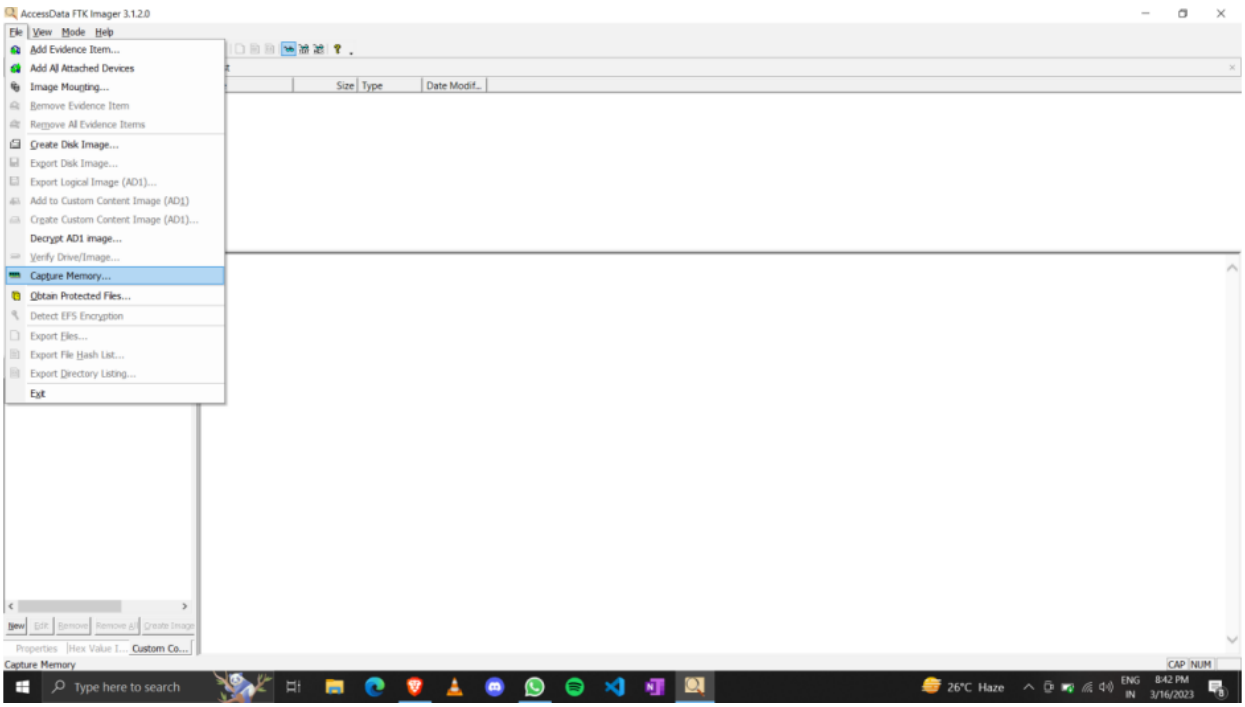
Practical - 10

Q). Perform Live Forensics in the Volatile Memory (Using FTK Imager).

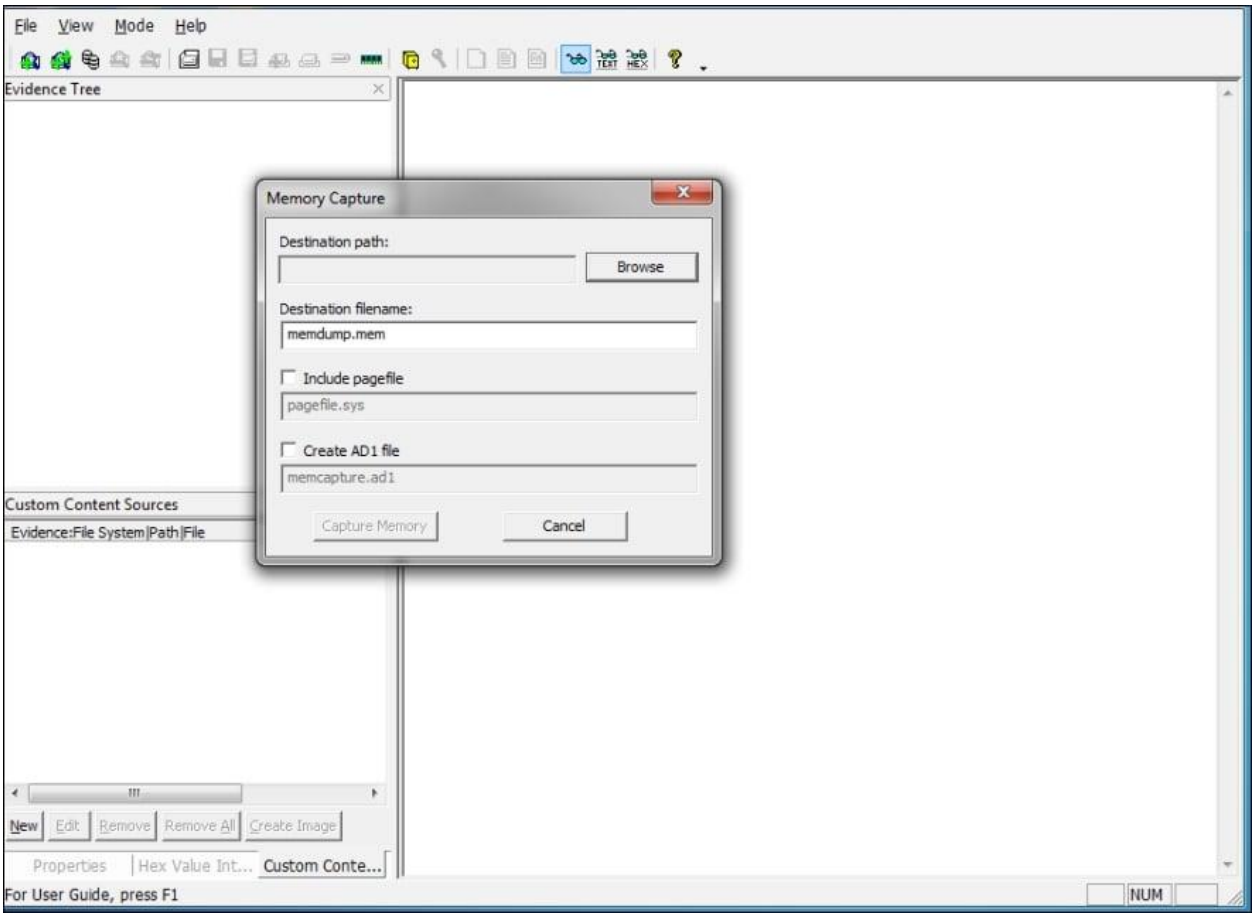
FTK Imager :

Procedure:

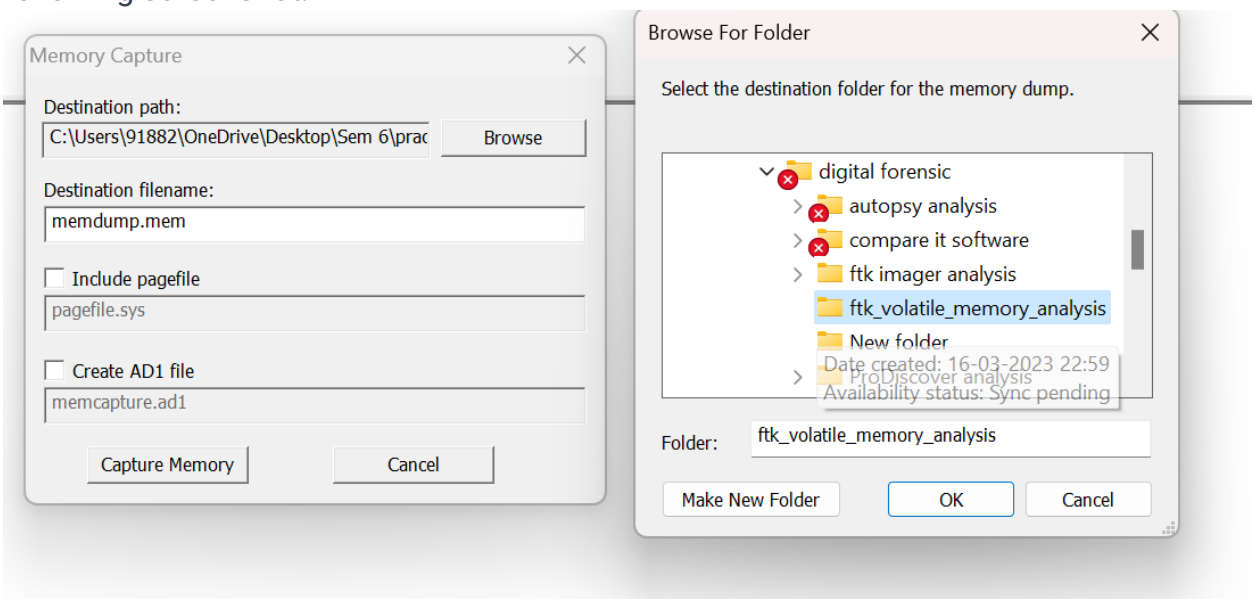
1. Launch FTK Imager and select the "Capture Memory" option from the File menu.



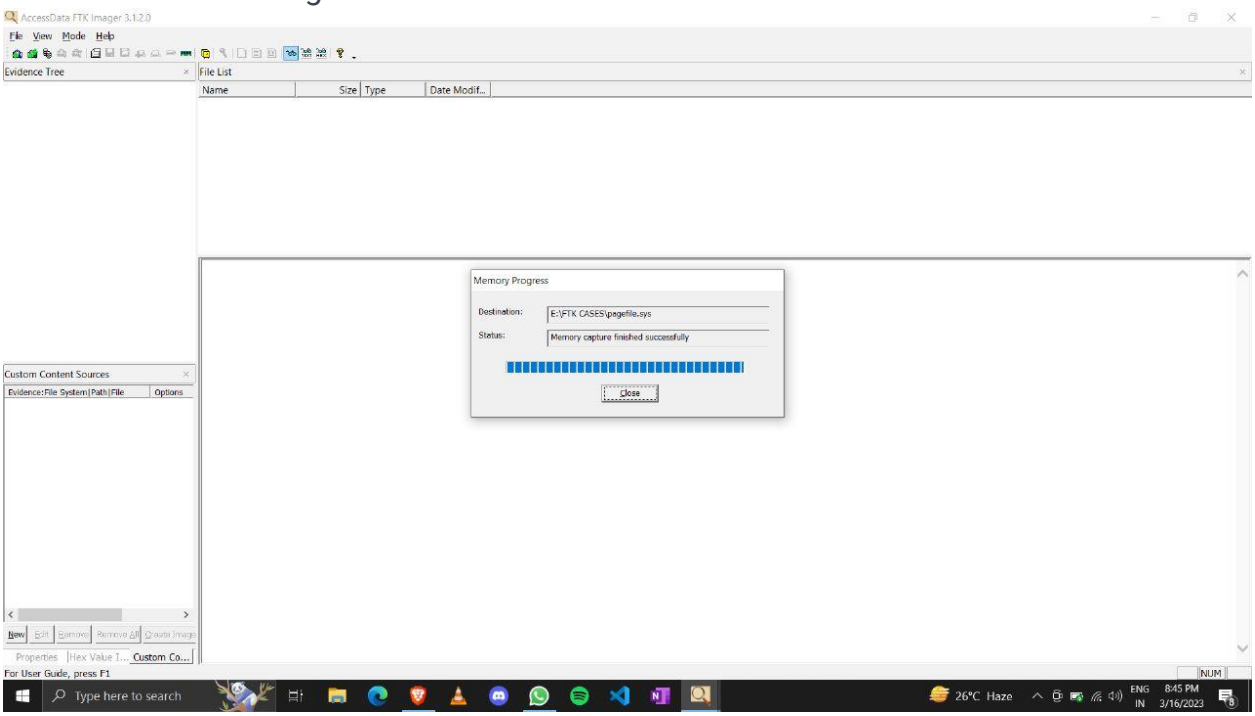
2. Browse the destination folder, where you want to save the acquired memory dump, as shown in the following screenshot:



3. Click on Browse and create a destination folder, as shown in the following screenshot:



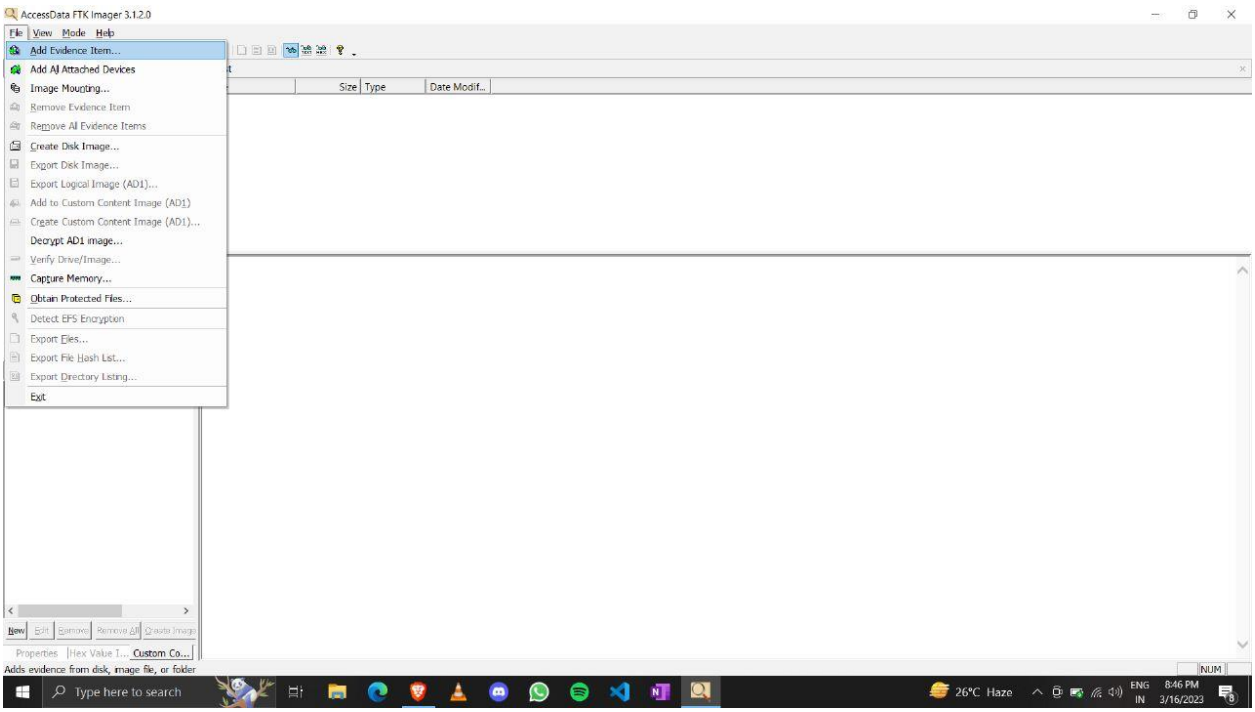
4. After creating the destination folder, click on Capture Memory, as shown in the following screenshot:



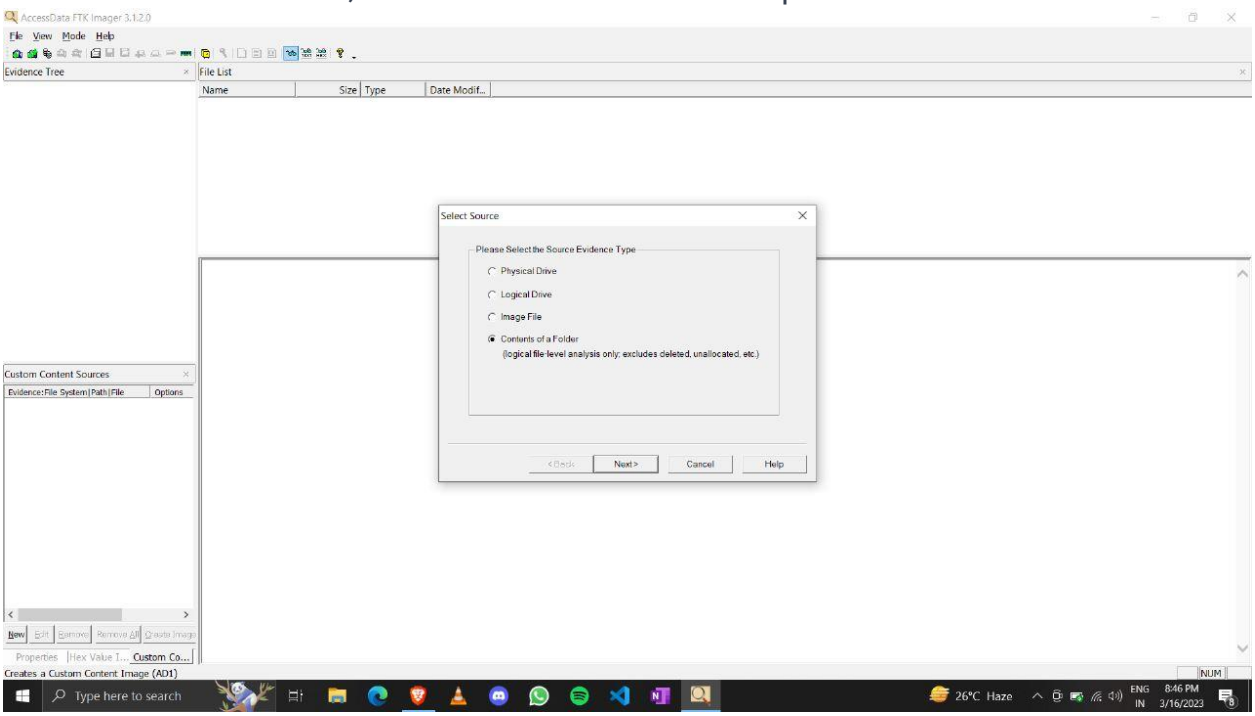
5. Once the acquisition is complete, save the image file to a secure location.

To analyze a memory image file in FTK Imager, follow these steps:

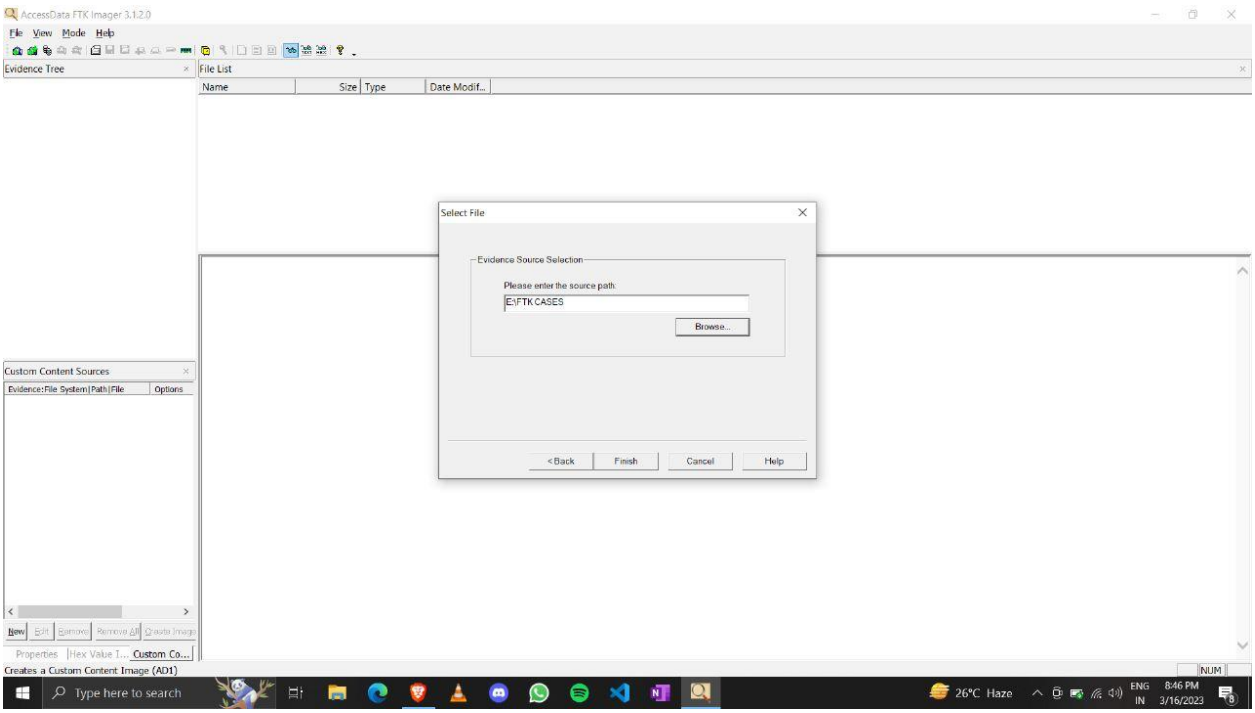
1. Click on "File" and select "Add Evidence Item".



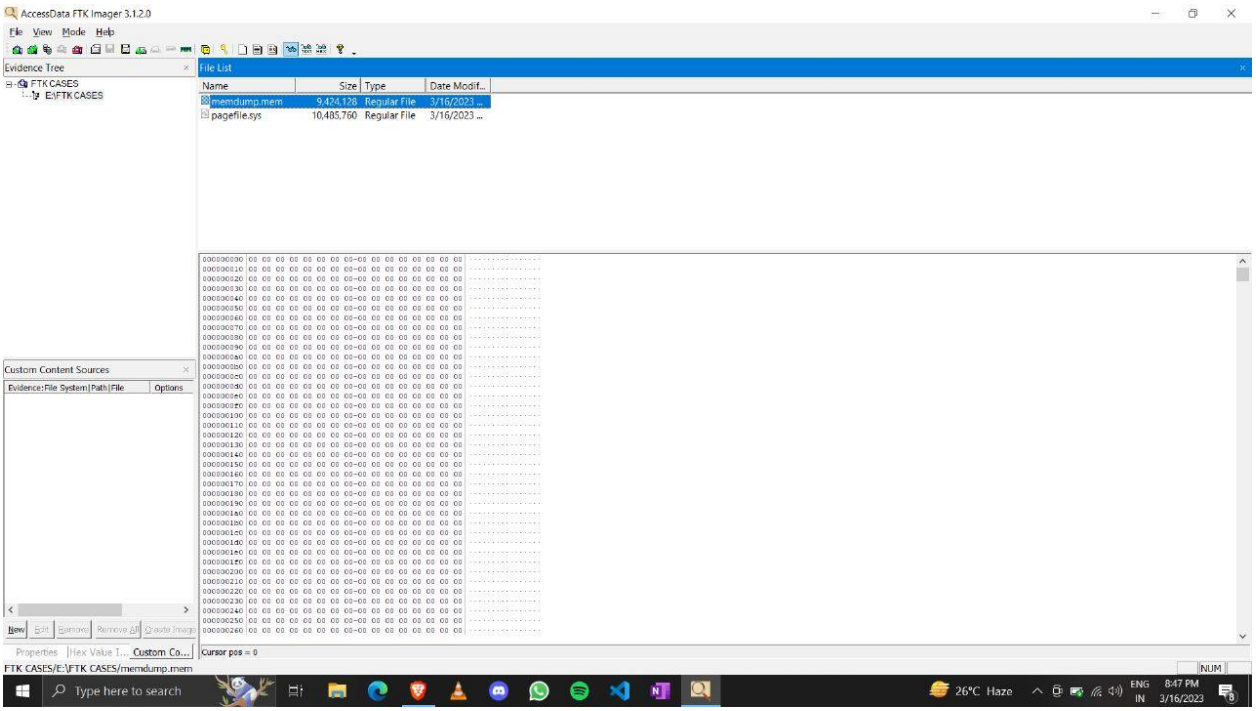
2. In Select source window, select "contents of a folder" option.



3. Navigate to the memory image file you wish to analyze and select it, then click Finish



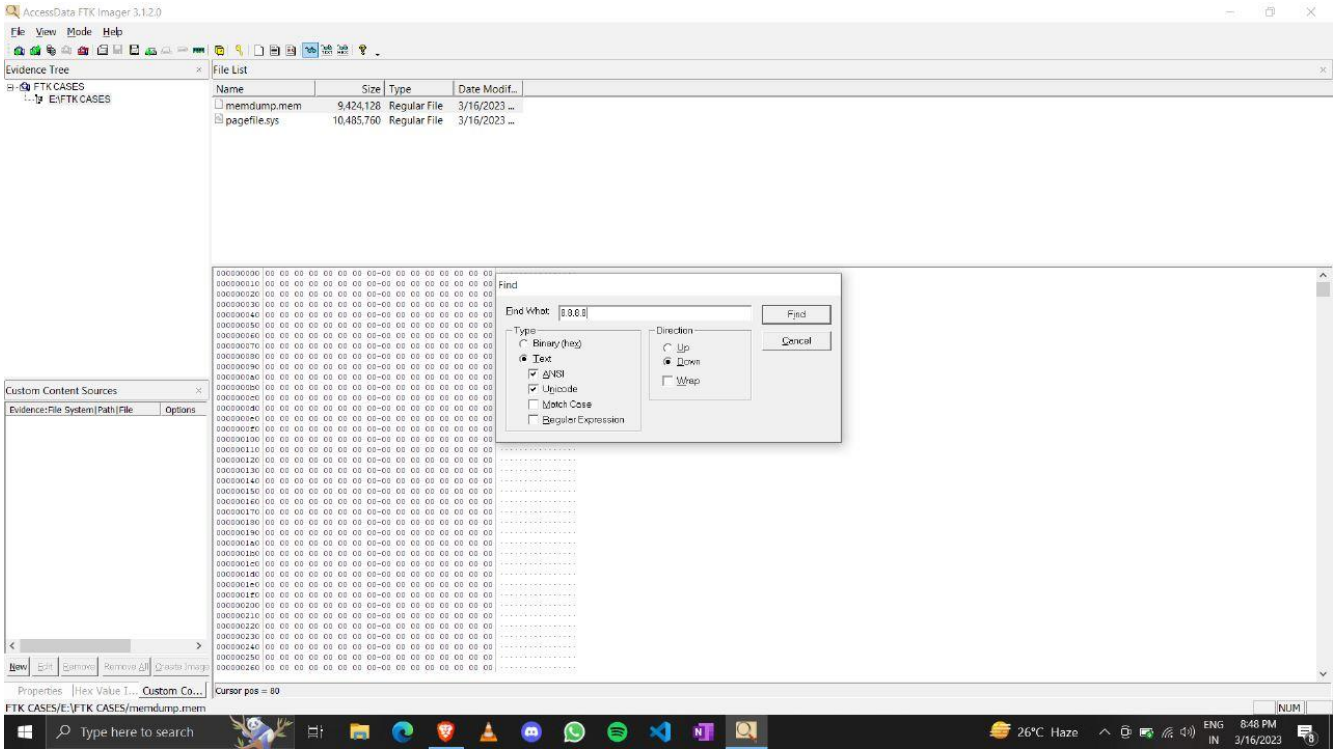
4. Once the file is added to FTK Imager, you can preview the file by selecting it in the Evidence Tree and clicking on the "Preview" tab.



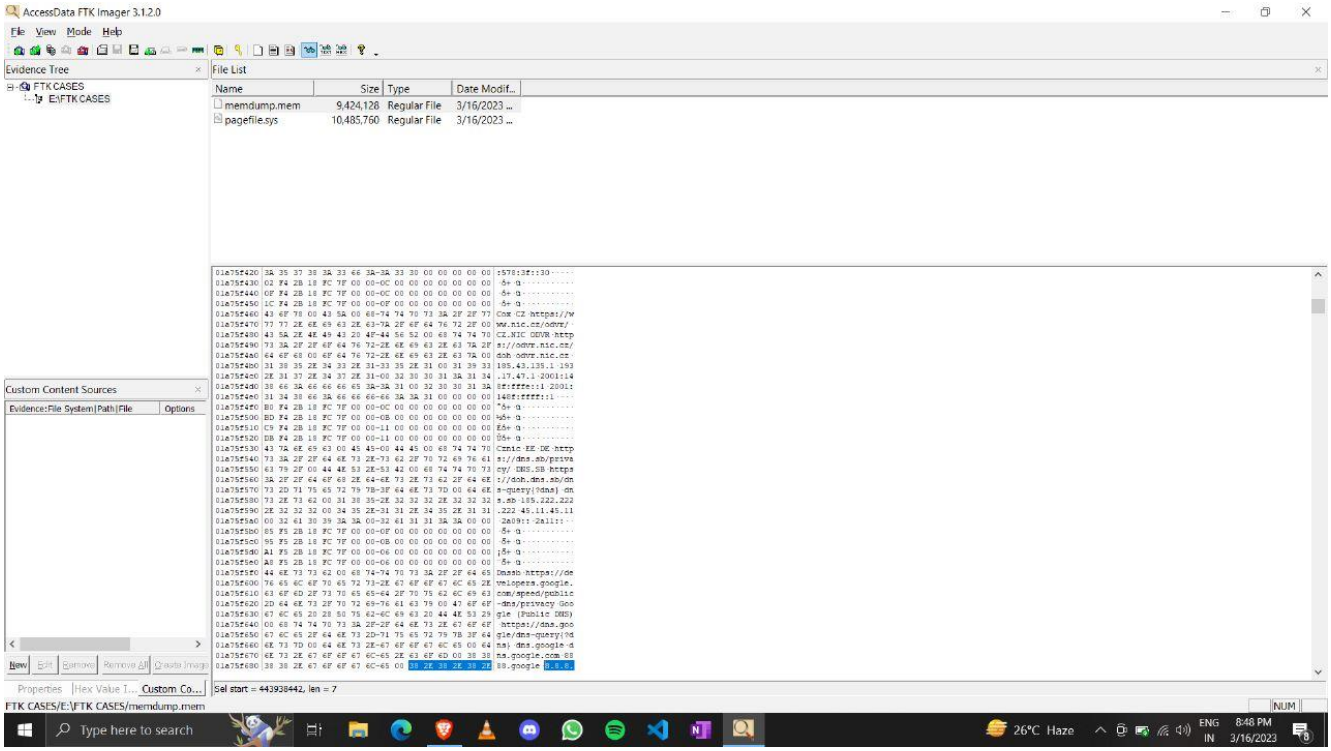
5. To analyze the file, you can use FTK Imager's built-in analysis tools

6. To use FTK Imager's built-in analysis tools, select the memory image file in the Evidence Tree and click on the "Analysis" tab. Here, you can view information about the system's processes, open network connections, and more.

7. You can also use FTK Imager's search function to search for specific keywords or strings within the memory image file. To do this, select the memory image file in the Evidence Tree and click on the "Search" tab. From here, you can enter your search terms and select the search options you wish to use.



8)By using this find function in this practical , we can find password as well many other required information.



Practical - 11

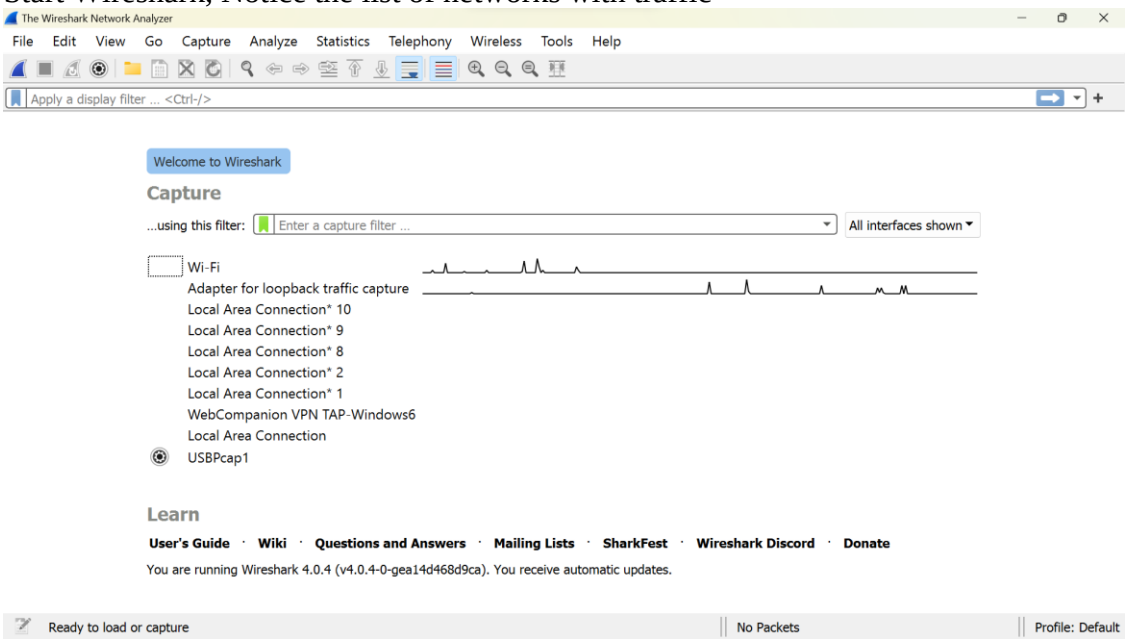
Q). Study the WIRESHARK tool for Network forensics.

Wireshark is a popular network protocol analyzer tool that is commonly used in network forensics investigations. It allows users to capture and analyze network traffic in real-time or from a saved capture file.

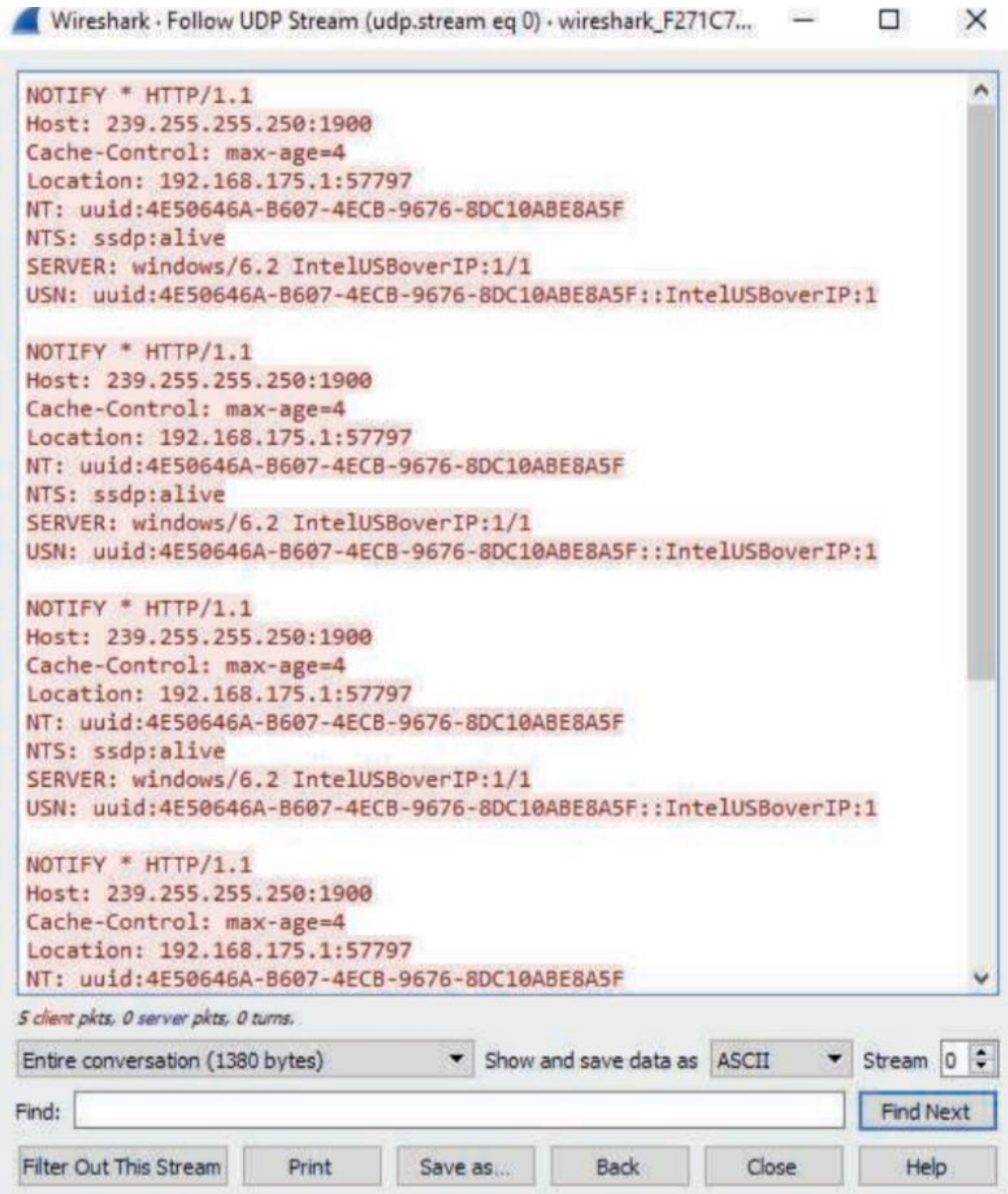
Wireshark can be used in a real-time environment to open saved trace files from packet captures. An important feature is its capability to rebuild sessions. To use this feature, right-click a frame in the upper pane and click Follow TCP Stream. Wireshark then traces the packets associated with an exploit.

To see how this tool works, download the most recent version of Wireshark for Windows (www.wireshark.org/download.html) and install it on your workstation.Then follow these steps:

1. Start Wireshark, Notice the list of networks with traffic

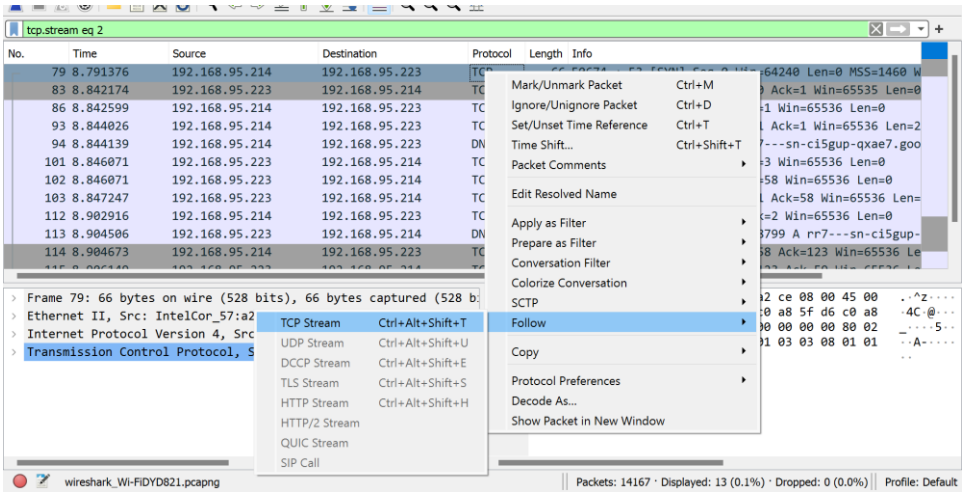


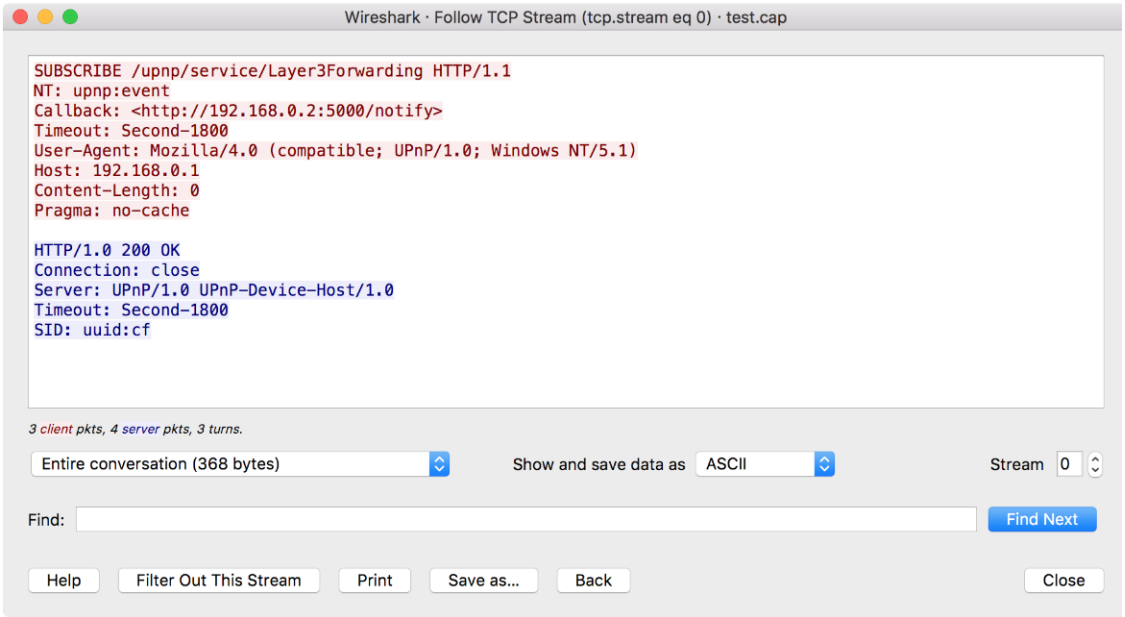
2. Double-click a network that's showing activity.In our case we are going to analyze Wi-Fi. (If you're not on a live network,ping another student or yourself and visit some Web sites and download a file to generate traffic. Then start this activity again.)
3. After several frames have been captured, click Stop.
4. After the trace has been loaded, scroll through the upper pane until you see a UDP frame or an SSOP frame. Right-click the frame, point to Follow, and click UDP Stream. You should see a window similar to given below :



5.) Review the information in this window, and then exit Wireshark.

Similarly do this for tcp pakcets



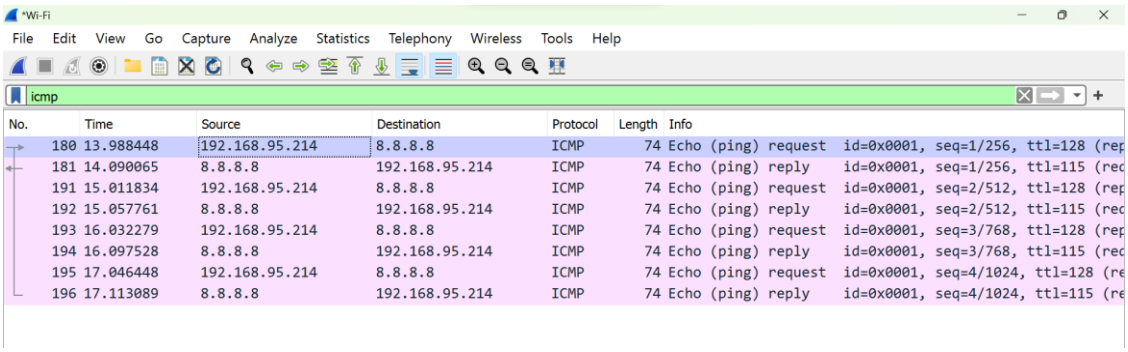


Review the information in this window for analyzing tcp packets , and then exit Wireshark.

Now to analize icmp pakcets we first need to analze the packet using ping command as show below :

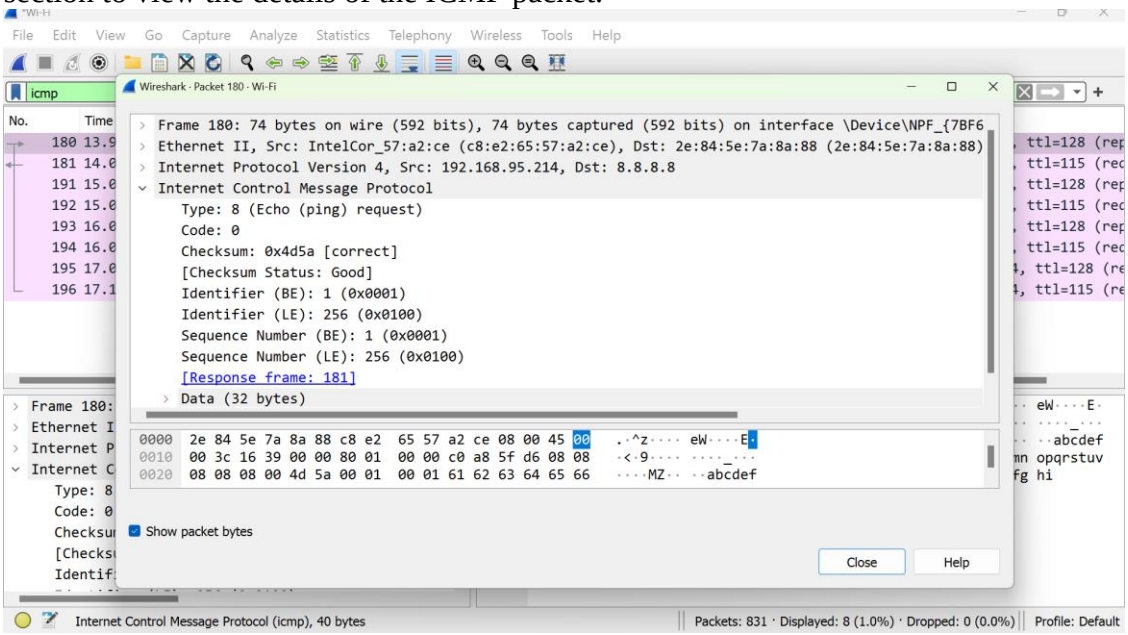
```
C:\Users\91882>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=101ms TTL=115
Reply from 8.8.8.8: bytes=32 time=46ms TTL=115
Reply from 8.8.8.8: bytes=32 time=65ms TTL=115
Reply from 8.8.8.8: bytes=32 time=66ms TTL=115

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 46ms, Maximum = 101ms, Average = 69ms
```

Now, in wireshark on display filter type icmp to show all icmp packets



select any ICMP packet by clicking on it in the packet list.Right click on it then click on show packets in New window

In the packet details pane, expand the "Internet Control Message Protocol" section to view the details of the ICMP packet.



Practical - 12

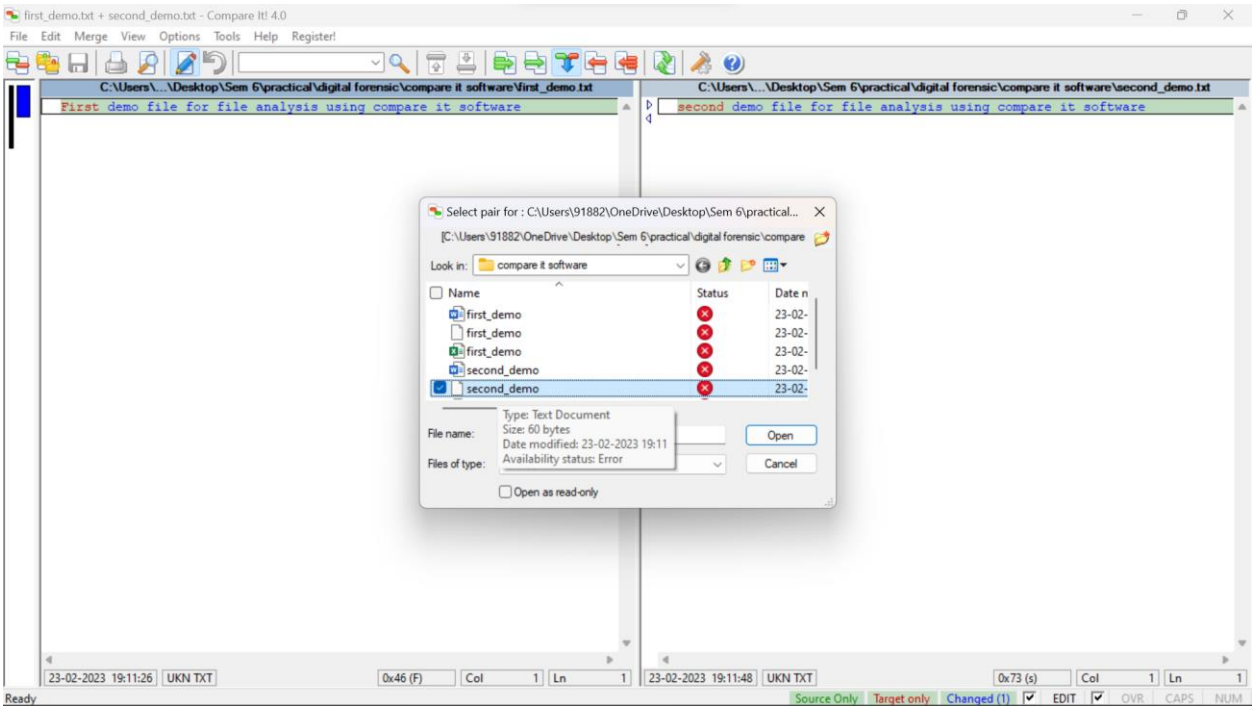
Q). Perform file analysis using "Compare It" Software

COMPARE IT :

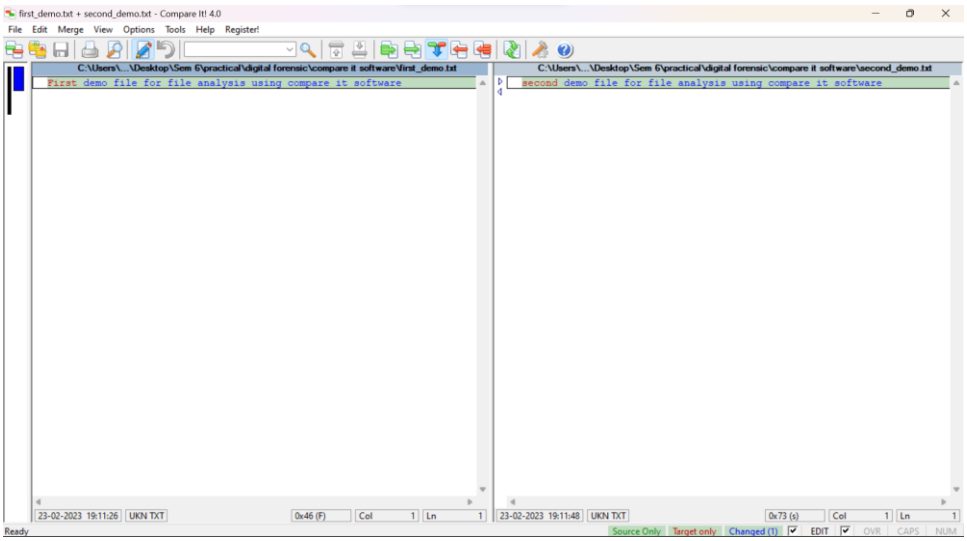
Procedure:

Click on Compare It Tool, It will show a window to select the files to be compared.

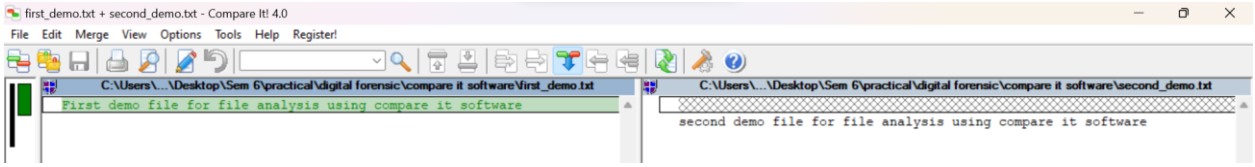
First select the first file and click on open and then select the second file and click on open.



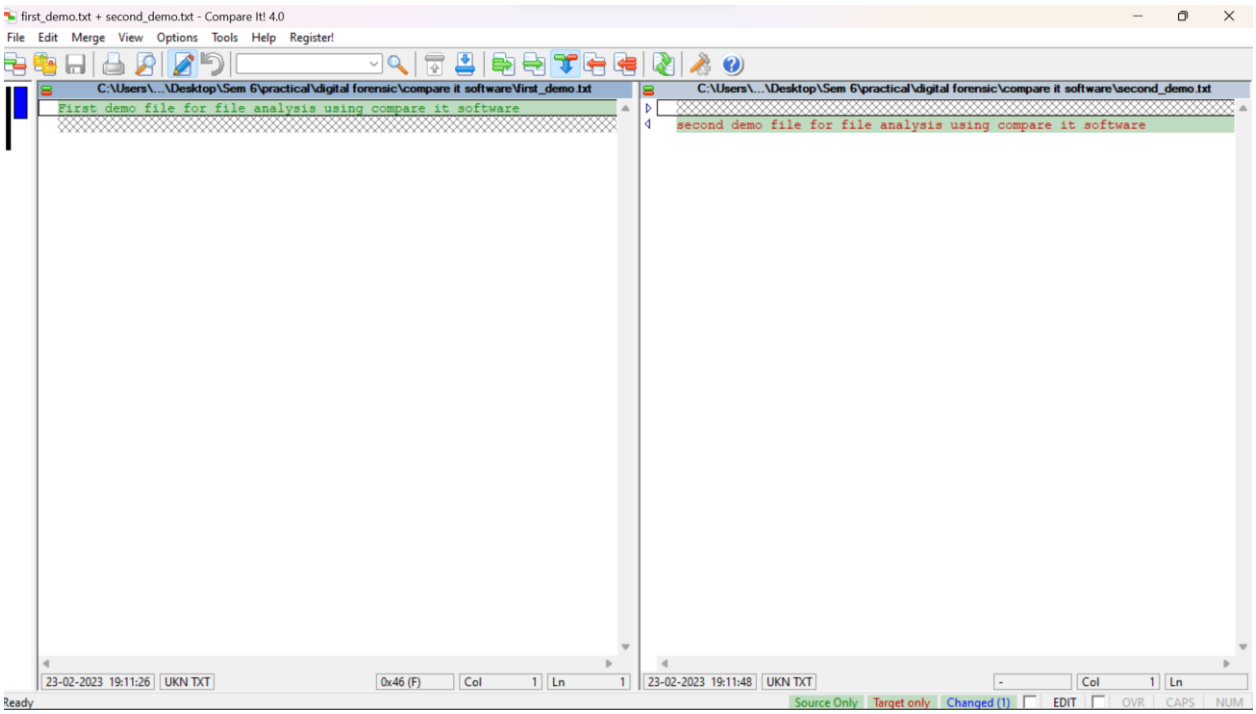
Now it will show us the changes in highlighted bar.



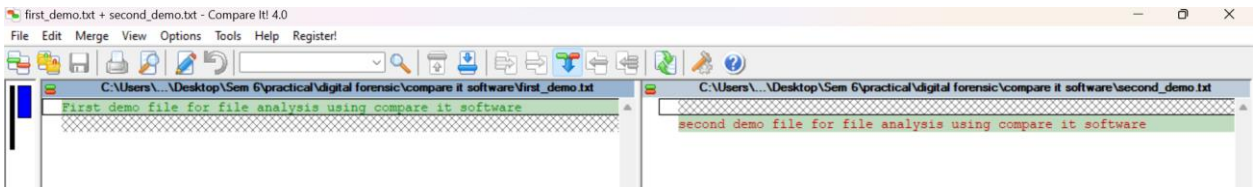
Now click on view and select Changes only. It will show all the changes simultaneously



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



Now select Edit checkbox in status bar. The cursor will move to the changed line and now the text can be edited.



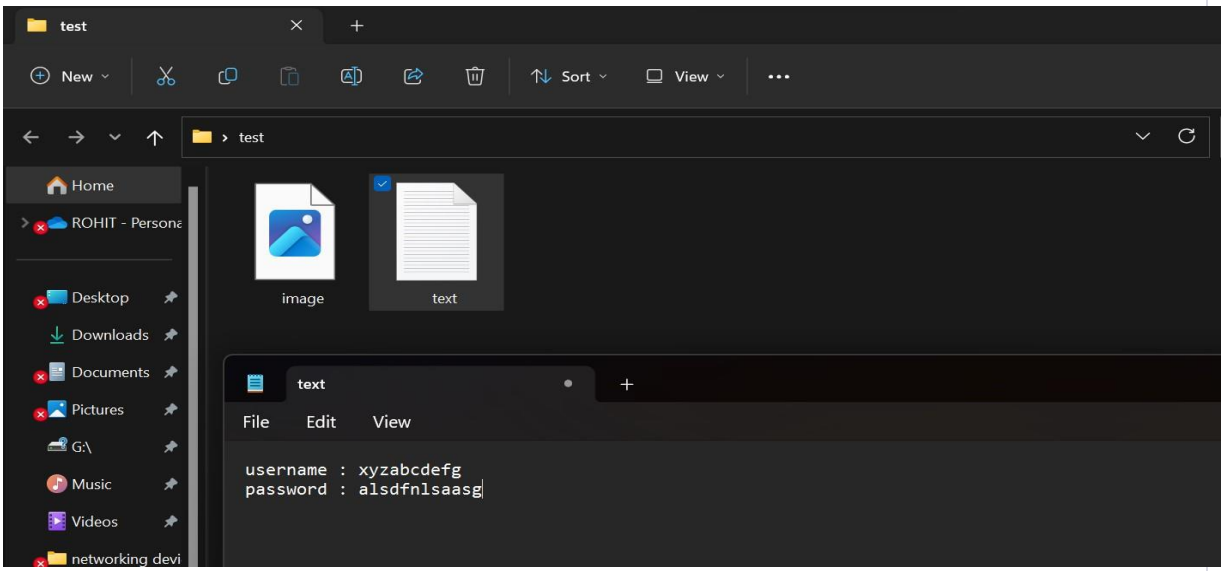
Practical - 13

Q). To study the steps for hiding any file behind an image Command Prompt (CMD). Use Compare IT! Software for further analysis

Procedure:

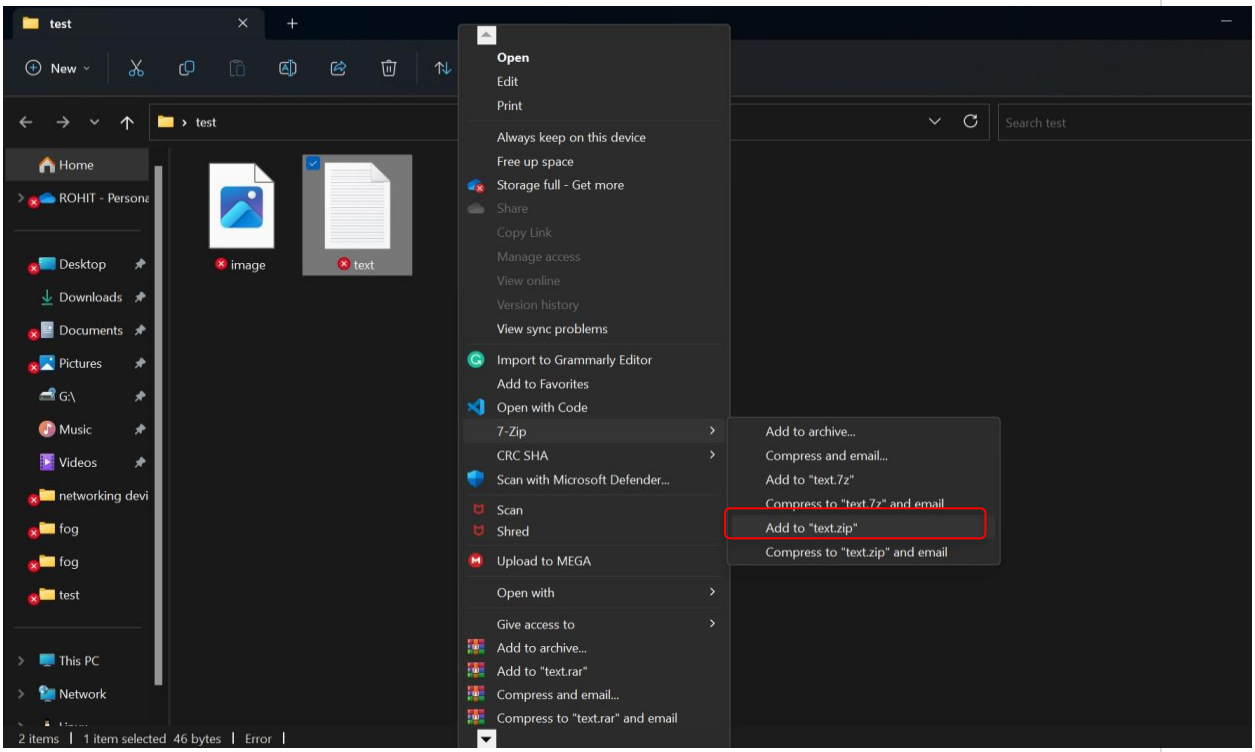
Hiding a file behind an image using Command Prompt involves a technique called "steganography," which allows you to conceal a file within another file. Here are the steps:

1. Choose the image: Select an image file (.jpg or .png) that you want to use to hide your file. Make sure it is a high -quality image with a large fi le size.
2. Create a copy of the image: Make a copy of the image and save it in a separate location, such as your desktop.
3. For this practical, I created a text document and placed fake login information in the text file as shown below :



4. Compress your file: Compress the file you want to hide into a ZIP or RAR archive using WinRAR or 7 -Zip. When you have your text file saved with the information you would like to have hidden, right -click on the image and hover over 7 -Zip. Then select "Add to text.zip."

This will create a zip folder.

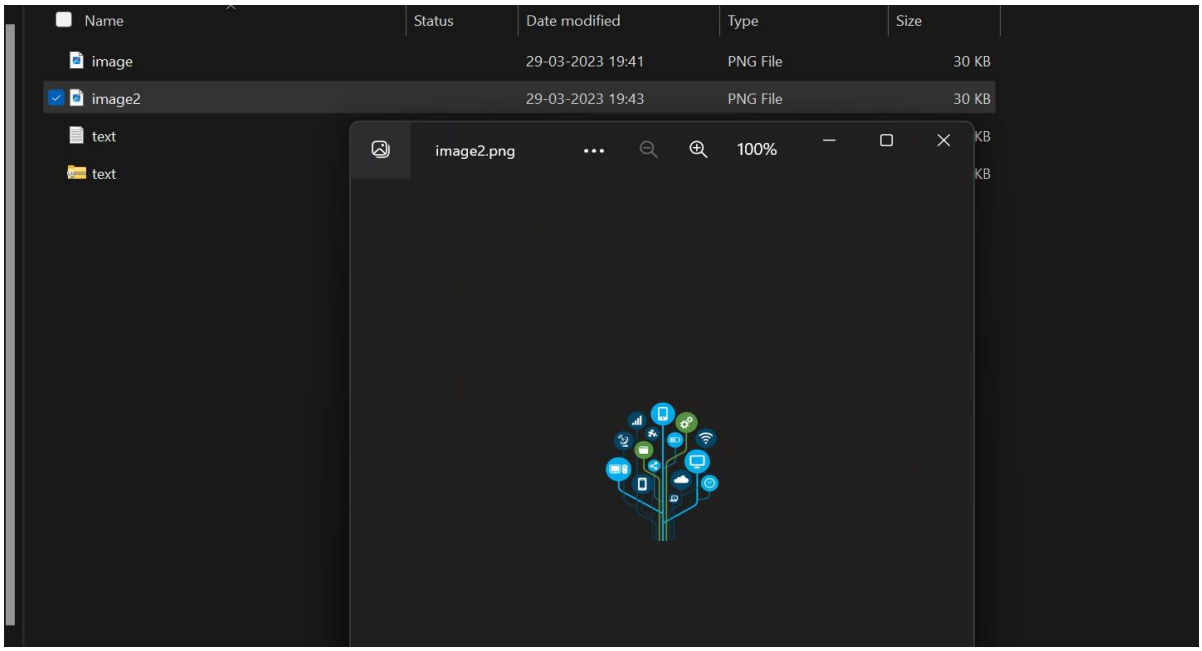


5. Open Command Prompt: Press the Windows key + R to open the Run dialog box. Type "cmd" and press Enter to open Command Prompt.
6. Change the directory: Change the directory to the location where the image and compressed file are stored. Use the "cd" command to navigate to the correct directory.
7. Merge the files: Use the following command to merge the image and compressed file: copy /b imagename.jpg + compressedfile. zip newimage.jpg . In my case we are merging image.png+text.zip file to image2.png

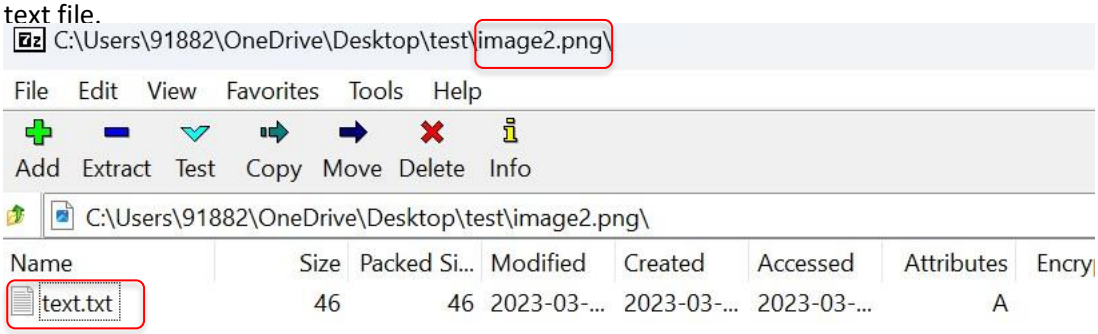
```
PS C:\Users\91882\OneDrive\Desktop\test> cmd /c 'copy /b image.png+text.zip image2.png'
image.png
text.zip
        1 file(s) copied.
PS C:\Users\91882\OneDrive\Desktop\test>
```

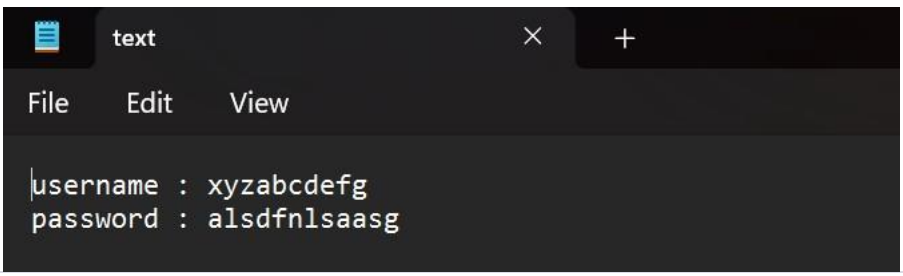
8. Check the new image: Close Command Prompt and navigate to the location where you saved the new image. Double -click it to open it and check if it opens correctly. You should not be

able to see the compressed file.



9. To access the hidden file: If you open the image2.png in 7-Zip, you should be able to see the .txt file. If you open that, you will see your text file. As shown below in screenshot , we have open the image2.png and text.txt file is hidden in it. You can open it to see the content of text file.





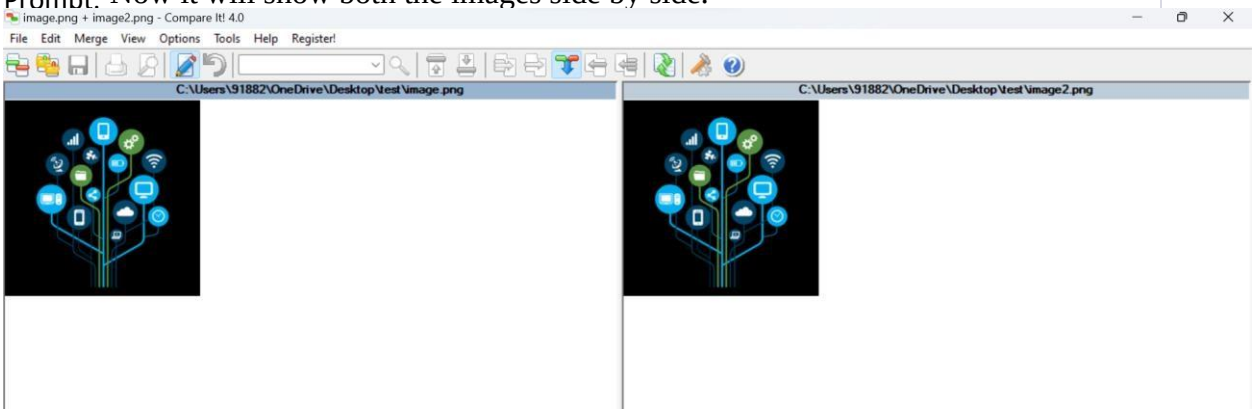
Note: Make sure to keep a backup of the original image and the compressed file in a safe location.

Using Compare It! For further analysis : -

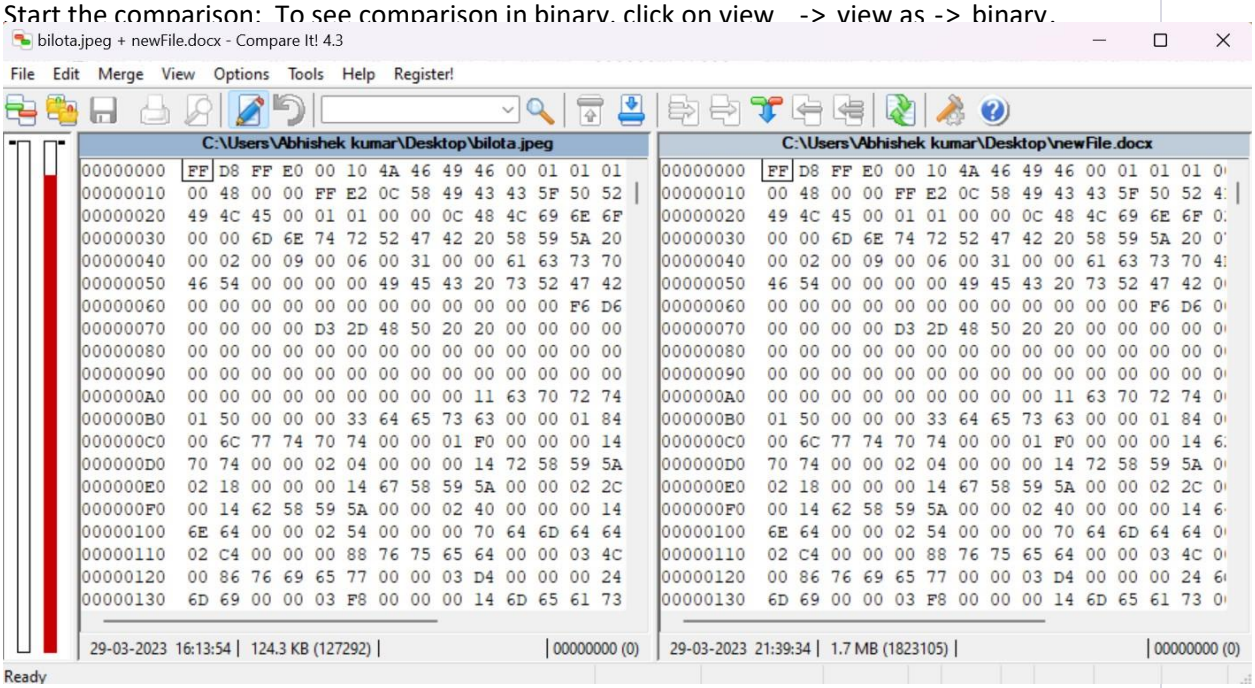
Compare It! is a software tool that allows you to compare and synchronize files and folders.

You can use it to compare the original image file and the new image file that you created using cmd . Here are the steps to use Compare It! for further analysis . To use Compare IT! software for further analysis, follow these steps:

1. Install Compare IT!: If you haven't already, download and install Compare IT! on your computer.
2. Open Compare IT!: Open Compa re IT! by double -clicking on the desktop icon or selecting it from the Start menu.
3. Select files to compare: Click on the "File" menu and select "Compare Files."
4. Choose the original image: Select the original image file that you used to hide your file.
5. Choo se the output image: Select the output image file that you created using Command Prompt. Now it will show both the images side by side.



6. Start the comparison: To see comparison in binary, click on view -> view as -> binary.



7. Analyze the results: Once the comparison process is complete, Compare IT! will display the results in a side -by-side view, highlighting the differences between the two images. You can analyze the differences in detail and decide how they differ from each other.

By comparing the original image file and the output image file created using Command Prompt, Compare IT! can help you identify any changes or modifications made to the image during the process of hiding the file behind it. This can help you determine if the image has been tampered with or modified in any way.

Practical - 14

Q). Study the John the ripper framework for Examining the encrypted file

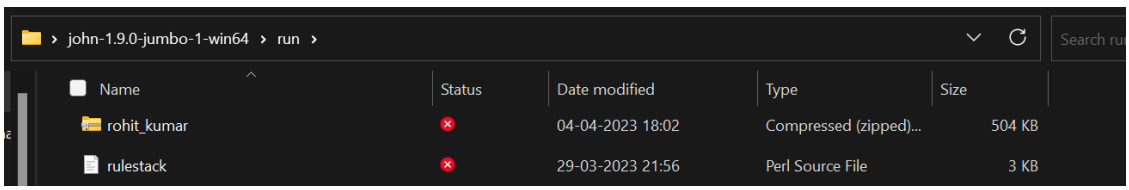
John the Ripper is a powerful open-source password cracking tool that can be used to examine and crack encrypted files. It is capable of cracking passwords for various operating systems, file formats, and encryption algorithms.

Procedure:

1.) Install John the Ripper on your system. You can download it from the official website at https://www.openwall.com/john/.

2.) Open the installed zip file of john the ripper and extract it to desktop .

3.)Place a password protected zip file in the sub-folder “run” which is present in the folder where we have extracted the john the ripper framework. Don’t select a zipped file with very strong password as it may take very long time to crack based on the computational capacity of your PC.



("rohit_kumar" is our password protected zip file).

4.) Now in "run" subfolder you will see many files and folders that can be used to decrypt a file we need to access this file using cmd.

To access john using cmd

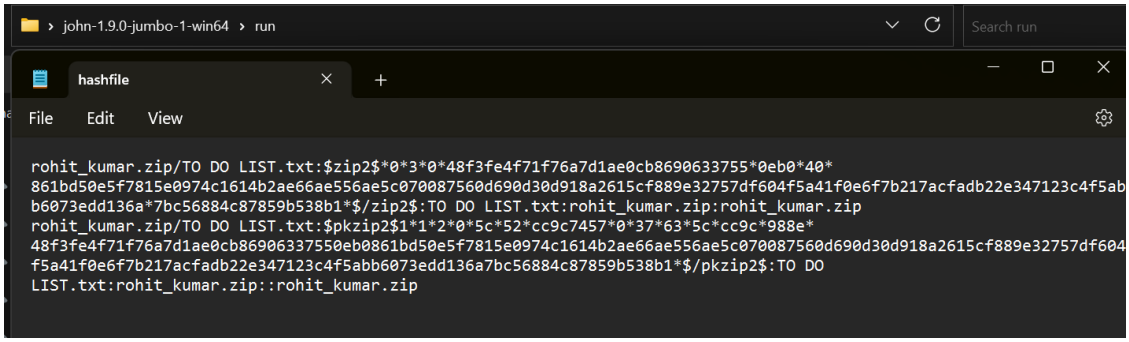
-> open cmd in run as administrator mode
-> then type cd [location of "run" file of john the ripper folder]
-> type john to see if its working or not

Now, we successfully accessed the john using cmd , lets see how to decrypt the encrypted file to examine its content

4.) First create a text file which contains the hash value. Use the command: zip2john.exe rohit_kumar.zip > hashfile.txt.

Hash file is very important file to crack the password

5.) The hashfile.txt will be stored in same folder where zip file is stored (i.e. in "run" folder)



6.) To crack the password of the zipped file, we have to analyze the hashfile.txt file. Write the following command to crack the password: “john.exe --format=zip rohit_kumar.zip hashfile.txt”.

Where

rohit_kumar.zip -> is the name of the zip file

hashfile.txt -> contains the generated hash value

"rohit" is the password of our protected zip file

7.) So now password is cracked you can use it to open and examine the content of encrypted file