

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**

DATEHEAD 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 :- <ul style="list-style-type: none"> ▪ Creating Forensic Image ▪ Check Integrity of Data ▪ Analyze Forensic Image 	8/12/2022		
2	Data Acquisition: <ul style="list-style-type: none"> ▪ 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 : <ul style="list-style-type: none"> ▪ 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 <ul style="list-style-type: none"> ▪ 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 <ul style="list-style-type: none"> • Mail Service Providers • Email protocols • Recovering emails • Analyzing email header 	23/02/2023		
10	Web Browser Forensics . <ul style="list-style-type: none"> ▪ 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

Name	Date modified	Type	Size
Netbeans	03-10-2022 14:30	File folder	
node	18-11-2022 03:20	File folder	
oracle11	03-10-2022 14:30	File folder	
software testing	10-10-2022 13:09	File folder	
Bhavika sawant SYBAF	03-11-2022 11:15	Microsoft PowerPoint presentation	42 KB
New Microsoft PowerPoint Presentation	02-11-2022 12:09	Microsoft PowerPoint presentation	42 KB
original	08-12-2022 10:56	File folder	

Steps:

First create a folder

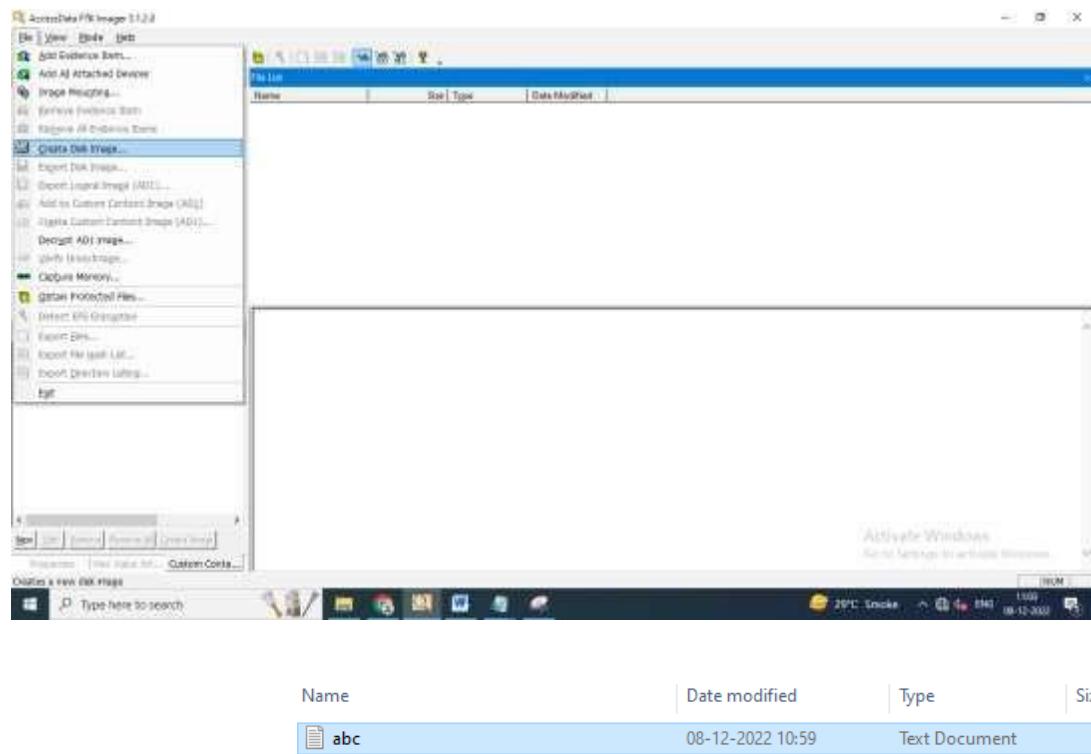
Name	Date modified	Type	Size
Cisco Packet Tracer	09-11-2022 08:46	Shortcut	2 KB
MongoDBCompass	03-12-2022 08:18	Shortcut	3 KB
Person 1 - Chrome	06-12-2022 10:16	Shortcut	3 KB
TurboC++	21-11-2022 12:44	Shortcut	1 KB
xssx - Chrome	08-12-2022 07:52	Shortcut	3 KB
zzz	08-12-2022 10:57	File folder	

In that folder create a folder name tha folder Forensic copy

Name	Date modified	Type	Size
Netbeans	03-10-2022 14:30	File folder	
node	18-11-2022 03:20	File folder	
oracle11	03-10-2022 14:30	File folder	
original	08-12-2022 11:00	File folder	
software testing	10-10-2022 13:09	File folder	
Bhavika sawant SYBAF	03-11-2022 11:15	Microsoft PowerPoint presentation	42 KB
New Microsoft PowerPoint Presentation	02-11-2022 12:09	Microsoft PowerPoint presentation	42 KB
forensic copy	08-12-2022 11:00	File folder	

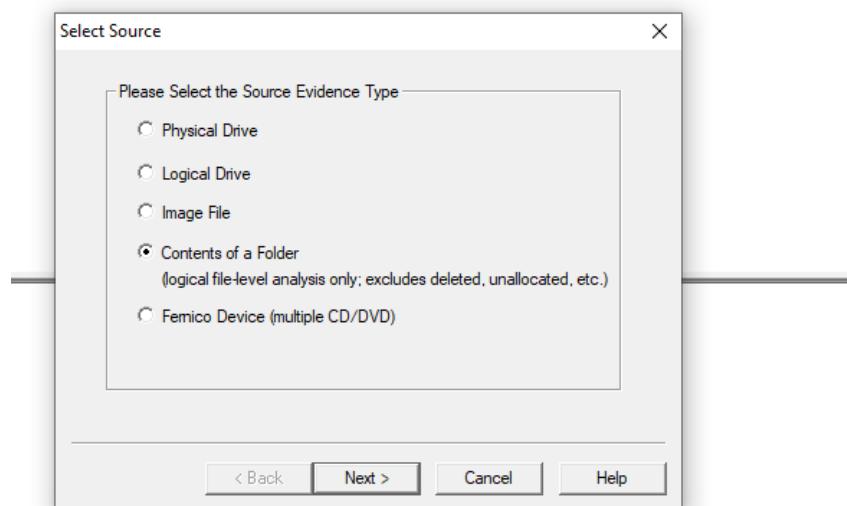
Creating Forensic Image

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

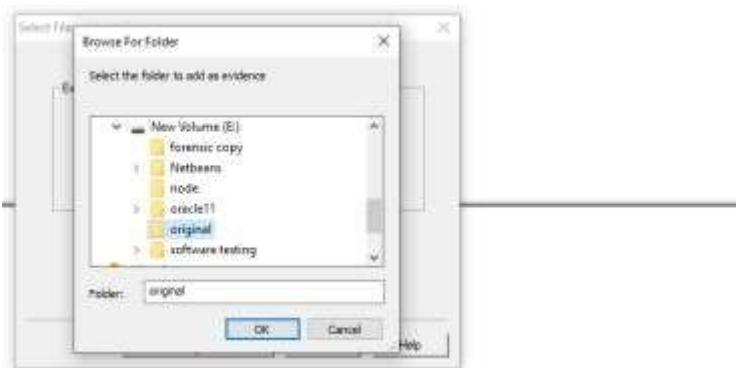


Select the folder

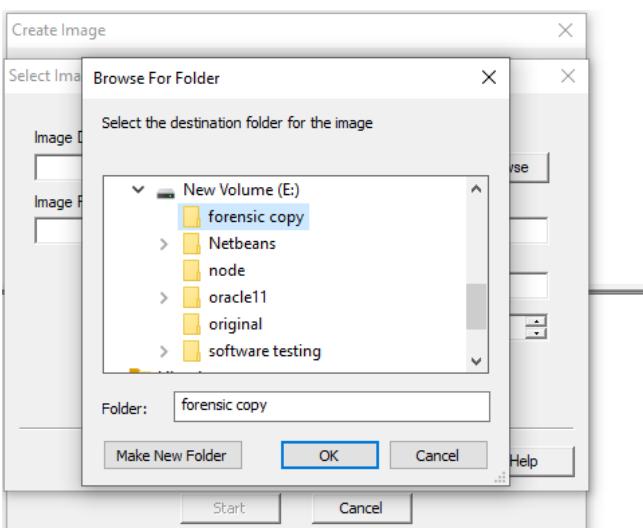
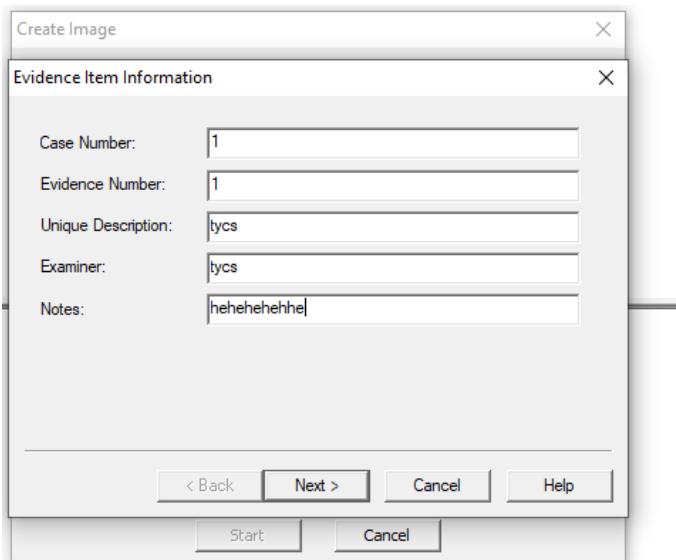
2. Select the source you want to make an image of and click Next.



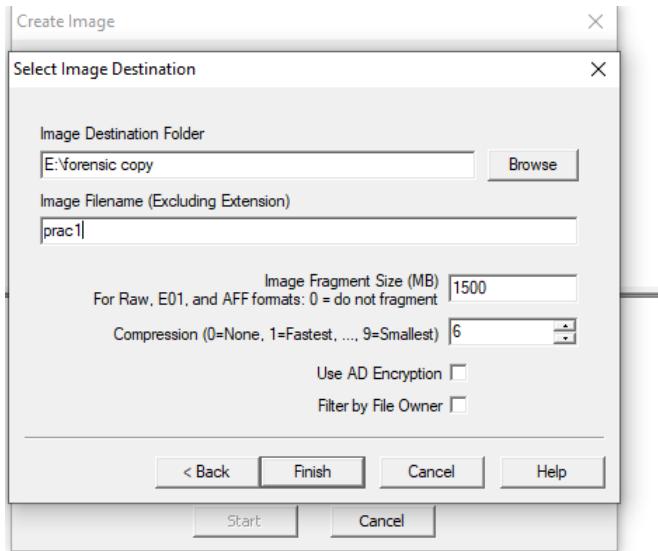
Select Original folder



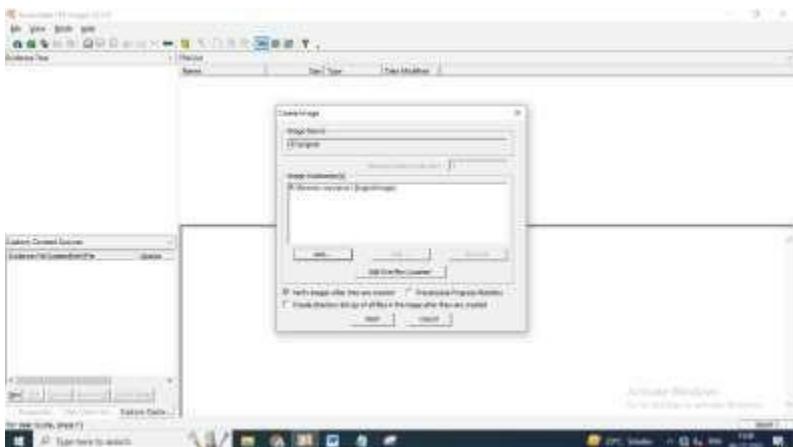
3. fill this



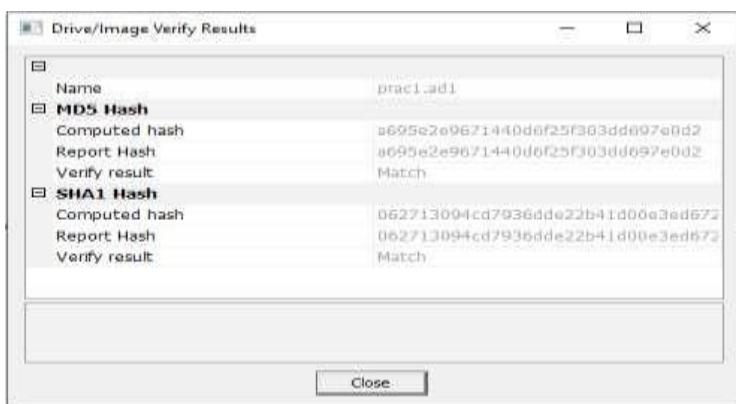
4. Browse the folder <finish>



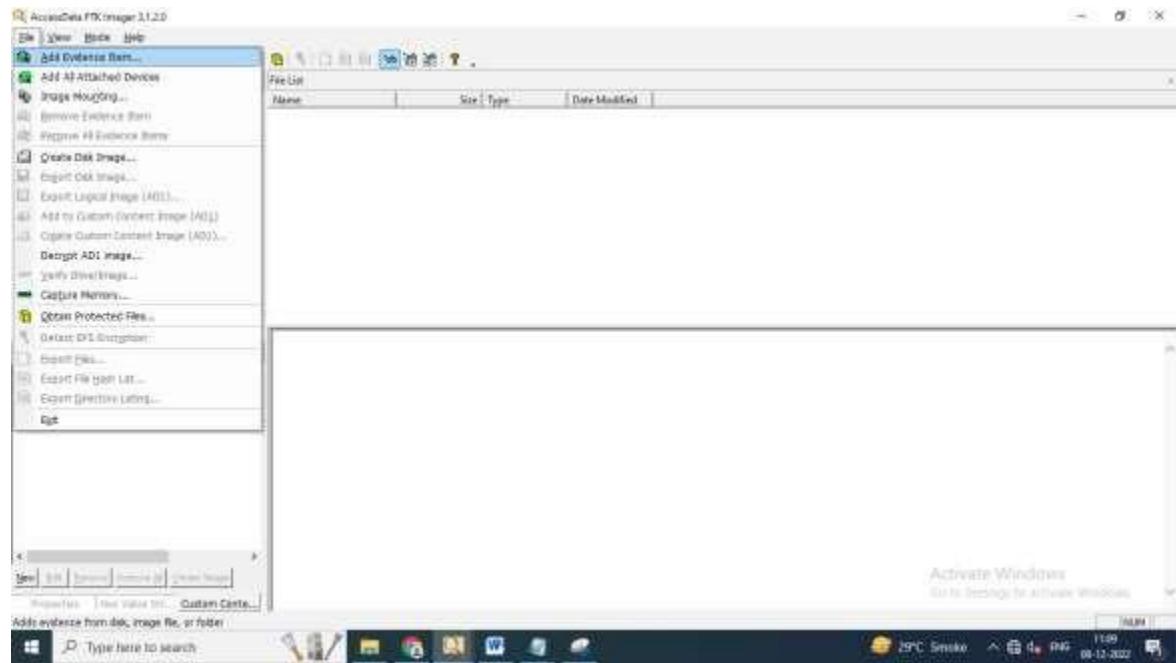
5. Add a folder <Start>



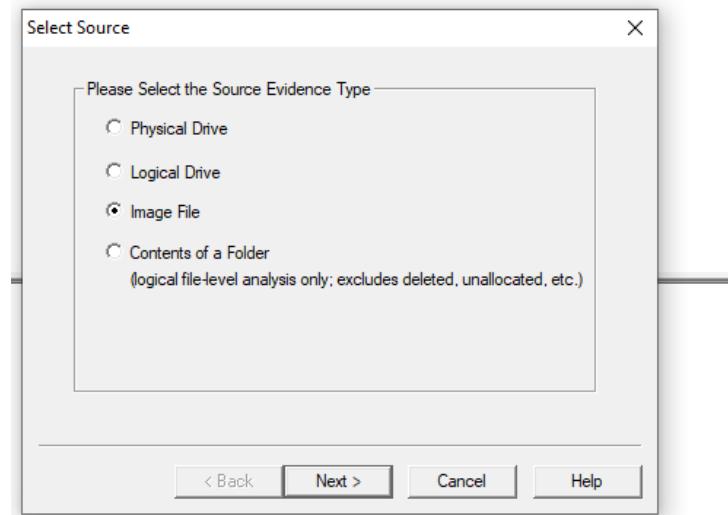
6. choose any <Close>



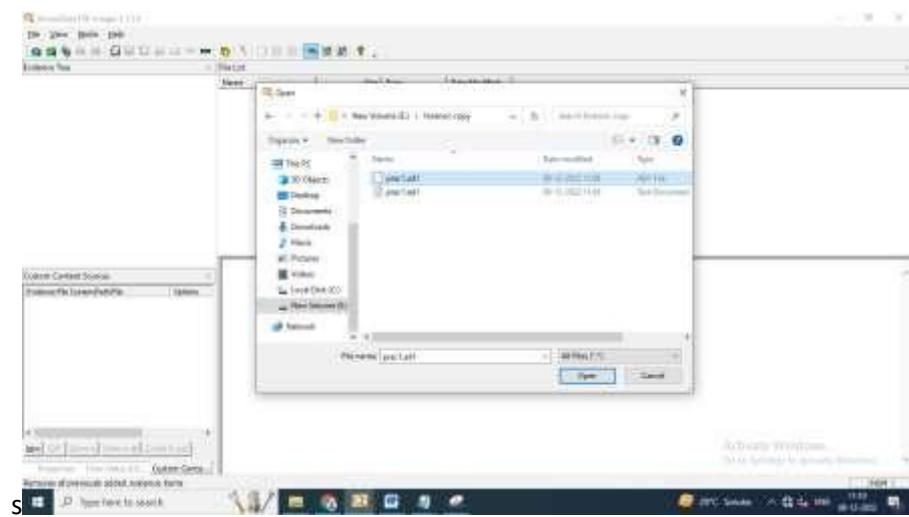
7.Add Evidence Item



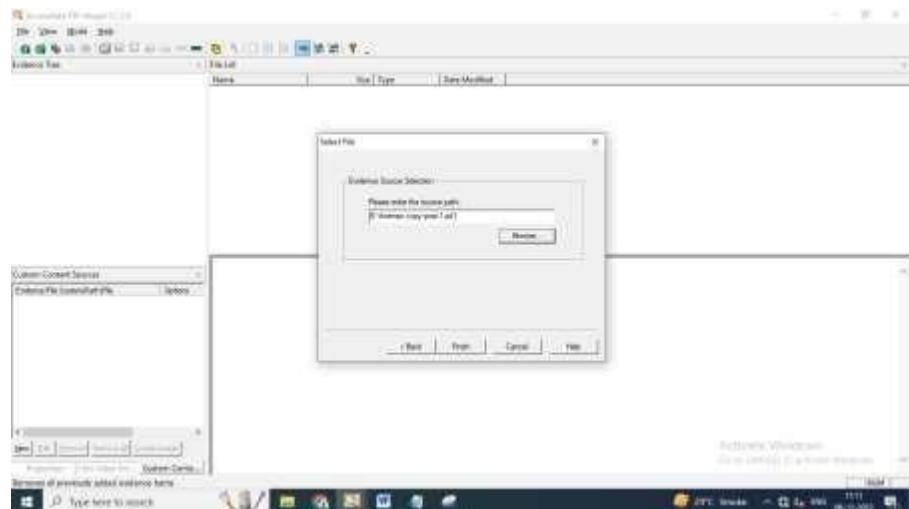
8.Select Image File <next>



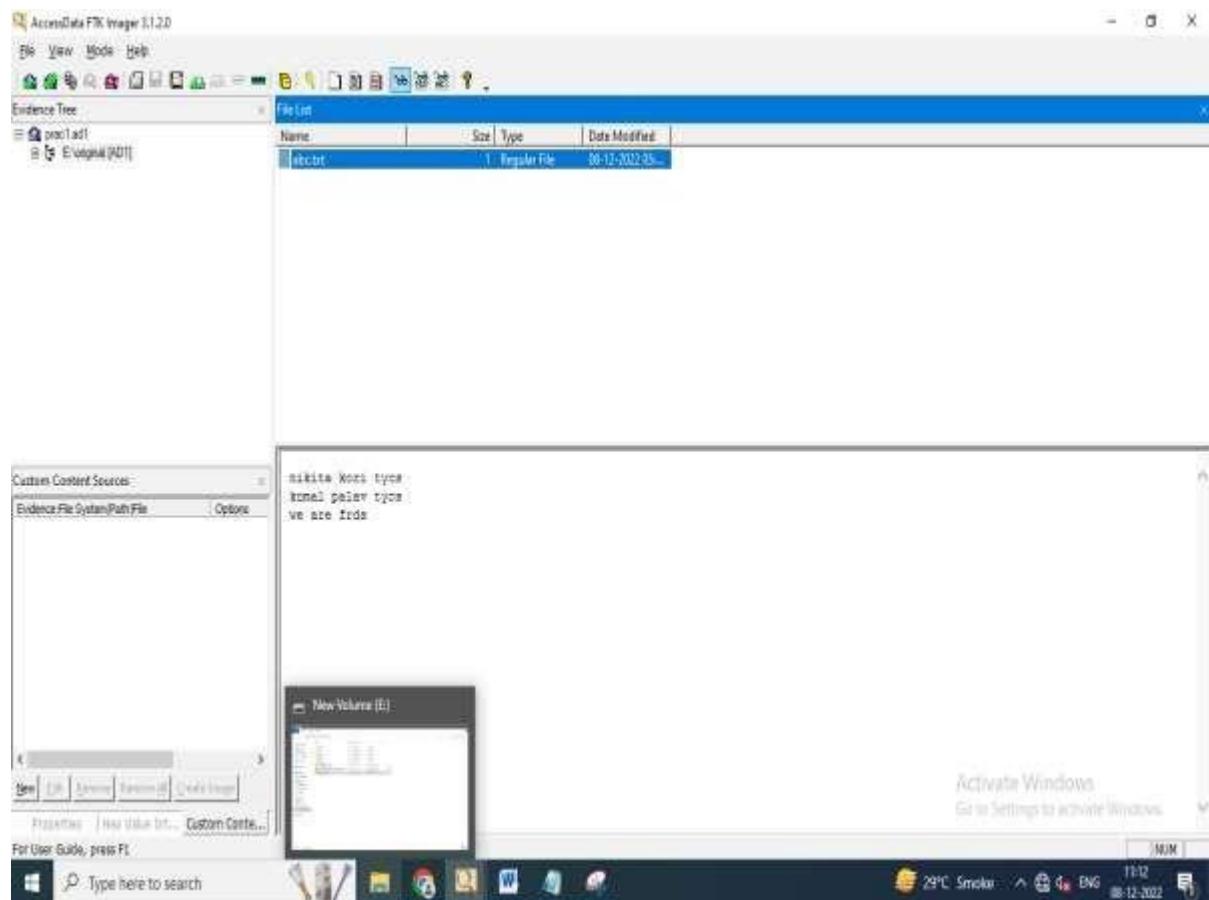
Select a folder you create.



Browser it.



THE OUTPUT:



Practical No : 2

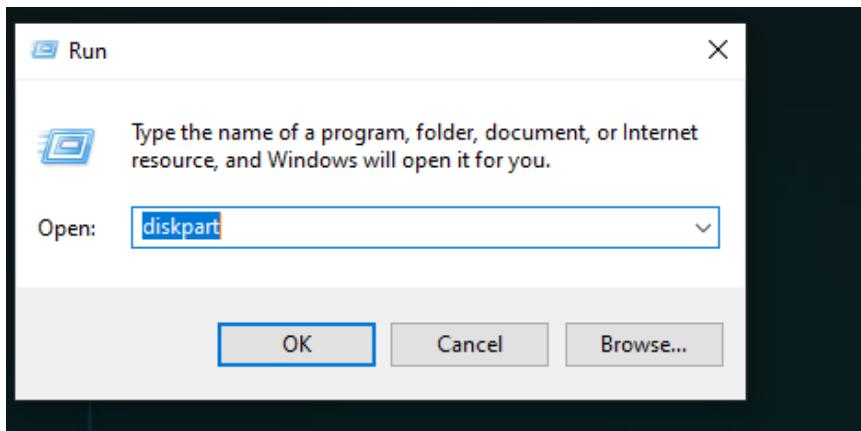
Aim: Data Acquisition:

- 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>
```

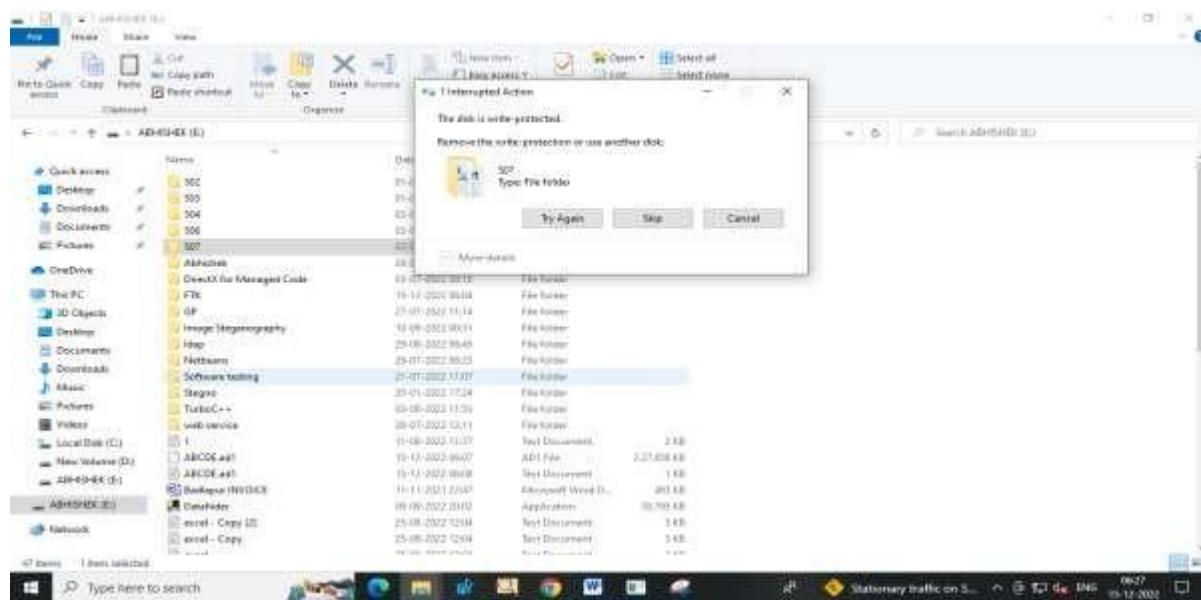
```
DISKPART> attributes disk  
Current Read-only State : No  
Read-only : No  
Boot Disk : No  
Pagefile Disk : No  
Hibernation File Disk : No  
Crashdump Disk : No  
Clustered Disk : No
```

```
DISKPART>
```

Run successfully

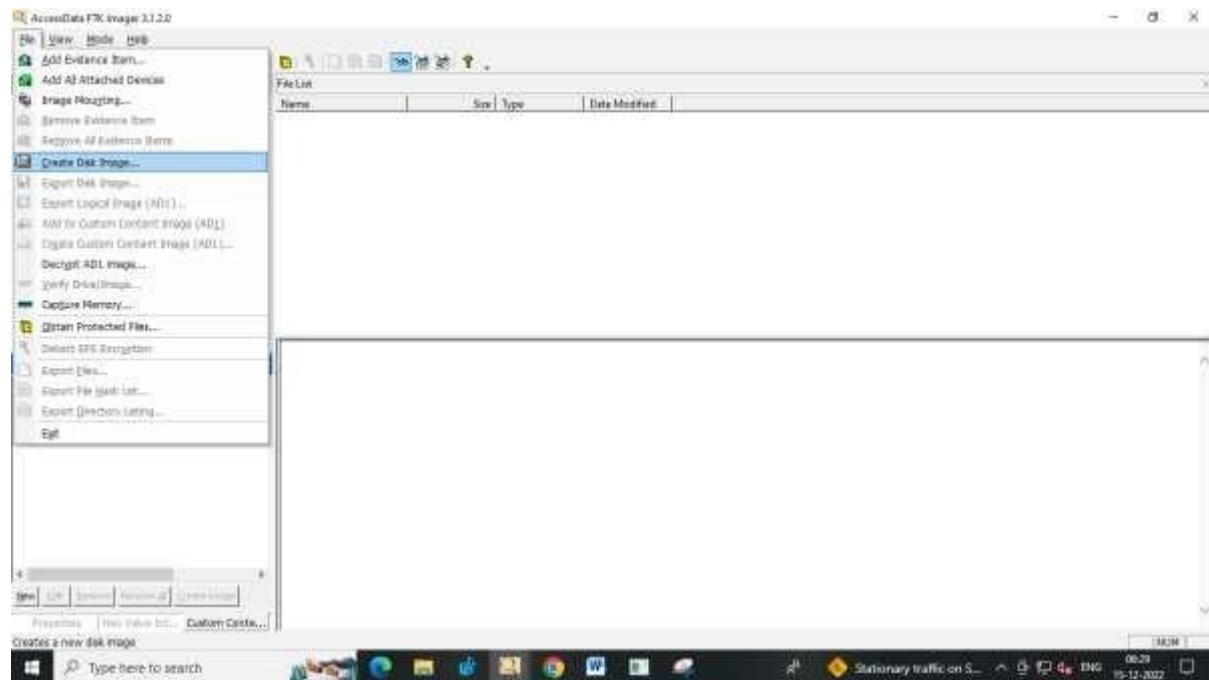
```
DISKPART> attributes disk set readonly  
Disk attributes set successfully.  
DISKPART>
```

Steps1: select any folder

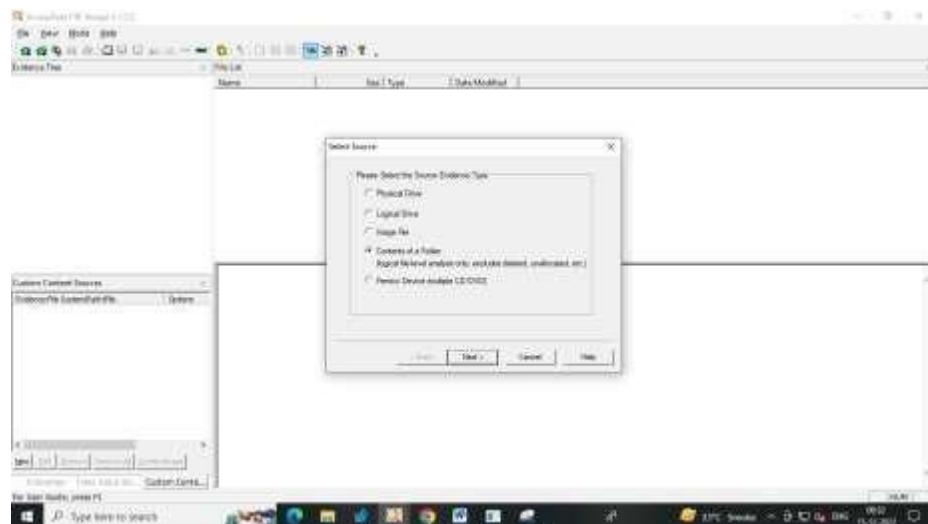


Steps:

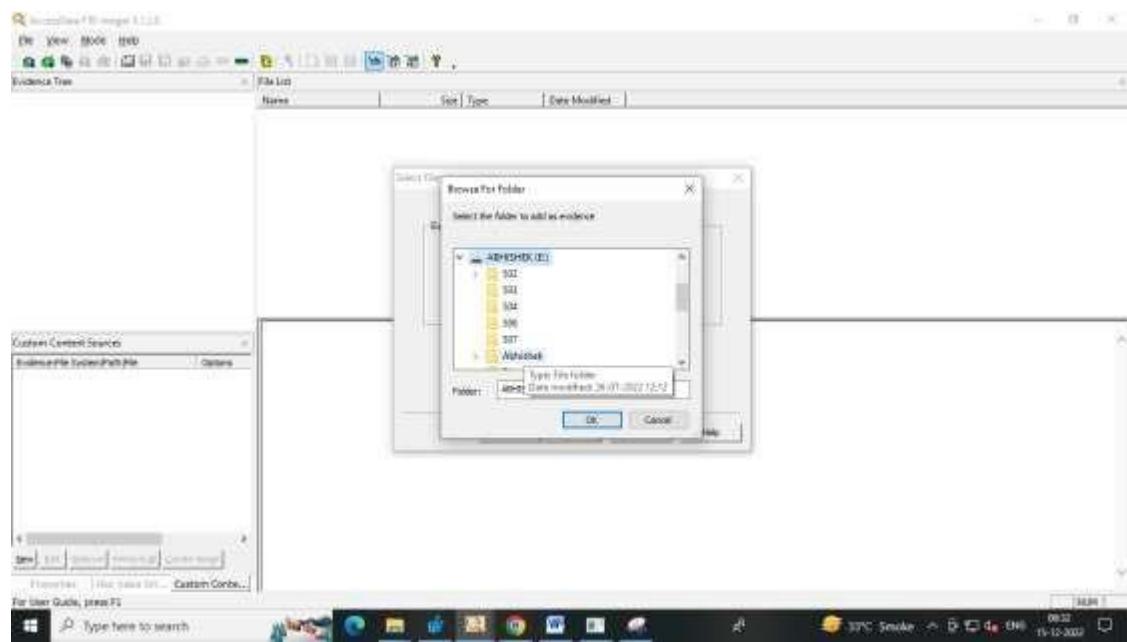
1.Create Disk Image



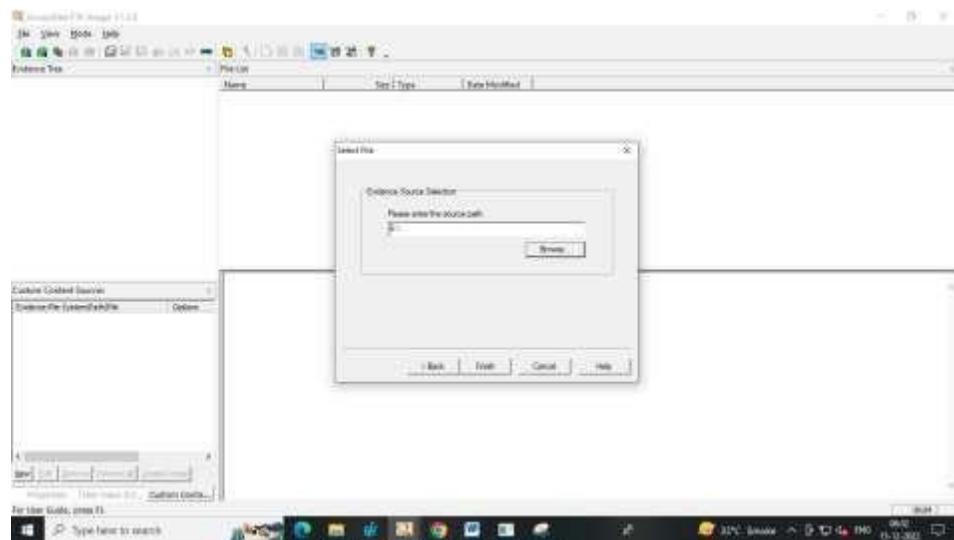
2.Select Contents of a Folder



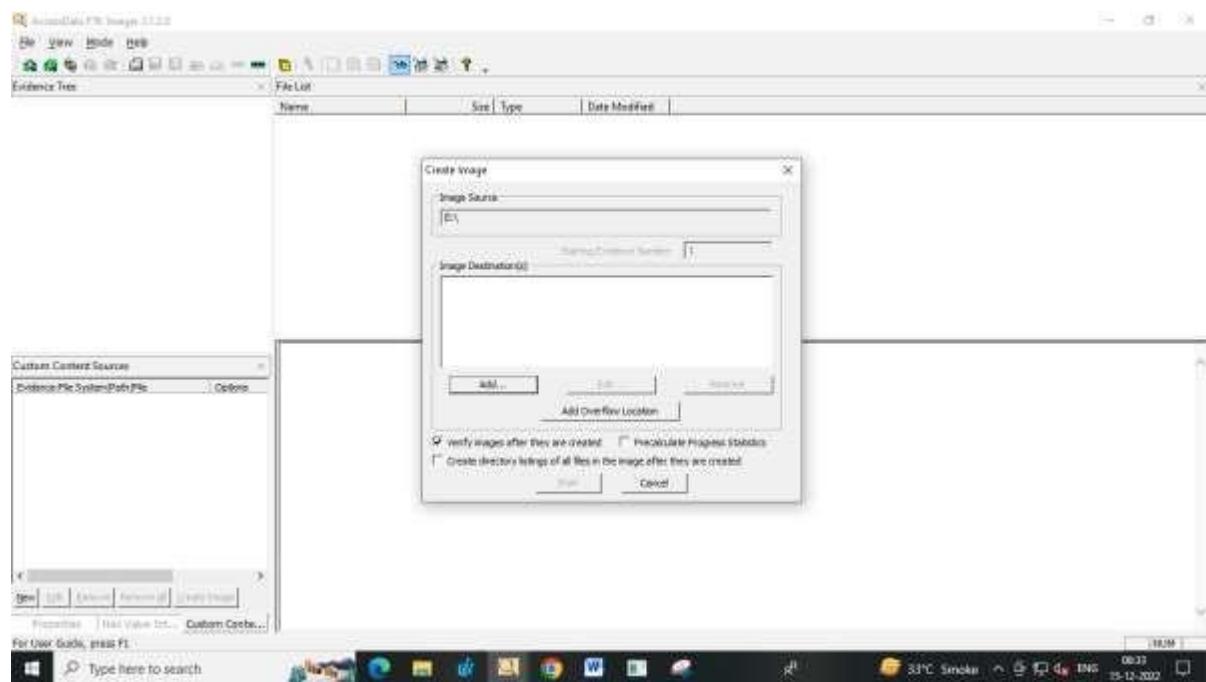
Select a folder<ok>



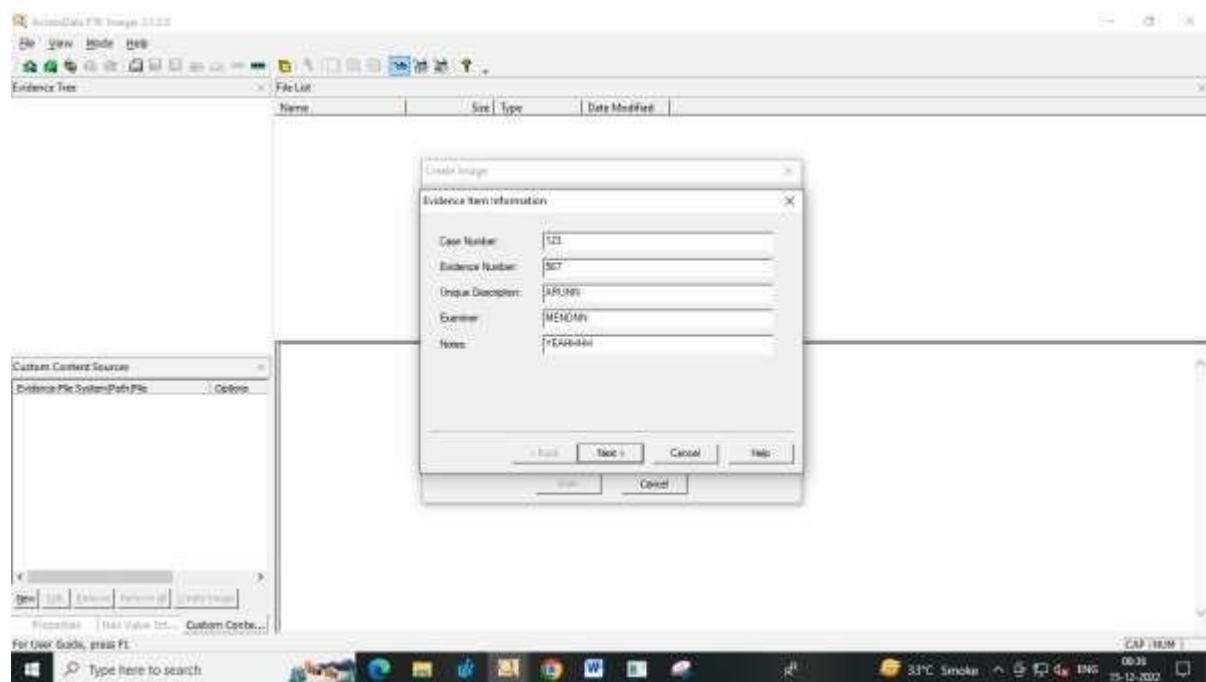
Browser it.



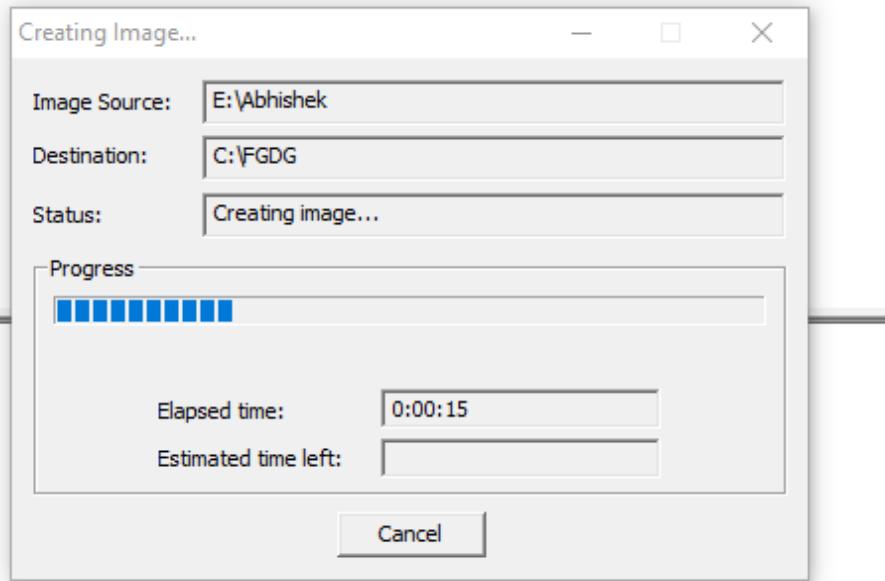
3. Add <Start>



5. Fill the case no <next>



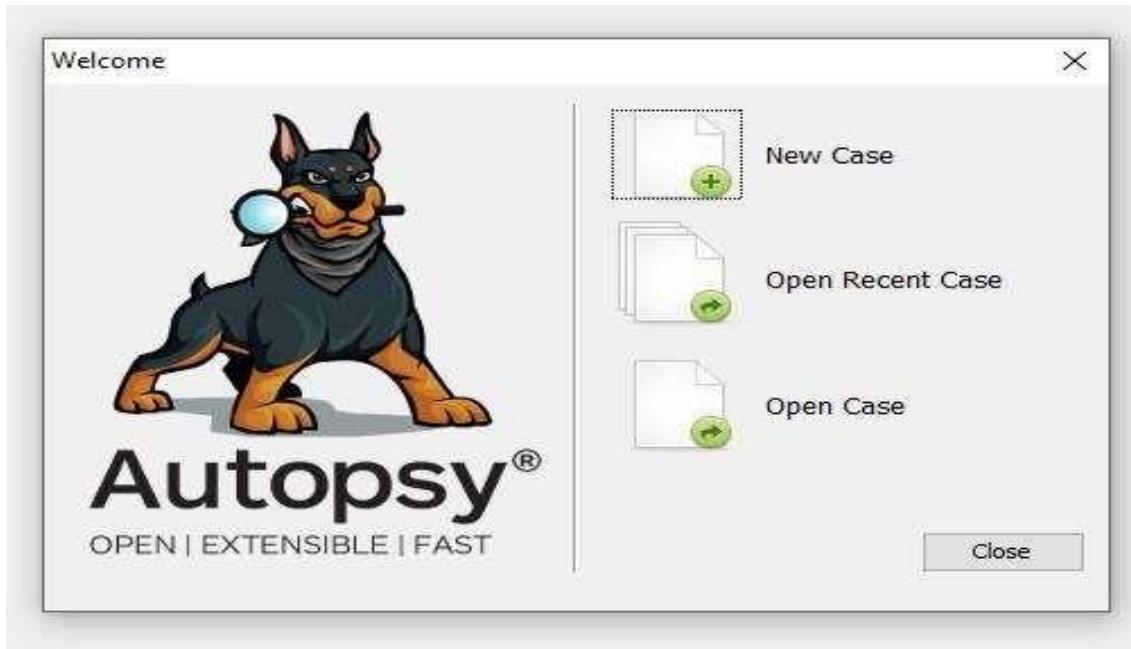
THE OUTPUT:



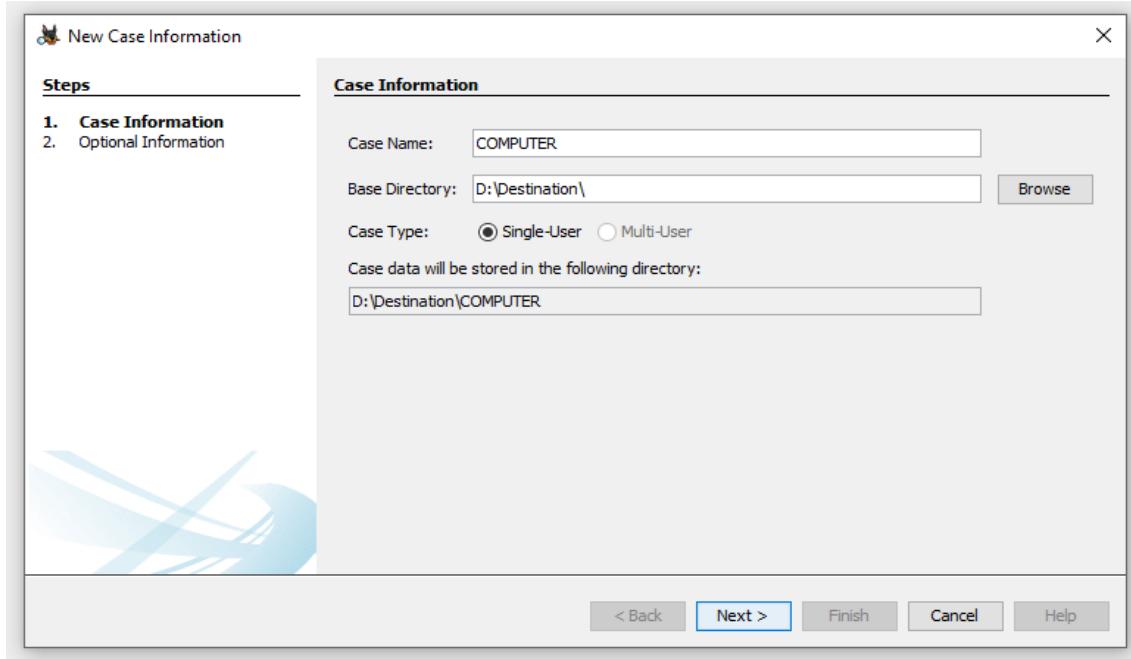
Practical No :- 3

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

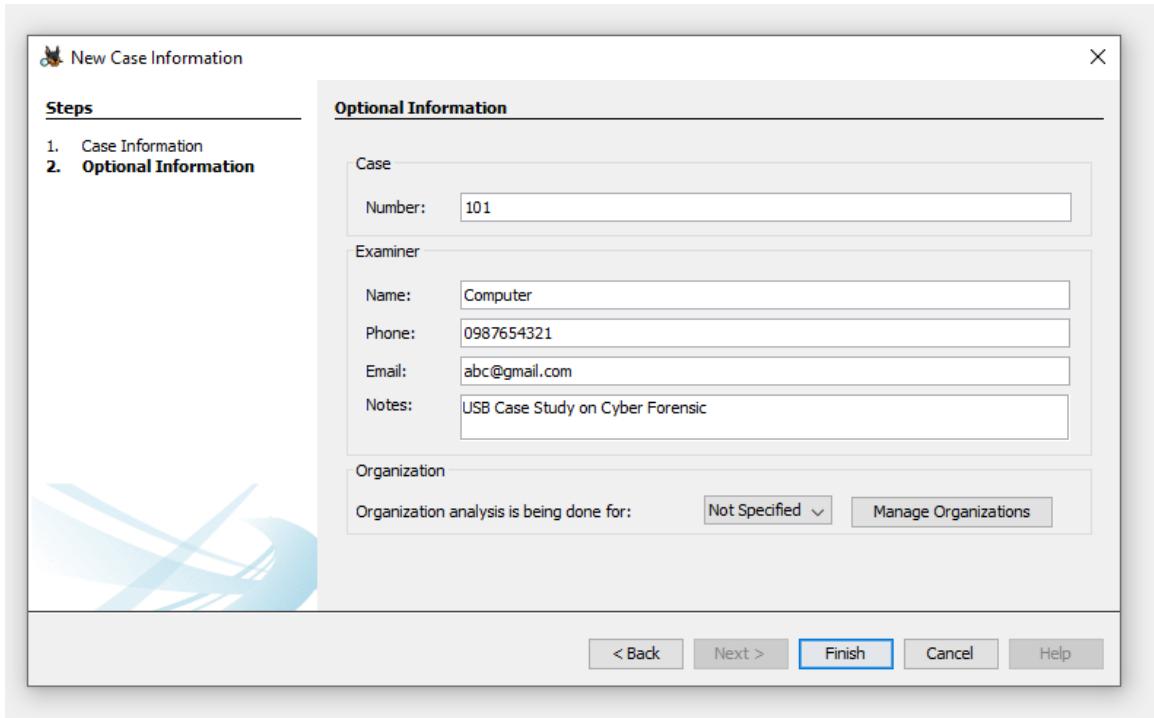
1. Start Autopsy -> Select New Case.



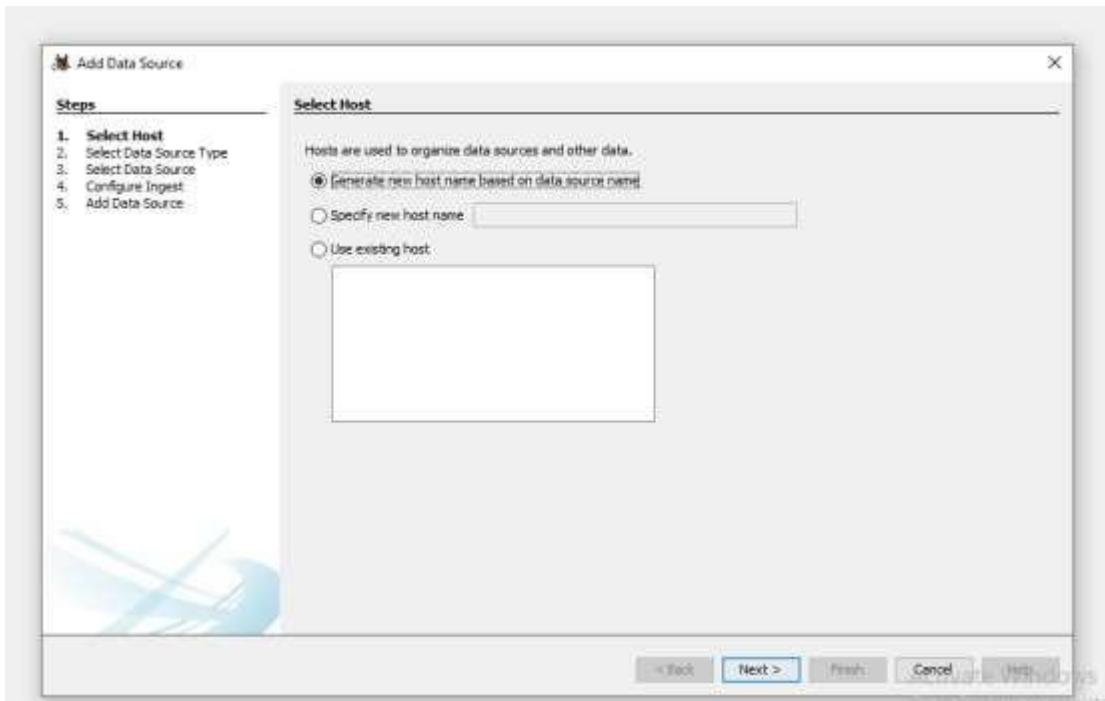
2. Enter Case Information -> Browse Base Directory & Click on Next



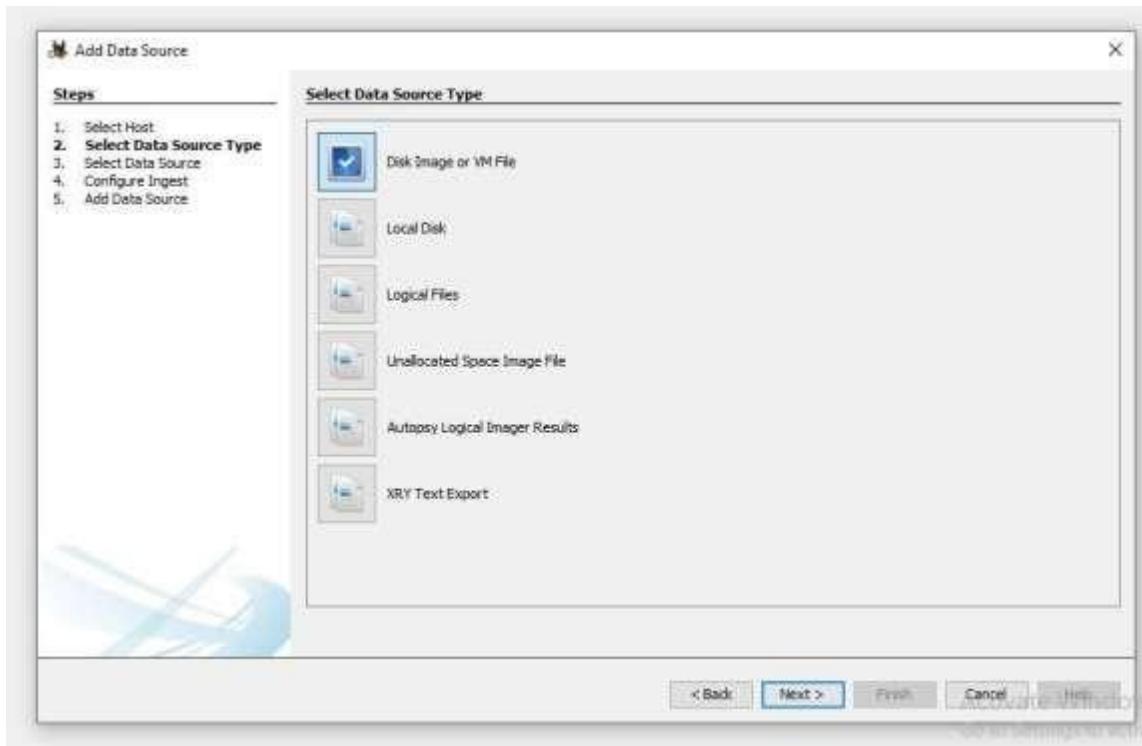
3. Fill all Optional Information.



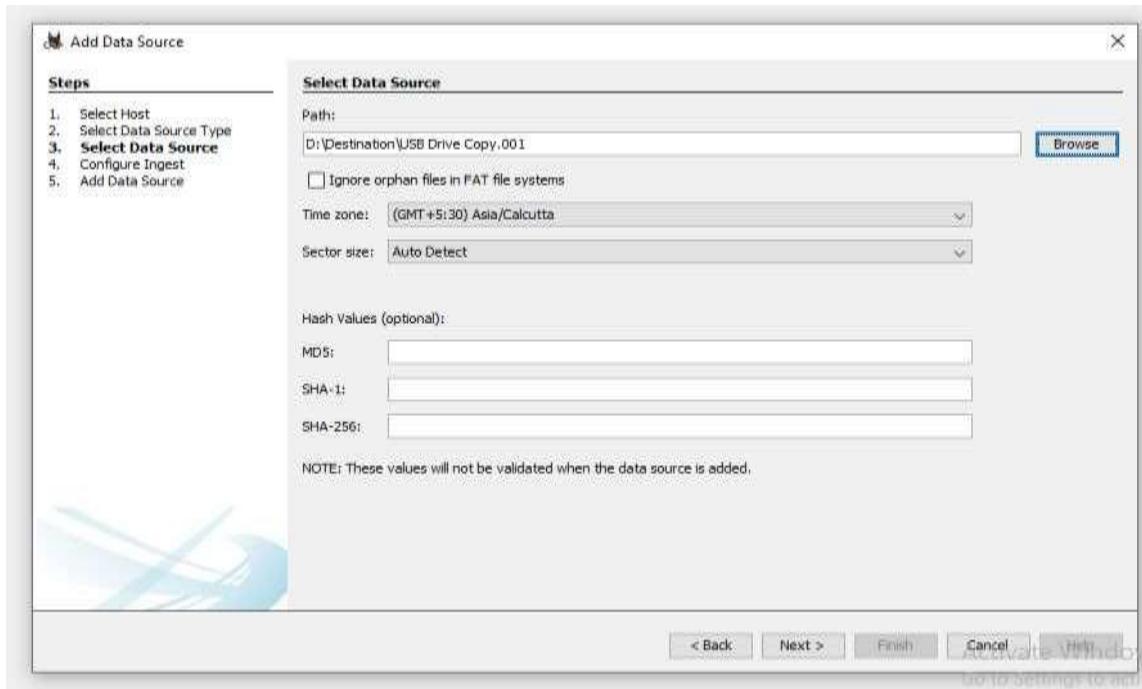
4. In Select Host we will select -> Generate new host name based on data source name and click on Next.



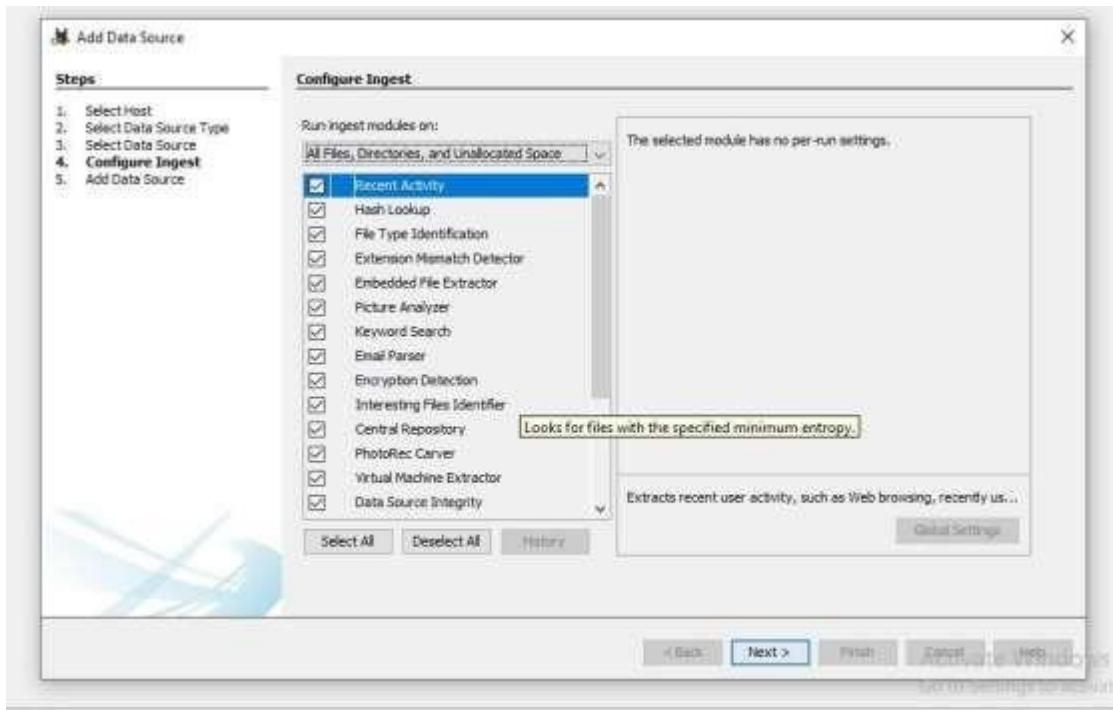
5. Select the type of Data Source that has to be added.



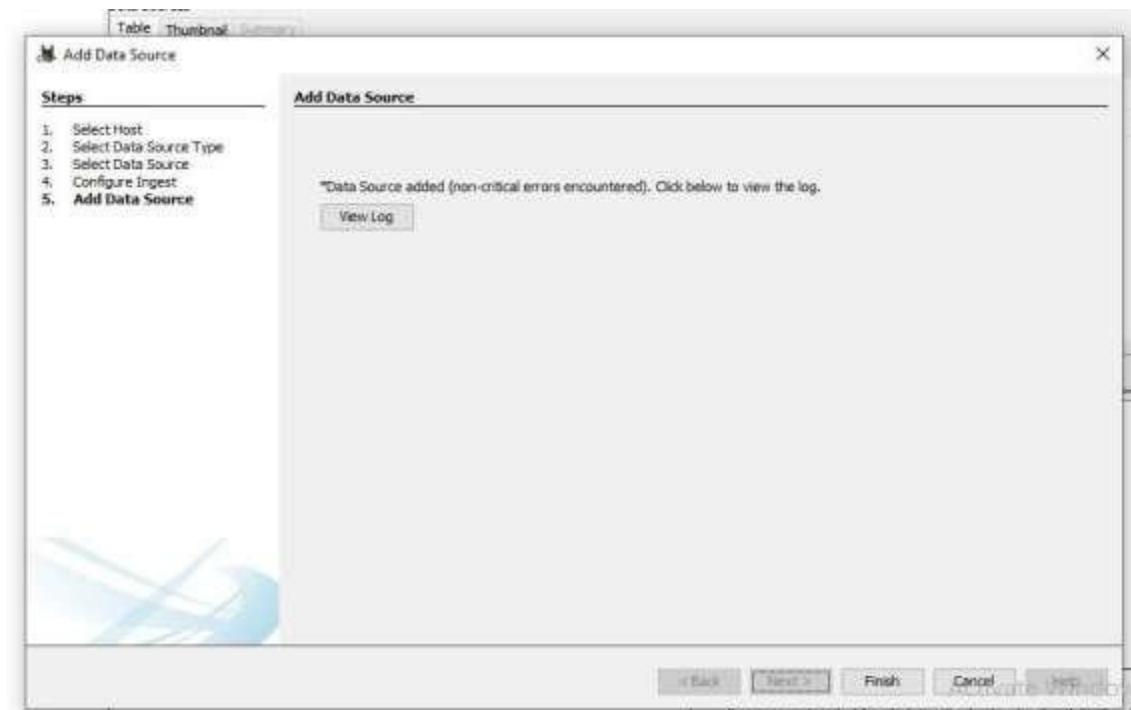
6. Select Data Source (here a previously made image file of USB is selected)



7. Select all ingest modules.



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



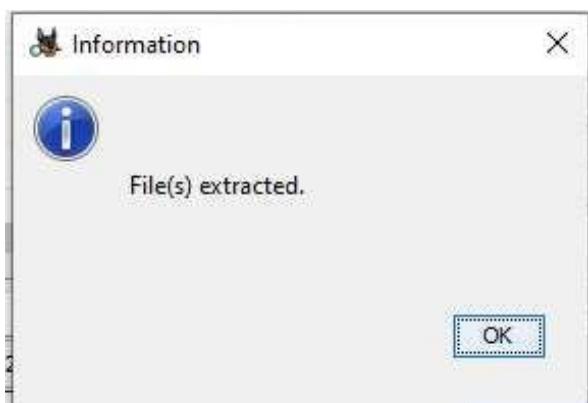
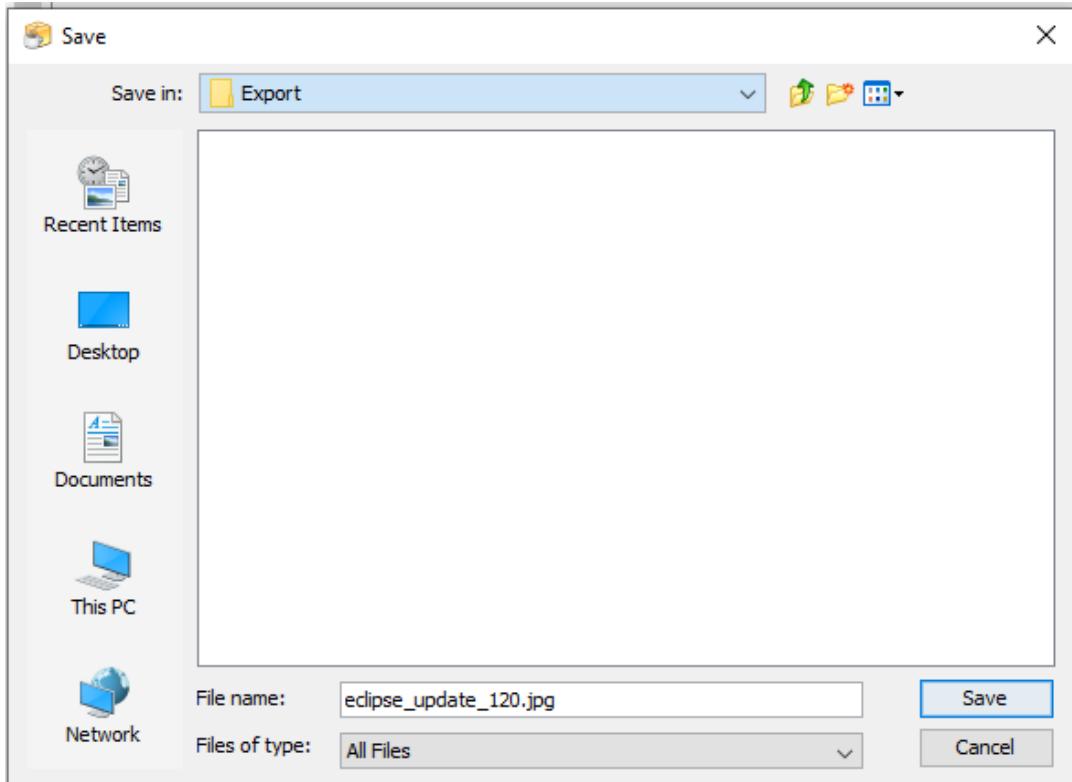
9. Now Autopsy window will appear and it will analyzing the disk that we have selected.

The screenshot shows the Autopsy 4.16.3 interface. On the left, a tree view displays a hierarchy of data sources, including 'USB Drive Copy.001_1.HDD' which contains numerous files and folders. The right side features a table view titled 'Table' showing a list of files. The columns include Name, S, C, O, Modified Time, Change Time, Access Time, Created Time, and Size. A specific file, 'eclipse_update_120.jpg', is highlighted in the table. At the bottom, there's a status bar indicating 'Analysing New File from USB Drive Copy.001'.

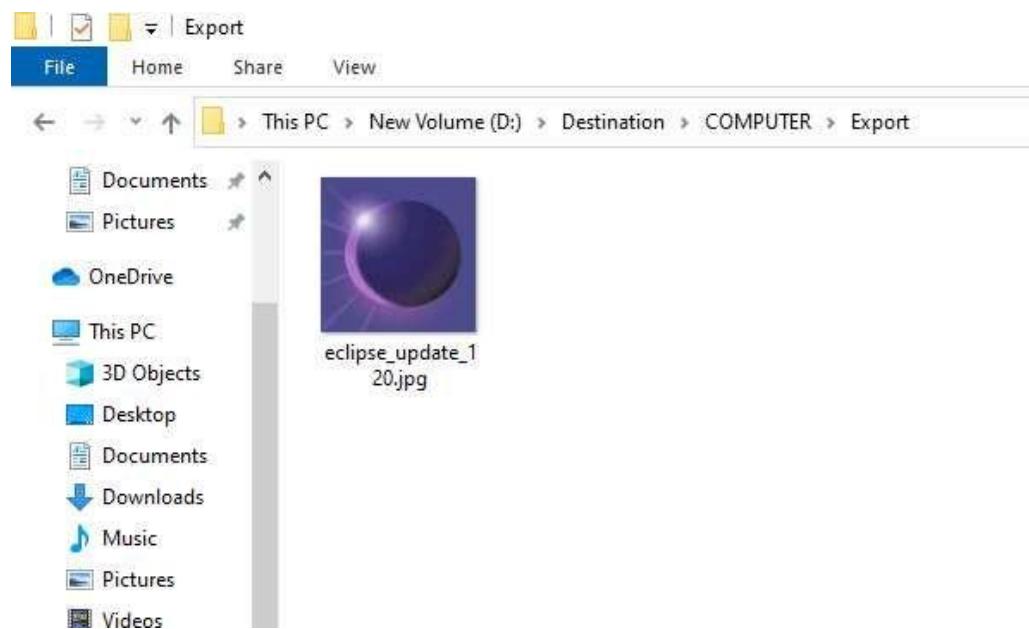
10. All files will appear in table tab select any file to see the data.
11. Expand the tree from left side panel to view the files and then expand the deleted files Node.
12. To recover the file, go to view node-> Deleted Files node -> Select any file -> Right click on it than select Extract Files option.

This screenshot shows the same Autopsy interface as above, but with a different focus. The 'Deleted Files' node is selected in the tree view on the left. A context menu is open over a file named 'eclipse_update_120.jpg'. The menu options include 'Properties', 'View File in Directory', 'View in New Window', 'Open in External Viewer - Ctrl+E', 'View File in Timeline...', 'Extract File(s)', 'Export Selected Rows for CSV', 'Add File Tag', 'Remove File Tag', 'Add/Edit Central Repository Comment', and 'Add File to Hash Set (Engage & analyze...)'. The status bar at the bottom indicates 'Analysing New File from USB Drive Copy.001'.

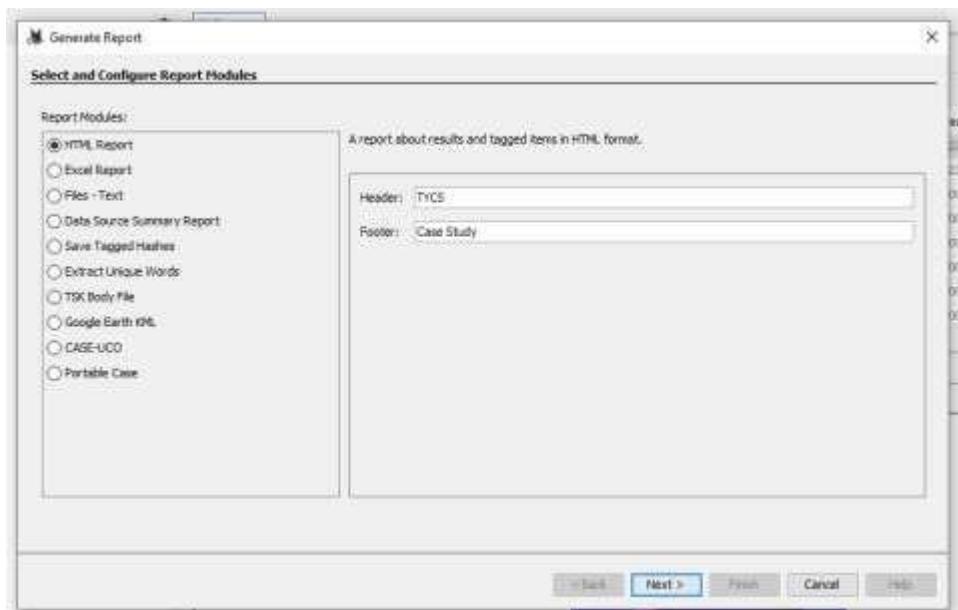
13. By default Export folder is choose to save the recovered file.

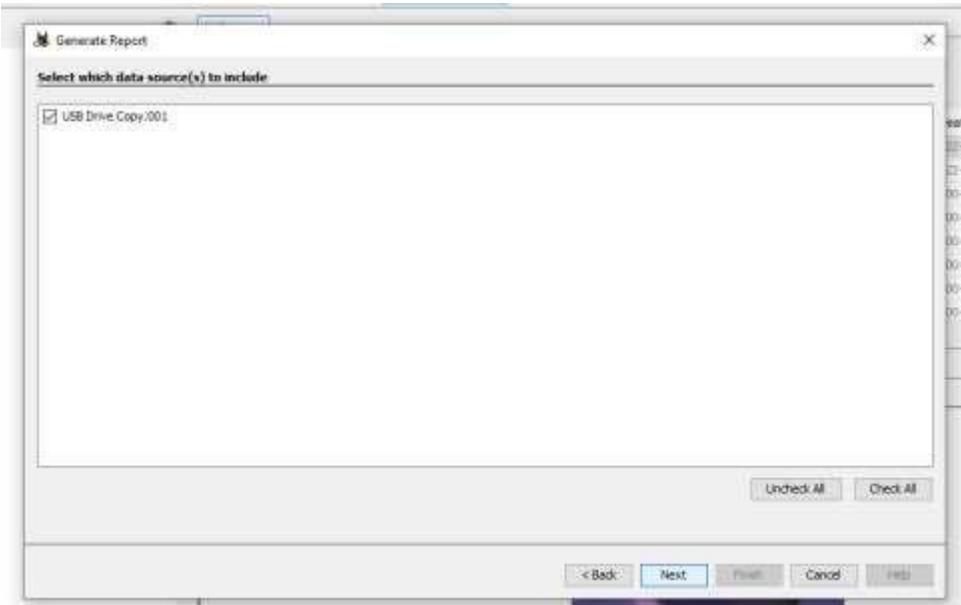


14. Now go to the Export Folder to view Recover file.

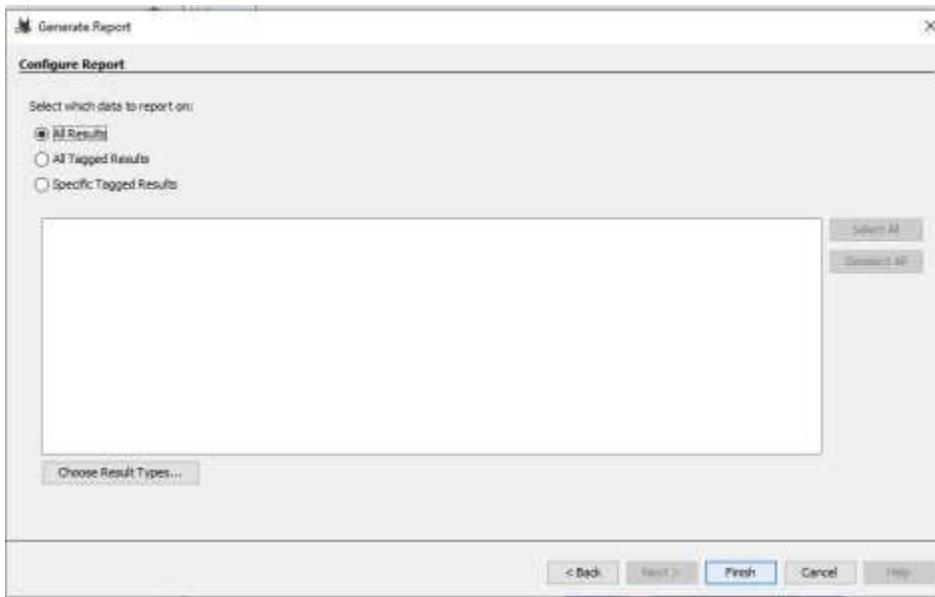


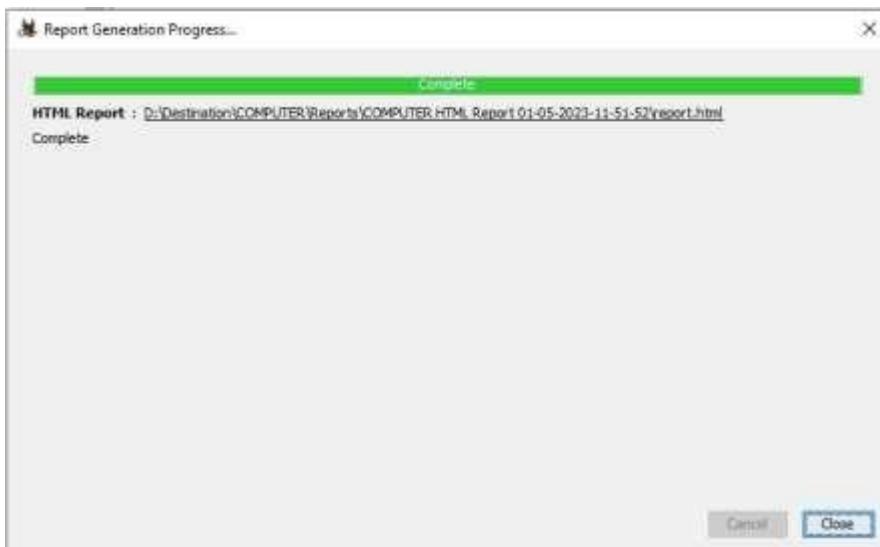
15. Select -> Logical files-> select sample file ->add->next ->Finish





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





Go to this path

Report Navigation

Case summary

Encryption Suspected (0)

Keyword Hits (1300)

Metadata (14)

Tagged Files (0)

Tagged Images (0)

Tagged Results (0)

Web Downloads (5)

Autopsy Forensic Report

Warning, this report was run before ingest services completed!

TYCS

Case: COMPUTER
Case Number: 101
Number of data sources in case: 1
Notes: USB Case Study on Cyber Forensic
Examiner: Computer

Image Information:

USB Drive Copy 001

Timezone: Asia/Calcutta

Path: D:\Destination\1\USB Drive Copy 001

Activate Windows
Go to Settings to activate Windows.

Practical no : 4

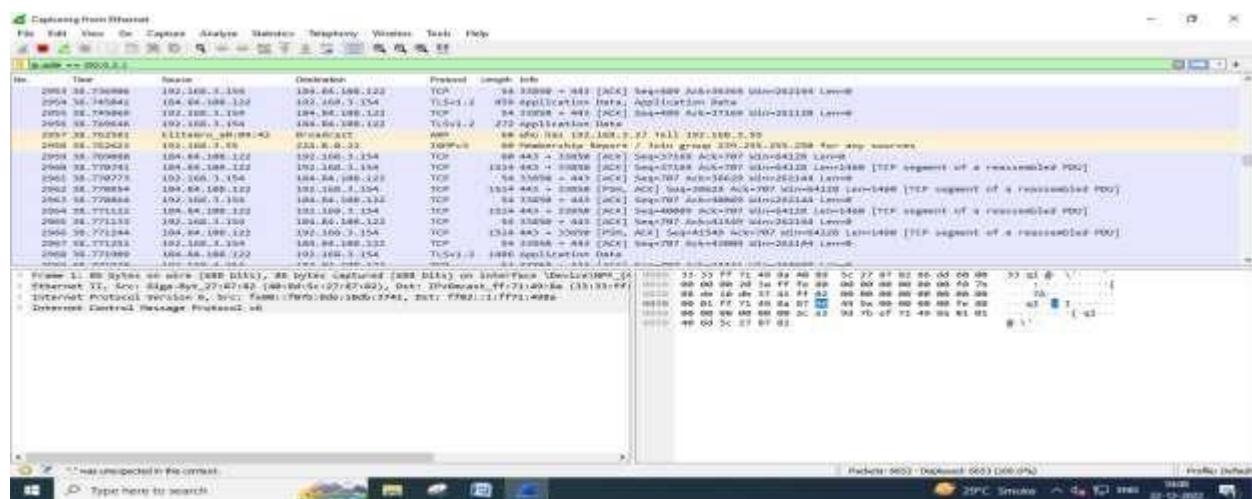
Aim : Capturing and Analyzing network packets using Wireshark (Fundamentals).

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

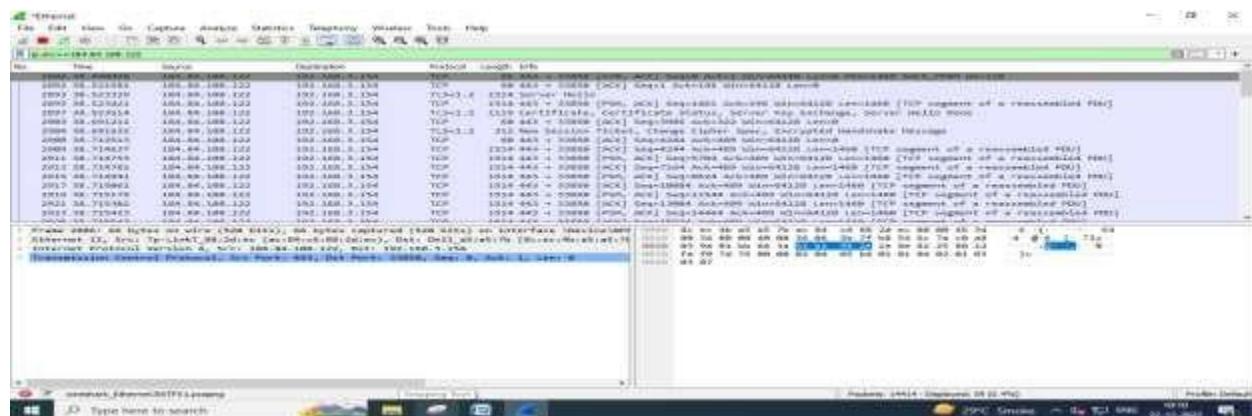
Steps :

Open the Wireshark and click on Ethernet.

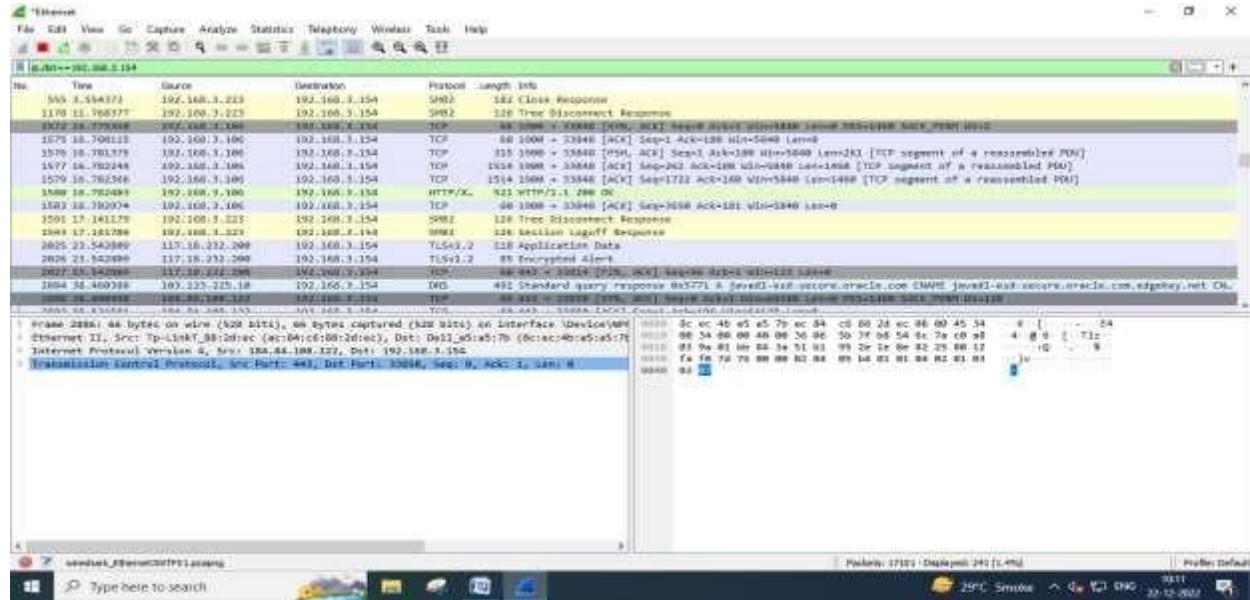
1. Display packets based on specific IP-address.
 - **ip.addr==192.0.2.1**



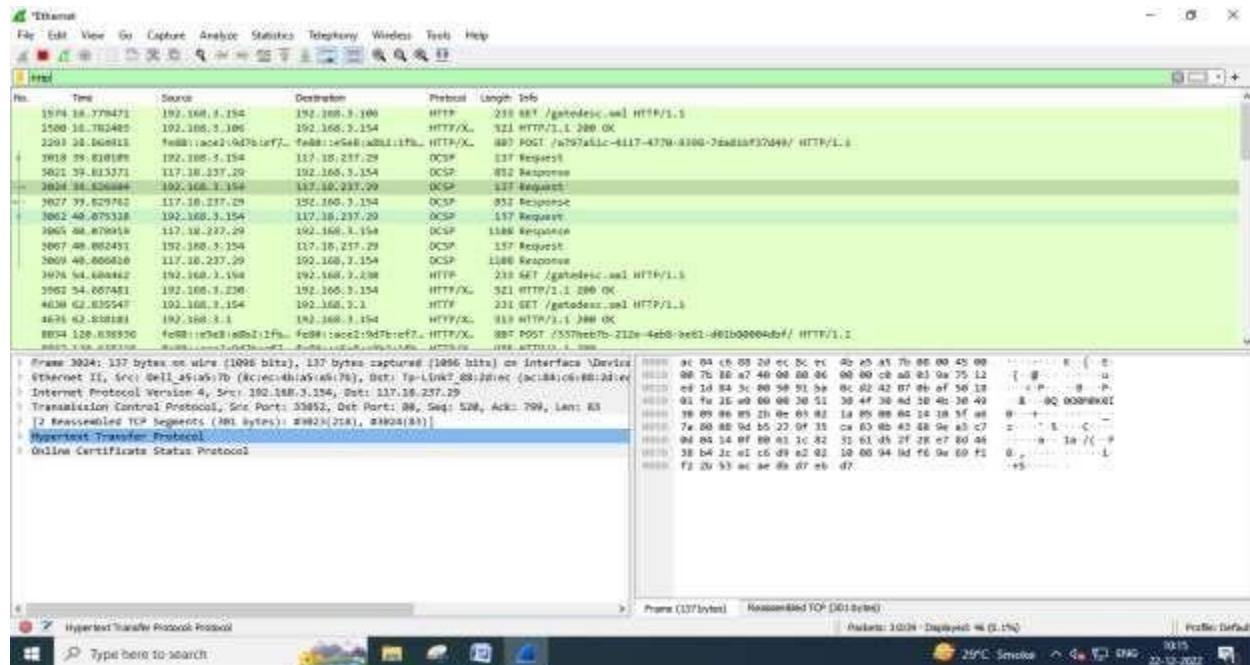
2. Display packets which are coming from specific IP-address.
 - **ip.scr==184.84.108.122**



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

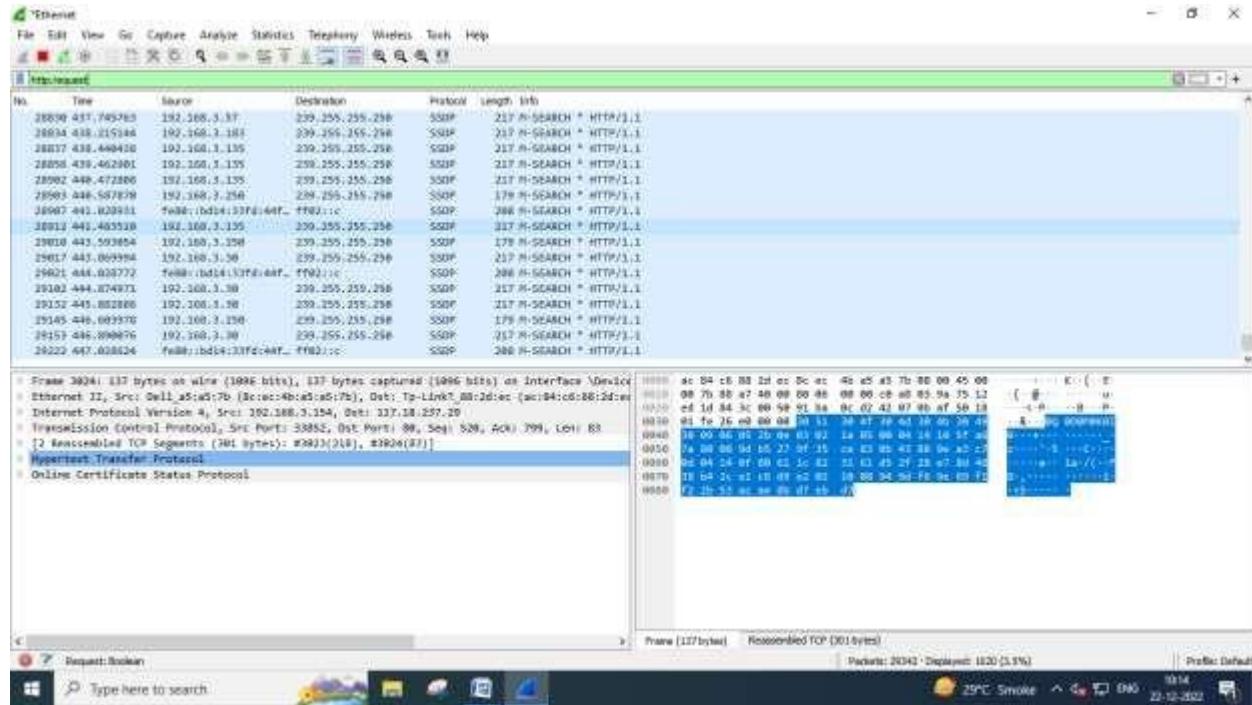


4. Display packets which are using http protocol.
- http



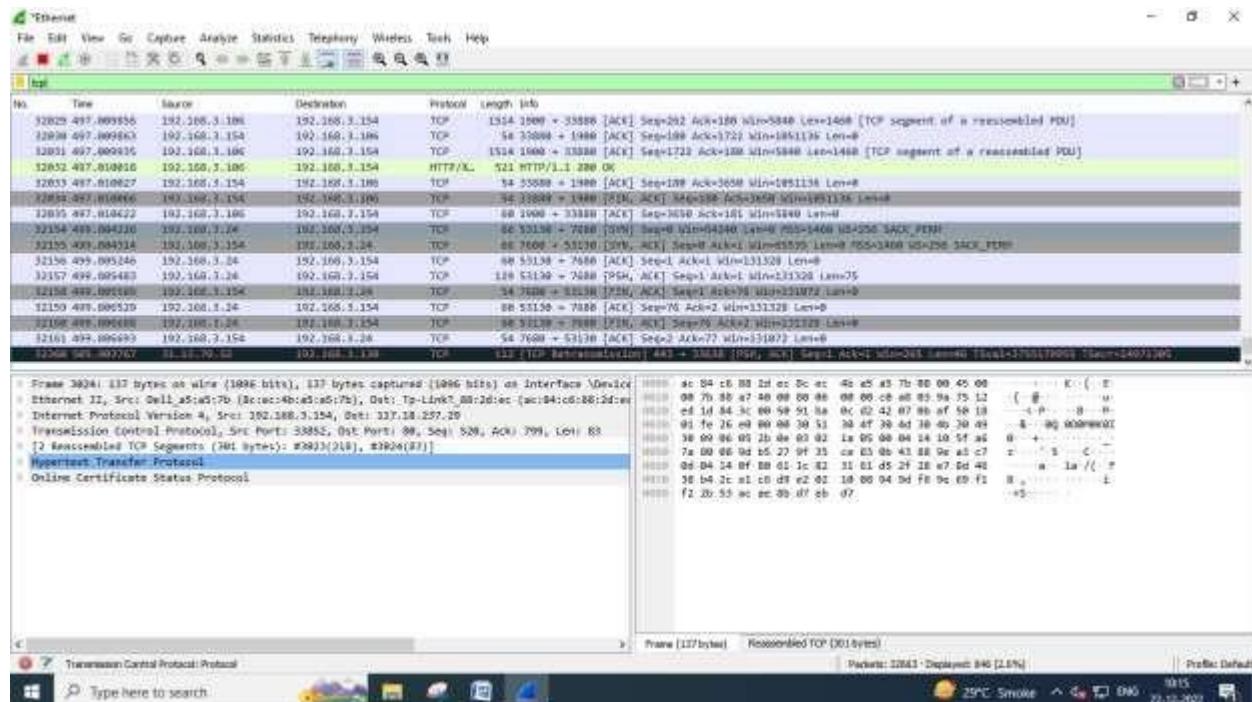
5. Display packets which are using http.request

- http.request

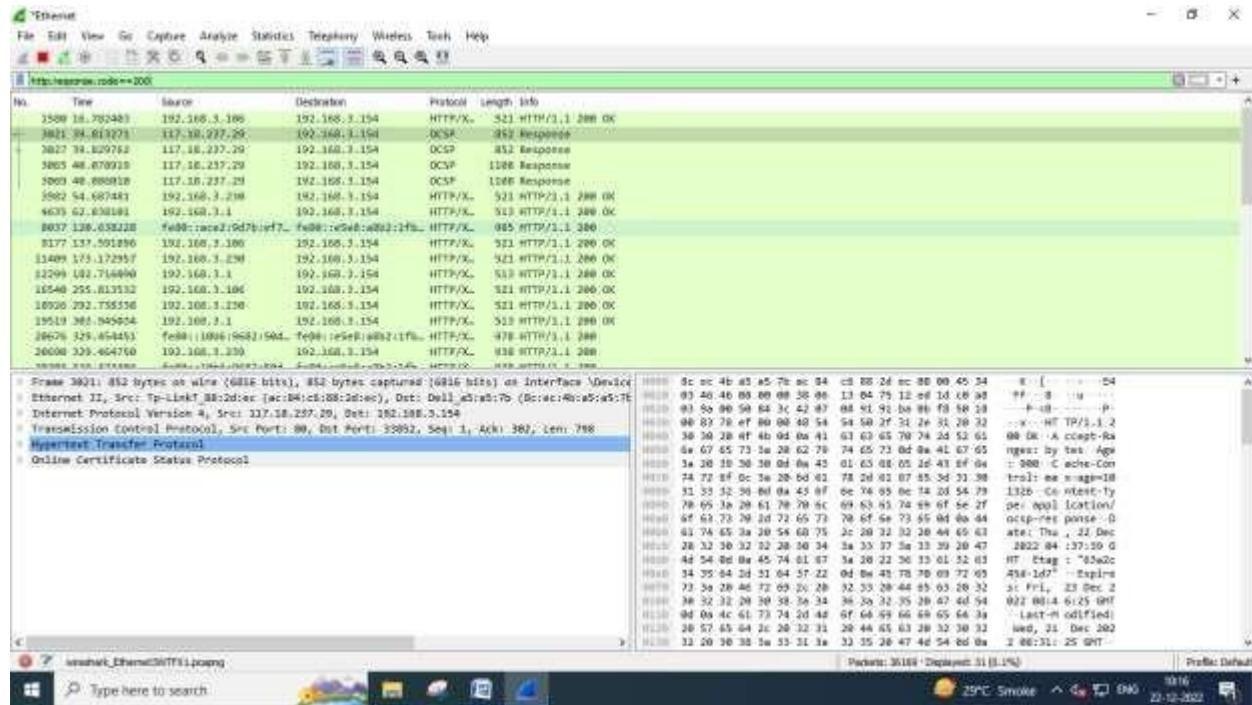


6. Display packets which are using TCP protocol.

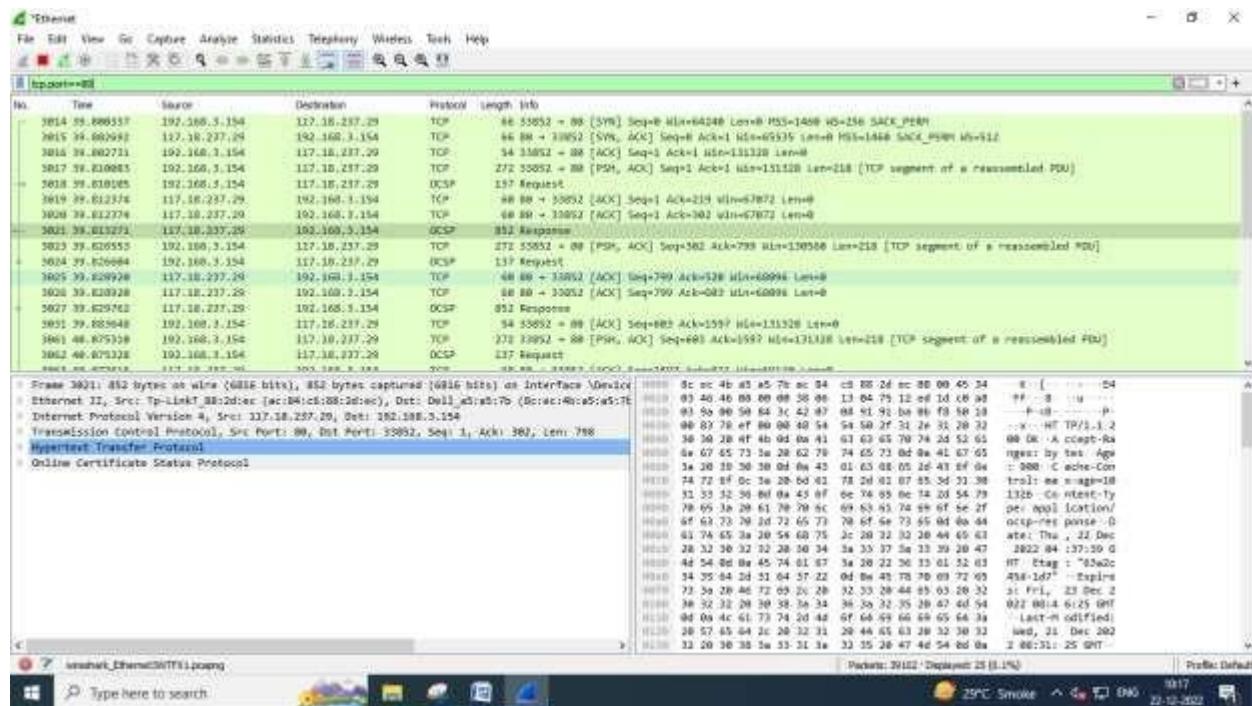
- tcp



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



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



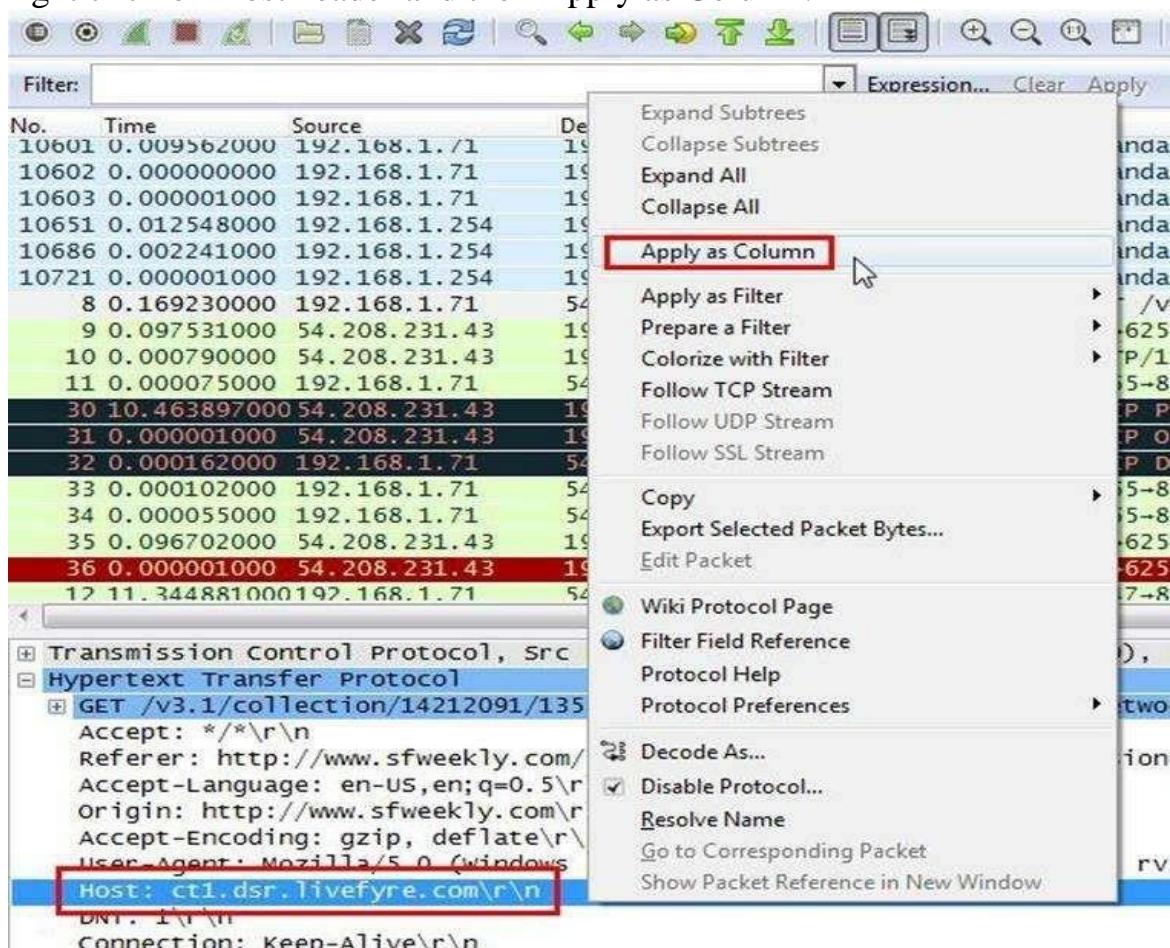
PRACTICAL 5

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

Time	Source	Destination	Protocol	Length	Host
11 0.055571000	192.168.1.254	192.168.1.71	DNS	222	
12 0.073696000	64.49.225.166	192.168.1.71	TCP	60	
13 0.000150000	192.168.1.71	64.49.225.166	TCP	54	
14 0.000056000	192.168.1.71	64.49.225.166	TCP	54	
15 0.036217000	fe80::856e:7b6d:6 ff02::1:3		LLMNR	88	
16 0.001465000	192.168.1.68	224.0.0.252	LLMNR	68	
17 0.041273000	64.49.225.166	192.168.1.71	TCP	60	
18 0.057682000	192.168.1.68	224.0.0.252	LLMNR	68	
19 0.244659000	192.168.1.71	66.165.133.65	HTTP	440	www.snopes.com
20 0.018898000	192.168.1.71	207.109.230.161	HTTP	1037	as.casalemedia.com
21 0.025753000	207.109.230.161	192.168.1.71	TCP	60	
22 0.053733000	66.165.133.65	192.168.1.71	HTTP	1514	
23 0.000839000	66.165.133.65	192.168.1.71	TCP	1514	
24 0.000057000	192.168.1.71	66.165.133.65	TCP	54	
25 0.000751000	66.165.133.65	192.168.1.71	TCP	1514	
26 0.000775000	66.165.133.65	192.168.1.71	TCP	1514	
27 0.000002000	66.165.133.65	192.168.1.71	TCP	1514	

80-41920 [ACK] Seq=2 Ack=2 Win=31 Len=0
Standard query 0xae89 A HP093DFD

www.snopes.com GE op.jpg HTTP
as.casalemedia.com GE snopes.com
8C vin=16566 L
HT page)
8C 37 Win=1752
41 37 Win=256
8C 37 Win=1752
8C 37 Win=1752
8C 37 Win=1752
8C 37 Win=1752

on interface 0
11:e2:b9 (ac:5d:10:11:e2:
165.133.65 (66.165.133.65
0), Seq: 1, Ack: 1, Len:

01 Firefox/29.0\r\nn

Follow TCP Stream

- Follow UDP Stream
- Follow SSL Stream
- Copy
- Protocol Preferences
- Decode As...
- Print...
- Show Packet in New Window

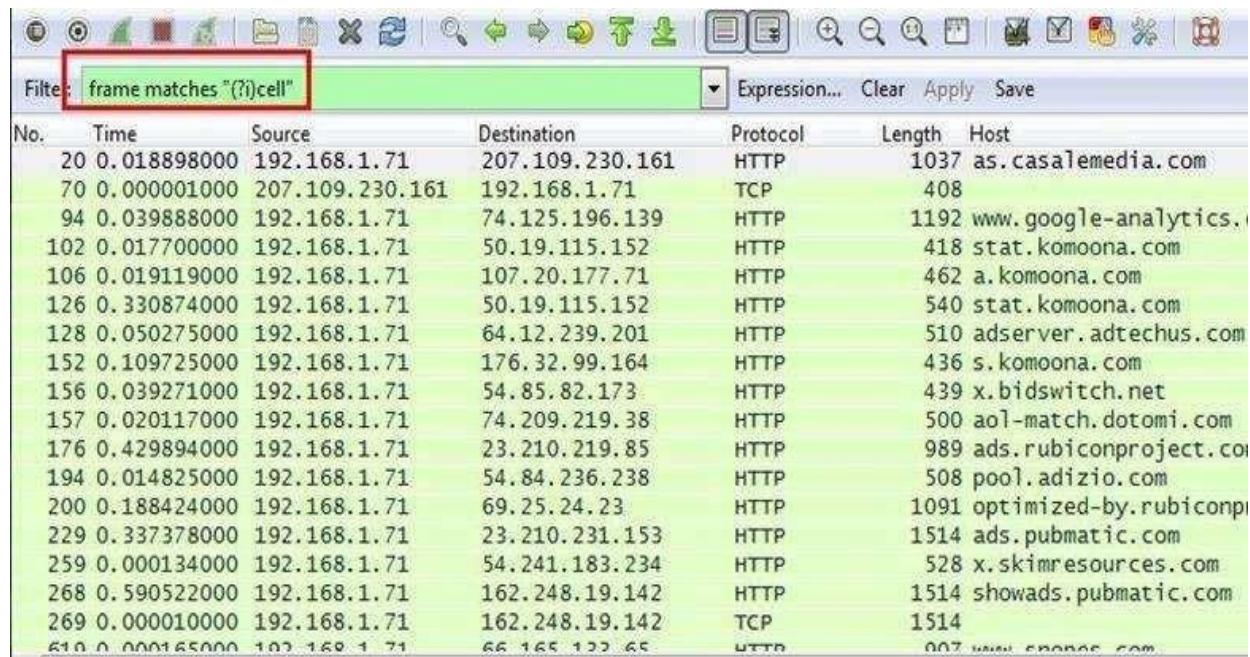
```

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/20100101 Firefox/29.0
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=OJMBNHECFANCNIJJGBBMBLDO
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||



The screenshot shows the NetworkMiner interface with a search bar at the top containing the expression: "frame matches \"(?!cell)". Below the search bar is a table of network traffic. The columns are: No., Time, Source, Destination, Protocol, Length, and Host. The table lists numerous entries, mostly HTTP requests from various IP addresses to different hosts like as.casalemedia.com, www.google-analytics.com, stat.komoona.com, etc.

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.com
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.com
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.rubicon
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	
510	0.000165000	192.168.1.71	66.165.122.65	HTTP	807	www.echange.com

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.

Filter: frame matches "(?)cell"						
Time	Source	Destination	Protocol	Length	Info	
20 0.018898000	192.168.1.71	207.109.230.161	HTTP	1037	GET /?s=81847&u=http%3A//www.snopes.com/horrors/techno/cellcharge.asp&f=1&id=4240355892,946	
70 0.000001000	207.109.230.161	192.168.1.71	TCP	408	80-41932 [PSH, ACK] Seq=2110 Ack=984 Win=16366 Len=254	
94 0.039888000	192.168.1.71	74.125.196.139	HTTP	1192	GET /__utm.gif?utmwv=5.5.1&utms=1&utmn=624349962&utmhn=www.snopes.com&utmcs=windows-1252&utm	
102 0.017700000	192.168.1.71	50.19.115.152	HTTP	418	GET /s?tagid=cad674dbf73589c9a110884ce3bb72_728_90&v=2.16&cb=516430883&ts=2 HTTP/1.1	
106 0.019119000	192.168.1.71	107.20.177.71	HTTP	462	GET /tag/cad674dbf73589c9a110884ce3bb72_728_90.js?1=http%3A%2F%2Fwww.snopes.com%2Fhorrors%	
126 0.330874000	192.168.1.71	50.19.115.152	HTTP	540	GET /s?tagid=cad674dbf73589c9a110884ce3bb72_v=2.16&cb=516430883&ts=-1&p=cad674dbf73589c9a	
128 0.050275000	192.168.1.71	64.12.239.201	HTTP	510	GET /addyn/3.0/9423.1/3142865/0/225/ADTECH; loc=100;target=_blank;misc=\$8TIMESTAMP\$0;rdclic	
152 0.109725000	192.168.1.71	176.32.99.164	HTTP	436	GET /passback/np/cad674dbf73589c9a110884ce3bb72.js HTTP/1.1	
156 0.039271000	192.168.1.71	54.85.82.173	HTTP	439	GET /sync?ssp=a01 HTTP/1.1	
157 0.020117000	192.168.1.71	74.209.219.38	HTTP	500	GET /a01/match?cb=https://ums.adtechus.com/mapuser?providerId=1013;userId=\$UID HTTP/1.1	
176 0.429894000	192.168.1.71	23.210.219.85	HTTP	989	GET /ad/9192.js HTTP/1.1	
194 0.014825000	192.168.1.71	54.84.236.238	HTTP	508	GET /sync?ssp=bildswitch_bildswitch_ssp_id=a01 HTTP/1.1	
200 0.188424000	192.168.1.71	69.25.24.23	HTTP	1091	GET /a/9192/19861/64229-2.js?&cb=0.18771559557158202&k_st=1&p_s=c&p_exp=1&p_pos=atf&p_scre	
229 0.337378000	192.168.1.71	23.210.231.153	HTTP	1511	GET /AdServer/js/showad.js?rm=516430883 HTTP/1.1	
259 0.000134000	192.168.1.71	54.241.183.234	HTTP	528	GET /provider+ad12f0&mode=check&uid=1039da81-f78e-44cc-a317-d4139ca80c0c HTTP/1.1	
268 0.590522000	192.168.1.71	162.248.19.142	HTTP	1511	GET /AdServerService/pubId=32702&siteId=46838&adId=80732&adWidth=728&adHeight=90&	
269 0.000010000	192.168.1.71	162.248.19.142	TCP	1514	41950-80 [ACK] Seq=1461 Ack=1 win=16445440 Len=1460	
610 0.000165000	107.149.1.71	66.168.122.66	HTTP	402	RST [Frame number=117chewan seq utm/1.1	

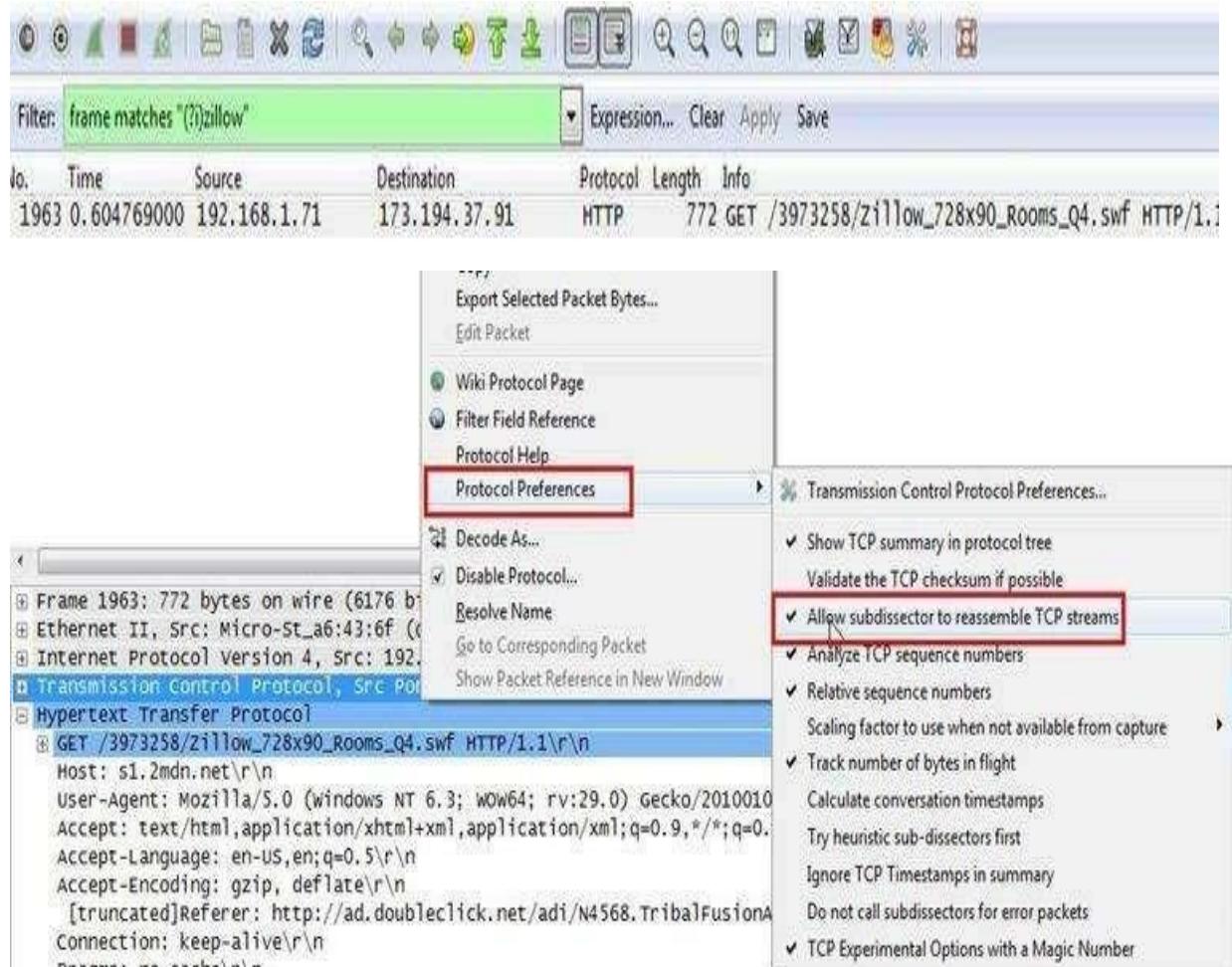
1. According to Zillow, what instrument will Ryan learn to play?

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

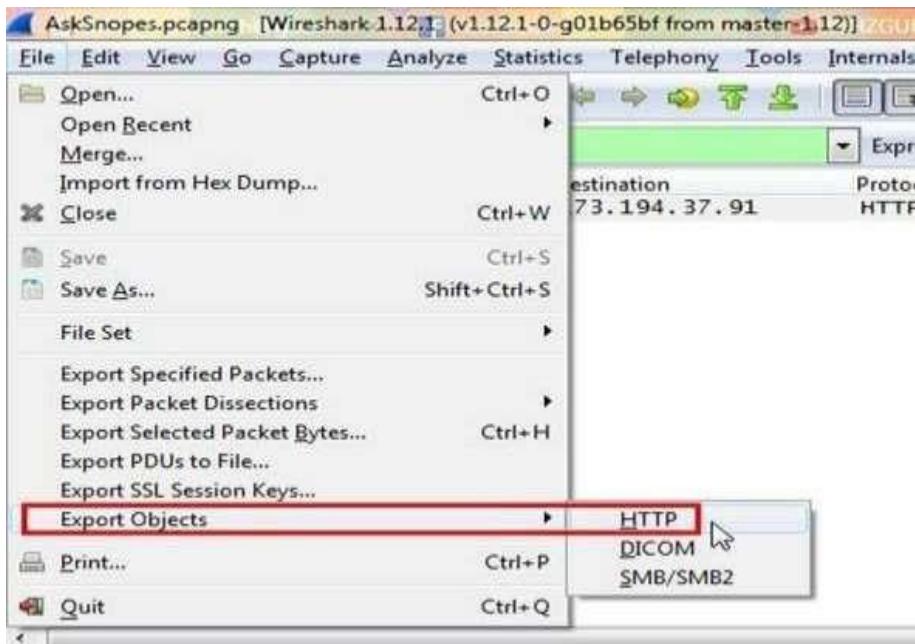
Filter: frame matches "(?)zillow"						
Time	Source	Destination	Protocol	Length	Info	
94 0.039888000	192.168.1.71	74.125.196.139	HTTP	1192	GET /__utm.gif	
95 0.004442000	199.189.107.4	192.168.1.71	TCP	60	80-41929 [ACK]	
96 0.000769000	199.189.107.4	192.168.1.71	TCP	60	[TCP Dup ACK 9]	
97 0.060923000	199.189.107.4	192.168.1.71	TCP	60	80-41930 [FIN,	
98 0.000136000	192.168.1.71	199.189.107.4	TCP	54	41930-80 [ACK]	
99 0.000052000	192.168.1.71	199.189.107.4	TCP	54	41930-80 [FIN,	
100 0.015401000	74.125.196.139	192.168.1.71	TCP	60	80-41931 [ACK]	
101 0.000796000	74.125.196.139	192.168.1.71	HTTP	458	HTTP/1.1 200 OK	
102 0.017700000	192.168.1.71	50.19.115.152	HTTP	418	GET /s?tagid=c	
103 0.011551000	192.168.1.71	74.125.196.139	TCP	54	41931-80 [ACK]	
104 0.029132000	199.189.107.4	192.168.1.71	TCP	60	80-41930 [ACK]	
105 0.000000000	199.189.107.4	192.168.1.71	TCP	60	[TCP Dup ACK 10]	
106 0.019119000	192.168.1.71	107.20.177.71	HTTP	462	GET /tag/cad674	
107 0.034965000	50.19.115.152	192.168.1.71	TCP	60	80-41934 [ACK]	
108 0.001555000	50.19.115.152	192.168.1.71	HTTP	338	HTTP/1.1 200 OK	
109 0.023341000	192.168.1.71	199.189.107.4	TCP	54	[TCP Retransmis	
110 0.016019000	192.168.1.71	50.19.115.152	TCP	54	41934-80 [ACK]	
111 0.019773000	107.20.177.71	102.168.1.71	TCP	60	80-41935 [ACK]	

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 reassemble TCP stream



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

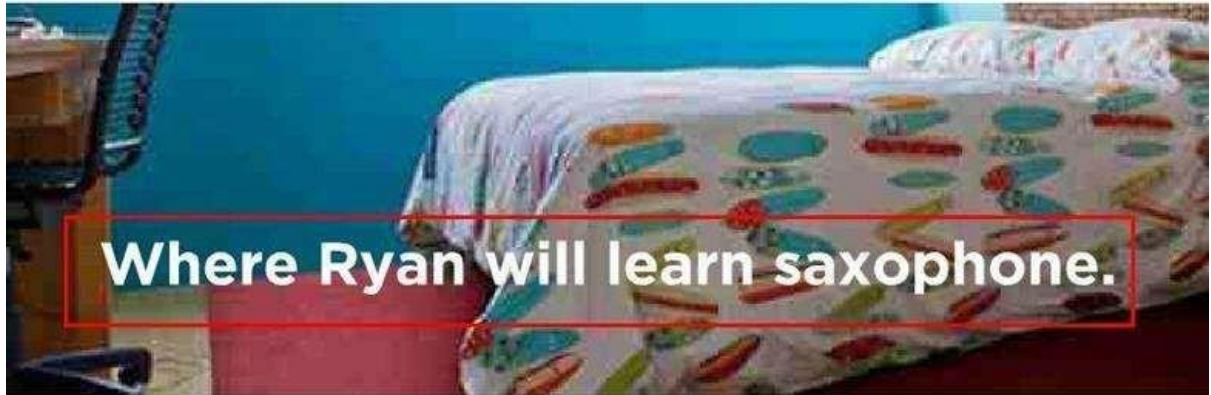
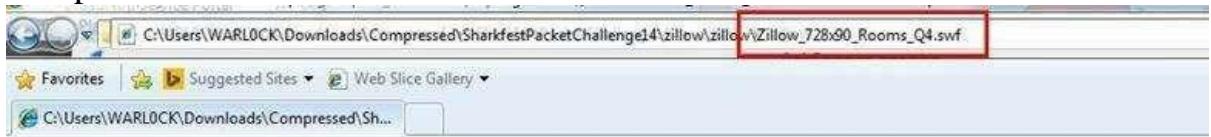


Click on save all.

Packet num	Hostname	Content Type	Size	Filename
52	www.snopes.com	image/jpeg	32 kB	site-bg-top.jpg
54		text/plain	15 bytes	
70	as.casalemedia.com	text/javascript	6735 bytes	cellcharge.asp?f=1&id=4240355892.9460454
101	www.google-analytics.com	image/gif	35 bytes	_utm.gif?utmwv=5.5.1&utms=1&utmn=624
108	stat.komoona.com	application/x-javascript	4 bytes	s?tagid=cad674db7f73589c9a110884ce73bb7:
112	a.komoona.com	application/x-javascript	815 bytes	cad674db7f73589c9a110884ce73bb72_728_90
129	stat.komoona.com	application/x-javascript	4 bytes	s?tagid=cad674db7f73589c9a110884ce73bb7:
133	adserver.adtechus.com	application/x-javascript	431 bytes	ADTECH;loc=100;target=_blank;misc=%5BTI
154	s.komoona.com	application/x-javascript	5603 bytes	cad674db7f73589c9a110884ce73bb72.js
182	ads.rubiconproject.com	text/javascript	18 kB	9192.js
205	optimized-by.rubiconproject.com	text/javascript	1852 bytes	64229-2.js?&cb=0.18771559557158202&tk_st:
212	ocsp.thawte.com	application/ocsp-request	115 bytes	\
215	ocsp.thawte.com	application/ocsp-response	1421 bytes	\
223	ocsp.thawte.com	application/ocsp-request	115 bytes	\
225	ocsp.thawte.com	application/ocsp-response	1421 bytes	\
251	ads.pubmatic.com	text/html	54 kB	showad.js?rn=516430883
261	x.skimresources.com	application/json	79 bytes	?provider=adizio&mode=check&uid=1039d:
330	pr.ybp.yahoo.com	image/gif	43 bytes	E6EF997B-80FE-4373-AB1F-500144B03A7B
334	rt.legolas-media.com	image/gif	6 bytes	lgrt?ci=12&ti=64523&pbi=11057
346	um.eqads.com	text/html	196 bytes	pub.aspx?
353	ads.pubmatic.com	text/html	454 bytes	ro_x914.html

At the bottom of the table, there are three buttons: "Help", "Save As", and "Save All". The "Save All" button is highlighted with a red box.

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



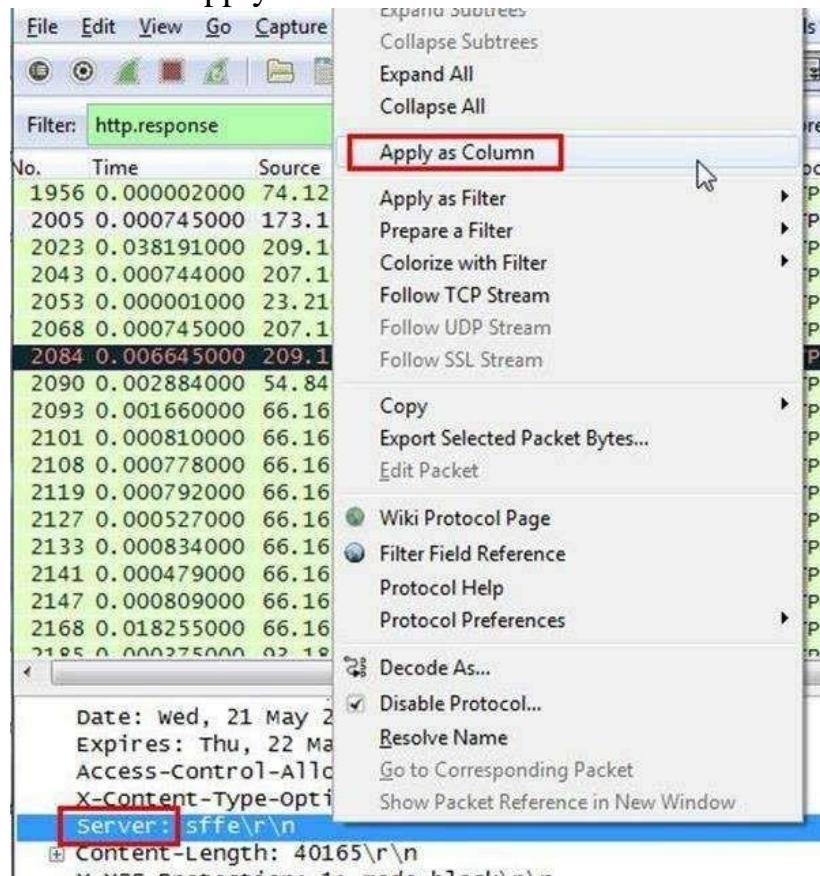
1. How many web servers are running Apache?

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.

Filter: http.response

No.	Time	Source	Destination	Protocol	Length	Info
1956	0.000002000	74.125.21.154	192.168.1.71	HTTP	432	HTTP/1.1 200 OK (text/javascript)
2005	0.000745000	173.194.37.91	192.168.1.71	HTTP	580	HTTP/1.1 200 OK (application/javascript)
2023	0.038191000	209.107.194.81	192.168.1.71	HTTP	1478	HTTP/1.1 200 OK (application/javascript)
2043	0.000744000	207.109.230.154	192.168.1.71	HTTP	1054	HTTP/1.1 200 OK (text/html)
2053	0.000001000	23.210.231.153	192.168.1.71	HTTP	178	HTTP/1.1 200 OK
2068	0.000745000	207.109.230.154	192.168.1.71	HTTP	1054	HTTP/1.1 200 OK (text/html)
2084	0.006645000	209.107.194.81	192.168.1.71	HTTP	1478	[TCP Retransmission] HTTP/1.1 200 OK (text/html)
2090	0.002884000	54.84.148.104	192.168.1.71	HTTP	626	HTTP/1.1 200 OK (GIF89a)
2093	0.001660000	66.165.133.65	192.168.1.71	HTTP	1201	HTTP/1.1 200 OK (GIF89a)
2101	0.000810000	66.165.133.65	192.168.1.71	HTTP	673	HTTP/1.1 200 OK (GIF89a)
2108	0.000778000	66.165.133.65	192.168.1.71	HTTP	324	HTTP/1.1 200 OK (GIF89a)
2119	0.000792000	66.165.133.65	192.168.1.71	HTTP	176	HTTP/1.1 200 OK (GIF89a)
2127	0.000527000	66.165.133.65	192.168.1.71	HTTP	591	HTTP/1.1 200 OK (GIF89a)
2133	0.000834000	66.165.133.65	192.168.1.71	HTTP	482	HTTP/1.1 200 OK (GIF89a)
2141	0.000479000	66.165.133.65	192.168.1.71	HTTP	592	HTTP/1.1 200 OK (GIF89a)
2147	0.000809000	66.165.133.65	192.168.1.71	HTTP	1414	HTTP/1.1 200 OK (GIF89a)

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



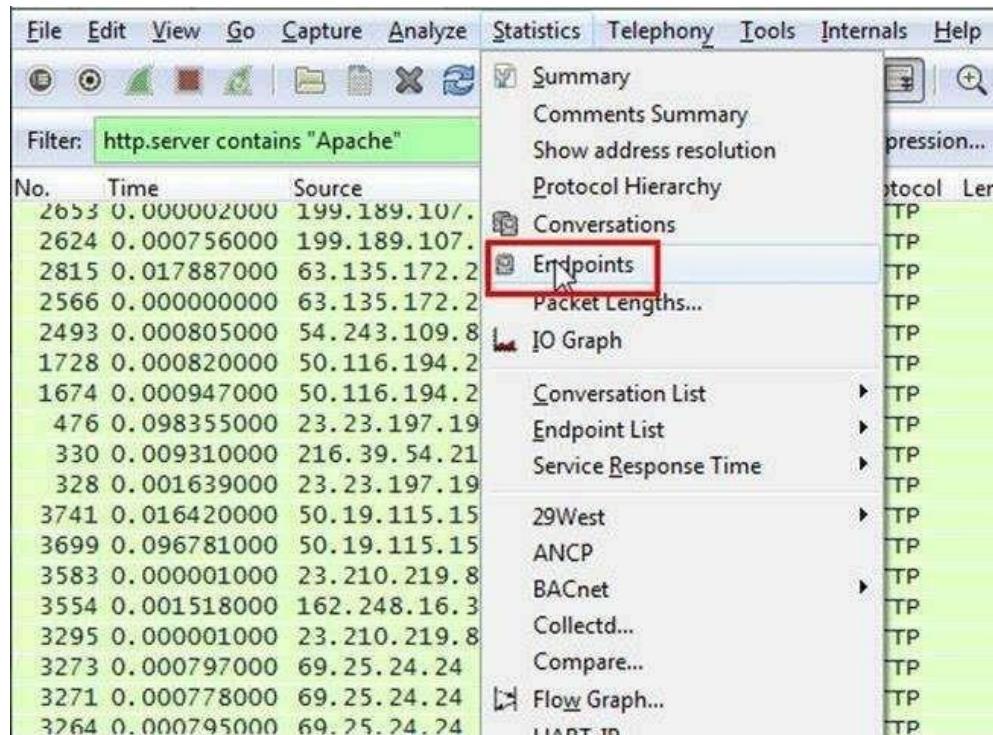
Now can see the server column where all server name is showing.

Destination	Protocol	Length	Server	Info
192.168.1.71	HTTP	828	sffe	HTTP/1.1 200 OK (JPEG/JFIF image)
192.168.1.71	HTTP	580	sffe	HTTP/1.1 200 OK (application/x-shockwave-flash)
192.168.1.71	HTTP	807	sffe	HTTP/1.1 200 OK (text/javascript)
192.168.1.71	HTTP	463	sffe	HTTP/1.1 200 OK (text/javascript)
192.168.1.71	HTTP	959	radiumone/1.2	HTTP/1.1 200 OK (GIF89a)
192.168.1.71	HTTP	525	radiumone/1.2	HTTP/1.1 200 OK (text/html)
192.168.1.71	HTTP	875	post/2.0	HTTP/1.1 200 OK (application/x-javascript)
192.168.1.71	OCSP	829	ocsp_responder	response
192.168.1.71	HTTP	1159	nginx/1.5.3	HTTP/1.1 302 Found
192.168.1.71	HTTP	1092	nginx/1.5.3	HTTP/1.1 302 Found
192.168.1.71	HTTP	626	nginx/1.4.7	HTTP/1.1 200 OK (GIF89a)
192.168.1.71	HTTP	685	nginx/1.4.7	HTTP/1.1 302 Moved Temporarily
192.168.1.71	HTTP	626	nginx/1.4.7	HTTP/1.1 200 OK (GIF89a)
192.168.1.71	HTTP	626	nginx/1.4.7	HTTP/1.1 200 OK (GIF89a)
192.168.1.71	HTTP	681	nginx/1.4.7	HTTP/1.1 302 Moved Temporarily
192.168.1.71	HTTP	323	nginx/1.4.3	TCP Out-Of-Order] HTTP/1.1 302 Found
192.168.1.71	HTTP	303	nginx/1.4.3	HTTP/1.1 302 Found
192.168.1.71	HTTP	225	nginx/1.2.0	HTTP/1.1 200 OK (application/x-javascript)

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||

Filter: http.server contains "Apache"							Expression...	Clear	Apply	Save
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	FDD	IPv4: 22	IPv6	IPX	JXTA	NCP	RSVP	SCTP	TCP: 77	Token
IPv4 Endpoints - Filter: http.send											
Address	↓ Packets	↓ Bytes	↓ Tx Packets	↓ Tx Bytes	↓ Rx Packets	↓ Rx Bytes	↓ Latitude	↓ Longitude	↓ Country	↓ City	↓ Organization
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	FDD	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	↓ Longitude	↓ Country	↓ City	↓ Organization
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 Name	is	chrome.exe	Include
Process Name	is	Procmon.exe	Exclude
Process Name	is	Procexp.exe	Exclude
Process Name	is	Autoruns.exe	Exclude
Process Name	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	\$Mft Mir	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

11:09... chrome.exe 5236 CreateFile C:\Users\COM-3\AppData\Local\Goog... SUCCESS Desired Access: Read Data/List Directory, Synchronize. Disposition: Open, Options: Directory, Synchronous IO Non-Halt, Attr... Riter, 1.

11:09... chrome.exe 5236 QueryDirectory C:\Users\COM-3\AppData\Local\Goog... SUCCESS D:\, 1:000119db, 2:000140db, 3:000195db, 4:000199log, 5:2fa877fe72a4b3293124114db06a50mp, 6:4ea16cb...

11:09... chrome.exe 5236 QueryDirectory C:\Users\COM-3\AppData\Local\Goog... NO MORE FILES Riter, History, 1: History.

11:09... chrome.exe 5236 CloseFile C:\Users\COM-3\AppData\Local\Goog... SUCCESS Desired Access: Read Data/List Directory, Synchronize. Disposition: Open, Options: Directory, Synchronous IO Non-Halt, Attr... Riter, History, 1: History.

11:09... chrome.exe 5236 CreateFile C:\Users\COM-3\AppData\Local\Goog... SUCCESS

Showing 1303 of 179857 events (0.72%) Backed by virtual memory

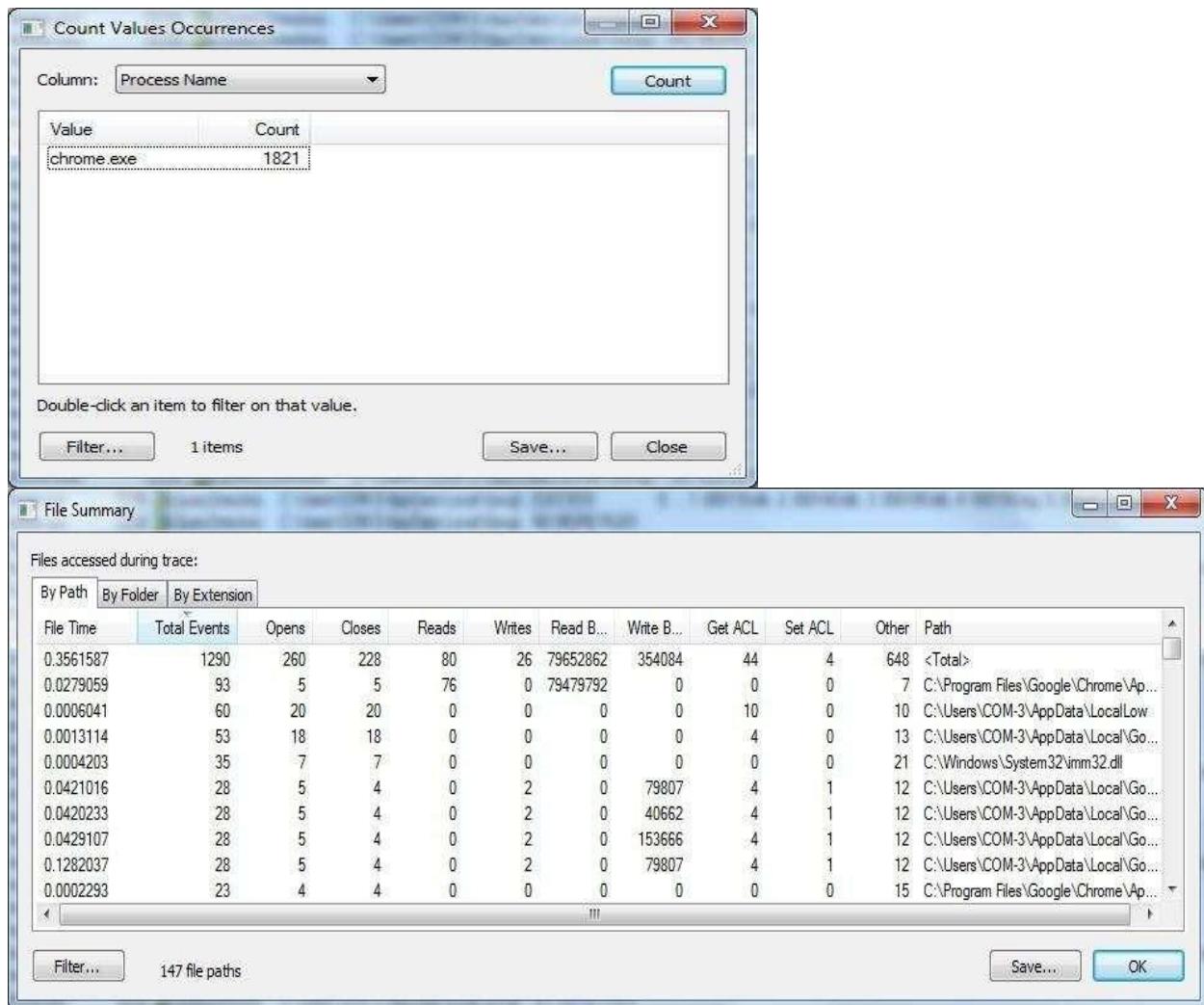
Process Tree

Only show processes still running at end of current trace Timelines cover displayed events only

Process	Description	Image Path	Life Time	Company	Own
Idle (0)					
System (4)					
chrome.exe (428)	Windows Session	C:\Windows\Syst...		Microsoft Corporat...	NT /
carica.exe (600)	Client Server Run...	C:\Windows\Syst...		Microsoft Corporat...	NT /
conhost.exe (3996)	Console Window	C:\Windows\Syst...		Microsoft Corporat...	NT /
conhost.exe (6000)	Console Window	C:\Windows\Syst...		Microsoft Corporat...	NT /
wininit.exe (650)	Windows Start-Up	C:\Windows\Syst...		Microsoft Corporat...	NT /
services.exe (118)	Services and Cont...	C:\Windows\Syst...		Microsoft Corporat...	NT /
wsvchost.exe (892)	Host Process for...	C:\Windows\Syst...		Microsoft Corporat...	NT /
wmiprvse.exe (156)	WMI Provider Host	C:\Windows\Syst...		Microsoft Corporat...	NT /
ARWSRV.C EXE (956)	Realtime Behavior...	C:\Program Files\...		Quick Heal Techn...	NT /
ScSvcSvcs.exe (980)	Browser Sandbox	C:\Program Files\...		Quick Heal Techn...	NT /
wsvchost.exe (1196)	Host Process for...	C:\Windows\Syst...		Microsoft Corporat...	NT /
wsvchost.exe (1272)	Host Process for...	C:\Windows\Syst...		Microsoft Corporat...	NT /
wsvchost.exe (1308)	Host Process for...	C:\Windows\Syst...		Microsoft Corporat...	NT /
Dwm.exe (2036)	Desktop Window	C:\Windows\kwin...		Microsoft Corporat...	CS-1

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

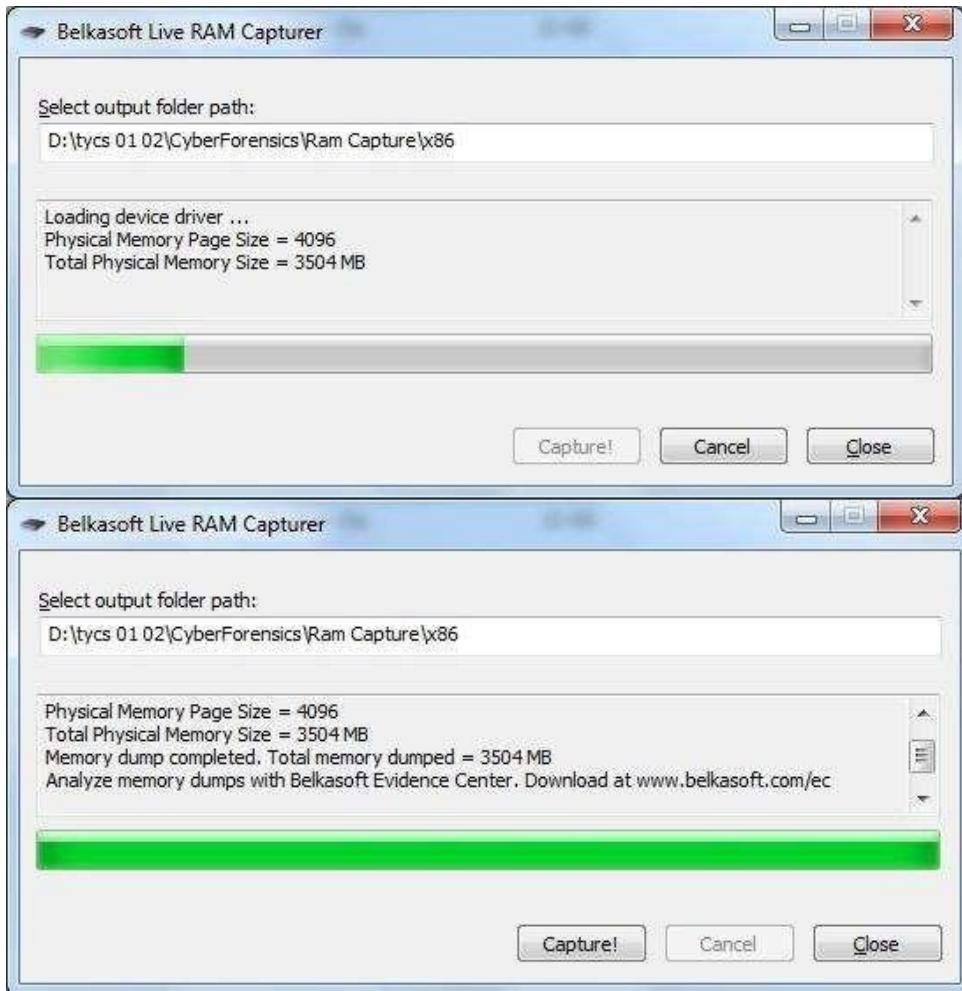


- **Capture RAM (Tool: RAMCapture)**

To Do:

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

Output:



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

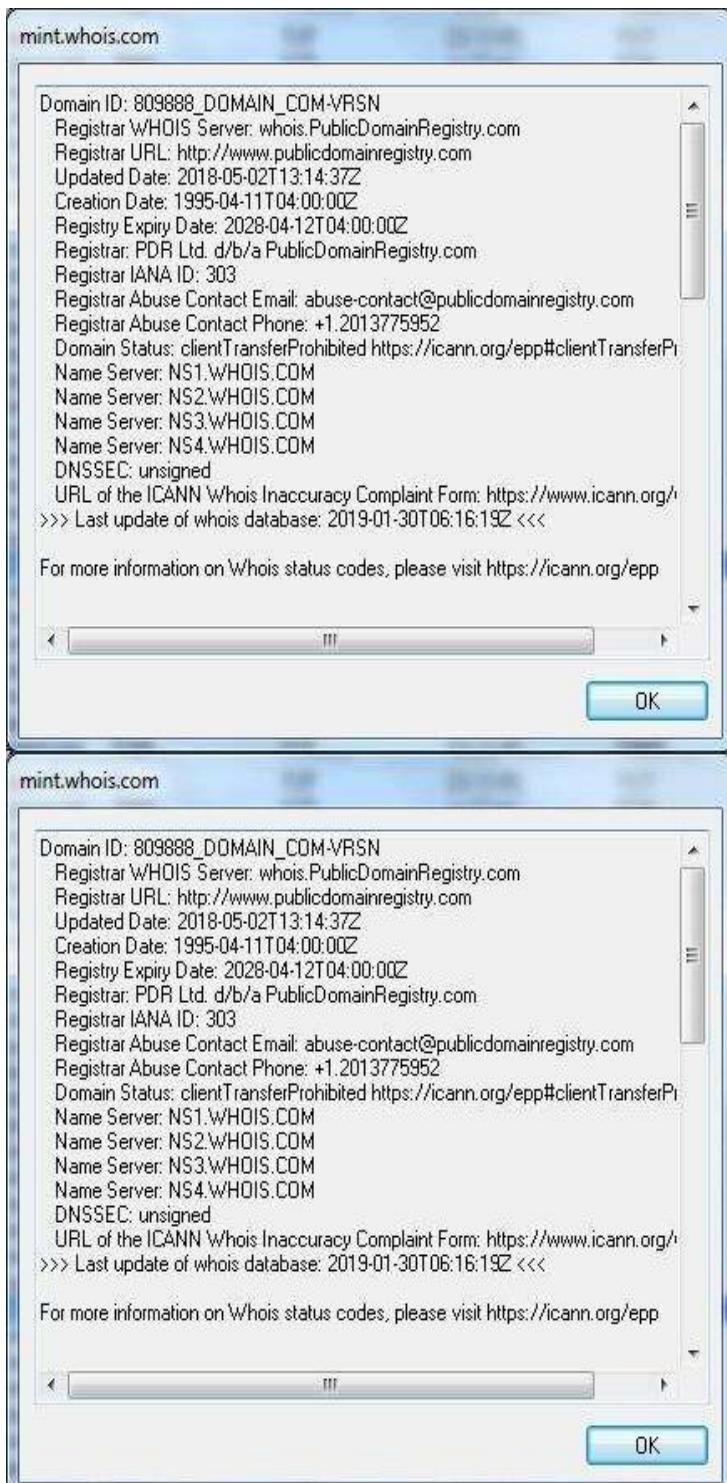
To Do: 1. Save to .txt file.

2. Whois

Output:

Process /	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets	Sent Bytes	Rcvd Packets	Rcvd Bytes
[System Proc... 0	0	TCP	CS-11-PC	1521	localhost	9600	TIME_WAIT				
[System Proc... 0	0	TCP	CS-11-PC	9589	localhost	1521	TIME_WAIT				
[System Proc... 0	0	TCP	CS-11-PC	9600	localhost	1521	TIME_WAIT				
[System Proc... 0	0	TCP	CS-11-PC	1521	localhost	9600	TIME_WAIT	4	792	4	
accsvc.exe	2844	TCP	CS-11-PC	62125	CS-11-PC	0	LISTENING				
accsvc.exe	2844	TCP	cs-11-pc	9571	ec213-200-151-2..	8080	ESTABLISHED	1	544	1	
chrome.exe	5236	TCP	cs-11-pc	3450	74.125.24.198	5228	ESTABLISHED				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	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	UDP	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	14.142.64.27.stats..	8080	ESTABLISHED				
EMLPROXY...	2924	TCP	CS-11-PC	17400	CS-11-PC	0	LISTENING				
java.exe	5248	TCP	CS-11-PC	1038	localhost	1038	ESTABLISHED	26	26		25
java.exe	5248	TCP	CS-11-PC	1038	localhost	1038	ESTABLISHED				
java.exe	5248	TCP	CS-11-PC	1158	CS-11-PC	0	LISTENING				
java.exe	5248	TCP	CS-11-PC	9520	CS-11-PC	0	LISTENING				
java.exe	5248	TCPV6	cs-11-pc	9520	cs-11-pc	0	LISTENING				
Endpoints: 99	Established: 9	Listening: 44	Time Wait: 4	Close Wait: 2							

Process /	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets	Sent Bytes	Rcvd Packets	Rcvd Bytes
[System Proc... 0	0	TCP	CS-11-PC	1521	localhost	10000	TIME_WAIT				
accsvc.exe	2844	TCP	CS-11-PC	62125	CS-11-PC	0	LISTENING				
accsvc.exe	2844	TCP	cs-11-pc	10072	ec213-200-151-2..	8080	ESTABLISHED	1	544	1	
chrome.exe	5236	TCP	CS-11-PC	10046	172.217.194.198	5228	ESTABLISHED				
chrome.exe	5236	TCP	cs-11-pc	9801	172.217.194.198	5228	ESTABLISHED	1	33	1	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	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	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	TCP	cs-11-pc	10040	104.19.195.151	Https..	ESTABLISHED	7	1.141	16	
chrome.exe	5236	TCP	CS-11-PC	57091	57091			5	1.355	7	
chrome.exe	5236	UDP	CS-11-PC	57092	*	*	*	4	2.767	7	
chrome.exe	5236	UDP	CS-11-PC	58349	*	*	*	3	1.417	4	
chromite.exe	5236	TCP	cs-11-pc	10140	rel..			2	843	5	
chrome.exe	5236	TCP	cs-11-pc	10141	mn..			4	1.579	16	
chrome.exe	5236	UDP	CS-11-PC	57789				4	2.767	7	
emagent.exe	5348	TCP	CS-11-PC	3838	CS-1						
emagent.exe	5348	TCP	CS-11-PC	10000	CS-1						
emagent.exe	5348	TCPV6	cs-11-pc	3938	cs-1						
EMLPROXY...	2924	TCP	CS-11-PC	17400							
java.exe	5248	TCP	CS-11-PC	1038	localhost	1038	ESTABLISHED	85	85		85
java.exe	5248	TCP	CS-11-PC	1038	localhost	1038	ESTABLISHED				
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				
java.exe	5248	TCP	CS-11-PC	1028	CS-11-PC	0	LISTENING				
java.exe	5248	TCPV6	cs-11-pc	1028	cs-11-pc	0	LISTENING				
java.exe	5248	TCP	CS-11-PC	5364	CS-11-PC	0	LISTENING				
JDNSRespo...	2824	UDP	cs-11-pc	5353	*	*	*				235
JDNSRespo...	2824	UDP	cs-11-pc	5353	*	*	*				
JDNSRespo...	2824	UDP	cs-11-pc	5353	*	*	*				
JDNSRespo...	2824	UDP	cs-11-pc	64645	*	*	*	4	208	4	
JDNSRespo...	2824	UDP	cs-11-pc	64645	*	*	*				
Jndrdrv.exe	3708	TCP	CS-11-PC	ms-slap4	CS-11-PC	0	LISTENING				
Jndrdrv.exe	3708	TCPV6	cs-11-pc	ms-slap4	cs-11-pc	0	LISTENING				
osqlcmd.exe	3932	TCP	CS-11-PC	3906	CS-11-PC	0	LISTENING				
osqlcmd.exe	3932	TCP	CS-11-PC	49162	CS-11-PC	0	LISTENING				
osqlcmd.exe	3932	TCP	CS-11-PC	49162	CS-11-PC	0	LISTENING				
Process Properties...											
End Process...											
Close Connection											
Whois...											
Copy											
Ctrl+C											





- **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 :

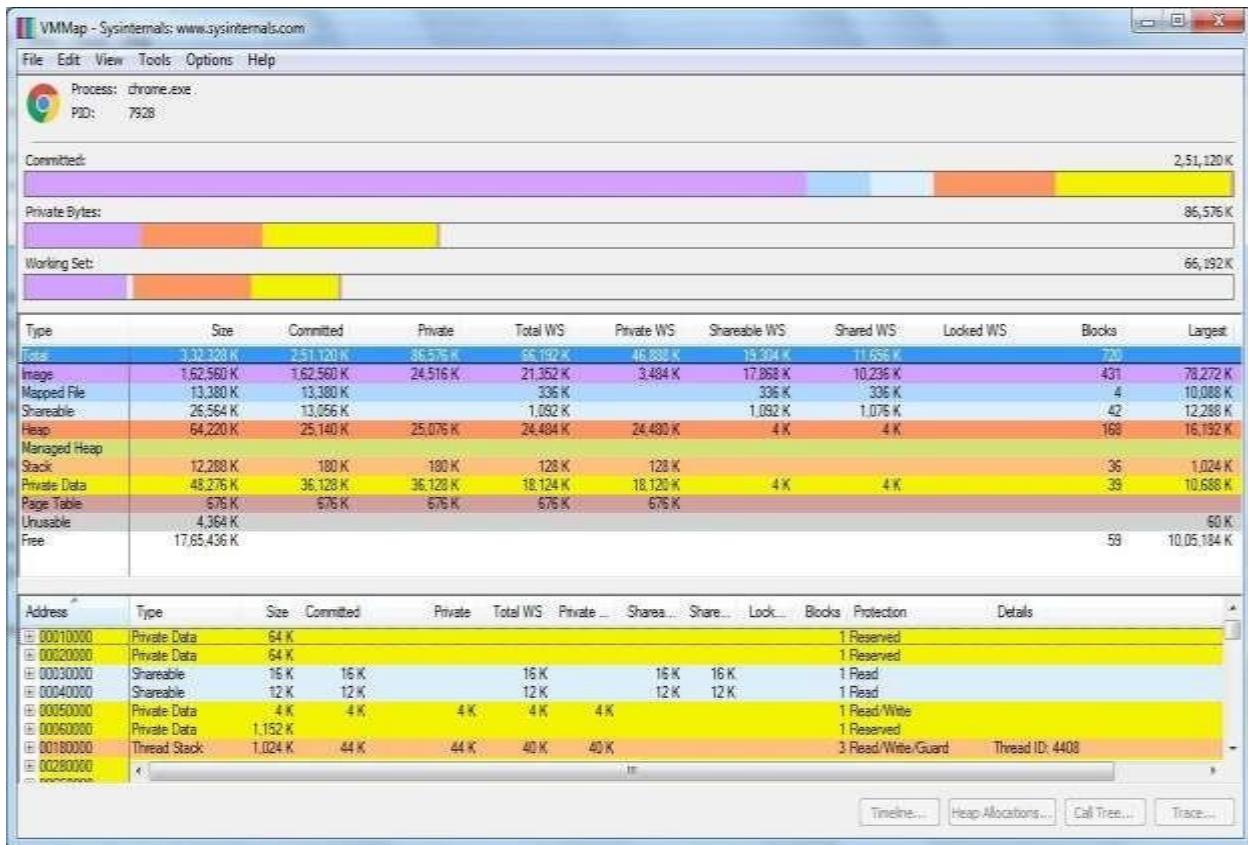
#	Time	Duration (s)	Disk	Request	Sector	Length
423	13.787719	0.00024796	0	Write	63667552	32
424	13.787794	0.00024796	0	Write	55563904	32
425	13.787965	0.00024796	0	Read	63667552	32
426	14.420242	0.00056267	0	Write	155440856	2048
427	14.615099	0.00201225	0	Write	1935616	8
428	14.615135	0.00095367	0	Write	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 :

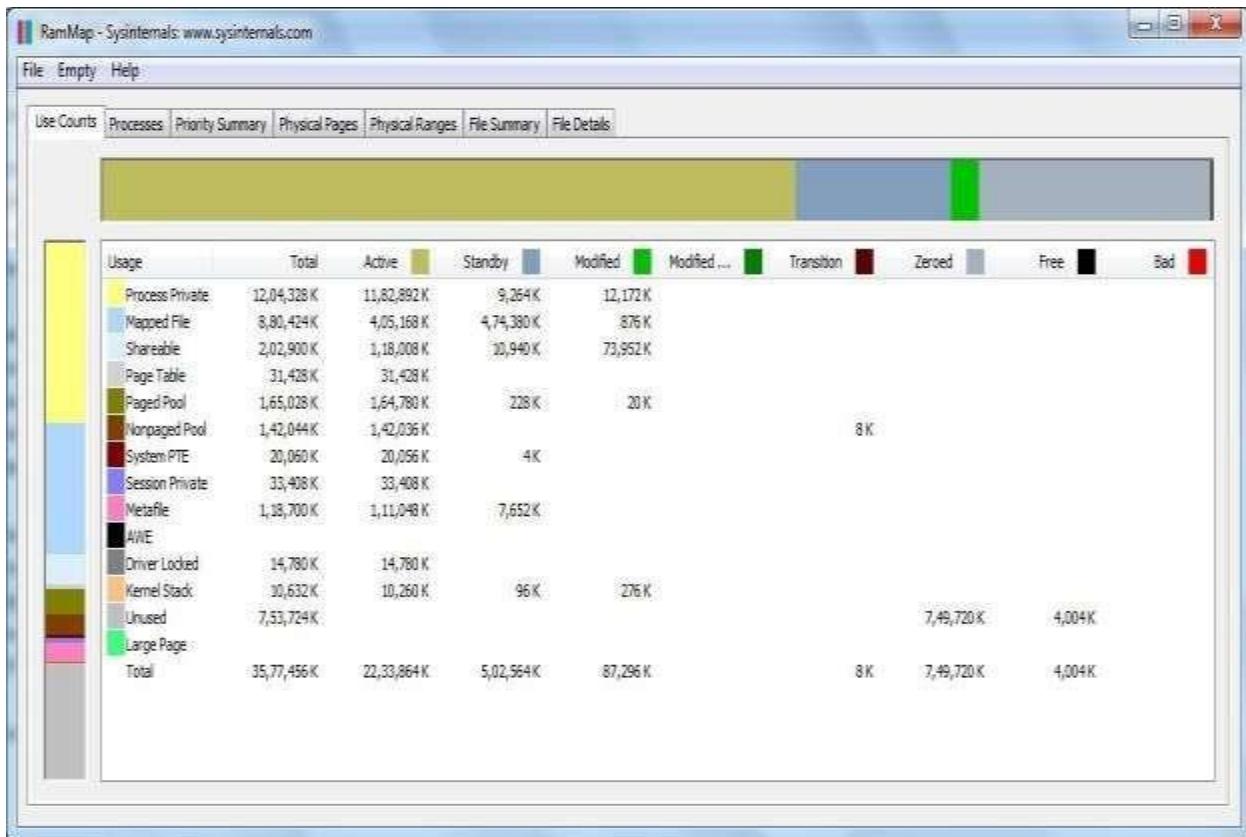


- Monitor Cache Memory (Tool: RAMMap)

TO DO :

1. Save to .RMP file.

Output:



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.



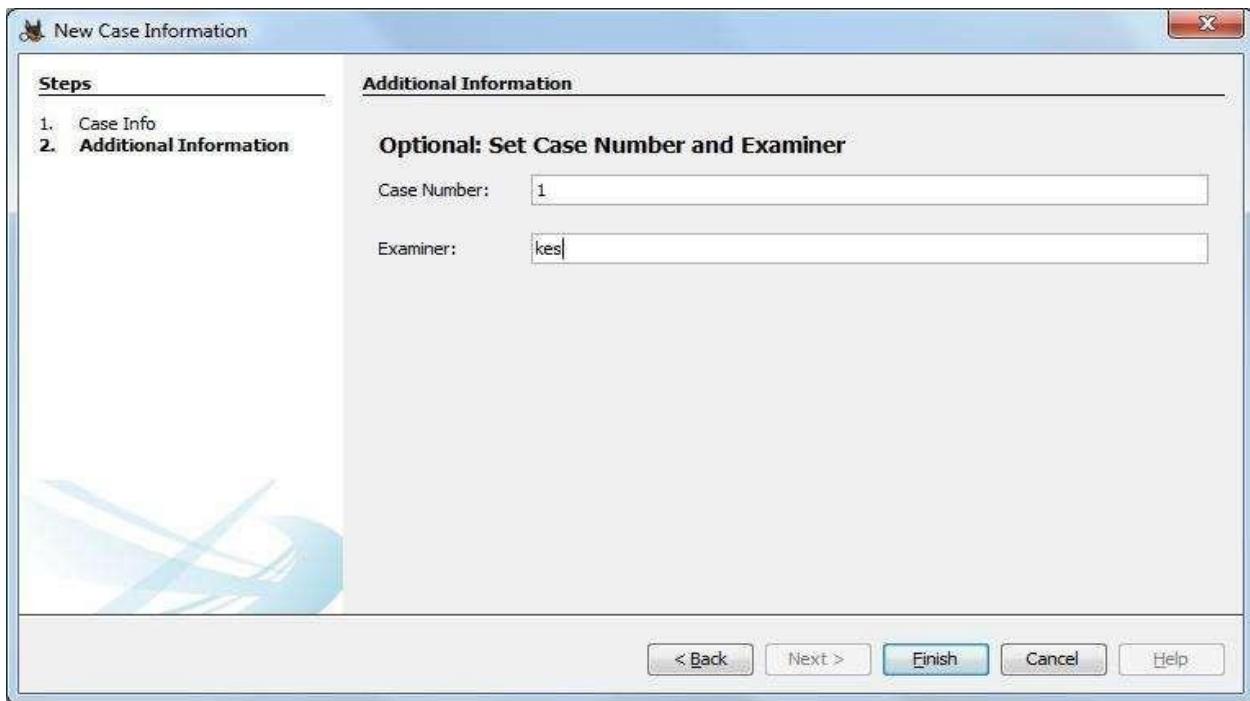
Step 2: Now create on New Case.



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



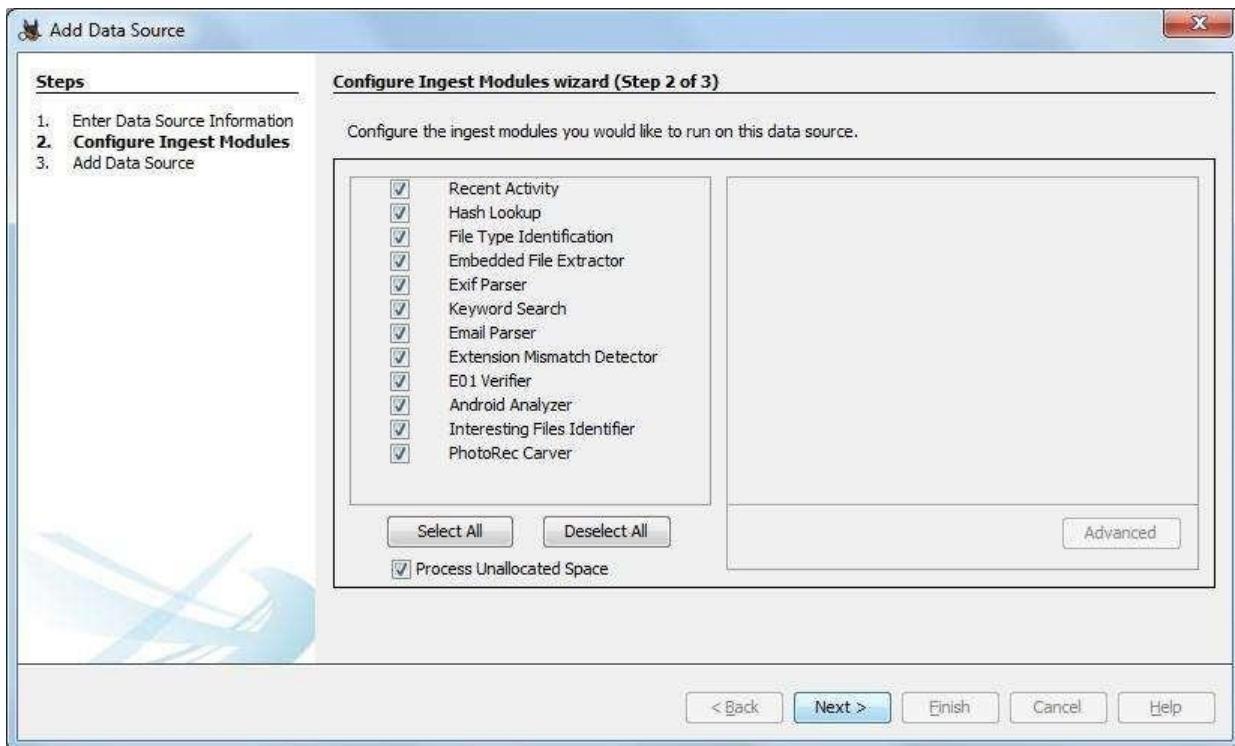
Step 4: Enter the additional Information and click on Finish.



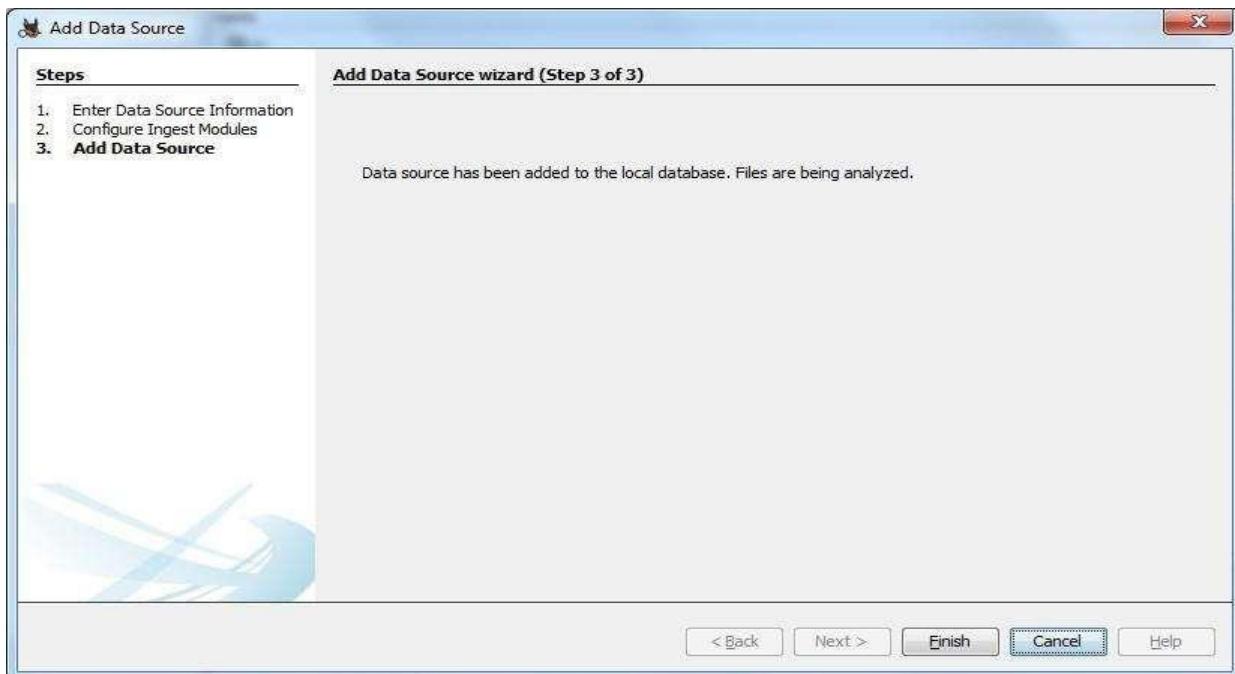
Step 5: Now Select Source Type as Local disk and Select Local disk form drop down list and click on Next.



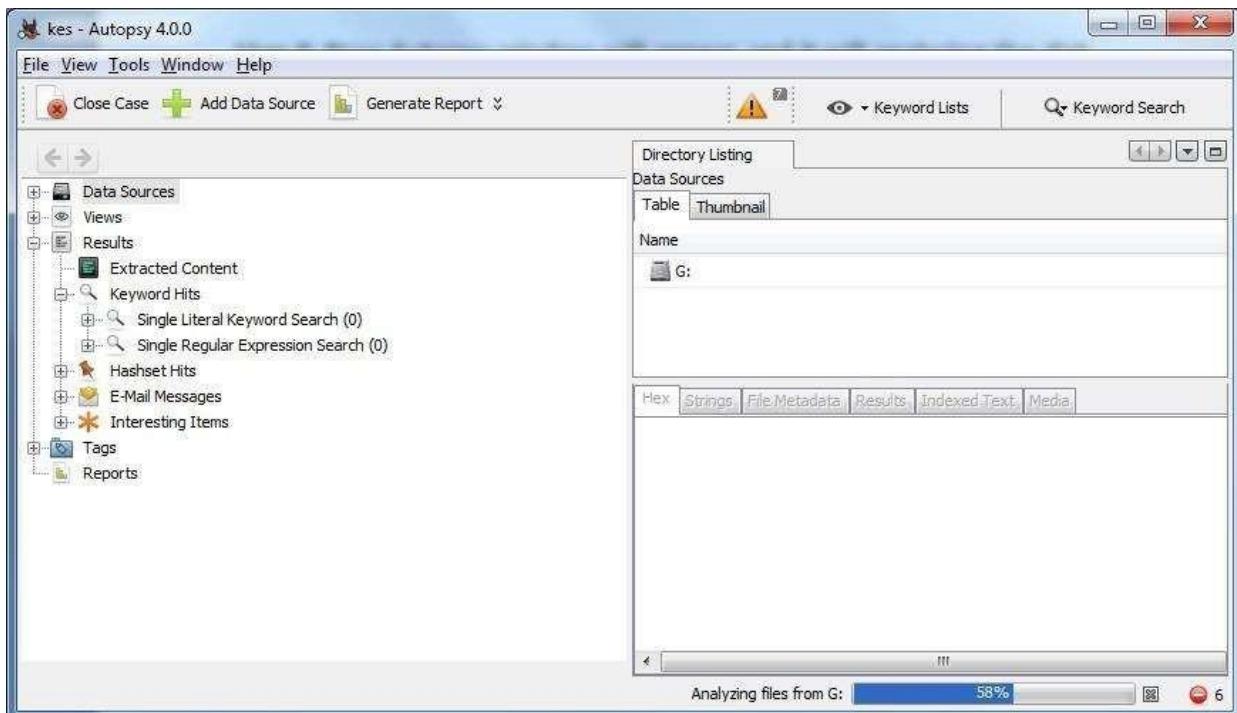
Step 6: Click on Next Button.



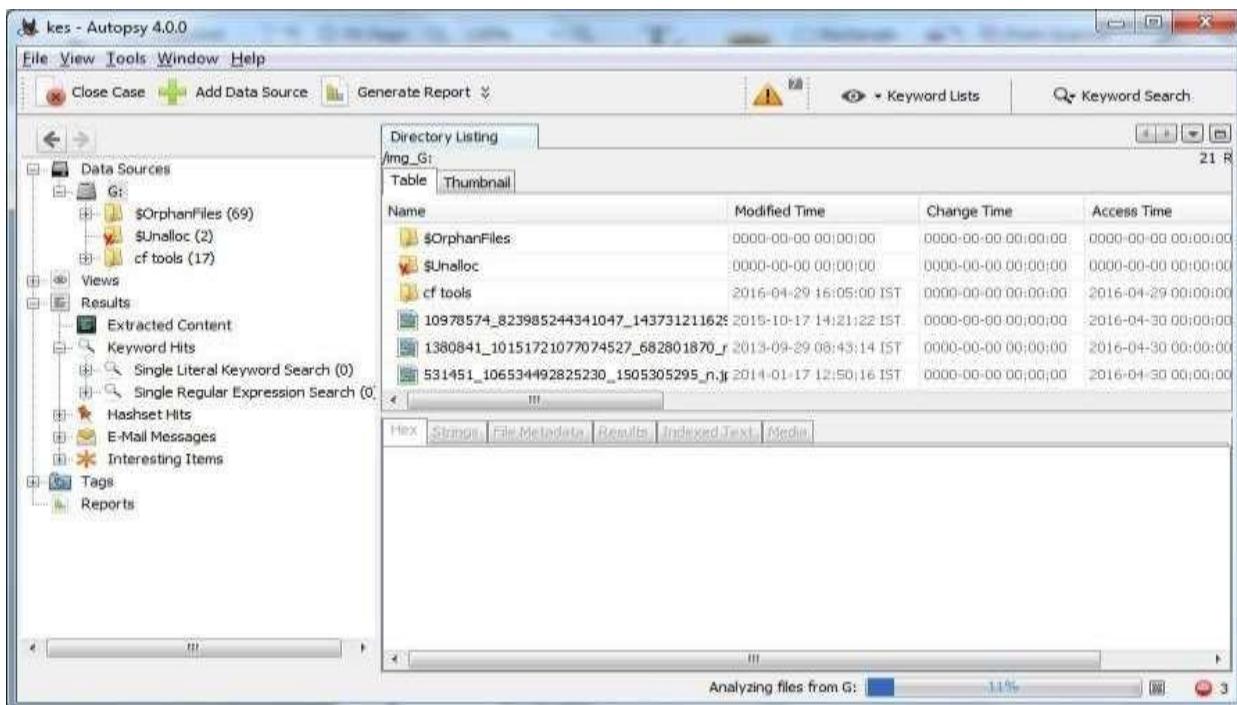
Step 7: Now click On Finish.



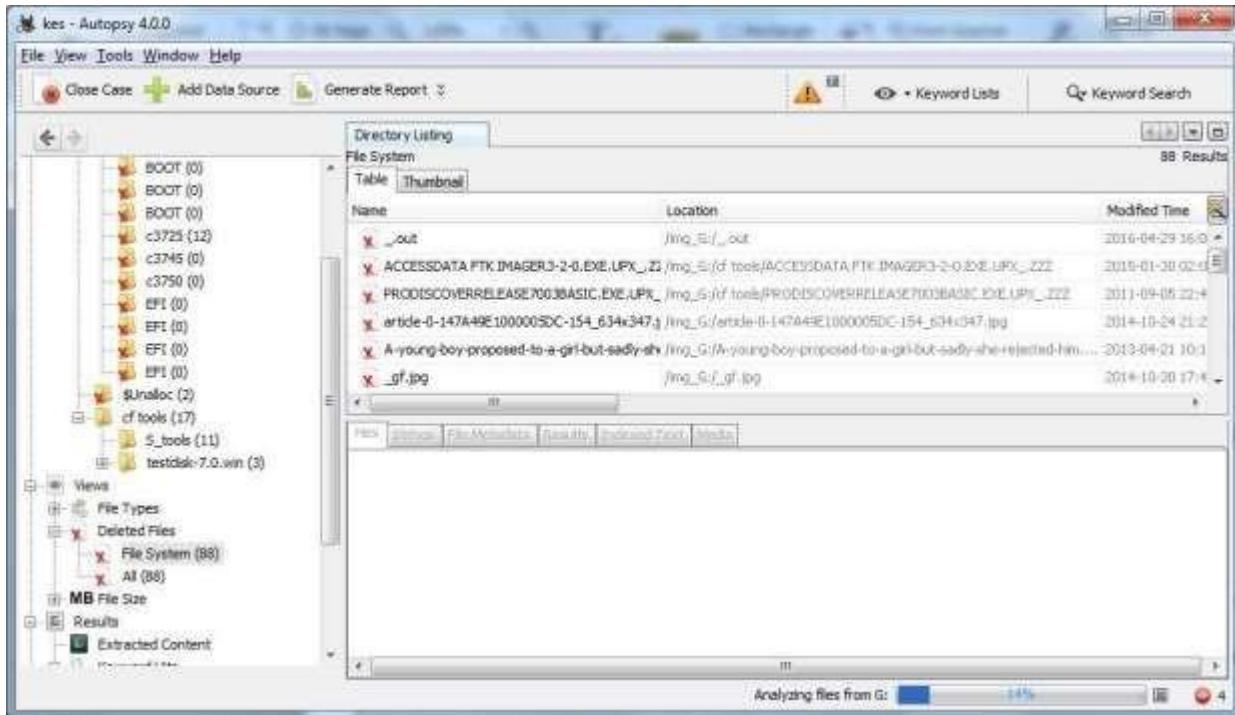
Step 8: Now Autopsy window will appear and it will analyzing the disk that we have selected.



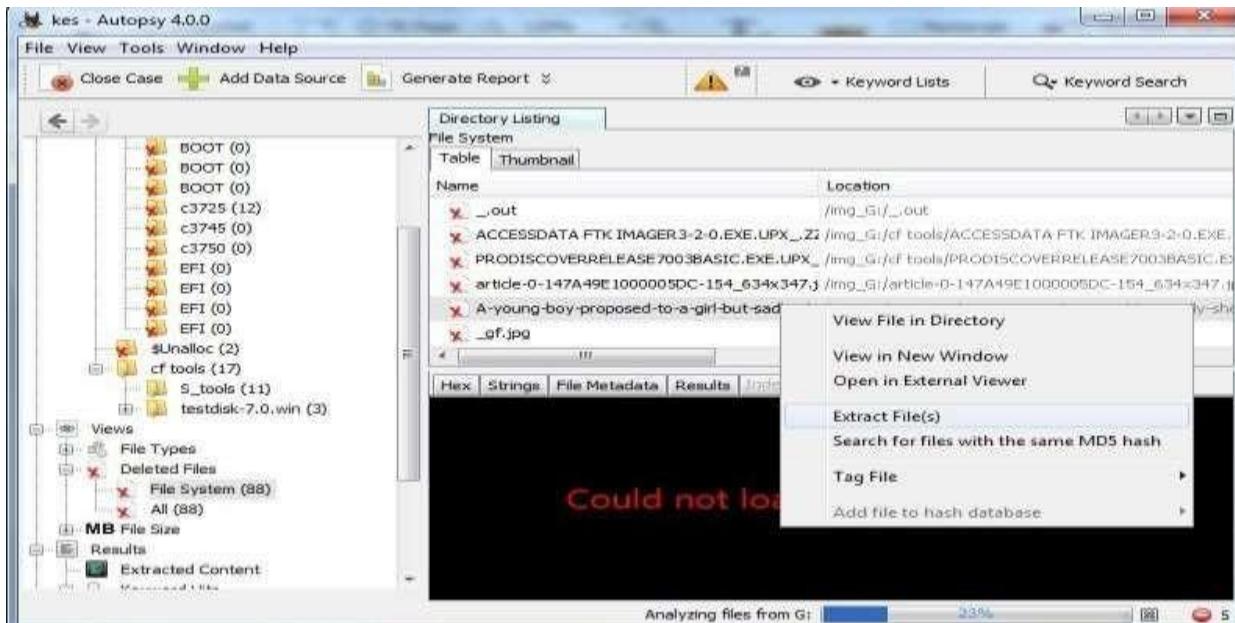
Step 9: All files will appear in table tab select any file to see the data.



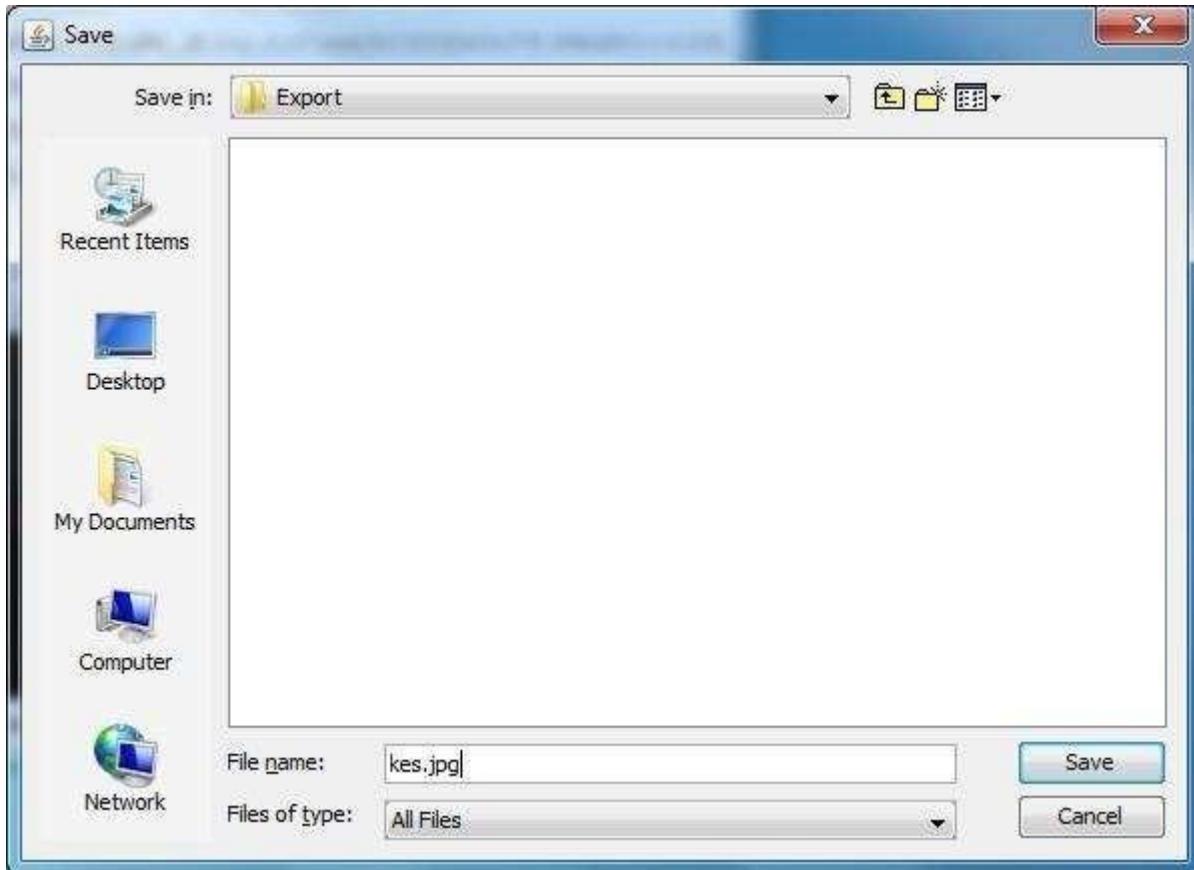
Step 10: Expand the tree from left side panel to view the document files.



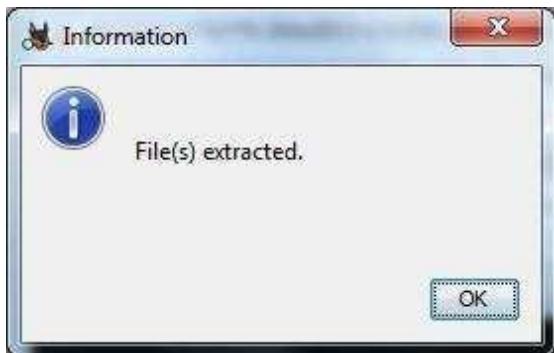
Step 11: To recover the file, go to view node-> Deleted Files node , here select any file and right click on it than select Extract Files option.



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



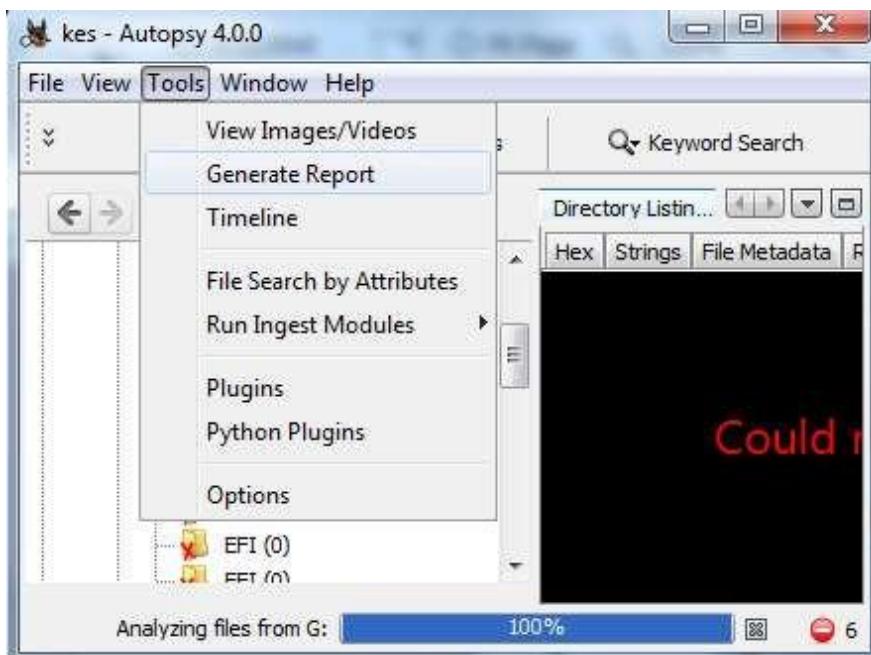
Sep 13 : Now Click on Ok.

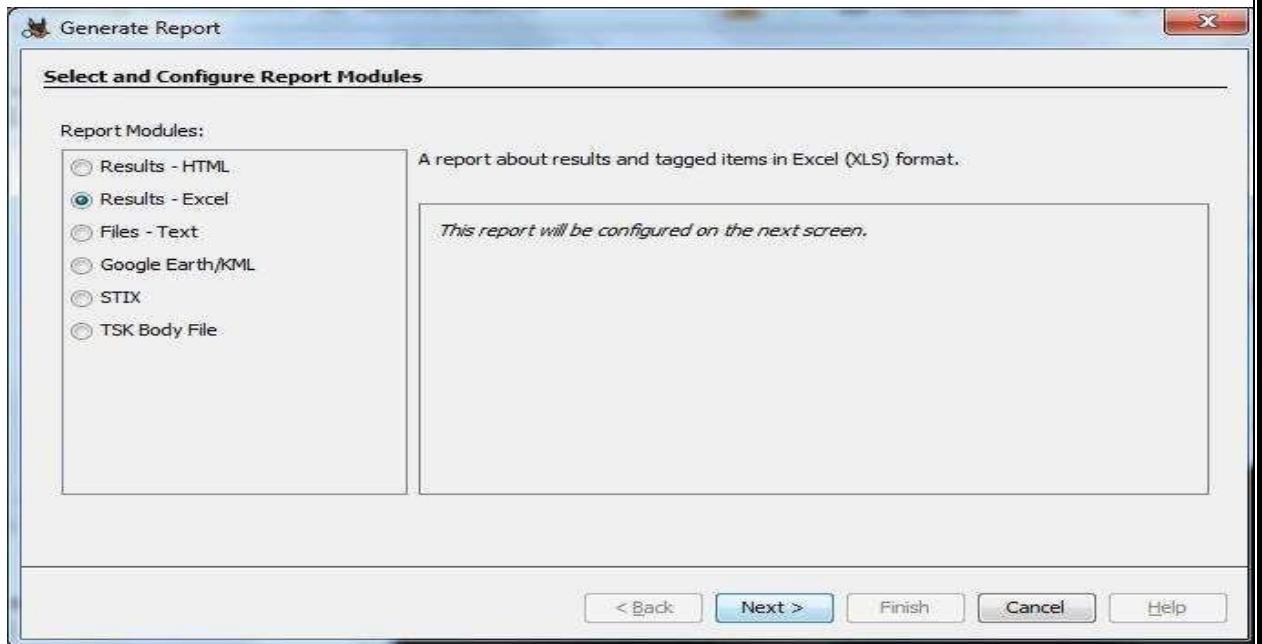


Step 14: Now go to the Export Folder to view Recover file.

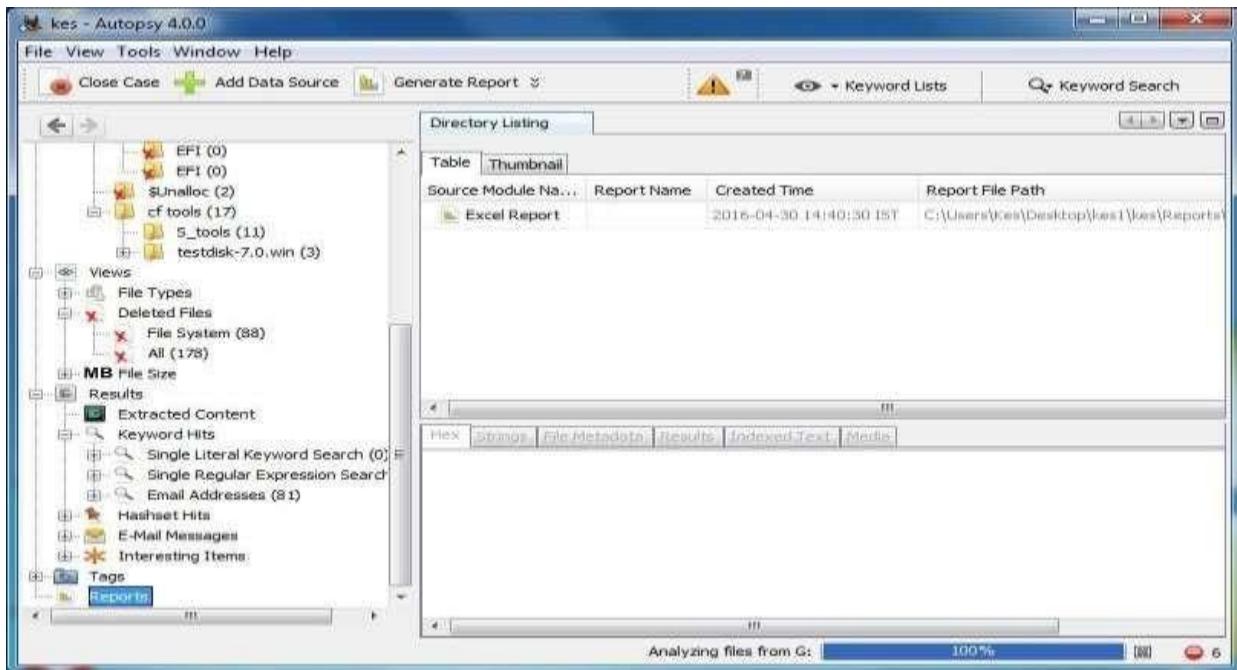


Step 15: Click on Generate Report from autopsy window and Select the Excel format and click on next.

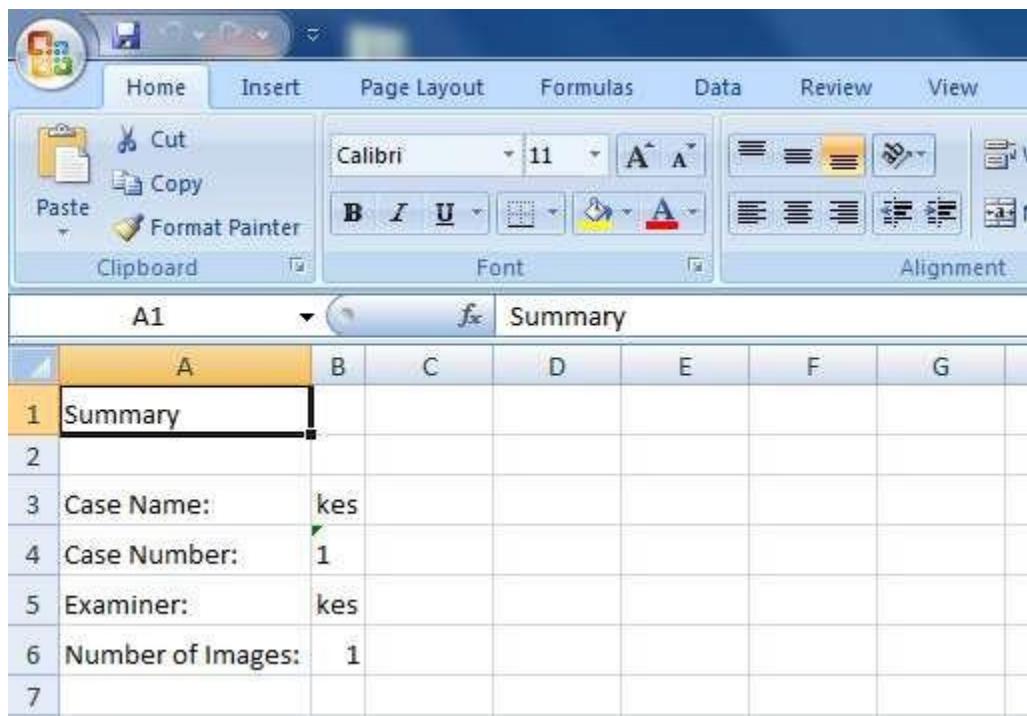




Step 16: Now Report is Generated So click on close Button .we can see the Report on Report Node.



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



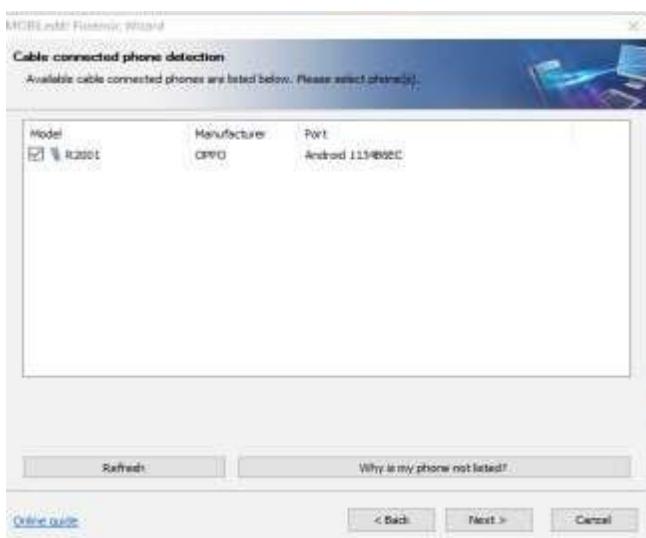
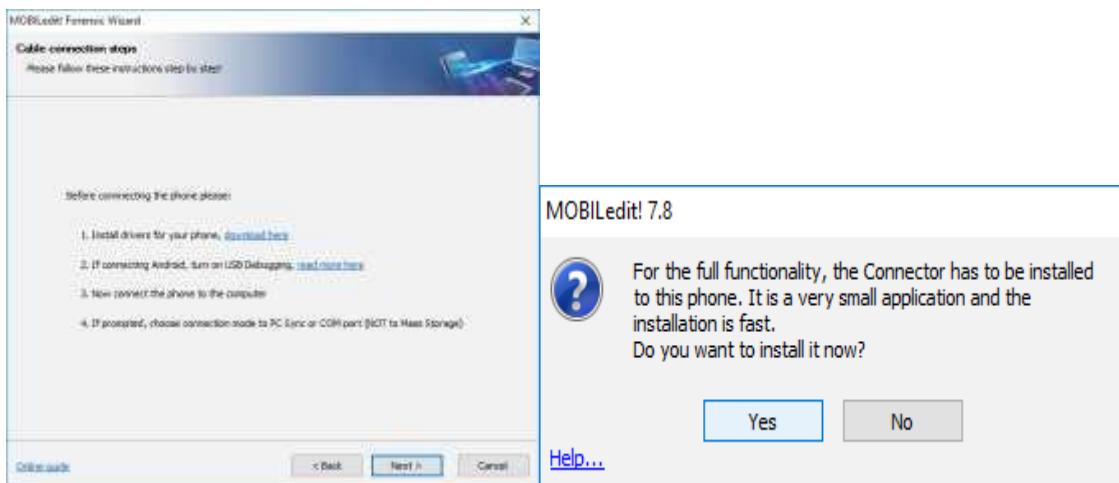
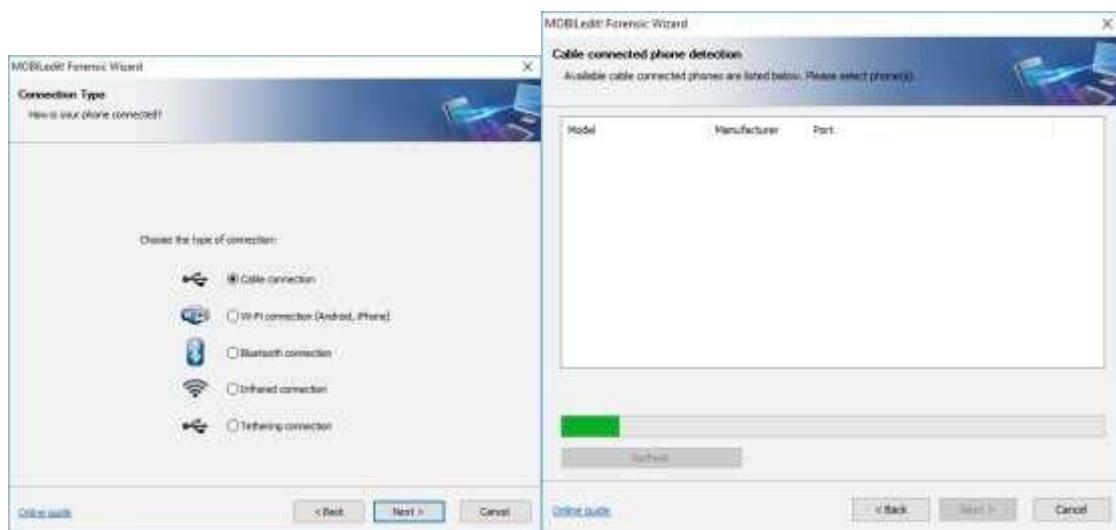
A screenshot of Microsoft Excel showing a table with 7 rows and 2 columns. The table is titled "Summary". The data is as follows:

	Summary
1	Summary
2	
3	Case Name: kes
4	Case Number: 1
5	Examiner: kes
6	Number of Images: 1
7	

PRACTICAL 8

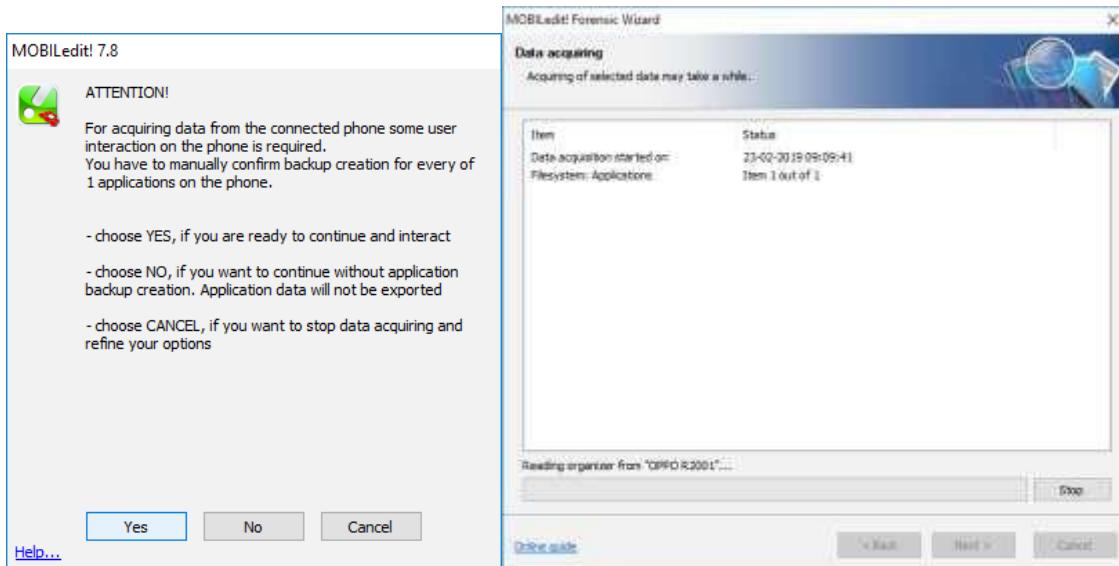
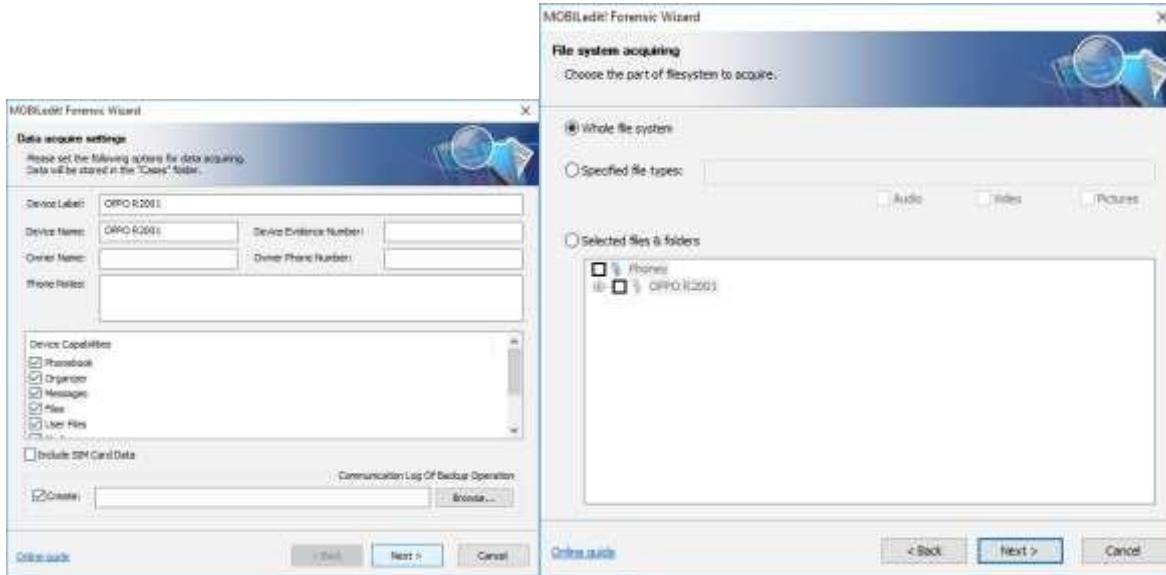
Aim :- Acquisition of Cell phones and Mobile devices .

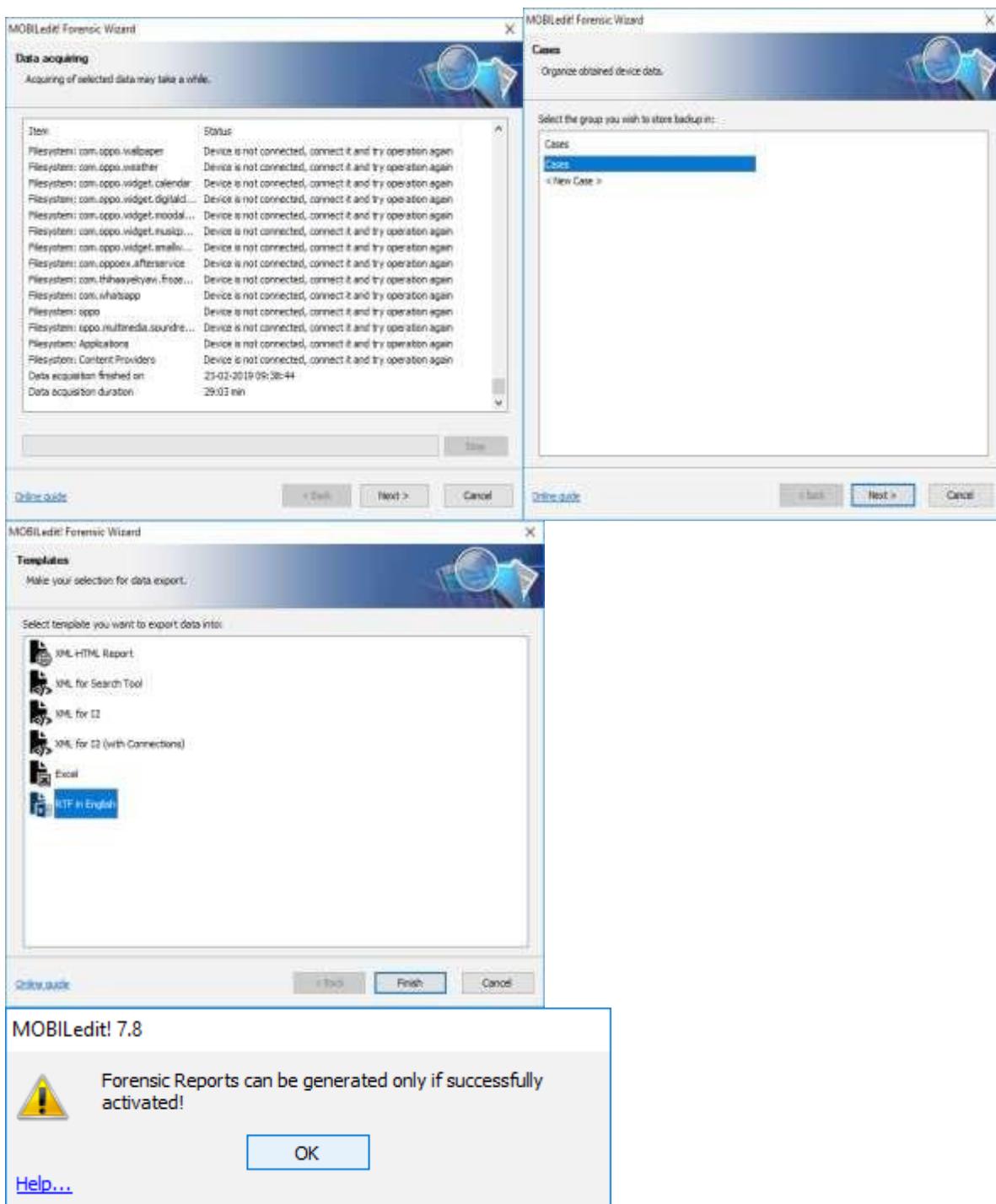




Working...

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





The screenshot shows the main interface of MOBILedit Forensic Lite. The title bar reads "MOBILedit Forensic Lite". The menu bar includes File, Edit, View, Device, Help, and a toolbar with Back, Forward, Import, Export, Print, Connect, Settings, and SIM Clone buttons. A search bar is at the top right.

The main area displays the device information for an "OPPO R2001 (23-02-2019 09:10:00) (Read-Only)". The device icon is an Android figure. The device details are:

- Manufacturer: OPPO
- Model: R2001
- IMEI: 355765048073256
- Operator: Not available
- Phone time: <unknown>
- Software revision: A2.2 (17)
- Connected via: Forensic Connector 1.14
- Network: GSM
- Platform: Android
- Data file: C:\Users\DELL\AppData\Roaming\MOBILEditForensic\00000001.dat
- Created by: DESKTOP-BS22RVM\DELL

On the right, there are four cards: "Phonebook (550)", "Call Logs", "Messages", and "Hex Dump". Below these are "Online Info" (Platform: Android 4.2.2 (17), IMEI: 355765048073256), "Reports", and "Open Data Folder".

The bottom status bar indicates "Not connected".

The screenshot shows the "Phonebook (550) - OPPO R2001 (23-02-2019 09:10:00)" screen. The title bar is identical to the main interface. The menu bar includes File, Edit, View, Phonebook, Action, and Help.

The main area displays a list of contacts under the "All (550)" tab. The contacts are:

Name	Label	Number
Mobile Phone	11	
Mobile Phone	2	+911400054208
Mobile Phone	3	9880552416
Mobile Phone	4	+918286332811
Mobile Phone	5	9880552418
Mobile Phone	6	+910286332811
Mobile Phone	7	+917877710850

Call Logs (97) - OPPO R2001 (23-02-2019 09:10:00)

Name	Number	Date
[Redacted]	+91140095401	22-02-2019 20:10:12
[Redacted]	+911400954448	22-02-2019 16:23:14
[Redacted]	+911400954496	22-02-2019 14:37:00
[Redacted]	+911400954499	21-02-2019 15:44:20
Sairat	+919930547534	20-02-2019 11:38:44
Sairat	+919930547534	20-02-2019 11:29:22
Sairat	+919930547534	20-02-2019 10:16:01
[Redacted]	+911400954496	19-02-2019 16:38:13
[Redacted]	+912229902000	19-02-2019 10:04:24
[Redacted]	+917977408836	18-02-2019 23:26:18
[Redacted]	+917977408836	18-02-2019 21:19:07
Papa	+919004480339	18-02-2019 20:25:20
Senthil Bhal	+919792346277	18-02-2019 20:17:29
[Redacted]	+911400954437	18-02-2019 19:43:53
Aarad IV	+91879888438	17-02-2019 23:44:42
Aarad IV	+91879888438	17-02-2019 21:28:48

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

Time	Sender / Recipient
21-02-2019 08:25:21	55256
22-02-2019 20:55:29	IZ-IDEA
22-02-2019 17:18:01	Aaaaa
22-02-2019 14:06:49	IM-655456
22-02-2019 14:15:48	IM-612345
22-02-2019 10:34:12	IM-6554563
21-02-2019 16:51:49	+919987501727
21-02-2019 16:44:12	MD-KOTAKB
21-02-2019 12:05:36	AX-IYCGOV
21-02-2019 09:09:27	IM-657886
22-02-2019 08:27:34	Dench Wolf/ Last playing now to Win 10000 CALL 10256 To Free.. Inc.
22-02-2019 14:08:05	07781-181007 To 18-3F14-B-121E411244-30021-3-192-0
22-02-2019 14:08:26	Chennai/ Win Rs.15 & Rs.15 worth FREE Recharge everyday.
21-02-2019 14:08:26	07778-121007 To 18-3F14-B-121E411244-30021-3-192-0
21-02-2019 08:16:34	Rs.1000 Win 1000 & Rs.1000 worth Rs.1000
21-02-2019 08:16:34	Limited Chennai/ Call 10256 To Free and Win Rs.15 worth Recharge everyday.. Inc.
21-02-2019 08:16:34	07778-121007 To 18-3F14-B-121E411244-30021-3-192-0
26-02-2019 09:09:27	Special OFFER Avail upto our first recharge to Rs.1000 Cashback in Exchange MRE4036WV1 GrandhipC Netnifty ..com
26-02-2019 09:09:27	Rs.10 to 55256Thc .. & Ag net

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 use email 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 integrates 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

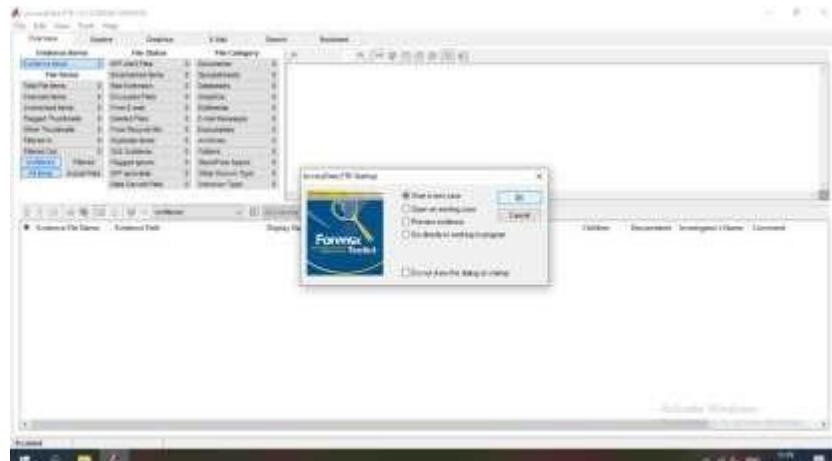
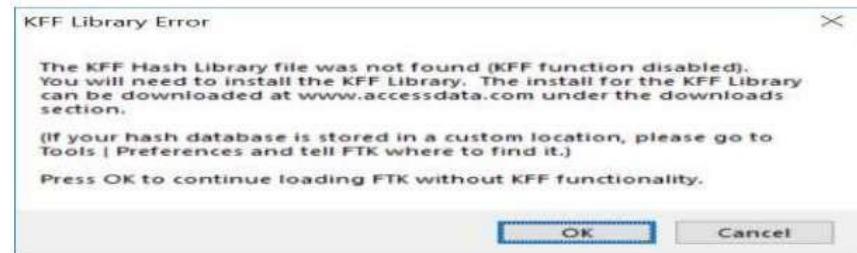
SMTP stands for Simple Mail Transfer Protocol. It was first proposed in 1982. It is a standard protocol used for sending e-mail efficiently and reliably over the internet. Simple Mail Transfer Protocol (SMTP) is the standard protocol for sending emails across the Internet.

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.

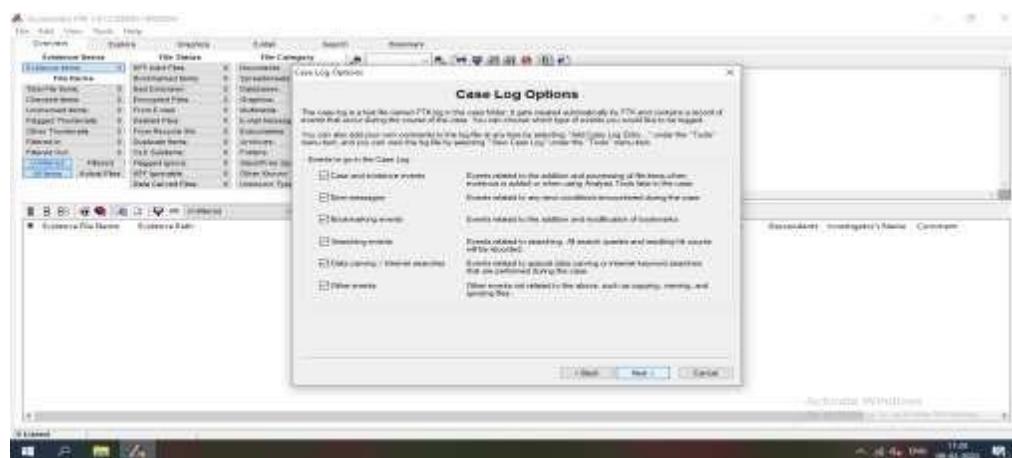
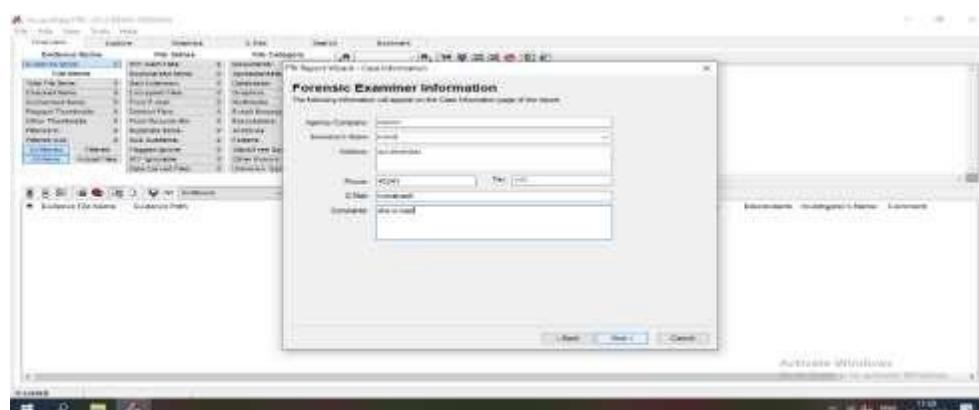
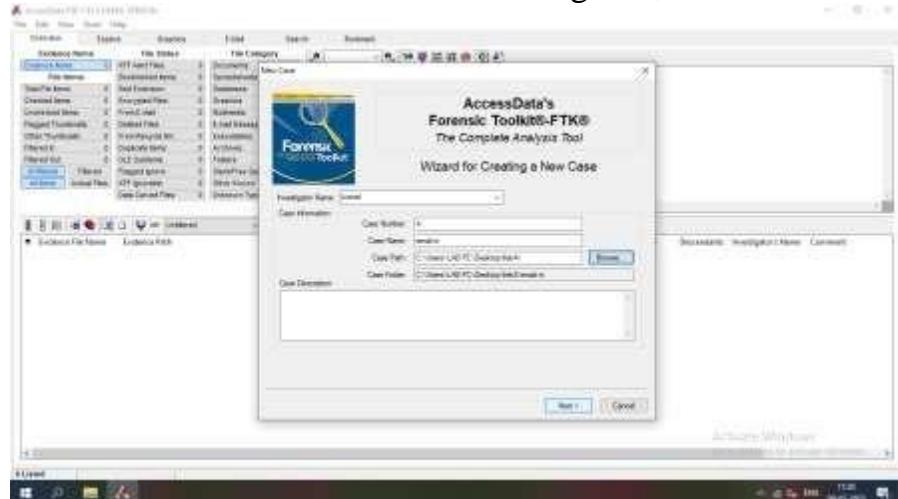
6. Click the Email Emphasis button, and then click Next.

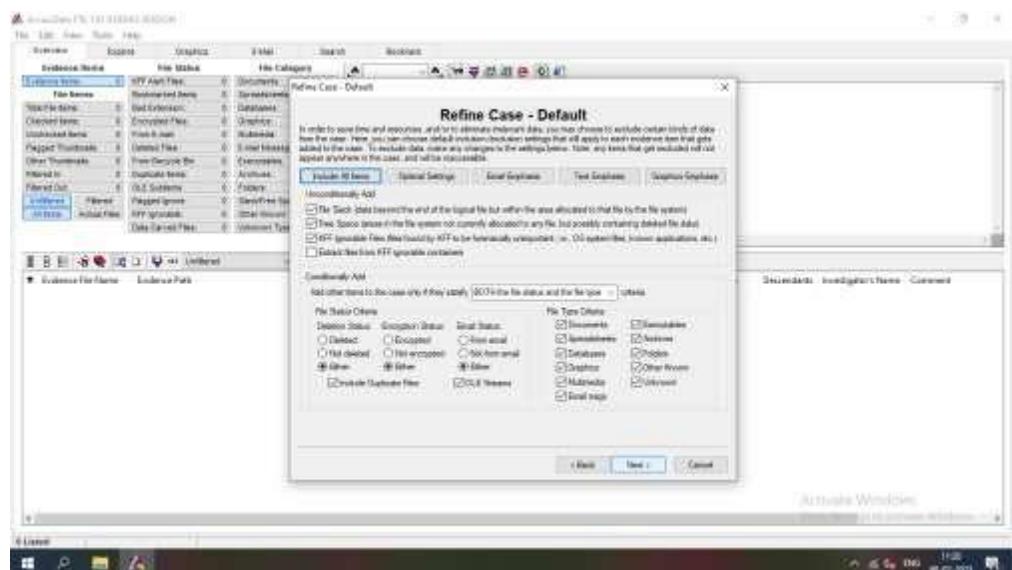
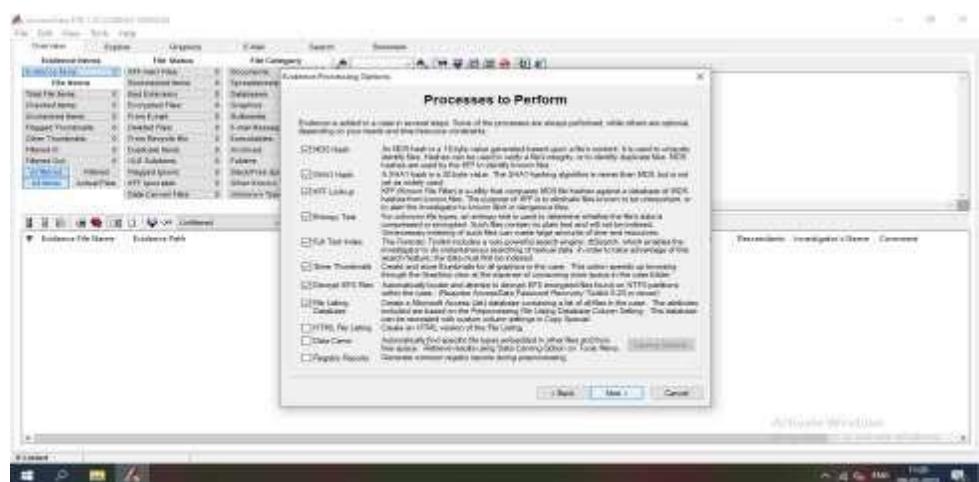
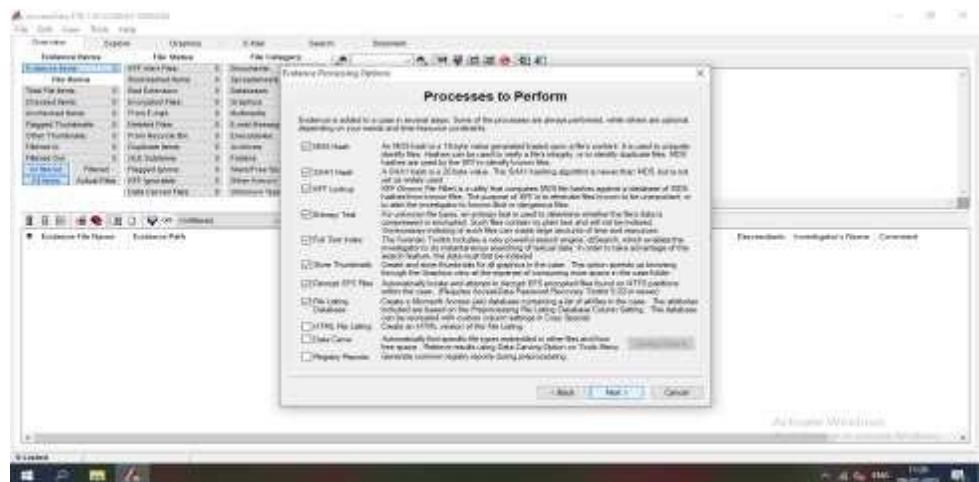
7. Click Next until you reach the Add Evidence to Case dialog box, and then click the Add Evidence button.

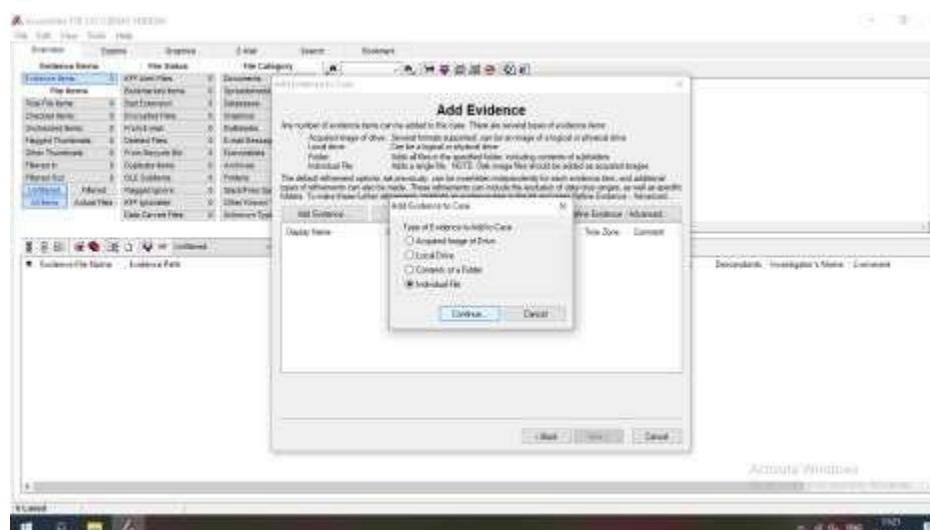
8. In the Add Evidence to Case dialog box, click the Individual File option button and then click Continue.

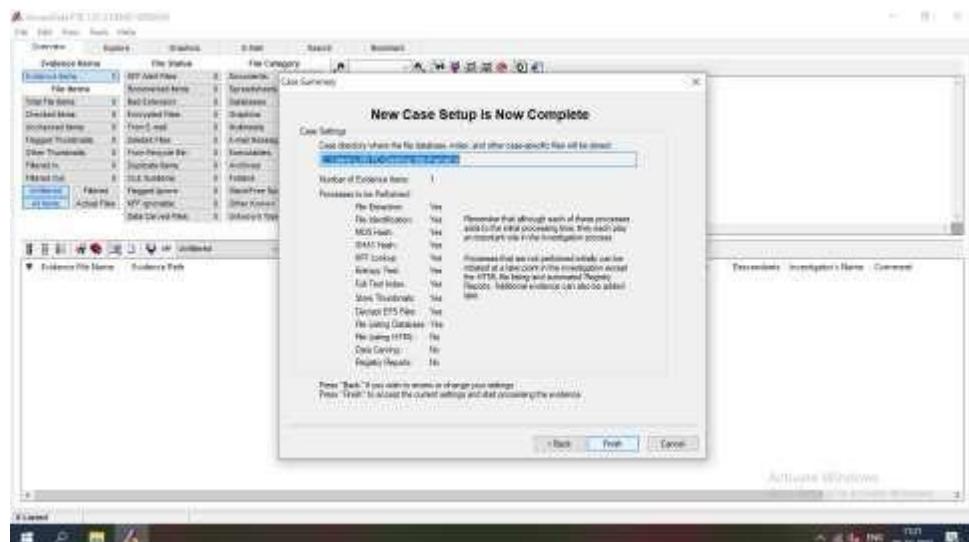
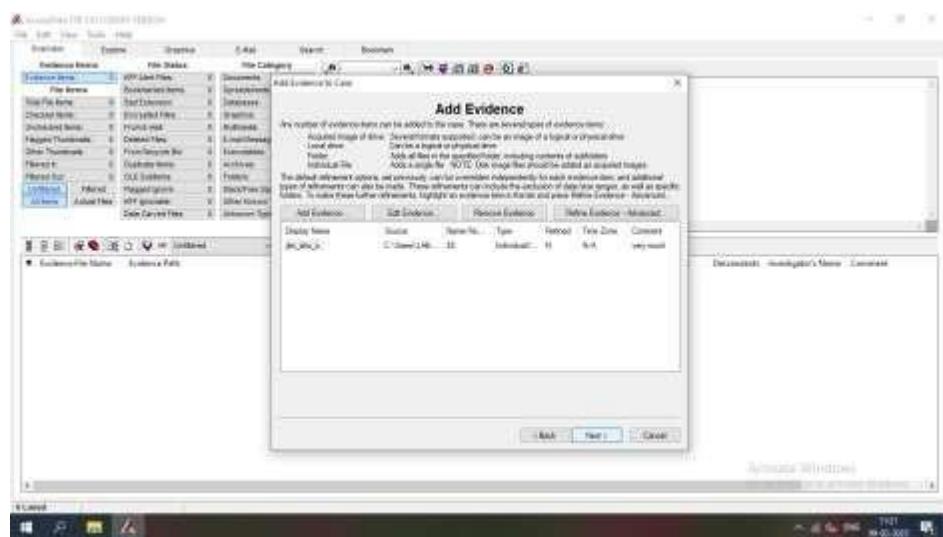
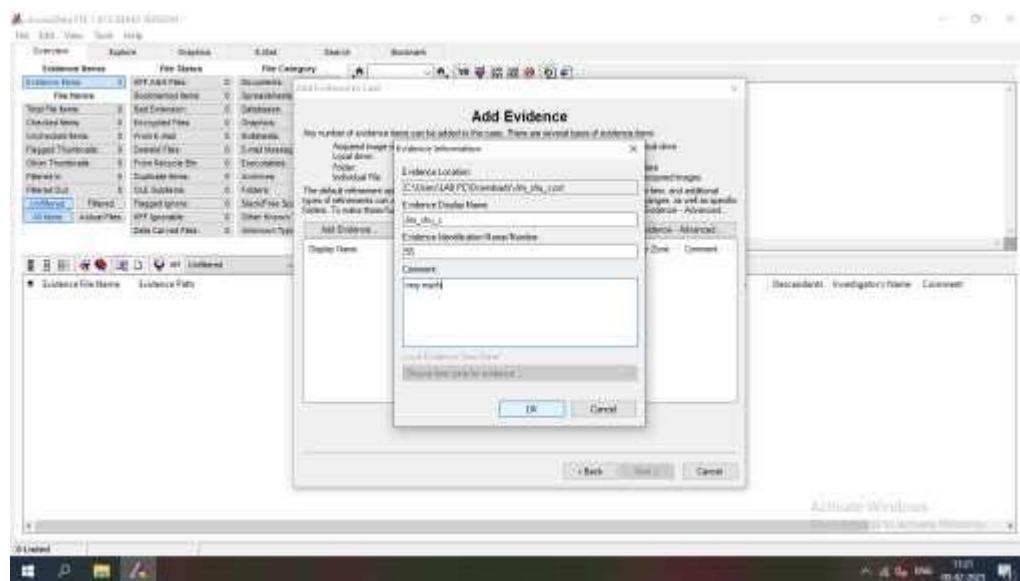
9. In the Select File dialog box, navigate to your work folder, click the Jim_shu's.pst file, and,then click Open.

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





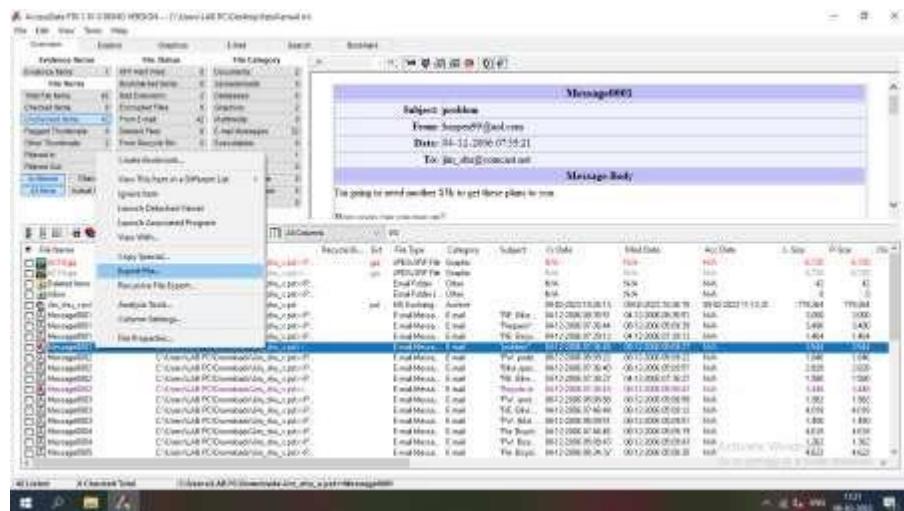




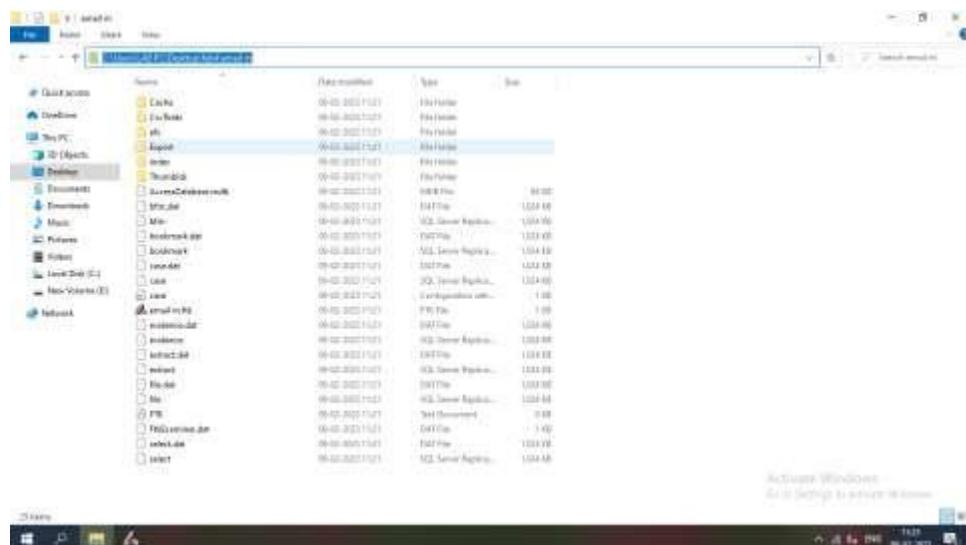
11. When the Add Evidence to Case dialog box opens, click Next. In the Case summary dialog box, click Finish.

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: jin_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%2Faol%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: 3450

Standard Header Information

Received: from imo-d20.mx.aol.com ([205.188.139.136])
 by secmax18.comcast.net (secmax18) with ESMTP
 id <2006120420521s18004fokge>; 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_cmt_v38_r7.6.) id i406.33cb6298 (60+34)
 for <jin_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 cianet-d01.mail.aol.com (v114.2) with ESMTP id MAILCIAAAOLD013-ec124573825b284; Sun, 03 Dec 2006 21:05:15 -0500
 To: jin_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

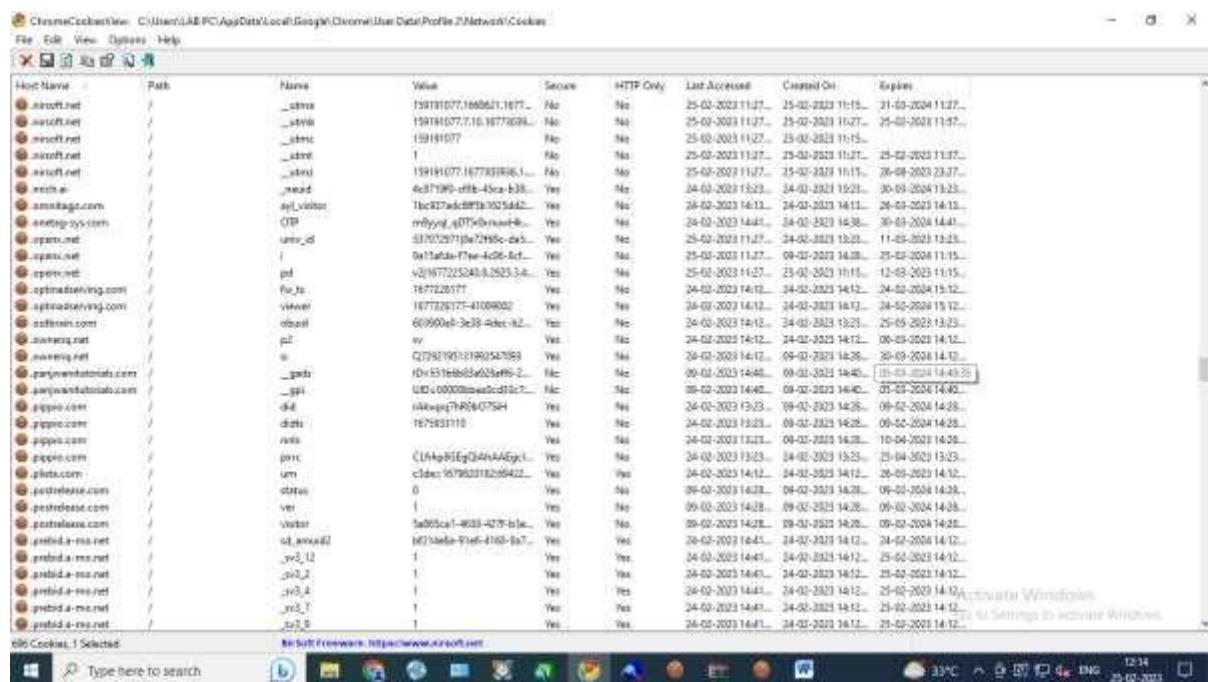
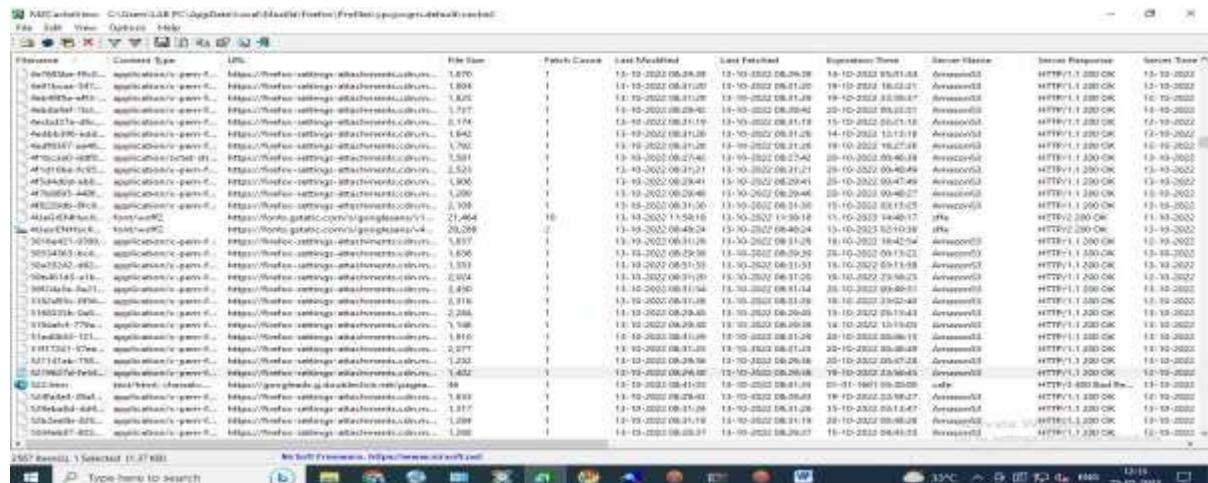
BrowsingHistoryView : BrowsingHistoryView is a utility that reads the history data of 4 different Web browsers (Internet Explorer, Mozilla Firefox, Google Chrome, and Safari) and displays the browsing history of all these Web browsers in one table. The browsing history table includes the following information: 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.



File Name	Content Type	URL	Last Accessed	Last Modified	Expiration Time	Last Checked	Hit	File Size	Subfolder Name	Full Path
19-HDCOL24V.jpg	image/jpeg	https://th.bing.com/th?id=OIP.yJ6B0ic30WhIeq...	25-02-2023 08:30:39	N/A	10-03-2023 15:29:10	N/A	1	4,216	39Y42014	C:\User\LAB
19-HKA61B.jpg	image/jpeg	https://th.bing.com/th?id=OIP.W28074bd46c...	25-02-2023 08:31:55	N/A	27-03-2023 03:06:51	N/A	1	3,176	39Y42014	C:\User\LAB
19-HK998E15.jpg	image/jpeg	https://th.bing.com/th?id=OIP.J65n7Jgk6wkkh...	25-02-2023 08:30:48	N/A	10-03-2023 15:08:14	N/A	1	5,348	39Y42014	C:\User\LAB
19-HD2QALQ.jpg	image/jpeg	https://th.bing.com/th?id=OIP.ZnemfThdOpwv...	25-02-2023 08:36:42	N/A	10-03-2023 08:12:05	N/A	3	5,424	39Y42014	C:\User\LAB
19-HQ9QD94.jpg	image/jpeg	https://th.bing.com/th?id=OIP.WG77ta852-rl...	24-02-2023 22:25:38	N/A	24-03-2023 02:08:23	N/A	2	3,468	39Y42014	C:\User\LAB
19-H76M7S.jpg	image/jpeg	https://th.bing.com/th?id=OIP.fA5tH919f9T...	23-02-2023 02:55:17	N/A	09-03-2023 01:03:38	N/A	4	5,718	39Y42014	C:\User\LAB
19-HA4X3D0.jpg	image/jpeg	https://th.bing.com/th?id=OIP.Mf6eLz2wv...	25-02-2023 08:33:19	N/A	10-03-2023 23:16:34	N/A	2	5,280	39Y42014	C:\User\LAB
19-H1TFDD0.jpg	image/jpeg	https://th.bing.com/th?id=OIP.4M6f62d...	25-02-2023 01:26:01	N/W	26-03-2023 20:47:12	N/A	1	1,077	39Y42014	C:\User\LAB
19-H150AMC.jpg	image/jpeg	https://th.bing.com/th?id=AJT6qA23A291830...	24-02-2023 22:25:39	N/A	24-03-2023 03:06:51	N/A	2	3,128	39Y42014	C:\User\LAB
19-H4PHL283.jpg	image/jpeg	https://th.bing.com/th?id=OIP.WQ.M4b...	25-02-2023 02:25:38	N/A	26-03-2023 08:15:49	N/A	2	1,768	39Y42014	C:\User\LAB
19-HK0TIV0.jpg	image/jpeg	https://th.bing.com/th?id=OIP.WQ.M4b...	25-02-2023 10:36:42	N/A	24-03-2023 03:04:07	N/A	3	2,015	39Y42014	C:\User\LAB
19-HQ3ASV0.jpg	image/jpeg	https://th.bing.com/th?id=OIC.T001LCC3773...	25-02-2023 10:36:42	N/A	24-03-2023 03:04:56	N/A	3	6,617	39Y42014	C:\User\LAB
19-HQ2ZUW0.jpg	image/jpeg	https://th.bing.com/th?id=OIP.3e9587489...	25-02-2023 08:16:13	N/W	26-03-2023 14:48:36	N/A	1	3,884	39Y42014	C:\User\LAB
19-HCTWV2Q.jpg	image/jpeg	https://th.bing.com/th?id=OIP.3f64PMH...	25-02-2023 01:21:19	N/W	04-03-2023 09:06:25	N/A	1	617	39Y42014	C:\User\LAB
19-HLQ3N05K.jpg	image/jpeg	https://www.bing.com/th?id=OIP.M4735d4...	25-02-2023 01:04:01	N/A	11-03-2023 01:04:01	N/A	1	5,733	39Y42014	C:\User\LAB
19-HQ1W4D0A.jpg	image/jpeg	https://th.bing.com/th?id=OIP.WQ.M4b...	25-02-2023 02:25:37	N/A	25-03-2023 12:03:57	N/A	1	4,754	39Y42014	C:\User\LAB
19-HQ1W4C0Q.jpg	image/jpeg	https://th.bing.com/th?id=OIC.5199485...	24-02-2023 22:25:38	N/A	26-03-2023 21:08:40	N/A	2	5,033	39Y42014	C:\User\LAB
19-HW2G304F.jpg	image/jpeg	https://th.bing.com/th?id=OIP.WQ.M4b...	25-02-2023 09:48:51	N/A	09-03-2023 20:15:51	N/A	3	5,887	39Y42014	C:\User\LAB
19-HV24001T.jpg	image/jpeg	https://th.bing.com/th?id=OIP.H7gPfH8...	25-02-2023 10:36:42	N/A	09-03-2023 12:22:47	N/A	2	5,247	39Y42014	C:\User\LAB
19-HA90710.jpg	image/jpeg	https://bing.com/th?id=OIS.GfAllCTAT7...	25-02-2023 08:31:11	N/W	27-03-2023 08:13:51	N/A	1	1,191	39Y42014	C:\User\LAB
19-HA4Q548F.jpg	image/jpeg	https://th.bing.com/th?id=Decorative-Letters-Y...	25-02-2023 01:28:01	N/A	29-03-2023 17:04:49	N/A	1	645	39Y42014	C:\User\LAB
19-HCIN809.jpg	image/jpeg	https://th.bing.com/th?id=OIP.WQ.M4b...	25-02-2023 11:26:48	N/A	26-03-2023 14:26:32	N/A	1	11,387	39Y42014	C:\User\LAB
19-H11992Z.jpg	image/jpeg	https://th.bing.com/th?id=OIC.00SWG...	25-02-2023 02:25:39	N/A	26-03-2023 10:04:23	N/A	2	2,939	39Y42014	C:\User\LAB
19-HHWED3.jpg	image/jpeg	https://th.bing.com/th?id=OIC.00SWG...	25-02-2023 10:36:42	N/A	11-03-2023 01:04:14	N/A	3	4,574	39Y42014	C:\User\LAB
19-HULLSDC0.jpg	image/jpeg	https://th.bing.com/th?id=OIC.2510859...	24-02-2023 10:25:38	N/A	26-03-2023 20:57:30	N/A	2	3,079	39Y42014	C:\User\LAB
19-HB7TMMX0.jpg	image/jpeg	https://th.bing.com/th?id=OIC.10d464a...	25-02-2023 10:36:42	N/A	21-03-2023 04:02:54	N/A	3	5,852	39Y42014	C:\User\LAB
19-H449320K.jpg	image/jpeg	https://th.bing.com/th?id=OIF.24nO43q...	25-02-2023 08:30:48	N/A	09-03-2023 23:53:28	N/A	2	3,011	39Y42014	C:\User\LAB
19-HDMMDR0A.jpg	image/jpeg	https://th.bing.com/th?id=OIC.D0154...	25-02-2023 10:56:54	N/A	23-03-2023 19:05:54	N/A	7	7,125	39Y42014	C:\User\LAB
19-HGD4HWY0.jpg	image/jpeg	https://th.bing.com/th?id=OIC.BA...	25-02-2023 02:58:04	N/W	34-03-2023 19:16:41	N/A	1	26,585	39Y42014	C:\User\LAB
19-H99W9HHM.jpg	image/jpeg	https://th.bing.com/th?id=OIC.e2347...	25-02-2023 08:37:09	N/W	37-03-2023 07:18:52	N/A	2	21,079	39Y42014	C:\User\LAB
19-HTQ2201D.jpg	image/jpeg	https://th.bing.com/th?id=OIC.073117...	25-02-2023 10:36:42	N/A	22-03-2023 04:06:14	N/A	7	4,495	39Y42014	C:\User\LAB
<hr/>										
File Name	Content Type	URL	Last Accessed	Last Modified	Expiration Time	Last Checked	Hit	File Size	Subfolder Name	Full Path
19-HCWWH001.jpg	image/jpeg	https://th.bing.com/th?id=OIC.00SWG...	25-02-2023 10:36:42	N/A	26-03-2023 04:06:14	N/A	7	4,495	39Y42014	C:\User\LAB
<hr/>										
File Name	Content Type	URL	Last Accessed	Last Modified	Expiration Time	Last Checked	Hit	File Size	Subfolder Name	Full Path
19-HCWWH001.jpg	image/jpeg	https://th.bing.com/th?id=OIC.00SWG...	25-02-2023 10:36:42	N/A	26-03-2023 04:06:14	N/A	7	4,495	39Y42014	C:\User\LAB
<hr/>										
File Name	Content Type	URL	Last Accessed	Last Modified	Expiration Time	Last Checked	Hit	File Size	Subfolder Name	Full Path
19-HCWWH001.jpg	image/jpeg	https://th.bing.com/th?id=OIC.00SWG...	25-02-2023 10:36:42	N/A	26-03-2023 04:06:14	N/A	7	4,495	39Y42014	C:\User\LAB
<hr/>										
File Name	Content Type	URL	Last Accessed	Last Modified	Expiration Time	Last Checked	Hit	File Size	Subfolder Name	Full Path
19-HCWWH001.jpg	image/jpeg	https://th.bing.com/th?id=OIC.00SWG...	25-02-2023 10:36:42	N/A	26-03-2023 04:06:14	N/A	7	4,495	39Y42014	C:\User\LAB
<hr/>										
File Name	Content Type	URL	Last Accessed	Last Modified	Expiration Time	Last Checked	Hit	File Size	Subfolder Name	Full Path
19-HCWWH001.jpg	image/jpeg	https://th.bing.com/th?id=OIC.00SWG...	25-02-2023 10:36:42	N/A	26-03-2023 04:06:14	N/A	7	4,495	39Y42014	C:\User\LAB
<hr/>										
File Name	Content Type	URL	Last Accessed	Last Modified	Expiration Time	Last Checked	Hit	File Size	Subfolder Name	Full Path
19-HCWWH001.jpg	image/jpeg	https://th.bing.com/th?id=OIC.00SWG...	25-02-2023 10:36:42	N/A	26-03-2023 04:06:14	N/A	7	4,495	39Y42014	C:\User\LAB
<hr/>										
File Name	Content Type	URL	Last Accessed	Last Modified	Expiration Time	Last Checked	Hit	File Size	Subfolder Name	Full Path
19-HCWWH001.jpg	image/jpeg	https://th.bing.com/th?id=OIC.00SWG...	25-02-2023 10:36:42	N/A	26-03-2023 04:06:14	N/A	7	4,495	39Y42014	C:\User\LAB
<hr/>										
File Name	Content Type	URL	Last Accessed	Last Modified	Expiration Time	Last Checked	Hit	File Size	Subfolder Name	Full Path
19-HCWWH001.jpg	image/jpeg	https://th.bing.com/th?id=OIC.00SWG...	25-02-2023 10:36:42	N/A	26-03-2023 04:06:14	N/A	7	4,495	39Y42014	C:\User\LAB
<hr/>										
File Name	Content Type	URL	Last Accessed	Last Modified	Expiration Time	Last Checked	Hit	File Size	Subfolder Name	Full Path
19-HCWWH001.jpg	image/jpeg	https://th.bing.com/th?id=OIC.00SWG...	25-02-2023 10:36:42	N/A	26-03-2023 04:06:14	N/A	7	4,495	39Y42014	C:\User\LAB
<hr/>										
File Name	Content Type	URL	Last Accessed	Last Modified	Expiration Time	Last Checked	Hit	File Size	Subfolder Name	Full Path
19-HCWWH001.jpg	image/jpeg	https://th.bing.com/th?id=OIC.00SWG...	25-02-2023 10:36:42	N/A	26-03-2023 04:06:14	N/A	7	4,495	39Y42014	C:\User\LAB
<hr/>										
File Name	Content Type	URL	Last Accessed	Last Modified	Expiration Time	Last Checked	Hit	File Size	Subfolder Name	Full Path
19-HCWWH001.jpg	image/jpeg	https://th.bing.com/th?id=OIC.00SWG...	25-02-2023 10:36:42	N/A	26-03-2023 04:06:14	N/A	7	4,495	39Y42014	C:\User\LAB
<hr/>										
File Name	Content Type	URL	Last Accessed	Last Modified	Expiration Time	Last Checked	Hit	File Size	Subfolder Name	Full Path
19-HCWWH001.jpg	image/jpeg	https://th.bing.com/th?id=OIC.00SWG...	25-02-2023 10:36:42	N/A	26-03-2023 04:06:14	N/A	7	4,495	39Y42014	C:\User\LAB
<hr/>										
File Name	Content Type	URL	Last Accessed	Last Modified	Expiration Time	Last Checked	Hit	File Size	Subfolder Name	Full Path
19-HCWWH001.jpg	image/jpeg	https://th.bing.com/th?id=OIC.00SWG...	25-02-2023 10:36:42	N/A	26-03-2023 04:06:14	N/A	7	4,495	39Y42014	C:\User\LAB
<hr/>										
File Name	Content Type	URL	Last Accessed	Last Modified	Expiration Time	Last Checked	Hit	File Size	Subfolder Name	Full Path
19-HCWWH001.jpg	image/jpeg	https://th.bing.com/th?id=OIC.00SWG...	25-02-2023 10:36:42	N/A	26-03-2023 04:06:14	N/A	7	4,495	39Y42014	C:\User\LAB
<hr/>										
File Name	Content Type	URL	Last Accessed	Last Modified	Expiration Time	Last Checked	Hit	File Size	Subfolder Name	Full Path
19-HCWWH001.jpg	image/jpeg	https://th.bing.com/th?id=OIC.00SWG...	25-02-2023 10:36:42	N/A	26-03-2023 04:06:14	N/A	7	4,495	39Y42014	C:\User\LAB
<hr/>										
File Name	Content Type	URL	Last Accessed	Last Modified	Expiration Time	Last Checked	Hit	File Size	Subfolder Name	Full Path
19-HCWWH001.jpg	image/jpeg	https://th.bing.com/th?id=OIC.00SWG...	25-02-2023 10:36:42	N/A	26-03-2023 04:06:14	N/A	7	4,495	39Y42014	C:\User\LAB
<hr/>										
File Name	Content Type	URL	Last Accessed	Last Modified	Expiration Time	Last Checked	Hit	File Size	Subfolder Name	Full Path
19-HCWWH001.jpg	image/jpeg	https://th.bing.com/th?id=OIC.00SWG...	25-02-2023 10:36:42	N/A	26-03-2023 04:06:14	N/A	7	4,495	39Y42014	C:\User\LAB
<hr/>										
File Name	Content Type	URL	Last Accessed	Last Modified	Expiration Time	Last Checked	Hit	File Size	Subfolder Name	Full Path
19-HCWWH001.jpg	image/jpeg	https://th.bing.com/th?id=OIC.00SWG...	25-02-2023 10:36:42	N/A	26-03-2023 04:06:14	N/A	7	4,495	39Y42014	C:\User\LAB
<hr/>										
File Name	Content Type	URL	Last Accessed	Last Modified	Expiration Time	Last Checked	Hit	File Size	Subfolder Name	Full Path
19-HCWWH001.jpg	image/jpeg	https://th.bing.com/th?id=OIC.00SWG...	25-02-2023 10:36:42	N/A	26-03-2023 04:06:14	N/A	7	4,495	39Y42014	C:\User\LAB
<hr/>										
File Name	Content Type	URL	Last Accessed	Last Modified	Expiration Time	Last Checked	Hit	File Size	Subfolder Name	Full Path
19-HCWWH001.jpg	image/jpeg	https://th.bing.com/th?id=OIC.0								