

CYBER FORENSICS PRACTICALS

INDEX

Practical No	Topic	Date	Page No	Remark
1	Creating a Forensic Image using FTK Imager: - Creating Forensic Image - Check Integrity of Data - Analyze Forensic Image	06-12-2021	3-9	
2	Data Acquisition: - Perform data acquisition using write blocker	06-12-2021	10-14	
3	Forensics Case Study: - Solve the Case study (image file) provide in lab using Autopsy	13-12-2021	15-21	
4	Capturing and analyzing network packets using Wireshark (Fundamentals): - Identification the live network - Capture Packets - Analyze the captured packets	03-01-2022	22-27	
5	Analyze the packets provided in lab and solve the questions using Wireshark : - What web server software is used by www.snopes.com ? - About what cell phone problem is the client concerned? - How many web servers are running Apache? - What hosts (IP addresses) think that jokes are more entertaining when they are explained?	10-01-2022	28-35	
6	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	17-01-2022	36-42	
7	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 access data and also Perform manually through command line	31-01-2022	43-54	

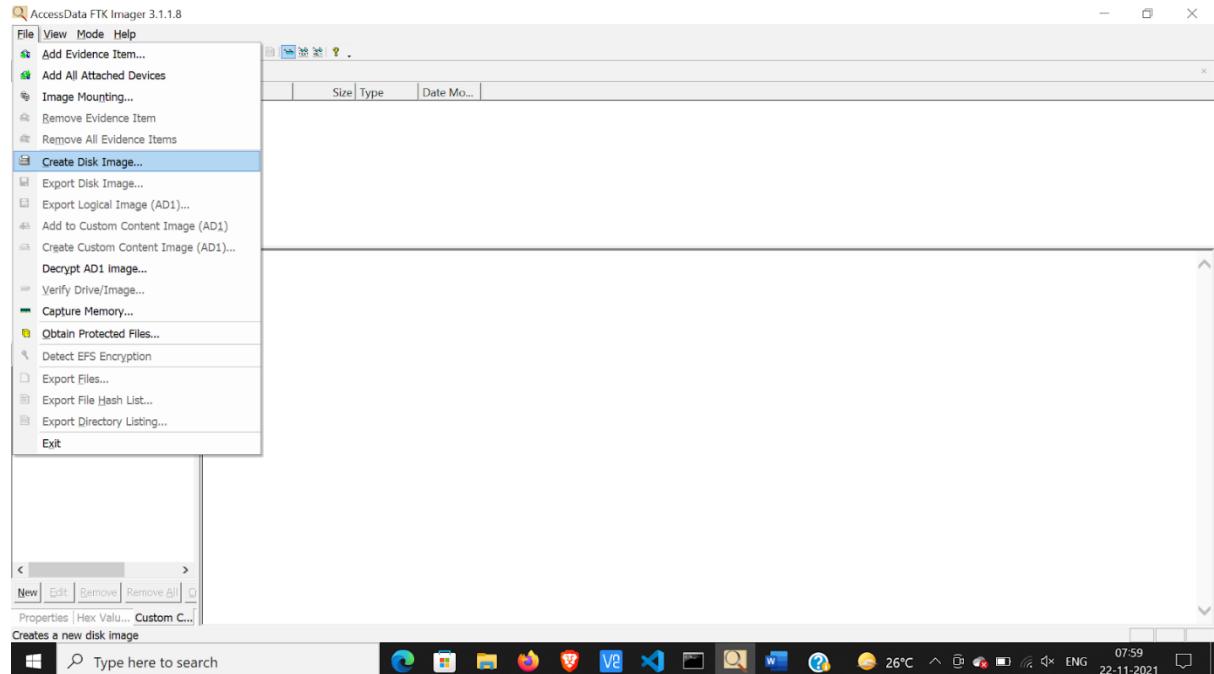
CYBER FORENSICS PRACTICALS

8	Acquisition of Cell phones and Mobile devices	21-02-2022	55-61	
9	Email Forensics - Mail Service Providers - Email protocols - Recovering emails - Analyzing email header	25-02-2022	62-71	
10	Web Browser Forensics - Web Browser working - Forensics activities on browser - Cache / Cookies analysis - Last Internet activity	14-02-2022	72-84	

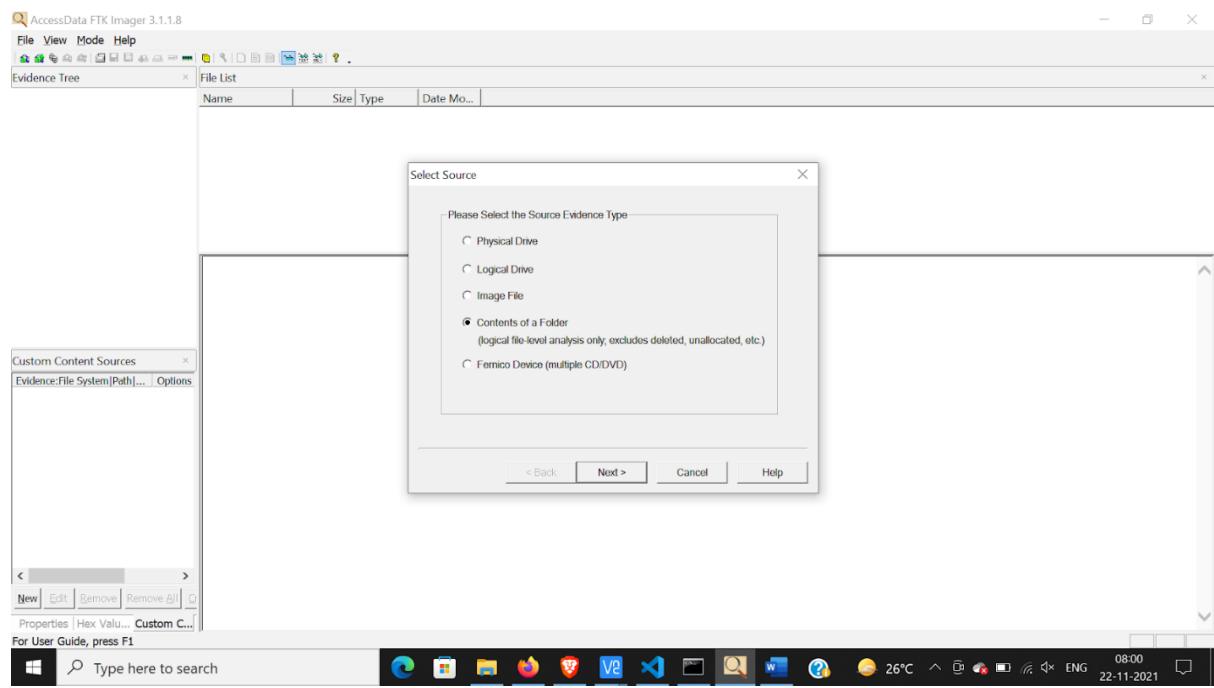
Practical : 1

Aim: Creating a Forensic Image using FTK Imager/Encase Imager:

CREATE A NEW DISK IMAGE

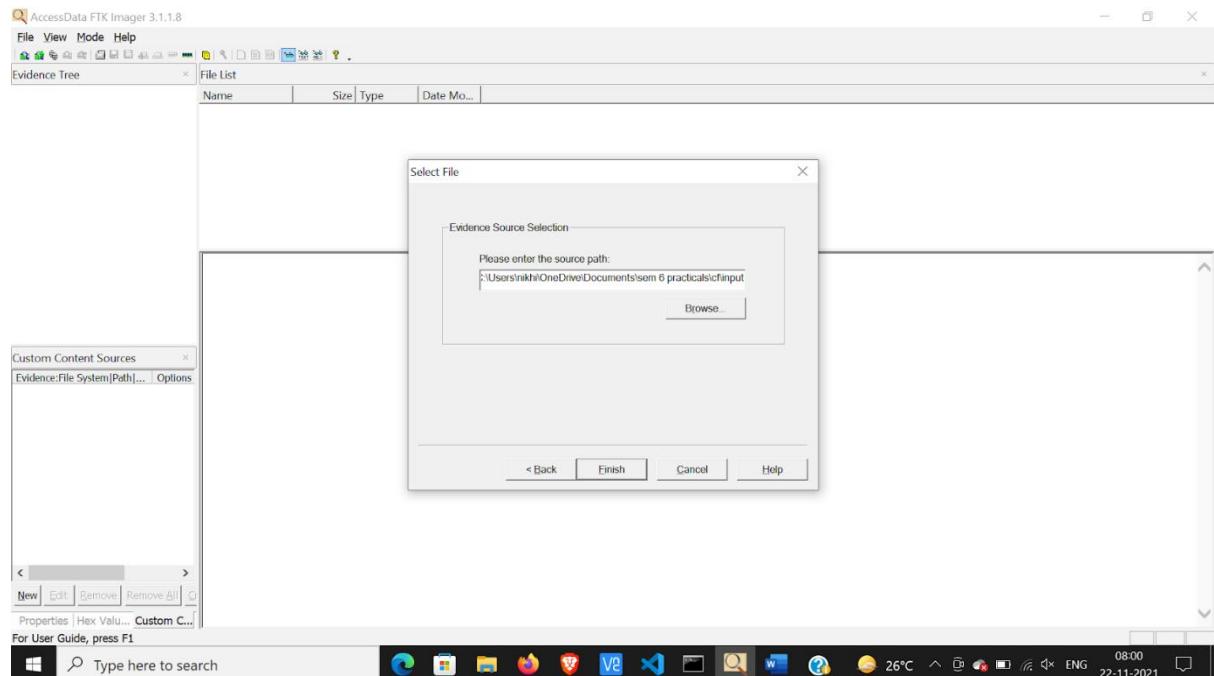


SELECT CONTENTS OF A FOLDER

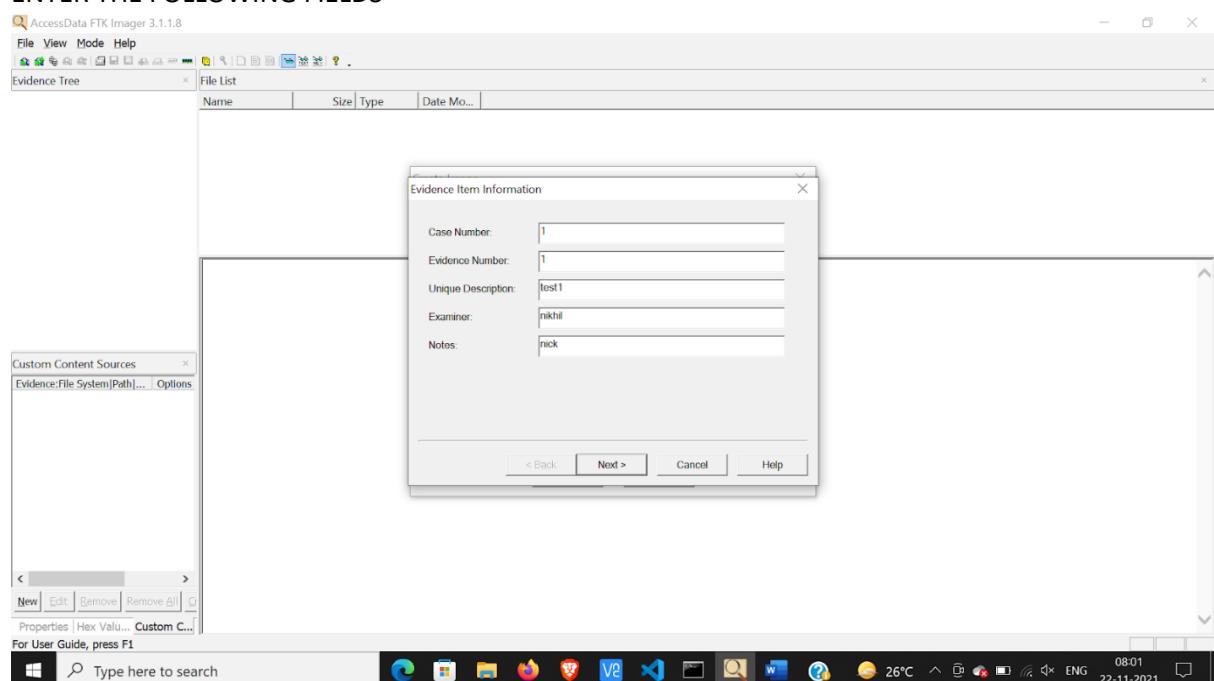


CYBER FORENSICS PRACTICALS

BROWSE THE FOLDER

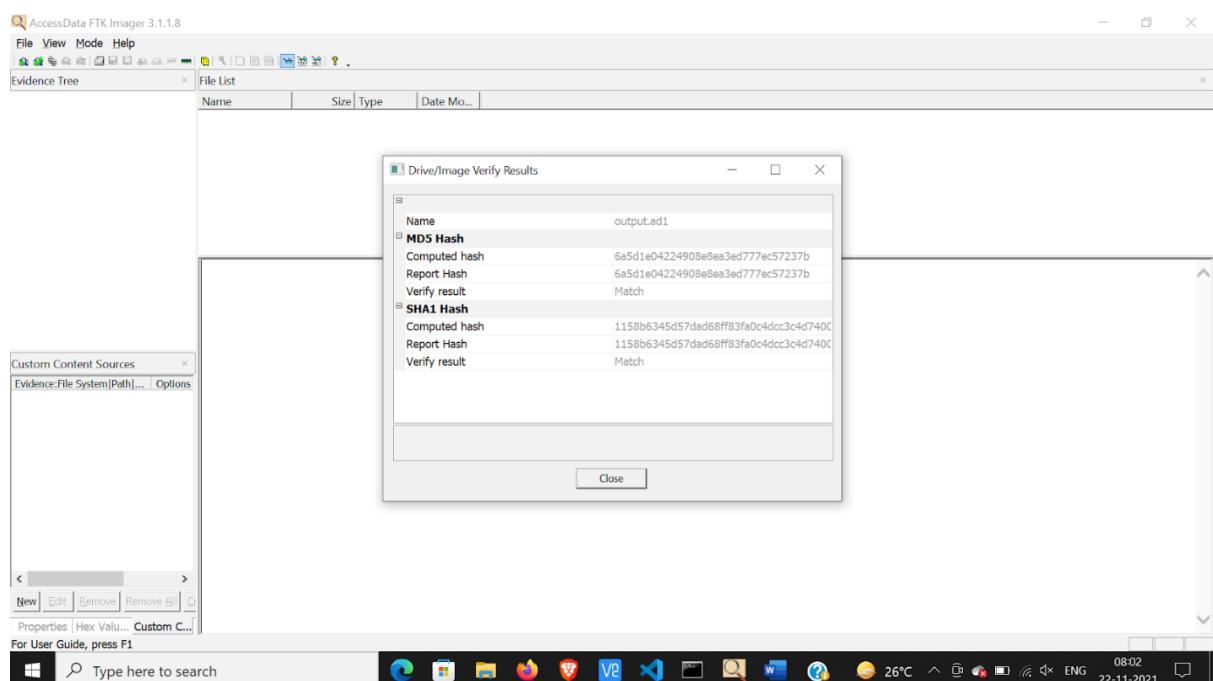
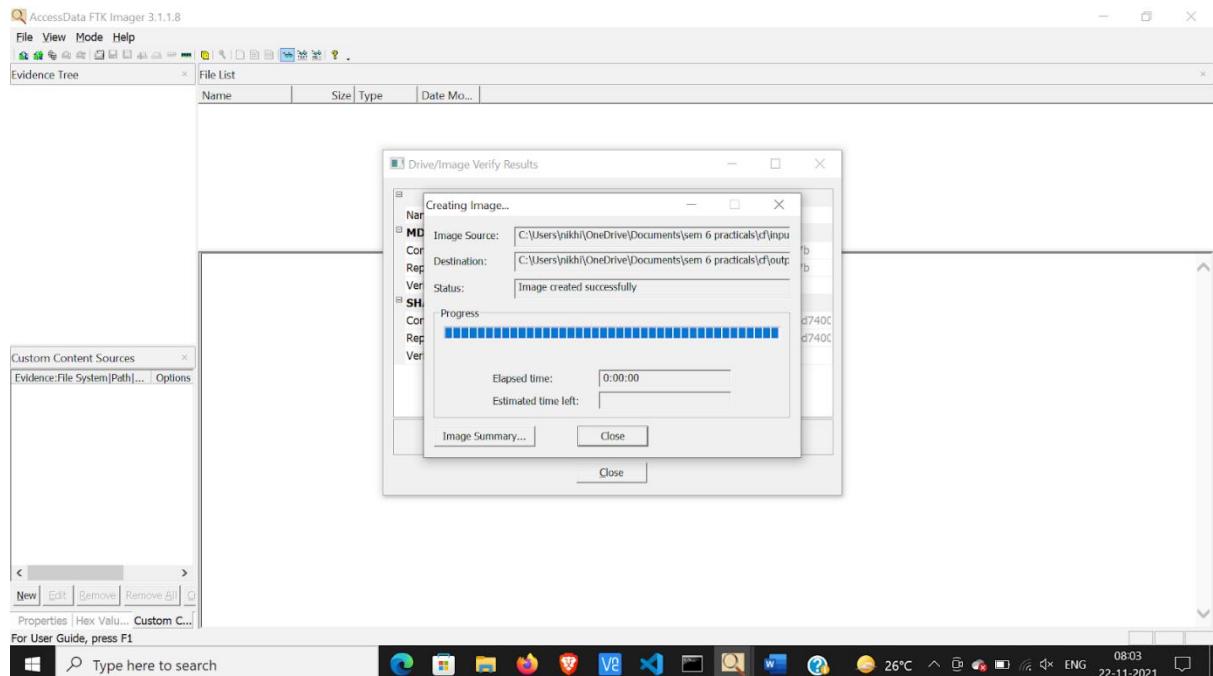


ENTER THE FOLLOWING FIELDS



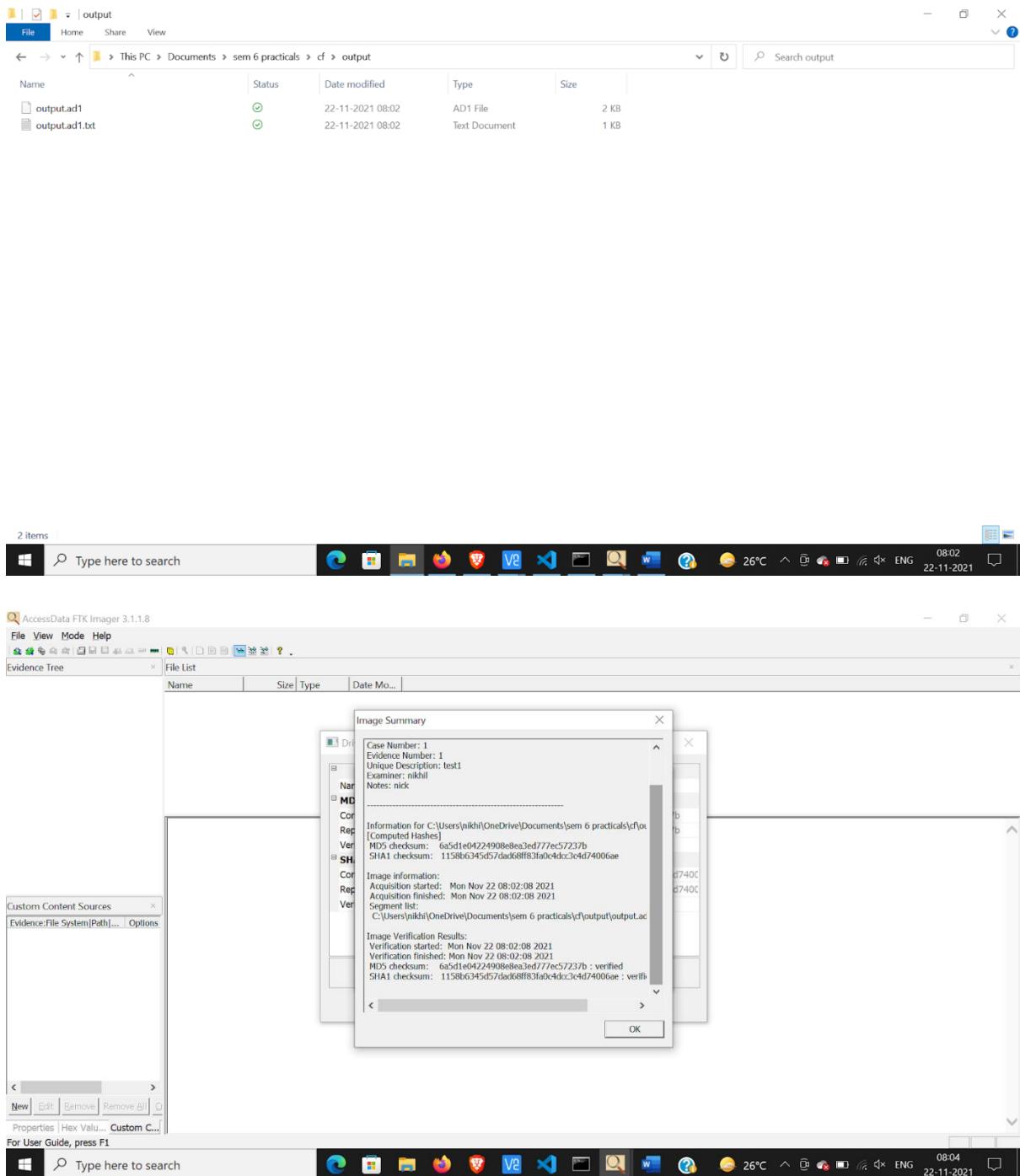
CYBER FORENSICS PRACTICALS

ENTER DESTINATION



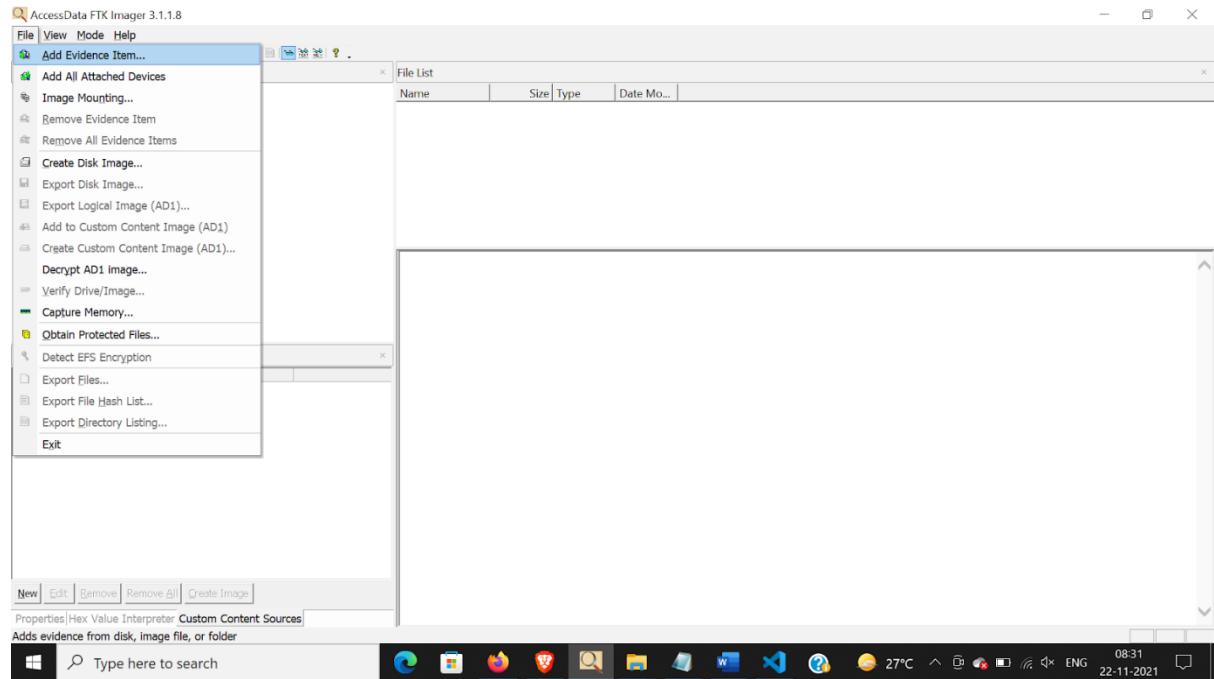
THIS IS HOW THE OUTPUT FILE WILL LOOK LIKE

CYBER FORENSICS PRACTICALS

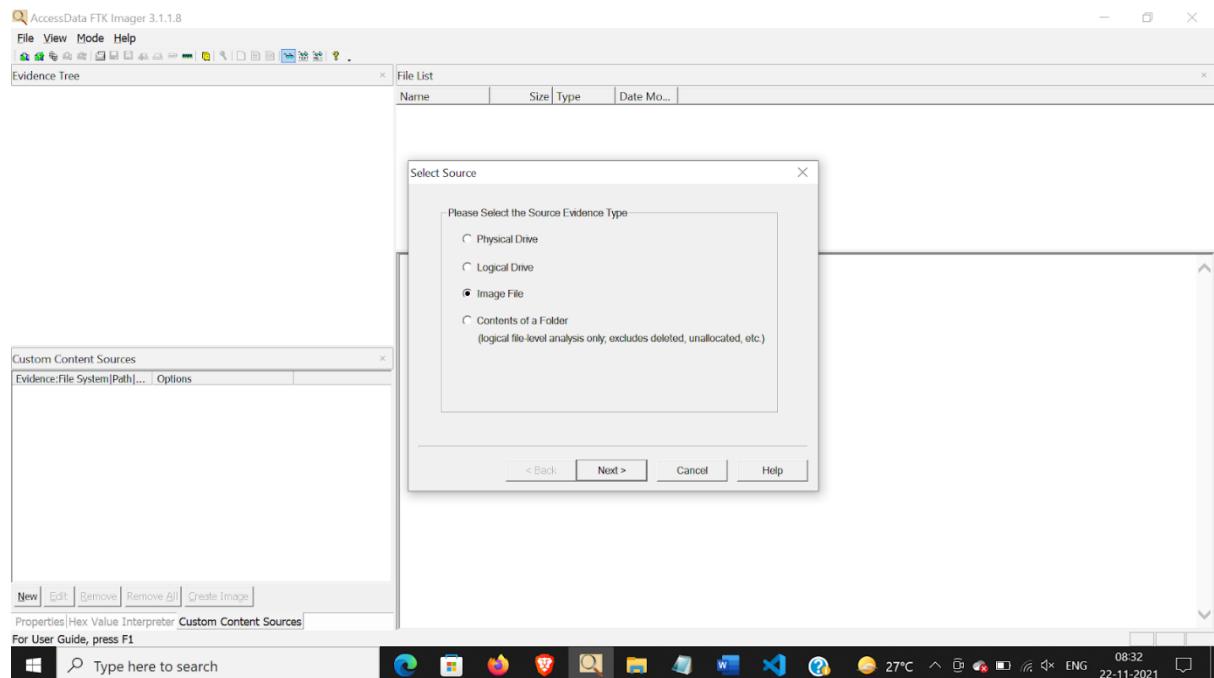


CYBER FORENSICS PRACTICALS

ADD EVIDENCE

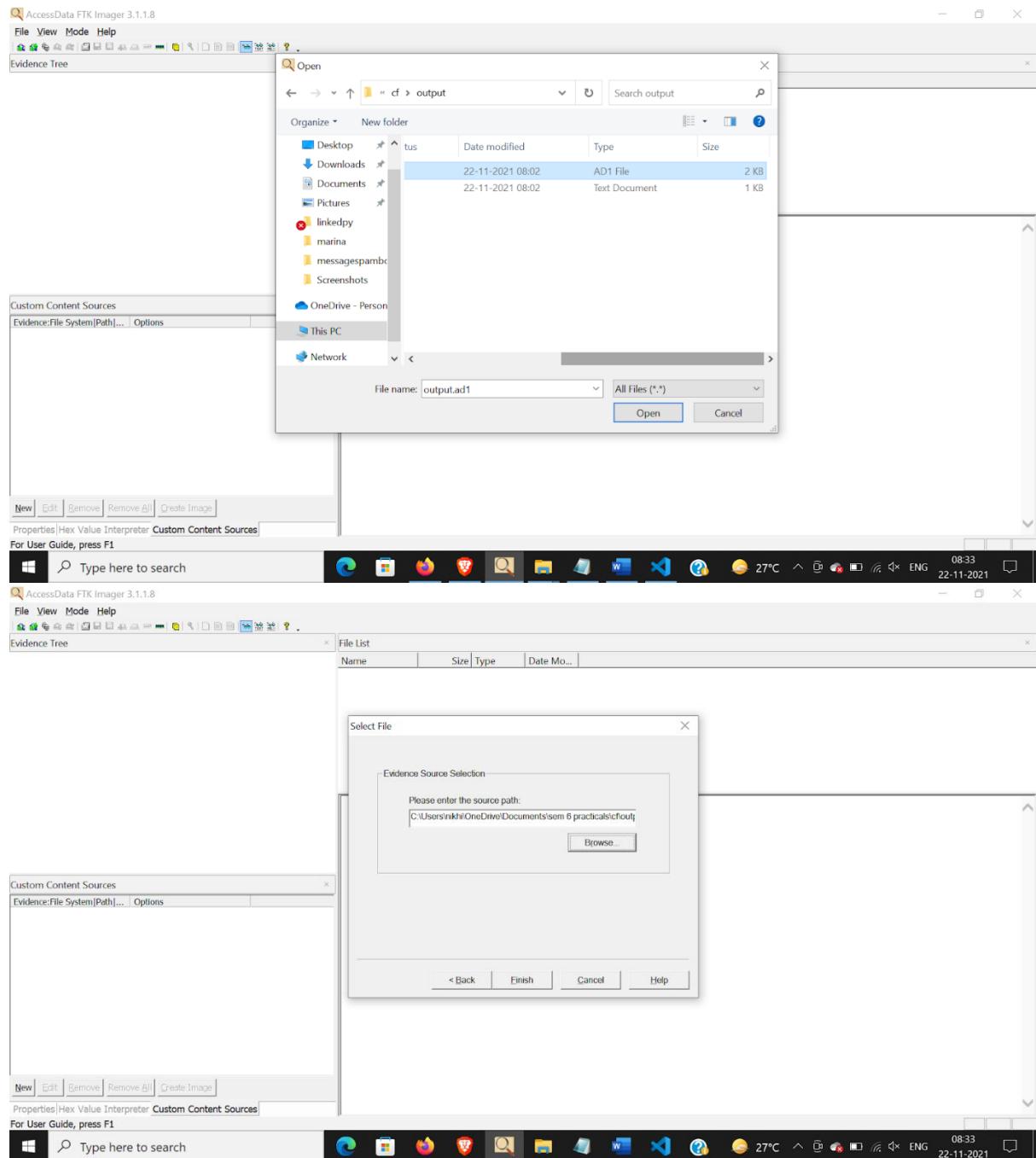


SELECT IMAGE FILE



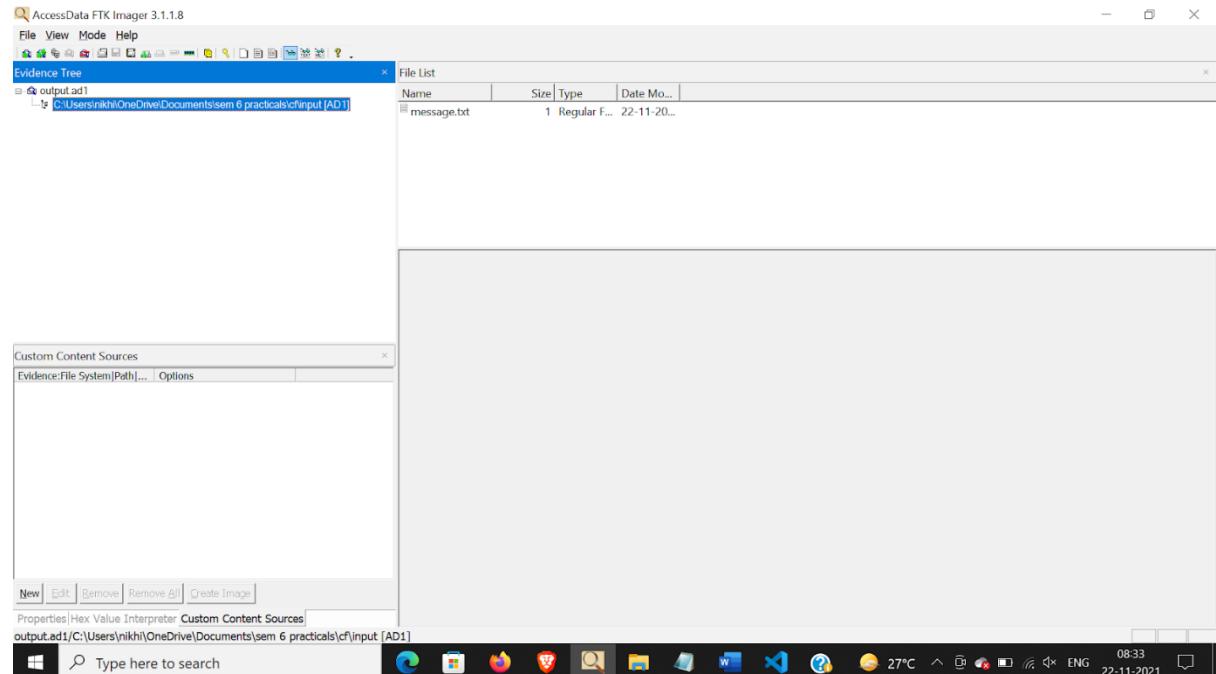
CYBER FORENSICS PRACTICALS

SELECT OUTPUT FILE



CYBER FORENSICS PRACTICALS

YOU CAN SEE THE OUTPUT FILE IN EVIDENCE TREE

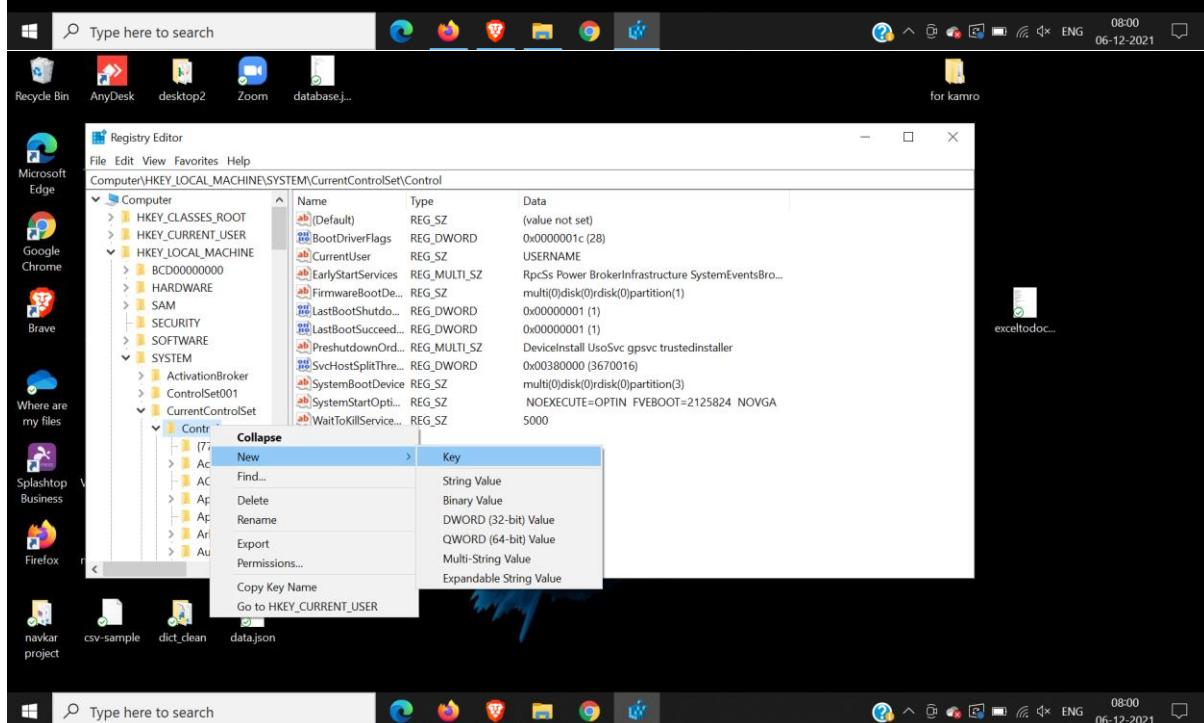
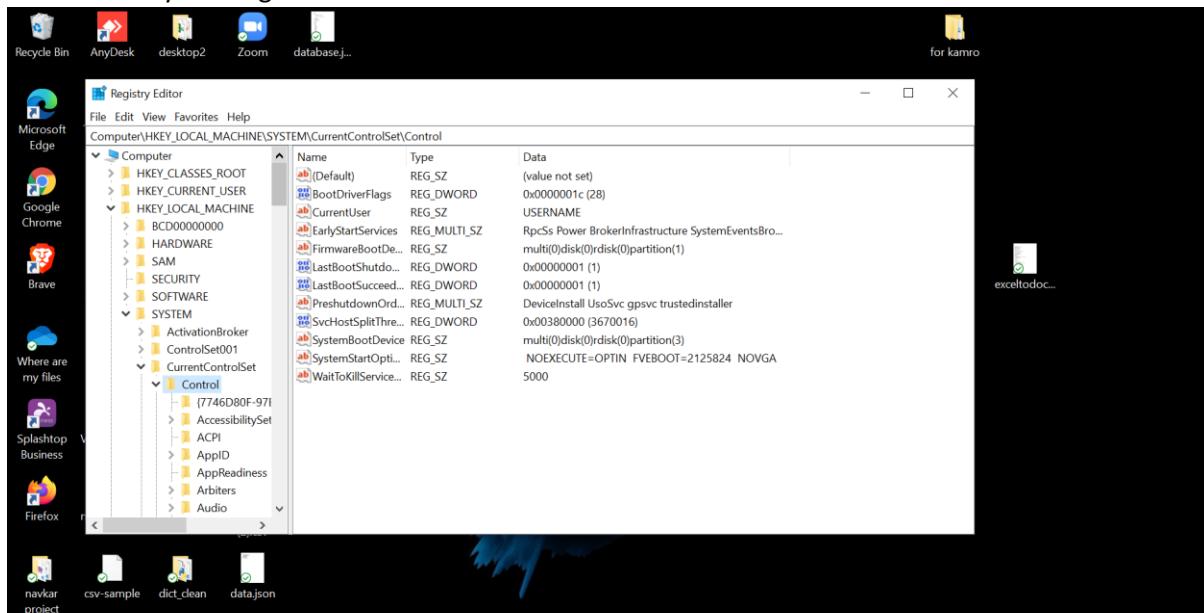


Practical:2

Aim:

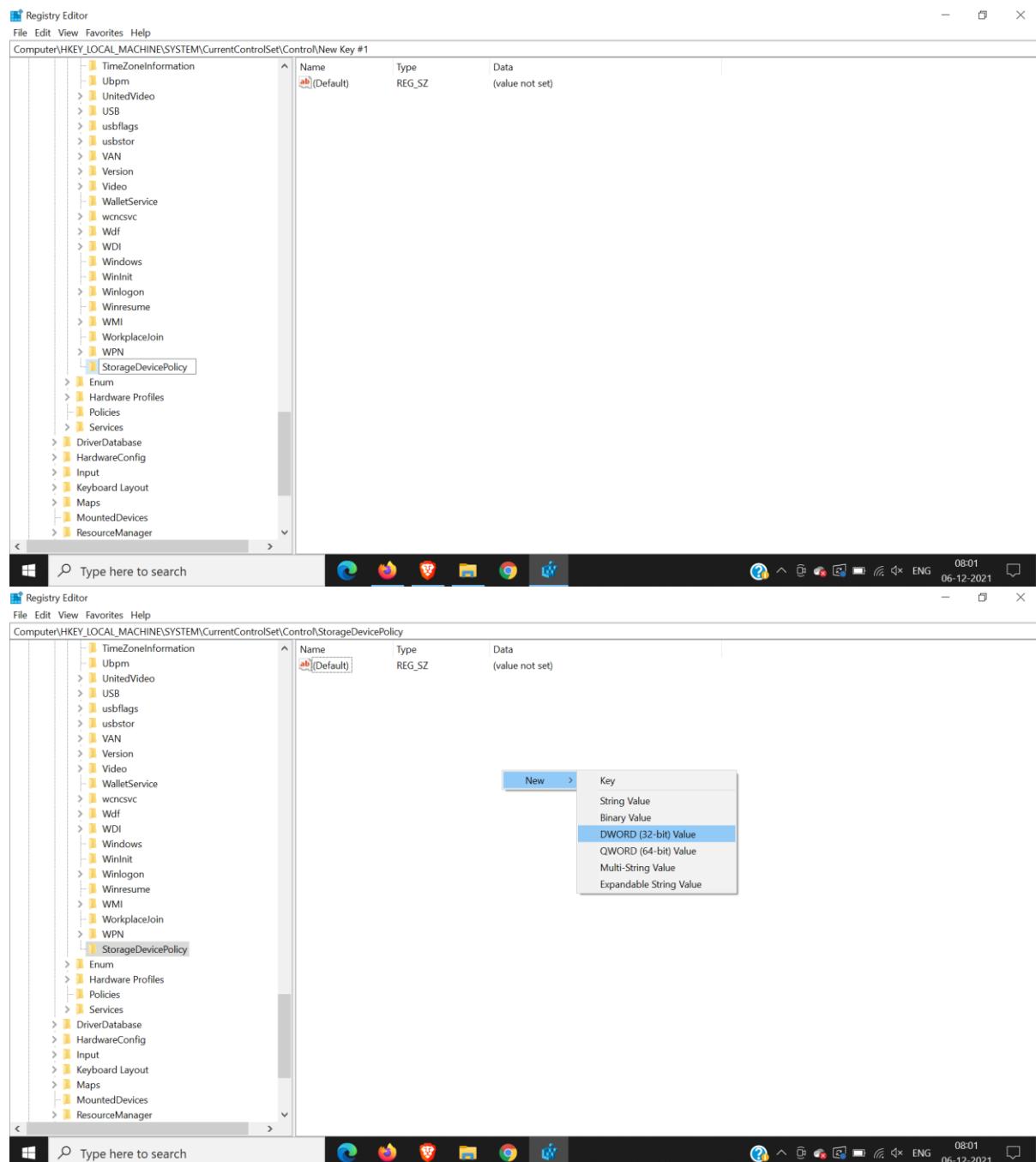
Open win registry editor using run>regedit

Go to Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\ and create new key
Name this key "StorageDevicePolicies"

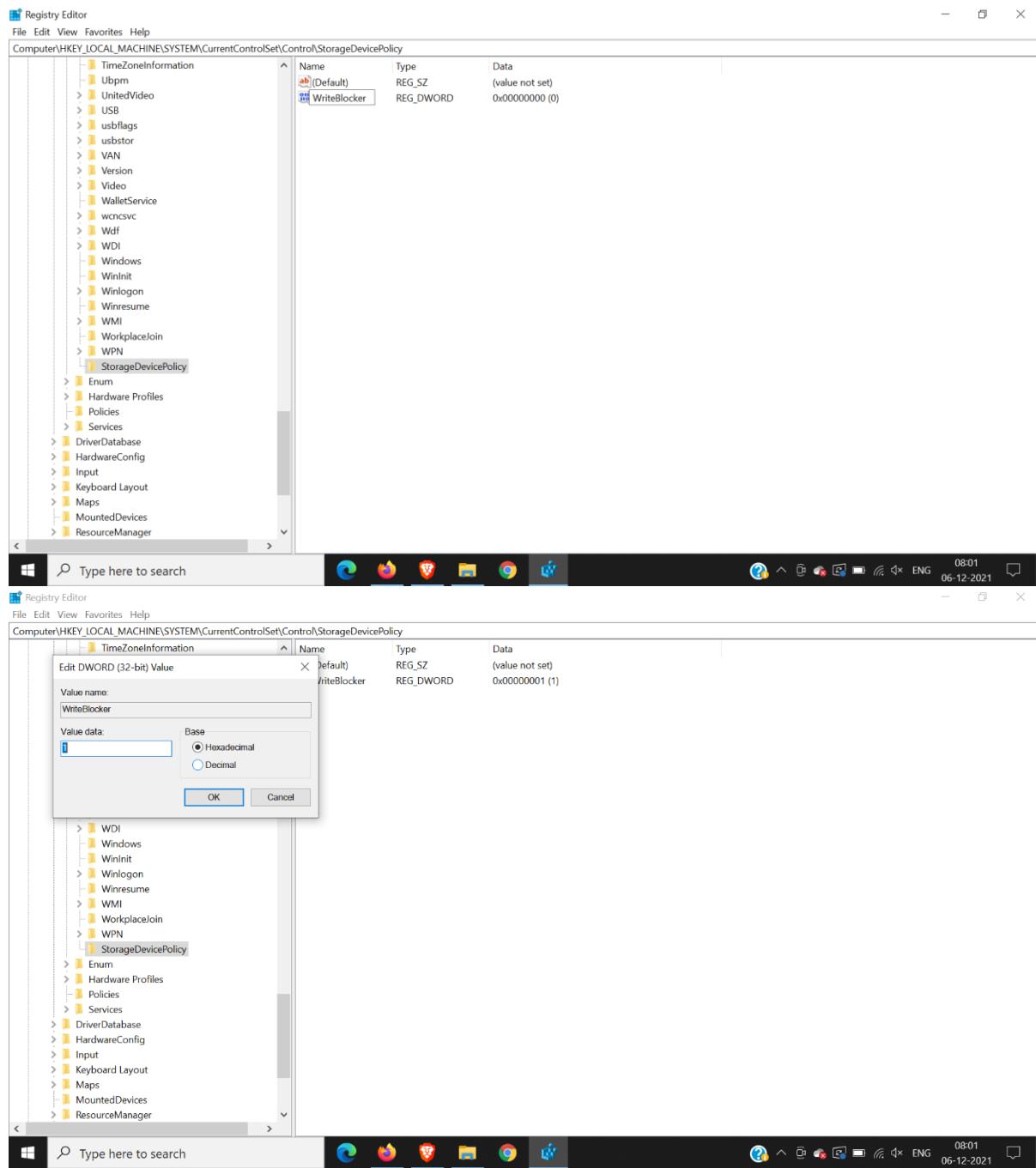


Make New Dword name it “WriteProtect”

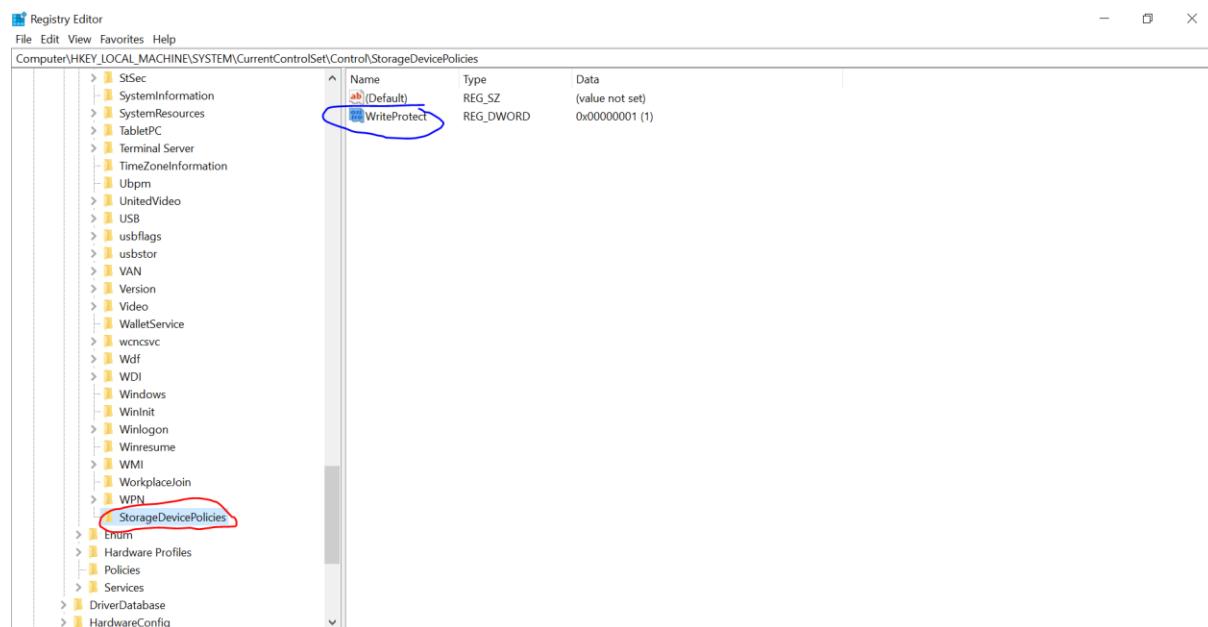
Enter Hexa value as 1



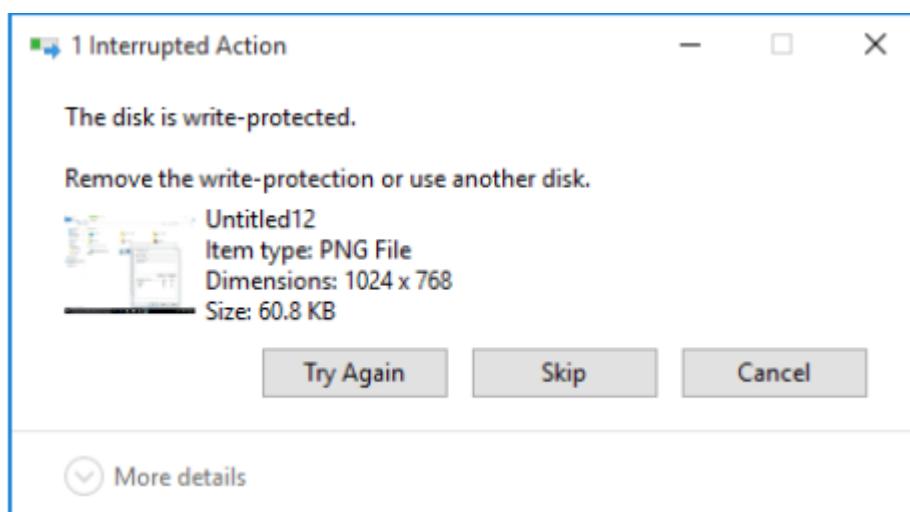
CYBER FORENSICS PRACTICALS



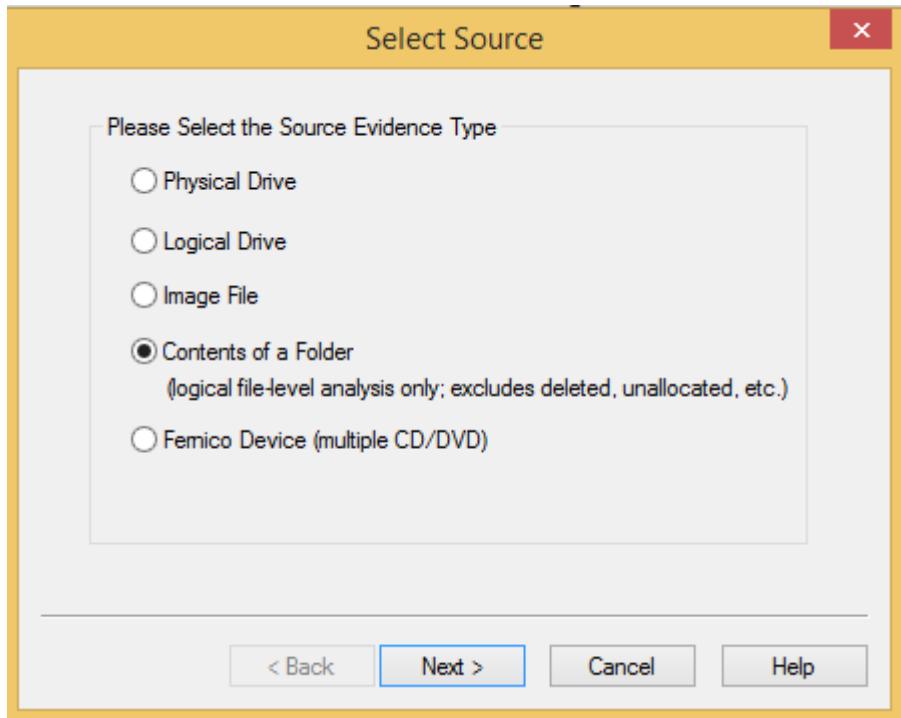
THE SPELLING IS VERY IMPORTANT RENAME IF YOU ENTERED WRONG
“StorageDevicePolicies”
“WriteProtect”



We can only open the file in the USB drive for reading, but it's not allowed to modify and save the changes back to USB drive.



Now Create image of the USB drive using FTK imager



Enter data into the required fields. Select the destination folder.
Image file is created and you can verify it.

Creating Image...

Image Source: \\.\PHYSICALDRIVE1

Destination: F:\sem\output

Status: Creating image...

Progress: [Progress bar]

Elapsed time: 0:18:35

Estimated time left: [empty]

Cancel

Drive/Image Verify Results

Name	case.adl
MDS Hash	70c16462466fe7ed54604ca9fcd0c1e1
Computed hash	70c16462466fe7ed54604ca9fcd0c1e1
Report Hash	70c16462466fe7ed54604ca9fcd0c1e1
Verify result	Match
SHA1 Hash	290a16e3b0b319c1cd1e99006cb6ed1f44
Computed hash	290a16e3b0b319c1cd1e99006cb6ed1f44
Report Hash	290a16e3b0b319c1cd1e99006cb6ed1f44
Verify result	Match

Close

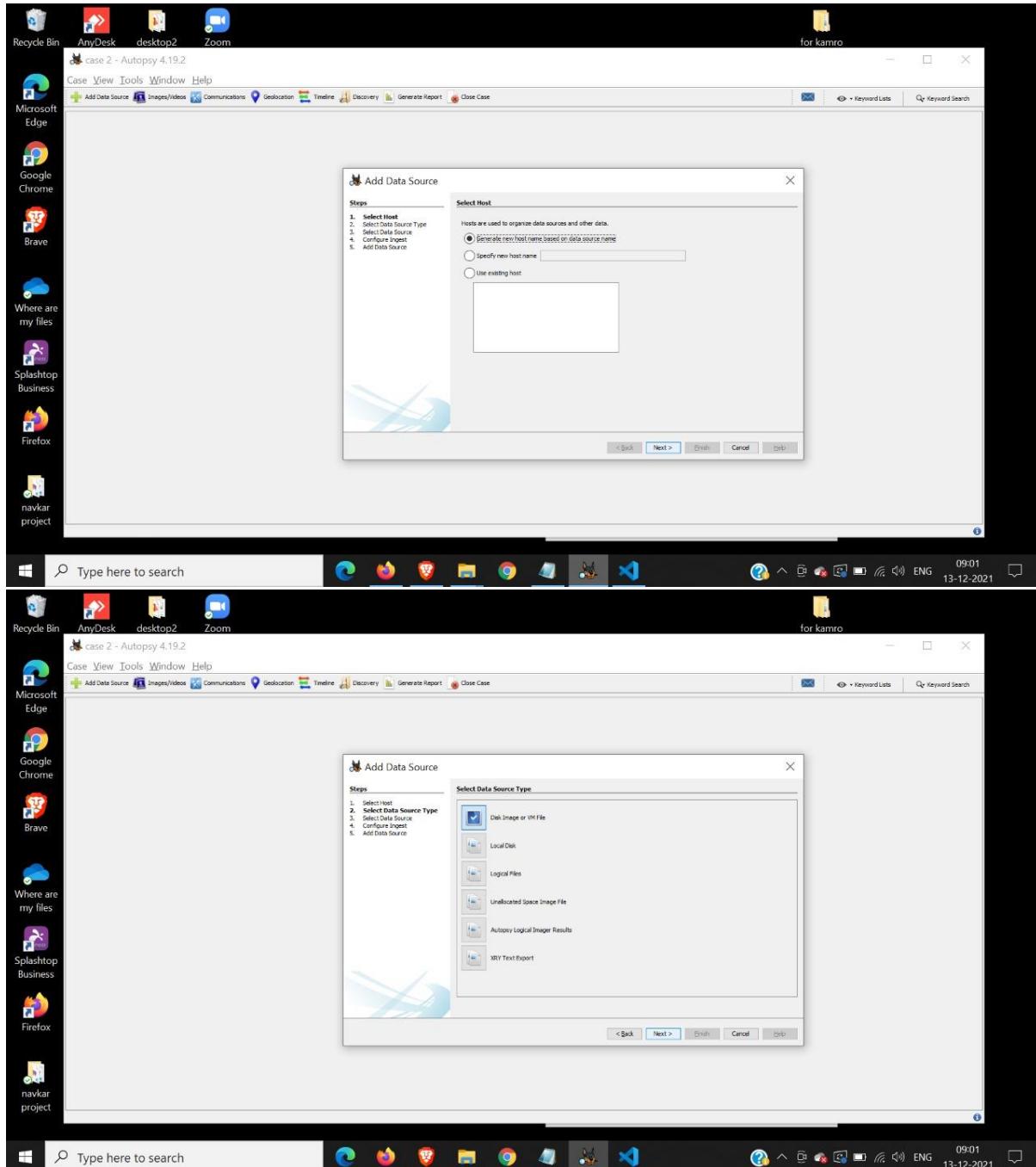
CYBER FORENSICS PRACTICALS

Practical No – 3

Aim: Forensics Case Study:

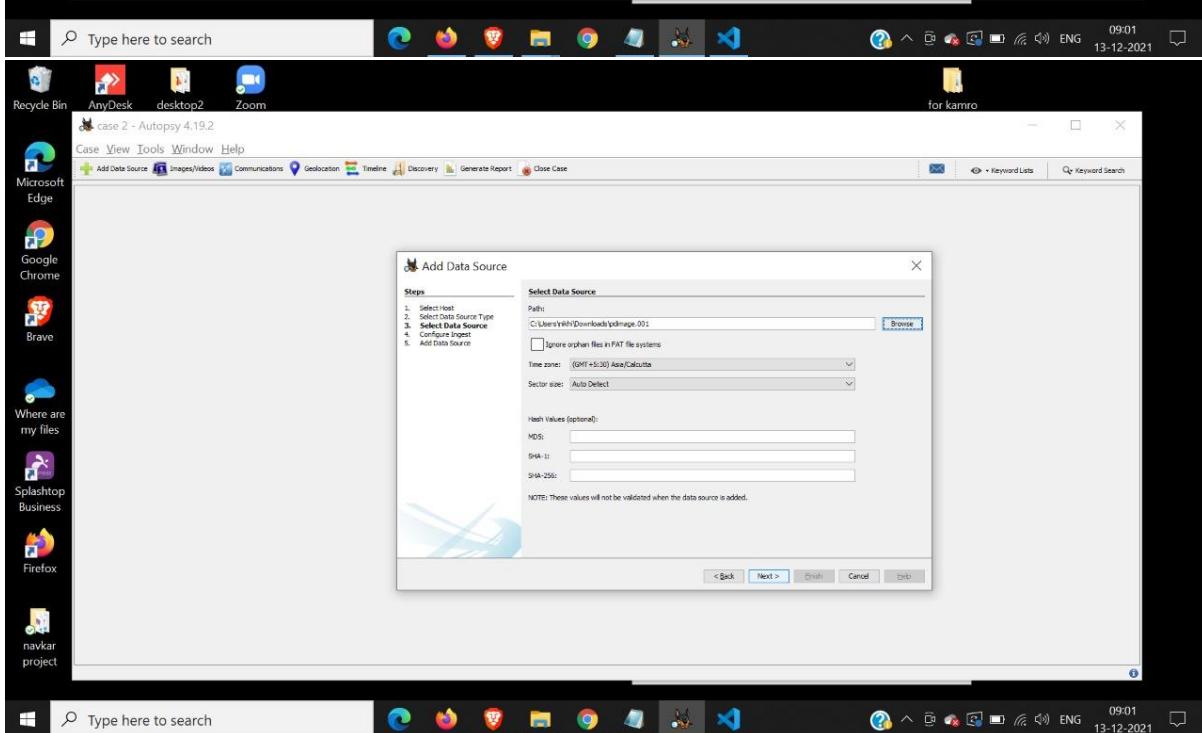
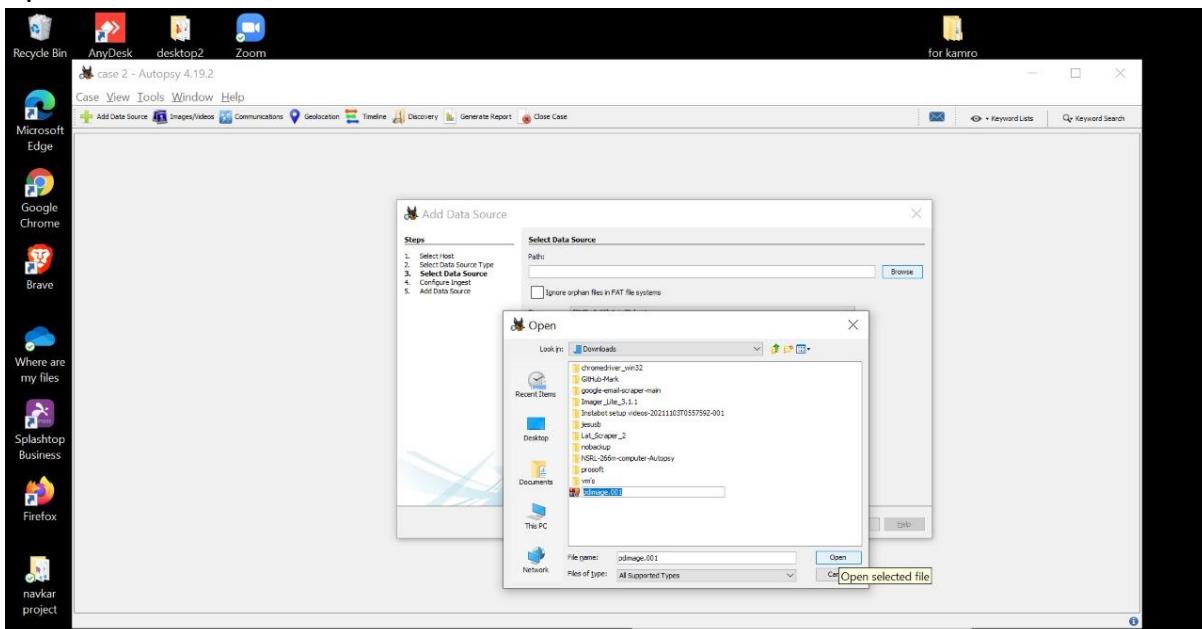
- Solve the Case study (image file) provide in lab using Autopsy

Install autopsy software and select new data source, select disk image or utf file

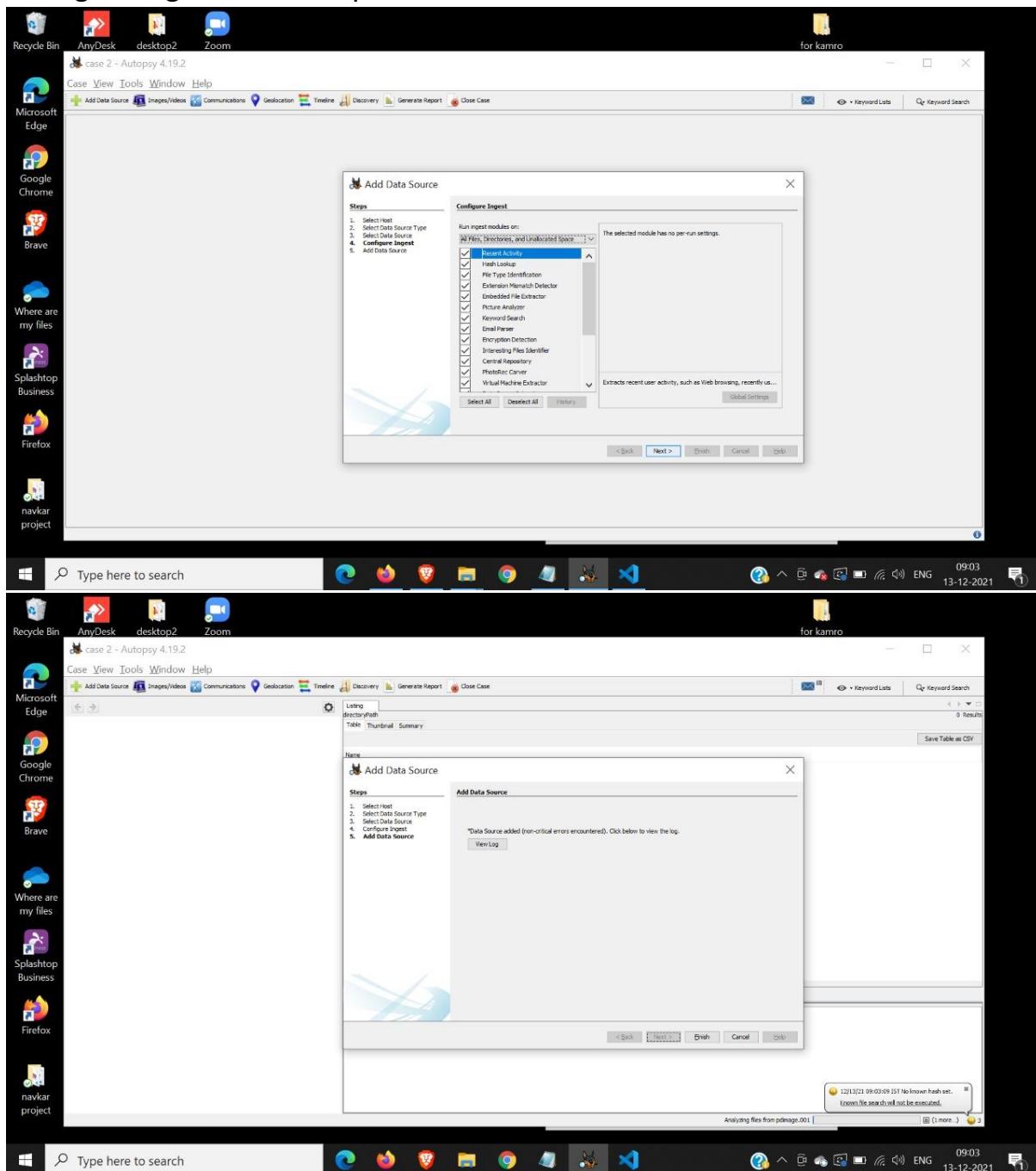


CYBER FORENSICS PRACTICALS

Browse and select the image of the pendrive made by ftk imager, enter the optional values if needed

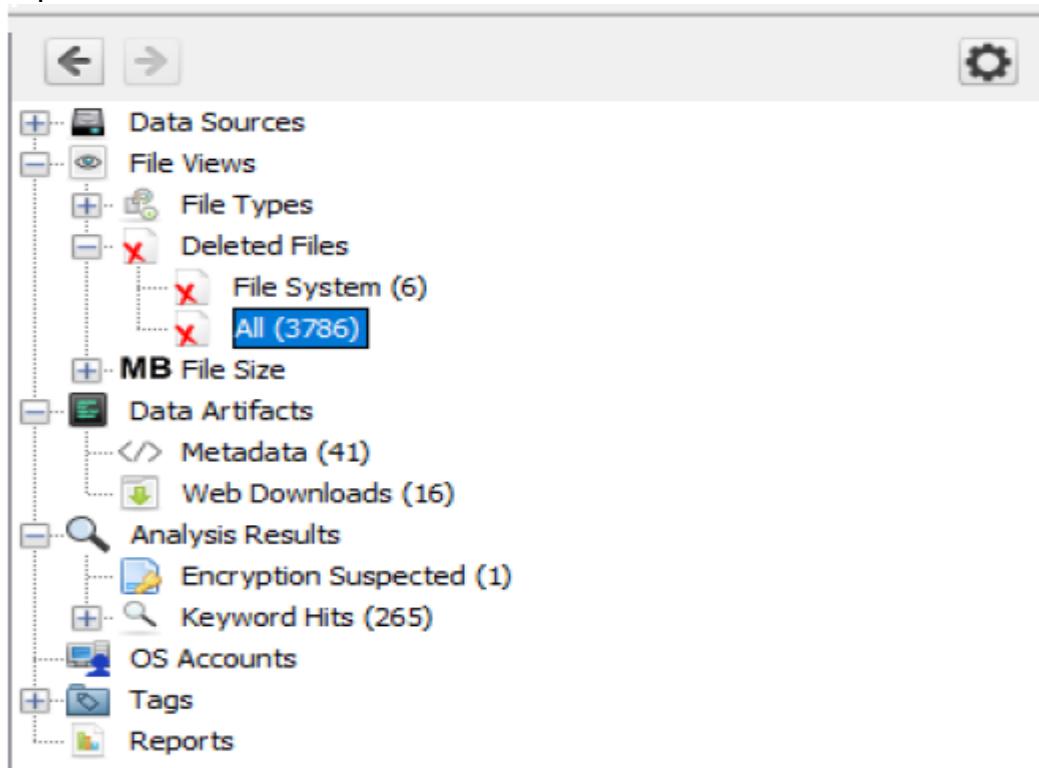


Configure ingest elect all options and add data source



On the left hierarchy lookup for deleted files

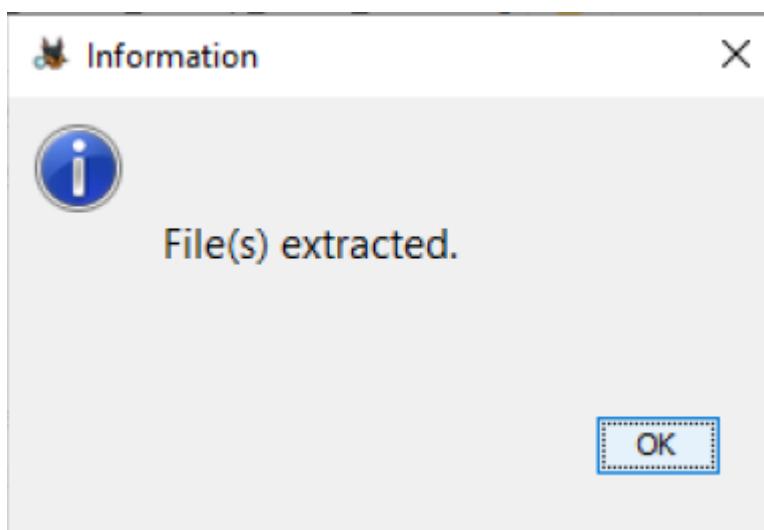
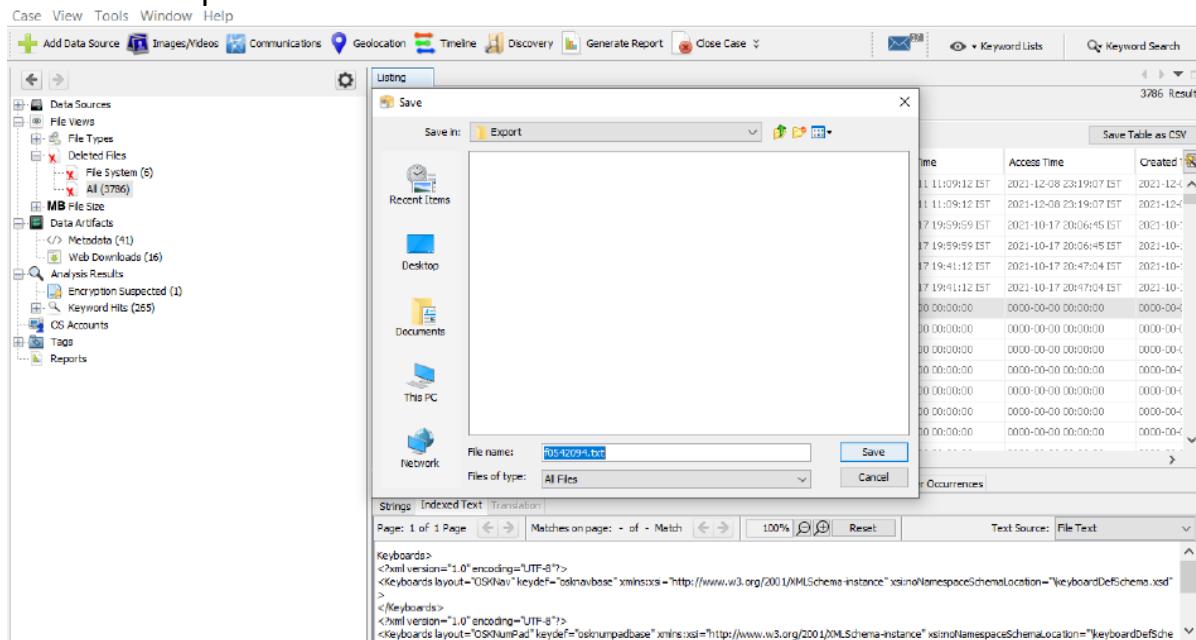
Expand it and click on All



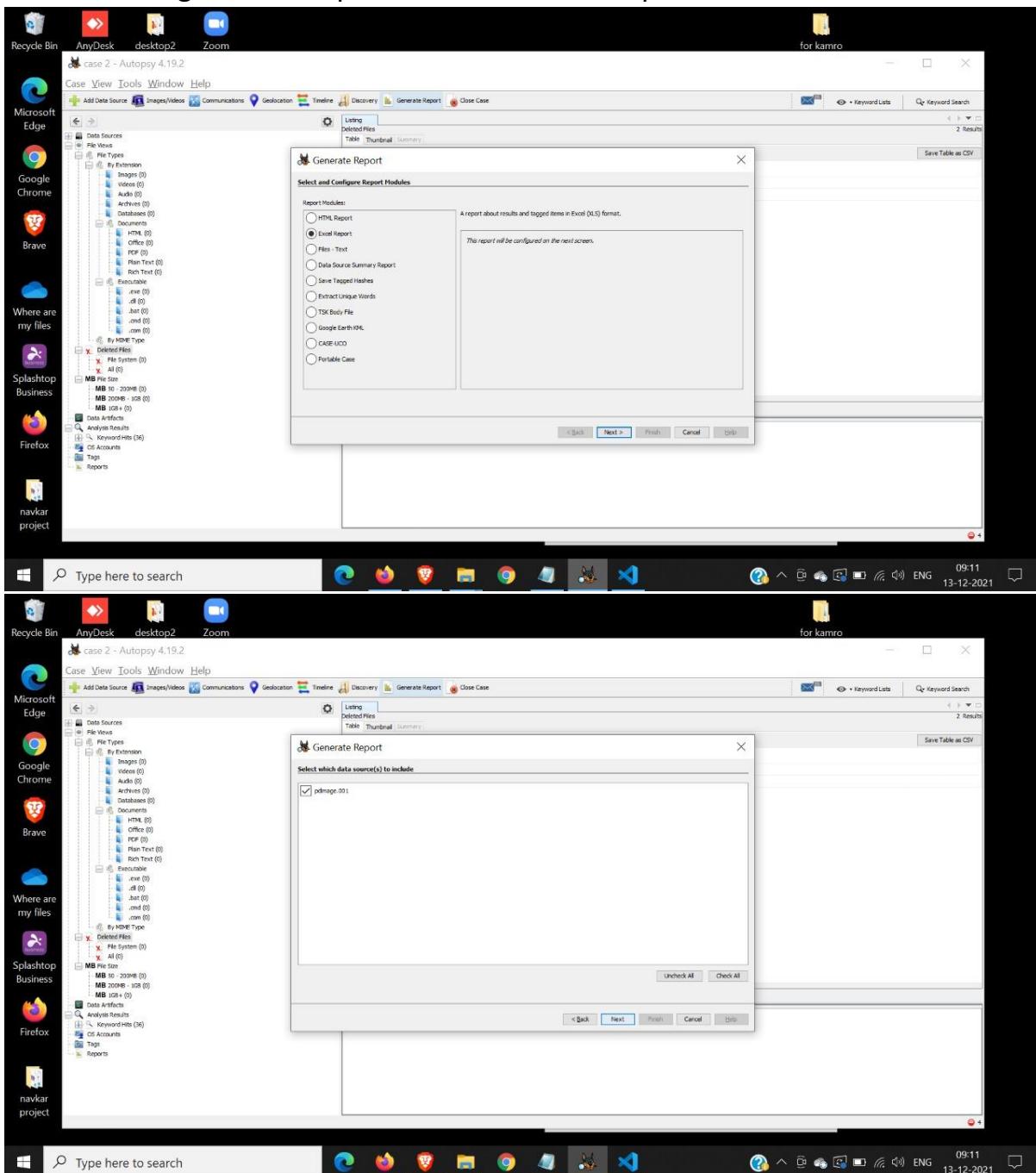
Right click on the table view and select Extract files

Name	S	C	O	Modified Time	Change Time	Access Time	Created
Anjar_654100 - Copy.rpt				2021-11-11 09:59:01 IST	2021-11-11 11:09:12 IST	2021-12-08 23:19:07 IST	2021-12-08 23:19:07 IST
Anjar_654100 - Copy.rpt.Zone.Identifier				2021-11-11 09:59:01 IST	2021-11-11 11:09:12 IST	2021-12-08 23:19:07 IST	2021-12-08 23:19:07 IST
_Getintopic.com_Parallels/Desktop_14.0.1_45154.dmg				2021-10-17 19:59:59 IST	2021-10-17 19:59:59 IST	2021-10-17 20:06:45 IST	2021-10-17 20:06:45 IST
_Getintopic.com_Parallels/Desktop_14.0.1_45154.dmg.Zone.Identifier				2021-10-17 19:59:59 IST	2021-10-17 19:59:59 IST	2021-10-17 20:06:45 IST	2021-10-17 20:06:45 IST
VirtualBox-6.1.22-144080-OSX.dmg				2021-10-17 19:41:12 IST	2021-10-17 19:41:12 IST	2021-10-17 20:47:04 IST	2021-10-17 20:47:04 IST
VirtualBox-6.1.22-144080-OSX.dmg.Zone.Identifier				2021-10-17 19:41:12 IST	2021-10-17 19:41:12 IST	2021-10-17 20:47:04 IST	2021-10-17 20:47:04 IST
f0542094.txt	1			00:00:00-00:00:00000000	00:00:00-00:00:00000000	00:00:00-00:00:00000000	00:00:00-00:00:00000000
f0599104.java				00:00:00	00:00:00-00:00:00000000	00:00:00-00:00:00000000	00:00:00-00:00:00000000
f0599112_clustercomp				00:00:00	00:00:00-00:00:00000000	00:00:00-00:00:00000000	00:00:00-00:00:00000000
f0599175_CM12RTGM				00:00:00	00:00:00-00:00:00000000	00:00:00-00:00:00000000	00:00:00-00:00:00000000
f0599520_CMISetup_D				00:00:00	00:00:00-00:00:00000000	00:00:00-00:00:00000000	00:00:00-00:00:00000000
f0700760_compcertctrl				00:00:00	00:00:00-00:00:00000000	00:00:00-00:00:00000000	00:00:00-00:00:00000000

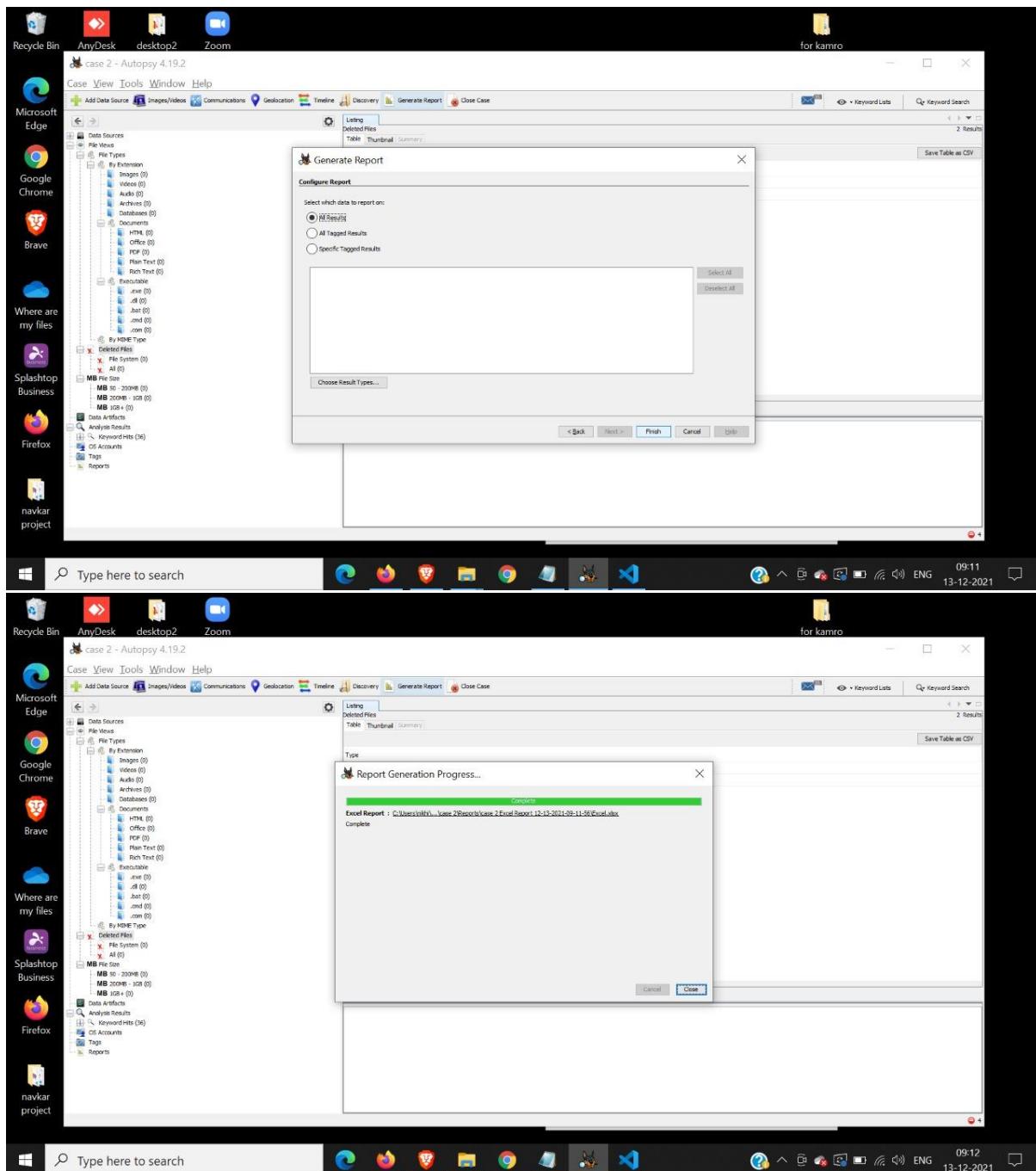
Select the export folder



Now click on generate report and select excel report

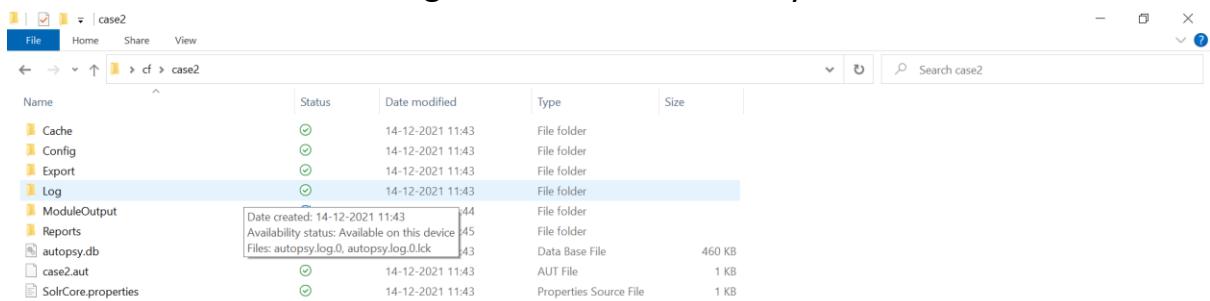


Click all results and select finish



CYBER FORENSICS PRACTICALS

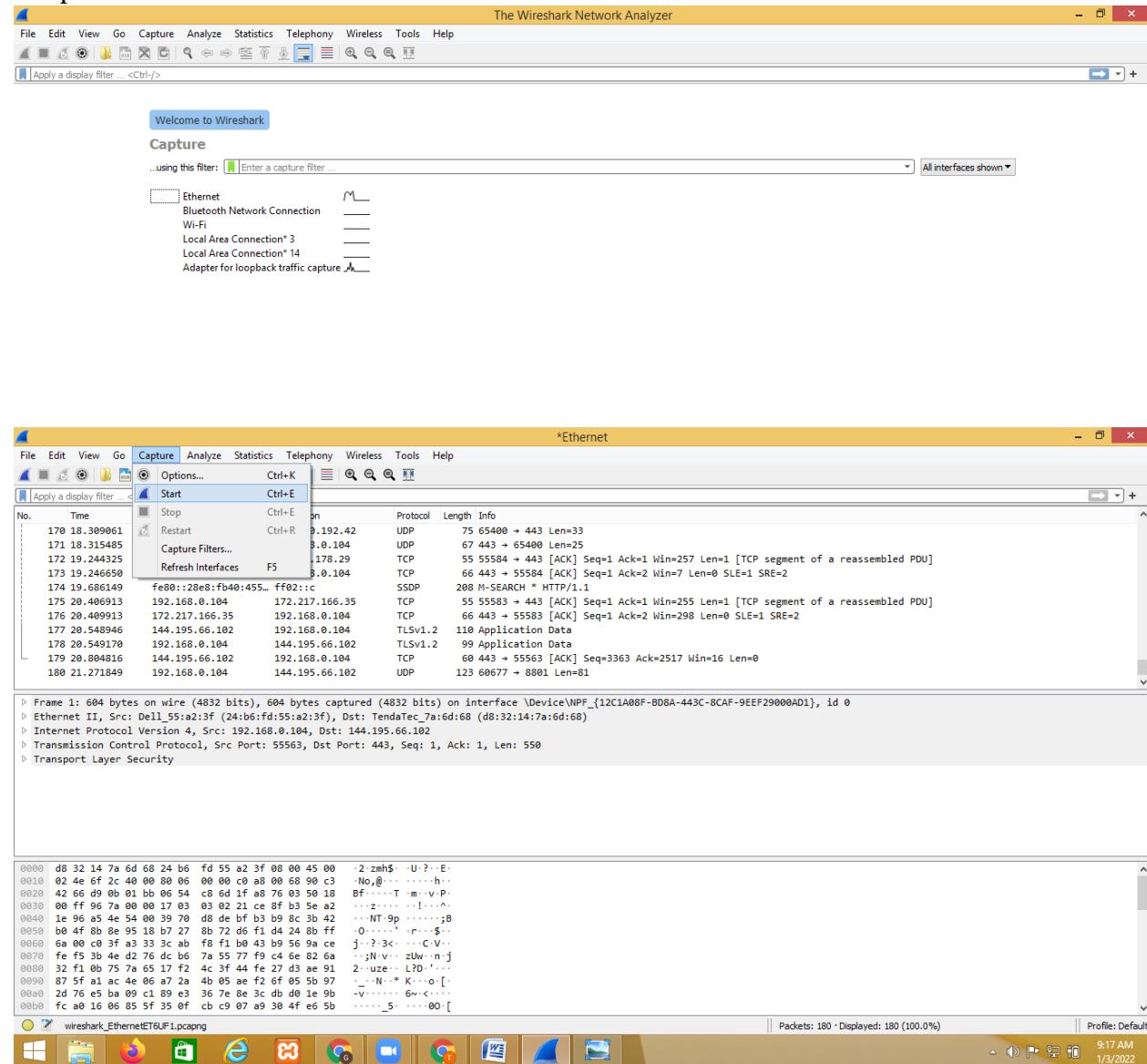
You can view the folders in generated base directory



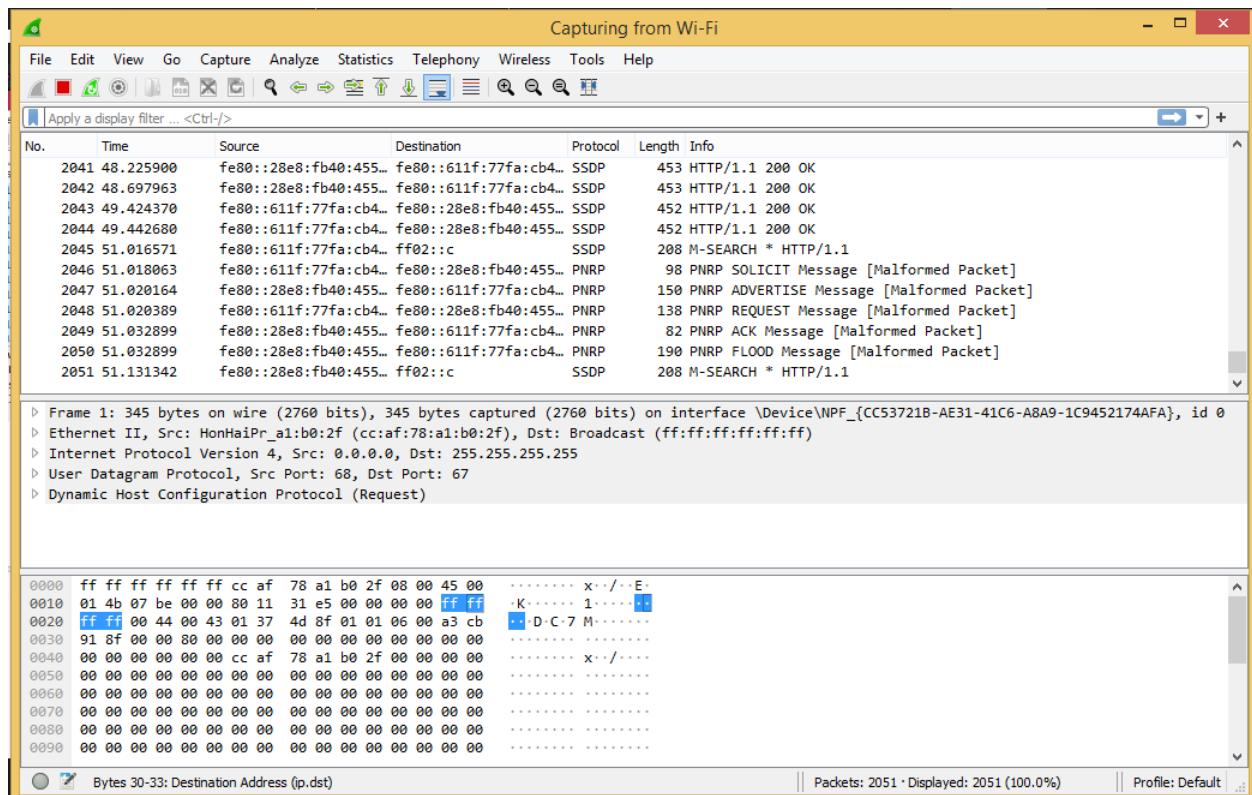
Row	Column	Value
1	A	z
2	A	
3	A	Case Name:
3	B	case2
4	A	Case Number:
4	B	2
5	A	Number of data sources in case:
5	B	1
6	A	Examiner:
6	B	nikhil
7	A	
8	A	
9	A	
10	A	
11	A	
12	A	
13	A	
14	A	
15	A	
16	A	
17	A	
18	A	

Practical:4**Aim: Capturing and analyzing network packets using Wireshark (Fundamentals):**

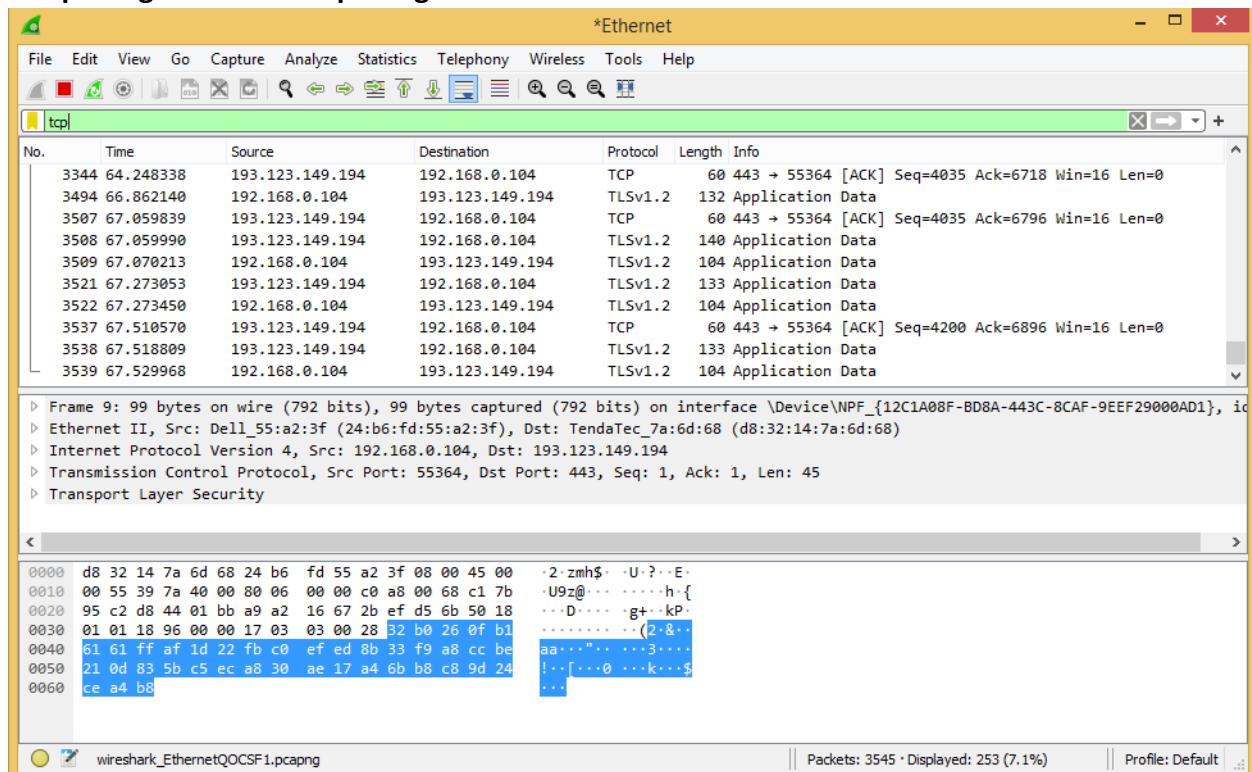
- Identification the live network
- Capture Packets
- Analyze the captured packets

1. Open Wireshark

CYBER FORENSICS PRACTICALS



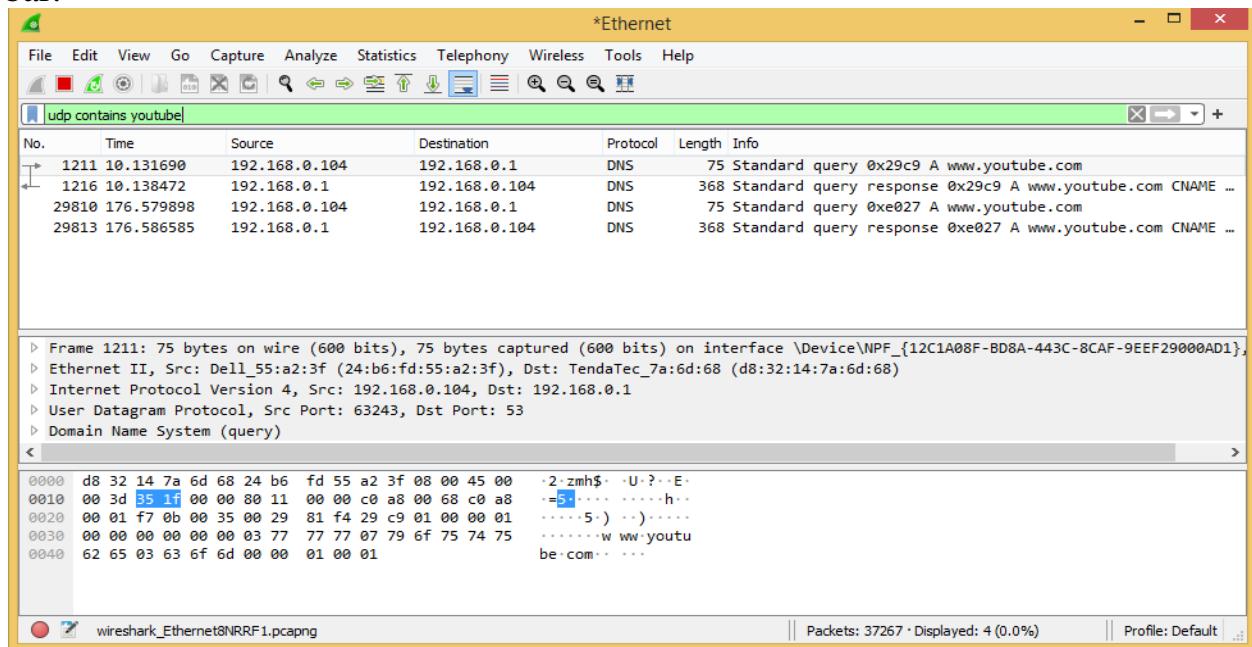
TCP package: search TCP package



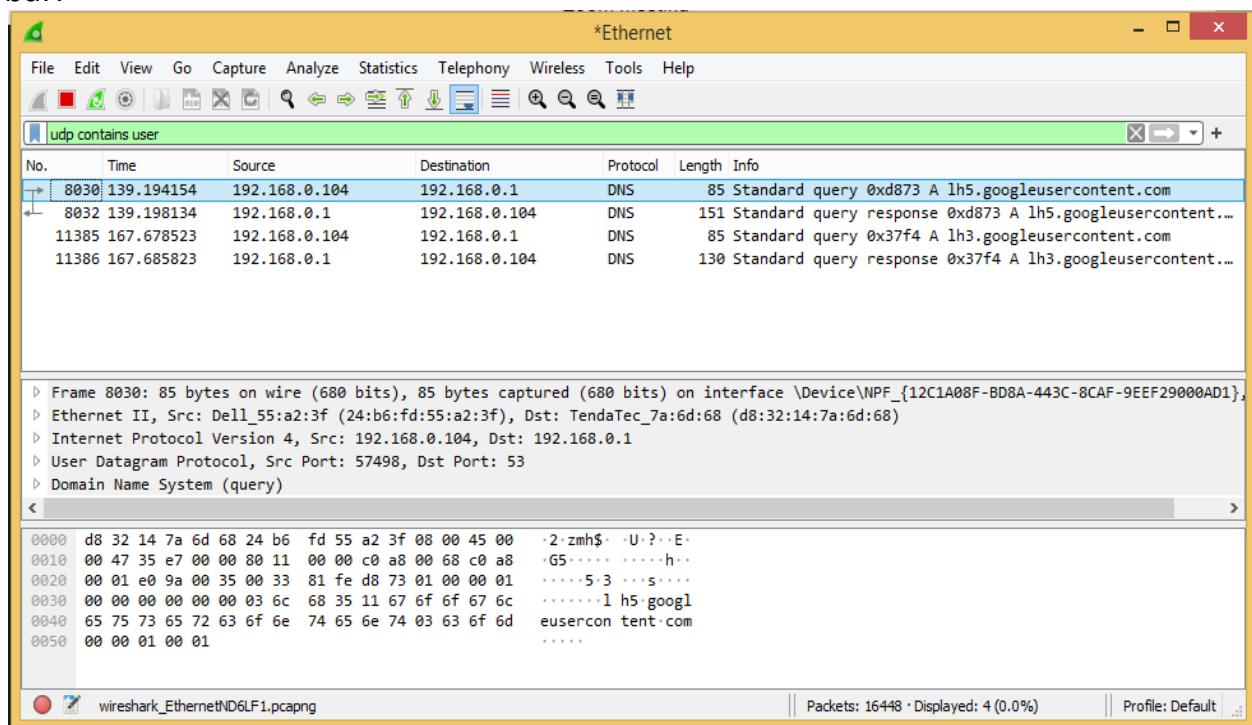
Analysis youtube data

Now go on browser and open youtube and perform some activity on the youtube

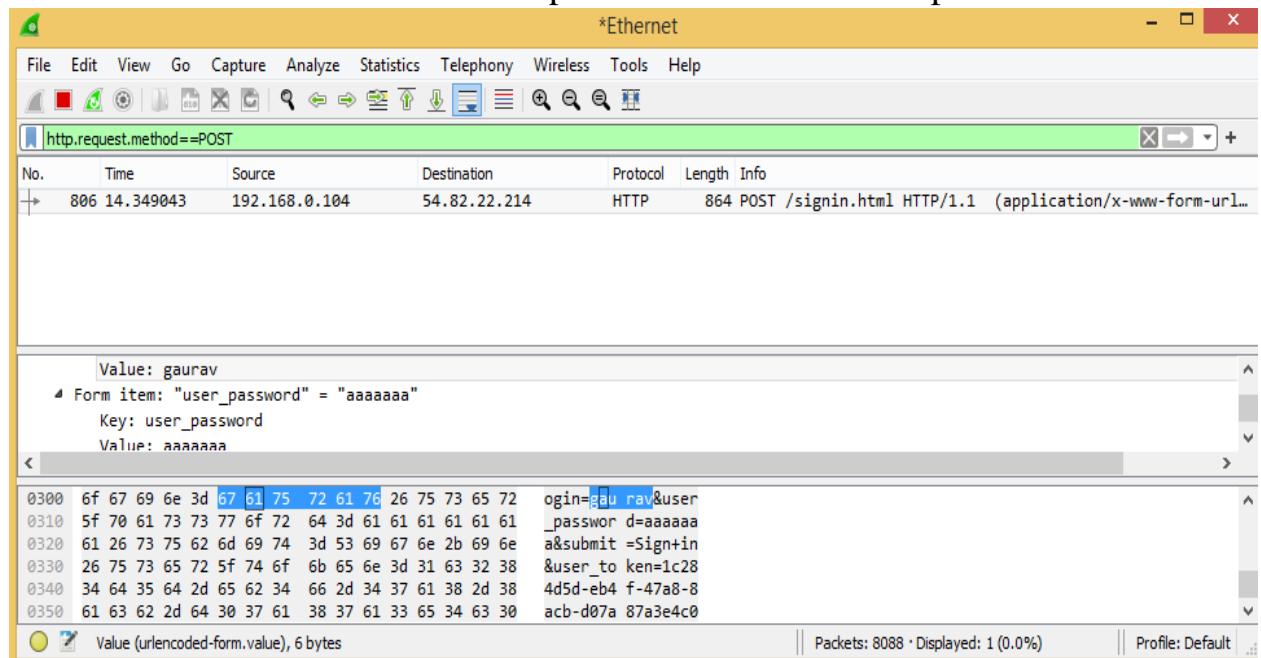
Now come back to Wireshark and enter **udp contains youtube** in the search bar.



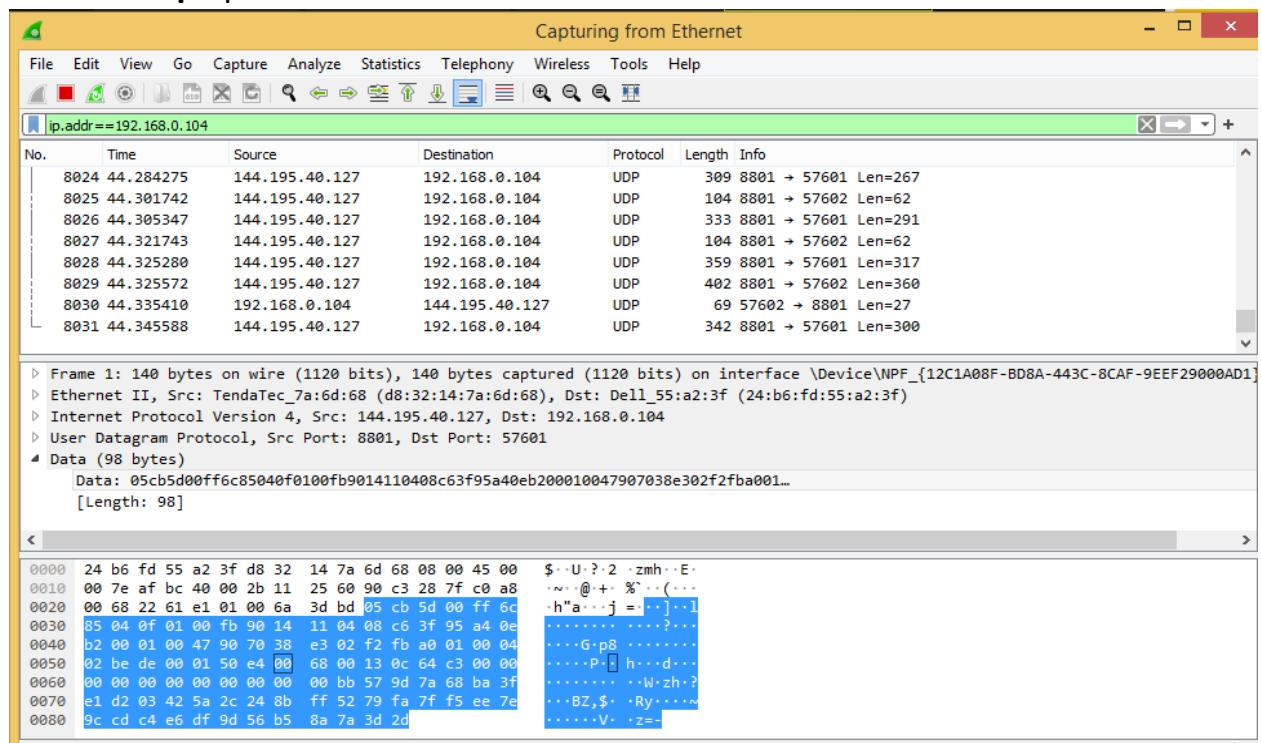
search udp contains user: Now go on browser, login in any secured website and Now come back to Wireshark and enter **udp contains user** in the search bar.



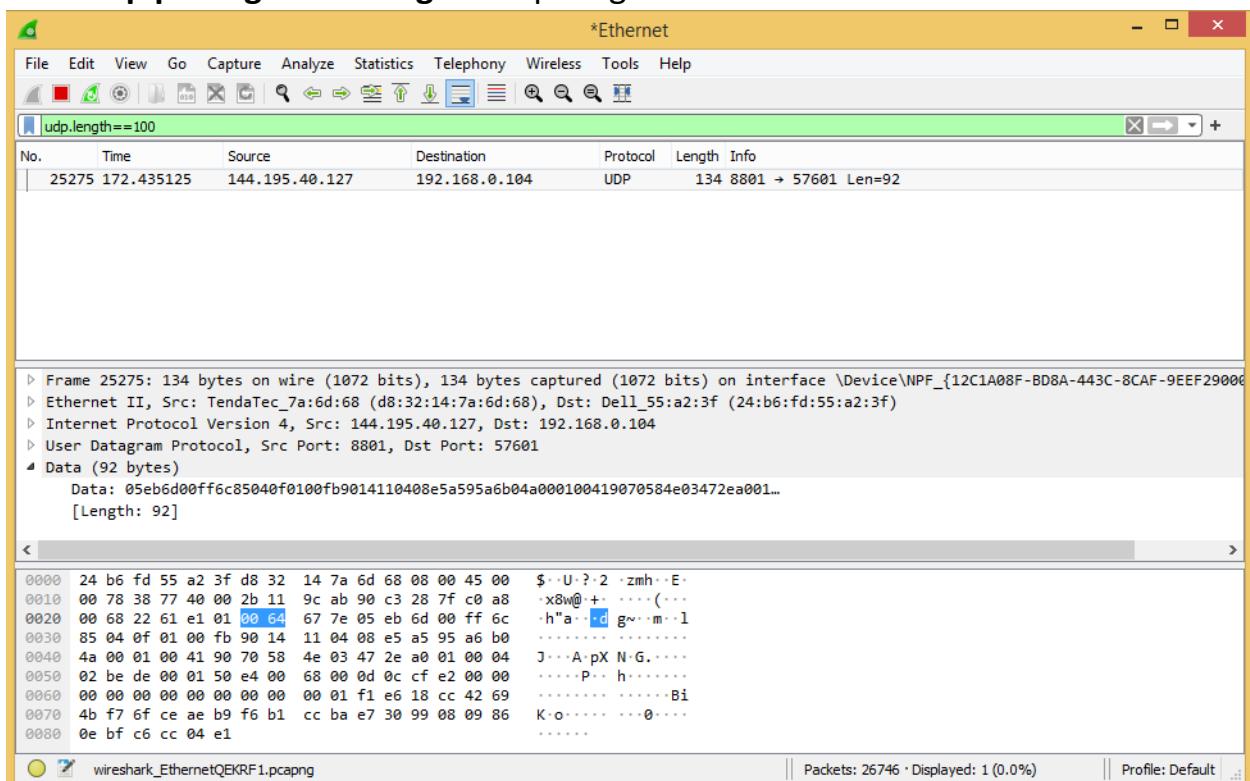
http website: go on browser, login in any unsecured website and Now come back to Wireshark and enter **http.request.method==POST** in the search bar. You can view the username and password because it is http website



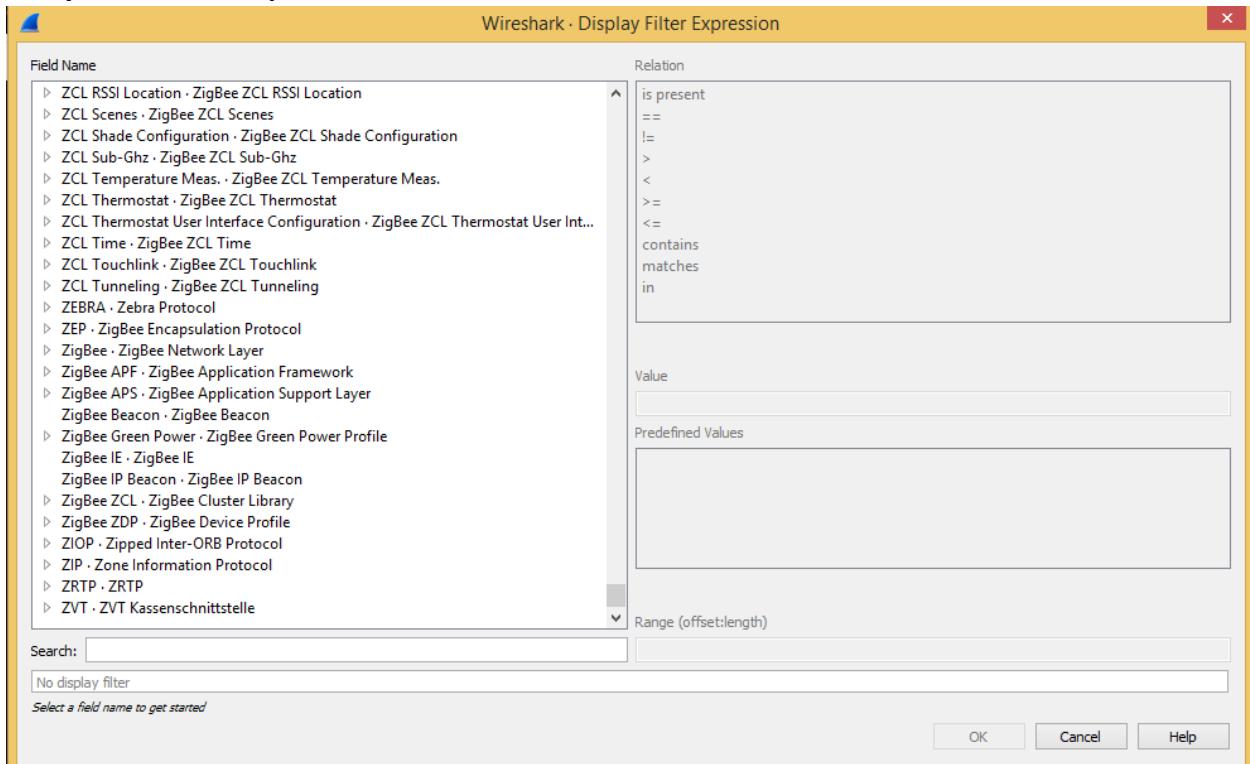
filter with ip: `ip.addr==192.168.0.104`



filter udp package with length : udp.length==100



Many other filter expression

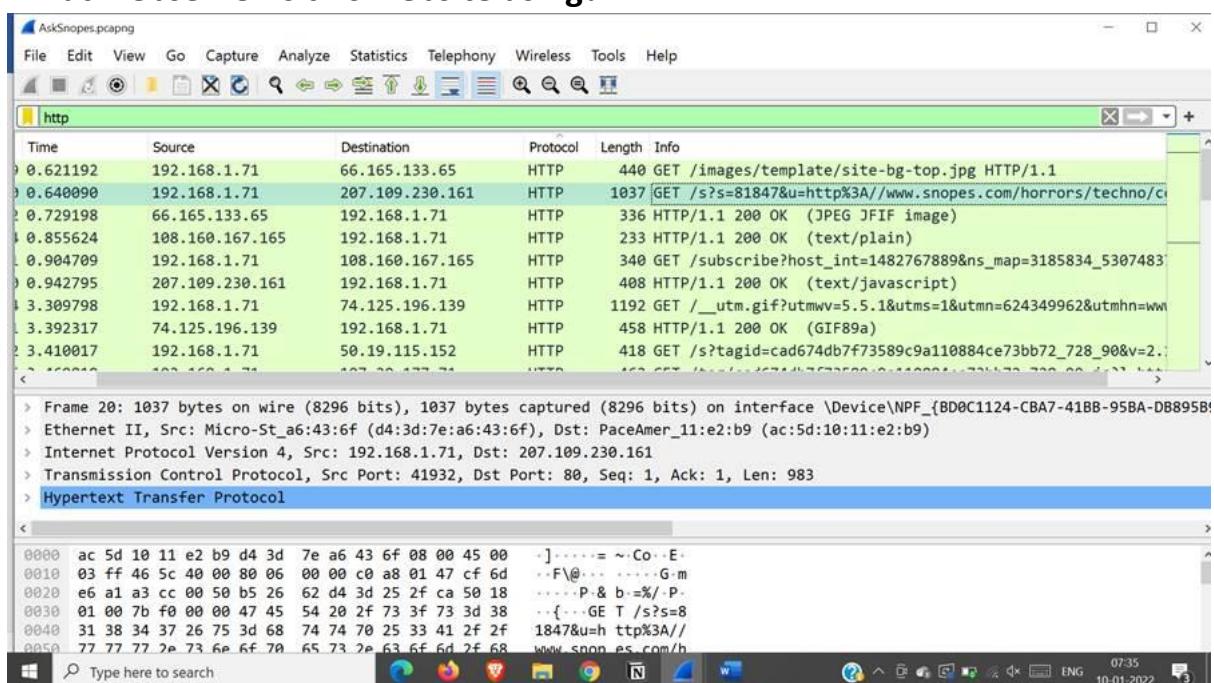


Practical-5

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

- What web server software is used by www.snopes.com?
- About what cell phone problem is the client concerned?
- According to Zillow, what instrument will Ryan learn to play?
- How many web servers are running Apache?
- What hosts (IP addresses) think that jokes are more entertaining when they are explained?

What webserver is this website using?



CYBER FORENSICS PRACTICALS

AskSnopes.pcapng

File Edit View Go Capture Analyze Statistics Telephony

http

Time	Source	Destination
0.621192	192.168.1.71	66.165.133.65
0.640090	192.168.1.71	207.109.230.161
0.729198	66.165.133.65	192.168.1.71
0.855624	108.160.167.165	192.168.1.71
0.904709	192.168.1.71	108.160.167.165
0.942795	207.109.230.161	192.168.1.71
1.309798	192.168.1.71	74.125.196.139
1.392317	74.125.196.139	192.168.1.71
2.3410017	192.168.1.71	50.19.115.152
< 160010	192.168.1.71	107.20.177.71

Hypertext Transfer Protocol

- > GET /s?s=81847&u=http%3A//www.snopes.com/horror
- Host: as.casalemedia.com\r\n
- User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:2.0) Gecko/20100101 Firefox/2.0
- Accept: */*\r\n
- Accept-Language: en-US,en;q=0.5\r\n

Apply as Column Ctrl+Shift+I

Apply as Filter

Prepare as Filter

Conversation Filter

Colorize with Filter

Follow

Copy

Show Packet Bytes... Ctrl+Shift+O

Export Packet Bytes... Ctrl+Shift+X

Wiki Protocol Page

Filter Field Reference

Protocol Preferences

Decode As... Ctrl+Shift+U

Go to Linked Packet

Show Linked Packet in New Window

media.co m-User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:2.0) Gecko/20100101 Firefox/2.0

Type here to search

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

Time	Source	Destination	Protocol	Length	Host	Info
19.0621192	192.168.1.71	66.165.133.65	HTTP	440	www.snopes.com	GET /images/template/si
20.0640090	192.168.1.71	207.109.230.161	HTTP	1037	as.casalemedia.com	GET /s?s=81847&u=http%3A
52.0729198	66.165.133.65	192.168.1.71	HTTP	336		HTTP/1.1 200 OK (JPEG)
54.0855624	108.160.167.165	192.168.1.71	HTTP	233		HTTP/1.1 200 OK (text/
61.0904709	192.168.1.71	108.160.167.165	HTTP	340	notify4.dropbox.com	GET /subscribe?host_int
70.0942795	207.109.230.161	192.168.1.71	HTTP	408		HTTP/1.1 200 OK (text/
94.3.309798	192.168.1.71	74.125.196.139	HTTP	1192	www.google-analytics.com	GET /_utm.gif?utmwv=5.
101.3.392317	74.125.196.139	192.168.1.71	HTTP	458		HTTP/1.1 200 OK (GIF89
102.3.410017	192.168.1.71	50.19.115.152	HTTP	418	stat.komoona.com	GET /?tagid=cad674db7f
< 160010	192.168.1.71	107.20.177.71	HTTP	160		GET /index.html?utmz=0.1000000000000000

> Frame 19: 440 bytes on wire (3520 bits), 440 bytes captured (3520 bits) on interface \Device\NPF_{BD0C1124-CBA7-41BB-95BA-DB895B96

> Ethernet II, Src: Micro-St_a6:43:6f (d4:3d:7e:a6:43:6f), Dst: PaceAmer_11:e2:b9 (ac:5d:10:11:e2:b9)

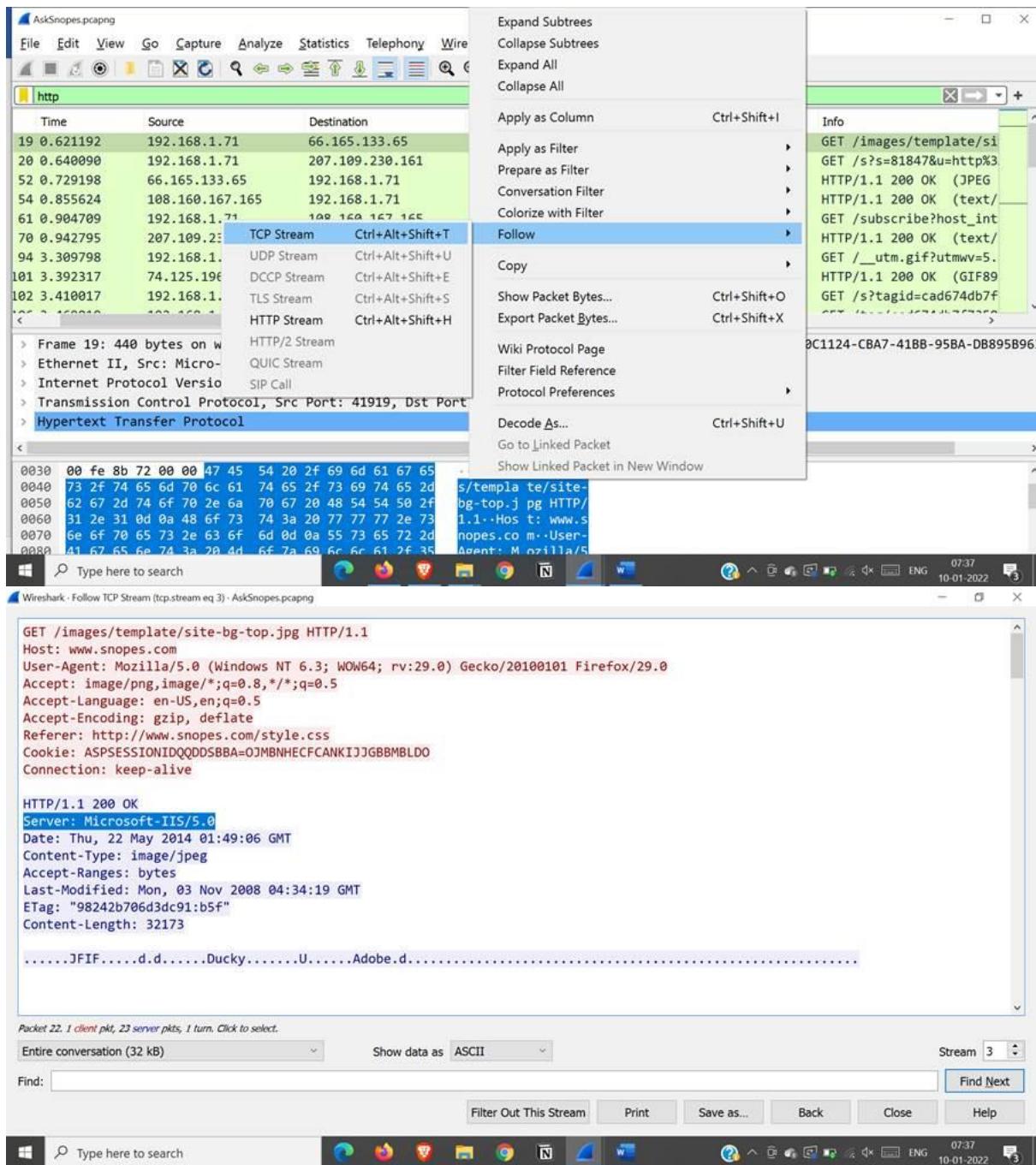
> Internet Protocol Version 4, Src: 192.168.1.71, Dst: 66.165.133.65

> Transmission Control Protocol, Src Port: 41919, Dst Port: 80, Seq: 1, Ack: 1, Len: 386

> Hypertext Transfer Protocol

Type here to search

CYBER FORENSICS PRACTICALS

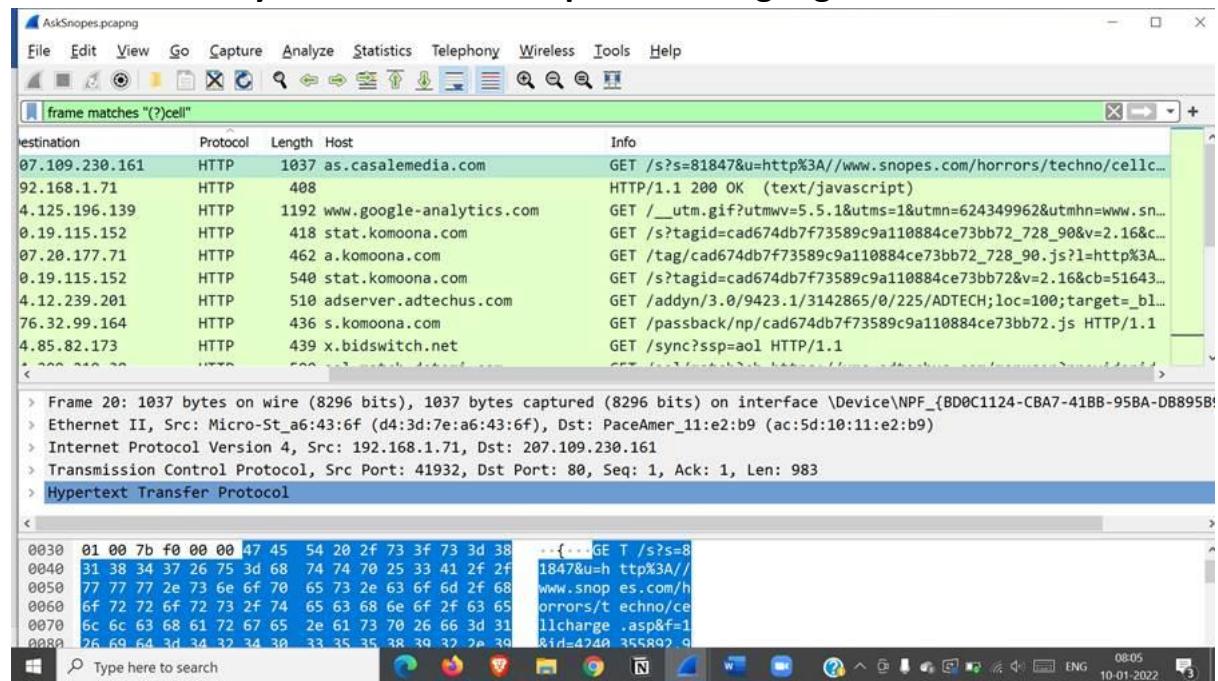


ANS-

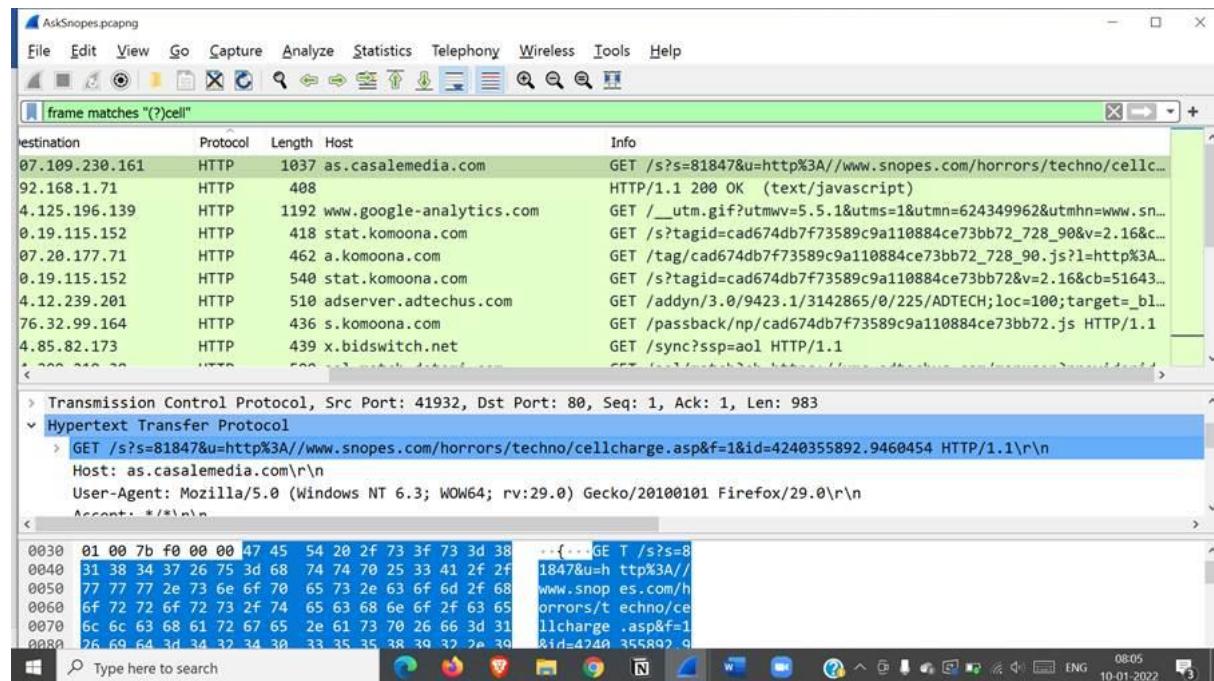
Server is Microsoft iis server

About what cell phone problem is the client concerned with?

-Search for a keyword cell in all cell packets using regex



-frame matches "(?cell"



ANS-

Client had searched for cell charge problem

How many webservers?

Into the filter type “ http.server contains "Apache" ” and search. Now click on Statistics – Endpoints.

Move to Ipv4. Check the Limit to display filter at the bottom and you can see that 22 servers are running Apache

The screenshot shows two instances of the Wireshark application. The top instance displays a list of captured HTTP responses. The bottom instance shows a context menu open over one of the responses, specifically for the packet containing the Apache server information.

Wireshark Top Window (http.response):

No.	Time	Source	Destination	Protocol	Length	Host	Server
2257	93.040810	66.165.133.65	192.168.1.71	HTTP	388		Microsoft-IIS/5.0
2266	93.076882	66.165.133.65	192.168.1.71	HTTP	388		Microsoft-IIS/5.0
2274	93.118148	66.165.133.65	192.168.1.71	HTTP	388		Microsoft-IIS/5.0
2277	93.159605	66.165.133.65	192.168.1.71	HTTP	388		Microsoft-IIS/5.0
161	7.047345	74.209.219.38	192.168.1.71	HTTP	303		nginx/1.4.3
665	25.844138	216.39.55.13	192.168.1.71	HTTP	60		YTS/1.20.13
1079	42.840984	50.97.236.98	192.168.1.71	HTTP	473		Apache/2.2.24 (Unix)
1084	42.871332	205.210.187.217	192.168.1.71	HTTP	1092		nginx/1.5.3
1649	76.607080	64.94.107.34	192.168.1.71	HTTP	603		QS
1656	76.630442	205.210.186.156	192.168.1.71	HTTP	1159		nginx/1.5.3
1667	76.726301	68.67.128.40	192.168.1.71	HTTP	739		
1674	76.899587	50.116.194.21	192.168.1.71	HTTP	1045		Apache-Coyote/1.1

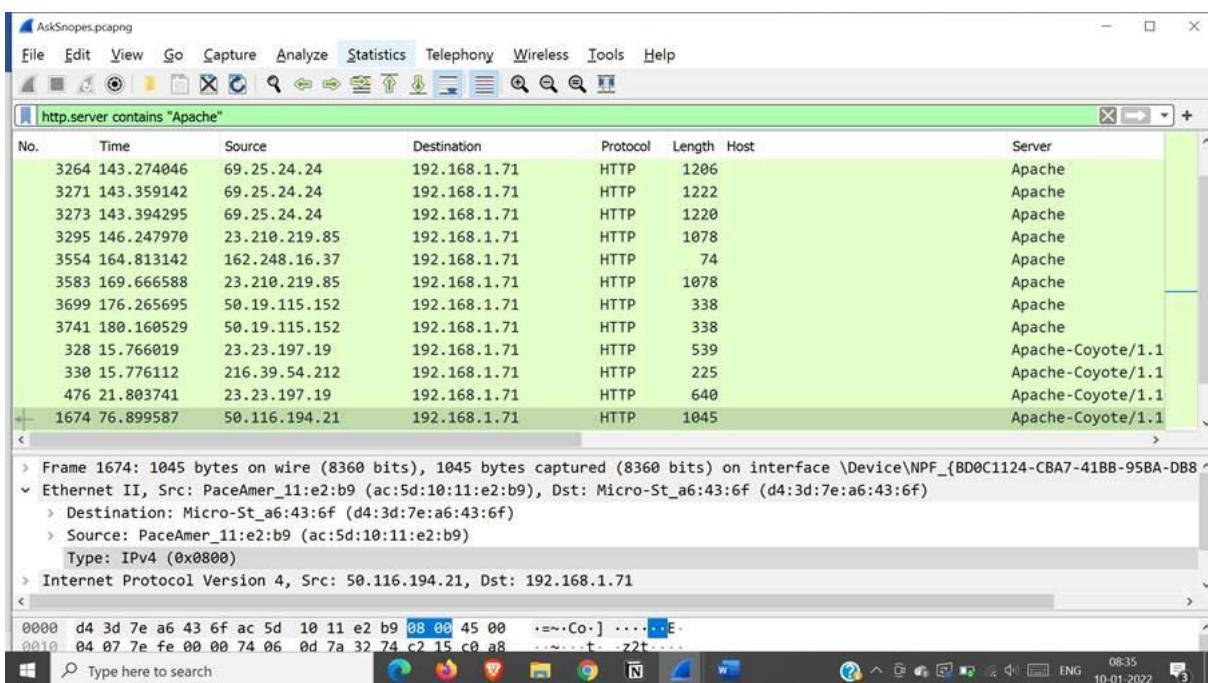
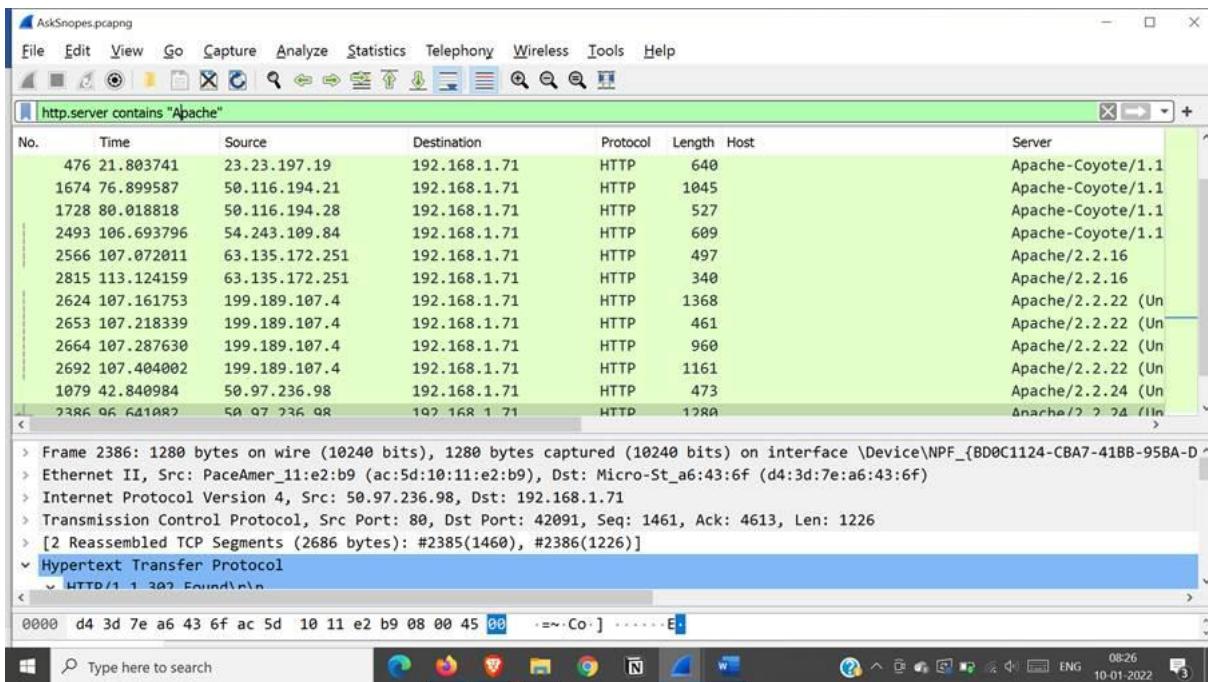
Wireshark Bottom Window (http.response):

[Content length: 0]
Date: Thu, 22 May 2014 01:49:21 GMT\r\n
Server: QS\r\n
\r\n
[HTTP response 1/1]
[Time since request: 0.036669000 seconds]

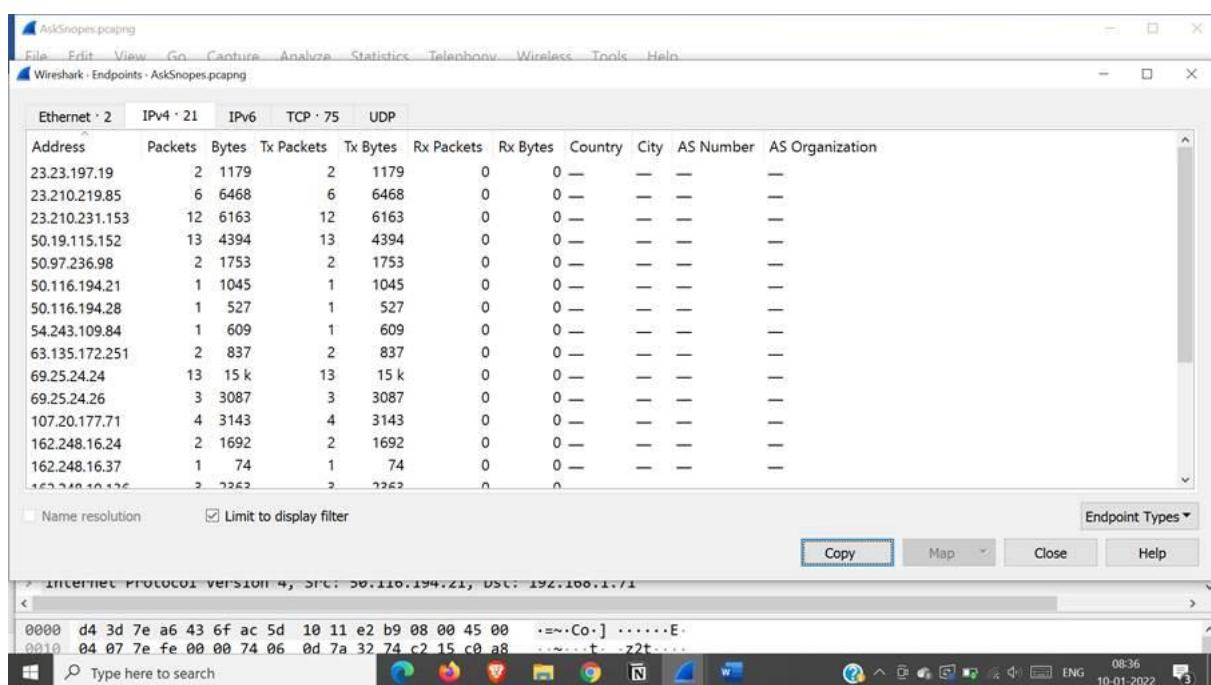
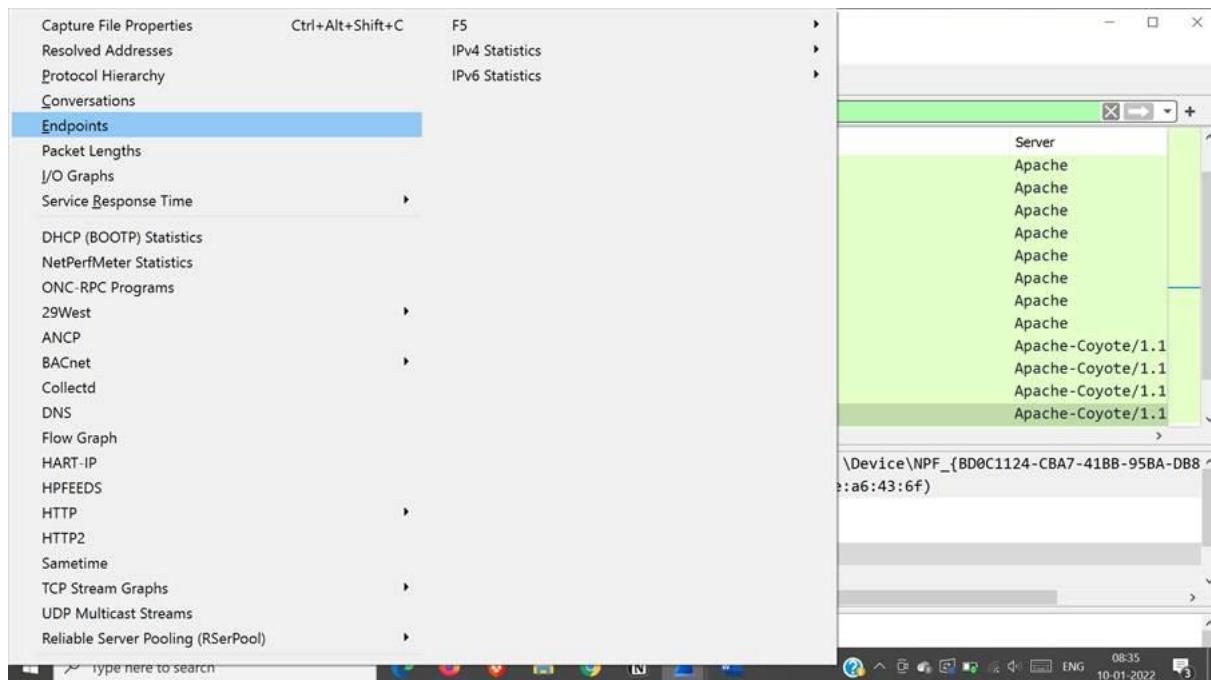
Context Menu (Open over Server: QS\r\n):

- Expand Subtrees
- Collapse Subtrees
- Expand All
- Collapse All
- Apply as Column Ctrl+Shift+I
- Apply as Filter
- Prepare as Filter
- Conversation Filter
- Colorize with Filter
- Follow
- Copy
- Show Packet Bytes... Ctrl+Shift+O
- Export Packet Bytes... Ctrl+Shift+X
- Wiki Protocol Page
- Filter Field Reference
- Protocol Preferences
- Decode As... Ctrl+Shift+U
- Go to Linked Packet
- Show Linked Packet in New Window

CYBER FORENSICS PRACTICALS



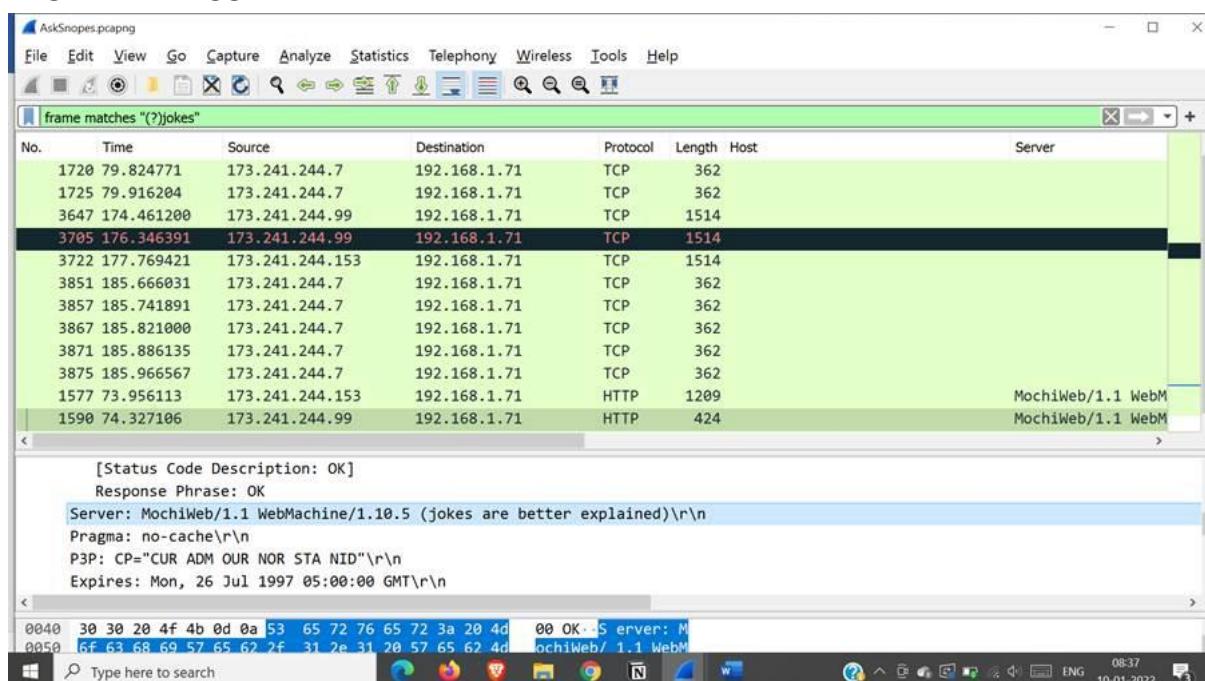
CYBER FORENSICS PRACTICALS



What hosts think Jokes are more entertaining when they are explained?

Search in filter: frame matches"(?)jokes"

To begin firstly search the keyword jokes into the filter type "frame matches"(?)jokes"" and click on the first row of result. Now move to the second frame, where you will find Hypertext Transfer Protocol expand it to see the GET method where you'll see what query the user has searched for i.e. jokes are more entertaining when they are explained . The IP address for the same is 173.241.244.99



Practical:6

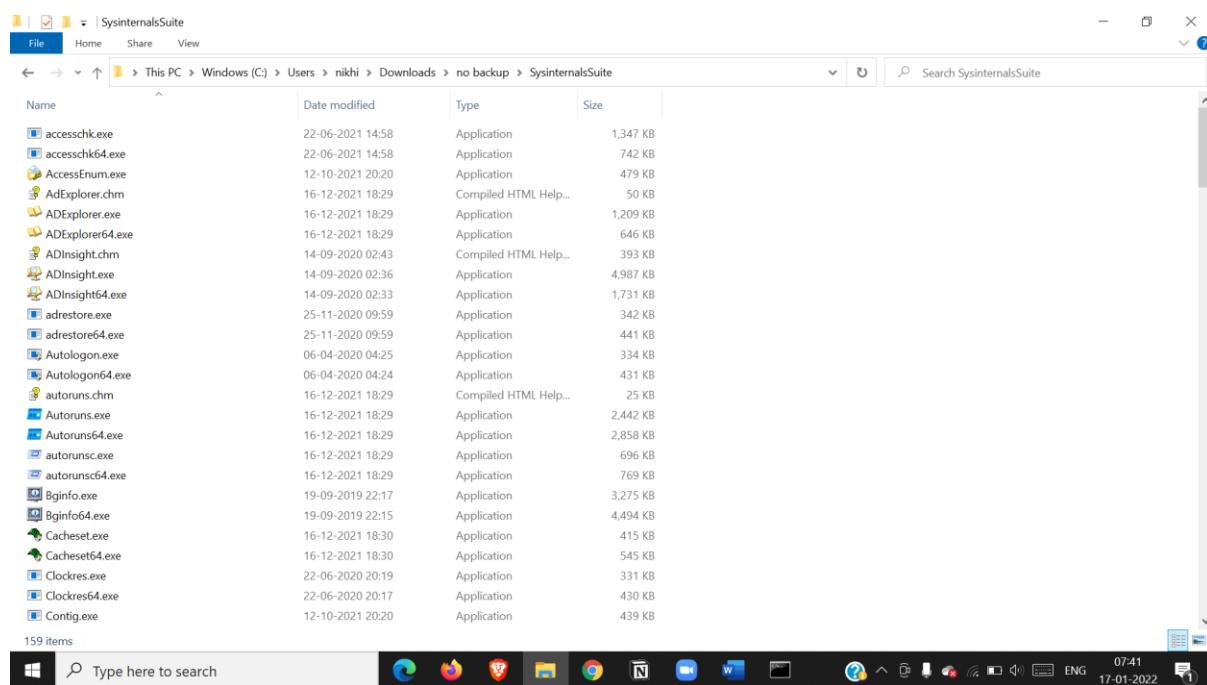
Aim: Using Sysinternals tools for Network Tracking and Process Monitoring:

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

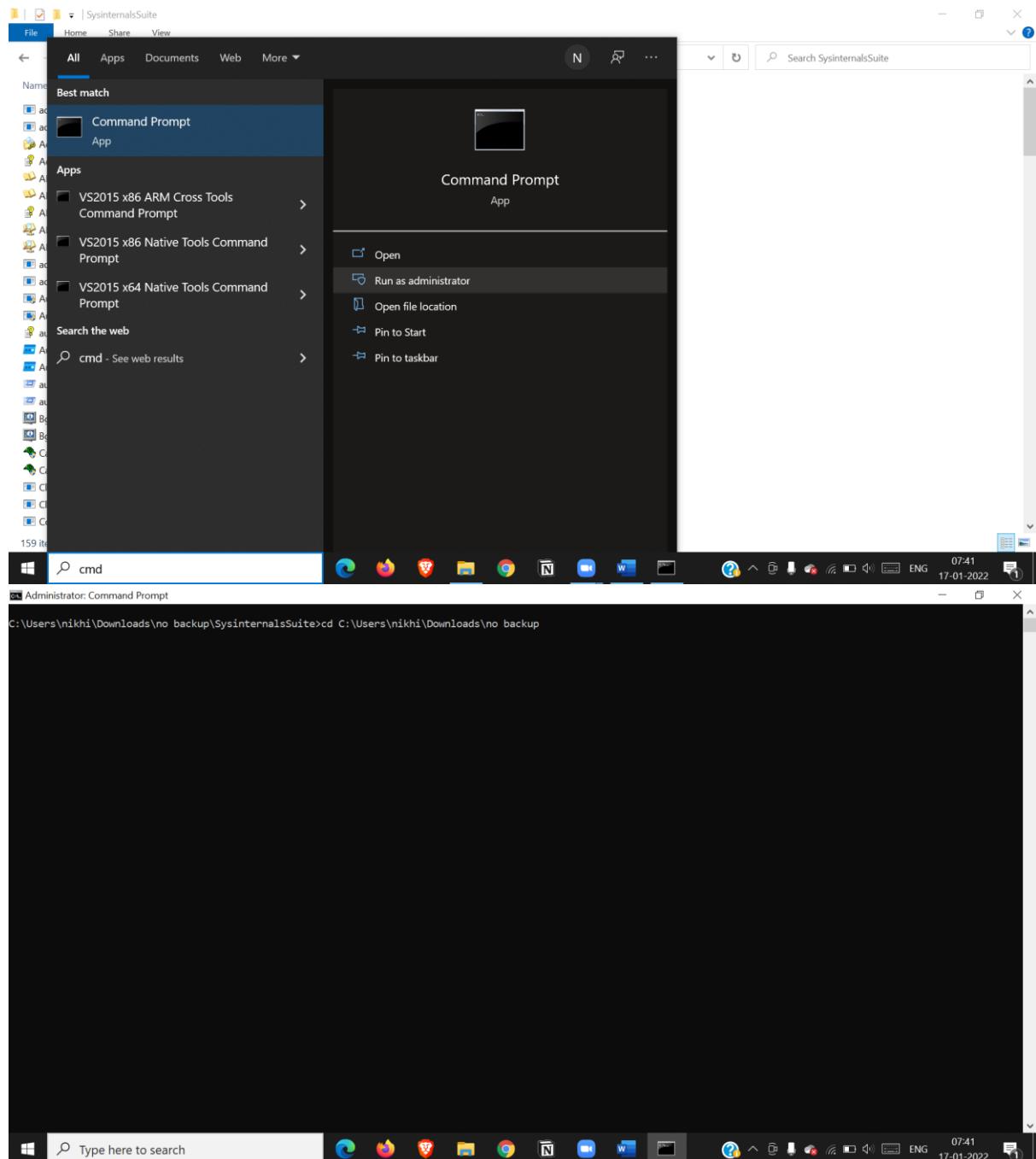
Sysinternal tools

The SysInternals suite of tools is **simply a set of Windows applications that can be downloaded for free from their section of the Microsoft Technet web site**. They are all portable, which means that not only do you not have to install them, you can stick them on a flash drive and use them from any PC.

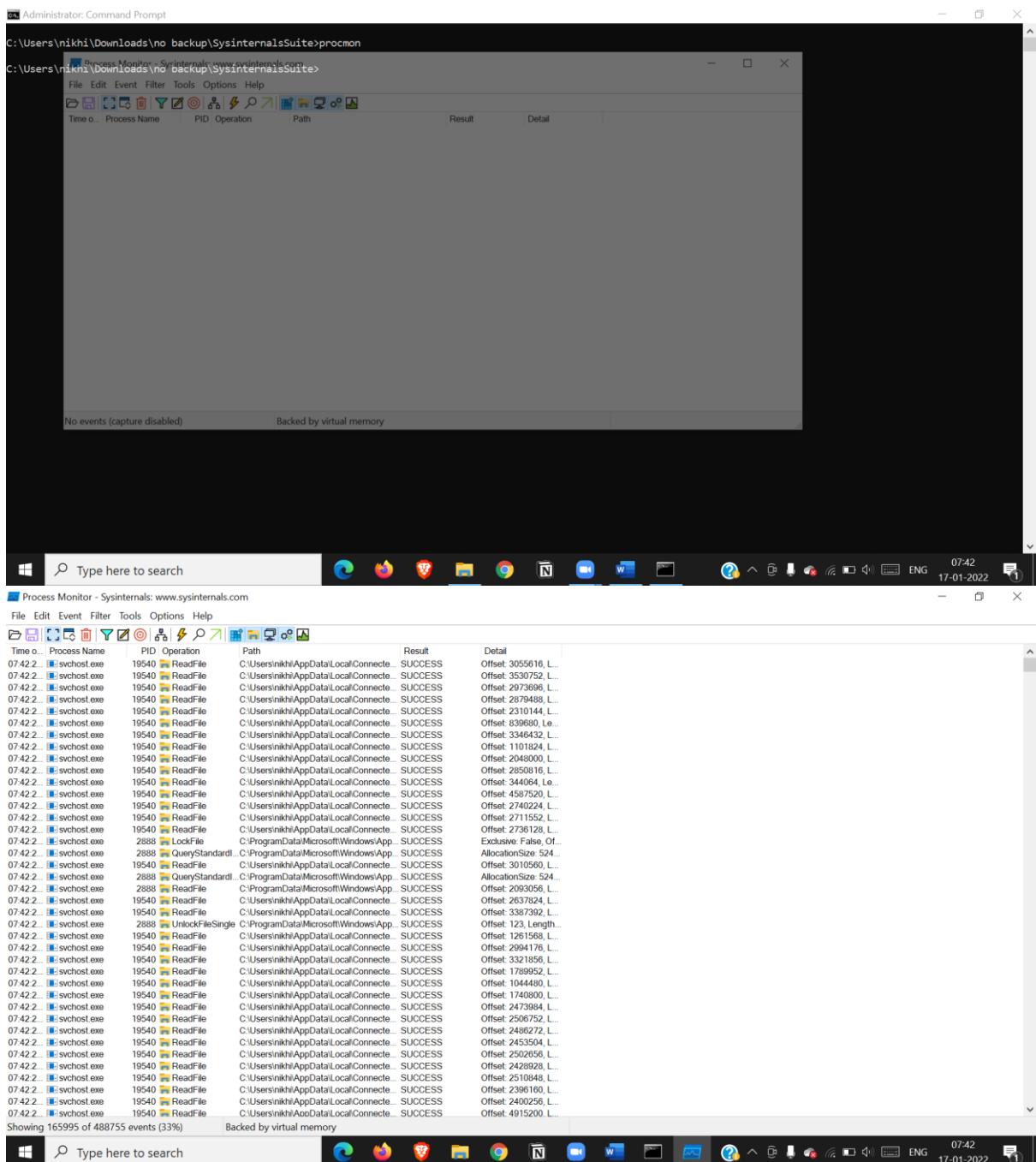
The Sysinternals tools are divided into six categories: File and Disk Utilities, Networking Utilities, Processes Utilities, Security Utilities, System Information and Miscellaneous Utilities. There are many tools, but the widely known are **AutoRuns, Process Monitor, Process Explorer, TCPView and RootkitRevealer**.



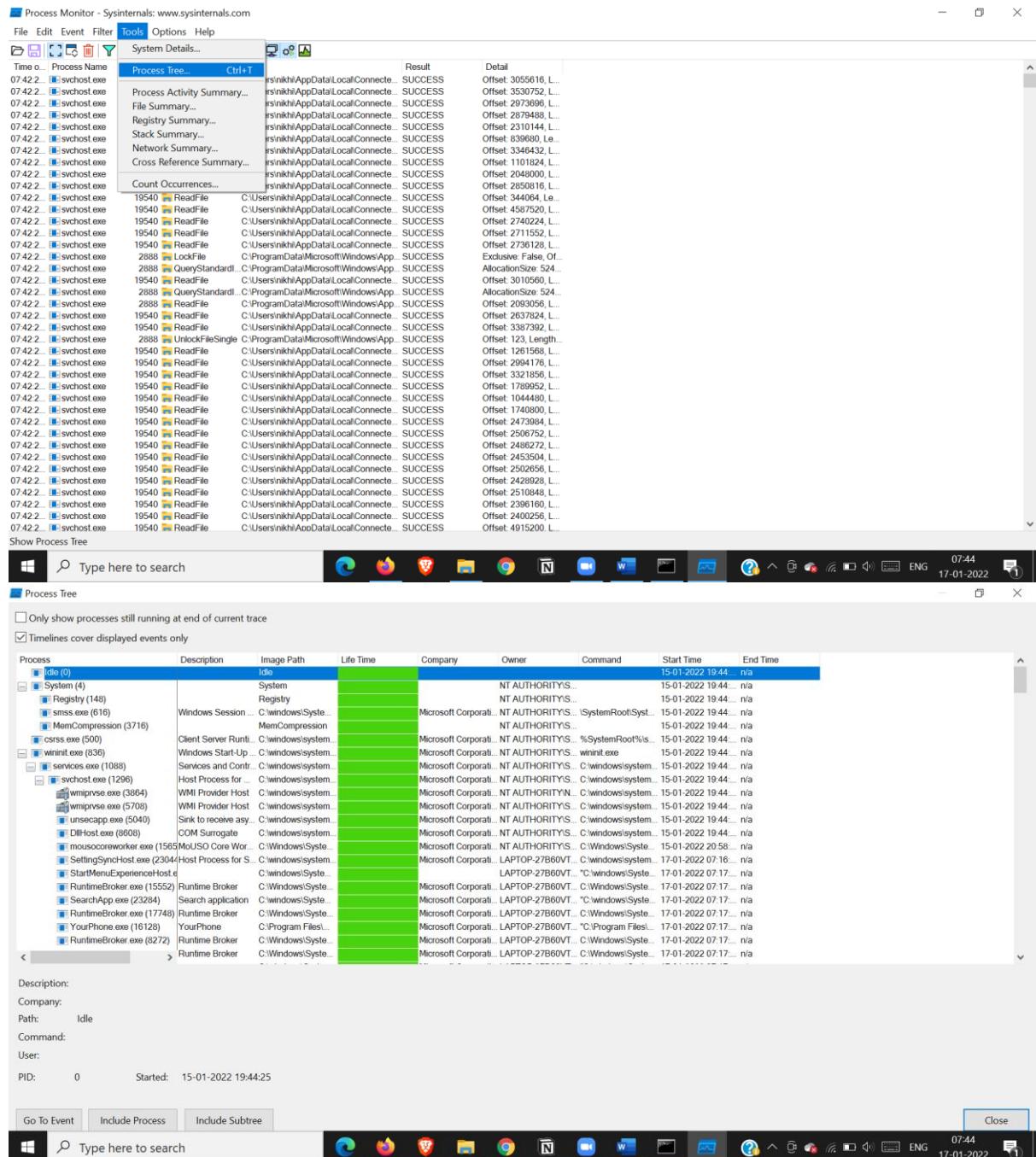
CYBER FORENSICS PRACTICALS



CYBER FORENSICS PRACTICALS

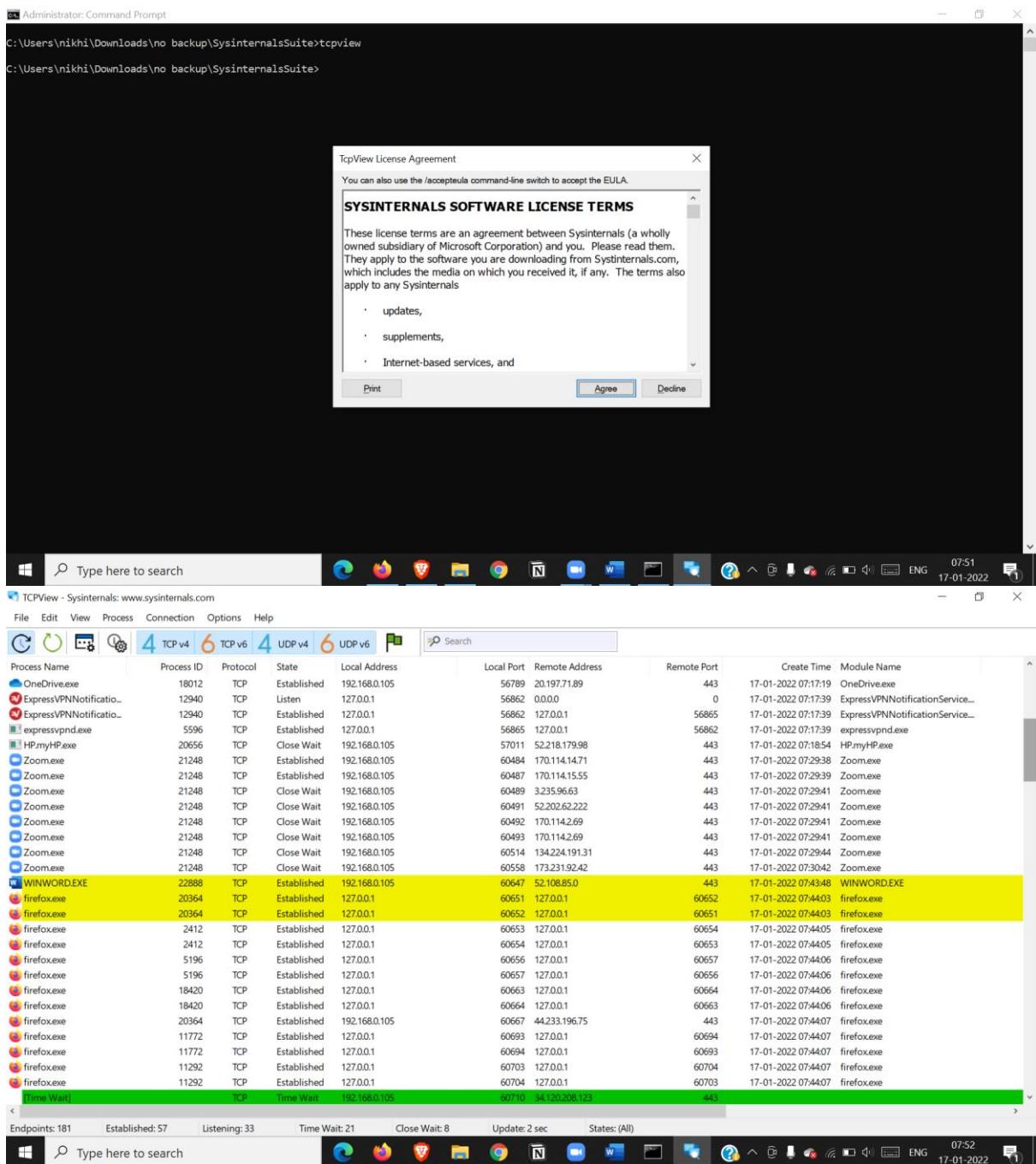


CYBER FORENSICS PRACTICALS



Tcp -udp packets

CYBER FORENSICS PRACTICALS



CYBER FORENSICS PRACTICALS

TCView - Sysinternals: www.sysinternals.com

File Edit View Process Connection Options Help

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

Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Time	Module Name
svchost.exe	11752	UDP	192.168.140.1		62421	*		17-01-2022 07:16:55	SSDPSPRV
svchost.exe	11752	UDP	192.168.105		62422	*		17-01-2022 07:16:55	SSDPSPRV
svchost.exe	11752	UDP	127.0.0.1		62423	*		17-01-2022 07:16:55	SSDPSPRV
svchost.exe	5160	UDP	127.0.0.1		62789	*		15-01-2022 19:44:36	iphlpvc
svchost.exe	4996	UDPv6	:		500	*		15-01-2022 19:44:36	IKEEXT
svchost.exe	11752	UDPV6	:		1900	*		17-01-2022 07:16:55	SSDPSPRV
svchost.exe	11752	UDPv6	fe80::3c2db07fd8b7c1		1900	*		17-01-2022 07:16:55	SSDPSPRV
svchost.exe	11752	UDPv6	fe80::3c2db07fd8b7c1		1900	*		17-01-2022 07:16:55	SSDPSPRV
svchost.exe	11752	UDPv6	fe80::3c2db07fd8b7c1		1900	*		17-01-2022 07:16:55	SSDPSPRV
svchost.exe	2012	UDPv6	:		3702	*		17-01-2022 07:16:55	FDResPub
svchost.exe	2012	UDPv6	:		3702	*		17-01-2022 07:18:45	FDResPub
svchost.exe	4996	UDPv6	:		4500	*		15-01-2022 19:44:36	IKEEXT
svchost.exe	2628	UDPv6	:		5353	*		17-01-2022 07:16:55	Dnscache
TeamViewer_Service.exe	5328	UDPv6	fe80::3c2db07fd8b7c1		5353	*		15-01-2022 19:44:39	TeamViewer
TeamViewer_Service.exe	5328	UDPv6	fe80::3c2db07fd8b7c1		5353	*		15-01-2022 19:44:39	TeamViewer
svchost.exe	2628	UDPv6	:		5355	*		17-01-2022 07:47:08	Dnscache
TeamViewer_Service.exe	5328	UDPv6	:		49682	*		15-01-2022 19:44:39	TeamViewer
svchost.exe	2012	UDPv6	:		60093	*		15-01-2022 20:38:02	FDResPub
svchost.exe	11752	UDPv6	fe80::fc8c93c53f659170		62416	*		17-01-2022 07:16:55	SSDPSPRV
svchost.exe	11752	UDPv6	fe80::3c2db07fd8b7c1		62417	*		17-01-2022 07:16:55	SSDPSPRV
svchost.exe	11752	UDPv6	fe80::c1ae6da0af24c1d7		62418	*		17-01-2022 07:16:55	SSDPSPRV
svchost.exe	11752	UDPV6	:		62419	*		17-01-2022 07:16:55	SSDPSPRV
brave.exe	21308	TCP	Syn Sent	127.0.0.1	61780	127.0.0.1	3500	17-01-2022 07:56:44	brave.exe
brave.exe	21308	TCP	Syn Sent	127.0.0.1	61781	127.0.0.1	3500	17-01-2022 07:56:45	brave.exe
brave.exe	21308	TCP	Syn Sent	127.0.0.1	61783	127.0.0.1	3500	17-01-2022 07:56:46	brave.exe
brave.exe	21308	TCP	Syn Sent	127.0.0.1	61785	127.0.0.1	50000	17-01-2022 07:56:46	brave.exe
brave.exe	21308	TCPv6	Syn Sent	:	61782	:1	50000	17-01-2022 07:56:46	brave.exe
brave.exe	21308	TCPv6	Syn Sent	:	61784	:1	3500	17-01-2022 07:56:46	brave.exe

Endpoints: 133 Established: 20 Listening: 33 Time Wait: 15 Close Wait: 5 Update: 2 sec States: (All)

Type here to search

Windows Taskbar: 07:56 17-01-2022

Firefox Process Properties window showing multiple Firefox instances and a Whois... option.

Whois: server-13-227-165-134.bom51.r.cloudfront.net

Domain Name: CLOUDFRONT.NET
 Registry Domain ID: 1457834866_DOMAIN_NET-VRSN
 Registrar WHOIS Server: whois.markmonitor.com
 Registrar URL: http://www.markmonitor.com
 Updated Date: 2019-05-07T23:07:15Z
 Creation Date: 2008-04-25T18:25:49Z
 Registry Expiry Date: 2024-04-25T18:25:49Z
 Registrar: MarkMonitor Inc.
 Registrar IANA ID: 292
 Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
 Registrar Abuse Contact Phone: +1.2083895740
 Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
 Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
 Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
 Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
 Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
 Name Server: NS-1306.AWSDNS-35.ORG
 Name Server: NS-1597.AWSDNS-07.CO.UK
 Name Server: NS-418.AWSDNS-52.COM
 Name Server: NS-666.AWSDNS-19.NET
 DNSSEC: unsigned

OK

Established 192.168.0.105 00:07 170.114.15.55 04:43

Diskmonitoring

CYBER FORENSICS PRACTICALS

Administrator: Command Prompt
Microsoft Windows [Version 10.0.19042.1466]
(c) Microsoft Corporation. All rights reserved.
C:\windows\system32>cd C:\Users\nikhil\Downloads\no backup\SysinternalsSuite
C:\Users\nikhil\Downloads\no backup\SysinternalsSuite>diskmon
C:\Users\nikhil\Downloads\no backup\SysinternalsSuite>

Diskmon License Agreement
You can also use the /accepteula command-line switch to accept the EULA.

SYSINTERNAIS SOFTWARE LICENSE TERMS

These license terms are an agreement between Sysinternals (a wholly owned subsidiary of Microsoft Corporation) and you. Please read them. They apply to the software you are downloading from Sysinternals.com, which includes the media on which you received it, if any. The terms also apply to any Sysinternals

- updates,
- supplements,
- Internet-based services, and

Print Agree Decline

Type here to search

Disk Monitor - Sysinternals: www.sysinternals.com

File Edit Options Help

#	Time	Duration (s)	Disk	Request	Sector	Length
31	0.635766	0.0000000	0	Write	6723848	16
32	0.635921	0.0000000	0	Write	89388956	40
33	0.636108	0.0000000	0	Write	6723984	8
34	0.665266	0.0000000	0	Write	34796448	8
35	1.317657	0.0000000	0	Read	26177600	32
36	1.320517	0.0000000	0	Read	26177528	8
37	1.919460	0.0000000	0	Write	89504080	16
38	1.919659	0.0000000	0	Write	82497880	264
39	1.919824	0.0000000	0	Write	54434728	240
40	1.919914	0.0000000	0	Write	119003752	80
41	2.233370	0.0000000	0	Read	244494040	8
42	2.251387	0.0000000	0	Read	244494832	8
43	2.667375	0.0000000	0	Read	232888664	64
44	3.064582	0.0000000	0	Read	19604824	16
45	3.074780	0.0000000	0	Read	9082048	16
46	3.081691	0.0000000	0	Read	20304364	56
47	3.082516	0.0000000	0	Read	195723293	24
48	3.083797	0.0000000	0	Read	194842034	32
49	3.281178	0.0000000	0	Write	10054008	8
50	3.281272	0.0000000	0	Write	130835608	48
51	3.281734	0.0000000	0	Write	3638528	8
52	3.282087	0.0000000	0	Write	154181656	8
53	3.282354	0.0000000	0	Write	6831848	16
54	3.282491	0.0000000	0	Write	6723848	48
55	3.283485	0.0000000	0	Write	89939456	16
56	3.283617	0.0000000	0	Write	188324304	8
57	3.283736	0.0000000	0	Write	188359864	8
58	3.283851	0.0000000	0	Write	206838984	8
59	3.283969	0.0000000	0	Write	206880624	16
60	3.284083	0.0000000	0	Write	206882024	8
61	3.284209	0.0000000	0	Write	206882616	16
62	3.284324	0.0000000	0	Write	6858760	8
63	3.284436	0.0000000	0	Write	6859596	8
64	3.284546	0.0000000	0	Write	6862304	8
65	3.284656	0.0000000	0	Write	6868144	8
66	3.284775	0.0000000	0	Write	6869432	8

Practical 7

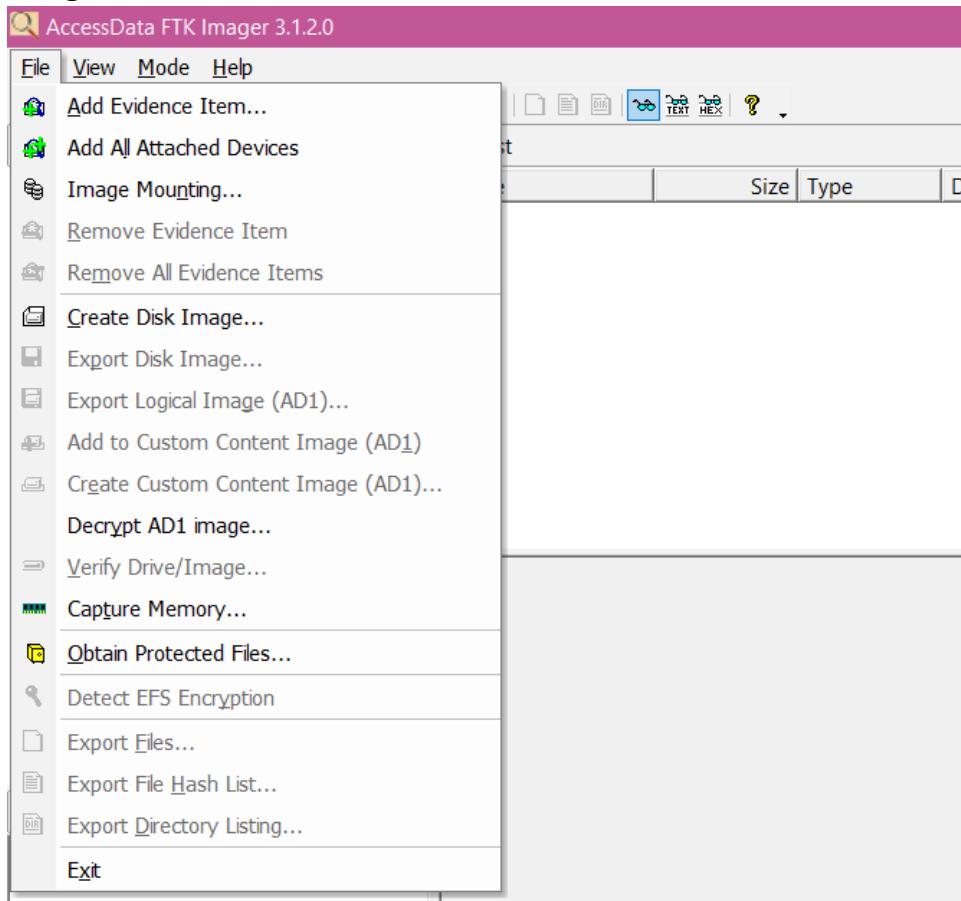
Aim: Recovering and Inspecting the recovered files.

I) Check for deleted files.

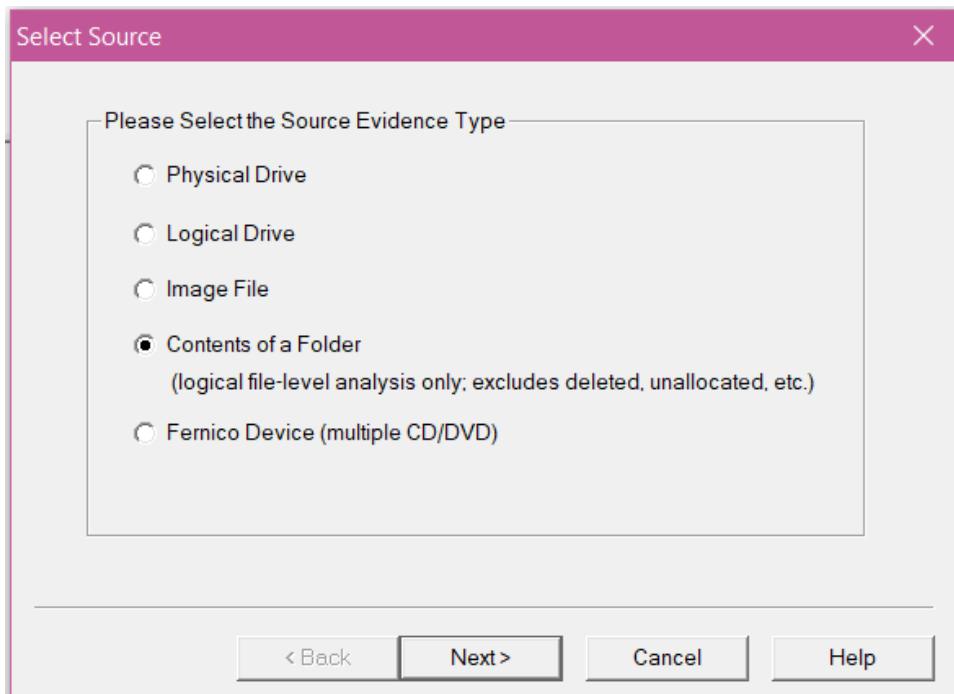
II) Recover the Deleted Files.

Steps:

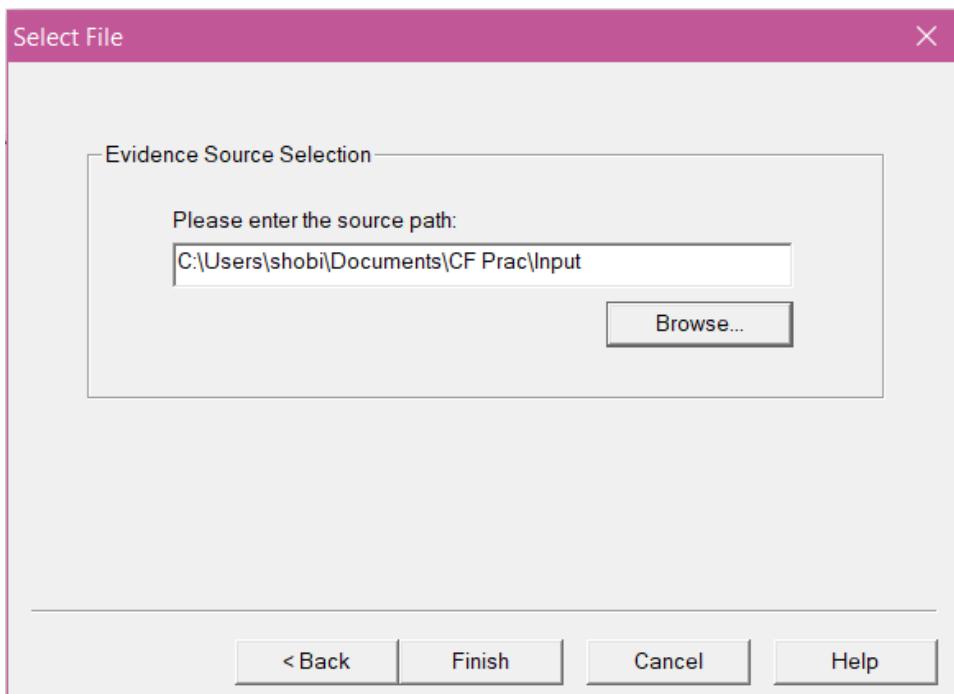
- 1) First, create a text file and paste some data in it and store it in a folder.
- 2) Open AccessData FTK Imager then click on file and select “Create Disk image”.



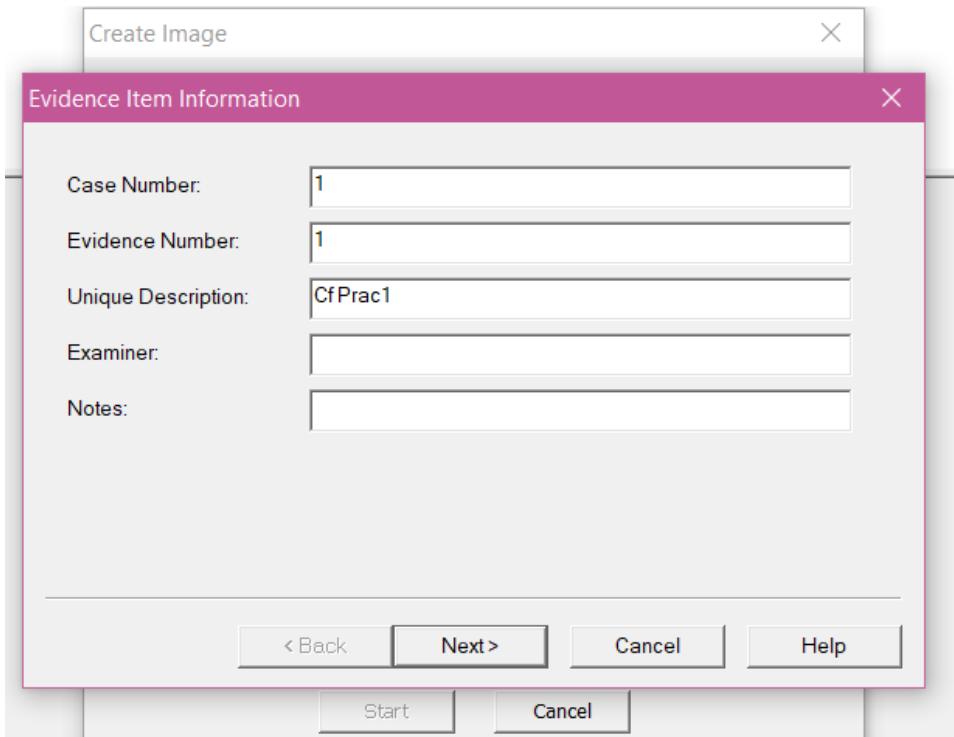
- 3) Select source as Content of a folder and click on next.



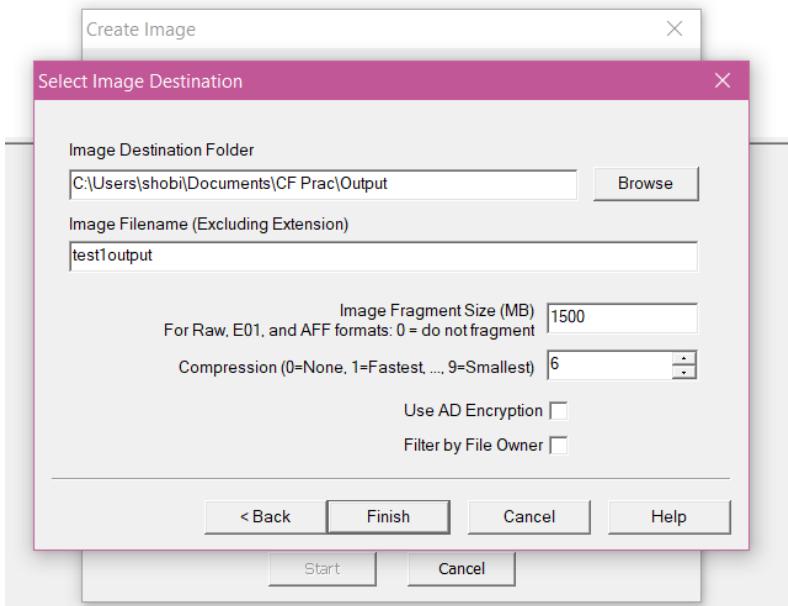
- 4) Then browse the source evidence that we created previously as a text file then click on finish.



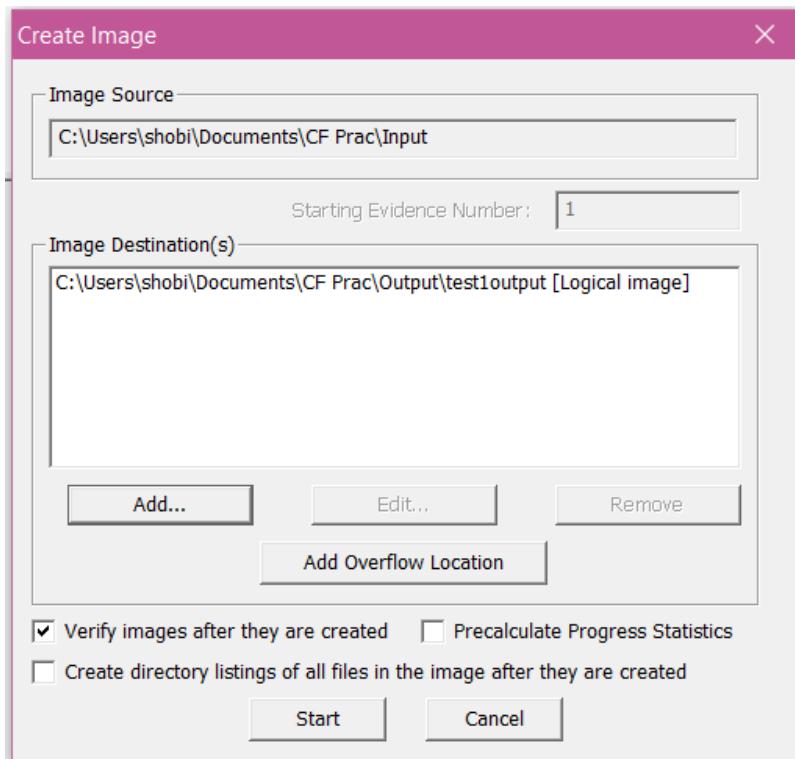
- 5) Enter the evidence item information and click on next.



6) Then browse the image destination folder and name the image file and click on finish.



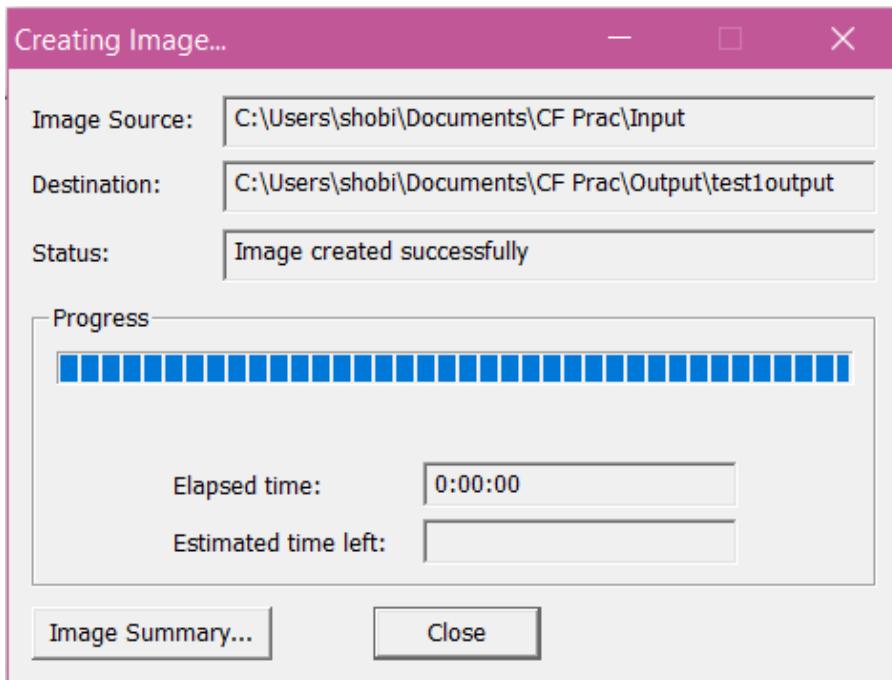
7) For creating an image, click on start.



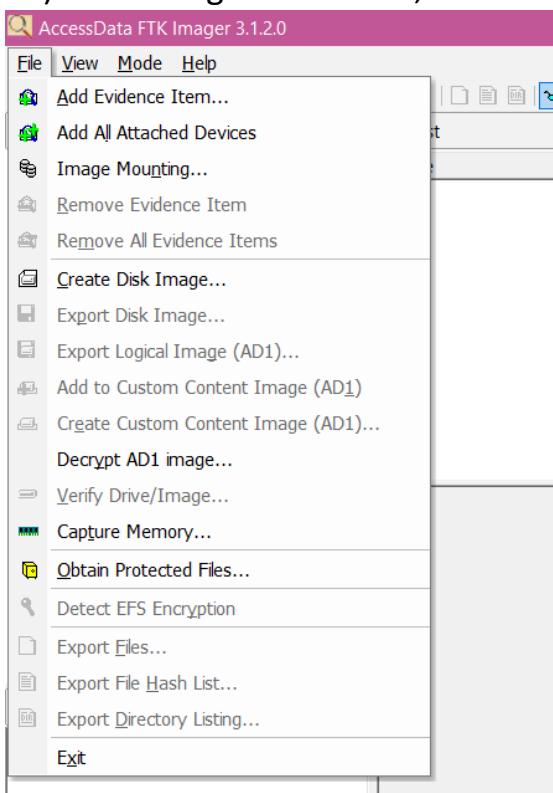
8) As we get the result, we can verify by looking at the verify result of both the hashing functions.

Drive/Image Verify Results	
	Name
	test1output.ad1
	MD5 Hash
	Computed hash
	a0da3cc21077c95da42568927fb16646
	Report Hash
	a0da3cc21077c95da42568927fb16646
	Verify result
	Match
	SHA1 Hash
	Computed hash
	b9ee7e734a0fbb67a57e364b1f8ab90673
	Report Hash
	b9ee7e734a0fbb67a57e364b1f8ab90673
	Verify result
	Match
Close	

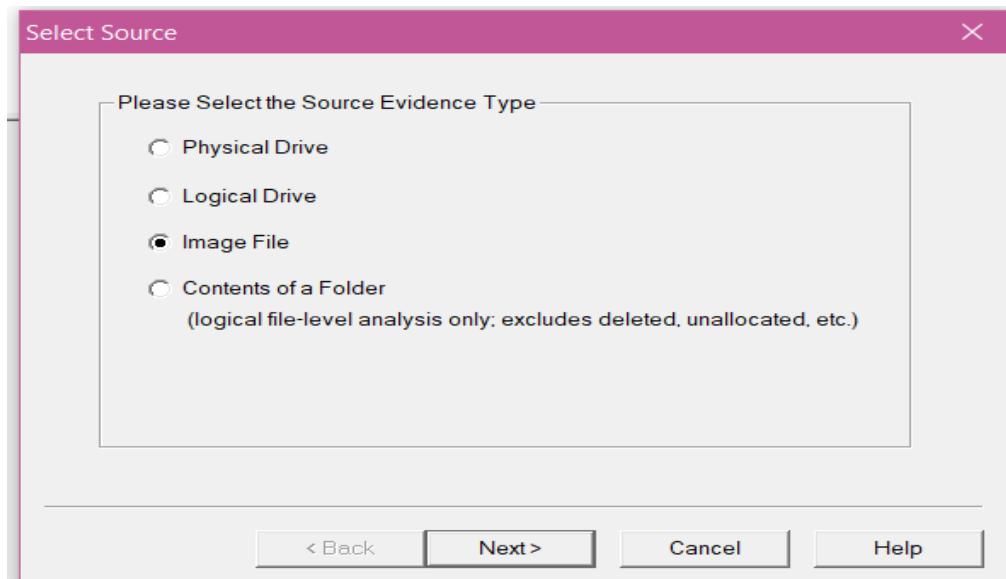
9) Atlast, we get the status of the creation and we can also view image summary.



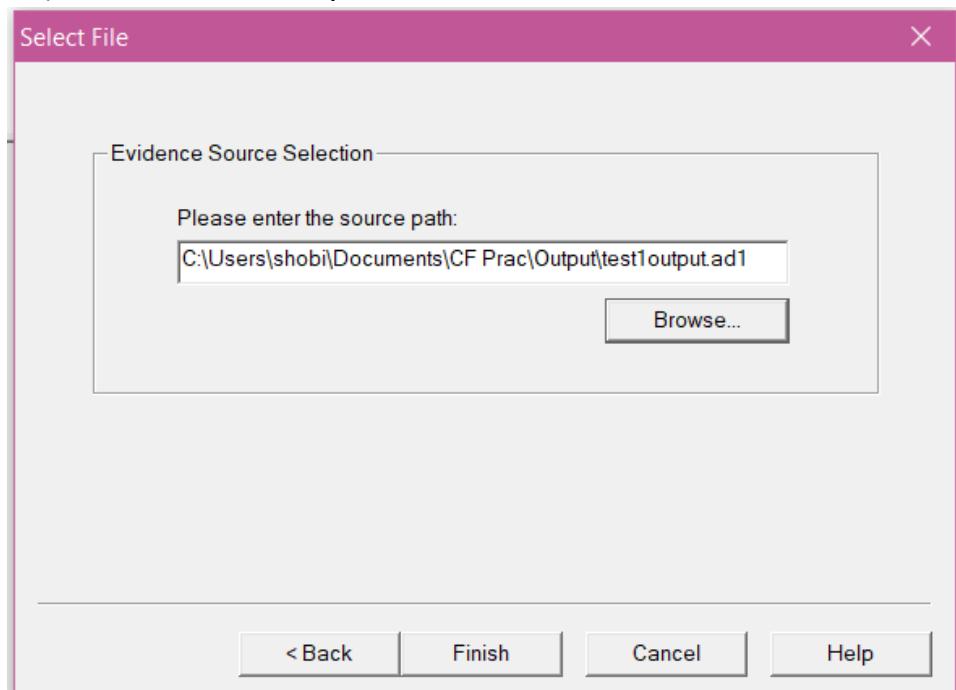
10) For adding an evidence, select “Add evidence item”.



11) Select source as image file and click on next.

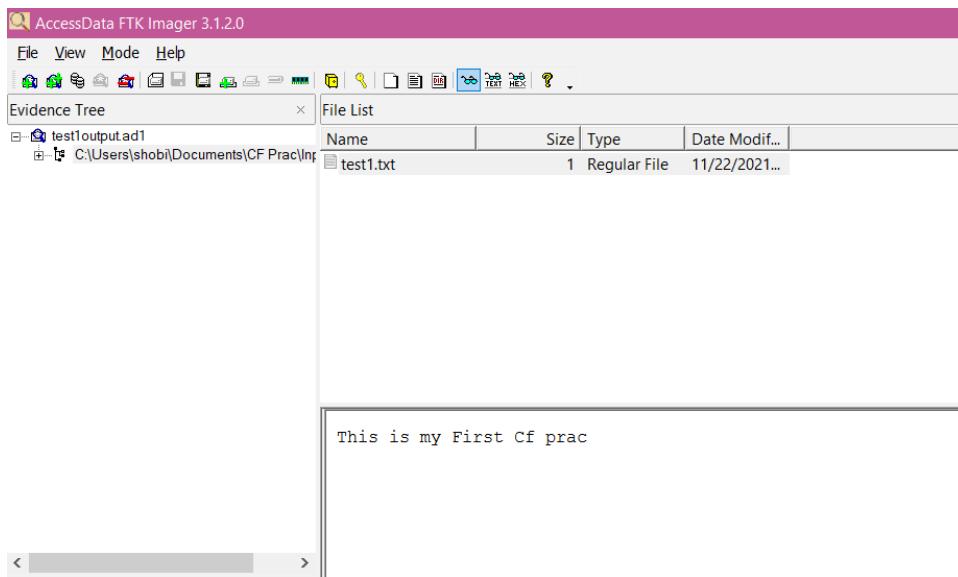


12) Then browse the path of the evidence source and click on finish.



13) In the evidence tree we can see the image file that we created.

CYBER FORENSICS PRACTICALS



III) Analyzing and inspecting the recovered files.

Perform this using recovery option in ENCASE and also Perform manually through command line.

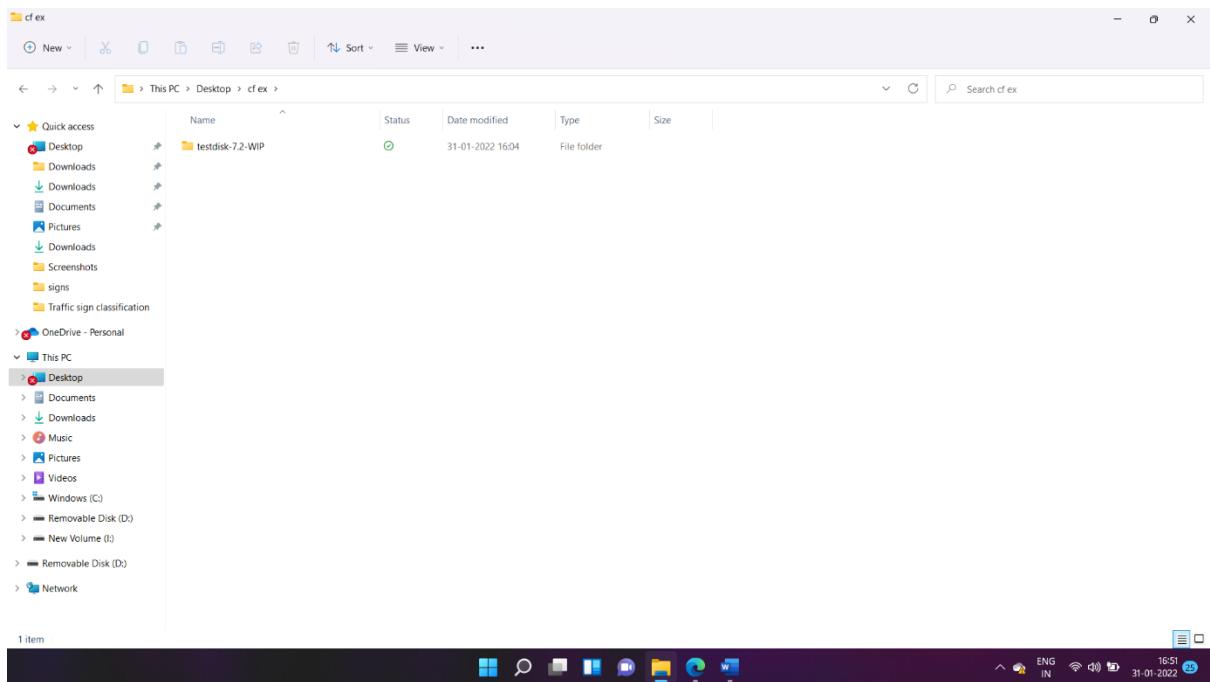
Steps:

1) Download TestDisk zip file.

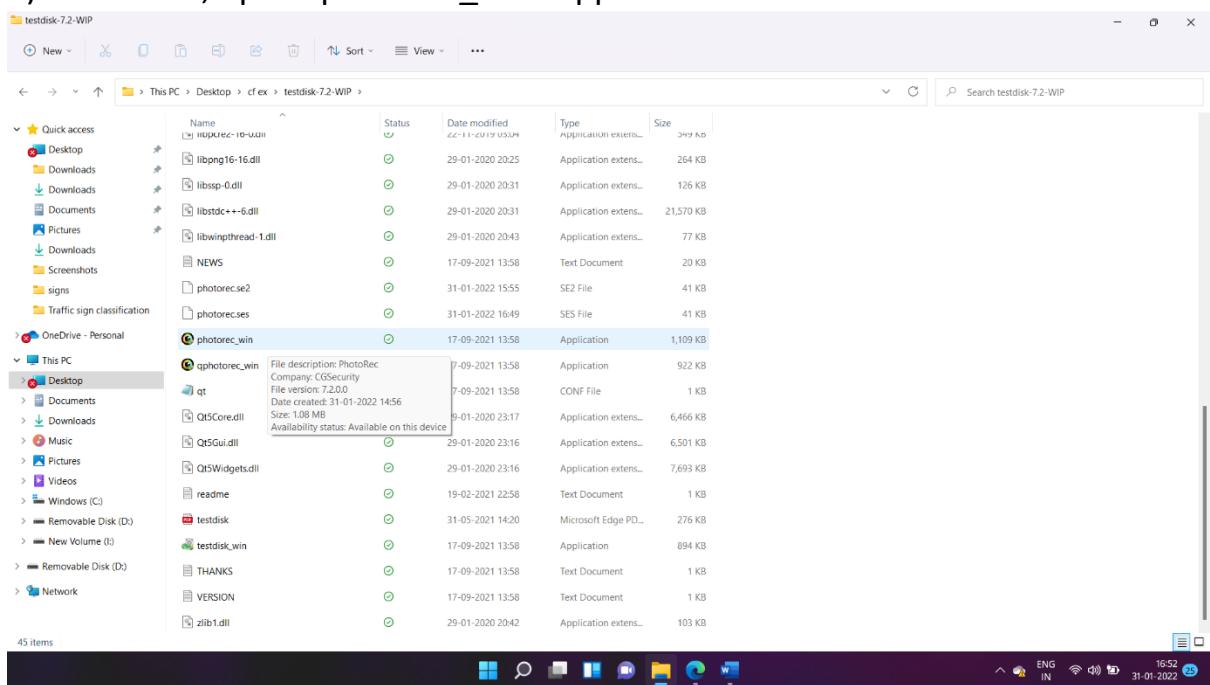
A screenshot of a web browser window. The address bar shows "TestDisk Download - CGSecurity" and the URL "https://www.cgsecurity.org/wiki/TestDisk_Download". The page content is about the TestDisk & PhotoRec data recovery tools. It includes a sidebar with links like "download", "Forum", "Donate", "Password recovery", "CmosPwd", "Lilo Password", "Chntpw for dos", "Security", "Publications", "Misc", "Mon CV (FR)", "PGP Public Key", "Euro coins", "Roller", "Links", "Share", and "Create Professional Invoices". The main content area has sections for "Beta: TestDisk & PhotoRec 7.2-WIP, Data Recovery" and "TestDisk 7.2-WIP Free download Windows". It lists supported operating systems: Dos/Win95/Win98, Windows (32-bit and 64-bit), Linux (32-bit and 64-bit), Mac OS X Intel (32-bit and 64-bit), and Mac OS X Intel 32-bit / OS X / macOS. A note mentions Marvell 88F628x Linux 2.6.32 support for Synology DS111, DS211, DS212+ NAS, Seagate BlackArmor NAS 220, QNAP ARM based including TS-410, and aarch64-QNAP-linux-gnu support for QNAP aarch64 (ARM 64-bit). A "Source code" link is also present. At the bottom, there's a cookie consent banner: "Cookies help us deliver our services. Some cookies serve for direct advertising (data collection for ads personalisation). By using our services, you agree to our use of cookies." with "More information" and "OK" buttons.

2) Extract the downloaded file in a folder.

CYBER FORENSICS PRACTICALS



3) In that file, open “photorec_win” application.



4) Then select the pen drive that you attached to your PC and proceed.

CYBER FORENSICS PRACTICALS

```
PhotoRec 7.2-WIP, Data Recovery Utility, September 2021
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

PhotoRec is free software, and
comes with ABSOLUTELY NO WARRANTY.

Select a media (use Arrow keys, then press Enter):
Disk \\.\PhysicalDrive0 - 512 GB / 476 GiB (RO) - NVMe MTFDHBA512QFD-1AX1AABHA
>Disk \\.\PhysicalDrive1 - 16 GB / 15 GiB (RO) - hp v210w

>[Proceed] [ Quit ]

Note:
Disk capacity must be correctly detected for a successful recovery.
If a disk listed above has an incorrect size, check HD jumper settings and BIOS
detection, and install the latest OS patches and disk drivers.
```

5) Then select the drive with the name of your pen drive and proceed.

```
PhotoRec 7.2-WIP, Data Recovery Utility, September 2021
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

Disk \\.\PhysicalDrive1 - 16 GB / 15 GiB (RO) - hp v210w

Partition          Start        End    Size in sectors
  No partition      0   0   1 1961  47  6  31506432 [Whole disk]
> 1 P FAT32 LBA      3   48  30 1961  47  5  31455183 [NO NAME]

>[ Search ] [Options] [File Opt] [ Quit ]
Start file recovery
```

6) Then select on Other and proceed.

CYBER FORENSICS PRACTICALS

```
PhotoRec 7.2-WIP, Data Recovery Utility, September 2021
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

1 P FAT32 LBA          3 48 30 1961 47 5  31455183 [NO NAME]

To recover lost files, PhotoRec needs to know the filesystem type where the
file were stored:
 ext2/ext3 ] ext2/ext3/ext4 filesystem
> Other   ] FAT/NTFS/HFS+/ReiserFS/...
```

7) Select “Whole” for extracting files from whole partition and proceed.

```
PhotoRec 7.2-WIP, Data Recovery Utility, September 2021
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

1 P FAT32 LBA          3 48 30 1961 47 5  31455183 [NO NAME]

Please choose if all space needs to be analysed:
 Free     ] Scan for file from FAT32 unallocated space only
> Whole   ] Extract files from whole partition
```

8) Then for going to another directory or drive use left arrow key on your keyboard, then select the pen drive to store the deleted data.

```
PhotoRec 7.2-WIP, Data Recovery Utility, September 2021

Please select a destination to save the recovered files to.
Do not choose to write the files to the same partition they were stored on.
Keys: Arrow keys to select another directory
      C when the destination is correct
      Q to quit

d---r-x-- 328384 328384      0 24-Jan-2022 08:43 c
>drwxr-xr-x 197609 197121      0 1-Jan-1980 00:00 d
drwxrwx--- 18    18      0 24-Jan-2022 08:43 i
```

9) After reaching the destination, press C key on the keyboard. After that the process will start.

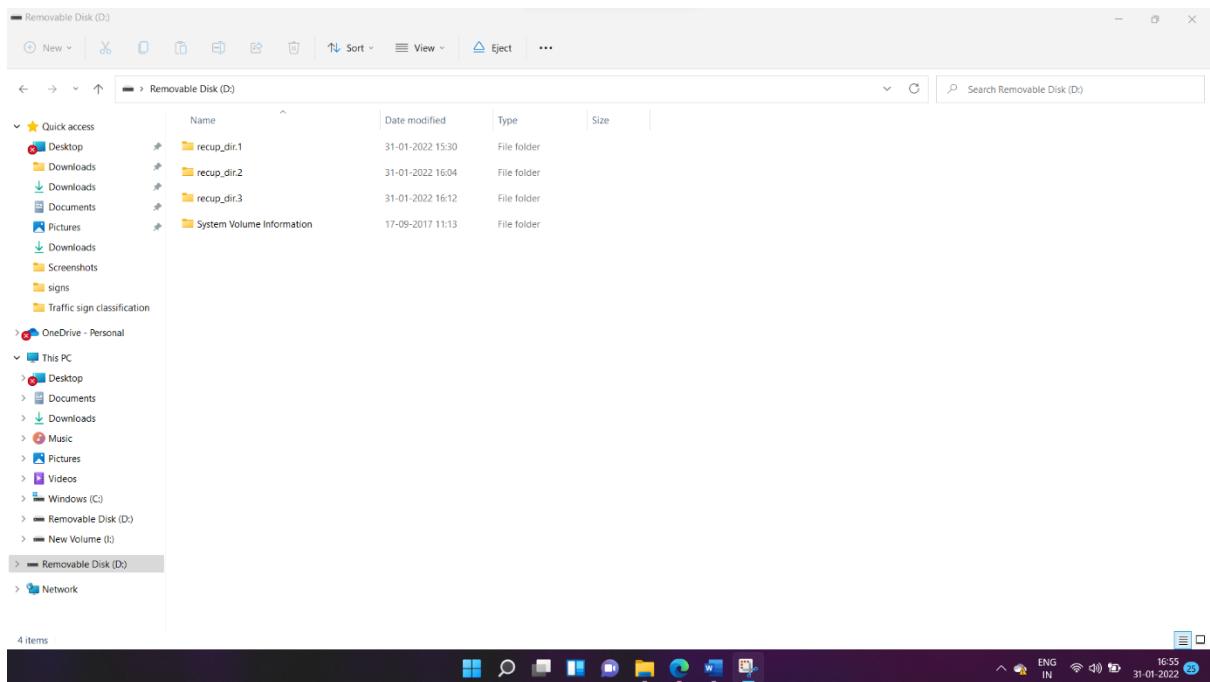
```
PhotoRec 7.2-WIP, Data Recovery Utility, September 2021

Please select a destination to save the recovered files to.
Do not choose to write the files to the same partition they were stored on.
Keys: Arrow keys to select another directory
      C when the destination is correct
      Q to quit
Directory D:\

>drwxrwxrwx  0  0   0          .
drwxrwxrwx  0  0   0          ..
drwxrwxrwx  0  0 1048576      $TXRAJNL.DAT
drwxrwxrwx  0  0 740833933     Gully Boy (2019).mkv
drwxrwxrwx  0  0 973681680     Kedarnath (2018) 720p WEB-DL x264 Hindi AAC 930MB [Www.MoviezAddicti
drwxrwxrwx  0  0 1152071275     Kesari (2019) Hindi 720p Pre-DVDRip x264 AAC - [Team MS].mkv
drwxrwxrwx  0  0 2874200      New.pptx
drwxrwxrwx  0  0   0          System Volume Information
drwxrwxrwx  0  0 20490        ipypaUDagN.vbs
drwxrwxrwx  0  0   0          recuper_dir.1
drwxrwxrwx  0  0   0          recuper_dir.2
drwxrwxrwx  0  0   0          recuper_dir.3
drwxrwxrwx  0  0 934540765     www.2MovieRulz.gs - URI The Surgical Strike (2019) 720p Hindi HDRip
drwxrwxrwx  0  0   165         ~$New.pptx
```

10) Atlast, we can see that the files that were deleted are successfully retrieved.

CYBER FORENSICS PRACTICALS

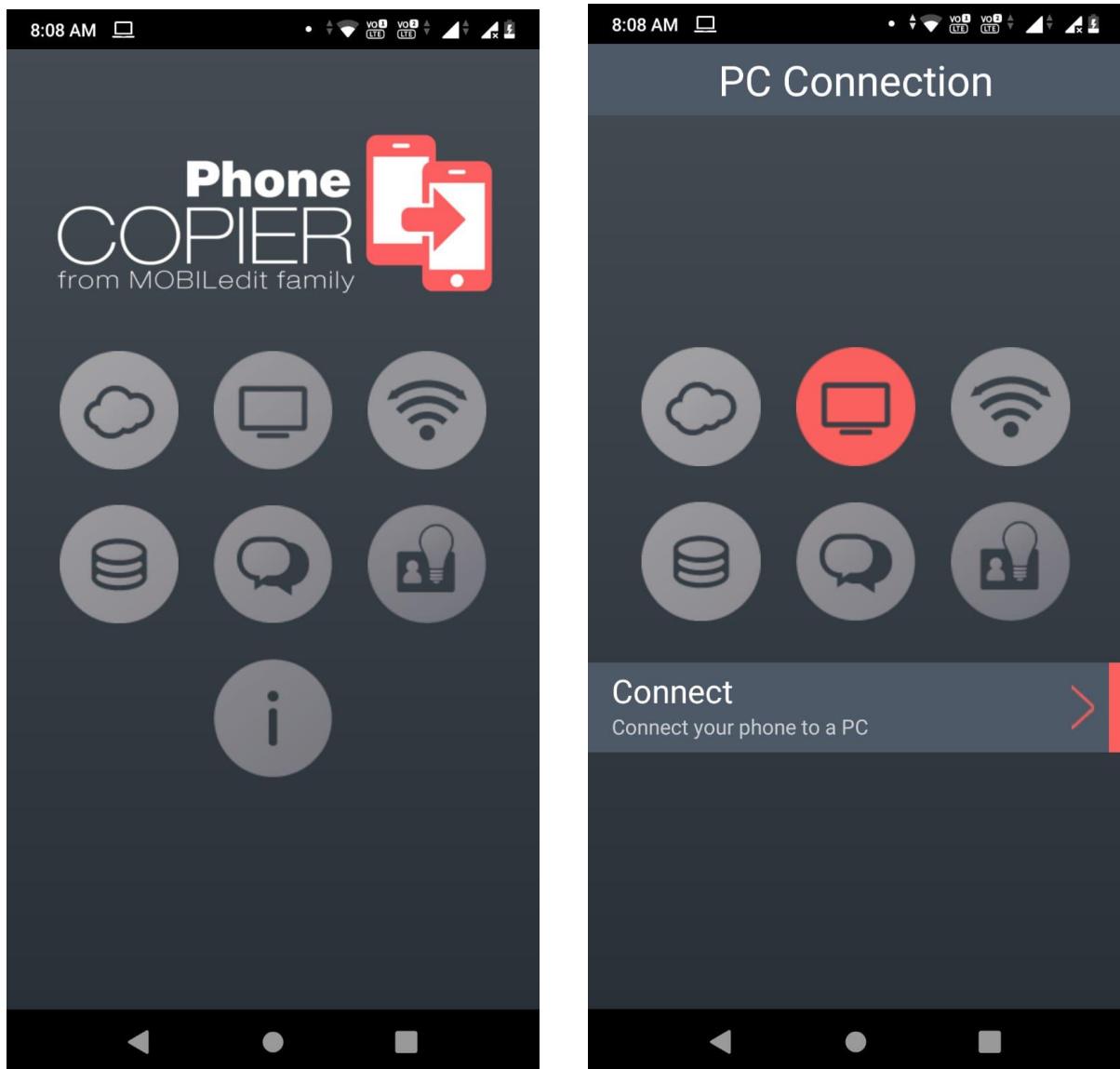


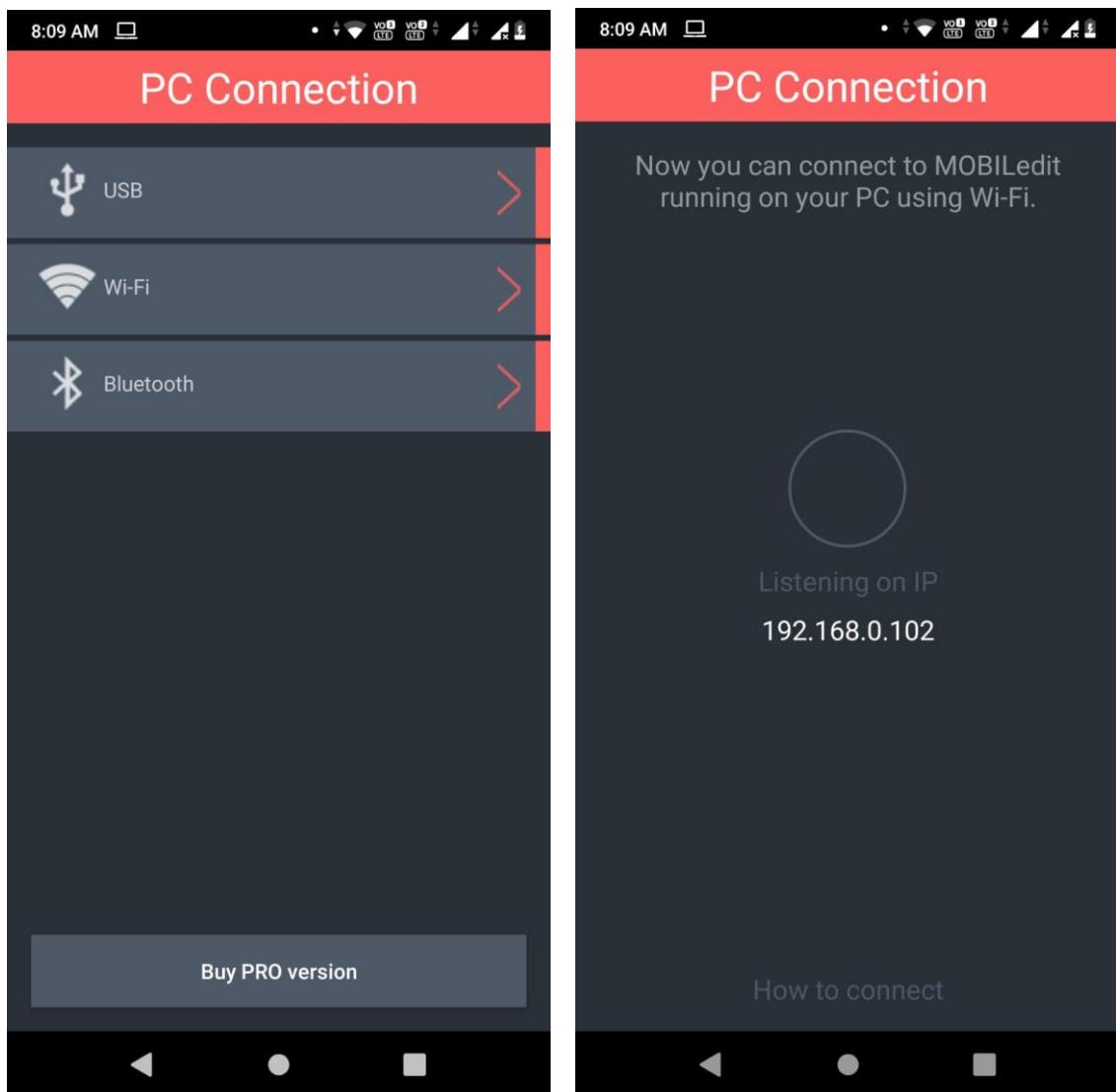
Practical:8

Aim: Acquisition of Cell phones and Mobile devices

MOBILE:

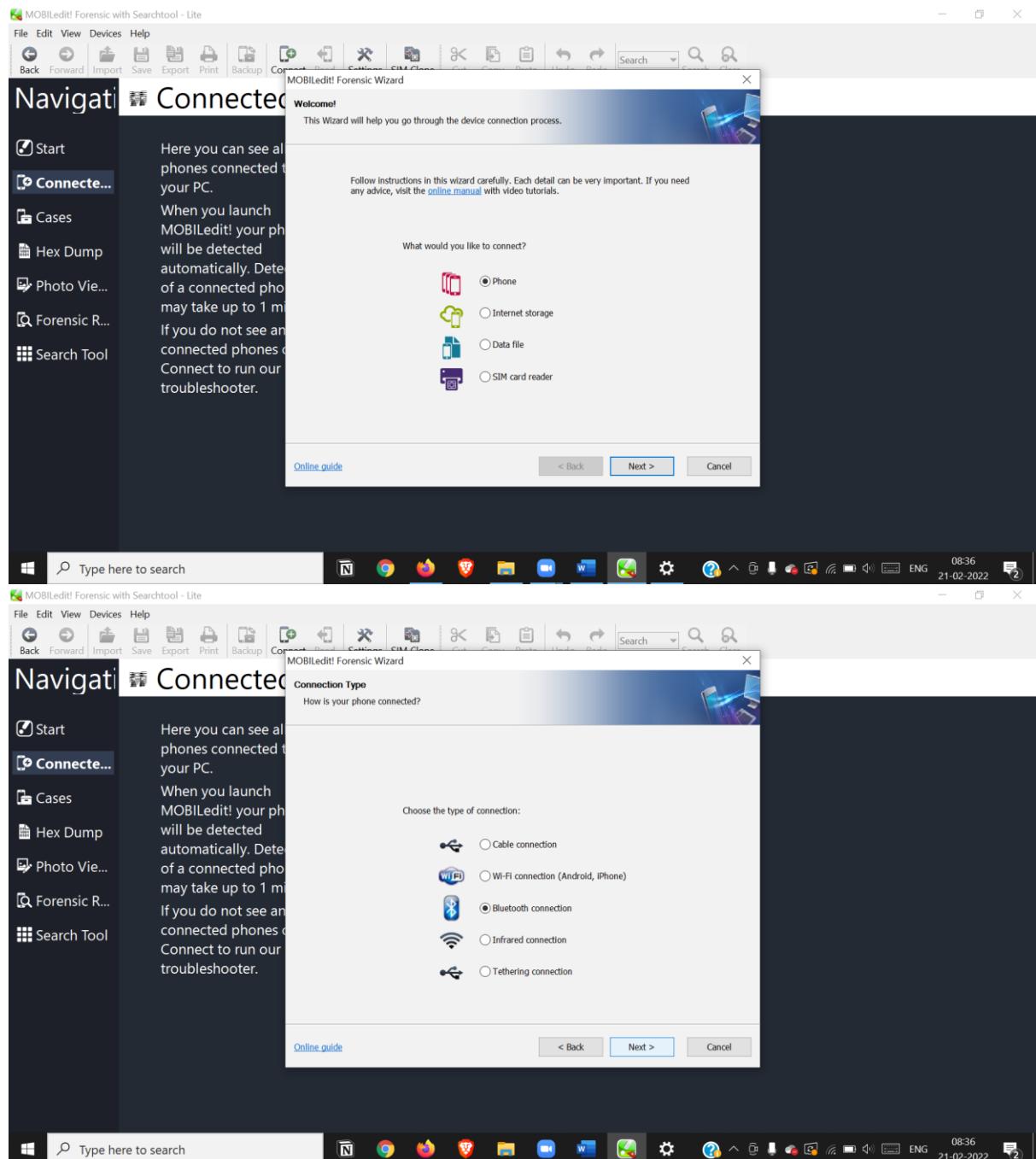
Download and install mobile edit on your android phone and connect to your pc



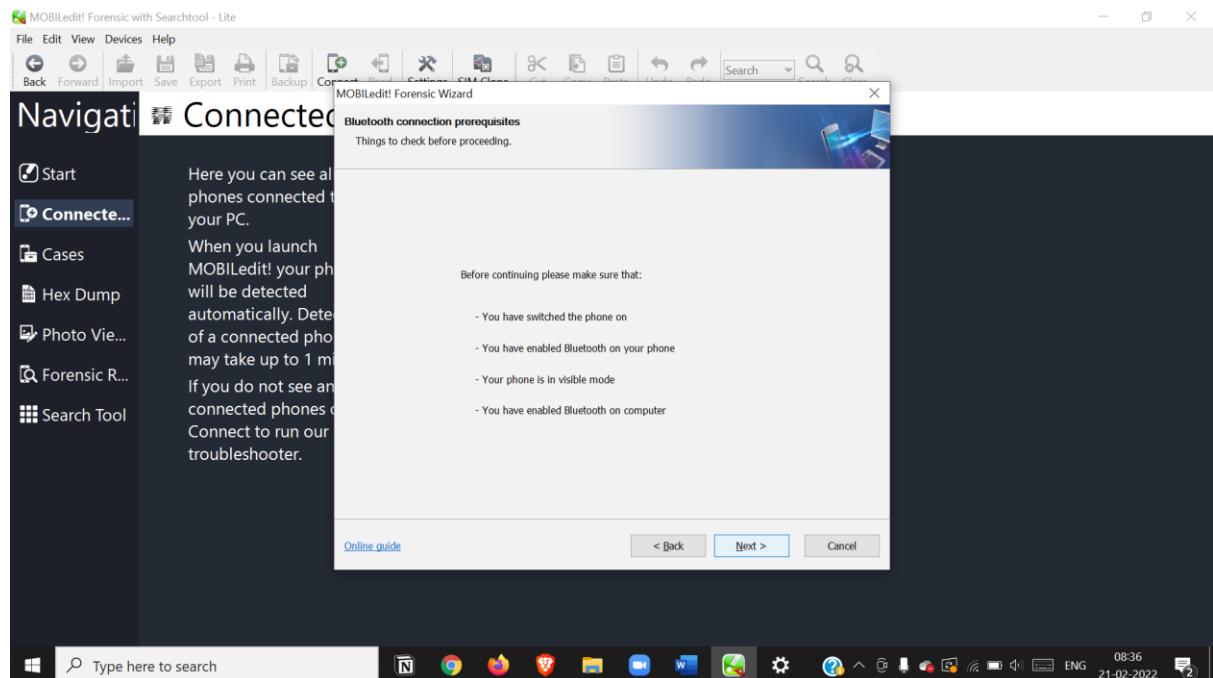


PC: Pair / connect with your pc using usb, Bluetooth or Wifi,
Then open MobileEdit in your pc

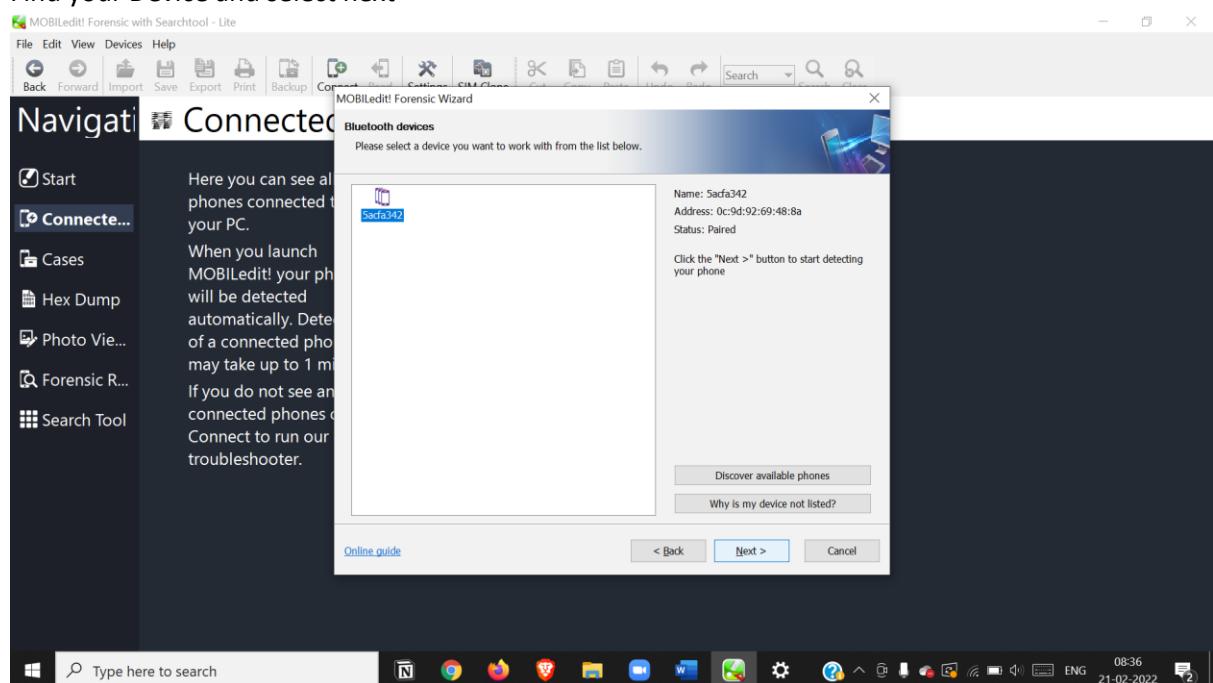
CYBER FORENSICS PRACTICALS



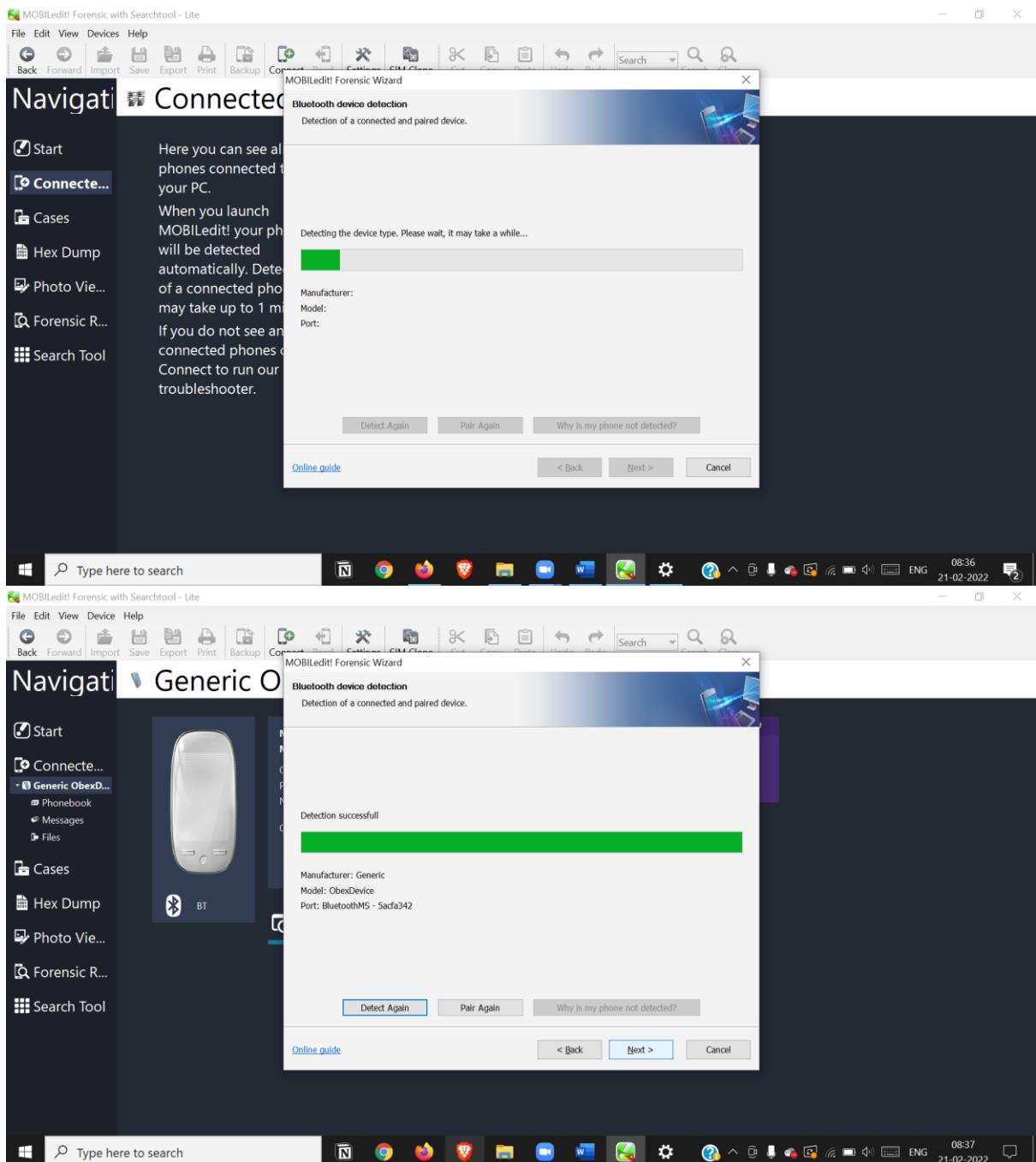
CYBER FORENSICS PRACTICALS



Find your Device and select next

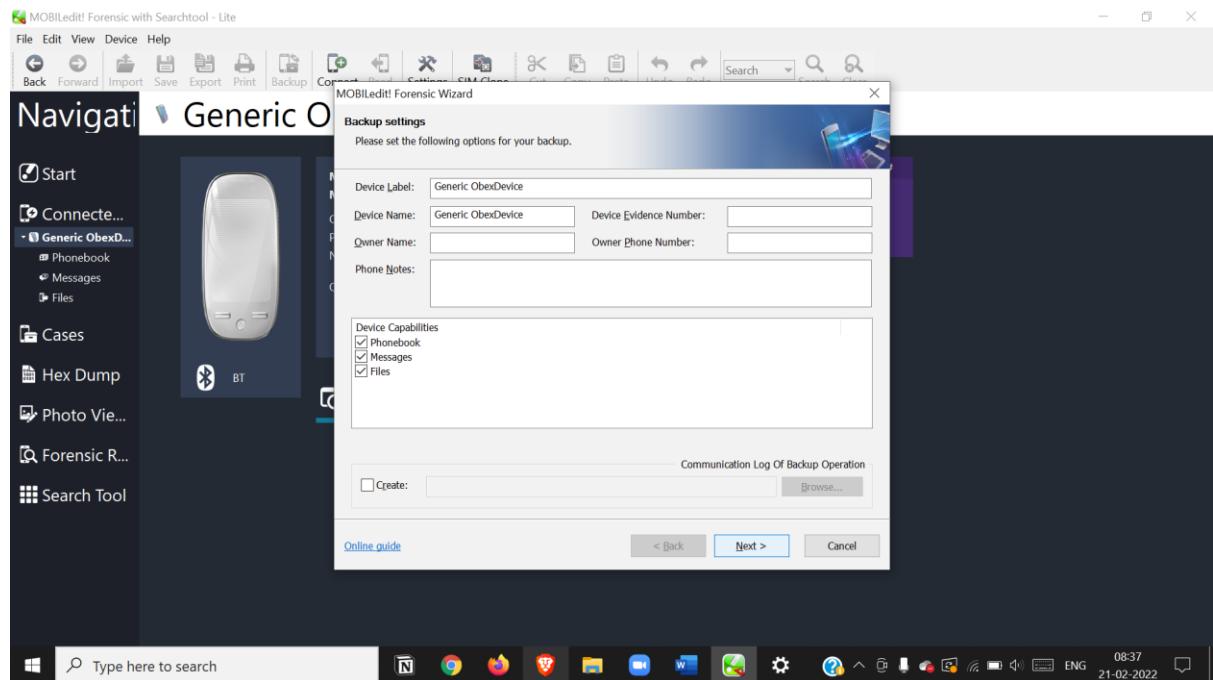


CYBER FORENSICS PRACTICALS

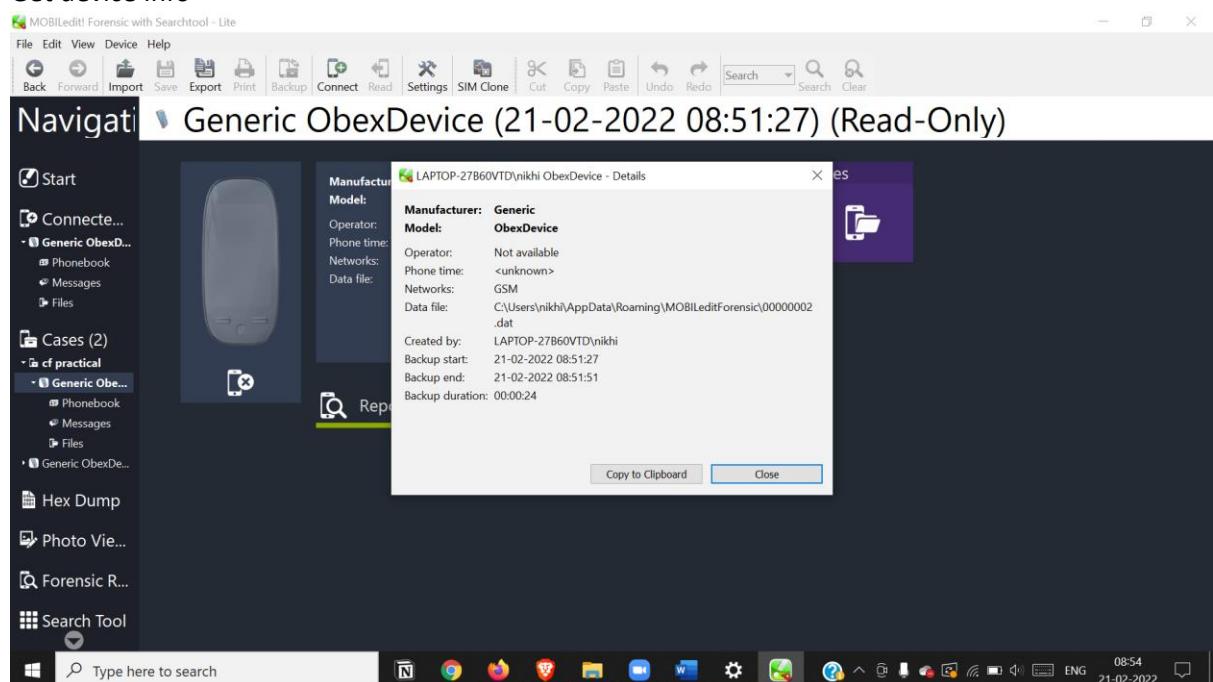


Set a Name for your device

CYBER FORENSICS PRACTICALS

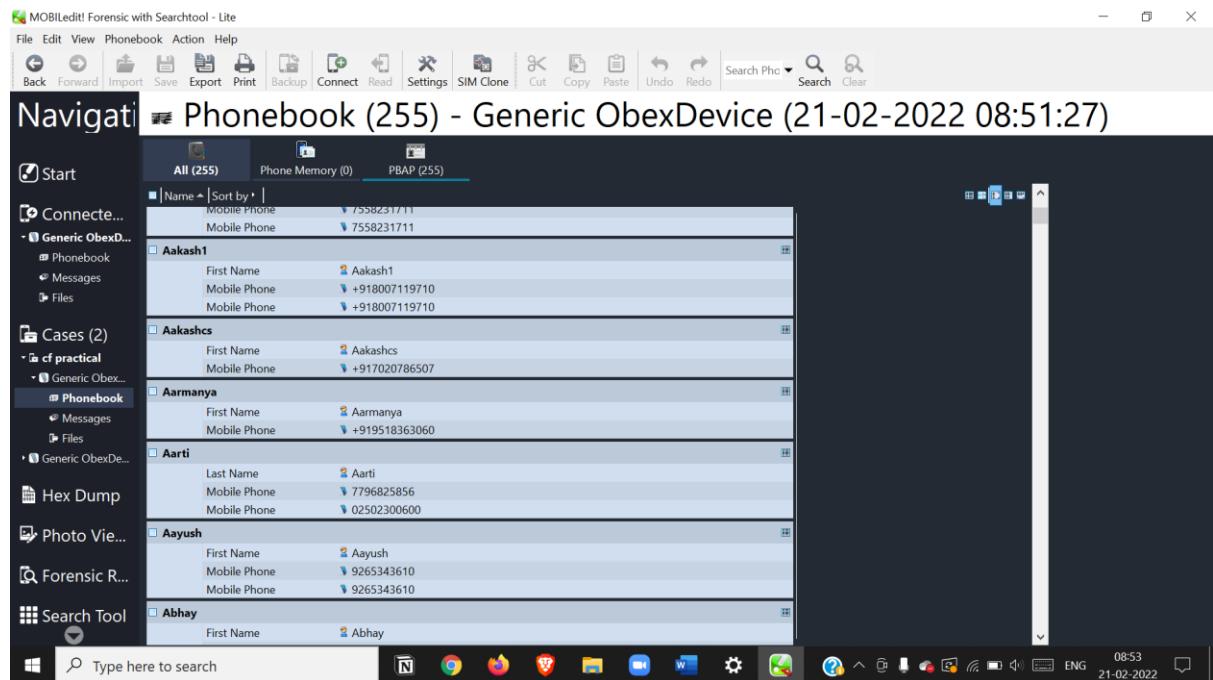


Get device Info

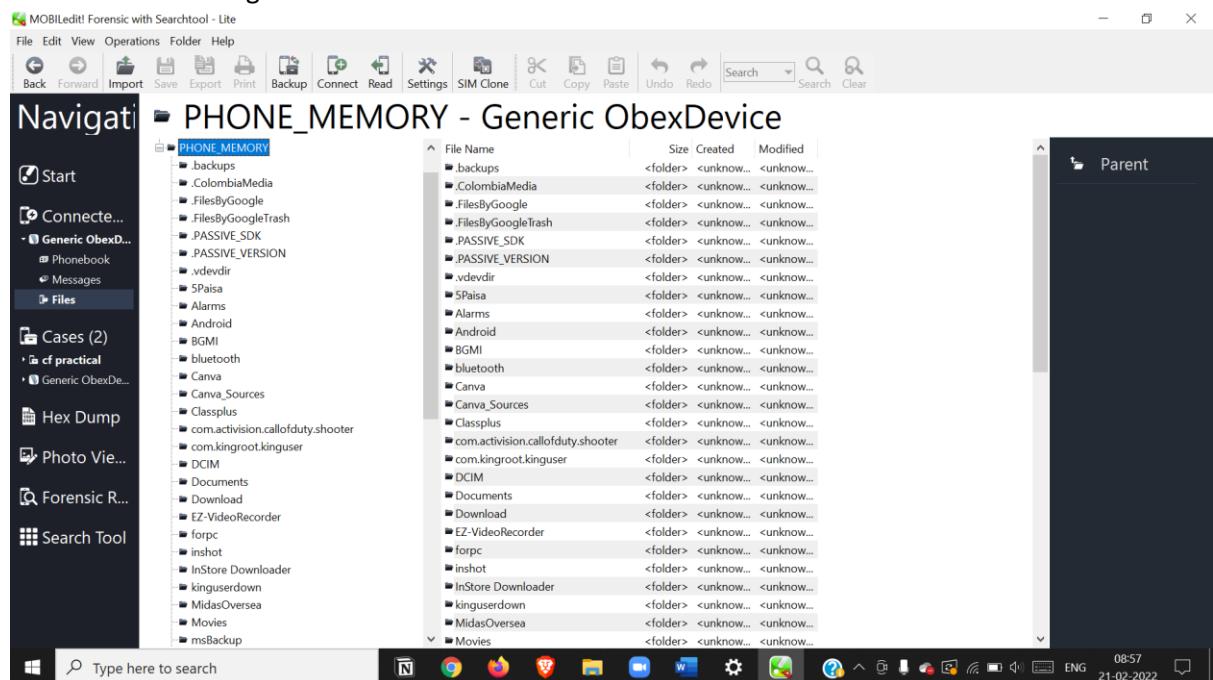


Get Phonebook Directory

CYBER FORENSICS PRACTICALS



Get Files and messages

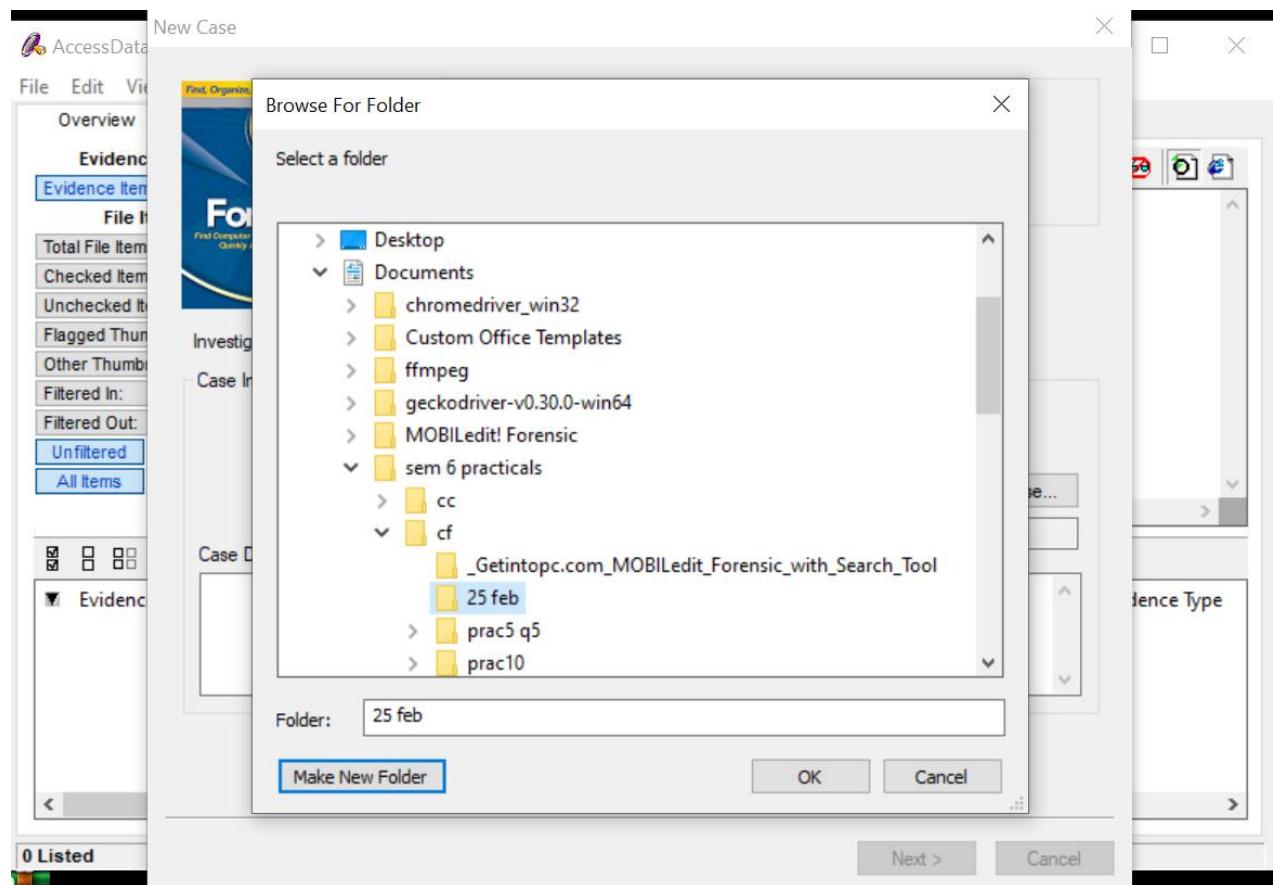


Practical 9

Aim: Email Forensics

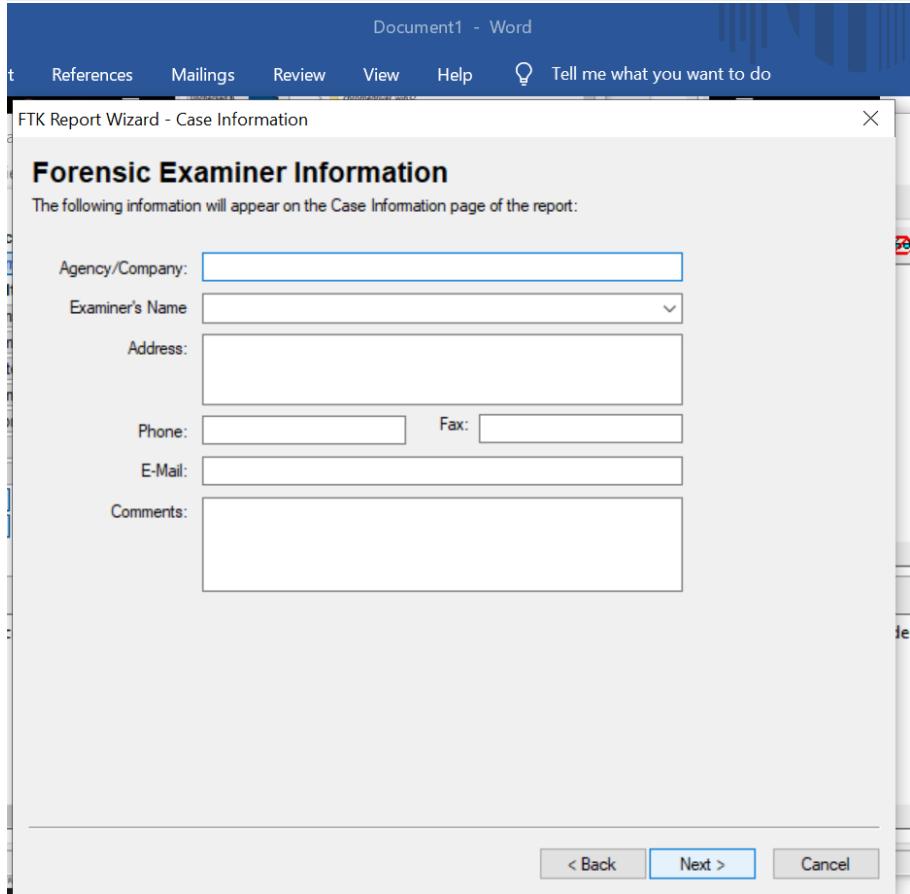
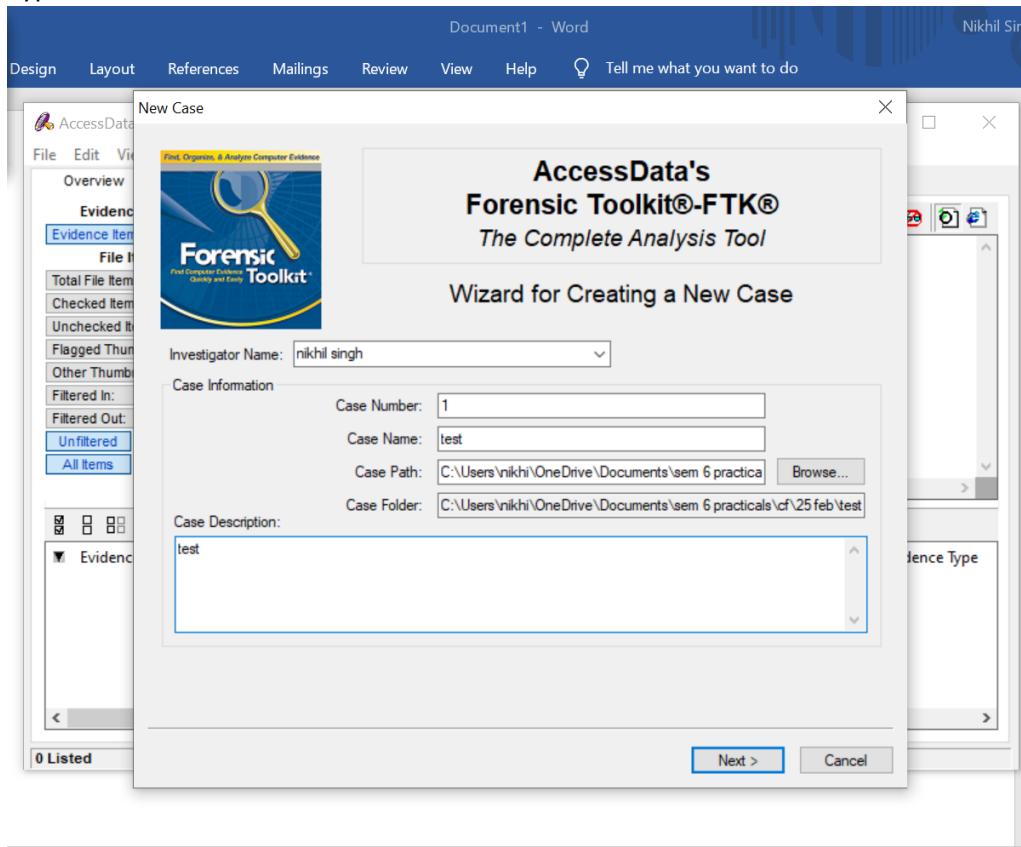
- Mail Service Providers
- Email protocols
- Recovering emails
- Analyzing email header

click Start a new case, and then click OK.



CYBER FORENSICS PRACTICALS

Type case Information and examiner information



CYBER FORENSICS PRACTICALS

Select case log options and all processes to perform

The screenshot shows two overlapping dialog boxes from the AccessData software interface.

Case Log Options Dialog:

- Events to go in the Case Log:**
 - Case and evidence events: Events related to the addition and processing of file items when evidence is added or when using Analysis Tools later in the case.
 - Error messages: Events related to any error conditions encountered during the case.
 - Bookmarking events: Events related to the addition and modification of bookmarks.
 - Searching events: Events related to searching. All search queries and resulting hit counts will be recorded.
 - Data carving / Internet searches: Events related to special data carving or internet keyword searches that are performed during the case.
 - Other events: Other events not related to the above, such as copying, viewing, and ignoring files.

Evidence Processing Options Dialog:

- Processes to Perform:**
 - MD5 Hash: An MD5 hash is a 16 byte value generated based upon a file's content. It is used to uniquely identify files. Hashes can be used to verify a file's integrity, or to identify duplicate files. MD5 hashes are used by the KFF to identify known files.
 - SHA1 Hash: A SHA1 hash is a 20 byte value. The SHA1 hashing algorithm is newer than MD5, but is not yet as widely used.
 - KFF Lookup: KFF (Known File Filter) is a utility that compares MD5 file hashes against a database of MD5 hashes from known files. The purpose of KFF is to eliminate files known to be unimportant, or to alert the investigator to known illicit or dangerous files.
 - Entropy Test: For unknown file types, an entropy test is used to determine whether the file's data is compressed or encrypted. Such files contain no plain text and will not be indexed. Unnecessary indexing of such files can waste large amounts of time and resources.
 - Full Text Index: The Forensic Toolkit includes a very powerful search engine, dtSearch, which enables the investigator to do instantaneous searching of textual data. In order to take advantage of this search feature, the data must first be indexed.
 - Store Thumbnails: Create and store thumbnails for all graphics in the case. This option speeds up browsing through the Graphics view at the expense of consuming more space in the case folder.
 - Decrypt EFS Files: Automatically locate and attempt to decrypt EFS encrypted files found on NTFS partitions within the case. (Requires AccessData Password Recovery Toolkit 5.20 or newer)
 - File Listing Database: Create a Microsoft Access (Jet) database containing a list of all files in the case. The attributes included are based on the Preprocessing File Listing Database Column Setting. This database can be recreated with custom column settings in Copy Special.
 - HTML File Listing: Create an HTML version of the File Listing.
 - Data Carve: Automatically find specific file types embedded in other files and from free space. Retrieve results using Data Carving Option on Tools Menu. Carving Options
 - Registry Reports: Generate common registry reports during preprocessing.

CYBER FORENSICS PRACTICALS

Select these options and add evidence information

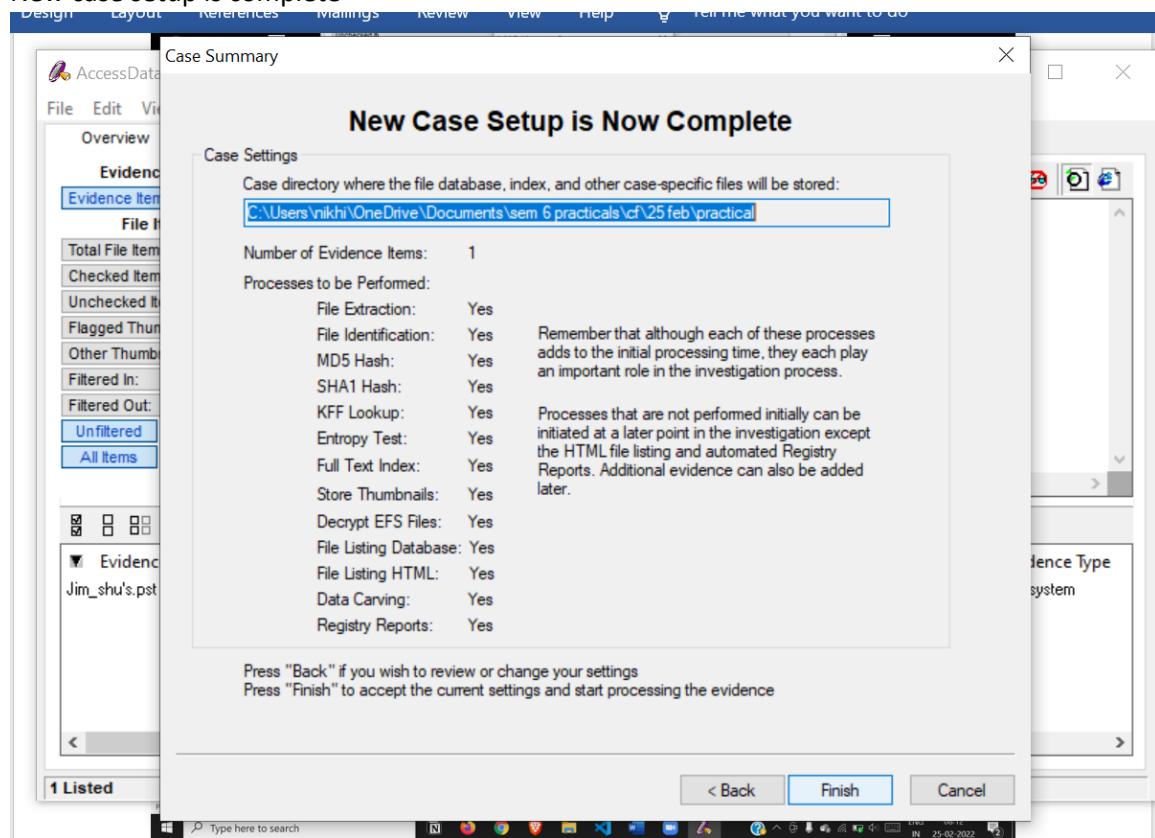
The screenshot displays four windows from a forensic analysis tool:

- Refine Case - Default**: A configuration window for refining case items. It includes tabs for "Include All Items" (selected), "Optimal Settings", "Email Emphasis", "Text Emphasis", and "Graphics Emphasis". Under "Unconditionally Add", checkboxes are selected for "File Slack", "Free Space", and "KFF Ignorable Files". Under "Conditionally Add", a dropdown menu shows "BOTH the file status and the file type". Below are sections for "File Status Criteria" (Deletion Status: Deleted, Encrypted; Email Status: From email, Not from email) and "File Type Criteria" (Documents, Spreadsheets, Databases, Graphics, Multimedia, Archives, Folders, Other Known, Unknown).
- Refine Index - Default**: A configuration window for refining index items. It includes tabs for "Unconditionally Index" (checkboxes for "File Slack", "Free Space", and "KFF Ignorable Files") and "Conditionally Index" (checkboxes for "File Status Criteria" and "File Type Criteria").
- Add Evidence to Case**: A window for adding evidence items. It shows a list of evidence types: Acquired Image of drive, Local drive, Folder, Individual File, and a note about acquired images. Below is a "Type of Evidence to Add to Case" dropdown with options: Acquired Image of Drive, Local Drive, Contents of a Folder, and Individual File (selected). Buttons include "Continue..." and "Cancel".
- Add Evidence**: A file selection dialog box titled "Select File". It shows a list of files in the "Downloads" folder:

Name	Type	Date modified
ftk181.rar	RAR archive	25-02-2022 07:20
Jim_shu's.pst	PST File	25-02-2022 07:19
ftk181	Earlier this week (4)	25-02-2022 07:19
4.40-TVBC-Syllabus-Computer	PDF document	21-02-2022 08:07
PhoneCopier_4_10_4_27874.apk	Android package file	21-02-2022 07:44
Mobileedit_v8.1.0_apkpure.com.apk	Android package file	21-02-2022 07:31
Getintopc.com_MOBILedit_Forensic_with_S...	EXE file	21-02-2022 07:31
Earlier this month (13)		
BrowserHistoryExaminer_v1.16.7_Installer.msi	MSI file	11-02-2022 18:17
Blackhook.drv	Driver file	09-02-2022 10:40

 The "File name:" field is set to "Jim_shu's.pst" and the "Files of type:" dropdown is set to "All Files (*.*)". Buttons include "Open" and "Cancel".

New case setup is complete

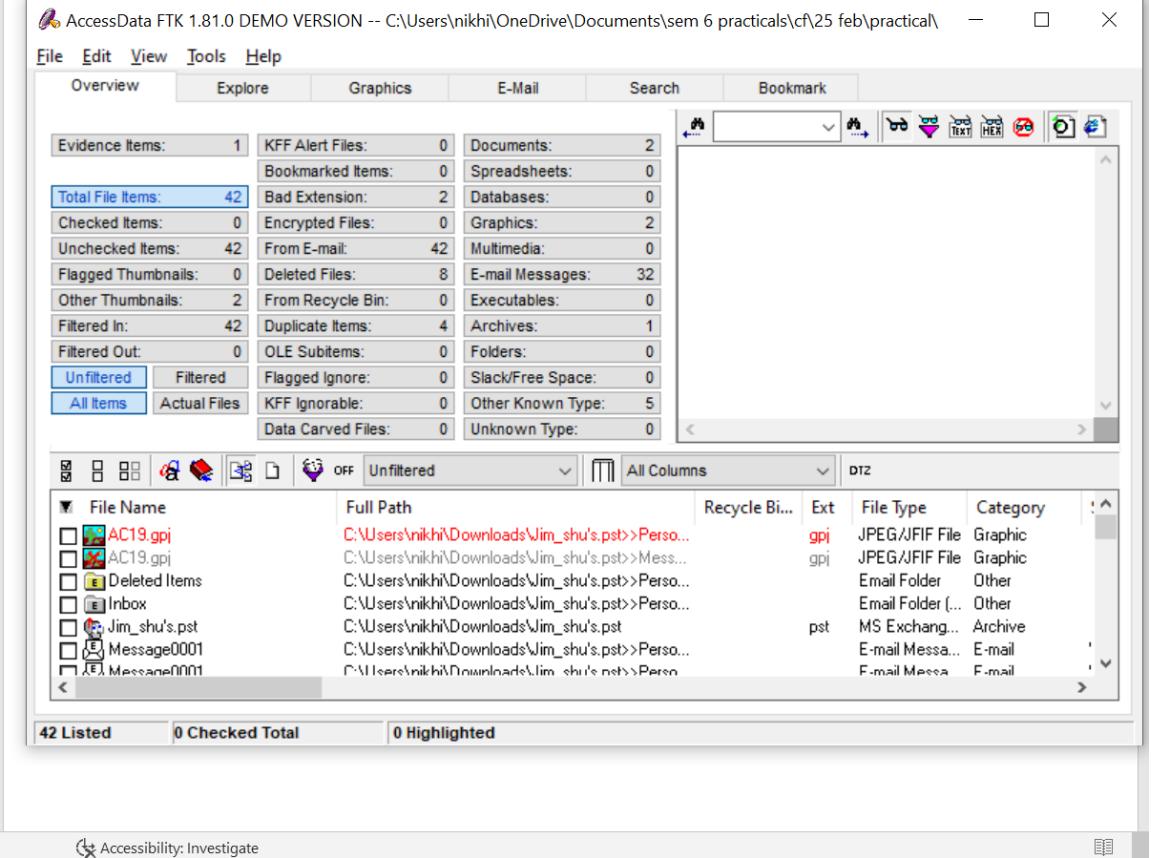


The screenshot shows the 'Evidence Items' view in AccessData FTK. The top menu includes File, Edit, View, Tools, and Help. The 'Explore' tab is selected in the navigation bar. The left sidebar shows file statistics: Total File Items (42), Checked Items (0), Unchecked Items (42), Flagged Thumbnails (0), Other Thumbnails (2), Filtered In (42), Filtered Out (0), Unfiltered (selected), and All Items. The main area displays a table of evidence items:

Evidence Items	File Status	File Category
Evidence Items: 1	KFF Alert Files: 0	Documents: 2
File Items	Bookmarked Items: 0	Spreadsheets: 0
Total File Items: 42	Bad Extension: 2	Databases: 0
Checked Items: 0	Encrypted Files: 0	Graphics: 2
Unchecked Items: 42	From E-mail: 42	Multimedia: 0
Flagged Thumbnails: 0	Deleted Files: 8	E-mail Messages: 32
Other Thumbnails: 2	From Recycle Bin: 0	Executables: 0
Filtered In: 42	Duplicate Items: 4	Archives: 1
Filtered Out: 0	OLE Subitems: 0	Folders: 0
Unfiltered (selected)	Flagged Ignore: 0	Slack/Free Space: 0
All Items	KFF Ignorable: 0	Other Known Type: 5
	Data Carved Files: 0	Unknown Type: 0

The preview pane on the right shows a file named 'Jim_shu's.pst' with a size of 2 MB. The bottom status bar shows '1 Listed'.

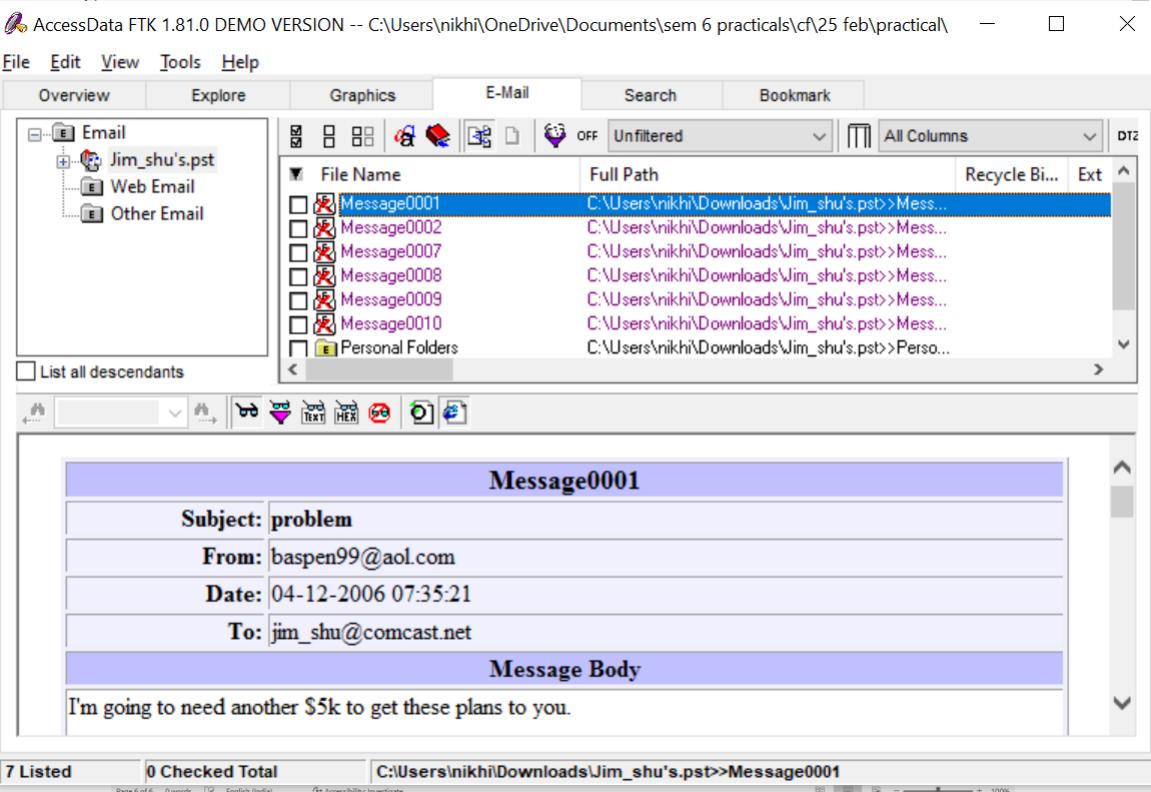
CYBER FORENSICS PRACTICALS

 AccessData FTK 1.81.0 DEMO VERSION -- C:\Users\nikhi\OneDrive\Documents\sem 6 practicals\cf\25 feb\practical\

Evidence Items: 1 **KFF Alert Files:** 0 **Documents:** 2
Total File Items: 42 **Bookmarked Items:** 0 **Spreadsheets:** 0
Checked Items: 0 **Bad Extension:** 2 **Databases:** 0
Unchecked Items: 42 **Encrypted Files:** 0 **Graphics:** 2
From E-mail: 42 **Deleted Files:** 8 **Multimedia:** 0
Flagged Thumbnails: 0 **From Recycle Bin:** 0 **E-mail Messages:** 32
Other Thumbnails: 2 **Duplicate Items:** 4 **Executables:** 0
Filtered In: 42 **OLE Subitems:** 0 **Archives:** 1
Filtered Out: 0 **Flagged Ignore:** 0 **Folders:** 0
Unfiltered **Filtered** **All Items** **Actual Files**

File Name	Full Path	Recycle Bi...	Ext	File Type	Category
AC19.gpi	C:\Users\nikhi\Downloads\Jim_shu's.pst>Perso...		gpi	JPEG/JFIF File	Graphic
AC19.gpi	C:\Users\nikhi\Downloads\Jim_shu's.pst>Mess...		gpi	JPEG/JFIF File	Graphic
Deleted Items	C:\Users\nikhi\Downloads\Jim_shu's.pst>Perso...			Email Folder	Other
Inbox	C:\Users\nikhi\Downloads\Jim_shu's.pst>Perso...			Email Folder (...	Other
Jim_shu's.pst	C:\Users\nikhi\Downloads\Jim_shu's.pst		pst	MS Exchange...	Archive
Message0001	C:\Users\nikhi\Downloads\Jim_shu's.pst>Perso...			E-mail Messa...	E-mail
Message0001	C:\Users\nikhi\Downloads\Jim_shu's.pst>Perso...			E-mail Messa...	E-mail

42 Listed 0 Checked Total 0 Highlighted

 AccessData FTK 1.81.0 DEMO VERSION -- C:\Users\nikhi\OneDrive\Documents\sem 6 practicals\cf\25 feb\practical\

File Name **Full Path** **Recycle Bi...** **Ext**

File Name	Full Path	Recycle Bi...	Ext
Message0001	C:\Users\nikhi\Downloads\Jim_shu's.pst>Mess...		
Message0002	C:\Users\nikhi\Downloads\Jim_shu's.pst>Mess...		
Message0007	C:\Users\nikhi\Downloads\Jim_shu's.pst>Mess...		
Message0008	C:\Users\nikhi\Downloads\Jim_shu's.pst>Mess...		
Message0009	C:\Users\nikhi\Downloads\Jim_shu's.pst>Mess...		
Message0010	C:\Users\nikhi\Downloads\Jim_shu's.pst>Mess...		
Personal Folders	C:\Users\nikhi\Downloads\Jim_shu's.pst>Perso...		

Message0001

Subject: problem
From: baspen99@aol.com
Date: 04-12-2006 07:35:21
To: jim_shu@comcast.net

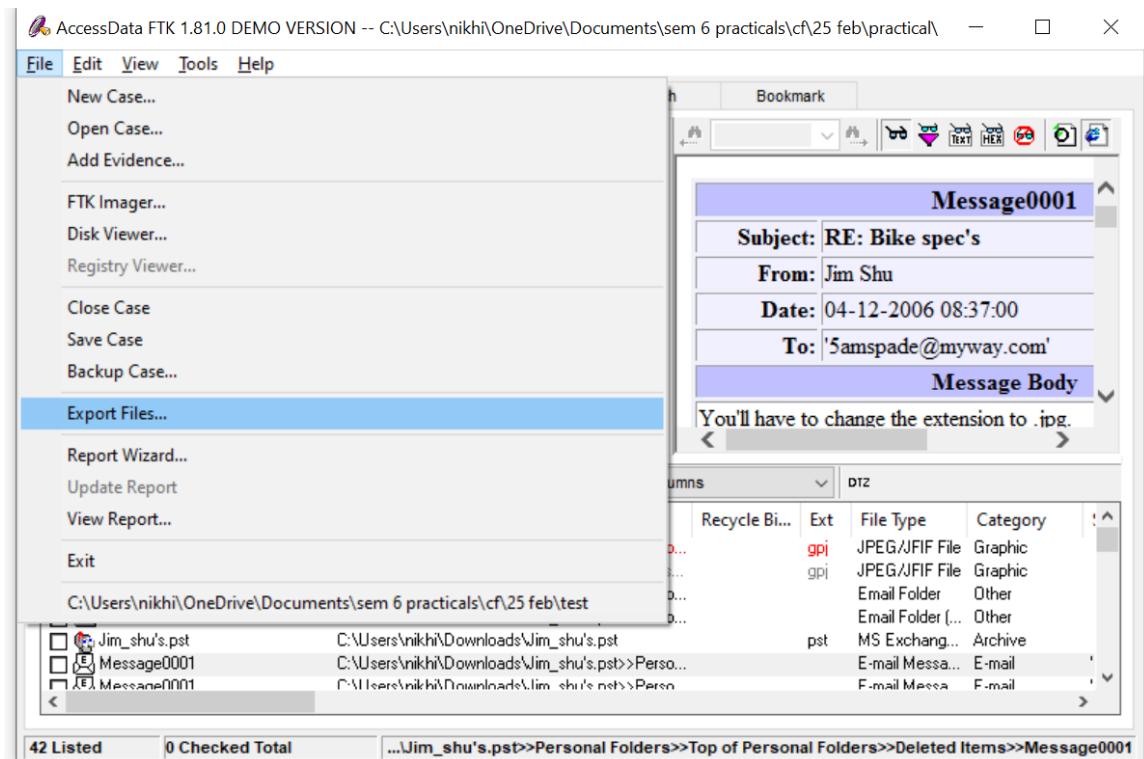
Message Body

I'm going to need another \$5k to get these plans to you.

7 Listed 0 Checked Total C:\Users\nikhi\Downloads\Jim_shu's.pst>>Message0001

Export case information

CYBER FORENSICS PRACTICALS



Part2

Launch detached information

The screenshot shows the AccessData FTK 1.81.0 interface. The 'Evidence Items' tab is selected, displaying a list of items. A context menu is open over the item 'Message0010'. The menu options include:

- Create Bookmark...
- View This Item in a Different List
- Ignore Item
- Launch Detached Viewer** (highlighted in blue)
- Launch Associated Program
- View With...
- Copy Special...
- Export File...
- Recursive File Export...

The main pane shows a list of files under the 'File Status' tab, with 'Message0010' selected. The status bar at the bottom indicates '42 Listed' and '0 Checked Total'.

CYBER FORENSICS PRACTICALS

View message headers and body

Message0010

Full path: C:\Users\nikhil\Downloads\Jim_shu's.pst>Message0010
File type: E-mail Message

Message0010	
Subject:	Waiting
From:	baspen99@aol.com
Date:	07-12-2006 07:41:57
To:	jim_shu@comcast.net
Message Body	
I'm in desperate need for some cash. what can you forward to me this week? Check out the new AOL < http://pr.atwola.com/promodk/1615326657x4311227241x4298082137/aof?redir=http%3A%2F%2Fwww%2Eaol%2Ecom%2Fnewaol%20 >. Most comprehensive set of free safety and security tools, free access to millions of high-quality videos from across the web, free AOL Mail and more.	

Outlook Header Information

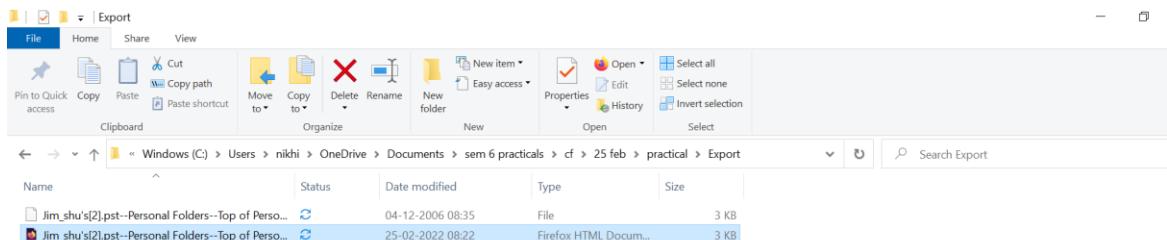
Conversation Topic: Waiting
Sender Name: baspen99@aol.com
Received By: Jim Shu
Delivery Time: 07-12-2006 07:41:57
Creation Time: 07-12-2006 07:46:07
Modification Time: 08-12-2006 05:07:50
Submit Time: 07-12-2006 07:41:45

Message0010

Full path: C:\Users\nikhil\Downloads\Jim_shu's.pst>Message0010
File type: E-mail Message

Outlook Header Information	
Conversation Topic:	Waiting
Sender Name:	baspen99@aol.com
Received By:	Jim Shu
Delivery Time:	07-12-2006 07:41:57
Creation Time:	07-12-2006 07:46:07
Modification Time:	08-12-2006 05:07:50
Submit Time:	07-12-2006 07:41:45
Flags:	1 = Read
Size:	5434
Standard Header Information	
Received:	from imo-m14.mx.aol.com ([64.12.138.204]) by rwmcmc19.comcast.net (rwmcmc19) with ESMTP id <20061207021157r1900bbubge>; Thu, 7 Dec 2006 02:11:57 +0000 X-Originating-IP: [64.12.138.204]
Received:	from Baspen99@aol.com by imo-m14.mx.aol.com (mail_out_v38_r7.6.) id i1c39.9f149a0 (60449) for <jim_shu@comcast.net>; Wed, 6 Dec 2006 21:11:47 -0500 (EST)
Received:	from mblk-d48 (mblk-d48.mblk.aol.com [205.188.212.232]) by ciaol-r01.mx.aol.com (v114.2) with ESMTP id MAILCIAOLR012-ec214577786132d; Wed, 06 Dec 2006 21:11:45 -0500 To: jim_shu@comcast.net Subject: Waiting Date: Wed, 06 Dec 2006 21:11:45 -0500 X-MB-Message-Source: WebUI MIME-Version: 1.0 From: baspen99@aol.com

CYBER FORENSICS PRACTICALS



/C/Users/nikhi/OneDrive/Documents/sem 6 practicals/cf/25 feb/practical/Export/Jim_shu's[2].pst--Personal Folders--Top of Perso...

Message0001

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

Message Body

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

-----Original Message-----
From: Sam [mailto:5amspade@myway.com]
Sent: Sunday, December 03, 2006 7:04 PM
To: Jim_shu@comcast.net
Subject: RE: Bike spec's

I think I can raise another 5 for you. Do you have something I can look at yet?

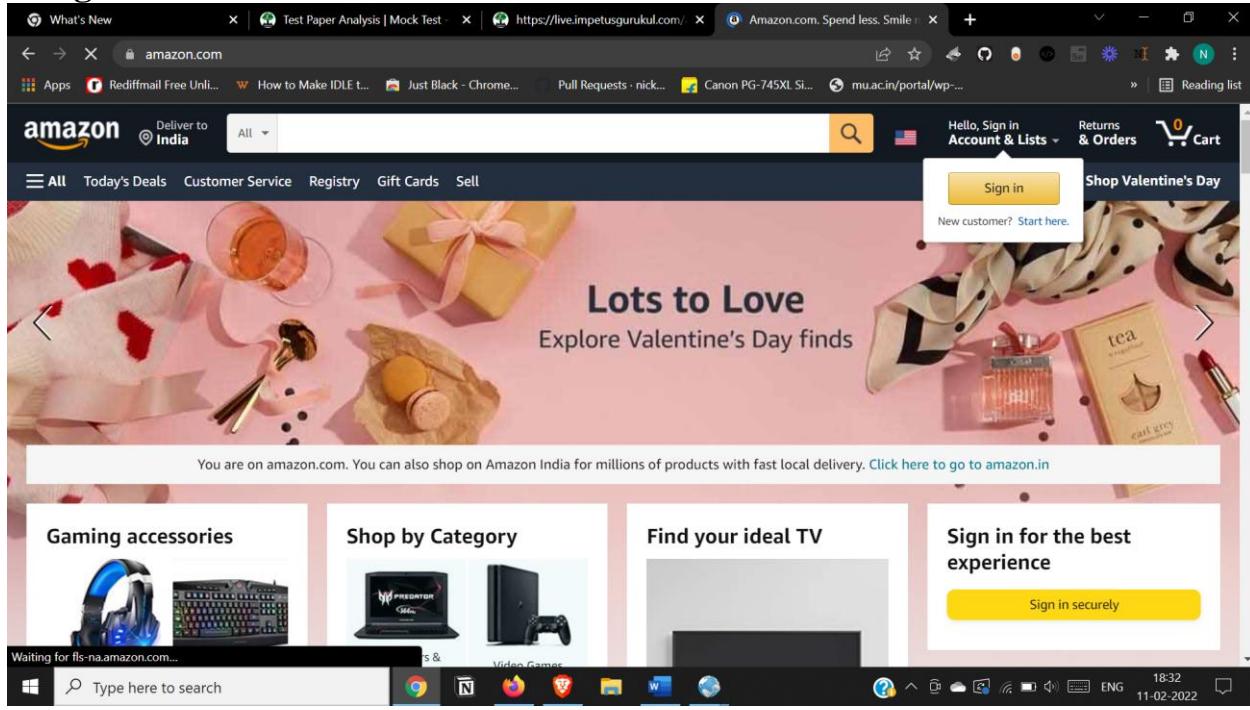
--- On Sun 12/03, Jim Shu <Jim_shu@comcast.net> wrote:
From: Jim Shu [mailto: Jim_shu@comcast.net]

PRACTICAL 10

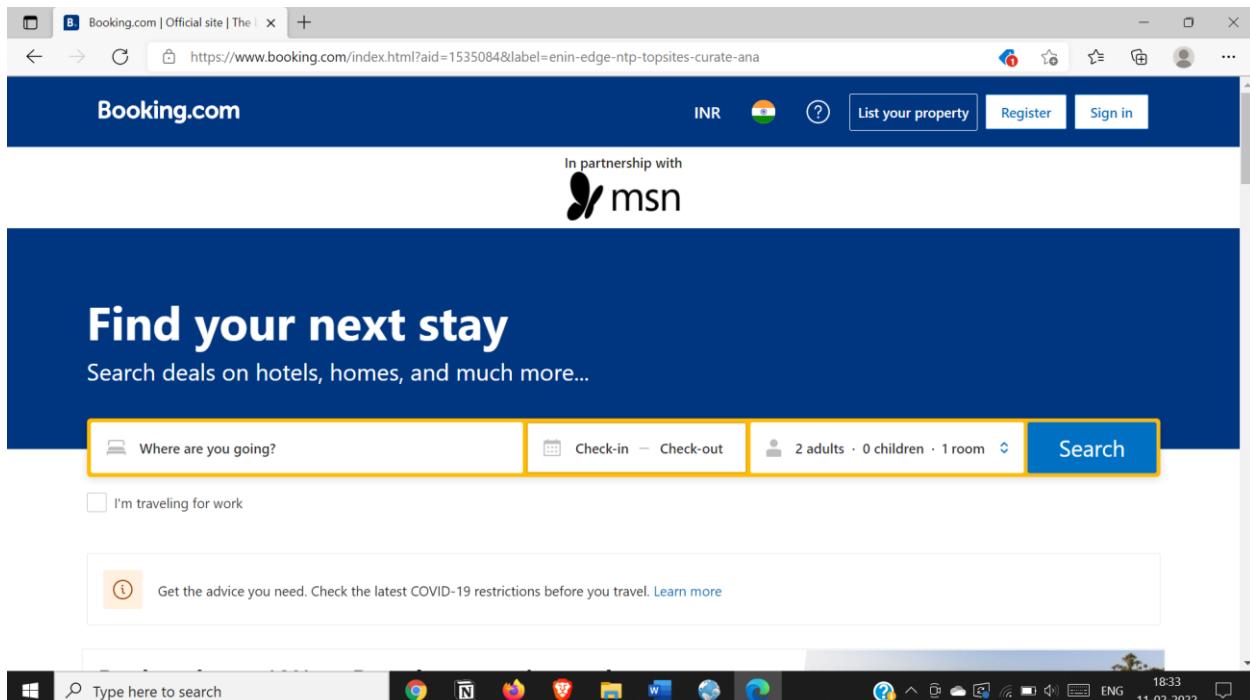
Aim :- Web Browser Forensics

- Web Browser working

Google Chrome

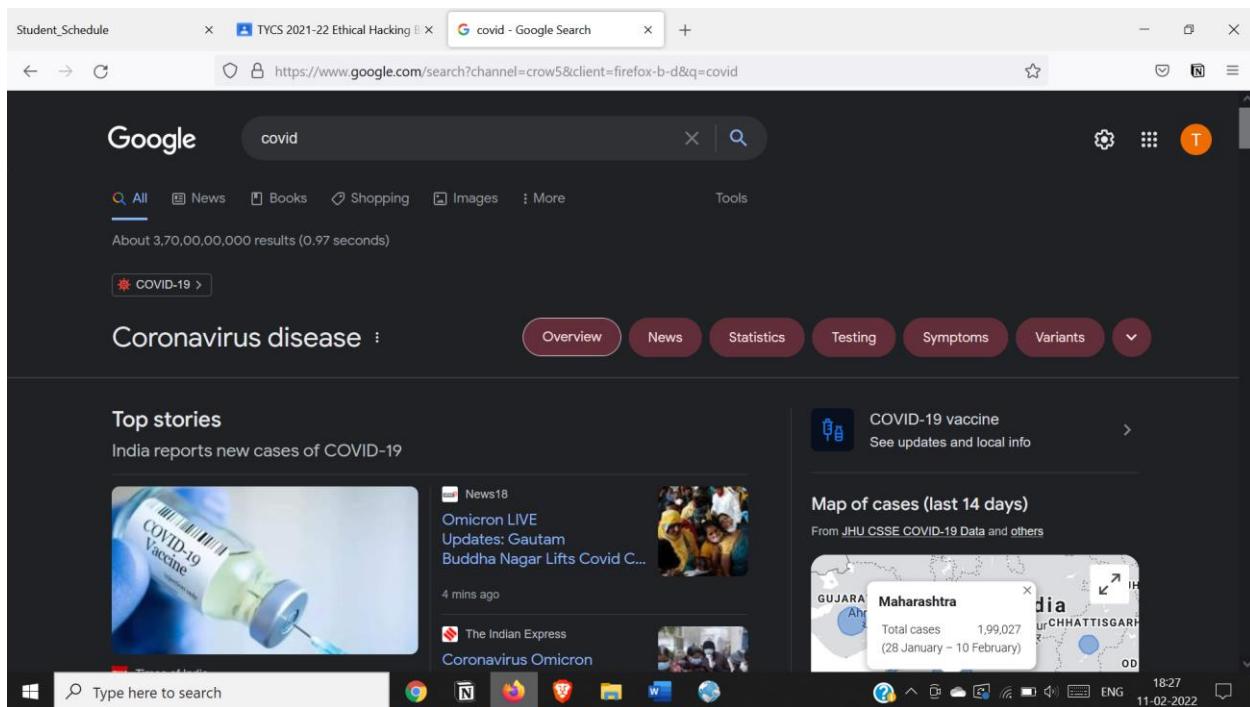


Microsoft Edge



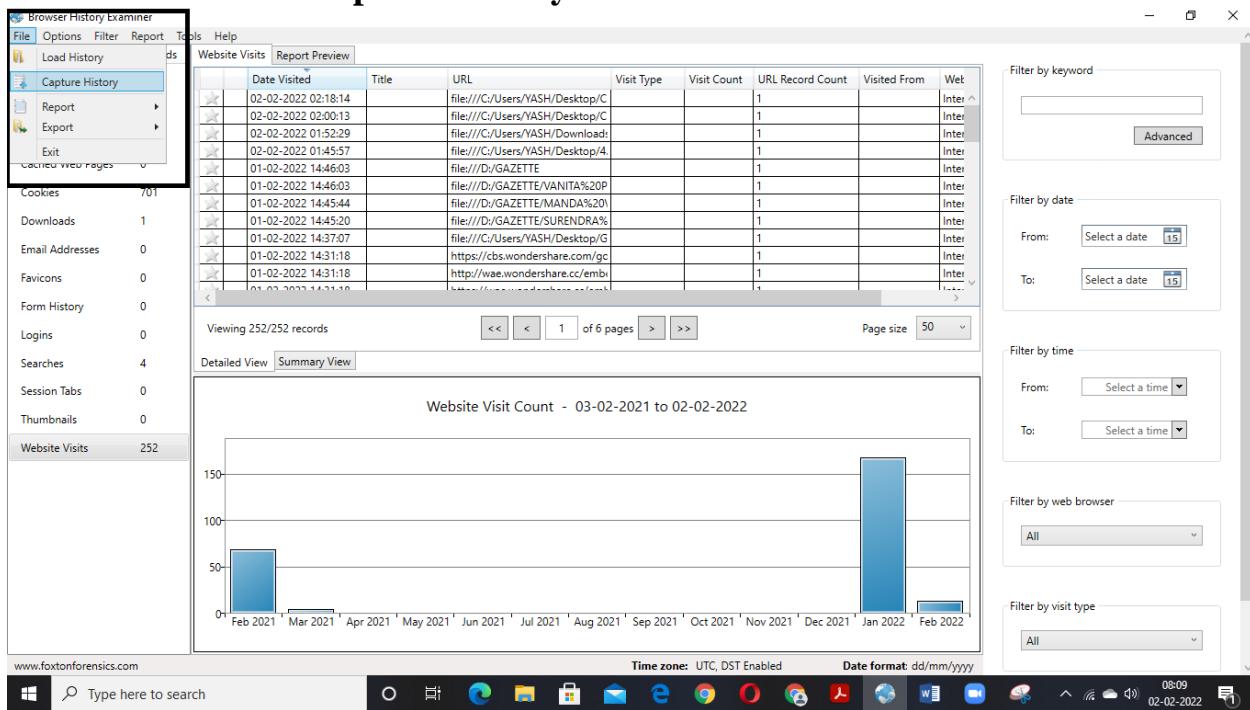
Firefox

CYBER FORENSICS PRACTICALS

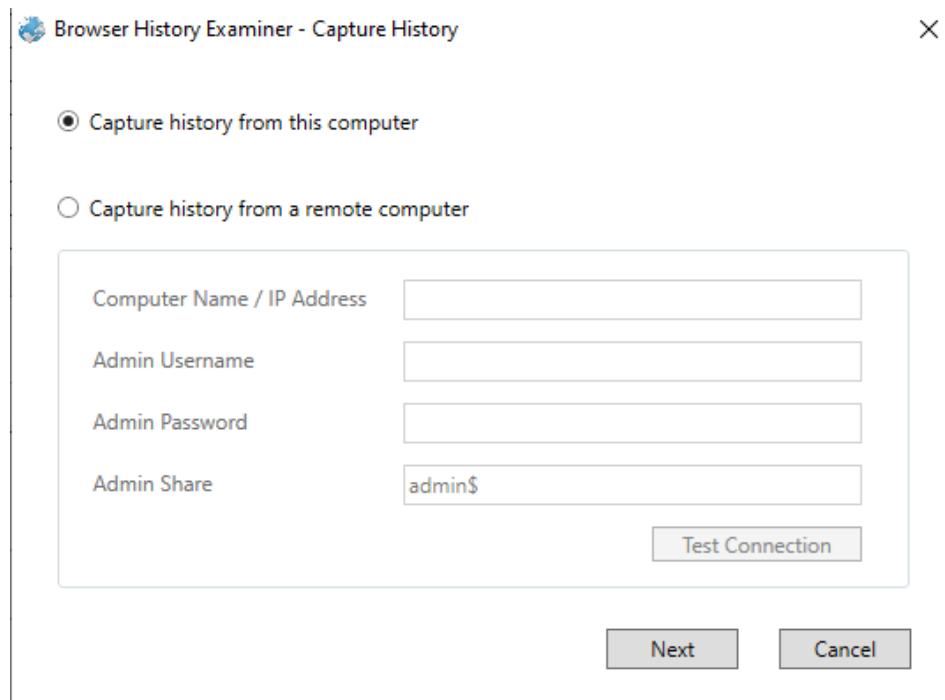


- Forensics activities on browser

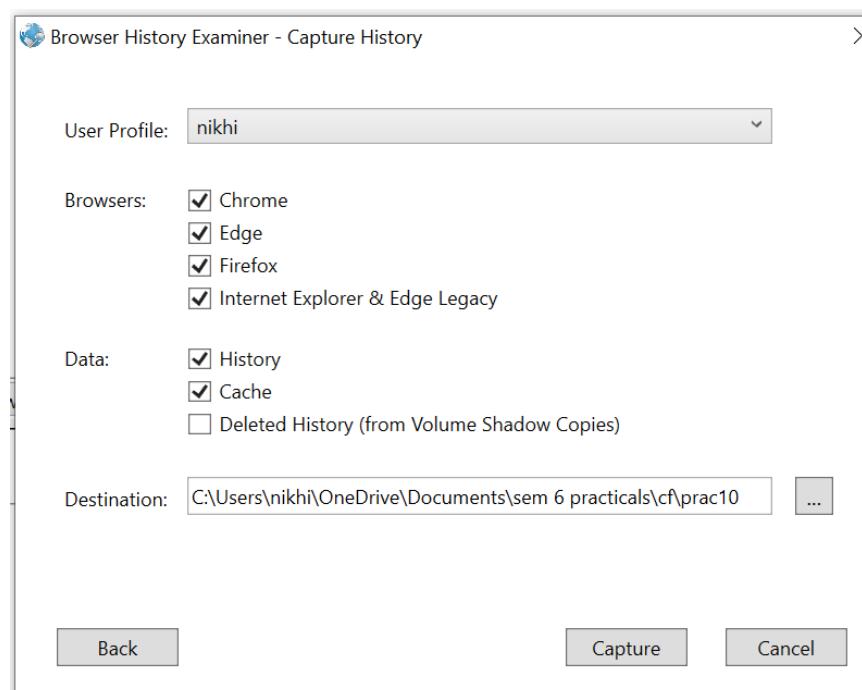
Go to File Menu > Capture History

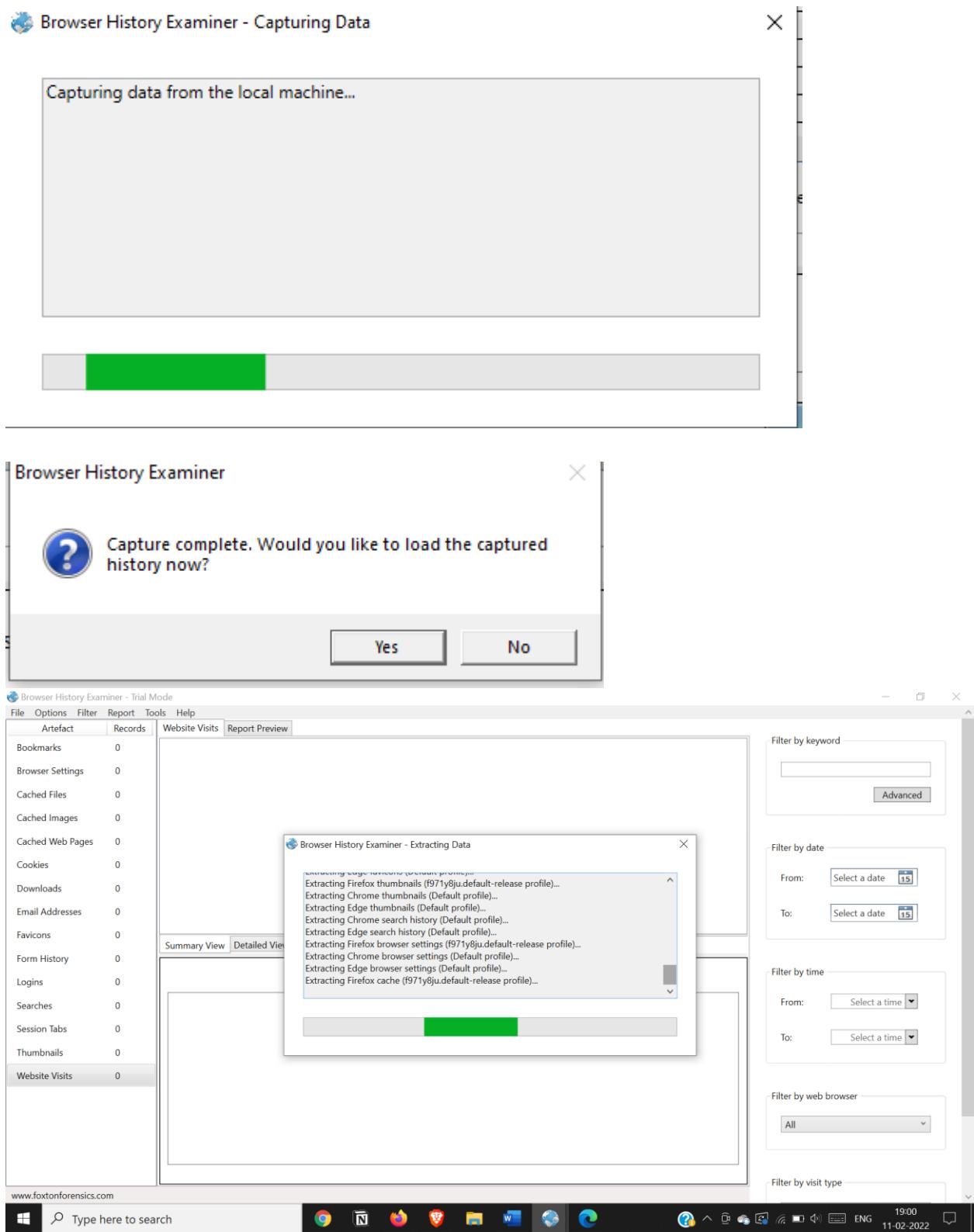


Click Next



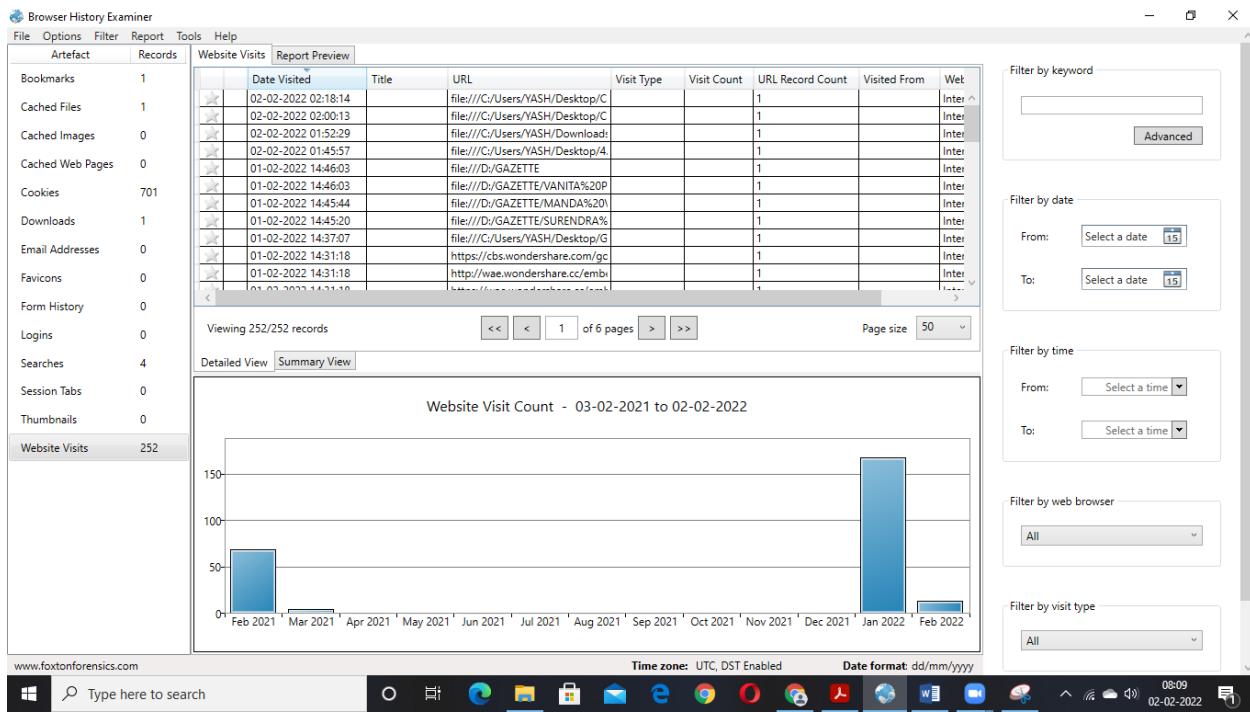
Give the path of folder in which you want to save your captured data and click on capture



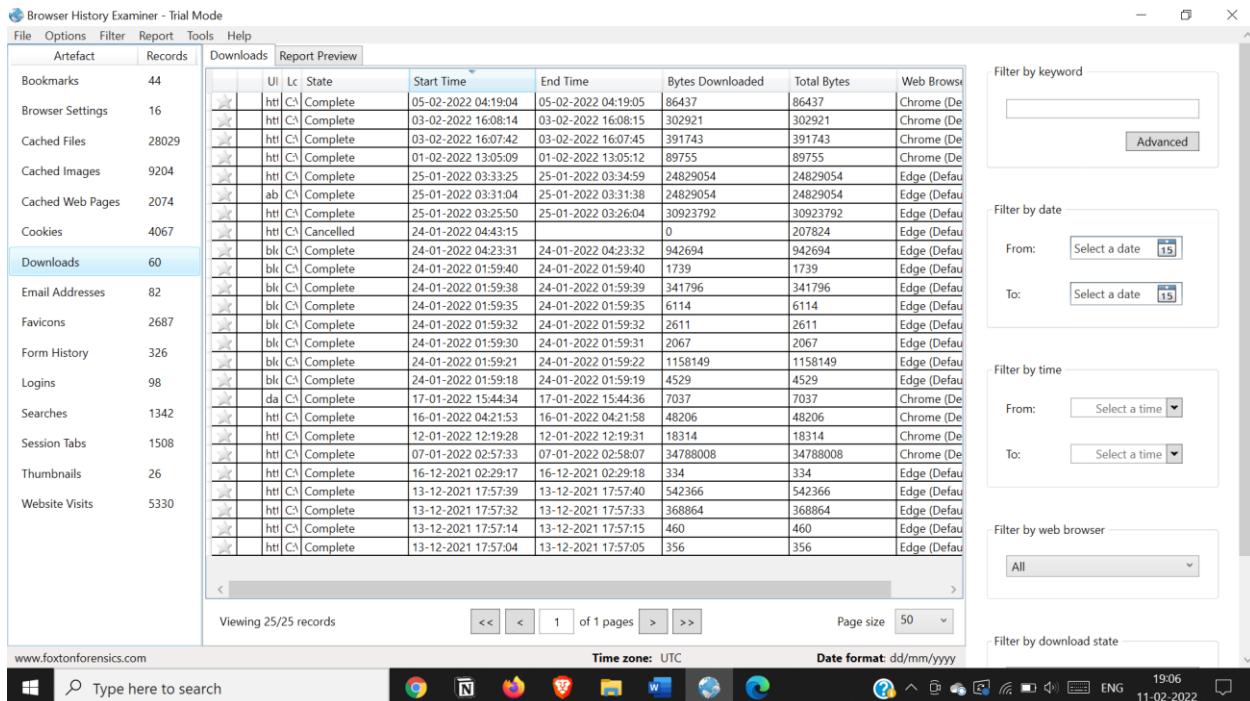


All the captured details are listed below

CYBER FORENSICS PRACTICALS



Downloads



Searches

CYBER FORENSICS PRACTICALS

Browser History Examiner - Trial Mode

Artefact	Records
Bookmarks	44
Browser Settings	16
Cached Files	28029
Cached Images	9204
Cached Web Pages	2074
Cookies	4067
Downloads	60
Email Addresses	82
Favicons	2687
Form History	326
Logins	98
Searches	1342
Session Tabs	1508
Thumbnails	26
Website Visits	5330

Searches Report Preview

Date Searched	Search Terms	Search Engine	URL	Source	Web Browser (Profile)
11-02-2022 12:57:01	covid	Google	https://www.google.com	Website Visit	Firefox (f971y8ju.default)
09-02-2022 13:11:12	youtube	Google	https://www.google.com	Chrome History	Chrome (Default)
09-02-2022 13:11:12	youtube	Google	https://www.google.com	Website Visit	Chrome (Default)
09-02-2022 13:11:11	youtube	Google	https://www.google.com	Website Visit	Chrome (Default)
09-02-2022 03:55:05	mic test	Google	https://www.google.com	Website Visit	Firefox (f971y8ju.default)
08-02-2022 14:50:42	focus meditation 3	Google	https://www.google.com	Chrome History	Chrome (Default)
08-02-2022 14:50:42	focus meditation 3	Google	https://www.google.com	Website Visit	Chrome (Default)
08-02-2022 14:50:41	focus meditation 3	Google	https://www.google.com	Website Visit	Chrome (Default)
08-02-2022 14:50:35	focus meditation	Google	https://www.google.com	Chrome History	Chrome (Default)
08-02-2022 14:50:35	focus meditation	Google	https://www.google.com	Website Visit	Chrome (Default)
08-02-2022 14:50:32	focus meditation	Google	https://www.google.com	Website Visit	Chrome (Default)
08-02-2022 14:50:31	focus meditation	Google	https://www.google.com	Website Visit	Chrome (Default)

Viewing 25/25 records

Filter by keyword
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
Filter by search engine

Time zone: UTC Date format: dd/mm/yyyy

www.foxtonforensics.com

Type here to search

19:05 11-02-2022 ENG

Website Visits

Browser History Examiner - Trial Mode

Artefact	Records
Bookmarks	44
Browser Settings	16
Cached Files	28029
Cached Images	9204
Cached Web Pages	2074
Cookies	4067
Downloads	60
Email Addresses	82
Favicons	2687
Form History	326
Logins	98
Searches	1342
Session Tabs	1508
Thumbnails	26
Website Visits	5330

Website Visits Report Preview

- live.impetusgurukul.com 4 visits
- amazon.com 3 visits
- google.com 2 visits
- classroom.google.com 2 visits
- booking.com 1 visits
- amazon.in 1 visits
- navkarfittings.000webhostapp.com 1 visits
- accounts.google.com 1 visits

Summary View Detailed View

Website Visit Count - 11-02-2022 to 11-02-2022

Time zone: UTC Date format: dd/mm/yyyy

Filter by keyword
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
Filter by visit type

Time zone: UTC Date format: dd/mm/yyyy

www.foxtonforensics.com

Type here to search

19:03 11-02-2022 ENG

Bookmarks

CYBER FORENSICS PRACTICALS

Browser History Examiner - Trial Mode

File Options Filter Report Tools Help

Artefact	Records	Bookmarks	Report Preview
Bookmarks	44		Date Added Last Modified Title URL Web Browser (Profile)
Browser Settings	16		18-01-2022 05:05:21 18-01-2022 05:05:21 Student_Schedule https://www.teachuseduma.firefox (971y8ju.default) AIMCA - Fastrack Test Serie https://live.impegsugurukul.chrome (Default)
Cached Files	28029		08-01-2022 13:45:53 07-10-2021 04:03:08 Getting Started https://www.mozilla.org/en.firefox (971y8ju.default) 07-10-2021 04:03:08 Get Help https://support.mozilla.org.firefox (971y8ju.default)
Cached Images	9204		07-10-2021 04:03:08 07-10-2021 04:03:08 Customize Firefox https://support.mozilla.org.firefox (971y8ju.default) 07-10-2021 04:03:08 Get Involved https://www.mozilla.org/en.firefox (971y8ju.default)
Cached Web Pages	2074		07-10-2021 04:03:08 07-10-2021 04:03:08 About Us https://www.mozilla.org/en.firefox (971y8ju.default) 06-10-2021 07:06:06 YouTube https://youtube.com.chrome (Default)
Cookies	4067		06-10-2021 07:05:51 Gmail https://accounts.google.com.chrome (Default) 06-10-2021 07:05:51 Maps https://maps.google.com.chrome (Default)
Downloads	60		05-10-2021 13:46:55 Utomik Games https://www.utmik.com/hedge (Default) B 05-10-2021 13:46:55 Booking.com https://www.booking.com/iedge (Default)
Email Addresses	82		05-10-2021 13:46:55 Express VPN https://js.redirect.hpm/jure-edge (Default) 05-10-2021 13:46:55 LastPass password manager https://js.redirect.hpm/jure-edge (Default)
Favicons	2687		15-07-2021 17:12:19 UNIX / Linux: 2 Ways to Add https://www.thegeekstuff.cc.chrome (Default) 30-01-2021 01:43:45 Codelabs for Android Devel https://developer.android.com.chrome (Default)
Form History	326		09-01-2021 12:47:49 FOSSASIA Internship Progra https://docs.google.com/f0chrome (Default) 09-01-2021 12:16:16 My groups https://groups.google.com.chrome (Default)
Logins	98		27-12-2020 06:12:34 Create a palette - Coolors https://coolors.co/1d2735-f.chrome (Default) 05-10-2020 03:07:09 classroom https://classroom.google.com.chrome (Default)
Searches	1342		04-07-2020 20:55:22 JavaScript - Events - Tutorial https://www.tutorialspoint.com.chrome (Default) 09-06-2020 09:57:11 My Money - PeoplePerHour https://www.peopleperhour.chrome (Default)
Session Tabs	1508		02-06-2020 06:50:34 Document file:///C/Users/Nikhil/Desktop.chrome (Default) 04-05-2020 18:33:35 How to Install PHP on Wind https://www.sitepoint.com.chrome (Default)
thumbnails	26		19-04-2020 18:15:58 File Manager https://www.000webhost.cc.chrome (Default)
Website Visits	5330		

Viewing 25/25 records << < 1 of 1 pages > >> Page size 50

Time zone: UTC Date format: dd/mm/yyyy

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 Undo Clear

www.foxtonforensics.com

Type here to search

Chrome Edge Firefox Opera Internet Explorer Microsoft Edge

19:06 11-02-2022 ENG

- Cache / Cookies analysis

Number of cache files and cookies gets captured

Browser History Examiner - Trial Mode

File Options Filter Report Tools Help

Artefact	Records	Cached Files	Report Preview
Bookmarks	44		Last Fetched
Browser Settings	16		Content Type
Cached Files	28029		URL
Cached Images	9204		Fetch Count
Cached Web Pages	2074		File Size (Bytes)
Cookies	4067		Web Browser (Profile)
Downloads	60		
Email Addresses	82		
Favicons	2687		
Form History	326		
Logins	98		
Searches	1342		
Session Tabs	1508		
Thumbnails	26		
Website Visits	5330		

Filter by keyword Advanced

Filter by date From: To:

Filter by time From: To:

Filter by web browser All

Filter by content type

Viewing 25/25 records << < 1 of 1 pages > >> Page size 50

Time zone: UTC Date format: dd/mm/yyyy

www.foxtonforensics.com

Type here to search

1906 11-02-2022

CYBER FORENSICS PRACTICALS

Browser History Examiner

File	Options	Filter	Report	Tools	Help				
Artifact	Records	Cookies	Report Preview						
Bookmarks	1		Date Created	URL	Last Accessed	Date Expires	Name	Content	Web Browser
Cached Files	6		31-03-2021 03:05:38	rubicongproject.cc		31-03-2022 03:05:37	khaos	KL9JGKZM-1X-A'	Internet Explorer
Cached Images	0		31-03-2021 03:05:38	rubicongproject.cc		31-03-2022 03:05:37	audit	1 PrvRZsLz9t9As	Internet Explorer
Cached Web Pages	0		31-03-2021 03:05:38	dpm.demdex.net		27-09-2021 03:05:38	dpm	04861118808584	Internet Explorer
Cookies	702		31-03-2021 03:05:38	demdex.net/		27-09-2021 03:05:38	demdex	04861118808584	Internet Explorer
Downloads	1		31-03-2021 03:05:38	amazon-adstyer		01-10-2021 03:05:37	ad-styer	Ax4o1AGrPUVKnI	Internet Explorer
Email Addresses	0		31-03-2021 03:05:37	spotxchange.com		31-03-2022 04:12:17	audience	95da7321-91c5-1	Internet Explorer
Favicons	0		31-03-2021 03:05:37	pubmatic.com/		29-06-2021 03:05:37	PUBMDCID	4	Internet Explorer
Form History	0		31-03-2021 03:05:37	pubmatic.com/		30-04-2021 03:05:37	PugT	1617156337	Internet Explorer
Logins	0		31-03-2021 03:05:37	casalemedia.com		29-06-2021 03:05:37	KRTBCOOKIE_218	22978-YCOp6wAvI	Internet Explorer
Searches	4		31-03-2021 03:05:37	casalemedia.com		31-03-2022 03:05:37	CMRUMB	586063d8f12760	Internet Explorer
Session Tabs	0		31-03-2021 03:05:37	casalemedia.com		01-04-2021 03:05:37	CMST	YGPY8W8j2PEA	Internet Explorer
Thumbnails	0		31-03-2021 03:05:37	casalemedia.com		01-04-2021 03:05:37	CMDD		Internet Explorer
Website Visits	257		31-03-2021 03:05:37	casalemedia.com		31-03-2022 03:05:37	CMID	YCOp8HT9vLozxi	Internet Explorer
			31-03-2021 03:05:37	casalemedia.com		29-06-2021 03:05:37	CMPS	261	Internet Explorer
			31-03-2021 03:05:37	casalemedia.com		29-06-2021 03:05:37	CMPRO	915	Internet Explorer
			31-03-2021 03:05:37	demdex.net/		27-09-2021 03:05:37	dextp	269-1-16171563;	Internet Explorer
			31-03-2021 03:05:37	adxns.com/		29-06-2021 03:05:36	uuid2	33240681077174	Internet Explorer
			31-03-2021 03:05:37	adxns.com/		29-06-2021 03:05:36	anj	dTM7klM4.FDunI	Internet Explorer
			31-03-2021 03:05:36	btrack.com/		29-06-2021 03:05:05	GLOBALID	2uKlc8-sIBd987F	Internet Explorer
			31-03-2021 03:05:36	postrelease.com/		31-03-2022 03:05:36	status	1	Internet Explorer
			31-03-2021 03:05:36	postrelease.com/		31-03-2022 03:05:36	ver	1	Internet Explorer
			31-03-2021 03:05:36	postrelease.com/		31-03-2022 03:05:36	visitor	19e3d560-56f8-4	Internet Explorer
			31-03-2021 03:05:36	3lift.com/		29-06-2021 03:05:35	tluid	13416152774261	Internet Explorer
			31-03-2021 03:05:35	rfihub.com/		25-04-2022 03:05:35	rud	H4sIAAAAAAAQAz	Internet Explorer
			31-03-2021 03:05:35	rfihub.com/		25-04-2022 03:05:35	eud	H4sIAAAAAAAQAz	Internet Explorer
			31-03-2021 03:05:35	tribalfusion.com/		30-04-2021 03:05:35	_cfuid	dcf7dc4befa9493	Internet Explorer
			31-03-2021 03:05:35	tribalfusion.com/		29-06-2021 03:05:35	ANON_ID	alntAZcqkaHbByI	Internet Explorer
			31-03-2021 03:05:35	tribalfusion.com/		29-06-2021 03:05:35	ANON_ID_old	alntAZcqkaHbByI	Internet Explorer
			31-03-2021 03:05:35	yahoo.com/		31-03-2022 09:05:35	GUC	AOEBAQFaZSpot	Internet Explorer

Viewing 702/702 records

Page size: 50

Filter by keyword Advanced

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

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

Filter by web browser All

Filter Undo Clear

www.foxtonforensics.com

Time zone: UTC, DST Enabled Date format: dd/mm/yyyy

10:26 02-02-2022

- Last Internet activity

Generating Report

Right Click on the content and click Add to report

CYBER FORENSICS PRACTICALS

Browser History Examiner

Artefact	Records	Date Created	URL	Last Accessed	Date Expires	Name	Content	Web Browse
Bookmarks	1	31-03-2021 03:05:38	rubiconproject.com/		31-03-2022 03:05:37	khaoz	KL9jGKZM-1X-A'	Internet Expl ^
Cached Files	6	31-03-2021 03:05:38	rubiconproject.com/		31-03-2022 03:05:37	audit	JPrvRZsLZh9As	Internet Expl
Cached Images	0	31-03-2021 03:05:38	dpm.demdex.net/		27-09-2021 03:5:38	dpm	04861118808584	Internet Expl
Cached Web Pages	0	31-03-2021 03:05:38	demdex.net/		27-09-2021 03:5:38	demdex	04861118808584	Internet Expl
Cookies	702	31-03-2021 03:05:38	amazon-adsystem.com/		27-09-2021 03:5:38	ad-id	Ax4o1AGPUYKn	Internet Expl
Downloads	1	31-03-2021 03:05:38	amazon-adsystem.com/		27-09-2021 03:5:38	ad-privacy	0	Internet Expl
Email Addresses	0	31-03-2021 03:05:37	spotxchange.com/		26-03-2021 03:5:37	audience	95da7321-91c5-	Internet Expl
Favicons	0	31-03-2021 03:05:37	pubmatic.com/		29-06-2021 03:05:37	PUBMDCID	4	Internet Expl
Form History	0	31-03-2021 03:05:37	pubmatic.com/		29-06-2021 03:05:37	PugT	1617156337	Internet Expl
Logins	0	31-03-2021 03:05:37	casalemedia.com/		29-06-2021 03:05:37	KRTBCOOKIE_21E	22978-YCOp6wAu	Internet Expl
Searches	4	31-03-2021 03:05:37	casalemedia.com/		31-03-2022 03:05:37	CMRUM3	586063d8f12760	Internet Expl
Session Tabs	0	31-03-2021 03:05:37	casalemedia.com/		01-04-2021 03:05:37	CMST	YGPV8WBj2PEA	Internet Expl
Thumbnails	0	31-03-2021 03:05:37	casalemedia.com/		01-04-2021 03:05:37	CMDD		Internet Expl
Website Visits	257	31-03-2021 03:05:37	casalemedia.com/		31-03-2022 03:05:37	CMID	YCoP8HT9VLoxt	Internet Expl
		31-03-2021 03:05:37	casalemedia.com/		29-06-2021 03:05:37	CMPS	261	Internet Expl
		31-03-2021 03:05:37	casalemedia.com/		29-06-2021 03:05:37	CMPRO	915	Internet Expl
		31-03-2021 03:05:37	demdex.net/		27-09-2021 03:05:37	dextp	269-1-16171563	Internet Expl
		31-03-2021 03:05:37	adnxs.com/		29-06-2021 03:05:36	uuid2	33240681071174	Internet Expl
		31-03-2021 03:05:37	adnxs.com/		29-06-2021 03:05:36	anj	dTM7kM4FDun	Internet Expl
		31-03-2021 03:05:36	ptrack.com/		29-06-2021 03:05:05	GLOBALID	2uKlc8-s18d987f	Internet Expl
		31-03-2021 03:05:36	postorelease.com/		31-03-2022 03:05:36	status	1	Internet Expl
		31-03-2021 03:05:36	postorelease.com/		31-03-2022 03:05:36	ver	1	Internet Expl
		31-03-2021 03:05:36	postorelease.com/		31-03-2022 03:05:36	visitor	19e3d560-56f8-4	Internet Expl
		31-03-2021 03:05:36	slift.com/		29-06-2021 03:05:35	tluid	13416152774261	Internet Expl
		31-03-2021 03:05:35	rifhub.com/		25-04-2022 03:05:35	rud	H4sIAAAAAAAA	Internet Expl
		31-03-2021 03:05:35	rifhub.com/		25-04-2022 03:05:35	eud	H4sIAAAAAAAA	Internet Expl
		31-03-2021 03:05:35	tribalfusion.com/		30-04-2021 03:05:35	_cfduid	dfc7dc4befa9493	Internet Expl
		31-03-2021 03:05:35	tribalfusion.com/		29-06-2021 03:05:35	ANON_ID	a1nTAZcqkaHb8y	Internet Expl
		31-03-2021 03:05:35	tribalfusion.com/		29-06-2021 03:05:35	ANON_ID_old	a1nTAZcqkaHb8y	Internet Expl

Viewing 702/702 records << < 1 of 15 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
 Filter: Undo Clear



Browser History Examiner

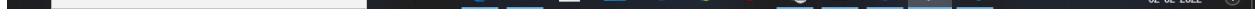
Artefact	Records	Cached Files	Report Preview
Bookmarks	1		
Cached Files	6		
Cached Images	0		
Cached Web Pages	0		
Cookies	702		
Downloads	1		
Email Addresses	0		
Favicons	0		
Form History	0		
Logins	0		
Searches	4		
Session Tabs	0		
Thumbnails	0		
Website Visits	257		

Cached Files Report Preview

Last Fetched	Content Type	URL	Fetch Count	File Size (Bytes)	Web Browser
02-02-2022 03:47:44	application/octet-stream	https://az667904.vo.msecnd.net/pub/Def...	4	12576	Internet Explorer
02-02-2022 03:23:35		/ccx.microsoft.net/api/settings/en	3	7155	Internet Explorer
02-02-2022 03:47:40		/az700632.vo.msecnd.net/pub/Ren...	1	1473	Internet Explorer
02-02-2022 01:34:15		/config.teams.microsoft.com/config/1	1	850	Internet Explorer
02-02-2022 03:47:42		/az700632.vo.msecnd.net/pub/Fig/1	1	205	Internet Explorer
		/az700632.vo.msecnd.net/pub/Fig/1	1	78	Internet Explorer

Viewing 6/6 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
 Filter by content type: All



Go to File menu and then Report>Save as PDF

CYBER FORENSICS PRACTICALS

Browser History Examiner - Trial Mode

	Last Fetched	Content Type	URL	Fetch Count	File Size (Bytes)	Web Browser (Profile)
Report	> Save as PDF	application/pdf	https://sharedcloud-pi...	30923792	Edge (Default)	
Export	> Save as HTML	application/pdf	https://www36.pdf2gc...	24829054	Edge (Default)	
Cached Images		text/javascript	https://hangouts.goog...	4	9106853	Firefox (971y8ju.default)
Cached Web Pages	2074	text/javascript	https://hangouts.goog...	8	9106853	Firefox (971y8ju.default)
Cookies	4067	text/javascript	https://hangouts.goog...	6	9106044	Firefox (971y8ju.default)
Downloads	60	text/javascript	https://www.gstatic.co...	18	6191493	Firefox (971y8ju.default)
Email Addresses	82	text/javascript	https://www.gstatic.co...	9	6153920	Firefox (971y8ju.default)
Favicons	2687	application/javascript	https://app.diagrams.r...	16	5672206	Chrome (Default)
Form History	326	application/javascript	https://rapidapi.com/...	16	5205375	Firefox (971y8ju.default)
Logins	98	text/javascript	https://www.google.cc...	28	4014905	Firefox (971y8ju.default)
Searches	1342	application/json	https://d.joinhoney.co...	1	3997541	Chrome (Default)
Session Tabs	1508	text/javascript	https://www.google.cc...	7	3989267	Firefox (971y8ju.default)
Thumbnails	26	text/javascript	https://www.google.cc...	10	3987393	Firefox (971y8ju.default)
Website Visits	5330	text/javascript	https://www.google.cc...	5	3987389	Firefox (971y8ju.default)
		text/javascript	https://www.google.cc...	9	3987389	Firefox (971y8ju.default)
		text/javascript	https://www.google.cc...	10	3987387	Firefox (971y8ju.default)
		application/x-javascript	https://images-na.ssl-i...	45	3571116	Firefox (971y8ju.default)
		application/octet-stream	https://raw.githubusercontent...	1	3538028	Firefox (971y8ju.default)
		application/javascript	https://cdn.jsdelivr.net...	7	3328160	Firefox (971y8ju.default)
		text/javascript	https://hangouts.goog...	7	3261481	Firefox (971y8ju.default)
		text/javascript	https://hangouts.goog...	12	3243258	Firefox (971y8ju.default)
		application/x-javascript	https://images-na.ssl-i...	12	3241246	Firefox (971y8ju.default)
		text/javascript	https://hangouts.goog...	7	3212371	Firefox (971y8ju.default)
		text/javascript	https://hangouts.goog...	12	3212326	Firefox (971y8ju.default)

Viewing 25/25 records

Time zone: UTC Date format: dd/mm/yyyy

From: Select a date To: Select a date

From: Select a time To: Select a time

All

Filter by content type

Report gets generated

History Report.pdf - Adobe Acrobat Reader DC (64-bit)

File Edit View Sign Window Help

Home Tools 4.40-TYBSC-Syllab... History Report.pdf

Date format: dd/mm/yyyy

Web Browser History Report

Created: 02-02-2022 10:37
Created using: Browser History Examiner v1.9
Time zone: UTC, DST Enabled
Date format: dd/mm/yyyy

Bookmarks

Date Added	Last Modified	Title	URL	Web Browser
		Bing	http://go.microsoft.com/fwlink/?LinkId=255142	Internet Explorer

Cached Files

Last Fetched	Content Type	URL	Fetch Count	File Size (Bytes)	Web Browser
02-02-2022 03:23:35		https://oxcs.microsoft.net/api/settings/en-US/xml/settings-tips?release=20h1&sku=Professional&...	3	7155	Internet Explorer
02-02-2022 01:34:15	application/json	https://config.teams.microsoft.com/config/v1/ODSP_Sync_Client/22.002.0103.0004?UpdateRing=Prod&O...	1	850	Internet Explorer

Cookies

Date Created	URL	Last Accessed	Date Expires	Name	Content	Web Browser
31-03-2021 03:05:38	rubiconproject.com/		31-03-2022 03:05:37	audit	1PrVRzLz9jKsh1nqNY9Mm+LrcqJljq2AwdArk10STZ0Vf2ZGMQQTsfYgrZB2VwUHzswKwM1kozlazit8oW2Sgb...bjrEO...	Internet Explorer
31-03-2021 03:05:38	demdex.net/		27-09-2021 03:05:38	demdex	048611188058453784222614254054679501	Internet Explorer
31-03-2021 03:05:38	amazon-adsystem.com/		01-04-2026 03:05:37	ad-privacy	0	Internet Explorer
31-03-2021 03:05:37	pubmatic.com/		29-06-2021 03:05:37	PUBMDCID	4	Internet Explorer
31-03-2021 03:05:37	casalemeda.com/		01-04-2021 03:05:37	CMST	YGPY8WBj2PEA	Internet Explorer

Downloads

URL	Local Path	State	Start Time	End Time	Bytes Downloaded	Total Bytes	Web Browser
https://www.google.com/intl/en_in/chrome/thank-you.htm?statecb=1&installdataindex=empty&defa...	C:\Users\YASH\Downloads\ChromeSetup.e						Edge

Exporting Report

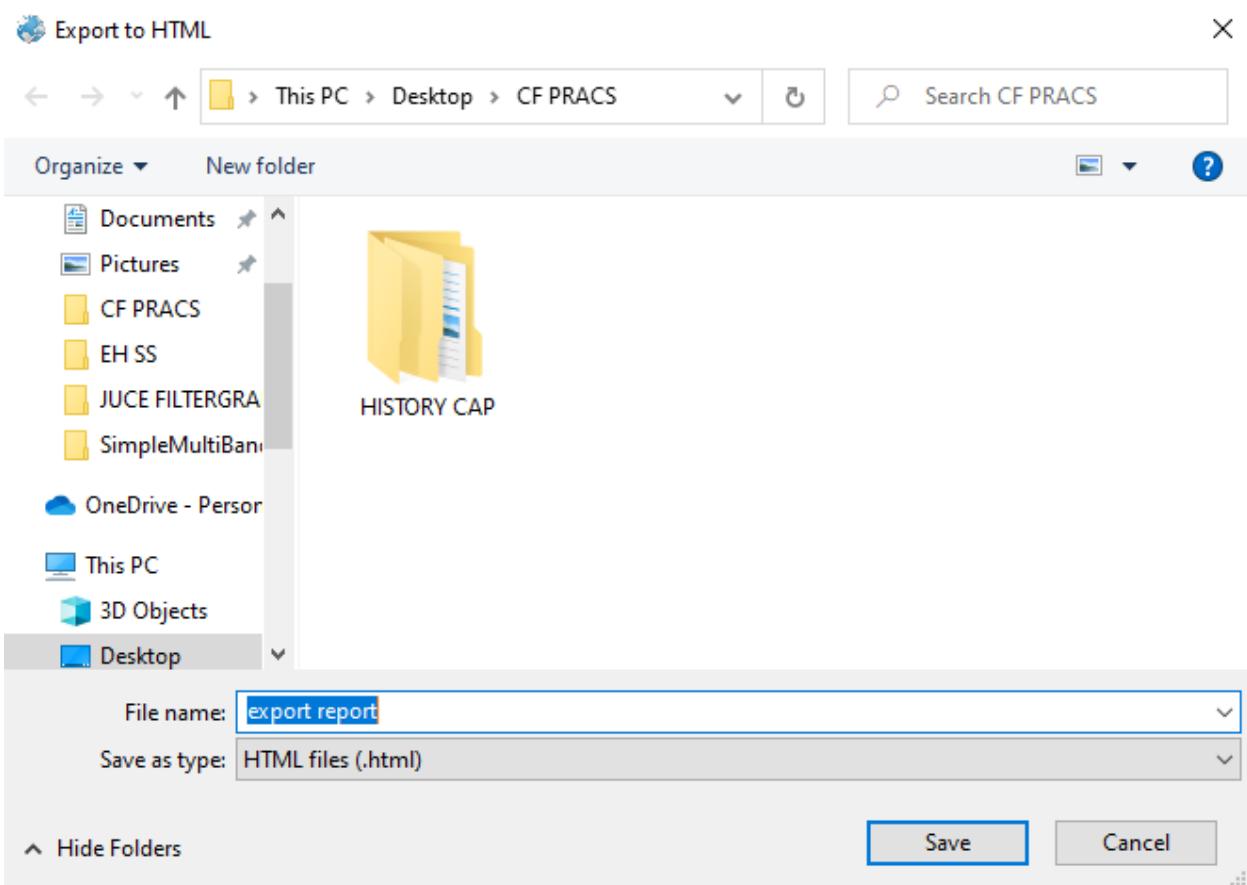
Go to File Menu Export > Export to Html

CYBER FORENSICS PRACTICALS

The screenshot shows the 'Browser History Examiner - Trial Mode' application window. The main pane displays a table of browser history items with columns: Last Fetched, Content Type, URL, Fetch Count, File Size (Bytes), and Web Browser (Profile). A context menu is open over one of the entries, with 'Export to HTML' selected. To the left, a sidebar lists various history categories with their respective record counts. On the right, there are several filter panels: 'Filter by keyword', 'Filter by date' (From: Select a date [15], To: Select a date [15]), 'Filter by time' (From: Select a time, To: Select a time), 'Filter by web browser' (All), and 'Filter by content type'. At the bottom, there's a search bar ('Type here to search') and a taskbar with icons for various applications.

Click on Export

This screenshot shows the 'Browser History Examiner - Export' dialog box. The top section, 'Select the data to export:', contains a list of checkboxes for various data types: Bookmarks, Cached Images, Cookies, Email Addresses, Form History, Searches, Thumbnails, Cached Files, Cached Web Pages, Downloads, Favicons, Logins, Session Tabs, and Website Visits. Most checkboxes are checked. Below this is the 'Export settings:' section, which includes three radio buttons: 'Export all records' (selected), 'Export currently filtered records', and 'Export records in report'. At the bottom are two buttons: 'Export' and 'Cancel'.



Report gets exported into html

Web Browser History Report

Created: 11-02-2022 19:09
 Created using: Browser History Examiner v1.16
 Time zone: UTC
 Date format: dd/mm/yyyy

Bookmarks

Date Added	Last Modified	Title	URL	Web Browser (Profile)
18-01-2022 05:05:21	18-01-2022 05:05:21	Student_Schedule	https://www.teachusedumation.com/weblogin/student_schedule.html	Firefox (f971y8ju.default-release)
08-01-2022 13:45:53		AIMCA - Fastrack Test Series - 2021- 22	https://live.impetusqurukul.com/aimca-fastrack-test-series-2021-22	Chrome (Default)
07-10-2021 04:03:08	07-10-2021 04:03:08	Getting Started	https://www.mozilla.org/en-US/firefox/central/	Firefox (f971y8ju.default-release)
07-10-2021 04:03:08	07-10-2021 04:03:08	Get Help	https://support.mozilla.org/en-US/products/firefox	Firefox (f971y8ju.default-release)
07-10-2021 04:03:08	07-10-2021 04:03:08	Customize Firefox	https://support.mozilla.org/en-US/kb/customize-firefox-controls-buttons-and-toolbars?utm_source=fire...	Firefox (f971y8ju.default-release)
07-10-2021 04:03:08	07-10-2021 04:03:08	Get Involved	https://www.mozilla.org/en-US/contribute/	Firefox (f971y8ju.default-release)
07-10-2021 04:03:08	07-10-2021 04:03:08	About Us	https://www.mozilla.org/en-US/about/	Firefox (f971y8ju.default-release)
06-10-2021 07:06:06		YouTube	https://youtube.com/	Chrome (Default)
06-10-2021 07:05:51		Gmail	https://accounts.google.com/b/0/AddMailService	Chrome (Default)
06-10-2021 07:05:51		Maps	https://maps.google.com/	Chrome (Default)
05-10-2021 13:46:55		Utomik Games	https://www.utmok.com/hp_edgefavourites	Edge (Default)
05-10-2021 13:46:55		Booking.com	https://www.booking.com/index.html?aid=1980379&label=edge2020	Edge (Default)

Last Internet Activity gets listed below in the exported report

CYBER FORENSICS PRACTICALS

Student_Schedule TYCS 2021-22 Ethical Hacking covid - Google Search Web Browser History Report

Time zone: UTC
Date format: dd/mm/yyyy

Bookmarks

Date Added	Last Modified	Title	URL	Web Browser (Profile)
18-01-2022 05:05:21	18-01-2022 05:05:21	Student_Schedule	https://www.teachasedumation.com/weblogin/student_schedule.html	Firefox (f971y8ju.default-release)
08-01-2022 13:45:53		AIMCA - Fastrack Test Series - 2021- 22	https://live.impetusgurukul.com/aimca-fastrack-test-series-2021-22	Chrome (Default)
07-10-2021 04:03:08	07-10-2021 04:03:08	Getting Started	https://www.mozilla.org/en-US/firefox/central/	Firefox (f971y8ju.default-release)
07-10-2021 04:03:08	07-10-2021 04:03:08	Get Help	https://support.mozilla.org/en-US/products/firefox	Firefox (f971y8ju.default-release)
07-10-2021 04:03:08	07-10-2021 04:03:08	Customize Firefox	https://support.mozilla.org/en-US/kb/customize-firefox-controls-buttons-and-toolbars?utm_source=fire...	Firefox (f971y8ju.default-release)
07-10-2021 04:03:08	07-10-2021 04:03:08	Get Involved	https://www.mozilla.org/en-US/contribute/	Firefox (f971y8ju.default-release)
07-10-2021 04:03:08	07-10-2021 04:03:08	About Us	https://www.mozilla.org/en-US/about/	Firefox (f971y8ju.default-release)
06-10-2021 07:06:06		YouTube	https://youtube.com/	Chrome (Default)
06-10-2021 07:05:51		Gmail	https://accounts.google.com/b/0/AddMailService	Chrome (Default)
06-10-2021 07:05:51		Maps	https://maps.google.com/	Chrome (Default)
05-10-2021 13:46:55		Utomik Games	https://www.utomik.com/hp_dgefavourites	Edge (Default)
05-10-2021 13:46:55		Booking.com	https://www.booking.com/index.html?aid=1980379&label=edge2020	Edge (Default)
05-10-2021 13:46:55		Express VPN	http://js.redirect.hp.com/jumpstation?bd=expressvpn&c=*&locale=en_us&pf=*s=*tp...	Edge (Default)
05-10-2021 13:46:55		LastPass password manager	http://js.redirect.hp.com/jumpstation?bd=lastpass&c=*&locale=*pf=*s=*tp=edge	Edge (Default)

07-10-2021

Highlight All Match Case Match Diacritics Whole Words 0 of 12 matches

Windows Taskbar: Type here to search, Chrome, Notepad, Firefox, Edge, File Explorer, Task View, Taskbar icons, ENG, 19:11, 11-02-2022

Student_Schedule TYCS 2021-22 Ethical Hacking covid - Google Search Web Browser History Report

file:///C/Users/nikhil/OneDrive/Documents/sem 6 practicals/cf/prac10/temp.html

Browser Settings

Name	Value	Web Browser (Profile)
Tabs Last Sync		Firefox (f971y8ju.default-release)
Sync Preferences	Yes	Edge (Default)
Sync Passwords	Yes	Edge (Default)
Sync Extensions	Yes	Edge (Default)
Sync Bookmarks	Yes	Edge (Default)
Sync Autofill	Yes	Edge (Default)
Last Sync Time	11-02-2022 13:03:23	Chrome (Default)
Last Sync Time	11-02-2022 13:03:10	Edge (Default)
Account Name (2)	SYCS45 Nik	Chrome (Default)
Account Name (1)	Nikhil Singh	Chrome (Default)
Account Name (0)	Nikhil Singh	Chrome (Default)
Account Name (0)		Edge (Default)
Account Email (2)	bsccs45@gmail.com	Chrome (Default)
Account Email (1)	nikhilsingh52645@gmail.com	Chrome (Default)
Account Email (0)	nikhilsingh892710@gmail.com	Chrome (Default)
Account Email (0)	nikhilsingh52645@outlook.com	Edge (Default)

Cached Files

Last Fetched	Content Type	URL	Fetch Count	File Size (Bytes)	Web Browser (Profile)
	application/pdf	https://sharedcloud-production-us-east-1-data-asset.s3-accelerate.amazonaws.com/c5697f39-5aeb-48f4-8...		30923792	Edge (Default)
	application/pdf	https://www36.pdf2go.com/dl/web7/download-file/a7f94843-6e24-4529-b0fe-		24920054	Edge (Default)

Windows Taskbar: Type here to search, Chrome, Notepad, Firefox, Edge, File Explorer, Task View, Taskbar icons, ENG, 19:10, 11-02-2022