

INDEX

Sr No.	Practical
1	<p>Creating a Forensic Image using FTK Imager/Encase Imager :</p> <ul style="list-style-type: none">• Creating Forensic Image• Check Integrity of Data• Analyze Forensic Image
2	<p>Data Acquisition:</p> <ul style="list-style-type: none">• Perform data acquisition using:• USB Write Blocker + Encase Imager• SATA Write Blocker + Encase Imager• Falcon Imaging Device
3	<p>Analyze the memory dump of a running computer system.</p> <ul style="list-style-type: none">• Extract volatile data, such as open processes, network connections, and registry information.
4	<p>Capturing and analyzing network packets using Wireshark (Fundamentals) :</p> <ul style="list-style-type: none">• Identification the live network• Capture Packets• Analyze the captured packets
5	<p>Using Sysinternals tools for Network Tracking and Process Monitoring:</p> <ul style="list-style-type: none">• Check Sysinternals tools• Monitor Live Processes• Capture RAM• Capture TCP/UDP packets• Monitor Hard Disk• Monitor Virtual Memory• Monitor Cache Memory

6	<p>Recovering and Inspecting deleted files</p> <ul style="list-style-type: none"> • 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
7	<p>Steganography Detection</p> <ul style="list-style-type: none"> • Detect hidden information or files within digital images using steganography analysis tools. • Extract and examine the hidden content.
8	<p>Mobile Device Forensics</p> <ul style="list-style-type: none"> • 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.
9	<p>Email Forensics</p> <ul style="list-style-type: none"> • Analyze email headers and content to trace the origin of suspicious emails. • Identify potential email forgeries or tampering.
10	<p>Web Browser Forensics</p> <ul style="list-style-type: none"> • 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 NO. 1

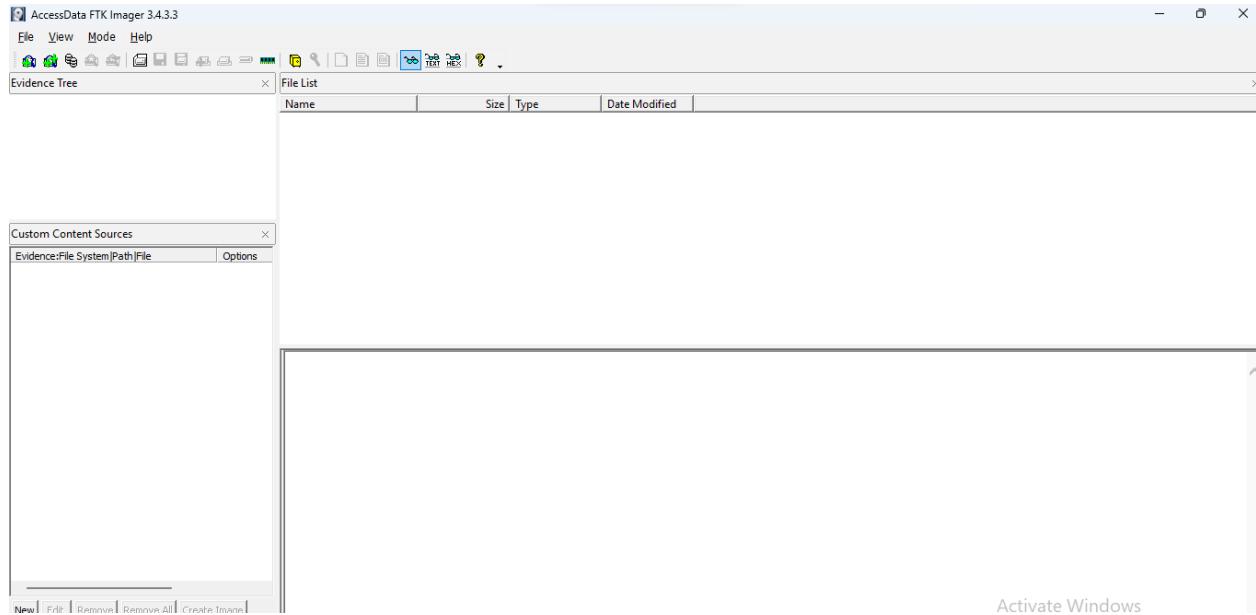
Aim:

Creating a Forensic Image using FTK Imager/Encase Imager:

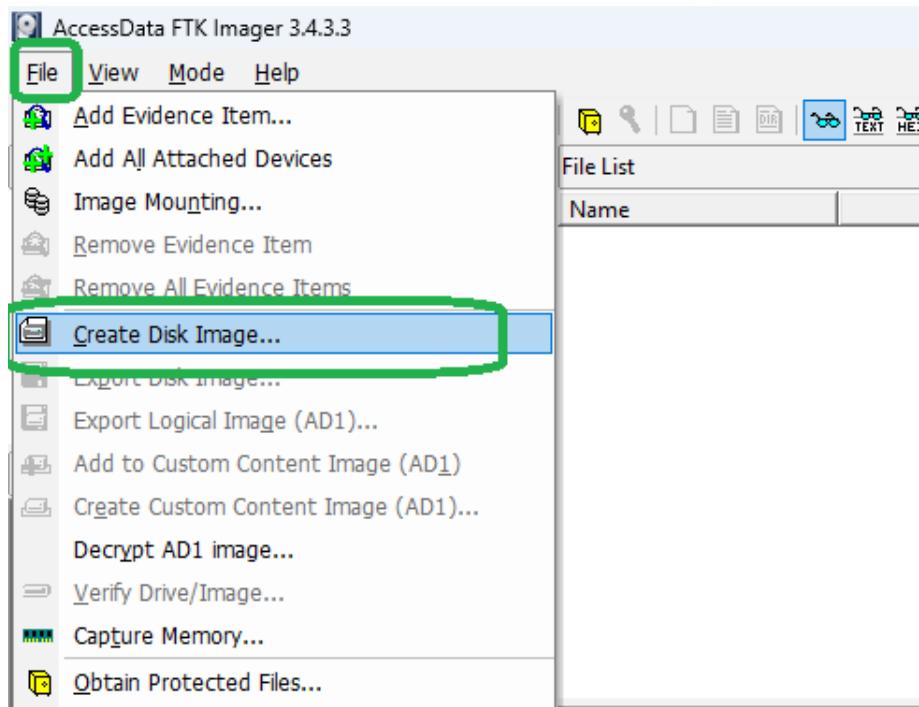
- Creating Forensic Image
- Check Integrity of Data
- Analyze Forensic Image

Practical:

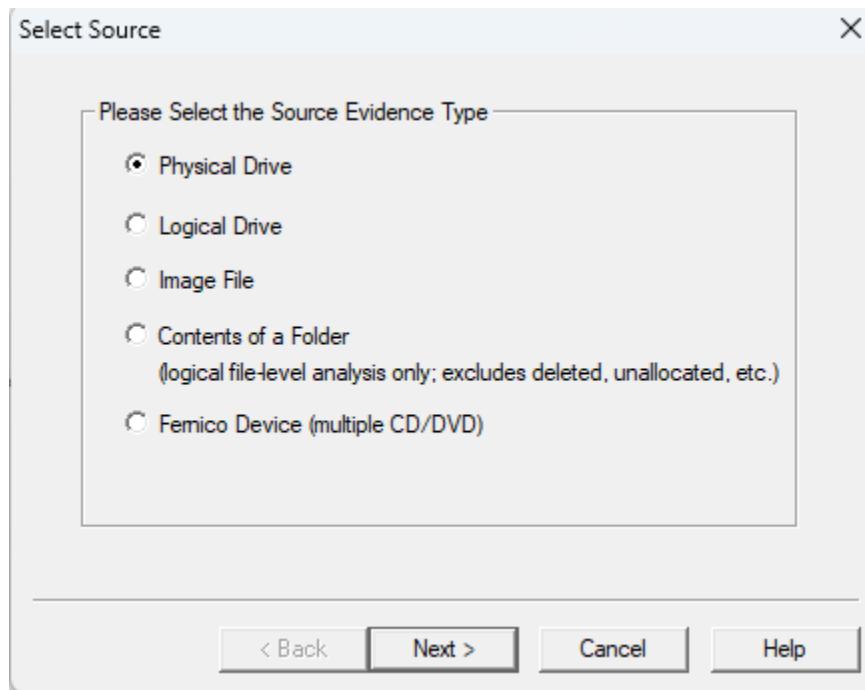
In this Practical we are going to use the FTK Imager to create Images of the evidences



Go to File → Create Disk Image

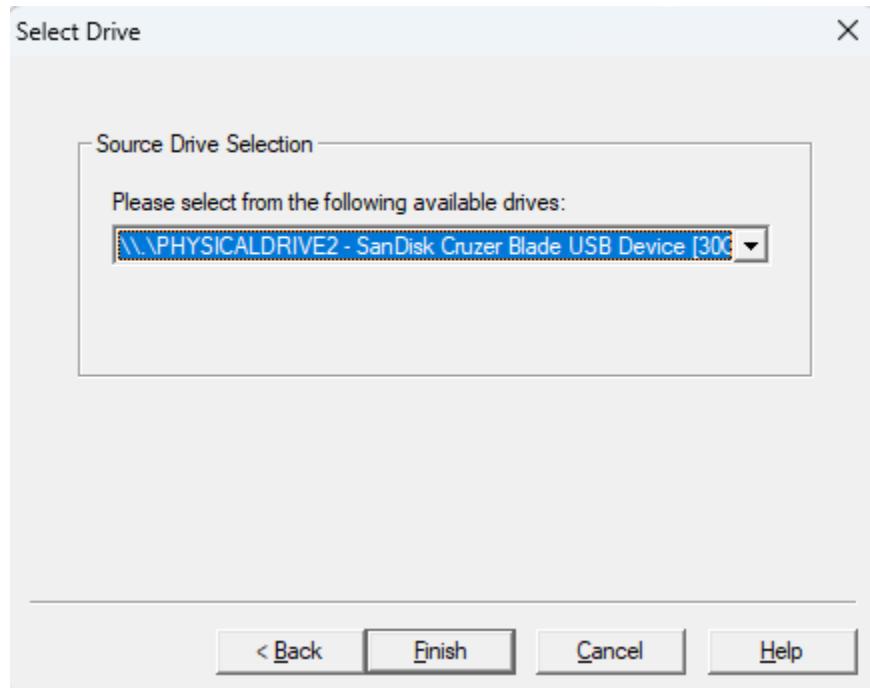


Select the source evidence type

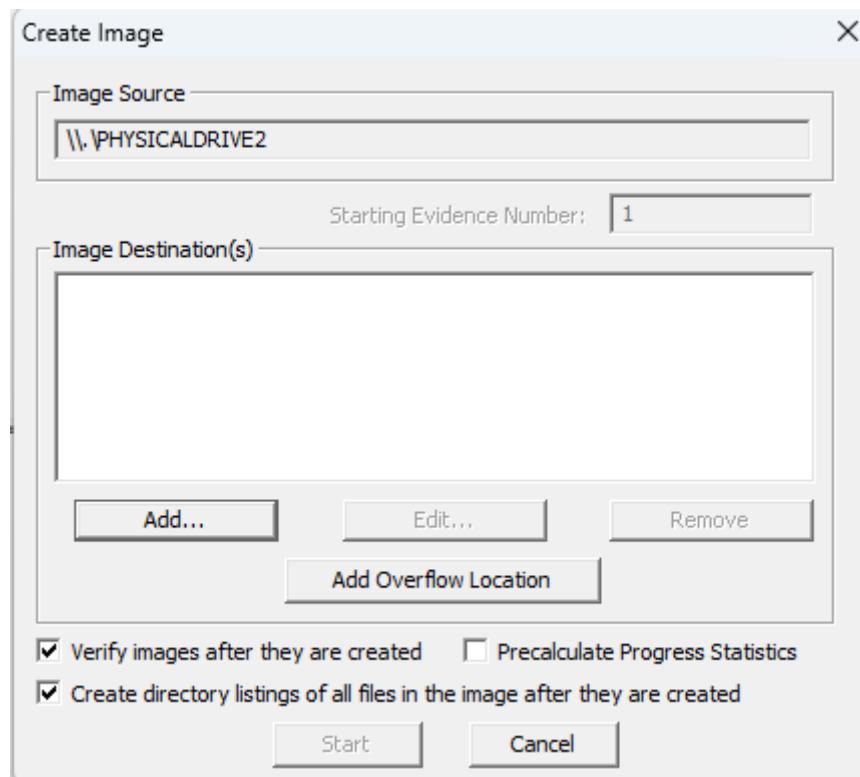


Here we are going to select the physical drive and proceed

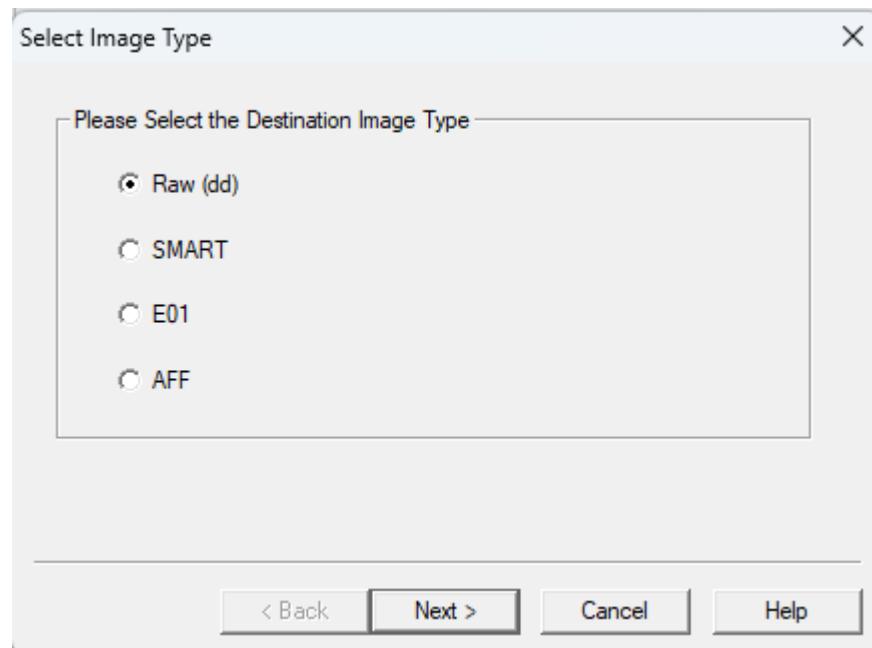
Then we browse the location of the **Pen drive** and click Finish



Now we add the location to create images



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

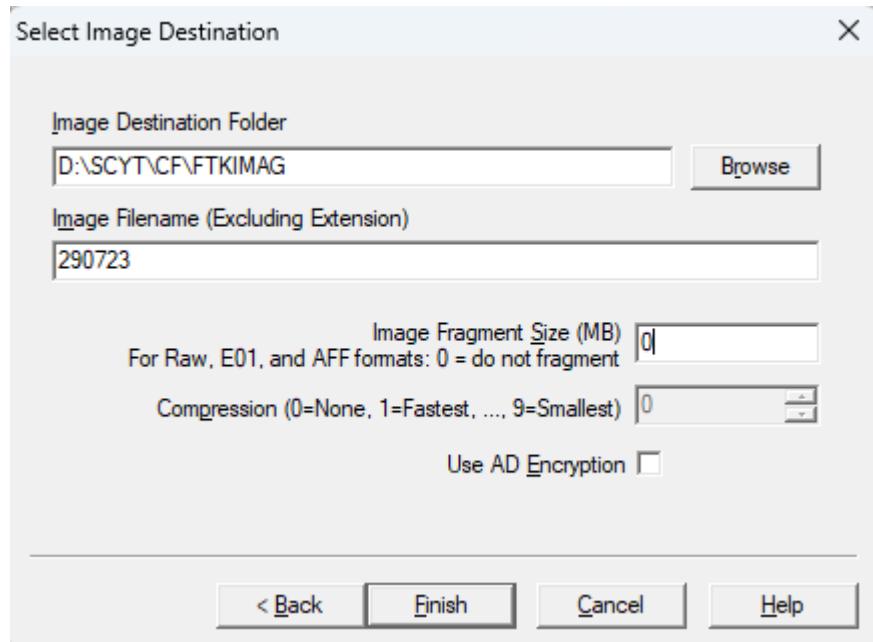


And now we fill the details required for the case

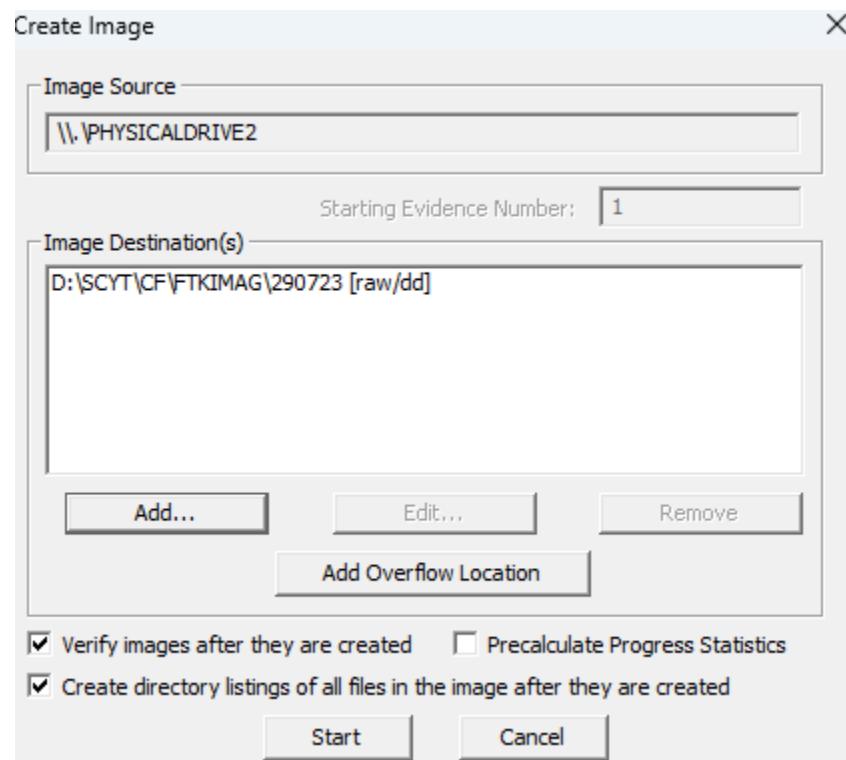
A dialog box titled "Evidence Item Information" with fields for Case Number (290723), Evidence Number (48), Unique Description (Sandisk Red & Black Colour 32GB), Examiner (Maddy), and Notes (New, Unused, Empty). At the bottom are buttons for "< Back", "Next >", "Cancel", and "Help".

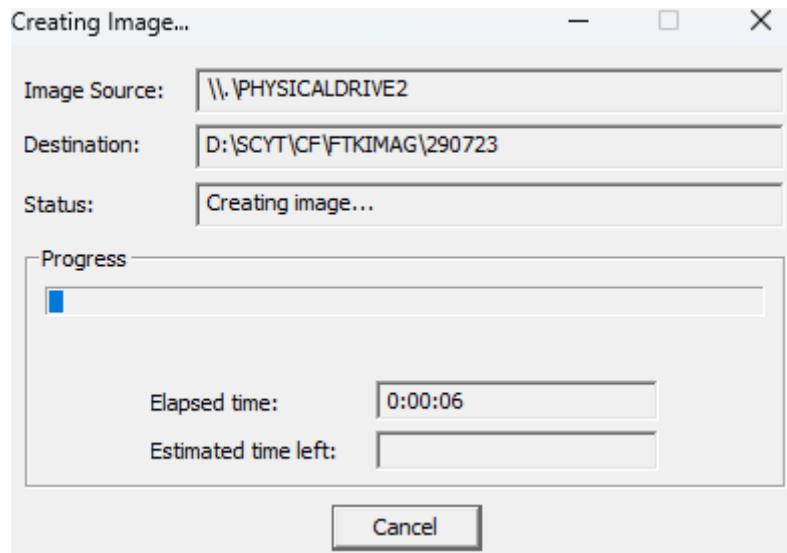
Create a folder to save the images to store in the system disk as the pen drive size cannot be stored in the same drive

Then paste that location to save the images and click Finish

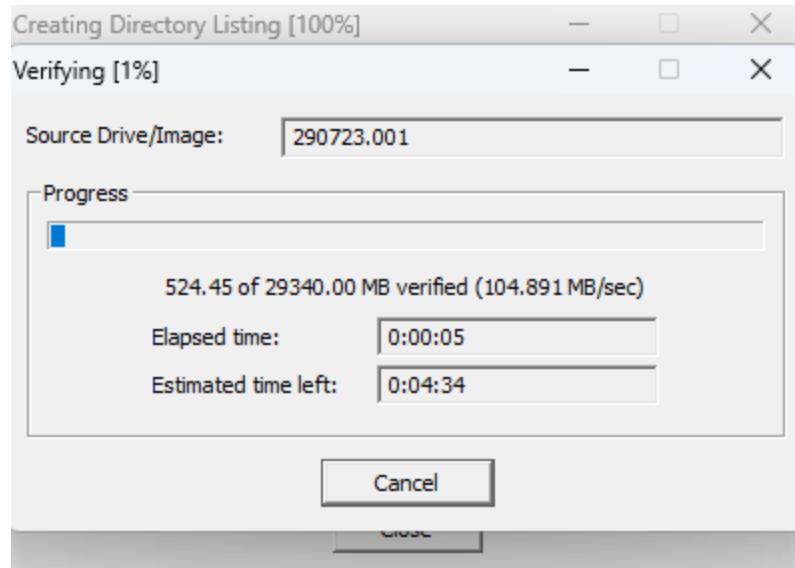


Then Click on Start and wait until the imaging is done





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

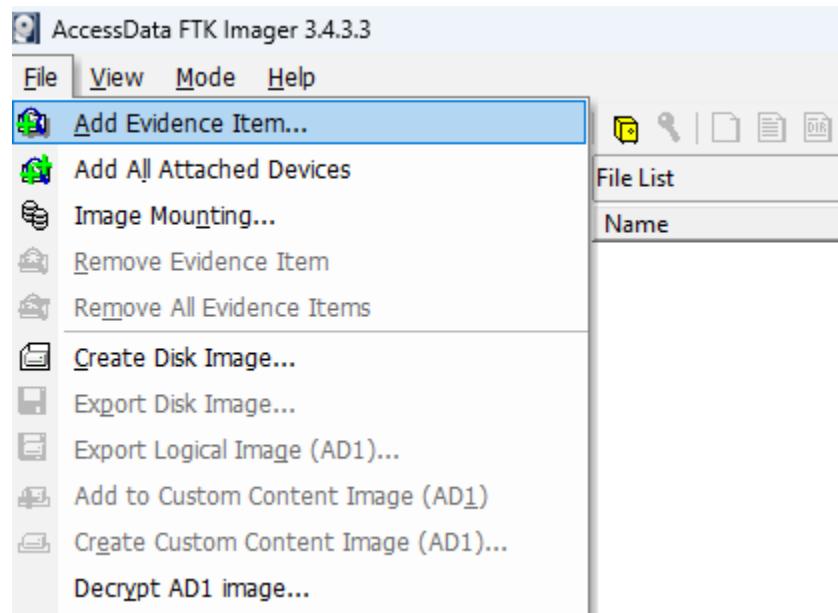
Drive/Image Verify Results	
Name	
Name	290723.001
Sector count	60088320
MD5 Hash	
Computed hash	592a08afa156587812828ff5df10164e
Report Hash	592a08afa156587812828ff5df10164e
Verify result	Match
SHA1 Hash	
Computed hash	82141f8b26552c9deff3d1caff1521ee8d
Report Hash	82141f8b26552c9deff3d1caff1521ee8d
Verify result	Match
Bad Sector List	
No bad sectors found.	
Close	

We take the image summary

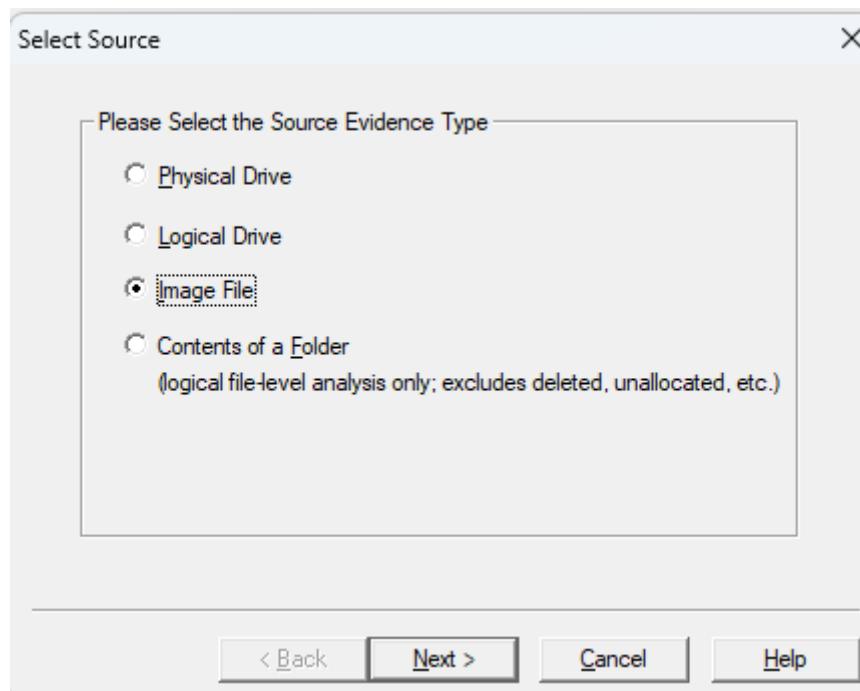
Image Summary	
Created By AccessData® FTK® Imager 3.4.3.3	
Case Information:	
Acquired using:	ADI3.4.3.3
Case Number:	290723
Evidence Number:	48
Unique description:	Sandisk Red & Black Colour 32GB
Examiner:	Maddy
Notes:	New, Unused, Empty
 Information for D:\SCYT\CF\FTKIMAG\290723:	
Physical Evidentiary Item (Source) Information:	
[Device Info]	
Source Type:	Physical
[Drive Geometry]	
Cylinders:	3,740
Tracks per Cylinder:	255
Sectors per Track:	63
Bytes per Sector:	512
Sector Count:	60,088,320
[Physical Drive Information]	
Drive Model:	SanDisk Cruzer Blade USB Device
OK	

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

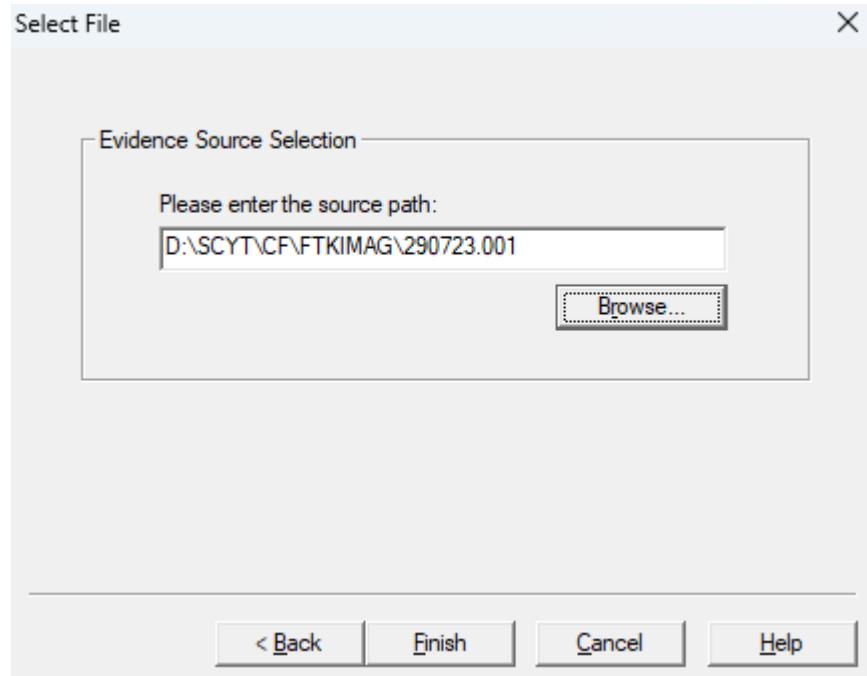
Go to File → Add Evidence Item



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 File List

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
IndexerVolumeGuid	1	Regular File	29-08-2023 10:...
IndexerVolumeGuid.Fi...	16	File Slack	
WPSettings.dat	1	Regular File	29-08-2023 10:...
WPSettings.dat.FileSlack	16	File Slack	

Custom Content Sources

Evidence:File System|Path|File Options

```

0000|2E 20 20 20 20 20 20 20-20 20 20 10 00 60 3D 57|. ....W
0010|1D 57 1D 57 00 00 40 57-1D 57 03 00 00 00 00 00 .W-W-BW-W.....
0020|2E 2E 20 20 20 20 20-20 20 20 10 00 60 3D 57.. ....W
0030|1D 57 1D 57 00 00 40 57-1D 57 00 00 00 00 00 00 .W-W-BW-W.....
0040|42 74 00 00 00 FF FF FF-FF FF FF OF 00 CE FF FF Bt...yyyyyy...yyy
0050|FF FF yyyy...yyyy...yyyy
0060|01 57 00 50 00 53 00 65-00 74 00 0F 00 CE 74 00 W-P-S-e-t...it.
0070|69 00 FF 00 67 00 73 00-2E 00 00 00 64 00 61 00 i-n-g-s...-da...
0080|57 50 53 45 54 54 7E 31-44 41 54 20 00 61 3D 57 WESETT-1DAT a-W
0090|1D 57 1D 57 00 00 40 57-1D 57 04 00 OC 00 00 00 .W-W-BW-W.....
00a0|42 47 00 75 00 69 00 64-00 00 00 0F 00 FF FF BG u-i-d...yyy
00b0|FF FF yyyy...yyyy...yyyy
00c0|01 49 00 6E 00 64 00 65-00 78 00 0F 00 FF 65 00 I-n-d-e-x...ye...
00d0|72 00 56 00 6F 00 6C 00-75 00 00 00 ED 00 65 00 r-V-o-l-u-m-e...
00e0|49 4E 44 45 58 45 7E 31-20 20 20 20 10 41 57 INDEXE-1 ..AW
00f0|1D 57 1D 57 00 00 42 57-1D 57 05 00 4C 00 00 00 .W-W-BW-W-L...
0100|00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... .
0110|00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... .

```

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 Softwares

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

https://www.amazon.com/usb-write-blocker/s?k=usb+write+blocker&language=en_US¤cy=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-encase-forensic-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>

The screenshot shows the Encase Forensic software interface. The top menu bar includes File, Edit, View, Tools, Help, New, Open, Save, Print, Add Device, Search, Logon, Refresh, Show Excluded, Show Deleted, Delete, and View History. Below the menu is a toolbar with icons for Cases, Text Styles, Table, Report, Gallery, Timeline, Disk, and Code. A navigation pane on the left displays a tree structure of cases, with the 'History' node expanded to show sub-folders like Internet and Email, Internet Explorer, Mozilla, and Opera. The main area features a table with columns: Name, URL, Host, User, Visit Count, and First Date. The table lists 25 entries, with row 18 selected. The details panel at the bottom provides specific information for the selected entry:

Name	URL	Host	User	Visit Count	First Date
16	http://start.mozilla.org/firefox?d1 start.mozilla.org	PC User	6	02/04/05 04:07:42PM	
17	http://webmail.netscape.com/_cc webmail.netscape.com	PC User	2	02/04/05 04:08:28PM	
18	http://webmail.netscape.com/ms; webmail.netscape.com	PC User	2	02/04/05 04:12:58PM	
19	http://webmail.netscape.com/ms; webmail.netscape.com	PC User	2	02/04/05 04:08:47PM	
20	http://webmail.netscape.com/con webmail.netscape.com	PC User	2	02/04/05 04:13:25PM	
21	http://webmail.netscape.com/con webmail.netscape.com	PC User	8	02/04/05 04:16:42PM	
22	http://webmail.netscape.com/ms; webmail.netscape.com	PC User	2	02/04/05 04:12:30PM	
23	http://webmail.netscape.com/ms; webmail.netscape.com	PC User	2	02/04/05 04:10:58PM	
24	http://webmail.netscape.com/ms; webmail.netscape.com	PC User	8	02/04/05 04:14:08PM	
25	http://webmail.netscape.com/_cc webmail.netscape.com	PC User	2	02/04/05 04:08:28PM	

Details panel (bottom):

- URL: http://webmail.netscape.com/msgview.adp?folder=SW5ib3g=&uid=223796
- Host: webmail.netscape.com
- User: PC User
- Visit Count: 2
- First Date: 02/04/05 04:12:58PM
- History Path: Internet and Email\Active\Documents and Settings\PC User\Application Data\Mozilla\Firefox\Profiles\03fh4udv.default\history.dat

Bottom status bar: Internet\Internet and Email\Active\Documents and Settings\PC User\Application Data\Mozilla\Firefox\Profiles\03fh4udv.default\history.dat (PS 1919634 LS 1919571 CL 479892 SO 358 FO 5990 LE 0)

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/cftt-technical/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-forensic-falcon-neo/>

<https://www.forensicfocus.com/articles/how-to-use-the-file-browser-feature-in-logicubes-forensic-falcon-neo/>

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

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



PRACTICAL NO. 3

Aim:

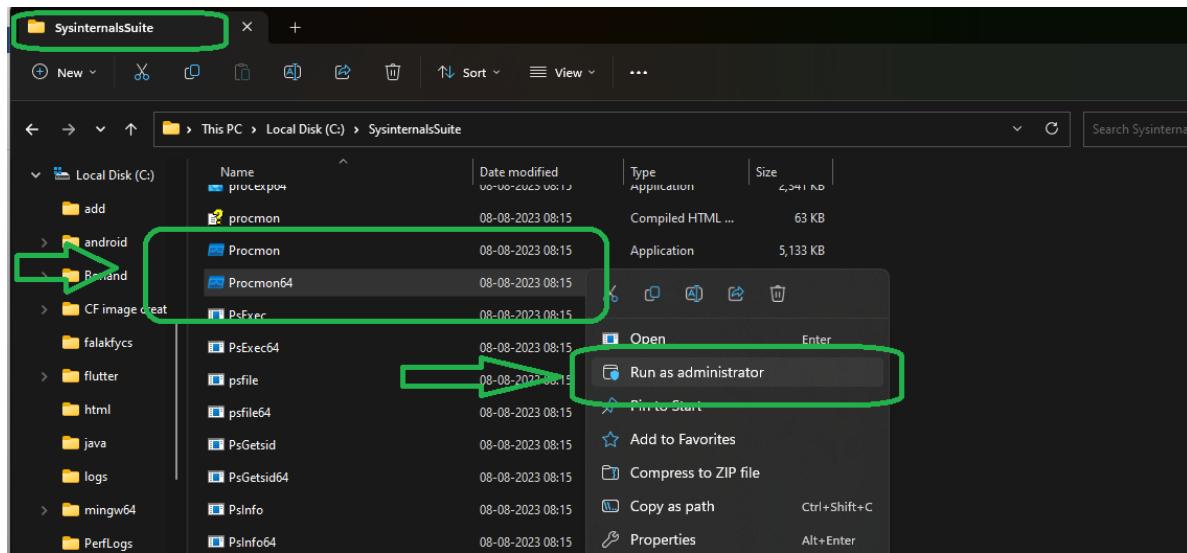
Analyze the memory dump of a running computer system.

- 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

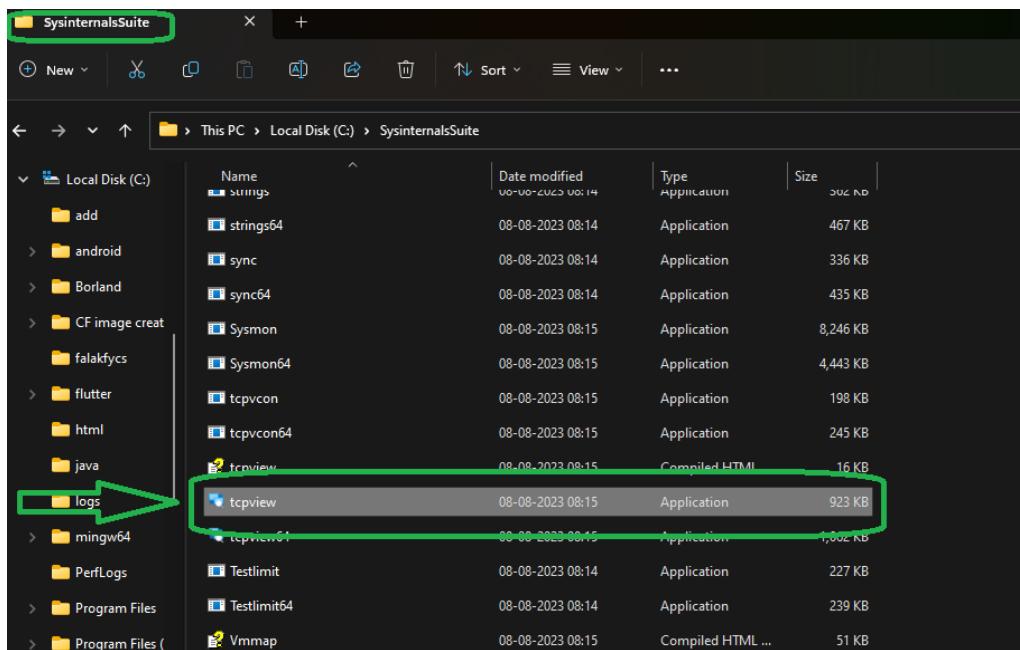


Process Monitor - Sysinternals: www.sysinternals.com

Time ...	Process Name	PID	Operation	Path	Result	Detail
08:27:...	svchost.exe	2644	ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset: 704512, Le...
08:27:...	Explorer.EXE	11808	ReadFile	C:\Windows\System32\MmCoreR.dll	SUCCESS	Offset: 995328, Le...
08:27:...	svchost.exe	2644	ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset: 692224, Le...
08:27:...	Explorer.EXE	11808	ReadFile	C:\Windows\System32\MmCoreR.dll	SUCCESS	Offset: 925696, Le...
08:27:...	svchost.exe	1656	UDP Receive	f02:fb:5353->fe80:2050:4fce:b495:8...	SUCCESS	Length: 30, sequu...
08:27:...	chrome.exe	9724	UDP Receive	f02:fb:5353->fe80:2050:4fce:b495:8...	SUCCESS	Length: 30, sequu...
08:27:...	svchost.exe	2644	ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset: 647168, Le...
08:27:...	Explorer.EXE	11808	QueryBasicInfor...	C:\Program Files\Windows Apps\Clipcha...	SUCCESS	CreationTime: 13:0...
08:27:...	Explorer.EXE	11808	ReadFile	C:\Program Files\Windows32\Taskbar.dll	SUCCESS	Offset: 2406400, L...
08:27:...	Explorer.EXE	11808	CloseFile	C:\Program Files\Windows Apps\Clipcha...	SUCCESS	
08:27:...	svchost.exe	2644	ReadFile	C:\Windows\System32\Reg...	Success	Offset: 638976, Le...
08:27:...	Explorer.EXE	11808	RegCloseKey	HKU\S-1-5-21-3130516669-347735452...	SUCCESS	
08:27:...	Explorer.EXE	11808	RegOpenKey	HKU\S-1-5-21-3130516669-347735452...	SUCCESS	Desired Access: R...
08:27:...	Explorer.EXE	11808	RegQueryKey	HKU\S-1-5-21-3130516669-347735452...	SUCCESS	Query: HandleTag...
08:27:...	Explorer.EXE	11808	RegOpenKey	HKU\S-1-5-21-3130516669-347735452...	REPARSE	Desired Access: R...
08:27:...	svchost.exe	2644	ReadFile	C:\Windows\System32\Windows.State...	SUCCESS	Offset: 6500352, L...
08:27:...	Explorer.EXE	11808	RegOpenKey	HKU\S-1-5-21-3130516669-347735452...	SUCCESS	Desired Access: R...
08:27:...	Explorer.EXE	11808	RegCloseKey	HKU\S-1-5-21-3130516669-347735452...	SUCCESS	Offset: 2718208, L...
08:27:...	Explorer.EXE	11808	ReadFile	C:\Windows\System32\Taskbar.dll	SUCCESS	
08:27:...	Explorer.EXE	11808	RegQueryValue	HKU\S-1-5-21-3130516669-347735452...	NAME NOT FOUND	Length: 12
08:27:...	Explorer.EXE	11808	RegCloseKey	HKU\S-1-5-21-3130516669-347735452...	SUCCESS	
08:27:...	Explorer.EXE	11808	ReadFile	C:\Windows\System32\BCP47mm.dll	SUCCESS	Offset: 180224, Le...
08:27:...	lsass.exe	1020	ReadFile	C:\Windows\System32\lsassv.dll	SUCCESS	Offset: 1540096, L...
08:27:...	svchost.exe	2644	ReadFile	C:\Windows\System32\Windows.State...	SUCCESS	Offset: 6434816, L...
08:27:...	Explorer.EXE	11808	ReadFile	C:\Windows\System32\Taskbar.dll	SUCCESS	Offset: 2529280, L...
08:27:...	lsass.exe	1020	ReadFile	C:\Windows\System32\lsassv.dll	SUCCESS	Offset: 1523712, L...
08:27:...	Explorer.EXE	11808	ReadFile	C:\Windows\System32\BCP47mm.dll	SUCCESS	Offset: 155648, Le...
08:27:...	svchost.exe	2644	ReadFile	C:\Windows\System32\Windows.State...	SUCCESS	Offset: 2512896, L...
08:27:...	lsass.exe	1020	ReadFile	C:\Windows\System32\lsassv.dll	SUCCESS	Offset: 6414336, L...
08:27:...	Explorer.EXE	11808	RegOpenKey	HKU\S-1-5-21-3130516669-347735452...	SUCCESS	Desired Access: R...
08:27:...	Explorer.EXE	11808	ReadFile	C:\Windows\SystemApps\Microsoft.Win...	SUCCESS	Offset: 6227968, L...
08:27:...	Explorer.EXE	11808	RegQueryKey	HKU\S-1-5-21-3130516669-347735452...	SUCCESS	Query: HandleTag...
08:27:...	Explorer.EXE	11808	RegOpenKey	HKU\S-1-5-21-3130516669-347735452...	REPARSE	Desired Access: R...
08:27:...	svchost.exe	2644	LockFile	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	Desired Access: R...
08:27:...	Explorer.EXE	11808	RegCloseKey	HKU\S-1-5-21-3130516669-347735452...	SUCCESS	Exclusive: False, O...
08:27:...	Explorer.EXE	11808	RegQueryKey	HKLM	SUCCESS	Query: Handle Tag...
08:27:...	Explorer.EXE	11808	RegOpenKey	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	Desired Access: R...

Network Connections

Go to SysinternalSuite → TCPview



TCPView - Sysinternals: www.sysinternals.com

File Edit View Process Connection Options Help

4 TCP v4 6 TCP v6 4 UDP v4 6 UDP v6 Search

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
accsvc.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	197.168.10.1	65538		

TCPView - Sysinternals: www.sysinternals.com

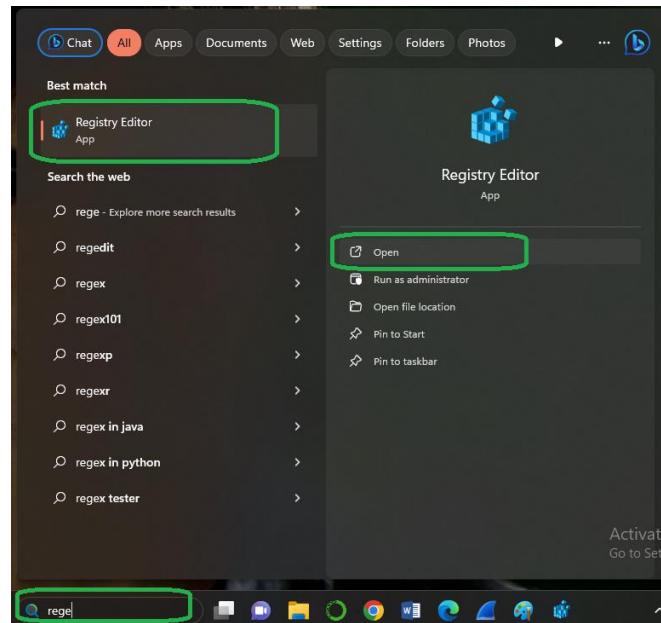
File Edit View Process Connection Options Help

4 TCP v4 6 TCP v6 4 UDP v4 6 UDP v6 Search

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	SSDPSPRV
svchost.exe	7720	UDPV6		fe80:3b4f:9f72:34ab:146	1900	*		05-09-2023 08:46:54	SSDPSPRV
svchost.exe	7720	UDPV6		fe80:3b4f:9f72:34ab:146	1900	*		05-09-2023 08:46:54	SSDPSPRV
svchost.exe	7720	UDPV6		fe80:3b4f:9f72:34ab:146	1900	*		05-09-2023 08:46:54	SSDPSPRV
dashHost.exe	5184	UDPV6		::	3702	*		05-09-2023 08:47:04	
dashHost.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

A screenshot of the Windows Registry Editor window. The title bar says "Registry Editor". The menu bar includes File, Edit, View, Favorites, and Help. The status bar at the bottom shows "Computer\HKEY_CURRENT_USER\AppEvents\Schemes\Names\Default". The left pane displays a tree view of registry keys under "Computer". The "Names" key is expanded, showing subkeys ".Default" and ".None". The ".Default" key is selected. The right pane shows a table with three columns: Name, Type, and Data. There is one entry: Name is ".Default", Type is "REG_SZ", and Data is "@mmres.dll,-800".

PRACTICAL NO. 4

Aim:

Capturing and analyzing network packets using Wireshark (Fundamentals):

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

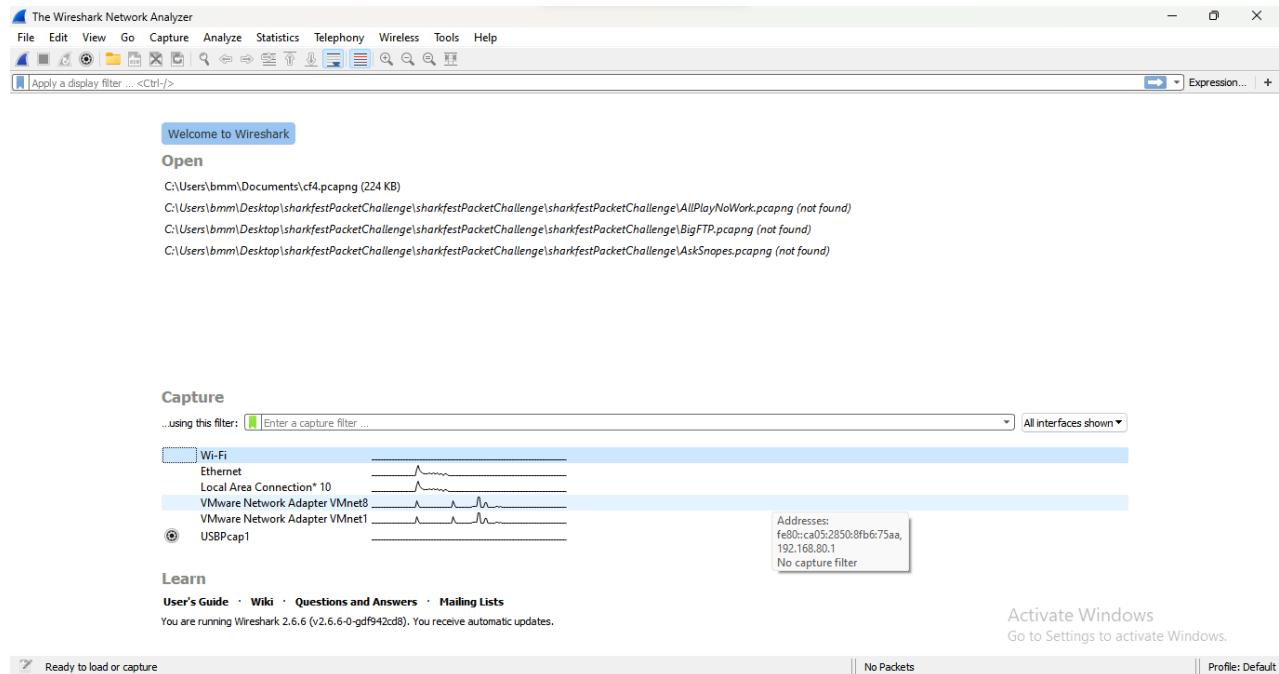
Practical:

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

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

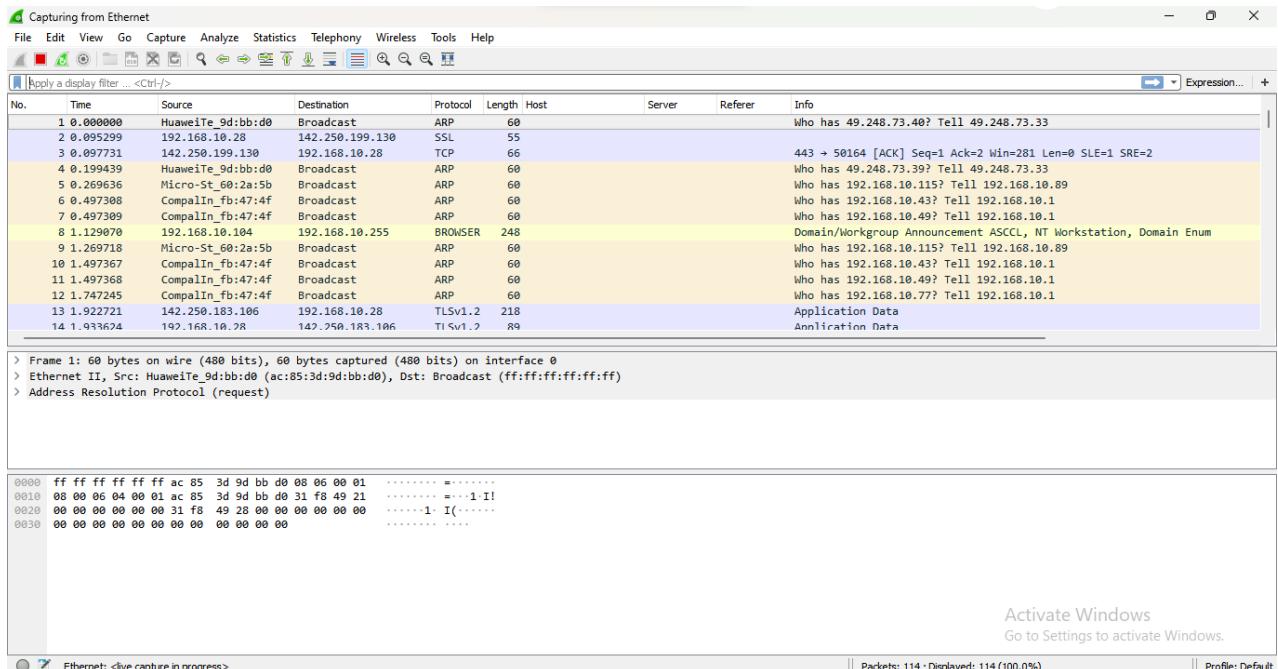
Identifying the Live Networks

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

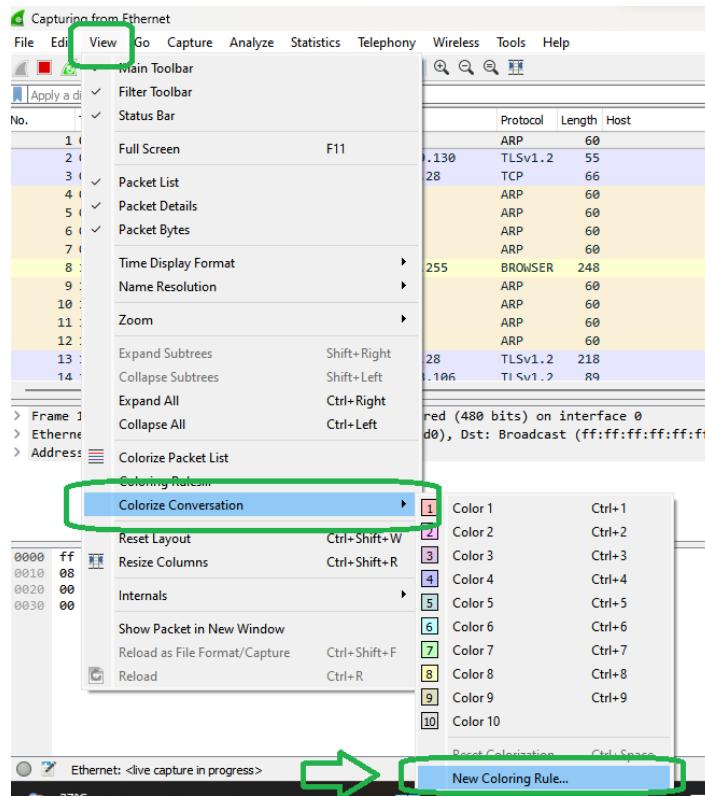
Color Coding Different packets are seen highlighted in various different colors. This is Wireshark's way of displaying traffic to help you easily identify the types of it.

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

Name	Filter
New coloring rule	eth.addr eq ac:85:3d:9d:bb:d0 and eth.addr eq ff:ff:ff:ff:ff:ff
New coloring rule	(ip.addr eq 192.168.10.115 and ip.addr eq 224.0.0.252) and (udp.port eq 52861 and udp.port eq 5355)
New coloring rule	(ip.addr eq 192.168.10.41 and ip.addr eq 239.255.255.250) and (udp.port eq 1900 and udp.port eq 1900)
Bad TCP	tcp.analysis.flags && !tcp.analysis.window_update
HSRP State Change	hsrp.state != 8 && hsrp.state != 16
Spanning Tree Topology Change	stp.type == 0x80
OSPF State Change	ospf.msg != 1
ICMP errors	icmp.type eq 3 icmp.type eq 4 icmp.type eq 5 icmp.type eq 11 icmpv6.type eq 1 icmpv6.type eq 2 icmpv6.type eq 3 icmpv6.type eq 4
ARP	arp
ICMP	icmp icmpv6
TCP RST	tcp.flags.reset eq 1
SCTP ABORT	sctp.chunk_type eq ABORT
TTL low or unexpected	(! ip.dst == 224.0.0.0/4 && ip.ttl < 5 && !(ipim && !ospf)) (ip.dst == 224.0.0.0/24 && ip.dst != 224.0.0.251 && ip.ttl != 1 && !(vrrp eth.fcs.status == "Bad" ip.checksum.status == "Bad" tcp.checksum.status == "Bad" udp.checksum.status == "Bad" sctp.checksum.status == "Bad" ip.sum == 0))
Checksum Errors	eth.fcs.status == "Bad" ip.checksum.status == "Bad" tcp.checksum.status == "Bad" udp.checksum.status == "Bad" sctp.checksum.status == "Bad" ip.sum == 0
SMB	smb nbss nbpx ipxsap netbios
HTTP	http tcp.port == 80 http2
IPX	ipx spx
DCERPC	dcerpc
Routing	hsrp eigrp ospf bgp cdp vrrp carp gvrp igmp ismp
TCP SYN/FIN	tcp.flags & 0x02 tcp.flags.fin == 1
TCP	tcp
UDP	udp
Broadcast	eth[0] & 1

Double click to edit. Drag to move. Rules are processed in order until a match is found.

+ - Foreground Background Apply as filter

OK Cancel Import... Export... Help

Now we analyze data using filters provided in the Wireshark application

Write the following commands in the given area to apply filter

The screenshot shows the Wireshark interface with a green box highlighting the 'Apply a display filter ... <Ctrl-/>' field at the top. A green arrow points from this field to the list of captured packets below. The packet list includes columns: No., Time, Source, Destination, Protocol, Length, Host, Server, Referer, and Info. Several packets are highlighted in yellow, and one is highlighted in blue.

No.	Time	Source	Destination	Protocol	Length	Host	Server	Referer	Info
1	0.000000	HuaweiTe_9d:bb:d0	Broadcast	ARP	60				Who has 49.248.73.
2	0.095299	192.168.10.28	142.250.199.130	TLSv1.2	55				
3	0.097731	142.250.199.130	192.168.10.28	TCP	66				443 → 50164 [ACK]
4	0.199439	HuaweiTe_9d:bb:d0	Broadcast	ARP	60				Who has 49.248.73.
5	0.269636	Micro-St_60:2a:5b	Broadcast	ARP	60				Who has 192.168.10
6	0.497308	CompaIn_fb:47:4f	Broadcast	ARP	60				Who has 192.168.10
7	0.497309	CompaIn_fb:47:4f	Broadcast	ARP	60				Who has 192.168.10
8	1.129070	192.168.10.104	192.168.10.255	BROWSER	248				Domain/Workgroup A
9	1.269718	Micro-St_60:2a:5b	Broadcast	ARP	60				Who has 192.168.10

Display filter command

1. Display packets based on specific IP-address

➤ ip.addr == 192.0.2.1

The screenshot shows the Wireshark interface with a green box highlighting the 'ip.addr == 192.0.2.1' filter in the display filter field at the top. A green arrow points from this field to the list of captured packets below. The packet list includes columns: No., Time, Source, Destination, Protocol, Length, Host, Server, Referer, and Info. Only one packet is visible in the list.

No.	Time	Source	Destination	Protocol	Length	Host	Server	Referer	Info
1	2.095299	192.168.10.28	142.250.199.130	TLSv1.2	55				443 → 50164 [ACK] Seq=1 Ack=2 Win=281 Len=0 SLE=1 SRE=2

Below the packet list, the status bar displays:

```
> Frame 2: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface 0
> Ethernet II, Src: f4:6b:8c:8e:6d:43 (f4:6b:8c:8e:6d:43), Dst: Sophos_6b:22:63 (7c:5a:1c:6b:22:63)
> Internet Protocol Version 4, Src: 192.168.10.28, Dst: 142.250.199.130
> Transmission Control Protocol, Src Port: 50164, Dst Port: 443, Seq: 1, Ack: 1, Len: 1
Secure Sockets Layer
```

At the bottom, the hex and ASCII panes show the captured data:

```
0000  7c 5a 1c 6b 22 63 f4 6b  8c 8e 6d 43 08 00 45 00 |Z k"ck .mC- E-
0010  00 29 d3 59 40 00 80 06  00 00 c0 a8 0a 1c 8e fa | ) Y@.....-
0020  c7 82 c3 f4 01 bb f6 b1  cb 71 81 bd 5e c7 50 10 |.....^p.
0030  01 ff 21 5d 00 00 00 00 |...!
```

2. Display packets which are coming from specific IP-address

➤ ip.src == 192.168.10.28

The screenshot shows the Wireshark interface with a capture window titled "ip.src == 192.168.10.28". The packet list pane displays 47 captured frames. The columns include No., Time, Source, Destination, Protocol, Length, Host, Server, Referer, and Info. Most frames are Application Data (TLSv1.2) between 192.168.10.28 and 142.250.199.130. A few frames are TCP segments (e.g., 50202 to 443). The details pane shows the raw hex and ASCII data for frame 2, which is a SYN segment. The bytes pane shows the raw hex and ASCII representation of the selected frame.

3. Display packets which are having specific IP-address destination

➤ ip.dst == 192.168.10.28

The screenshot shows the Wireshark interface with a capture window titled "ip.dst == 192.168.10.28". The packet list pane displays 24178 captured frames. The columns include No., Time, Source, Destination, Protocol, Length, Host, Server, Referer, and Info. The traffic consists primarily of TLSv1.3 connections between 192.168.10.28 and various servers. The details pane shows the raw hex and ASCII data for frame 24142, which is a SYN-ACK segment. The bytes pane shows the raw hex and ASCII representation of the selected frame.

4. Display packets which are using http protocol

➤ http

*Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Source	Destination	Protocol	Length	Host	Server	Referer	Info
13394	707.487777	15.207.161.196	HTTP	475				HTTP/1.1 200 OK (application/text)
13736	717.161381	15.207.161.196	HTTP	467				HTTP/1.1 200 OK (application/text)
14476	766.786676	15.207.161.196	HTTP	531				HTTP/1.1 200 OK (application/text)
18354	1047.517522	15.207.161.196	HTTP	531				HTTP/1.1 200 OK (application/text)
18477	1048.661494	15.207.161.196	HTTP	475				HTTP/1.1 200 OK (application/text)
18567	1058.070626	15.207.161.196	HTTP	487				HTTP/1.1 200 OK (application/text)
19534	1104.939537	15.207.161.196	HTTP	475				HTTP/1.1 200 OK (application/text)
22078	1281.576883	15.207.161.196	HTTP	507				HTTP/1.1 200 OK (application/text)
23760	1294.837652	15.207.161.196	HTTP	467				HTTP/1.1 200 OK (application/text)
23878	1296.327264	15.207.161.196	HTTP	443				HTTP/1.1 200 OK (application/text)
23900	1296.495246	15.207.161.196	HTTP	467				HTTP/1.1 200 OK (application/text)
23911	1296.675119	15.207.161.196	HTTP	435				HTTP/1.1 200 OK (application/text)
24134	1300.398024	15.207.161.196	HTTP	595				HTTP/1.1 200 OK (application/text)
25160	1377.298821	15.207.161.196	HTTP	539				HTTP/1.1 200 OK (application/text)

```
> Frame 24134: 595 bytes on wire (4760 bits), 595 bytes captured (4760 bits) on interface 0
> Ethernet II, Src: Sophos_6b:22:63 (7c:5a:1c:6b:22:63), Dst: f4:6b:8c:8e:6d:43 (f4:6b:8c:8e:6d:43)
> Internet Protocol Version 4, Src: 15.207.161.196, Dst: 192.168.10.28
> Transmission Control Protocol, Src Port: 8080, Dst Port: 50399, Seq: 1597, Ack: 1786, Len: 541
> Hypertext Transfer Protocol
> Media Type
```

```
0000 f4 6b 8c 8e 6d 43 7c 5a 1c 6b 22 63 08 00 45 00 -k-mC|Z-k"c-E-
0010 02 45 71 81 40 00 f2 06 98 0f cf a1 c4 c0 a8 -Eq @...-
0020 0a 1c 1f 98 c4 df e6 e2 7d dc 80 72 84 5b 50 18 .....}r[P-
0030 0e 7e 89 a9 00 00 48 54 54 50 2f 31 2e 31 20 32 ~~~~HT TP/1.1.2
0040 3a 30 28 4f 4b 0d 0a 44 61 74 65 3a 20 4d 6f 6e 00 OK-D ate: Mon
0050 2a 20 30 34 20 53 65 70 20 30 32 33 20 30 33 , 04 Sep 2023 03
0060 3a 34 31 3a 35 35 20 47 4d 54 0d 0a 43 6f 6e 74 :41:55 G MT-Cont
0070 65 6e 74 2d 54 79 70 65 3a 20 61 70 70 6c 69 63 ent-Type : applic
0080 61 74 69 6f 6e 2f 74 65 78 74 0d 0a 43 6f 6e 74 ation+te xt-Cont
0090 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 34 30 38 0d ent-Leng th: 408
00a0 0a 43 6f 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 :Connect ion: kee
00b0 70 2d 61 6c 69 76 65 0d 0a 0d 0a 2d 72 69 41 66 p-alive .....riAF
```

Activate Windows
Go to Settings to activate

5. Display packets which are using http request

➤ http.request

*Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http.request

No.	Time	Source	Destination	Protocol	Length	Host	Server	Referer	Info
22473	1227.983626	192.168.10.28	239.255.255.250	SSDP	217	239.255.255.250...			M-SEARCH * HTTP/1.1
22480	1228.983366	192.168.10.28	239.255.255.250	SSDP	217	239.255.255.250...			M-SEARCH * HTTP/1.1
22481	1228.998397	192.168.10.28	239.255.255.250	SSDP	217	239.255.255.250...			M-SEARCH * HTTP/1.1
22562	1229.990761	192.168.10.28	239.255.255.250	SSDP	217	239.255.255.250...			M-SEARCH * HTTP/1.1
22563	1230.006359	192.168.10.28	239.255.255.250	SSDP	217	239.255.255.250...			M-SEARCH * HTTP/1.1
22571	1230.999480	192.168.10.28	239.255.255.250	SSDP	217	239.255.255.250...			M-SEARCH * HTTP/1.1
22572	1231.014622	192.168.10.28	239.255.255.250	SSDP	217	239.255.255.250...			M-SEARCH * HTTP/1.1
23758	1294.832336	192.168.10.28	15.207.161.196	HTTP	423	prourl.itsecure...			POST /URLCategorizerService/URLCategorize HTTP
23869	1296.321801	192.168.10.28	15.207.161.196	HTTP	403	prourl.itsecure...			POST /URLCategorizerService/URLCategorize HTTP
23898	1296.480517	192.168.10.28	15.207.161.196	HTTP	435	prourl.itsecure...			POST /URLCategorizerService/URLCategorize HTTP
23908	1296.663753	192.168.10.28	15.207.161.196	HTTP	391	prourl.itsecure...			POST /URLCategorizerService/URLCategorize HTTP
23917	1296.698987	192.168.10.28	129.227.29.114	HTTP	244	conn-service-in...			GET /generate204 HTTP/1.1
24132	1300.391412	192.168.10.28	15.207.161.196	HTTP	403	prourl.itsecure...			POST /URLCategorizerService/URLCategorize HTTP
24794	1347.980233	192.168.10.28	239.255.255.250	SSDP	217	239.255.255.250...			M-SEARCH * HTTP/1.1

```
> Frame 24132: 403 bytes on wire (3224 bits), 403 bytes captured (3224 bits) on interface 0
> Ethernet II, Src: Sophos_6b:22:63 (7c:5a:1c:6b:22:63), Dst: f4:6b:8c:8e:6d:43 (f4:6b:8c:8e:6d:43)
> Internet Protocol Version 4, Src: 192.168.10.28, Dst: 15.207.161.196
> Transmission Control Protocol, Src Port: 50399, Dst Port: 8080, Seq: 1437, Ack: 1597, Len: 349
> Hypertext Transfer Protocol
> HTML Form URL Encoded: application/x-www-form-urlencoded
```

```
0000 7c 5a 1c 6b 22 63 f4 6b 8c 8e 6d 43 08 00 45 00 |Z-k"c-k-mC-E-
0010 01 85 ed e1 40 00 80 06 00 00 c0 a8 0a 1c 0f cf .....@.....
0020 a1 c4 c4 df 1f 98 80 72 82 fe e6 e2 7d dc 50 18 .....}r[P-
0030 04 00 7d cf 00 00 50 4f 53 54 20 2f 55 52 4c 43 ..}PO ST /URLC
0040 61 74 65 67 6f 72 69 7a 65 72 53 65 72 76 69 63 ategoriz erServic
0050 65 2f 55 52 4c 43 61 74 65 67 6f 72 69 74 65 20 e/URLCat egorize
0060 48 54 50 2f 31 2e 31 0d 0a 43 6f 6e 74 65 6e HTTP/1.1 --Content
0070 74 2d 54 79 70 65 3a 20 61 70 70 6c 69 63 61 74 t-Type: applicat
0080 69 6f 6e 2f 78 2d 77 77 72 2d 66 6f 72 6d 2d 75 ion/x-w w-form-u
0090 72 6c 65 6e 63 6f 64 65 64 0d 0a 55 73 65 72 2d rlencode d>User-
00a0 41 67 65 6e 74 3a 20 6a 73 6f 6e 68 74 74 70 0d Agent: j sonhttp-
00b0 0a 48 6f 73 74 3a 20 70 72 6f 75 72 6c 2e 69 74 Host: p rourrl.it
```

Activate Windows
Go to Settings to activate

6. Display packets which are using TCP protocol

➤ tcp

The screenshot shows the Wireshark interface with the "tcp" filter applied. A single TCP packet is selected for detailed analysis. The packet details pane shows:

```

> Frame 24132: 403 bytes on wire (3224 bits), 403 bytes captured (3224 bits) on interface 0
> Ethernet II, Src: f4:6b:8c:8e:6d:43 (f4:6b:8c:8e:6d:43), Dst: Sophos_6b:22:63 (7c:5a:1c:6b:22:63)
> Internet Protocol Version 4, Src: 192.168.10.28, Dst: 15.207.161.196
> Transmission Control Protocol, Src Port: 50399, Dst Port: 8080, Seq: 1437, Ack: 1597, Len: 349
> Hypertext Transfer Protocol
> HTML Form URL Encoded: application/x-www-form-urlencoded
  
```

The selected packet's hex dump is as follows:

```

0000  7c 5a 1c 6b 22 63 f4 6b 8c 8e 6d 43 08 00 45 00 |Z-k*c-k...mC-E-
0010  01 85 ed e1 40 00 80 06 00 00 c0 a8 0a 1c 0f cf .....@.....
0020  a1 c4 d4 df 1f 98 80 72 82 fe e6 e2 7d dc 58 18 .....r.....}P-
0030  04 00 7d cf 00 00 50 4f 53 54 20 2f 55 52 4c 43 .....}PO ST /URLC
0040  61 74 65 67 6f 72 69 7a 65 72 53 65 72 76 69 63 categoriz erServic
0050  65 2f 55 52 4c 43 61 74 65 67 6f 72 69 7a 65 20 e/URLCat egorize
0060  48 54 50 2f 31 2e 31 0d 0a 43 6f 6e 74 65 6e HTTP/1.1 Conten
0070  74 2d 54 79 70 65 3a 20 61 70 6c 69 63 61 74 t-Type: applicat
0080  69 6f 6e 2f 78 2d 77 77 66 6f 72 6d 2d 75 ion/x-ww w-form-u
0090  72 6c 63 6f 64 65 64 0d 0a 55 73 65 72 2d rlencode d:User-
00a0  41 67 65 6e 74 3a 20 6a 73 6f 6e 68 74 70 6d Agent: j sonhttp-
00b0  0a 48 6f 73 74 3a 20 70 72 6f 75 72 6c 2e 69 74 Host: p rourl.it
  
```

Activate Window
Go to Settings to ac

7. Display packets having no error connecting to server

➤ http.response.code==200

The screenshot shows the Wireshark interface with the "http.response.code == 200" filter applied. A single HTTP response packet is selected for detailed analysis. The packet details pane shows:

```

> Frame 23911: 435 bytes on wire (3480 bits), 435 bytes captured (3480 bits) on interface 0
> Ethernet II, Src: Sophos_6b:22:63 (7c:5a:1c:6b:22:63), Dst: f4:6b:8c:8e:6d:43 (f4:6b:8c:8e:6d:43)
> Internet Protocol Version 4, Src: 15.207.161.196, Dst: 192.168.10.28
> Transmission Control Protocol, Src Port: 8080, Dst Port: 50399, Seq: 1216, Ack: 1437, Len: 381
> Hypertext Transfer Protocol
> Media Type
  
```

The selected packet's hex dump is as follows:

```

0000  f4 6b 8c 8e 6d 43 7c 5a 1c 6b 22 63 08 00 45 00 |k-mC|Z-k*c-E-
0010  01 a5 71 80 40 00 f2 06 99 7a 0f cf a1 c4 c0 a8 ..@...z...
0020  0a 1c 1f 98 c4 df e6 e2 7c 5f 80 72 82 fe 58 18 .....|_r.-P-
0030  00 7a d9 9b 00 00 48 54 54 58 2f 31 2e 31 20 32 .z...TP/1.1 2
0040  30 38 20 4f 4b 0d 0a 44 61 74 65 3a 20 4d 6f 6e 00 OK-D ate: Mon
0050  2c 20 30 34 20 52 65 70 20 32 30 33 20 30 33 , 04 Sep 2023 03
0060  3a 34 31 3a 35 32 20 47 4d 54 0d 0a 43 6f 6e 74 :41:52 G MT:Cont
0070  65 6e 74 2d 54 79 70 65 3a 20 61 70 70 6c 69 63 ent-Type: applic
0080  61 74 69 6f 6e 2f 74 65 78 74 0d 0a 43 6f 6e 74 ation/te xt:Cont
0090  65 6e 74 2d 4c 65 6e 67 74 68 3a 20 32 34 38 0d ent-Leng th: 248
00a0  0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 Connect ion: kee
00b0  70 2d 61 6c 69 76 65 0d 0a 0d 0a 52 56 5a 73 4c p-alive: ...RVZsL
  
```

Activate Window
Go to Settings to active

8. Display packets having port number 80, 443

➤ `tcp.port==80 || udp.port==443`

*Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.port == 80

No.	Time	Source	Destination	Protocol	Length	Host	Server	Referer	Info
18651	1056.033875	129.227.29.114	192.168.10.28	TCP	60				80 → 61438 [FIN, ACK] Seq=252 Ack=253
18652	1056.072862	129.227.29.114	192.168.10.28	TCP	60				[TCP Retransmission] 80 → 61438 [ACK] Seq=253 Ack=192
18656	1056.142564	129.227.29.114	192.168.10.28	TCP	60				80 → 61438 [ACK] Seq=253 Ack=192
21848	1190.915180	129.227.29.114	192.168.10.28	TCP	66				80 → 61445 [SYN, ACK] Seq=0 Ack=1
21853	1191.098378	129.227.29.114	192.168.10.28	TCP	60				80 → 61445 [ACK] Seq=1 Ack=191 Wi
21868	1192.132699	129.227.29.114	192.168.10.28	HTTP	305		nginx		HTTP/1.1 204 No Content
21869	1192.132701	129.227.29.114	192.168.10.28	TCP	60				80 → 61445 [FIN, ACK] Seq=252 Ack=253
21872	1192.319049	129.227.29.114	192.168.10.28	TCP	60				80 → 61445 [ACK] Seq=253 Ack=192
22044	1200.903703	129.227.29.114	192.168.10.28	TCP	66				80 → 61446 [SYN, ACK] Seq=0 Ack=1
22047	1200.911287	129.227.29.114	192.168.10.28	TCP	60				80 → 61446 [ACK] Seq=1 Ack=191 Wi
22048	1200.921342	129.227.29.114	192.168.10.28	HTTP	305		nginx		HTTP/1.1 204 No Content
22049	1200.921342	129.227.29.114	192.168.10.28	TCP	60				80 → 61446 [FIN, ACK] Seq=252 Ack=253
22052	1200.923718	129.227.29.114	192.168.10.28	TCP	60				80 → 61446 [ACK] Seq=253 Ack=192
23915	1296.688350	129.227.29.114	192.168.10.28	TCP	66				80 → 61456 [SYN, ACK] Seq=0 Ack=1

> Frame 22052: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
> Ethernet II, Src: Sophos_6b:22:63 (7c:5a:1c:6b:22:63), Dst: f4:6b:8c:8e:6d:43 (f4:6b:8c:8e:6d:43)
> Internet Protocol Version 4, Src: 129.227.29.114, Dst: 192.168.10.28
> Transmission Control Protocol, Src Port: 80, Dst Port: 61446, Seq: 253, Ack: 192, Len: 0

0000 f4 6b 8c 8e 6d 43 7c 5a 1c 6b 22 63 08 00 45 00 ··k·-mC|Z ·k"c·-E·
0010 00 28 17 99 40 00 40 06 b9 1d 81 e3 1d 72 c0 a8 ('· @@· ···r···
0020 0a 1c 00 50 f0 06 ac b4 ce 80 59 6a 4a 50 10 ···P··· ···YjJP·
0030 00 ed ae 58 00 00 00 00 00 00 00 00 00 00 00 00 ···X··· ····

The screenshot shows a Wireshark capture of network traffic. The packet list pane displays 2531 UDP packets from source 192.168.10.28 to destination 142.250.192.74, all on port 443. The details pane shows the structure of one frame, which is a User Datagram Protocol (UDP) packet. The bytes pane shows the raw hex and ASCII data of the captured frame.

No.	Time	Source	Destination	Protocol	Length	Host	Server	Referer	Info
2287	75.460960	192.168.10.28	142.250.192.74	UDP	1292				61370 → 443 Len=1250
2299	75.623692	192.168.10.28	142.250.192.74	UDP	1292				61370 → 443 Len=1250
2304	76.244388	192.168.10.28	142.250.192.74	UDP	1292				61370 → 443 Len=1250
2327	76.596989	192.168.10.28	142.250.192.74	UDP	1292				61371 → 443 Len=1250
2349	76.780520	192.168.10.28	142.250.192.74	UDP	1292				61373 → 443 Len=1250
2377	76.937969	192.168.10.28	142.250.192.74	UDP	1292				61371 → 443 Len=1250
2398	77.144852	192.168.10.28	142.250.192.74	UDP	1292				61373 → 443 Len=1250
2436	77.408296	192.168.10.28	142.250.192.74	UDP	1292				61370 → 443 Len=1250
2437	77.567800	192.168.10.28	142.250.192.74	UDP	1292				61371 → 443 Len=1250
2454	77.685925	192.168.10.28	142.250.192.74	UDP	1292				61373 → 443 Len=1250
2494	78.396922	192.168.10.28	142.250.192.74	UDP	1292				61375 → 443 Len=1250
2515	78.697740	192.168.10.28	142.250.192.74	UDP	1292				61375 → 443 Len=1250
2516	78.698781	192.168.10.28	142.250.192.74	UDP	1292				61371 → 443 Len=1250
2531	78.911451	192.168.10.28	142.250.192.74	UDP	1292				61373 → 443 Len=1250

> Frame 2287: 1292 bytes on wire (10336 bits), 1292 bytes captured (10336 bits) on interface 0
> Ethernet II, Src: f4:6b:8c:8e:6d:43 (f4:6b:8c:8e:6d:43), Dst: Sophos_6b:22:63 (7c:5a:1c:6b:22:63)
> Internet Protocol Version 4, Src: 192.168.10.28, Dst: 142.250.192.74
> User Datagram Protocol, Src Port: 61370, Dst Port: 443
> Data (1250 bytes)

0000 7c 5a 1c 6b 22 63 f4 6b 8c 8e 6d 43 08 00 45 00 |Z-k"c·k ··mC··E·
0010 04 fe 2b e8 40 00 3e 11 f1 fd c0 a8 0a 1c 8e fa ·+@> ······
0020 c0 4a ef ba 01 bb 04 ea 3c 43 c7 00 00 00 01 08 ·J····· <C·····
0030 c3 5d 49 4f 89 51 a2 9c 00 00 44 d0 a8 7d f2 71 ·]·O Q· ··D· }·q
0040 c8 fb 80 89 78 01 66 4a 67 c4 9a b2 71 f3 78 7a ···x·f3 g· ·q xz
0050 07 98 9d bf 63 f4 6b 49 ed f1 c6 04 3c 9e 23 d5 ···c·K! ··<#·
0060 bc 0c 64 47 21 35 c1 d7 26 a6 47 29 2f 0a 32 07 ·dG!5 ··&·G· /·-·
0070 27 85 7c 22 a6 26 5d cf 94 27 01 21 ec b9 54 '|"&| ··'!···!T
0080 18 c9 19 72 76 8e 78 7b e7 10 91 b5 3e 06 e8 b6 ·rv·x{ ···>···
0090 17 5e 06 a2 94 5c 25 c1 5b 6c 93 ab 99 16 c3 dd ^··\% [l·····
00a0 d7 86 9e b2 52 3d 33 7f 0f 15 cd 04 ed b1 b0 23 ·R=3 ······#
00b0 1c b7 fc e8 3d cf 3b eb 28 a3 73 19 97 da 68 f5 ···=·; ·(·s··h·

9. Display packets which contains keyword facebook

➤ tcp contains facebook

No.	Time	Source	Destination	Protocol	Length	Host	Server	Referer	Info
7140	391.930122	192.168.10.28	157.240.16.16	TLSv1.3	583				Client Hello
7141	391.930160	192.168.10.28	157.240.16.16	TLSv1.3	583				Client Hello
28288	1498.375536	192.168.10.28	157.240.242.34	TLSv1.3	472				Client Hello
29506	1508.440146	192.168.10.28	157.240.16.16	TLSv1.3	583				Client Hello
34147	1655.749190	192.168.10.28	157.240.16.32	TLSv1.3	472				Client Hello
34261	1656.659636	192.168.10.28	157.240.16.16	TLSv1.2	478				Client Hello

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

AIM:

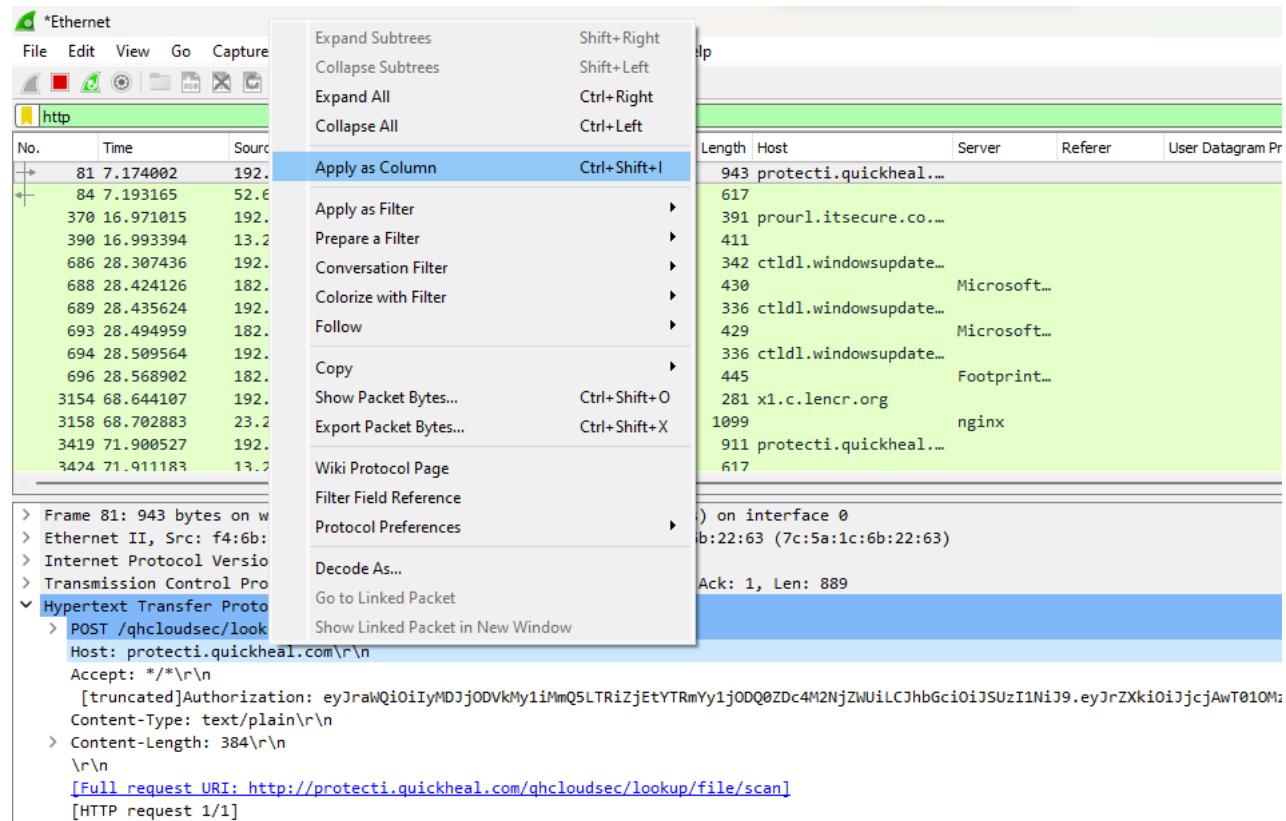
Analyze the packets provided in lab and solve the questions using Wireshark

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

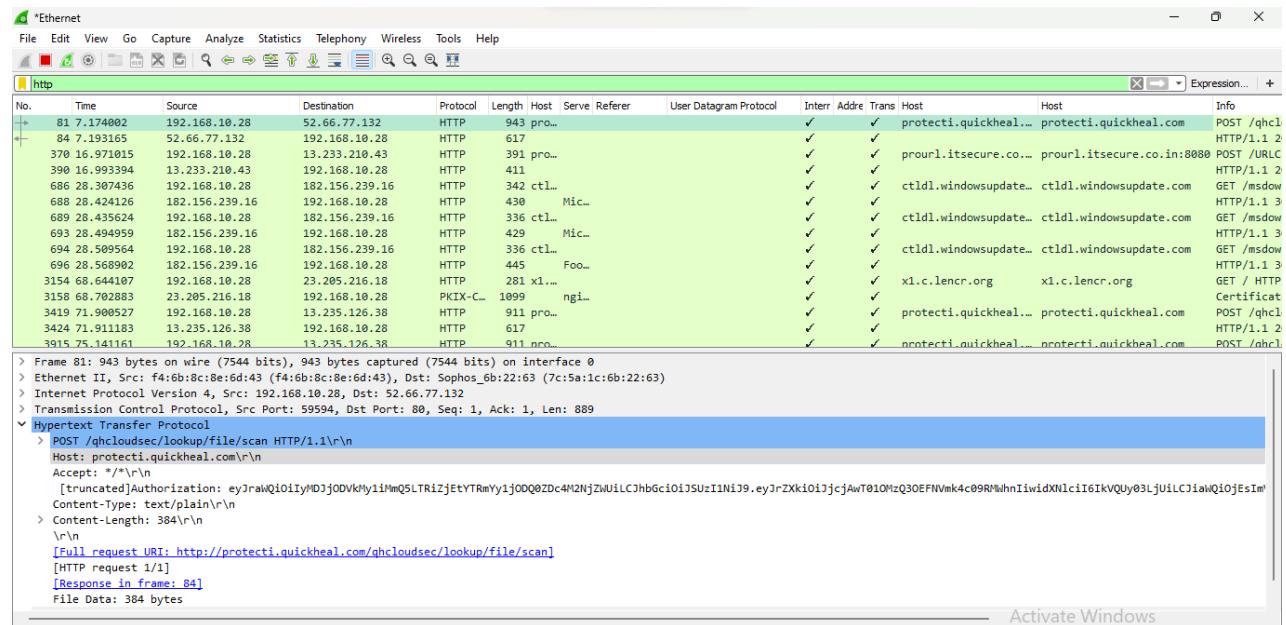
Analysis –

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

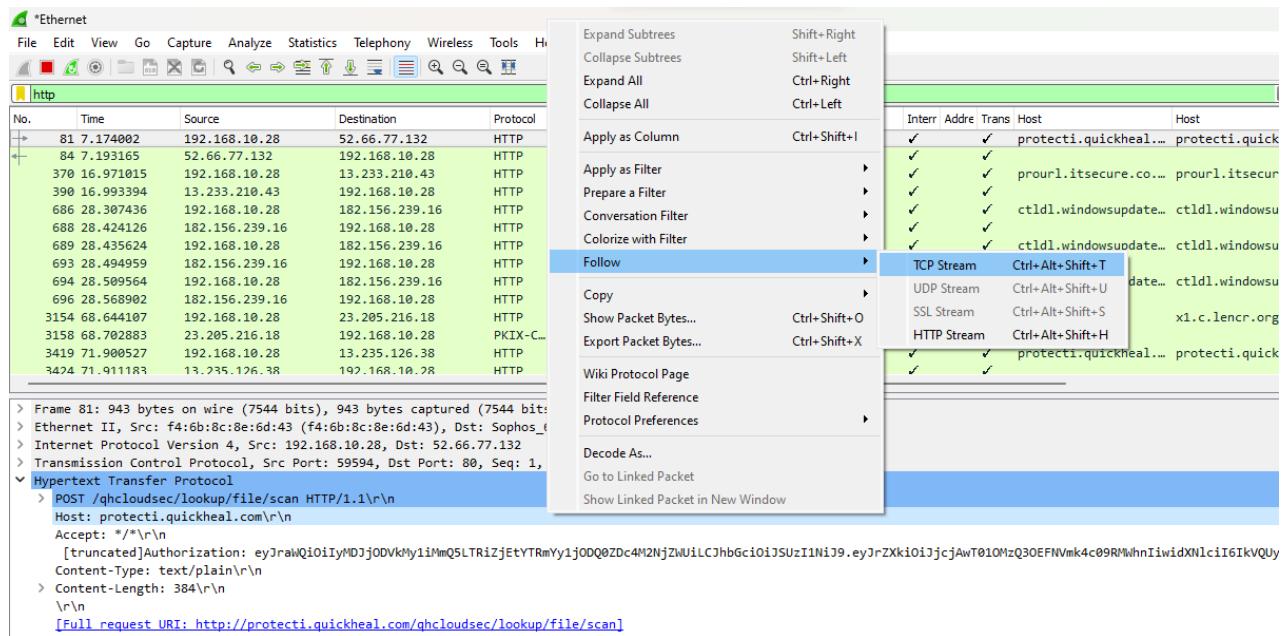
First find the requests from **HTTP** and click on and **request** then on the **lower table of details** Select on **HyperText Transfer Protocol → Host** and **Right Click** on that and Select **Apply as Filter**



Now we can see the **Host**



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



```

Wireshark - Follow TCP Stream (tcp.stream eq 9) - Ethernet

POST /qhcloudsec/lookup/file/scan HTTP/1.1
Host: protecti.quickheal.com
Accept: */*
Authorization: eyJraWQiOiIyMDIjODVkJy1iMmQ5LTRizjEtYTrmYy1j0DQ0ZDc4M2NjZWUiLCjhGciOiJSUzI1NiJ9.eyJrZXkiOiJjcjAwT010MzQ30EFNVmk4c09RMWhnIiwiidXNlciI6IkVQJy
Content-Type: text/plain\r\n
Content-Length: 384\r\n
[Full request URI: http://protecti.quickheal.com/qhcloudsec/lookup/file/scan]

7970Mh1HmN1FQF50EHci8v6zul9-
Kee7Ge5G0_TMZowqz5C8T61h9Pd1qK2yELj82_oIHUVB5tg3JUwsx8By2oI9b_s8PkgnycCd4Chs7lWNs8hBKIZjg79MQDKceYv3VgHdJIqdsL7QMw0iSinfawj9sI
-6SnS9gU-ZGW0WQHWOKC3yGCSOJN8yh_XPCp-
uHyazGpy60CDU4DDcm7MwBYpkWx0D_AEkx2D41xHdDrNv23uCI5140wjj4hs3rjtXzLsLR7koswIEybQVnduu7Iyf3w7MkenDw9UQylSHfEpRVA0KH0Y_VqGaw-
nB04_-psCuxsrQUL0ULfp75FUZYhiciMlsSijr3aGSozf6_vnzm-JR7j8UGBPqNy_IBuXHTTP/1.1 200 OK
Date: Fri, 08 Sep 2023 06:22:36 GMT
Content-Type: text/plain
Content-Length: 374
X-SERVER-ID: UUhQVEk=
Via: HTTP/1.1 forward.http.proxy:3128
Connection: keep-alive

1uJRULc5Lhu_I1FMRF440Veq7CoGaUILuaQn2HeqOkBivDdkEJU0NN_tzzvpm0G-Map9BtKRjIRQuq4QejDC397qCnTtzJJUm0N0gSWCGcG7g0Q7_7-
NsDcbx00Lr6xtYdUw6JyattdIkIhwYRw513LAVV1F9g0R7rt515d-
wAh809eeFEAxtMkH0EQ65LP7Vhluscl21j4Xx_YfhfGTXrcCERpdfY81bo7YSxhT7lhv0rC5DHvrsAtudu2gK13o7Tlwksbg333Wvd5B_Q_CreqH0IXKUJ6iSHm
_oSc5YbJc_FZ3o03-clpXD-oAuBQVS8BIYwzG_IAu2lInmK2r9QXA8rrZj9vPgcG4Bn6MHyt0ejrA

```

1 client pkt, 1 server pkt, 1 turn.

Entire conversation (1452 bytes) Show and save data as ASCII Stream 9

Find: Find Next

Filter Out This Stream Print Save as... Back Close Help

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”**

No.	Time	Source	Destination	Protocol	Length	Host	Serve	Referer	User Datagram Protocol	Inter	Addr	Trans	Host	Info
2085	101.165285	104.208.16.88	192.168.10.28	TCP	1514					✓	✓			443 → 58656 [ACK] Seq=4381 Ack=518 Wir
2346	119.530513	192.168.10.28	192.168.10.1	DNS	85		✓			✓	✓			Standard query 0xedfb A fd.api.iris.mi
2347	119.540691	192.168.10.1	192.168.10.28	DNS	208		✓			✓	✓			Standard query response 0xedfb A fd.ap
2351	119.638227	192.168.10.28	20.24.121.134	TLSv1.2	353		✓			✓	✓			Client Hello
2356	119.733913	20.24.121.134	192.168.10.28	TLSv1.2	1514		✓			✓	✓			
2357	119.733920	20.24.121.134	192.168.10.28	TLSv1.2	1514		✓			✓	✓			Ignored Unknown Record
2360	119.734256	20.24.121.134	192.168.10.28	TLSv1.2	1514		✓			✓	✓			Ignored Unknown Record
213	6.762757	192.168.10.28	239.255.255.250	SSDP	217	239.25...	✓			✓	✓			239.255.255... M-SEARCH * HTTP/1.1
225	7.765877	192.168.10.28	239.255.255.250	SSDP	217	239.25...	✓			✓	✓			239.255.255... M-SEARCH * HTTP/1.1
234	8.772968	192.168.10.28	239.255.255.250	SSDP	217	239.25...	✓			✓	✓			239.255.255... M-SEARCH * HTTP/1.1
252	9.780504	192.168.10.28	239.255.255.250	SSDP	217	239.25...	✓			✓	✓			239.255.255... M-SEARCH * HTTP/1.1
474	27.935260	192.168.10.52	239.255.255.250	SSDP	217	239.25...	✓			✓	✓			239.255.255... M-SEARCH * HTTP/1.1
479	28.935641	192.168.10.52	239.255.255.250	SSDP	217	239.25...	✓			✓	✓			239.255.255... M-SEARCH * HTTP/1.1
487	29.941067	192.168.10.52	239.255.255.250	SSDP	217	239.25...	✓			✓	✓			239.255.255... M-SEARCH * HTTP/1.1
494	30.942066	192.168.10.52	239.255.255.250	SSDP	217	239.25...	✓			✓	✓			239.255.255... M-SEARCH * HTTP/1.1

> Frame 213: 217 bytes on wire (1736 bits), 217 bytes captured (1736 bits) on interface 0
> Ethernet II, Src: f4:6b:8c:0e:6d:43 (f4:6b:8c:0e:6d:43), Dst: IPv4mcast_7ff:ff:fa (01:00:5e:7f:ff:fa)
> Internet Protocol Version 4, Src: 192.168.10.28, Dst: 239.255.255.250
> User Datagram Protocol, Src Port: 62928, Dst Port: 1900
> Simple Service Discovery Protocol

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.

No.	Time	Source	Destination	Protocol	Length	Host	Serve	Referer	User Datagram Protocol	Inter	Addr	Trans	Host	Info
2085	101.165285	104.208.16.88	192.168.10.28	TCP	1514					✓	✓			443 → 58656 [ACK] Seq=4381 Ack=518 Wir
2346	119.530513	192.168.10.28	192.168.10.1	DNS	85		✓			✓	✓			Standard query 0xedfb A fd.api.iris.mi
2347	119.540691	192.168.10.1	192.168.10.28	DNS	208		✓			✓	✓			Standard query response 0xedfb A fd.ap
2351	119.638227	192.168.10.28	20.24.121.134	TLSv1.2	353		✓			✓	✓			Client Hello
2356	119.733913	20.24.121.134	192.168.10.28	TLSv1.2	1514		✓			✓	✓			Ignored Unknown Record
2357	119.733920	20.24.121.134	192.168.10.28	TLSv1.2	1514		✓			✓	✓			Ignored Unknown Record
2360	119.734256	20.24.121.134	192.168.10.28	TLSv1.2	1514		✓			✓	✓			Ignored Unknown Record
213	6.762757	192.168.10.28	239.255.255.250	SSDP	217	239.25...	✓			✓	✓			239.255.255... M-SEARCH * HTTP/1.1
225	7.765877	192.168.10.28	239.255.255.250	SSDP	217	239.25...	✓			✓	✓			239.255.255... M-SEARCH * HTTP/1.1
234	8.772968	192.168.10.28	239.255.255.250	SSDP	217	239.25...	✓			✓	✓			239.255.255... M-SEARCH * HTTP/1.1
252	9.780504	192.168.10.28	239.255.255.250	SSDP	217	239.25...	✓			✓	✓			239.255.255... M-SEARCH * HTTP/1.1
474	27.935260	192.168.10.52	239.255.255.250	SSDP	217	239.25...	✓			✓	✓			239.255.255... M-SEARCH * HTTP/1.1
479	28.935641	192.168.10.52	239.255.255.250	SSDP	217	239.25...	✓			✓	✓			239.255.255... M-SEARCH * HTTP/1.1
487	29.941067	192.168.10.52	239.255.255.250	SSDP	217	239.25...	✓			✓	✓			239.255.255... M-SEARCH * HTTP/1.1
494	30.942066	192.168.10.52	239.255.255.250	SSDP	217	239.25...	✓			✓	✓			239.255.255... M-SEARCH * HTTP/1.1

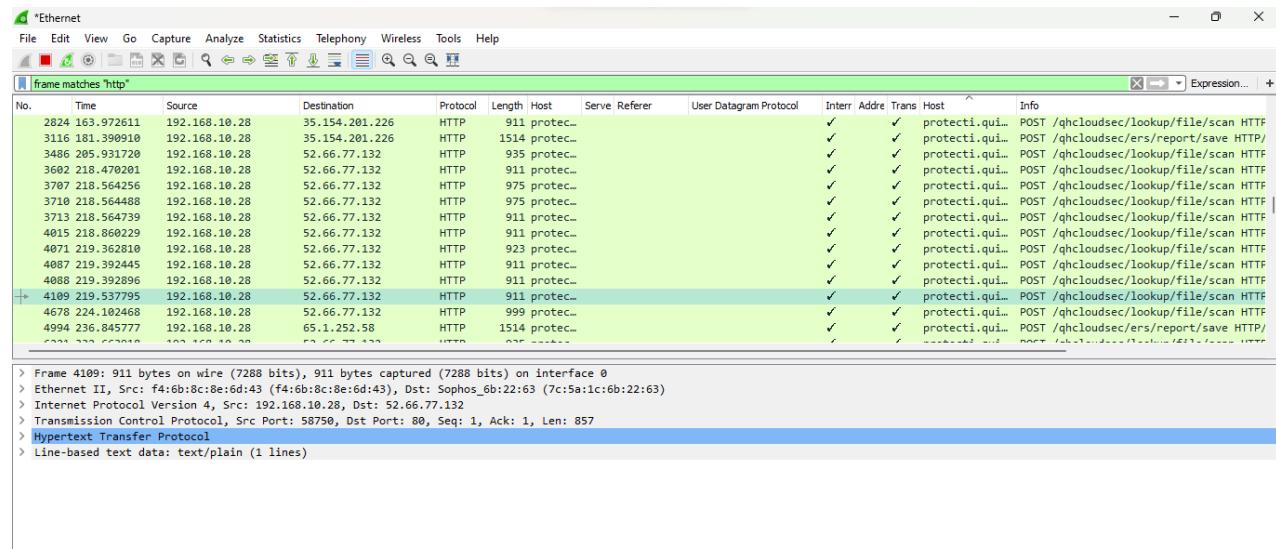
> Frame 213: 217 bytes on wire (1736 bits), 217 bytes captured (1736 bits) on interface 0
> Ethernet II, Src: f4:6b:8c:0e:6d:43 (f4:6b:8c:0e:6d:43), Dst: IPv4mcast_7ff:ff:fa (01:00:5e:7f:ff:fa)
> Internet Protocol Version 4, Src: 192.168.10.28, Dst: 239.255.255.250
> User Datagram Protocol, Src Port: 62928, Dst Port: 1900
> Simple Service Discovery Protocol
> M-SEARCH * HTTP/1.1\r\nHOST: 239.255.255.250:1900\r\nMAN: "ssdp:discover"\r\n\r\n[Full request URI: http://239.255.255.250:1900*]
[HTTP request 1/4]
[Next request in frame: 225]

Activate Windows

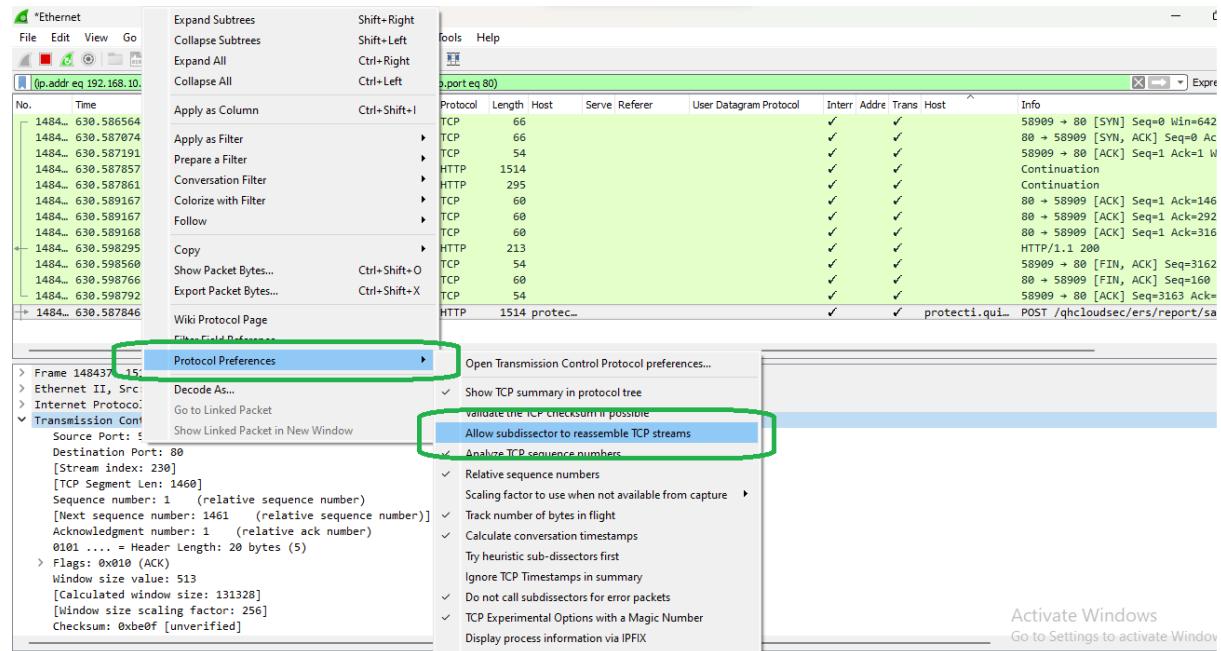
3. According to http, what data will TCP show?

Analysis –

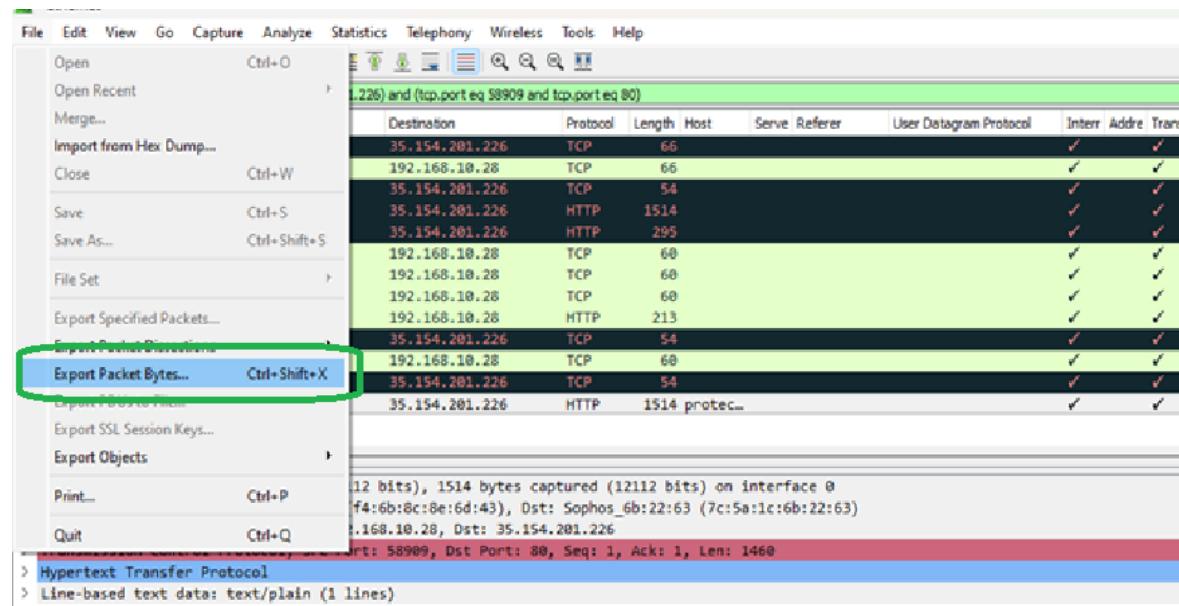
As we did in the last challenge, we will apply a regular express filter for the Google keyword. Apply frame matched “http”.



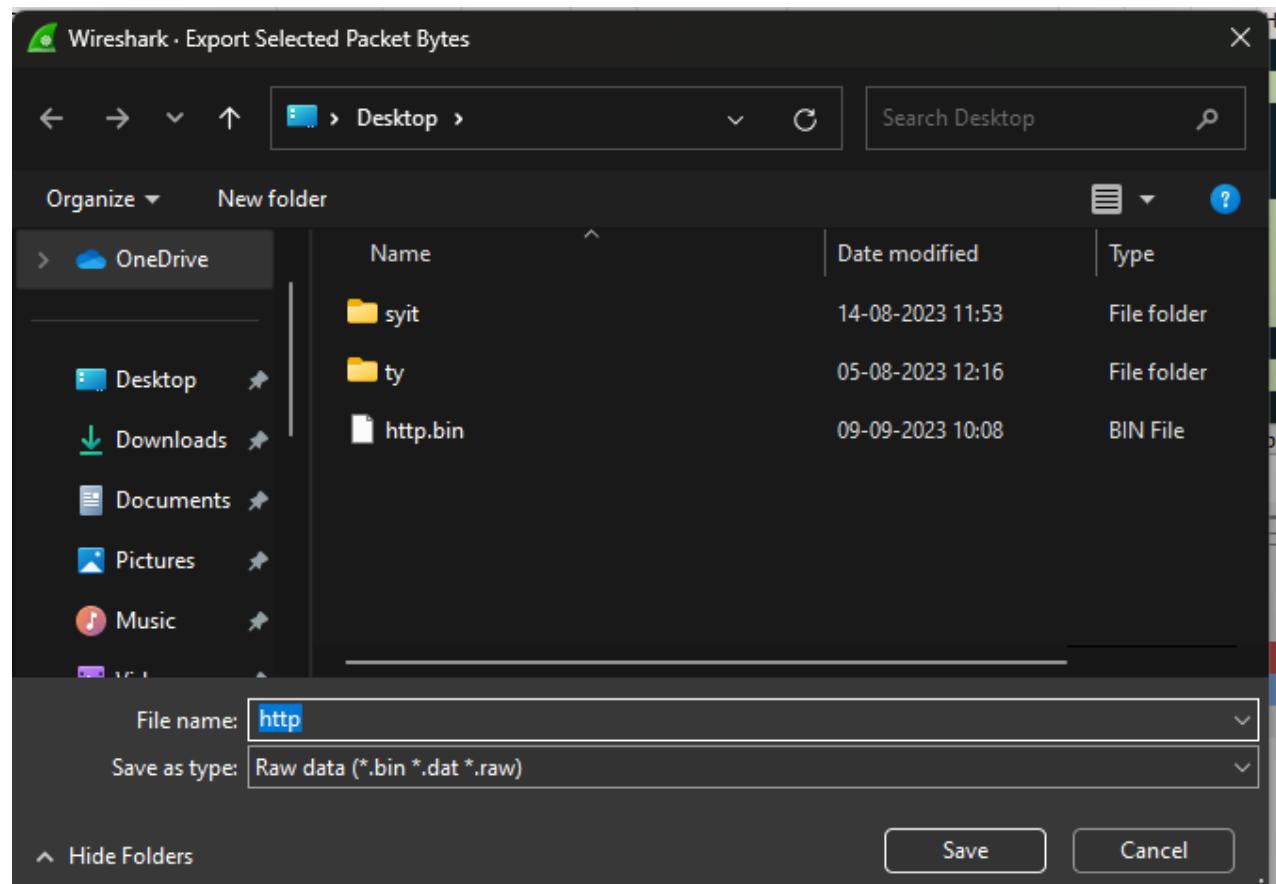
Select the packet and expand the Hypertext Transfer Protocol tab right click on Transmission Control Protocol Go to Protocol Preferences and check Allow subdissector to resemble TCP stream with HTTP spanning bodies.



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



Click on save all.

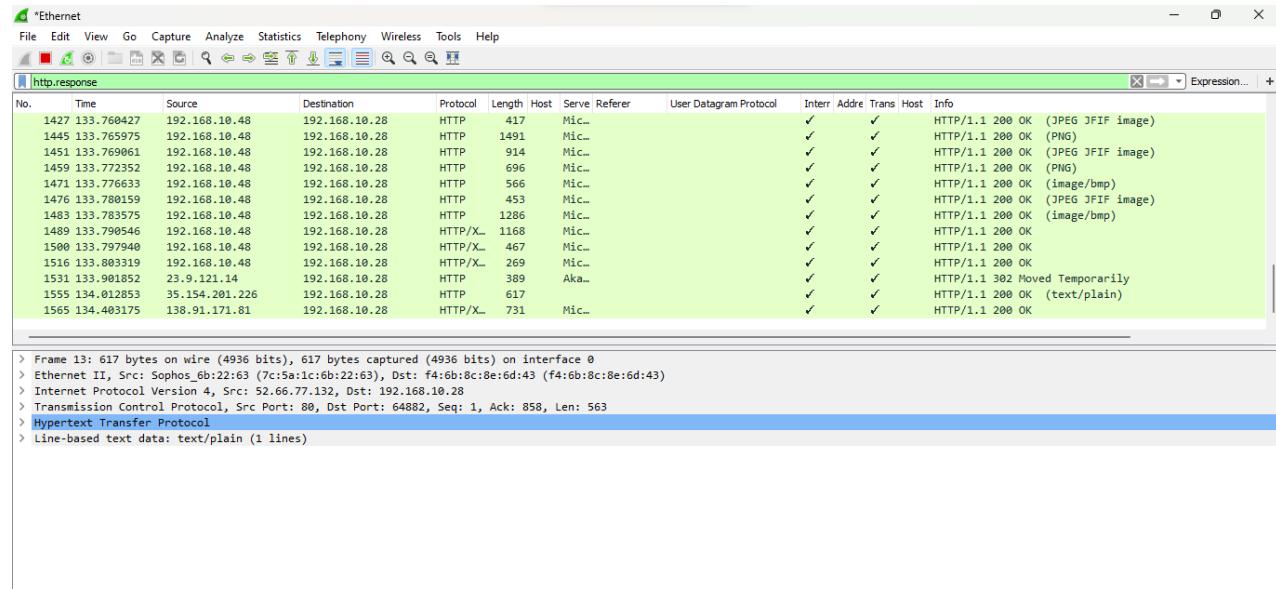


After checking it seems only the packets transfer were to connect the machine to the internet.

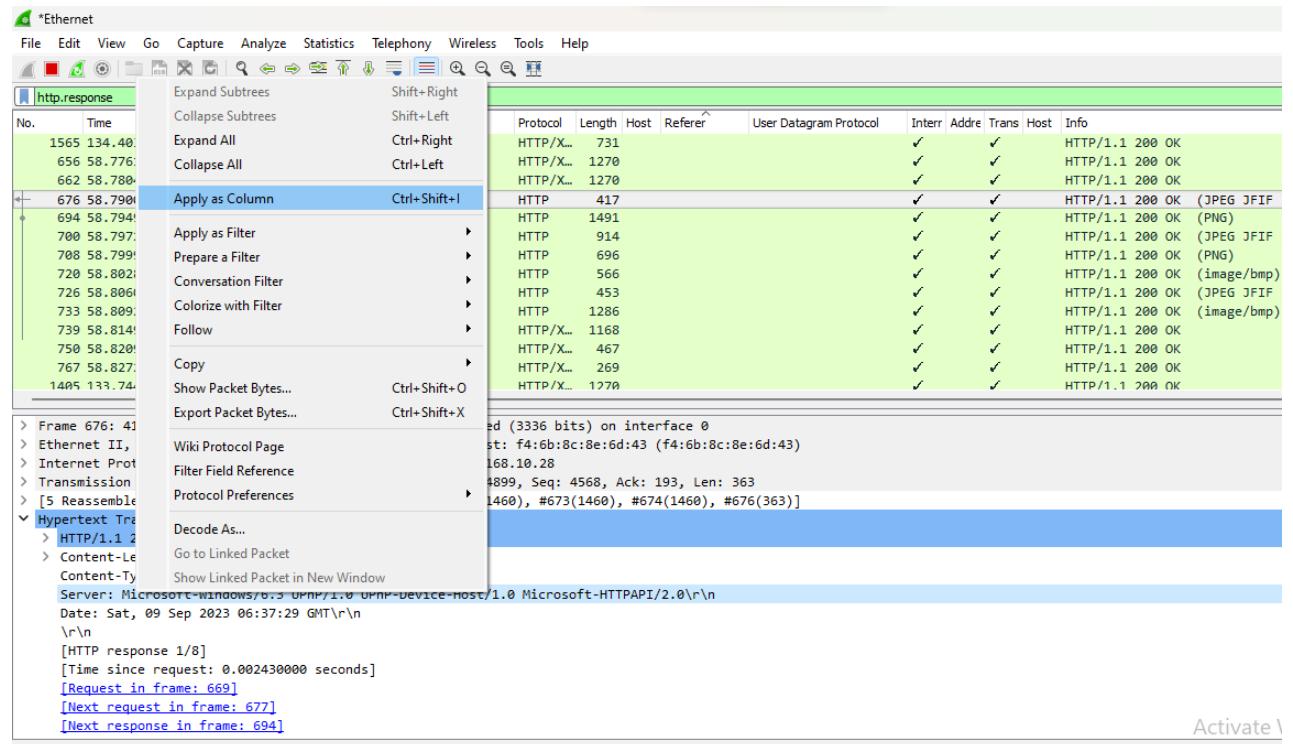
4. How many web servers are running Microsoft?

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.

No.	Time	Source	Destination	Protocol	Length	Host	Referer	Server	User Datagram Protocol	Inter	Addr	Trans	Host	Info
733	58.809293	192.168.10.47	192.168.10.28	HTTP	1286			Microsoft-Windows/6.3 UPnP/1.0 UPnP-Device-H...	✓	✓			HTTP/1.1 :	
739	58.814959	192.168.10.47	192.168.10.28	HTTP/X...	1168			Microsoft-Windows/6.3 UPnP/1.0 UPnP-Device-H...	✓	✓			HTTP/1.1 :	
750	58.826924	192.168.10.47	192.168.10.28	HTTP/X...	467			Microsoft-Windows/6.3 UPnP/1.0 UPnP-Device-H...	✓	✓			HTTP/1.1 :	
767	58.827250	192.168.10.47	192.168.10.28	HTTP/X...	269			Microsoft-Windows/6.3 UPnP/1.0 UPnP-Device-H...	✓	✓			HTTP/1.1 :	
782	58.923739	23.9.121.14	192.168.10.28	HTTP	389			AkamaiGhost	✓	✓			HTTP/1.1 :	
807	59.348985	20.231.121.79	192.168.10.28	HTTP/X...	731			Microsoft-IIS/10.0	✓	✓			HTTP/1.1 :	
982	94.327644	192.168.10.1	192.168.10.28	HTTP	384			Microsoft-IIS/10.0	✓	✓			HTTP/1.1 :	
985	94.339059	192.168.10.1	192.168.10.28	HTTP	384			Microsoft-IIS/10.0	✓	✓			HTTP/1.1 :	
988	94.346552	192.168.10.1	192.168.10.28	HTTP	384			Microsoft-IIS/10.0	✓	✓			HTTP/1.1 :	
991	94.354057	192.168.10.1	192.168.10.28	HTTP	384			Microsoft-IIS/10.0	✓	✓			HTTP/1.1 :	
994	94.368437	192.168.10.1	192.168.10.28	HTTP	384			Microsoft-IIS/10.0	✓	✓			HTTP/1.1 :	
997	94.368192	192.168.10.1	192.168.10.28	HTTP	384			Microsoft-IIS/10.0	✓	✓			HTTP/1.1 :	
1000	94.376016	192.168.10.1	192.168.10.28	HTTP	384			Microsoft-IIS/10.0	✓	✓			HTTP/1.1 :	
1003	94.381398	192.168.10.1	192.168.10.28	HTTP	384			Microsoft-TTS/10.0	✓	✓			HTTP/1.1 :	

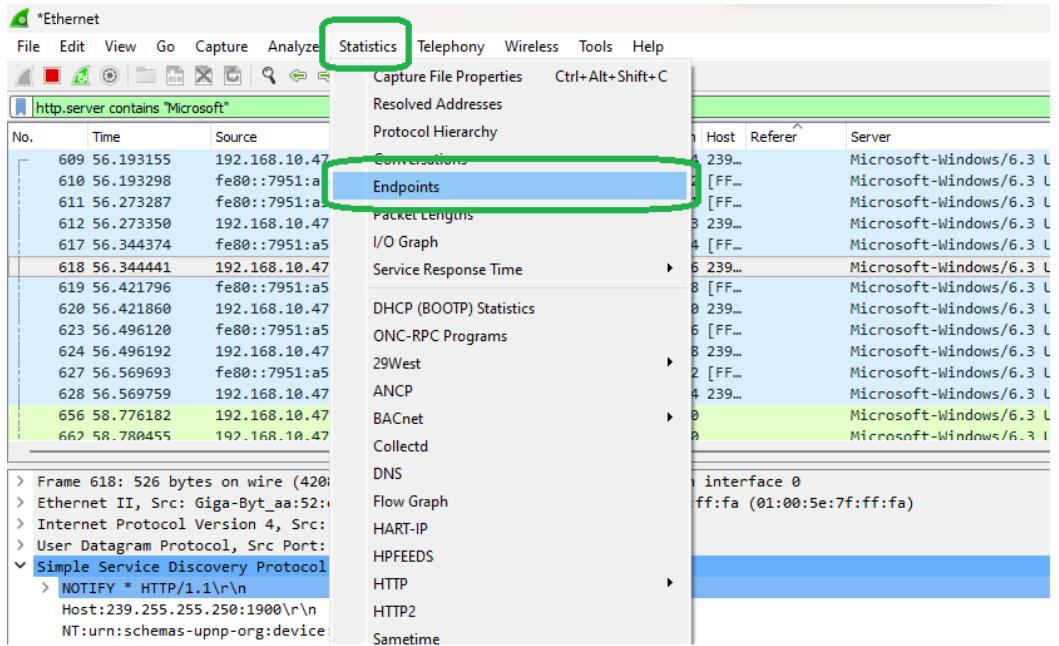
```
> Frame 1000: 384 bytes on wire (3072 bits), 384 bytes captured (3072 bits) on interface 0
> Ethernet II, Src: CompaqIn_f8:47:4f (98:29:a6:f8:47:4f), Dst: f4:6b:8c:8e:6d:43 (f4:6b:8c:8e:6d:43)
> Internet Protocol Version 4, Src: 192.168.10.1, Dst: 192.168.10.28
> Transmission Control Protocol, Src Port: 8101, Dst Port: 64904, Seq: 1981, Ack: 1169, Len: 330
`- Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Content-Type: application/x-unknown\r\n
    Last-Modified: Mon, 29 Nov 2021 06:23:48 GMT\r\n
    Accept-Ranges: bytes\r\n
    ETag: "10c73eab94d710"\r\n
    Server: Microsoft-IIS/10.0\r\n
    X-Frame-Options: SAMEORIGIN\r\n
    X-XSS-Protection: 1;mode=block\r\n
    X-Content-Type-Options: nosniff\r\n
    Date: Sat, 27 Nov 2021 06:23:48 GMT\r\n
```

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”**

No.	Time	Source	Destination	Protocol	Length	Host	Referer	Server	User Datagram Protocol	Inter	Addr	Trans	Host	Info
609	56.193155	192.168.10.47	239.255.255.250	SSDP	474	239...		Microsoft-Windows/6.3 UPnP/1.0 UPnP-Device-H...	✓				239...	
610	56.193298	fe80::7951:a59d:8ef...	ff02::c	SSDP	502	[FF...				[FF...				[FF...
611	56.273287	fe80::7951:a59d:8ef...	ff02::c	SSDP	511	[FF...		Microsoft-Windows/6.3 UPnP/1.0 UPnP-Device-H...	✓				239...	
612	56.273350	192.168.10.47	239.255.255.250	SSDP	483	239...		Microsoft-Windows/6.3 UPnP/1.0 UPnP-Device-H...	✓				239...	
617	56.344374	fe80::7951:a59d:8ef...	ff02::c	SSDP	554	[FF...		Microsoft-Windows/6.3 UPnP/1.0 UPnP-Device-H...	✓				239...	
618	56.344441	192.168.10.47	239.255.255.250	SSDP	526	239...		Microsoft-Windows/6.3 UPnP/1.0 UPnP-Device-H...	✓				239...	
619	56.421796	fe80::7951:a59d:8ef...	ff02::c	SSDP	568	[FF...		Microsoft-Windows/6.3 UPnP/1.0 UPnP-Device-H...	✓				239...	
620	56.421860	192.168.10.47	239.255.255.250	SSDP	540	239...		Microsoft-Windows/6.3 UPnP/1.0 UPnP-Device-H...	✓				239...	
623	56.496120	fe80::7951:a59d:8ef...	ff02::c	SSDP	566	[FF...		Microsoft-Windows/6.3 UPnP/1.0 UPnP-Device-H...	✓				239...	
624	56.496192	192.168.10.47	239.255.255.250	SSDP	538	239...		Microsoft-Windows/6.3 UPnP/1.0 UPnP-Device-H...	✓				239...	
627	56.569693	fe80::7951:a59d:8ef...	ff02::c	SSDP	582	[FF...		Microsoft-Windows/6.3 UPnP/1.0 UPnP-Device-H...	✓				239...	
628	56.569759	192.168.10.47	239.255.255.250	SSDP	554	239...		Microsoft-Windows/6.3 UPnP/1.0 UPnP-Device-H...	✓				239...	
656	58.776182	192.168.10.47	192.168.10.28	HTTP/X...	1270			Microsoft-Windows/6.3 UPnP/1.0 UPnP-Device-H...	✓	✓			HTTP/1.1 :	
662	58.780455	192.168.10.47	192.168.10.28	HTTP/X...	1270			Microsoft-Windows/6.3 UPnP/1.0 UPnP-Device-H...	✓	✓			HTTP/1.1 :	

```
> Frame 609: 474 bytes on wire (3792 bits), 474 bytes captured (3792 bits) on interface 0
> Ethernet II, Src: Giga-Byt_aaa:S2:e0 (1c:1b:0d:aa:S2:e0), Dst: IPv4mcast_7ff:ff:fa (01:00:5e:7f:ff:fa)
> Internet Protocol Version 4, Src: 192.168.10.47, Dst: 239.255.255.250
> User Datagram Protocol, Src Port: 1900, Dst Port: 1900
`- Simple Service Discovery Protocol
  > NOTIFY * HTTP/1.1\r\n
    Host:239.255.255.250:1900\r\n
    NT:upnp:rootdevice\r\n
    NTS:ssdp:alive\r\n
    Location:http://192.168.10.47:2869/upnphost/udhisapi.dll?content=uuid:f33dfca1-0fa9-44ad-a64c-b9395679a96c\r\n
    USN:uuid:f33dfca1-0fa9-44ad-a64c-b9395679a96c\r\n
```

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



It will show all connections.

Wireshark - Endpoints - Ethernet										
Ethernet · 61	IPv4 · 133	IPv6 · 53	TCP · 430	UDP · 635						
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	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	—	—	—	—

Name resolution Limit to display filter

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

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>

Sysinternals Suite - Sysinternals | learn.microsoft.com/en-us/sysinternals/downloads/sysinternals-suite

To get future Google Chrome updates, you'll need Windows 10 or later. This computer is using Windows 8.1.

Learn / Sysinternals / Downloads /

Sysinternals Suite

Article • 06/07/2023 • 8 contributors

By Mark Russinovich

Updated: July 26, 2023

[Download Sysinternals Suite](#) (45.2 MB)

[Download Sysinternals Suite for Nano Server](#) (9.5 MB)

[Download Sysinternals Suite for ARM64](#) (14.3 MB)

[Install Sysinternals Suite from the Microsoft Store](#)

Additional resources

Documentation

Sysinternals Utilities - Sysinternals

Evaluate and find out how to install, deploy and maintain Windows with Sysinternals utilities.

Sysinternals - Sysinternals

Library, learning resources, downloads, support, and community. Evaluate and find how to install, deploy, and maintain Wind

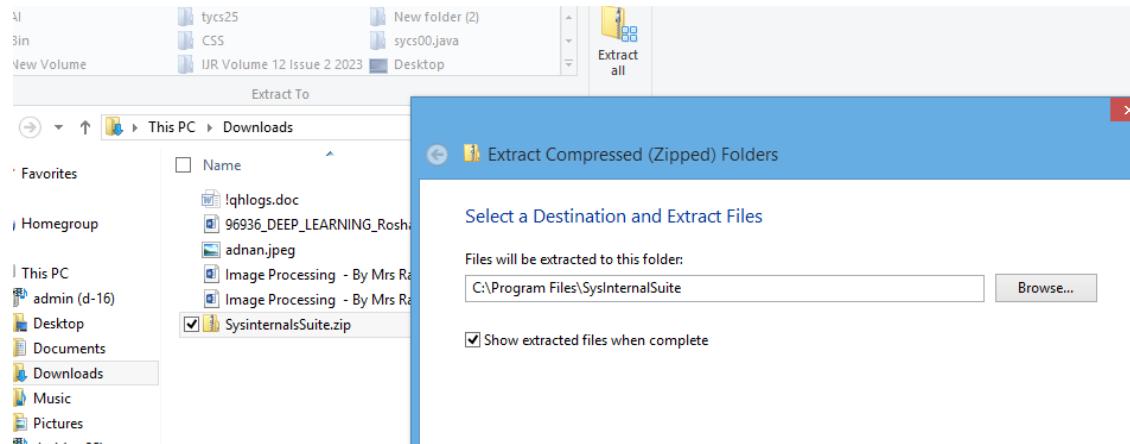
Sysinternals Process Utilities - Sysinternals

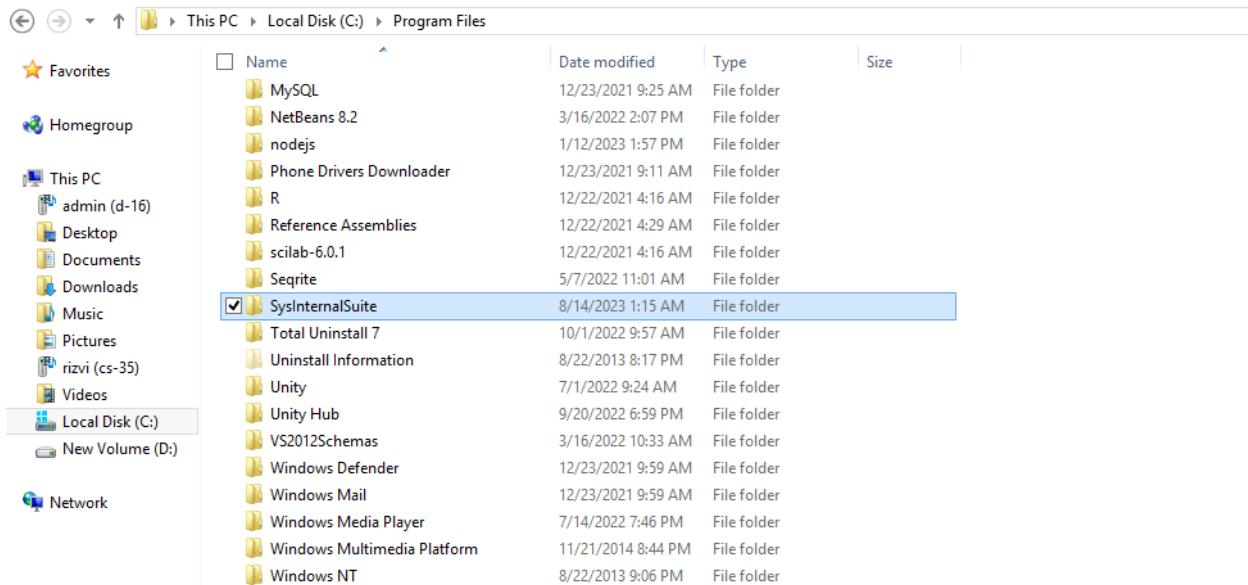
Windows Sysinternals process utilities

Show 5 more

Activate Windows

Then Extract the file to the desired directory





This screenshot shows the Windows File Explorer interface. The left sidebar displays 'Favorites', 'Homegroup', 'This PC' (with sub-folders like admin (d-16), Desktop, Documents, Downloads, Music, Pictures, rizvi (cs-35), Videos), 'Local Disk (C:)', 'New Volume (D:)', and 'Network'. The main pane shows a list of files and folders under 'Program Files'. A blue selection bar highlights the 'SysInternalSuite' folder, which contains sub-items like Total Uninstall 7, Uninstall Information, Unity, Unity Hub, VS2012Schemas, Windows Defender, Windows Mail, Windows Media Player, Windows Multimedia Platform, and Windows NT.

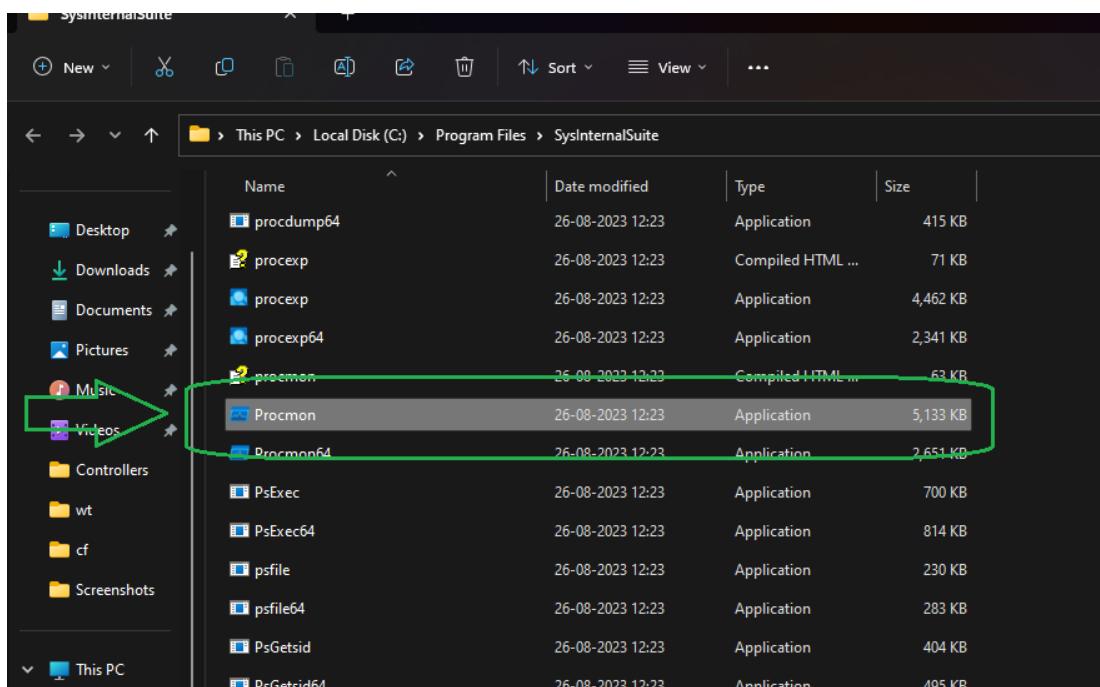
Name	Date modified	Type	Size
MySQL	12/23/2021 9:25 AM	File folder	
NetBeans 8.2	3/16/2022 2:07 PM	File folder	
nodejs	1/12/2023 1:57 PM	File folder	
Phone Drivers Downloader	12/23/2021 9:11 AM	File folder	
R	12/22/2021 4:16 AM	File folder	
Reference Assemblies	12/22/2021 4:29 AM	File folder	
scilab-6.0.1	12/22/2021 4:16 AM	File folder	
Sqrite	5/7/2022 11:01 AM	File folder	
SysInternalSuite	8/14/2023 1:15 AM	File folder	
Total Uninstall 7	10/1/2022 9:57 AM	File folder	
Uninstall Information	8/22/2013 8:17 PM	File folder	
Unity	7/1/2022 9:24 AM	File folder	
Unity Hub	9/20/2022 6:59 PM	File folder	
VS2012Schemas	3/16/2022 10:33 AM	File folder	
Windows Defender	12/23/2021 9:59 AM	File folder	
Windows Mail	12/23/2021 9:59 AM	File folder	
Windows Media Player	7/14/2022 7:46 PM	File folder	
Windows Multimedia Platform	11/21/2014 8:44 PM	File folder	
Windows NT	8/22/2013 9:06 PM	File folder	

Monitor Live Processes

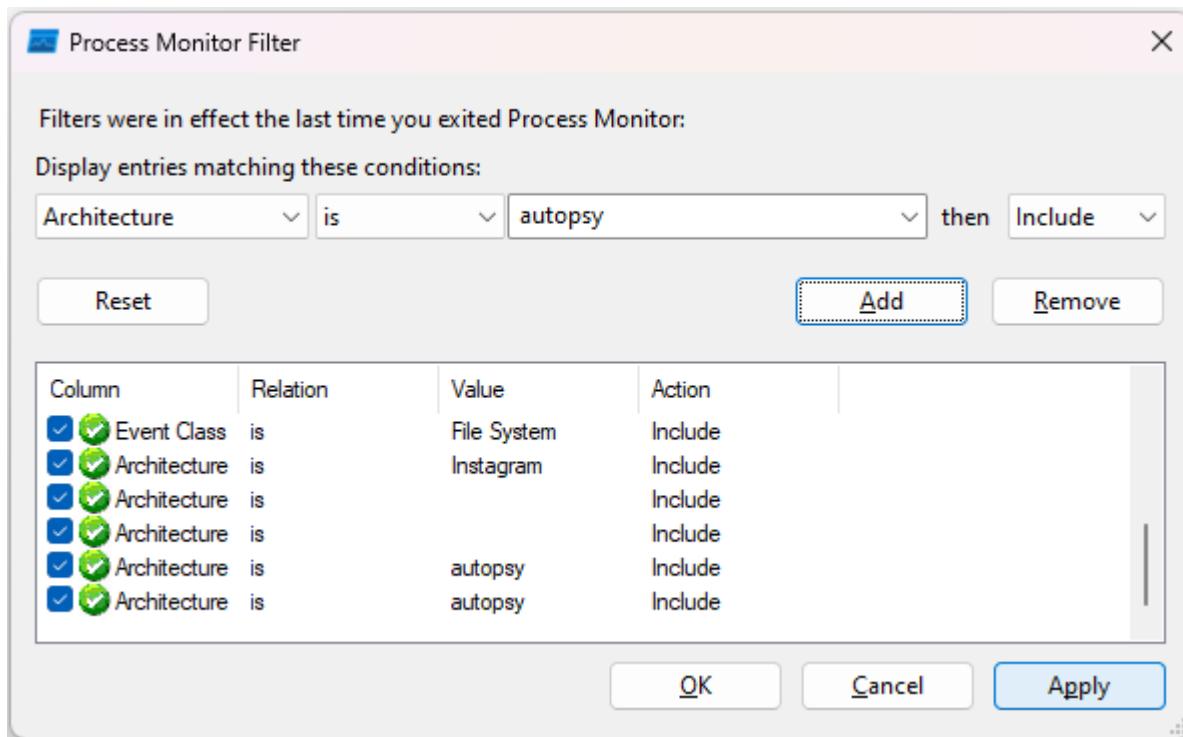
Process Monitor is an advanced monitoring tool for Windows that show real-time file system, Registry and process/thread activity. It combines the features of two legacy SysInternals utilities, Filemon and Regmon, and adds an extensive list of enhancements including rich non-destructive filtering, comprehensive 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

File	Edit	Event	Filter	Tools	Options	Help
Time...	Process Name	PID	Operation	Path	Result	Detail
08:27...	svchost.exe	2644	ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset: 704512, Le...
08:27...	Explorer.EXE	11808	ReadFile	C:\Windows\System32\MMCoreR.dll	SUCCESS	Offset: 995328, Le...
08:27...	svchost.exe	2644	ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset: 692224, Le...
08:27...	Explorer.EXE	11808	ReadFile	C:\Windows\System32\MMCoreR.dll	SUCCESS	Offset: 925696, Le...
08:27...	svchost.exe	1656	UDP Receive	f0ff:fb:5353 -> fe80:2050:4fce:b495:8...: SUCCESS	Length: 30, sequn...	
08:27...	chrome.exe	9724	UDP Receive	f0ff:fb:5353 -> fe80:2050:4fce:b495:8...: SUCCESS	Length: 30, sequn...	
08:27...	svchost.exe	2644	ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset: 647168, Le...
08:27...	Explorer.EXE	11808	QueryBasicInfo...	C:\Program Files\Windows Apps\Clipcha...	SUCCESS	CreationTime: 13:0...
08:27...	Explorer.EXE	11808	ReadFile	C:\Windows\System32\Taskbar.dll	SUCCESS	Offset: 2406400, Le...
08:27...	Explorer.EXE	11808	CloseFile	C:\Program Files\Windows Apps\Clipcha...	SUCCESS	
08:27...	svchost.exe	2644	ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset: 638976, Le...
08:27...	Explorer.EXE	11808	RegCloseKey	HKUS\1-5-21-3130516669-347735452...: SUCCESS	Desired Access: R...	
08:27...	Explorer.EXE	11808	RegOpenKey	HKUS\1-5-21-3130516669-347735452...: SUCCESS	Query: HandleTag...	
08:27...	Explorer.EXE	11808	RegQueryKey	HKUS\1-5-21-3130516669-347735452...: SUCCESS	Desired Access: R...	
08:27...	Explorer.EXE	11808	RegOpenKey	HKUS\1-5-21-3130516669-347735452...: REPARSE	Desired Access: R...	
08:27...	svchost.exe	2644	ReadFile	C:\Windows\System32\Windows.State...	SUCCESS	Desired Access: R...
08:27...	Explorer.EXE	11808	RegOpenKey	HKUS\1-5-21-3130516669-347735452...: SUCCESS	Desired Access: R...	
08:27...	Explorer.EXE	11808	RegCloseKey	HKUS\1-5-21-3130516669-347735452...: SUCCESS	Desired Access: R...	
08:27...	Explorer.EXE	11808	RegOpenKey	C:\Windows\System32\Taskbar.dll	SUCCESS	Offset: 2718208, Le...
08:27...	Explorer.EXE	11808	RegQueryValue	HKUS\1-5-21-3130516669-347735452...: NAME NOT FOUND	Length: 12	
08:27...	Explorer.EXE	11808	RegCloseKey	HKUS\1-5-21-3130516669-347735452...: SUCCESS		
08:27...	svchost.exe	1020	ReadFile	C:\Windows\System32\BCP74mm.dll	SUCCESS	Offset: 180224, Le...
08:27...	svchost.exe	2644	ReadFile	C:\Windows\System32\Windows.State...	SUCCESS	Offset: 1540096, Le...
08:27...	Explorer.EXE	11808	ReadFile	C:\Windows\System32\Taskbar.dll	SUCCESS	Offset: 6434816, Le...
08:27...	svchost.exe	1020	ReadFile	C:\Windows\System32\Vsasrv.dll	SUCCESS	Offset: 2529280, Le...
08:27...	Explorer.EXE	11808	ReadFile	C:\Windows\System32\BCP74mm.dll	SUCCESS	Offset: 1523712, Le...
08:27...	svchost.exe	2644	ReadFile	C:\Windows\System32\Taskbar.dll	SUCCESS	Offset: 1556468, Le...
08:27...	svchost.exe	1020	ReadFile	C:\Windows\System32\Windows.State...	SUCCESS	Offset: 2512896, Le...
08:27...	svchost.exe	2644	ReadFile	C:\Windows\System32\Vsasrv.dll	SUCCESS	Offset: 6414336, Le...
08:27...	svchost.exe	1020	ReadFile	C:\Windows\System32\Vsasrv.dll	SUCCESS	Offset: 1519616, Le...
08:27...	svchost.exe	2644	ReadFile	C:\Windows\System32\Taskbar.dll	SUCCESS	Desired Access: R...
08:27...	svchost.exe	1020	ReadFile	C:\Windows\System32\Vsasrv.dll	SUCCESS	Offset: 6434816, Le...
08:27...	svchost.exe	1020	ReadFile	C:\Windows\System32\BCP74mm.dll	SUCCESS	Offset: 1523712, Le...
08:27...	svchost.exe	2644	ReadFile	C:\Windows\System32\Taskbar.dll	SUCCESS	Offset: 1556468, Le...
08:27...	svchost.exe	1020	ReadFile	C:\Windows\System32\Windows.State...	SUCCESS	Offset: 2512896, Le...
08:27...	svchost.exe	2644	ReadFile	C:\Windows\System32\Vsasrv.dll	SUCCESS	Offset: 6414336, Le...
08:27...	svchost.exe	1020	ReadFile	C:\Windows\System32\Vsasrv.dll	SUCCESS	Offset: 1519616, Le...
08:27...	svchost.exe	2644	LockFile	C:\ProgramData\Microsoft\Windows\...: SUCCESS	Desired Access: R...	
08:27...	svchost.exe	1020	LockFile	C:\ProgramData\Microsoft\Windows\...: SUCCESS	Exclusive: False, O...	
08:27...	svchost.exe	2644	LockFile	C:\ProgramData\Microsoft\Windows\...: SUCCESS	Query: HandleTag...	
08:27...	svchost.exe	1020	LockFile	C:\ProgramData\Microsoft\Windows\...: SUCCESS	Desired Access: R...	
08:27...	svchost.exe	2644	LockFile	C:\ProgramData\Microsoft\Windows\...: SUCCESS	Exclusive: False, O...	
08:27...	svchost.exe	1020	LockFile	C:\ProgramData\Microsoft\Windows\...: SUCCESS	Query: HandleTag...	
08:27...	svchost.exe	2644	LockFile	C:\ProgramData\Microsoft\Windows\...: SUCCESS	Desired Access: R...	

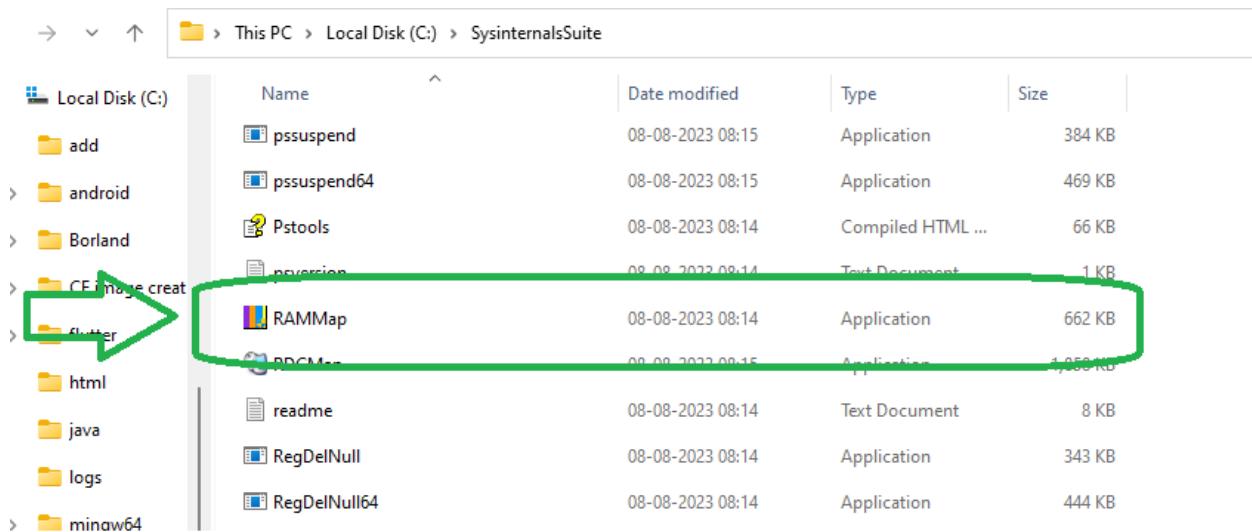
Capture RAM

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:

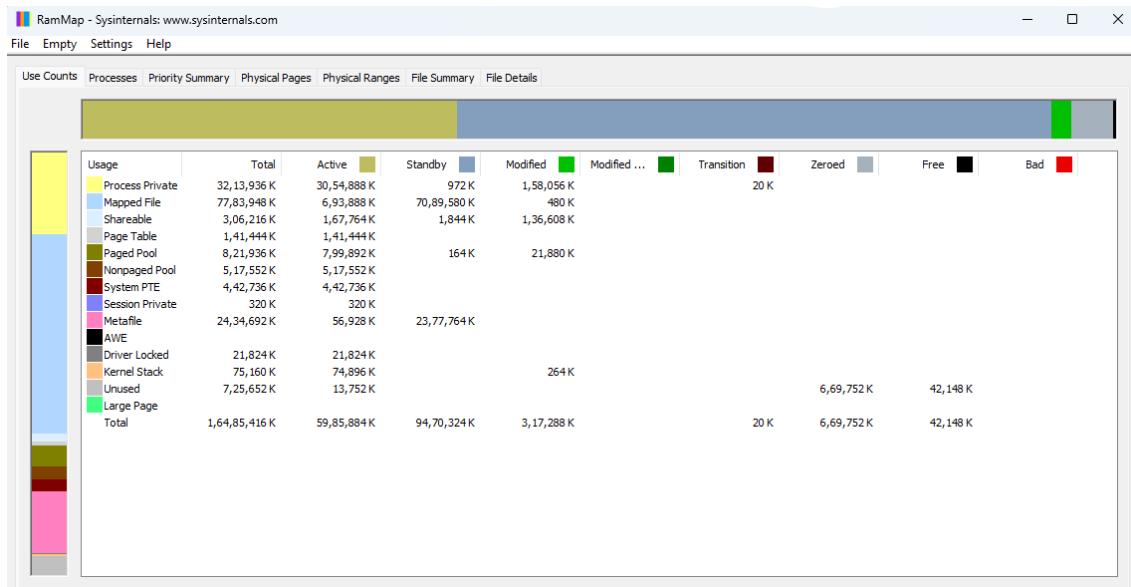
- **Use Counts:** usage summary by type and paging list
- **Processes:** process working set sizes
- **Priority Summary:** prioritized standby list sizes
- **Physical Pages:** per-page use for all physical memory
- **Physical Ranges:** physical memory addresses
- **File Summary:** file data in RAM by 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 or menu item to toggle the display of resolved names.

Using Tcpcvcon

Tcpcvcon usage is similar to that of the built-in Windows netstat utility

Usage

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

STEPS

Download TCPView

	Name	Date modified	Type	Size
Local Disk (C)	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
Borland	tcpview	08-08-2023 08:15	Application	923 KB
	tcpview64	08-08-2023 08:15	Application	1,053 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

```

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
  
```

TCPView - Sysinternals: www.sysinternals.com

File Edit View Process Connection Options Help

4 TCP v4 6 TCP v6 4 UDP v4 6 UDP v6 Search

Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Time	Module Name
svchost.exe	1328	TCP	Listen	0.0.0.0	135	0.0.0.0	0	29-08-2023 07:05:11	RpcSs
System	4	TCP	Listen	192.168.10.28	139	0.0.0.0	0	29-08-2023 08:36:37	System
System	4	TCP	Listen	192.168.44.1	139	0.0.0.0	0	29-08-2023 08:36:35	System
System	4	TCP	Listen	192.168.80.1	139	0.0.0.0	0	29-08-2023 08:36:35	System
vmware-authd.exe	5800	TCP	Listen	0.0.0.0	902	0.0.0.0	0	29-08-2023 07:05:12	VMAuthdService
vmware-authd.exe	5800	TCP	Listen	0.0.0.0	912	0.0.0.0	0	29-08-2023 07:05:12	VMAuthdService
sqlserv.exe	8936	TCP	Listen	127.0.0.1	1434	0.0.0.0	0	29-08-2023 07:05:15	MSSQLSERVER
mysqld.exe	4652	TCP	Listen	0.0.0.0	3306	0.0.0.0	0	29-08-2023 07:05:13	MySQL
epmd.exe	6996	TCP	Listen	0.0.0.0	4369	0.0.0.0	0	29-08-2023 07:05:13	epmd.exe
epmd.exe	6996	TCP	Established	127.0.0.1	4369	127.0.0.1	49694	29-08-2023 07:05:13	CDPSvc
svchost.exe	10804	TCP	Listen	0.0.0.0	5040	0.0.0.0	0	29-08-2023 08:36:32	svchost.exe
erl.exe	6756	TCP	Listen	127.0.0.1	5984	0.0.0.0	0	29-08-2023 07:05:14	erl.exe
emlproxy.exe	4496	TCP	Listen	127.0.0.1	17400	0.0.0.0	0	29-08-2023 07:05:11	Core Mail Protection
mongod.exe	4688	TCP	Listen	127.0.0.1	27017	0.0.0.0	0	29-08-2023 07:05:12	MongoDB
lsass.exe	688	TCP	Listen	0.0.0.0	49664	0.0.0.0	0	29-08-2023 07:05:11	lsass.exe
wininit.exe	936	TCP	Listen	0.0.0.0	49665	0.0.0.0	0	29-08-2023 07:05:11	wininit.exe
svchost.exe	1944	TCP	Listen	0.0.0.0	49666	0.0.0.0	0	29-08-2023 07:05:11	svchost.exe
svchost.exe	2980	TCP	Listen	0.0.0.0	49667	0.0.0.0	0	29-08-2023 07:05:11	EventLog
smonler.exe	4164	TCP	Listen	0.0.0.0	49668	0.0.0.0	0	29-08-2023 07:05:11	smonler.exe

Endpoints: 117 Established: 15 Listening: 37 Time Wait: 9 Close Wait: 6 Update: 2 sec States: (All)

TCPView - Sysinternals: www.sysinternals.com

File Edit View Process Connection Options Help

4 TCP v4 6 TCP v6 4 UDP v4 6 UDP v6 Search

Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Time	Module Name
svchost.exe	6108	UDP	127.0.0.1	51273	*	29-08-2023 08:36:36	SSDP_SRV		
WINWORD.EXE	5704	UDP	127.0.0.1	51807	*	29-08-2023 07:08:11	WINWORD.EXE		
svchost.exe	2140	UDP	127.0.0.1	52266	*	29-08-2023 07:05:13	netprofm		
dashHost.exe	3764	UDP	0.0.0.0	61128	*	29-08-2023 08:36:46	dashHost.exe		
chrome.exe	15968	UDP	0.0.0.0	5353	*	29-08-2023 08:36:46	chrome.exe		
chrome.exe	15968	UDP	0.0.0.0	5353	*	29-08-2023 08:36:46	chrome.exe		
chrome.exe	15968	UDP	0.0.0.0	5353	*	29-08-2023 08:36:46	chrome.exe		
svchost.exe	1536	UDPV6	::	123	*	29-08-2023 08:37:16	W32Time		
svchost.exe	4544	UDPV6	::	500	*	29-08-2023 07:05:11	IKEEXT		
svchost.exe	6108	UDPV6	::1	1900	*	29-08-2023 08:36:35	SSDP_SRV		
svchost.exe	6108	UDPV6	fe80::3b4f:9f72:34ab:146	1900	*	29-08-2023 08:36:35	SSDP_SRV		
svchost.exe	6108	UDPV6	fe80::3b4f:9f72:34ab:146	1900	*	29-08-2023 08:36:35	SSDP_SRV		
svchost.exe	6108	UDPV6	fe80::3b4f:9f72:34ab:146	1900	*	29-08-2023 08:36:35	SSDP_SRV		
dashHost.exe	3764	UDPV6	::	3702	*	29-08-2023 08:36:46	dashHost.exe		
dashHost.exe	3764	UDPV6	::	3702	*	29-08-2023 08:36:46	dashHost.exe		
svchost.exe	4544	UDPV6	::	4500	*	29-08-2023 07:05:11	IKEEXT		
chrome.exe	15968	UDPV6	::	5353	*	29-08-2023 08:36:46	chrome.exe		
svchost.exe	1772	UDPV6	::	5353	*	29-08-2023 08:36:37	DnsCache		
chrome.exe	15968	UDPV6	::	5353	*	29-08-2023 08:36:46	chrome.exe		

Endpoints: 122 Established: 15 Listening: 37 Time Wait: 10 Close Wait: 6 Update: 2 sec States: (All)

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

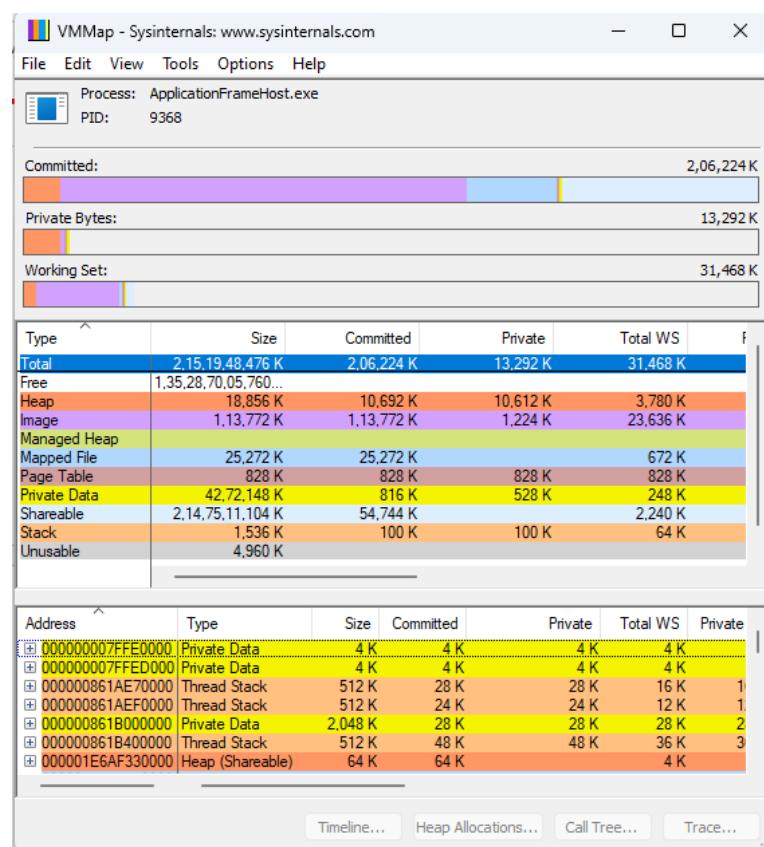
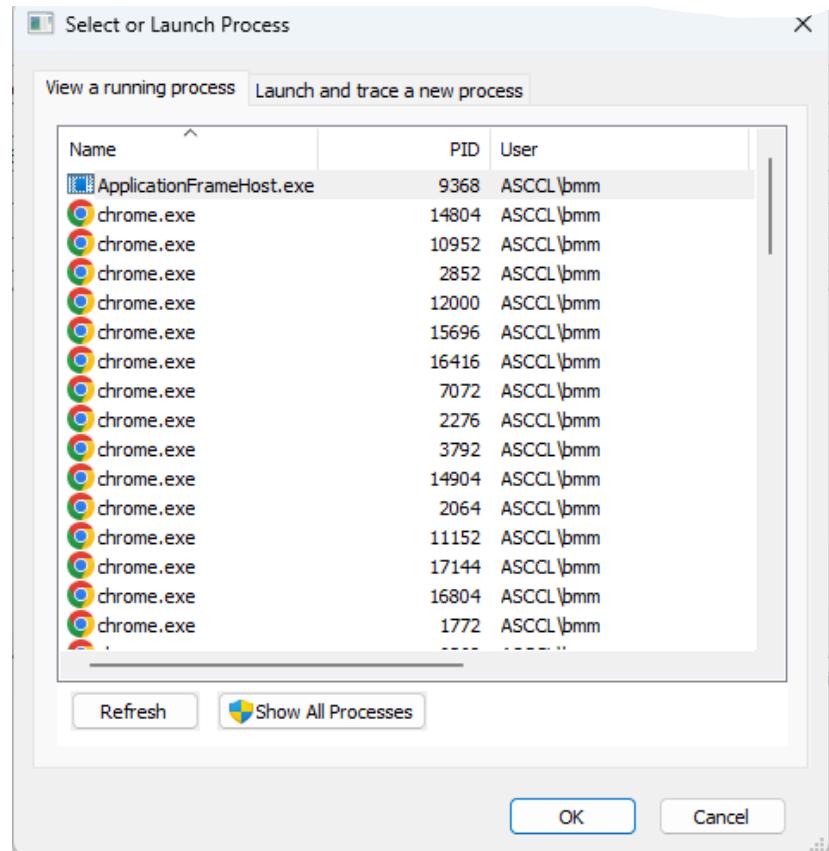
#	Time	Duration (s)	Disk	Request	Sector	Length	
345	42.980874	0.00000000	1	Write	377607112	160	
346	42.980944	0.00000000	1	Write	377481320	8	
347	42.981136	0.00000000	1	Write	377481184	8	
348	42.982512	0.00000000	0	Write	6104864	32	
349	42.982624	0.00000000	0	Write	6102944	8	
350	42.996067	0.00000000	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	46.828938	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

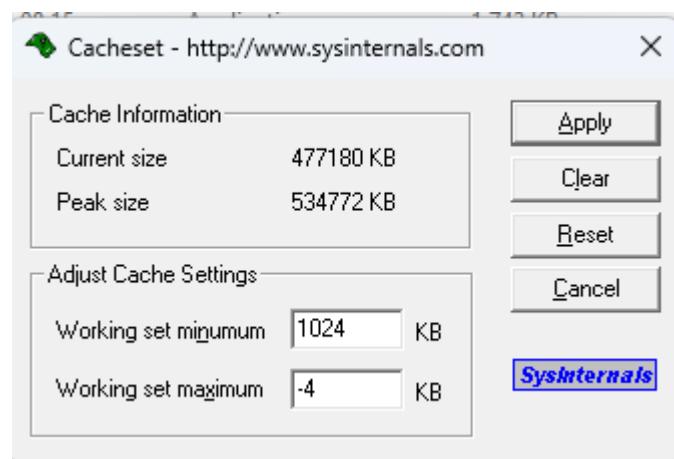
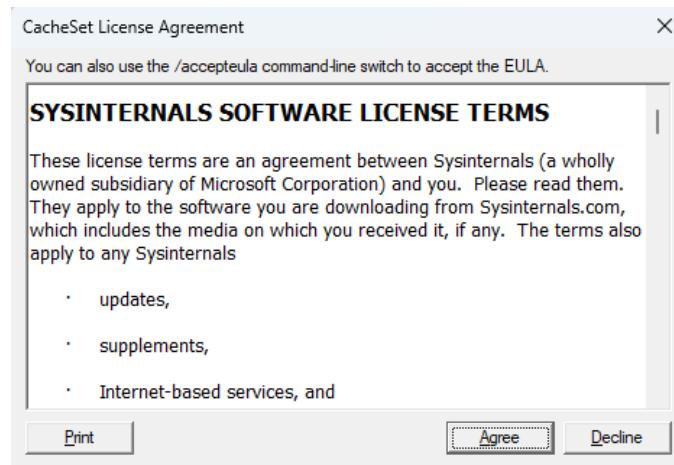
Sysinternal → VMMAP



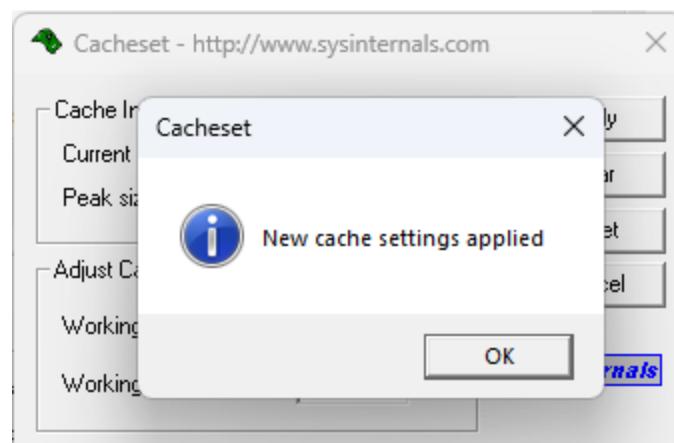
Monitor Cache Memory

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

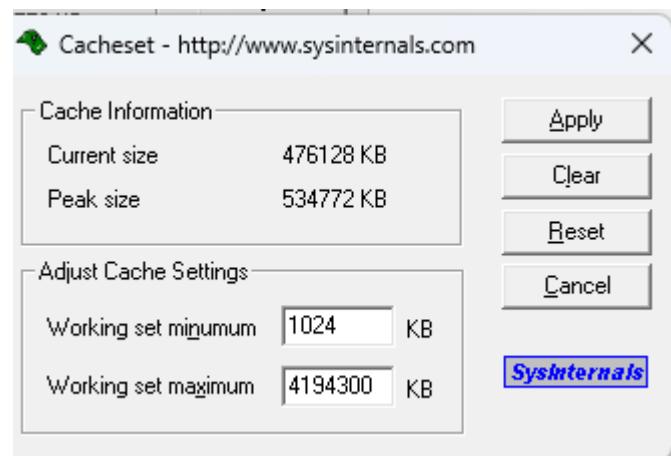
Give all the permissions and Click on Agree



Click on apply



After applying the changes



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

 New Case Information X

Steps

1. Case Information
2. Optional Information

Case Information

Case Name:

Base Directory: Browse

Case Type: Single-user Multi-user

Case data will be stored in the following directory:

< Back Next > Finish Cancel Help

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

 New Case Information X

Steps

1. Case Information
2. Optional Information

Optional Information

Case

Number:

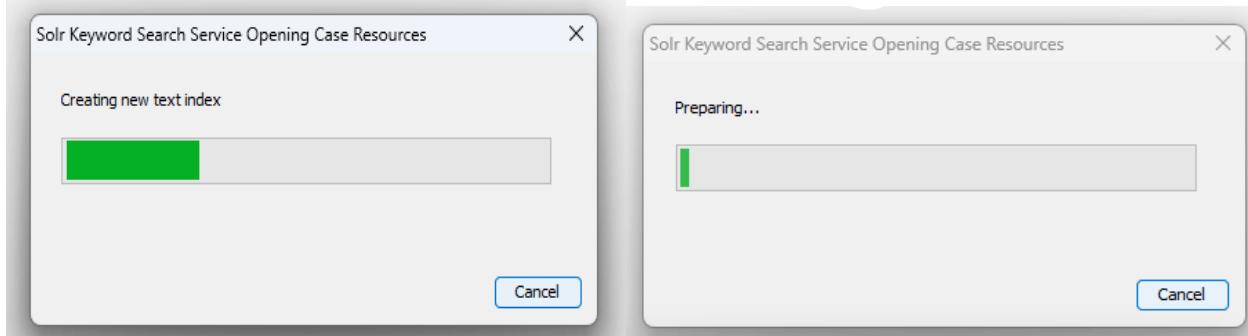
Examiner

Name:
Phone:
Email:
Notes:

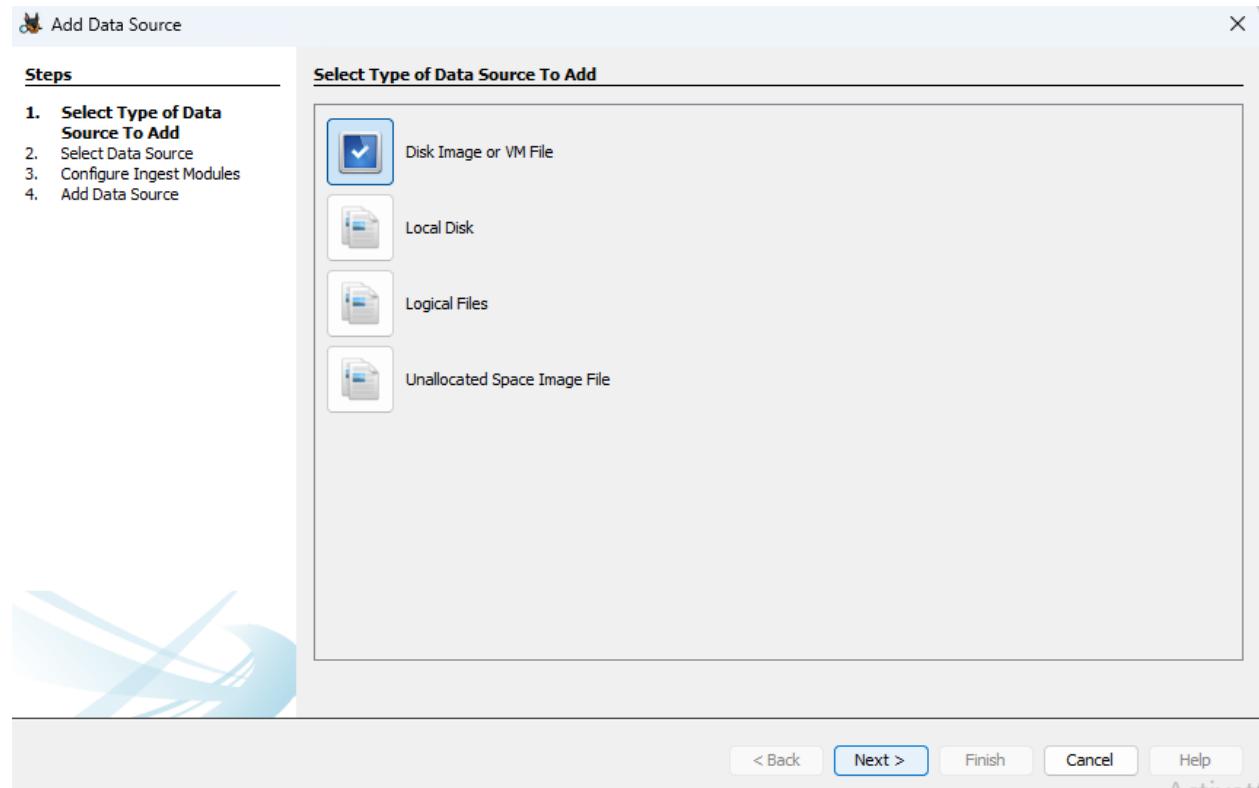
Organization

Organization analysis is being done for: Manage Organizations

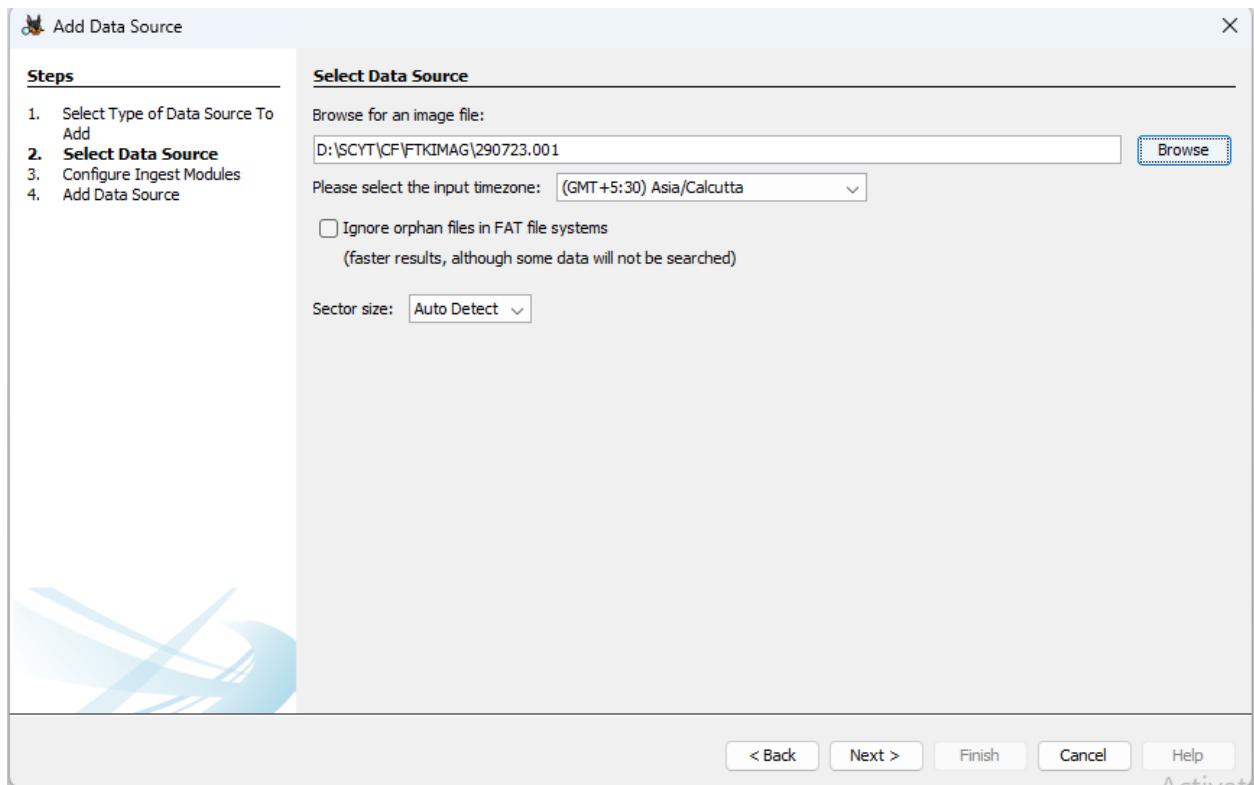
< Back Next > Finish Cancel Help



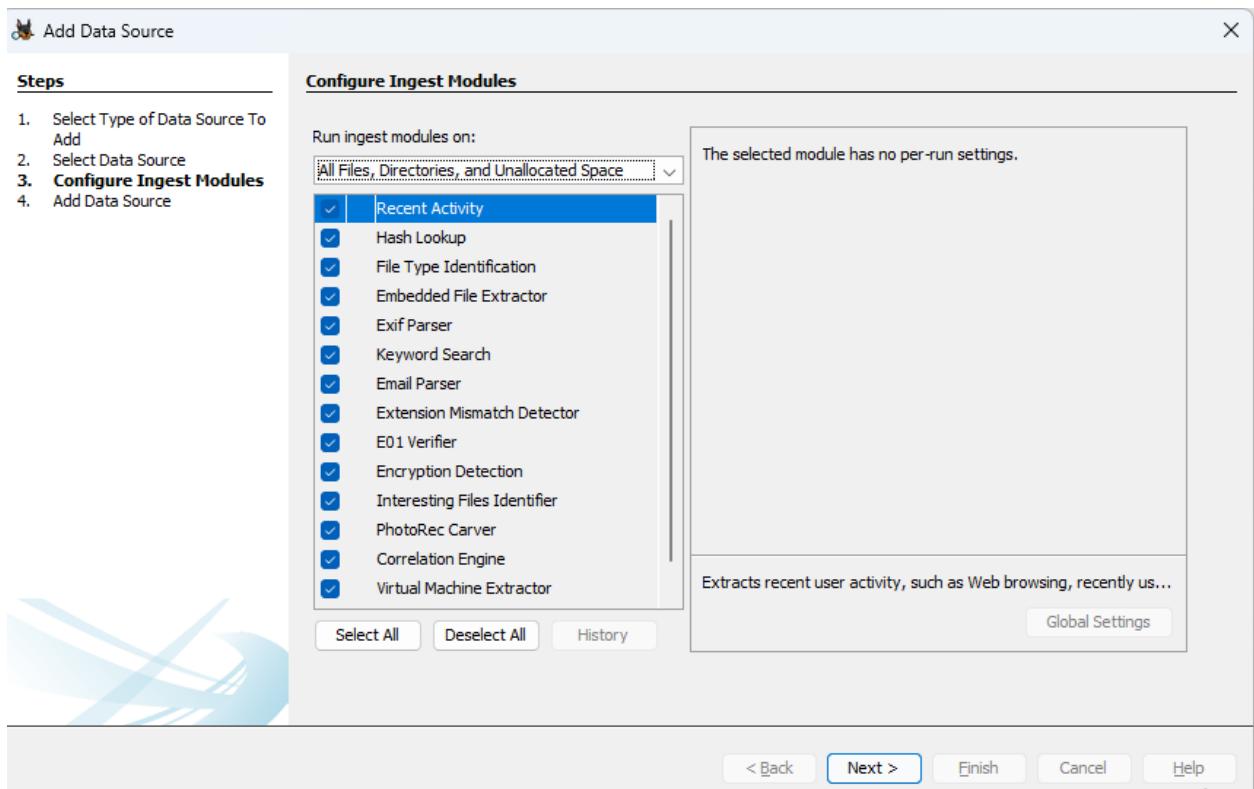
Select on Disk Image or VM File and Click Next



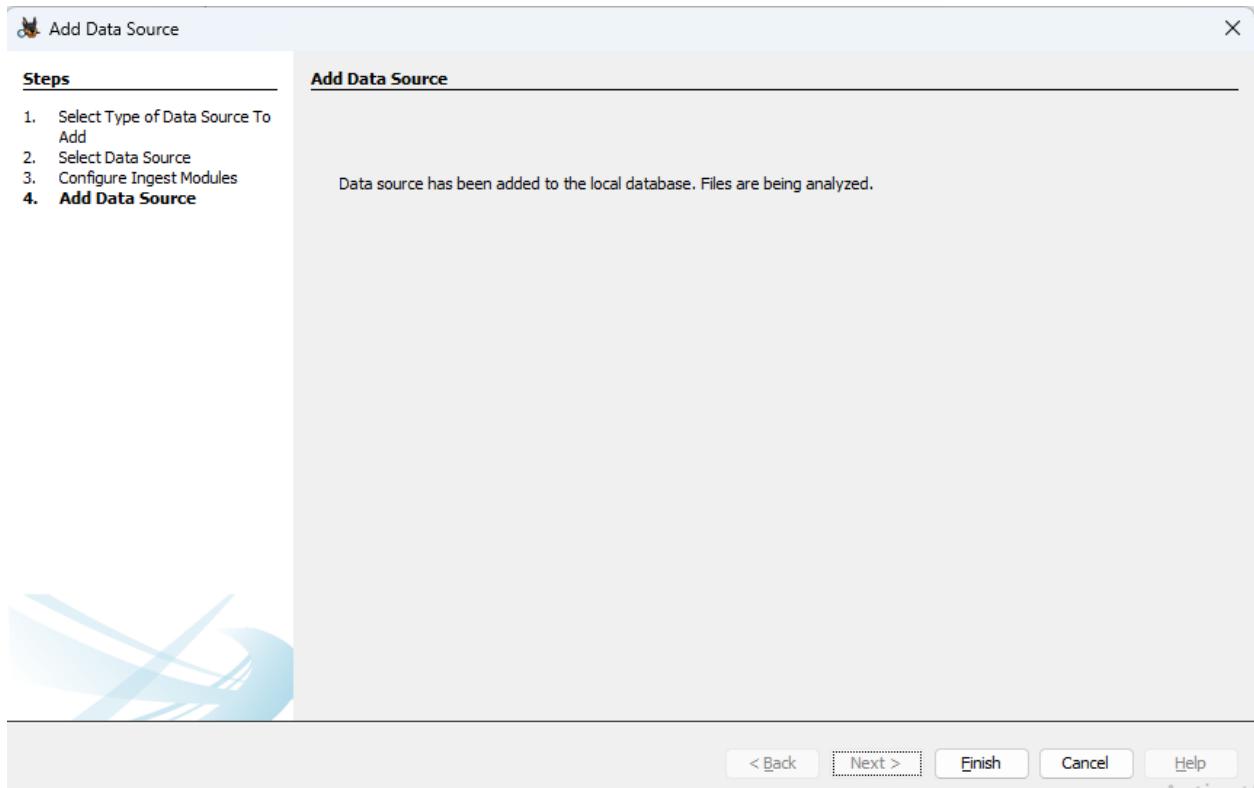
Give the destination of the image and click next



Select the ingest module and click next



See the acknowledgement and click finish



Now we check the files recovered

The screenshot shows the Autopsy 4.9.1 interface with the following details:

- Case:** 290723 - Autopsy 4.9.1
- Menu:** Case, View, Tools, Window, Help
- Toolbar:** Add Data Source, Images/Videos, Communications, Timeline, Generate Report, Close Case.
- Left Sidebar:** Data Sources (290723.001), Views (File Types, Deleted Files, File System (21), All (21)), MB File Size, Results (Extracted Content, Keyword Hits, Single Literal Keyword Search (0), Single Regular Expression Search (0)), Hashset Hts, E-Mail Messages, Interesting Items, Accounts, Tags, Reports.
- Central Area:** File System table with 21 results.

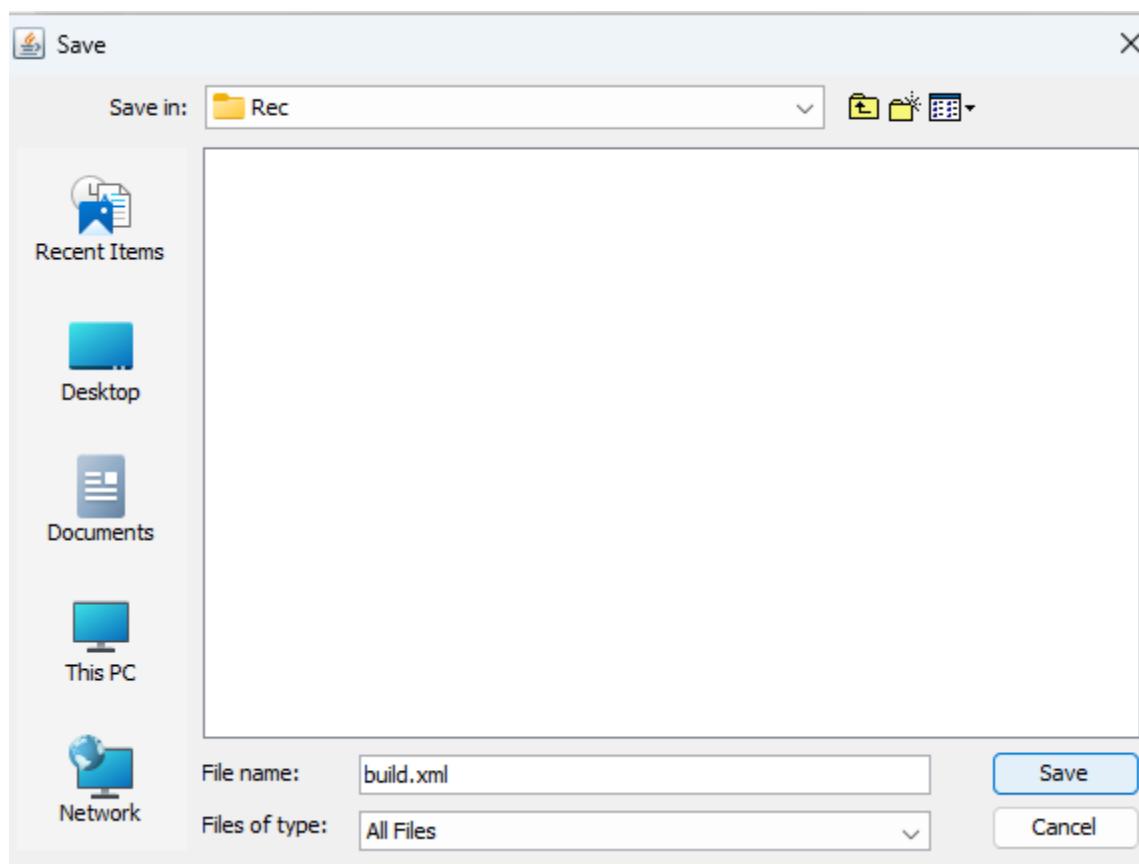
Name	S	C	Location	Modified Time	Change Time	Access Time	Count
EFISECTOR			/img_290723.001/vol_v02/\$OrphanFiles/EFISECTOR	2019-12-06 17:05:28 IST	0000-00-00 00:00:00	0000-00-00 00:00:00	0
EFI			/img_290723.001/vol_v02/\$OrphanFiles/EFI	2019-12-06 09:05:28 IST	0000-00-00 00:00:00	2019-12-06 00:00:00 IST	2
BOOT			/img_290723.001/vol_v02/\$OrphanFiles/BOOT	2019-12-06 09:05:28 IST	0000-00-00 00:00:00	2019-12-06 00:00:00 IST	2
BOOTX64.EFI			/img_290723.001/vol_v02/\$OrphanFiles/BOOTX64.EFI	2019-12-06 17:05:16 IST	0000-00-00 00:00:00	2019-12-06 00:00:00 IST	2
EFISECTOR			/img_290723.001/vol_v02/\$OrphanFiles/EFISECTOR	2019-12-06 17:05:30 IST	0000-00-00 00:00:00	0000-00-00 00:00:00	0
EFI			/img_290723.001/vol_v02/\$OrphanFiles/EFI	2019-12-06 09:05:30 IST	0000-00-00 00:00:00	2019-12-06 00:00:00 IST	2
BOOT			/img_290723.001/vol_v02/\$OrphanFiles/BOOT	2019-12-06 09:05:30 IST	0000-00-00 00:00:00	2019-12-06 00:00:00 IST	2
BOOTX64.EFI			/img_290723.001/vol_v02/\$OrphanFiles/BOOTX64.EFI	2019-12-06 17:05:18 IST	0000-00-00 00:00:00	2019-12-06 00:00:00 IST	2
build.xml			/img_290723.001/vol_v02/\$OrphanFiles/build.xml	2022-09-26 14:06:42 IST	0000-00-00 00:00:00	2023-01-07 00:00:00 IST	2
build			/img_290723.001/vol_v02/\$OrphanFiles/build	2022-09-26 14:22:28 IST	0000-00-00 00:00:00	2023-01-07 00:00:00 IST	2
lib			/img_290723.001/vol_v02/\$OrphanFiles/lib	2022-09-26 14:06:44 IST	0000-00-00 00:00:00	2023-01-07 00:00:00 IST	2
NBPROJ~1			/img_290723.001/vol_v02/\$OrphanFiles/NBPROJ~1	2022-09-26 14:06:42 IST	0000-00-00 00:00:00	2023-01-07 00:00:00 IST	2
src			/img_290723.001/vol_v02/\$OrphanFiles/src	2022-09-26 14:06:42 IST	0000-00-00 00:00:00	2023-01-07 00:00:00 IST	2
web			/img_290723.001/vol_v02/\$OrphanFiles/web	2022-09-26 14:19:02 IST	0000-00-00 00:00:00	2023-01-07 00:00:00 IST	2
H^~L^~H~,^\$			/img_290723.001/vol_v02/\$OrphanFiles/H^~L^~H~,^\$	1998-04-04 17:26:16 IST	0000-00-00 00:00:00	1980-07-16 00:00:00 IST	1
H^~L^~H~,^\$^			/img_290723.001/vol_v02/\$OrphanFiles/H^~L^~H~,^\$^	1998-04-04 17:26:16 IST	0000-00-00 00:00:00	1980-07-16 00:00:00 IST	1
~~~~~@#@			/img_290723.001/vol_v02/\$OrphanFiles/~~~~~@#@	2004-01-16 06:00:00 IST	0000-00-00 00:00:00	0000-00-00 00:00:00	0
tf@D\$pH~,^\$^			/img_290723.001/vol_v02/\$OrphanFiles/tf@D\$pH~,^\$^	1998-04-04 17:10:16 IST	0000-00-00 00:00:00	1980-05-08 00:00:00 IST	1
~~~~~@#@			/img_290723.001/vol_v02/\$OrphanFiles/~~~~~@#@	2000-09-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0
~~~m!~~~^~~~			/img_290723.001/vol_v02/\$OrphanFiles/~~~m!~~~^~~~	1981-09-30 16:26:02 IST	0000-00-00 00:00:00	1980-04-08 00:00:00 IST	1
f693ba26.83a			/img_290723.001/vol_v02/\$OrphanFiles/f693ba26.83a	1992-08-10 03:56:04 IST	0000-00-00 00:00:00	2007-01-17 00:00:00 IST	2

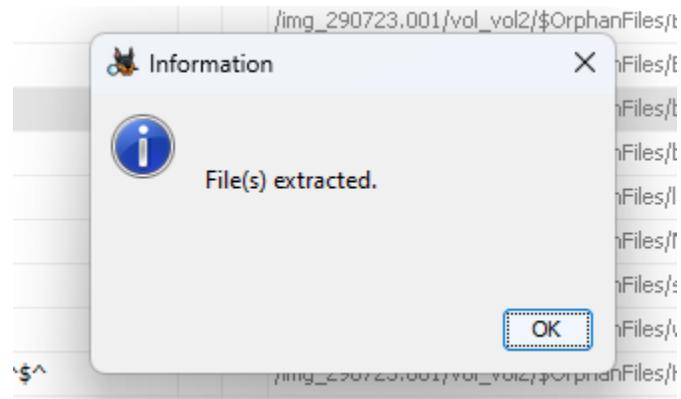
We see the Deleted Files

Now We Extract/Recover some deleted files

X	BOOT	/img_290723.001/vol_vol2/\$OrphanFiles/BOOT	2019-1
X	BOOTX64.EFI	/img_290723.001/vol_vol2/\$OrphanFiles/BOOTX64.EFI	2019-1
X	build.xml		2022-C
X	build		2022-C
X	lib		2022-C
X	NBPROJ~1		
X	src		2022-C
X	web		2022-C
X	H^^L^^H^,^\$^		
X	H^^L^^H^,^\$^		
X	^^^^^^^^,@@@		
X	tf^D\$pH^,^\$^		
X	^^^^^^^^,^^^		
X	^^^mV^^^,^^^		
X	f693ba26.83a		1992-C
<input checked="" type="checkbox"/>	f0048429.txt	/img_290723.001/vol_vol2//\$CarvedFiles/f0048429.txt	0000-C

Set a directory for the recovered files

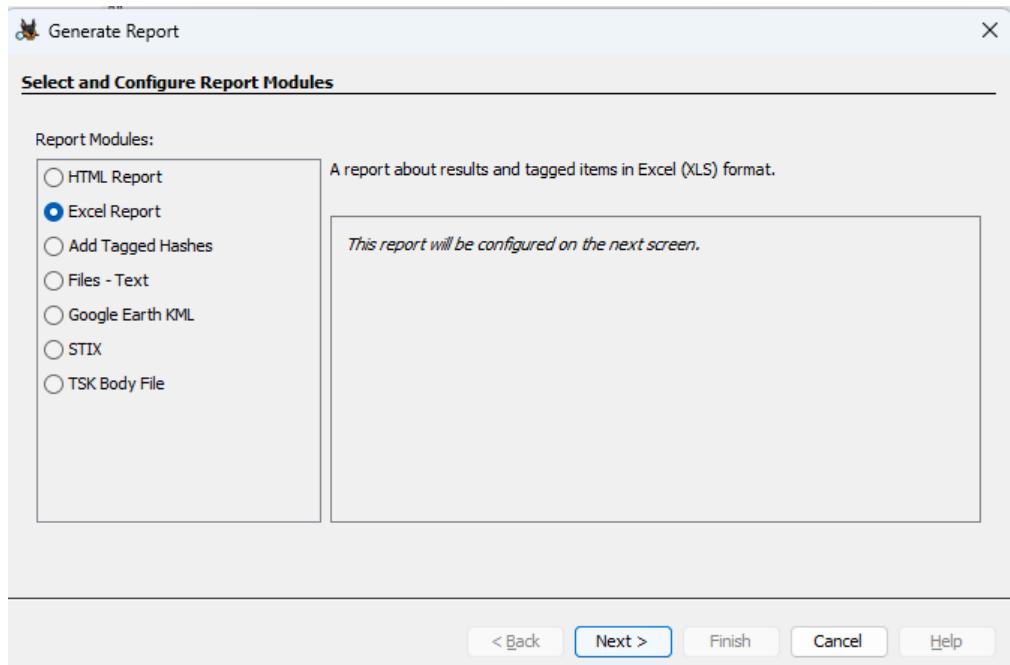




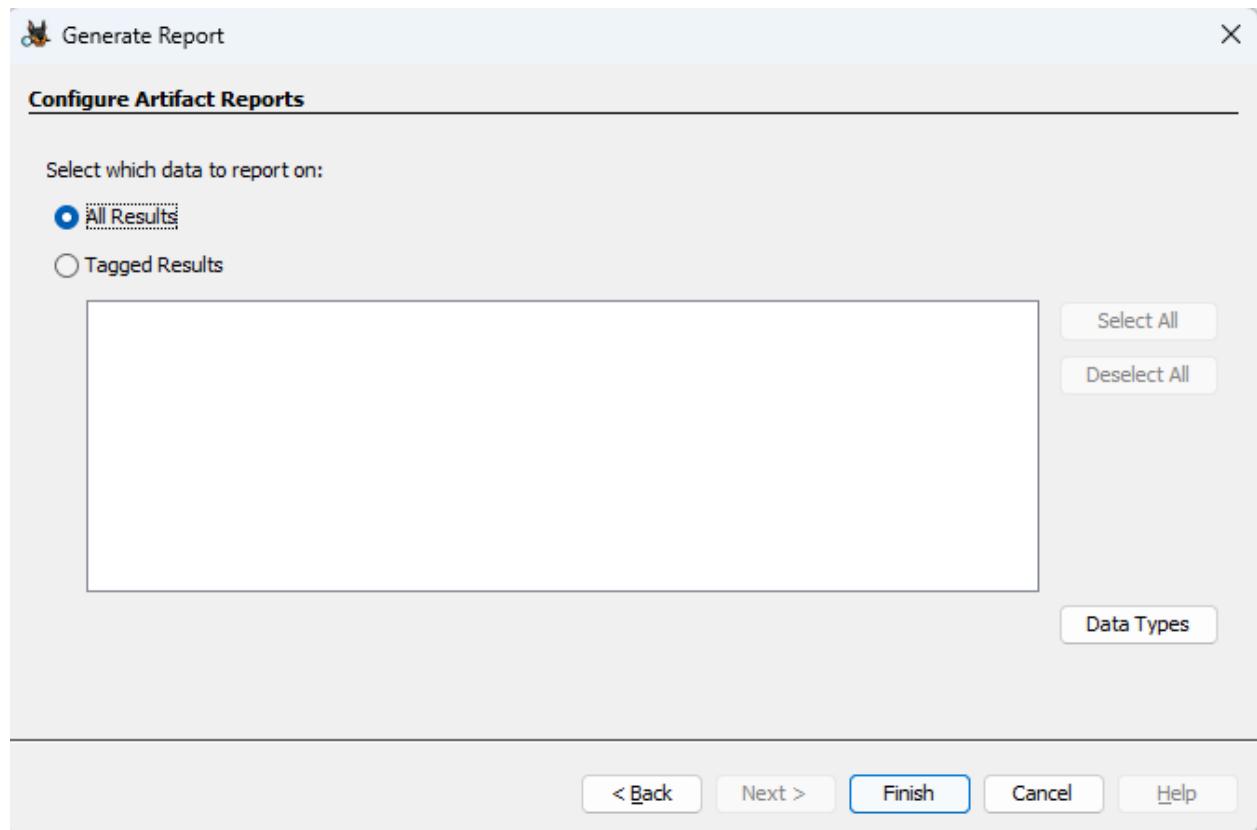
Now we Generate a Report of the Autopsy done

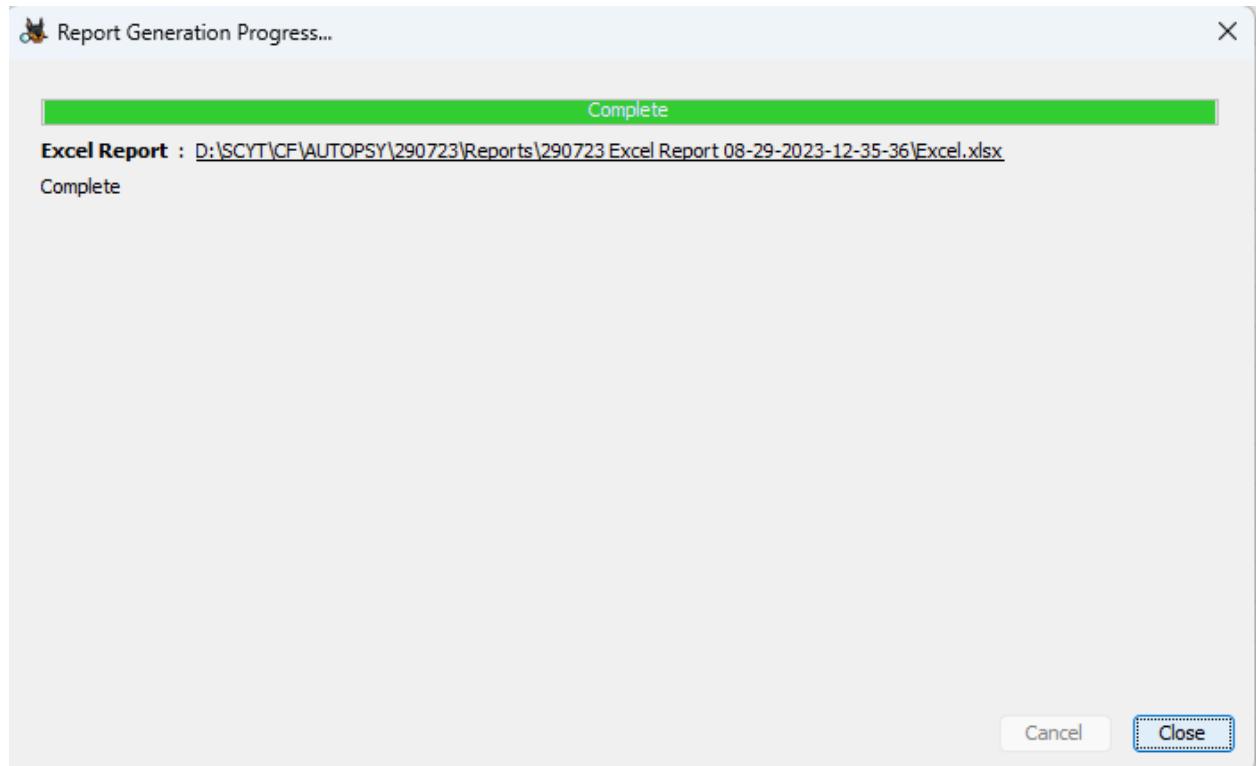
Name	S	C	Location	Modified Time	Change Time	Access Time
BOOTX64.EFI			/img_290723.001/vol_vo2/\$OrphanFiles/BOOTX64.EFI	2019-12-06 17:05:16 IST	0000-00-00 00:00:00	2019-12-06 00:00:00 IST
EFISECTOR			/img_290723.001/vol_vo2/\$OrphanFiles/EFISECTOR	2019-12-06 17:05:30 IST	0000-00-00 00:00:00	0000-00-00 00:00:00
EFI			/img_290723.001/vol_vo2/\$OrphanFiles/EFI	2019-12-06 09:05:30 IST	0000-00-00 00:00:00	2019-12-06 00:00:00 IST
BOOT			/img_290723.001/vol_vo2/\$OrphanFiles/BOOT	2019-12-06 09:05:30 IST	0000-00-00 00:00:00	2019-12-06 00:00:00 IST
BOOTX64.EFI			/img_290723.001/vol_vo2/\$OrphanFiles/BOOTX64.EFI	2019-12-06 17:05:18 IST	0000-00-00 00:00:00	2019-12-06 00:00:00 IST
build.xml			/img_290723.001/vol_vo2/\$OrphanFiles/build.xml	2022-09-26 14:06:42 IST	0000-00-00 00:00:00	2023-01-07 00:00:00 IST
build			/img_290723.001/vol_vo2/\$OrphanFiles/build	2022-09-26 14:22:28 IST	0000-00-00 00:00:00	2023-01-07 00:00:00 IST
lib			/img_290723.001/vol_vo2/\$OrphanFiles/lib	2022-09-26 14:06:44 IST	0000-00-00 00:00:00	2023-01-07 00:00:00 IST
NBPROJ~1			/img_290723.001/vol_vo2/\$OrphanFiles/NBPROJ~1	2022-09-26 14:06:42 IST	0000-00-00 00:00:00	2023-01-07 00:00:00 IST
src			/img_290723.001/vol_vo2/\$OrphanFiles/src	2022-09-26 14:06:42 IST	0000-00-00 00:00:00	2023-01-07 00:00:00 IST
web			/img_290723.001/vol_vo2/\$OrphanFiles/web	2022-09-26 14:19:02 IST	0000-00-00 00:00:00	2023-01-07 00:00:00 IST
H^~L^~H^~,^\$^			/img_290723.001/vol_vo2/\$OrphanFiles/H^~L^~H^~,^\$^	1998-04-04 17:26:16 IST	0000-00-00 00:00:00	1980-07-16 00:00:00 IST
H^~L^~H^~,^\$^			/img_290723.001/vol_vo2/\$OrphanFiles/H^~L^~H^~,^\$^	1998-04-04 17:26:16 IST	0000-00-00 00:00:00	1980-07-16 00:00:00 IST
~~~~~,@@@			/img_290723.001/vol_vo2/\$OrphanFiles/~~~~~,@...	2004-01-16 06:00:00 IST	0000-00-00 00:00:00	0000-00-00 00:00:00
t^~D\$pH^~,^\$^			/img_290723.001/vol_vo2/\$OrphanFiles/t^~D\$pH^~,^\$^	1998-04-04 17:10:16 IST	0000-00-00 00:00:00	1980-05-08 00:00:00 IST
~~~~~			/img_290723.001/vol_vo2/\$OrphanFiles/~~~~~	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
~~^mV~~^~,^\$^			/img_290723.001/vol_vo2/\$OrphanFiles/~~^mV~~^~,^\$^	1981-09-30 16:26:02 IST	0000-00-00 00:00:00	1980-04-08 00:00:00 IST

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

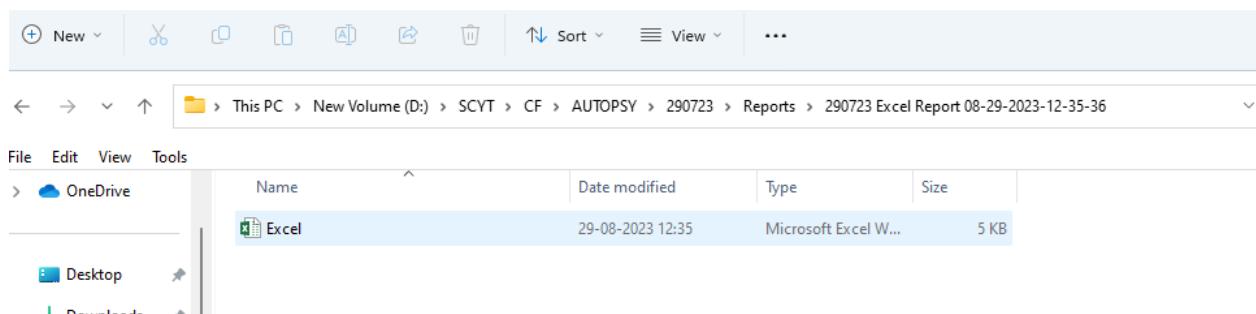


Now select all results this will generate all the reports and click finish. The other option only generate the report for tagged one only.





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



The screenshot shows a Microsoft Excel spreadsheet titled "Summary". The "Summary" tab is selected at the bottom. The data is organized into columns A through F:

	A	B	C	D	E	F
1	Summary					
2						
3	Case Name:	290723				
4	Case Number:	290723				
5	Examiner:	Maddy				
6	Number of Images:	1				
7						
8						
9						
10						
11						
12						
13						
14						
15						
16						
17						
18						
19						
20						
21						
22						

A	B	C	D	E	F
E-Mail To	E-Mail From	Subject	Date Sent	Date Received	Path
2 'Samsrade@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 'Samsrade@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 'Samsrade@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 'Samsrade@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

A	B	C	I
<b>1 Email Addresses</b>			
2 %@clients.l.google.com	Source File		Tags
3 Preview	/img_04092023_masood.001/vol_vo1//\$Unalloc/Unalloc_1878_3915776_1077723136		
4 llients.l.google.com%@clients.l.google.com%hclients.l.google.			
5 llients.l.google.com%@clients.l.google.com%hclients.l.google.	/img_04092023_masood.001/vol_vo1/\$OrphanFiles/_LLPA^1.PCA		
6 llients.l.google.com%@clients.l.google.com%hclients.l.google.	/img_04092023_masood.001/vol_vo1/\$OrphanFiles/_ROTEU^LEXE		
7 llients.l.google.com%@clients.l.google.com%hclients.l.google.	/img_04092023_masood.001/vol_vo1/\$OrphanFiles/aftnnndbn.umd		
8			
9 -239034676-0-1001@flonetwork.com			
10 Preview	Source File		Tags
11 jjz4znrtw-239034676-0-1001@flonetwork.com<[work.com]4676-0	/img_04092023_masood.001/vol_vo1//\$Unalloc/Unalloc_1878_3915776_1077723136		
12 jjz4znrtw-239034676-0-1001@flonetwork.com<[work.com]4676-0	/img_04092023_masood.001/vol_vo1/_S/Proteus 8.11 SP0 Pro HomeMade Electronics.exe		
13			
14 200612032123.609457386a225c@rly-xm04.mx.aol.com			
15 Preview	Source File		Tags
16 -05001n-reply-to:<>200612032123.609457386a225c@rly-xm04.mx.aol.com<>x-mb-message-source	/img_04092023_masood.001/vol_vo1//\$Unalloc/Unalloc_1878_3915776_1077723136		
17 -05001n-reply-to:<>200612032123.609457386a225c@rly-xm04.mx.aol.com<>x-mb-message-source	/img_04092023_masood.001/vol_vo1/_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_vo1//\$Unalloc/Unalloc_1878_3915776_1077723136		
22 7h1tmaccano_id<>20061204013940.a88906765f@mprdmxin.myway.com<>mail.comcast.net000	/img_04092023_masood.001/vol_vo1//\$CarvedFiles/f0333408.pst/AC19.gpj		

A	B	C	D
1 Review Status	ID	Tags	
2 Undecided	Samspade@myway.com		
3 Undecided	Samspade@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@gooovy.com		
13 Undecided	terrysadler@gooovy.com		
14			

A	B	C	D	
1	File	Extension	MIME Type	Path
2 AC19.gpj	gpj	image/jpeg	/img_04092023_masood.001/vol_vo1//\$OrphanFiles/_IM_SH^1.PST/AC19.gpj	
3 AC19.gpj	gpj	image/jpeg	/img_04092023_masood.001/vol_vo1//\$CarvedFiles/f0333408.pst/AC19.gpj	
4				
5				

## PRACTICAL NO. 7

### Aim:

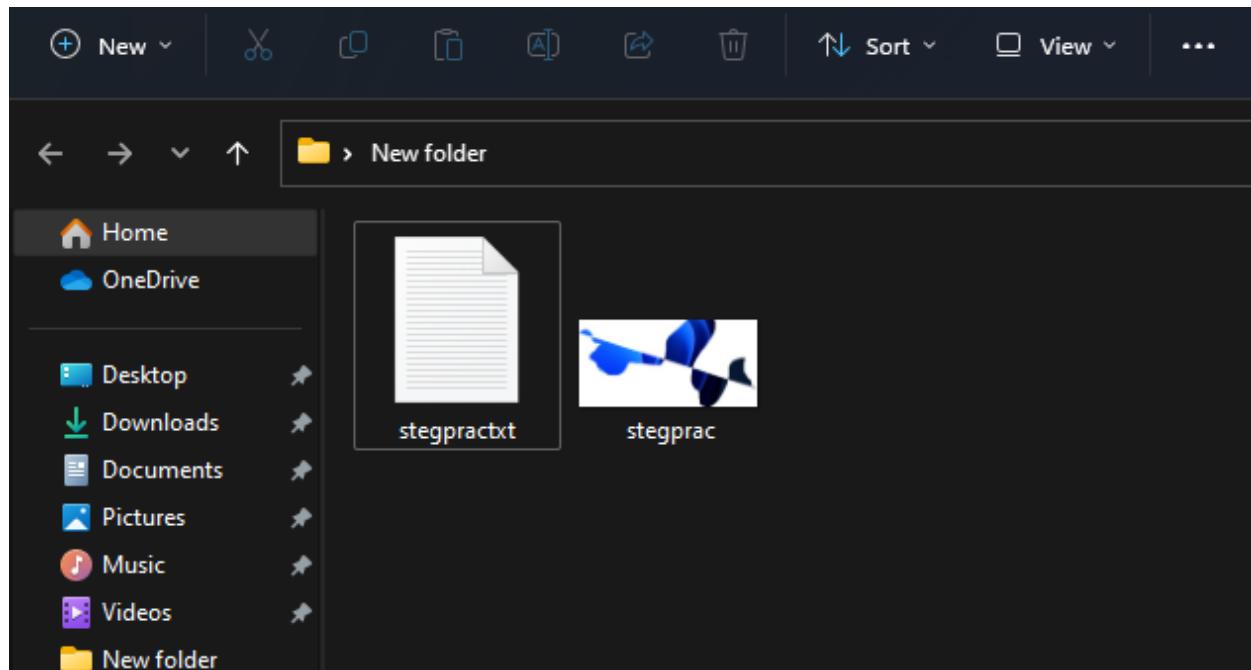
Steganography Detection

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

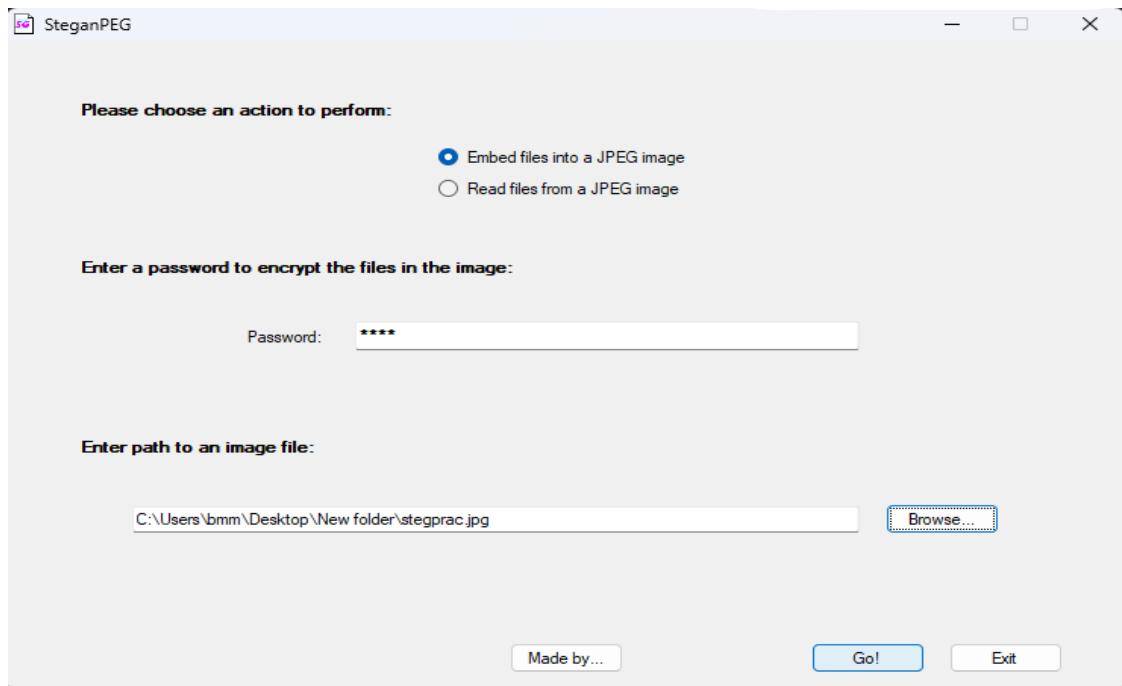
### Practical:

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

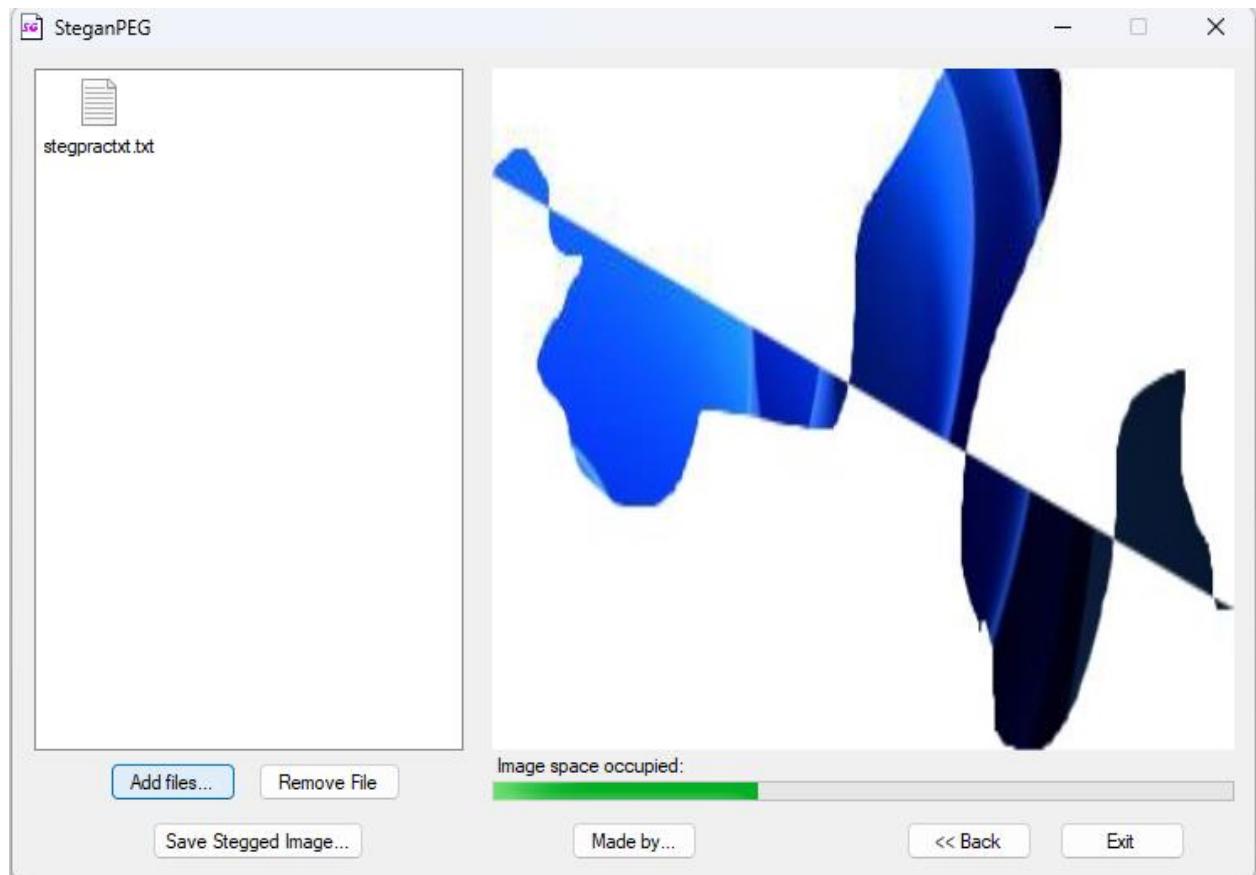
Create a folder to keep the image and message file and store the txt file and image



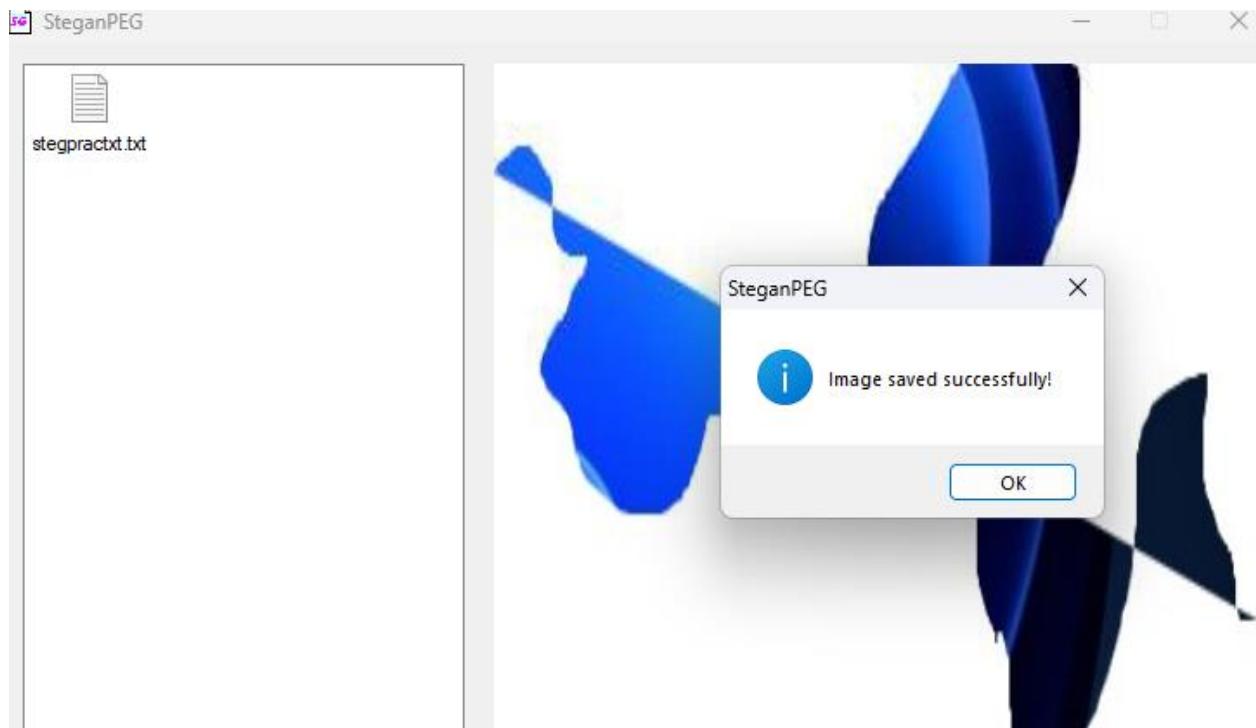
Open the SteganPEG and give a password and browse the path of the image



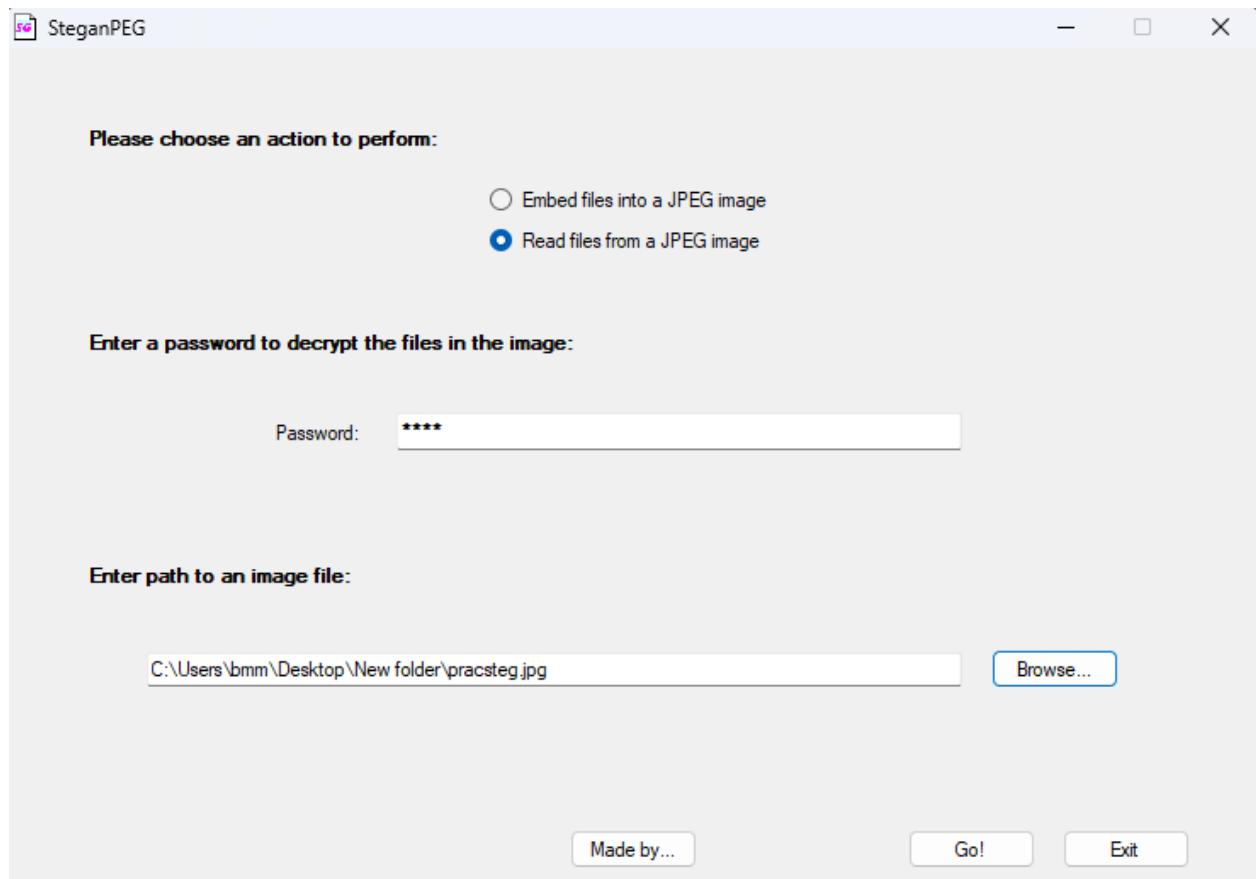
First we are going to add some files in the captured image

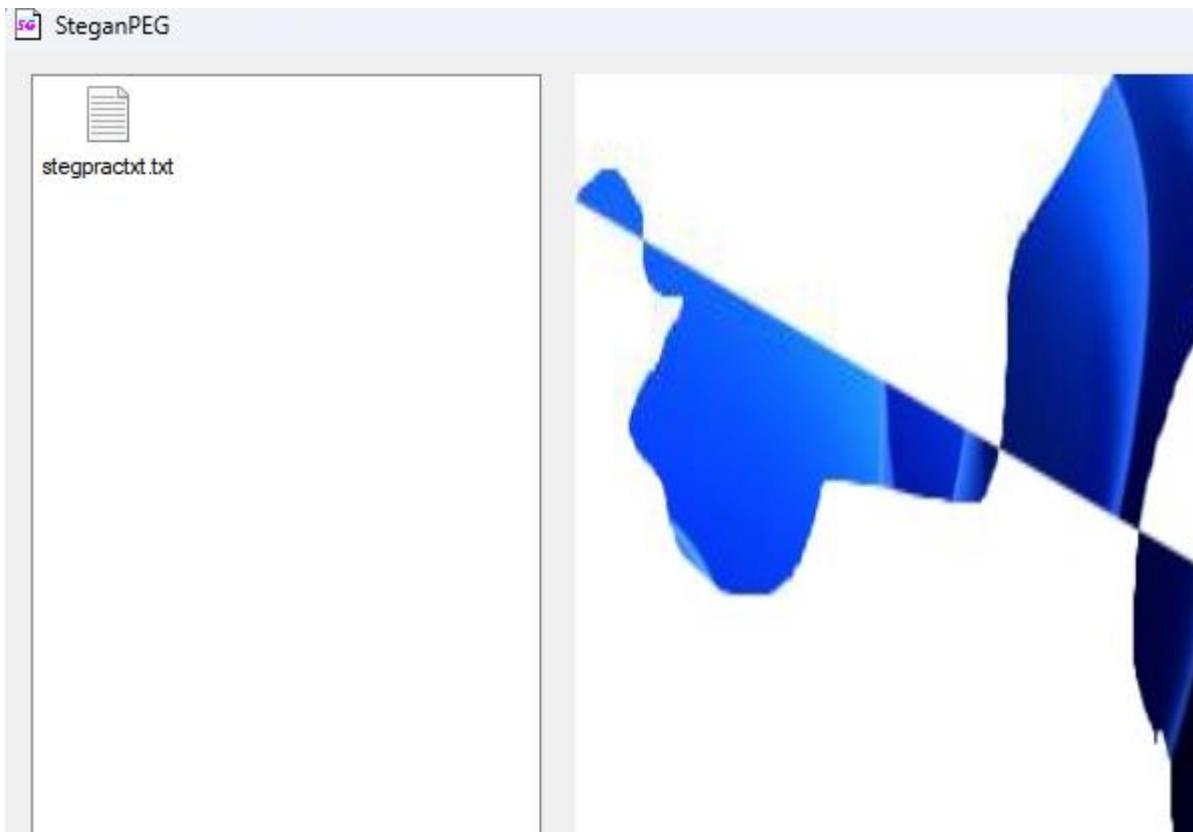


Save the stegged image



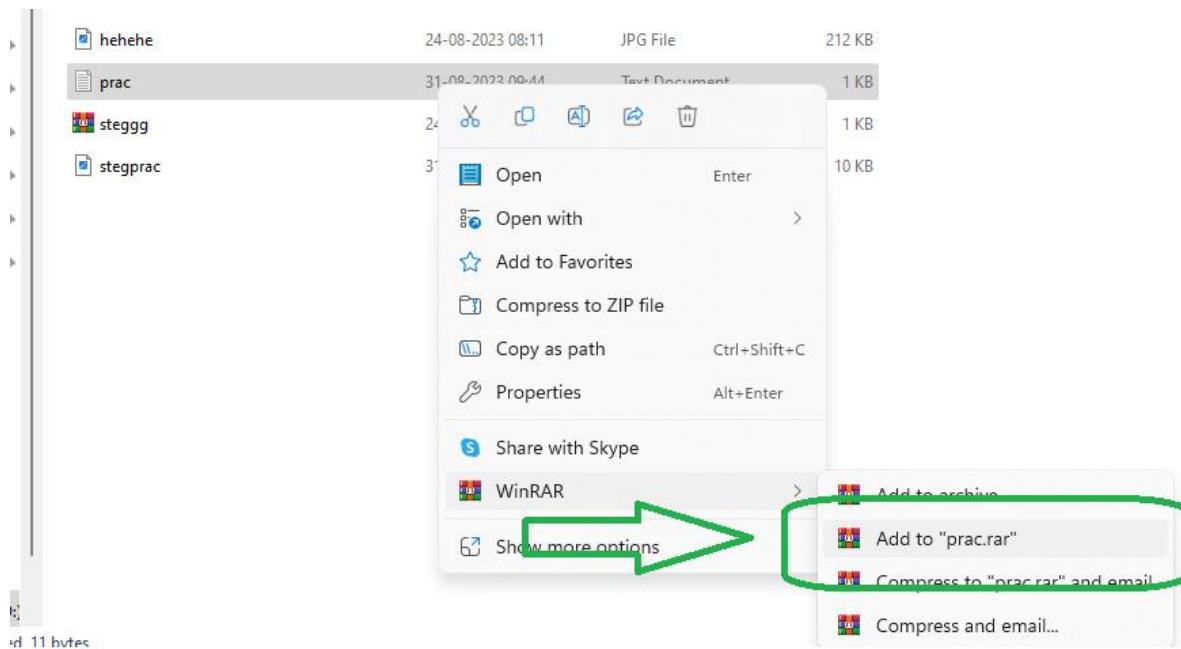
Open the saved image with the assigned password and view the image with hidden files





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.

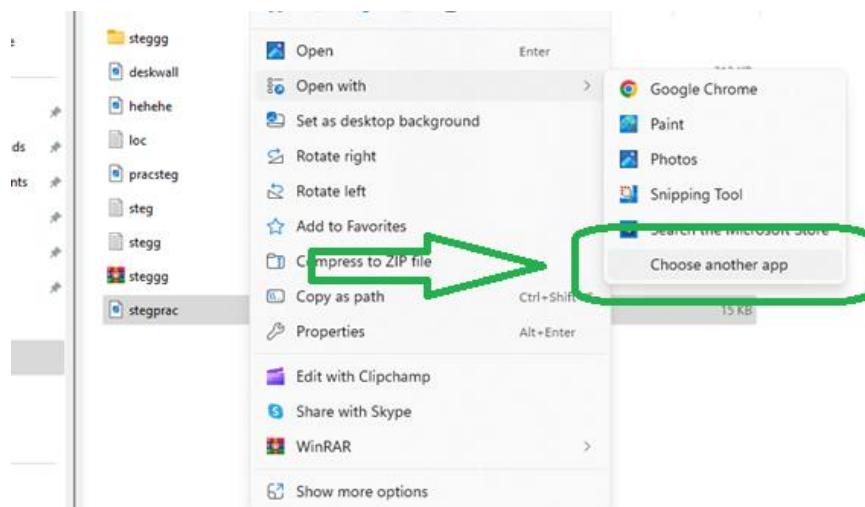
D:\SCYT\CF\STEG>
```

Then create a shortcut for WinRAR on the desktop

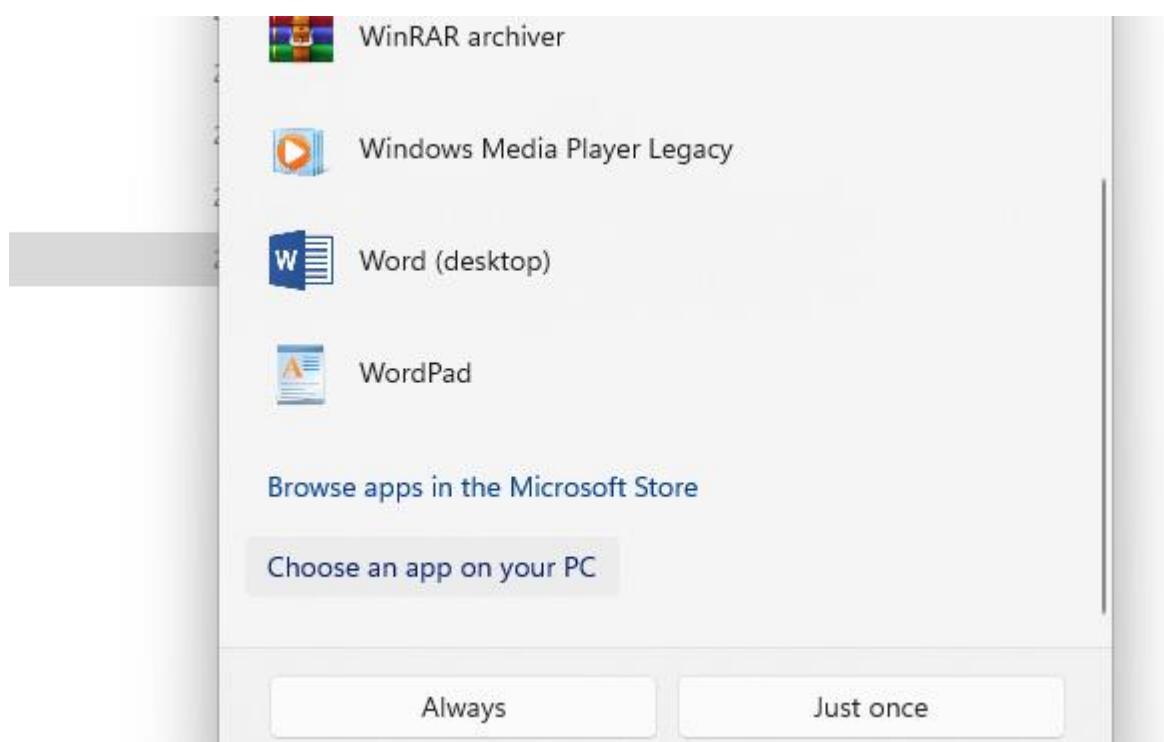


Then open the image using the shortcut

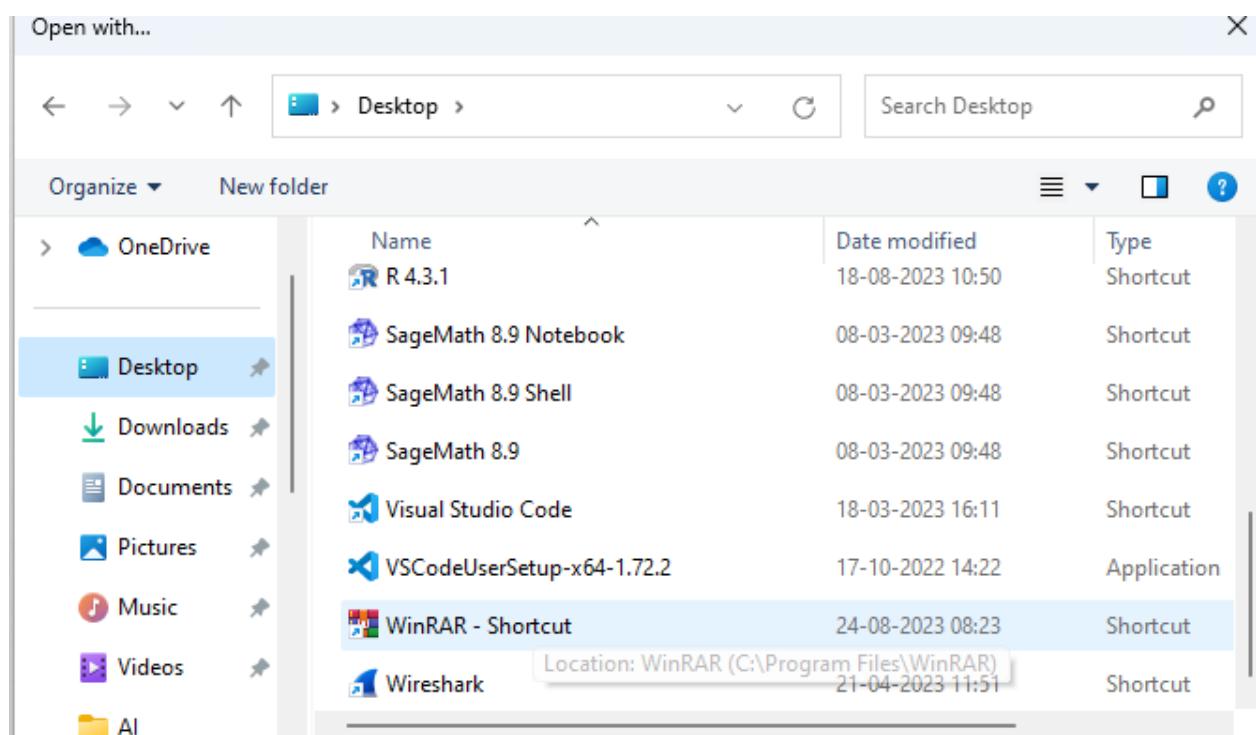
**Right Click on the image → Open with → Choose another app**

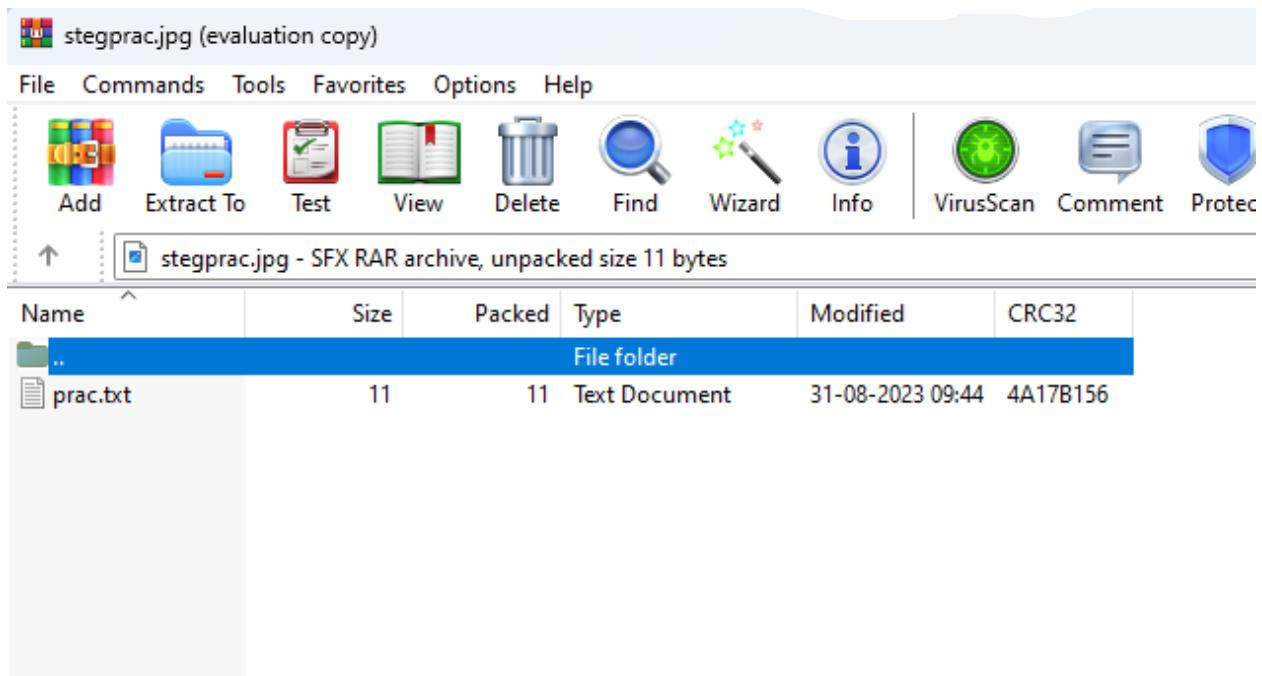


Select Choose another app → choose an app on your pc

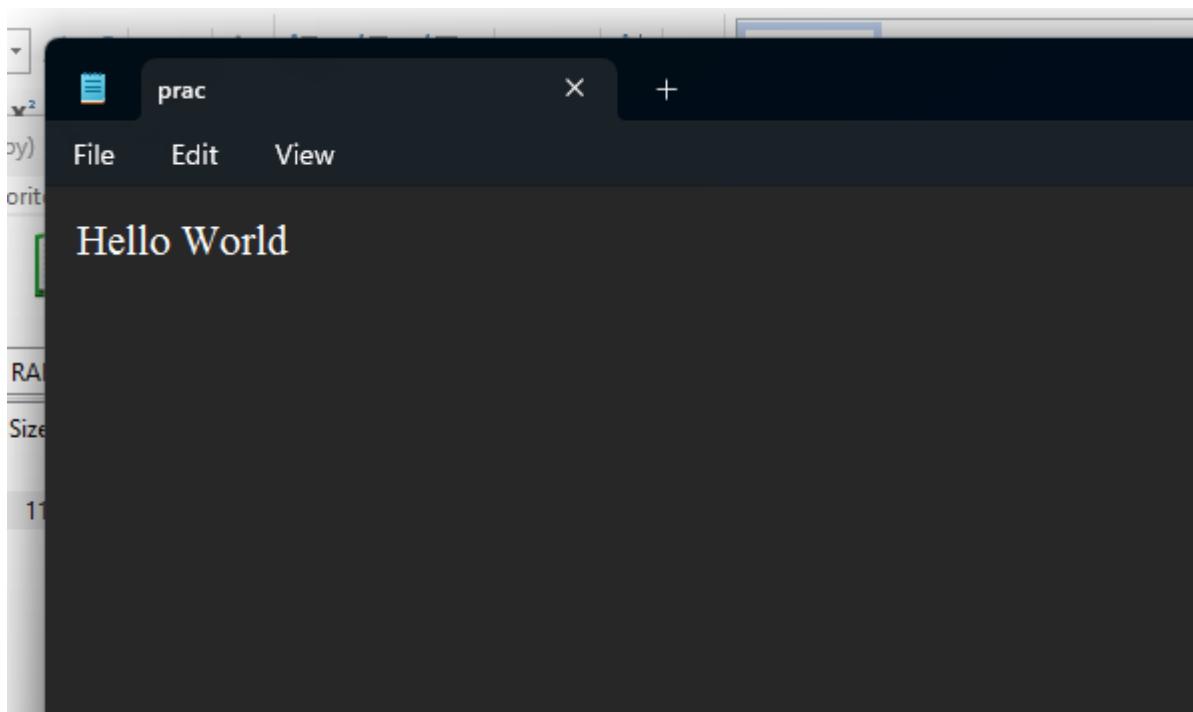


Then Desktop → Shortcut created of WinRAR and Select Just Once





View the Extracted File



## PRACTICAL NO. 8

### Aim:

Mobile Device Forensics

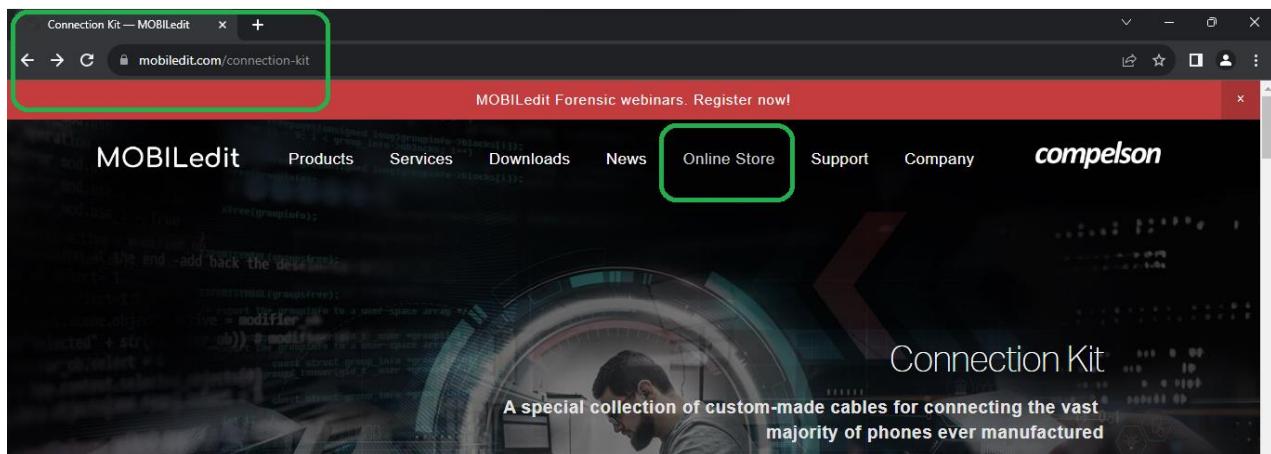
- Perform a forensic analysis of a mobile device, such as a smartphone or tablet.
- Retrieve call logs, text messages, and other relevant data for investigative purposes.

### Practical:

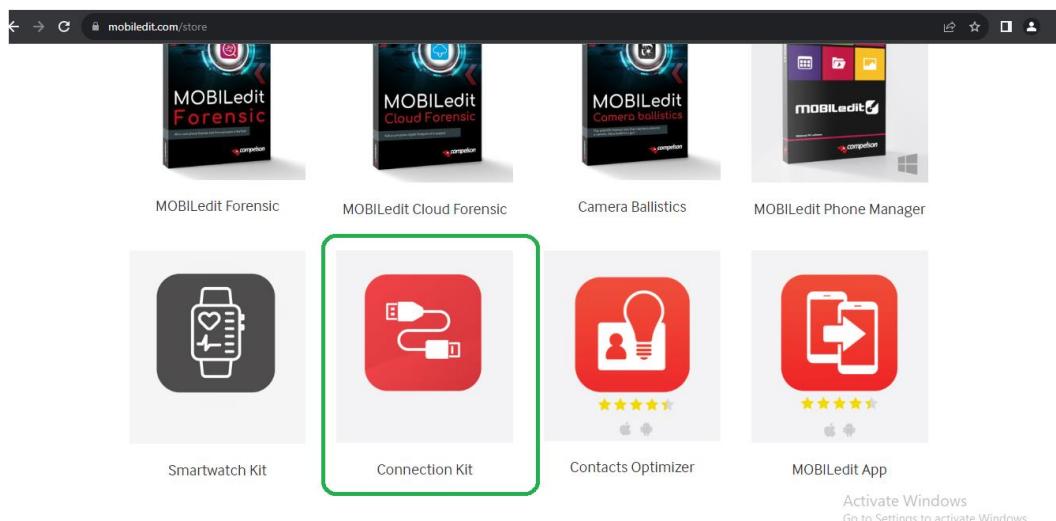
In this Practical we are going to perform the mobile forensic using the MOBILedit Forensic toolkit

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**

A screenshot of a web browser showing the MOBILedit Connection Kit product page. The page has a red header bar with the text "MOBILedit Forensic webinars. Register now!". Below the header is a dark navigation bar with links for Products, Services, Downloads, News, Online Store, Support, and Company. The main content area features a large image of a red USB cable with two white connectors. To the right of the image is the product name "Connection Kit" and a brief description: "A very special collection of high quality custom-made USB cables that covers a vast majority of phones. Also included is a comprehensive compilation of all necessary drivers. The entire collection is universally compatible with other software solutions. If you are a forensic professional, this product is a must have." Below the description is a price of "\$1000". At the bottom of the page is a "CONTACT US TO BUY" button and a note about activating Windows.

Then we go to the software

A screenshot of a web browser showing the MOBILedit software store page. The page has a black header bar with the text "Activate Windows" and a "Shopping Cart" icon. Below the header is a search bar with the placeholder "Search". The main content area is titled "Choose a product:" and shows four software packages: "MOBILedit Forensic" (highlighted with a green border), "MOBILedit Cloud Forensic", "Camera Ballistics", and "MOBILedit Phone Manager". At the bottom of the page is a note about activating Windows.

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

**MOBILedit Forensic**

**MOBILedit Forensic** is an all-in-one solution for data extraction from phones, smartwatches and clouds. It utilizes both physical and logical data acquisition, has excellent application analysis, deleted data recovery, a wide range of supported devices, fine-tuned reports, concurrent processing, and easy-to-use interface. With a brand new approach, MOBILedit Forensic is much stronger in security bypassing than ever before.

MOBILedit Forensic offers maximum functionality at a fraction of the price of other tools. It can be used as the only tool in a lab or as an enhancement to other tools with its data compatibility. When integrated with Camera Ballistics it scientifically analyzes camera photo origins.

[Learn More](#)

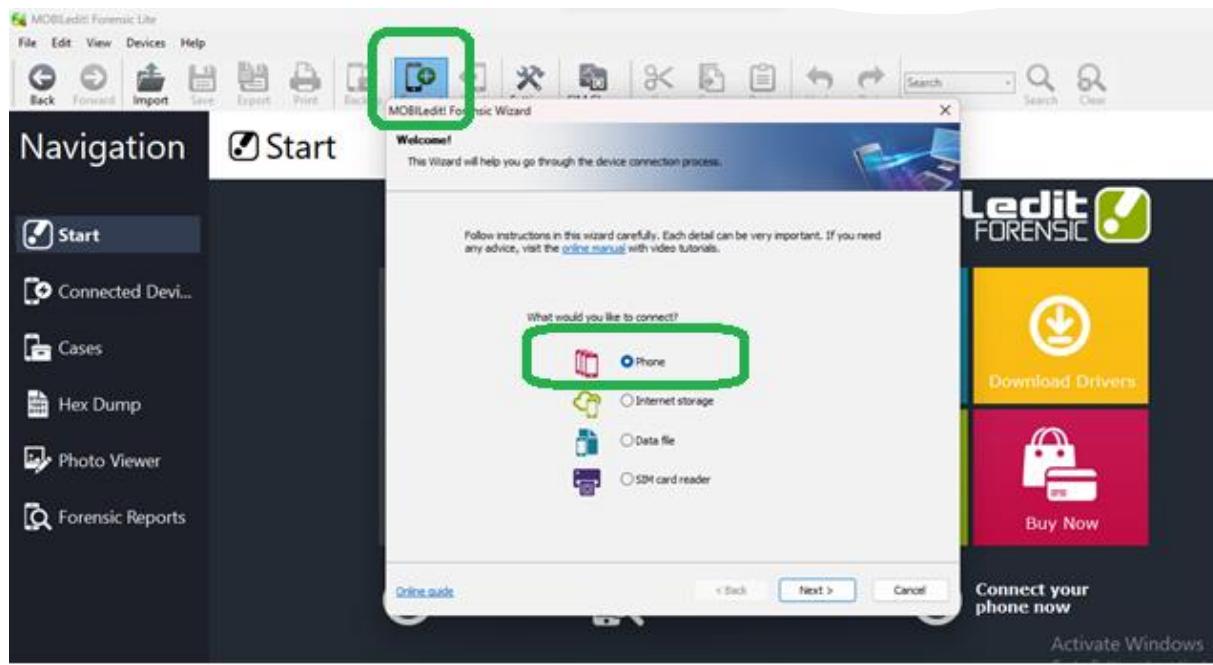
**Activate Windows**  
Go to Settings to activate Windows.

Forensic Single Phone	Forensic Standard	Forensic Pro / Pro+
\$99*	\$2,250*	Contact us
Pay per phone	Unlimited phones	All features of Standard plus:
6 month of updates	One-time license fee	Deleted data
1 computer	12 months of updates	Security bypassing
Phone forensic at logical level	1 computer	Physical analysis
App analysis	Phone forensic at logical level	App downgrade
	App analysis	Smartwatch forensics
	Unlimited imports	Malware and spyware detection
		Photo object recognition
		Face matcher
		UFED support
		Cloud forensic (optional)

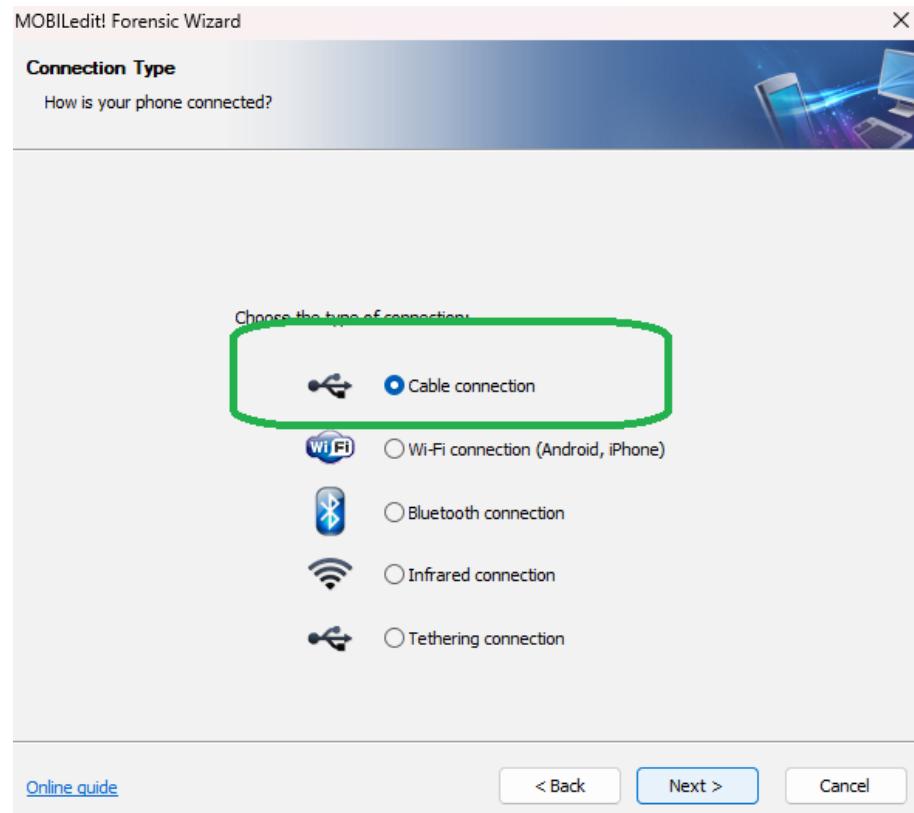
Now we are going to start the Practical

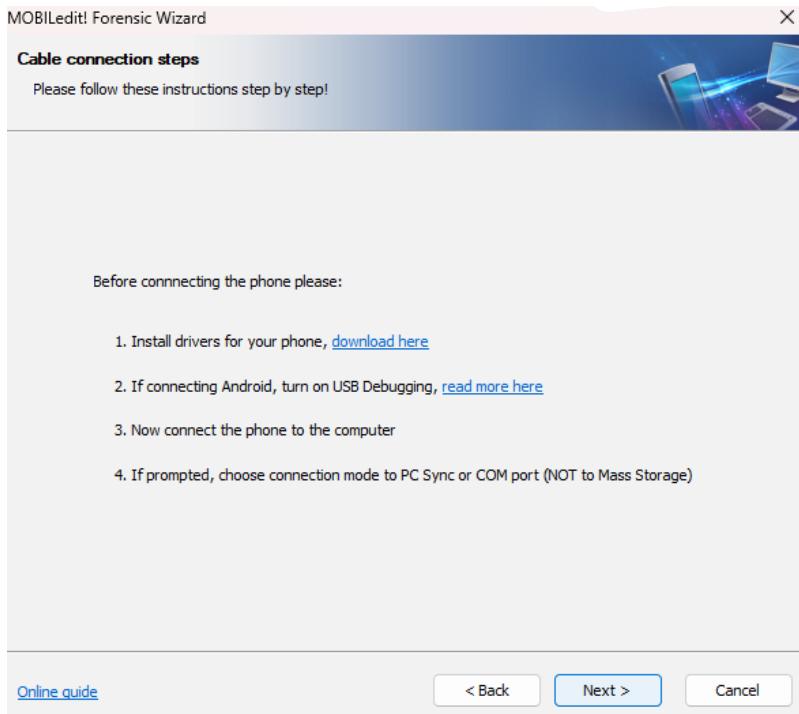


Click on connect and Select the type of forensic device to work with. Here we are going with Phone

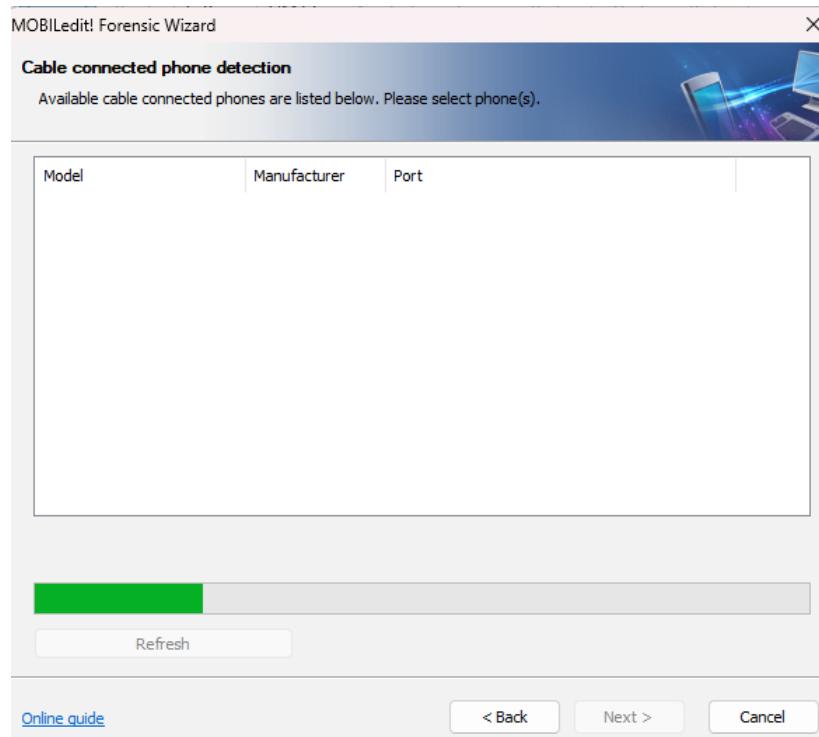


Click **Next** and **Select the type of Connection** with the **Mobile Phone**. Here we are going to Select **Cable Connection** and click **Next**

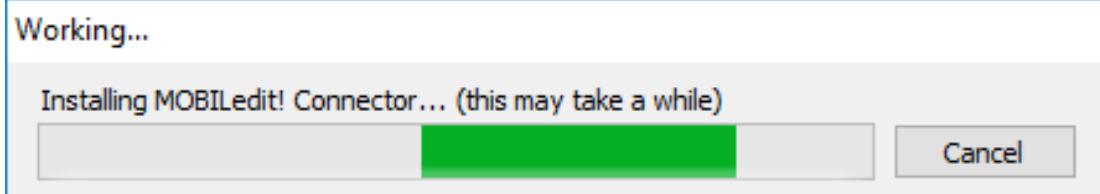
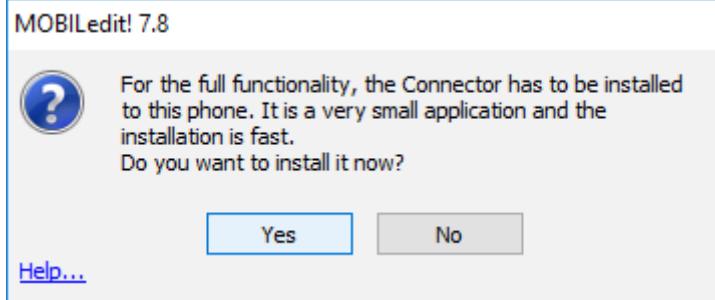




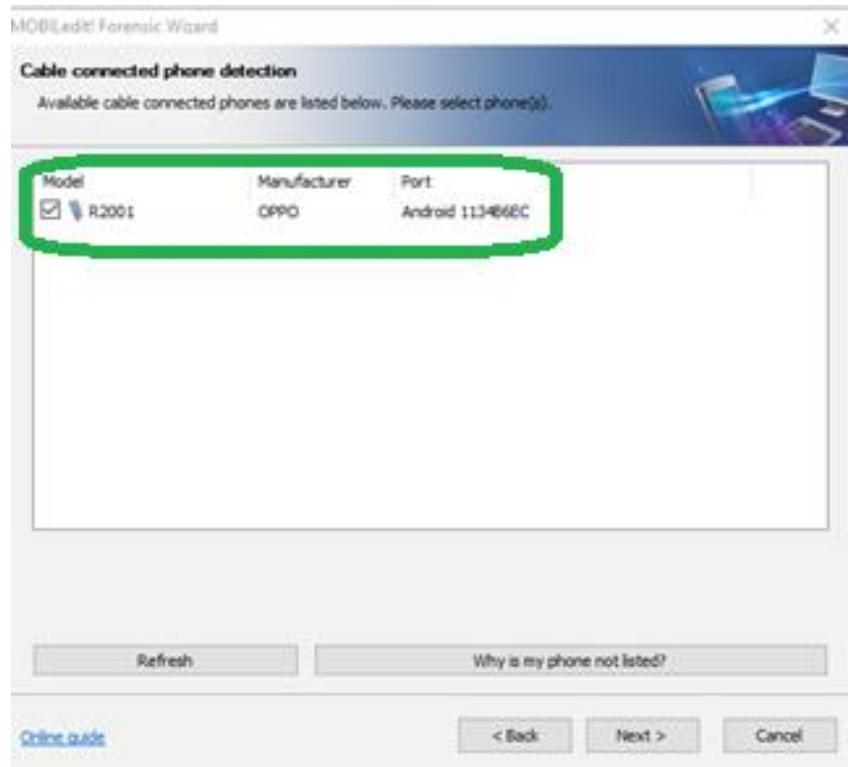
Click Next and let it Scan the Device, If **Found** click Next, If **Not Found** Perform these steps and Retry  
**"Go to Phone Settings and open Developer Option and Enable it, and then Allow USB Debugging"**



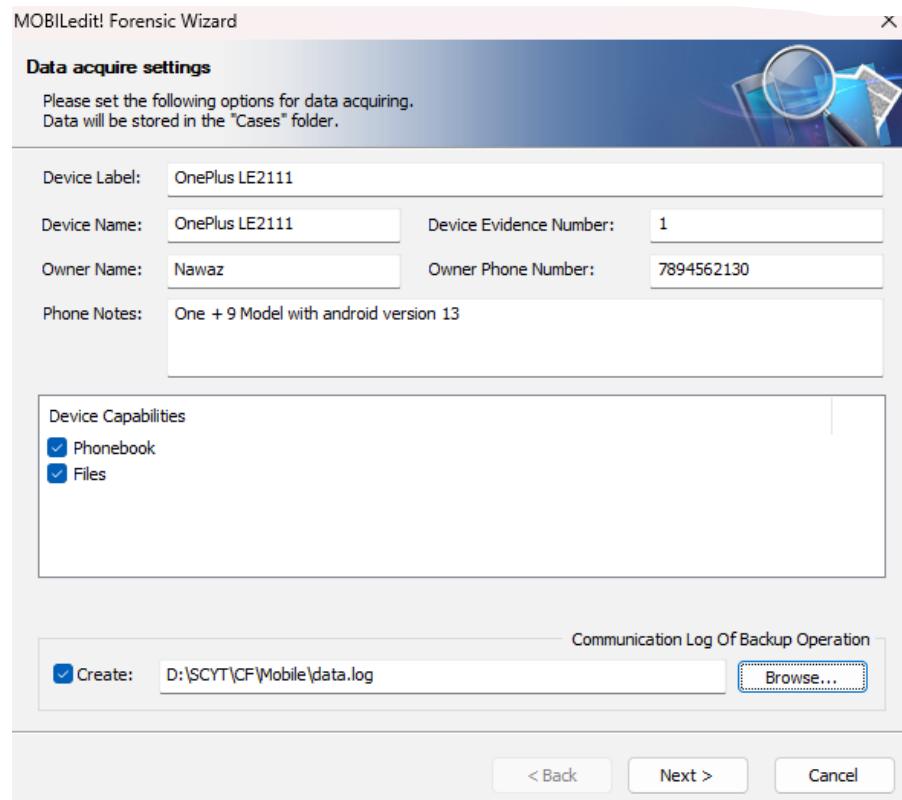
Then connect it with a connector for efficient data recovery



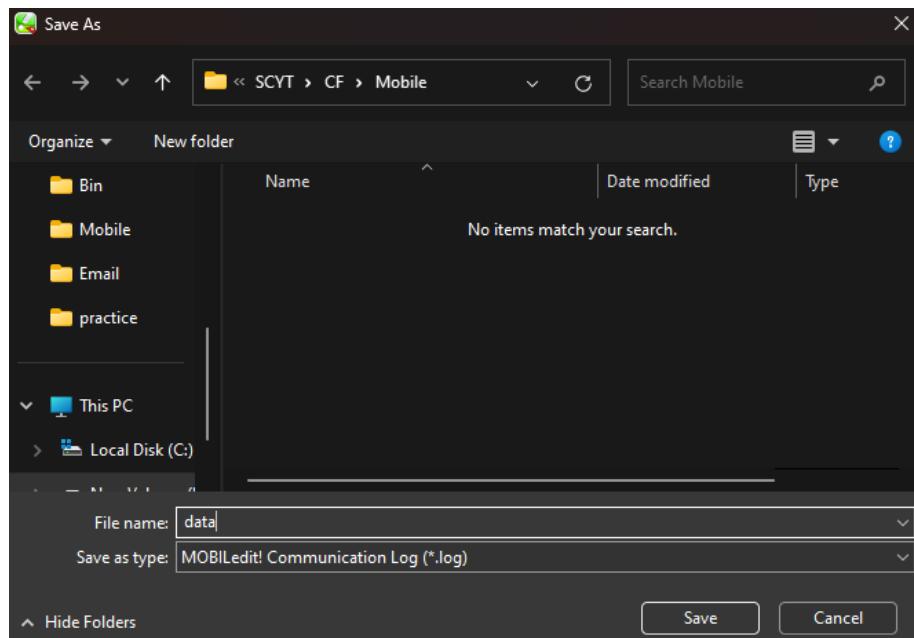
We got a device connected



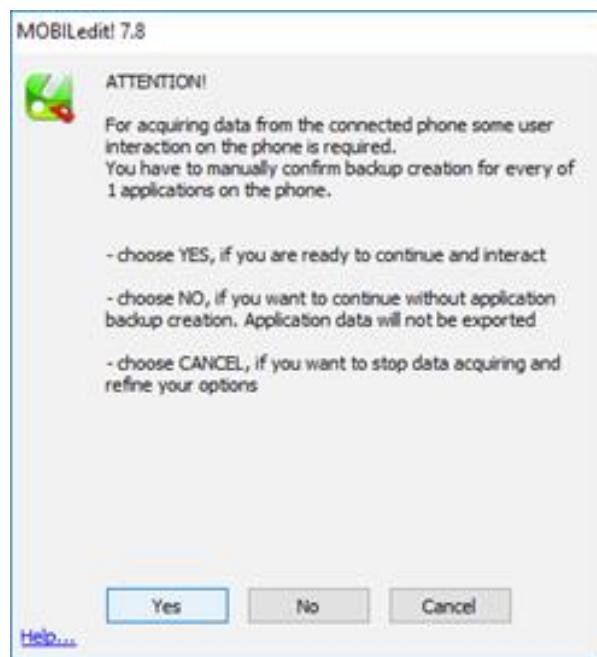
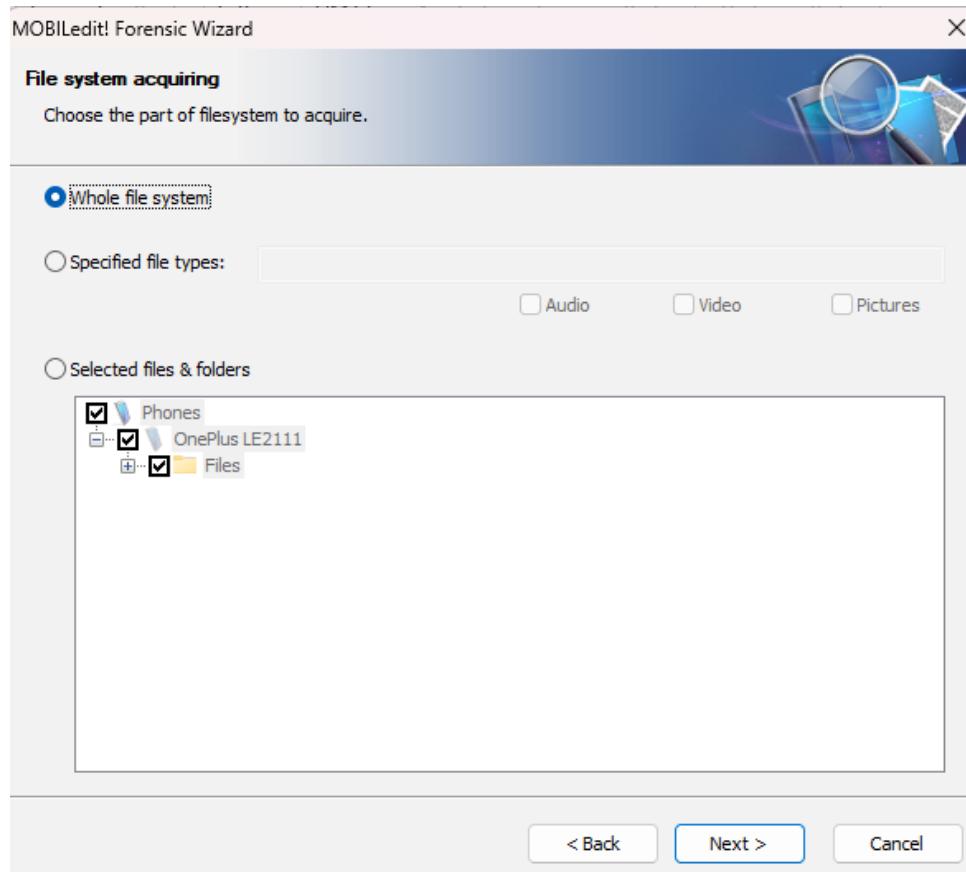
This is the device we are going to use and click on next



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

The image contains four screenshots of the MOBILedit! Forensic Wizard software interface, specifically the 'Data acquiring' step. Each screenshot shows a table of items and their acquisition status.

**Screenshot 1 (Left):**

Item	Status
Data acquisition started on	13-09-2023 10:37:31
Filesystem: Info	Initializing...

Scanning "Files\Internal shared storage\Pictures\thumbnails\" folder for selected files... Stop

**Screenshot 2 (Top Right):**

Item	Status
Data acquisition started on	13-09-2023 10:37:31
Filesystem: Info	The operation completed successfully.
Filesystem: Canva	The operation completed successfully.
Filesystem: thumbnails	The operation completed successfully.
Filesystem: Giphy	The operation completed successfully.
Filesystem: Picsart	The operation completed successfully.
Filesystem: AI Photo Enhancer	The operation completed successfully.
Filesystem: Instagram	The operation completed successfully.
Filesystem: Screenshots	The operation completed successfully.
Filesystem: SquareBlend	The operation completed successfully.
Filesystem: Truecaller Images	The operation completed successfully.
Filesystem: Pictures	The operation completed successfully.
Filesystem: .Ota	Item 1 out of 1

Reading file "OnePlus9Oxygen_22.1.47 OTA_1470_all_2203102115_9570fb5.zip" from "OnePlus LE2111"... (46 Stop

**Screenshot 3 (Bottom Left):**

Item	Status
Filesystem: SquareBlend	The operation completed successfully.
Filesystem: Truecaller Images	The operation completed successfully.
Filesystem: Pictures	The operation completed successfully.
Filesystem: .Ota	The operation completed successfully.
Filesystem: Scoompa Video	The operation completed successfully.
Filesystem: Reverse	The operation completed successfully.
Filesystem: thumbnails	The operation completed successfully.
Filesystem: Whatsapp	The operation completed successfully.
Filesystem: Canva	The operation completed successfully.
Filesystem: Creative content writing	The operation completed successfully.
Filesystem: BrandSpot365	The operation completed successfully.
Filesystem: com_account_usercenter	The operation completed successfully.
Filesystem: com_account_usercenter...	The operation completed successfully.
Filesystem: playlist	The operation completed successfully.
Filesystem: playlist1	The operation completed successfully.
Filesystem: Download	Item 1 out of 15

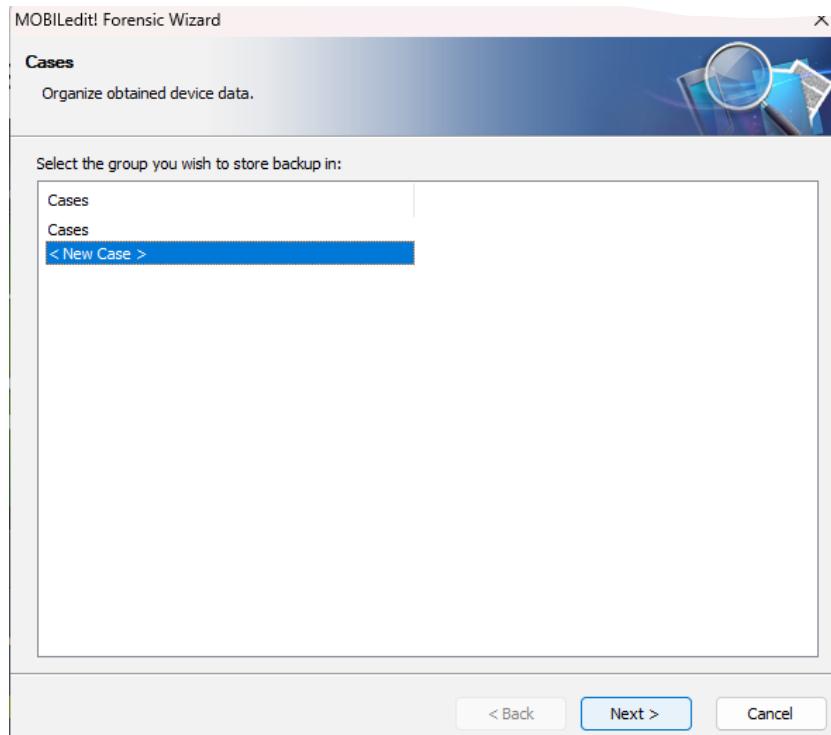
Reading file "Raaghul.2023.1080p.WEB.HDRip.Hindi.HQ.Dub.DD.2.0.x264.mkv" from "OnePlus LE2111"... (28 Stop

**Screenshot 4 (Bottom Right):**

Item	Status
Filesystem: SquareBlend	The operation completed successfully.
Filesystem: Truecaller Images	The operation completed successfully.
Filesystem: Pictures	The operation completed successfully.
Filesystem: .Ota	The operation completed successfully.
Filesystem: Scoompa Video	The operation completed successfully.
Filesystem: Reverse	The operation completed successfully.
Filesystem: thumbnails	The operation completed successfully.
Filesystem: Whatsapp	The operation completed successfully.
Filesystem: Canva	The operation completed successfully.
Filesystem: Creative content writing	The operation completed successfully.
Filesystem: BrandSpot365	The operation completed successfully.
Filesystem: com_account_usercenter	The operation completed successfully.
Filesystem: com_account_usercenter...	The operation completed successfully.
Filesystem: playlist	The operation completed successfully.
Filesystem: playlist1	The operation completed successfully.
Filesystem: Download	Item 1 out of 15

Reading file "Raaghul.2023.1080p.WEB.HDRip.Hindi.HQ.Dub.DD.2.0.x264.mkv" from "OnePlus LE2111"... (1 sec(s) Stop

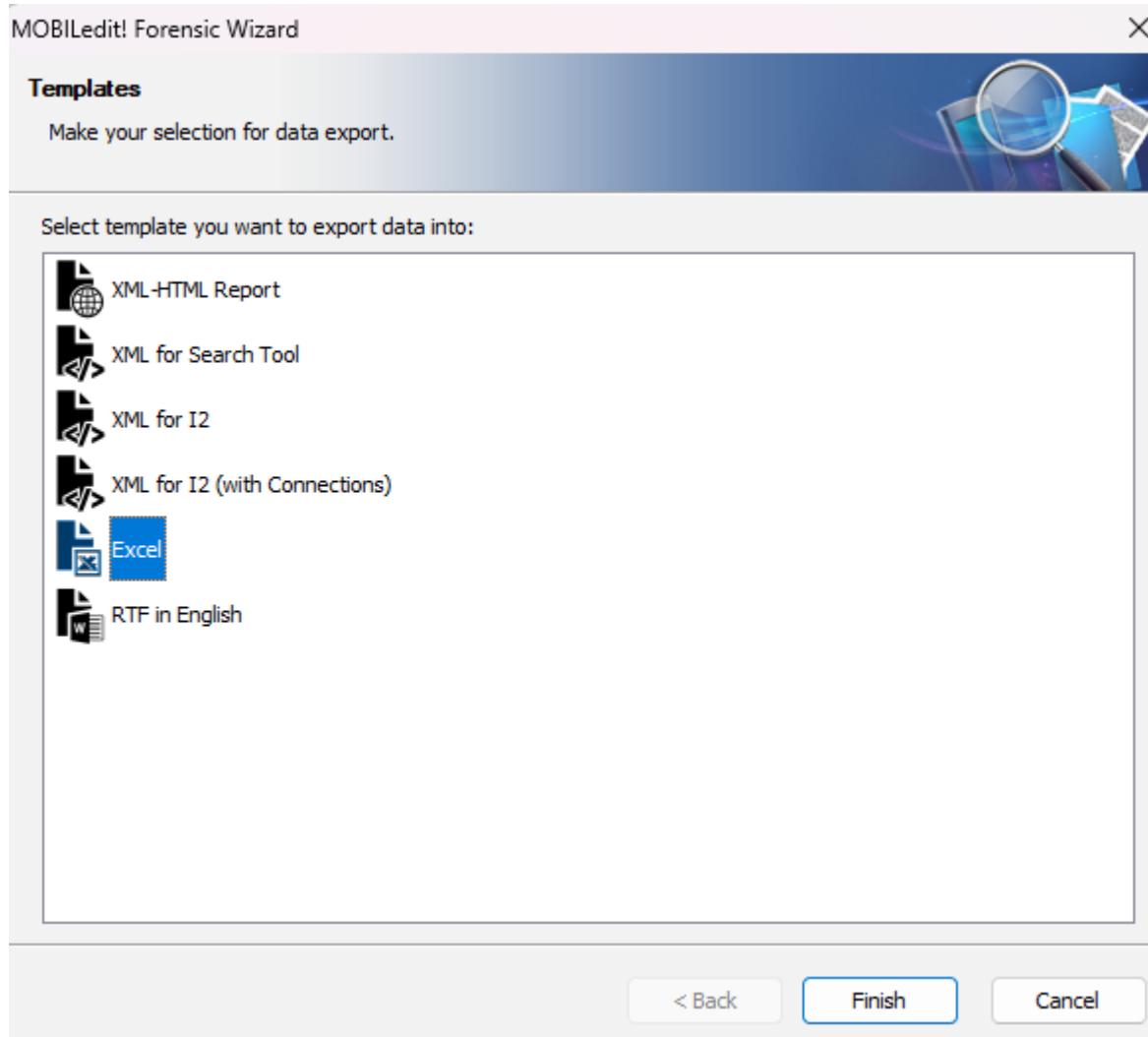
Open the **Case** and **Organize** and decide the **Format** in which we need the **Acquisition**



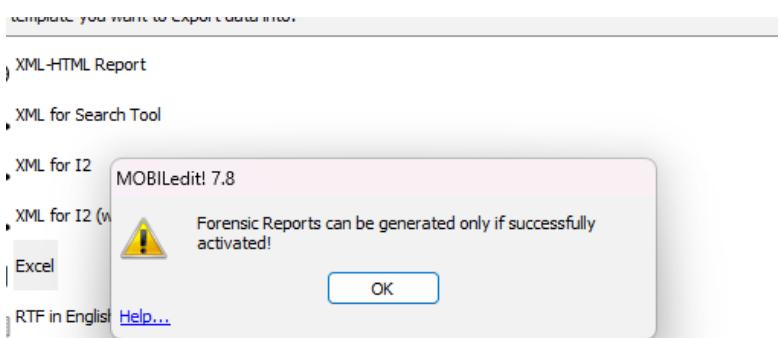
Fill in the details of the Investigator

The screenshot shows the 'New case' step of the MOBILedit! Forensic Wizard. The title bar says 'MOBILedit! Forensic Wizard' and the window title is 'New case'. The sub-instruction 'Create a new case for obtained data.' is displayed. The interface is divided into sections: 'Case Details' (Label: One+9, Number: 130923), 'Notes' (Performed with 128GB Storage device), and 'Investigator Details' (Name: Suraj, E-mail: kaduvettisuraj@gmail.com, Phone Number: 7895461320). At the bottom are buttons for '< Back', 'Next >', and 'Cancel'.

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



A Success Message will be Prompted



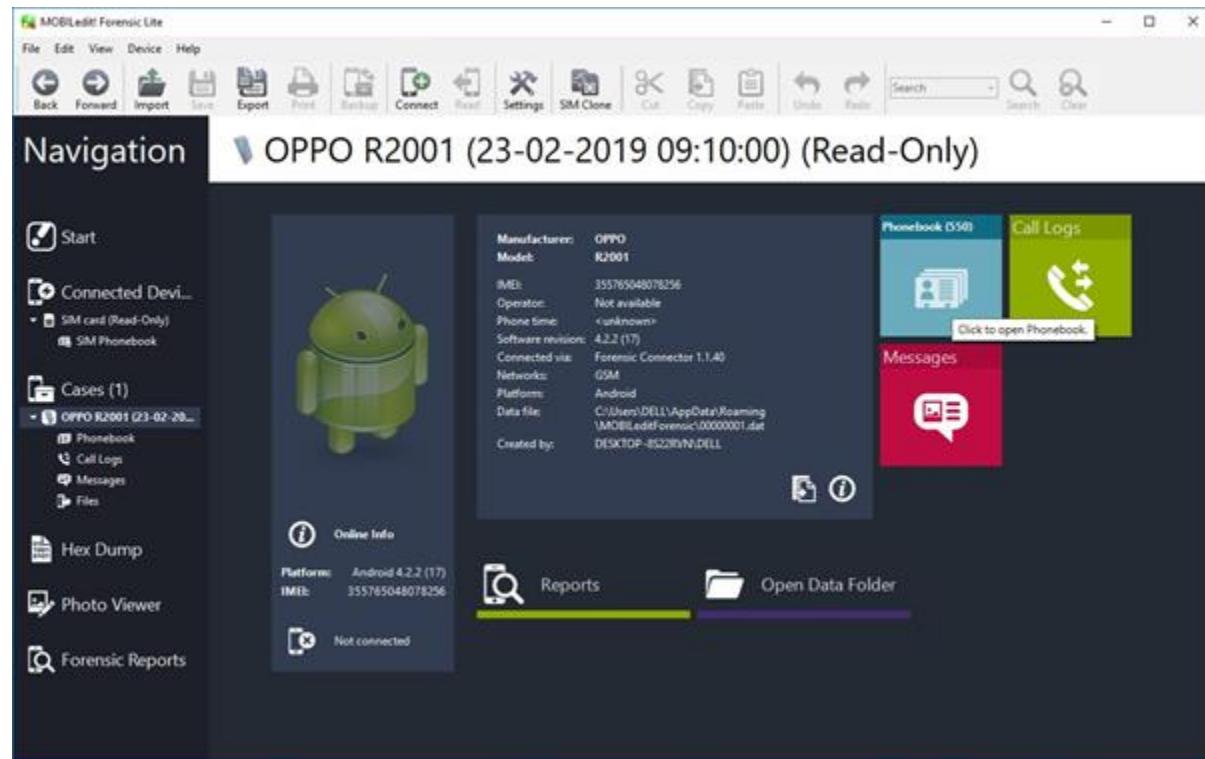
Now we are going to **view** and **analyze** the **data acquired** form the **Performed Acquisition**

We have performed of Two Mobile Devices

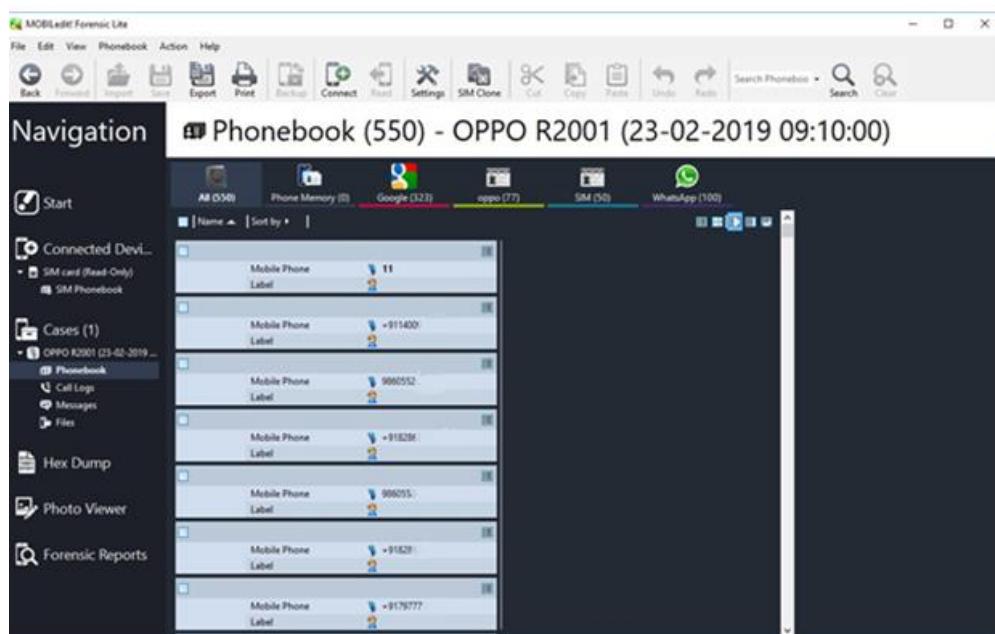
The First One is the Oppo Reno 2

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

**Call Logs (97) - OPPO R2001 (23-02-2019 09:10:00)**

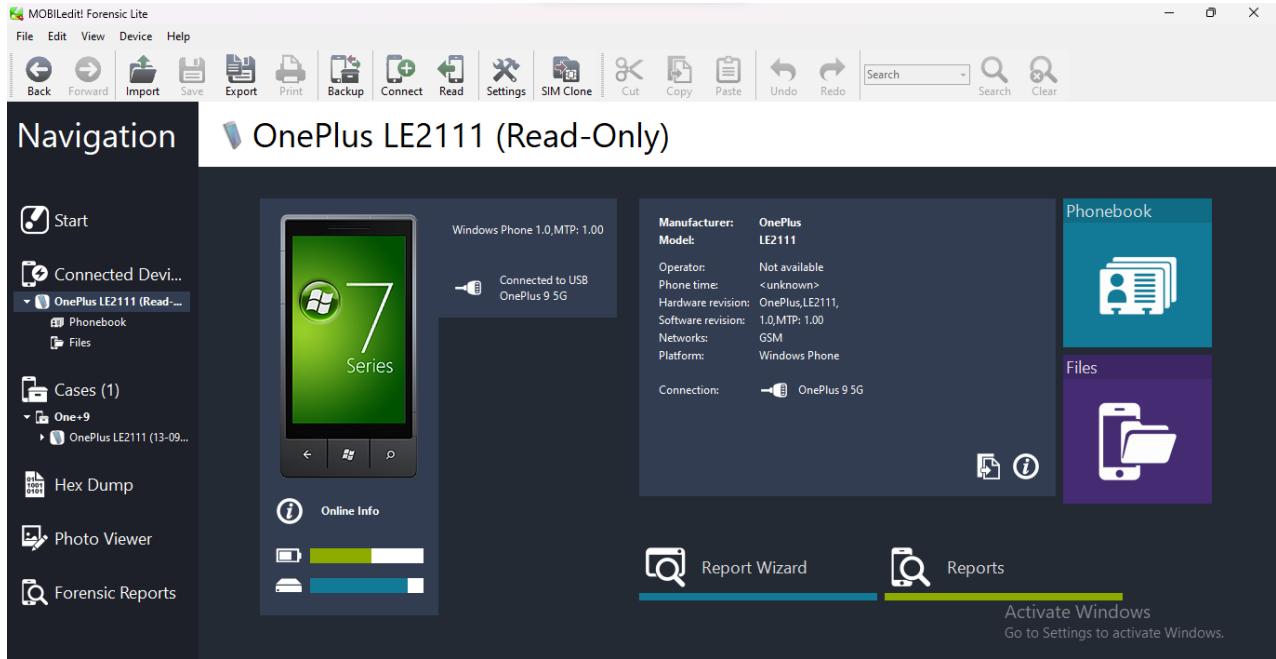
Name	Number	Date
[REDACTED]	+91146	22-02-2019 20:10:12
[REDACTED]	+911400	22-02-2019 16:23:14
[REDACTED]	+9114...	22-02-2019 14:37:00
[REDACTED]	+91141	21-02-2019 15:44:20
Sair	+9199...	20-02-2019 11:38:44
Sai	+919...	20-02-2019 11:29:22
Sak.	+91993...	20-02-2019 10:16:51
[REDACTED]	+9114C	19-02-2019 16:30:13
[REDACTED]	+9122...	19-02-2019 10:04:24
[REDACTED]	+917971...	18-02-2019 21:26:18
[REDACTED]	+917974...	18-02-2019 21:19:07
Papi	+91905...	18-02-2019 20:25:20
Sant	+919321...	18-02-2019 20:17:29
[REDACTED]	+9114005...	18-02-2019 19:43:53
Aa	+918790...	17-02-2019 21:44:42
Aan	+91879...	17-02-2019 21:29:40

And here we can see the messages on the device

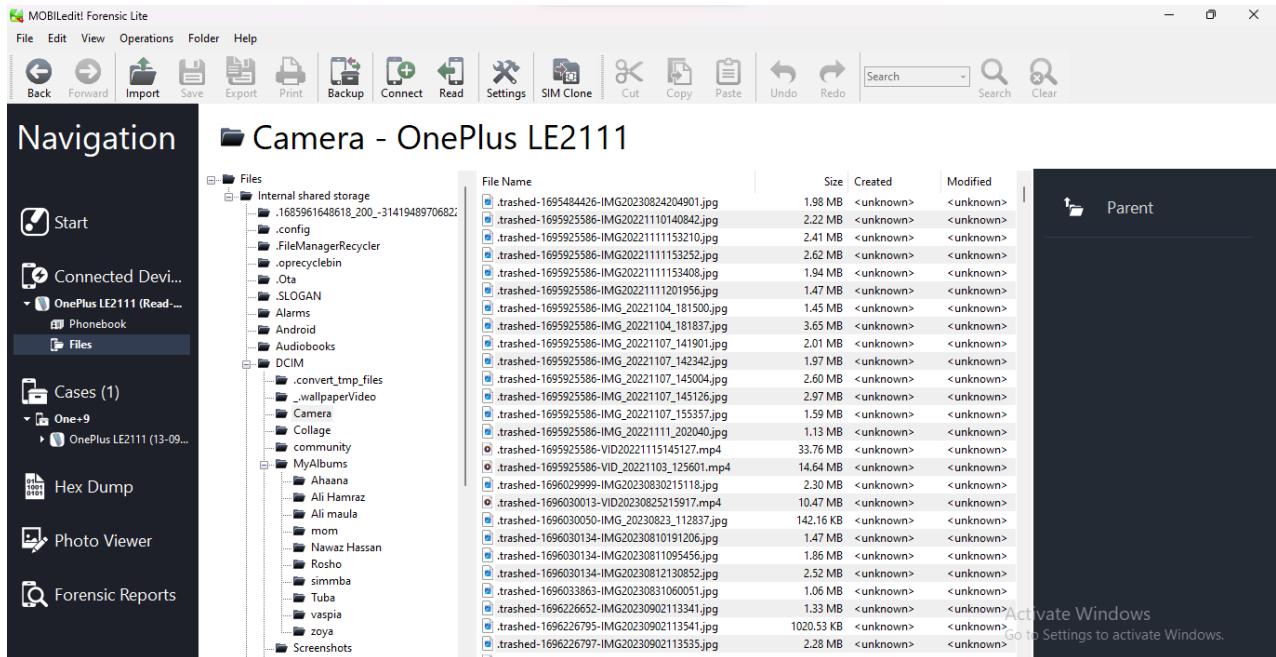
**Messages - OPPO R2001 (23-02-2019 09:10:00)**

Conversation	Date	Message Content
IDEA	22-02-2019 20:59:25	Dear User! Start playing game to Win GOLD voucher worth Rs 25000. CALL 95256 Tollfree, TNC
Aaa[REDACTED]	22-02-2019 17:19:31	Abc@9999999999 25 02 2019 17:19:31 25.02.2019 17:19:31 9999999999
IM-65[REDACTED]	22-02-2019 14:46:43	22-02-2019 09:27:34
IM-612[REDACTED]	22-02-2019 14:15:48	Chancell Win Rs 65 & Rs 25 worth FREE Recharge Everyday. Dial *777# (DishFree) TNC
IM-65[REDACTED]	22-02-2019 10:34:12	21-02-2019 14:09:26
+919981[REDACTED]	21-02-2019 16:52:49	Rs 3000 Worth Recharge Rs 15000 Worth Rs 15000 Worth Rs 30000 Worth Rs 30000
MD-K[REDACTED]	21-02-2019 16:44:12	21-02-2019 09:19:34
AX-IY[REDACTED]	21-02-2019 12:05:36	Limited Offer! Call 95256 Tollfree and Win Rs 65 worth Recharge Everyday. TNC
IM-65[REDACTED]		26-01-2019 09:09:37

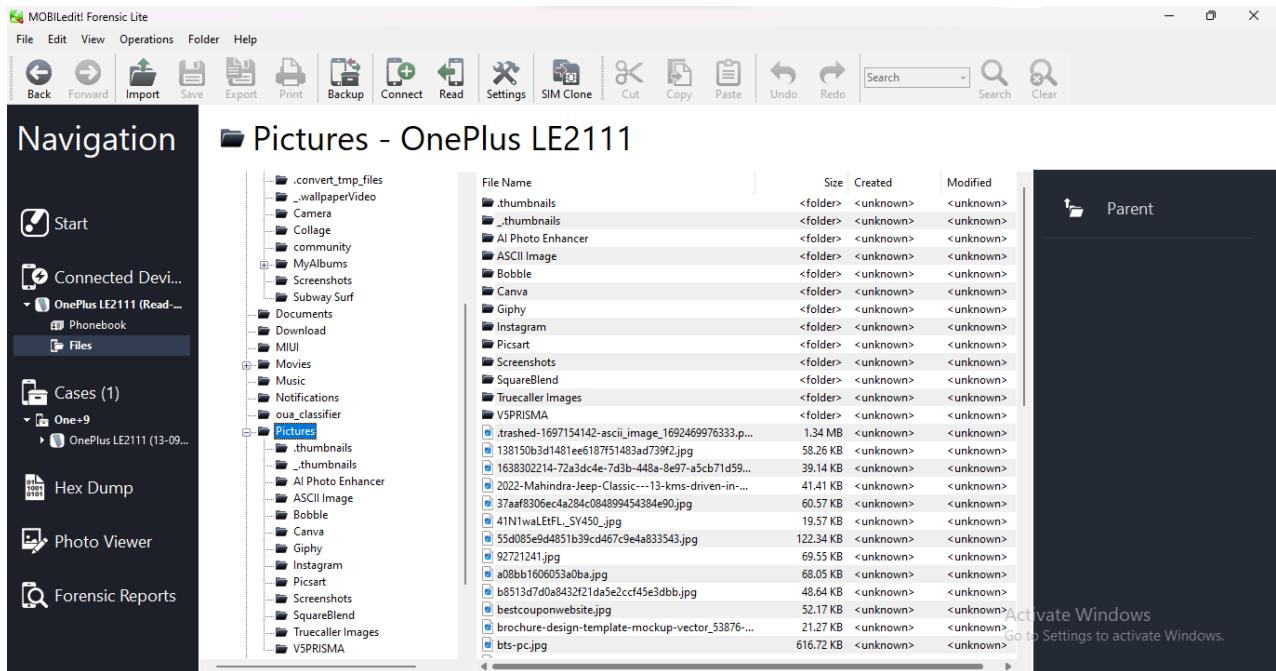
## Display of the Second Device One⁺ 9



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**

```
data
File Edit View
3085.2070 [4:drvman:10532] <: WPD Device - GetStatus
3085.2125 [2:api:10532] GetParameter(GLOBAL:0xffff, 0xffff03f8, &x0FF0FC08,
&x0FF1FC08) returned 0x490
3085.2195 [2:api:10532] GetParameter(GLOBAL:0xffff, 0xffff0402, &x0FF0FC08,
&x0FF1FC08) returned 0x2afd
3085.2219 [2:api:10532] GetParameter(GLOBAL:0xffff, 0xffff041b, &x0FF0FC08,
&x0FF1FC08) returned 0x2afd
```

Ln 1, Col 1 | 100% | Windows (CRLF) | UTF-8

## 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.

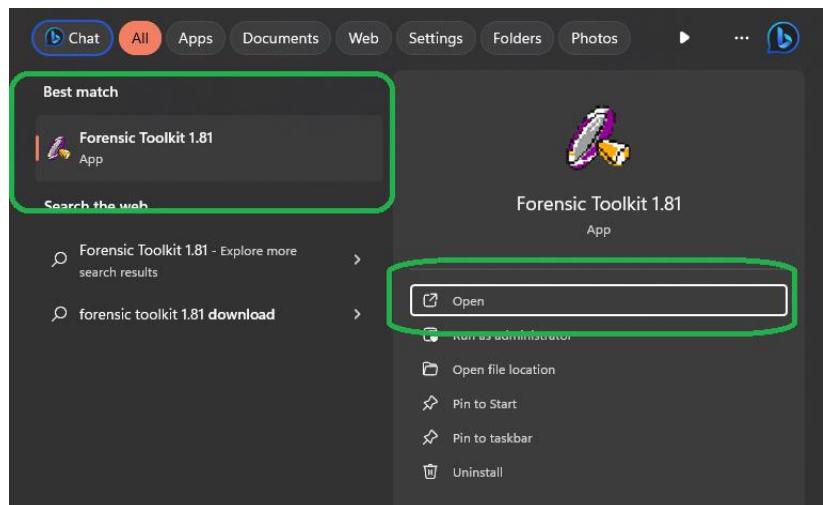
Martha asked her CIO, to have an IT employee copy the Outlook .pst file from Jim Shu's old computer to a USB drive.

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.

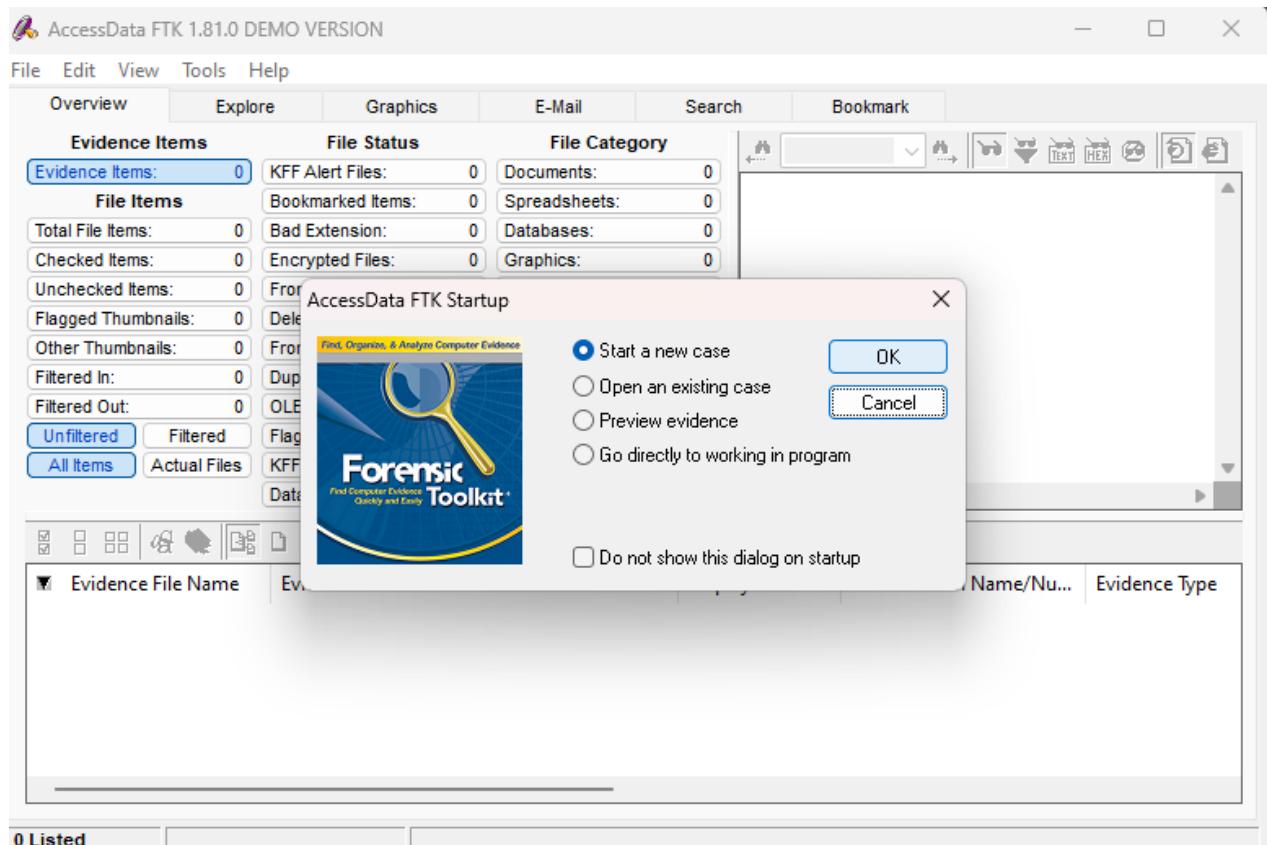
Recovering Email

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**



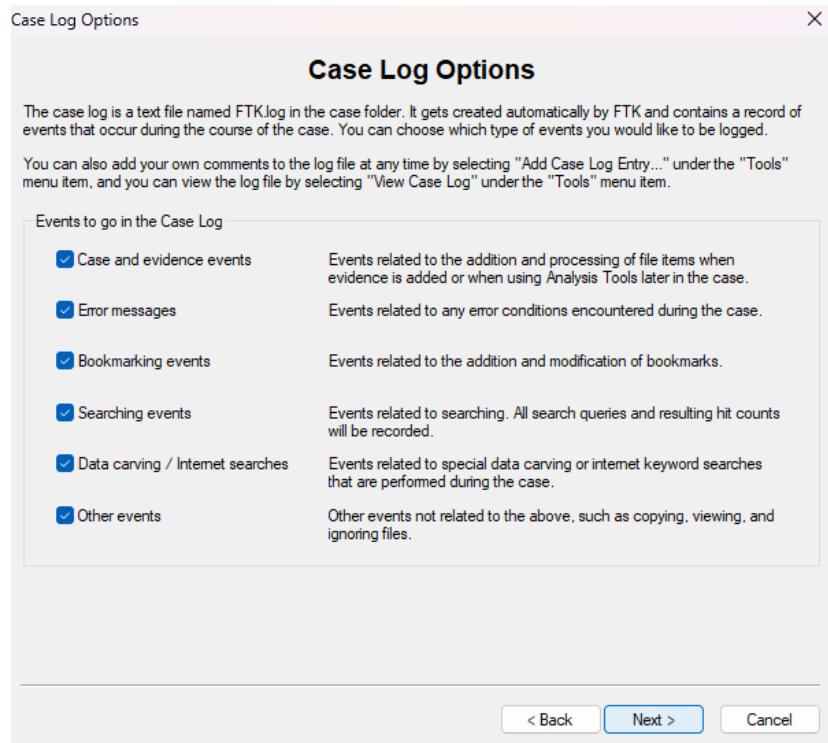
## Create a new File



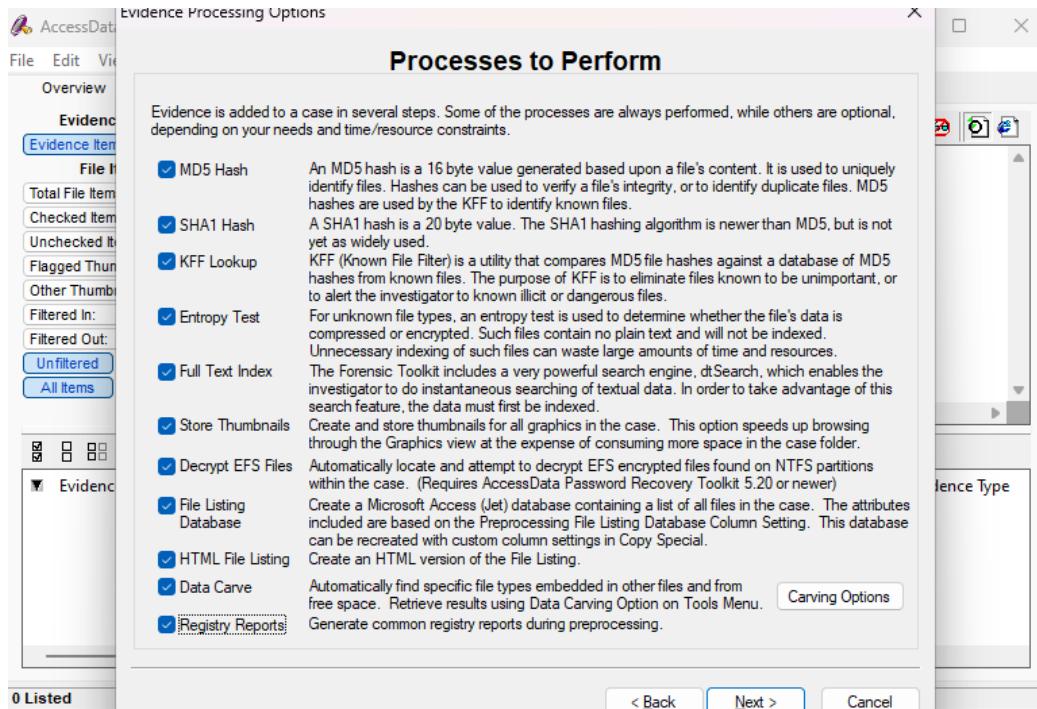
Fill the details of the Examiner

The screenshot shows the "FTK Report Wizard - Case Information" dialog. The title bar says "FTK Report Wizard - Case Information" and the main section is titled "Forensic Examiner Information". It says "The following information will appear on the Case Information page of the report:". There are several input fields: "Agency/Company: rizvi", "Examiner's Name: Aamir" (in a dropdown menu), "Address: Carter Road, Bandra, Mumbai", "Phone: 9876452310", "Fax: [empty]", "E-Mail: aamir10@gmail.com" (with the cursor in it), and "Comments: email analysis". At the bottom, there are buttons for "< Back", "Next >" (highlighted in blue), and "Cancel".

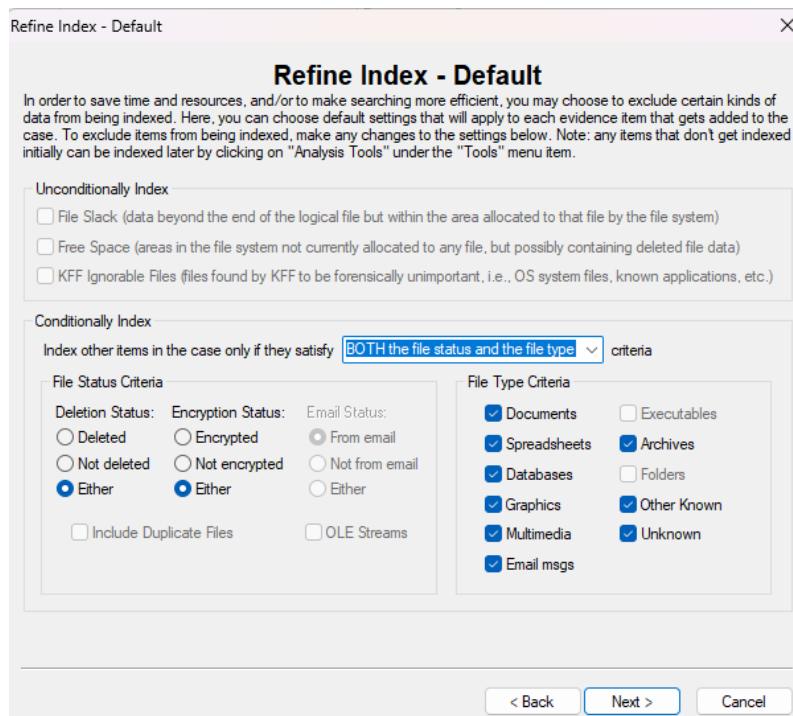
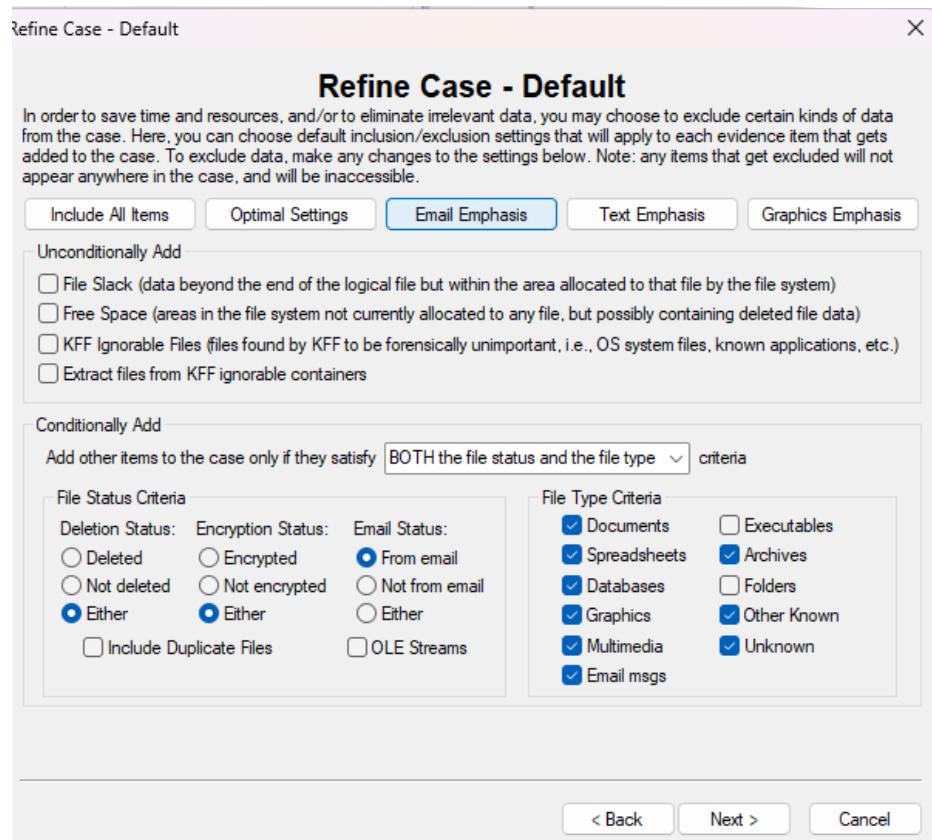
Click on all the options and Click Next



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**.

Add Evidence to Case

## Add Evidence

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

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

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

Add Evidence... Edit Evidence... Remove Evidence Refine Evidence - Advanced...

Display Name	Source	Name/Nu...	Type	Refined	Time Zone	Comment

< Back Next > Cancel

options, set previously, can be overridden independently for each evidence item, a n also be made. These refinements can include the exclusion of date/size ranges, further refinements, highlight an evidence item in the list and press Refine Evidence

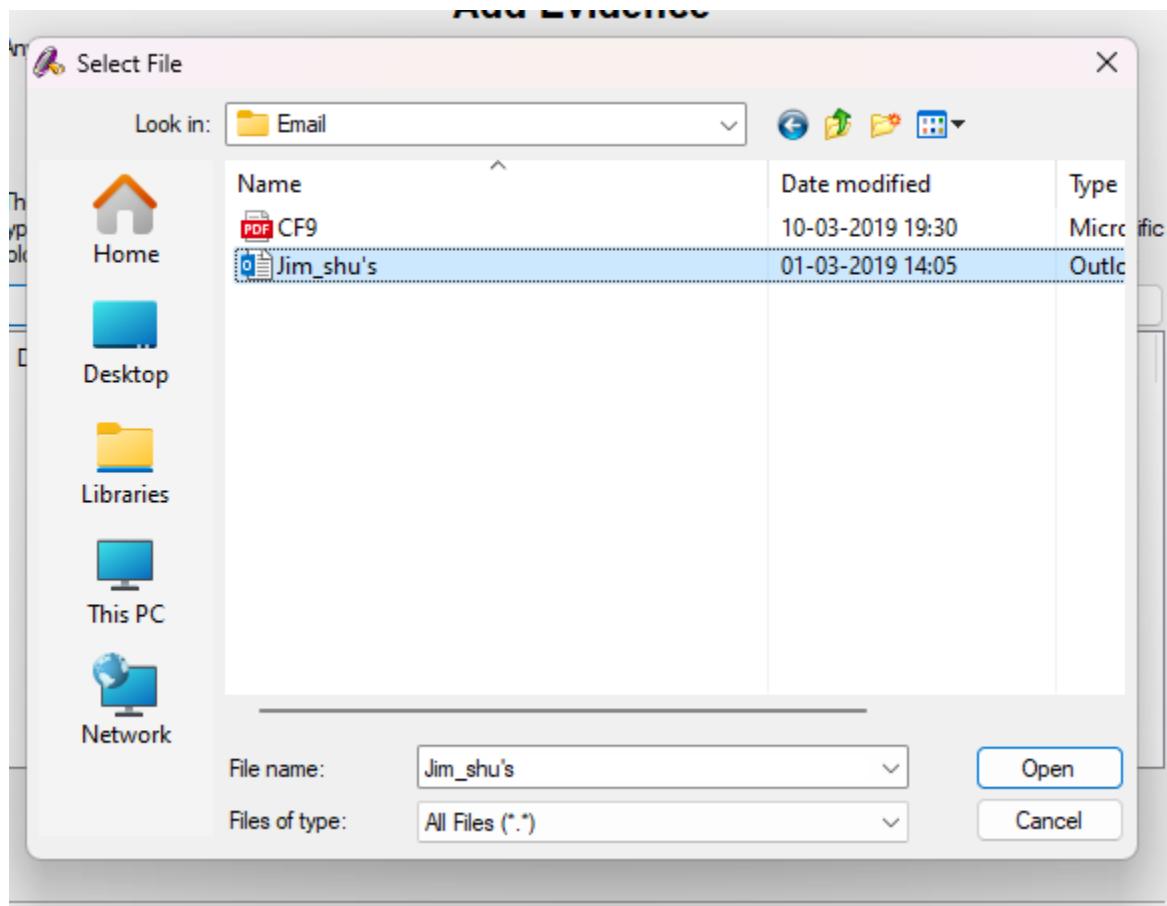
Add Evidence to Case

Type of Evidence to Add to Case

Acquired Image of Drive  
 Local Drive  
 Contents of a Folder  
 Individual File

Continue... Cancel

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

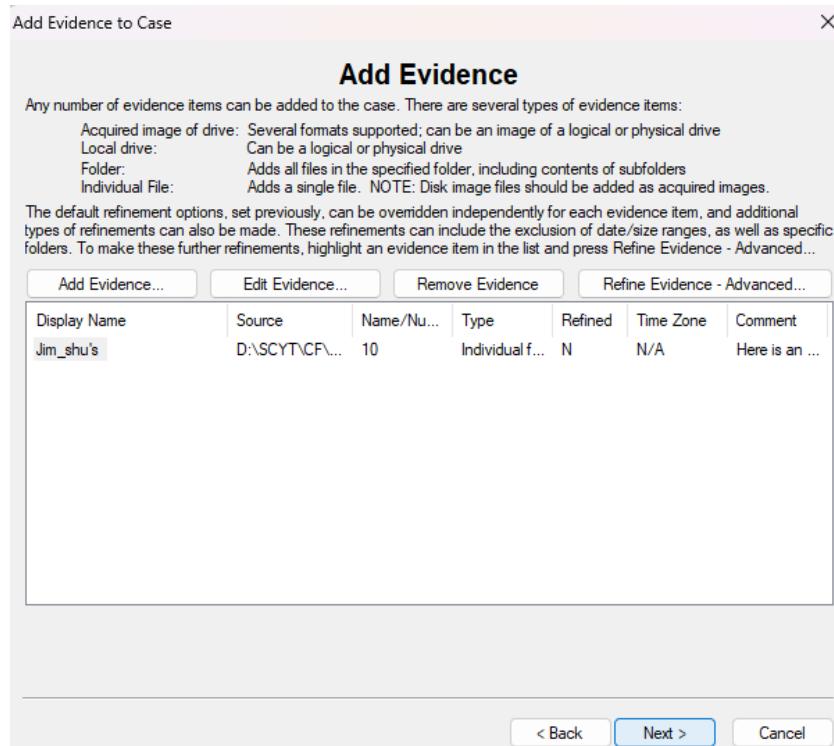


Give some data

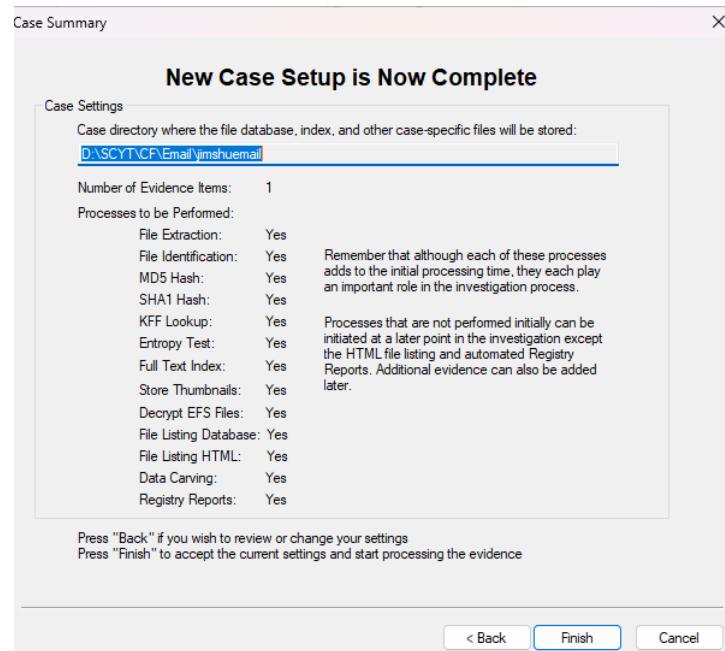
The screenshot shows the 'Evidence Information' dialog box. It contains fields for Evidence Location (D:\ASCYT\NCF\Email\Jim_shu's.pst), Evidence Display Name (Jim_shu's), Evidence Identification Name/Number (10), and a Comment section containing the text 'Here is an example for the email'. At the bottom, there is a Local Evidence Time Zone dropdown set to 'Choose time zone for evidence ...' and 'OK' and 'Cancel' buttons.

Evidence Location:	D:\ASCYT\NCF\Email\Jim_shu's.pst
Evidence Display Name:	Jim_shu's
Evidence Identification Name/Number:	10
Comment:	Here is an example for the email
Local Evidence Time Zone:	Choose time zone for evidence ...

Complete the steps and Click on Next



Click on finish and see the data



AccessData FTK 1.81.0 DEMO VERSION -- D:\SCYT\CF>Email\jimshuemail\

File Edit View Tools Help

Overview Explore Graphics E-Mail Search Bookmark

**Evidence Items**

Evidence Items:	1
File Items	
Total File Items:	40
Checked Items:	0
Unchecked Items:	40
Flagged Thumbnails:	0
Other Thumbnails:	1
Filtered In:	40
Filtered Out:	0
Unfiltered	Filtered
All Items	Actual Files

**File Status**

KFF Alert Files:	0
Bookmarked Items:	0
Bad Extension:	1
Encrypted Files:	0
From E-mail:	40
Deleted Files:	6
From Recycle Bin:	0
Duplicate Items:	2
OLE Subitems:	0
Flagged Ignore:	0
KFF Ignorable:	0
Data Carved Files:	0

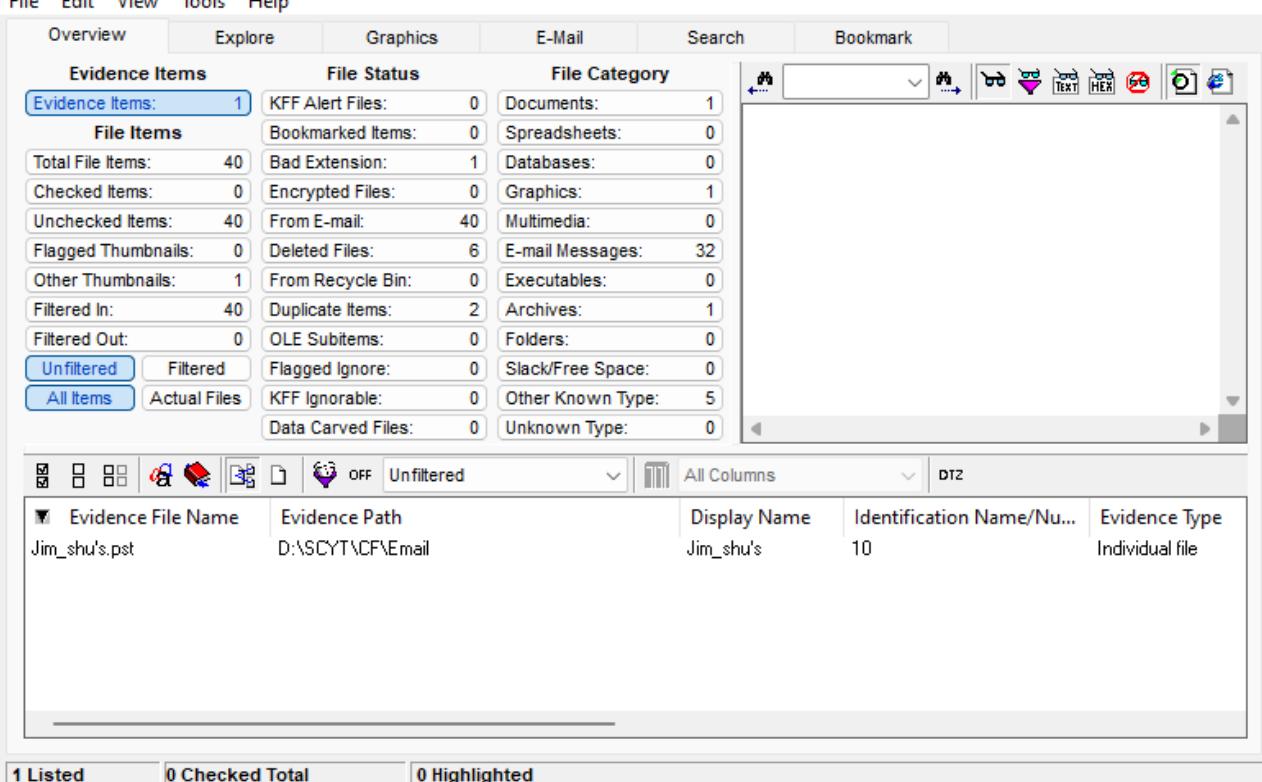
**File Category**

Documents:	1
Spreadsheets:	0
Databases:	0
Graphics:	1
Multimedia:	0
E-mail Messages:	32
Executables:	0
Archives:	1
Folders:	0
Slack/Free Space:	0
Other Known Type:	5
Unknown Type:	0

File View Options: OFF Unfiltered All Columns DTZ

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

1 Listed 0 Checked Total 0 Highlighted



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.

AccessData FTK 1.81.0 DEMO VERSION -- D:\SCYT\CF\Email\jimshuemail\

File Edit View Tools Help

Overview Explore Graphics E-Mail Search Bookmark

Evidence Items:	1	KFF Alert Files:	0	Documents:	1
Bookmarked Items:	0	Spreadsheets:	0		
Total File Items:	40	Bad Extension:	1	Databases:	0
Checked Items:	0	Encrypted Files:	0	Graphics:	1
Unchecked Items:	40	From E-mail:	40	ImageFiles:	0
Flagged Thumbnails:	0	Deleted Files:		E-mail Messages:	32
Other Thumbnails:	1	From Recycle Bin:		Executables:	0
Filtered In:	40	Duplicate Items:	2	Archives:	1
Filtered Out:	0	OLE Subitems:	0	Folders:	0
Unfiltered	Filtered	Flagged Ignore:	0	Slack/Free Space:	0
All Items	Actual Files	KFF Ignorable:	0	Other Known Type:	5
		Data Carved Files:	0	Unknown Type:	0

File Name Full Path Recycle Bi... Ext File Type Category

Message0001	D:\SCYT\CF\Email\Jim_shu's.pst>>Personal Fol...			E-mail Messa...	E-mail
Message0001	D:\SCYT\CF\Email\Jim_shu's.pst>>Personal Fol...			E-mail Messa...	E-mail
Message0001	D:\SCYT\CF\Email\Jim_shu's.pst>>Personal Fol...			E-mail Messa...	E-mail
Message0001	D:\SCYT\CF\Email\Jim_shu's.pst>>Message0001			E-mail Messa...	E-mail
Message0002	D:\SCYT\CF\Email\Jim_shu's.pst>>Personal Fol...			E-mail Messa...	E-mail
Message0002	D:\SCYT\CF\Email\Jim_shu's.pst>>Personal Fol...			E-mail Messa...	E-mail
Message0002	D:\SCYT\CF\Email\Jim_shu's.pst>>Personal Fol...			E-mail Messa...	E-mail

32 Listed 0 Checked Total 0 Highlighted

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.

The screenshot shows the AccessData FTK 1.81.0 interface. On the left, a tree view displays a folder structure under 'Email' for 'Jim_shu's.pst'. A right-click context menu is open over a deleted item in the 'Personal Fold' folder. The menu options include 'Create Bookmark...', 'View This Item in a Different List >', 'Launch Detached Viewer' (which is highlighted with a green box), 'Launch Associated Program', 'View With...', 'Copy Special...', 'Export File...', 'Recursive File Export...', 'Analysis Tools...', and 'Column Settings...'. The main pane shows a message titled 'Message0001' with the following details:

**Message0001**

**Subject:** RE: Bike spec's  
**From:** Jim Shu  
**Date:** 04-12-2006 08:37:00  
**To:** '5amspade@myway.com'

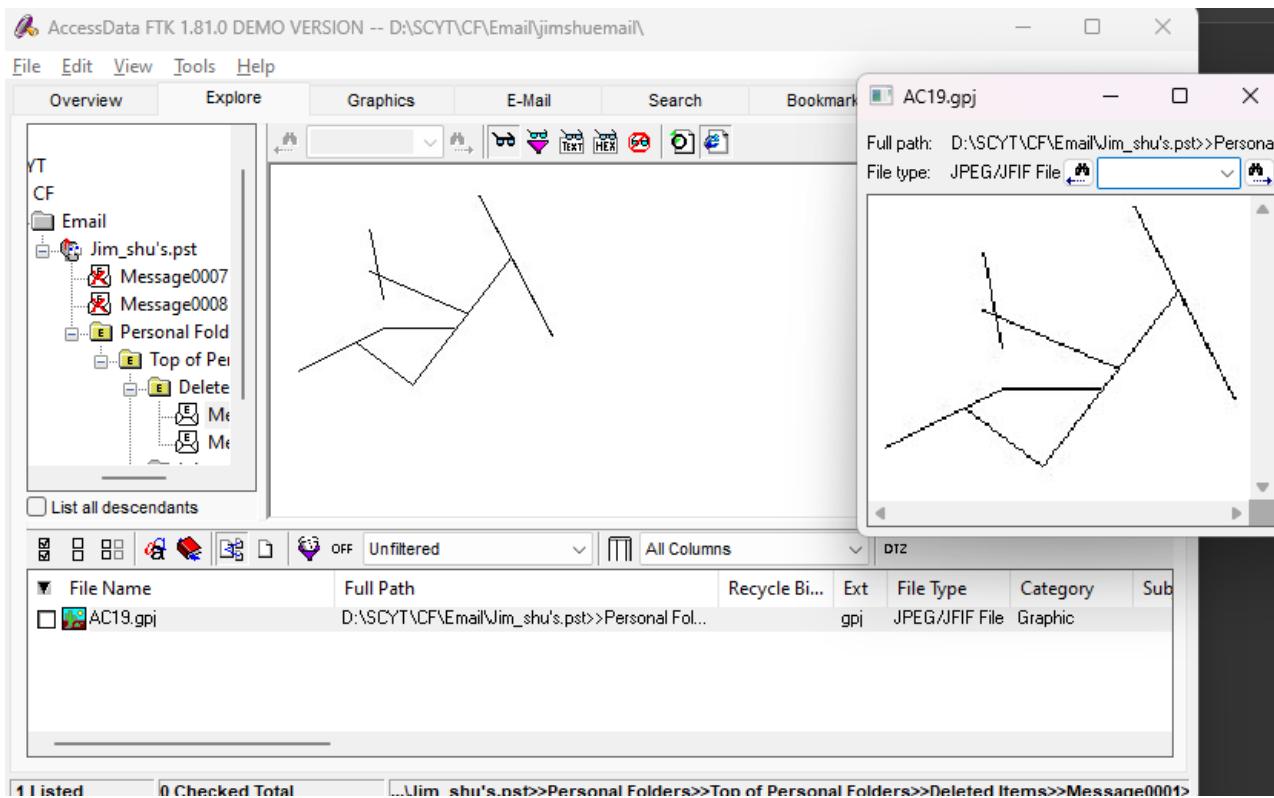
**Message Body**

You'll have to change the extension to .jpg.  
I'm in need of money, can you send a downpayment?

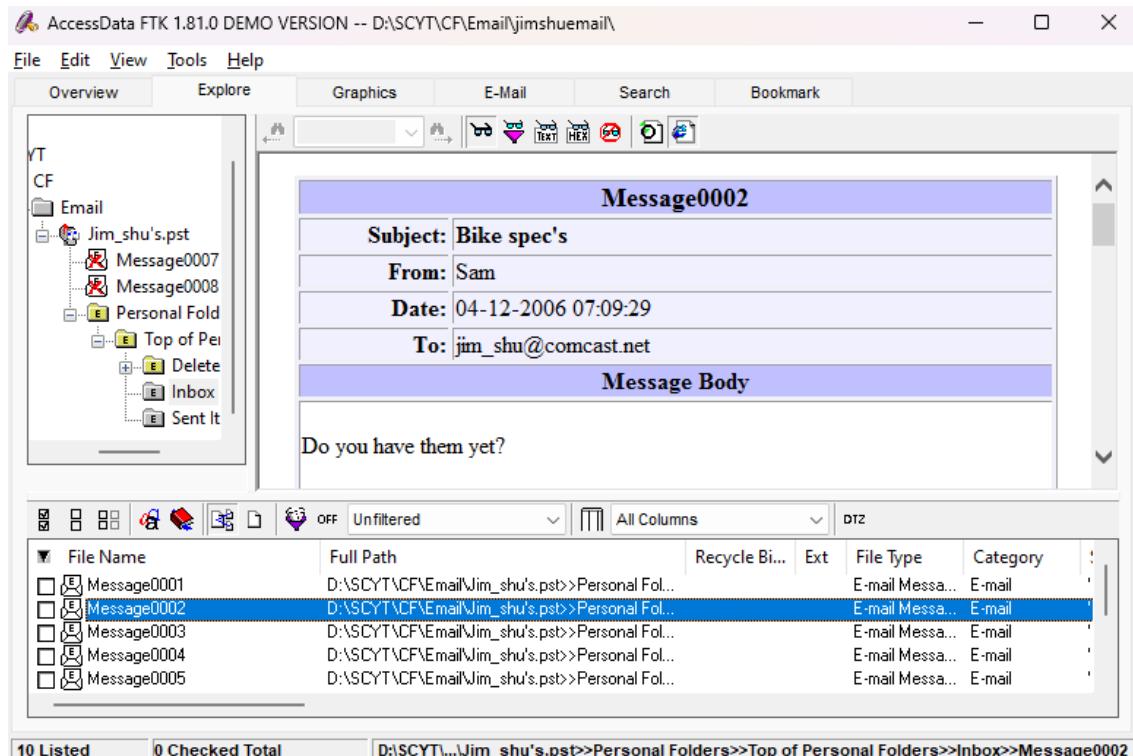
The bottom pane shows a file list with one item: 'AC19.gpi'.

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

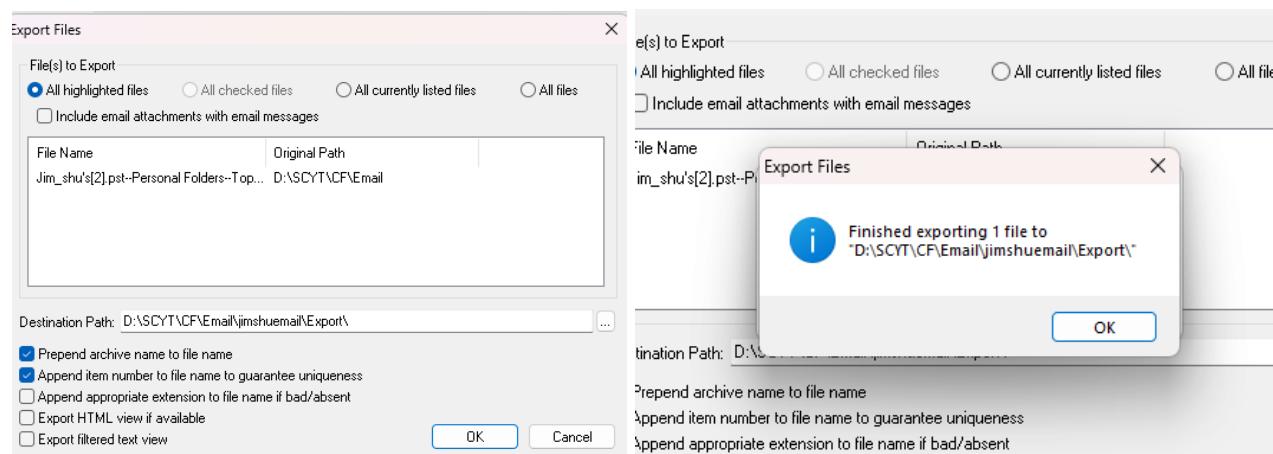
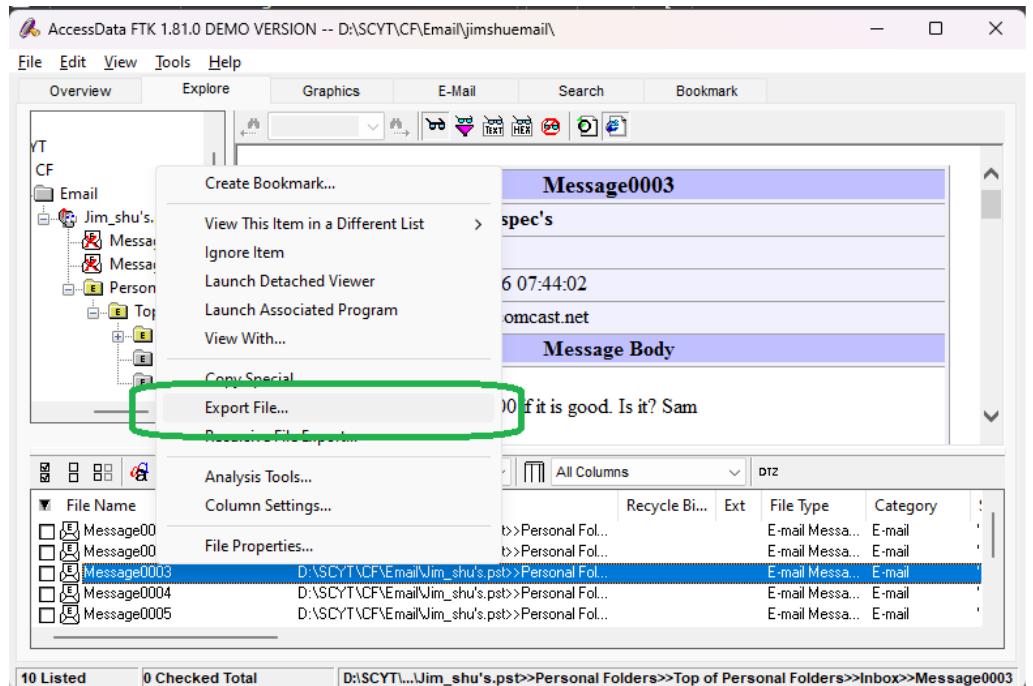
This screenshot is similar to the previous one, but the 'Launch Detached Viewer' option in the context menu is highlighted with a green box. The rest of the interface and message details are identical to the first screenshot.



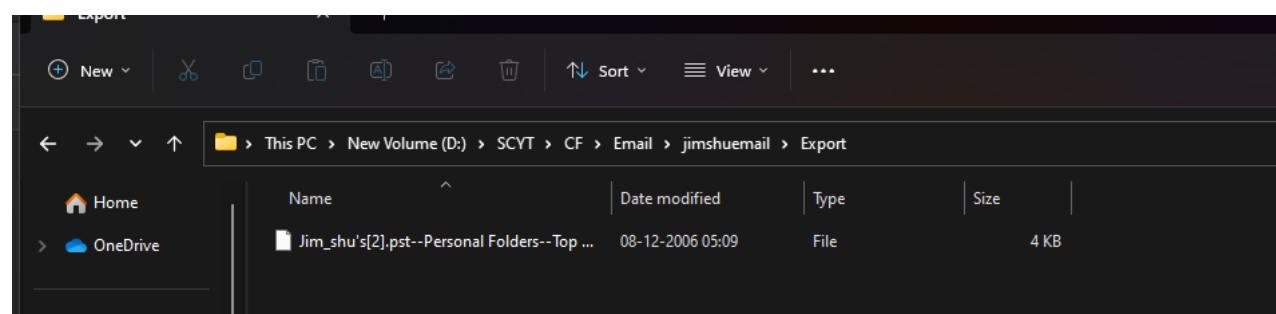
For analyzing header follow following steps: Click the E-Mail tab. In the tree view, click to expand all folders, and then click the Inbox folder. In the File List pane at the upper right, click Message0003; as shown in the pane at the bottom, it's from Sam and is addressed to [jim_shu@comcast.net](mailto:jim_shu@comcast.net).



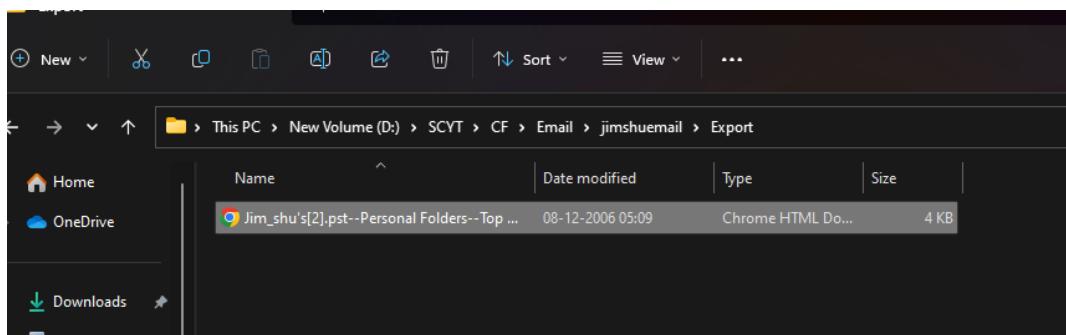
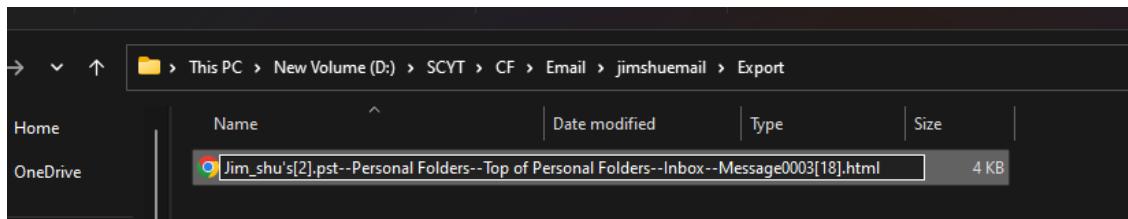
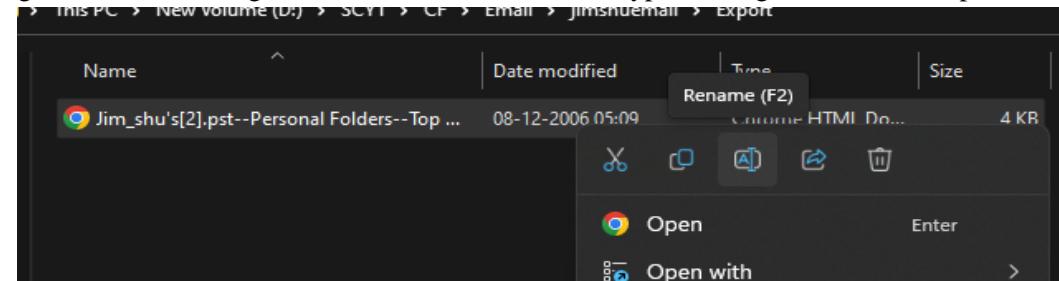
Right-click on any message say Message0003 in the File List pane and click Export File. In the Export Files dialog box, click OK.



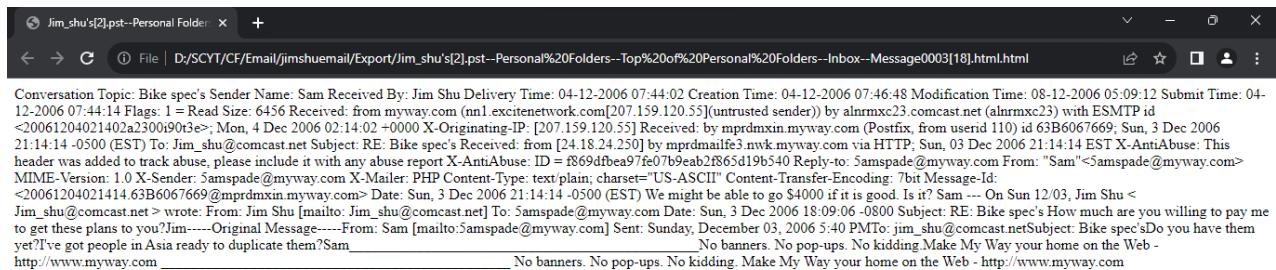
FTK saves exported files in the HTML format with no extension.



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.



## PRACTICAL NO. 10

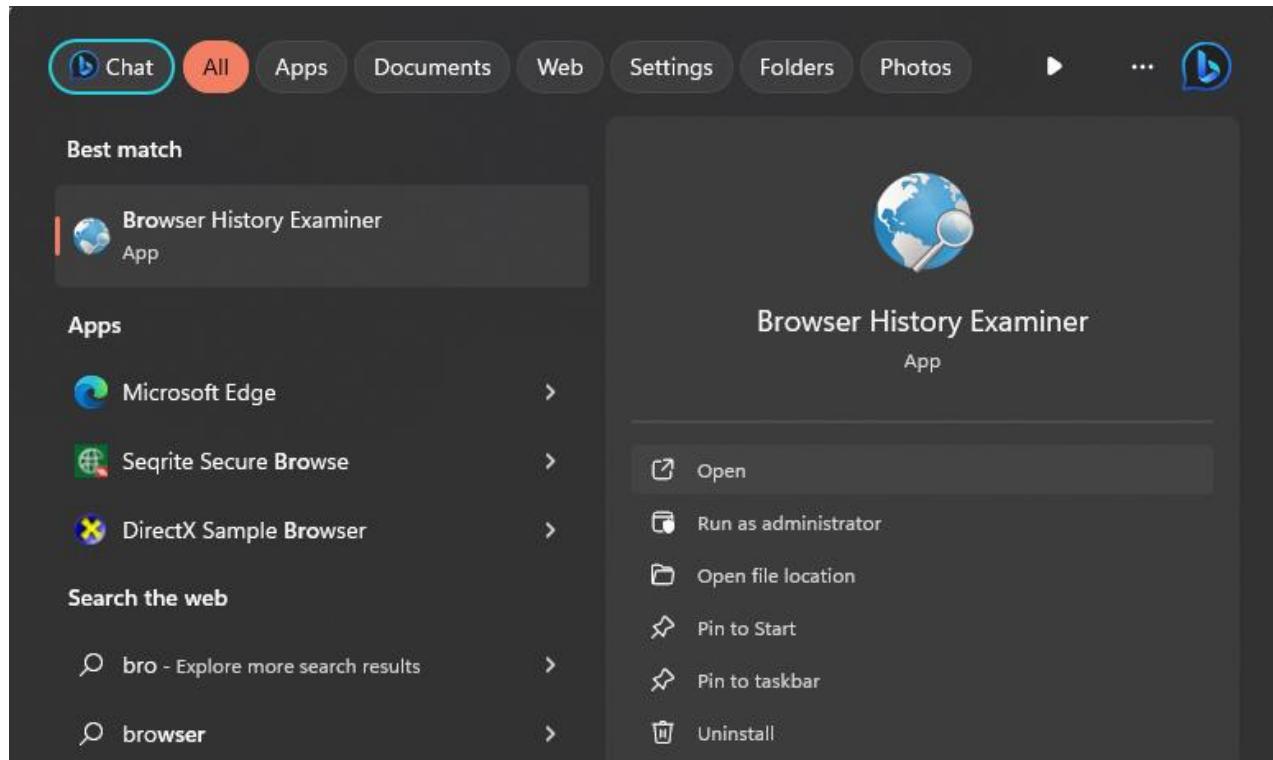
### Aim:

Web Browser Forensics

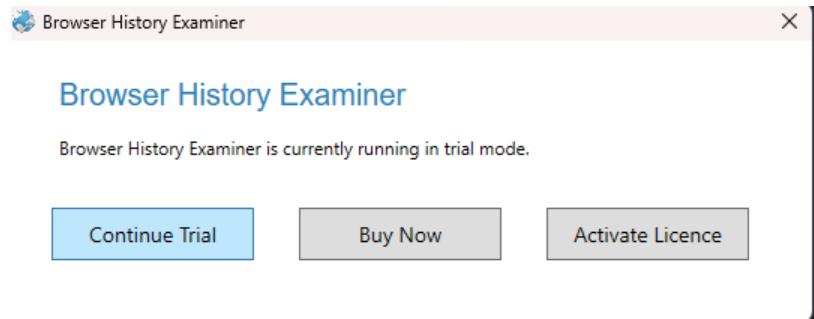
- Analyze browser artifacts, including history files, bookmarks, and download records.
- Analyze cache and cookies data to reconstruct user-browsing history and identify visited websites or online activities.
- Extract the relevant log or timestamp file, analyze its contents and interpret the timestamp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

### Practical:

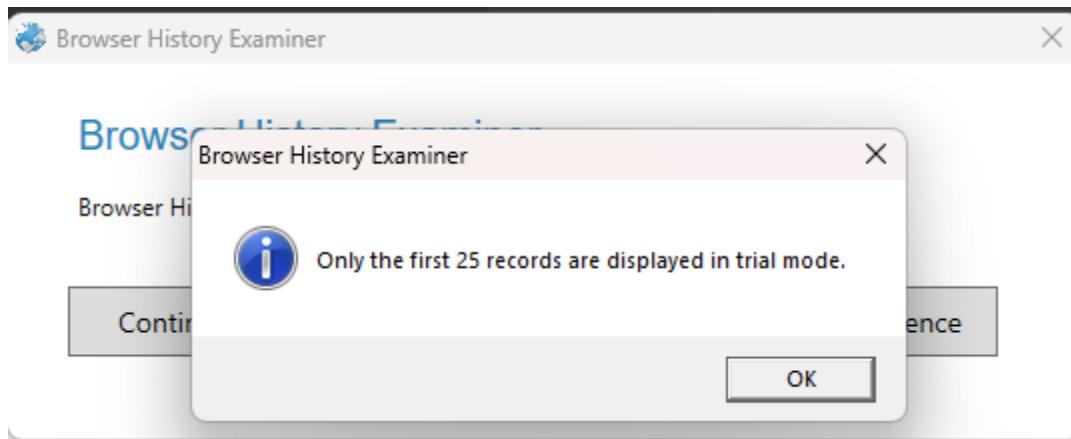
We are going to use the **Browser History Examiner**. Run it as Administrator..



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



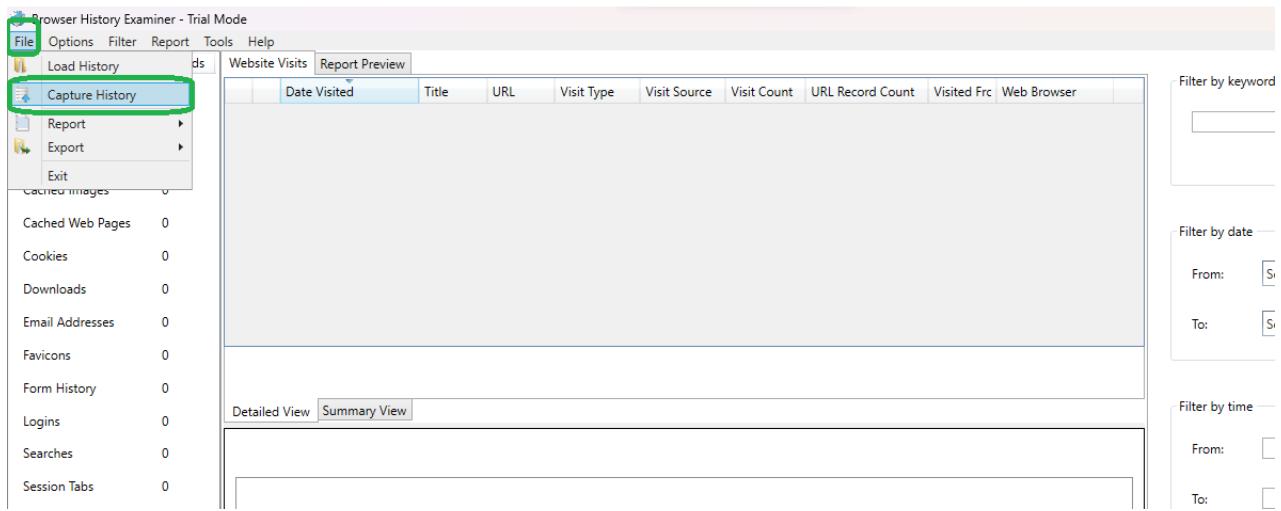
Click on Continue Trail



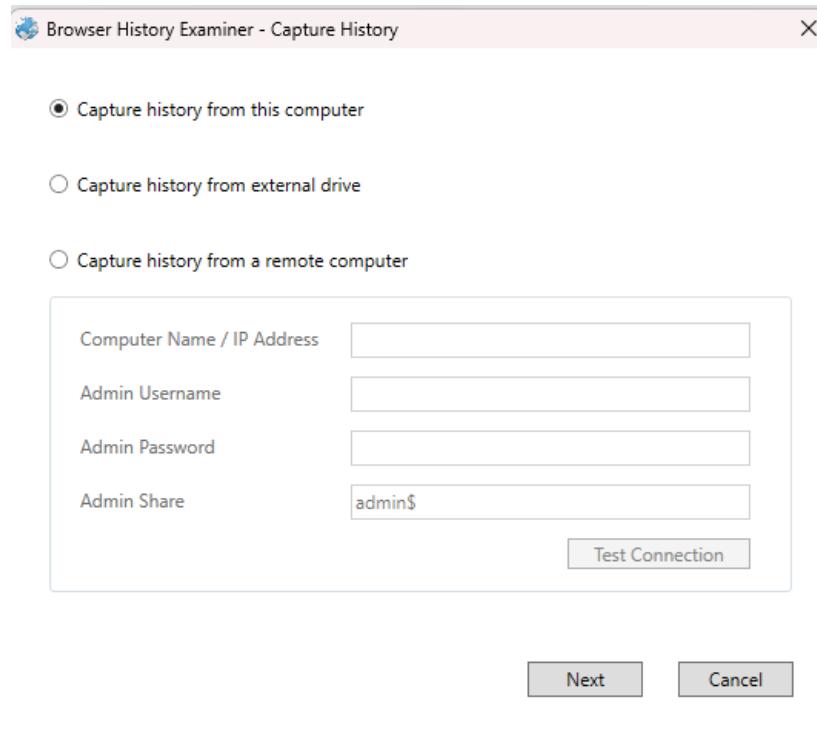
Click OK

This is the Interface of the Application

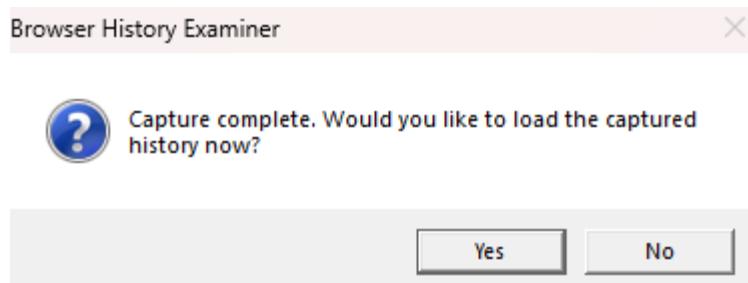
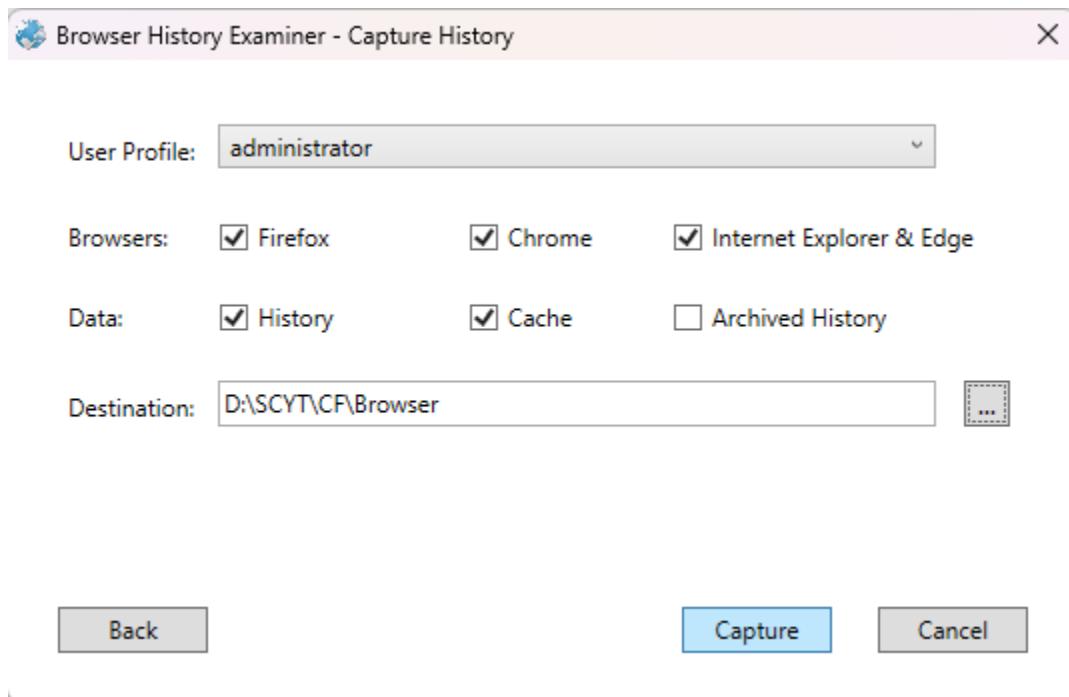
Go to File → Capture History



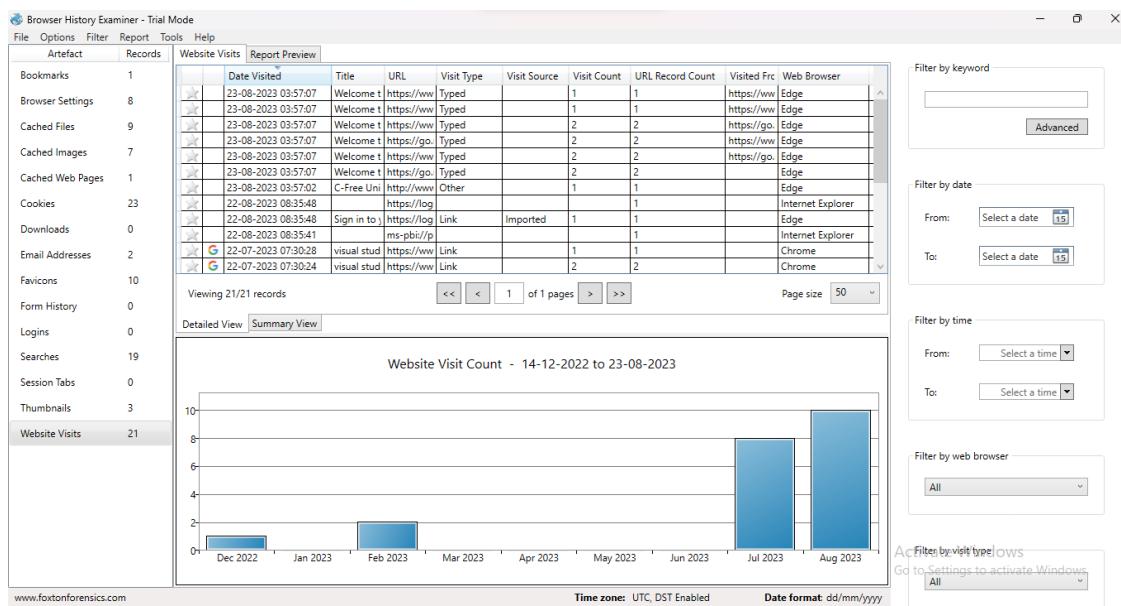
We are going to capture from this device only Select on that and click Next



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

The screenshot shows the 'Bookmarks' tab in the 'Browser History Examiner - Trial Mode' interface. The left sidebar lists artifacts: Bookmarks (1), Browser Settings (8), Cached Files (9), Cached Images (7), Cached Web Pages (1), Cookies (23), and Downloads (0). The main pane displays a table with columns: Date Added, Last Modified, Title, URL, and Web Browser. One entry is shown: Bing, added on [date] at [time], last modified on [date] at [time], with the URL <http://go.microsoft.com/fwlink/p/?Link> and Web Browser set to Internet Explorer. Filter options for keyword and date are visible on the right.

Here we can see the browser settings

The screenshot shows the 'Browser Settings' tab in the 'Browser History Examiner - Trial Mode' interface. The left sidebar lists artifacts: Bookmarks (1), Browser Settings (8), Cached Files (9), Cached Images (7), Cached Web Pages (1), Cookies (23), and Downloads (0). The main pane displays a table with columns: Name, Value, and Web Browser. Eight entries are listed under Sync: Sync Apps (Yes, Edge), Sync Autofill (Yes, Edge), Sync Bookmarks (Yes, Edge), Sync Extensions (Yes, Edge), Sync Passwords (Yes, Edge), Sync Preferences (Yes, Edge), Sync Tabs (No, Edge), and Sync Typed URLs (No, Edge). Filter options for keyword, date, and time are visible on the right.

Here we can see the cached files

The screenshot shows the 'Cached Files' tab in the 'Browser History Examiner - Trial Mode' interface. The left sidebar lists artifacts: Bookmarks (1), Browser Settings (8), Cached Files (9), Cached Images (7), Cached Web Pages (1), Cookies (23), and Downloads (0). The main pane displays a table with columns: Last Fetched, Content Type, URL, Fetch Count, File Size (Bytes), and Web Browser. Nine entries are listed, all from Microsoft Edge, with URLs like <https://aadcdn.msftauth.net/shared/1.0/co>, <https://aadcdn.msftauth.net/ests/2.1/contx>, and <https://aadcdn.msftauth.net/ests/2.1/contx>. Filter options for keyword, date, and time are visible on the right.

Here we can see the cached images

Browser History Examiner - Trial Mode

File Options Filter Report Tools Help

Artifact Records Cached Images Report Preview

	Last Fetched	Content Type	URL	Fetch Count	File Size (Bytes)	Web Browser
Bookmarks	1	image/svg+xml	https://aadcdn.msftauth.net/shared/1.0/content/r/1	3651	Internet Explorer	
Browser Settings	8	image/gif	https://aadcdn.msftauth.net/shared/1.0/content/r/1	3620	Internet Explorer	
Cached File	9	image/gif	https://aadcdn.msftauth.net/shared/1.0/content/r/1	2672	Internet Explorer	
Cached Images	7	image/svg+xml	https://aadcdn.msftauth.net/shared/1.0/content/r/1	1864	Internet Explorer	
Cached Web Pages	1	image/svg+xml	https://aadcdn.msftauth.net/shared/1.0/content/r/1	1378	Internet Explorer	
Cookies	23	image/svg+xml	https://aadcdn.msftauth.net/shared/1.0/content/r/1	899	Internet Explorer	
Downloads	0	image/svg+xml	https://aadcdn.msftauth.net/shared/1.0/content/r/1	222	Internet Explorer	
Email Addresses	2					
Favicons	10					
Form History	0					
Logins	0					
Searches	19					
Session Tabs	0					
Thumbnails	3					
Website Visits	21					

Viewing 7/7 records

Page size: 50

Filter by keyword:

Filter by date: From: Select a date To: Select a date

Filter by time: From: Select a time

Filter by web browser: All

Filter Windows:  Skip to Settings to activate Windows

Here we can see the cached webpages

Browser History Examiner - Trial Mode

File Options Filter Report Tools Help

Artifact Records Cached Web Pages Report Preview

	Last Fetched	URL	Fetch Count	File Size (Bytes)	Web Browser
Bookmarks	1				
Browser Settings	8				
Cached Files	9				
Cached Images	7				
Cached Web Pages	1				
Cookies	23				
Downloads	0				
Email Addresses	2				
Favicons	10				
Form History	0				
Logins	0				
Searches	19				

Viewing 1/1 records

Page size: 50

Filter by keyword:  Advanced

Filter by date: From: Select a date To: Select a date

Filter by time: From: Select a time

Here we can see the cookies stored

Browser History Examiner - Trial Mode

File Options Filter Report Tools Help

Artifact Records Cookies Report Preview

	Date Created	URL	Last Accessed	Date Expires	Name	Content	Web Browser
Bookmarks	1	msn.com/	22-07-2023 05:11:01	15-08-2024 05:11:02	MUID	392592F187B26B	Edge
Browser Settings	8	g.msn.com/	22-07-2023 05:11:01	29-07-2023 05:11:02	MR	0	Edge
Cached Files	9	live.com/	22-07-2023 05:10:41	15-08-2024 05:10:42	MUID	2F13847EF5E36B	Edge
Cached Images	7	bing.com/	06-01-2023 10:34:56	31-01-2024 10:34:57	MUID	09DB3FCAFEEA67	Edge
Cached Web Pages	1	www.bing.com/	22-07-2023 05:46:32	15-08-2024 05:46:32	MUIDB	09DB3FCAFEEA67	Edge
Cookies	23	bing.com/	06-01-2023 10:34:56	31-01-2024 10:34:57	_EDGE_V	1	Edge
Downloads	0	bing.com/	06-01-2023 10:34:56	06-01-2025 10:34:57	SRCHD	AF=NOMFORM	Edge
Email Addresses	2	bing.com/	06-01-2023 10:34:56	06-01-2025 10:34:57	SRCHUID	V=2&GUID=F3E30	Edge
Favicons	10	bing.com/	06-01-2023 10:34:56	06-01-2025 10:34:57	SRCHUSR	DOB=20230106	Edge
Form History	0	bing.com/	22-07-2023 05:46:32	22-07-2025 05:46:32	SRCHPGUSR	SRCHLANG=en&k	Edge
Logins	0	bing.com/	22-07-2023 05:39:48	22-07-2023 17:39:48	SUID	M	Edge
Searches	19	login.microsofton	22-08-2023 08:35:48	21-09-2023 08:35:49	buid	0.AVYAME_N-B6f	Edge
Session Tabs	0	login.microsofton	22-08-2023 08:35:53	21-09-2023 08:35:53	fpc	Atl64KFtOJAIMP	Edge
Thumbnails	3	login.microsofton	22-08-2023 08:35:48	15-09-2024 08:35:48	brcap	0	Edge
Website Visits	21	www.bing.com/	22-07-2023 07:31:12	15-08-2024 07:31:13	MUIDB	02B7C9F658384A	Edge
		bing.com/	14-12-2022 09:46:56	14-12-2024 09:46:57	SRCHUID	V=2&GUID=5D81	Edge
		bing.com/	14-12-2022 09:46:56	14-12-2023 09:46:57	CortanaAppUID	6E148F4EAC1031	Edge
		bing.com/	14-12-2022 09:46:56	14-12-2024 09:46:57	SRCHD	AF=NOMFORM	Edge
		bing.com/	14-12-2022 09:46:56	14-12-2024 09:46:57	SRCHUSR	DOB=20221214	Edge
		bing.com/	22-07-2023 07:31:15	15-08-2024 07:31:15	SRCHHPGUSR	SRCHLANG=en&k	Edge
		bing.com/	14-12-2022 09:47:11	14-12-2024 09:47:12	ANON	A=2C7B78C7DDA	Edge
		bing.com/	22-07-2023 05:10:35	22-07-2023 17:10:36	SUID	A	Edge
		login.microsofton	22-07-2023 07:12:26	21-08-2023 07:12:27	fpc	AuHs6tZyQ1LmN	Edge

Filter by keyword:

Filter by date: From: Select a date To: Select a date

Filter by time: From: Select a time

Filter by web browser: All

Here we can see the emails used for logins

Last Used	Email Address	Domain	Source	Web Browser
22-08-2023 08:35:48	ashwiniparab146@gmail.com	login.microsoftonline.com	Website Visit	Internet Explorer
22-08-2023 08:35:48	ashwiniparab146@gmail.com	login.microsoftonline.com	Website Visit	Edge

Here we can see the favicons

URL	Page URL	Expires	Last Updated	Web Browser
https://cdn.sstatic.net/Sites/stackoverflowfl	https://stackoverflow.com/questions/4		22-07-2023 07:28:01	Chrome
https://cdn.sstatic.net/Sites/stackoverflowfl	https://stackoverflow.com/questions/4		22-07-2023 07:28:01	Chrome
G https://www.google.com/favicon.ico	https://www.google.com/search?q=go		22-07-2023 07:27:28	Chrome
G https://www.google.com/favicon.ico	https://www.google.com/search?q=go		22-07-2023 07:27:28	Chrome
G https://www.google.com/favicon.ico	https://www.google.com/search?q=anc		22-07-2023 07:27:28	Chrome
G https://www.google.com/favicon.ico	https://www.google.com/search?q=anc		22-07-2023 07:27:28	Chrome
G https://www.google.com/favicon.ico	https://www.google.com/search?q=visi		22-07-2023 07:27:28	Chrome
G https://www.google.com/favicon.ico	https://www.google.com/search?q=visi		22-07-2023 07:27:28	Chrome
G https://www.google.com/favicon.ico	https://www.google.com/search?q=visi		22-07-2023 07:27:28	Chrome
G https://www.google.com/favicon.ico	https://www.google.com/search?q=visi		22-07-2023 07:27:28	Chrome

Here we can see the searches

Date Searched	Search Terms	Search Engine	URL	Source	Web Browser
22-07-2023 07:30:28	visual studio is missing neces	Google	https://www.google.com/sea	Chrome History	Chrome
22-07-2023 07:30:28	visual studio is missing neces	Google	https://www.google.com/sea	Website Visit	Chrome
22-07-2023 07:30:24	visual studio is missing neces	Google	https://www.google.com/sea	Chrome History	Chrome
22-07-2023 07:30:24	visual studio is missing neces	Google	https://www.google.com/sea	Website Visit	Chrome
22-07-2023 07:30:23	visual studio is missing neces	Google	https://www.google.com/sea	Website Visit	Chrome
22-07-2023 07:27:47	android licenses	Google	https://www.google.com/sea	Chrome History	Chrome
22-07-2023 07:27:47	android licenses	Google	https://www.google.com/sea	Website Visit	Chrome
22-07-2023 07:27:47	android licenses	Google	https://www.google.com/sea	Website Visit	Chrome
22-07-2023 07:27:27	google	Google	https://www.google.com/sea	Chrome History	Chrome
22-07-2023 07:27:27	google	Google	https://www.google.com/sea	Website Visit	Chrome
22-07-2023 07:27:27	google	Google	https://www.google.com/sea	Website Visit	Chrome
G	google	Google	https://www.google.com/sea	Favicon	Chrome
G	google	Google	https://www.google.com/sea	Favicon	Chrome

Here we see the thumbnails

Browser History Examiner - Trial Mode

File Options Filter Report Tools Help

Artefact	Records	Thumbnail	Title	Filename	Last Updated	Web Browser
Bookmarks	1		https://chrome.google.com/websl	Web Store		Chrome
Browser Settings	8		https://www.office.com/	Office		Edge
Cached Files	9		https://go.microsoft.com/fwlink/?l	Welcome to Microsoft Edge		Edge
Cached Images	7					
Cached Web Pages	1					
Cookies	23					
Downloads	0					
Email Addresses	2					
Favicons	10					
Form History	0					
Logins	0					
Searches	19					
Session Tabs	0					
Thumbnails	3					
Website Visits	21					

Viewing 3/3 records << < 1 of 1 pages > >> Page size 50

Here we can see the websites visits

Browser History Examiner - Trial Mode

File Options Filter Report Tools Help

Artefact	Records	Website Visits	Report Preview
Bookmarks	1		Date Visited Title URL Visit Type Visit Source Visit Count URL Record Count Visited Frc Web Browser
Browser Settings	8		23-08-2023 03:57:07 Welcome t https://ww/ Typed 1 1 Edge
Cached Files	9		23-08-2023 03:57:07 Welcome t https://ww/ Typed 2 2 Edge
Cached Images	7		23-08-2023 03:57:07 Welcome t https://go. Typed 2 2 Edge
Cached Web Pages	1		23-08-2023 03:57:07 Welcome t https://ww/ Typed 2 2 Edge
Cookies	23		23-08-2023 03:57:02 C-Free Un http://ww/ Other 1 1 Edge
Downloads	0		22-08-2023 08:35:48 Sign in to https://log Link Imported 1 1 Internet Explorer
Email Addresses	2		22-08-2023 08:35:41 ms-pbi/p 1 1 Internet Explorer
Favicons	10		22-07-2023 07:30:28 visual stud https://ww/ Link 1 1 Chrome
Form History	0		22-07-2023 07:30:24 visual stud https://ww/ Link 2 2 Chrome
Logins	0		
Searches	19		
Session Tabs	0		
Thumbnails	3		
Website Visits	21		

Viewing 21/21 records << < 1 of 1 pages > >> Page size 50

Detailed View Summary View

Website Visit Count - 14-12-2022 to 23-08-2023

Filter by keyword

Filter by date

From: Select a date 15 To: Select a date 15

Filter by time

From: Select a time To: Select a time

Filter by web browser

All

Filter by visit type

Allows