SHRI G.P.M. DEGREE COLLEGE OF SCIENCE & COMMERCE

SHRI G.P.M. DEGREE COLLEGE OF SCIENCE & COMMERCE.

(COMMITED TO EXCELLENCE IN EDUCATION)

CERTIFICATE

This is to certify that Mr/Ms._____

a student of TY.**BSC-CS** Roll no: _____ has completed the required number of practicals in the subject of _____

as prescribed by the UNIVERSITY OF MUMBAI under my supervision during the academic year 2024-2025.

…….. ……

Prof. Incharge Principal

…… ……

External Examiner Course Co-ordinator

Professor Name: Ms. Akansha Mishra	Class : TY.BSC-CS Semester : Sem V (2024-2025)
Course code : USCSP5041	Subject: Cyber Forensics

Index

		Monitor Cache Memory		
6		Recovering and Inspecting deleted files • Check for Deleted Files • Recover the Deleted Files • Analyzing and Inspecting the recovered files Perform this using recovery option in ENCASE and also Perform manually through command line	53-64	
7		Steganography Detection • Detect hidden information or files within digital images using steganography analysis tools. Extract and examine the hidden content.	65-72	
8		Mobile Device Forensics • Perform a forensic analysis of a mobile device, such as a smartphone or tablet. Retrieve call logs, text messages, and other relevant data for investigative purposes.	73-87	
9		Email Forensics • Analyze email headers and content to trace the origin of suspicious emails. • Identify potential email forgeries or tampering.	89-101	
10		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.	102-110	

PRACTICAL NO. 1

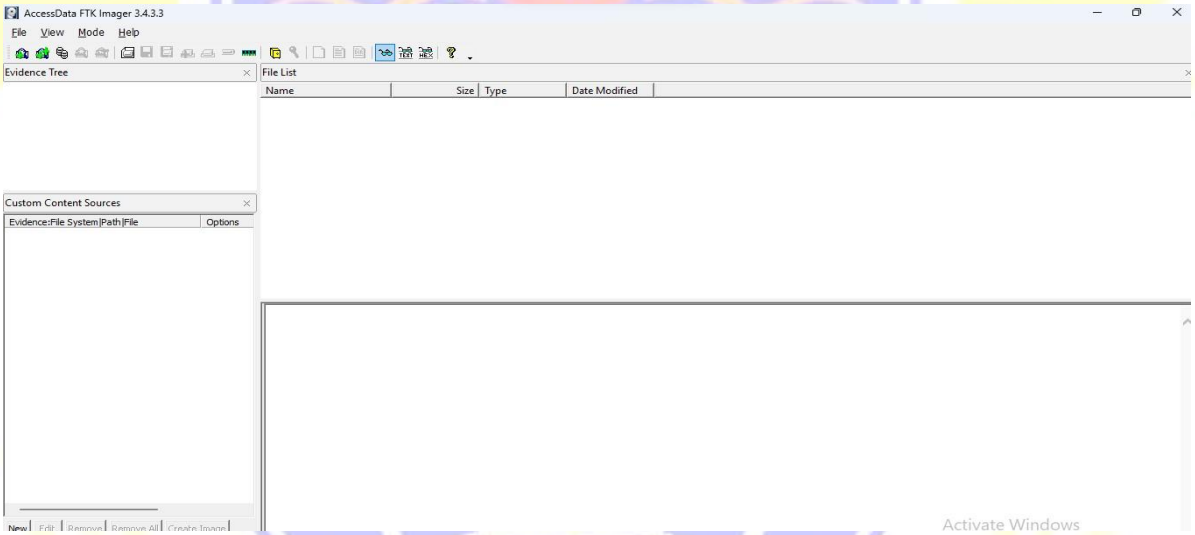
Aim:

Creating a Forensic Image using FTK Imager/Encase Imager:

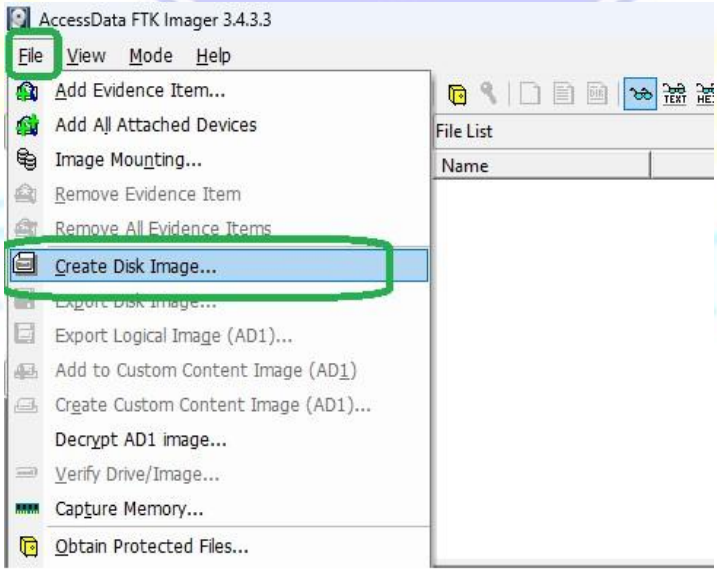
- Creating Forensic Image
- Check Integrity of Data
- Analyze Forensic Image

Practical:

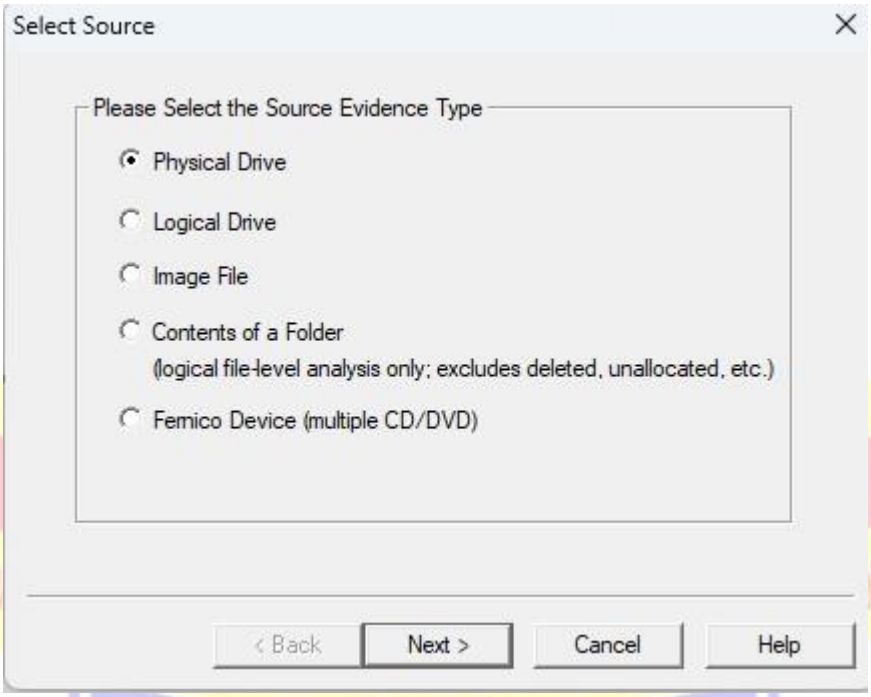
In this Practical we are going to use the FTK Imager to create Images of the evidences



Go to File → Create Disk Image

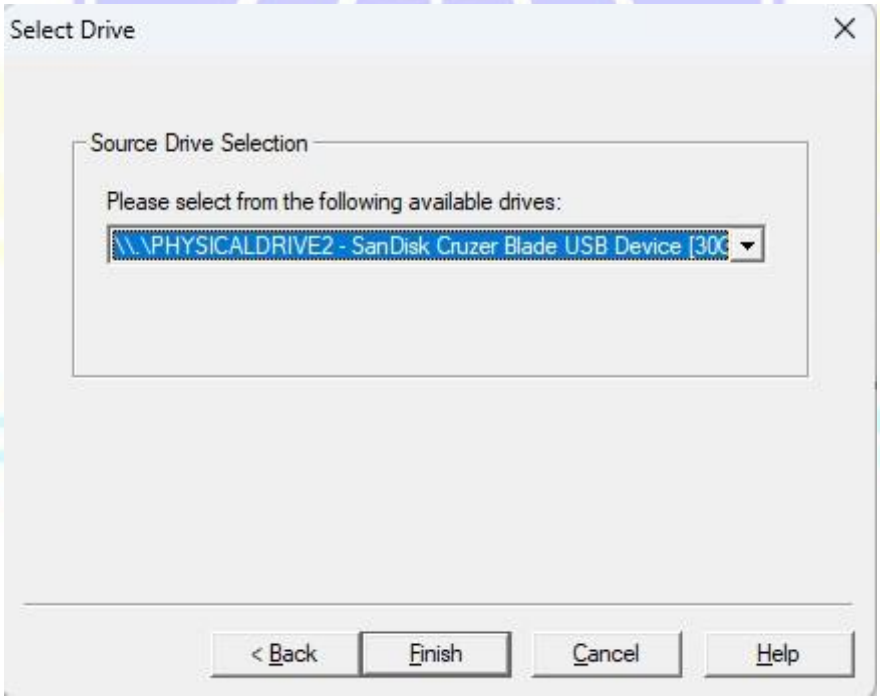


Select the source evidence type

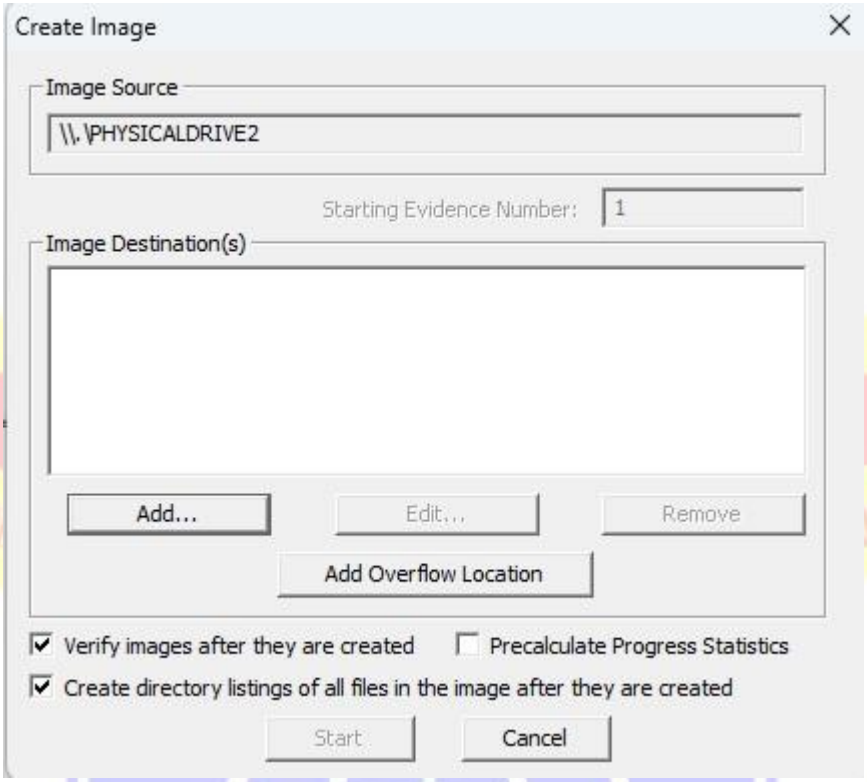


Here we are going to select the physical drive and proceed

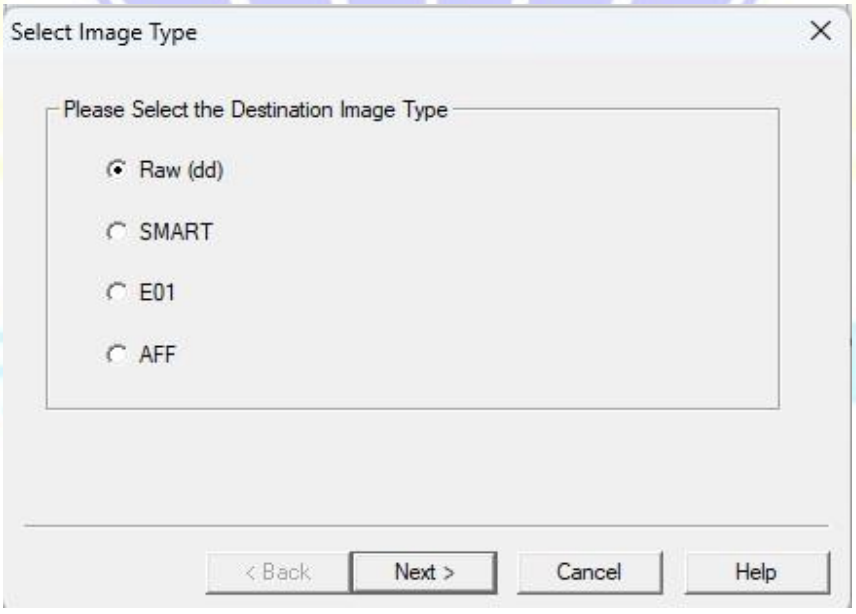
Then we browse the location of the **Pen drive** and click Finish



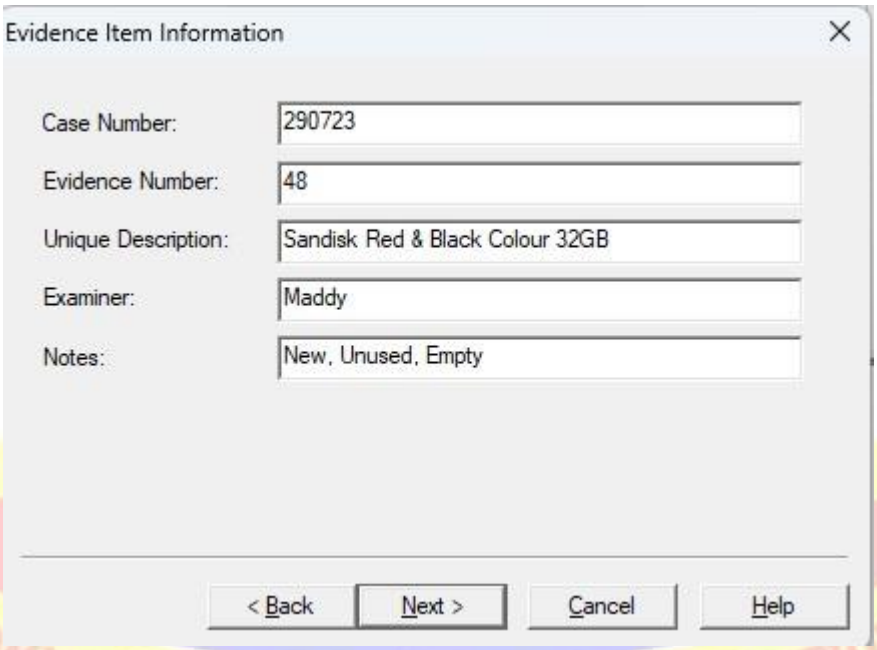
Now we add the location to create images



In this we are going to select the **raw (dd)** format

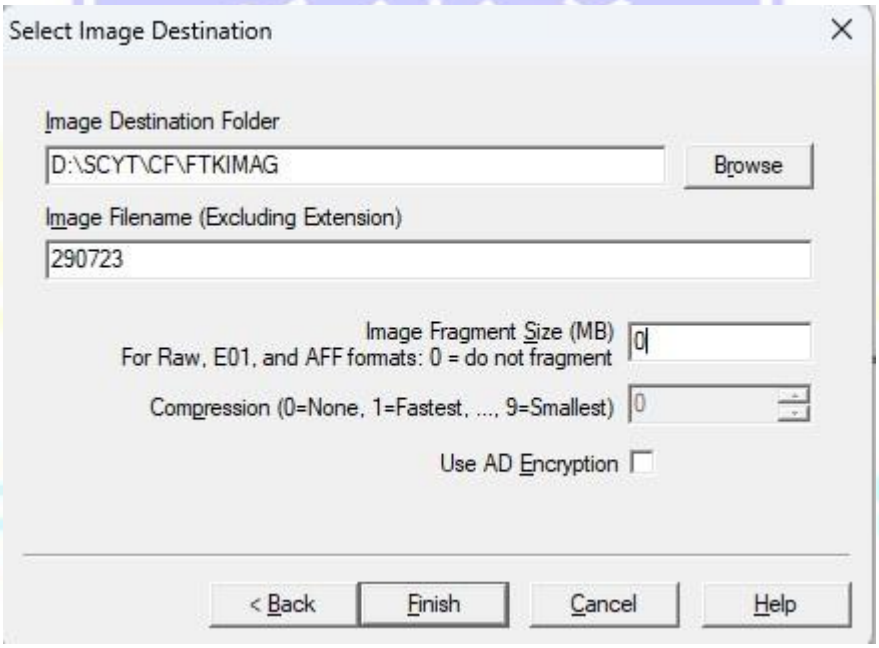


And now we fill the details required for the case

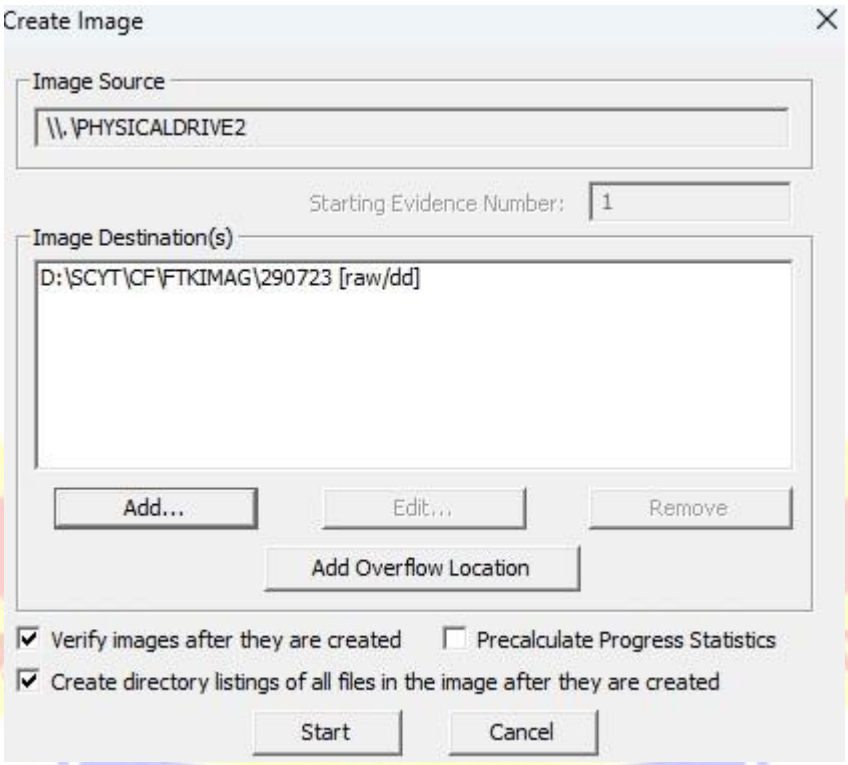


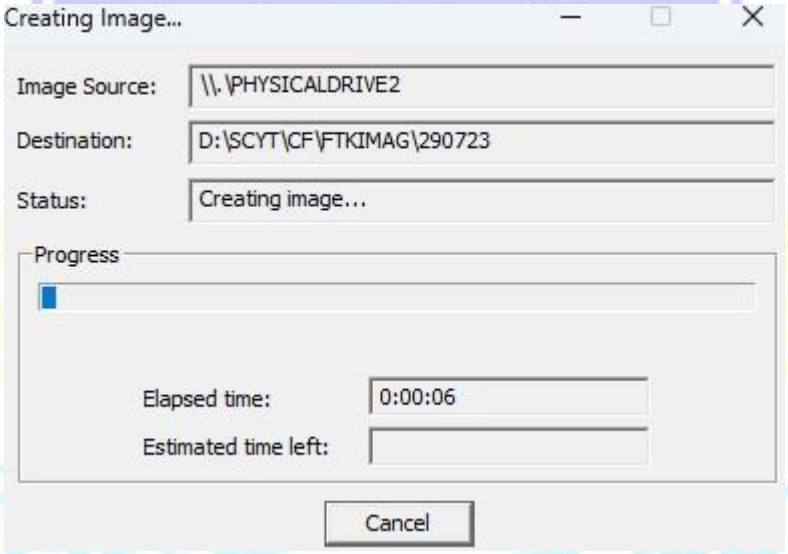
Create a folder to save the images to store in the system disk as the pen drive size cannot be stored in the same drive

Then paste that location to save the images and click Finish

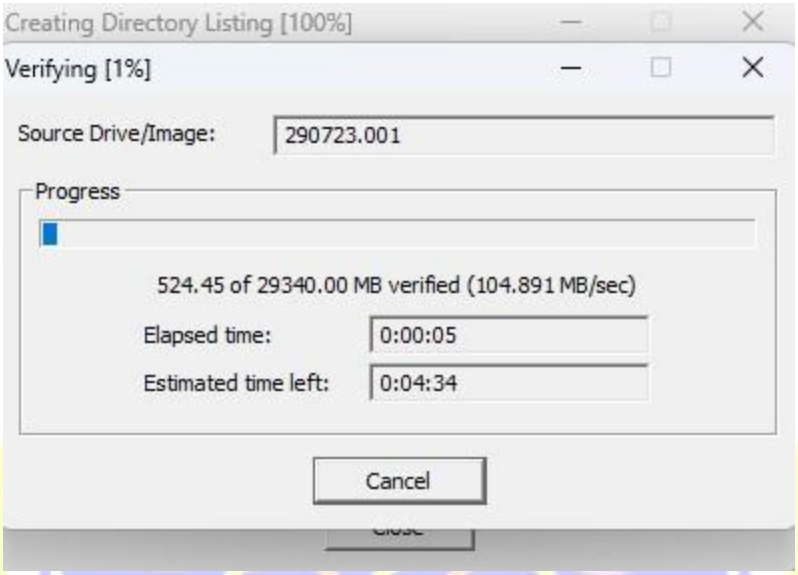


Then Click on Start and wait until the imaging is done

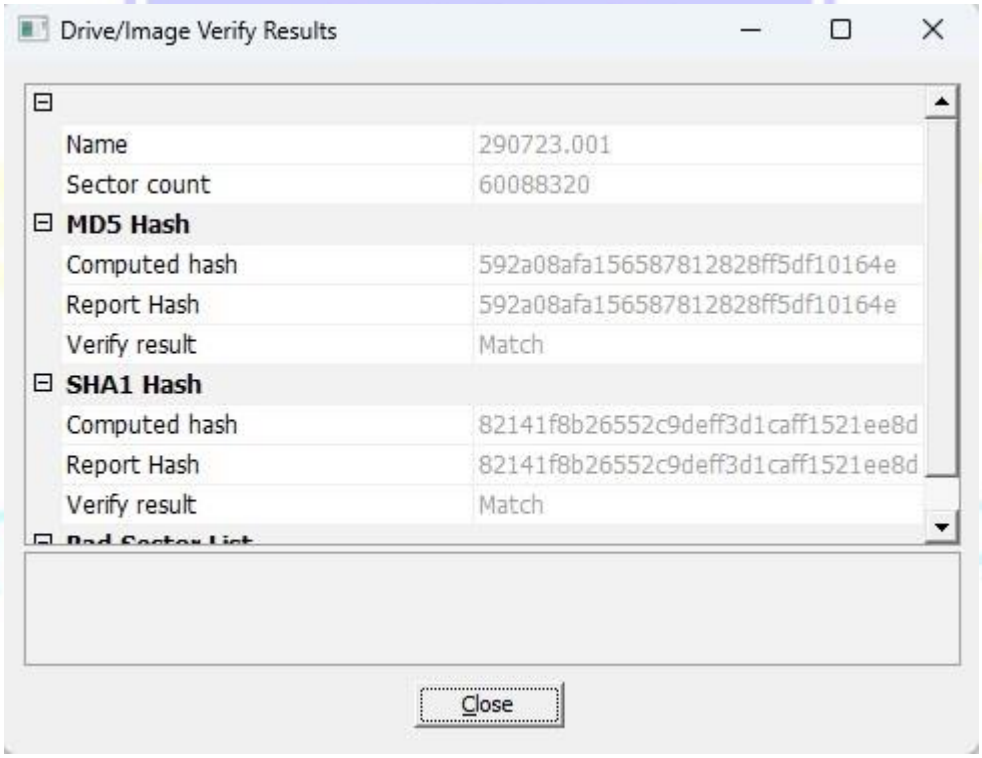




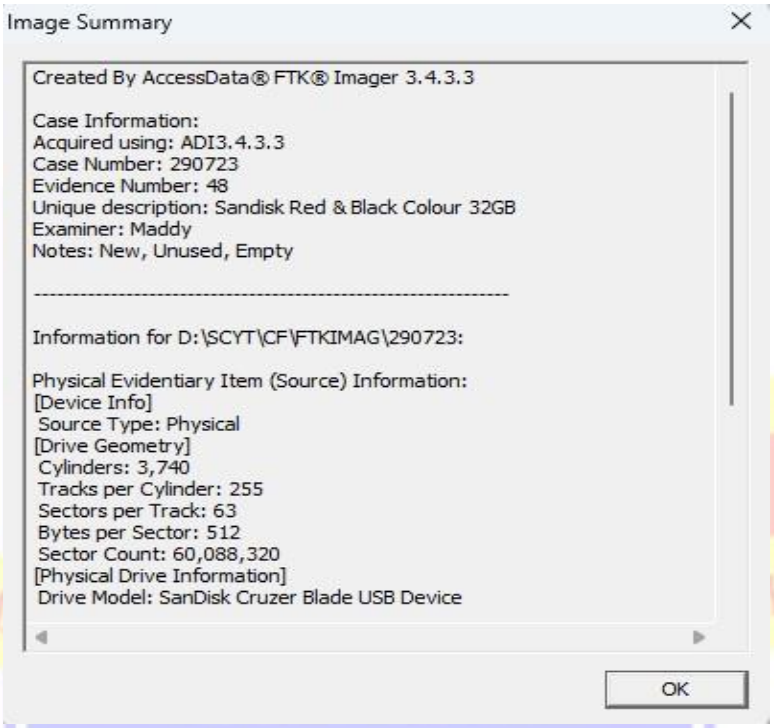
Now it will verify



This is the Hash Value CheckSum given if it matches the original values then the evidence is original if not the evidence is been misplaced

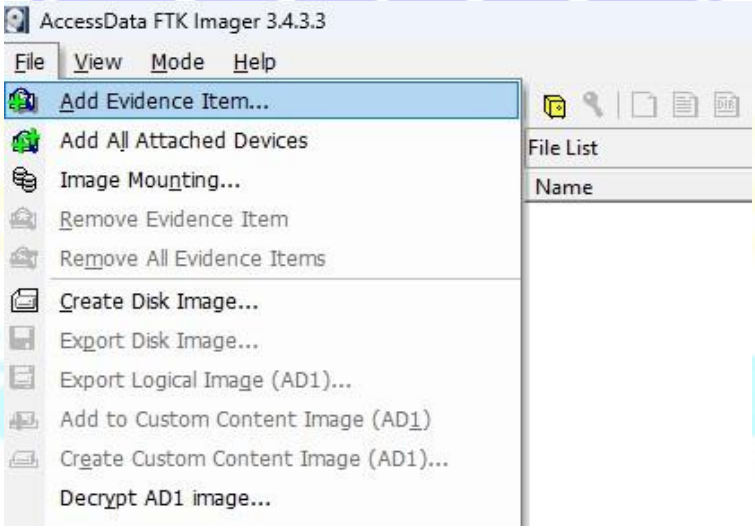


We take the image summary

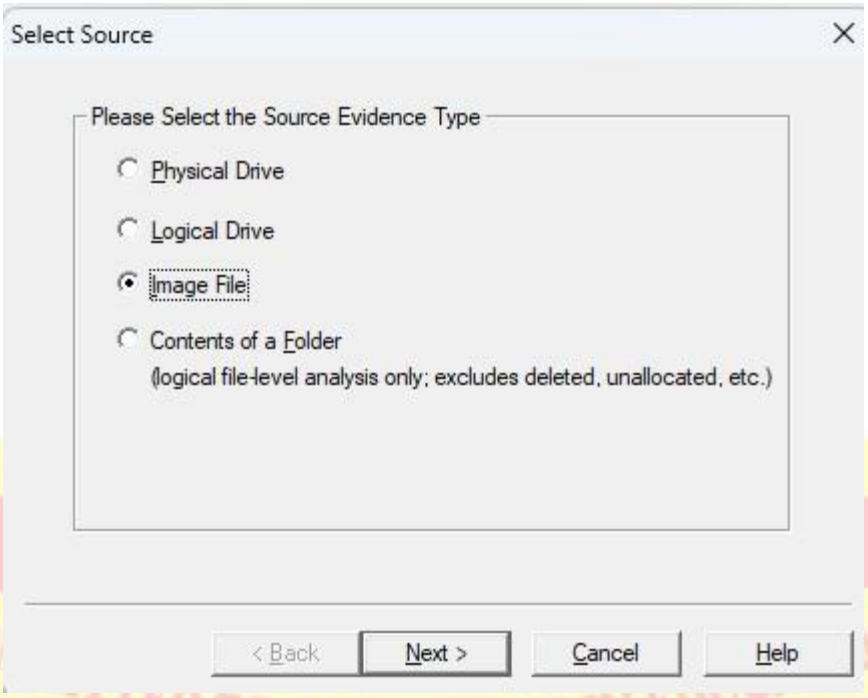


Now we are going to view the images in the FTK Imager

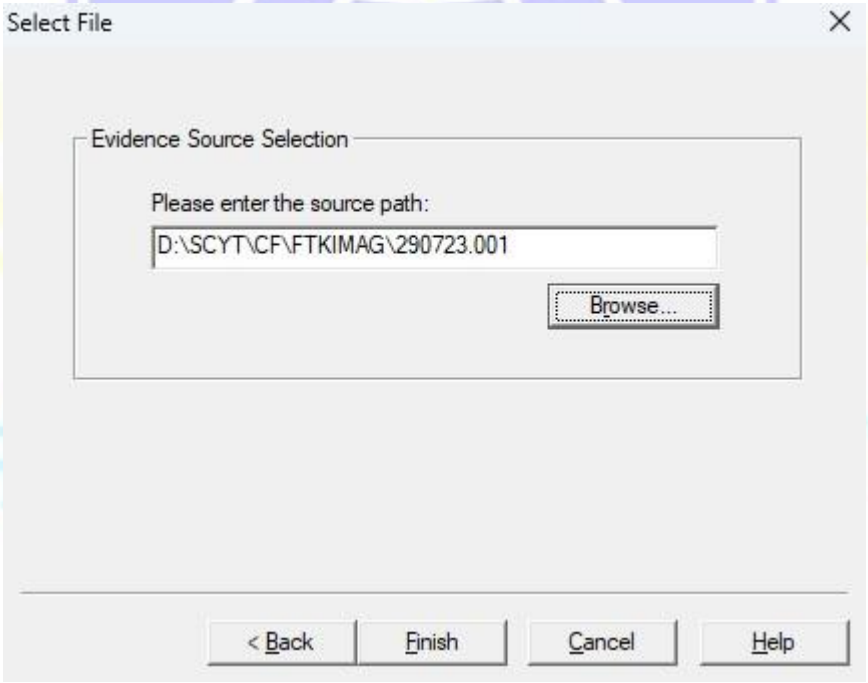
Go to File → Add Evidence Item



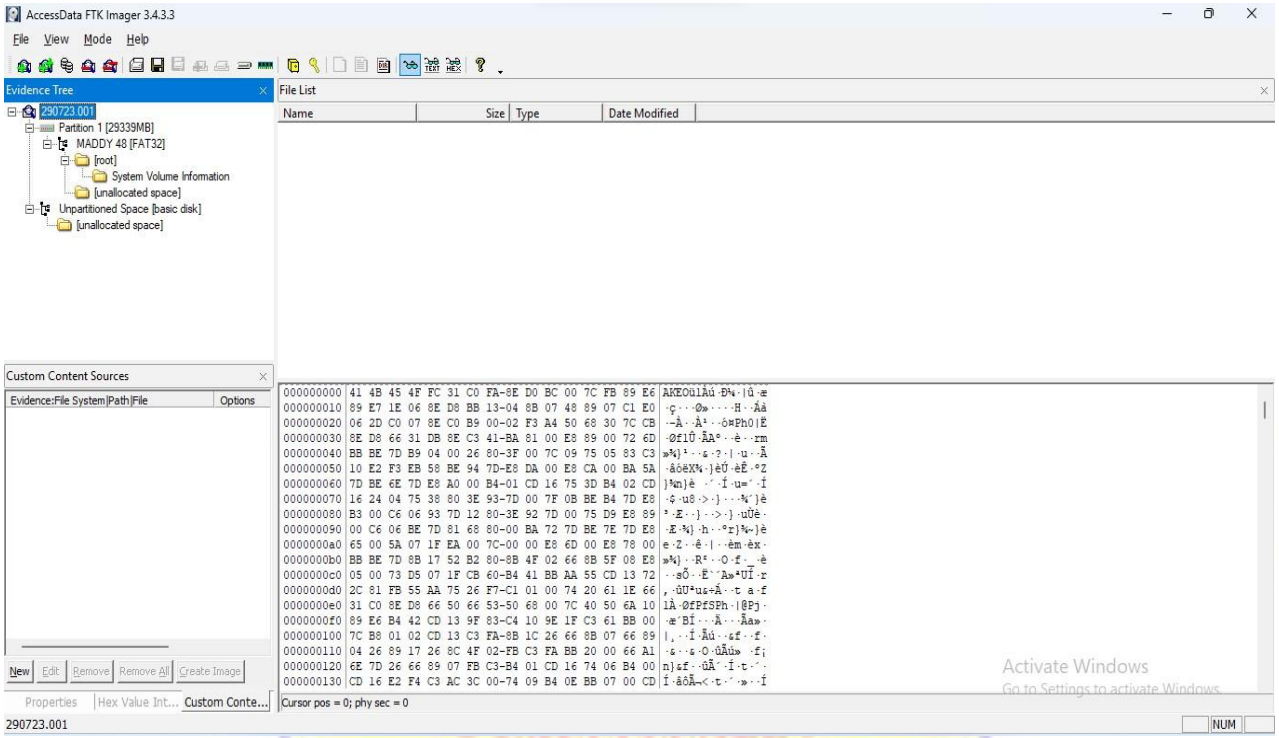
Then select the type of the evidence here it is Image File



Give the directory of the images created using the FTK Imager and click Finish



Here we can see the data shown by the FTK Imager


AccessData FTK Imager 3.4.3.3
File View Mode Help
Evidence Tree
290723.001
Partition 1 [29339MB]
MADDY 48 [FAT32]
[root]
System Volume Information
[unallocated space]
Unpartitioned Space [basic disk]
[unallocated space]
File List
Name
Size
Type
Date Modified
Custom Content Sources
Evidence:File System|Path|File
Options
New
Edit
Remove
Remove All
Create Image
Properties
Hex Value Int...
Custom Conte...
Cursor pos = 0; phy sec = 0
290723.001
NUM
Activate Windows
Go to Settings to activate Windows.

Result:

Creating a forensic image ensures that the data is preserved without any alterations, which is crucial for maintaining evidence integrity in a forensic investigation.

Learning Outcomes:

- Understand how to create a forensic image using FTK Imager/Encase Imager.
- Learn to verify the integrity of data to ensure no tampering.
- Develop skills to analyze forensic images and extract useful evidence.

Course Outcomes:

- Gain practical knowledge of forensic image creation and data preservation.
- Ability to perform data integrity checks and confirm the authenticity of evidence.
- Apply analytical techniques to examine forensic images for investigative purposes.

Conclusion:

Viva Questions:

1. What is a forensic image, and why is it important?
2. How does FTK Imager verify the integrity of data?
3. Can you explain the difference between creating an image and analyzing it?
4. What role does data integrity play in a forensic investigation?

PRACTICAL NO: 2

Aim:

Data Acquisition:

- Perform data acquisition using:
- USB Write Blocker + Encase Imager
- SATA Write Blocker + Encase Imager
- Falcon Imaging Device

Practical:

USB Writer Blocker + Encase Imager

Hardware and Paid Software's:

https://www.getfastforensics.com/write-blockers

https://www.amazon.com/usb-write-blocker/s?k=usb+write+blocker&language=en_US&currency=INR

http://www.orionforensics.com/forensics-tools/orion-usb-write-blocker/

For Open-Source Software:

https://sourceforge.net/projects/usbwriteblockerforwindows8/

Encase Imager:

Encase is a forensic suite produced by Guidance Software (now part of OpenText) that is popular with commercial providers. A standard license comes in at around $3500 around ₹289242

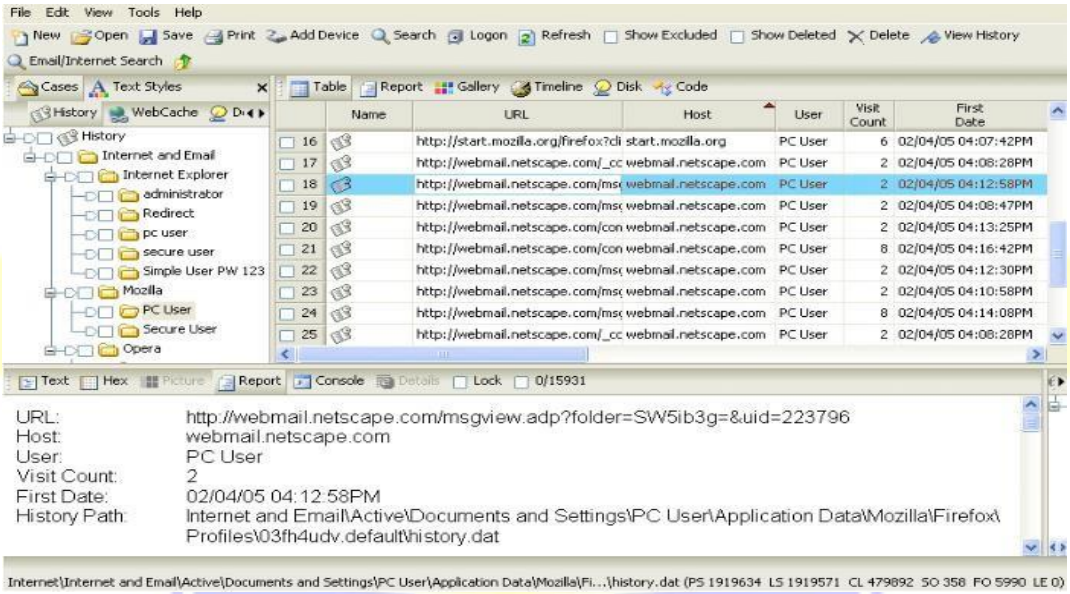
Overview PDF for the Encase Imager:

https://www.opentext.com/assets/documents/en-US/pdf/opentext-po-encaseforensic-en.pdf

https://www.forensicstore.com/product/encase-forensic-v8-06/

YouTube link to see the working of the Encase Imager:

https://www.youtube.com/watch?v=obmRoD3ChSc



Here is an Overview of the Encase Imager:

https://www.hackingarticles.in/forensic-imaging-encase/

SATA Write Blocker + Encase Imager

Overview of Write Blockers

https://linuxhint.com/best_hardware_write_blockers/

https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt/cftttechnical/hardware

Setup of the Write Blocker

https://www.youtube.com/watch?v=Kmm8iaa76rQ

Falcon Imaging Device

About Info of the Falcon Imaging Device

https://www.logicube.com/shop/forensic-falcon-neo/

http://www.edasfox.com/product/forensic-falcon-neo/

https://www.secureindia.in/?page_id=1068

Prices of the Falcon Imaging Device

https://www.indiamart.com/proddetail/forensic-falcon-2850471543448.html

Documentation and Videos for Demonstration of the Working of the Flacon Imaging Device

https://www.forensicfocus.com/articles/how-to-create-a-logical-image-on-falcon-neo/

https://www.forensicfocus.com/articles/how-to-image-to-a-network-repository-with-logicubes-forensicfalcon-neo/

https://www.forensicfocus.com/articles/how-to-use-the-file-browser-feature-in-logicubes-forensic-falconneo/

https://www.youtube.com/watch?v=YSLSi1QpjUs https://www.youtube.com/watch?v=rZLndjf1hPs

Result:

Data acquisition using different write blockers (USB, SATA) and imaging devices like Falcon ensures that evidence is captured without any modification to the original media, maintaining its integrity for forensic analysis.

Learning Outcomes:

- Understand how to perform data acquisition using write blockers and imaging tools.
- Learn the use of USB and SATA write blockers to prevent data alteration.
- Develop skills to use Falcon Imaging Device for secure data acquisition.

Course Outcomes:

- Gain practical knowledge of data acquisition techniques using various write blockers.
- Ability to prevent data tampering while capturing forensic evidence.
- Apply different methods for acquiring forensic images safely and securely.

Conclusion:

Viva Questions:

1. What is the purpose of a write blocker in digital forensics?
2. How does using a USB write blocker differ from using a SATA write blocker?
3. What is the Falcon Imaging Device, and when is it used?
4. Why is it important to maintain data integrity during acquisition?

PRACTICAL NO: 3

Aim:

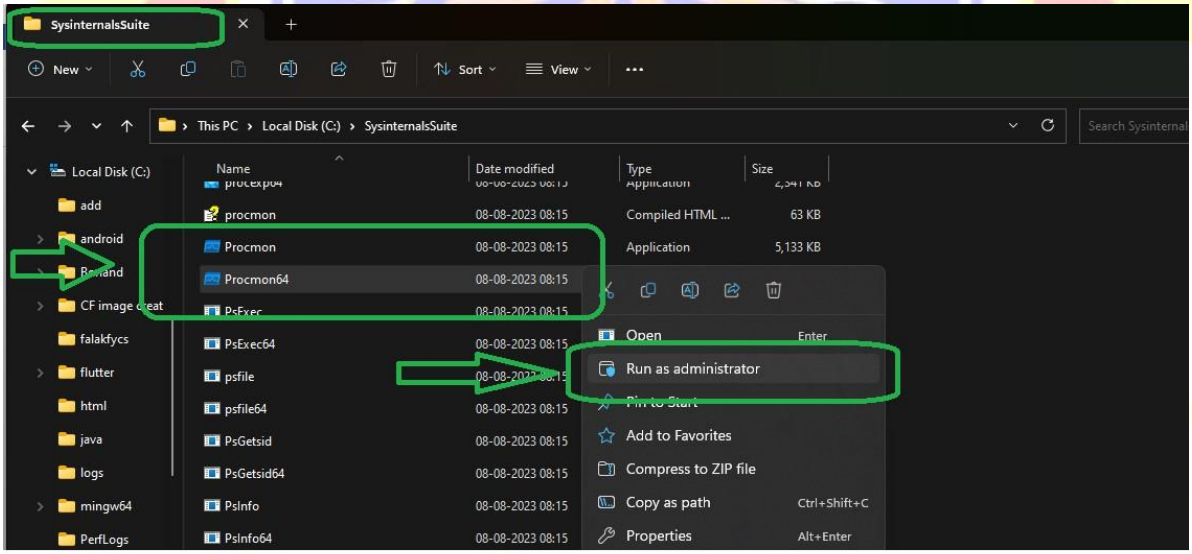
Analyze the memory dump of a running computer system.

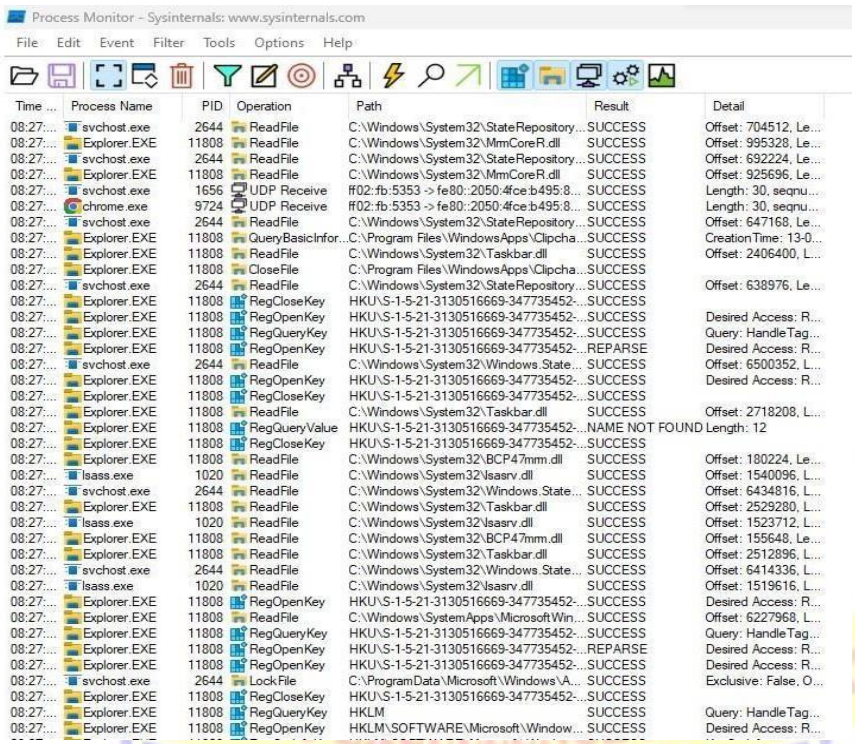
- Extract volatile data, such as open processes, network connections, and registry information.

Practical:

Open Process

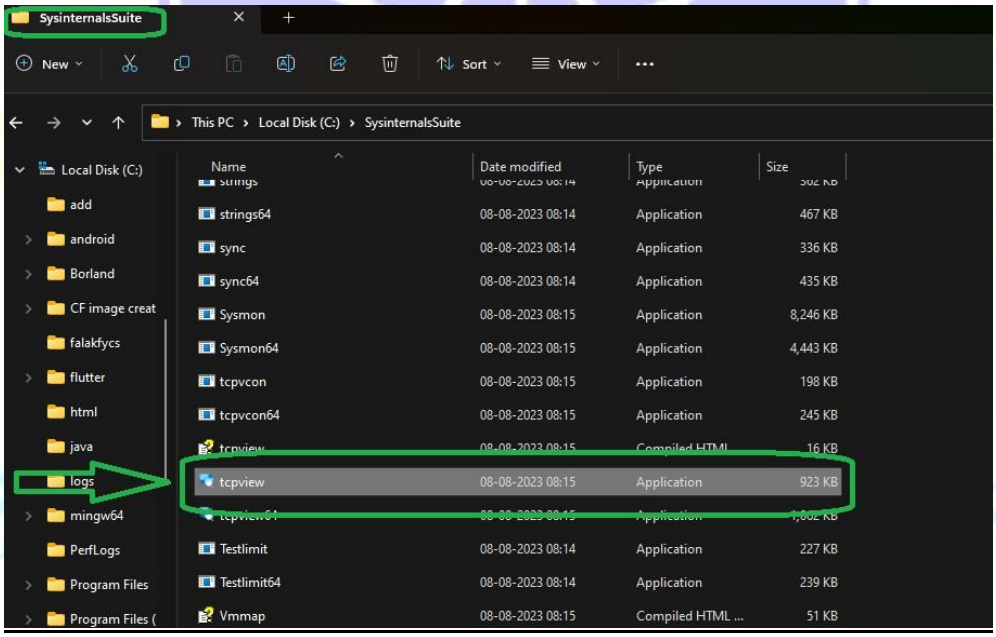
Go to Sysinternal Suite → **ProcMon** →Right Click on it and **Open As Administrator**

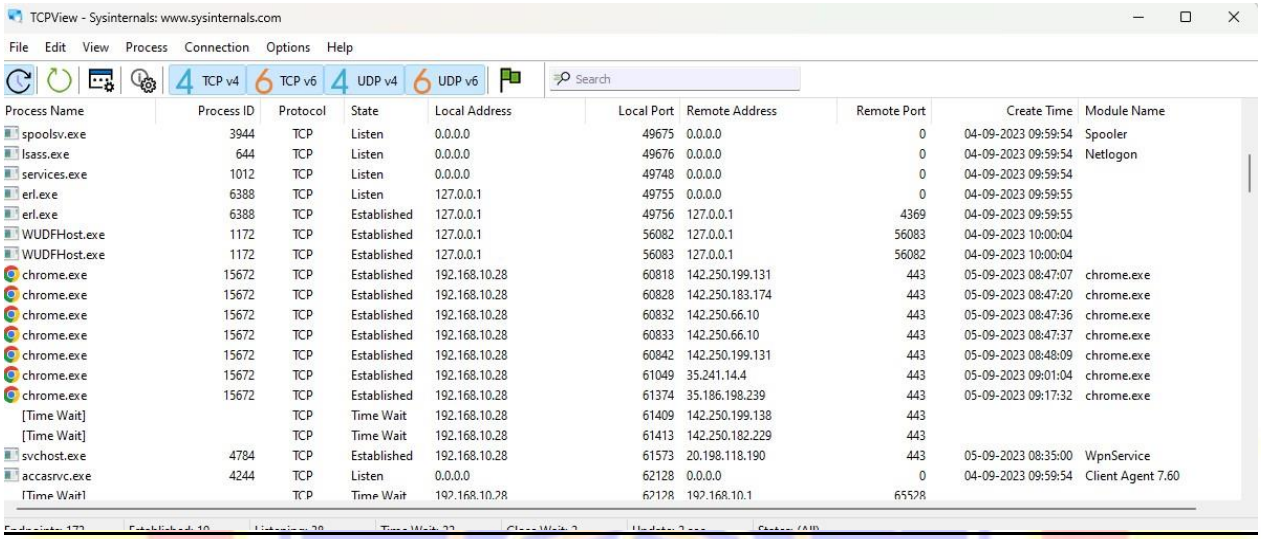




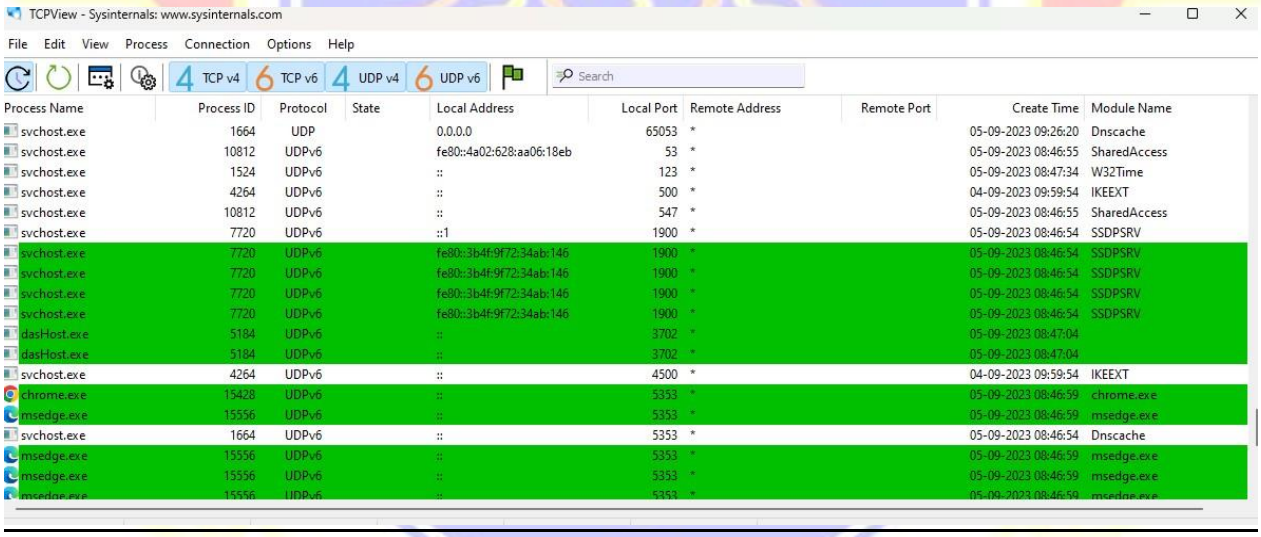
Network Connections

Go to SysinternalSuite→ TCPview





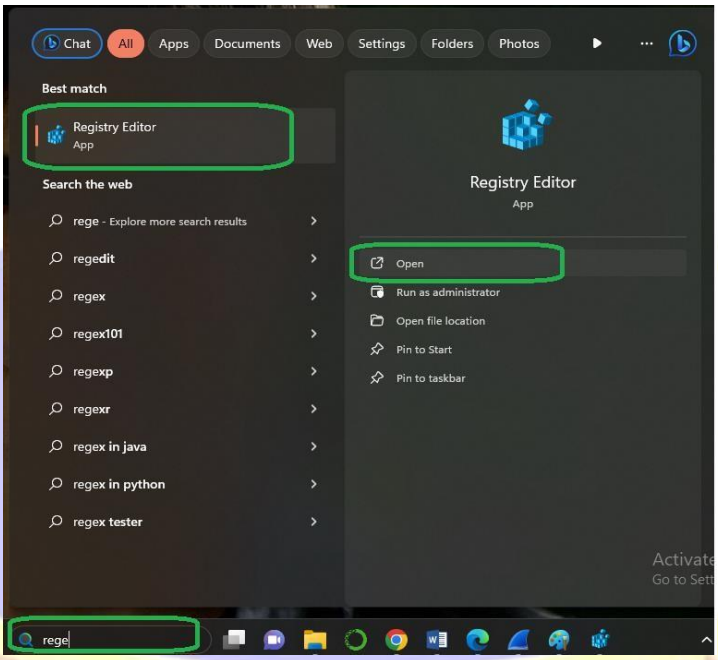
Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Time	Module Name
spoolsv.exe	3944	TCP	Listen	0.0.0.0	49675	0.0.0.0	0	04-09-2023 09:59:54	Spooler
lsass.exe	644	TCP	Listen	0.0.0.0	49676	0.0.0.0	0	04-09-2023 09:59:54	Netlogon
services.exe	1012	TCP	Listen	0.0.0.0	49748	0.0.0.0	0	04-09-2023 09:59:54	
erl.exe	6388	TCP	Listen	127.0.0.1	49755	0.0.0.0	0	04-09-2023 09:59:55	
erl.exe	6388	TCP	Established	127.0.0.1	49756	127.0.0.1	4369	04-09-2023 09:59:55	
WUDFHost.exe	1172	TCP	Established	127.0.0.1	56082	127.0.0.1	56083	04-09-2023 10:00:04	
WUDFHost.exe	1172	TCP	Established	127.0.0.1	56083	127.0.0.1	56082	04-09-2023 10:00:04	
chrome.exe	15672	TCP	Established	192.168.10.28	60818	142.250.199.131	443	05-09-2023 08:47:07	chrome.exe
chrome.exe	15672	TCP	Established	192.168.10.28	60828	142.250.183.174	443	05-09-2023 08:47:20	chrome.exe
chrome.exe	15672	TCP	Established	192.168.10.28	60832	142.250.66.10	443	05-09-2023 08:47:36	chrome.exe
chrome.exe	15672	TCP	Established	192.168.10.28	60833	142.250.66.10	443	05-09-2023 08:47:37	chrome.exe
chrome.exe	15672	TCP	Established	192.168.10.28	60842	142.250.199.131	443	05-09-2023 08:48:09	chrome.exe
chrome.exe	15672	TCP	Established	192.168.10.28	61049	35.241.14.4	443	05-09-2023 09:01:04	chrome.exe
chrome.exe	15672	TCP	Established	192.168.10.28	61374	35.186.198.239	443	05-09-2023 09:17:32	chrome.exe
[Time Wait]		TCP	Time Wait	192.168.10.28	61409	142.250.199.138	443		
[Time Wait]		TCP	Time Wait	192.168.10.28	61413	142.250.182.229	443		
svchost.exe	4784	TCP	Established	192.168.10.28	61573	20.198.118.190	443	05-09-2023 08:35:00	WpnService
accasrvc.exe	4244	TCP	Listen	0.0.0.0	62128	0.0.0.0	0	04-09-2023 09:59:54	Client Agent 7.60
[Time Wait]		TCP	Time Wait	192.168.10.28	62128	192.168.10.1	65528		



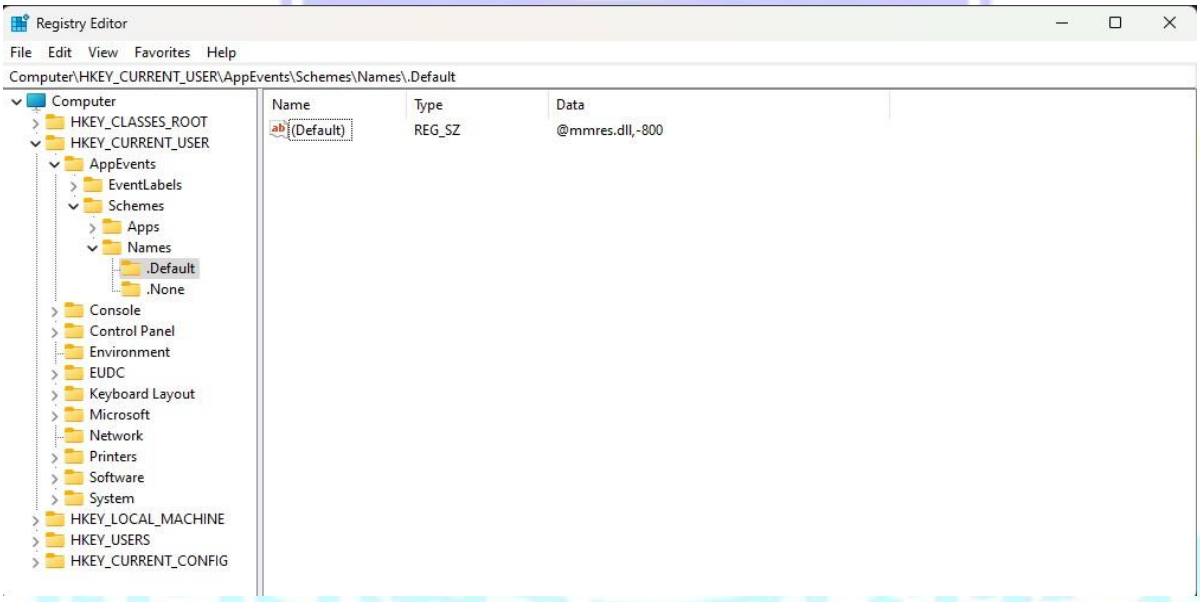
Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Time	Module Name
svchost.exe	1664	UDP		0.0.0.0	65053	*		05-09-2023 09:26:20	Dnscache
svchost.exe	10812	UDPv6		fe80::4a02:628:aa06:18eb	53	*		05-09-2023 08:46:55	SharedAccess
svchost.exe	1524	UDPv6		::	123	*		05-09-2023 08:47:34	W32Time
svchost.exe	4264	UDPv6		::	500	*		04-09-2023 09:59:54	IKEEXT
svchost.exe	10812	UDPv6		::	547	*		05-09-2023 08:46:55	SharedAccess
svchost.exe	7720	UDPv6		::1	1900	*		05-09-2023 08:46:54	SSDPSRV
svchost.exe	7720	UDPv6		fe80::3b4f:9f72:34ab:146	1900	*		05-09-2023 08:46:54	SSDPSRV
svchost.exe	7720	UDPv6		fe80::3b4f:9f72:34ab:146	1900	*		05-09-2023 08:46:54	SSDPSRV
svchost.exe	7720	UDPv6		fe80::3b4f:9f72:34ab:146	1900	*		05-09-2023 08:46:54	SSDPSRV
svchost.exe	7720	UDPv6		fe80::3b4f:9f72:34ab:146	1900	*		05-09-2023 08:46:54	SSDPSRV
dasHost.exe	5184	UDPv6		::	3702	*		05-09-2023 08:47:04	
dasHost.exe	5184	UDPv6		::	3702	*		05-09-2023 08:47:04	
svchost.exe	4264	UDPv6		::	4500	*		04-09-2023 09:59:54	IKEEXT
chrome.exe	15428	UDPv6		::	5353	*		05-09-2023 08:46:59	chrome.exe
msedge.exe	15556	UDPv6		::	5353	*		05-09-2023 08:46:59	msedge.exe
svchost.exe	1664	UDPv6		::	5353	*		05-09-2023 08:46:54	Dnscache
msedge.exe	15556	UDPv6		::	5353	*		05-09-2023 08:46:59	msedge.exe
msedge.exe	15556	UDPv6		::	5353	*		05-09-2023 08:46:59	msedge.exe
msedge.exe	15556	UDPv6		::	5353	*		05-09-2023 08:46:59	msedge.exe

Registry Information

Click on **Search Bar** on the **Taskbar** → Type **Regedit** → Click on **Registry Editor**



View the desired registries to be analyzed



Result:

Analyzing a memory dump helps extract volatile data such as open processes, network connections, and registry information, which is crucial for investigating running systems in real-time.

Learning Outcomes:

- Understand how to analyze a memory dump from a running computer system.
- Learn to extract volatile data like open processes, network connections, and registry details.
- Develop skills to interpret and analyze memory dumps for investigative purposes.

Course Outcomes:

- Gain practical knowledge of memory dump analysis and its significance in forensics.
- Ability to extract and examine volatile data for real-time investigation.
- Apply techniques to analyze critical system information from memory dumps.

Conclusion:

Viva Questions:

1. What is a memory dump, and why is it important in digital forensics?
2. How can volatile data be extracted from a memory dump?
3. What kind of information can be obtained from analyzing a memory dump?
4. Why is analyzing network connections crucial during a forensic investigation?

PRACTICAL NO: 4

Aim:

Capturing and analyzing network packets using WireShark (Fundamentals):

- Identification the live network
- Capture Packets
- Analyze the captured packets

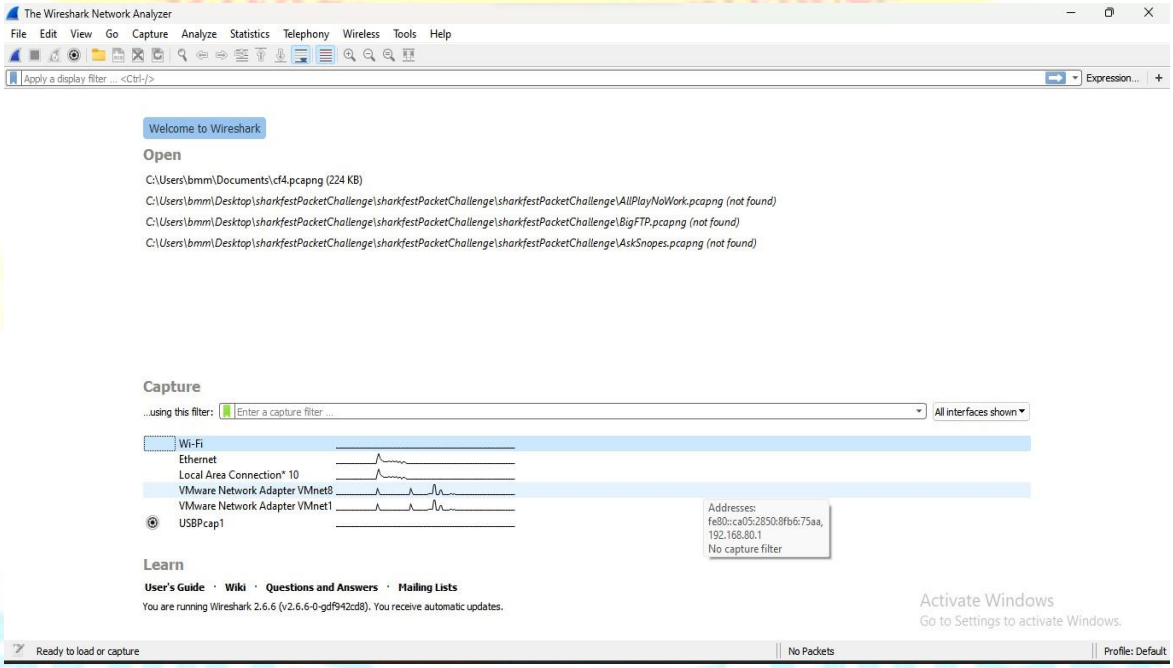
Practical:

In this practical only **identification**, **capturing** and **analysis** is done.

We will also **solve some cases to understand the practical clearly.**

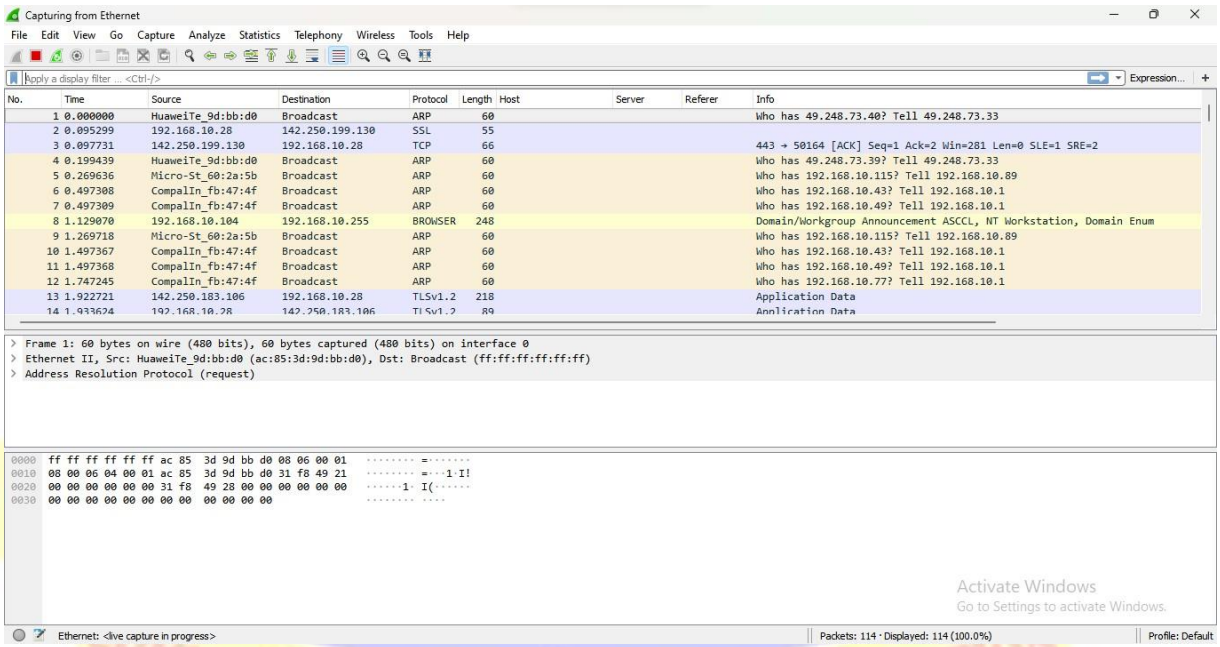
Identifying the Live Networks

We are using **WireShark**, an application used to identify, capture and analyze the network traffics.



Capturing Network

We are now going to capture a network of Ethernet



As soon as you single-click on your network interface's name, you can see how the packets are working in real time. WireShark will capture all the packets going in and out of our systems.

Analyze the Captured Packets

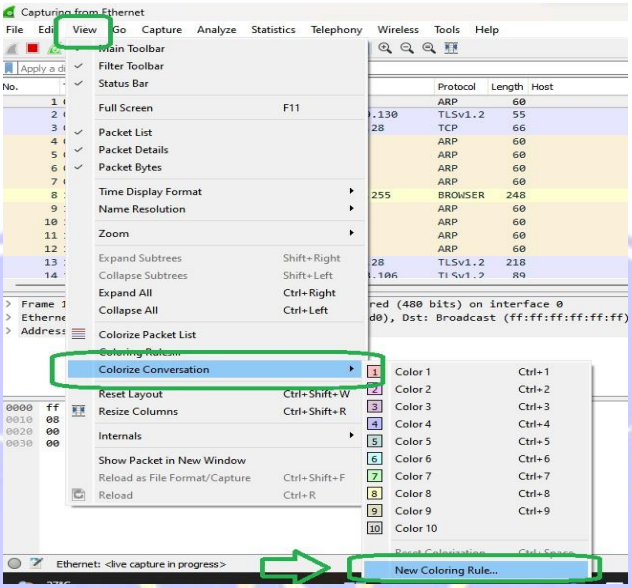
Color Coding Different packets are seen highlighted in various different colors. This is WireShark's way of displaying traffic to help you easily identify the types of it.

Default colors are:

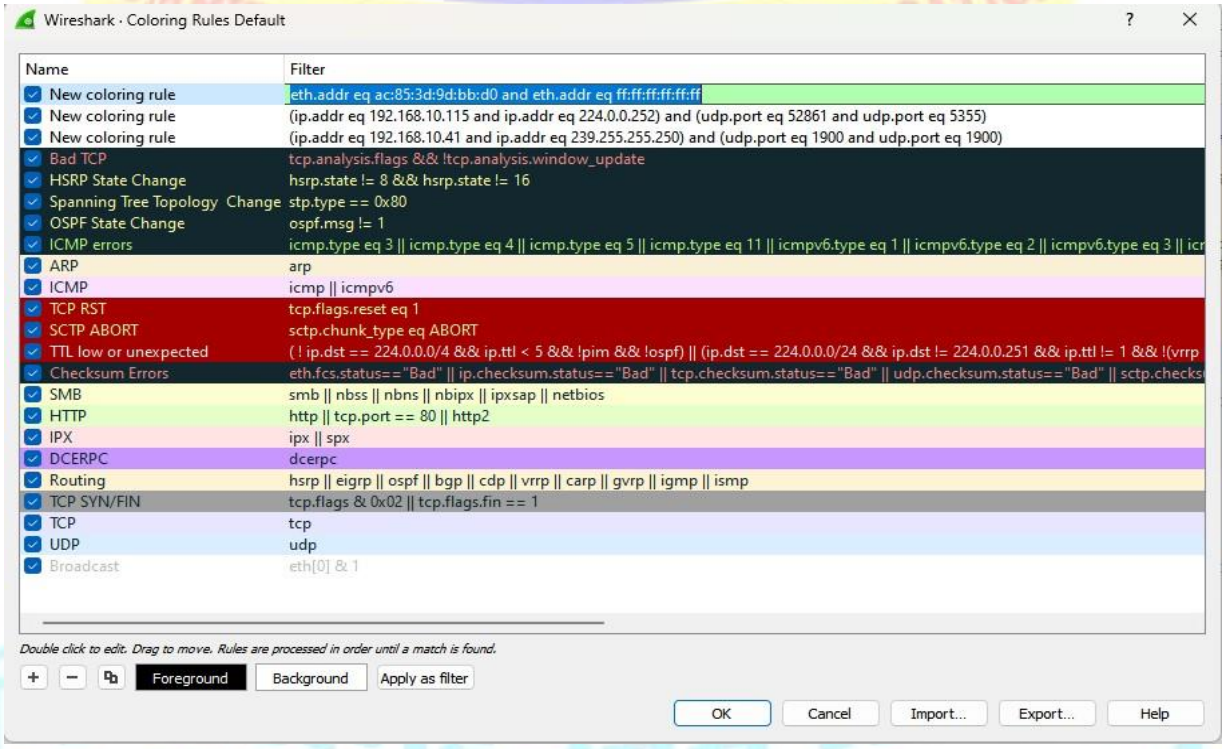
- Light Purple color for TCP traffic
- Light Blue color for UDP traffic
- Black color identifies packets with errors

Example these packets are delivered in an unordered manner.

Click on View → Colorize Conversation → New Coloring Rule

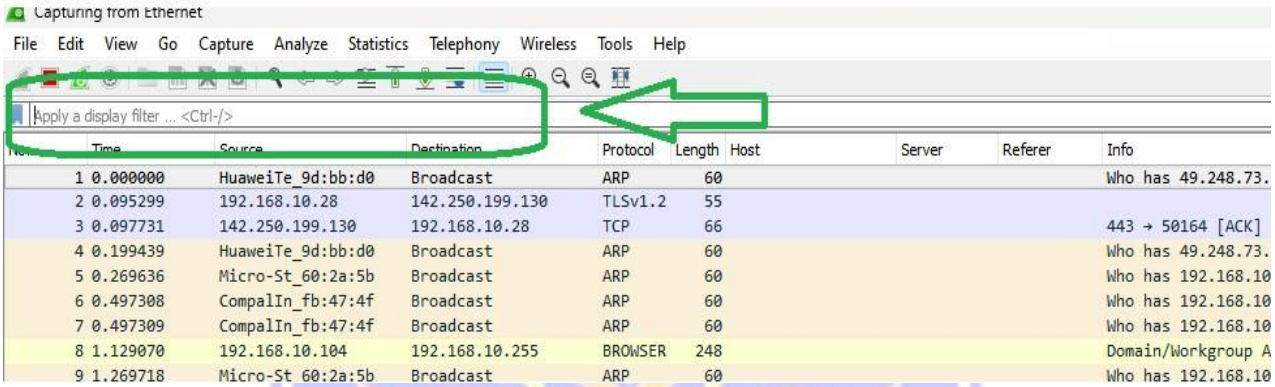


Here we can see the Default Colors given for every **Packet Capturing**

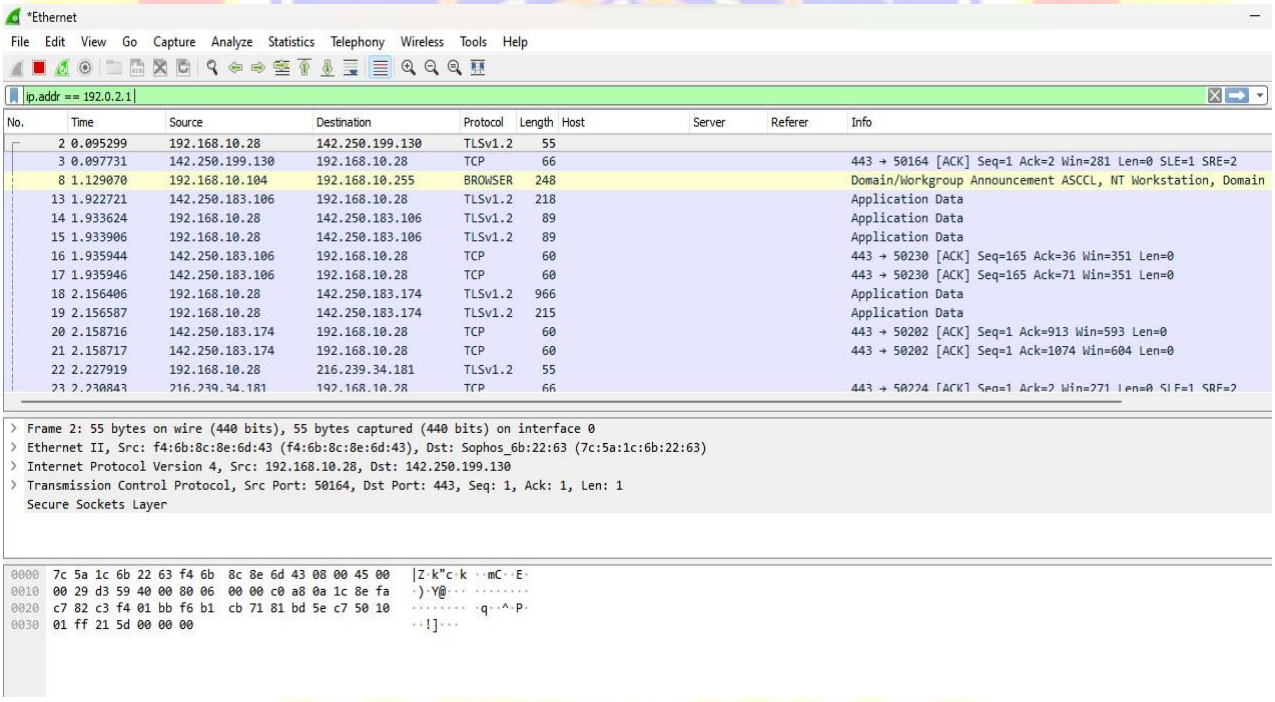


Now we analyze data using filters provided in the WireShark application

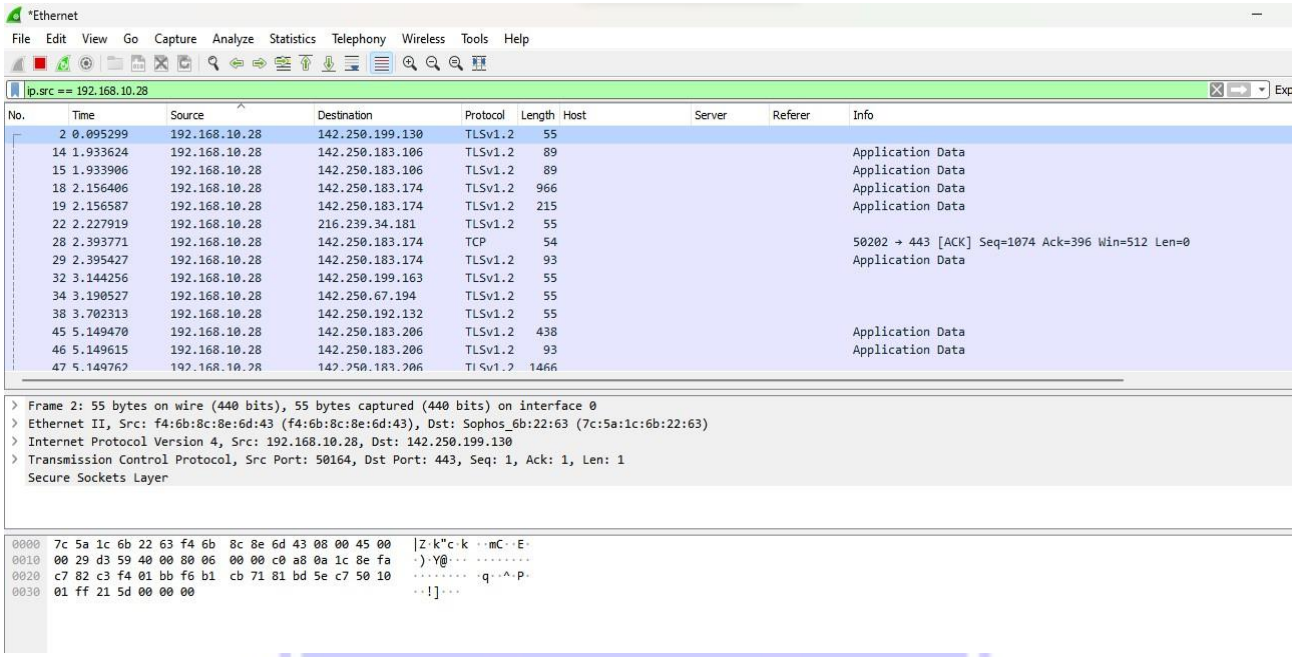
Write the following commands in the given area to apply filter



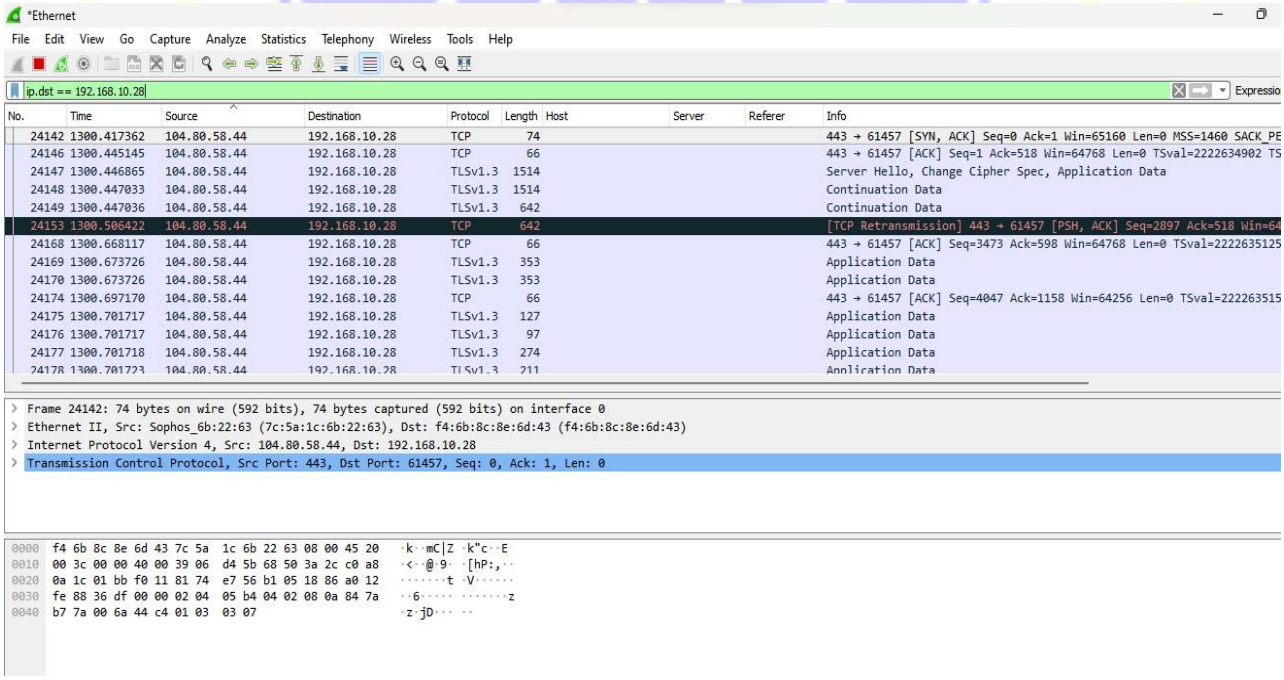
- ip.addr == 192.0.2.1



1. Display packets which are coming from specific IP-address
   - ip.src == 192.168.10.28

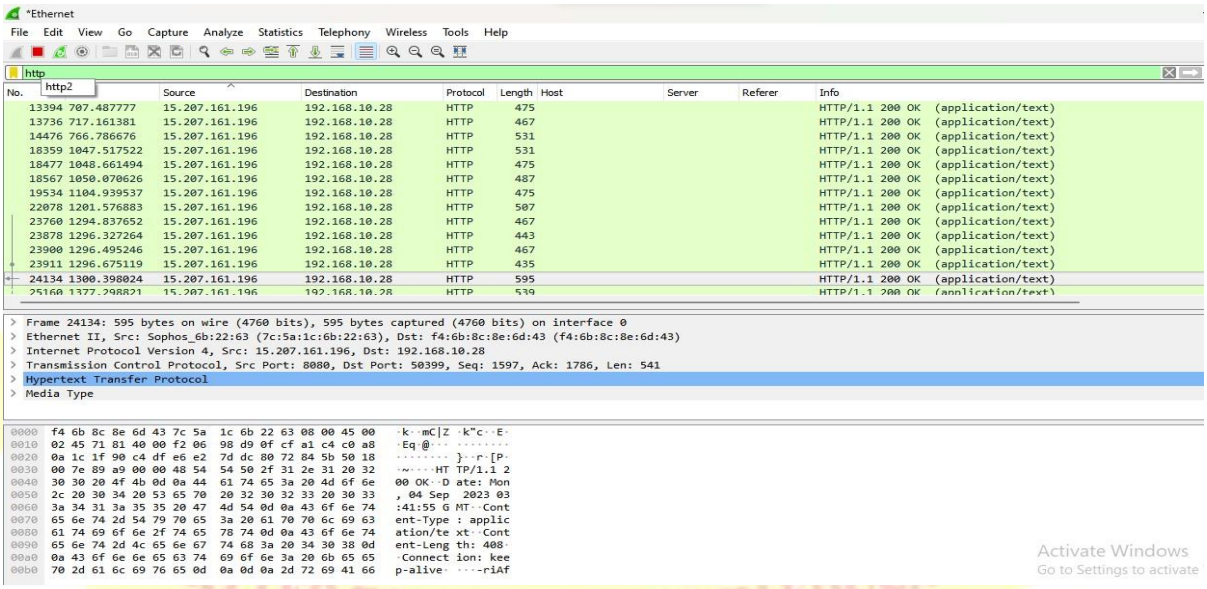


2. Display packets which are having specific IP-address destination
   - ip.dst == 192.168.10.28

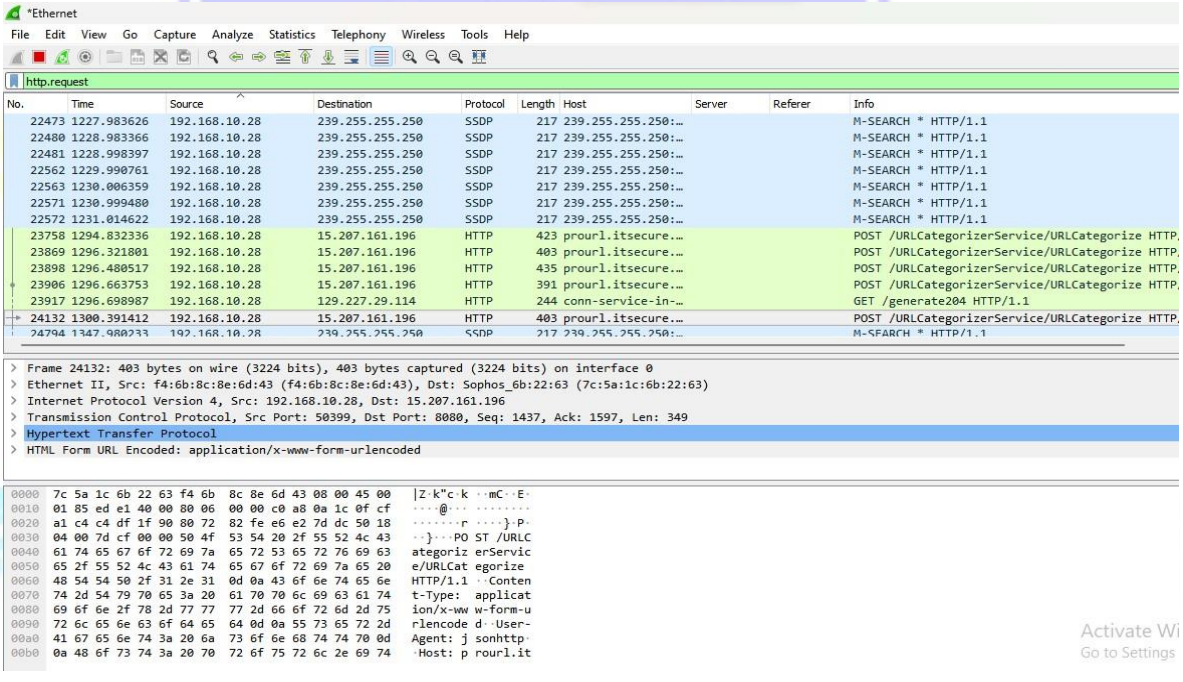


3.Display packets which are using http protocol

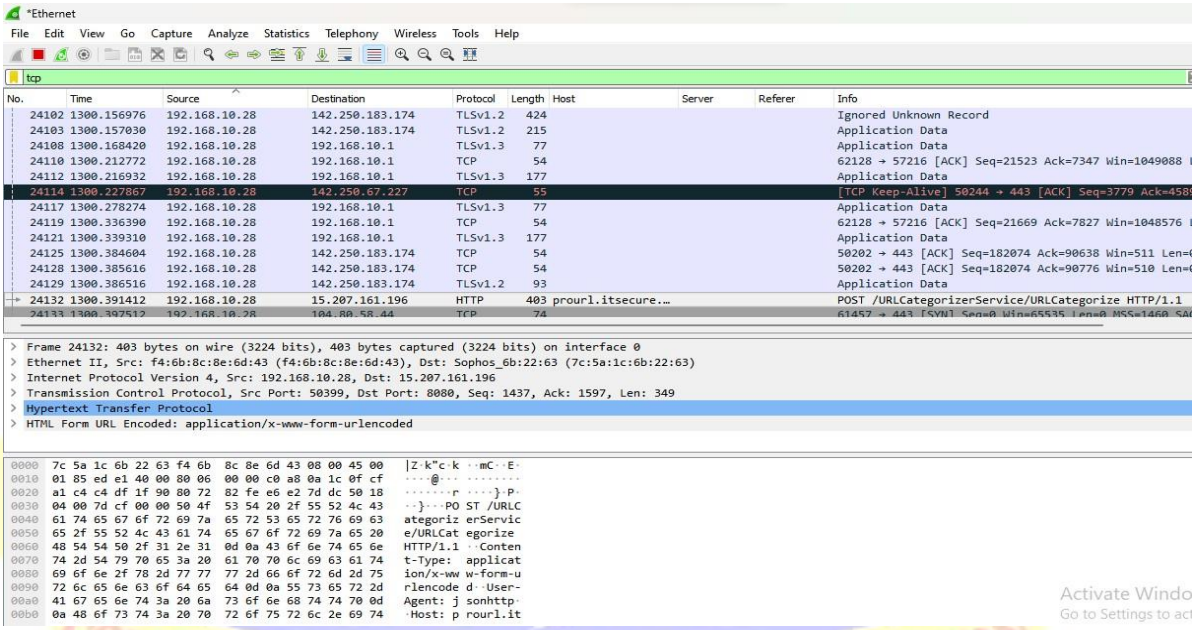
- http



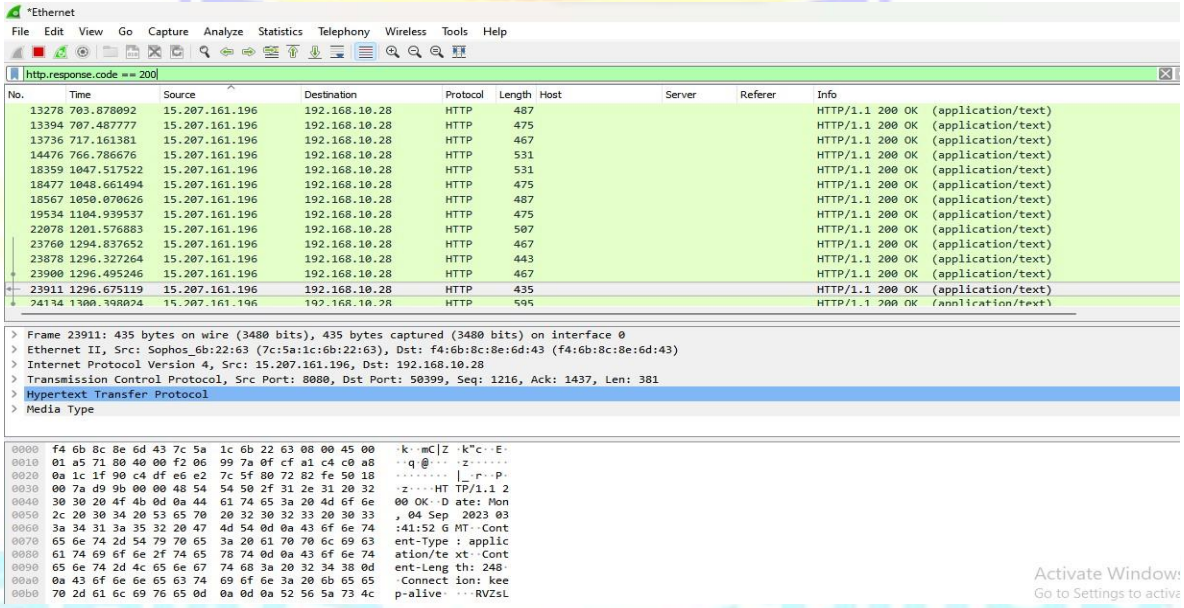
3. Display packets which are using http request
   - http.request



4. Display packets which are using TCP protocol
   - tcp

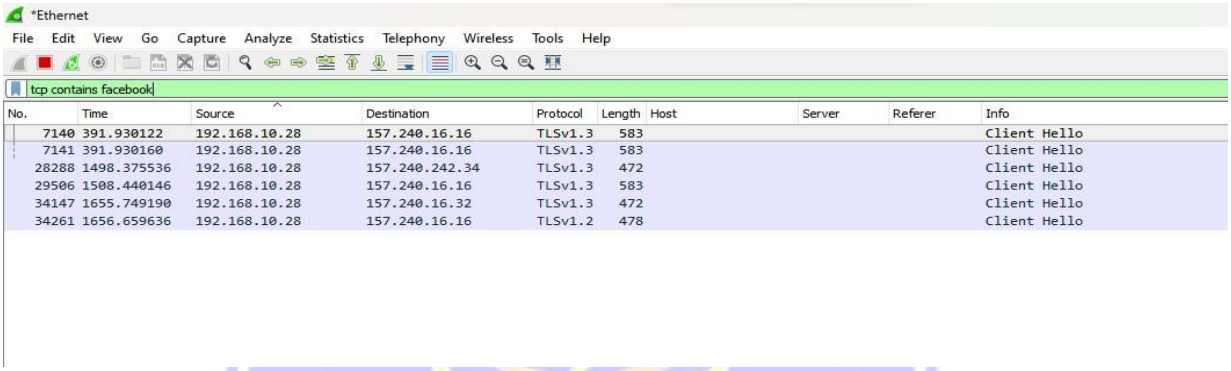


5. Display packets having no error connecting to server
   - http.response.code==200



6. Display packets having port number 80, 443
   - tcp.port==80 || udp.port==443

7. Display packets which that contains keyword facebook
   - tcp contains facebook



Now we are going to perform a **Case Study**

AIM:

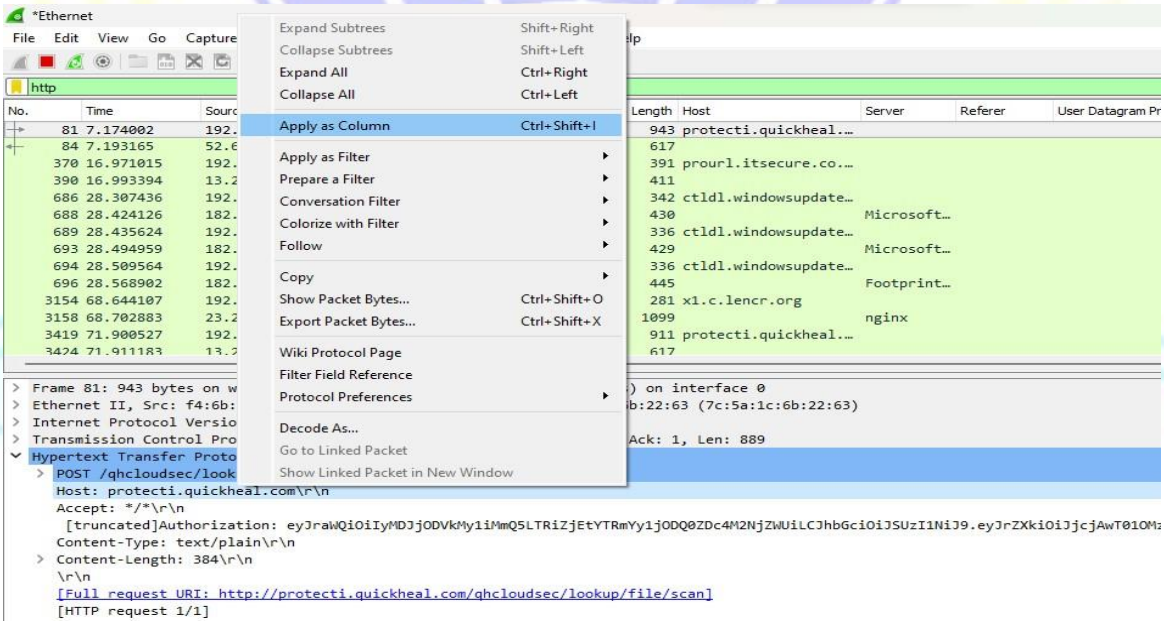
Analyze the packets provided in lab and solve the questions using Wireshark

1. What web server software issued by go.microsoft.com?

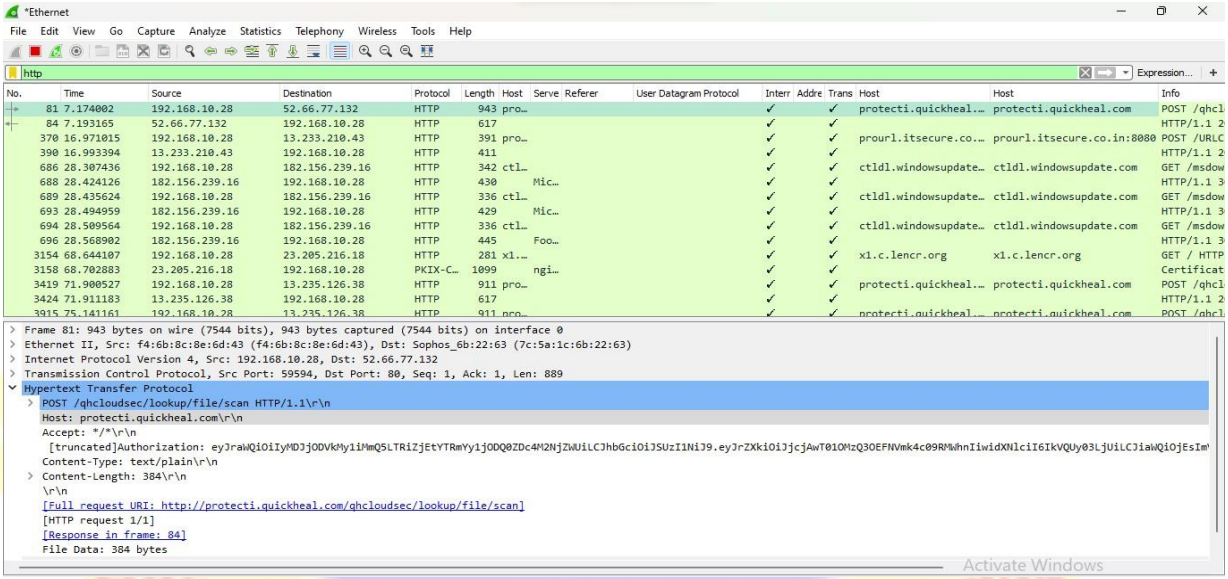
Analysis –

The domain name be found from host header so we will set host header column where we will see all domain name. Select any HTTP request and expand the Hypertext Transfer Protocol then right click on Host header and then Apply as Column

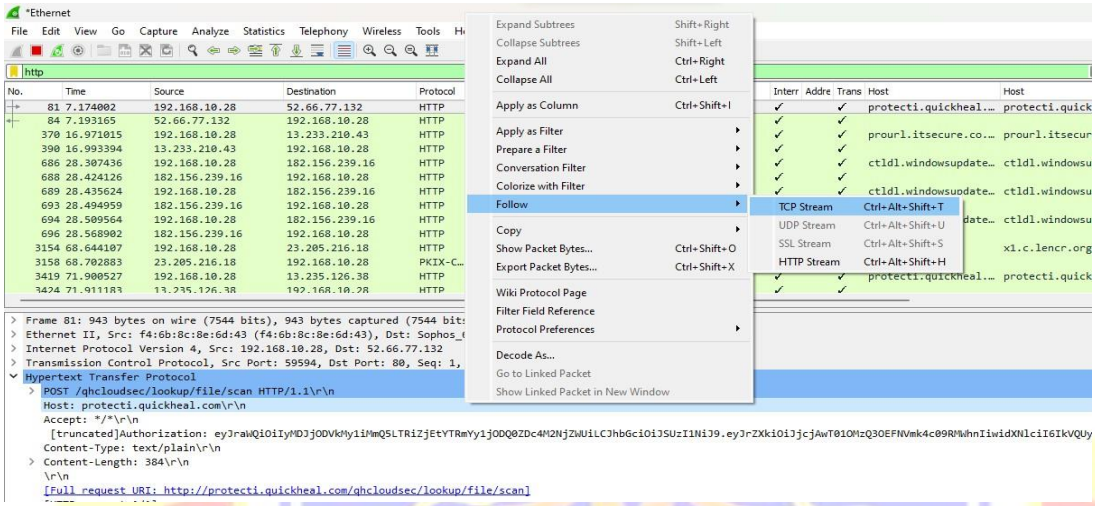
First find the requests from **HTTP** and click on and **request** then on the **lower table of details** Select on
HyperText Transfer Protocol → **Host** and **Right Click** on that and Select **Apply as Filter**

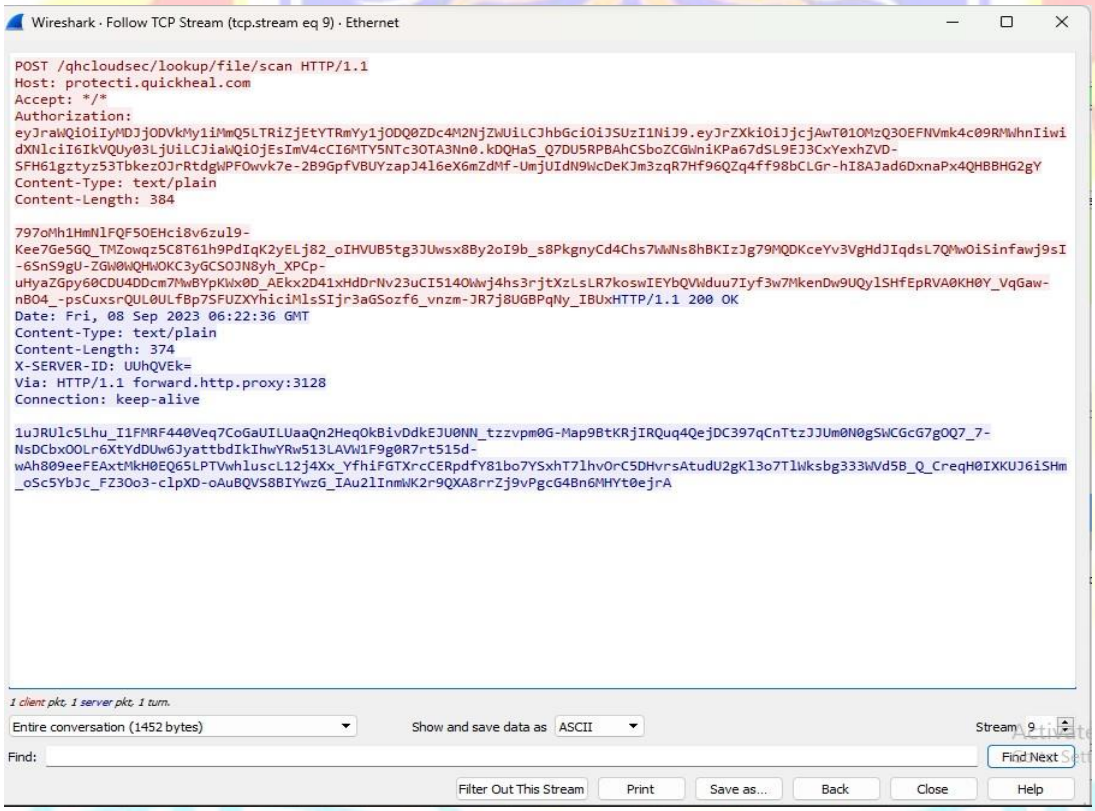


Now we can see the **Host**



Right click on the **selected packet** and then select **Follow → TCP stream**



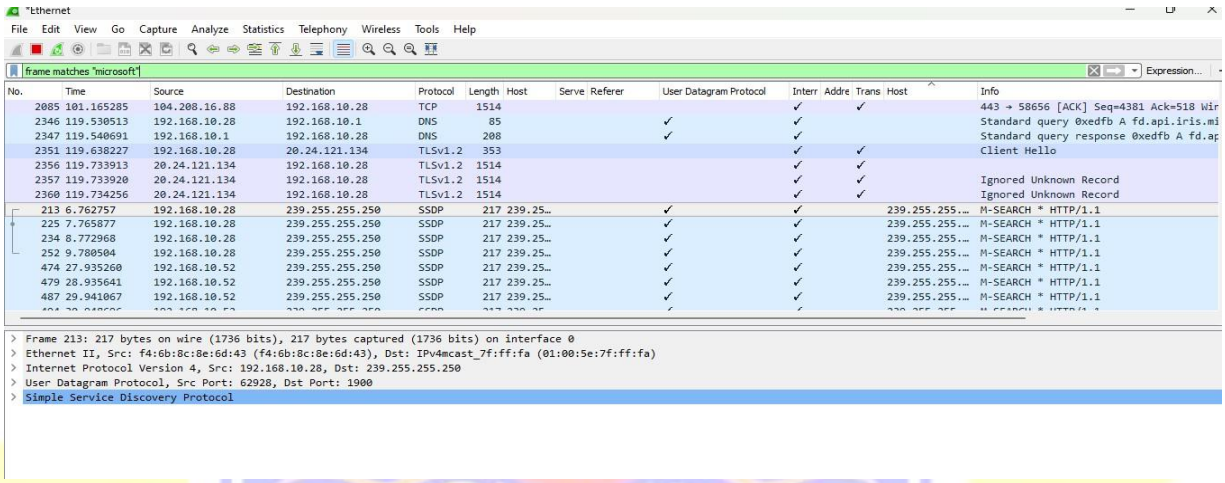


2. About what cell phone problem is the client concerned?

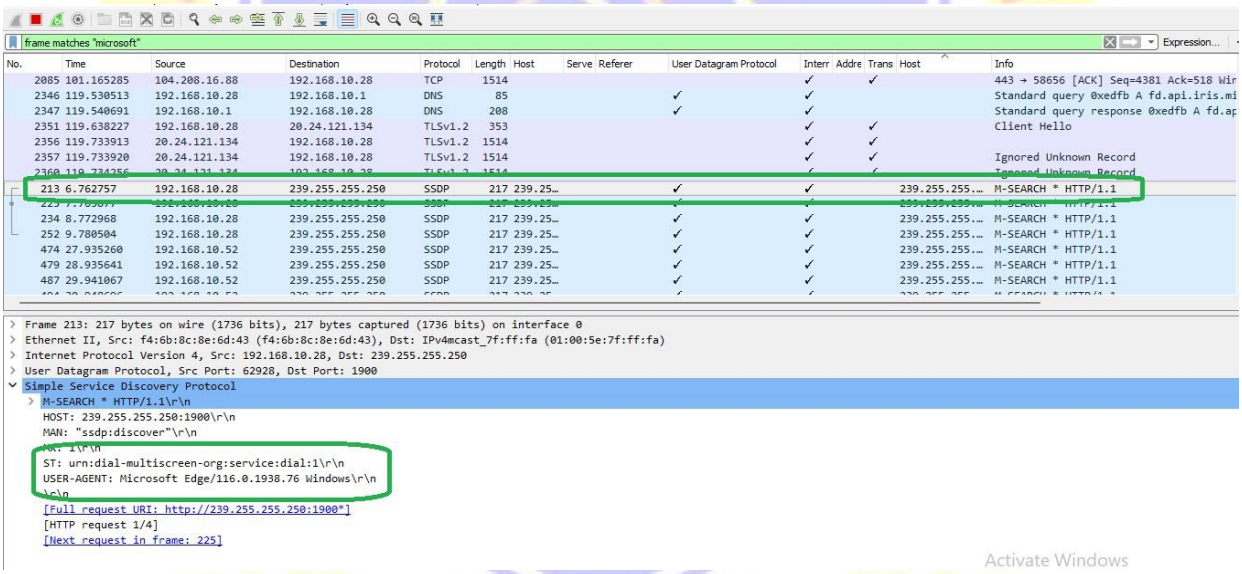
Analysis –

Client talking about cell so we search for cell keyword in whole packets. We will use regular express for searching the cell keyword. Apply frame matches "()"

In the **search frame** type **frame matches "microsoft"**



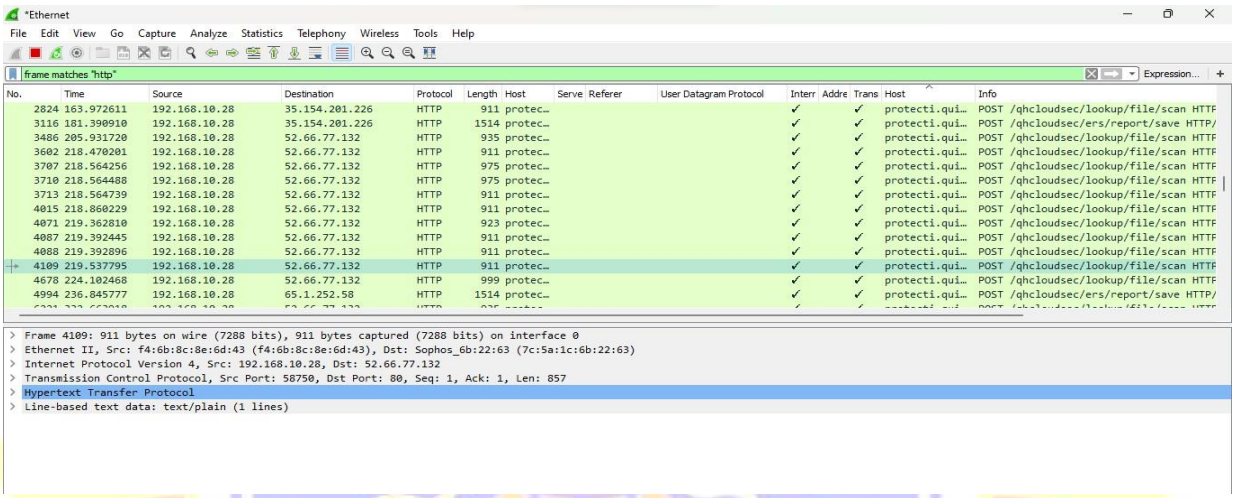
After applying the filter now, we will start to check every HTTP request. We noticed in the first HTTP request microsoft keyword is in URL and it was about Microsoft Edge connection.



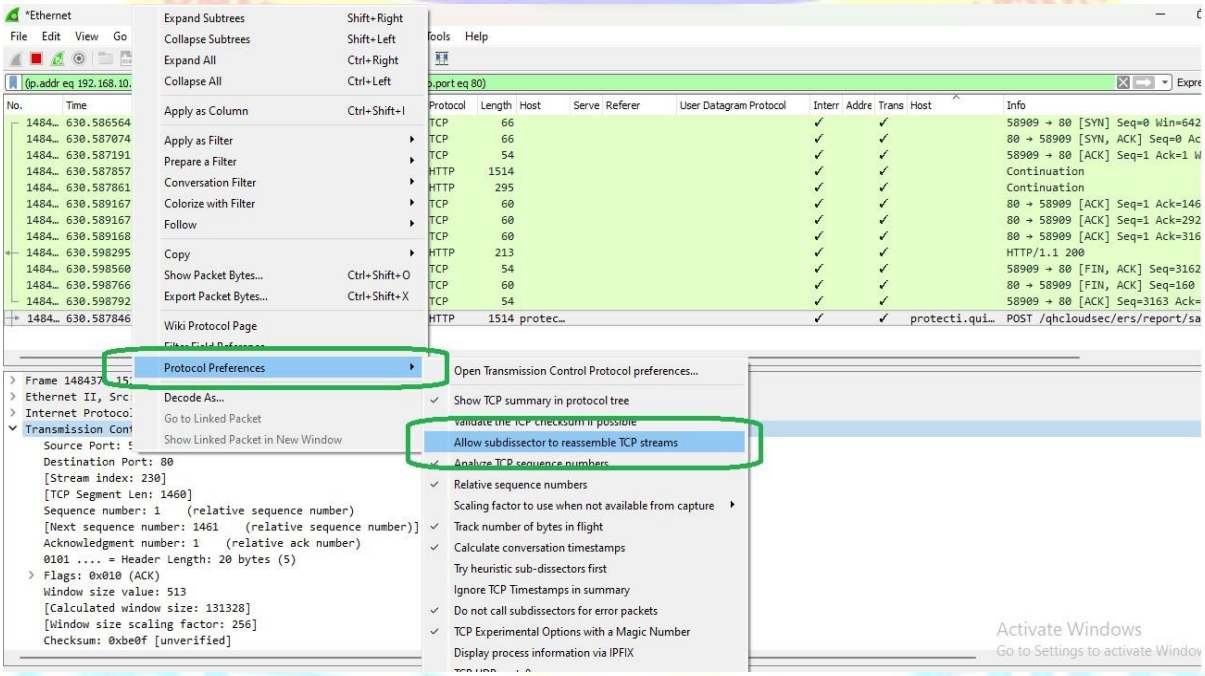
3. According to http, what data will TCP show?

Analysis –

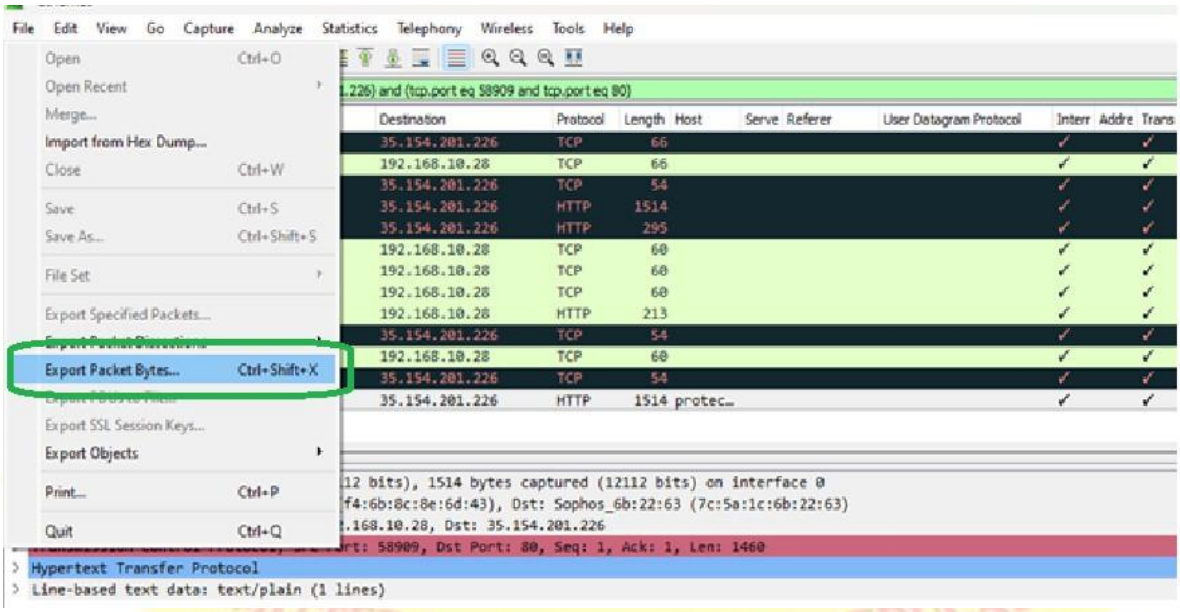
As we did in the last challenge, we will **apply a regular express filter** for the Google **keyword**. **Apply frame matched "http"** .



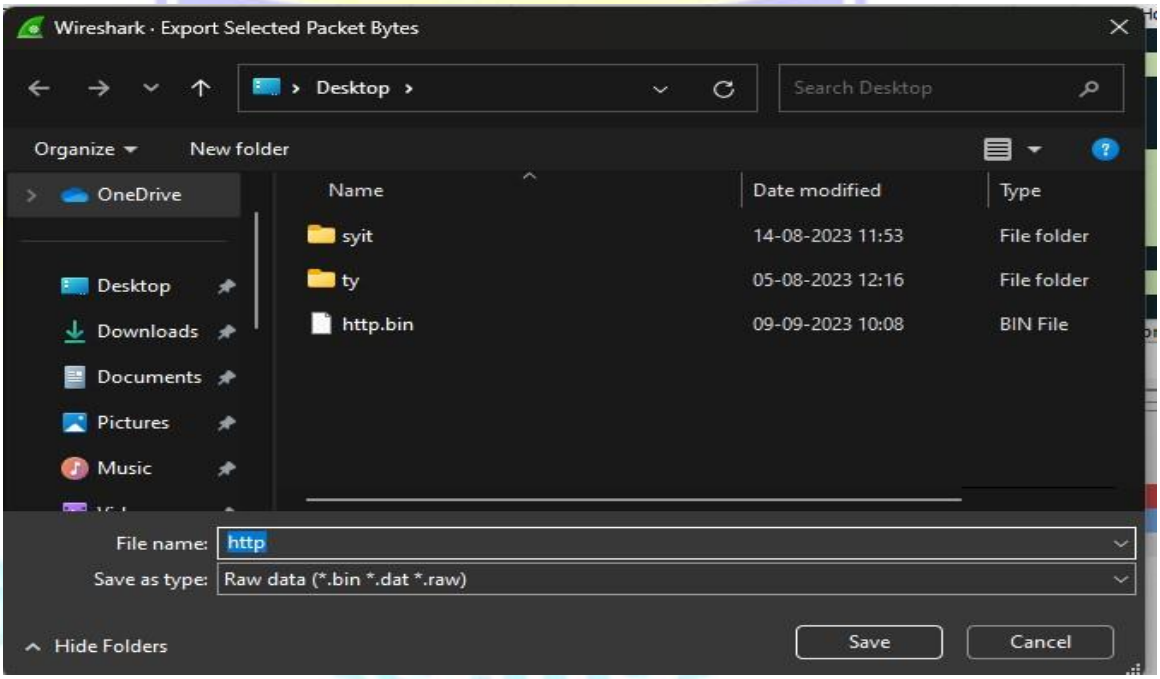
Select the packet and **expand the Hypertext Transfer Protocol** tab **right click** on **Transmission Control Protocol** **Go to Protocol Preferences** and **check Allow subdissector** to resemble TCP stream with HTTP spanning bodies.



Now **Go to file** and **select Export Objects** → **HTTP**. It will save all objects from the packet.



Click on save all.

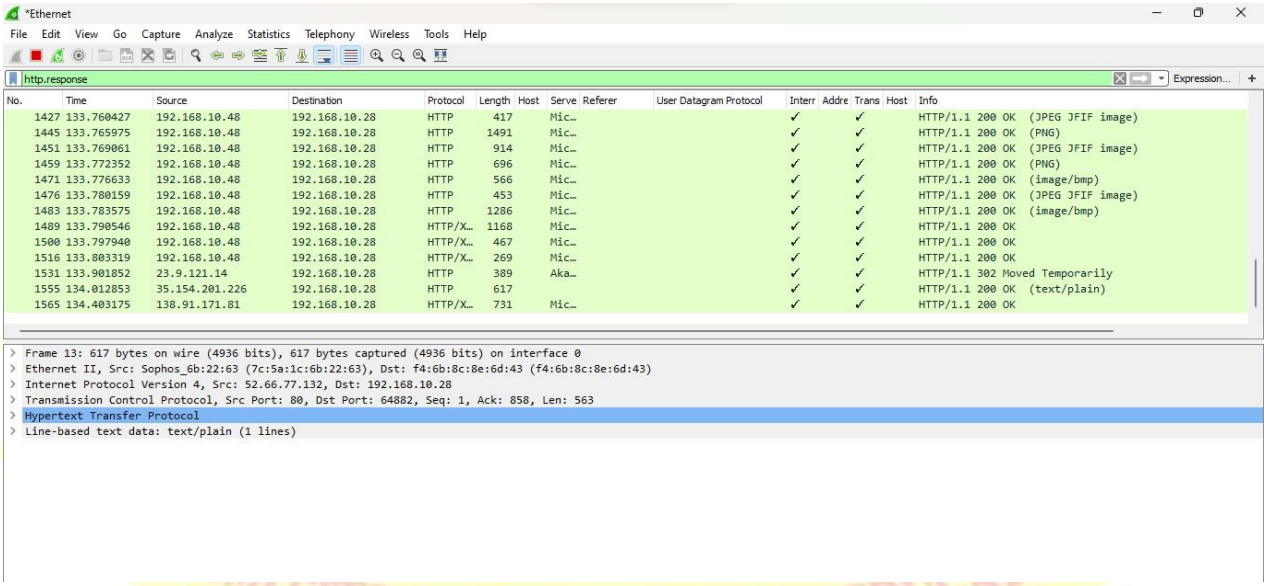


After checking it seems only the packets transfer were to connect the machine to the internet.

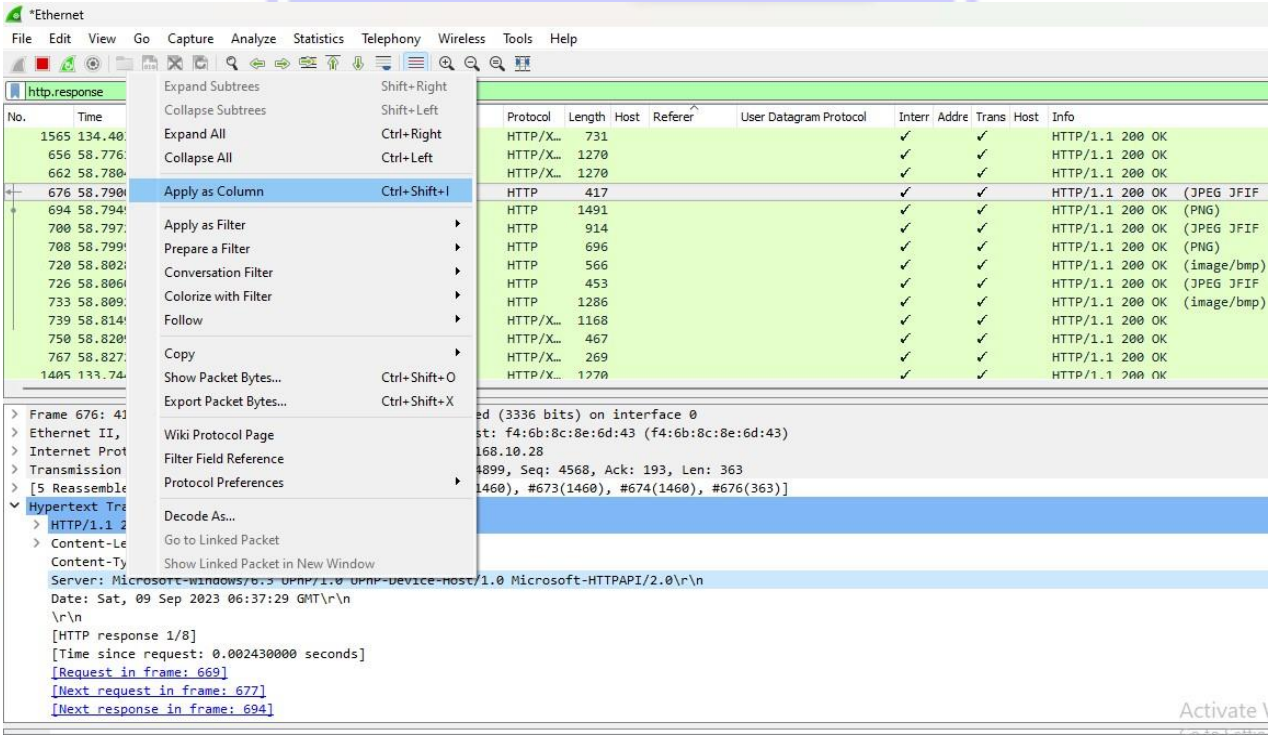
4. How many web servers are running Microsoft?

Analysis –

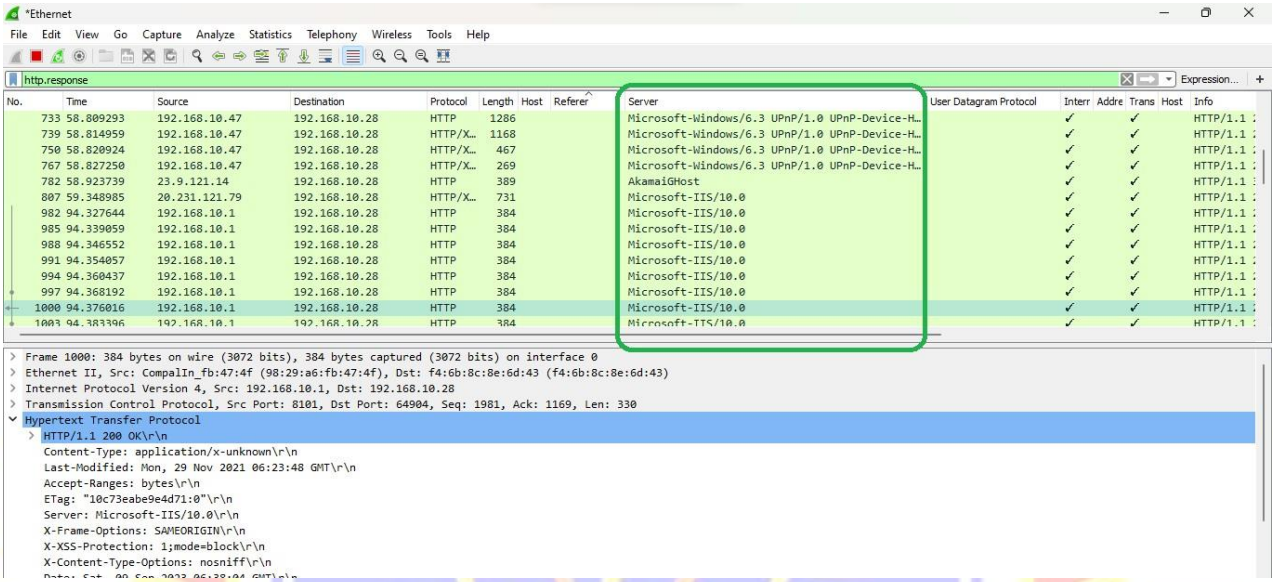
The web server name can be retrieved from **HTTP response header**. So will apply filter **http.response** and we can see all http response packets.



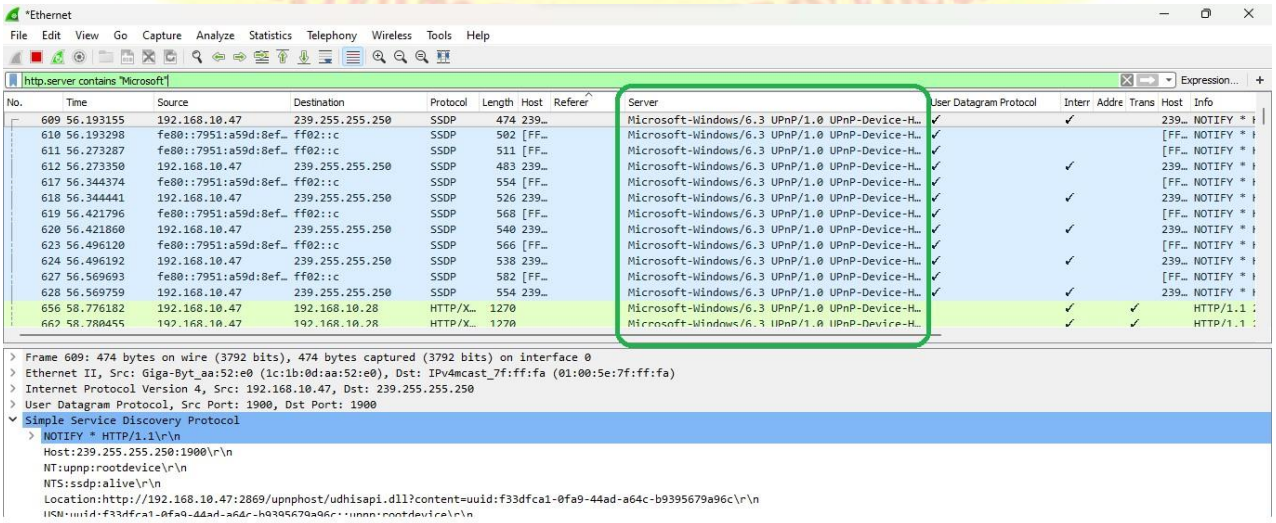
Now we will set the server header as column select any packet and right click on it then select Apply as Column.



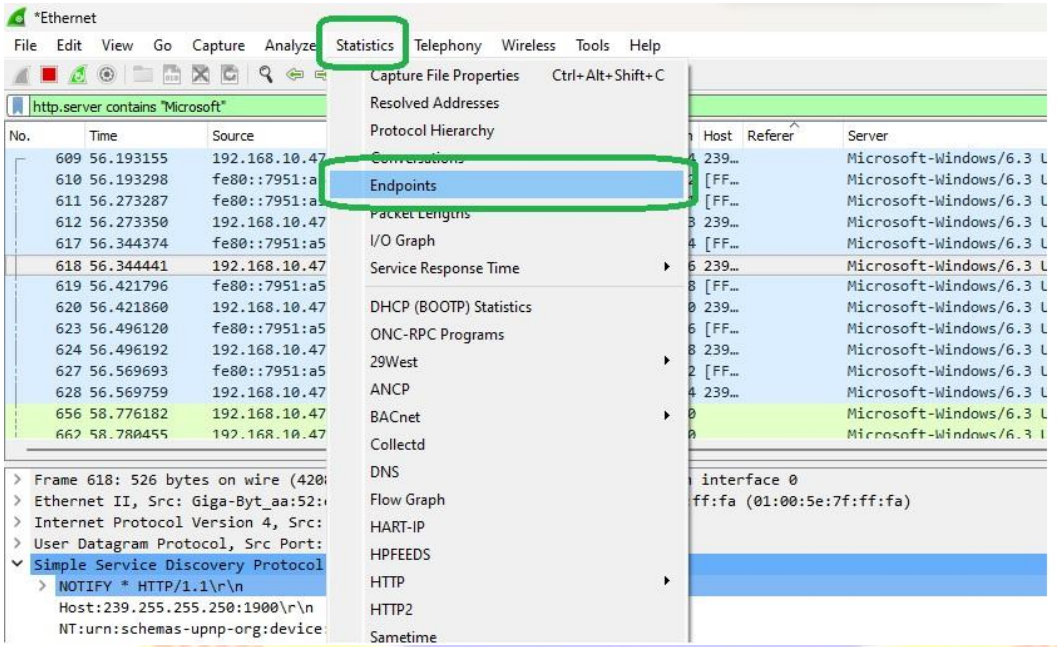
Now can see the server column where all server name is showing.



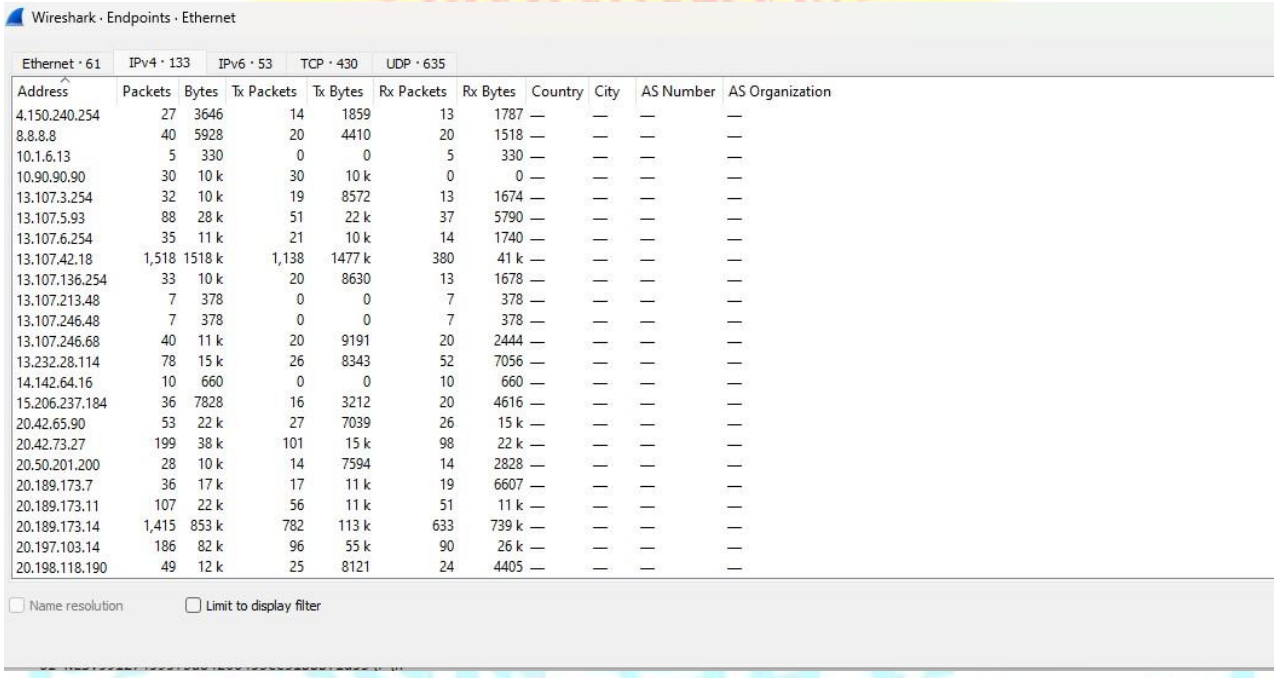
Now we have to check how many Apache packets are there we can't count manually for each packet so we will apply another filter **http.server contains "Microsoft"**



After applying filter **Go to Statistics** → **Endpoints**

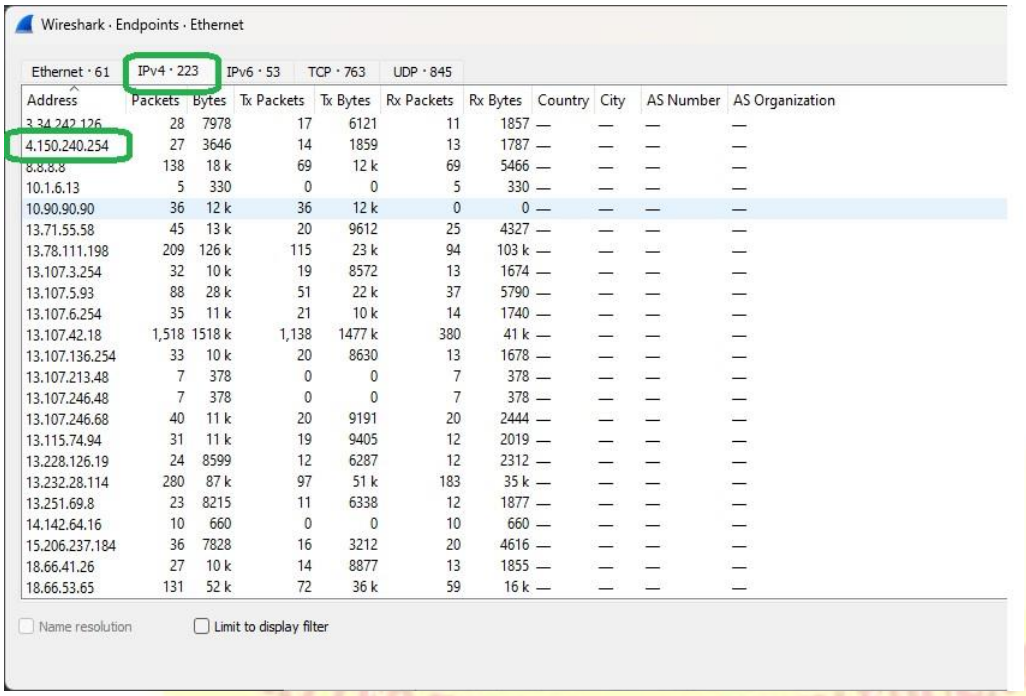


It will show all connections.



Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	AS Number	AS Organization
4.150.240.254	27	3646	14	1859	13	1787	—	—	—	—
8.8.8.8	40	5928	20	4410	20	1518	—	—	—	—
10.1.6.13	5	330	0	0	5	330	—	—	—	—
10.90.90.90	30	10 k	30	10 k	0	0	—	—	—	—
13.107.3.254	32	10 k	19	8572	13	1674	—	—	—	—
13.107.5.93	88	28 k	51	22 k	37	5790	—	—	—	—
13.107.6.254	35	11 k	21	10 k	14	1740	—	—	—	—
13.107.42.18	1,518	1518 k	1,138	1477 k	380	41 k	—	—	—	—
13.107.136.254	33	10 k	20	8630	13	1678	—	—	—	—
13.107.213.48	7	378	0	0	7	378	—	—	—	—
13.107.246.48	7	378	0	0	7	378	—	—	—	—
13.107.246.68	40	11 k	20	9191	20	2444	—	—	—	—
13.232.28.114	78	15 k	26	8343	52	7056	—	—	—	—
14.142.64.16	10	660	0	0	10	660	—	—	—	—
15.206.237.184	36	7828	16	3212	20	4616	—	—	—	—
20.42.65.90	53	22 k	27	7039	26	15 k	—	—	—	—
20.42.73.27	199	38 k	101	15 k	98	22 k	—	—	—	—
20.50.201.200	28	10 k	14	7594	14	2828	—	—	—	—
20.189.173.7	36	17 k	17	11 k	19	6607	—	—	—	—
20.189.173.11	107	22 k	56	11 k	51	11 k	—	—	—	—
20.189.173.14	1,415	853 k	782	113 k	633	739 k	—	—	—	—
20.197.103.14	186	82 k	96	55 k	90	26 k	—	—	—	—
20.198.118.190	49	12 k	25	8121	24	4405	—	—	—	—

Check the limit to display filter then it will show the actual Microsoft connections. Now there are showing 223 connections but will exclude 4.150.240.254 because it is client's IP not a server IP so there are actual 222 Microsoft servers.



Wireshark · Endpoints · Ethernet

Ethernet · 61 | IPv4 · 223 | IPv6 · 53 | TCP · 763 | UDP · 845

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	AS Number	AS Organization
3.34.242.126	28	7978	17	6121	11	1857	—	—	—	—
4.150.240.254	27	3646	14	1859	13	1787	—	—	—	—
8.8.8.8	138	18 k	69	12 k	69	5466	—	—	—	—
10.1.6.13	5	330	0	0	5	330	—	—	—	—
10.90.90.90	36	12 k	36	12 k	0	0	—	—	—	—
13.71.55.58	45	13 k	20	9612	25	4327	—	—	—	—
13.78.111.198	209	126 k	115	23 k	94	103 k	—	—	—	—
13.107.3.254	32	10 k	19	8572	13	1674	—	—	—	—
13.107.5.93	88	28 k	51	22 k	37	5790	—	—	—	—
13.107.6.254	35	11 k	21	10 k	14	1740	—	—	—	—
13.107.42.18	1,518	1518 k	1,138	1477 k	380	41 k	—	—	—	—
13.107.136.254	33	10 k	20	8630	13	1678	—	—	—	—
13.107.213.48	7	378	0	0	7	378	—	—	—	—
13.107.246.48	7	378	0	0	7	378	—	—	—	—
13.107.246.68	40	11 k	20	9191	20	2444	—	—	—	—
13.115.74.94	31	11 k	19	9405	12	2019	—	—	—	—
13.228.126.19	24	8599	12	6287	12	2312	—	—	—	—
13.232.28.114	280	87 k	97	51 k	183	35 k	—	—	—	—
13.251.69.8	23	8215	11	6338	12	1877	—	—	—	—
14.142.64.16	10	660	0	0	10	660	—	—	—	—
15.206.237.184	36	7828	16	3212	20	4616	—	—	—	—
18.66.41.26	27	10 k	14	8877	13	1855	—	—	—	—
18.66.53.65	131	52 k	72	36 k	59	16 k	—	—	—	—

Name resolution | Limit to display filter

CONCLUSION:

We have successfully analyzed the packets provided and solved the questions using WireShark

Result:

Capturing and analyzing network packets using Wireshark helps identify live networks and extract critical information from the captured data, which is essential for network forensics and investigation.

Learning Outcomes:

- Understand how to capture and analyze network packets using Wireshark.
- Learn to identify live networks and extract relevant information.
- Develop skills to analyze packet data for investigative purposes.

Course Outcomes:

- Gain practical knowledge of using Wireshark for network packet capture and analysis.
- Ability to identify live networks and analyze captured packets effectively.
- Apply network forensic techniques to investigate network traffic**.**

Conclusion:

Viva Questions:

1. What is Wireshark, and why is it used in network forensics?
2. How can you identify a live network using Wireshark?
3. What kind of data can be analyzed from captured packets?
4. Why is packet analysis important in network forensics?

PRACTICAL NO: 5

Aim:

Using Sysinternals tools for Network Tracking and Process Monitoring:

- Check Sysinternals tools
- Monitor Live Processes
- Capture RAM
- Capture TCP/UDP packets
- Monitor Hard Disk
- Monitor Virtual Memory
- Monitor Cache Memory

Practical:

Lets Check If the **Sysinternal Suite** is **Available** on the **System**

Check SysInternals Tools

STEPS

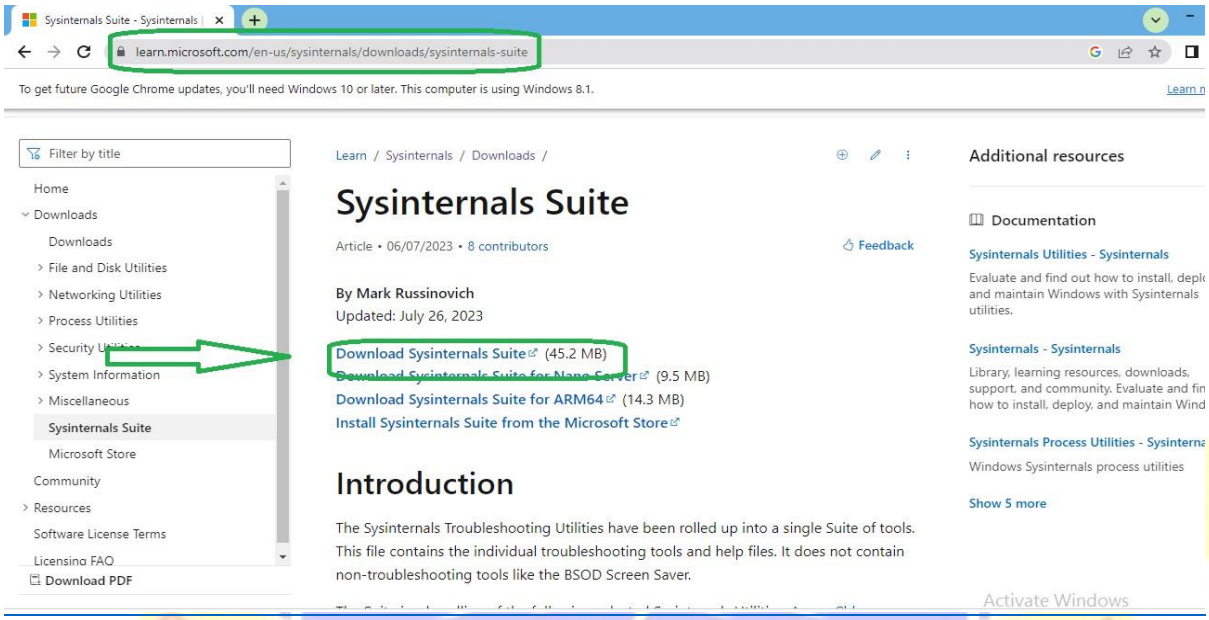
Google → sysinternal tools

If **Available** Then **Skip** the **Installation Part**

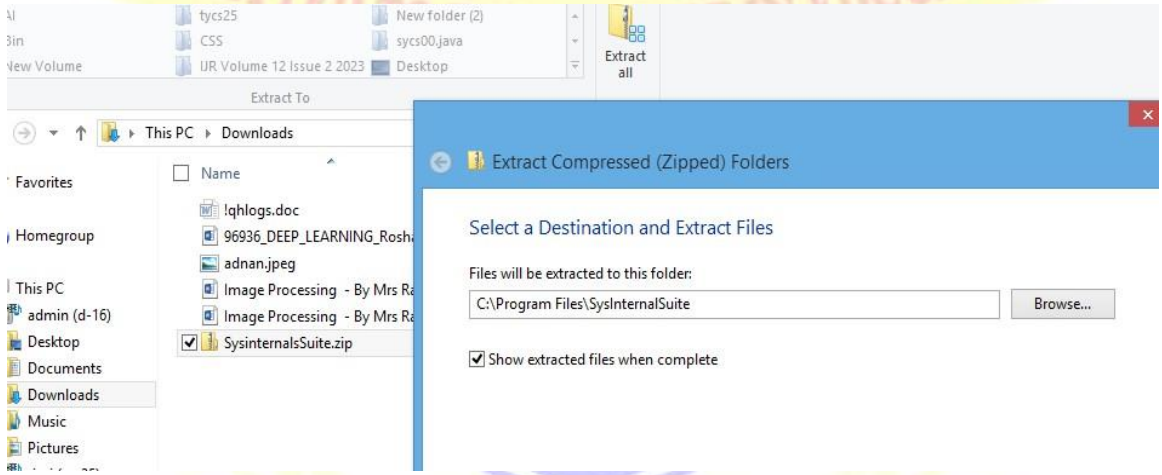
Let's Install the **Sysinternal Suite** for **Windows** We

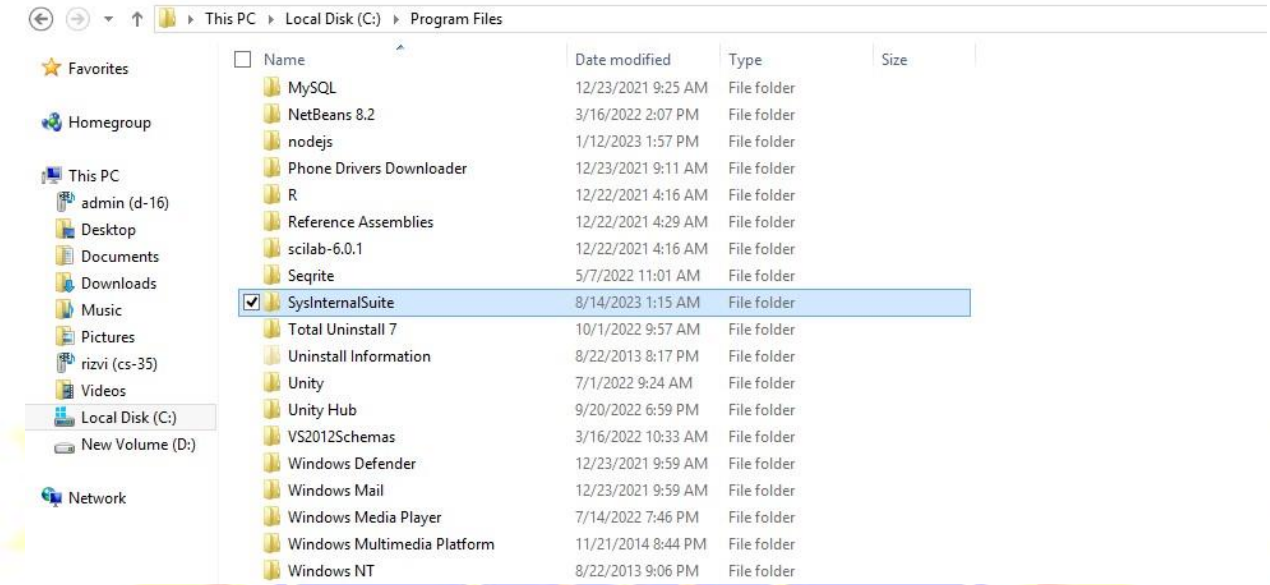
can download the zip file from the given link

https://learn.microsoft.com/en-us/sysinternals/downloads/sysinternals-suite



Then Extract the file to the desired directory



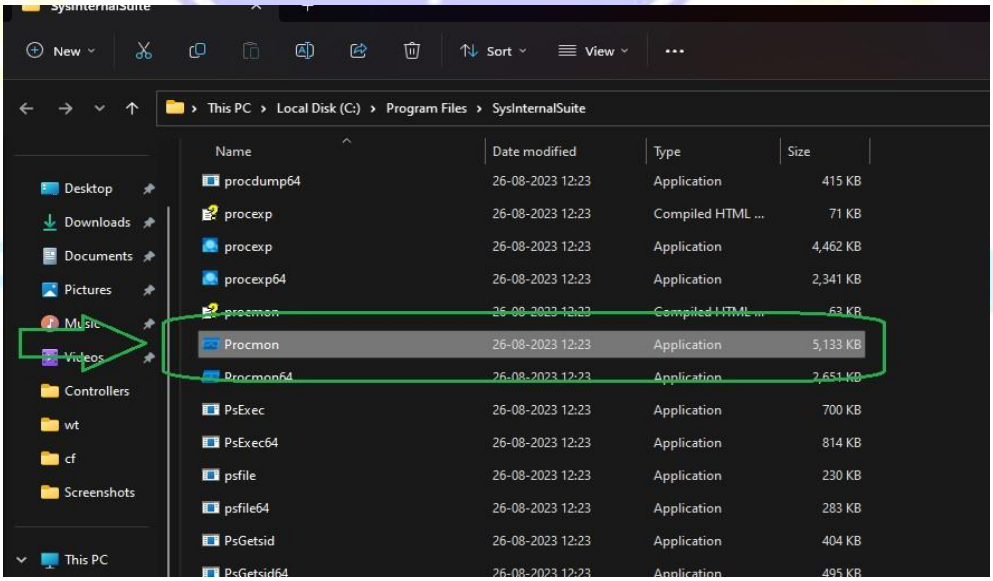


Monitor Live Processes

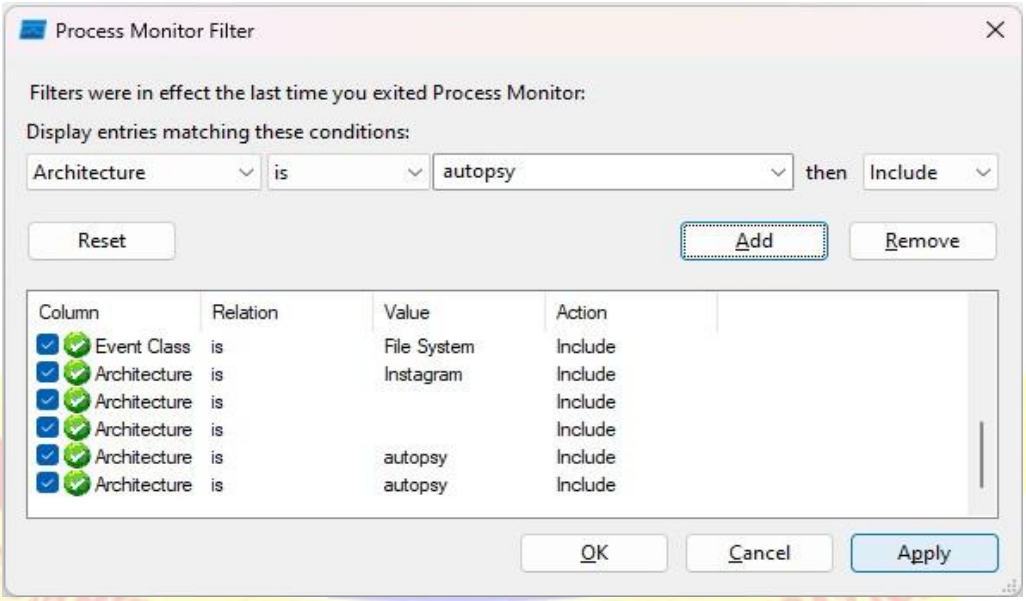
Process Monitor is an advanced monitoring tool for Windows that show real-time file system. Registry and process/thread activity. It combines the features of two legacy SysInternals utilities, Filemon and Regmon, and adds an extensive list of enhancements including rich non-destructive filtering, comprehensive event properties such as session IDs and user names, reliable process information, full thread stacks with integrated symbol support for each operation, simultaneous logging to a file, and much more.

STEPS

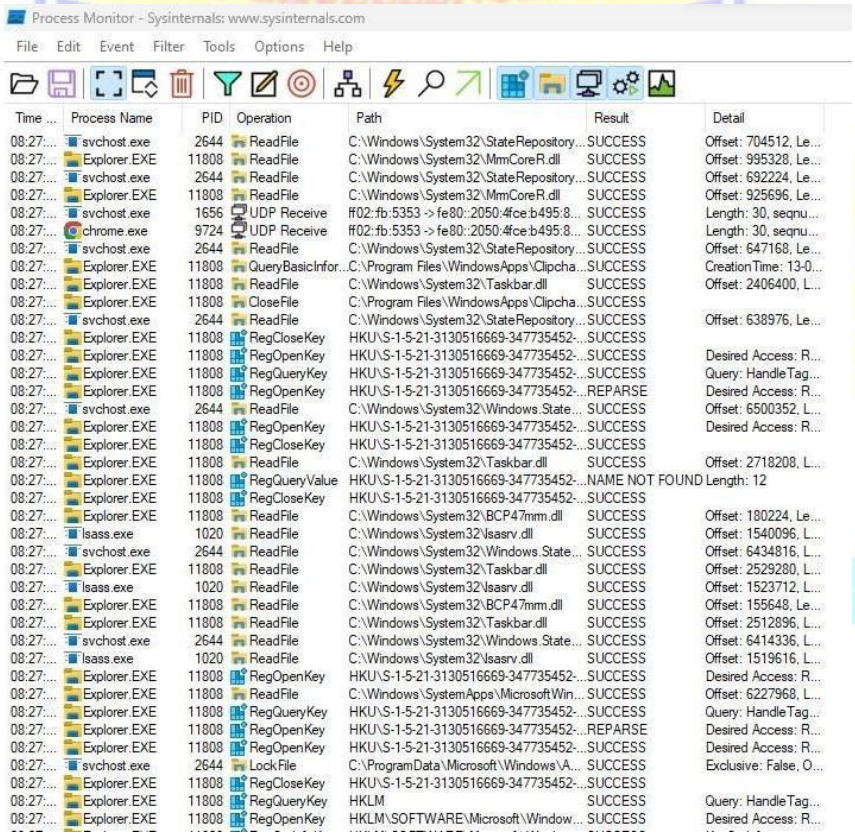
Sysinternal → procmon



Then allow the permissions and then Select all the processes to be viewed



Then Click on Apply and then OK Then see the displayed Processes



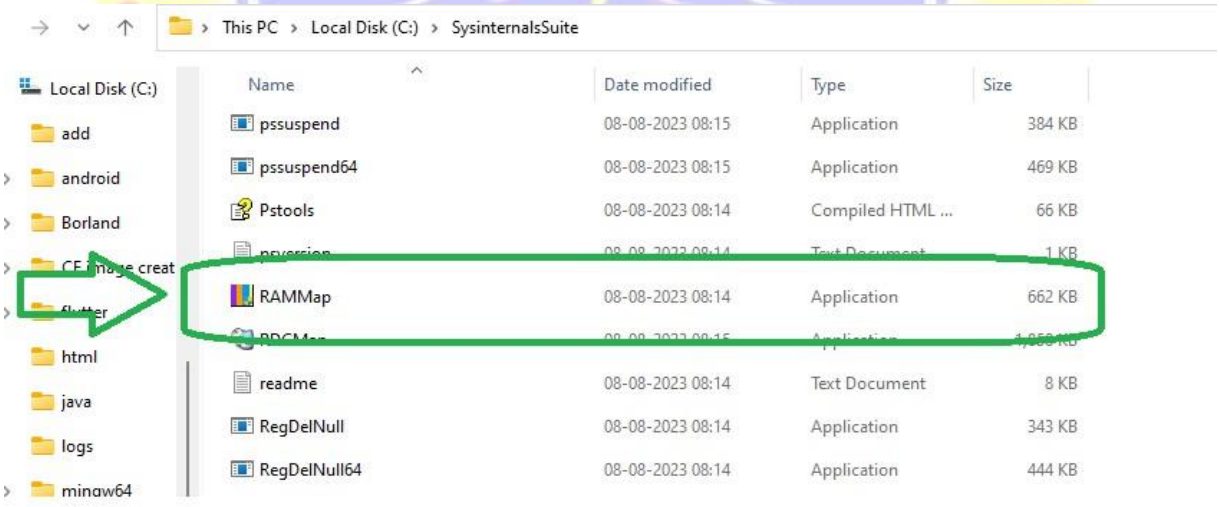
Capture RAM

RAMMap is an advanced physical memory usage analysis utility for Windows Vista and higher. It presents usage information in different ways on its several different tabs:

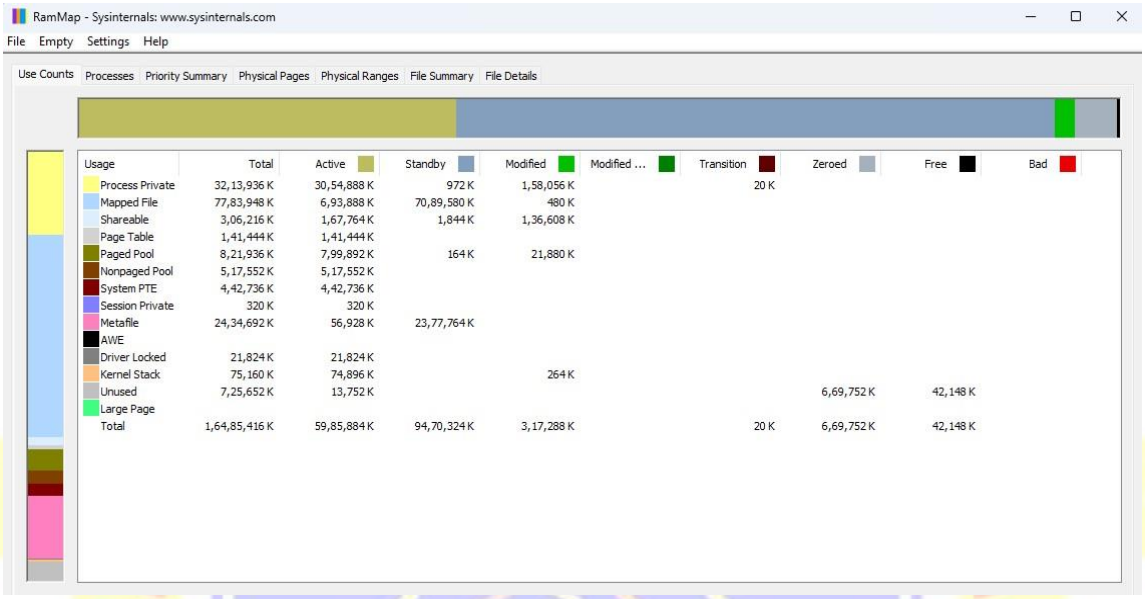
- **Use Counts**: usage summary by type and paging list
- **Processes**: process working set sizes
- **Priority Summary**: prioritized standby list sizes
- **Physical Pages**: per-page use for all physical memory
- **Physical Ranges**: physical memory addresses
- **File Summary**: file data in RAM by file
- **File Details**: individual physical pages by file

STEPS

Sysinternal → RAMMap



Then allow the permissions and view the mapping



Capture TCP/UDP packets

TCPView is Windows program that will show you detailed listening's of all TCP and UDP endpoints on your system, including the local and remote addresses and the state of TCP connections.

Using TCPView:

When you start TCPView it will enumerate all the active TCP and UDP endpoints, resolving all IP address to their domain name versions. You can use a toolbar button on menu item to toggle the display of resolves names.

Using Tcpvcon

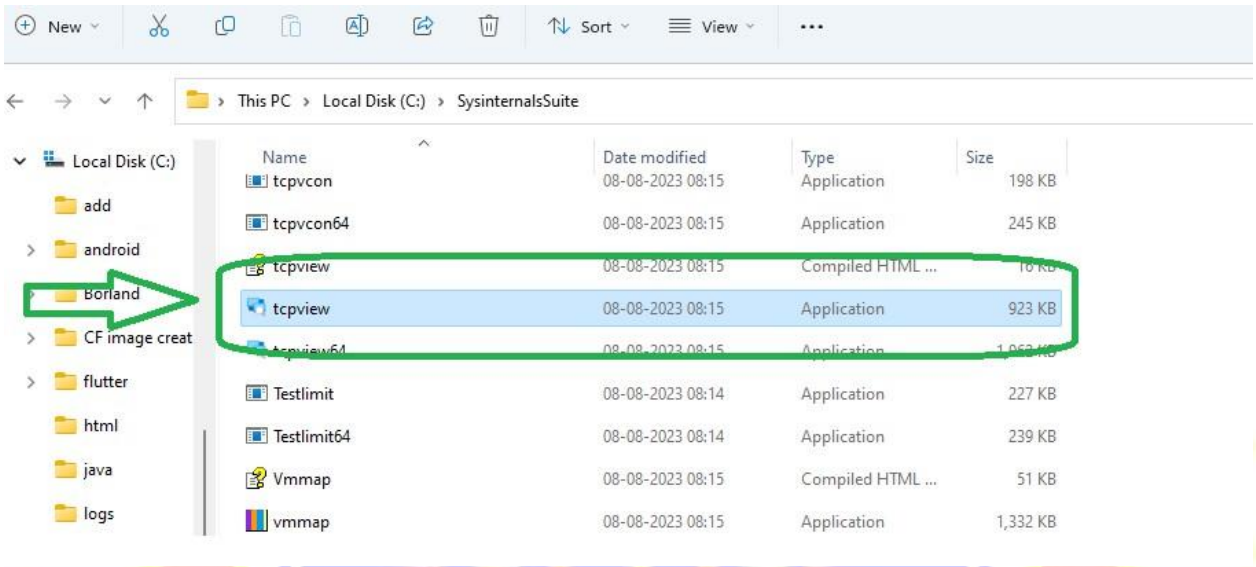
Tcpvcon using is similar to that of the built-in Windows netstat utility

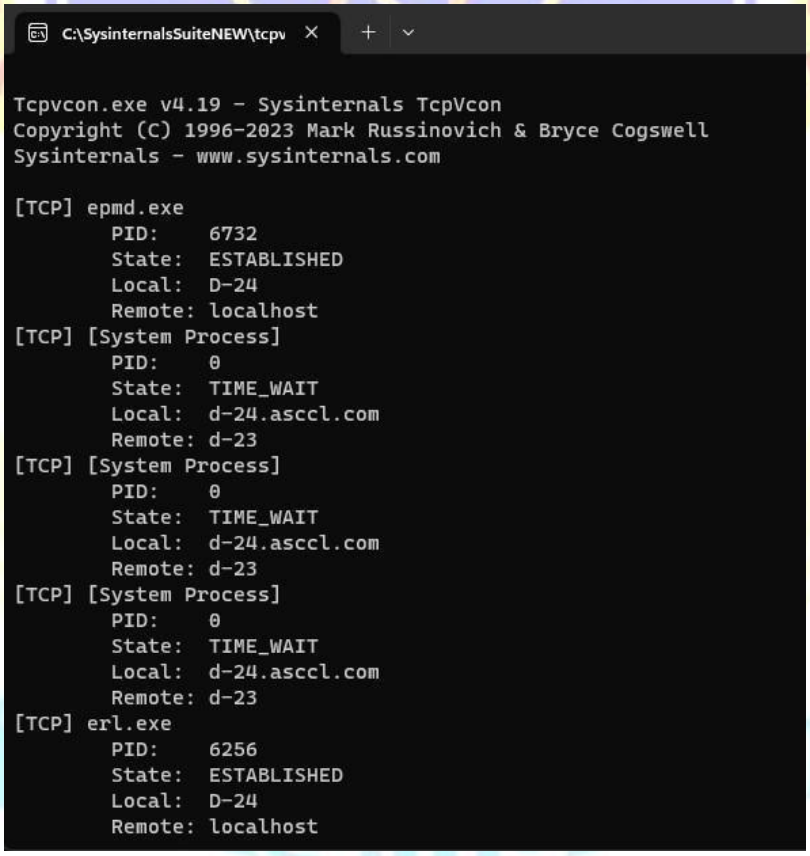
Usage

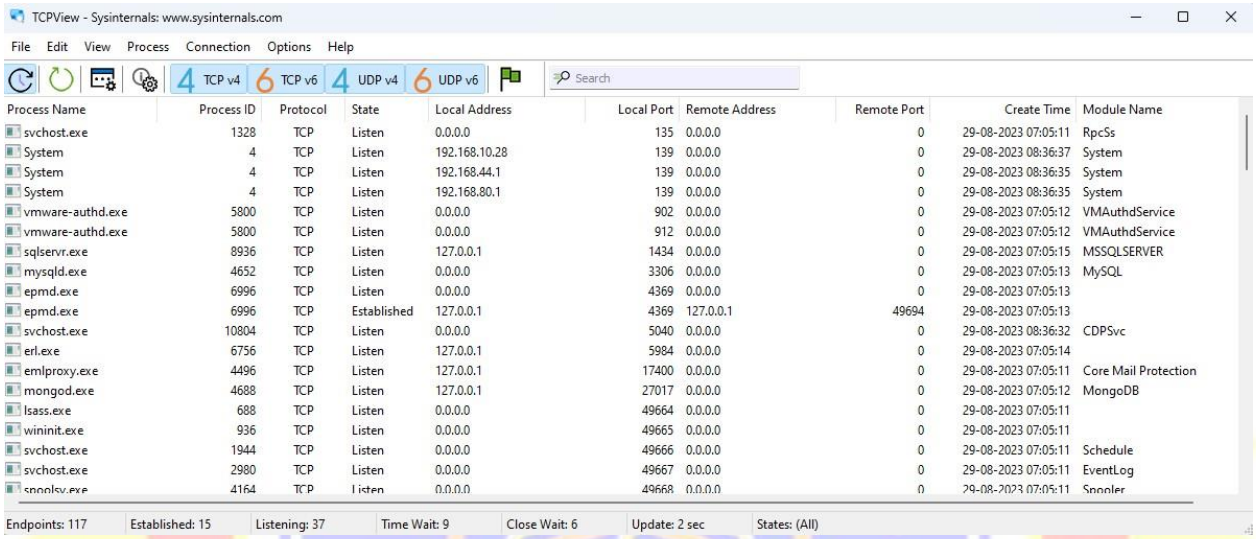
Tcpvcon [-a] [-c] [-n] [process name or PID]

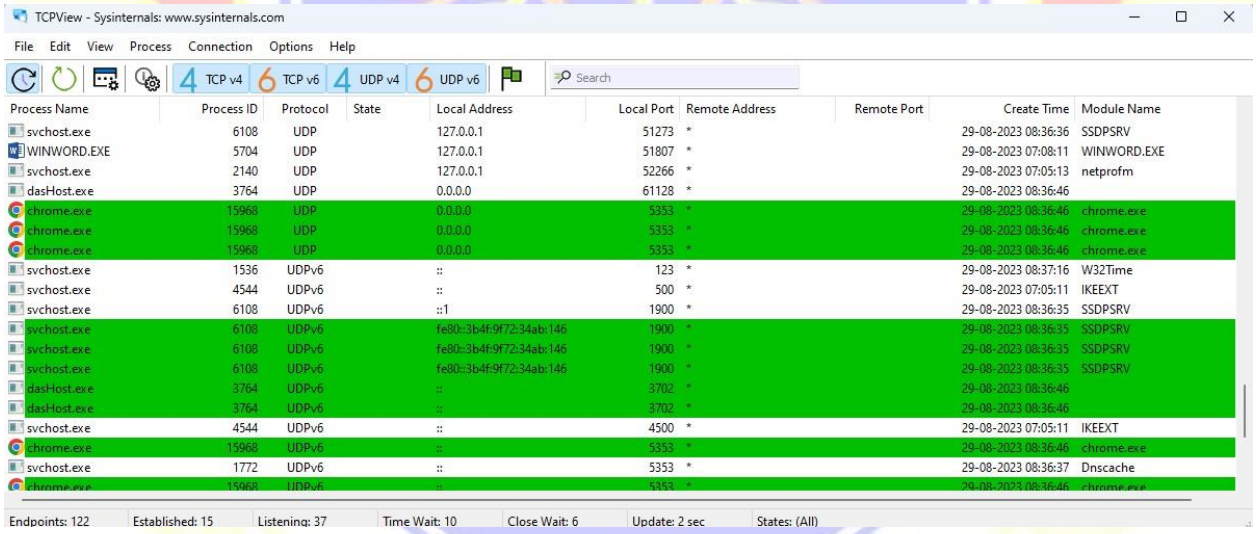
STEPS

Download TCPView


New
Sort
View
This PC › Local Disk (C:) › SysinternalsSuite
Local Disk (C:)
add
android
Borland
CF image creat
flutter
html
java
logs
Name
Date modified
Type
Size
tcpvcon 08-08-2023 08:15 Application 198 KB
tcpvcon64 08-08-2023 08:15 Application 245 KB
tcpview 08-08-2023 08:15 Compiled HTML ... 16 KB
tcpview 08-08-2023 08:15 Application 923 KB
Testlimit 08-08-2023 08:14 Application 227 KB
Testlimit64 08-08-2023 08:14 Application 239 KB
Vmmap 08-08-2023 08:15 Compiled HTML ... 51 KB
vmmap 08-08-2023 08:15 Application 1,332 KB


C:\SysinternalsSuiteNEW\tcpv
Tcpvcon.exe v4.19 - Sysinternals TcpVcon
Copyright (C) 1996-2023 Mark Russinovich & Bryce Cogswell
Sysinternals - www.sysinternals.com
[TCP] epmd.exe
PID: 6732
State: ESTABLISHED
Local: D-24
Remote: localhost
[TCP] [System Process]
PID: 0
State: TIME_WAIT
Local: d-24.asccl.com
Remote: d-23
[TCP] [System Process]
PID: 0
State: TIME_WAIT
Local: d-24.asccl.com
Remote: d-23
[TCP] [System Process]
PID: 0
State: TIME_WAIT
Local: d-24.asccl.com
Remote: d-23
[TCP] erl.exe
PID: 6256
State: ESTABLISHED
Local: D-24
Remote: localhost



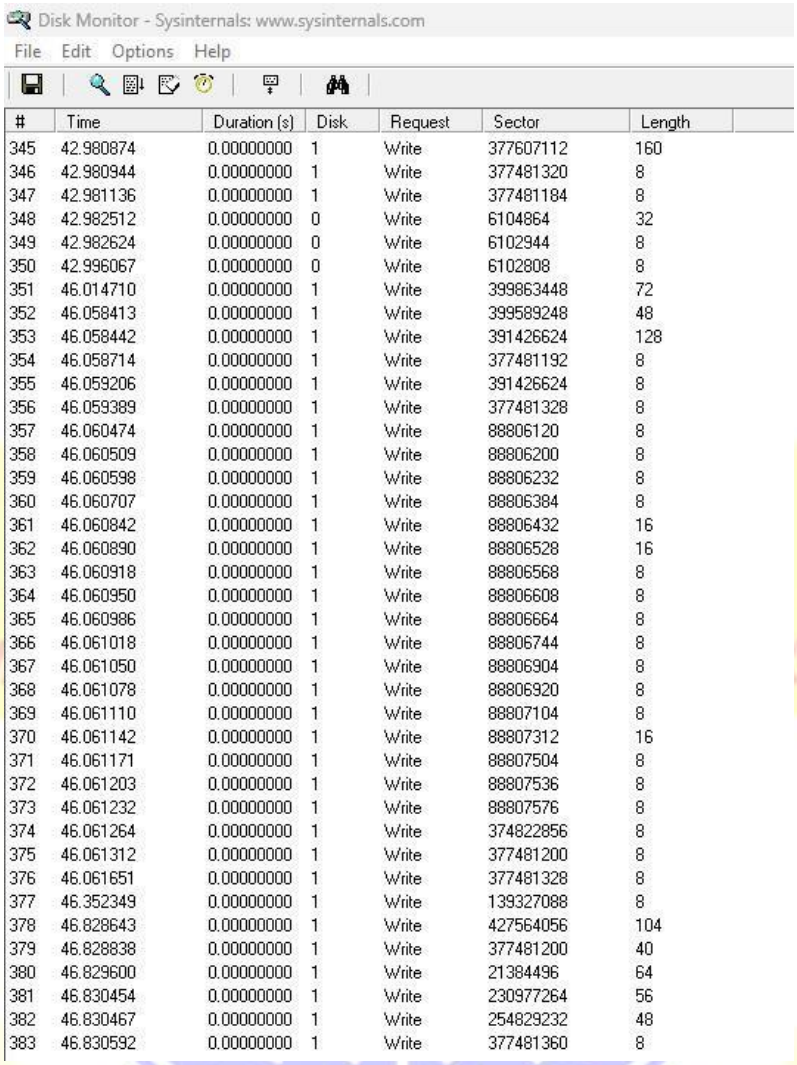


Monitor Hard Disk

DiskMon is an application that logs and displays all hard disk activity on a Windows system

STEPS

Download DiskMon → Run as Administrator


Disk Monitor - Sysinternals: www.sysinternals.com

File Edit Options Help

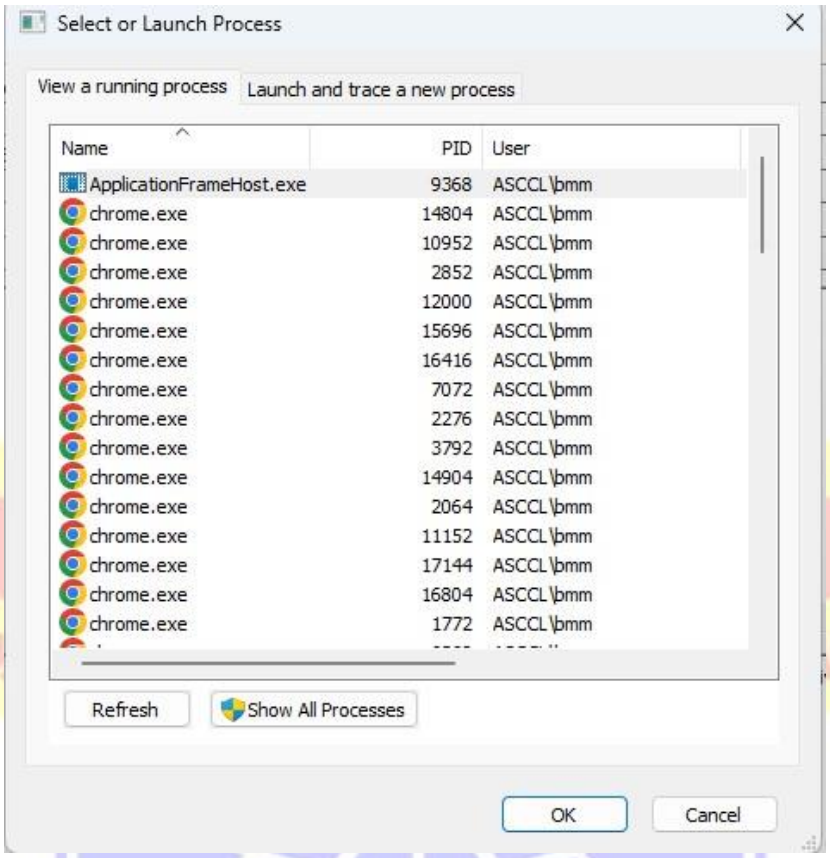
#	Time	Duration (s)	Disk	Request	Sector	Length
345	42.980874	0.00000000	1	Write	377607112	160
346	42.980944	0.00000000	1	Write	377481320	8
347	42.981136	0.00000000	1	Write	377481184	8
348	42.982512	0.00000000	0	Write	6104864	32
349	42.982624	0.00000000	0	Write	6102944	8
350	42.996067	0.00000000	0	Write	6102808	8
351	46.014710	0.00000000	1	Write	399863448	72
352	46.058413	0.00000000	1	Write	399589248	48
353	46.058442	0.00000000	1	Write	391426624	128
354	46.058714	0.00000000	1	Write	377481192	8
355	46.059206	0.00000000	1	Write	391426624	8
356	46.059389	0.00000000	1	Write	377481328	8
357	46.060474	0.00000000	1	Write	88806120	8
358	46.060509	0.00000000	1	Write	88806200	8
359	46.060598	0.00000000	1	Write	88806232	8
360	46.060707	0.00000000	1	Write	88806384	8
361	46.060842	0.00000000	1	Write	88806432	16
362	46.060890	0.00000000	1	Write	88806528	16
363	46.060918	0.00000000	1	Write	88806568	8
364	46.060950	0.00000000	1	Write	88806608	8
365	46.060986	0.00000000	1	Write	88806664	8
366	46.061018	0.00000000	1	Write	88806744	8
367	46.061050	0.00000000	1	Write	88806904	8
368	46.061078	0.00000000	1	Write	88806920	8
369	46.061110	0.00000000	1	Write	88807104	8
370	46.061142	0.00000000	1	Write	88807312	16
371	46.061171	0.00000000	1	Write	88807504	8
372	46.061203	0.00000000	1	Write	88807536	8
373	46.061232	0.00000000	1	Write	88807576	8
374	46.061264	0.00000000	1	Write	374822856	8
375	46.061312	0.00000000	1	Write	377481200	8
376	46.061651	0.00000000	1	Write	377481328	8
377	46.352349	0.00000000	1	Write	139327088	8
378	46.828643	0.00000000	1	Write	427564056	104
379	46.828838	0.00000000	1	Write	377481200	40
380	46.829600	0.00000000	1	Write	21384496	64
381	46.830454	0.00000000	1	Write	230977264	56
382	46.830467	0.00000000	1	Write	254829232	48
383	46.830592	0.00000000	1	Write	377481360	8

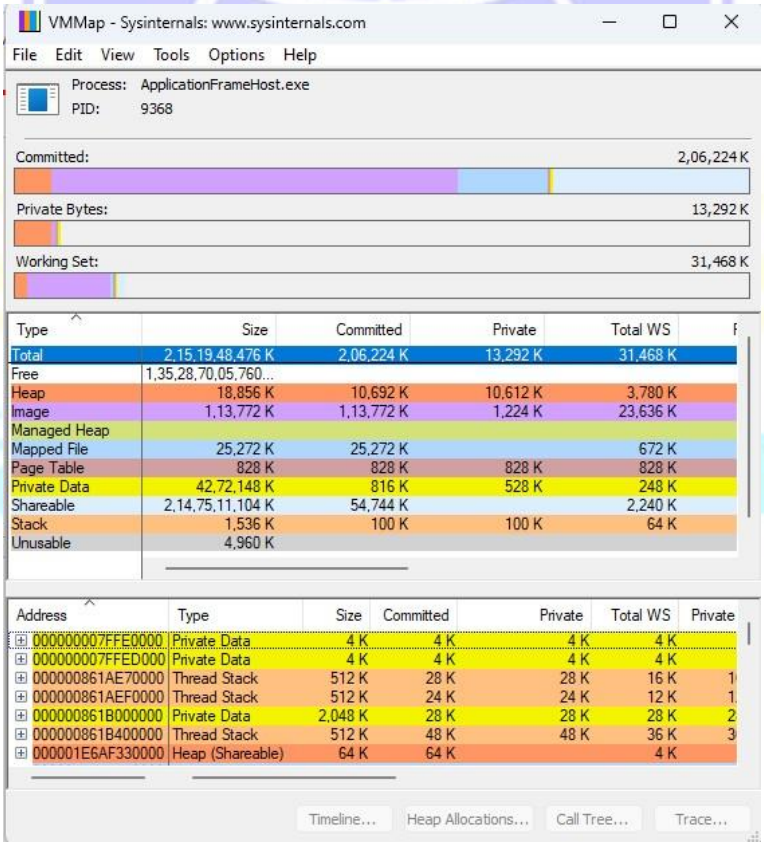
Monitor Virtual Memory

VMMap is a process virtual and physical memory analysis. It shows a breakdown of a process's committed virtual memory types as well as the amount of physical memory working set assigned by the operating system to those types.

STEPS

Sysinternal → VMMap

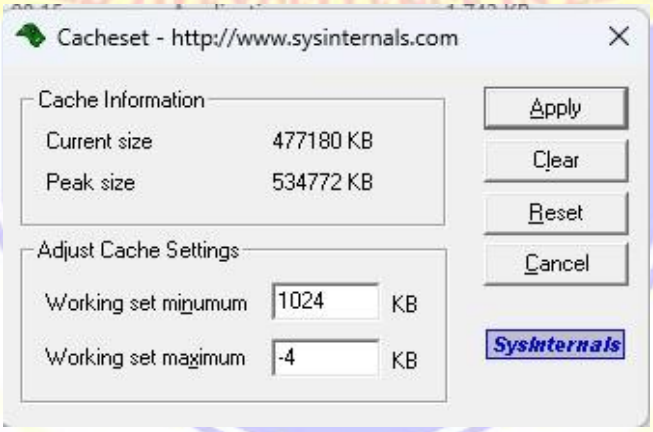

Select or Launch Process
View a running process
Launch and trace a new process
Name
PID
User
ApplicationFrameHost.exe 9368 ASCCL\bmm
chrome.exe 14804 ASCCL\bmm
chrome.exe 10952 ASCCL\bmm
chrome.exe 2852 ASCCL\bmm
chrome.exe 12000 ASCCL\bmm
chrome.exe 15696 ASCCL\bmm
chrome.exe 16416 ASCCL\bmm
chrome.exe 7072 ASCCL\bmm
chrome.exe 2276 ASCCL\bmm
chrome.exe 3792 ASCCL\bmm
chrome.exe 14904 ASCCL\bmm
chrome.exe 2064 ASCCL\bmm
chrome.exe 11152 ASCCL\bmm
chrome.exe 17144 ASCCL\bmm
chrome.exe 16804 ASCCL\bmm
chrome.exe 1772 ASCCL\bmm
Refresh
Show All Processes
OK
Cancel


VMMap - Sysinternals: www.sysinternals.com
File Edit View Tools Options Help
Process: ApplicationFrameHost.exe
PID: 9368
Committed: 2,06,224 K
Private Bytes: 13,292 K
Working Set: 31,468 K
Type Size Committed Private Total WS
Total 2,15,19,48,476 K 2,06,224 K 13,292 K 31,468 K
Free 1,35,28,70,05,760...
Heap 18,856 K 10,692 K 10,612 K 3,780 K
Image 1,13,772 K 1,13,772 K 1,224 K 23,636 K
Managed Heap
Mapped File 25,272 K 25,272 K 672 K
Page Table 828 K 828 K 828 K 828 K
Private Data 42,72,148 K 816 K 528 K 248 K
Shareable 2,14,75,11,104 K 54,744 K 2,240 K
Stack 1,536 K 100 K 100 K 64 K
Unusable 4,960 K
Address Type Size Committed Private Total WS Private
000000007FFE0000 Private Data 4 K 4 K 4 K 4 K
000000007FFED000 Private Data 4 K 4 K 4 K 4 K
000000861AE70000 Thread Stack 512 K 28 K 28 K 16 K
000000861AEF0000 Thread Stack 512 K 24 K 24 K 12 K
000000861B000000 Private Data 2,048 K 28 K 28 K 28 K
000000861B400000 Thread Stack 512 K 48 K 48 K 36 K
000001E6AF330000 Heap (Shareable) 64 K 64 K 4 K
Timeline... Heap Allocations... Call Tree... Trace...

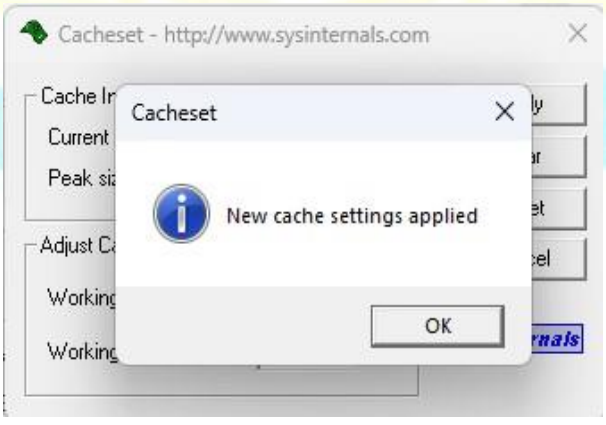
Monitor Cache Memory

CacheSet is an applet that allows you to manipulate the working the set parameters of the system file cahce. Unlike CacheMan, CacheSet runs on all versions and will work without modifications on new Service Pack releases.

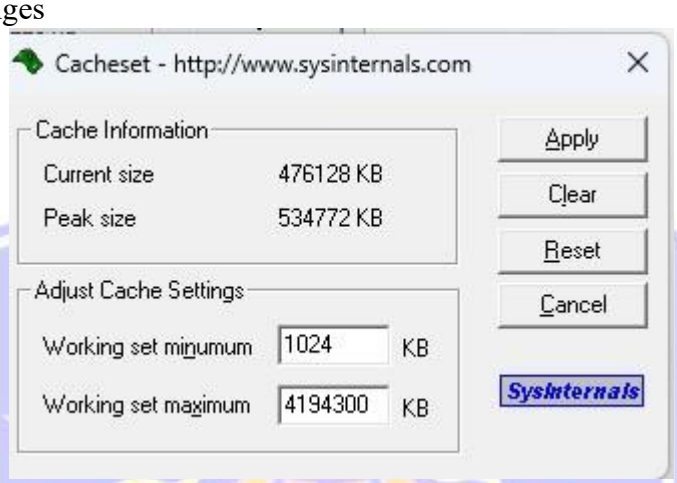
Give all the permissions and Click on Agree



Click on apply



After applying the changes



Result:

Using Sysinternals tools for network tracking and process monitoring enables real-time observation of system processes and network activity, crucial for identifying potential security threats and system performance issues.

Learning Outcomes:

- Understand how to use Sysinternals tools for monitoring live processes and network activity.
- Learn to capture RAM and TCP/UDP packets for analysis.
- Develop skills to monitor hard disk, virtual memory, and cache memory effectively.

Course Outcomes:

- Gain practical knowledge of using Sysinternals tools for system and network monitoring.
- Ability to track processes and capture network packets for forensic analysis.
- Apply monitoring techniques to identify and investigate system performance and security issues.

Conclusion:

Viva Questions:

1. What are Sysinternals tools, and how are they used in forensics?
2. How can you monitor live processes using Sysinternals?
3. What information can be captured from RAM and network packets?
4. Why is monitoring cache and virtual memory important in forensic investigations?

PRACTICAL NO: 6

Aim:

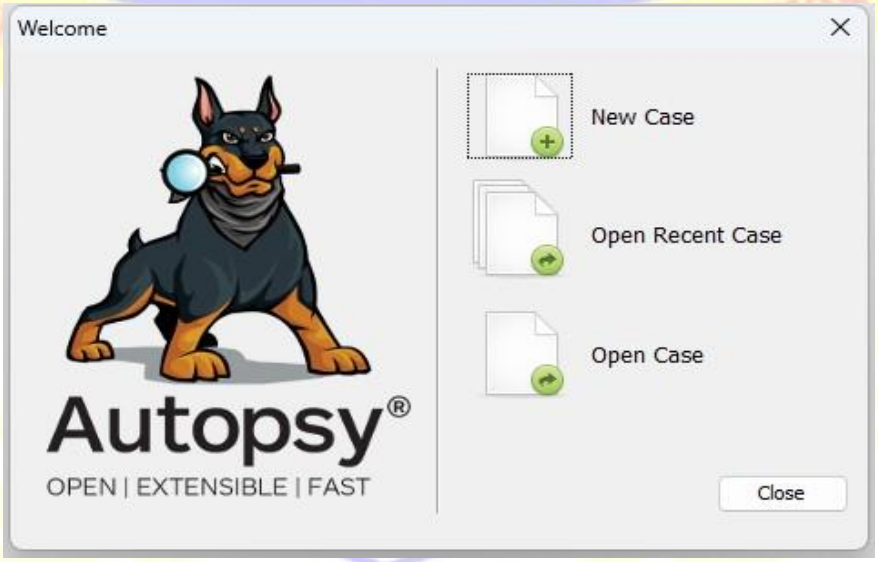
Recovering and Inspecting deleted files

- Check for Deleted Files
- Recover the Deleted Files
- Analyzing and Inspecting the recovered files
- Perform this using recovery option in ENCASE and also Perform manually through command line

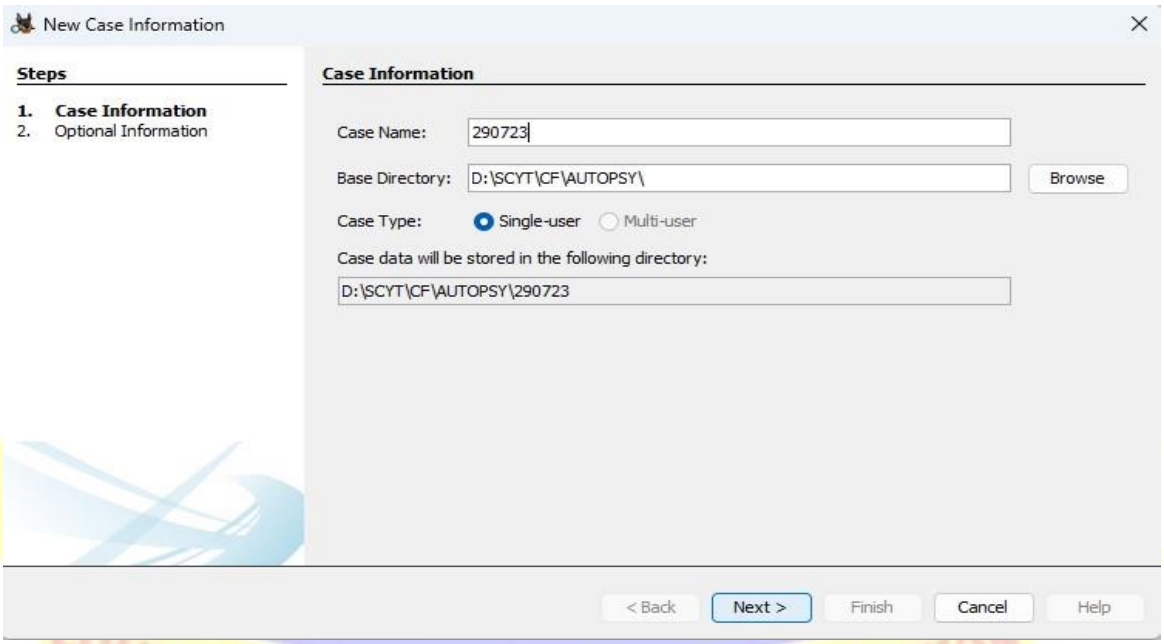
Practical:

In this Practical we are going to use the Autopsy, an application used to check, recover, analyze and inspect the deleted files using the Image evidence created

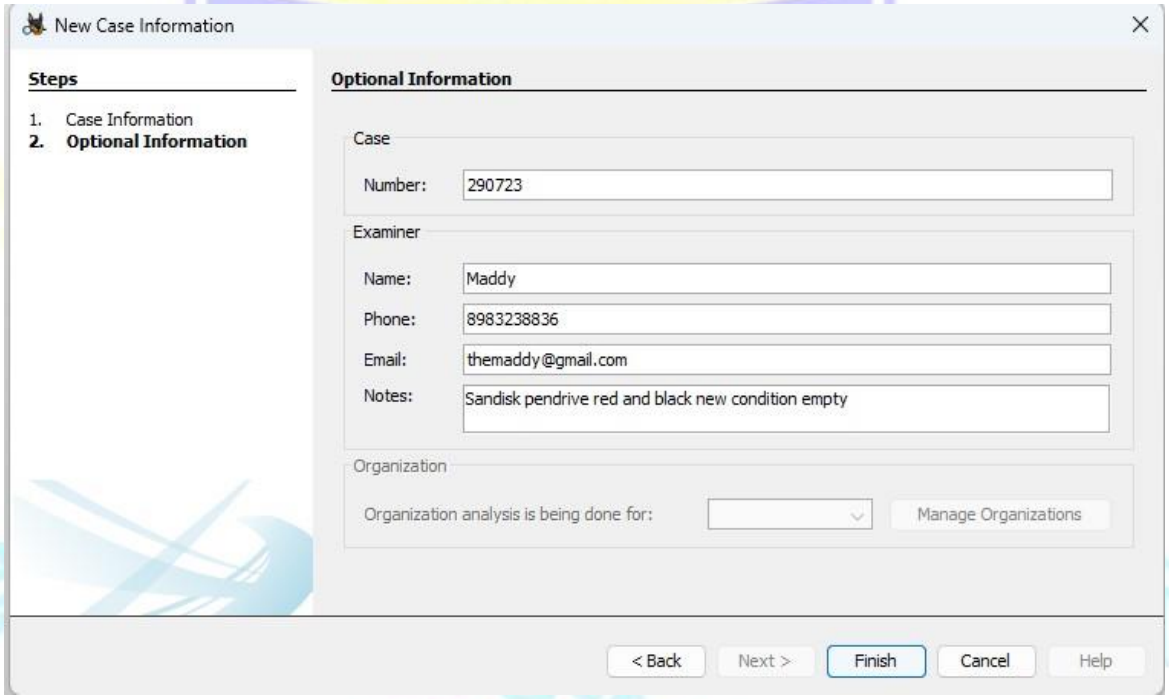
Open Autopsy and Click on New Case

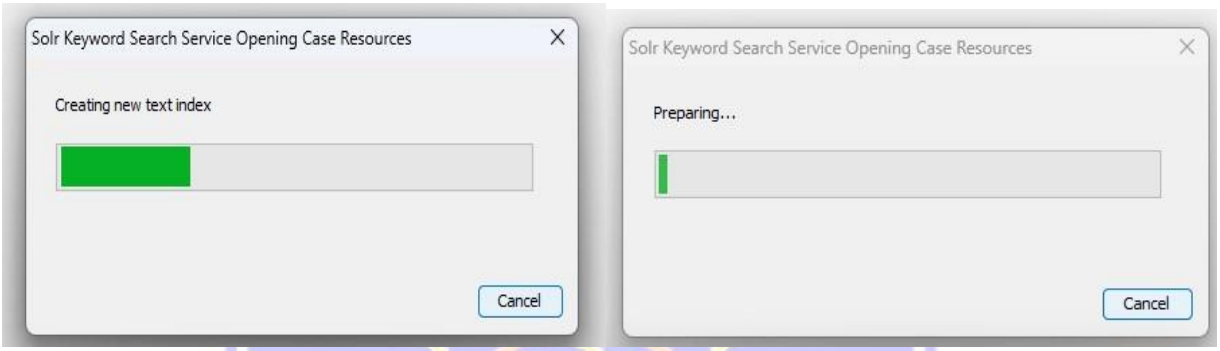


Give a case name and browse the destination to save the autopsy file

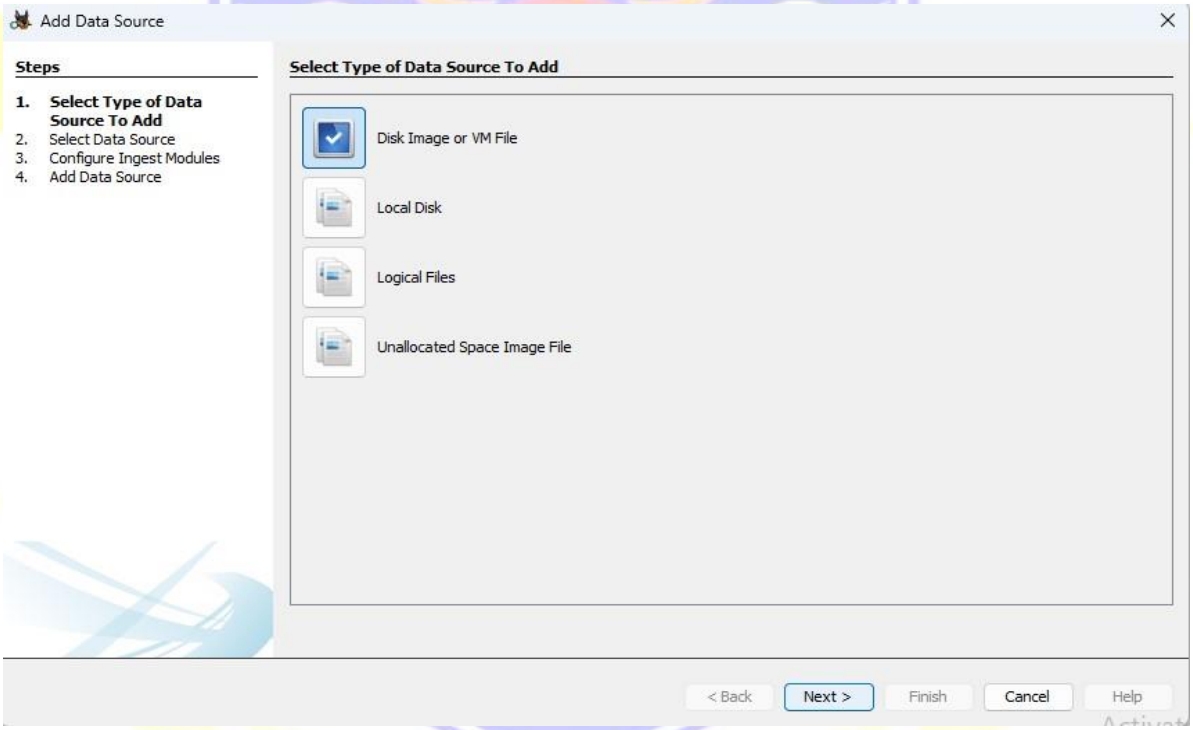


Then give the case number and the details as per the case number when performing the FTK Imager Practical 1

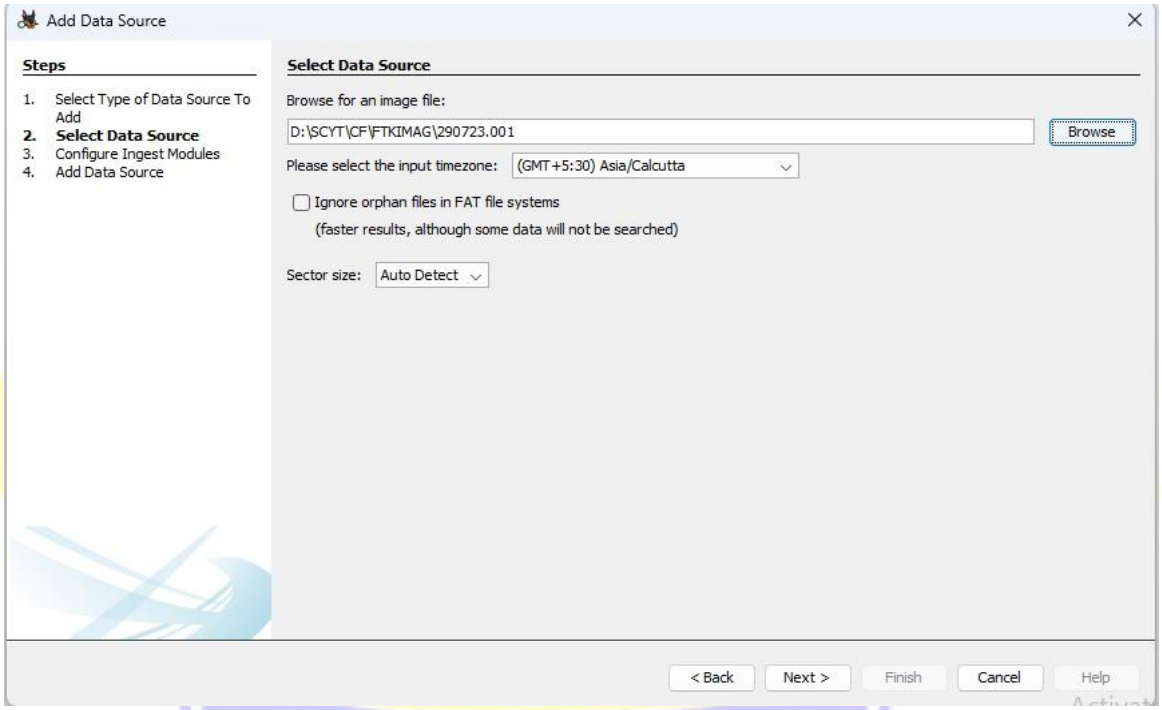




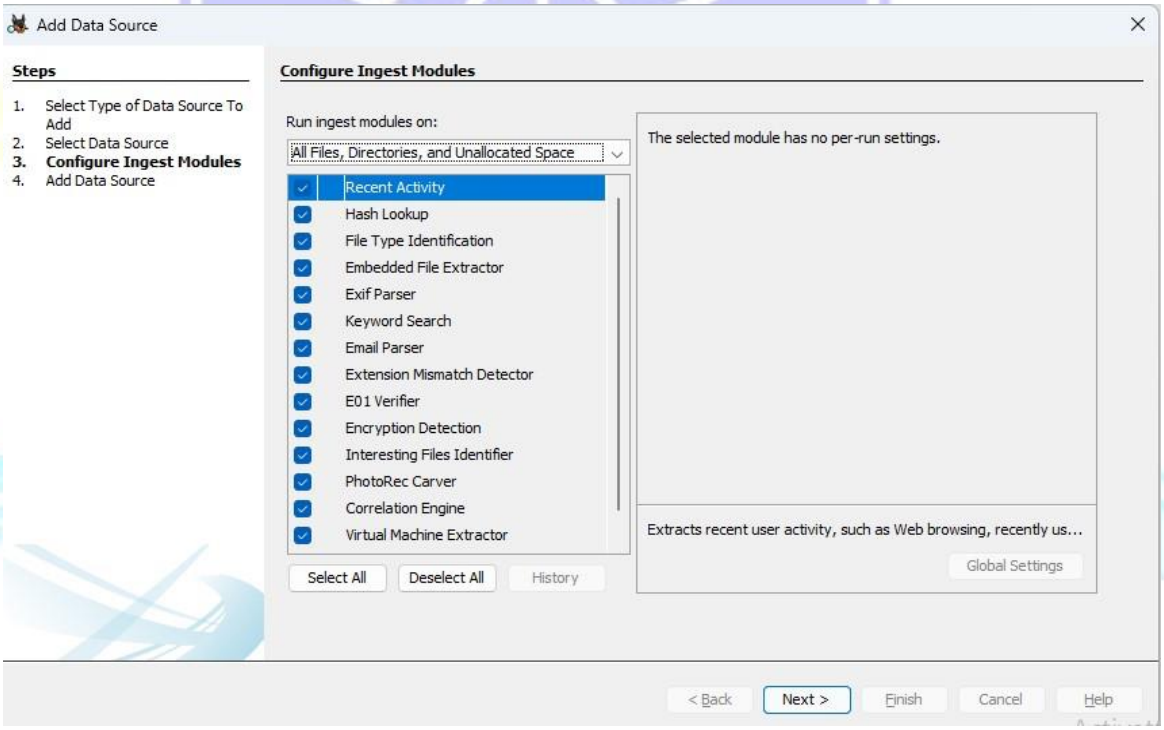
Select on Disk Image or VM File and Click Next



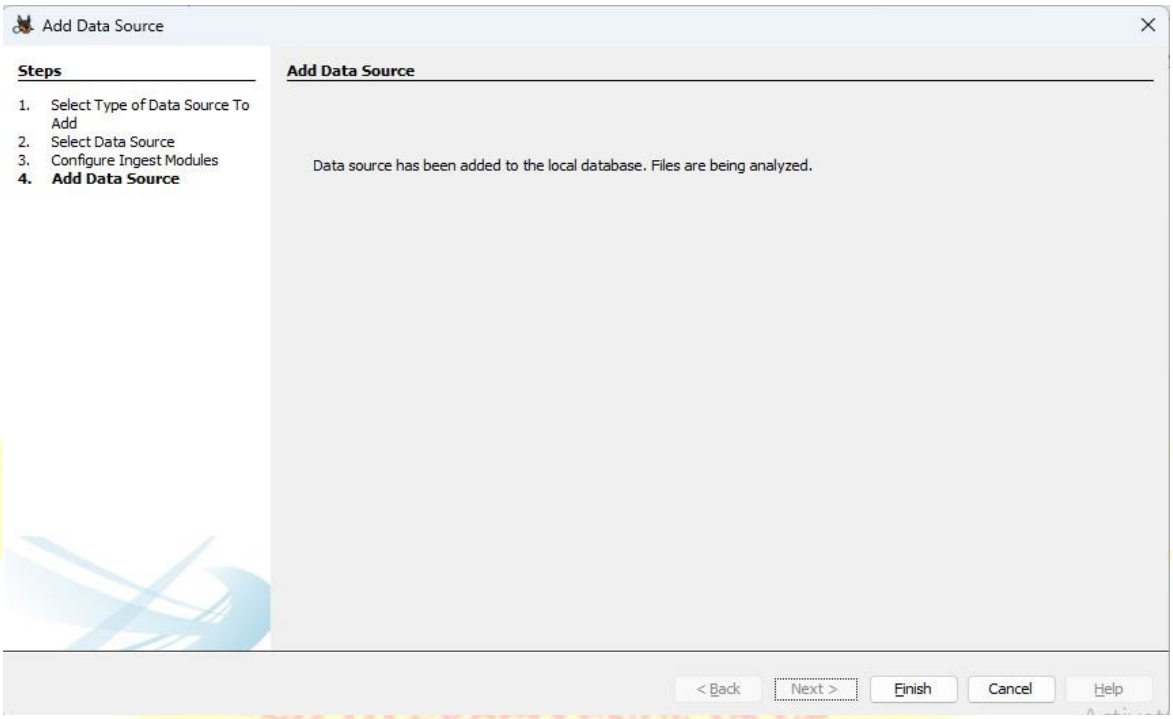
Give the destination of the image and click next



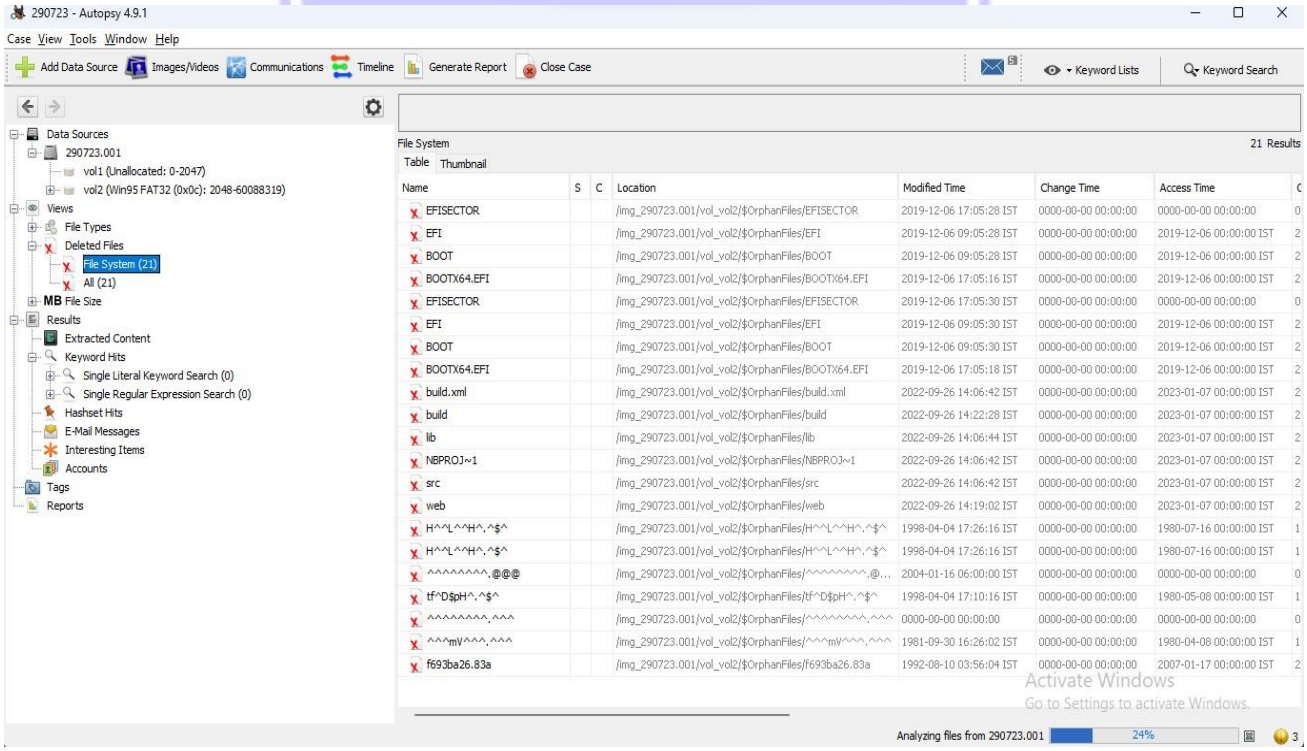
Select the ingest module and click next



See the acknowledgement and click finish

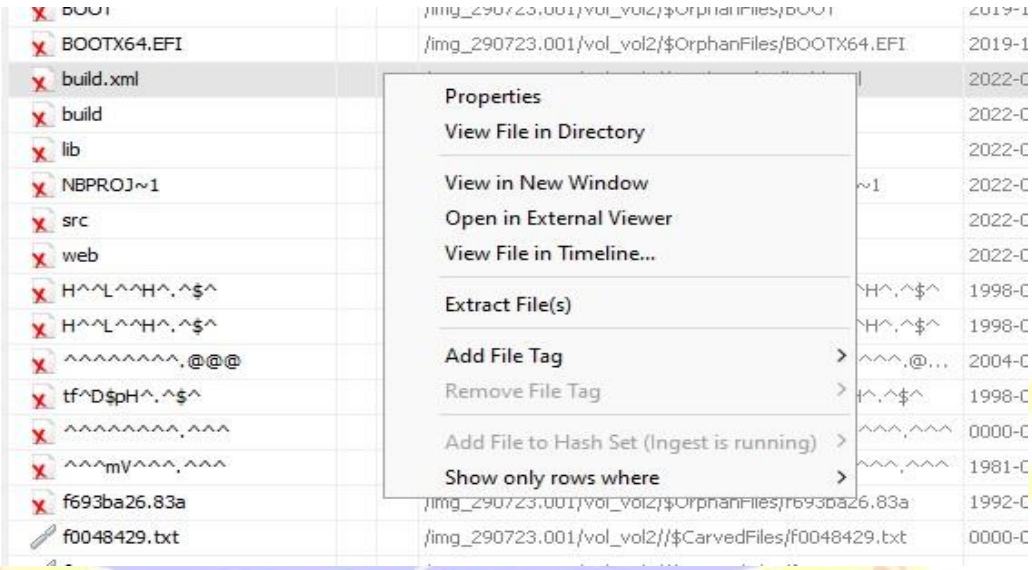


Now we check the files recovered

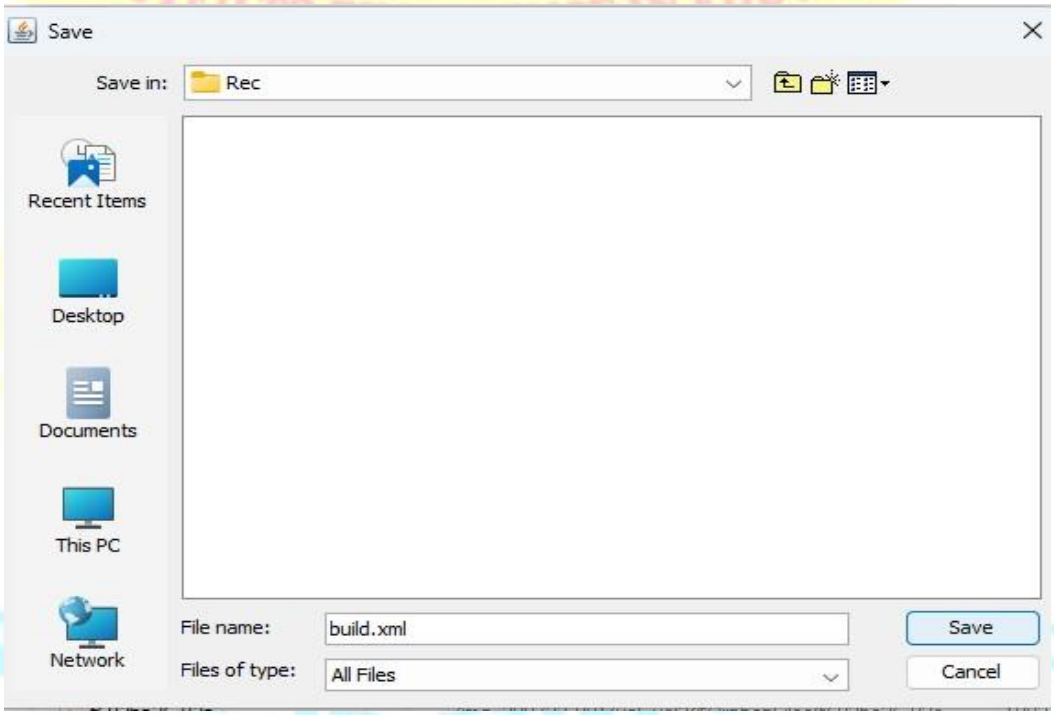


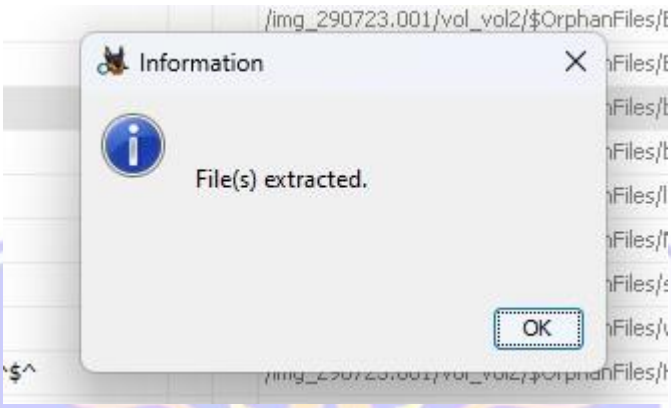
We see the Deleted Files

Now We Extract/Recover some deleted files

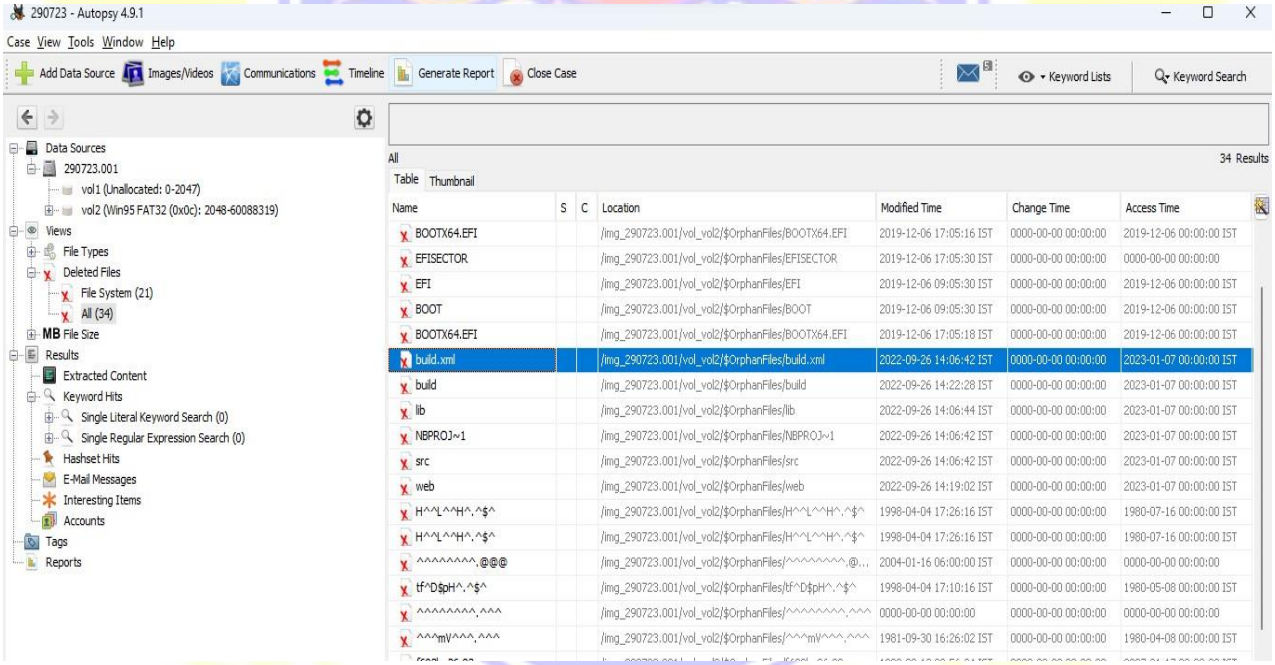


Set a directory for the recovered files

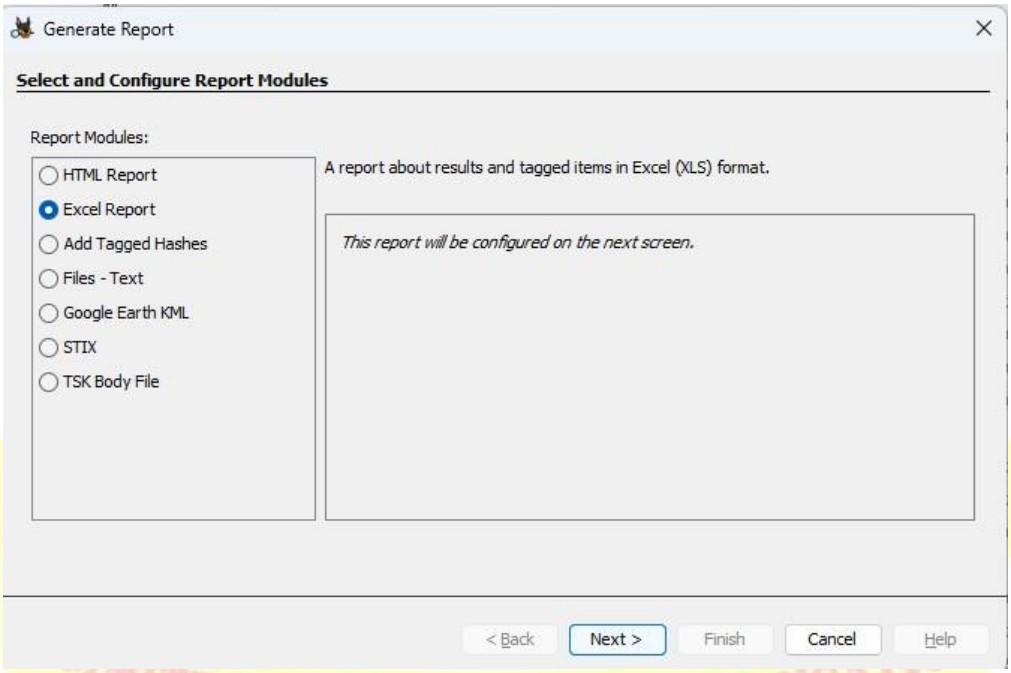




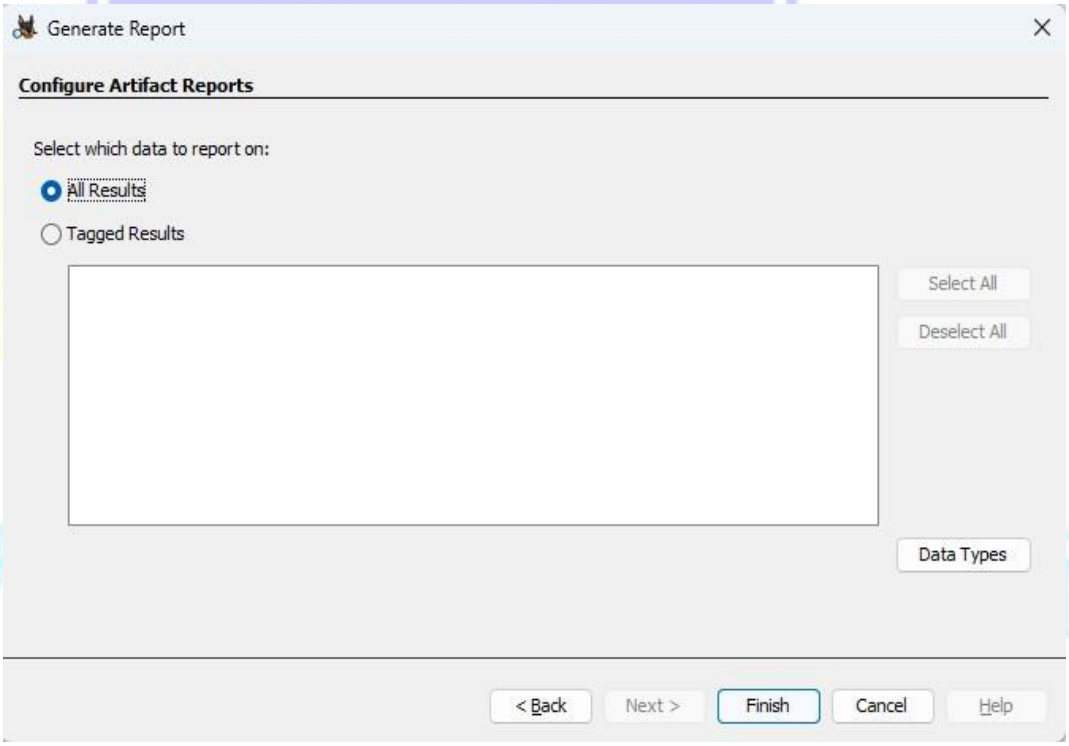
Now we Generate a Report of the Autopsy done

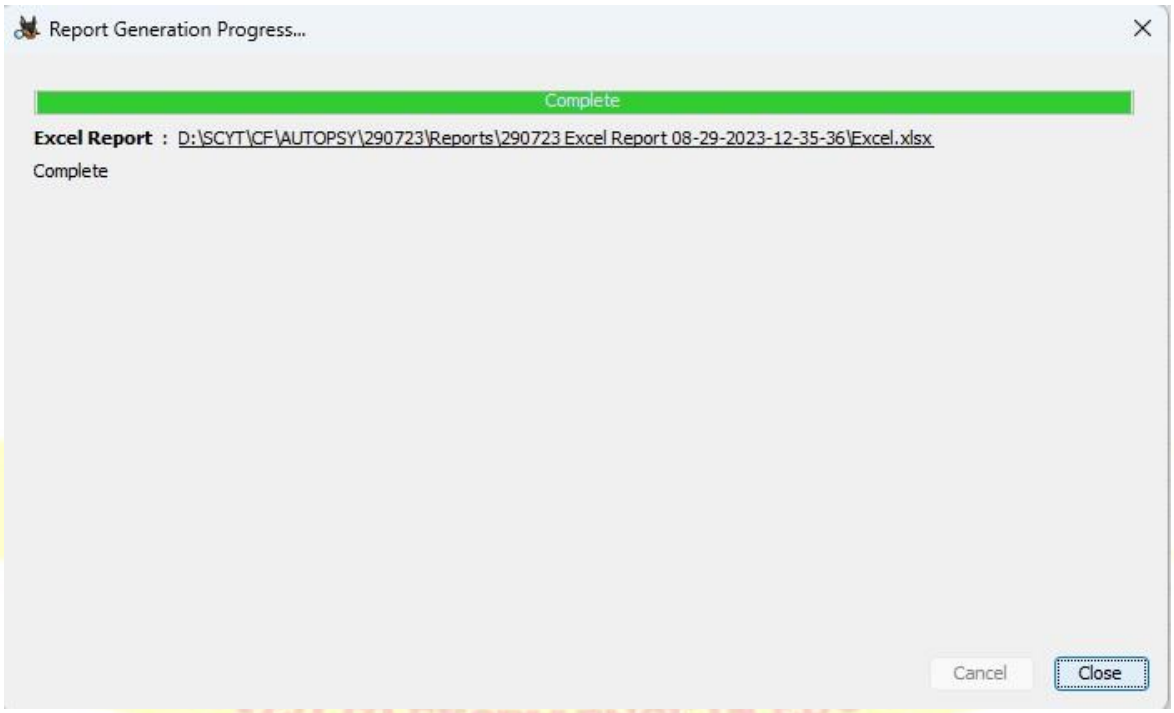


Select a type to store the data and click next. Here we are going to generate the report in Excel.

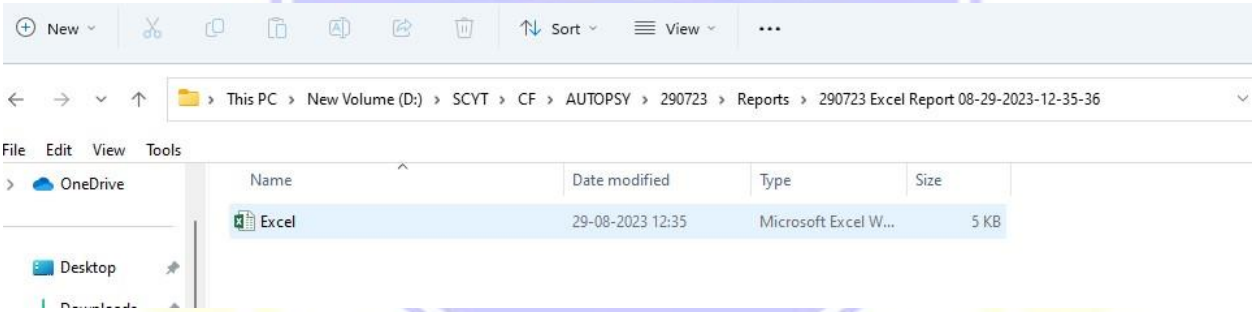


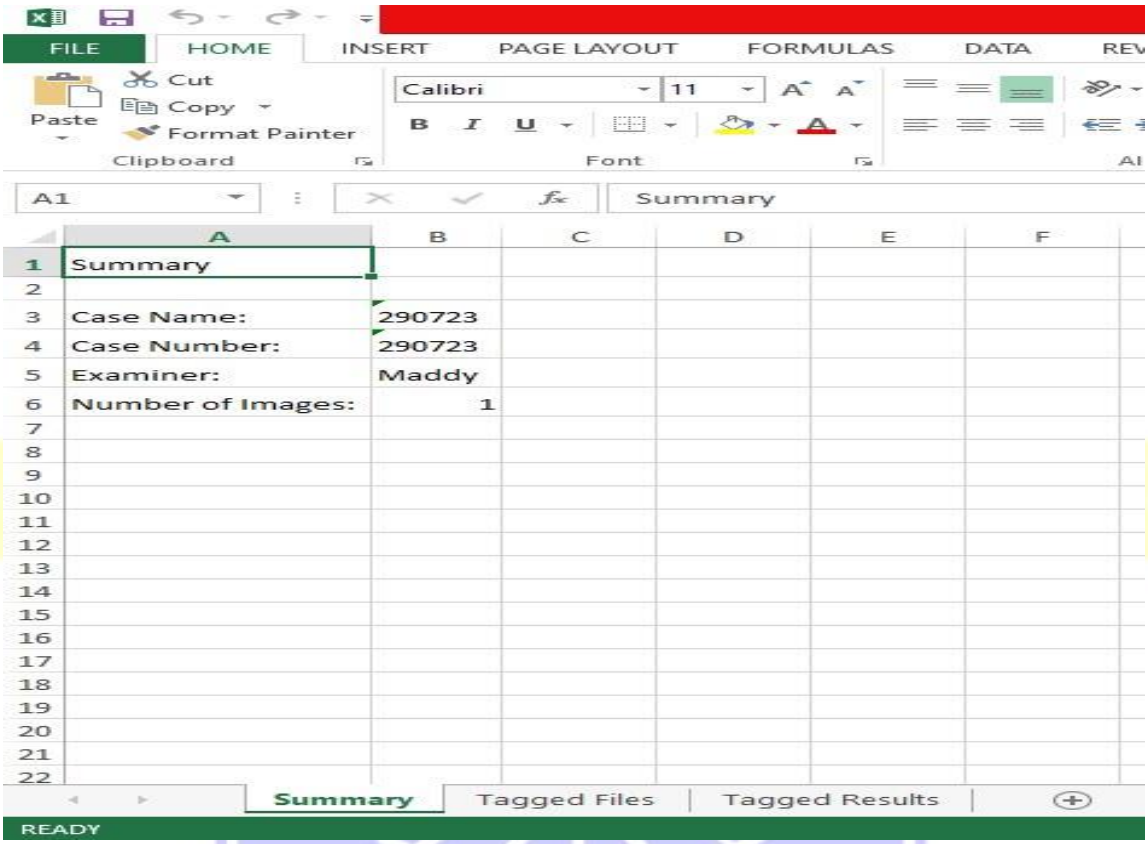
Now select all results this will generate all the reports and click finish. The other option only generate the report for tagged one only.





Click on close and open the excel from the directory it is stored





	A	B
1	Summary	
2		
3	Case Name:	290723
4	Case Number:	290723
5	Examiner:	Maddy
6	Number of Images:	1

Summary | Tagged Files | Tagged Results

READY

	A	B	C	D	E	F	G	H	I
1	Date Taken	Device Manufacturer	Device Model	Latitude	Longitude	Altitude	Source File	Tags	
2	2022-06-10 18:10:21 IST	realme	realme 6				/img_04092023_masood.001/vol_vol2/IMG20220610181021.jpg		
3	2022-06-10 18:10:27 IST	realme	realme 6				/img_04092023_masood.001/vol_vol2/IMG20220610181027.jpg		
4	2022-06-10 18:10:30 IST	realme	realme 6				/img_04092023_masood.001/vol_vol2/IMG20220610181030.jpg		
5	2022-06-10 18:10:34 IST	realme	realme 6				/img_04092023_masood.001/vol_vol2/IMG20220610181034.jpg		
6	2022-06-10 18:23:26 IST	realme	realme 6				/img_04092023_masood.001/vol_vol2//$CarvedFiles/f0000000.jpg		
7	2022-06-10 18:24:07 IST	realme	realme 6				/img_04092023_masood.001/vol_vol2//$CarvedFiles/f0005120.jpg		
8	2022-06-10 18:24:13 IST	realme	realme 6				/img_04092023_masood.001/vol_vol2//$CarvedFiles/f0012256.jpg		
9	2022-06-10 18:24:17 IST	realme	realme 6				/img_04092023_masood.001/vol_vol2//$CarvedFiles/f0016320.jpg		
10	2022-06-10 18:24:37 IST	realme	realme 6				/img_04092023_masood.001/vol_vol2//$CarvedFiles/f0020864.jpg		
11	2022-06-10 18:34:20 IST	realme	realme 6				/img_04092023_masood.001/vol_vol2/IMG20220610183420.jpg		
12	2022-06-10 18:34:25 IST	realme	realme 6				/img_04092023_masood.001/vol_vol2/IMG20220610183425.jpg		
13	2022-06-10 18:34:37 IST	realme	realme 6				/img_04092023_masood.001/vol_vol2/IMG20220610183437.jpg		
14	2022-06-10 18:34:53 IST	realme	realme 6				/img_04092023_masood.001/vol_vol2/IMG20220610183453.jpg		
15									
16									
17									

	A	B	C	D	E	F
1	E-Mail To	E-Mail From	Subject	Date Sent	Date Received	Path
2	'5amspade@myway.com'	Jim Shu: Jim_shu@comcast.net	RE: Bike spec's	2006-12-04 07:39:00 IST	2006-12-04 07:39:00 IST	\\Top of Personal Folders\Sent Items
3	'5amspade@myway.com'	Jim Shu: Jim_shu@comcast.net	RE: Bike spec's	2006-12-04 07:39:00 IST	2006-12-04 07:39:00 IST	\\Top of Personal Folders\Sent Items
4	'5amspade@myway.com'	Jim Shu: Jim_shu@comcast.net	RE: Bike spec's	2006-12-04 08:37:00 IST	2006-12-04 08:37:00 IST	\\Top of Personal Folders\Deleted Items
5	'5amspade@myway.com'	Jim Shu: Jim_shu@comcast.net	RE: Bike spec's	2006-12-04 08:37:00 IST	2006-12-04 08:37:00 IST	\\Top of Personal Folders\Deleted Items
6	'baspen99@aol.com'	Jim Shu: Jim_shu@comcast.net	RE: Waiting	2006-12-07 07:51:00 IST	2006-12-07 07:51:00 IST	\\Top of Personal Folders\Sent Items
7	'baspen99@aol.com'	Jim Shu: Jim_shu@comcast.net	RE: Waiting	2006-12-07 07:51:00 IST	2006-12-07 07:51:00 IST	\\Top of Personal Folders\Sent Items
8	'jim_shu1@yahoo.com'	Jim Shu: Jim_shu@comcast.net	FW: Activate your account	2006-12-08 05:08:00 IST	2006-12-08 05:08:00 IST	\\Top of Personal Folders\Sent Items
9	'jim_shu1@yahoo.com'	Jim Shu: Jim_shu@comcast.net	FW: Activate your account	2006-12-08 05:08:00 IST	2006-12-08 05:08:00 IST	\\Top of Personal Folders\Sent Items
10	'jim_shu1@yahoo.com'	Jim Shu: Jim_shu@comcast.net	FW: Bicycle offer	2006-12-08 05:07:00 IST	2006-12-08 05:07:00 IST	\\Top of Personal Folders\Sent Items
11	'jim_shu1@yahoo.com'	Jim Shu: Jim_shu@comcast.net	FW: Bicycle offer	2006-12-08 05:07:00 IST	2006-12-08 05:07:00 IST	\\Top of Personal Folders\Sent Items
12	'jim_shu1@yahoo.com'	Jim Shu: Jim_shu@comcast.net	FW: Bicycle offer	2006-12-08 05:08:00 IST	2006-12-08 05:08:00 IST	\\Top of Personal Folders\Sent Items
13	'jim_shu1@yahoo.com'	Jim Shu: Jim_shu@comcast.net	FW: Bicycle offer	2006-12-08 05:08:00 IST	2006-12-08 05:08:00 IST	\\Top of Personal Folders\Sent Items
14	'jim_shu1@yahoo.com'	Jim Shu: Jim_shu@comcast.net	FW: Bicycle offer	2006-12-08 05:08:00 IST	2006-12-08 05:08:00 IST	\\Top of Personal Folders\Sent Items
15	'jim_shu1@yahoo.com'	Jim Shu: Jim_shu@comcast.net	FW: Bicycle offer	2006-12-08 05:08:00 IST	2006-12-08 05:08:00 IST	\\Top of Personal Folders\Sent Items
16	'jim_shu1@yahoo.com'	Jim Shu: Jim_shu@comcast.net	FW: Bicycle offer	2006-12-08 05:09:00 IST	2006-12-08 05:09:00 IST	\\Top of Personal Folders\Sent Items
17	'jim_shu1@yahoo.com'	Jim Shu: Jim_shu@comcast.net	FW: Bicycle offer	2006-12-08 05:09:00 IST	2006-12-08 05:09:00 IST	\\Top of Personal Folders\Sent Items
18	'jim_shu1@yahoo.com'	Jim Shu: Jim_shu@comcast.net	FW: Bike spec's	2006-12-08 05:07:00 IST	2006-12-08 05:07:00 IST	\\Top of Personal Folders\Sent Items
19	'jim_shu1@yahoo.com'	Jim Shu: Jim_shu@comcast.net	FW: Bike spec's	2006-12-08 05:07:00 IST	2006-12-08 05:07:00 IST	\\Top of Personal Folders\Sent Items
20	'jim_shu1@yahoo.com'	Jim Shu: Jim_shu@comcast.net	FW: Bike spec's	2006-12-08 05:08:00 IST	2006-12-08 05:08:00 IST	\\Top of Personal Folders\Sent Items
21	'jim_shu1@yahoo.com'	Jim Shu: Jim_shu@comcast.net	FW: Bike spec's	2006-12-08 05:08:00 IST	2006-12-08 05:08:00 IST	\\Top of Personal Folders\Sent Items
22	'jim_shu1@yahoo.com'	Jim Shu: Jim_shu@comcast.net	FW: Bike spec's	2006-12-08 05:09:00 IST	2006-12-08 05:09:00 IST	\\Top of Personal Folders\Sent Items
23	'jim_shu1@yahoo.com'	Jim Shu: Jim_shu@comcast.net	FW: Bike spec's	2006-12-08 05:09:00 IST	2006-12-08 05:09:00 IST	\\Top of Personal Folders\Sent Items

Summary | EXIF Metadata | E-Mail Messages | Keyword Hits | Accounts - Email | Extension Misc ...

	A	B	C
1	Email Addresses		
2	%@clients.l.google.com		
3	Preview	Source File	Tags
4	lients.l.google.com«%@clients.l.google.com«%hclients.l.google.	/img_04092023_masood.001/vol_vol2//$Unalloc/Unalloc_1878_3915776_1077723136	
5	lients.l.google.com«%@clients.l.google.com«%hclients.l.google.	/img_04092023_masood.001/vol_vol2/$OrphanFiles/_LLPLA~1.PCA	
6	lients.l.google.com«%@clients.l.google.com«%hclients.l.google.	/img_04092023_masood.001/vol_vol2/$OrphanFiles/_ROTEU~1.EXE	
7	lients.l.google.com«%@clients.l.google.com«%hclients.l.google.	/img_04092023_masood.001/vol_vol2/$OrphanFiles/aftnndbn.umd	
8			
9	-239034676-0-1001@flonetwork.com		
10	Preview	Source File	Tags
11	jjjz4znt«-239034676-0-1001@flonetwork.com«>[work.com>[4676-0	/img_04092023_masood.001/vol_vol2//$Unalloc/Unalloc_1878_3915776_1077723136	
12	jjjz4znt«-239034676-0-1001@flonetwork.com«>[work.com>[4676-0	/img_04092023_masood.001/vol_vol2/_S/Proteus 8.11 SP0 Pro HomeMade Electronics.exe	
13			
14	200612032123.609457386a225c@rly-xm04.mx.aol.com		
15	Preview	Source File	Tags
16	-0500in-reply-to: <«200612032123.609457386a225c@rly-xm04.mx.aol.com«>x-mb-message-sourc	/img_04092023_masood.001/vol_vol2//$Unalloc/Unalloc_1878_3915776_1077723136	
17	-0500in-reply-to: <«200612032123.609457386a225c@rly-xm04.mx.aol.com«>x-mb-message-sourc	/img_04092023_masood.001/vol_vol2/_S/Proteus 8.11 SP0 Pro HomeMade Electronics.exe	
18			
19	20061204013940.a88906765f@mprdmxin.myway.com		
20	Preview	Source File	Tags
21	etmail.comcast.net<«20061204013940.a88906765f@mprdmxin.myway.com«>mail.comcast.net000	/img_04092023_masood.001/vol_vol2//$Unalloc/Unalloc_1878_3915776_1077723136	
22	7bitmessage-id: <«20061204013940.a88906765f@mprdmxin.myway.com«>date: sun, 3 dec	/img_04092023_masood.001/vol_vol2//$CarvedFiles/f0333408.pst	

Summary | EXIF Metadata | E-Mail Messages | Keyword Hits | Accounts - Email | Extension Misc ...

	A	B	C	D
1	Review Status	ID	Tags	
2	Undecided	5amspade@myway.com		
3	Undecided	5amspade@myway.com		
4	Undecided	baspen99@aol.com		
5	Undecided	baspen99@aol.com		
6	Undecided	jim_shu1@yahoo.com		
7	Undecided	jim_shu1@yahoo.com		
8	Undecided	jim_shu@comcast.net		
9	Undecided	jim_shu@comcast.net		
10	Undecided	martha.dax@superiorbicycles.biz		
11	Undecided	martha.dax@superiorbicycles.biz		
12	Undecided	terrysadler@goowy.com		
13	Undecided	terrysadler@goowy.com		
14				

A1 | File

	A	B	C	D
1	File	Extension	MIME Type	Path
2	AC19.gpj	gpj	image/jpeg	/img_04092023_masood.001/vol_vol2/$OrphanFiles/_IM_SH~1.PST/AC19.gpj
3	AC19.gpj	gpj	image/jpeg	/img_04092023_masood.001/vol_vol2//$CarvedFiles/f0333408.pst/AC19.gpj
4				
5				

Result:

Recovering and inspecting deleted files allows forensic investigators to retrieve potentially valuable evidence that may have been removed from the file system, which is crucial for building a case.

Learning Outcomes:

- Understand how to check for and recover deleted files using forensic tools.
- Learn to analyze and inspect recovered files for relevant information.
- Develop skills to perform file recovery manually through command line and using ENCASE.

Course Outcomes:

- Gain practical knowledge of file recovery techniques in digital forensics.
- Ability to inspect and analyze deleted files to identify critical evidence.
- Apply various recovery methods to retrieve deleted data effectively.

Conclusion:

Viva Questions:

1. What methods can be used to recover deleted files in forensics?
2. How does ENCASE facilitate the recovery of deleted files?
3. What is the significance of inspecting recovered files?
4. Can you explain the command-line process for file recovery?

PRACTICAL NO: 7

Aim:

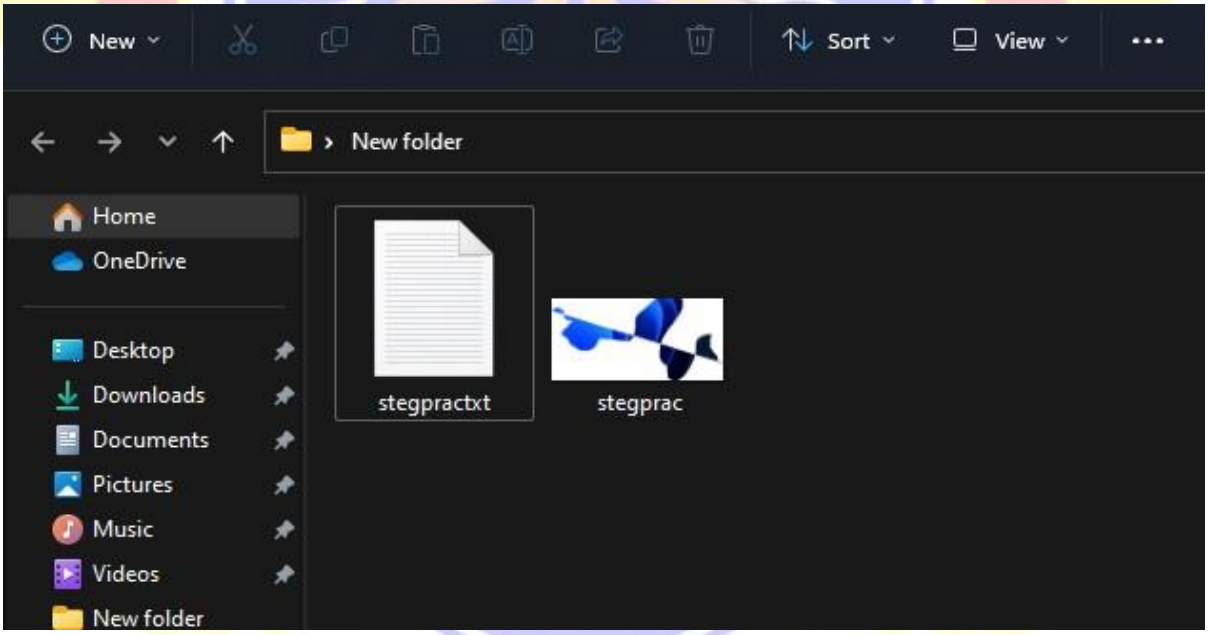
Steganography Detection

- Detect hidden information or files within digital images using steganography analysis tools.
- Extract and examine the hidden content.

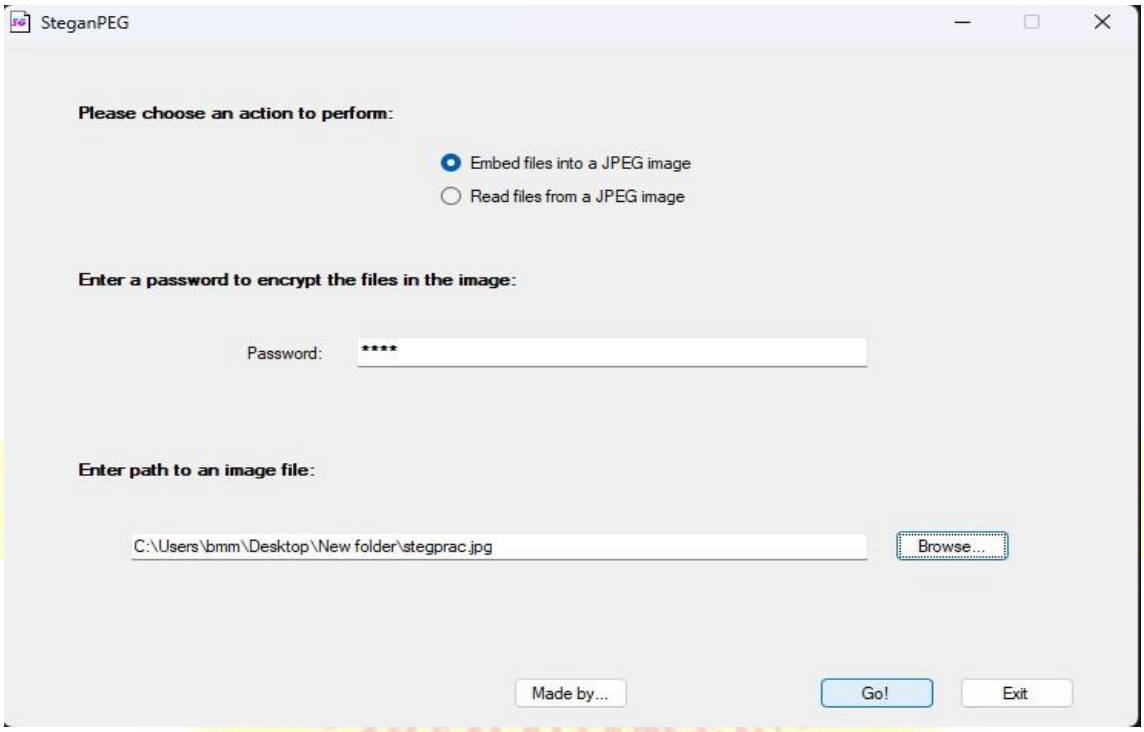
Practical:

In this Practical we are going to use the **SteganPEG** to check the hidden files in the given Image

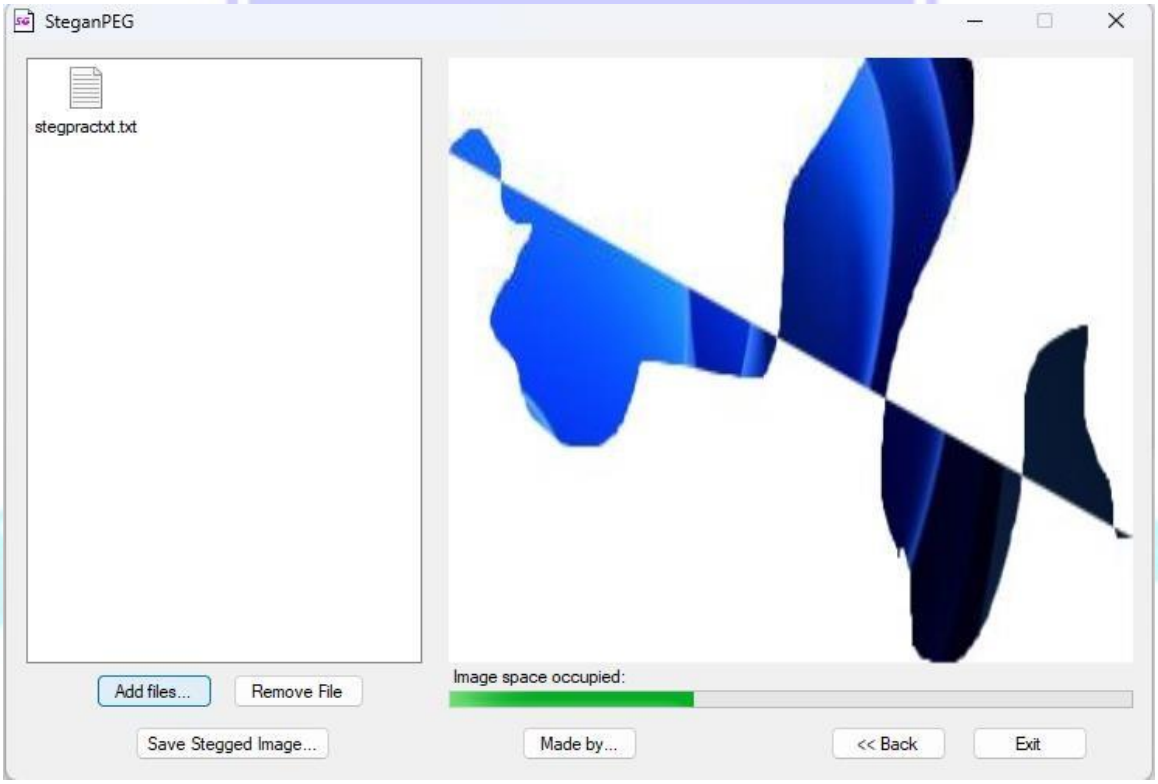
Create a folder to keep the image and message file and store the txt file and image



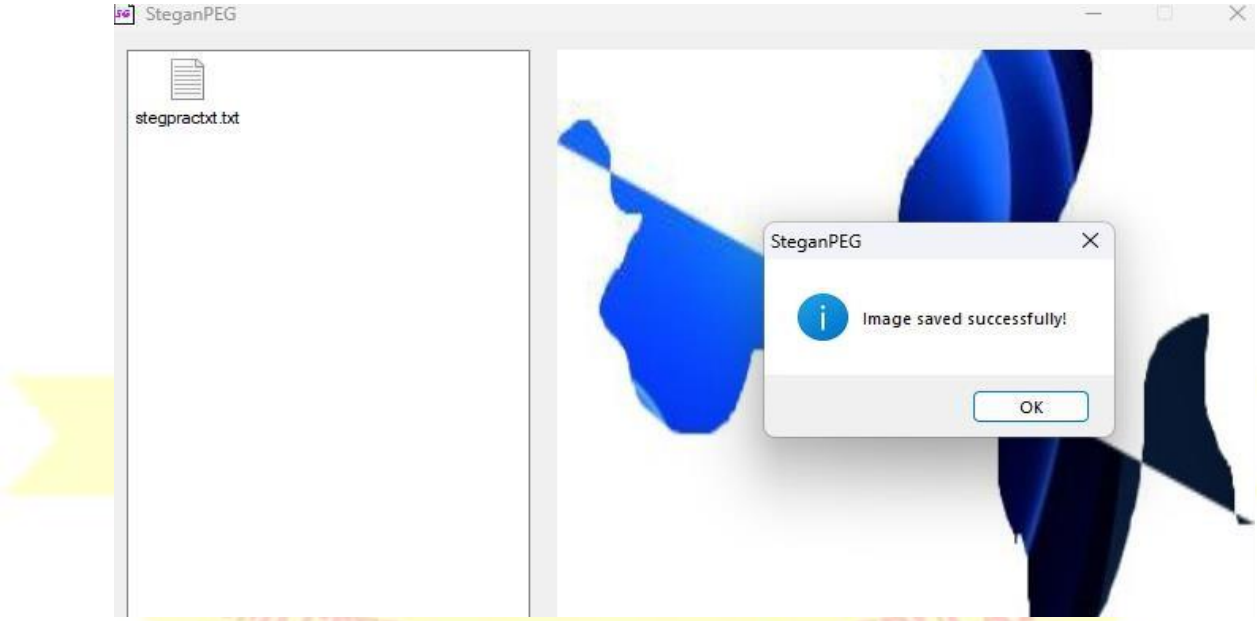
Open the SteganPEG and give a password and browse the path of the image



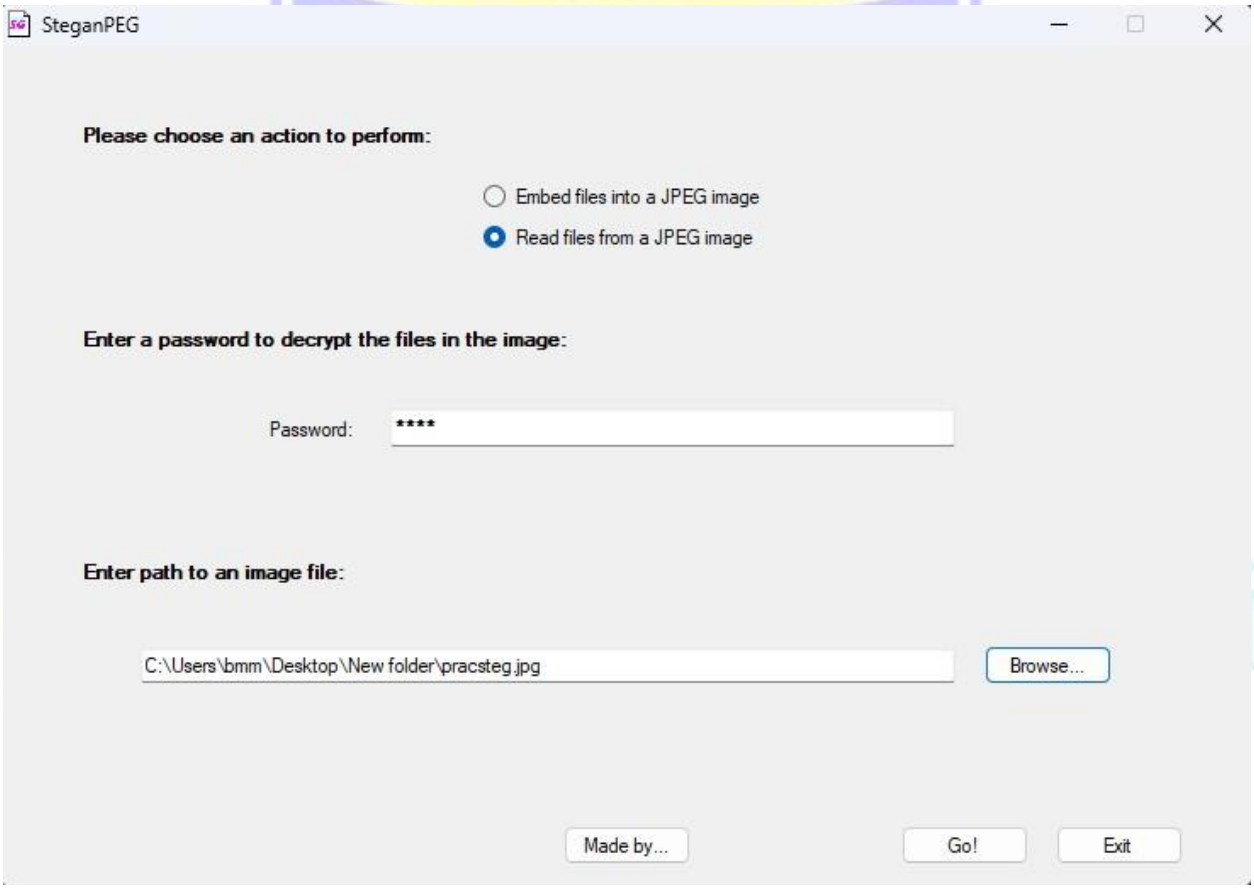
First we are going to add some files in the captured image

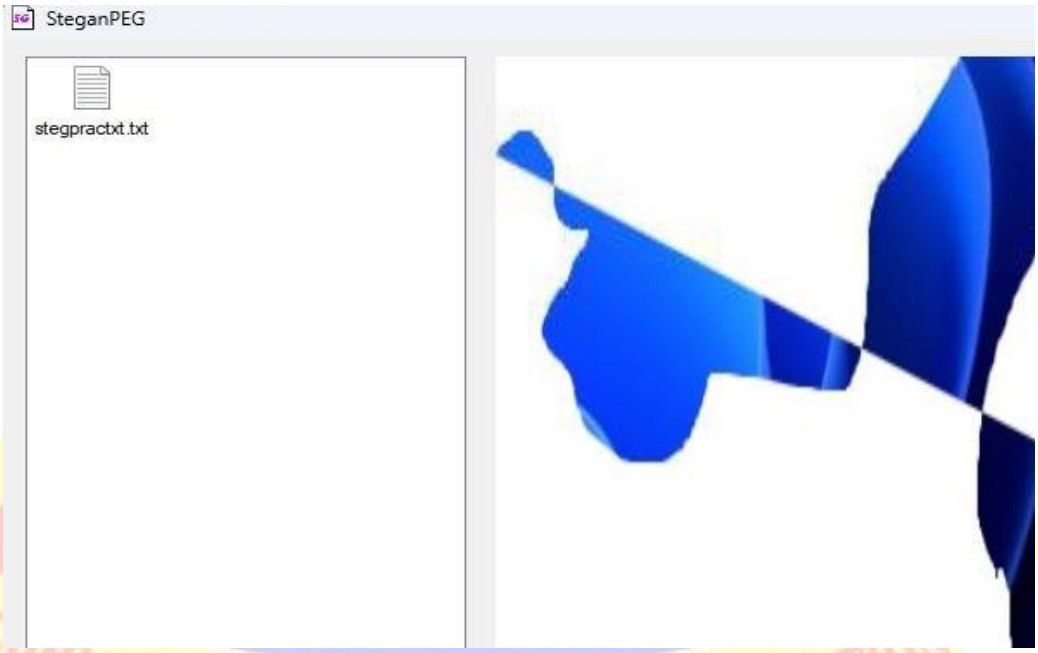


Save the stegged image



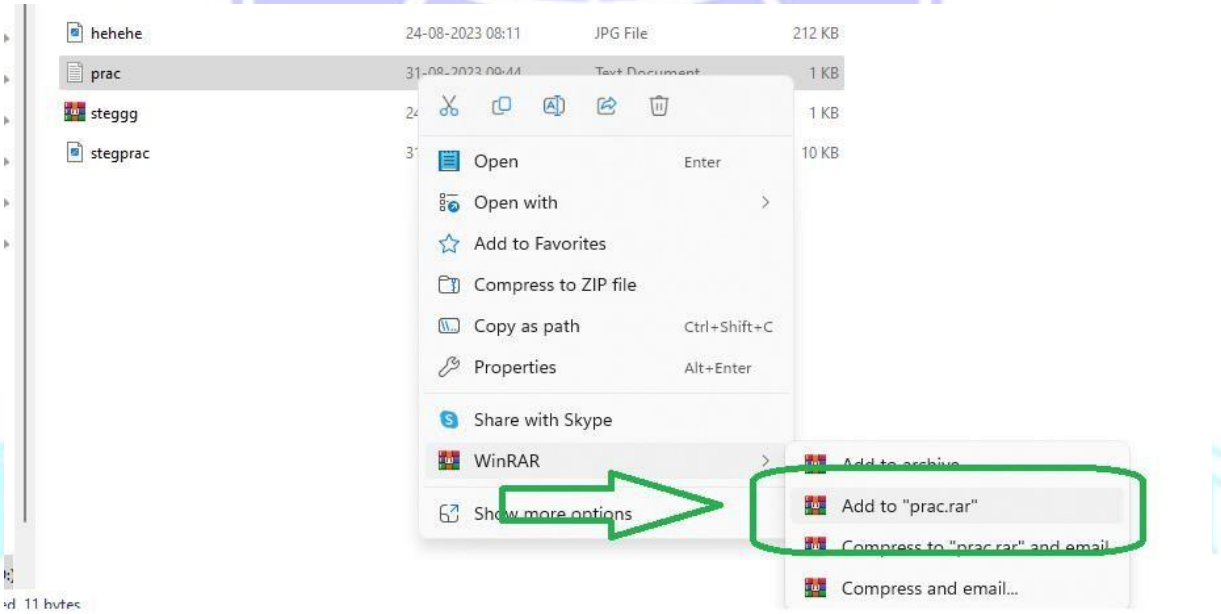
Open the saved image with the assigned password and view the image with hidden files





Now we are going to do the **stegging process** using **Command Prompt** and **viewing** the Image using the
WinRAR

Make a zip file of the text file



Go to **Command Prompt** and **Type** the **Syntax**

C:\Users\bmm\Desktop\New Folder>copy/b stegprac.jpg + stegpractxt.rar

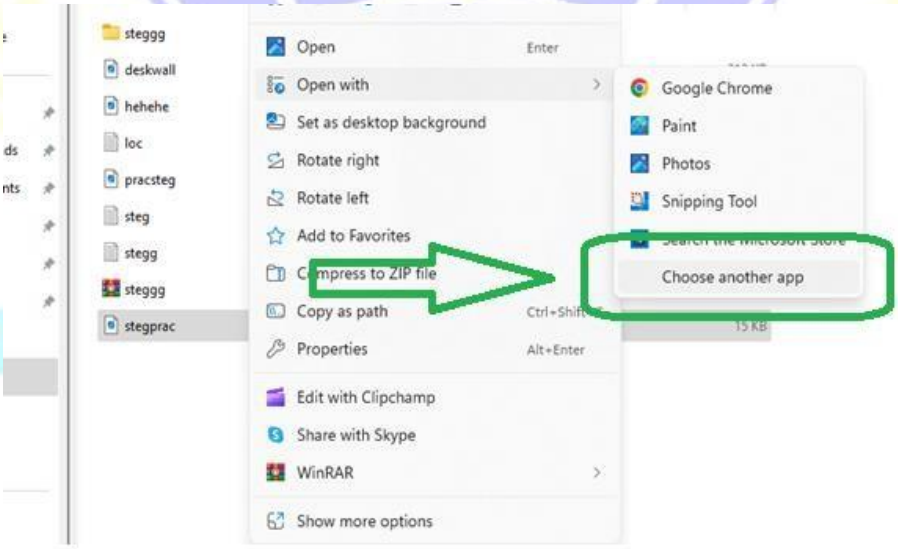
```
D:\SCYT\CF\STEG>copy /b stegprac.jpg + prac.rar
stegprac.jpg
prac.rar
        1 file(s) copied.

D:\SCYT\CF\STEG>
```

Then create a shortcut for WinRAR on the desktop

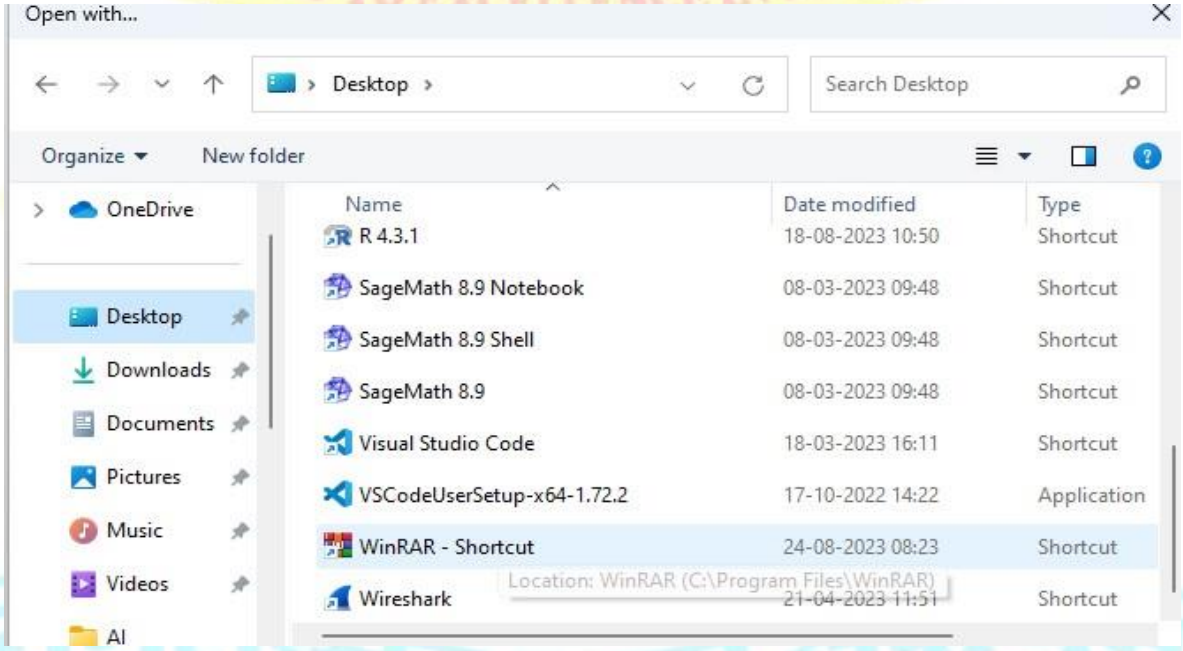
Then open the image using the shortcut

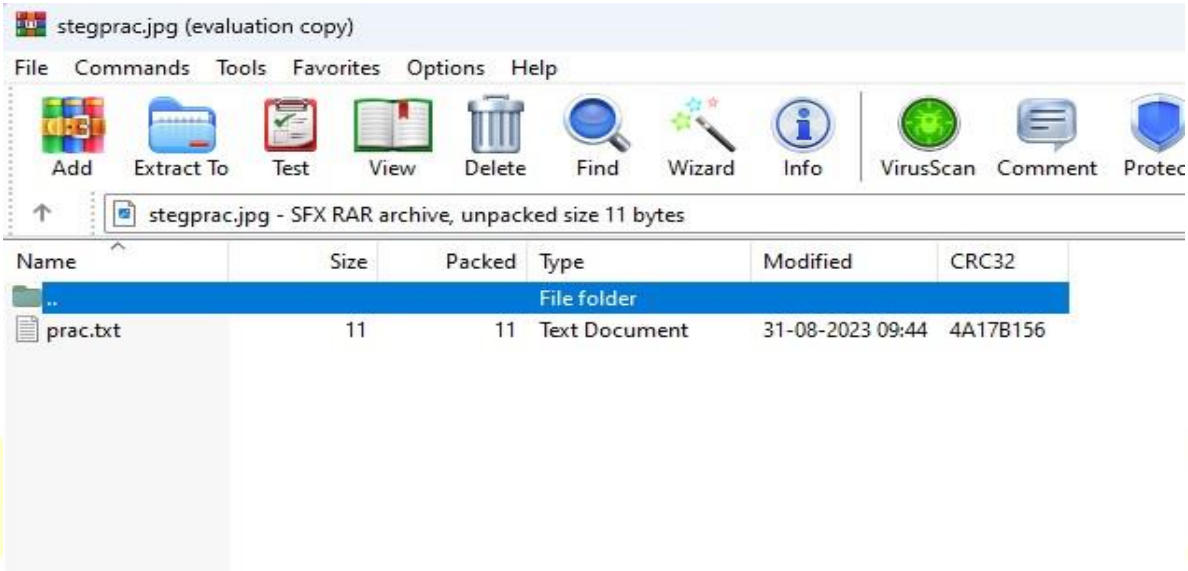
Right Click on the image → Open with → Choose another app



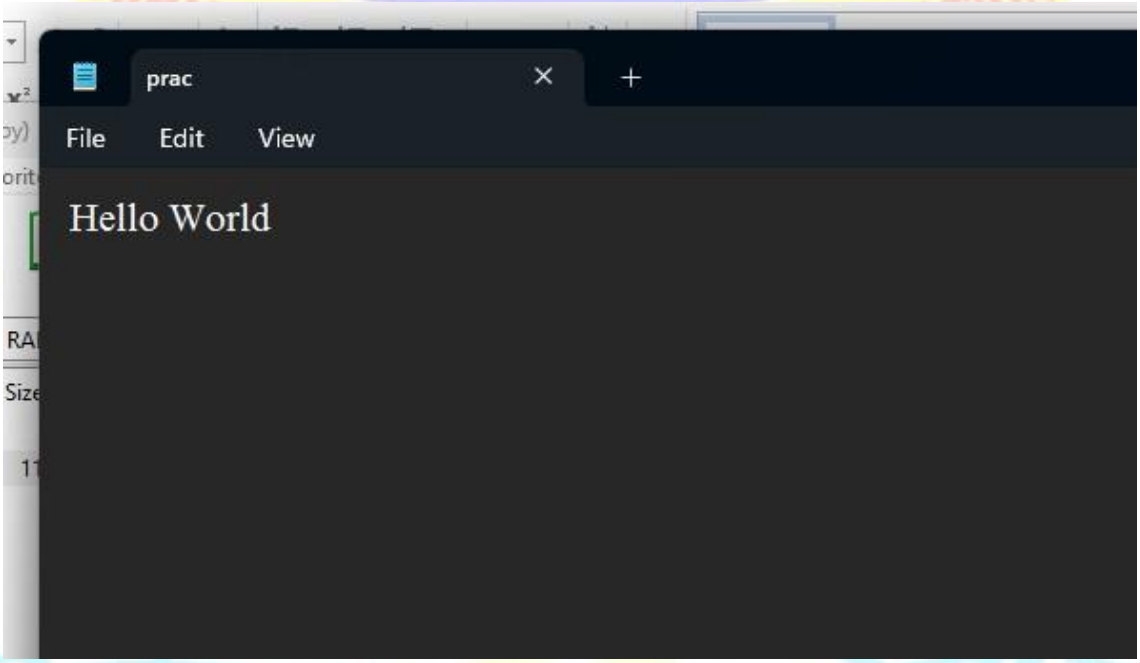
Select **Choose another app** → **choose an app on your pc**

Then **Desktop** → **Shortcut created of WinRAR** and **Select Just Once**





View the Extracted File



Result:

Detecting steganography allows forensic investigators to uncover hidden information or files within digital images, which can be vital in identifying malicious activities or hidden evidence.

Learning Outcomes:

- Understand how to detect hidden information in digital images using steganography analysis tools.
- Learn to extract and examine hidden content effectively.
- Develop skills to analyze digital images for signs of steganography.

Course Outcomes:

- Gain practical knowledge of steganography detection techniques in digital forensics.
- Ability to identify and extract hidden information from digital media.
- Apply analytical skills to assess the implications of steganography in investigations.

Conclusion:

Viva Questions:

1. What is steganography, and how is it used to hide information?
2. What tools can be used for steganography detection in digital images?
3. How can you extract hidden content from an image?
4. Why is it important to analyze images for signs of steganography in forensics?

PRACTICAL NO: 8

Aim:

Mobile Device Forensics

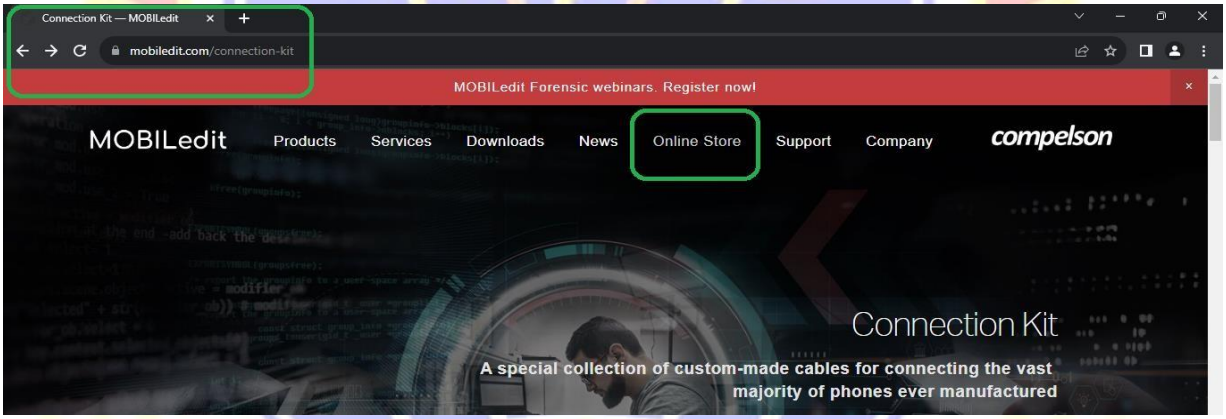
- Perform a forensic analysis of a mobile device, such as a smartphone or tablet.
- Retrieve call logs, text messages, and other relevant data for investigative purposes.

Practical:

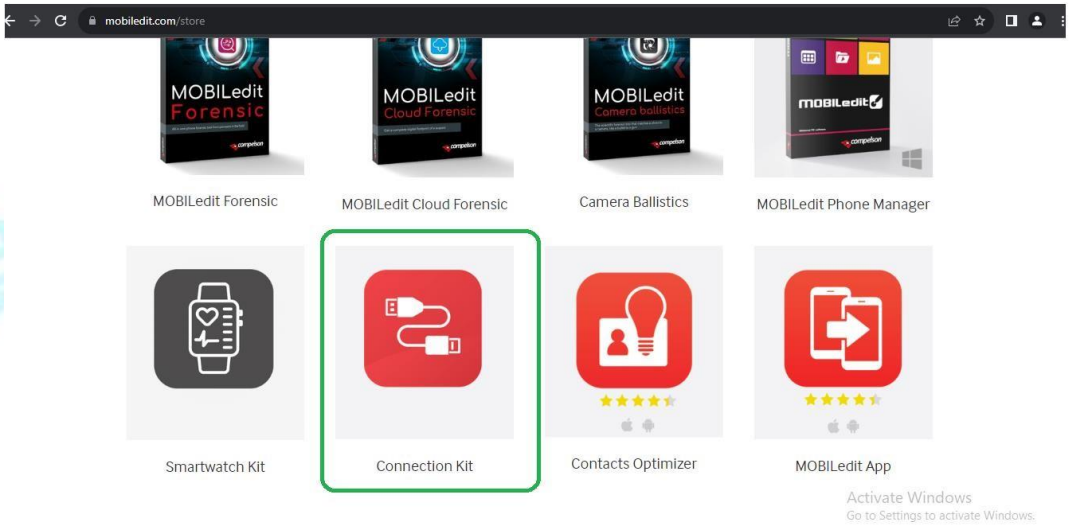
In this Practical we are going to perform the mobile forensic using the MOBILedit Forensic toolkit

We are going to download the MOBILedit toolkit

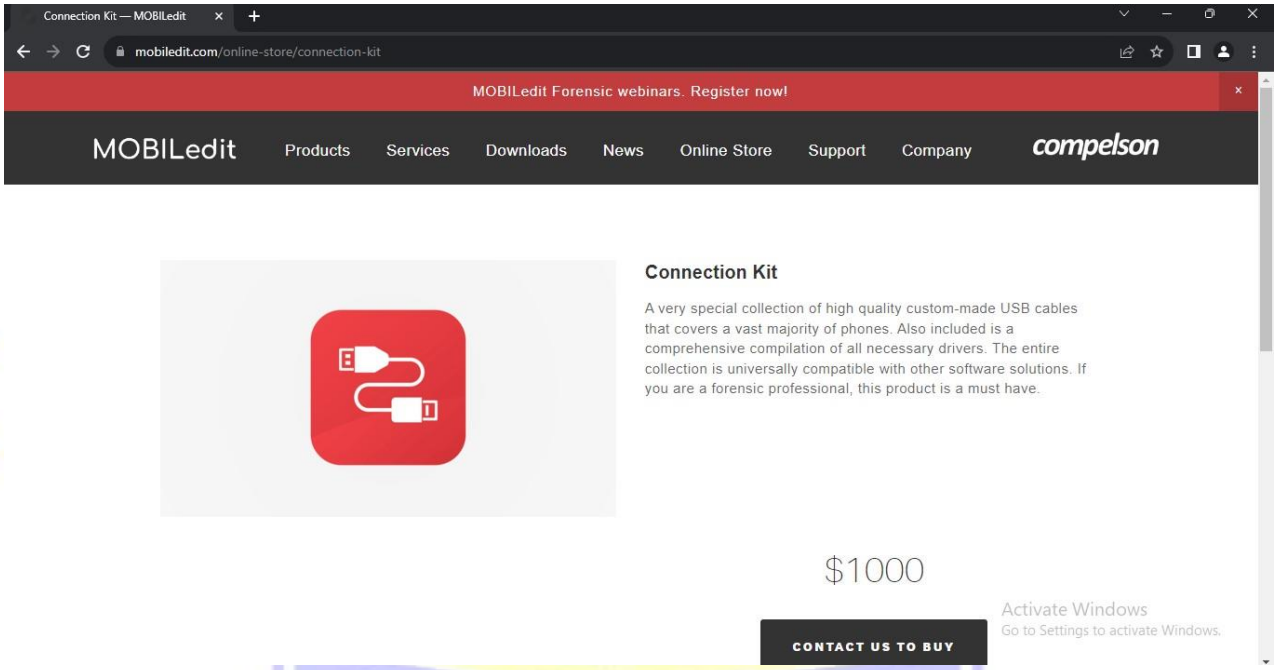
Got to the link https://www.mobiledit.com/connection-kit



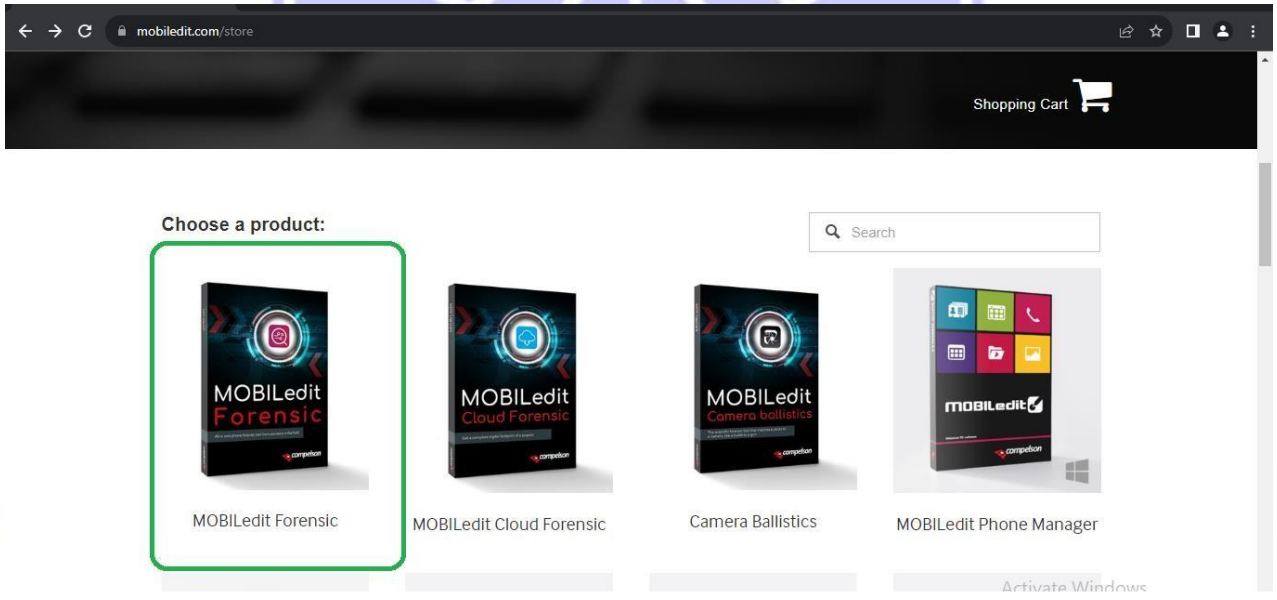
Then Click on **Online Store** then Scroll down to the Products



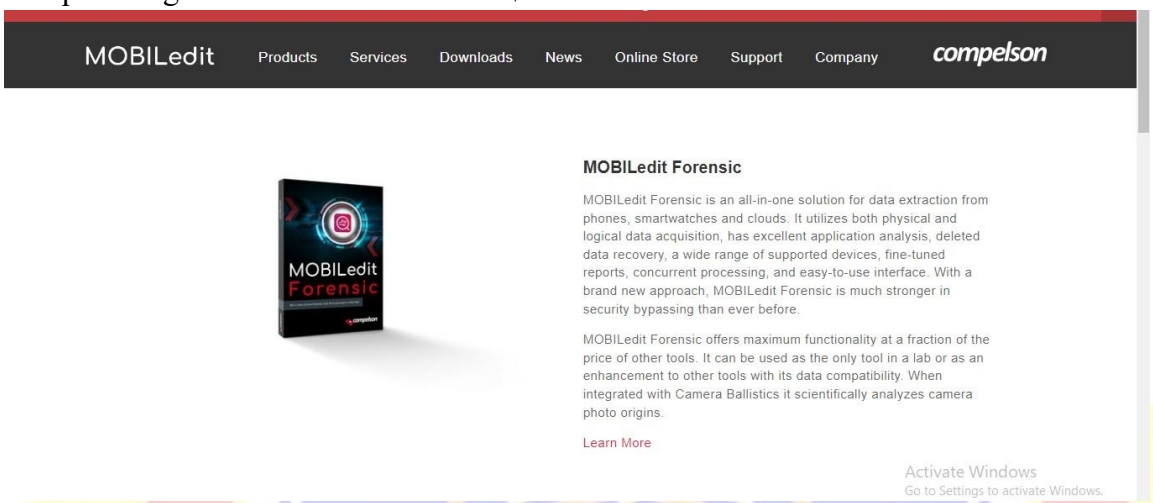
The Price is given below. It is around $1000

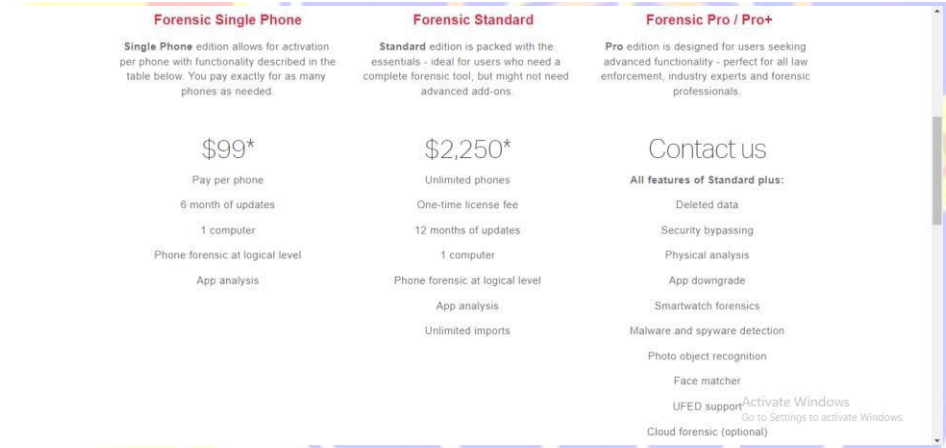


Then we go to the software



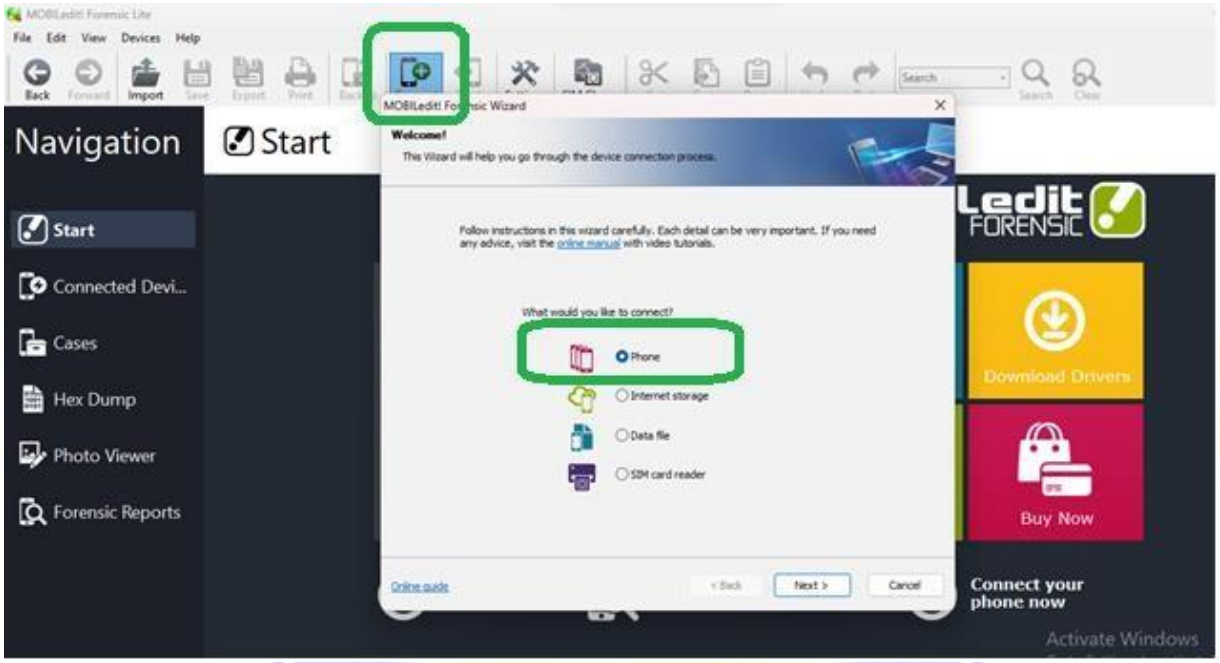
The price is given below. It starts from $99 to few Thousands of Dollars



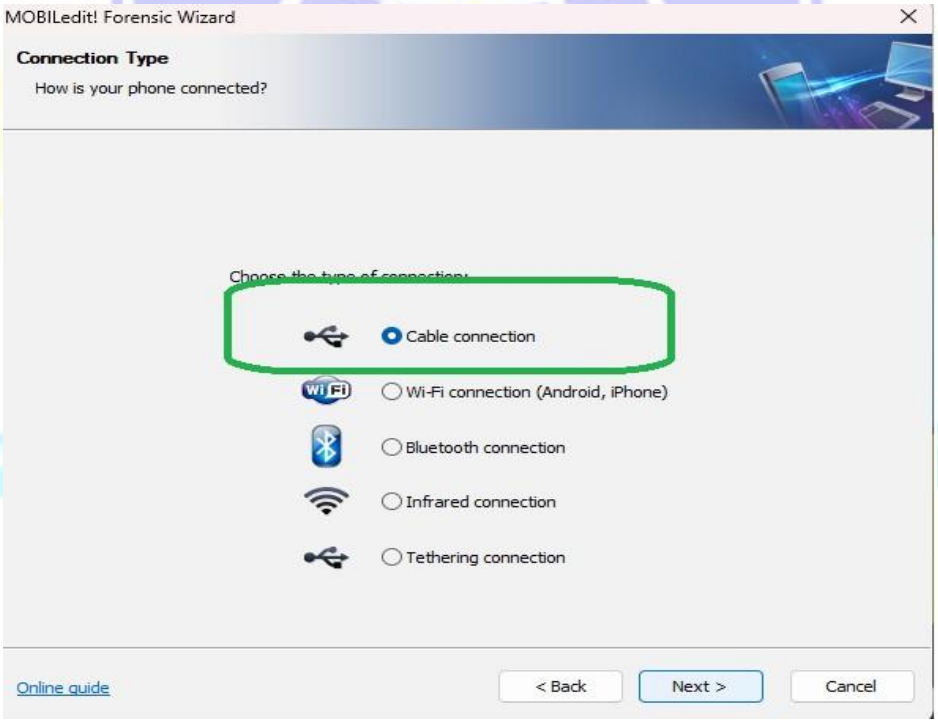


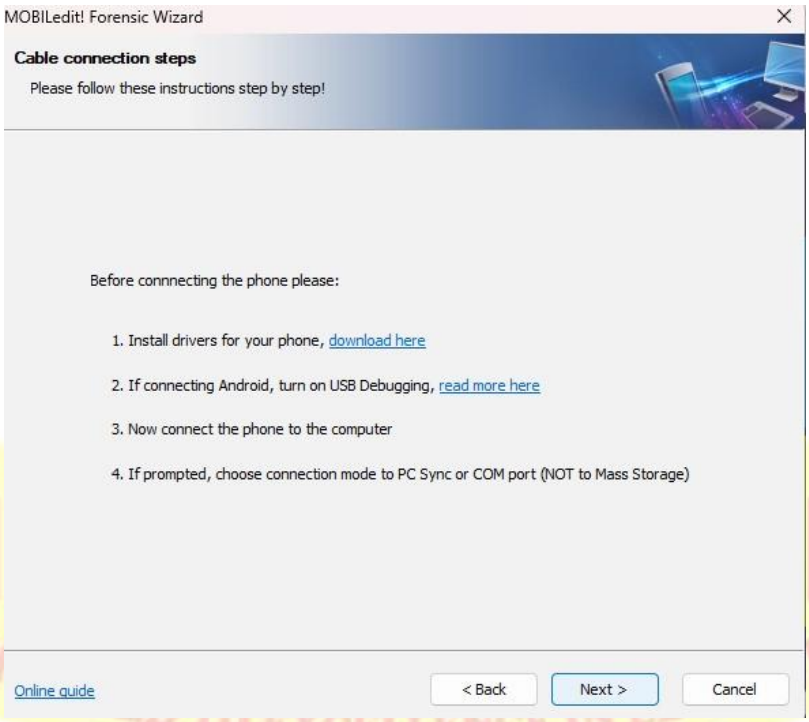
Now we are going to start the Practical

Click on **connect** and **Select the type of forensic device** to work with. Here we are going with **Phone**

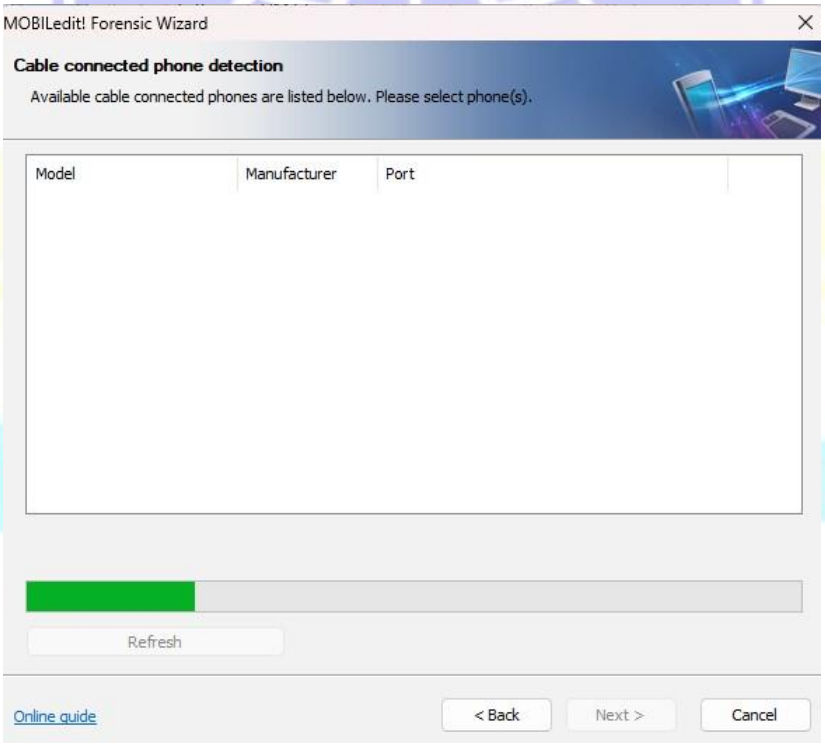


Click **Next** and **Select the type of Connection** with the **Mobile Phone.** Here we are going to Select **Cable Connection** and click Next

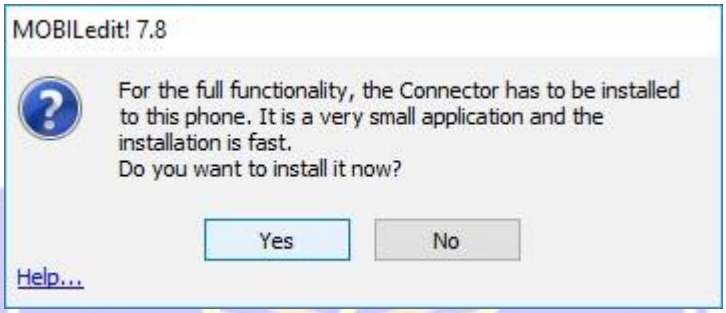


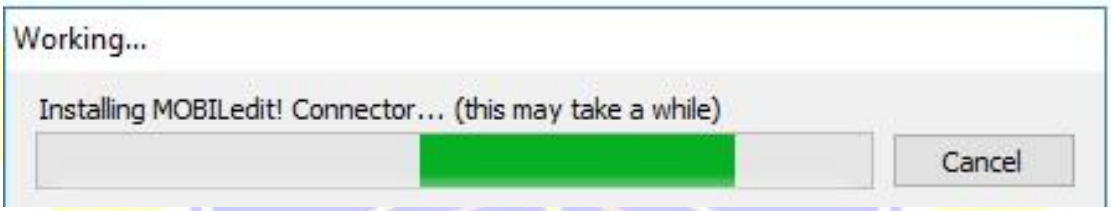


Click **Next** and let it **Scan the Device**, If ***Found*** click **Next**, If ***Not Found*** **Perform these steps and Retry** *"Go to Phone Settings and open Developer Option and Enable it, and then Allow USB Debugging"*

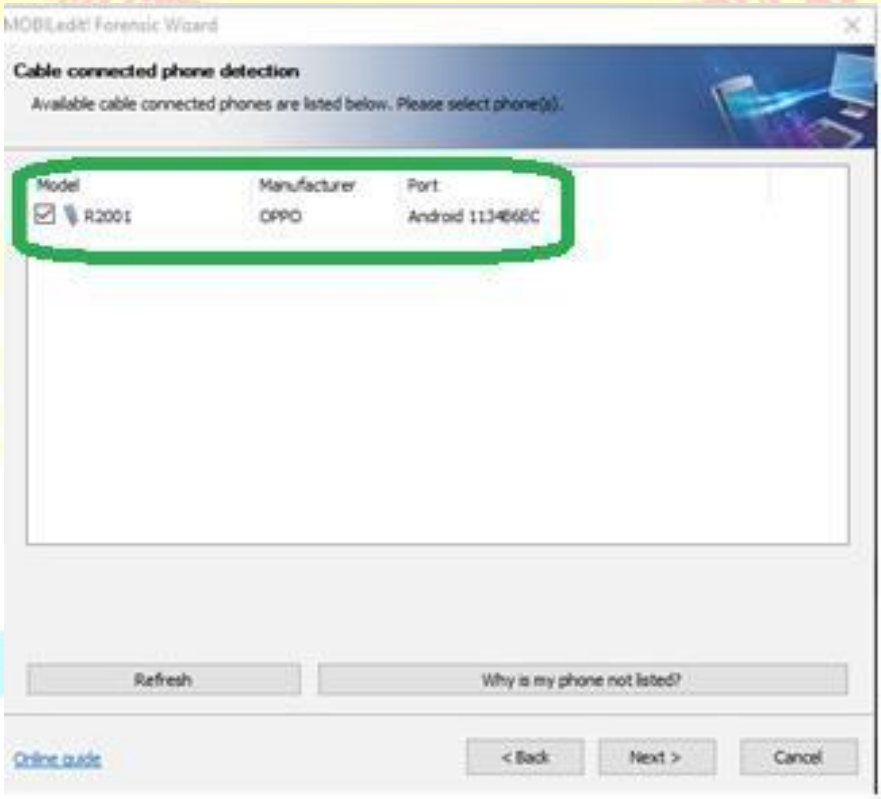


Then connect it with a connector for efficient data recovery

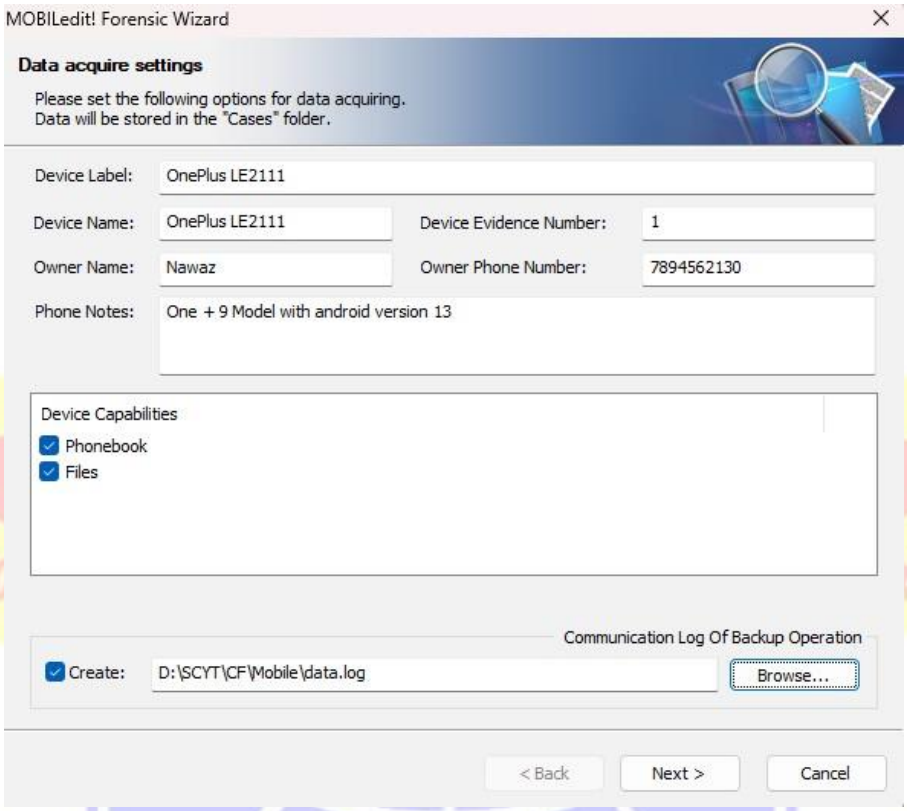




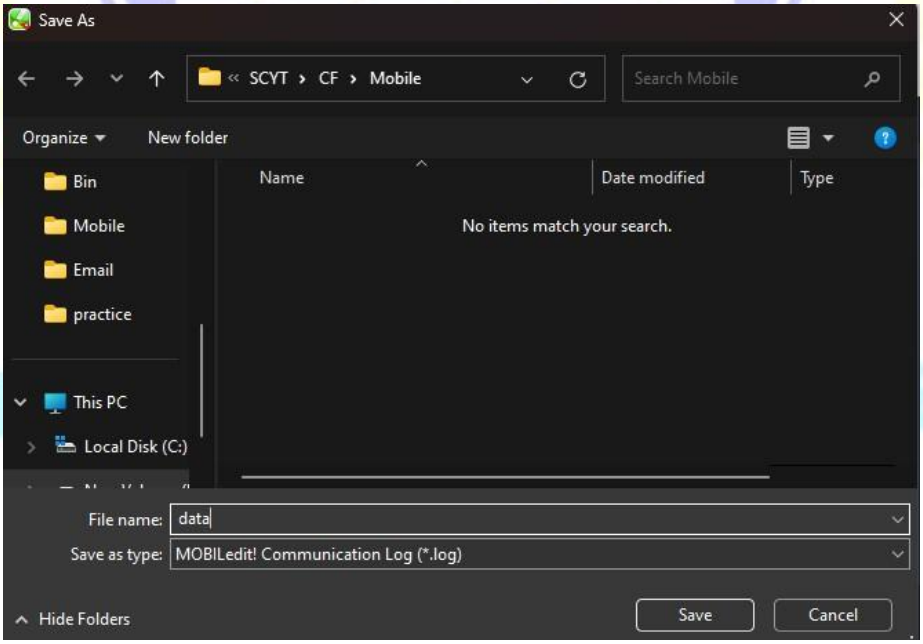
We got a device connected



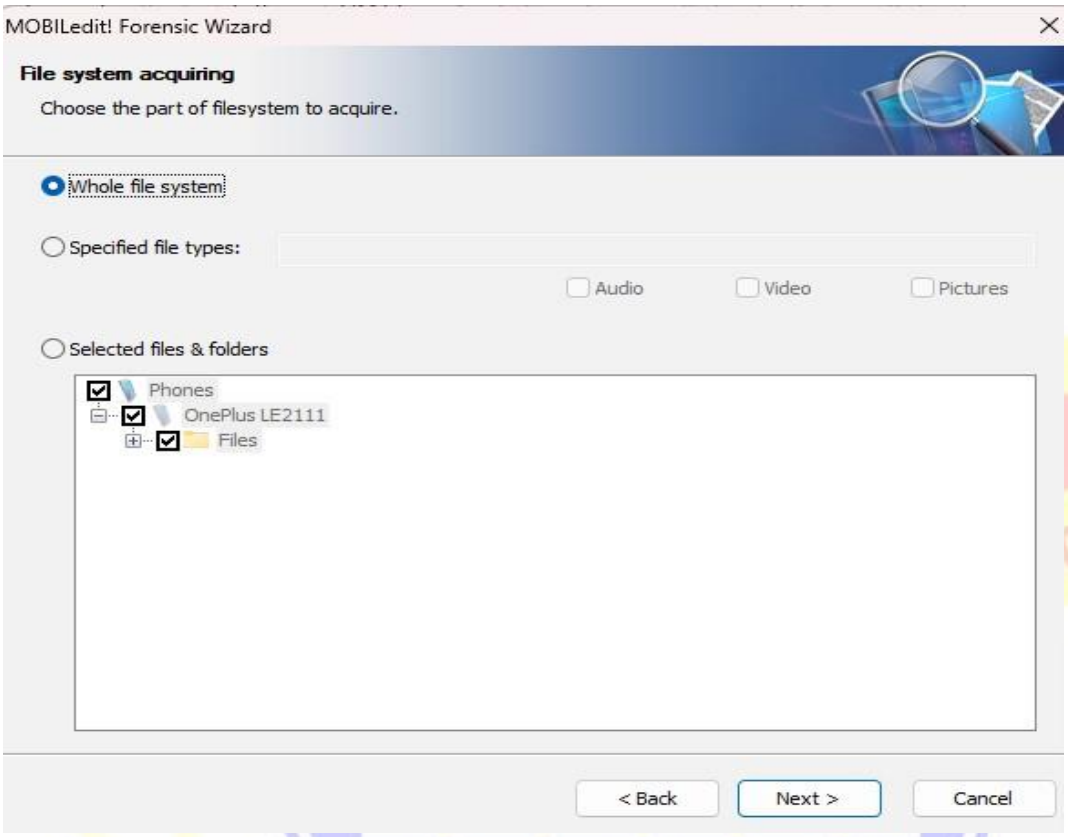
This is the device we are going to use and click on next

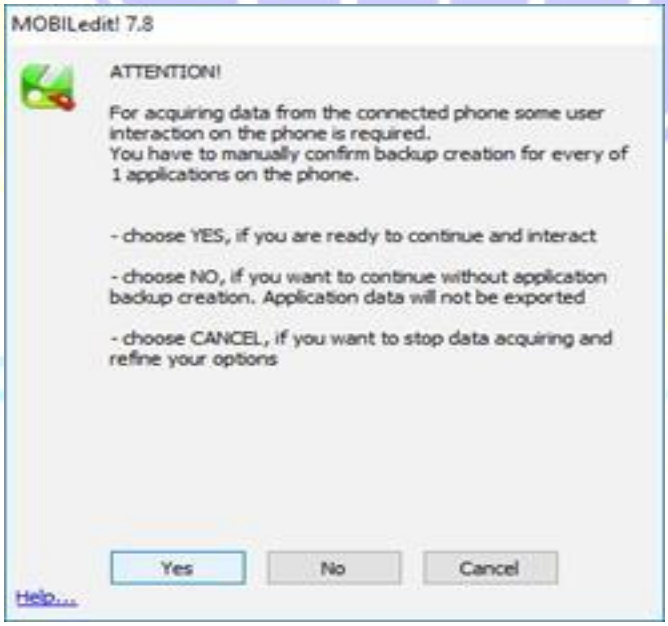


Fill the details and browse a directory to store the logs

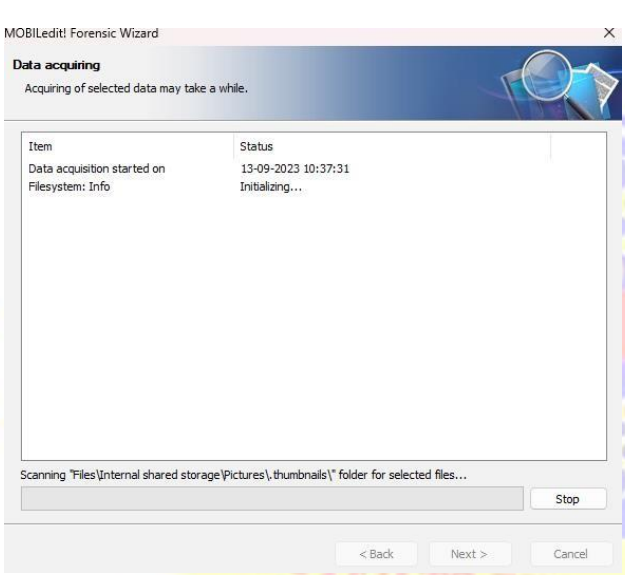


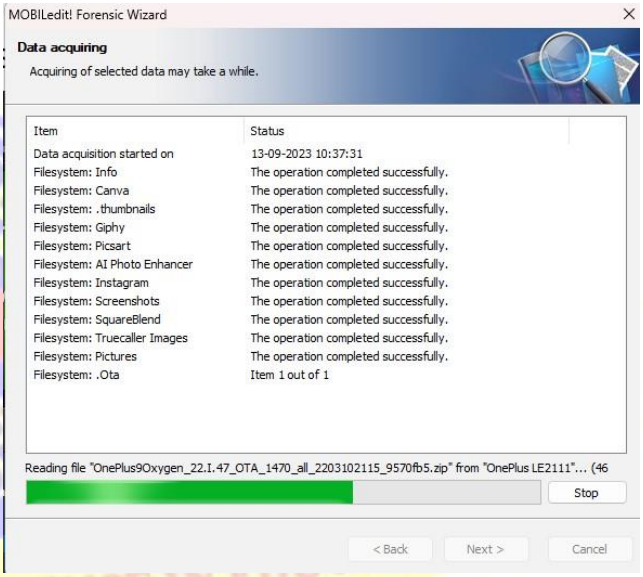
Then Click on Next then Select the **Acquisition** we want Here **we are going to acquire all the data from the device**

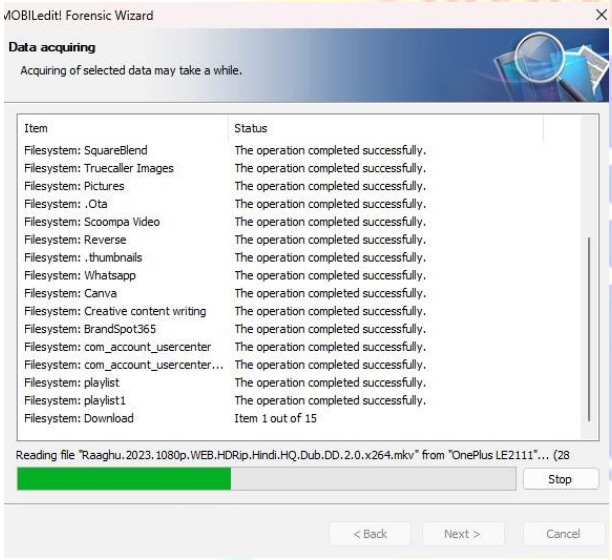


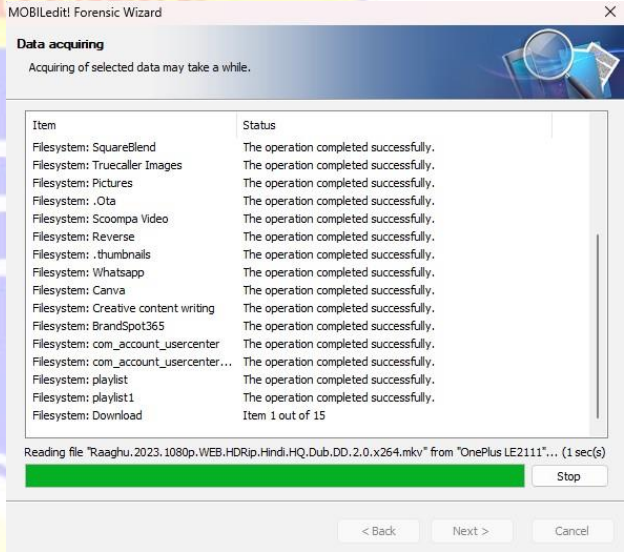


Click on Yes and Wait for the Acquisition to be completed

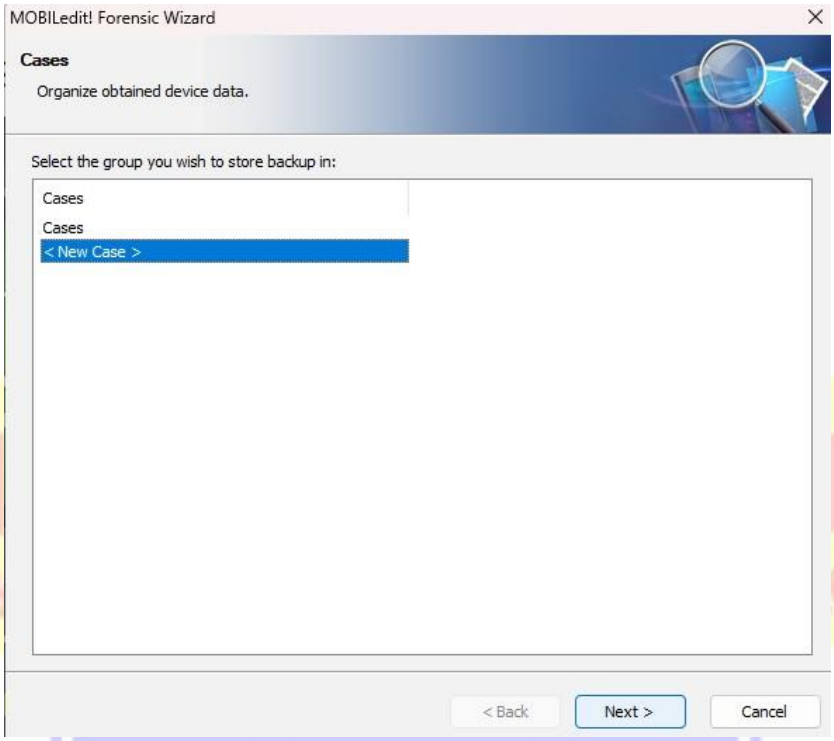




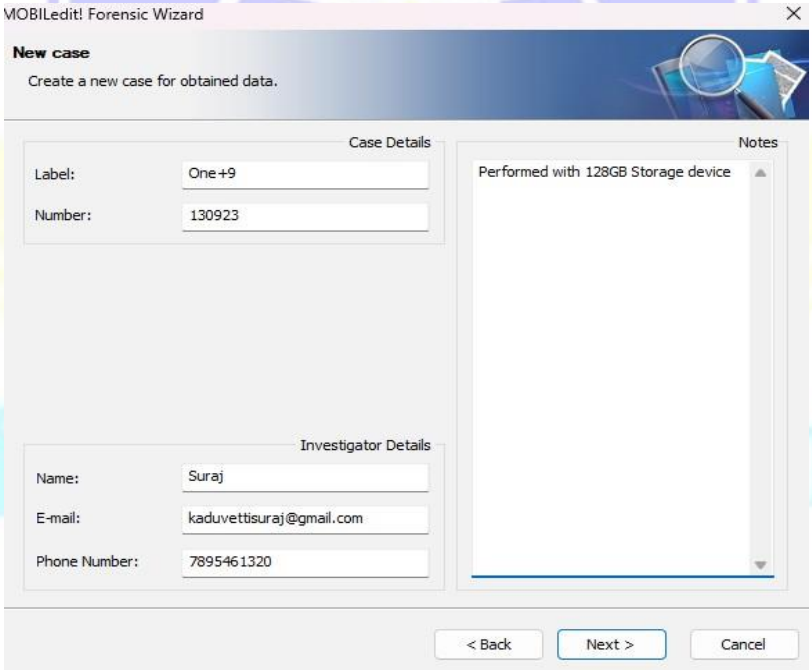




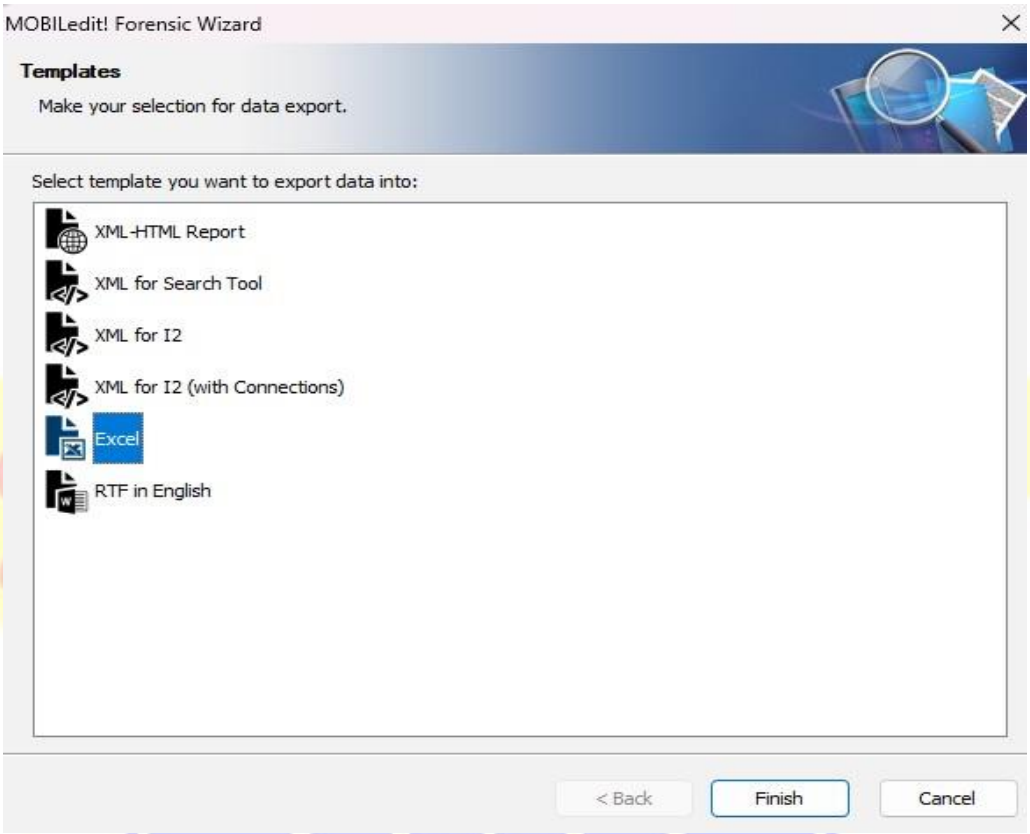
Open the **Case** and **Organize** and decide the **Format** in which we need the **Acquisition**



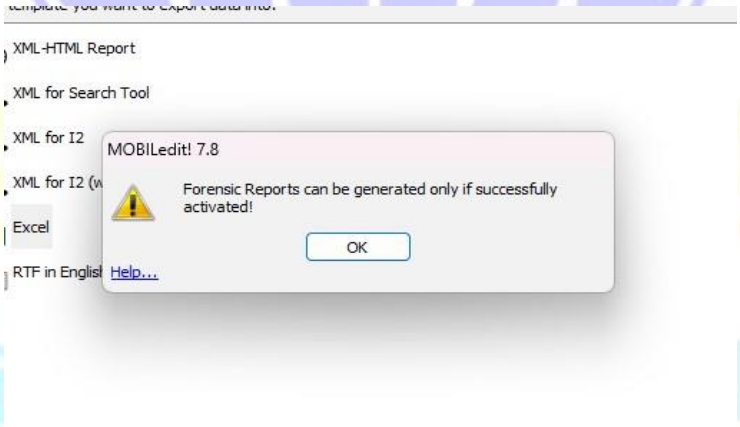
Fill in the details of the Investigator



Select the type of format to display the data. Here we are going to display it in Excel.



A Success Message will be Prompted



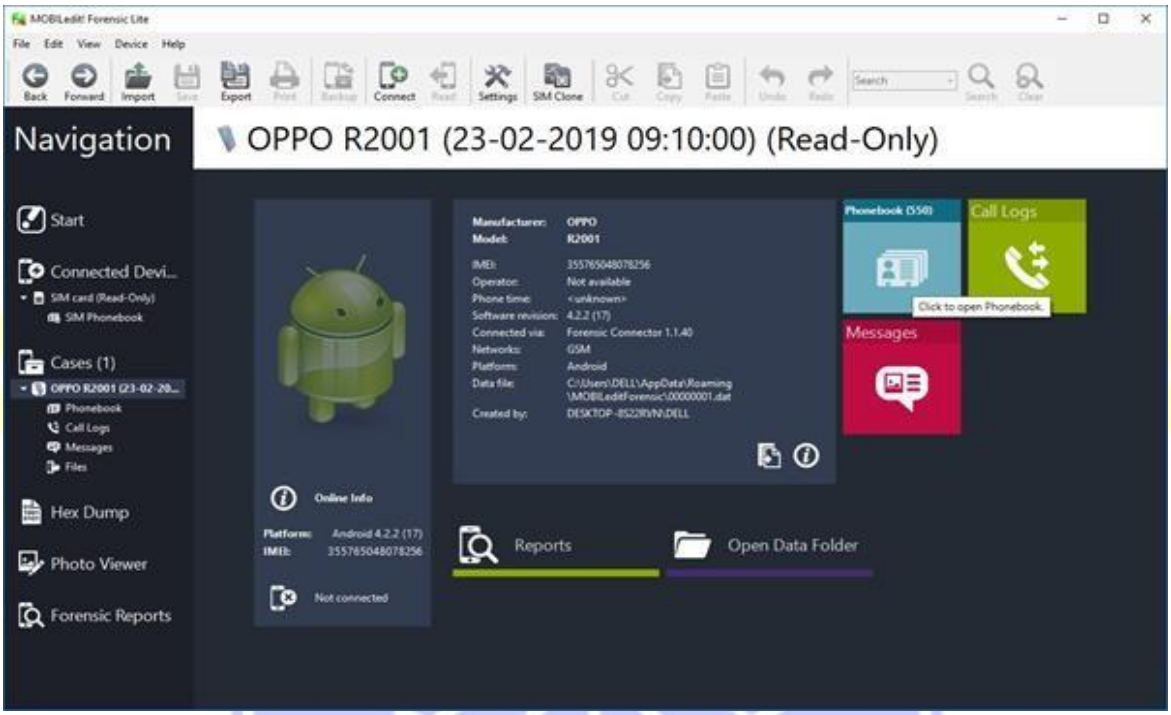
Now we are going to **view** and **analyze** the **data acquired** form the **Performed Acquisition**

We have performed of Two Mobile Devices

The First One is the Oppo Reno 2

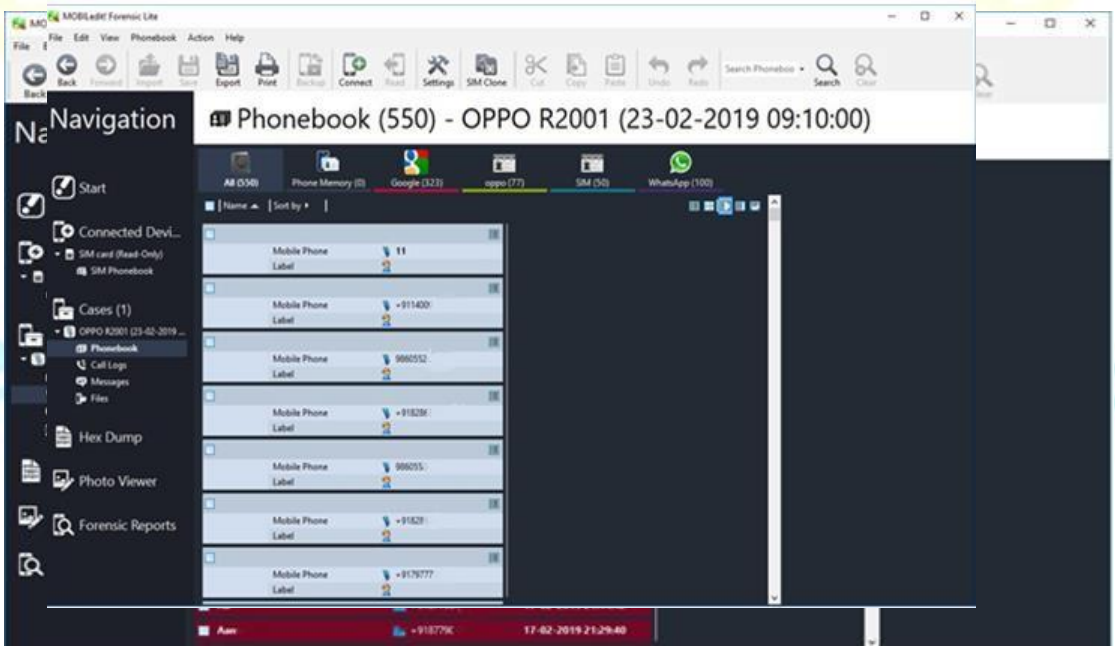
Second One is the One^{+} 9

Display of the First Device Oppo Reno 2

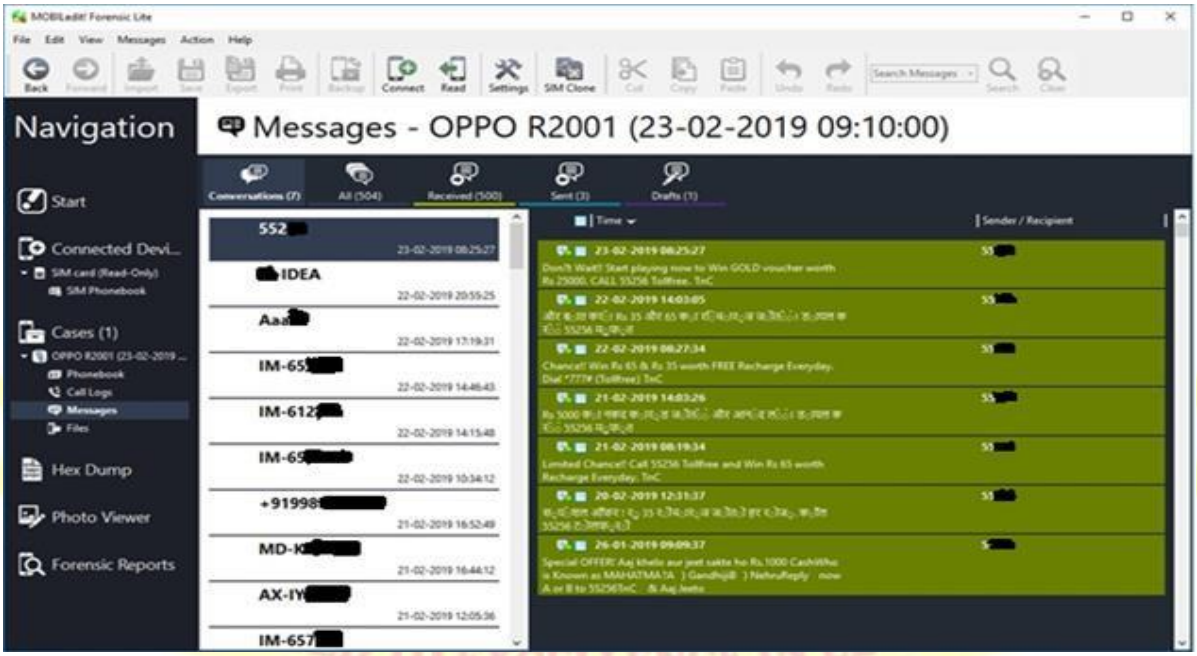


Here we can see the Phonebook of the device

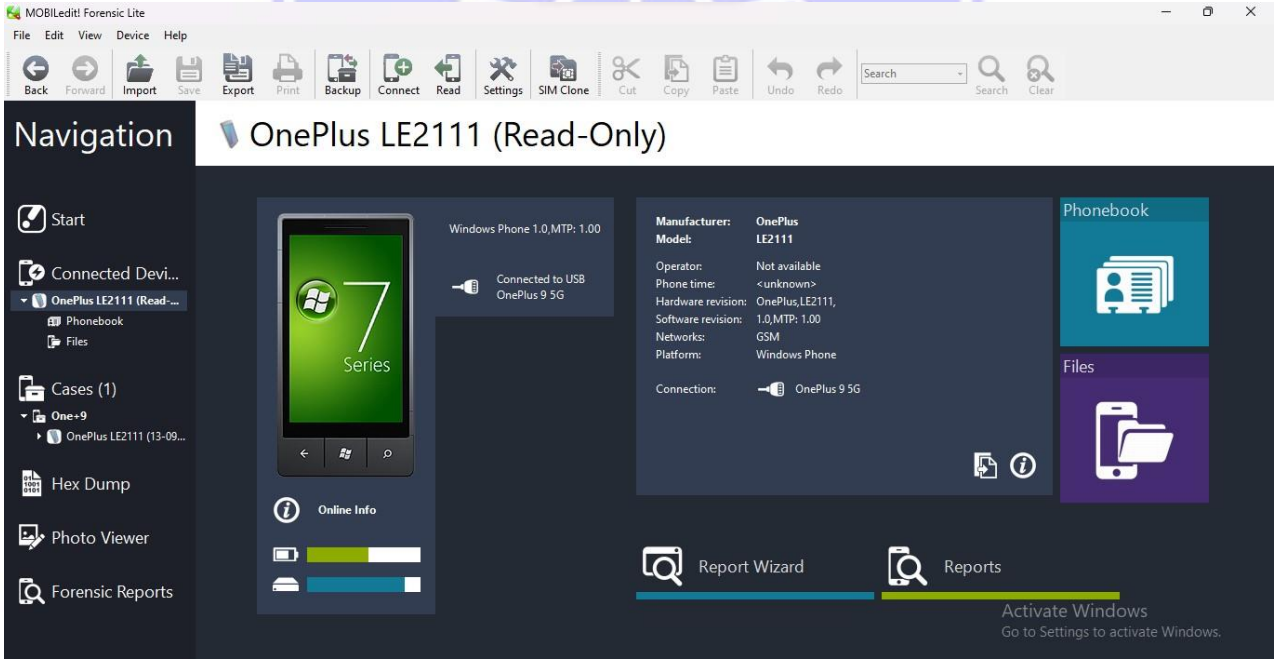
And here we can see the Call Logs



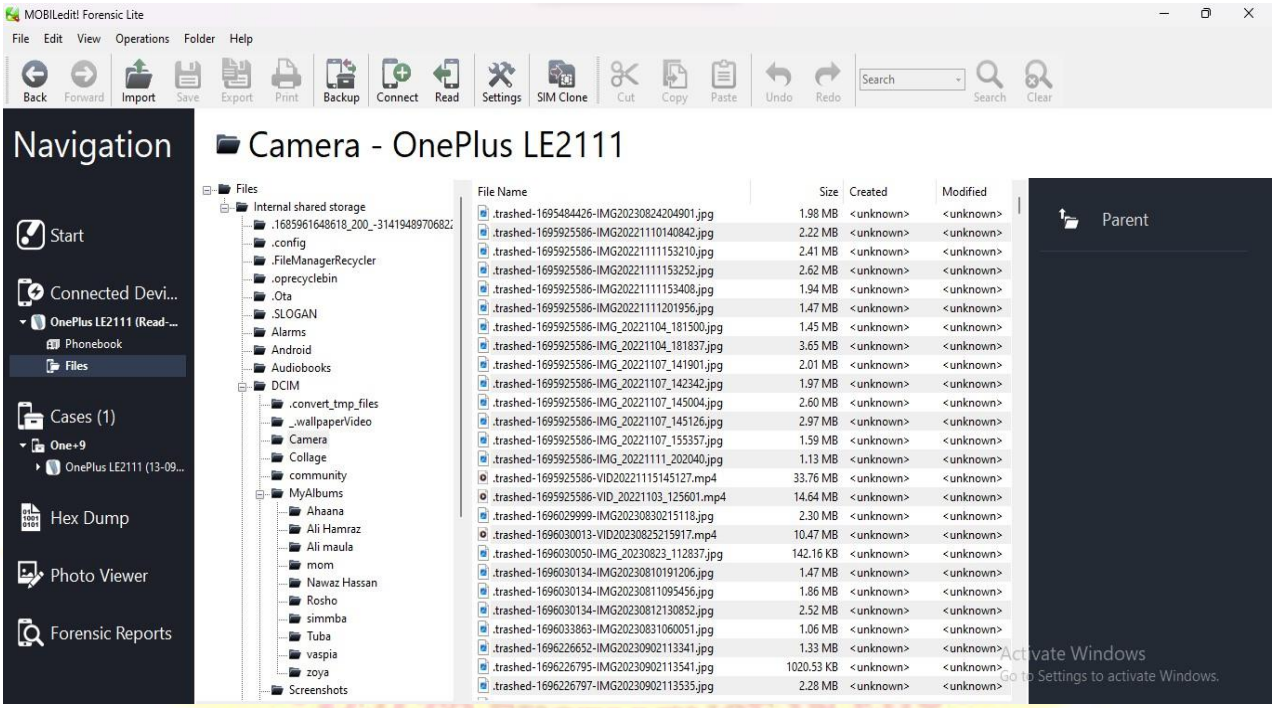
And here we can see the messages on the device



Display of the Second Device One+ 9



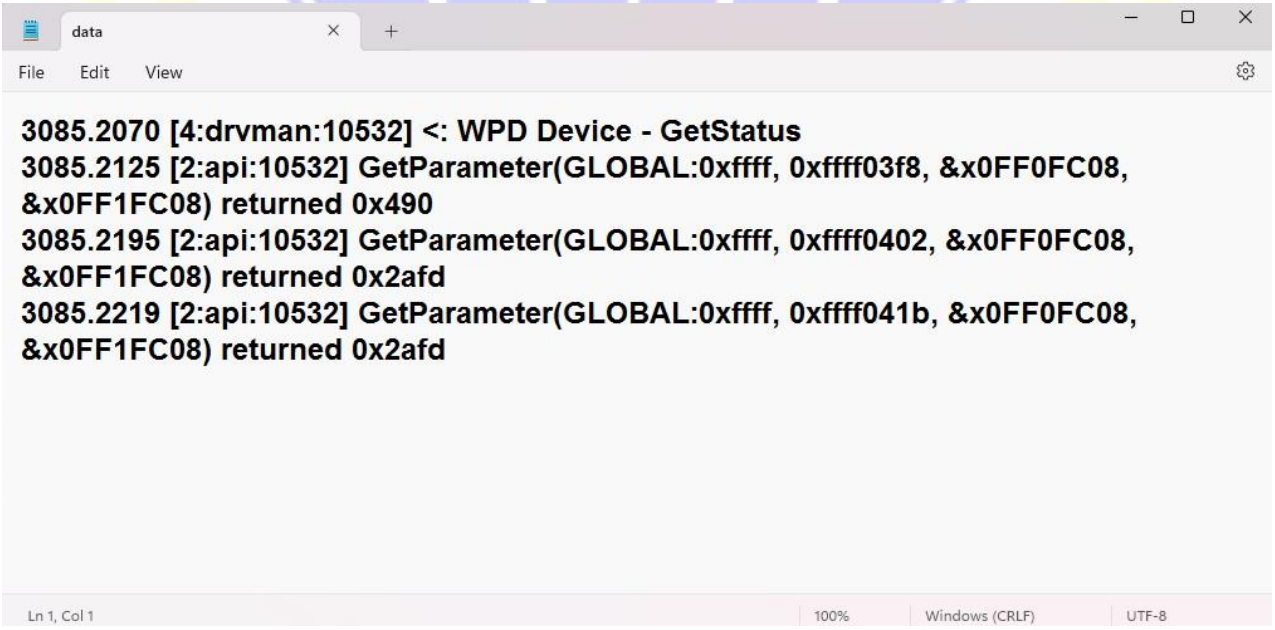
Here we can see the Files → Internal Storage → DCIM → Camera



Here we can see the Files → Internal Storage → Pictures

Now we are going to **Generate** and **Analyze** the **Report**

This is the **data.log** file we created before we started the **Acquisition**



Result:

Performing a forensic analysis of a mobile device allows investigators to retrieve crucial data such as call logs, text messages, and app information, which are essential for understanding user behavior and activities.

Learning Outcomes:

- Understand how to conduct a forensic analysis of mobile devices like smartphones and tablets.
- Learn to retrieve and analyze call logs, text messages, and other relevant data.
- Develop skills to extract information from mobile applications for investigative purposes.

Course Outcomes:

- Gain practical knowledge of mobile device forensics and its importance in investigations.
- Ability to recover and interpret data from various mobile applications and features.
- Apply mobile forensic techniques to gather evidence effectively.

Conclusion:

Viva Questions:

1. What are the main steps involved in mobile device forensics?
2. How can call logs and text messages be retrieved from a smartphone?
3. What challenges do forensic investigators face when analyzing mobile devices?
4. Why is it important to analyze app data during a mobile forensic investigation?

PRACTICAL NO: 9

Aim:

Email Forensics

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

Practical:

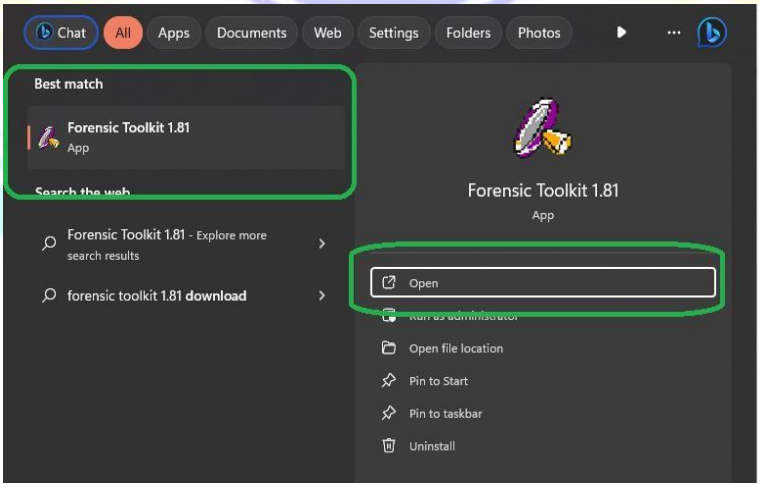
Here we are going to use the AccessData FTK

FTK can filter or find files specific to e-mail clients and servers.
You can configure these filters when you enter search parameters.
Because of Jim's responses to a poor performance review, the CEO of Superior Bicycles,Martha Dax, suspects he might have obtained sensitive information about the company's business model that he's leaking to a competitor.
Martha asked her CIO, to have an IT employee copy the Outlook .pst file from Jim Shu's old computer to a USB drive.
To process this investigation, we need to examine the Jim_shu's.pst file, locate the message, and export it for further analysis of its header to see how Jim might have received it.

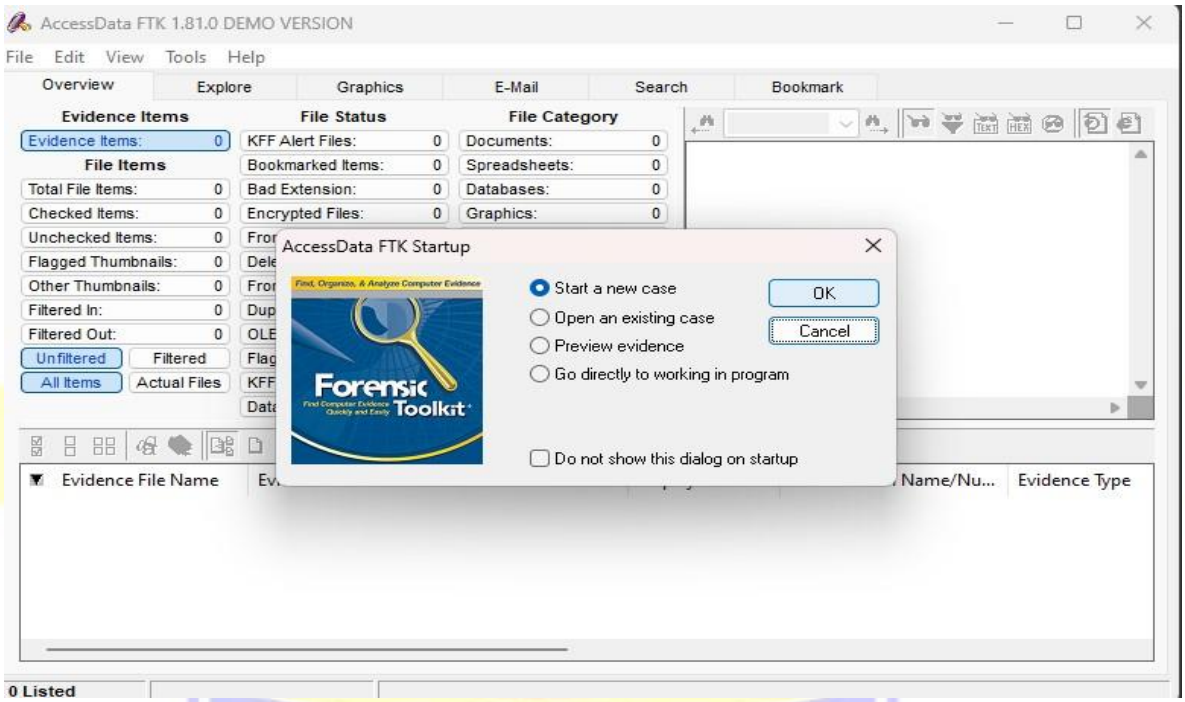
Recovering Email

Start **AccessData FTK** and click **Start a new case**, then click **OK**.

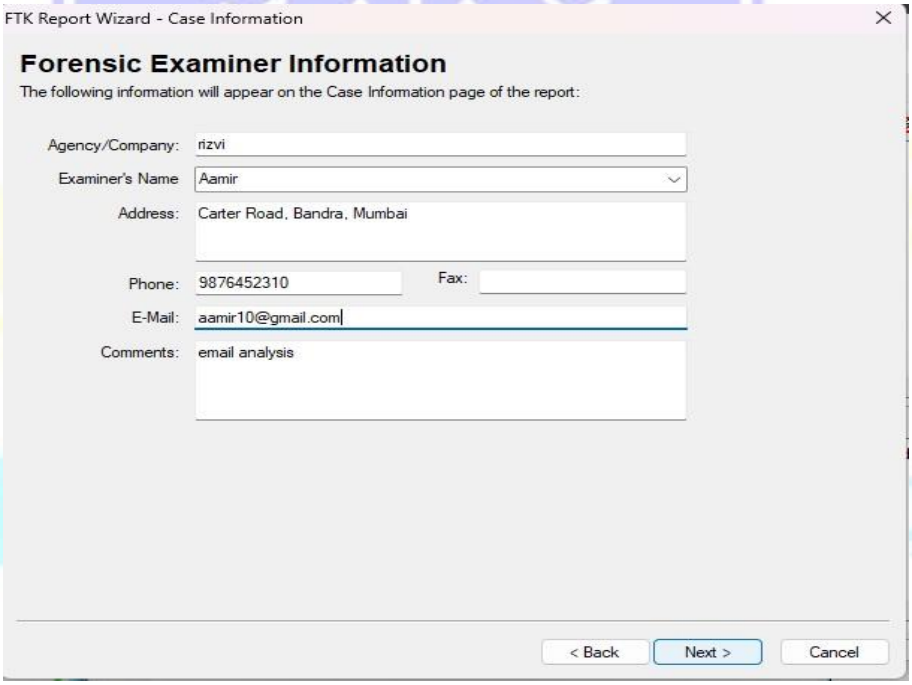
Click **Next** until you reach the **Refine Case - Default dialog box** Click the **Email Emphasis button**, and then click **Next**



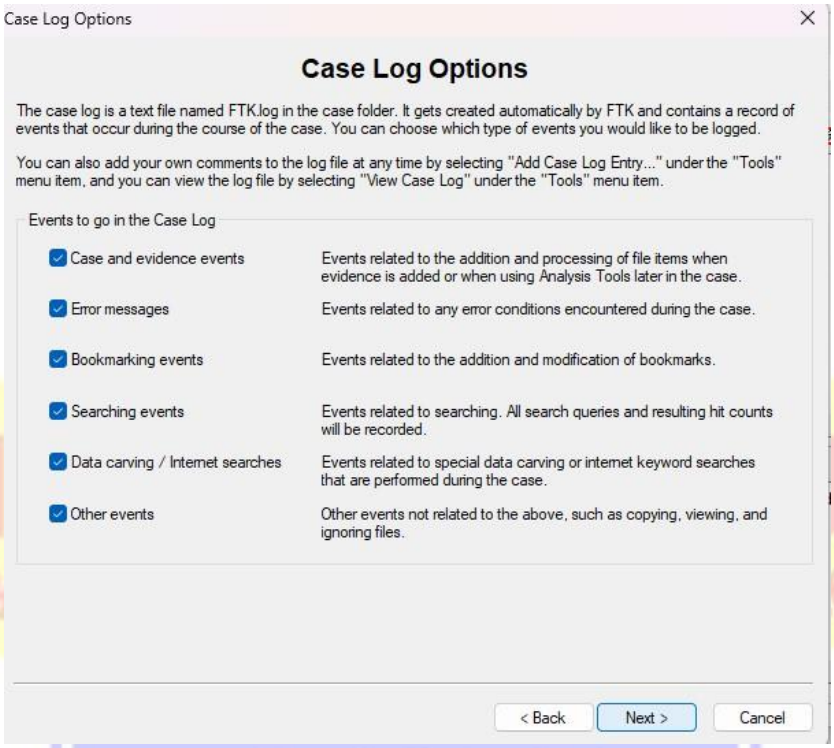
Create a new File



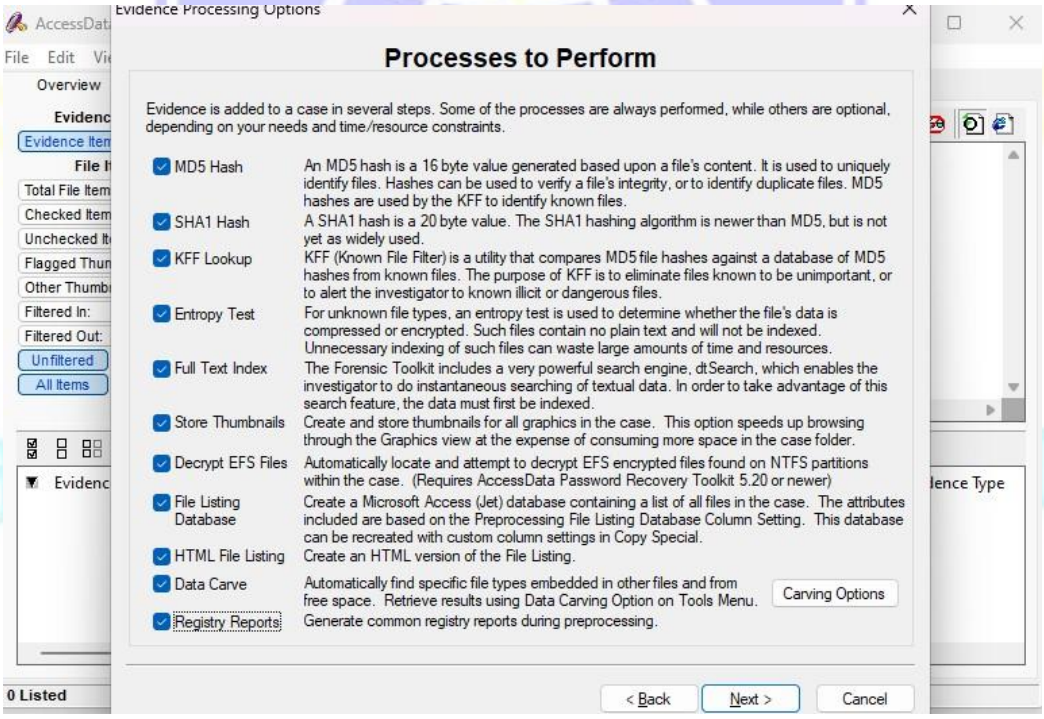
Fill the details of the Examiner



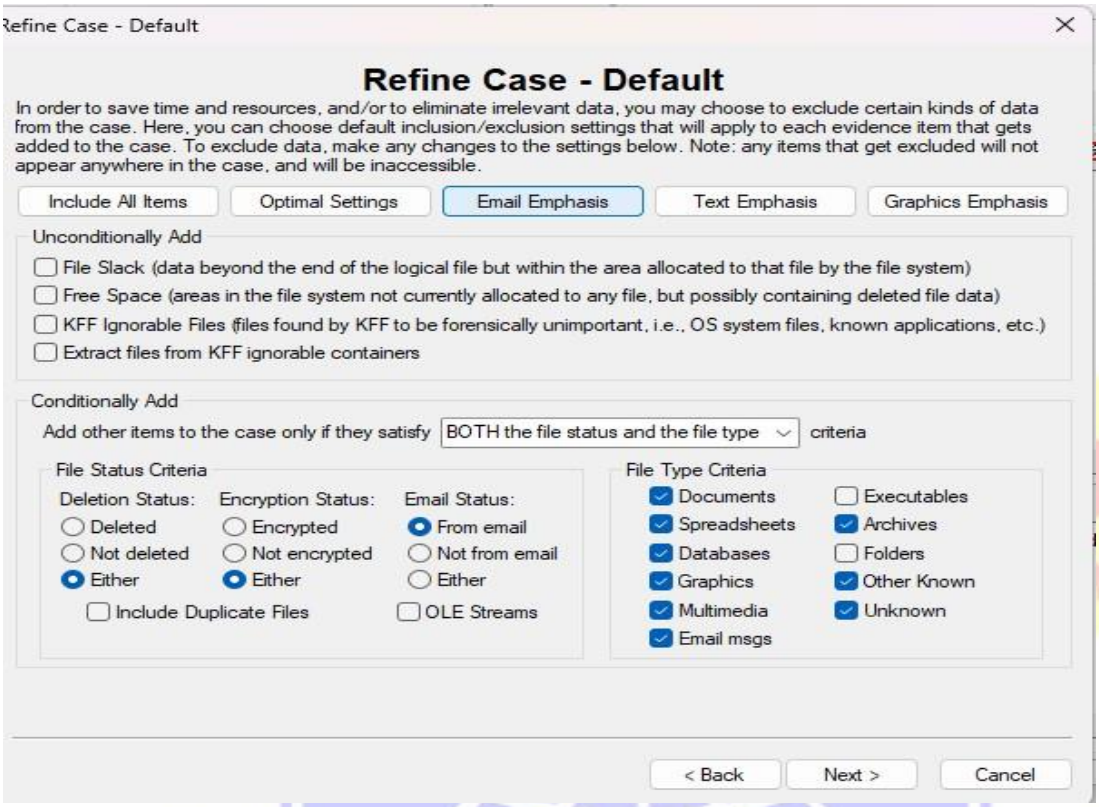
Click on all the options and Click Next

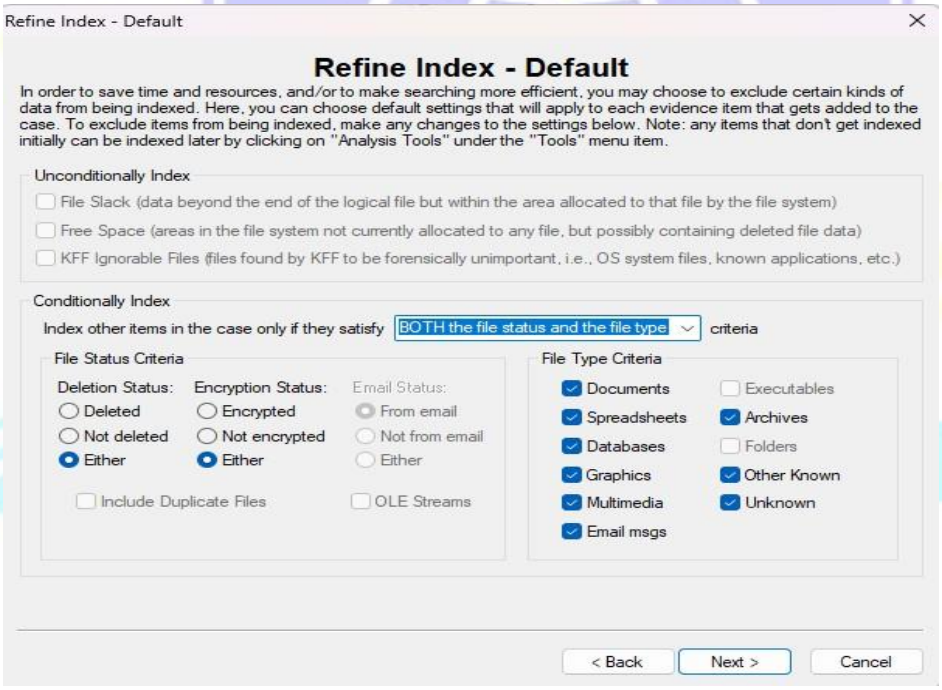


Select all the options

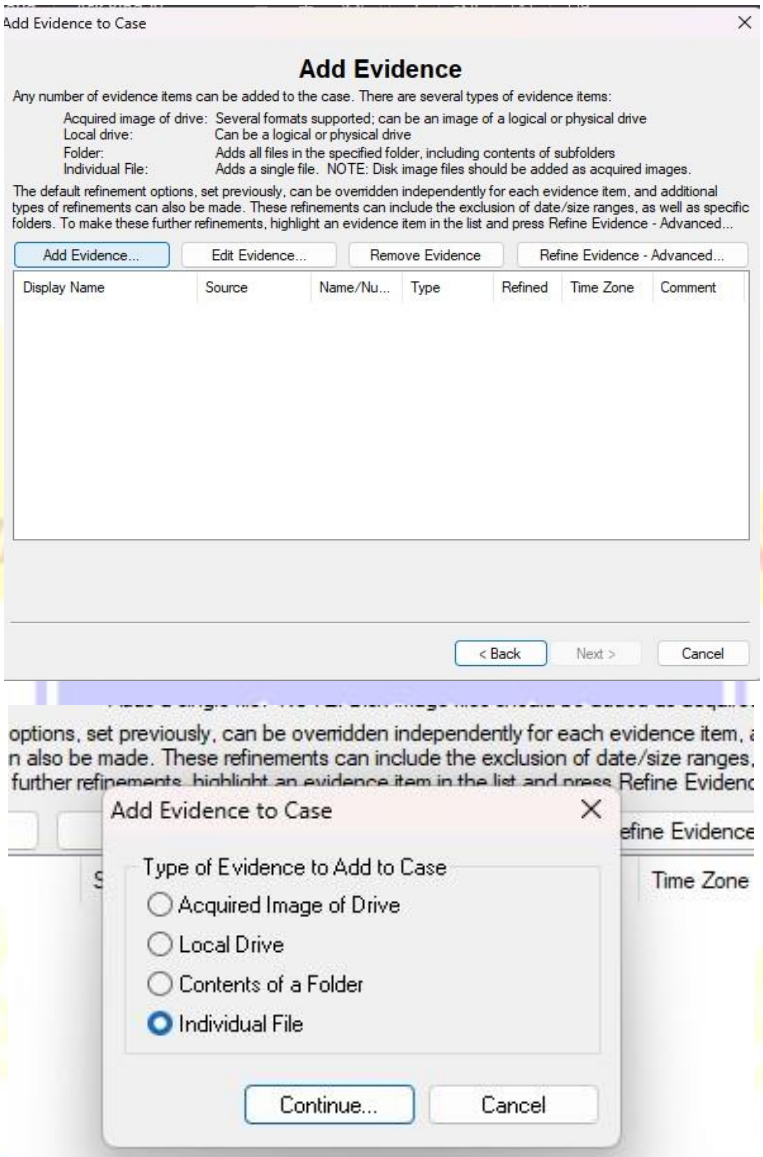


Now we have reached the Email Emphasis section

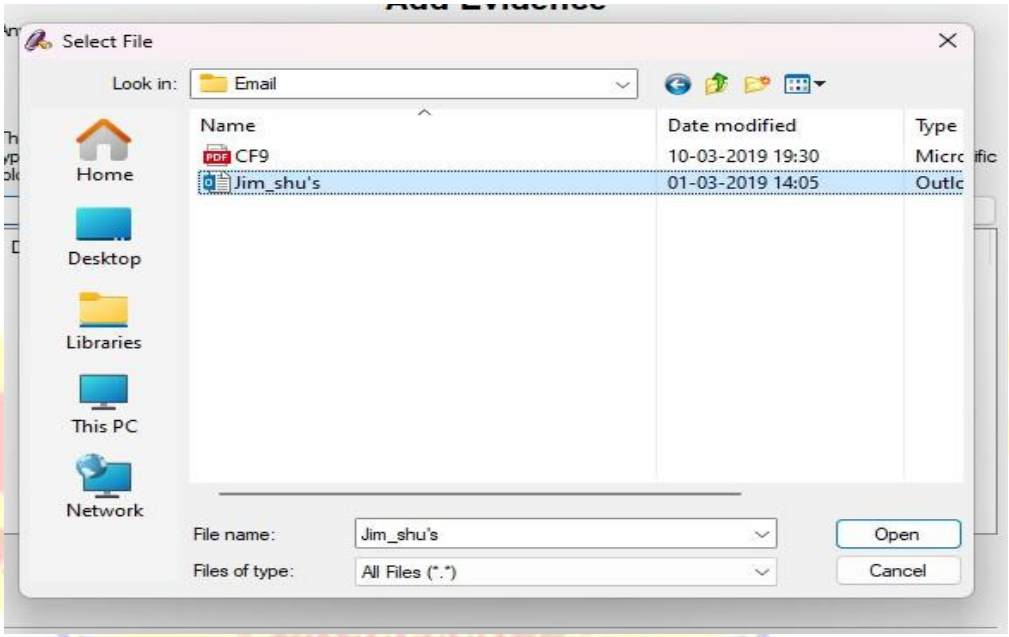




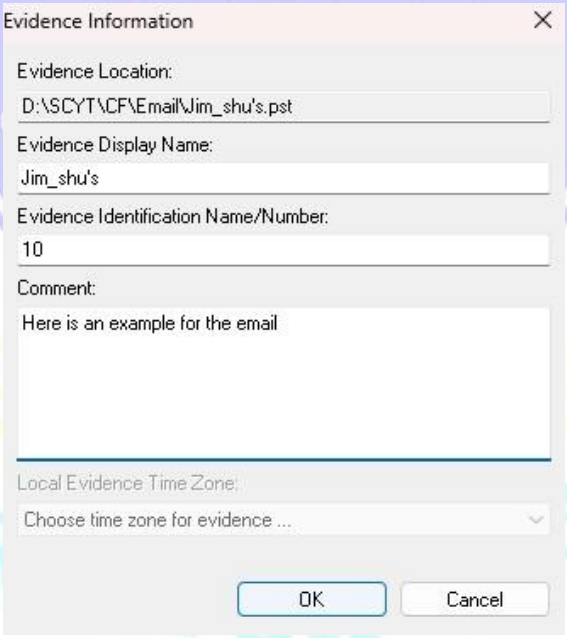
Click Next until you reach the **Add Evidence** to **Case dialog box**, and then click the **Add Evidence button**. In the **Add Evidence** to **Case dialog box**, click the **Individual File option button**, and then click **Continue**.



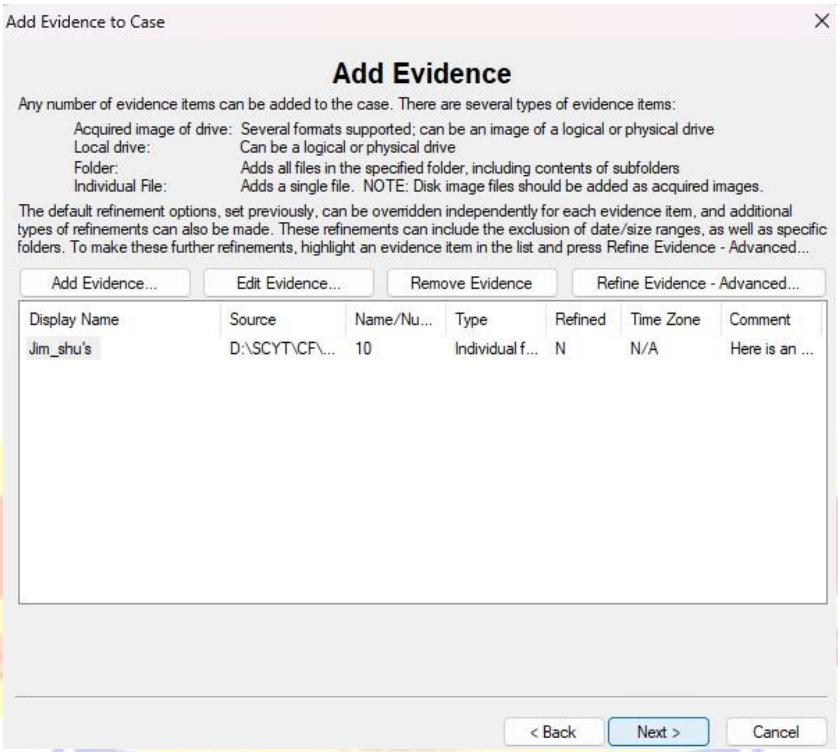
In the Select **File dialog box**, **navigate to your work folder**, click the **Jim_shu's.pst file**, and then click **Open**.



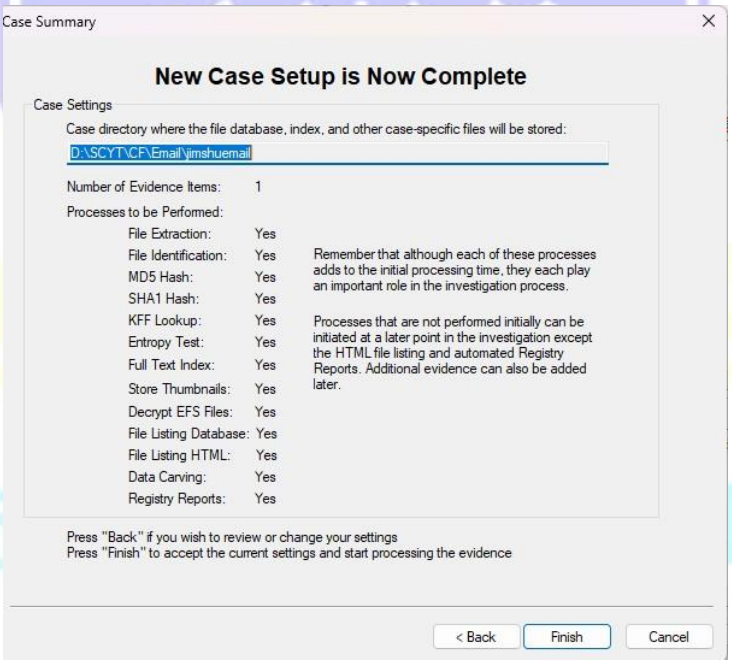
Give some data

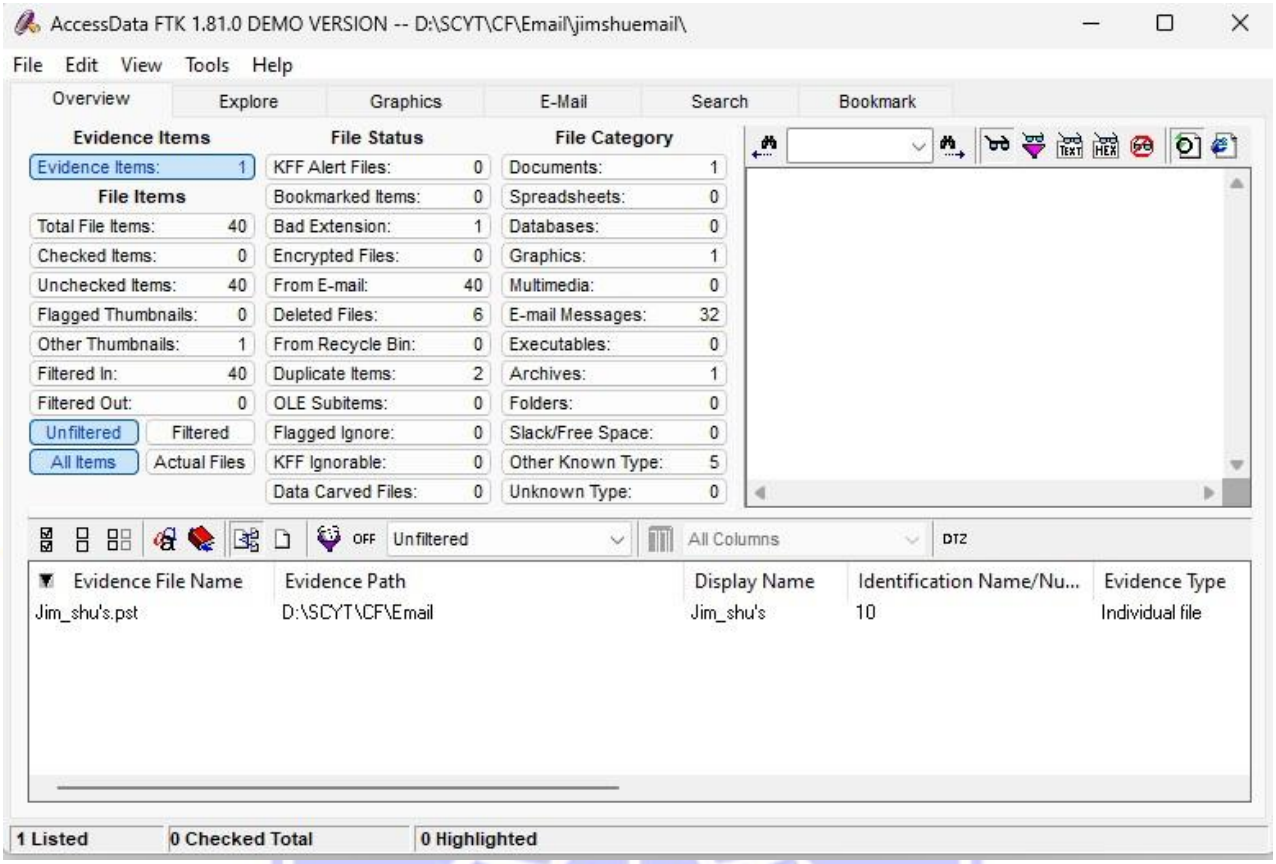


Complete the steps and Click on Next

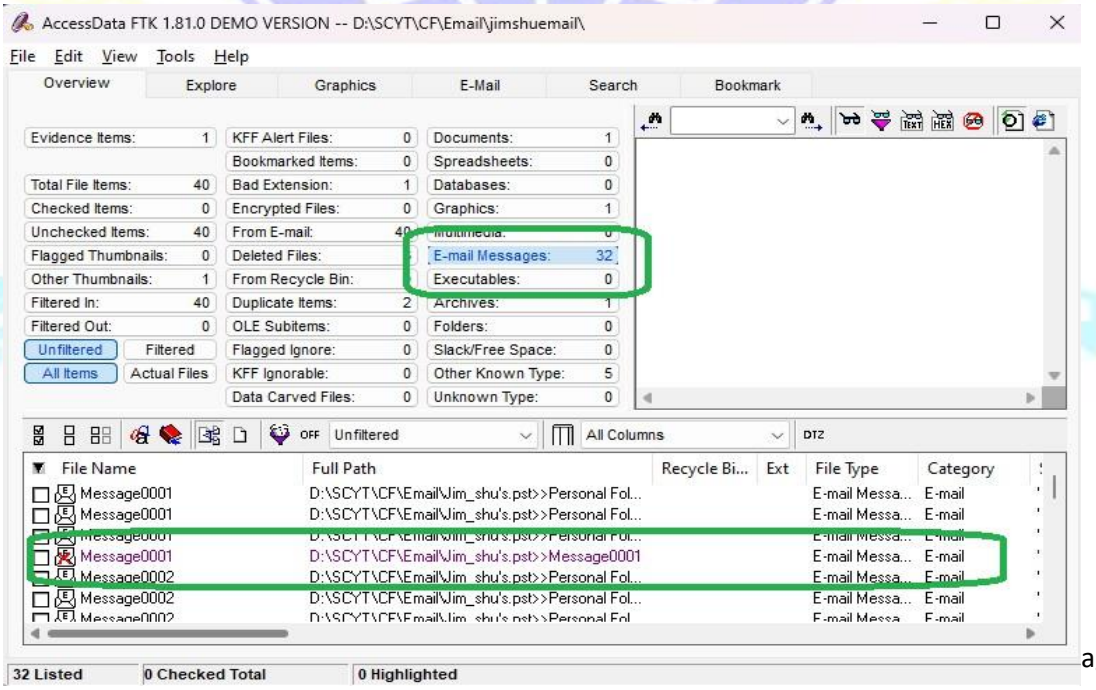


Click on finish and see the data

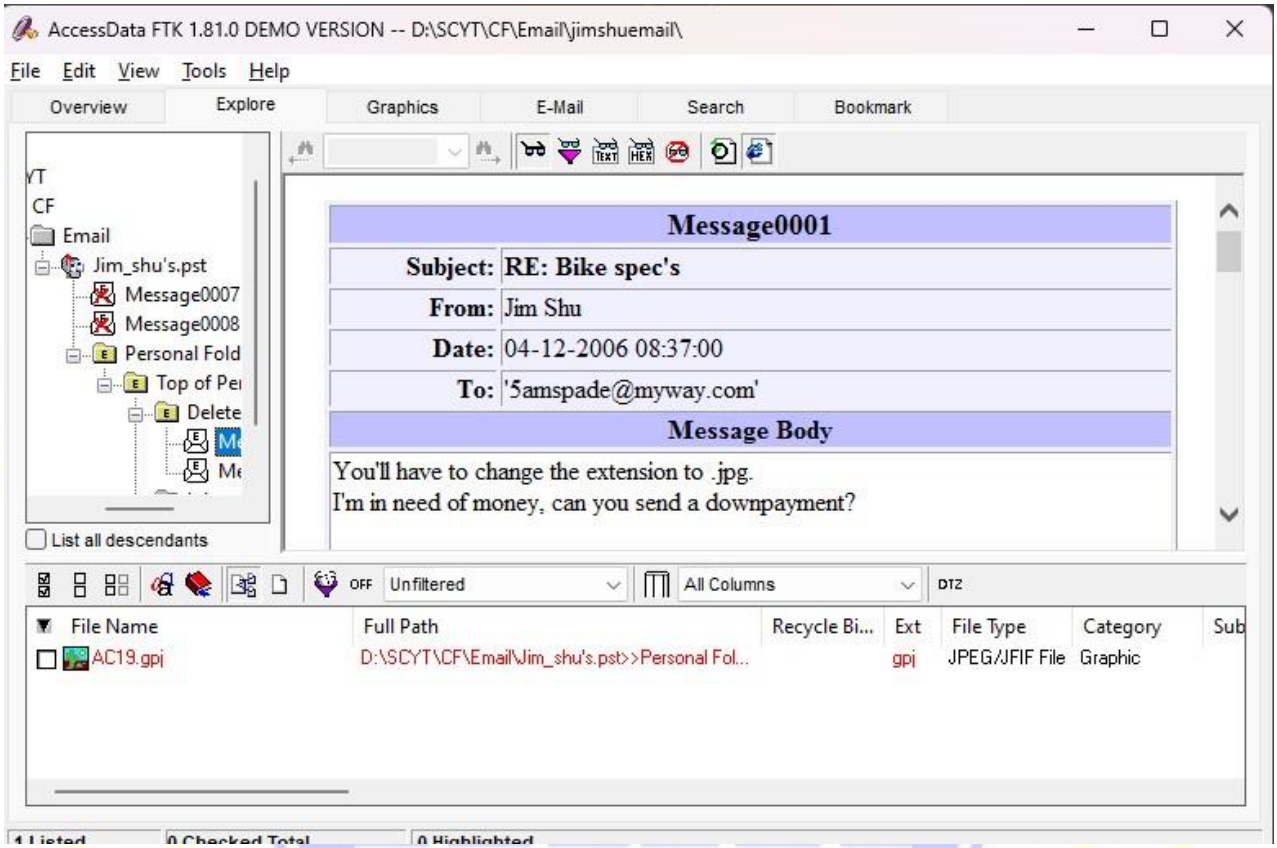




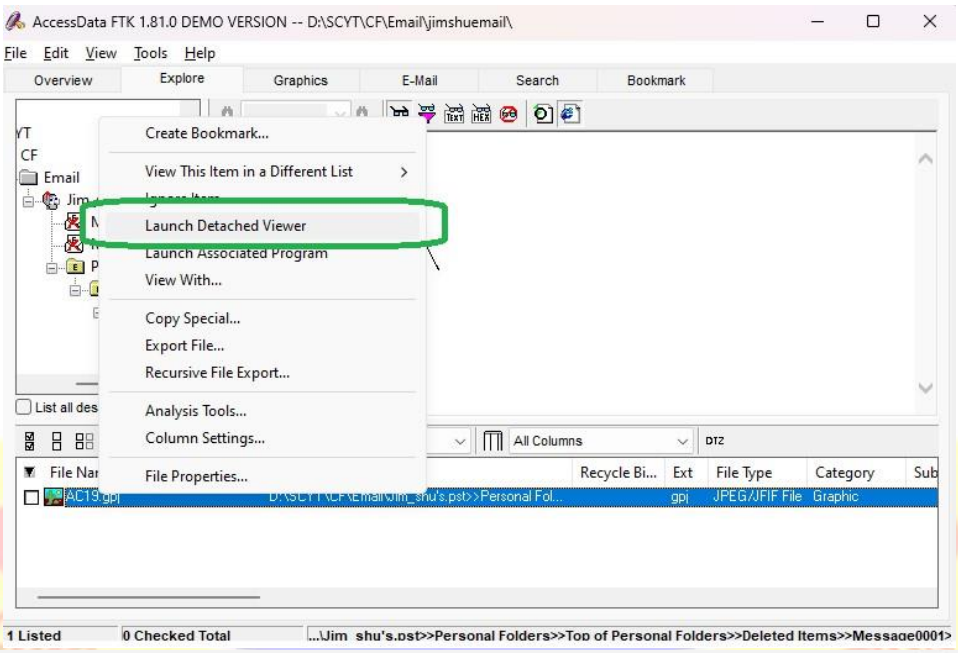
When the Add Evidence to Case dialog box opens, click Next. In the Case summary dialog box, click Finish. When FTK finishes processing the file, in the main FTK window, click the Email Messages button, and then click the Full Path column header to sort the records.

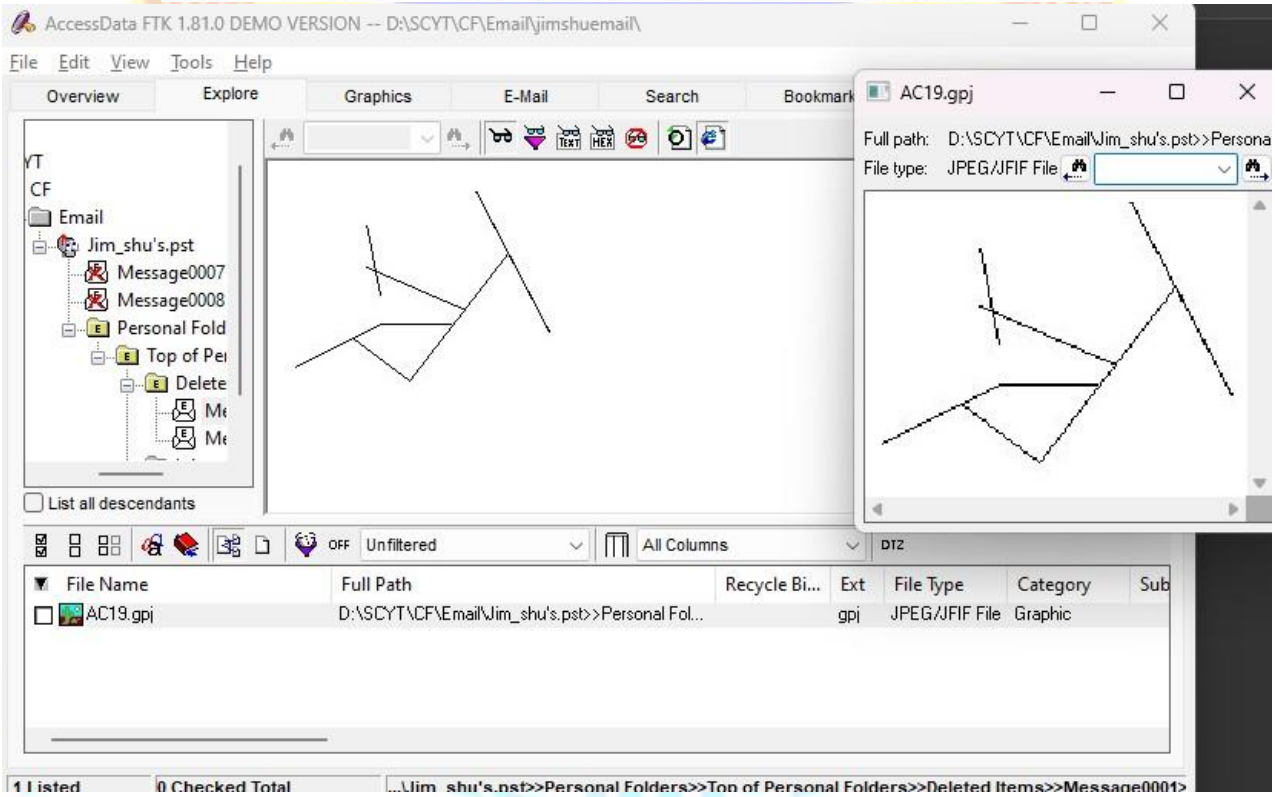


For email recovery follow following steps: Click the E-Mail tab. In the tree view, click to expand all folders, and then click the Deleted Items folder.

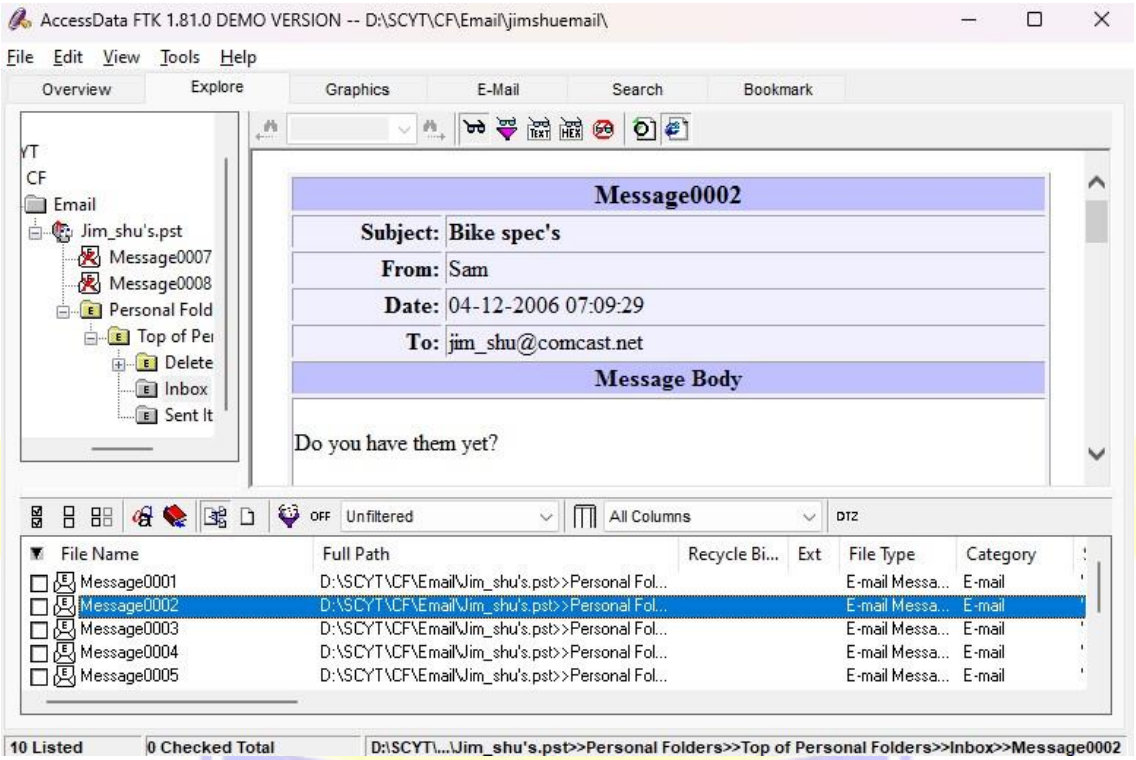


Select any message say Message0001 right click and select option Launch Detached Viewer and you can see detail of deleted message.

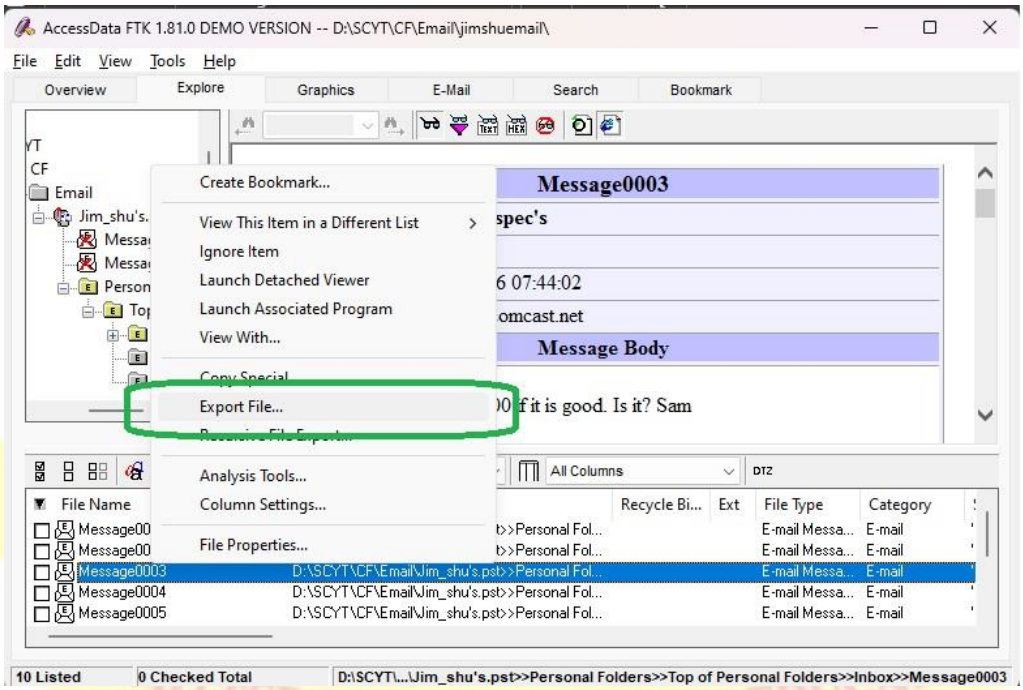


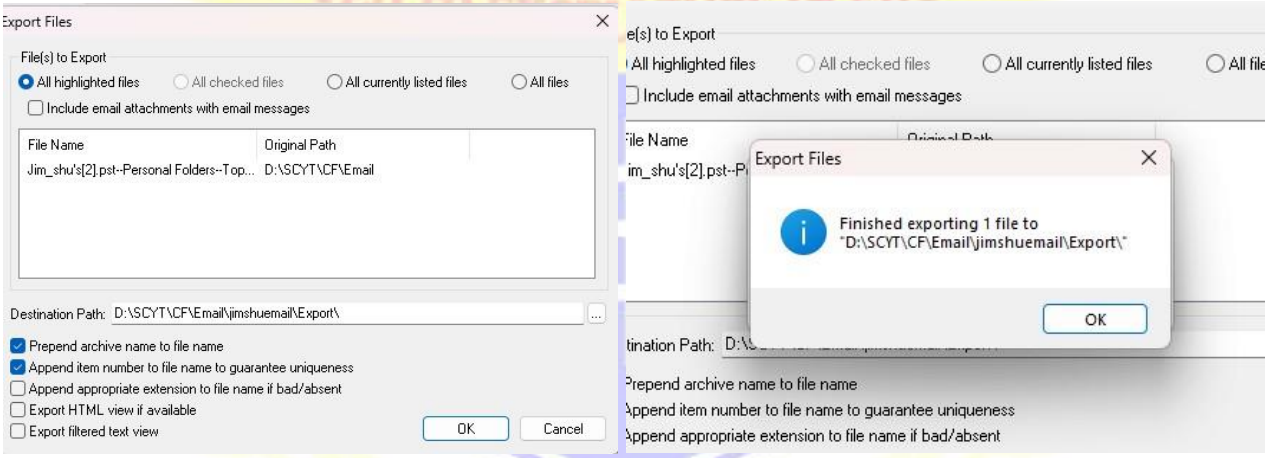


For analyzing header follow following steps: Click the E-Mail tab. In the tree view, click to expand all folders, and then click the Inbox folder. In the File List pane at the upper right, click Message0003; as shown in the pane at the bottom, it's from Sam and is addressed to Jim_shu@comcast.net.

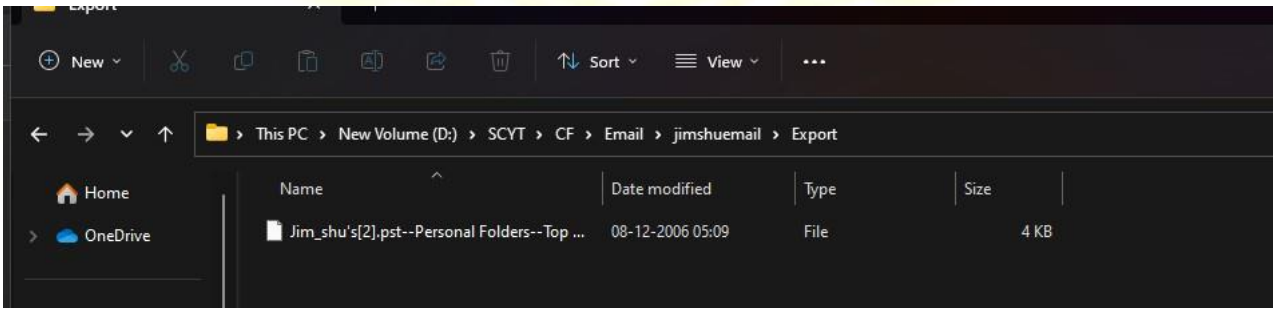


Right-click on any message say Message0003 in the File List pane and click Export File. In the Export Files dialog box, click OK.

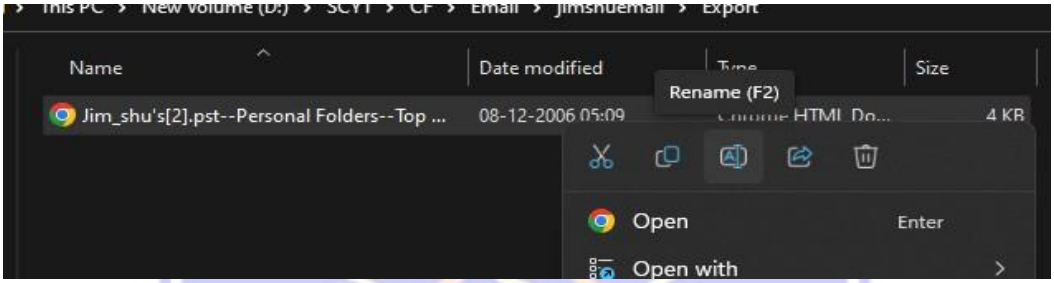


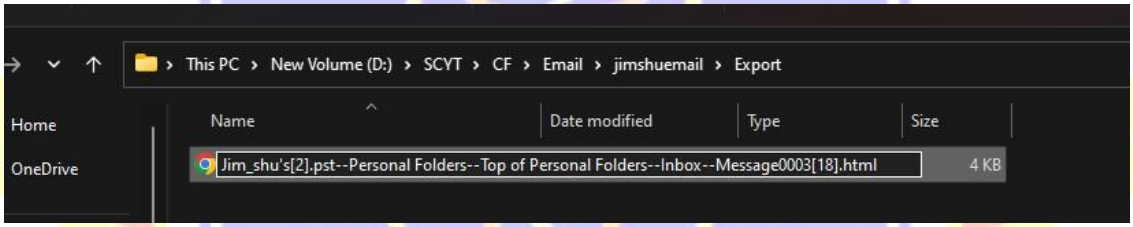


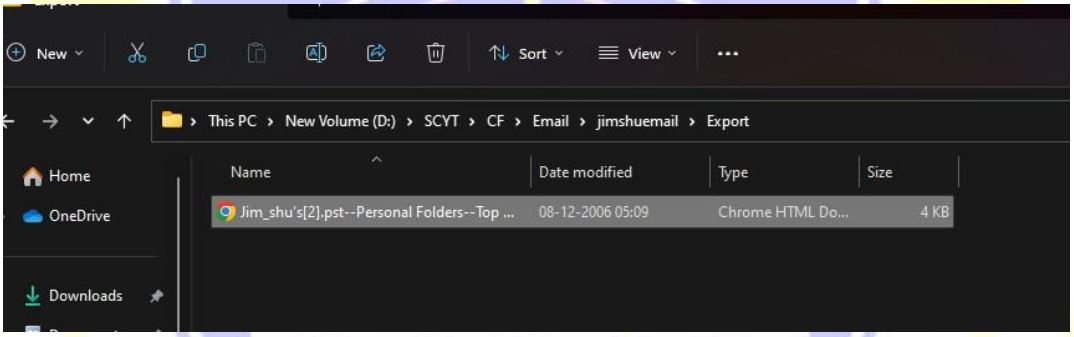
FTK saves exported files in the HTML format with no extension.



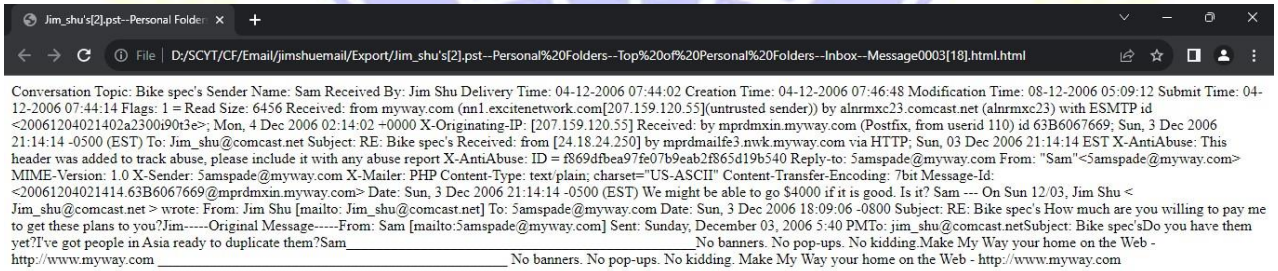
Right-click the Message0003 file and click Rename. Type Message0003.html and press Enter







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



Result:

Analyzing email headers and content allows forensic investigators to trace the origin of suspicious emails and identify potential forgeries or tampering, which is essential for cybersecurity investigations.

Learning Outcomes:

- Understand how to analyze email headers for forensic investigation.
- Learn to identify the origin and authenticity of emails through header analysis.
- Develop skills to detect potential email forgeries or tampering.

Course Outcomes:

- Gain practical knowledge of email forensics and its significance in investigations.
- Ability to interpret email headers and extract relevant information.
- Apply analytical techniques to assess the integrity of email communications.

Conclusion:

Viva Questions:

1. What information can be found in an email header?
2. How can you determine the authenticity of an email using its headers?
3. What are common signs of email forgery or tampering?
4. Why is email forensics important in cybersecurity investigations?

PRACTICAL NO: 10

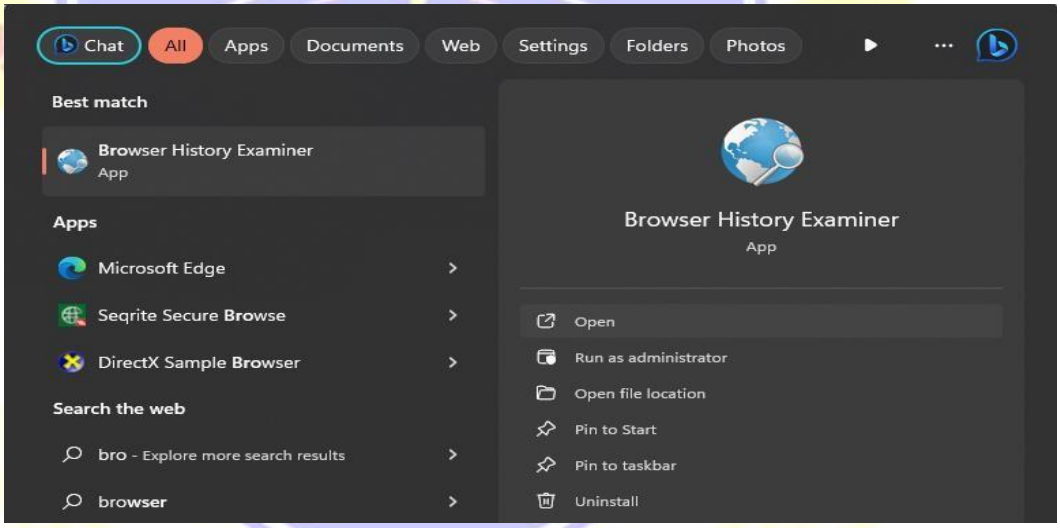
Aim:

Web Browser Forensics

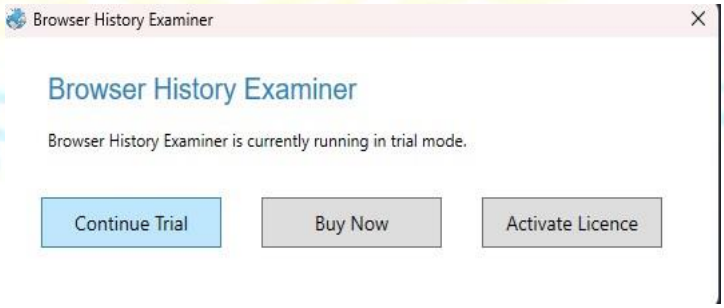
- Analyze browser artifacts, including history files, bookmarks, and download records.
- Analyze cache and cookies data to reconstruct user-browsing history and identify visited websites or online activities.
- Extract the relevant log or timestamp file, analyze its contents and interpret the timestamp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

Practical:

We are going to use the **Browser History Examiner** Run it as Administrator.

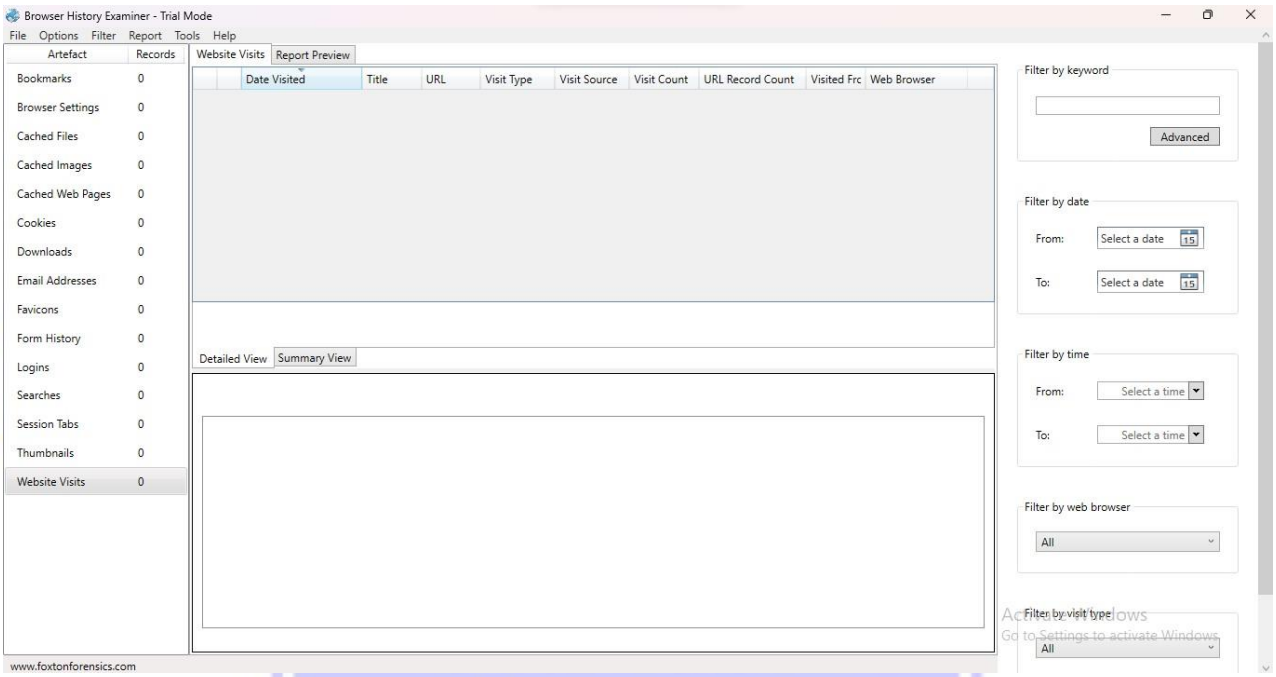


It is a **Paid Software** but has a **free–trail to get a total of 25 records from all the browsers in the device**



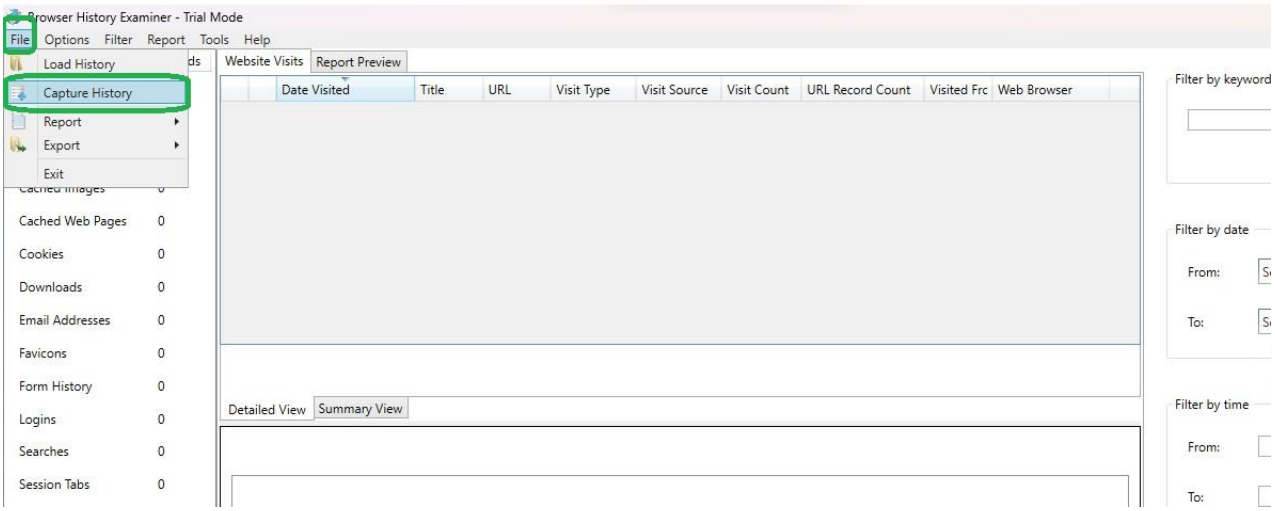
Click on Continue Trail

Click OK

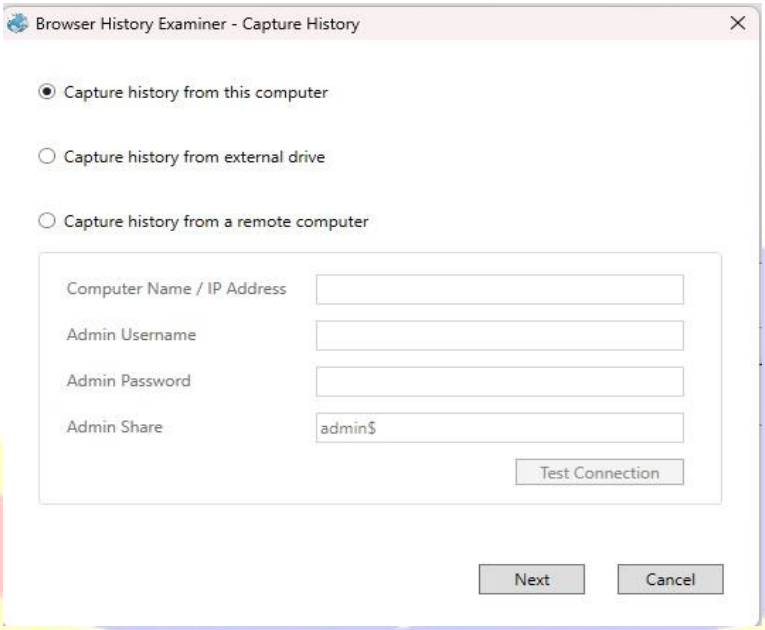


This is the Interface of the Application

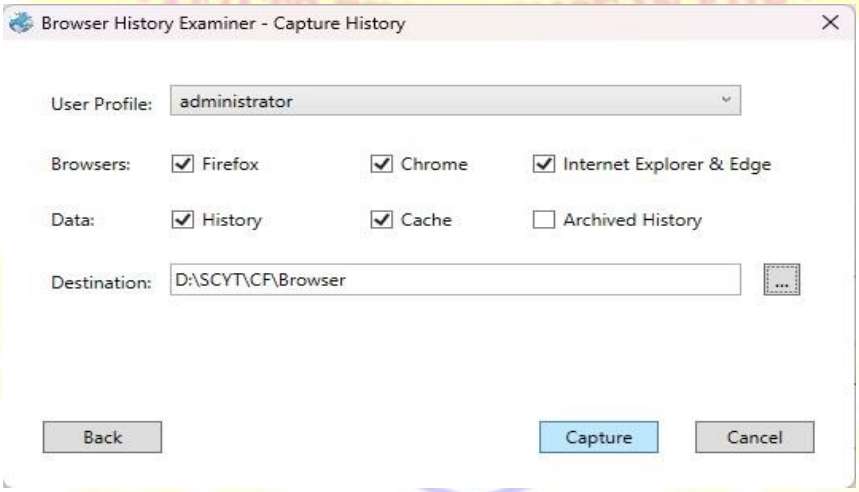
Go to File → Capture History

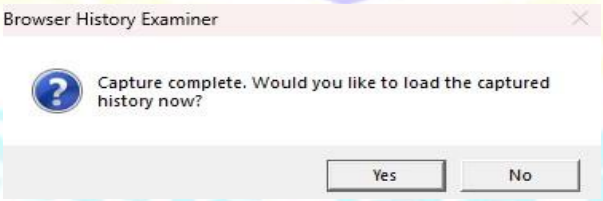


We are going to capture from this device only Select on that and click Next

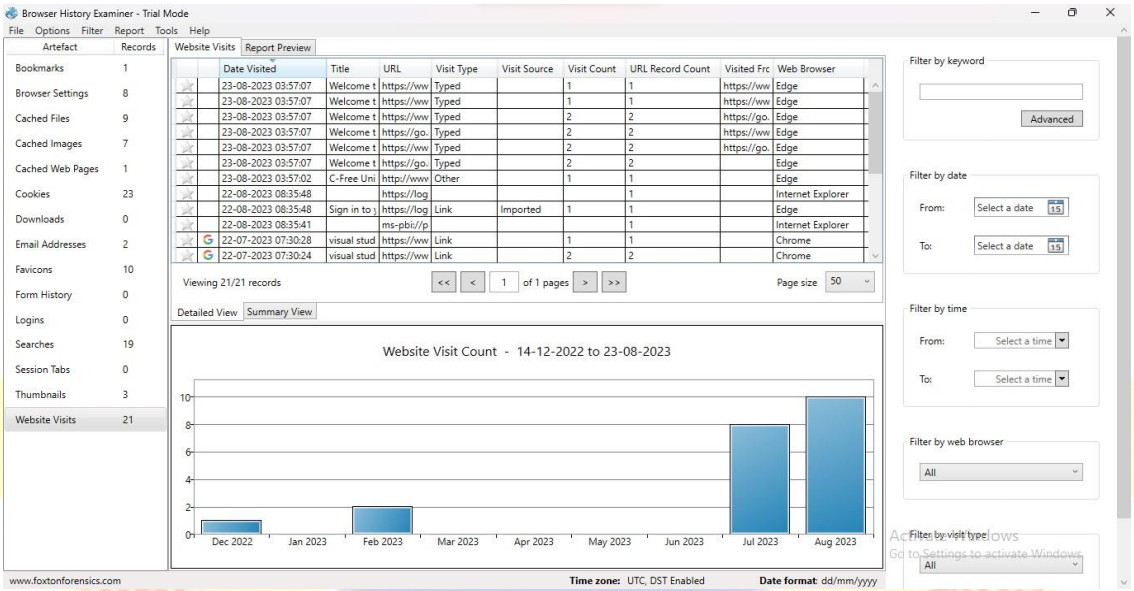


Select the Browser we want the history and give a directory to save those history extracted files

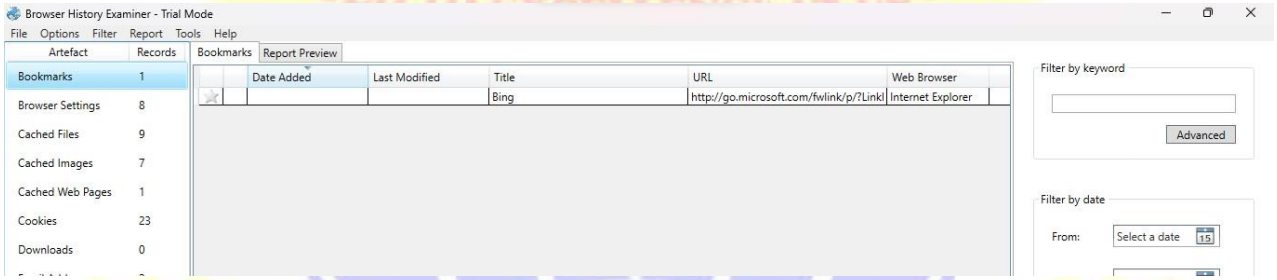




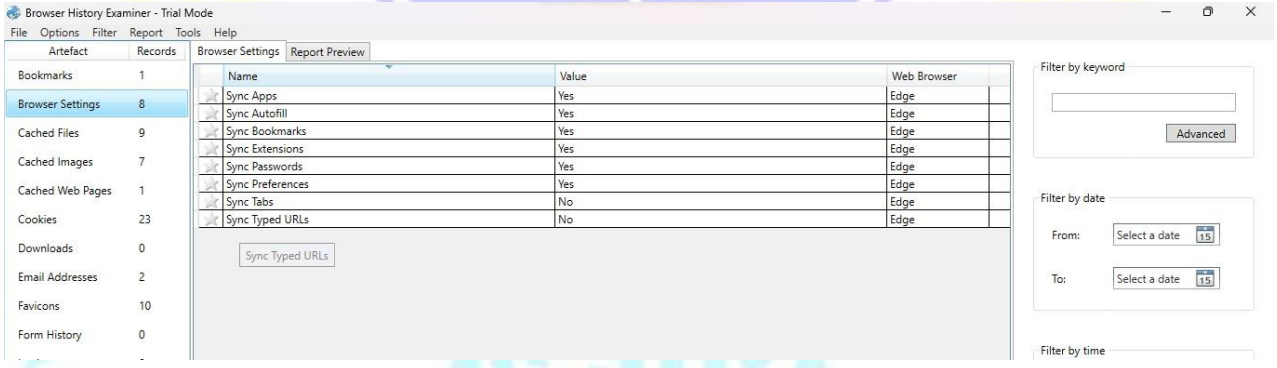
Here we can see the websites visited



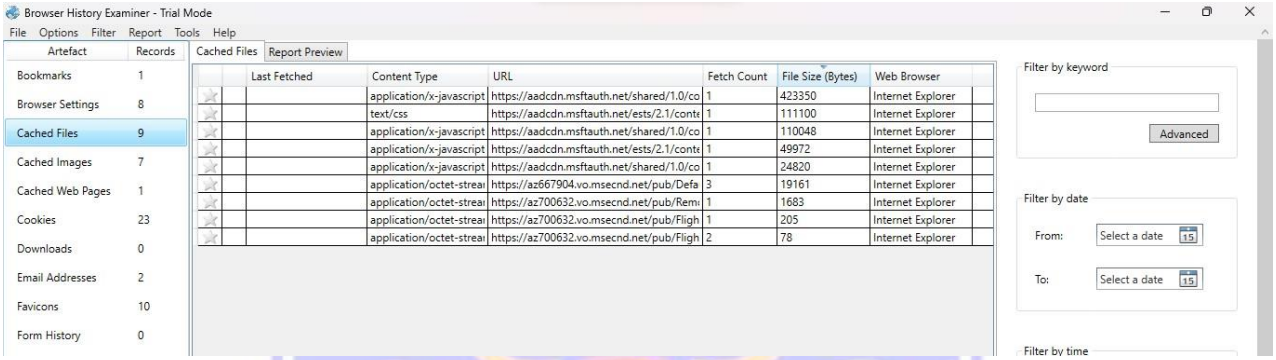
Here we can see the bookmarks



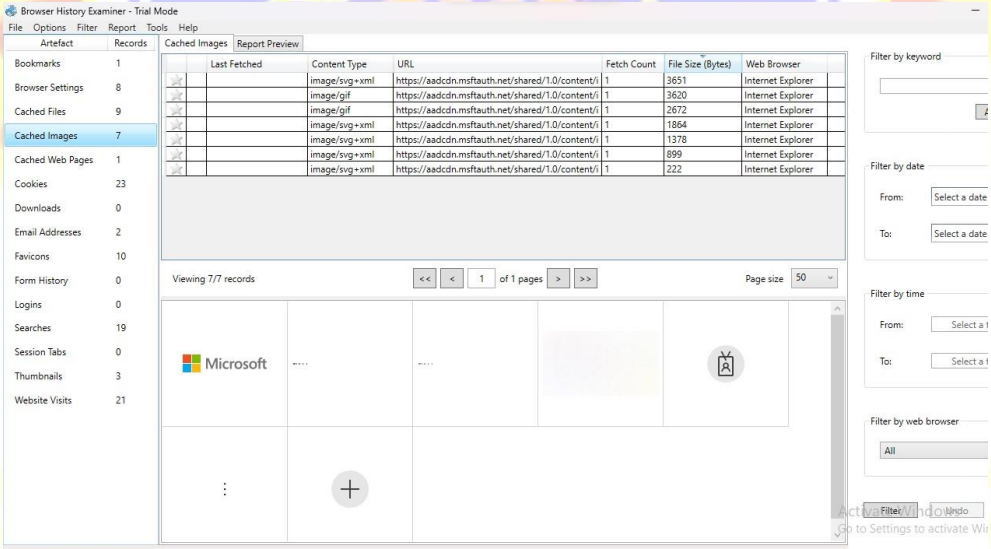
Here we can see the browser settings



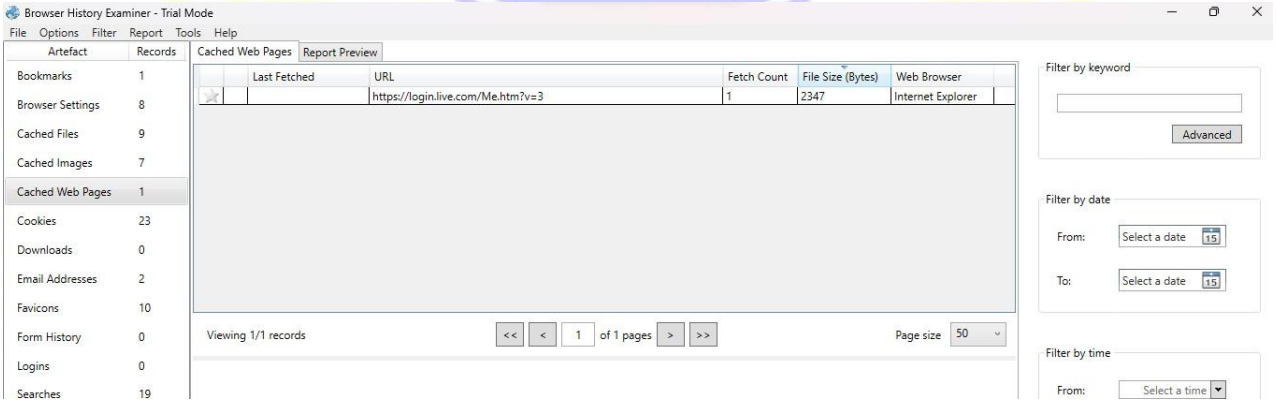
Here we can see the cached files



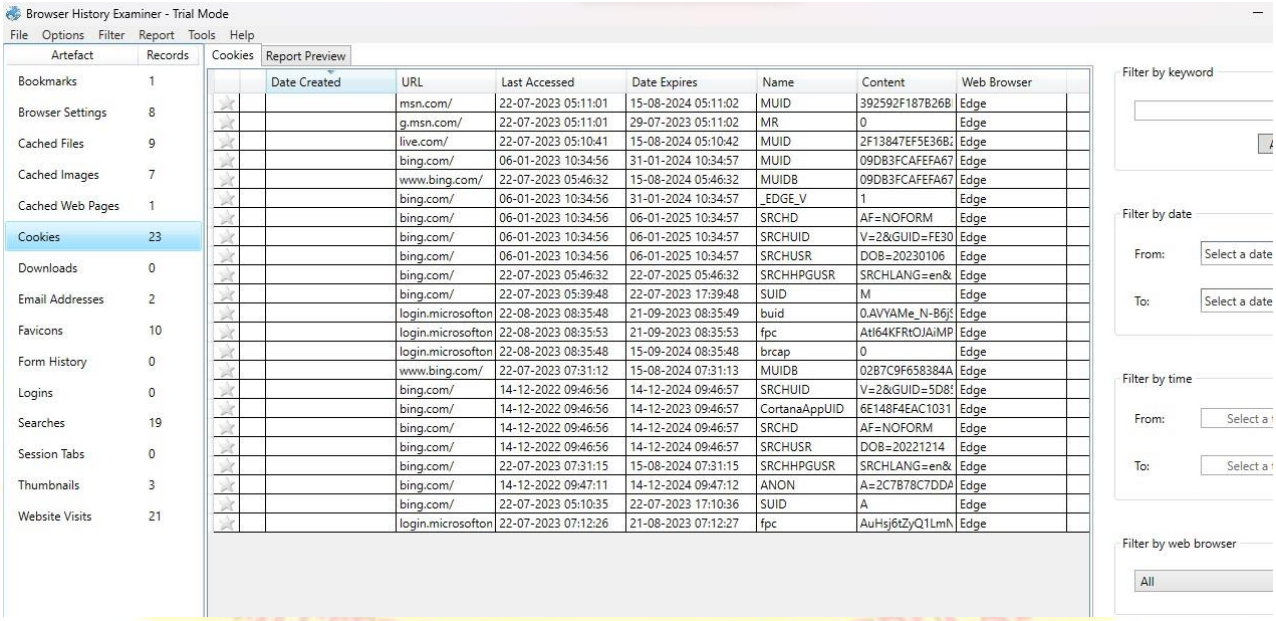
Here we can see the cached images



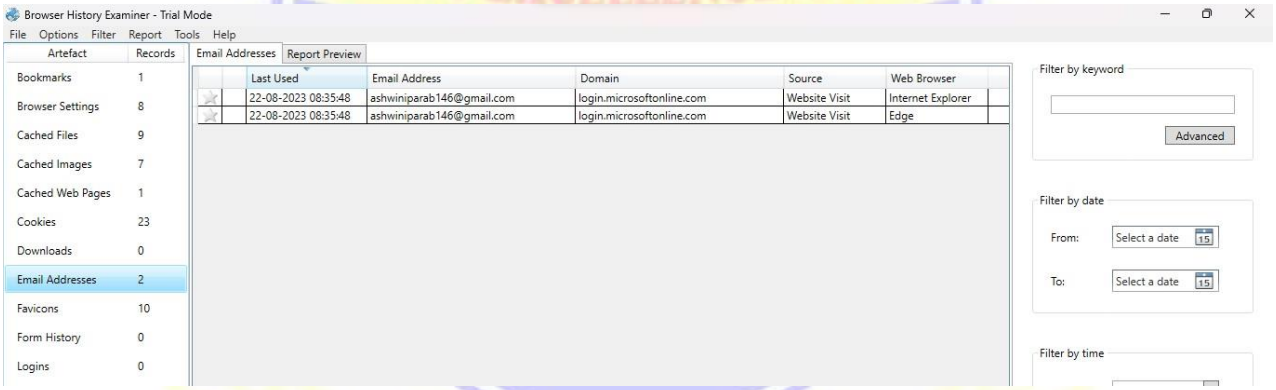
Here we can the cached webpages



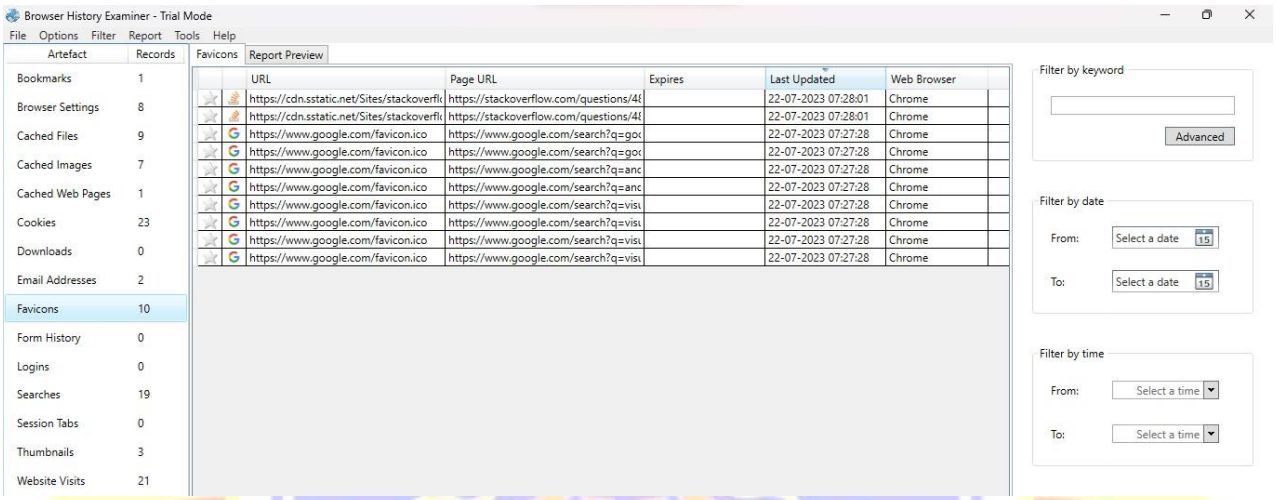
Here we can see the cookies stored



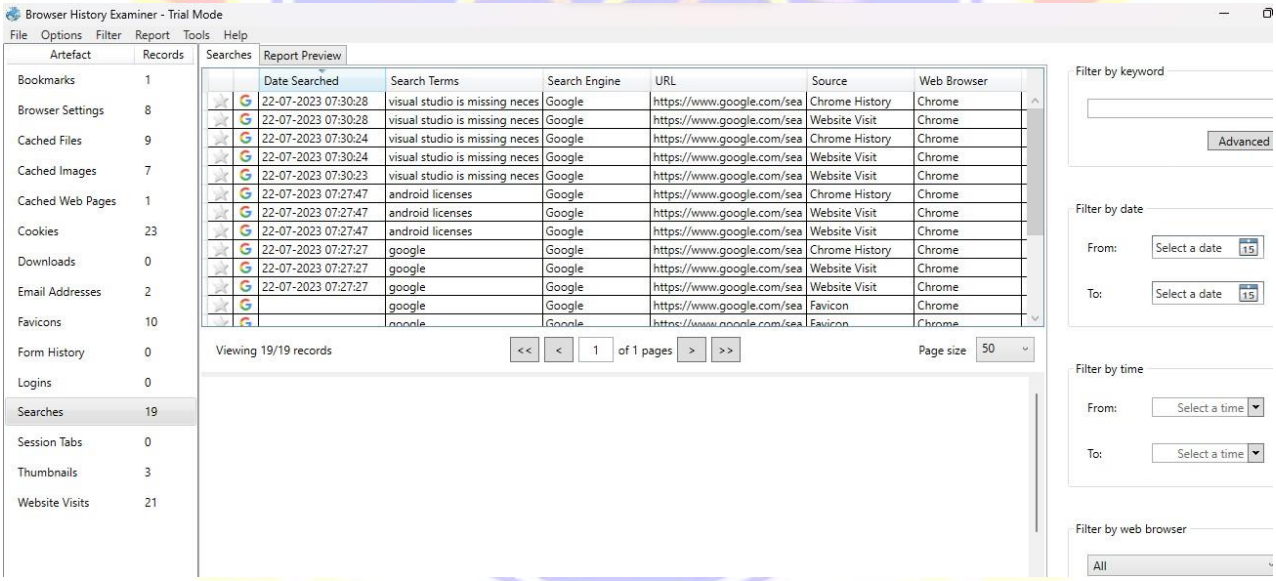
Here we can see the emails used for logins



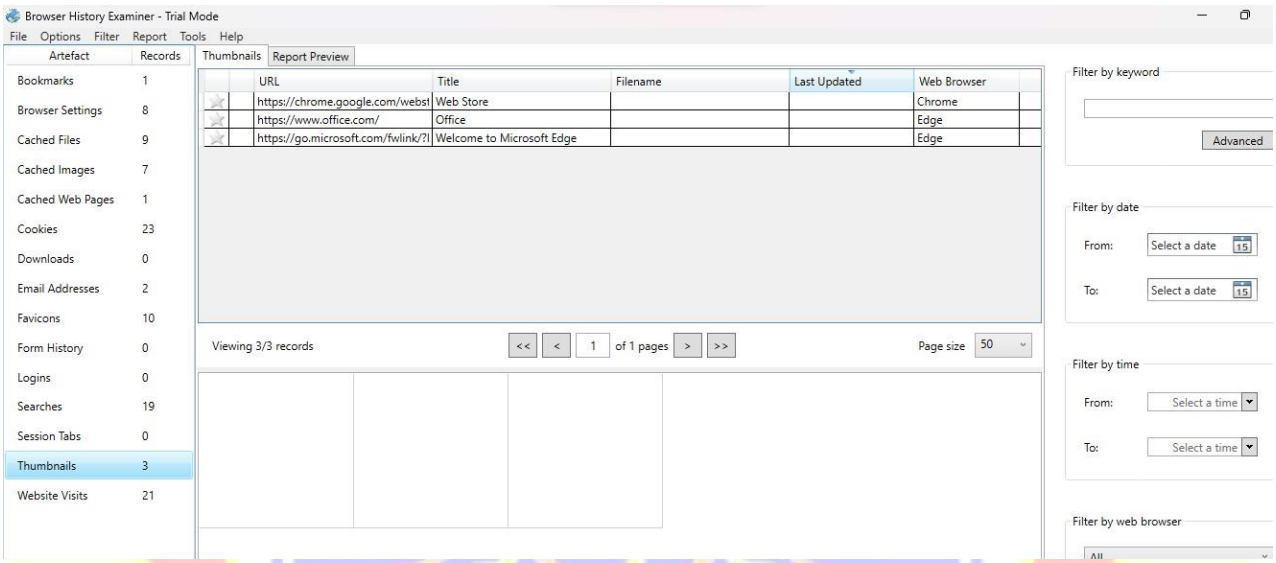
Here we can see the favicons



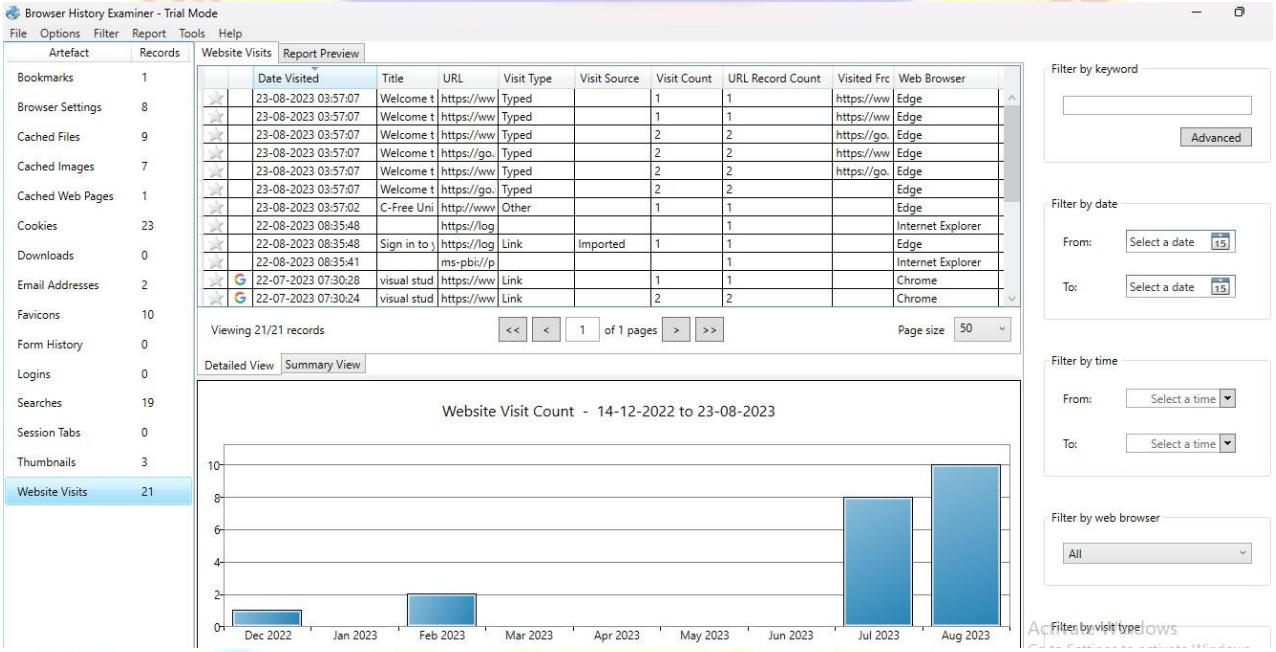
Here we can see the searches



Here we see the thumbnails



Here we can see the websites visits



Result:

Analyzing web browser artifacts, such as history files, bookmarks, and cache data, helps forensic investigators reconstruct user browsing history and identify online activities, which is vital for understanding user behavior.

Learning Outcomes:

- Understand how to analyze browser artifacts for forensic investigations.
- Learn to extract and interpret data from history files, bookmarks, and cache.
- Develop skills to reconstruct user browsing history to identify visited websites and online activities.

Course Outcomes:

- Gain practical knowledge of web browser forensics and its significance in investigations.
- Ability to analyze cache and cookie data to determine user behavior.
- Apply techniques to extract and interpret browser-related evidence effectively.

Conclusion:

Viva Questions:

1. What types of artifacts can be analyzed in web browser forensics?
2. How can cache data provide insights into user behavior?
3. What is the significance of analyzing bookmarks in a forensic investigation?
4. Why is reconstructing browsing history important in understanding online activities?