

# PRACTICAL 1

## Aim : Creating a Forensic Image using FTK Imager/Encase Imager

- a) Creating Forensic Image
- b) Check Integrity of Data
- c) Analyze Forensic Image

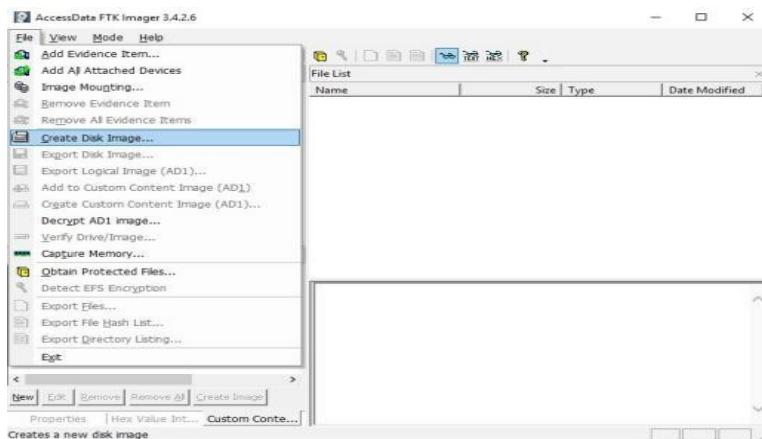
### Note:-

**Before creating the disk image you need to create Two folders on the system and Name them as Input and Output Respectively**

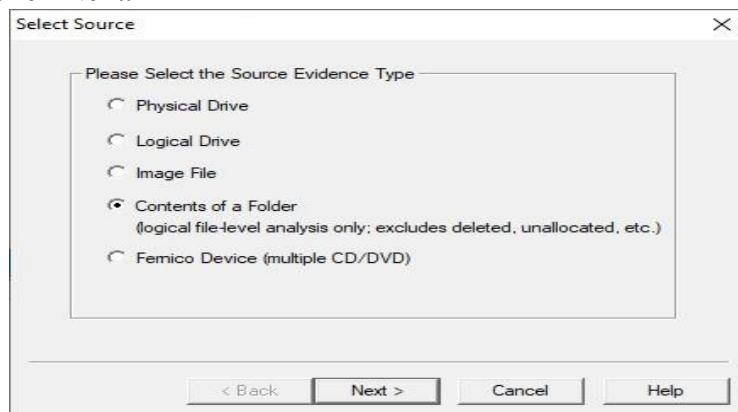
### Steps :

#### a) Creating Forensic Image

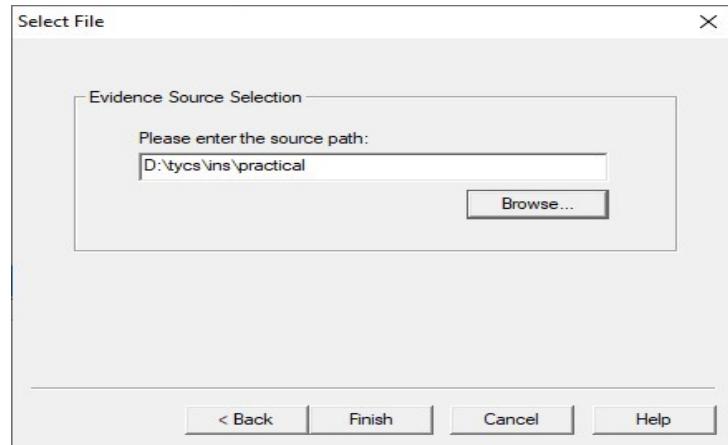
1. Click File, and then Create Disk Image, or click the button on the tool bar.



2. Select the source evidence type you want to make an image of (Select Content of a folder)and click Next.



3. Select the source evidence file with path .(Select the input Folder which you created)



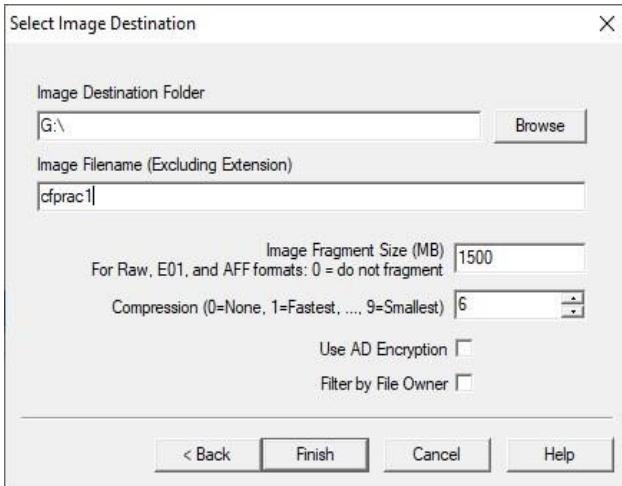
4. Click on “add” to add image destination

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

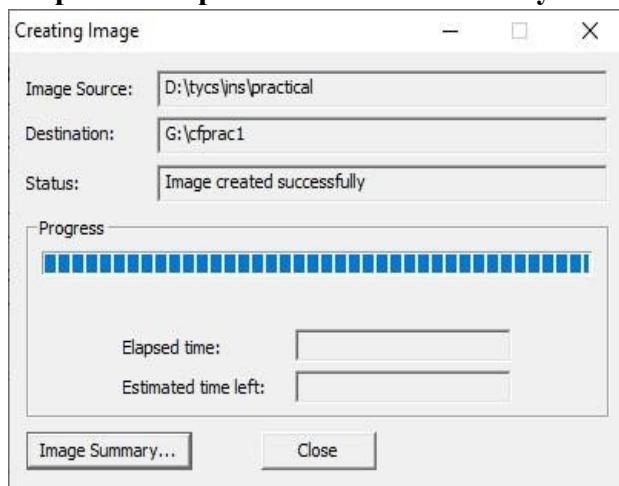
**Note:** If the destination folder you select is on a drive that does not have sufficient

free space to store the entire image file, FTK Imager prompts for a new destination folder when all available space has been used in the first location.

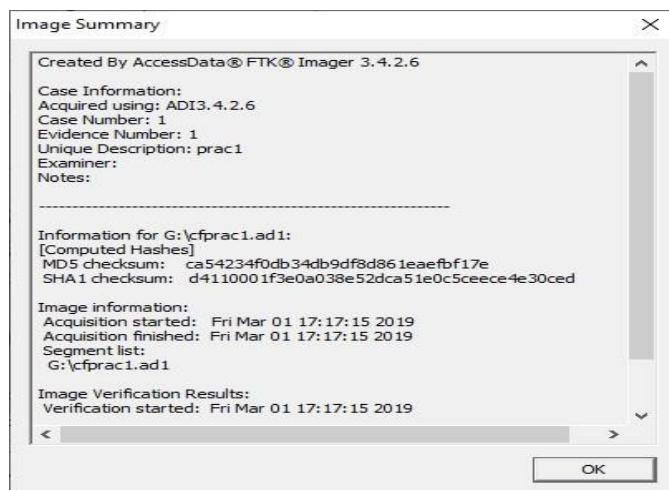
5. In the Image Filename field, specify a name for the image file but do not specify a file extension.



6. After adding the image destination path click on finish and start the image processing.  
**(Here Select the output folder path to Store the recovery file in it)**

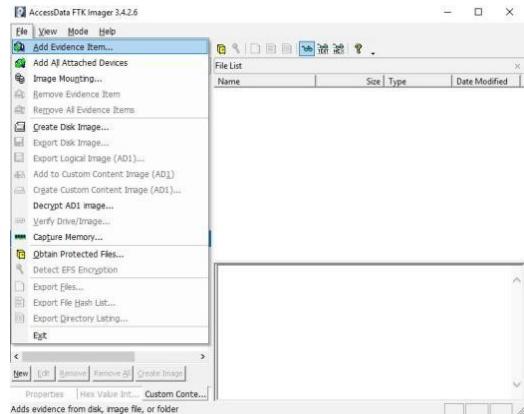


7. After the images are successfully created, click Image Summary to view detailed file information, including MD5 and SHA1 checksums.

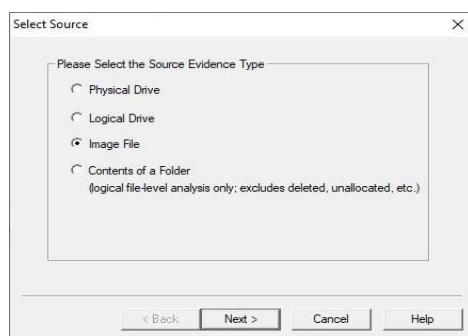


**b) Analyze Forensic Image:**

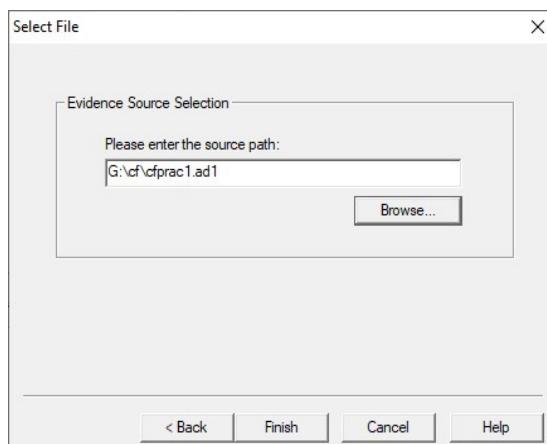
- a) Click on Add Evidence Item to add evidence from disk, image file or folder.



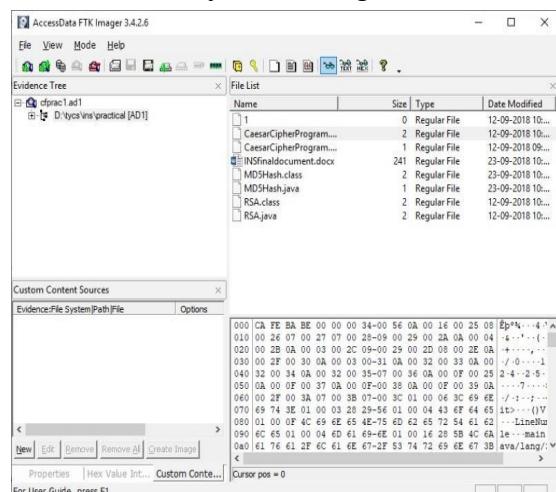
- b) Now select the source evidence type as image file.



- c) Open the created evidence image file



- d) Now select Evidence Tree and analyze the image file.



## PRACTICAL 2

### Aim : Data Acquisition

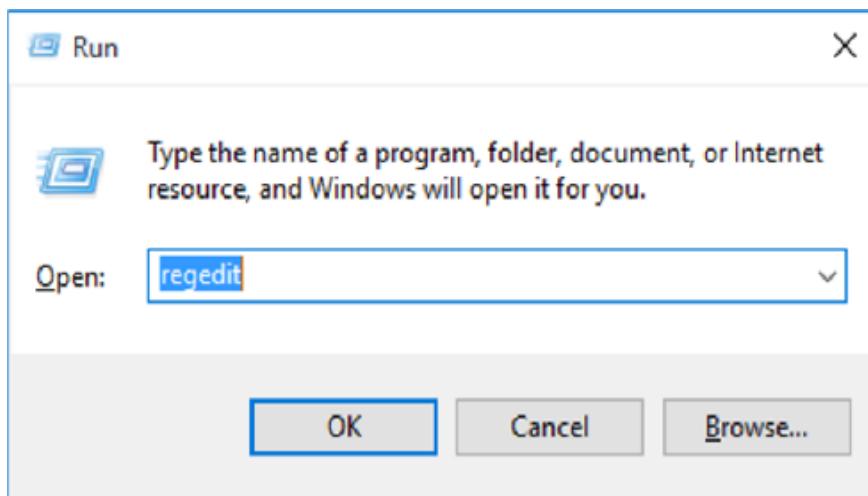
Perform data acquisition using:

- USB Write Blocker + FTK Imager

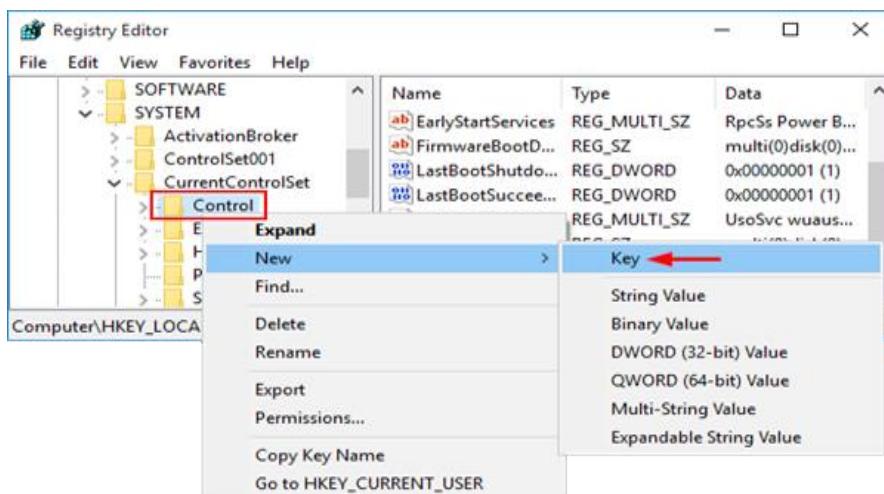
### Steps :

Enable USB Write Block in Windows 10, 8 and 7 using registry

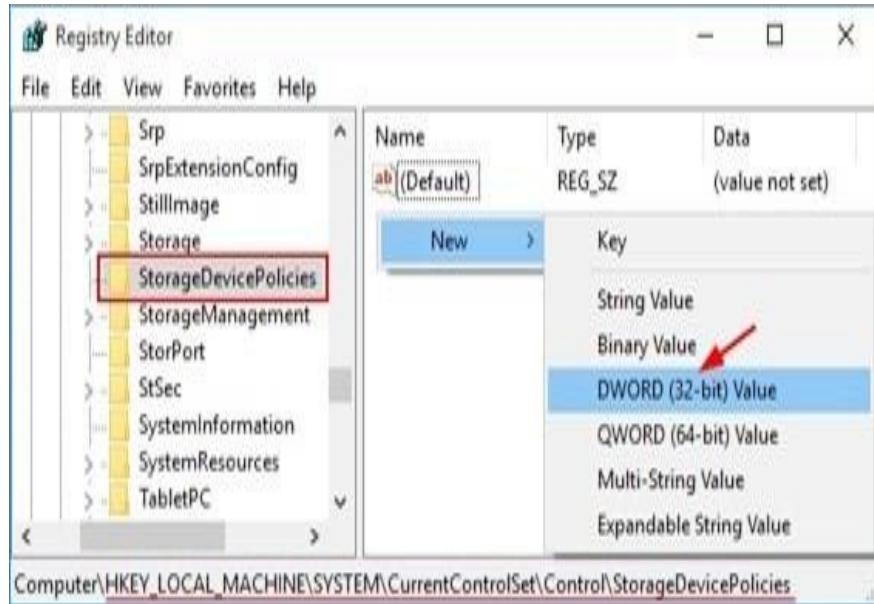
1. Press the Windows key + R to open the Run box. Type regedit and press Enter.



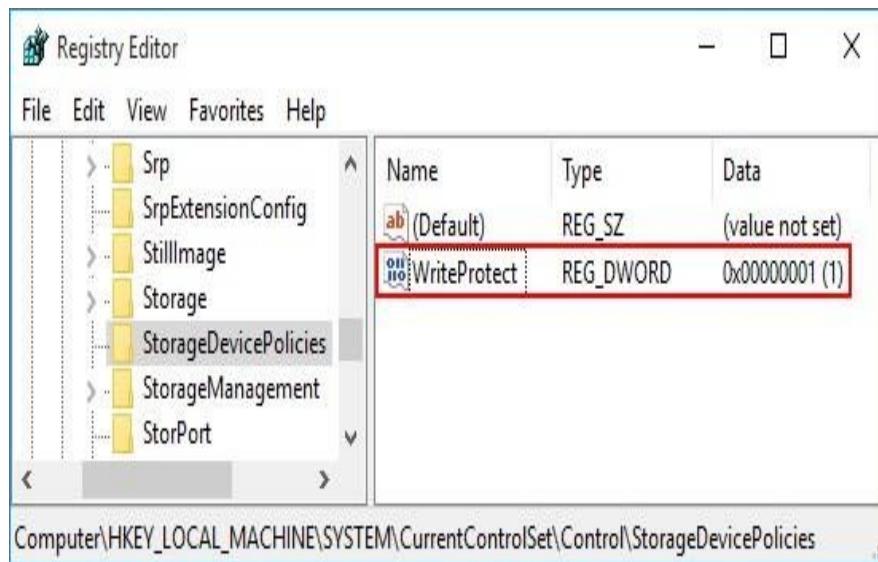
2. This will open the Registry Editor. Navigate to the following key:  
HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control
3. Right-click on the **Control** key in the left pane, select New -> Key.
4. Name it as StorageDevicePolicies



5. Select the StorageDevicePolicies key in the left pane, then right-click on any empty space in the right pane and select **New > DWORD (32-bit) Value**. Name it WriteProtect



6. Double-click on WriteProtect and then change the value data from 0 to 1.

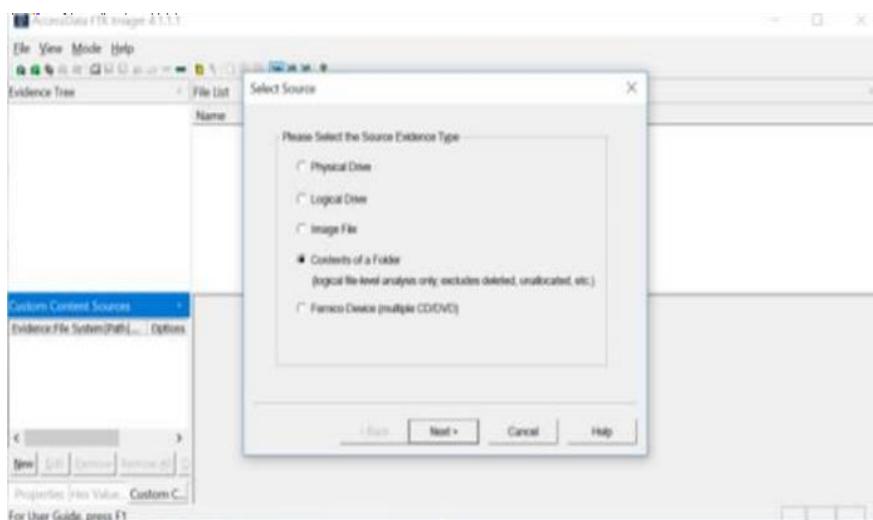


7. The new setting takes effect immediately. Every user who tries to copy / move data to USB devices or format USB drive will get the error message “*The disk is write-protected*”.
8. We can only open the file in the USB drive for reading, but it’s not allowed to modify and save the changes back to USB drive.



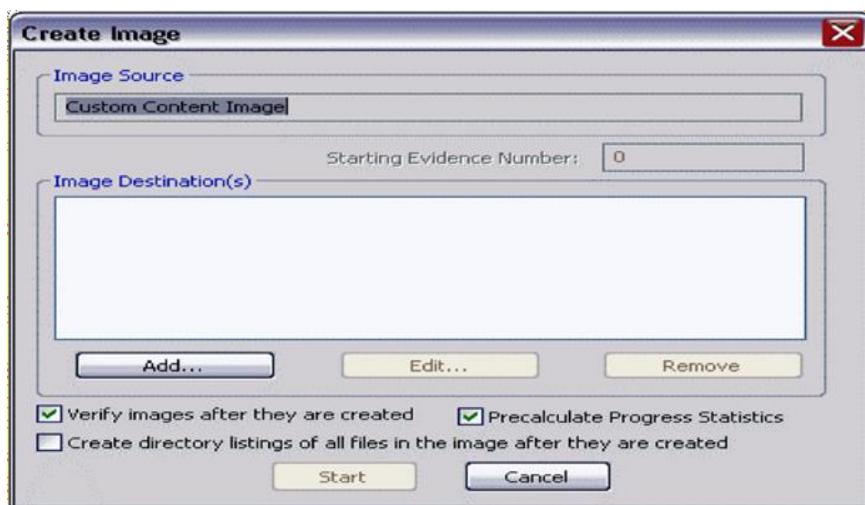
So this is how you can enable write protection to all connected USB drives. If you want to disable write protection at a later time, just open Registry Editor and set the WriteProtect value to 0.

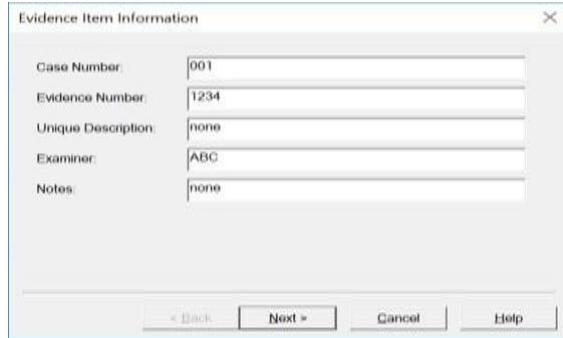
#### 9. Now Create image of the USB drive using FTK imager



10. Select the USB drive folder by browsing and click next & Finish.

11. In the Create Image dialog, click Add.





- You can compare the stored hashes of your image content by checking the Verify images after they are created box. If a file doesn't have a hash, this option will generate one.
- You can list the entire contents of your images with path, creation dates, whether files were deleted, and other metadata. The list is saved in a tab-separated value format

12. Select the type of image you want to create, and then click Next

Two overlapping dialog boxes. The top one is 'Select Image Destination' with fields for 'Image Destination Folder' (C:\Users\Kauser\Desktop), 'Image Filename (Excluding Extension)' (left empty), 'Image Fragment Size (MB)' (1500), 'Compression (0=None, 1=Fastest, ..., 9=Smallest)' (3), and checkboxes for 'Use AD Encryption' and 'Filter by File Owner'. The bottom one is 'Creating Image...' showing 'Image Source' (E:\), 'Destination' (C:\Users\Kauser\Desktop\blah), 'Status' ('Creating image...'), a progress bar at 100%, 'Elapsed time' (0:00:05), and an 'Estimated time left' field (empty). Both dialogs have '&lt; Back', 'Finish', 'Cancel', and 'Help' buttons at the bottom.

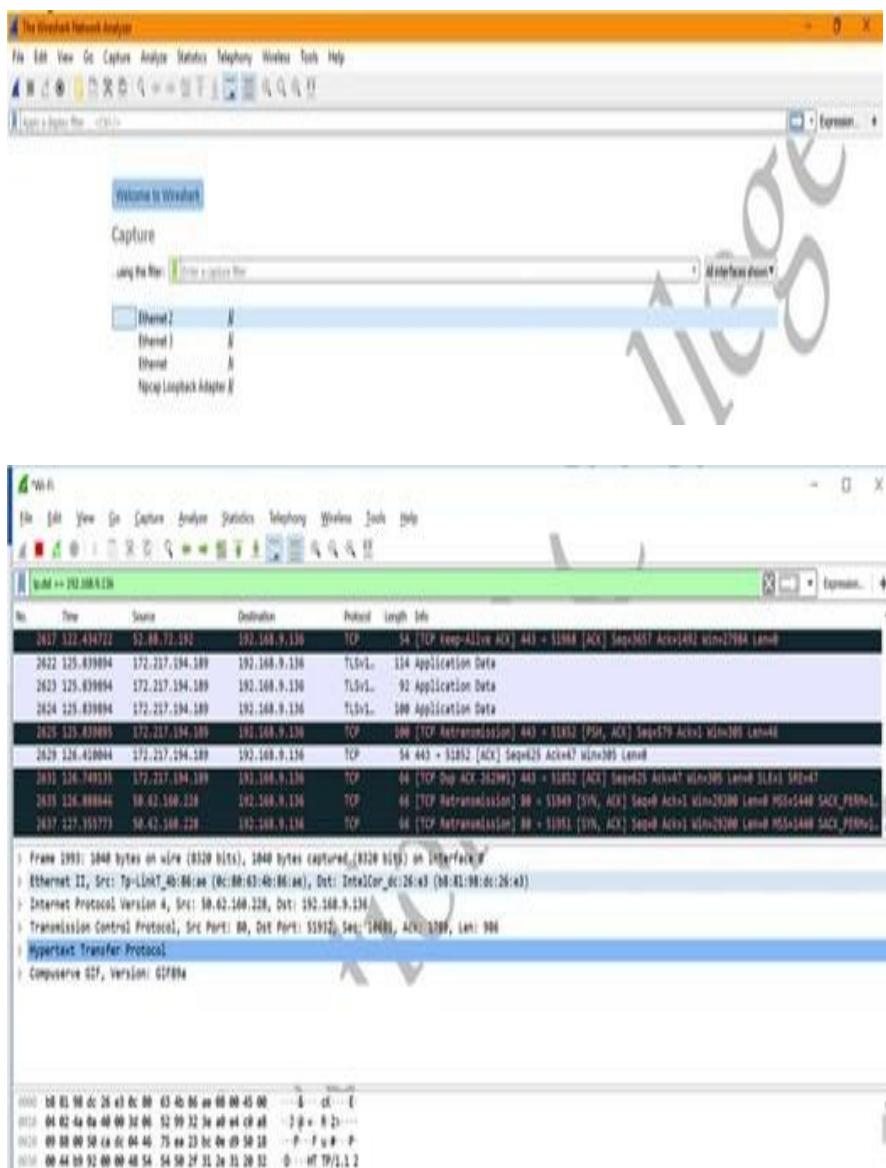
## PRACTICAL 3

### Aim : Capturing and analyzing network packets using Wireshark.

- a) Identification the live network
- b) Capture Packets
- c) Analyze the captured packets

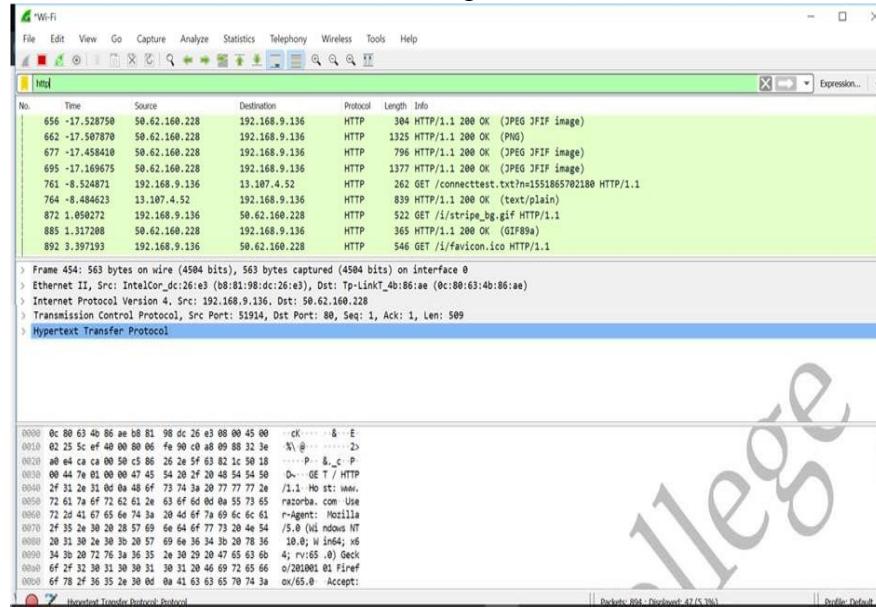
### Steps :

5. Open Wireshark and click on Ethernet.

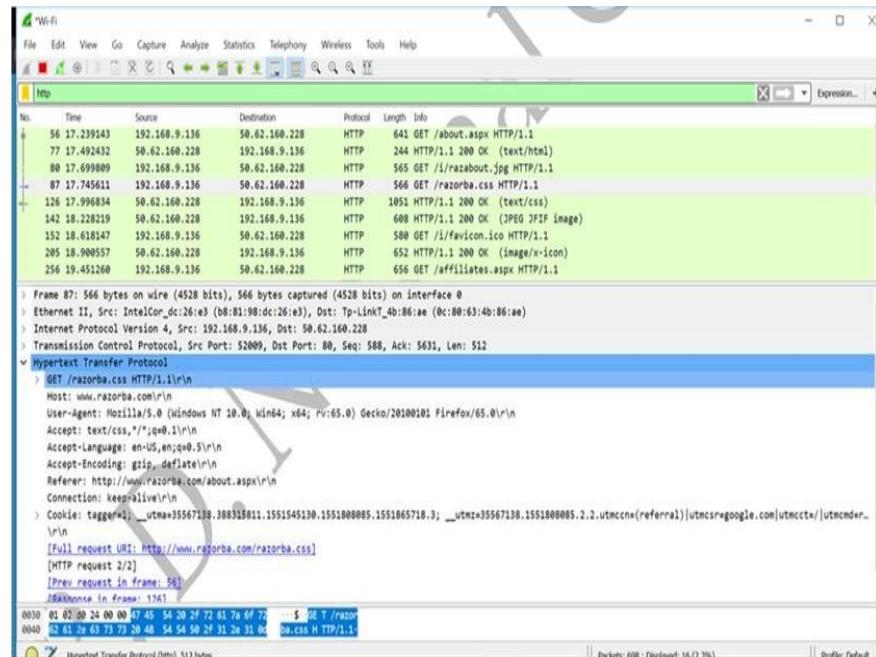


6. Now go on browser and open any unsecured website i.e and perform some activity on the website.

7. Now come back to Wireshark and enter http in the search bar



8. Now click on the get request and see the details.



## **PRACTICAL 4**

### **Aim : Using Sysinternals tools for Network Tracking and Process Monitoring:**

- a) Check Sysinternals tools
- b) Monitor Live Processes
- c) Capture RAM
- d) Capture TCP/UDP packets
- e) Monitor Hard Disk
- f) Monitor Virtual Memory
- g) Monitor Cache Memory

### **Steps :**

- a) **Check Sysinternals tools:** Windows Sysinternals tools are utilities to manage, diagnose, troubleshoot, and monitor a Microsoft Windows environment.

The following are the categories of Sysinternals Tools:

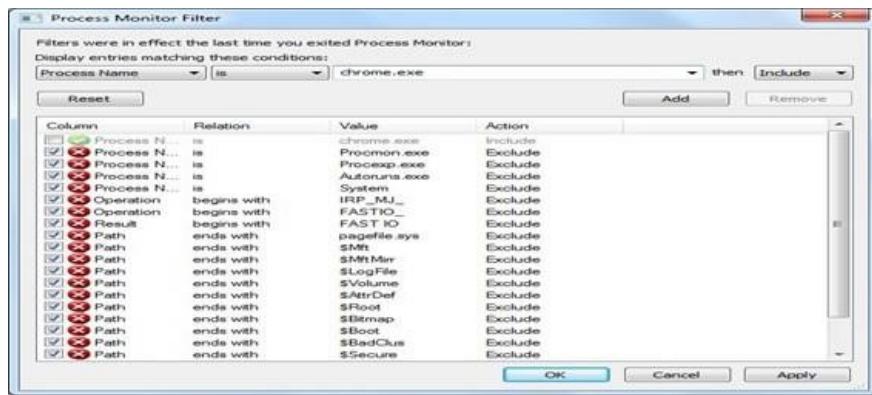
- 1. File and Disk Utilities
- 2. Networking Utilities
- 3. Process Utilities
- 4. Security Utilities
- 5. System Information Utilities
- 6. Miscellaneous Utilities

- b) **Monitor Live Process:(Tool: ProMon)**

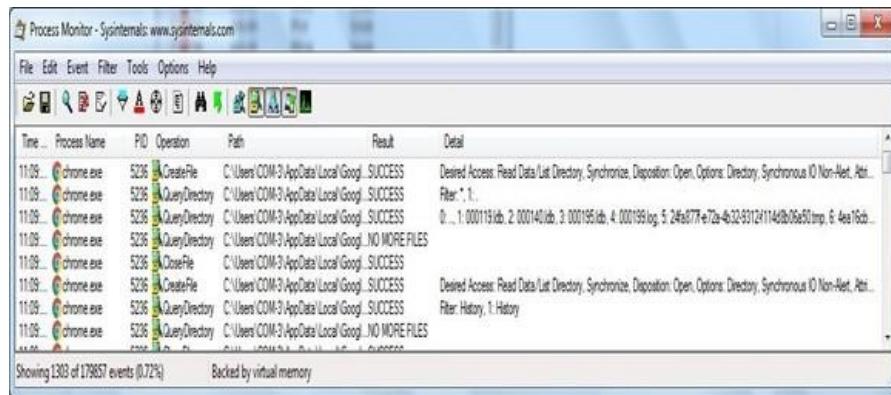
#### **To Do:**

- 1. Filter (Process Name or PID or Architecture, etc)
- 2. Process Tree
- 3. Process Activity Summary
- 4. Count Occurrences

#### **Output:**



1. Click on Tools → Select Process tree → Close



2. Tools → Count Occurrence → Click on Count



File Summary											
Files accessed during trace:											
	Total Events	Opens	Closes	Reads	Writes	Read B...	Write B...	Get ACL	Set ACL	Other	Path
0.3561587	1290	260	228	80	26	79652862	354084	44	4	648	<Total>
0.0290599	93	5	5	76	0	79479792	0	0	0	7	C:\Program Files\Google\Chrome\Ap...
0.0060401	60	20	20	0	0	0	0	10	0	10	C:\Users\COM-3\AppData\Local\Low...
0.0013114	53	18	18	0	0	0	0	4	0	13	C:\Users\COM-3\AppData\Local\Ge...
0.0004203	35	7	7	0	0	0	0	0	0	21	C:\Windows\System32\vm32.dll
0.0421016	28	5	4	0	2	0	79807	4	1	12	C:\Users\COM-3\AppData\Local\Ge...
0.0420233	28	5	4	0	2	0	40662	4	1	12	C:\Users\COM-3\AppData\Local\Ge...
0.0429107	28	5	4	0	2	0	153666	4	1	12	C:\Users\COM-3\AppData\Local\Ge...
0.1282037	28	5	4	0	2	0	29807	4	1	12	C:\Users\COM-3\AppData\Local\Ge...
0.0002293	23	4	4	0	0	0	0	0	0	15	C:\Program Files\Google\Chrome\Ap...

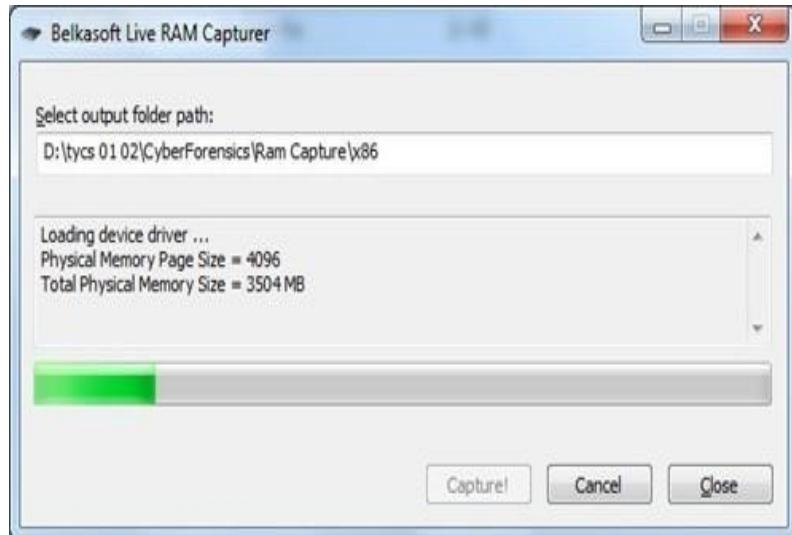
Filter... 147 file paths Save... OK

### c) Capture RAM(Tools: RAMCapture):

#### To Do:

1. Click Capture
2. Creates a .mem file of the system memory (RAM) utilized.
3. Process Activity  
SummaryCount Occurrences

#### Output:



### d) Capture TCP/UDP packets (Tool; TCPview):

#### To Do:

1. Save to .txt file.
2. Whois

#### Output:

TOPView - Systematic www.sysinternals.com

File Options Process View Help

A → □

Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets	Sent Bytes	Recv Packets	Recv Bytes
System Process_0	0	TCP	CS-11-PC	1523	localhost	9000	TIME_WAIT				
System Process_0	0	TCP	CS-11-PC	9599	localhost	1521	TIME_WAIT				
System Process_0	0	TCP	CS-11-PC	9601	localhost	1521	TIME_WAIT				
System Process_0	0	TCP	CS-11-PC	1521	localhost	9000	TIME_WAIT				
accservice.exe	2044	TCP	CS-11-PC	62125	CS-11-PC	0	LISTENING				
accservice.exe	2044	TCP	cs-11-pc	9571	scsi12-20-151-2	8000	ESTABLISHED	1	544	1	
chrome.exe	526	TCP	cs-11-PC	9591	192.168.1.108	5228	ESTABLISHED				
chrome.exe	526	UDP	CS-11-PC	5263	-	-	-				
chrome.exe	526	UDP	CS-11-PC	5263	-	-	-				
chrome.exe	526	UDP	CS-11-PC	5263	-	-	-				
chrome.exe	526	UDP	CS-11-PC	5263	-	-	-				
chrome.exe	526	UDP	CS-11-PC	5263	-	-	-				
chrome.exe	526	UDP	CS-11-PC	5263	-	-	-				
chrome.exe	526	UDP	cs-11-pc	5263	-	-	-				
chrome.exe	526	UDP	cs-11-pc	5263	-	-	-				
chrome.exe	526	UDP	cs-11-pc	5263	-	-	-				
chrome.exe	526	UDP	cs-11-pc	5263	-	-	-				
chromedriver.exe	5349	TCP	CS-11-PC	2038	CS-11-PC	0	LISTENING				
chromedriver.exe	5349	TCP	CS-11-PC	10000	CS-11-PC	0	LISTENING				
chromedriver.exe	5349	TCP	cs-11-pc	2038	cs-11-pc	0	LISTENING				
EMPROXY...	254	TCP	cs-11-pc	8962	141.64.64.27.nat.8000	8000	ESTABLISHED				
EMPROXY...	254	TCP	CS-11-PC	17430	CS-11-PC	0	LISTENING				
java.exe	5240	TCP	CS-11-PC	1038	localhost	1039	ESTABLISHED	26	26	26	
java.exe	5240	TCP	CS-11-PC	1039	localhost	1038	ESTABLISHED				
java.exe	5240	TCP	CS-11-PC	1158	CS-11-PC	0	LISTENING				
java.exe	5240	TCP	CS-11-PC	9525	CS-11-PC	0	LISTENING				
java.exe	5240	TCP	cs-11-pc	9526	cs-11-pc	0	LISTENING				

Endpoints 0 Established 9 Listening 44 Time Wait 4 Close Wait 2

Evidence Item Information

Case Number: 1

Evidence Number: 1

Unique Description: prac1

Examiner:

Notes:

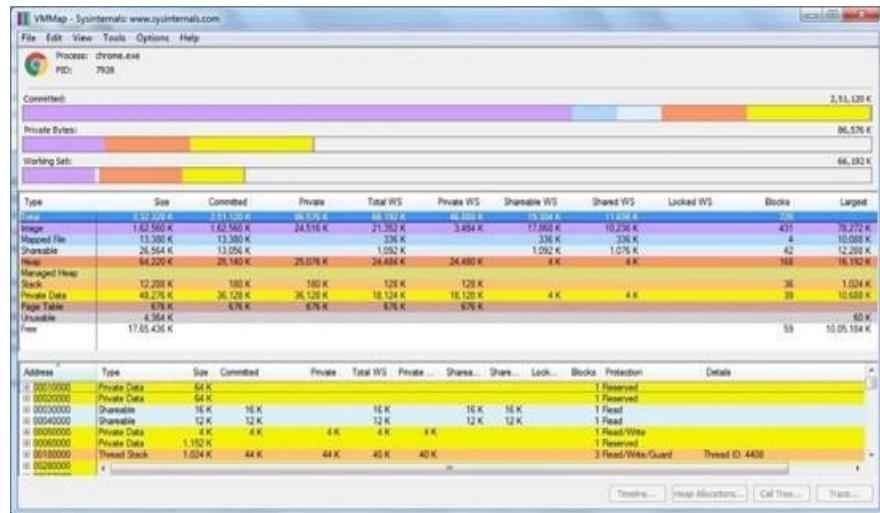
< Back Next > Cancel Help

### e) Monitor Virtual Memory (Tools: VMMap):

#### To Do:

1. Options – Show Free & UnusableRegions Check operations performed in the disk as per time and sectors affected.
2. File → Select Process e.g. chrome.exe
3. Save to .mmp file.

## Output:

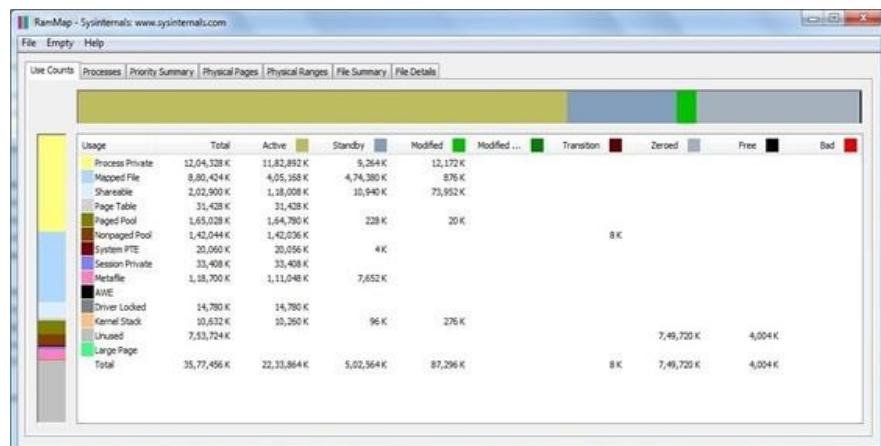


## f) Monitor Cache Memory (Tools: RAMMap):

### To Do:

- Save to .RMP file

## Output:



# PRACTICAL 5

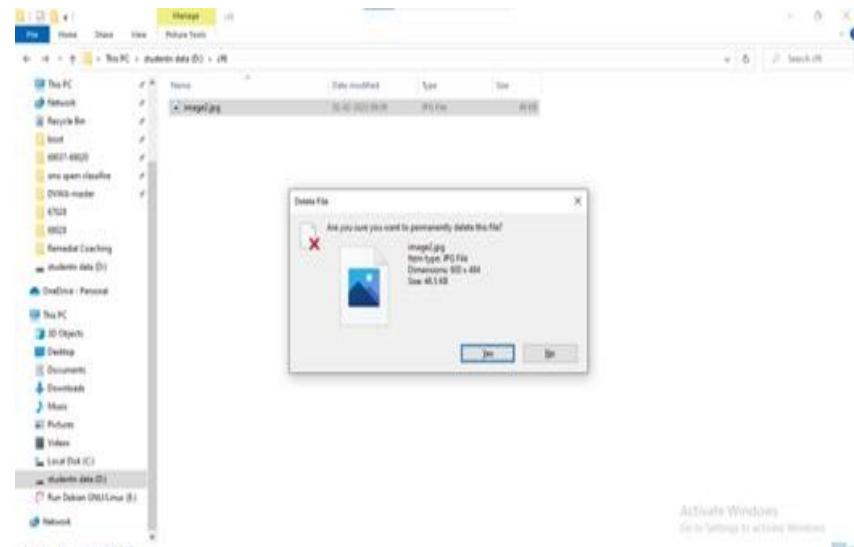
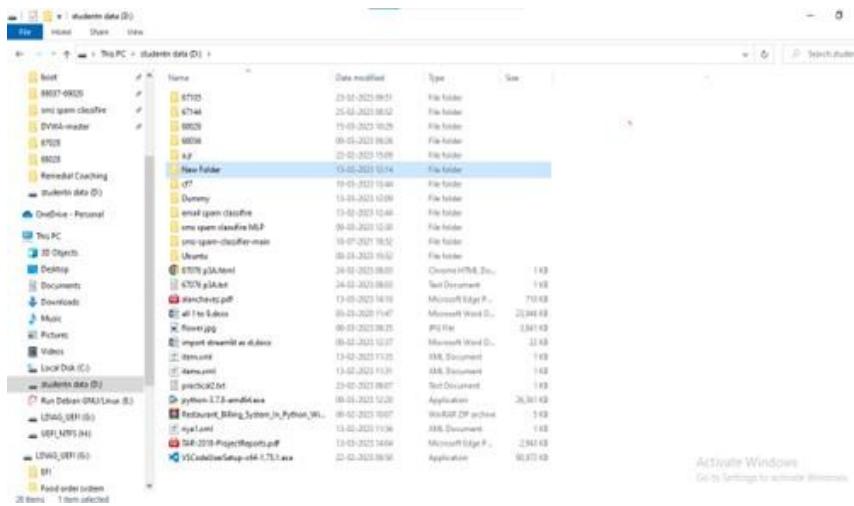
## Aim : Recovering & Inspecting Deleted files.

- a) Check for Deleted Files
- b) Recover the Deleted Files
- c) Analyzing & Inspecting the recovered files

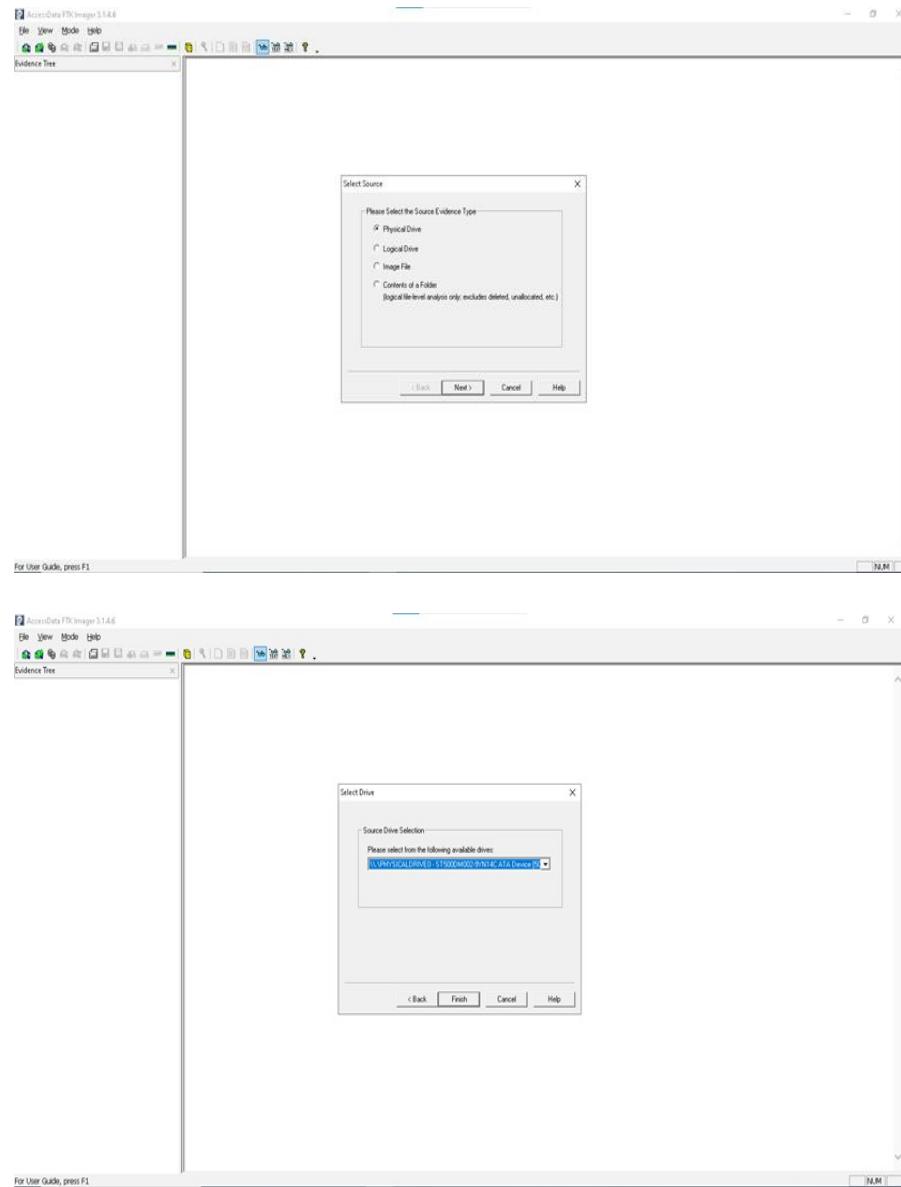
### Steps :

#### a) Creating Forensic Image

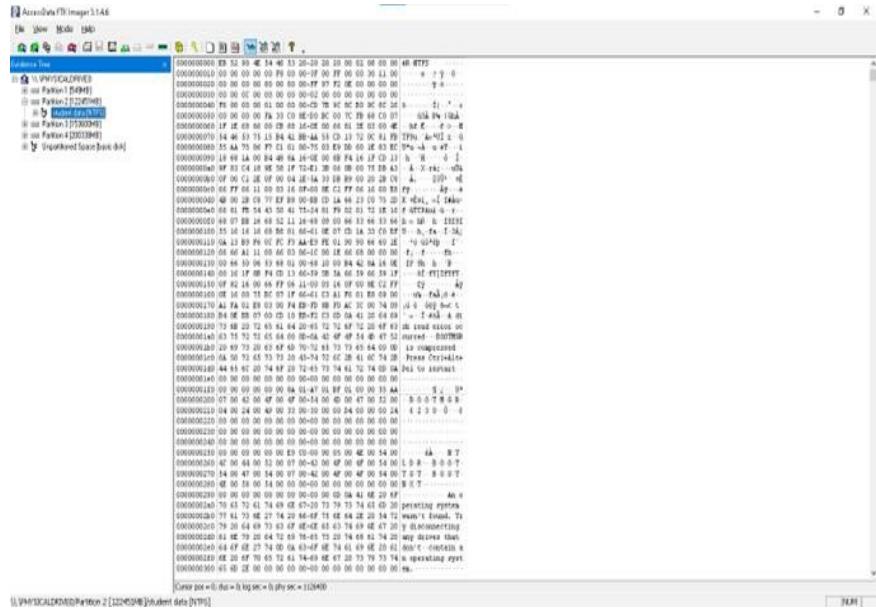
1. In CS server Create a new Folder → Copy Paste some file in it → Delete that file permanently.



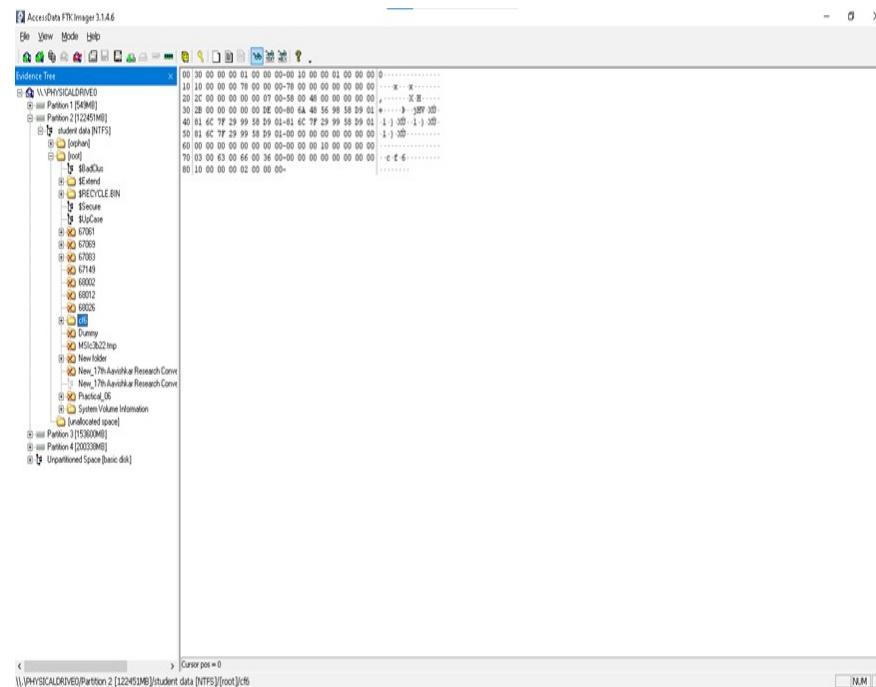
2. Open AccessData FTK Imager. Click on File → Add evidence item → PhysicalDrive → next → Keep Selected ‘Physical Drive’ → Finish



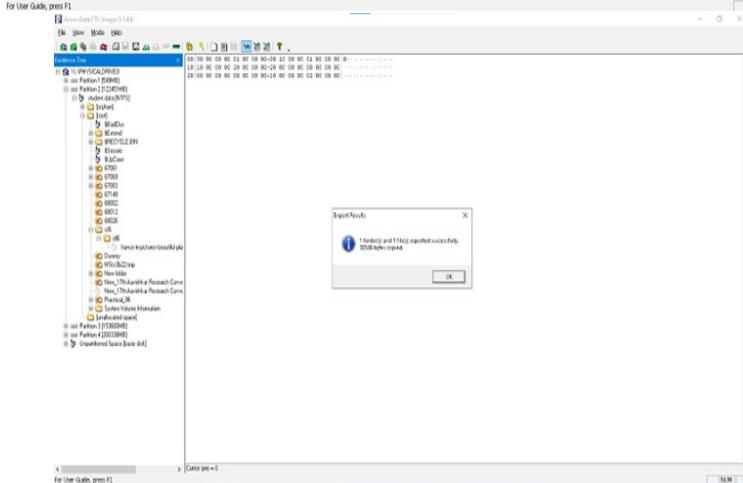
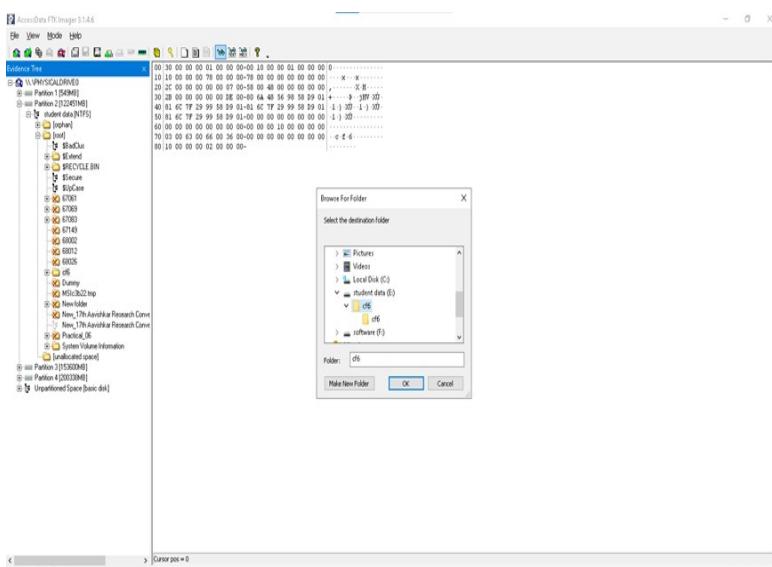
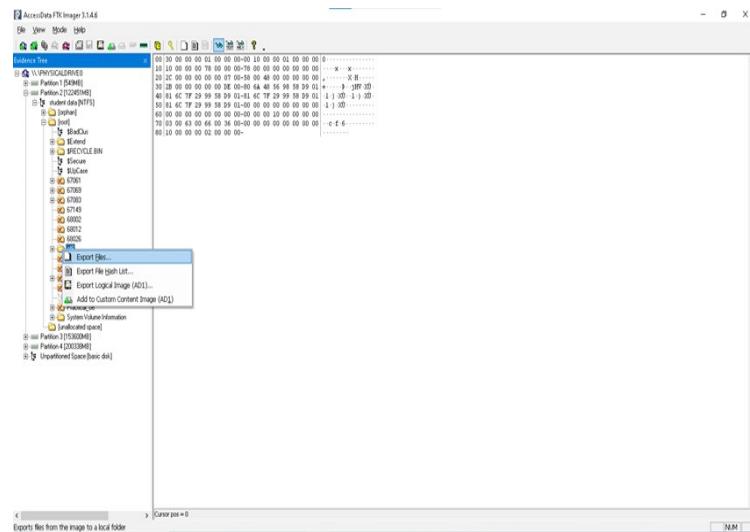
3. Evidence Tree appears and hash values
  - Now Expand evidence Tree → Then select Volume on which you have save the folder and File.
  - Now Expand (+) New Volume (NTFS) → Click on bar like loading appears & certain options appears



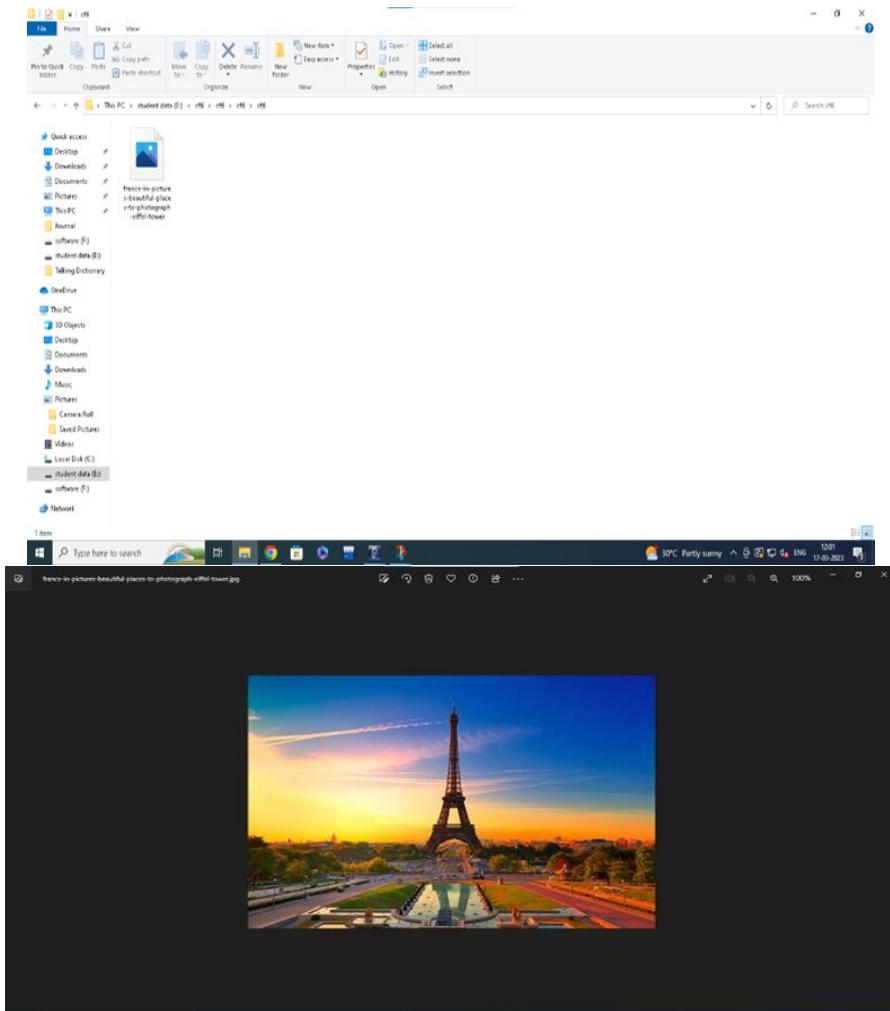
#### 4. Now expand (+) root → Select the Folder from where you have deleted file



#### 5. Right Click on the file which you want to recover → Click on Export file → Give Destination Path from Which you have deleted the file → save and Recover file → ok



6. Now browse the Folder to the folder where you saved recovered file you will file find the ‘file’ our file got recover.



## **PRACTICAL 6**

### **Aim : Mobile Device Forensics:**

- a) Perform a forensic analysis of a mobile device, such as a smartphone or tablet.
- b) Retrieve call logs, text messages, and other relevant data for investigative purposes.

### **Steps :**

#### **1. Perform a forensic analysis of a mobile device, such as a smartphone or tablet.**

1. Download maledit forensic tool in mobile.
2. Open Mobileit tool in PC



3. Click on connect.



4. Connect your mobile device to the system. Click on phone → Next



5. Click the Connection.



6. Open the mobiledit tool in phone and click on the type of connection (i.e Wifi) → Copy the IP address and enter it in the PC and click next.

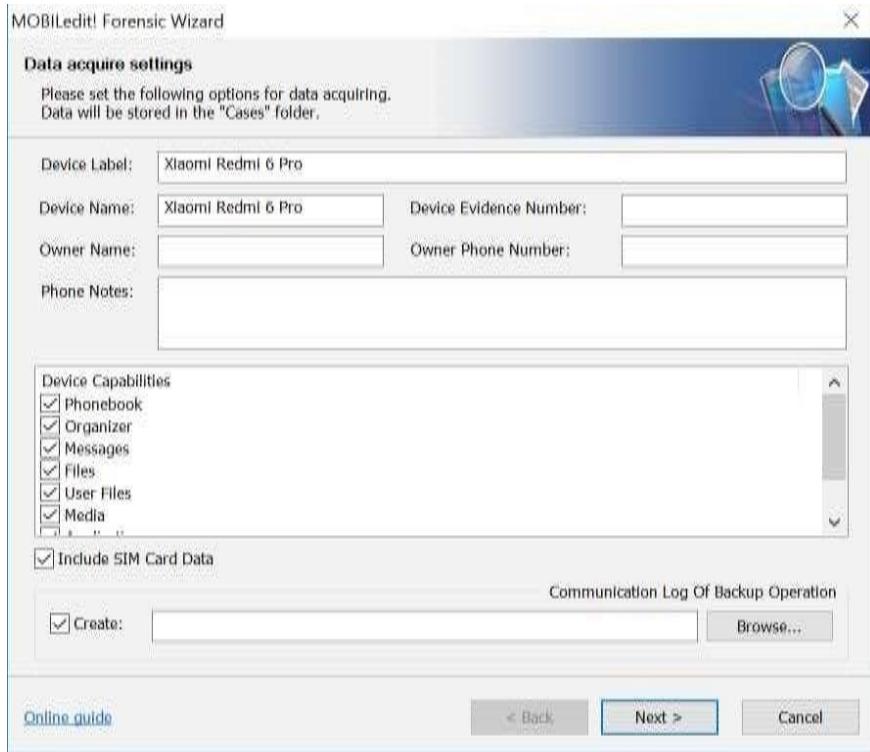


7. It shows the phone which is connected. Click on Next.

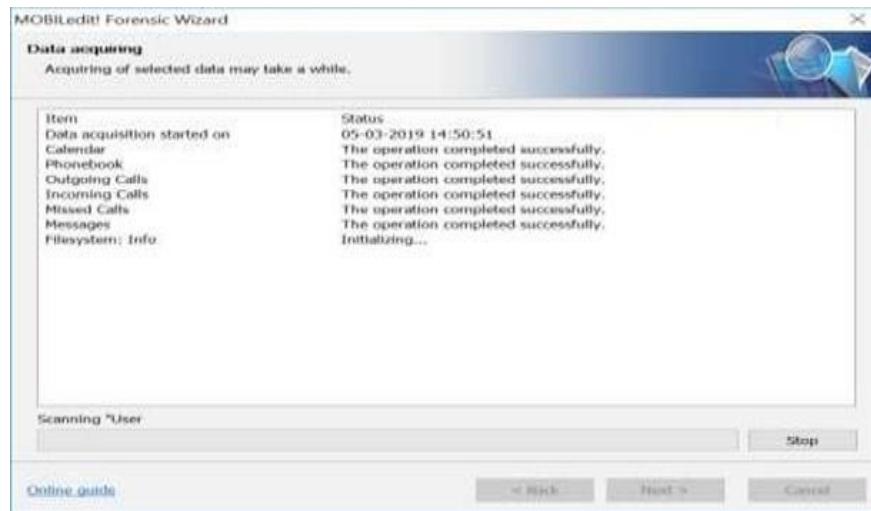
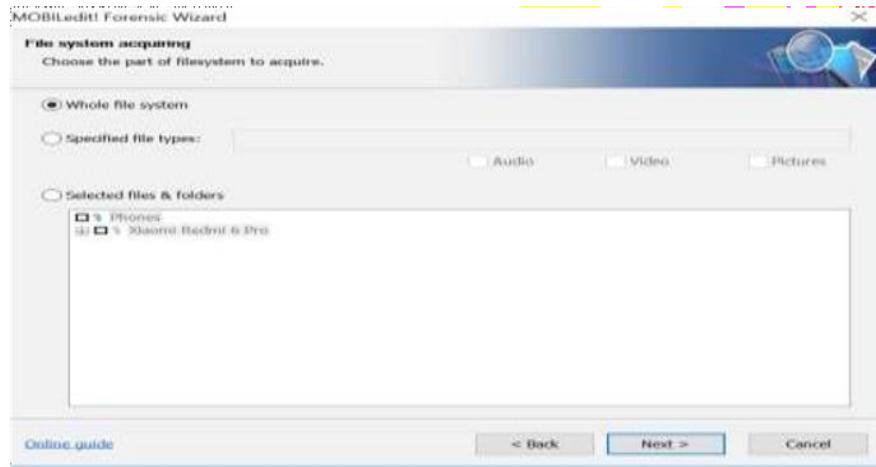


## 2. Retrieve call logs, text messages, and other relevant data for investigative purposes.

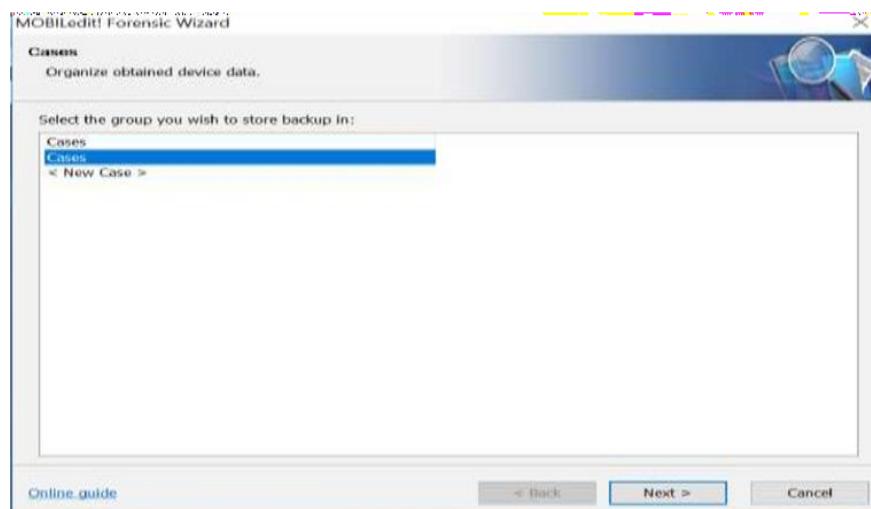
8. Click on Next.



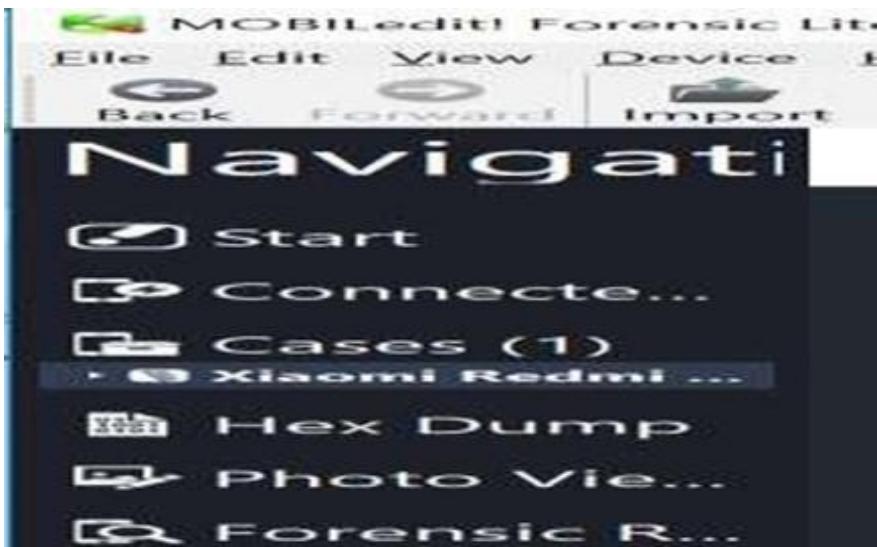
9. Click on Whole system and click Next.



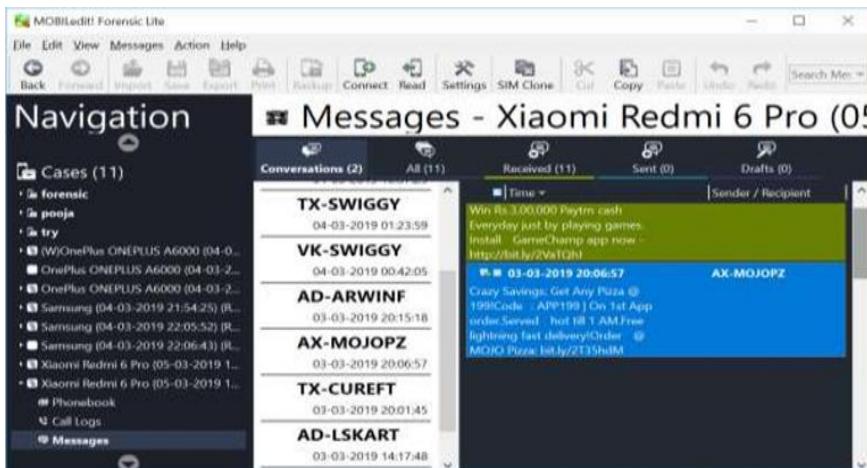
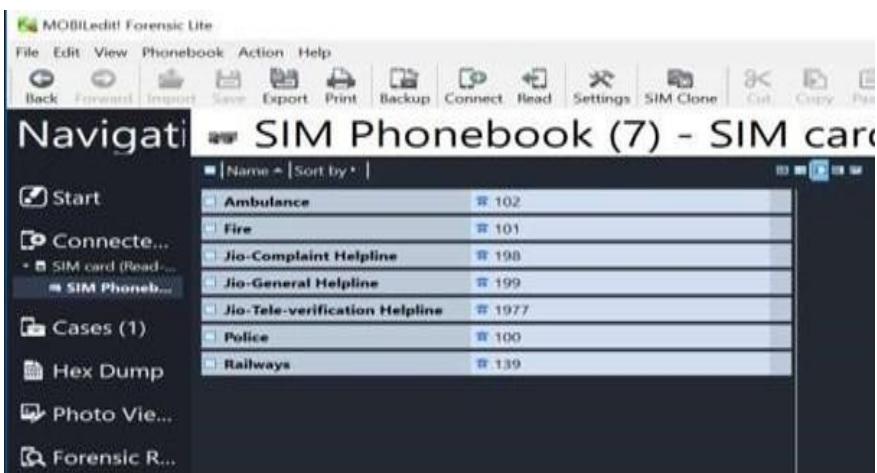
10. Click on case and click next.



11. Click on your device in the left panel.



12. You can see all the files.



## PRACTICAL 7

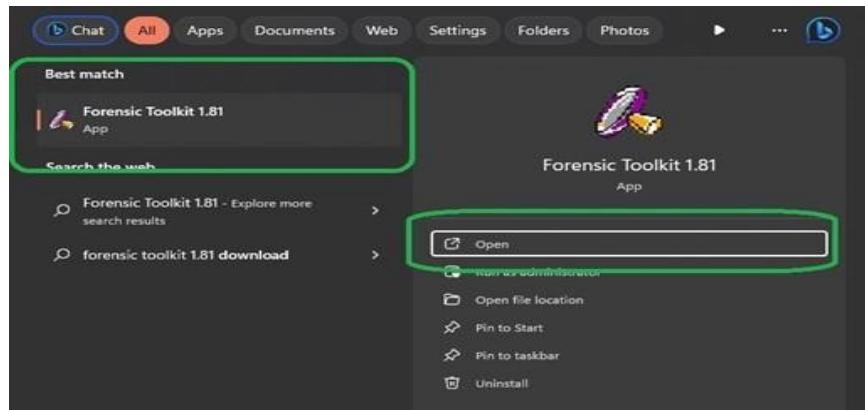
### Aim : Email Forensics:

- Analyze email headers & content to trace the origin of suspicious emails.
- Identify potential email forgeries or tampering.

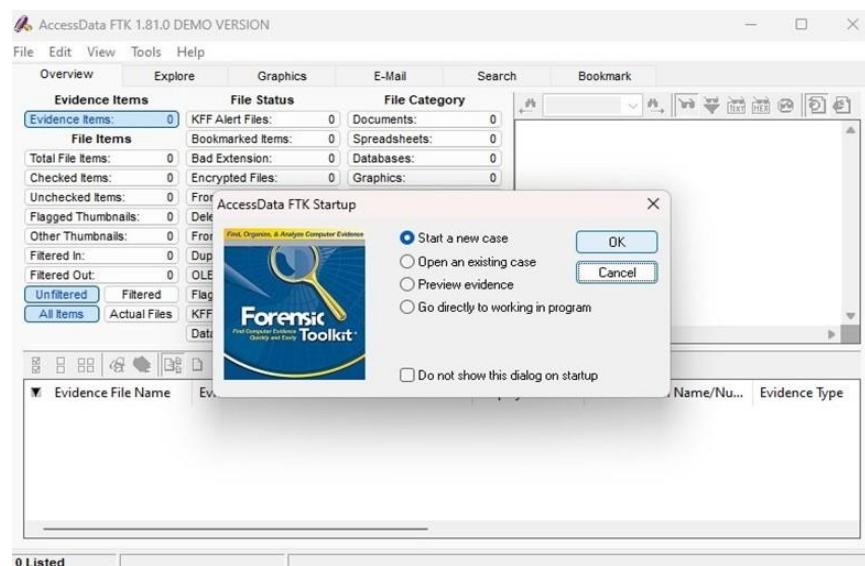
### Steps :

#### Recovering Email

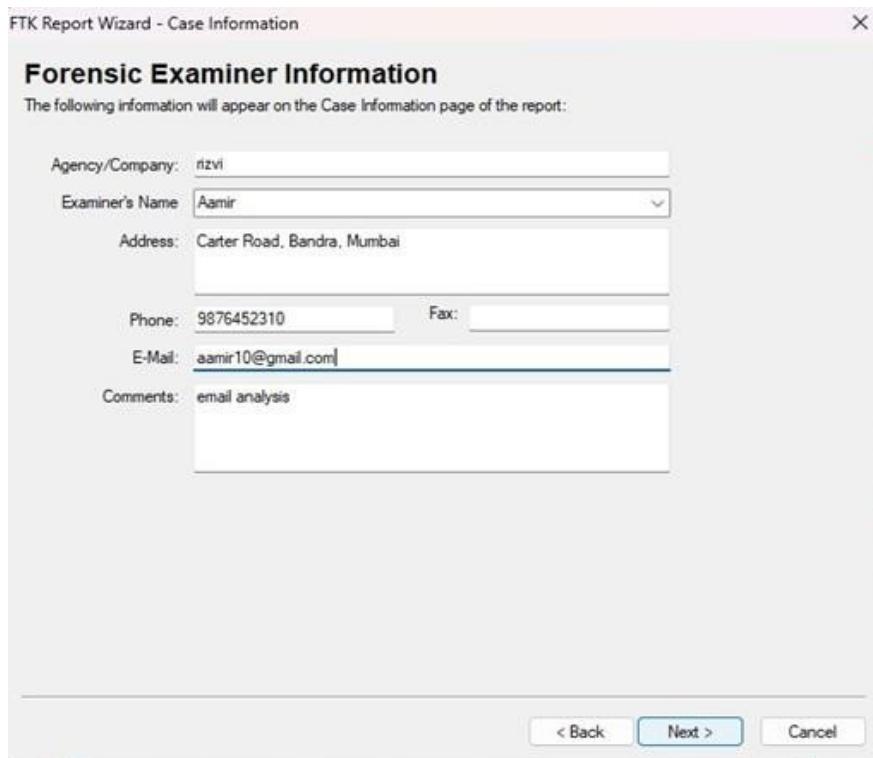
- Start AccessData FTK and click **Start a new case**, then click **OK**.
- Click **Next** until you reach the **Refine Case - Default dialog box** Click the **EmailEmphasis button**, and then click **Next**



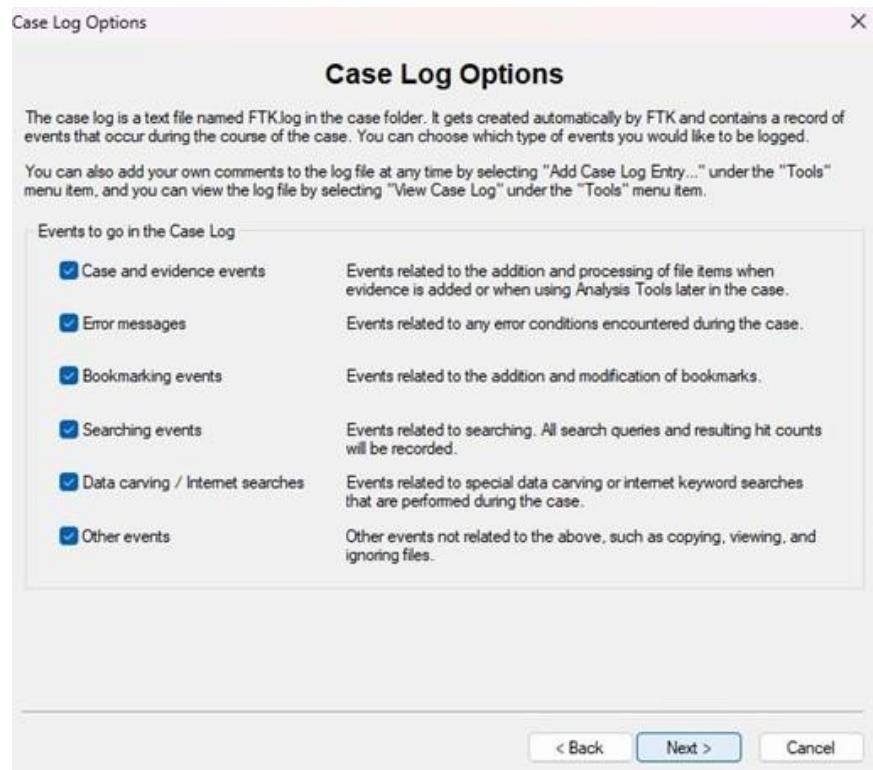
- Create a new File.



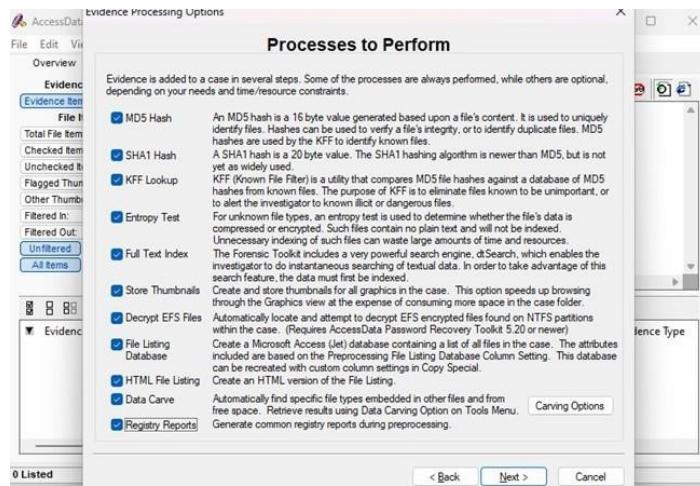
4. Fill the details of the Examiner.



5. Click on all the options and Click Next



## 6. Select all the options.



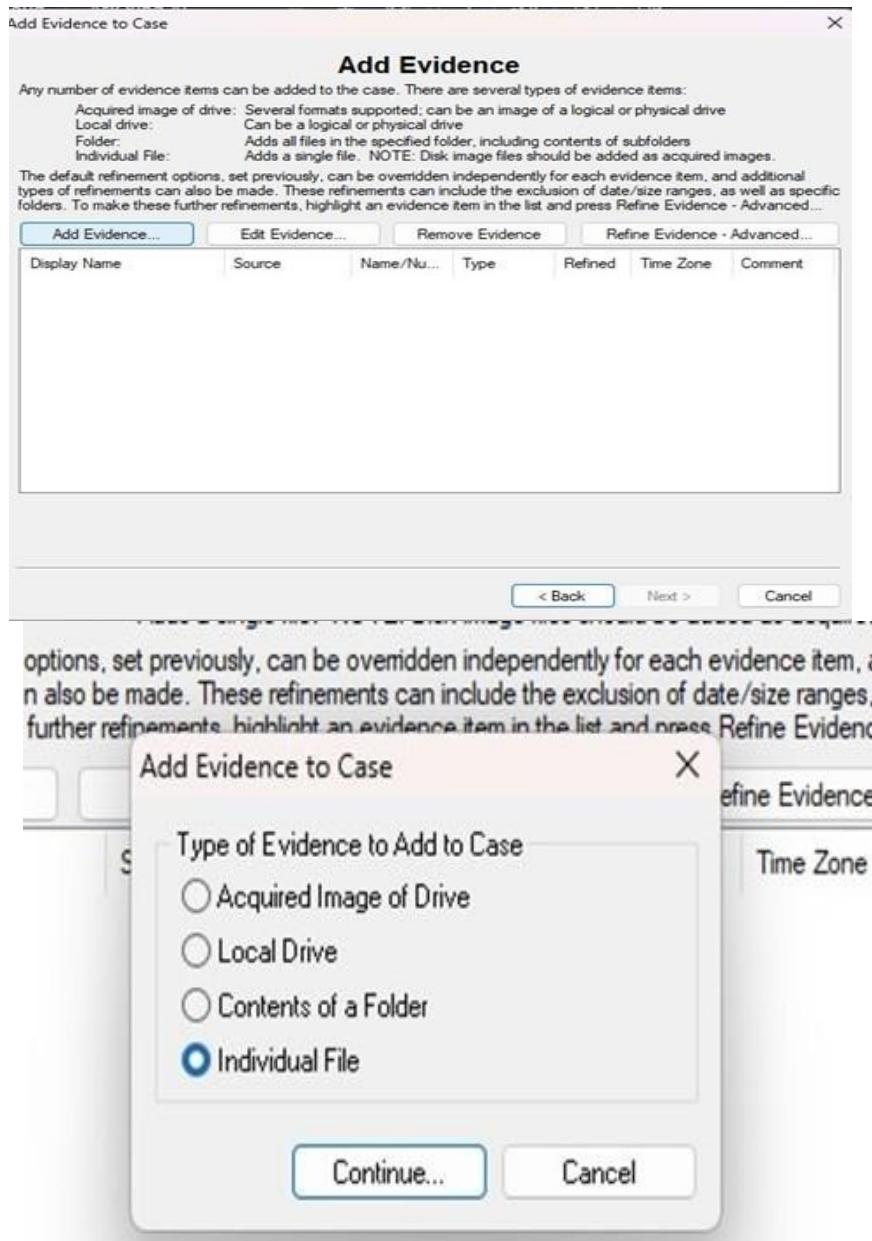
## 7. Now we have reached the Email Emphasis section.

The screenshot shows the 'Refine Case - Default' dialog box with the 'Email Emphasis' tab selected. It contains sections for 'Unconditionally Add' (checkboxes for File Slack, Free Space, KFF Ignorable Files, and Extract files from KFF ignorable containers), 'Conditionally Add' (checkbox for BOTH file status and file type), and 'File Type Criteria' (checkboxes for Documents, Spreadsheets, Databases, Graphics, Multimedia, Archives, Folders, Other Known, Unknown, and Email msgs). Below this is another 'Refine Case - Default' dialog box with similar settings.

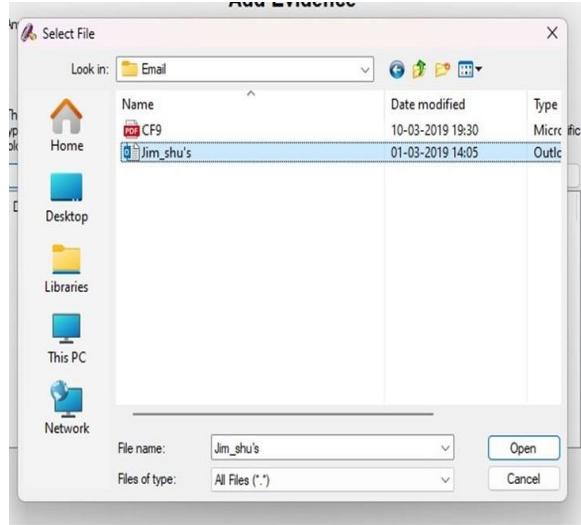
  

The screenshot shows the 'Refine Index - Default' dialog box with the 'Email Emphasis' tab selected. It contains sections for 'Unconditionally Index' (checkboxes for File Slack, Free Space, KFF Ignorable Files), 'Conditionally Index' (checkbox for BOTH file status and file type), and 'File Type Criteria' (checkboxes for the same categories as the previous dialog). Both dialogs have back, next, and cancel buttons at the bottom.

8. Click Next until you reach the **Add Evidence to Case dialog box**, and then click the **Add Evidence button**. In the **Add Evidence to Case dialog box**, click the **Individual File option button**, and then click **Continue**.



9. In the **Select File dialog box**, navigate to your work folder, click the **Jim\_shu's.pstfile**, and then click **Open**.



10. Give some data.

**Evidence Information**

**Evidence Location:**  
D:\SCYT\CF\Email\Jim\_shu's.pst

**Evidence Display Name:**  
Jim\_shu's

**Evidence Identification Name/Number:**  
10

**Comment:**  
Here is an example for the email

**Local Evidence Time Zone:**  
Choose time zone for evidence ...

**OK**    **Cancel**

11. Complete the steps and Click on Next.

**Add Evidence to Case**

**Add Evidence**

Any number of evidence items can be added to the case. There are several types of evidence items:

- Acquired image of drive: Several formats supported; can be an image of a logical or physical drive
- Local drive: Can be a logical or physical drive
- Folder: Adds all files in the specified folder, including contents of subfolders
- Individual File: Adds a single file. NOTE: Disk image files should be added as acquired images.

The default refinement options, set previously, can be overridden independently for each evidence item, and additional types of refinements can also be made. These refinements can include the exclusion of date/size ranges, as well as specific folders. To make these further refinements, highlight an evidence item in the list and press Refine Evidence - Advanced...

Add Evidence...	Edit Evidence...	Remove Evidence	Refine Evidence - Advanced...			
Display Name Jim_shu's	Source D:\SCYT\CF\...	Name/Nu... 10	Type Individual f...	Refined N	Time Zone N/A	Comment Here is an ...

< Back    **Next >**    Cancel

12. Click on finish and see the data.

Case Summary

New Case Setup Is Now Complete

Case Settings

Case directory where the file database, index, and other case-specific files will be stored:  
D:\SCYTVCF\Email\jimshuemail

Number of Evidence Items: 1

Processes to be Performed:

File Extraction:	Yes	
File Identification:	Yes	Remember that although each of these processes adds to the initial processing time, they each play an important role in the investigation process.
MD5 Hash:	Yes	
SHA1 Hash:	Yes	
KFF Lookup:	Yes	Processes that are not performed initially can be initiated at a later point in the investigation except the HTML file listing and automated Registry Reports. Additional evidence can also be added later.
Entropy Test:	Yes	
Full Text Index:	Yes	
Store Thumbnails:	Yes	
Decrypt EFS Files:	Yes	
File Listing Database:	Yes	
File Listing HTML:	Yes	
Data Carving:	Yes	
Registry Reports:	Yes	

Press "Back" if you wish to review or change your settings  
Press "Finish" to accept the current settings and start processing the evidence

< Back Finish Cancel

AccessData FTK 1.81.0 DEMO VERSION -- D:\SCYTVCF\Email\jimshuemail

File Edit View Tools Help

Overview Explore Graphics E-Mail Search Bookmark

Evidence Items File Status File Category

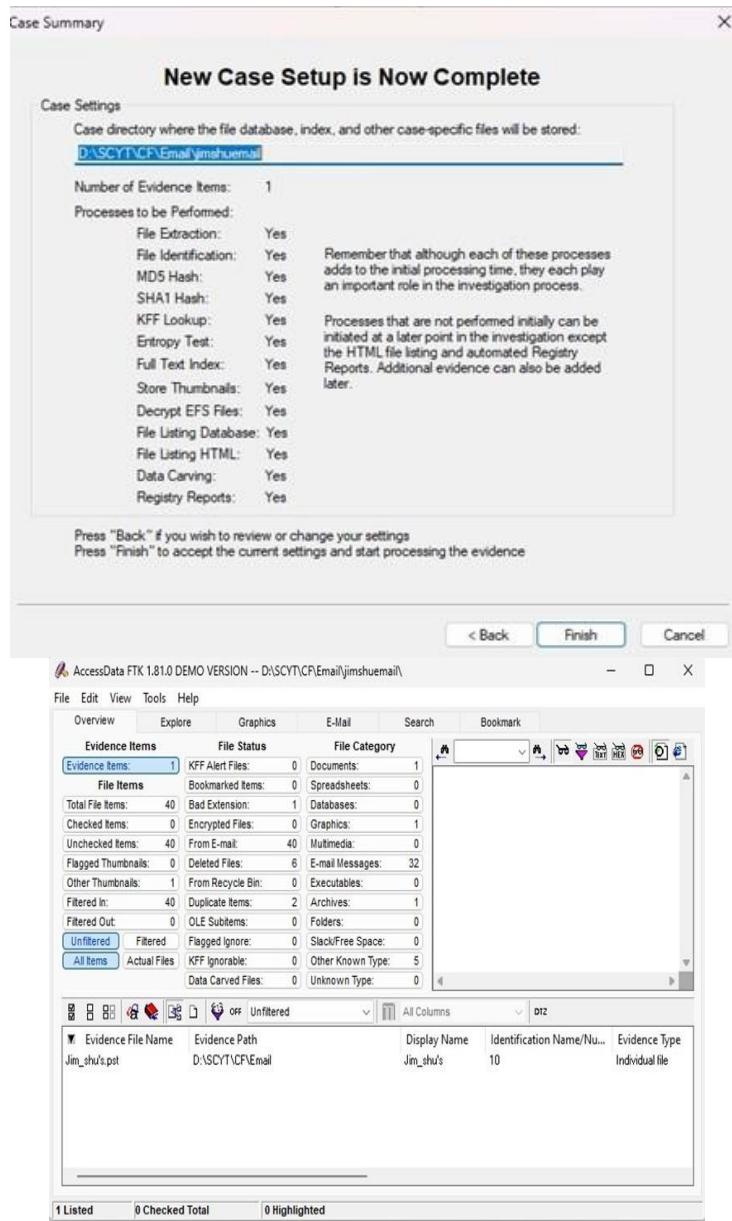
Evidence Items	KFF Alert Files	Documents	1
Total File Items:	40	Bad Extension:	0
Checked Items:	0	Encrypted Files:	0
Unchecked Items:	40	From E-mail:	40
Flagged Thumbnails:	0	Deleted Files:	6
Other Thumbnails:	1	From Recycle Bin:	0
Filtered In:	40	Executables:	0
Filtered Out:	0	Duplicate Items:	2
All Items	Actual Files	Archives:	1
		OLE Subtypes:	0
		Flags:	0
		Flagged Ignore:	0
		Slack/Free Space:	0
		Other Known Type:	5
		Data Carved Files:	0
		Unknown Type:	0

File Items Bookmarked Items Spreadsheets Databases Graphics Multimedia Executables Archives Folders Slack/Free Space Other Known Type Unknown Type

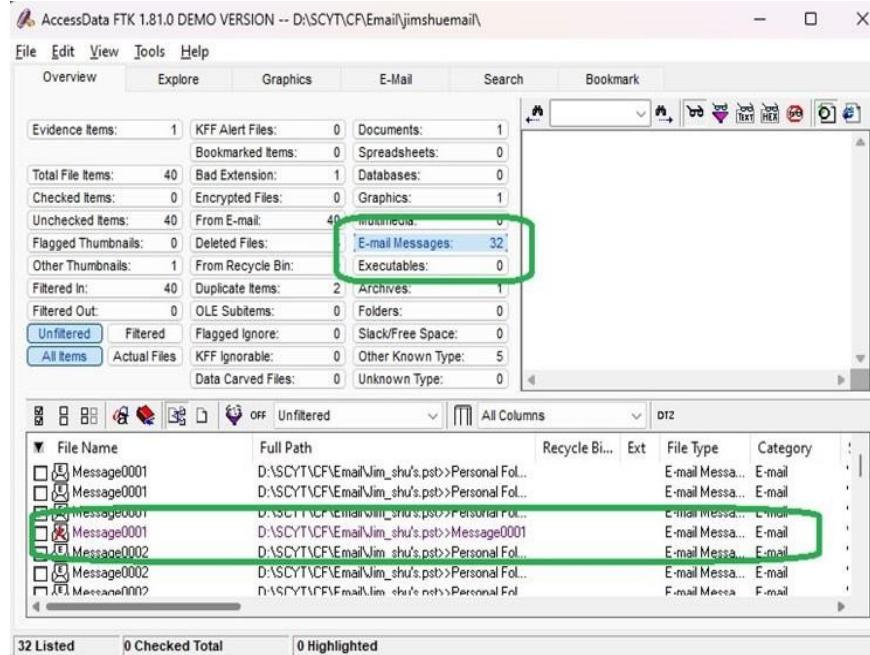
All Columns

Evidence File Name	Evidence Path	Display Name	Identification Name/Number	Evidence Type
Jim_shu's.pst	D:\SCYTVCF\Email	Jim_shu's	10	Individual file

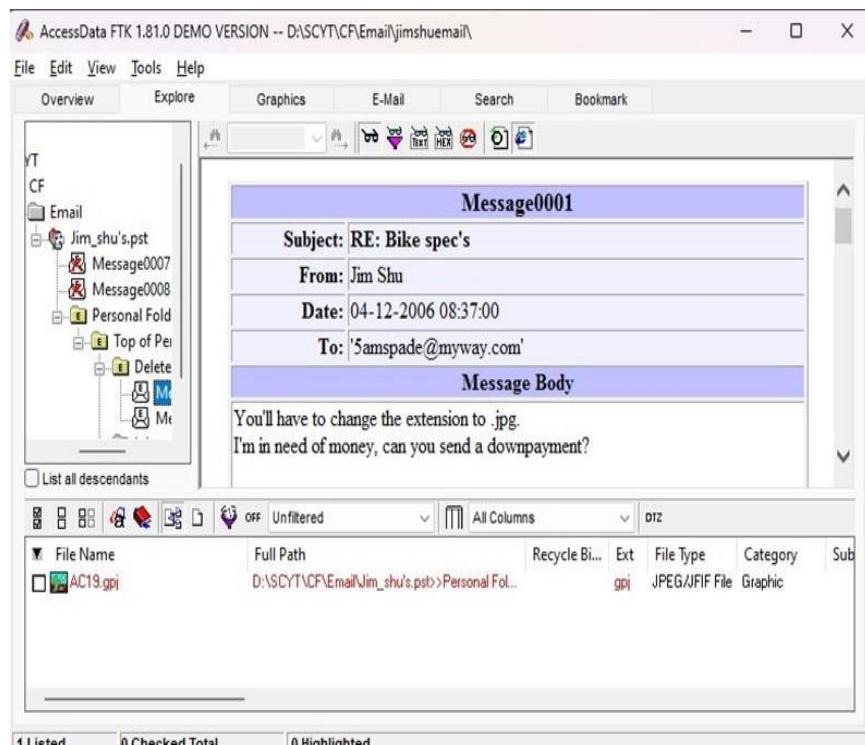
1 Listed 0 Checked Total 0 Highlighted



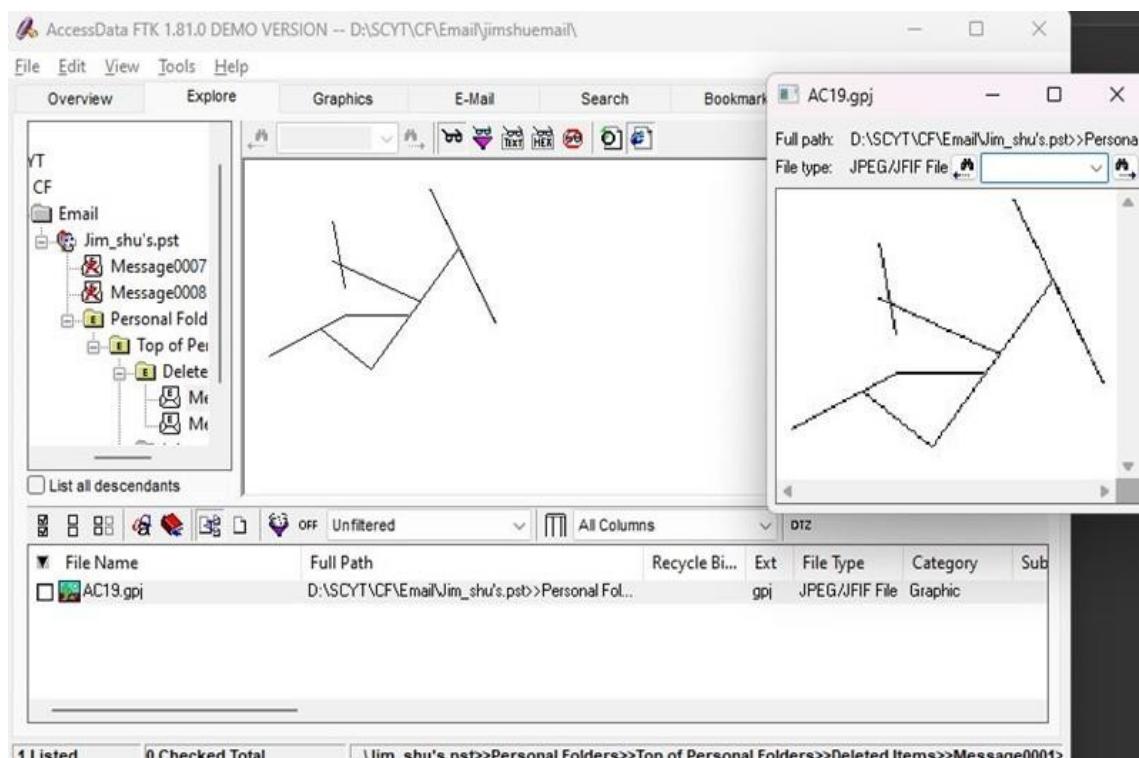
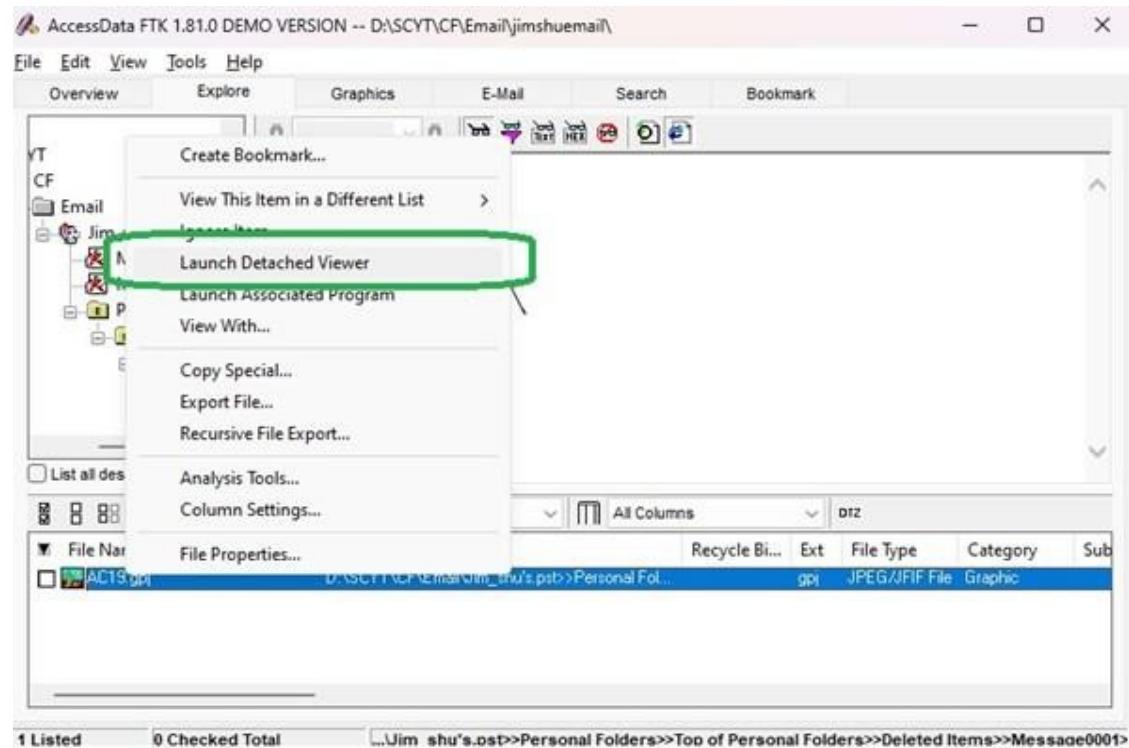
13. When the Add Evidence to Case dialog box opens, click Next. In the Case summary dialog box, click Finish. When FTK finishes processing the file, in the main FTK window, click the Email Messages button, and then click the Full Path column header to sort the records.



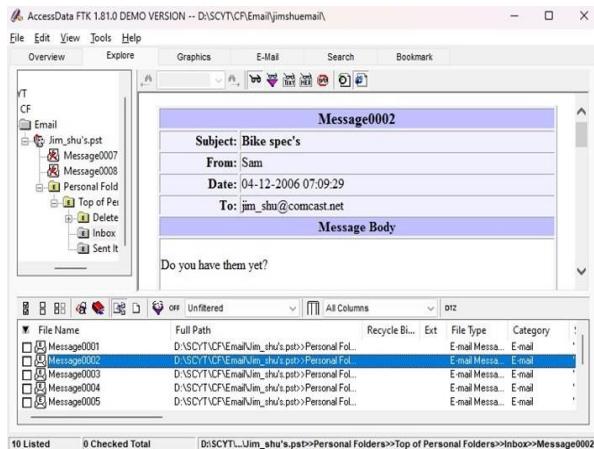
14. For email recovery follow following steps: Click the E-Mail tab. In the tree view, click to expand all folders, and then click the Deleted Items folder.



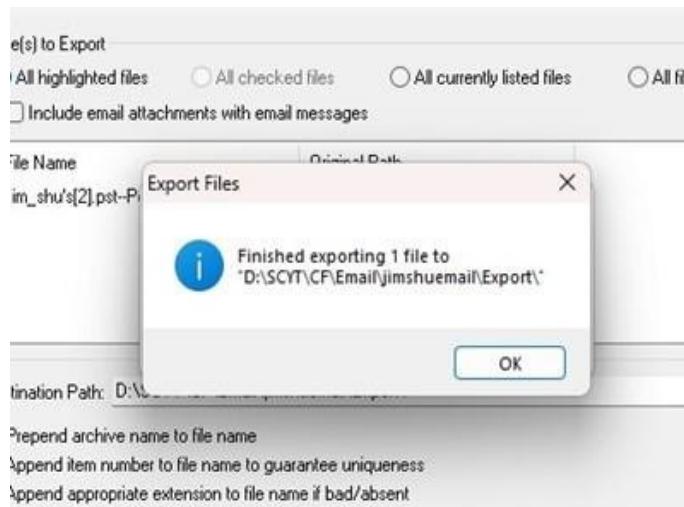
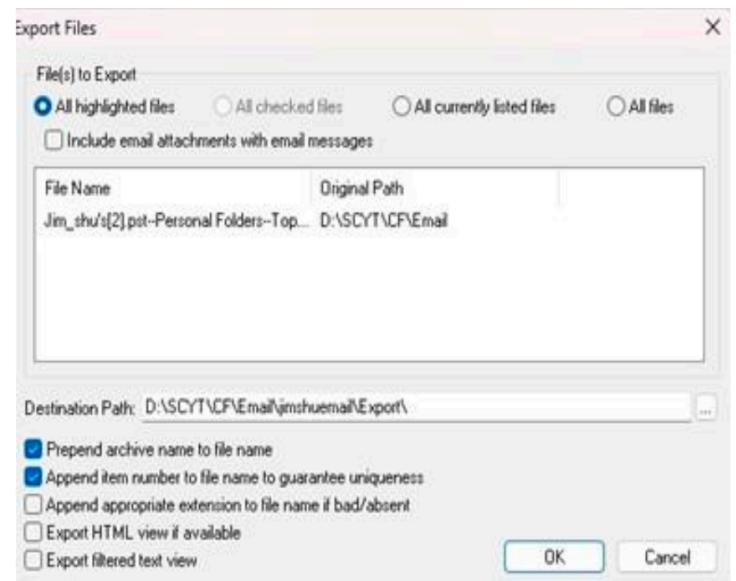
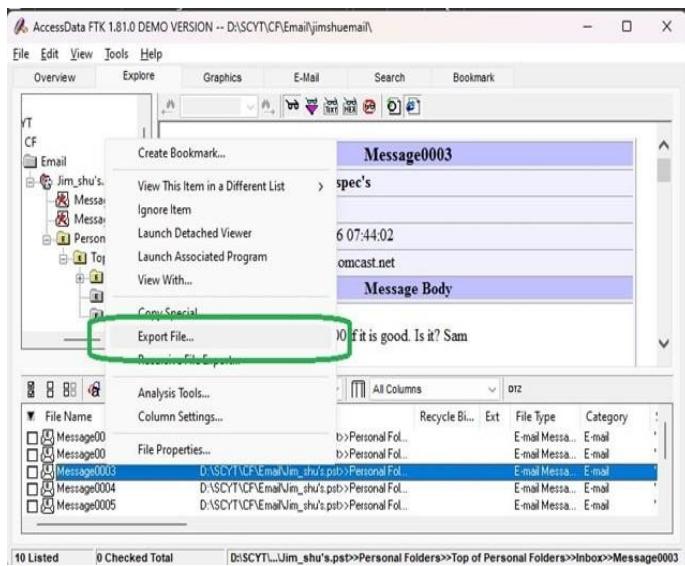
15. Select any message say Message0001 right click and select option Launch DetachedViewer and you can see detail of deleted message.



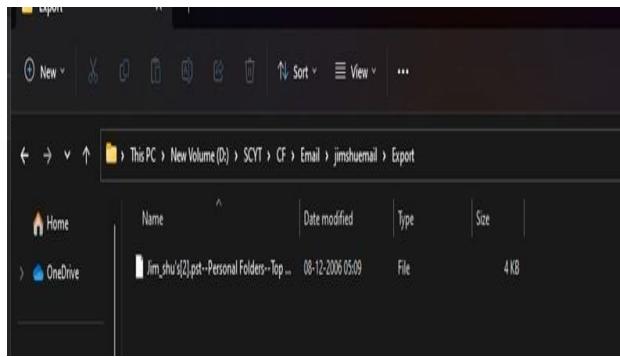
16. For analyzing header follow following steps: Click the E-Mail tab. In the tree view, click to expand all folders, and then click the Inbox folder. In the File List pane at the upper right, click Message0003; as shown in the pane at the bottom, it's from Sam and is addressed to [Jim\\_shu@comcast.net](mailto:jim_shu@comcast.net).



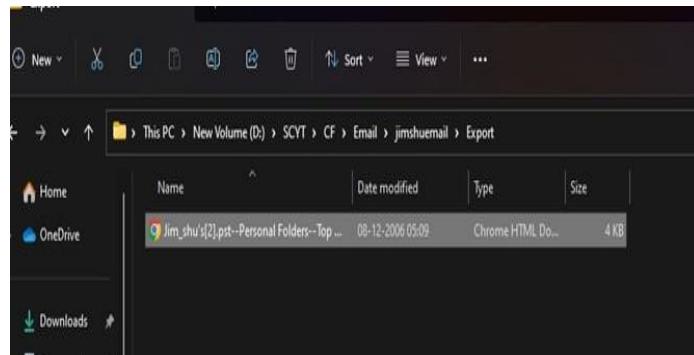
17. Right-click on any message say Message0003 in the File List pane and click Export File. In the Export Files dialog box, click OK.



18. FTK saves exported files in the HTML format with no extension.



19. Right-click the Message0003 file and click Rename. Type Message0003.html and pressEnter.



20. Double-click Message0003.html to view it in a Web browser.



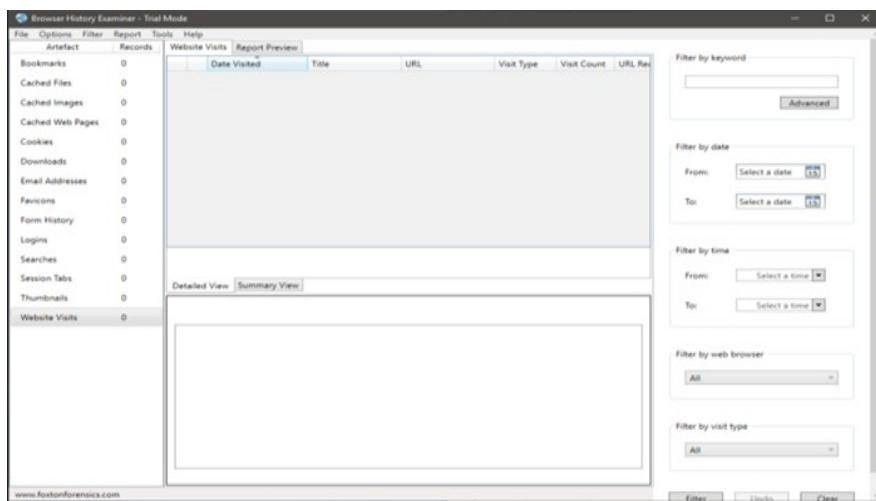
## PRACTICAL 8

### Aim : Web Browser Forensics:

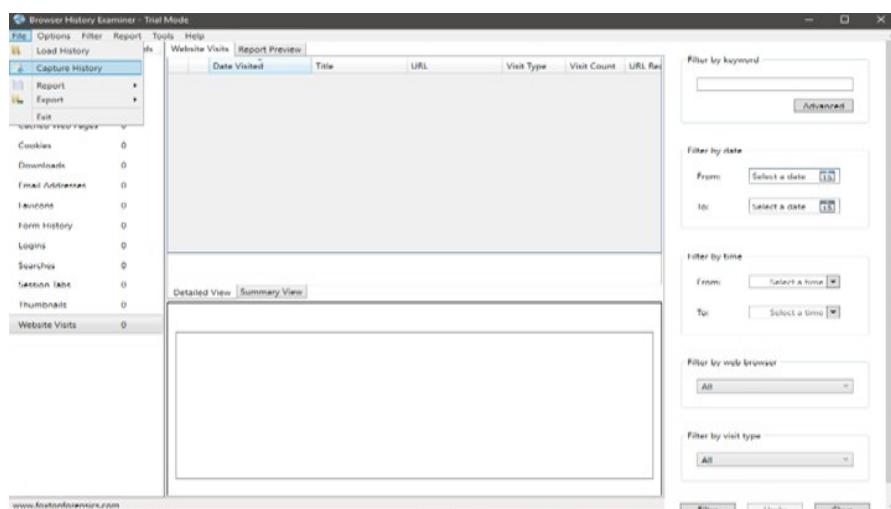
- Analyze browser artifacts, including history files, bookmarks, and download records.
- Analyze cache and cookies data to reconstruct user-browsing history and identify visited websites or online activities.
- Extract the relevant log or timestamp file, analyze its contents and interpret the timestamp data to determine the user's last internet activity and associated details.

### Steps :

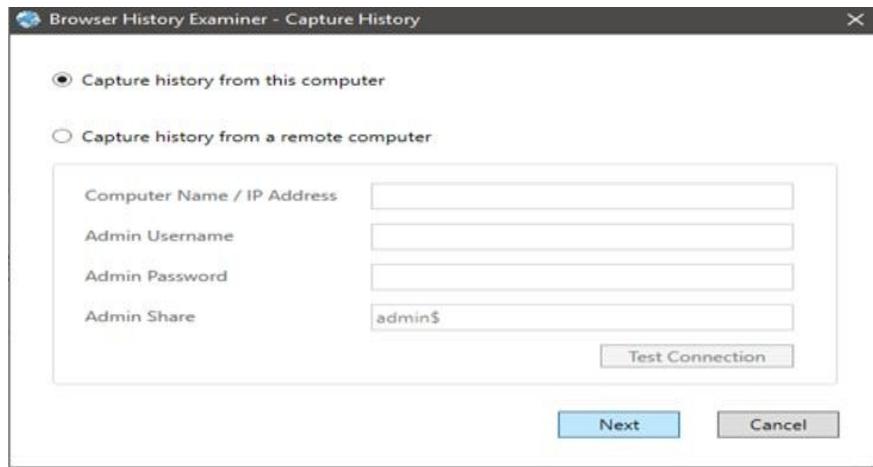
1. Open Browser History Examiner.



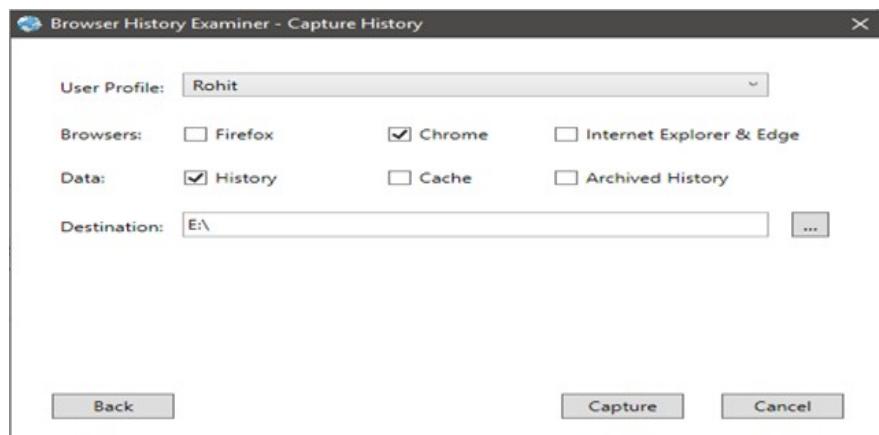
2. Click on file → Capture History.



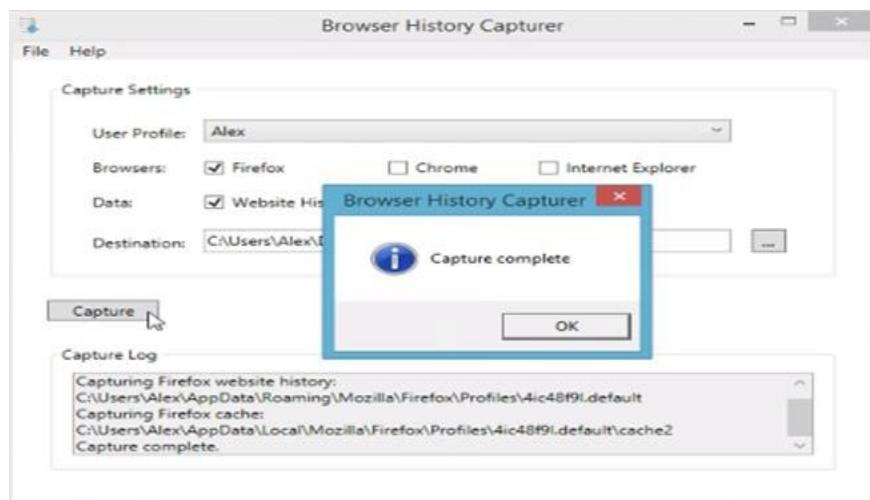
3. Select the capture folder and click on next.



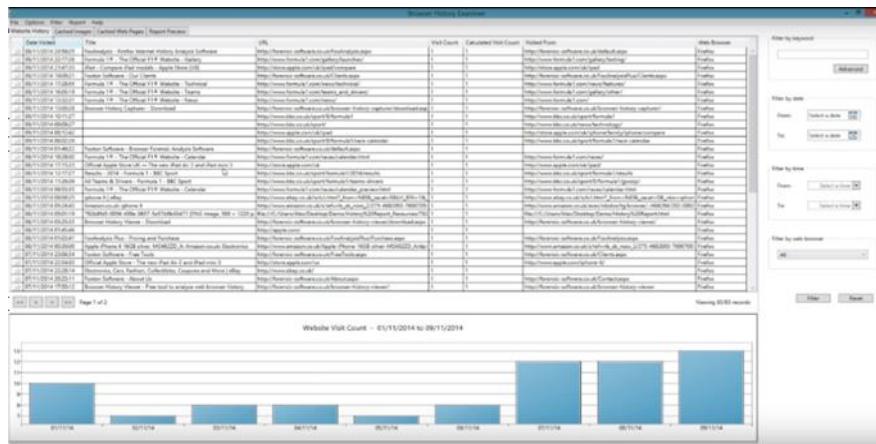
4. Enter the destination to capture the data.



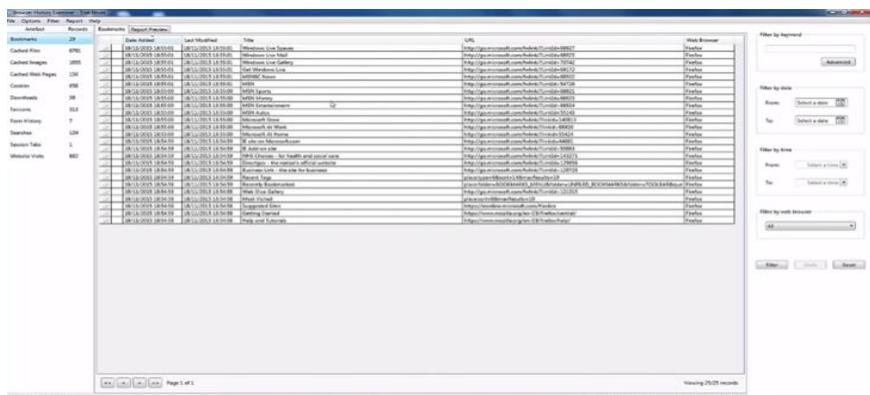
5. The history is been extracting.



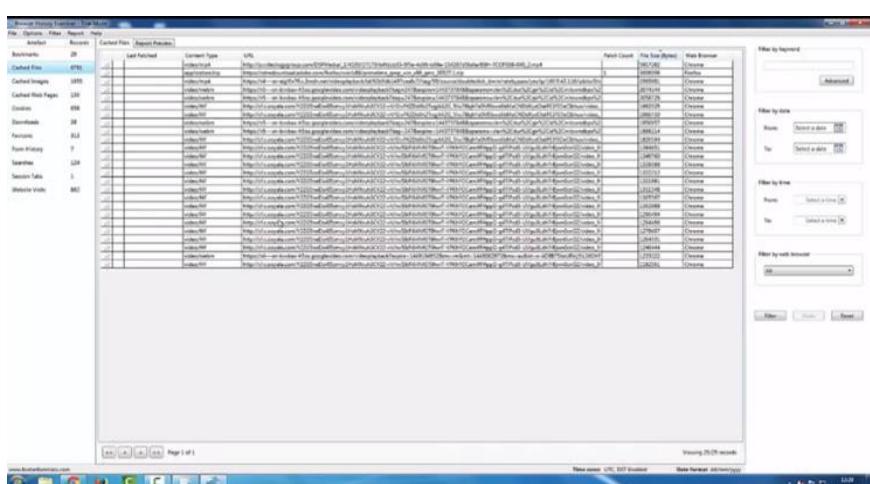
6. The data has been retrieved.



7. On the left panel click on bookmarks.



8. On the left panel click on cached files.



9. On the left panel click on cached images.

The screenshot shows the 'Browser History Examiner - Trial Mode' interface. On the left, a sidebar lists various history categories with their counts: Bookmarks (29), Cached Files (470), Cached Images (405), Cached Web Pages (139), Cookies (608), Downloads (16), Favorites (512), Form History (7), Session Tabs (128), and History Items (407). The 'Cached Images' category is selected. The main pane displays a table titled 'Cached Images - Report Results' with columns: Last Accessed, Content Type, Date Expired, Name, and File Size (bytes). The table lists numerous entries, each corresponding to a thumbnail preview of a cached image. A large preview area below the table shows a grid of these thumbnails. Filter and search options are available on the right side of the main window.

10. On the left panel click on cookies.

This screenshot shows the 'Cookies' report in the 'Browser History Examiner - Trial Mode'. The left sidebar shows the 'Cookies' category is selected. The main pane displays a table titled 'Cookies - Report Results' with columns: Date Created, URL, Last Accessed, Date Expired, Name, Content, and File Browser. The table lists many cookie entries, each with a small preview icon next to it. The interface includes standard filtering and search tools on the right.

11. To create Reports; Click on file → Report and save the report as pdf or html page.

The screenshot shows the 'File' menu open, specifically the 'Report' submenu. The 'Report' option is highlighted. A dropdown menu from this option shows two choices: 'Save as PDF' and 'Save as HTML'. Both options are currently highlighted in blue, indicating they are the active choices.