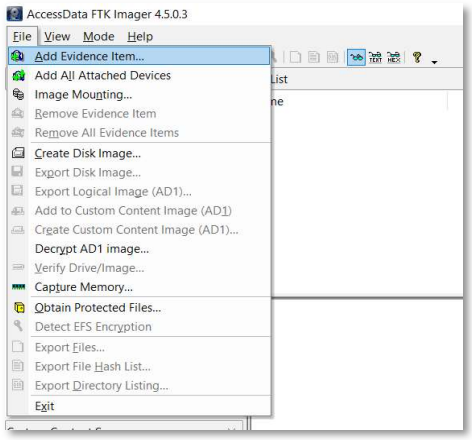
TOPIC
Practical 1 : Creating a Forensic Image using FTK Imager/Encase Image: - Creating Forensic Image (not to be done) - Analyze Forensic Image - Check Integrity of Data
Practical 2: Data Acquisition: Extract Images, Text files from RECYCLER and unallocated space using FTK Imager
Practical 3: Forensics Case Study: - Solve the Case study (image file) using Autopsy
Practical 4: Capturing and analyzing network packets using Wireshark
Practical 5: Using Sysinternals tools for Network Tracking and Process Monitoring
Practical 6: Recovering and inspecting deleted files
Practical 7: Email Forensics
Practical 8: Web Browser Forensics

Practical 1

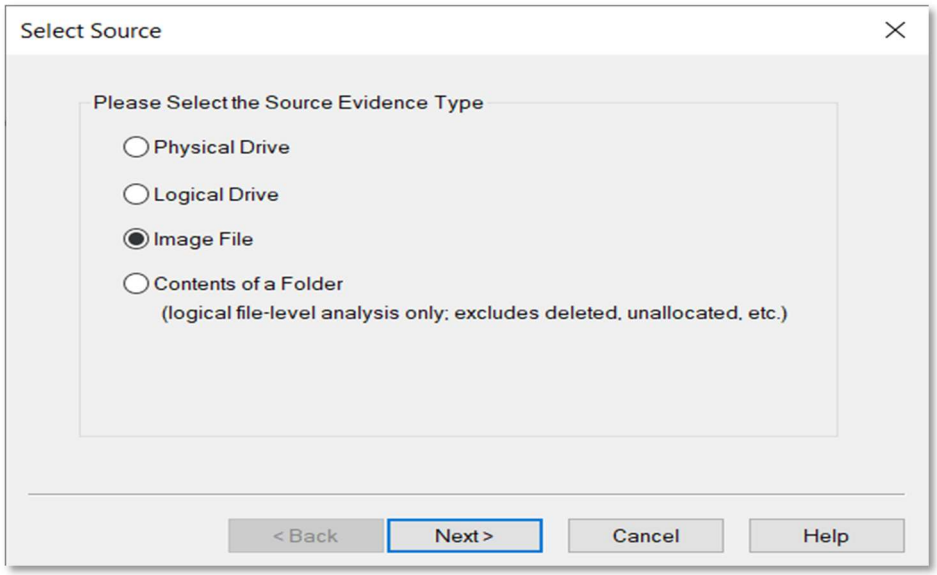
a) **Creating Forensic Images FTK**
(not to be performed precious.img is provided)

b) Analyze Forensic Image: (to be performed on precious.img)

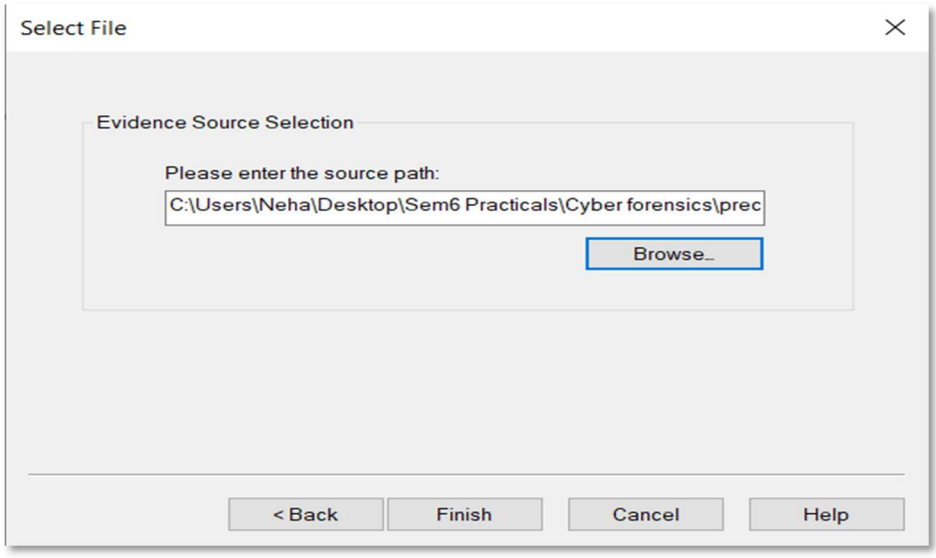
1. Click on Add Evidence Item to add evidence from disk, image file or folder.



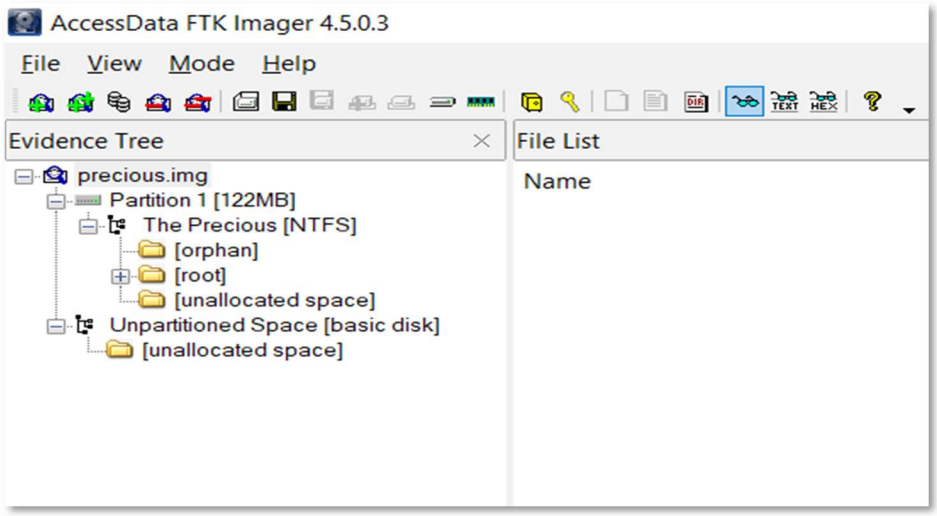
2. Now select the source evidence type as physical drive, logical drive or image file. We have selected image file and click on next.



3. Select virtual drive image & click on open option. Select the source path and click on finish.



4. Now select Evidence Tree and analyze the virtual disk as physical disk.



5. Here we can analyze disk image by noticing these items:

In the left pane, a tree-structured list of the contents of C drive appears

- **RECYCLER** contains files in the recycle bin

html file from RECYCLER

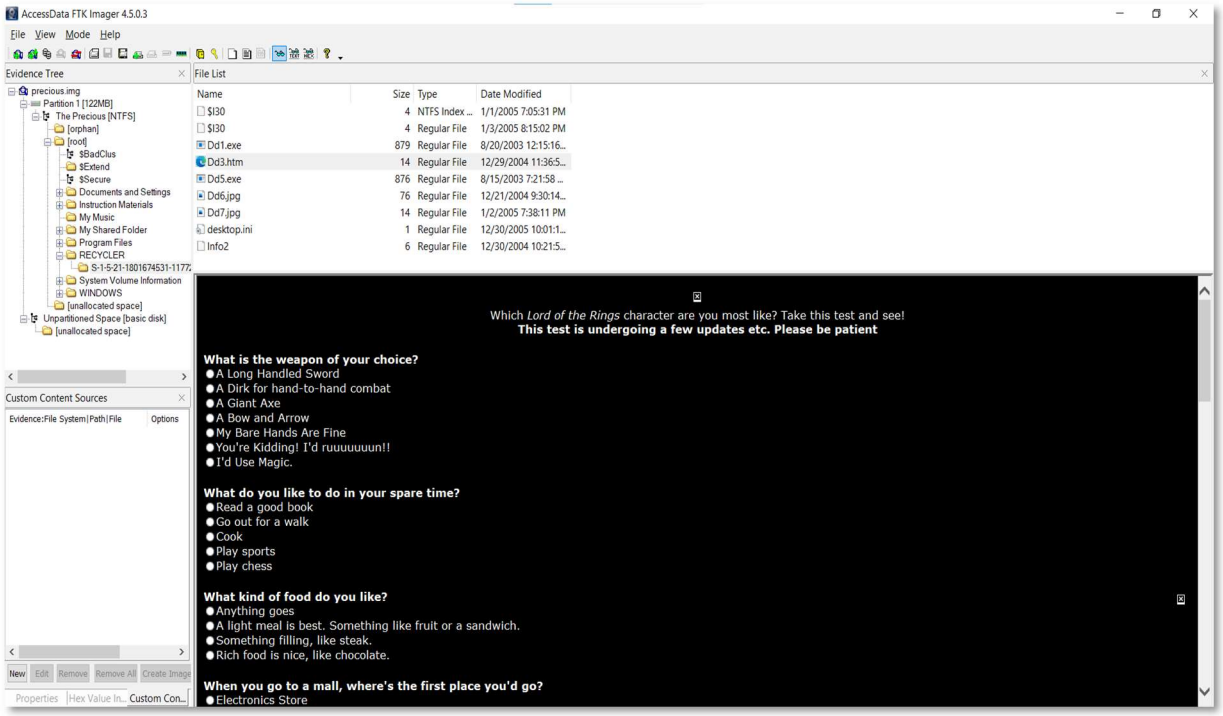
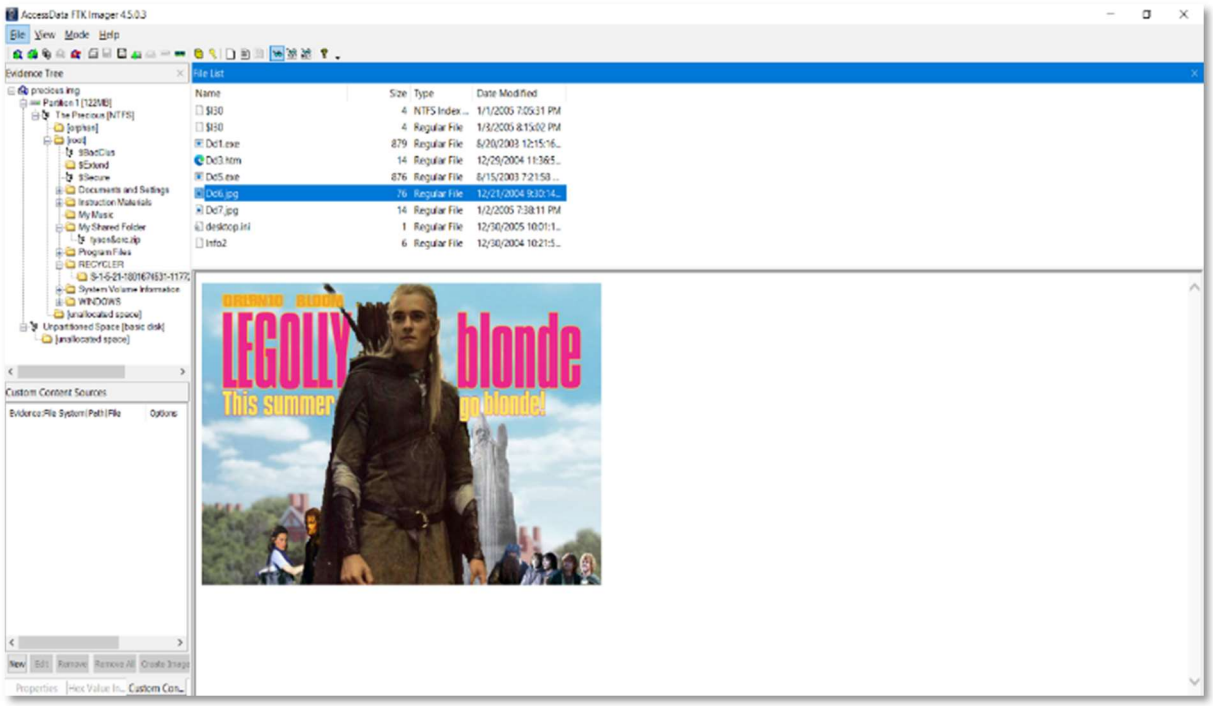
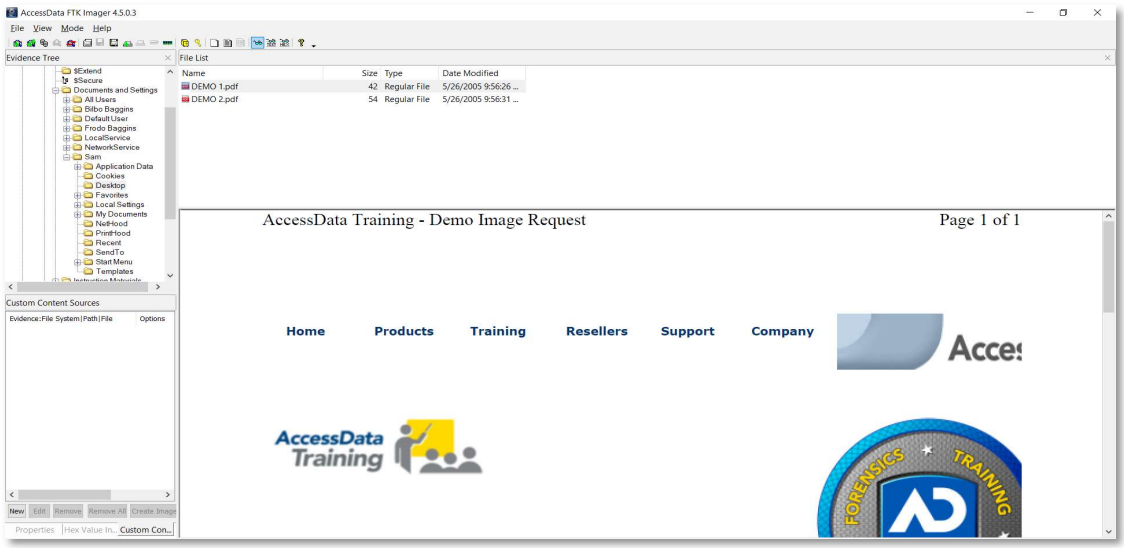


Image file from RECYCLER

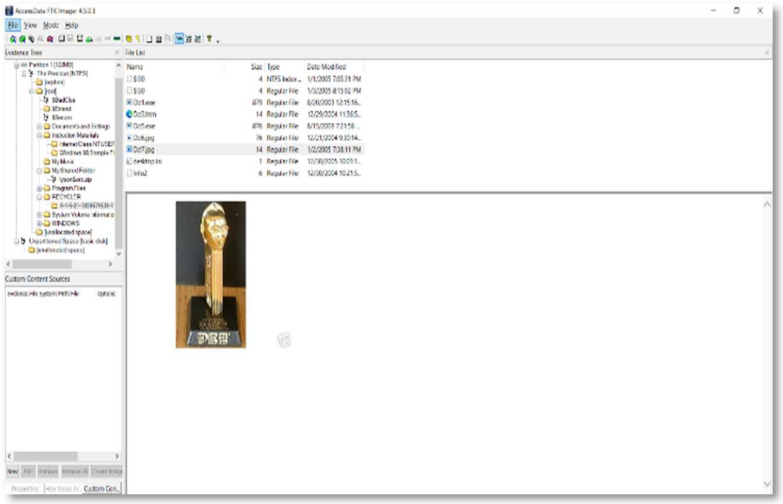


PDF file from document & settings folder

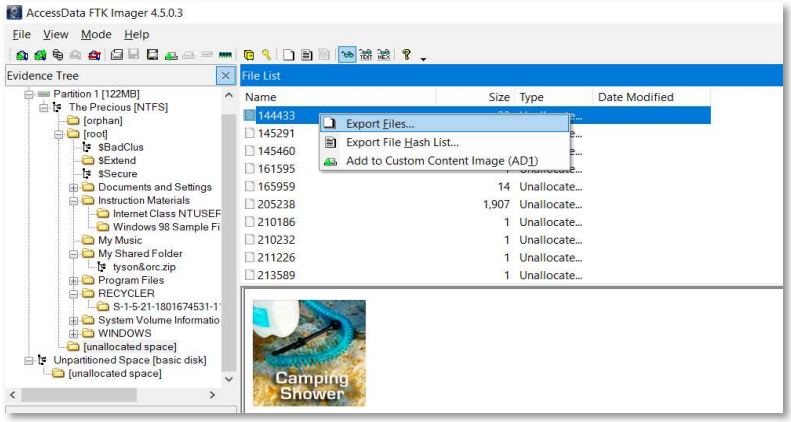


c) Extract Images, Text files from RECYCLER and unallocated space using FTK Imager

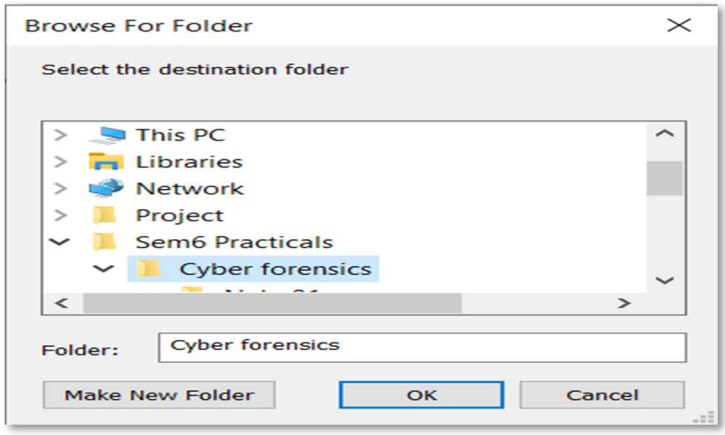
1. View Deleted File(s) in the Recycler.
Navigate to RECYCLER --> RECYCLER SUBDIR Click on the jpg file if it exists.



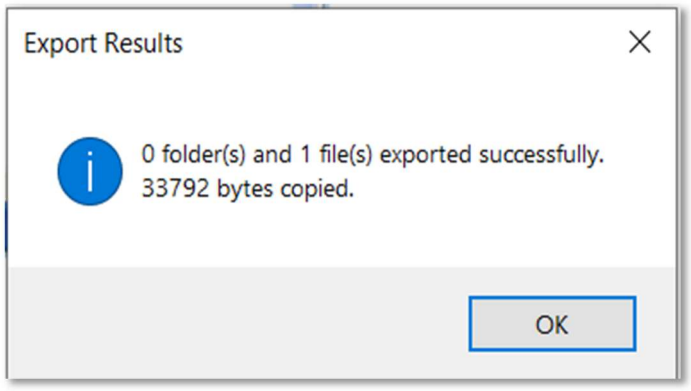
2. Recover deleted image using option Export File. Right Click on the file that contains the picture Select Export Files



3. Select the destination folder. Click the OK Button.



4. Export Results Click the OK Button

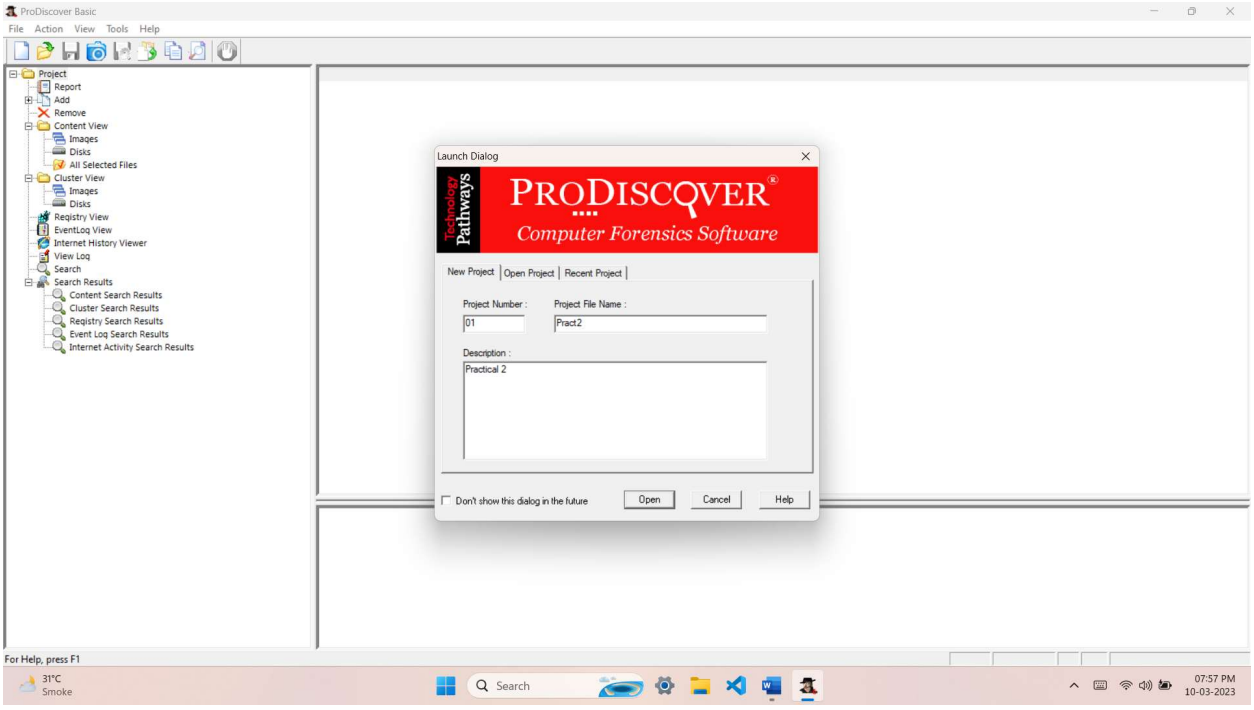


Practical 2

AIM: Perform data acquisition using: ProDiscover

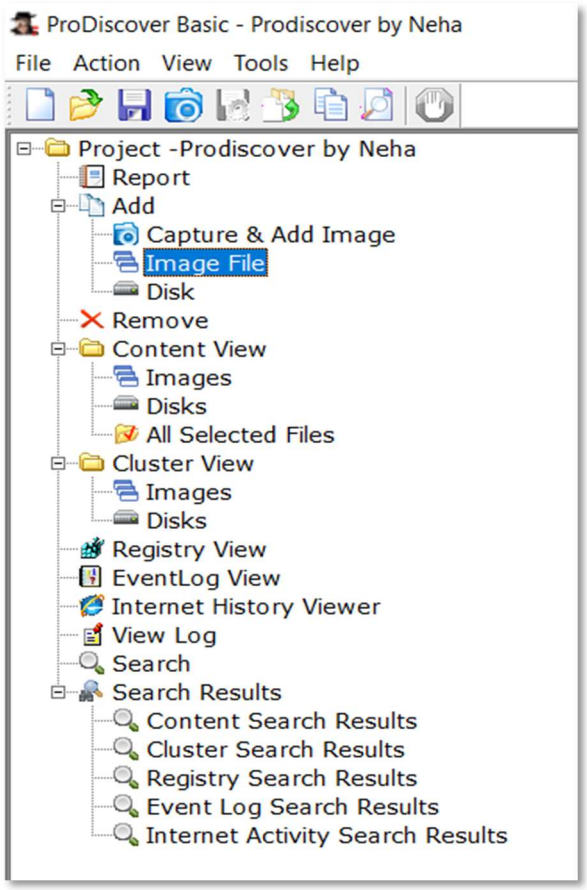
Steps:

1. First Open Prodiscover Basic and start with new case

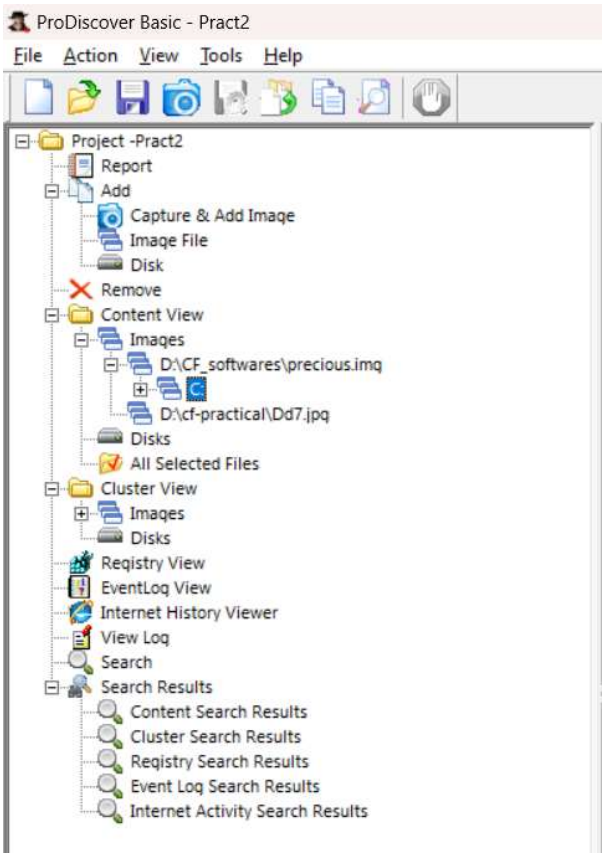


2. created project appears in left pane and select add>image file

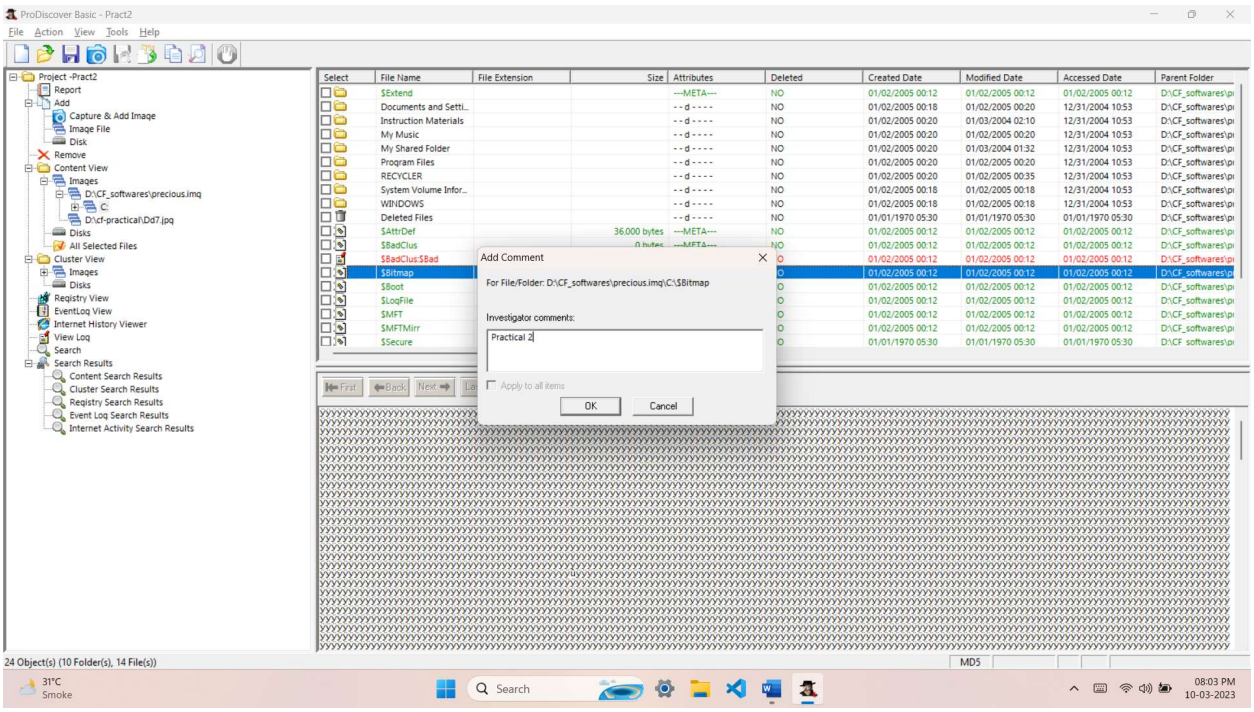
Add precious.img file and previously recovered jpg file



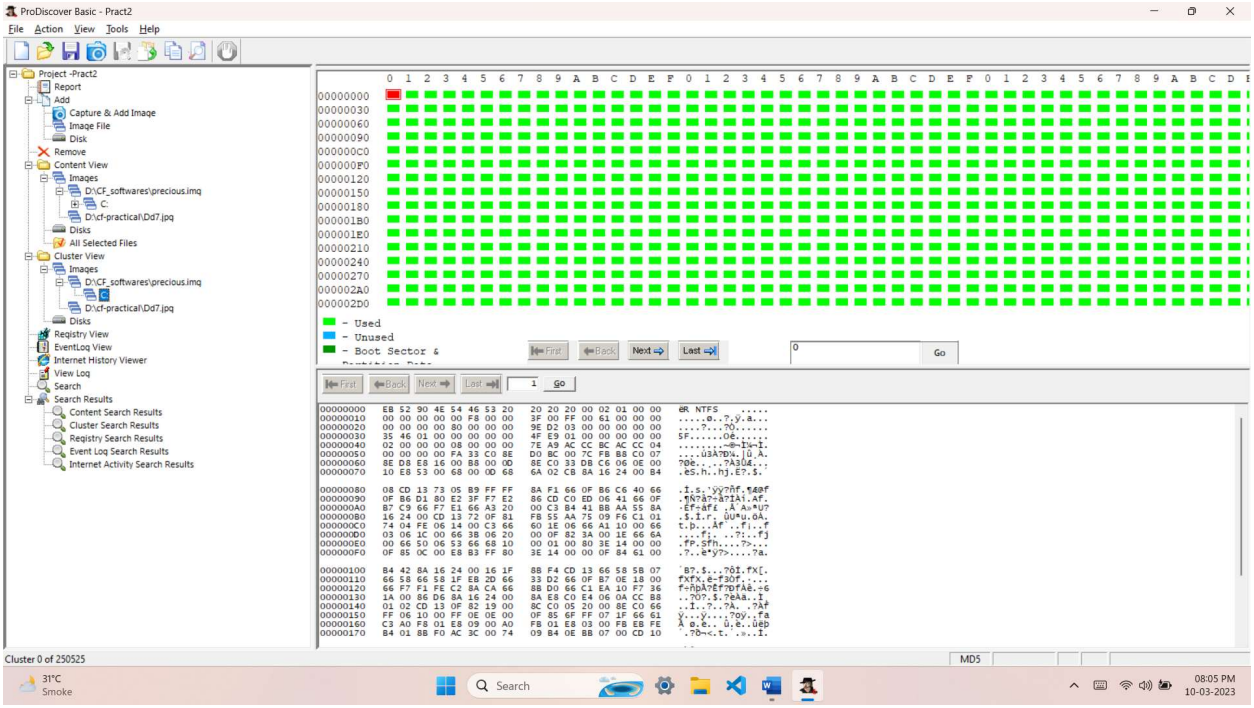
3. Open the image exported, go to Content View > Images in left pane.



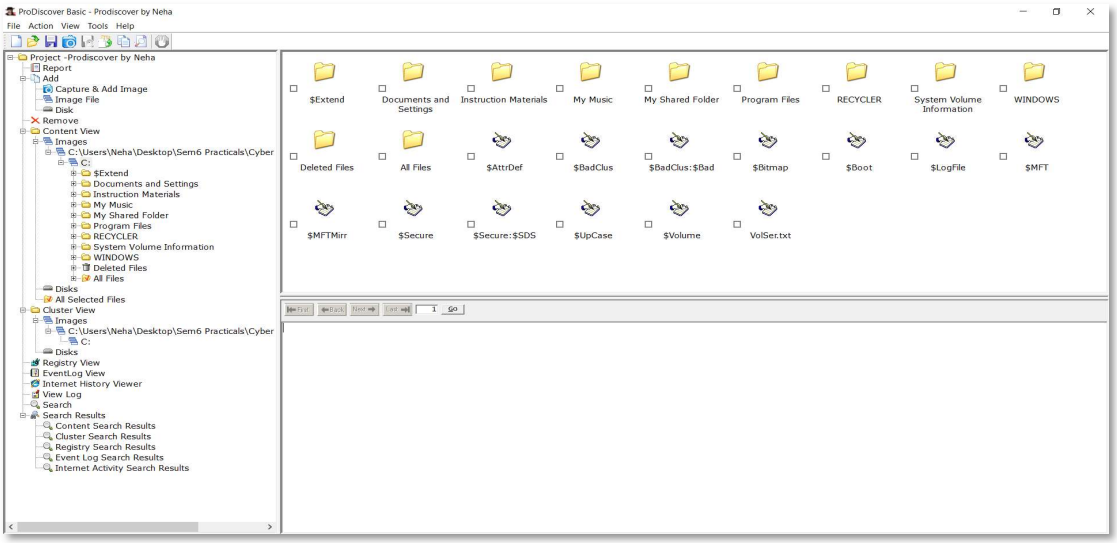
4. Click on any File and type a comment.



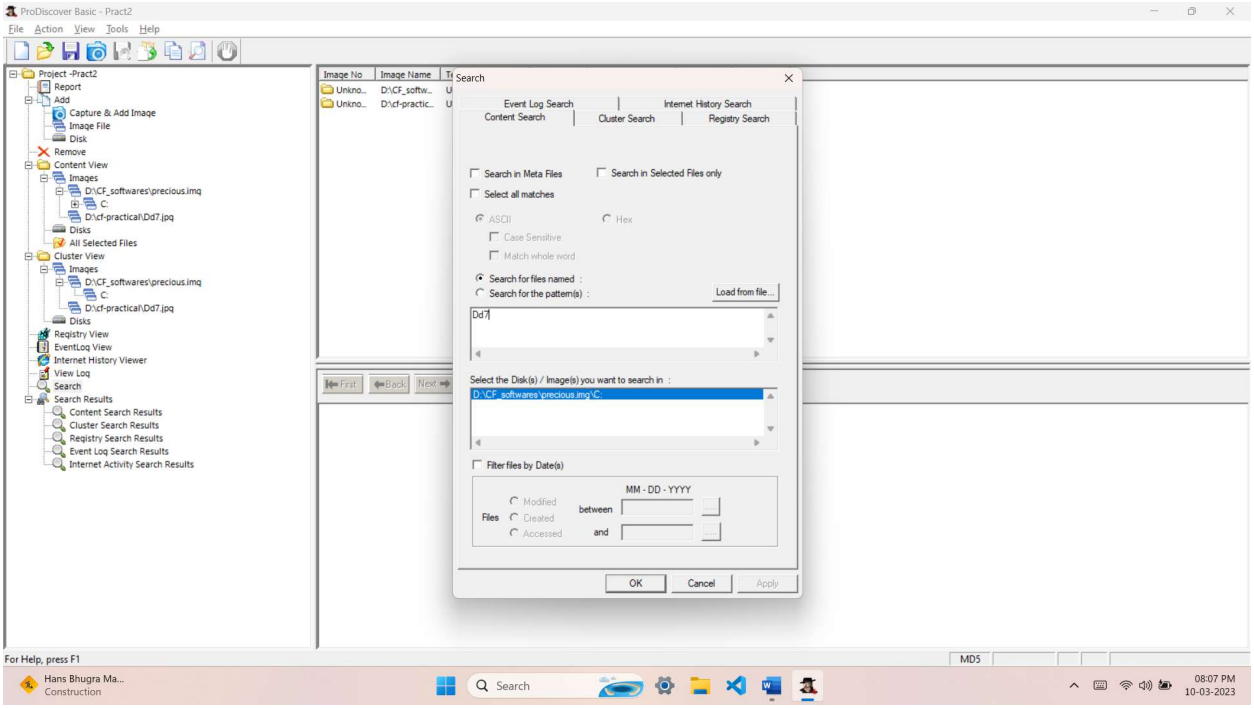
5. in the sidebar click o cluster view is seen from the cluster view in left panel.



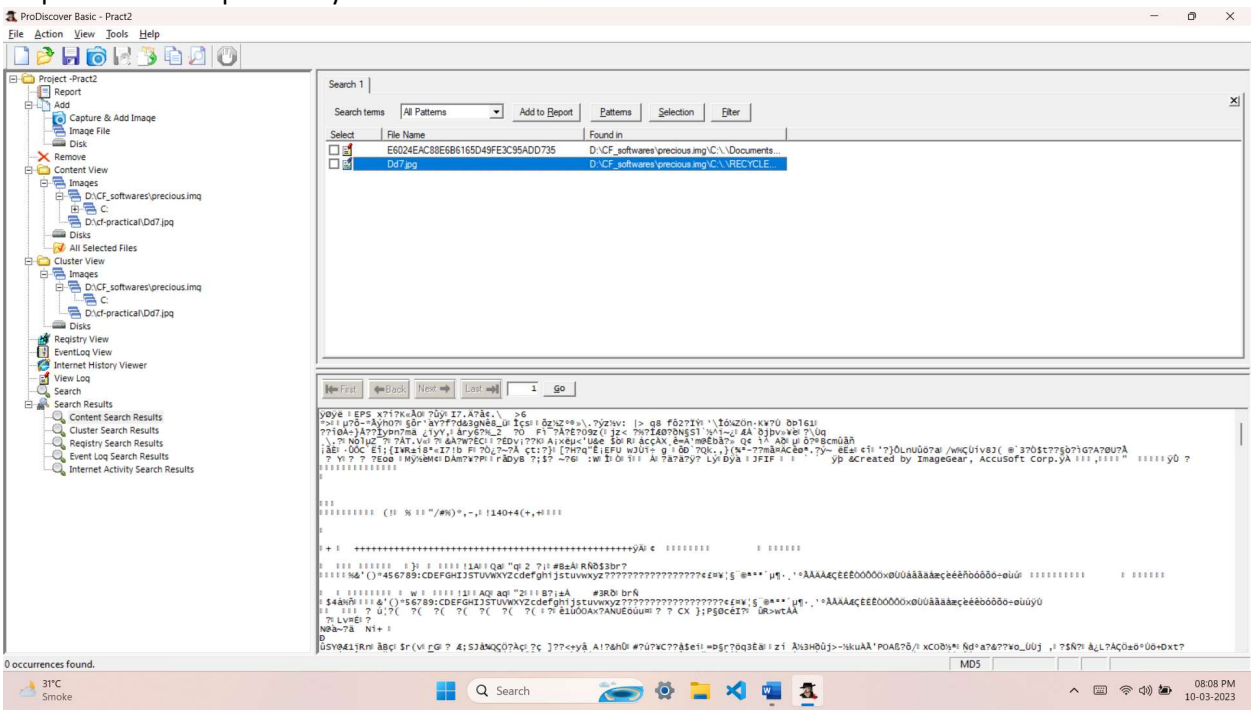
6. We can also view gallery view by going view > gallery view.



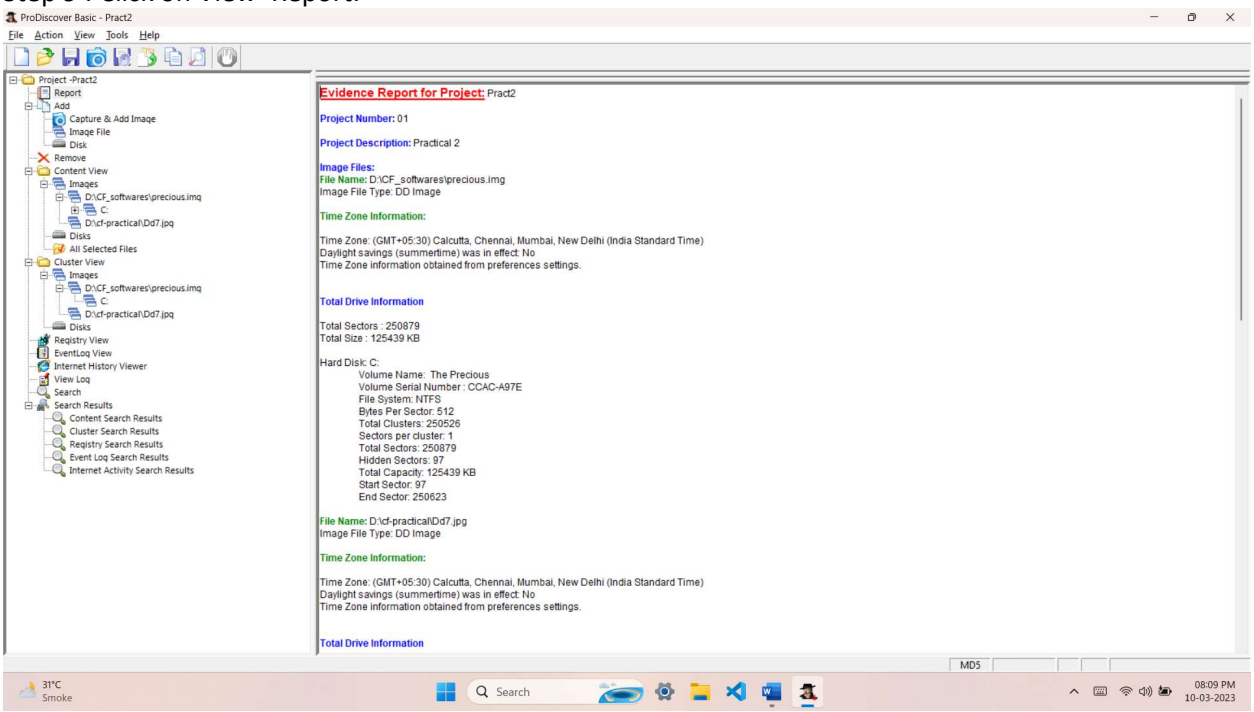
7. Keyword search.
Click on Search in left pane and
Select click on **search for files named**
Enter the file name to be searched in the image created.



Step 8: Select Output of Keyword search.



Step 9 : Click on View>Report.

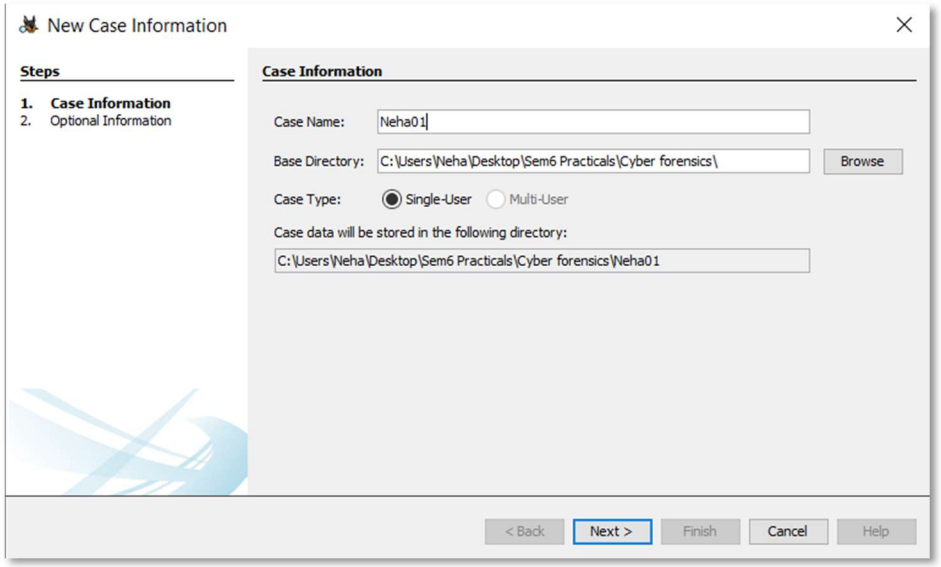


Practical 3

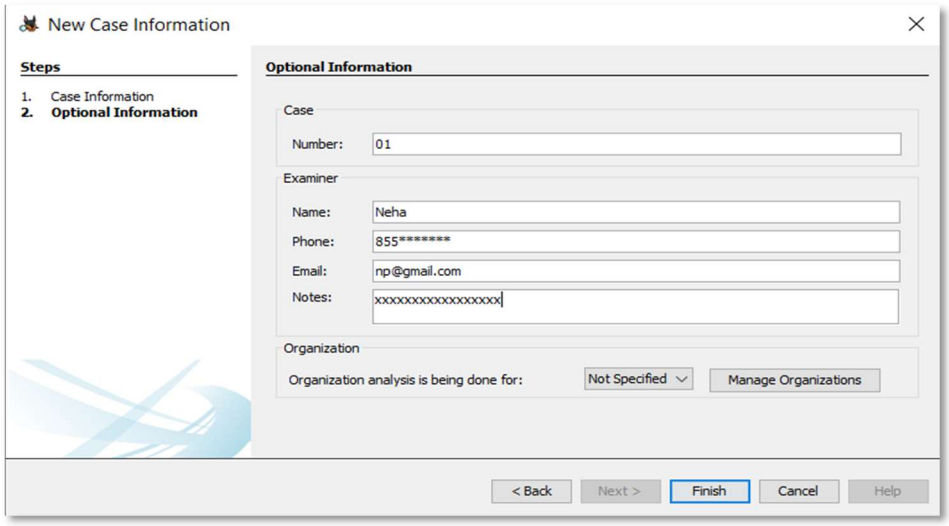
AIM: Forensics Case Study: - Solve the Case study (image file) using Autopsy

1. To create a case, Select new case

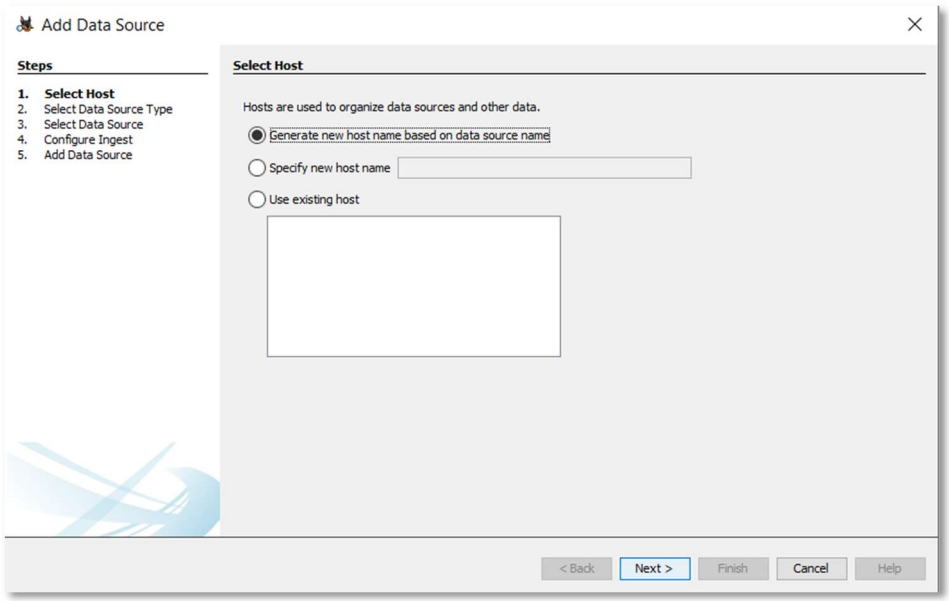
2. You will need to supply it with the name of the case and a directory to store the case results into.



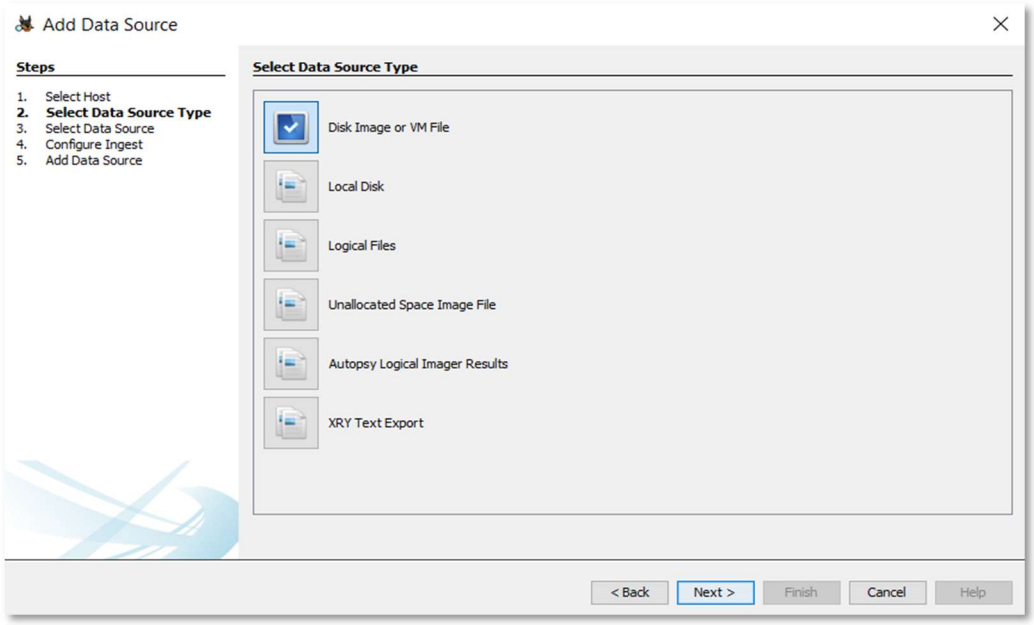
You can optionally provide case numbers and other details



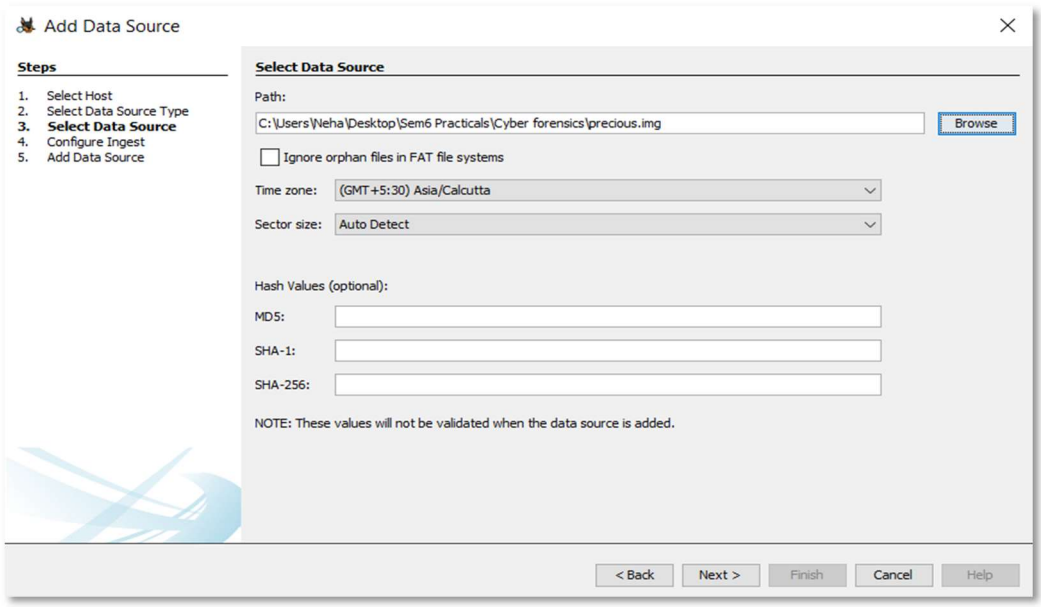
After adding case information it will automatically redirect to add data source wizard Click on next



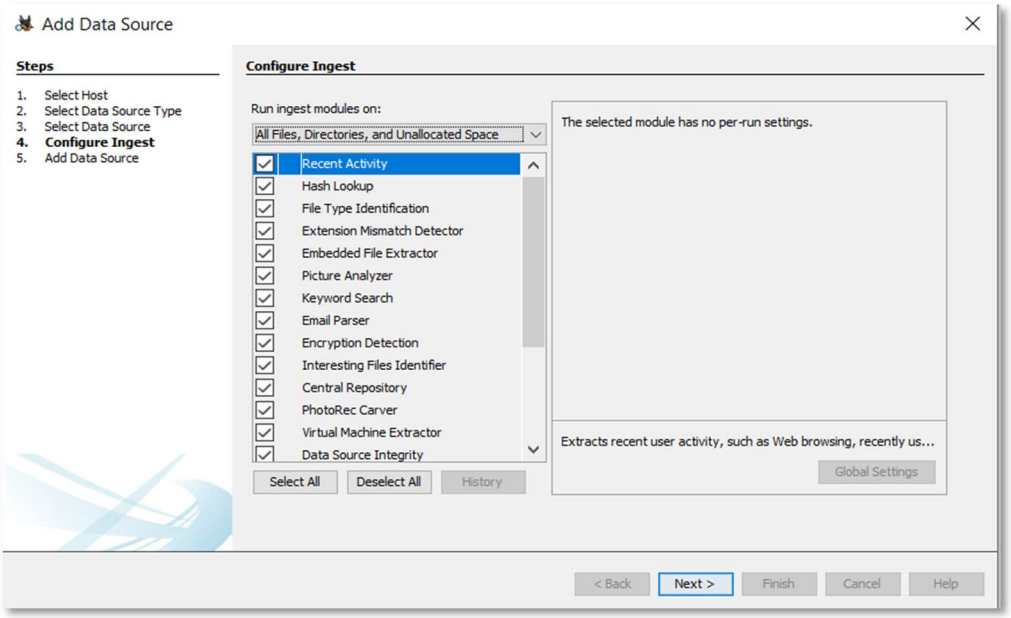
You will need to choose the type of input data source to add image.
Click on disk image or VM file then click on next



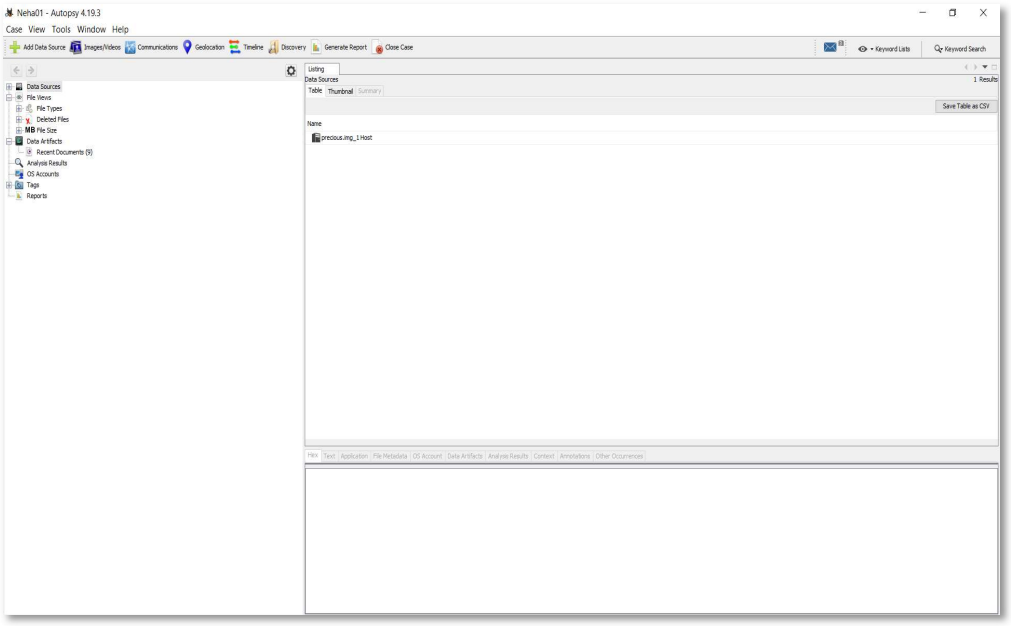
Next, supply it with the location of the source to add.



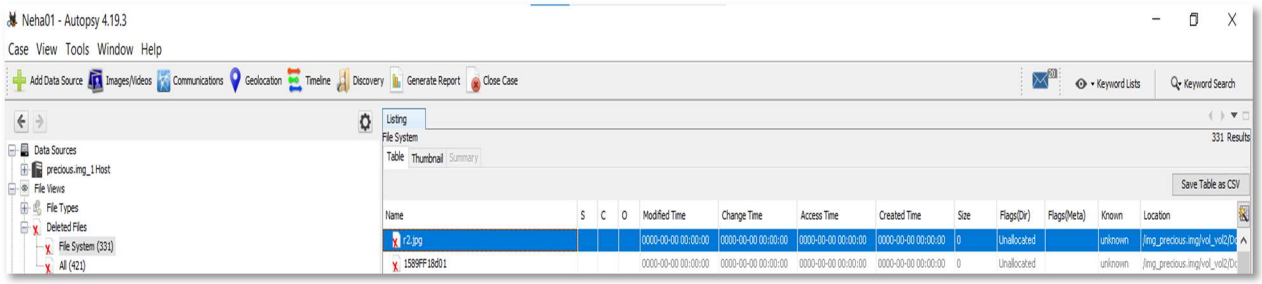
Click on next and finish



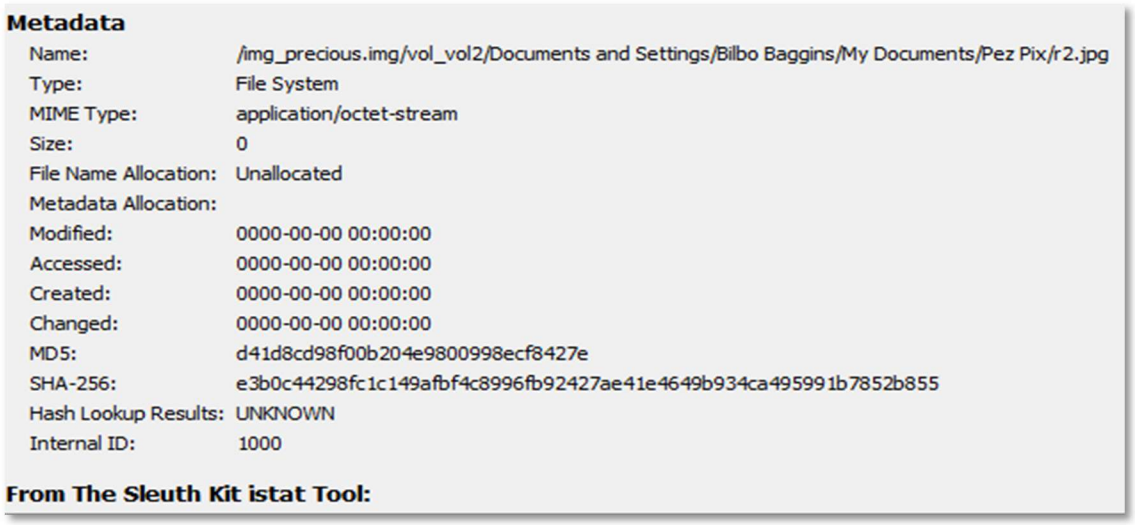
Autopsy will start to analyze these data sources and add them to the case and internal database



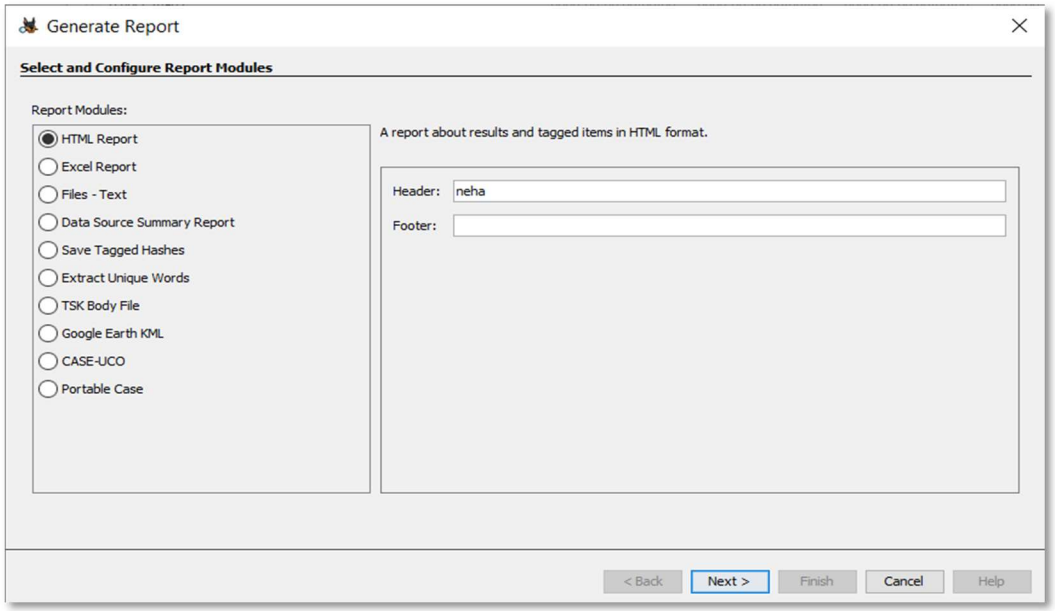
Click on deleted files < file system select first image



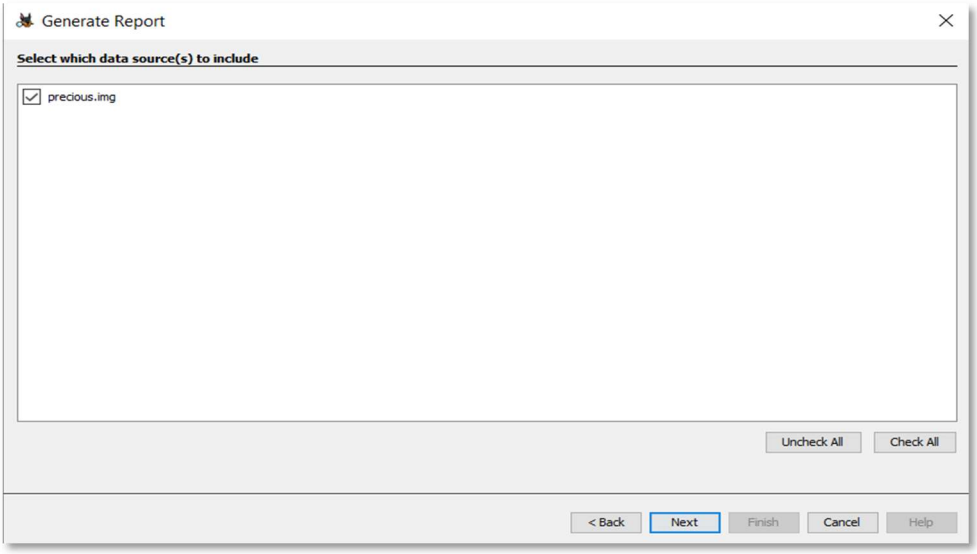
You can see metadata of image file



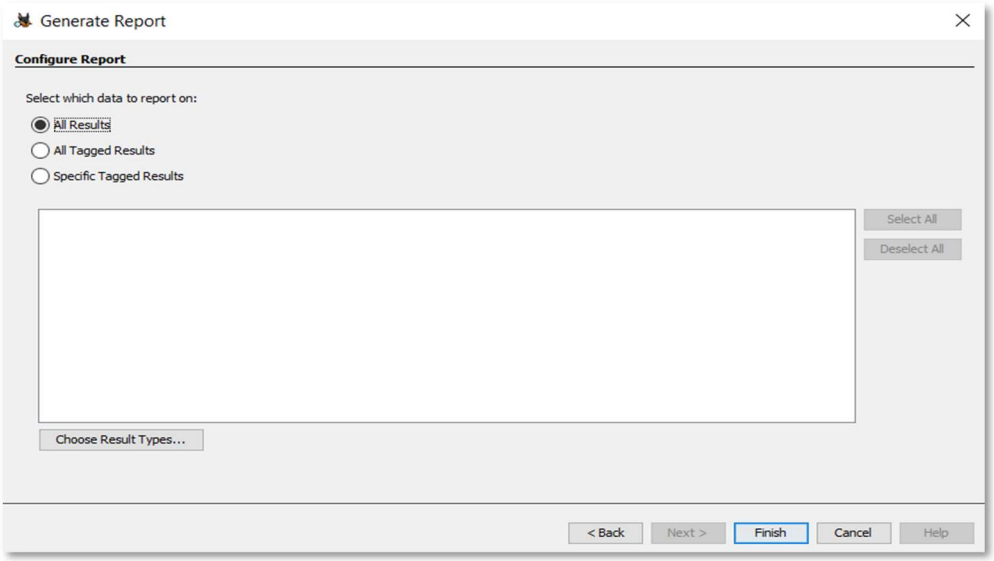
Click on html report



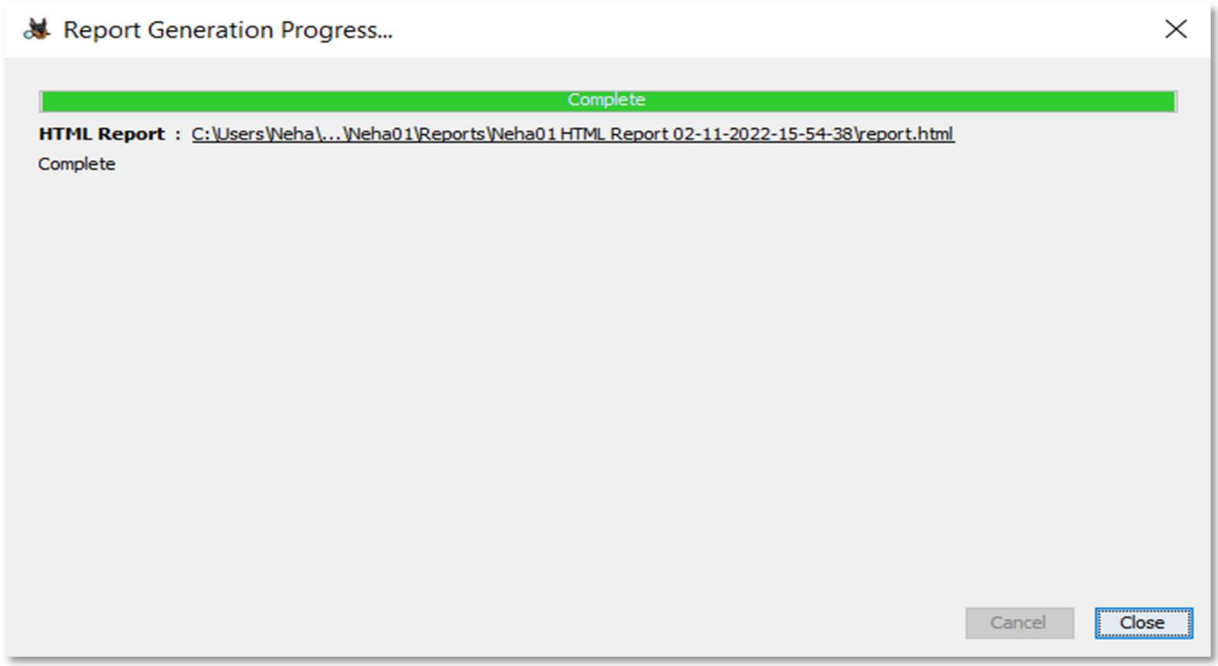
click on check box then click on next

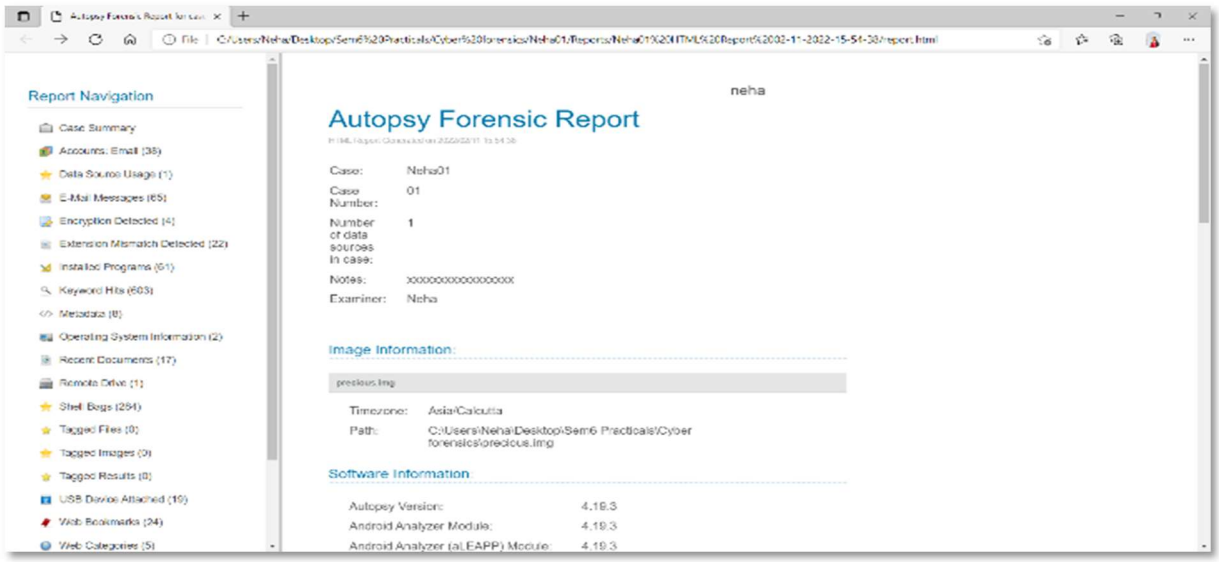


Click on all results radio button



Html report is generated click on link it will redirect to browser



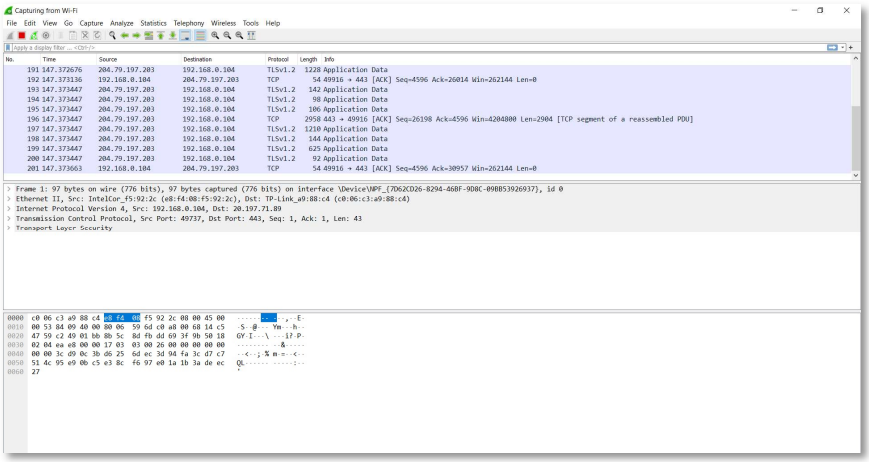


Practical 4

AIM: Capturing and analyzing network packets using Wireshark (Fundamentals) :
- Identification the live network
- Capture Packets
- Analyze the captured packets

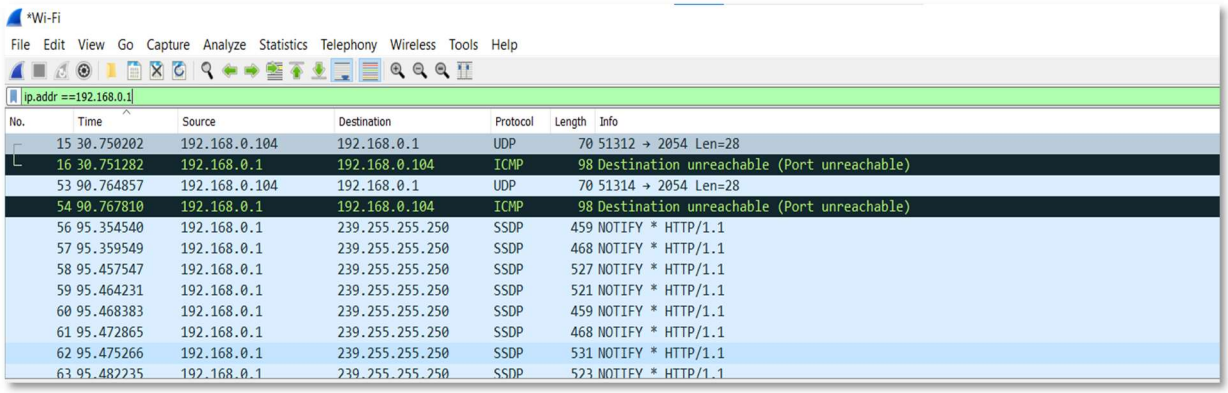
Capturing Packets
Select wifi/Ethernet

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

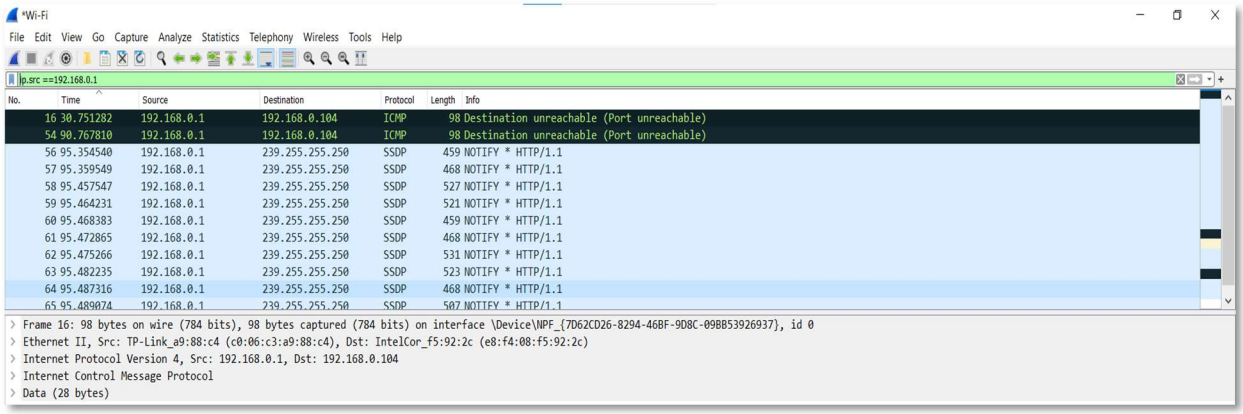


Display filter command –

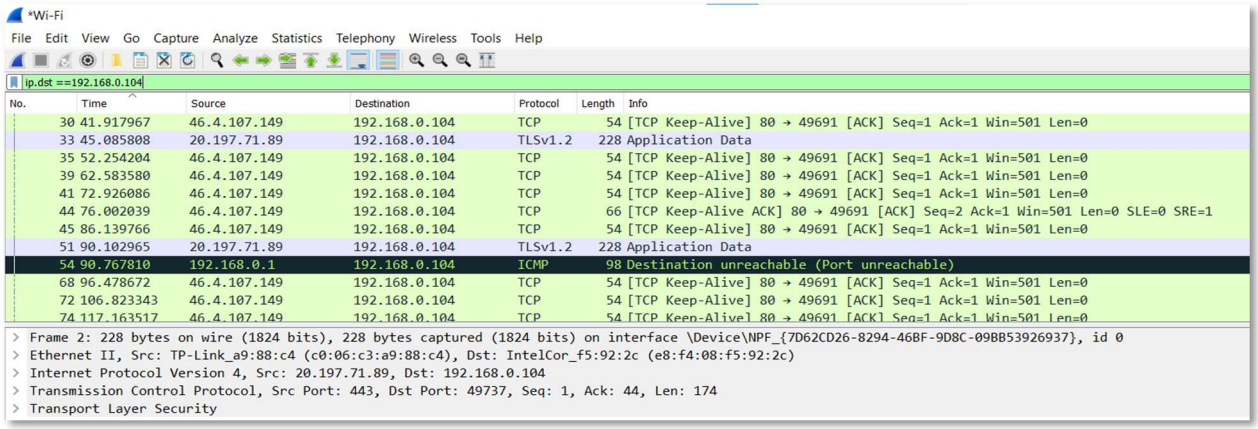
1. ip.addr ==192.168.0.1 (change ip based on current scenario)



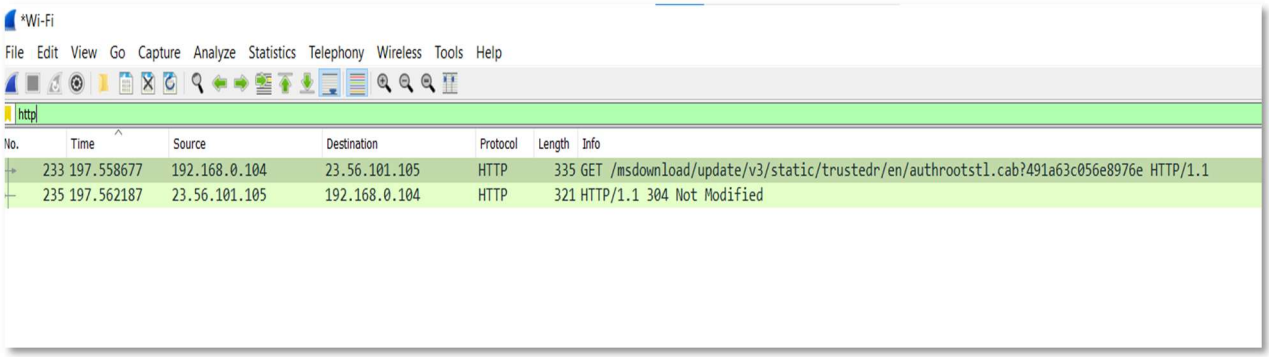
2. ip.src ==192.168.0.1 (change ip based on current scenario)



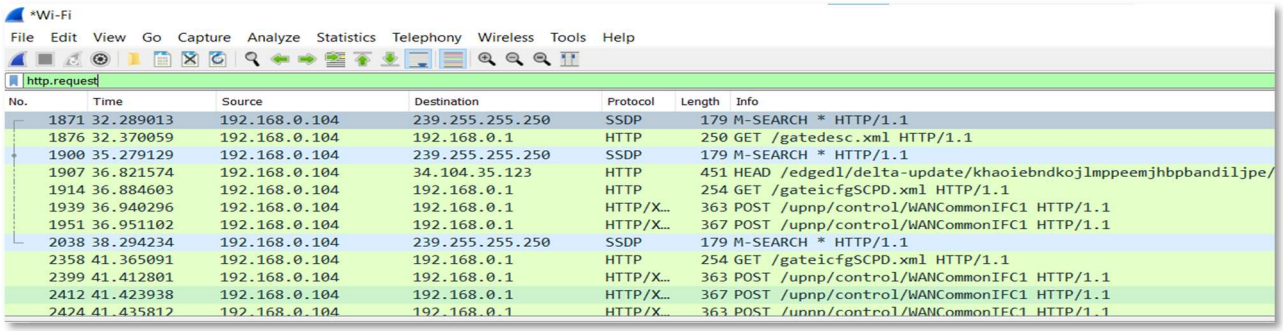
3. ip.dst ==192.168.0.104 (change ip based on current scenario)



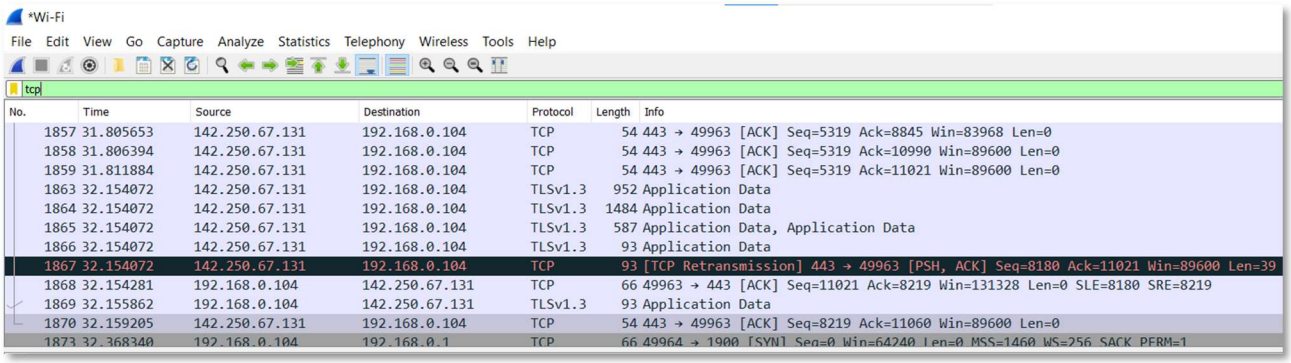
4. http (start recording and search for http website and visit any website which is of http)



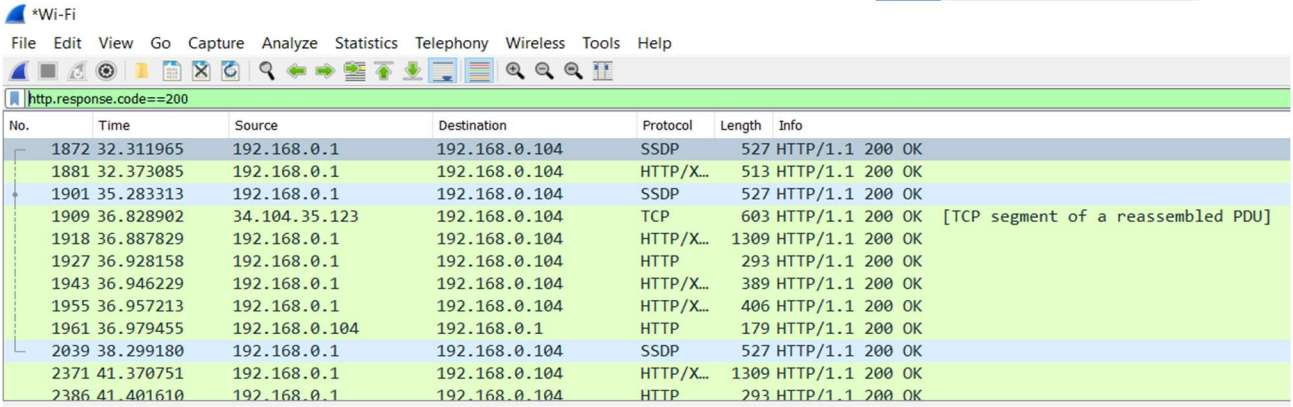
5. http.request



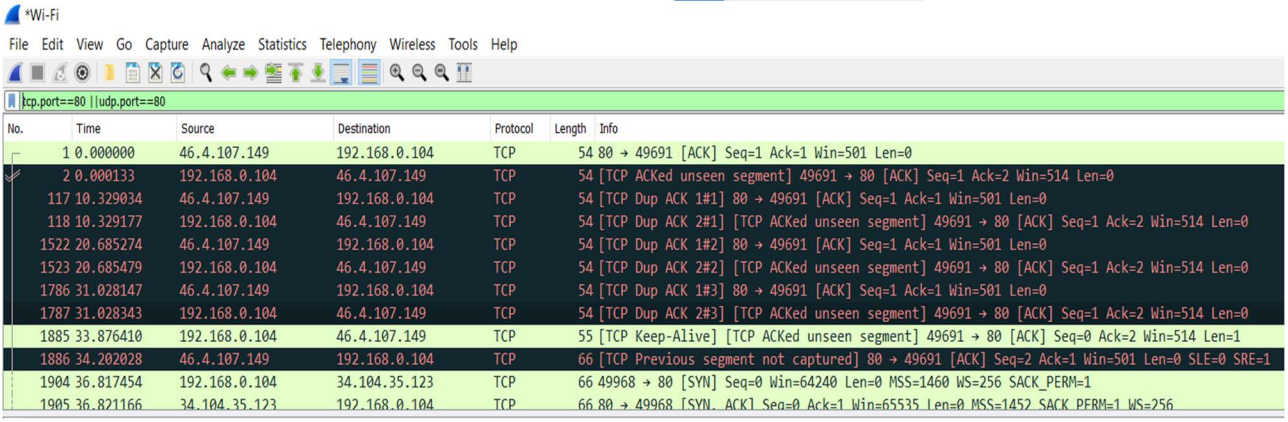
6. Tcp



7. **http.response.code==200**



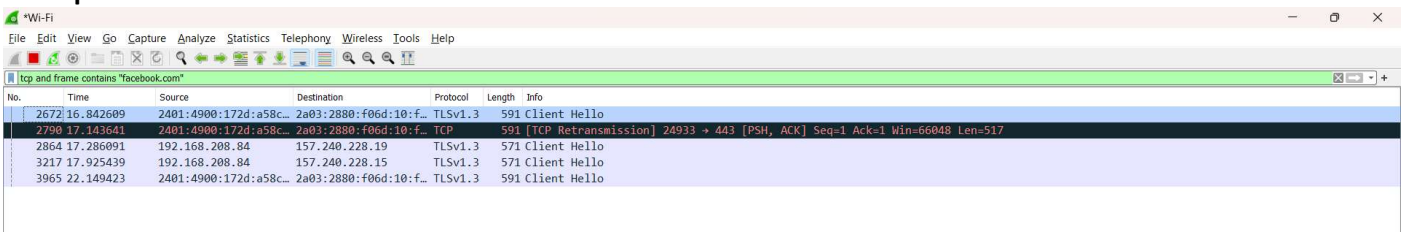
8. **tcp.port==80 ||udp.port==80**



9. Go to facebook.com

   tcp and frame contains "facebook.com"

   tcp and frame contains "facebook"



Practical 5

AIM :- Using Sysinternals tools for Network Tracking and Process Monitoring :

- Monitor LiveProcesses
- CaptureRAM
- Capture TCP/UDP packets
- Monitor HardDisk
- Monitor VirtualMemory
- Monitor CacheMemory

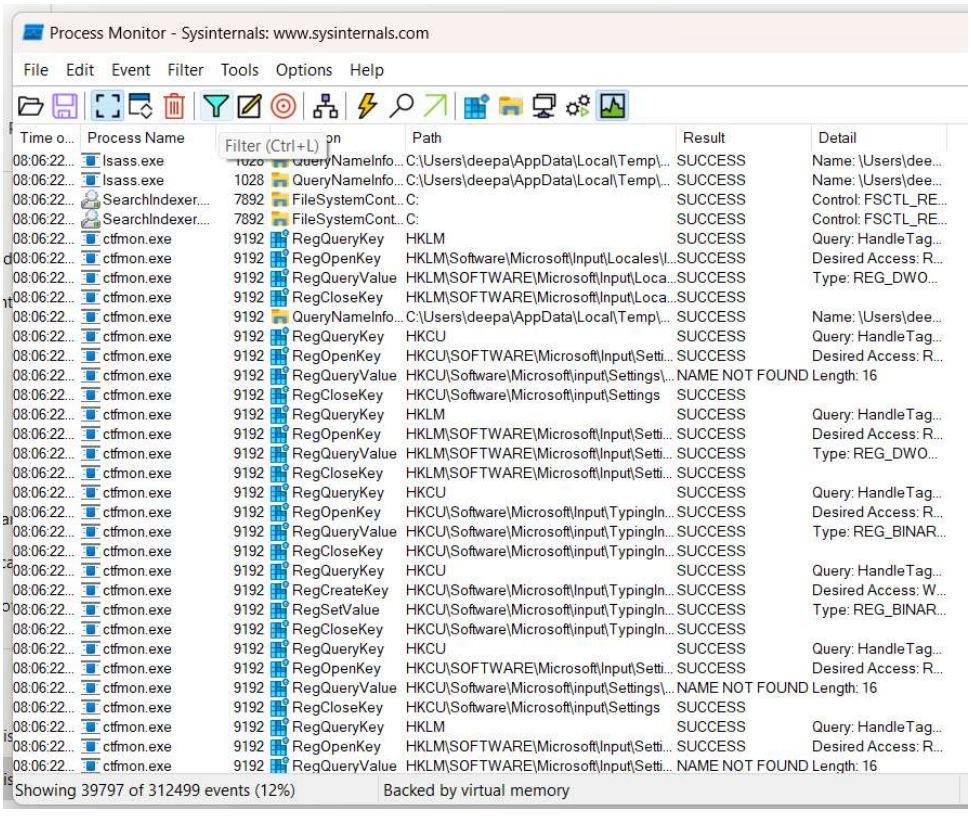
Monitor Live Processes : (Tool: ProcMon) ToDo:

1. Filter (Process Name or PID or Architecture,etc)
2. ProcessTree
3. Process ActivitySummary
4. CountOccurrences

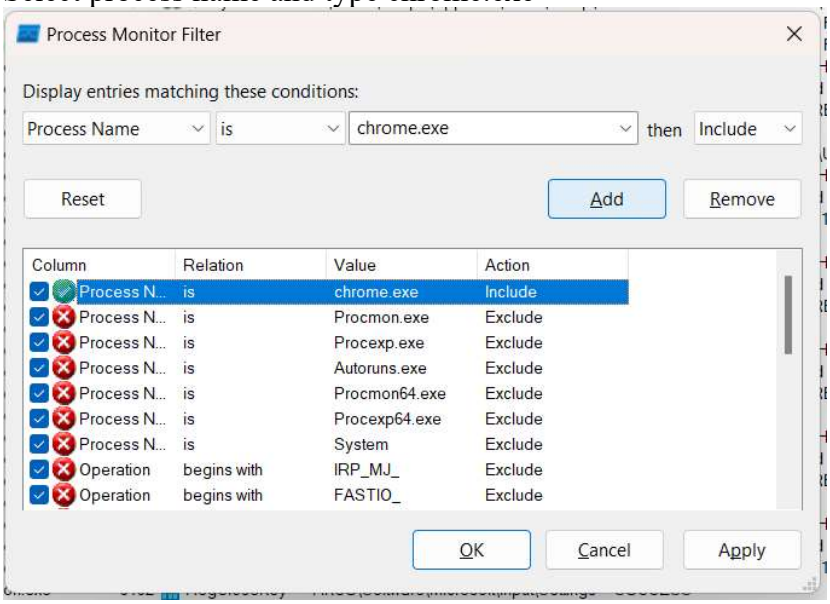
Filter (Process Name or PID or Architecture)

Open chrome and go to any website to start the process

Click on filter or Ctrl + L

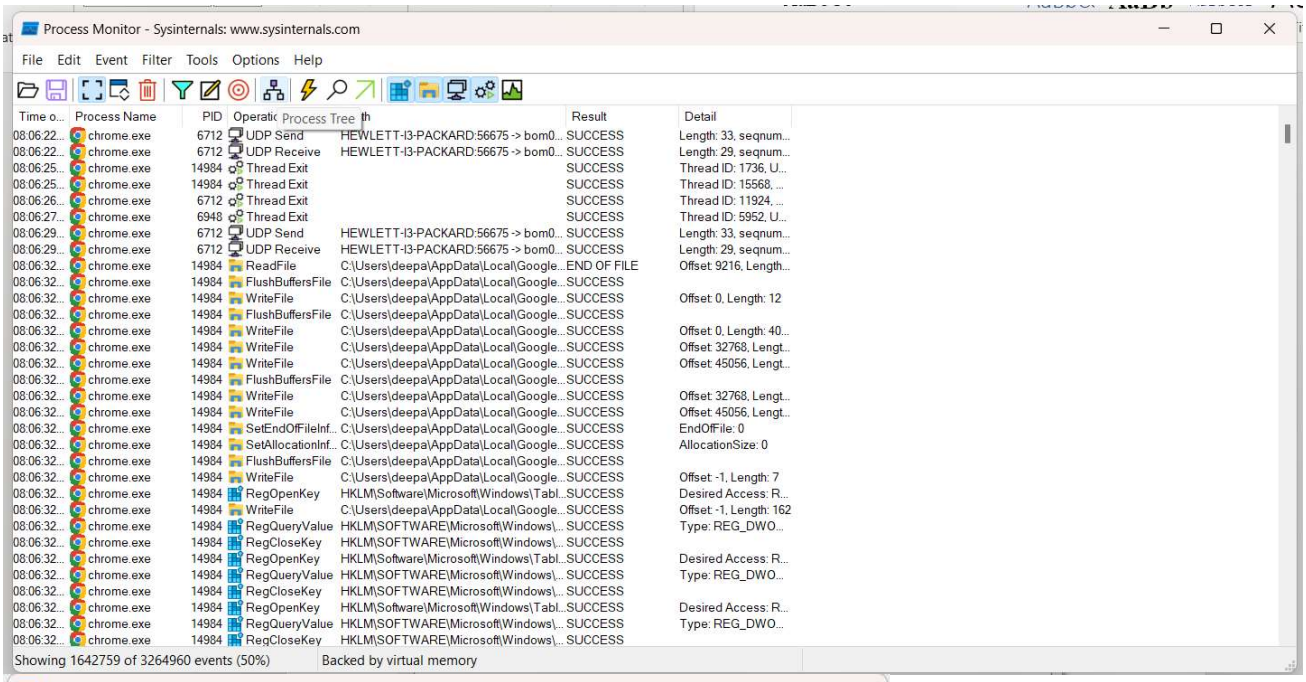


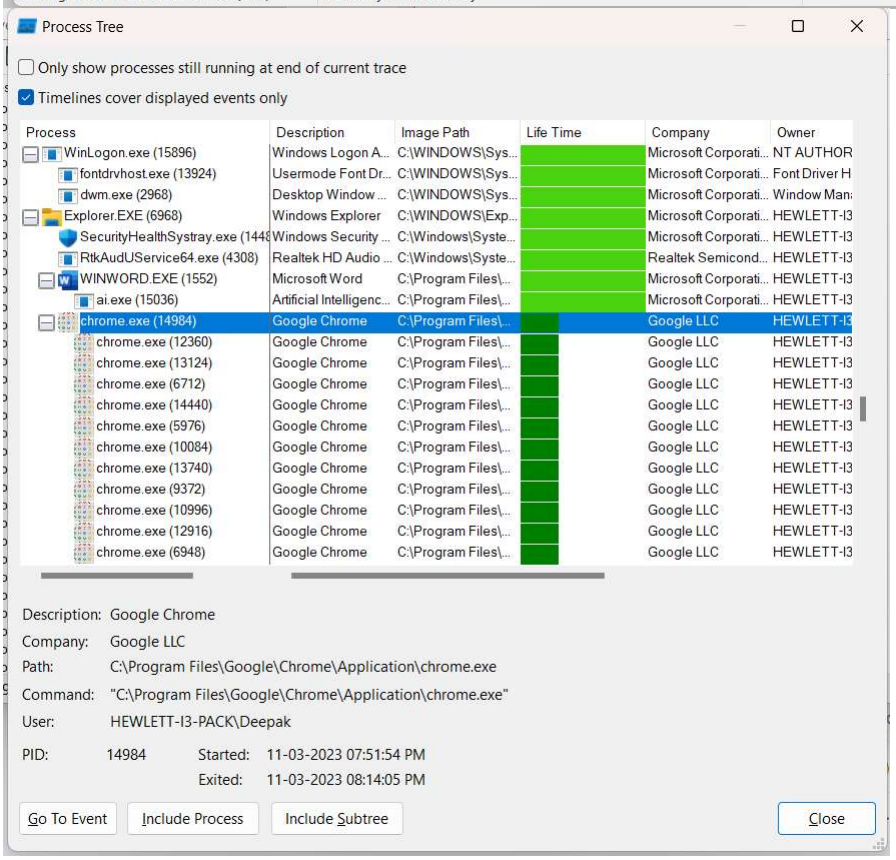
Select process name and type chrome.exe



ProcessTree

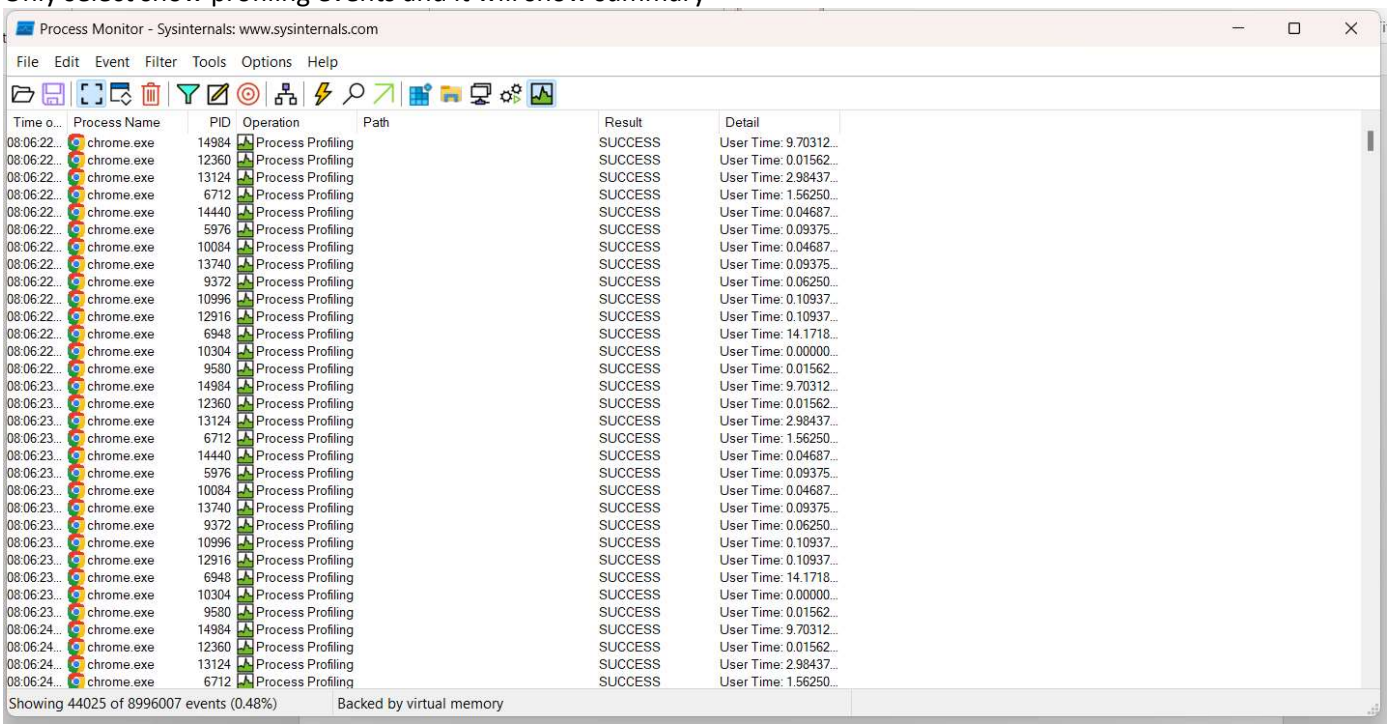
Select Process Tree





Process ActivitySummary

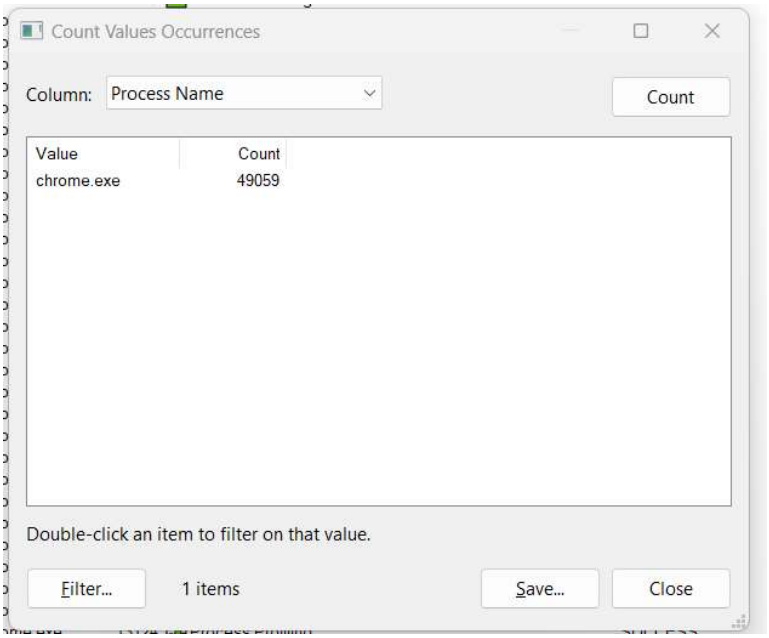
Only select show profiling events and it will show summary



Count Occurrences

Tools > Count Occurrence

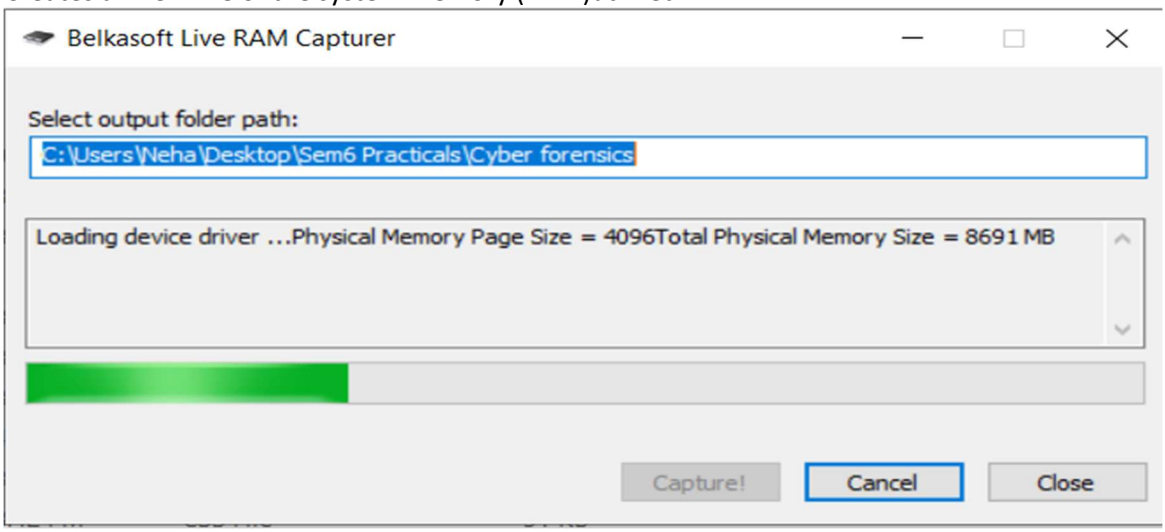
Select Process Name

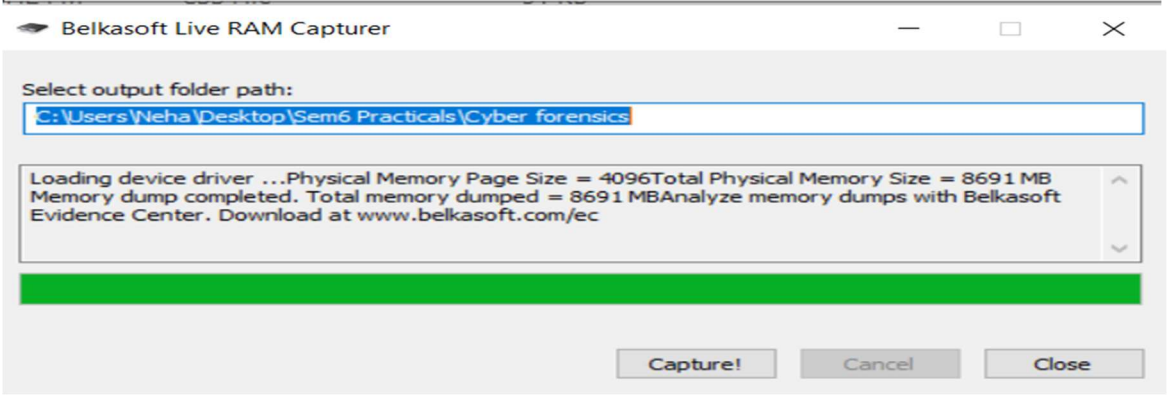


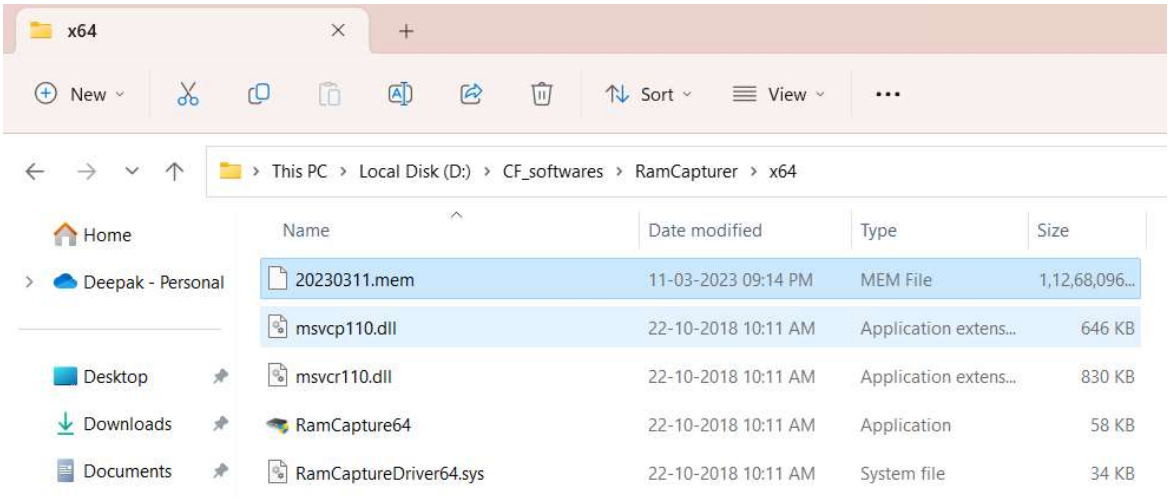
Capture RAM (Tool:RAMCapture)

To Do:

Click Capture
Creates a .mem file of the system memory (RAM)utilized.

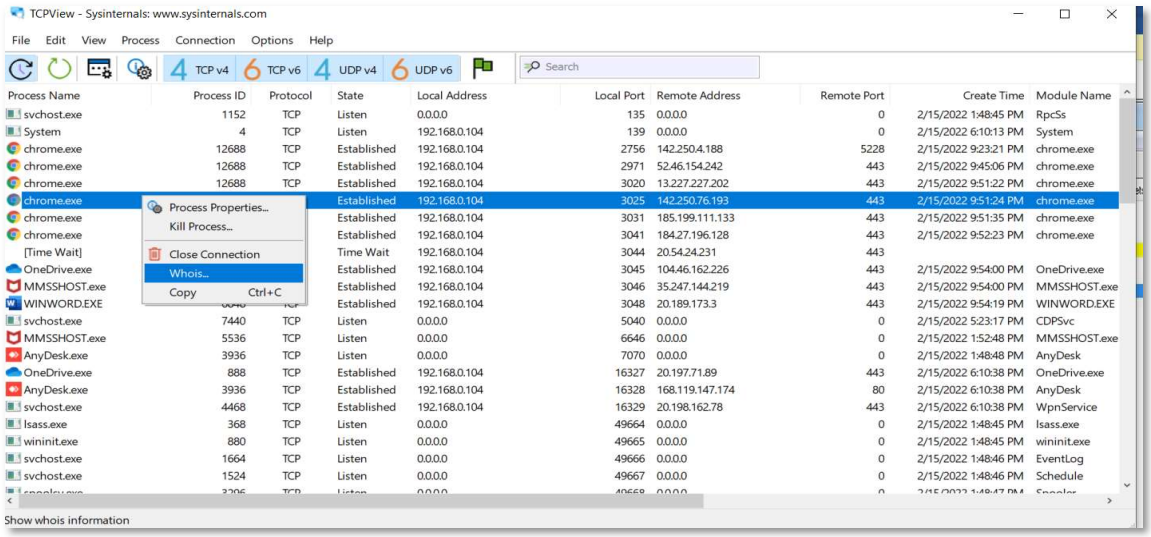


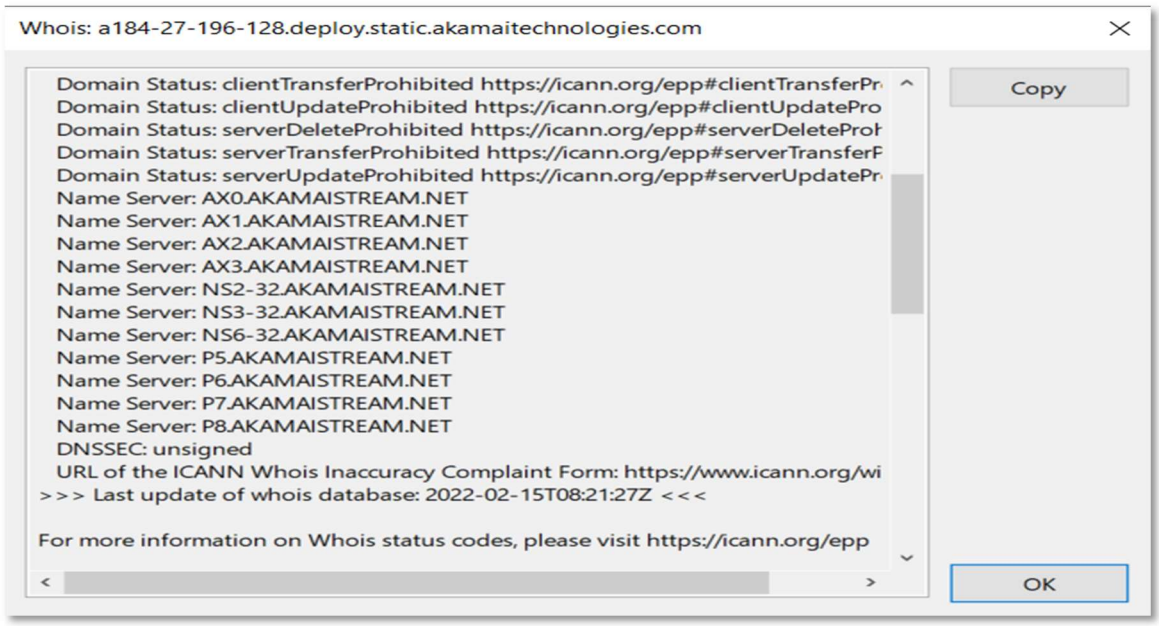




Capture TCP/UDP packets (Tool: TcpView):

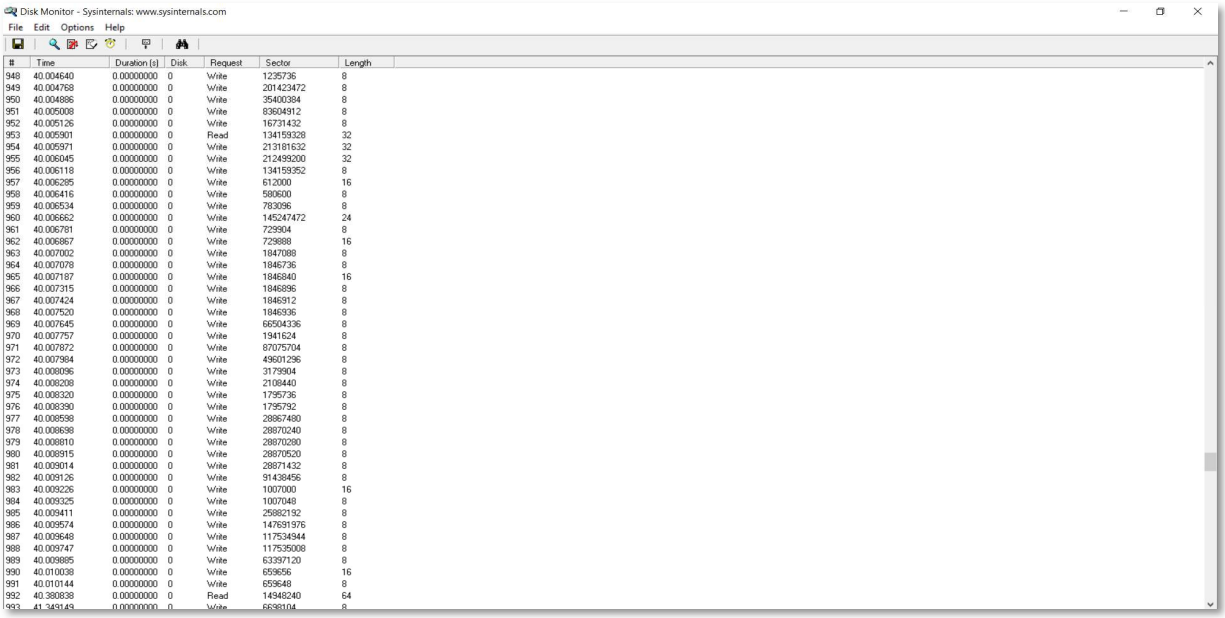
To Do: Save to .txtfile. as Whois





Monitor Hard Disk (Tool: DiskMon): To Do:

1. Save to .logfile.
2. Check operations performed in the disk as per time and sectors affected.

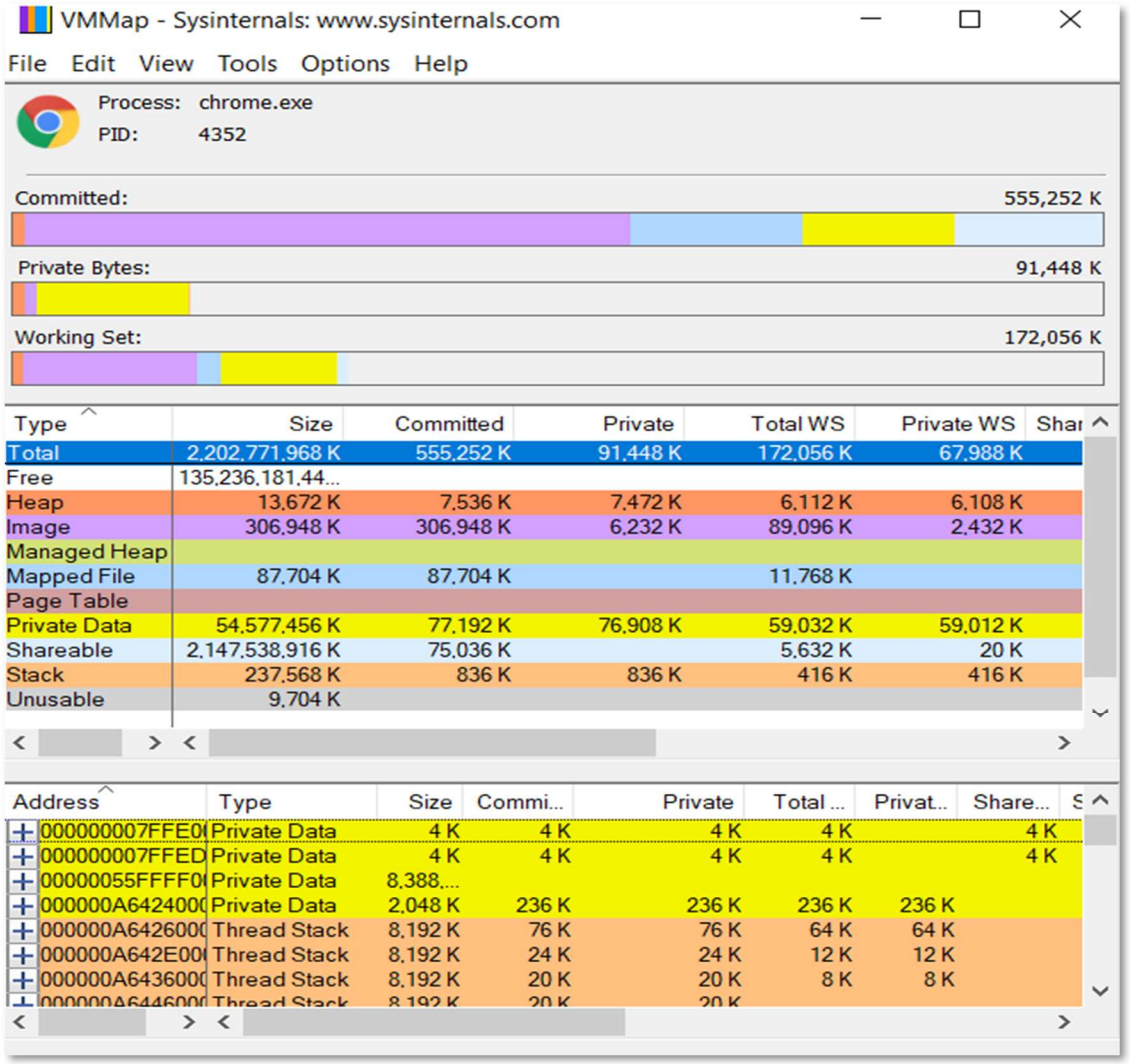


#	Time	Duration (s)	Disk	Request	Sector	Length
948	40.004640	0.00000000	0	Write	1235736	8
949	40.004768	0.00000000	0	Write	201423472	8
950	40.004886	0.00000000	0	Write	35400384	8
951	40.005008	0.00000000	0	Write	83604912	8
952	40.005126	0.00000000	0	Write	16731432	8
953	40.005901	0.00000000	0	Read	134159328	32
954	40.005971	0.00000000	0	Write	213181632	32
955	40.006045	0.00000000	0	Write	212499200	32
956	40.006118	0.00000000	0	Write	134159352	8
957	40.006295	0.00000000	0	Write	612000	16
958	40.006416	0.00000000	0	Write	580600	8
959	40.006534	0.00000000	0	Write	783096	8
960	40.006662	0.00000000	0	Write	145247472	24
961	40.006781	0.00000000	0	Write	729904	8
962	40.006867	0.00000000	0	Write	729888	16
963	40.007002	0.00000000	0	Write	1847088	8
964	40.007078	0.00000000	0	Write	1846736	8
965	40.007187	0.00000000	0	Write	1846840	16
966	40.007315	0.00000000	0	Write	1846896	8
967	40.007424	0.00000000	0	Write	1846912	8
968	40.007520	0.00000000	0	Write	1846936	8
969	40.007645	0.00000000	0	Write	66504336	8
970	40.007757	0.00000000	0	Write	1941624	8
971	40.007872	0.00000000	0	Write	87075704	8
972	40.007984	0.00000000	0	Write	49601296	8
973	40.008096	0.00000000	0	Write	3179904	8
974	40.008208	0.00000000	0	Write	2108440	8
975	40.008320	0.00000000	0	Write	1795736	8
976	40.008390	0.00000000	0	Write	1795792	8
977	40.008598	0.00000000	0	Write	28867480	8
978	40.008698	0.00000000	0	Write	28870240	8
979	40.008810	0.00000000	0	Write	28870280	8
980	40.008915	0.00000000	0	Write	28870520	8
981	40.009014	0.00000000	0	Write	28871432	8
982	40.009126	0.00000000	0	Write	91438456	8
983	40.009226	0.00000000	0	Write	1007000	16
984	40.009325	0.00000000	0	Write	1007048	8
985	40.009411	0.00000000	0	Write	25882192	8
986	40.009574	0.00000000	0	Write	147691976	8
987	40.009648	0.00000000	0	Write	117534944	8
988	40.009747	0.00000000	0	Write	117535008	8
989	40.009885	0.00000000	0	Write	63397120	8
990	40.010038	0.00000000	0	Write	659656	16
991	40.010144	0.00000000	0	Write	659648	8
992	40.380838	0.00000000	0	Read	14948240	64
993	41.349143	0.00000000	0	Write	6636104	8

Monitor Virtual Memory (Tool : VMMAP):

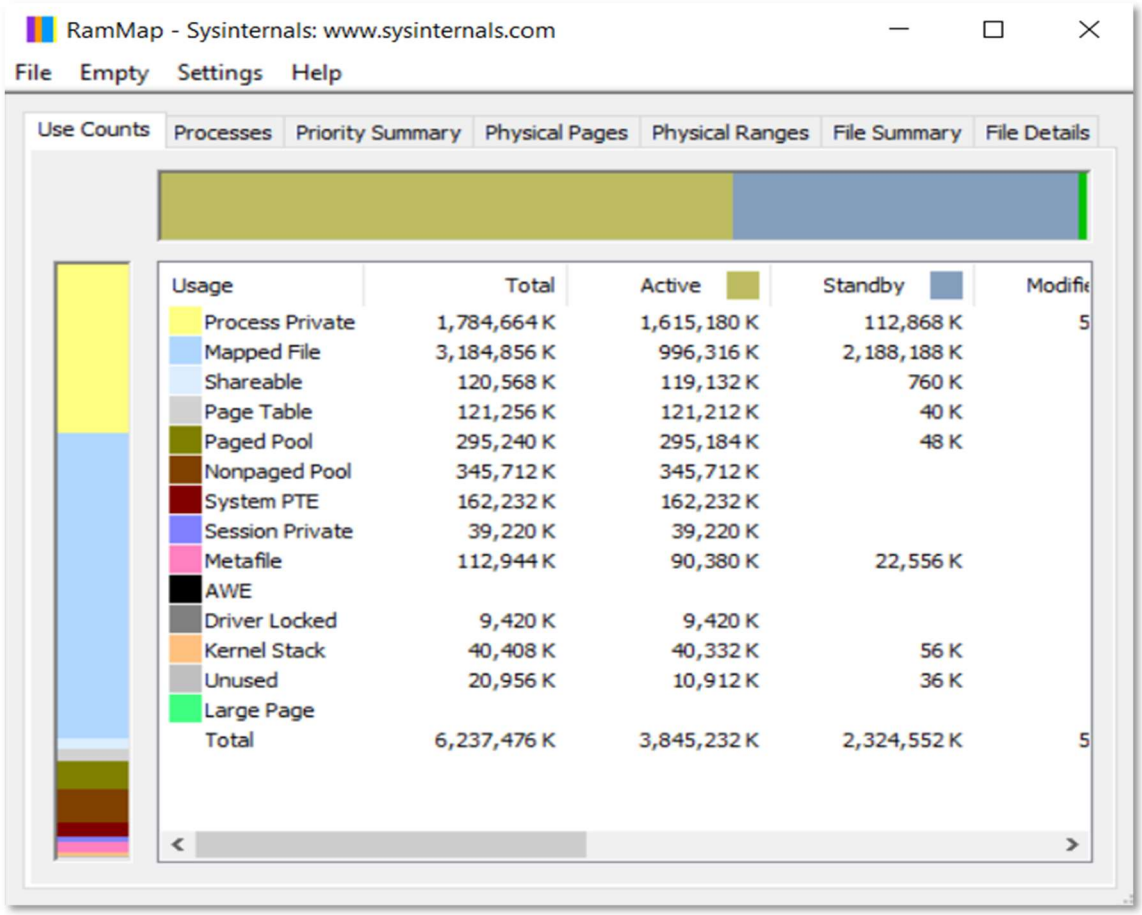
To Do:

e.g.chrome.exe Save to .mmpfile.



Monitor Cache Memory
(Tool:RAMMap) TO DO :

1. Save to .RMPfile.



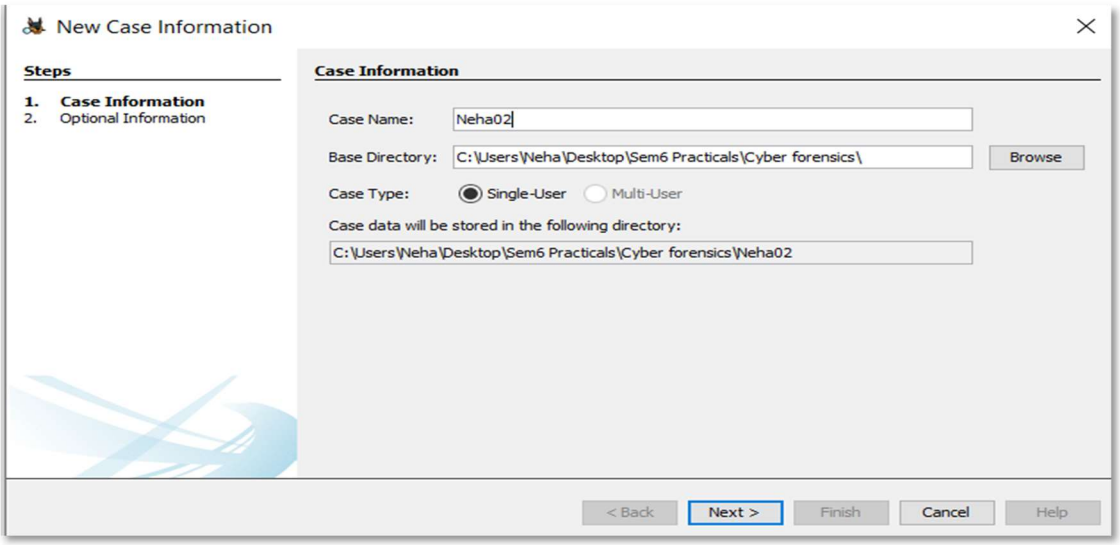
Practical 6

AIM: Recovering and Inspecting deleted files

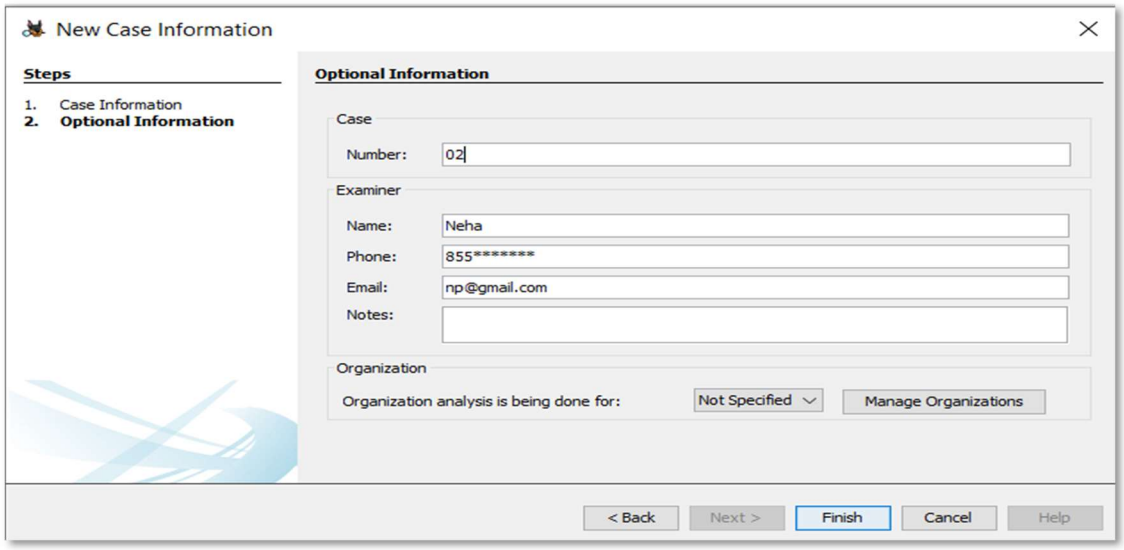
- Check for Deleted Files
- Recover the Deleted Files
- Analyzing and Inspecting the recovered files

Step 1 start autopsy from desktop Now create on New Case.

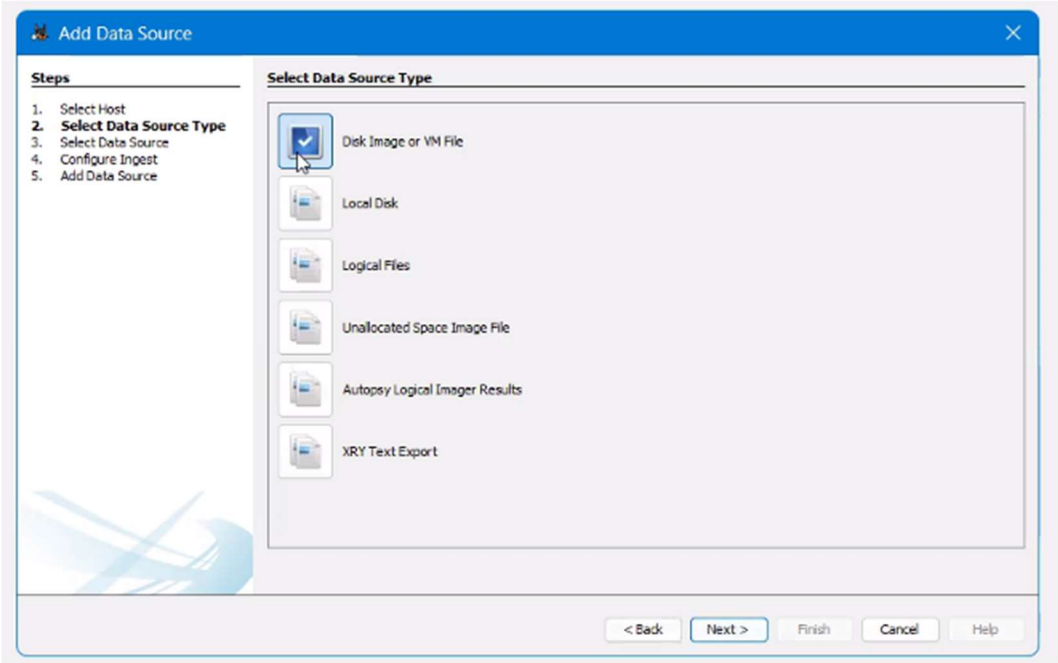
Step 2: Enter the New case Information and click on Next Button.



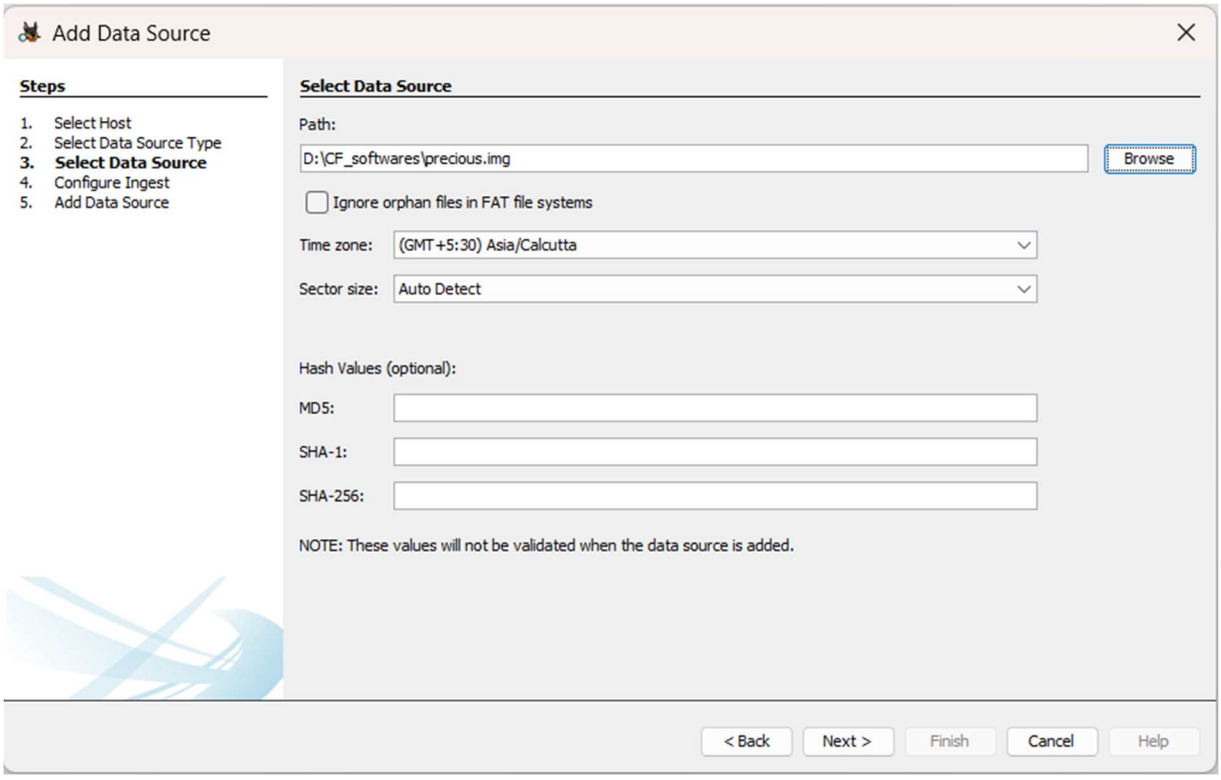
Step 3: Enter the additional Information and click on Finish.



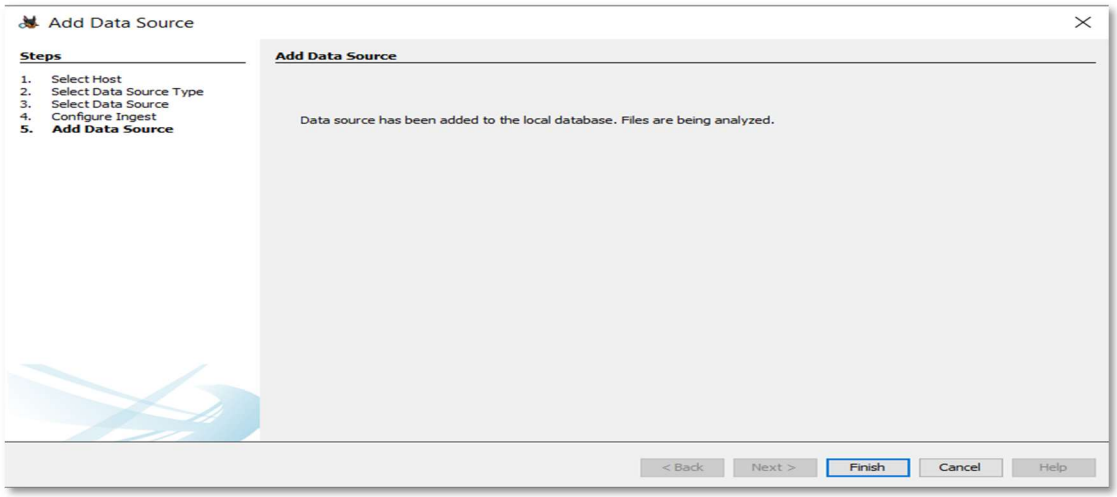
Step 4: Now Select Source Type as Local disk and Select Local disk form drop down list and click on Next.



Step 5: add precious.img



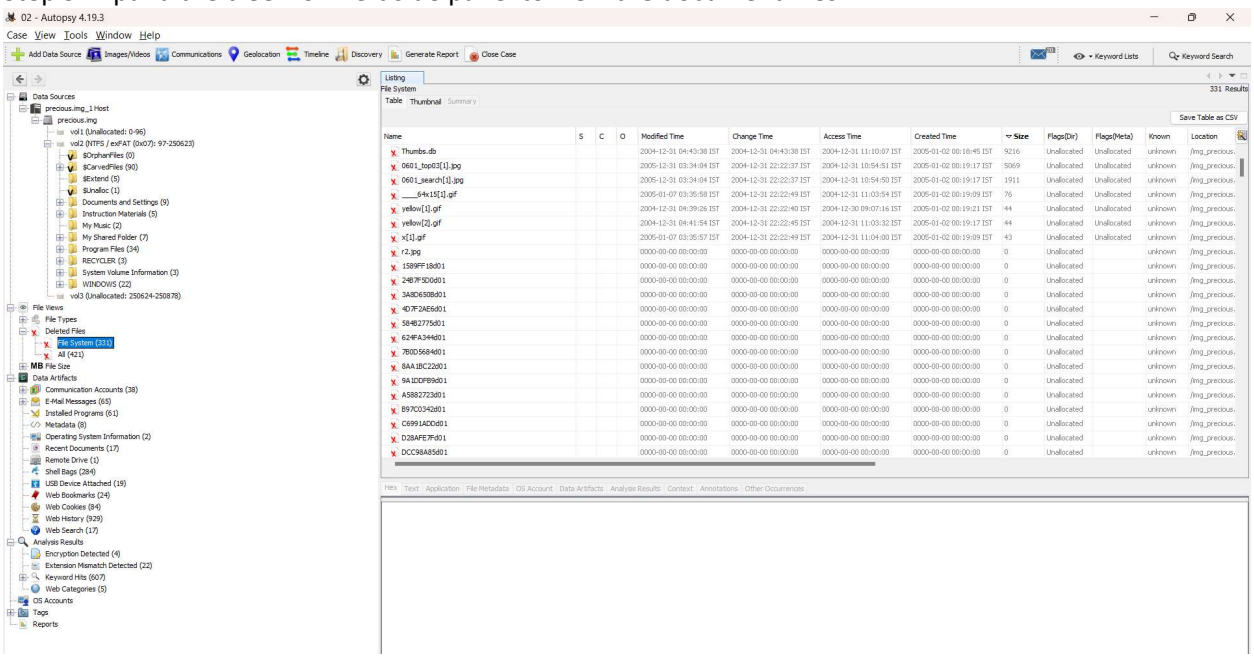
Step 6: Now click On Finish.



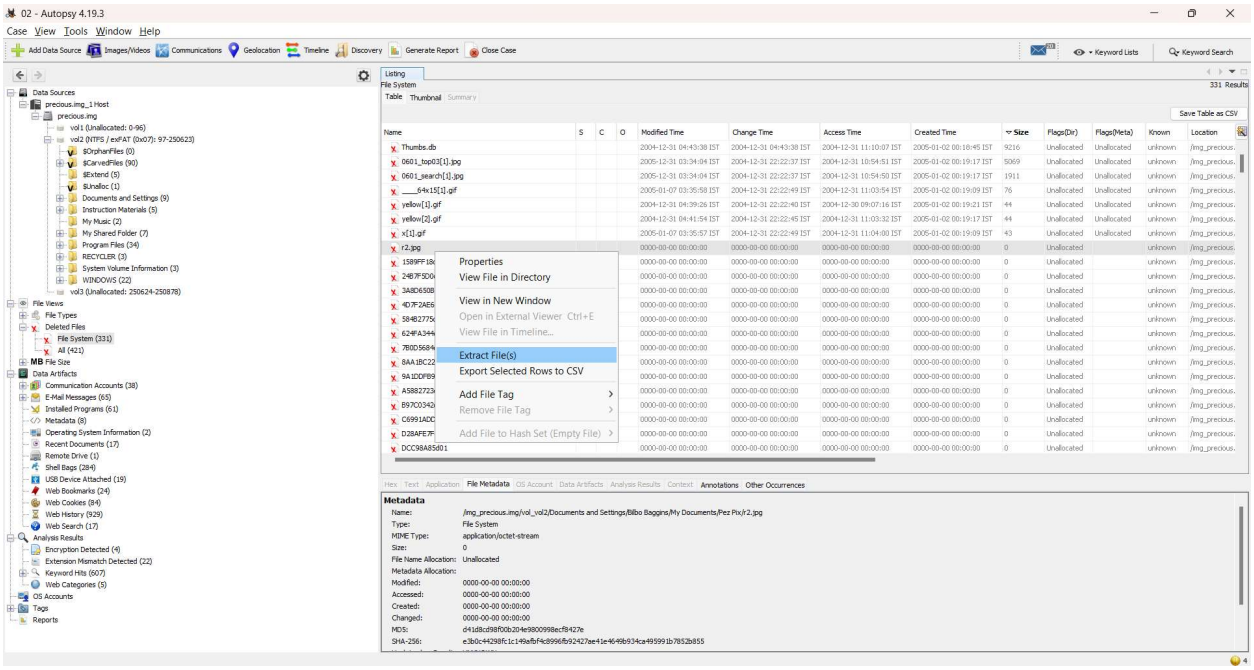
Step 7: Now Autopsy window will appear and it will analyzing the disk that we have selected.

Step 8: All files will appear in table tab select any file to see the data.

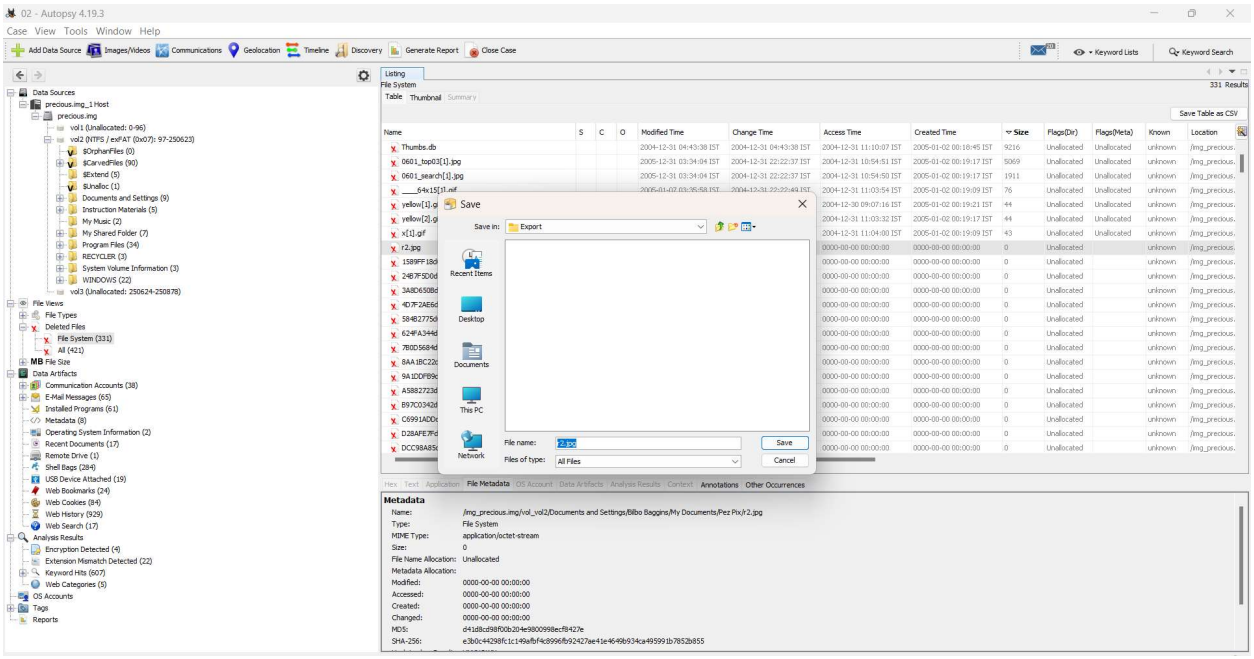
Step 9:Expand the tree from left side panel to view the document files.



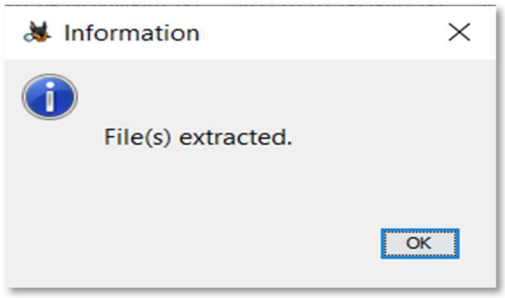
Step 10: To recover the file, go to Deleted Files > File System , here select any file and right click on it than select Extract Files option.



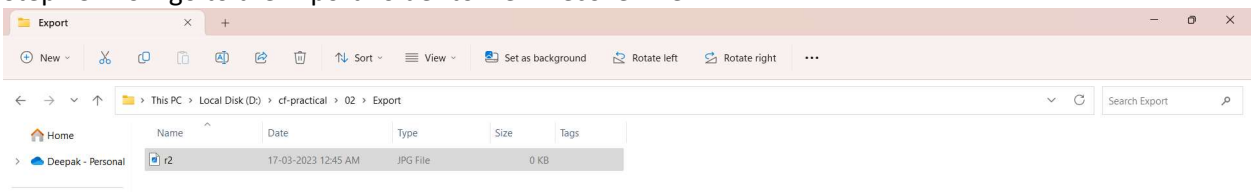
Step 11: By default Export folder is choose to save the recovered file.



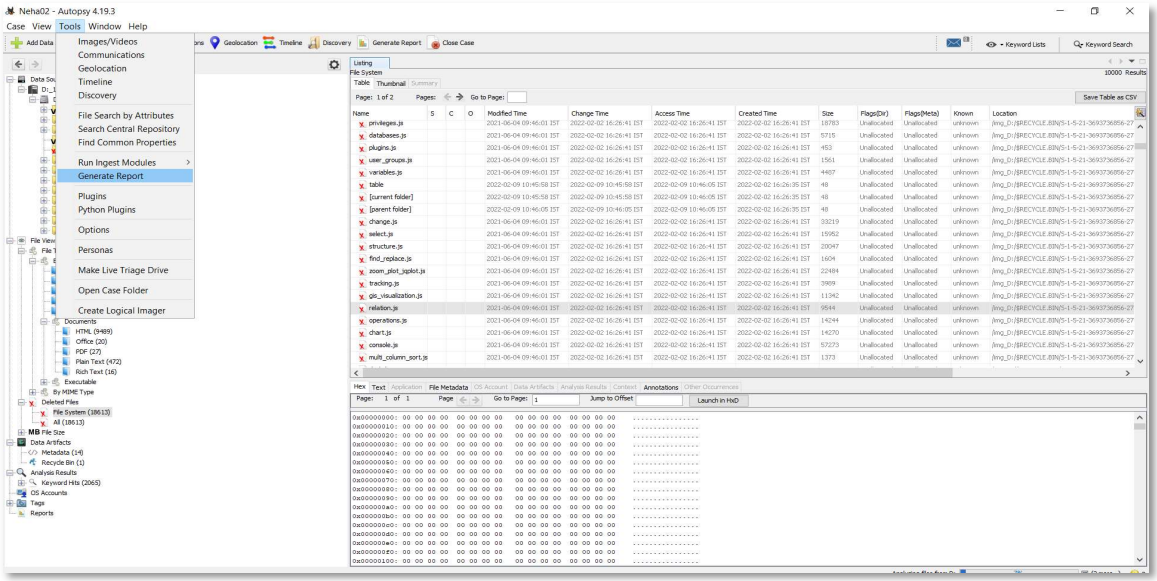
Step 12 : Now Click on Ok.

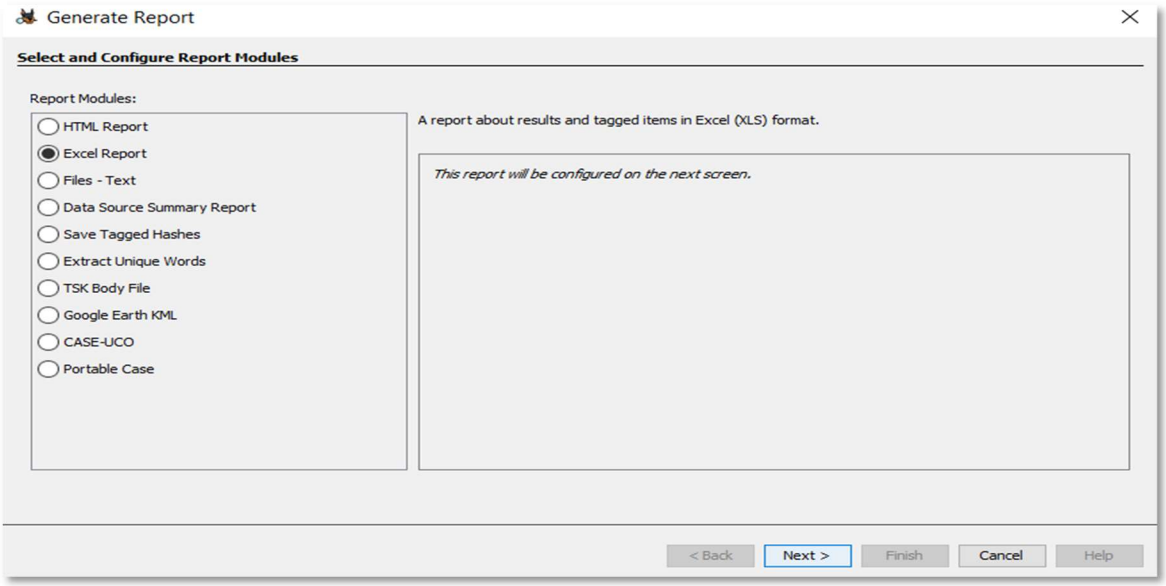


Step 13: Now go to the Export Folder to view Recover file.

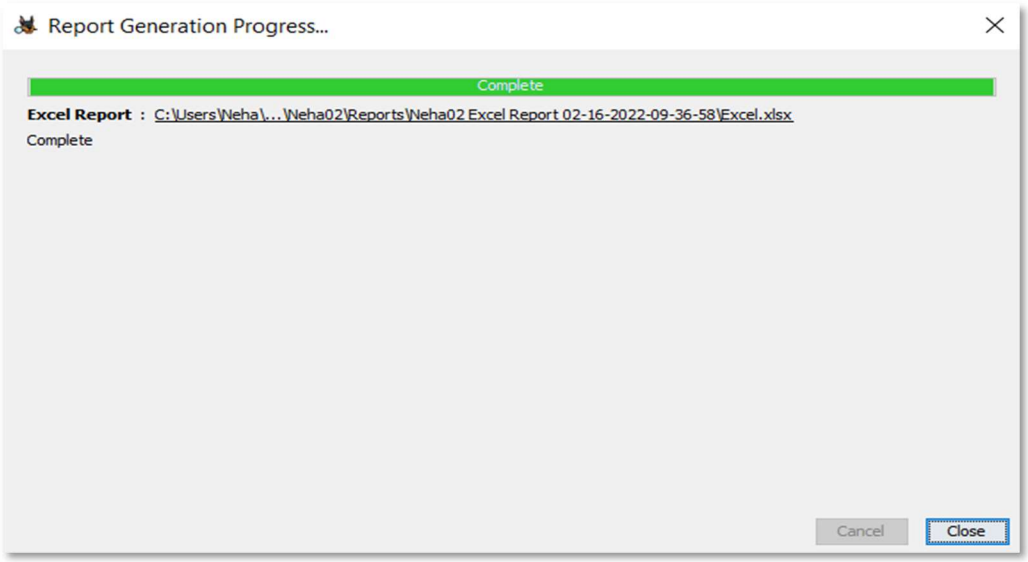


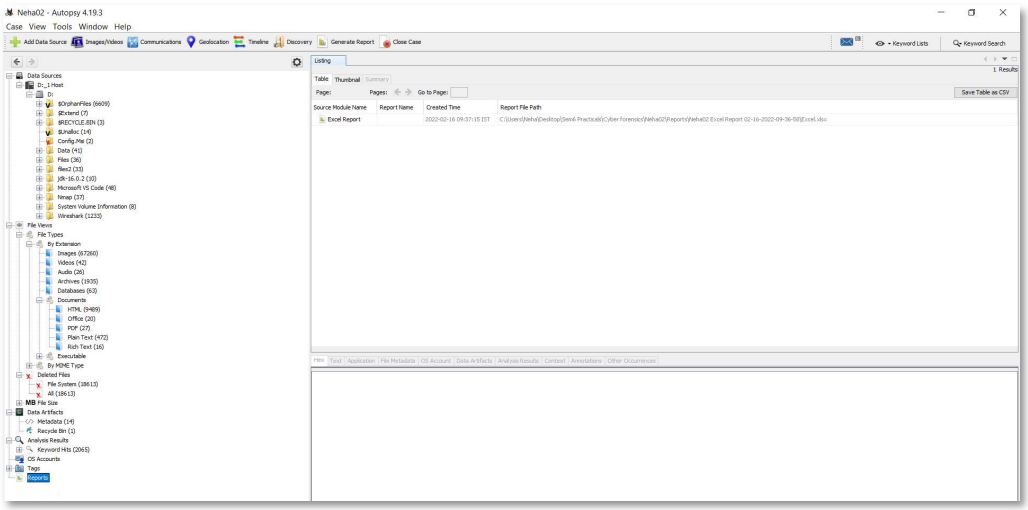
Step 14: Click on Generate Report from autopsy window and Select the Excel format and click on next.



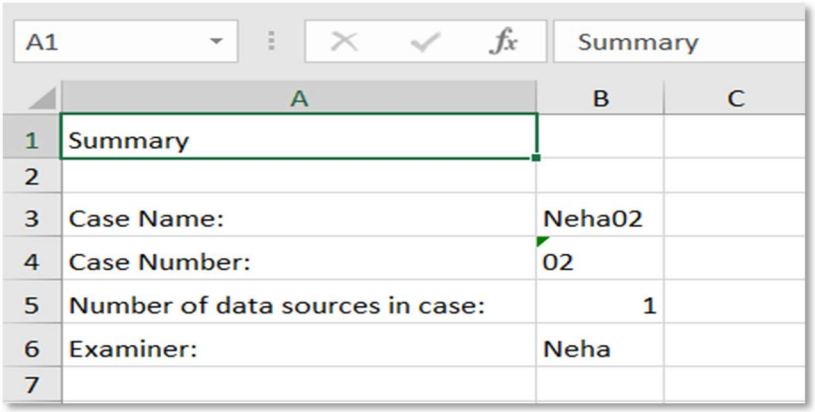


Step 15: Now Report is Generated So click on close Button .we can see the Report on Report Node.





Step 17: Now open the Report folder and Open Excel File.



	A	B	C
1	Summary		
2			
3	Case Name:	Neha02	
4	Case Number:	02	
5	Number of data sources in case:	1	
6	Examiner:	Neha	
7			

Practical 7

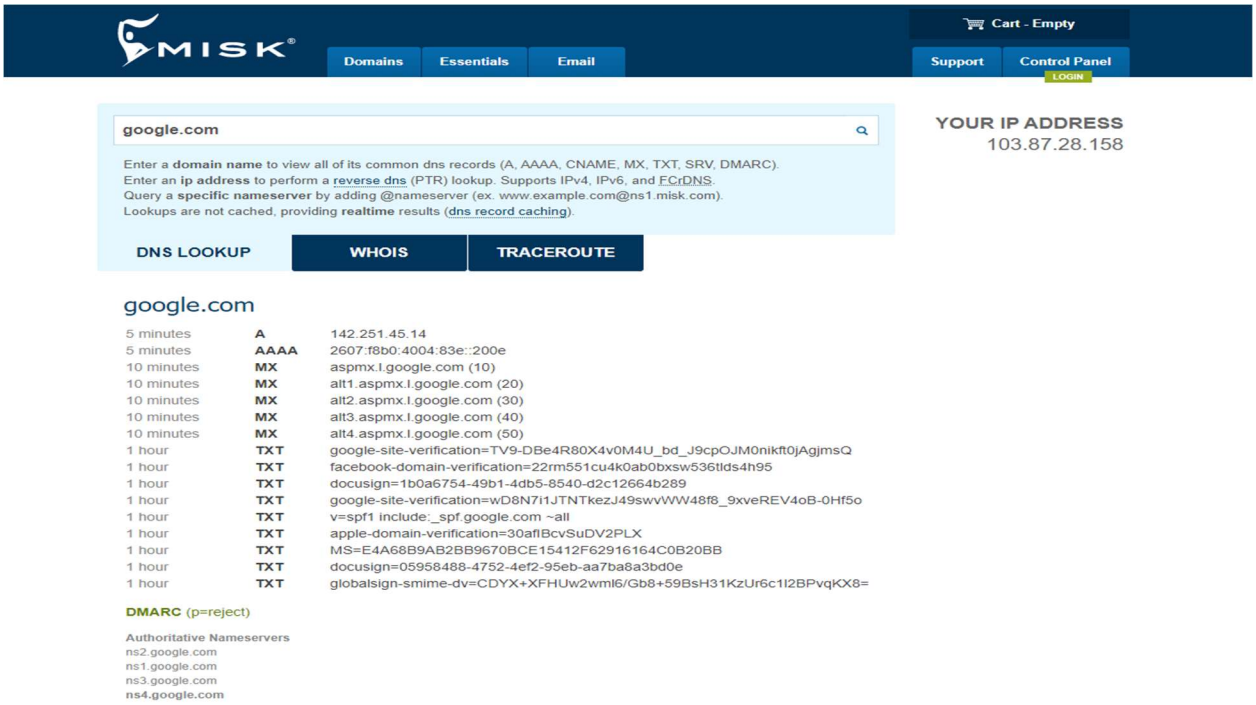
AIM: Email Forensics –

1. Mail Service Providers

Step 1 : Find MX Record.

MX records points a domain's incoming email provider responsible for processing those messages.

a) Go to http://www.misk.com/tools/ # dns
b) Enter your domain name.
c) Press Enter on your keyboard. A list of all dns records for the name will appear.
d) Copy the Ip address of A

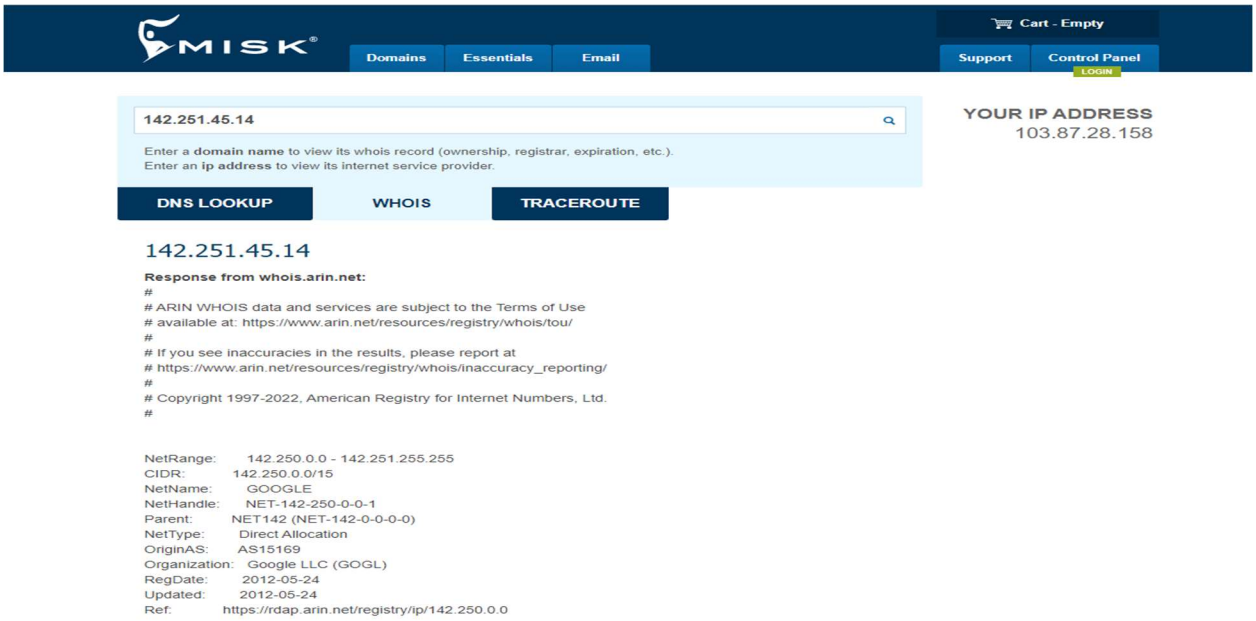


2. IP WHOIS:

a) Go the same site select whois and enter the copied hostname.

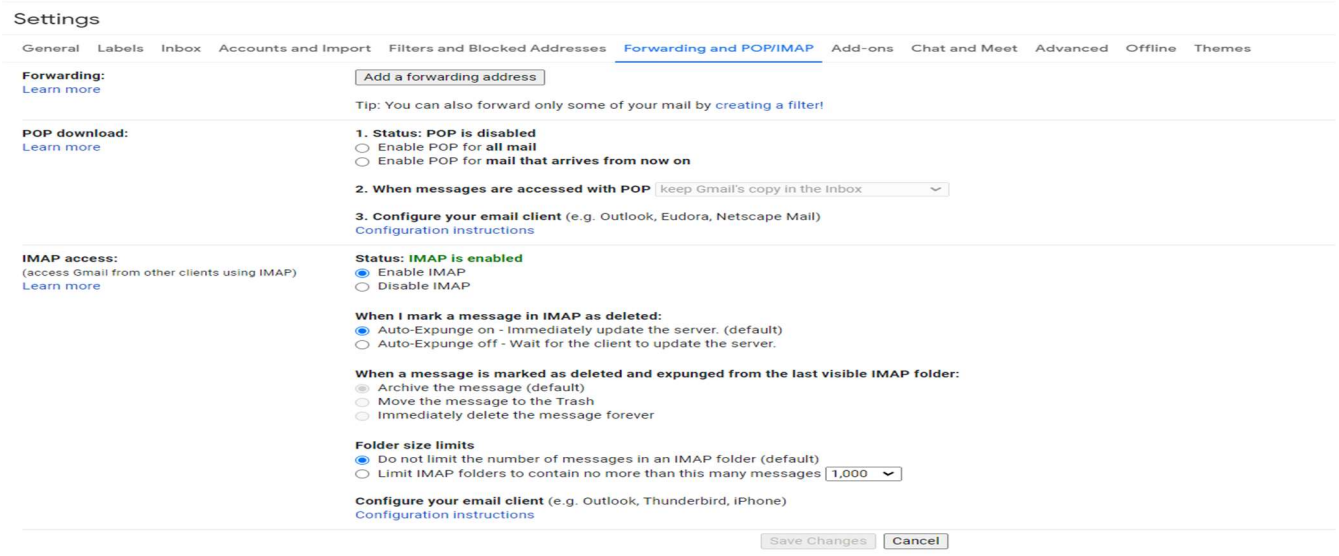
b) Press enter on your keyboard.

c) The IP address whois record will appear.



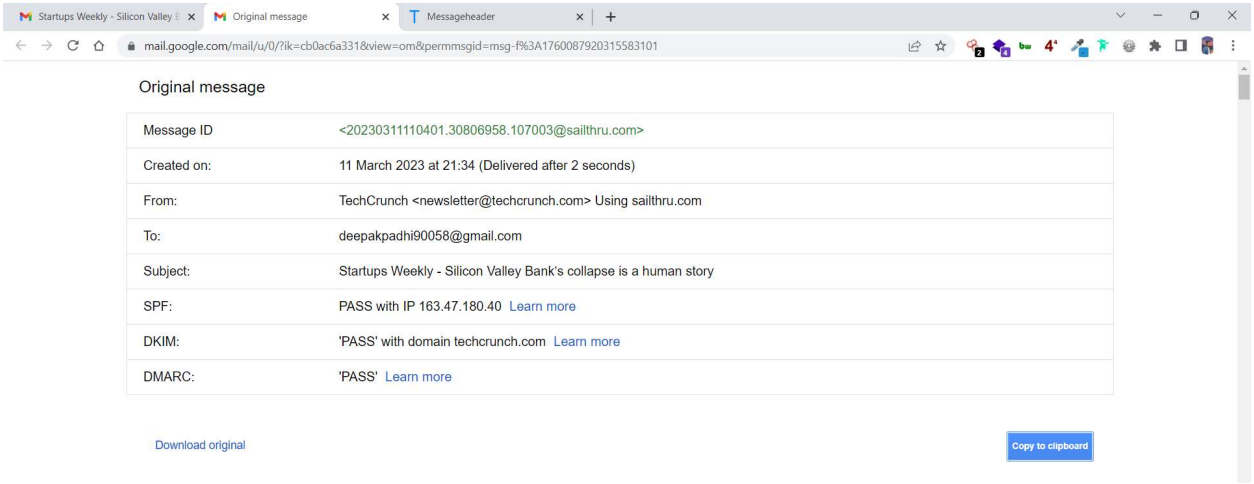
3. Email protocols –

a) On your computer, open Gmail.
b) In the top right corner, click settings.
c) Click on forwarding and POP/IMAP tab
d) Now you can see that which protocol your email is using. Here it is using POP and IMAPs

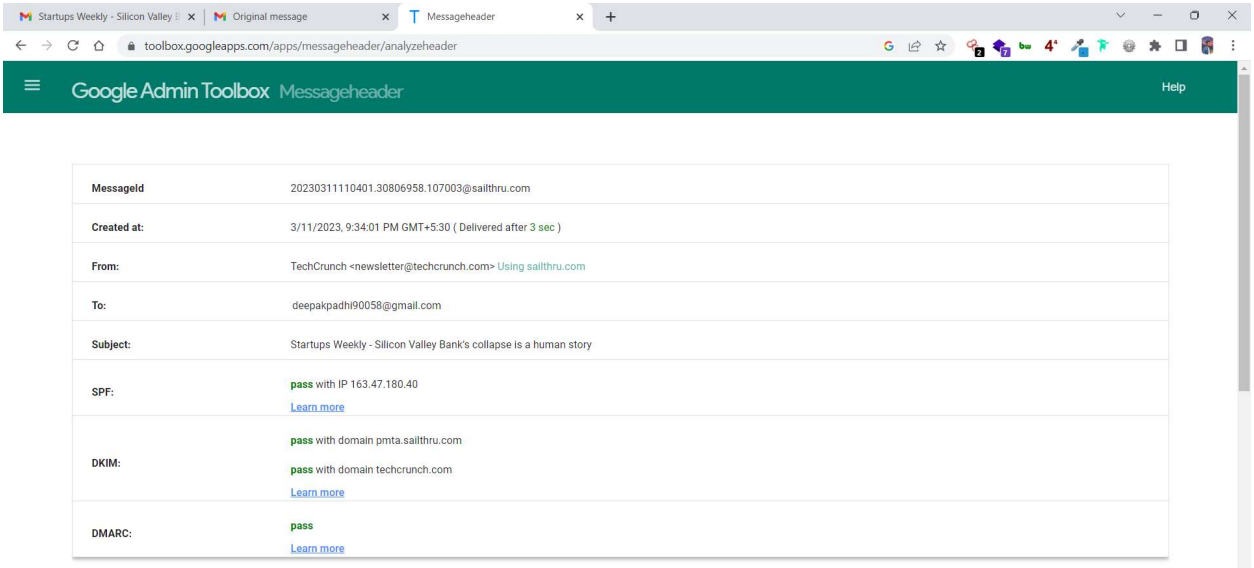


4. Analyzing email headers.

a) Open the email you want to analyze the header for.
b) Next to reply, click on the three dots.
c) Click show original.
d) Click on copy to clipboard.

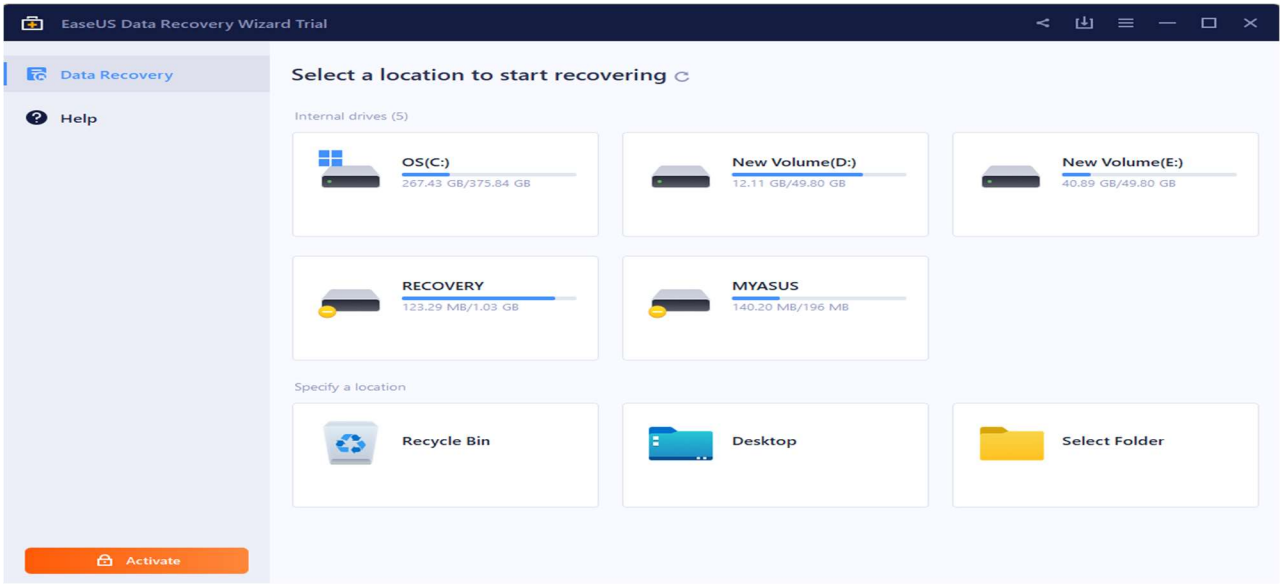


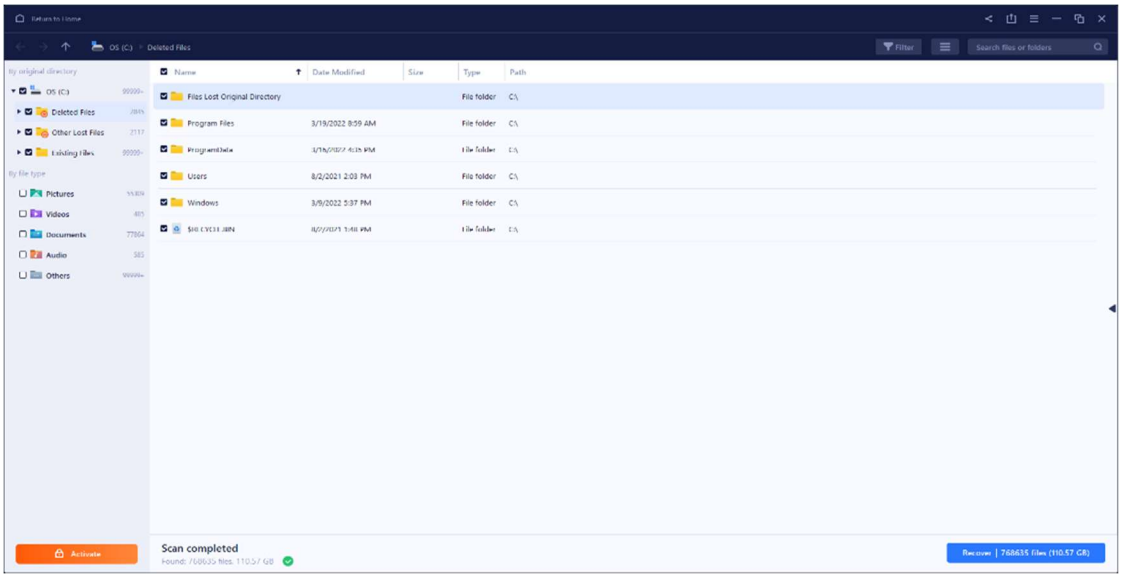
e) Open the message header tool. (http://toolbox.googleapps.com/messageheader)
f) Paste the header the paste box.
g) Then click on analyse the above header.



5. Recovering emails –

1. To recover the emails here we are using EaseUS recovery tools.
Run the email recovery software.
2. Click on scan to let the software scan and find the lost emails.
Step 2:
1. Find the lost emails .
2. Deleted files: If you accidentally delete the email files, they will appear.
3. Lost files: All lost files will appear here.





Practical 8

Aim: Web Browser Forensics .

-Web Browser working

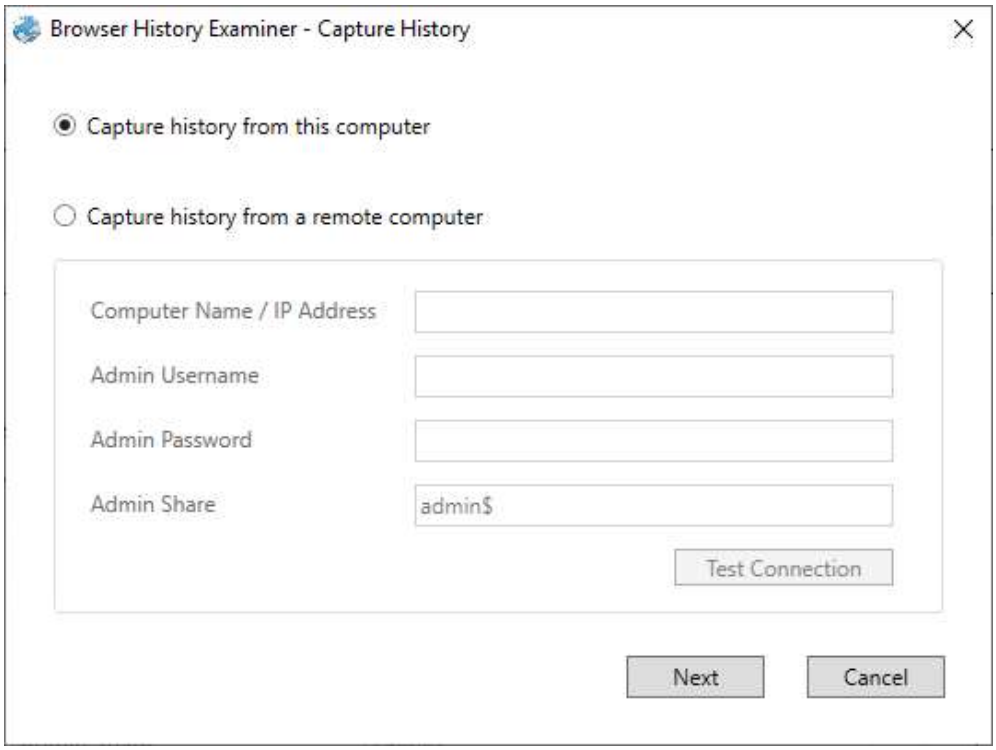
-Forensics activities on browser

-Cache / Cookies analysis

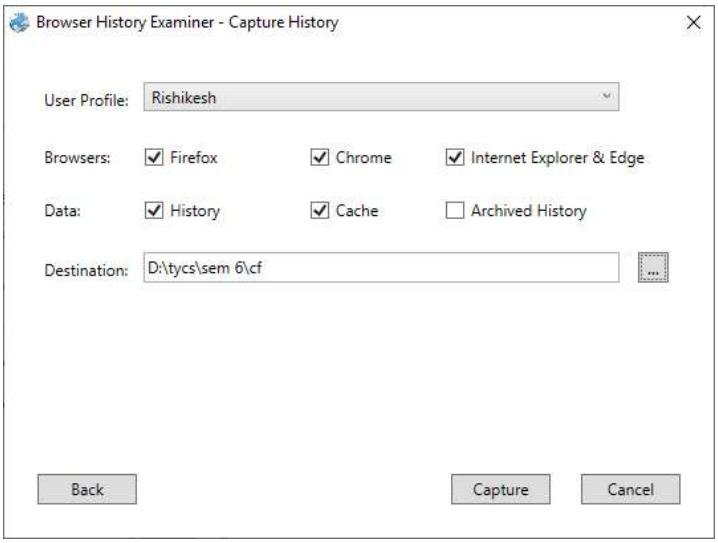
-Last Internet activity

Steps:

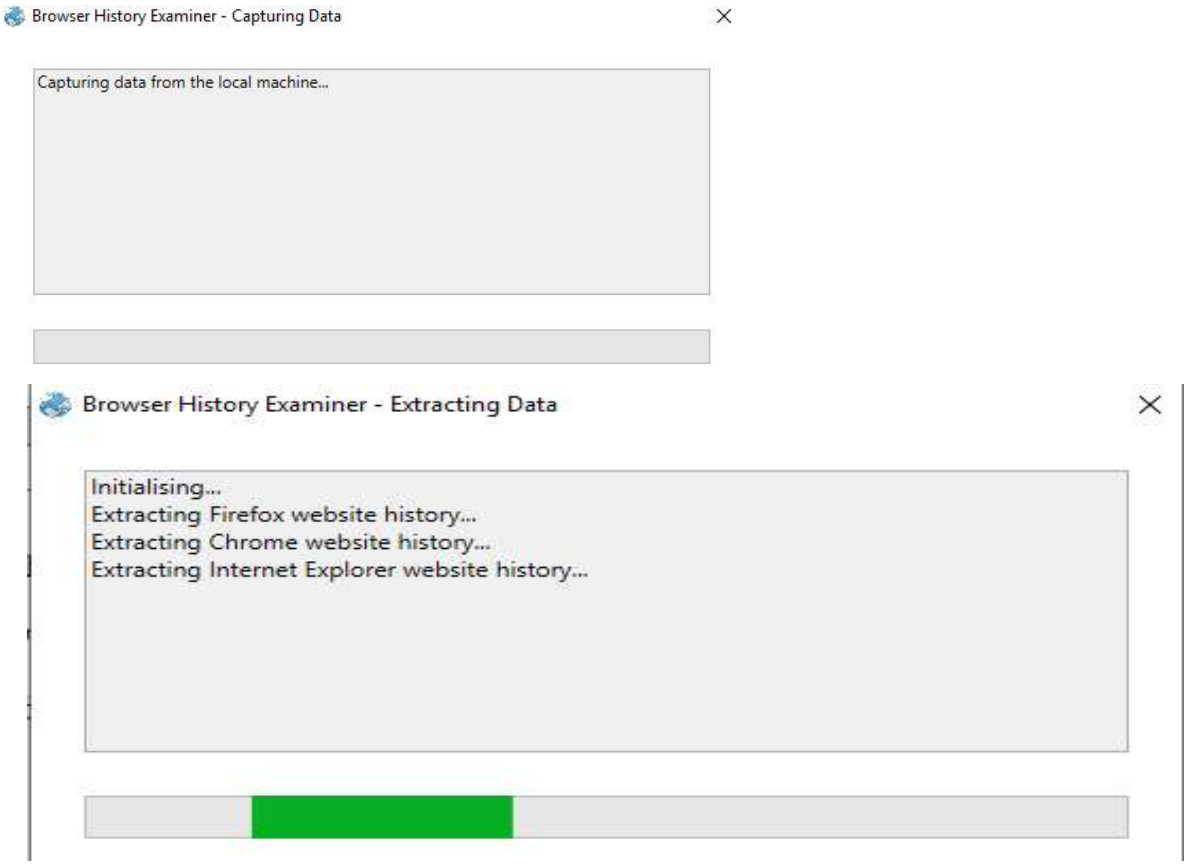
1. Download and install BrowserHistoryExaminer.
2. Open BrowserHistoryExaminer.
3. Click on continue trail
4. Click on Capture history
5. Select the default.



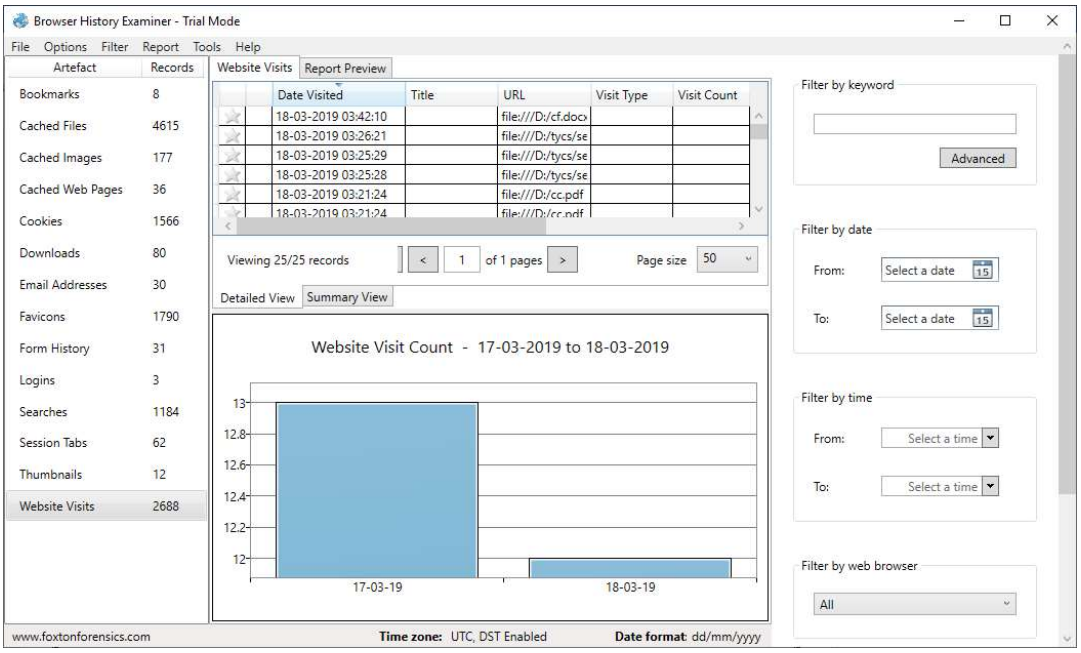
Enter the destination path to capture the data.



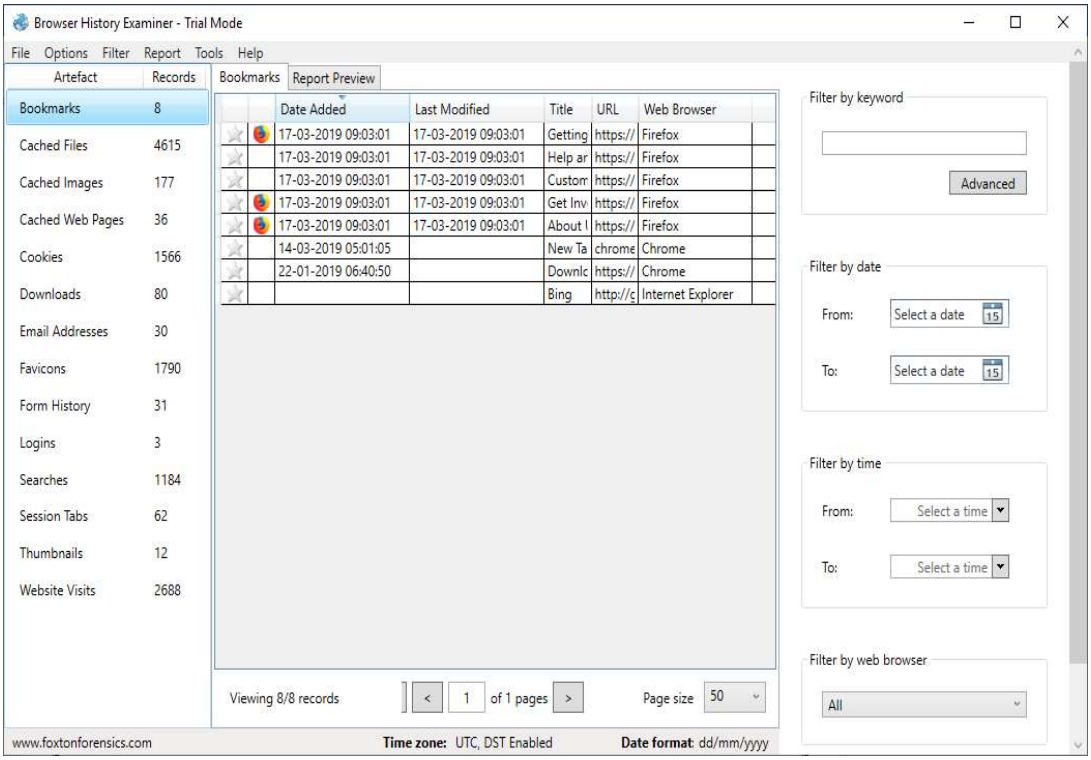
Follow the onscreen directions
The History is been extracting.



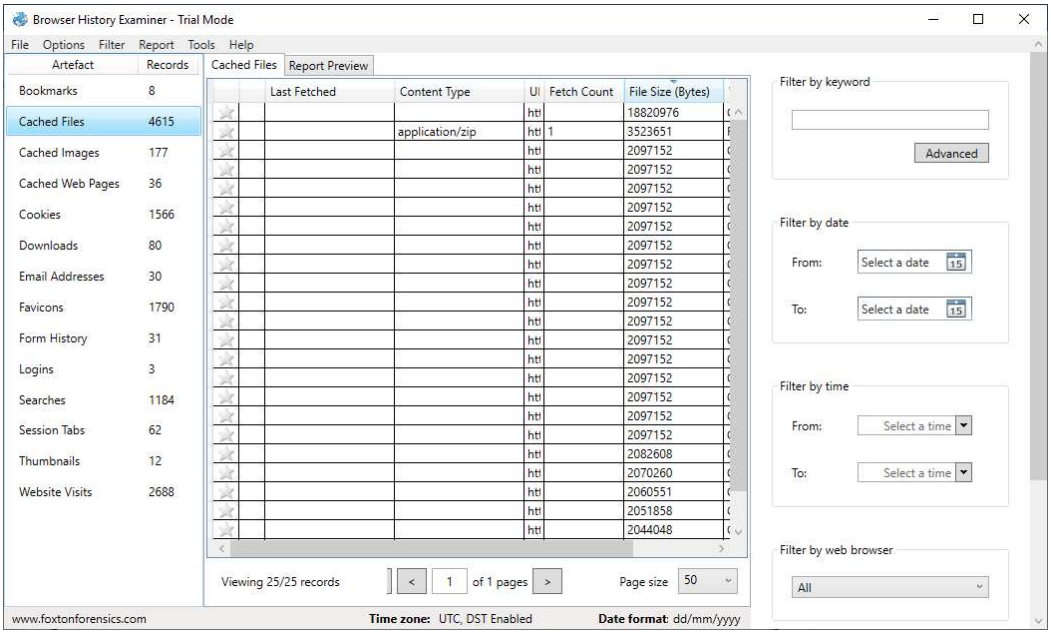
The data has been retrieved.



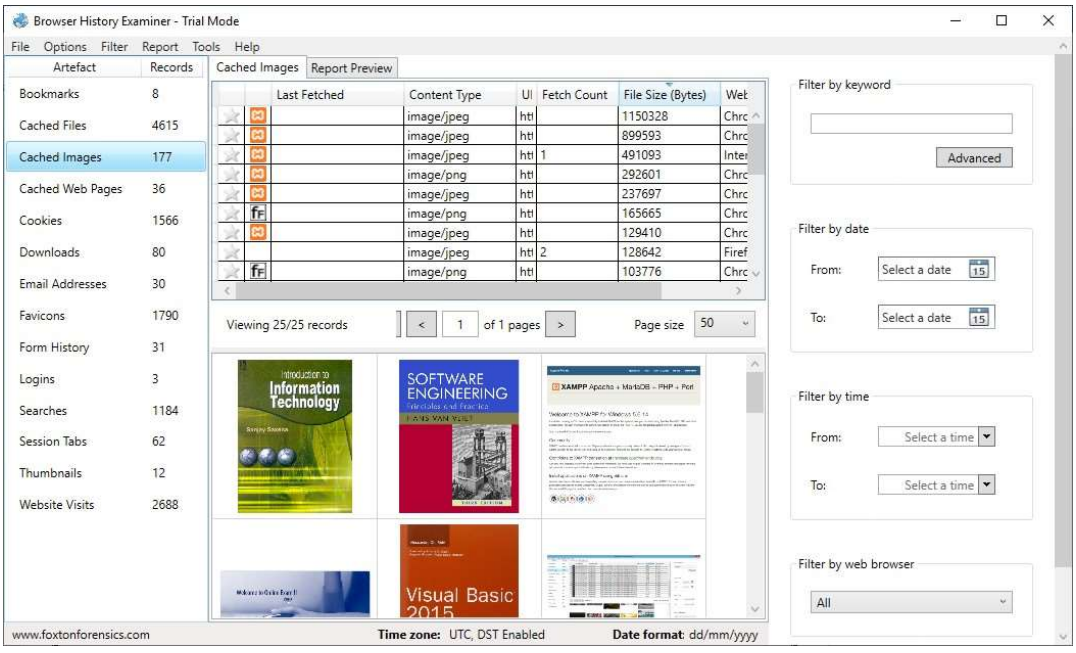
On the left panel click on bookmarks.



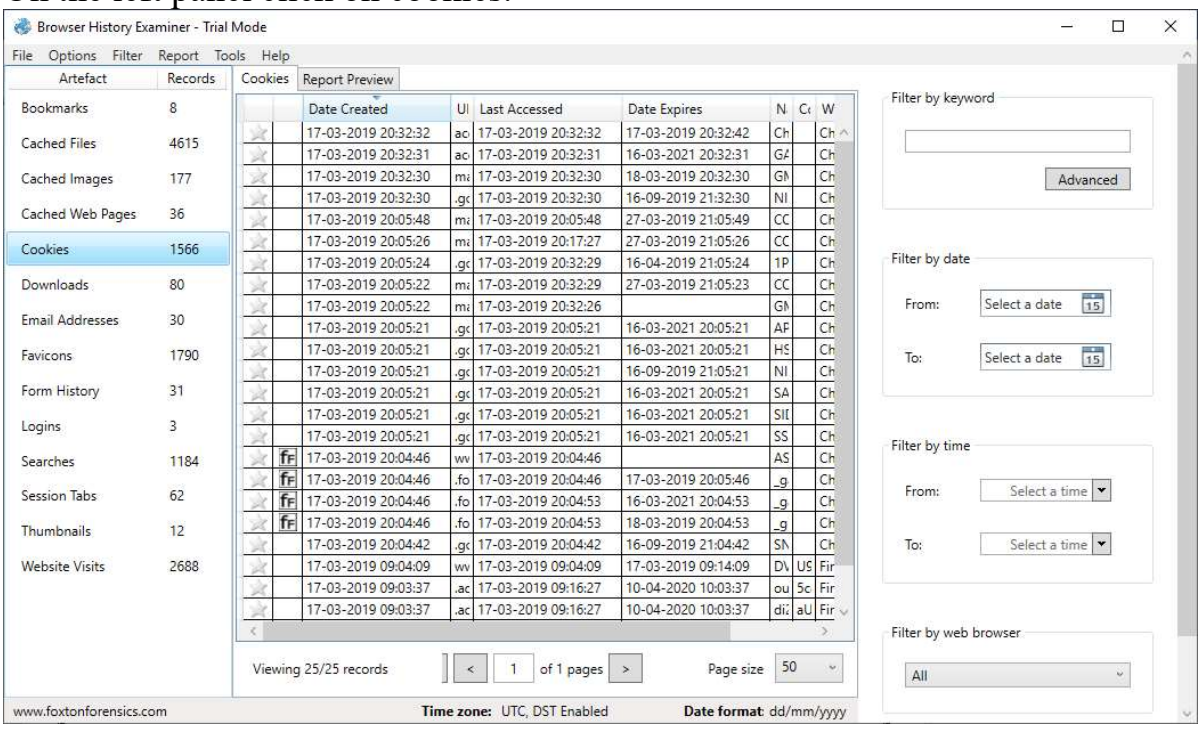
On the left panel click on cached files.



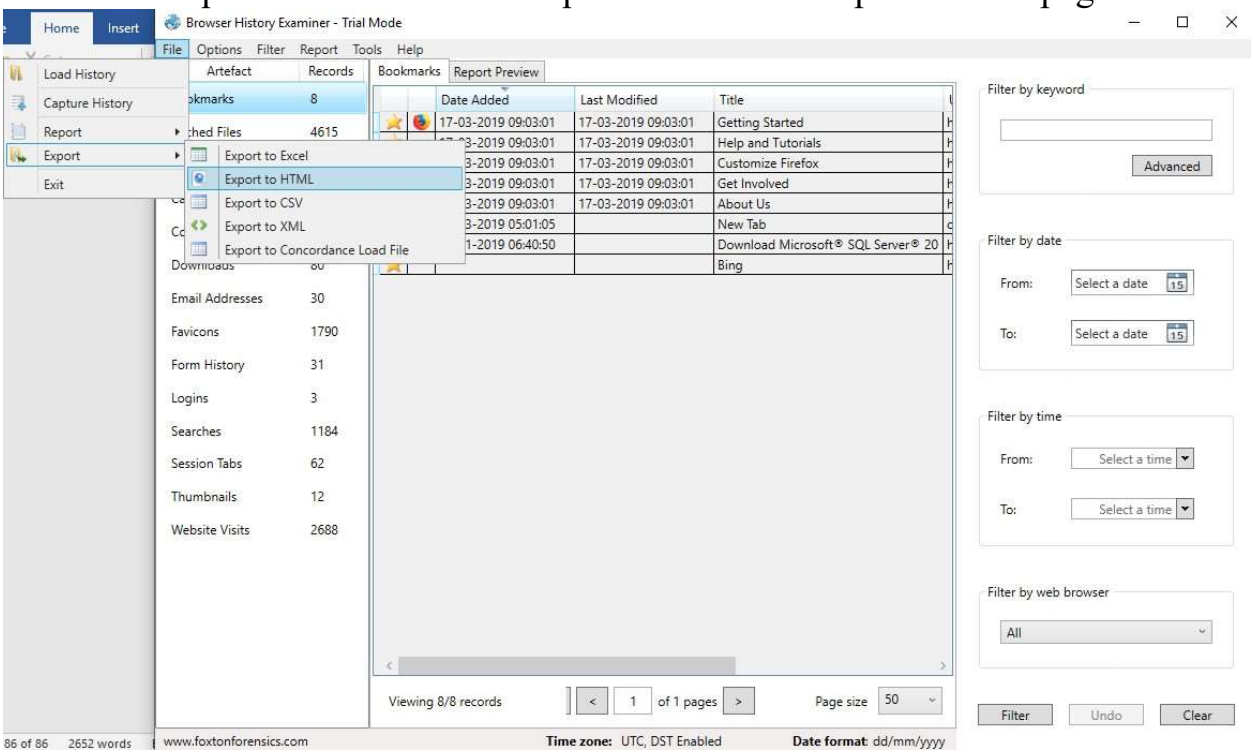
On the left panel click on cached images.



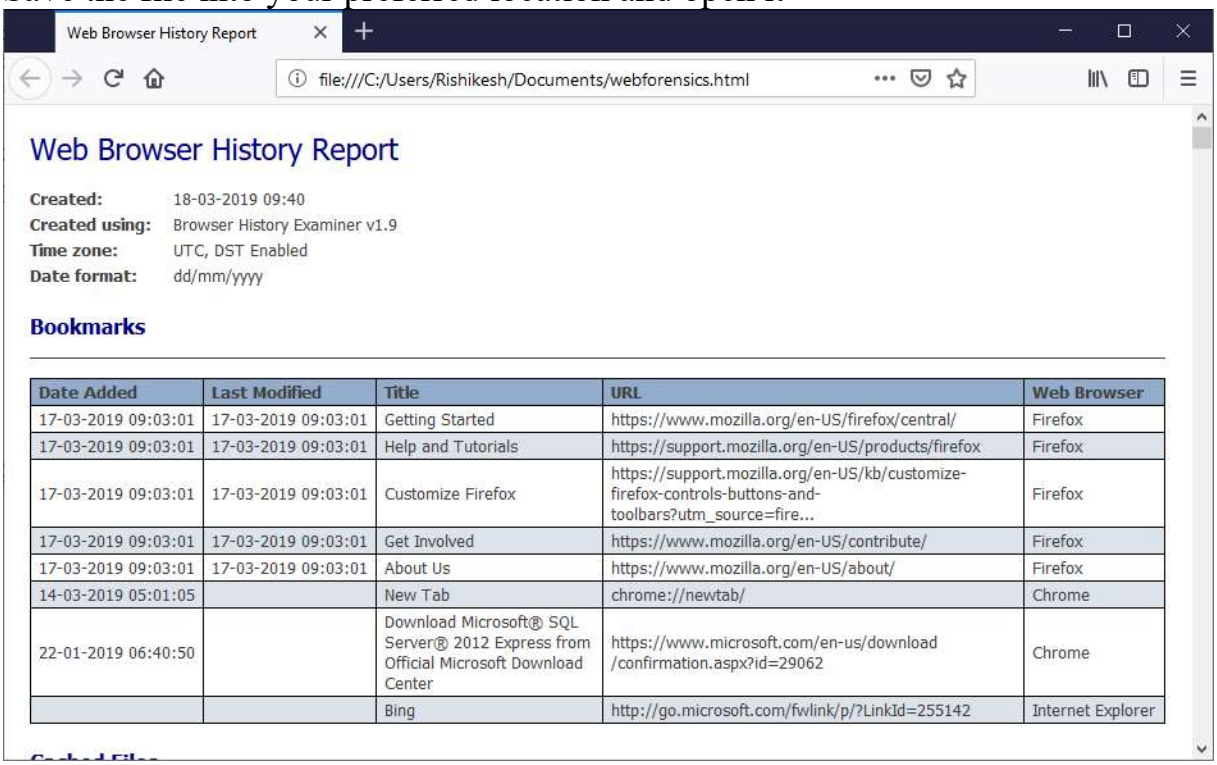
On the left panel click on cookies.



To Create Reports. Click on file > Export and save the report as html page.



Save the file into your preferred location and open it



Web Browser History Report

Created: 18-03-2019 09:40
Created using: Browser History Examiner v1.9
Time zone: UTC, DST Enabled
Date format: dd/mm/yyyy

Bookmarks

Date Added	Last Modified	Title	URL	Web Browser
17-03-2019 09:03:01	17-03-2019 09:03:01	Getting Started	https://www.mozilla.org/en-US/firefox/central/	Firefox
17-03-2019 09:03:01	17-03-2019 09:03:01	Help and Tutorials	https://support.mozilla.org/en-US/products/firefox	Firefox
17-03-2019 09:03:01	17-03-2019 09:03:01	Customize Firefox	https://support.mozilla.org/en-US/kb/customize-firefox-controls-buttons-and-toolbars?utm_source=fire...	Firefox
17-03-2019 09:03:01	17-03-2019 09:03:01	Get Involved	https://www.mozilla.org/en-US/contribute/	Firefox
17-03-2019 09:03:01	17-03-2019 09:03:01	About Us	https://www.mozilla.org/en-US/about/	Firefox
14-03-2019 05:01:05		New Tab	chrome://newtab/	Chrome
22-01-2019 06:40:50		Download Microsoft® SQL Server® 2012 Express from Official Microsoft Download Center	https://www.microsoft.com/en-us/download/confirmation.aspx?id=29062	Chrome
		Bing	http://go.microsoft.com/fwlink/p/?LinkId=255142	Internet Explorer