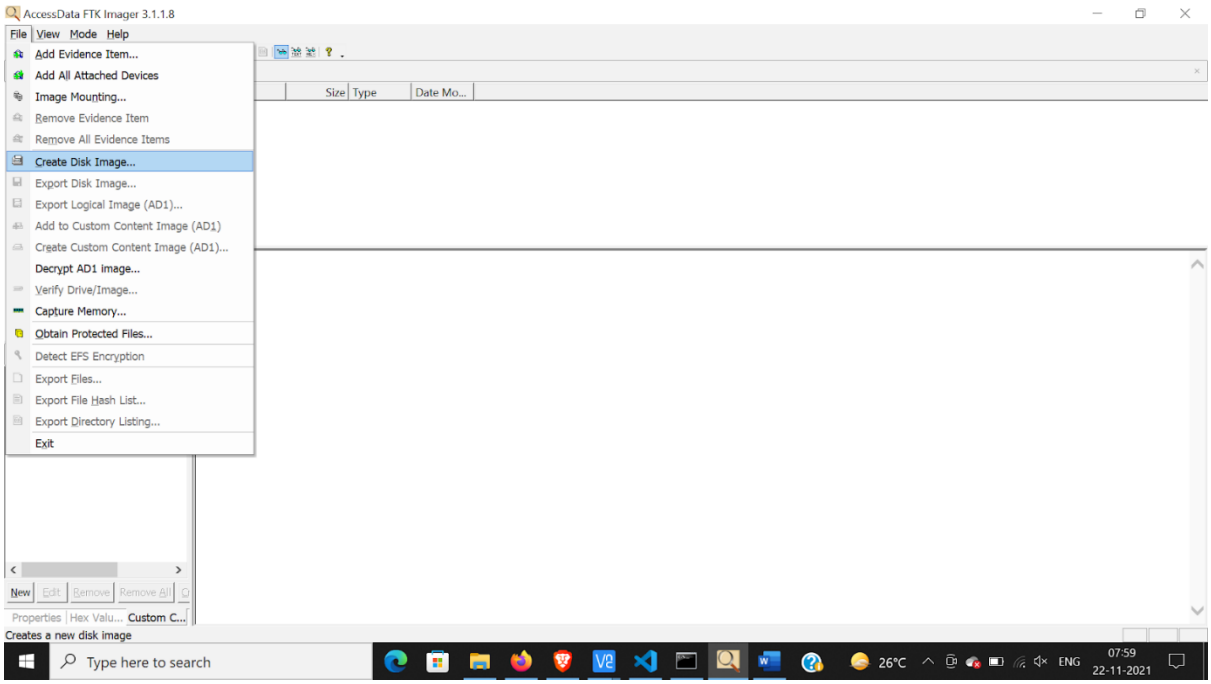
INDEX

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	

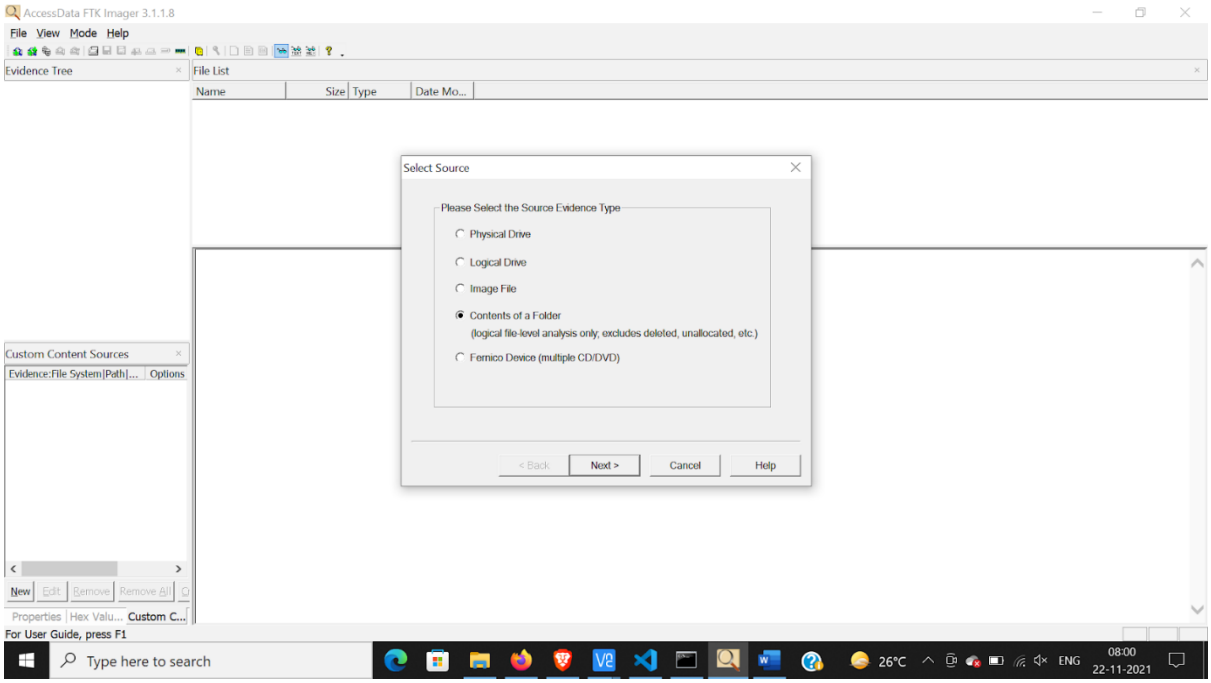
Practical : 1

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

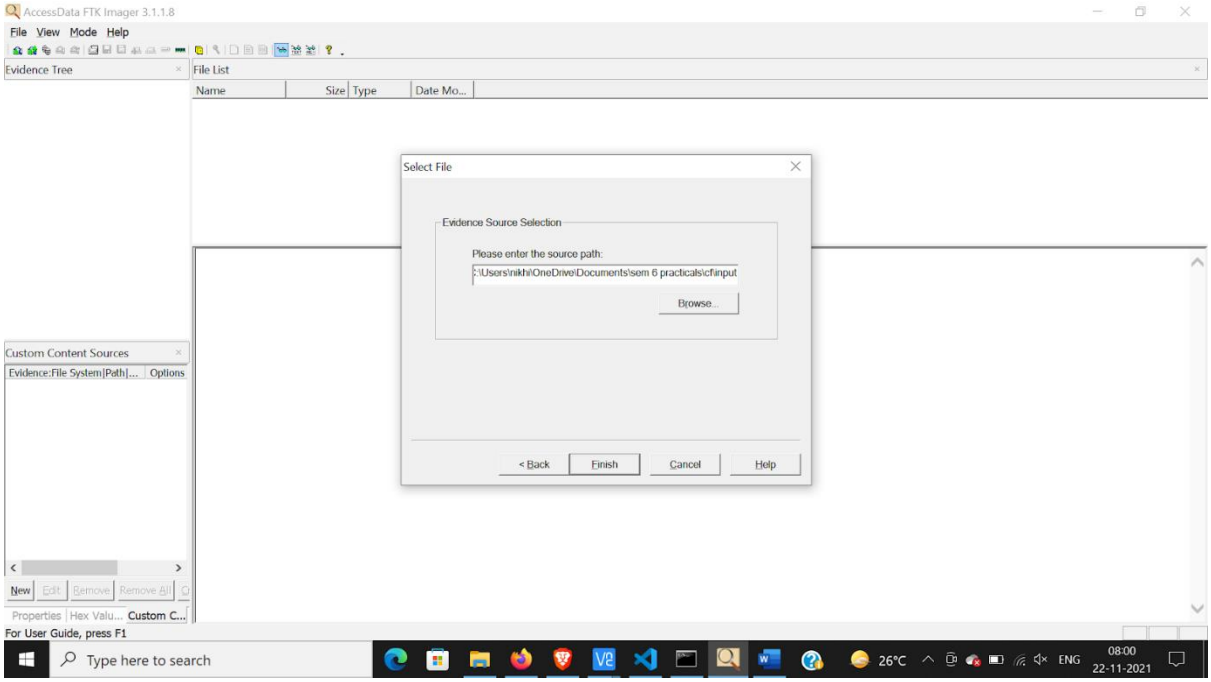
CREATE A NEW DISK IMAGE



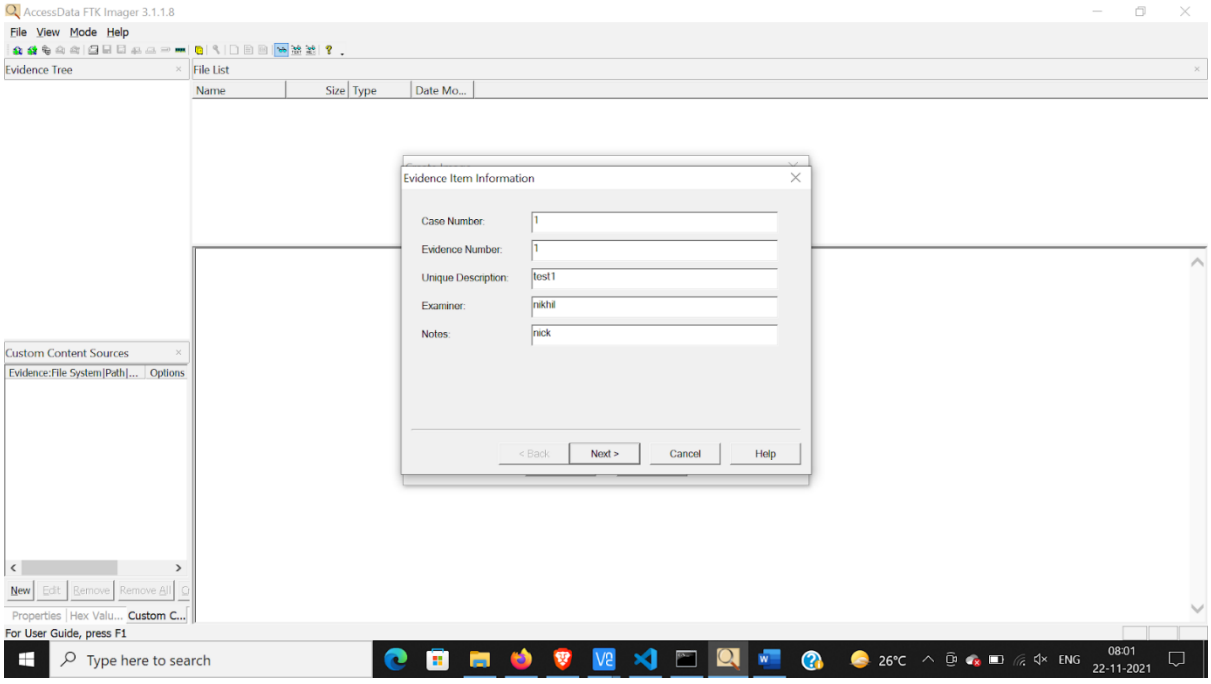
SELECT CONTENTS OF A FOLDER



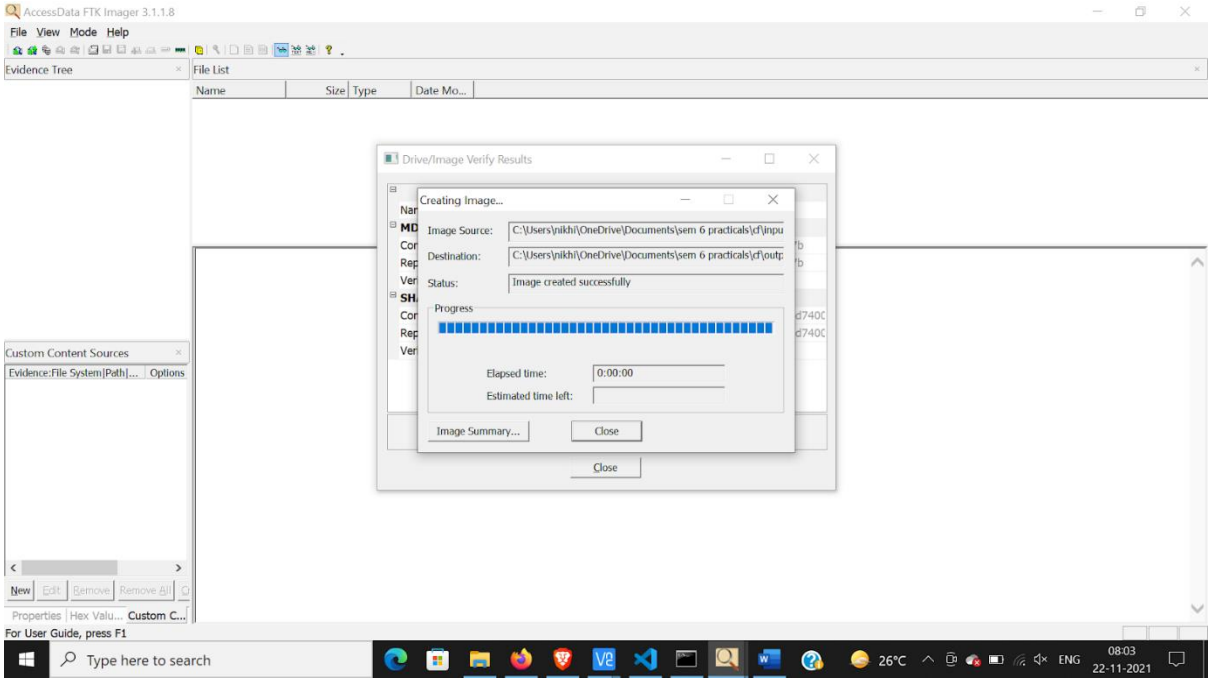
BROWSE THE FOLDER

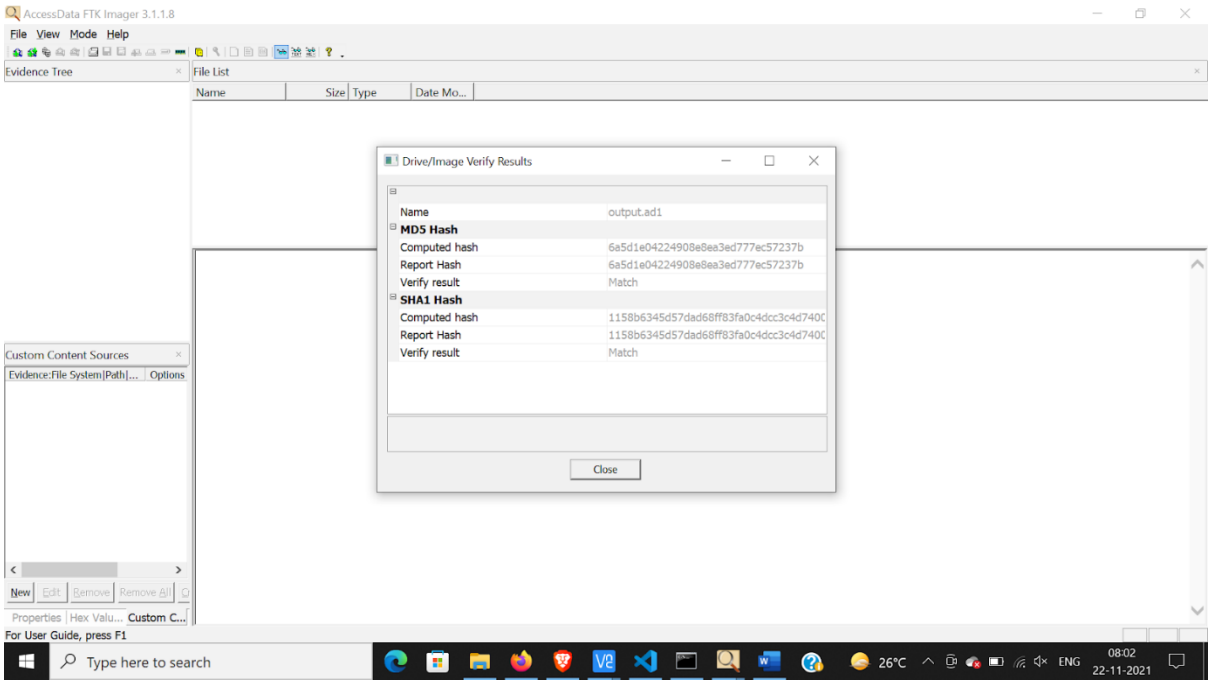


ENTER THE FOLLOWING FIELDS

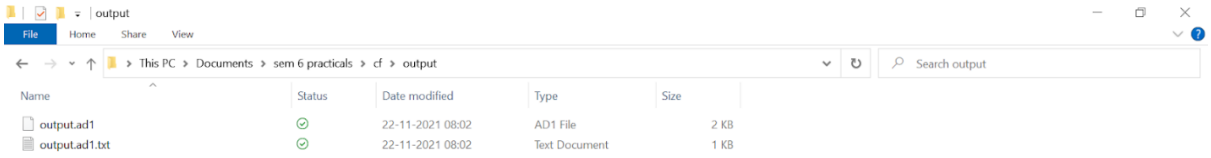


ENTER DESTINATION

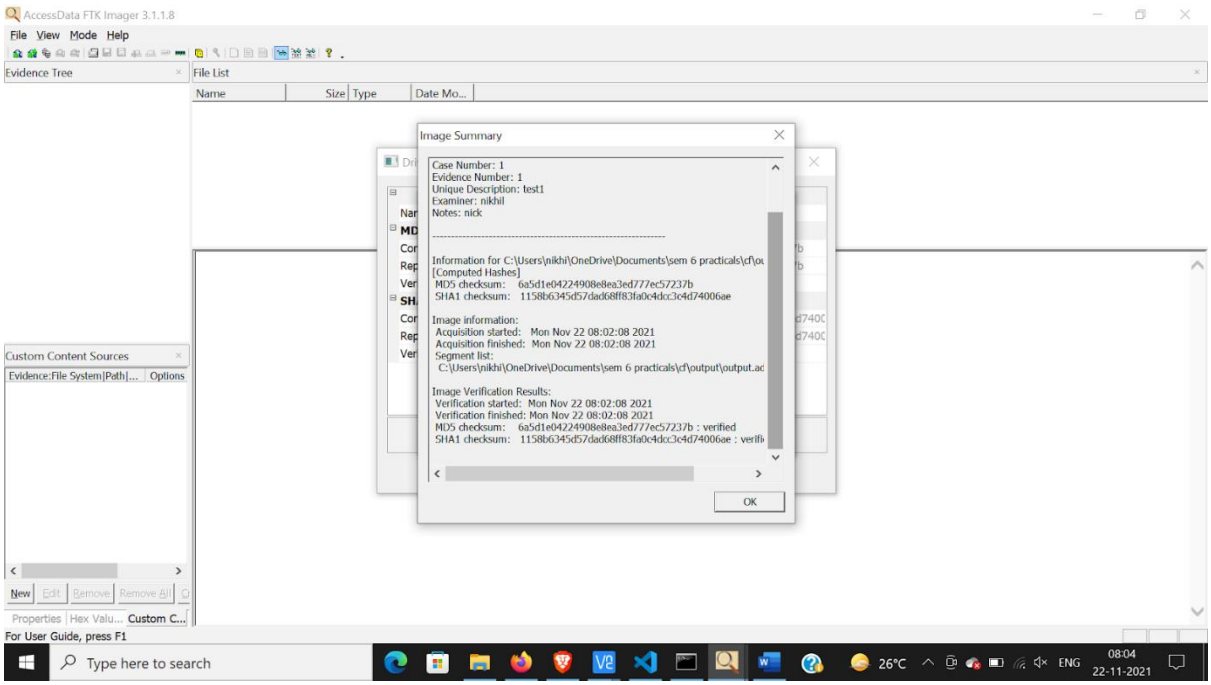




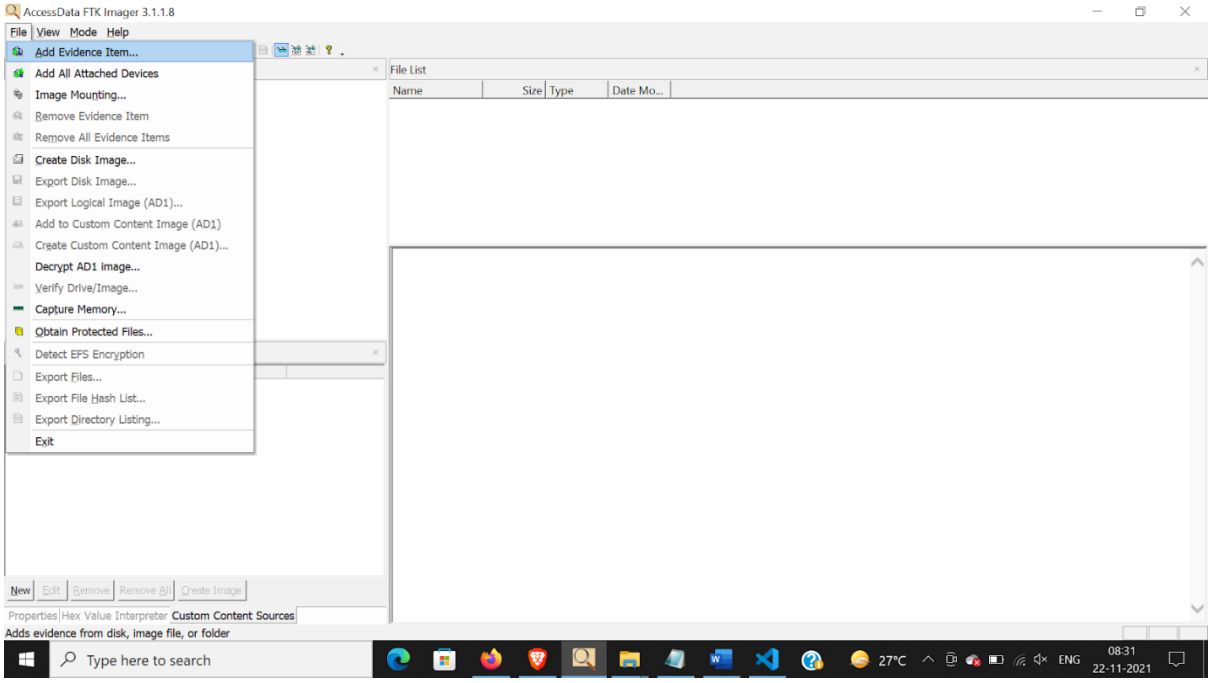
THIS IS HOW THE OUTPUT FILE WILL LOOK LIKE


output
File
Home
Share
View
This PC › Documents › sem 6 practicals › cf › output
Search output
Name
Status
Date modified
Type
Size
output.ad1
22-11-2021 08:02
AD1 File
2 KB
output.ad1.txt
22-11-2021 08:02
Text Document
1 KB

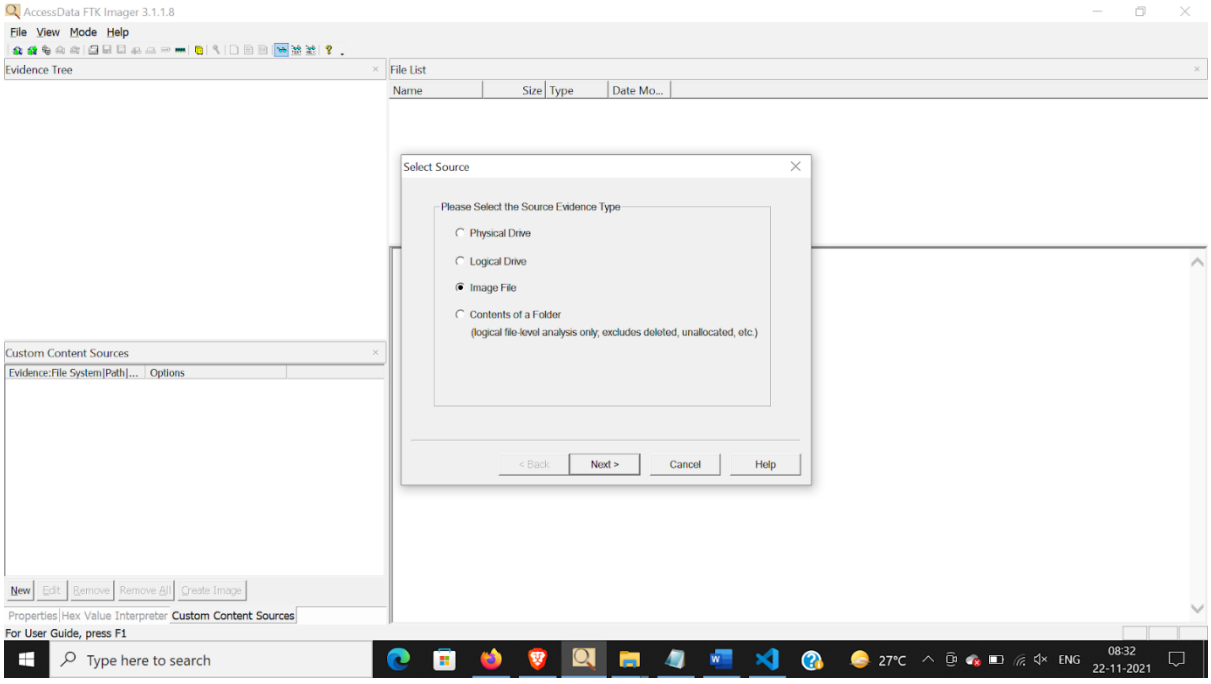

2 items
Type here to search
26°C
ENG
08:02
22-11-2021


AccessData FTK Imager 3.1.1.8
File View Mode Help
Evidence Tree
File List
Name
Size
Type
Date Mo...
Image Summary
Case Number: 1
Evidence Number: 1
Unique Description: test1
Examiner: nikhil
Notes: nick
Information for C:\Users\nikhi\OneDrive\Documents\sem 6 practicals\cf\ou
[Computed Hashes]
MD5 checksum: 6a5d1e04224908e8ea3ed777ec57237b
SHA1 checksum: 1158b6345d57dad68ff83fa0c4dcc3c4d74006ae
Image information:
Acquisition started: Mon Nov 22 08:02:08 2021
Acquisition finished: Mon Nov 22 08:02:08 2021
Segment list:
C:\Users\nikhi\OneDrive\Documents\sem 6 practicals\cf\output\output.ad
Image Verification Results:
Verification started: Mon Nov 22 08:02:08 2021
Verification finished: Mon Nov 22 08:02:08 2021
MD5 checksum: 6a5d1e04224908e8ea3ed777ec57237b : verified
SHA1 checksum: 1158b6345d57dad68ff83fa0c4dcc3c4d74006ae : verifi
OK
Custom Content Sources
Evidence:File System|Path|...
Options
New
Edit
Remove
Remove All
Properties
Hex Valu...
Custom C...
For User Guide, press F1
Type here to search
26°C
ENG
08:04
22-11-2021

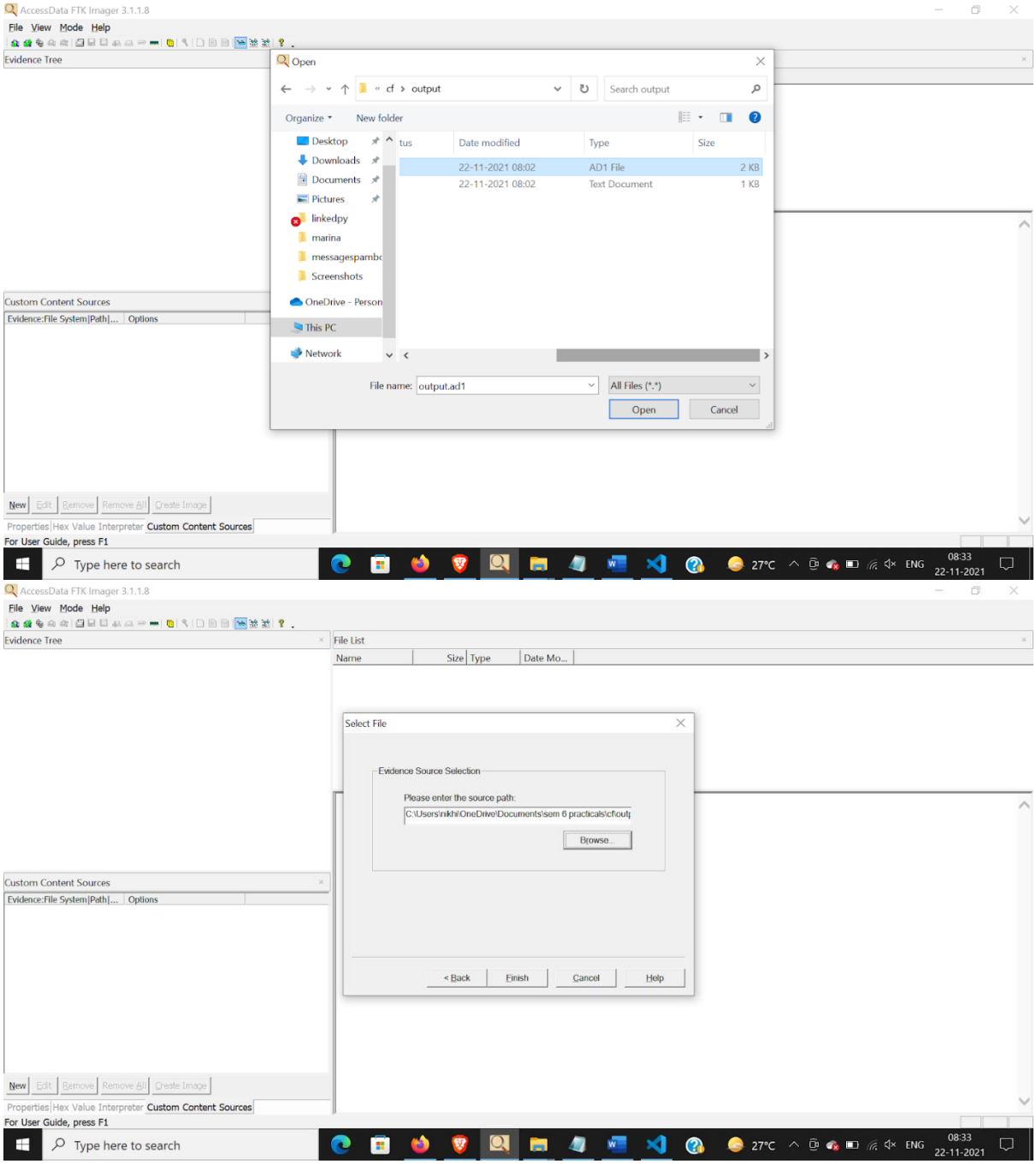
ADD EVIDENCE



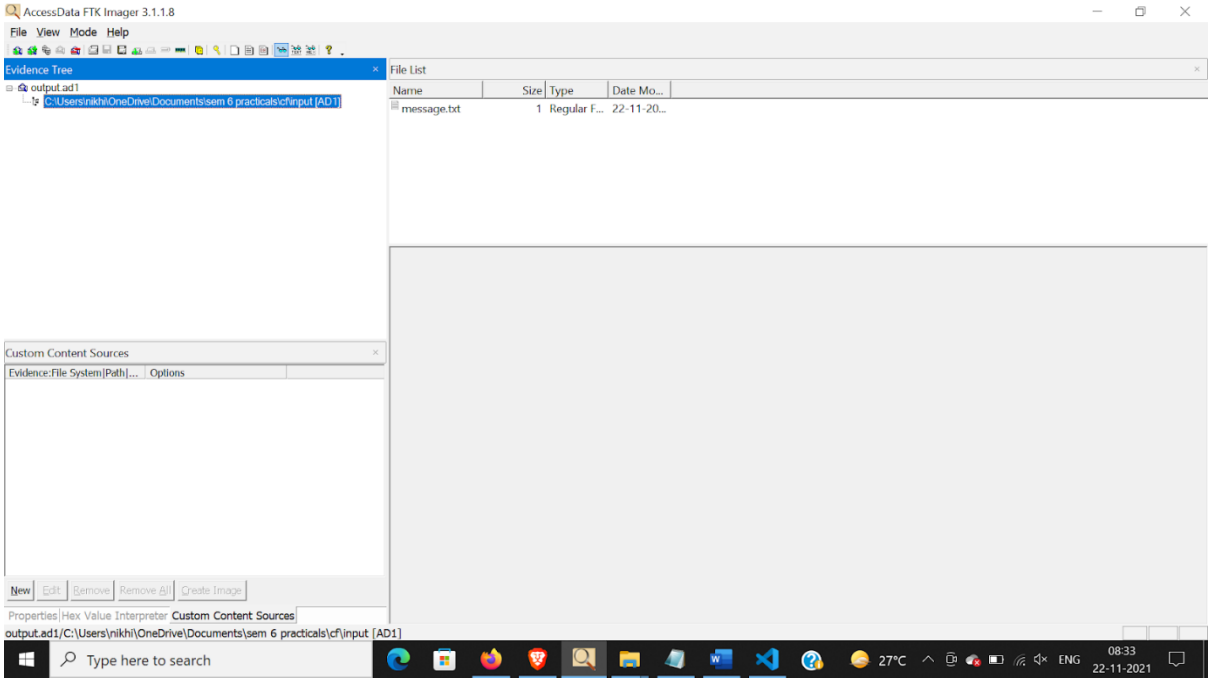
SELECT IMAGE FILE



SELECT OUTPUT FILE



YOU CAN SEEE THE OUTPUT FILE IN EVIDENCE TREE



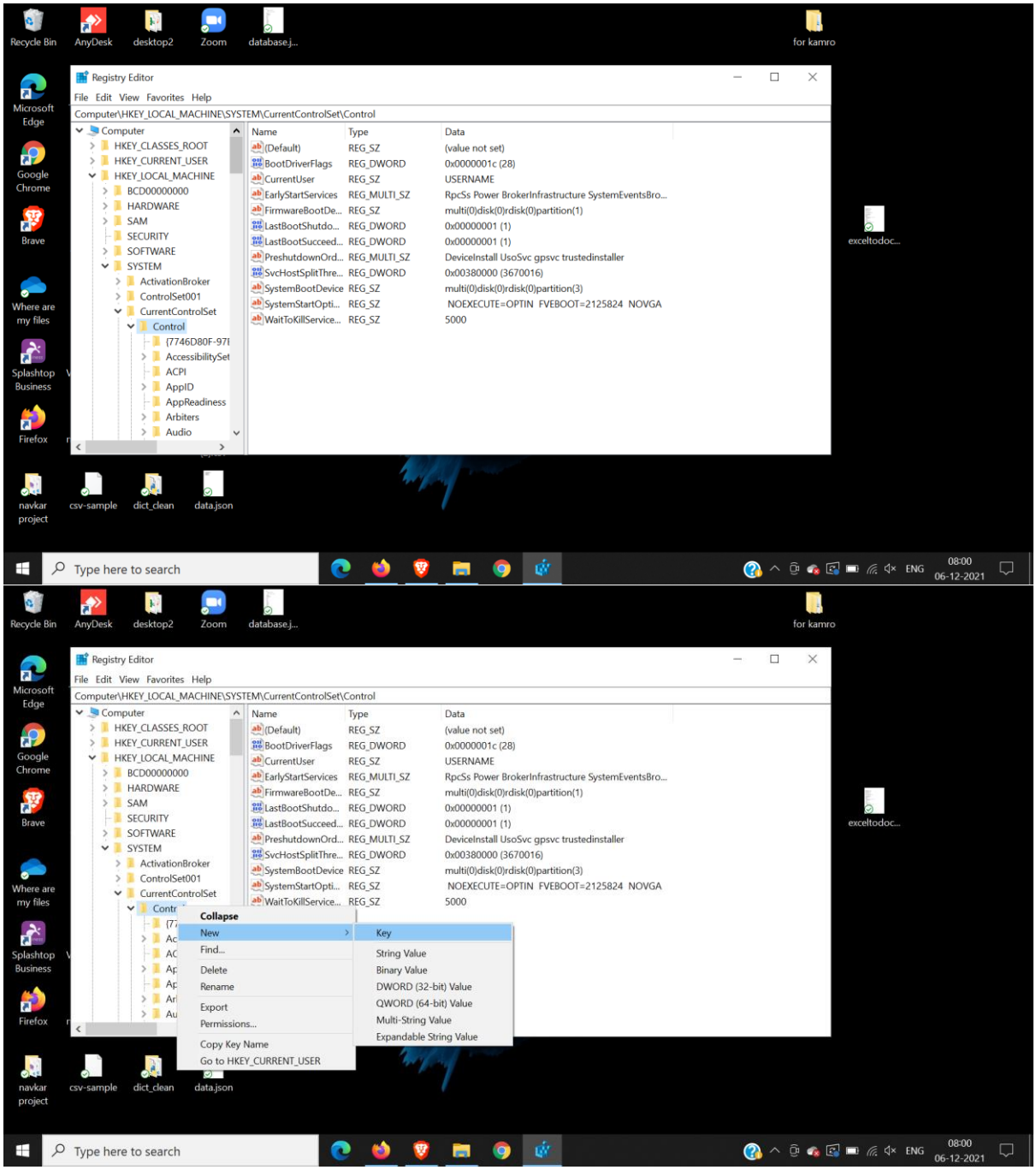
Practical:2

Aim:

Open win registory editor using run>regedit

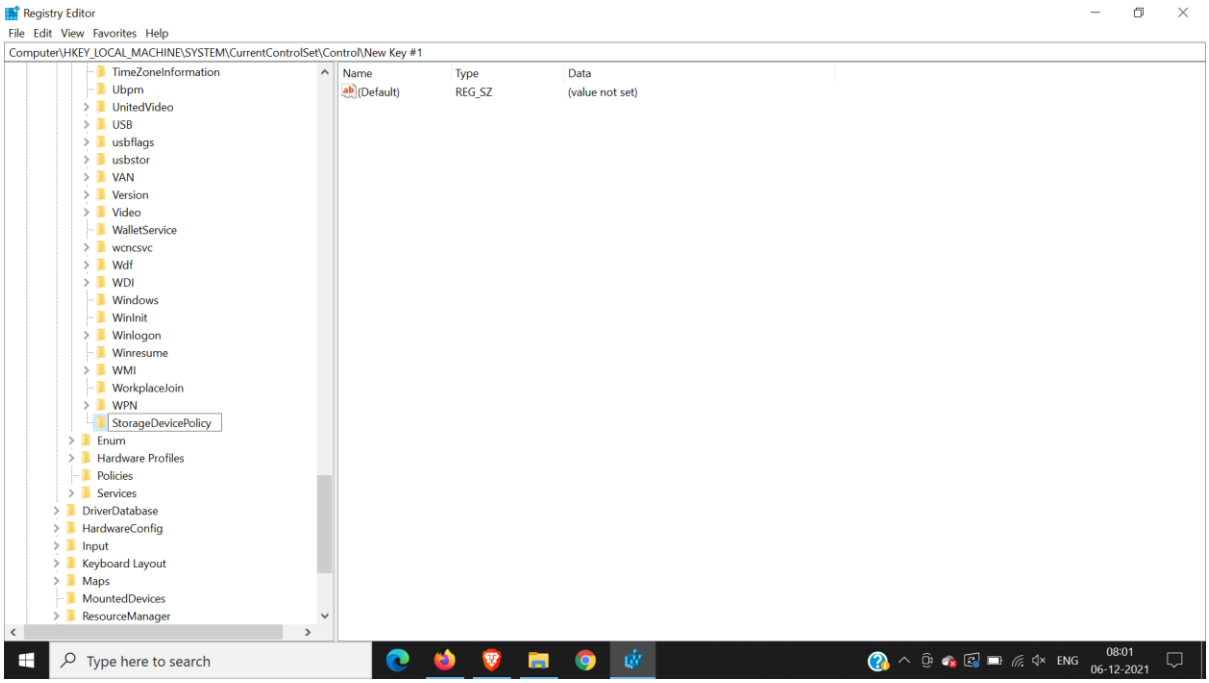
Go to Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\ and create new key

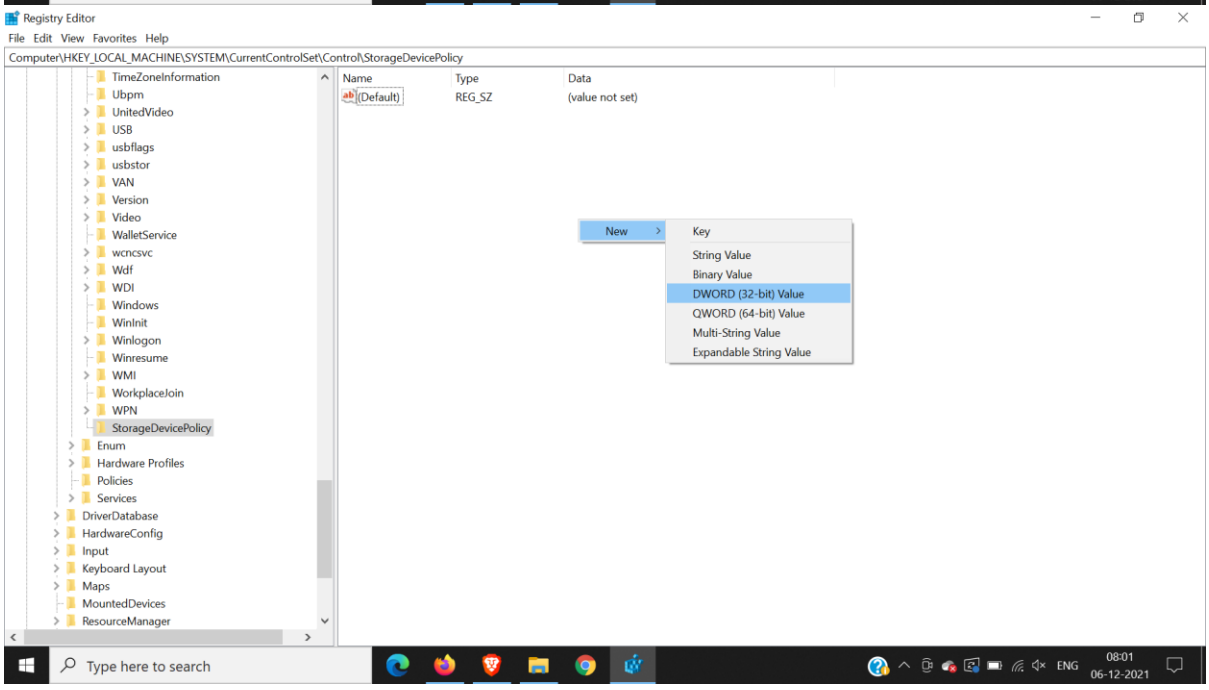
Name this key “StorageDevicePolicies”

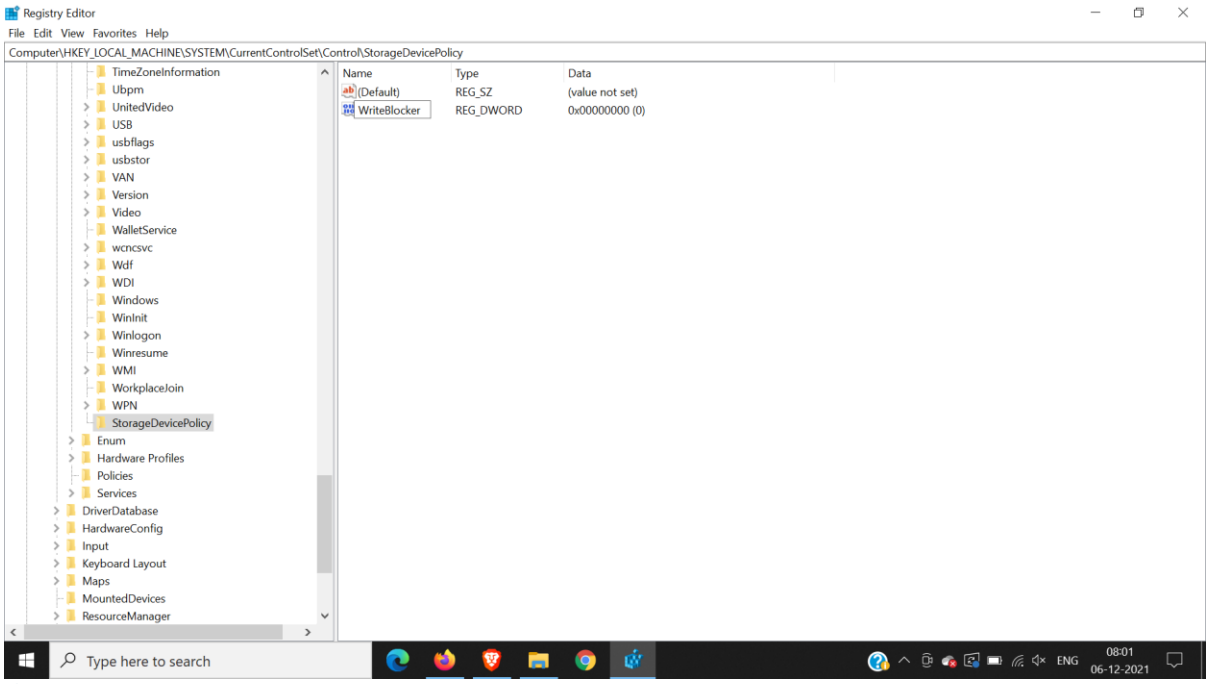


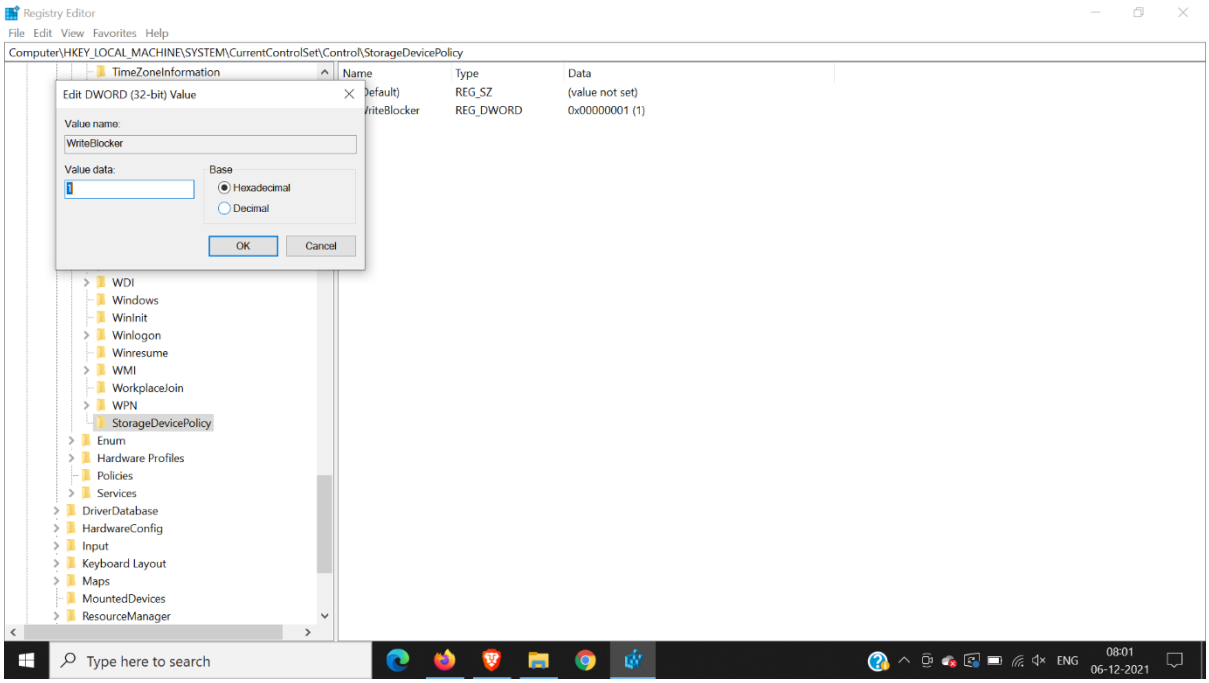
Make New Dword name it “WriteProtect”

Enter Hexa value as 1

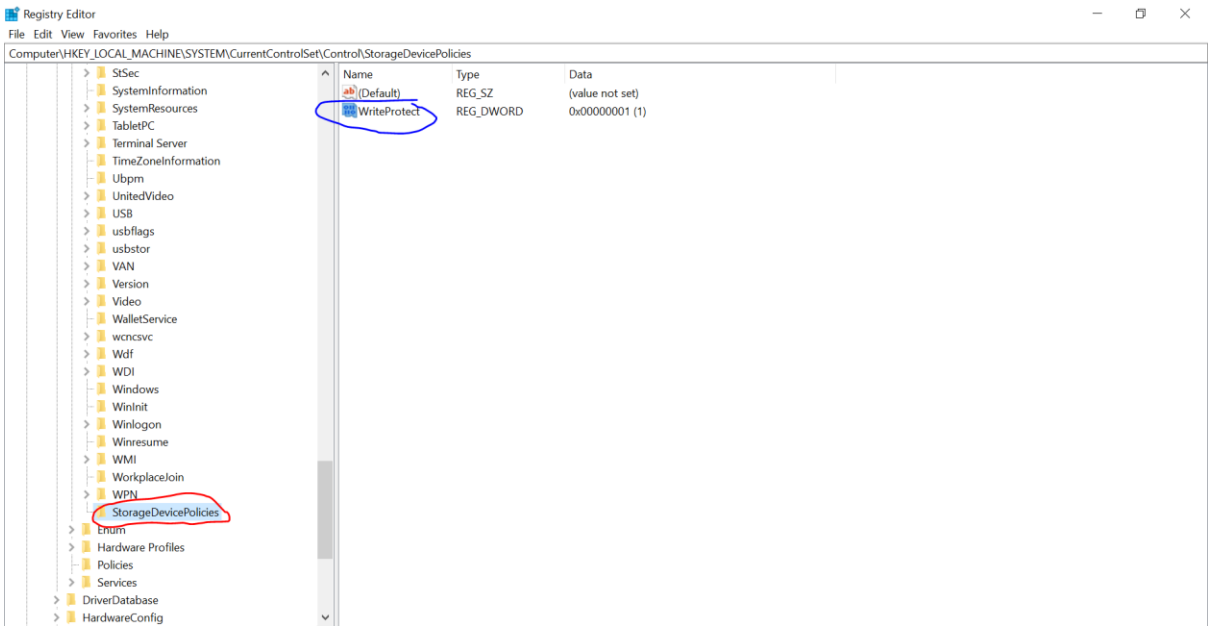




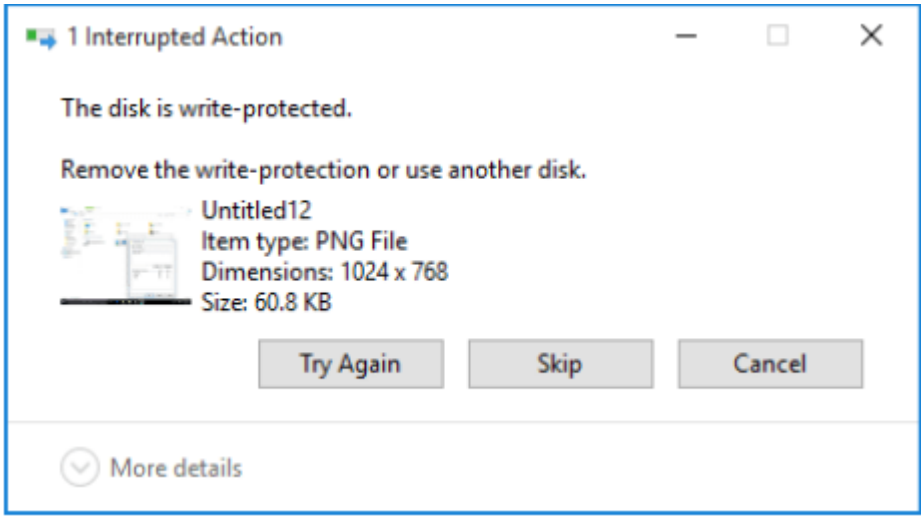

Registry Editor
File Edit View Favorites Help
Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\StorageDevicePolicy
TimeZoneInformation
Ubpm
UnitedVideo
USB
usbflags
usbstor
VAN
Version
Video
WalletService
wcncsvc
Wdf
WDI
Windows
WinInit
Winlogon
Winresume
WMI
WorkplaceJoin
WPN
StorageDevicePolicy
Enum
Hardware Profiles
Policies
Services
DriverDatabase
HardwareConfig
Input
Keyboard Layout
Maps
MountedDevices
ResourceManager
Name
Type
Data
(Default)
REG_SZ
(value not set)
WriteBlocker
REG_DWORD
0x00000000 (0)
Type here to search
ENG
08:01
06-12-2021


Registry Editor
File Edit View Favorites Help
Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\StorageDevicePolicy
Edit DWORD (32-bit) Value
Value name:
WriteBlocker
Value data:
1
Base
Hexadecimal
Decimal
OK
Cancel
REG_SZ
(value not set)
REG_DWORD
0x00000001 (1)
Type here to search
ENG
08:01
06-12-2021

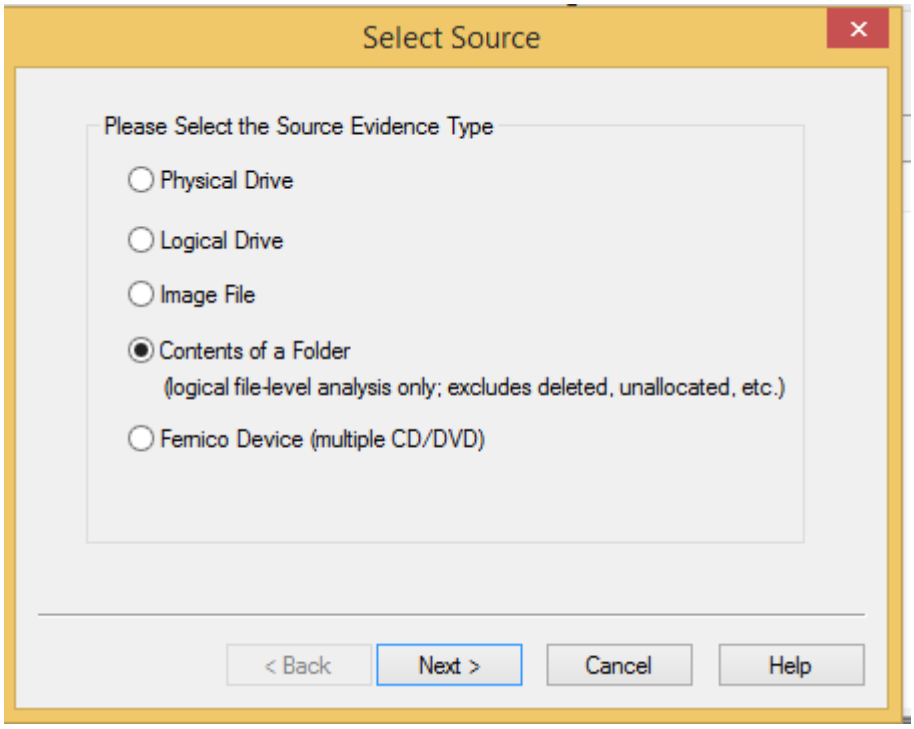
THE SPELLING IS VERY IMPORTANT RENAME IF YOU ENTERED WRONG
“StorageDevicePolicies”
“WriteProtect”



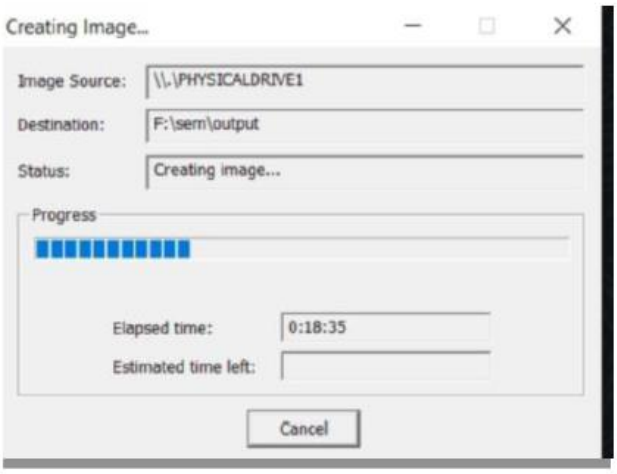
We can only open the file in the USB drive for reading, but it’s not allowed to modify and save the changes back to USB drive.

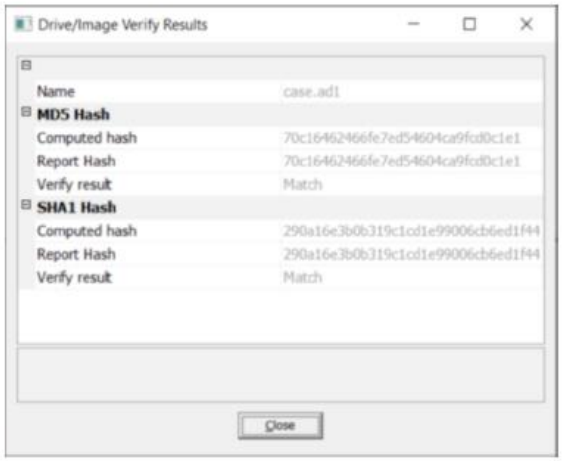


Now Create image of the USB drive using FTK imager



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



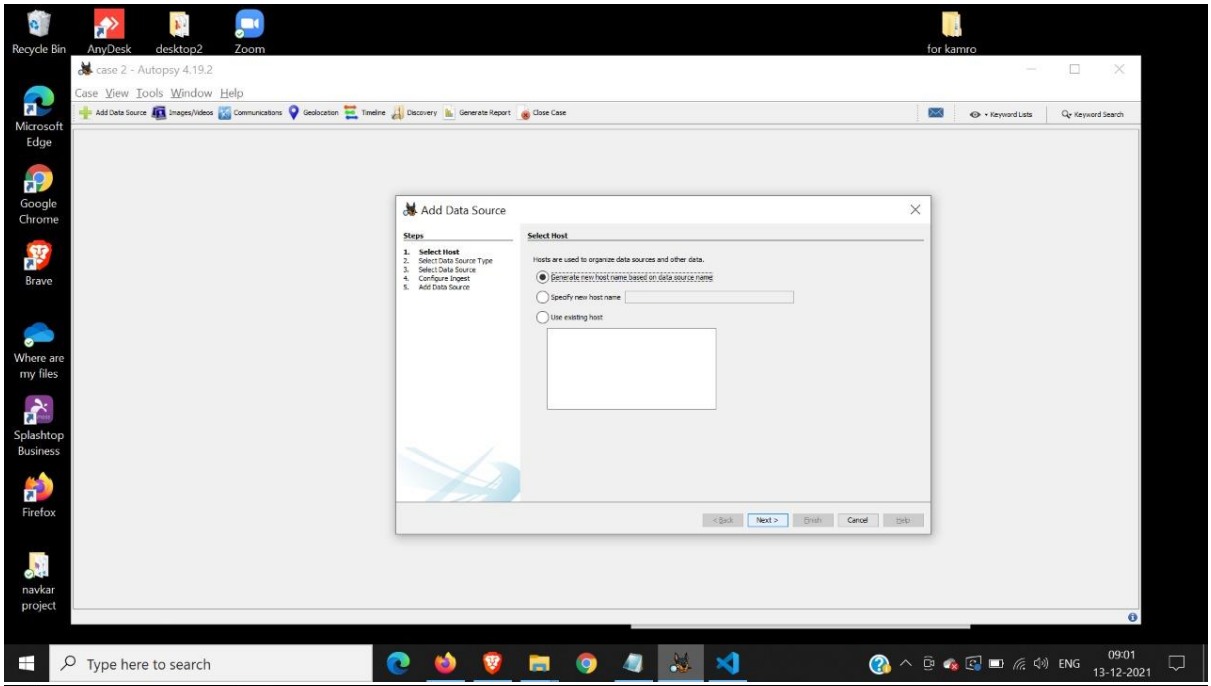


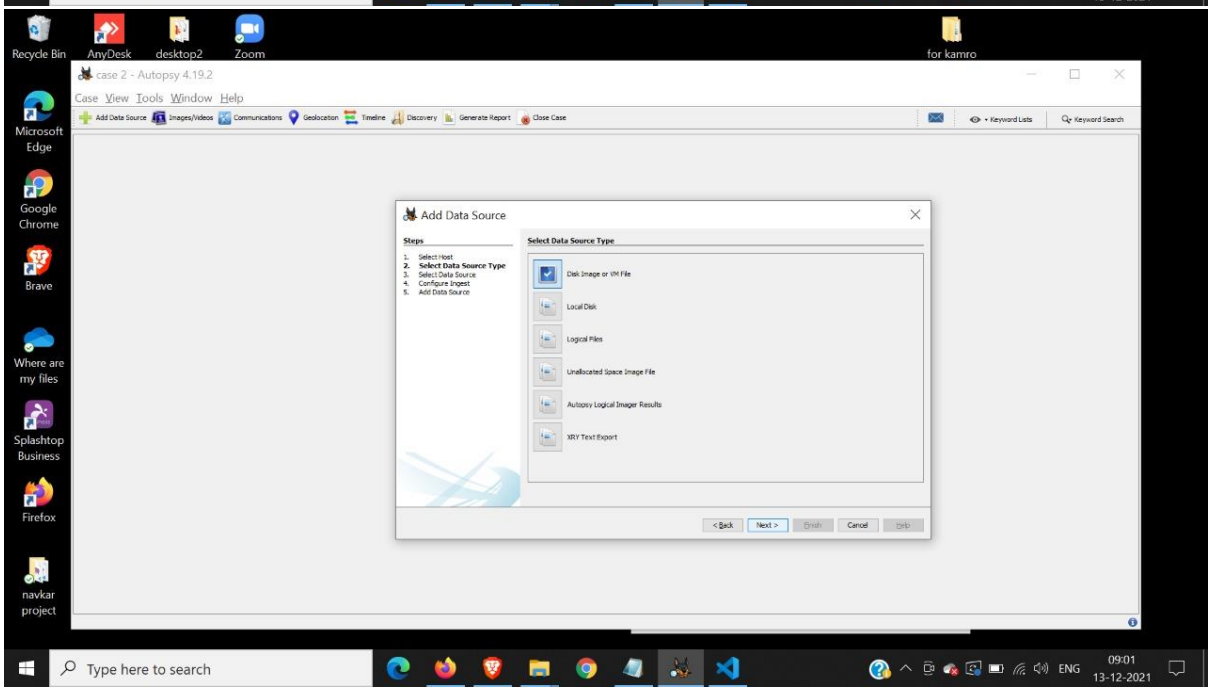
Practical No – 3

Aim: Forensics Case Study:

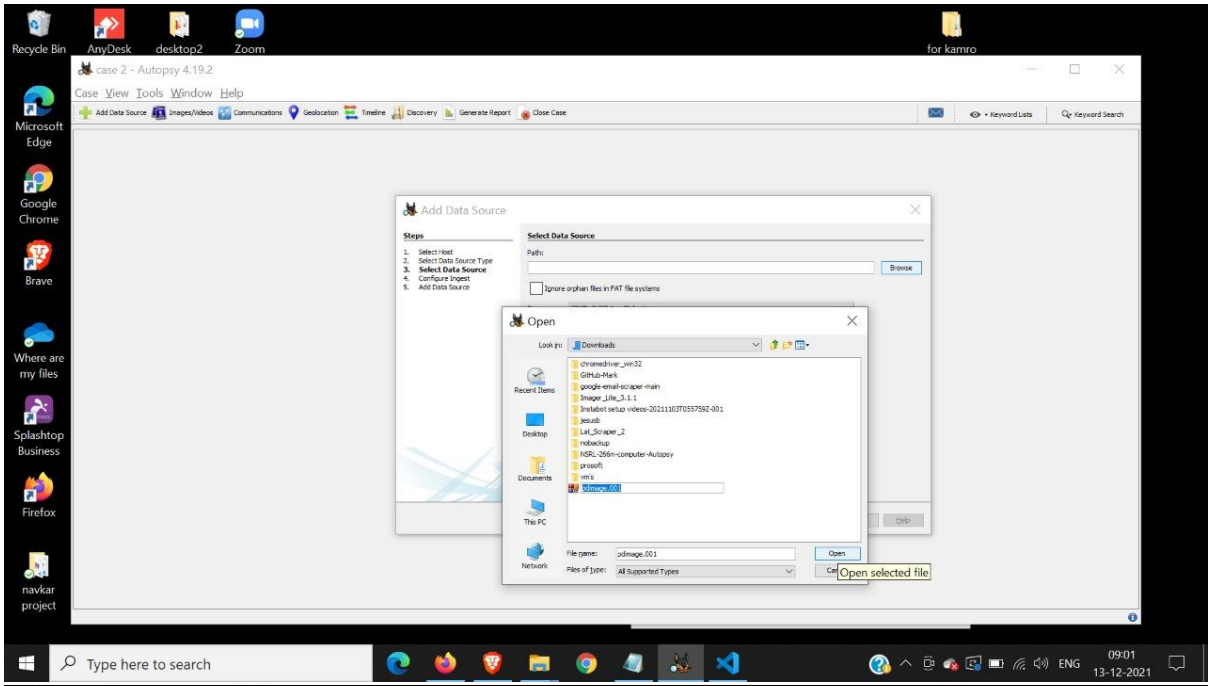
- Solve the Case study (image file) provide in lab using Autopsy

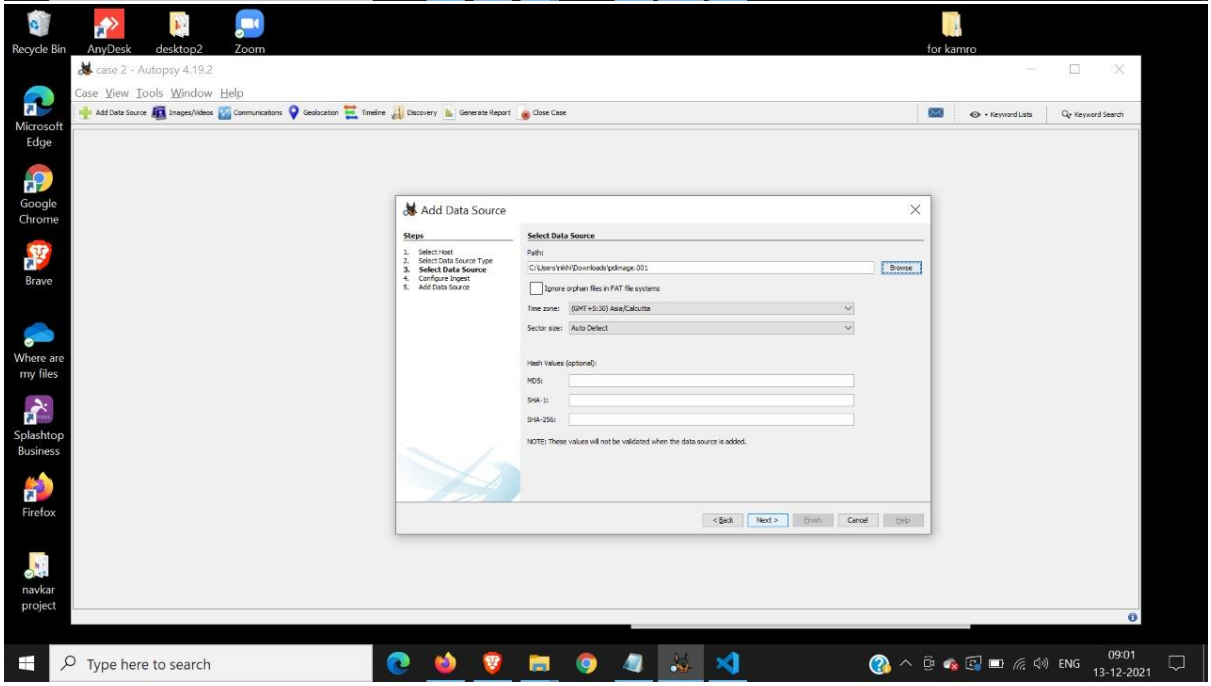
Install autopsy software and select new data source, select disk image or utf file



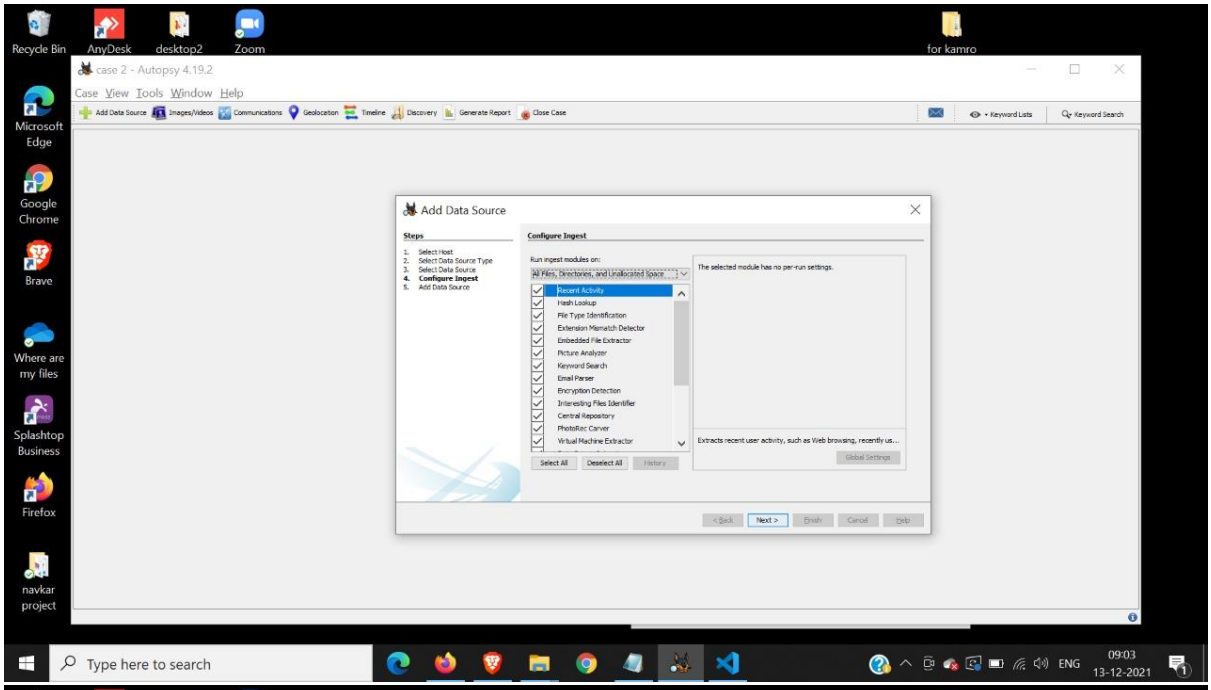


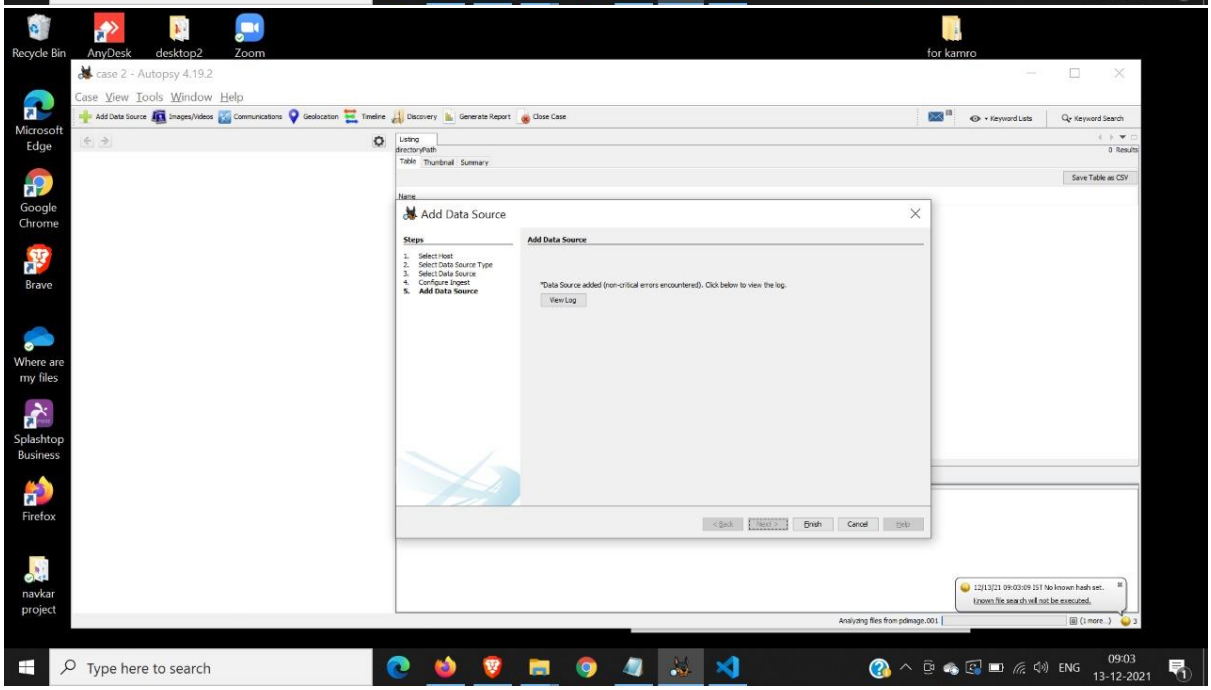
Browse and select the image of the pendrive made by ftk imager, enter the optional values if needed





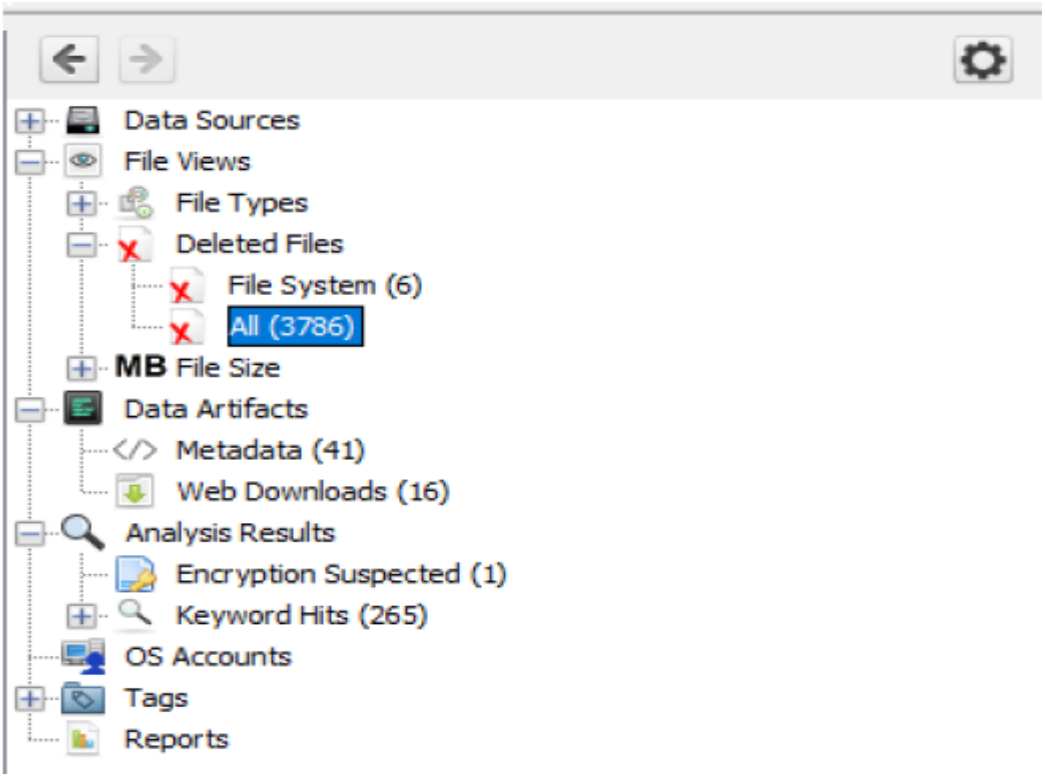
Configure ingest elect all options and add data source



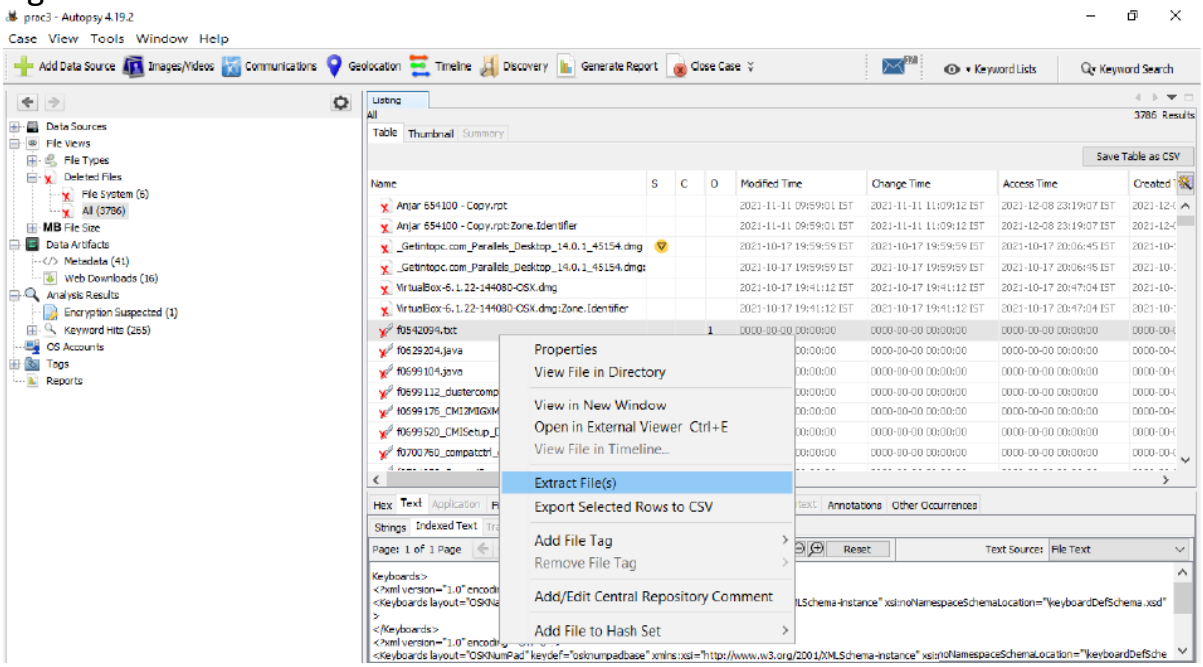


On the left hierarchy lookup for deleted files

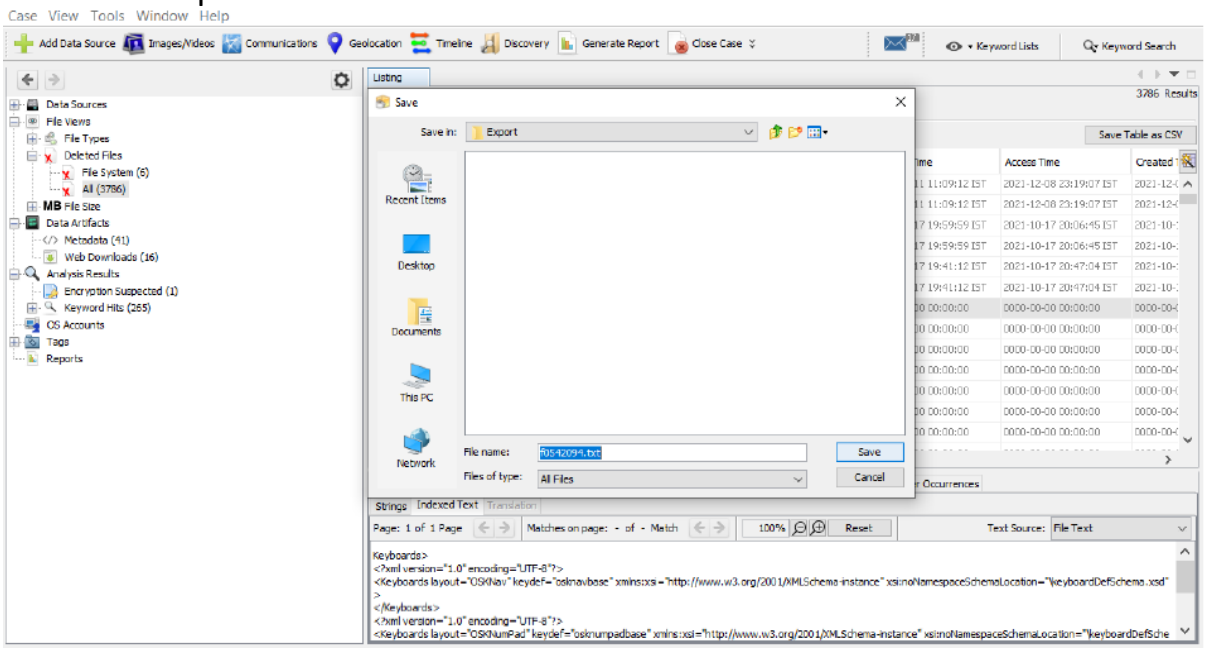
Expand it and click on All

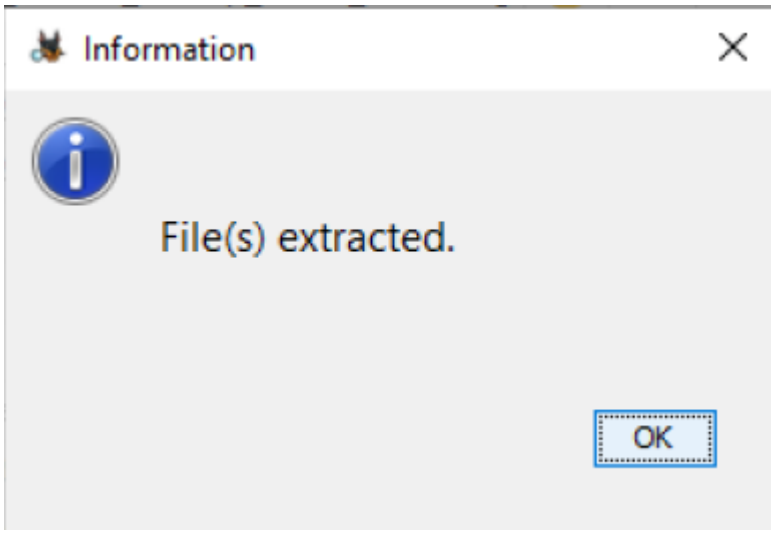


Right click on the table view and select Extract files

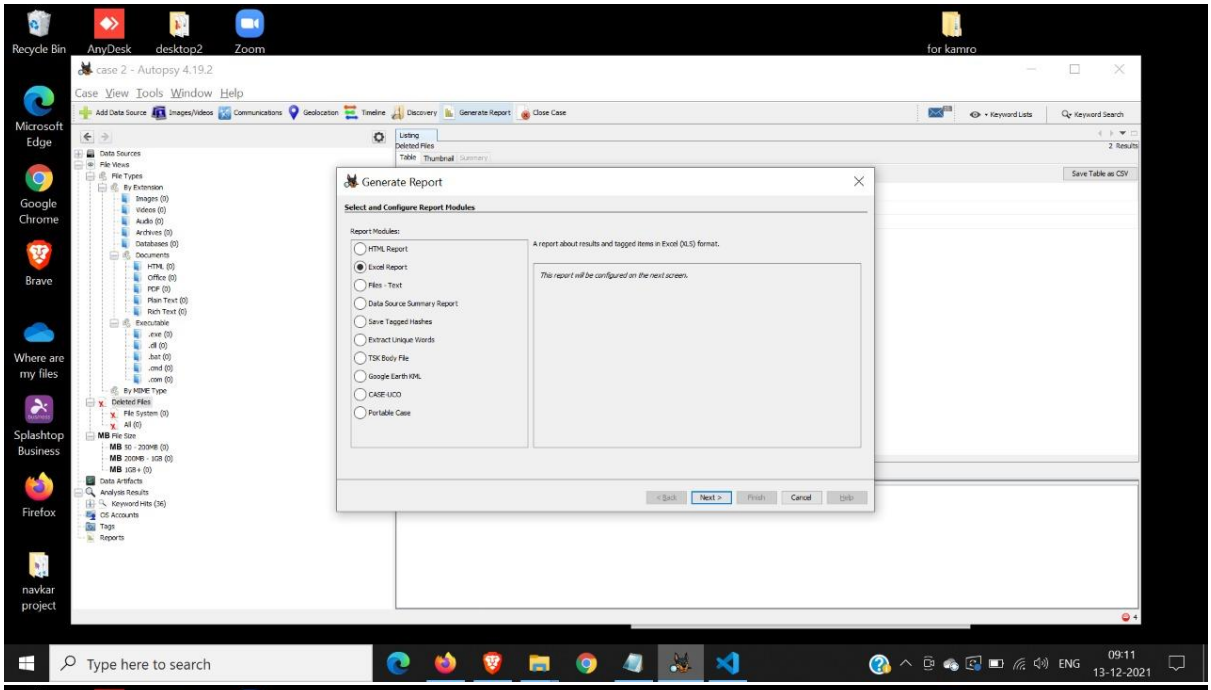


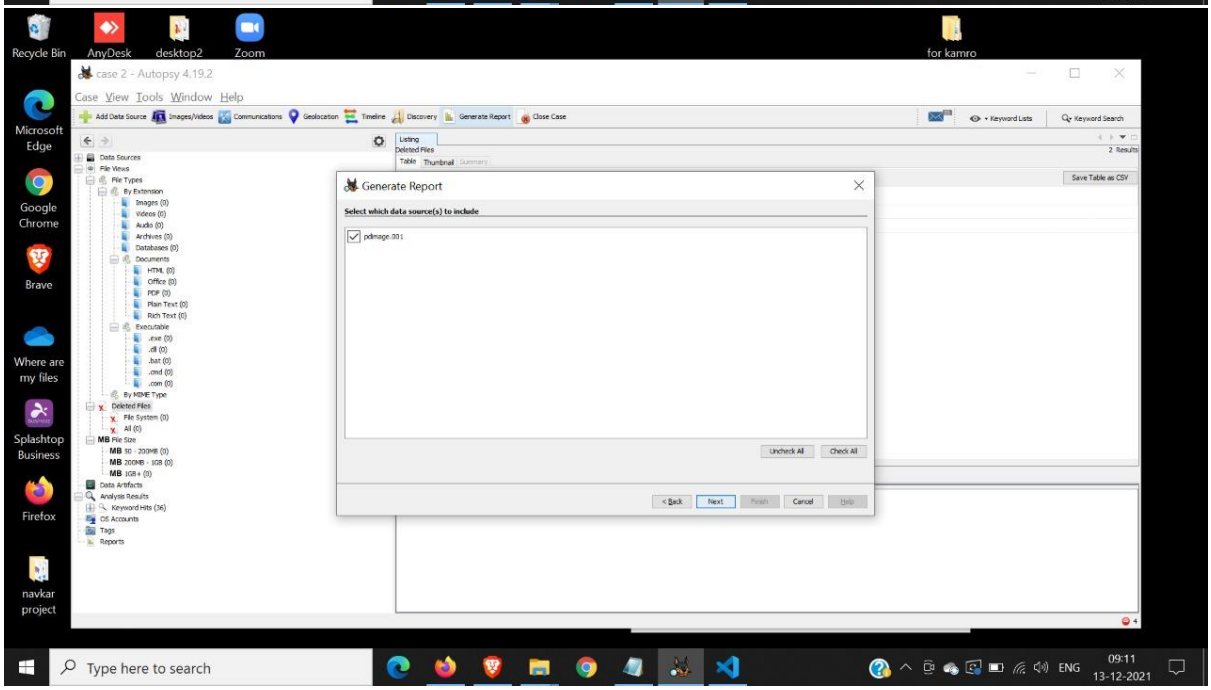
Select the export folder



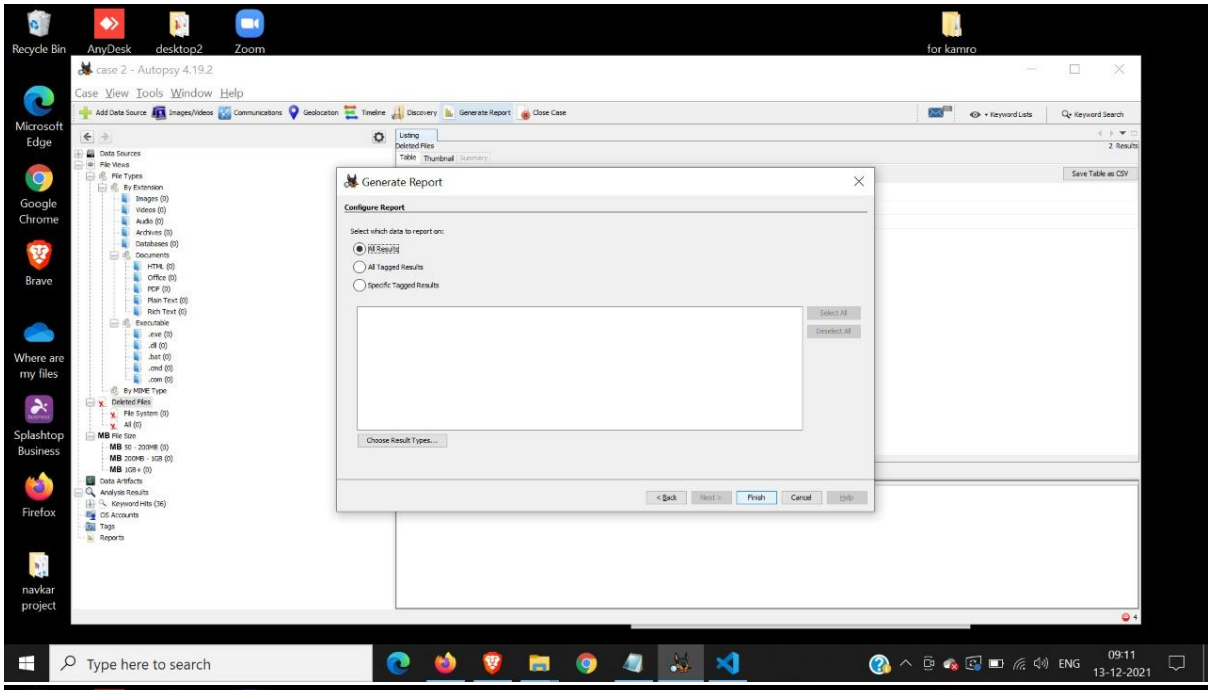


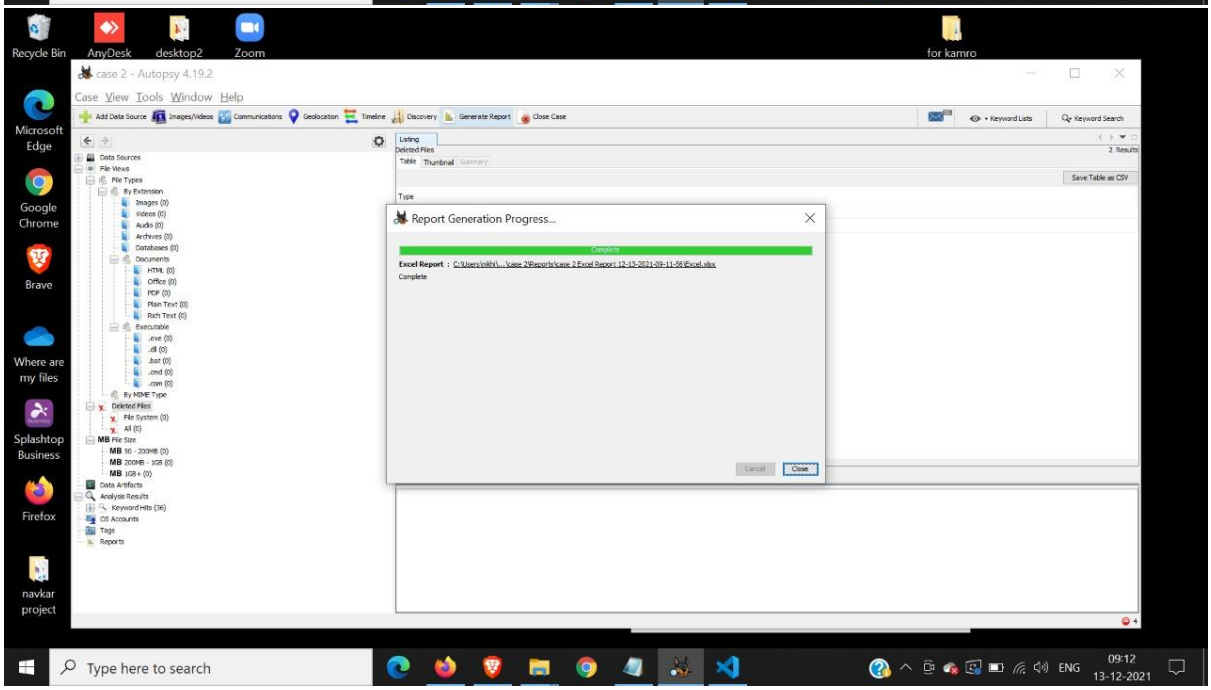
Now click on generate report and select excel report



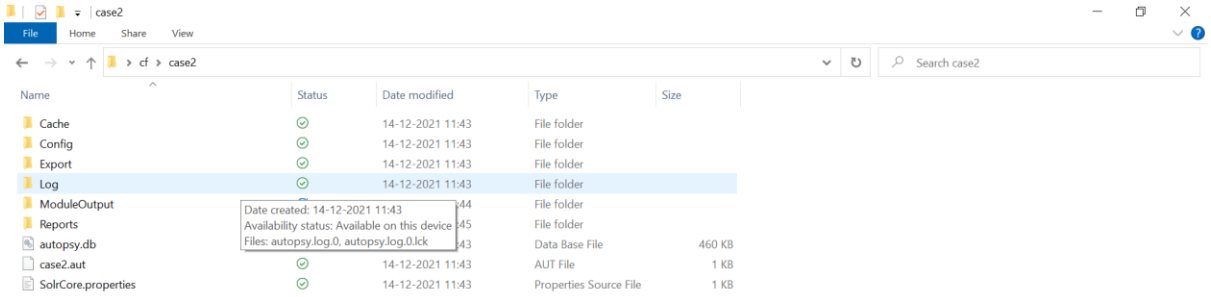


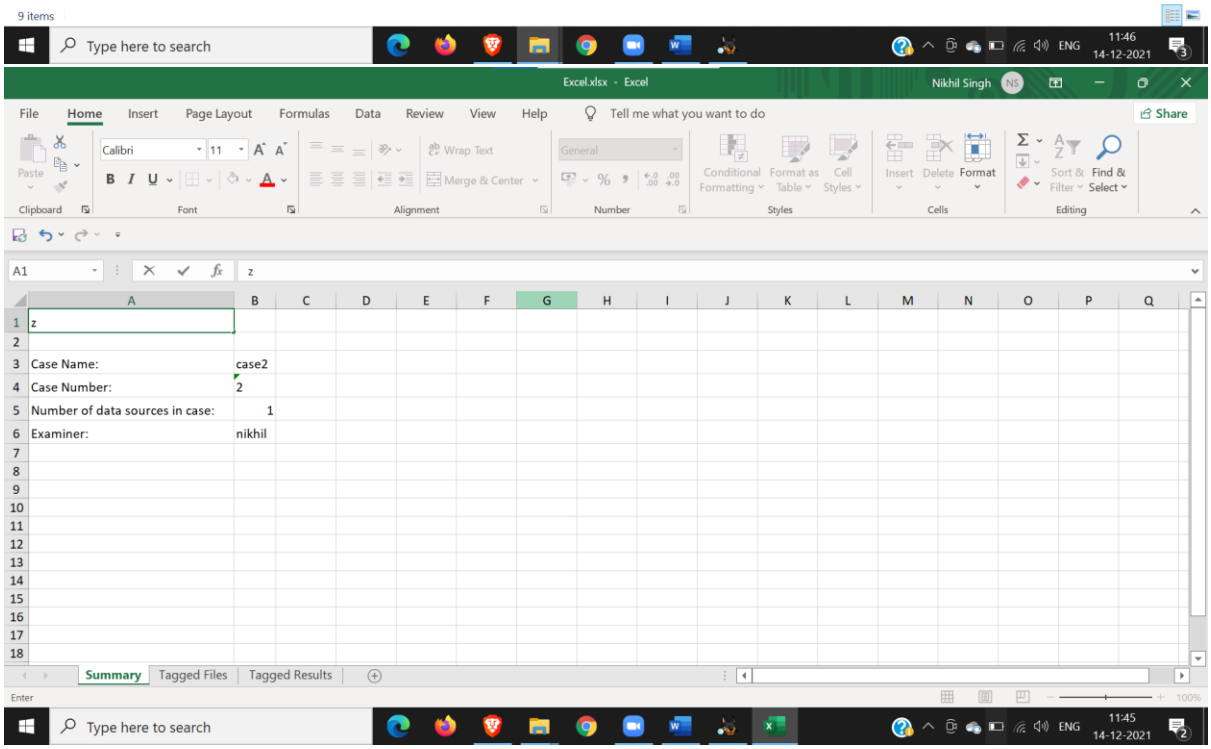
Click all results and select finish





You can view the folders in generated base directory

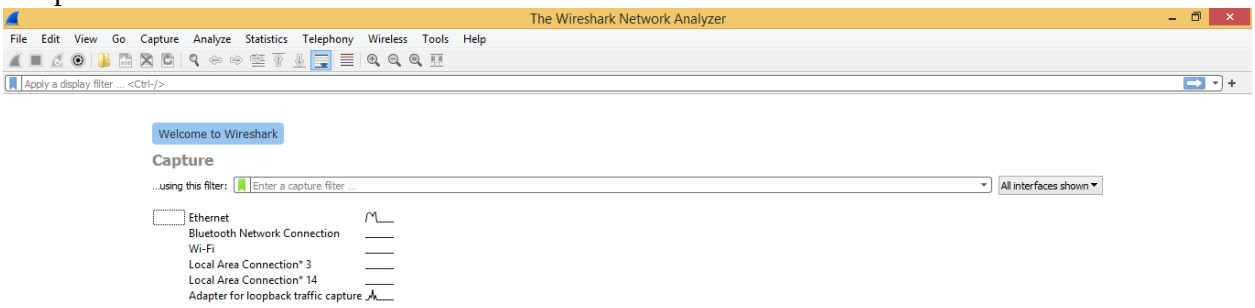


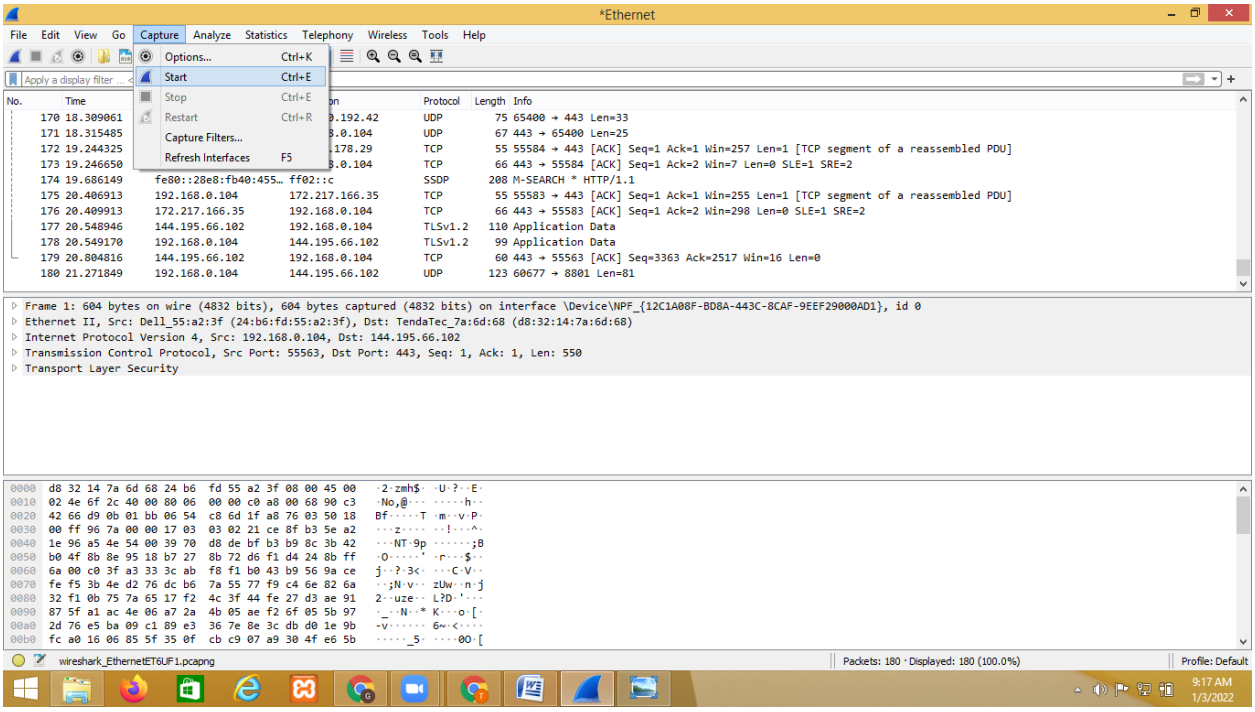


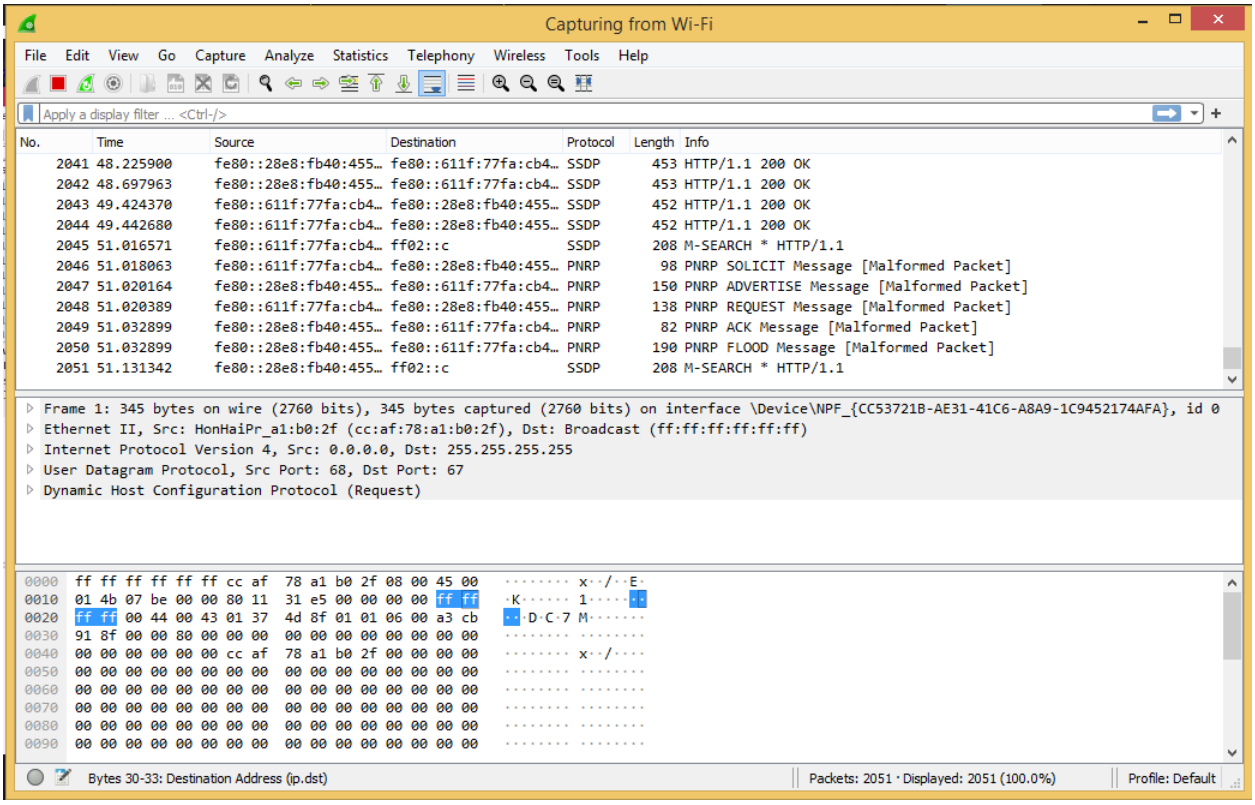
Practical:4

Aim: Capturing and analyzing network packets using Wireshark (Fundamentals):
- Identification the live network
- Capture Packets
- Analyze the captured packets

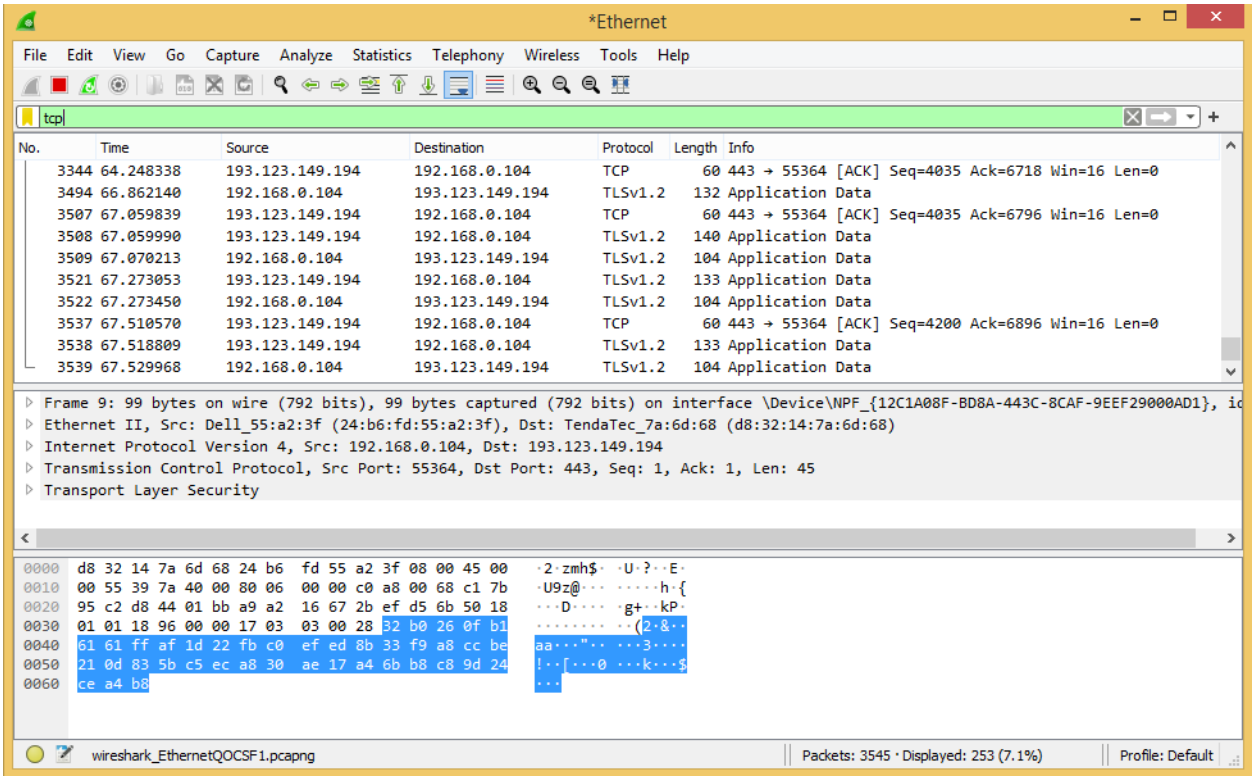
1. Open Wireshark







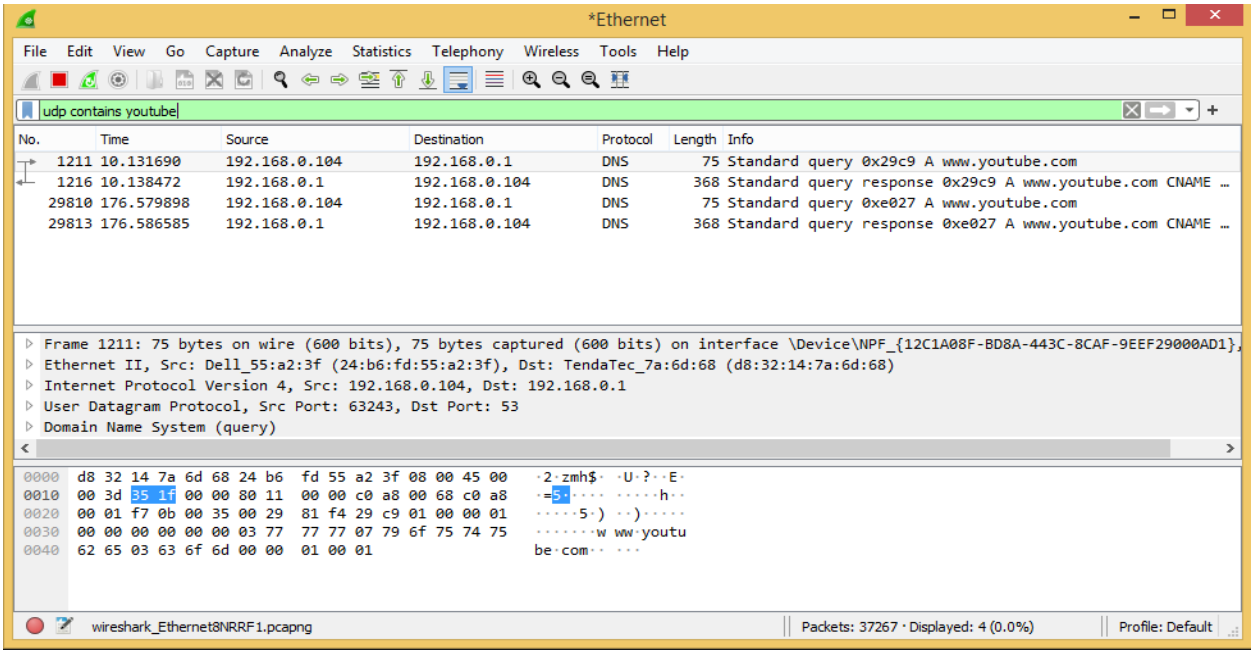
TCP package: search TCP package



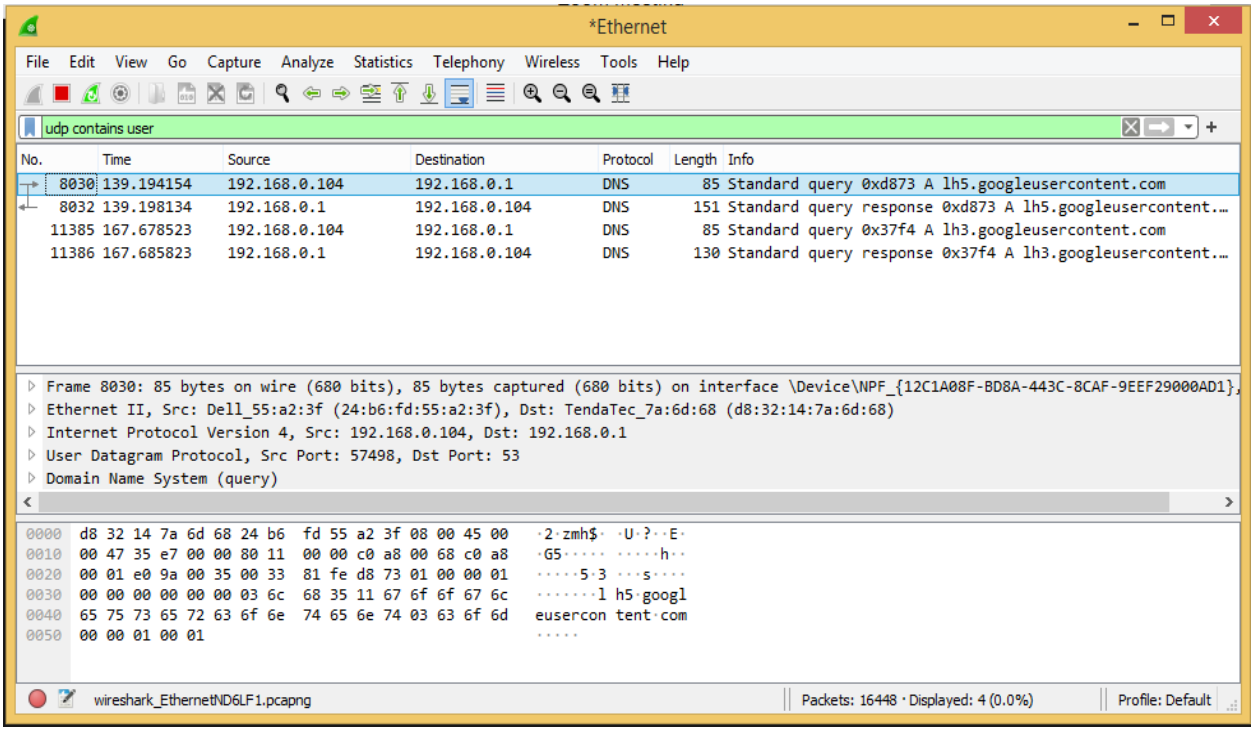
Analysis youtube data

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

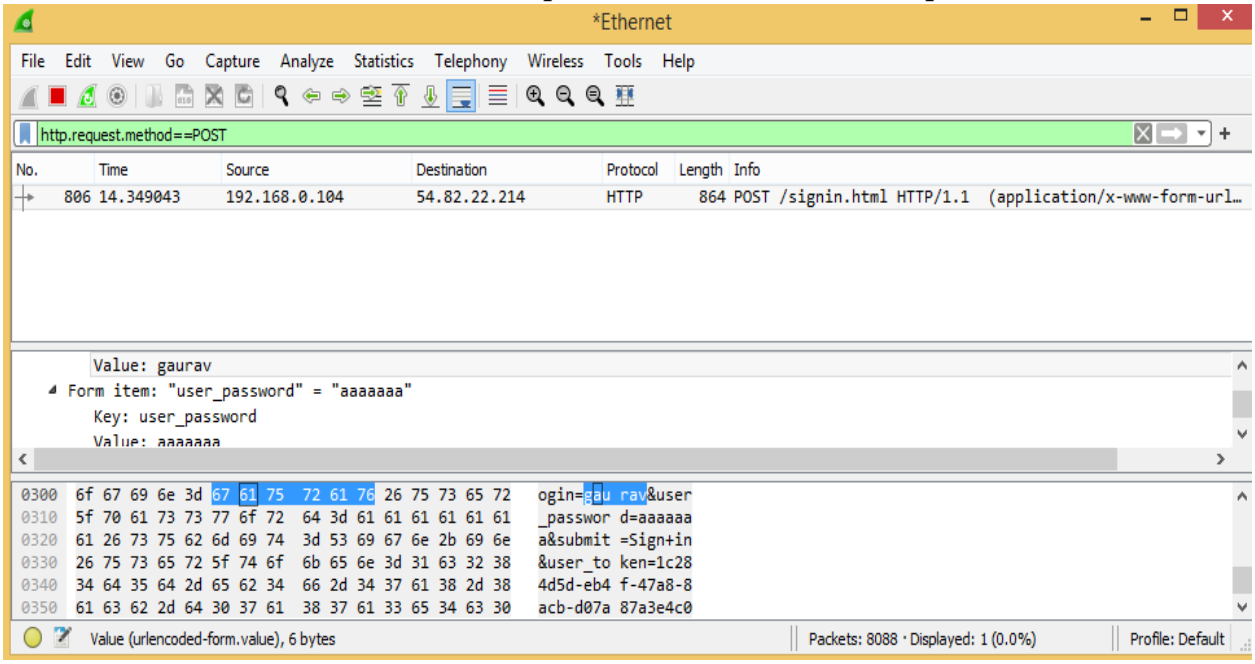
Now come back to Wireshark and enter **udp contains youtube** in the search bar.



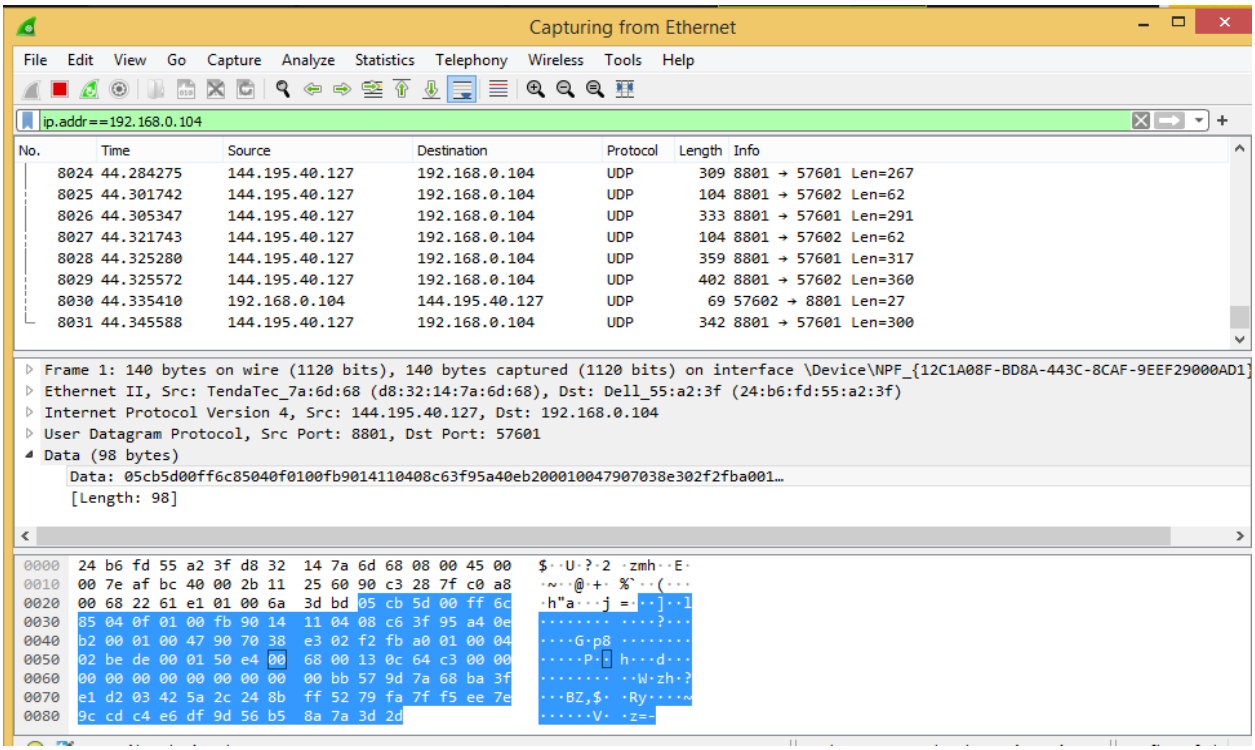
search udp contains user: Now go on browser, login in any secured website and Now come back to Wireshark and enter **udp contains user** in the search bar.



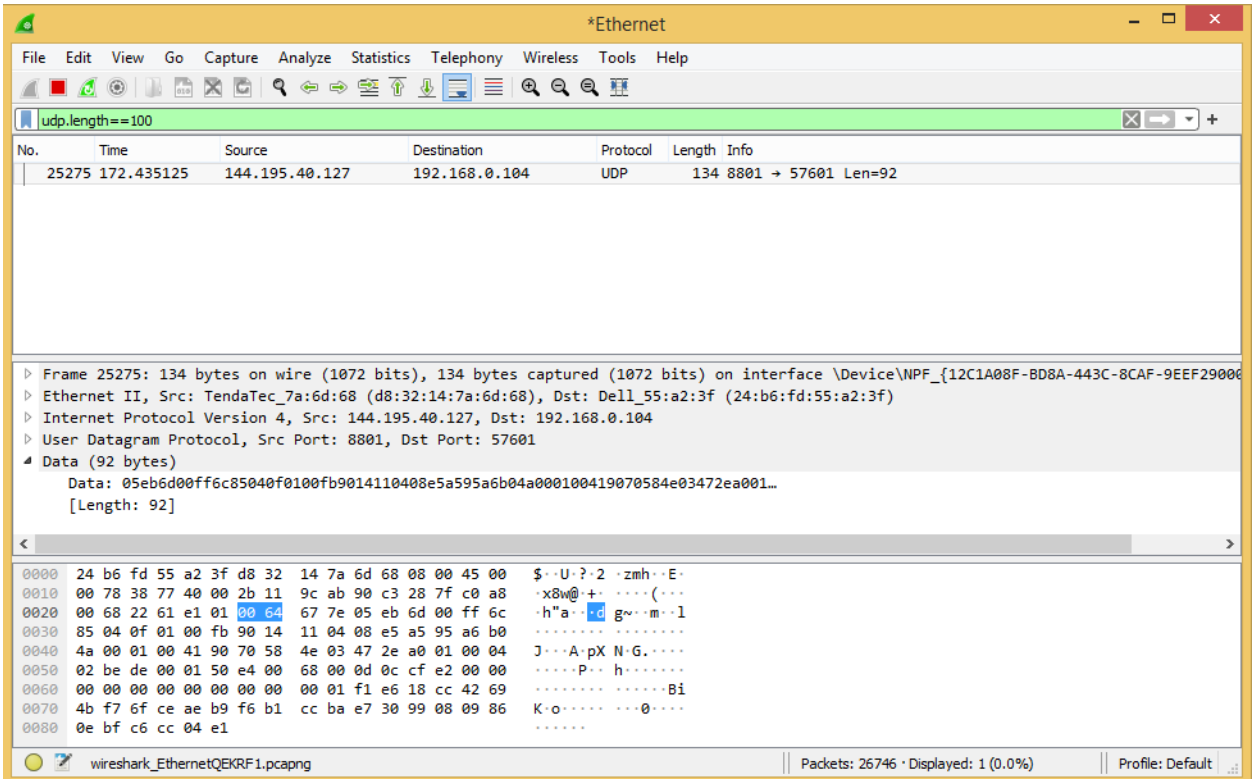
http website: go on browser, login in any unsecured website and Now come back to Wireshark and enter **http.request.method==POST** in the search bar.You can view the username and password because it is http website



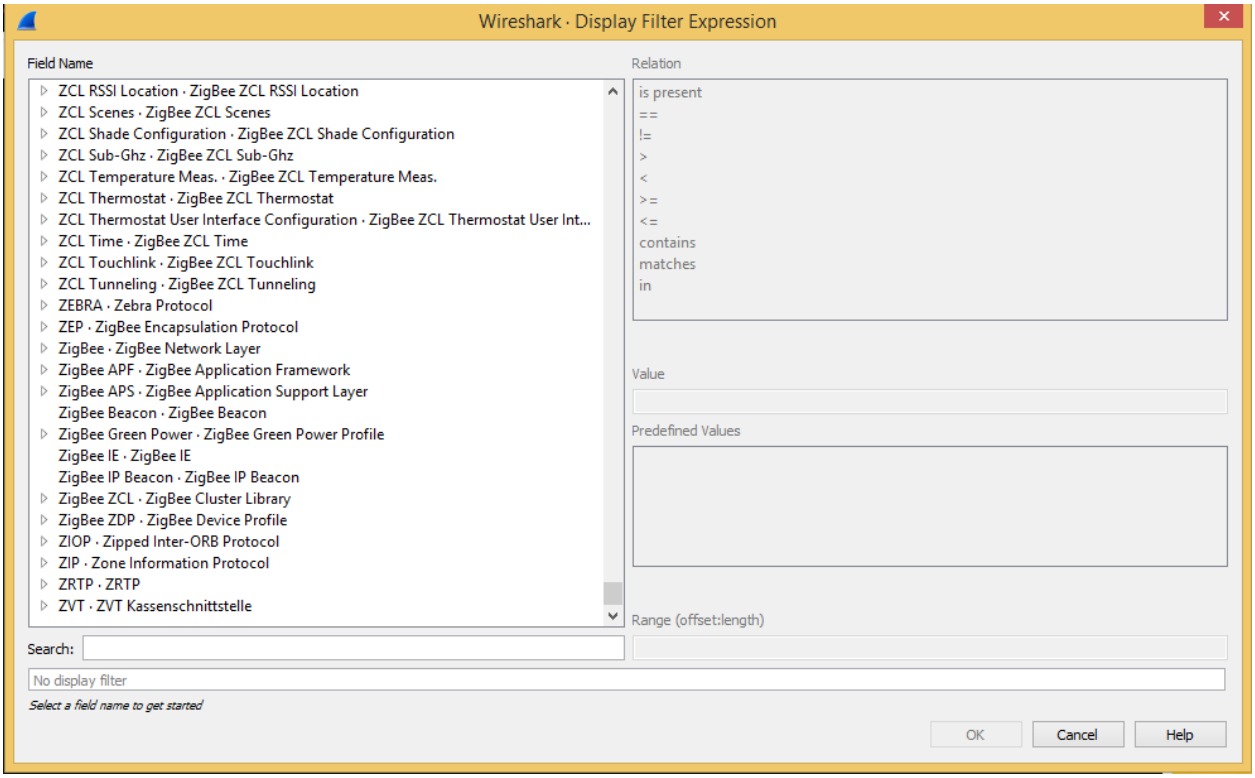
filter with ip: ip.addr==192.168.0.104



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?

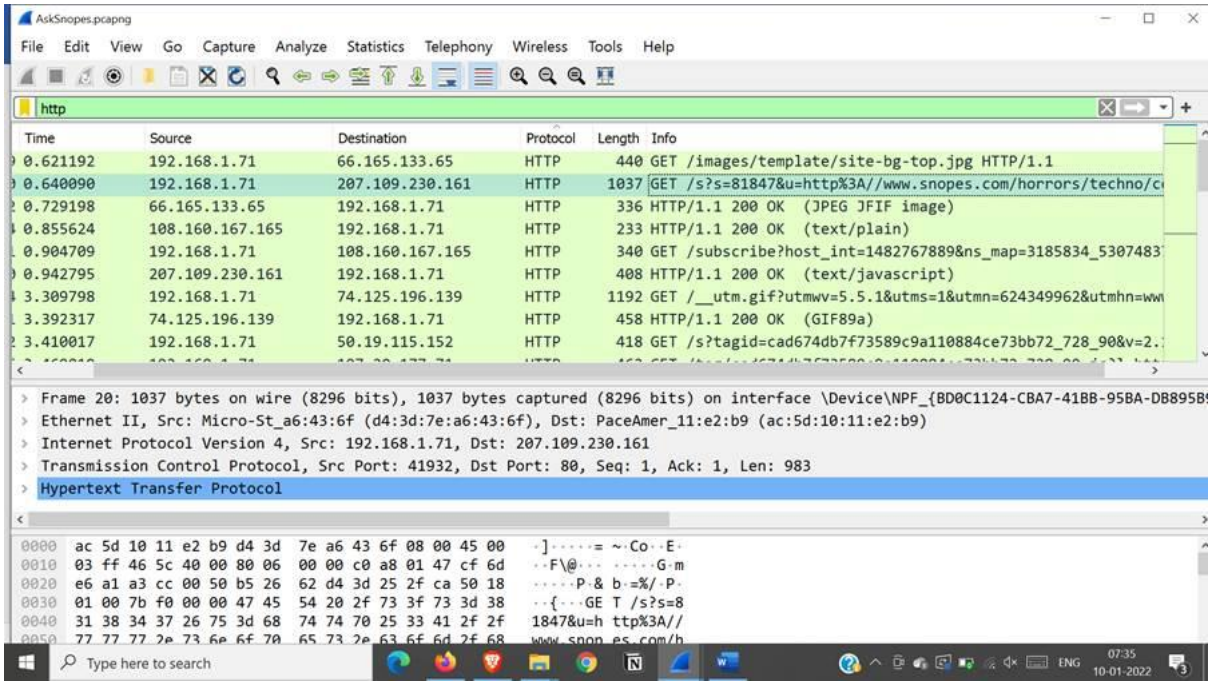
- About what cell phone problem is the client concerned?

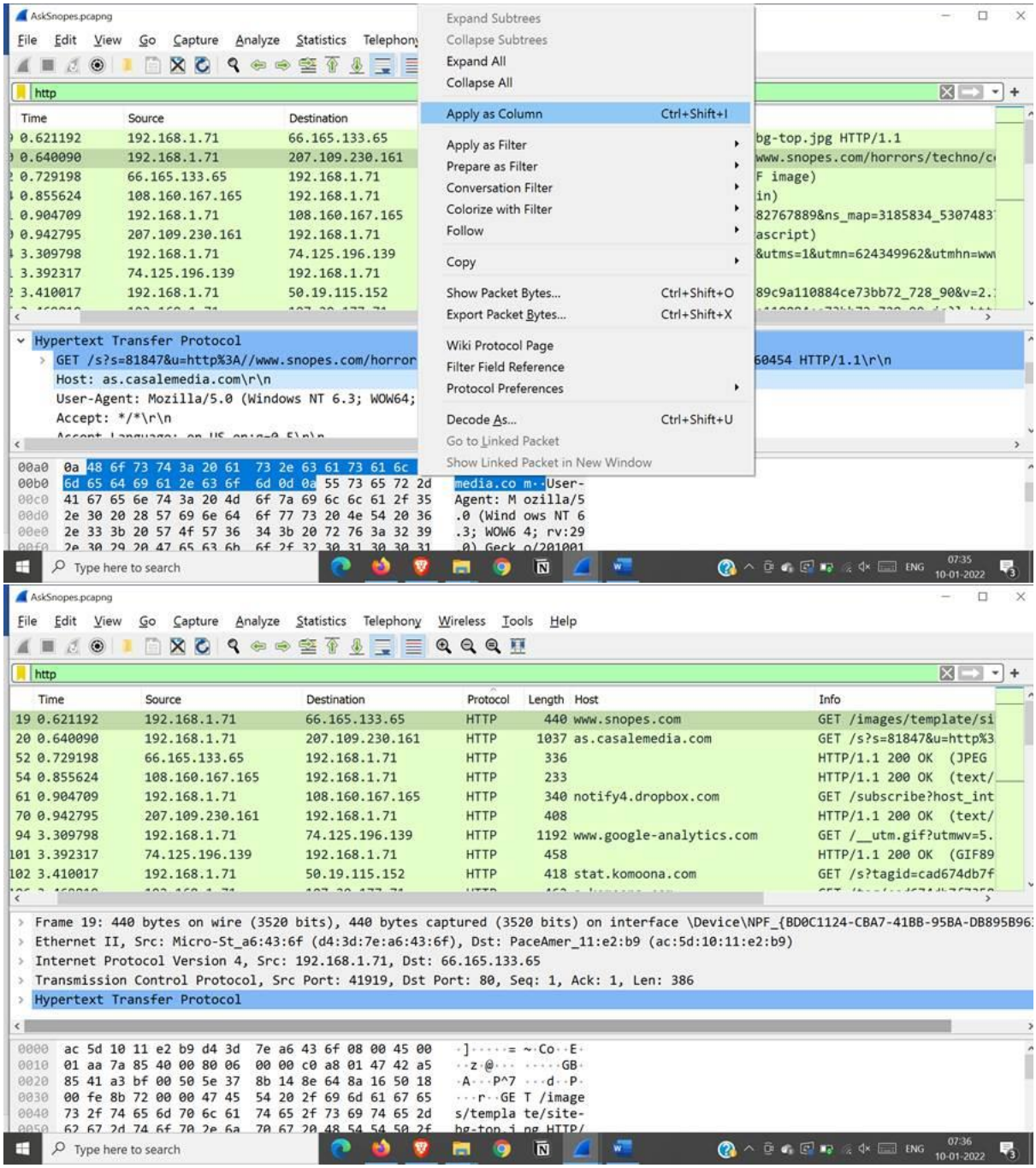
- According to Zillow, what instrument will Ryan learn to play?

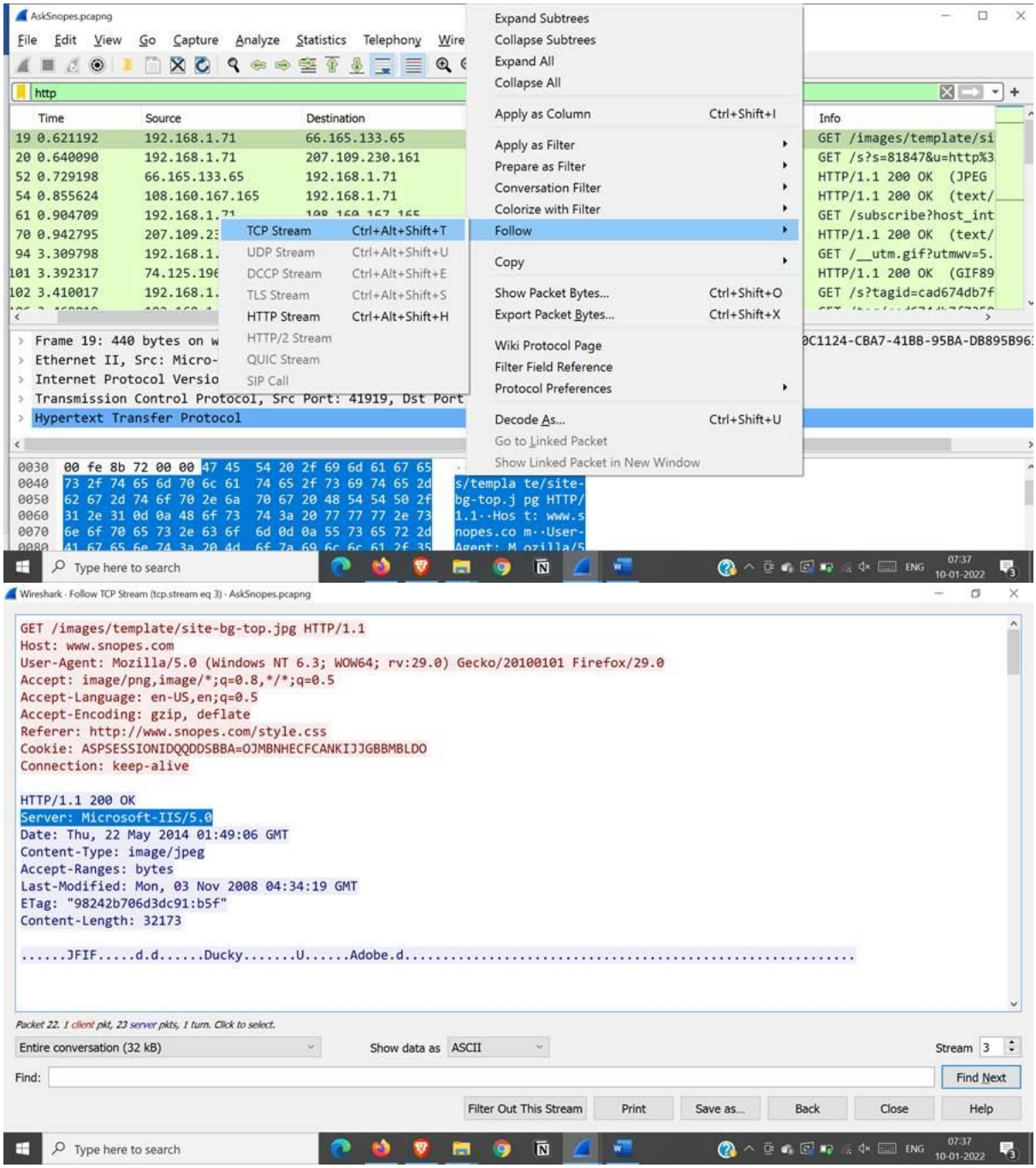
- How many web servers are running Apache?

- What hosts (IP addresses) think that jokes are more entertaining when they are explained?

What webserver is this website using?




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
3.309798 192.168.1.71 74.125.196.139
3.392317 74.125.196.139 192.168.1.71
3.410017 192.168.1.71 50.19.115.152
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
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;
Accept: */*\r\n
00a0 0a 48 6f 73 74 3a 20 61 73 2e 63 61 73 61 6c
00b0 6d 65 64 69 61 2e 63 6f 6d 0d 0a 55 73 65 72 2d
00c0 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35
00d0 2e 30 20 28 57 69 6e 64 6f 77 73 20 4e 54 20 36
00e0 2e 33 3b 20 57 4f 57 36 34 3b 20 72 76 3a 32 39
media.co m··User-
Agent: M ozilla/5
.0 (Wind ows NT 6
.3; WOW6 4; rv:29
Type here to search
ENG 07:35 10-01-2022
AskSnopes.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Time Source Destination Protocol Length Host Info
19 0.621192 192.168.1.71 66.165.133.65 HTTP 440 www.snopes.com GET /images/template/si
20 0.640090 192.168.1.71 207.109.230.161 HTTP 1037 as.casalemedia.com GET /s?s=81847&u=http%3
52 0.729198 66.165.133.65 192.168.1.71 HTTP 336 HTTP/1.1 200 OK (JPEG
54 0.855624 108.160.167.165 192.168.1.71 HTTP 233 HTTP/1.1 200 OK (text/
61 0.904709 192.168.1.71 108.160.167.165 HTTP 340 notify4.dropbox.com GET /subscribe?host_int
70 0.942795 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 /s?tagid=cad674db7f
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
0000 ac 5d 10 11 e2 b9 d4 3d 7e a6 43 6f 08 00 45 00
0010 01 aa 7a 85 40 00 80 06 00 00 c0 a8 01 47 42 a5
0020 85 41 a3 bf 00 50 5e 37 8b 14 8e 64 8a 16 50 18
0030 00 fe 8b 72 00 00 47 45 54 20 2f 69 6d 61 67 65
0040 73 2f 74 65 6d 70 6c 61 74 65 2f 73 69 74 65 2d
Type here to search
ENG 07:36 10-01-2022

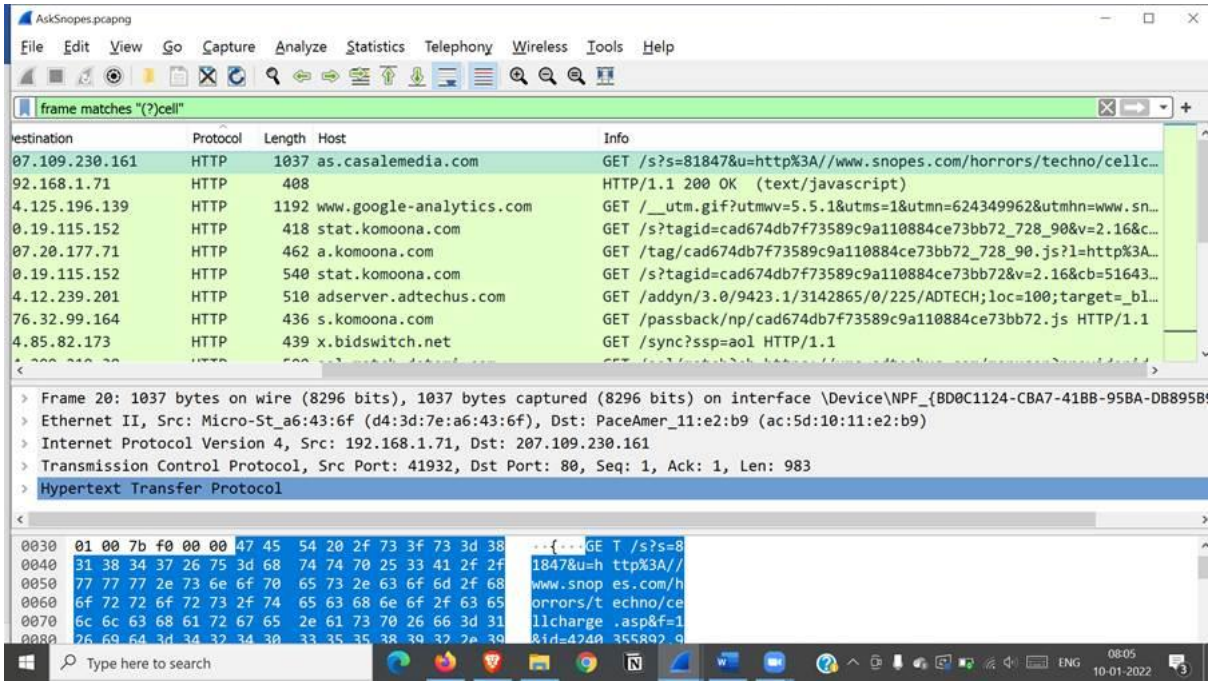


ANS-

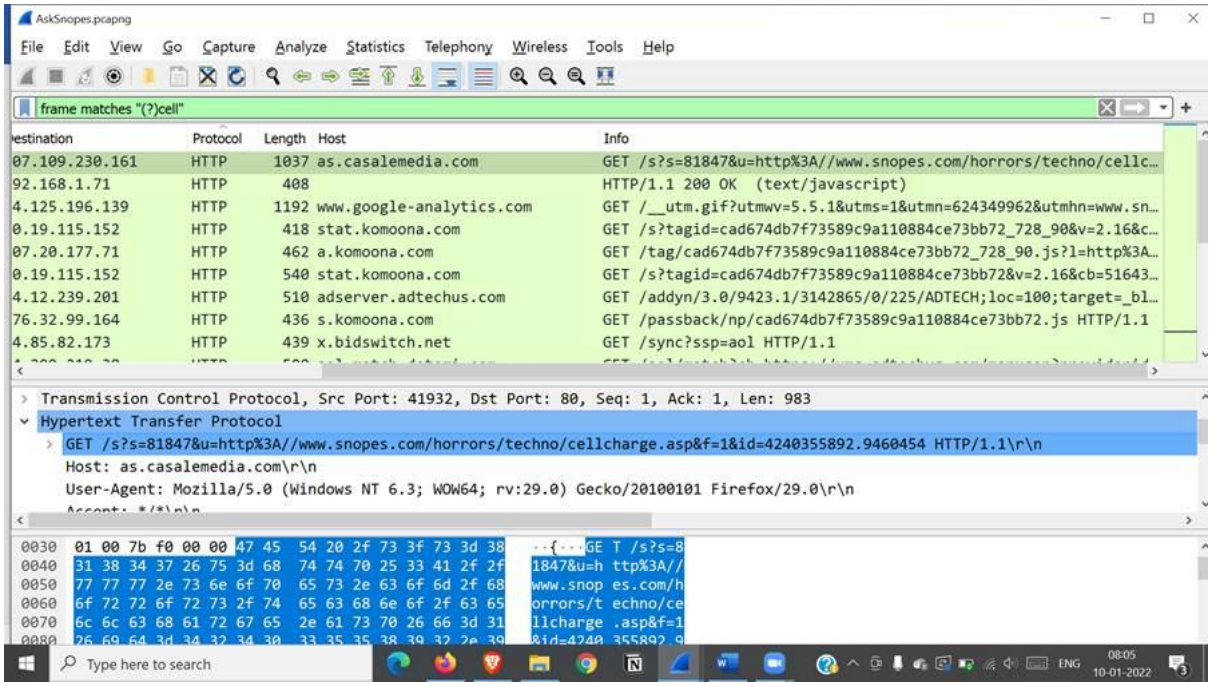
Server is Microsoft iis server

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-

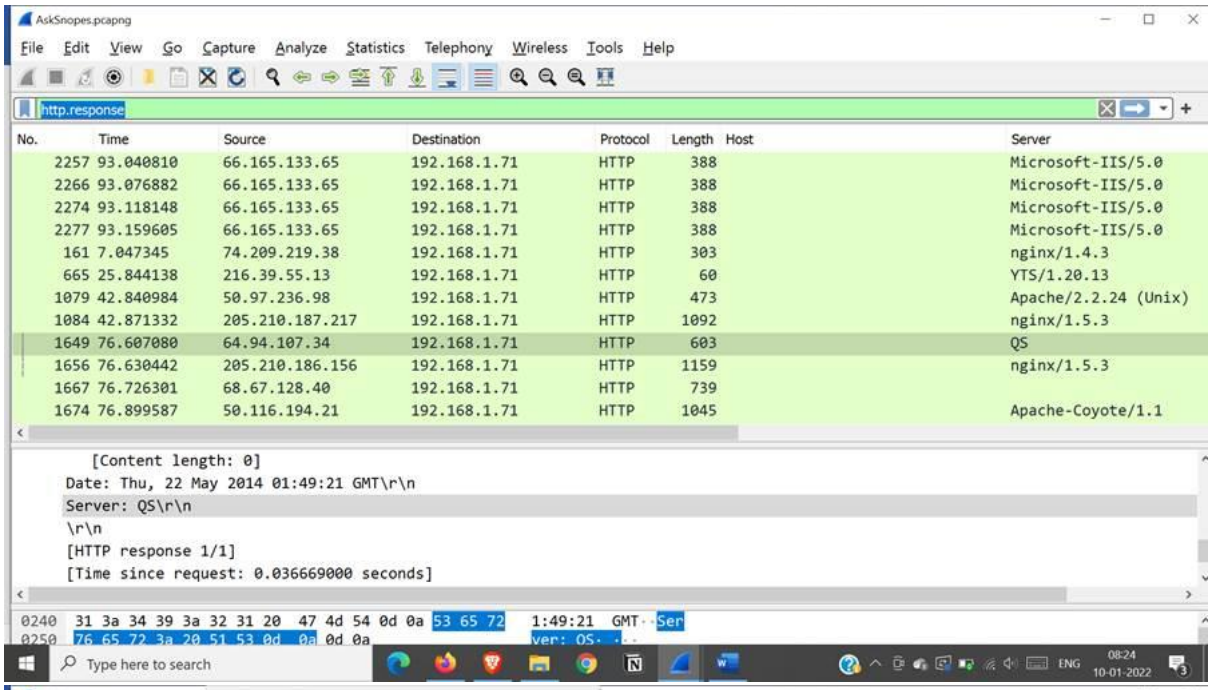
Client had searched for cell charge problem

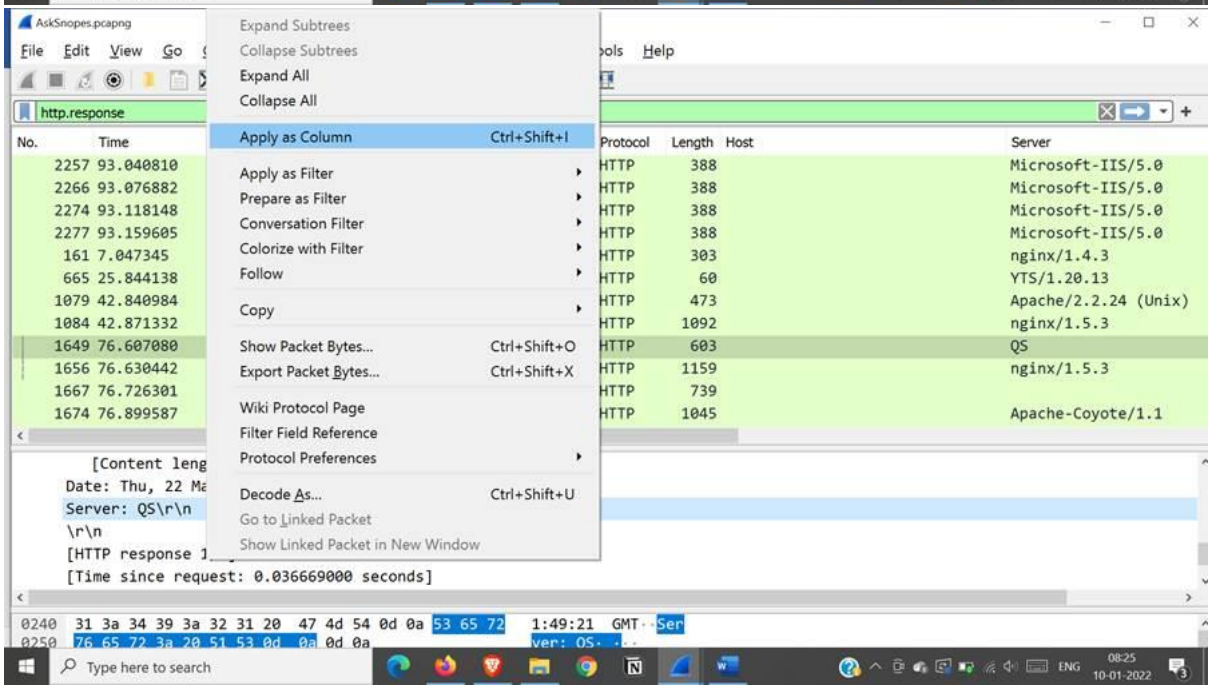
How many webservers?

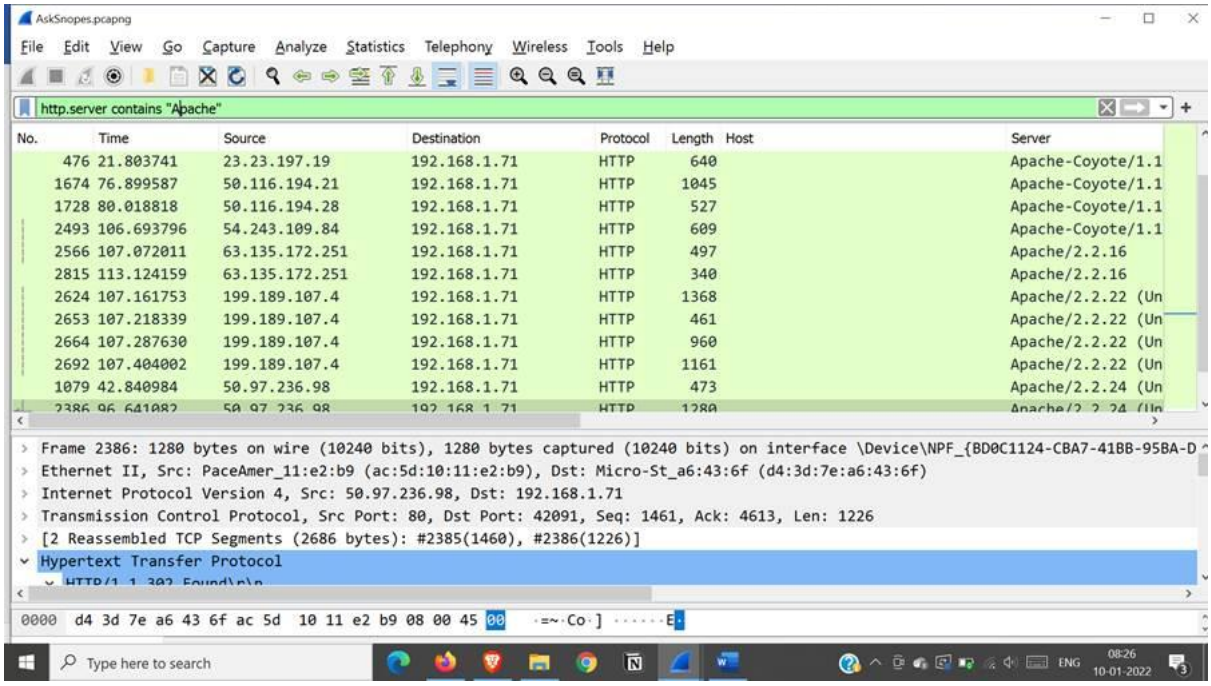
Into the filter type " http.server contains "Apache" " and search. Now click on Statistics – Endpoints.

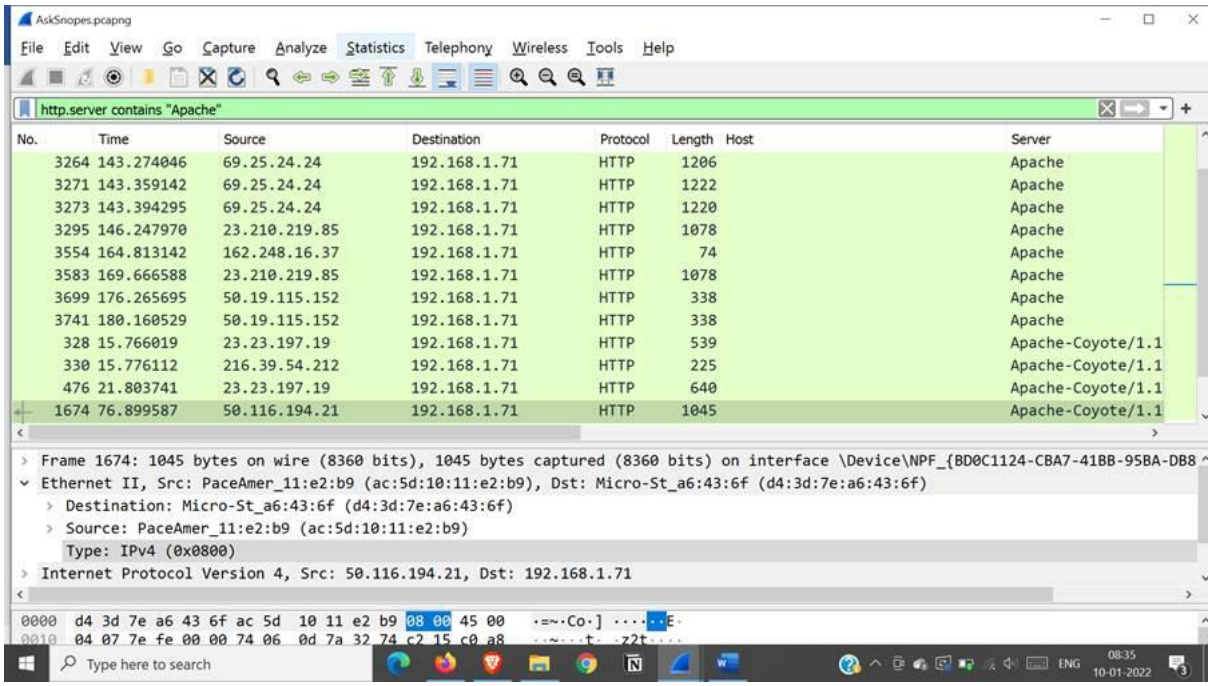
Move to Ipv4. Check the Limit to display filter at the bottom and you can see that 22 servers are

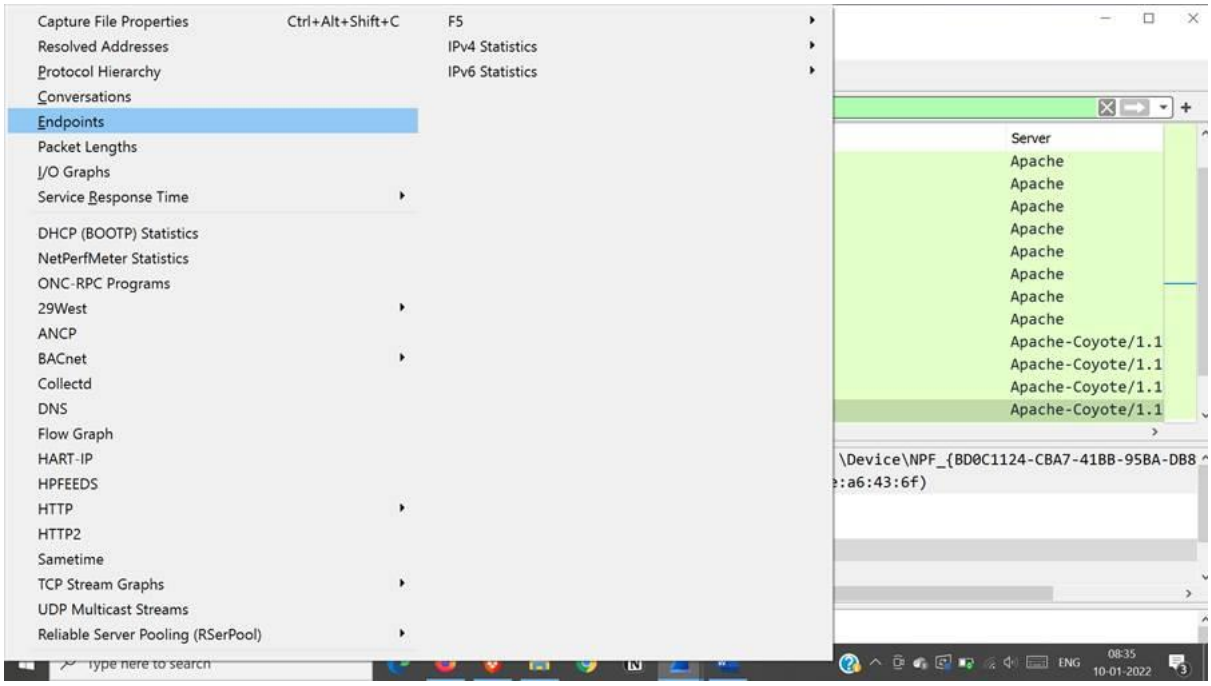
running Apach

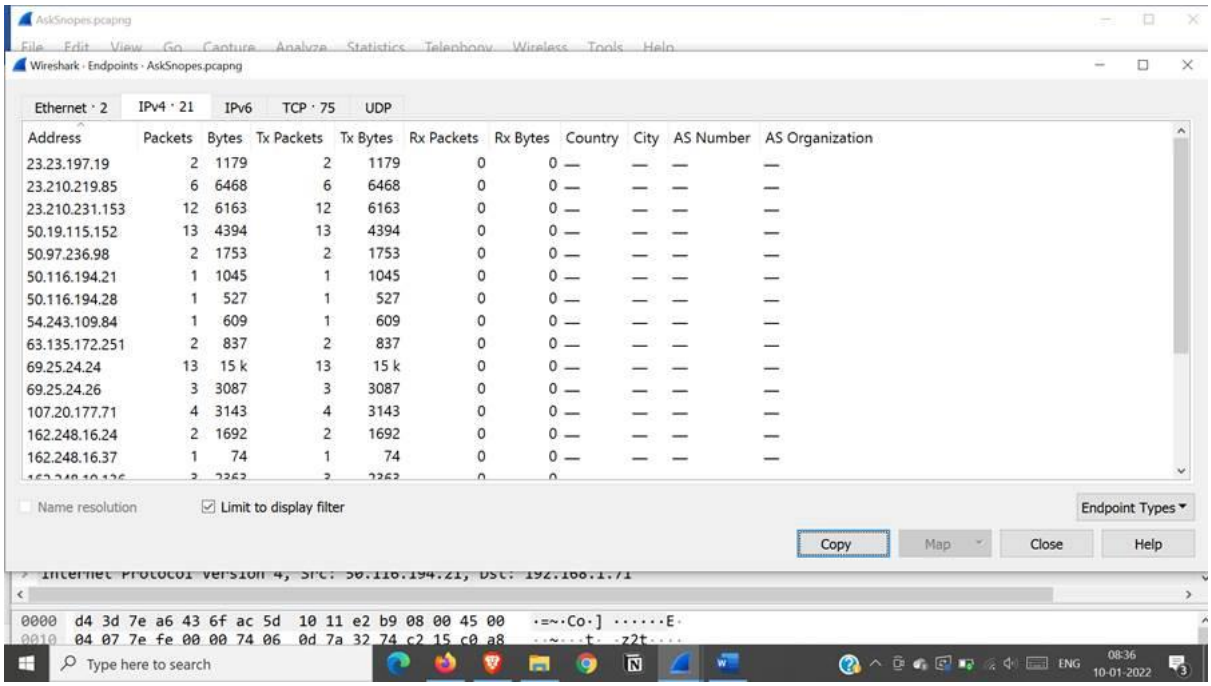





AskSnopes.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http.server contains "Apache"
No. Time Source Destination Protocol Length Host Server
476 21.803741 23.23.197.19 192.168.1.71 HTTP 640 Apache-Coyote/1.1
1674 76.899587 50.116.194.21 192.168.1.71 HTTP 1045 Apache-Coyote/1.1
1728 80.018818 50.116.194.28 192.168.1.71 HTTP 527 Apache-Coyote/1.1
2493 106.693796 54.243.109.84 192.168.1.71 HTTP 609 Apache-Coyote/1.1
2566 107.072011 63.135.172.251 192.168.1.71 HTTP 497 Apache/2.2.16
2815 113.124159 63.135.172.251 192.168.1.71 HTTP 340 Apache/2.2.16
2624 107.161753 199.189.107.4 192.168.1.71 HTTP 1368 Apache/2.2.22 (Un
2653 107.218339 199.189.107.4 192.168.1.71 HTTP 461 Apache/2.2.22 (Un
2664 107.287630 199.189.107.4 192.168.1.71 HTTP 960 Apache/2.2.22 (Un
2692 107.404002 199.189.107.4 192.168.1.71 HTTP 1161 Apache/2.2.22 (Un
1079 42.840984 50.97.236.98 192.168.1.71 HTTP 473 Apache/2.2.24 (Un
Frame 2386: 1280 bytes on wire (10240 bits), 1280 bytes captured (10240 bits) on interface \Device\NPF_{BD0C1124-CBA7-41BB-95BA-D
Ethernet II, Src: PaceAmer_11:e2:b9 (ac:5d:10:11:e2:b9), Dst: Micro-St_a6:43:6f (d4:3d:7e:a6:43:6f)
Internet Protocol Version 4, Src: 50.97.236.98, Dst: 192.168.1.71
Transmission Control Protocol, Src Port: 80, Dst Port: 42091, Seq: 1461, Ack: 4613, Len: 1226
[2 Reassembled TCP Segments (2686 bytes): #2385(1460), #2386(1226)]
Hypertext Transfer Protocol
0000 d4 3d 7e a6 43 6f ac 5d 10 11 e2 b9 08 00 45 00
Type here to search
ENG 08:26 10-01-2022


AskSnopes.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http.server contains "Apache"
No. Time Source Destination Protocol Length Host Server
3264 143.274046 69.25.24.24 192.168.1.71 HTTP 1206 Apache
3271 143.359142 69.25.24.24 192.168.1.71 HTTP 1222 Apache
3273 143.394295 69.25.24.24 192.168.1.71 HTTP 1220 Apache
3295 146.247970 23.210.219.85 192.168.1.71 HTTP 1078 Apache
3554 164.813142 162.248.16.37 192.168.1.71 HTTP 74 Apache
3583 169.666588 23.210.219.85 192.168.1.71 HTTP 1078 Apache
3699 176.265695 50.19.115.152 192.168.1.71 HTTP 338 Apache
3741 180.160529 50.19.115.152 192.168.1.71 HTTP 338 Apache
328 15.766019 23.23.197.19 192.168.1.71 HTTP 539 Apache-Coyote/1.1
330 15.776112 216.39.54.212 192.168.1.71 HTTP 225 Apache-Coyote/1.1
476 21.803741 23.23.197.19 192.168.1.71 HTTP 640 Apache-Coyote/1.1
1674 76.899587 50.116.194.21 192.168.1.71 HTTP 1045 Apache-Coyote/1.1
Frame 1674: 1045 bytes on wire (8360 bits), 1045 bytes captured (8360 bits) on interface \Device\NPF_{BD0C1124-CBA7-41BB-95BA-DB8
Ethernet II, Src: PaceAmer_11:e2:b9 (ac:5d:10:11:e2:b9), Dst: Micro-St_a6:43:6f (d4:3d:7e:a6:43:6f)
Destination: Micro-St_a6:43:6f (d4:3d:7e:a6:43:6f)
Source: PaceAmer_11:e2:b9 (ac:5d:10:11:e2:b9)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 50.116.194.21, Dst: 192.168.1.71
0000 d4 3d 7e a6 43 6f ac 5d 10 11 e2 b9 08 00 45 00
Type here to search
ENG 08:35 10-01-2022

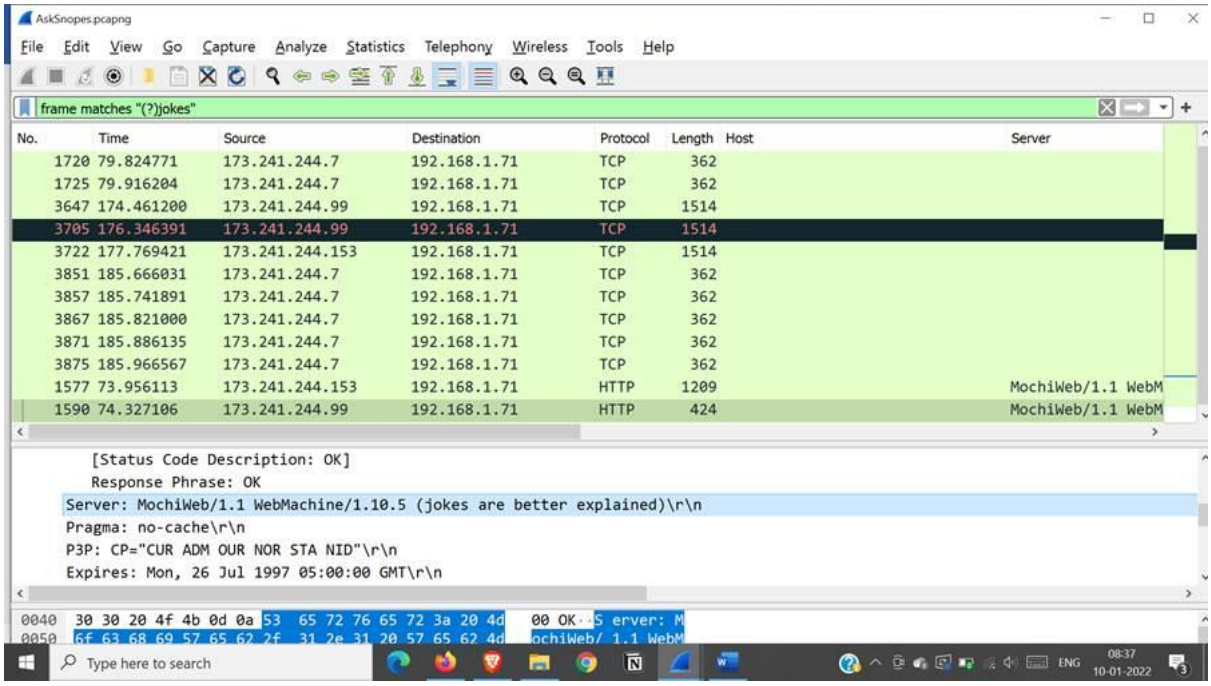

Capture File Properties Ctrl+Alt+Shift+C
Resolved Addresses
Protocol Hierarchy
Conversations
Endpoints
Packet Lengths
I/O Graphs
Service Response Time
DHCP (BOOTP) Statistics
NetPerfMeter Statistics
ONC-RPC Programs
29West
ANCP
BACnet
Collectd
DNS
Flow Graph
HART-IP
HPFEEDS
HTTP
HTTP2
Sametime
TCP Stream Graphs
UDP Multicast Streams
Reliable Server Pooling (RSerPool)
F5
IPv4 Statistics
IPv6 Statistics
Server
Apache
Apache-Coyote/1.1
\Device\NPF_{BD0C1124-CBA7-41BB-95BA-DB8
:a6:43:6f)
Type here to search
ENG
08:35
10-01-2022


AskSnopes.pcapng
Wireshark · Endpoints · AskSnopes.pcapng
Ethernet · 2
IPv4 · 21
IPv6
TCP · 75
UDP
Address Packets Bytes Tx Packets Tx Bytes Rx Packets Rx Bytes Country City AS Number AS Organization
23.23.197.19 2 1179 2 1179 0 0
23.210.219.85 6 6468 6 6468 0 0
23.210.231.153 12 6163 12 6163 0 0
50.19.115.152 13 4394 13 4394 0 0
50.97.236.98 2 1753 2 1753 0 0
50.116.194.21 1 1045 1 1045 0 0
50.116.194.28 1 527 1 527 0 0
54.243.109.84 1 609 1 609 0 0
63.135.172.251 2 837 2 837 0 0
69.25.24.24 13 15 k 13 15 k 0 0
69.25.24.26 3 3087 3 3087 0 0
107.20.177.71 4 3143 4 3143 0 0
162.248.16.24 2 1692 2 1692 0 0
162.248.16.37 1 74 1 74 0 0
Name resolution
Limit to display filter
Endpoint Types
Copy
Map
Close
Help
0000 d4 3d 7e a6 43 6f ac 5d 10 11 e2 b9 08 00 45 00
Type here to search
ENG
08:36
10-01-2022

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



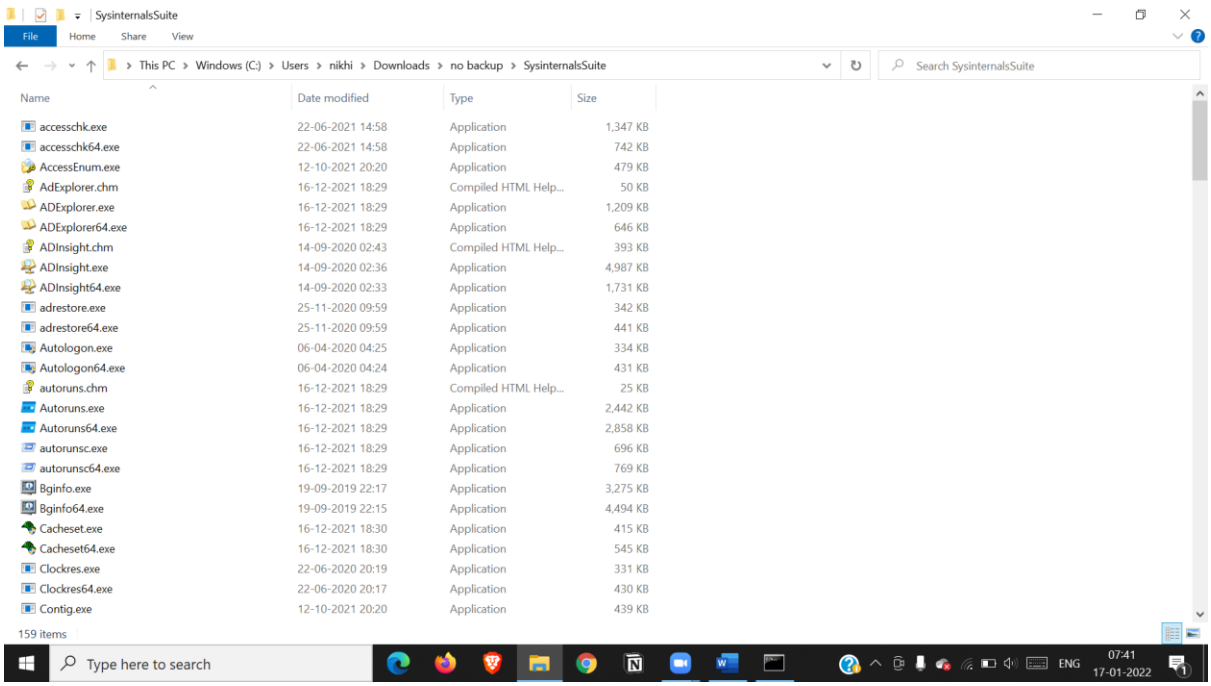
Practical:6

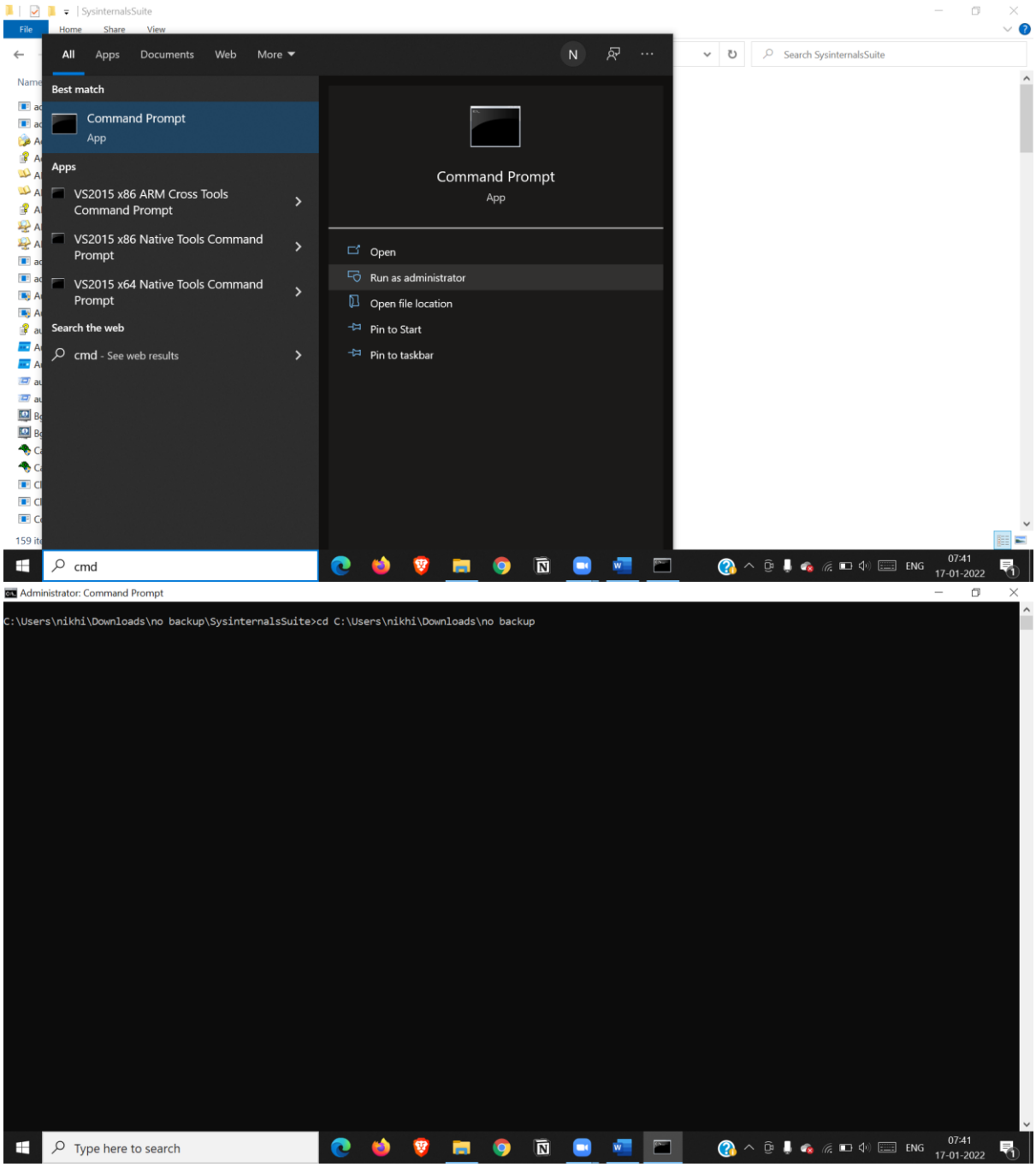
Aim: Using Sysinternals tools for Network Tracking and Process Monitoring:
-Check Sysinternals tools
-Monitor Live Processes
-Capture RAM-Capture
-TCP/UDP packets
-Monitor Hard Disk
-Monitor Virtual Memory
-Monitor Cache Memory

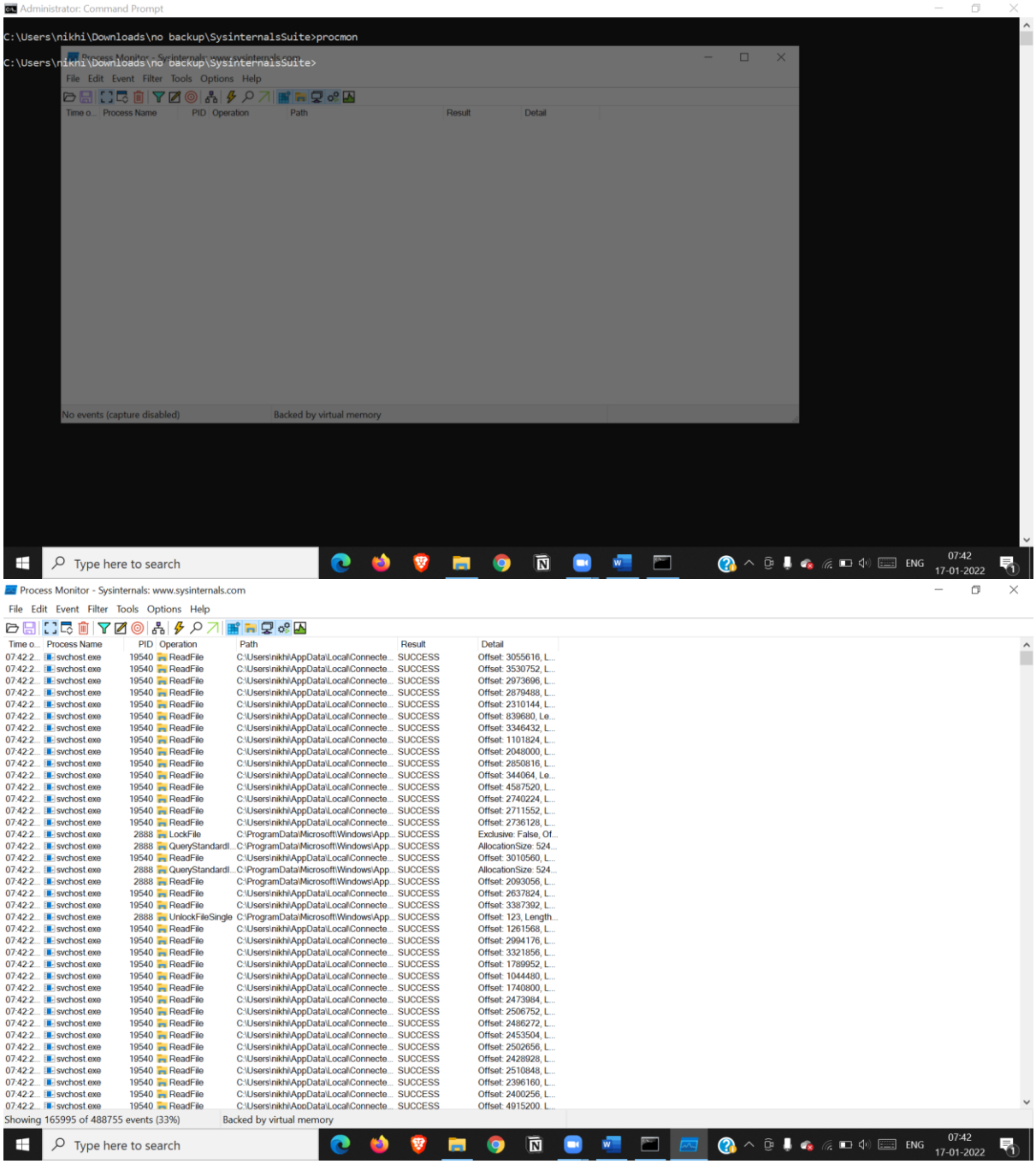
Sysinternal tools

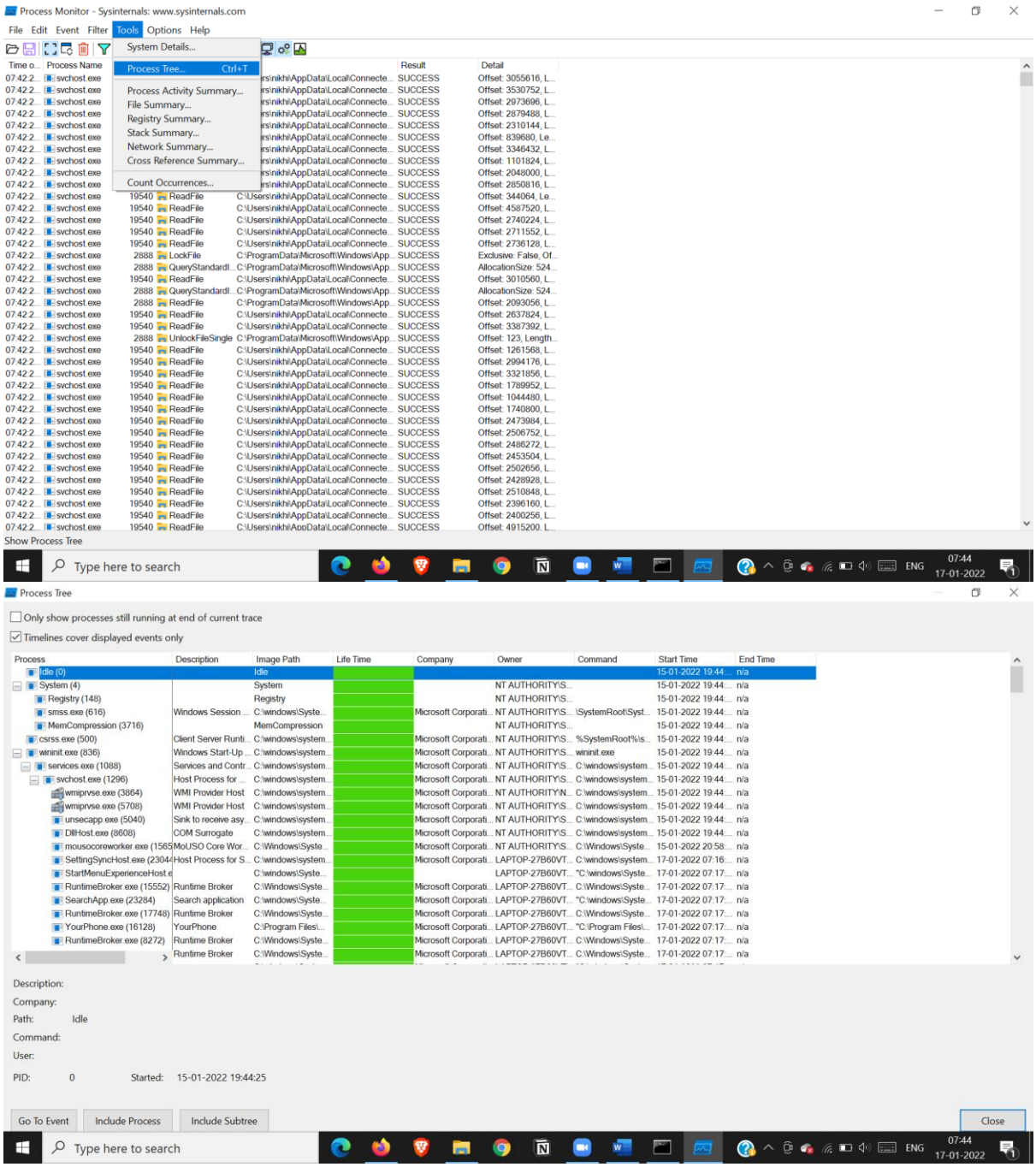
The SysInternals suite of tools is **simply a set of Windows applications that can be downloaded for free from their section of the Microsoft** Technet web site. They are all portable, which means that not only do you not have to install them, you can stick them on a flash drive and use them from any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

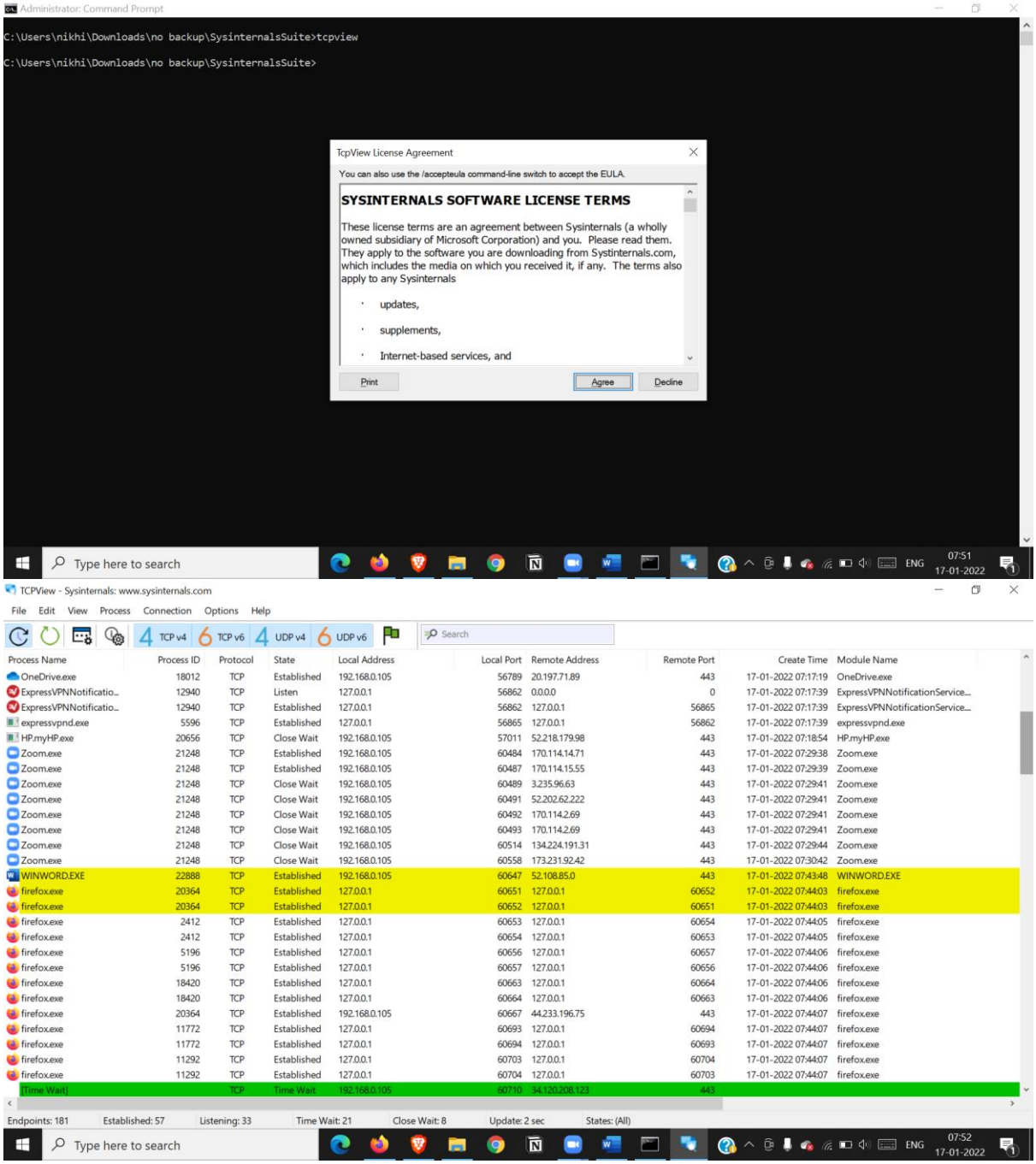



SysinternalsSuite
File
Home
Share
View
Search SysinternalsSuite
All
Apps
Documents
Web
More
Best match
Command Prompt
App
Apps
VS2015 x86 ARM Cross Tools Command Prompt
VS2015 x86 Native Tools Command Prompt
VS2015 x64 Native Tools Command Prompt
Search the web
cmd - See web results
Command Prompt
App
Open
Run as administrator
Open file location
Pin to Start
Pin to taskbar
cmd
ENG
07:41
17-01-2022
Administrator: Command Prompt
C:\Users\nikhi\Downloads\no backup\SysinternalsSuite>cd C:\Users\nikhi\Downloads\no backup
Type here to search
ENG
07:41
17-01-2022

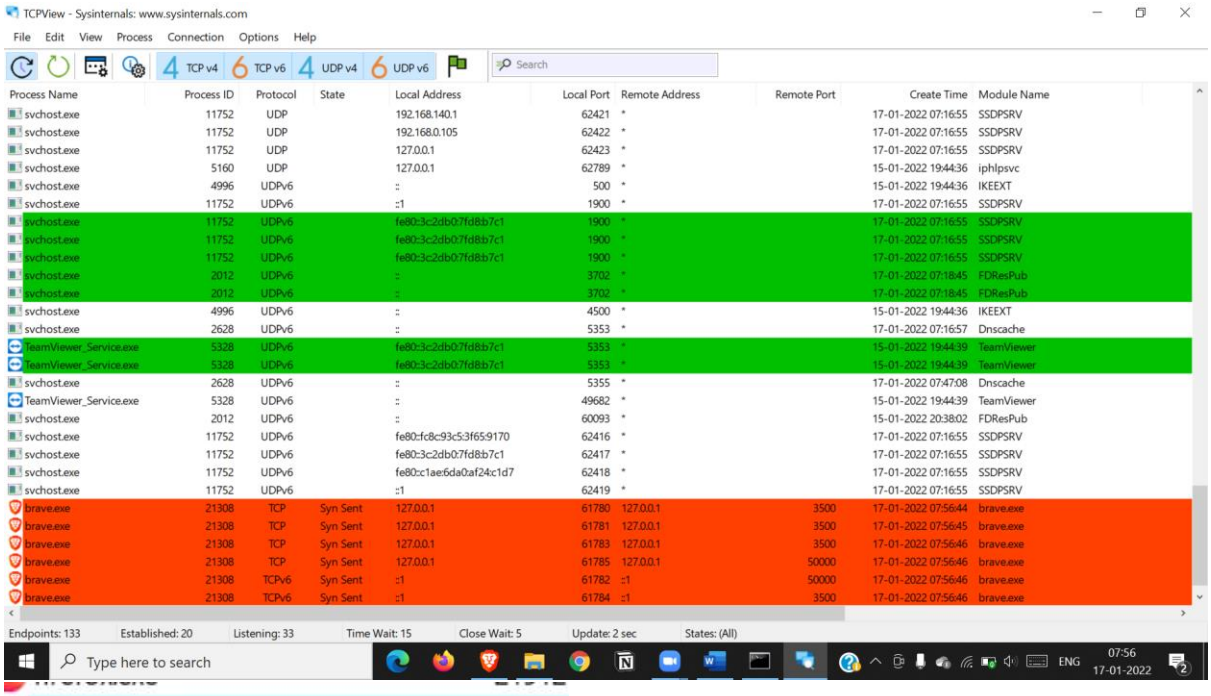

Administrator: Command Prompt
C:\Users\nikhi\Downloads\no backup\SysinternalsSuite>procmon
C:\Users\nikhi\Downloads\no backup\SysinternalsSuite>
Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Time o... Process Name PID Operation Path Result Detail
No events (capture disabled)
Backed by virtual memory
Type here to search
ENG
07:42
17-01-2022
Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Time o... Process Name PID Operation Path Result Detail
Showing 165995 of 488755 events (33%)
Backed by virtual memory
Type here to search
ENG
07:42
17-01-2022

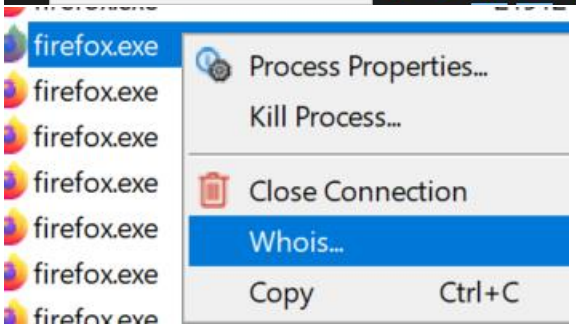


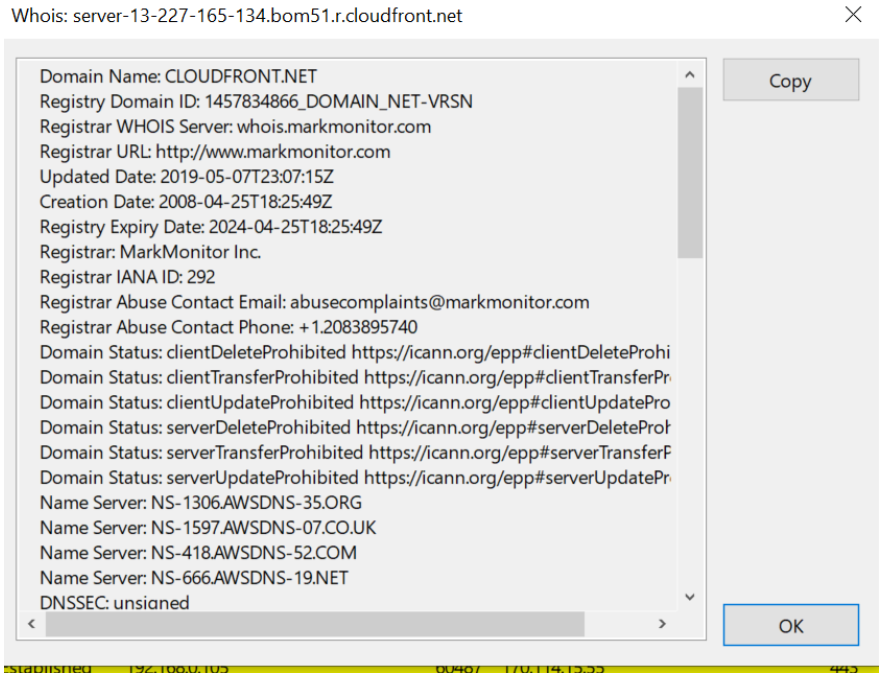
Tcp -udp packets


Administrator: Command Prompt
C:\Users\nikhi\Downloads\no backup\SysinternalsSuite>tcpview
C:\Users\nikhi\Downloads\no backup\SysinternalsSuite>
TcpView License Agreement
You can also use the /accepteula command-line switch to accept the EULA.
SYSINTERNALS 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 Systinternals.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
ENG
07:51
17-01-2022

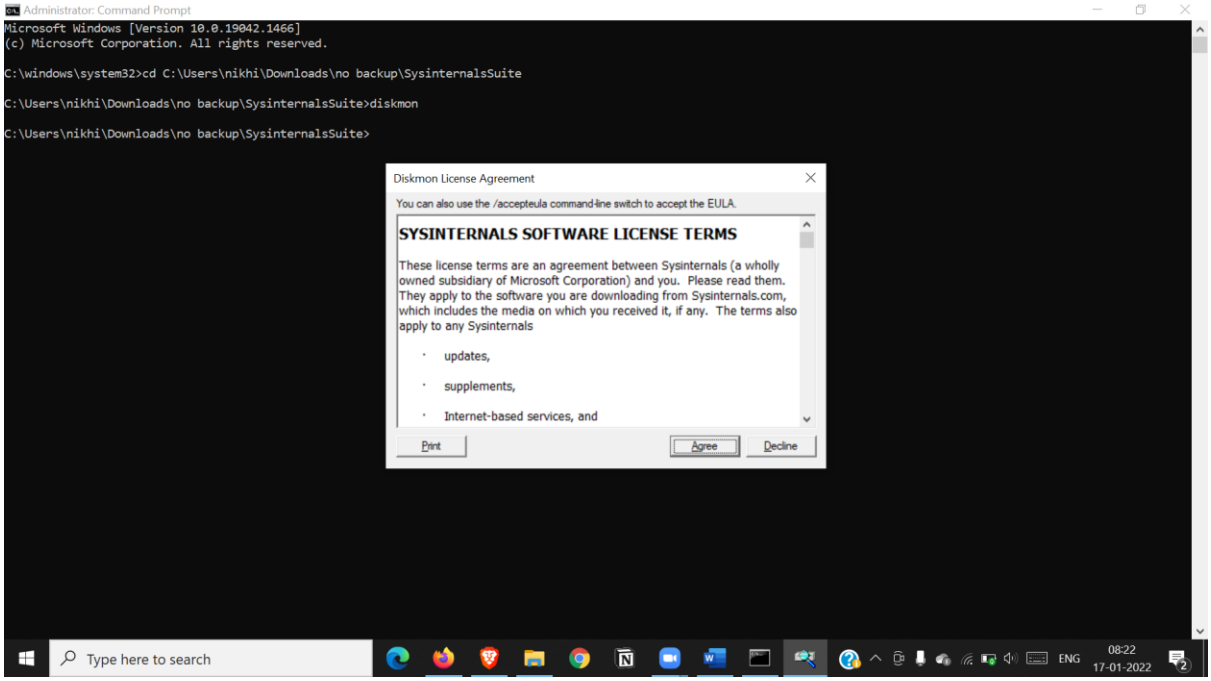
TCPView - Sysinternals: www.sysinternals.com
File Edit View Process Connection Options Help
TCP v4 TCP v6 UDP v4 UDP v6
Search
Process Name | Process ID | Protocol | State | Local Address | Local Port | Remote Address | Remote Port | Create Time | Module Name
OneDrive.exe 18012 TCP Established 192.168.0.105 56789 20.197.71.89 443 17-01-2022 07:17:19 OneDrive.exe
ExpressVPNNotificatio... 12940 TCP Listen 127.0.0.1 56862 0.0.0.0 0 17-01-2022 07:17:39 ExpressVPNNotificationService...
ExpressVPNNotificatio... 12940 TCP Established 127.0.0.1 56862 127.0.0.1 56865 17-01-2022 07:17:39 ExpressVPNNotificationService...
expressvpnd.exe 5596 TCP Established 127.0.0.1 56865 127.0.0.1 56862 17-01-2022 07:17:39 expressvpnd.exe
HP.myHP.exe 20656 TCP Close Wait 192.168.0.105 57011 52.218.179.98 443 17-01-2022 07:18:54 HP.myHP.exe
Zoom.exe 21248 TCP Established 192.168.0.105 60484 170.114.14.71 443 17-01-2022 07:29:38 Zoom.exe
Zoom.exe 21248 TCP Established 192.168.0.105 60487 170.114.15.55 443 17-01-2022 07:29:39 Zoom.exe
Zoom.exe 21248 TCP Close Wait 192.168.0.105 60489 3.235.96.63 443 17-01-2022 07:29:41 Zoom.exe
Zoom.exe 21248 TCP Close Wait 192.168.0.105 60491 52.202.62.222 443 17-01-2022 07:29:41 Zoom.exe
Zoom.exe 21248 TCP Close Wait 192.168.0.105 60492 170.114.2.69 443 17-01-2022 07:29:41 Zoom.exe
Zoom.exe 21248 TCP Close Wait 192.168.0.105 60493 170.114.2.69 443 17-01-2022 07:29:41 Zoom.exe
Zoom.exe 21248 TCP Close Wait 192.168.0.105 60514 134.224.191.31 443 17-01-2022 07:29:44 Zoom.exe
Zoom.exe 21248 TCP Close Wait 192.168.0.105 60558 173.231.92.42 443 17-01-2022 07:30:42 Zoom.exe
WINWORD.EXE 22888 TCP Established 192.168.0.105 60647 52.108.85.0 443 17-01-2022 07:43:48 WINWORD.EXE
firefox.exe 20364 TCP Established 127.0.0.1 60651 127.0.0.1 60652 17-01-2022 07:44:03 firefox.exe
firefox.exe 20364 TCP Established 127.0.0.1 60652 127.0.0.1 60651 17-01-2022 07:44:03 firefox.exe
firefox.exe 2412 TCP Established 127.0.0.1 60653 127.0.0.1 60654 17-01-2022 07:44:05 firefox.exe
firefox.exe 2412 TCP Established 127.0.0.1 60654 127.0.0.1 60653 17-01-2022 07:44:05 firefox.exe
firefox.exe 5196 TCP Established 127.0.0.1 60656 127.0.0.1 60657 17-01-2022 07:44:06 firefox.exe
firefox.exe 5196 TCP Established 127.0.0.1 60657 127.0.0.1 60656 17-01-2022 07:44:06 firefox.exe
firefox.exe 18420 TCP Established 127.0.0.1 60663 127.0.0.1 60664 17-01-2022 07:44:06 firefox.exe
firefox.exe 18420 TCP Established 127.0.0.1 60664 127.0.0.1 60663 17-01-2022 07:44:06 firefox.exe
firefox.exe 20364 TCP Established 192.168.0.105 60667 44.233.196.75 443 17-01-2022 07:44:07 firefox.exe
firefox.exe 11772 TCP Established 127.0.0.1 60693 127.0.0.1 60694 17-01-2022 07:44:07 firefox.exe
firefox.exe 11772 TCP Established 127.0.0.1 60694 127.0.0.1 60693 17-01-2022 07:44:07 firefox.exe
firefox.exe 11292 TCP Established 127.0.0.1 60703 127.0.0.1 60704 17-01-2022 07:44:07 firefox.exe
firefox.exe 11292 TCP Established 127.0.0.1 60704 127.0.0.1 60703 17-01-2022 07:44:07 firefox.exe
[Time Wait] TCP Time Wait 192.168.0.105 60710 34.120.208.123 443
Endpoints: 181 Established: 57 Listening: 33 Time Wait: 21 Close Wait: 8 Update: 2 sec States: (All)
Type here to search
ENG
07:52
17-01-2022

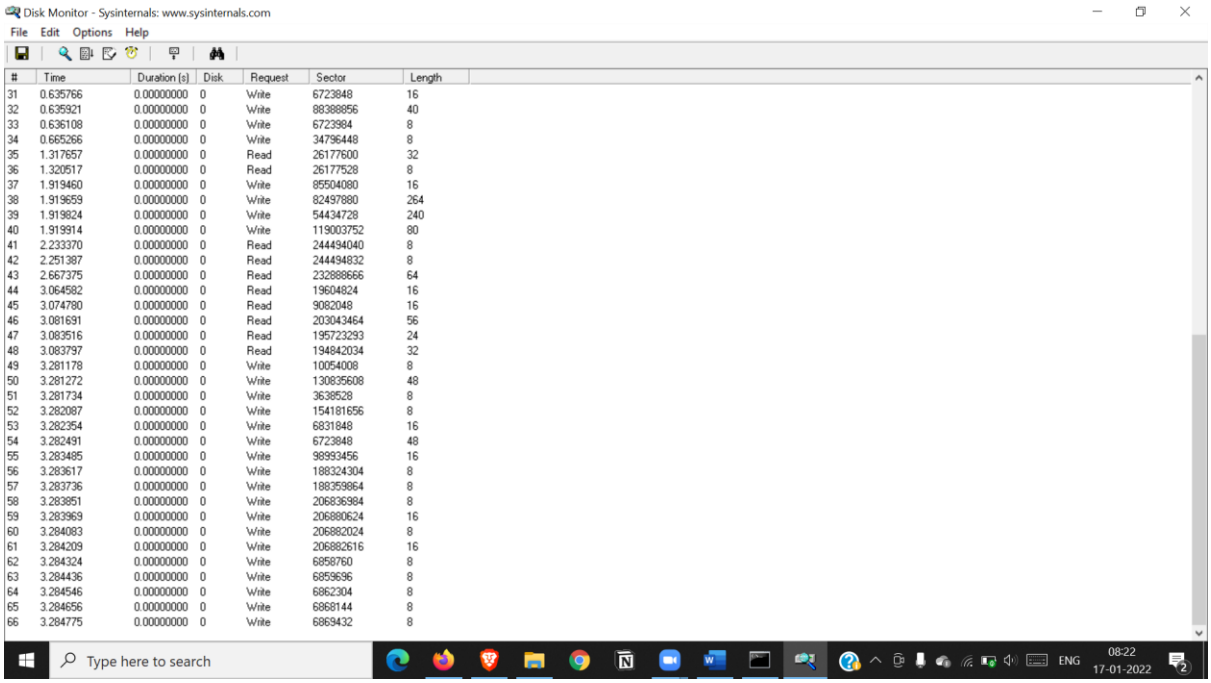






Diskmonitoring


Administrator: Command Prompt
Microsoft Windows [Version 10.0.19042.1466]
(c) Microsoft Corporation. All rights reserved.
C:\windows\system32>cd C:\Users\nikhi\Downloads\no backup\SysinternalsSuite
C:\Users\nikhi\Downloads\no backup\SysinternalsSuite>diskmon
C:\Users\nikhi\Downloads\no backup\SysinternalsSuite>
Diskmon License Agreement
You can also use the /accepteula command-line switch to accept the EULA.
SYSINTERNALS 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
ENG
08:22
17-01-2022


Disk Monitor - Sysinternals: www.sysinternals.com
File Edit Options Help
Time Duration (s) Disk Request Sector Length
31 0.635766 0.00000000 0 Write 6723848 16
32 0.635921 0.00000000 0 Write 88388856 40
33 0.636108 0.00000000 0 Write 6723984 8
34 0.665266 0.00000000 0 Write 34796448 8
35 1.317657 0.00000000 0 Read 26177600 32
36 1.320517 0.00000000 0 Read 26177528 8
37 1.919460 0.00000000 0 Write 85504080 16
38 1.919659 0.00000000 0 Write 82497880 264
39 1.919824 0.00000000 0 Write 54434728 240
40 1.919914 0.00000000 0 Write 119003752 80
41 2.233370 0.00000000 0 Read 244494040 8
42 2.251387 0.00000000 0 Read 244494832 8
43 2.667375 0.00000000 0 Read 232888666 64
44 3.064582 0.00000000 0 Read 19604824 16
45 3.074780 0.00000000 0 Read 9082048 16
46 3.081691 0.00000000 0 Read 203043464 56
47 3.083516 0.00000000 0 Read 195723293 24
48 3.083797 0.00000000 0 Read 194842034 32
49 3.281178 0.00000000 0 Write 10054008 8
50 3.281272 0.00000000 0 Write 130835608 48
51 3.281734 0.00000000 0 Write 3638528 8
52 3.282087 0.00000000 0 Write 154181656 8
53 3.282354 0.00000000 0 Write 6831848 16
54 3.282491 0.00000000 0 Write 6723848 48
55 3.283485 0.00000000 0 Write 98993456 16
56 3.283617 0.00000000 0 Write 188324304 8
57 3.283736 0.00000000 0 Write 188359864 8
58 3.283851 0.00000000 0 Write 206836984 8
59 3.283969 0.00000000 0 Write 206880624 16
60 3.284083 0.00000000 0 Write 206882024 8
61 3.284209 0.00000000 0 Write 206882616 16
62 3.284324 0.00000000 0 Write 6858760 8
63 3.284436 0.00000000 0 Write 6859696 8
64 3.284546 0.00000000 0 Write 6862304 8
65 3.284656 0.00000000 0 Write 6868144 8
66 3.284775 0.00000000 0 Write 6869432 8
Type here to search
ENG
08:22
17-01-2022

Practical 7

Aim: Recovering and Inspecting the recovered files.

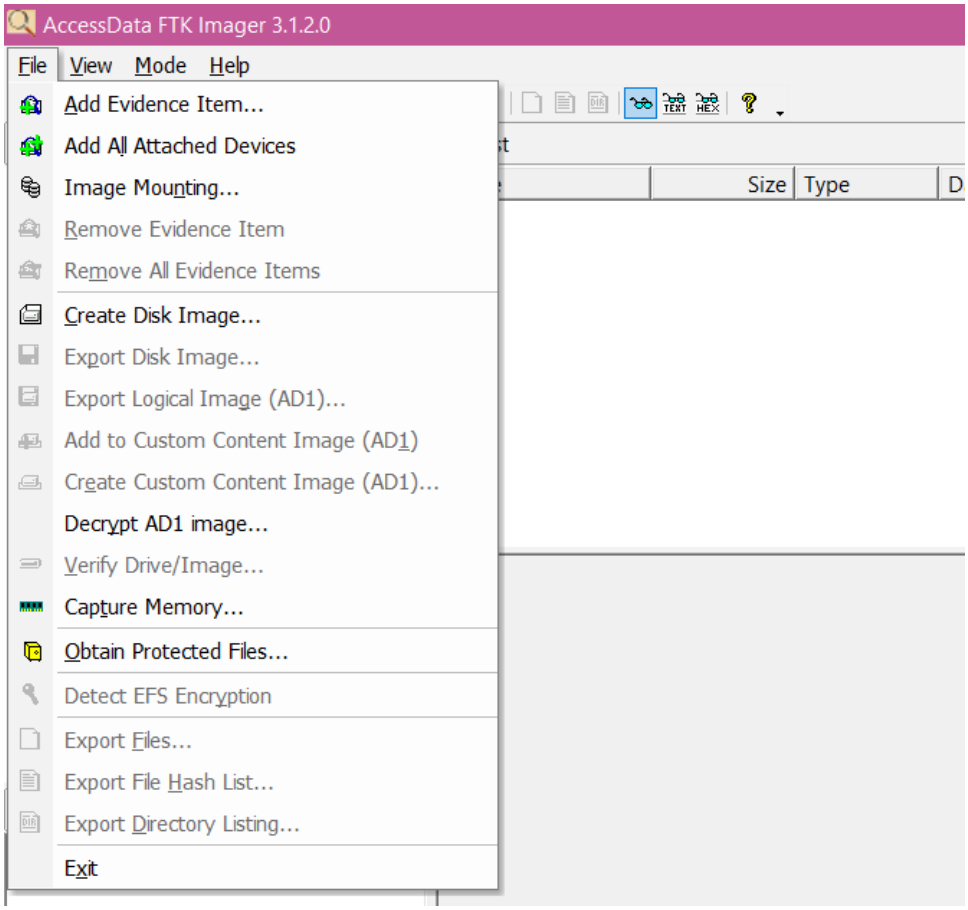
I) Check for deleted files.

II) Recover the Deleted Files.

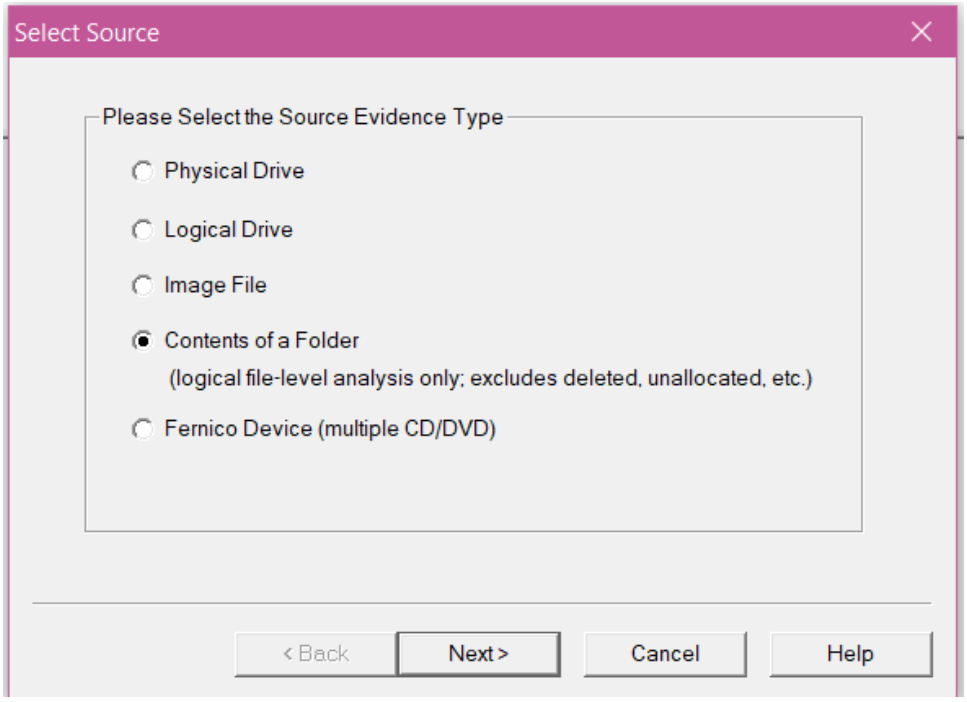
Steps:

1) First, create a text file and paste some data in it and store it in a folder.

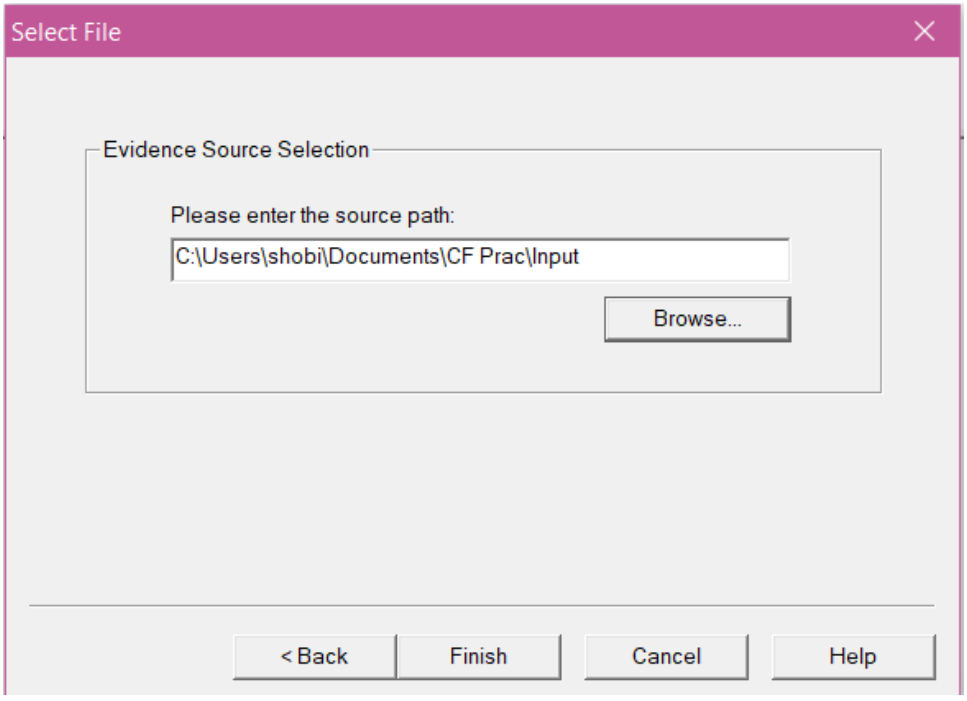
2) Open AccessData FTK Imager then click on file and select “Create Disk image”.



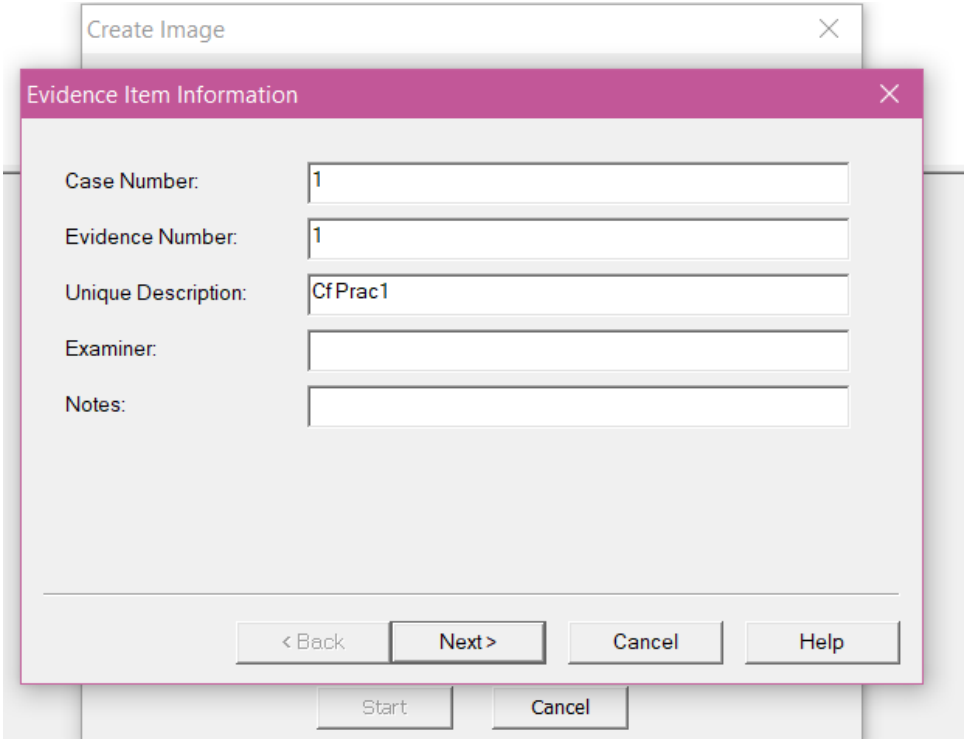
3) Select source as Content of a folder and click on next.



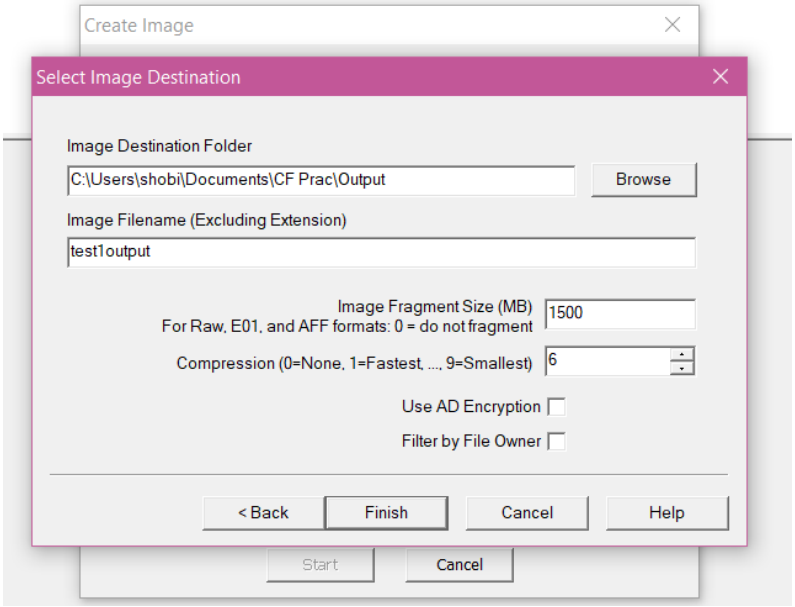
4) Then browse the source evidence that we created previously as a text file then click on finish.



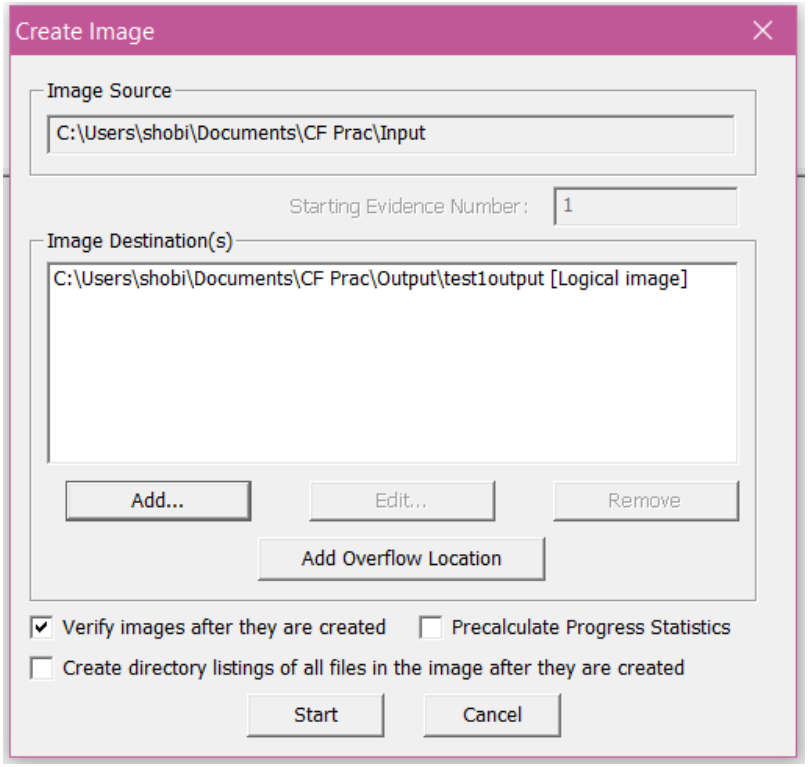
5) Enter the evidence item information and click on next.



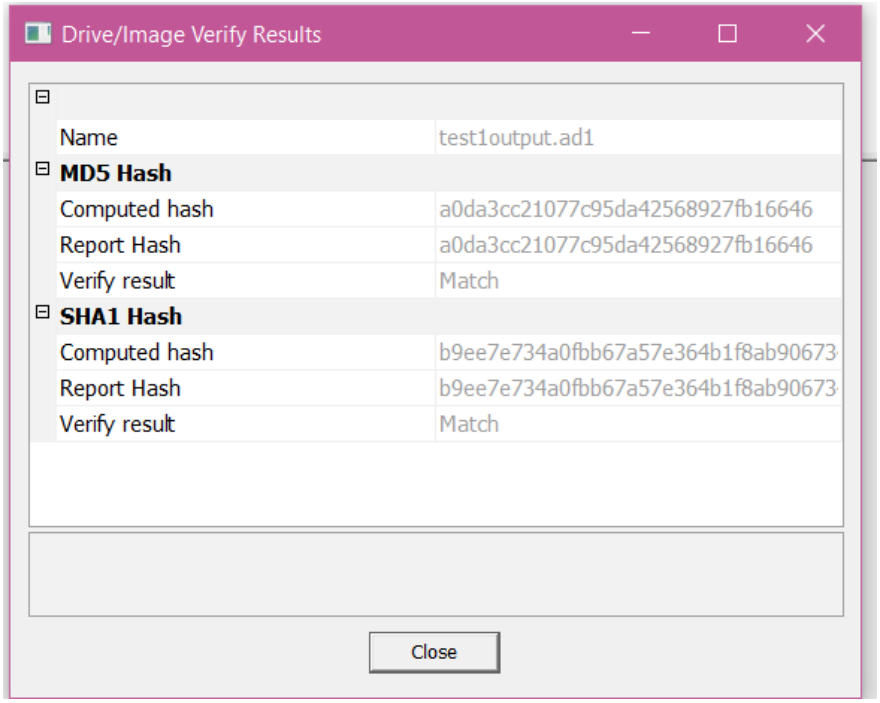
6) Then browse the image destination folder and name the image file and click on finish.



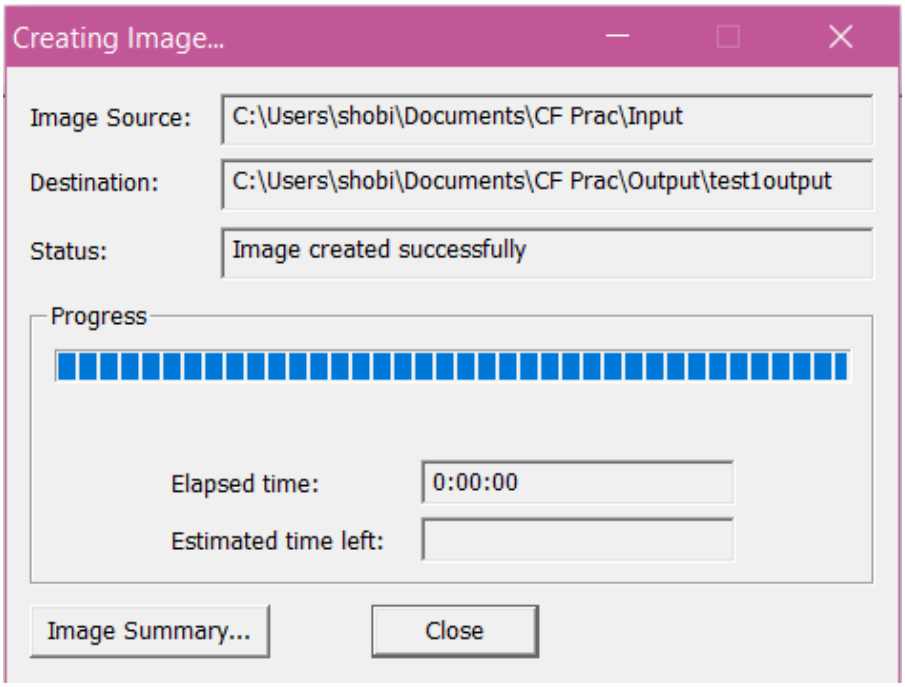
7) For creating and image, click on start.



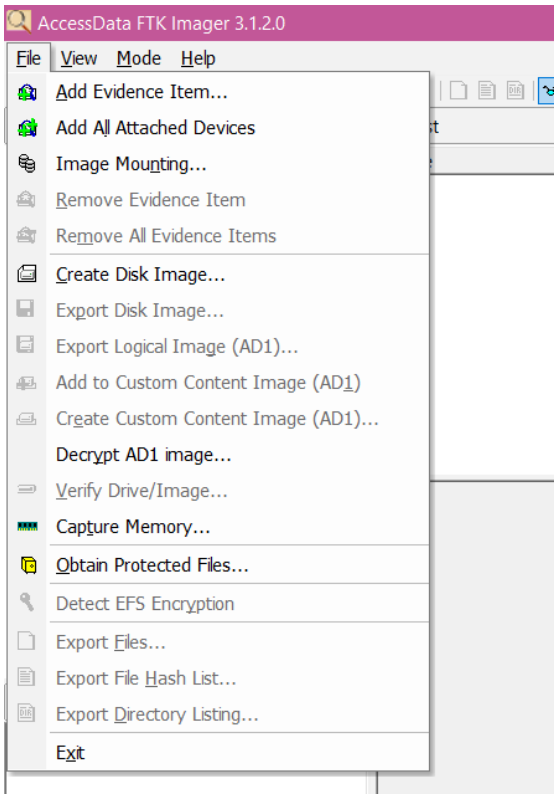
8) As we get the result, we can verify by looking at the verify result of both the hashing functions.



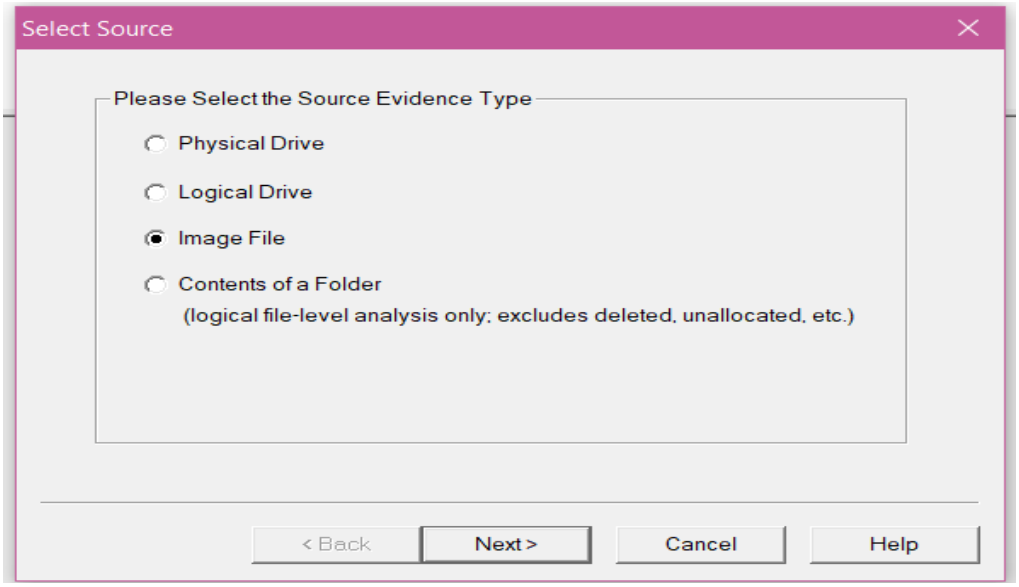
9) Atlast, we get the status of the creation and we can also view image summary.



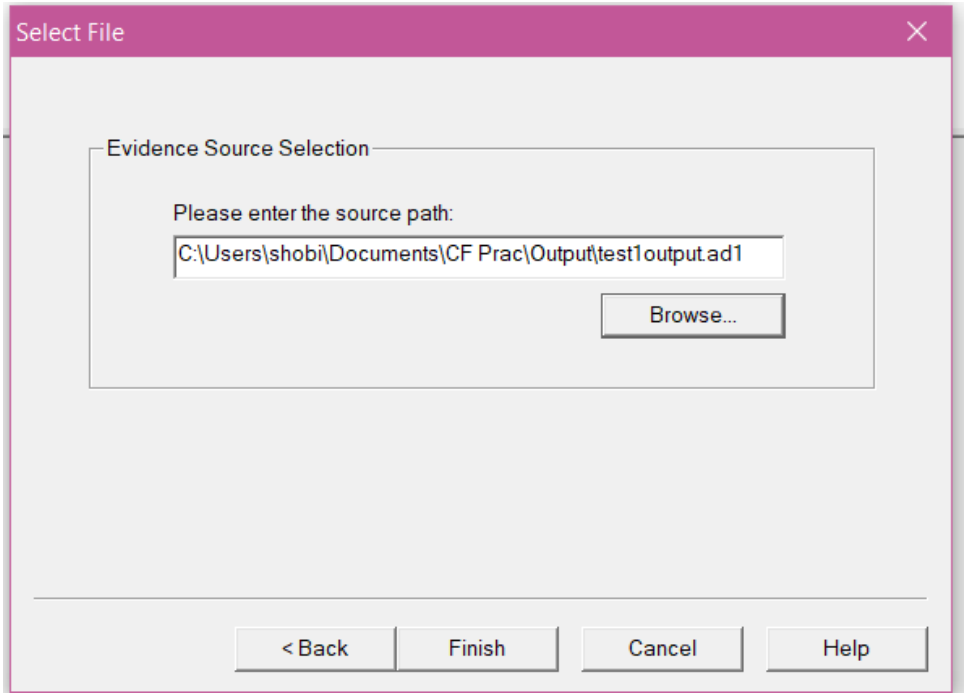
10) For adding an evidence, select “Add evidence item”.



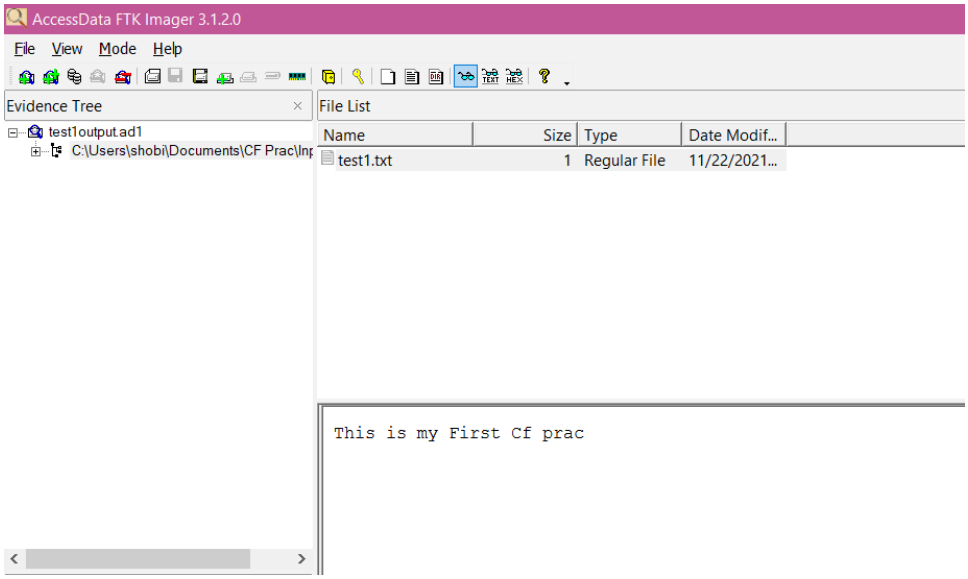
11) Select source as image file and click on next.



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.

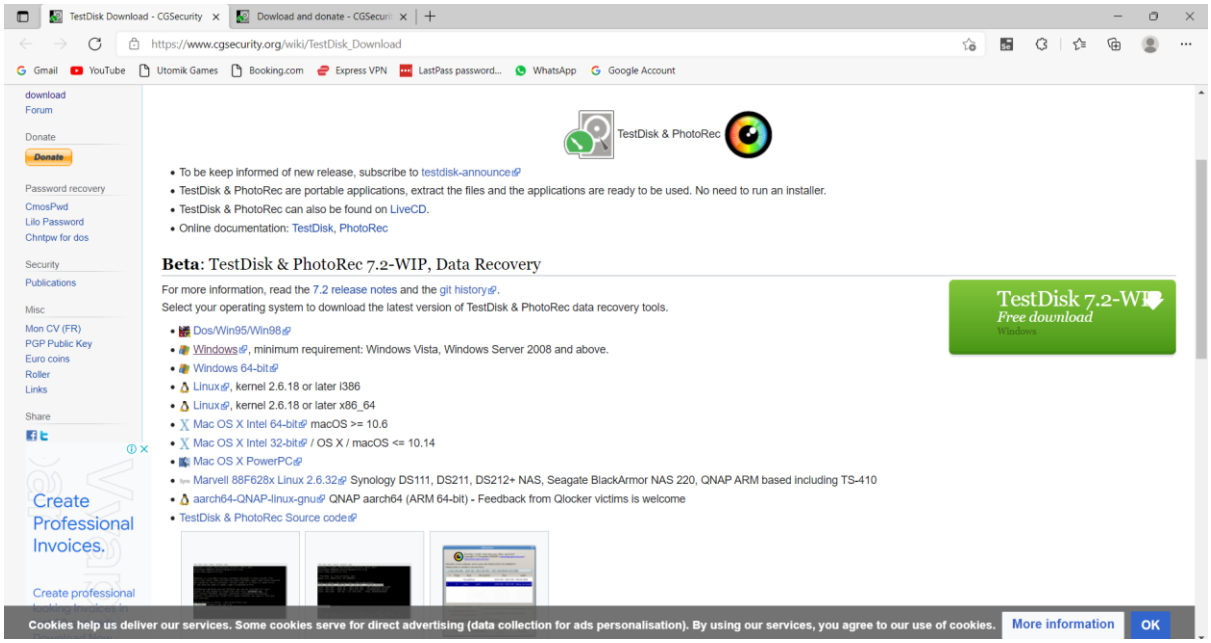


III) Analyzing and inspecting the recovered files.

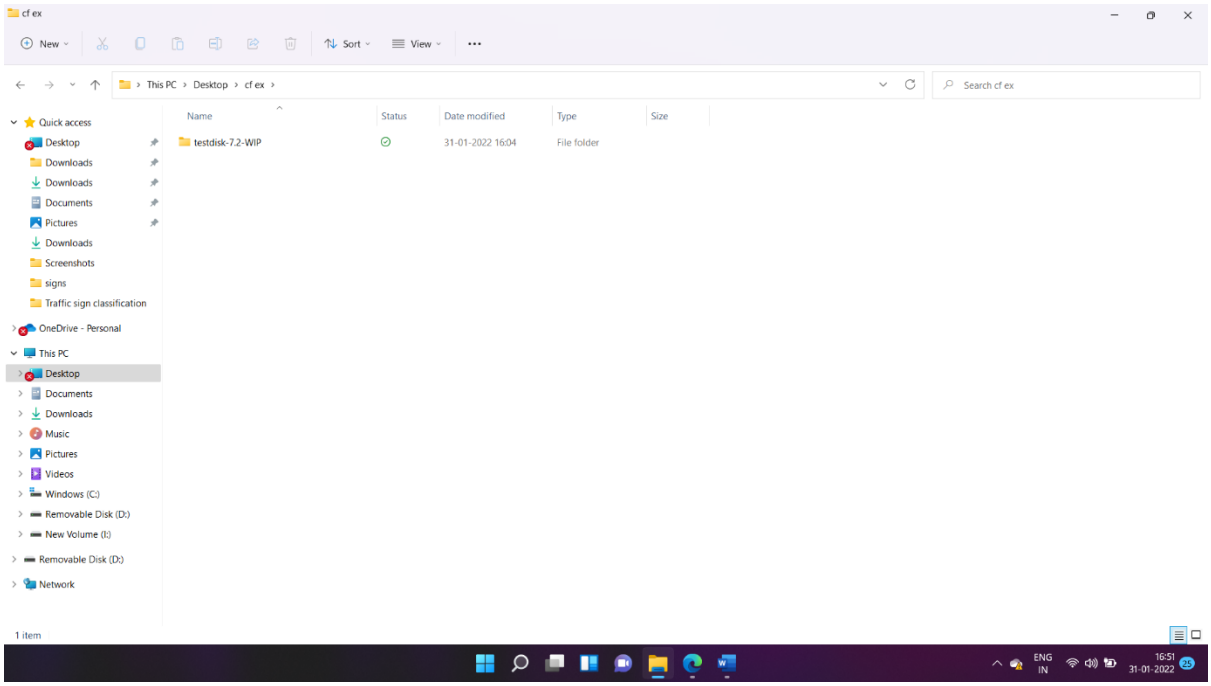
Perform this using recovery option in ENCASE and also Perform manually through command line.

Steps:

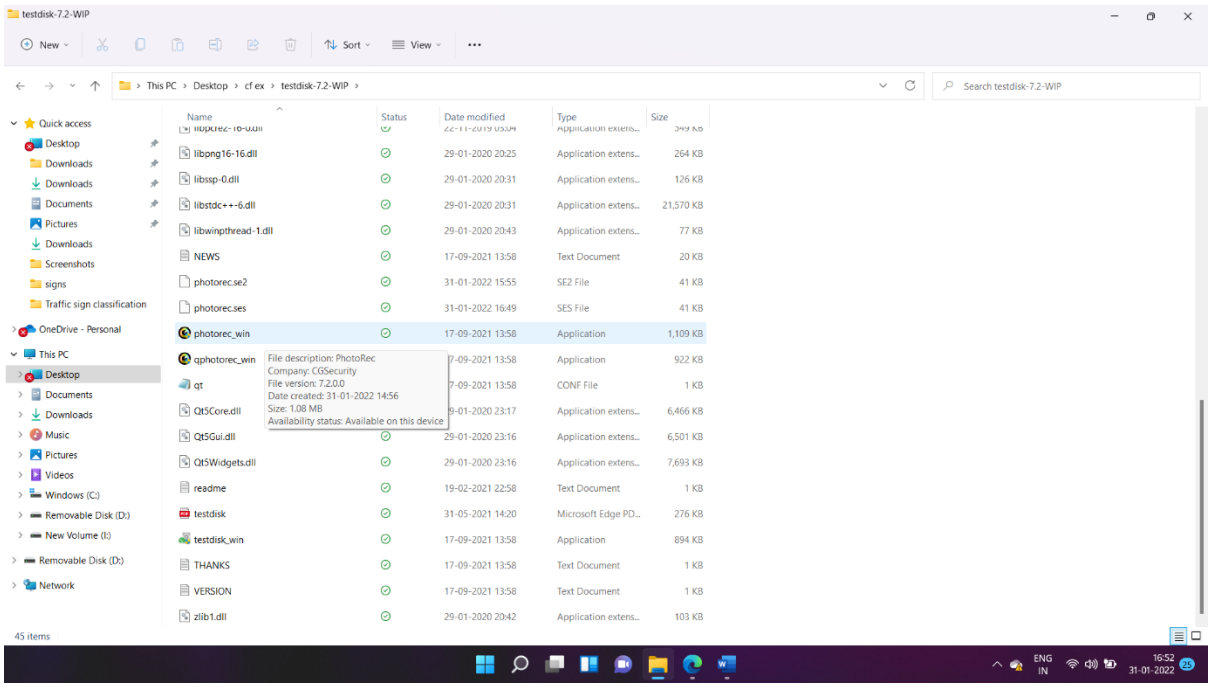
1) Download TestDisk zip file.



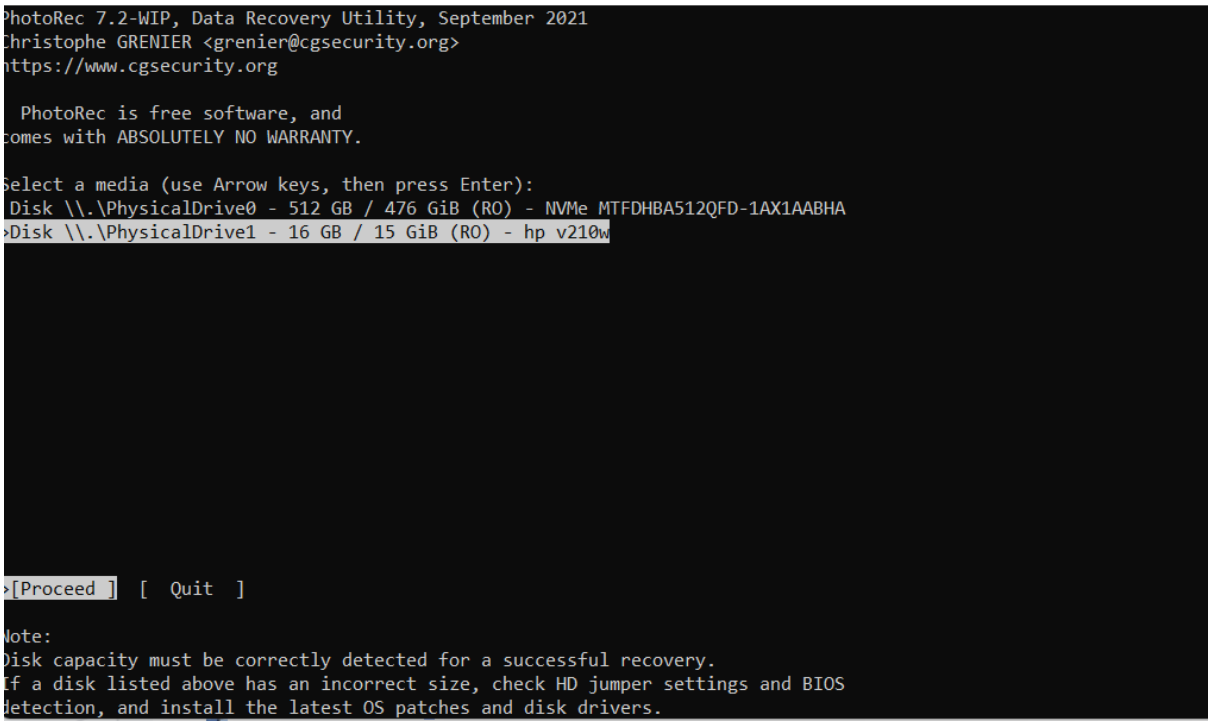
2) Extract the downloaded file in a folder.



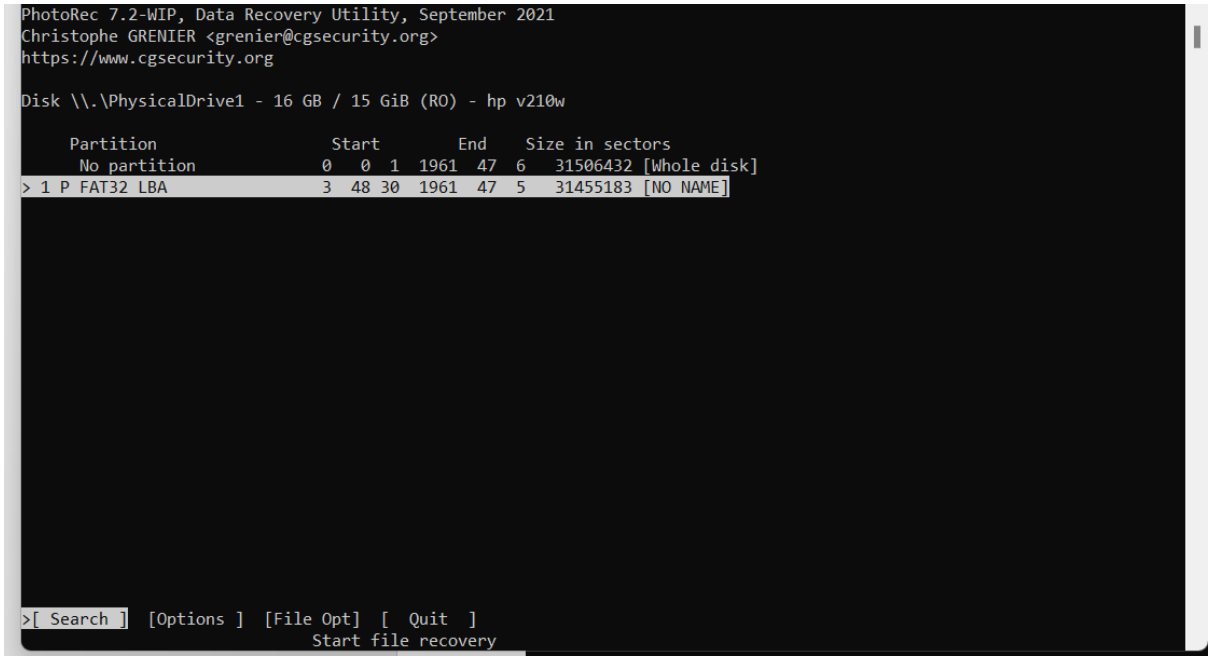
3) In that file, open “photorec_win” application.



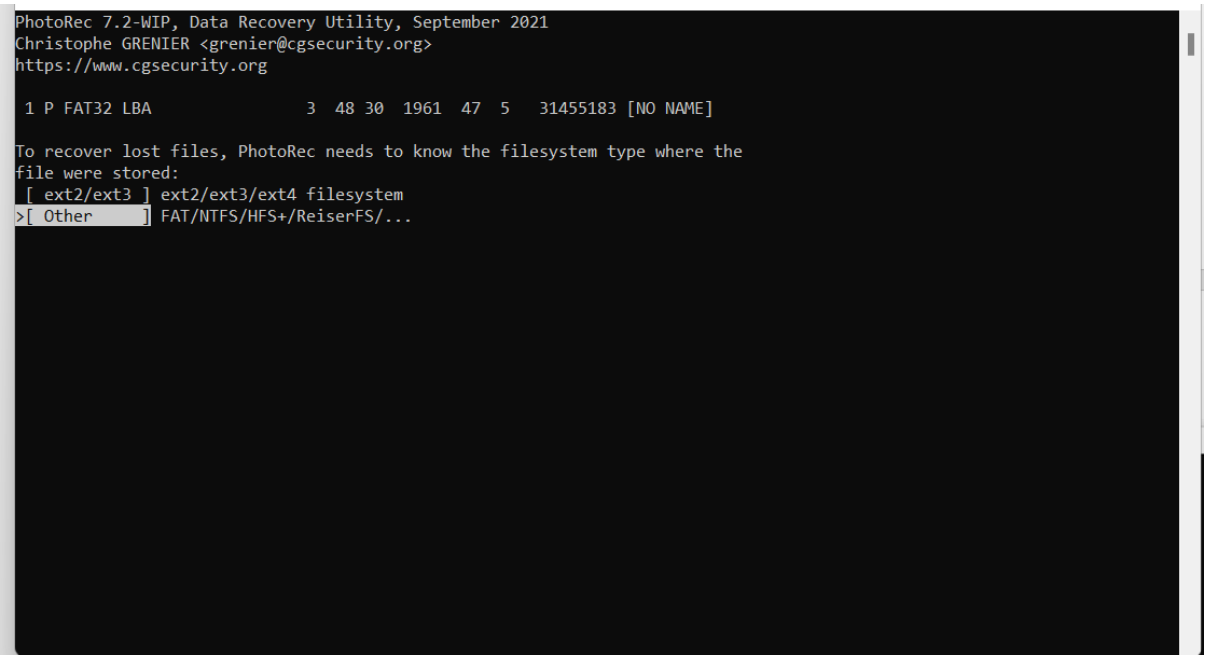
4) Then select the pen drive that you attached to your PC and proceed.



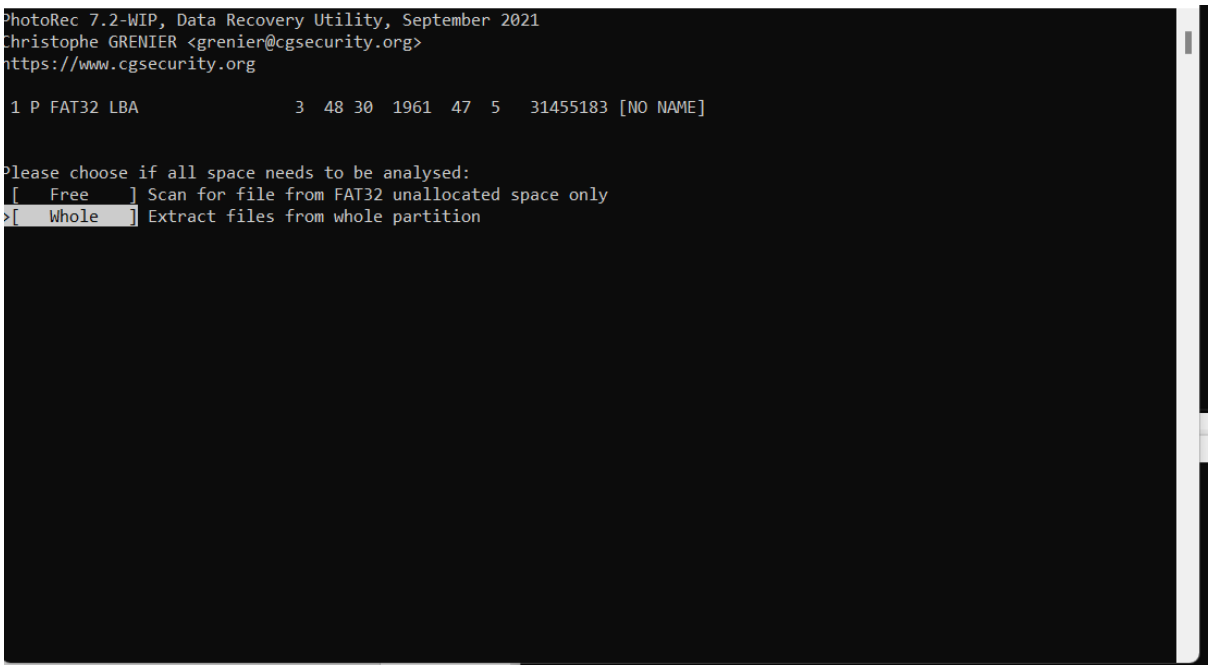
5) Then select the drive with the name of your pen drive and proceed.



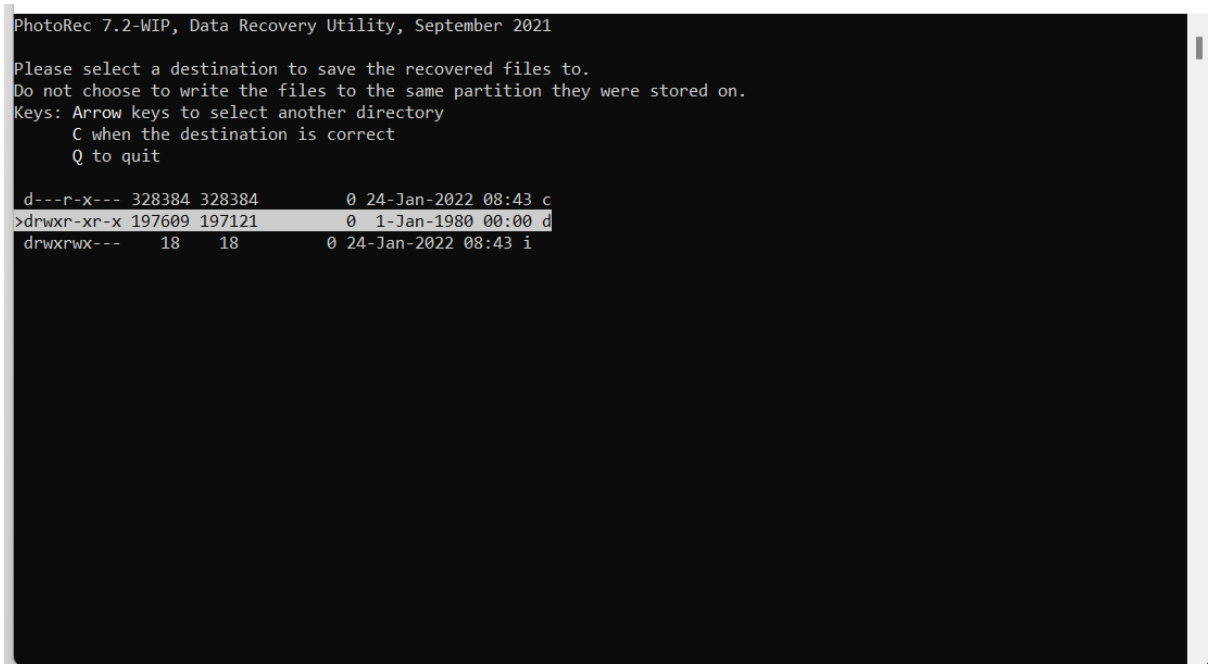
6) Then select on Other and proceed.



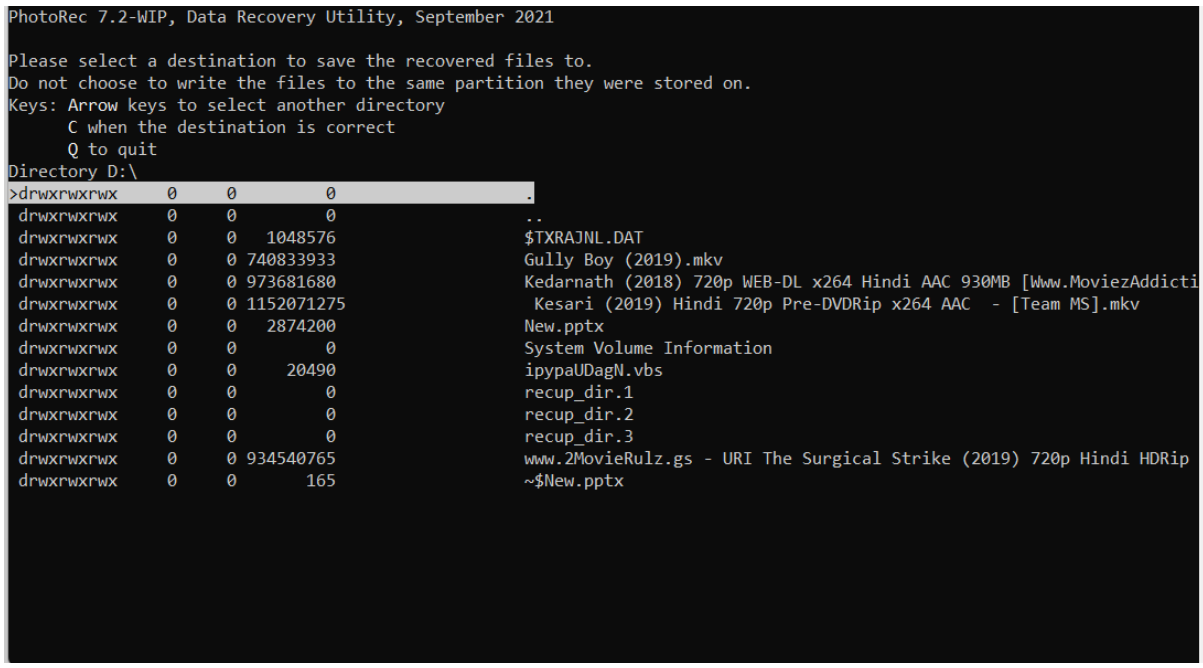
7) Select “Whole” for extracting files from whole partition and proceed.



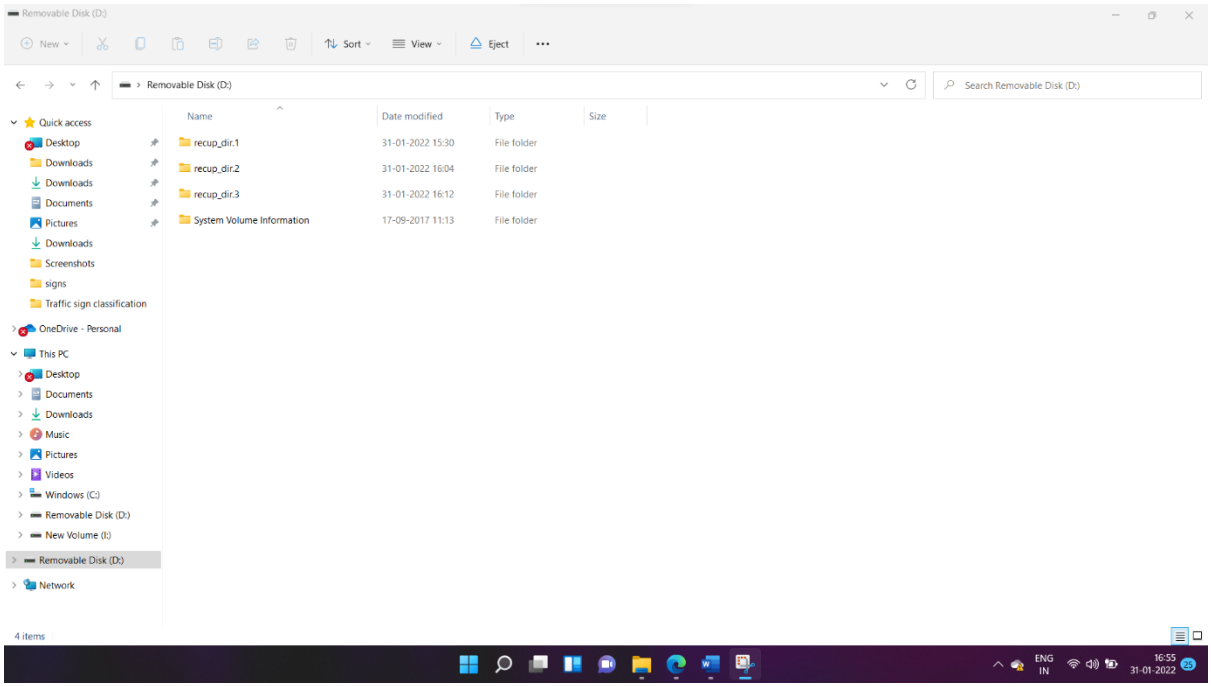
8) Then for going to another directory or drive use left arrow key on your keyboard, then select the pen drive to store the deleted data.



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



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

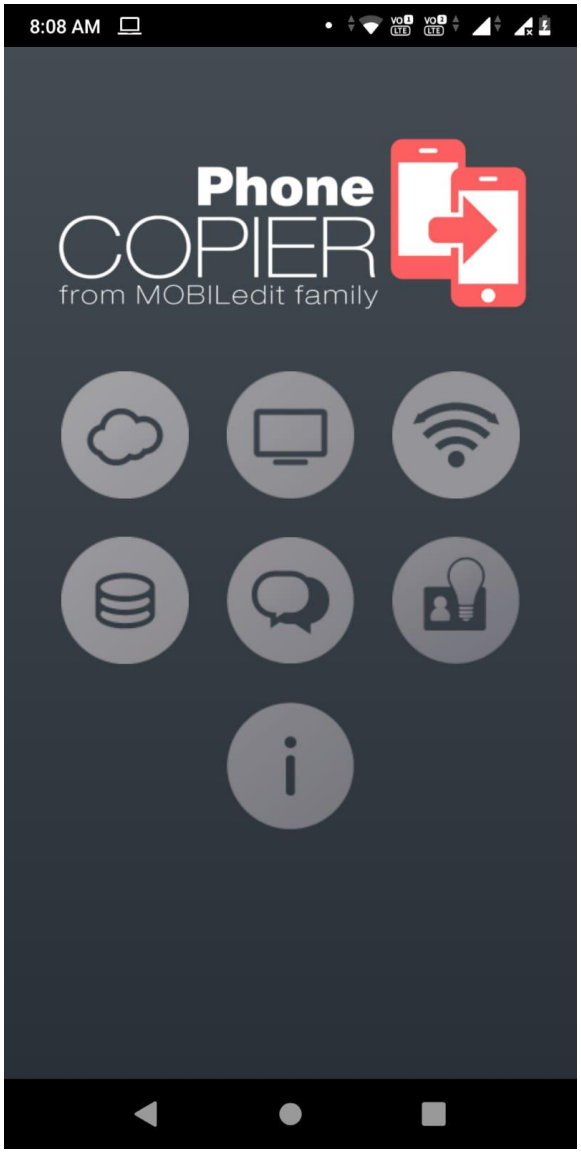

Removable Disk (D:)
New
Sort
View
Eject
Removable Disk (D:)
Search Removable Disk (D:)
Quick access
Desktop
Downloads
Downloads
Documents
Pictures
Downloads
Screenshots
signs
Traffic sign classification
OneDrive - Personal
This PC
Desktop
Documents
Downloads
Music
Pictures
Videos
Windows (C:)
Removable Disk (D:)
New Volume (I:)
Removable Disk (D:)
Network
Name
Date modified
Type
Size
recup_dir.1
31-01-2022 15:30
File folder
recup_dir.2
31-01-2022 16:04
File folder
recup_dir.3
31-01-2022 16:12
File folder
System Volume Information
17-09-2017 11:13
File folder
4 items
ENG
IN
16:55
31-01-2022

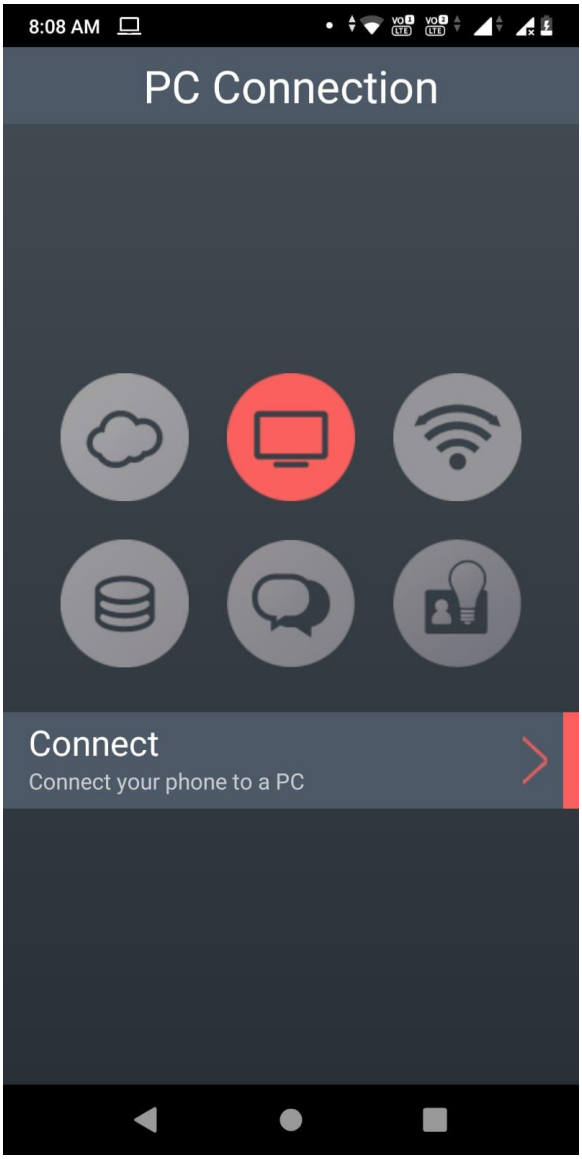
Practical:8

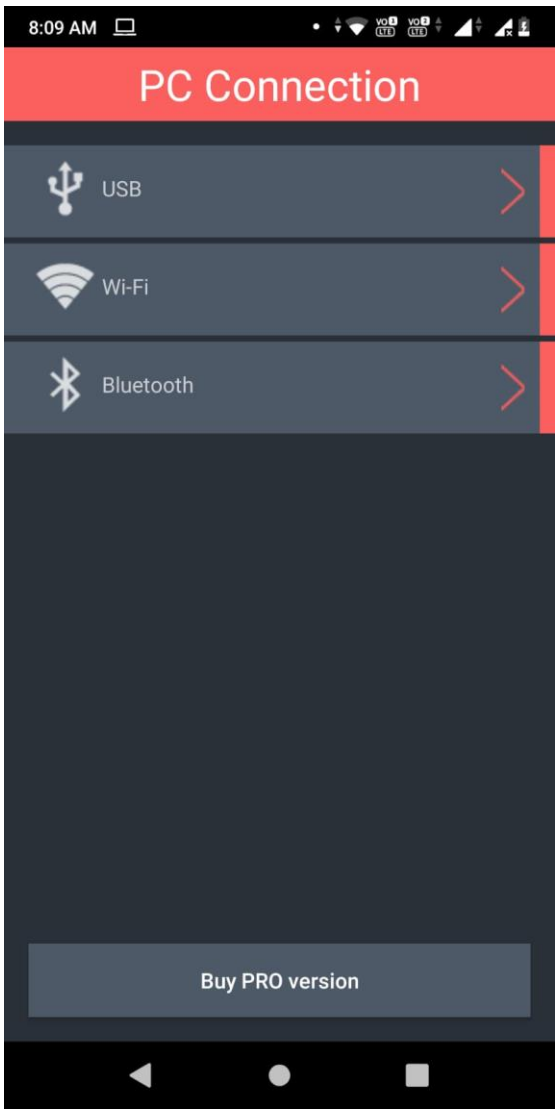
Aim: Acquisition of Cell phones and Mobile devices

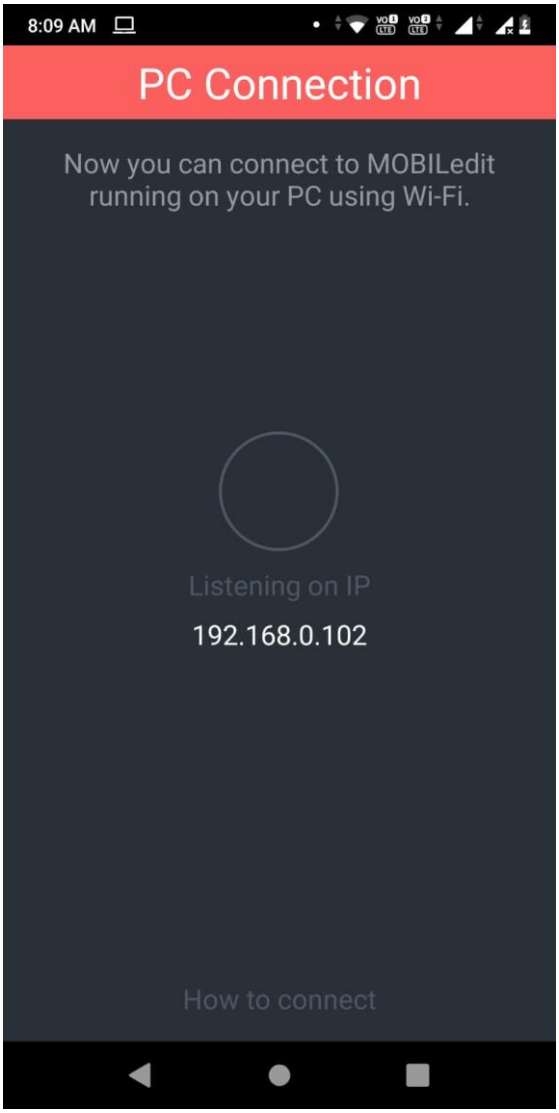
MOBILE:

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

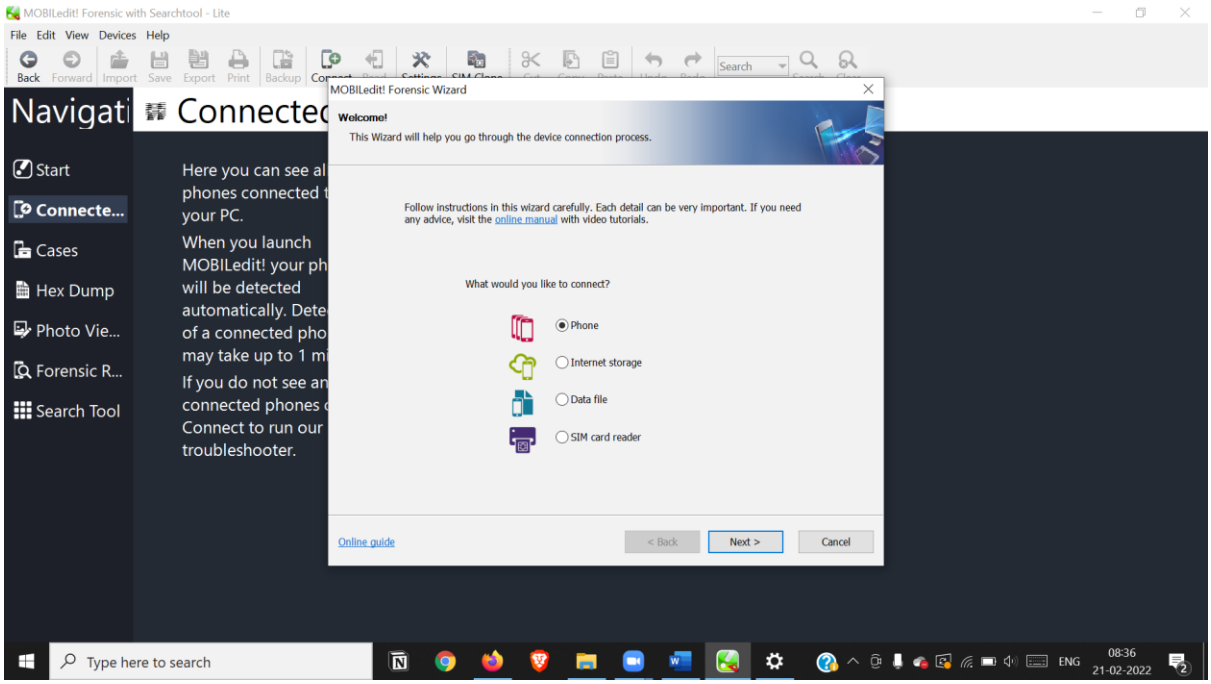


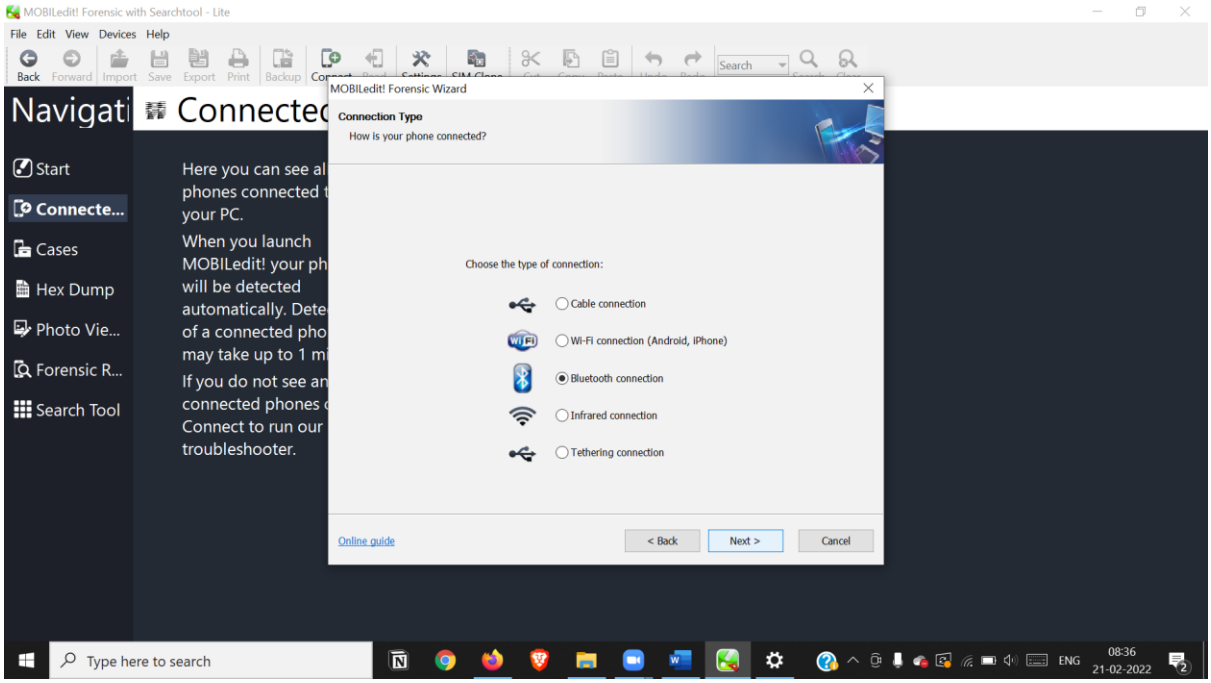


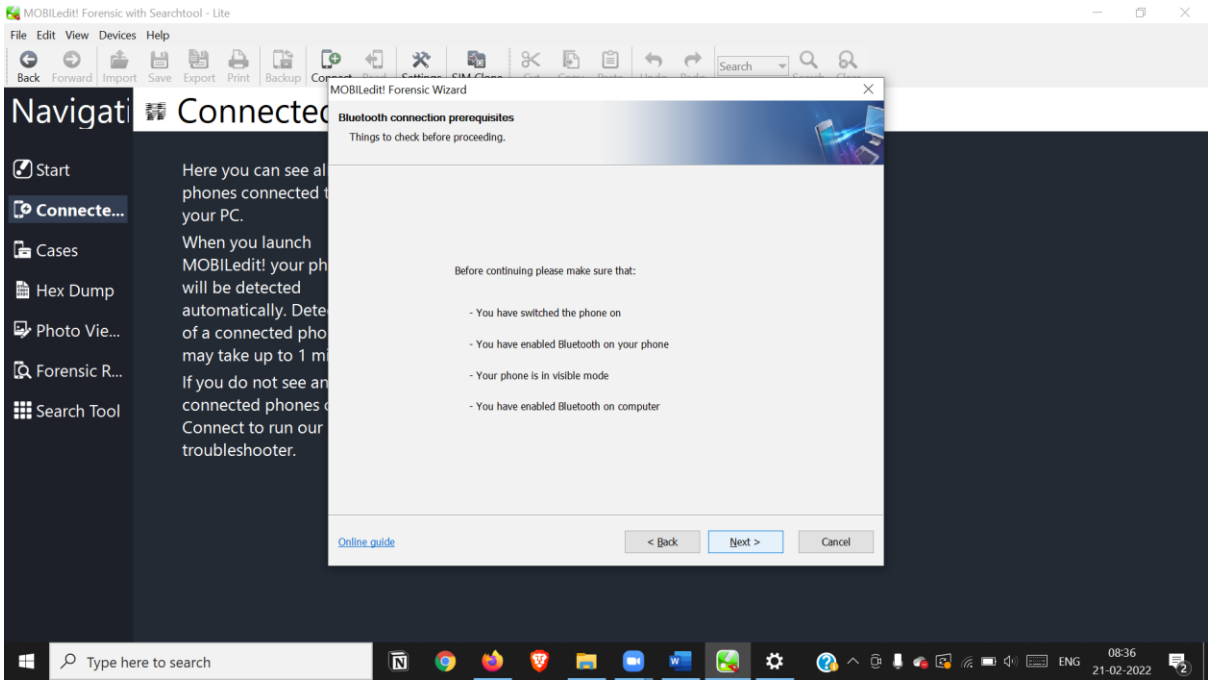




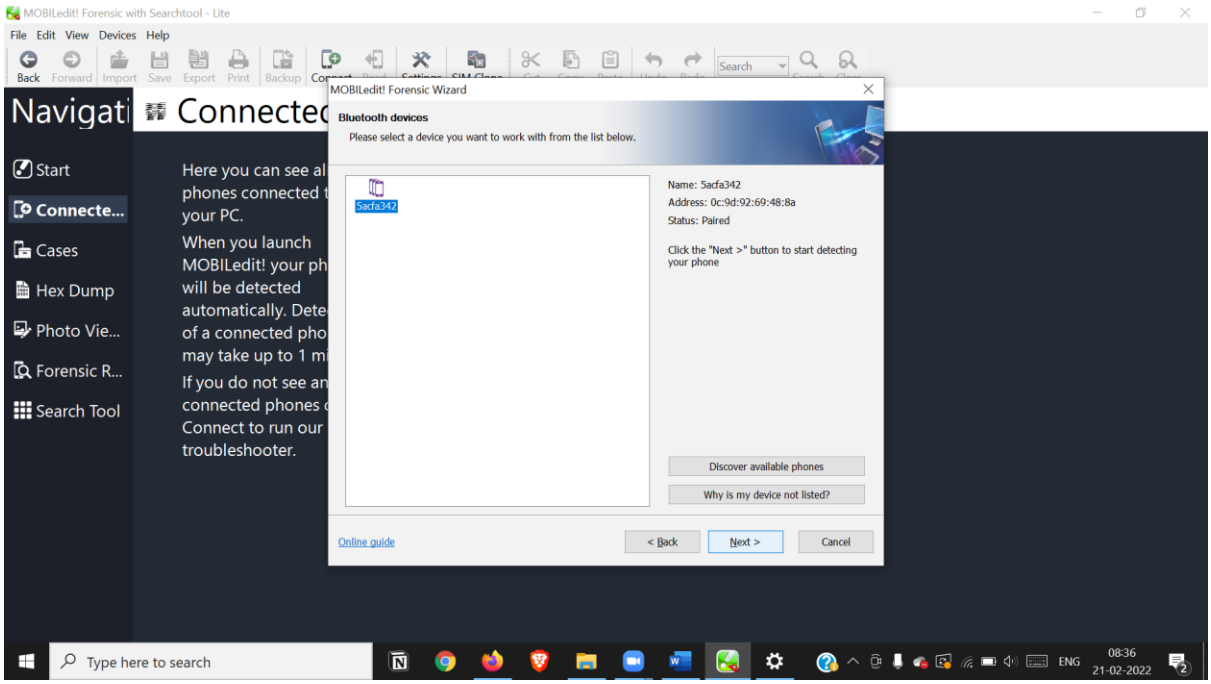
PC: Pair / connect with your pc using usb, Bluetooth or Wifi,
Then open MobileEdit in your pc

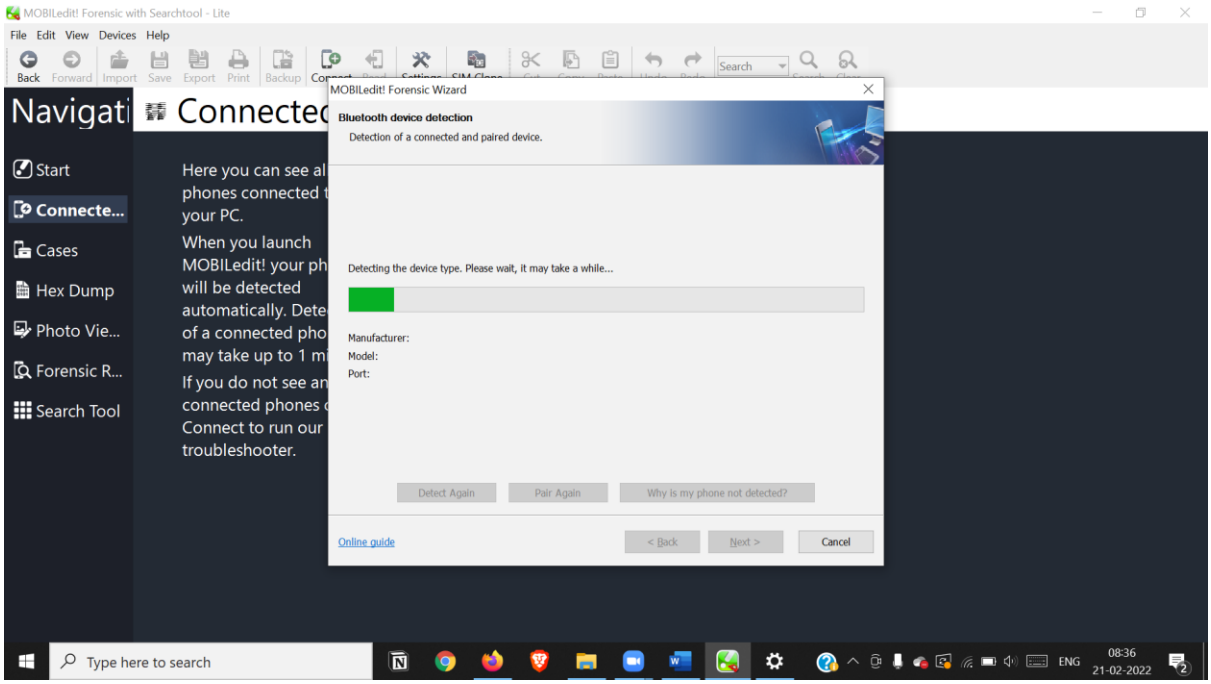

MOBILedit! Forensic with Searchtool - Lite
File Edit View Devices Help
Back Forward Import Save Export Print Backup
Search
Navigati
Connecte
Start
Connecte...
Cases
Hex Dump
Photo Vie...
Forensic R...
Search Tool
Here you can see al
phones connected t
your PC.
When you launch
MOBILedit! your ph
will be detected
automatically. Dete
of a connected pho
may take up to 1 mi
If you do not see an
connected phones
Connect to run our
troubleshooter.
MOBILedit! Forensic Wizard
Welcome!
This Wizard will help you go through the device connection process.
Follow instructions in this wizard carefully. Each detail can be very important. If you need any advice, visit the online manual with video tutorials.
What would you like to connect?
Phone
Internet storage
Data file
SIM card reader
Online guide
< Back
Next >
Cancel
Type here to search
ENG
08:36
21-02-2022

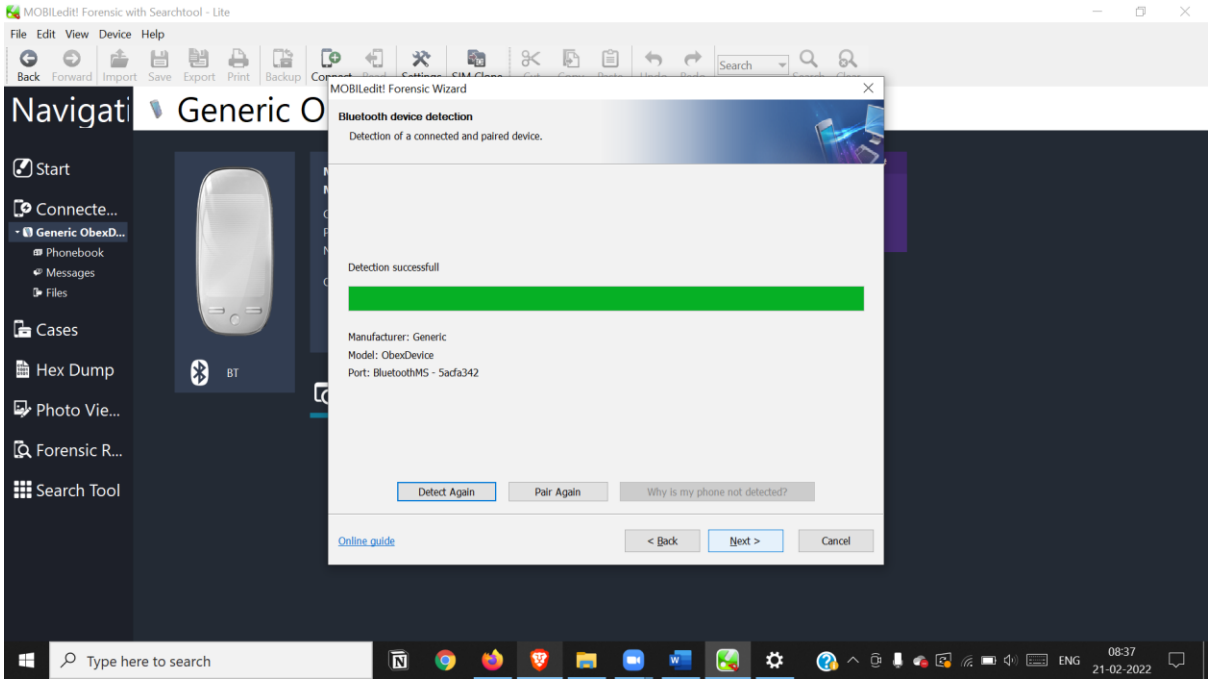

MOBILedit! Forensic with Searchtool - Lite
File Edit View Devices Help
Back Forward Import Save Export Print Backup
Search
Navigati
Connecte
Start
Connecte...
Cases
Hex Dump
Photo Vie...
Forensic R...
Search Tool
Here you can see al
phones connected t
your PC.
When you launch
MOBILedit! your ph
will be detected
automatically. Dete
of a connected pho
may take up to 1 mi
If you do not see an
connected phones
Connect to run our
troubleshooter.
MOBILedit! Forensic Wizard
Connection Type
How is your phone connected?
Choose the type of connection:
Cable connection
Wi-Fi connection (Android, iPhone)
Bluetooth connection
Infrared connection
Tethering connection
Online guide
< Back
Next >
Cancel
Type here to search
ENG
08:36
21-02-2022



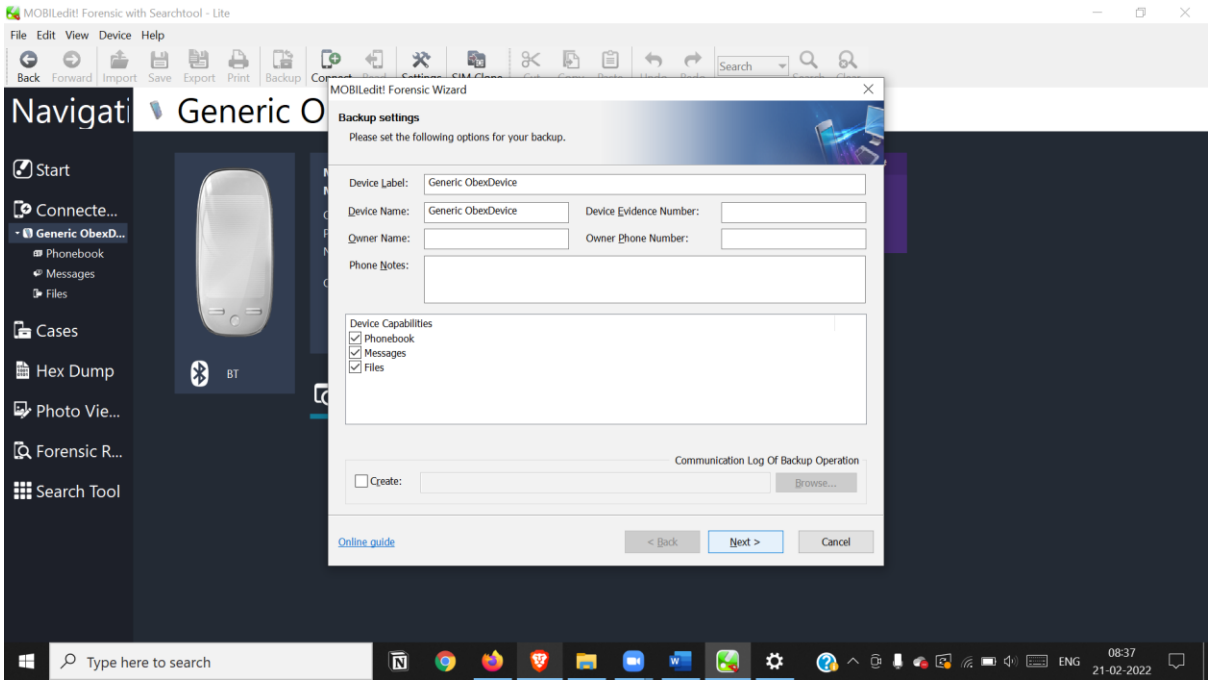
Find your Device and select next



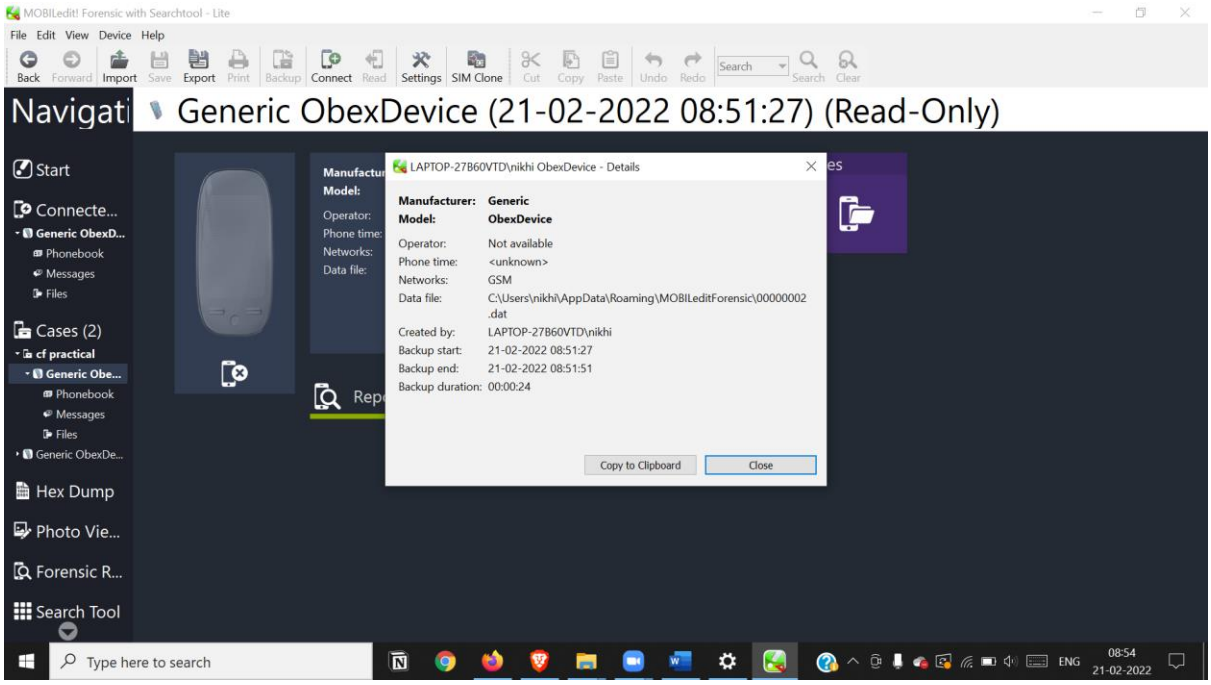




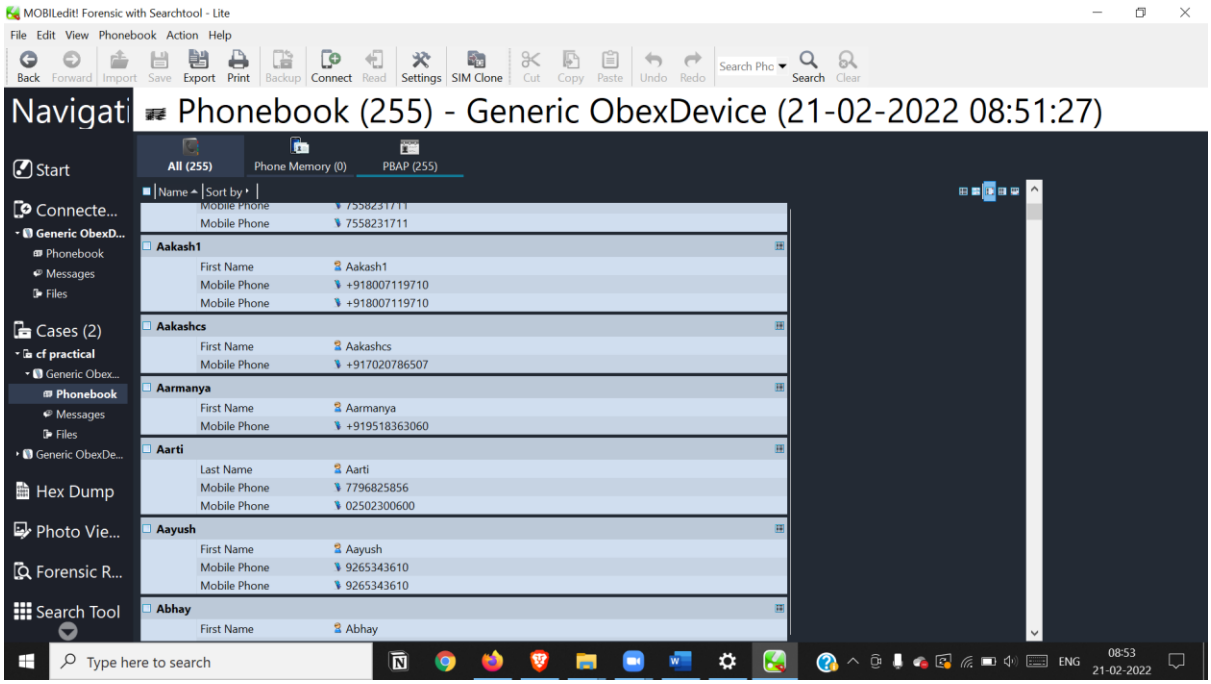
Set a Name for your device



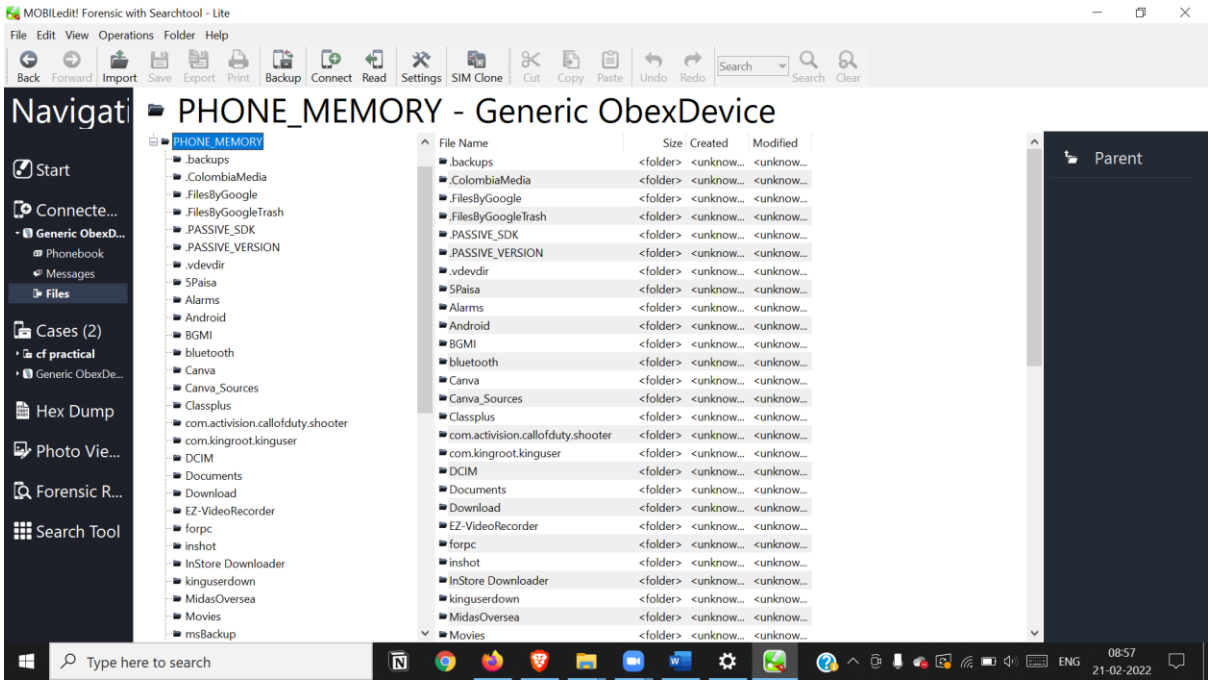
Get device Info



Get Phonebook Directory



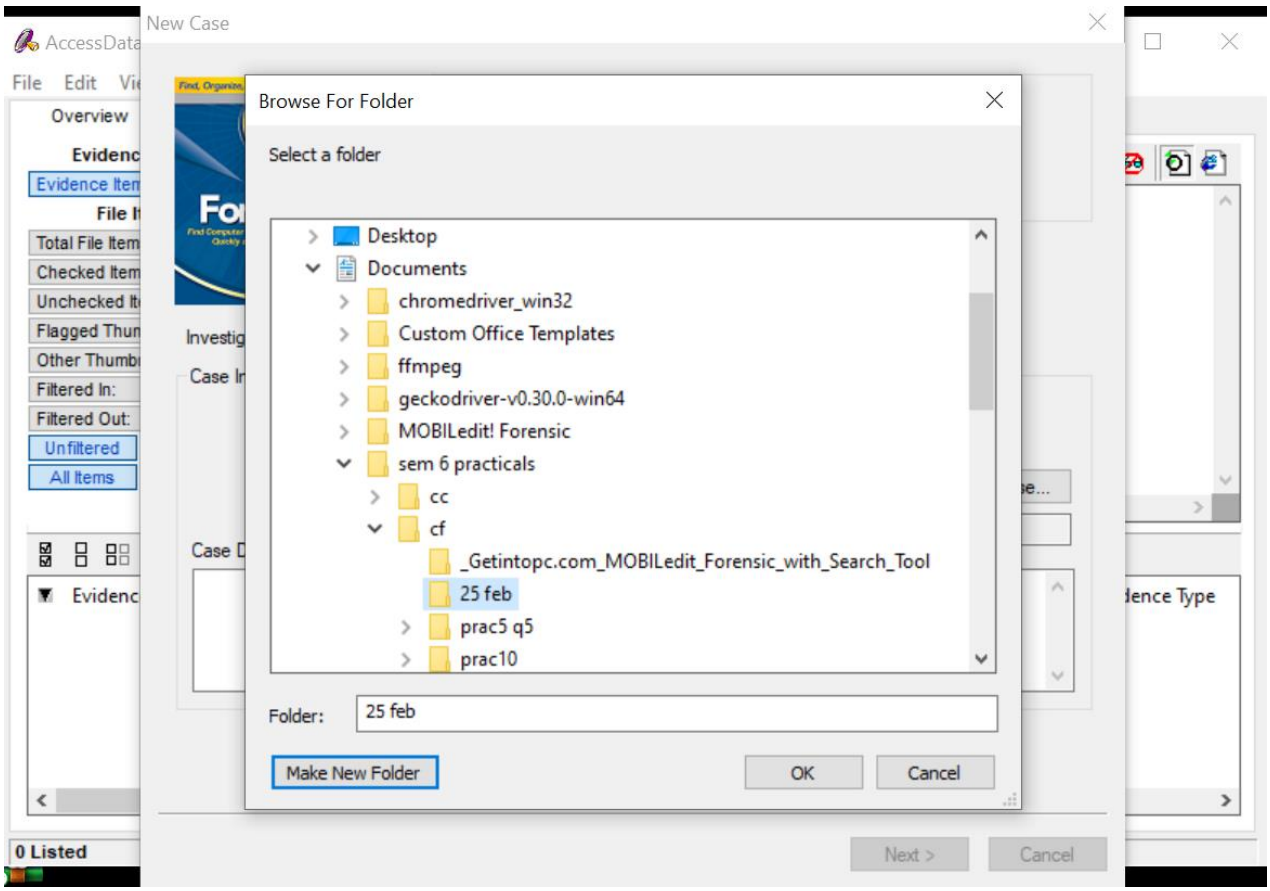
Get Files and messages



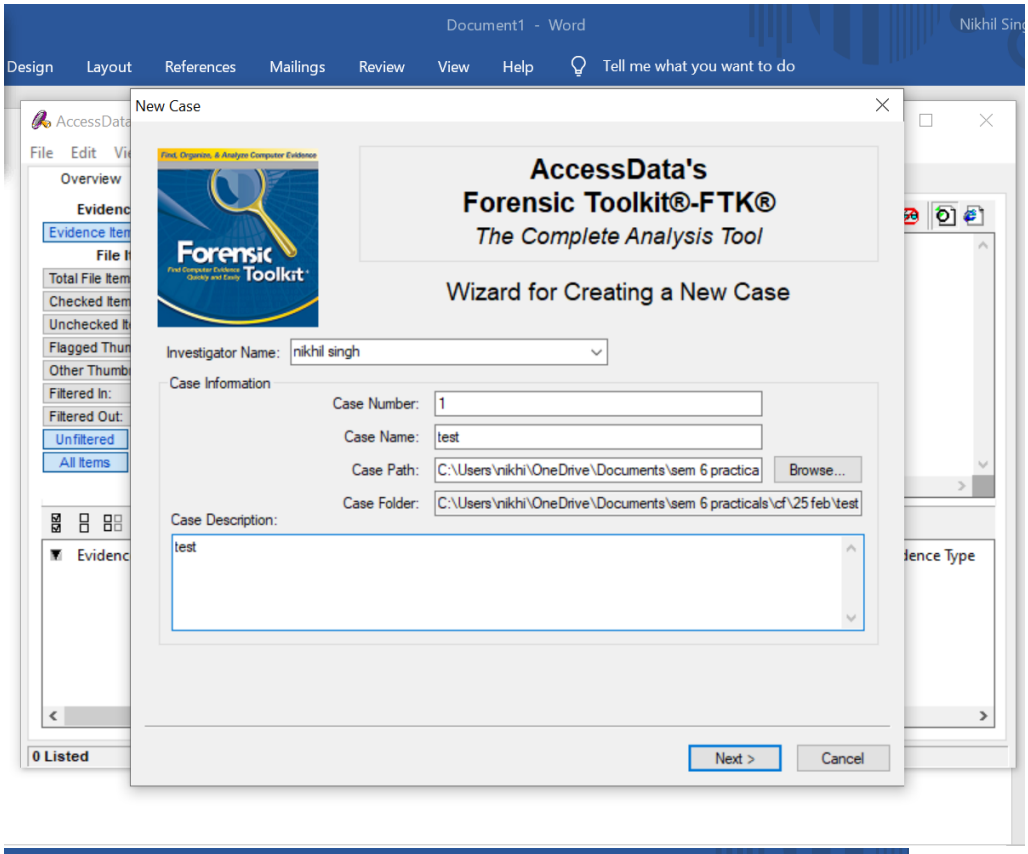
Practical 9

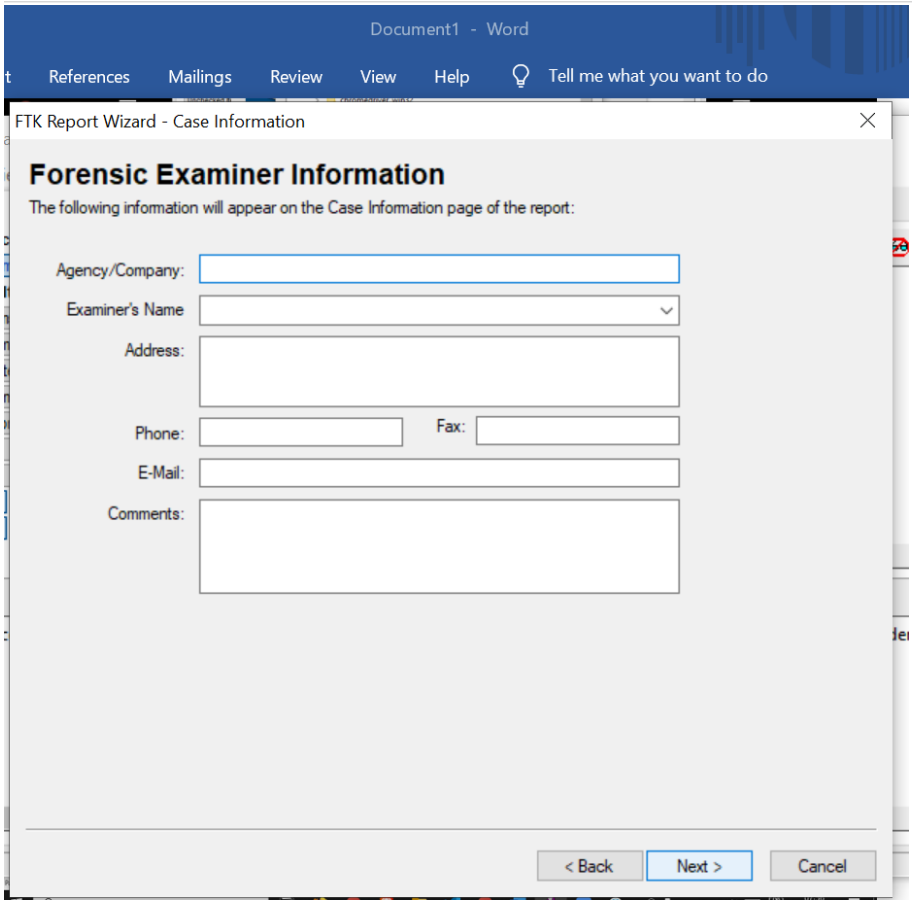
Aim: Email Forensics
- Mail Service Providers
- Email protocols
- Recovering emails
- Analyzing email header

click Start a new case, and then click OK.

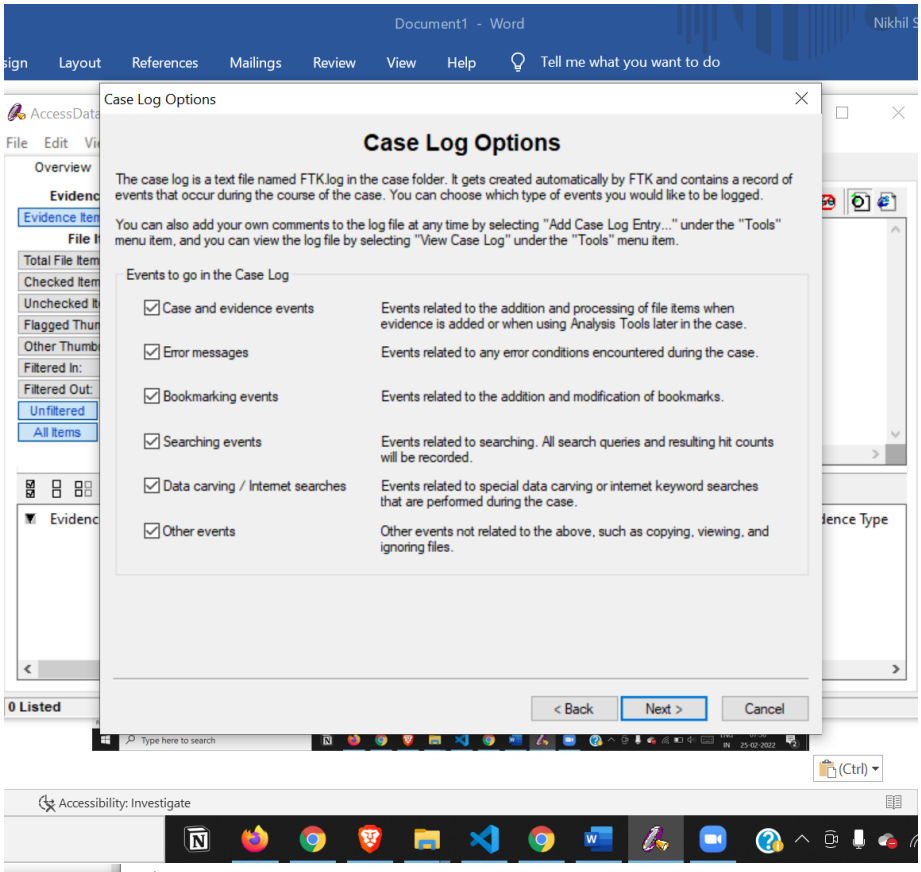


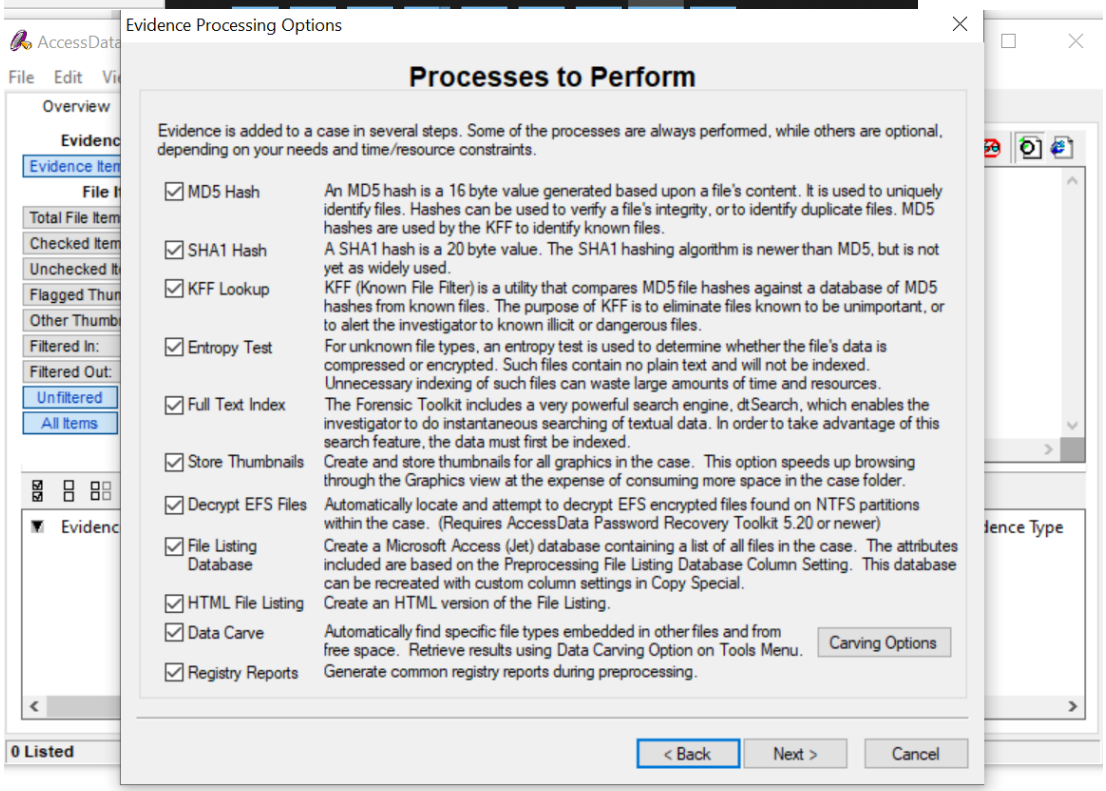
Type case Information and examiner information



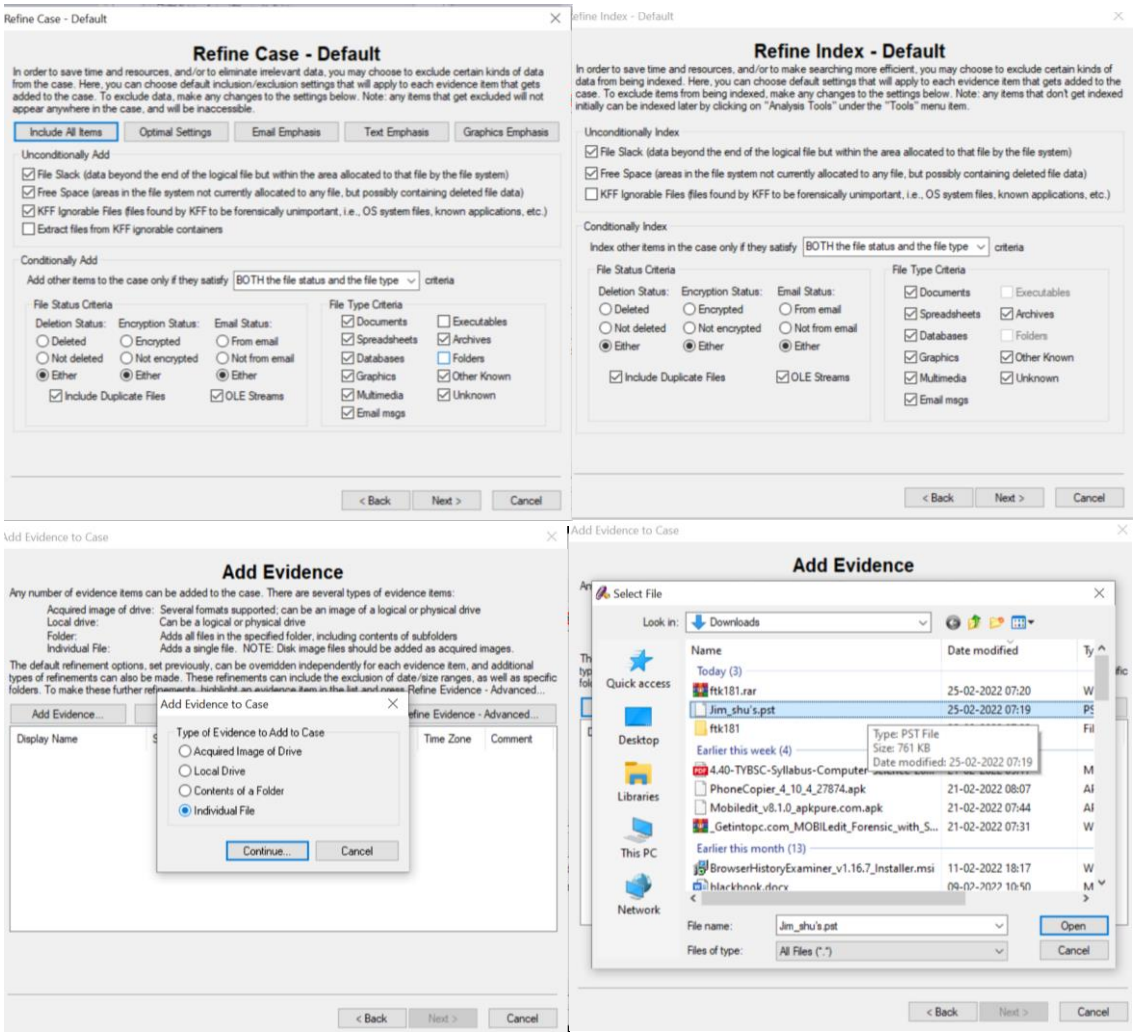


Select case log options and all processes to perform

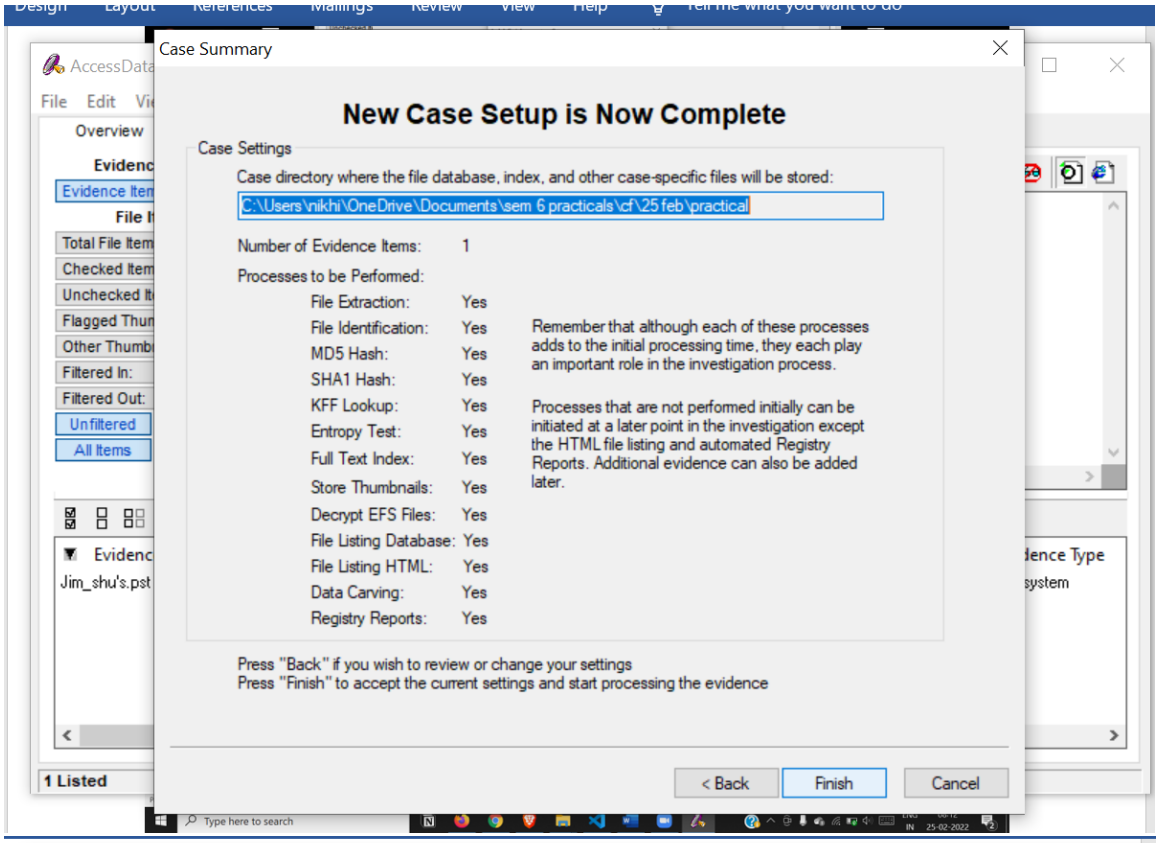


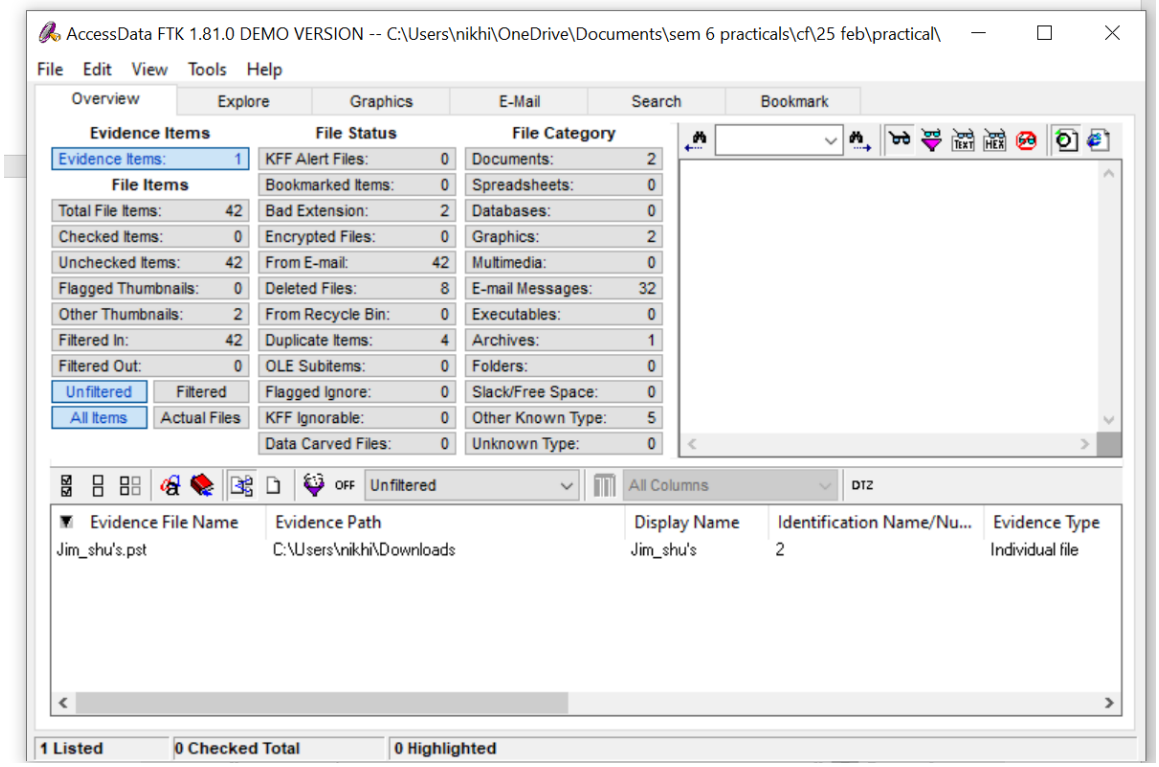


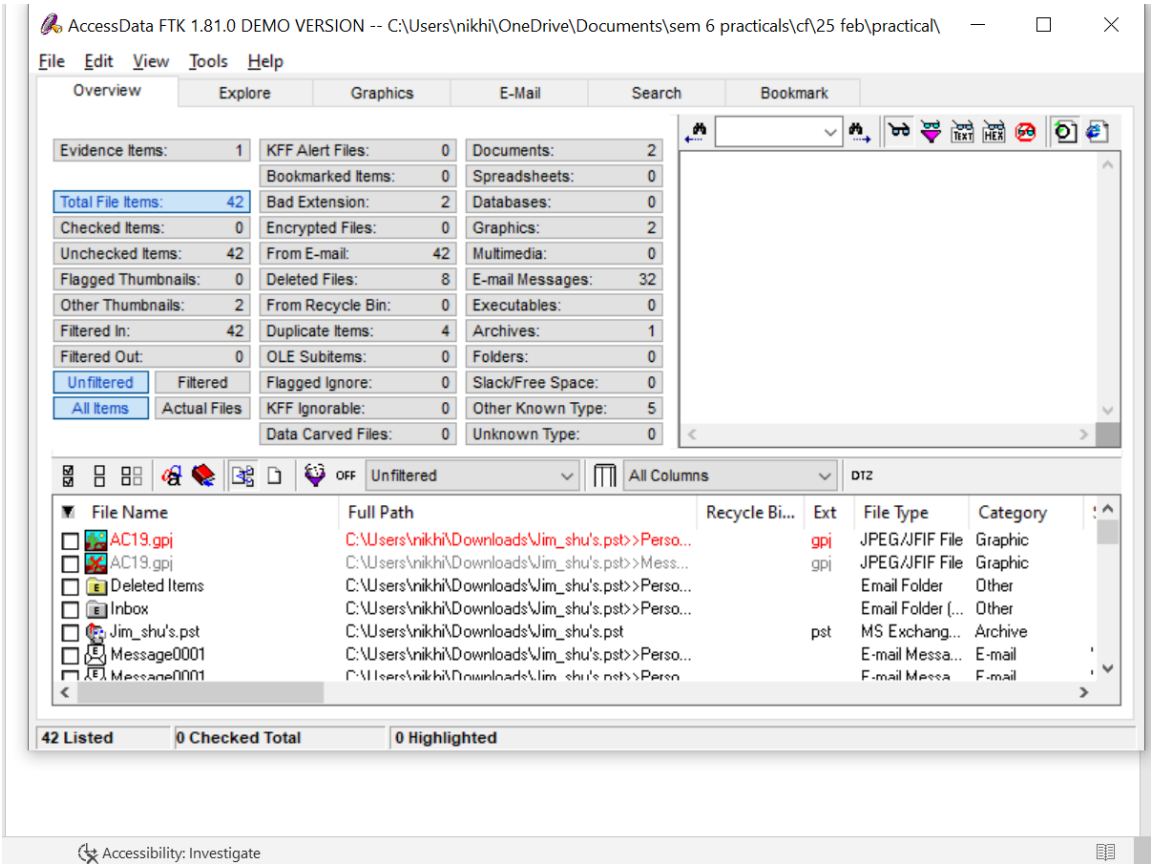
Select these options and add evidence information

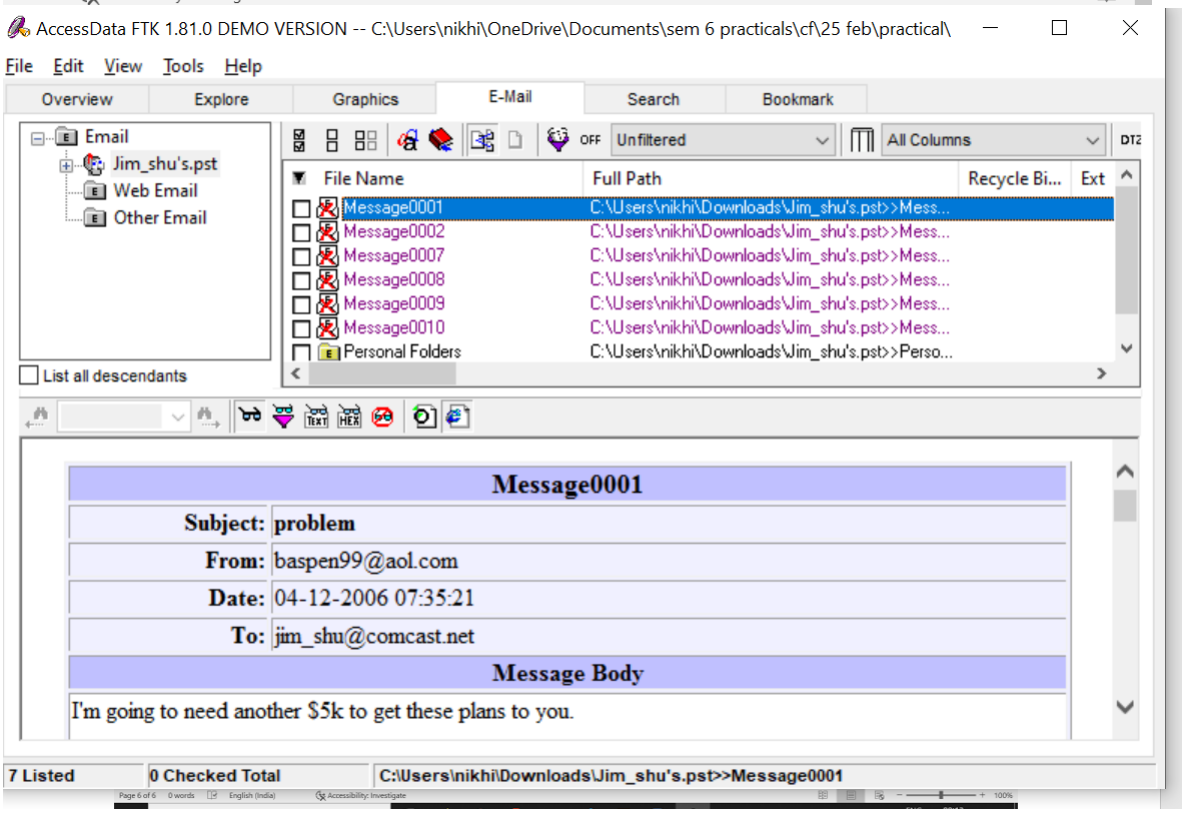


New case setup is complete

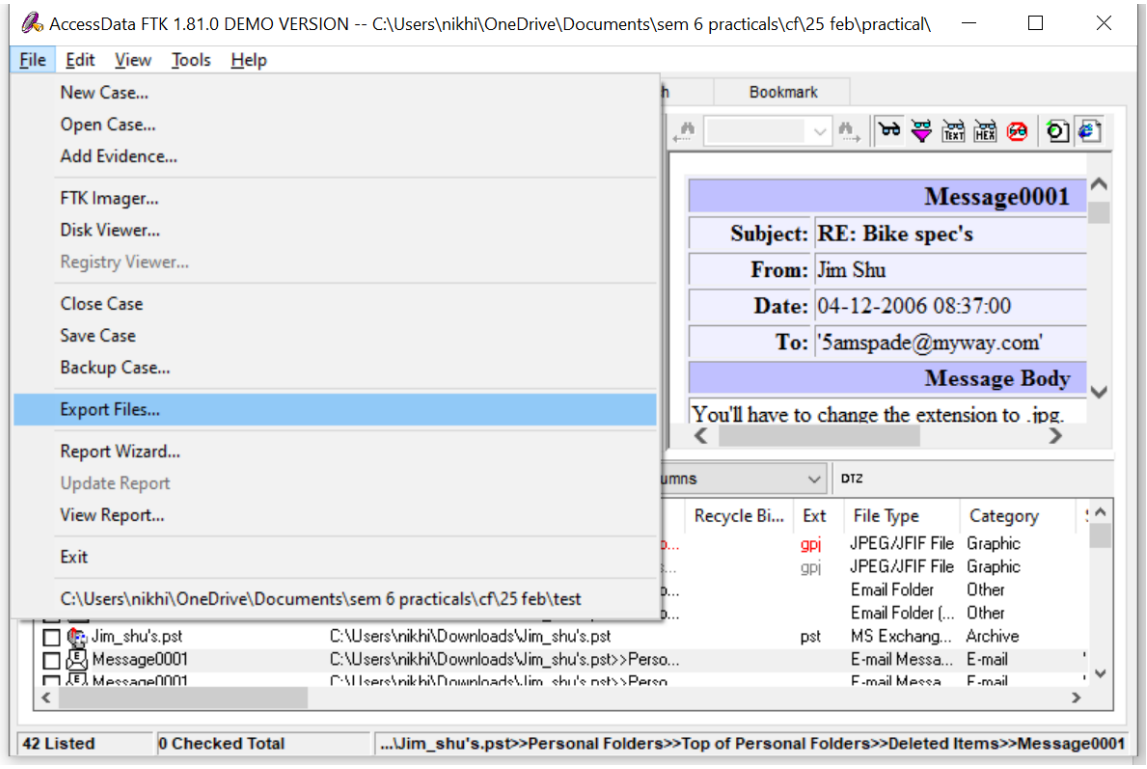






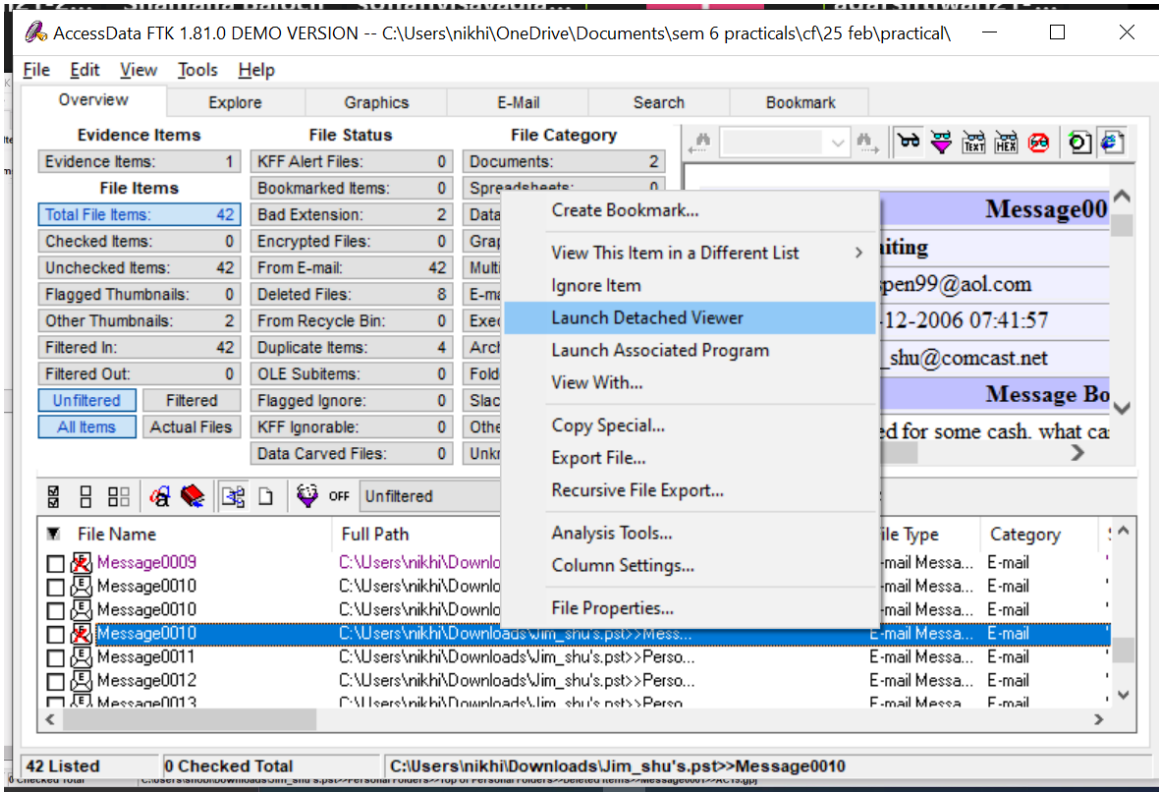


Export case information

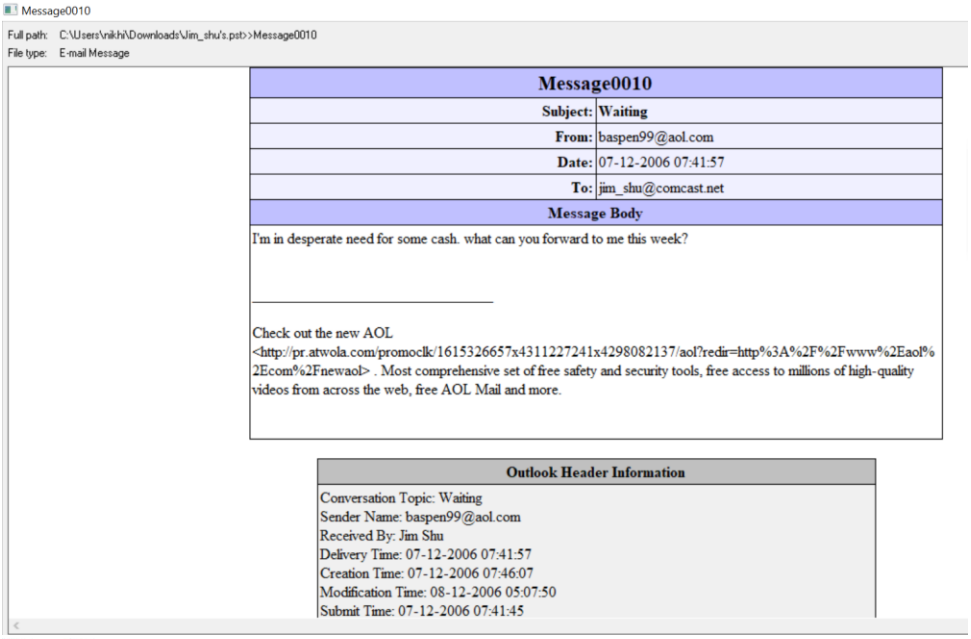

AccessData FTK 1.81.0 DEMO VERSION -- C:\Users\nikhi\OneDrive\Documents\sem 6 practicals\cf\25 feb\practical\
File Edit View Tools Help
New Case...
Open Case...
Add Evidence...
FTK Imager...
Disk Viewer...
Registry Viewer...
Close Case
Save Case
Backup Case...
Export Files...
Report Wizard...
Update Report
View Report...
Exit
C:\Users\nikhi\OneDrive\Documents\sem 6 practicals\cf\25 feb\test
Bookmark
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.
Recycle Bi... Ext File Type Category
gpj JPEG/JFIF File Graphic
Email Folder Other
Email Folder (... Other
Jim_shu's.pst C:\Users\nikhi\Downloads\Jim_shu's.pst pst MS Exchang... Archive
Message0001 C:\Users\nikhi\Downloads\Jim_shu's.pst>>Perso... E-mail Messa... E-mail
42 Listed
0 Checked Total
...\Jim_shu's.pst>>Personal Folders>>Top of Personal Folders>>Deleted Items>>Message0001

Part2

Launch detached information



View message headers and body


Message0010

Full path: C:\Users\nikhi\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

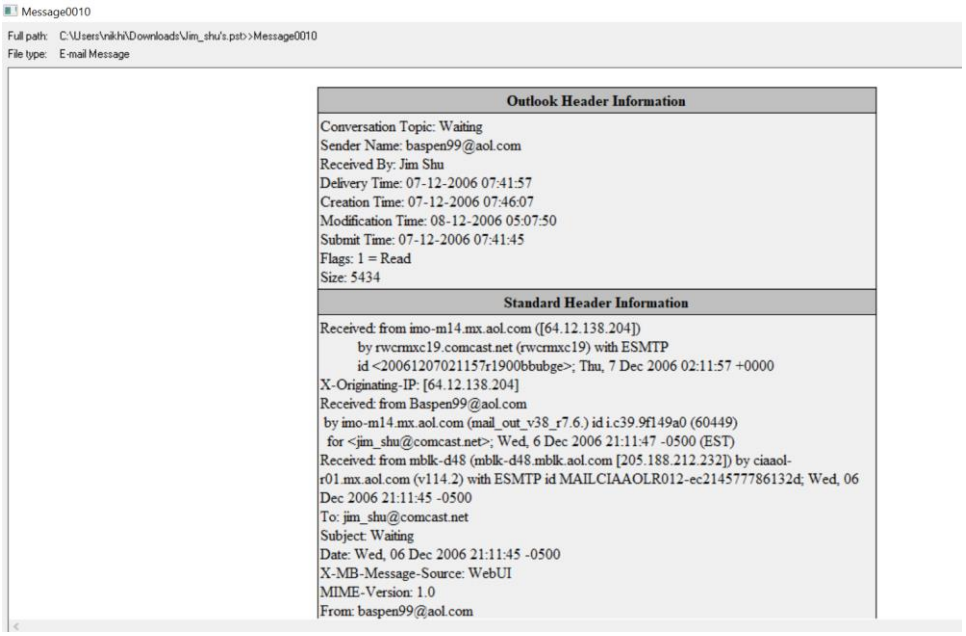
Message Body

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/promoclk/1615326657x4311227241x4298082137/aol?redir=http%3A%2F%2Fwww%2Eaol%2Ecom%2Fnewaol> . 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

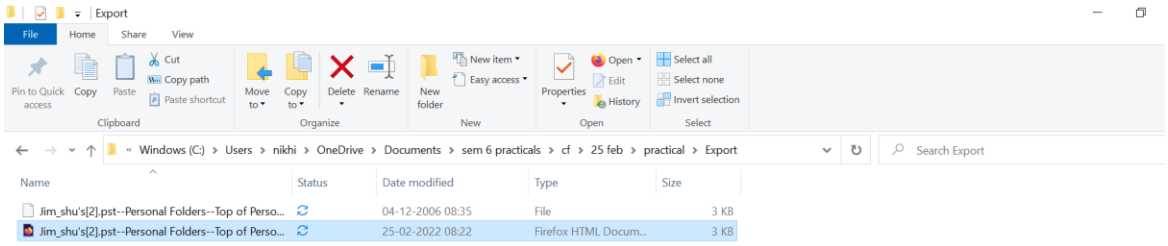
Full path: C:\Users\nikhi\Downloads\Jim_shu's.pst>>Message0010
File type: E-mail Message

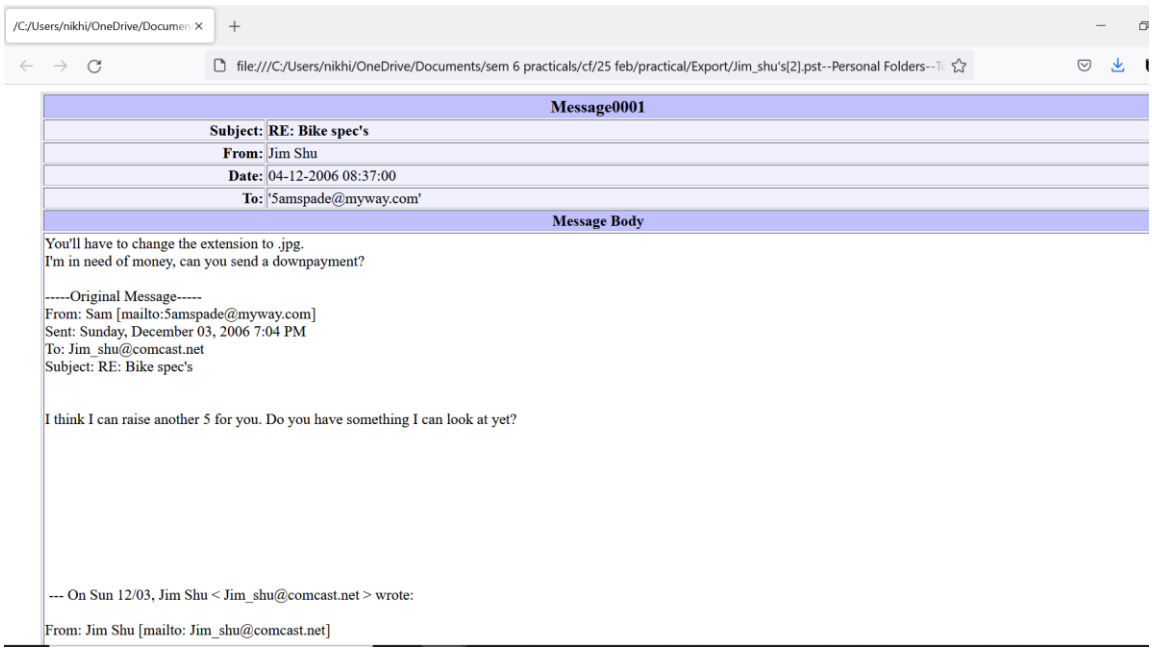
Outlook Header Information

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 rwcrmxc19.comcast.net (rwcrmxc19) 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 i.c39.9f149a0 (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 ciaaol-r01.mx.aol.com (v114.2) with ESMTP id MAILCIAAOLR012-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


Export
File
Home
Share
View
Cut
Copy path
Paste shortcut
Pin to Quick access
Copy
Paste
Move to
Copy to
Delete
Rename
New folder
New item
Easy access
Properties
Open
Edit
History
Select all
Select none
Invert selection
Clipboard
Organize
New
Open
Select
Windows (C:) › Users › nikhi › OneDrive › Documents › sem 6 practicals › cf › 25 feb › practical › Export
Search Export
Name
Status
Date modified
Type
Size
Jim_shu's[2].pst--Personal Folders--Top of Perso...
04-12-2006 08:35
File
3 KB
Jim_shu's[2].pst--Personal Folders--Top of Perso...
25-02-2022 08:22
Firefox HTML Docum...
3 KB

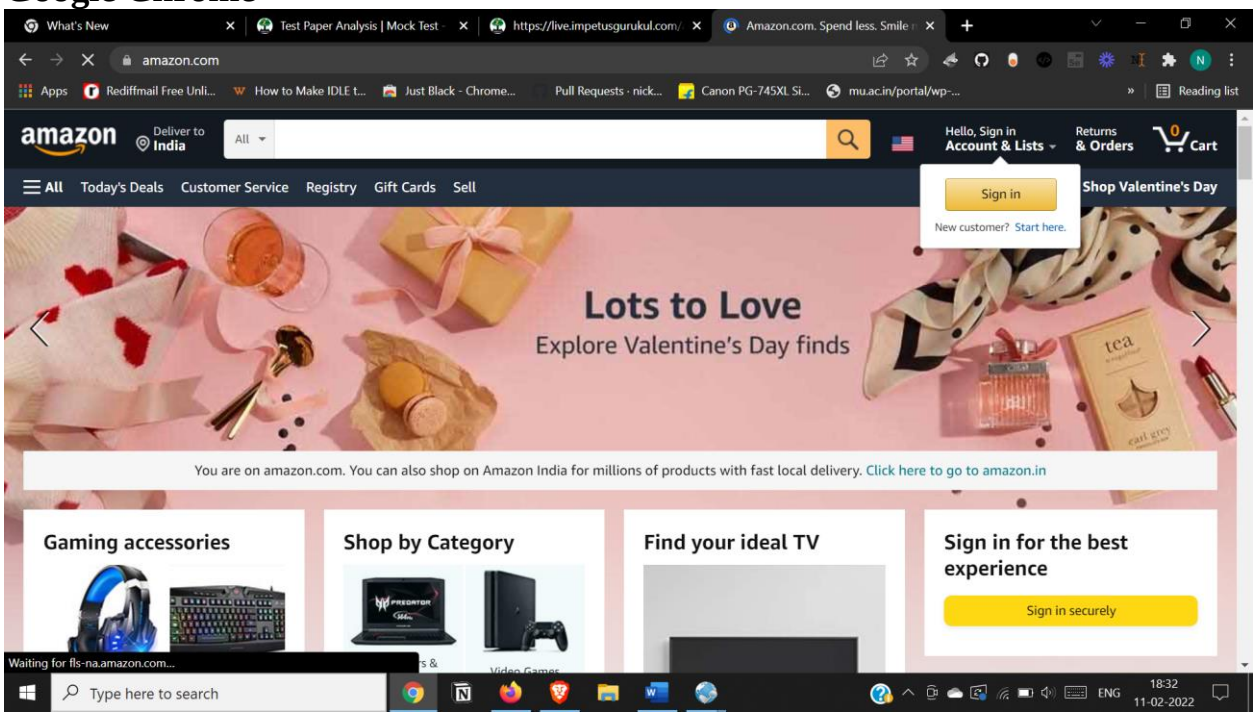

/C:/Users/nikhi/OneDrive/Documen
file:///C:/Users/nikhi/OneDrive/Documents/sem 6 practicals/cf/25 feb/practical/Export/Jim_shu's[2].pst--Personal Folders--
Message0001
Subject: RE: Bike spec's
From: Jim Shu
Date: 04-12-2006 08:37:00
To: '5amspade@myway.com'
Message Body
You'll have to change the extension 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

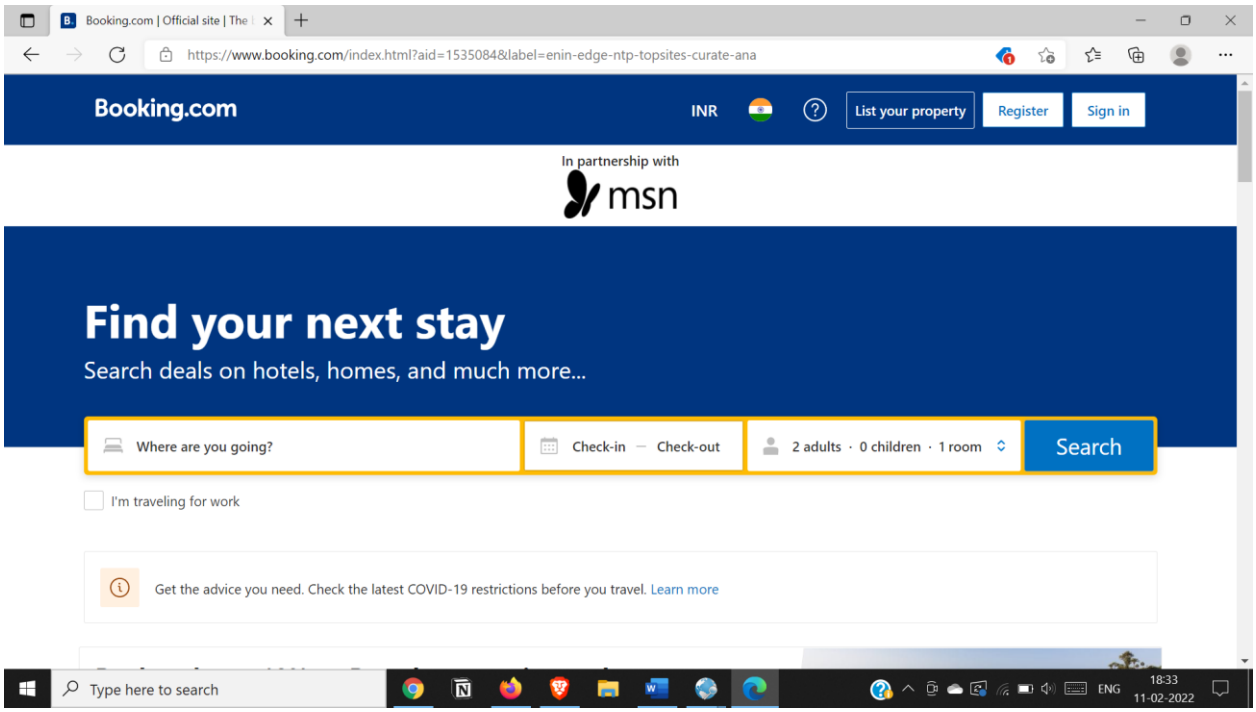
Aim :- Web Browser Forensics

- Web Browser working

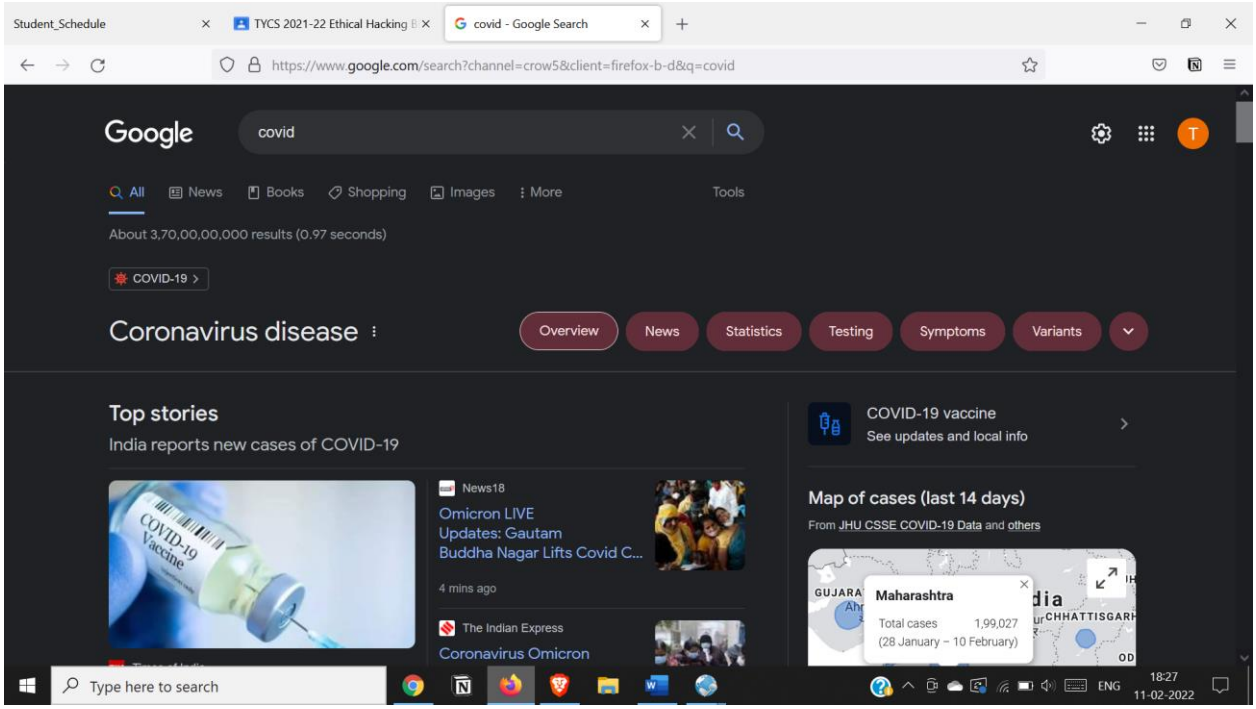
Google Chrome



Microsoft Edge

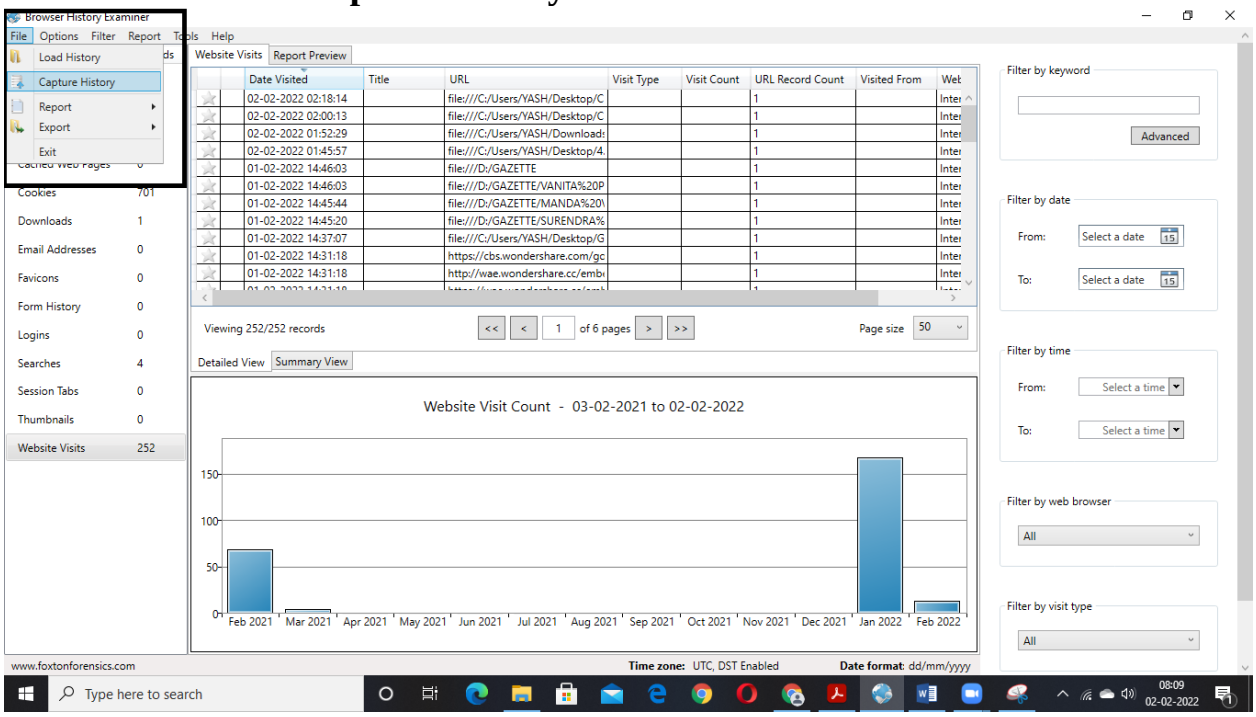


Firefox

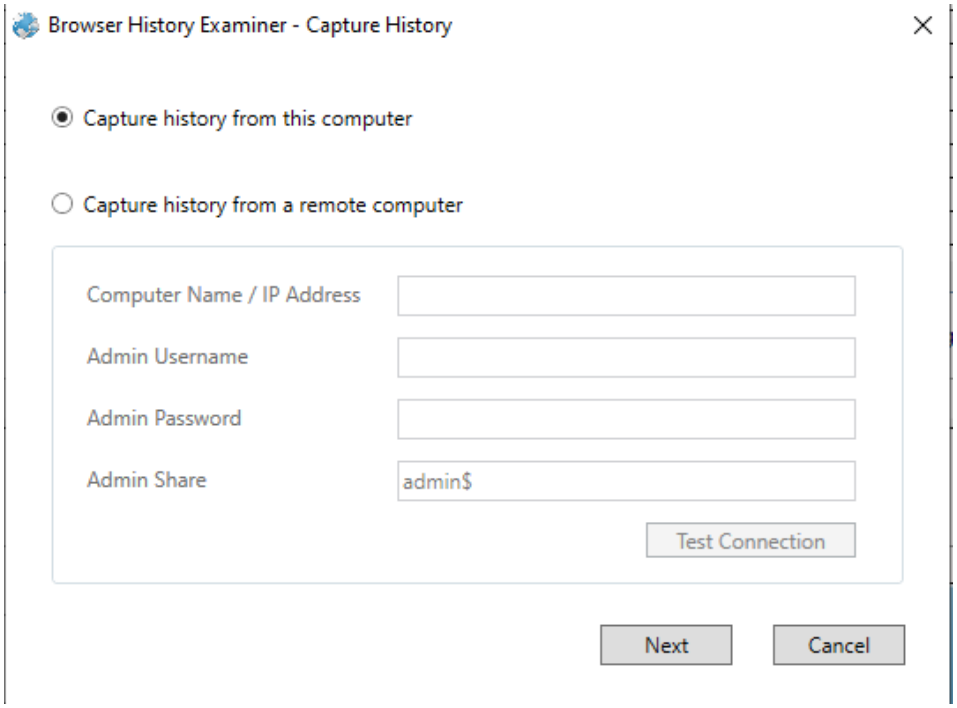


- Forensics activities on browser

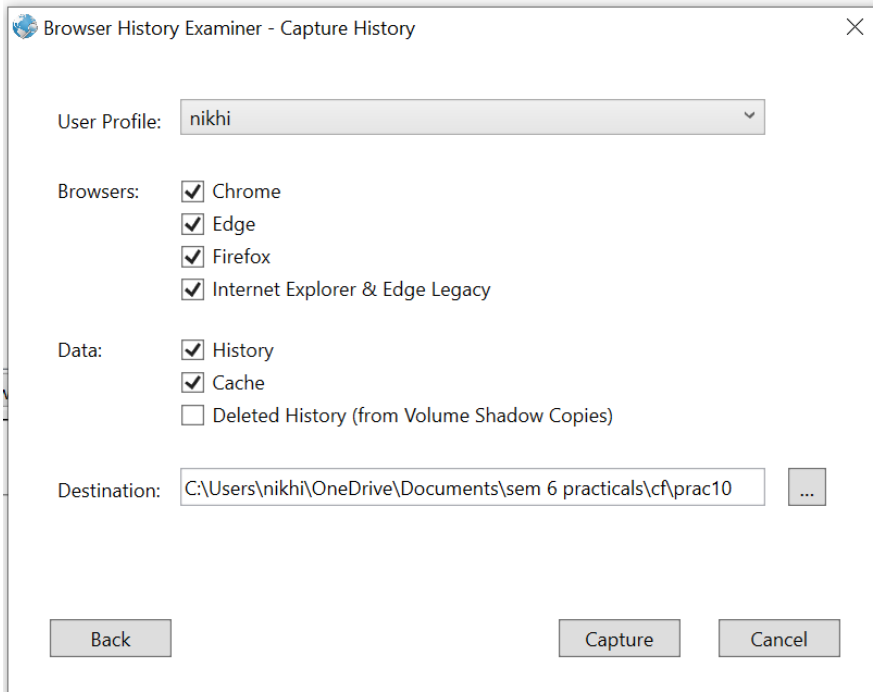
Go to File Menu > Capture History

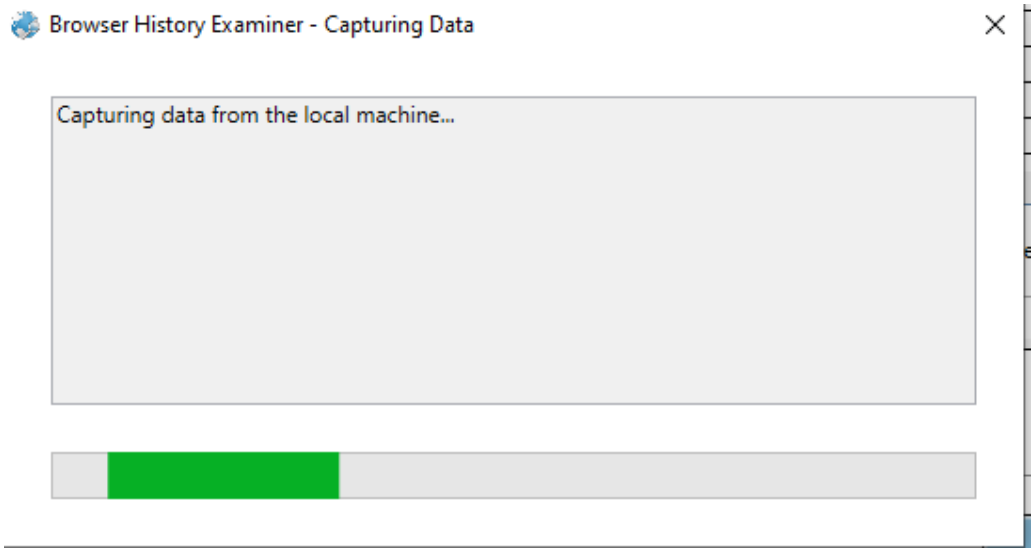


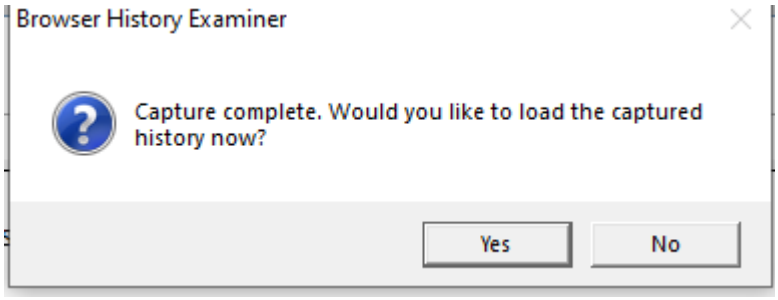
Click Next

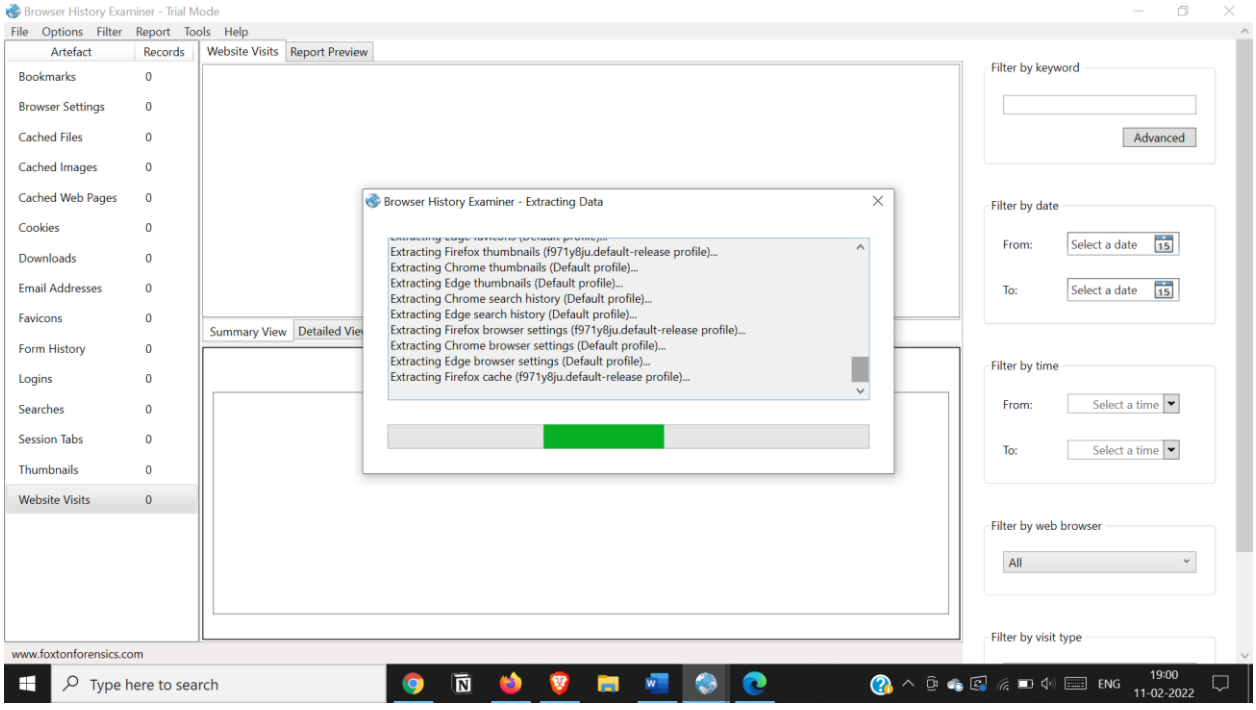


Give the path of folder in which you want to save your captured data and click on capture

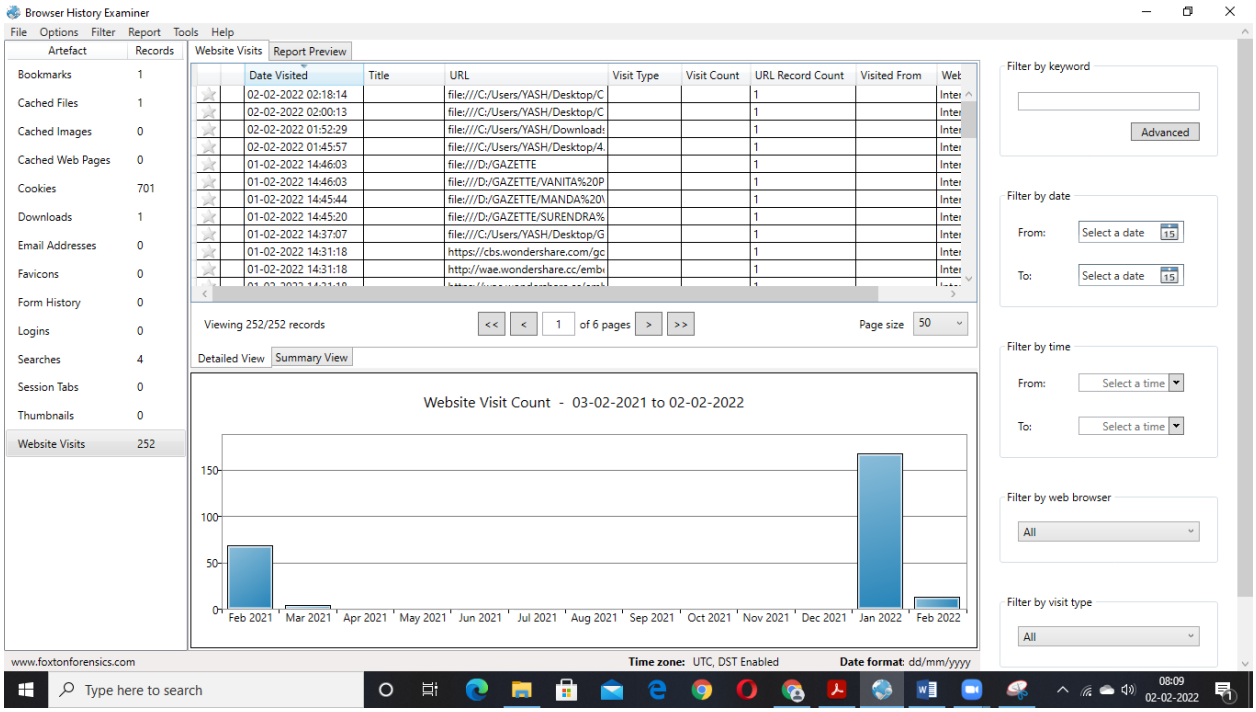




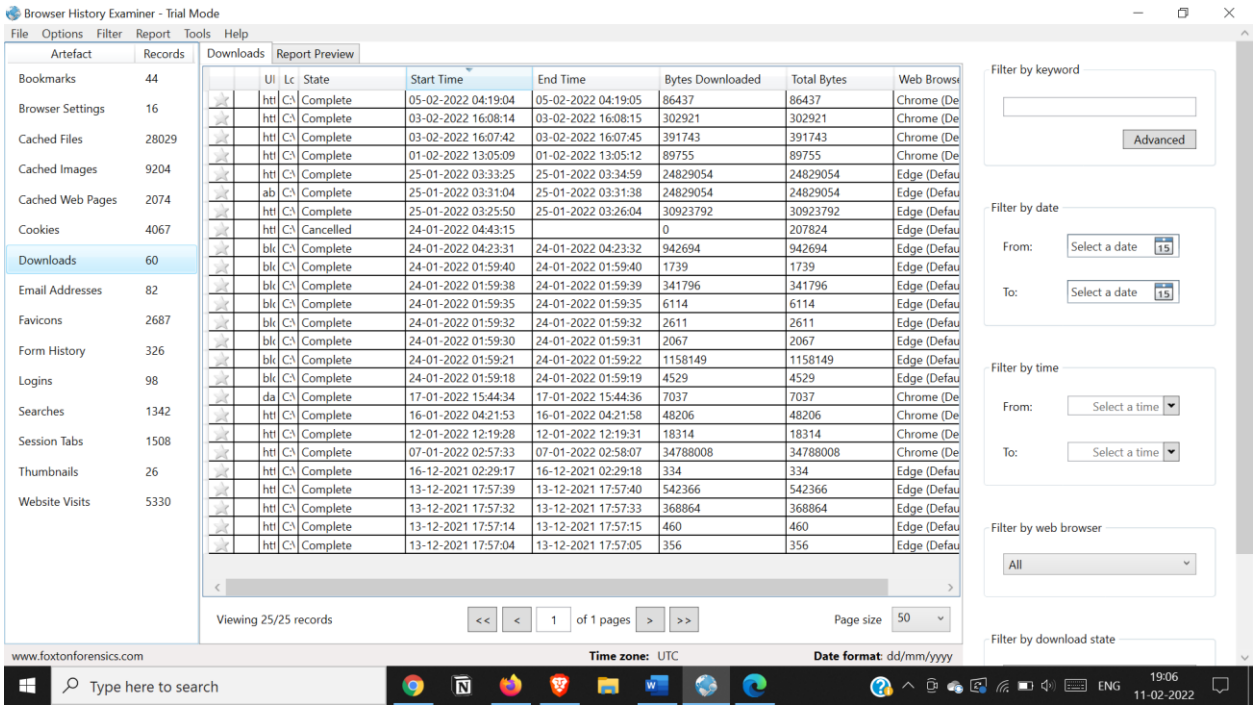




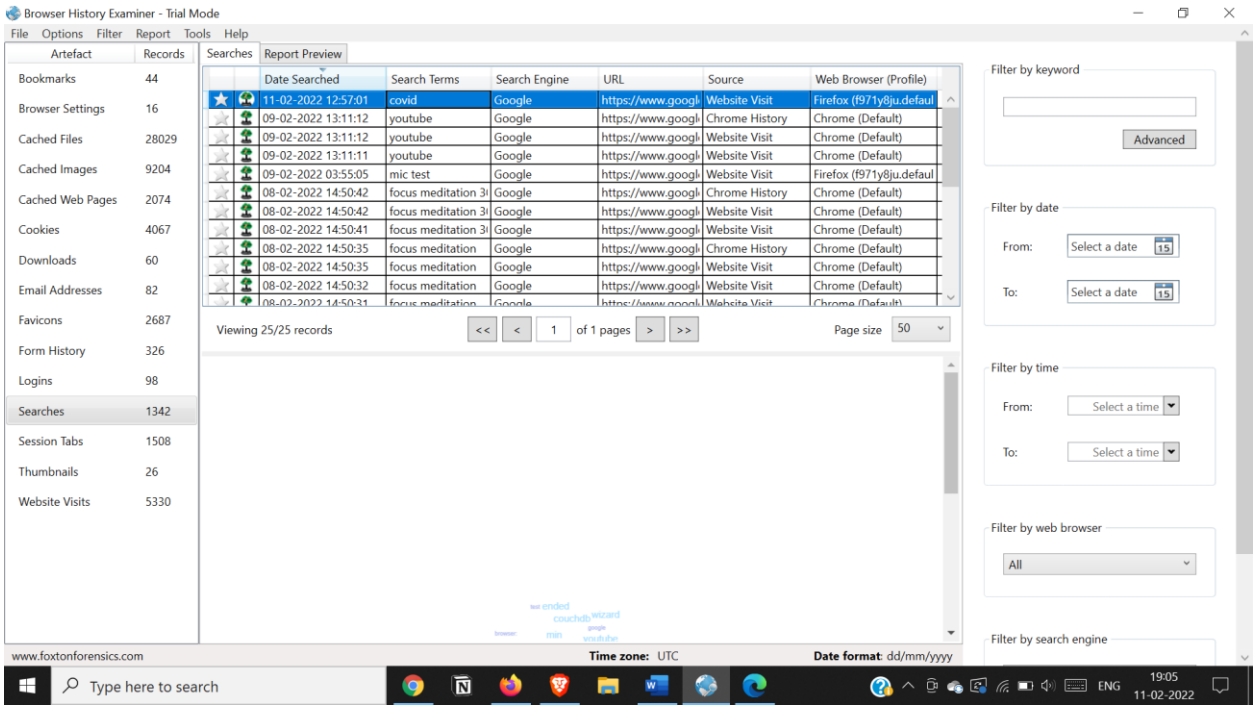
All the captured details are listed below



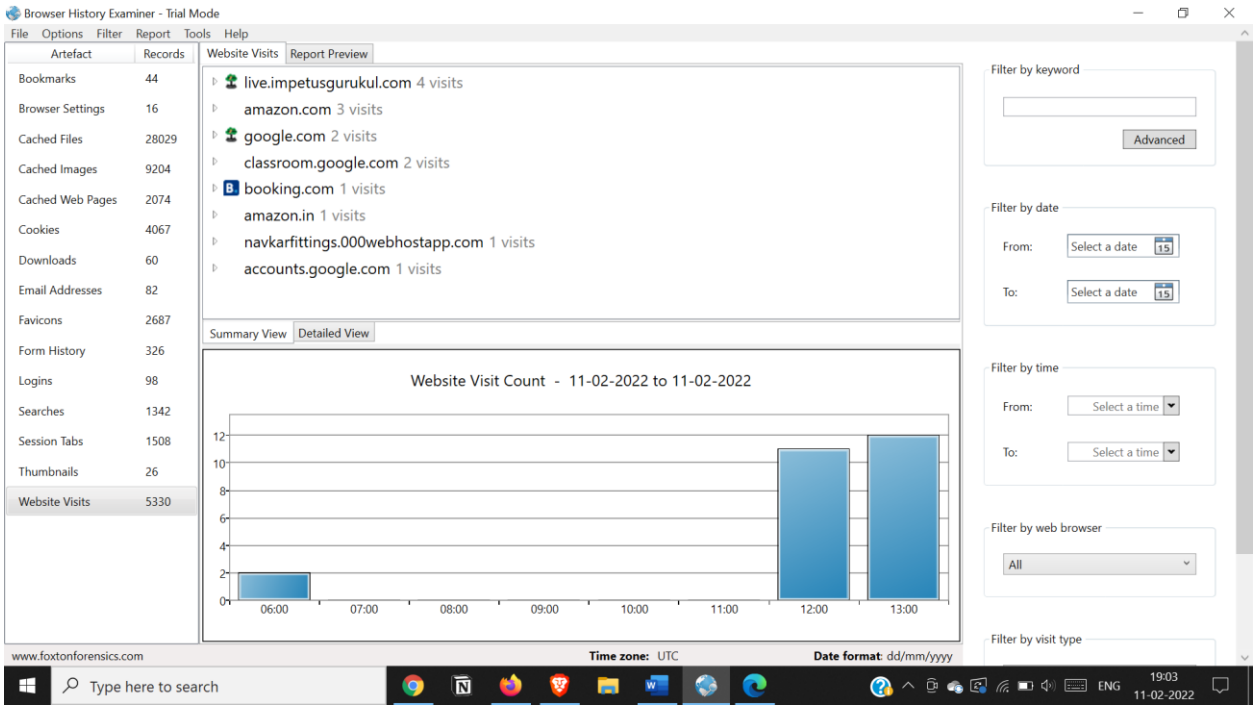
Downloads



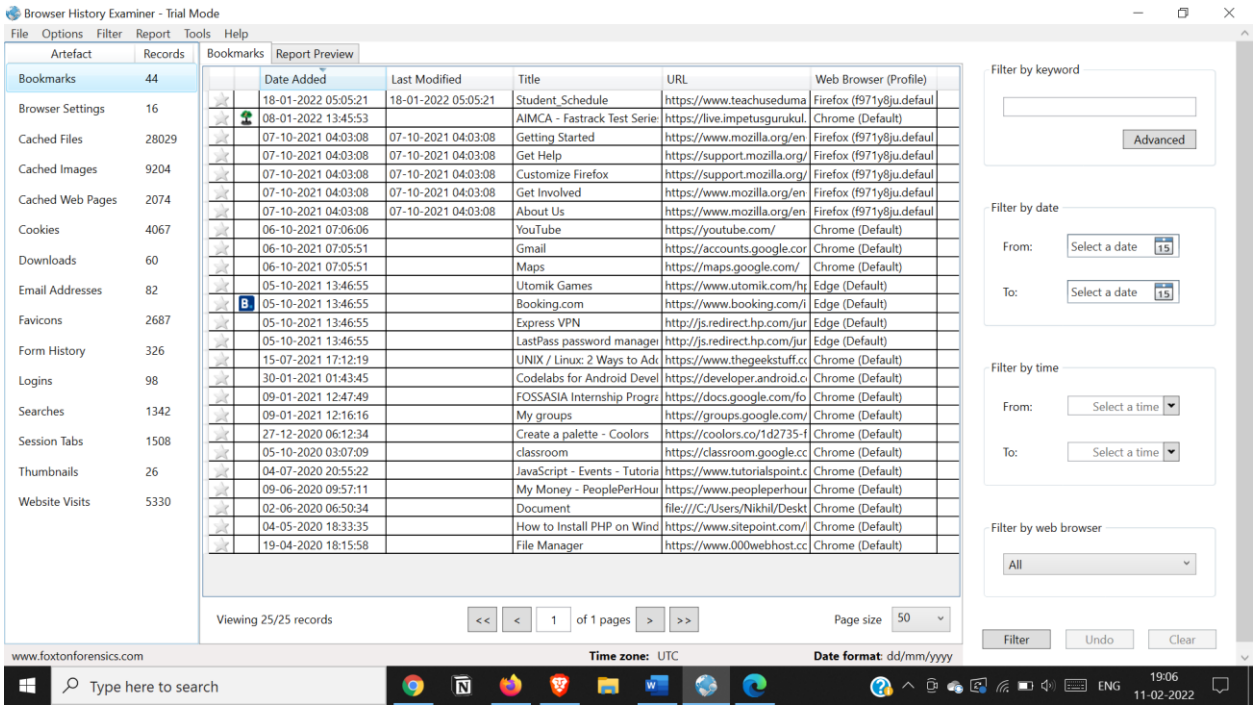
Searches



Website Visits

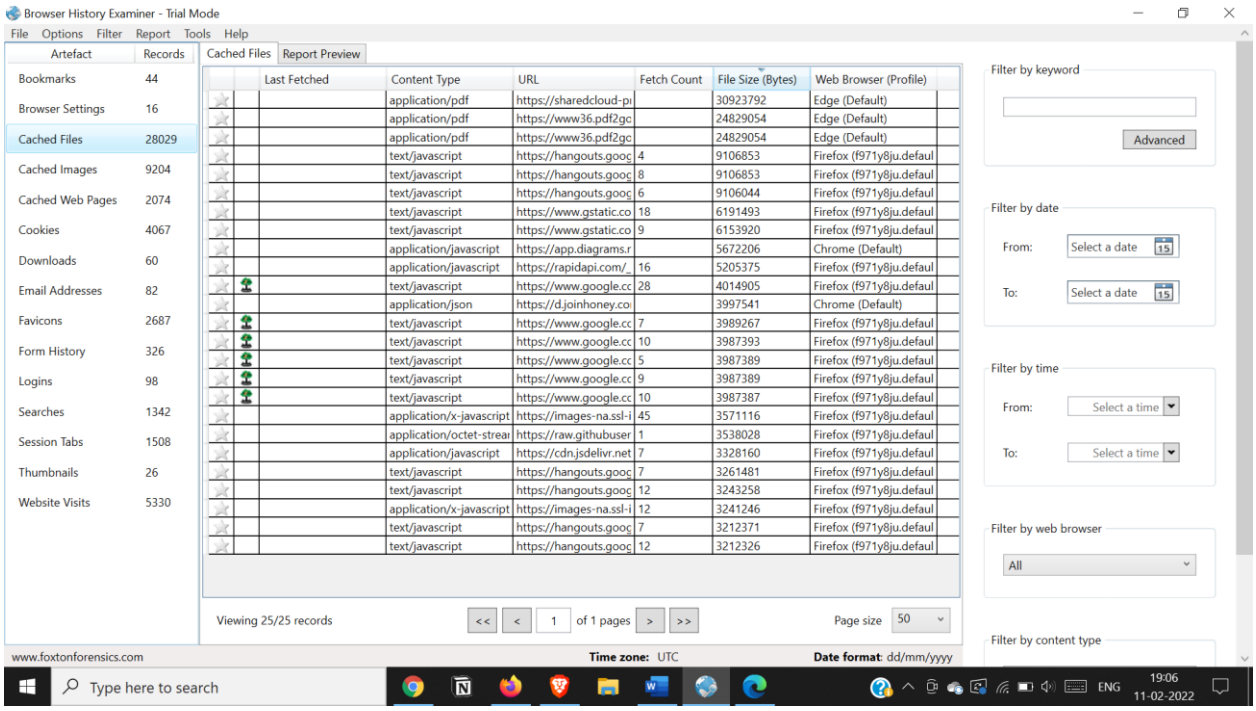


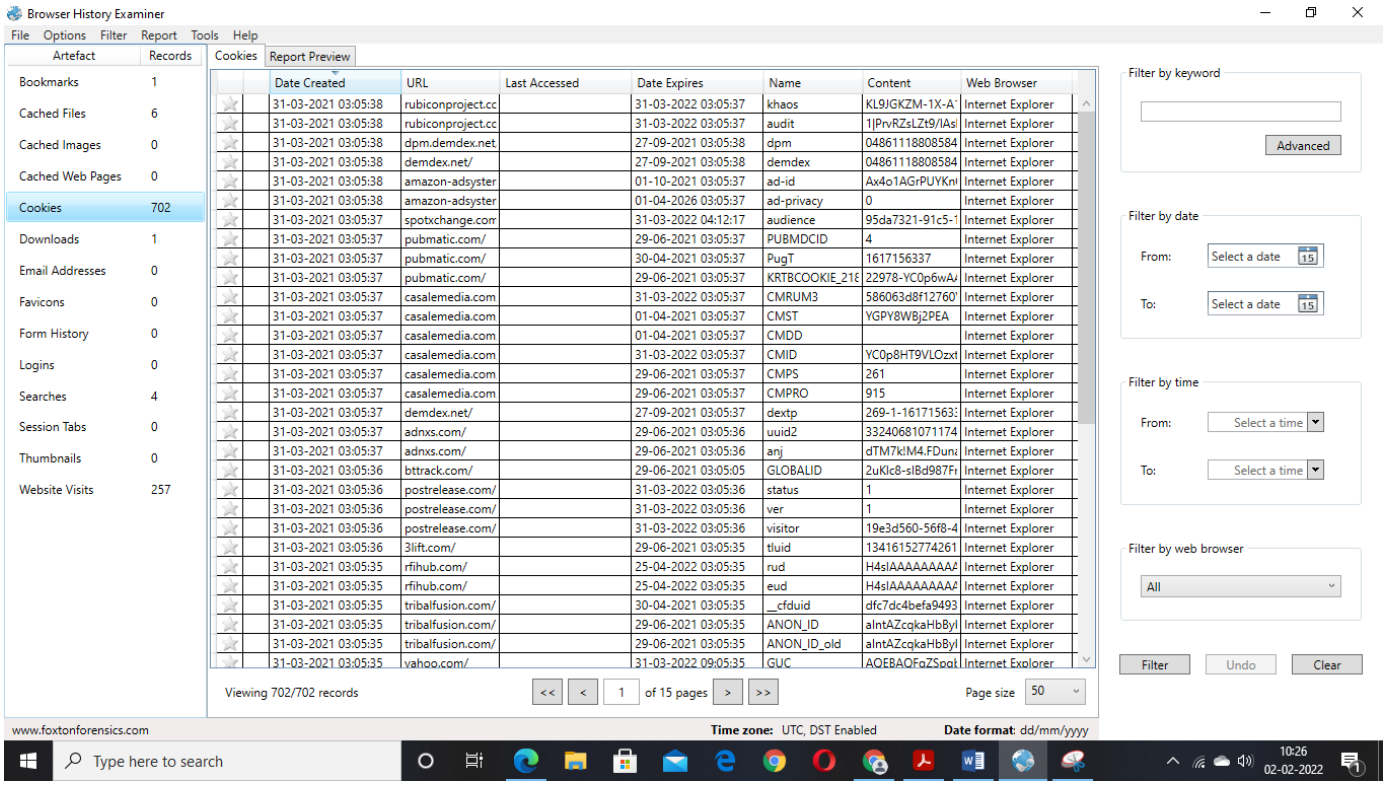
Bookmarks



- Cache / Cookies analysis

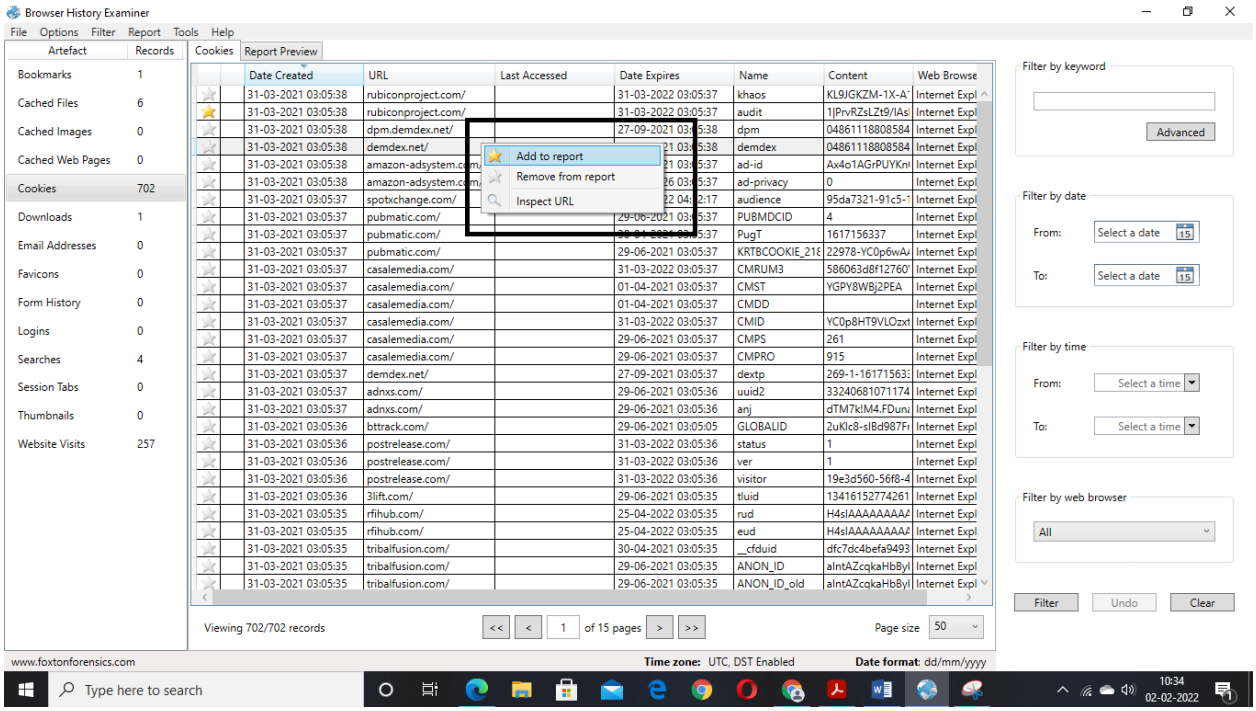
Number of cache files and cookies gets captured

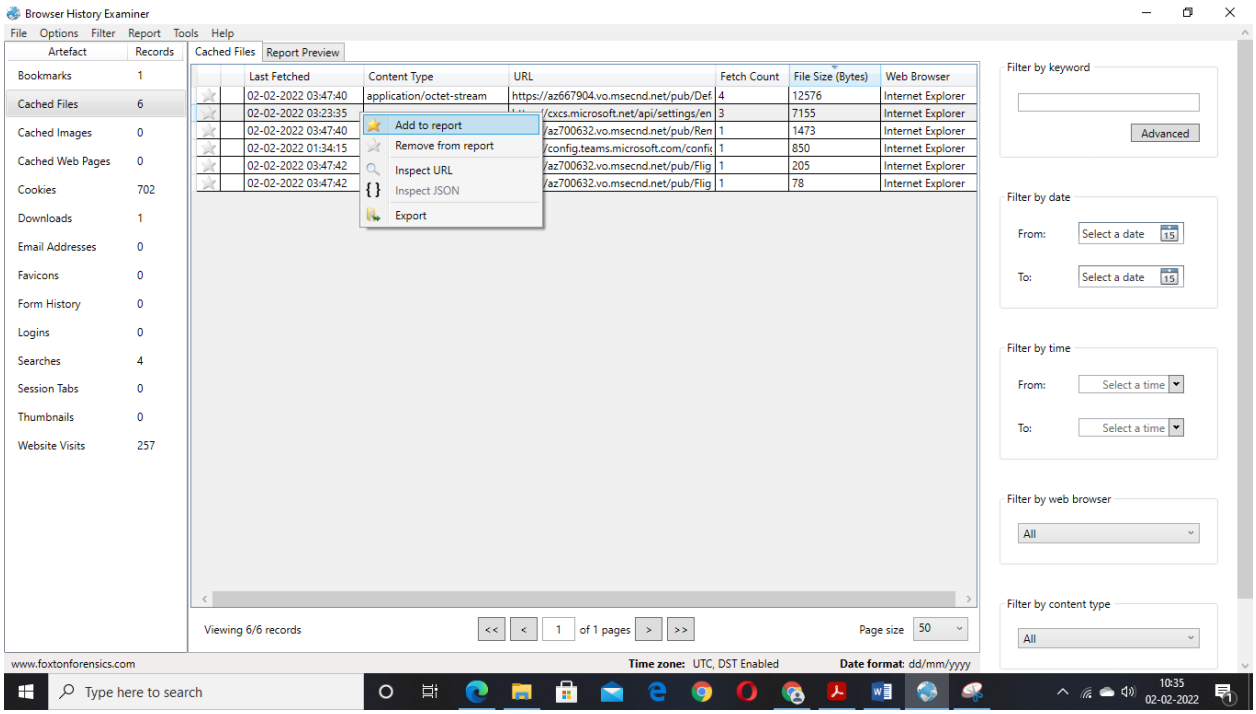




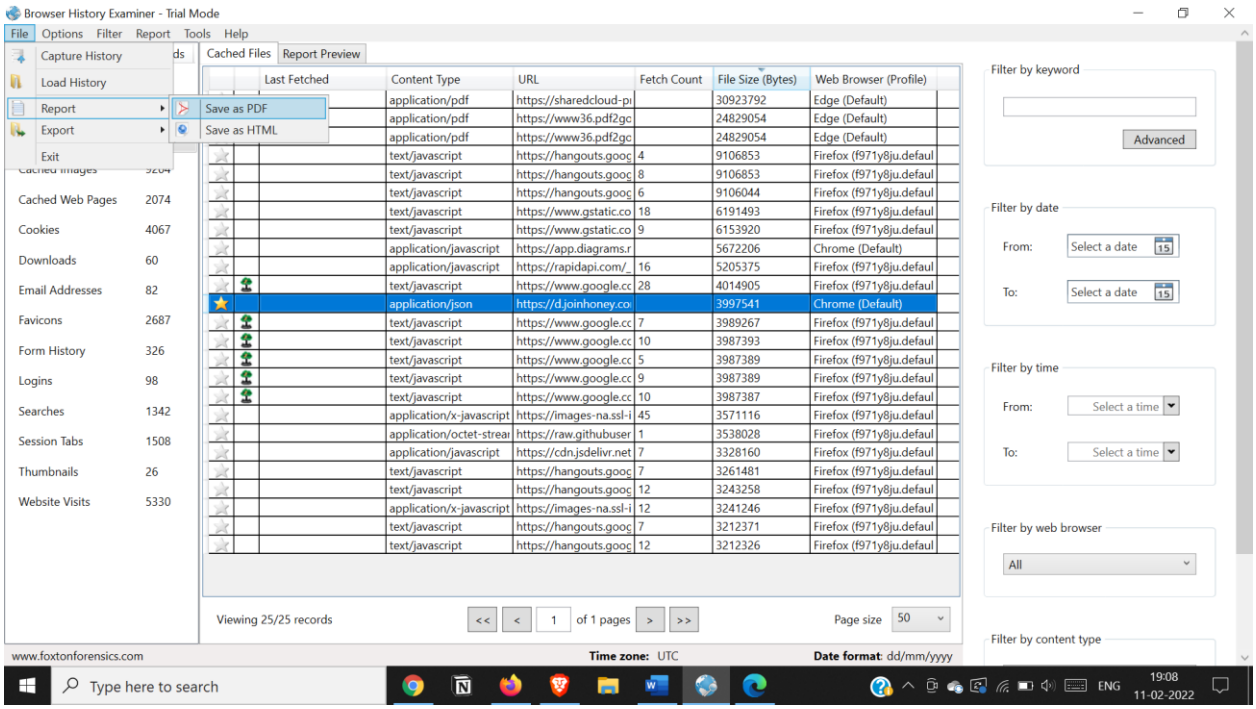
- Last Internet activity

Generating Report
Right Click on the content and click Add to report

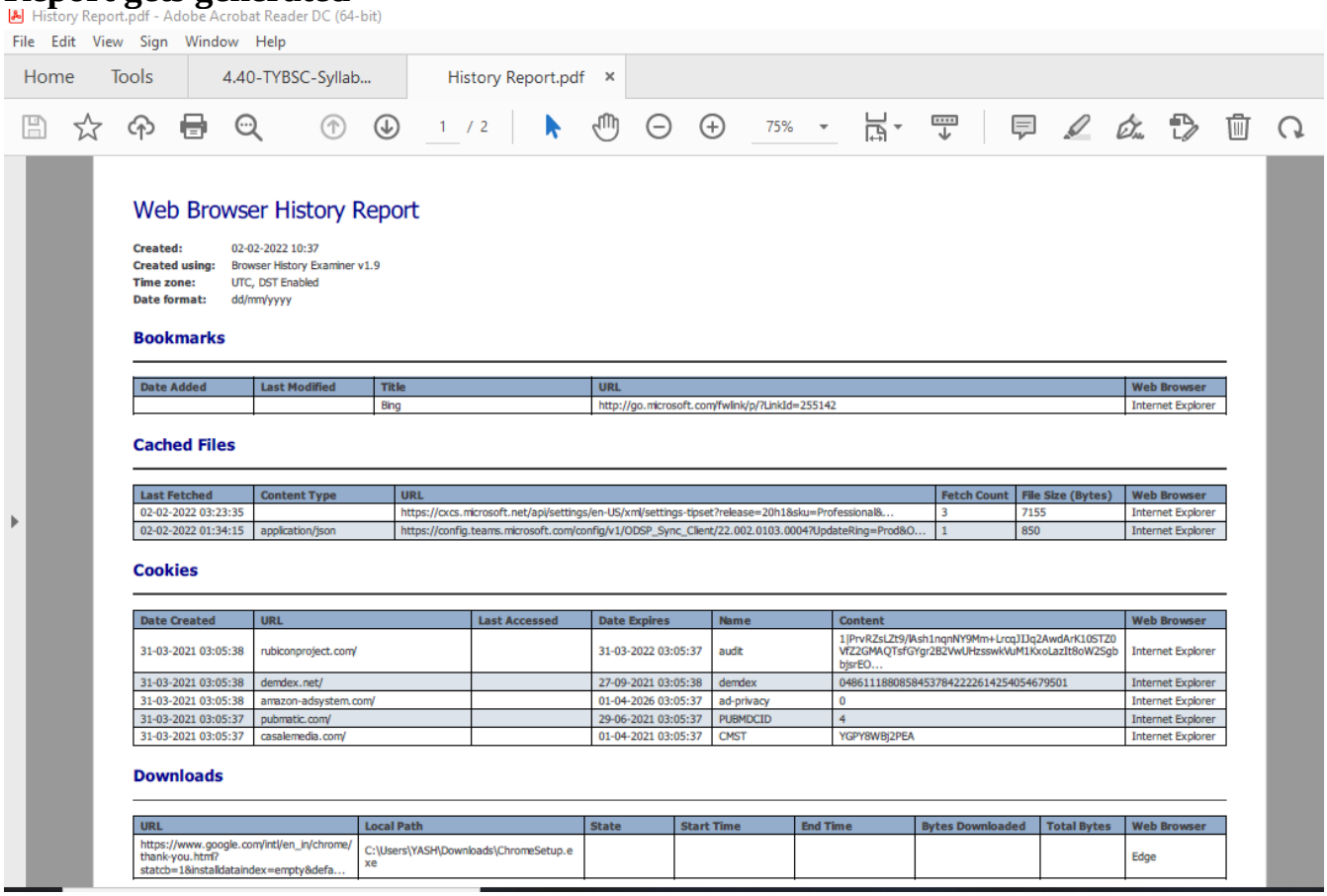




Go to File menu and then Report>Save as PDF

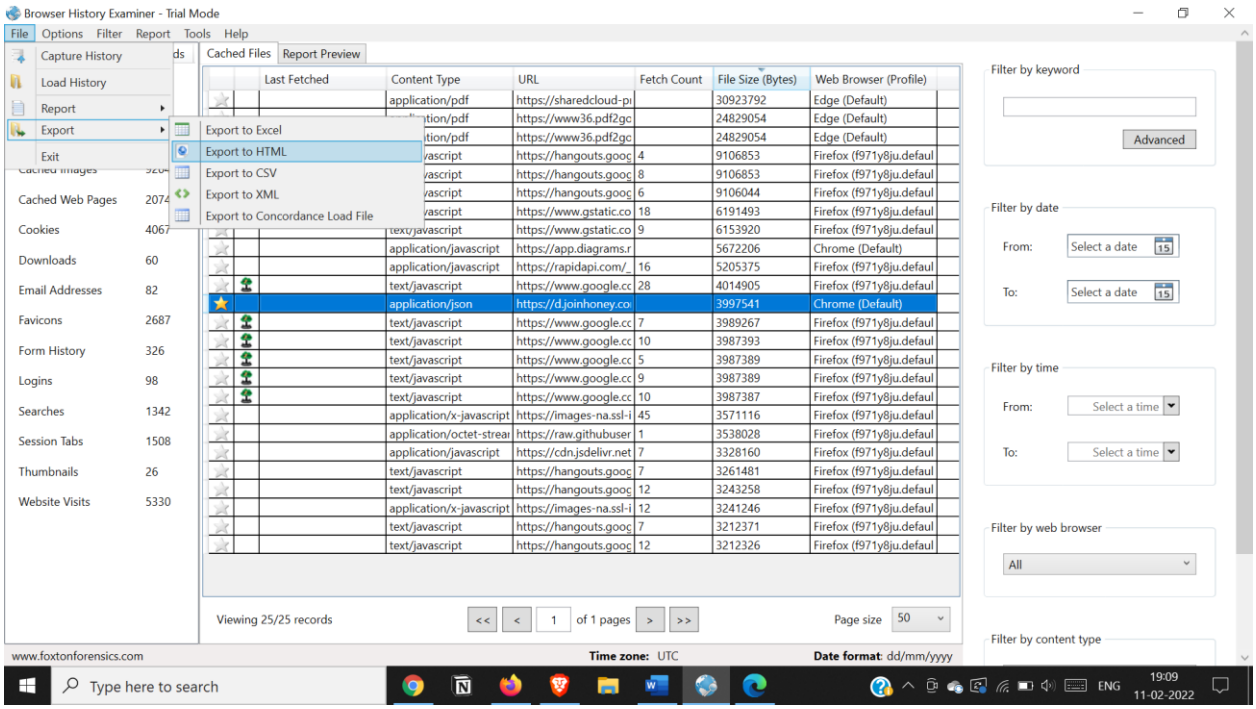


Report gets generated

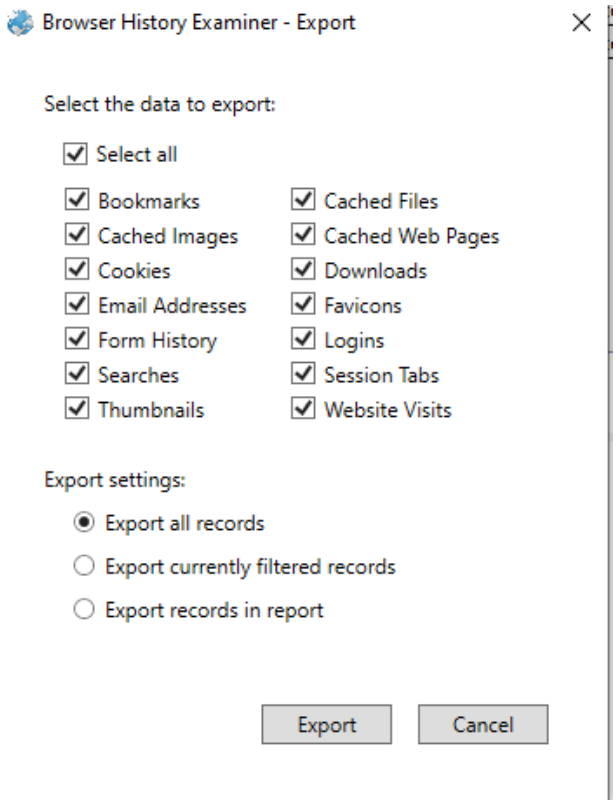


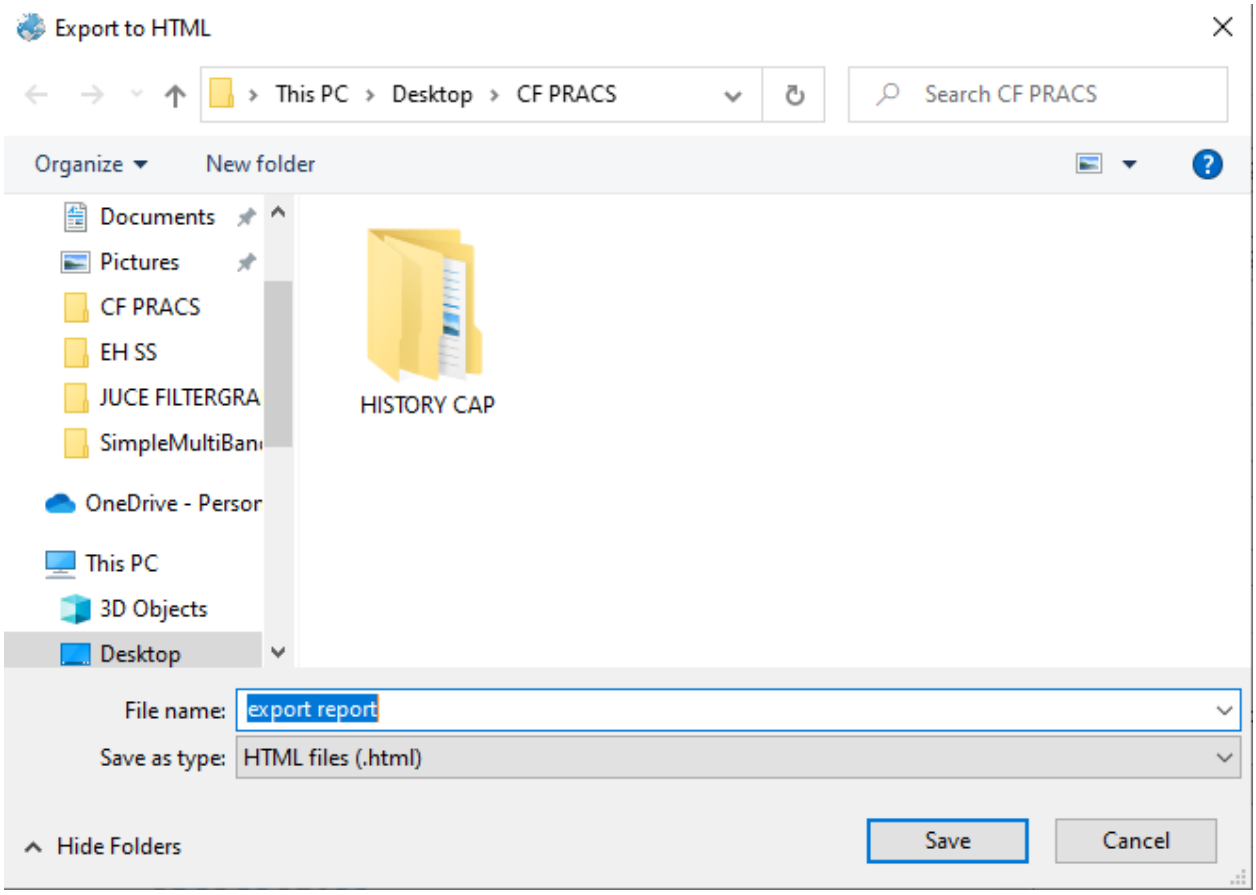
Exporting Report

Go to File Menu Export > Export to Html

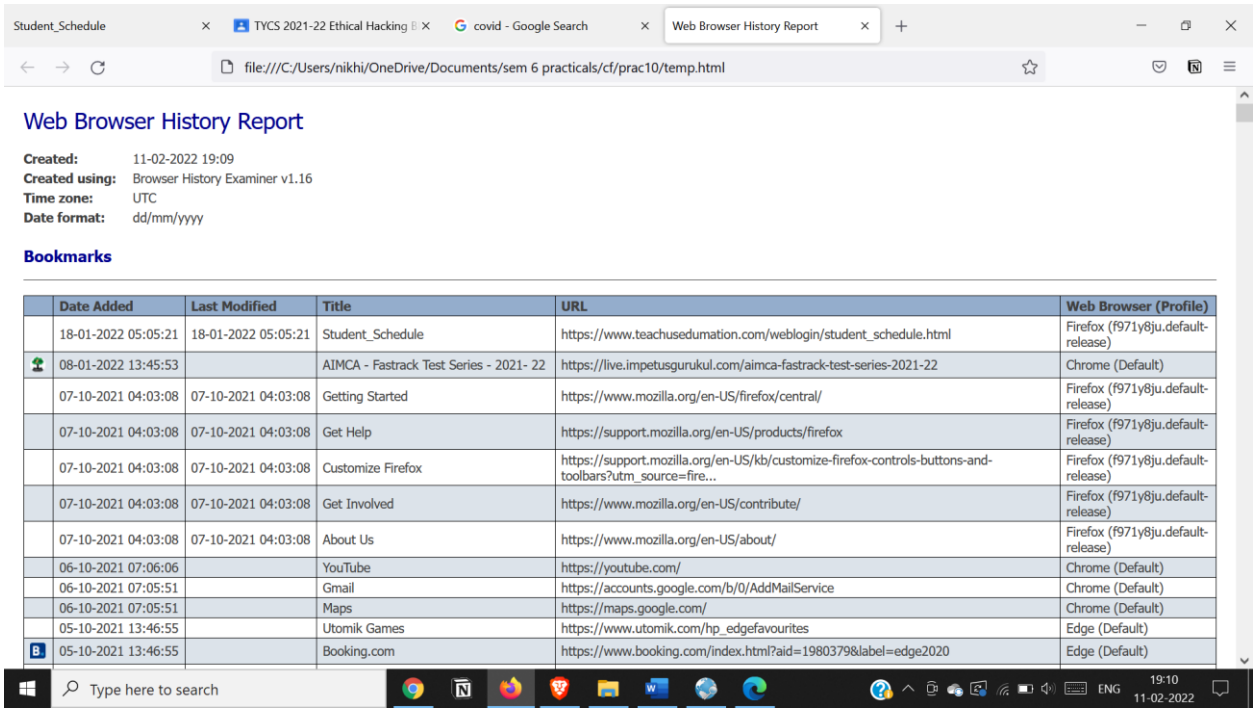


Click on Export

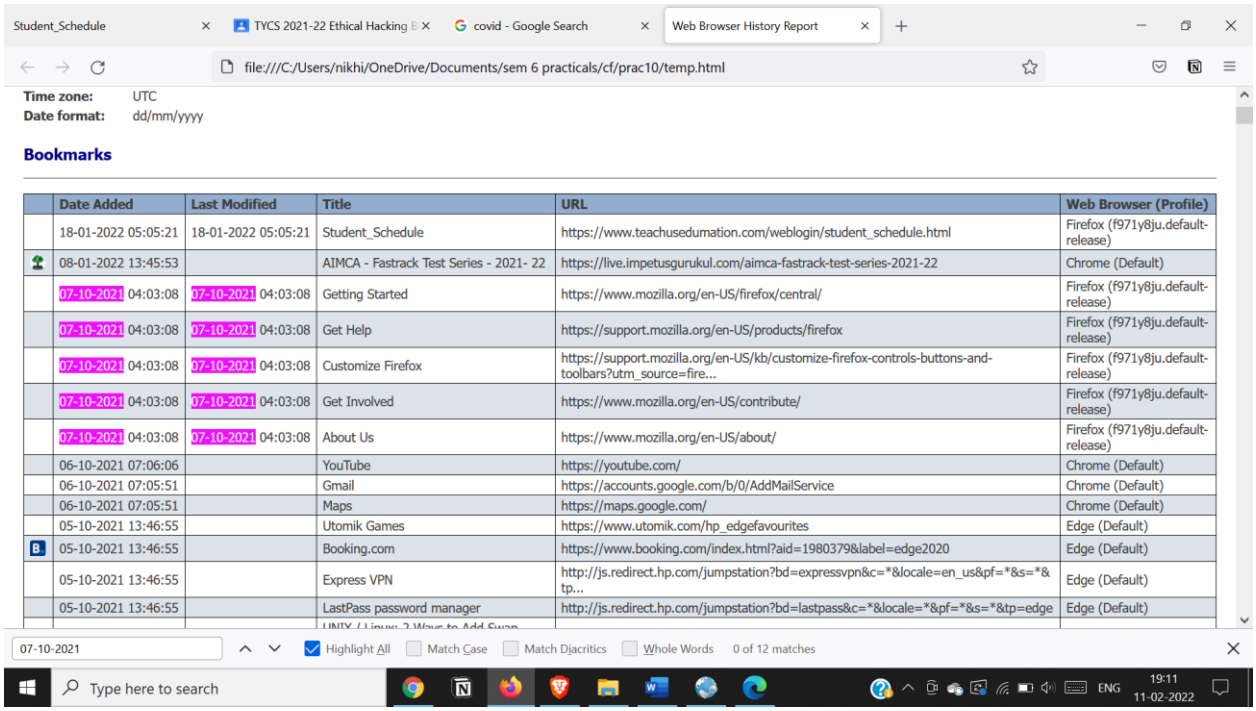


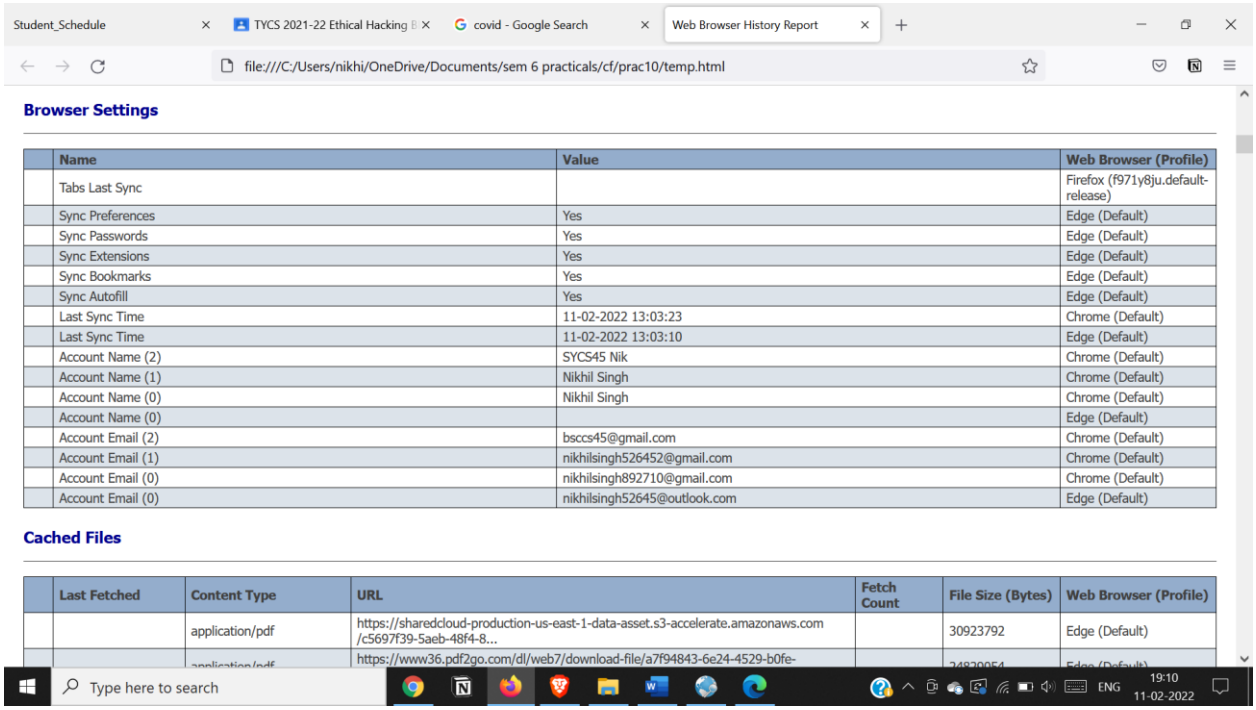


Report gets exported into html



Last Internet Activity gets listed below in the exported report


Student_Schedule
TYCS 2021-22 Ethical Hacking
covid - Google Search
Web Browser History Report
file:///C:/Users/nikhi/OneDrive/Documents/sem 6 practicals/cf/prac10/temp.html
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.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_edgefavourites | 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
Type here to search
ENG
19:11
11-02-2022


Student_Schedule
TYCS 2021-22 Ethical Hacking
covid - Google Search
Web Browser History Report
file:///C:/Users/nikhi/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) | nikhilsingh526452@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)
https://www36.pdf2go.com/dl/web7/download-file/a7f94843-6e24-4529-b0fe-
Type here to search
ENG
19:10
11-02-2022