



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



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

**(COMMITTED TO EXCELLENCE IN EDUCATION)**

# **CERTIFICATE**

This is to certify that Mr/Ms. \_\_\_\_\_  
a student of TY.**BSC-CS** Roll no: \_\_\_\_\_ has completed the required number of practicals  
in the subject of \_\_\_\_\_  
as prescribed by the UNIVERSITY OF MUMBAI under my supervision during the  
academic year 2024-2025.

.....  
Prof. Incharge

.....  
Principal

.....  
External Examiner

.....  
Course Co-ordinator

Professor Name: Ms. Akansha Mishra	Class : TY.BSC-CS Semester : Sem V (2024-2025)
------------------------------------	---

Course code : USCSP5041	Subject: Cyber Forensics
-------------------------	--------------------------

Sr. No.	Date	Index	Page No.	Sign
1		<p>Creating a Forensic Image using FTK Imager/Encase Imager :</p> <ul style="list-style-type: none"> <li>• Creating Forensic Image</li> <li>• Check Integrity of Data</li> <li>• Analyze Forensic Image</li> </ul>	1-10	
2		<p>Data Acquisition:</p> <ul style="list-style-type: none"> <li>• Perform data acquisition using:</li> <li>• USB Write Blocker + Encase Imager</li> <li>• SATA Write Blocker + Encase Imager</li> <li>• Falcon Imaging Device</li> </ul>	11-15	
3		<p>Analyze the memory dump of a running computer system.</p> <ul style="list-style-type: none"> <li>• Extract volatile data, such as open processes, network connections, and registry information.</li> </ul>	16-20	
4		<p>Capturing and analyzing network packets using Wireshark (Fundamentals) :</p> <ul style="list-style-type: none"> <li>• Identification the live network</li> <li>• Capture Packets</li> </ul> <p>Analyze the captured packets</p>	21-39	
5		<p>Using Sysinternals tools for Network Tracking and Process Monitoring :</p> <ul style="list-style-type: none"> <li>• Check Sysinternals tools</li> <li>• Monitor Live Processes</li> <li>• Capture RAM</li> <li>• Capture TCP/UDP packets</li> <li>• Monitor Hard Disk</li> <li>• Monitor Virtual Memory</li> </ul>	40-52	

		Monitor Cache Memory		
6		<p>Recovering and Inspecting deleted files</p> <ul style="list-style-type: none"> <li>• Check for Deleted Files</li> <li>• Recover the Deleted Files</li> <li>• Analyzing and Inspecting the recovered files</li> </ul> <p>Perform this using recovery option in ENCASE and also Perform manually through command line</p>	53-64	
7		<p>Steganography Detection</p> <ul style="list-style-type: none"> <li>• Detect hidden information or files within digital images using steganography analysis tools.</li> </ul> <p>Extract and examine the hidden content.</p>	65-72	
8		<p>Mobile Device Forensics</p> <ul style="list-style-type: none"> <li>• Perform a forensic analysis of a mobile device, such as a smartphone or tablet.</li> </ul> <p>Retrieve call logs, text messages, and other relevant data for investigative purposes.</p>	73-87	
9		<p>Email Forensics</p> <ul style="list-style-type: none"> <li>• Analyze email headers and content to trace the origin of suspicious emails.</li> <li>• Identify potential email forgeries or tampering.</li> </ul>	89-101	
10		<p>Web Browser Forensics</p> <ul style="list-style-type: none"> <li>• Analyze browser artifacts, including history files, bookmarks, and download records.</li> <li>• Analyze cache and cookies data to reconstruct user-browsing history and identify visited websites or online activities. <ul style="list-style-type: none"> <li>• 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.</li> </ul> </li> </ul>	102-110	



## PRACTICAL NO. 1

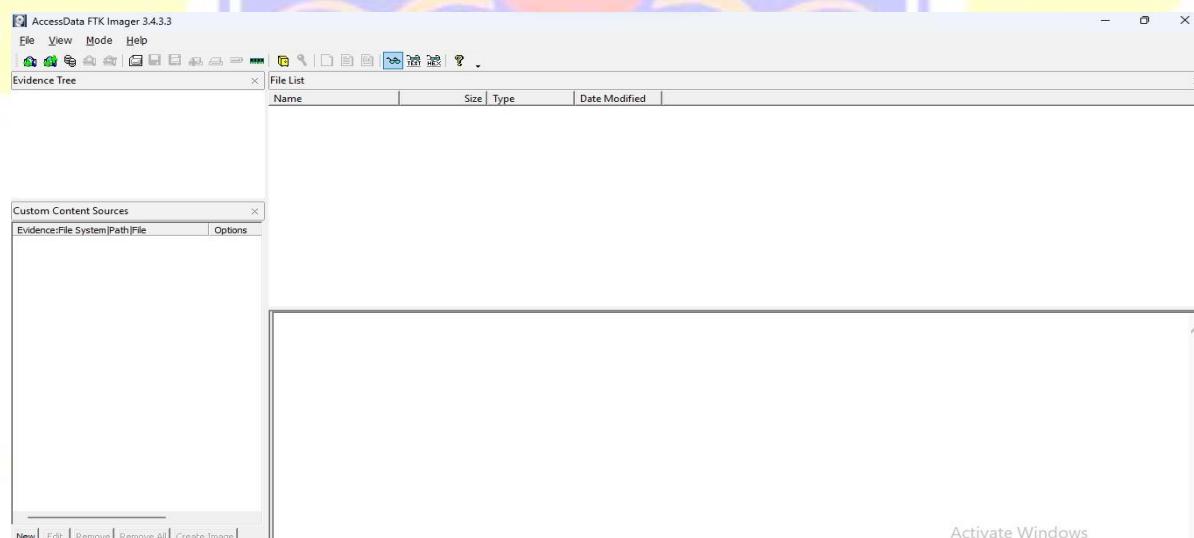
### Aim:

Creating a Forensic Image using FTK Imager/Encase Imager:

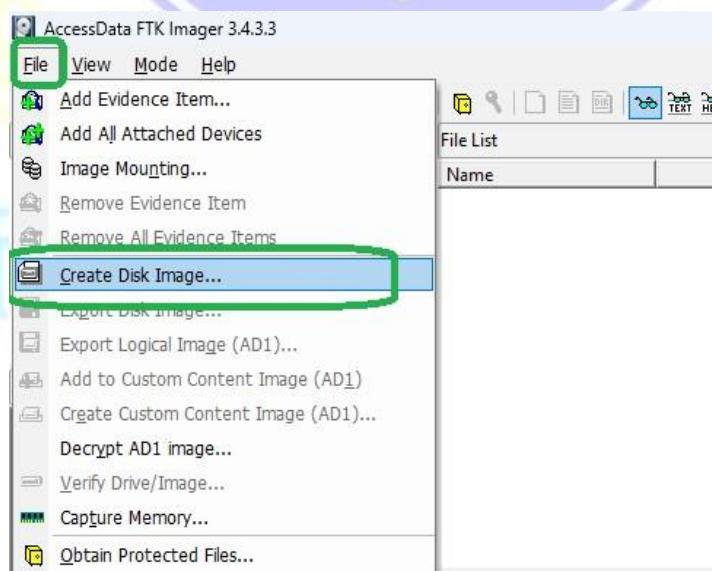
- Creating Forensic Image
- Check Integrity of Data
- Analyze Forensic Image

### Practical:

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



Go to File → Create Disk Image



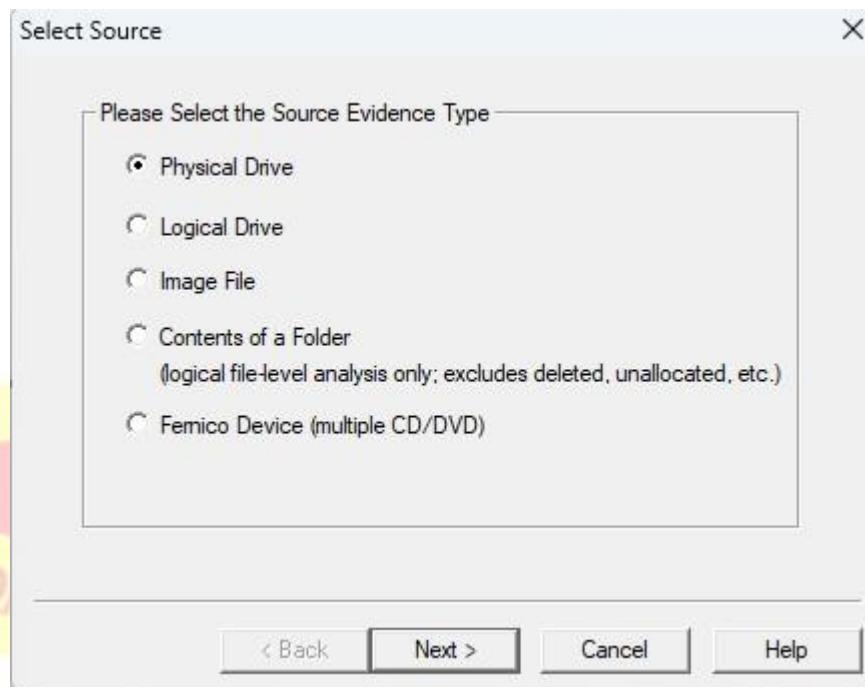


## SHRI G.P.M. DEGREE COLLEGE

Department of Computer

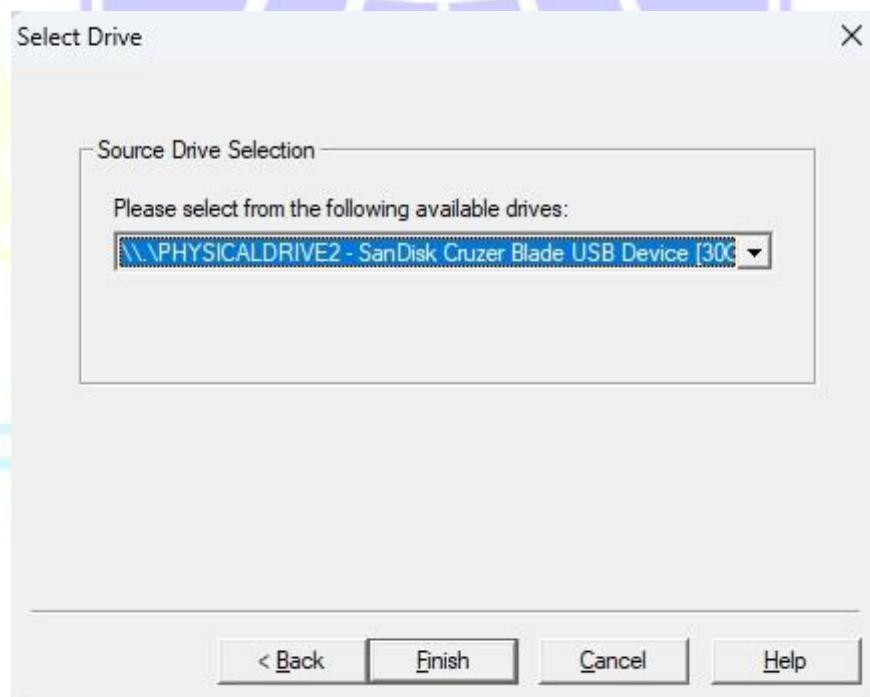
Vision.. Innovation.. Solution.. Presentation

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





## SHRI G.P.M. DEGREE COLLEGE

Department of Computer

Vision.. Innovation.. Solution.. Presentation

Now we add the location to create images

Create Image

Image Source  
\\.\PHYSICALDRIVE2

Starting Evidence Number: 1

Image Destination(s)

Add... Edit... Remove  
Add Overflow Location

Verify images after they are created    Precalculate Progress Statistics  
 Create directory listings of all files in the image after they are created

Start Cancel

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

Select Image Type

Please Select the Destination Image Type

Raw (dd)  
 SMART  
 E01  
 AFF

< Back Next > Cancel Help

And now we fill the details required for the case



## SHRI G.P.M. DEGREE COLLEGE

Department of Computer

Vision.. Innovation.. Solution.. Presentation

Evidence Item Information X

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

[< Back](#) [Next >](#) [Cancel](#) [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

Select Image Destination X

Image Destination Folder	D:\SCYT\CF\FTKIMAG	<a href="#">Browse</a>
Image Filename (Excluding Extension)	290723	
Image Fragment Size (MB) For Raw, E01, and AFF formats: 0 = do not fragment	0	
Compression (0=None, 1=Fastest, ..., 9=Smallest)	0	
<input type="checkbox"/> Use AD Encryption		

[< Back](#) [Finish](#) [Cancel](#) [Help](#)

Then Click on Start and wait until the imaging is done



## SHRI G.P.M. DEGREE COLLEGE

Department of Computer

Vision.. Innovation.. Solution.. Presentation

Create Image X

Image Source:

Starting Evidence Number:

Image Destination(s):

Verify images after they are created  Precalculate Progress Statistics  
 Create directory listings of all files in the image after they are created

Creating Image... - □ X

Image Source:

Destination:

Status:

Progress:

Elapsed time:

Estimated time left:

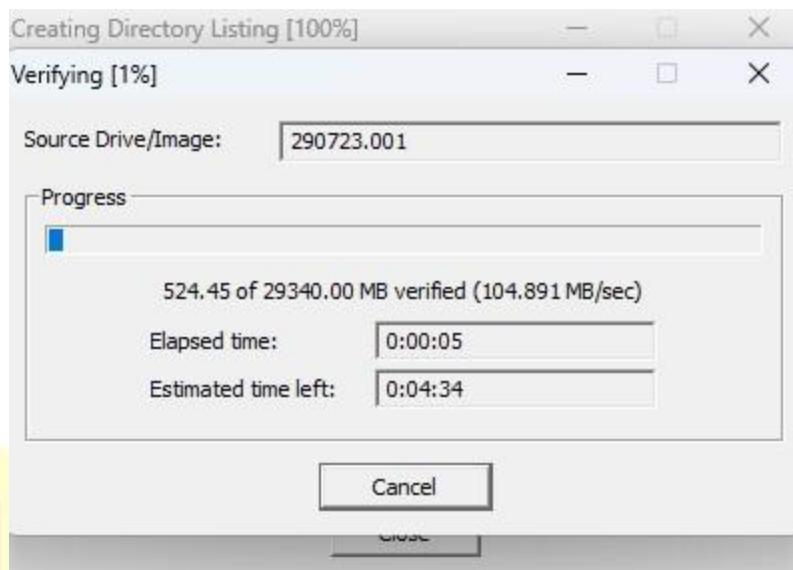
Now it will verify



## SHRI G.P.M. DEGREE COLLEGE

Department of Computer

Vision.. Innovation.. Solution.. Presentation



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

Drive/Image Verify Results	
	Name
	290723.001
	Sector count
	60088320
	<b>MD5 Hash</b>
	Computed hash
	592a08afa156587812828ff5df10164e
	Report Hash
	592a08afa156587812828ff5df10164e
	Verify result
	Match
	<b>SHA1 Hash</b>
	Computed hash
	82141f8b26552c9deff3d1caff1521ee8d
	Report Hash
	82141f8b26552c9deff3d1caff1521ee8d
	Verify result
	Match
	<u>Bad Sector List</u>
	[Empty list box]

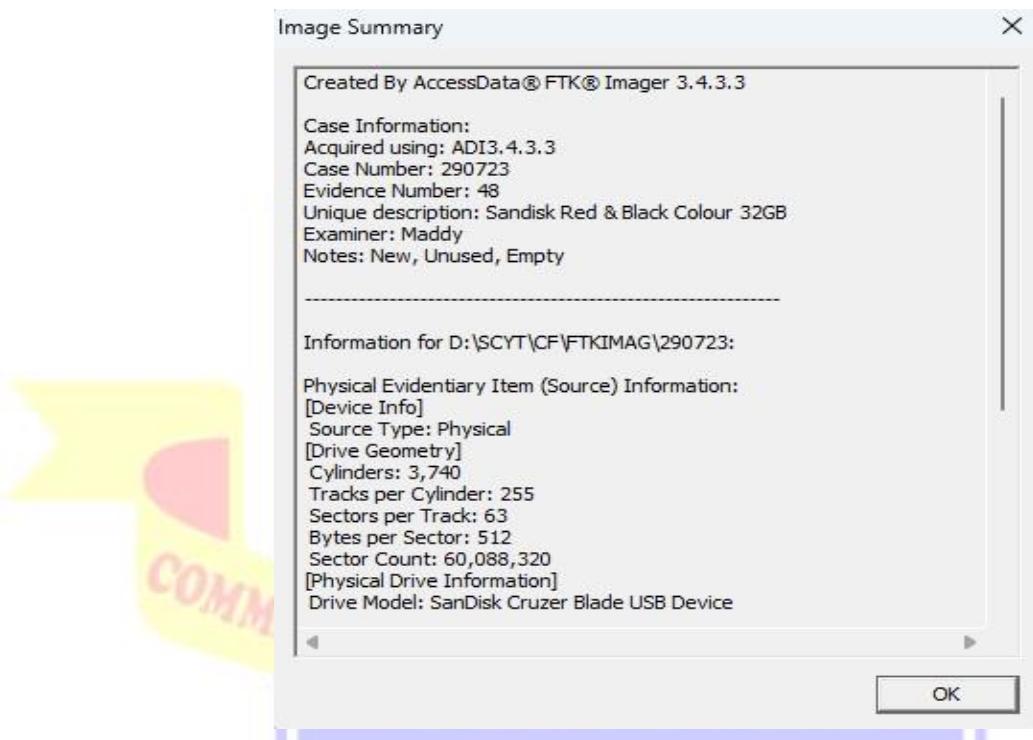


## SHRI G.P.M. DEGREE COLLEGE

Department of Computer

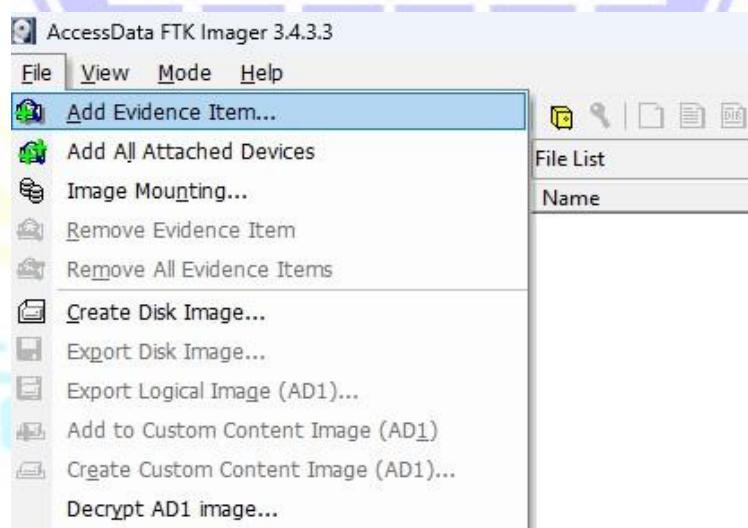
Vision.. Innovation.. Solution.. Presentation

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



## SHRI G.P.M. DEGREE COLLEGE

Department of Computer

Vision.. Innovation.. Solution.. Presentation

Select Source

Please Select the Source Evidence Type

Physical Drive  
 Logical Drive  
 Image File  
 Contents of a Folder  
(logical file-level analysis only; excludes deleted, unallocated, etc.)

< Back    Next >    Cancel    Help

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

Select File

Evidence Source Selection

Please enter the source path:  
D:\SCYT\CF\FTKIMAG\290723.001

Browse...

< Back    Finish    Cancel    Help

Here we can see the data shown by the FTK Imager



# SHRI G.P.M. DEGREE COLLEGE

Department of Computer

Vision.. Innovation.. Solution.. Presentation

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]

Custom Content Sources

Evidence:File System|Path|File Options

Activate Windows  
Go to Settings to activate Windows.

New Edit Remove Remove All Create Image

Properties Hex Value Int... Custom Conte...

Cursor pos = 0; phy sec = 0

NUM



### Result:

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

### Learning Outcomes:

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

### Course Outcomes:

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

### Conclusion:

### Viva Questions:

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



## PRACTICAL NO: 2

### Aim:

Data Acquisition:

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

### Practical:

USB Writer Blocker + Encase Imager



### **Hardware and Paid Software's:**

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

[https://www.amazon.com/usb-write-blocker/s?k=usb+write+blocker&language=en\\_US&currency=INR](https://www.amazon.com/usb-write-blocker/s?k=usb+write+blocker&language=en_US&currency=INR)

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

### **For Open-Source Software:**

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

### **Encase Imager:**

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

### **Overview PDF for the Encase Imager:**

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



# SHRI G.P.M. DEGREE COLLEGE

Department of Computer

Vision.. Innovation.. Solution.. Presentation

<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. On the left, there's a tree view of 'History' containing 'Internet and Email' and 'Mozilla' sections. Under 'Internet and Email', there are sub-folders like 'Internet Explorer' (with 'administrator', 'Redirect', 'pc user', 'secure user', and 'Simple User PW 123') and 'Opera'. On the right, a table lists 25 history items with columns for Name, URL, Host, User, Visit Count, and First Date. Item 18 is selected, showing its details: URL is <http://webmail.netscape.com/msgview.adp?folder=SW5ib3g=&uid=223796>, Host is webmail.netscape.com, User is PC User, Visit Count is 2, First Date is 02/04/05 04:12:58PM, and History Path is Internet and Email\Active\Documents and Settings\PC User\Application Data\Mozilla\Firefox\Profiles\03fh4udv.default\history.dat. Below the table, a text box displays the same information.

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://linuxhint.com/best_hardware_write_blockers/)



## SHRI G.P.M. DEGREE COLLEGE

Department of Computer

Vision.. Innovation.. Solution.. Presentation

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

Setup of the Write Blocker

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

### Falcon Imaging Device



About Info of the Falcon Imaging Device

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

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

[https://www.secureindia.in/?page\\_id=1068](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-falcon-neo/>



## SHRI G.P.M. DEGREE COLLEGE

Department of Computer

Vision.. Innovation.. Solution.. Presentation

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

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



COMMITTED TO EXCELLENCE IN EDUCATION



निर्मलसनेह उत्तम सेवाधर्म

**Result:**

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

**Learning Outcomes:**

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

**Course Outcomes:**

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

**Conclusion:****Viva Questions:**

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



## PRACTICAL NO: 3

### Aim:

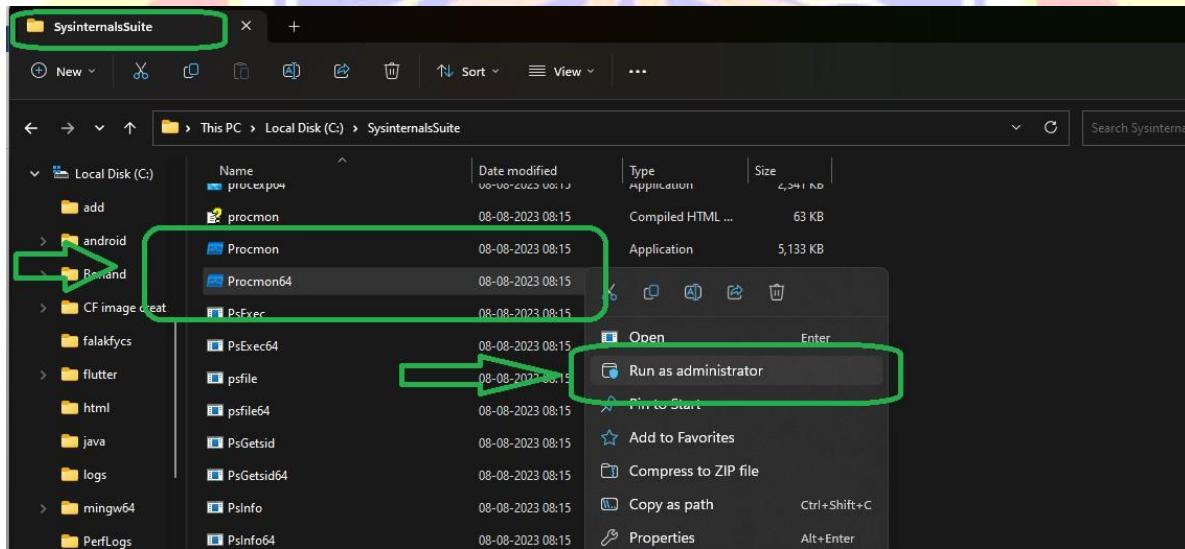
Analyze the memory dump of a running computer system.

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

### Practical:

#### Open Process

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





# SHRI G.P.M. DEGREE COLLEGE

Department of Computer

Vision.. Innovation.. Solution.. Presentation

Process Monitor - Sysinternals: www.sysinternals.com						
Time ...	Process Name	PID	Operation	Path	Result	Detail
08:27...	svchost.exe	2644	ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset: 704512, Le...
08:27...	Explorer EXE	11808	ReadFile	C:\Windows\System32\MmCoreR.dll	SUCCESS	Offset: 995328, Le...
08:27...	svchost.exe	2644	ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset: 692224, Le...
08:27...	svchost.exe	11808	ReadFile	C:\Windows\System32\MmCoreR.dll	SUCCESS	Offset: 925696, Le...
08:27...	svchost.exe	1656	UDP Receive	F02:fb:5353->fe80:2050:fc:b495:8...	SUCCESS	Length: 30, sequen...
08:27...	chrome.exe	9724	UDP Receive	F02:fb:5353->fe80:2050:fc:b495:8...	SUCCESS	Length: 30, sequen...
08:27...	svchost.exe	2644	ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset: 647168, Le...
08:27...	svchost.exe	11808	QueryBasicInfor...	C:\Program Files\Windows Apps\Clipcha...	SUCCESS	CreationTime: 13-0...
08:27...	svchost.exe	11808	ReadFile	C:\Windows\System32\Taskbar.dll	SUCCESS	Offset: 2406400, L...
08:27...	svchost.exe	11808	CloseFile	C:\Program Files\Windows Apps\Clipcha...	SUCCESS	Offset: 2406400, L...
08:27...	svchost.exe	2644	ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset: 638976, Le...
08:27...	svchost.exe	11808	RegCloseKey	HKU\S-1-5-21-3130516669-347735452...	SUCCESS	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	RegQueryKey	HKU\S-1-5-21-3130516669-347735452...	SUCCESS	Desired Access: R...
08:27...	svchost.exe	2644	ReadFile	C:\Windows\System32\Windows.State...	SUCCESS	Offset: 6500352, L...
08:27...	svchost.exe	11808	ReadFile	C:\Windows\System32\Windows.State...	SUCCESS	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	RegCloseKey	HKU\S-1-5-21-3130516669-347735452...	SUCCESS	Offset: 2718208, L...
08:27...	svchost.exe	11808	RegQueryValue	HKU\S-1-5-21-3130516669-347735452...	NAME NOT FOUND	Length: 12
08:27...	svchost.exe	11808	RegCloseKey	HKU\S-1-5-21-3130516669-347735452...	SUCCESS	Offset: 180224, Le...
08:27...	svchost.exe	1020	ReadFile	C:\Windows\System32\BCP47mm.dll	SUCCESS	Offset: 1540096, L...
08:27...	svchost.exe	2644	ReadFile	C:\Windows\System32\Windows.State...	SUCCESS	Offset: 6434816, L...
08:27...	svchost.exe	11808	ReadFile	C:\Windows\System32\Taskbar.dll	SUCCESS	Offset: 2529280, L...
08:27...	svchost.exe	1020	ReadFile	C:\Windows\System32\Taskbar.dll	SUCCESS	Offset: 1523712, L...
08:27...	svchost.exe	11808	ReadFile	C:\Windows\System32\BCP47mm.dll	SUCCESS	Offset: 155648, L...
08:27...	svchost.exe	2644	ReadFile	C:\Windows\System32\Windows.State...	SUCCESS	Offset: 2512896, L...
08:27...	svchost.exe	1020	ReadFile	C:\Windows\System32\Windows.State...	SUCCESS	Offset: 6414336, L...
08:27...	svchost.exe	11808	RegOpenKey	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	Desired Access: R...
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	2644	LockFile	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	Exclusive: False, O...
08:27...	svchost.exe	11808	RegCloseKey	HKU\S-1-5-21-3130516669-347735452...	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	Desired Access: R...

## Network Connections

Go to SysinternalSuite → TCPview

SysinternalsSuite					
This PC > Local Disk (C:) > SysinternalsSuite					
	Name	Date modified	Type	Size	...
	strings	08-08-2023 08:14	Application	467 KB	
	strings64	08-08-2023 08:14	Application	336 KB	
	sync	08-08-2023 08:14	Application	435 KB	
	sync64	08-08-2023 08:14	Application	8,246 KB	
	Sysmon	08-08-2023 08:15	Application	4,443 KB	
	Sysmon64	08-08-2023 08:15	Application	198 KB	
	tcpvcon	08-08-2023 08:15	Application	245 KB	
	tcpvcon64	08-08-2023 08:15	Application	16 KB	
	tcpview	08-08-2023 08:15	Compiled HTML	923 KB	
	tcpview\$	08-08-2023 08:15	Application	1,002 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	



# SHRI G.P.M. DEGREE COLLEGE

Department of Computer

Vision.. Innovation.. Solution.. Presentation

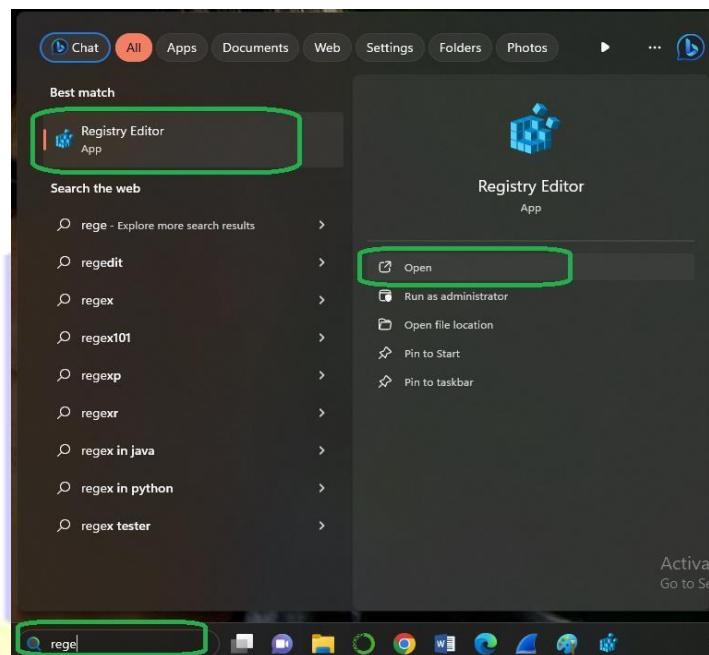
TCPView - Sysinternals: www.sysinternals.com										
Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Time	Module Name	
spoolsv.exe	3944	TCP	Listen	0.0.0.0	49675	0.0.0.0	0	04-09-2023 09:59:54	Spooler	
lsass.exe	644	TCP	Listen	0.0.0.0	49676	0.0.0.0	0	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	192.168.10.1	65528			

TCPView - Sysinternals: www.sysinternals.com										
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::4a0:628: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	IKEEKT	
svchost.exe	10812	UDPV6	::		547	*		05-09-2023 08:46:55	SharedAccess	
svchost.exe	7720	UDPV6	::1		1900	*		05-09-2023 08:46:54	SSDPSRV	
svchost.exe	7720	UDPV6	fe80::3b4f:9f72:34ab:146		1900	*		05-09-2023 08:46:54	SSDPSRV	
svchost.exe	7720	UDPV6	fe80::3b4f:9f72:34ab:146		1900	*		05-09-2023 08:46:54	SSDPSRV	
svchost.exe	7720	UDPV6	fe80::3b4f:9f72:34ab:146		1900	*		05-09-2023 08:46:54	SSDPSRV	
svchost.exe	7720	UDPV6	fe80::3b4f:9f72:34ab:146		1900	*		05-09-2023 08:46:54	SSDPSRV	
dashost.exe	5184	UDPV6	::		3702	*		05-09-2023 08:47:04		
dashost.exe	5184	UDPV6	::		3702	*		05-09-2023 08:47:04		
svchost.exe	4264	UDPV6	::		4500	*		04-09-2023 09:59:54	IKEEKT	
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	

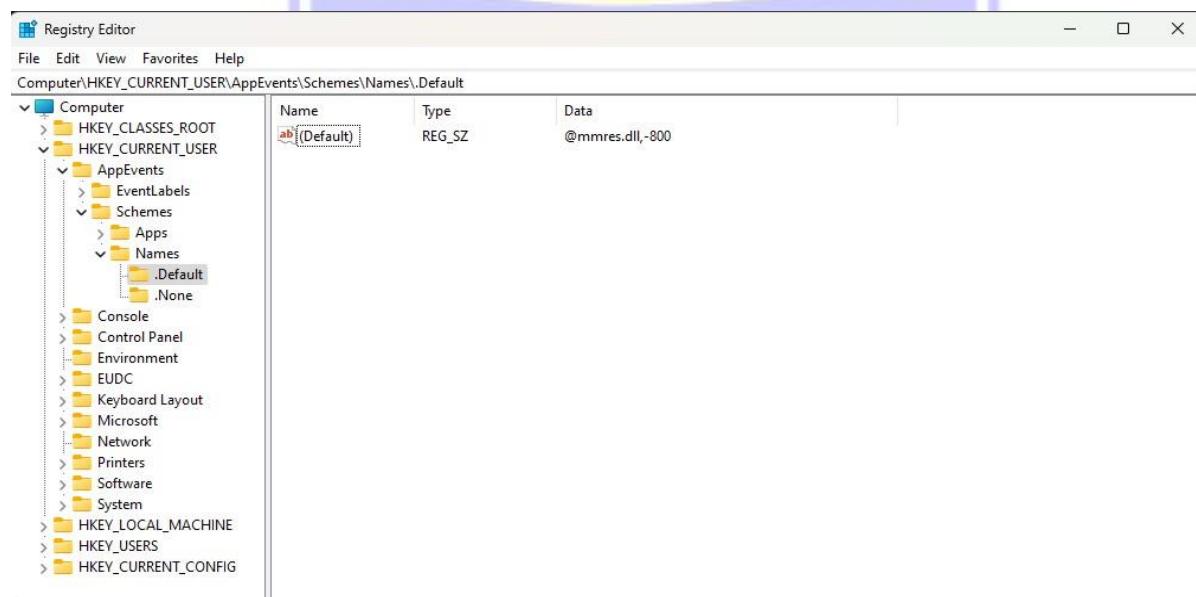
## Registry Information

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

निम्नलिखित जारी सेवाधरम



View the desired registries to be analyzed





## Result:

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

## Learning Outcomes:

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

## Course Outcomes:

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

## Conclusion:

## Viva Questions:

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



## PRACTICAL NO: 4

### Aim:

Capturing and analyzing network packets using WireShark (Fundamentals):

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

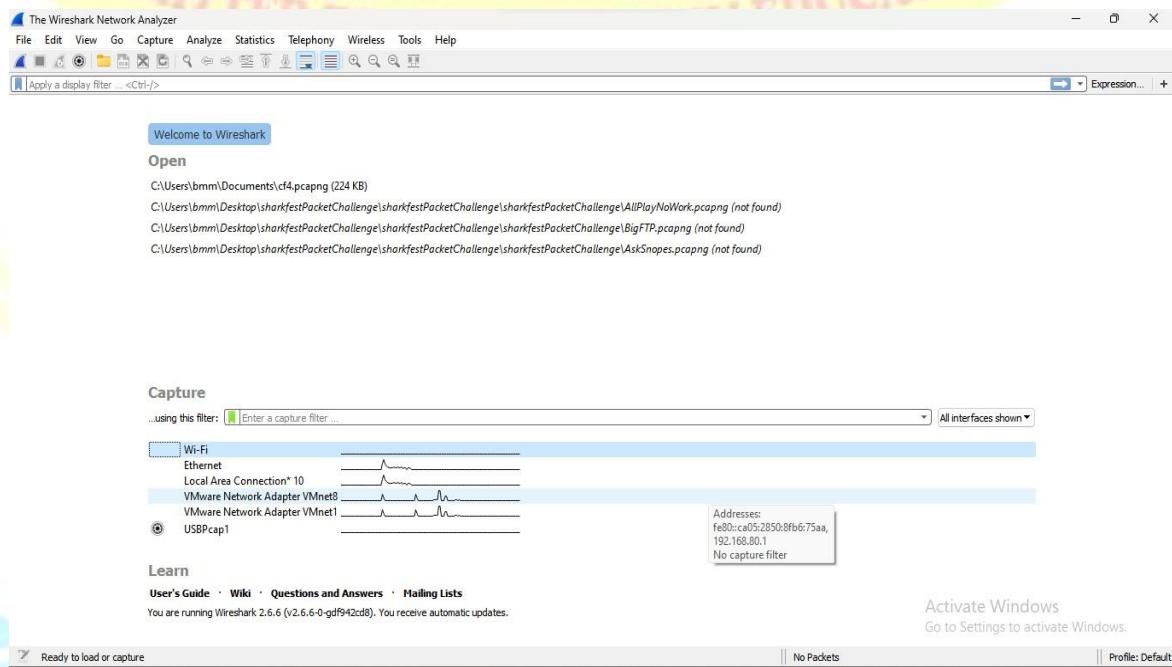
### Practical:

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

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

#### Identifying the Live Networks

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



### Capturing Network

We are now going to capture a network of Ethernet



# SHRI G.P.M. DEGREE COLLEGE

## Department of Computer

Vision.. Innovation.. Solution.. Presentation

The screenshot shows the WireShark application window. At the top, the menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help, and a search bar labeled 'Apply a display filter... <Ctrl-/>'. Below the menu is a toolbar with various icons for file operations and analysis. The main pane displays a list of network packets. The columns include No., Time, Source, Destination, Protocol, Length, Host, Server, Referer, and Info. The 'Info' column provides detailed descriptions of each packet's content. A yellow highlight covers several lines of the packet list, likely indicating selected traffic. Below the list, a status bar shows 'Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0'. The bottom of the window shows a hex dump of the selected packet, with bytes 0000 through 0030 displayed. The footer contains links to 'Activate Windows', 'Go to Settings to activate Windows.', and 'Profile: Default'.

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

### Analyze the Captured Packets

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

Default colors are:

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

Example these packets are delivered in an unordered manner.

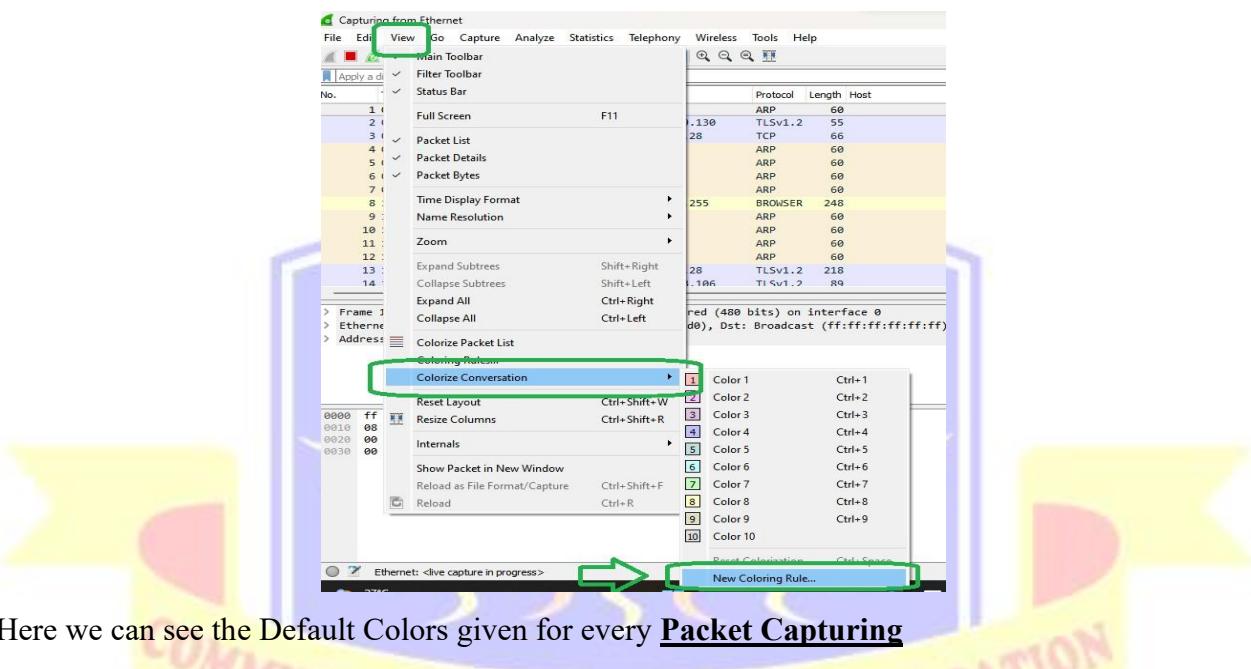
Click on View → Colorize Conversation → New Coloring Rule



# SHRI G.P.M. DEGREE COLLEGE

Department of Computer

Vision.. Innovation.. Solution.. Presentation



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

This screenshot shows the 'Coloring Rules Default' dialog in Wireshark. It lists various rules with their corresponding filters and colors. The rules include:

Name	Filter	Color
New coloring rule	eth.addr eq ac:85:3d:9d:bb:d0 and eth.addr eq ff:ff:ff:ff:ff:ff	Color 1
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)	Color 2
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)	Color 3
Bad TCP	tcp.analysis.flags && !tcp.analysis.window_update	Color 4
HSRP State Change	hsrp.state != 8 && hsrp.state != 16	Color 5
Spanning Tree Topology Change	stp.type == 0x80	Color 6
OSPF State Change	ospf.msg != 1	Color 7
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	Color 8
ARP	arp	Color 9
ICMP	icmp    icmpv6	Color 10
TCP RST	tcp.flags.reset eq 1	
SCTP ABORT	sctp.chunk_type eq ABORT	
TTL low or unexpected	(! ip.dst == 224.0.0/4 && ip.ttl < 5 && !(ipm && !lospf))    (ip.dst == 224.0.0/24 && ip.dst != 224.0.0.251 && ip.ttl != 1 && !(vrrp eth.fcs.status=="Bad"    ip.checksum.status=="Bad"    tcp.checksum.status=="Bad"    udp.checksum.status=="Bad"    sctp.checksum.status=="Bad"))	
Checksum Errors	smb    nbss    nbns    nbipx    ipxsap    netbios	
SMB	http    tcp.port == 80    http2	
HTTP	http    ipx    spx	
IPX		
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	

At the bottom of the dialog, there are buttons for '+', 'Foreground', 'Background', 'Apply as filter', 'OK', 'Cancel', 'Import...', 'Export...', and 'Help'.

Now we analyze data using filters provided in the Wireshark application

Write the following commands in the given area to apply filter



# SHRI G.P.M. DEGREE COLLEGE

Department of Computer

Vision.. Innovation.. Solution.. Presentation

Capturing from Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

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	CompalIn_fb:47:4f	Broadcast	ARP	60				Who has 192.168.10
7	0.497309	CompalIn_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

➤ ip.addr == 192.0.2.1

\*Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 192.0.2.1

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 ASCCL, 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	2.230843	216.239.34.181	192.168.10.28	TCP	66				443 + 50224 [ACK] Seq=1 Ack=2 Win=271 Len=0 SLE=1 SRE=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 .)@.....  
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 ..!]....



# SHRI G.P.M. DEGREE COLLEGE

Department of Computer

Vision.. Innovation.. Solution.. Presentation

## 1. Display packets which are coming from specific IP-address

➤ ip.src == 192.168.10.28

The screenshot shows the Wireshark interface with the filter set to "ip.src == 192.168.10.28". The packet list pane displays several TLSv1.2 and TCP connections initiated by the source IP. The details pane shows the structure of a selected TLS message, and the bytes pane shows the raw hex and ASCII data.

No.	Time	Source	Destination	Protocol	Length	Host	Server	Referer	Info
2	0.895299	192.168.10.28	142.250.199.130	TLSv1.2	55				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
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
22	2.227919	192.168.10.28	216.239.34.181	TLSv1.2	55				Application Data
28	2.393771	192.168.10.28	142.250.183.174	TCP	54				50202 > 443 [ACK] Seq=1074 Ack=396 Win=512 Len=0
29	2.395427	192.168.10.28	142.250.183.174	TLSv1.2	93				Application Data
32	3.144256	192.168.10.28	142.250.199.163	TLSv1.2	55				Application Data
34	3.190527	192.168.10.28	142.250.67.194	TLSv1.2	55				Application Data
38	3.702313	192.168.10.28	142.250.192.132	TLSv1.2	55				Application Data
45	5.149470	192.168.10.28	142.250.183.206	TLSv1.2	438				Application Data
46	5.149615	192.168.10.28	142.250.183.206	TLSv1.2	93				Application Data
47	5.14976	192.168.10.28	142.250.183.206	TLSv1.2	1466				

> Frame 2: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface 0  
> Ethernet II, Src: Sophos\_6b:22:63 (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"e|k ..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 ...]  
0040

## 2. Display packets which are having specific IP-address destination

➤ ip.dst == 192.168.10.28

The screenshot shows the Wireshark interface with the filter set to "ip.dst == 192.168.10.28". The packet list pane displays several TCP and TLS connections originating from various hosts to the destination IP. The details pane shows the structure of a selected TCP message, and the bytes pane shows the raw hex and ASCII data.

No.	Time	Source	Destination	Protocol	Length	Host	Server	Referer	Info
24142	1300.417362	184.80.58.44	192.168.10.28	TCP	74				443 > 61457 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK PE
24146	1300.445145	184.80.58.44	192.168.10.28	TCP	66				443 > 61457 [ACK] Seq=1 Ack=518 Win=64768 Len=0 TSval=2222634902 TS
24147	1300.446865	184.80.58.44	192.168.10.28	TLSv1.3	1514				Server Hello, Change Cipher Spec, Application Data
24148	1300.447033	184.80.58.44	192.168.10.28	TLSv1.3	1514				Continuation Data
24149	1300.447036	184.80.58.44	192.168.10.28	TLSv1.3	642				Continuation Data
24153	1300.506422	184.80.58.44	192.168.10.28	TCP	642				[TCP Retransmission] 443 > 61457 [PSH, ACK] Seq=2897 Ack=518 Win=64
24168	1300.668117	184.80.58.44	192.168.10.28	TCP	66				443 > 61457 [ACK] Seq=3473 Ack=598 Win=64768 Len=0 TSval=2222635125
24169	1300.673726	184.80.58.44	192.168.10.28	TLSv1.3	353				Application Data
24170	1300.673726	184.80.58.44	192.168.10.28	TLSv1.3	353				Application Data
24174	1300.701710	184.80.58.44	192.168.10.28	TCP	66				443 > 61457 [ACK] Seq=4047 Ack=1158 Win=64256 Len=0 TSval=222263515
24175	1300.701717	184.80.58.44	192.168.10.28	TLSv1.3	127				Application Data
24176	1300.701717	184.80.58.44	192.168.10.28	TLSv1.3	97				Application Data
24177	1300.701718	184.80.58.44	192.168.10.28	TLSv1.3	274				Application Data
24178	1300.701723	184.80.58.44	192.168.10.28	TLSv1.3	211				Application Data

> Frame 24142: 74 bytes on wire (592 bits), 74 bytes captured (592 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: 184.80.58.44, Dst: 192.168.10.28  
> Transmission Control Protocol, Src Port: 443, Dst Port: 61457, Seq: 0, Ack: 1, Len: 0

0000 f4 6b 8c 8e 6d 43 7c 5a 1c 6b 22 63 08 00 45 20 |k ..mC|Z -k"e| E  
0010 00 3c 00 00 40 00 39 06 d4 5b 68 50 3a 2c c0 a8 < .. @ 9 .. [hP, ..  
0020 0a 1c 01 bb f0 11 81 74 e7 56 b1 05 18 86 a0 12 ..... t ..V ..  
0030 fe 88 36 df 00 02 04 05 04 04 02 08 0a 84 7a ..6 .. ..z ..  
0040 b7 7a 00 6a 44 c4 01 03 03 07 z ..j0 .. ..



# SHRI G.P.M. DEGREE COLLEGE

Department of Computer

Vision.. Innovation.. Solution.. Presentation

### 3. Display packets which are using http protocol

➤ http

No.	Source	Destination	Protocol	Length	Host	Server	Referer	Info
13394	707.487777	15.207.161.196	HTTP	475				HTTP/1.1 200 OK (application/text)
13736	717.161381	15.207.161.196	HTTP	467				HTTP/1.1 200 OK (application/text)
14476	766.786676	15.207.161.196	HTTP	531				HTTP/1.1 200 OK (application/text)
16359	1047.517522	15.207.161.196	HTTP	531				HTTP/1.1 200 OK (application/text)
16477	1048.651494	15.207.161.196	HTTP	475				HTTP/1.1 200 OK (application/text)
18567	1050.078626	15.207.161.196	HTTP	475				HTTP/1.1 200 OK (application/text)
19534	1104.939537	15.207.161.196	HTTP	475				HTTP/1.1 200 OK (application/text)
22078	1201.576883	15.207.161.196	HTTP	507				HTTP/1.1 200 OK (application/text)
23760	1294.837652	15.207.161.196	HTTP	467				HTTP/1.1 200 OK (application/text)
23878	1296.327264	15.207.161.196	HTTP	443				HTTP/1.1 200 OK (application/text)
23908	1296.495246	15.207.161.196	HTTP	467				HTTP/1.1 200 OK (application/text)
23911	1296.675119	15.207.161.196	HTTP	435				HTTP/1.1 200 OK (application/text)
24134	1300.398824	15.207.161.196	HTTP	595				HTTP/1.1 200 OK (application/text)
24148	1477.948823	14.768.161.196	HTTP	444				HTTP/1.1 200 OK (application/text)

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

Activate Windows  
Go to Settings to activate

### 3. 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
23750	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,
23906	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	con-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	1347.9480233	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: f4:6b:8c:8e:6d:43 (f4:6b:8c:8e:6d:43), Dst: Sophos_6b:22:63 (7c:5a:1c:6b:22:63)
> Internet Protocol Version 4, Src: 192.168.10.28, Dst: 15.207.161.196
> Transmission Control Protocol, Src Port: 8080, Dst Port: 50399, Seq: 1437, Ack: 1597, Len: 349
> Hypertext Transfer Protocol
> HTML Form URL Encoded: application/x-www-form-urlencoded
```

Activate Wi  
Go to Settings

### 4. Display packets which are using TCP protocol

➤ tcp



# SHRI G.P.M. DEGREE COLLEGE

## Department of Computer

Vision.. Innovation.. Solution.. Presentation

\*Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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 I
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] S0244 → 443 [ACK] Seq=3779 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 I
24121	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	1300.386516	192.168.10.28	142.250.183.174	TCP	54				50202 → 443 [ACK] Seq=182074 Ack=90776 Win=510 Len=4
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	1300.347512	192.168.10.28	164.88.58.44	TCP	74				61454 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 Snd

> Frame 24132: 403 bytes on wire (3224 bits), 403 bytes captured (3224 bits) on interface 0  
 > Ethernet II, Src: f4:6b:8c:8e:6d:43 (f4:6b:8c:8e:6d:43), Dst: Sophos\_6b:22:63 (7c:5a:1c:6b:22:63)  
 > Internet Protocol Version 4, Src: 192.168.10.28, Dst: 15.207.161.196  
 > Transmission Control Protocol, Src Port: 50399, Dst Port: 8080, Seq: 1437, Ack: 1597, Len: 349

> Hypertext Transfer Protocol  
 > HTML Form URL Encoded: application/x-www-form-urlencoded

```
0000  7c 5a 1c 6b 22 63 f4 6b 8c 8e 6d 43 00 00 45 00 |Z k" c k ..mC..E
0010  01 85 ed e1 40 00 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 70 cf d0 00 00 50 4f 53 54 20 21 55 52 4c 43 ..}..PO ST /URLC
0040  61 74 65 67 6f 72 69 7a 65 72 53 65 72 76 69 63 aategoriz 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 58 2f 31 23 31 0d 0a 43 6f 6e 74 65 6e HTTP/1.1 ..Conten
0070  74 2d 54 79 70 65 3a 28 61 70 70 66 69 63 61 74 t-type: applicat
0080  69 6f 62 2f 78 2d 77 77 7d 2d 66 67 72 6d 2d 75 ion/x-w w-form-u
0090  72 6c 66 63 6f 64 65 64 0d 0a 55 73 65 72 2d rlencode d: User-
00a0  41 67 65 66 74 3a 29 6a 73 6f 6e 68 74 74 70 0d Agent: j sonhttp-
00b0  0a 48 6f 73 74 3a 29 70 72 6f 75 72 6c 2e 69 74 ..Host: p rourl.it
```

Activate Window  
Go to Settings to activate

5. Display packets having no error connecting to server

➤ http.response.code==200

\*Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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	766.786670	15.207.161.196	192.168.10.28	HTTP	531				HTTP/1.1 200 OK (application/text)
18359	1847.517522	15.207.161.196	192.168.10.28	HTTP	531				HTTP/1.1 200 OK (application/text)
18477	1948.661494	15.207.161.196	192.168.10.28	HTTP	475				HTTP/1.1 200 OK (application/text)
18567	1850.870626	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)
22978	1201.576883	15.207.161.196	192.168.10.28	HTTP	507				HTTP/1.1 200 OK (application/text)
23766	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	1296.327264	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: f4:6b:8c:8e:6d:43 (f4:6b:8c:8e:6d:43)  
 > Internet Protocol Version 4, Src: 15.207.161.196, Dst: 192.168.10.28  
 > Transmission Control Protocol, Src Port: 8080, Dst Port: 50399, Seq: 1216, Ack: 1437, Len: 381  
 > Hypertext Transfer Protocol  
 > Media Type

```
0000  f4 6b 8c 8e 6d 43 7c 5a 1c 6b 22 63 00 00 45 00 |k ..mC|Z k" c ..E
0010  01 a5 71 80 49 09 f2 06 99 7a 0f cf a1 c4 c0 a8 ..@.....
0020  a1 c4 c4 df 1f 90 80 72 82 fe e6 e2 7d dc 50 18 ..}...r ...};P
0030  00 7a d9 9b 00 08 54 50 2f 31 2e 31 29 32 z...HT TP/1.1 2
0040  30 38 20 34 4f 4b 0d 0a 44 61 74 65 3a 29 4d 6f 6e 00 OK-D ate: Mon
0050  2c 20 30 34 20 53 65 70 20 32 30 32 33 2d 30 33 , 04 Sep 2023 03
0060  3d 34 31 3a 35 32 2d 47 4d 54 0d 0a 43 6f 6e 74 :141:52 G MT-Cont
0070  65 6e 74 2d 54 79 70 65 3a 28 61 70 70 66 69 63 ent-type: applic
0080  61 74 69 6f 6e 2f 74 65 78 74 0d 0a 43 6f 6e 74 ation/te xt-Cont
0090  65 6e 74 2d 4c 65 6e 67 74 68 3a 20 32 34 38 0d ent-Leng th: 248
00a0  0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 .Connect ion: kee
00b0  70 2d 61 6c 69 76 65 0d 0a 0d 0a 52 56 5a 73 4c p-alive: ...RVZsL
```

Activate Window  
Go to Settings to activate

6. Display packets having port number 80, 443

➤ tcp.port==80 || udp.port==443



# SHRI G.P.M. DEGREE COLLEGE

## Department of Computer

Vision.. Innovation.. Solution.. Presentation

\*Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.port == 80

No.	Time	Source	Destination	Protocol	Length	Host	Server	Referer	Info
18651	1056.033875	129.227.29.114	192.168.10.28	TCP	60				80 → 61438 [FIN, ACK] Seq=252 Ack=253
18652	1056.072862	129.227.29.114	192.168.10.28	TCP	60				[TCP Retransmission] 80 → 61438 [SYN, ACK] Seq=253 Ack=254
18656	1056.142564	129.227.29.114	192.168.10.28	TCP	60				80 → 61438 [ACK] Seq=254 Ack=255
21848	1190.915180	129.227.29.114	192.168.10.28	TCP	66				80 → 61445 [SYN, ACK] Seq=0 Ack=1
21853	1191.098378	129.227.29.114	192.168.10.28	TCP	60				80 → 61445 [ACK] Seq=1 Ack=191
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
22048	1200.921342	129.227.29.114	192.168.10.28	HTTP	305		nginx		HTTP/1.1 204 No Content
22049	1200.921342	129.227.29.114	192.168.10.28	TCP	60				80 → 61446 [FIN, ACK] Seq=252 Ack=253
22052	1200.923718	129.227.29.114	192.168.10.28	TCP	60				80 → 61446 [ACK] Seq=253 Ack=192
23915	1296.68R350	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 |···X··· ···

\*Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

udp.port == 443

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	77.406296	192.168.10.28	142.250.192.74	UDP	1292				61370 → 443 Len=1250
2437	77.5567800	192.168.10.28	142.250.192.74	UDP	1292				61371 → 443 Len=1250
2454	77.685952	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	HTTP	1292				61373 → 443 Len=1250

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

0000 7c 5a 1c 6b 22 63 f4 6b 8c 8e 6d 43 08 00 45 00 |Z ·k"c· k ·mC··E·
0010 04 fe 2b e8 40 00 34 11 f1 fd c0 a8 0a 1c 8e fa |+@> ···
0020 c0 4a ef ba 01 bb 04 ea 3c 43 c7 00 00 00 01 08 |J ··· <C···
0030 a3 5d 49 4f 89 51 a2 9c 00 00 44 d8 a8 7d f2 71 |] O Q ··· D ·} q
0040 c8 fb 00 89 78 01 66 4a 67 c4 9b 21 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 |··dg!5 ·& 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{ ···> ··T
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 |···= j ·( s ·h

## 7. Display packets which that contains keyword facebook

➤ tcp contains facebook



# SHRI G.P.M. DEGREE COLLEGE

Department of Computer

Vision.. Innovation.. Solution.. Presentation

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

No.	Time	Source	Length	Host	Server	Referer	User Datagram Pr
81	7.174002	192.168.10.28	943	protecti.quickheal...			
84	7.193165	192.168.10.28	52				
370	16.971015	192.168.10.28	391	prourl.itsecure.co...			
390	16.993394	192.168.10.28	411				
686	28.307436	192.168.10.28	342	ctld1.windowsupdate...			
688	28.424126	192.168.10.28	430				
689	28.435624	192.168.10.28	336	ctld1.windowsupdate...			
693	28.494959	192.168.10.28	429				
694	28.509564	192.168.10.28	336	ctld1.windowsupdate...			
696	28.568902	192.168.10.28	445				
3154	68.644107	192.168.10.28	281	x1.c.lencr.org			
3158	68.702883	192.168.10.28	1099				
3419	71.900527	192.168.10.28	911	protecti.quickheal...			
3424	71.911183	192.168.10.28	617				



# SHRI G.P.M. DEGREE COLLEGE

Department of Computer

Vision.. Innovation.. Solution.. Presentation

Now we can see the Host

\*Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Host	Serve	Referer	User Datagram Protocol	Interr	Addre	Trans	Host	Host	Info
81	7.174002	192.168.10.28	52.66.77.132	HTTP	943	pro...				✓	✓	✓	protecti.quickheal...	protecti.quickheal.com	POST /ghcl
84	7.193165	52.66.77.132	192.168.10.28	HTTP	617					✓	✓				HTTP/1.1 2
370	16.971015	192.168.10.28	13.233.218.43	HTTP	391	pro...				✓	✓	✓	prourl.itsecure.co...	prourl.itsecure.co.in:8080	POST /URLC
390	16.993394	13.233.210.43	192.168.10.28	HTTP	411					✓	✓				HTTP/1.1 2
686	28.307436	192.168.10.28	182.156.239.16	HTTP	342	ctl...				✓	✓	✓	ctld1.windowsupdate...	ctld1.windowsupdate.com	HTTP/1.1 3
688	28.424126	182.156.239.16	192.168.10.28	HTTP	430	Mic...				✓	✓	✓	ctld1.windowsupdate...	ctld1.windowsupdate.com	HTTP/1.1 3
689	28.435624	192.168.10.28	182.156.239.16	HTTP	336	ctl...				✓	✓	✓	ctld1.windowsupdate...	ctld1.windowsupdate.com	HTTP/1.1 3
693	28.494959	182.156.239.16	192.168.10.28	HTTP	429	Mic...				✓	✓	✓			HTTP/1.1 3
694	28.509564	192.168.10.28	182.156.239.16	HTTP	336	ctl...				✓	✓	✓	ctld1.windowsupdate...	ctld1.windowsupdate.com	GET /msdow
696	28.568902	182.156.239.16	192.168.10.28	HTTP	445	Foo...				✓	✓	✓			HTTP/1.1 3
3154	68.644107	192.168.10.28	23.205.216.18	HTTP	281	x1...				✓	✓	✓	x1.c.lencr.org	x1.c.lencr.org	GET / HTTP
3158	68.702883	23.205.216.18	192.168.10.28	PKIX-C...	1099	ngi...				✓	✓	✓			Certificat
3419	71.900527	192.168.10.28	13.235.126.38	HTTP	911	pro...				✓	✓	✓	protecti.quickheal...	protecti.quickheal.com	POST /ghcl
3424	71.911183	13.235.126.38	192.168.10.28	HTTP	617					✓	✓	✓	nprotecti.quickheal...	nprotecti.quickheal.com	HTTP/1.1 2
3915	75.141161	192.168.10.28	13.235.126.38	HTTP	911	nn...				✓	✓	✓	nprotecti.quickheal...	nprotecti.quickheal.com	POST /ghcl

> Frame 81: 943 bytes on wire (7544 bits), 943 bytes captured (7544 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: 52.66.77.132  
> Transmission Control Protocol, Src Port: 59594, Dst Port: 80, Seq: 1, Ack: 1, Len: 889

✓ Hypertext Transfer Protocol  
> POST /ghclousec/lookup/file/scan HTTP/1.1\r\n Host: protecti.quickheal.com\r\n Accept: \*/\*\r\n [truncated]Authorization: eyJraiwQ10iIyMDjjoDVKhylMmQ5LTrizjEtYTRmYij0DQ8ZDc4H2hJ2WU1LCJhbGciOiJSUzI1NiJ9.eyJrZXkiOiJjcjAwT01OMzQ30EFVmK4c09R%WnIiwidXNlciiG1kVQuy03LjUiLCJiaWQiOEsIm\r\n Content-Type: text/plain\r\n Content-Length: 384\r\n \r\n [Full request URI: http://protecti.quickheal.com/ghclousec/lookup/file/scan]  
[HTTP request 1/1]  
[Response in frame: 84]  
File Data: 384 bytes

Activate Windows

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





# SHRI G.P.M. DEGREE COLLEGE

## Department of Computer

Vision.. Innovation.. Solution.. Presentation

```

Frame 81: 943 bytes on wire (7544 bits), 943 bytes captured (7544 bits)
Ethernet II, Src: Sophos_1 [08:00:00:00:00:01], Dst: Sophos_1 [08:00:00:00:00:01]
Internet Protocol Version 4, Src: 192.168.10.28, Dst: 52.66.77.132
Transmission Control Protocol, Src Port: 59594, Dst Port: 80, Seq: 1, Ack: 1
HTTP Transfer Protocol
    > POST /qhcloudsec/lookup/file/scan HTTP/1.1\r\n
    Host: protecti.quickheal.com\r\n
    Accept: */*\r\n
    Authorization: eyJraWQiOiIyMDJjODVkyM1iMmQ5LTrIZjEtYTRmYy1jODQ0ZDc4M2NjZwUiLCJhbGciOiJSUzI1NiJ9.eyJrZXkiOiJjcjAwT010MzQ30EFNmK4c09RMWhnIiwi
    dXNlciI6IkVQy0SlJuilCjiawQiojeSImV4cCI6NT5NtC30TA3Nn0.kDQHAs_Q7DU5RPBACsboZGwn1kPa67dSL9EJ3CxYexhZVD-
    SFH61gztz53Tbkez0JrtdgWPFOwvk7e-2B96pfVBUYzapJ4l6x6MdMf-UmjUiIdN9WcDeKJm3zqR7Hf96QZq4ff98bCLGr-hI8A3ad6DxnaPx4QHBBHG2gY
    Content-Type: text/plain\r\n
    Content-Length: 384\r\n
    [Full request URI: http://protecti.quickheal.com/qhcloudsec/lookup/file/scan]

```

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

```

POST /qhcloudsec/lookup/file/scan HTTP/1.1
Host: protecti.quickheal.com
Accept: */*
Authorization: eyJraWQiOiIyMDJjODVkyM1iMmQ5LTrIZjEtYTRmYy1jODQ0ZDc4M2NjZwUiLCJhbGciOiJSUzI1NiJ9.eyJrZXkiOiJjcjAwT010MzQ30EFNmK4c09RMWhnIiwi
dXNlciI6IkVQy0SlJuilCjiawQiojeSImV4cCI6NT5NtC30TA3Nn0.kDQHAs_Q7DU5RPBACsboZGwn1kPa67dSL9EJ3CxYexhZVD-
SFH61gztz53Tbkez0JrtdgWPFOwvk7e-2B96pfVBUYzapJ4l6x6MdMf-UmjUiIdN9WcDeKJm3zqR7Hf96QZq4ff98bCLGr-hI8A3ad6DxnaPx4QHBBHG2gY
Content-Type: text/plain
Content-Length: 384
Date: Fri, 08 Sep 2023 06:22:36 GMT
Content-Type: text/plain
Content-Length: 374
X-SERVER-ID: UUhQVEk=
Via: HTTP/1.1 forward.http.proxy:3128
Connection: keep-alive

7970Mh1HmN1FQF50EHci8v6zu19-
Kee7Ge5Q0_TMZowqz5C8T61h9Pd1qK2yElj82_oIHVB5tgg3JUwsx8Byo2I9b_s8Pkgnycd4chs7MNns8hBKIZg79MQDKceYv3VgHdJIqdsL7Qm0iSinfawj9sI
-6nS9sgu-ZGW0QhWOKC3yGCSOJN8yh_XPCp-
uHyazGpy60CDU4DDcm7NwBypKlx0D_AEx2041xHdDrNv23uCI5140lwj4hs3rjtXzLsLR7koswIEYbQVWduu7Ifyf3w7MkenDw9UQy1SHfEpRVA0KH0Y_VqGaw-
nB04_-psCuxsrQuL0ULfbp7SFUZXhiciMlsSIjr3aG5ozf6_vnzm-JR7j8UGBPqNy_IBUxHTTP/1.1 200 OK

```

1 client pkt, 1 server pkt. 1 turn.

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

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

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

### Analysis –

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

In the search frame type **frame matches “microsoft”**



# SHRI G.P.M. DEGREE COLLEGE

Department of Computer

Vision.. Innovation.. Solution.. Presentation

No.	Time	Source	Destination	Protocol	Length	Host	Serve	Referer	User Datagram Protocol	Interr	Addre	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 0x0edfb A fd.api.iris.mi
2347	119.540691	192.168.10.1	192.168.10.28	DNS	208				✓	✓				Standard query response 0x0edfb 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				✓	✓				Ignore Unknown Record
2357	119.733920	20.24.121.134	192.168.10.28	TLSv1.2	1514				✓	✓				Ignore Unknown Record
2360	119.734256	20.24.121.134	192.168.10.28	TLSv1.2	1514				✓	✓				Ignore Unknown Record
213	6.762757	192.168.10.28	239.255.255.250	SSDP	217	239.25...			✓	✓				239.255.255... M-SEARCH * HTTP/1.1
225	7.765877	192.168.10.28	239.255.255.250	SSDP	217	239.25...			✓	✓				239.255.255... M-SEARCH * HTTP/1.1
234	8.772968	192.168.10.28	239.255.255.250	SSDP	217	239.25...			✓	✓				239.255.255... M-SEARCH * HTTP/1.1
252	9.780504	192.168.10.28	239.255.255.250	SSDP	217	239.25...			✓	✓				239.255.255... M-SEARCH * HTTP/1.1
474	27.935260	192.168.10.52	239.255.255.250	SSDP	217	239.25...			✓	✓				239.255.255... M-SEARCH * HTTP/1.1
479	28.935641	192.168.10.52	239.255.255.250	SSDP	217	239.25...			✓	✓				239.255.255... M-SEARCH * HTTP/1.1
487	29.941067	192.168.10.52	239.255.255.250	SSDP	217	239.25...			✓	✓				239.255.255... M-SEARCH * HTTP/1.1
494	30.941066	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:8e:6d:43 (f4:6b:8c:8e: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	Interr	Addre	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 0x0edfb A fd.api.iris.mi
2347	119.540691	192.168.10.1	192.168.10.28	DNS	208				✓	✓				Standard query response 0x0edfb 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				✓	✓				Ignore Unknown Record
2357	119.733920	20.24.121.134	192.168.10.28	TLSv1.2	1514				✓	✓				Ignore Unknown Record
2360	119.734256	20.24.121.134	192.168.10.28	TLSv1.2	1514				✓	✓				Ignore Unknown Record
213	6.762757	192.168.10.28	239.255.255.250	SSDP	217	239.25...			✓	✓				239.255.255... M-SEARCH * HTTP/1.1
225	7.765877	192.168.10.28	239.255.255.250	SSDP	217	239.25...			✓	✓				239.255.255... M-SEARCH * HTTP/1.1
234	8.772968	192.168.10.28	239.255.255.250	SSDP	217	239.25...			✓	✓				239.255.255... M-SEARCH * HTTP/1.1
252	9.780504	192.168.10.28	239.255.255.250	SSDP	217	239.25...			✓	✓				239.255.255... M-SEARCH * HTTP/1.1
474	27.935260	192.168.10.52	239.255.255.250	SSDP	217	239.25...			✓	✓				239.255.255... M-SEARCH * HTTP/1.1
479	28.935641	192.168.10.52	239.255.255.250	SSDP	217	239.25...			✓	✓				239.255.255... M-SEARCH * HTTP/1.1
487	29.941067	192.168.10.52	239.255.255.250	SSDP	217	239.25...			✓	✓				239.255.255... M-SEARCH * HTTP/1.1
494	30.941066	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:8e:6d:43 (f4:6b:8c:8e:6d:43), Dst: IPv4mcast\_7ff:ff:fa (01:00:5e:7f:ff:fa)  
> Internet Protocol Version 4, Src: 192.168.10.28, Dst: 239.255.255.250  
> User Datagram Protocol, Src Port: 62928, Dst Port: 1900  
> Simple Service Discovery Protocol  
> M-SEARCH \* HTTP/1.1\r\nHOST: 239.255.255.250:1900\r\nMAN: "ssdp:discover"\r\n\r\n[Full request URL: http://239.255.255.250:1900/\r\n[HTTP request 1/4]\r\n[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”.



# SHRI G.P.M. DEGREE COLLEGE

Department of Computer

Vision.. Innovation.. Solution.. Presentation

The screenshot shows the Wireshark interface with a list of captured frames. Frame 4109 is selected, which corresponds to the highlighted packet in the list. The packet details show it's an HTTP POST request from 192.168.10.28 to 192.168.10.28, port 80, to '/qhcloudsec/ers/report/save HTTP/1.1'. The payload contains the text 'protecti.qui... POST /qhcloudsec/ers/report/save HTTP/1.1'. The expanded Hypertext Transfer Protocol tab shows the request and response messages.

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

The screenshot shows the Wireshark interface with a list of captured frames. The protocol tree on the left shows 'tcp.port eq 80'. The 'Protocol Preferences' dialog box is open, and the 'Transmission Control Protocol' section is selected. The 'Allow subdissector to reassemble TCP streams' checkbox is checked and highlighted with a green box. Other options like 'Validate the TCP checksum if possible' and 'Analyze TCP sequence numbers' are also visible.

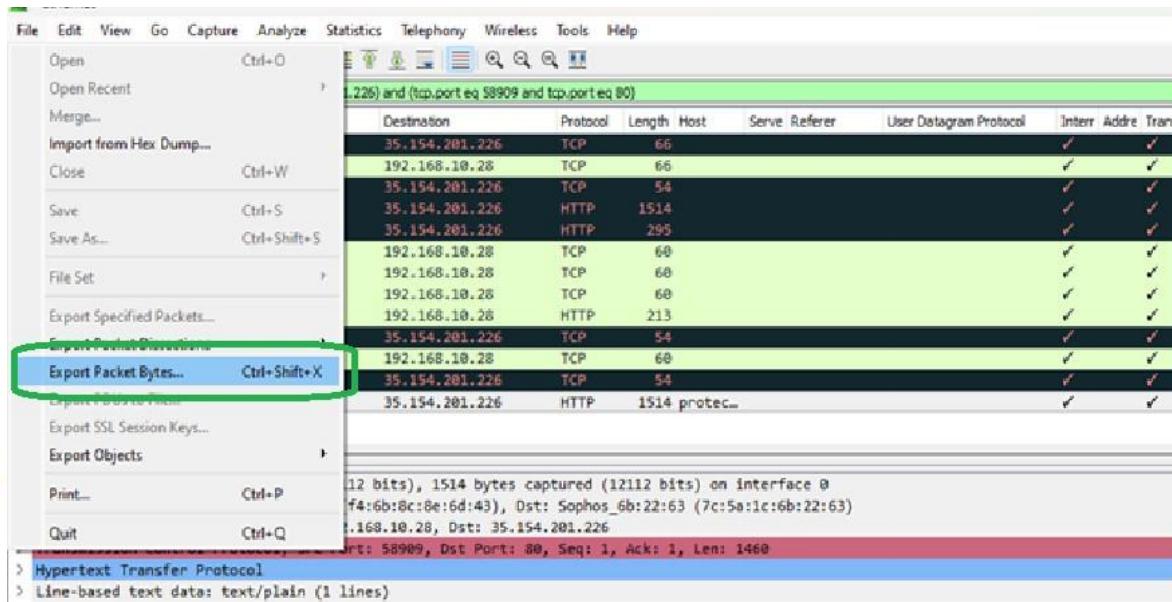


# SHRI G.P.M. DEGREE COLLEGE

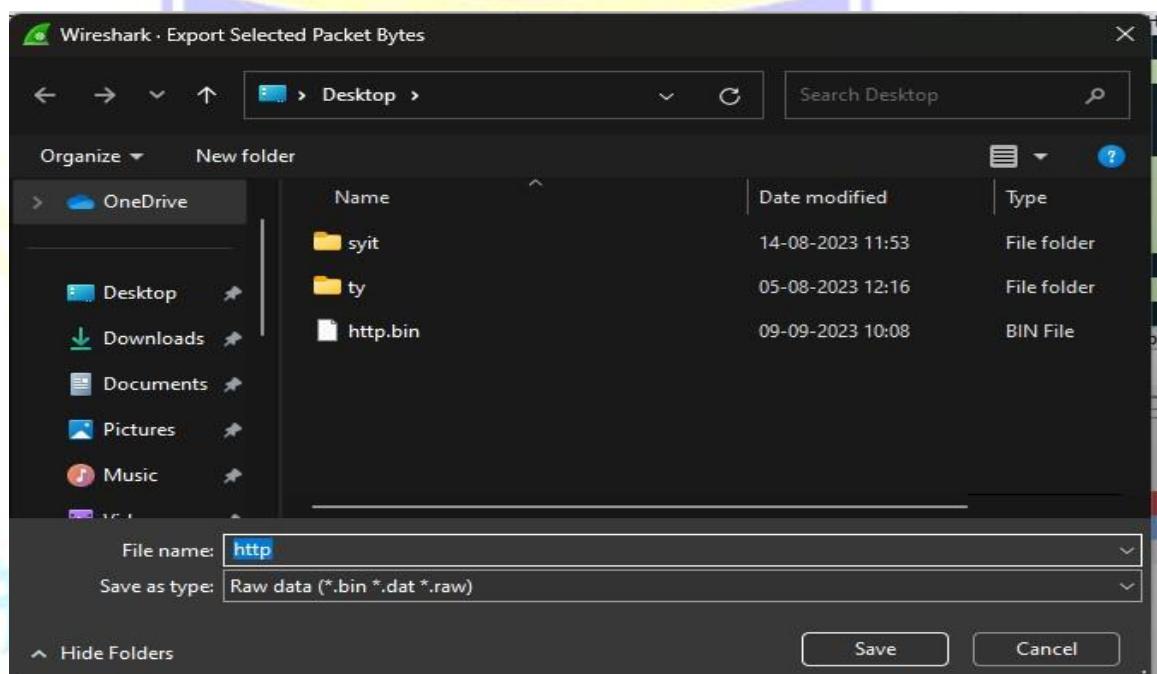
Department of Computer

Vision.. Innovation.. Solution.. Presentation

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 –



# SHRI G.P.M. DEGREE COLLEGE

Department of Computer

Vision.. Innovation.. Solution.. Presentation

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.

No.	Time	Source	Destination	Protocol	Length	Host	Serve	Referer	User Datagram Protocol	Interr	Addre	Trans	Host	Info
1427	133.760427	192.168.10.48	192.168.10.28	HTTP	417	Mic..				✓	✓		HTTP/1.1 200 OK (JPEG/JFIF image)	
1445	133.765975	192.168.10.48	192.168.10.28	HTTP	1491	Mic..				✓	✓		HTTP/1.1 200 OK (PNG)	
1451	133.769061	192.168.10.48	192.168.10.28	HTTP	914	Mic..				✓	✓		HTTP/1.1 200 OK (JPEG/JFIF image)	
1459	133.772352	192.168.10.48	192.168.10.28	HTTP	696	Mic..				✓	✓		HTTP/1.1 200 OK (PNG)	
1471	133.776633	192.168.10.48	192.168.10.28	HTTP	566	Mic..				✓	✓		HTTP/1.1 200 OK (image/bmp)	
1476	133.780159	192.168.10.48	192.168.10.28	HTTP	453	Mic..				✓	✓		HTTP/1.1 200 OK (JPEG/JFIF image)	
1483	133.783575	192.168.10.48	192.168.10.28	HTTP	1286	Mic..				✓	✓		HTTP/1.1 200 OK (image/bmp)	
1489	133.790546	192.168.10.48	192.168.10.28	HTTP/X...	1168	Mic..				✓	✓		HTTP/1.1 200 OK	
1508	133.797940	192.168.10.48	192.168.10.28	HTTP/X...	467	Mic..				✓	✓		HTTP/1.1 200 OK	
1516	133.803319	192.168.10.48	192.168.10.28	HTTP/X...	269	Mic..				✓	✓		HTTP/1.1 200 OK	
1531	133.901852	23.9.121.14	192.168.10.28	HTTP	389	Aka..				✓	✓		HTTP/1.1 302 Moved Temporarily	
1555	134.012853	35.154.201.226	192.168.10.28	HTTP	617					✓	✓		HTTP/1.1 200 OK (text/plain)	
1565	134.403175	138.91.171.81	192.168.10.28	HTTP/X...	731	Mic..				✓	✓		HTTP/1.1 200 OK	

> Frame 13: 617 bytes on wire (4936 bits), 617 bytes captured (4936 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: 52.66.77.132, Dst: 192.168.10.28  
> Transmission Control Protocol, Src Port: 80, Dst Port: 64882, Seq: 1, Ack: 858, Len: 563  
> Hypertext Transfer Protocol  
> Line-based text data: text/plain (1 lines)

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

No.	Time	Protocol	Length	Host	Referer	User Datagram Protocol	Interr	Addre	Trans	Host	Info
1565	134.40	HTTP/X...	731				✓	✓		HTTP/1.1 200 OK (JPEG/JFIF image)	
656	58.776	HTTP/X...	1270				✓	✓		HTTP/1.1 200 OK	
662	58.780	HTTP/X...	1270				✓	✓		HTTP/1.1 200 OK	
676	58.790	HTTP	417				✓	✓		HTTP/1.1 200 OK (JPEG/JFIF image)	
694	58.794	HTTP	1491				✓	✓		HTTP/1.1 200 OK (PNG)	
708	58.797	HTTP	914				✓	✓		HTTP/1.1 200 OK (JPEG/JFIF)	
708	58.799	HTTP	696				✓	✓		HTTP/1.1 200 OK (PNG)	
720	58.802	HTTP	566				✓	✓		HTTP/1.1 200 OK (image/bmp)	
726	58.806	HTTP	453				✓	✓		HTTP/1.1 200 OK (JPEG/JFIF)	
733	58.809	HTTP	1286				✓	✓		HTTP/1.1 200 OK (image/bmp)	
739	58.814	HTTP/X...	1168				✓	✓		HTTP/1.1 200 OK	
750	58.820	HTTP/X...	467				✓	✓		HTTP/1.1 200 OK	
767	58.827	HTTP/X...	269				✓	✓		HTTP/1.1 200 OK	
1405	133.74	HTTP/X...	1770				✓	✓		HTTP/1.1 200 OK	

> Frame 676: 41 bytes on wire (3336 bits), 41 bytes captured (3336 bits) on interface 0  
> Ethernet II, Src: f4:6b:8c:8e:6d:43 (f4:6b:8c:8e:6d:43), Dst: 192.168.10.28 (192.168.10.28)  
> Internet Protocol Version 4, Src: 52.66.77.132, Dst: 192.168.10.28  
> Transmission Control Protocol, Seq: 4568, Ack: 193, Len: 363  
> [5 Reassembled fragments]  
> Hypertext Transfer Protocol  
> HTTP/1.1 200 OK  
> Content-Length: 363  
> Content-Type: text/html  
Server: Microsoft-Windows/6.3.0 UPnP/1.0 UPnP-Device-Mgmt/1.0 Microsoft-HTTPAPI/2.0\r\n\r\n  
Date: Sat, 09 Sep 2023 06:37:29 GMT\r\n\r\n  
[HTTP response 1/8]  
[Time since request: 0.002430000 seconds]  
[Request in frame: 669]  
[Next request in frame: 6771]  
[Next response in frame: 694]

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



# SHRI G.P.M. DEGREE COLLEGE

Department of Computer

Vision.. Innovation.. Solution.. Presentation

No.	Time	Source	Destination	Protocol	Length	Host	Referer	Server	User Datagram Protocol	Interr	Addre	Trans	Host	Info
733	58.809293	192.168.10.47	192.168.10.28	HTTP	1286			Microsoft-Windows/6.3 UPnP/1.0 UPnP-Device-H...		✓	✓		HTTP/1.1 :	
739	58.814959	192.168.10.47	192.168.10.28	HTTP/X...	1168			Microsoft-Windows/6.3 UPnP/1.0 UPnP-Device-H...		✓	✓		HTTP/1.1 :	
750	58.820924	192.168.10.47	192.168.10.28	HTTP/X...	467			Microsoft-Windows/6.3 UPnP/1.0 UPnP-Device-H...		✓	✓		HTTP/1.1 :	
767	58.827250	192.168.10.47	192.168.10.28	HTTP/X...	269			Microsoft-Windows/6.3 UPnP/1.0 UPnP-Device-H...		✓	✓		HTTP/1.1 :	
782	58.923739	23.9.121.14	192.168.10.28	HTTP	389			AkamaiHost		✓	✓		HTTP/1.1 :	
807	59.348985	20.231.121.79	192.168.10.28	HTTP/X...	731			Microsoft-IIS/10.0		✓	✓		HTTP/1.1 :	
982	94.327644	192.168.10.1	192.168.10.28	HTTP	384			Microsoft-IIS/10.0		✓	✓		HTTP/1.1 :	
985	94.339859	192.168.10.1	192.168.10.28	HTTP	384			Microsoft-IIS/10.0		✓	✓		HTTP/1.1 :	
988	94.346552	192.168.10.1	192.168.10.28	HTTP	384			Microsoft-IIS/10.0		✓	✓		HTTP/1.1 :	
991	94.354087	192.168.10.1	192.168.10.28	HTTP	384			Microsoft-IIS/10.0		✓	✓		HTTP/1.1 :	
994	94.360437	192.168.10.1	192.168.10.28	HTTP	384			Microsoft-IIS/10.0		✓	✓		HTTP/1.1 :	
997	94.368192	192.168.10.1	192.168.10.28	HTTP	384			Microsoft-IIS/10.0		✓	✓		HTTP/1.1 :	
1000	94.376016	192.168.10.1	192.168.10.28	HTTP	384			Microsoft-IIS/10.0		✓	✓		HTTP/1.1 :	
1003	94.383396	192.168.10.1	192.168.10.28	HTTP	384			Microsoft-IIS/10.0		✓	✓		HTTP/1.1 :	

```
> Frame 1000: 384 bytes on wire (3072 bits), 384 bytes captured (3072 bits) on interface 0
> Ethernet II, Src: Compaq_1fb:47:4f (98:29:a6:fb:47:4f), Dst: f4:6b:8c:8e:6d:43 (f4:6b:8c:8e:6d:43)
> Internet Protocol Version 4, Src: 192.168.10.1, Dst: 192.168.10.28
> Transmission Control Protocol, Src Port: 8181, Dst Port: 64904, Seq: 1981, Ack: 1169, Len: 330
✓ Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Content-Type: application/x-unknown\r\n\r\n
    Last-Modified: Mon, 29 Nov 2021 06:23:48 GMT\r\n
    Accept-Ranges: bytes\r\n
    ETag: "10c73abe9e4ad71:0"\r\n
    Server: Microsoft-IIS/10.0\r\n
    X-Frame-Options: SAMEORIGIN\r\n
    X-XSS-Protection: 1;mode=block\r\n
    X-Content-Type-Options: nosniff\r\n
    Date: Sun, 28 Nov 2021 06:23:48 GMT\r\n
```

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

No.	Time	Source	Destination	Protocol	Length	Host	Referer	Server	User Datagram Protocol	Interr	Addre	Trans	Host	Info
609	56.193155	192.168.10.47	239.255.255.250	SSDP	474	239...		Microsoft-Windows/6.3 UPnP/1.0 UPnP-Device-H...		✓			239...	NOTIFY * ;
610	56.193298	fe80::7951:a59d:8ef0:ff02::c		SSDP	502	[FF...		Microsoft-Windows/6.3 UPnP/1.0 UPnP-Device-H...		✓			[FF...	NOTIFY * ;
611	56.273287	fe80::7951:a59d:8ef0:ff02::c		SSDP	511	[FF...		Microsoft-Windows/6.3 UPnP/1.0 UPnP-Device-H...		✓			[FF...	NOTIFY * ;
612	56.273350	192.168.10.47	239.255.255.250	SSDP	483	239...		Microsoft-Windows/6.3 UPnP/1.0 UPnP-Device-H...		✓			239...	NOTIFY * ;
617	56.273356	fe80::7951:a59d:8ef0:ff02::c		SSDP	554	[FF...		Microsoft-Windows/6.3 UPnP/1.0 UPnP-Device-H...		✓			[FF...	NOTIFY * ;
618	56.344441	192.168.10.47	239.255.255.250	SSDP	526	239...		Microsoft-Windows/6.3 UPnP/1.0 UPnP-Device-H...		✓			239...	NOTIFY * ;
619	56.421796	fe80::7951:a59d:8ef0:ff02::c		SSDP	568	[FF...		Microsoft-Windows/6.3 UPnP/1.0 UPnP-Device-H...		✓			[FF...	NOTIFY * ;
620	56.421860	192.168.10.47	239.255.255.250	SSDP	540	239...		Microsoft-Windows/6.3 UPnP/1.0 UPnP-Device-H...		✓			239...	NOTIFY * ;
623	56.499128	fe80::7951:a59d:8ef0:ff02::c		SSDP	566	[FF...		Microsoft-Windows/6.3 UPnP/1.0 UPnP-Device-H...		✓			[FF...	NOTIFY * ;
624	56.499132	192.168.10.47	239.255.255.250	SSDP	538	239...		Microsoft-Windows/6.3 UPnP/1.0 UPnP-Device-H...		✓			239...	NOTIFY * ;
627	56.569693	fe80::7951:a59d:8ef0:ff02::c		SSDP	582	[FF...		Microsoft-Windows/6.3 UPnP/1.0 UPnP-Device-H...		✓			[FF...	NOTIFY * ;
628	56.569759	192.168.10.47	239.255.255.250	SSDP	554	239...		Microsoft-Windows/6.3 UPnP/1.0 UPnP-Device-H...		✓			239...	NOTIFY * ;
656	58.776182	192.168.10.47	192.168.10.28	HTTP/X...	1270			Microsoft-Windows/6.3 UPnP/1.0 UPnP-Device-H...		✓	✓		HTTP/1.1 :	
662	58.780455	192.168.10.47	192.168.10.28	HTTP/X...	1770			Microsoft-Windows/6.3 UPnP/1.0 UPnP-Device-H...		✓	✓		HTTP/1.1 :	

```
> Frame 609: 474 bytes on wire (3792 bits), 474 bytes captured (3792 bits) on interface 0
> Ethernet II, Src: Giga-Byt_aaa52:e0 (1c:1b:0d:aa:52:e0), Dst: IPv4mcast_7:f7:ff:fa (01:00:5e:7f:ff:fa)
> Internet Protocol Version 4, Src: 192.168.10.47, Dst: 239.255.255.250
> User Datagram Protocol, Src Port: 1900, Dst Port: 1900
✓ Simple Service Discovery Protocol
  > NOTIFY * HTTP/1.1\r\n
    Host:239.255.255.250:1900\r\n
    NT:upnp:rootdevice\r\n
    NTS:ssdp:alive\r\n
    Location:http://192.168.10.47:2869/upnphost/udhisapi.dll?content=uuid:f33dfca1-0fa9-44ad-a64c-b9395679a96c\r\n
    USN:uuid:f33dfca1-0fa9-44ad-a64c-b9395679a96c\r\n
```

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



# SHRI G.P.M. DEGREE COLLEGE

Department of Computer

Vision.. Innovation.. Solution.. Presentation

No.	Time	Source	Host	Referer	Server
609	56.193155	192.168.10.47	1 [239...]		Microsoft-Windows/6.3 L
610	56.193298	fe80::7951:a	2 [FF...]		Microsoft-Windows/6.3 L
611	56.273287	fe80::7951:a	3 [FF...]		Microsoft-Windows/6.3 L
612	56.273350	192.168.10.47	3 [239...]		Microsoft-Windows/6.3 L
617	56.344374	fe80::7951:a5	4 [FF...]		Microsoft-Windows/6.3 L
618	56.344441	192.168.10.47	6 [239...]		Microsoft-Windows/6.3 L
619	56.421796	fe80::7951:a5	8 [FF...]		Microsoft-Windows/6.3 L
620	56.421860	192.168.10.47	9 [239...]		Microsoft-Windows/6.3 L
623	56.496120	fe80::7951:a5	6 [FF...]		Microsoft-Windows/6.3 L
624	56.496192	192.168.10.47	8 [239...]		Microsoft-Windows/6.3 L
627	56.569693	fe80::7951:a5	2 [FF...]		Microsoft-Windows/6.3 L
628	56.569759	192.168.10.47	4 [239...]		Microsoft-Windows/6.3 L
656	58.776182	192.168.10.47	0 [0]		Microsoft-Windows/6.3 L
662	58.780455	192.168.10.47	0 [0]		Microsoft-Windows/6.3 L

Frame 618: 526 bytes on wire (420 bits), 526 bytes captured (420 bits) on interface 0  
Ethernet II, Src: Giga-Byt\_aa:52:, Dst: Microsoft-Broadcom/Broadcom (08:00:22:aa:52:00)  
Internet Protocol Version 4, Src: 192.168.10.47, Dst: 239.255.255.250  
User Datagram Protocol, Src Port: 1900, Dst Port: 1900  
Simple Service Discovery Protocol  
NOTIFY \* HTTP/1.1  
Host:239.255.255.250:1900  
NT:urn:schemas-upnp-org:device

It will show all connections.

Ethernet · 61	IPv4 · 133	IPv6 · 53	TCP · 430	UDP · 635						
Address	packets	bytes	tx packets	rx bytes	rx packets	rx bytes	country	city	AS number	AS organization
4.150.240.254	27	3646	14	1859	13	1787	—	—	—	—
8.8.8.8	40	5928	20	4410	20	1518	—	—	—	—
10.1.6.13	5	330	0	0	5	330	—	—	—	—
10.90.90.90	30	10 k	30	10 k	0	0	—	—	—	—
13.107.3.254	32	10 k	19	8572	13	1674	—	—	—	—
13.107.5.93	88	28 k	51	22 k	37	5790	—	—	—	—
13.107.6.254	35	11 k	21	10 k	14	1740	—	—	—	—
13.107.42.18	1,518	1518 k	1,138	1477 k	380	41 k	—	—	—	—
13.107.136.254	33	10 k	20	8630	13	1678	—	—	—	—
13.107.213.48	7	378	0	0	7	378	—	—	—	—
13.107.246.48	7	378	0	0	7	378	—	—	—	—
13.107.246.68	40	11 k	20	9191	20	2444	—	—	—	—
13.232.28.114	78	15 k	26	8343	52	7056	—	—	—	—
14.142.64.16	10	660	0	0	10	660	—	—	—	—
15.206.237.184	36	7828	16	3212	20	4616	—	—	—	—
20.42.65.90	53	22 k	27	7039	26	15 k	—	—	—	—
20.42.73.27	199	38 k	101	15 k	98	22 k	—	—	—	—
20.50.201.200	28	10 k	14	7594	14	2828	—	—	—	—
20.189.173.7	36	17 k	17	11 k	19	6607	—	—	—	—
20.189.173.11	107	22 k	56	11 k	51	11 k	—	—	—	—
20.189.173.14	1,415	853 k	782	113 k	633	739 k	—	—	—	—
20.197.103.14	186	82 k	96	55 k	90	26 k	—	—	—	—
20.198.118.190	49	12 k	25	8121	24	4405	—	—	—	—

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.



## SHRI G.P.M. DEGREE COLLEGE

Department of Computer

Vision.. Innovation.. Solution.. Presentation

Wireshark · Endpoints · Ethernet

Ethernet · 61	IPv4 · 223	IPv6 · 53	TCP · 763	UDP · 845							
Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	AS Number	AS Organization	
3.34.242.126	28	7978	17	6121	11	1857	—	—	—	—	
4.150.240.254	27	3646	14	1859	13	1787	—	—	—	—	
18.8.8.8	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

NIHIL STANTE KARMA SANGAM



### Result:

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

### Learning Outcomes:

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

### Course Outcomes:

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

### Conclusion:

### Viva Questions:

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



## PRACTICAL NO: 5

### Aim:

Using Sysinternals tools for Network Tracking and Process Monitoring;

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

### Practical:

Lets Check If the Sysinternal Suite is Available on the System

#### Check SysInternals Tools

#### STEPS

Google → sysinternal tools

If Available Then Skip the Installation Part

Let's Install the Sysinternal Suite for Windows We

can download the zip file from the given link

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



# SHRI G.P.M. DEGREE COLLEGE

Department of Computer

Vision.. Innovation.. Solution.. Presentation

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

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

Filter by title

Home

Downloads

Downloads

> File and Disk Utilities

> Networking Utilities

> Process Utilities

> Security Utilities

> System Information

> Miscellaneous

Sysinternals Suite

Microsoft Store

Community

> Resources

Software License Terms

Licensing FAQ

Download PDF

Learn / Sysinternals / Downloads /

## Sysinternals Suite

Article • 06/07/2023 • 8 contributors

By Mark Russinovich

Updated: July 26, 2023

Download Sysinternals Suite (45.2 MB)

Download Sysinternals Suite for Nano Server (9.5 MB)

Download Sysinternals Suite for ARM64 (14.3 MB)

Install Sysinternals Suite from the Microsoft Store

Feedback

Additional resources

Documentation

Sysinternals Utilities - Sysinternals

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

Sysinternals - Sysinternals

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

Sysinternals Process Utilities - Sysinternals

Windows Sysinternals process utilities

Show 5 more

Activate Windows

Then Extract the file to the desired directory

tyc525

bin

New folder (2)

View Volume

css

sycs00Java

UJR Volume 12 Issue 2 2023

Desktop

Extract all

Extract To

This PC > Downloads

Favorites

Homegroup

This PC

admin (d-16)

Desktop

Documents

Downloads

Music

Pictures

Name

lqhlogs.doc

96936\_DEEP\_LEARNING\_Roshan

adnan.jpeg

Image Processing - By Mrs Roshan

Image Processing - By Mrs Roshan

SysinternalsSuite.zip

Select a Destination and Extract Files

Files will be extracted to this folder:

C:\Program Files\SysInternalsSuite

Show extracted files when complete



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

## Monitor Live Processes

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

## STEPS

Sysinternal → procmon

Name	Date modified	Type	Size
procdump64	26-08-2023 12:23	Application	415 KB
procexp	26-08-2023 12:23	Compiled HTML ...	71 KB
procexp	26-08-2023 12:23	Application	4,462 KB
procexp64	26-08-2023 12:23	Application	2,341 KB
<b>Procmon</b>	<b>26-08-2023 12:23</b>	<b>Compiled HTML ...</b>	<b>63 KB</b>
Procmon	26-08-2023 12:23	Application	5,133 KB
Procmon64	26-08-2023 12:23	Application	2,651 KB
PsExec	26-08-2023 12:23	Application	700 KB
PsExec64	26-08-2023 12:23	Application	814 KB
psfile	26-08-2023 12:23	Application	230 KB
psfile64	26-08-2023 12:23	Application	283 KB
PsGetsid	26-08-2023 12:23	Application	404 KB
PsGetsid64	26-08-2023 12:23	Application	495 KB

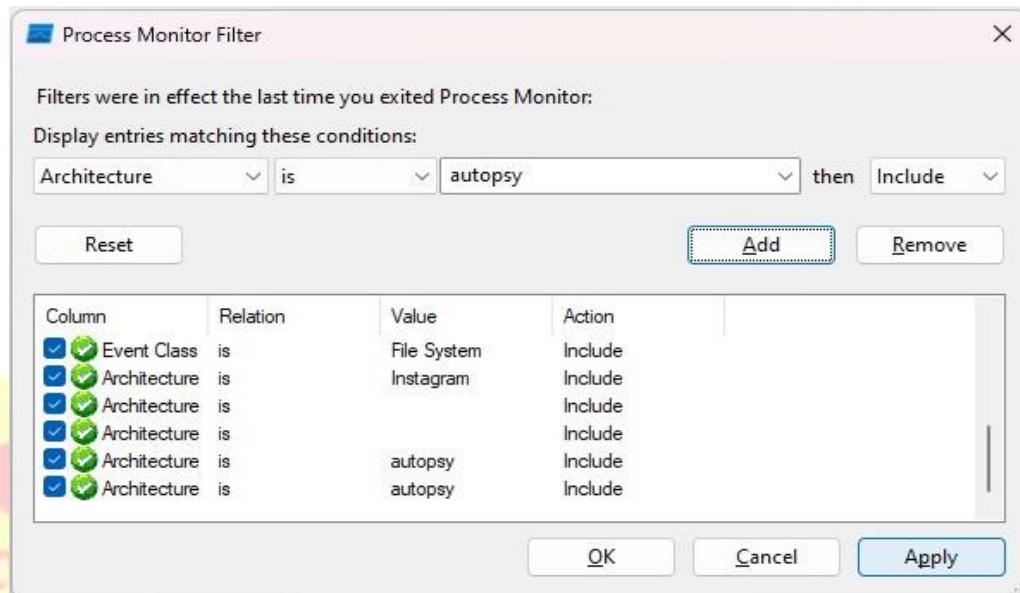


# SHRI G.P.M. DEGREE COLLEGE

Department of Computer

Vision.. Innovation.. Solution.. Presentation

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

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	F02:fb:5353->fe80:2050:4fce:b495:8...	SUCCESS	Length: 30, sequ...
08:27...	chrome.exe	9724	UDP Receive	F02:fb:5353->fe80:2050:4fce:b495:8...	SUCCESS	Length: 30, sequ...
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	Creation Time: 13:0...
08:27...	Explorer.EXE	11808	ReadFile	C:\Windows\System32\Taskbar.dll	SUCCESS	Offset: 2406400, L...
08:27...	svchost.exe	11808	CloseFile	C:\Program Files\Windows Apps\Clipcha...	SUCCESS	
08:27...	svchost.exe	2644	ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset: 638976, Le...
08:27...	Explorer.EXE	11808	RegCloseKey	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...	svchost.exe	2644	ReadFile	C:\Windows\System32\Taskbar.dll	SUCCESS	Offset: 2718208, L...
08:27...	Explorer.EXE	11808	RegQueryValue	HKU\S-1-5-21-3130516669-347735452...	NONE	NAME NOT FOUND Length: 12
08:27...	svchost.exe	11808	RegCloseKey	HKU\S-1-5-21-3130516669-347735452...	SUCCESS	
08:27...	svchost.exe	1020	ReadFile	C:\Windows\System32\Nsasrv.dll	SUCCESS	Offset: 180224, Le...
08:27...	svchost.exe	2644	ReadFile	C:\Windows\System32\Windows.State...	SUCCESS	Offset: 1540096, L...
08:27...	svchost.exe	1020	ReadFile	C:\Windows\System32\Nsasrv.dll	SUCCESS	Offset: 6434816, L...
08:27...	svchost.exe	11808	RegOpenKey	HKU\S-1-5-21-3130516669-347735452...	SUCCESS	Desired Access: R...
08:27...	svchost.exe	11808	RegCloseKey	HKU\S-1-5-21-3130516669-347735452...	SUCCESS	Desired Access: R...
08:27...	svchost.exe	1020	ReadFile	C:\Windows\System32\Taskbar.dll	SUCCESS	Offset: 2529280, L...
08:27...	svchost.exe	11808	ReadFile	C:\Windows\System32\BCP47mm.dll	SUCCESS	Offset: 1523712, L...
08:27...	svchost.exe	11808	ReadFile	C:\Windows\System32\Taskbar.dll	SUCCESS	Offset: 2512896, L...
08:27...	svchost.exe	2644	LockFile	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	Offset: 6414336, L...
08:27...	svchost.exe	11808	RegOpenKey	HKU\S-1-5-21-3130516669-347735452...	SUCCESS	Desired Access: R...
08:27...	svchost.exe	11808	RegCloseKey	HKU\S-1-5-21-3130516669-347735452...	SUCCESS	Desired Access: R...
08:27...	svchost.exe	11808	RegQueryKey	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	Query: HandleTag...
08:27...	svchost.exe	11808	RegOpenKey	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	Desired Access: R...



### Capture RAM

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

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

### STEPS

Sysinternals → RAMMap

This PC > Local Disk (C:) > SysinternalsSuite				
	Name	Date modified	Type	Size
Local Disk (C:)	pssuspend	08-08-2023 08:15	Application	384 KB
	pssuspend64	08-08-2023 08:15	Application	469 KB
> android	Pstools	08-08-2023 08:14	Compiled HTML ...	66 KB
> Borland	ppversion	09-08-2022 08:14	Text Document	1 KB
> CE Image creat	RAMMap	08-08-2023 08:14	Application	662 KB
> flutter	RPCM...	09-08-2022 08:15	Application	1,053 KB
	readme	08-08-2023 08:14	Text Document	8 KB
	RegDelNull	08-08-2023 08:14	Application	343 KB
	RegDelNull64	08-08-2023 08:14	Application	444 KB
> html				
java				
logs				
minaw64				

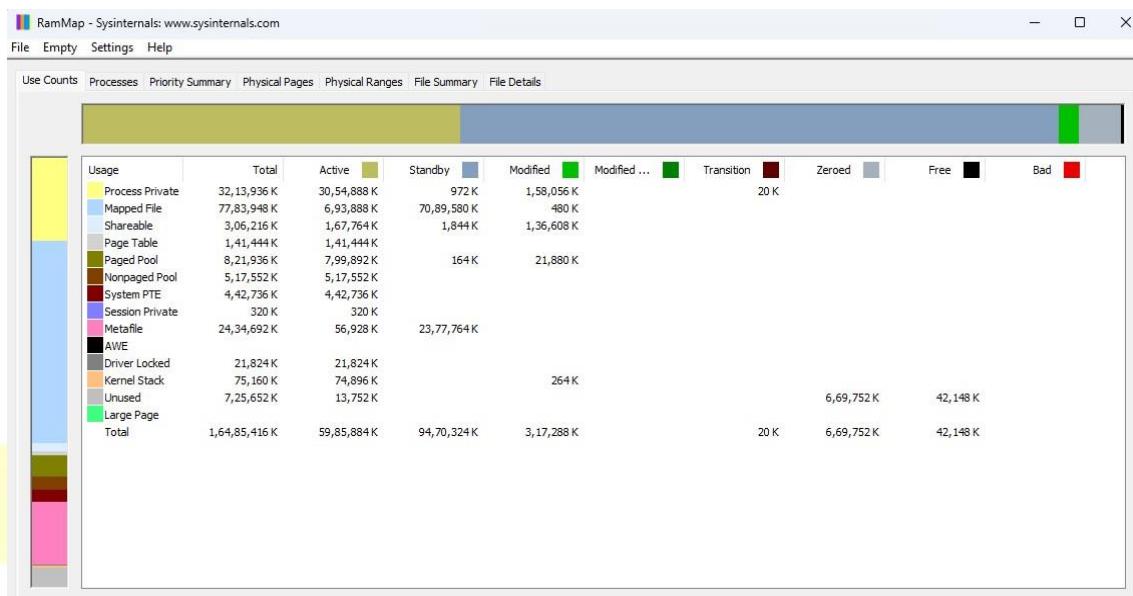
Then allow the permissions and view the mapping



# SHRI G.P.M. DEGREE COLLEGE

Department of Computer

Vision.. Innovation.. Solution.. Presentation



## 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



# SHRI G.P.M. DEGREE COLLEGE

Department of Computer

Vision.. Innovation.. Solution.. Presentation

Screenshot of a Windows File Explorer window showing the contents of the Local Disk (C:) drive. The path is This PC > Local Disk (C:) > SysinternalsSuite. A green arrow points from the 'Borland' folder to the 'tcpview' file, which is highlighted with a green border. The table below lists the files in the directory.

Name	Date modified	Type	Size
tcpcon	08-08-2023 08:15	Application	198 KB
tcpcon64	08-08-2023 08:15	Application	245 KB
tcpview	08-08-2023 08:15	Compiled HTML ...	10 KB
tcpview	08-08-2023 08:15	Application	923 KB
tcpview64	08-08-2023 08:15	Application	1,063 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

Screenshot of a terminal window titled 'C:\SysinternalsSuiteNEW\tcpv'. The window displays the output of the Tcpvcon.exe v4.19 command, showing network connections. The output is as follows:

```
Tcpvcon.exe v4.19 - Sysinternals TcpVcon
Copyright (C) 1996-2023 Mark Russinovich & Bryce Cogswell
Sysinternals - www.sysinternals.com

[TCP] epmd.exe
    PID: 6732
    State: ESTABLISHED
    Local: D-24
    Remote: localhost
[TCP] [System Process]
    PID: 0
    State: TIME_WAIT
    Local: d-24.asccl.com
    Remote: d-23
[TCP] [System Process]
    PID: 0
    State: TIME_WAIT
    Local: d-24.asccl.com
    Remote: d-23
[TCP] [System Process]
    PID: 0
    State: TIME_WAIT
    Local: d-24.asccl.com
    Remote: d-23
[TCP] erl.exe
    PID: 6256
    State: ESTABLISHED
    Local: D-24
    Remote: localhost
```



# SHRI G.P.M. DEGREE COLLEGE

Department of Computer

Vision.. Innovation.. Solution.. Presentation

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 07:05:12	VMAuthdService
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
sqlservr.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	6996	TCP	Established	127.0.0.1	4369	127.0.0.1	49694	29-08-2023 07:05:13	
svchost.exe	10804	TCP	Listen	0.0.0.0	5040	0.0.0.0	0	29-08-2023 08:36:32	CDPSvc
enl.exe	6756	TCP	Listen	127.0.0.1	5984	0.0.0.0	0	29-08-2023 07:05:14	
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	
wininit.exe	936	TCP	Listen	0.0.0.0	49665	0.0.0.0	0	29-08-2023 07:05:11	
svchost.exe	1944	TCP	Listen	0.0.0.0	49666	0.0.0.0	0	29-08-2023 07:05:11	Schedule
svchost.exe	2980	TCP	Listen	0.0.0.0	49667	0.0.0.0	0	29-08-2023 07:05:11	EventLog
snnolov.exe	4164	TCP	Listen	0.0.0.0	49668	0.0.0.0	0	29-08-2023 07:05:11	Snnolov

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	SSDPSPRV
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	
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	SSDPSPRV
svchost.exe	6108	UDPV6	fe80::3b4f:9f72:34ab:146	1900	*			29-08-2023 08:36:35	SSDPSPRV
svchost.exe	6108	UDPV6	fe80::3b4f:9f72:34ab:146	1900	*			29-08-2023 08:36:35	SSDPSPRV
svchost.exe	6108	UDPV6	fe80::3b4f:9f72:34ab:146	1900	*			29-08-2023 08:36:35	SSDPSPRV
dashHost.exe	3764	UDPV6	::	3702	*			29-08-2023 08:36:46	
dashHost.exe	3764	UDPV6	::	3702	*			29-08-2023 08:36:46	
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	::	5283	*			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



## SHRI G.P.M. DEGREE COLLEGE

Department of Computer

Vision.. Innovation.. Solution.. Presentation

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

### Monitor Virtual Memory

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

### STEPS

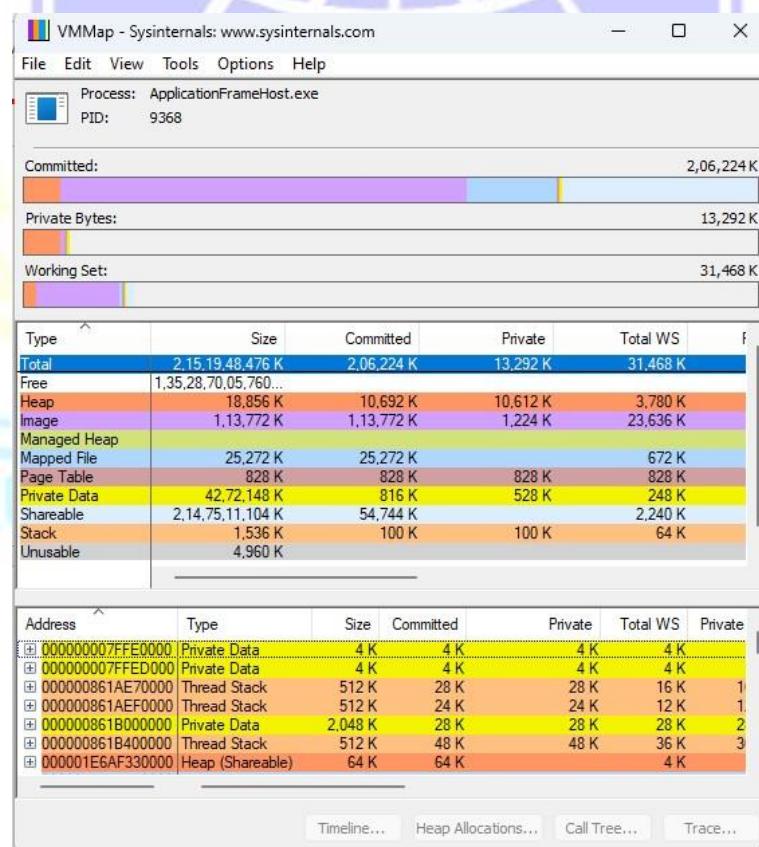
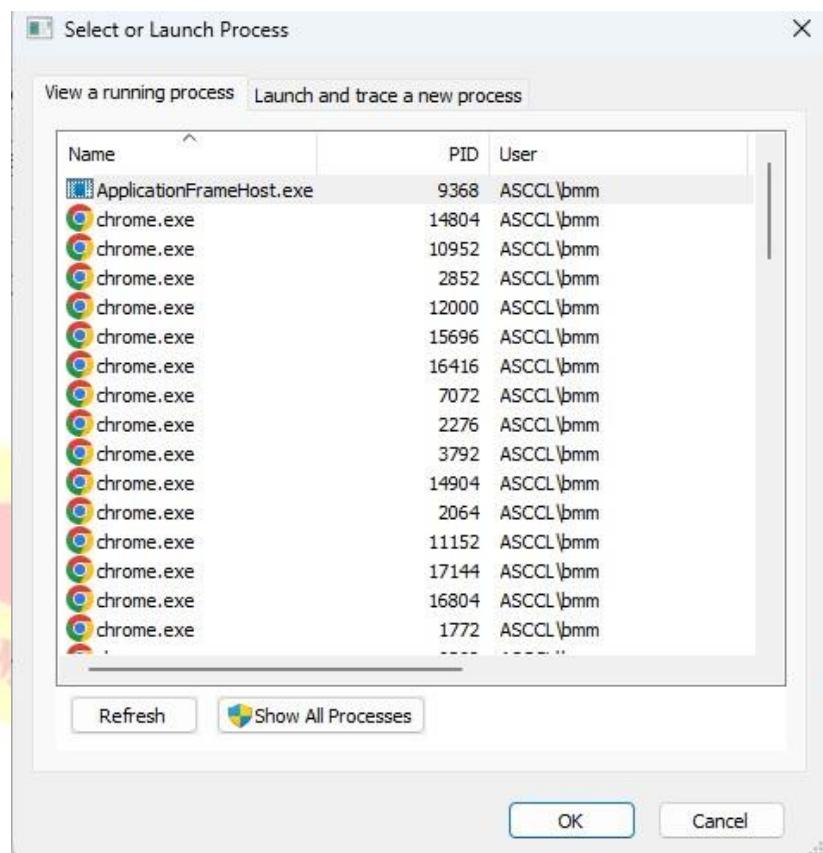
Sysinternal → VMMAP



# SHRI G.P.M. DEGREE COLLEGE

Department of Computer

Vision.. Innovation.. Solution.. Presentation

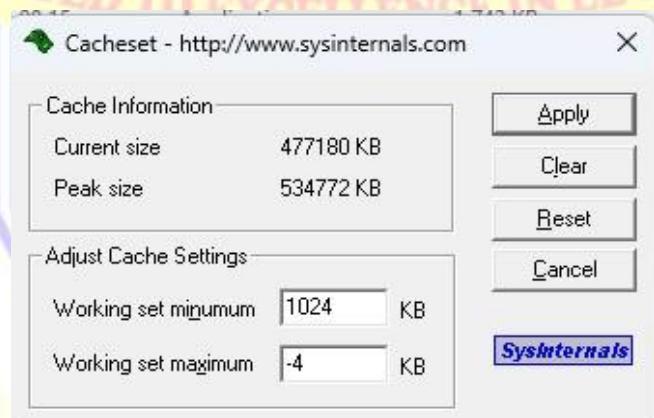
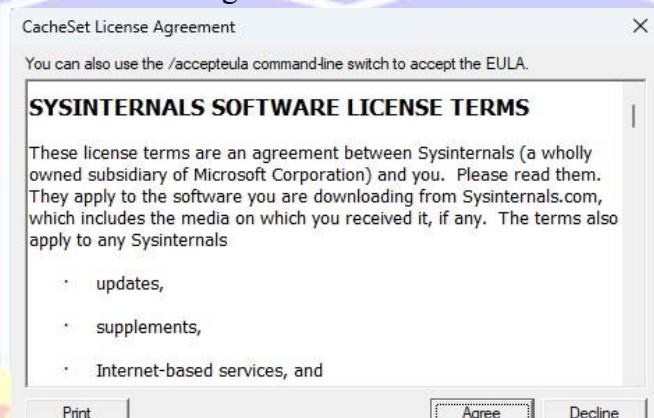




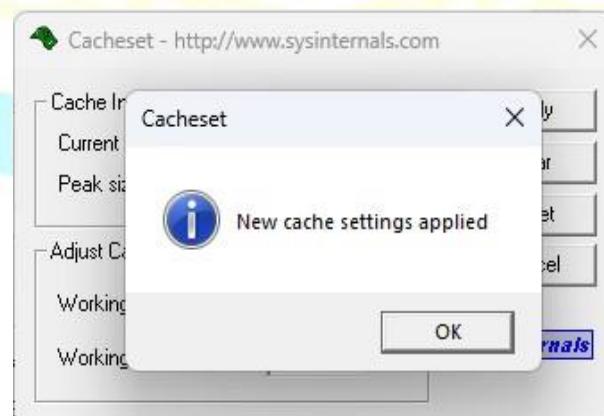
## Monitor Cache Memory

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



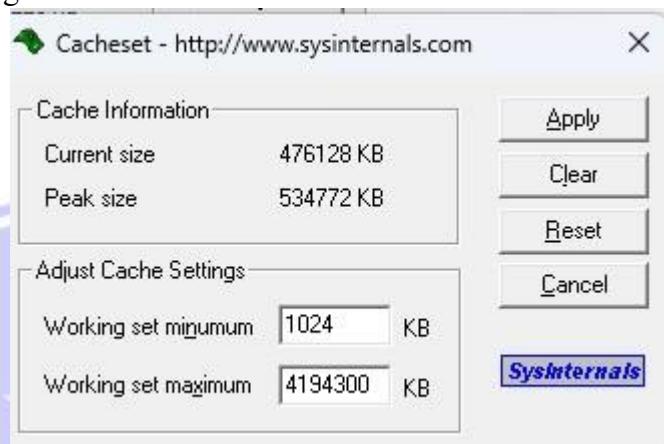


## SHRI G.P.M. DEGREE COLLEGE

Department of Computer

Vision.. Innovation.. Solution.. Presentation

After applying the changes



**Result:**

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

**Learning Outcomes:**

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

**Course Outcomes:**

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

**Conclusion:****Viva Questions:**

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



## PRACTICAL NO: 6

### Aim:

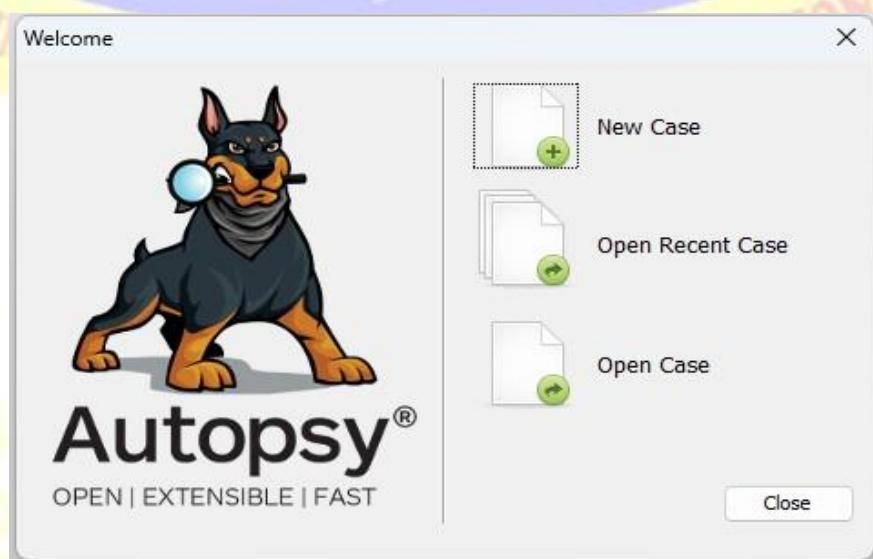
Recovering and Inspecting deleted files

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

### Practical:

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

Open Autopsy and Click on New Case



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



# SHRI G.P.M. DEGREE COLLEGE

## Department of Computer

Vision.. Innovation.. Solution.. Presentation

New Case Information

**Steps**

1. Case Information  
2. Optional Information

**Case Information**

Case Name: 290723

Base Directory: D:\SCYT\CF\AUTOPSY\

Case Type:  Single-user  Multi-user

Case data will be stored in the following directory:  
D:\SCYT\CF\AUTOPSY\290723

< Back    Help

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: 290723

Examiner

Name: Maddy

Phone: 8983238836

Email: themaddy@gmail.com

Notes: Sandisk pendrive red and black new condition empty

Organization

Organization analysis is being done for:

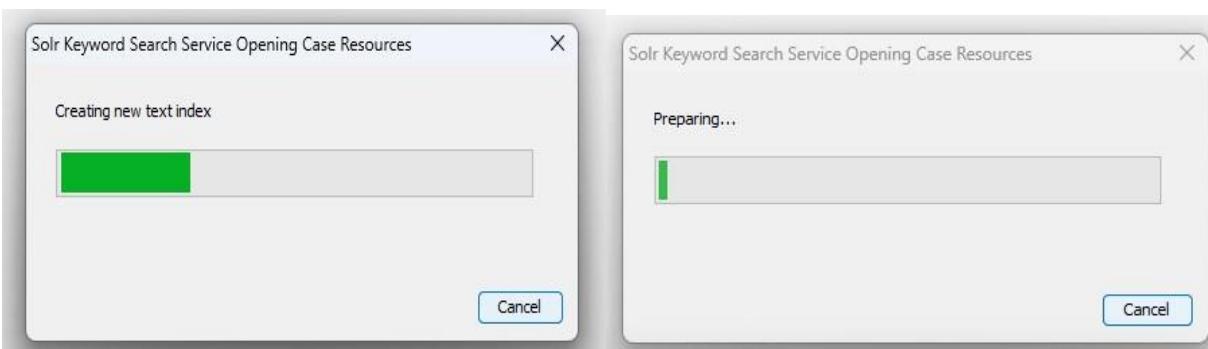
< Back    Help



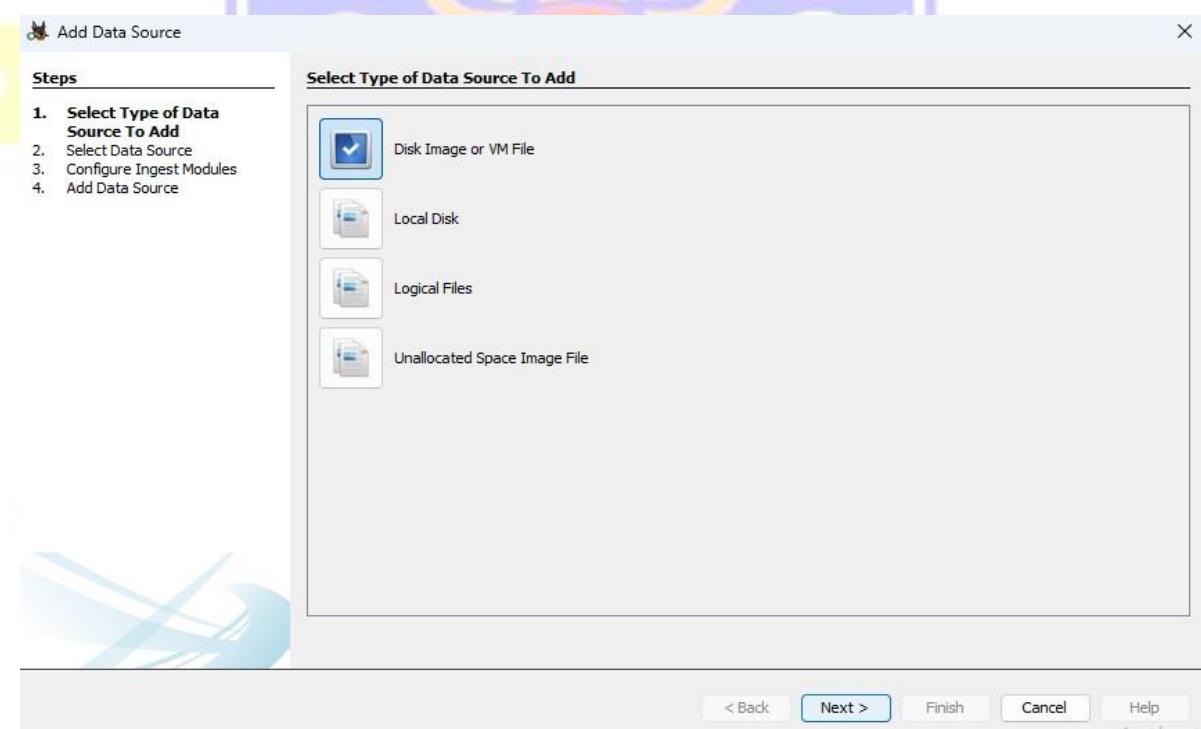
## SHRI G.P.M. DEGREE COLLEGE

Department of Computer

Vision.. Innovation.. Solution.. Presentation



Select on Disk Image or VM File and Click Next



निर्मलासनेह उत्तम सेवाधर्म



# SHRI G.P.M. DEGREE COLLEGE

Department of Computer

Vision.. Innovation.. Solution.. Presentation

Give the destination of the image and click next

Add Data Source

**Steps**

- Select Type of Data Source To Add
- Select Data Source**
- Configure Ingest Modules
- Add Data Source

**Select Data Source**

Browse for an image file:  
D:\SCYT\CF\FTKIMAG\290723.001

Please select the input timezone: (GMT+5:30) Asia/Calcutta

Ignore orphan files in FAT file systems  
(faster results, although some data will not be searched)

Sector size: Auto Detect

< Back Next > Finish Cancel Help

Select the ingest module and click next

Add Data Source

**Steps**

- Select Type of Data Source To Add
- Select Data Source
- Configure Ingest Modules**
- Add Data Source

**Configure Ingest Modules**

Run ingest modules on:

All Files, Directories, and Unallocated Space

The selected module has no per-run settings.

Recent Activity

Hash Lookup  
File Type Identification  
Embedded File Extractor  
Exif Parser  
Keyword Search  
Email Parser  
Extension Mismatch Detector  
E01 Verifier  
Encryption Detection  
Interesting Files Identifier  
PhotoRec Carver  
Correlation Engine  
Virtual Machine Extractor

Select All Deselect All History Global Settings

< Back Next > Finish Cancel Help

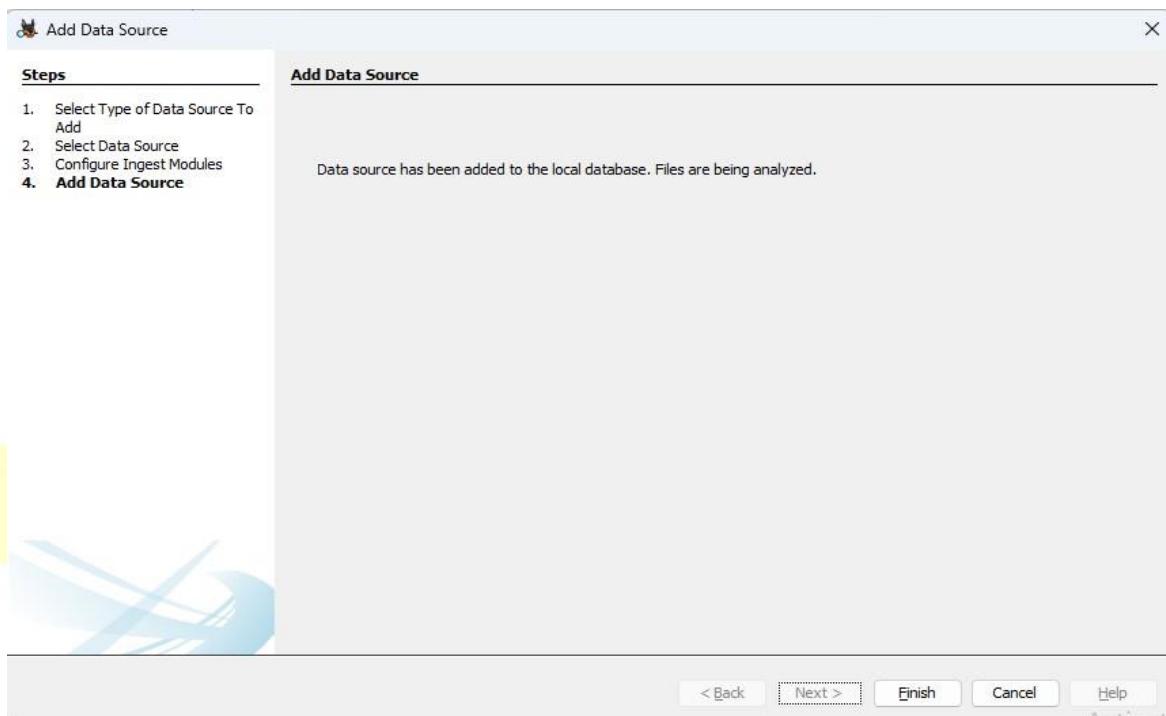
See the acknowledgement and click finish



# SHRI G.P.M. DEGREE COLLEGE

Department of Computer

Vision.. Innovation.. Solution.. Presentation



Now we check the files recovered

The screenshot shows the Autopsy 4.9.1 interface with the case number 290723. The left sidebar includes sections like Data Sources, Views, File Types, Deleted Files (highlighted), MB File Size, Results, Extracted Content, Keyword Hits, Hashset Hits, E-Mail Messages, Interesting Items, Accounts, Tags, and Reports. The main pane displays a table titled 'File System' with 21 results. The columns are Name, S, C, Location, Modified Time, Change Time, Access Time, and C. The table lists various recovered files and folders, many of which are marked with a red X icon. A status bar at the bottom indicates 'Analyzing files from 290723.001' and '24%'.

Name	S	C	Location	Modified Time	Change Time	Access Time	C
EFISECTOR			/img_290723.001/vol_v02/\$OrphanFiles/EFISECTOR	2019-12-06 17:05:28 IST	0000-00-00 00:00:00	0000-00-00 00:00:00	0
EFI			/img_290723.001/vol_v02/\$OrphanFiles/EFI	2019-12-06 09:05:28 IST	0000-00-00 00:00:00	2019-12-06 00:00:00 IST	2
BOOT			/img_290723.001/vol_v02/\$OrphanFiles/BOOT	2019-12-06 09:05:28 IST	0000-00-00 00:00:00	2019-12-06 00:00:00 IST	2
BOOTX64.EFI			/img_290723.001/vol_v02/\$OrphanFiles/BOOTX64.EFI	2019-12-06 17:05:16 IST	0000-00-00 00:00:00	2019-12-06 00:00:00 IST	2
EFISECTOR			/img_290723.001/vol_v02/\$OrphanFiles/EFISECTOR	2019-12-06 17:05:30 IST	0000-00-00 00:00:00	0000-00-00 00:00:00	0
EFI			/img_290723.001/vol_v02/\$OrphanFiles/EFI	2019-12-06 09:05:30 IST	0000-00-00 00:00:00	2019-12-06 00:00:00 IST	2
BOOT			/img_290723.001/vol_v02/\$OrphanFiles/BOOT	2019-12-06 09:05:30 IST	0000-00-00 00:00:00	2019-12-06 00:00:00 IST	2
BOOTX64.EFI			/img_290723.001/vol_v02/\$OrphanFiles/BOOTX64.EFI	2019-12-06 17:05:18 IST	0000-00-00 00:00:00	2019-12-06 00:00:00 IST	2
build.xml			/img_290723.001/vol_v02/\$OrphanFiles/build.xml	2022-09-26 14:06:42 IST	0000-00-00 00:00:00	2023-01-07 00:00:00 IST	2
build			/img_290723.001/vol_v02/\$OrphanFiles/build	2022-09-26 14:22:28 IST	0000-00-00 00:00:00	2023-01-07 00:00:00 IST	2
lib			/img_290723.001/vol_v02/\$OrphanFiles/lib	2022-09-26 14:06:44 IST	0000-00-00 00:00:00	2023-01-07 00:00:00 IST	2
NBPROJ~1			/img_290723.001/vol_v02/\$OrphanFiles/NBPROJ~1	2022-09-26 14:06:42 IST	0000-00-00 00:00:00	2023-01-07 00:00:00 IST	2
src			/img_290723.001/vol_v02/\$OrphanFiles/src	2022-09-26 14:06:42 IST	0000-00-00 00:00:00	2023-01-07 00:00:00 IST	2
web			/img_290723.001/vol_v02/\$OrphanFiles/web	2022-09-26 14:19:02 IST	0000-00-00 00:00:00	2023-01-07 00:00:00 IST	2
H^~L^~H~,^\$^			/img_290723.001/vol_v02/\$OrphanFiles/H^~L^~H~,^\$^	1998-04-04 17:26:16 IST	0000-00-00 00:00:00	1980-07-16 00:00:00 IST	1
H^~L^~H~,^\$^			/img_290723.001/vol_v02/\$OrphanFiles/H^~L^~H~,^\$^	1998-04-04 17:26:16 IST	0000-00-00 00:00:00	1980-07-16 00:00:00 IST	1
~~~~~@@@			/img_290723.001/vol_v02/\$OrphanFiles/~~~~~@@@	2004-01-16 06:00:00 IST	0000-00-00 00:00:00	0000-00-00 00:00:00	0
t^D\$pH~,^\$^			/img_290723.001/vol_v02/\$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_v02/\$OrphanFiles/~~~~~ ,~~~	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0
~~^m\~~^,~~~			/img_290723.001/vol_v02/\$OrphanFiles/~~^m\~~^,~~~	1981-09-30 16:26:02 IST	0000-00-00 00:00:00	1980-04-08 00:00:00 IST	1
f693ba26.83a			/img_290723.001/vol_v02/\$OrphanFiles/f693ba26.83a	1992-08-10 03:56:04 IST	0000-00-00 00:00:00	2007-01-17 00:00:00 IST	2

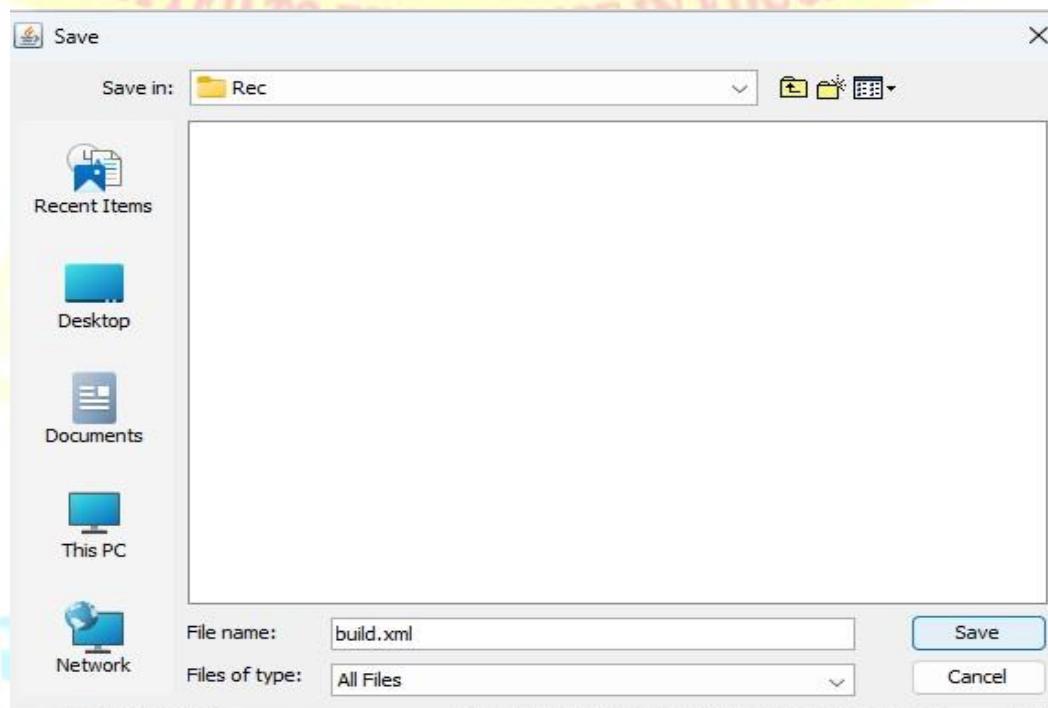
We see the Deleted Files

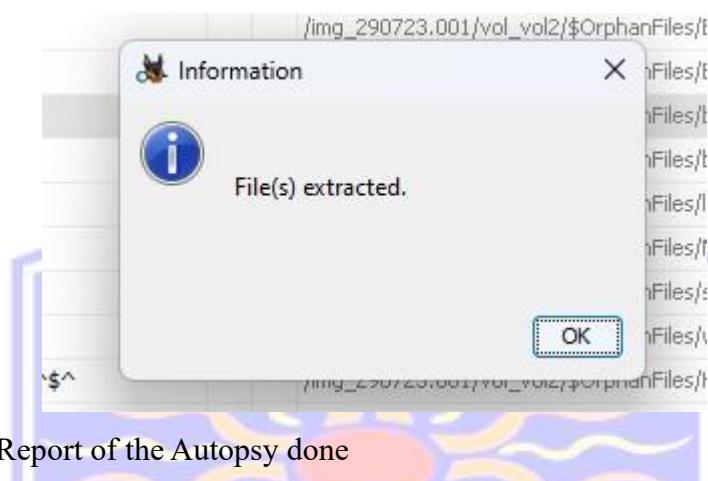


Now We Extract/Recover some deleted files

X BOOT1	jImg_290723.001/vol_vo1/\$OrphanFiles/BOOT1	2019-1
X BOOTX64.EFI	/img_290723.001/vol_vo1/\$OrphanFiles/BOOTX64.EFI	2019-1
X build.xml		2022-C
X build		2022-C
X lib		2022-C
X NBPROJ~1		
X src		2022-C
X web		2022-C
X H^~L^~H^.~\$^		1998-C
X H^~L^~H^.~\$^		1998-C
X ~~~~~~.@@@		
X tf^D\$pH^.~\$^		2004-C
X ~~~~~~.~~~		
X ~~~mV~~~,~~~		
X f693ba26.83a		1992-C
f0048429.txt	/img_290723.001/vol_vo1/\$CarvedFiles/f0048429.txt	0000-C
...		

Set a directory for the recovered files





Now we Generate a Report of the Autopsy done

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



# SHRI G.P.M. DEGREE COLLEGE

Department of Computer

Vision.. Innovation.. Solution.. Presentation

Generate Report

### Select and Configure Report Modules

Report Modules:

<input type="radio"/> HTML Report	A report about results and tagged items in Excel (XLS) format.
<input checked="" type="radio"/> Excel Report	<i>This report will be configured on the next screen.</i>
<input type="radio"/> Add Tagged Hashes	
<input type="radio"/> Files - Text	
<input type="radio"/> Google Earth KML	
<input type="radio"/> STIX	
<input type="radio"/> TSK Body File	

< Back    Next >    Finish    Cancel    Help

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

Generate Report

### Configure Artifact Reports

Select which data to report on:

All Results

Tagged Results

Select All    Deselect All

Data Types

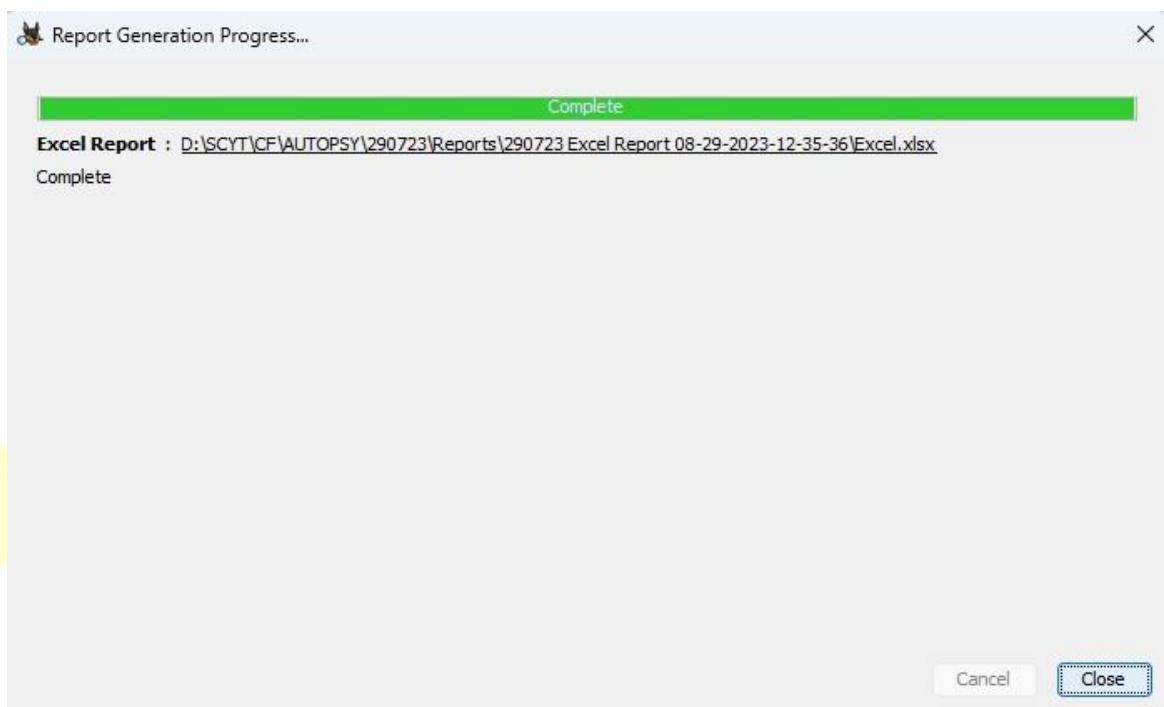
< Back    Next >    Finish    Cancel    Help



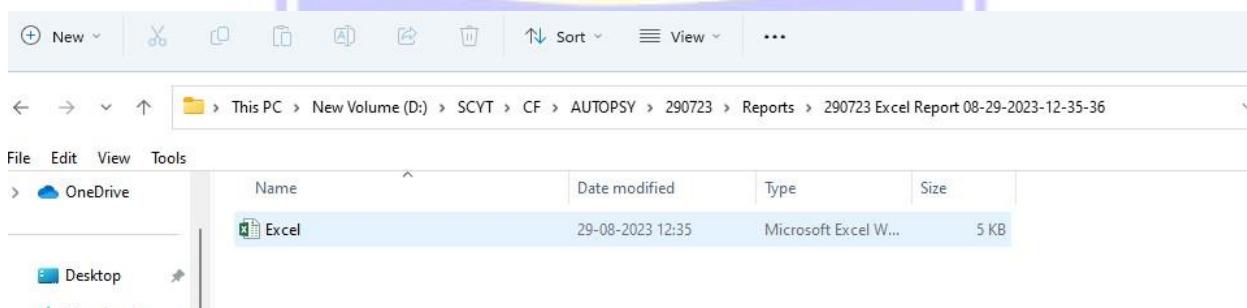
## SHRI G.P.M. DEGREE COLLEGE

Department of Computer

Vision.. Innovation.. Solution.. Presentation



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





# SHRI G.P.M. DEGREE COLLEGE

Department of Computer

Vision.. Innovation.. Solution.. Presentation

The screenshot shows a Microsoft Excel spreadsheet. The top ribbon menu includes FILE, HOME, INSERT, PAGE LAYOUT, FORMULAS, DATA, and REV. The HOME tab is selected, showing font options like Calibri (size 11), bold, italic, underline, and alignment tools. The A1 cell is selected, and the formula bar shows "Summary". The main table has rows 1 through 22. Row 1 contains "Summary". Rows 3 through 6 contain data: "Case Name: 290723", "Case Number: 290723", "Examiner: Maddy", and "Number of Images: 1". Rows 7 through 22 are empty. Below the table, tabs for "Summary", "Tagged Files", and "Tagged Results" are visible, along with a plus sign icon.

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					

The screenshot shows a Microsoft Excel spreadsheet with a table containing 14 rows of data. The columns are labeled A through I. Column A is "Date Taken", column B is "Device Manufacturer", column C is "Device Model", column D is "Latitude", column E is "Longitude", column F is "Altitude", column G is "Source File", and column H is "Tags". The data consists of 14 entries, all from June 10, 2022, at 18:10 IST, taken with a realme 6 device. The source files listed are various image files with unique names.

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_vo2/IMG20220610181021.jpg	
3	2022-06-10 18:10:27 IST	realme	realme 6				/img_04092023_masood.001/vol_vo2/IMG20220610181027.jpg	
4	2022-06-10 18:10:30 IST	realme	realme 6				/img_04092023_masood.001/vol_vo2/IMG20220610181030.jpg	
5	2022-06-10 18:10:34 IST	realme	realme 6				/img_04092023_masood.001/vol_vo2/IMG20220610181034.jpg	
6	2022-06-10 18:23:26 IST	realme	realme 6				/img_04092023_masood.001/vol_vo2/\$CarvedFiles/f0000000.jpg	
7	2022-06-10 18:24:07 IST	realme	realme 6				/img_04092023_masood.001/vol_vo2/\$CarvedFiles/f0005120.jpg	
8	2022-06-10 18:24:13 IST	realme	realme 6				/img_04092023_masood.001/vol_vo2/\$CarvedFiles/f0012256.jpg	
9	2022-06-10 18:24:17 IST	realme	realme 6				/img_04092023_masood.001/vol_vo2/\$CarvedFiles/f0016320.jpg	
10	2022-06-10 18:24:37 IST	realme	realme 6				/img_04092023_masood.001/vol_vo2/\$CarvedFiles/f0020864.jpg	
11	2022-06-10 18:34:20 IST	realme	realme 6				/img_04092023_masood.001/vol_vo2/IMG20220610183420.jpg	
12	2022-06-10 18:34:25 IST	realme	realme 6				/img_04092023_masood.001/vol_vo2/IMG20220610183425.jpg	
13	2022-06-10 18:34:37 IST	realme	realme 6				/img_04092023_masood.001/vol_vo2/IMG20220610183437.jpg	
14	2022-06-10 18:34:53 IST	realme	realme 6				/img_04092023_masood.001/vol_vo2/IMG20220610183453.jpg	
15								
16								
17								



# SHRI G.P.M. DEGREE COLLEGE

## Department of Computer

Vision.. Innovation.. Solution.. Presentation

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	Source File		Tags
4 clients.l.google.com%@clients.l.google.com%&%clients.l.google.	/img_04092023_masood.001/vol_vol2/\$Unalloc/Unalloc_1878_3915776_1077723136		
5 clients.l.google.com%@clients.l.google.com%&%clients.l.google.	/img_04092023_masood.001/vol_vol2/\$OrphanFiles/_LLPLA~1.PCA		
6 clients.l.google.com%@clients.l.google.com%&%clients.l.google.	/img_04092023_masood.001/vol_vol2/\$OrphanFiles/_ROTEU~1.LEXE		
7 clients.l.google.com%@clients.l.google.com%&%clients.l.google.	/img_04092023_masood.001/vol_vol2/\$OrphanFiles/aftnnndbn.udmd		
8			
-239034676-0-1001@flonetnetwork.com			
10 Preview	Source File		Tags
11 jjj24zntx~239034676-0-1001@flonetnetwork.com>[work.com]>[4676-0	/img_04092023_masood.001/vol_vol2/\$Unalloc/Unalloc_1878_3915776_1077723136		
12 jjj24zntx~239034676-0-1001@flonetnetwork.com>[work.com]>[4676-0	/img_04092023_masood.001/vol_vol2/_S_Proteus 8.11 SP0 Pro HomeMade Electronics.exe		
13			
14 200612032123.609457386a225c@rly-xm04.mx.aol.com			
15 Preview	Source File		Tags
16 -0500in-reply-to:<<200612032123.609457386a225c@rly-xm04.mx.aol.com>>x-mb-message-sourc	/img_04092023_masood.001/vol_vol2/\$Unalloc/Unalloc_1878_3915776_1077723136		
17 -0500in-reply-to:<<200612032123.609457386a225c@rly-xm04.mx.aol.com>>x-mb-message-sourc	/img_04092023_masood.001/vol_vol2/_S_Proteus 8.11 SP0 Pro HomeMade Electronics.exe		
18			
19 20061204013940.a88906765f@mprdmixin.myway.com			
20 Preview	Source File		Tags
21 email.comcast.net<<20061204013940.a88906765f@mprdmixin.myway.com>>mail.comcast.net000	/img_04092023_masood.001/vol_vol2/\$Unalloc/Unalloc_1878_3915776_1077723136		
22 7h1tmccan0.idc<<20061204013940.a88906765f@mprdmixin.myway.com>>date_sun_3.doc	/img_04092023_masood.001/vol_vol2/\$CarvedFiles/f0333408.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@goowy.com		
13 Undecided	terrysadler@goowy.com		
14			

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

**Result:**

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

**Learning Outcomes:**

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

**Course Outcomes:**

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

**Conclusion:****Viva Questions:**

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



## PRACTICAL NO: 7

### Aim:

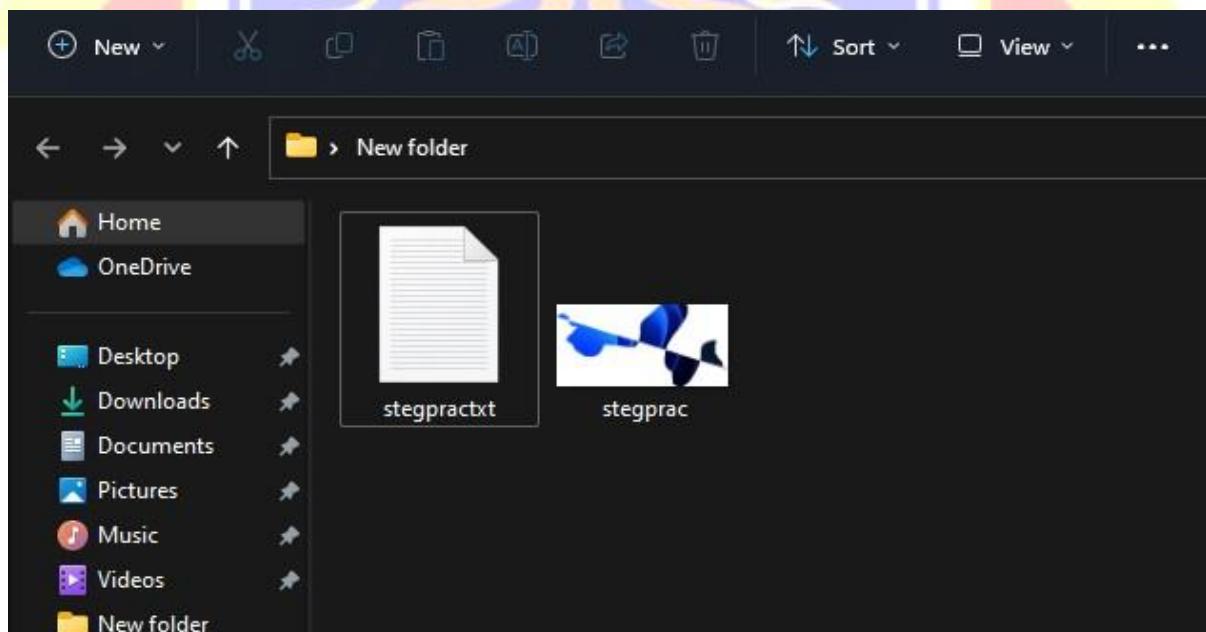
Steganography Detection

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

### Practical:

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

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



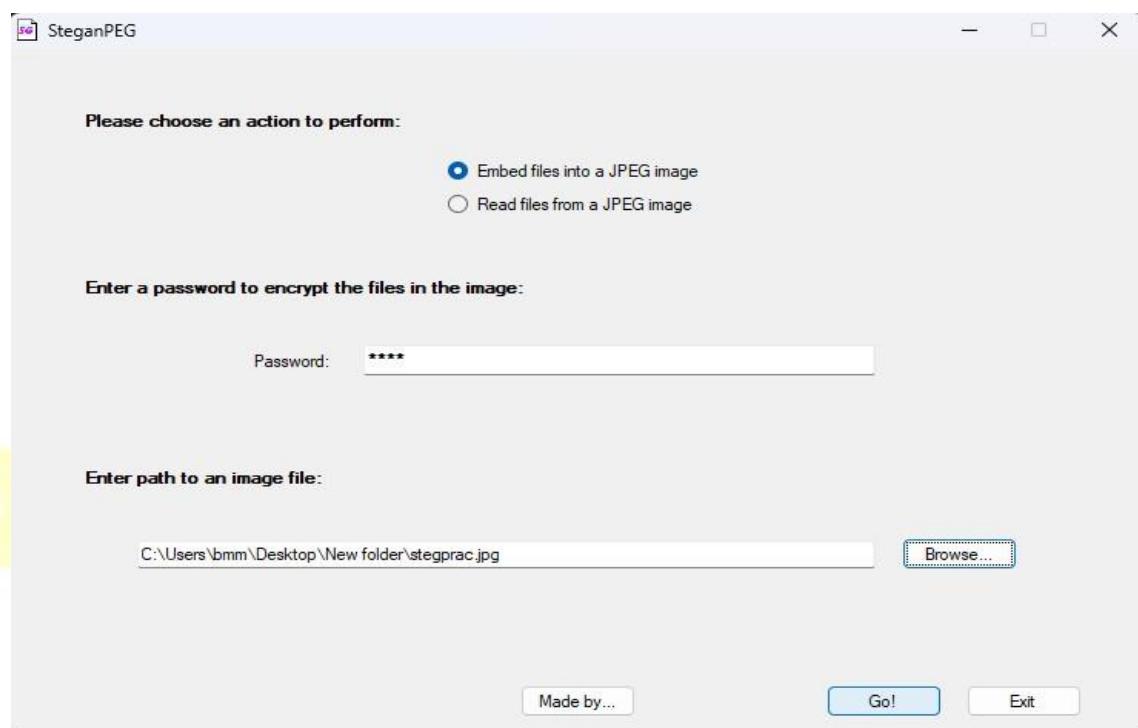
Open the SteganPEG and give a password and browse the path of the image



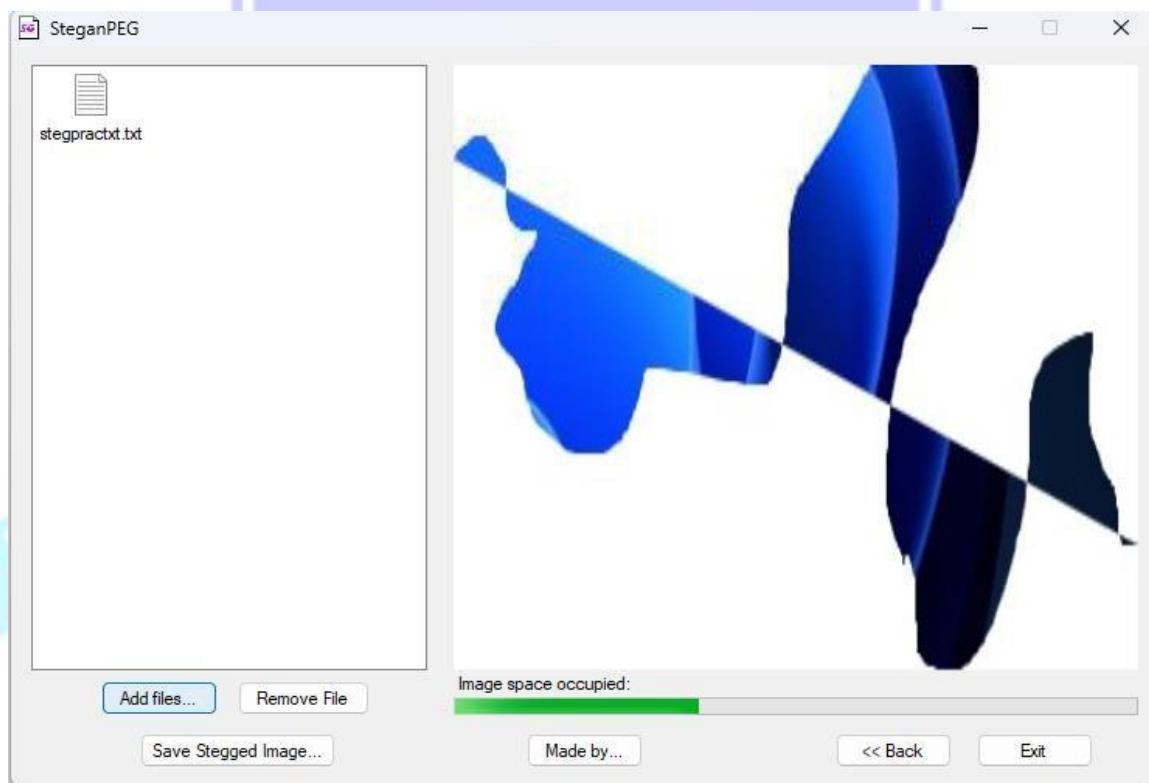
# SHRI G.P.M. DEGREE COLLEGE

Department of Computer

Vision.. Innovation.. Solution.. Presentation



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



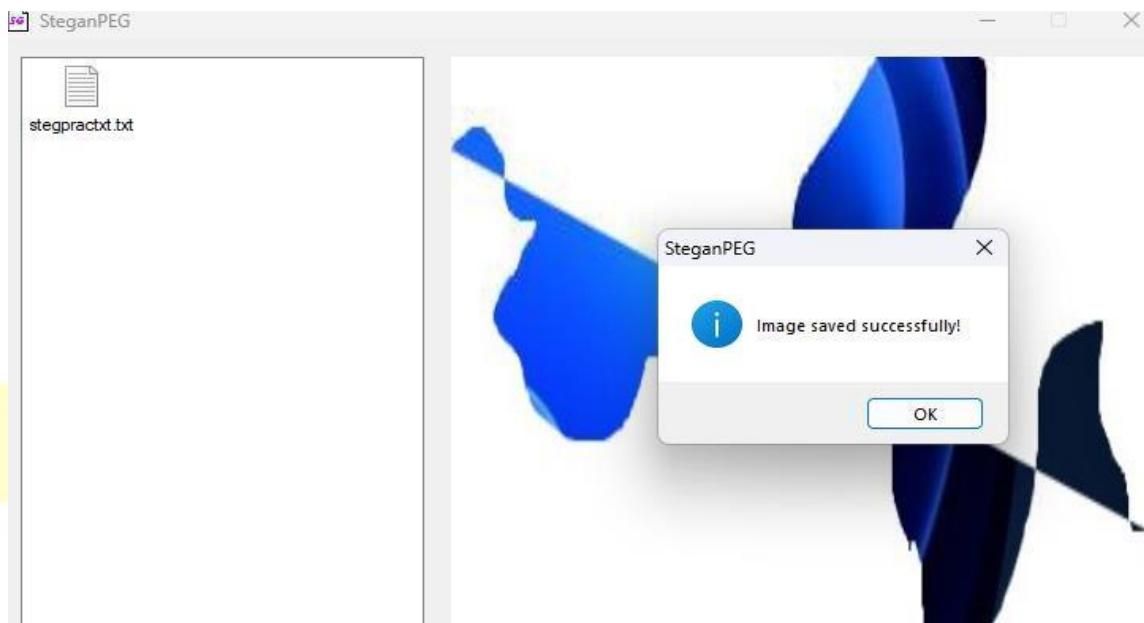


## SHRI G.P.M. DEGREE COLLEGE

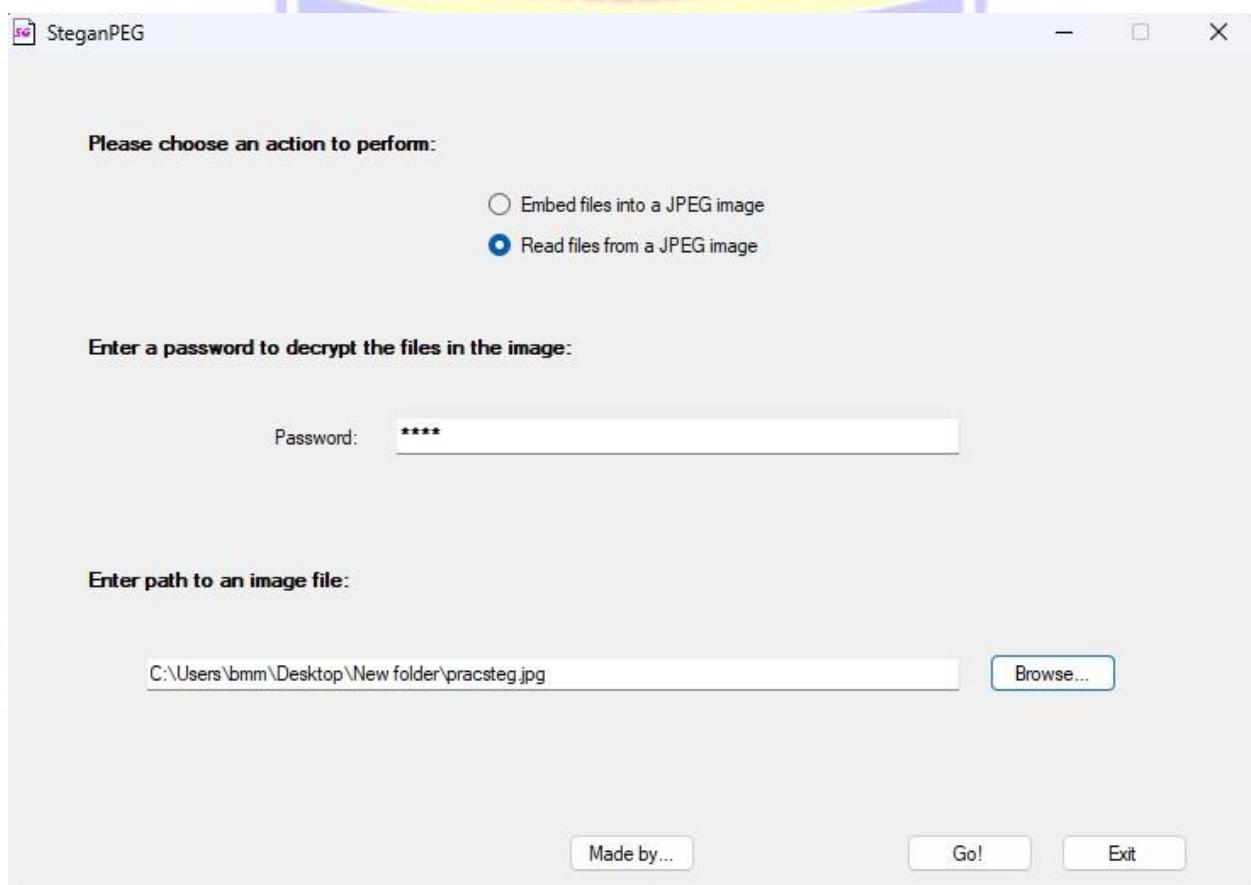
Department of Computer

Vision.. Innovation.. Solution.. Presentation

Save the stegged image



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

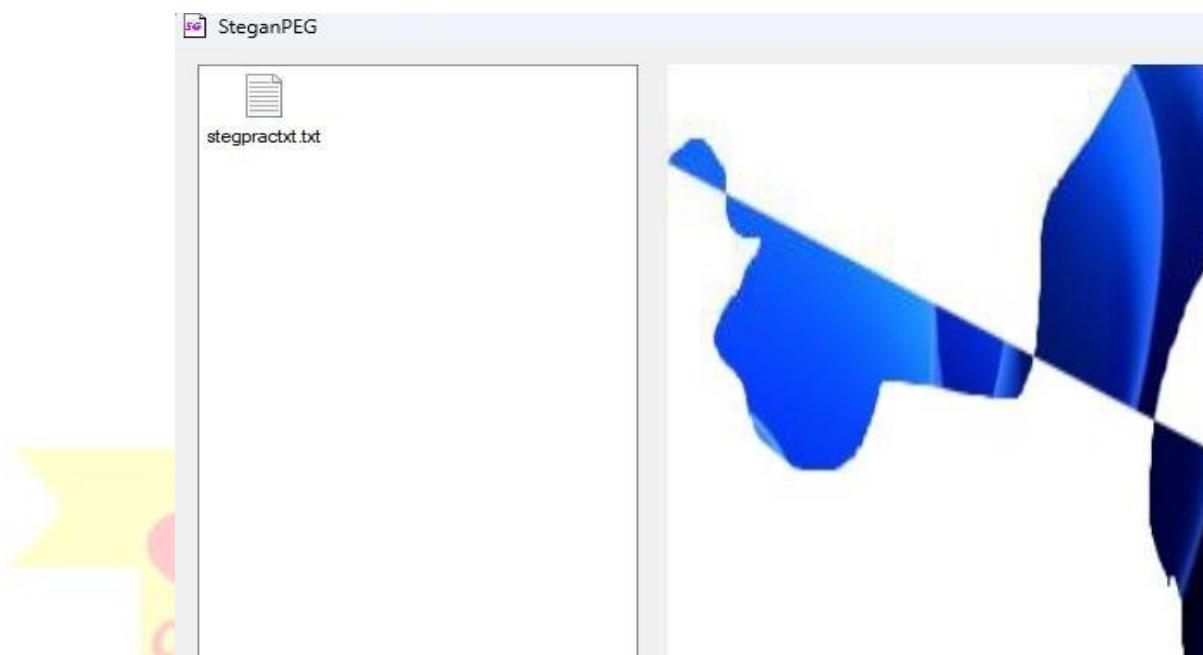




# SHRI G.P.M. DEGREE COLLEGE

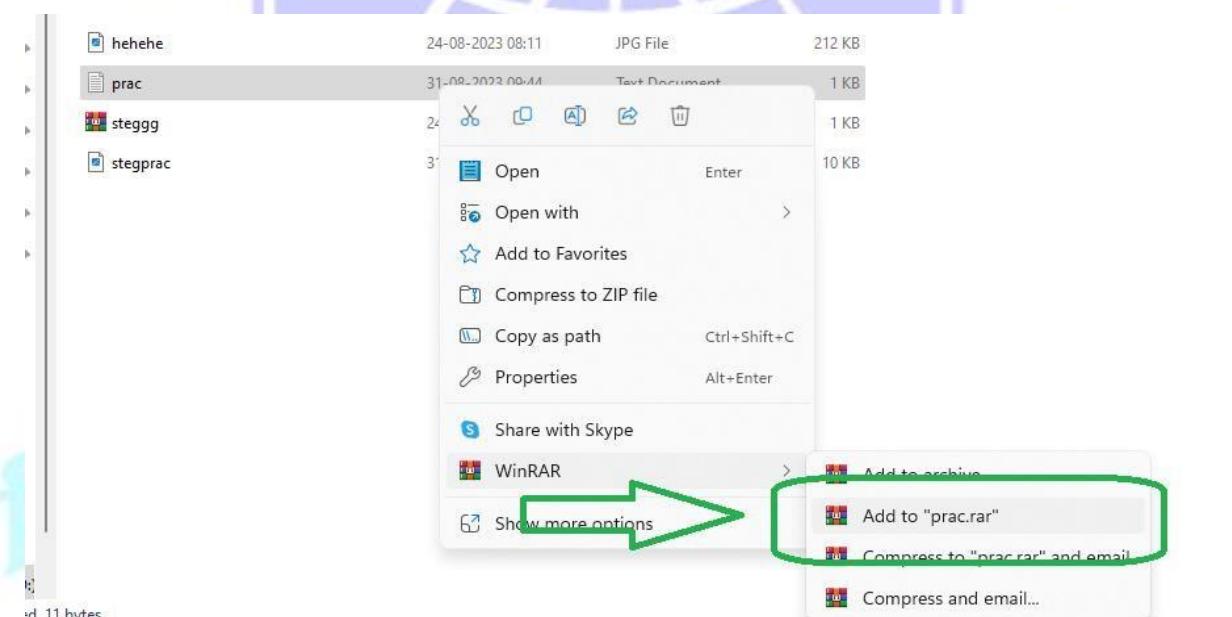
Department of Computer

Vision.. Innovation.. Solution.. Presentation



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
```



## SHRI G.P.M. DEGREE COLLEGE

Department of Computer

Vision.. Innovation.. Solution.. Presentation

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

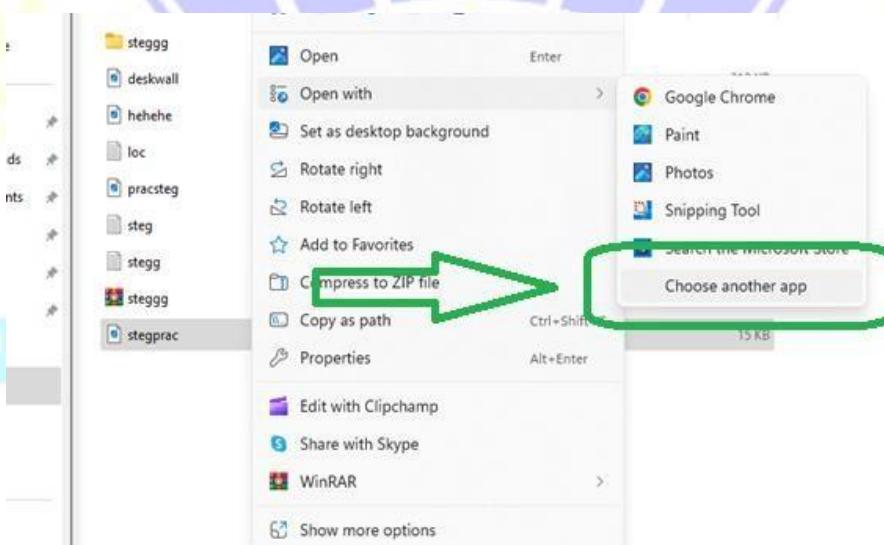
D:\SCYT\CF\STEG>
```

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





## SHRI G.P.M. DEGREE COLLEGE

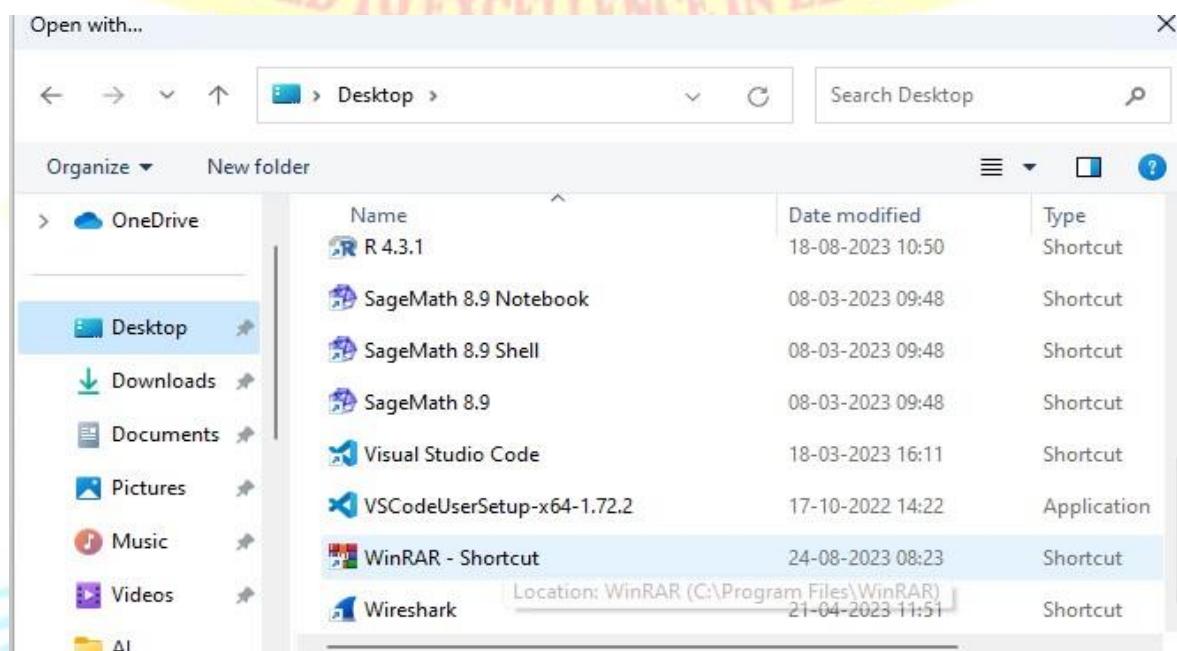
Department of Computer

Vision.. Innovation.. Solution.. Presentation

Select Choose another app → choose an app on your pc



Then Desktop → Shortcut created of WinRAR and Select Just Once

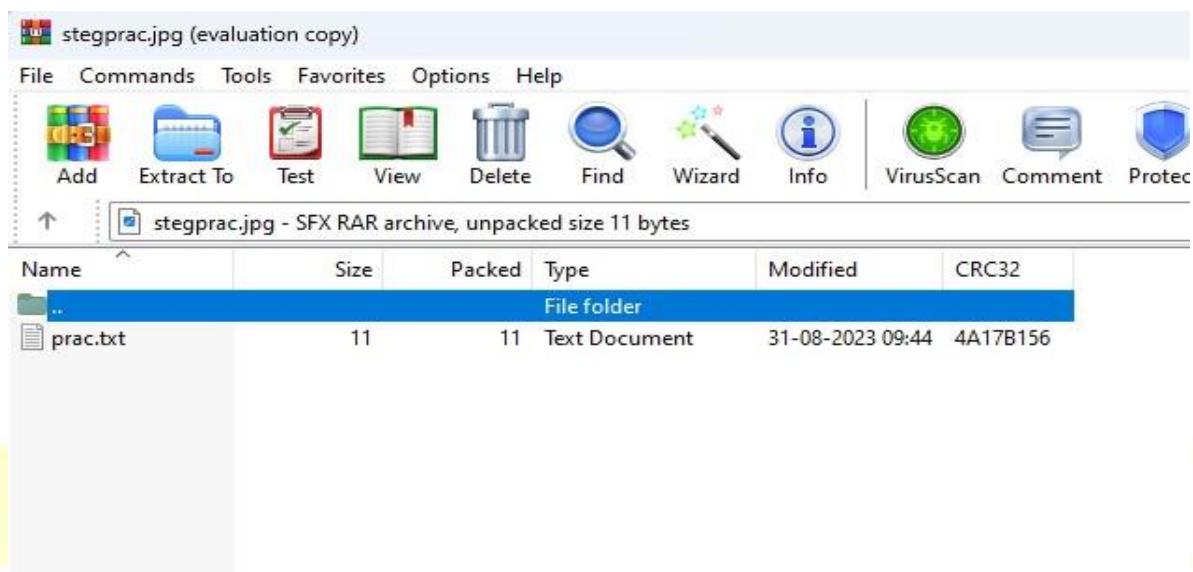




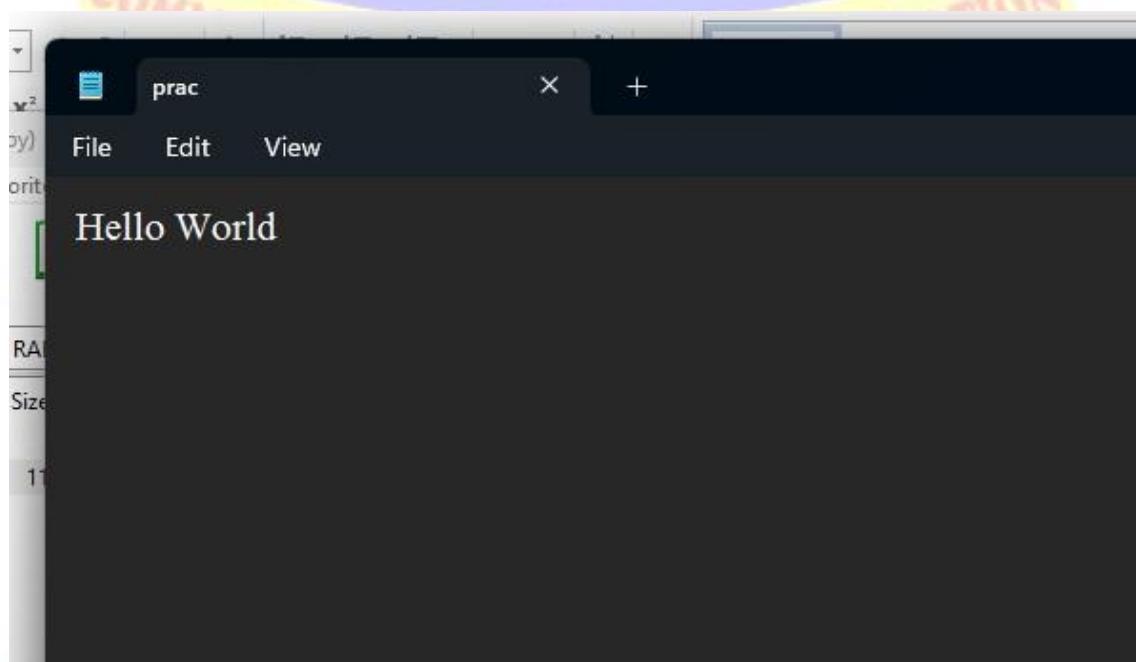
## SHRI G.P.M. DEGREE COLLEGE

Department of Computer

Vision.. Innovation.. Solution.. Presentation



View the Extracted File



**Result:**

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

**Learning Outcomes:**

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

**Course Outcomes:**

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

**Conclusion:****Viva Questions:**

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



## PRACTICAL NO: 8

### Aim:

Mobile Device Forensics

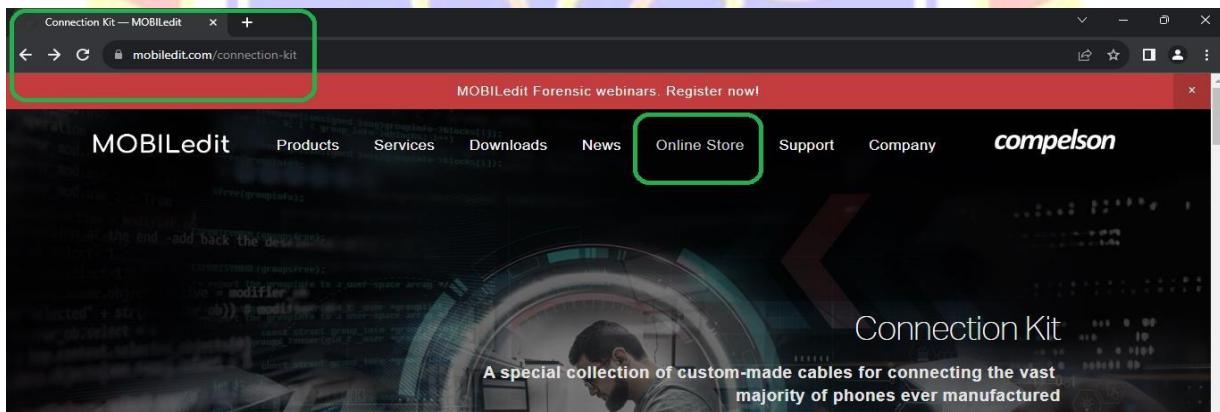
- Perform a forensic analysis of a mobile device, such as a smartphone or tablet.
- Retrieve call logs, text messages, and other relevant data for investigative purposes.

### Practical:

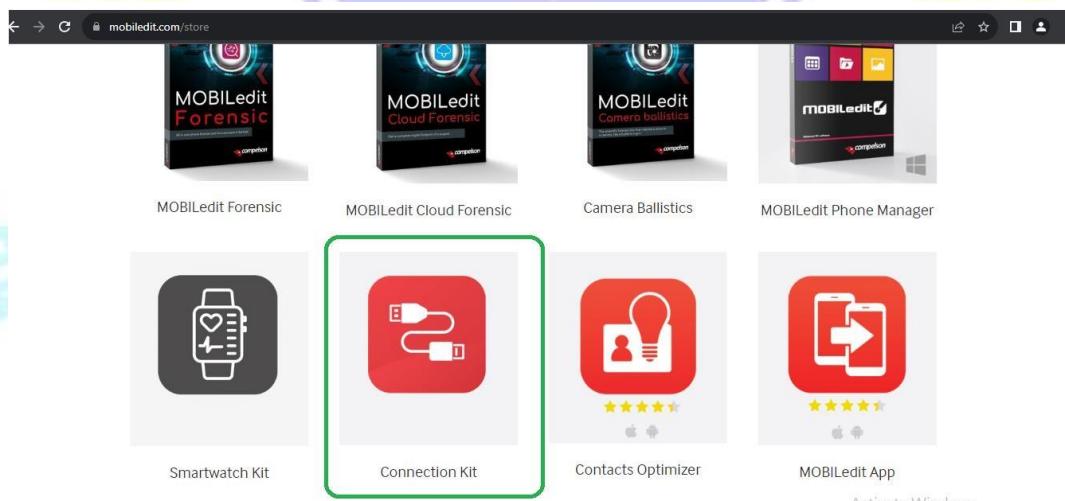
In this Practical we are going to perform the mobile forensic using the MOBILedit Forensic toolkit

We are going to download the MOBILedit toolkit

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



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



Activate Windows  
Go to Settings to activate Windows.



## SHRI G.P.M. DEGREE COLLEGE

Department of Computer

Vision.. Innovation.. Solution.. Presentation

The Price is given below. It is around \$1000

A screenshot of a web browser displaying the MOBILedit Connection Kit product page. The page features a large red icon of two USB cables. The title 'Connection Kit' is at the top, followed by a detailed 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'. A 'CONTACT US TO BUY' button is visible, along with a note to activate Windows.

Then we go to the software

A screenshot of a web browser displaying the MOBILedit store page. The page has a dark header with a search bar and a shopping cart icon. Below the header, there's 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'. To the right of the products is a 'Search' input field and a note to 'Activate Windows'.



# SHRI G.P.M. DEGREE COLLEGE

Department of Computer

Vision.. Innovation.. Solution.. Presentation

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
		Go to Settings to activate Windows.
		Cloud forensic (optional)

Now we are going to start the Practical



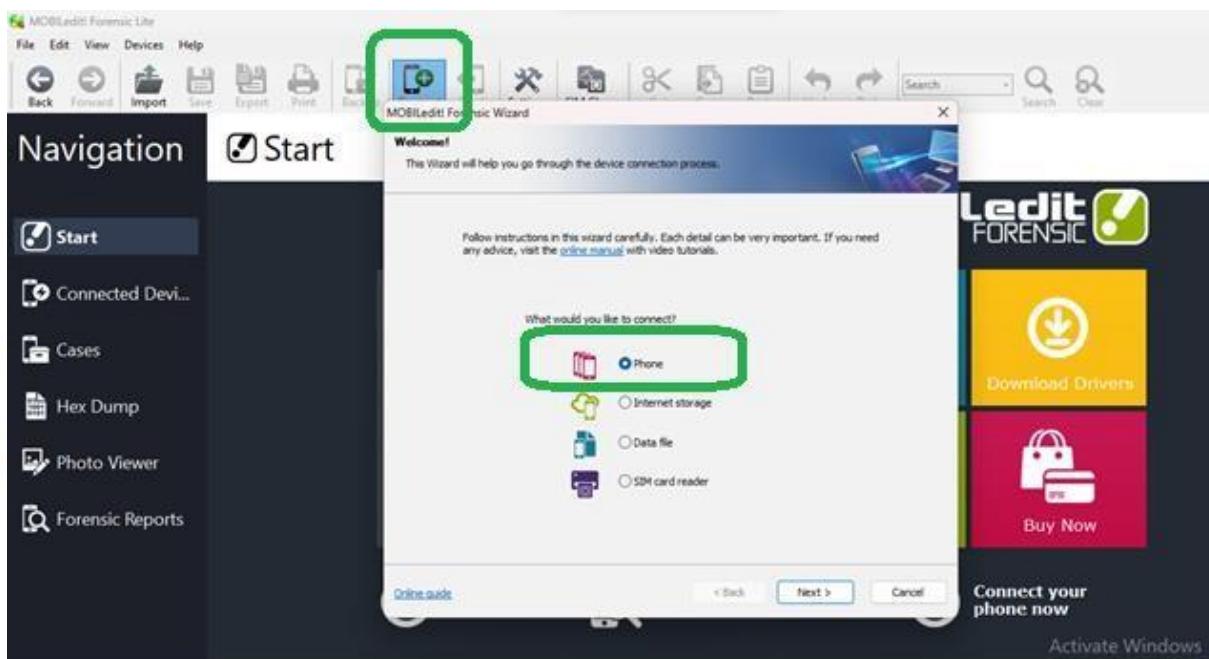


# SHRI G.P.M. DEGREE COLLEGE

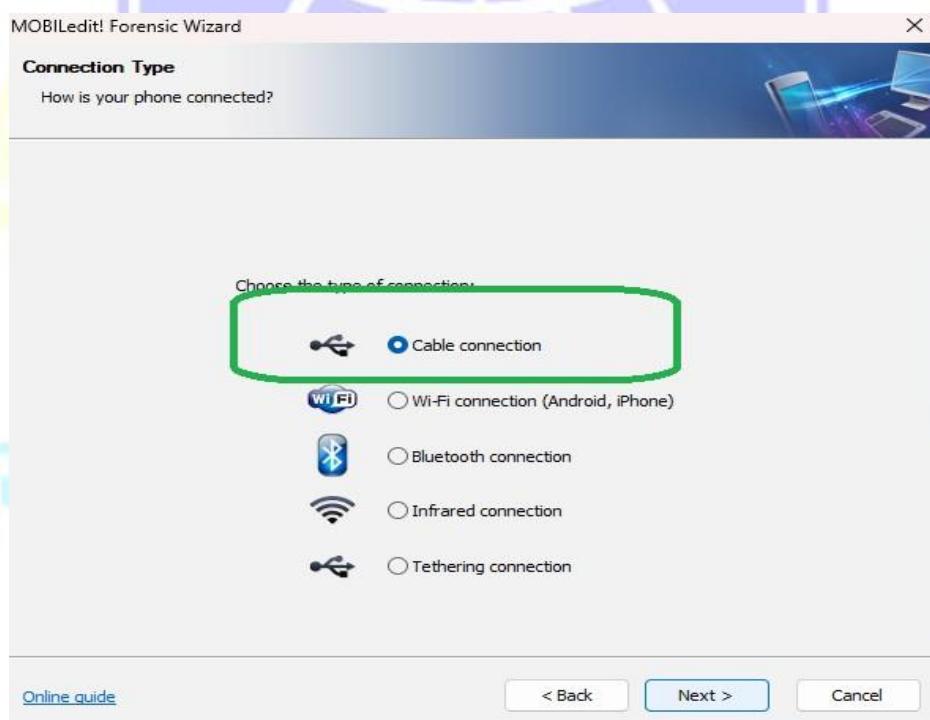
Department of Computer

Vision.. Innovation.. Solution.. Presentation

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





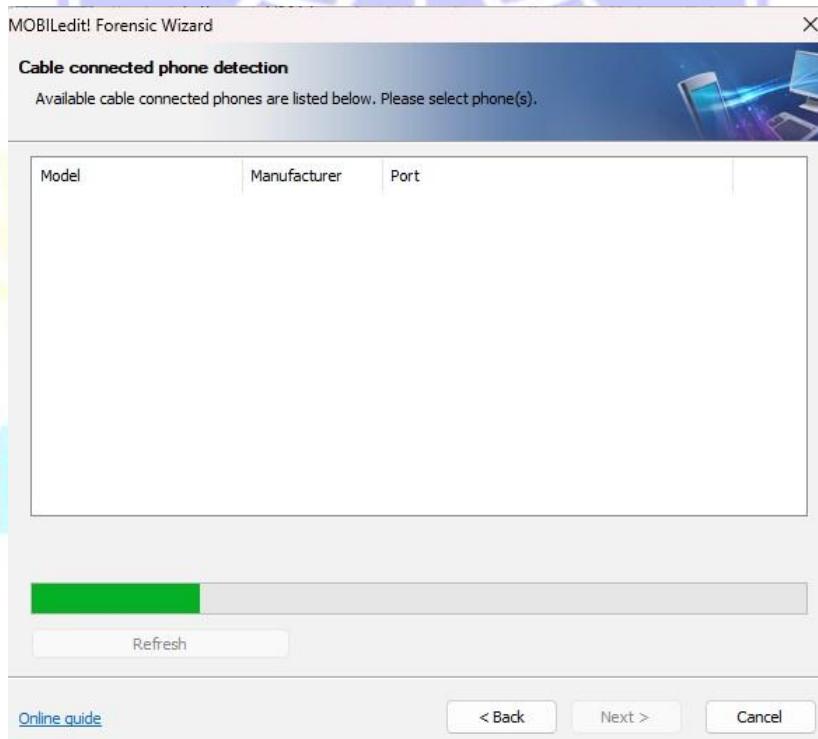
## SHRI G.P.M. DEGREE COLLEGE

Department of Computer

Vision.. Innovation.. Solution.. Presentation



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"



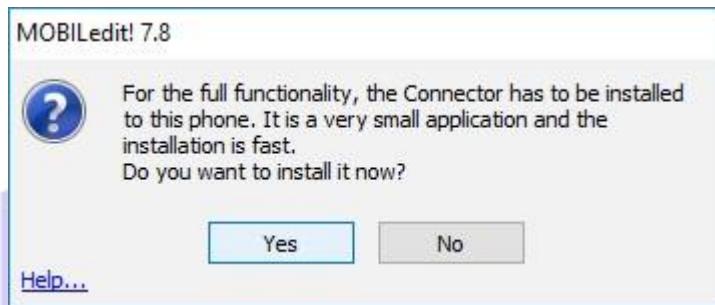


## SHRI G.P.M. DEGREE COLLEGE

Department of Computer

Vision.. Innovation.. Solution.. Presentation

Then connect it with a connector for efficient data recovery

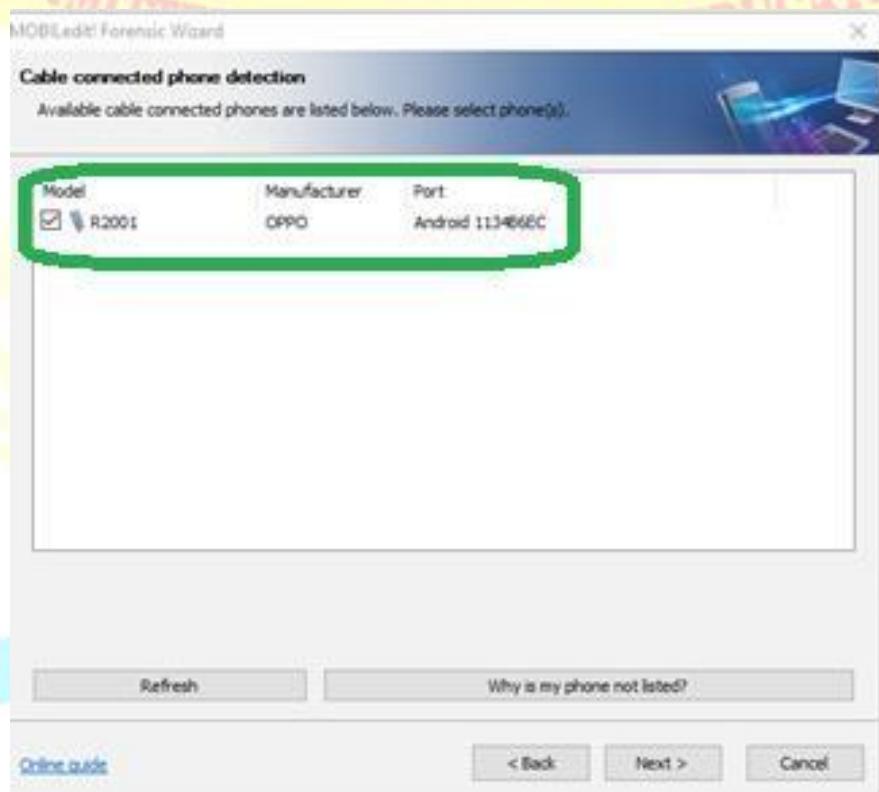


Working...

Installing MOBILedit! Connector... (this may take a while)

Cancel

We got a device connected



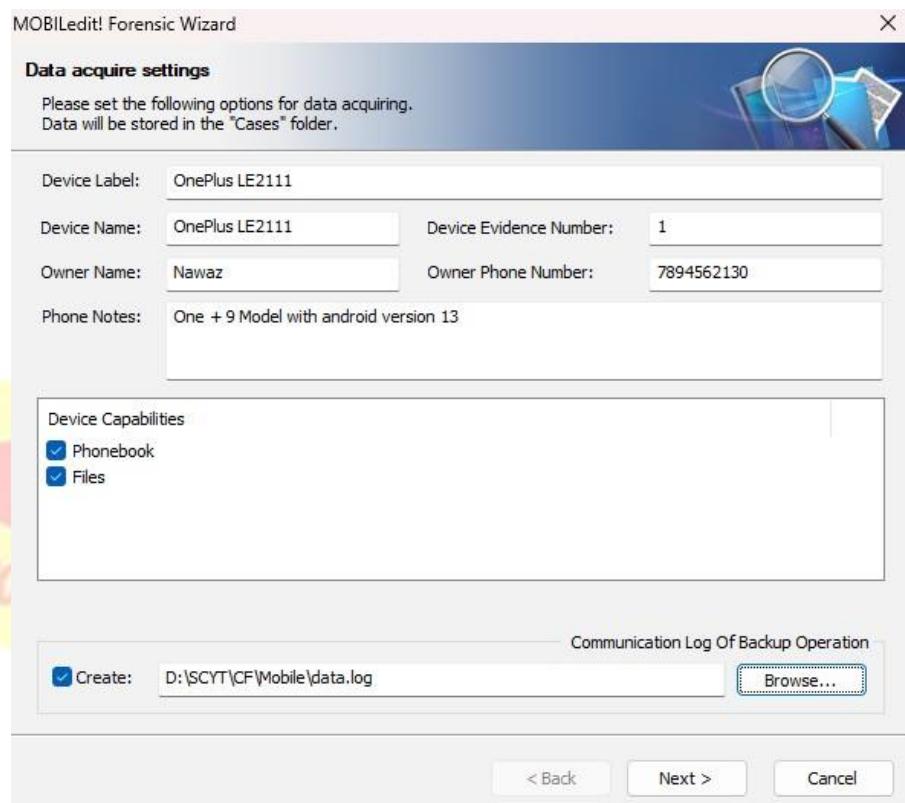


# SHRI G.P.M. DEGREE COLLEGE

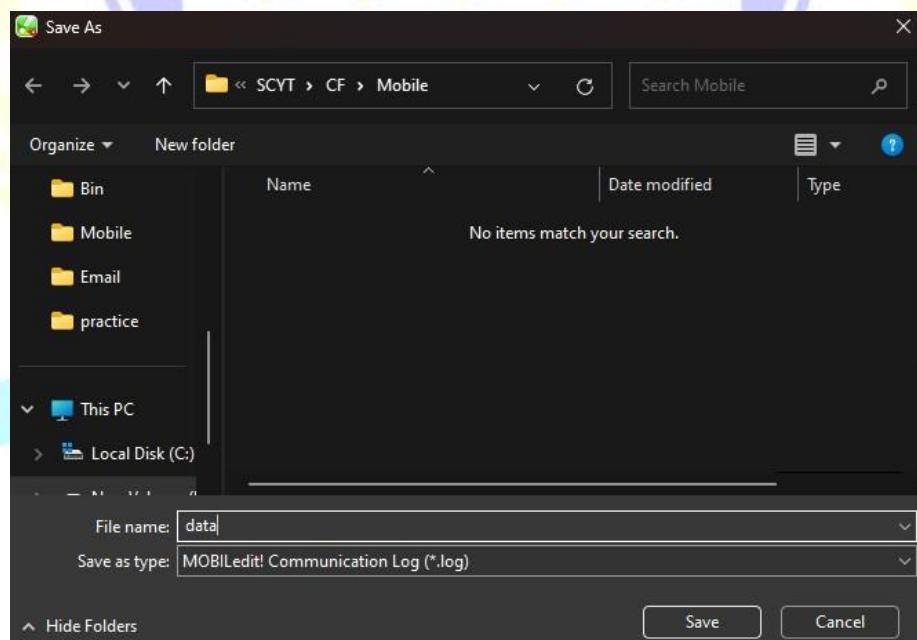
Department of Computer

Vision.. Innovation.. Solution.. Presentation

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



Fill the details and browse a directory to store the logs



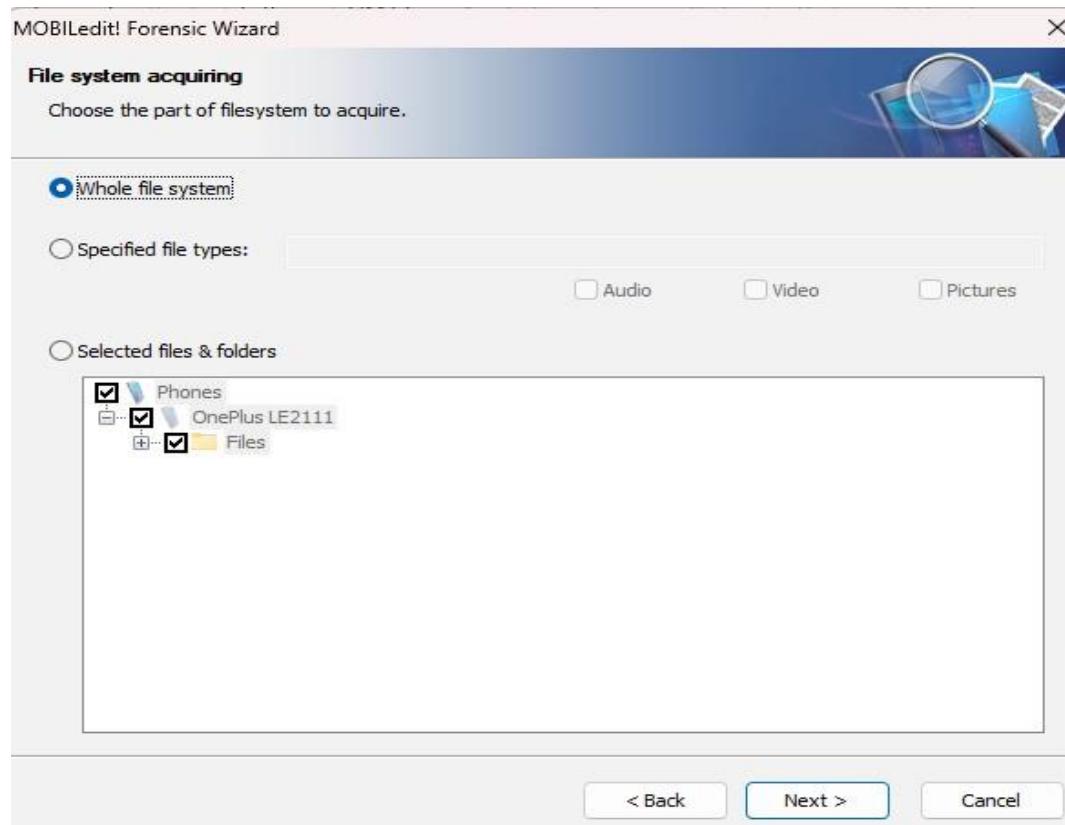


## SHRI G.P.M. DEGREE COLLEGE

Department of Computer

Vision.. Innovation.. Solution.. Presentation

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





# SHRI G.P.M. DEGREE COLLEGE

Department of Computer

Vision.. Innovation.. Solution.. Presentation

Click on Yes and Wait for the Acquisition to be completed

The image shows two side-by-side windows of the MOBILedit! Forensic Wizard. Both windows are titled "Data acquiring" and show a progress bar at the bottom indicating file reading operations.

**Left Window (Top):**

- Scanning "Files\Internal shared storage\Pictures\thumbnails\" folder for selected files...
- Data acquisition started on 13-09-2023 10:37:31
- Filesystem: Info
- Status: Initializing...

**Right Window (Top):**

- Reading file "OnePlus9Oxygen\_22.I.47 OTA\_1470\_all\_2203102115\_9570fb5.zip" from "OnePlus LE2111"...
- Item: Data acquisition started on 13-09-2023 10:37:31
- Status: The operation completed successfully.
- Filesystem: Info
- Status: The operation completed successfully.
- Filesystem: Canva
- Status: The operation completed successfully.
- Filesystem: .thumbnails
- Status: The operation completed successfully.
- Filesystem: Giphy
- Status: The operation completed successfully.
- Filesystem: Picsart
- Status: The operation completed successfully.
- Filesystem: AI Photo Enhancer
- Status: The operation completed successfully.
- Filesystem: Instagram
- Status: The operation completed successfully.
- Filesystem: Screenshots
- Status: The operation completed successfully.
- Filesystem: SquareBlend
- Status: The operation completed successfully.
- Filesystem: Truecaller Images
- Status: The operation completed successfully.
- Filesystem: Pictures
- Status: The operation completed successfully.
- Filesystem: .Ota
- Status: Item 1 out of 1

**Left Window (Bottom):**

- Reading file "Raaghu.2023.1080p.WEB.HDRip.Hindi.HQ.Dub.DD.2.0.x264.mkv" from "OnePlus LE2111"...
- Item: The operation completed successfully.
- Status: The operation completed successfully.
- Filesystem: SquareBlend
- Status: The operation completed successfully.
- Filesystem: Truecaller Images
- Status: The operation completed successfully.
- Filesystem: Pictures
- Status: The operation completed successfully.
- Filesystem: .Ota
- Status: The operation completed successfully.
- Filesystem: Scoompa Video
- Status: The operation completed successfully.
- Filesystem: Reverse
- Status: The operation completed successfully.
- Filesystem: .thumbnails
- Status: The operation completed successfully.
- Filesystem: Whatsapp
- Status: The operation completed successfully.
- Filesystem: Canva
- Status: The operation completed successfully.
- Filesystem: Creative content writing
- Status: The operation completed successfully.
- Filesystem: BrandSpot365
- Status: The operation completed successfully.
- Filesystem: com\_account\_usercenter...
- Status: The operation completed successfully.
- Filesystem: com\_account\_usercenter...
- Status: The operation completed successfully.
- Filesystem: playlist
- Status: The operation completed successfully.
- Filesystem: playlist1
- Status: The operation completed successfully.
- Filesystem: Download
- Status: Item 1 out of 15

**Right Window (Bottom):**

- Reading file "Raaghu.2023.1080p.WEB.HDRip.Hindi.HQ.Dub.DD.2.0.x264.mkv" from "OnePlus LE2111"...
- Item: The operation completed successfully.
- Status: The operation completed successfully.
- Filesystem: SquareBlend
- Status: The operation completed successfully.
- Filesystem: Truecaller Images
- Status: The operation completed successfully.
- Filesystem: Pictures
- Status: The operation completed successfully.
- Filesystem: .Ota
- Status: The operation completed successfully.
- Filesystem: Scoompa Video
- Status: The operation completed successfully.
- Filesystem: Reverse
- Status: The operation completed successfully.
- Filesystem: .thumbnails
- Status: The operation completed successfully.
- Filesystem: Whatsapp
- Status: The operation completed successfully.
- Filesystem: Canva
- Status: The operation completed successfully.
- Filesystem: Creative content writing
- Status: The operation completed successfully.
- Filesystem: BrandSpot365
- Status: The operation completed successfully.
- Filesystem: com\_account\_usercenter...
- Status: The operation completed successfully.
- Filesystem: com\_account\_usercenter...
- Status: The operation completed successfully.
- Filesystem: playlist
- Status: The operation completed successfully.
- Filesystem: playlist1
- Status: The operation completed successfully.
- Filesystem: Download
- Status: Item 1 out of 15

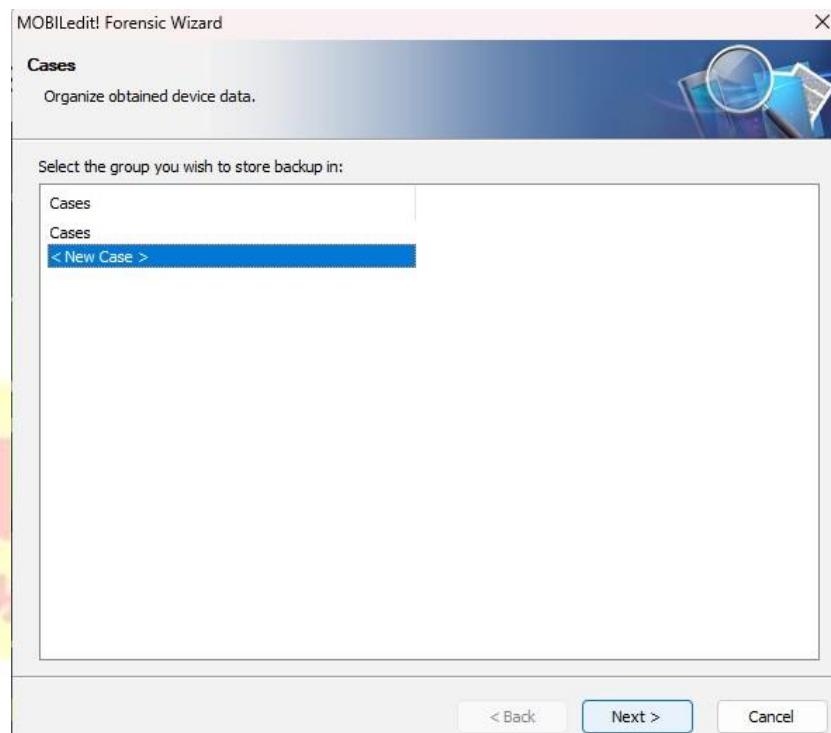


## SHRI G.P.M. DEGREE COLLEGE

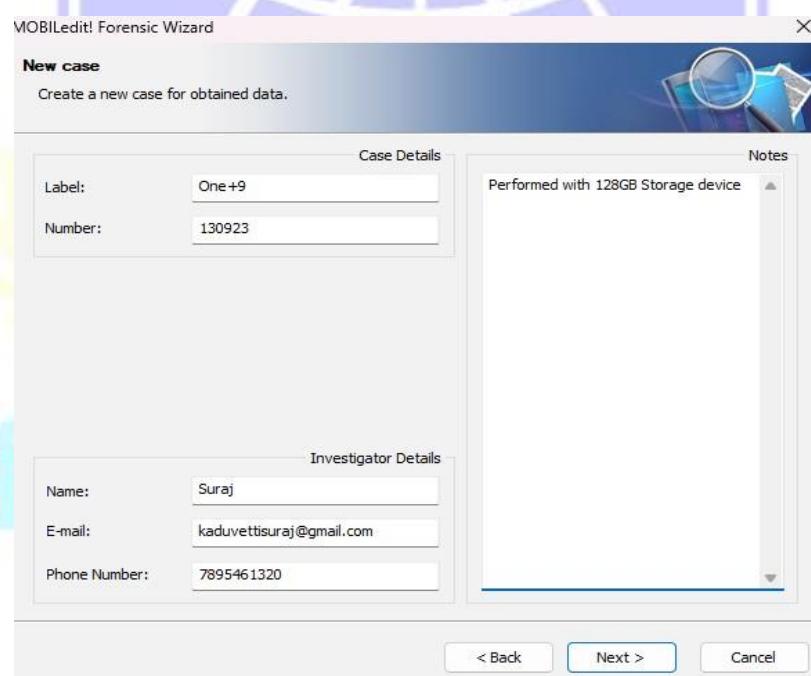
Department of Computer

Vision.. Innovation.. Solution.. Presentation

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



Fill in the details of the Investigator



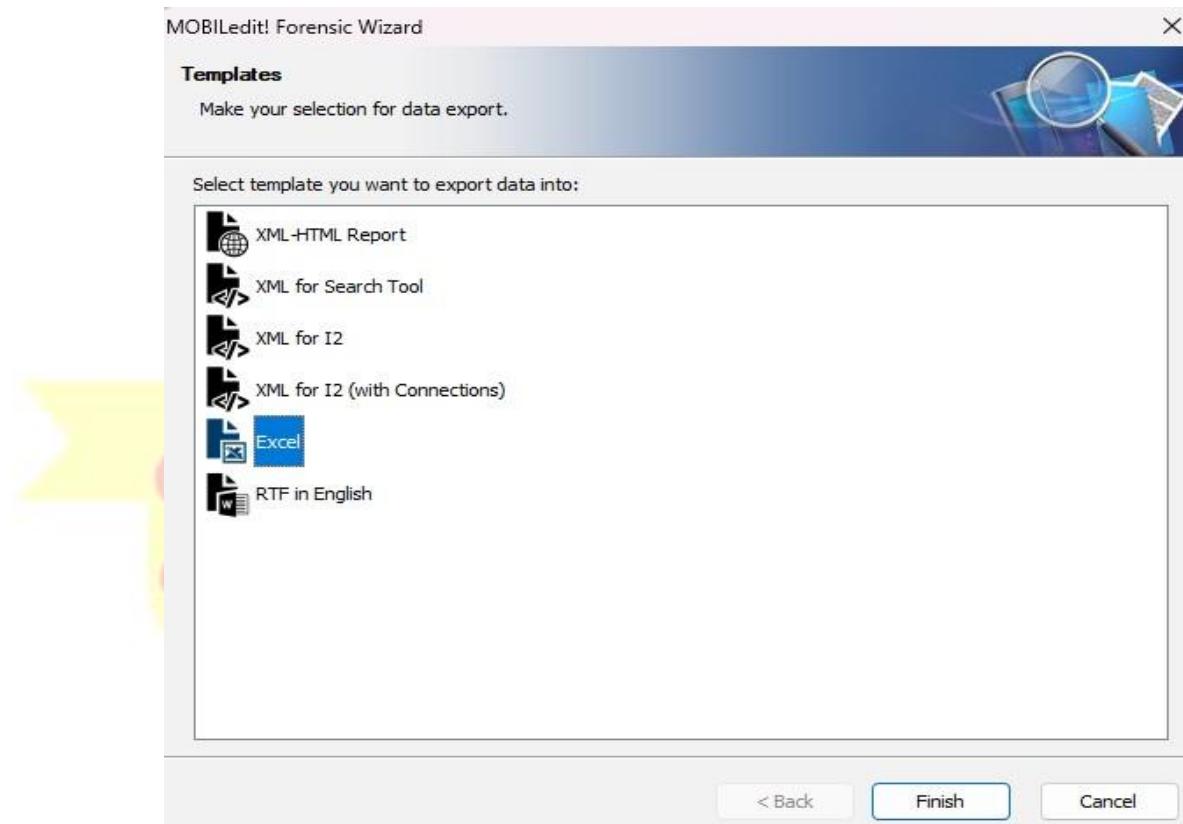


## SHRI G.P.M. DEGREE COLLEGE

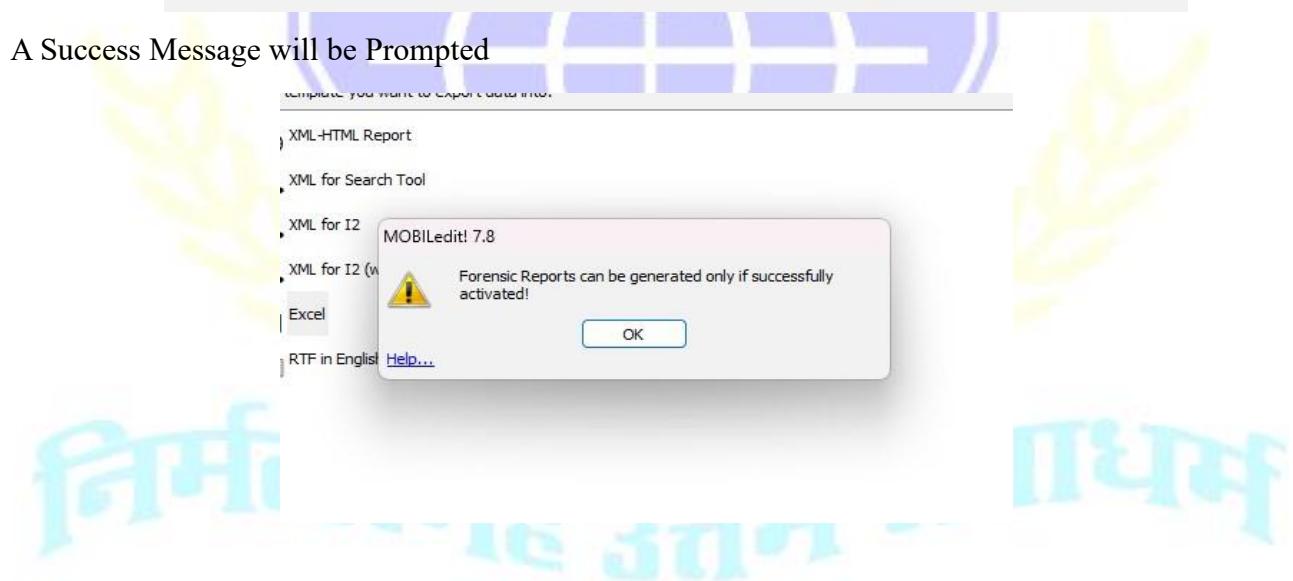
Department of Computer

Vision.. Innovation.. Solution.. Presentation

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**

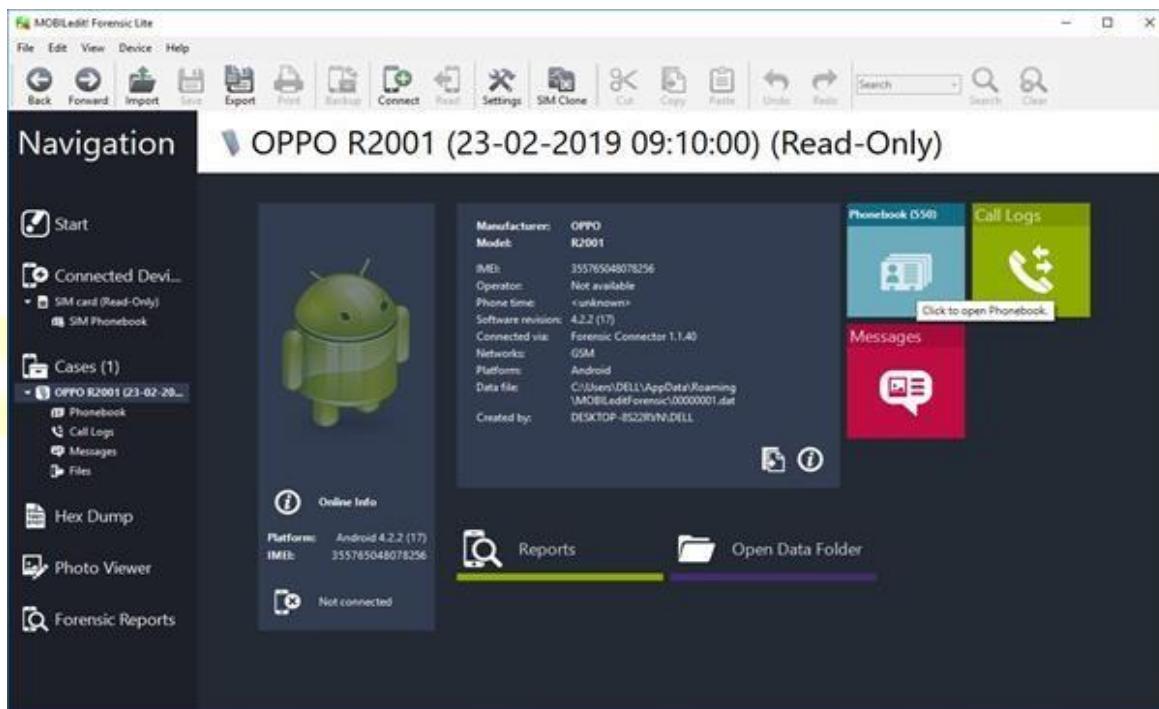
We have performed of Two Mobile Devices

The First One is the Oppo Reno 2



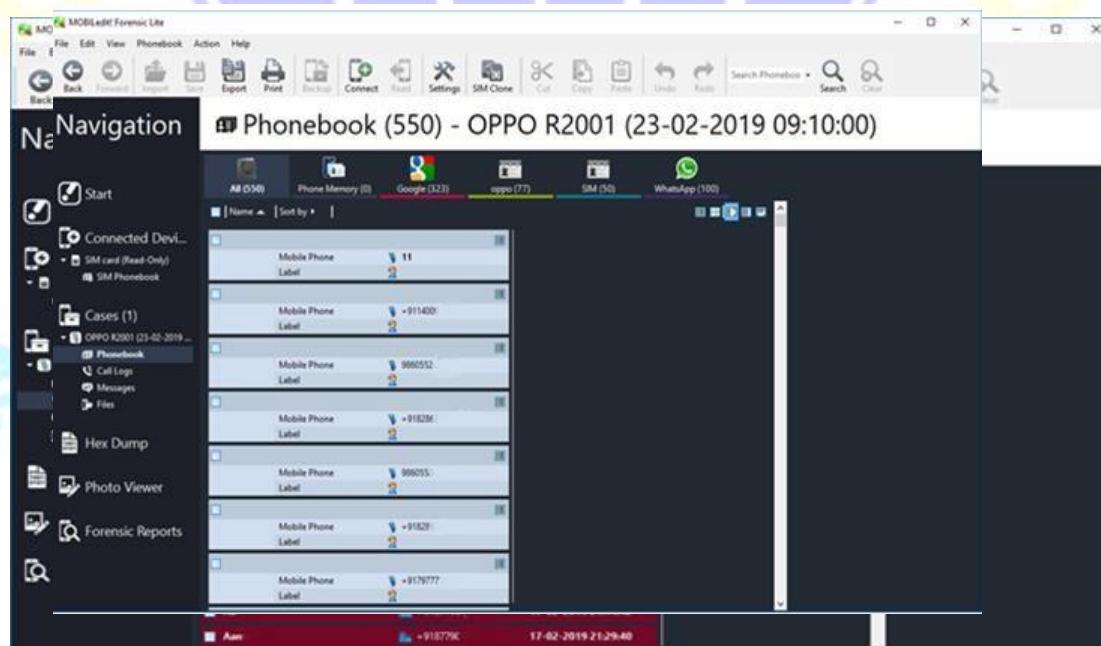
Second One is the One<sup>+</sup> 9

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





# SHRI G.P.M. DEGREE COLLEGE

Department of Computer

Vision.. Innovation.. Solution.. Presentation

And here we can see the messages on the device

The screenshot shows the 'Messages' tab in MOBILedit! Forensic Lite. The title bar reads 'Messages - OPPO R2001 (23-02-2019 09:10:00)'. The left sidebar has a 'Navigation' section with options like Start, Connected Device (OPPO R2001), Cases (1), Hex Dump, Photo Viewer, and Forensic Reports. The main area displays a list of messages. The 'Received (500)' tab is selected. A message from 'IDEA' dated 22-02-2019 at 20:59:25 is highlighted. Other messages include 'Aaa' (22-02-2019 17:19:31), 'IM-65' (22-02-2019 14:46:43), 'IM-612' (22-02-2019 14:15:48), 'IM-65' (22-02-2019 10:34:12), '+91998' (21-02-2019 16:52:49), 'MD-K' (21-02-2019 16:46:12), 'AX-IY' (21-02-2019 12:05:36), and 'IM-657' (21-02-2019 12:05:36). The right side shows a search bar and filter options.

Display of the Second Device One<sup>+</sup> 9

The screenshot shows the main interface of MOBILedit! Forensic Lite. The title bar reads 'MOBILedit! Forensic Lite'. The left sidebar has a 'Navigation' section with options like Start, Connected Device (OnePlus LE2111 (Read-Only)), Cases (1), Hex Dump, Photo Viewer, and Forensic Reports. The central area shows a smartphone icon with 'Windows Phone 1.0, MTP: 1.00' and 'Connected to USB OnePlus 9 5G'. To the right, there's a summary of the device: Manufacturer: OnePlus, Model: LE2111, Operator: Not available, Phone time: <unknown>, Hardware revision: OnePlus,LE2111, Software revision: 1.0,MTP: 1.00, Networks: GSM, Platform: Windows Phone. Below this, it says 'Connection: OnePlus 9 5G'. On the right, there are two sections: 'Phonebook' (with a contact icon) and 'Files' (with a file/folder icon). At the bottom, there are 'Report Wizard' and 'Reports' buttons, and a link to 'Activate Windows'.

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



# SHRI G.P.M. DEGREE COLLEGE

Department of Computer

Vision.. Innovation.. Solution.. Presentation

The screenshot shows the MOBILedit! Forensic Lite interface. The left sidebar has a 'Navigation' section with icons for Start, Connected Device (OnePlus LE2111), Cases (One+9), Hex Dump, Photo Viewer, and Forensic Reports. The main area shows a file tree under 'Camera - OnePlus LE2111'. The 'Files' folder contains 'Internal shared storage' which includes subfolders like .1685961648618\_200\_, .config, .FileManagerRecycler, .oprecyclebin, .Ota, .SLOGAN, Alarms, Android, Audiobooks, DCIM, .convert\_tmp\_files, .wallpaperVideo, Camera, Collage, community, MyAlbums (containing Ahsana, Ali Hamraz, Ali maula, mom, Nawaz Hassan, Rosho, simmba, Tuba, vaszia, zoya), and Screenshots. A large list of files is shown on the right, each with columns for File Name, Size, Created, and Modified. A 'Parent' button is at the top right of the file list.

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**

```
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 0x2af
3085.2219 [2:api:10532] GetParameter(GLOBAL:0xffff, 0xffff041b, &x0FF0FC08,
&x0FF1FC08) returned 0x2af
```

**Result:**

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

**Learning Outcomes:**

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

**Course Outcomes:**

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

**Conclusion:****Viva Questions:**

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



## PRACTICAL NO: 9

### Aim:

Email Forensics

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

### Practical:

Here we are going to use the AccessData FTK

FTK can filter or find files specific to e-mail clients and servers.

You can configure these filters when you enter search parameters.

Because of Jim's responses to a poor performance review, the CEO of Superior Bicycles, Martha Dax, suspects he might have obtained sensitive information about the company's business model that he's leaking to a competitor.

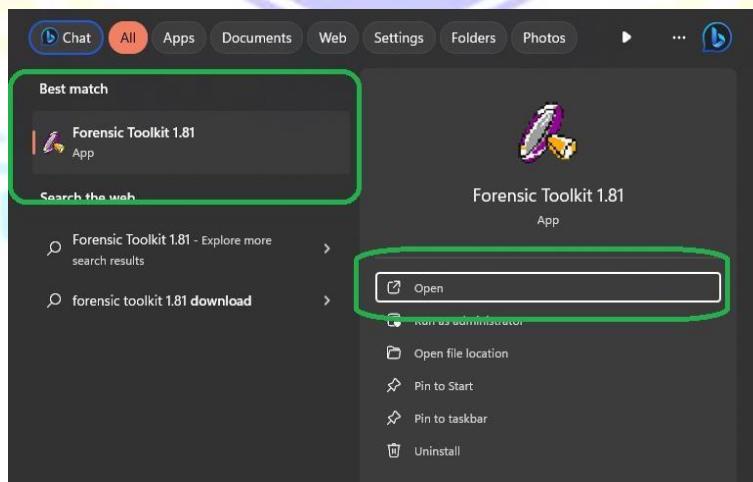
Martha asked her CIO, to have an IT employee copy the Outlook .pst file from Jim Shu's old computer to a USB drive.

To process this investigation, we need to examine the Jim\_shu's.pst file, locate the message, and export it for further analysis of its header to see how Jim might have received it.

### Recovering Email

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

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



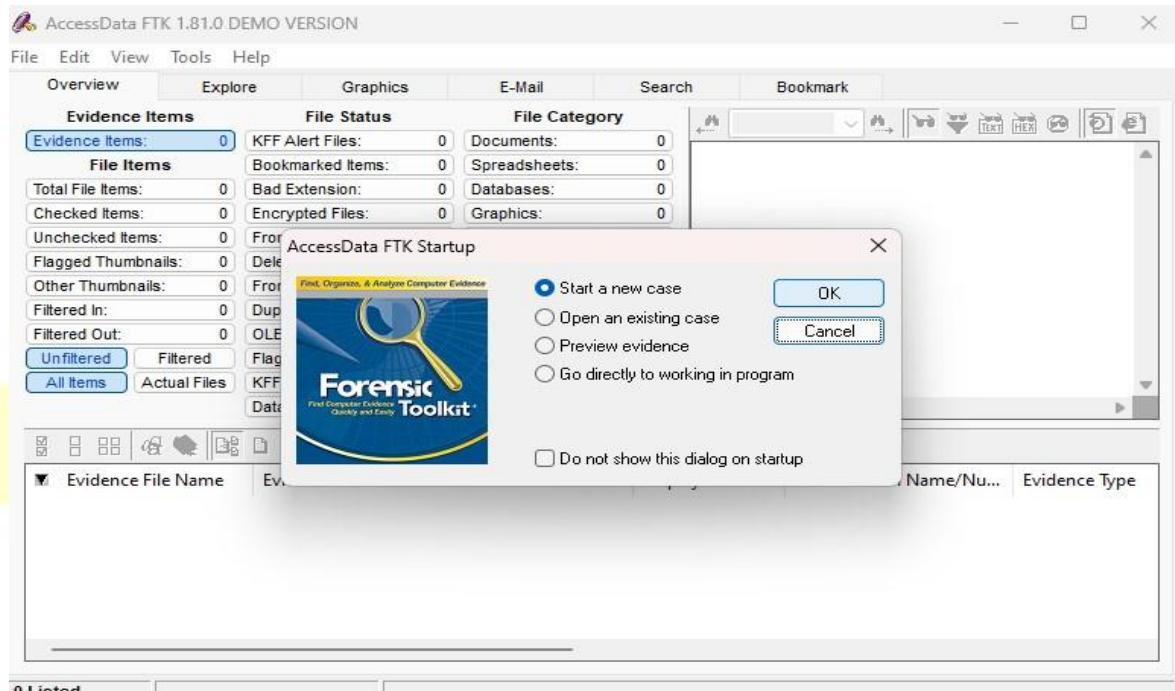


# SHRI G.P.M. DEGREE COLLEGE

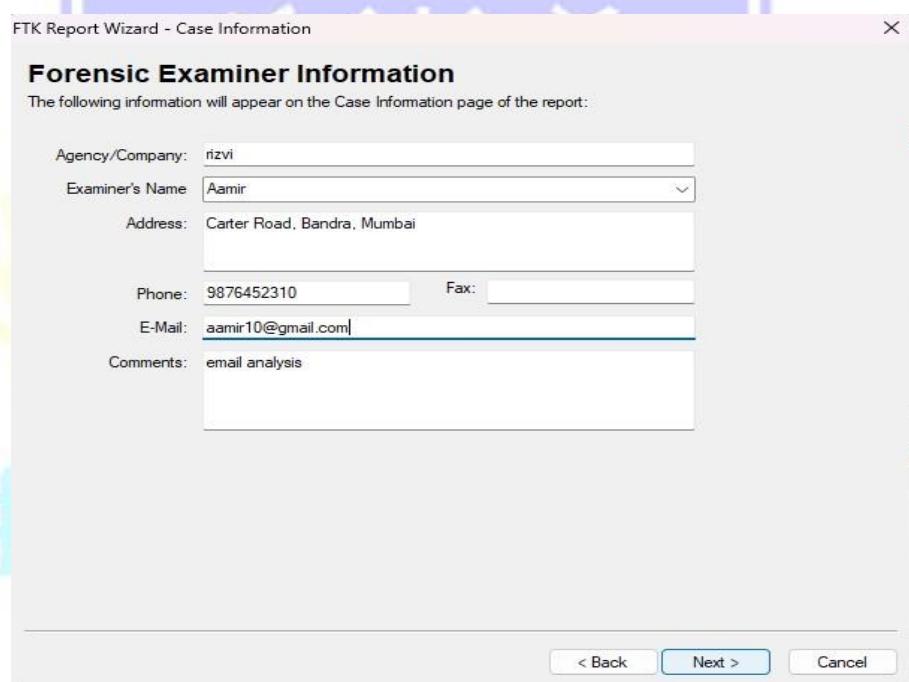
Department of Computer

Vision.. Innovation.. Solution.. Presentation

## Create a new File



## Fill the details of the Examiner



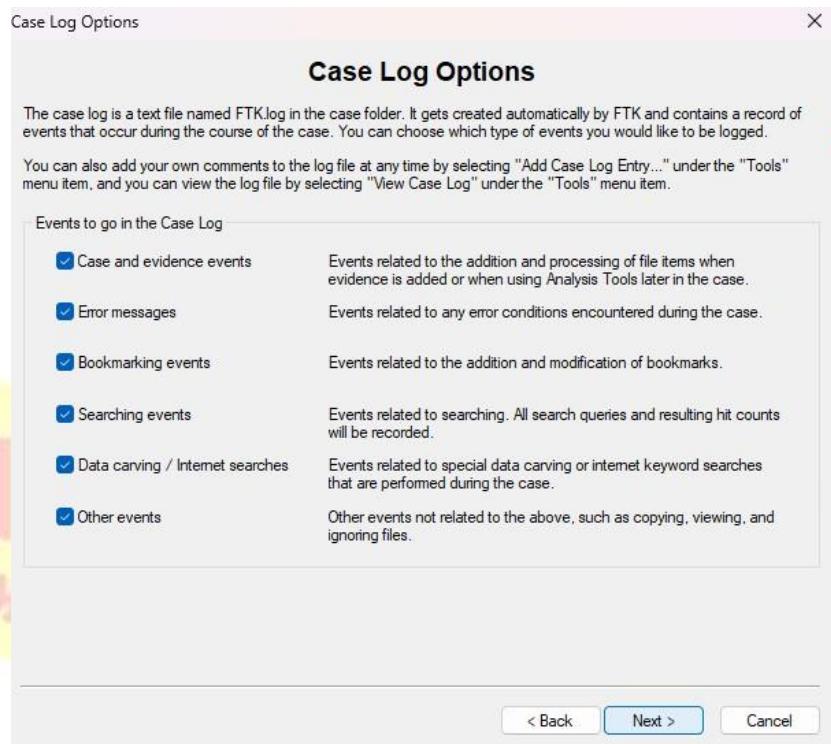


# SHRI G.P.M. DEGREE COLLEGE

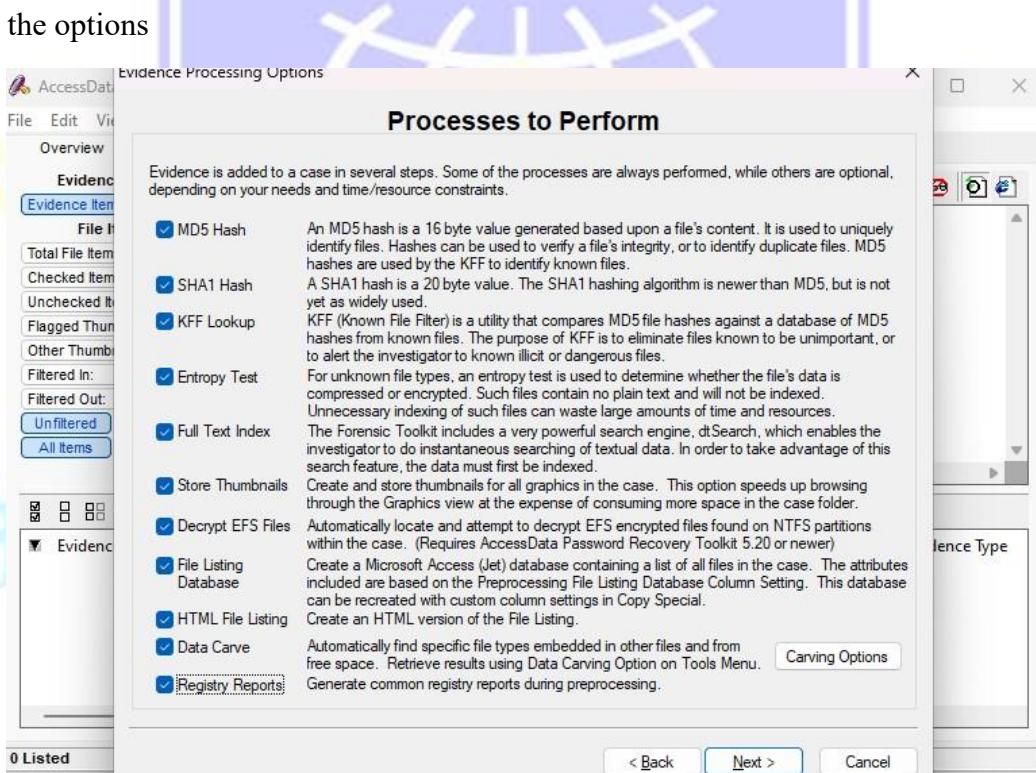
Department of Computer

Vision.. Innovation.. Solution.. Presentation

Click on all the options and Click Next



Select all the options





# SHRI G.P.M. DEGREE COLLEGE

Department of Computer

Vision.. Innovation.. Solution.. Presentation

Now we have reached the Email Emphasis section

Refine Case - Default

### Refine Case - Default

In order to save time and resources, and/or to eliminate irrelevant data, you may choose to exclude certain kinds of data from the case. Here, you can choose default inclusion/exclusion settings that will apply to each evidence item that gets added to the case. To exclude data, make any changes to the settings below. Note: any items that get excluded will not appear anywhere in the case, and will be inaccessible.

Include All Items    Optimal Settings    **Email Emphasis**    Text Emphasis    Graphics Emphasis

Unconditionally Add

File Slack (data beyond the end of the logical file but within the area allocated to that file by the file system)  
 Free Space (areas in the file system not currently allocated to any file, but possibly containing deleted file data)  
 KFF Ignorable Files (files found by KFF to be forensically unimportant, i.e., OS system files, known applications, etc.)  
 Extract files from KFF ignorable containers

Conditionally Add

Add other items to the case only if they satisfy BOTH the file status and the file type criteria

<b>File Status Criteria</b>	<b>File Type Criteria</b>
Deletion Status: <input type="radio"/> Deleted <input type="radio"/> Not deleted <input checked="" type="radio"/> Either	Encryption Status: <input type="radio"/> Encrypted <input type="radio"/> Not encrypted <input checked="" type="radio"/> Either
<input type="checkbox"/> From email <input type="checkbox"/> Not from email <input type="checkbox"/> Either <input type="checkbox"/> Include Duplicate Files	<input checked="" type="checkbox"/> Documents <input type="checkbox"/> Executables <input checked="" type="checkbox"/> Spreadsheets <input checked="" type="checkbox"/> Archives <input checked="" type="checkbox"/> Databases <input type="checkbox"/> Folders <input checked="" type="checkbox"/> Graphics <input checked="" type="checkbox"/> Other Known <input checked="" type="checkbox"/> Multimedia <input checked="" type="checkbox"/> Unknown <input checked="" type="checkbox"/> Email msgs

< Back    Next >    Cancel

Refine Index - Default

### Refine Index - Default

In order to save time and resources, and/or to make searching more efficient, you may choose to exclude certain kinds of data from being indexed. Here, you can choose default settings that will apply to each evidence item that gets added to the case. To exclude items from being indexed, make any changes to the settings below. Note: any items that don't get indexed initially can be indexed later by clicking on "Analysis Tools" under the "Tools" menu item.

Unconditionally Index

File Slack (data beyond the end of the logical file but within the area allocated to that file by the file system)  
 Free Space (areas in the file system not currently allocated to any file, but possibly containing deleted file data)  
 KFF Ignorable Files (files found by KFF to be forensically unimportant, i.e., OS system files, known applications, etc.)

Conditionally Index

Index other items in the case only if they satisfy BOTH the file status and the file type criteria

<b>File Status Criteria</b>	<b>File Type Criteria</b>
Deletion Status: <input type="radio"/> Deleted <input type="radio"/> Not deleted <input checked="" type="radio"/> Either	Encryption Status: <input type="radio"/> Encrypted <input type="radio"/> Not encrypted <input checked="" type="radio"/> Either
<input type="checkbox"/> From email <input type="checkbox"/> Not from email <input type="checkbox"/> Either <input type="checkbox"/> Include Duplicate Files	<input checked="" type="checkbox"/> Documents <input type="checkbox"/> Executables <input checked="" type="checkbox"/> Spreadsheets <input checked="" type="checkbox"/> Archives <input checked="" type="checkbox"/> Databases <input type="checkbox"/> Folders <input checked="" type="checkbox"/> Graphics <input checked="" type="checkbox"/> Other Known <input checked="" type="checkbox"/> Multimedia <input checked="" type="checkbox"/> Unknown <input checked="" type="checkbox"/> Email msgs

< Back    Next >    Cancel

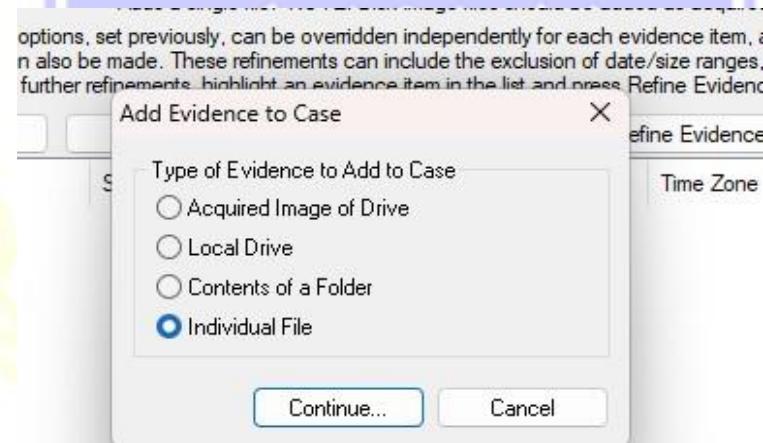
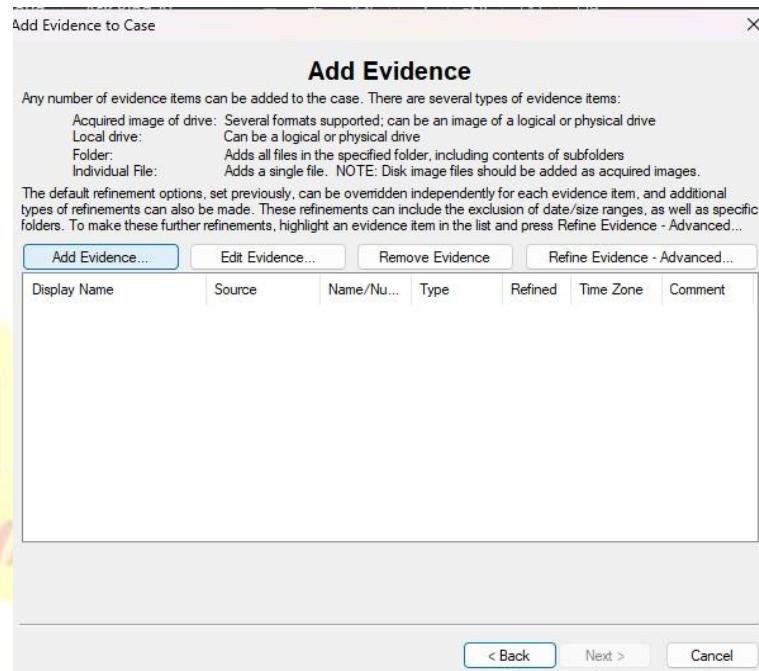


## SHRI G.P.M. DEGREE COLLEGE

Department of Computer

Vision.. Innovation.. Solution.. Presentation

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**.



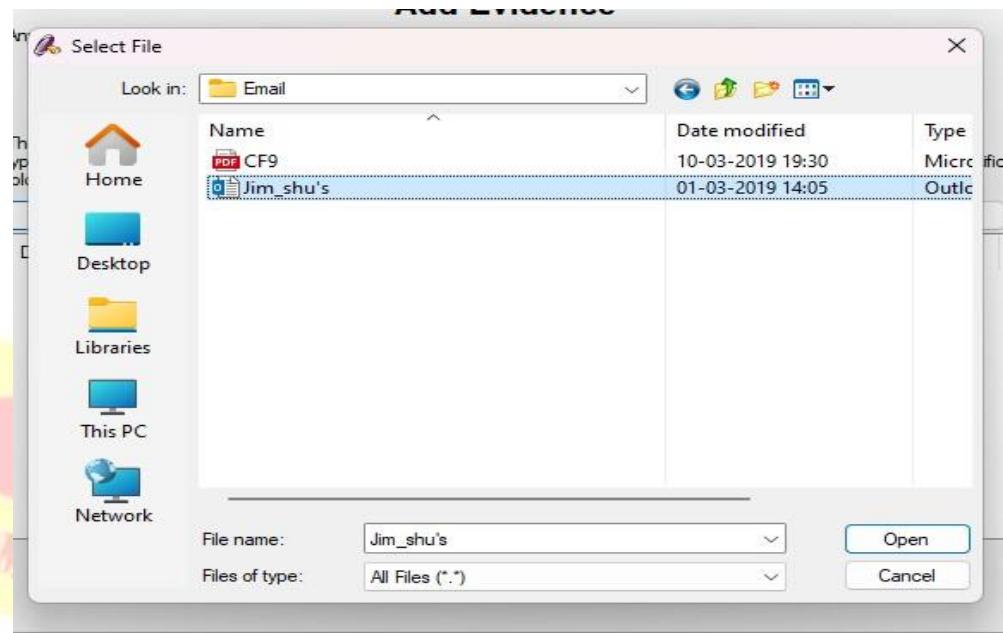


## SHRI G.P.M. DEGREE COLLEGE

Department of Computer

Vision.. Innovation.. Solution.. Presentation

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

**Evidence Information**

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

Evidence Display Name:  
Jim\_shu's

Evidence Identification Name/Number:  
10

Comment:  
Here is an example for the email

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

OK Cancel

Complete the steps and Click on Next



# SHRI G.P.M. DEGREE COLLEGE

Department of Computer

Vision.. Innovation.. Solution.. Presentation

Add Evidence to Case X

### Add Evidence

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

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

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

[Add Evidence...](#) [Edit Evidence...](#) [Remove Evidence](#) [Refine Evidence - Advanced...](#)

Display Name	Source	Name/Nu...	Type	Refined	Time Zone	Comment
Jim_shu's	D:\SCYT\CF\...	10	Individual f...	N	N/A	Here is an ...

[< Back](#) [Next >](#) [Cancel](#)

Click on finish and see the data

Case Summary X

### New Case Setup is Now Complete

Case Settings

Case directory where the file database, index, and other case-specific files will be stored:  
**D:\SCYT\CF\Email\jimshu@mail**

Number of Evidence Items: 1

Processes to be Performed:

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

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

[< Back](#) [Finish](#) [Cancel](#)



# SHRI G.P.M. DEGREE COLLEGE

Department of Computer

Vision.. Innovation.. Solution.. Presentation

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

File Edit View Tools Help

Overview Explore Graphics E-Mail Search Bookmark

Evidence Items	File Status	File Category
Evidence Items: 1	KFF Alert Files: 0	Documents: 1
	Bookmarked Items: 0	Spreadsheets: 0
Total File Items: 40	Bad Extension: 1	Databases: 0
Checked Items: 0	Encrypted Files: 0	Graphics: 1
Unchecked Items: 40	From E-mail: 40	Multimedia: 0
Flagged Thumbnails: 0	Deleted Files: 6	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
<input type="button" value="Unfiltered"/> <input type="button" value="Filtered"/>	Flagged Ignore: 0	Slack/Free Space: 0
<input type="button" value="All Items"/> <input type="button" value="Actual Files"/>	KFF Ignorable: 0	Other Known Type: 5
	Data Carved Files: 0	Unknown Type: 0

File Name Evidence Path Display Name Identification Name/Number Evidence Type

Jim\_shu's.pst D:\SCYT\CF>Email Jim\_shu's 10 Individual file

1 Listed 0 Checked Total 0 Highlighted

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

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

File Edit View Tools Help

Overview Explore Graphics E-Mail Search Bookmark

Evidence Items	File Status	File Category
Evidence Items: 1	KFF Alert Files: 0	Documents: 1
	Bookmarked Items: 0	Spreadsheets: 0
Total File Items: 40	Bad Extension: 1	Databases: 0
Checked Items: 0	Encrypted Files: 0	Graphics: 1
Unchecked Items: 40	From E-mail: 40	Multimedia: 0
Flagged Thumbnails: 0	Deleted Files: 32	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
<input type="button" value="Unfiltered"/> <input type="button" value="Filtered"/>	Flagged Ignore: 0	Slack/Free Space: 0
<input type="button" value="All Items"/> <input type="button" value="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

32 Listed 0 Checked Total 0 Highlighted



## SHRI G.P.M. DEGREE COLLEGE

Department of Computer

Vision.. Innovation.. Solution.. Presentation

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

The screenshot shows the AccessData FTK software interface. The menu bar includes File, Edit, View, Tools, and Help. The tabs at the top are Overview, Explore, Graphics, E-Mail (which is selected), Search, and Bookmark. The left pane displays a tree view of email folders under 'Email'. A folder named 'Jim\_shu's.pst' is expanded, showing sub-folders 'Message0007' and 'Message0008', and a 'Personal Fold' folder containing 'Top of Pe...' and other items. A checkbox 'List all descendants' is present. The right pane shows the details of 'Message0001'. The message header includes:

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

The message body contains the text:

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

At the bottom, a table provides file details:

File Name	Full Path	Recycle Bi...	Ext	File Type	Category	Sub
AC19.jpg	D:\SCYT\CF>Email\Jim_shu's.pst>Personal Fol...		gpi	JPEG/JFIF File	Graphic	

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



# SHRI G.P.M. DEGREE COLLEGE

Department of Computer

Vision.. Innovation.. Solution.. Presentation

The screenshot shows two windows of the AccessData FTK 1.81.0 application. The top window displays a context menu for a file named 'AC19.gpi' located in the 'Deleted Items' folder. The menu options include 'Create Bookmark...', 'View This Item in a Different List', 'Ignore Item', 'Launch Detached Viewer' (which is highlighted with a green oval), 'Launch Associated Program', 'View With...', 'Copy Special...', 'Export File...', 'Recursive File Export...', 'Analysis Tools...', and 'Column Settings...'. The bottom window shows the 'Detached Viewer' pane displaying the image 'AC19.gpi', which is a graphic file. The file properties listed are Full path: D:\SCYT\CF\Email\Jim\_shu's.pst>Personal Fol... and File type: JPEG/JFIF File Graphic.

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).



# SHRI G.P.M. DEGREE COLLEGE

Department of Computer

Vision.. Innovation.. Solution.. Presentation

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

File Edit View Tools Help

Overview Explore Graphics E-Mail Search Bookmark

Message0002

Subject: Bike spec's  
From: Sam  
Date: 04-12-2006 07:09:29  
To: jim\_shu@comcast.net

Message Body

Do you have them yet?

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

<input type="checkbox"/> Message0001	D:\SCYT\CF>Email\Jim_shu's.pst>>Personal Fol...			E-mail Messa...	E-mail
<input checked="" type="checkbox"/> Message0002	D:\SCYT\CF>Email\Jim_shu's.pst>>Personal Fol...			E-mail Messa...	E-mail
<input type="checkbox"/> Message0003	D:\SCYT\CF>Email\Jim_shu's.pst>>Personal Fol...			E-mail Messa...	E-mail
<input type="checkbox"/> Message0004	D:\SCYT\CF>Email\Jim_shu's.pst>>Personal Fol...			E-mail Messa...	E-mail
<input type="checkbox"/> Message0005	D:\SCYT\CF>Email\Jim_shu's.pst>>Personal Fol...			E-mail Messa...	E-mail

10 Listed 0 Checked Total D:\SCYT\...\Jim\_shu's.pst>>Personal Folders>>Top of Personal Folders>>Inbox>>Message0002

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

निर्मलासनेह उत्तम सेवाधर्म



# SHRI G.P.M. DEGREE COLLEGE

Department of Computer

Vision.. Innovation.. Solution.. Presentation

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

File Edit View Tools Help

Overview Explore Graphics E-Mail Search Bookmark

YT CF Email Jim\_shu's... Message003

Create Bookmark... View This Item in a Different List > spec's

Ignore Item Launch Detached Viewer 6 07:44:02

Person Launch Associated Program omcast.net

Top View With... Message Body

Copy Special Export File... 10 if it is good. Is it? Sam

Properties File Export

Analysis Tools... Column Settings... File Properties...

All Columns Recycle Bi... Ext File Type Category

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

10 Listed 0 Checked Total D:\SCYT\... Jim\_shu's.pst>>Personal Folders>>Top of Personal Folders>>Inbox>>Message003

Export Files

File(s) to Export

All highlighted files  All checked files  All currently listed files  All files

Include email attachments with email messages

File Name: Jim\_shu's[2].pst-Personal Folders-Top... Original Path: D:\SCYT\CF\Email

Destination Path: D:\SCYT\CF\Email\jimshuemail\Export\

Prepend archive name to file name  
 Append item number to file name to guarantee uniqueness  
 Append appropriate extension to file name if bad/absent  
 Export HTML view if available  
 Export filtered text view

OK Cancel

File Name: Jim\_shu's[2].pst-Personal Folders-Top... Original Path: D:\SCYT\CF\Email\jimshuemail\Export\

Destination Path: D:\SCYT\CF\Email\jimshuemail\Export\

Prepend archive name to file name  
 Append item number to file name to guarantee uniqueness  
 Append appropriate extension to file name if bad/absent

OK

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

New Sort View ...

This PC > New Volume (D:) > SCYT > CF > Email > jimshuemail > Export

Name	Date modified	Type	Size
Jim_shu's[2].pst--Personal Folders--Top ...	08-12-2006 05:09	File	4 KB

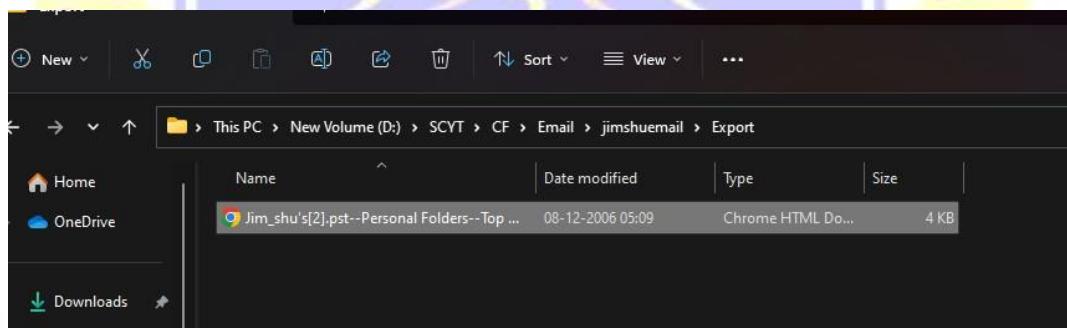
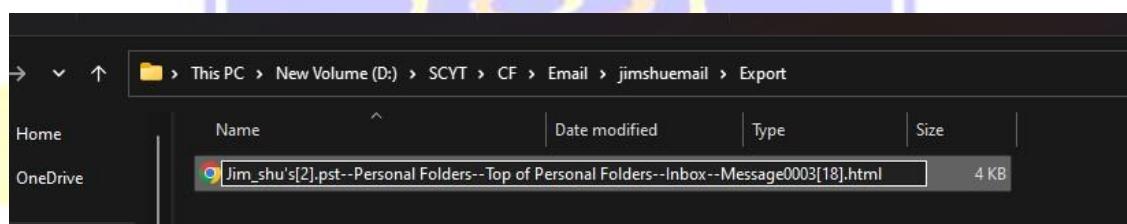
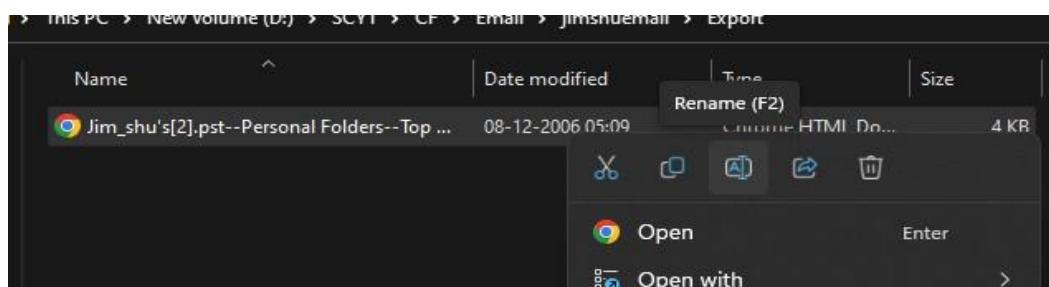


# SHRI G.P.M. DEGREE COLLEGE

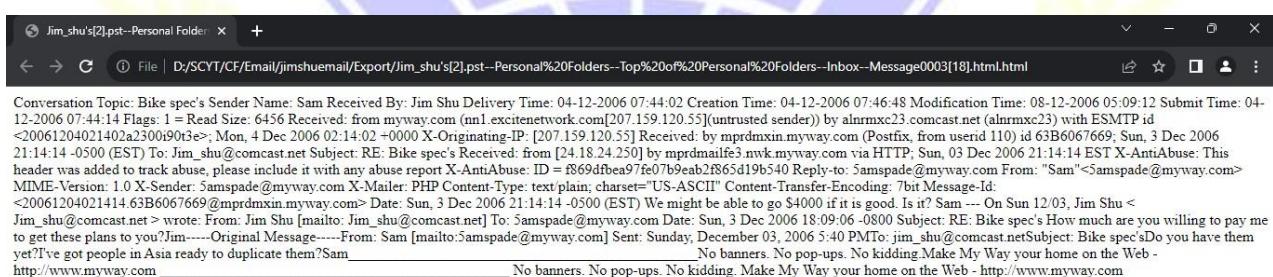
Department of Computer

Vision.. Innovation.. Solution.. Presentation

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



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



**Result:**

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

**Learning Outcomes:**

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

**Course Outcomes:**

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

**Conclusion:****Viva Questions:**

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



## PRACTICAL NO: 10

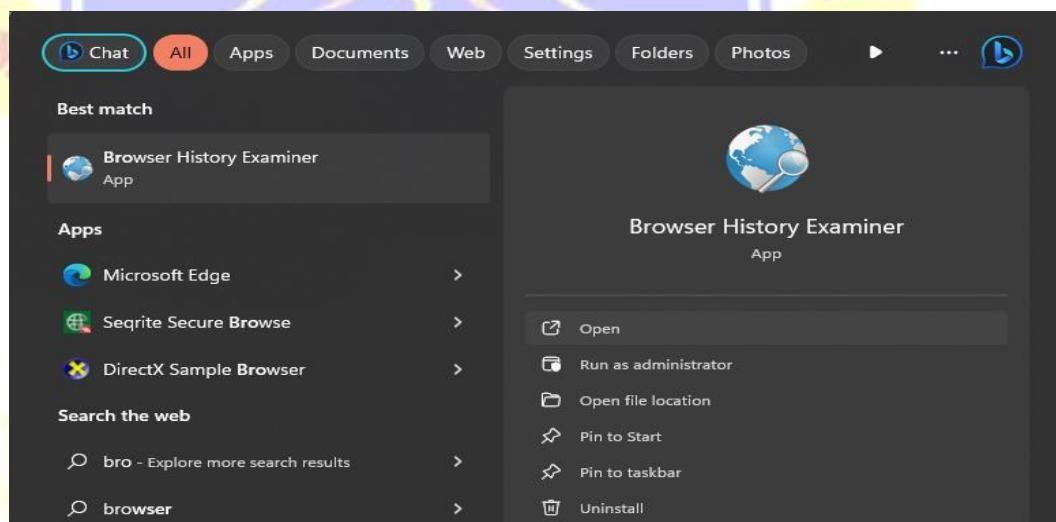
### Aim:

Web Browser Forensics

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

### Practical:

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



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



Click on Continue Trail



# SHRI G.P.M. DEGREE COLLEGE

Department of Computer

Vision.. Innovation.. Solution.. Presentation

Click OK

The screenshot shows the 'Browser History Examiner - Trial Mode' application window. The menu bar includes File, Options, Filter, Report, Tools, and Help. The 'File' menu is open, showing options like Load History, Capture History (which is highlighted with a red box), Report, Export, and Exit. The main pane displays a table of website visits with columns: Date Visited, Title, URL, Visit Type, Visit Source, Visit Count, URL Record Count, Visited Frc, and Web Browser. A toolbar above the table includes buttons for Date Visited, Title, URL, Visit Type, Visit Source, Visit Count, URL Record Count, Visited Frc, and Web Browser. To the right of the table are several filter panels: 'Filter by keyword' (with a text input field and an 'Advanced' button), 'Filter by date' (with 'From' and 'To' dropdowns), 'Filter by time' (with 'From' and 'To' dropdowns), and 'Filter by web browser' (with a dropdown set to 'All'). A status bar at the bottom indicates 'www.foxtonforensics.com'.

This is the Interface of the Application

Go to File → Capture History

This screenshot is identical to the one above, showing the 'Browser History Examiner - Trial Mode' application window. The 'File' menu is open, and the 'Capture History' option is highlighted with a red box. The rest of the interface, including the table of website visits and filter panels, remains the same.

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



## SHRI G.P.M. DEGREE COLLEGE

Department of Computer

Vision.. Innovation.. Solution.. Presentation

Browser History Examiner - Capture History

Capture history from this computer  
 Capture history from external drive  
 Capture history from a remote computer

Computer Name / IP Address	<input type="text"/>
Admin Username	<input type="text"/>
Admin Password	<input type="password"/>
Admin Share	<input type="text"/> admin\$

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

Browser History Examiner - Capture History

User Profile:

Browsers:  Firefox  Chrome  Internet Explorer & Edge

Data:  History  Cache  Archived History

Destination:

Browser History Examiner

Capture complete. Would you like to load the captured history now?



# SHRI G.P.M. DEGREE COLLEGE

Department of Computer

Vision.. Innovation.. Solution.. Presentation

Here we can see the websites visited

The screenshot shows the 'Website Visits' tab of the Browser History Examiner. The main table lists 21 records of website visits. A summary chart titled 'Website Visit Count - 14-12-2022 to 23-08-2023' shows the count of visits per month, with a significant peak 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	https://ww	Typed		1	1	https://ww	Edge
23-08-2023 03:57:07	Welcome t	https://ww	Typed		1	1	https://ww	Edge
23-08-2023 03:57:07	Welcome t	https://ww	Typed		2	2	https://ww	Edge
23-08-2023 03:57:07	Welcome t	https://go.	Typed		2	2	https://ww	Edge
23-08-2023 03:57:07	Welcome t	https://ww	Typed		2	2	https://ww	Edge
23-08-2023 03:57:07	Welcome t	https://go.	Typed		2	2	https://ww	Edge
23-08-2023 03:57:02	C-Free Uni	http://www	Other		1	1		Edge
22-08-2023 08:35:48		https://log				1		Internet Explorer
22-08-2023 08:35:48	Sign in to	https://log	Link	Imported	1	1		Edge
22-08-2023 08:35:41		mi-pbl/p				1		Internet Explorer
22-07-2023 07:30:28	visual stud	https://ww	Link		1	1		Chrome
22-07-2023 07:30:24	visual stud	https://ww	Link		2	2		Chrome

Here we can see the bookmarks

The screenshot shows the 'Bookmarks' tab of the Browser History Examiner. It displays a single record for a bookmark named 'Bing' with the URL 'http://go.microsoft.com/fwlink/p/?Link1'. The interface includes various filtering options on the right side.

Date Added	Last Modified	Title	URL	Web Browser
		Bing	http://go.microsoft.com/fwlink/p/?Link1	Internet Explorer

Here we can see the browser settings

The screenshot shows the 'Browser Settings' tab of the Browser History Examiner. It lists 8 settings, all of which are set to 'Yes' except for 'Sync Tabs' which is 'No'. The interface includes various filtering options on the right side.

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



# SHRI G.P.M. DEGREE COLLEGE

## Department of Computer

Vision.. Innovation.. Solution.. Presentation

Here we can see the cached files

The screenshot shows the 'Browser History Examiner - Trial Mode' interface. The 'Cached Files' tab is selected in the left sidebar. The main pane displays a table of cached files with columns: Last Fetched, Content Type, URL, Fetch Count, File Size (Bytes), and Web Browser. All entries are for Internet Explorer. A yellow box highlights the 'Cached Files' tab in the sidebar.

Artefact	Records
Bookmarks	1
Browser Settings	8
<b>Cached Files</b>	<b>9</b>
Cached Images	7
Cached Web Pages	1
Cookies	23
Downloads	0
Email Addresses	2
Favicons	10
Form History	0

Last Fetched	Content Type	URL	Fetch Count	File Size (Bytes)	Web Browser
1	application/x-javascript	https://aadcdn.msftauth.net/shared/1.0/co	1	423350	Internet Explorer
	text/css	https://aadcdn.msftauth.net/ests/2.1/cont	1	111100	Internet Explorer
	application/x-javascript	https://aadcdn.msftauth.net/shared/1.0/co	1	110048	Internet Explorer
	application/x-javascript	https://aadcdn.msftauth.net/ests/2.1/cont	1	49972	Internet Explorer
	application/x-javascript	https://aadcdn.msftauth.net/ests/1.0/co	1	24820	Internet Explorer
	application/octet-stream	https://az67904.vo.msecnd.net/pub/Defa	3	19161	Internet Explorer
	application/octet-stream	https://az700632.vo.msecnd.net/pub/Remi	1	1683	Internet Explorer
	application/octet-stream	https://az700632.vo.msecnd.net/pub/Figh	1	205	Internet Explorer
	application/octet-stream	https://az700632.vo.msecnd.net/pub/Figh	2	78	Internet Explorer

Here we can see the cached images

The screenshot shows the 'Browser History Examiner - Trial Mode' interface. The 'Cached Images' tab is selected in the left sidebar. The main pane displays a table of cached images with columns: Last Fetched, Content Type, URL, Fetch Count, File Size (Bytes), and Web Browser. All entries are for Internet Explorer. A yellow box highlights the 'Cached Images' tab in the sidebar.

Artefact	Records
Bookmarks	1
Browser Settings	8
<b>Cached Files</b>	<b>9</b>
<b>Cached Images</b>	<b>7</b>
Cached Web Pages	1
Cookies	23
Downloads	0
Email Addresses	2
Favicons	10
Form History	0
Logins	0
Searches	19
Session Tabs	0
Thumbnails	3
Website Visits	21

Last Fetched	Content Type	URL	Fetch Count	File Size (Bytes)	Web Browser
1	image/svg+xml	https://aadcdn.msftauth.net/shared/1.0/content/	1	3651	Internet Explorer
	image/gif	https://aadcdn.msftauth.net/shared/1.0/content/	1	3620	Internet Explorer
	image/gif	https://aadcdn.msftauth.net/shared/1.0/content/	1	2672	Internet Explorer
	image/svg+xml	https://aadcdn.msftauth.net/shared/1.0/content/	1	1864	Internet Explorer
	image/svg+xml	https://aadcdn.msftauth.net/shared/1.0/content/	1	1378	Internet Explorer
	image/svg+xml	https://aadcdn.msftauth.net/shared/1.0/content/	1	899	Internet Explorer
	image/svg+xml	https://aadcdn.msftauth.net/shared/1.0/content/	1	222	Internet Explorer

Here we can see the cached webpages

The screenshot shows the 'Browser History Examiner - Trial Mode' interface. The 'Cached Web Pages' tab is selected in the left sidebar. The main pane displays a table of cached web pages with columns: Last Fetched, URL, Fetch Count, File Size (Bytes), and Web Browser. One entry is for Internet Explorer. A yellow box highlights the 'Cached Web Pages' tab in the sidebar.

Artefact	Records
Bookmarks	1
Browser Settings	8
<b>Cached Files</b>	<b>9</b>
Cached Images	7
<b>Cached Web Pages</b>	<b>1</b>
Cookies	23
Downloads	0
Email Addresses	2
Favicons	10
Form History	0
Logins	0
Searches	19

Last Fetched	URL	Fetch Count	File Size (Bytes)	Web Browser
	https://login.live.com/Me.htm?v=3	1	2347	Internet Explorer



# SHRI G.P.M. DEGREE COLLEGE

Department of Computer

Vision.. Innovation.. Solution.. Presentation

Here we can see the cookies stored

Browser History Examiner - Trial Mode

Artefact	Records	Cookies	Report Preview
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		
Thumbnail	3		
Website Visits	21		

Date Created URL Last Accessed Date Expires Name Content Web Browser

msn.com/	22-07-2023 05:11:01	15-08-2024 05:11:02	MUID	392592F187B26B	Edge
g.msn.com/	22-07-2023 05:11:01	29-07-2023 05:11:02	MR	0	Edge
live.com/	22-07-2023 05:10:41	15-08-2024 05:10:42	MUID	2F13847EF5E36B	Edge
bing.com/	06-01-2023 10:34:56	31-01-2024 10:34:57	MUID	09DB3FCFAFEA67	Edge
www.bing.com/	22-07-2023 05:46:32	15-08-2024 05:46:32	MUIDB	09DB3FCFAFEA67	Edge
bing.com/	06-01-2023 10:34:56	31-01-2024 10:34:57	_EDGE_V	1	Edge
bing.com/	06-01-2023 10:34:56	06-01-2025 10:34:57	SRCHD	AF=NOFORM	Edge
bing.com/	06-01-2023 10:34:56	06-01-2025 10:34:57	SRCHUID	V=2&GUID=FE30	Edge
bing.com/	06-01-2023 10:34:56	06-01-2025 10:34:57	SRCHUSR	DOB=20230106	Edge
bing.com/	22-07-2023 05:46:32	22-07-2025 05:46:32	SRCHHPGUSR	SRCHLANG=en&	Edge
bing.com/	22-07-2023 05:39:48	22-07-2023 17:39:48	SUID	M	Edge
login.microsofton	22-08-2023 08:35:48	21-09-2023 08:35:49	buid	0AVAYAMe_N-B6j	Edge
login.microsofton	22-08-2023 08:35:53	21-09-2023 08:35:53	fpc	Au164KFROIAIMP	Edge
login.microsofton	22-08-2023 08:35:48	15-09-2024 08:35:48	brcap	0	Edge
www.bing.com/	22-07-2023 07:31:12	15-08-2024 07:31:13	MUIDB	02B7C9F658384A	Edge
bing.com/	14-12-2022 09:46:56	14-12-2024 09:46:57	SRCHUID	V=2&GUID=5D8:	Edge
bing.com/	14-12-2022 09:46:56	14-12-2023 09:46:57	CortanaAppUID	6E148F4EAC1031	Edge
bing.com/	14-12-2022 09:46:56	14-12-2024 09:46:57	SRCHD	AF=NOFORM	Edge
bing.com/	14-12-2022 09:46:56	14-12-2024 09:46:57	SRCHUSR	DOB=20221214	Edge
bing.com/	22-07-2023 07:31:15	15-08-2024 07:31:15	SRCHHPGUSR	SRCHLANG=en&	Edge
bing.com/	14-12-2022 09:47:11	14-12-2024 09:47:12	ANON	A=2C7B78C7DDA	Edge
bing.com/	22-07-2023 05:10:35	22-07-2023 17:10:36	SUID	A	Edge
login.microsofton	22-07-2023 07:12:26	21-08-2023 07:12:27	fpc	AuHsj6tZyQ1LmN	Edge

Filter by keyword \_\_\_\_\_

Filter by date  
From: \_\_\_\_\_ To: \_\_\_\_\_

Filter by time  
From: \_\_\_\_\_ To: \_\_\_\_\_

Filter by web browser  
All

Here we can see the emails used for logins

Browser History Examiner - Trial Mode

Artefact	Records	Email Addresses	Report Preview
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		

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

Filter by keyword \_\_\_\_\_

Filter by date  
From: \_\_\_\_\_ To: \_\_\_\_\_

Filter by time \_\_\_\_\_

Here we can see the favicons



# SHRI G.P.M. DEGREE COLLEGE

## Department of Computer

Vision.. Innovation.. Solution.. Presentation

Browser History Examiner - Trial Mode

File Options Filter Report Tools Help

Artefact	Records	Favicons	Report Preview
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		
Website Visits	21		

Filter by keyword  Advanced

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

Filter by time From: Select a time  To: Select a time

Here we can see the searches

Browser History Examiner - Trial Mode

File Options Filter Report Tools Help

Artefact	Records	Searches	Report Preview
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		
Website Visits	21		

Viewing 19/19 records    of 1 pages   Page size

Filter by keyword  Advanced

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

Filter by time From: Select a time  To: Select a time

Filter by web browser All

Here we see the thumbnails



# SHRI G.P.M. DEGREE COLLEGE

## Department of Computer

Vision.. Innovation.. Solution.. Presentation

Browser History Examiner - Trial Mode

File Options Filter Report Tools Help

Artefact	Records
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
Website Visits	21

URL Title Filename Last Updated Web Browser

https://chrome.google.com/webst	Web Store			Chrome
https://www.office.com/	Office			Edge
https://go.microsoft.com/fwlink/?!	Welcome to Microsoft Edge			Edge

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

Filter by keyword  
Advanced

Filter by date  
From: Select a date [15] To: Select a date [15]

Filter by time  
From: Select a time [ ] To: Select a time [ ]

Filter by web browser  
All

Here we can see the websites visits

Browser History Examiner - Trial Mode

File Options Filter Report Tools Help

Artefact	Records
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
Website Visits	21

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	https://ww	Typed		1	1	https://ww	Edge
23-08-2023 03:57:07	Welcome t	https://ww	Typed		1	1	https://ww	Edge
23-08-2023 03:57:07	Welcome t	https://ww	Typed		2	2	https://go	Edge
23-08-2023 03:57:07	Welcome t	https://go	Typed		2	2	https://ww	Edge
23-08-2023 03:57:07	Welcome t	https://ww	Typed		2	2	https://go	Edge
23-08-2023 03:57:07	Welcome t	https://go	Typed		2	2		Edge
23-08-2023 03:57:02	C-Free Uni	http://www	Other		1	1		Edge
22-08-2023 08:35:48	https://log					1		Internet Explorer
22-08-2023 08:35:48	Sign in to s	https://log	Link	Imported	1	1		Edge
22-08-2023 08:35:41	ms-pbi://p					1		Internet Explorer
G 22-07-2023 07:30:28	visual stud	https://ww	Link		1	1		Chrome
G 22-07-2023 07:30:24	visual stud	https://ww	Link		2	2		Chrome

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

Detailed View Summary View

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

Filter by keyword  
Advanced

Filter by date  
From: Select a date [15] To: Select a date [15]

Filter by time  
From: Select a time [ ] To: Select a time [ ]

Filter by web browser  
All

Filter by visit type  
All

**Result:**

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

**Learning Outcomes:**

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

**Course Outcomes:**

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

**Conclusion:****Viva Questions:**

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