CERTIFICATE

V.K KRISHNA MENON COLLEGE OF COMMERCE AND ECONOMICS

&

SHARAD SHANKAR DIGHE COLLEGE OF SCIENCE BHANDUP EAST, MUMBAI-400042

This is to certify that Mr.Manish Gupta Roll No:12 has successfully completed **Cyber Forensics** Practical of **Semester VI** for partial fulfilment of B.Sc. Degree course in Computer Science of University of Mumbai in academic year 2022-2023 under the guidance of **Miss.Subha Nair**

DATE HEAD OF THE DEPARTMENT

Teacher-in-charge EXAMINER

INDEX

SR.No	TOPICS	DATE	PAGE NO.	SIGN
1	**Creating a Forensic Image using FTK Imager/Encase Imager :-** ▪ **Creating Forensic Image** ▪ **Check Integrity of Data** ▪ **Analyze Forensic Image**	**8/12/2022**		
2	**Data Acquisition:** ▪ **Perform data acquisition using:** ▪ **USB Write Blocker + FTK Imager**	**15/12/2022**		
3	**Forensics Case Study : Solve the Case study (image file) provide in lab using Encase Investigator or Autopsy .**	**22/12/2023**		
4	**Capturing and analyzing network packets using Wireshark :** ▪ **Identification the live network** ▪ **Capture Packets** ▪ **Analyze the captured packets**	**12/01/2023**		
5	**Analyze the packets provided in lab and solve the questions using Wireshark**	**19/01/2023**		
6	**Using Sysinternals tools for Network Tracking and Process Monitoring**	**02/02/2023**		
7	**Recovering and Inspecting deleted files Check for Deleted Files** ▪ **Recover the Deleted Files** ▪ **Analyzing and Inspecting the recovered files**	**09/02/2023**		
8	**Acquisition of Cell phones and Mobile devices**	**16/02/2023**		
9	**Email Forensics** • **Mail Service Providers** • **Email protocols** • **Recovering emails** • **Analyzing email header**	**23/02/2023**		
10	**Web Browser Forensics .** ▪ **Web Browser working** ▪ **Forensics activities on browser** ▪ **Cache / Cookies analysis** ▪ **Last Internet activity**	**09/03/2023**		

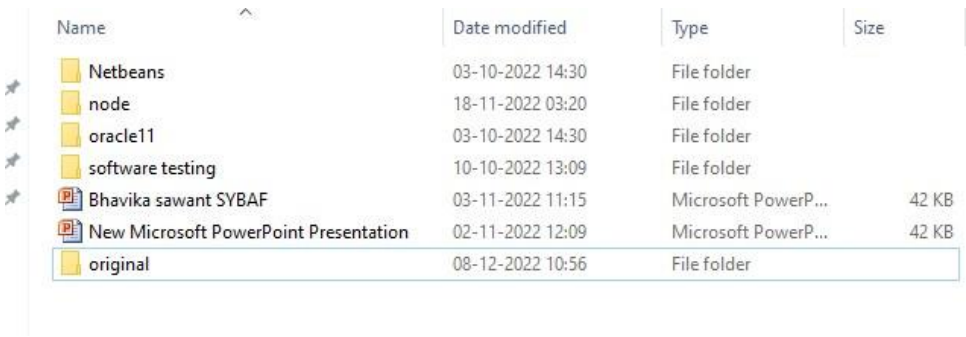
Practical No :- 1

AIM : Create a Forensics image using FTK imager

-Creating Forensic Image

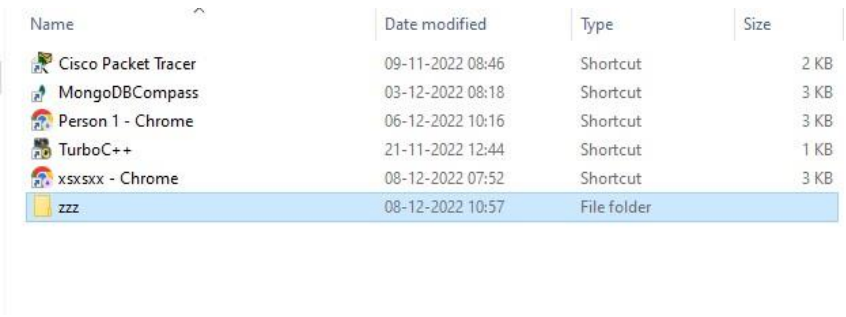
-Check Integrity of Data

-Analyze Forensic Image



Steps:

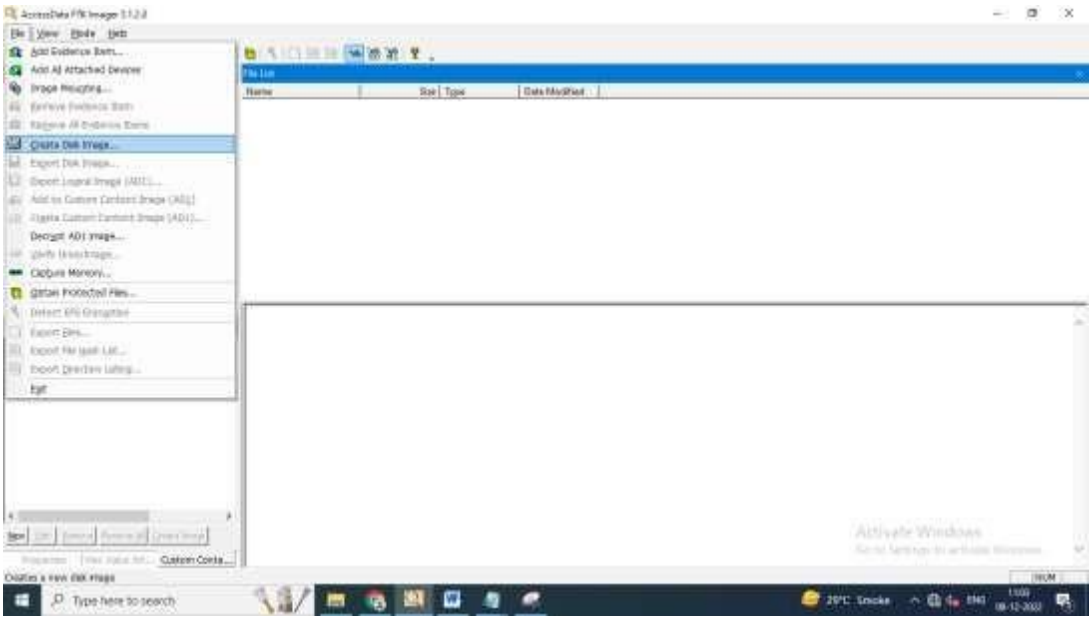
First create a folder

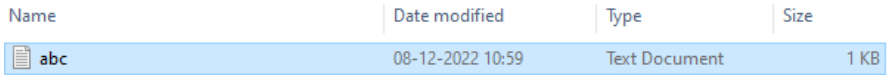


In that folder create a folder name tha folder Forensic copy

Creating Forensic Image

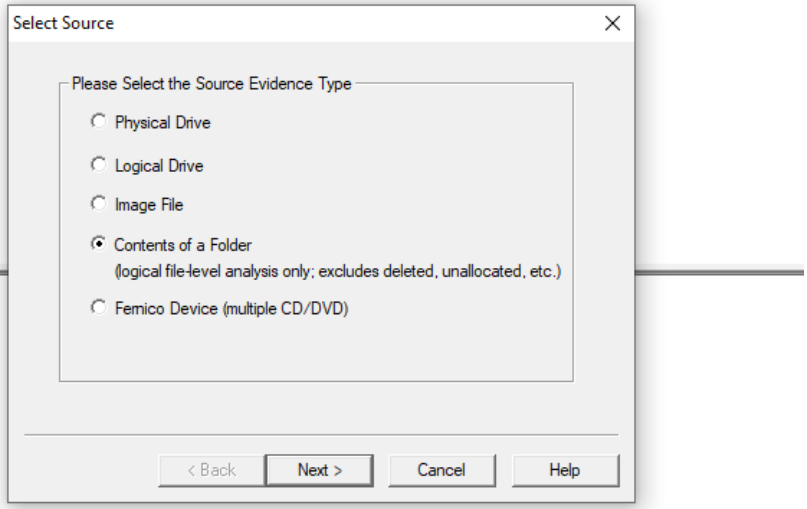
1. Click File, and then Create Disk Image, or click the button on the tool bar.



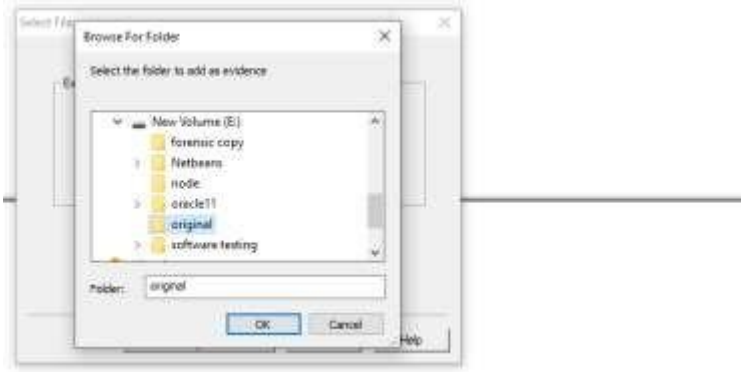


Select the folder

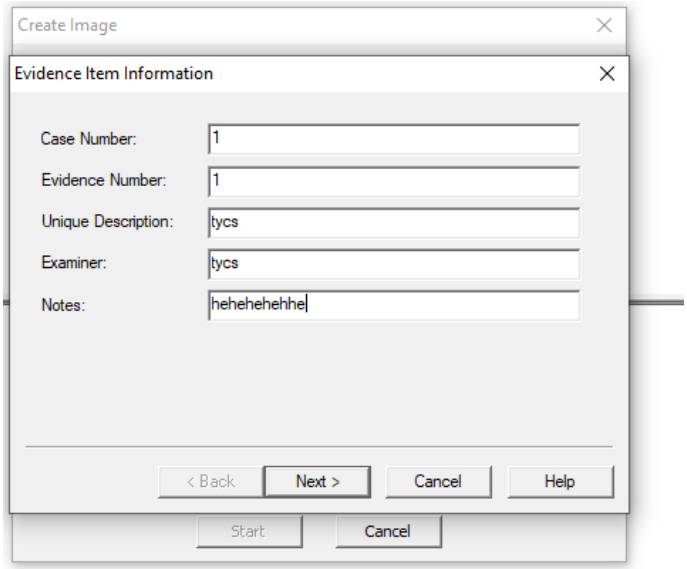
2. Select the source you want to make an image of and click Next.

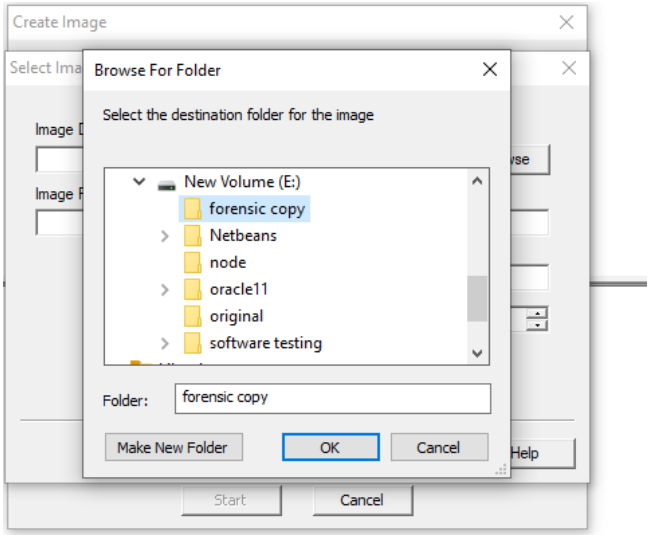


Select Original folder

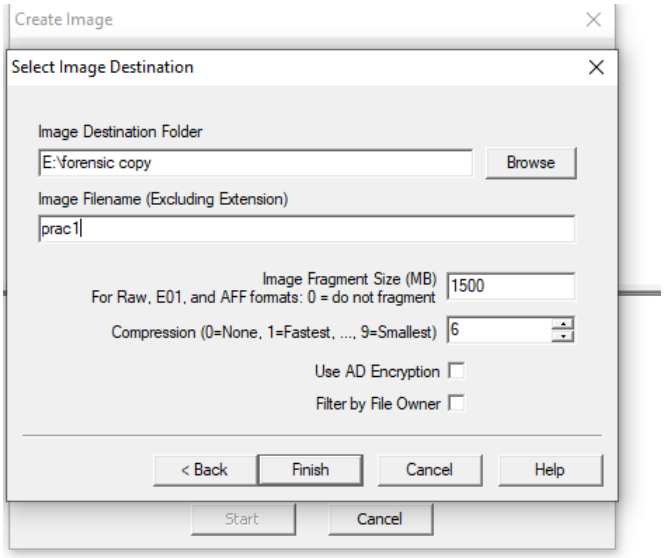

Browse For Folder
Select the folder to add as evidence
New Volume (E:)
forensic copy
Netbeans
node
oracle11
original
software testing
Folder:
original
OK
Cancel
Help

3. fill this

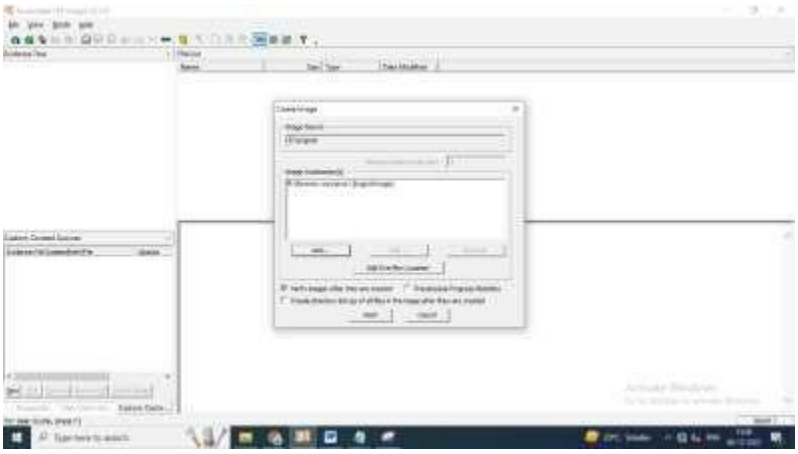

Create Image
Evidence Item Information
Case Number:
1
Evidence Number:
1
Unique Description:
tycs
Examiner:
tycs
Notes:
hehehehehhe
< Back
Next >
Cancel
Help
Start
Cancel


Create Image
Browse For Folder
Select the destination folder for the image
New Volume (E:)
forensic copy
Netbeans
node
oracle11
original
software testing
Folder:
forensic copy
Make New Folder
OK
Cancel
Help
Start
Cancel

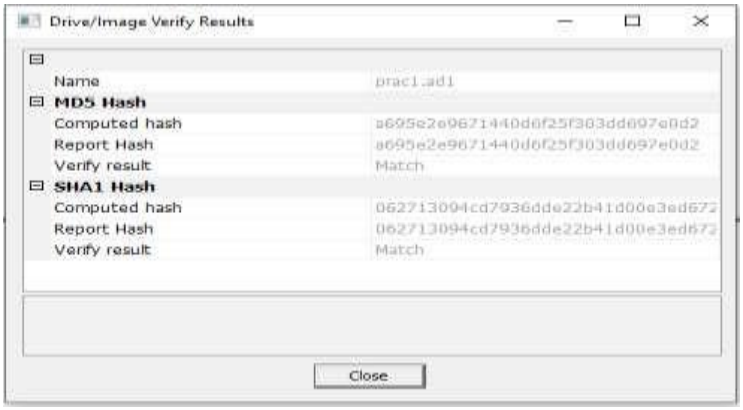
4. Browse the folder <finish>



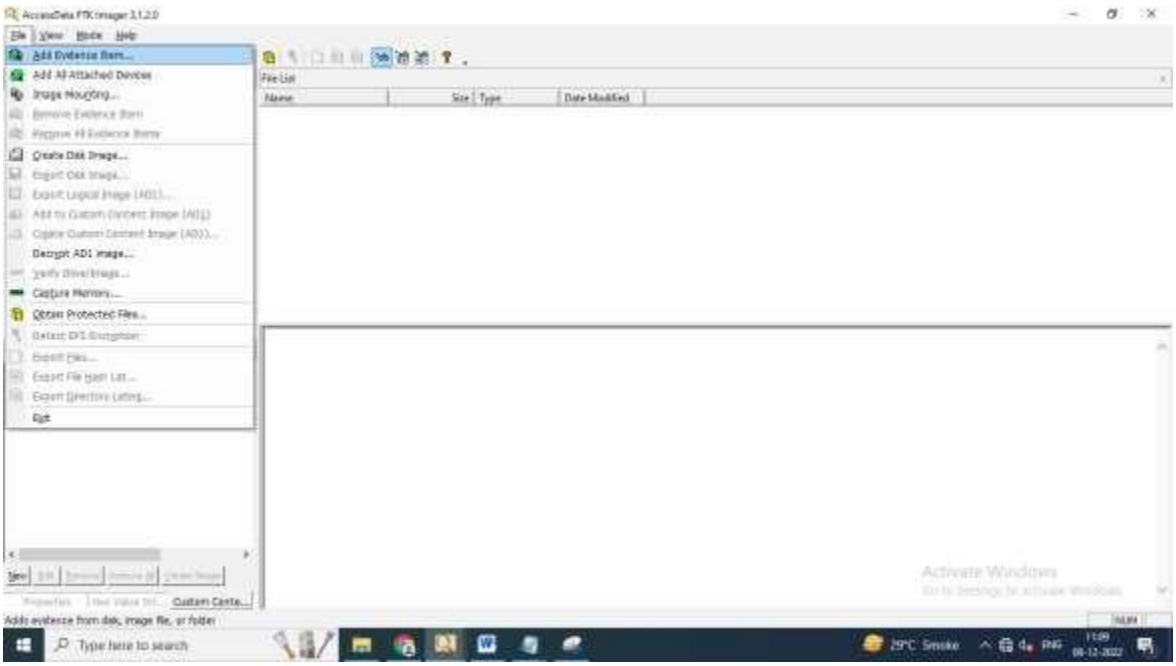
5. Add a folder <Start>



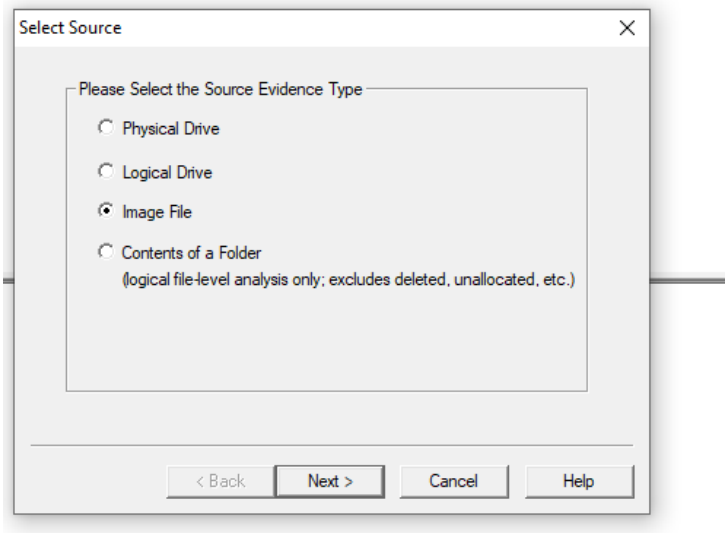
6.choose any <Close>



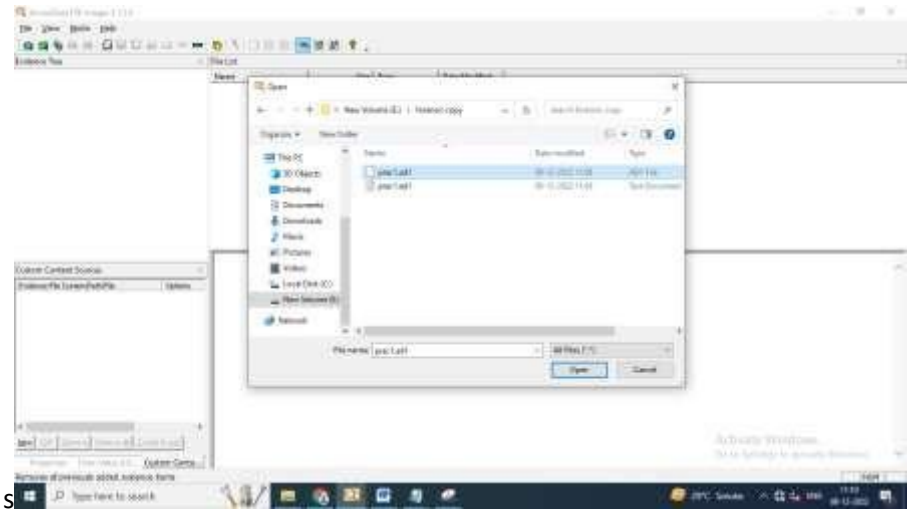
7.Add Evidence Item



8.Select Image File <next>

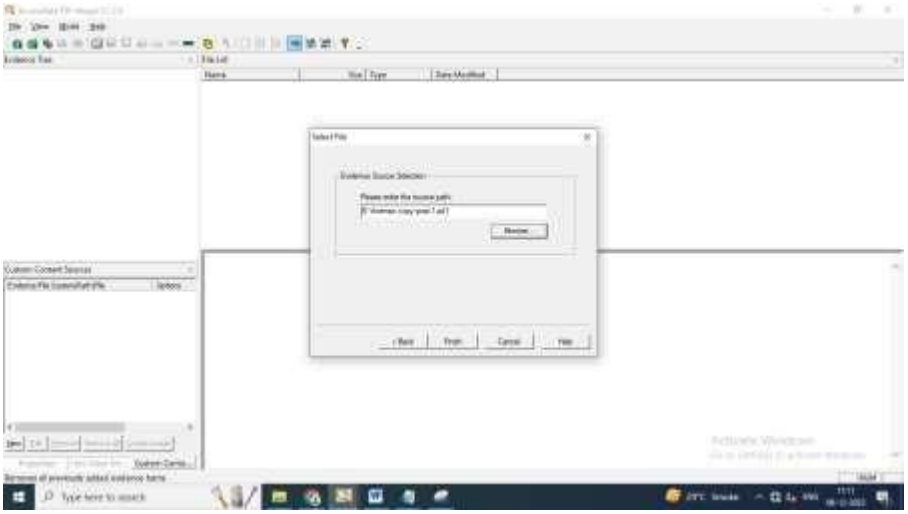


Select a folder you create.

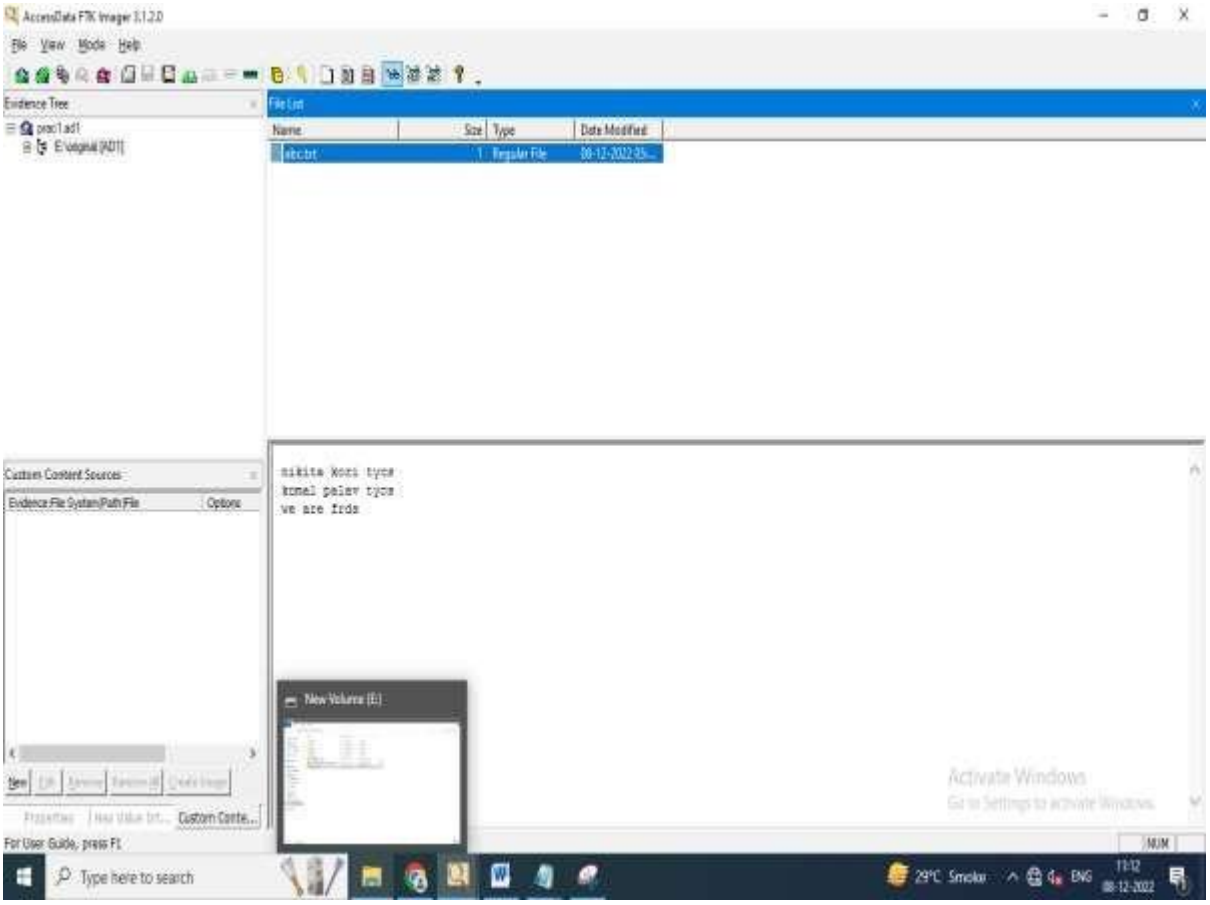


S

Browser it.



THE OUTPUT:


AccessData FTK Imager 3.1.2.0
File View Mode Help
Evidence Tree
File List
Name
Size
Type
Date Modified
abcdot
Regular File
Custom Content Sources
Evidence File System|Path|File
Options
nikita kori tyce
komal palav tyce
we are frds
New Volume (E:)
Activate Windows
Type here to search
29°C Smoke
ENG

Practical No : 2

Aim: Data Acquisition:

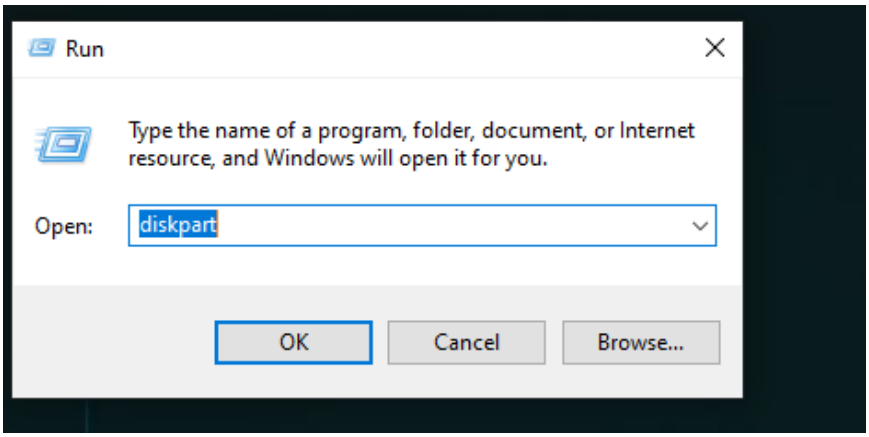
- Perform data acquisition using:

- USB Write Blocker + FTK Imager

Steps:

Enable USB Write Block in Windows 10, 8 and 7 using registry

1.Press the Windows key + R to open the Run box. Type regedit and press Enter.



Open command prompt

```
Microsoft DiskPart version 10.0.19041.964

Copyright (C) Microsoft Corporation.
On computer: DESKTOP-U79P21N

DISKPART> list disk

  Disk ###  Status         Size     Free     Dyn  Gpt
  --------  -------------  -------  -------  ---  ---
  Disk 0    Online          931 GB  1024 KB        *
  Disk 1    Online         3862 MB   384 KB

DISKPART>
```

Select disk 1

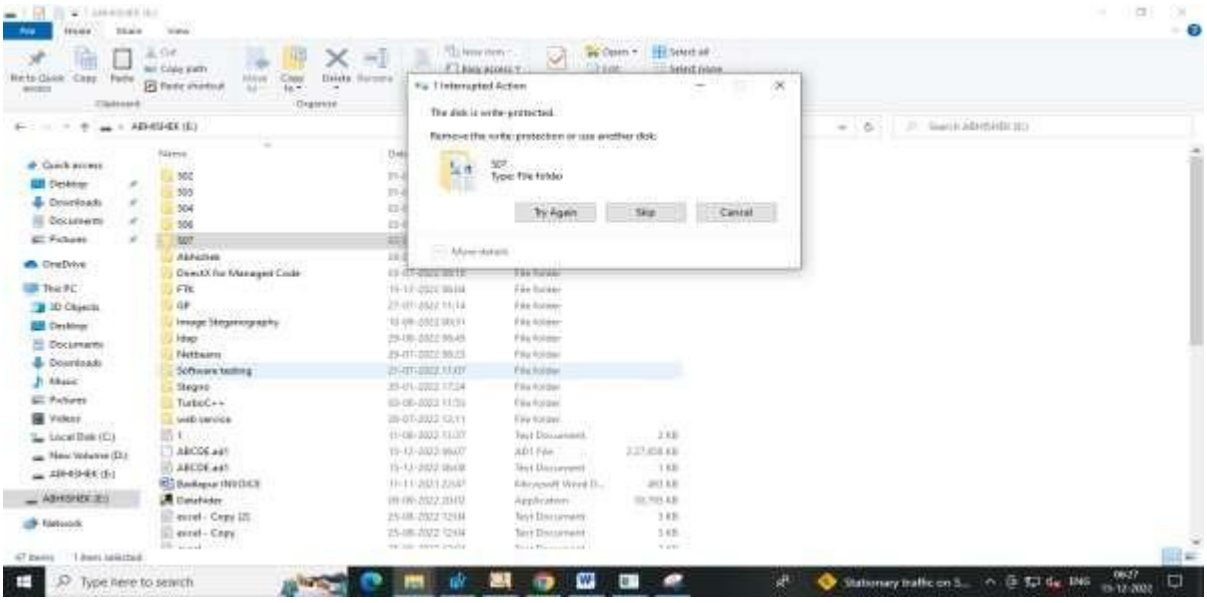
```
DISKPART> Select disk 1

Disk 1 is now the selected disk.

DISKPART>
```

```
DISKPART> attributes disk
Current Read-only State : No
Read-only  : No
Boot Disk  : No
Pagefile Disk  : No
Hibernation File Disk  : No
Crashdump Disk  : No
Clustered Disk  : No

DISKPART>
```

Run successfully

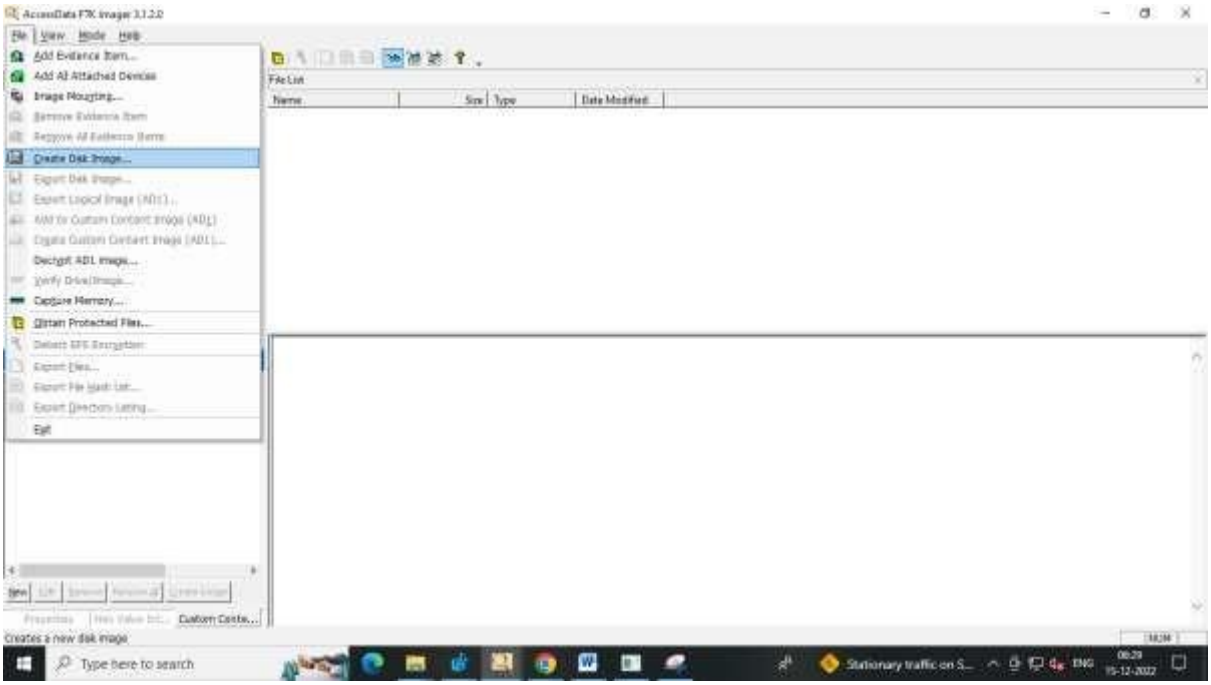
```
DISKPART> attributes disk set readonly

Disk attributes set successfully.

DISKPART>
```

Steps1: select any folder

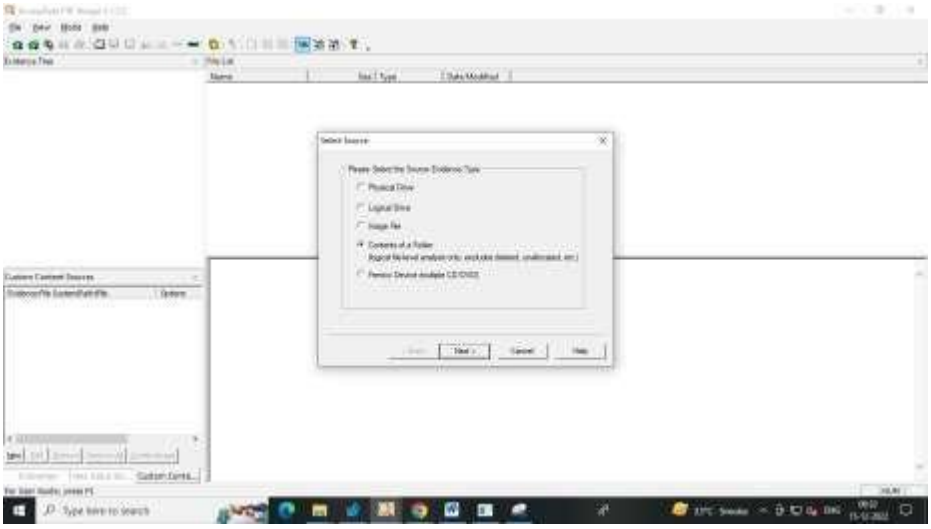


Steps:

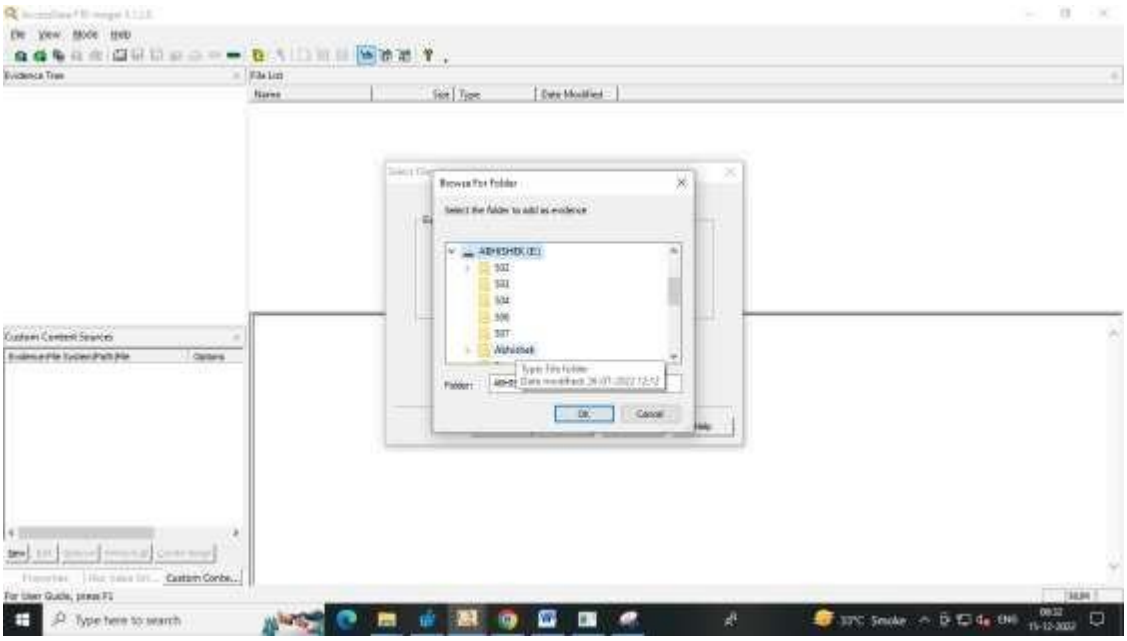
1.Create Disk Image



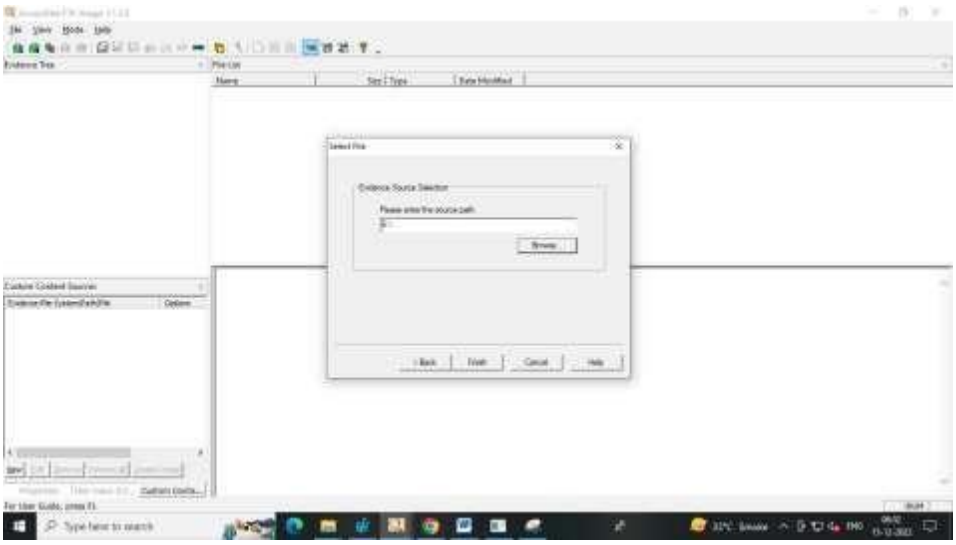
2.Select Contents of a Folder



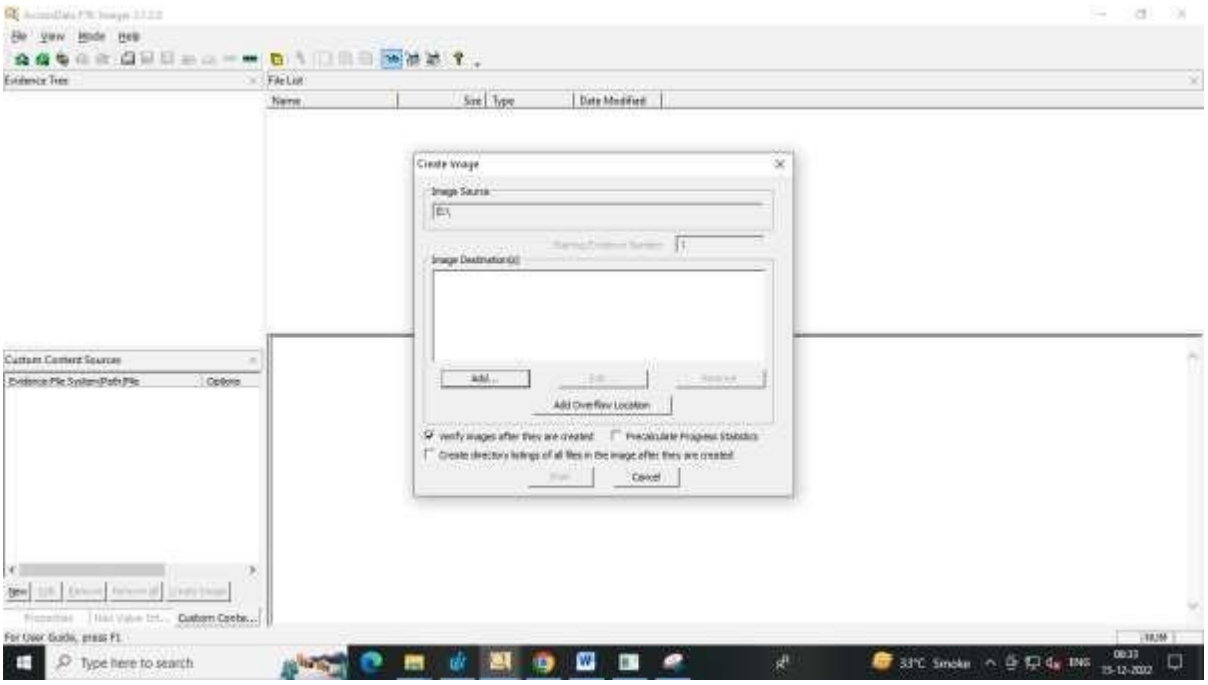
Select a folder<ok>



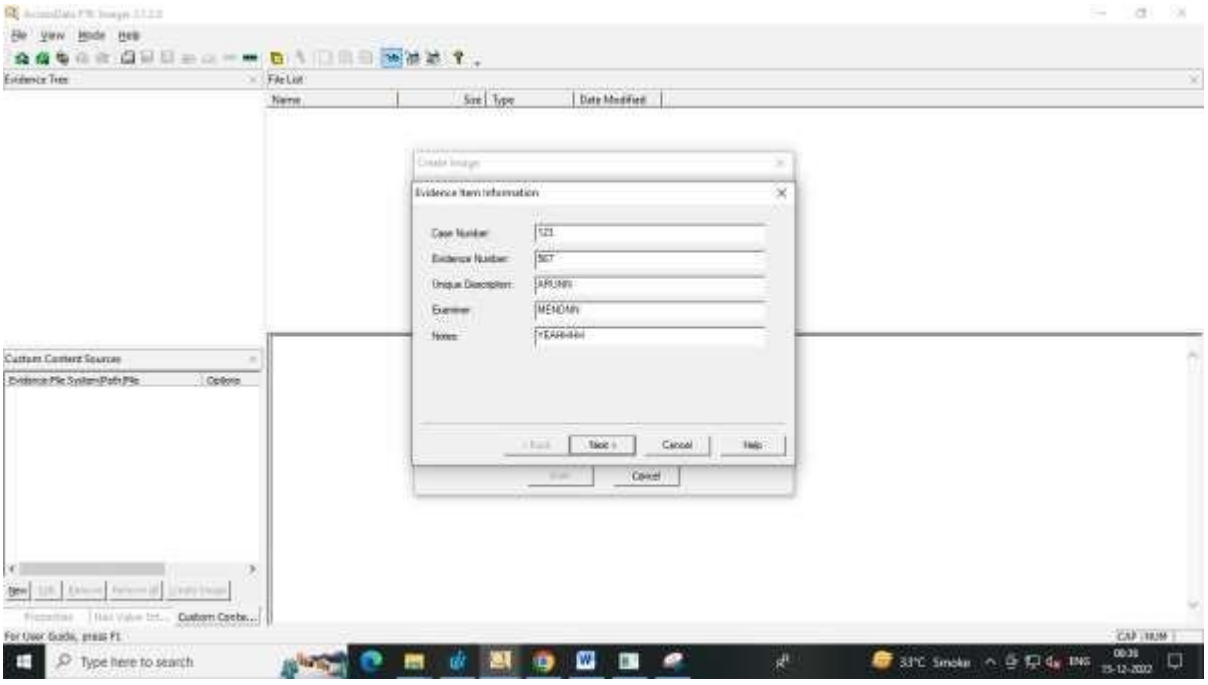
Browser it.



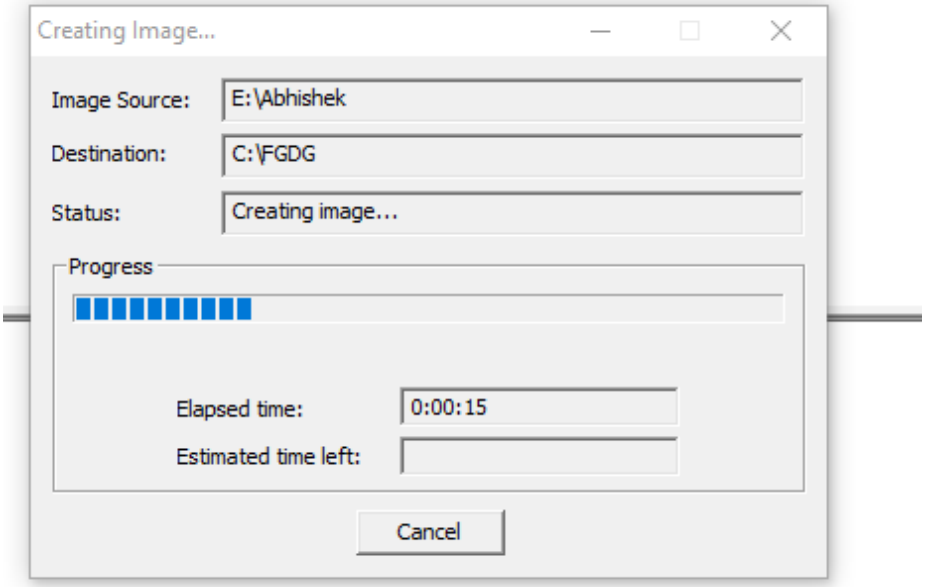
3. Add <Start>



5. Fill the case no <next>



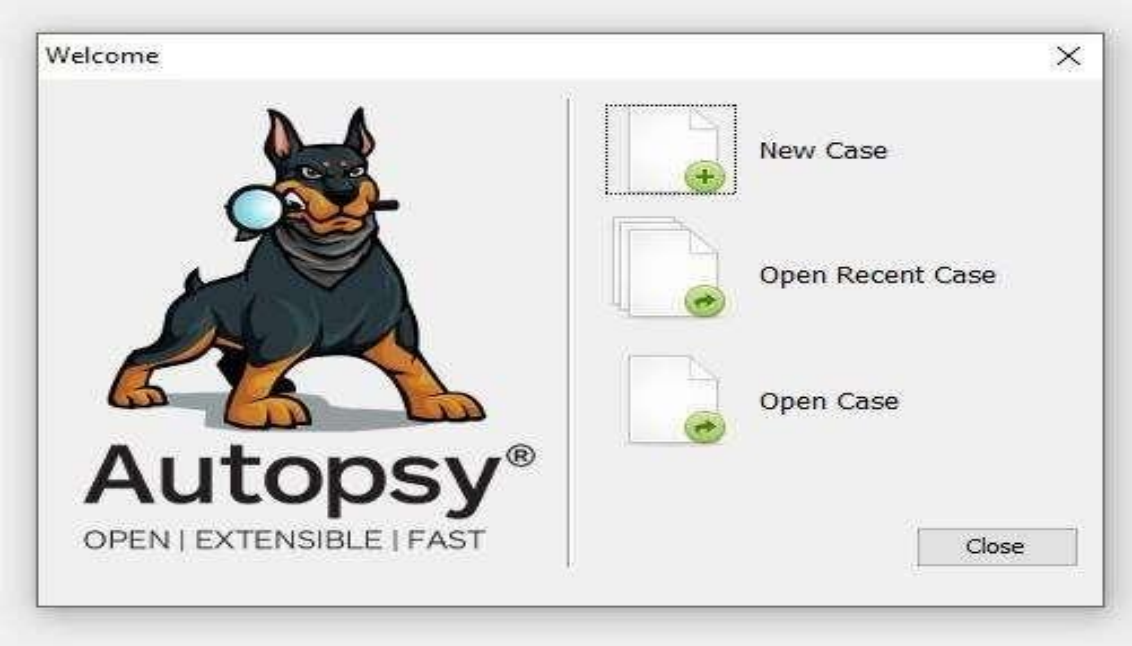
THE OUTPUT:


Creating Image...
Image Source:
E:\Abhishek
Destination:
C:\FGDG
Status:
Creating image...
Progress
Elapsed time:
0:00:15
Estimated time left:
Cancel

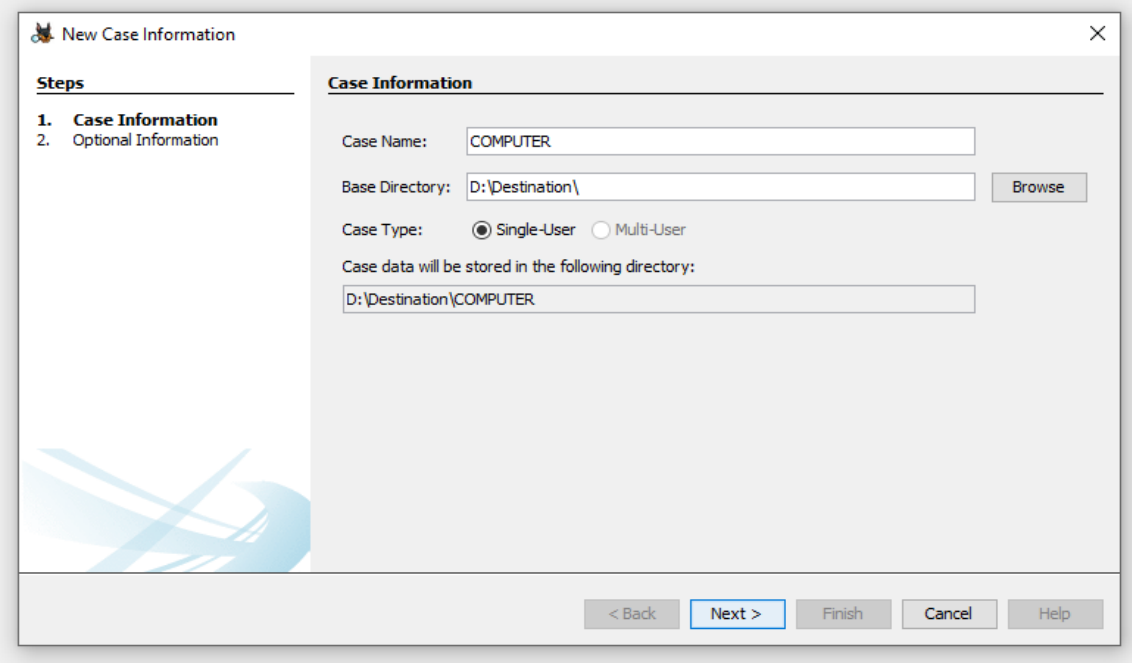
Practical No :- 3

Aim :- Solve the Case study provide in lab using Encase Investigator or Autopsy. Steps :-

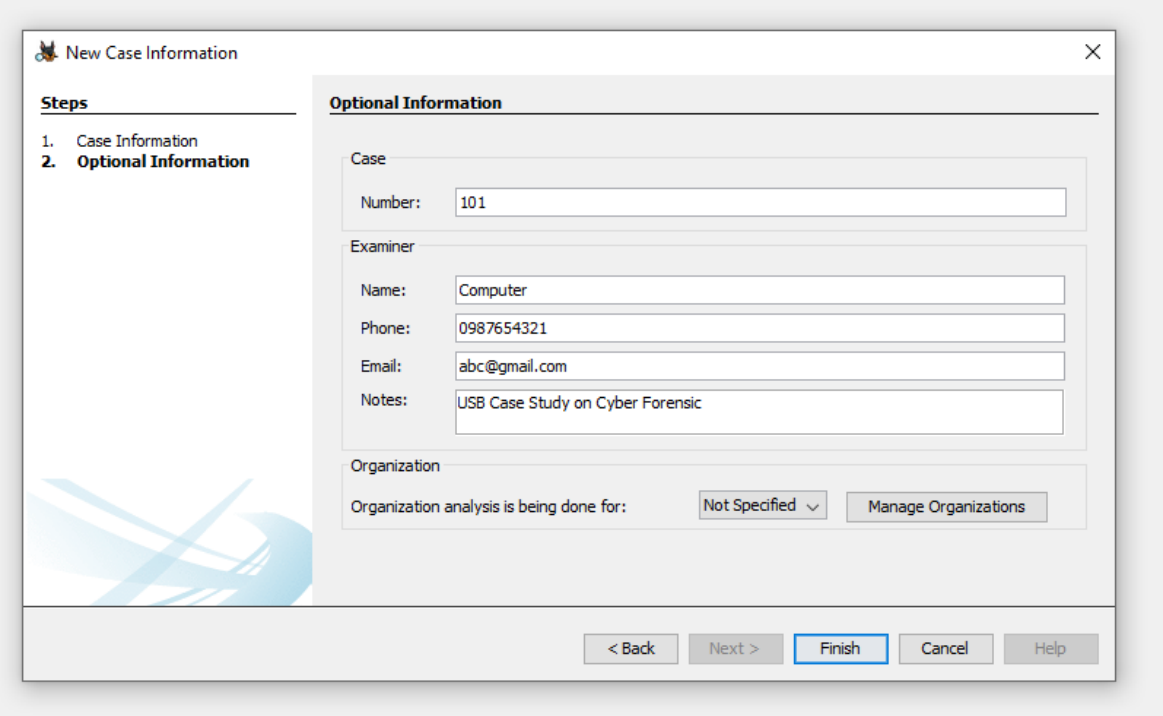
1. Start Autopsy -> Select New Case.



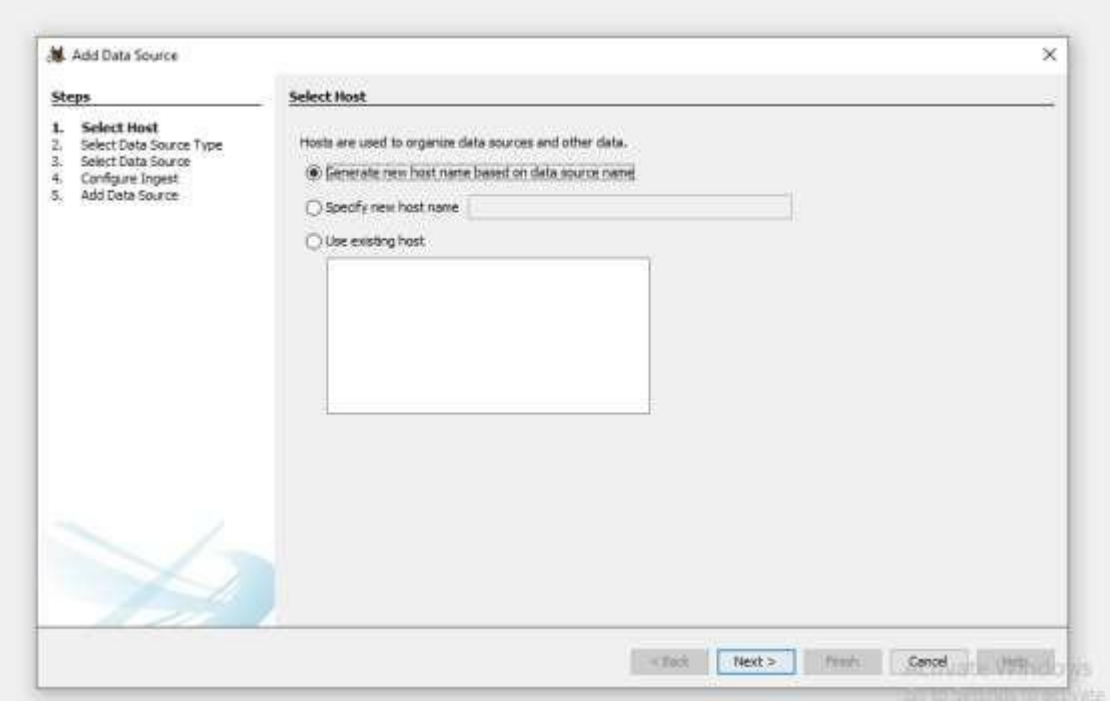
2. Enter Case Information -> Browse Base Directory & Click on Next



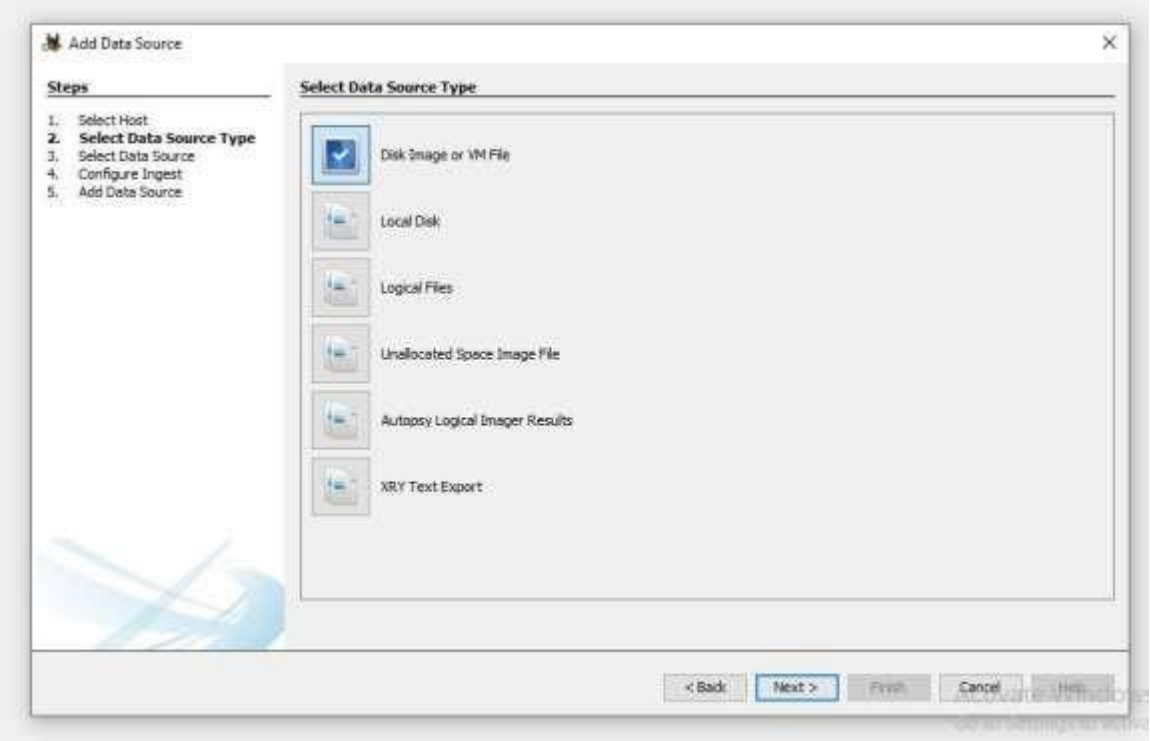
3. Fill all Optional Information.



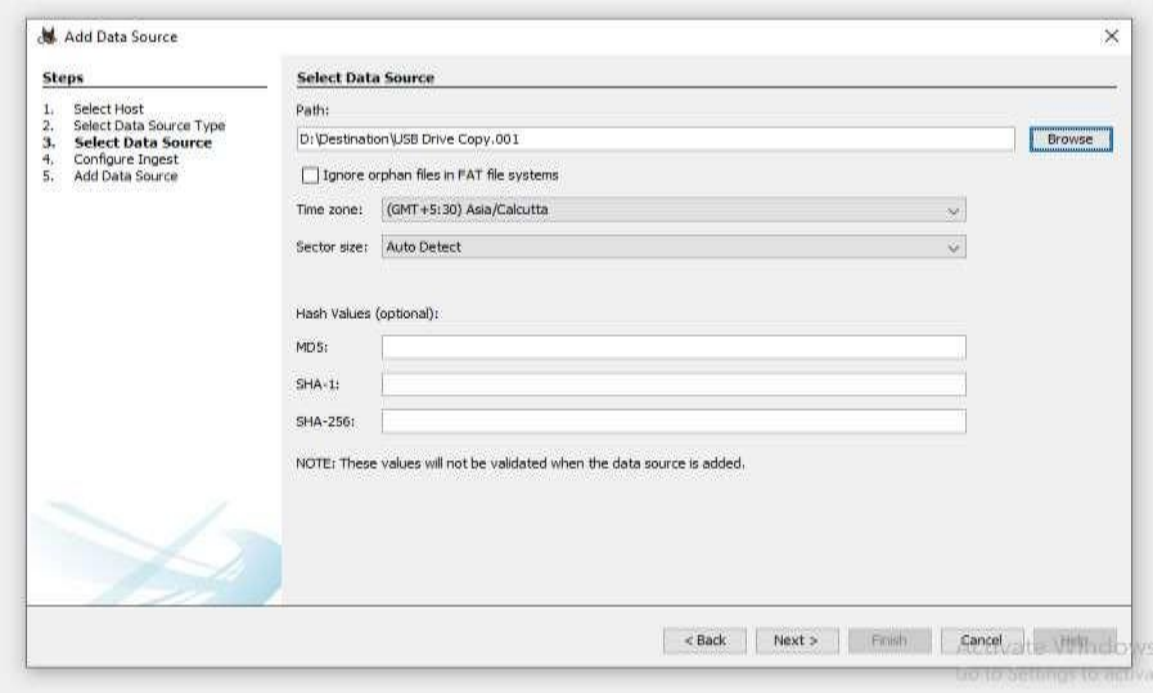
4. In Select Host we will select -> Generate new host name based on data source name and click on Next.



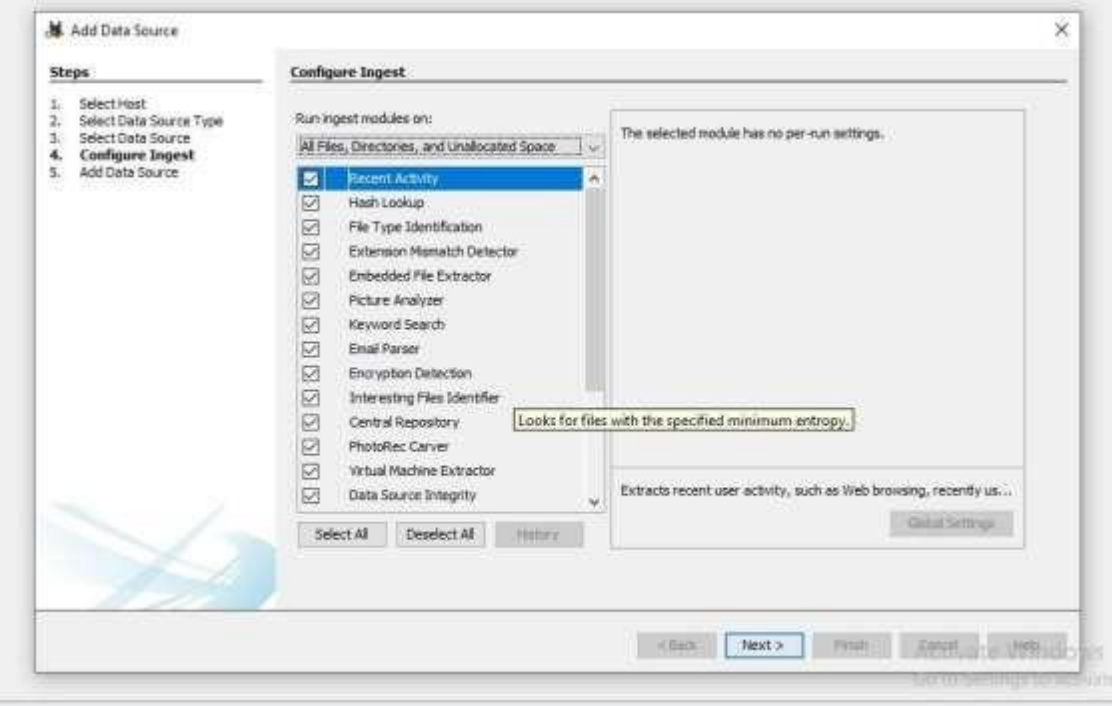
5. Select the type of Data Source that has to be added.



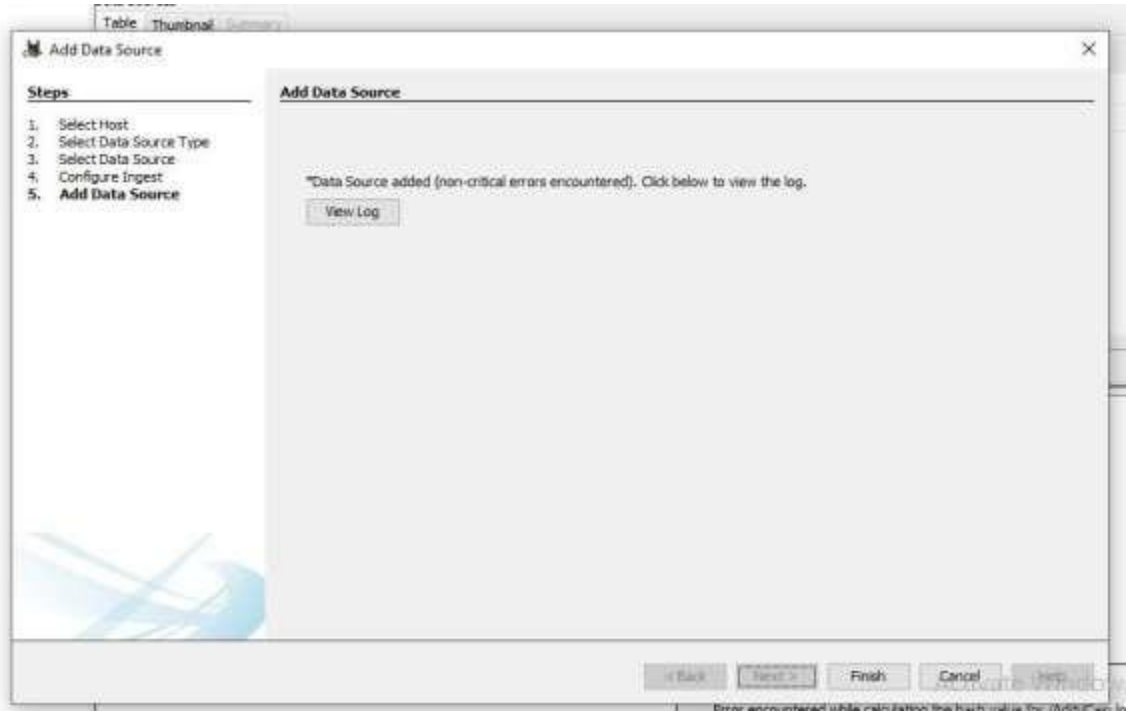
6. Select Data Source (here a previously made image file of USB is selected)



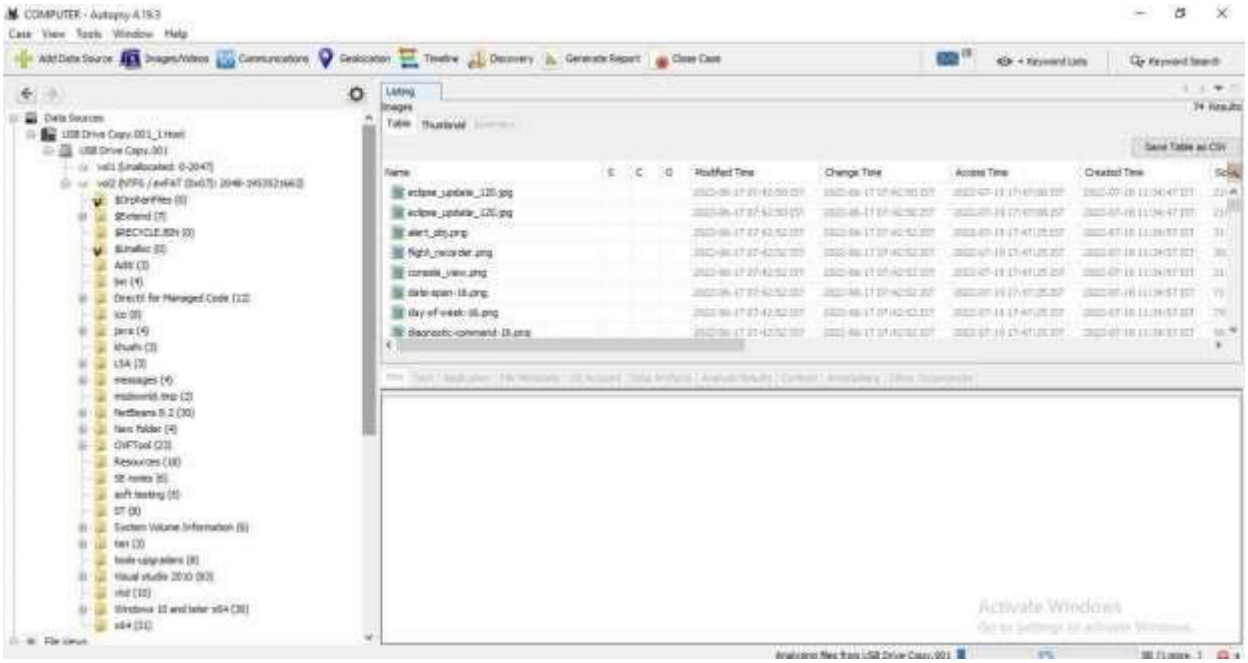
7. Select all ingest modules.



8. Wait for Data source to process and be added to local database and Click Finish.



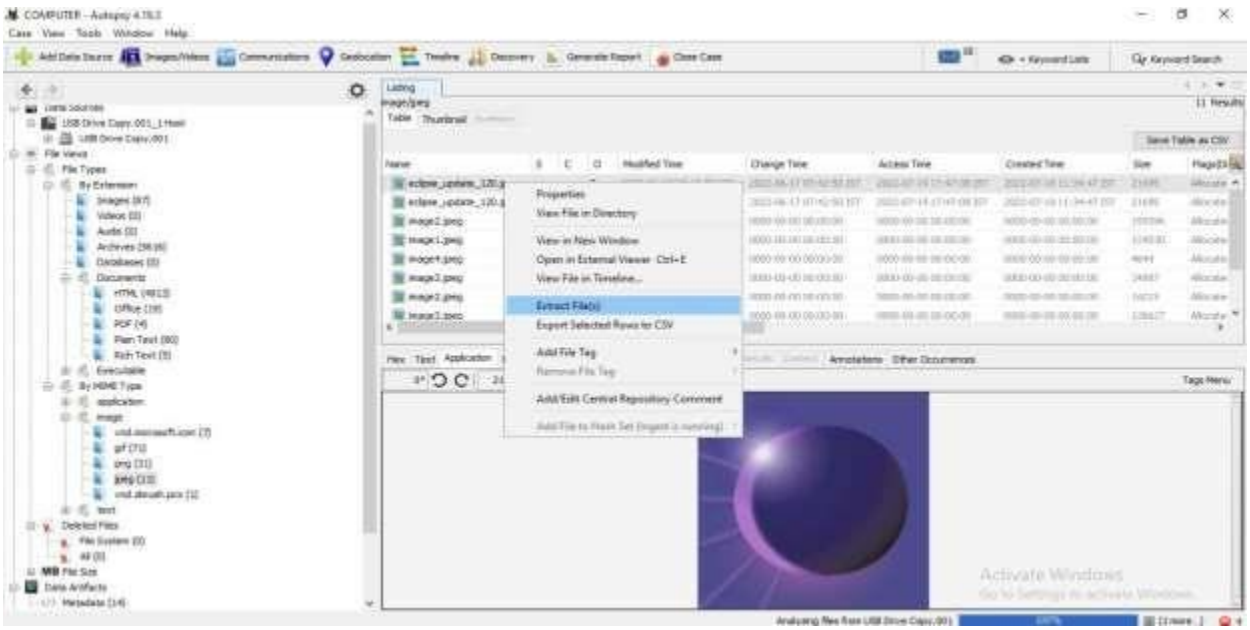
9. Now Autopsy window will appear and it will analyzing the disk that we have selected.



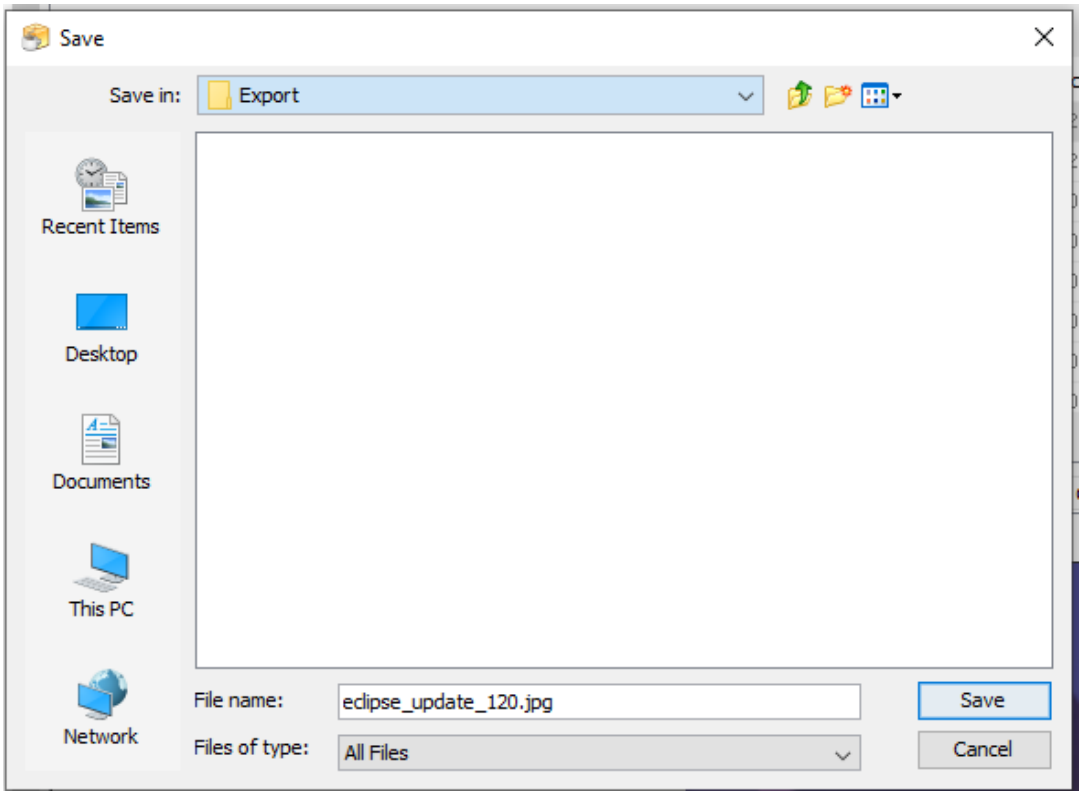
10. All files will appear in table tab select any file to see the data.

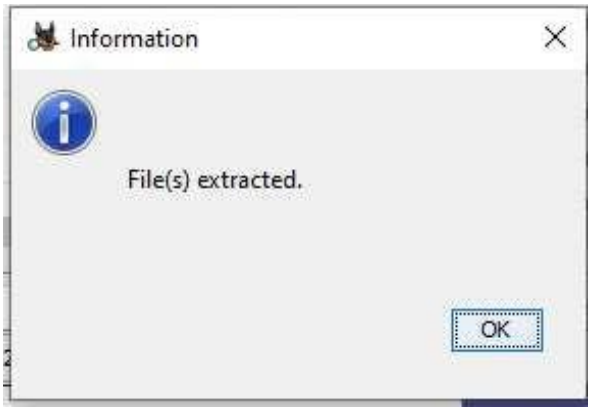
11. Expand the tree from left side panel to view the files and then expand the deleted files Node.

12. To recover the file, go to view node-> Deleted Files node -> Select any file -> Right click on it than select Extract Files option.

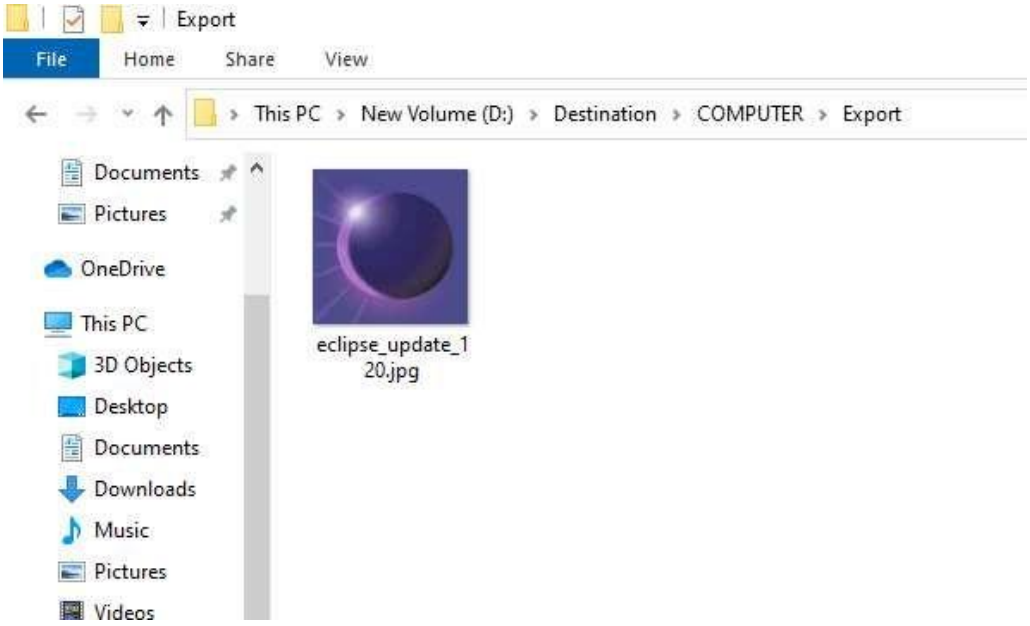


13. By default Export folder is choose to save the recovered file.

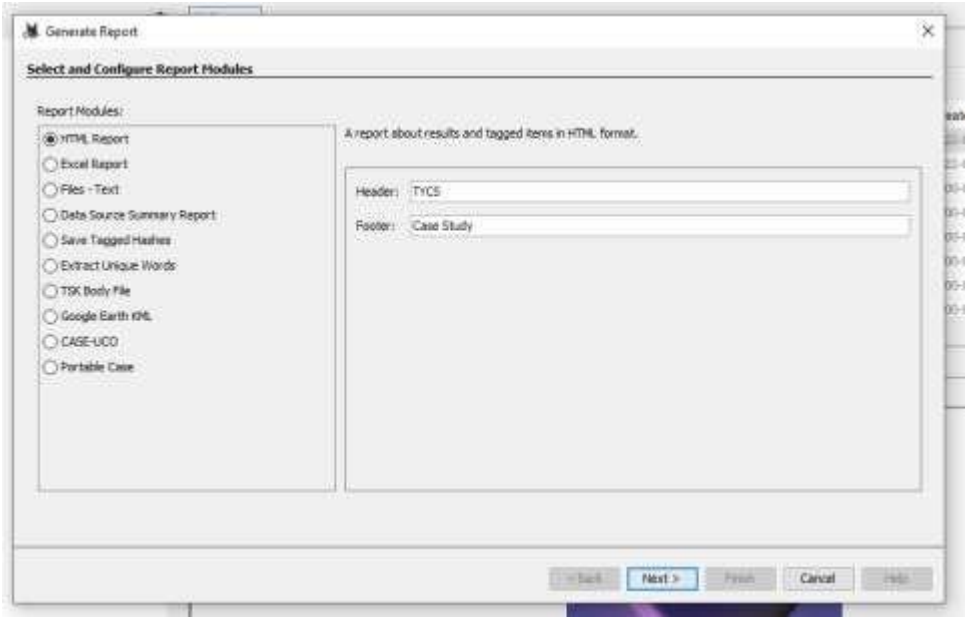


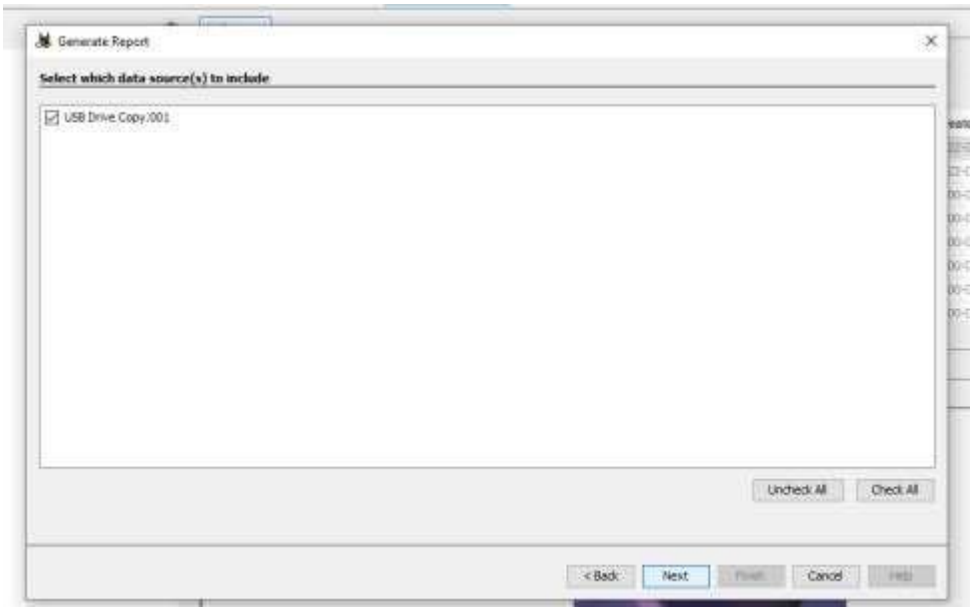


14. Now go to the Export Folder to view Recover file.

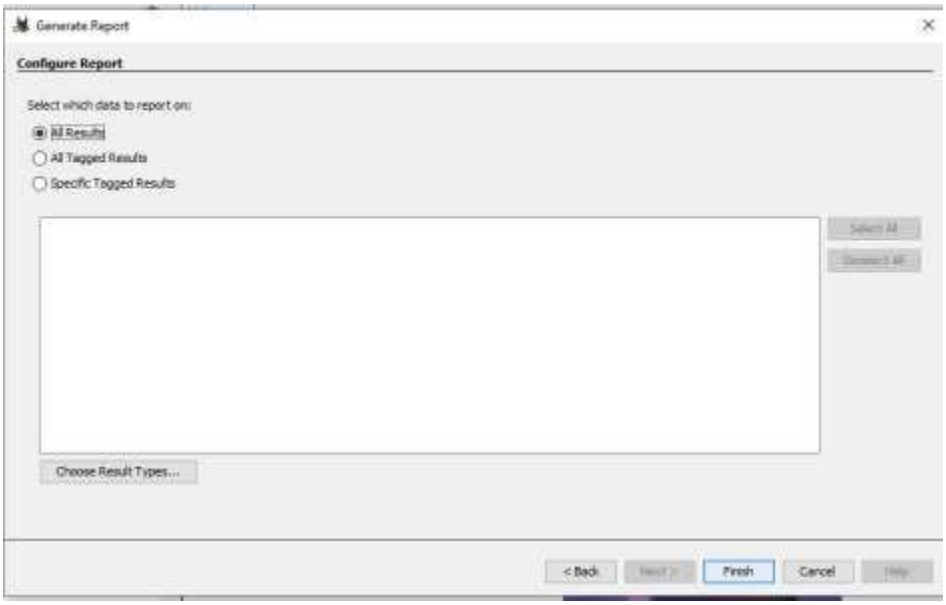


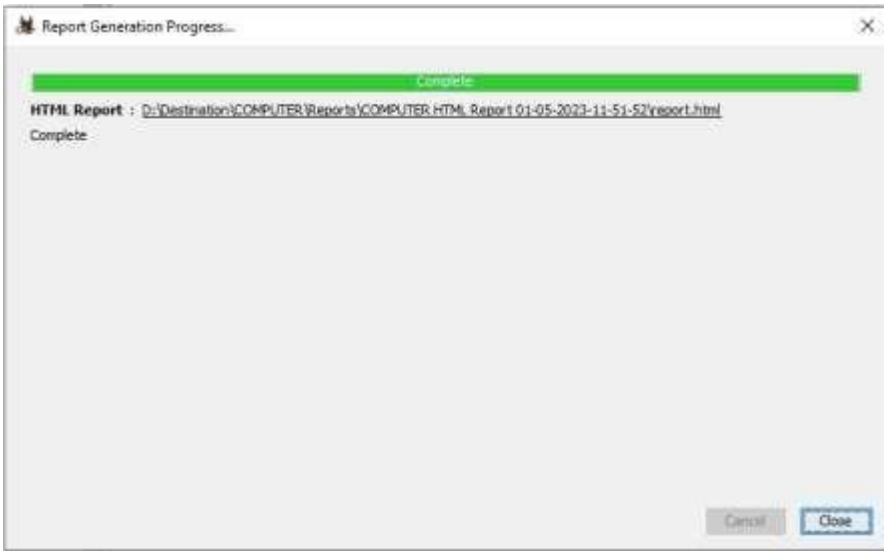
15. Select -> Logical files-> select sample file ->add->next ->Finish

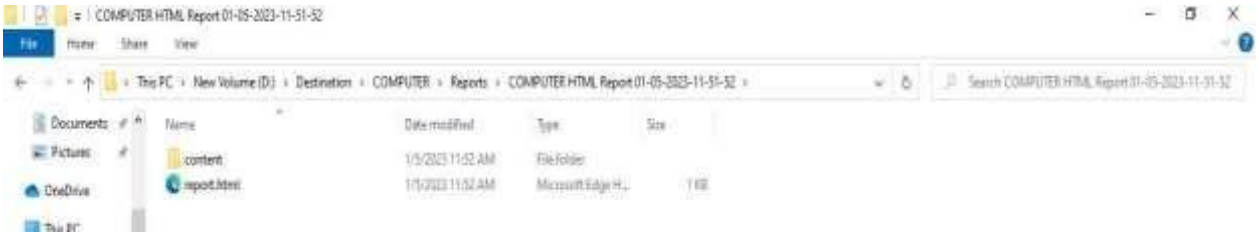




16. Then Generate Report->Click on Generate Report.







Go to this path

Practical no : 4

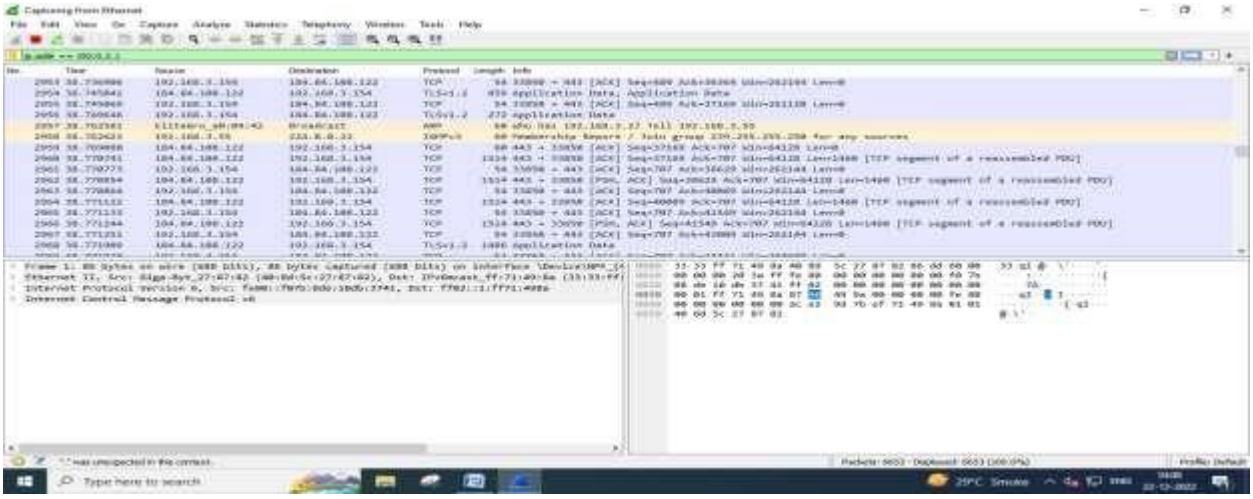
Aim : Capturing and Analyzing network packets using Wireshark (Fundamentals).

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

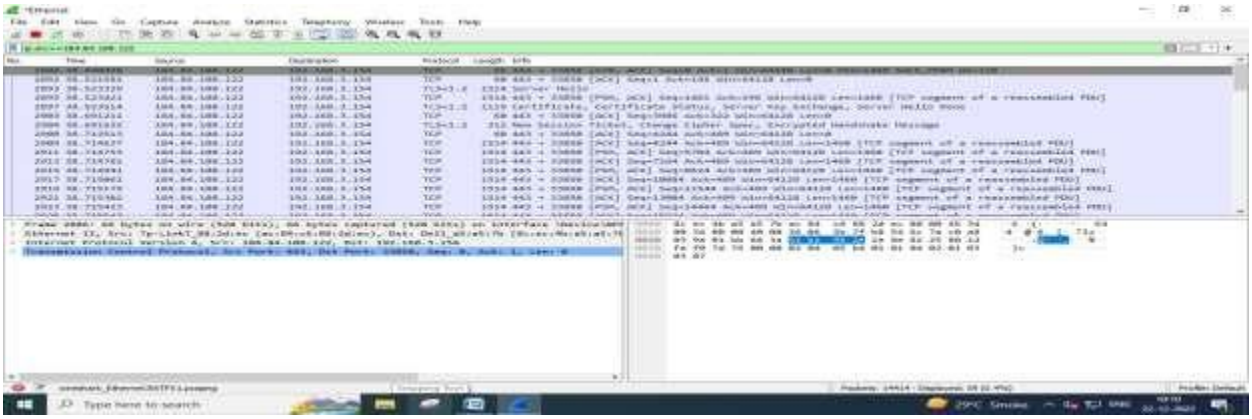
Steps :

Open the Wireshark and click on Ethernet.

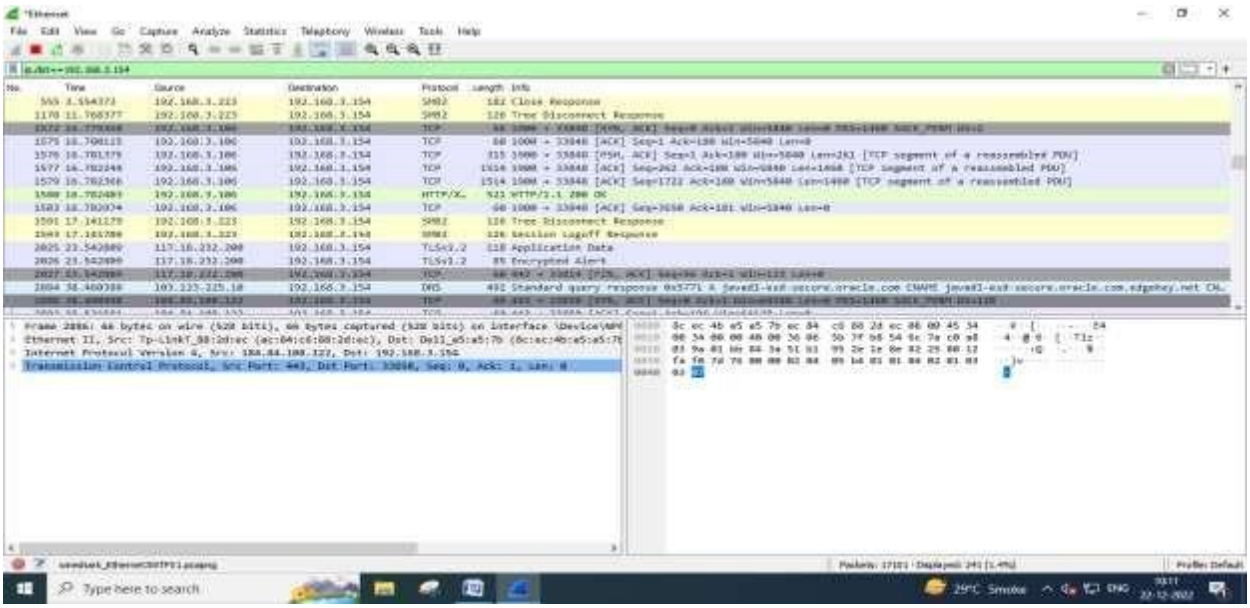
1. Display packets based on specific IP-address.
   - **ip.addr==192.0.2.1**



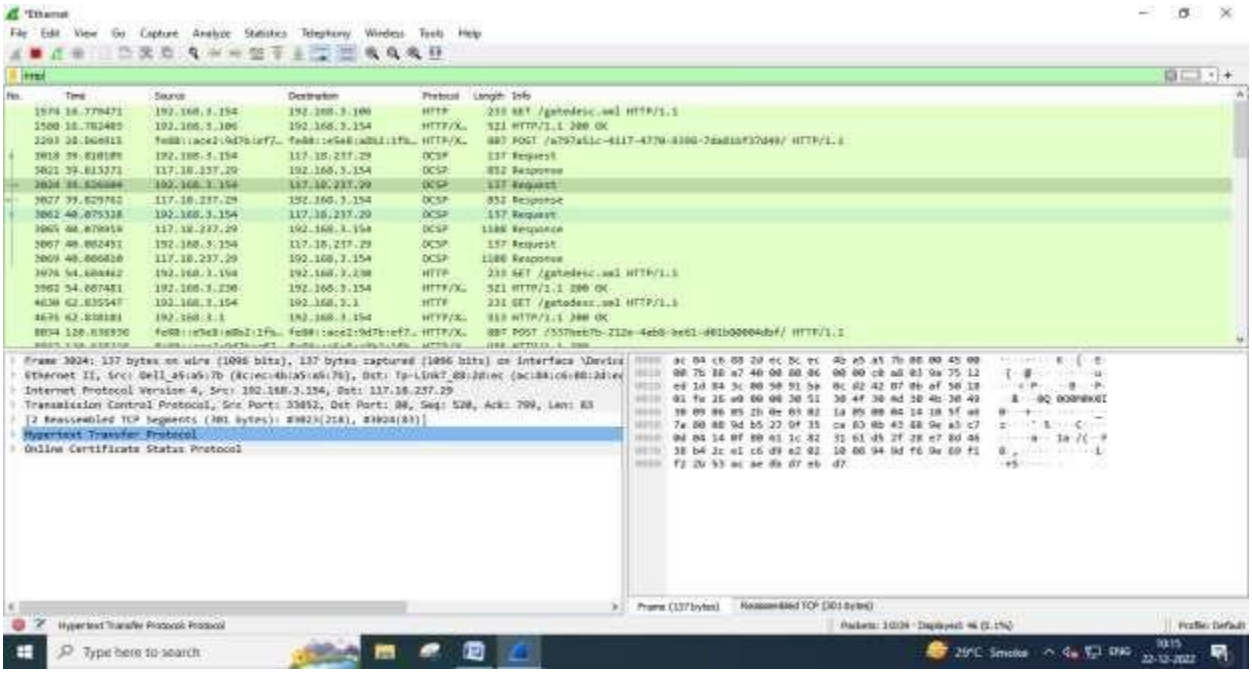
2. Display packets which are coming from specific IP-address.
   - **ip.scr==184.84.108.122**



3. Display packets which are having specific IP-address destination.
   - **ip.dst==192.168.3.154**

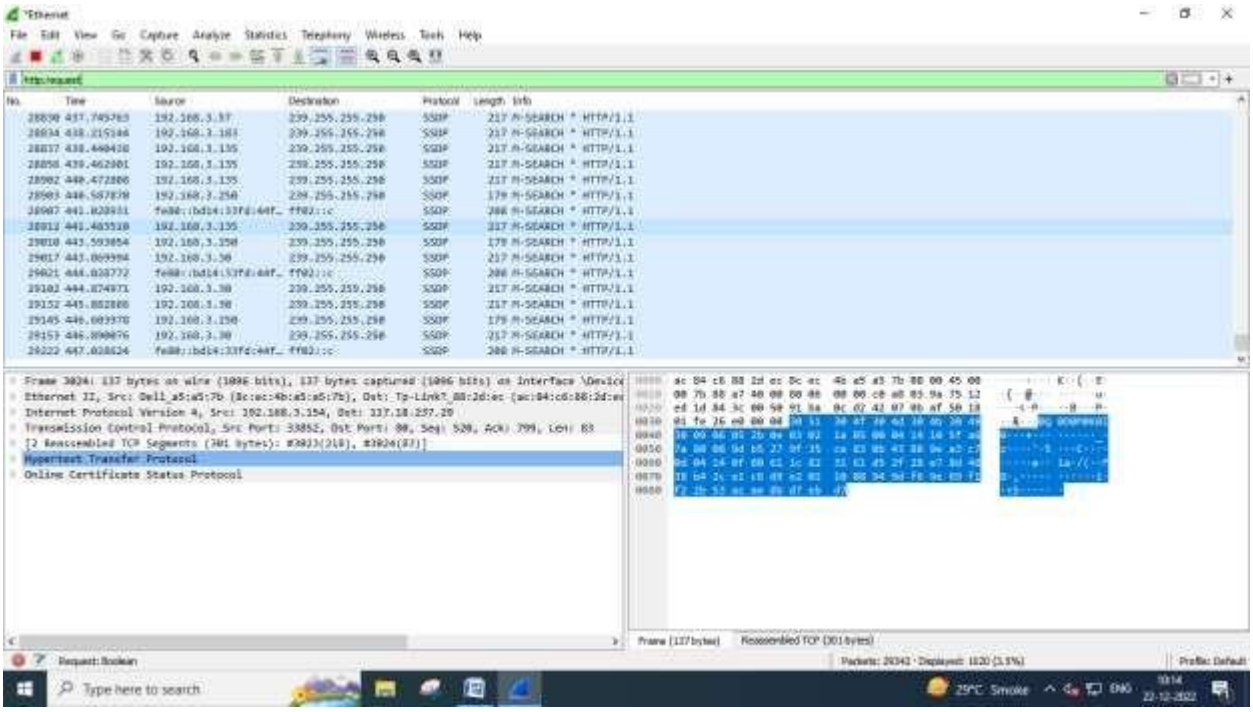


4. Display packets which are using http protocol.
   - **http**



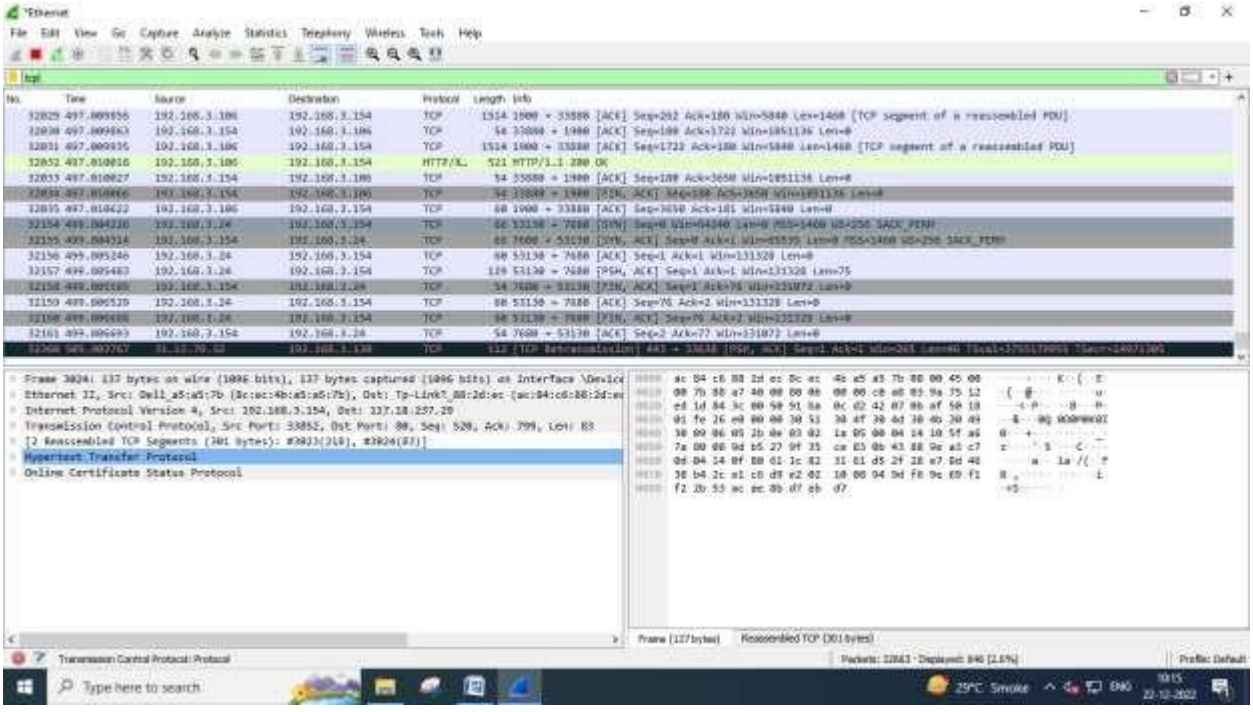
5. Display packets which are using http.request

- **http.request**

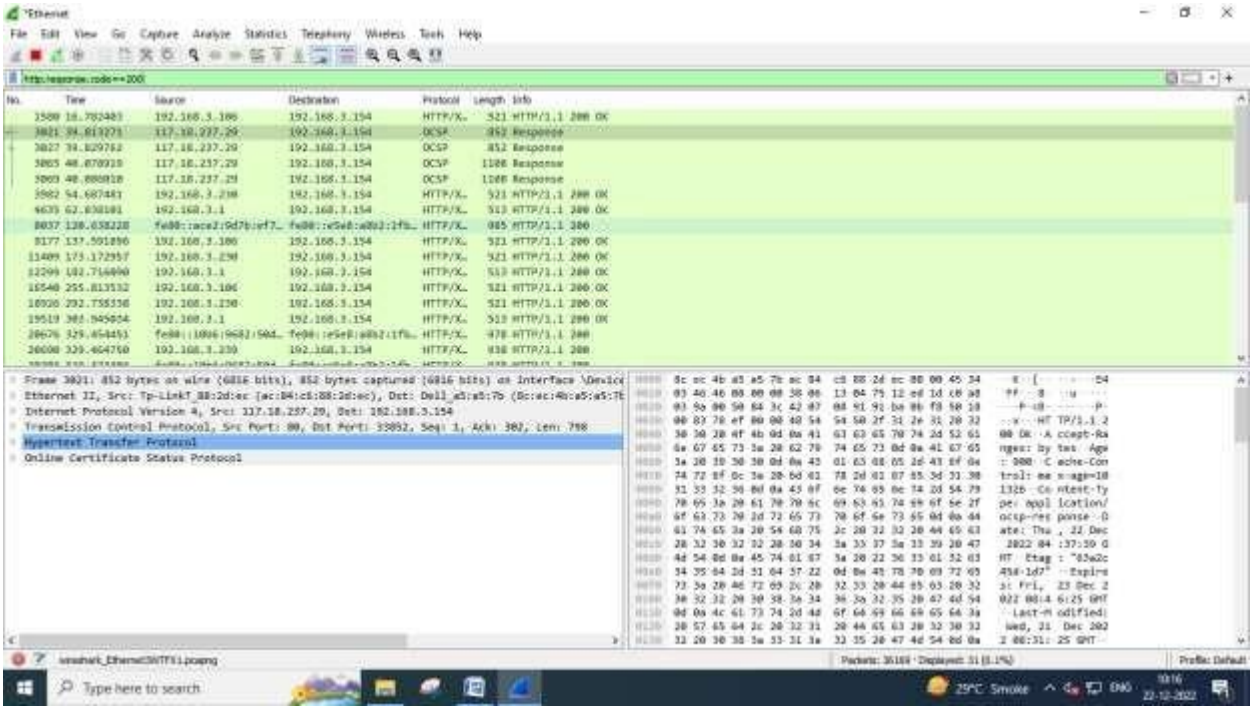


6. Display packets which are using TCP protocol.

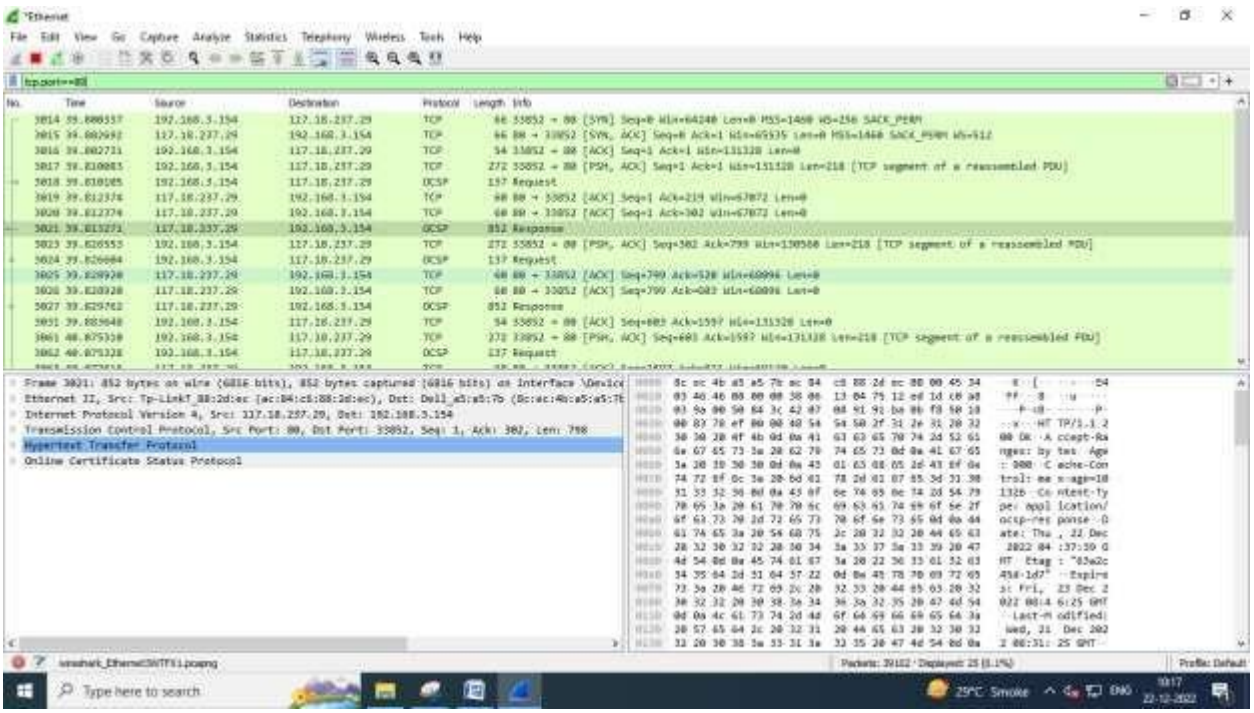
- **tcp**



7. Display packets having no error connecting to server.
   - **http.response.code==200**



8. Display packets having port number 80
   - **tcp.port==80**



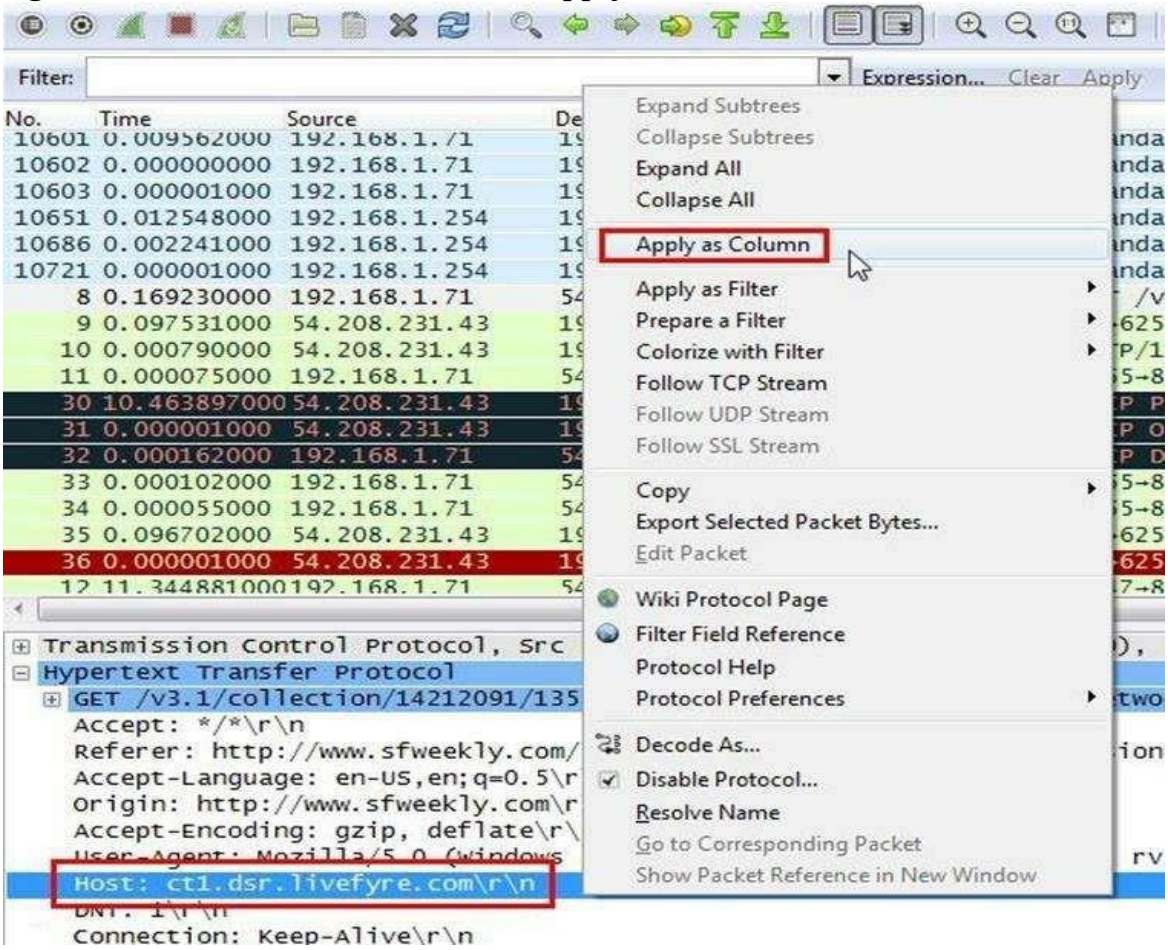
PRACTICAL 5

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?

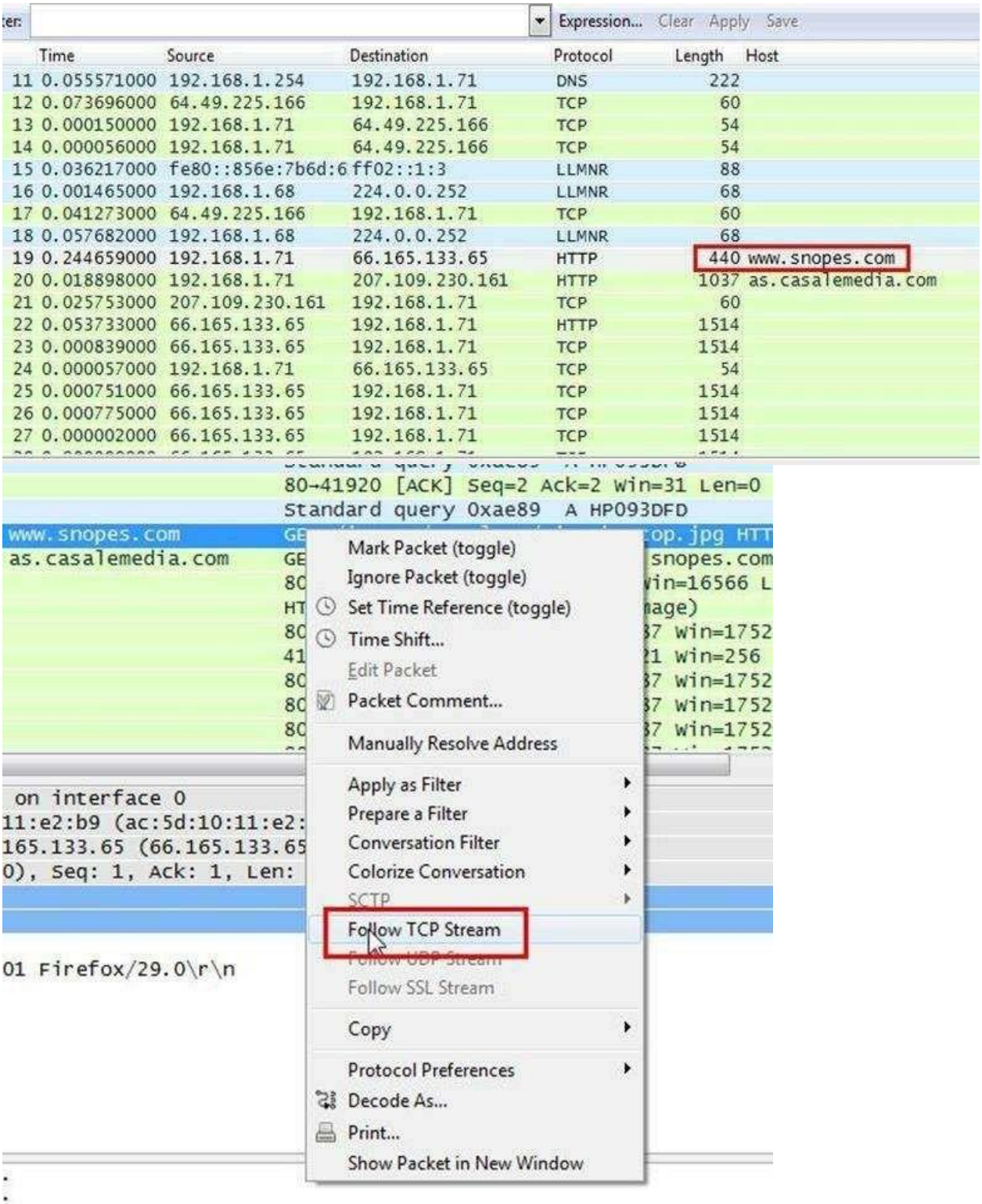
1. What web server software issued by www.snopes.com?

Analysis – The domain name be found from host header so we will set host header column where we will see all domain name. Select any HTTP request and expand the Hypertext Transfer Protocol then right click on Host header and then Apply as Column.



Now we can see our host www.snopes.com in host column.

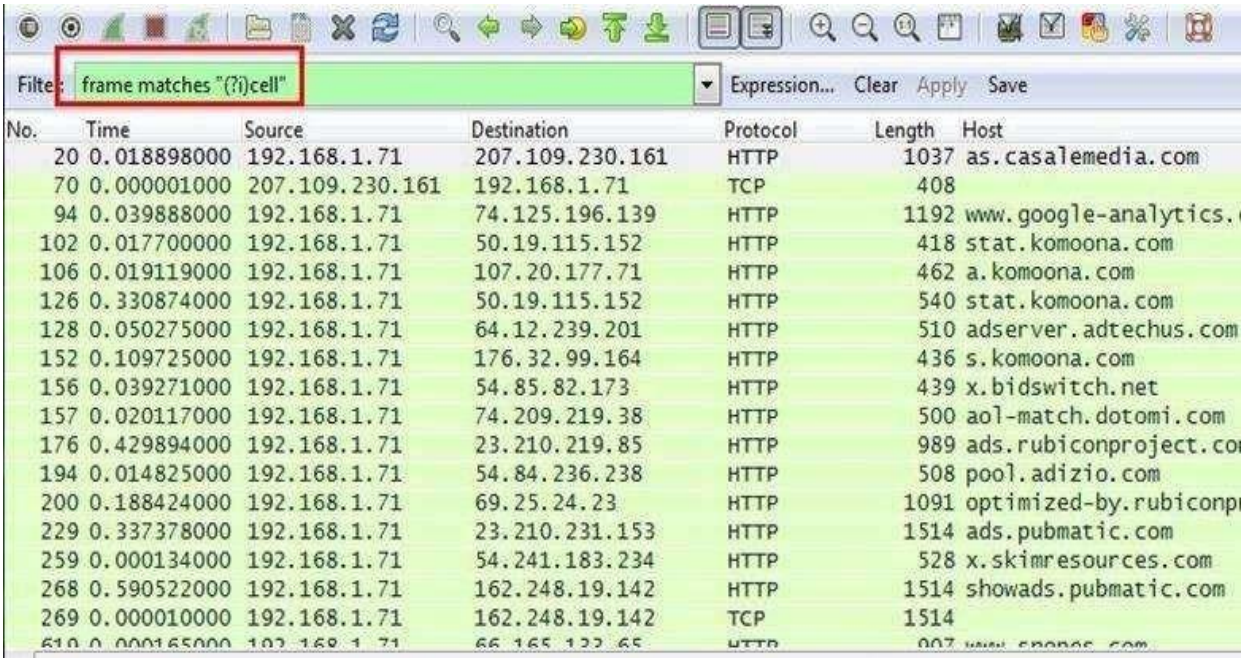
Now we can see the webserver name in server header it is Microsoft IIS 5.0



Stream Content

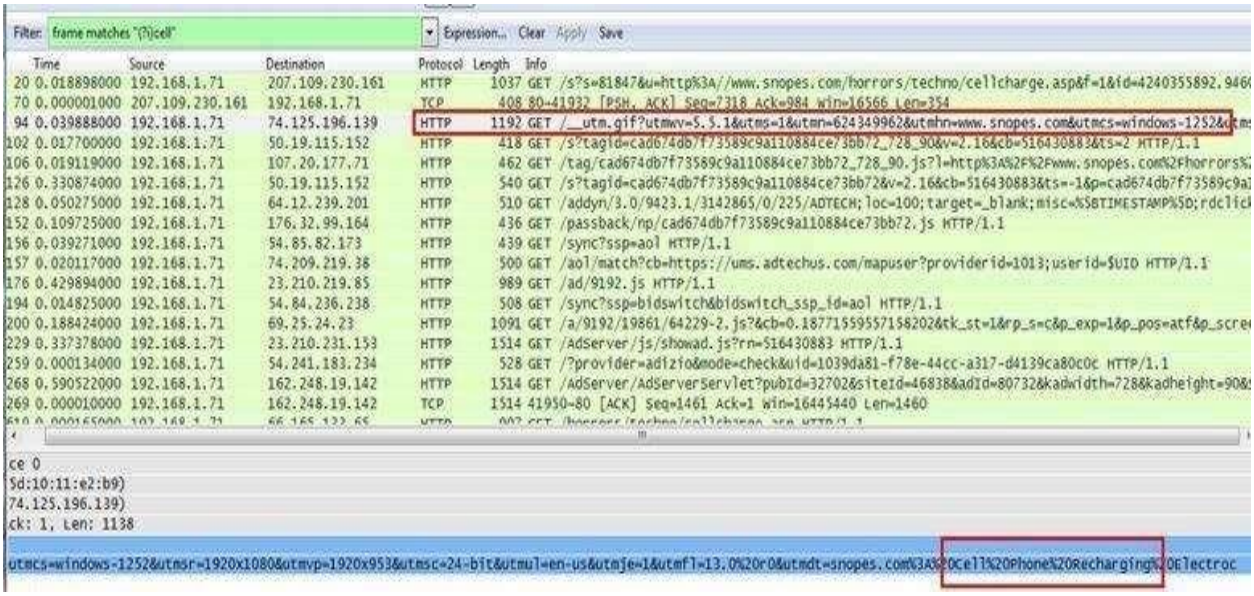
```
GET /images/template/site-bg-top.jpg HTTP/1.1
Host: www.snopes.com
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:29.0) Gecko/2
Accept: image/png,image/*;q=0.8,*/*;q=0.5
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.snopes.com/style.css
Cookie: ASPSESSIONIDQQDDSBBA=OJMBNHECFCANKIJJGBBMBLDO
Connection: keep-alive

HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
Date: Thu, 22 May 2014 01:49:06 GMT
Content-Type: image/jpeg
Accept-Ranges: bytes
Last-Modified: Mon, 03 Nov 2008 04:34:19 GMT
ETag: "98242b706d3dc91:b5f"
Content-Length: 32173

......JFIF.....d.d......Ducky.......U......Adobe.
d.....................................................
```

Analysis – Client talking about cell so we search for cell keyword in whole packets. We will use regular express for searching the cell keyword. Apply frame matches –(?!) cell‖



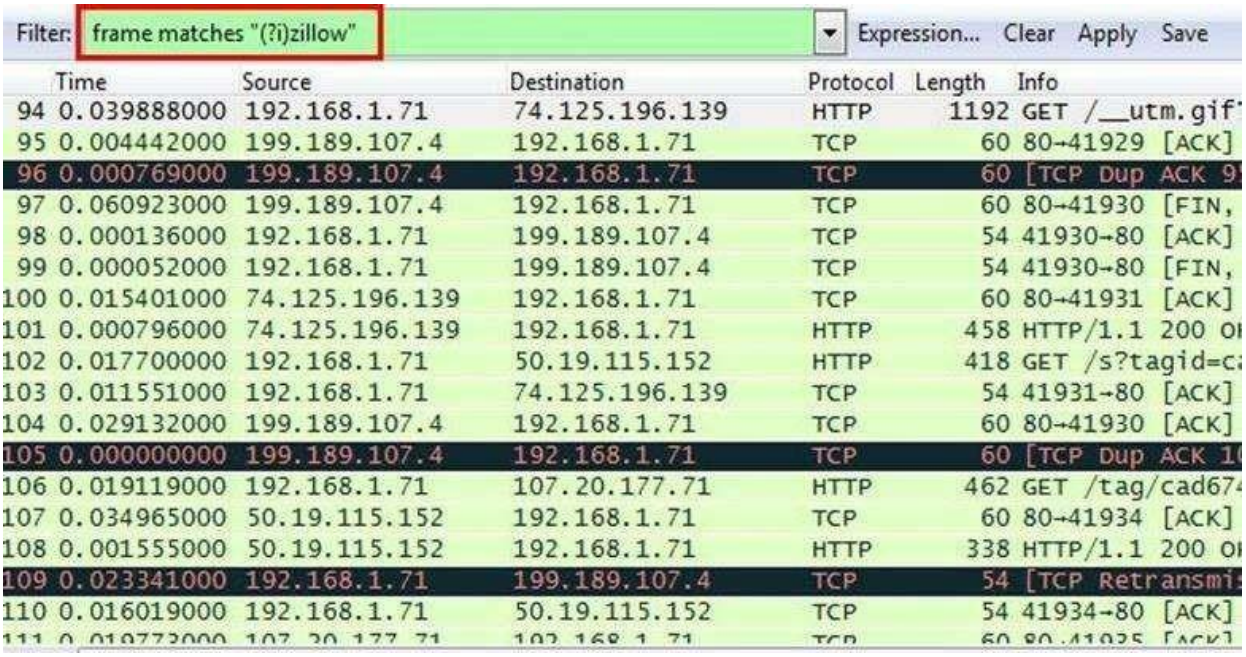
No.	Time	Source	Destination	Protocol	Length	Host
20	0.018898000	192.168.1.71	207.109.230.161	HTTP	1037	as.casalemedia.com
70	0.000001000	207.109.230.161	192.168.1.71	TCP	408	
94	0.039888000	192.168.1.71	74.125.196.139	HTTP	1192	www.google-analytics.
102	0.017700000	192.168.1.71	50.19.115.152	HTTP	418	stat.komoona.com
106	0.019119000	192.168.1.71	107.20.177.71	HTTP	462	a.komoona.com
126	0.330874000	192.168.1.71	50.19.115.152	HTTP	540	stat.komoona.com
128	0.050275000	192.168.1.71	64.12.239.201	HTTP	510	adserver.adtechus.com
152	0.109725000	192.168.1.71	176.32.99.164	HTTP	436	s.komoona.com
156	0.039271000	192.168.1.71	54.85.82.173	HTTP	439	x.bidswitch.net
157	0.020117000	192.168.1.71	74.209.219.38	HTTP	500	aol-match.dotomi.com
176	0.429894000	192.168.1.71	23.210.219.85	HTTP	989	ads.rubiconproject.co
194	0.014825000	192.168.1.71	54.84.236.238	HTTP	508	pool.adizio.com
200	0.188424000	192.168.1.71	69.25.24.23	HTTP	1091	optimized-by.rubiconp
229	0.337378000	192.168.1.71	23.210.231.153	HTTP	1514	ads.pubmatic.com
259	0.000134000	192.168.1.71	54.241.183.234	HTTP	528	x.skimresources.com
268	0.590522000	192.168.1.71	162.248.19.142	HTTP	1514	showads.pubmatic.com
269	0.000010000	192.168.1.71	162.248.19.142	TCP	1514	

After applying the filter now, we will start to check every HTTP request. We noticed in the first HTTP request cell keyword is in URL and it was about cell phone charging issue.



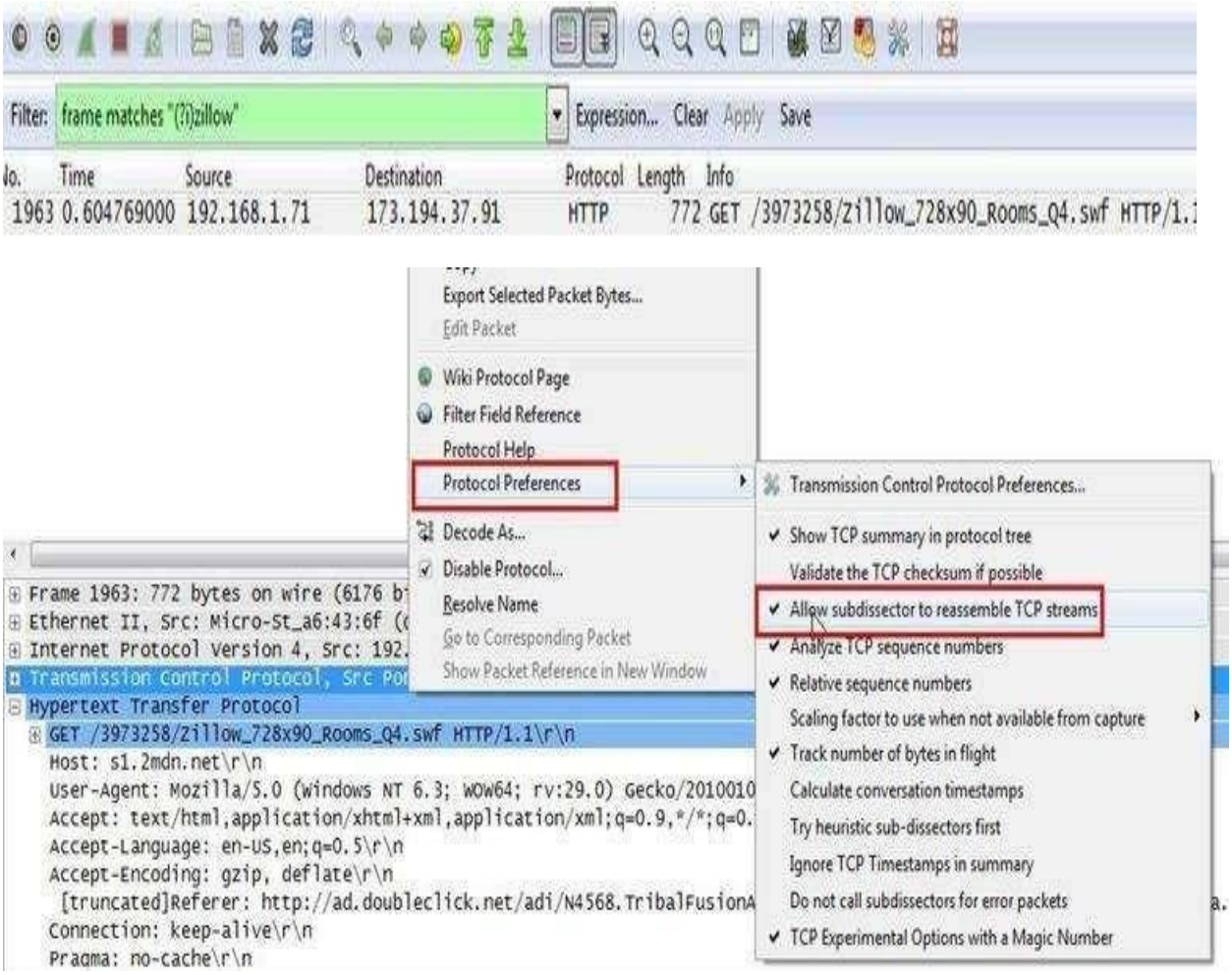
1. According to Zillow, what instrument will Ryan learn to play?

Analysis – As we did in the last challenge, we will apply a regular express filter for the Zillow keyword. Apply frame matched –(?!) zillow‖

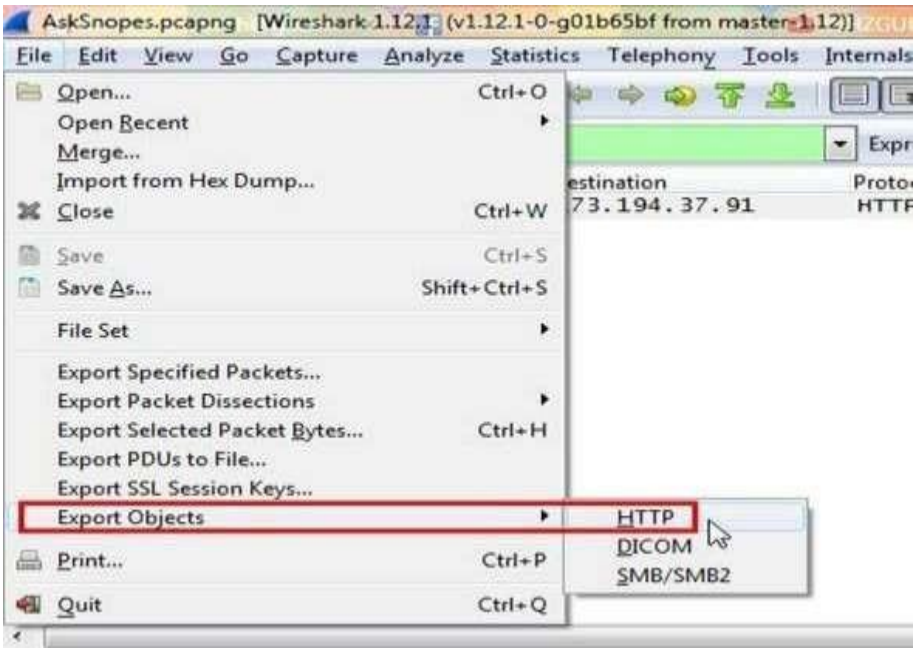


After applying the filter, we found only one packet with the Zillow keyword

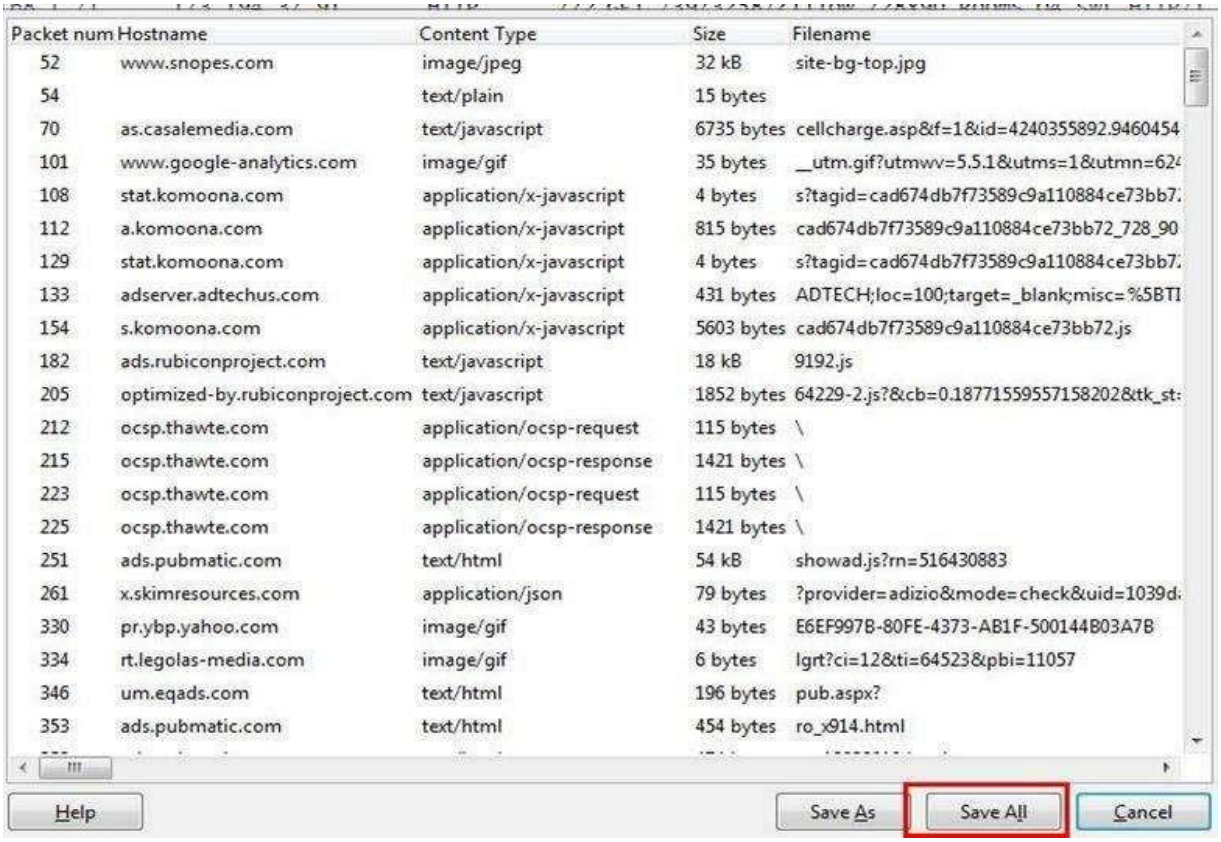
Select the packet and expand the Hypertext Transfer Protocol tab right click on it go to Protocol Preferences and check Allow subdissector to resemble TCP stream



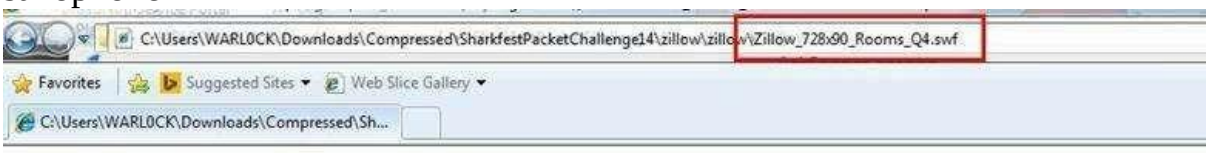
Now go to file and select Export Objects > HTTP. It will save all objects from the packet.



Click on save all.

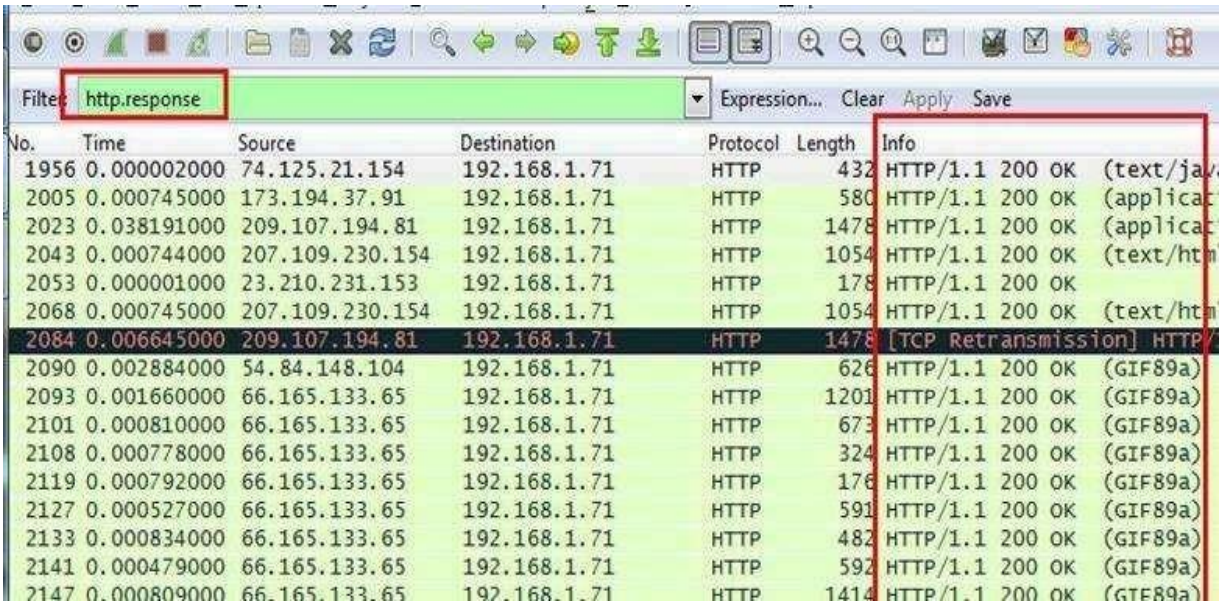


After saving all files in a directory and we found a swf file with name Zillow. After opening the flash file, we saw that Zillow was trying to learn saxophone

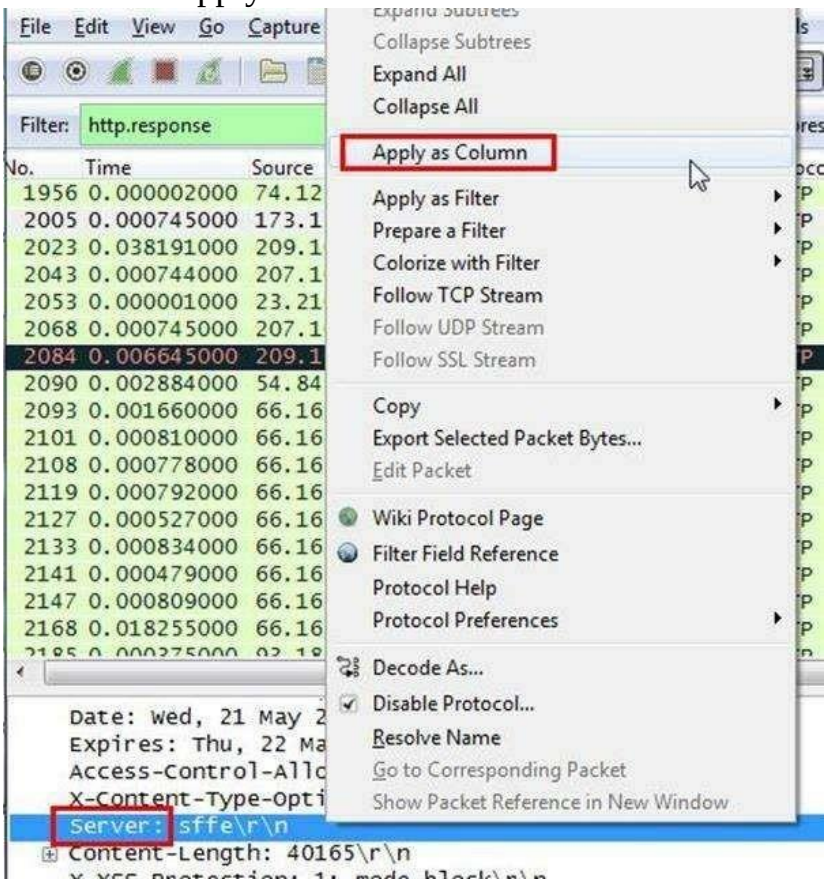


1. How many web servers are running Apache?

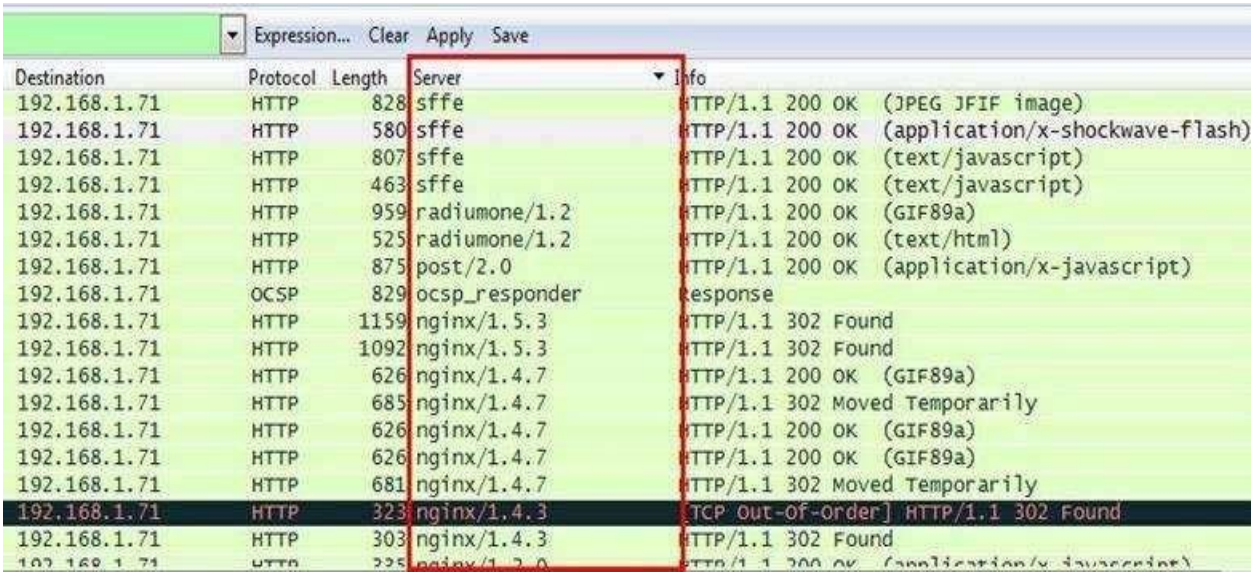
Analysis – The web server name can be retrieved from HTTP response header. So will apply filter http. response and we can see all http response packets.



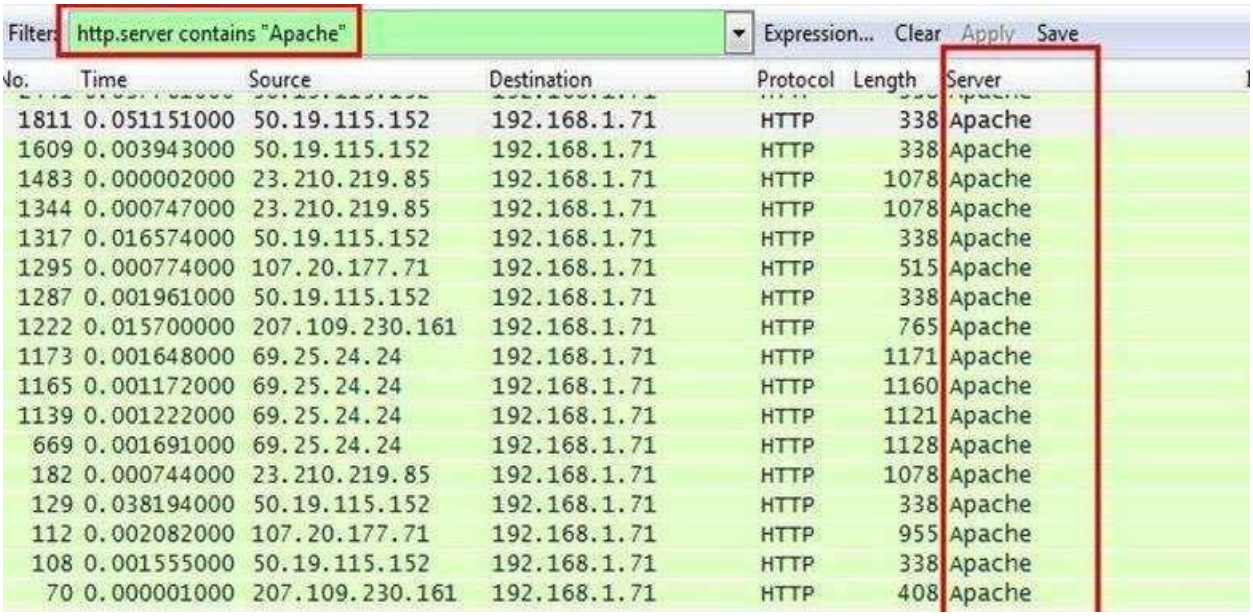
Now we will set the server header as column select any packet and right click on it then select Apply as Column



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

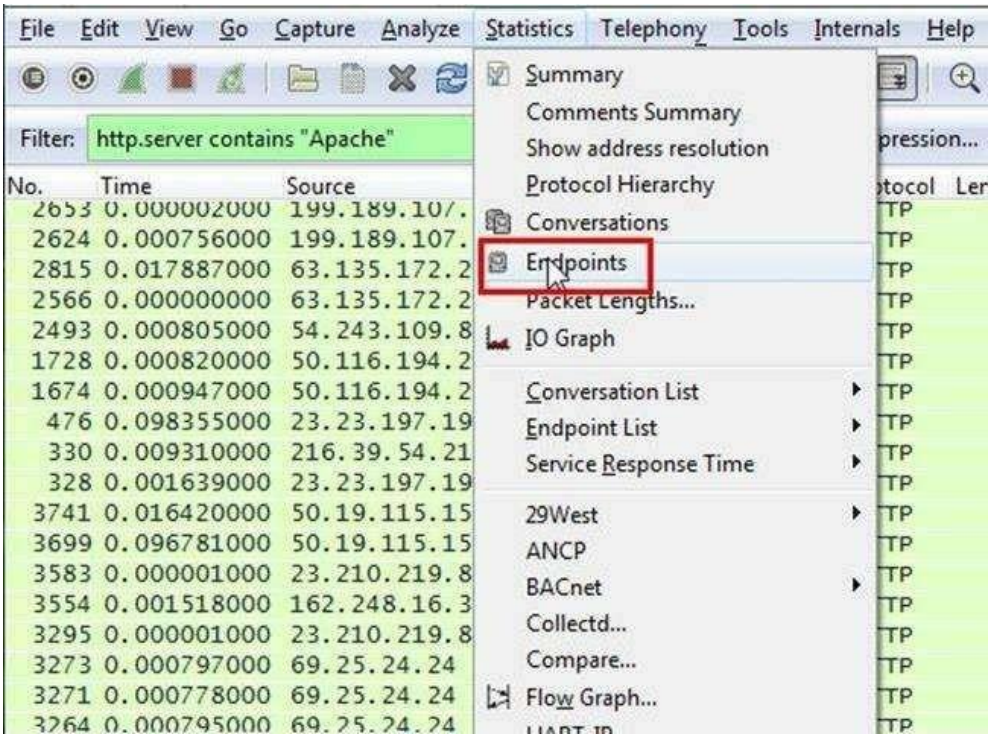


Now we have to check how many Apache packets are there we can't count manually for each packet so we will apply another filter http.server contains –Apache‖

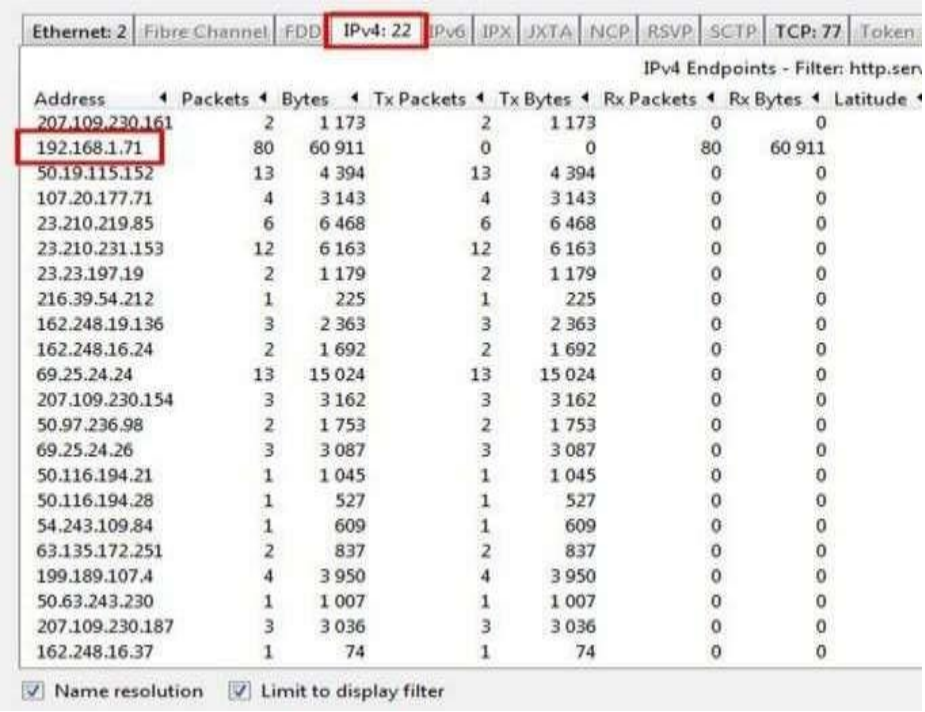


No.	Time	Source	Destination	Protocol	Length	Server
1811	0.051151000	50.19.115.152	192.168.1.71	HTTP	338	Apache
1609	0.003943000	50.19.115.152	192.168.1.71	HTTP	338	Apache
1483	0.000002000	23.210.219.85	192.168.1.71	HTTP	1078	Apache
1344	0.000747000	23.210.219.85	192.168.1.71	HTTP	1078	Apache
1317	0.016574000	50.19.115.152	192.168.1.71	HTTP	338	Apache
1295	0.000774000	107.20.177.71	192.168.1.71	HTTP	515	Apache
1287	0.001961000	50.19.115.152	192.168.1.71	HTTP	338	Apache
1222	0.015700000	207.109.230.161	192.168.1.71	HTTP	765	Apache
1173	0.001648000	69.25.24.24	192.168.1.71	HTTP	1171	Apache
1165	0.001172000	69.25.24.24	192.168.1.71	HTTP	1160	Apache
1139	0.001222000	69.25.24.24	192.168.1.71	HTTP	1121	Apache
669	0.001691000	69.25.24.24	192.168.1.71	HTTP	1128	Apache
182	0.000744000	23.210.219.85	192.168.1.71	HTTP	1078	Apache
129	0.038194000	50.19.115.152	192.168.1.71	HTTP	338	Apache
112	0.002082000	107.20.177.71	192.168.1.71	HTTP	955	Apache
108	0.001555000	50.19.115.152	192.168.1.71	HTTP	338	Apache
70	0.000001000	207.109.230.161	192.168.1.71	HTTP	408	Apache

After applying filter go to Statistics > Endpoints



It will show all connections



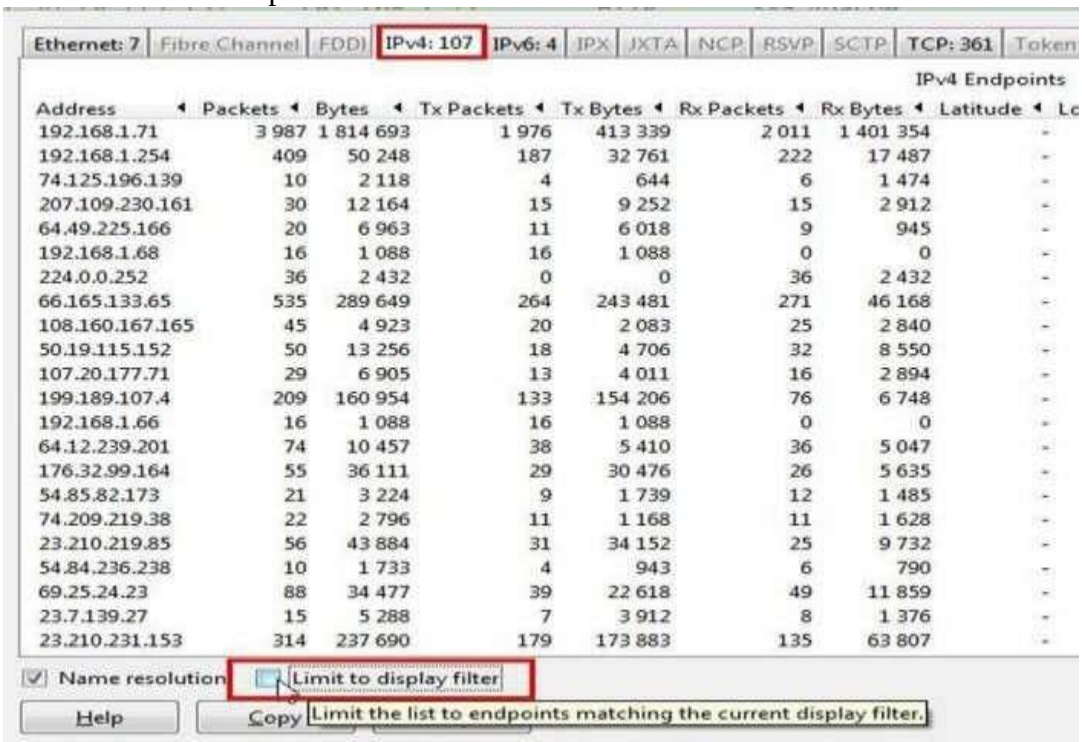
Ethernet: 2 | Fibre Channel | FDDI | IPv4: 22 | IPv6 | IPX | JXTA | NCP | RSVP | SCTP | TCP: 77 | Token

IPv4 Endpoints - Filter: http.ser

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Latitude
207.109.230.161	2	1 173	2	1 173	0	0	
192.168.1.71	80	60 911	0	0	80	60 911	
50.19.115.152	13	4 394	13	4 394	0	0	
107.20.177.71	4	3 143	4	3 143	0	0	
23.210.219.85	6	6 468	6	6 468	0	0	
23.210.231.153	12	6 163	12	6 163	0	0	
23.23.197.19	2	1 179	2	1 179	0	0	
216.39.54.212	1	225	1	225	0	0	
162.248.19.136	3	2 363	3	2 363	0	0	
162.248.16.24	2	1 692	2	1 692	0	0	
69.25.24.24	13	15 024	13	15 024	0	0	
207.109.230.154	3	3 162	3	3 162	0	0	
50.97.236.98	2	1 753	2	1 753	0	0	
69.25.24.26	3	3 087	3	3 087	0	0	
50.116.194.21	1	1 045	1	1 045	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	
199.189.107.4	4	3 950	4	3 950	0	0	
50.63.243.230	1	1 007	1	1 007	0	0	
207.109.230.187	3	3 036	3	3 036	0	0	
162.248.16.37	1	74	1	74	0	0	

Name resolution | Limit to display filter

Check the limit to display filter then it will show the actual Apache connections. Now there are showing 22 connections but will exclude 192.168.1.71 because it is client's IP not a server IP so there are actual 21 Apache servers..



Ethernet: 7 | Fibre Channel | FDDI | IPv4: 107 | IPv6: 4 | IPX | JXTA | NCP | RSVP | SCTP | TCP: 361 | Token

IPv4 Endpoints

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Latitude	Lo
192.168.1.71	3 987	1 814 693	1 976	413 339	2 011	1 401 354	-	
192.168.1.254	409	50 248	187	32 761	222	17 487	-	
74.125.196.139	10	2 118	4	644	6	1 474	-	
207.109.230.161	30	12 164	15	9 252	15	2 912	-	
64.49.225.166	20	6 963	11	6 018	9	945	-	
192.168.1.68	16	1 088	16	1 088	0	0	-	
224.0.0.252	36	2 432	0	0	36	2 432	-	
66.165.133.65	535	289 649	264	243 481	271	46 168	-	
108.160.167.165	45	4 923	20	2 083	25	2 840	-	
50.19.115.152	50	13 256	18	4 706	32	8 550	-	
107.20.177.71	29	6 905	13	4 011	16	2 894	-	
199.189.107.4	209	160 954	133	154 206	76	6 748	-	
192.168.1.66	16	1 088	16	1 088	0	0	-	
64.12.239.201	74	10 457	38	5 410	36	5 047	-	
176.32.99.164	55	36 111	29	30 476	26	5 635	-	
54.85.82.173	21	3 224	9	1 739	12	1 485	-	
74.209.219.38	22	2 796	11	1 168	11	1 628	-	
23.210.219.85	56	43 884	31	34 152	25	9 732	-	
54.84.236.238	10	1 733	4	943	6	790	-	
69.25.24.23	88	34 477	39	22 618	49	11 859	-	
23.7.139.27	15	5 288	7	3 912	8	1 376	-	
23.210.231.153	314	237 690	179	173 883	135	63 807	-	

Name resolution | Limit to display filter

Help | Copy | Limit the list to endpoints matching the current display filter.

CONCLUSION: We have successfully analyzed the packets provided and solved the questions using wireshark.

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

Check Sysinternals tools : Windows Sysinternals tools are utilities to manage, diagnose, troubleshoot, and monitor a Microsoft Windows environment.

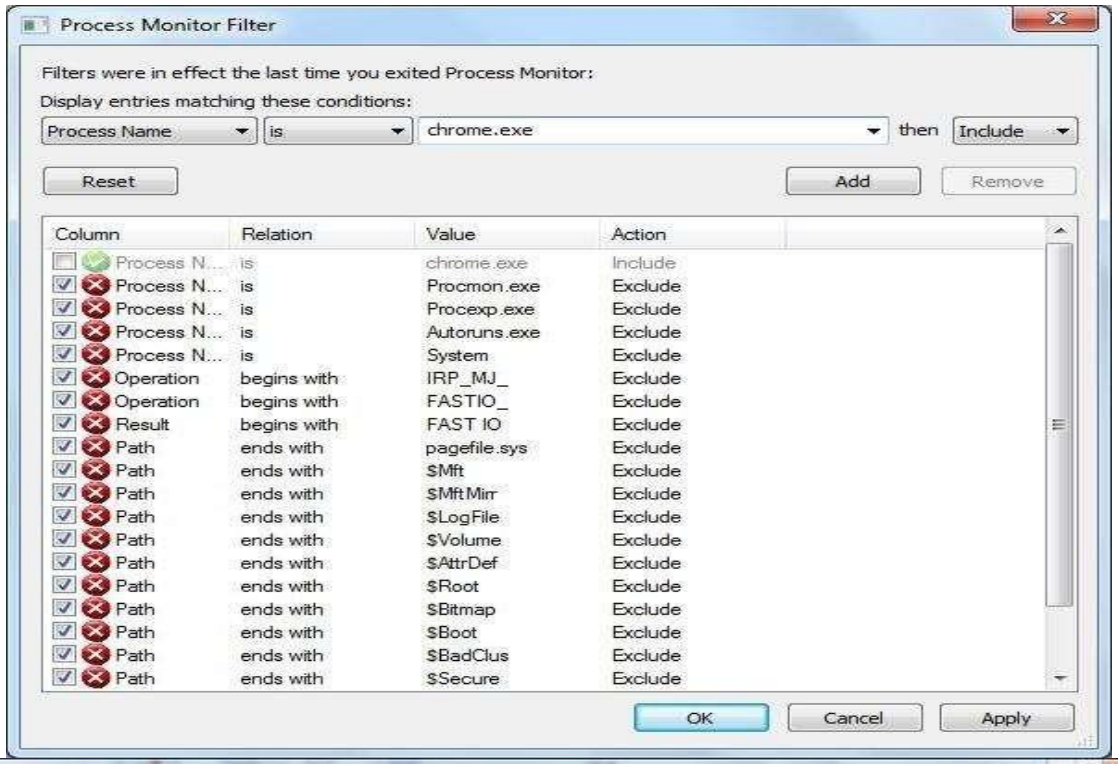
The following are the categories of Sysinternals Tools:

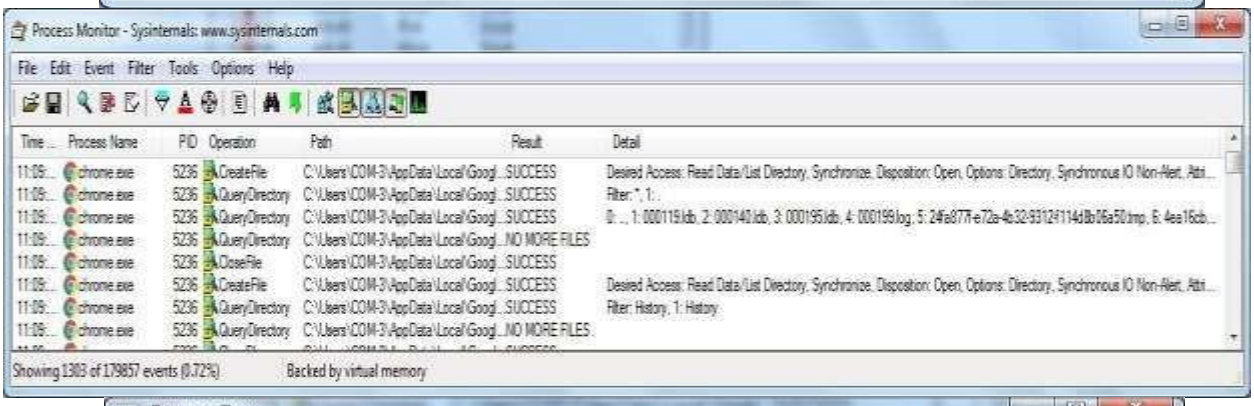
1. File and Disk Utilities
2. Networking Utilities
3. Process Utilities
4. Security Utilities
5. System Information Utilities
6. Miscellaneous Utilities

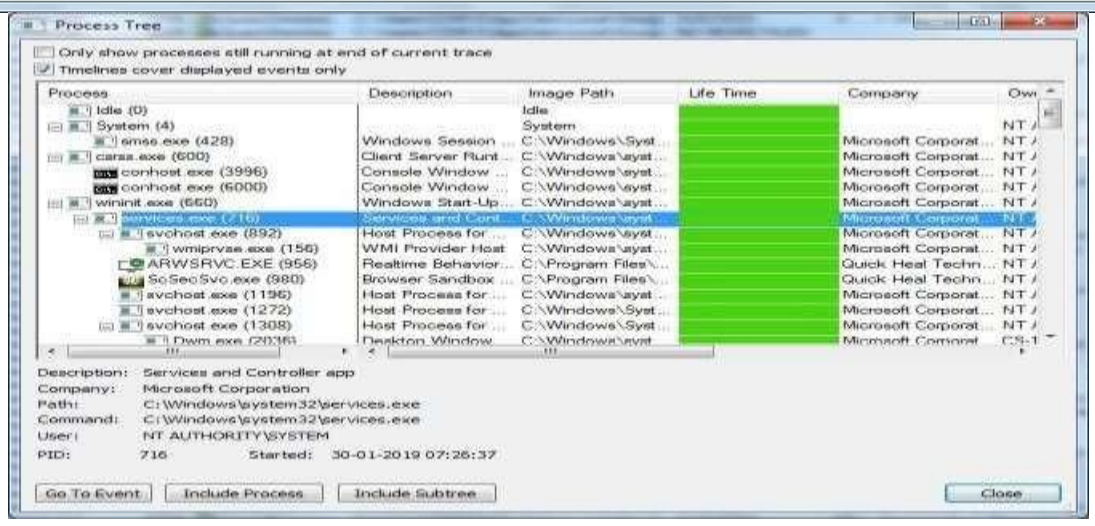
- **Monitor Live Processes :**
  (Tool: ProcMon) To Do:

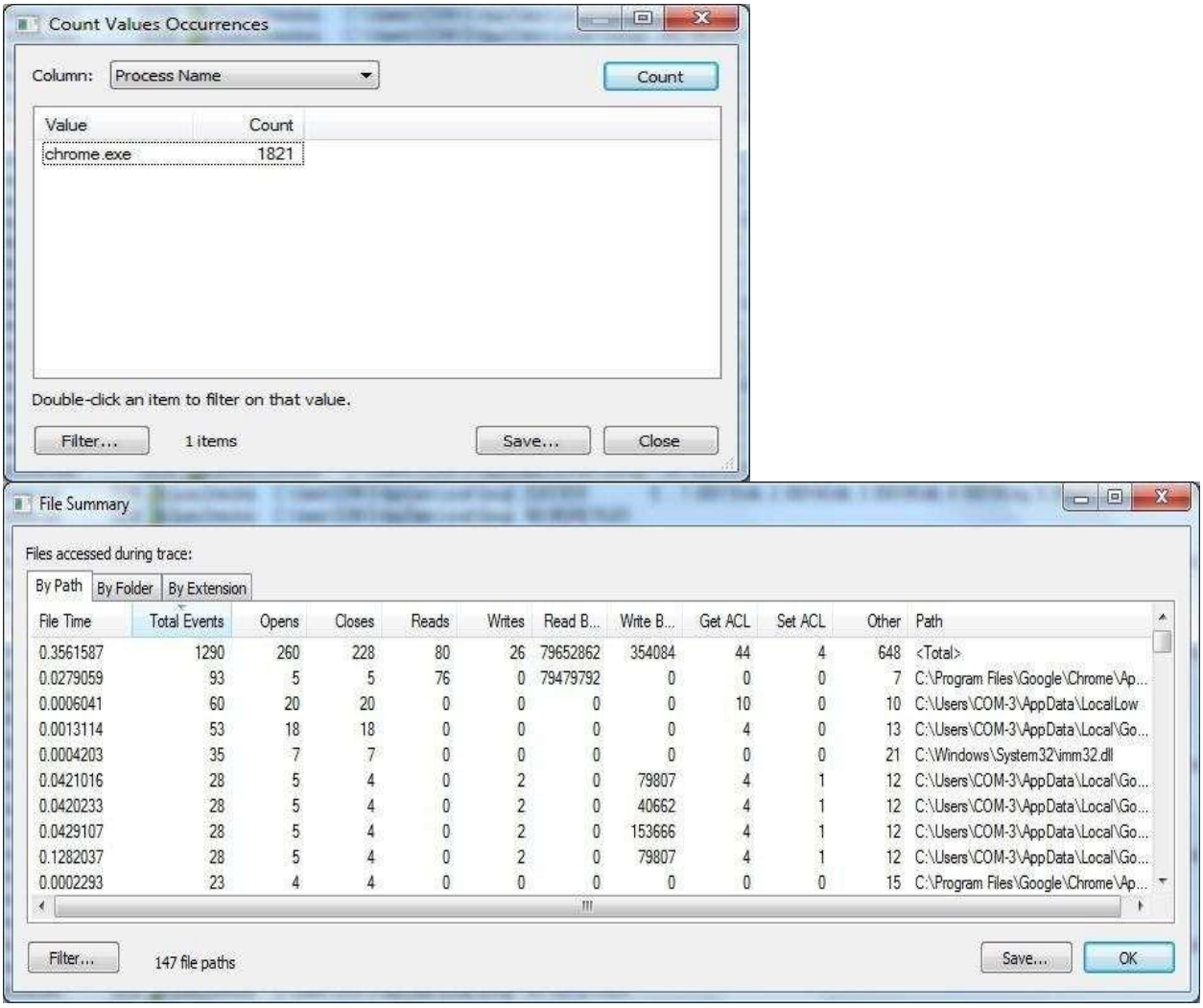
1. Filter (Process Name or PID or Architecture, etc)
2. Process Tree
3. Process Activity Summary
4. Count Occurrences

Output:


Process Monitor Filter
Filters were in effect the last time you exited Process Monitor:
Display entries matching these conditions:
Process Name
is
chrome.exe
then
Include
Reset
Add
Remove
Column
Relation
Value
Action
Process N... is chrome.exe Include
Process N... is Procmon.exe Exclude
Process N... is Procexp.exe Exclude
Process N... is Autoruns.exe Exclude
Process N... is System Exclude
Operation begins with IRP_MJ_ Exclude
Operation begins with FASTIO_ Exclude
Result begins with FAST IO Exclude
Path ends with pagefile.sys Exclude
Path ends with $Mft Exclude
Path ends with $MftMirr Exclude
Path ends with $LogFile Exclude
Path ends with $Volume Exclude
Path ends with $AttrDef Exclude
Path ends with $Root Exclude
Path ends with $Bitmap Exclude
Path ends with $Boot Exclude
Path ends with $BadClus Exclude
Path ends with $Secure Exclude
OK
Cancel
Apply


Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Time ... Process Name PID Operation Path Result Detail
Showing 1303 of 179857 events (0.72%)
Backed by virtual memory


Process Tree
Only show processes still running at end of current trace
Timelines cover displayed events only
Process
Description
Image Path
Life Time
Company
Description: Services and Controller app
Company: Microsoft Corporation
Path: C:\Windows\system32\services.exe
Command: C:\Windows\system32\services.exe
User: NT AUTHORITY\SYSTEM
PID: 716 Started: 30-01-2019 07:26:37
Go To Event
Include Process
Include Subtree
Close

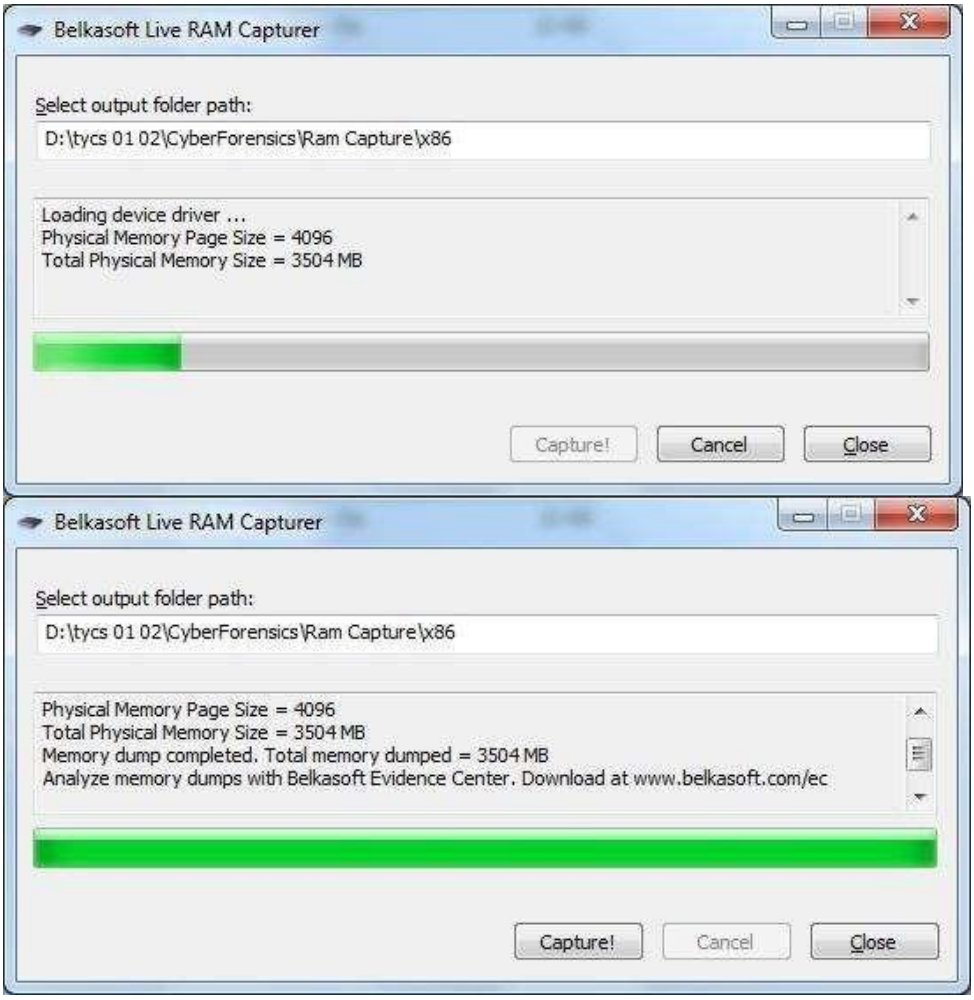


- **Capture RAM (Tool: RAMCapture)**

To Do:

1. Click Capture
2. Creates a .mem file of the system memory (RAM) utilized.

Output:

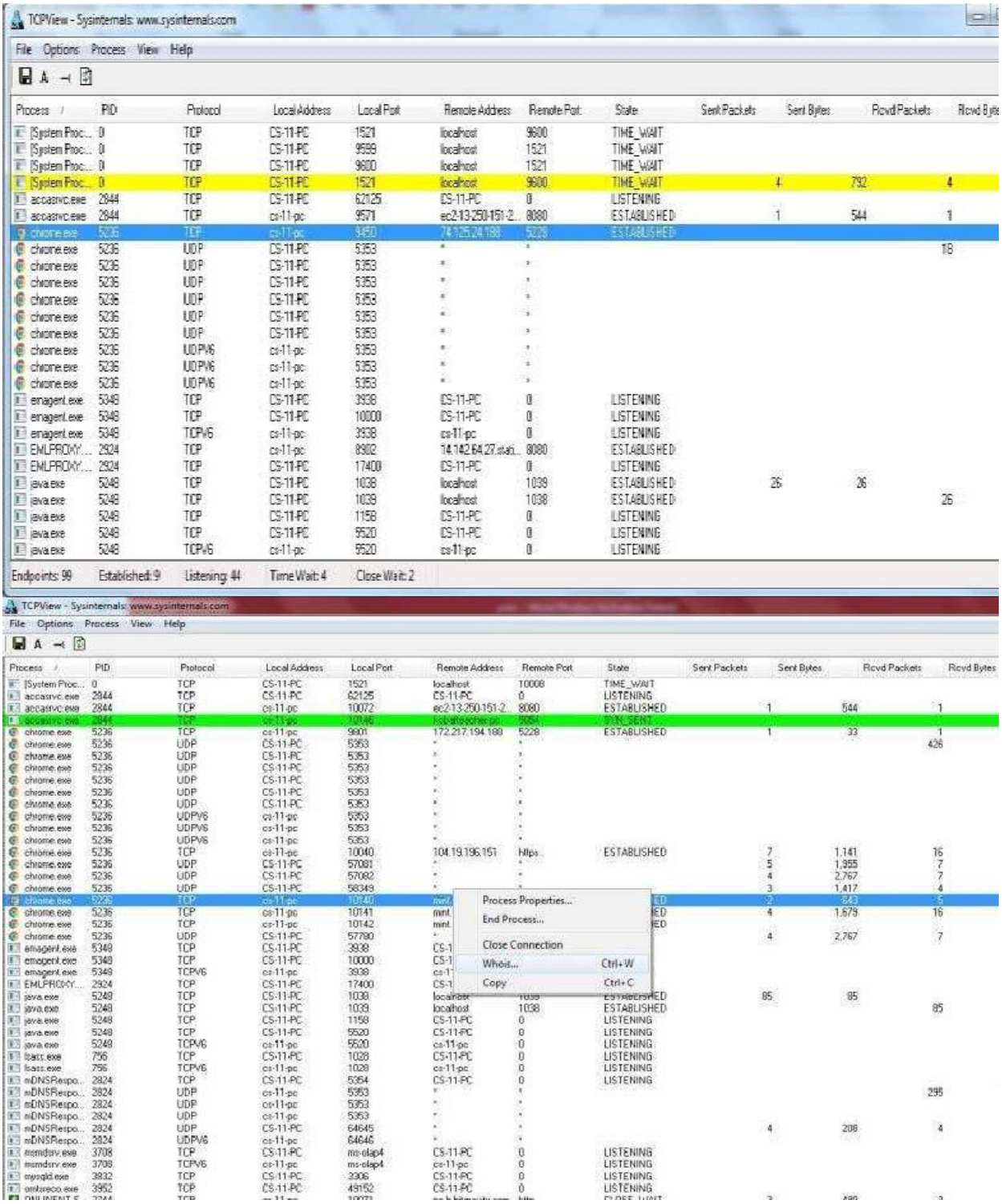


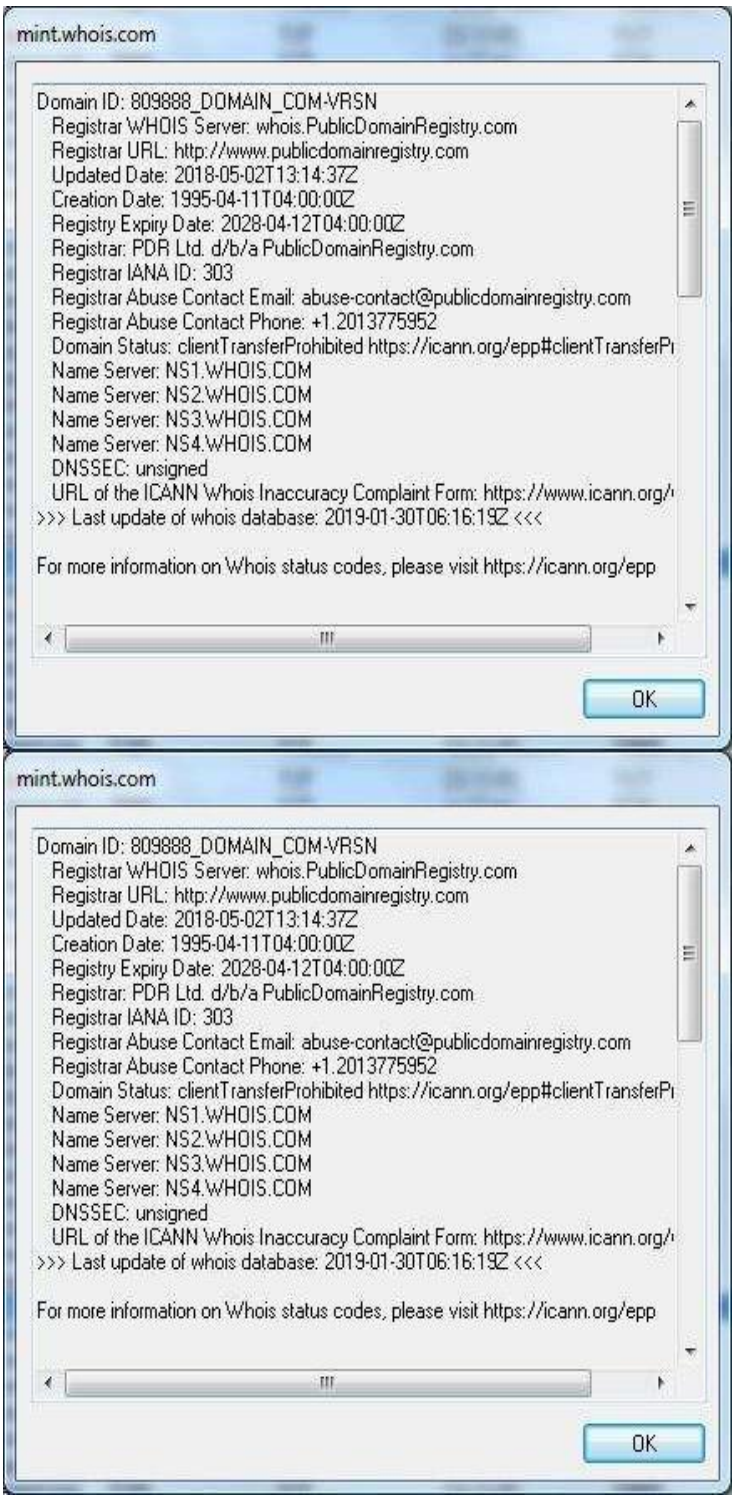
- **Capture TCP/UDP packets (Tool: TcpView) :**

To Do: 1. Save to .txt file.

2. Whois

Output:


TCPView - Sysinternals: www.sysinternals.com
File Options Process View Help
Process PID Protocol Local Address Local Port Remote Address Remote Port State Sent Packets Sent Bytes Rcvd Packets Rcvd Bytes
[System Proc... 0 TCP CS-11-PC 1521 localhost 9600 TIME_WAIT
[System Proc... 0 TCP CS-11-PC 9599 localhost 1521 TIME_WAIT
[System Proc... 0 TCP CS-11-PC 9600 localhost 1521 TIME_WAIT
[System Proc... 0 TCP CS-11-PC 1521 localhost 9600 TIME_WAIT 4 792 4
accasrvc.exe 2844 TCP CS-11-PC 62125 CS-11-PC 0 LISTENING
accasrvc.exe 2844 TCP cs-11-pc 9571 ec2-13-250-151-2... 8080 ESTABLISHED 1 544 1
chrome.exe 5236 TCP cs-11-pc 9450 74.125.24.188 5228 ESTABLISHED
chrome.exe 5236 UDP CS-11-PC 5353 * * 18
chrome.exe 5236 UDP CS-11-PC 5353 * *
chrome.exe 5236 UDP CS-11-PC 5353 * *
chrome.exe 5236 UDP CS-11-PC 5353 * *
chrome.exe 5236 UDP CS-11-PC 5353 * *
chrome.exe 5236 UDP CS-11-PC 5353 * *
chrome.exe 5236 UDPV6 cs-11-pc 5353 * *
chrome.exe 5236 UDPV6 cs-11-pc 5353 * *
chrome.exe 5236 UDPV6 cs-11-pc 5353 * *
emagent.exe 5348 TCP CS-11-PC 3938 CS-11-PC 0 LISTENING
emagent.exe 5348 TCP CS-11-PC 10000 CS-11-PC 0 LISTENING
emagent.exe 5348 TCPV6 cs-11-pc 3938 cs-11-pc 0 LISTENING
EMLPROXY... 2924 TCP cs-11-pc 8902 74.142.64.27.stati... 8080 ESTABLISHED
EMLPROXY... 2924 TCP CS-11-PC 17400 CS-11-PC 0 LISTENING
java.exe 5248 TCP CS-11-PC 1038 localhost 1039 ESTABLISHED 26 26
java.exe 5248 TCP CS-11-PC 1039 localhost 1038 ESTABLISHED 26
java.exe 5248 TCP CS-11-PC 1158 CS-11-PC 0 LISTENING
java.exe 5248 TCP CS-11-PC 5520 CS-11-PC 0 LISTENING
java.exe 5248 TCPV6 cs-11-pc 5520 cs-11-pc 0 LISTENING
Endpoints: 99 Established: 9 Listening: 44 Time Wait: 4 Close Wait: 2
TCPView - Sysinternals: www.sysinternals.com
File Options Process View Help
Process PID Protocol Local Address Local Port Remote Address Remote Port State Sent Packets Sent Bytes Rcvd Packets Rcvd Bytes
[System Proc... 0 TCP CS-11-PC 1521 localhost 10008 TIME_WAIT
accasrvc.exe 2844 TCP CS-11-PC 62125 CS-11-PC 0 LISTENING
accasrvc.exe 2844 TCP cs-11-pc 10072 ec2-13-250-151-2... 8080 ESTABLISHED 1 544 1
chrome.exe 5236 TCP cs-11-pc 9901 172.217.194.188 5228 ESTABLISHED 1 33 1
chrome.exe 5236 UDP CS-11-PC 5353 * * 426
chrome.exe 5236 UDP CS-11-PC 5353 * *
chrome.exe 5236 UDP CS-11-PC 5353 * *
chrome.exe 5236 UDP CS-11-PC 5353 * *
chrome.exe 5236 UDP CS-11-PC 5353 * *
chrome.exe 5236 UDP CS-11-PC 5353 * *
chrome.exe 5236 UDPV6 cs-11-pc 5353 * *
chrome.exe 5236 UDPV6 cs-11-pc 5353 * *
chrome.exe 5236 UDPV6 cs-11-pc 5353 * *
chrome.exe 5236 TCP cs-11-pc 10040 104.19.196.151 https ESTABLISHED 7 1,141 16
chrome.exe 5236 UDP CS-11-PC 57081 * * 5 1,955 7
chrome.exe 5236 UDP CS-11-PC 57082 * * 4 2,767 7
chrome.exe 5236 UDP CS-11-PC 58349 * * 3 1,417 4
chrome.exe 5236 TCP cs-11-pc 10140 mrl... ED 2 843 5
chrome.exe 5236 TCP cs-11-pc 10141 mrl... ED 4 1,679 16
chrome.exe 5236 TCP cs-11-pc 10142 mrl... ED
chrome.exe 5236 UDP CS-11-PC 57780 * * 4 2,767 7
emagent.exe 5348 TCP CS-11-PC 3938 CS-11-PC 0 LISTENING
emagent.exe 5348 TCP CS-11-PC 10000 CS-11-PC 0 LISTENING
emagent.exe 5348 TCPV6 cs-11-pc 3938 cs-11-pc 0 LISTENING
EMLPROXY... 2924 TCP CS-11-PC 17400 CS-11-PC 0 LISTENING
java.exe 5248 TCP CS-11-PC 1038 localhost 1039 ESTABLISHED 85 85
java.exe 5248 TCP CS-11-PC 1039 localhost 1038 ESTABLISHED 85
java.exe 5248 TCP CS-11-PC 1158 CS-11-PC 0 LISTENING
java.exe 5248 TCP CS-11-PC 5520 CS-11-PC 0 LISTENING
java.exe 5248 TCPV6 cs-11-pc 5520 cs-11-pc 0 LISTENING
lsass.exe 756 TCP CS-11-PC 1028 CS-11-PC 0 LISTENING
lsass.exe 756 TCPV6 cs-11-pc 1028 cs-11-pc 0 LISTENING
mDNSRespo... 2824 TCP CS-11-PC 5354 CS-11-PC 0 LISTENING
mDNSRespo... 2824 UDP cs-11-pc 5353 * * 295
mDNSRespo... 2824 UDP cs-11-pc 5353 * *
mDNSRespo... 2824 UDP cs-11-pc 5353 * *
mDNSRespo... 2824 UDP CS-11-PC 64645 * * 4 208 4
mDNSRespo... 2824 UDPV6 cs-11-pc 64645 * *
msmdsrv.exe 3708 TCP CS-11-PC ms-olap4 CS-11-PC 0 LISTENING
msmdsrv.exe 3708 TCPV6 cs-11-pc ms-olap4 cs-11-pc 0 LISTENING
mysqld.exe 3932 TCP CS-11-PC 3306 CS-11-PC 0 LISTENING
omtsreco.exe 3952 TCP CS-11-PC 49152 CS-11-PC 0 LISTENING
Process Properties...
End Process...
Close Connection
Whois... Ctrl+W
Copy Ctrl+C

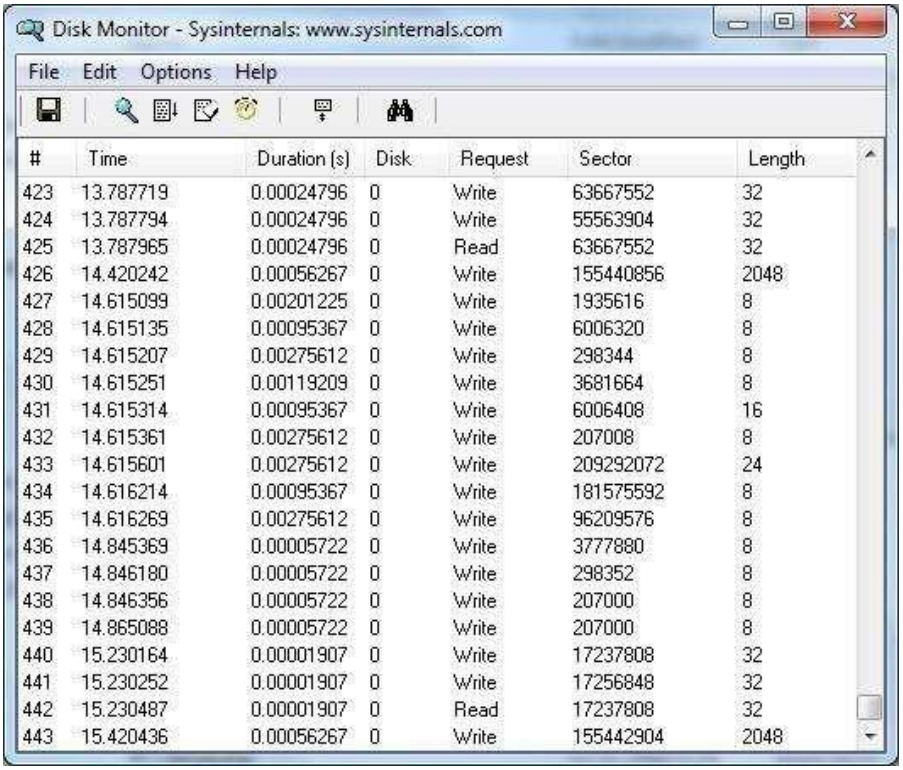

mint.whois.com
Domain ID: 809888_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.PublicDomainRegistry.com
Registrar URL: http://www.publicdomainregistry.com
Updated Date: 2018-05-02T13:14:37Z
Creation Date: 1995-04-11T04:00:00Z
Registry Expiry Date: 2028-04-12T04:00:00Z
Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com
Registrar IANA ID: 303
Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com
Registrar Abuse Contact Phone: +1.2013775952
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferPr
Name Server: NS1.WHOIS.COM
Name Server: NS2.WHOIS.COM
Name Server: NS3.WHOIS.COM
Name Server: NS4.WHOIS.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/
>>> Last update of whois database: 2019-01-30T06:16:19Z <<<
For more information on Whois status codes, please visit https://icann.org/epp
OK
mint.whois.com
Domain ID: 809888_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.PublicDomainRegistry.com
Registrar URL: http://www.publicdomainregistry.com
Updated Date: 2018-05-02T13:14:37Z
Creation Date: 1995-04-11T04:00:00Z
Registry Expiry Date: 2028-04-12T04:00:00Z
Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com
Registrar IANA ID: 303
Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com
Registrar Abuse Contact Phone: +1.2013775952
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferPr
Name Server: NS1.WHOIS.COM
Name Server: NS2.WHOIS.COM
Name Server: NS3.WHOIS.COM
Name Server: NS4.WHOIS.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/
>>> Last update of whois database: 2019-01-30T06:16:19Z <<<
For more information on Whois status codes, please visit https://icann.org/epp
OK

- **Monitor Hard Disk (Tool: DiskMon) :**

To Do:

1. Save to .log file.
2. Check operations performed in the disk as per time and sectors affected.

Output :



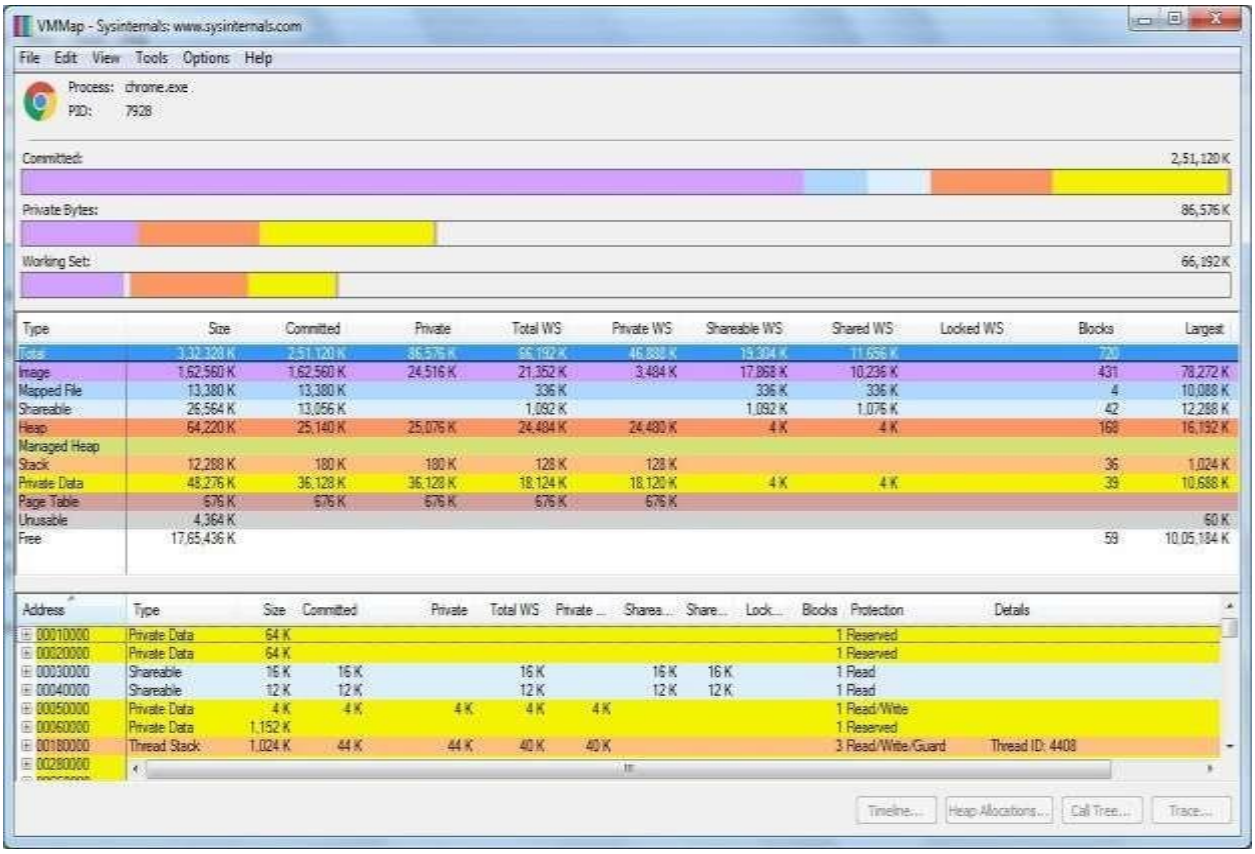
#	Time	Duration (s)	Disk	Request	Sector	Length
423	13.787719	0.00024796	0	Write	63667552	32
424	13.787794	0.00024796	0	Write	55563904	32
425	13.787965	0.00024796	0	Read	63667552	32
426	14.420242	0.00056267	0	Write	155440856	2048
427	14.615099	0.00201225	0	Write	1935616	8
428	14.615135	0.00095367	0	Write	6006320	8
429	14.615207	0.00275612	0	Write	298344	8
430	14.615251	0.00119209	0	Write	3681664	8
431	14.615314	0.00095367	0	Write	6006408	16
432	14.615361	0.00275612	0	Write	207008	8
433	14.615601	0.00275612	0	Write	209292072	24
434	14.616214	0.00095367	0	Write	181575592	8
435	14.616269	0.00275612	0	Write	96209576	8
436	14.845369	0.00005722	0	Write	3777880	8
437	14.846180	0.00005722	0	Write	298352	8
438	14.846356	0.00005722	0	Write	207000	8
439	14.865088	0.00005722	0	Write	207000	8
440	15.230164	0.00001907	0	Write	17237808	32
441	15.230252	0.00001907	0	Write	17256848	32
442	15.230487	0.00001907	0	Read	17237808	32
443	15.420436	0.00056267	0	Write	155442904	2048

- **Monitor Virtual Memory (Tool : VMMAP) :**

To Do:

1. Options – Show Free & Unusable Regions
2. File-> Select Process e.g. chrome.exe
3. Save to .mmp file.

Output :

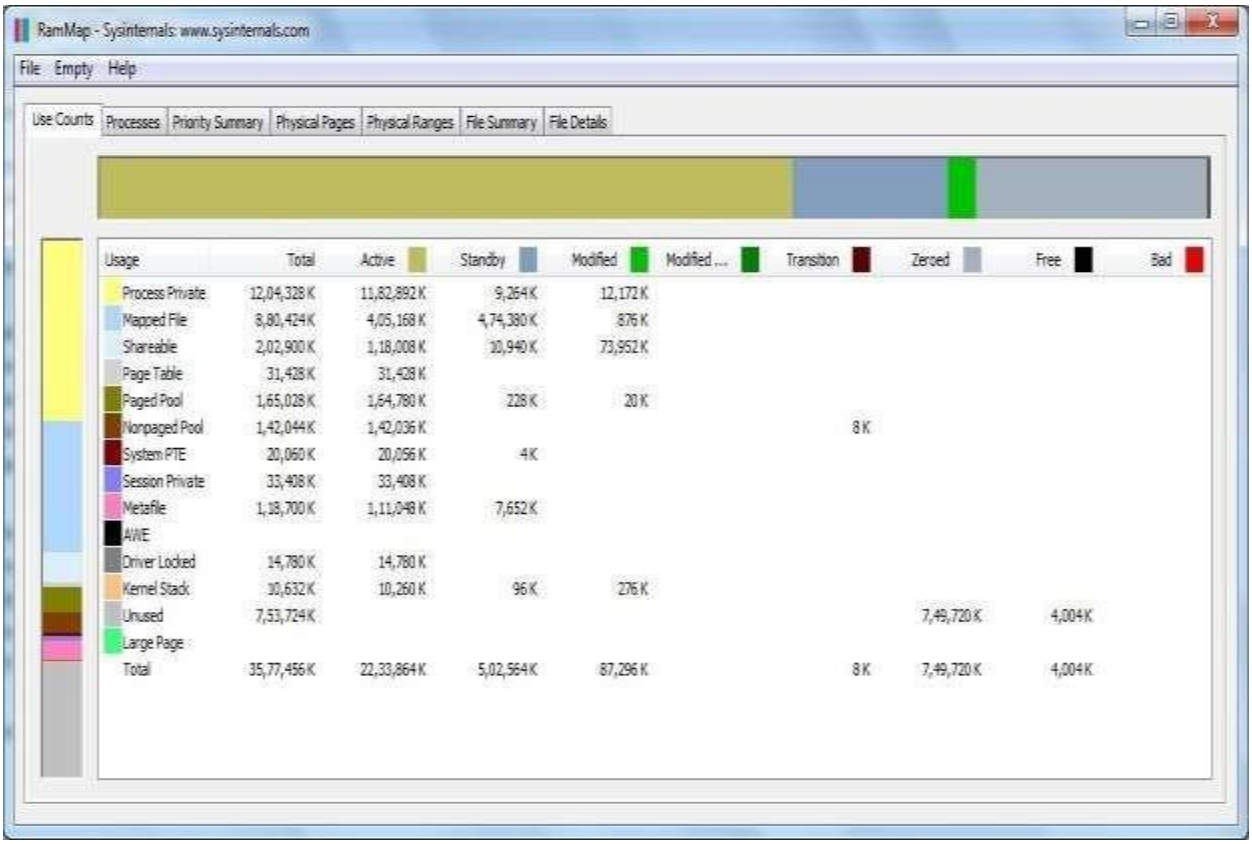


- **Monitor Cache Memory (Tool: RAMMap)**

  TO DO :

  1. Save to .RMP file.

Output:



Usage	Total	Active	Standby	Modified	Modified ...	Transition	Zeroed	Free	Bad
Process Private	12,04,328 K	11,82,892 K	9,264 K	12,172 K					
Mapped File	8,80,424 K	4,05,168 K	4,74,380 K	876 K					
Shareable	2,02,900 K	1,18,008 K	10,940 K	73,952 K					
Page Table	31,428 K	31,428 K							
Paged Pool	1,65,028 K	1,64,780 K	228 K	20 K					
Nonpaged Pool	1,42,044 K	1,42,036 K				8 K			
System PTE	20,060 K	20,056 K	4 K						
Session Private	33,408 K	33,408 K							
Metafile	1,18,700 K	1,11,048 K	7,652 K						
AWE									
Driver Locked	14,780 K	14,780 K							
Kernel Stack	10,632 K	10,260 K	96 K	276 K					
Unused	7,53,724 K						7,49,720 K	4,004 K	
Large Page									
Total	35,77,456 K	22,33,864 K	5,02,564 K	87,296 K		8 K	7,49,720 K	4,004 K	

PRACTICAL 7

AIM : - Recovering and Inspecting deleted files

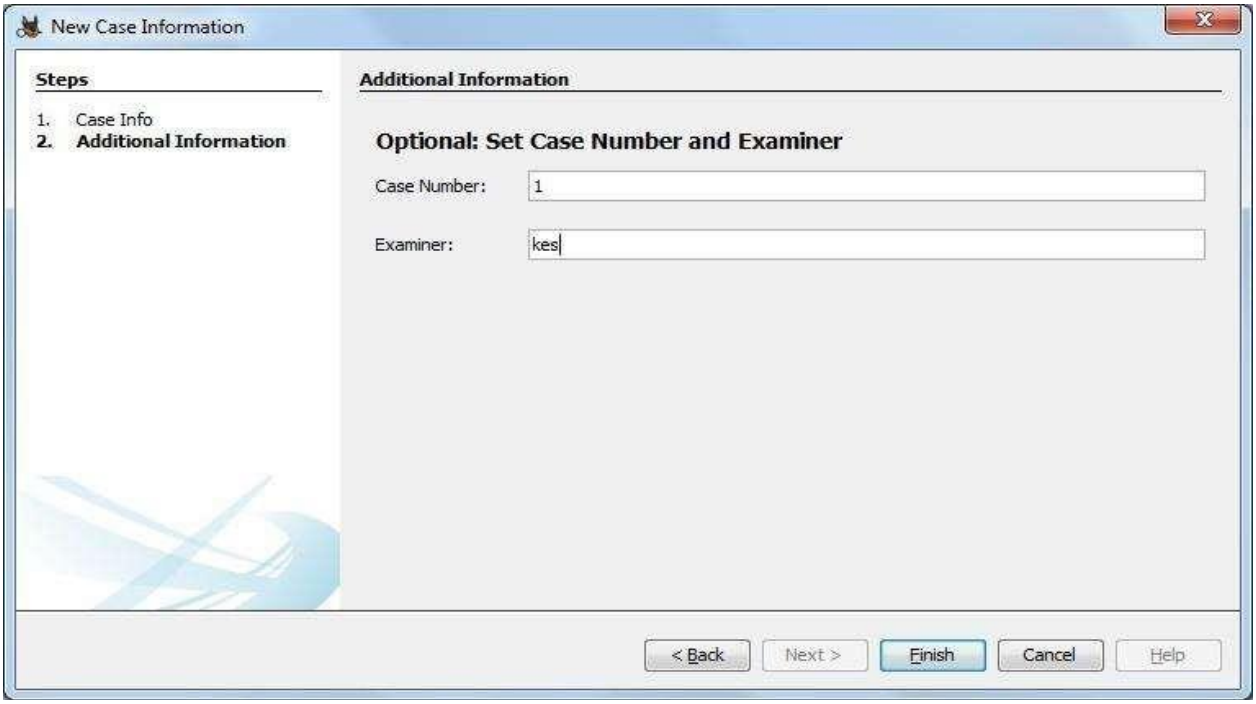
- Check for Deleted Files
- Recover the Deleted Files
- Analyzing and Inspecting the recovered files

Step 1: Start Autopsy from Desktop.

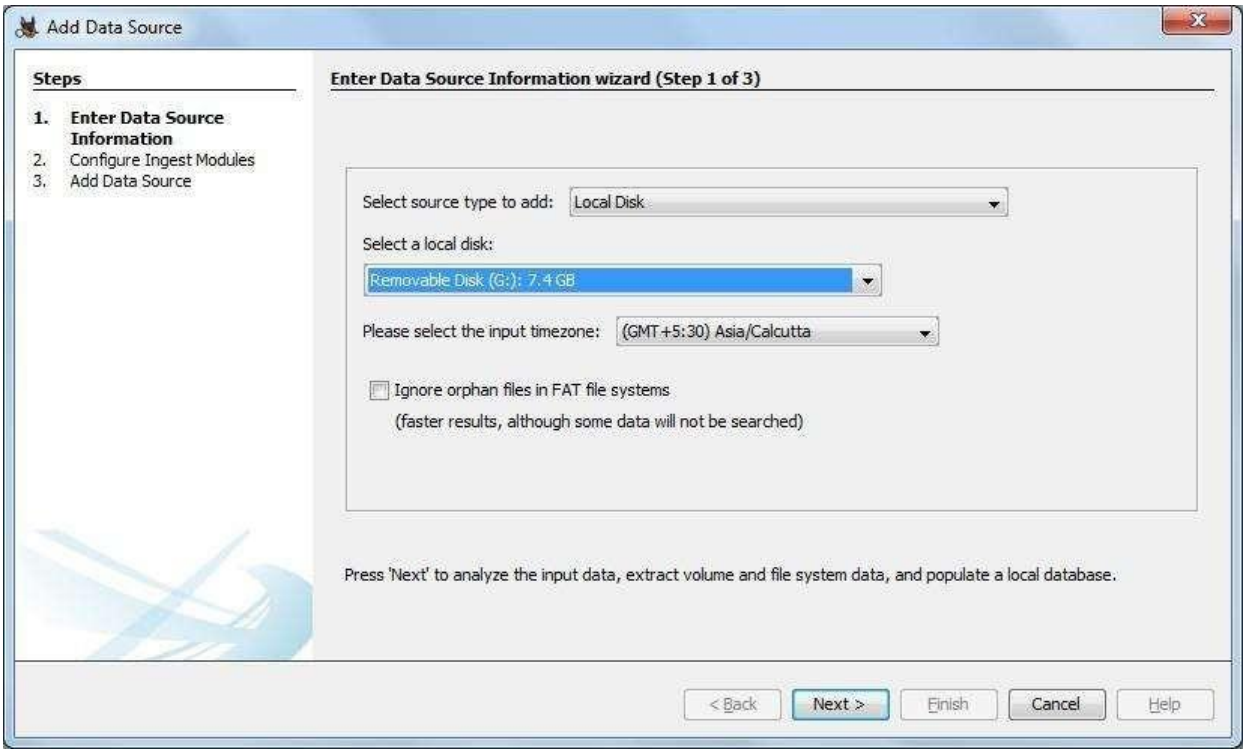
Step 2: Now create on New Case.

Step 3: Enter the New case Information and click on Next Button.

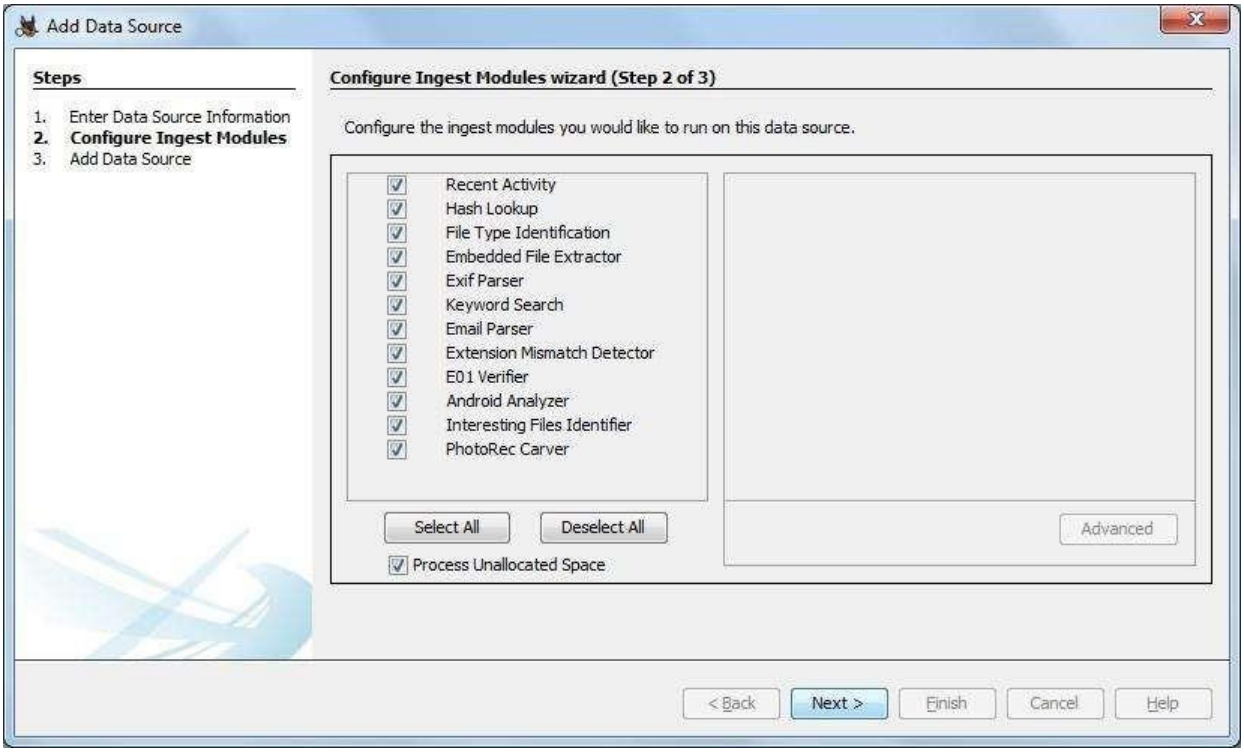
Step 4: Enter the additional Information and click on Finish.



Step 5: Now Select Source Type as Local disk and Select Local disk form drop down list and click on Next.

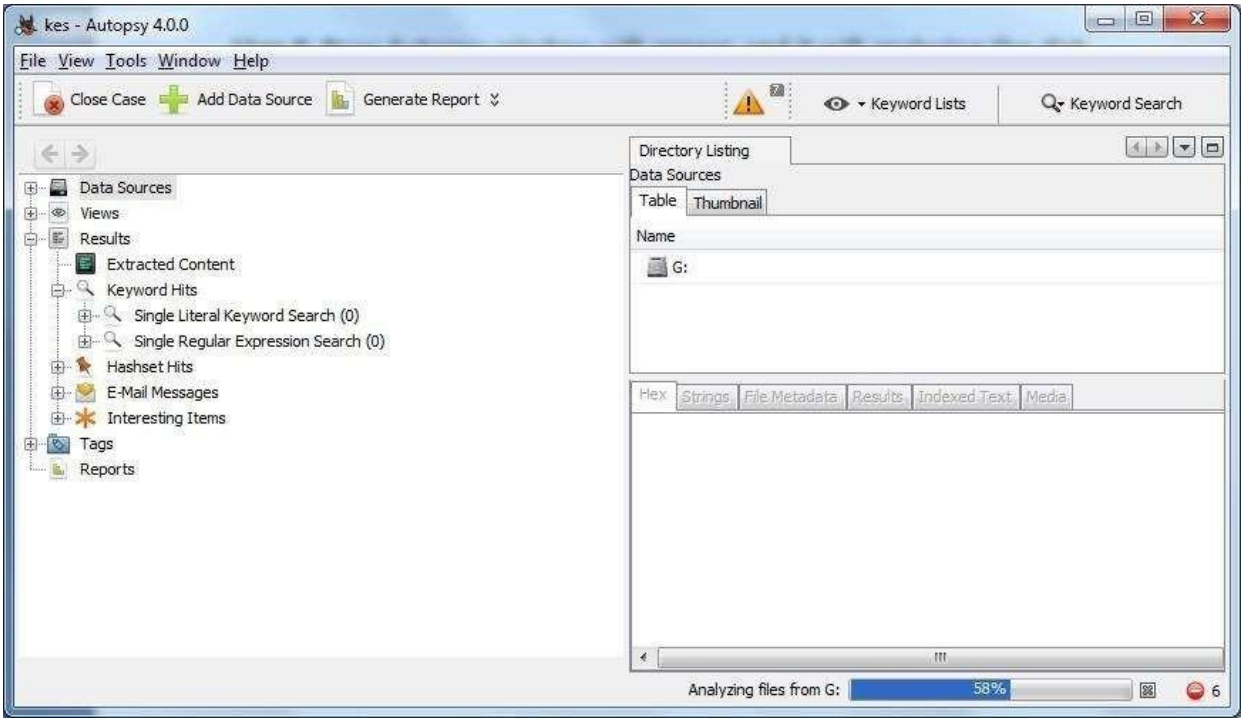


Step 6: Click on Next Button.

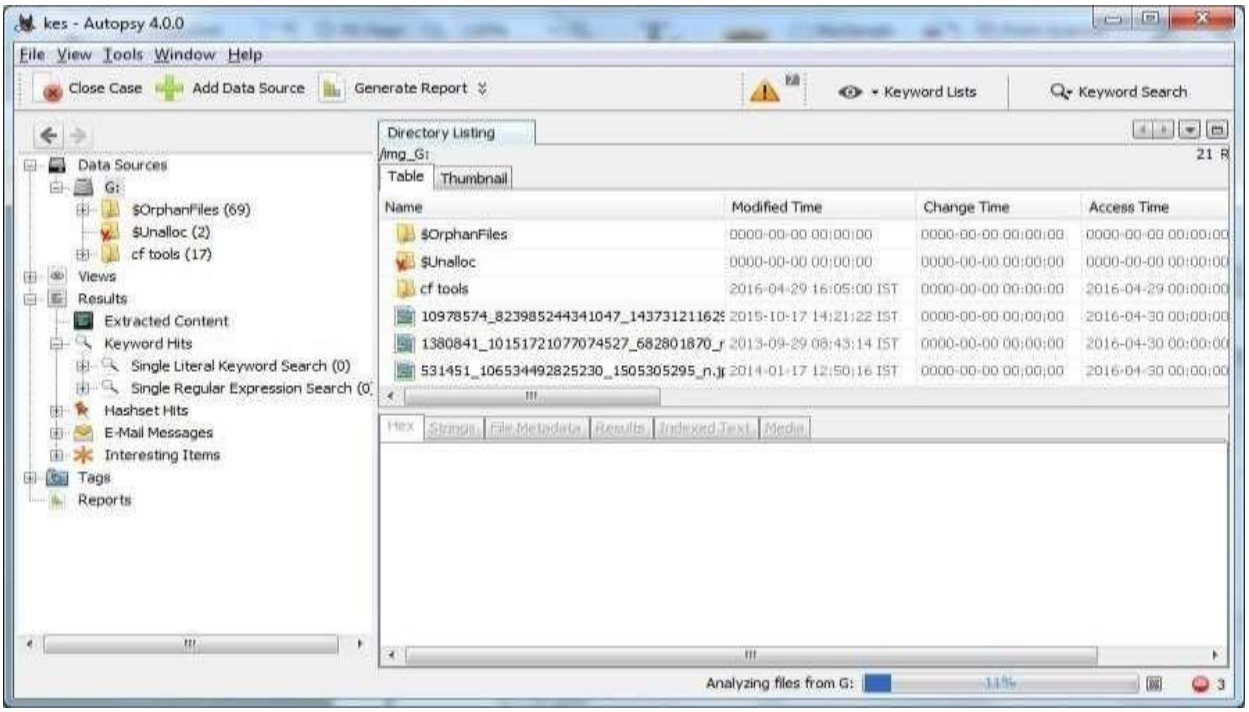


Step 7: Now click On Finish.

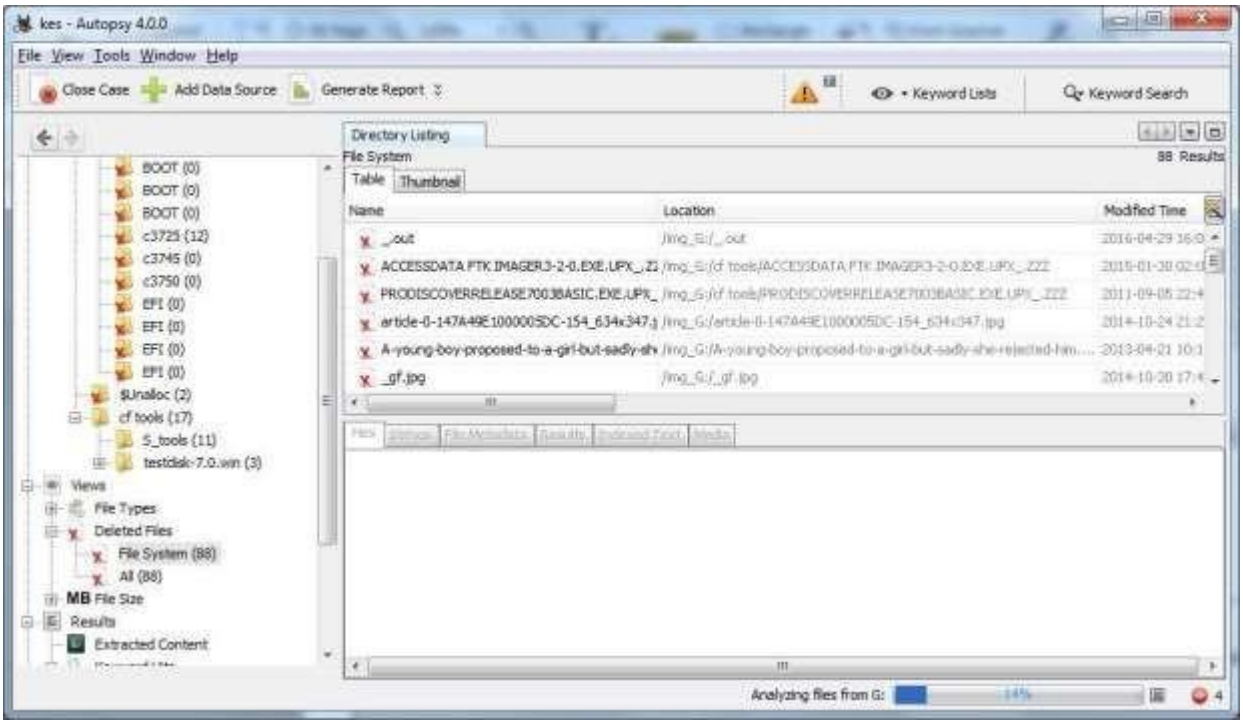
Step 8: Now Autopsy window will appear and it will analyzing the disk that we have selected.



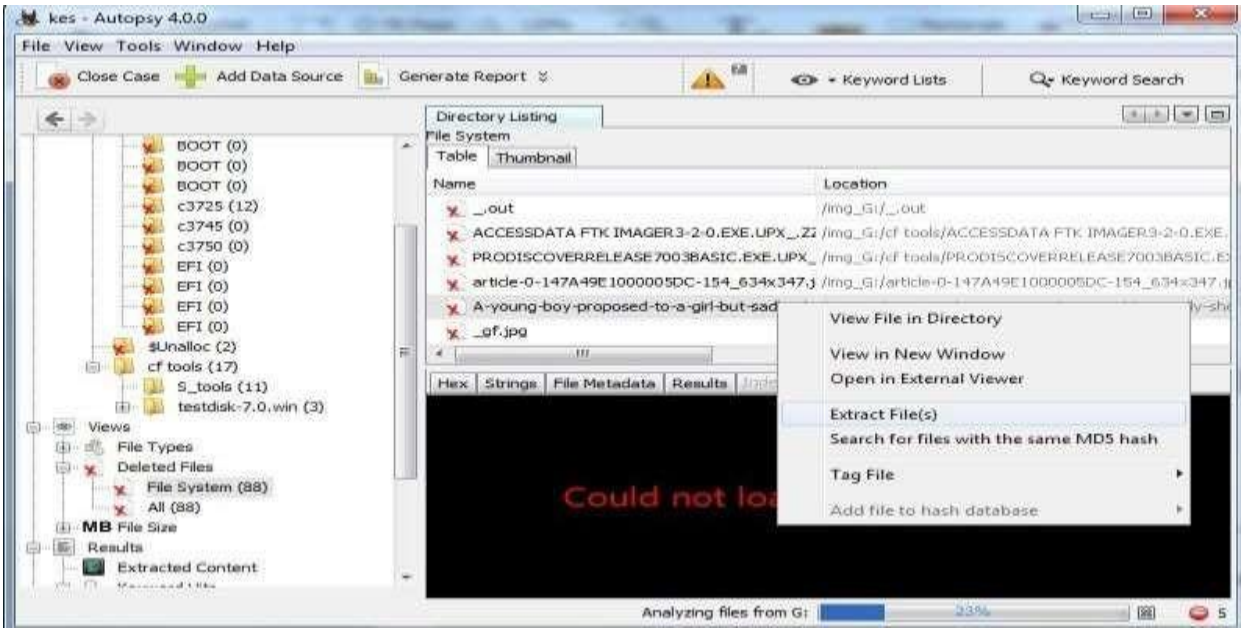
Step 9: All files will appear in table tab select any file to see the data.



Step 10:Expand the tree from left side panel to view the document files.



Step 11: To recover the file, go to view node-> Deleted Files node , here select any file and right click on it than select Extract Files option.

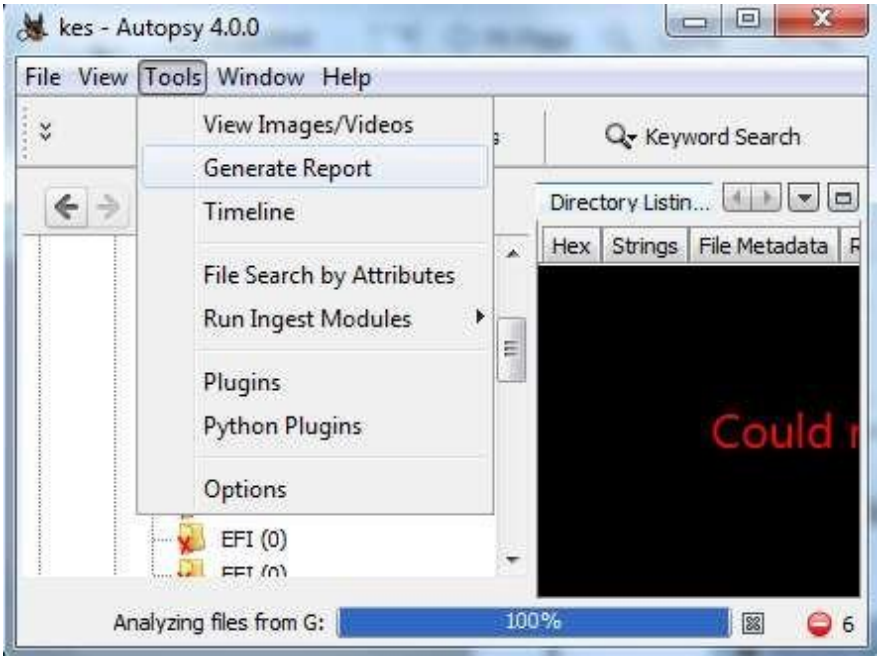


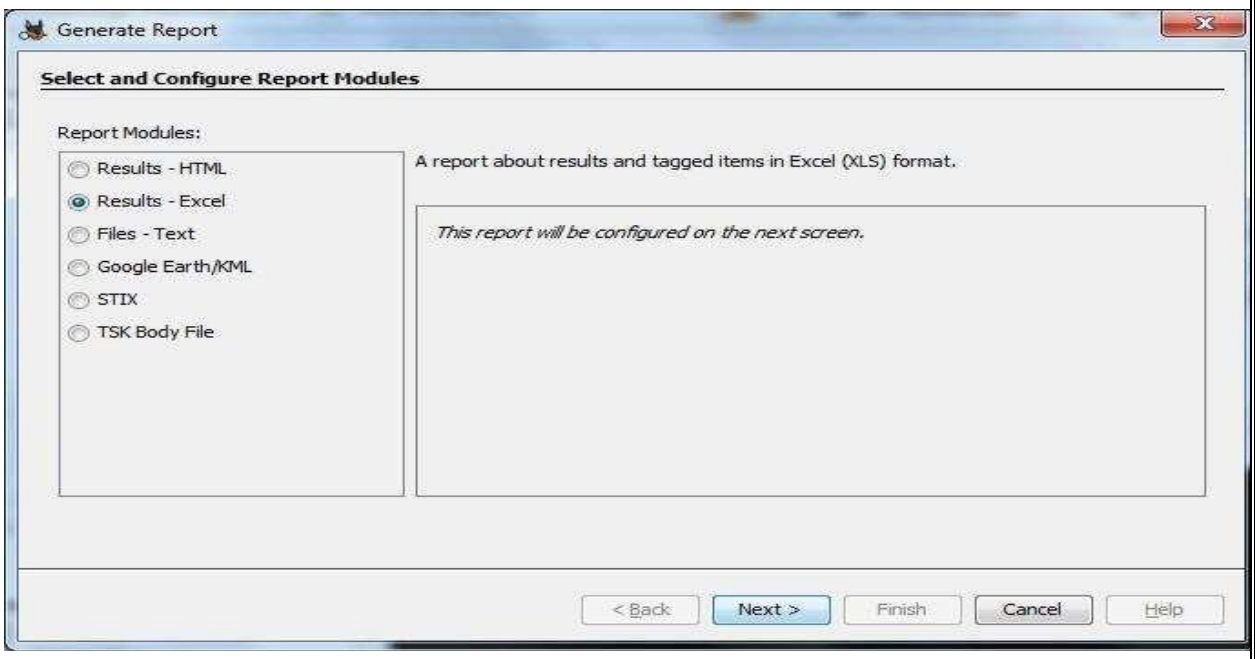
Step 12: By default Export folder is choose to save the recovered file.

Sep 13 : Now Click on Ok.

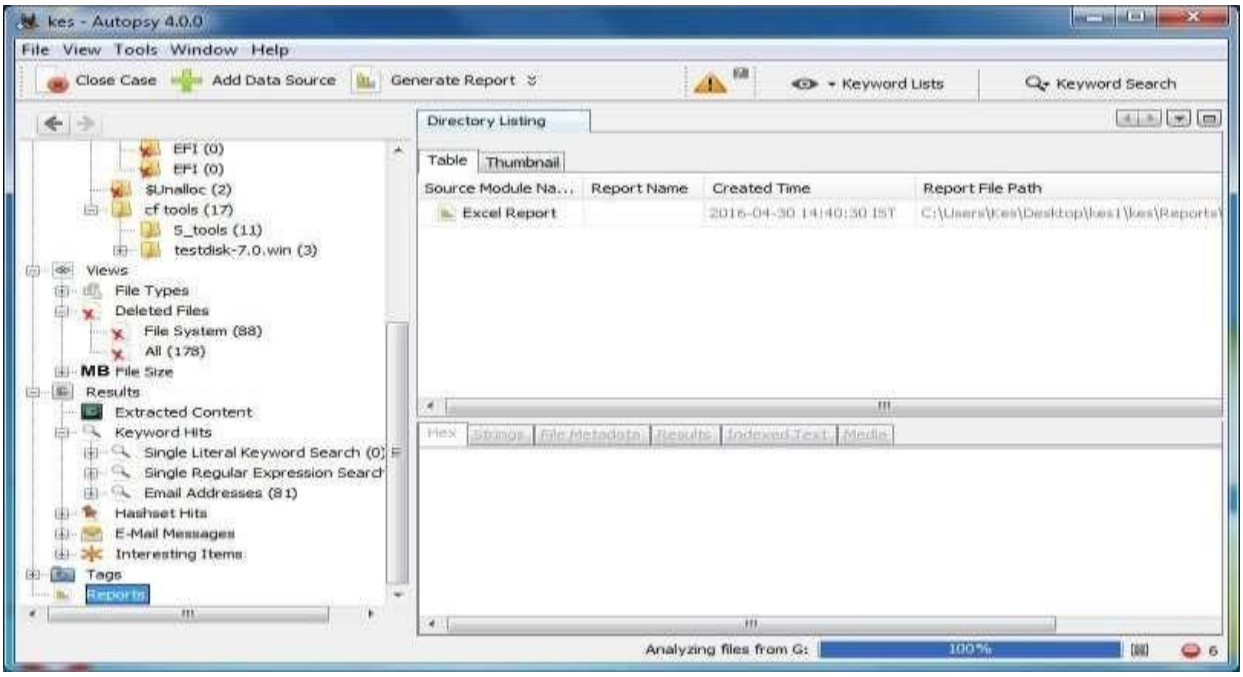
Step 14: Now go to the Export Folder to view Recover file.

Step 15: Click on Generate Report from autopsy window and Select the Excel format and click on next.

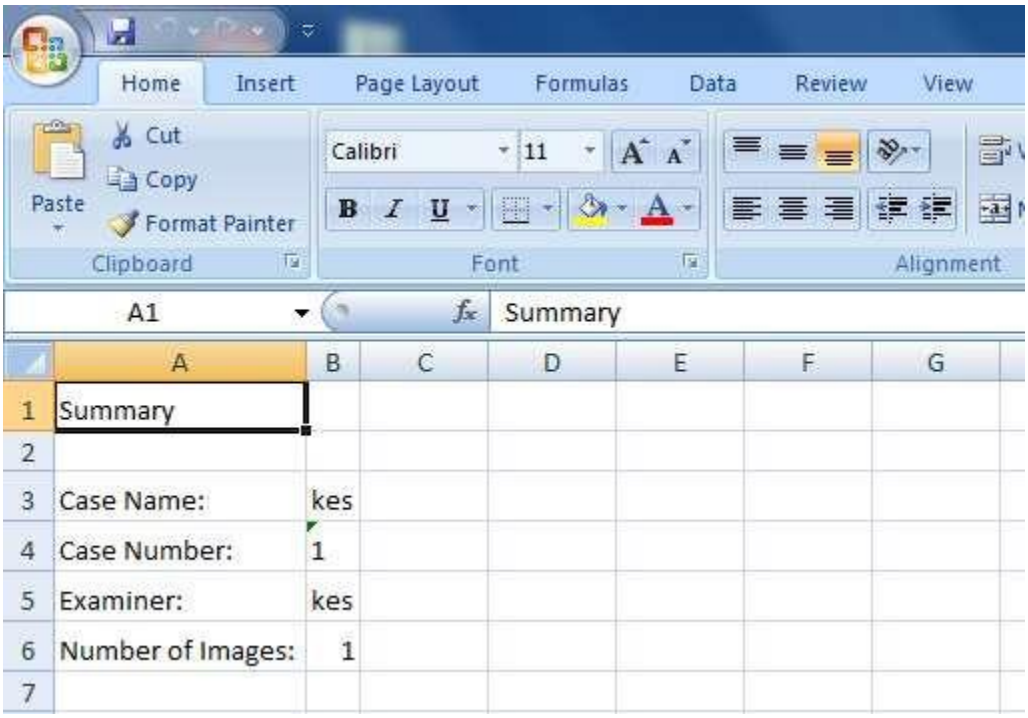




Step 16: Now Report is Generated So click on close Button .we can see the Report on Report Node.

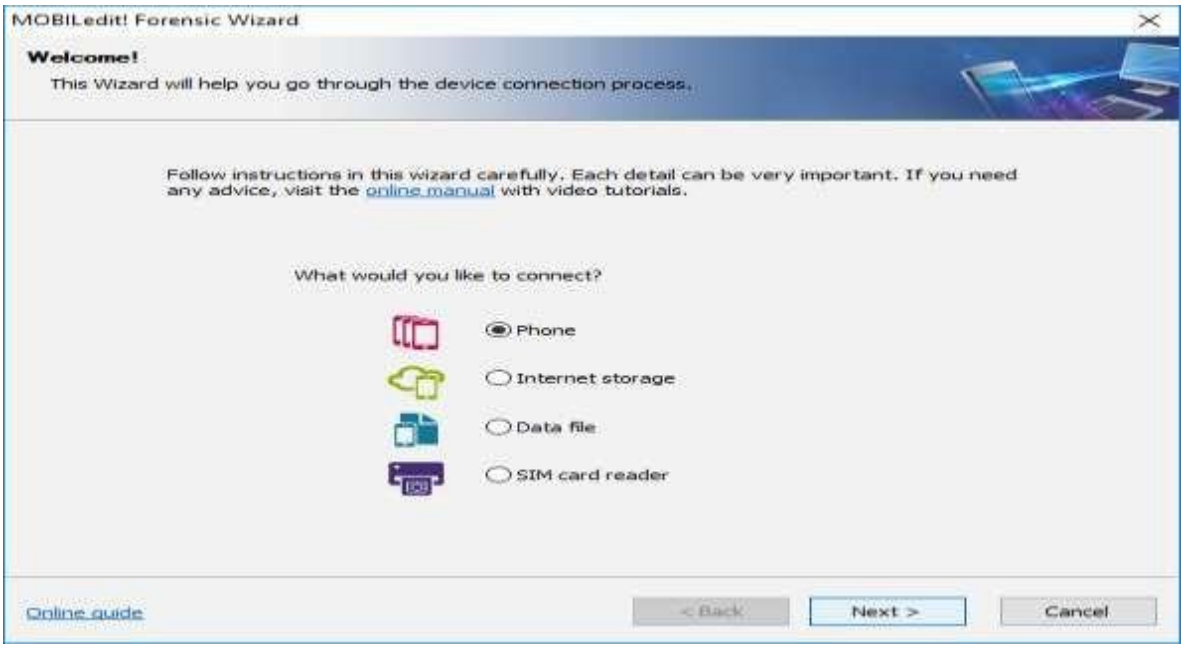


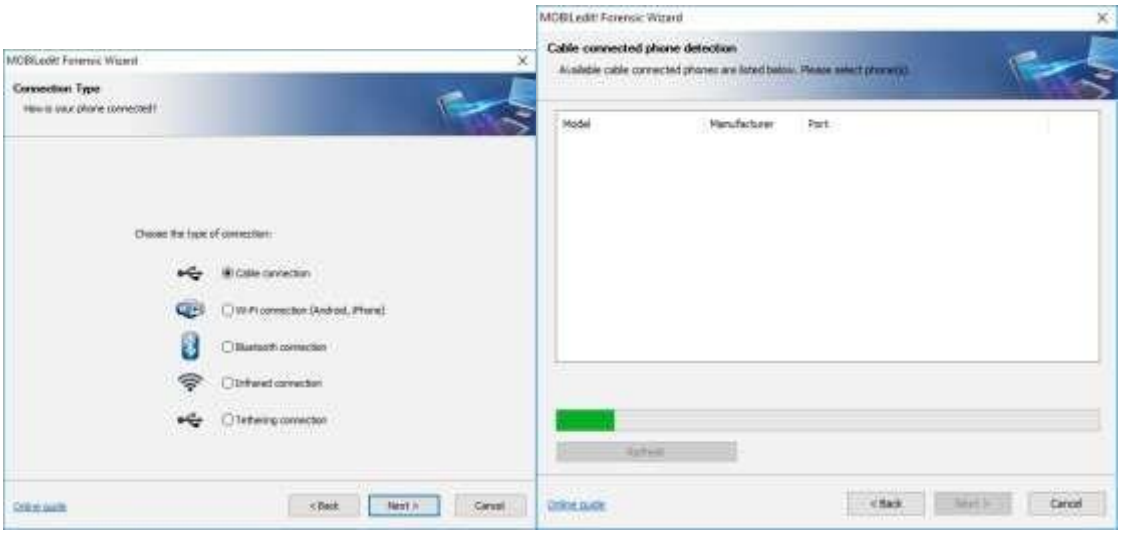
Step 17: Now open the Report folder and Open Excel File.

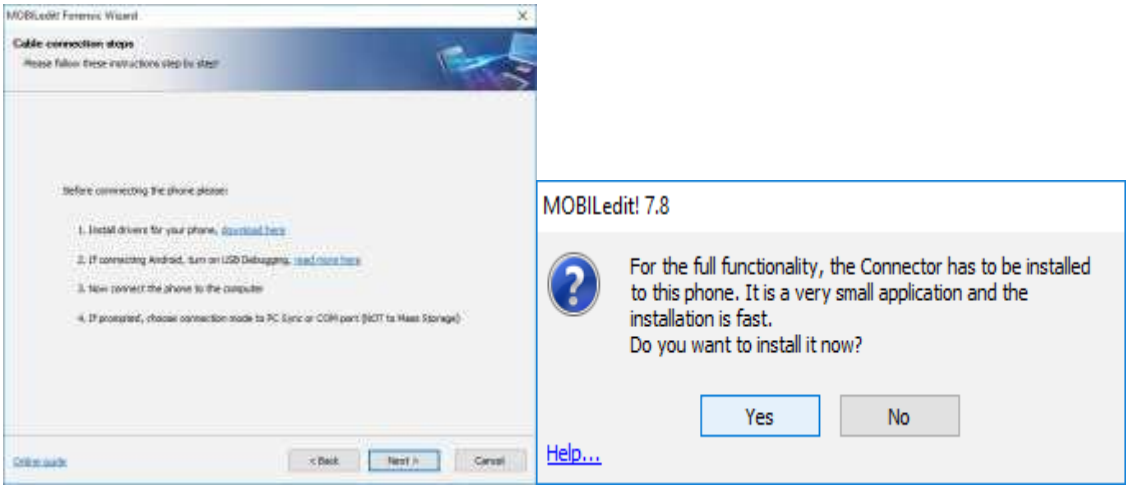

Home
Insert
Page Layout
Formulas
Data
Review
View
Cut
Copy
Format Painter
Paste
Clipboard
Calibri
11
Font
Alignment
A1
Summary
Summary
Case Name:
kes
Case Number:
1
Examiner:
kes
Number of Images:
1

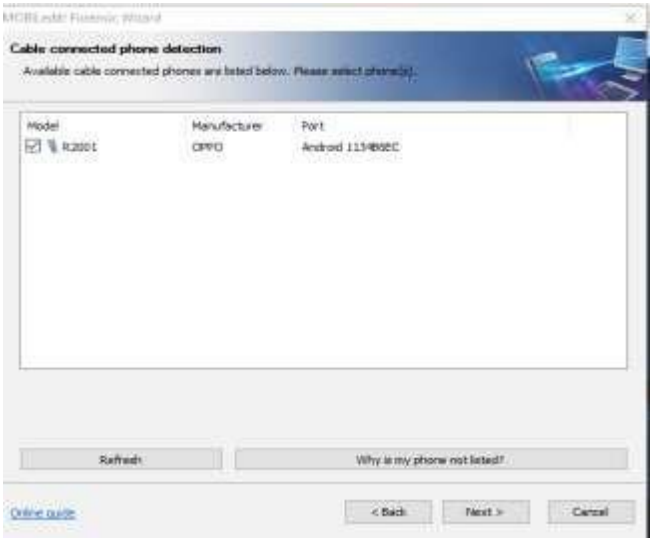
PRACTICAL 8

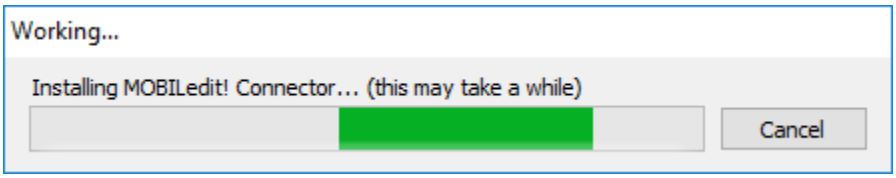
Aim :- Acquisition of Cell phones and Mobile devices .

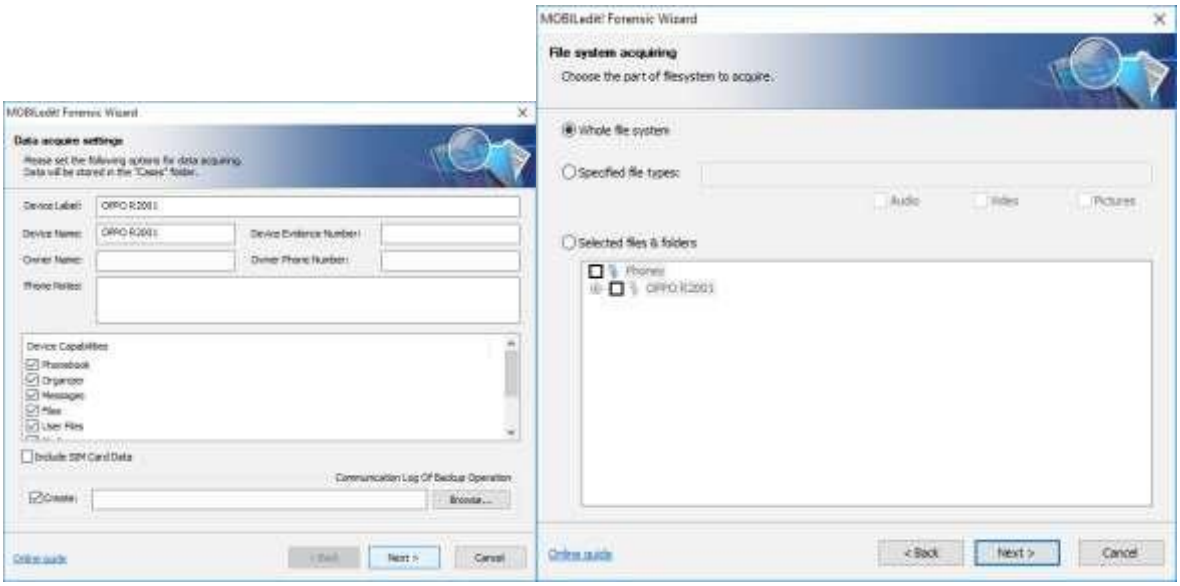


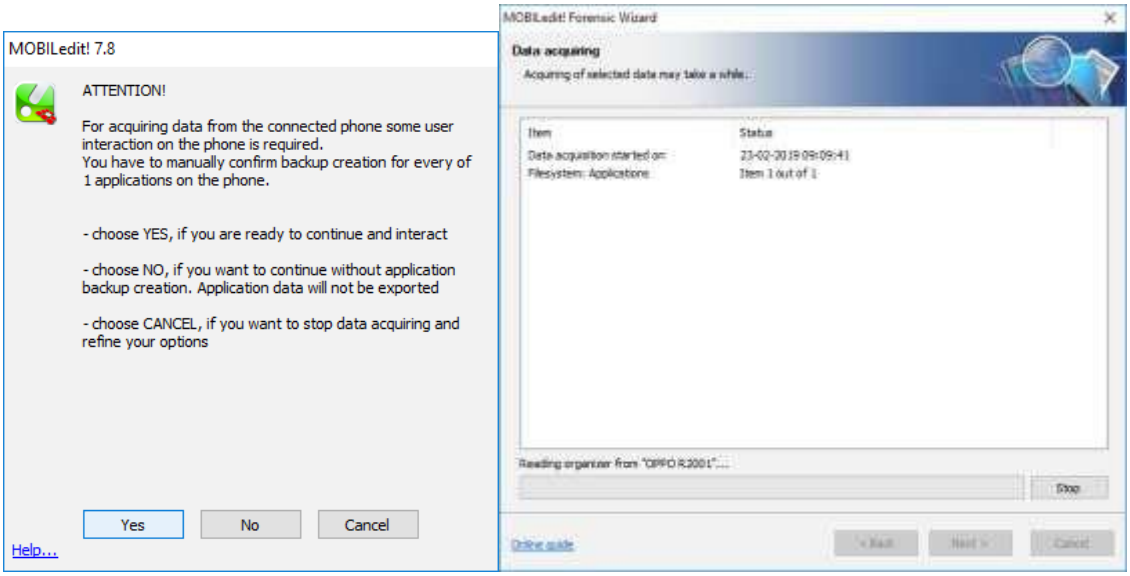

MOBILedit! Forensic Wizard
Connection Type
Choose the type of connection:
Cable connection
Wi-Fi connection (Android, iPhone)
Bluetooth connection
Infrared connection
Tethering connection
Online guide
< Back
Next >
Cancel
MOBILedit! Forensic Wizard
Cable connected phone detection
Model
Manufacturer
Port
Refresh
Online guide
< Back
Next >
Cancel

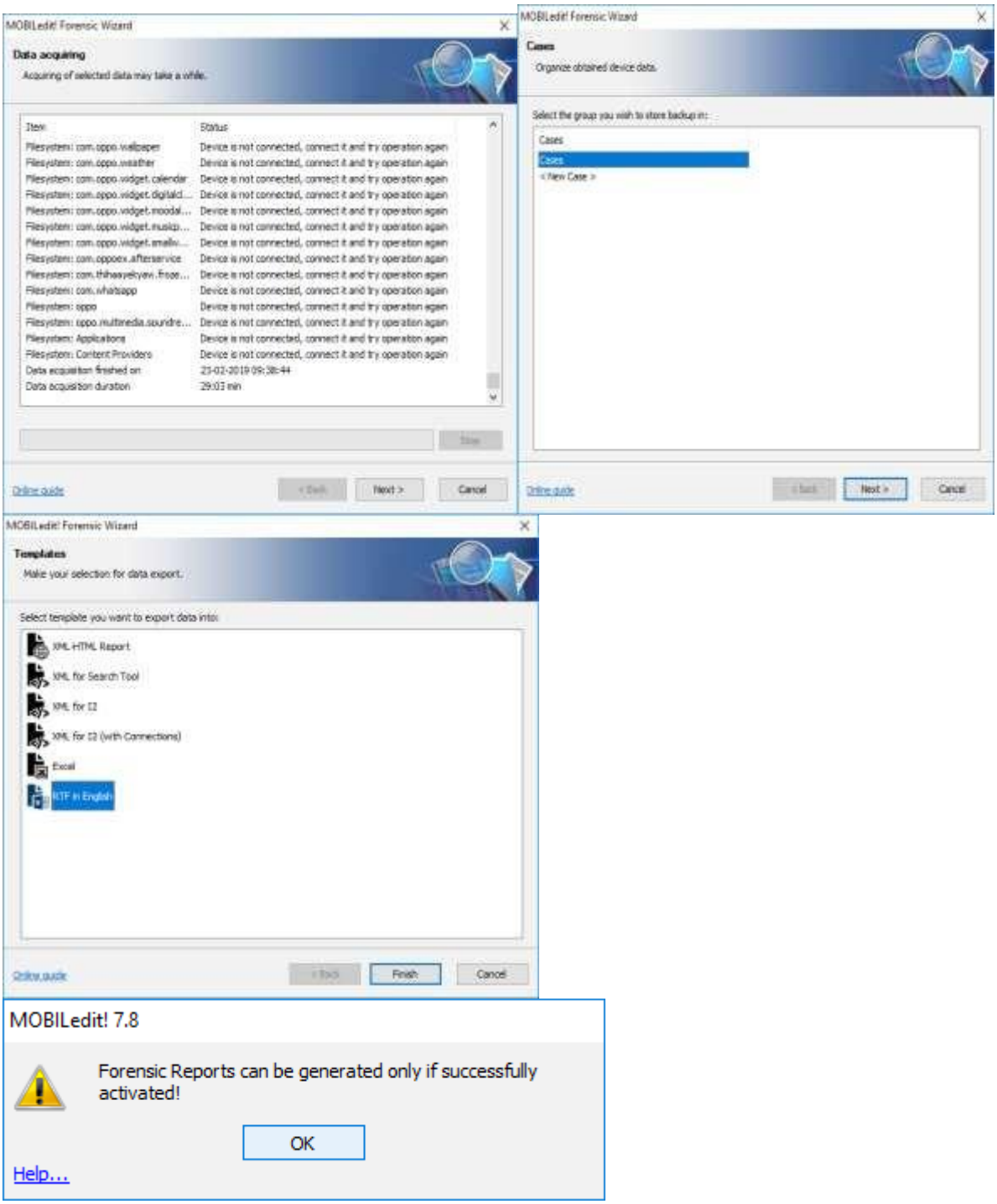

MOBILedit! Forensic Wizard
Cable connection steps
Before connecting the phone please:
1. Install drivers for your phone, download here
2. If connecting Android, turn on USB Debugging, read more here
3. Now connect the phone to the computer
4. If prompted, choose connection mode to PC Sync or COM port (NOT to Mass Storage)
Online guide
< Back
Next >
Cancel
MOBILedit! 7.8
For the full functionality, the Connector has to be installed to this phone. It is a very small application and the installation is fast.
Do you want to install it now?
Yes
No
Help...

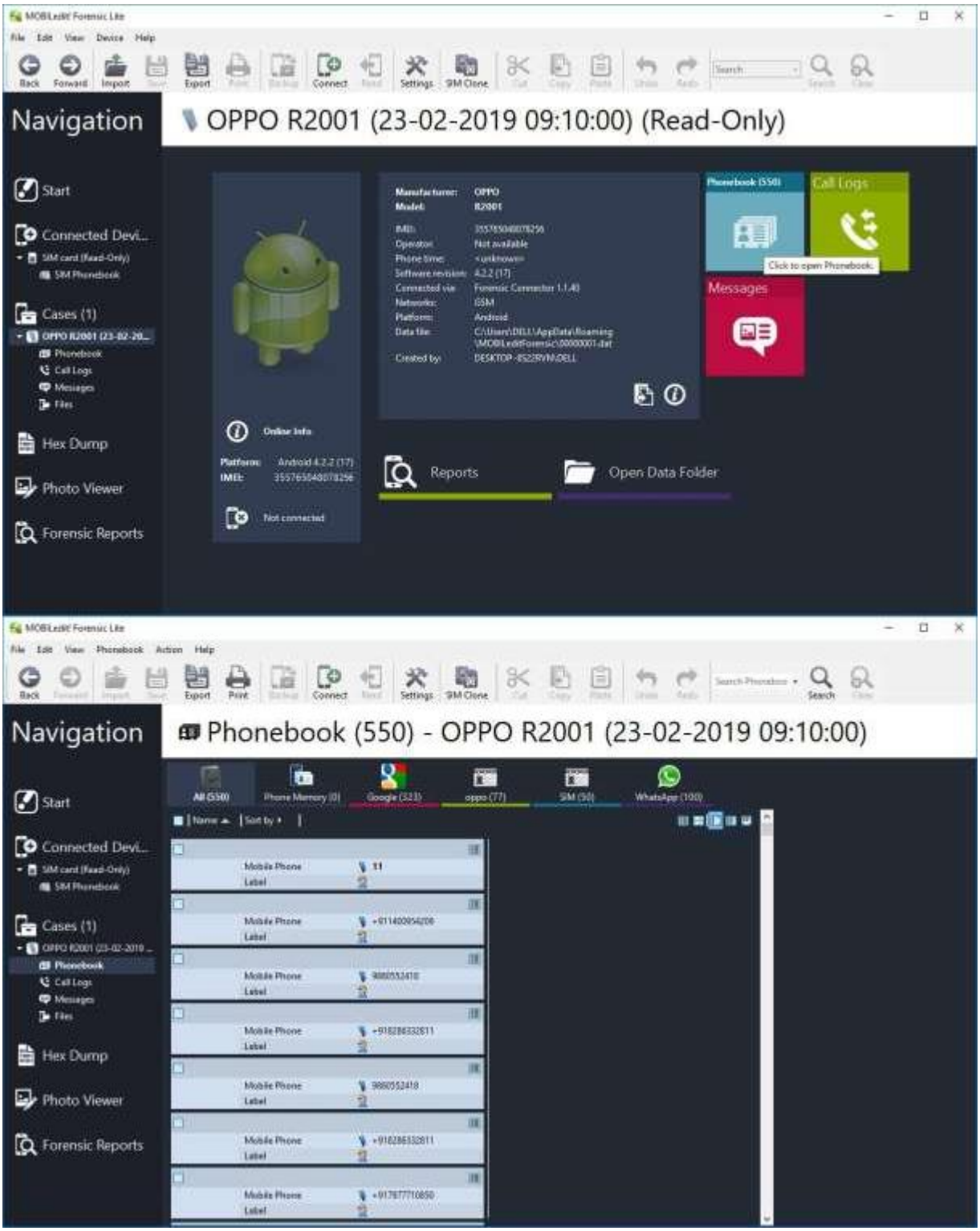

Cable connected phone detection
Model
Manufacturer
Port
Refresh
Why is my phone not listed?
Online guide
< Back
Next >
Cancel

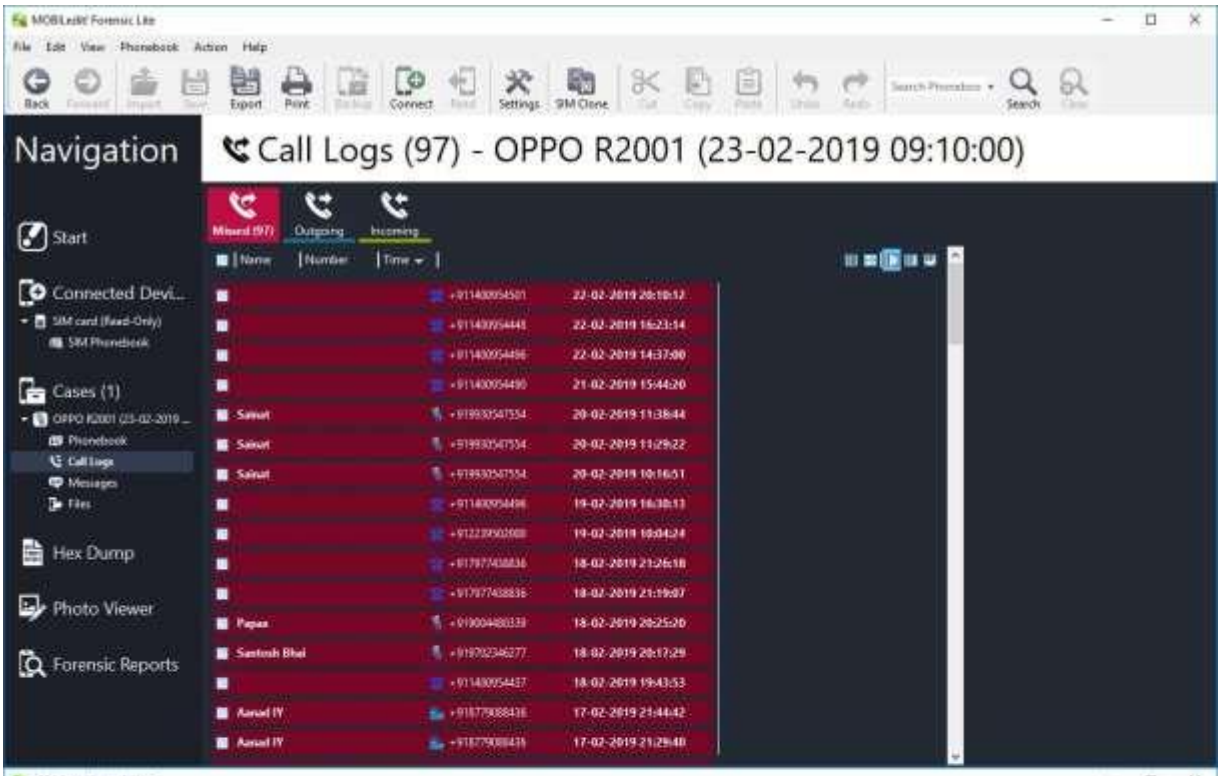

Working...
Installing MOBILedit! Connector... (this may take a while)
Cancel

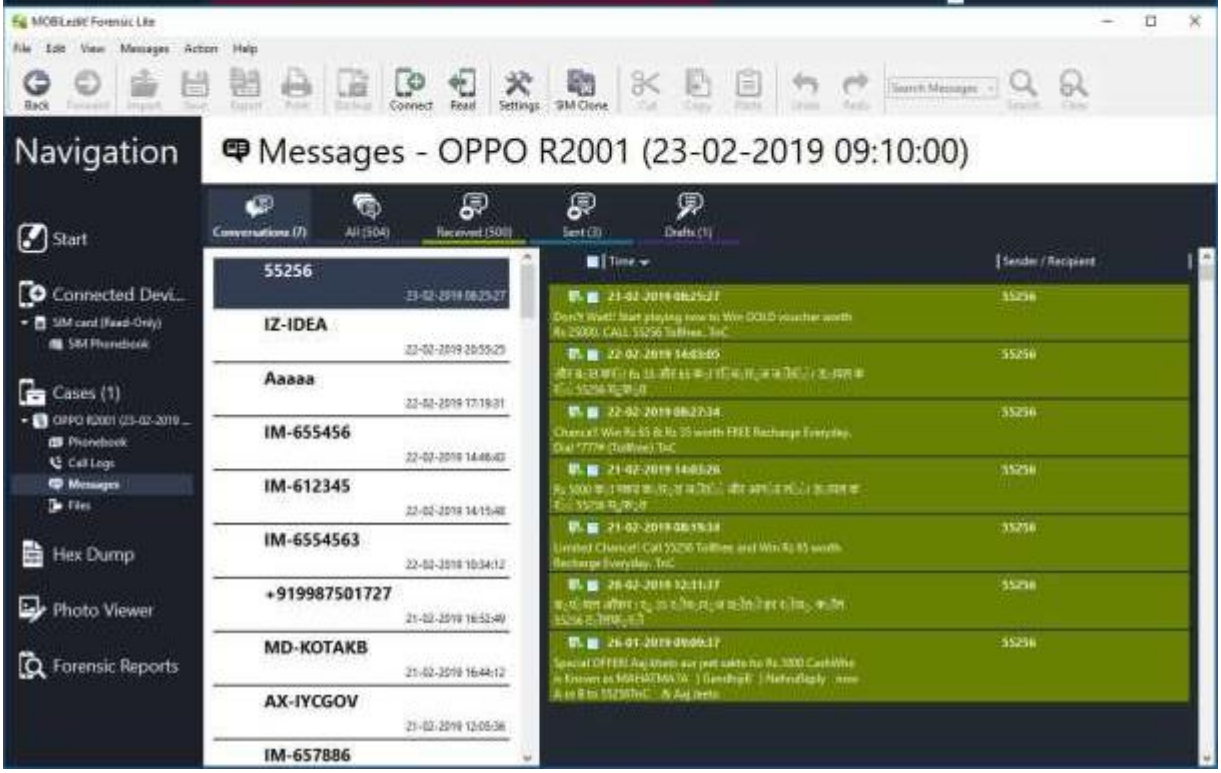

MOBILedit! Forensic Wizard
File system acquiring
Choose the part of filesystem to acquire.
Whole file system
Specified file types:
Selected files & folders
< Back
Next >
Cancel


MOBILedit! 7.8
ATTENTION!
For acquiring data from the connected phone some user interaction on the phone is required.
You have to manually confirm backup creation for every of 1 applications on the phone.
- choose YES, if you are ready to continue and interact
- choose NO, if you want to continue without application backup creation. Application data will not be exported
- choose CANCEL, if you want to stop data acquiring and refine your options
Yes
No
Cancel
Help...
MOBILedit! Forensic Wizard
Data acquiring
Acquiring of selected data may take a while.
Item
Status
Stop


MOBILedit! Forensic Wizard
Data acquiring
Acquiring of selected data may take a while.
Item
Status
Data acquisition finished on
21-02-2019 09:38:44
Data acquisition duration
29:03 min
Online guide
< Back
Next >
Cancel
MOBILedit! Forensic Wizard
Cases
Organize obtained device data.
Select the group you wish to store backup in:
Cases
< New Case >
Online guide
< Back
Next >
Cancel
MOBILedit! Forensic Wizard
Templates
Make your selection for data export.
Select template you want to export data into:
XML HTML Report
XML for Search Tool
XML for I2
XML for I2 (with Connections)
Excel
RTF in English
Online guide
< Back
Finish
Cancel
MOBILedit! 7.8
Forensic Reports can be generated only if successfully activated!
OK
Help...


Navigation
OPPO R2001 (23-02-2019 09:10:00) (Read-Only)
Start
Connected Devi...
Cases (1)
Hex Dump
Photo Viewer
Forensic Reports
Phonebook (550)
Call Logs
Messages
Reports
Open Data Folder
Navigation
Phonebook (550) - OPPO R2001 (23-02-2019 09:10:00)
Start
Cases (1)
Hex Dump
Photo Viewer
Forensic Reports


Navigation
Call Logs (97) - OPPO R2001 (23-02-2019 09:10:00)
Start
Connected Devi...
Cases (1)
Hex Dump
Photo Viewer
Forensic Reports


Navigation
Messages - OPPO R2001 (23-02-2019 09:10:00)
55256
IZ-IDEA
Aaaaa
IM-655456
IM-612345
IM-6554563
+919987501727
MD-KOTAKB
AX-IYCGOV
IM-657886
Start
Connected Devi...
Cases (1)
Hex Dump
Photo Viewer
Forensic Reports

Practical no:9

Aim: E-mail Forensics

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

- **Mail Service Providers**

An email service provider (ESP) is a company that offers email marketing or bulk email services. An ESP may provide tracking information showing the status of email sent to each member of an address list. ESPs also often provide the ability to segment an address list into interest groups or categories, allowing the user to send targeted information to people who they believe will value the correspondence. Here are nine features to look for when you select your business email service:

- **Spam Filter** - Spam messages are a huge time waster. You don't want to spend your valuable time reading them. That's why you want an email service that has a system in place to detect and filter out inbox spam.

- **Reliability -** Your business email provider needs to be up and running when you need it. Your email should always be available. Email downtime could result in lost or unhappy customers.

- **Integration -** Some email services work well with other business tools such as calendars, and productivity suites. If your business relies heavily on such tools, consider an email package that integrates with the other tools you already use.

- **Security -** With email hacks being a regular news item, you want your business email provider to offer strong measures to keep your accounts secure. You need to keep your messages safe and don't want any unauthorized use of your email account.

- **Ease of Use** - As your business grows, more of your staff members need to create and useemail accounts. Reduce staff training time by selecting an email service provider that's easy to use.

- **Archive Capabilities -** The best business email providers provide a way for you to save, store, and organize your email messages and drafts. For many businesses, keeping an accurate and well-organized record of business communication is vital.

- **Advanced Features** - When running a small business, advanced email features such as the ability to recall sent messages or schedule tasks within email can be important. Which advanced features are most important depends on your unique business needs.

- **Reputation -** Your business email service provider needs to have a good reputation. Remember, your email address is one of the first pieces of information prospective client see**.**

- **Storage -** When selecting an email service provider, keep in mind the amount of storage space included with your account. You don't want to run out of space.

1.Gmail:

One of the most popular and best email service providers, Gmail is used for personal and business communications alike. According to statistics reported by TechCrunch in 2016, over a billion people use Gmail. Gmail has a good reputation and includes many advanced features such as the Undo Send feature and Email Forwarding. Since this service is owned by search engine giant, Google, naturally it includes a powerful search utility and filter system. Google has also added strengthened security measures such as two-step verification and powerful spam filters to make it less likely that your account is hacked or that you receive junk messages. Finally, it integrate cleanly with popular productivity tools including Google Calendar and Google Docs**.**

2. Outlook

Microsoft's Outlook.com email provider is a strong option if you're looking for the best email provider. Statistics from Microsoft show that Outlook had over 400 million users in 2016. This popular email package has the support and resources of tech giant Microsoft behind it. Outlook.com offers advanced features such as Clutter, which finds emails that are likely of low priority and separates them from your inbox. Another advanced Outlook.com feature is
the ability to Undelete, or recover an email after you've accidentally discarded a message.Outlook integrates well with popular software including other Microsoft products.

3.iCloud Mail

iCloud email is a possible email choice if you frequently access your email package from your Apple mobile device. Apple employs several security features to make sure that your iCloud account is not compromised including two-step verification or two-factor authentication. There's also a spam filter.

4. Yahoo Mail

Yahoo! was one of the early Internet companies, dating back to 1994. Yahoo! Mail is popular with many users. In 2016, it was announced that the company was acquired by Verizon Despite the recent changes to Yahoo! ownership, you can still sign up for a Yahoo! Mail
account. Some Yahoo! Mail features you can benefit from if you choose it as your email

provider include:

Auto deletion of Trash messages after 90 days
Huge storage capacity (1 TB)
Built-in web search tool, calendar, and notepad
Spam filters and SSL encryption

5. AOL Mail

AOL is another early Internet company. In the 1980s the company was known as America Online. It was purchased by Verizon in 2015. The email component of the organization remains a popular and strong service that has earned its place on this list of the best email
services. Key AOL Mail features include advanced spam filters and virus protection. It's also known for the ability to personalize your email address with the MyAddress feature that lets you

select your own email domain name.

6. Zoho Mail

Although Zoho Mail has several premium levels available, there is also a free level available that allows you to have up to 25 users. For many small businesses, this will be enough—so we have included the email service on our list of the best free email providers. With the free level of Zoho Mail, you are limited to 5 GB of storage per user. It does include antivirus protection and spam filtering. This email service integrates with other Zoho productivity tools such as calendar, tasks, and notes.

- **Email Protocols**

  E-mail Protocols are set of rules that help the client to properly transmit the information to or from the mail server The most commonly used Email protocols on the internet - POP3, IMAP and SMTP. Each one of them has specific function and way of work.

- **POP3**

  Post Office Protocol version 3 (POP3) is a standard mail protocol used to receive emails from a remote server to a local email client. POP3 allows you to download email messages on your local computer and read them even when you are offline. Note, that when you use POP3 to connect to your email account, messages are downloaded locally and removed from the email server. This means that if you access your account from multiple locations, that may not be the best option for you. On the other hand, if you use POP3, your messages are stored on your local computer, which reduces the space your email account uses on your web server.

  By default, the POP3 protocol works on two ports:

- Port 110 - this is the default POP3 non-encrypted port
- Port 995 - this is the port you need to use if you want to connect using POP3 securely

- **IMAP**

  The Internet Message Access Protocol (IMAP) is a mail protocol used for accessing email on a remote web server from a local client. IMAP and POP3

are the two most commonly used Internet mail protocols for retrieving emails. Both protocols are supported by all modern email clients and web servers. While the POP3 protocol assumes that your email is being accessed only from one application, IMAP allows simultaneous access by multiple clients. This is why IMAP is more suitable for you if you're going to access your email from different locations or if your messages are managed by multiple users.

By default, the IMAP protocol works on two ports:

- Port 143 - this is the default IMAP non-encrypted port
- Port 993 - this is the port you need to use if you want to connect using IMAP securely

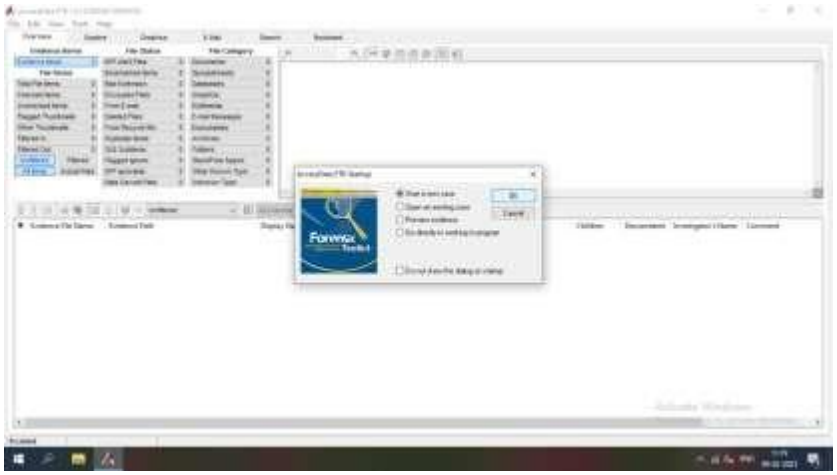
SMTP

SMTP stands for Simple Mail Transfer Protocol. It was first proposed in 1982. It is a standard protocol used for sending e-mail efficiently and reliably over the internet. Simple Mail Transfer Protocol (SMTP) is the standard protocol for sending emails across the Internet.

By default, the SMTP protocol works on three ports:

- Port 25 - this is the default SMTP non-encrypted port
- Port 2525 - this port is opened on all SiteGround servers in case port 25 is filtered (by your ISP for example) and you want to send non-encrypted emails with SMTP
- Port 465 - this is the port used if you want to send messages using SMTP securely

- **Recovering email using AccessData FTK:**
  1. Start AccessData FTK by right-clicking the AccessData FTK desktop icon, clicking Run as administrator, and clicking Continue in the UAC message box (if you're using Vista). If you're prompted with a warning message and/or notification (see Figure below), click OK as needed to continue. If asked whether you want to save the existing default case click Yes.



2. When the AccessData FTK Startup dialog box opens, click Start a new case, and then click OK.

3. In the New Case dialog box, type your name for the investigator name, and type the case number and case name. Click Browse, navigate to and click your work folder, click OK, and then click Next

4.In the Case Information dialog box, enter your investigator information, and then click Next.

5. Click Next until you reach the Refine Case - Default dialog box, shown in Figure below.

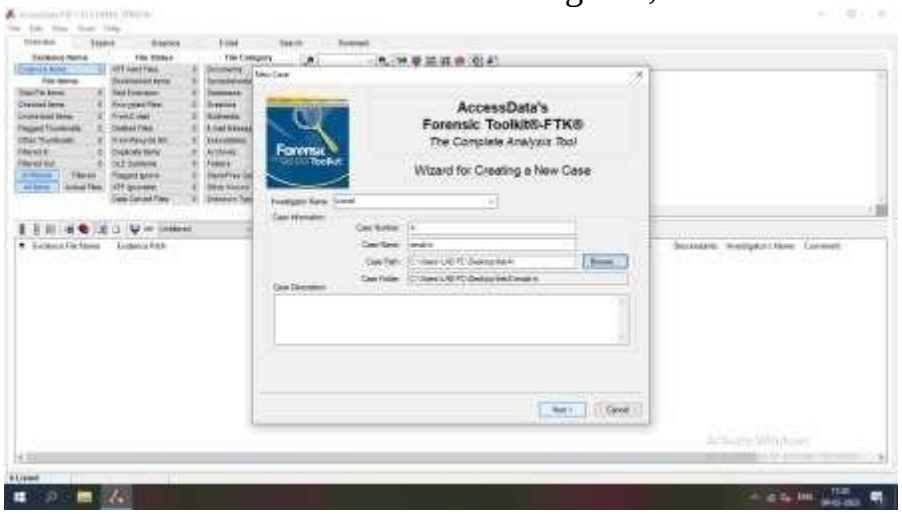
6. Click the Email Emphasis button, and then click Next.

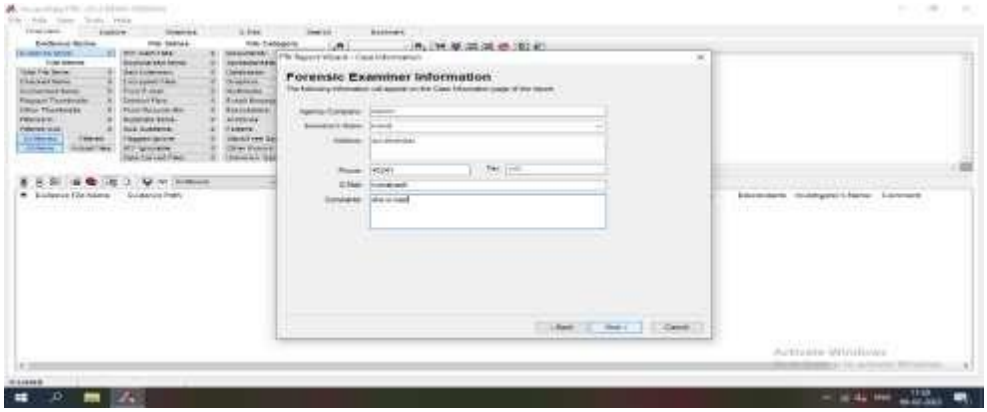
7. Click Next until you reach the Add Evidence to Case dialog box, and then click the Add Evidence button.

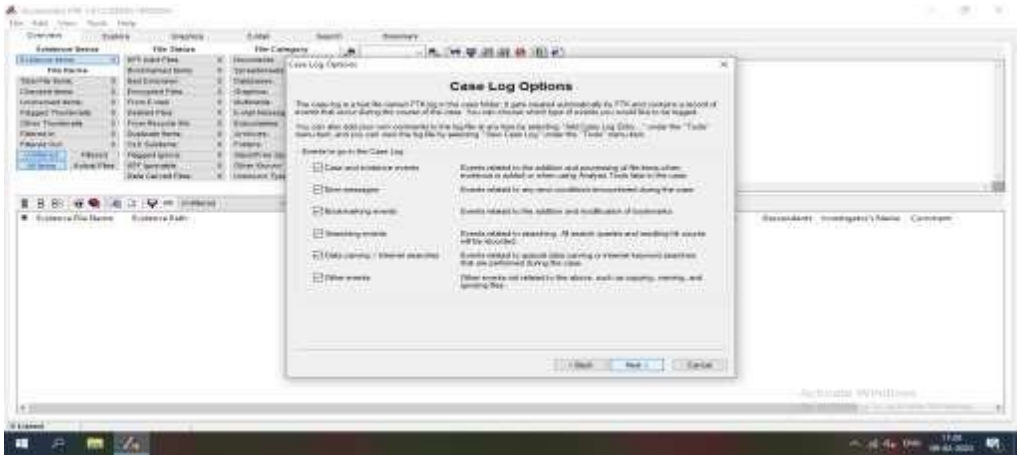
8. In the Add Evidence to Case dialog box, click the Individual File option button and then click Continue.

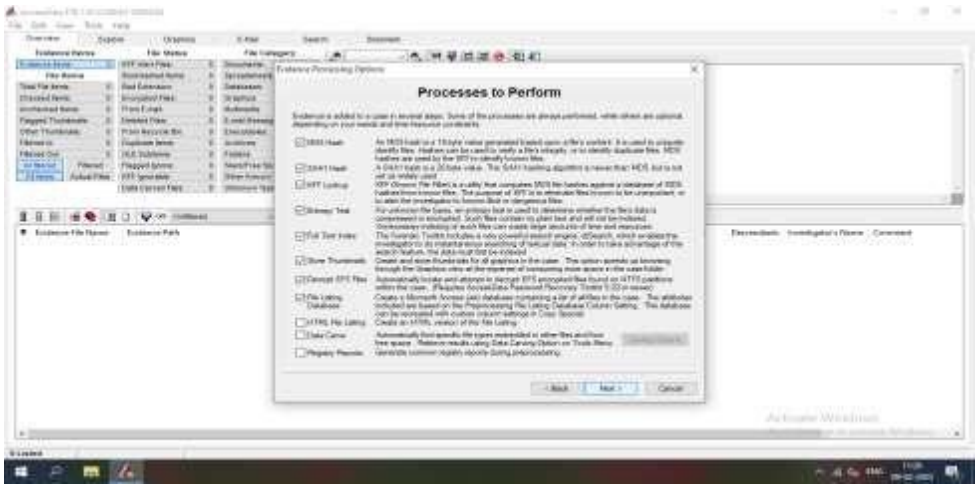
9. In the Select File dialog box, navigate to your work folder, click the Jim_shu's.pst file, and,then click Open.

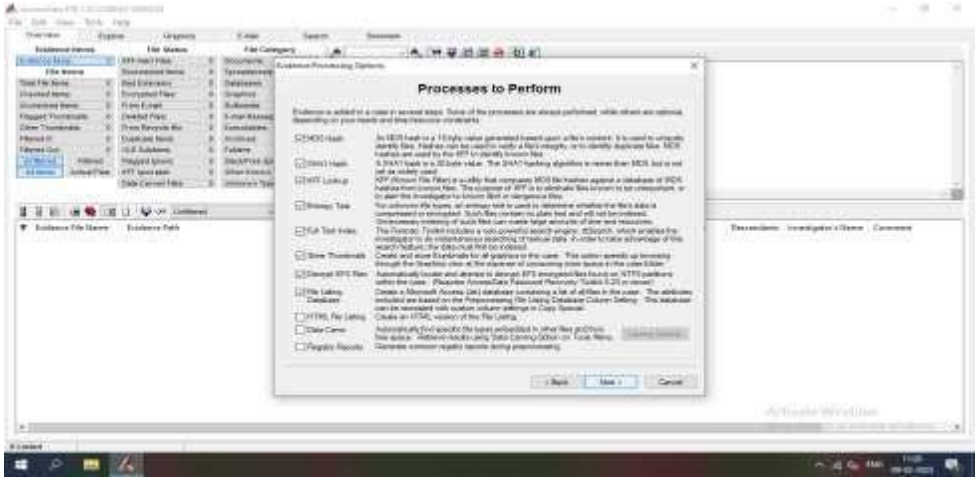
10. In the Evidence Information dialog box, click OK.

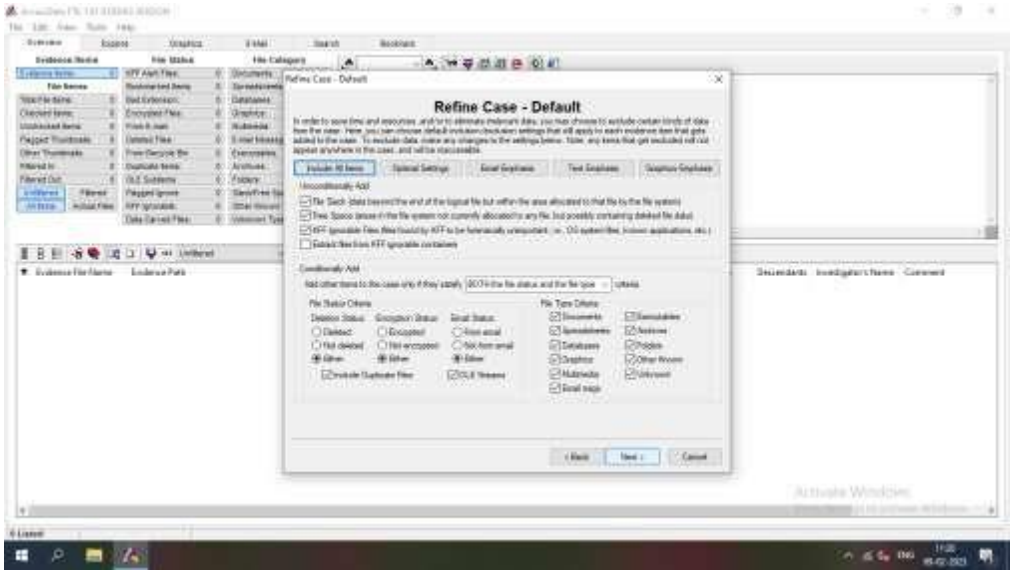


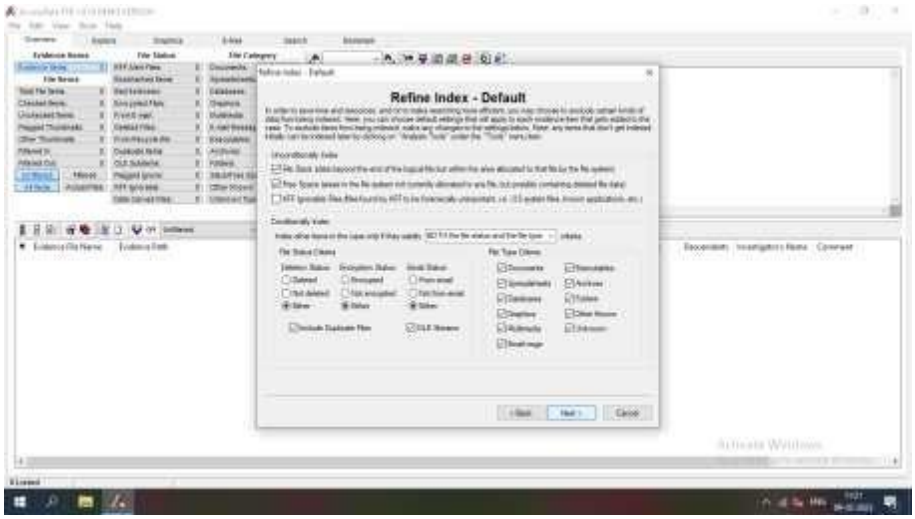


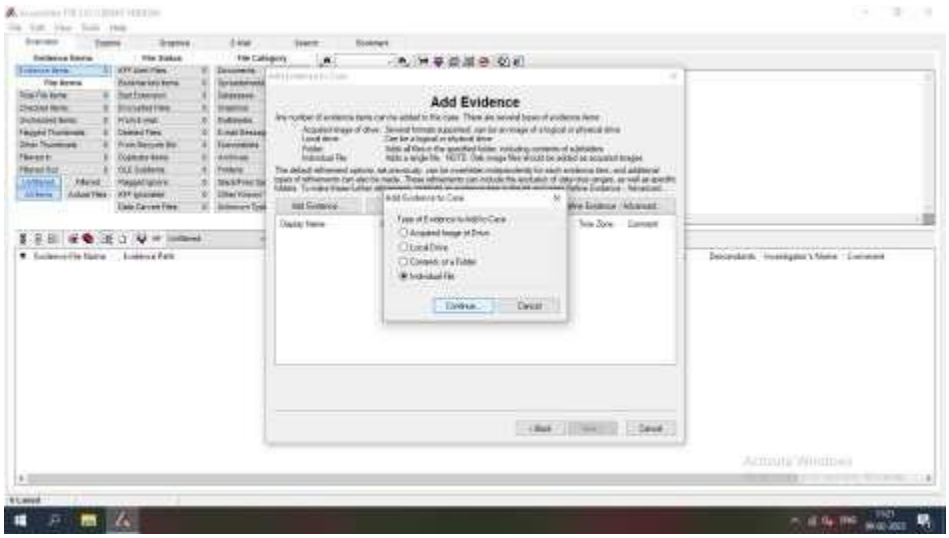


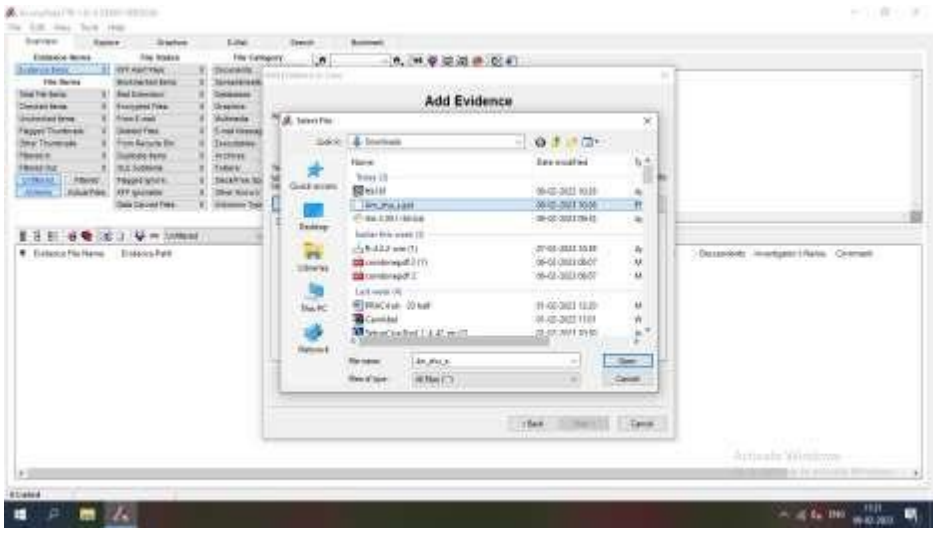

Processes to Perform

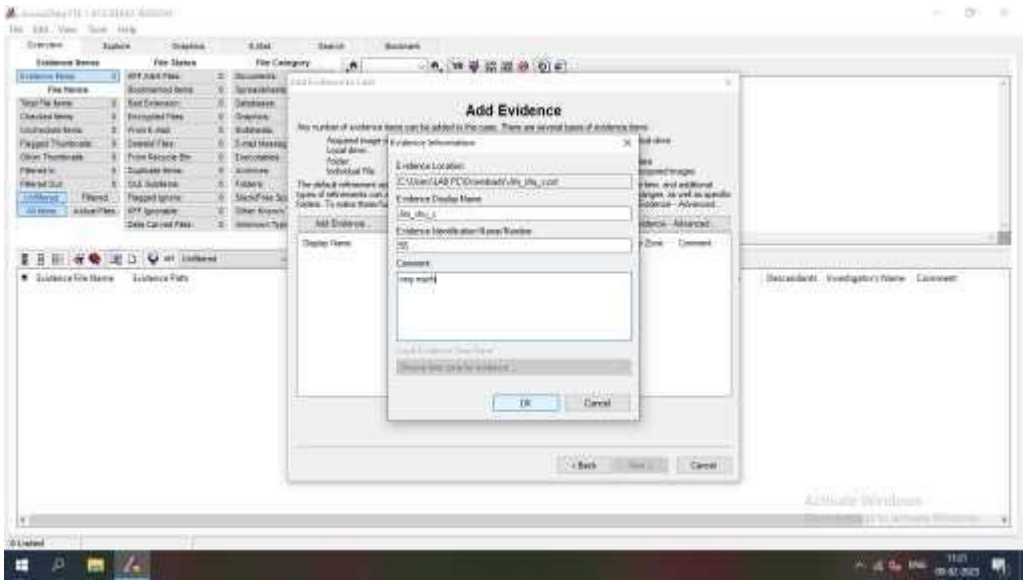

Processes to Perform

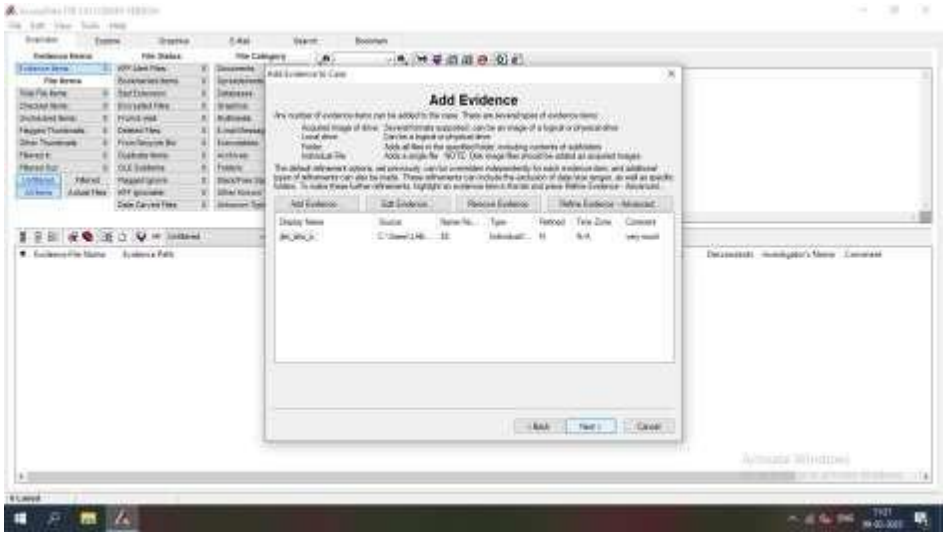

Refine Case - Default

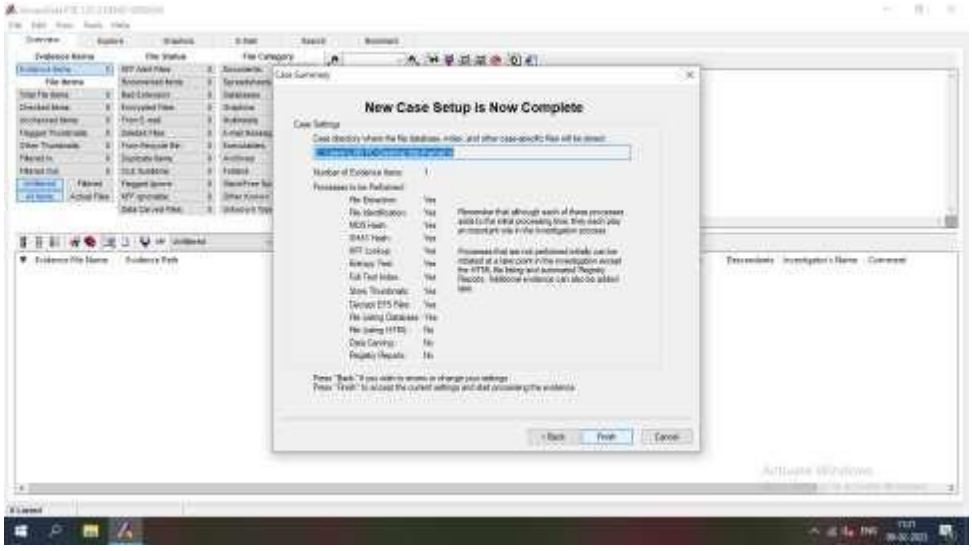

Refine Index - Default


Add Evidence


Add Evidence


Add Evidence
Evidence Location:
Comment:
very much
OK
Cancel
< Back
Cancel

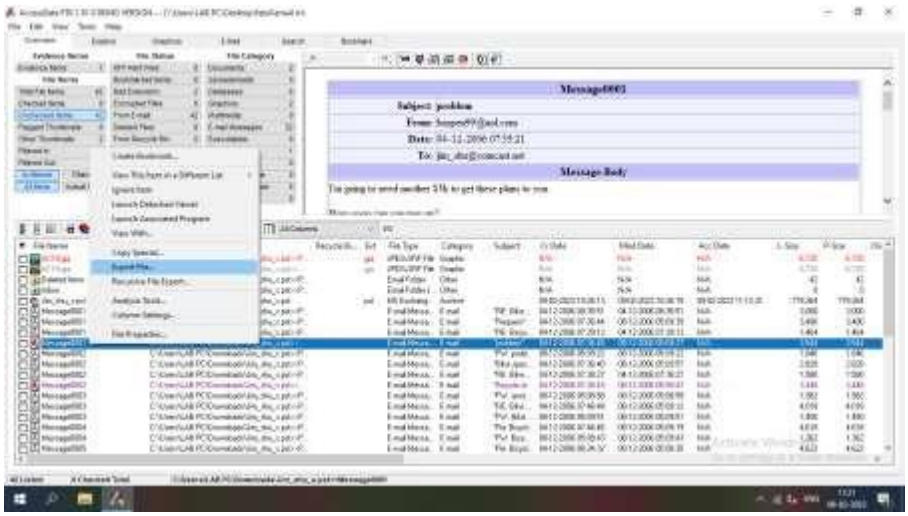

Add Evidence
Add Evidence
Edit Evidence
Remove Evidence
Refine Evidence - Advanced...
< Back
Next >
Cancel


New Case Setup Is Now Complete
Case Settings
Number of Evidence Items: 1
Processes to be Performed
< Back
Finish
Cancel

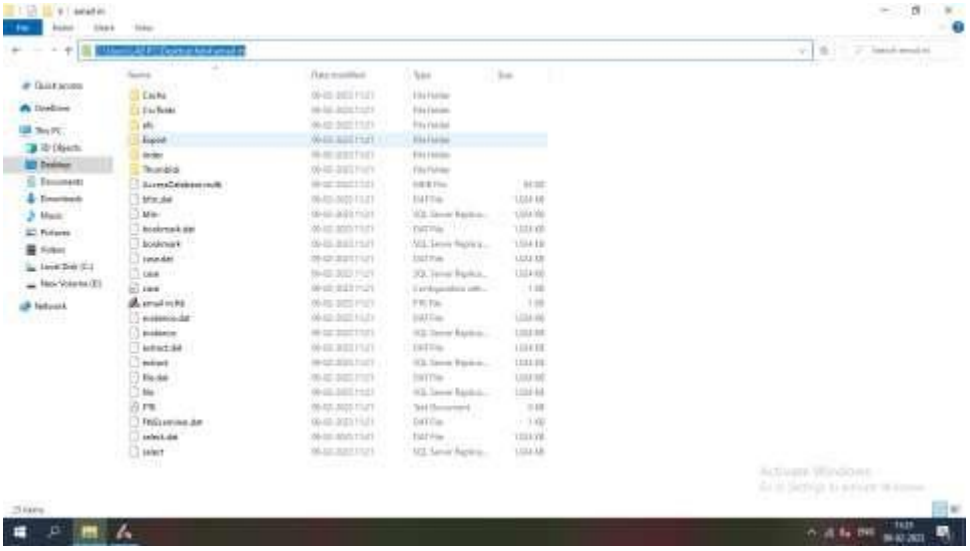
11. When the Add Evidence to Case dialog box opens, click Next. In the Case summary dialog box, click Finish.

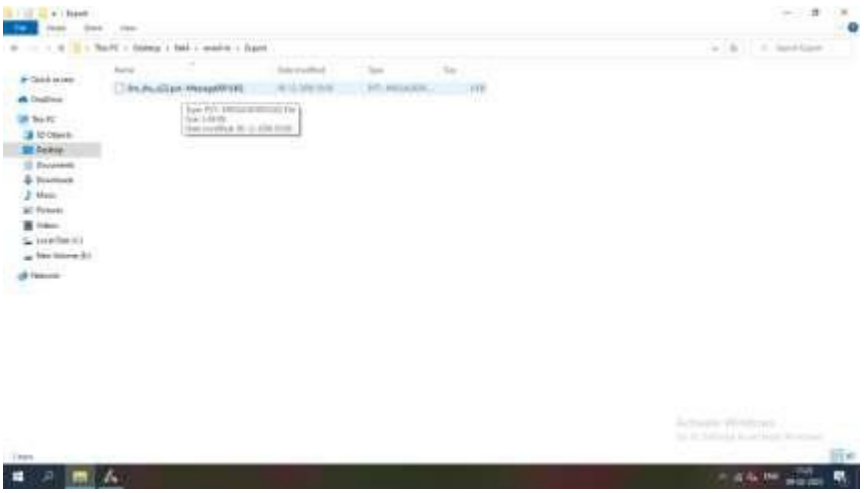
12. When FTK finishes processing the file, in the main FTK window, click the E-mail Messages button, and then click the Full Path column header to sort the records.

- Right-click Message0010 in the File List pane and click Export File. In the Export Files dialog box, click OK



- Open the Export folder to view the Email Files, Open the HTML file in browser





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.

How soon can you pay up?

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: problem Sender Name: baspen99@aol.com Received By: Jim Shu Delivery Time: 04-12-2006 07:35:21 Creation Time: 04-12-2006 07:36:45 Modification Time: 08-12-2006 05:09:27 Submit Time: 04-12-2006 07:35:15 Flags: 1 = Read Size: 5450
Standard Header Information
Received: from imo-d20.mx.aol.com ([205.188.139.136]) by sccrmxc18.comcast.net (sccrmxc18) with ESMTP id <20061204020521s18004fbkge>; Mon, 4 Dec 2006 02:05:21 +0000 X-Originating-IP: [205.188.139.136] Received: from Baspen99@aol.com by imo-d20.mx.aol.com (mail_out_v38_r7.6.) id i.406.33cb6298 (60434) for <jim_shu@comcast.net>; Sun, 3 Dec 2006 21:05:18 -0500 (EST) Received: from FWM-D21 (fwm-d21.webmail.aol.com [205.188.160.213]) by cianol-d01.mail.aol.com (v114.2) with ESMTP id MAILCIAAOLD013-ec124573825b284; Sun, 03 Dec 2006 21:05:15 -0500 To: jim_shu@comcast.net Subject: problem Date: Sun, 03 Dec 2006 21:05:15 -0500 X-MB-Message-Source: WebUI MIME-Version: 1.0 From: baspen99@aol.com X-MB-Message-Type: User Content-Type: multipart/alternative;

Practical 10

Aim : Web Browser Forensic

BrowsingHistoryView : BrowsingHistoryView is a utility that reads the history data of 4 different Web browsers (Internet Explorer, Mozilla Firefox, Google Chrome, and Safari) and displays the browsing history of all these Web browsers in one table. The browsing history table includes the following information: Visited URL, Title, Visit Time, Visit Count, Web browser and User Profile. BrowsingHistoryView allows you to watch the browsing history of all user profiles in a running system, as well as to get the browsing history from external hard drive. You can also export the browsing history into csv/tab-delimited/html/xml file from the user interface, or from command-line, without displaying any user interface.

IECacheView : IECacheView is a small utility that reads the cache folder of Internet Explorer, and displays the list of all files currently stored in the cache. For each cache file, the following information is displayed: Filename, Content Type, URL, Last Accessed Time, Last Modified Time, Expiration Time, Number Of Hits, File Size, Folder Name, and full path of the cache filename. You can easily save the cache information into text/html/xml file, or copy the cache table to the clipboard and then paste it to another application, like Excel or OpenOffice Spreadsheet.

MZCookiesView : MZCookiesView is an alternative to the standard 'Cookie Manager' provided by Netscape and Mozilla browsers. It displays the details of all cookies stored inside the cookies file (cookies.txt) in one table, and allows you to save the cookies list into text, HTML or XML file, delete unwanted cookies, and backup/restore the cookies file.

MZCacheView : MZCacheView is a small utility that reads the cache folder of Firefox/Mozilla/Netscape Web browsers, and displays the list of all files currently stored in the cache. For each cache file, the following information is displayed: URL, Content type, File size, Last modified time, Last fetched time, Expiration time, Fetch count, Server name, and more.You can easily select one or more items from the cache list, and then extract the files to another folder, or copy the URLs list to the clipboard.

ChromeCacheView : ChromeCacheView is a small utility that reads the cache folder of Google Chrome Web browser, and displays the list of all files currently stored in the cache. For each cache file, the following information is displayed: URL, Content type, File size, Last accessed time, Expiration time, Server name, Server response, and more. You can easily select one or more items from the cache list, and then extract the files to another folder, or copy the URLs list to the clipboard.