University Of Mumbai
Institute of Distance & Open Learning

PRACTICAL JOURNAL IN PAPER-II

CYBER FORENSICS

SUBMITTED BY

DEVANG VIJAY DESHMUKH APPLICATION ID: 137062 SEAT NO: 0103557

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY PART-II

ACADEMIC YEAR 2021-2022

INSTITUTE OF DISTANCE AND OPEN LEARNING
IDOL BUILDING, VIDYANAGARI,
SANTACRUZ (EAST), MUMBAI-400 098

CONDUCTED AT
RIZVI COLLEGE OF ARTS, SCIENCE AND COMMERCE
BANDRA (W), MUMBAI 400050

University of Mumbai

Institute of Distance & Open Learning

Dr.Shankar Dayal Sharama Bhavan, Kalina,
Vidanagari, Santacruz (E), Mumbai-400 098.

Certificate

This is to certify that

Mr. **DEVANG VIJAY DESHMUKH** Application ID: **137062**, Seat No: **0103557** from Rizvi College of Arts, Science and Commerce Bandra(W), Mumbai 400050 has successfully completed all the practical of Paper **II** titled **CYBER FORENSICS** for M.sc (IT) Part II in the academic year 2021-2022.

Section I _____

Section II_____

_____ _____

MSc (IT) Co-ordinator, IDOL External Examiner

INDEX

PRACTICAL 1

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

- **Creating Forensic Image**
- **Check Integrity of Data**
- **Analyse Forensic Image**
-

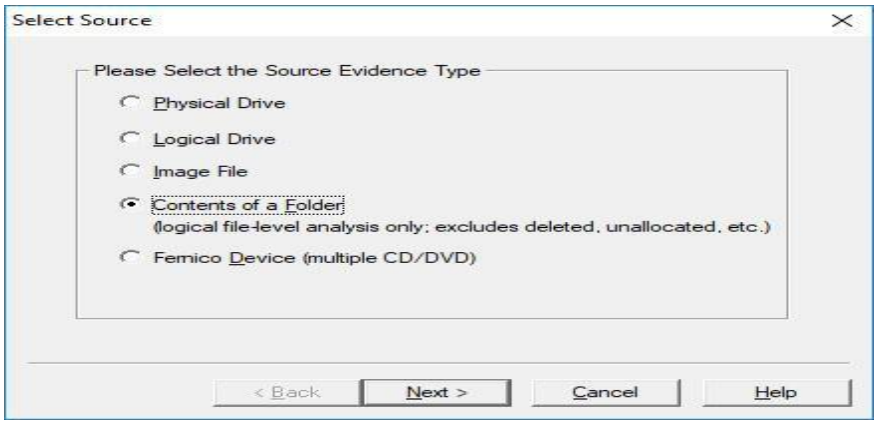
FTK Imager allows you to make several different types of forensic images. In addition, drive content and hash lists can be exported.

a) Creating Forensic Image

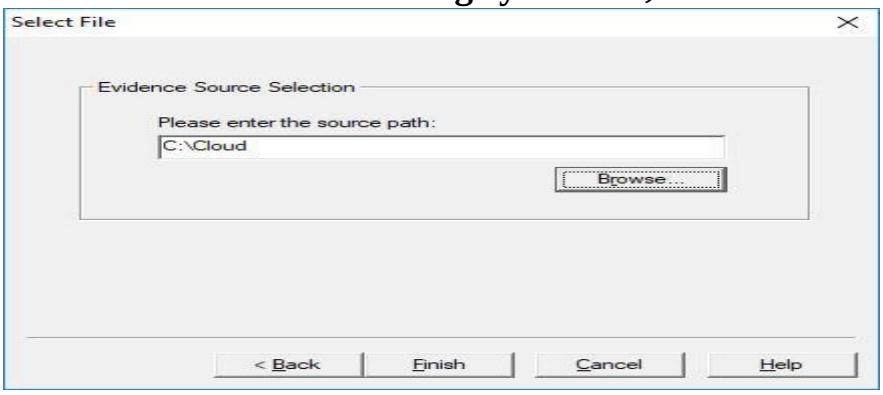
FTK Imager allows you to write an image file to a single destination or to simultaneously write multiple image files to multiple destinations using the same source data or drive.

To create a forensic image

1. **Click File > Create Disk Image.**
2. **In the Select Source dialog box, select the source you want to make an image of.**



3. **Click Next.**
4. **Click Yes**
5. **Browse to the source of the image you want, and then click Finish.**

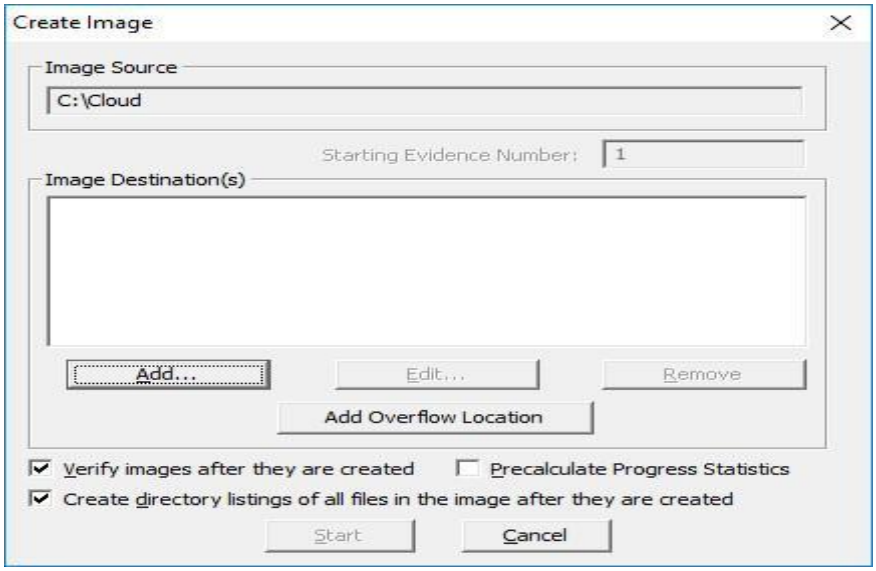


6. In the Create Image dialog,

6.a. Compare the stored hashes of your image content by checking the Verify images after they are created box. If a file doesn't have a hash, this option will generate one.

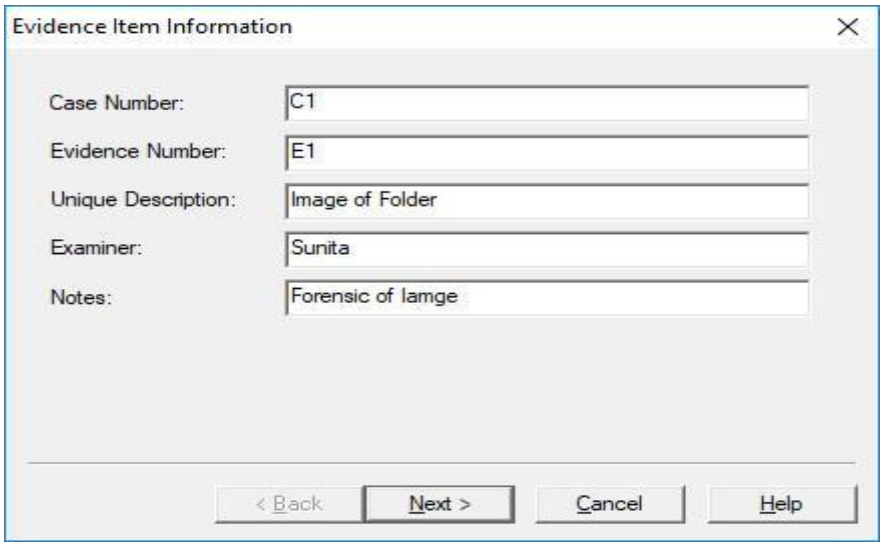
6.b. List the entire contents of your images with path, creation dates, whether files were deleted, and other metadata. The list is saved in tab-separated value (.CSV) format.

6.c. click Add.



7. Click Next.

8. Specify Evidence Item Information. All Evidence Item Information is optional, but it is helpful to have the information easily accessible in case it is called into question at any time after creation



9. Click Next.

10. In the Image Destination Folder field Click Browse to find and select the desired location.

11. In the Image Filename field, specify a name for the image file but do not specify a file extension

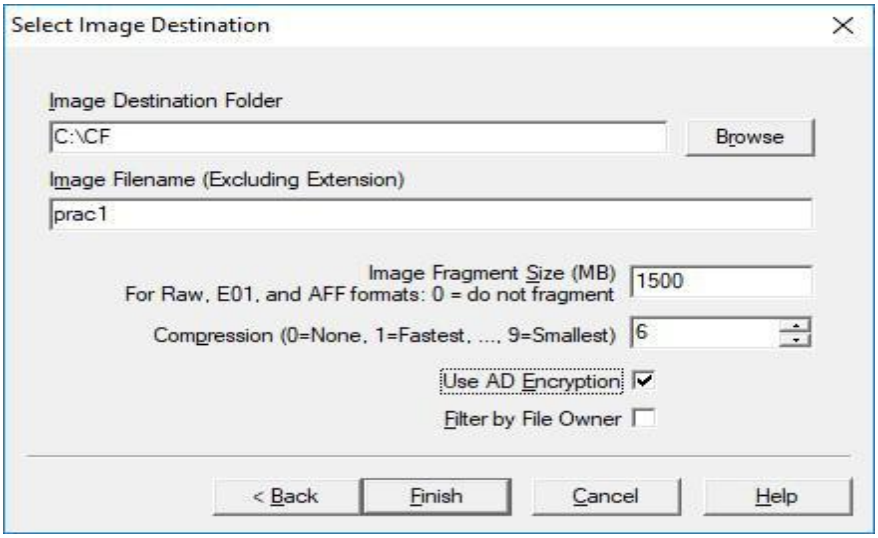
12.a.Specify the Image fragment Size:

Default Image Fragment Size = 1500 MB
The S01 format is limited by design to sizes between 1 MB and 2047 MB (2 GB). Compressed block pointers are 31- bit numbers (the high bit is a compressed flag), which limits the size of any one segment to two gigabytes.

12.b. Select the compression level to use.

0=No Compression
1=Fastest, Least Compression (faster, and also slightly smaller than a 0-compression file)
9=Slowest, Most Compression (smallest file, slowest to create).
Numbers between 1 and 9 produce an image with varying levels of compression to speed ratio.

13. To encrypt the new image with AD Encryption, mark the Use AD Encryption box.

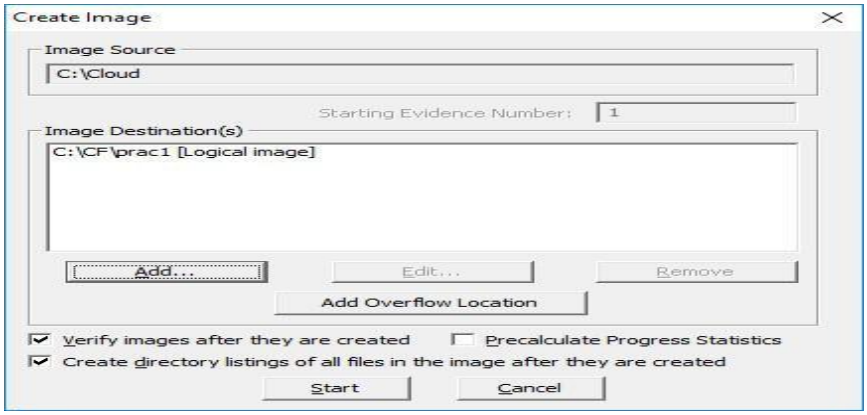


14. When AD Encryption is selected, you can choose between encrypting with a password, or encrypting with a certificate.

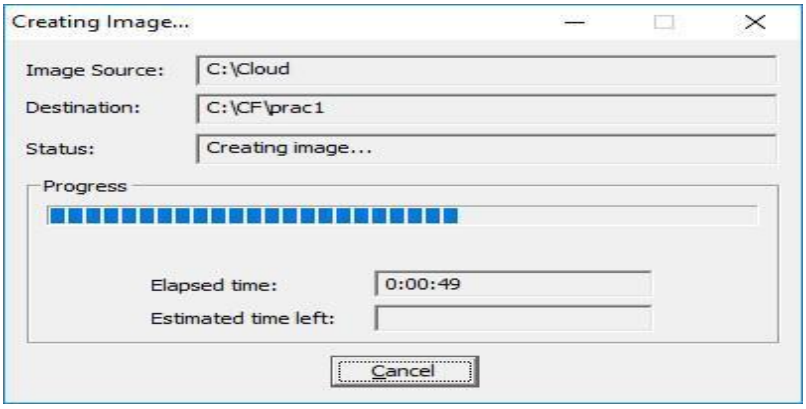
15. When encryption selections are made, click OK to save selections and return to the Create Image dialog.

16. To add another image destination (i.e., a different saved location or image file type), click Add, and repeat steps

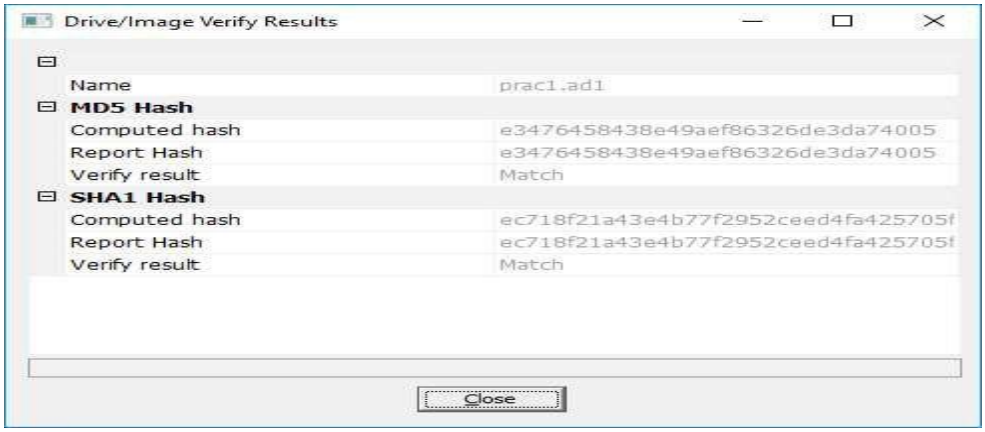
17. **Click Start to begin the imaging process.**



18. A progress dialog appears that shows the following

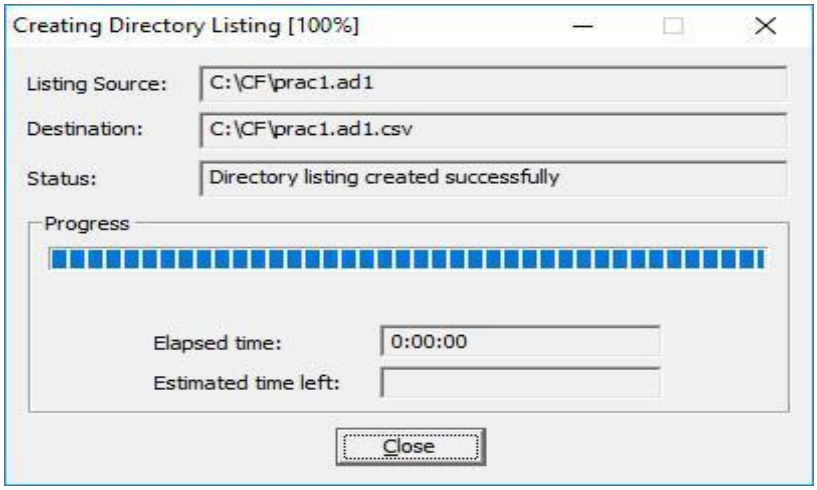


19. After the images are successfully created, the Drive/Image Verify Results box shows detailed image information, including MD5 and SHA1 check sums, and bad sectors.

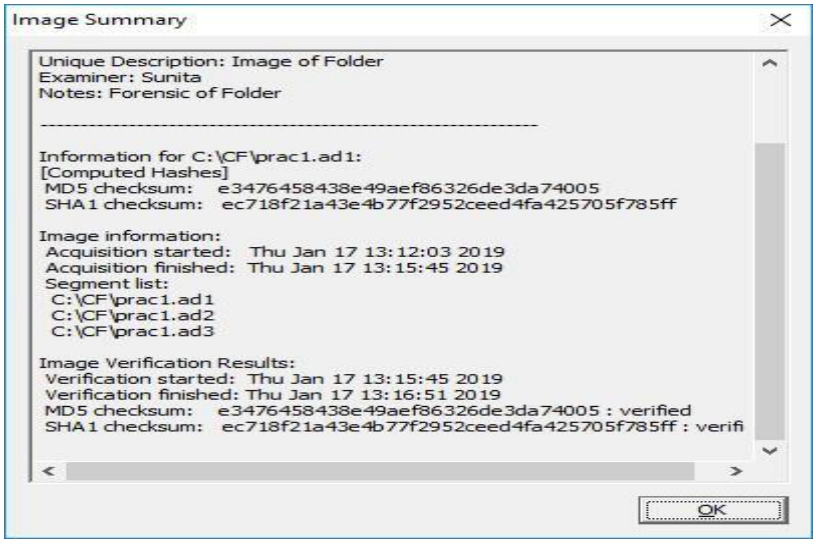


20. Click on Close to close the Drive/Image Verify Results box

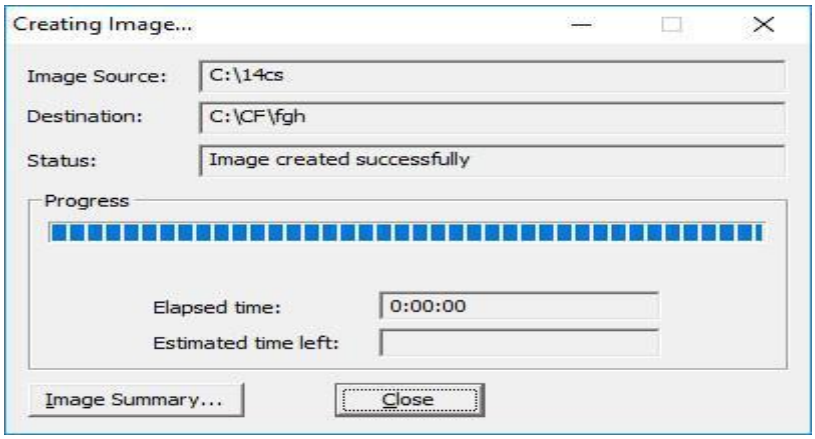
21. Click on Close to close the Creating Directory Listing dialog



22. Click Image Summary to close the Image Summary. The Image Summary also includes the data you entered in the Evidence Item Information dialog.



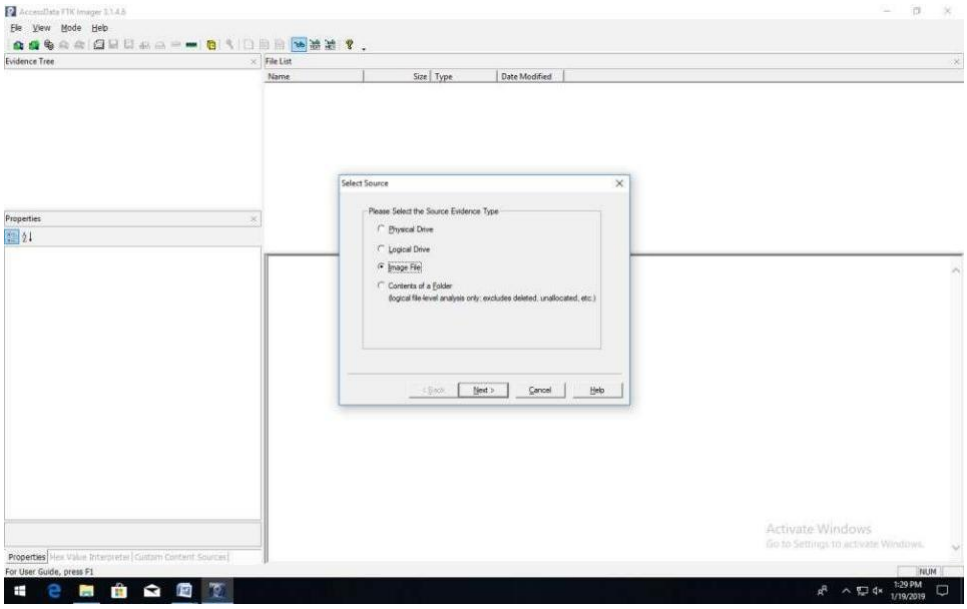
23. Click Close to exit back to Imager.



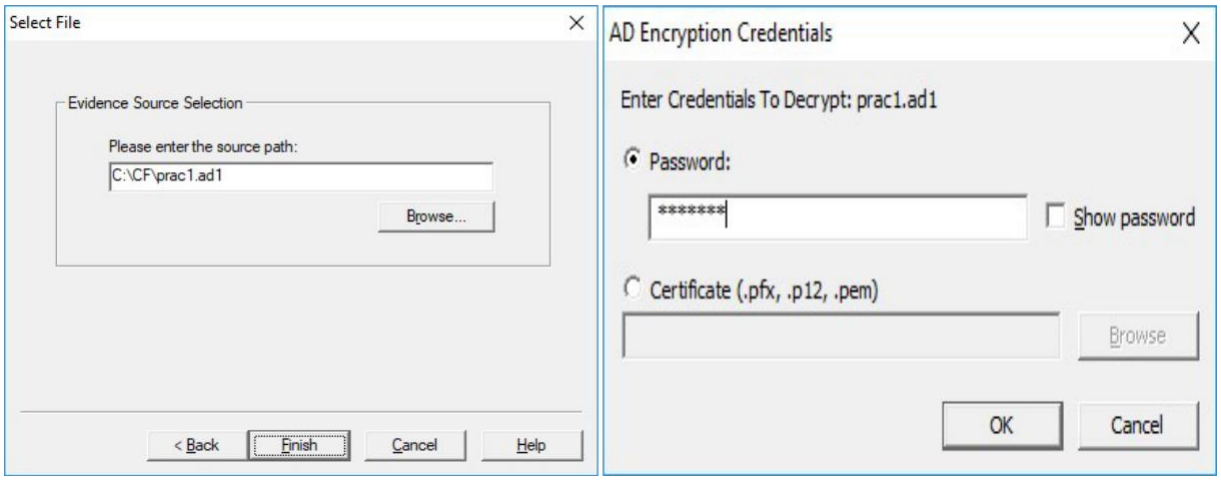
b) Check Integrity of Data

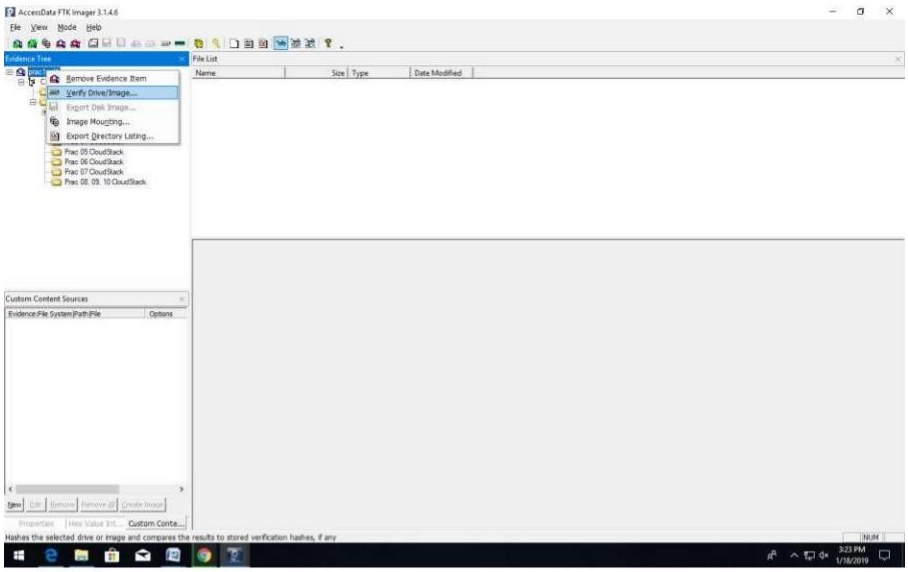
Hashing is the process of generating a unique value based on a file's contents. This value can then be used to prove that a copy of a file has not been altered in any way from the original file. It is computationally infeasible for an altered file to generate the same hash number as the original version of that file. The Export File Hash List feature in FTK Imager uses the MD5 and SHA1 hash algorithms to generate hash numbers for files.

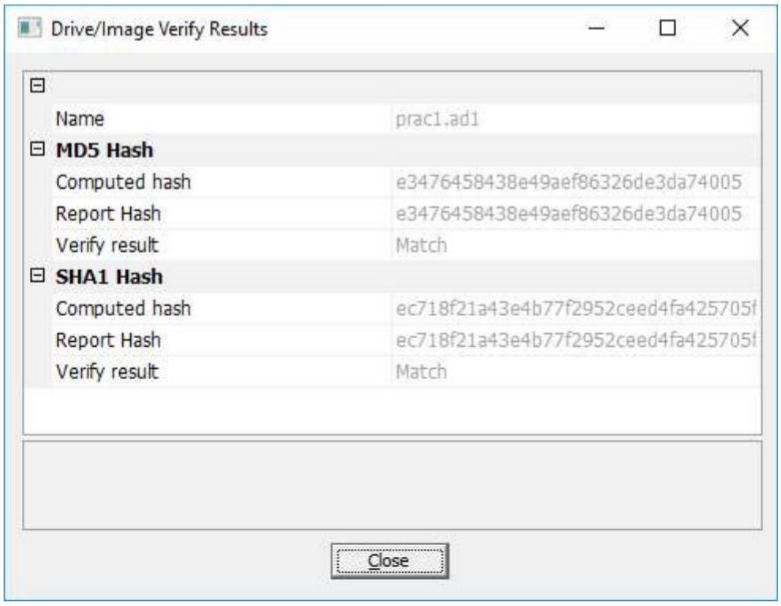
Go to File->Add Evidence Item..->Select Option as Image File



Browse your image file->Click on Finish button-> enter password and Click on Ok button





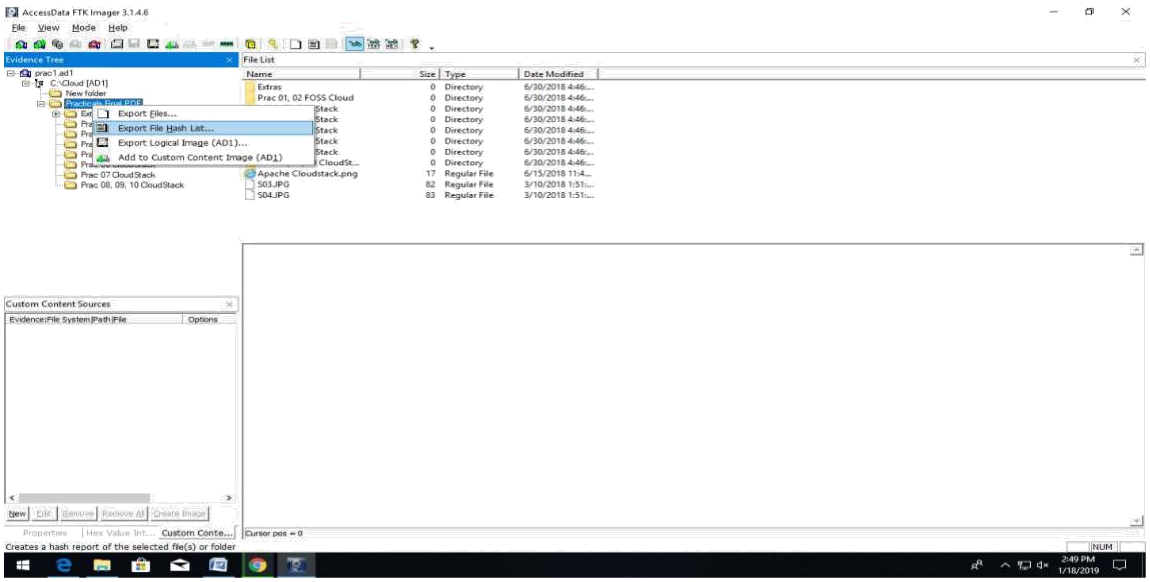


To generate and export hash values to a list

1. In the Evidence Tree, select the folder that contains the objects you want to hash. The object's contents are displayed in the File List.

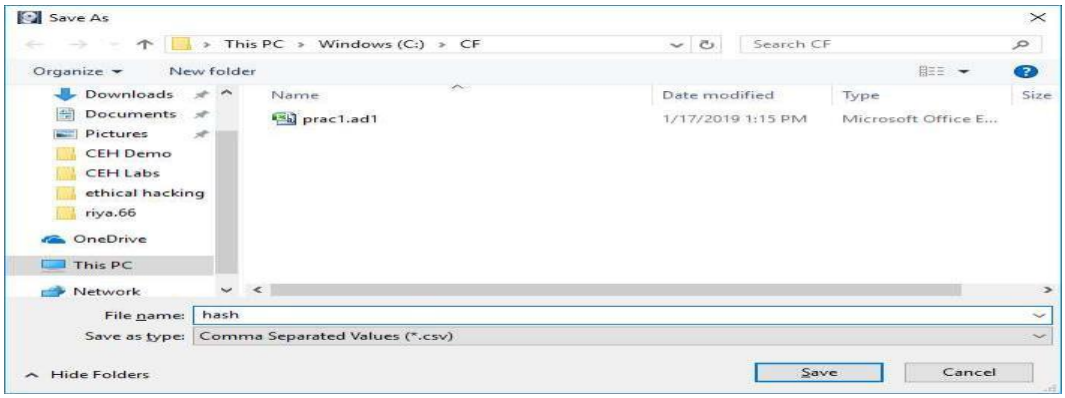
2. In the File List, select the folders or files you want to hash. If you select a folder, all the files contained in the folder and its sub folders are hashed.

3. Click File > Export File Hash List

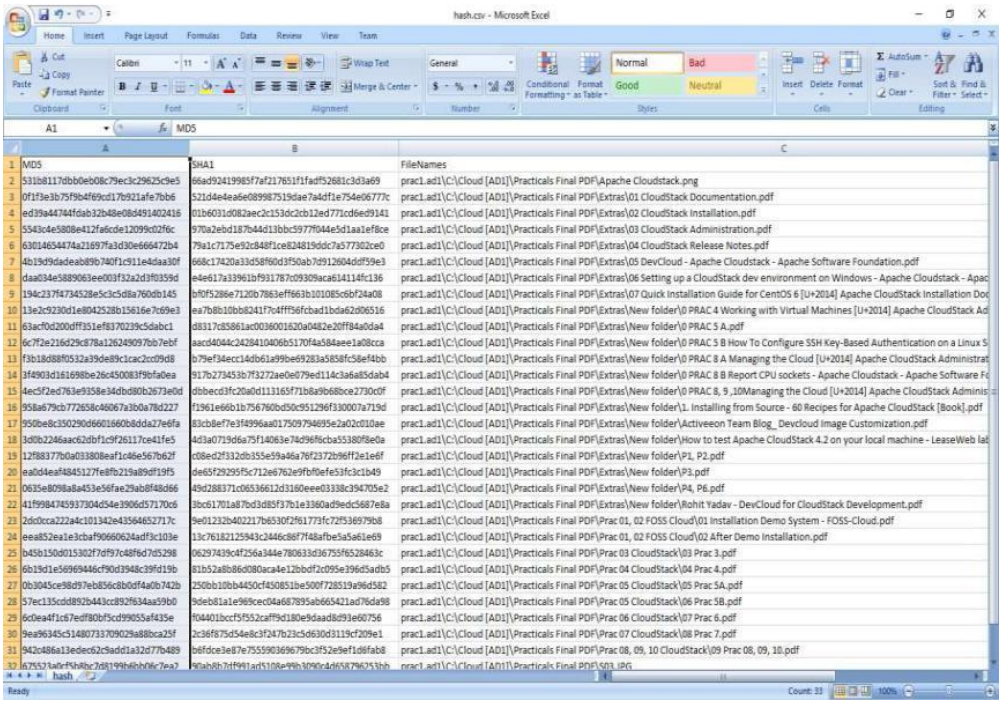


4. In the Save As dialog, type a name for the file hash list in the File Name field.

5. Click Save.



The hash list is saved as a file of comma-separated values (*.CSV).



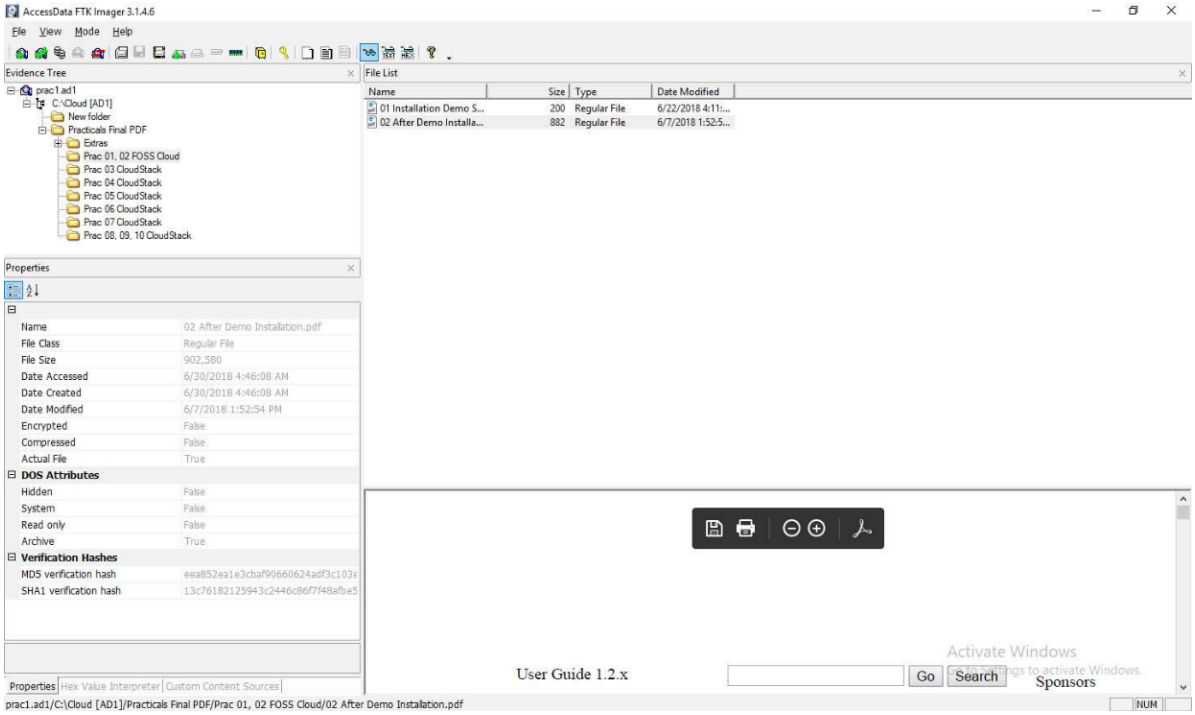
c) Analyze Forensic Image

a. Open Image using Add Evidence Item Option.

b. Select any folder from Evidence Tree.

c. Files will be displayed in File List

d. Select any File and you can view Properties of file in Properties Box



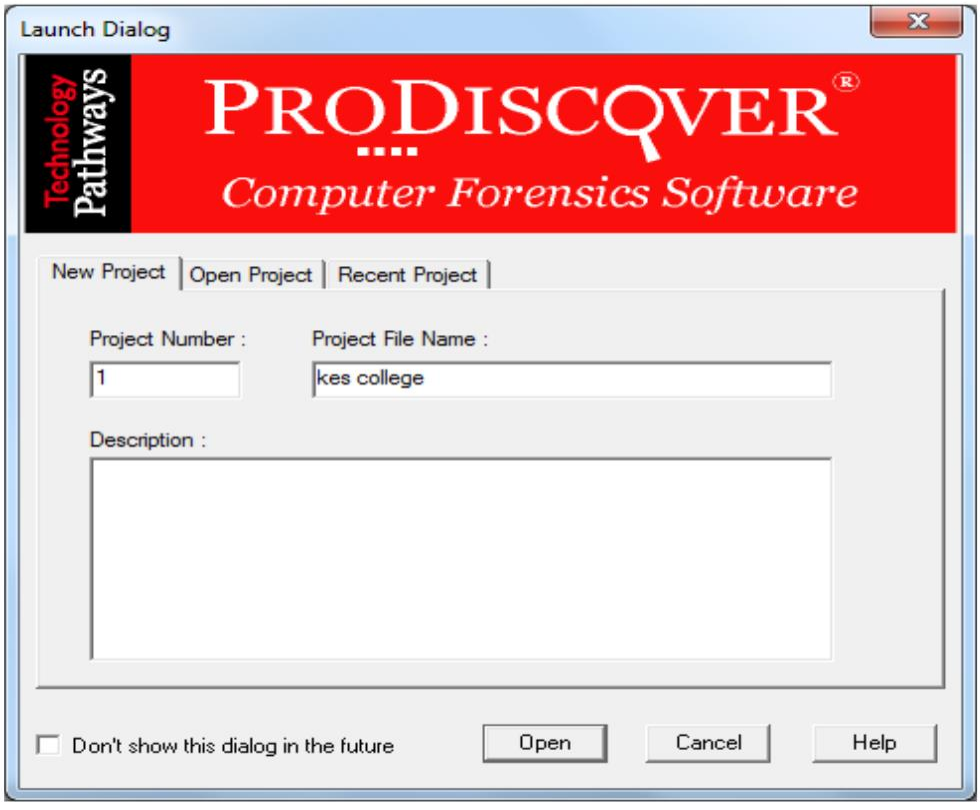
PRACTICAL 2

Aim: Creating an Image of content of folder from system

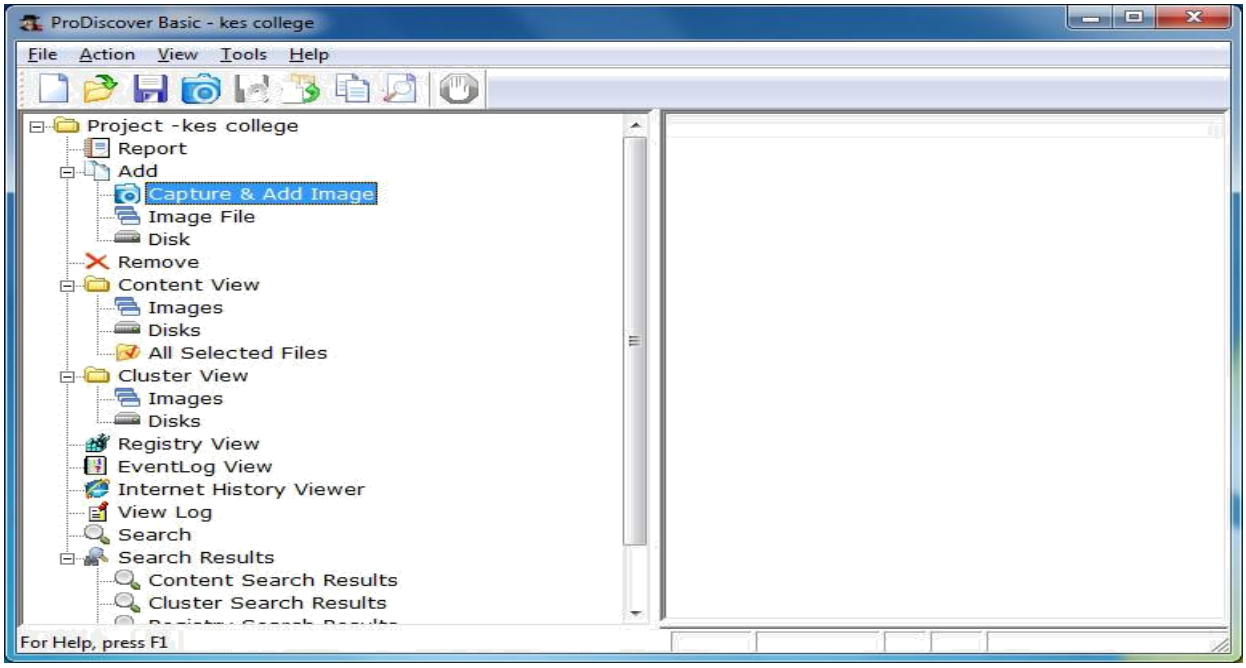
Data Acquisition:
Perform data acquisition using:
USB Write Blocker + FTK Imager

Steps:

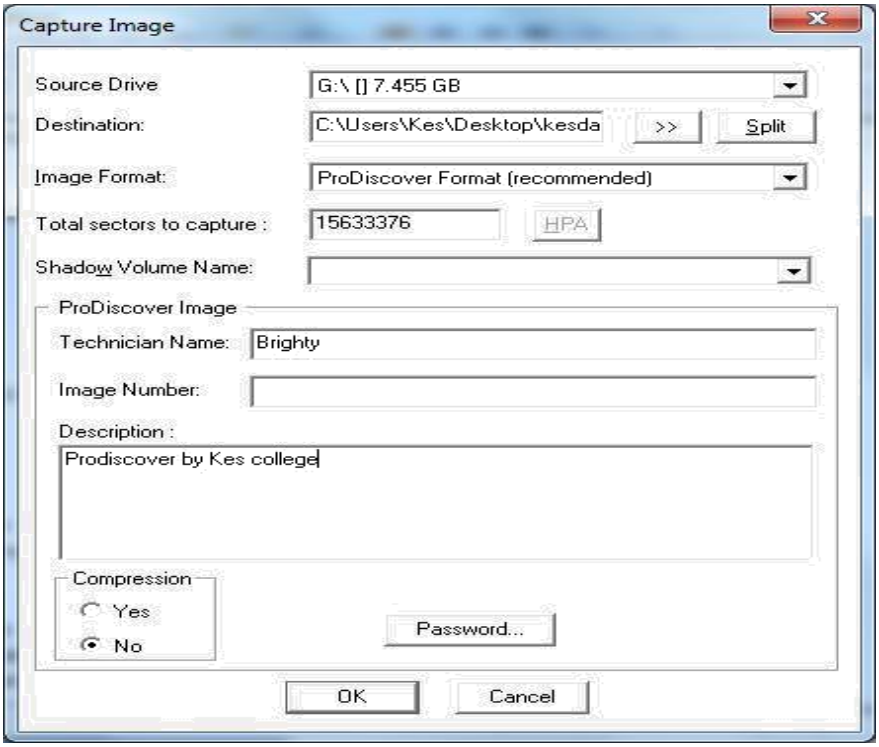
Step 1: First Open Prodiscover Basic and start with new case.



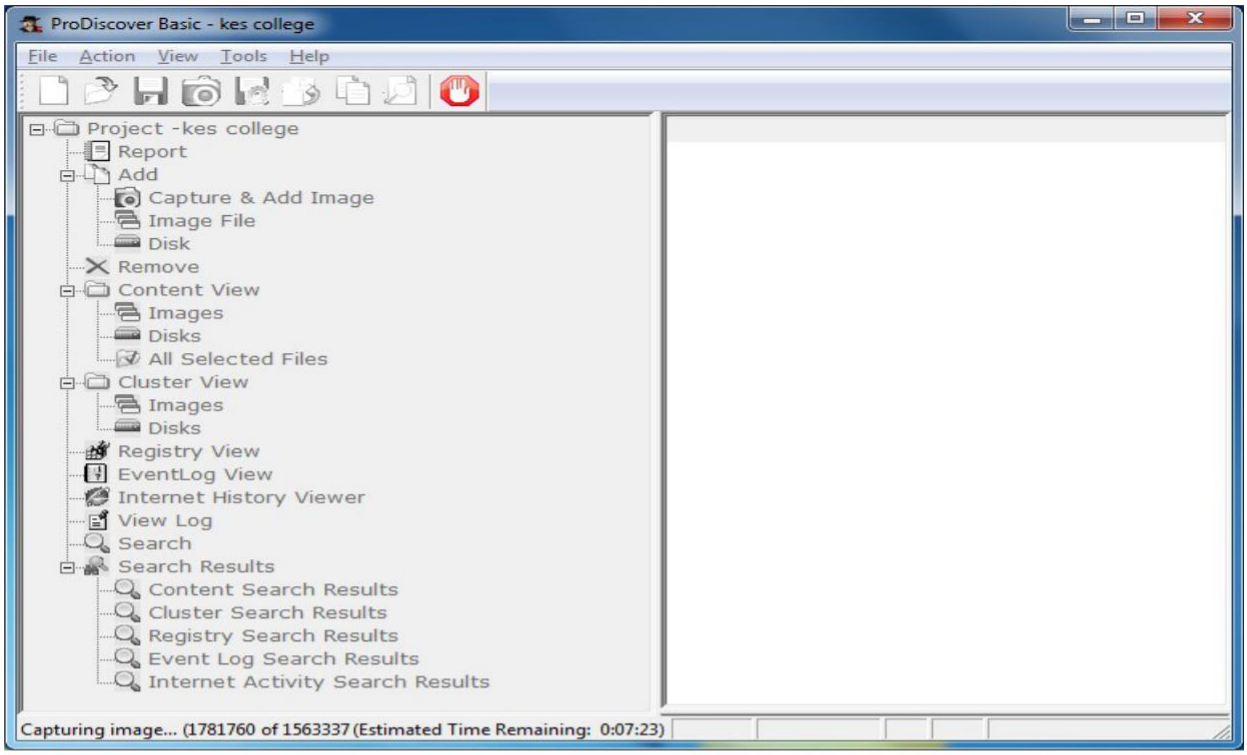
Step 2: The created project appears in left pane and select add>capture & add image.

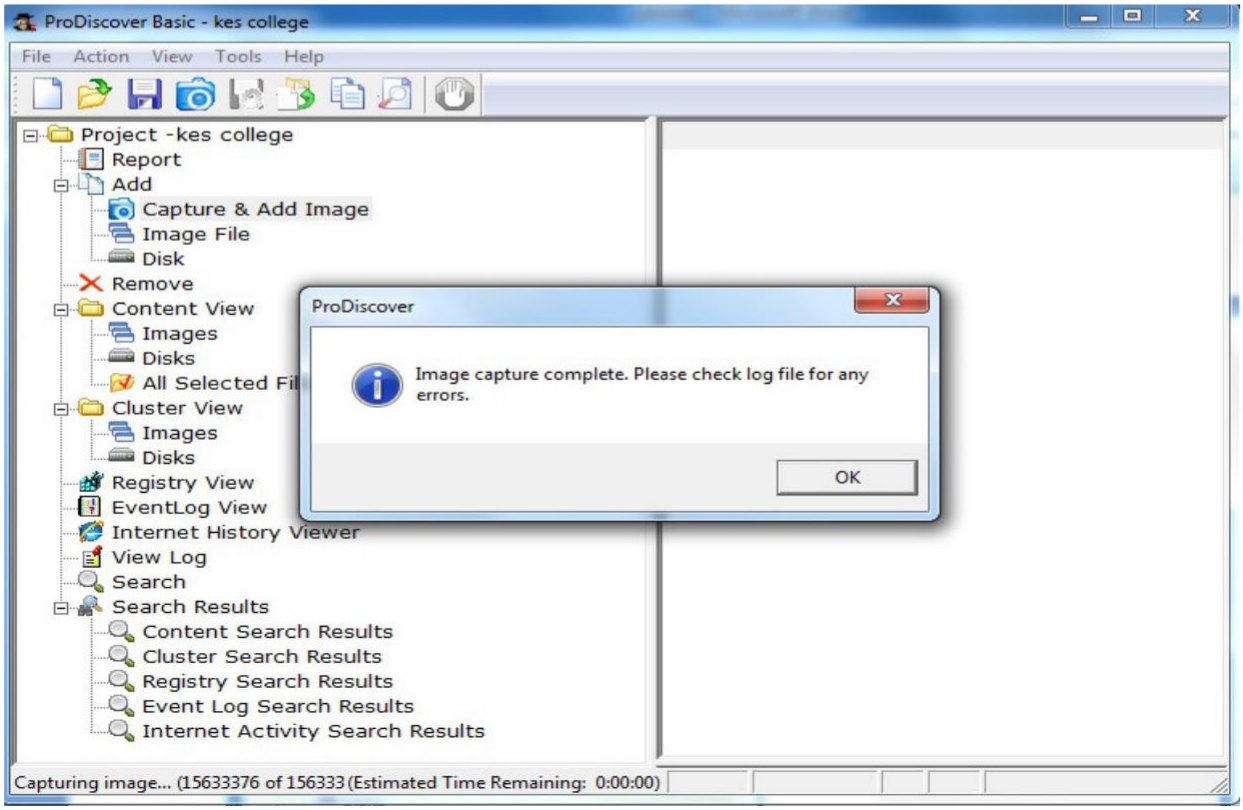


Step 3: fill the details as below. And click ok.

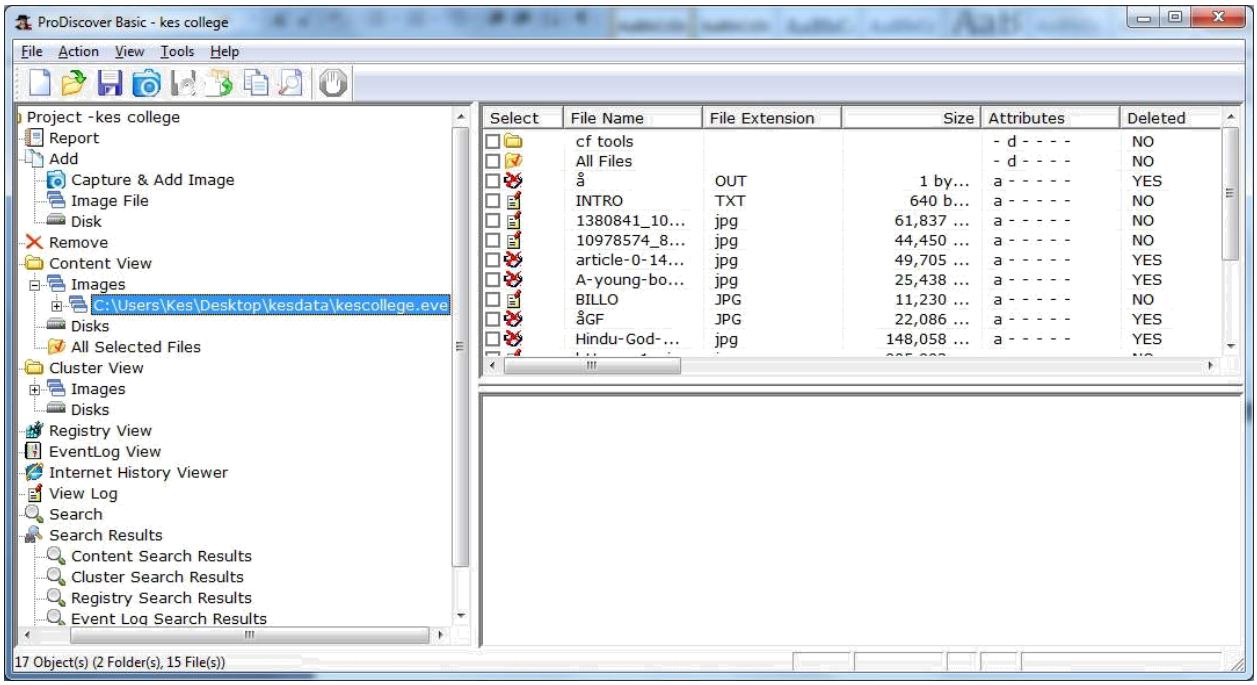


Step 4: capturing of image starts.

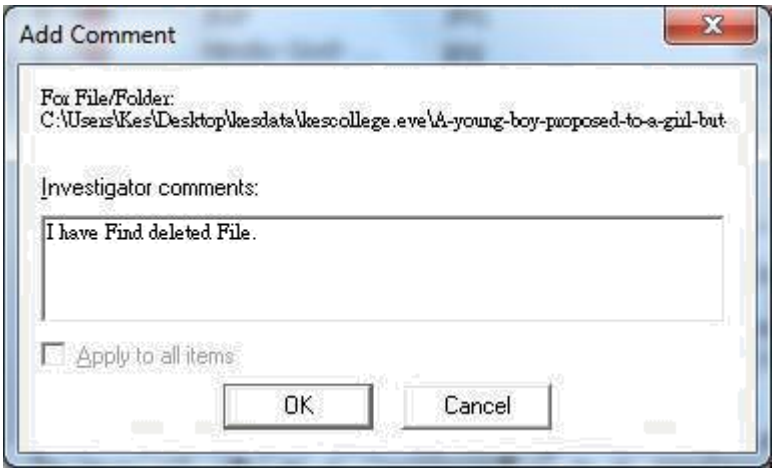




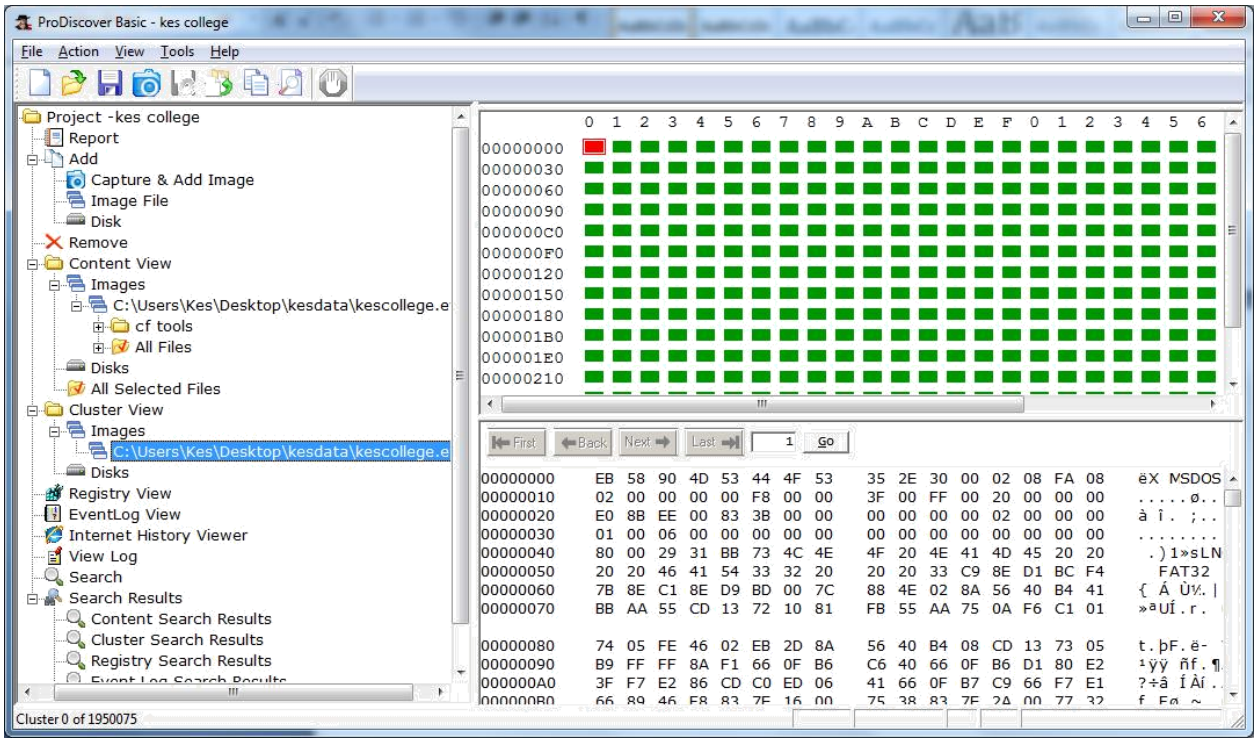
Step 5: Open the image created, go to Add > Images in left pane.



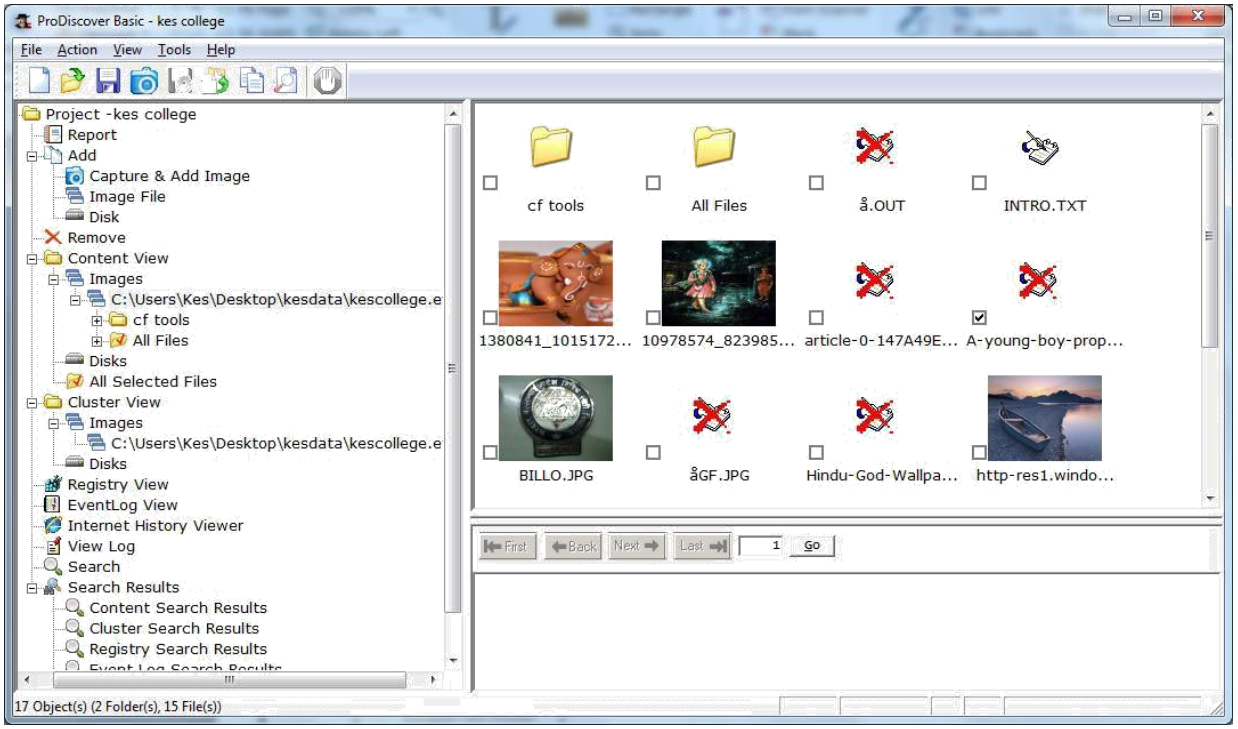
Step 6: Click on any File and type a comment.



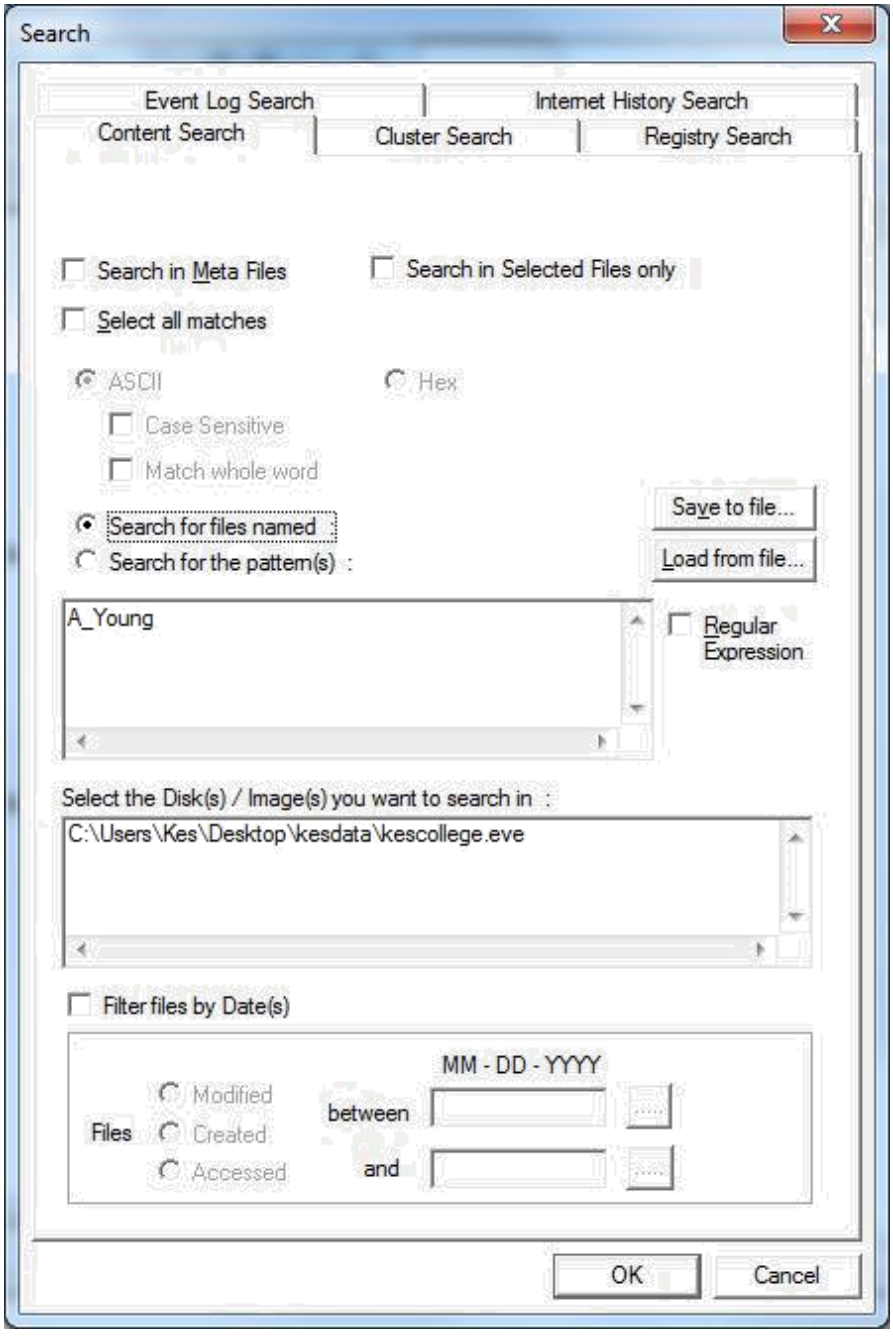
Step 7 : the cluster view is seen from the cluster view in left panel.



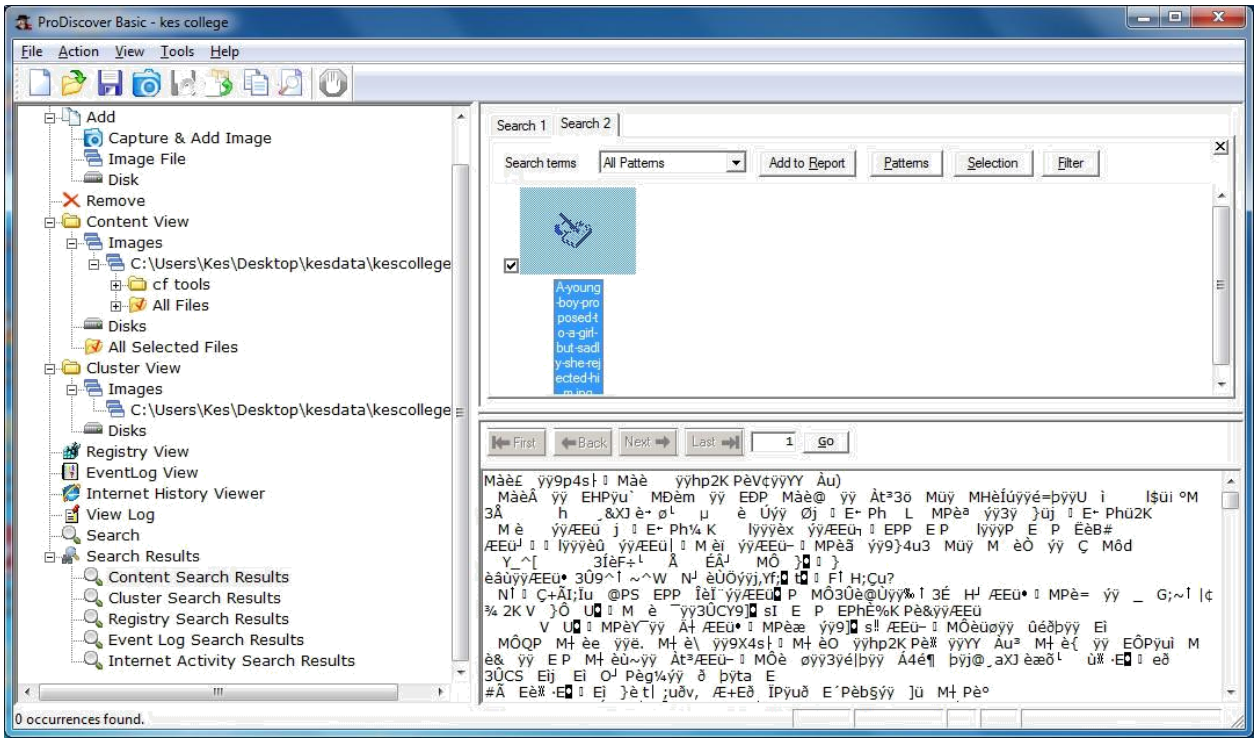
Step 8 : We can also view gallery view by Right Click.



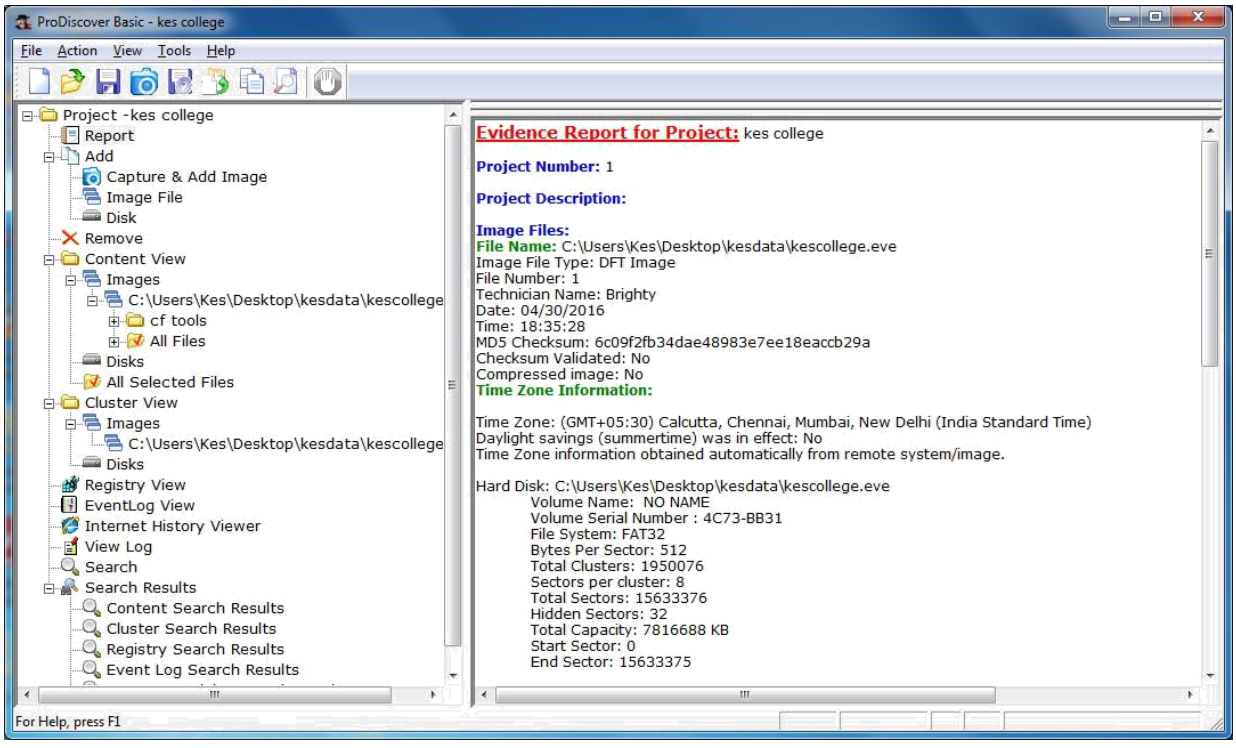
Step 9: Keyword search. Click on Search in left pane and Enter the file name to be searched in the image created.

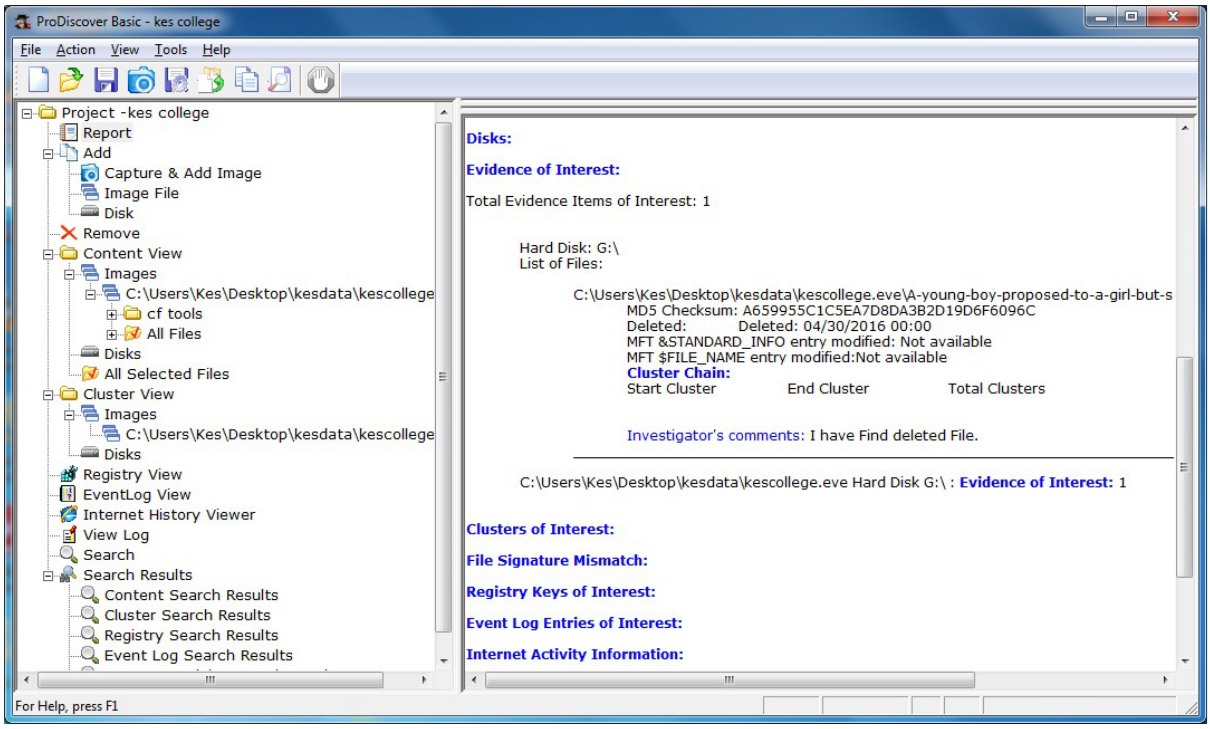


Step 10 : Output of Keyword search.



Step 11 : Click on View>Report.




ProDiscover Basic - kes college
File Action View Tools Help
Project -kes college
Report
Add
Capture & Add Image
Image File
Disk
Remove
Content View
Images
C:\Users\Kes\Desktop\kesdata\kescollege
cf tools
All Files
Disks
All Selected Files
Cluster View
Images
C:\Users\Kes\Desktop\kesdata\kescollege
Disks
Registry View
EventLog View
Internet History Viewer
View Log
Search
Search Results
Content Search Results
Cluster Search Results
Registry Search Results
Event Log Search Results
Disks:
Evidence of Interest:
Total Evidence Items of Interest: 1
Hard Disk: G:\
List of Files:
C:\Users\Kes\Desktop\kesdata\kescollege.eve\A-young-boy-proposed-to-a-girl-but-s
MD5 Checksum: A659955C1C5EA7D8DA3B2D19D6F6096C
Deleted: Deleted: 04/30/2016 00:00
MFT &STANDARD_INFO entry modified: Not available
MFT $FILE_NAME entry modified:Not available
Cluster Chain:
Start Cluster End Cluster Total Clusters
Investigator's comments: I have Find deleted File.
C:\Users\Kes\Desktop\kesdata\kescollege.eve Hard Disk G:\ : Evidence of Interest: 1
Clusters of Interest:
File Signature Mismatch:
Registry Keys of Interest:
Event Log Entries of Interest:
Internet Activity Information:
For Help, press F1

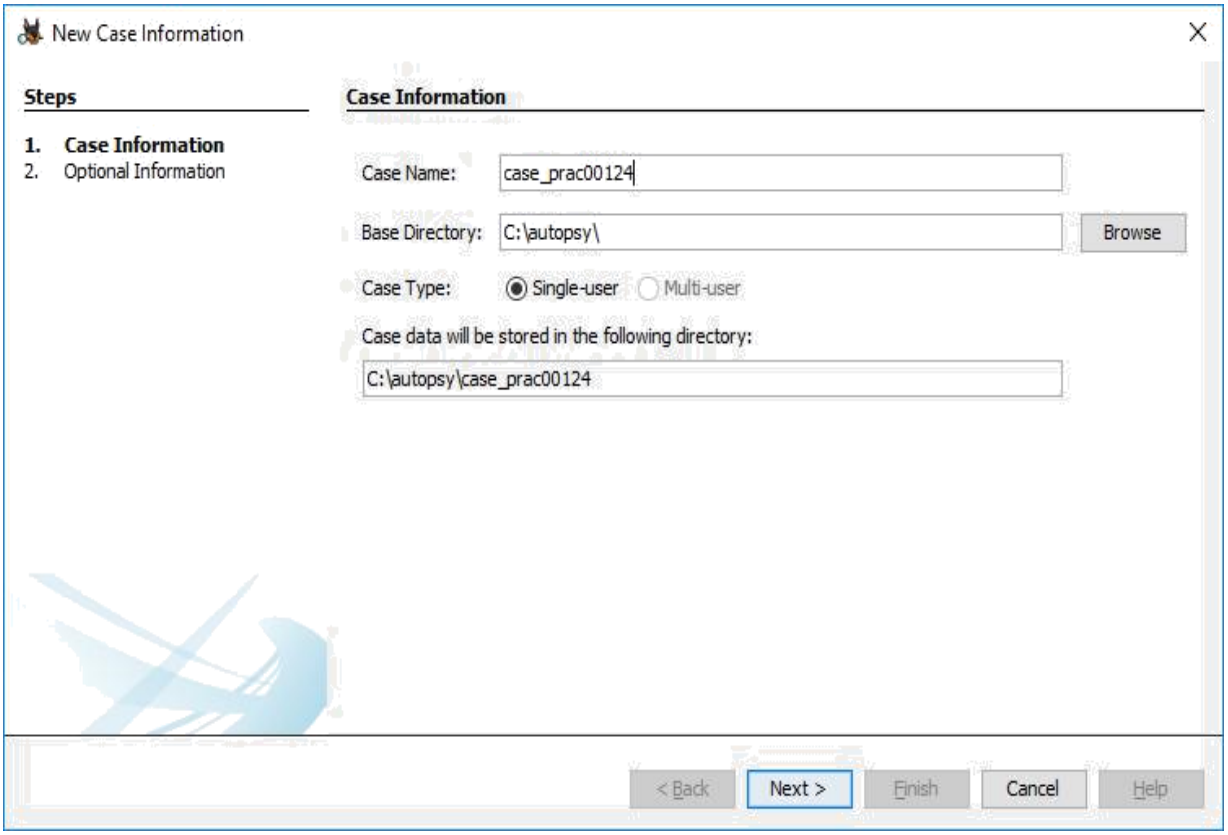
PRACTICAL 3

AIM: - Solve the Case study (image file) provide in lab using Encase Investigator or Autopsy.

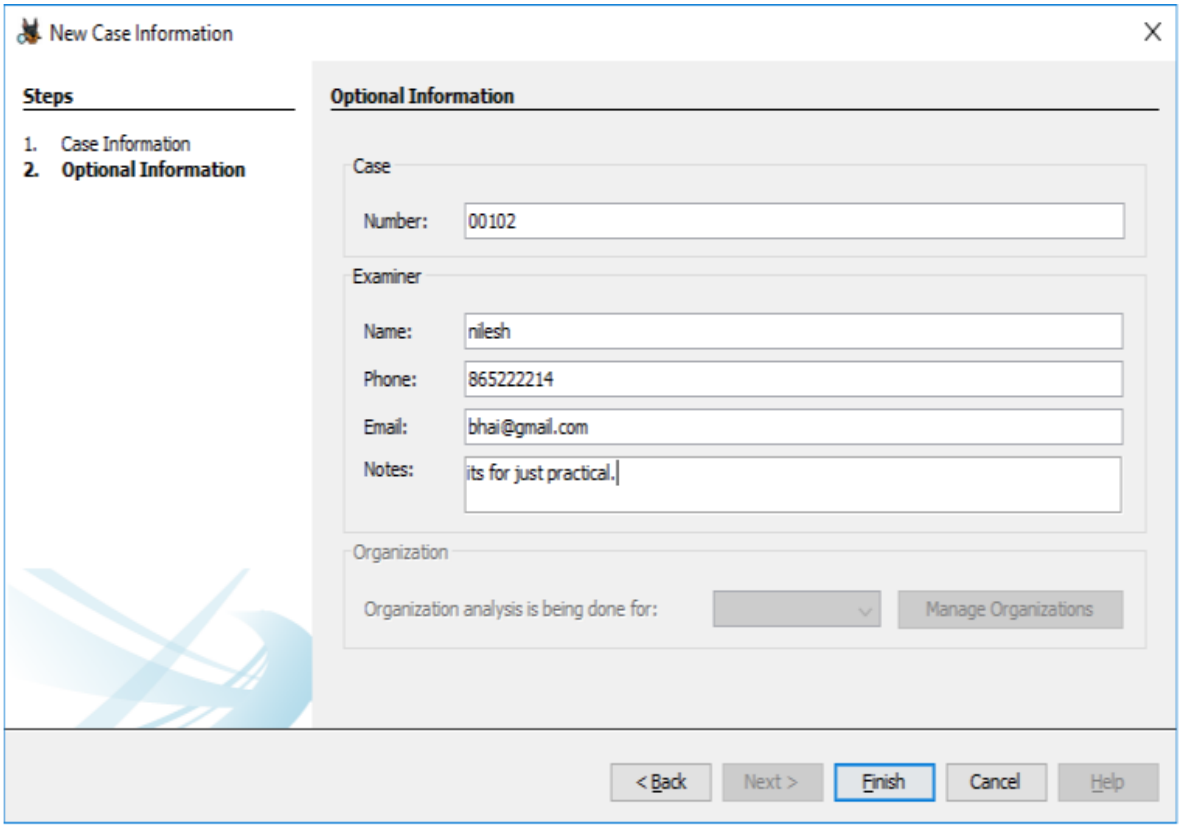
Step 1: Open Autopsy

Step 2 : Click on new case

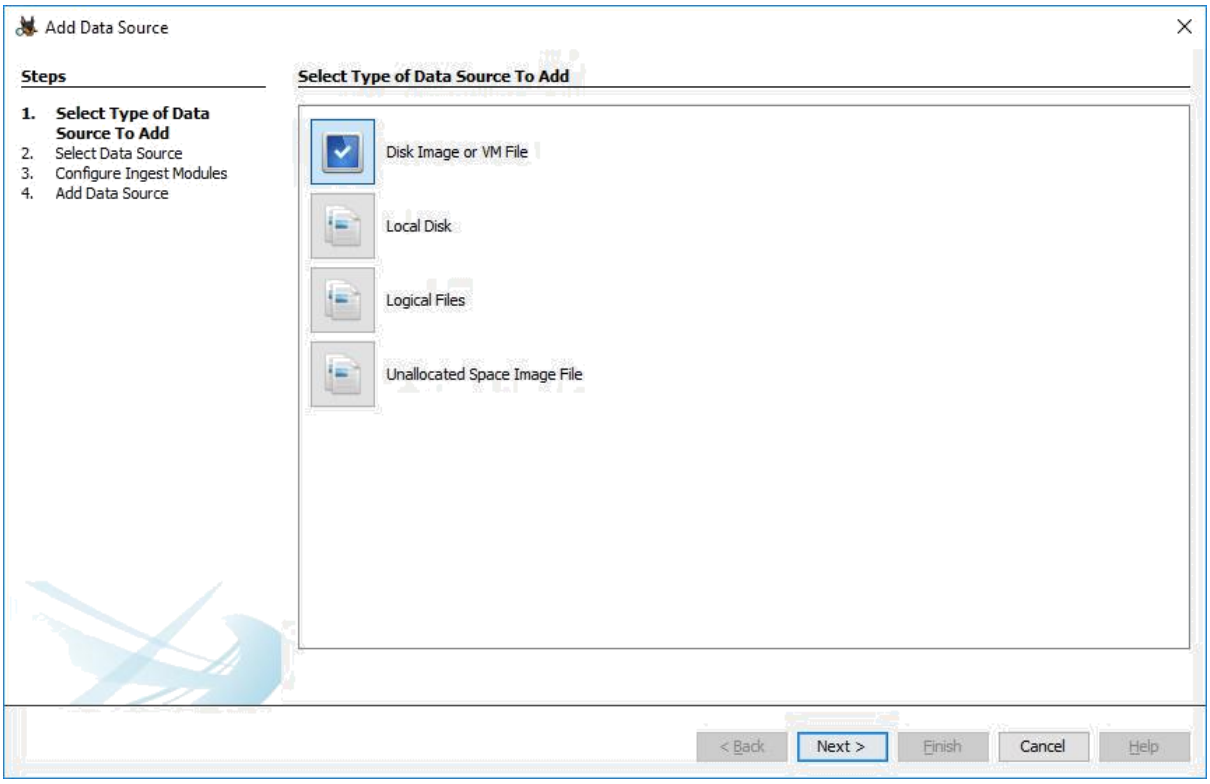
Step 3 : Enter details regarding the case and click on next button.



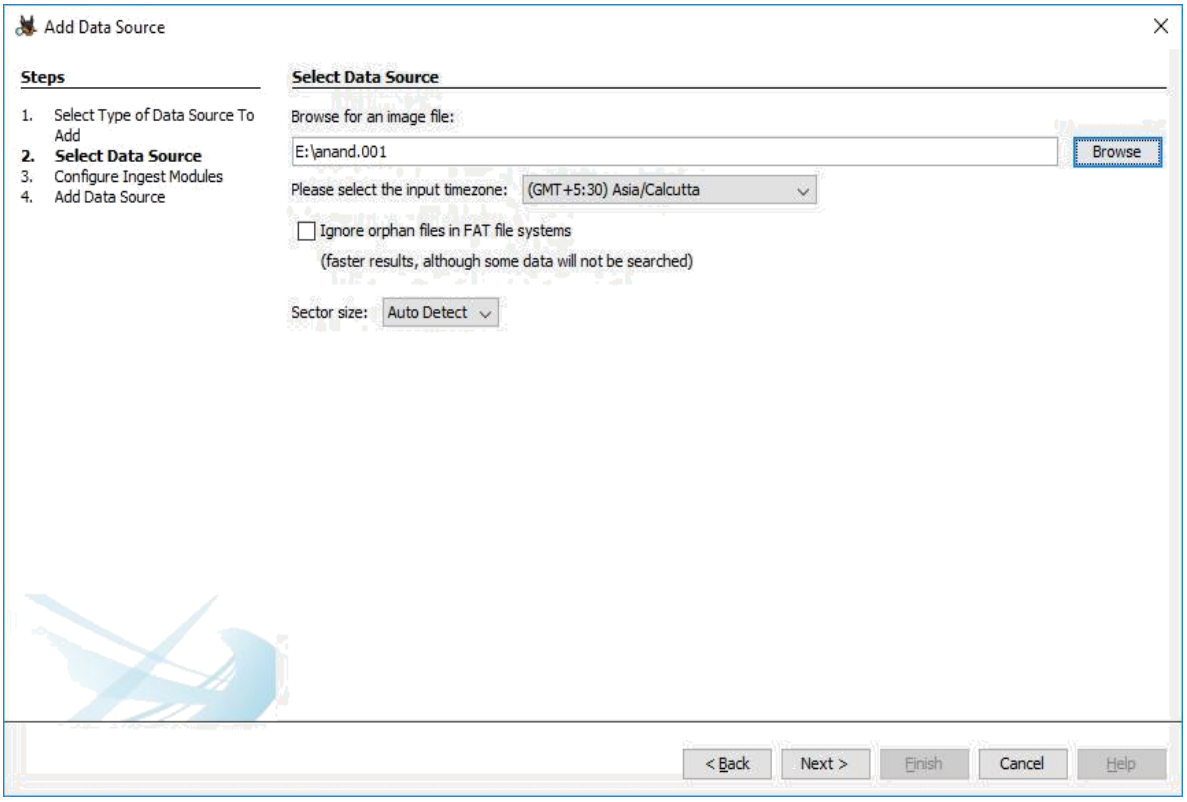
Step 4 : Enter further details and click on next button



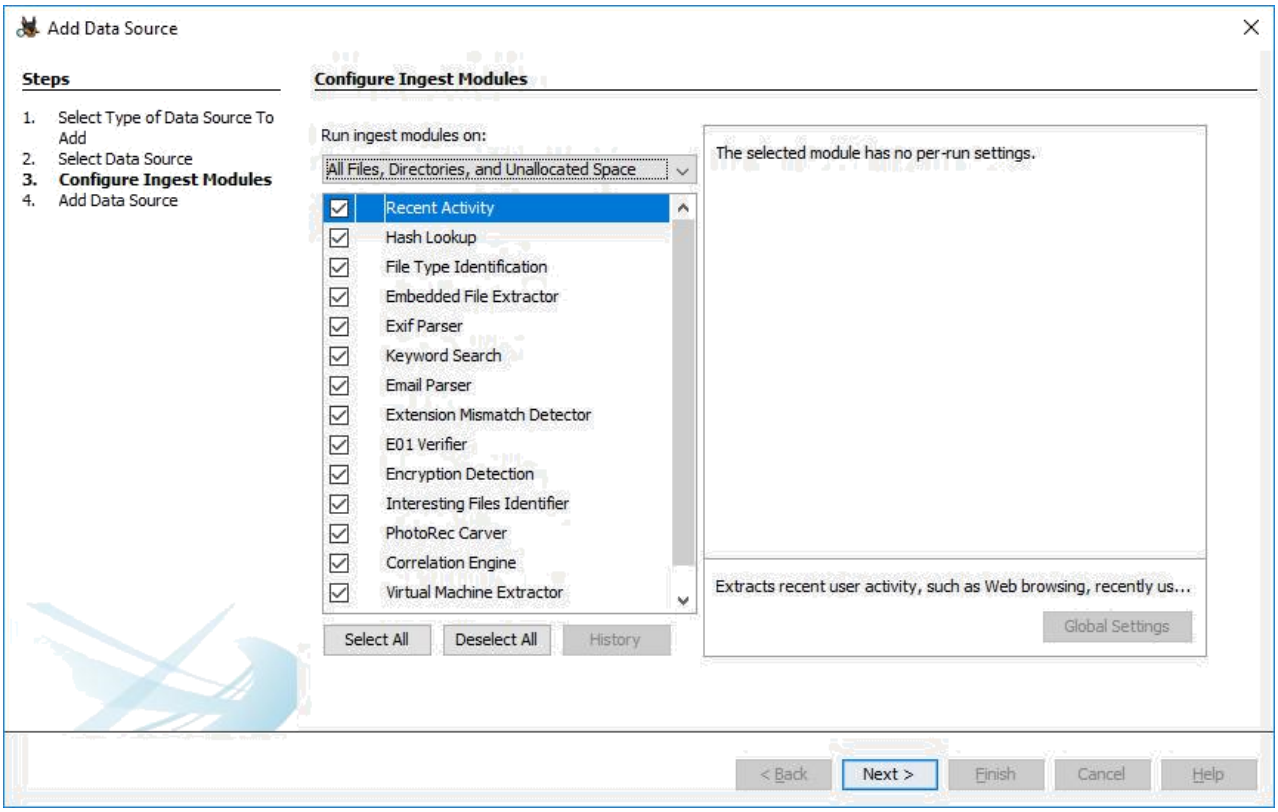
Step 5 : Now here we have to select Type of data source to add , in our case disk image or VM file and click on next



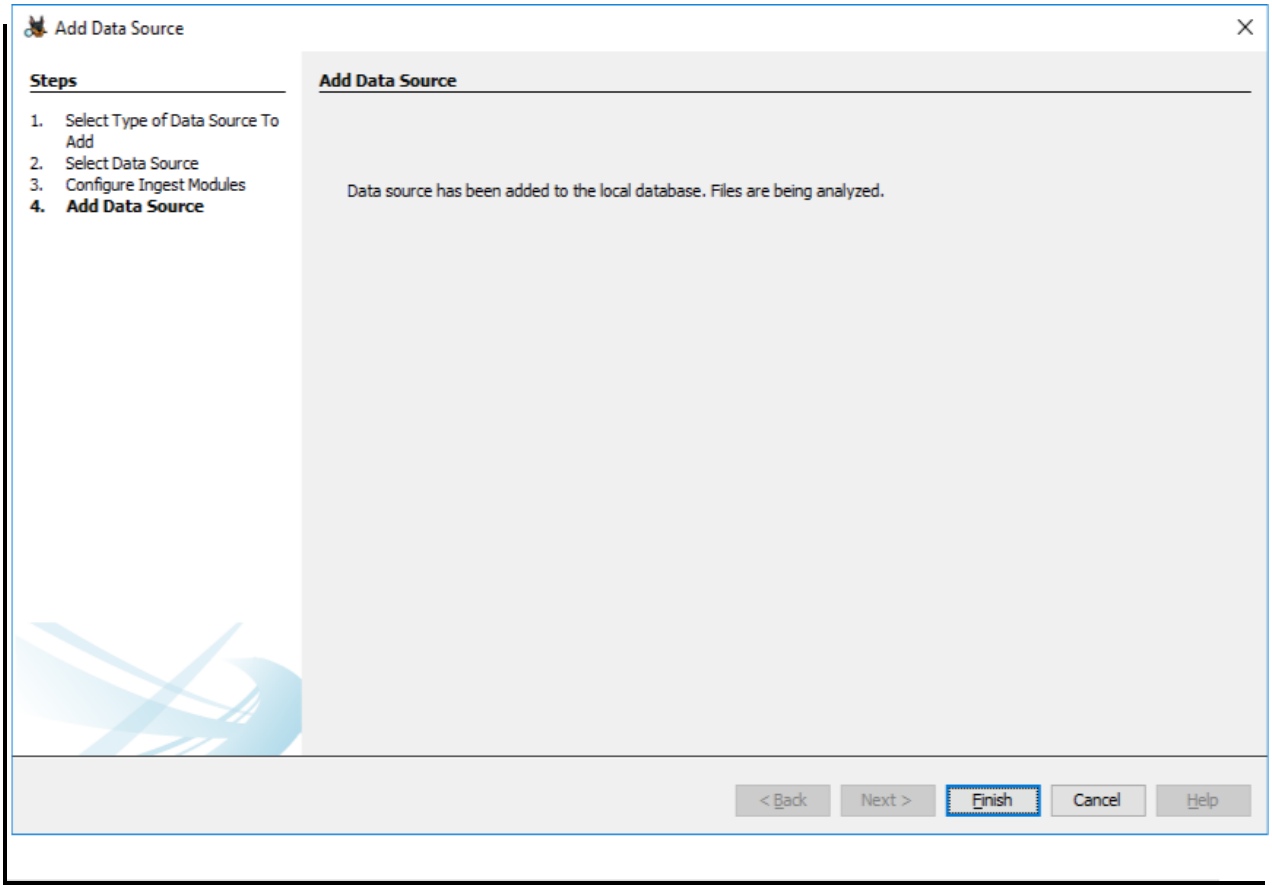
Step 6 : Now we have to select image file and click on next button



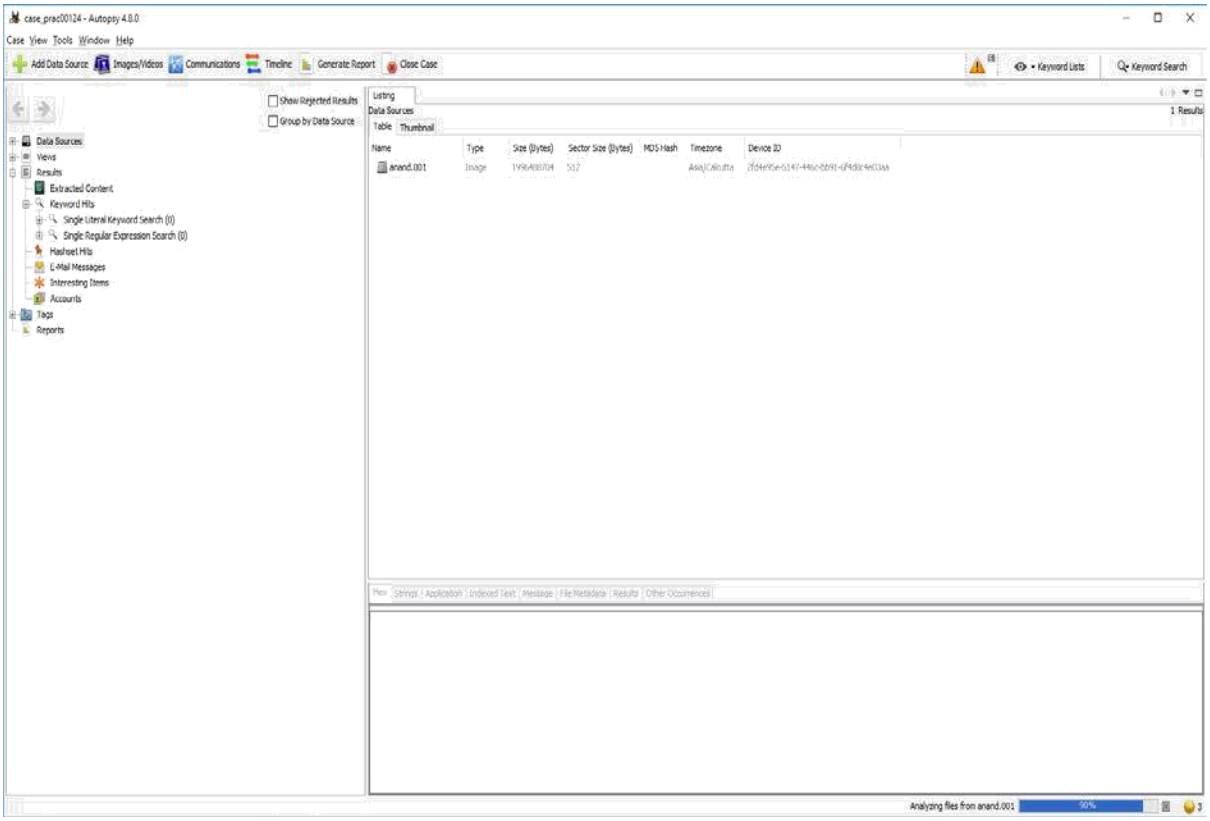
Step 7 : Now click on select all in order to Run ingest modules on: and click on next.



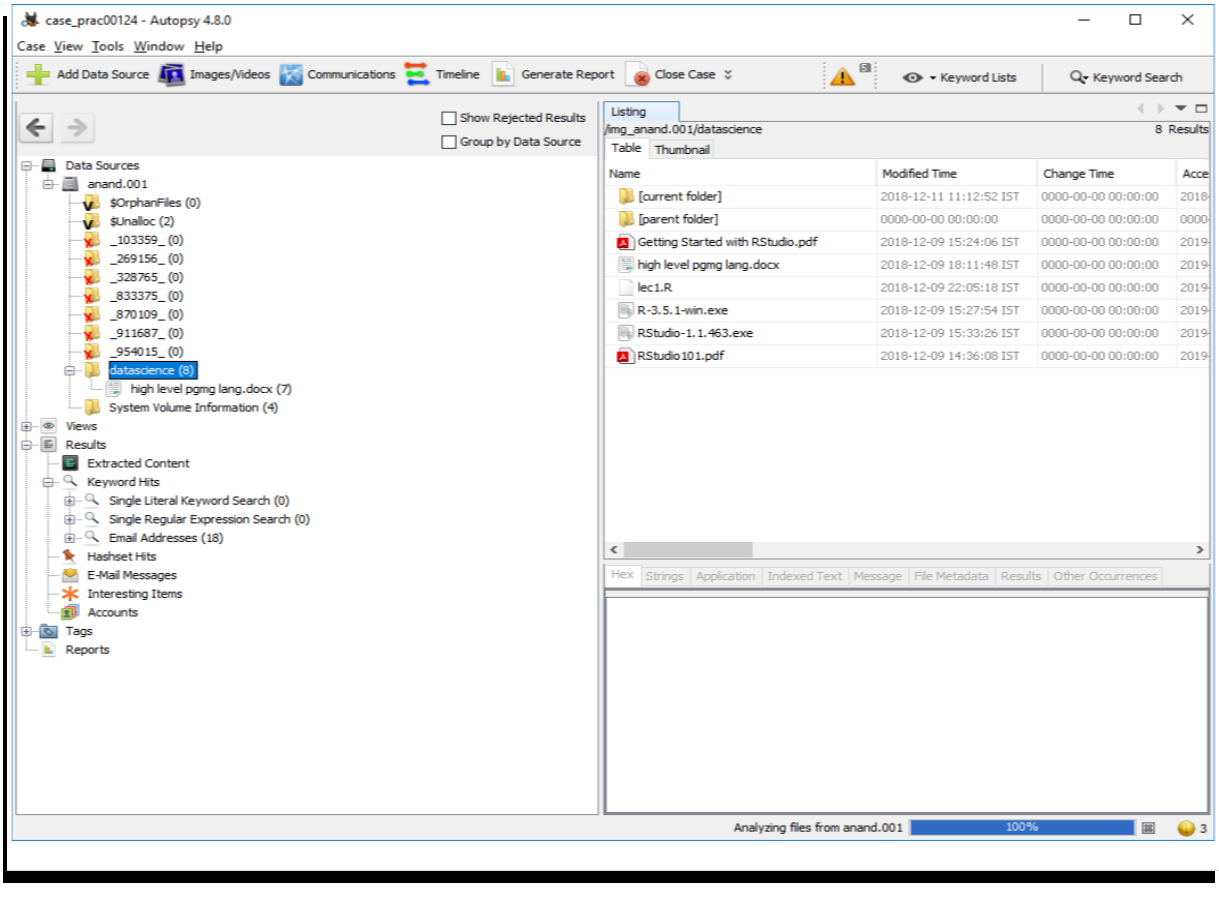
Step 8 : Now click on finish



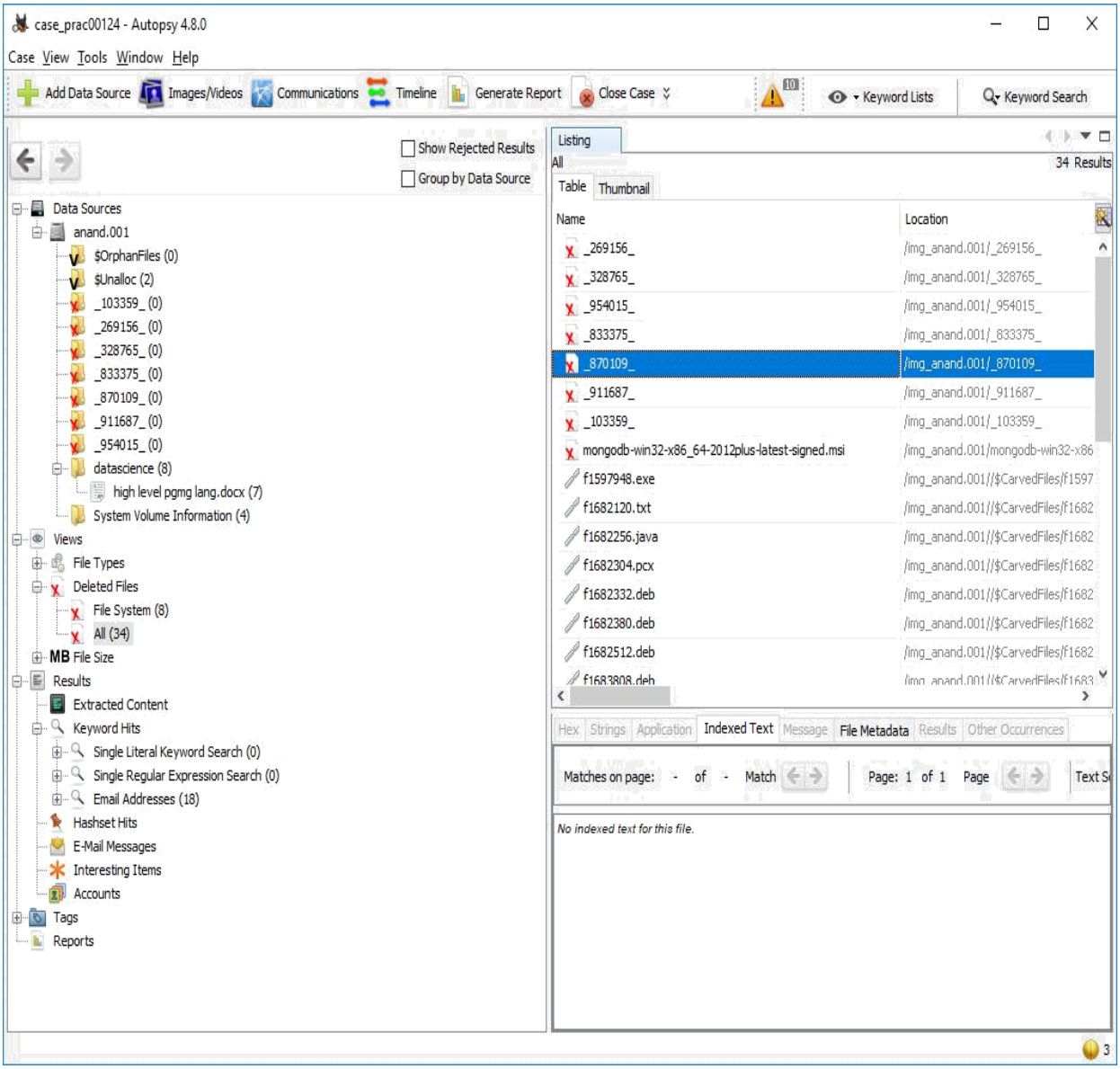
Step 9 : Now Autopsy window will appear and it will analyse the disk that we have selected .



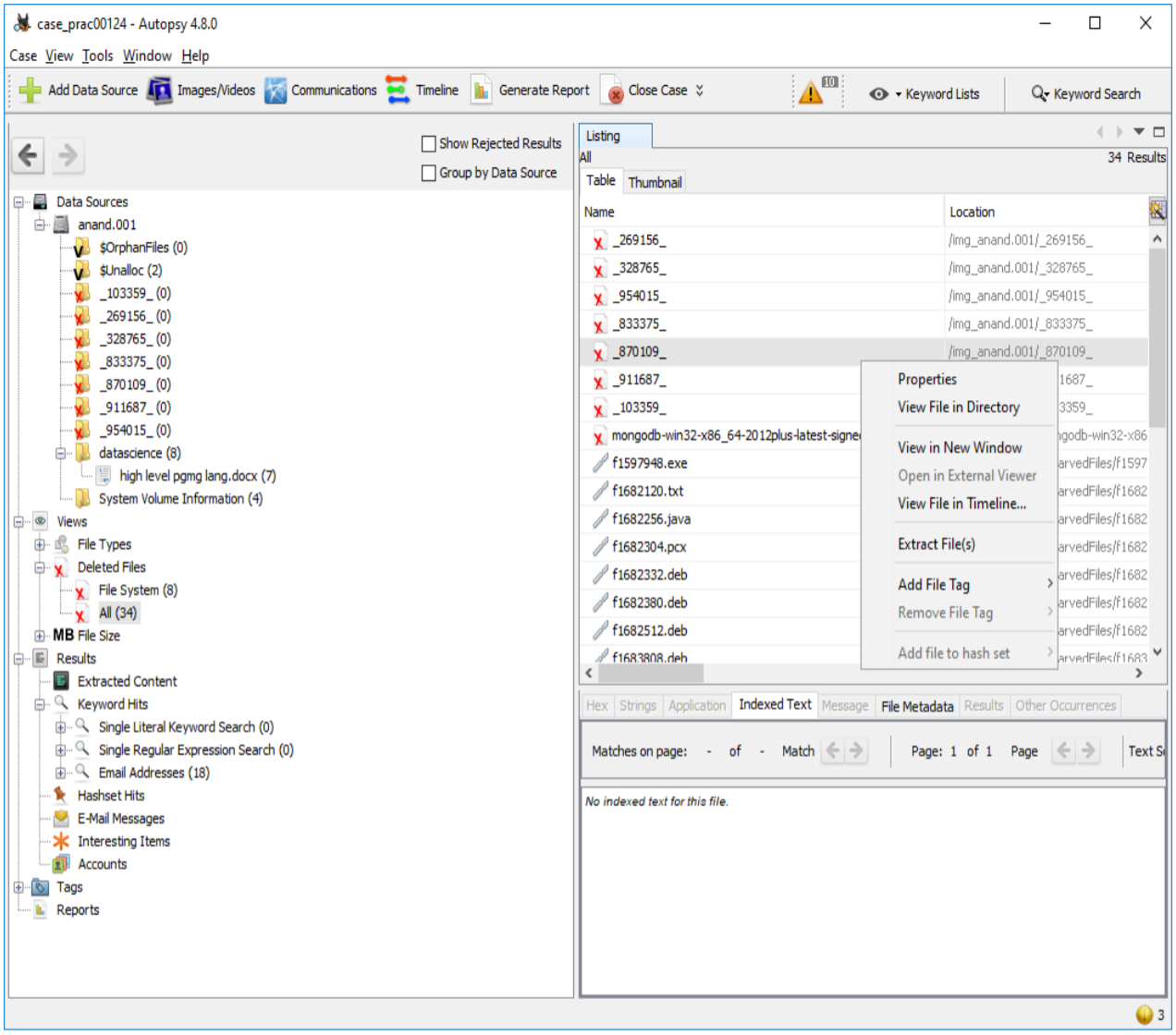
Step 10 : All image files appears in the Table tab. Select any file to see the data



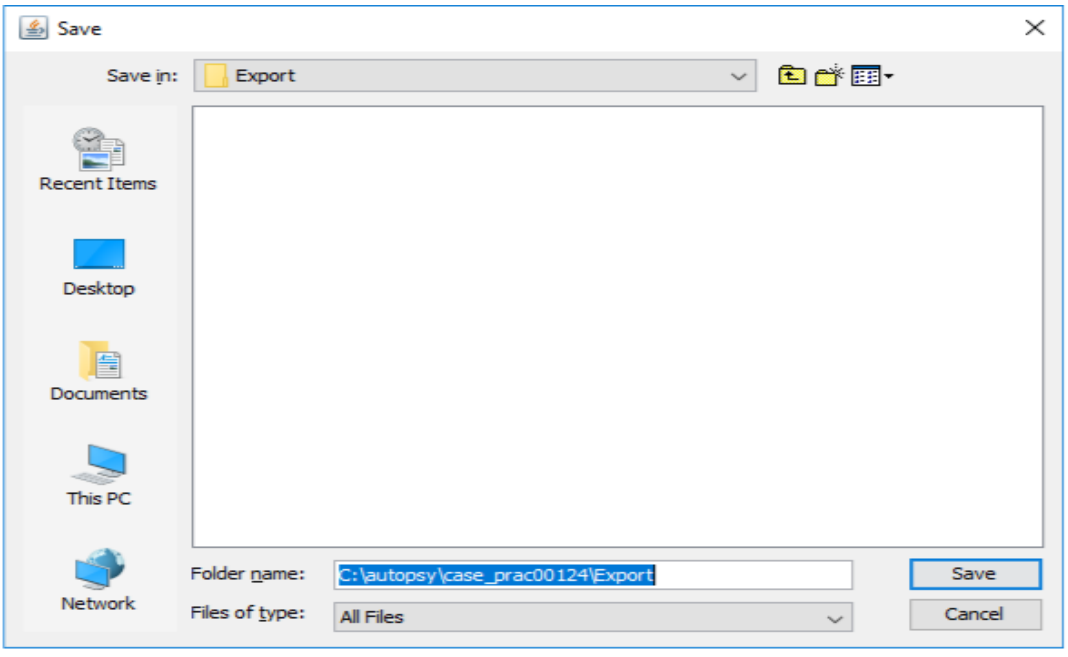
Step 11 : Expand the tree from left side panel to view the document files.



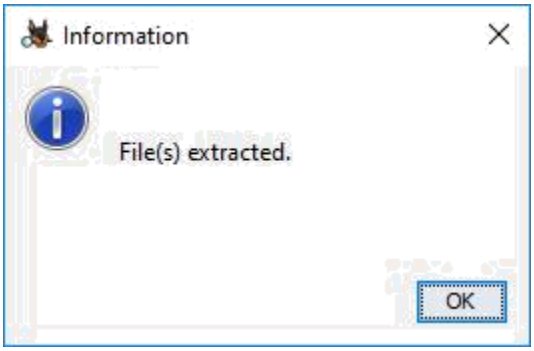
Step 12 : To recover the files , go to view code → Deleted files node , here select any file and right click on it then select Extract files option



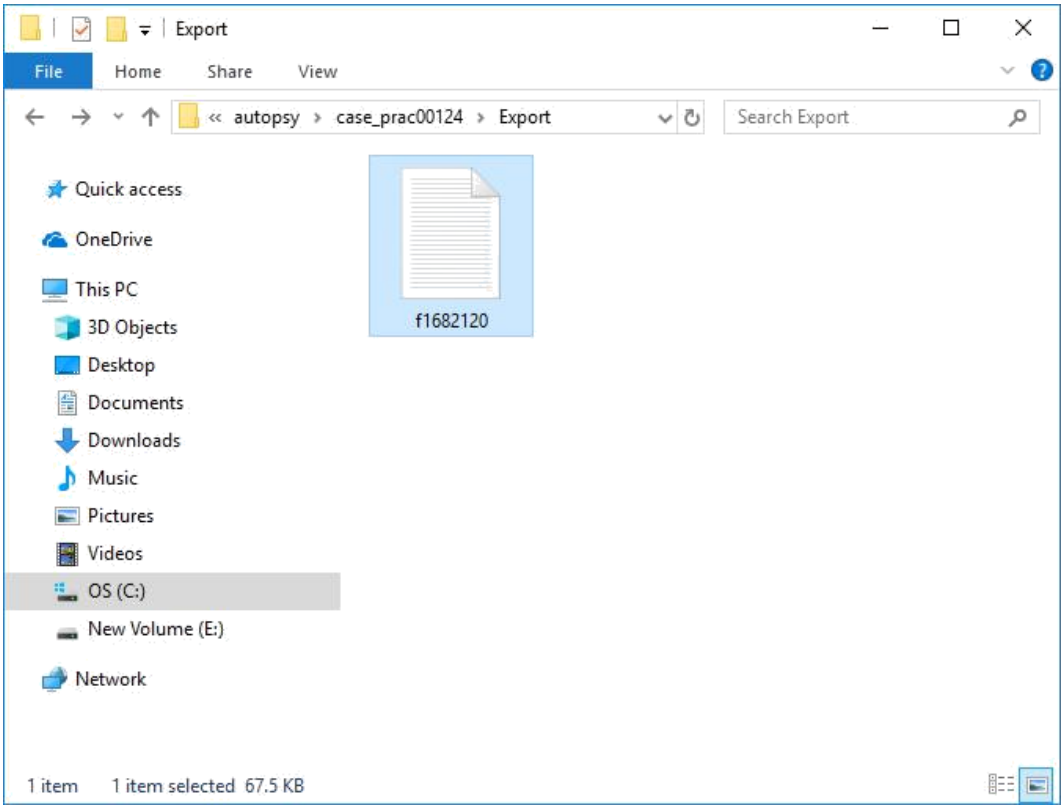
Step 12: Select Path where you want to save extracted file and click on save .



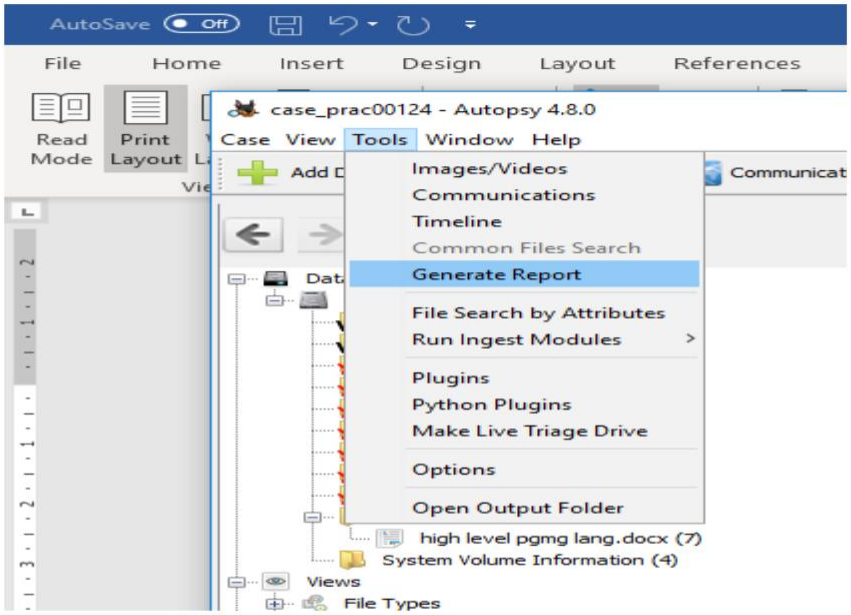
Step 13 : Now click on OK



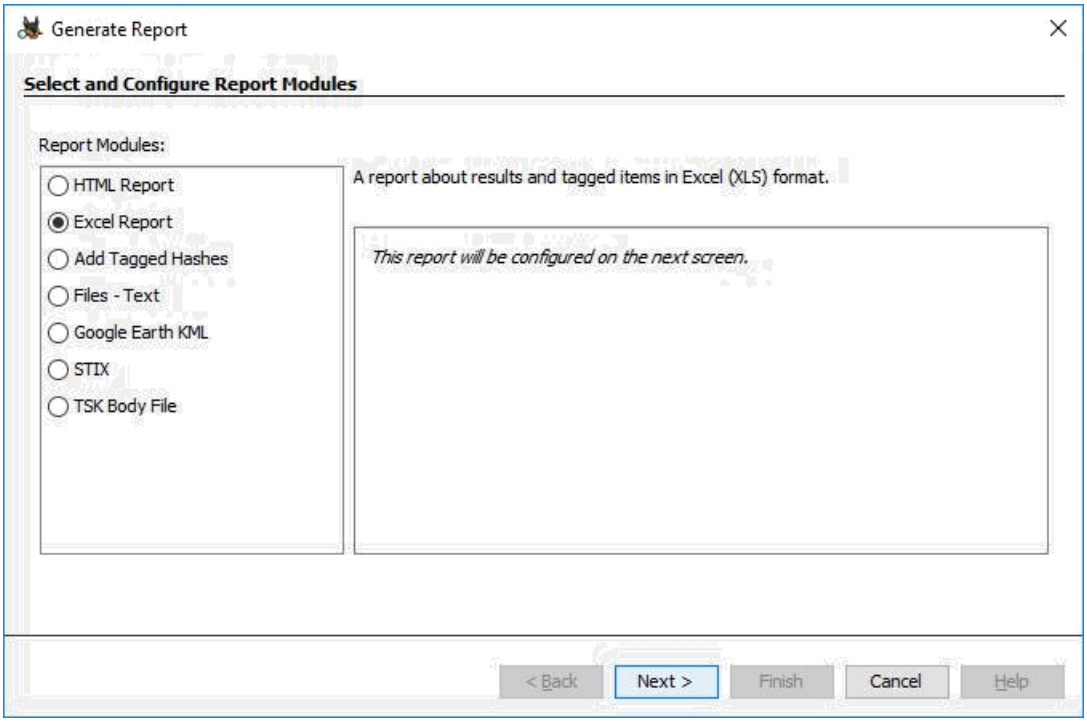
Step 14 : Now go to C:\autopsy\case_prac00124\Export folder to see recover file



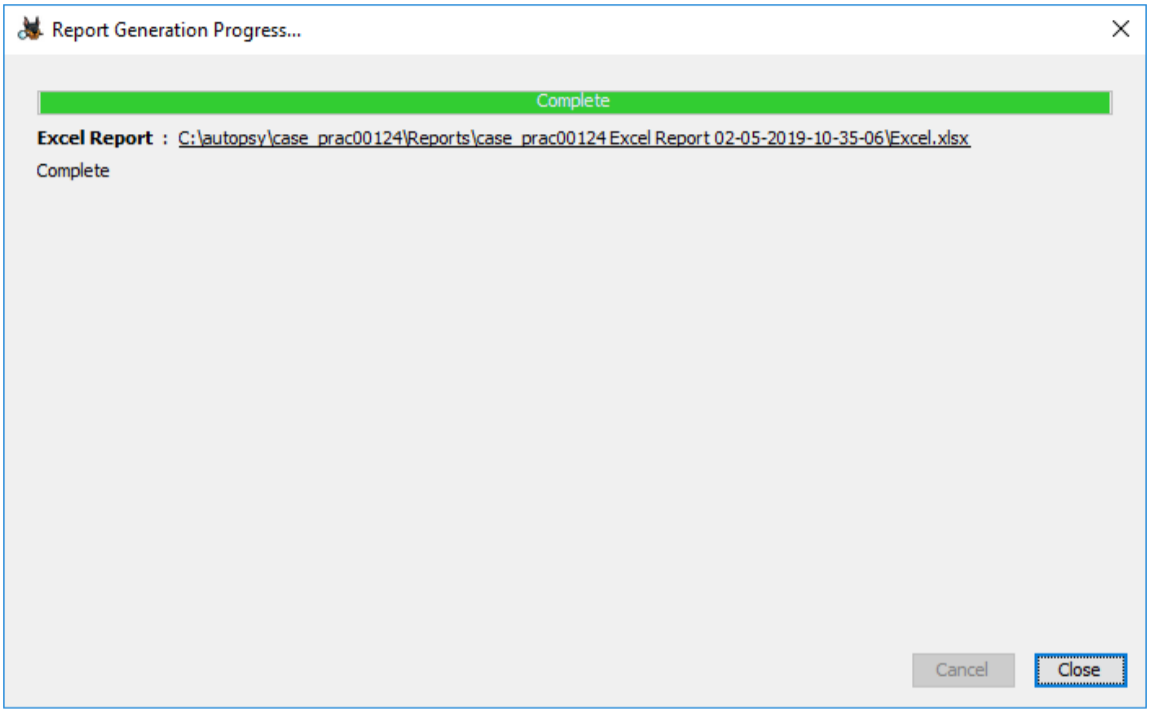
Step 15 : Click on generate report from Autopsy window and select the Excel format and click on next



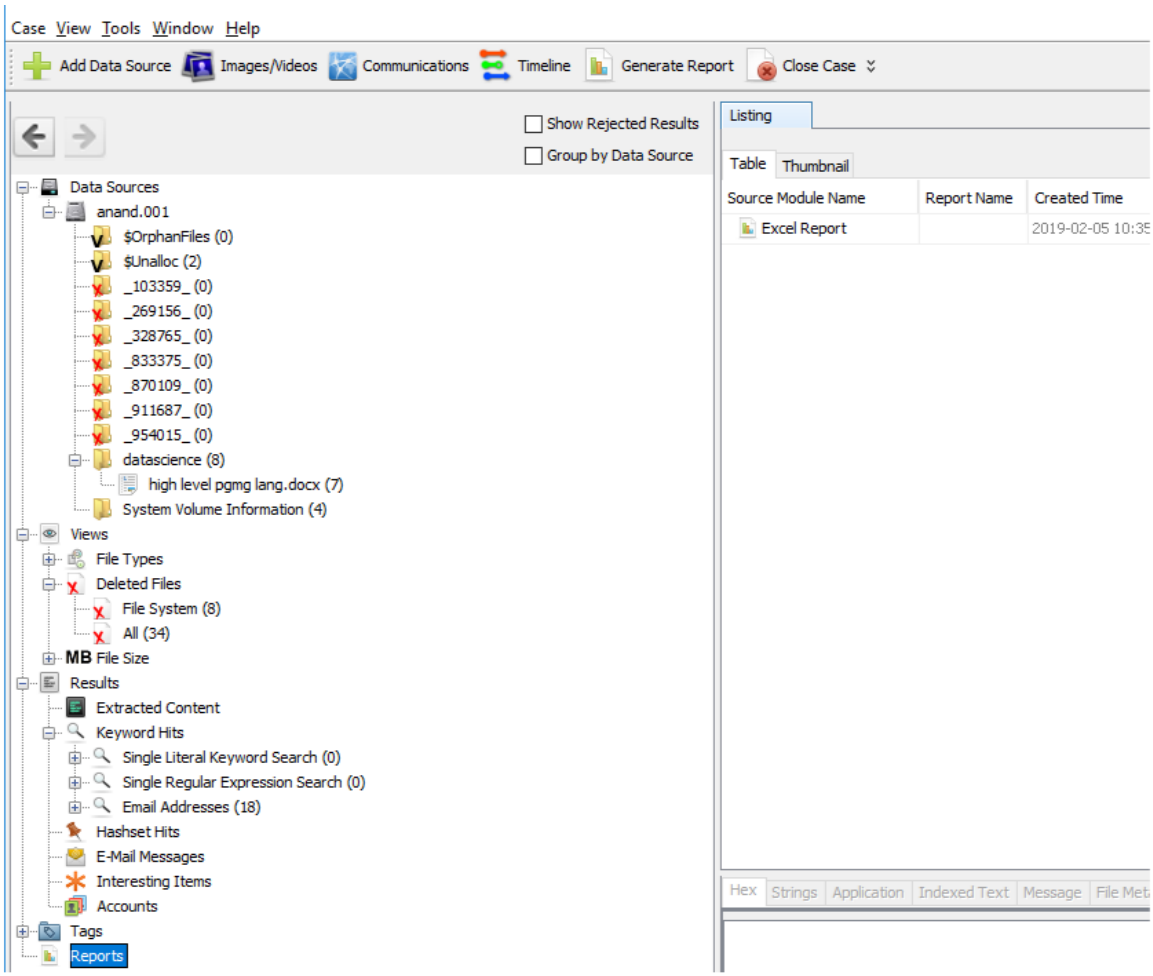
Step 16 : This window will appear



Step 17 : Now report is generated so click on close button. We can see the Report on Report Node



Step 18 : Click on report



PRACTICAL 4

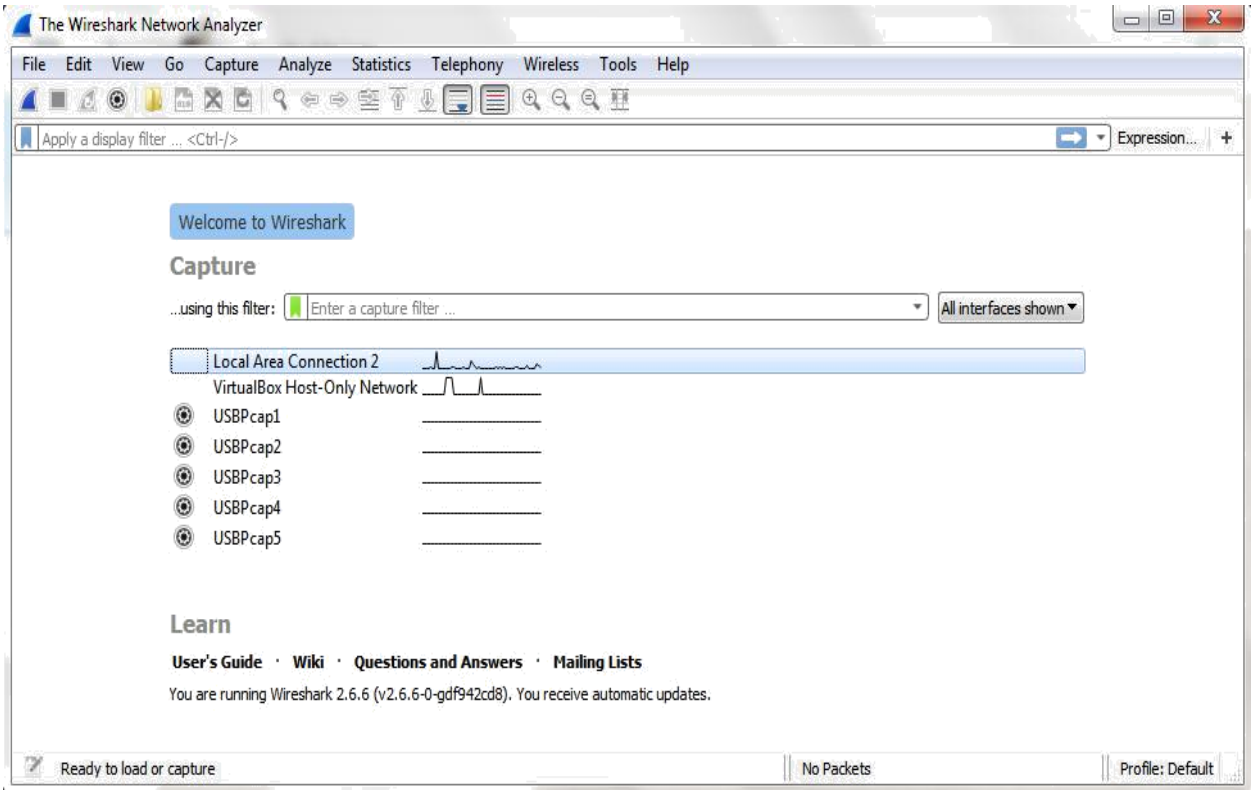
AIM : Capturing and analyzing network packets using Wireshark (Fundamentals) :

Identification the live network
Capture Packets
Analyze the captured packets

Capturing Packets

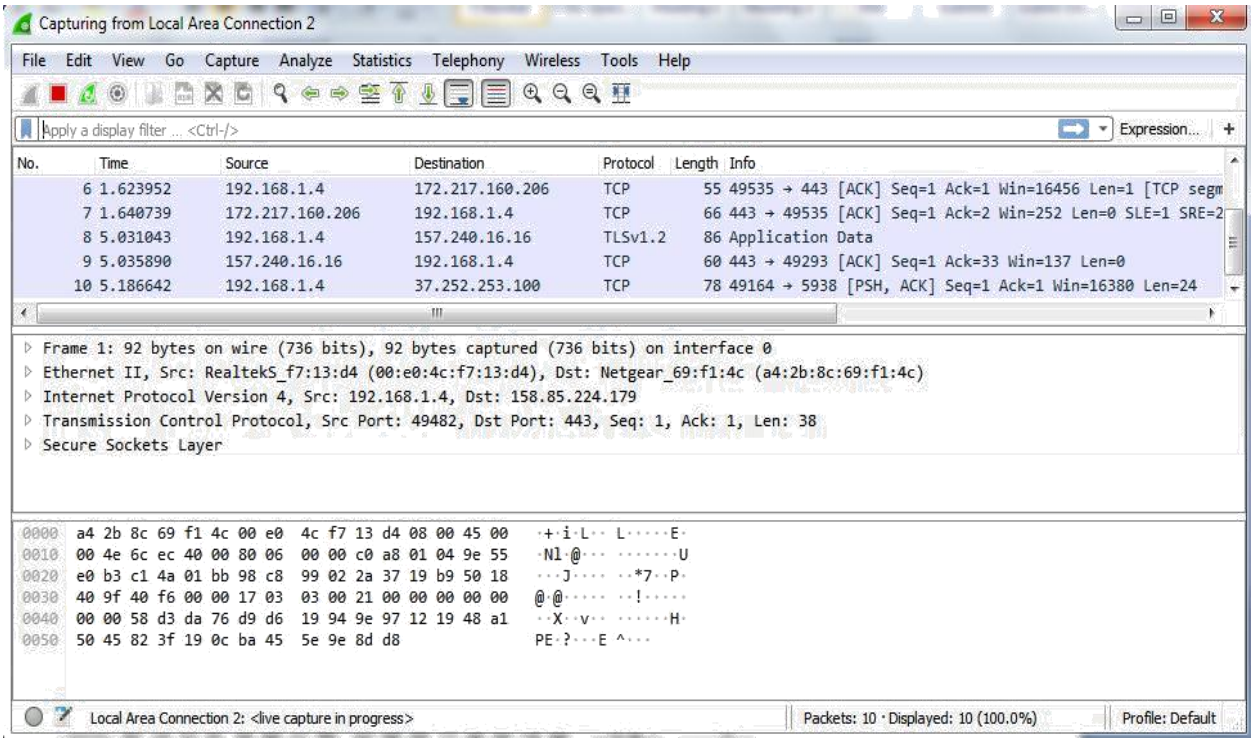
Capture traffic on your wireless network, click your wireless interface.

You can configure advanced features by clicking Capture > Options, but this isn't necessary for now.



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

Promiscuous mode is the mode in which you can see all the packets from other systems on the network and not only the packets send or received from your network adapter. Promiscuous mode is enabled by default. To check if this mode is enabled, go to Capture and Select Options. Under this window check, if the checkbox is selected and activated at the bottom of the window. The checkbox says “Enable promiscuous mode on all interfaces”.



The red box button “STOP” on the top left side of the window can be clicked to stop the capturing of traffic on the network.

Color Coding

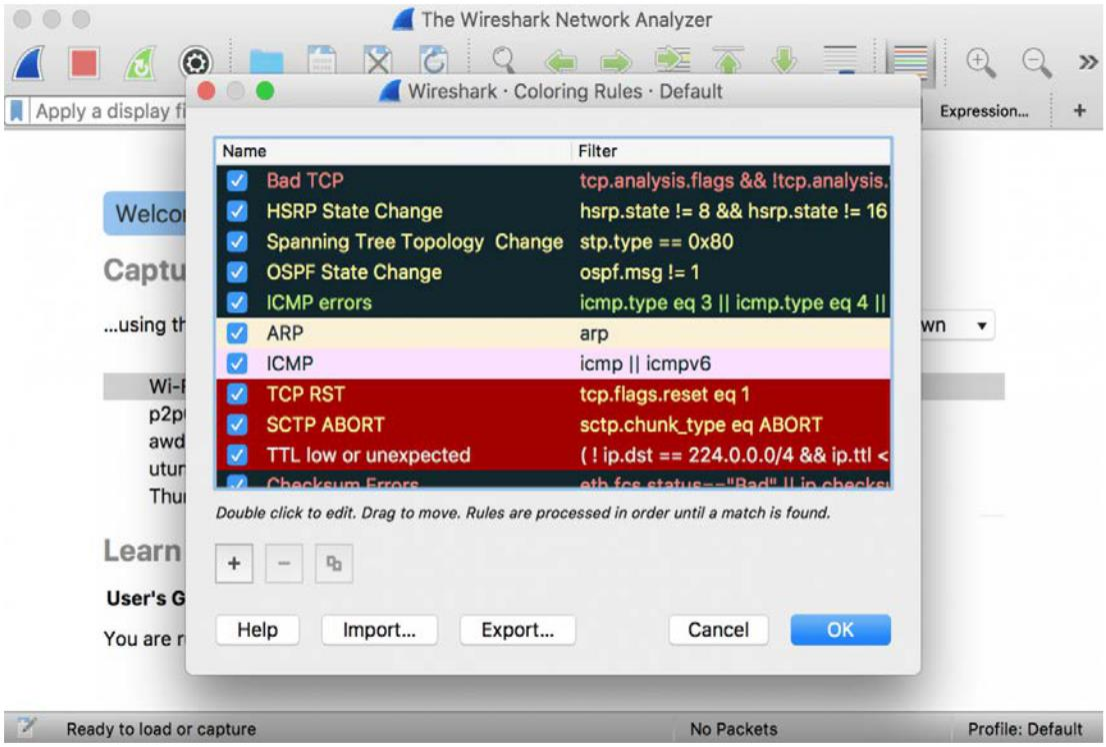
Different packets are seen highlighted in various different colors. This is Wireshark’s way of displaying traffic to help you easily identify the types of it. Default colors are:

Light Purple color for TCP traffic

Light Blue color for UDP traffic

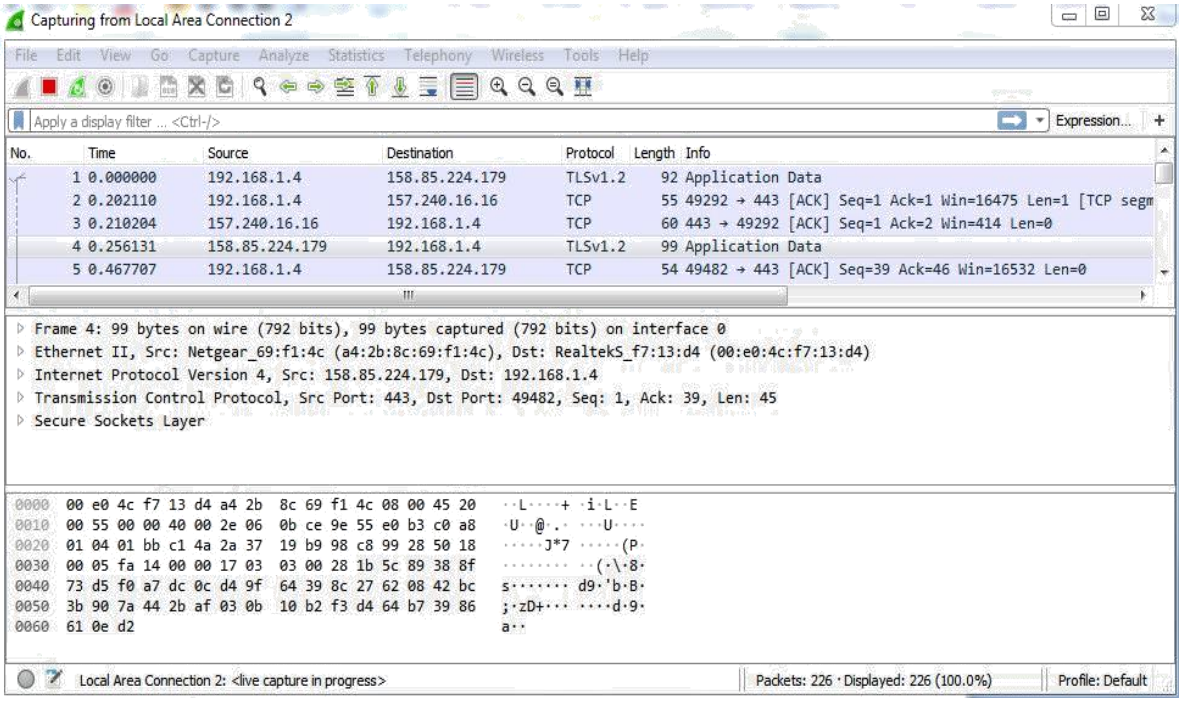
Black color identifies packets with errors – example these packets are delivered in an unordered manner.

To check the color coding rules click on View and select Coloring Rules. These color coding rules can be customized and modified to fit your needs.

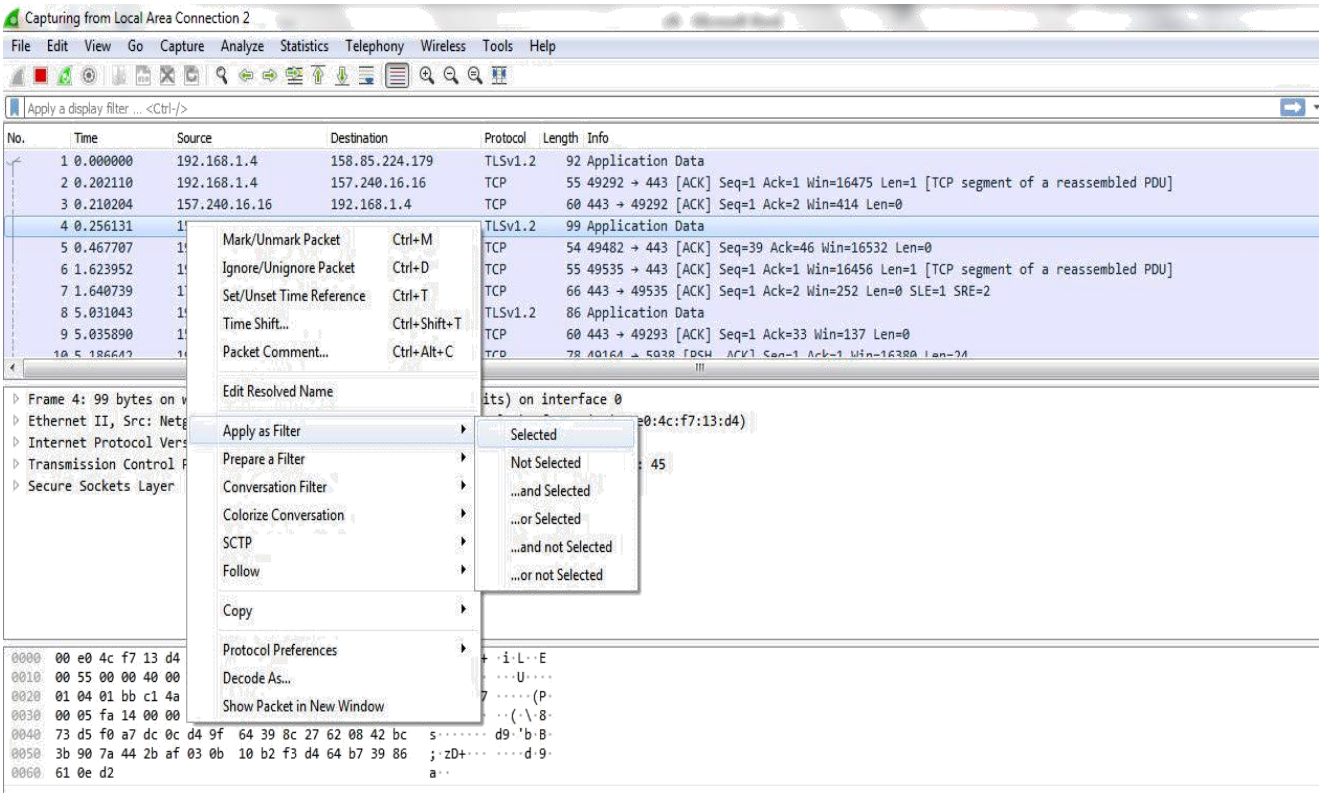


Analyze the captured Packets:

First of all, click on a packet and select it. Now, you can scroll down to view all its details.



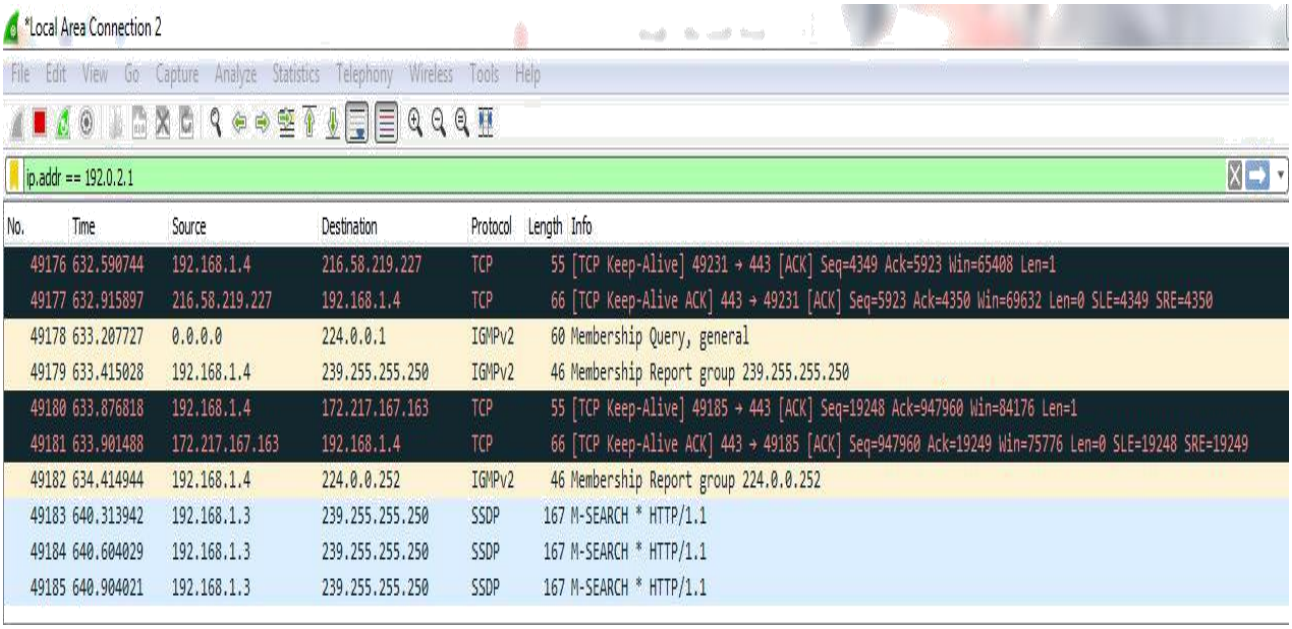
Filters can also be created from here. Right-click on one of any details. From the menu select Apply as Filter drop-down menu so filter based on it can be created.



Display filter command –

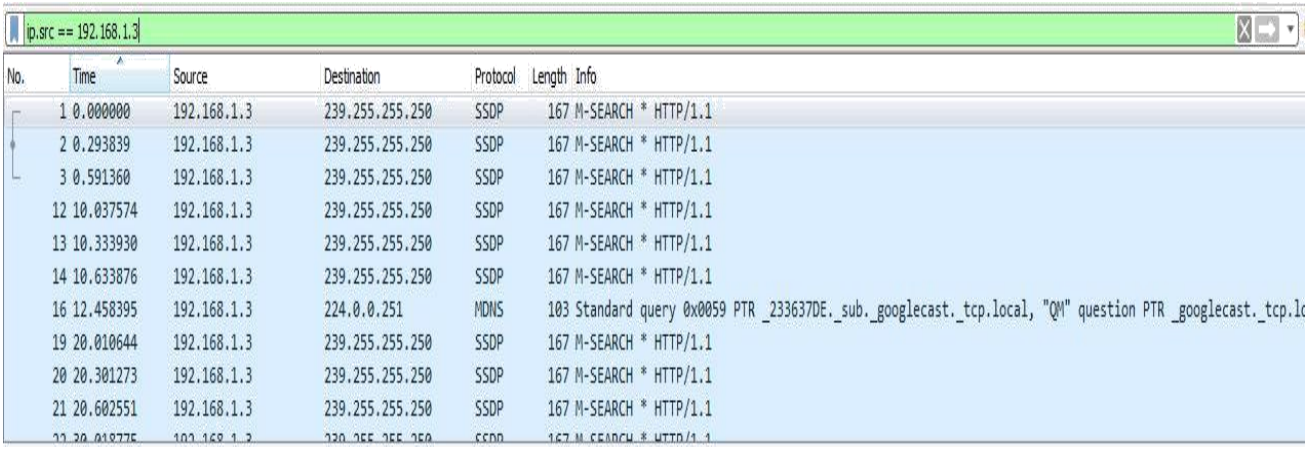
1. Display packets based on specific IP-address

   ip.addr == 192.0.2.1



2. Display packets which are coming from specific IP-address

ip.src == 192.168.1.3

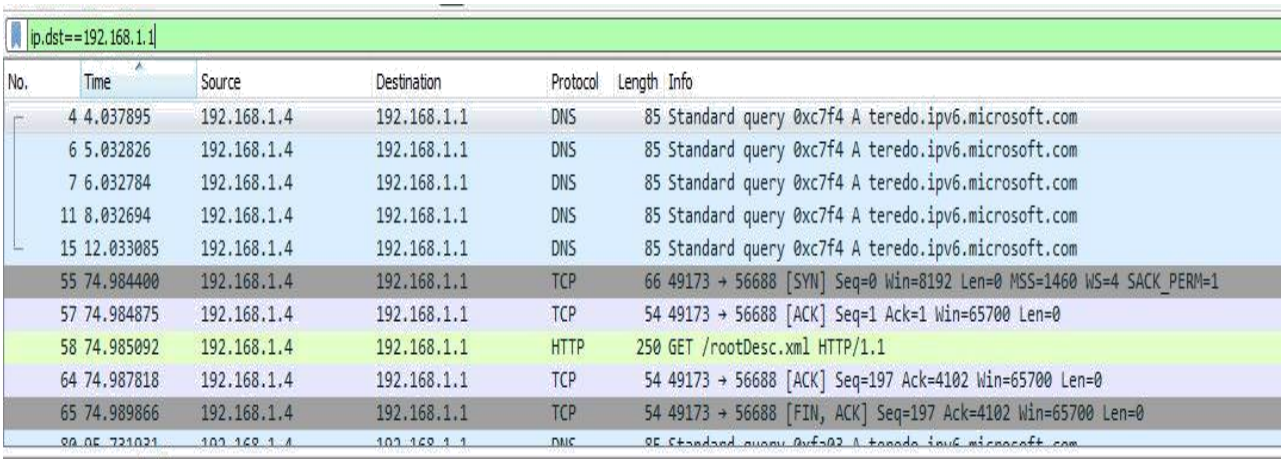


ip.src == 192.168.1.3

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.3	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
2	0.293839	192.168.1.3	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
3	0.591360	192.168.1.3	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
12	10.037574	192.168.1.3	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
13	10.333930	192.168.1.3	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
14	10.633876	192.168.1.3	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
16	12.458395	192.168.1.3	224.0.0.251	MDNS	103	Standard query 0x0059 PTR _233637DE._sub._googlecast._tcp.local, "QM" question PTR _googlecast._tcp.lo
19	20.010644	192.168.1.3	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
20	20.301273	192.168.1.3	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
21	20.602551	192.168.1.3	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1

3.Display packets which are having specific IP-address destination

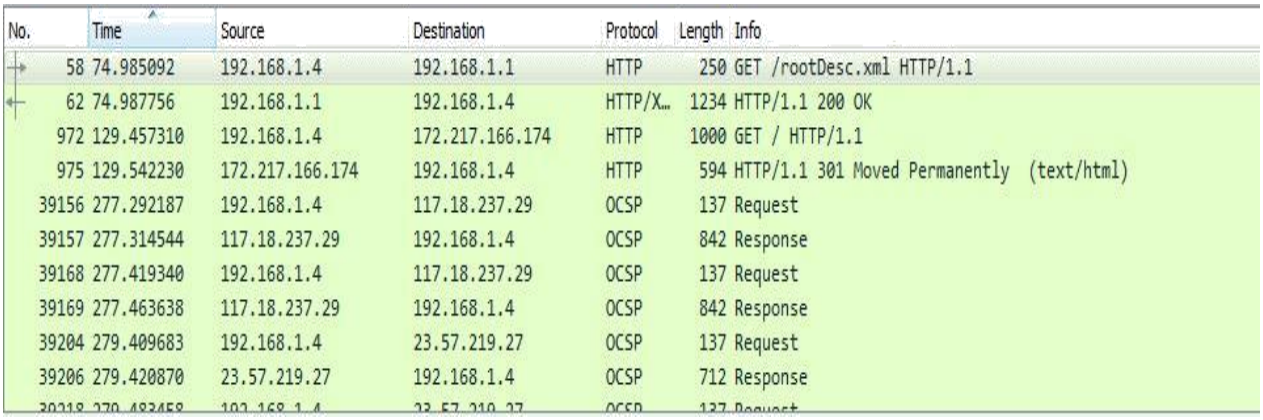
ip.dst == 192.168.1.1



ip.dst==192.168.1.1

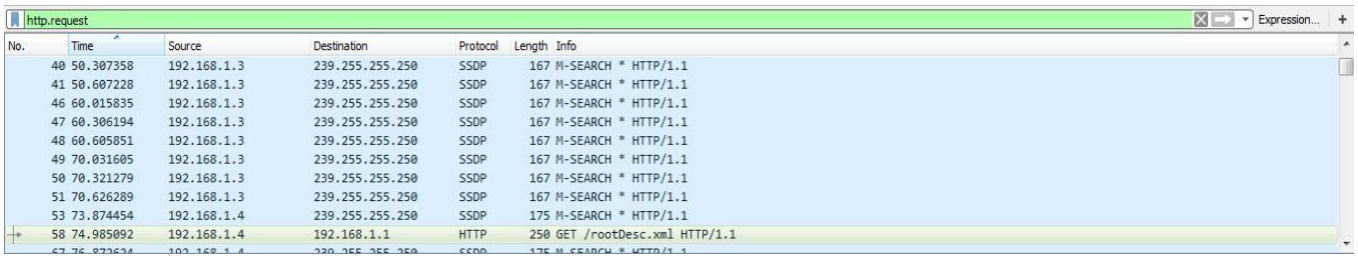
No.	Time	Source	Destination	Protocol	Length	Info
4	4.037895	192.168.1.4	192.168.1.1	DNS	85	Standard query 0xc7f4 A teredo.ipv6.microsoft.com
6	5.032826	192.168.1.4	192.168.1.1	DNS	85	Standard query 0xc7f4 A teredo.ipv6.microsoft.com
7	6.032784	192.168.1.4	192.168.1.1	DNS	85	Standard query 0xc7f4 A teredo.ipv6.microsoft.com
11	8.032694	192.168.1.4	192.168.1.1	DNS	85	Standard query 0xc7f4 A teredo.ipv6.microsoft.com
15	12.033085	192.168.1.4	192.168.1.1	DNS	85	Standard query 0xc7f4 A teredo.ipv6.microsoft.com
55	74.984400	192.168.1.4	192.168.1.1	TCP	66	49173 → 56688 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
57	74.984875	192.168.1.4	192.168.1.1	TCP	54	49173 → 56688 [ACK] Seq=1 Ack=1 Win=65700 Len=0
58	74.985092	192.168.1.4	192.168.1.1	HTTP	250	GET /rootDesc.xml HTTP/1.1
64	74.987818	192.168.1.4	192.168.1.1	TCP	54	49173 → 56688 [ACK] Seq=197 Ack=4102 Win=65700 Len=0
65	74.989866	192.168.1.4	192.168.1.1	TCP	54	49173 → 56688 [FIN, ACK] Seq=197 Ack=4102 Win=65700 Len=0

4.Display packets which are using http protocol http

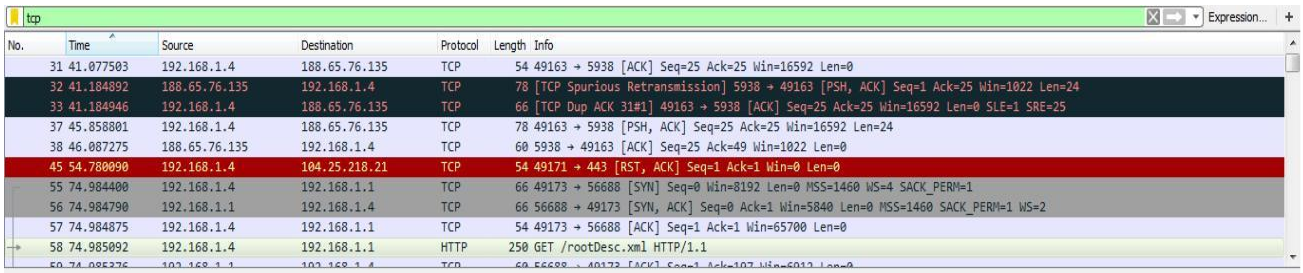


No.	Time	Source	Destination	Protocol	Length	Info
58	74.985092	192.168.1.4	192.168.1.1	HTTP	250	GET /rootDesc.xml HTTP/1.1
62	74.987756	192.168.1.1	192.168.1.4	HTTP/X…	1234	HTTP/1.1 200 OK
972	129.457310	192.168.1.4	172.217.166.174	HTTP	1000	GET / HTTP/1.1
975	129.542230	172.217.166.174	192.168.1.4	HTTP	594	HTTP/1.1 301 Moved Permanently (text/html)
39156	277.292187	192.168.1.4	117.18.237.29	OCSP	137	Request
39157	277.314544	117.18.237.29	192.168.1.4	OCSP	842	Response
39168	277.419340	192.168.1.4	117.18.237.29	OCSP	137	Request
39169	277.463638	117.18.237.29	192.168.1.4	OCSP	842	Response
39204	279.409683	192.168.1.4	23.57.219.27	OCSP	137	Request
39206	279.420870	23.57.219.27	192.168.1.4	OCSP	712	Response

5.Display packets which are using http request http.request

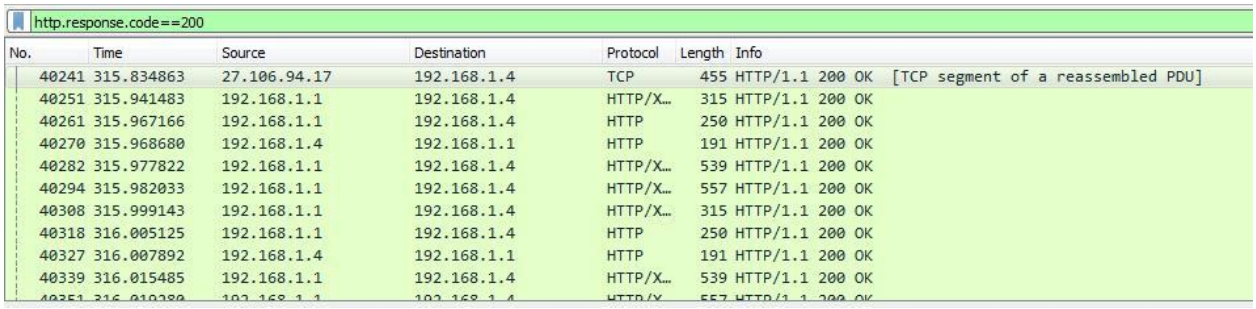


6.Display packets which are using TCP protocol tcp



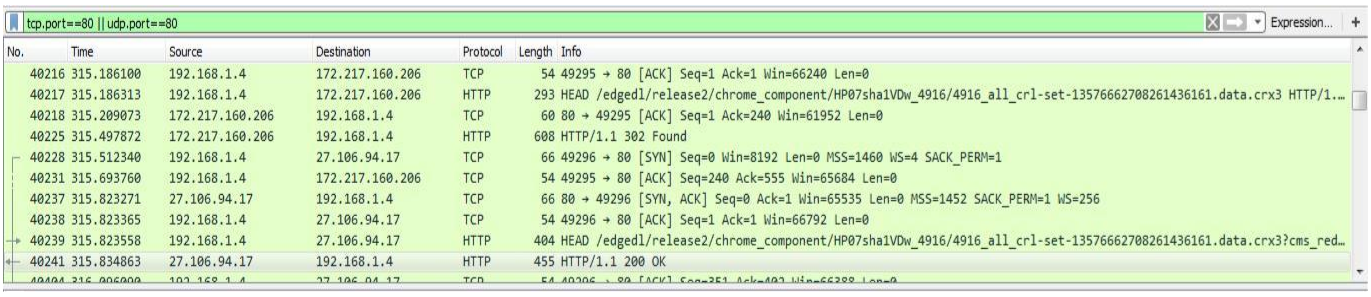
7.Display packets having no error connecting to server

http.response.code==200

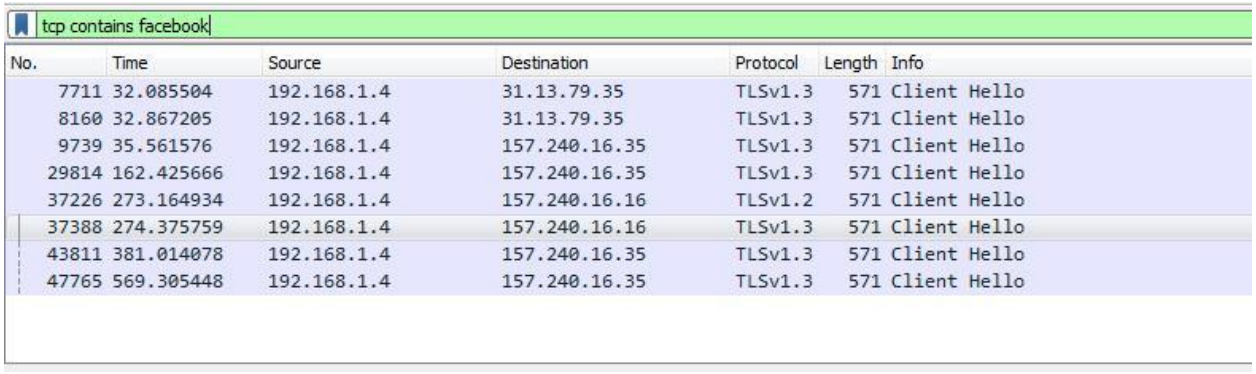


8.Display packets having port number 80

tcp.port==80 || udp.port==80



9.Display packets which that contains keyword facebook tcp contains facebook



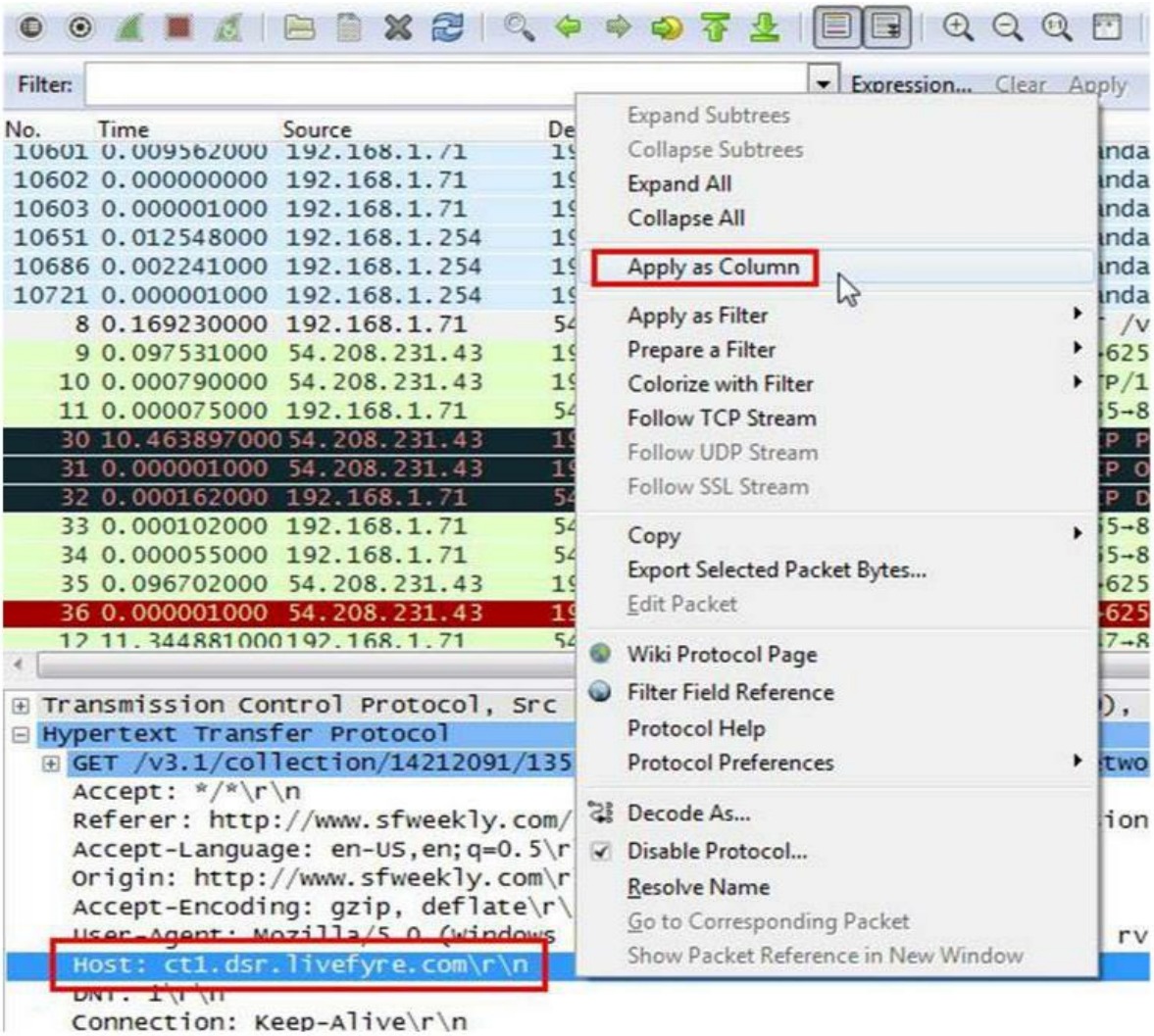
PRACTICAL 5

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

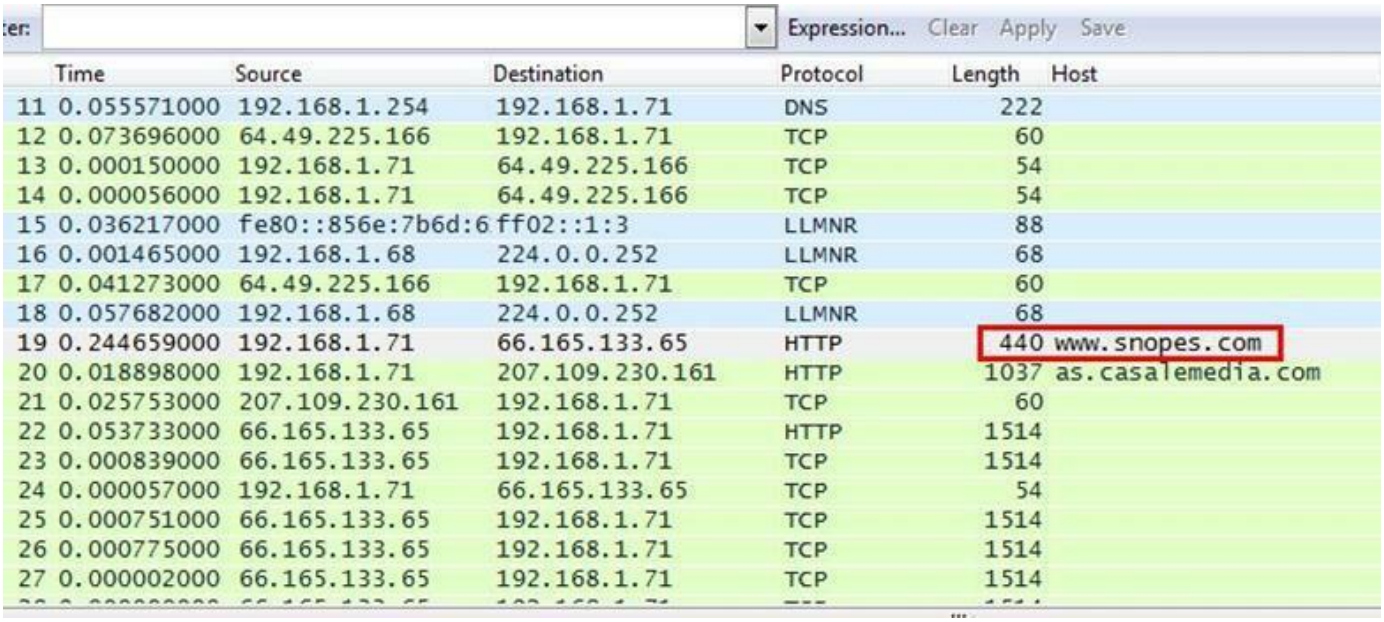
What web server software is used by www.snopes.com?
About what cell phone problem is the client concerned?
According to Zillow, what instrument will Ryan learn to play?
How many web servers are running Apache?

What 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.

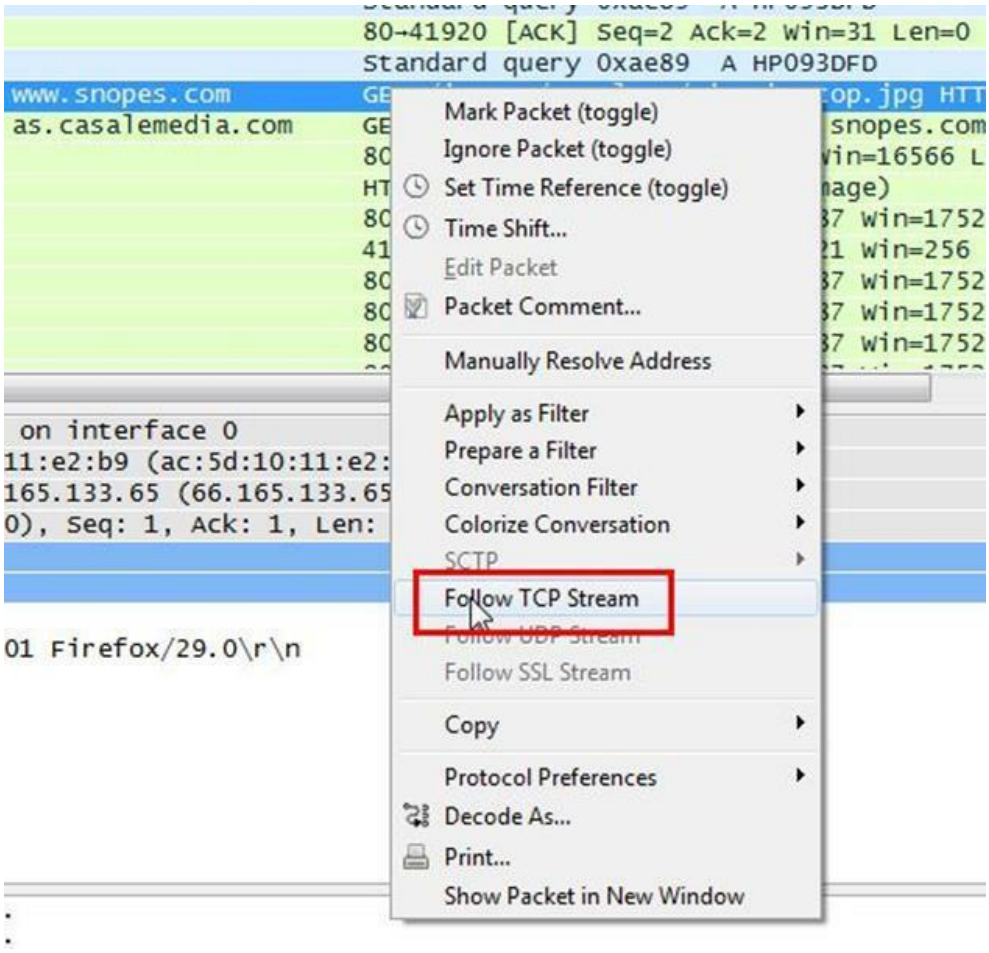


Now we can see our host www.snopes.com in host column.



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	

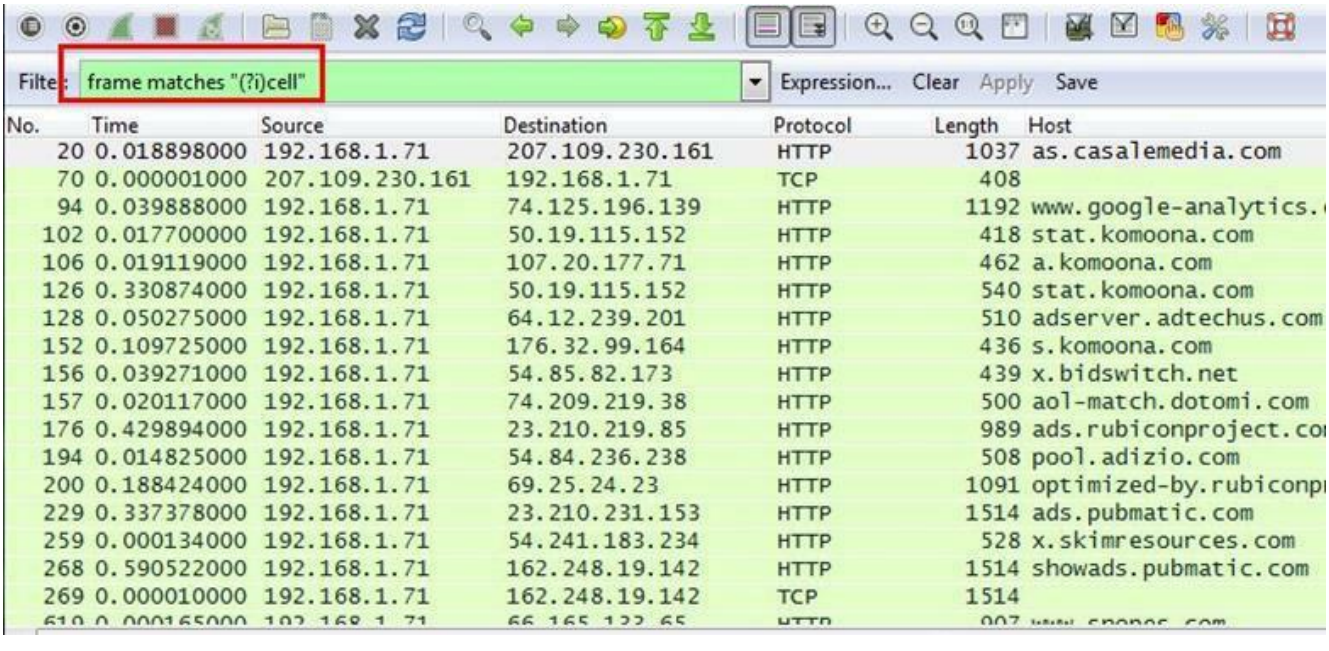
Right click on the selected packet and then select Follow TCP stream.



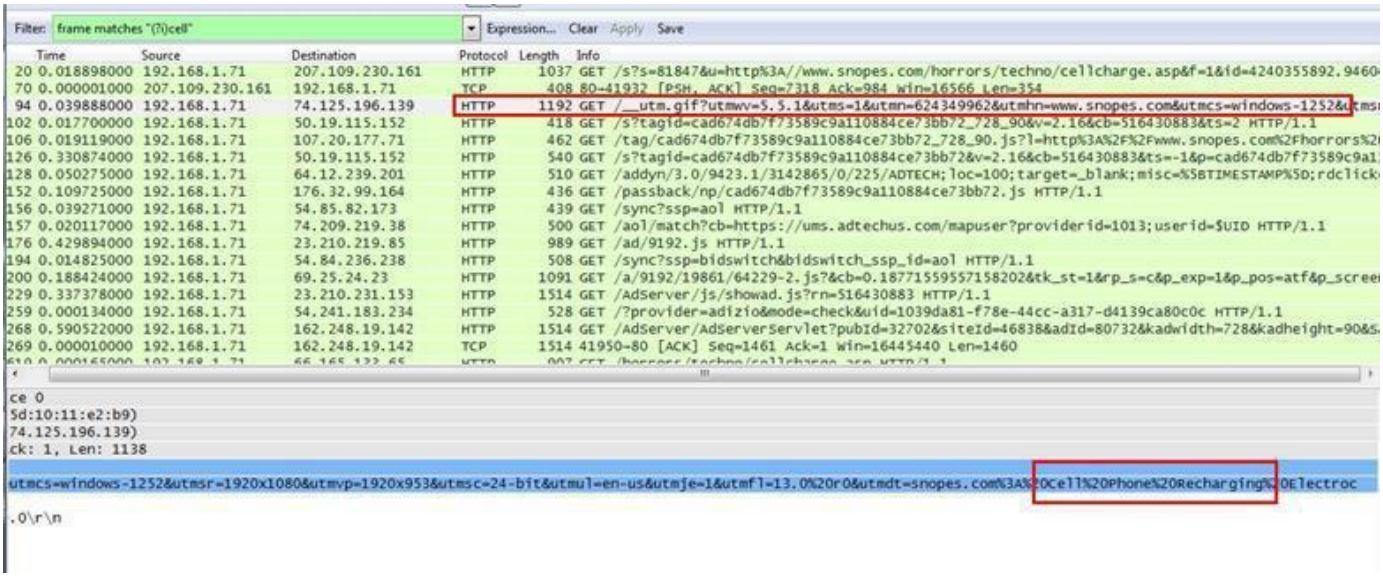
Now we can see the webserver name in server header it is Microsoft IIS 5.0

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

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

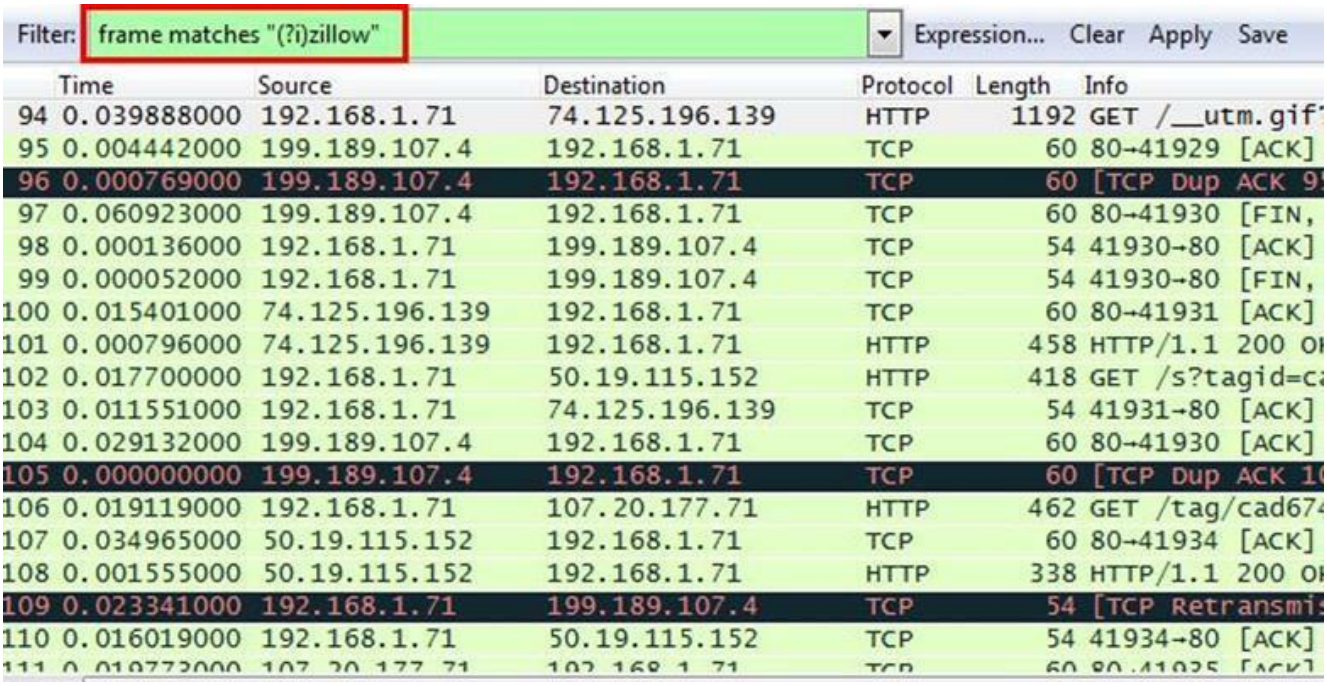


After applying the filter now, we will start to check every HTTP request. We noticed in the first HTTP request cell keyword is in URL and it was about cell phone charging issue.



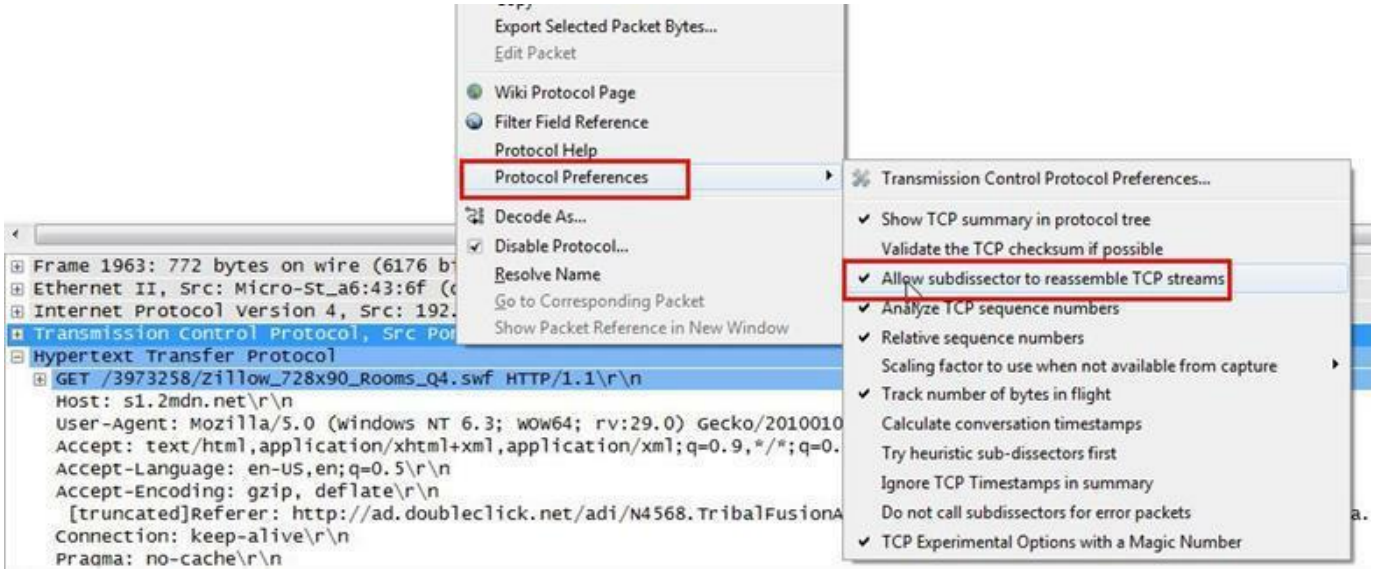
3. According to Zillow, what instrument will Ryan learn to play?

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

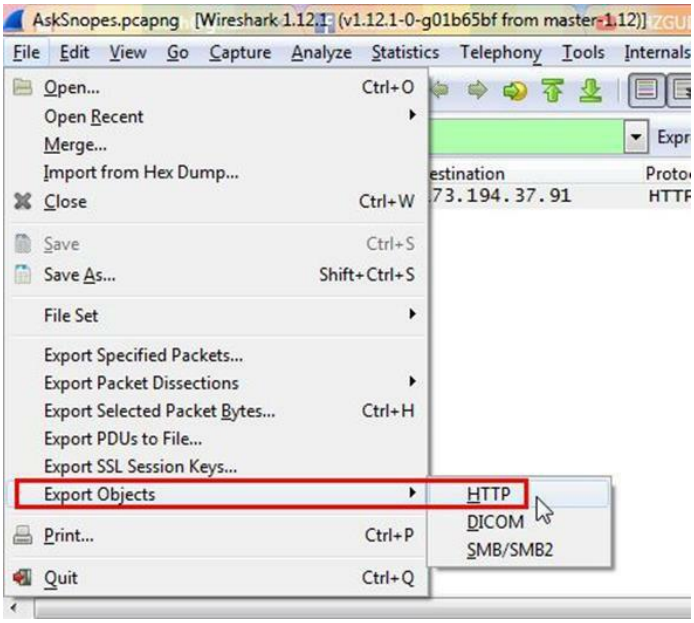


After applying the filter, we found only one packet with the Zillow keyword

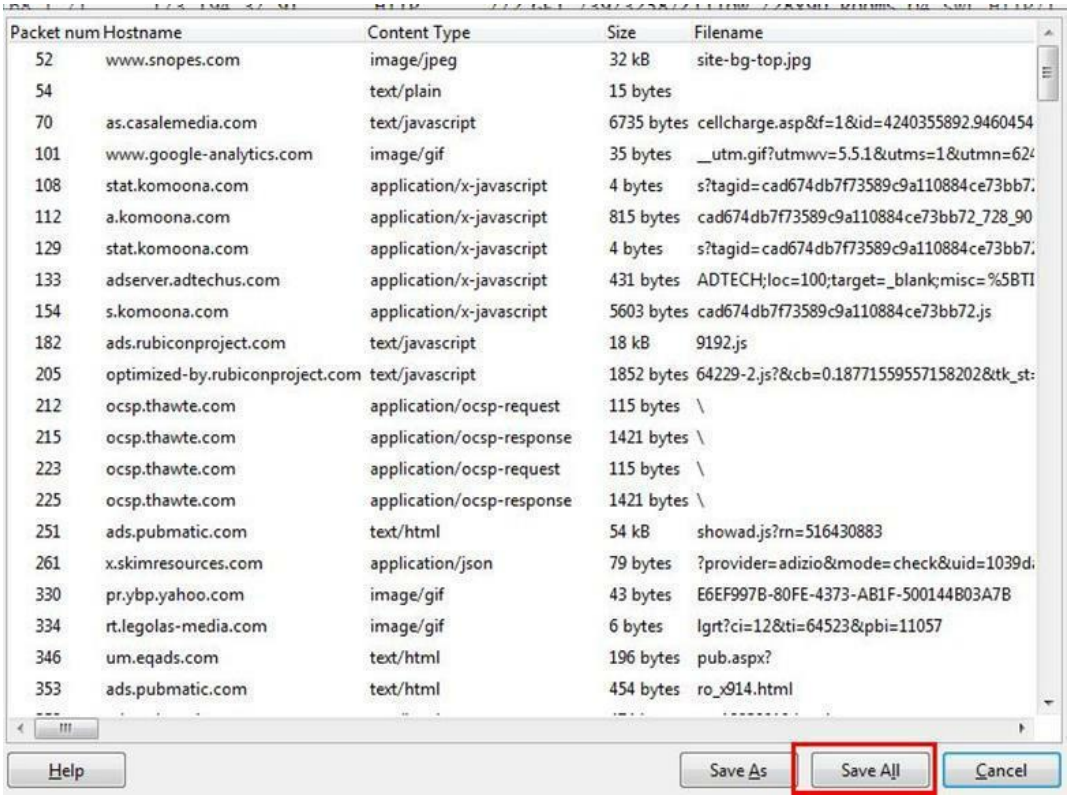
Select the packet and expand the Hypertext Transfer Protocol tab right click on it go to Protocol Preferences and check Allow subdissector to resemble TCP stream.



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



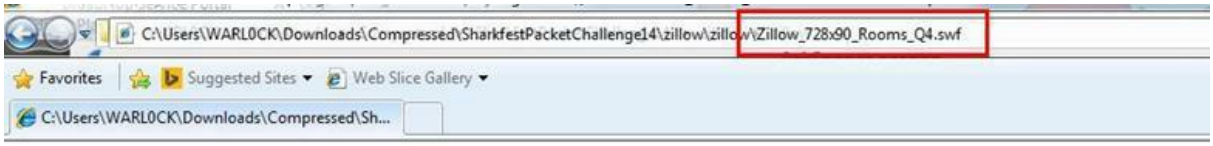
Click on save all.



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

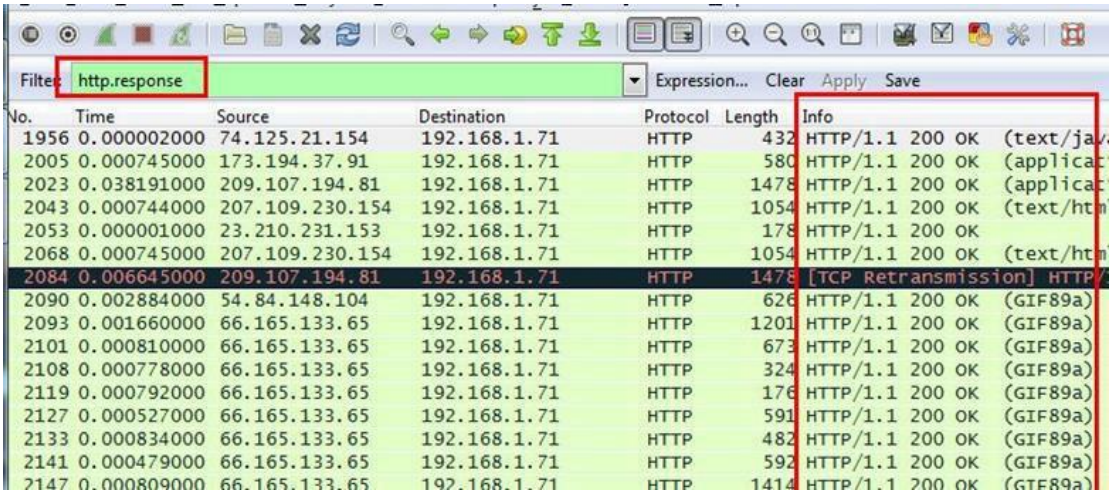
Help | Save As | Save All | Cancel

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.

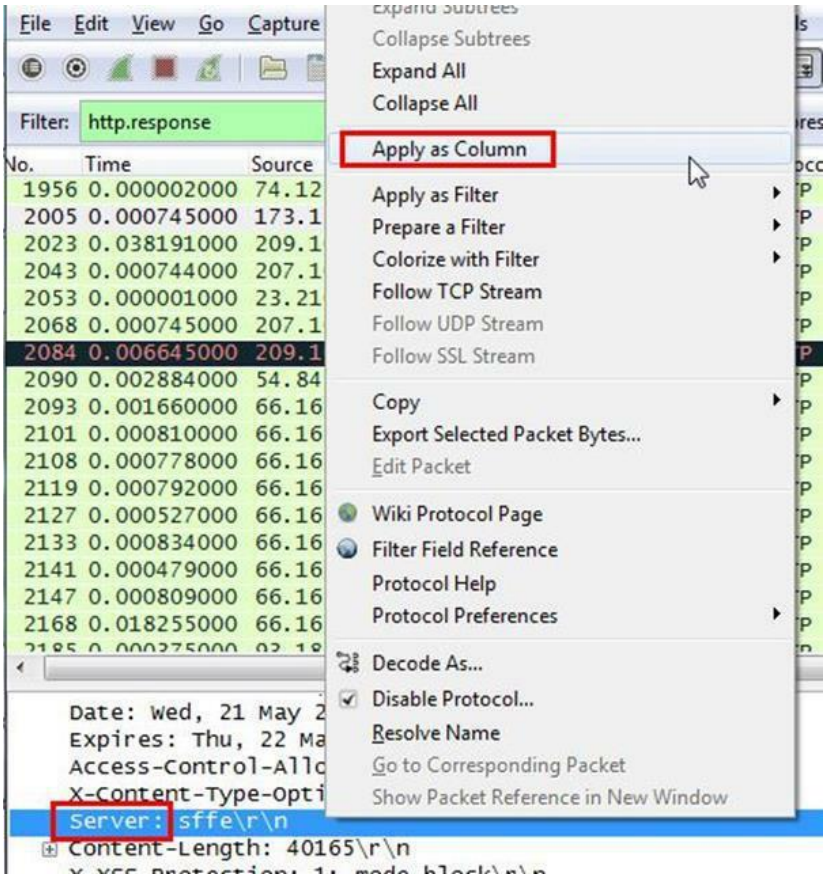


4. How many web servers are running Apache?

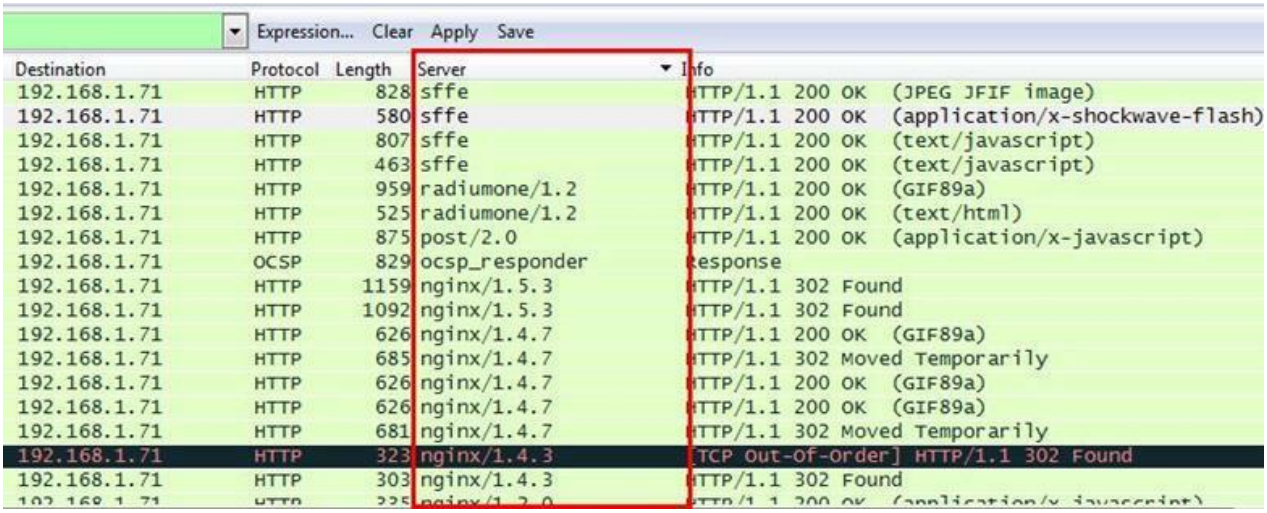
Analysis – The web server name can be retrieved from HTTP response header. So will apply filter http. response and we can see all http response packets.



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

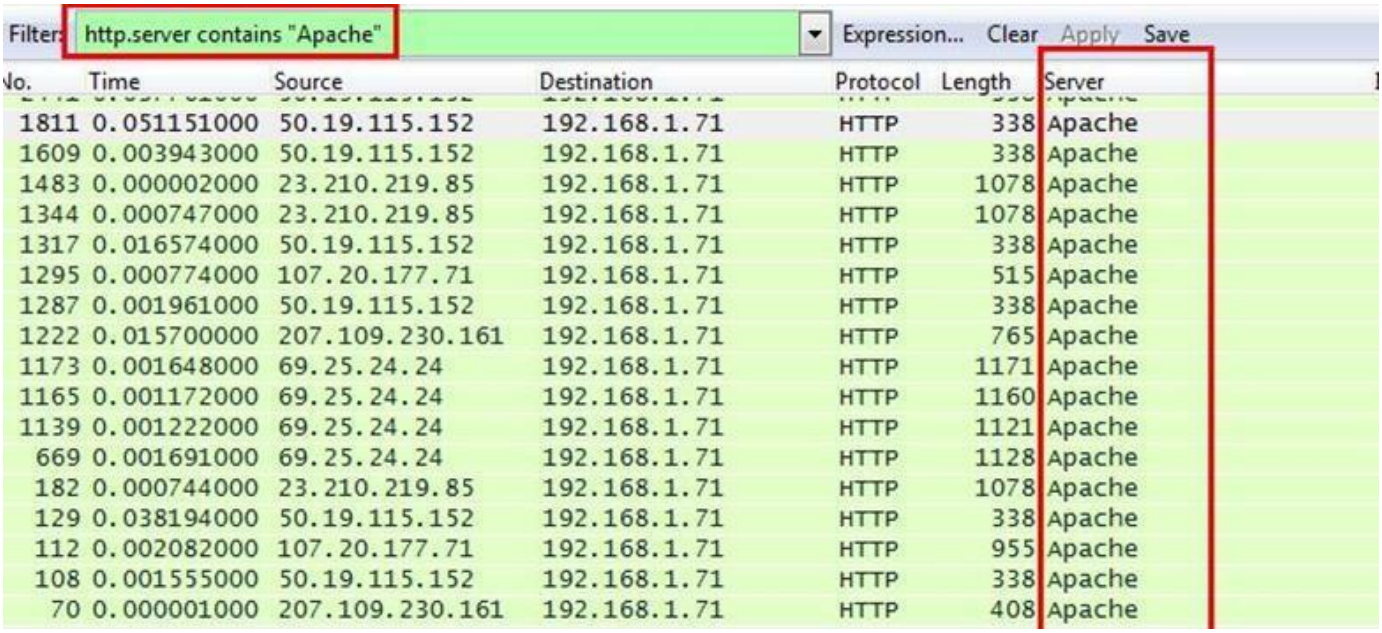


Now can see the server column where all server name is showing.



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

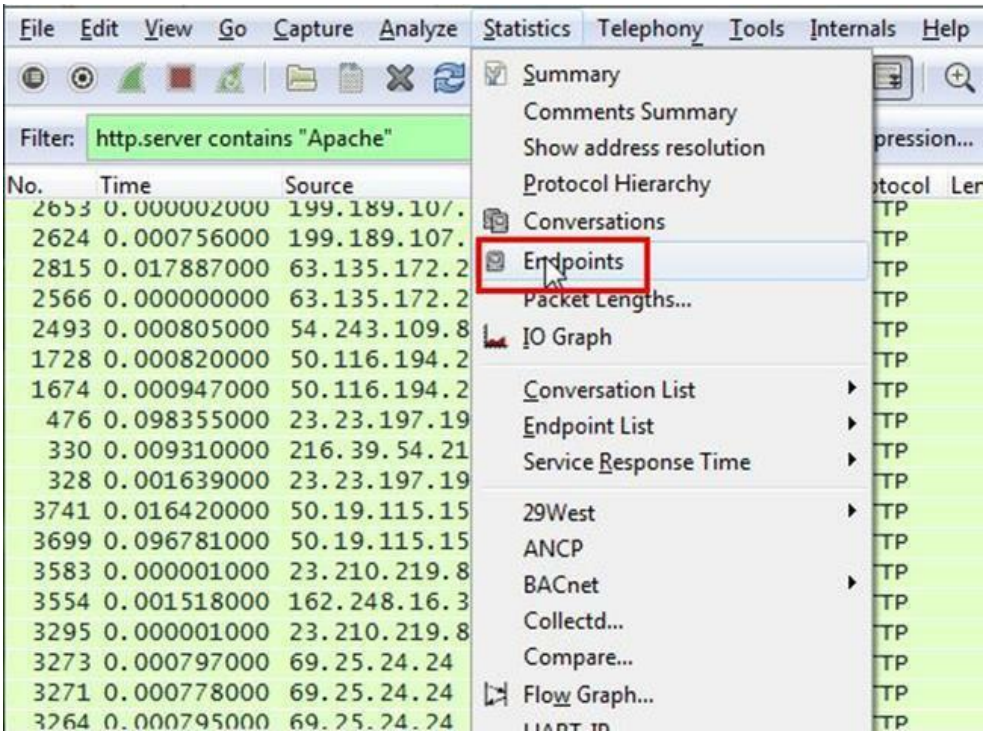
Now we have to check how many Apache packets are there we can't count manually for each packet so we will apply another filter http.server contains "Apache"



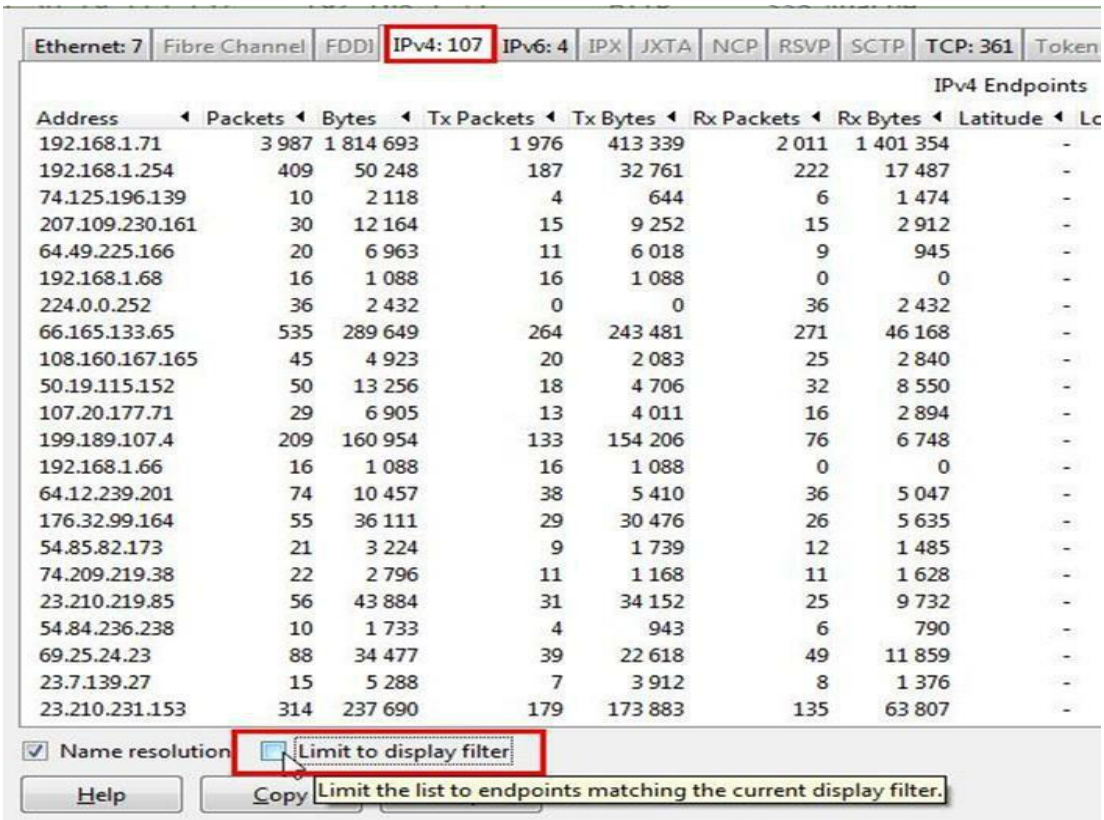
Filter: http.server contains "Apache"

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

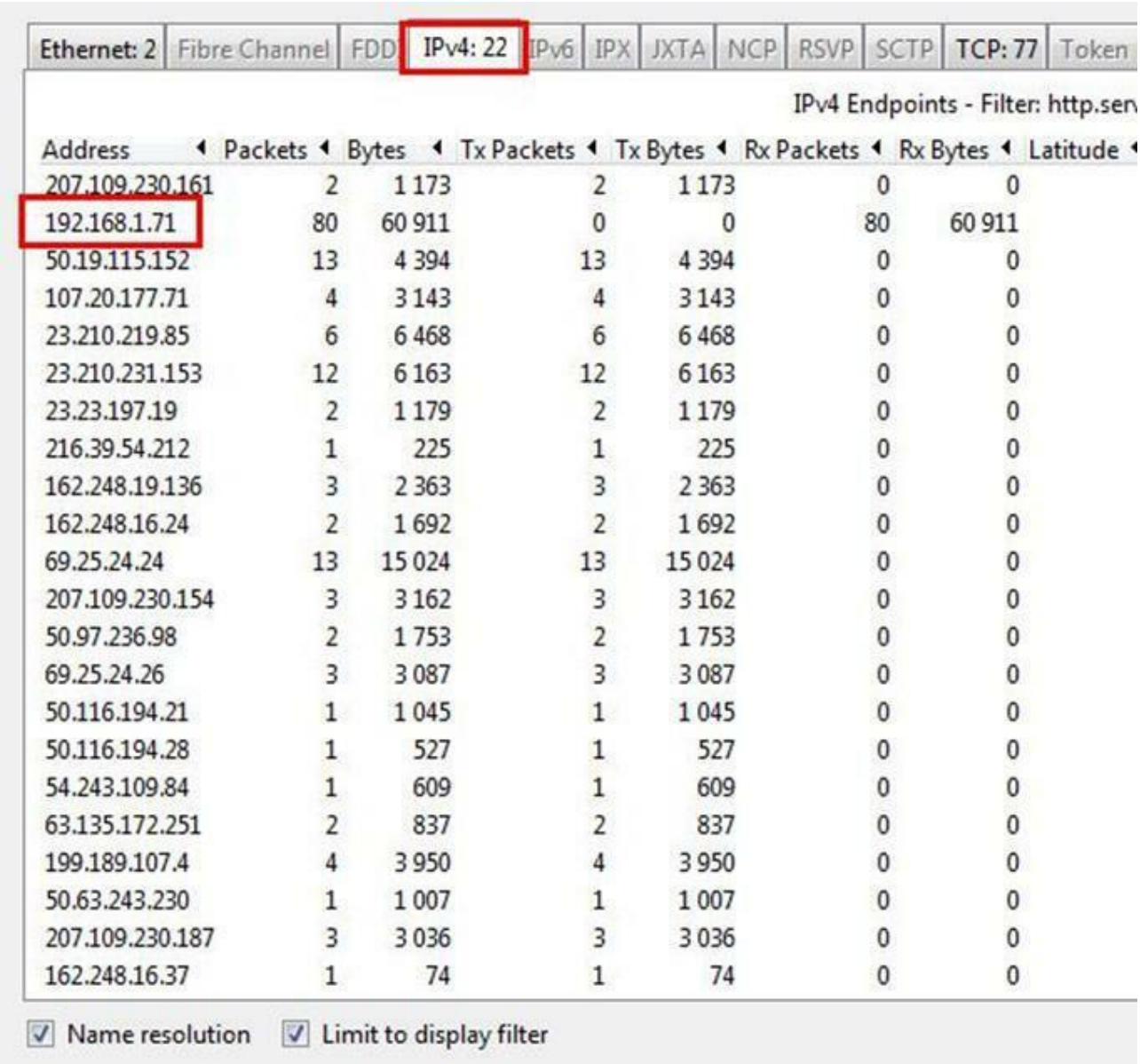
After applying filter go to Statistics > Endpoints



It will show all connections



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.



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	

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

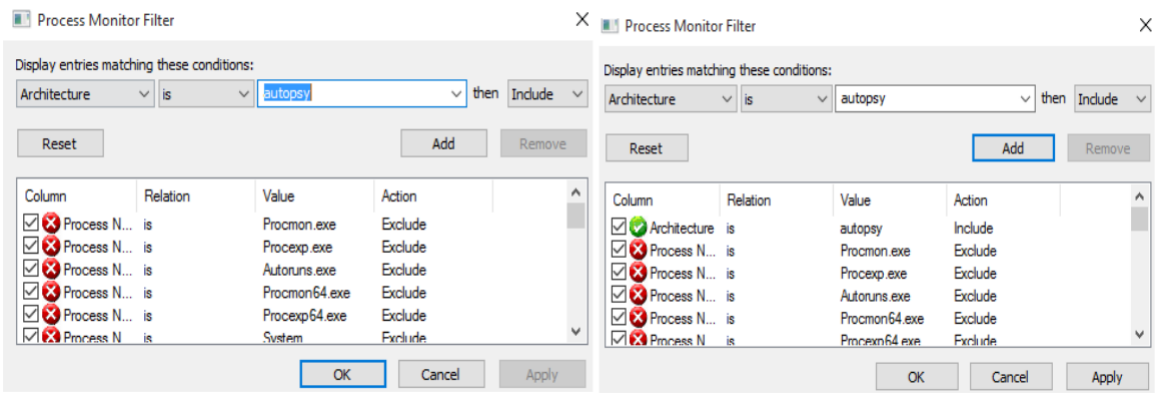
1. Check Sysinternals tools

Google → sysinternal tools

2. Monitor Live Processes

Process Monitor is an advanced monitoring tool for Windows that shows real-time file system, Registry and process/thread activity. It combines the features of two legacy Sysinternals utilities, *Filemon* and *Regmon*, and adds an extensive list of enhancements including rich and non-destructive filtering, comprehensive event properties such session IDs and user names, reliable process information, full thread stacks with integrated symbol support for each operation, simultaneous logging to a file, and much more. Its uniquely powerful features will make Process Monitor a core utility in your system troubleshooting and malware hunting toolkit.

Sysinternal → procmon



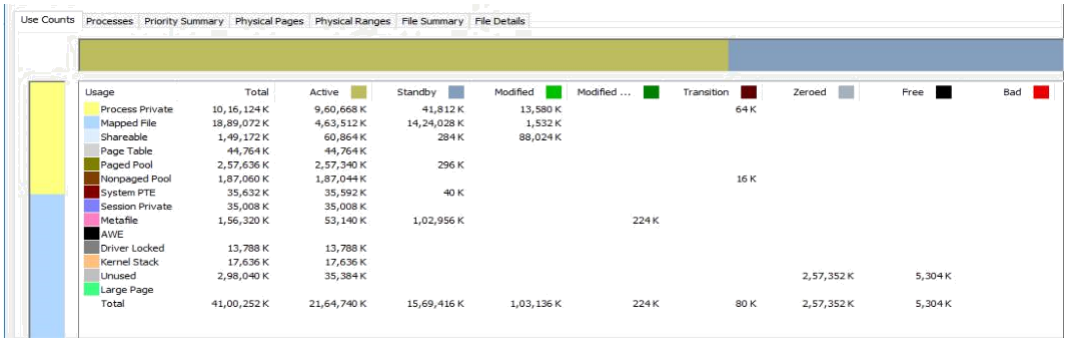
3. Capture RAM

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

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

Use RAMMap to gain understanding of the way Windows manages memory, to analyze application memory usage, or to answer specific questions about how RAM is being allocated. RAMMap's refresh feature enables you to update the display and it includes support for saving and loading memory snapshots.

STEPS sysinternal → RAMMap



Usage	Total	Active	Standby	Modified	Modified ...	Transition	Zeroed	Free	Bad
Process Private	10,16,124 K	9,60,668 K	41,812 K	13,580 K		64 K			
Mapped File	18,89,072 K	4,63,512 K	14,24,028 K	1,532 K					
Shareable	1,49,172 K	60,864 K	284 K	88,024 K					
Page Table	44,764 K	44,764 K							
Paged Pool	2,57,636 K	2,57,340 K	296 K						
Nonpaged Pool	1,87,060 K	1,87,044 K				16 K			
System PTE	35,632 K	35,592 K	40 K						
Session Private	35,008 K	35,008 K							
Metafile	1,56,320 K	53,140 K	1,02,956 K		224 K				
AWE									
Driver Locked	13,788 K	13,788 K							
Kernel Stack	17,636 K	17,636 K							
Unused	2,98,040 K	35,384 K					2,57,352 K	5,304 K	
Large Page									
Total	41,00,252 K	21,64,740 K	15,69,416 K	1,03,136 K	224 K	80 K	2,57,352 K	5,304 K	

4.Capture TCP/UDP packets

TCPView is a Windows program that will show you detailed listings of all TCP and UDP endpoints on your system, including the local and remote addresses and state of TCP connections. On Windows Server 2008, Vista, and XP, TCPView also reports the name of the process that owns the endpoint. TCPView provides a more informative and conveniently presented subset of the Netstat program that ships with Windows. The TCPView download includes Tcpvcon, a command-line version with the same functionality.

Using TCPView

When you start TCPView it will enumerate all active TCP and UDP endpoints, resolving all IP addresses to their domain name versions. You can use a toolbar button or menu item to toggle the display of resolved names. On Windows XP systems, TCPView shows the name of the process that owns each endpoint.By default, TCPView updates every second, but you can use the **Options|Refresh Rate** menu item to change the rate. Endpoints that change state from one update to the next are highlighted in yellow; those that are deleted are shown in red, and new endpoints are shown in green.You can close established TCP/IP connections (those labeled with a state of ESTABLISHED) by selecting **File|Close Connections**, or by right-clicking on a connection and choosing **Close Connections** from the resulting context menu.You can save TCPView's output window to a file using the **Save** menu item.

Using Tcpvcon

Tcpvcon usage is similar to that of the built-in Windows netstat utility:

Usage: tcpvcon [-a] [-c] [-n] [process name or PID]

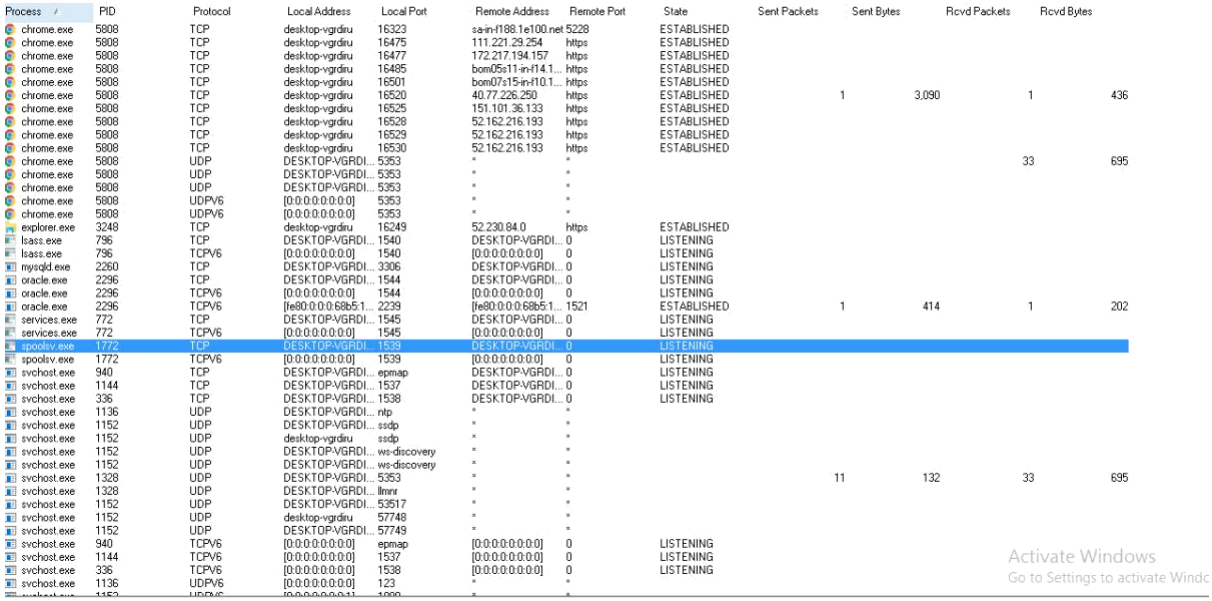
Parameter	Description
-a	Show all endpoints (default is to show established TCP connections).

-c Print output as CSV.

-n Don't resolve addresses.

STEPS

Download TCPView

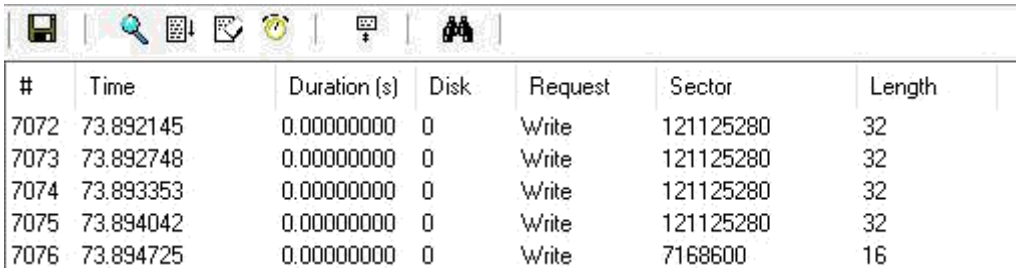


Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets	Sent Bytes	Rcvd Packets	Rcvd Bytes
chrome.exe	5808	TCP	desktop-vgrdiru	16323	sa-in-f188.1e100.net	5228	ESTABLISHED				
chrome.exe	5808	TCP	desktop-vgrdiru	16475	111.221.29.254	https	ESTABLISHED				
chrome.exe	5808	TCP	desktop-vgrdiru	16477	172.217.194.157	https	ESTABLISHED				
chrome.exe	5808	TCP	desktop-vgrdiru	16485	bom05s11-in-f14.1...	https	ESTABLISHED				
chrome.exe	5808	TCP	desktop-vgrdiru	16501	bom07s15-in-f10.1...	https	ESTABLISHED				
chrome.exe	5808	TCP	desktop-vgrdiru	16520	40.77.226.250	https	ESTABLISHED	1	3,090	1	436
chrome.exe	5808	TCP	desktop-vgrdiru	16525	151.101.36.133	https	ESTABLISHED				
chrome.exe	5808	TCP	desktop-vgrdiru	16528	52.162.216.193	https	ESTABLISHED				
chrome.exe	5808	TCP	desktop-vgrdiru	16529	52.162.216.193	https	ESTABLISHED				
chrome.exe	5808	TCP	desktop-vgrdiru	16530	52.162.216.193	https	ESTABLISHED				
chrome.exe	5808	UDP	DESKTOP-VGRDI...	5353	*	*				33	695
chrome.exe	5808	UDP	DESKTOP-VGRDI...	5353	*	*					
chrome.exe	5808	UDP	DESKTOP-VGRDI...	5353	*	*					
chrome.exe	5808	UDPV6	[0:0:0:0:0:0:0:0]	5353	*	*					
chrome.exe	5808	UDPV6	[0:0:0:0:0:0:0:0]	5353	*	*					
explorer.exe	3248	TCP	desktop-vgrdiru	16249	52.230.84.0	https	ESTABLISHED				
lsass.exe	796	TCP	DESKTOP-VGRDI...	1540	DESKTOP-VGRDI...	0	LISTENING				
lsass.exe	796	TCPV6	[0:0:0:0:0:0:0:0]	1540	[0:0:0:0:0:0:0:0]	0	LISTENING				
mysqld.exe	2260	TCP	DESKTOP-VGRDI...	3306	DESKTOP-VGRDI...	0	LISTENING				
oracle.exe	2296	TCP	DESKTOP-VGRDI...	1544	DESKTOP-VGRDI...	0	LISTENING				
oracle.exe	2296	TCPV6	[0:0:0:0:0:0:0:0]	1544	[0:0:0:0:0:0:0:0]	0	LISTENING				
oracle.exe	2296	TCPV6	[fe80:0:0:0:68b5:1...	2239	[fe80:0:0:0:68b5:1...	1521	ESTABLISHED	1	414	1	202
services.exe	772	TCP	DESKTOP-VGRDI...	1545	DESKTOP-VGRDI...	0	LISTENING				
services.exe	772	TCPV6	[0:0:0:0:0:0:0:0]	1545	[0:0:0:0:0:0:0:0]	0	LISTENING				
spoolsv.exe	1772	TCP	DESKTOP-VGRDI...	1539	DESKTOP-VGRDI...	0	LISTENING				
spoolsv.exe	1772	TCPV6	[0:0:0:0:0:0:0:0]	1539	[0:0:0:0:0:0:0:0]	0	LISTENING				
svchost.exe	940	TCP	DESKTOP-VGRDI...	epmap	DESKTOP-VGRDI...	0	LISTENING				
svchost.exe	1144	TCP	DESKTOP-VGRDI...	1537	DESKTOP-VGRDI...	0	LISTENING				
svchost.exe	336	TCP	DESKTOP-VGRDI...	1538	DESKTOP-VGRDI...	0	LISTENING				
svchost.exe	1136	UDP	DESKTOP-VGRDI...	ntp	*	*					
svchost.exe	1152	UDP	DESKTOP-VGRDI...	ssdp	*	*					
svchost.exe	1152	UDP	desktop-vgrdiru	ssdp	*	*					
svchost.exe	1152	UDP	DESKTOP-VGRDI...	ws-discovery	*	*					
svchost.exe	1152	UDP	DESKTOP-VGRDI...	ws-discovery	*	*					
svchost.exe	1328	UDP	DESKTOP-VGRDI...	5353	*	*		11	132	33	695
svchost.exe	1328	UDP	DESKTOP-VGRDI...	llmnr	*	*					
svchost.exe	1152	UDP	DESKTOP-VGRDI...	53517	*	*					
svchost.exe	1152	UDP	desktop-vgrdiru	57748	*	*					
svchost.exe	1152	UDP	DESKTOP-VGRDI...	57749	*	*					
svchost.exe	940	TCPV6	[0:0:0:0:0:0:0:0]	epmap	[0:0:0:0:0:0:0:0]	0	LISTENING				
svchost.exe	1144	TCPV6	[0:0:0:0:0:0:0:0]	1537	[0:0:0:0:0:0:0:0]	0	LISTENING				
svchost.exe	336	TCPV6	[0:0:0:0:0:0:0:0]	1538	[0:0:0:0:0:0:0:0]	0	LISTENING				
svchost.exe	1136	UDPV6	[0:0:0:0:0:0:0:0]	123	*	*					

5. Monitor Hard Disk

DiskMon is an application that logs and displays all hard disk activity on a Windows system. You can also minimize *DiskMon* to your system tray where it acts as a disk light, presenting a green icon when there is disk-read activity and a red icon when there is disk-write activity.

Download DiskMon → Run as administrator

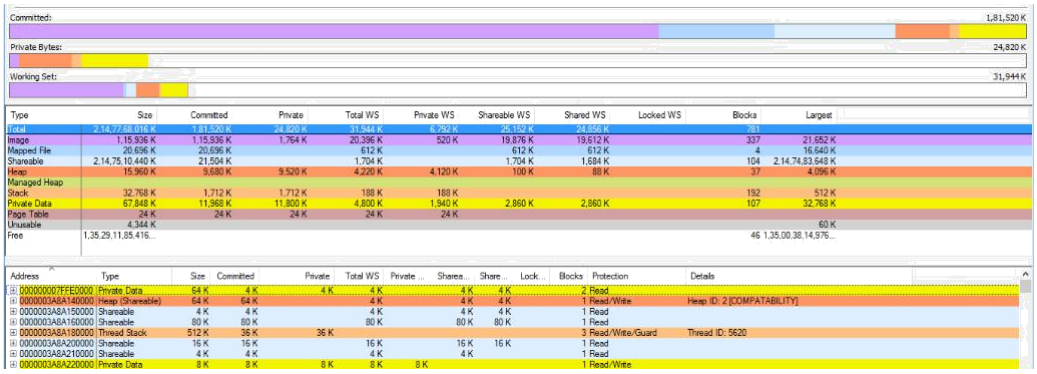


#	Time	Duration (s)	Disk	Request	Sector	Length
7072	73.892145	0.00000000	0	Write	121125280	32
7073	73.892748	0.00000000	0	Write	121125280	32
7074	73.893353	0.00000000	0	Write	121125280	32
7075	73.894042	0.00000000	0	Write	121125280	32
7076	73.894725	0.00000000	0	Write	7168600	16

6.Monitor Virtual Memory

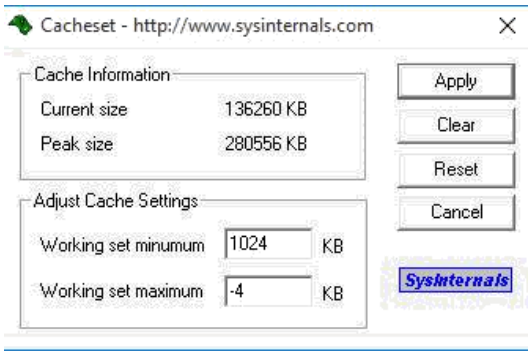
VMMap is a process virtual and physical memory analysis utility. It shows a breakdown of a process's committed virtual memory types as well as the amount of physical memory (working set) assigned by the operating system to those types. Besides graphical representations of memory usage, VMMap also shows summary information and a detailed process memory map. Powerful filtering and refresh capabilities allow you to identify the sources of process memory usage and the memory cost of application features

sysinternal → VMMap



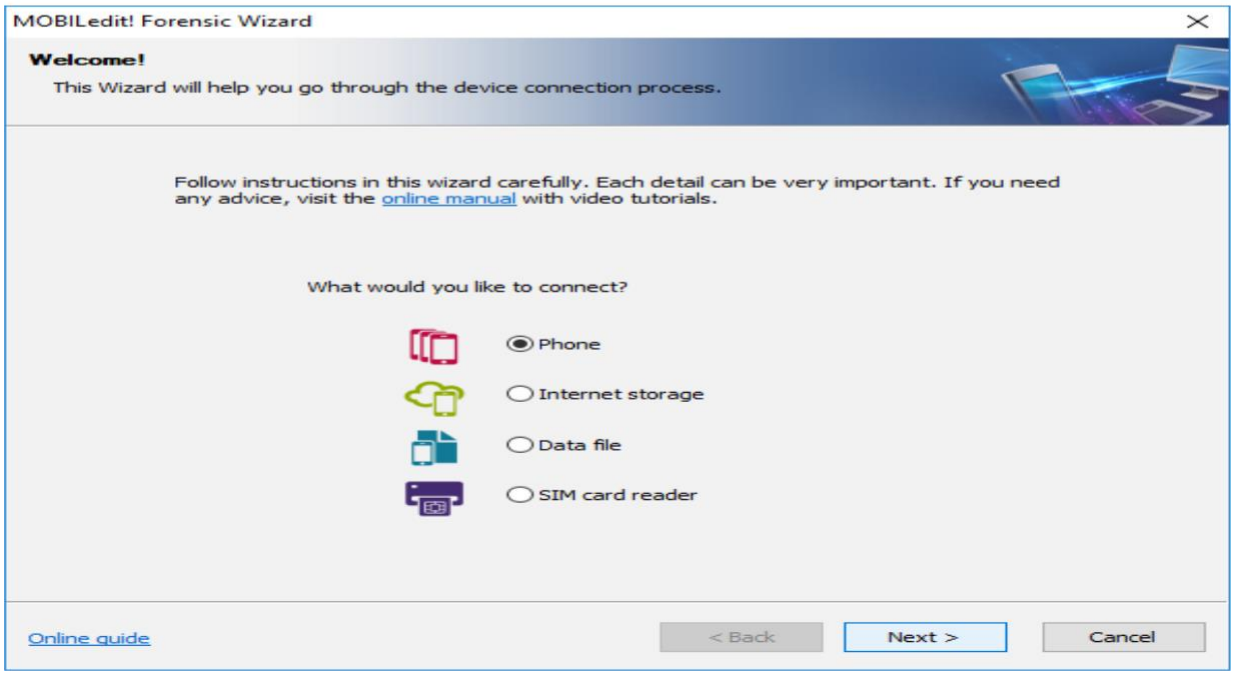
7.Monitor Cache Memory

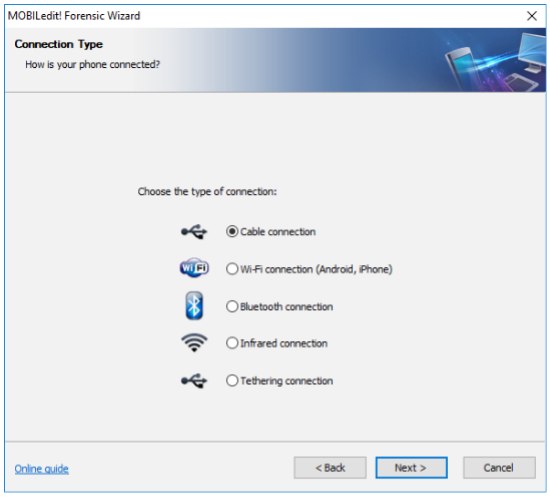
CacheSet is an applet that allows you to manipulate the working-set parameters of the system file cache. Unlike CacheMan, *CacheSet* runs on all versions of NT and will work without modifications on new Service Pack releases. In addition to providing you the ability to control the minimum and maximum working set sizes, it also allows you to reset the Cache's working set, forcing it to grow as necessary from a minimal starting point. Also unlike CacheMan, changes made with *CacheSet* have an immediate effect on the size of the Cache.

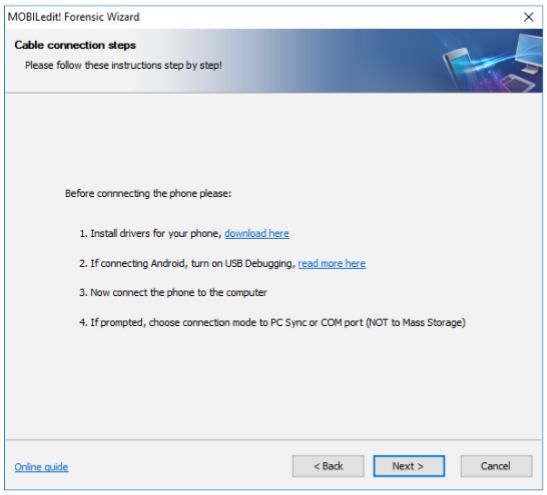


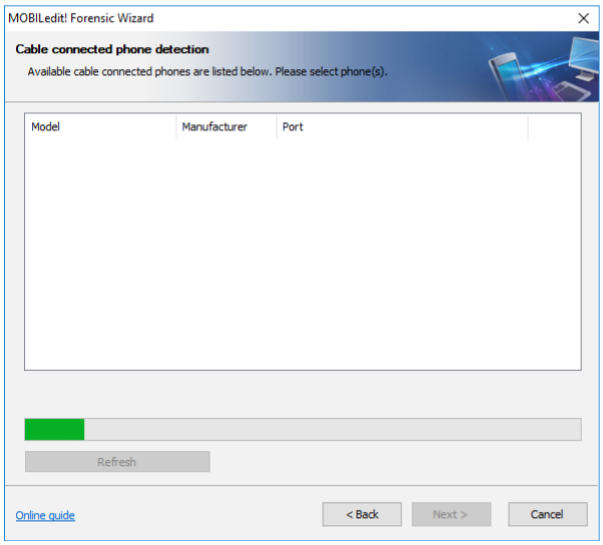
PRACTICAL 7

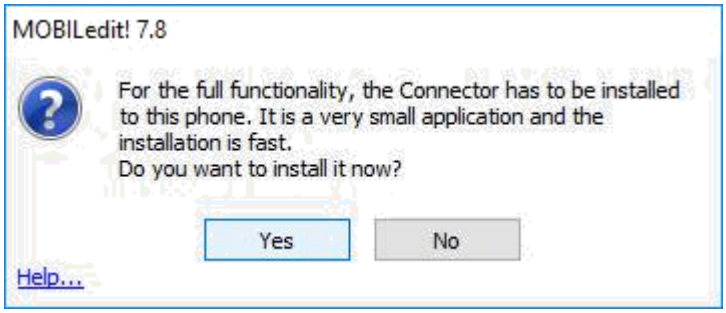
AIM: Investigate the Mobile Device.

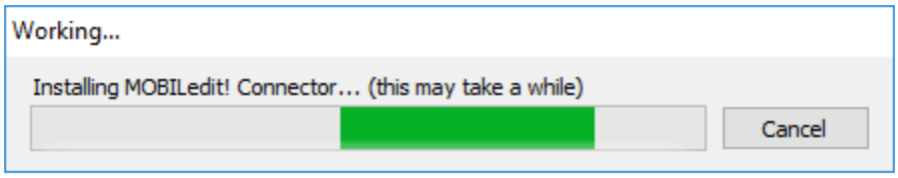


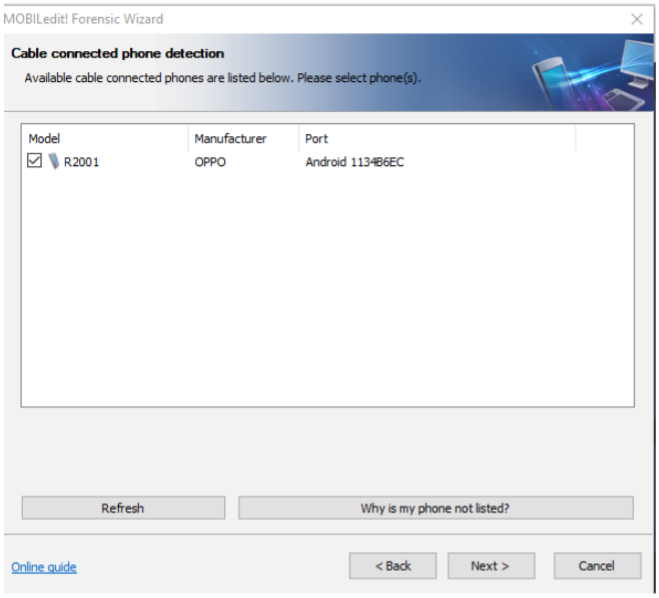

MOBILedit! Forensic Wizard
Connection Type
How is your phone connected?
Choose the type of connection:
Cable connection
Wi-Fi connection (Android, iPhone)
Bluetooth connection
Infrared connection
Tethering connection
Online guide
< Back
Next >
Cancel

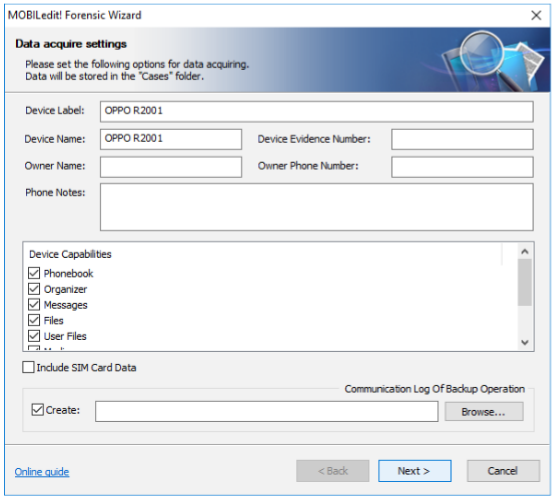

MOBILedit! Forensic Wizard
Cable connection steps
Please follow these instructions step by step!
Before connnecting the phone please:
1. Install drivers for your phone, download here
2. If connecting Android, turn on USB Debugging, read more here
3. Now connect the phone to the computer
4. If prompted, choose connection mode to PC Sync or COM port (NOT to Mass Storage)
Online guide
< Back
Next >
Cancel

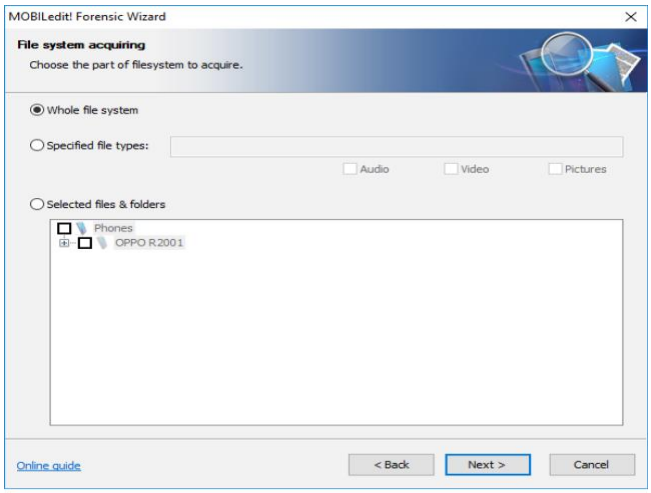

MOBILedit! Forensic Wizard
Cable connected phone detection
Available cable connected phones are listed below. Please select phone(s).
Model
Manufacturer
Port
Refresh
Online guide
< Back
Next >
Cancel

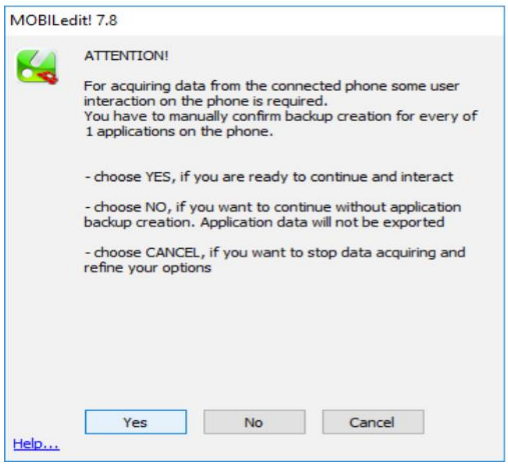

MOBILedit! 7.8
For the full functionality, the Connector has to be installed to this phone. It is a very small application and the installation is fast.
Do you want to install it now?
Yes
No
Help...

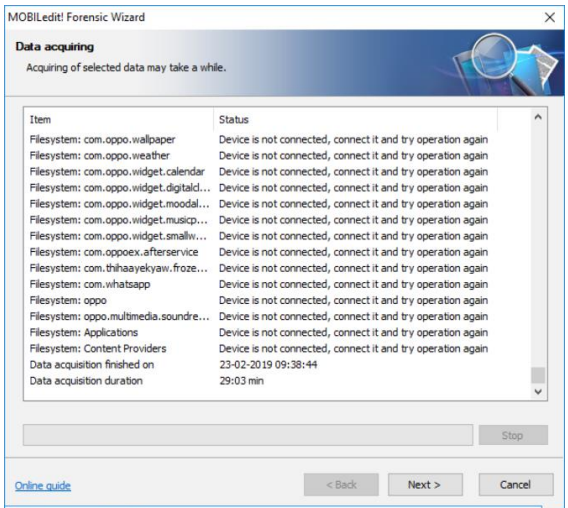

Working...
Installing MOBILedit! Connector... (this may take a while)
Cancel

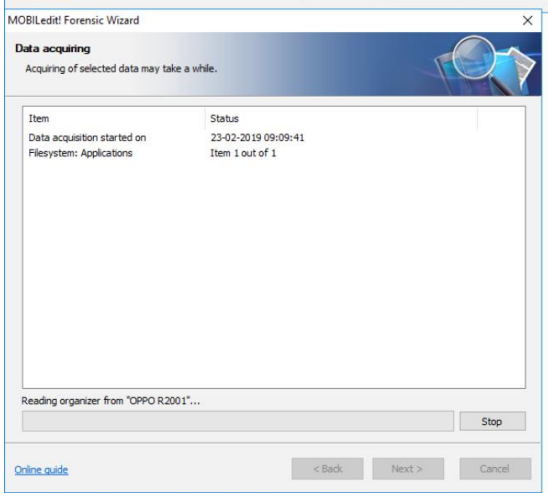

MOBILedit! Forensic Wizard
Cable connected phone detection
Available cable connected phones are listed below. Please select phone(s).
Model
Manufacturer
Port
R2001
OPPO
Android 1134B6EC
Refresh
Why is my phone not listed?
Online guide
< Back
Next >
Cancel

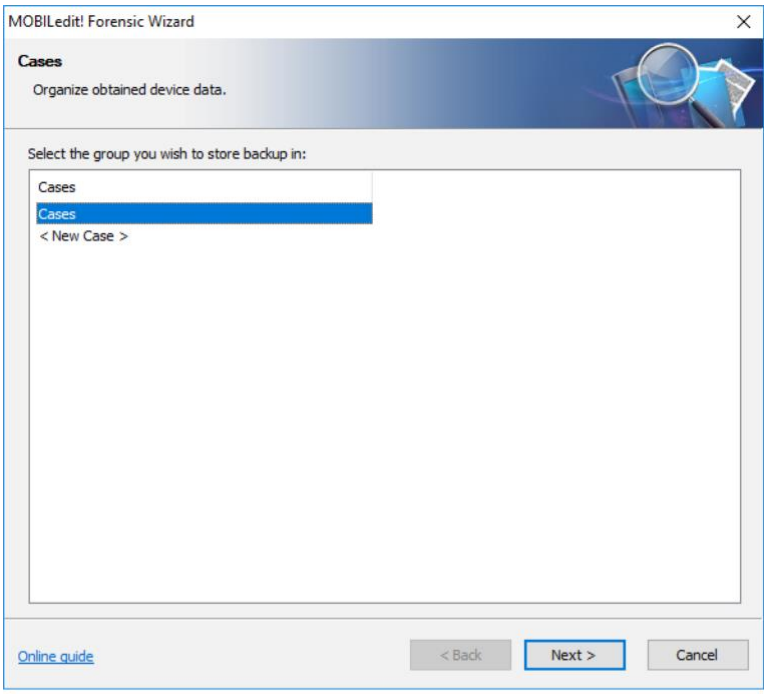

MOBILedit! Forensic Wizard
Data acquire settings
Please set the following options for data acquiring.
Data will be stored in the "Cases" folder.
Device Label:
OPPO R2001
Device Name:
OPPO R2001
Device Evidence Number:
Owner Name:
Owner Phone Number:
Phone Notes:
Device Capabilities
Phonebook
Organizer
Messages
Files
User Files
Include SIM Card Data
Communication Log Of Backup Operation
Create:
Browse...
Online guide
< Back
Next >
Cancel

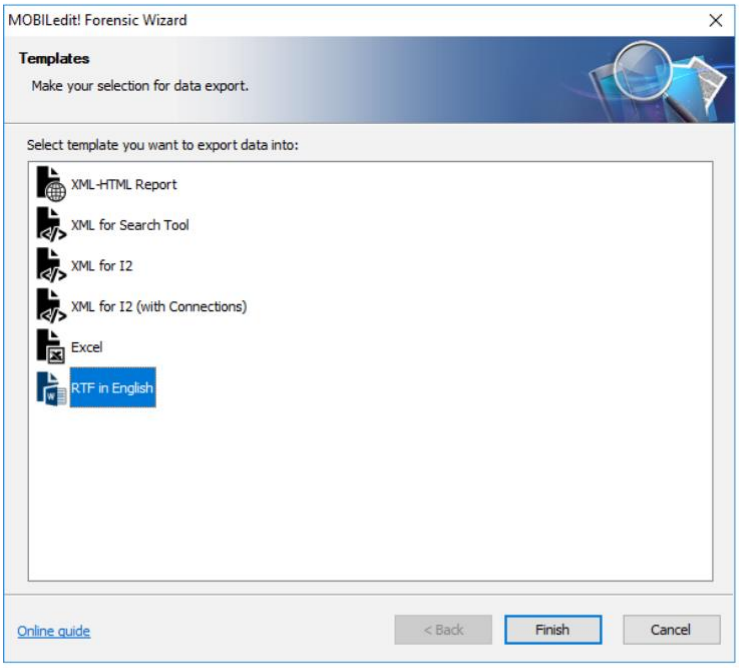

MOBILedit! Forensic Wizard
File system acquiring
Choose the part of filesystem to acquire.
Whole file system
Specified file types:
Audio
Video
Pictures
Selected files & folders
Phones
OPPO R2001
Online guide
< Back
Next >
Cancel

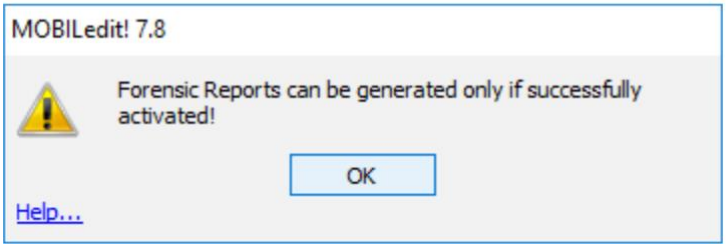

MOBILedit! 7.8
ATTENTION!
For acquiring data from the connected phone some user interaction on the phone is required.
You have to manually confirm backup creation for every of 1 applications on the phone.
- choose YES, if you are ready to continue and interact
- choose NO, if you want to continue without 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...

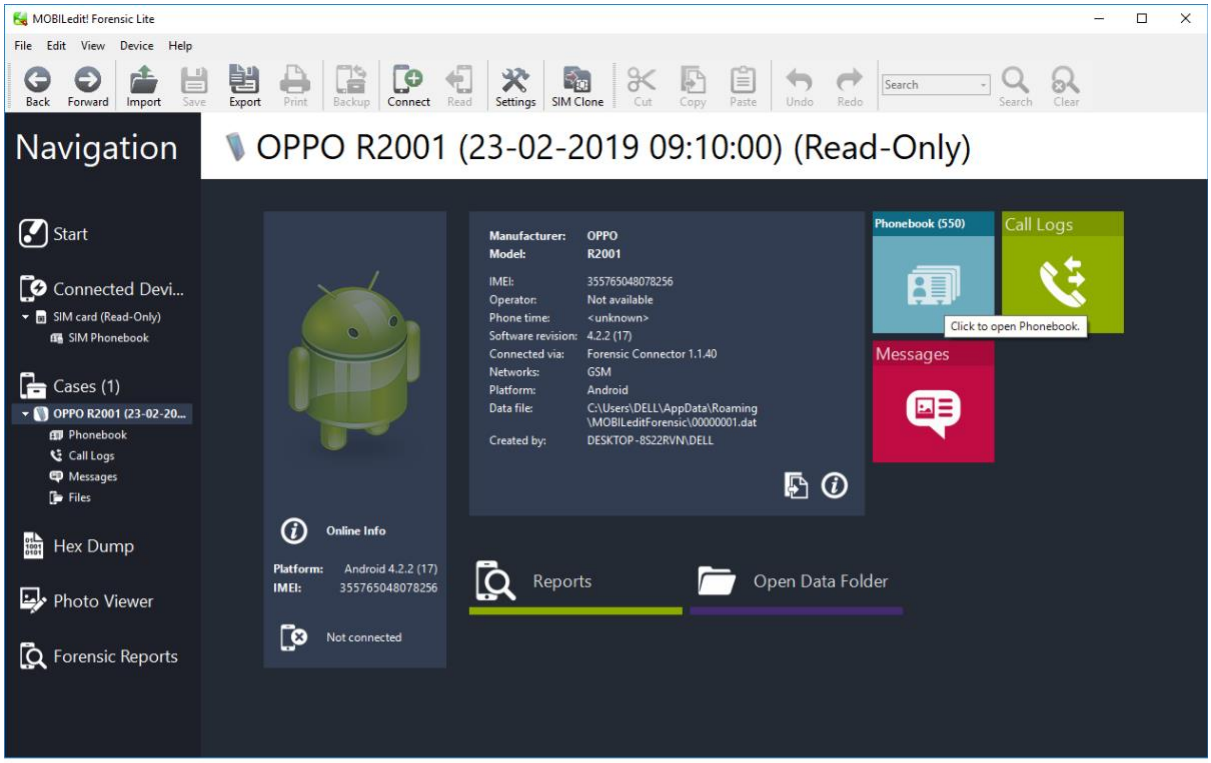

MOBILedit! Forensic Wizard
Data acquiring
Acquiring of selected data may take a while.
Item
Status
Filesystem: com.oppo.wallpaper
Device is not connected, connect it and try operation again
Filesystem: com.oppo.weather
Device is not connected, connect it and try operation again
Filesystem: com.oppo.widget.calendar
Device is not connected, connect it and try operation again
Filesystem: com.oppo.widget.digitalcl...
Device is not connected, connect it and try operation again
Filesystem: com.oppo.widget.moodal...
Device is not connected, connect it and try operation again
Filesystem: com.oppo.widget.musicp...
Device is not connected, connect it and try operation again
Filesystem: com.oppo.widget.smallw...
Device is not connected, connect it and try operation again
Filesystem: com.oppoex.afterservice
Device is not connected, connect it and try operation again
Filesystem: com.thihaayekyaw.froze...
Device is not connected, connect it and try operation again
Filesystem: com.whatsapp
Device is not connected, connect it and try operation again
Filesystem: oppo
Device is not connected, connect it and try operation again
Filesystem: oppo.multimedia.soundre...
Device is not connected, connect it and try operation again
Filesystem: Applications
Device is not connected, connect it and try operation again
Filesystem: Content Providers
Device is not connected, connect it and try operation again
Data acquisition finished on
23-02-2019 09:38:44
Data acquisition duration
29:03 min
Stop
Online guide
< Back
Next >
Cancel

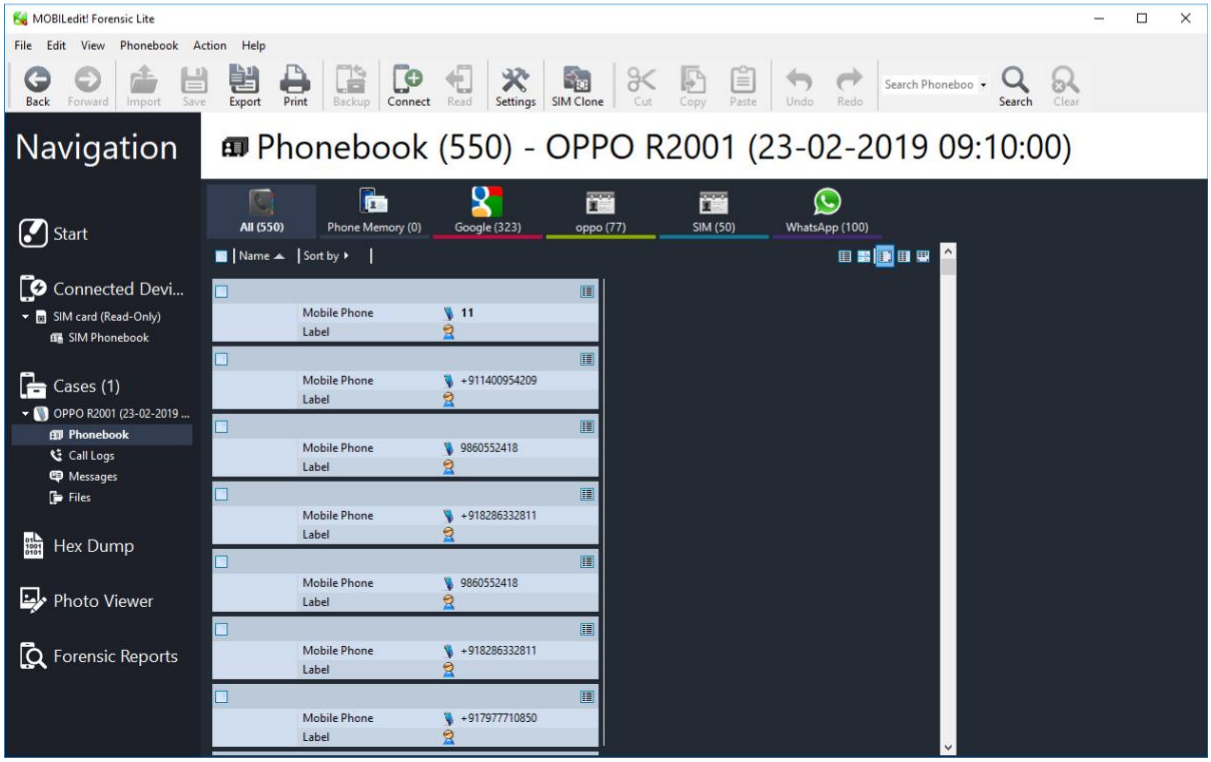

MOBILedit! Forensic Wizard
Data acquiring
Acquiring of selected data may take a while.
Item
Status
Data acquisition started on
23-02-2019 09:09:41
Filesystem: Applications
Item 1 out of 1
Reading organizer from "OPPO R2001"...
Stop
Online guide
< Back
Next >
Cancel

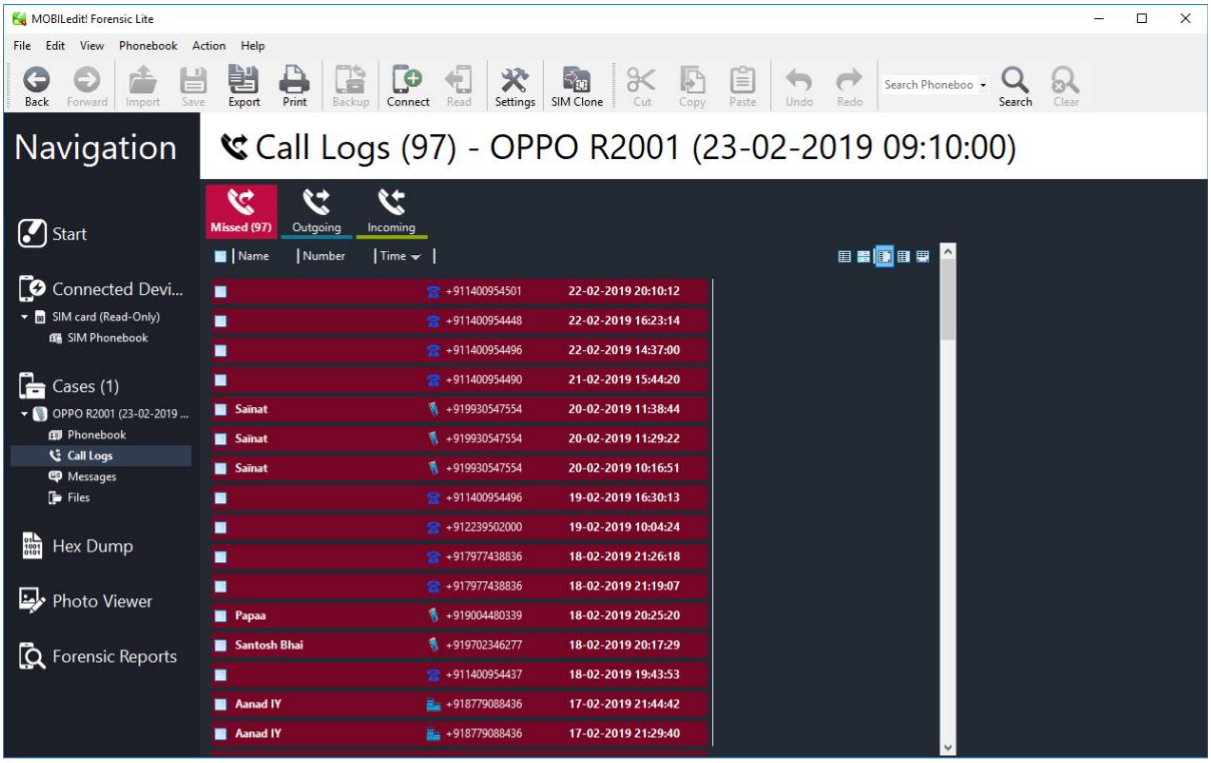

MOBILedit! Forensic Wizard
Cases
Organize obtained device data.
Select the group you wish to store backup in:
Cases
Cases
< New Case >
Online guide
< Back
Next >
Cancel

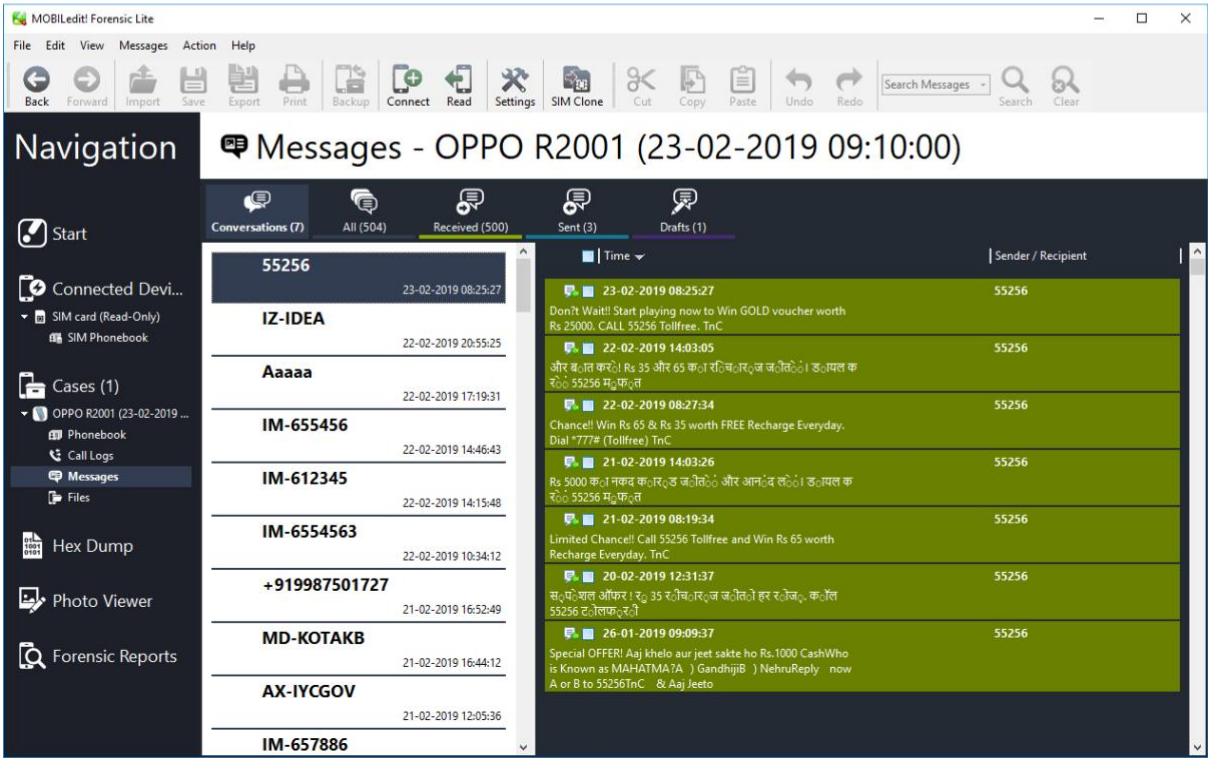

MOBILedit! Forensic Wizard
Templates
Make your selection for data export.
Select template you want to export data into:
XML-HTML Report
XML for Search Tool
XML for I2
XML for I2 (with Connections)
Excel
RTF in English
Online guide
< Back
Finish
Cancel


MOBILedit! 7.8
Forensic Reports can be generated only if successfully activated!
OK
Help...


MOBILedit! Forensic Lite
File Edit View Device Help
Back Forward Import Save Export Print Backup Connect Read Settings SIM Clone Cut Copy Paste Undo Redo Search Search Clear
Navigation
OPPO R2001 (23-02-2019 09:10:00) (Read-Only)
Start
Connected Devi...
SIM card (Read-Only)
SIM Phonebook
Cases (1)
OPPO R2001 (23-02-20...
Phonebook
Call Logs
Messages
Files
Hex Dump
Photo Viewer
Forensic Reports
Manufacturer: OPPO
Model: R2001
IMEI: 355765048078256
Operator: Not available
Phone time: <unknown>
Software revision: 4.2.2 (17)
Connected via: Forensic Connector 1.1.40
Networks: GSM
Platform: Android
Data file: C:\Users\DELL\AppData\Roaming\MOBILeditForensic\00000001.dat
Created by: DESKTOP-8S22RVN\DELL
Phonebook (550)
Call Logs
Click to open Phonebook.
Messages
Online Info
Platform: Android 4.2.2 (17)
IMEI: 355765048078256
Not connected
Reports
Open Data Folder


MOBILedit! Forensic Lite
File Edit View Phonebook Action Help
Back Forward Import Save Export Print Backup Connect Read Settings SIM Clone Cut Copy Paste Undo Redo Search Phoneboo Search Clear
Navigation
Phonebook (550) - OPPO R2001 (23-02-2019 09:10:00)
Start
Connected Devi...
SIM card (Read-Only)
SIM Phonebook
Cases (1)
OPPO R2001 (23-02-2019 ...
Phonebook
Call Logs
Messages
Files
Hex Dump
Photo Viewer
Forensic Reports
All (550)
Phone Memory (0)
Google (323)
oppo (77)
SIM (50)
WhatsApp (100)
Name
Sort by
Mobile Phone 11
Label
Mobile Phone +911400954209
Label
Mobile Phone 9860552418
Label
Mobile Phone +918286332811
Label
Mobile Phone 9860552418
Label
Mobile Phone +918286332811
Label
Mobile Phone +917977710850
Label


MOBILedit! Forensic Lite
File Edit View Phonebook Action Help
Back Forward Import Save Export Print Backup Connect Read Settings SIM Clone Cut Copy Paste Undo Redo Search Phoneboo Search Clear
Navigation
Call Logs (97) - OPPO R2001 (23-02-2019 09:10:00)
Start
Connected Devi...
SIM card (Read-Only)
SIM Phonebook
Cases (1)
OPPO R2001 (23-02-2019 ...
Phonebook
Call Logs
Messages
Files
Hex Dump
Photo Viewer
Forensic Reports
Missed (97)
Outgoing
Incoming
Name
Number
Time
+911400954501 22-02-2019 20:10:12
+911400954448 22-02-2019 16:23:14
+911400954496 22-02-2019 14:37:00
+911400954490 21-02-2019 15:44:20
Saïnat +919930547554 20-02-2019 11:38:44
Saïnat +919930547554 20-02-2019 11:29:22
Saïnat +919930547554 20-02-2019 10:16:51
+911400954496 19-02-2019 16:30:13
+912239502000 19-02-2019 10:04:24
+917977438836 18-02-2019 21:26:18
+917977438836 18-02-2019 21:19:07
Papaa +919004480339 18-02-2019 20:25:20
Santosh Bhai +919702346277 18-02-2019 20:17:29
+911400954437 18-02-2019 19:43:53
Aanad IY +918779088436 17-02-2019 21:44:42
Aanad IY +918779088436 17-02-2019 21:29:40


MOBILedit! Forensic Lite
File Edit View Messages Action Help
Back Forward Import Save Export Print Backup Connect Read Settings SIM Clone Cut Copy Paste Undo Redo Search Messages Search Clear
Navigation
Messages - OPPO R2001 (23-02-2019 09:10:00)
Start
Connected Devi...
SIM card (Read-Only)
SIM Phonebook
Cases (1)
OPPO R2001 (23-02-2019 ...
Phonebook
Call Logs
Messages
Files
Hex Dump
Photo Viewer
Forensic Reports
Conversations (7)
All (504)
Received (500)
Sent (3)
Drafts (1)
55256 23-02-2019 08:25:27
IZ-IDEA 22-02-2019 20:55:25
Aaaaa 22-02-2019 17:19:31
IM-655456 22-02-2019 14:46:43
IM-612345 22-02-2019 14:15:48
IM-6554563 22-02-2019 10:34:12
+919987501727 21-02-2019 16:52:49
MD-KOTAKB 21-02-2019 16:44:12
AX-IYCGOV 21-02-2019 12:05:36
IM-657886
Time
Sender / Recipient
23-02-2019 08:25:27 55256
Don?t Wait!! Start playing now to Win GOLD voucher worth Rs 25000. CALL 55256 Tollfree. TnC
22-02-2019 14:03:05 55256
और बात करो! Rs 35 और 65 का रिचारज जीतो। डायल क रो 55256 मुफ्त
22-02-2019 08:27:34 55256
Chance!! Win Rs 65 & Rs 35 worth FREE Recharge Everyday. Dial *777# (Tollfree) TnC
21-02-2019 14:03:26 55256
Rs 5000 का नकद कारड जीतो और आनंद लो। डायल क रो 55256 मुफ्त
21-02-2019 08:19:34 55256
Limited Chance!! Call 55256 Tollfree and Win Rs 65 worth Recharge Everyday. TnC
20-02-2019 12:31:37 55256
सुपरशल ऑफर ! रु 35 रीचारज जीतो हर रोज. कॉल 55256 टोलफ्रीरी
26-01-2019 09:09:37 55256
Special OFFER! Aaj khelo aur jeet sakte ho Rs.1000 CashWho is Known as MAHATMA?A) GandhijiB) NehruReply now A or B to 55256TnC & Aaj Jeeto

PRACTICAL 8

AIM: Investigate Email File Given.

FTK can filter or find files specific to e-mail clients and servers. You can configure these filters when you enter search parameters.

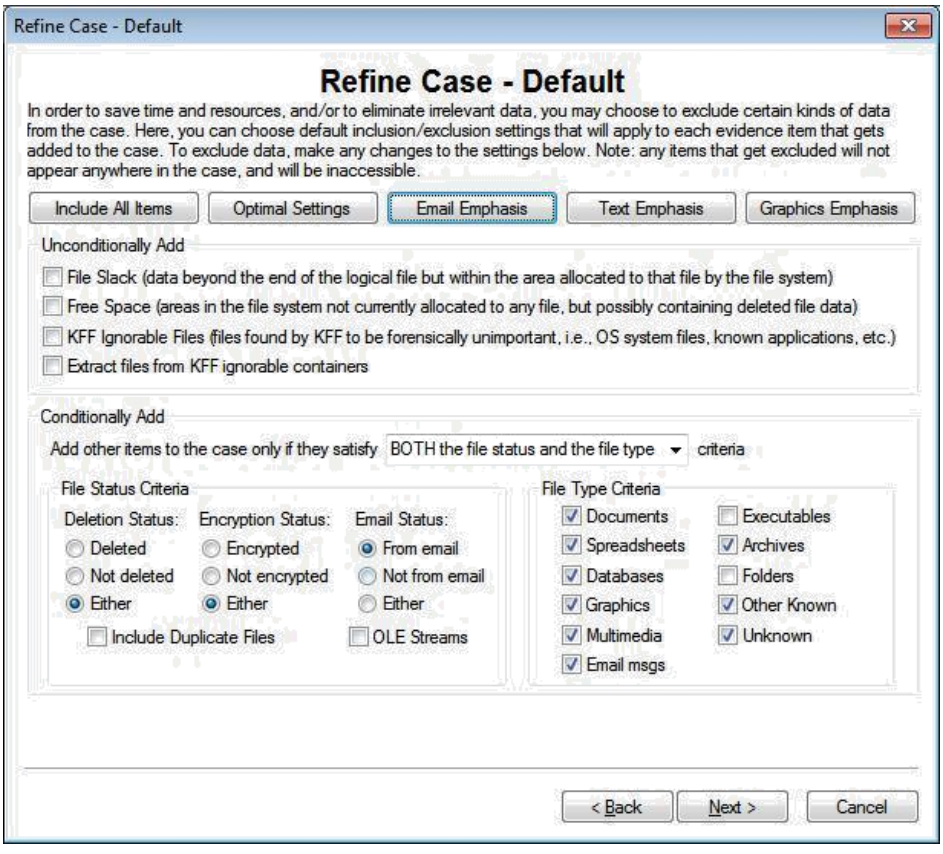
Because of Jim's responses to a poor performance review, the CEO of Superior Bicycles,Martha Dax, suspects he might have obtained sensitive information about the company's business model that he's leaking to a competitor.

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

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

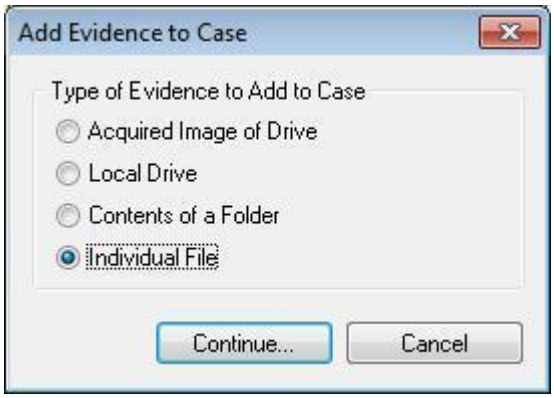
Recovering Email

Start AccessData FTK and click **Start a new case**, then click **OK**. Click **Next** until you reach the **Refine Case - Default** dialog box Click the **Email Emphasis** button, and then click **Next**

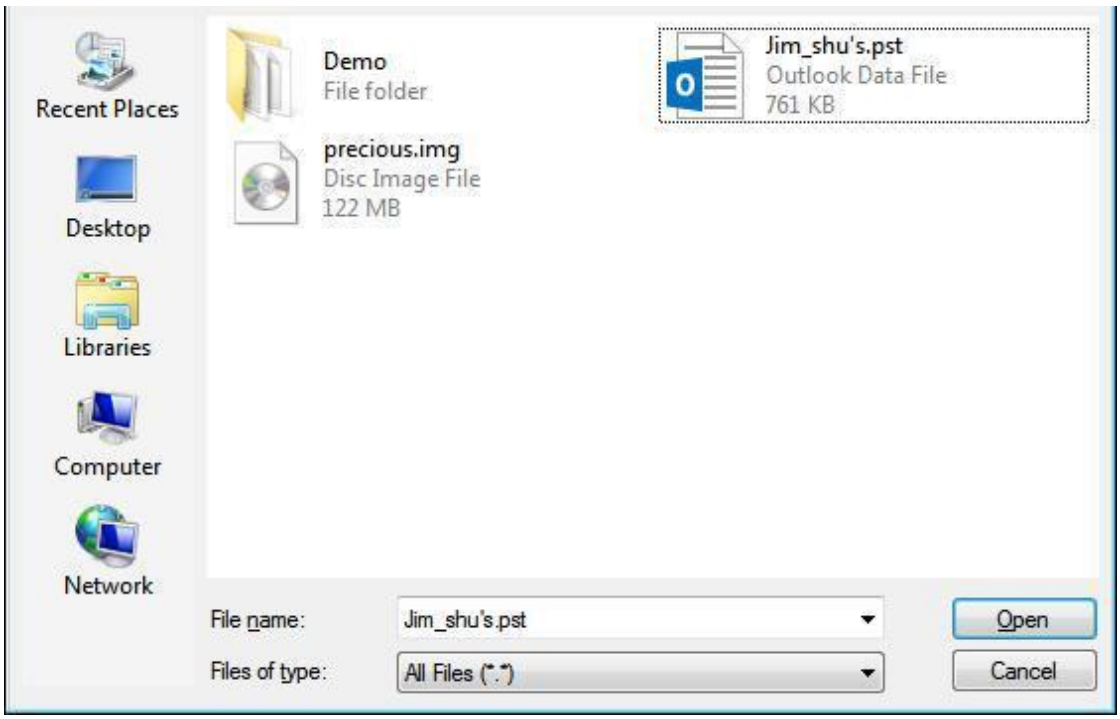


Click **Next** until you reach the **Add Evidence to Case** dialog box, and then click the **Add Evidence** button.

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

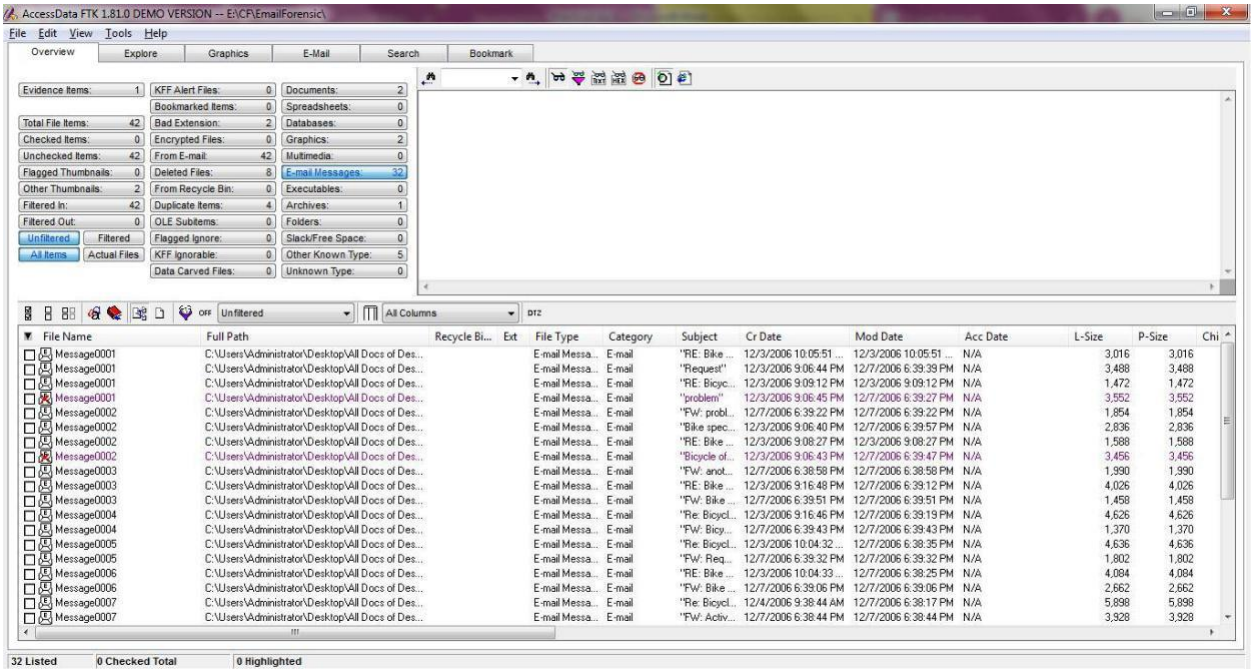


In the **Select File** dialog box, navigate to your work folder, click the **Jim_shu's.pst file**, and then click **Open**.



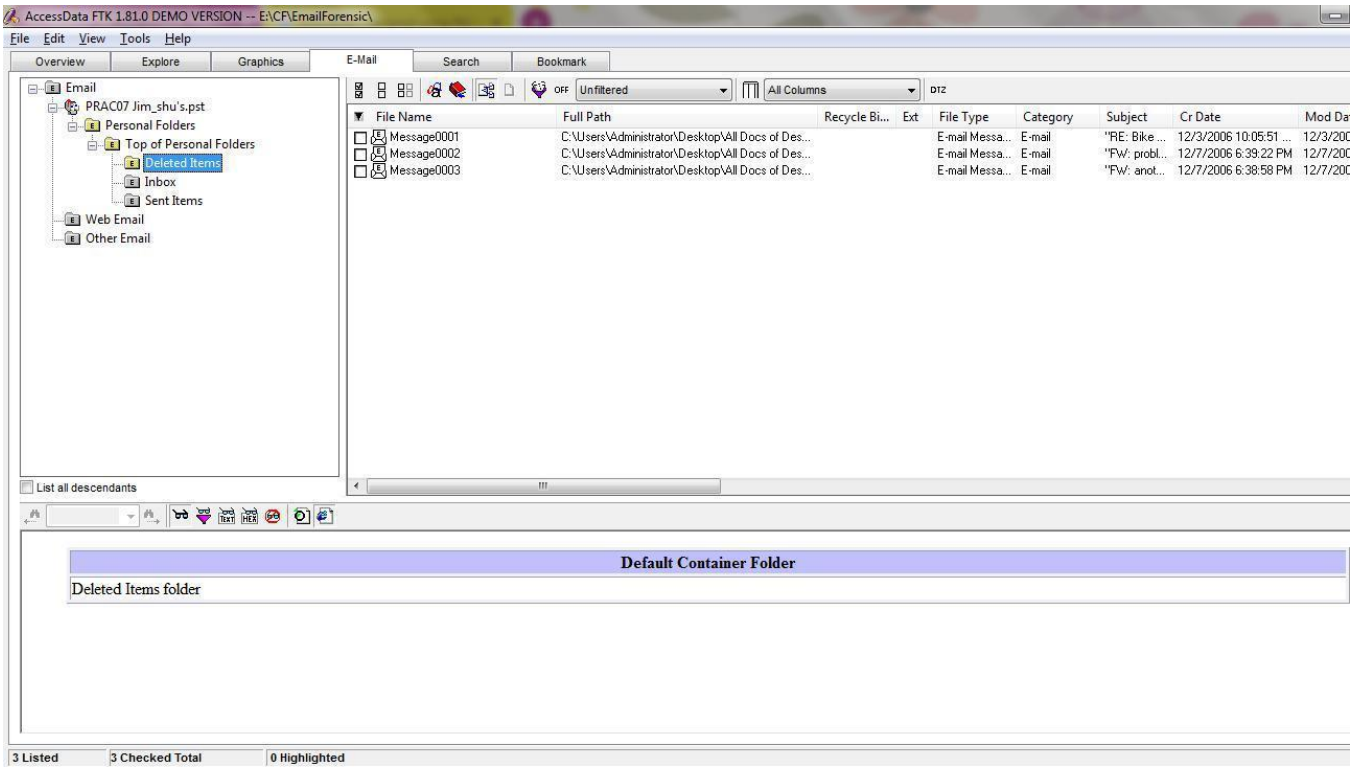
When the **Add Evidence to Case** dialog box opens, click **Next**. In the **Case summary** dialog box, click **Finish**.

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

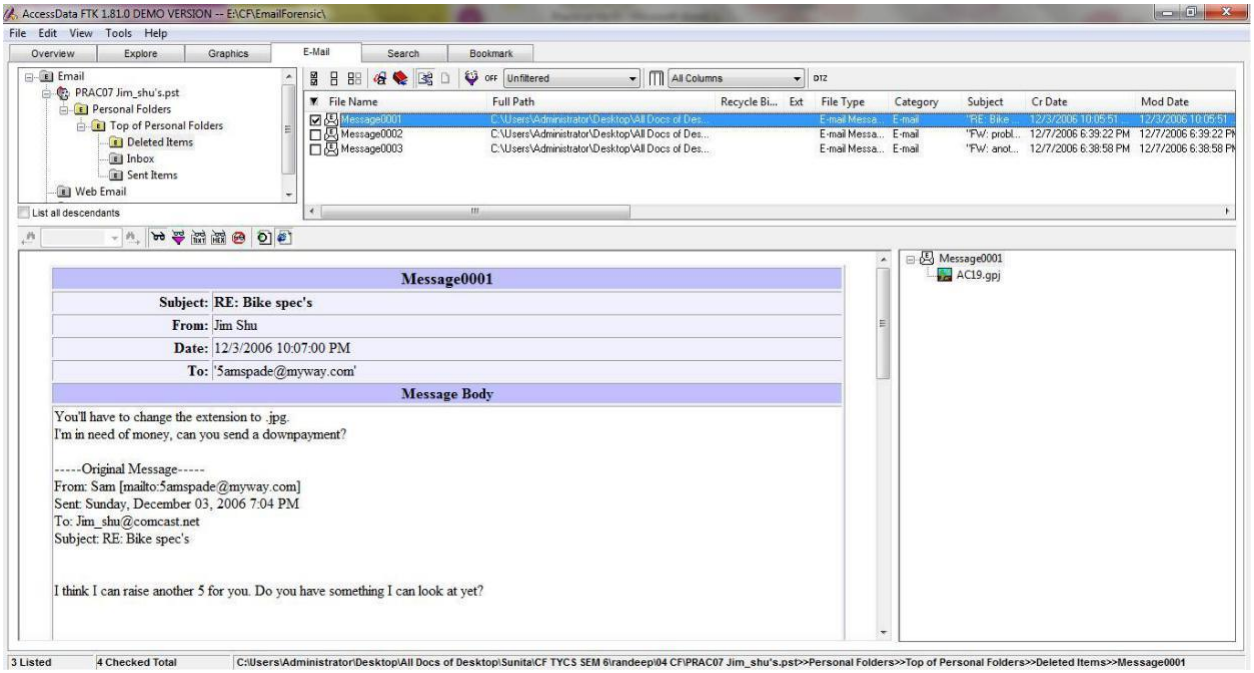


For email recovery follow following steps:

Click the **E-Mail** tab. In the tree view, click to expand all folders, and then click the **Deleted Items** folder.



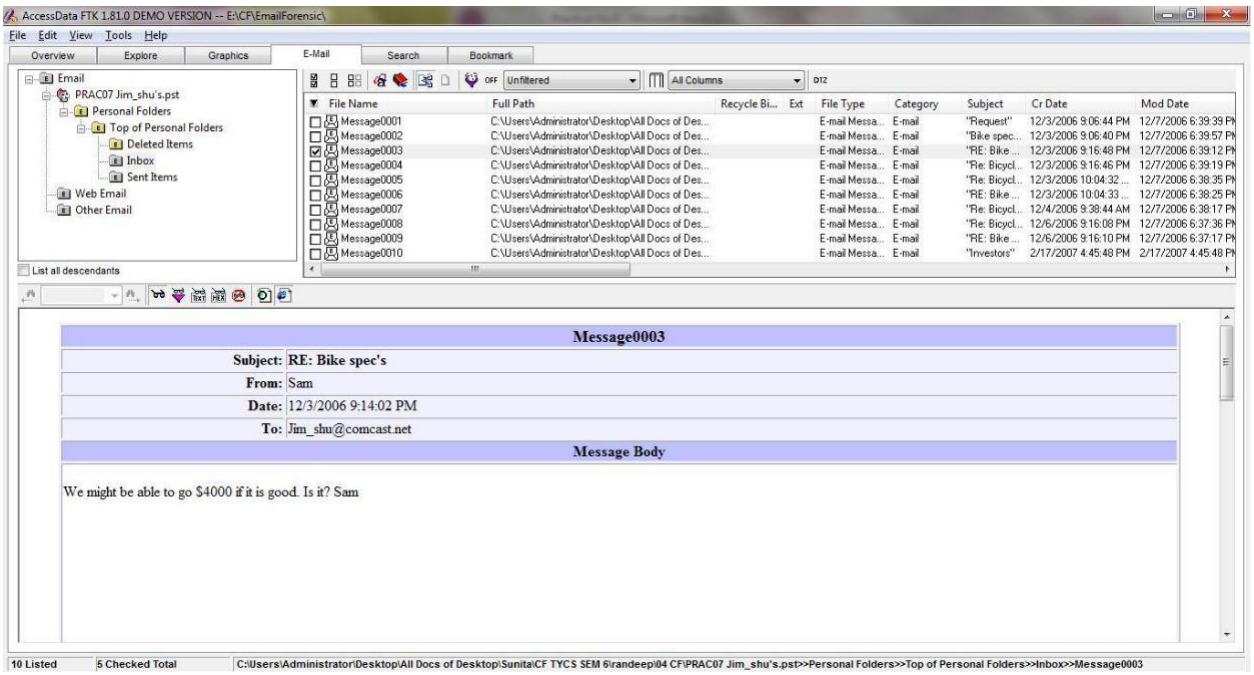
Select any message say Message0001 right click and select option Launch Detached Viewer and you can see detail of deleted message.



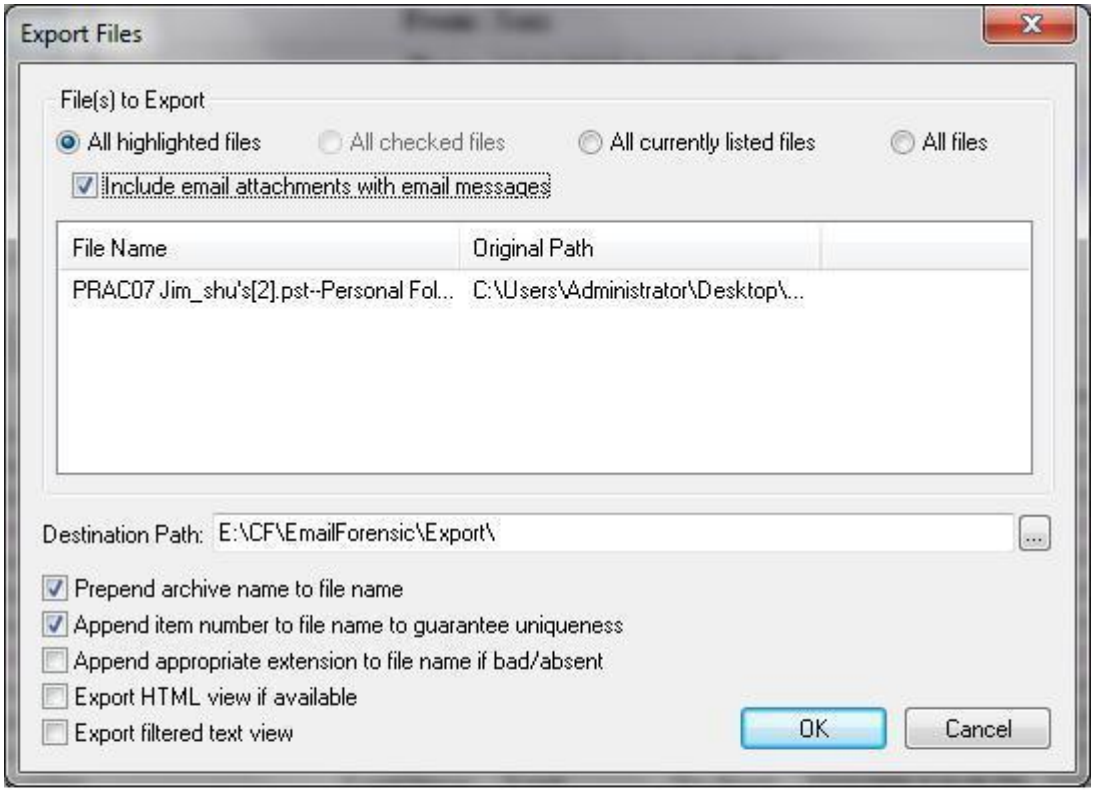
For analyzing header follow following steps:

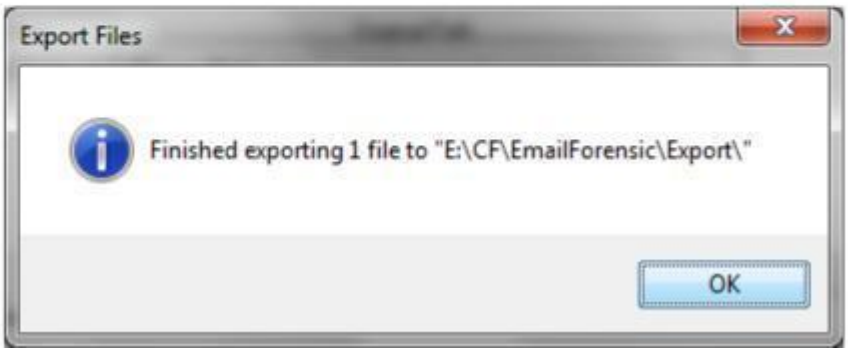
Click the **E-Mail** tab. In the tree view, click to expand all folders, and then click the **Inbox** folder.

In the File List pane at the upper right, click Message0003; as shown in the pane at the bottom, it's from **Sam** and is addressed to**Jim_shu@comcast.net.**

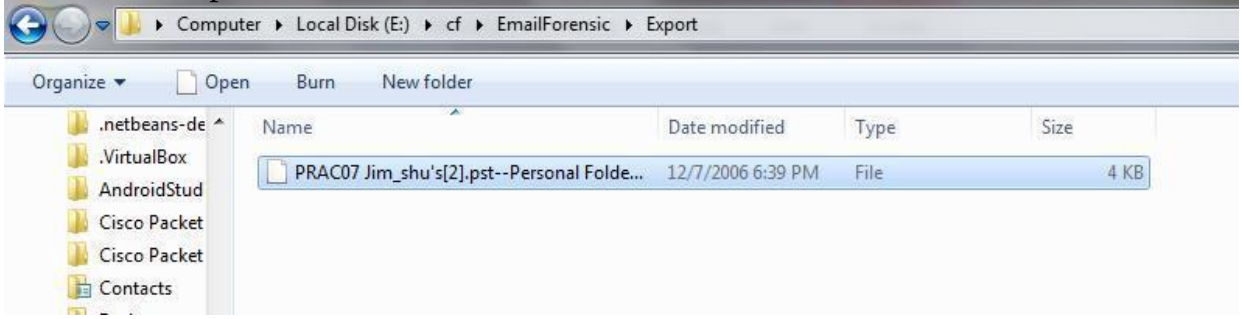


Right-click on any message say Message0003 in the File List pane and click Export File. In the Export Files dialog box, click OK.

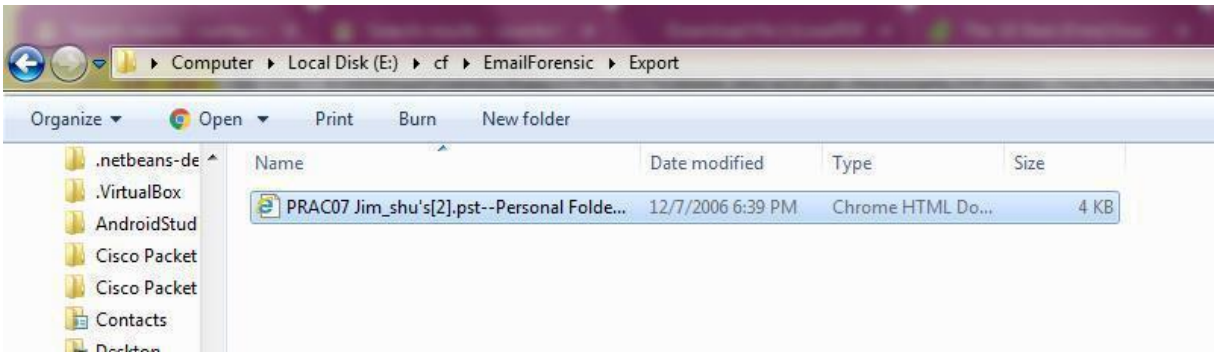




FTK saves exported files in the HTML format with no extension.



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



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

PRACTICAL 9

Aim: Web Browser Forensics .

-Web Browser working

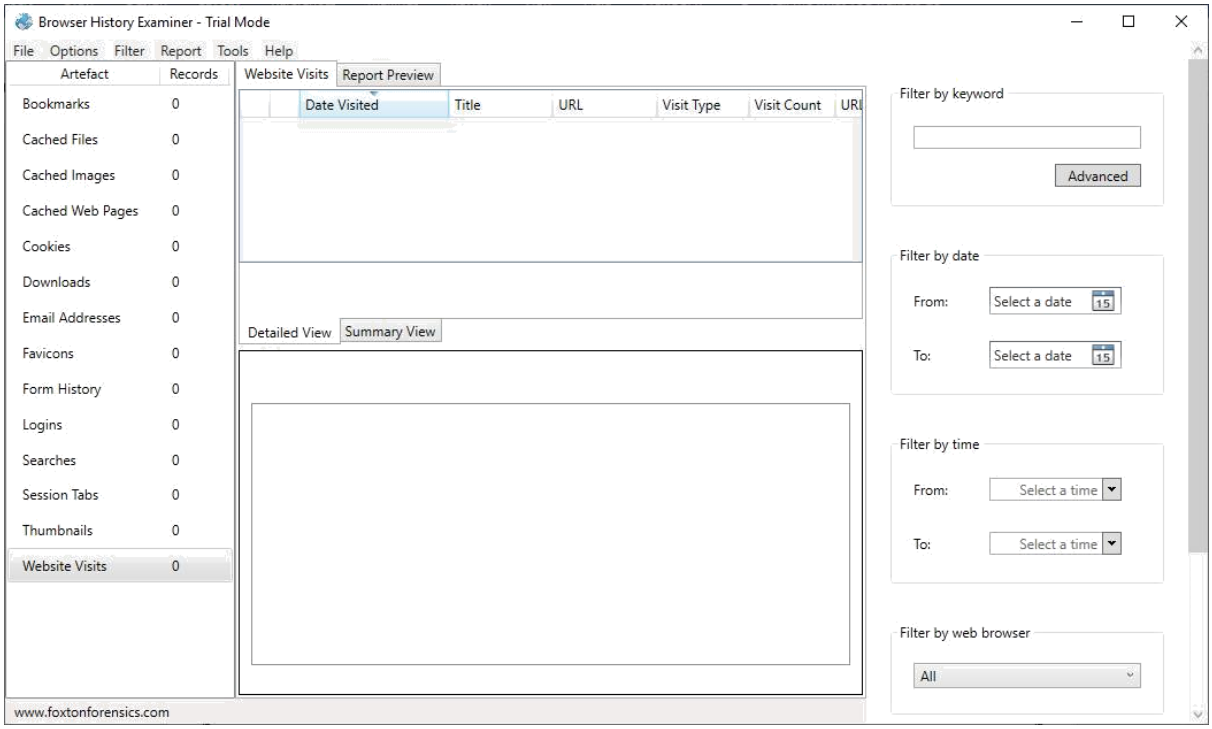
-Forensics activities on browser

-Cache / Cookies analysis

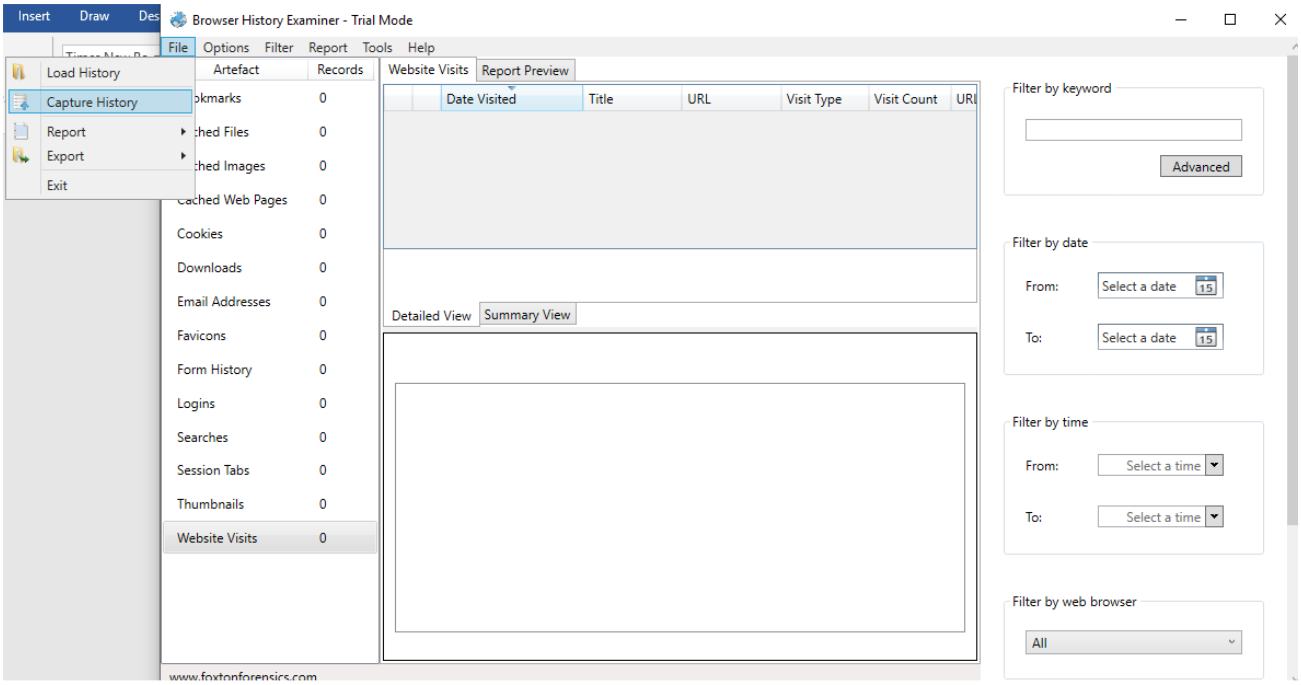
-Last Internet activity

Steps:

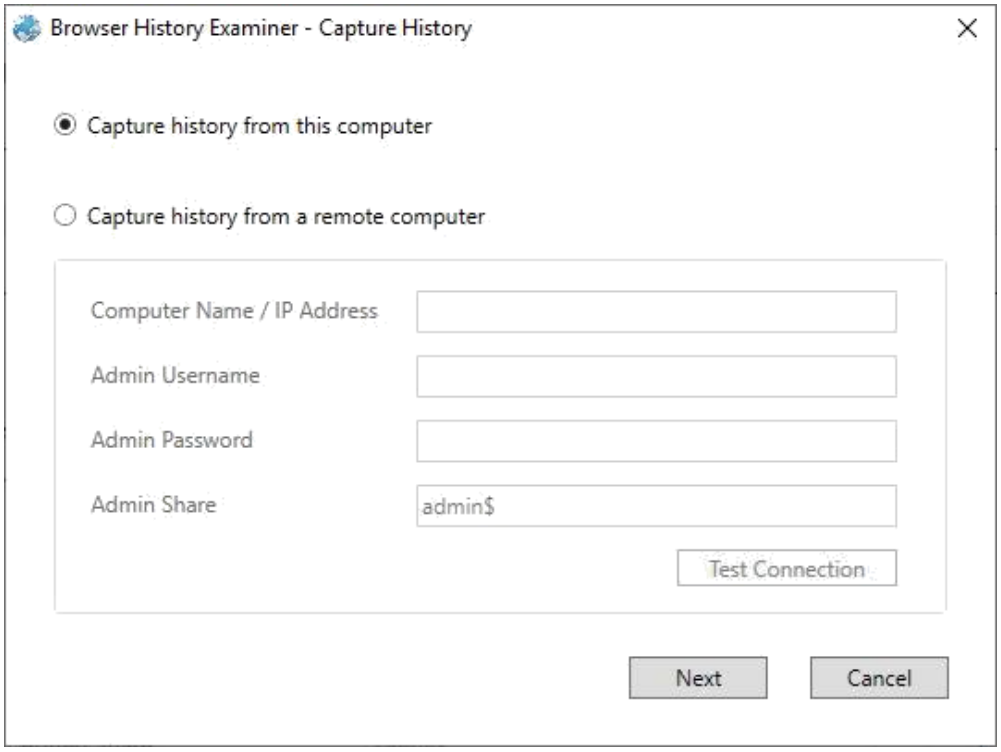
1. Open BrowserHistoryExaminer.



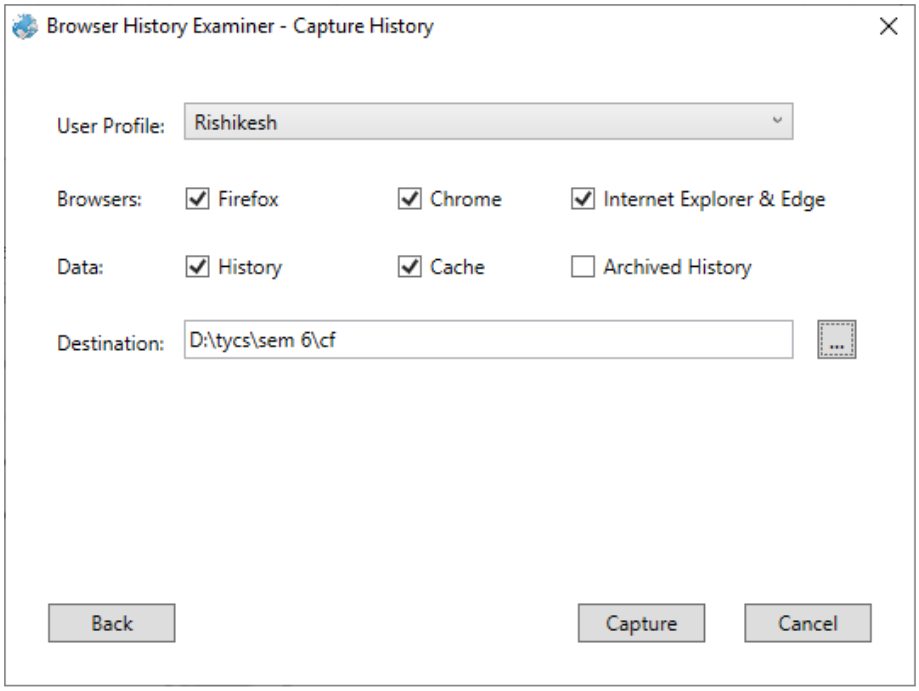
2. Click on file > Capture History



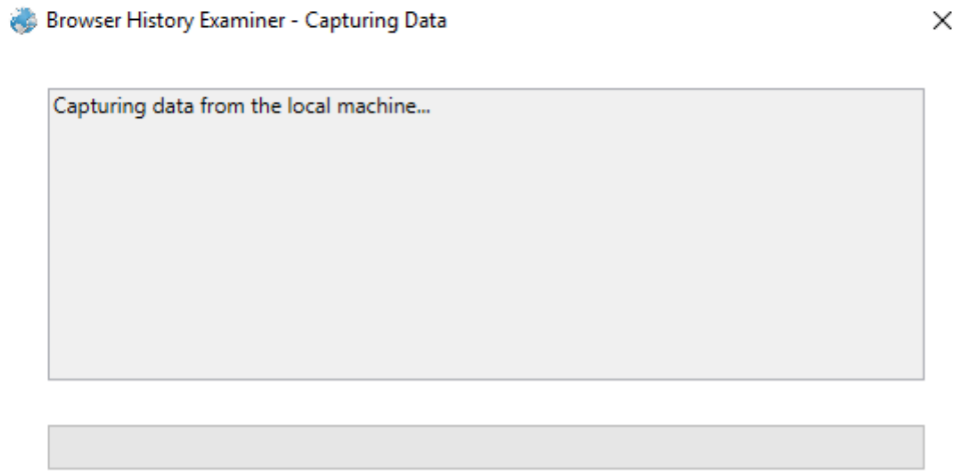
3. Select the capture folder and click on next.

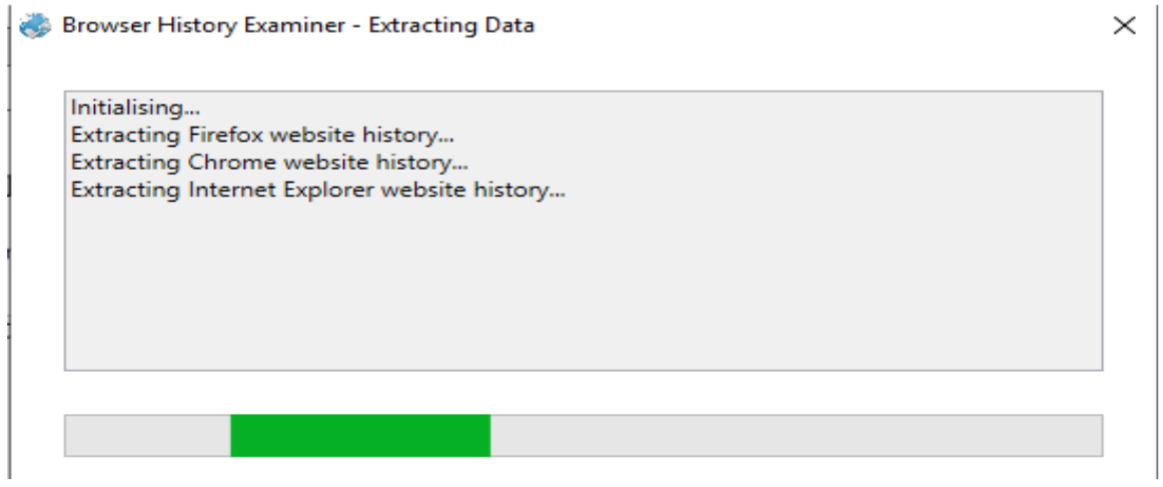


4. Enter the destination to capture the data.

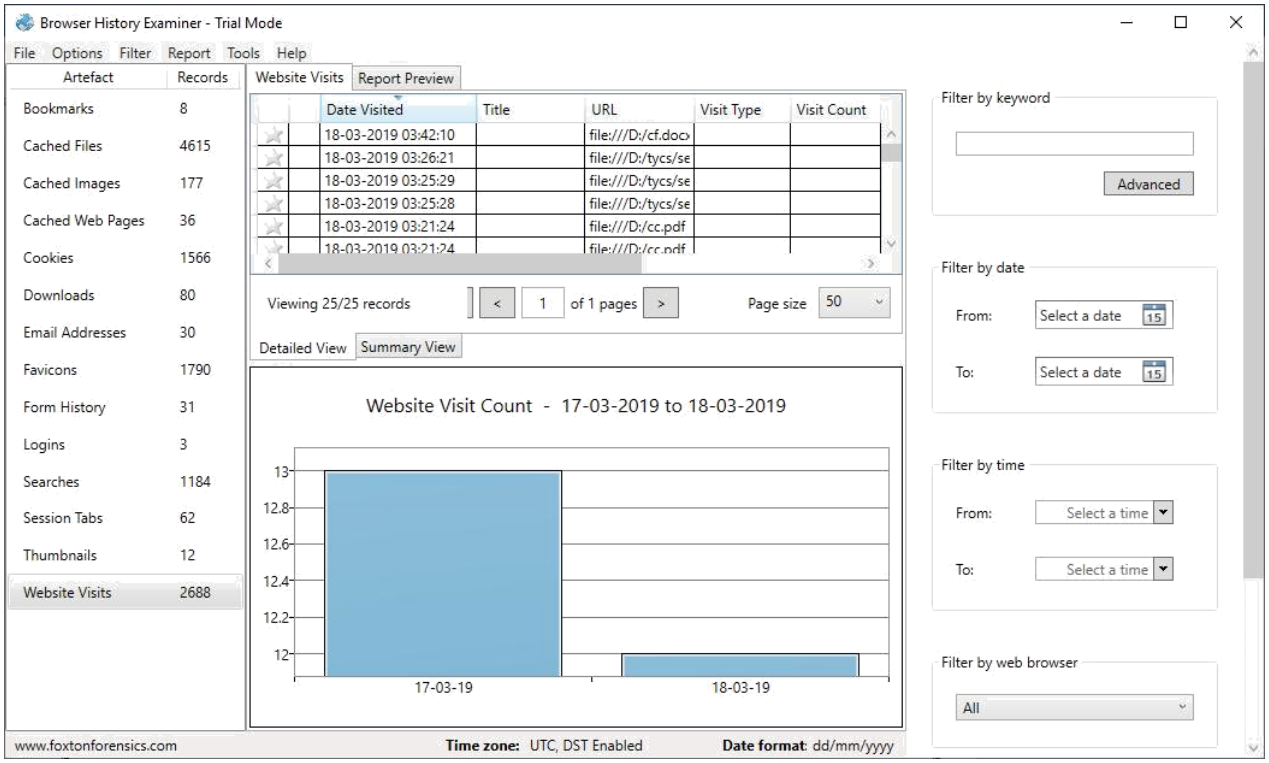


5. The History is been extracting.

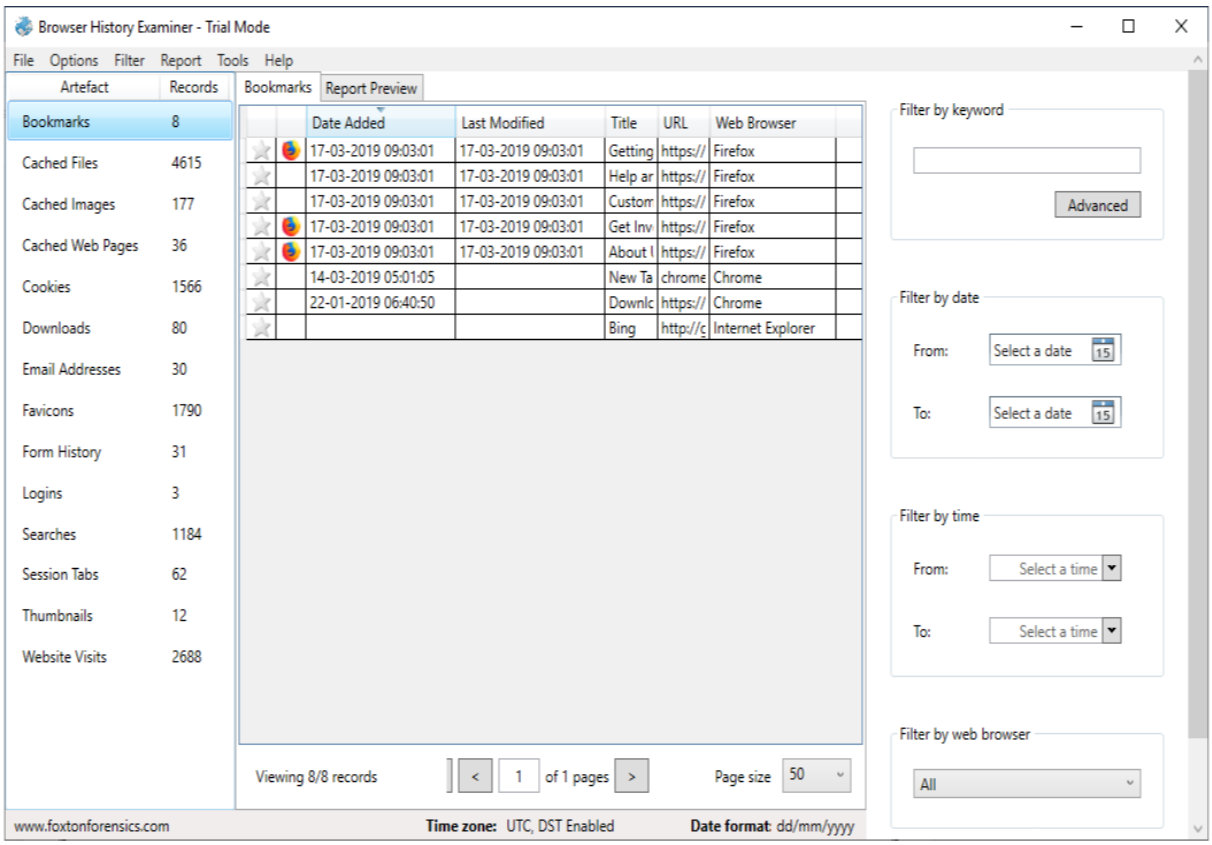




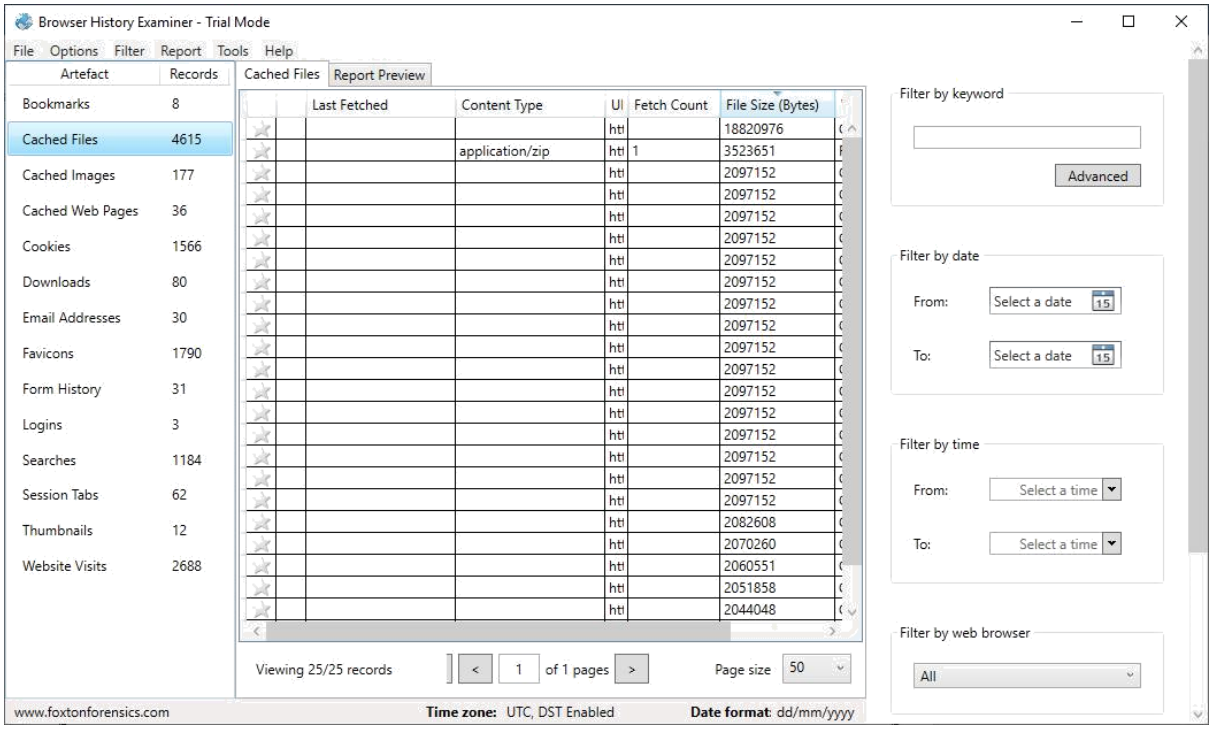
6. The data has been retrieved.



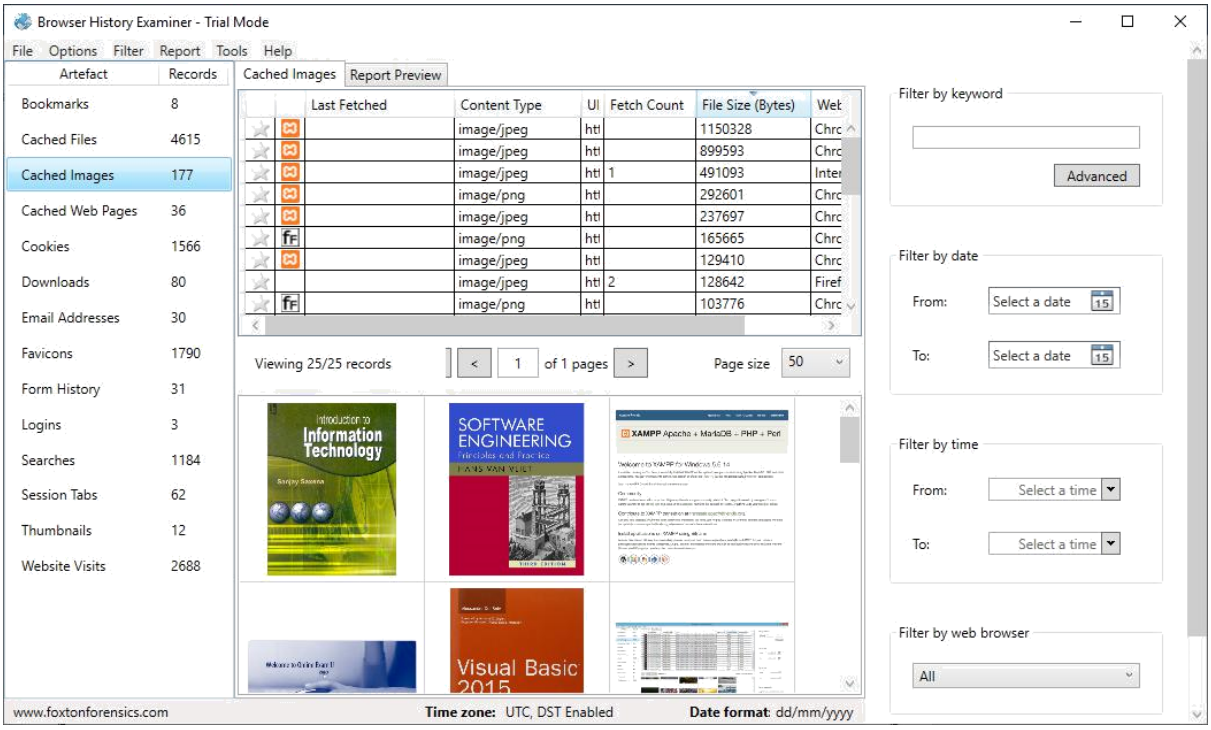
7. On the left panel click on bookmarks.



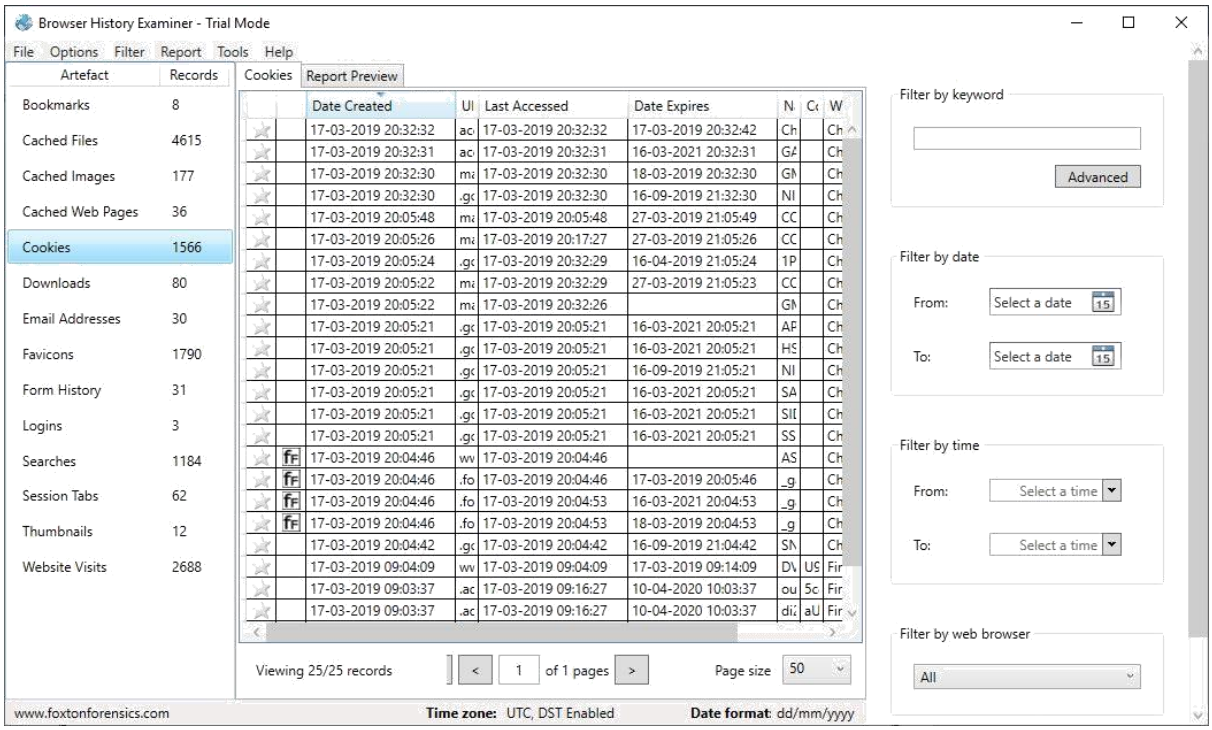
8. On the left panel click on cached files.



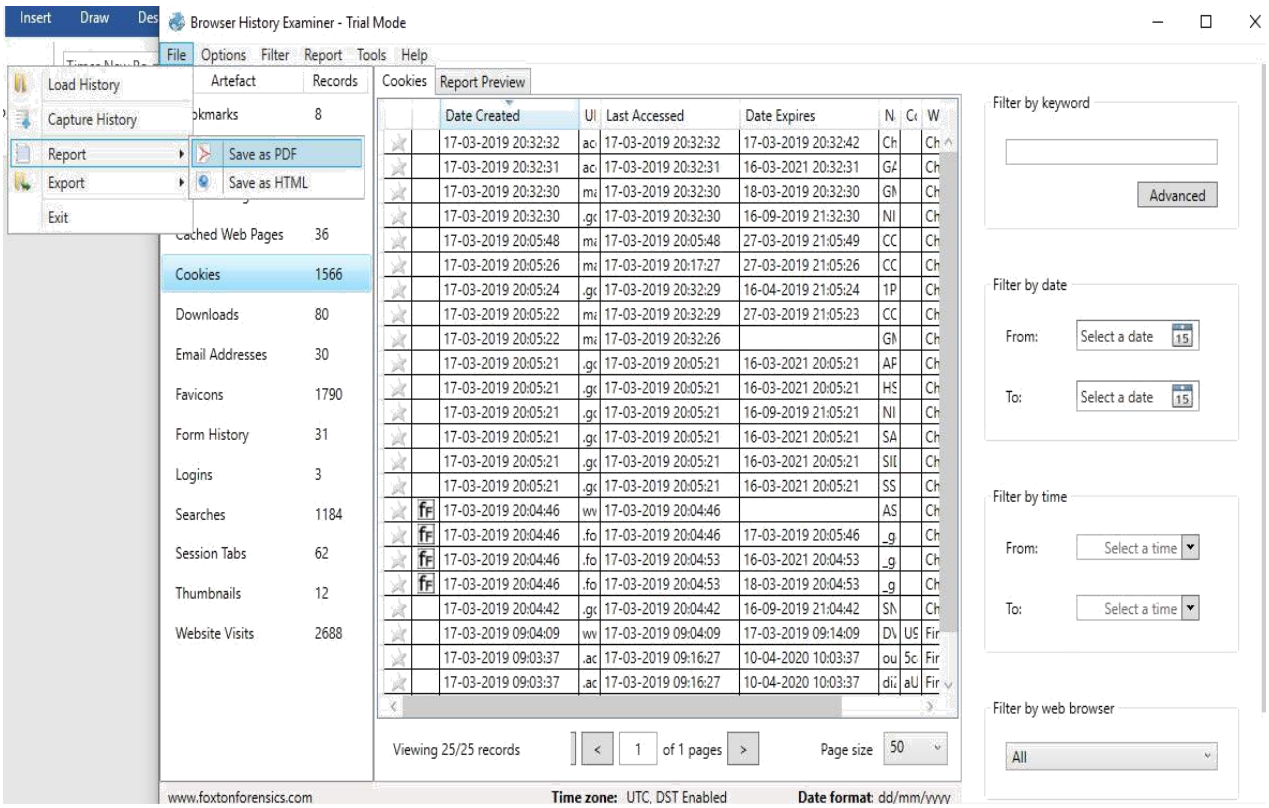
9. On the left panel click on cached images.

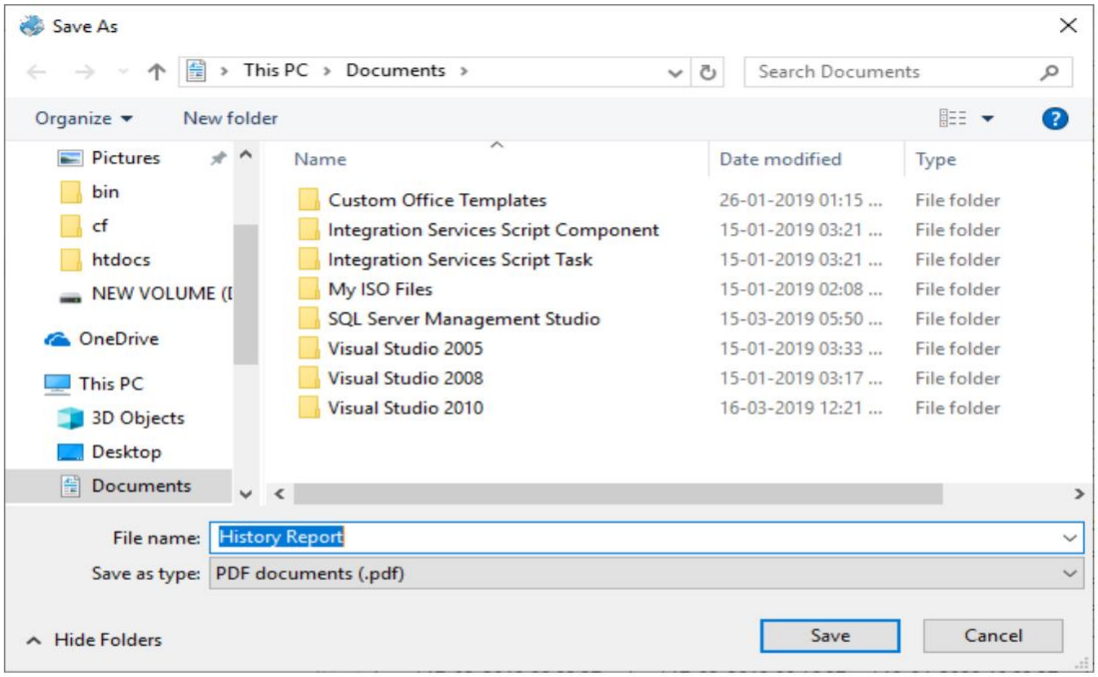


10. On the left panel click on cookies.



11. To Create Reports. Click on file > Report and save the report as pdf or html page.





Web Browser History Report

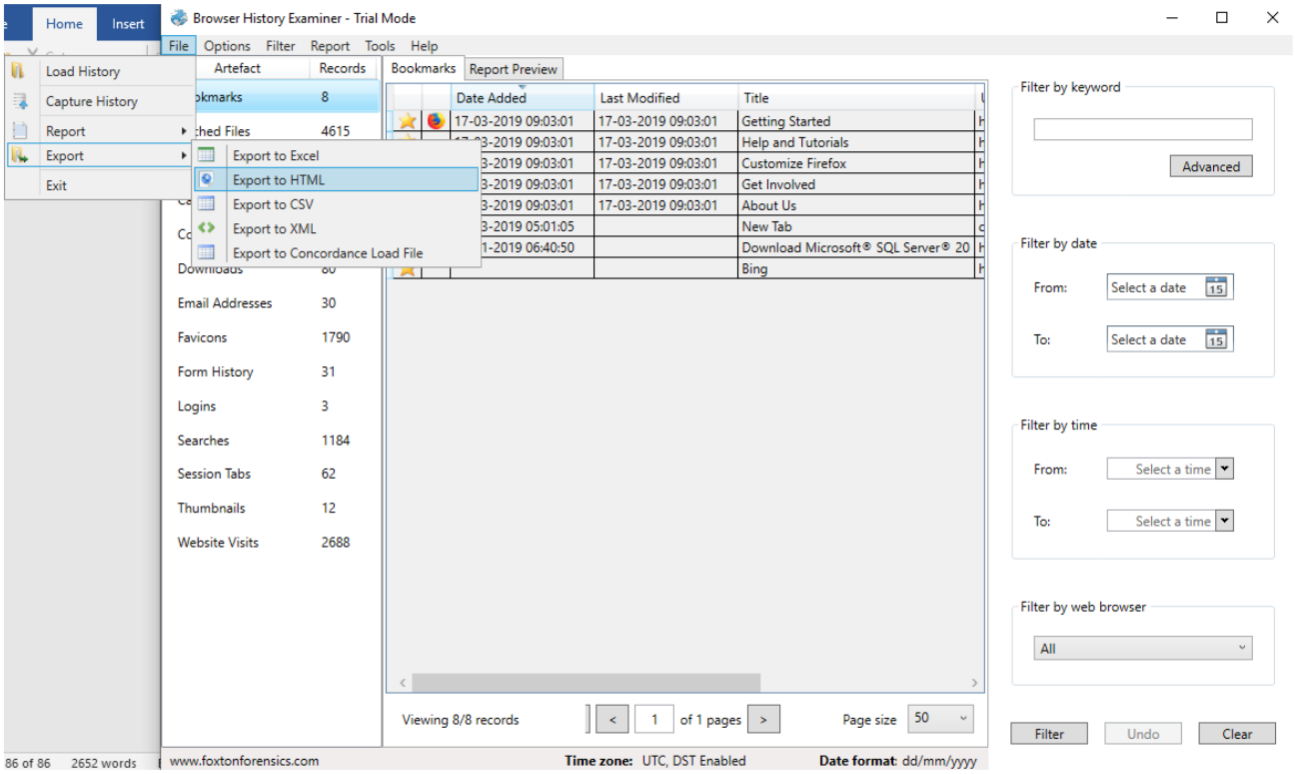
Created: 18-03-2019 09:36
Created using: Browser History Examiner v1.9
Time zone: UTC, DST Enabled
Date format: dd/mm/yyyy

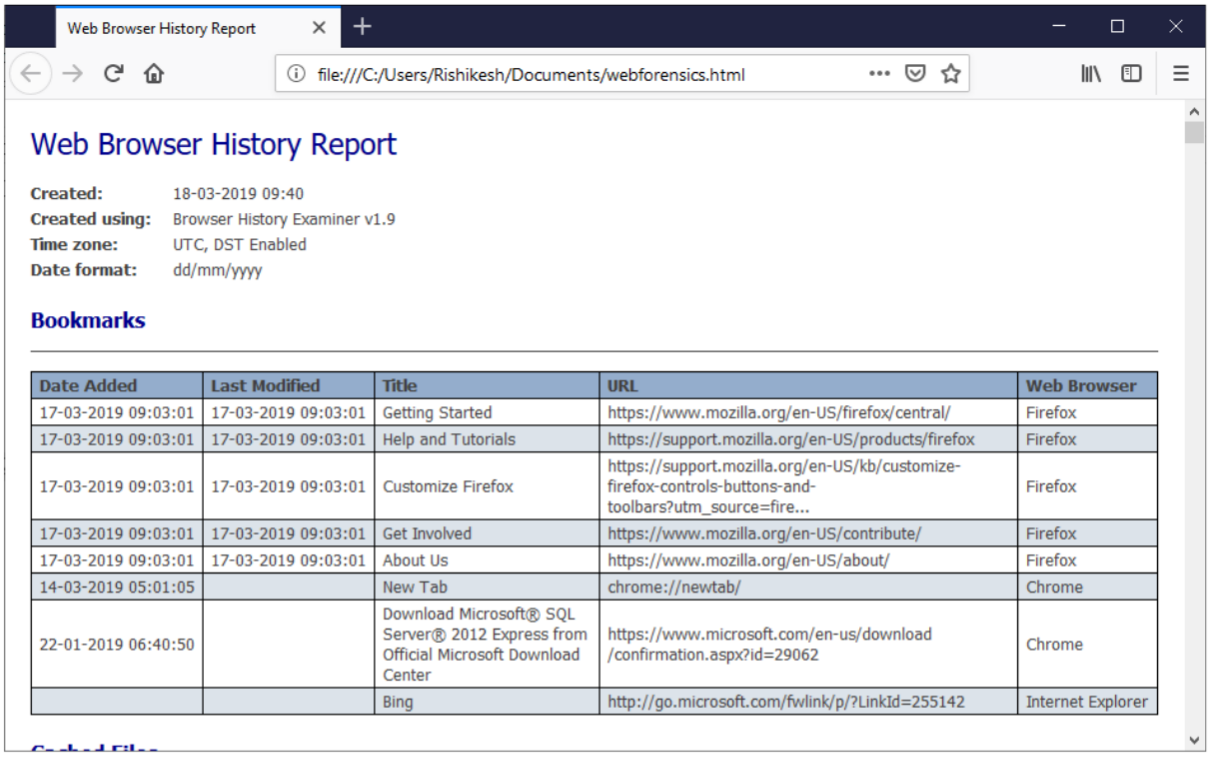
Bookmarks

Date Added	Last Modified	Title	URL	Web Browser
17-03-2019 09:03:01	17-03-2019 09:03:01	Getting Started	https://www.mozilla.org/en-US/firefox/central/	Firefox
17-03-2019 09:03:01	17-03-2019 09:03:01	Help and Tutorials	https://support.mozilla.org/en-US/products/firefox	Firefox
17-03-2019 09:03:01	17-03-2019 09:03:01	Customize Firefox	https://support.mozilla.org/en-US/kb/customize-firefox-controls-buttons-and-toolbars?utm_source=fire...	Firefox
17-03-2019 09:03:01	17-03-2019 09:03:01	Get Involved	https://www.mozilla.org/en-US/contribute/	Firefox
17-03-2019 09:03:01	17-03-2019 09:03:01	About Us	https://www.mozilla.org/en-US/about/	Firefox
14-03-2019 05:01:05		New Tab	chrome://newtab/	Chrome
22-01-2019 06:40:50		Download Microsoft® SQL Server® 2012 Express from Official Microsoft Download Center	https://www.microsoft.com/en-us/download/confirmation.aspx?id=29062	Chrome
		Bing	http://go.microsoft.com/fwlink/p/?LinkId=255142	Internet Explorer

Cached Files

Last Fetched	Content Type	URL	Fetch Count	File Size (Bytes)	Web Browser
		https://mail-attachment.googleusercontent.com/attachment/u/0/?ui=2&ik=5c151dfa36&attid=0.1&a...		18820976	Chrome
	application/zip	https://r4---sn-4p8xoxu-cvhe.gvt1.com/edgedl/widevine-cdm/4.10.1146.0-win-x64.zip?cms_redirect=yes&a...	1	3523651	Firefox
		https://r3---sn-4p8xoxu-cvhe.googlevideo.com/videoplayback?ei=uYyLXNeQA4eiLAb4h7K4Cg&dur=152.733...		2097152	Chrome
		https://r3---sn-4p8xoxu-cvhe.googlevideo.com/videoplayback?ei=uYyLXNeQA4eiLAb4h7K4Cg&dur=152.733...		2097152	Chrome
		https://r3---sn-4p8xoxu-cvhe.googlevideo.com/videoplayback?ei=uYyLXNeQA4eiLAb4h7K4Cg&dur=152.733...		2097152	Chrome





Web Browser History Report

Created: 18-03-2019 09:40
Created using: Browser History Examiner v1.9
Time zone: UTC, DST Enabled
Date format: dd/mm/yyyy

Bookmarks

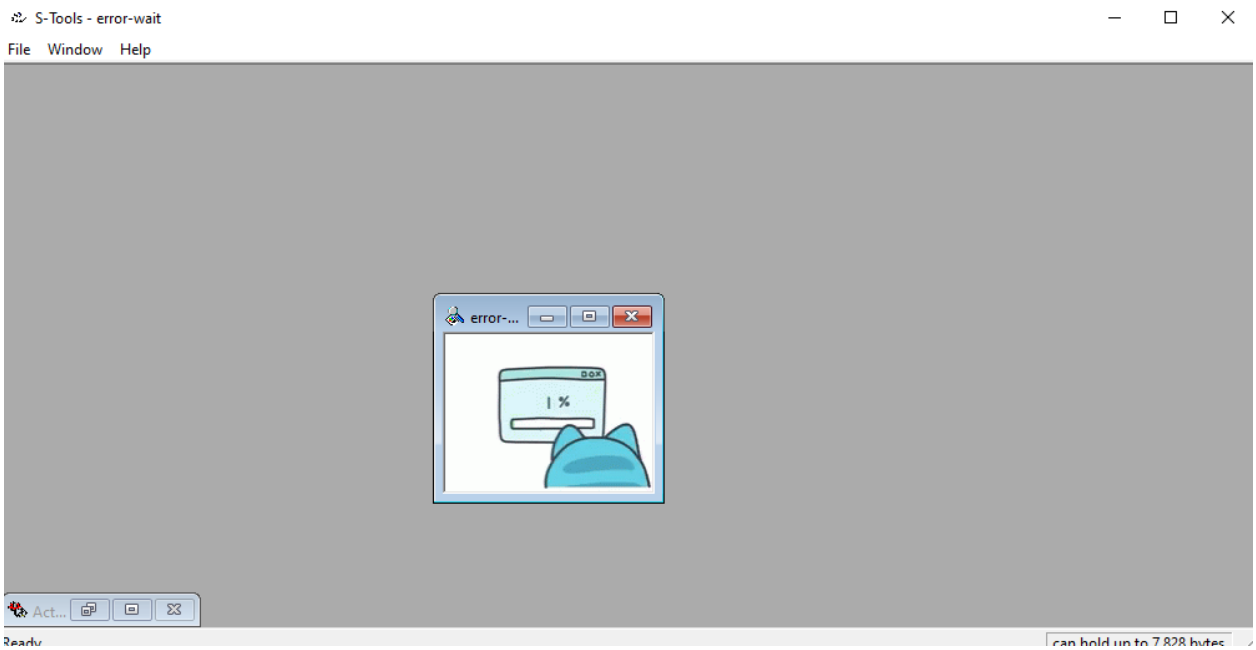
Date Added	Last Modified	Title	URL	Web Browser
17-03-2019 09:03:01	17-03-2019 09:03:01	Getting Started	https://www.mozilla.org/en-US/firefox/central/	Firefox
17-03-2019 09:03:01	17-03-2019 09:03:01	Help and Tutorials	https://support.mozilla.org/en-US/products/firefox	Firefox
17-03-2019 09:03:01	17-03-2019 09:03:01	Customize Firefox	https://support.mozilla.org/en-US/kb/customize-firefox-controls-buttons-and-toolbars?utm_source=fire...	Firefox
17-03-2019 09:03:01	17-03-2019 09:03:01	Get Involved	https://www.mozilla.org/en-US/contribute/	Firefox
17-03-2019 09:03:01	17-03-2019 09:03:01	About Us	https://www.mozilla.org/en-US/about/	Firefox
14-03-2019 05:01:05		New Tab	chrome://newtab/	Chrome
22-01-2019 06:40:50		Download Microsoft® SQL Server® 2012 Express from Official Microsoft Download Center	https://www.microsoft.com/en-us/download/confirmation.aspx?id=29062	Chrome
		Bing	http://go.microsoft.com/fwlink/p/?LinkId=255142	Internet Explorer

PRACTICAL 10

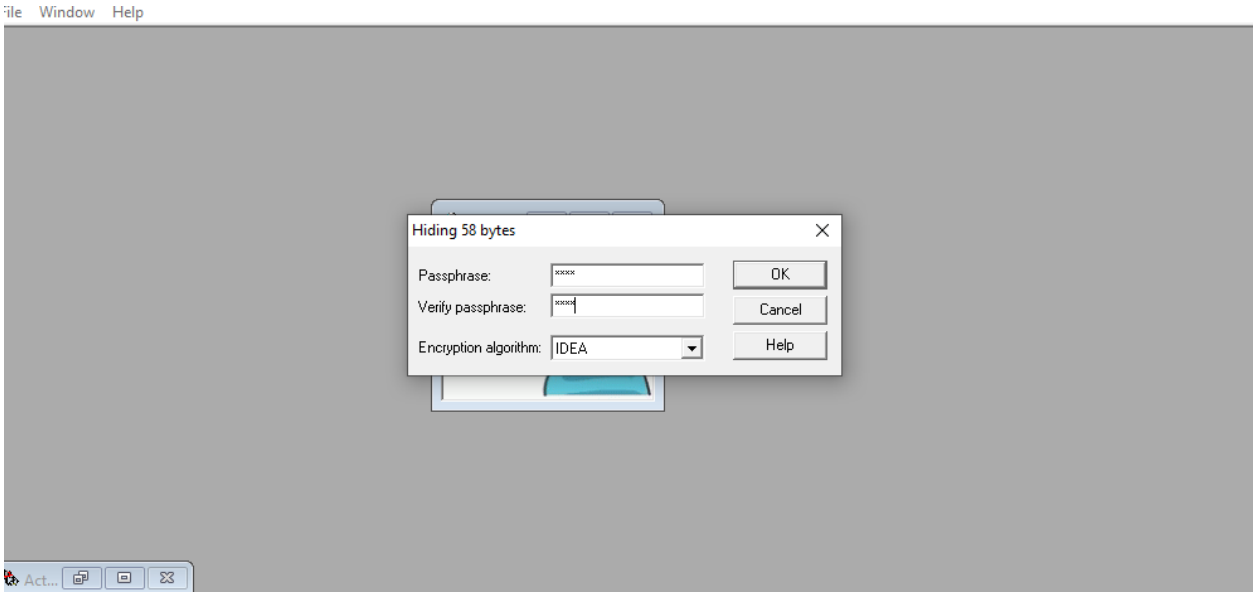
A.Using Steganography Tools [S-Tools]

Step 1: The dark gray background area is used for droping the image or sound files into.

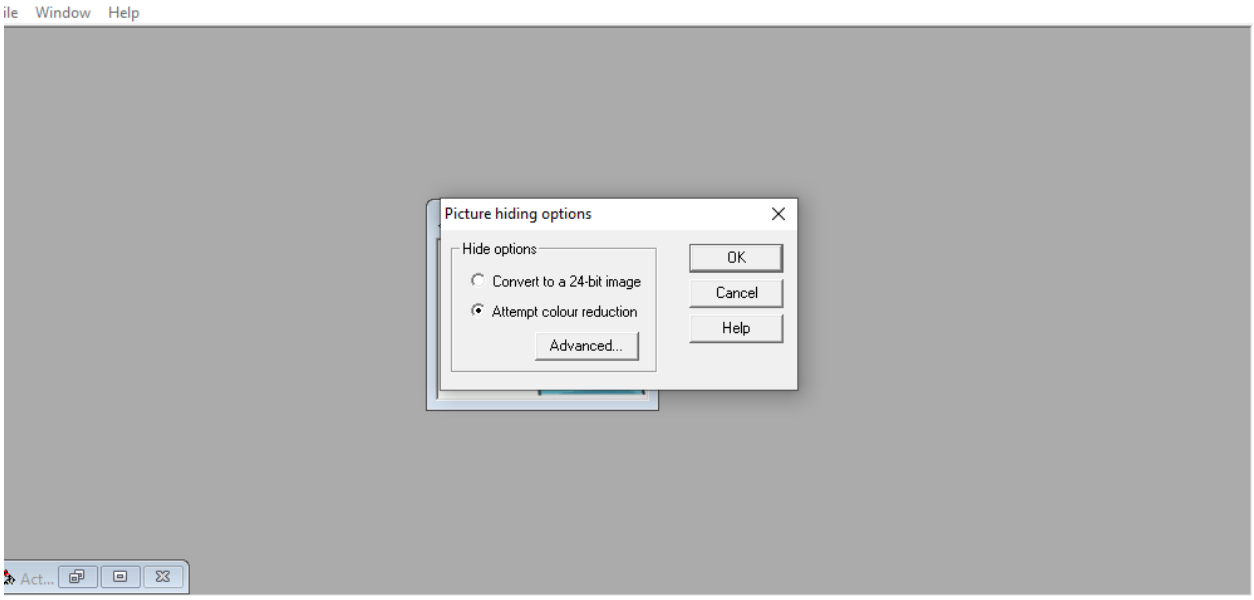
Step 2: After opening S-Tools (S-Tools.exe) and Windows Explorer, drag Cover File.gif into the main working area of S-Tools



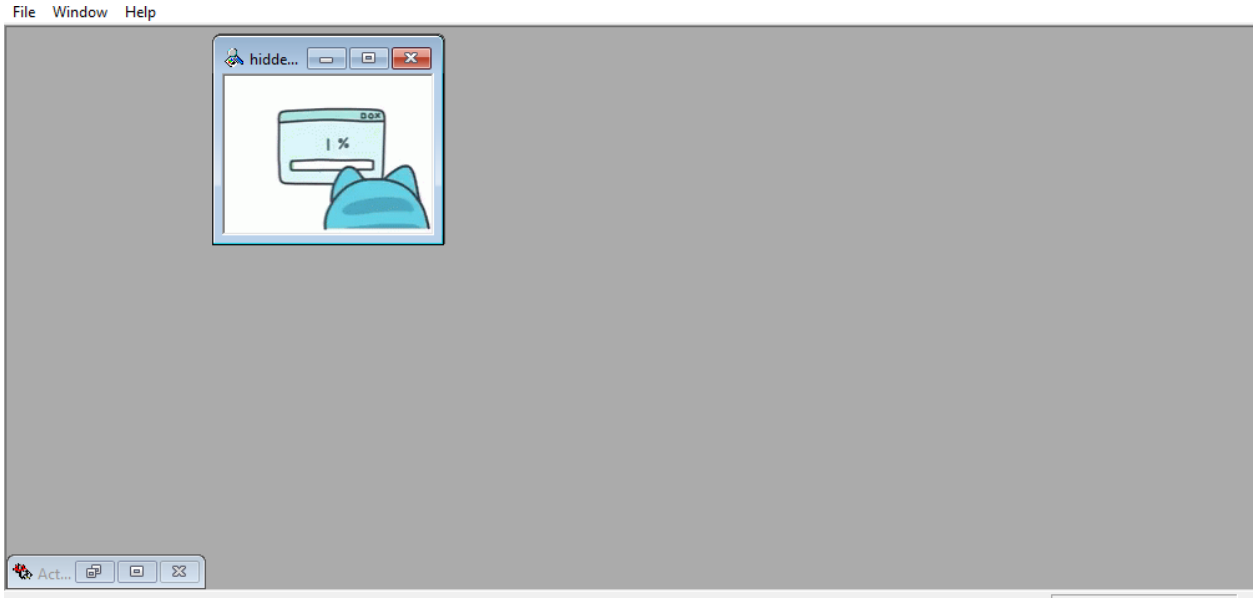
Step 3: The pass phrase is used in generating the pseudorandom number that is used to insert the bits into the cover file. S-Tools gives a choice between IDEA, DES, TripleDES, and MDC encryption algorithms



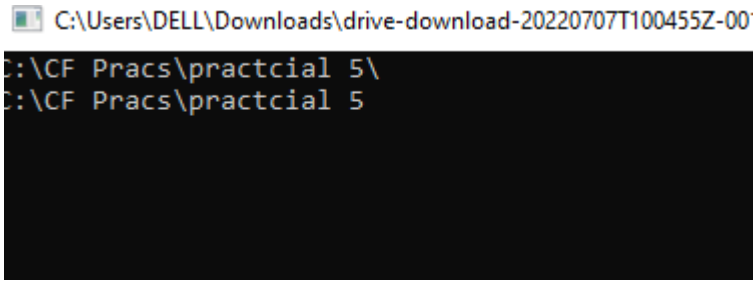
Step 4: To have S-Tools process the GIF file, a dialog box prompts for choices to be made



Step 5 : When S-Tools finishes inserting the data, the output image will display with the marker "hidden data" at the top



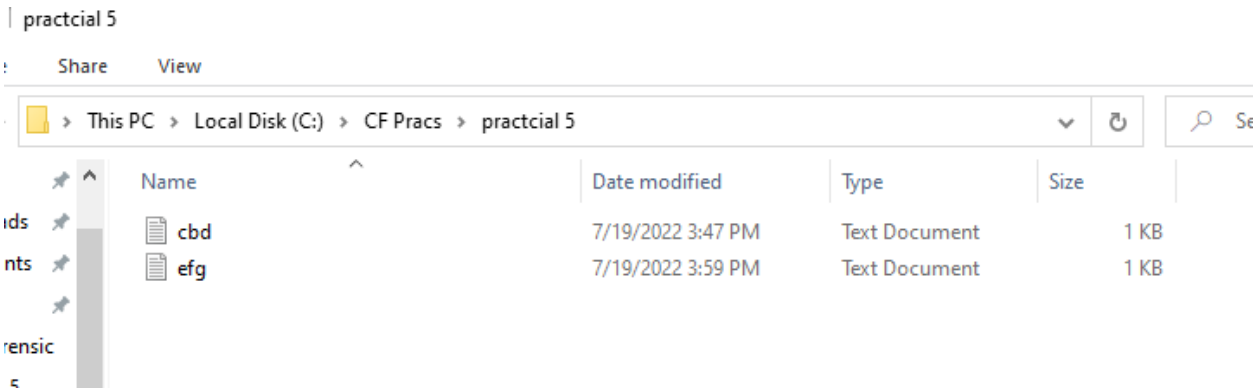
B. Using Whitespace Stegnography tool SNOW



snow -C -m “MessageToHide” -p “Password” “InputTextFile” “OutputTextFile”

C:\Users\DELL\Downloads\drive-download-20220707T100455Z-001\SNOW.EXE

```
C:\CF Pracs\practcial 5>snow -C -m "Practical number 5 " -p "kaushal" cbd.txt efg.txt
Compressed by 35.67%
Message exceeded available space by approximately 788.54%
An extra 4 lines were added.
```



C:\Users\DELL\Downloads\drive-download-20220707T100455Z-001\SNOW.EXE

```
C:\CF Pracs\practical 5>snow -C -p "kaushal" efg.txt
Practical number 5
C:\CF Pracs\practical>
C:\CF Pracs\practical>
```