

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	Recovering and Inspecting deleted files <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	Steganography Detection <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	Mobile Device Forensics <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	Email Forensics <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	Web Browser Forensics <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

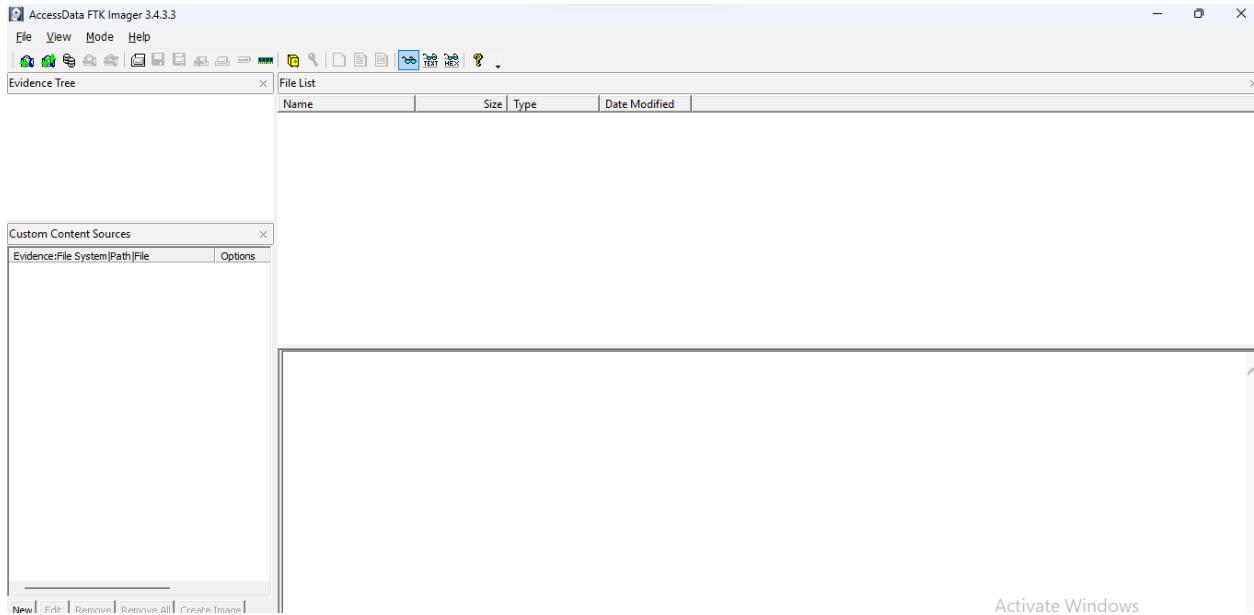
Aim:

Creating a Forensic Image using FTK Imager/Encase Imager:

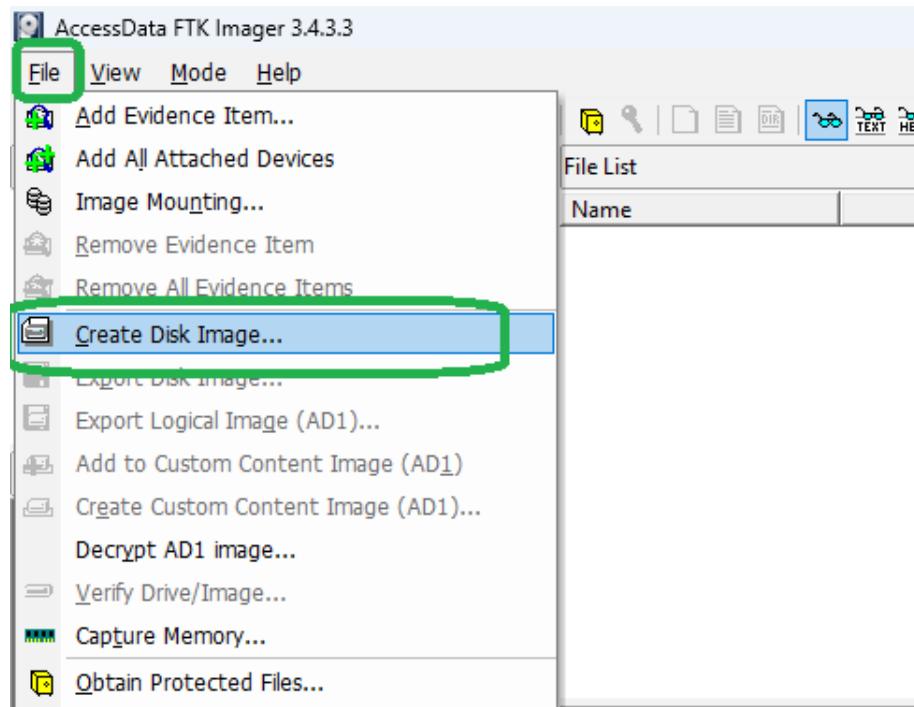
- Creating Forensic Image
- Check Integrity of Data
- Analyze Forensic Image

Practical:

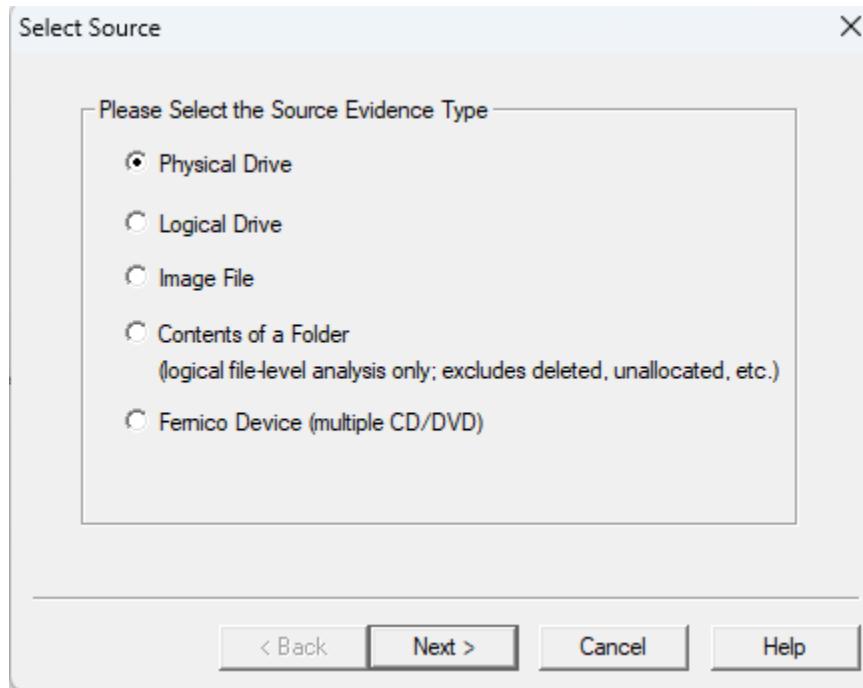
In this Practical we are going to use the FTK Imager to create Images of the evidences



Go to File → Create Disk Image

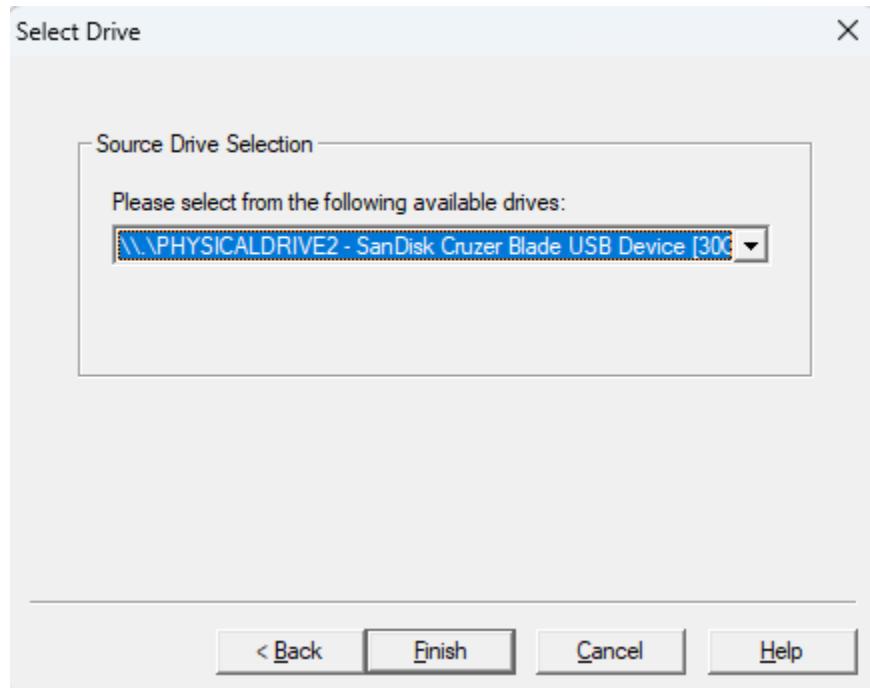


Select the source evidence type

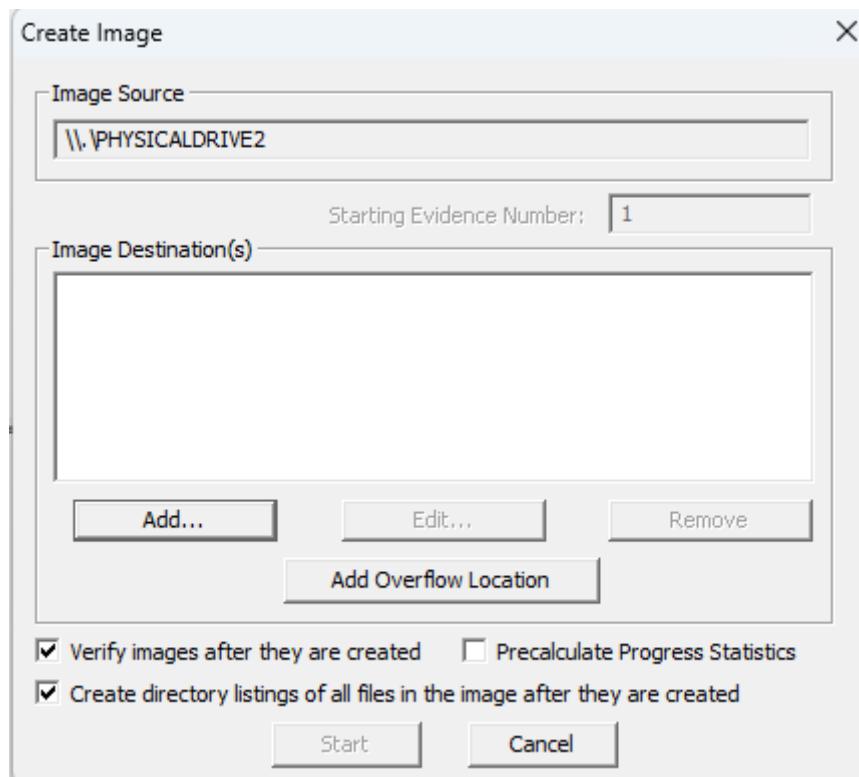


Here we are going to select the physical drive and proceed

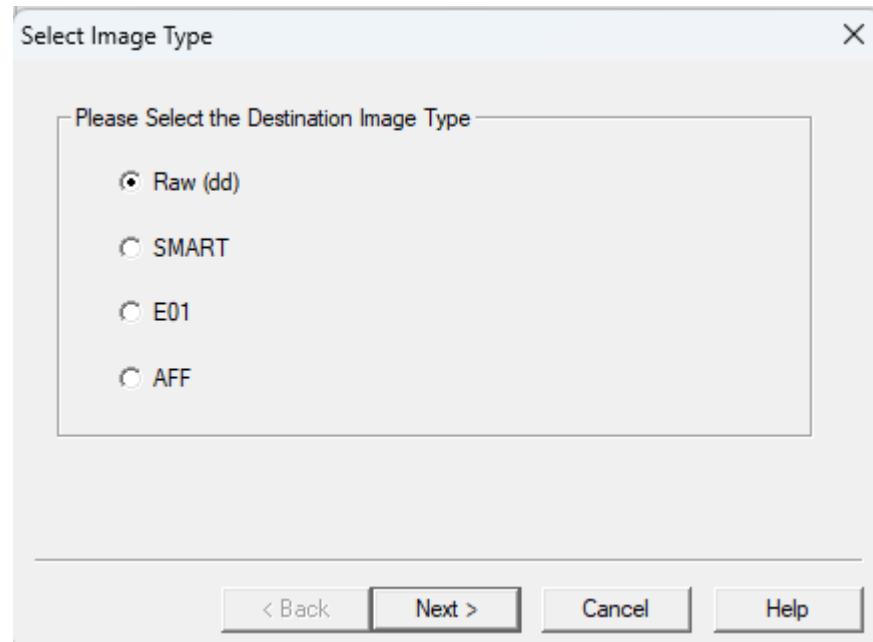
Then we browse the location of the **Pen drive** and click Finish



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

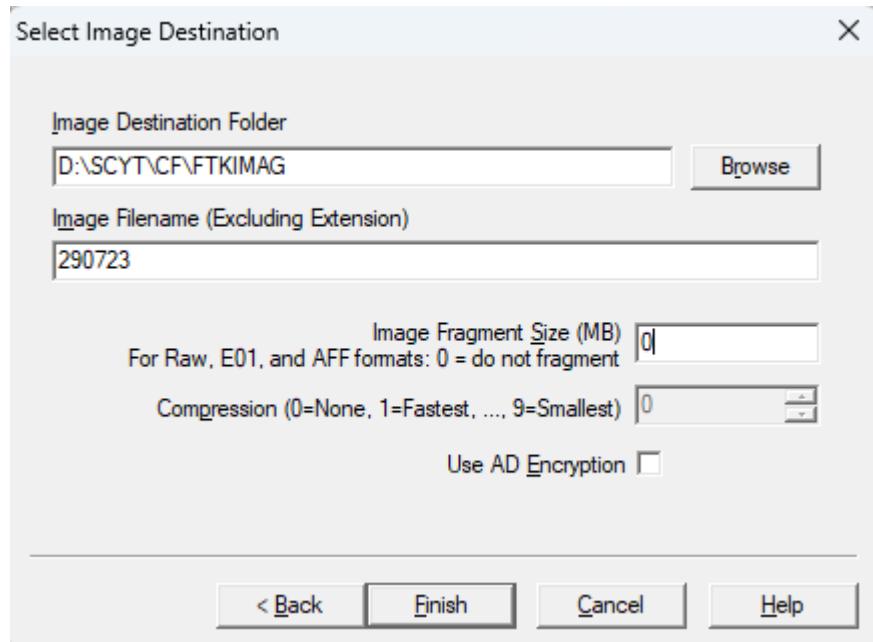
A screenshot of a software dialog box titled "Evidence Item Information". It contains five input fields with the following data:

- Case Number: 290723
- Evidence Number: 48
- Unique Description: Sandisk Red & Black Colour 32GB
- Examiner: Maddy
- Notes: New, Unused, Empty

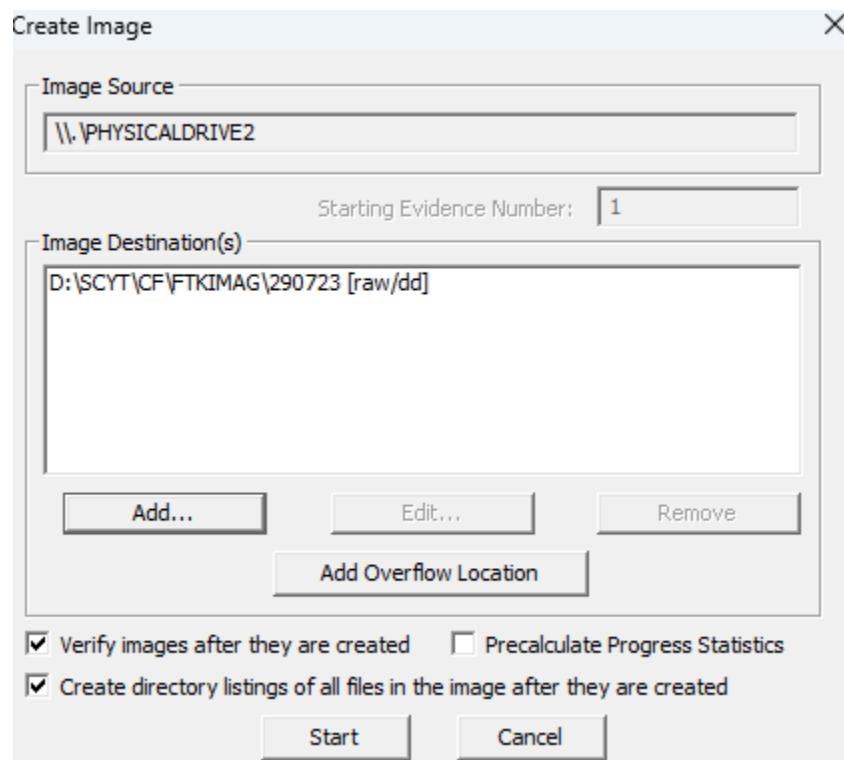
At the bottom are buttons for "< Back", "Next >" (highlighted in grey), "Cancel", and "Help".

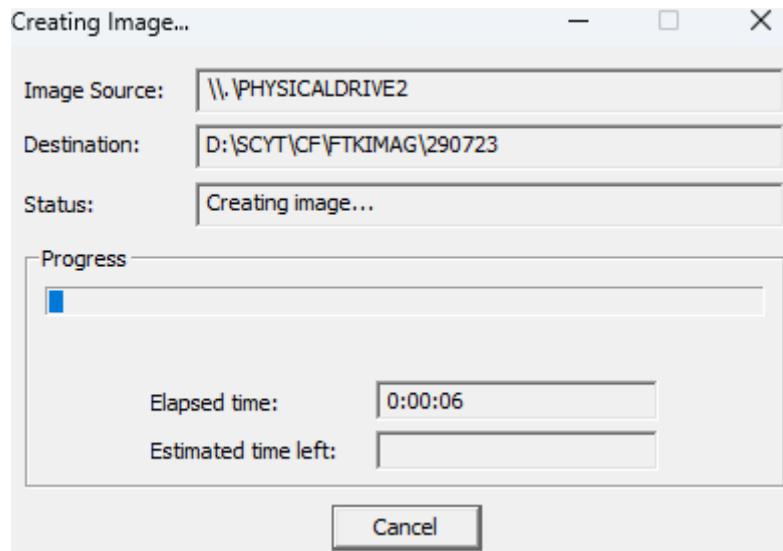
Create a folder to save the images to store in the system disk as the pen drive size cannot be stored in the same drive

Then paste that location to save the images and click Finish

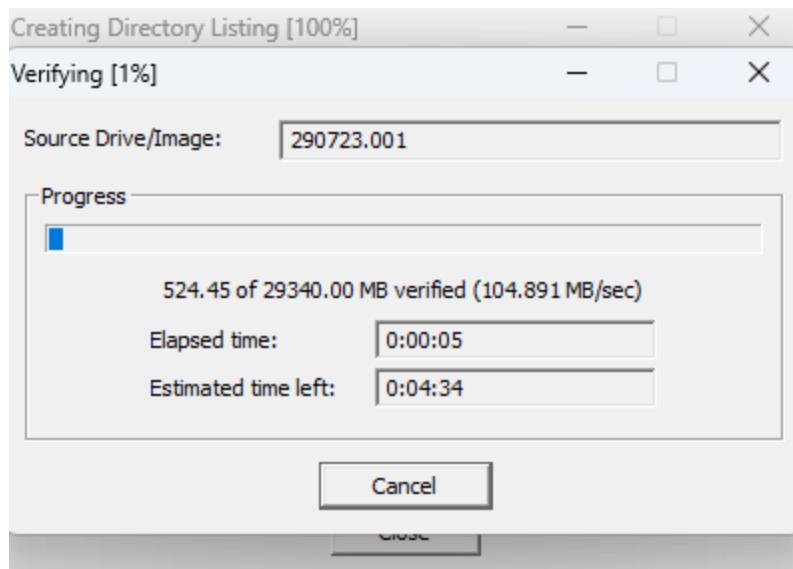


Then Click on Start and wait until the imaging is done

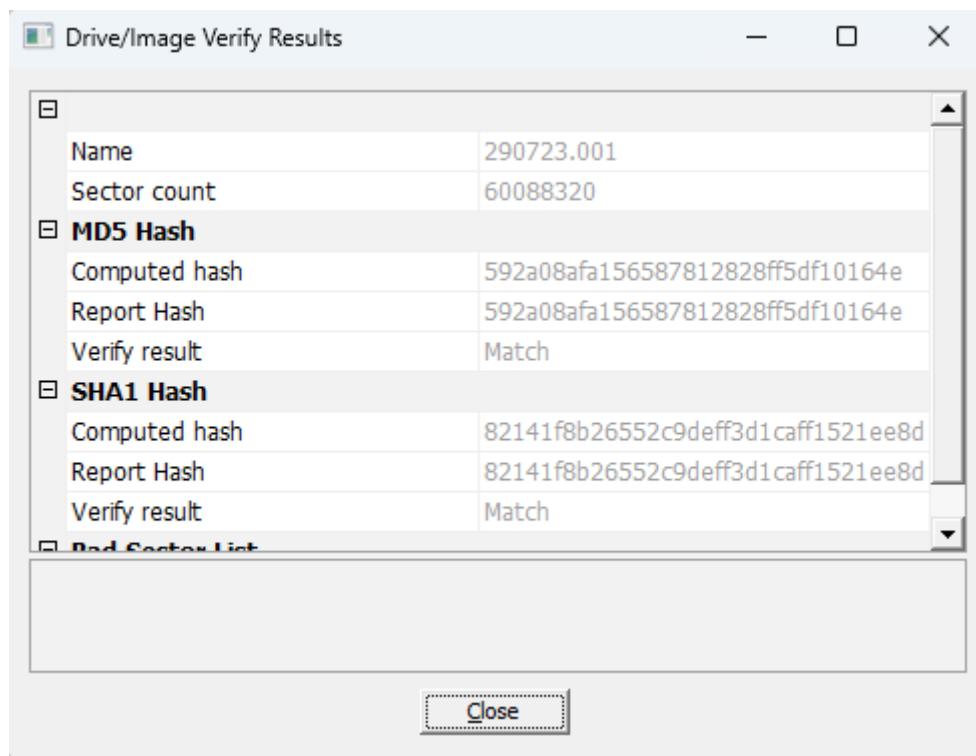




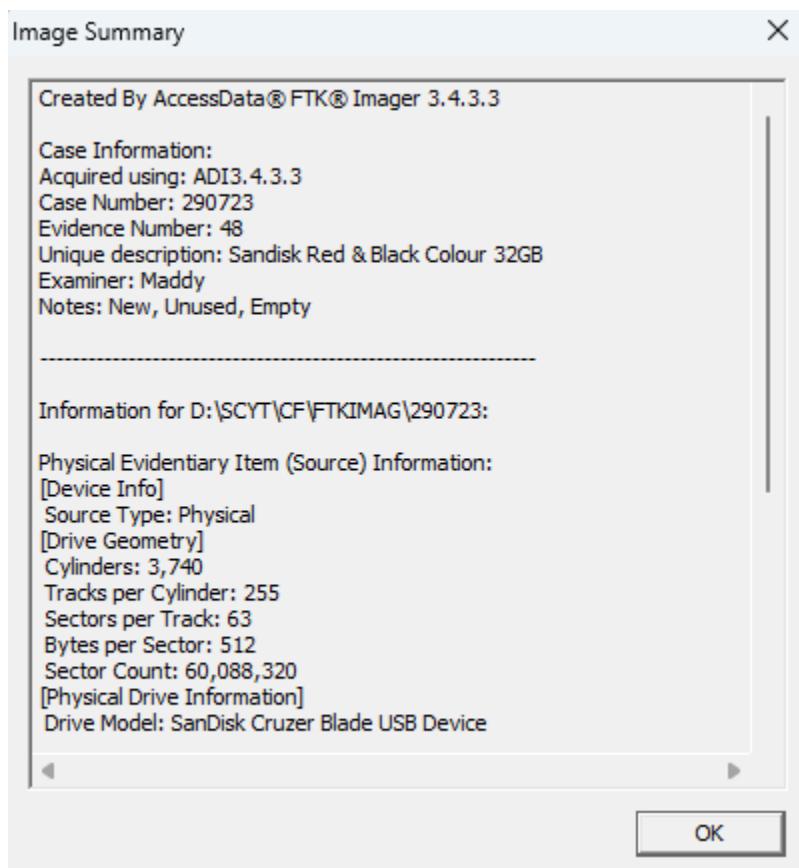
Now it will verify



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

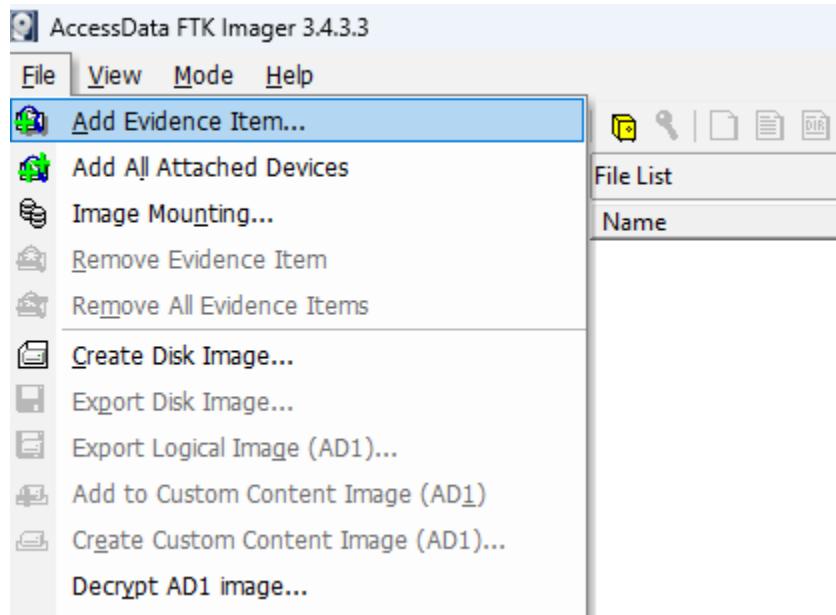


We take the image summary

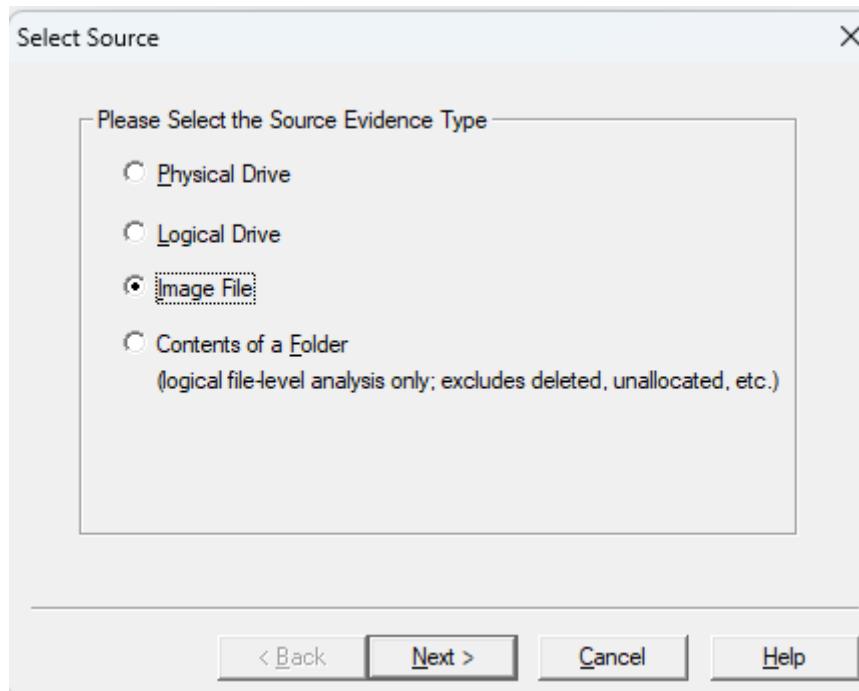


Now we are going to view the images in the FTK Imager

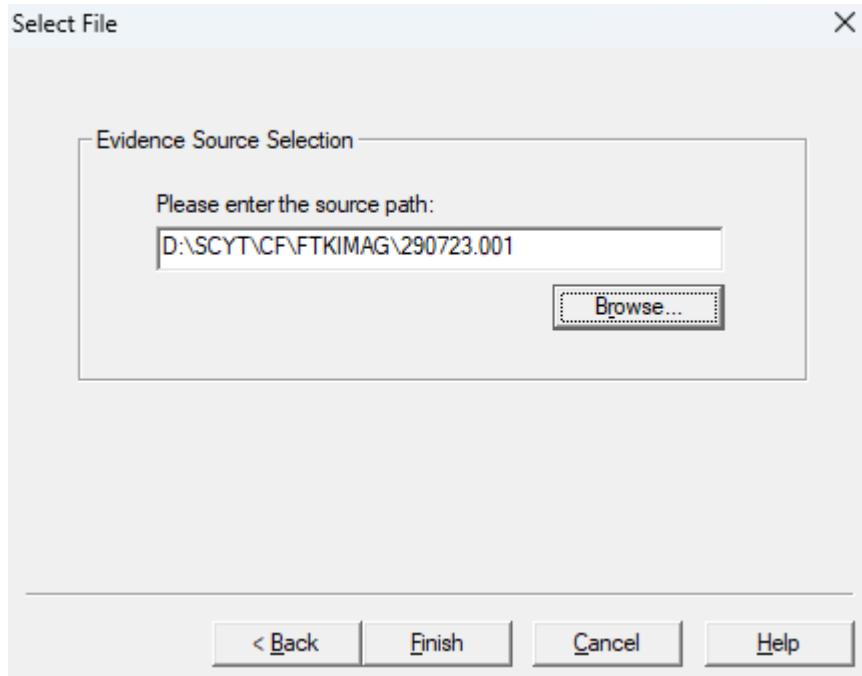
Go to File → Add Evidence Item



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



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



Here we can see the data shown by the FTK Imager

Name	Size	Type	Date Modified
000000000 41 4B 45 4F FC 31 C0 FA-SE DO BC 90 7C FB 89 E6 AKEOGLAü-BN-1d-e			
000000010 89 E7 1E 06 8E D8 BB 13-04 8B 07 48 89 07 C1 E0 c...@...-H-Aa			
000000020 06 2D C0 07 8E C0 B9 00-02 F3 A4 50 68 30 7C CB -A-A...-öphoiE			
000000030 8E D8 66 31 DB 8E C3 41-B8 81 00 E8 89 00 72 6D öf10 ÄA...-e...rm			
000000040 00 00 00 00 BE TD B9 80 26 80-3F 00 70 09 00 05 83 C3 341-4-7-1-u-A			
000000050 10 E2 F3 EB 58 B8 94 1D-00 00 00 00 00 00 00 00 00 BA SA ädeXW)eU-ä#*2			
000000060 7D 80 00 00 E8 A0 00 B0-01 CD 16 75 3B B0 CD [name]e -1-1-1			
000000070 16 24 04 75 38 80 93-7D 00 70 0B 00 B4 7D 08 05 > -N)ä			
000000080 B3 00 06 06 93 7D 12 80-3E 92 7D 00 75 D9 E8 89 E-...->-1 wö			
000000090 00 C6 06 BE 70 81 68 80-00 BA 72 7D BE 7E TD E8 E...-h...*%)-ä			
0000000a0 e5 00 9A 07 17 EA 00 7C-00 00 E2 6D 00 E8 78 00 e-2- -ä-äm-äx			
0000000b0 BB BE 7D 8B 17 52 B2 80-3B 4F 02 66 88 5F 08 E0 E8 h...-R...-O-f...ä			
0000000c0 05 00 73 D5 07 1F CB 60-84 41 B8 55 CD 13 72 -äö...E...äwÜ!z			
0000000d0 2C 81 EB 55 AA 75 26 F7-C1 01 00 74 20 61 1E 66 ,0Wus-ä...-t a.f			
0000000e0 31 C0 8E D8 66 50 66 53-50 68 00 7C 40 50 6A 10 l...öPfSPH-(8Pj			
0000000f0 89 E6 B4 42 CD 13 9F 83-C4 10 90 1F C3 61 BB 00 e...Bj...-ä...ää-			
000000100 7C B8 01 02 CD 13 C3 FA-8B 1C 24 66 88 07 66 81 l...-i...äü...-äf...-f...			
000000110 04 26 89 17 24 8C 4F 02-FB C3 FA BB 20 00 66 A1 e...-o-0-ñä...-f;			
000000120 6E 7D 26 66 88 07 FB C3-B4 01 CD 16 74 06 B4 00 n)ef...-ää...-i...-t...-i			
000000130 CD 16 E2 F4 C3 AC 3C 00-74 09 B4 0E BB 07 00 CD i...ä5...< t...-> .i			

RIZVI COLLEGE OF ARTS, SCIENCE AND COMMERCE
TYBSC CS SEM V – CYBER FORENSIC

AccessData FTK Imager 3.4.3.3

File View Mode Help

Evidence Tree File List

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 20 10 00 60 3D 57
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
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 00 00 CE FF FF	Bt...yyyyyy
0050	FF FF FF FF FF FF FF-FF FF FF 00 00 FF FF FF FF	yyyyyyyyyyyy
0060	01 57 00 50 00 53 00 65-00 74 00 0F 00 CE 74 00	W-P-S-e-t
0070	69 00 FE 00 67 00 73 00-2E 00 00 00 64 00 61 00	ings-.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 0C 00 00 00	W-W-BW-W
00a0	42 47 00 75 00 69 00 64-00 00 00 0F 00 FF FF FF	BG-u-i-d
00b0	FF FF FF FF FF FF FF-FF FF FF 00 00 FF FF FF FF	yyyyyyyyyyyy
00c0	01 49 00 6E 00 64 00 65-00 78 00 0F 00 FF 65 00	I-n-d-e-x-y-e
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 00 10 41 57	INDEXE-1
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 Email/Internet Search, Cases, Text Styles, Table, Report, Gallery, Timeline, Disk, and Code. The main window has a tree view on the left under 'Cases' labeled 'History' with categories like Internet and Email, Internet Explorer, Mozilla, and Opera. To the right is a table view with columns: Name, URL, Host, User, Visit Count, and First Date. The table lists 25 entries, with entry 18 selected. Below the table is a detailed view of entry 18, showing 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, and History Path: Internet\Internet and Email\Active\Documents and Settings\PC User\Application Data\Mozilla\Firefox\Profiles\03fh4udv.default\history.dat. At the bottom, there is a status bar with the path 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:

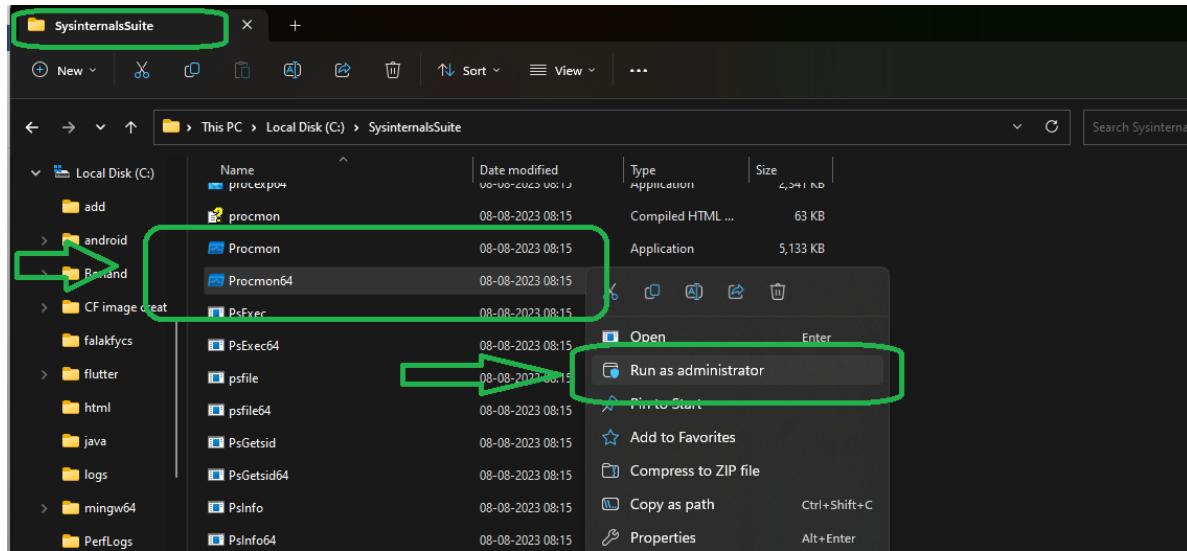
Analyze the memory dump of a running computer system.

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

Practical:

Open Process

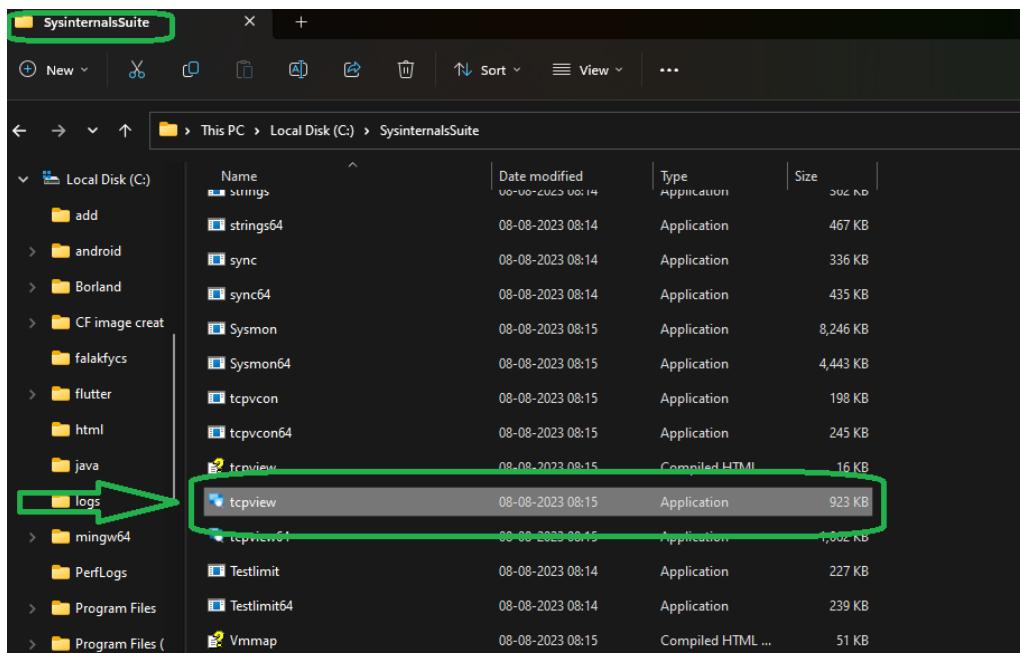
Go to Sysinternal Suite → ProcMon → Right Click on it and Open As Administrator



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: 926569, Le...
08:27:...	svchost.exe	1656	UDP Receive	f02:fb:5353->fe80:2050:4fce:b495:8...	SUCCESS	Length: 30, sequn...
08:27:...	chrome.exe	9724	UDP Receive	f02: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	QueryBasicInfor...	C:\Program Files\Windows Apps\Clipcha...	SUCCESS	CreationTime: 13-0...
08:27:...	Explorer.EXE	11808	ReadFile	C:\Windows\System32\Taskbar.dll	SUCCESS	Offset: 2406400, L...
08:27:...	svchost.exe	2644	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	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	Desired Access: R...
08:27:...	Explorer.EXE	11808	ReadFile	C:\Windows\System32\Taskbar.dll	SUCCESS	Offset: 2718208, L...
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\lsass.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\lsass.dll	SUCCESS	Offset: 1523712, L...
08:27:...	Explorer.EXE	11808	ReadFile	C:\Windows\System32\BCP47mm.dll	SUCCESS	Offset: 155648, Le...
08:27:...	Explorer.EXE	11808	ReadFile	C:\Windows\System32\Taskbar.dll	SUCCESS	Offset: 2512896, L...
08:27:...	svchost.exe	2644	ReadFile	C:\Windows\System32\Windows.State...	SUCCESS	Offset: 6414336, L...
08:27:...	lsass.exe	1020	ReadFile	C:\Windows\System32\lsass.dll	SUCCESS	Offset: 1519616, 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\MicrosoftWin...	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	Desired Access: R...
08:27:...	Explorer.EXE	11808	RegQueryKey	HKLM	SUCCESS	Exclusive: False, O...
08:27:...	Explorer.EXE	11808	RegOpenKey	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	Query: Handle Tag...

Network Connections

Go to SysinternalSuite → TCPview



RIZVI COLLEGE OF ARTS, SCIENCE AND COMMERCE
TYBSC CS SEM V – CYBER FORENSIC

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

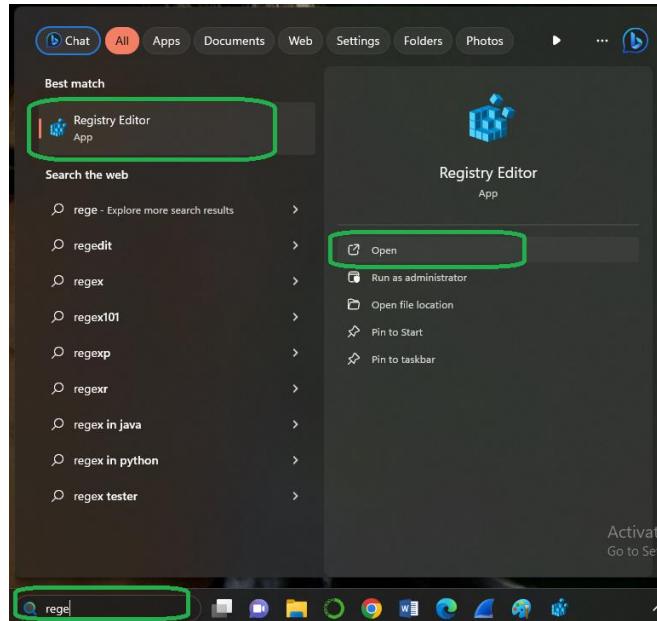
File Edit View Process Connection Options Help

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

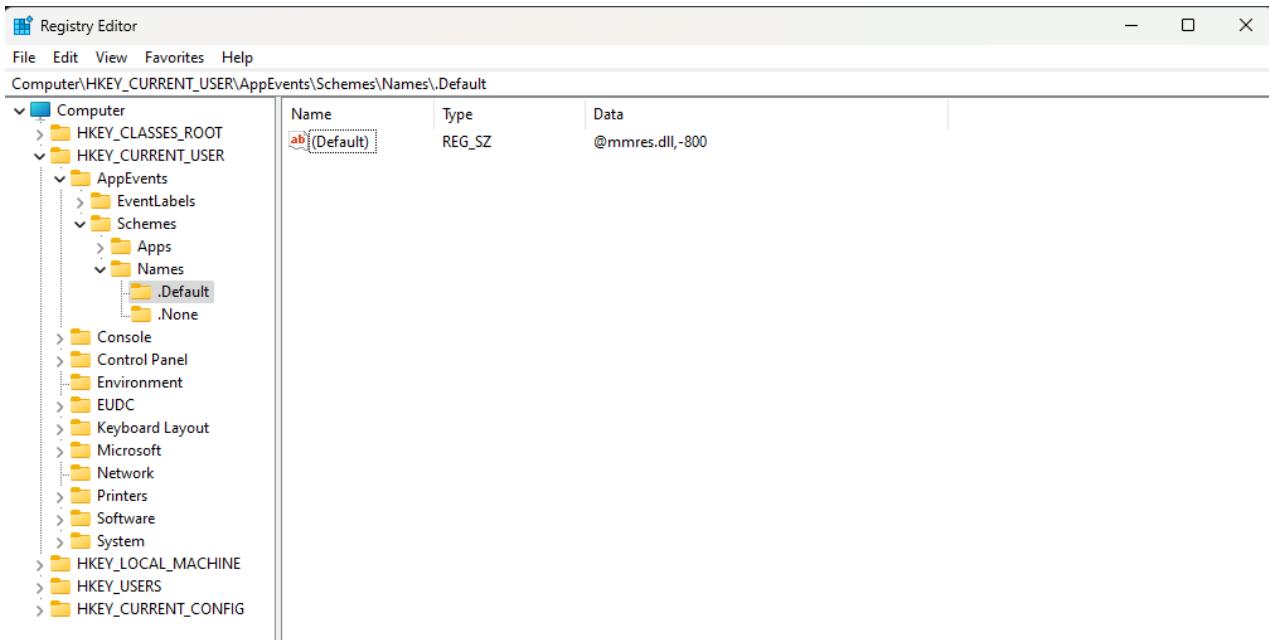
Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Time	Module Name
svchost.exe	1664	UDP		0.0.0.0	65053	*		05-09-2023 09:26:20	Dnscache
svchost.exe	10812	UDPV6		fe80:4a02:628:aa06:18eb	53	*		05-09-2023 08:46:55	SharedAccess
svchost.exe	1524	UDPV6		::	123	*		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
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



PRACTICAL NO. 4

Aim:

Capturing and analyzing network packets using Wireshark (Fundamentals):

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

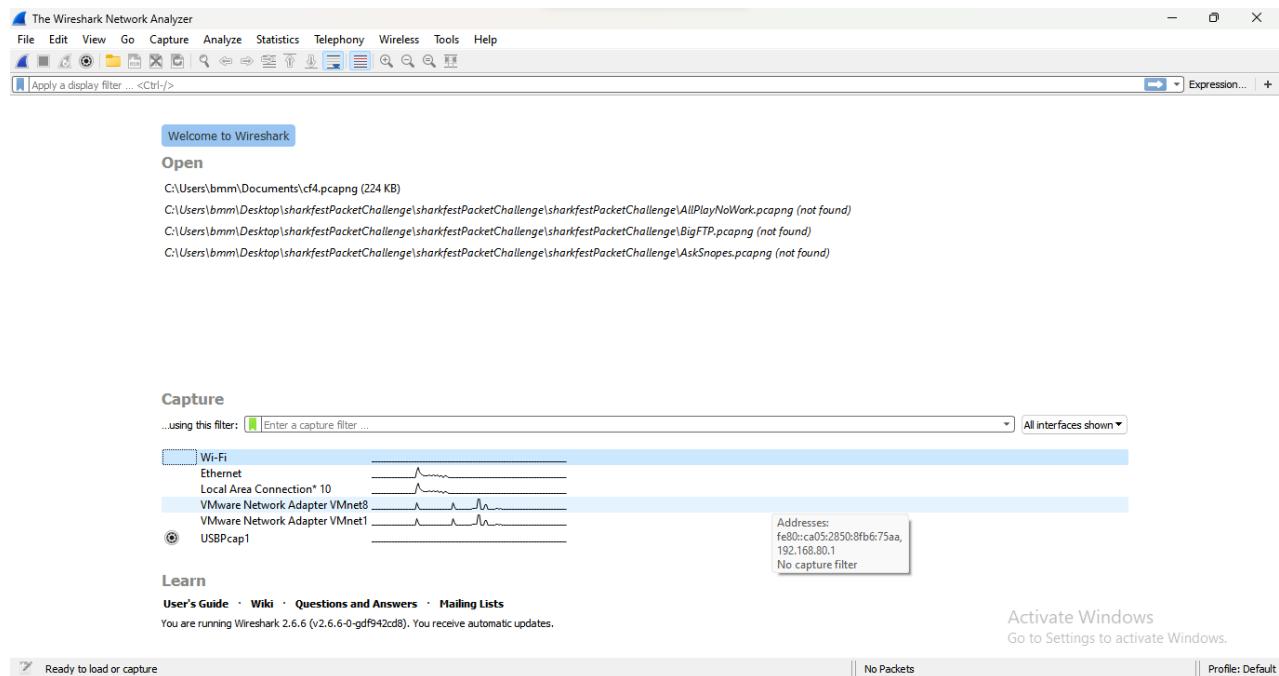
Practical:

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

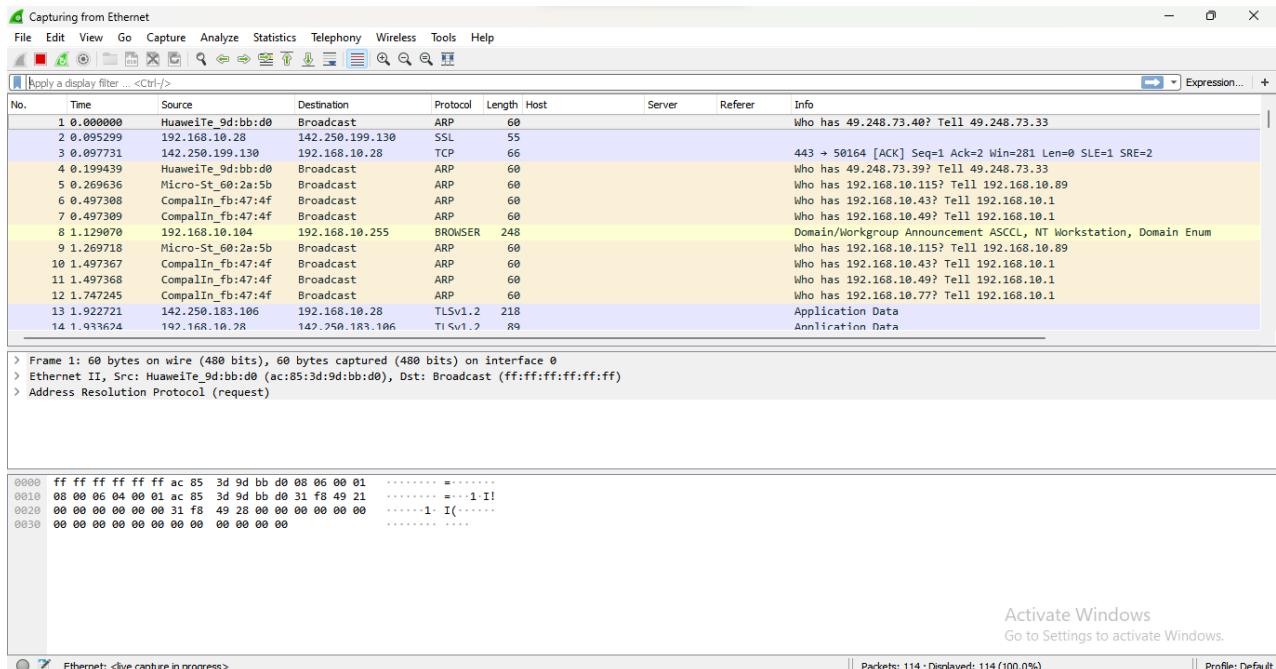
We are using **WireShark**, an application used to identify, capture and analyze the network traffics.



Capturing Network

We are now going to capture a network of Ethernet

RIZVI COLLEGE OF ARTS, SCIENCE AND COMMERCE
TYBSC CS SEM V – CYBER FORENSIC



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

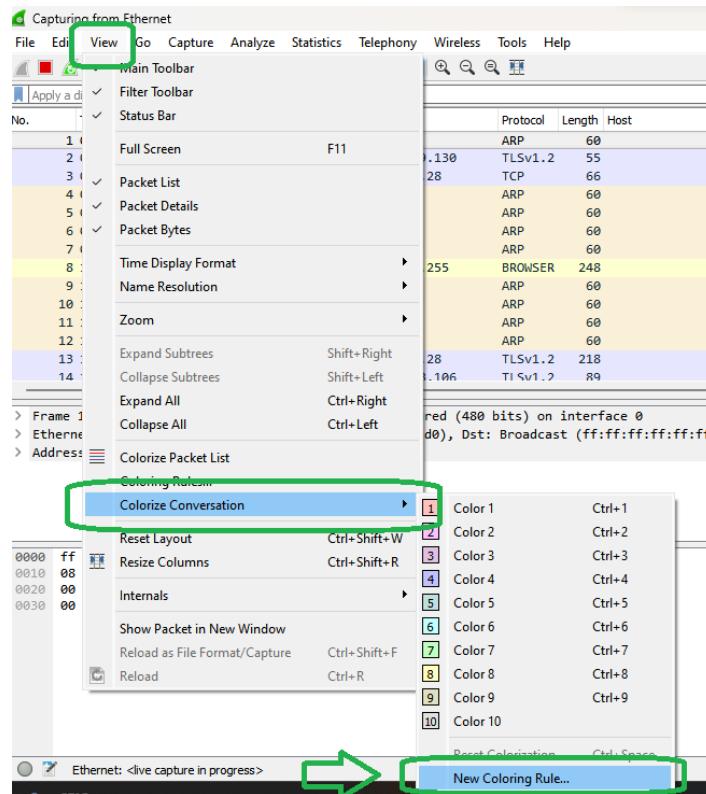
Color Coding Different packets are seen highlighted in various different colors. This is Wireshark's way of displaying traffic to help you easily identify the types of it.

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 Conversations → 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 && !(ip.proto == 17 && ip.ttl == 1)) && !(ip.dst == 224.0.0.251 && ip.ttl == 1 && !(ip.proto == 17 && ip.ttl == 1))
Checksum Errors	eth.fcs.status=="Bad" ip.checksum.status=="Bad" tcp.checksum.status=="Bad" udp.checksum.status=="Bad" sctp.checksum.status=="Bad"
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 network packets below. The packet list includes columns for No., Time, Source, Destination, Protocol, Length, Host, Server, Referer, and Info.

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' field in the display filter bar. A green arrow points from this field to the list of captured network packets below. The packet list includes columns for No., Time, Source, Destination, Protocol, Length, Host, Server, Referer, and Info.

No.	Time	Source	Destination	Protocol	Length	Host	Server	Referer	Info
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] Seq=1 Ack=2 Win=281 Len=0 SLE=1 SRE=2
8	1.129070	192.168.10.104	192.168.10.255	BROWSER	248				Domain/Workgroup Announcement ASCLL, NT Workstation, Domain
13	1.922721	142.250.183.106	192.168.10.28	TLSv1.2	218				Application Data
14	1.933624	192.168.10.28	142.250.183.106	TLSv1.2	89				Application Data
15	1.933906	192.168.10.28	142.250.183.106	TLSv1.2	89				Application Data
16	1.935944	142.250.183.106	192.168.10.28	TCP	60				443 → 50230 [ACK] Seq=165 Ack=36 Win=351 Len=0
17	1.935946	142.250.183.106	192.168.10.28	TCP	60				443 → 50230 [ACK] Seq=165 Ack=71 Win=351 Len=0
18	2.156406	192.168.10.28	142.250.183.174	TLSv1.2	966				Application Data
19	2.156587	192.168.10.28	142.250.183.174	TLSv1.2	215				Application Data
20	2.158716	142.250.183.174	192.168.10.28	TCP	60				443 → 50202 [ACK] Seq=1 Ack=913 Win=593 Len=0
21	2.158717	142.250.183.174	192.168.10.28	TCP	60				443 → 50202 [ACK] Seq=1 Ack=1074 Win=604 Len=0
22	2.227919	192.168.10.28	216.239.34.181	TLSv1.2	55				
23	2.730843	216.239.34.1R1	192.168.10.28	TCP	66				443 → 50224 [ACK] Seq=1 Ack=2 Win=271 Len=0 SLE=1 SRF=2

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

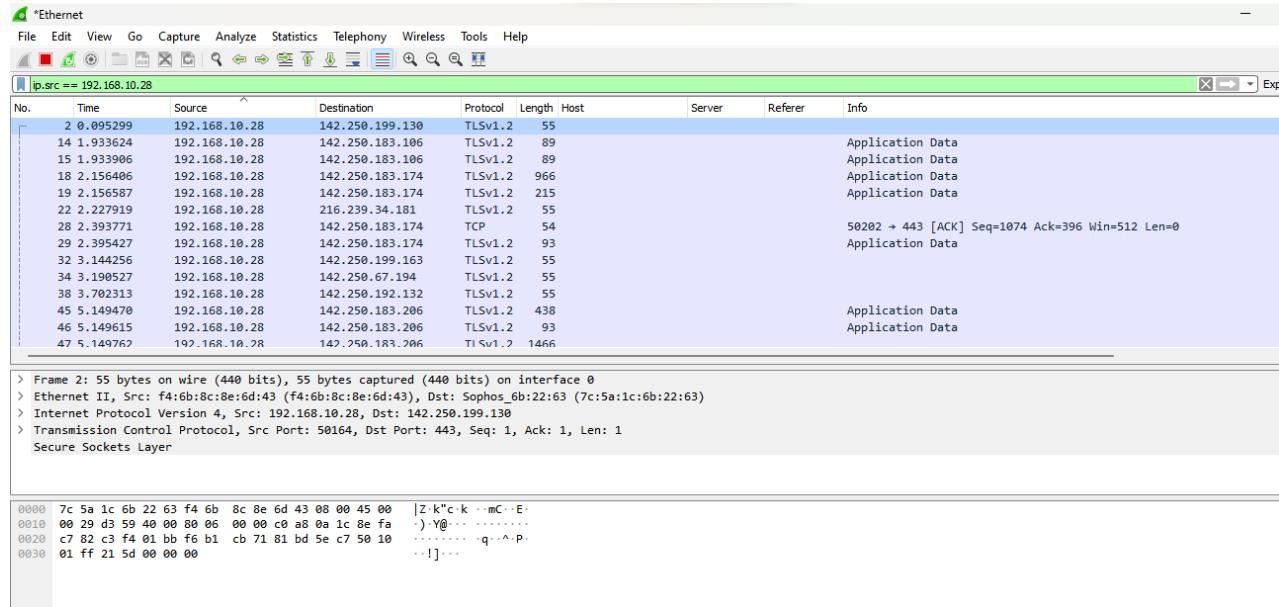
```

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 |.....·q-^·p-
0030  01 ff 21 5d 00 00 00 00 ..!]...

```

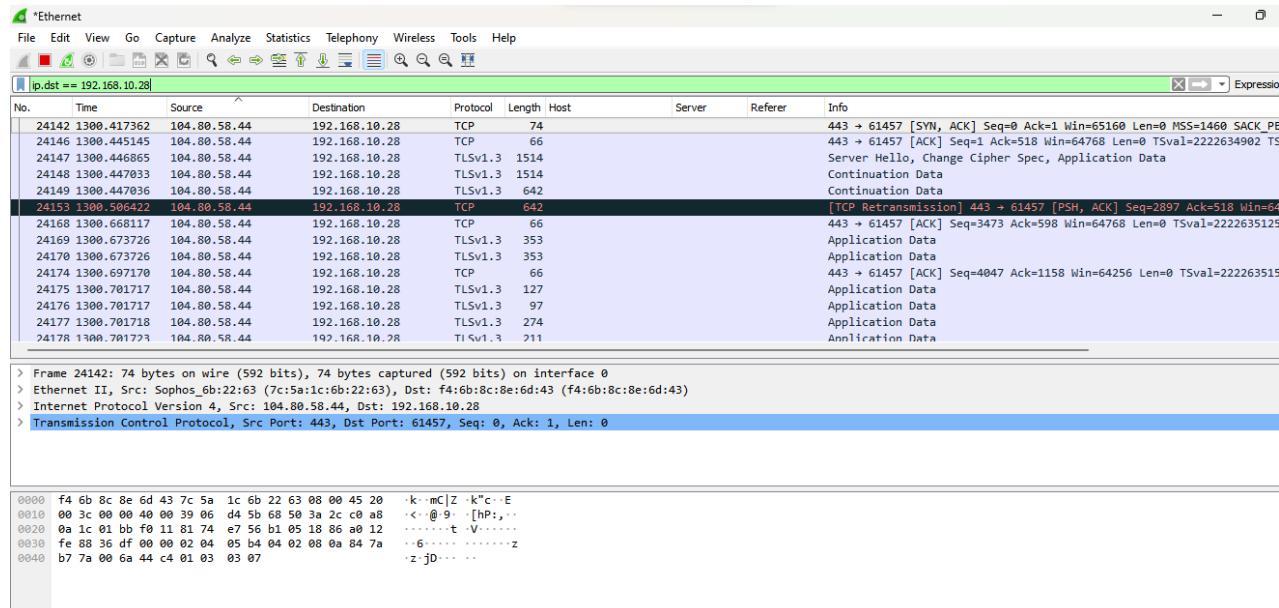
2. Display packets which are coming from specific IP-address

➤ ip.src == 192.168.10.28



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

➤ ip.dst == 192.168.10.28



4. Display packets which are using http protocol

➤ http

No.	Source	Destination	Protocol	Length	Host	Server	Referer	Info
13394	707.487777	15.207.161.196	192.168.10.28	HTTP	475			HTTP/1.1 200 OK (application/text)
13736	717.161381	15.207.161.196	192.168.10.28	HTTP	467			HTTP/1.1 200 OK (application/text)
14476	766.786676	15.207.161.196	192.168.10.28	HTTP	531			HTTP/1.1 200 OK (application/text)
18350	1047.517522	15.207.161.196	192.168.10.28	HTTP	531			HTTP/1.1 200 OK (application/text)
18477	1048.661494	15.207.161.196	192.168.10.28	HTTP	475			HTTP/1.1 200 OK (application/text)
18567	1050.070626	15.207.161.196	192.168.10.28	HTTP	487			HTTP/1.1 200 OK (application/text)
19534	1104.939537	15.207.161.196	192.168.10.28	HTTP	475			HTTP/1.1 200 OK (application/text)
22078	1281.576883	15.207.161.196	192.168.10.28	HTTP	507			HTTP/1.1 200 OK (application/text)
23760	1294.837652	15.207.161.196	192.168.10.28	HTTP	467			HTTP/1.1 200 OK (application/text)
23878	1296.327264	15.207.161.196	192.168.10.28	HTTP	443			HTTP/1.1 200 OK (application/text)
23900	1296.495246	15.207.161.196	192.168.10.28	HTTP	467			HTTP/1.1 200 OK (application/text)
23911	1296.675119	15.207.161.196	192.168.10.28	HTTP	435			HTTP/1.1 200 OK (application/text)
24134	1300.398024	15.207.161.196	192.168.10.28	HTTP	595			HTTP/1.1 200 OK (application/text)
25160	1377.298821	15.207.161.196	192.168.10.28	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:e6:d4:3 (f4:6b:8c:e6:d4:3)
> 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 09 0f cf a1 c4 c0 a8 -Eq @...-
0020  00 1c 1f 98 c4 df e6 e2 7d dc 80 72 84 5b 50 18 .....}r[P-
0030  00 7e 89 a9 00 00 48 54 54 50 2f 31 2e 31 20 32 .....,HT TP/1.1.2
0040  30 30 20 4f 4b 0d 0a 44 61 74 65 3a 20 4d 6f 6e 00 OK-D ate: Mon
0050  20 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

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:e6:d4:3 (f4:6b:8c:e6:d4:3)
> 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"e-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 90 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 7a 65 20 e/URLCat egorize
0060  48 54 54 20 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-ww 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 Wi
Go to Settings

RIZVI COLLEGE OF ARTS, SCIENCE AND COMMERCE
TYBSC CS SEM V – CYBER FORENSIC

6. Display packets which are using TCP protocol

➤ tcp

No.	Time	Source	Destination	Protocol	Length	Host	Server	Referer	Info
24102	1300.156976	192.168.10.28	142.250.183.174	TLSv1.2	424				Ignored Unknown Record
24103	1300.157030	192.168.10.28	142.250.183.174	TLSv1.2	215				Application Data
24108	1300.168420	192.168.10.28	192.168.10.1	TLSv1.3	77				Application Data
24110	1300.212772	192.168.10.28	192.168.10.1	TCP	54				62128 → 57216 [ACK] Seq=21523 Ack=7347 Win=1049088
24112	1300.216932	192.168.10.28	192.168.10.1	TLSv1.3	177				Application Data
24114	1300.227867	192.168.10.28	142.250.67.227	TCP	55				[TCP Keep-Alive] 50244 → 443 [ACK] Seq=37799 Ack=4588
24117	1300.278274	192.168.10.28	192.168.10.1	TLSv1.3	77				Application Data
24119	1300.336390	192.168.10.28	192.168.10.1	TCP	54				62128 → 57216 [ACK] Seq=21669 Ack=7827 Win=1048576
24120	1300.339310	192.168.10.28	192.168.10.1	TLSv1.3	177				Application Data
24125	1300.384604	192.168.10.28	142.250.183.174	TCP	54				50202 → 443 [ACK] Seq=182074 Ack=90638 Win=511 Len=4
24128	1300.385616	192.168.10.28	142.250.183.174	TCP	54				50202 → 443 [ACK] Seq=182074 Ack=90776 Win=510 Len=6
24129	1300.386516	192.168.10.28	142.250.183.174	TLSv1.2	93				Application Data
24132	1300.391412	192.168.10.28	15.207.161.196	HTTP	403	prourl.itsecure...			POST /URLCategorizerService/URLCategorize HTTP/1.1
24133	1300.397512	192.168.10.28	104.80.58.44	TCP	74				61457 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK

> Frame 24132: 403 bytes on wire (3224 bits), 403 bytes captured (3224 bits) on interface 0
> Ethernet II, Src: f4:b6:8c:8e:6d:43 (f4:b6:8c: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

```
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 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 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 7d 66 6f 72 6d 2d 75  ion/x-w 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 66 74 3a 20 6a 73 6f 6e 68 74 74 0d  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 Windo
Go to Settings to ac

7. Display packets having no error connecting to server

➤ http.response.code==200

No.	Time	Source	Destination	Protocol	Length	Host	Server	Referer	Info
13278	703.878092	15.207.161.196	192.168.10.28	HTTP	487				HTTP/1.1 200 OK (application/text)
13394	707.487777	15.207.161.196	192.168.10.28	HTTP	475				HTTP/1.1 200 OK (application/text)
13736	717.161381	15.207.161.196	192.168.10.28	HTTP	467				HTTP/1.1 200 OK (application/text)
14476	766.786676	15.207.161.196	192.168.10.28	HTTP	531				HTTP/1.1 200 OK (application/text)
18356	1047.517522	15.207.161.196	192.168.10.28	HTTP	531				HTTP/1.1 200 OK (application/text)
18477	1048.661494	15.207.161.196	192.168.10.28	HTTP	475				HTTP/1.1 200 OK (application/text)
18567	1050.070626	15.207.161.196	192.168.10.28	HTTP	487				HTTP/1.1 200 OK (application/text)
19534	1104.939537	15.207.161.196	192.168.10.28	HTTP	475				HTTP/1.1 200 OK (application/text)
22078	1201.576883	15.207.161.196	192.168.10.28	HTTP	507				HTTP/1.1 200 OK (application/text)
23760	1294.837652	15.207.161.196	192.168.10.28	HTTP	467				HTTP/1.1 200 OK (application/text)
23878	1296.327264	15.207.161.196	192.168.10.28	HTTP	443				HTTP/1.1 200 OK (application/text)
23900	1296.495246	15.207.161.196	192.168.10.28	HTTP	467				HTTP/1.1 200 OK (application/text)
23911	1296.675119	15.207.161.196	192.168.10.28	HTTP	435				HTTP/1.1 200 OK (application/text)
24134	1300.398024	15.207.161.196	192.168.10.28	HTTP	595				HTTP/1.1 200 OK (application/text)

> 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:b6:8c:8e:6d:43 (f4:b6:8c: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

```
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 0f 02 06 99 7a 0f cf a1 c4 c0 a8  ..q @... z...
0020  0a 1c 1f 98 c4 df e6 e2 7c 5f 80 72 82 fe 50 18  .....|_r-P-
0030  00 7a d9 9b 00 08 48 54 50 2f 31 2e 31 20 32  z....TP/1.1 2
0040  30 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 32 33 20 30 33 , 04 Sep 2023 03
0060  3a 34 31 3a 35 32 20 47 4d 0d 0a 43 6f 6e 74 :41:52 G MT-Cont
0070  65 6e 74 2d 54 79 70 65 3a 20 61 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 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										
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 [TCP Retransmission] 80 → 61438 [ACK] Seq=253 Ack=192	
18652	1056.072862	129.227.29.114	192.168.10.28	TCP	60				80 → 61445 [SYN, ACK] Seq=0 Ack=1	
18656	1056.142564	129.227.29.114	192.168.10.28	TCP	60				80 → 61445 [ACK] Seq=1 Ack=191 Wi-Fi	
21848	1190.915180	129.227.29.114	192.168.10.28	TCP	66				HTTP/1.1 204 No Content	
21853	1190.908378	129.227.29.114	192.168.10.28	TCP	60				80 → 61445 [ACK] Seq=1 Ack=191 Wi-Fi	
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-Fi	
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	1206.688350	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 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 00 00  ..X.... ....

```

*Ethernet										
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..E..k..mC|...
0010  04 fe 2b e8 40 00 3e 11 f1 fd c0 a8 0a 1c 8a fa  .+ @>.....
0020  c0 4a ef ba 01 bb 04 ea 3c 43 c7 00 00 00 01 08  .J.....<C.....
0030  a3 5d e9 4f 89 51 a2 9c 00 00 44 d0 a8 7d f2 71  .] -Q ..D ..}q
0040  c8 fb 80 89 78 01 66 4a 67 c4 9a b2 71 f3 78 7a  ...x..fJ g ..q ..xz
0050  07 98 9d bf 63 f4 6b 49 ed f1 c6 04 3c 9e 23 d5  ...c ..kI ..<#.
0060  bc 0c 64 47 21 35 c1 d7 26 a6 47 29 2f 0a 32 07  .dG15 ..& G)/.2.
0070  27 85 7c 22 a6 26 5d cf 94 27 a0 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  ..^..% ..[1....
00a0  d7 86 9e b2 52 3d 33 7f 9f 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:

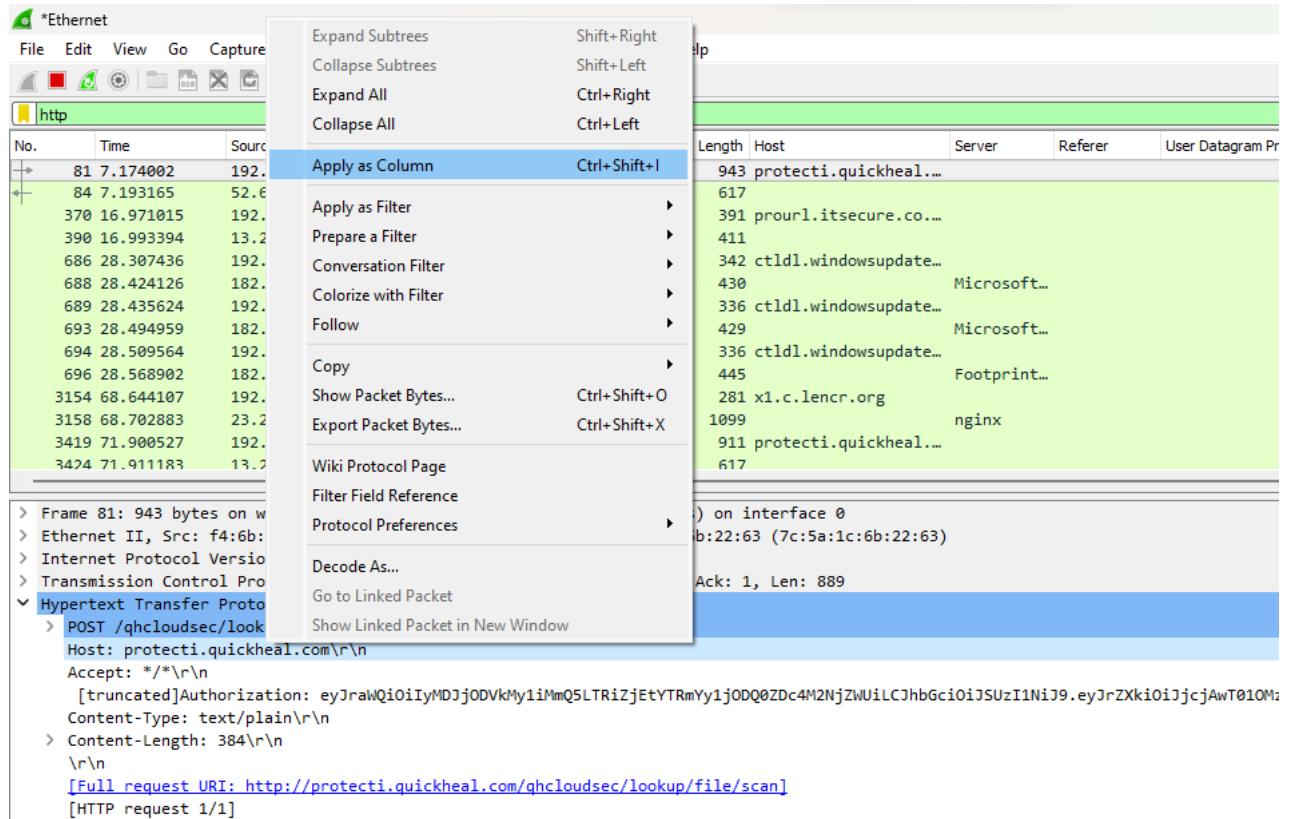
Analyze the packets provided in lab and solve the questions using Wireshark

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

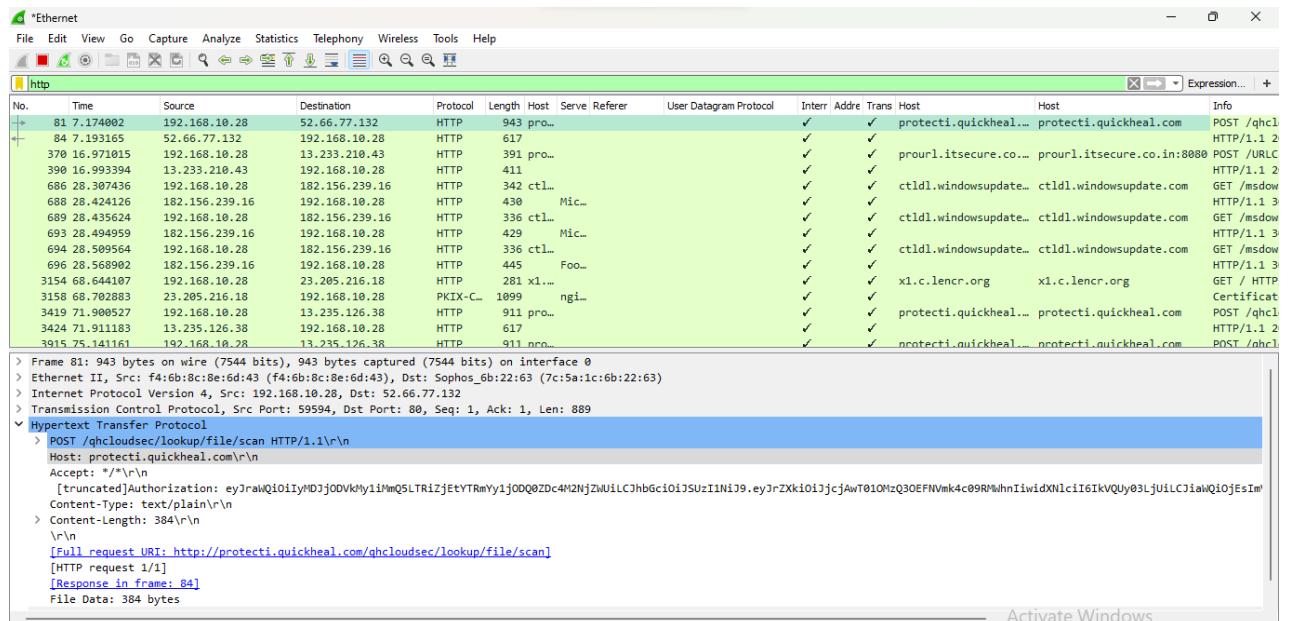
Analysis –

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

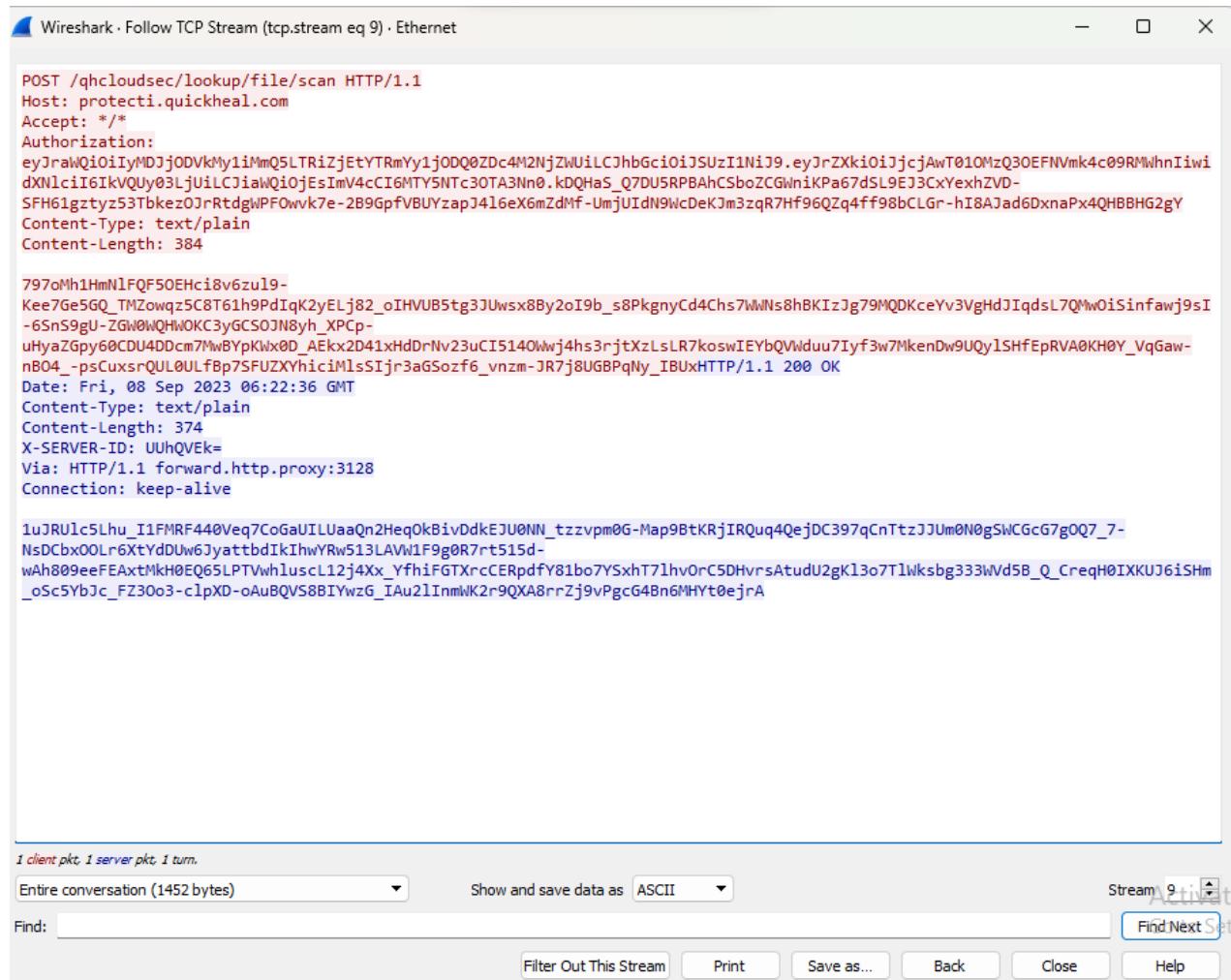
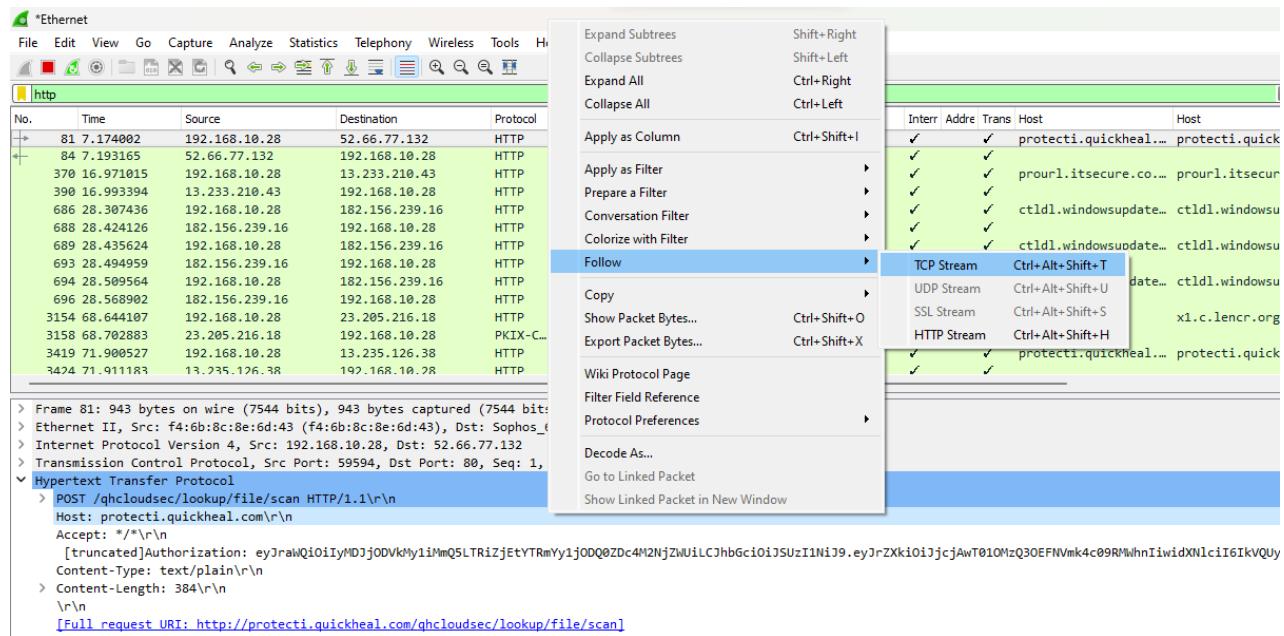
First find the requests from HTTP and click on and request then on the lower table of details Select on HyperText Transfer Protocol → Host and Right Click on that and Select Apply as Filter



Now we can see the Host



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



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	Interf	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
488	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	Interf	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
488	30.942066	192.168.10.52	239.255.255.250	SSDP	217	239.25...			✓	✓					239.255.255... M-SEARCH * HTTP/1.1

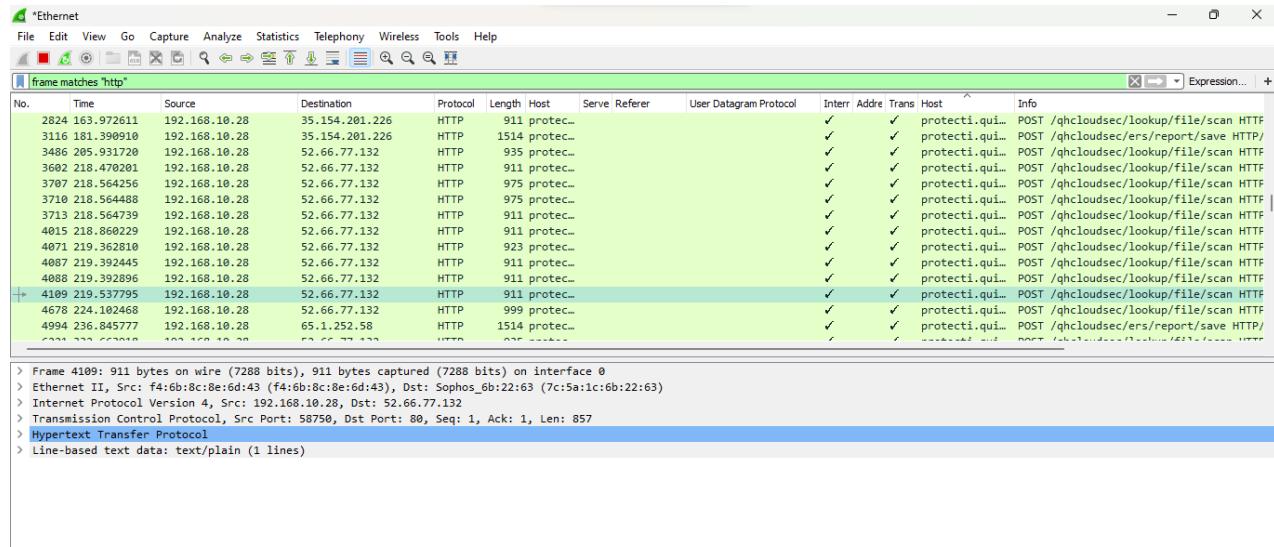
```
> Frame 213: 217 bytes on wire (1736 bits), 217 bytes captured (1736 bits) on interface 0
> Ethernet II, Src: f4:6b:8c:0e:6d:43 (f4:6b:8c:0e:6d:43), Dst: IPv4mcast_7ff:ff:fa (01:00:5e:7f:ff:fa)
> Internet Protocol Version 4, Src: 192.168.10.28, Dst: 239.255.255.250
> User Datagram Protocol, Src Port: 62928, Dst Port: 1900
> Simple Service Discovery Protocol
  > M-SEARCH * HTTP/1.1\r\n
    HOST: 239.255.255.250:1900\r\n
    MAN: "ssdp:discover"\r\n
    User-Agent: Microsoft Edge/116.0.1938.76 Windows\r\n
  \r\n
  [Full request URI: http://239.255.255.250:1900*]
  [HTTP request 1/4]
  [Next request in frame: 225]
```

Activate Windows

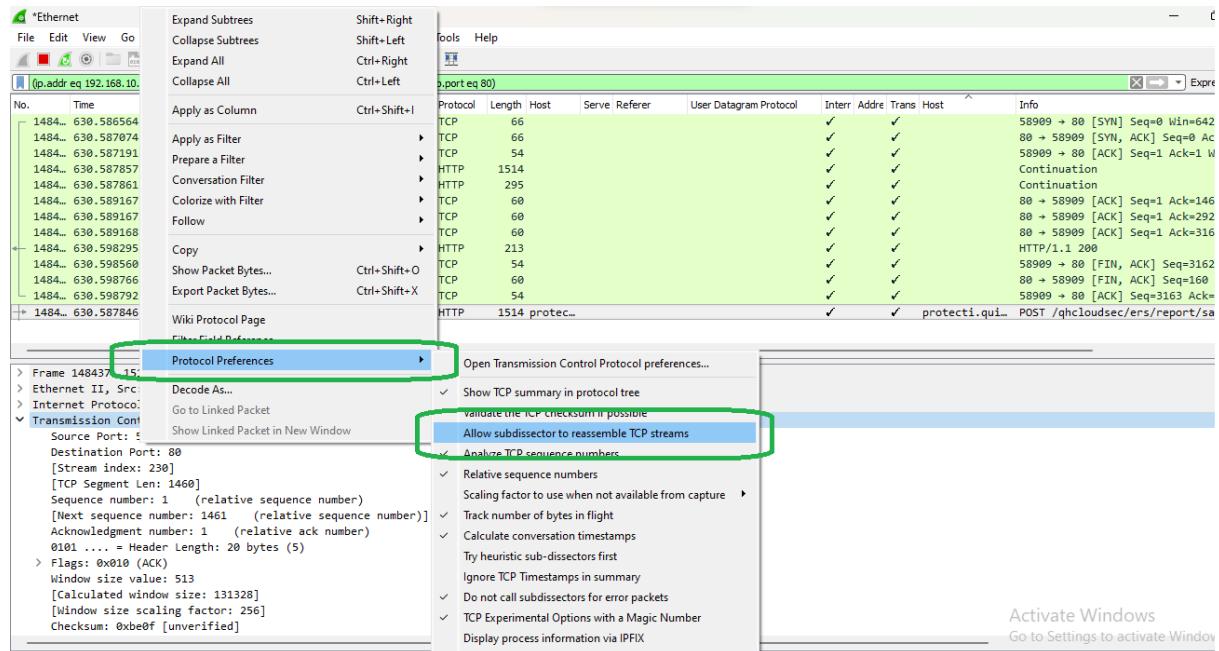
3. According to http, what data will TCP show?

Analysis –

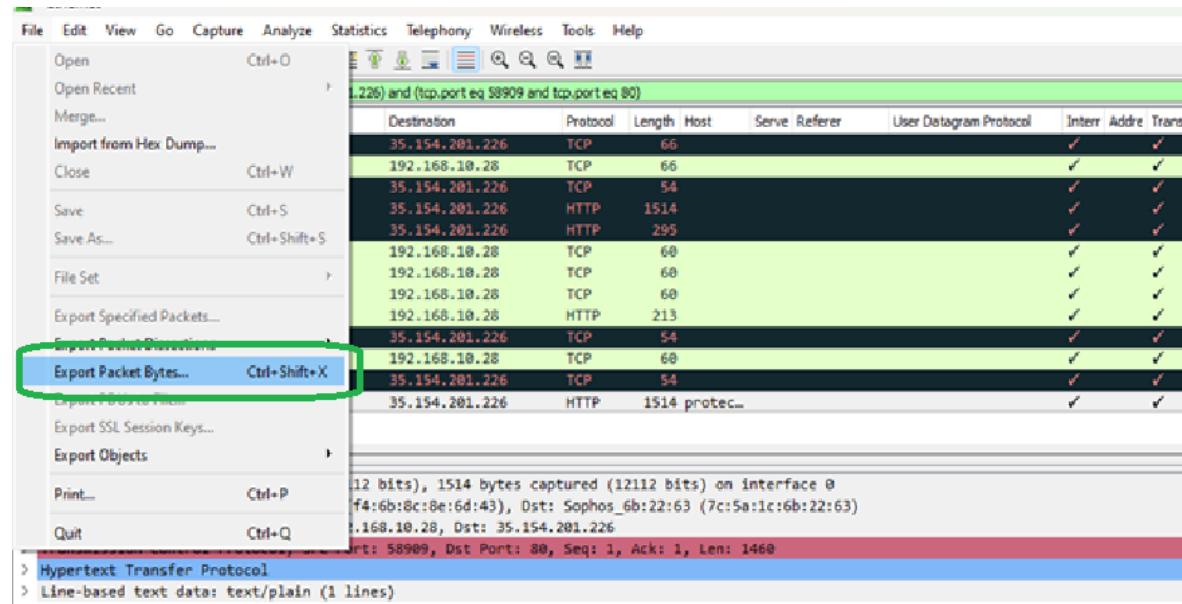
As we did in the last challenge, we will **apply a regular express filter** for the Google keyword. **Apply frame matched “http”.**



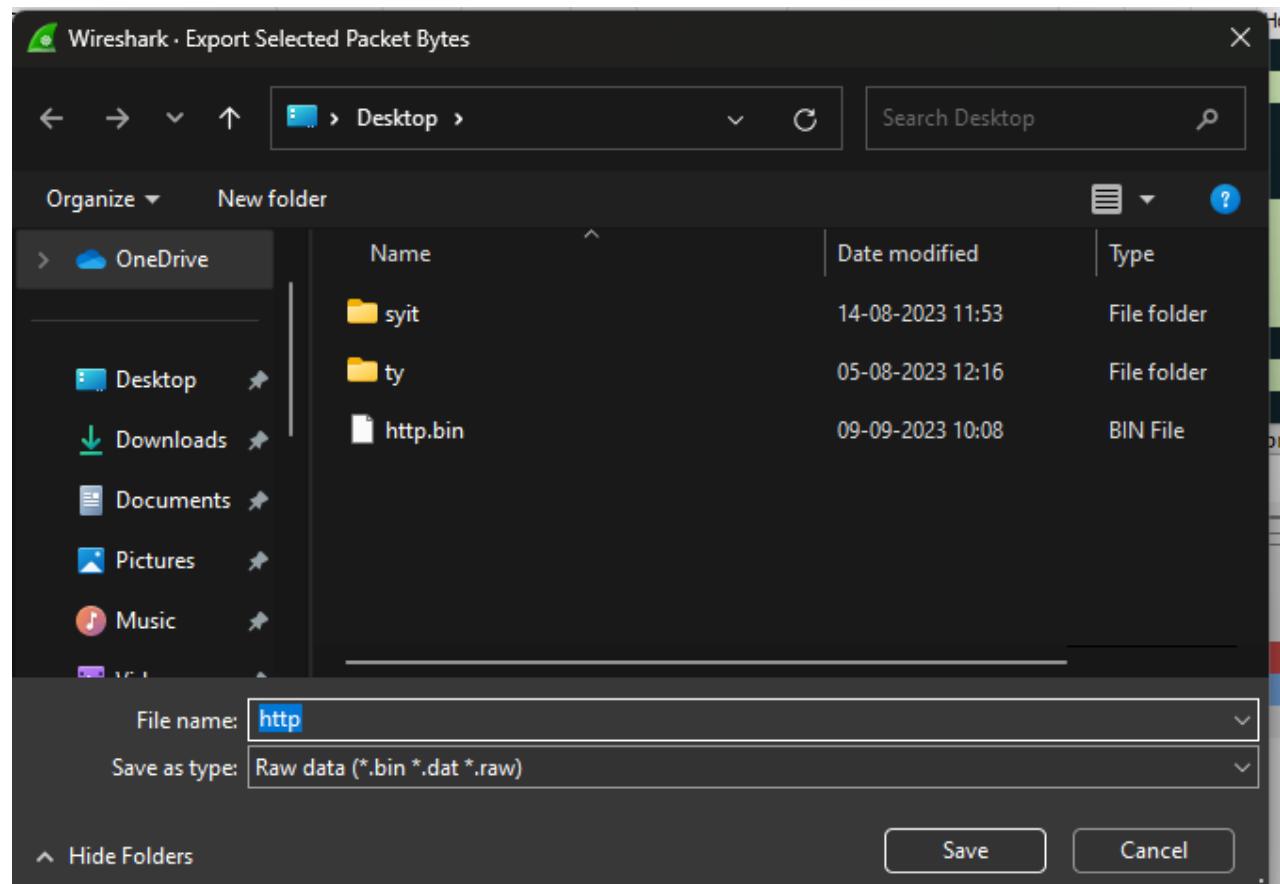
Select the packet and expand the Hypertext Transfer Protocol tab right click on Transmission Control Protocol Go to Protocol Preferences and check Allow subdissector to reassemble TCP stream with HTTP spanning bodies.



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



Click on save all.

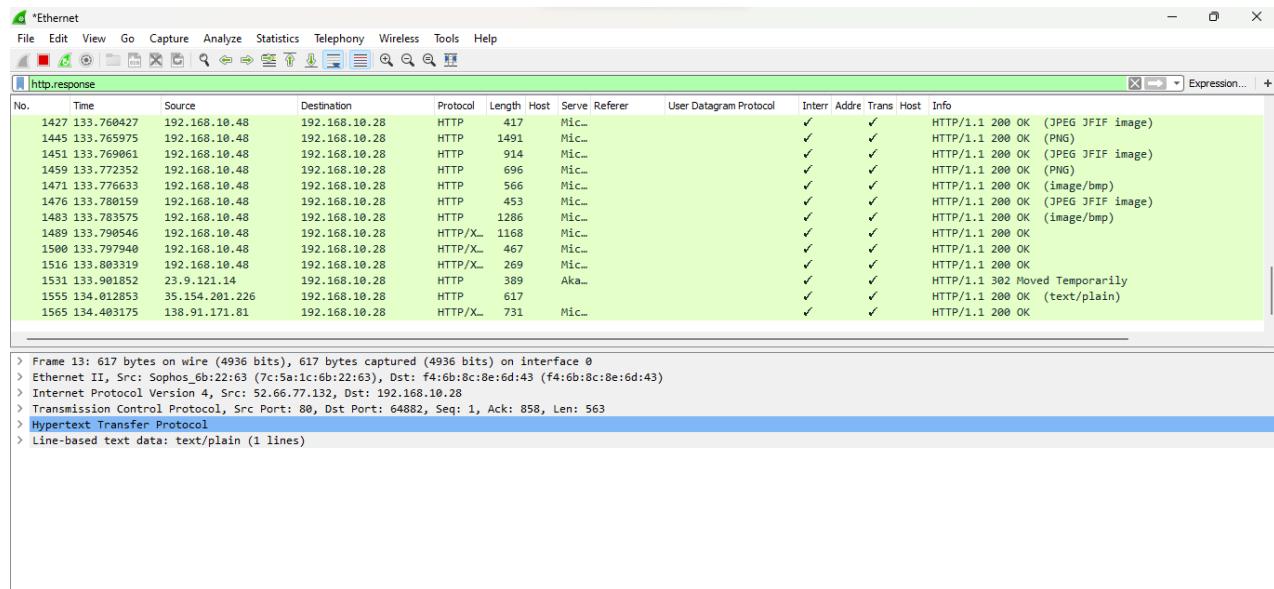


After checking it seems only the packets transfer were to connect the machine to the internet.

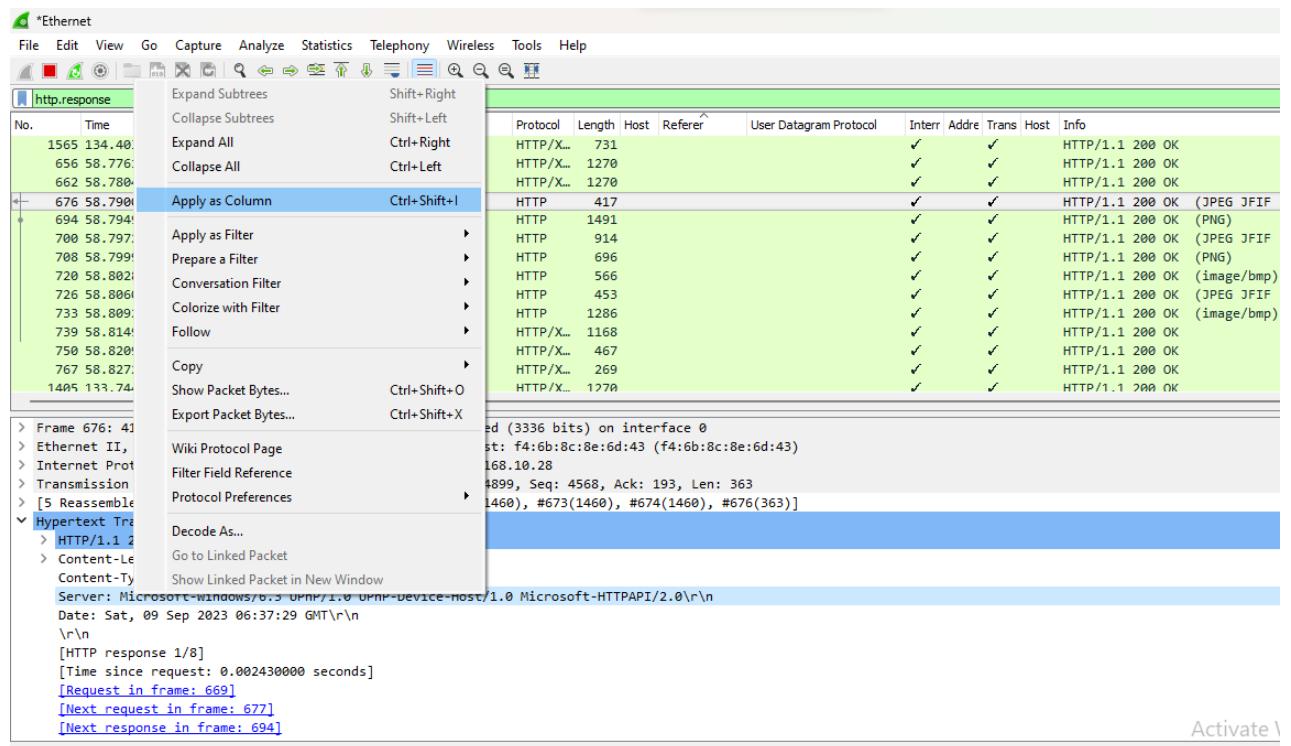
4. How many web servers are running Microsoft?

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.

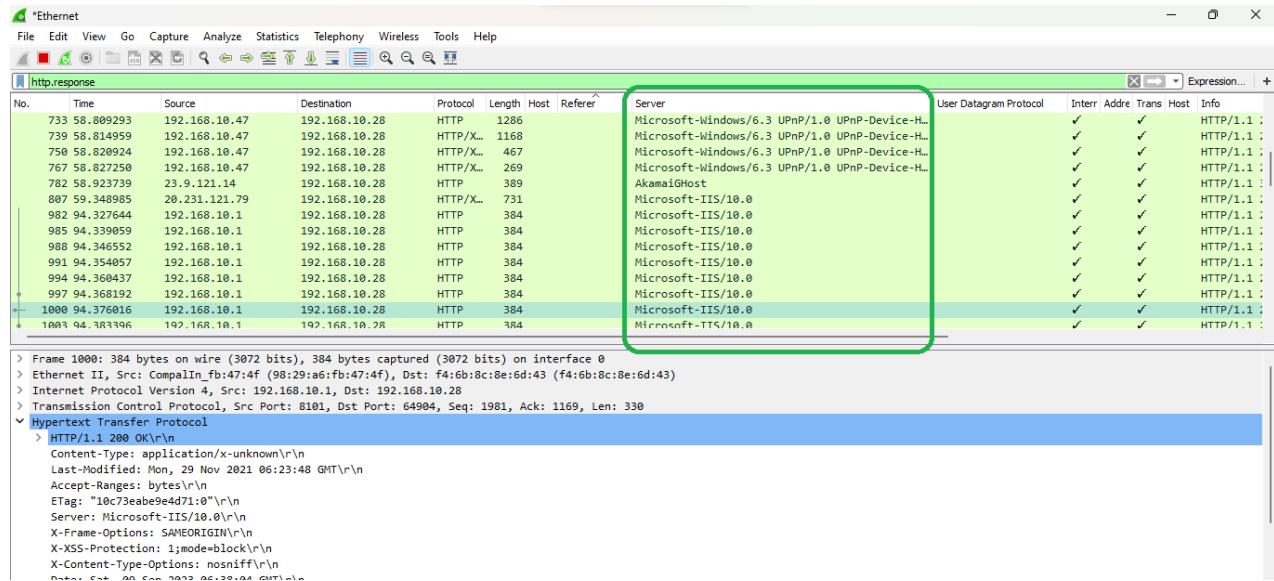


Now we will set the server header as column select any packet and right click on it then select Apply as Column.

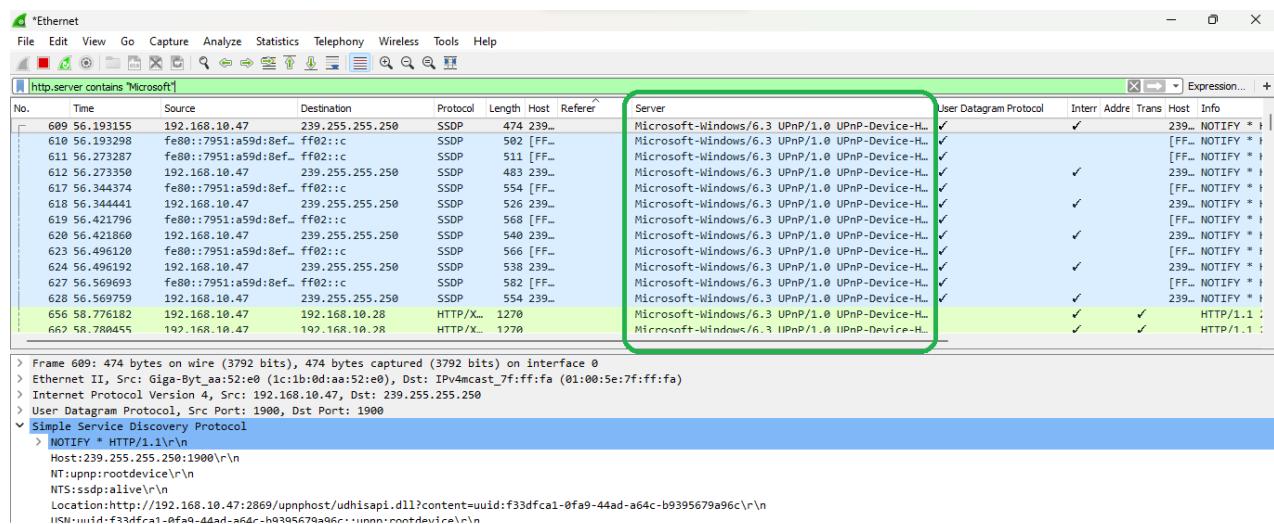


RIZVI COLLEGE OF ARTS, SCIENCE AND COMMERCE
TYBSC CS SEM V – CYBER FORENSIC

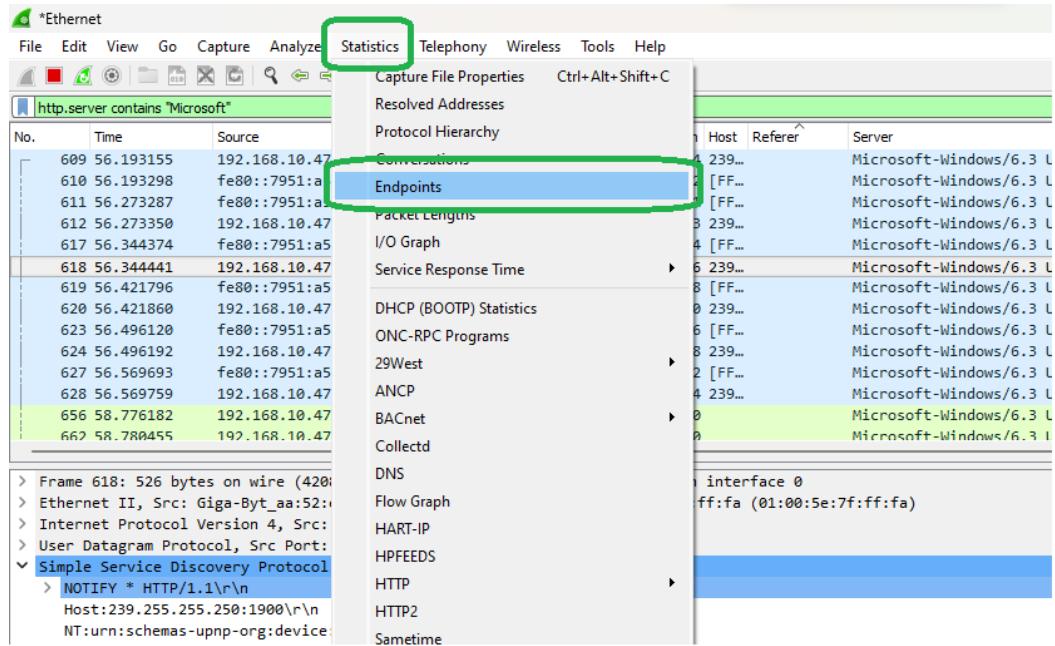
Now can see the server column where all server name is showing.



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



After applying filter [Go to Statistics → Endpoints](#)



It will show all connections.

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.

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

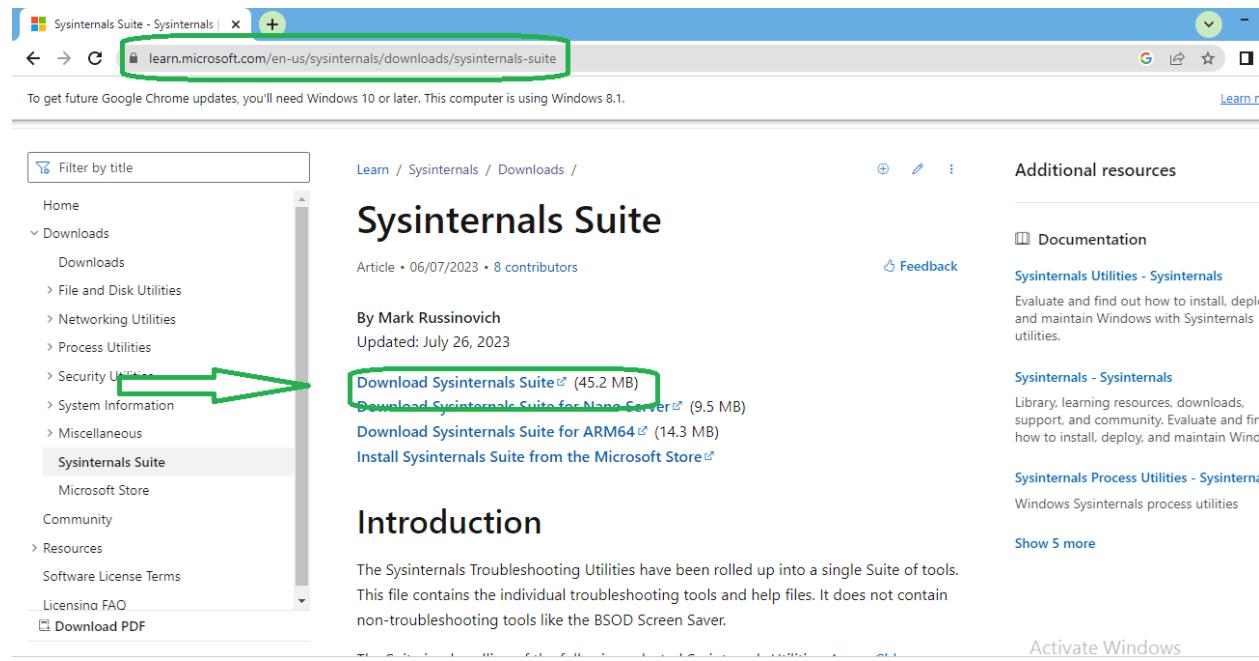
Google → sysinternal tools

If Available Then Skip the Installation Part

Let's Install the Sysinternal Suite for Windows

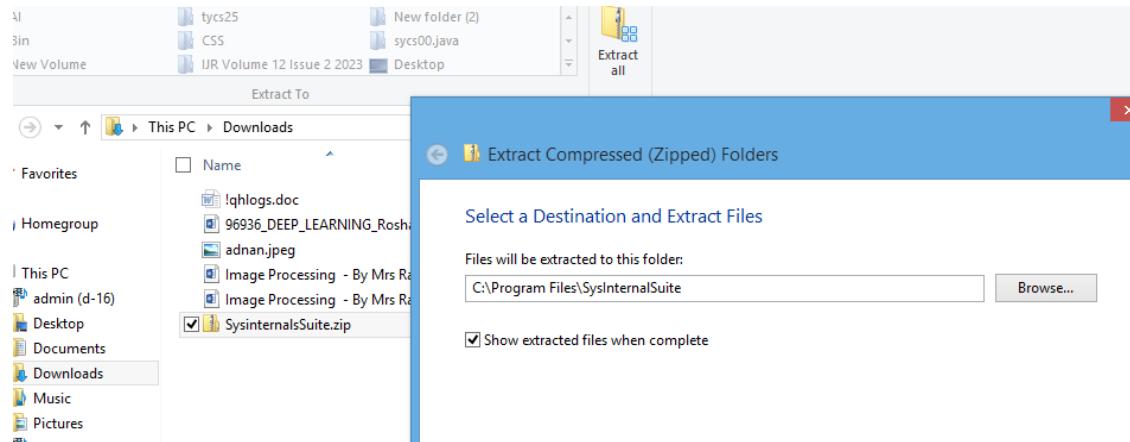
We can download the zip file from the given link

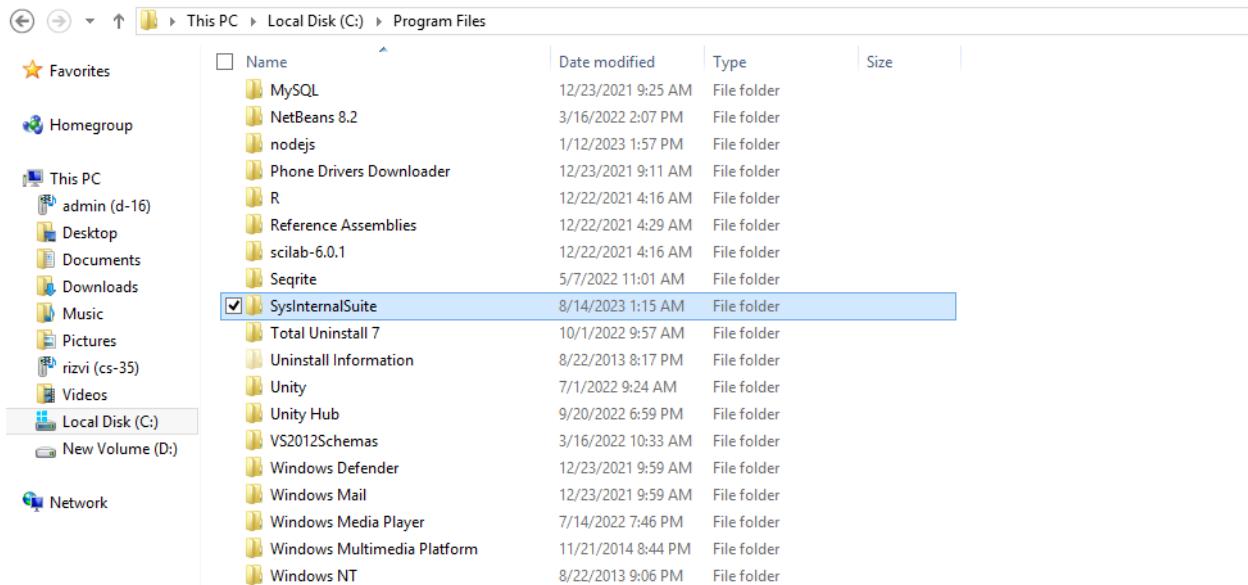
<https://learn.microsoft.com/en-us/sysinternals/downloads/sysinternals-suite>



The screenshot shows a web browser window with the URL learn.microsoft.com/en-us/sysinternals/downloads/sysinternals-suite. The page displays the 'Sysinternals Suite' article by Mark Russinovich, updated on July 26, 2023. It features several download links: 'Download Sysinternals Suite' (45.2 MB), 'Download Sysinternals Suite for Nano Server' (9.5 MB), 'Download Sysinternals Suite for ARM64' (14.3 MB), and 'Install Sysinternals Suite from the Microsoft Store'. The left sidebar has a 'Downloads' section with various utility categories, and a green arrow points from the 'Downloads' link to the 'Download Sysinternals Suite' link.

Then Extract the file to the desired directory



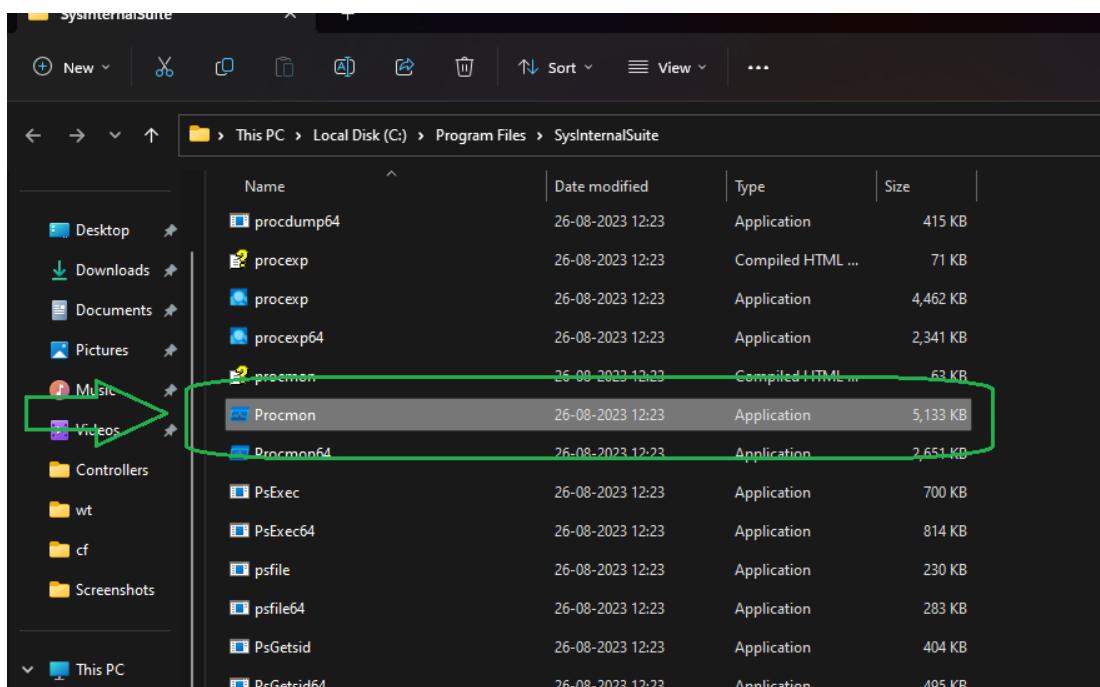


Monitor Live Processes

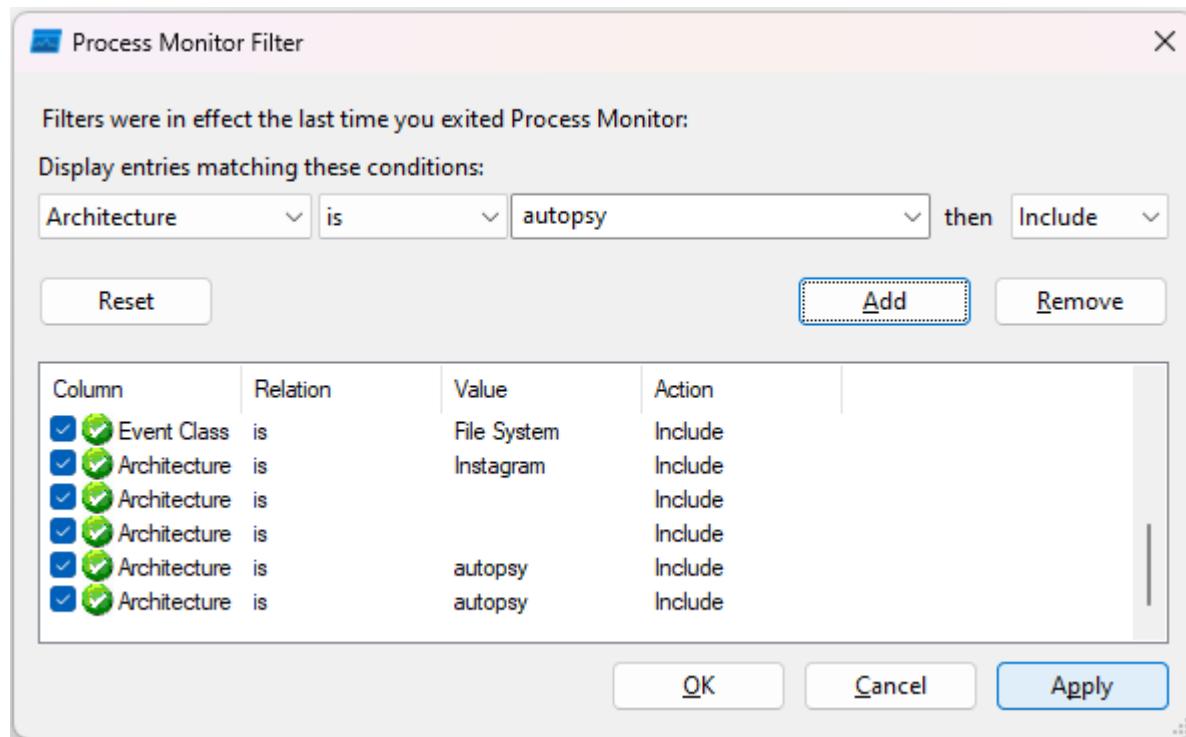
Process Monitor is an advanced monitoring tool for Windows that show real-time file system, Registry and process/thread activity. It combines the features of two legacy SysInternals utilities, Filemon and Regmon, and adds an extensive list of enhancements including rich non-destructive filtering, comprehensive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

STEPS

Sysinternal → procmon



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



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

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\MmCore.R.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\MmCore.R.dll	SUCCESS	Offset: 925696, Le...
08:27:...	svchost.exe	1656	UDP Receive	f#02:fb:5353 -> fe80:2050:4fce:b495:8...	SUCCESS	Length: 30, seqnu...
08:27:...	chrome.exe	9724	UDP Receive	f#02:fb:5353 -> fe80:2050:4fce:b495:8...	SUCCESS	Length: 30, seqnu...
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...
08:27:...	Explorer.EXE	11808	ReadFile	C:\Windows\System32\Taskbar.dll	SUCCESS	Offset: 2406400, L...
08:27:...	Explorer.EXE	11808	CloseFile	C:\Program Files\Windows Apps\Clipcha...	SUCCESS	Offset: 638976, Le...
08:27:...	svchost.exe	2644	ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset: 638976, Le...
08:27:...	Explorer.EXE	11808	RegCloseKey	HKU\S-1-5-21-3130516669-347735452...	SUCCESS	Desired Access: R...
08:27:...	Explorer.EXE	11808	RegOpenKey	HKU\S-1-5-21-3130516669-347735452...	SUCCESS	Query: HandleTag...
08:27:...	Explorer.EXE	11808	RegQueryKey	HKU\S-1-5-21-3130516669-347735452...	SUCCESS	Desired Access: R...
08:27:...	svchost.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:...	svchost.exe	11808	ReadFile	C:\Windows\System32\Taskbar.dll	SUCCESS	Offset: 155648, Le...
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	Offset: 180224, Le...
08:27:...	svchost.exe	11808	ReadFile	C:\Windows\System32\BCP47mm.dll	SUCCESS	Offset: 1540096, L...
08:27:...	svchost.exe	11808	RegOpenKey	HKU\S-1-5-21-3130516669-347735452...	SUCCESS	Offset: 6434816, L...
08:27:...	svchost.exe	11808	RegCloseKey	HKU\S-1-5-21-3130516669-347735452...	SUCCESS	Offset: 25229280, L...
08:27:...	svchost.exe	11808	ReadFile	C:\Windows\System32\Taskbar.dll	SUCCESS	Offset: 1523712, L...
08:27:...	svchost.exe	11808	ReadFile	C:\Windows\System32\Iasrv.dll	SUCCESS	Offset: 155648, Le...
08:27:...	svchost.exe	11808	ReadFile	C:\Windows\System32\BCP47mm.dll	SUCCESS	Offset: 2512896, L...
08:27:...	svchost.exe	11808	ReadFile	C:\Windows\System32\Windows.State...	SUCCESS	Offset: 6414336, L...
08:27:...	svchost.exe	11808	RegOpenKey	HKU\S-1-5-21-3130516669-347735452...	SUCCESS	Offset: 1519616, L...
08:27:...	svchost.exe	11808	RegCloseKey	HKU\S-1-5-21-3130516669-347735452...	SUCCESS	Desired Access: R...
08:27:...	svchost.exe	11808	RegQueryKey	HKU\S-1-5-21-3130516669-347735452...	SUCCESS	Offset: 6227968, L...
08:27:...	svchost.exe	11808	RegOpenKey	HKU\S-1-5-21-3130516669-347735452...	REPARSE	Desired Access: R...
08:27:...	svchost.exe	11808	RegOpenKey	HKU\S-1-5-21-3130516669-347735452...	SUCCESS	Desired Access: R...
08:27:...	svchost.exe	11808	LockFile	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	Exclusive: False, O...
08:27:...	svchost.exe	11808	RegCloseKey	HKLM\Software\Microsoft\Window...	SUCCESS	Query: HandleTag...
08:27:...	svchost.exe	11808	RegQueryKey	HKLM\Software\Microsoft\Window...	SUCCESS	Desired Access: R...
08:27:...	svchost.exe	11808	RegOpenKey	HKLM\Software\Microsoft\Window...	SUCCESS	Query: HandleTag...

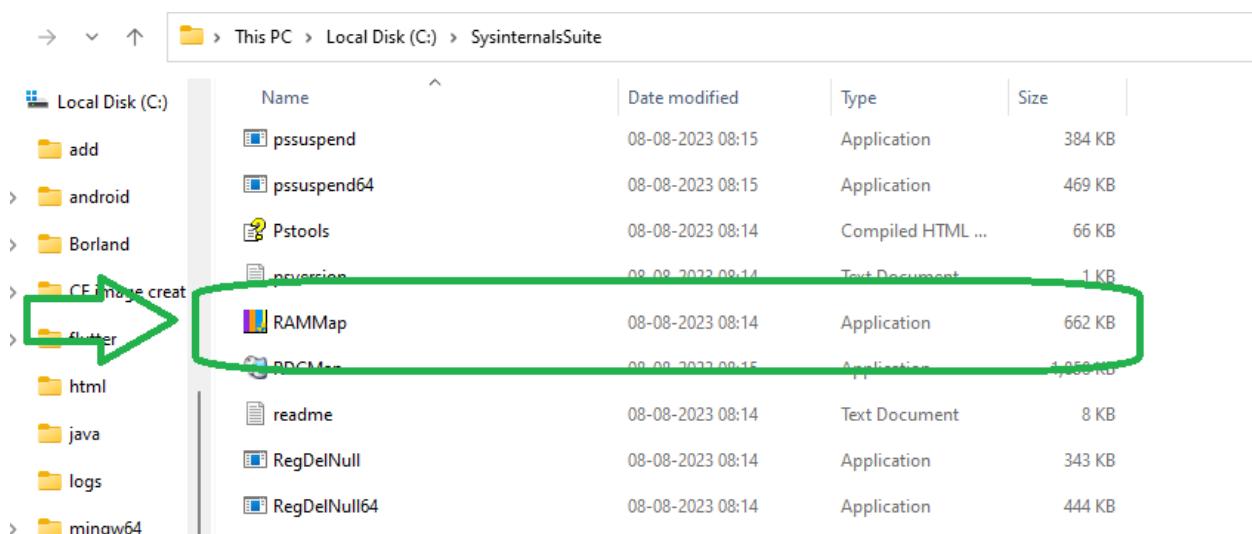
Capture RAM

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:

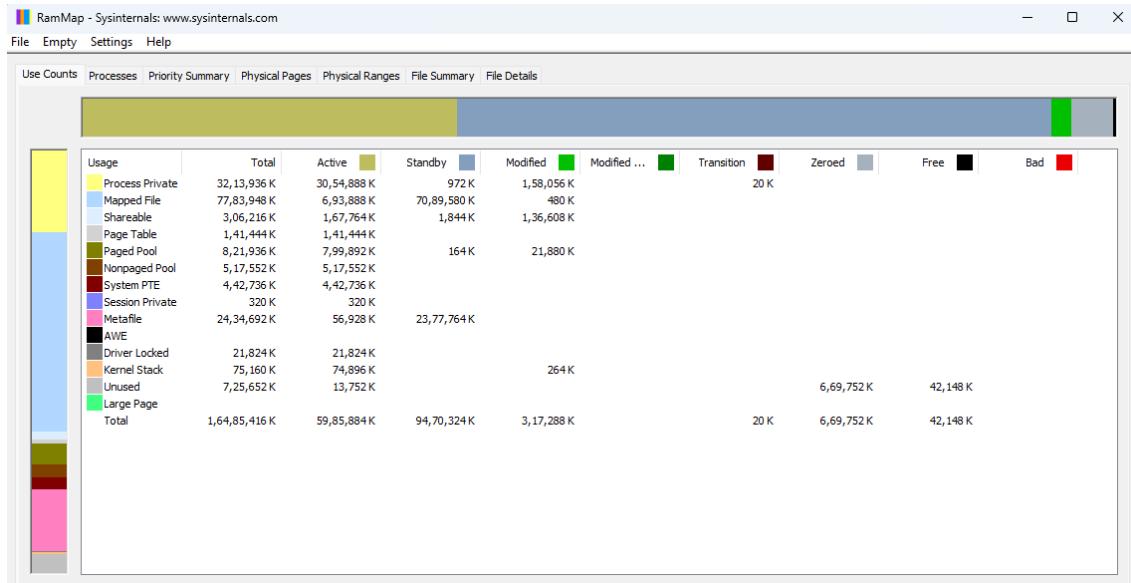
- **Use Counts:** usage summary by type and paging list
- **Processes:** process working set sizes
- **Priority Summary:** prioritized standby list sizes
- **Physical Pages:** per-page use for all physical memory
- **Physical Ranges:** physical memory addresses
- **File Summary:** file data in RAM by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

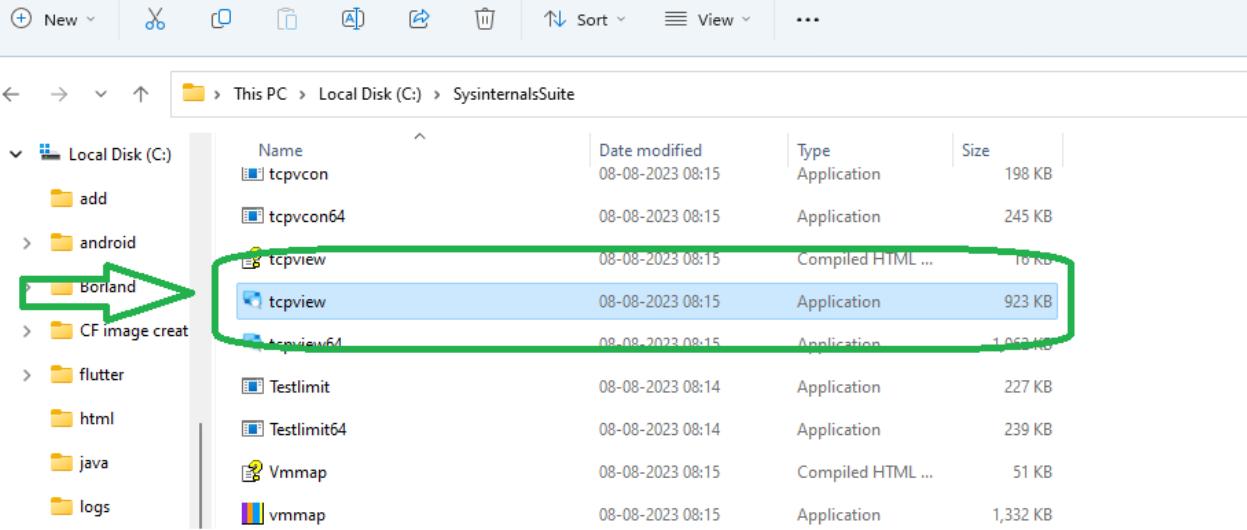
Tcpcvcon usage is similar to that of the built-in Windows netstat utility

Usage

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

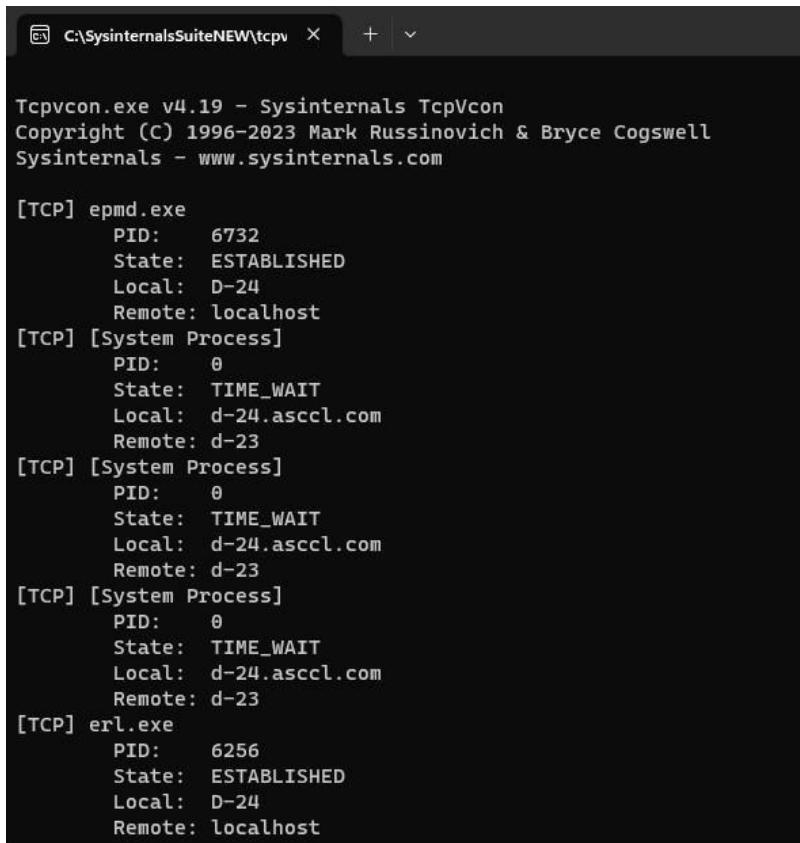
STEPS

Download TCPView



File Explorer window showing the contents of Local Disk (C):\SysinternalsSuite. The 'tcpview' application is selected and highlighted with a green box. A green arrow points from the 'Borland' folder to the 'tcpview' application.

Name	Date modified	Type	Size
tcpvcon	08-08-2023 08:15	Application	198 KB
tcpvcon64	08-08-2023 08:15	Application	245 KB
tcpview	08-08-2023 08:15	Compiled HTML ...	16 KB
tcpview	08-08-2023 08:15	Application	923 KB
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



TcpView application window showing network connections:

```
C:\SysinternalsSuiteNEW\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
```

RIZVI COLLEGE OF ARTS, SCIENCE AND COMMERCE
TYBSC CS SEM V – CYBER FORENSIC

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
smoner.exe	4164	TCP	Listen	0.0.0.0	49668	0.0.0.0	0	29-08-2023 07:05:11	smoner.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	SSDPWRV		
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	SSDPSRV		
svchost.exe	6108	UDPV6	fe80::3b4f:9f72:34ab:146	1900	*	29-08-2023 08:36:35	SSDPSRV		
svchost.exe	6108	UDPV6	fe80::3b4f:9f72:34ab:146	1900	*	29-08-2023 08:36:35	SSDPSRV		
svchost.exe	6108	UDPV6	fe80::3b4f:9f72:34ab:146	1900	*	29-08-2023 08:36:35	SSDPSRV		
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

#	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

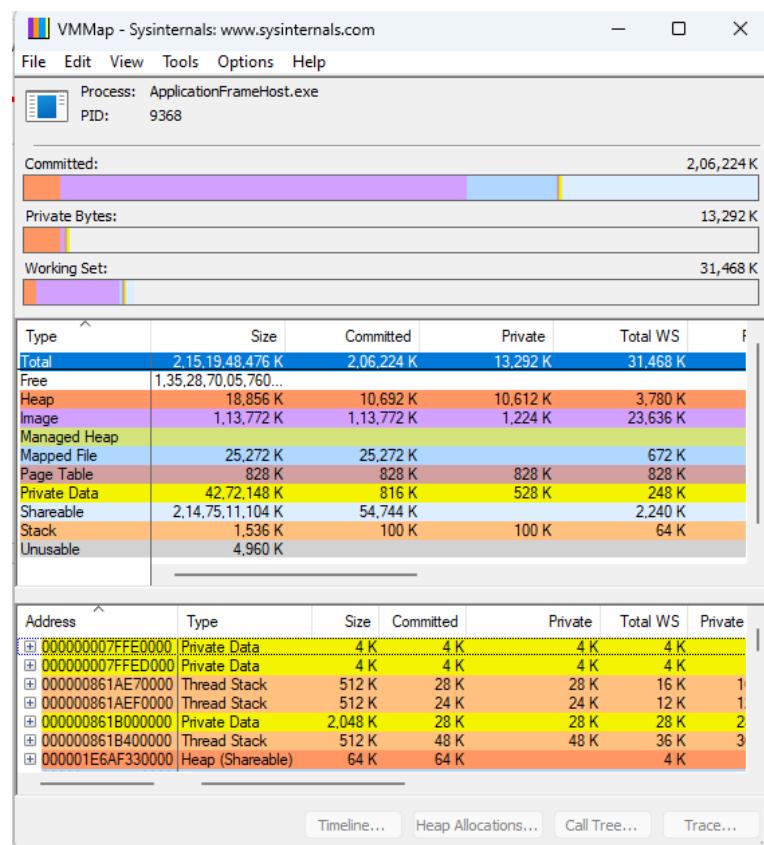
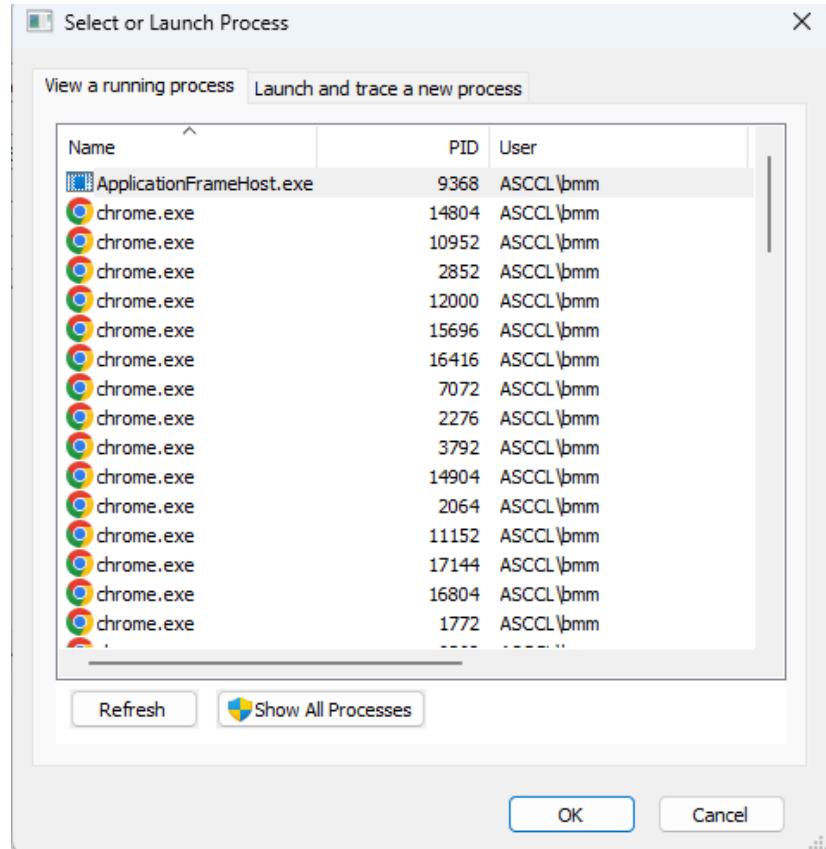
Monitor Virtual Memory

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

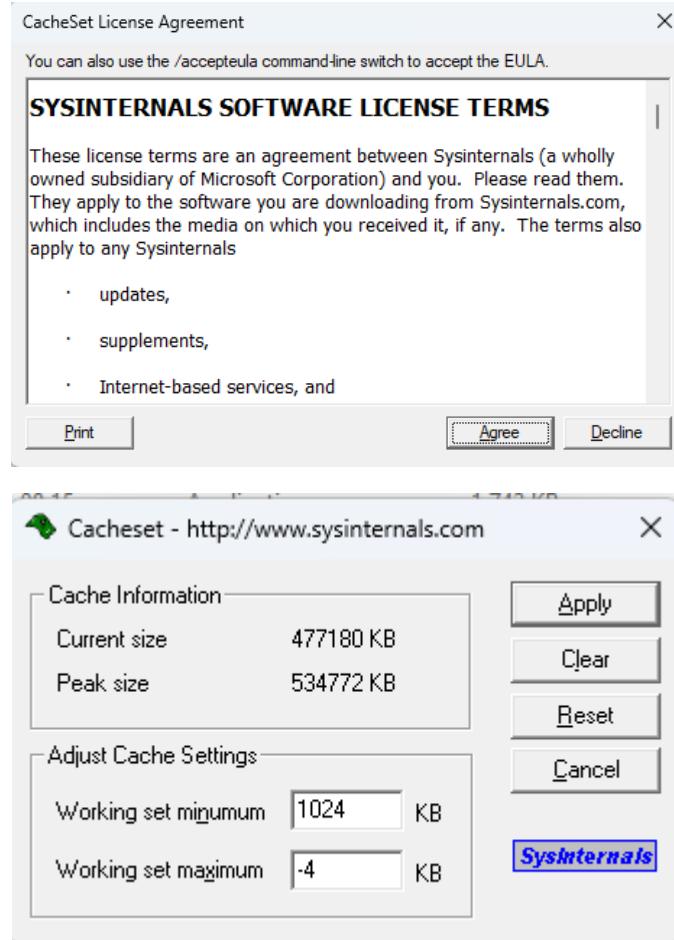
RIZVI COLLEGE OF ARTS, SCIENCE AND COMMERCE
TYBSC CS SEM V – CYBER FORENSIC



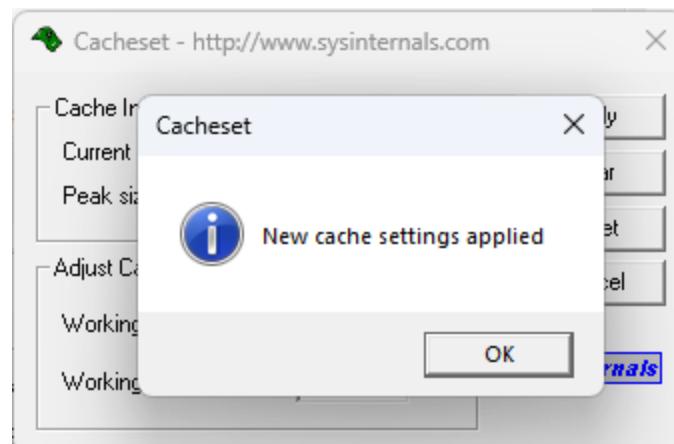
Monitor Cache Memory

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.

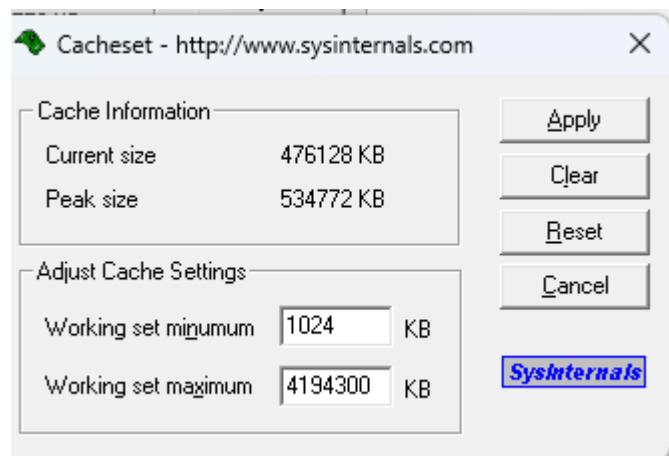
Give all the permissions and Click on Agree



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

Steps

1. Case Information
2. Optional Information

Case Information

Case Name:

Base Directory:

Case Type: Single-user Multi-user

Case data will be stored in the following directory:

< Back

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

New Case Information

Steps

1. Case Information
2. Optional Information

Optional Information

Case

Number:

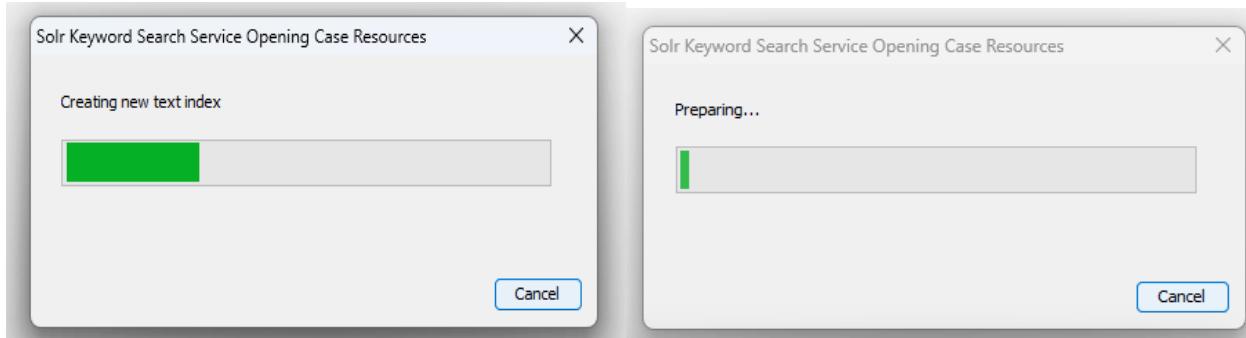
Examiner

Name:
Phone:
Email:
Notes:

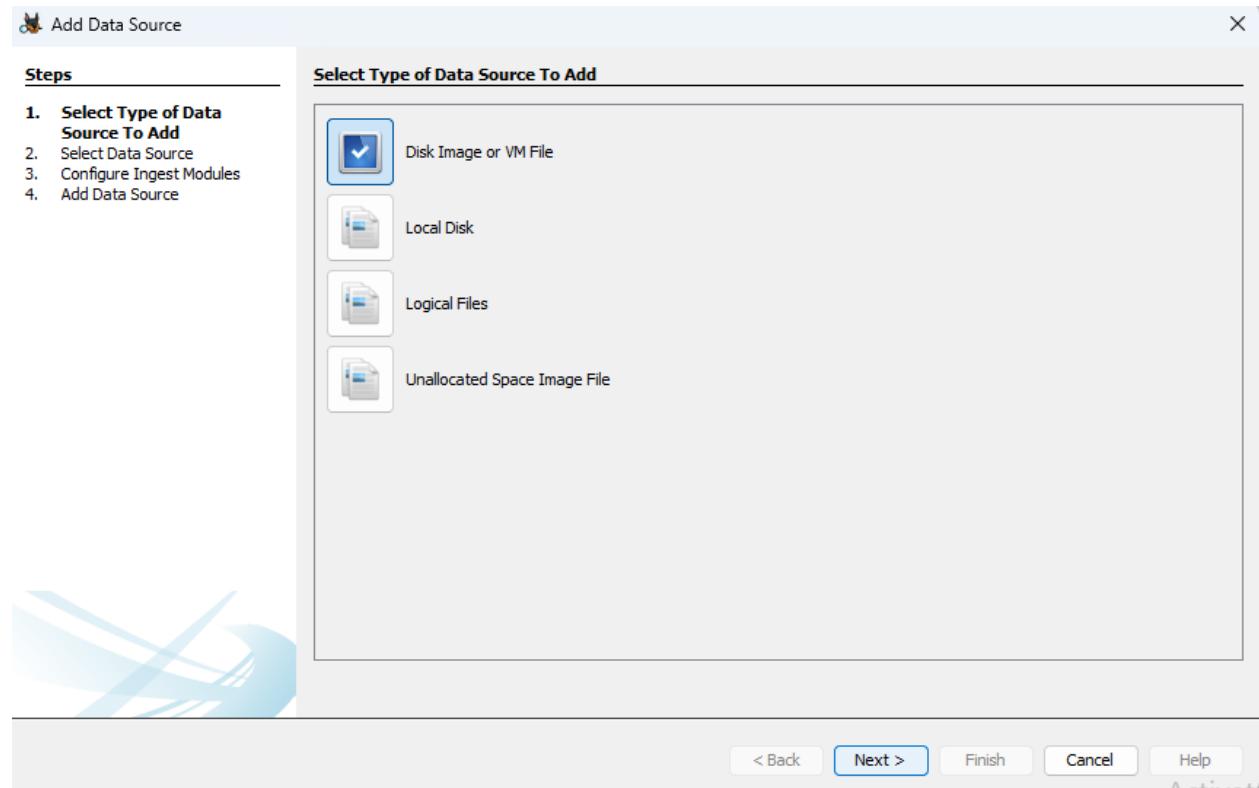
Organization

Organization analysis is being done for:

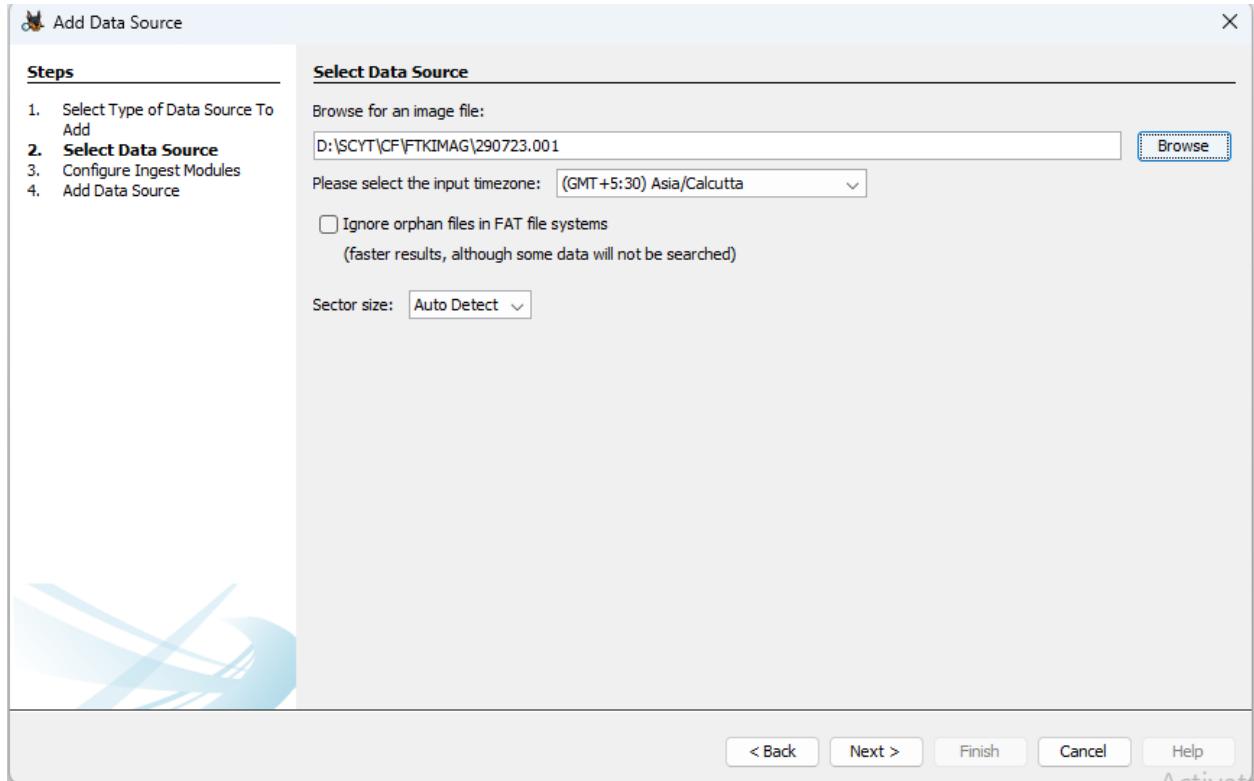
< Back



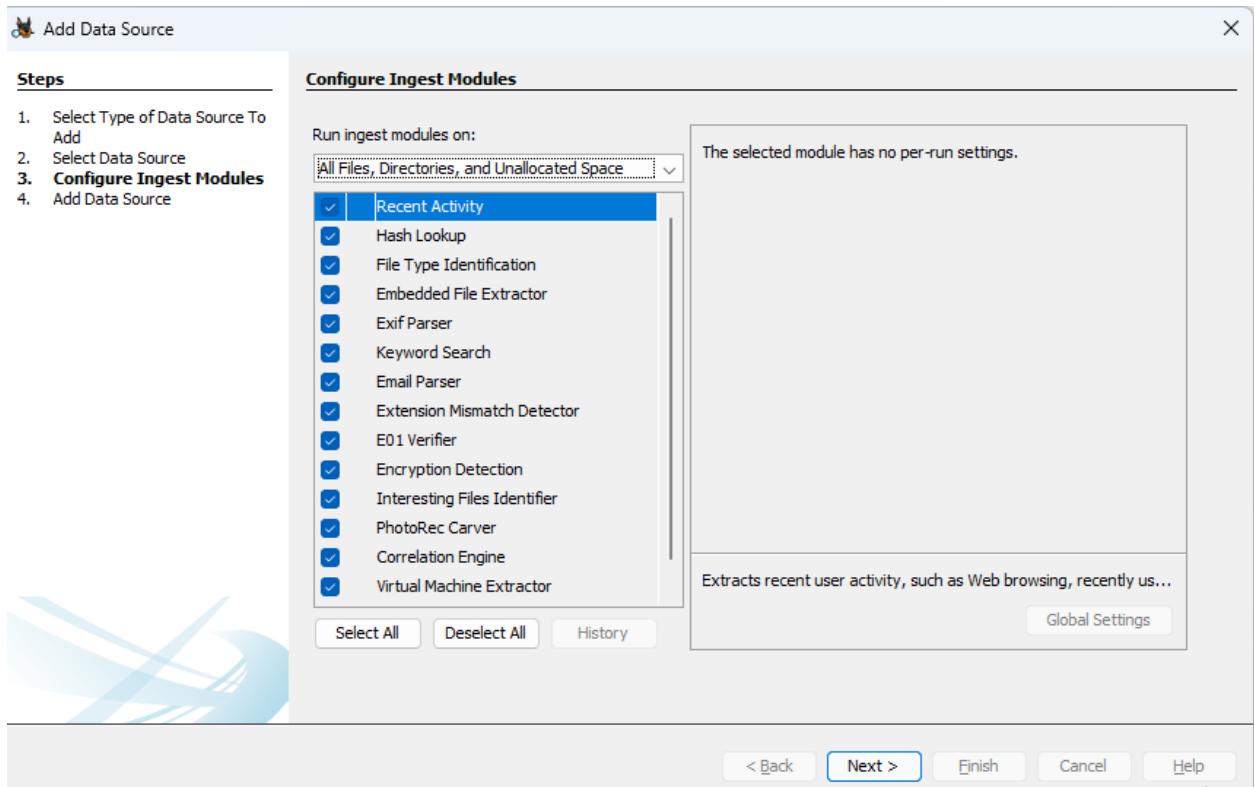
Select on Disk Image or VM File and Click Next



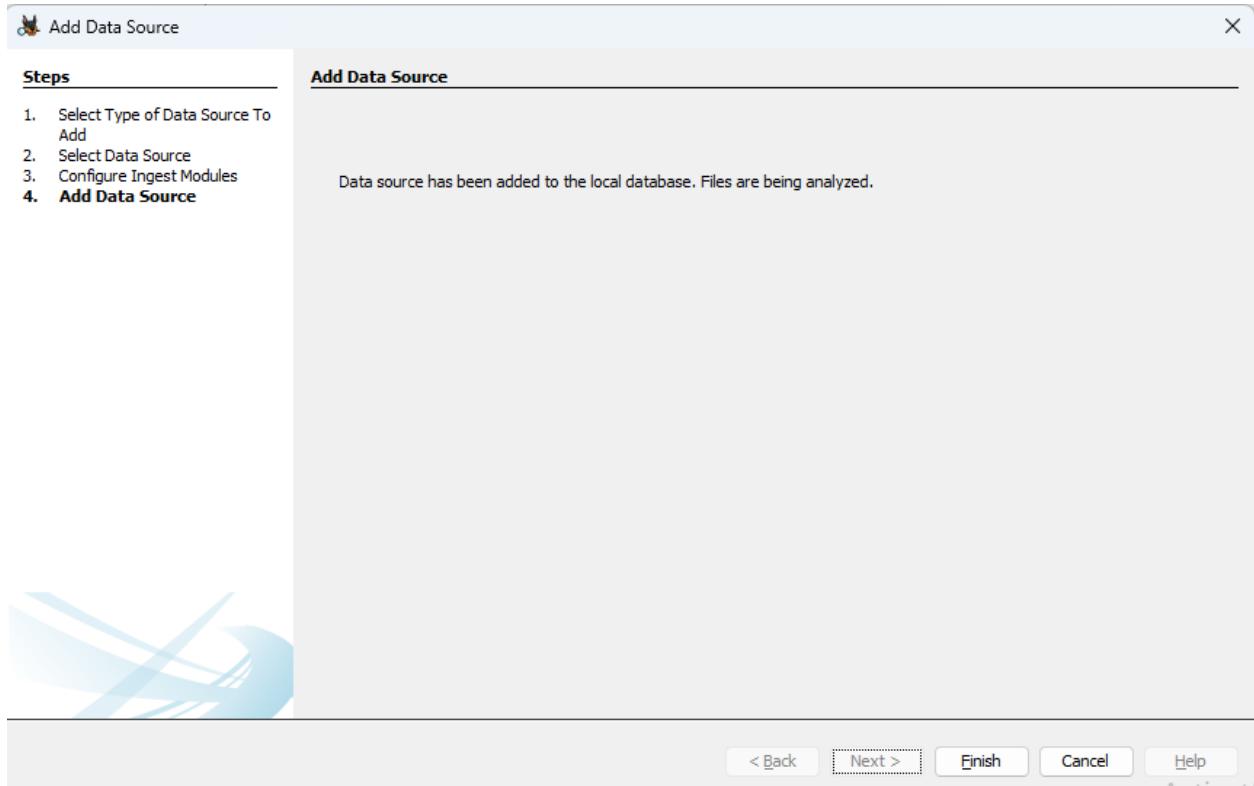
Give the destination of the image and click next



Select the ingest module and click next



See the acknowledgement and click finish



Now we check the files recovered

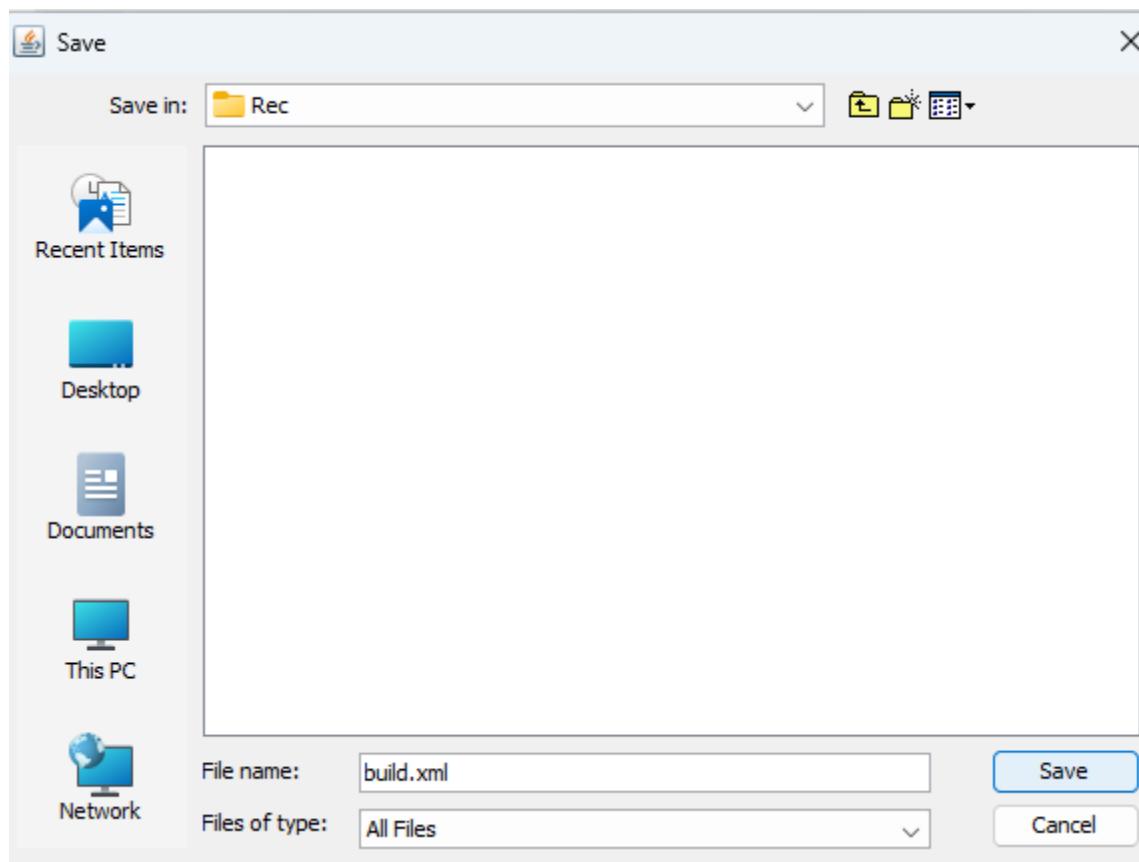
Name	S	C	Location	Modified Time	Change Time	Access Time	C
EFISECTOR			/Img_290723.001/vol_vol2/\$OrphanFiles/EFISECTOR	2019-12-06 17:05:28 IST	0000-00-00 00:00:00	0000-00-00 00:00:00	0
EFI			/Img_290723.001/vol_vol2/\$OrphanFiles/EFI	2019-12-06 09:05:28 IST	0000-00-00 00:00:00	2019-12-06 00:00:00 IST	2
BOOT			/Img_290723.001/vol_vol2/\$OrphanFiles/BOOT	2019-12-06 17:05:28 IST	0000-00-00 00:00:00	2019-12-06 00:00:00 IST	2
BOOTX64.EFI			/Img_290723.001/vol_vol2/\$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_vol2/\$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_vol2/\$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_vol2/\$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_vol2/\$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_vol2/\$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_vol2/\$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_vol2/\$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_vol2/\$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_vol2/\$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_vol2/\$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^H^H^\$^			/Img_290723.001/vol_vol2/\$OrphanFiles/H^L^H^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^H^H^\$^			/Img_290723.001/vol_vol2/\$OrphanFiles/H^L^H^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_vol2/\$OrphanFiles/~~~~~@@@	2004-01-16 06:00:00 IST	0000-00-00 00:00:00	0000-00-00 00:00:00	0
t^D\$pH^~\$^			/Img_290723.001/vol_vol2/\$OrphanFiles/t^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_vol2/\$OrphanFiles/~~~~~	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0
~~~mV~~~			/Img_290723.001/vol_vol2/\$OrphanFiles/~~~mV~~~	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_vol2/\$OrphanFiles/f693ba26.83a	1992-08-10 03:56:04 IST	0000-00-00 00:00:00	2007-01-17 00:00:00 IST	2

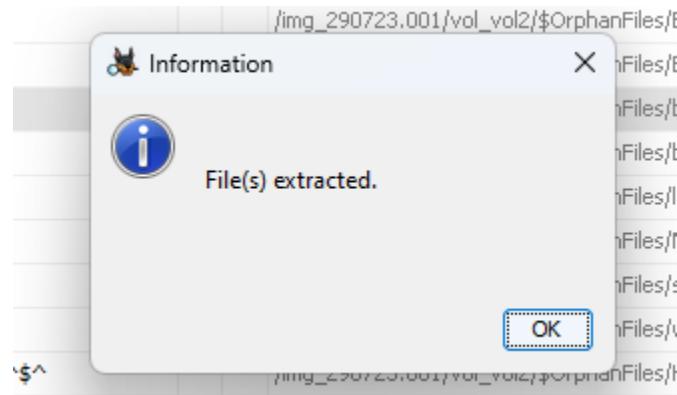
We see the Deleted Files

Now We Extract/Recover some deleted files

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

Set a directory for the recovered files

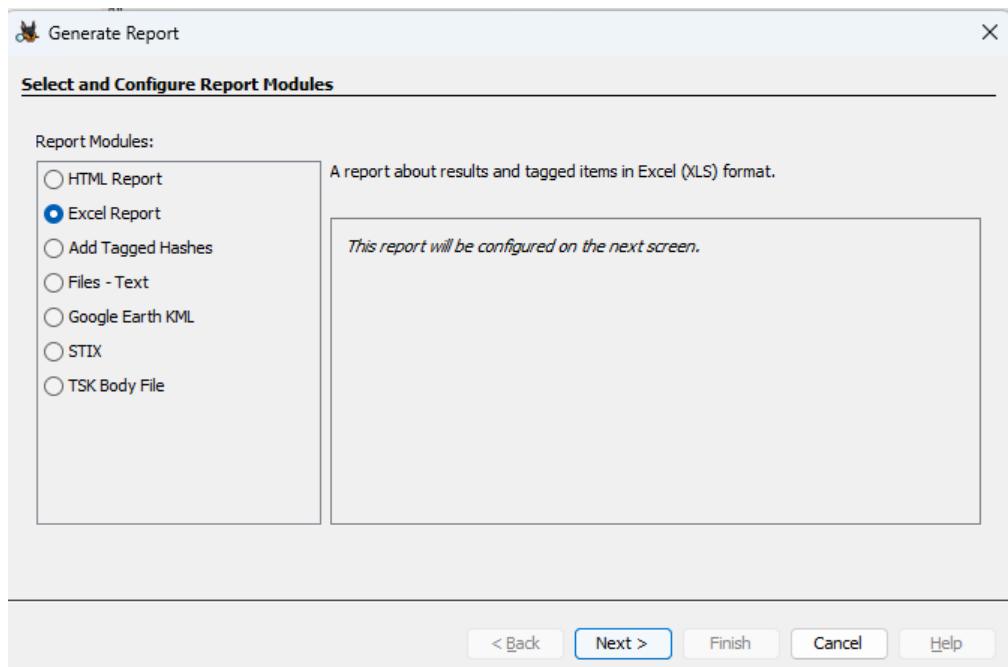




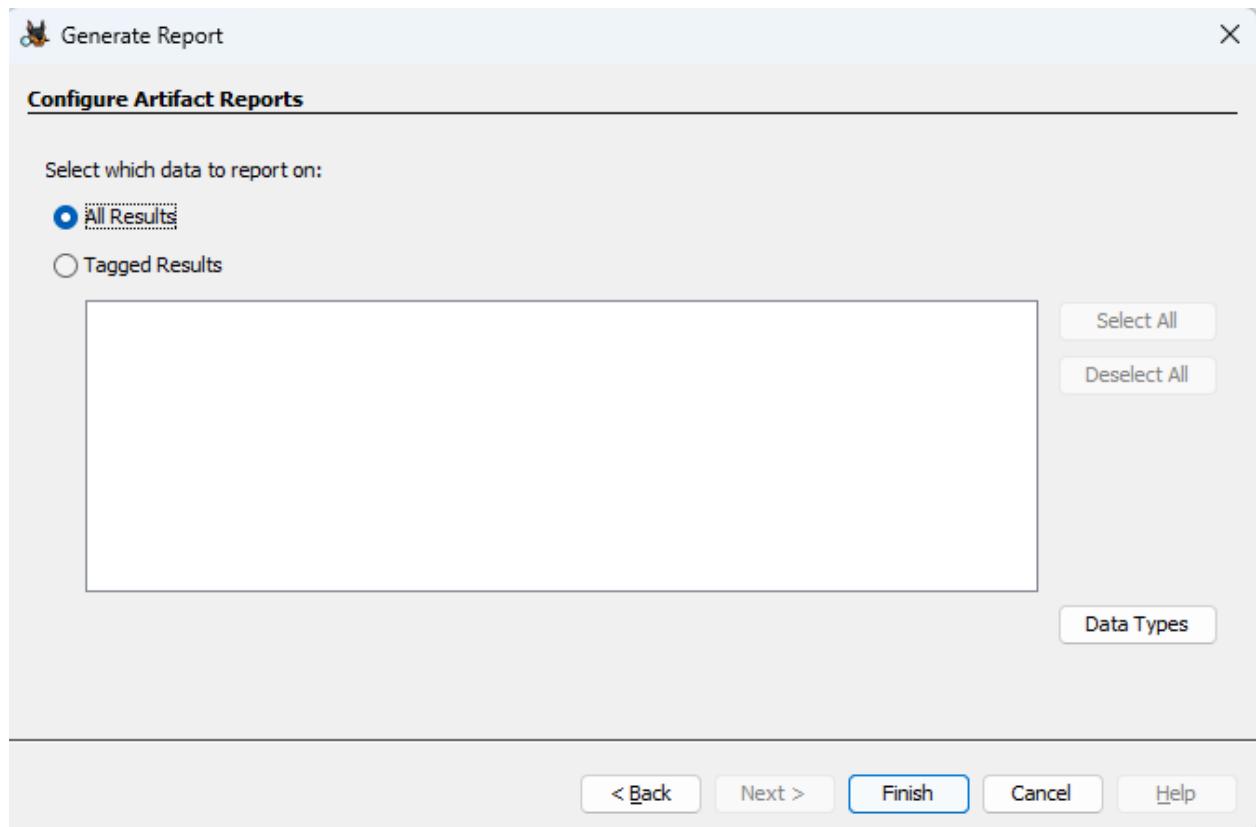
Now we Generate a Report of the Autopsy done

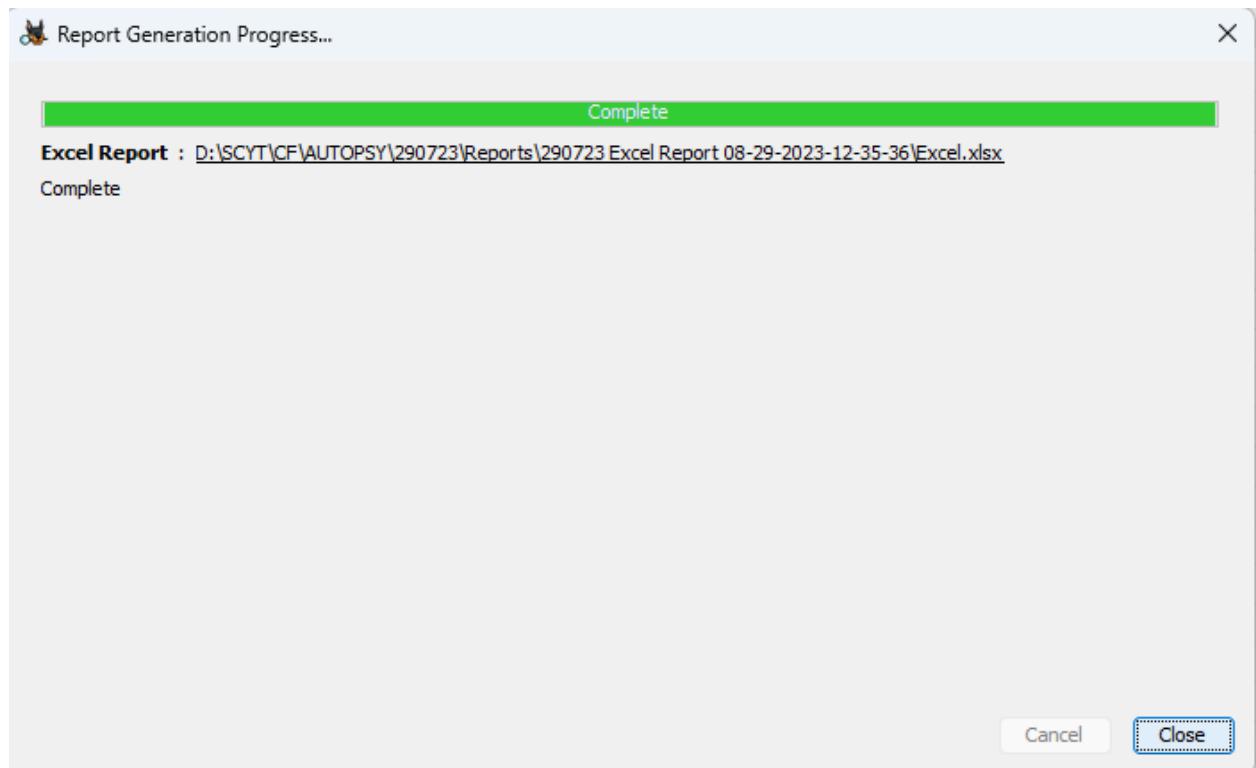
Name	Location	Modified Time	Change Time	Access Time
BOOTX64.EFI	/img_290723.001/vol_vo2/\$OrphanFiles/BOOTX64.EFI	2019-12-06 17:05:16 IST	0000-00-00 00:00:00	2019-12-06 00:00:00 IST
EFISECTOR	/img_290723.001/vol_vo2/\$OrphanFiles/EFISECTOR	2019-12-06 17:05:30 IST	0000-00-00 00:00:00	0000-00-00 00:00:00
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
<b>build.xml</b>	<b>/img_290723.001/vol_vo2/\$OrphanFiles/build.xml</b>	<b>2022-09-26 14:06:42 IST</b>	<b>0000-00-00 00:00:00</b>	<b>2023-01-07 00:00:00 IST</b>
x 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
x 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
x NPROJ~1	/img_290723.001/vol_vo2/\$OrphanFiles/NPROJ~1	2022-09-26 14:06:42 IST	0000-00-00 00:00:00	2023-01-07 00:00:00 IST
x 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
x 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
x 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
x 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
x ~~~~~~,@@@	/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
x tf^@SpH^~,^\$^	/img_290723.001/vol_vo2/\$OrphanFiles/tf^@SpH^~,^\$^	1998-04-04 17:10:16 IST	0000-00-00 00:00:00	1980-05-08 00:00:00 IST
x ~~~~~~	/img_290723.001/vol_vo2/\$OrphanFiles/~~~~~~	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
x ^~~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.

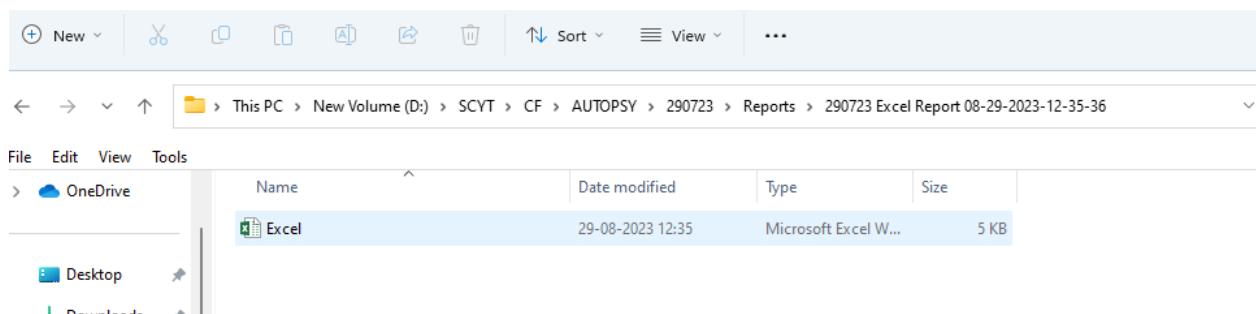


Now select all results this will generate all the reports and click finish. The other option only generate the report for tagged one only.





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



RIZVI COLLEGE OF ARTS, SCIENCE AND COMMERCE  
TYBSC CS SEM V – CYBER FORENSIC

The screenshot shows two Excel sheets: 'Summary' and 'Log'.

**Summary Sheet:**

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					

**Log Sheet:**

A	B	C	D	E	F	G	H	I
1 Date Taken	Device Manufacturer	Device Model	Latitude	Longitude	Altitude	Source File	Tags	
2 2022-06-10 18:10:21 IST	realme	realme 6				/img_04092023_masood.001/vol_vo1/IMG20220610181021.jpg		
3 2022-06-10 18:10:27 IST	realme	realme 6				/img_04092023_masood.001/vol_vo1/IMG20220610181027.jpg		
4 2022-06-10 18:10:30 IST	realme	realme 6				/img_04092023_masood.001/vol_vo1/IMG20220610181030.jpg		
5 2022-06-10 18:10:34 IST	realme	realme 6				/img_04092023_masood.001/vol_vo1/IMG20220610181034.jpg		
6 2022-06-10 18:23:26 IST	realme	realme 6				/img_04092023_masood.001/vol_vo1//\$CarvedFiles/f0000000.jpg		
7 2022-06-10 18:24:07 IST	realme	realme 6				/img_04092023_masood.001/vol_vo1//\$CarvedFiles/f0005120.jpg		
8 2022-06-10 18:24:13 IST	realme	realme 6				/img_04092023_masood.001/vol_vo1//\$CarvedFiles/f0012256.jpg		
9 2022-06-10 18:24:17 IST	realme	realme 6				/img_04092023_masood.001/vol_vo1//\$CarvedFiles/f0016320.jpg		
10 2022-06-10 18:24:37 IST	realme	realme 6				/img_04092023_masood.001/vol_vo1//\$CarvedFiles/f0020864.jpg		
11 2022-06-10 18:34:20 IST	realme	realme 6				/img_04092023_masood.001/vol_vo1/IMG20220610183420.jpg		
12 2022-06-10 18:34:25 IST	realme	realme 6				/img_04092023_masood.001/vol_vo1/IMG20220610183425.jpg		
13 2022-06-10 18:34:37 IST	realme	realme 6				/img_04092023_masood.001/vol_vo1/IMG20220610183437.jpg		
14 2022-06-10 18:34:53 IST	realme	realme 6				/img_04092023_masood.001/vol_vo1/IMG20220610183453.jpg		
15								
16								
17								

RIZVI COLLEGE OF ARTS, SCIENCE AND COMMERCE  
TYBSC CS SEM V – CYBER FORENSIC

A	B	C	D	E	F
1 E-Mail To	E-Mail From	Subject	Date Sent	Date Received	Path
2 'Samspade@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 'Samspade@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 'Samspade@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 'Samspade@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
1 Email Addresses			
2 %@clients.l.google.com			
3 Preview			
4 llients.l.google.com%@clients.l.google.com%hclients.l.google.	Source File		Tags
5 llients.l.google.com%@clients.l.google.com%hclients.l.google.	/img_04092023_masood.001/vol_vo1//\$Unalloc/Unalloc_1878_3915776_1077723136		
6 llients.l.google.com%@clients.l.google.com%hclients.l.google.	/img_04092023_masood.001/vol_vo1/\$OrphanFiles/_LPLA^1.PCA		
7 llients.l.google.com%@clients.l.google.com%hclients.l.google.	/img_04092023_masood.001/vol_vo1/\$OrphanFiles/_ROTEU^LEXE		
8	/img_04092023_masood.001/vol_vo1/\$OrphanFiles/aftnnndbn.umd		
9 -239034676-0-1001@flonetwork.com			
10 Preview			
11 jjz4zntr-239034676-0-1001@flonetwork.com<work.com>[4676-0	Source File		Tags
12 jjz4zntr-239034676-0-1001@flonetwork.com<work.com>[4676-0	/img_04092023_masood.001/vol_vo1//\$Unalloc/Unalloc_1878_3915776_1077723136		
13	/img_04092023_masood.001/vol_vo1/_S_Proteus 8.11 SP0 Pro HomeMade Electronics.exe		
14 200612032123.609457386a225c@rly-xm04.mx.aol.com			
15 Preview			
16 -0500n-reply-to: <>200612032123.609457386a225c@rly-xm04.mx.aol.com<>x-mb-message-sourc	Source File		Tags
17 -0500n-reply-to: <>200612032123.609457386a225c@rly-xm04.mx.aol.com<>x-mb-message-sourc	/img_04092023_masood.001/vol_vo1//\$Unalloc/Unalloc_1878_3915776_1077723136		
18	/img_04092023_masood.001/vol_vo1/_S_Proteus 8.11 SP0 Pro HomeMade Electronics.exe		
19 20061204013940.a88906765f@mprdmxin.myway.com			
20 Preview			
21 etmail.comcast.net<20061204013940.a88906765f@mprdmxin.myway.com>mail.comcast.net000	Source File		Tags
22 7hntmacan.id<>20061204013940.a88906765f@mprdmxin.myway.com>mail.comcast.net000	/img_04092023_masood.001/vol_vo1//\$Unalloc/Unalloc_1878_3915776_1077723136		
23	/img_04092023_masood.001/vol_vo1/\$OrphanFiles/f1322d08.net		

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:

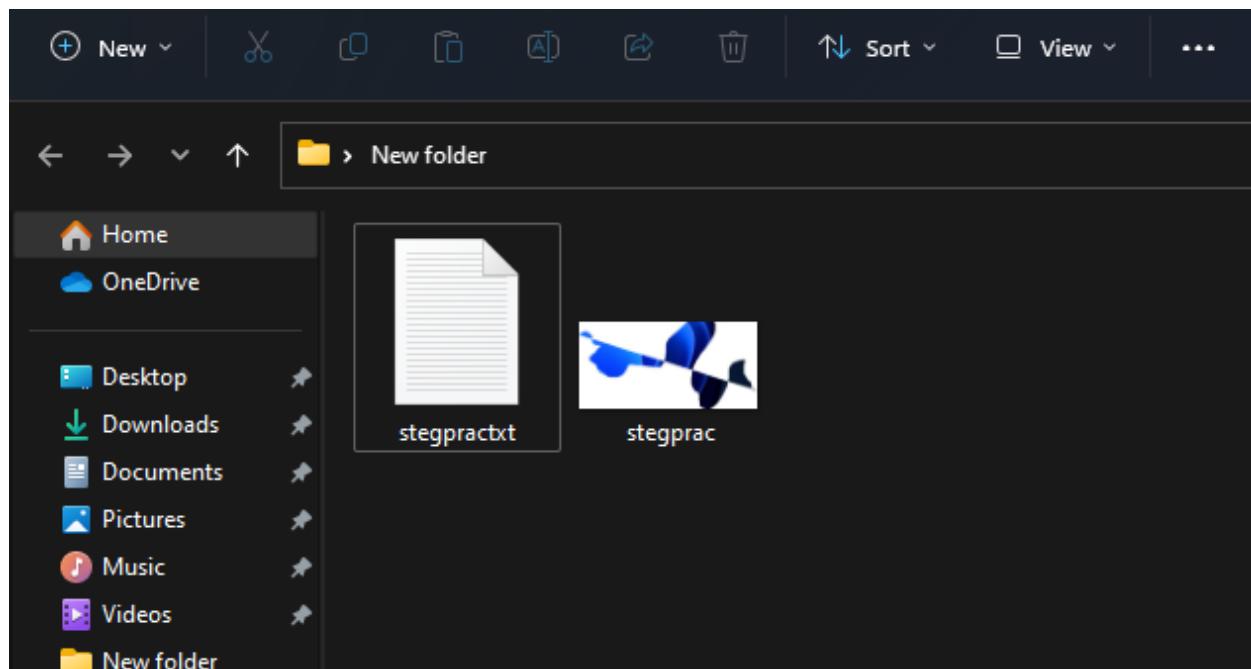
Steganography Detection

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

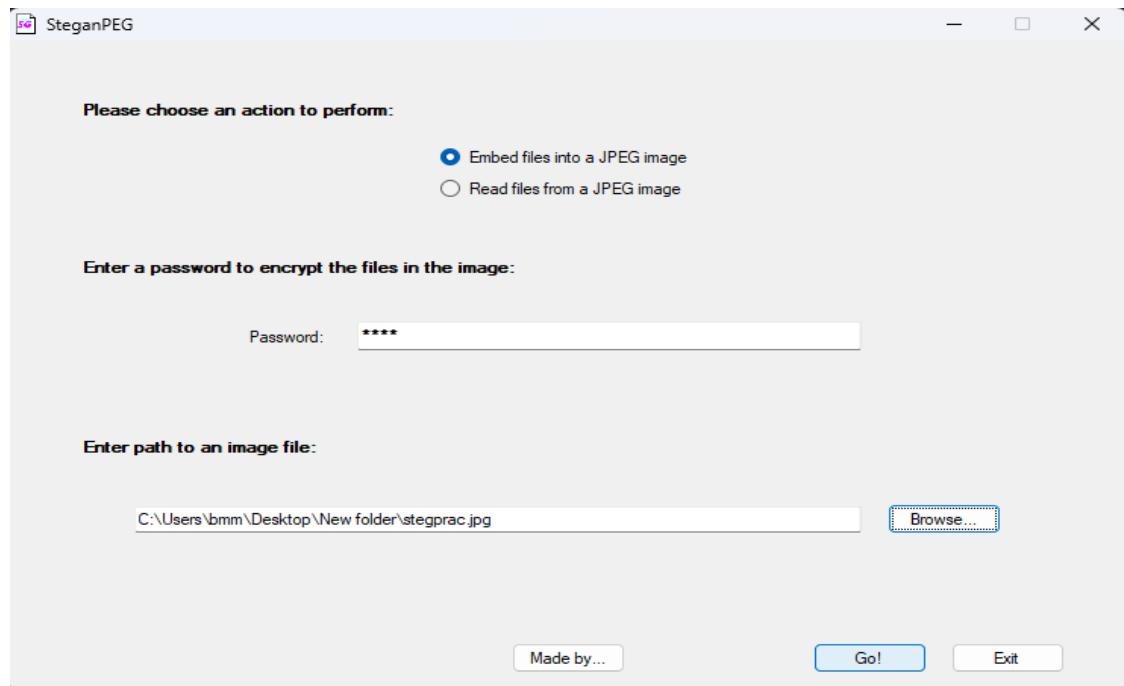
### Practical:

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

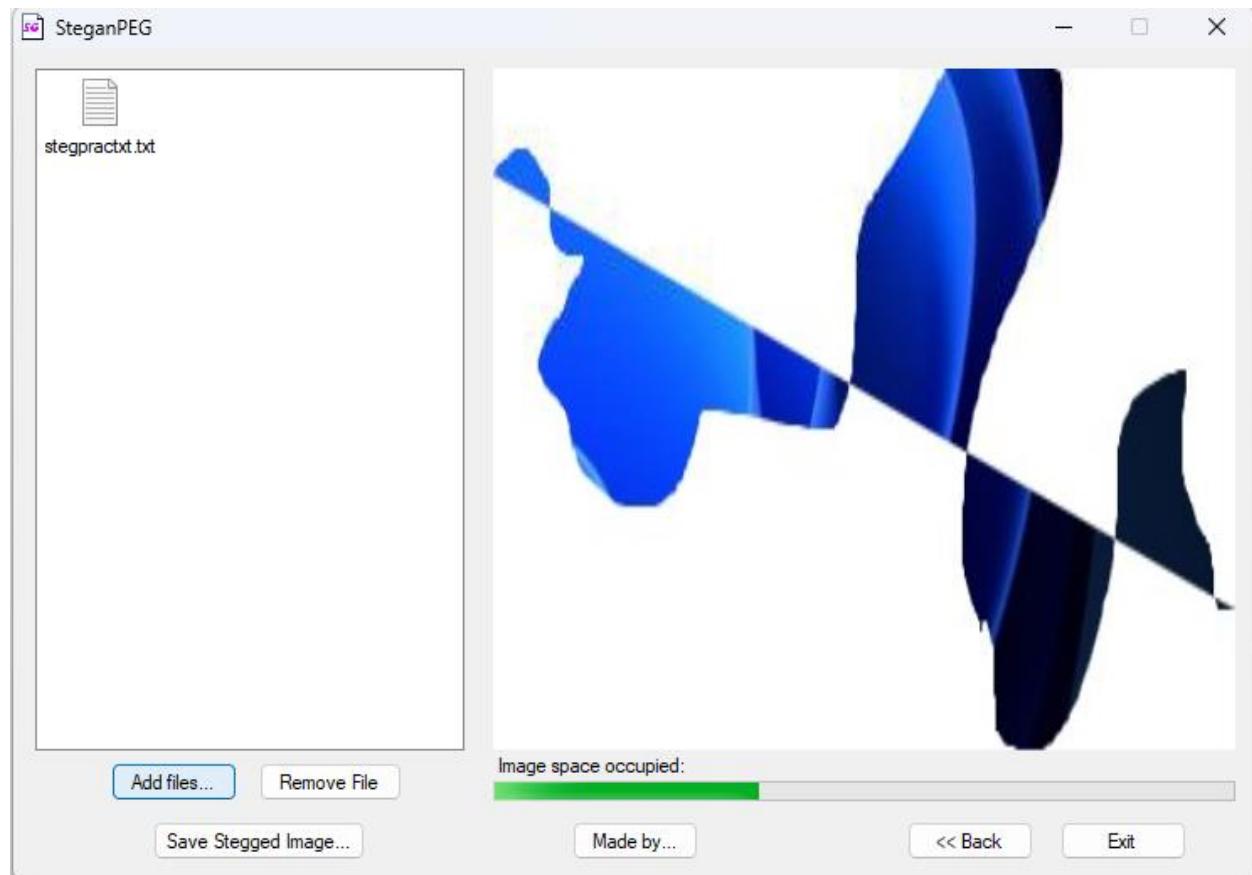
Create a folder to keep the image and message file and store the txt file and image



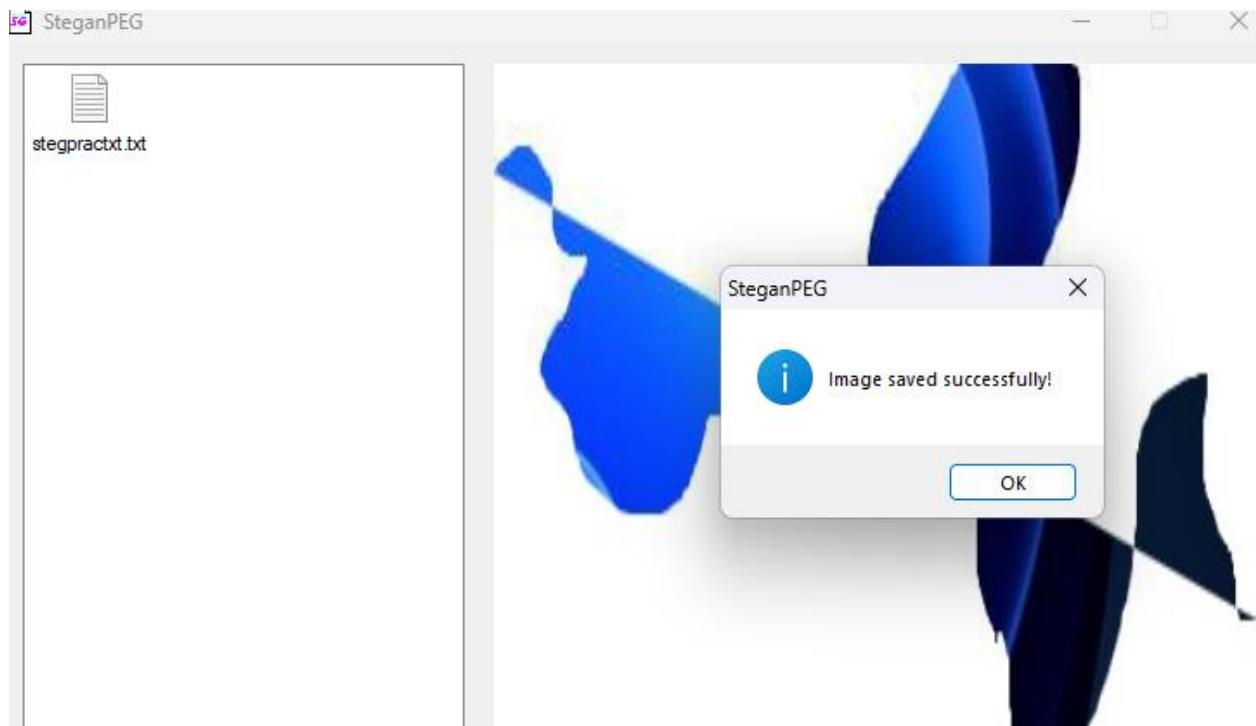
Open the SteganPEG and give a password and browse the path of the image



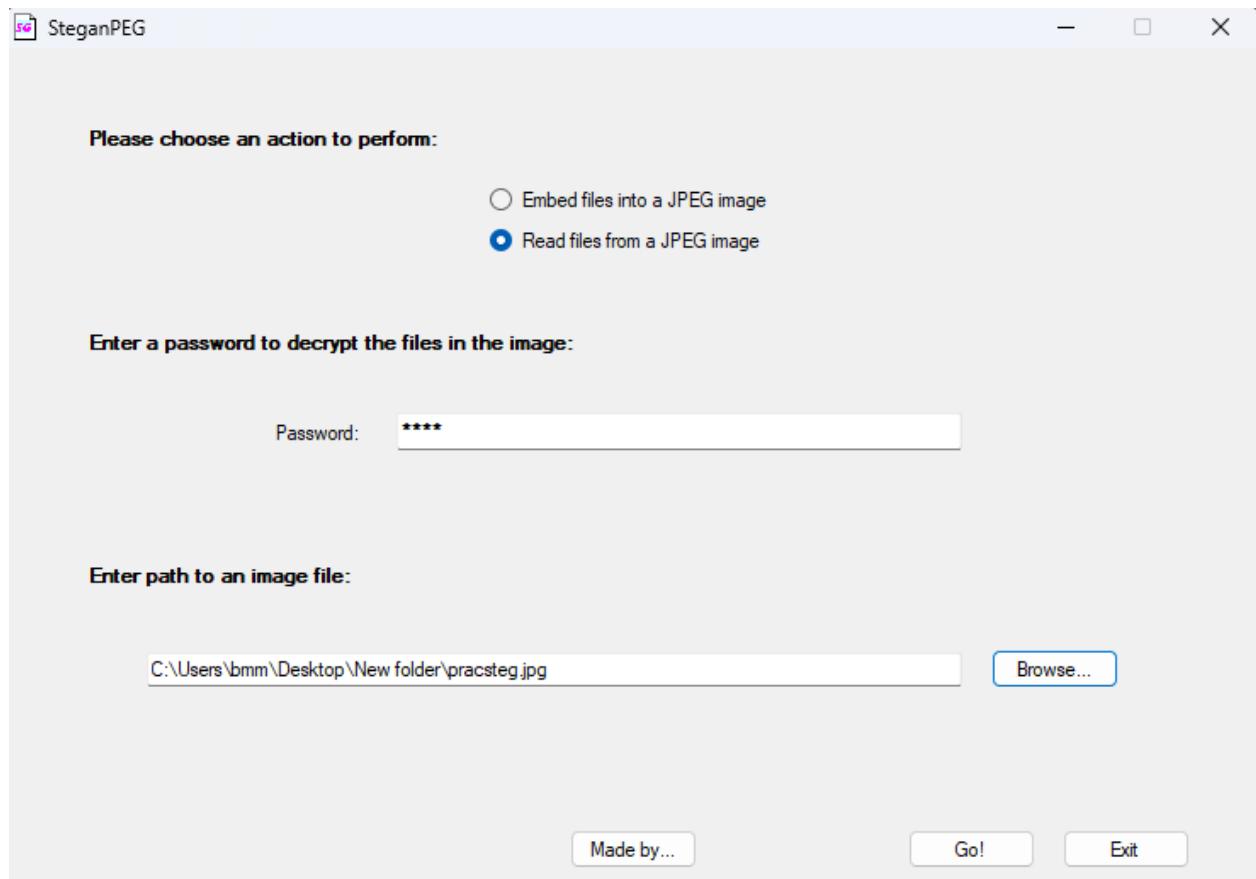
First we are going to add some files in the captured image

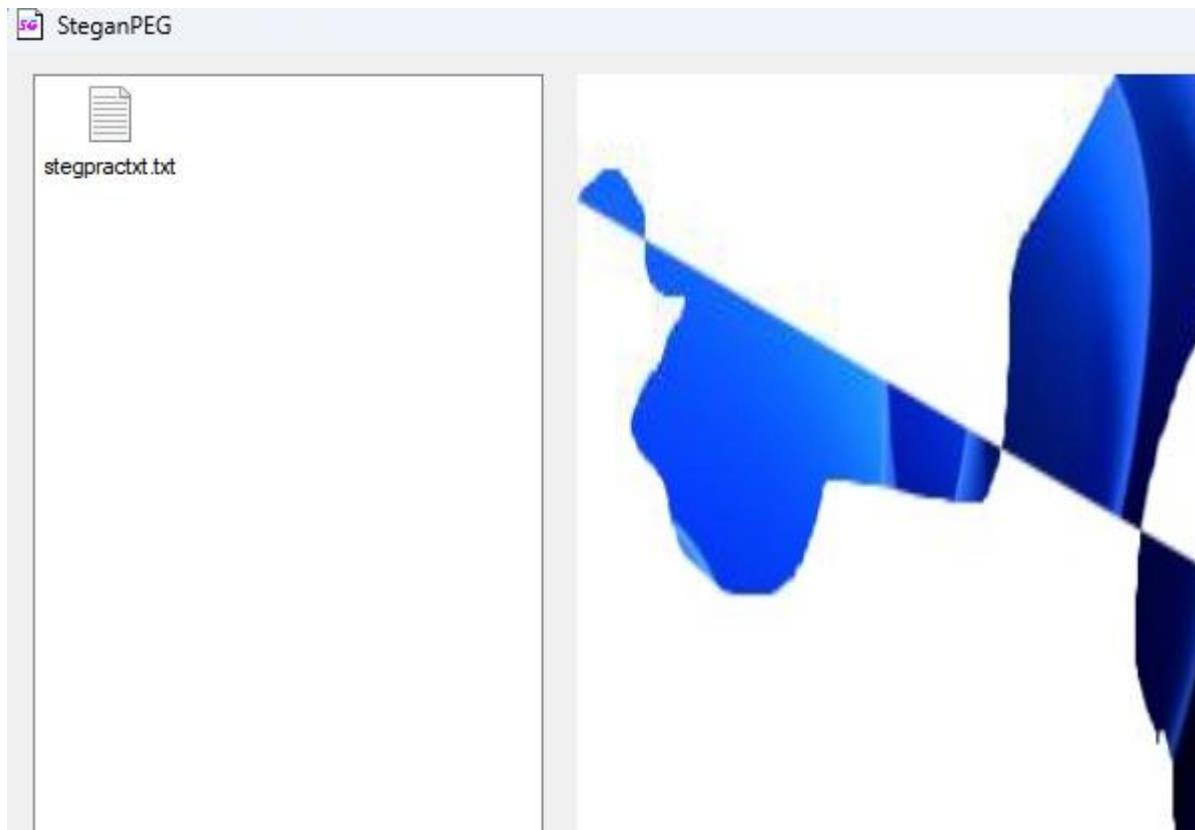


Save the stegged image



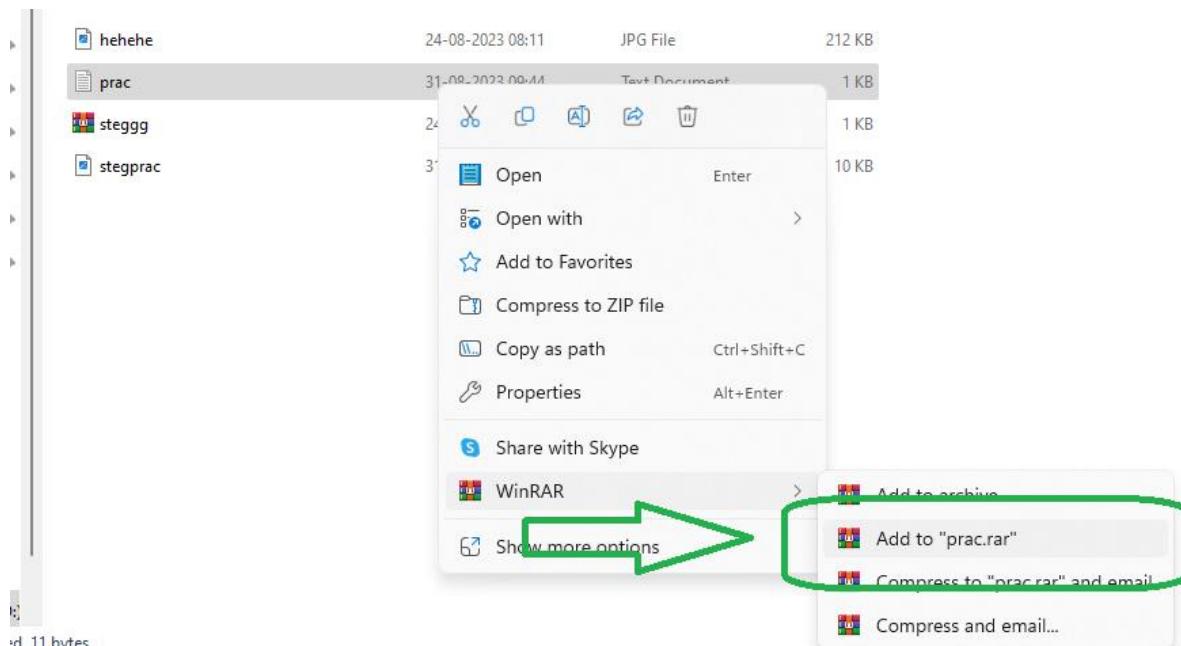
Open the saved image with the assigned password and view the image with hidden files





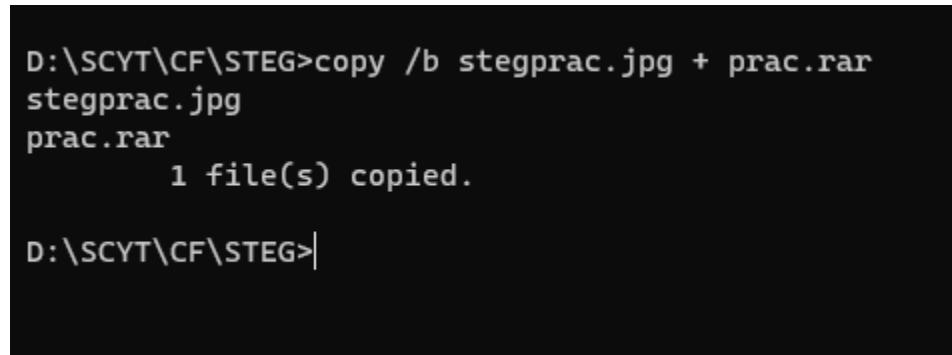
Now we are going to do the stegging process using Command Prompt and viewing the Image using the WinRAR.

Make a zip file of the text file



Go to Command Prompt and Type the Syntax

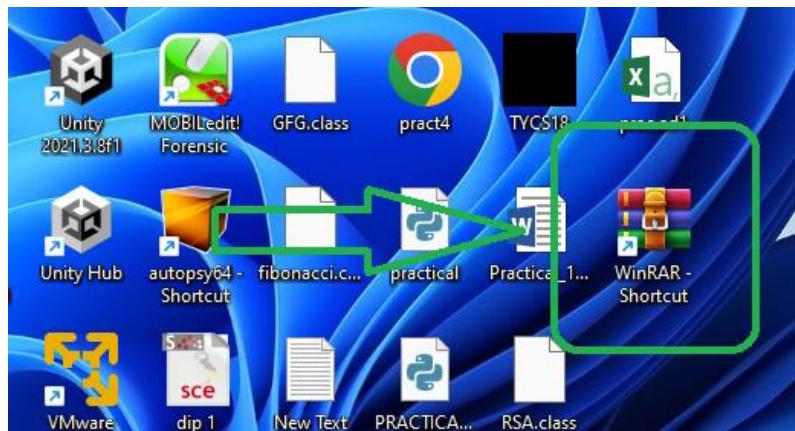
C:\Users\bmm\Desktop>New Folder>copy/b stegprac.jpg + stegpractxt.rar



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

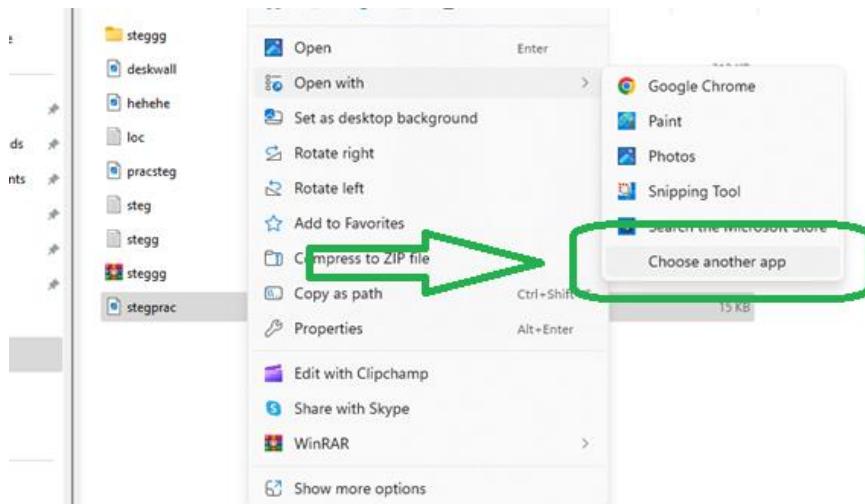
D:\SCYT\CF\STEG>
```

Then create a shortcut for WinRAR on the desktop

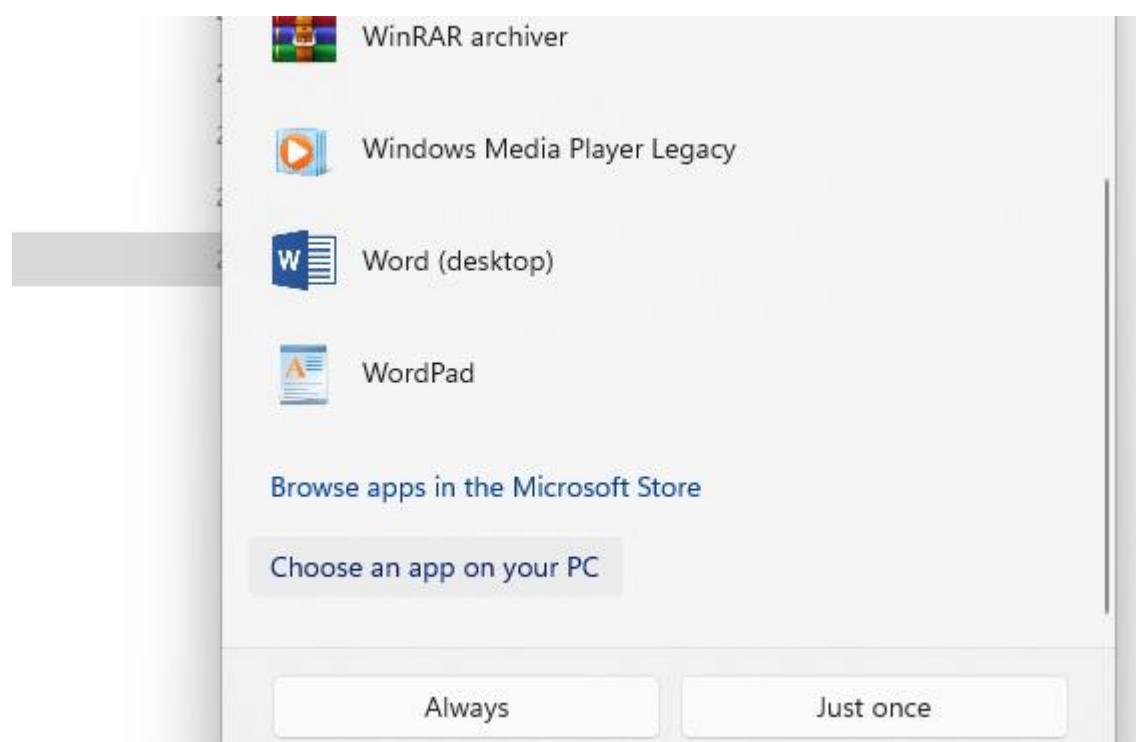


Then open the image using the shortcut

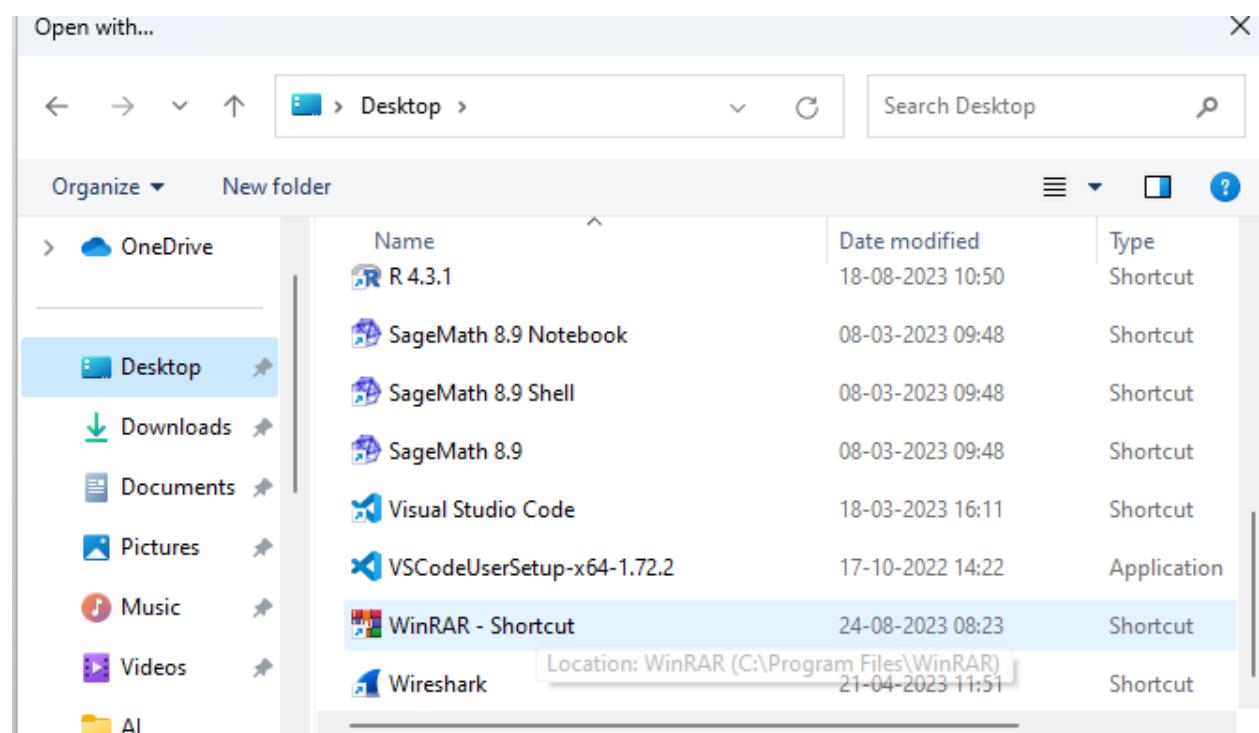
**Right Click on the image → Open with → Choose another app**

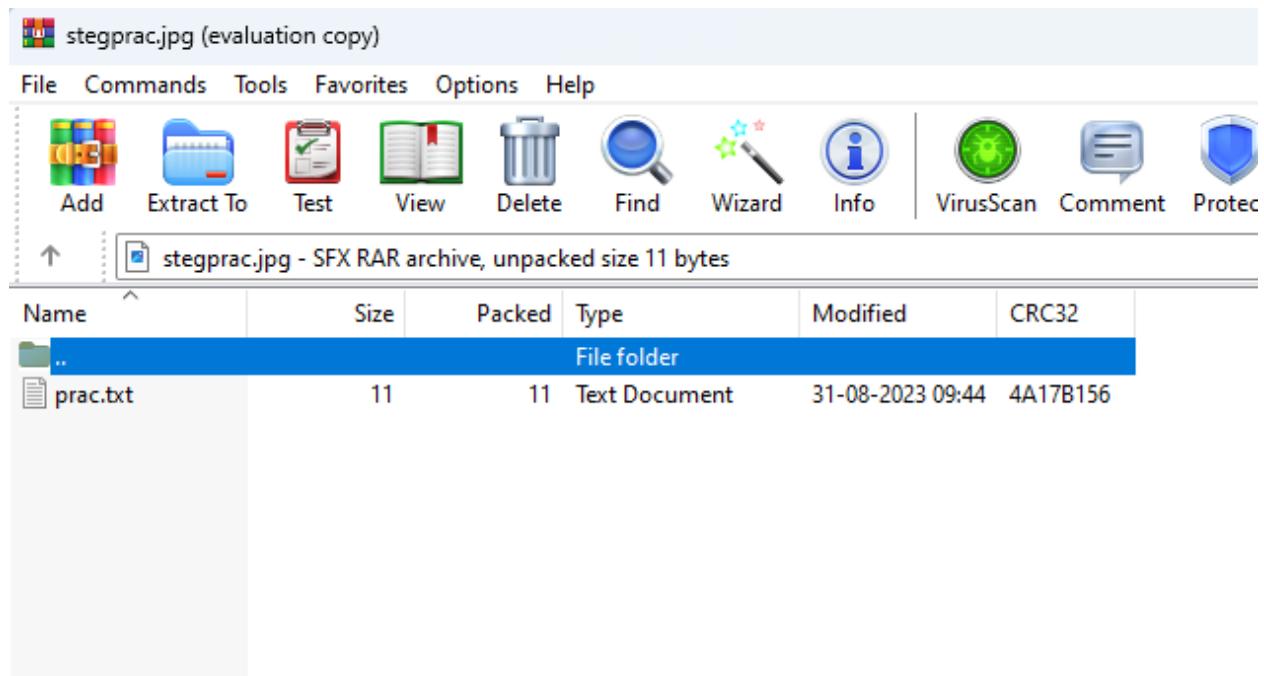


Select Choose another app → choose an app on your pc

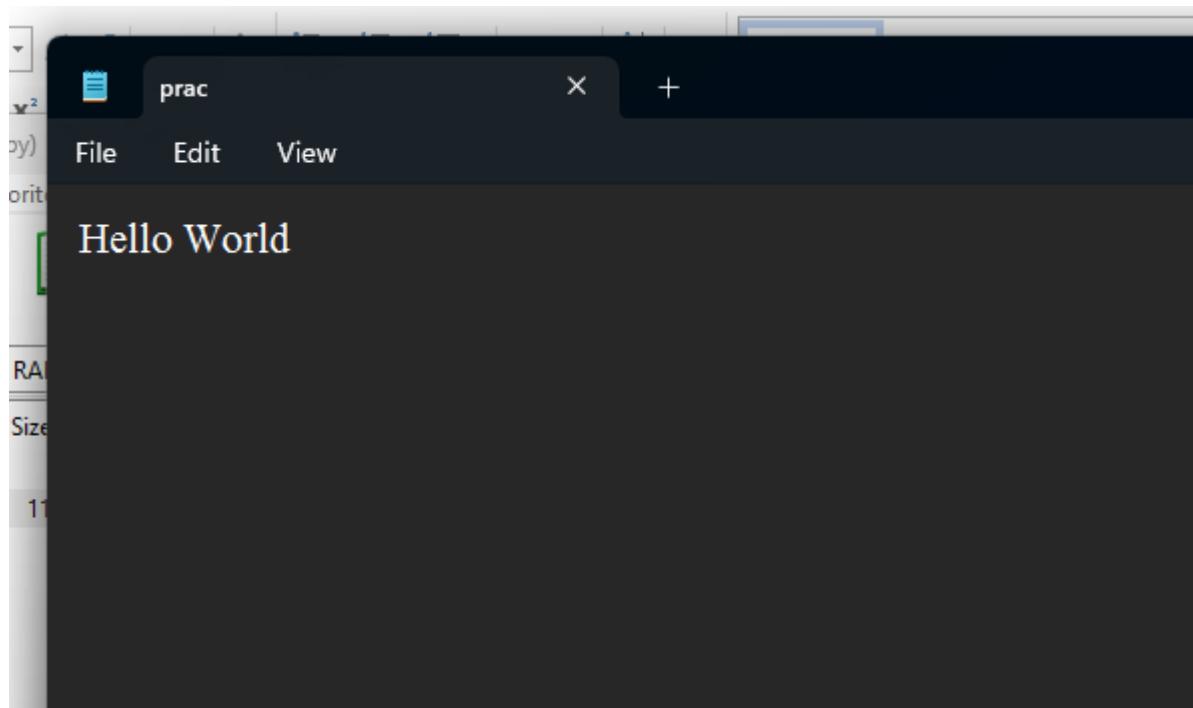


Then Desktop → Shortcut created of WinRAR and Select Just Once





View the Extracted File



## PRACTICAL NO. 8

### Aim:

Mobile Device Forensics

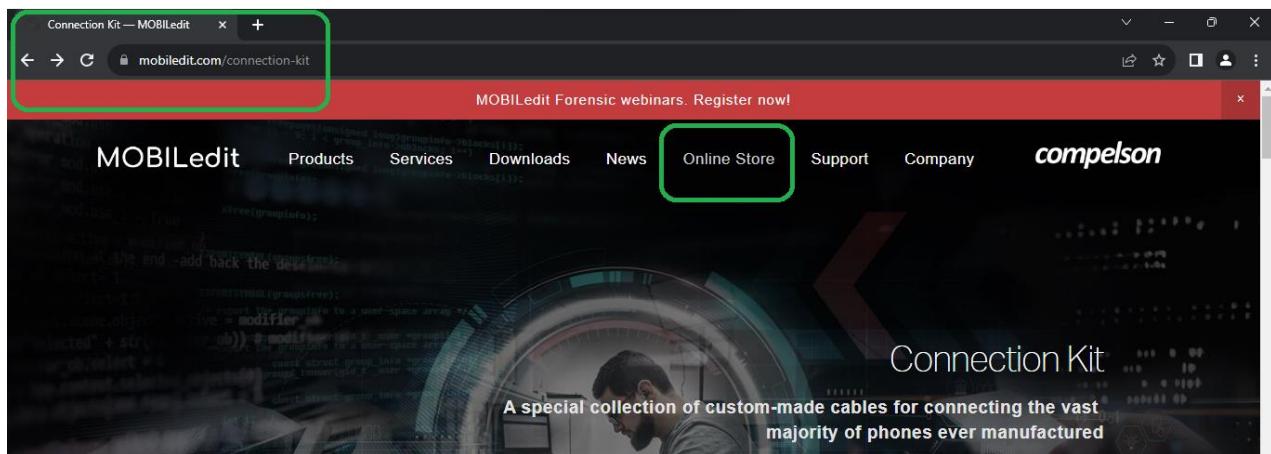
- Perform a forensic analysis of a mobile device, such as a smartphone or tablet.
- Retrieve call logs, text messages, and other relevant data for investigative purposes.

### Practical:

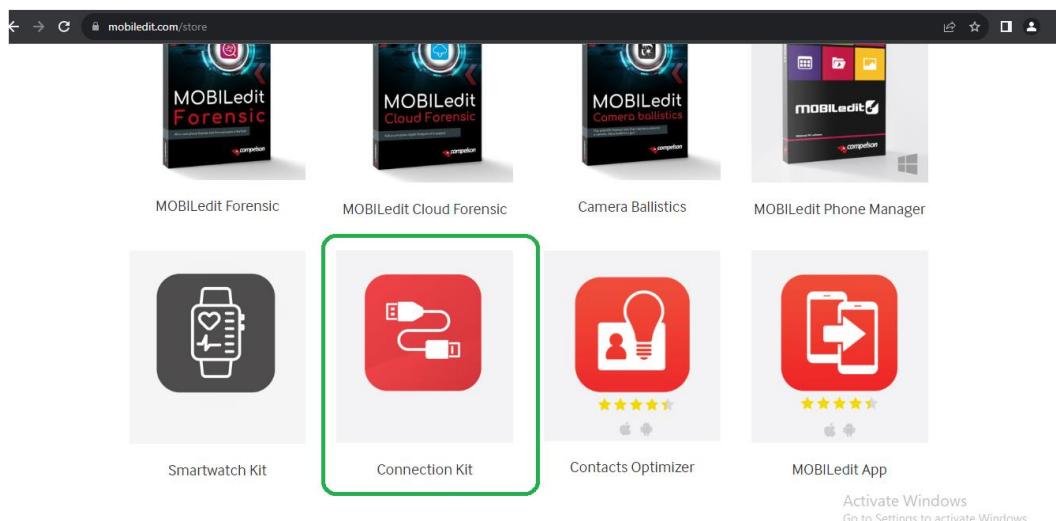
In this Practical we are going to perform the mobile forensic using the MOBILedit Forensic toolkit

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. To the right of the navigation bar is the "compelion" logo. The main content area features a large red square icon containing a white USB cable. To the right of the icon 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. The page has a black header bar with the text "mobileedit.com/store". Below the header is a dark navigation bar with links for Products, Services, Downloads, News, Online Store, Support, and Company. To the right of the navigation bar is the "compelion" logo. The main content area features a search bar with the placeholder "Search" and a "Shopping Cart" icon. Below the search bar is a section titled "Choose a product:" with four software boxes: "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.

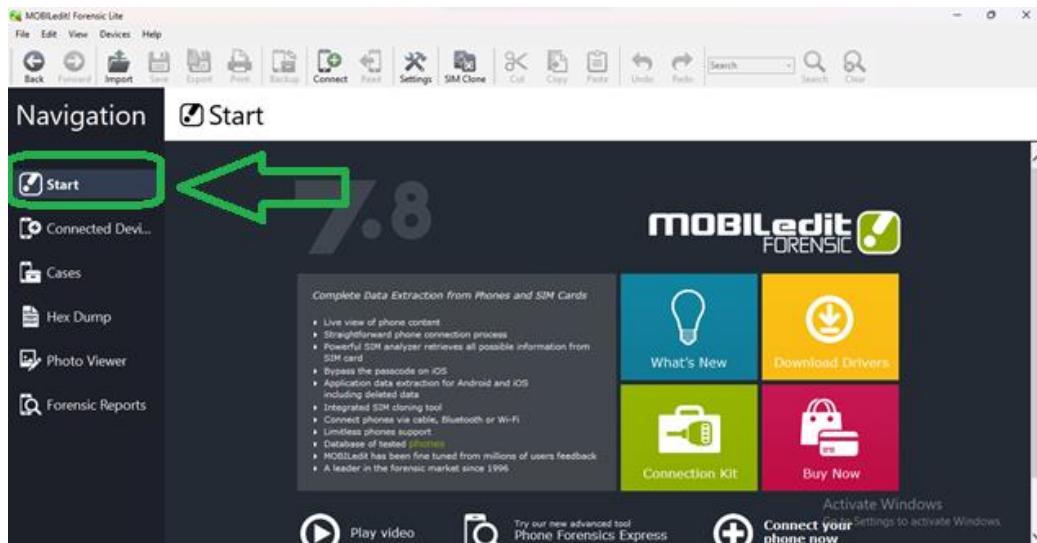
MOBILedit Forensic offers maximum functionality at a fraction of the price of other tools. It can be used as the only tool in a lab or as an enhancement to other tools with its data compatibility. When integrated with Camera Ballistics it scientifically analyzes camera photo origins.

[Learn More](#)

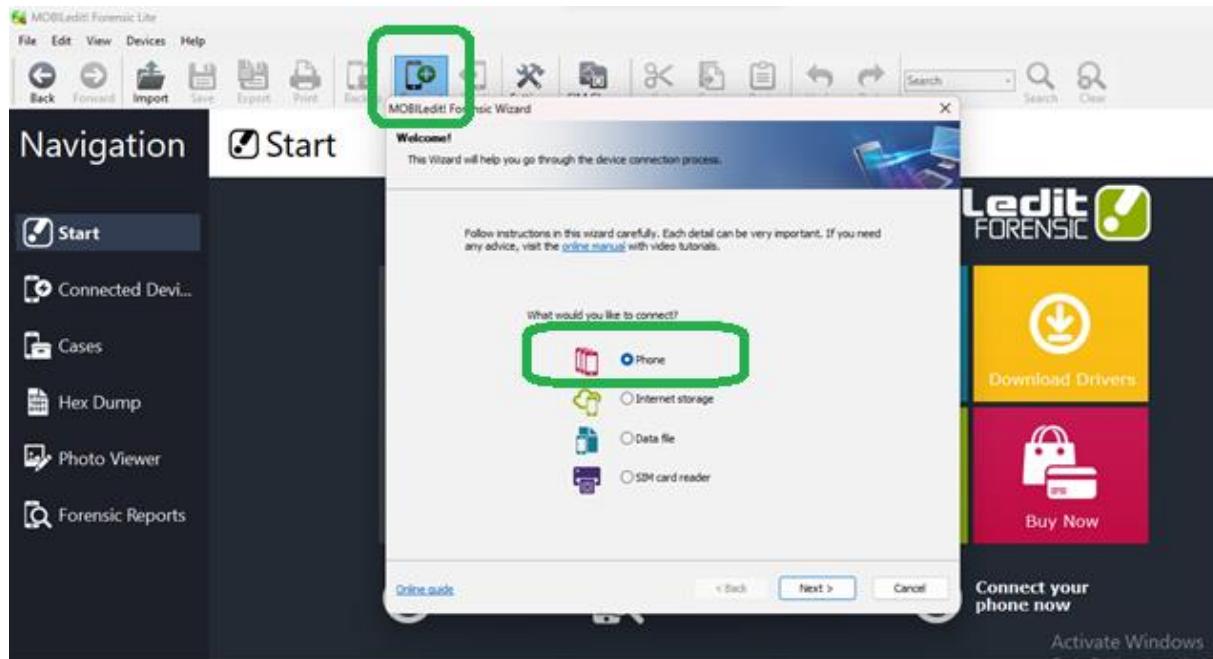
**Activate Windows**  
Go to Settings to activate Windows.

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)

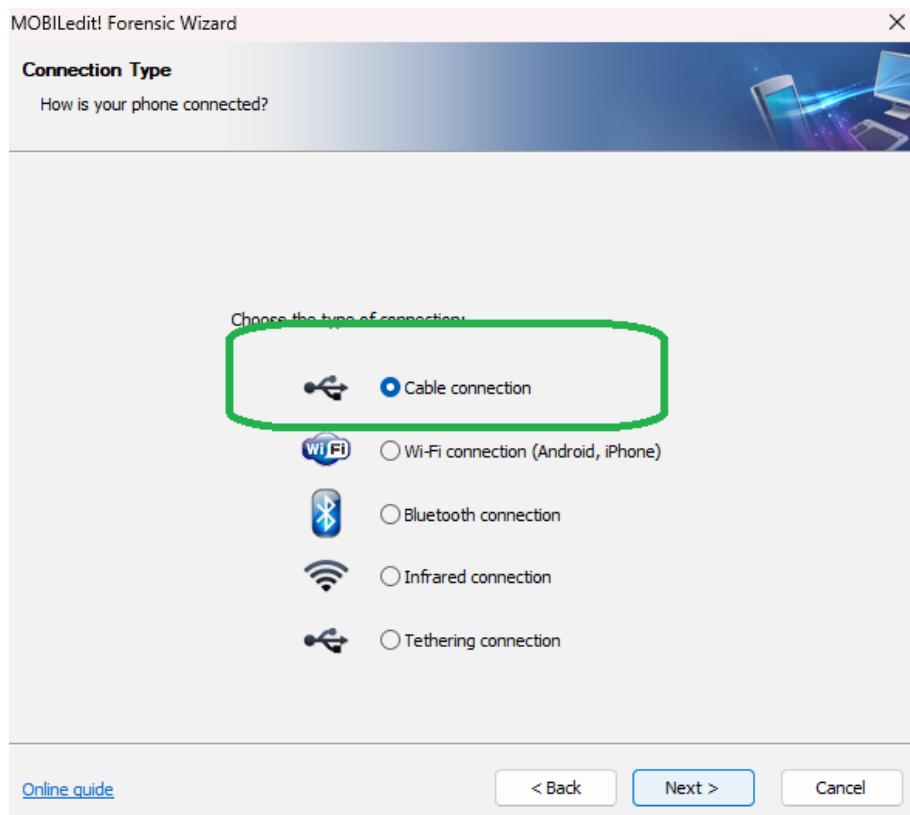
Now we are going to start the Practical

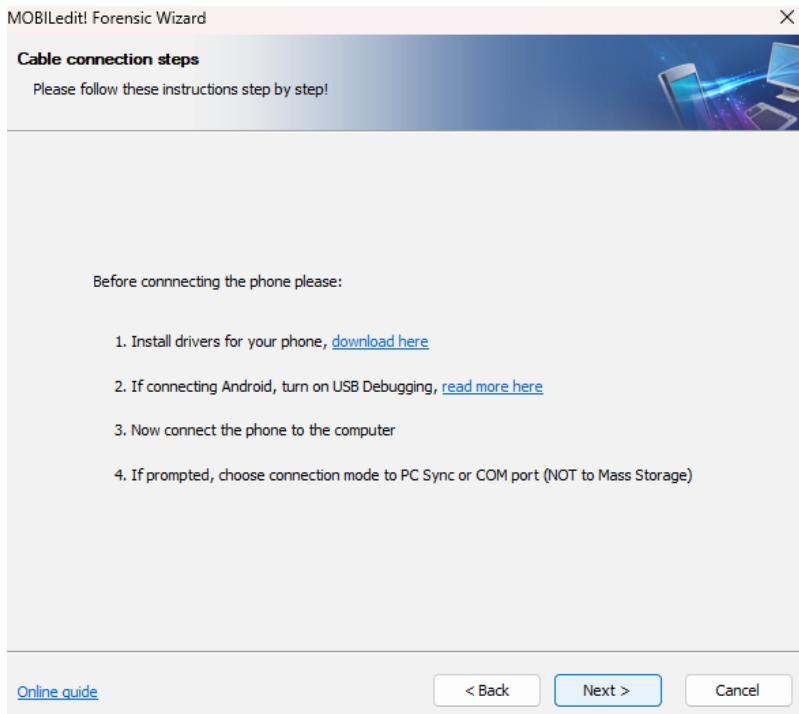


Click on **connect** and Select the type of forensic device to work with. Here we are going with **Phone**

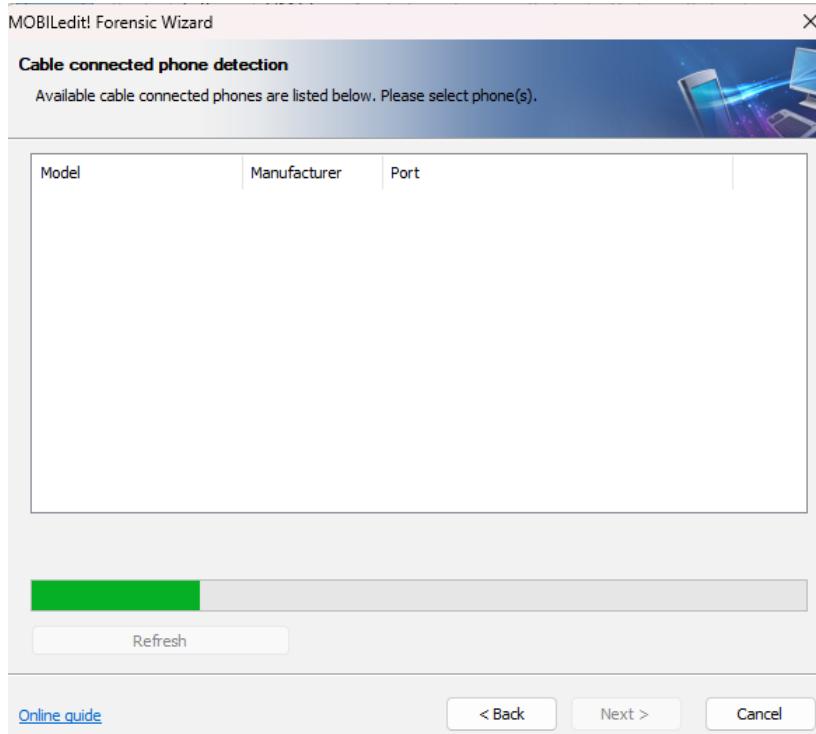


Click Next and Select the type of Connection with the Mobile Phone. Here we are going to Select **Cable Connection** and click Next

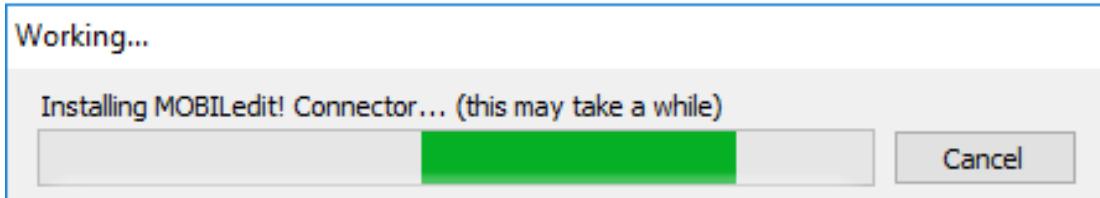
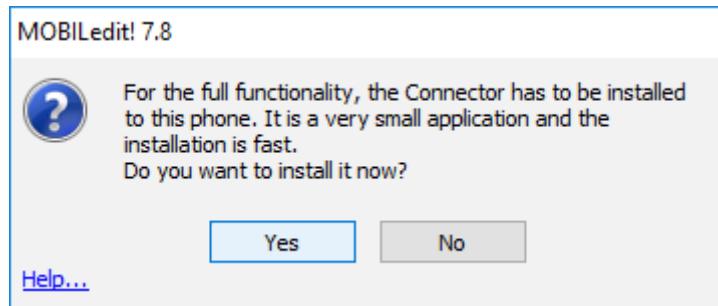




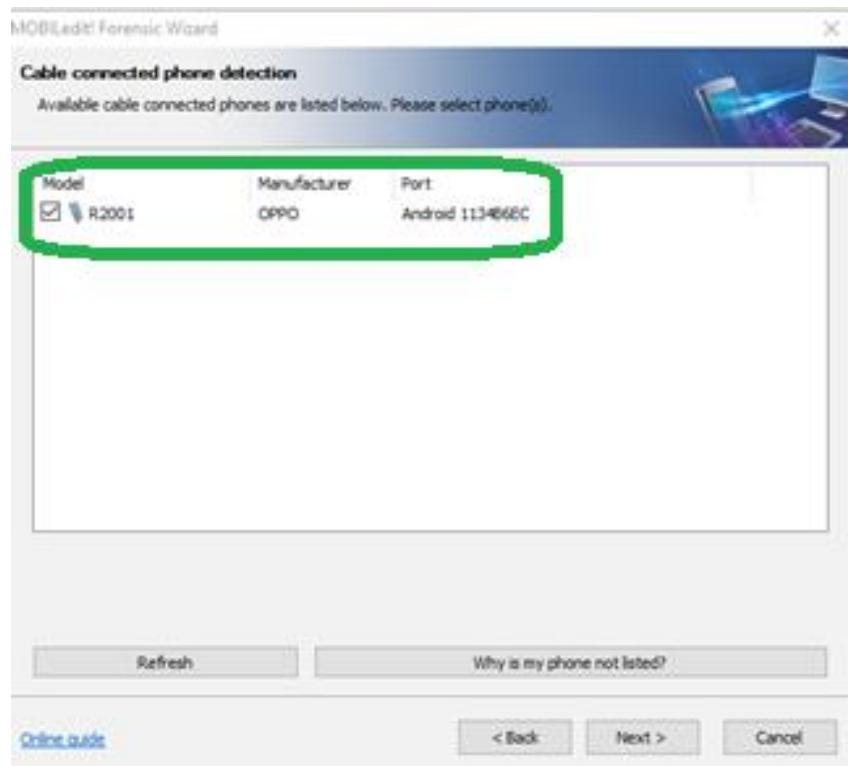
Click Next and let it Scan the Device, If Found click Next, If Not Found Perform these steps and Retry  
**"Go to Phone Settings and open Developer Option and Enable it, and then Allow USB Debugging"**



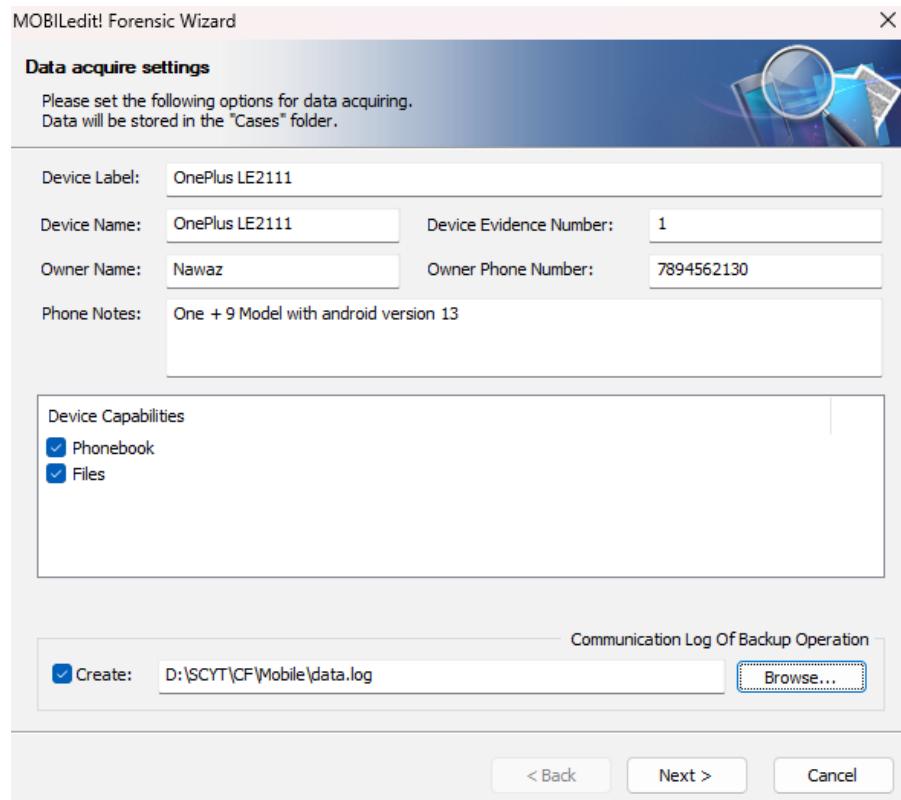
Then connect it with a connector for efficient data recovery



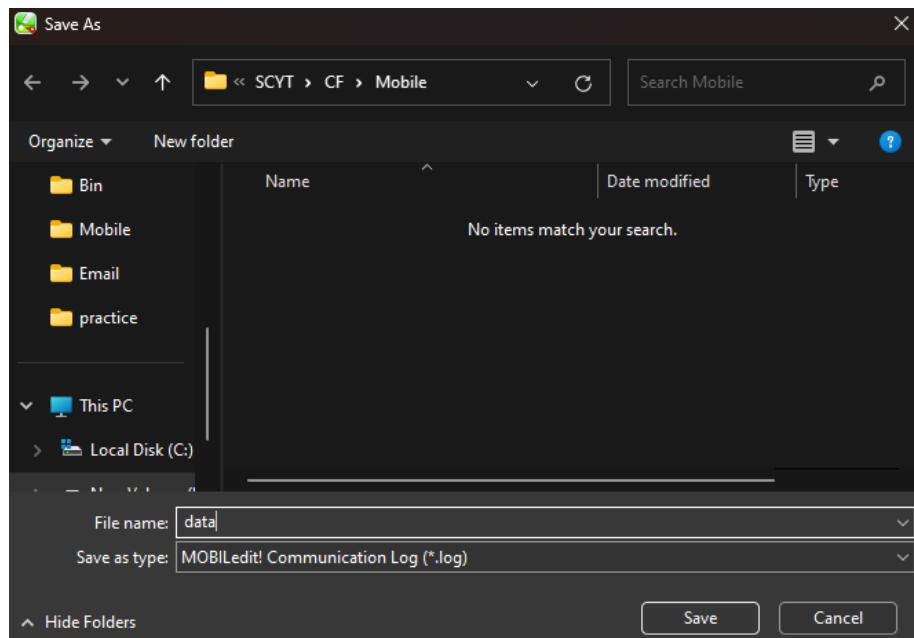
We got a device connected



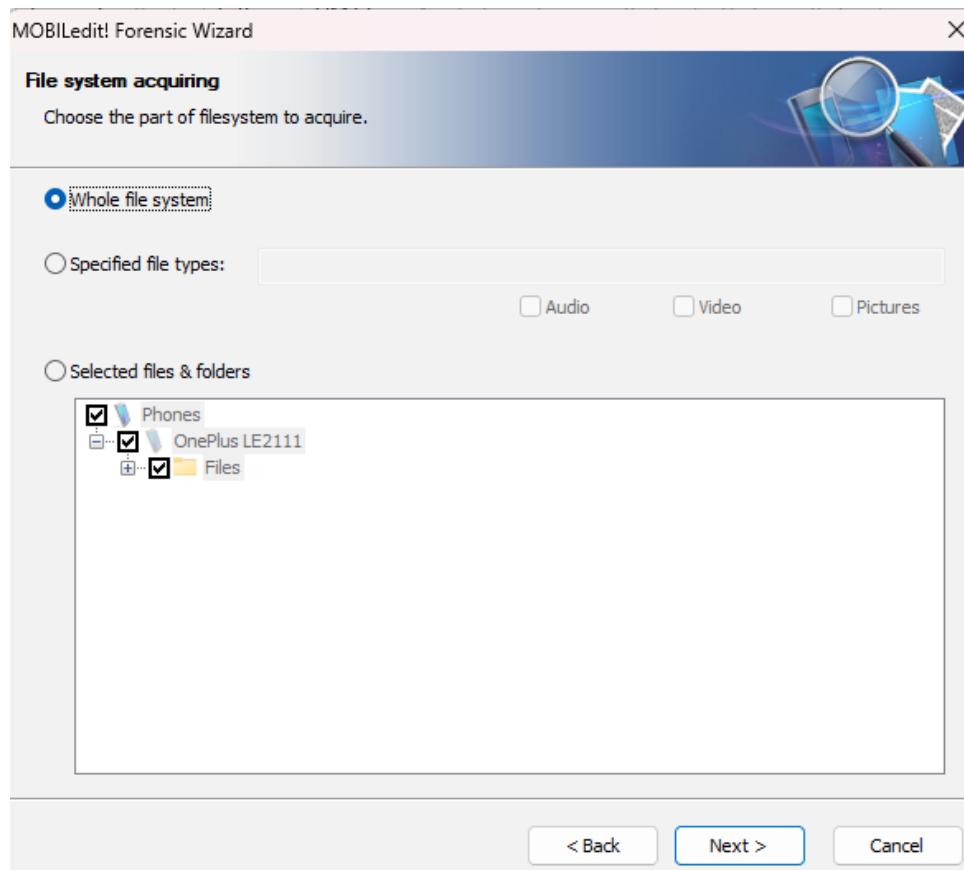
This is the device we are going to use and click on next



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**



RIZVI COLLEGE OF ARTS, SCIENCE AND COMMERCE  
TYBSC CS SEM V – CYBER FORENSIC

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 being processed and their 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: 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

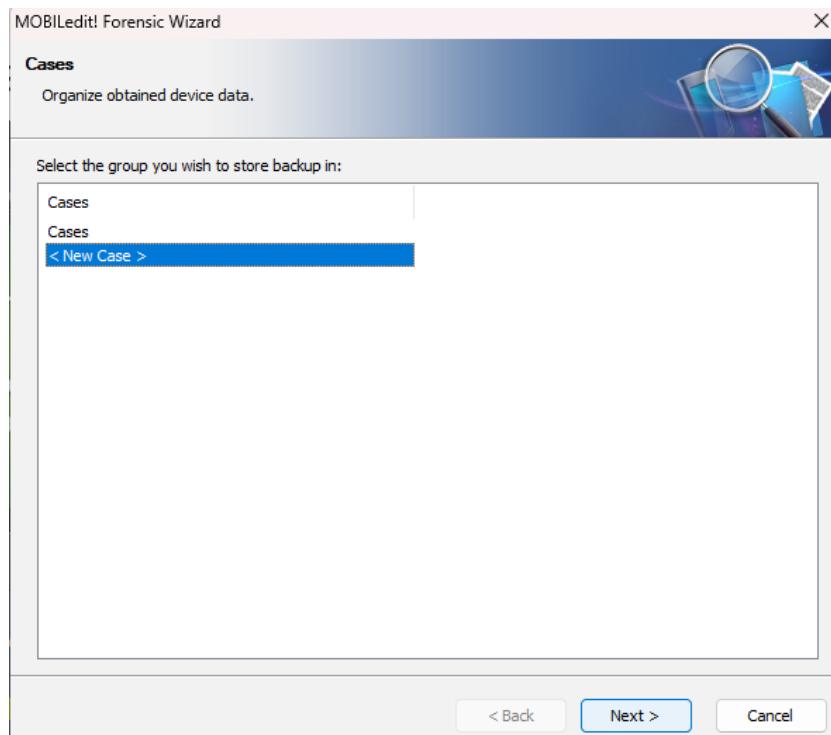
Reading file "Raaghу.2023.1080p.WEB.HDRip.Hindi.HQ.Dub.DD.2.0.x264.mkv" from "OnePlus LE2111"... (28 Stop

**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: 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 "Raaghу.2023.1080p.WEB.HDRip.Hindi.HQ.Dub.DD.2.0.x264.mkv" from "OnePlus LE2111"... (1 sec(s) Stop

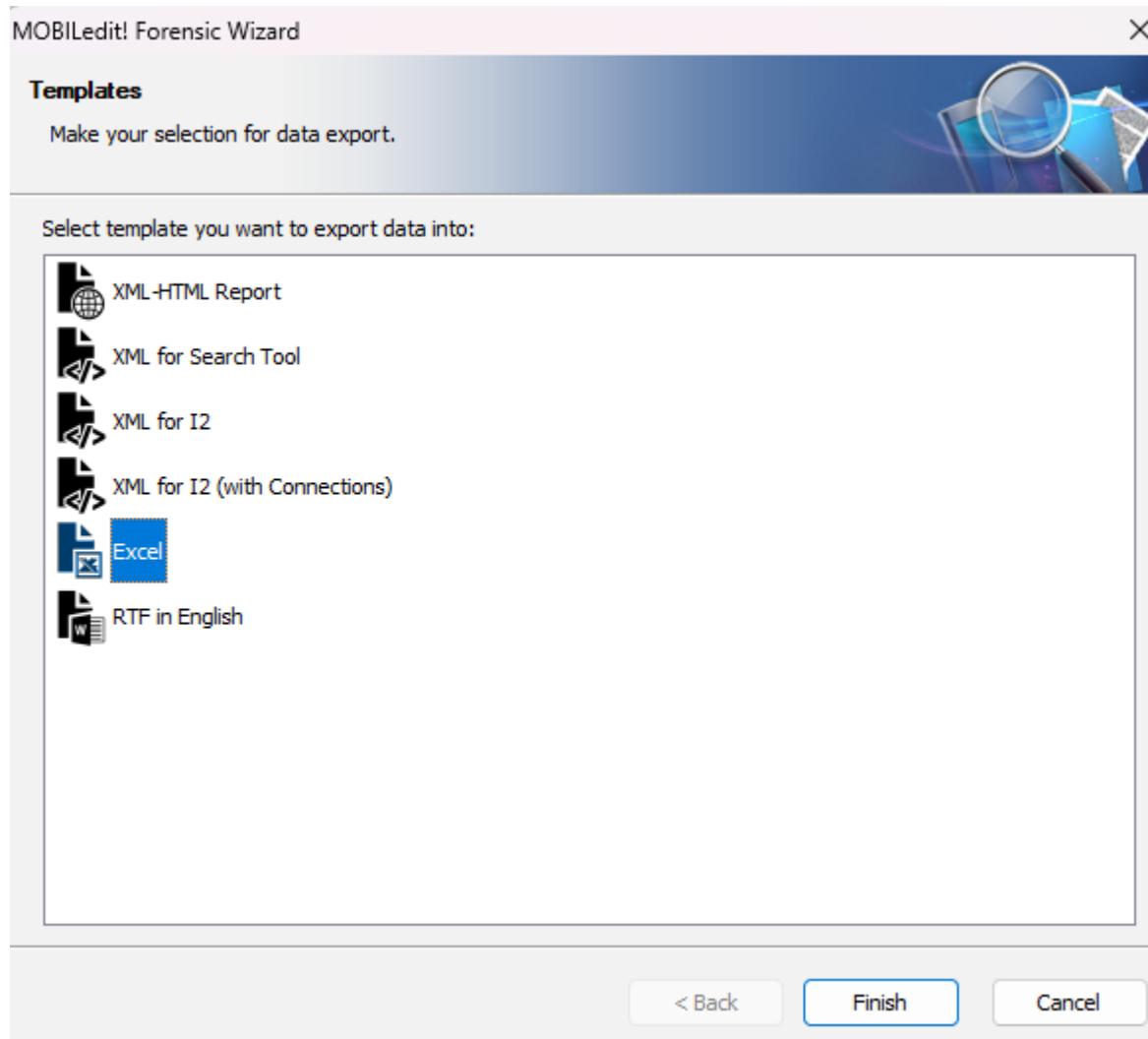
Open the **Case** and **Organize** and decide the **Format** in which we need the **Acquisition**



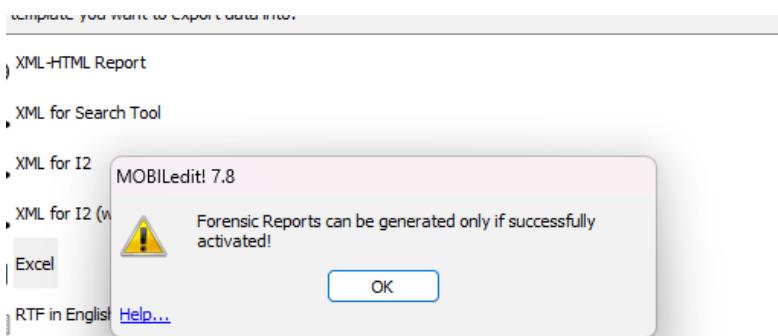
Fill in the details of the Investigator

The screenshot shows the 'New case' configuration screen. The title bar says 'MOBILedit! Forensic Wizard'. Below it, a section titled 'New case' with the sub-instruction 'Create a new case for obtained data.' is visible. On the left, 'Case Details' are listed: 'Label:' with value 'One+9' and 'Number:' with value '130923'. On the right, 'Notes' are listed: 'Performed with 128GB Storage device'. At the bottom, 'Investigator Details' are listed: 'Name:' with value 'Suraj', 'E-mail:' with value 'kaduvettisuraj@gmail.com', and 'Phone Number:' with value '7895461320'. At the very bottom, there 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



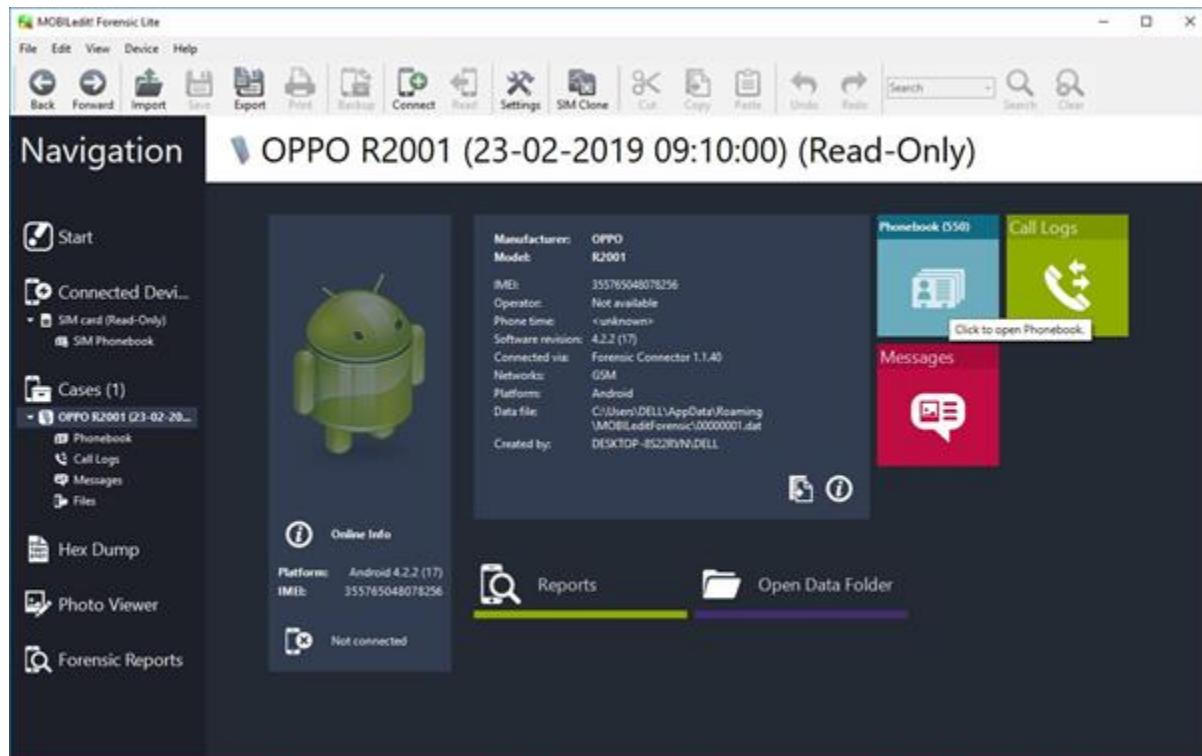
Now we are going to **view** and **analyze** the **data acquired** form the **Performed Acquisition**

We have performed of Two Mobile Devices

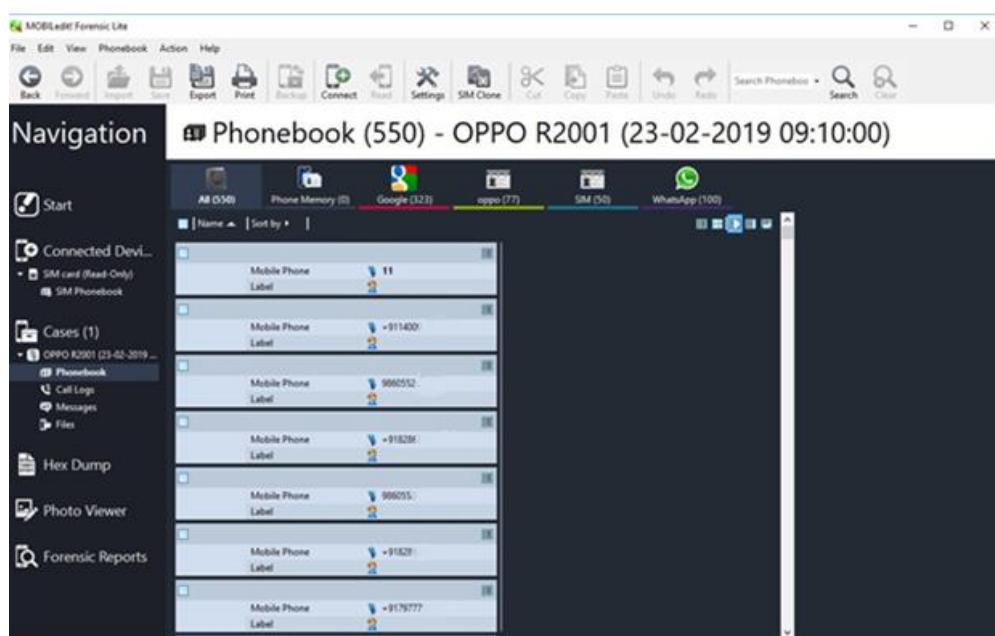
The First One is the Oppo Reno 2

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)**

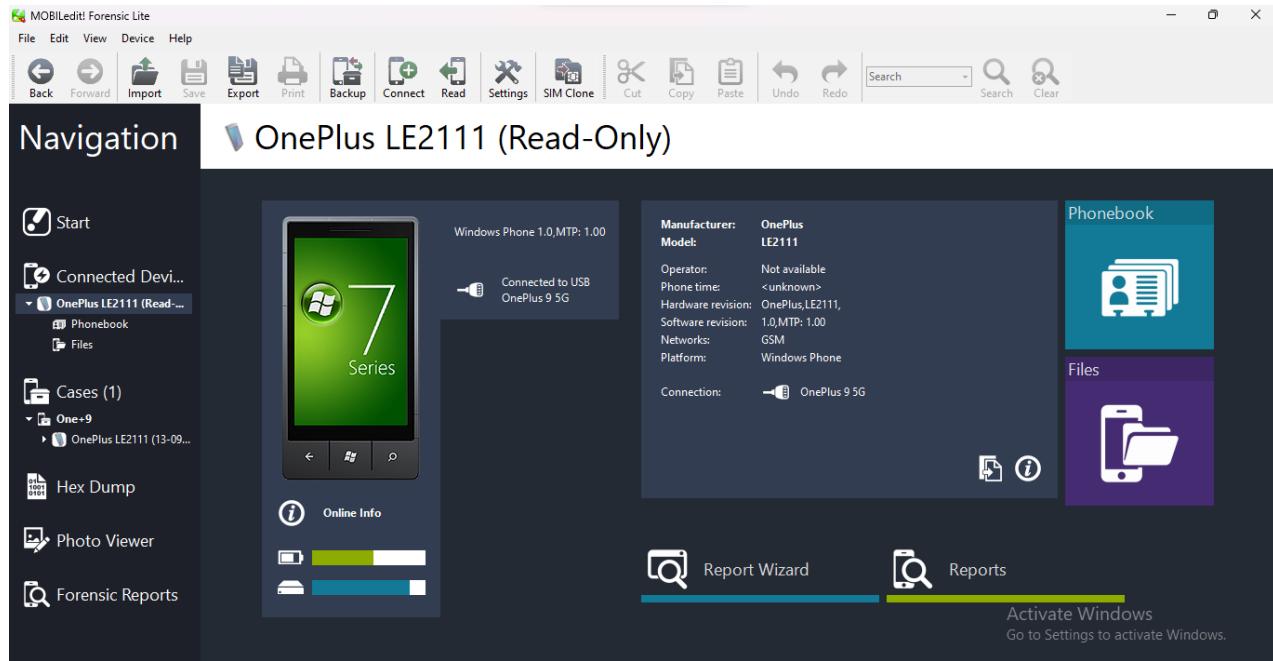
Name	Number	Time
[REDACTED]	+91146	22-02-2019 20:10:12
[REDACTED]	+911400	22-02-2019 16:23:14
[REDACTED]	+9114...	22-02-2019 14:37:00
[REDACTED]	+91141	21-02-2019 15:44:20
Sair	+9199...	20-02-2019 11:38:44
Sai	+919...	20-02-2019 11:29:22
Sak.	+91993...	20-02-2019 10:16:51
[REDACTED]	+9114C	19-02-2019 16:30:13
[REDACTED]	+9122...	19-02-2019 10:04:24
[REDACTED]	+91797...	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

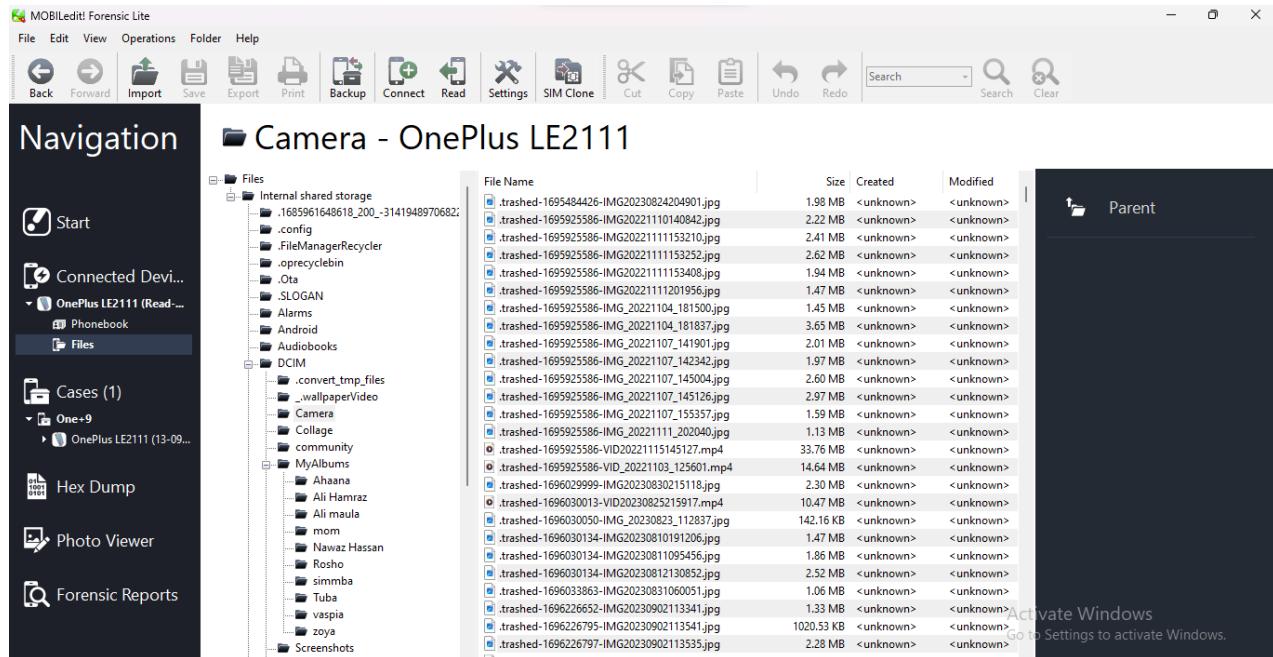
**Messages - OPPO R2001 (23-02-2019 09:10:00)**

Sender / Recipient	Date	Time
IDEA	23-02-2019	08:25:27
Aaa [REDACTED]	22-02-2019	20:59:25
IM-65 [REDACTED]	22-02-2019	17:19:31
IM-612 [REDACTED]	22-02-2019	14:46:43
IM-65 [REDACTED]	22-02-2019	14:15:48
+919981 [REDACTED]	21-02-2019	10:34:12
MD-K [REDACTED]	21-02-2019	16:44:12
AX-IY [REDACTED]	21-02-2019	12:05:36
IM-657 [REDACTED]	21-02-2019	12:05:36
[REDACTED]	23-02-2019	08:25:27
Drafts (1)	23-02-2019	08:25:27
[REDACTED]	22-02-2019	14:03:05
[REDACTED]	22-02-2019	08:25:27
[REDACTED]	22-02-2019	08:25:27
[REDACTED]	21-02-2019	14:03:26
[REDACTED]	21-02-2019	08:19:34
[REDACTED]	20-02-2019	12:31:37
[REDACTED]	26-01-2019	09:09:37

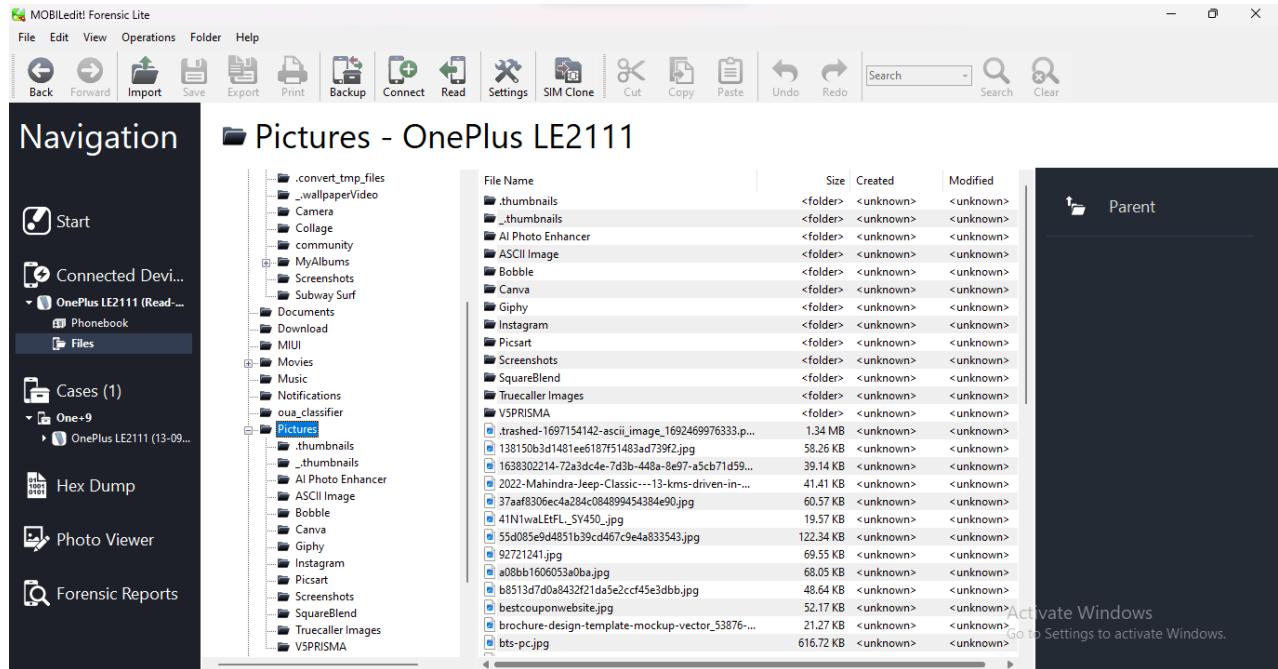
### Display of the Second Device One⁺ 9



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.

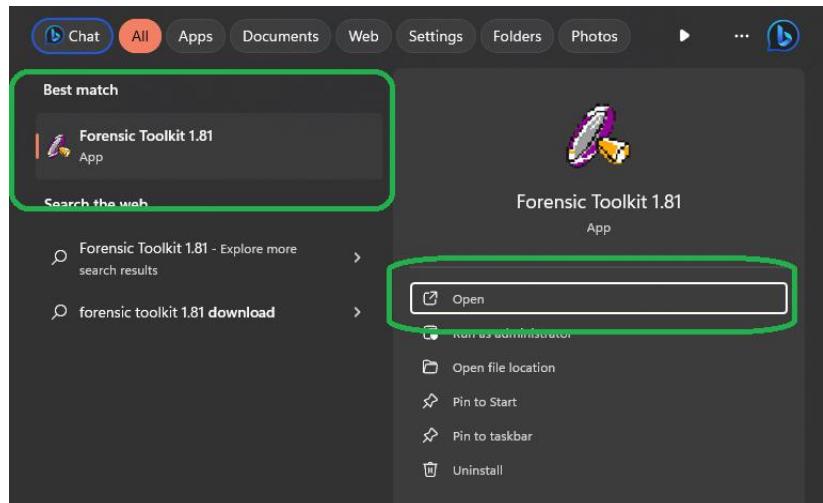
Martha asked her CIO, to have an IT employee copy the Outlook .pst file from Jim Shu's old computer to a USB drive.

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.

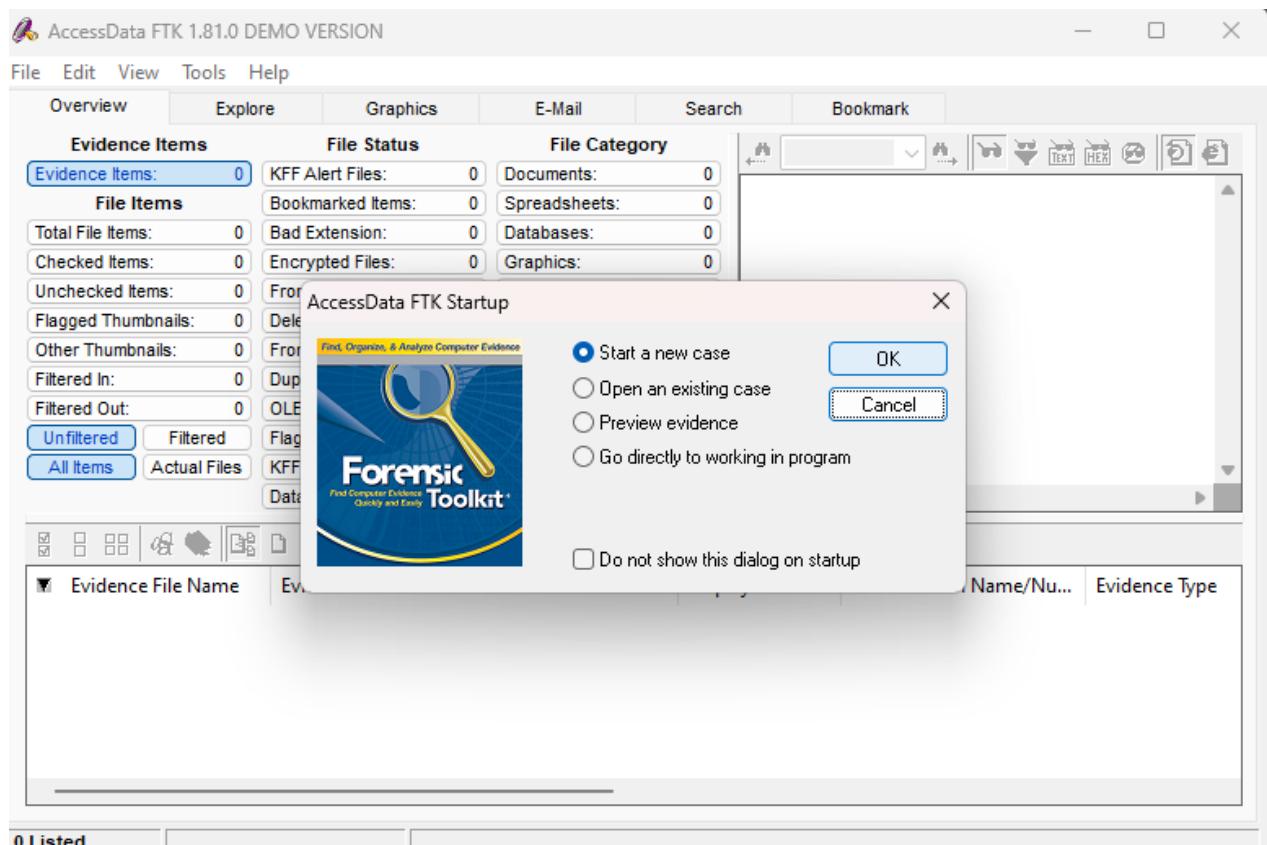
Recovering Email

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**



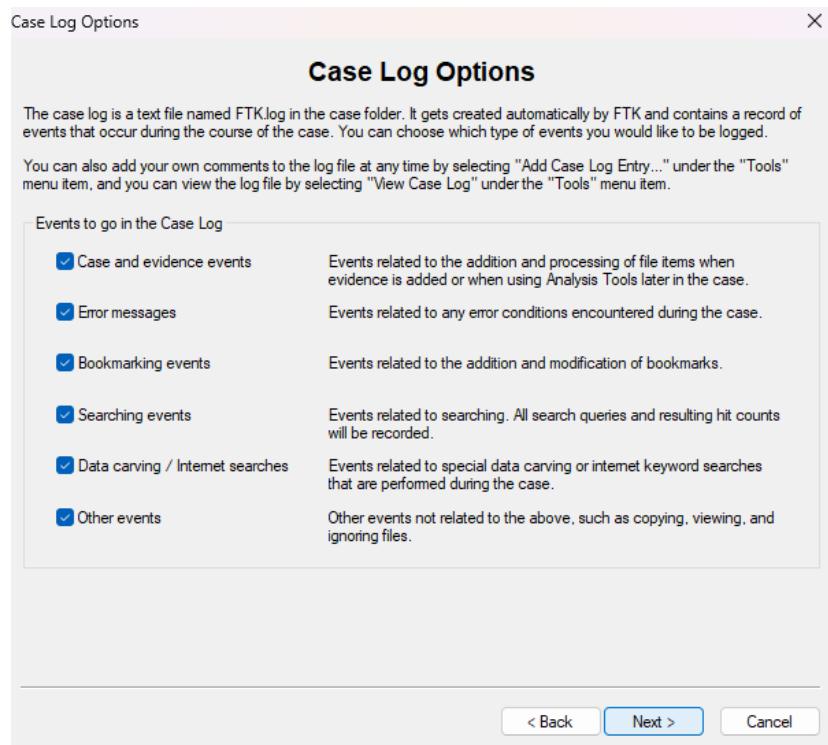
Create a new File



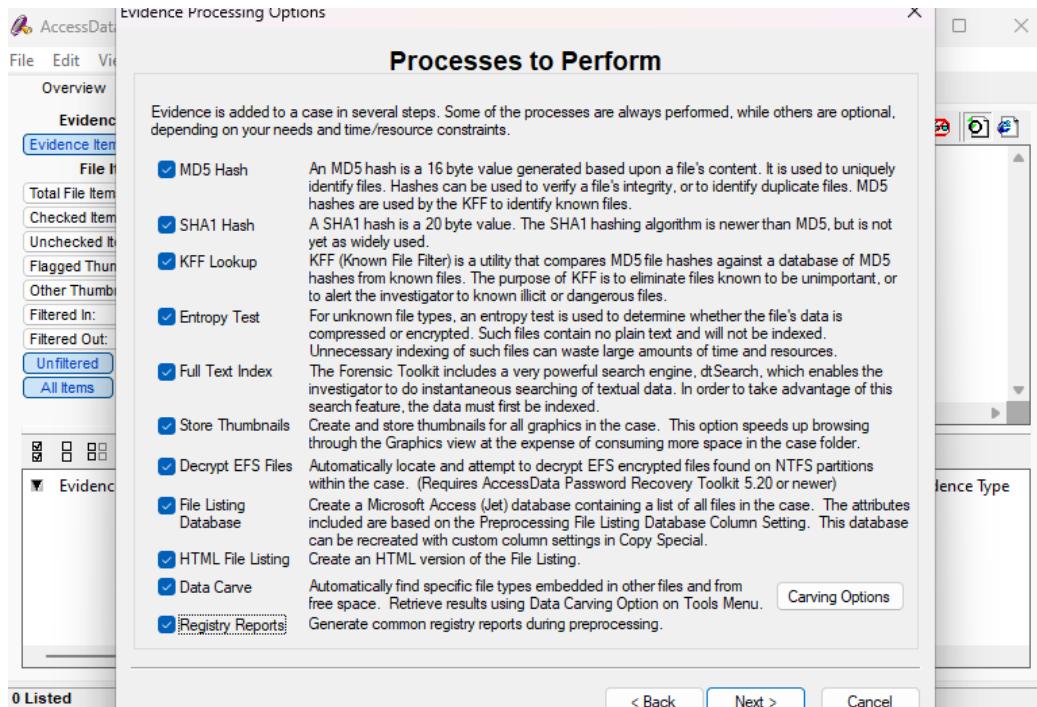
Fill the details of the Examiner

The screenshot shows the 'FTK Report Wizard - Case Information' dialog. The title bar says 'FTK Report Wizard - Case Information'. The main section is titled 'Forensic Examiner Information' with the sub-instruction 'The following information will appear on the Case Information page of the report:'. There are several input fields: 'Agency/Company:' with the value 'rizvi', 'Examiner's Name' dropdown set to 'Aamir', 'Address:' with the value 'Carter Road, Bandra, Mumbai', 'Phone:' with the value '9876452310', 'Fax:' empty, 'E-Mail:' with the value 'aamir10@gmail.com', and 'Comments:' with the value 'email analysis'. At the bottom are navigation buttons: '< Back', 'Next >', and 'Cancel'.

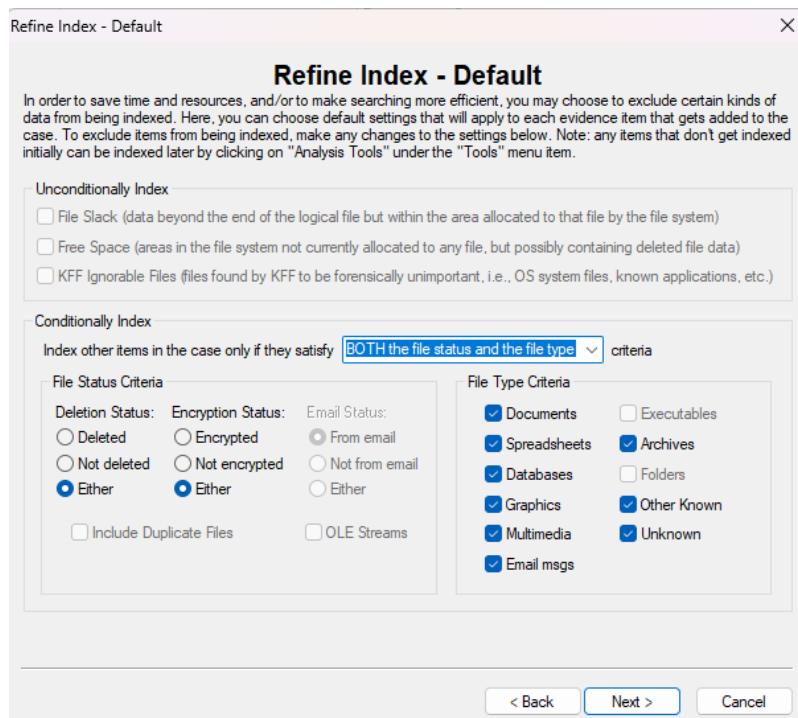
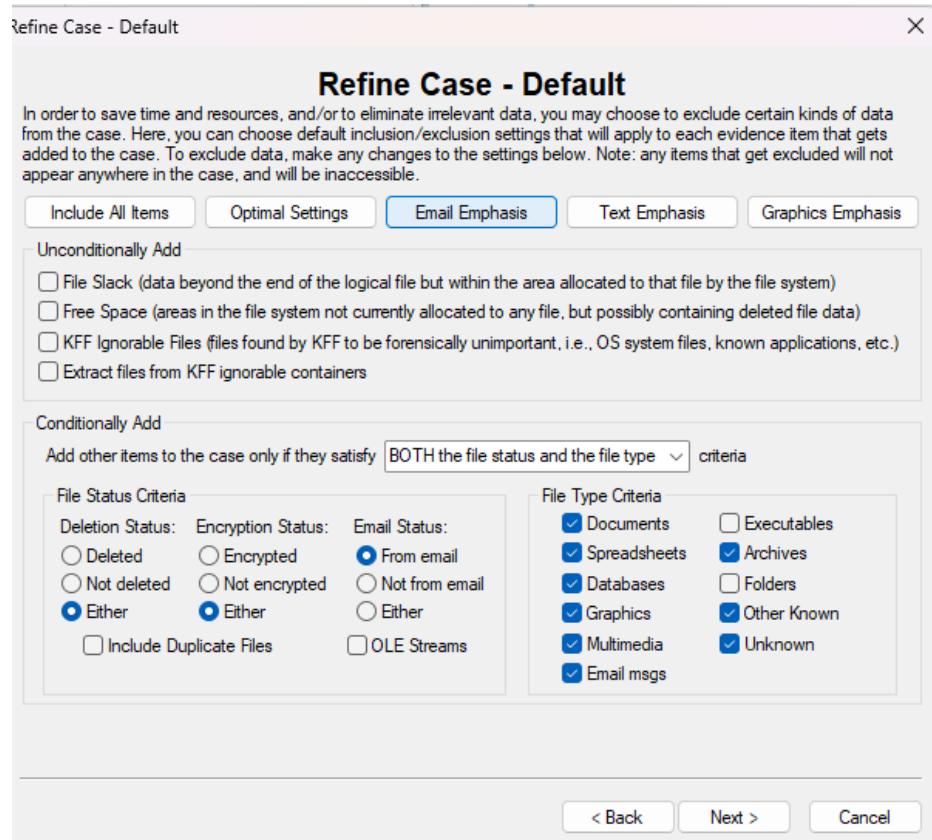
Click on all the options and Click Next



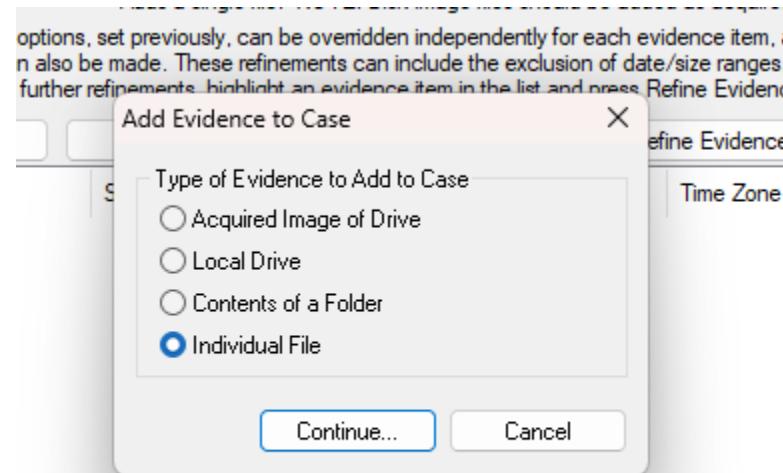
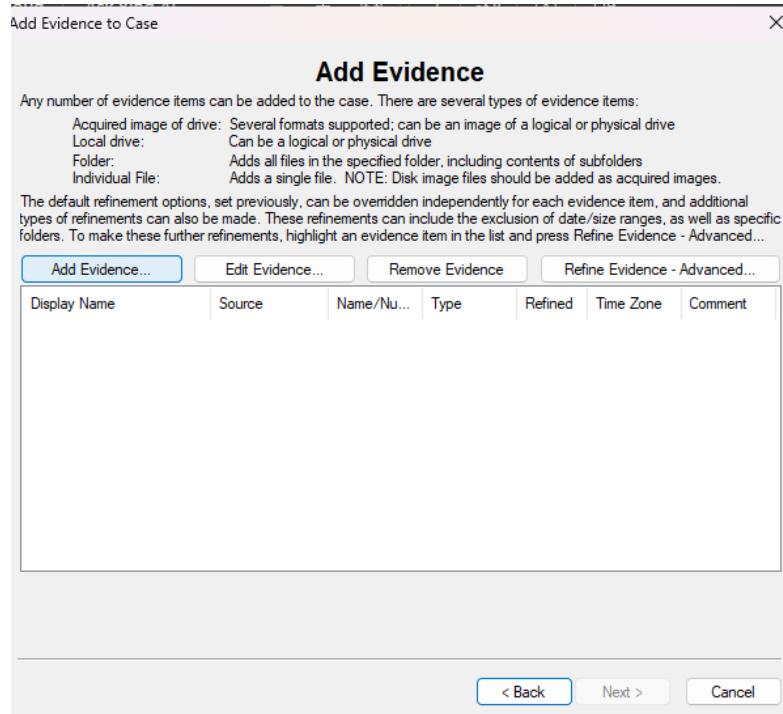
Select all the options



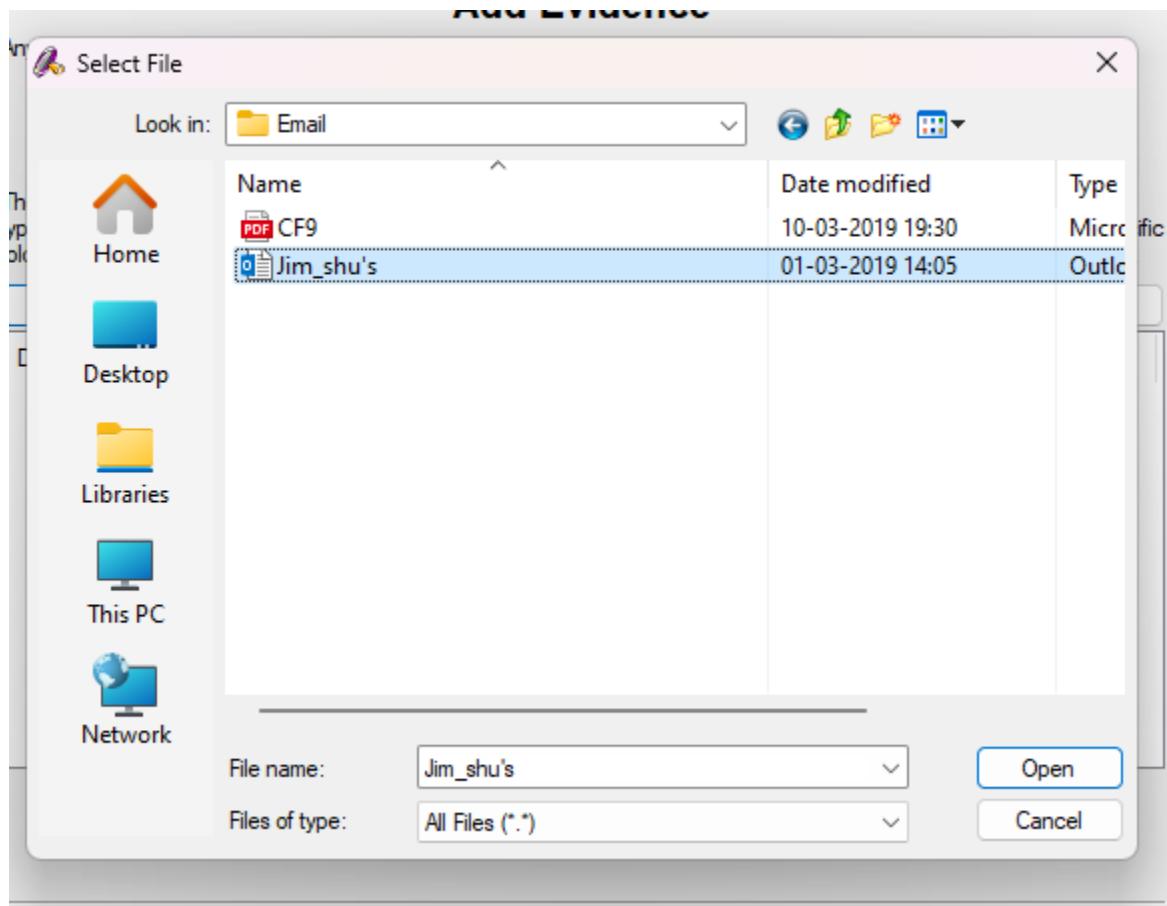
Now we have reached the Email Emphasis section



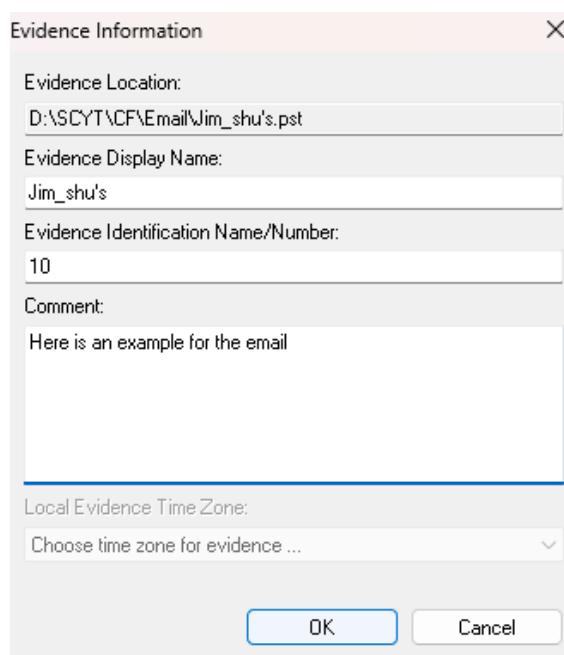
Click Next until you reach the **Add Evidence to Case dialog box**, and then click the **Add Evidence button**. In the **Add Evidence to Case dialog box**, click the **Individual File option button**, and then click **Continue**.



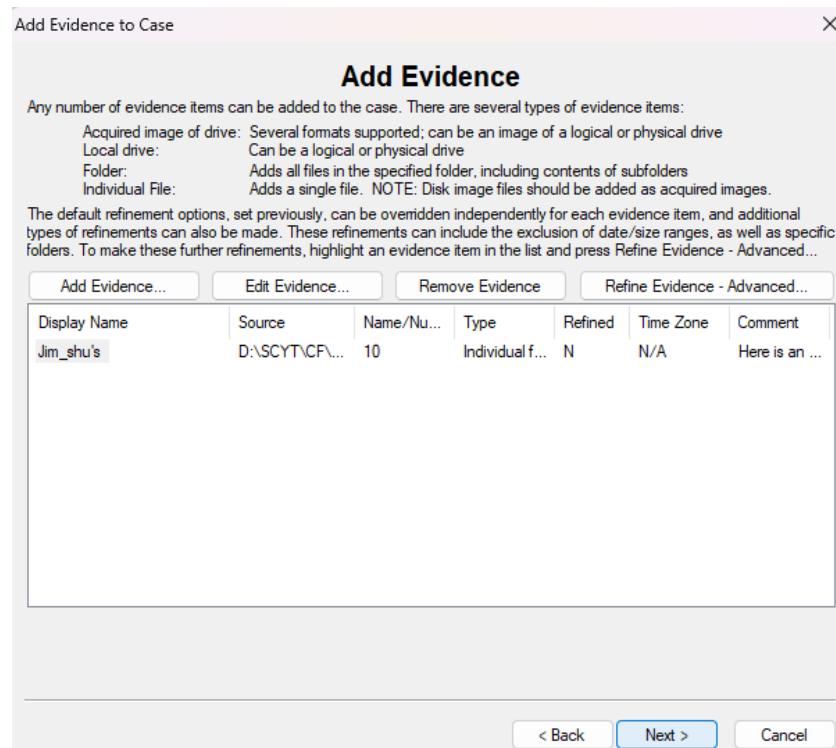
In the Select File dialog box, navigate to your work folder, click the Jim_shu's.pst file, and then click Open.



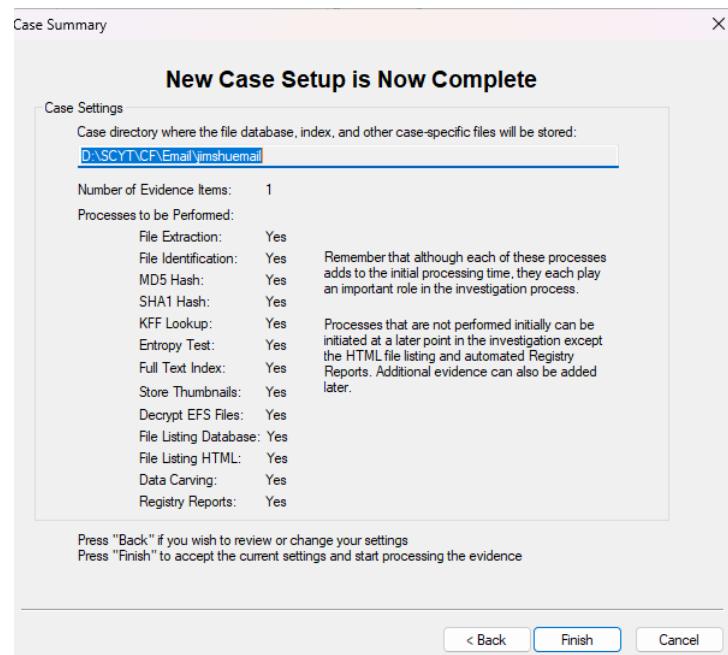
Give some data



Complete the steps and Click on Next



Click on finish and see the data



The screenshot shows the AccessData FTK 1.81.0 DEMO VERSION interface. The main window displays various evidence items and their status. On the left, there's a sidebar with tabs for Overview, Explore, Graphics, E-Mail, Search, and Bookmark. The Overview tab is selected. Below it, the Evidence Items section shows a count of 1 item. The File Status section lists items like KFF Alert Files (0), Bookmarked Items (0), and E-mail Messages (32). The File Category section lists categories like Documents (1), Spreadsheets (0), and E-mail Messages (32). The bottom part of the interface is a table showing detailed information about the single evidence item:

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

At the bottom, status indicators show 1 Listed, 0 Checked Total, and 0 Highlighted.

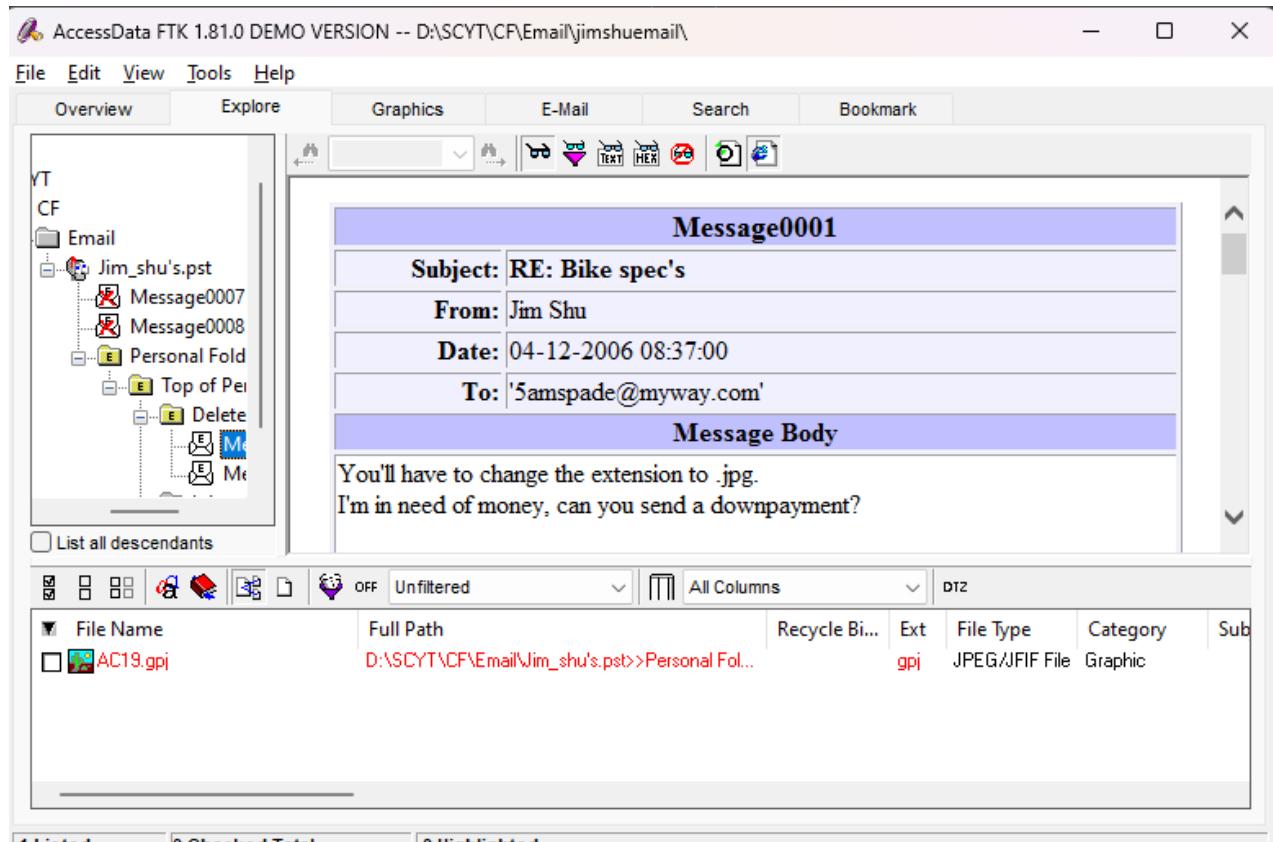
When the Add Evidence to Case dialog box opens, click Next. In the Case summary dialog box, click Finish. When FTK finishes processing the file, in the main FTK window, click the Email Messages button, and then click the Full Path column header to sort the records.

**Evidence Items:** 1 **KFF Alert Files:** 0 **Documents:** 1  
**Total File Items:** 40 **Bookmarked Items:** 0 **Spreadsheets:** 0  
**Checked Items:** 0 **Bad Extension:** 1 **Databases:** 0  
**Unchecked Items:** 40 **From E-mail:** 40 **ImageFiles:** 0  
**Flagged Thumbnails:** 0 **Deleted Files:** 0 **E-mail Messages:** 32  
**Other Thumbnails:** 1 **From Recycle Bin:** 0 **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

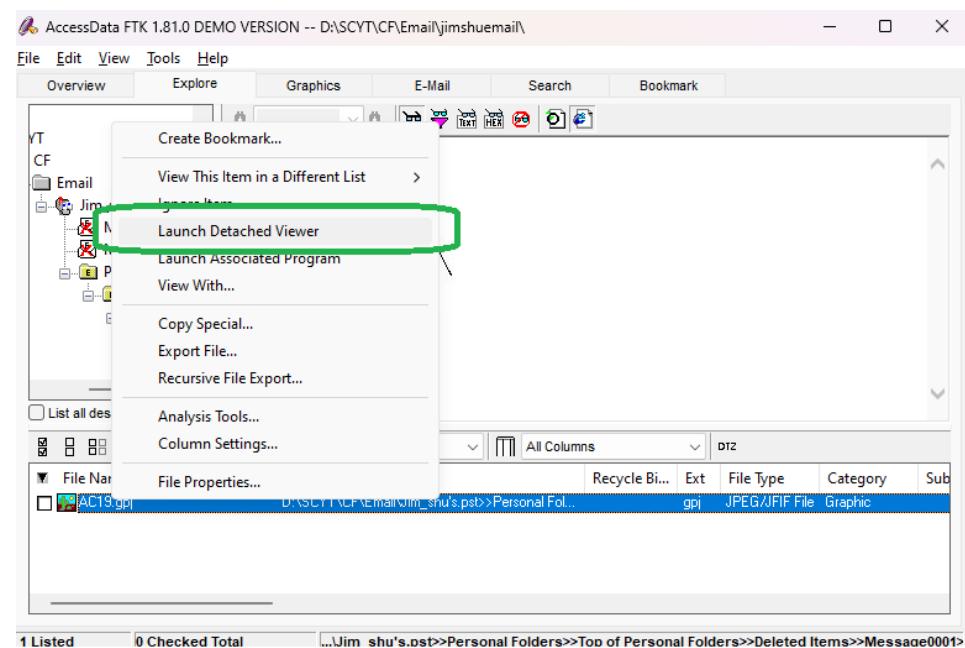
File Name	Full Path	Recycle Bi...	Ext	File Type	Category
Message0001	D:\SCYT\CF\Email\Jim_shu's.pst>>Personal Fol...			E-mail Messa...	E-mail
Message0001	D:\SCYT\CF\Email\Jim_shu's.pst>>Personal Fol...			E-mail Messa...	E-mail
Message0001	D:\SCYT\CF\Email\Jim_shu's.pst>>Personal Fol...			E-mail Messa...	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
Message0002	D:\SCYT\CF\Email\Jim_shu's.pst>>Personal Fol...			E-mail Messa...	E-mail

32 Listed | 0 Checked Total | 0 Highlighted

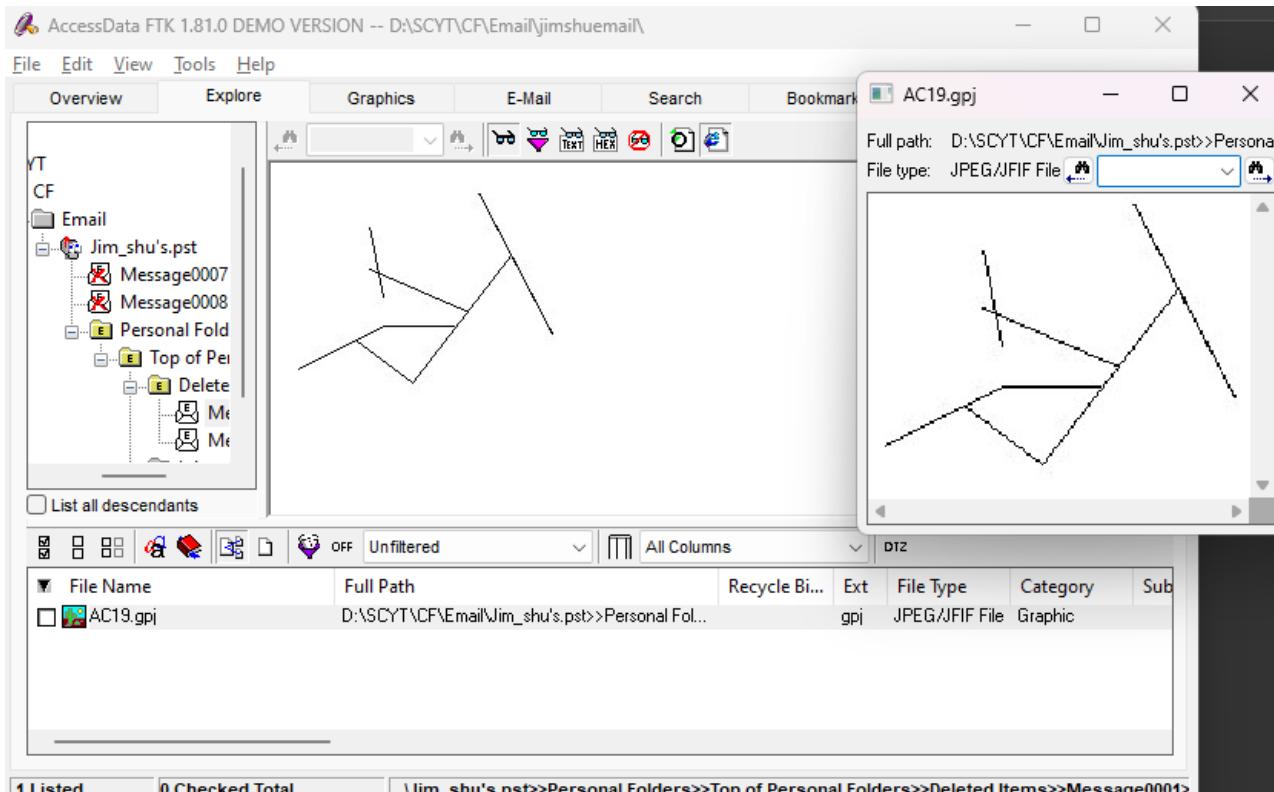
For email recovery follow following steps: Click the E-Mail tab. In the tree view, click to expand all folders, and then click the Deleted Items folder.



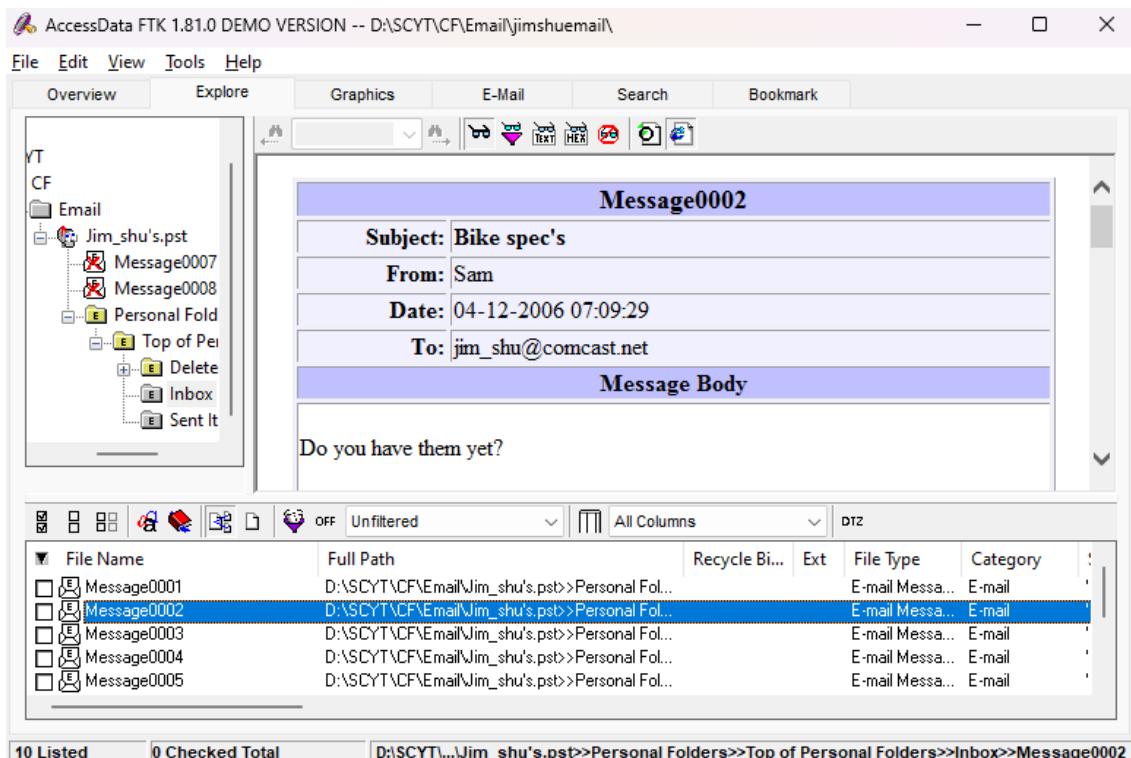
Select any message say Message0001 right click and select option Launch Detached Viewer and you can see detail of deleted message.



RIZVI COLLEGE OF ARTS, SCIENCE AND COMMERCE  
TYBSC CS SEM V – CYBER FORENSIC

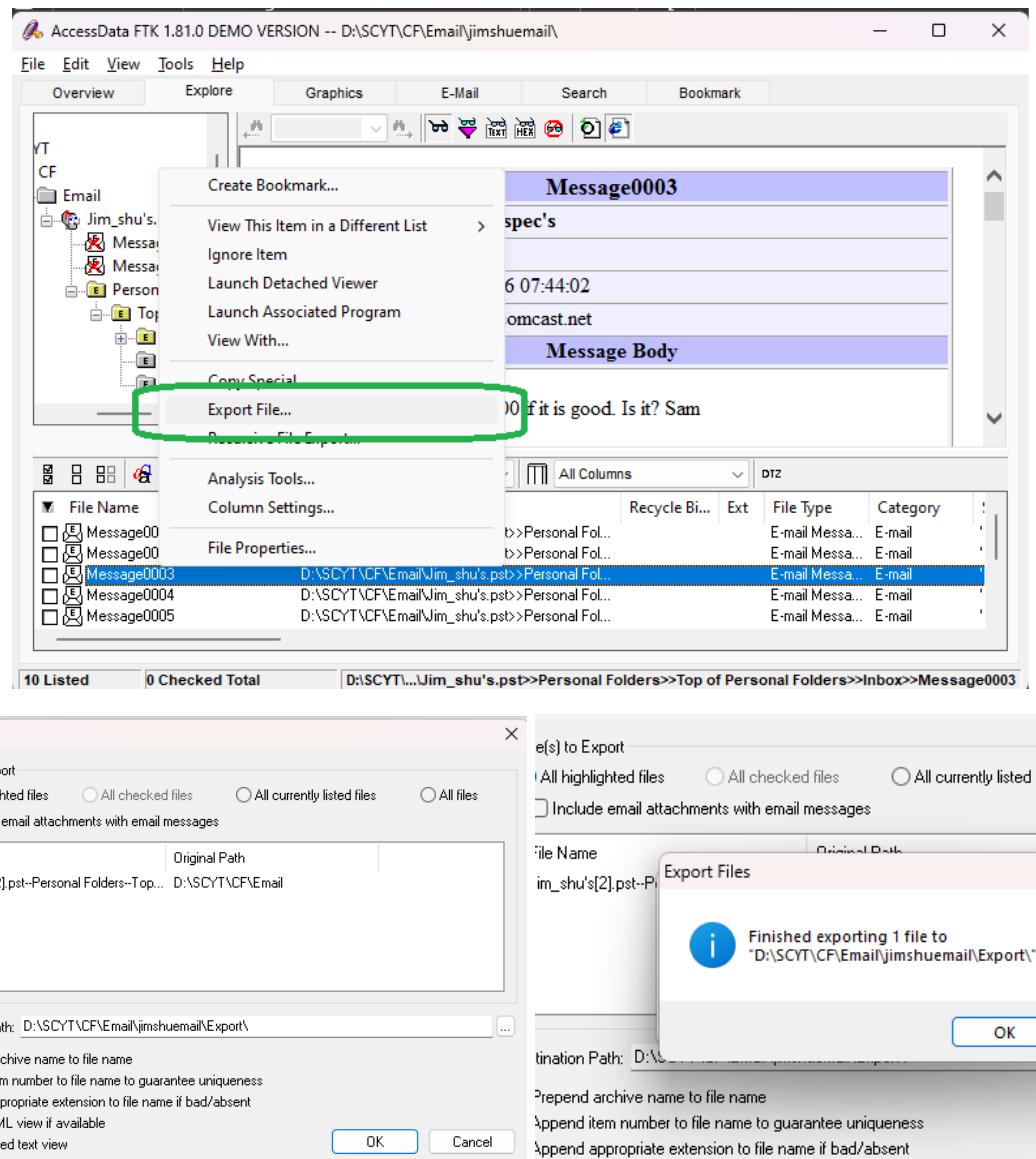


For analyzing header follow following steps: Click the E-Mail tab. In the tree view, click to expand all folders, and then click the Inbox folder. In the File List pane at the upper right, click Message0003; as shown in the pane at the bottom, it's from Sam and is addressed to [Jim_shu@comcast.net](mailto:jim_shu@comcast.net).

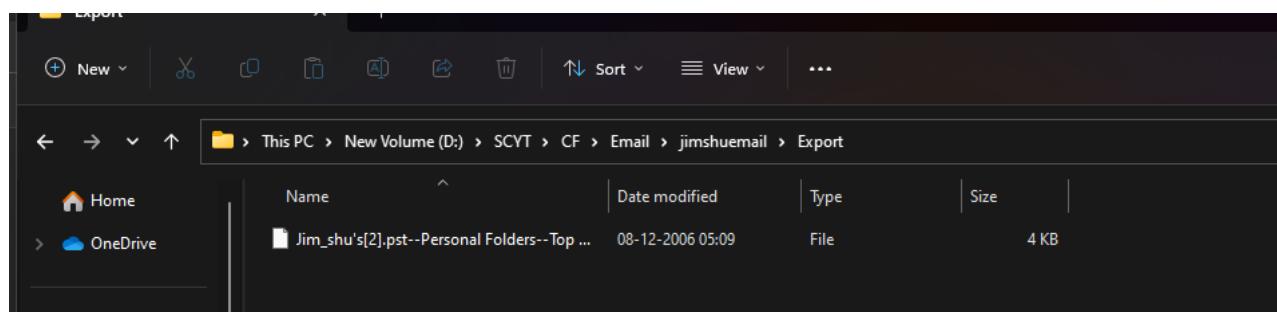


RIZVI COLLEGE OF ARTS, SCIENCE AND COMMERCE  
TYBSC CS SEM V – CYBER FORENSIC

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

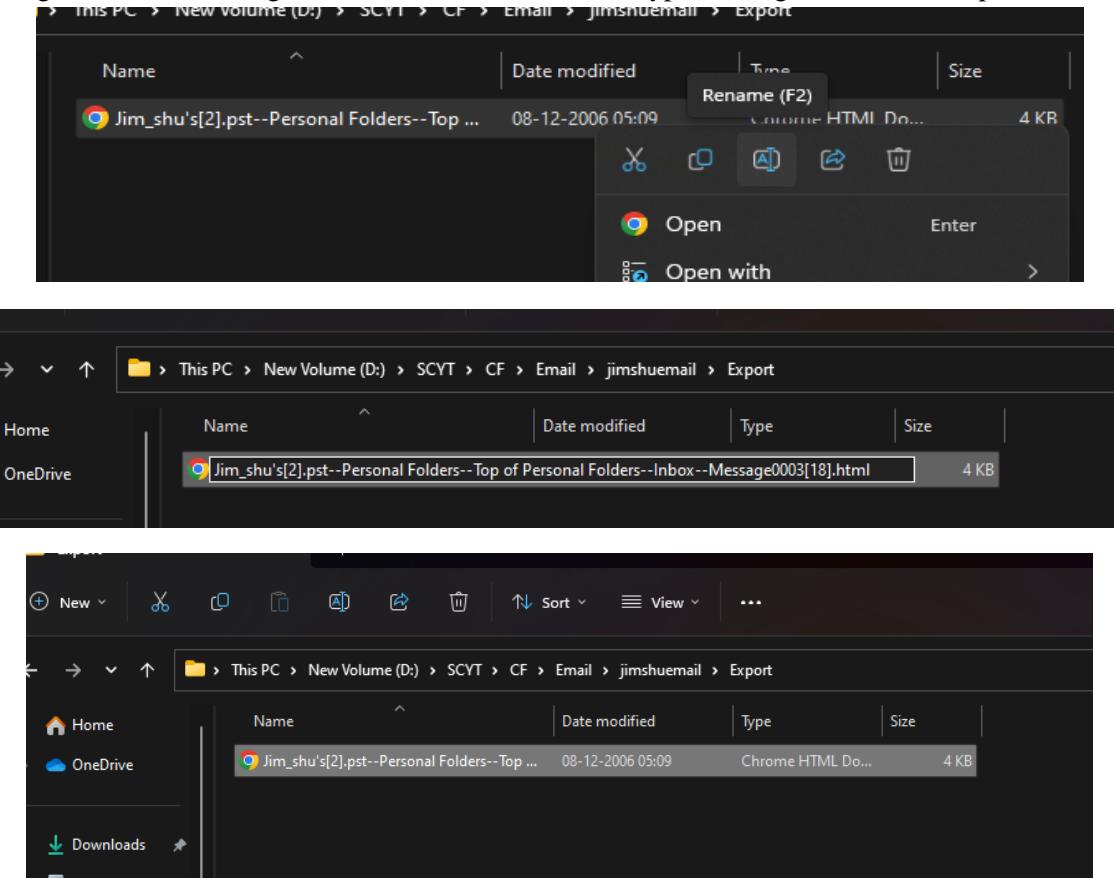


FTK saves exported files in the HTML format with no extension.

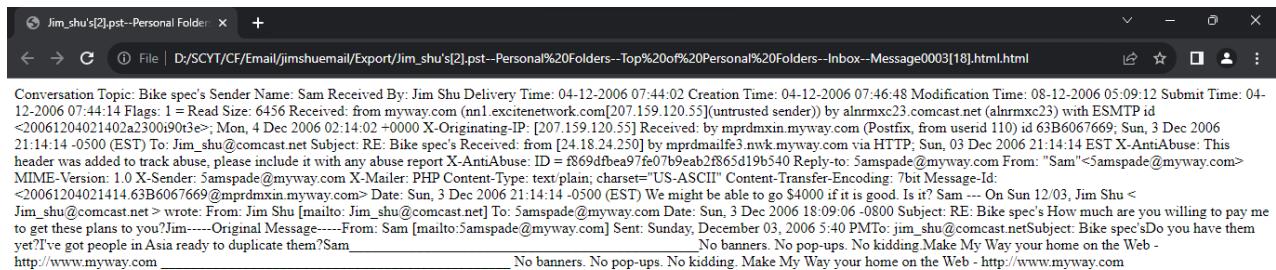


RIZVI COLLEGE OF ARTS, SCIENCE AND COMMERCE  
TYBSC CS SEM V – CYBER FORENSIC

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

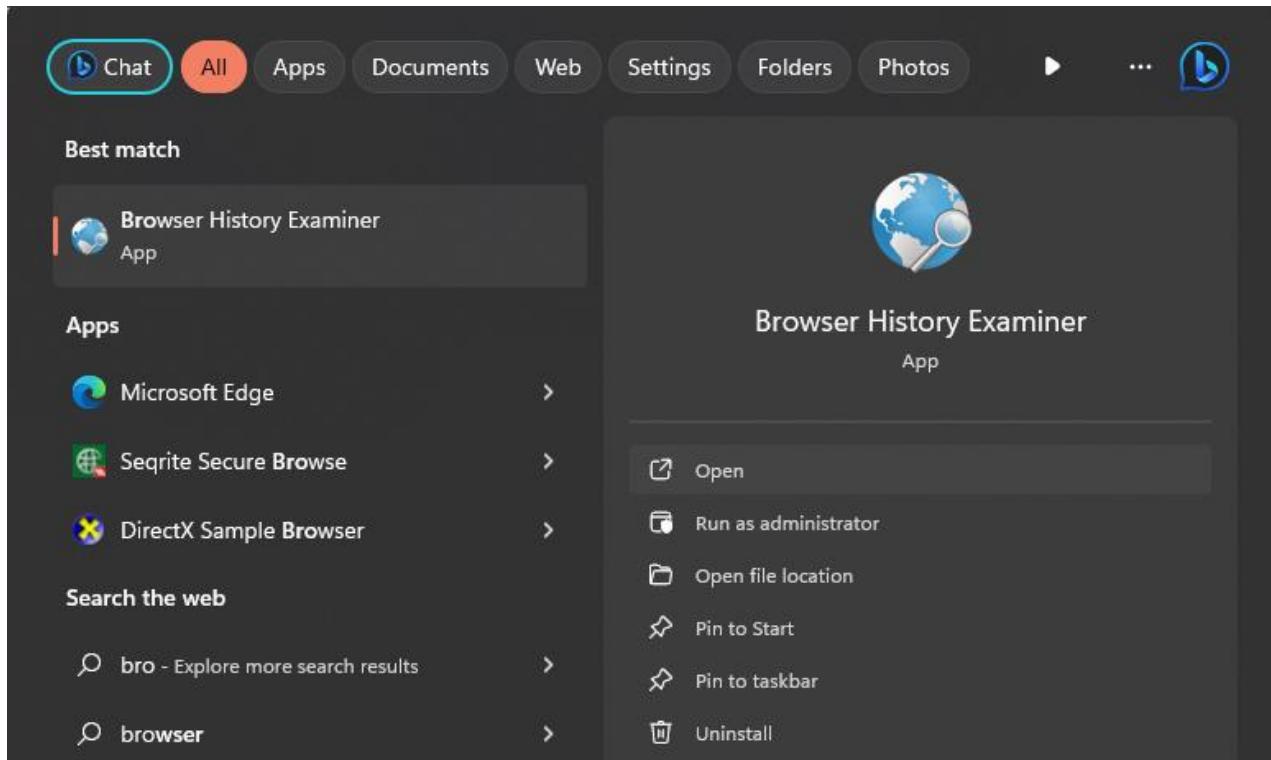
### Aim:

Web Browser Forensics

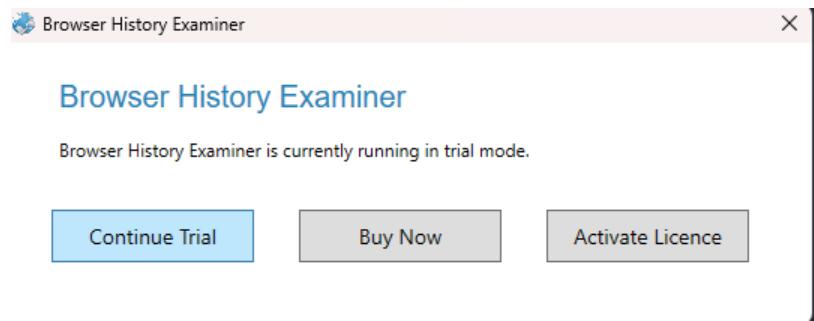
- Analyze browser artifacts, including history files, bookmarks, and download records.
- Analyze cache and cookies data to reconstruct user-browsing history and identify visited websites or online activities.
- Extract the relevant log or timestamp file, analyze its contents and interpret the timestamp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

### Practical:

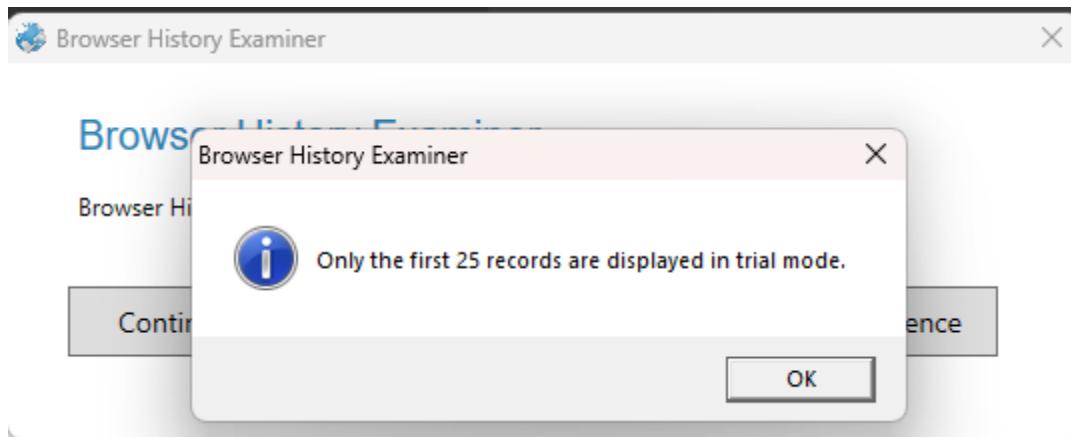
We are going to use the **Browser History Examiner**. Run it as Administrator..



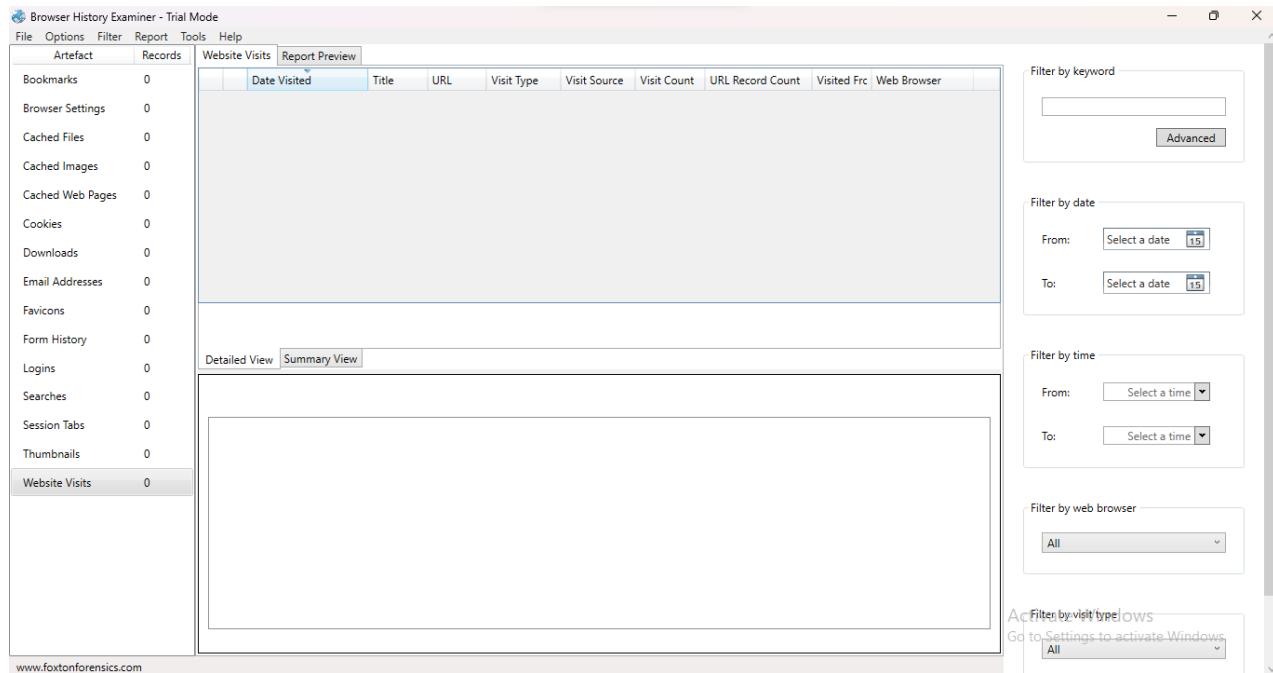
It is a **Paid Software** but has a **free-trail** to get a total of **25 records** from all the browsers in the device



Click on Continue Trail

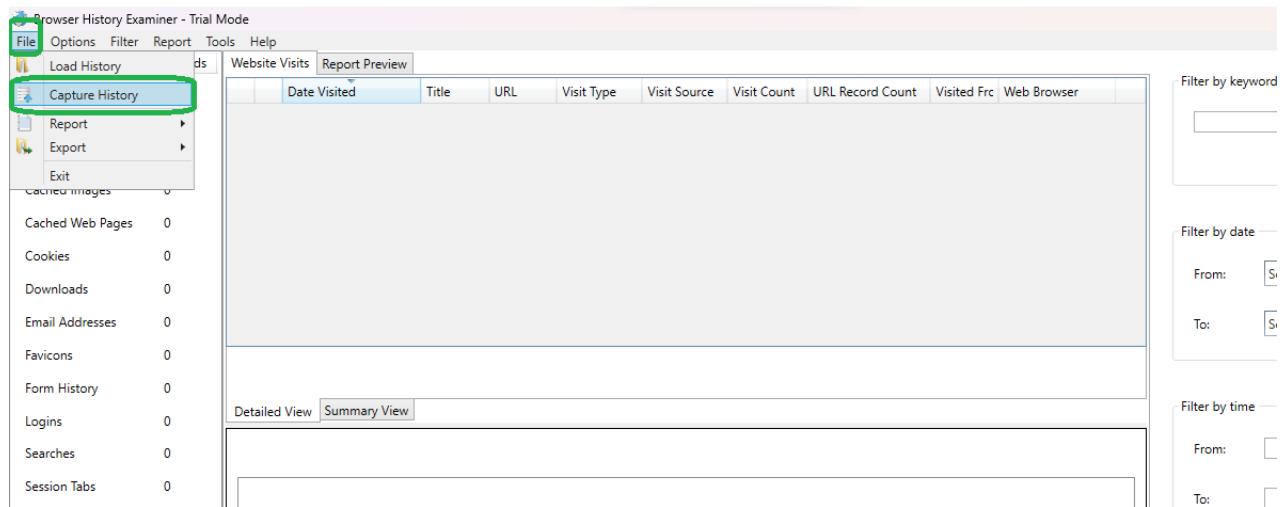


Click OK

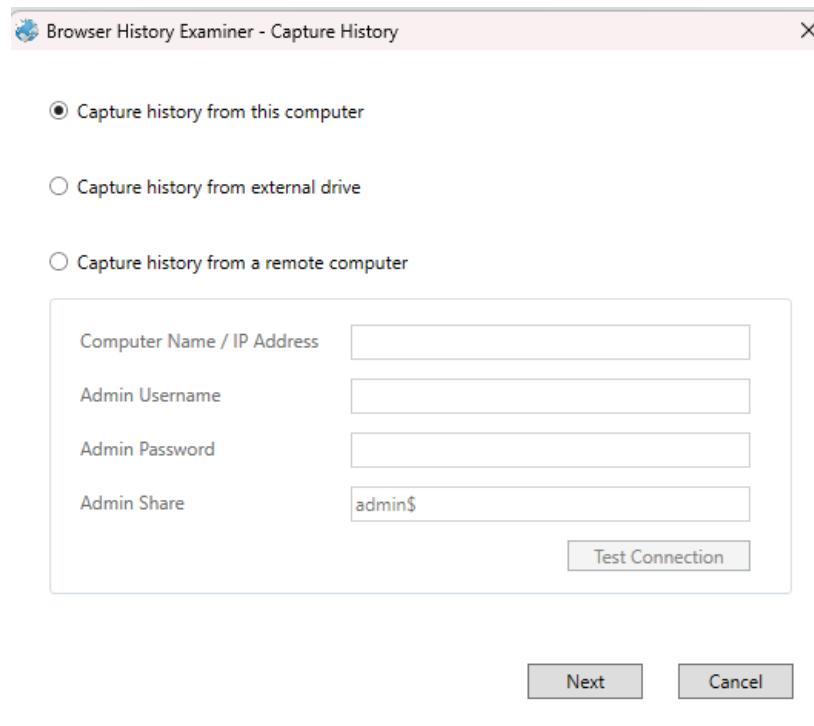


This is the Interface of the Application

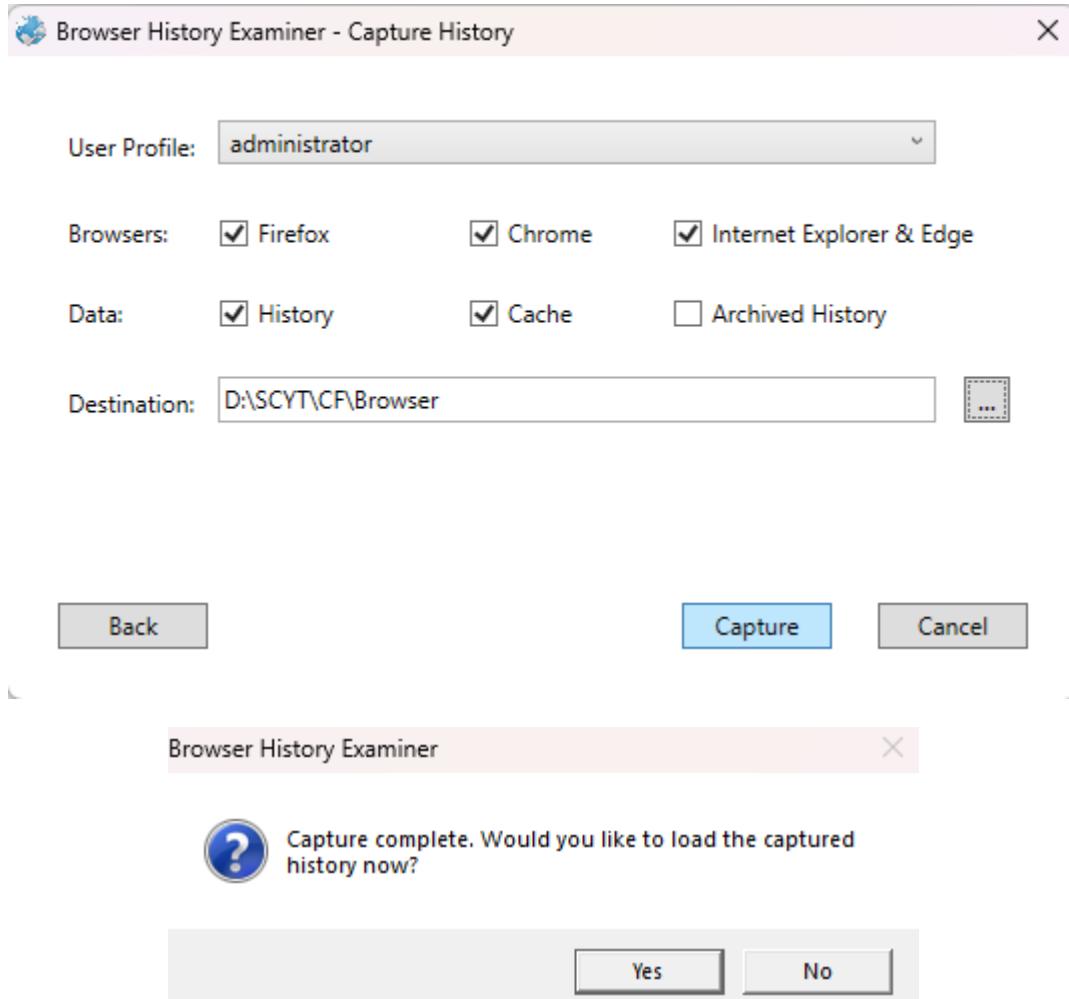
Go to File → Capture History



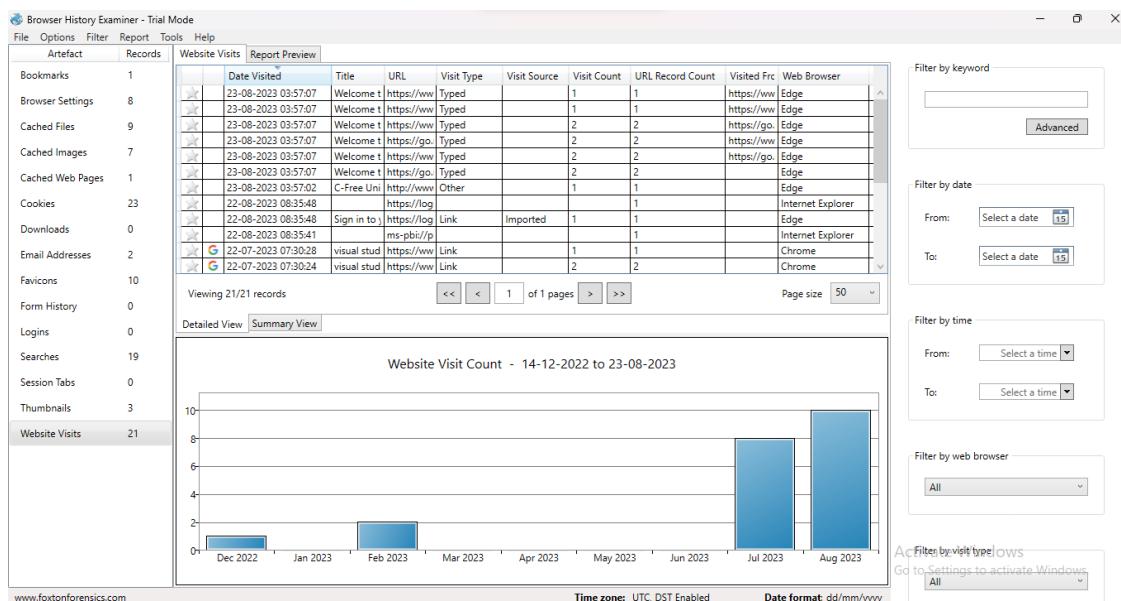
We are going to capture from this device only Select on that and click Next



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

Date Added	Last Modified	Title	URL	Web Browser
		Bing	http://go.microsoft.com/fwlink/p/?Link	Internet Explorer

Here we can see the browser settings

Name	Value	Web Browser
Sync Apps	Yes	Edge
Sync Autocomplete	Yes	Edge
Sync Bookmarks	Yes	Edge
Sync Extensions	Yes	Edge
Sync Passwords	Yes	Edge
Sync Preferences	Yes	Edge
Sync Tabs	No	Edge
Sync Typed URLs	No	Edge

Here we can see the cached files

Last Fetched	Content Type	URL	Fetch Count	File Size (Bytes)	Web Browser
	application/x-javascript	https://aadcdn.mstfauth.net/shared/1.0/co	1	423350	Internet Explorer
	text/css	https://aadcdn.mstfauth.net/ests/2.1/contx	1	111100	Internet Explorer
	application/x-javascript	https://aadcdn.mstfauth.net/shared/1.0/co	1	110048	Internet Explorer
	application/x-javascript	https://aadcdn.mstfauth.net/ests/2.1/contx	1	49972	Internet Explorer
	application/x-javascript	https://aadcdn.mstfauth.net/shared/1.0/co	1	24820	Internet Explorer
	application/octet-stream	https://az567904.vo.msecnd.net/pub/Defa	3	19161	Internet Explorer
	application/octet-stream	https://az700632.vo.msecnd.net/pub/Rem	1	1683	Internet Explorer
	application/octet-stream	https://az700632.vo.msecnd.net/pub/Fligh	1	205	Internet Explorer
	application/octet-stream	https://az700632.vo.msecnd.net/pub/Fligh	2	78	Internet Explorer

Here we can see the cached images

RIZVI COLLEGE OF ARTS, SCIENCE AND COMMERCE  
TYBSC CS SEM V – CYBER FORENSIC

The screenshot shows the 'Cached Images' section of the Browser History Examiner. The left sidebar lists various artifacts with their counts: Bookmarks (1), Browser Settings (8), Cached File (9), 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), and Website Visits (21). The main pane displays a table with columns: Last Fetched, Content Type, URL, Fetch Count, File Size (Bytes), and Web Browser. There are 7 records listed, all from 'aadcdn.msftauth.net/shared/1.0/content/r' with various file types like image/svg+xml and image/gif. The file sizes range from 899 to 3651 bytes. The 'Web Browser' column shows 'Internet Explorer' for all entries.

Here we can see the cached webpages

The screenshot shows the 'Cached Web Pages' section of the Browser History Examiner. The left sidebar lists artifacts: Bookmarks (1), Browser Settings (8), Cached Files (9), Cached Images (7), and Cached Web Pages (1). The main pane shows a single record in a table: 'Last Fetched' is '22-07-2023 05:11:01', 'URL' is 'https://login.live.com/Me.htm?v=3', 'Fetch Count' is '1', 'File Size (Bytes)' is '2347', and 'Web Browser' is 'Internet Explorer'. The status bar at the bottom indicates 'Viewing 1/1 records'.

Here we can see the cookies stored

The screenshot shows the 'Cookies' section of the Browser History Examiner. The left sidebar lists artifacts: 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), Session Tabs (0), Thumbnails (3), and Website Visits (21). The main pane displays a table with columns: Date Created, URL, Last Accessed, Date Expires, Name, Content, and Web Browser. There are 23 records listed, mostly from 'bing.com/' and 'msn.com/'. The 'Content' column contains various cookie values like 'MUID', 'SRCHUID', and session IDs. The 'Web Browser' column shows 'Edge' for all entries. The status bar at the bottom indicates 'Viewing 23/23 records'.

Here we can see the emails used for logins

The screenshot shows the 'Email Addresses' tab selected in the 'Report Preview' section of the software. The interface includes a navigation bar with File, Options, Filter, Report, Tools, and Help. On the left, a sidebar lists various artifacts with their counts: 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). The main pane displays a table with columns: Last Used, Email Address, Domain, Source, and Web Browser. Two entries are listed:

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

On the right, there are three filter panels: 'Filter by keyword' (with a search input and 'Advanced' button), 'Filter by date' (with 'From' and 'To' dropdowns), and 'Filter by time' (with 'From' and 'To' dropdowns).

Here we can see the favicons

The screenshot shows the 'Favicons' tab selected in the 'Report Preview' section. The interface is similar to the previous one, with a navigation bar and a sidebar listing artifacts. The main pane shows a table with columns: URL, Page URL, Expires, Last Updated, and Web Browser. Multiple entries for Google favicons are listed:

URL	Page URL	Expires	Last Updated	Web Browser
https://cdn.sstatic.net/Sites/stackoverflow/	https://stackoverflow.com/questions/41		22-07-2023 07:28:01	Chrome
https://cdn.sstatic.net/Sites/stackoverflow/	https://stackoverflow.com/questions/41		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=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

Filtering and date/time selection options are also present on the right.

Here we can see the searches

The screenshot shows the 'Searches' tab selected in the 'Report Preview' section. The interface is consistent with the others. The main pane displays a table with columns: Date Searched, Search Terms, Search Engine, URL, Source, and Web Browser. Numerous search terms related to 'visual studio' and 'android licenses' are listed:

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
22-07-2023 07:27:27	google	Google	https://www.google.com/sea	Favicon	Chrome
22-07-2023 07:27:27	google	Google	https://www.google.com/sea	Favicon	Chrome

Filtering by keyword, date, time, and web browser is available on the right side.

RIZVI COLLEGE OF ARTS, SCIENCE AND COMMERCE  
TYBSC CS SEM V – CYBER FORENSIC

Here we see the thumbnails

The screenshot shows the 'Browser History Examiner - Trial Mode' interface. The left sidebar lists various artifact types with their counts: 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), Session Tabs (0), Thumbnails (3), and Website Visits (21). The main pane displays a table of thumbnails for the 'Thumbnails' category, showing columns for URL, Title, Filename, Last Updated, and Web Browser. A filter panel on the right allows filtering by keyword, date, time, and web browser.

URL	Title	Filename	Last Updated	Web Browser
<a href="https://chrome.google.com/websl">https://chrome.google.com/websl</a>	Web Store			Chrome
<a href="https://www.office.com/">https://www.office.com/</a>	Office			Edge
<a href="https://go.microsoft.com/fwlink/?">https://go.microsoft.com/fwlink/?</a>	Welcome to Microsoft Edge			Edge

Here we can see the websites visits

The screenshot shows the 'Browser History Examiner - Trial Mode' interface. The left sidebar lists various artifact types with their counts, identical to the previous screenshot. The main pane displays a table of website visits, showing columns for Date Visited, Title, URL, Visit Type, Visit Source, Visit Count, URL Record Count, Visited Frc, and Web Browser. Below the table is a bar chart titled 'Website Visit Count - 14-12-2022 to 23-08-2023'. The chart shows visit counts for each month from December 2022 to August 2023. A detailed view of the chart shows a peak in visits in August 2023.

Date Visited	Title	URL	Visit Type	Visit Source	Visit Count	URL Record Count	Visited Frc	Web Browser
23-08-2023 03:57:07	Welcome t	<a href="https://ww">https://ww</a>	Typed		1	1	<a href="https://ww">https://ww</a>	Edge
23-08-2023 03:57:07	Welcome t	<a href="https://ww">https://ww</a>	Typed		1	1	<a href="https://ww">https://ww</a>	Edge
23-08-2023 03:57:07	Welcome t	<a href="https://ww">https://ww</a>	Typed		2	2	<a href="https://go">https://go</a>	Edge
23-08-2023 03:57:07	Welcome t	<a href="https://go">https://go</a>	Typed		2	2	<a href="https://ww">https://ww</a>	Edge
23-08-2023 03:57:07	Welcome t	<a href="https://ww">https://ww</a>	Typed		2	2	<a href="https://go">https://go</a>	Edge
23-08-2023 03:57:07	C-Free Un	<a href="http://ww">http://ww</a>	Other		1	1		Edge
22-08-2023 08:35:48	Sign in to )	<a href="https://log">https://log</a>	Link	Imported	1	1		Internet Explorer
22-08-2023 08:35:41	ms-pbi/p				1	1		Internet Explorer
22-07-2023 07:30:28	visual stud	<a href="https://ww">https://ww</a>	Link		1	1		Chrome
22-07-2023 07:30:24	visual stud	<a href="https://ww">https://ww</a>	Link		2	2		Chrome

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

The bar chart displays the following approximate data:

Month	Visit Count
Dec 2022	1
Jan 2023	2
Feb 2023	2
Jul 2023	8
Aug 2023	10