

Prof.Ajay Pashankar

Department Of Computer Science & Information Technology



 ajaypashankar7

 Prof.Ajay Pashankar



www.profajaypashankar.com

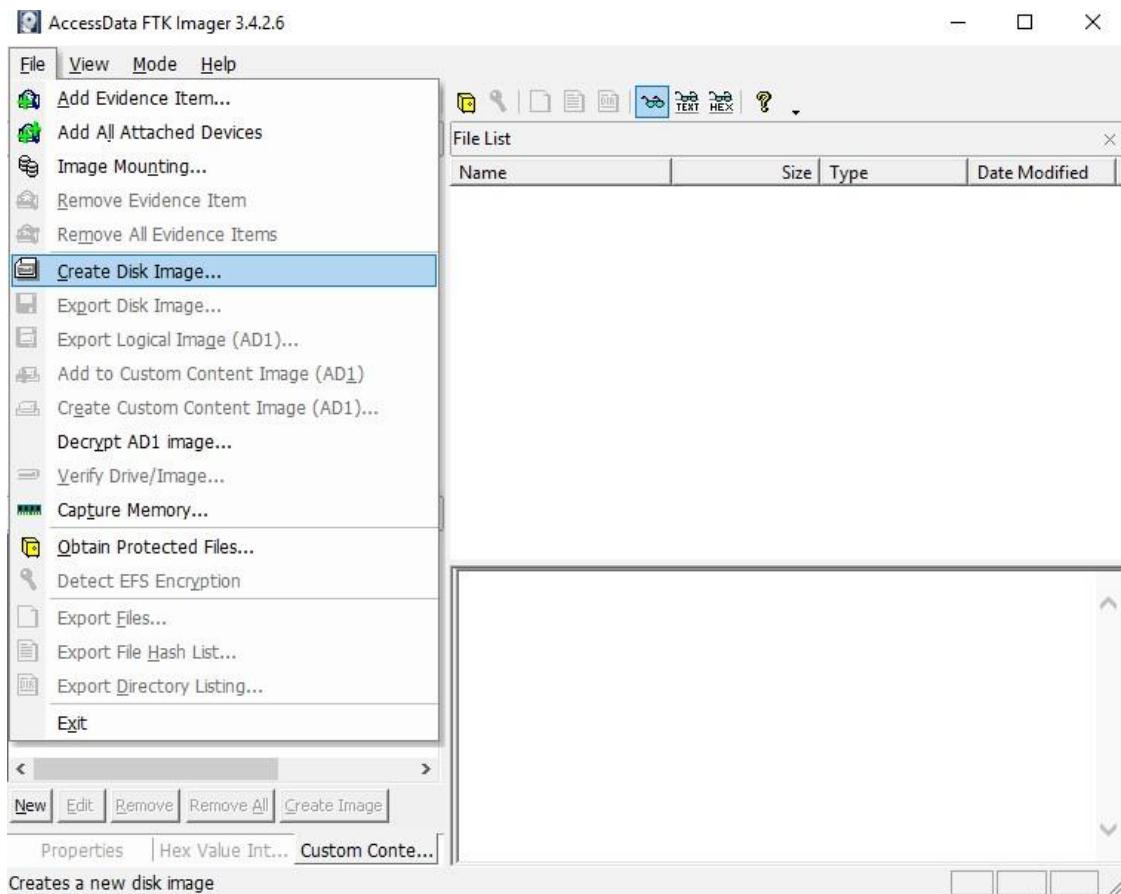
PRACTICAL 1

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

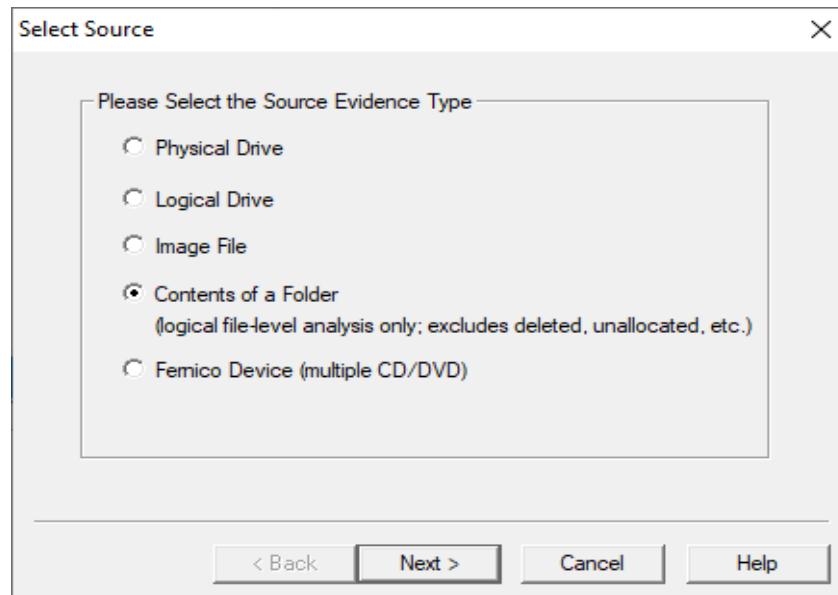
- Creating Forensic Image
- Check Integrity of Data
- Analyze Forensic Image

➤ Creating Forensic Image

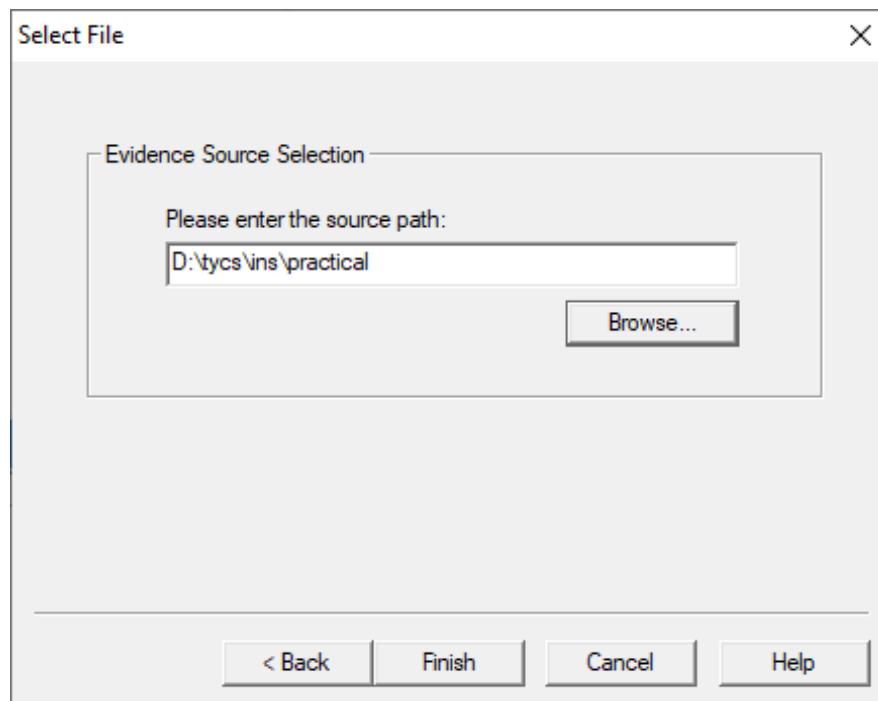
1. Click File, and then Create Disk Image, or click the button on the tool bar.



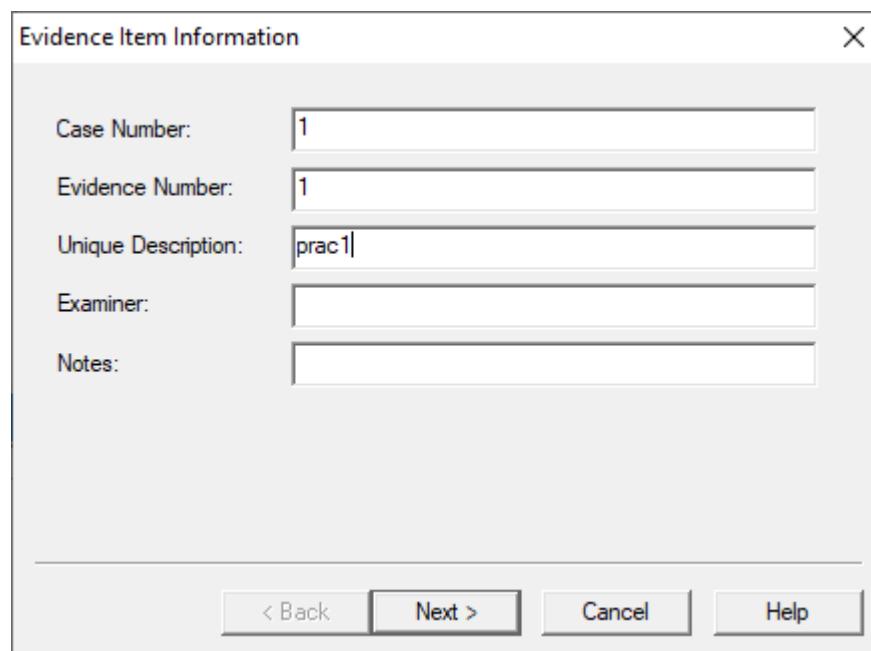
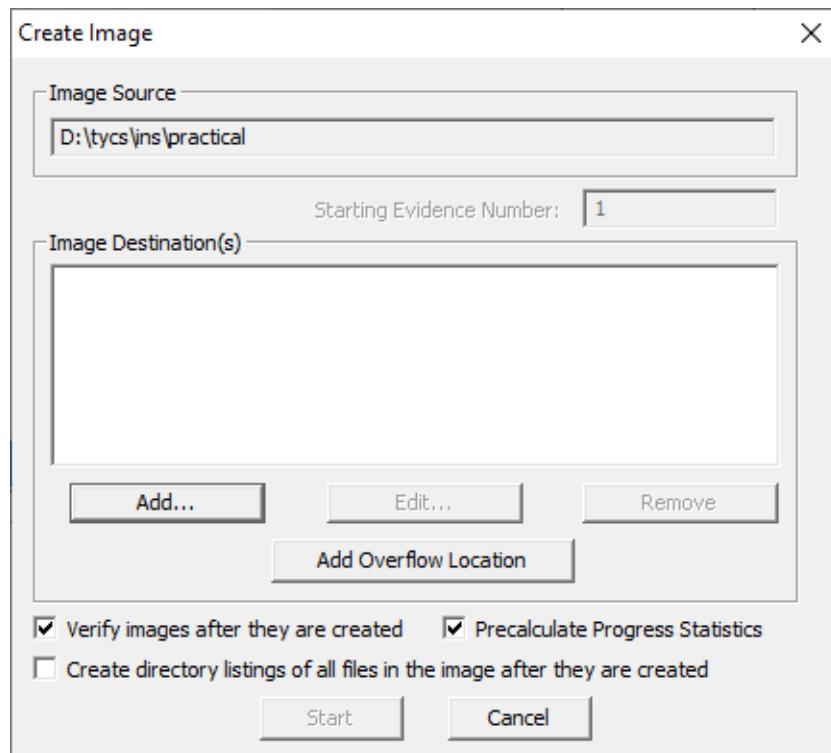
2. Select the source evidence type you want to make an image of and click Next.



3. Select the source evidence file with path .

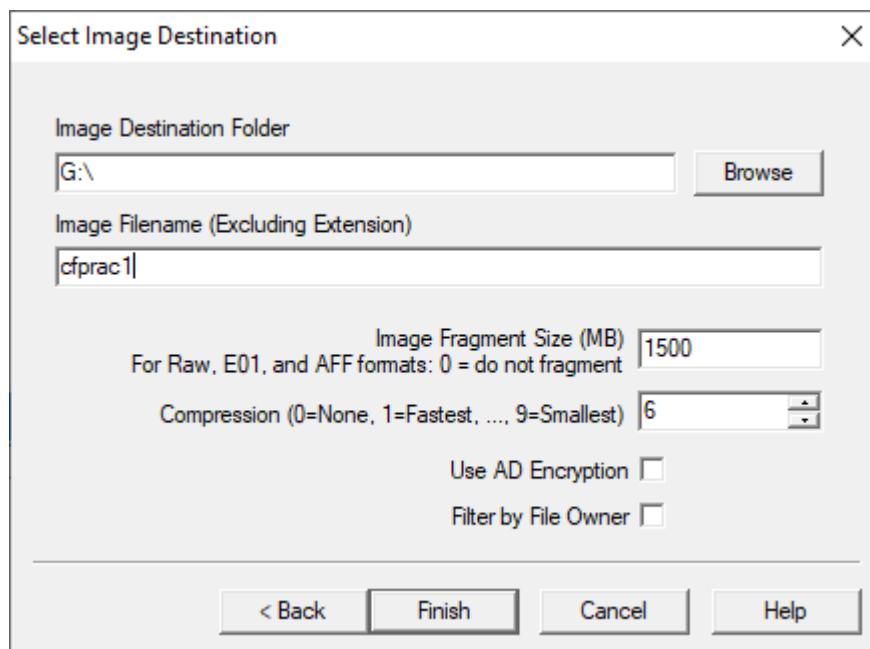


Click on “add” to add image destination

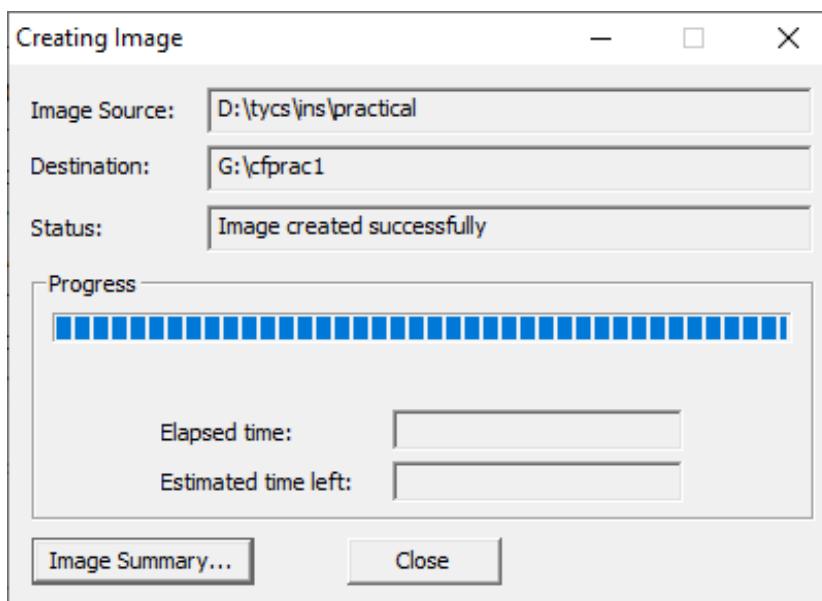


4. In the Image Destination Folder field, type the location path where you want to save the image file, or click **Browse** to find to the desired location.

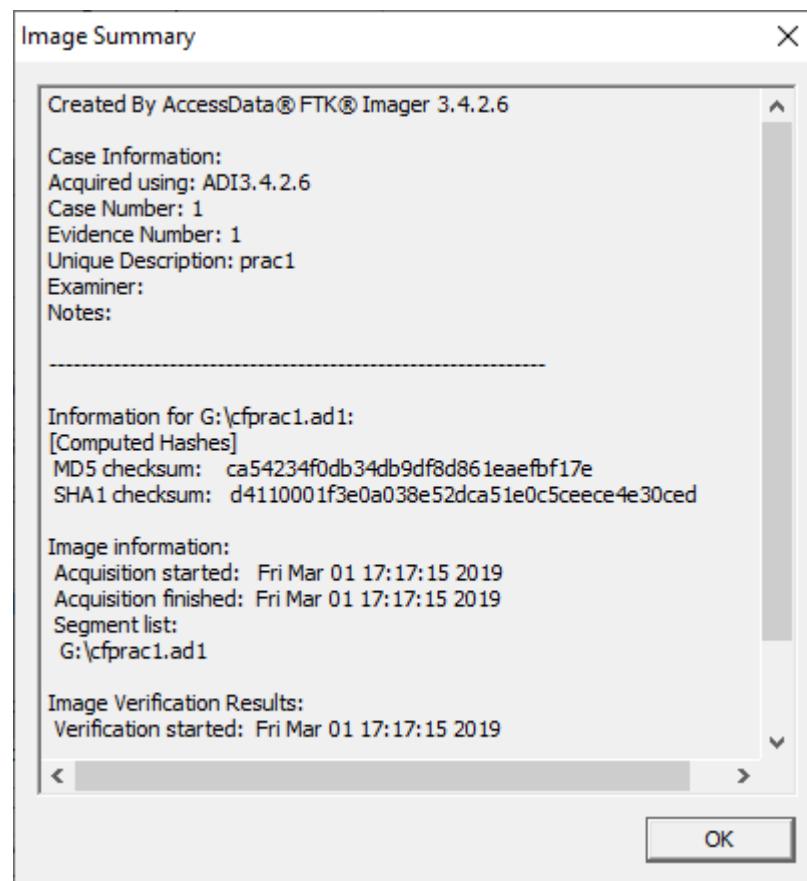
Note: If the destination folder you select is on a drive that does not have sufficient free space to store the entire image file, FTK Imager prompts for a new destination folder when all available space has been used in the first location. In the Image Filename field, specify a name for the image file but do not specify a file extension.



5. After adding the image destination path click on finish and start the image processing.

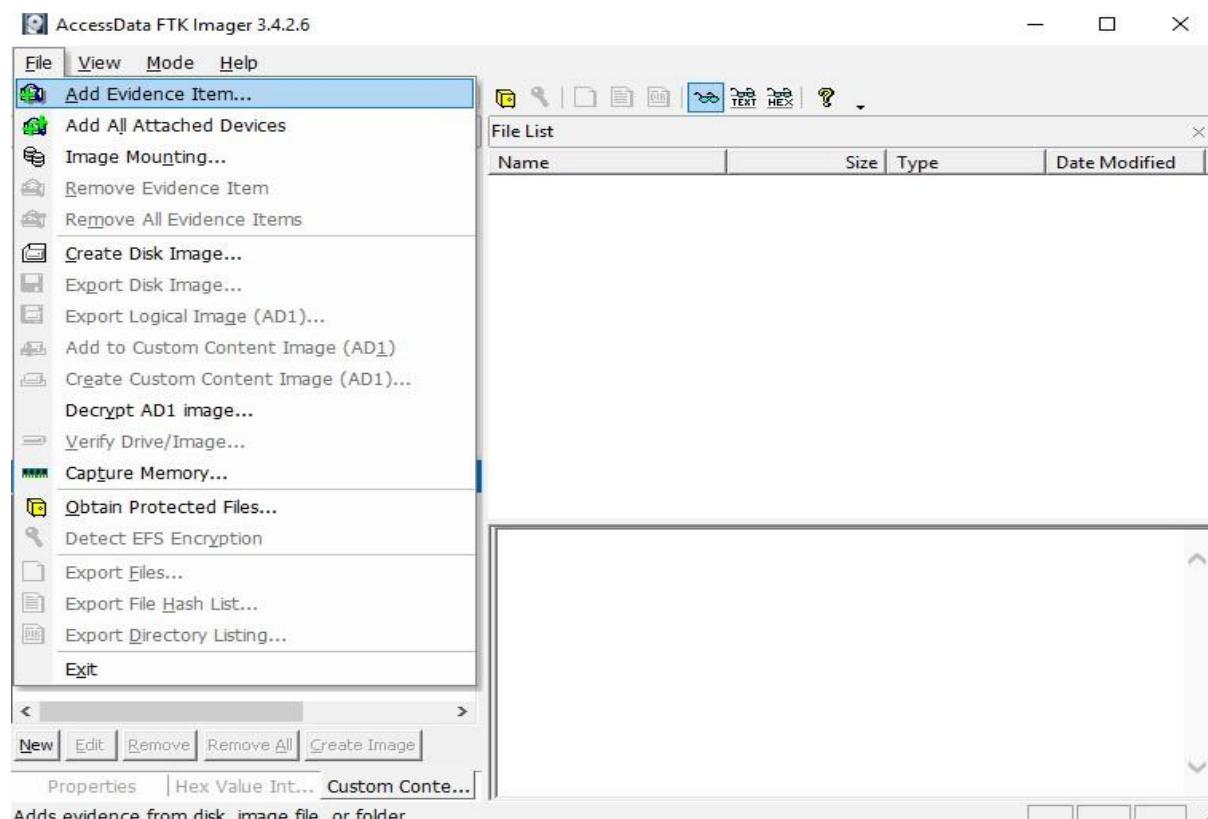


6. After the images are successfully created, click Image Summary to view detailed file information, including MD5 and SHA1 checksums.

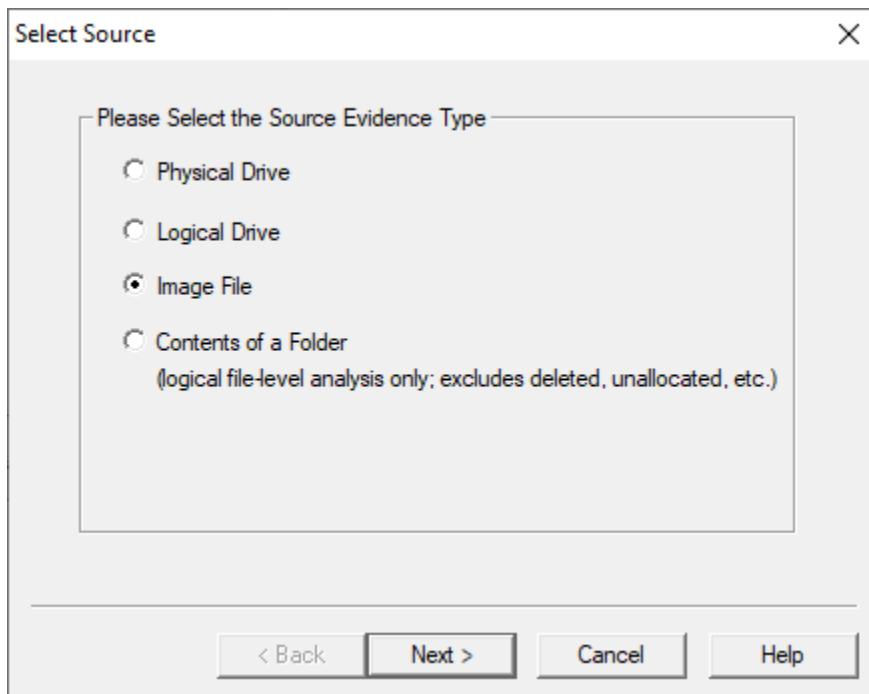


Analyze Forensic Image:

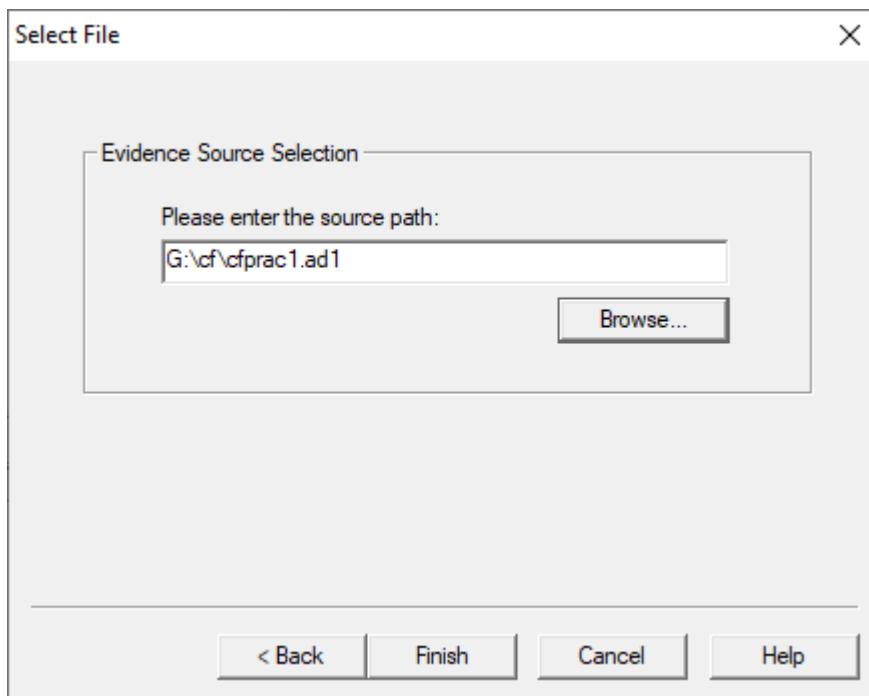
Click on Add Evidence Item to add evidence from disk, image file or folder.



Now select the source evidence type as image file.



Open the created evidence image file



Now select Evidence Tree and analyze the image file .

The screenshot shows the AccessData FTK Imager 3.4.2.6 interface. The top menu bar includes File, View, Mode, and Help. The toolbar contains various icons for file operations like Open, Save, Copy, Paste, and Find. The Evidence Tree pane on the left shows a folder structure with 'cprac1.ad1' expanded, revealing 'D:\tycs\ins\practical [AD1]'. The File List pane on the right displays a table of files with columns for Name, Size, Type, and Date Modified. The table includes entries for several Java files and a Word document. The bottom pane, Custom Content Sources, shows a list of sources with options to New, Edit, Remove, Remove All, and Create Image. A large hex dump window is open, showing binary data starting at address 000. The dump includes ASCII characters and some recognizable file signatures like 'Java' and 'LineNw'. The status bar at the bottom indicates 'Cursor pos = 0'.

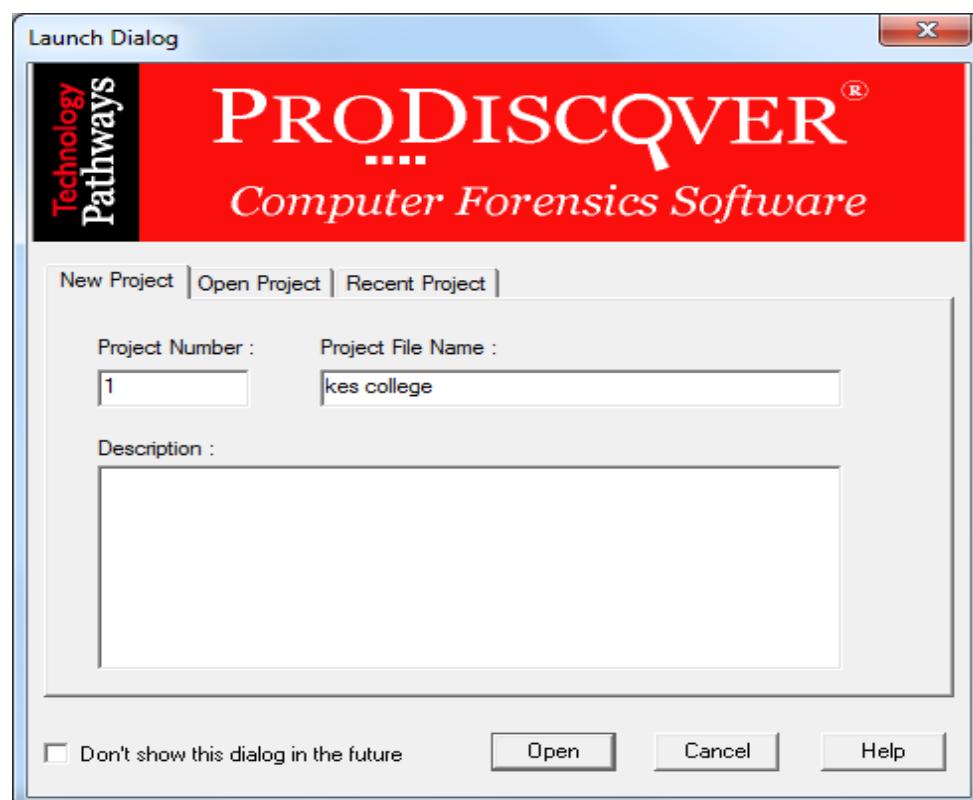
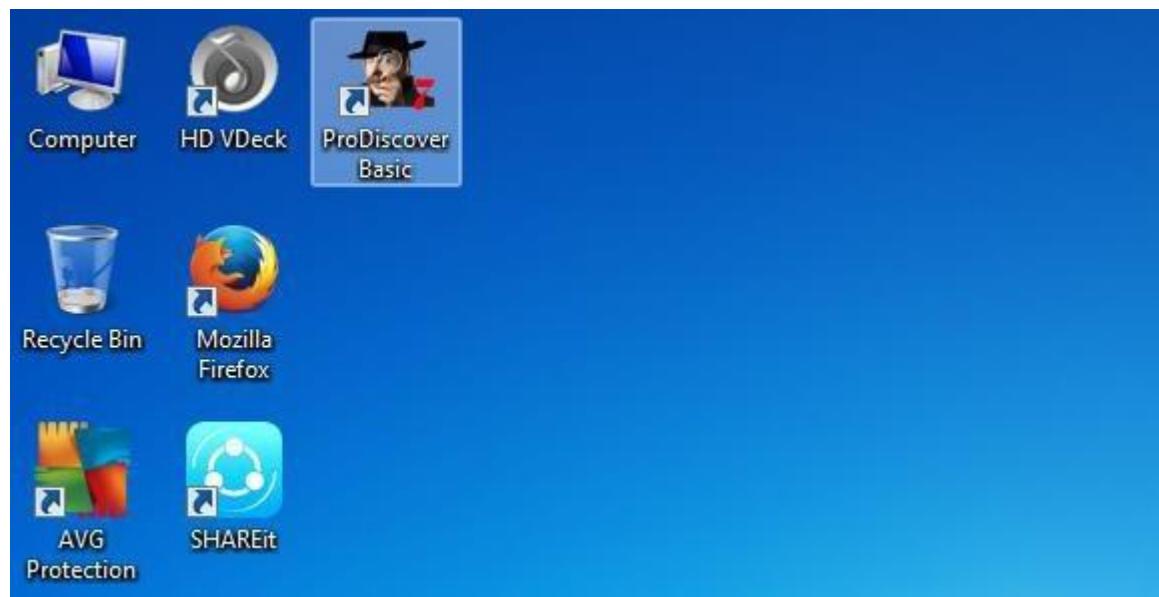
PRACTICAL 2

Aim: Data Acquisition:

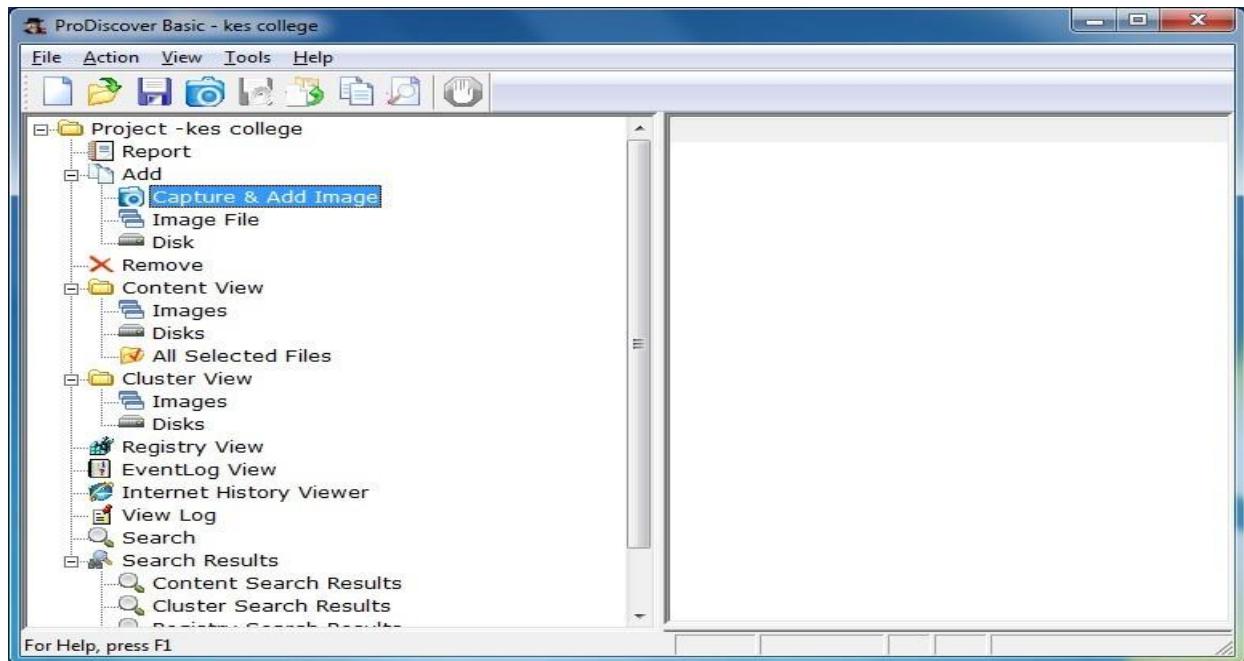
- Perform data acquisition using:
- USB Write Blocker + FTK Imager

Steps:

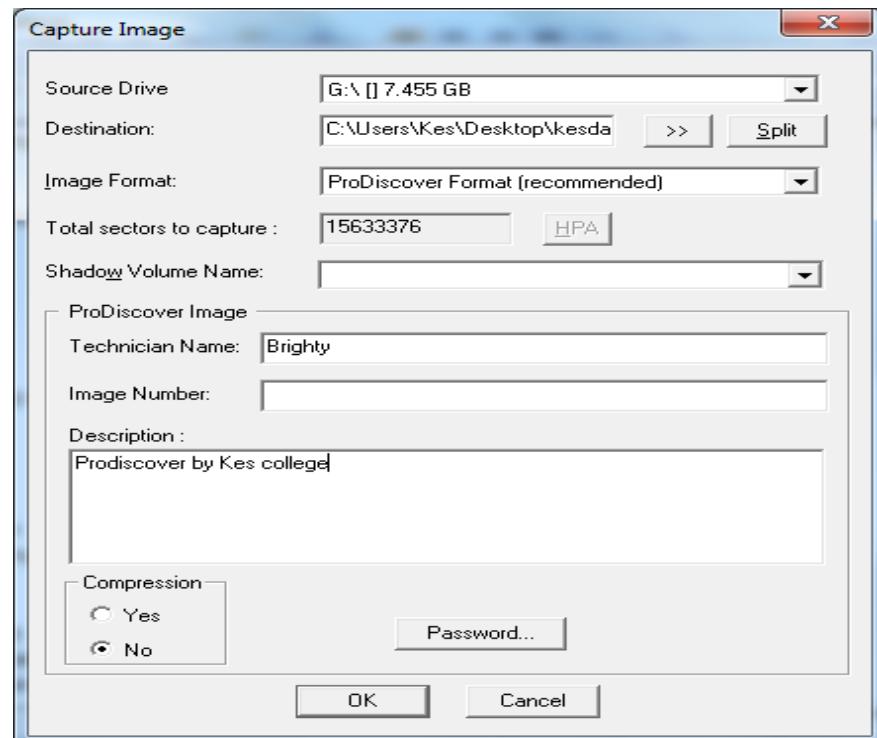
Step 1: First Open Prodiscover Basic and start with new case.



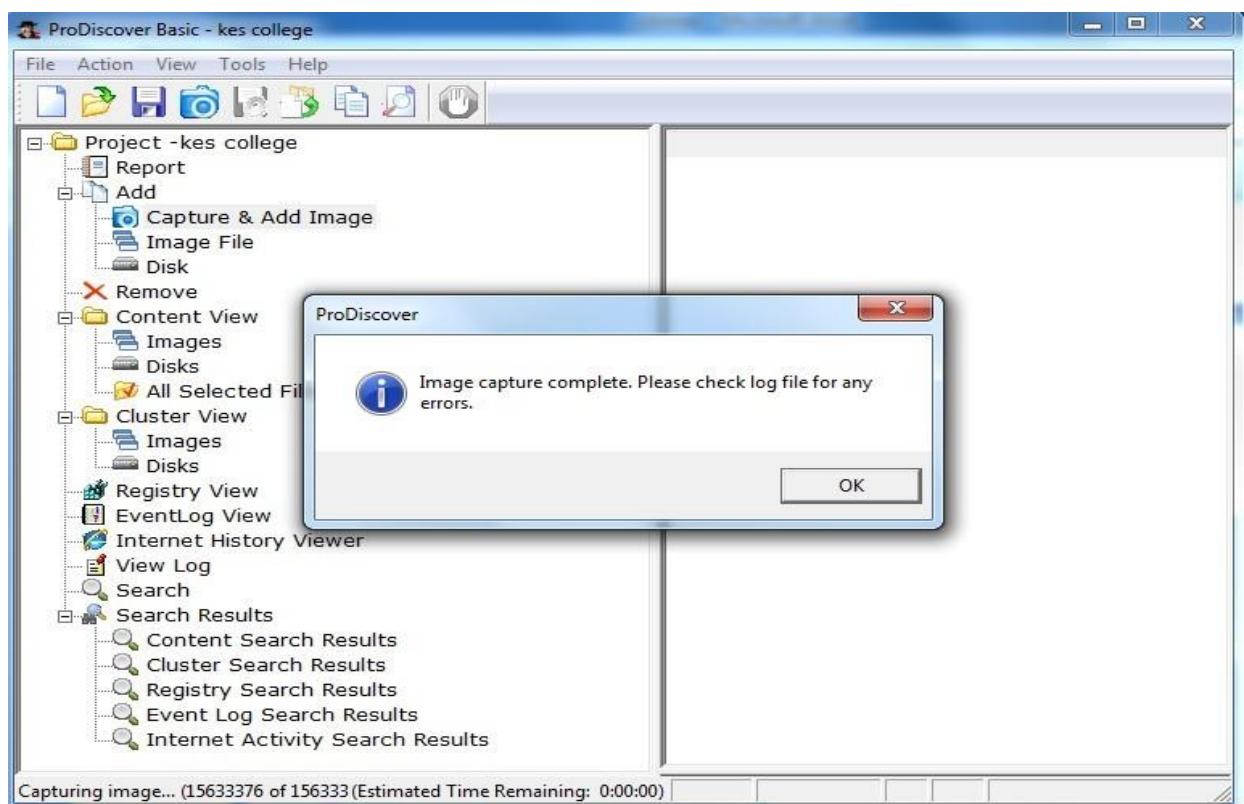
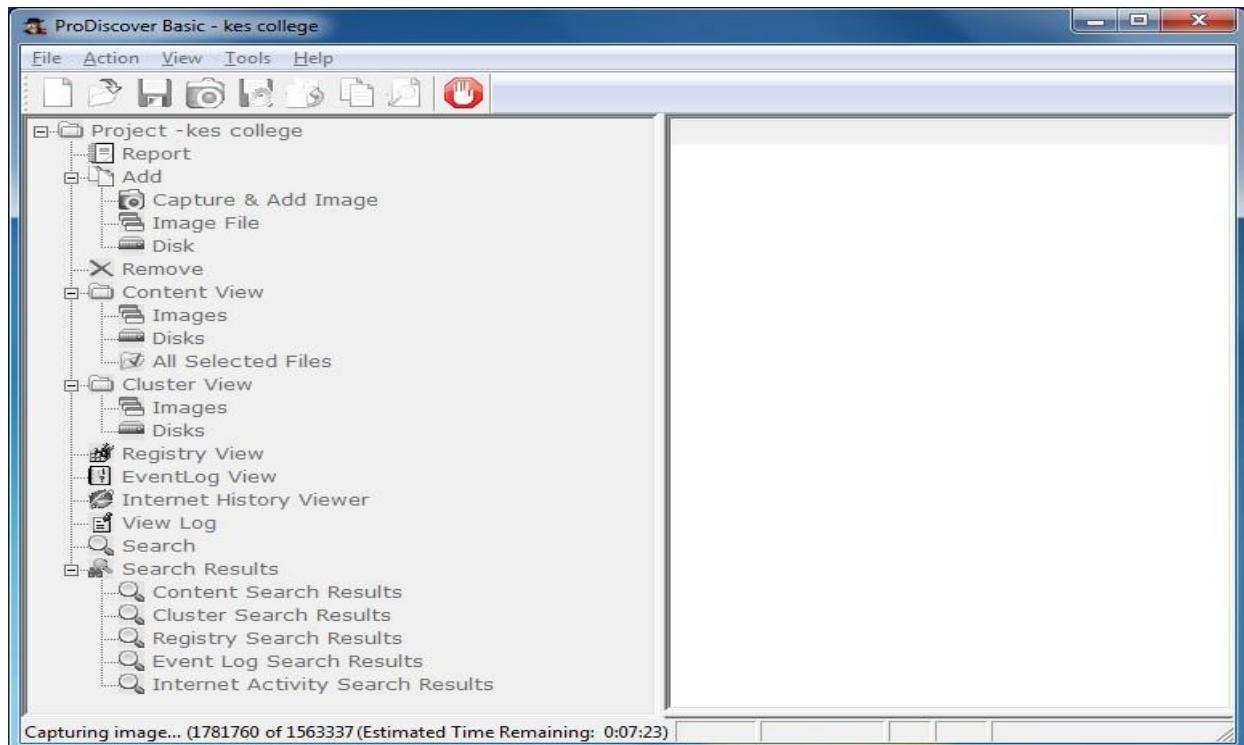
Step 2: The created project appears in left pane and select add>capture & add image.



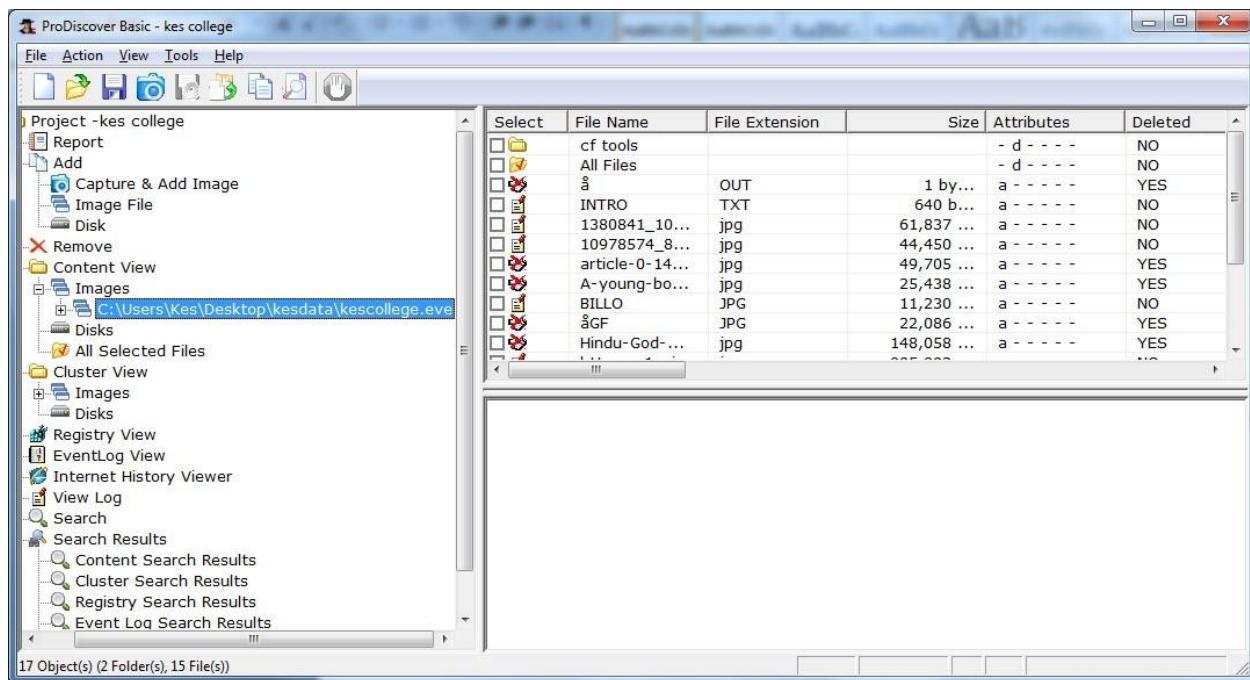
Step 3: fill the details as below. And click ok.



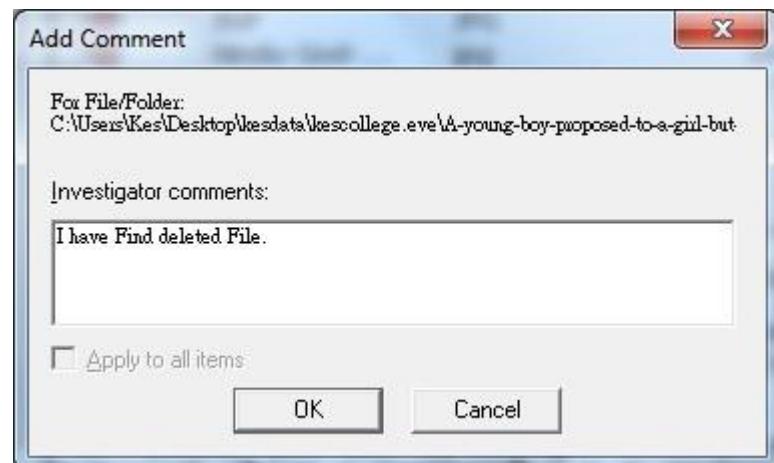
Step 4: capturing of image starts.



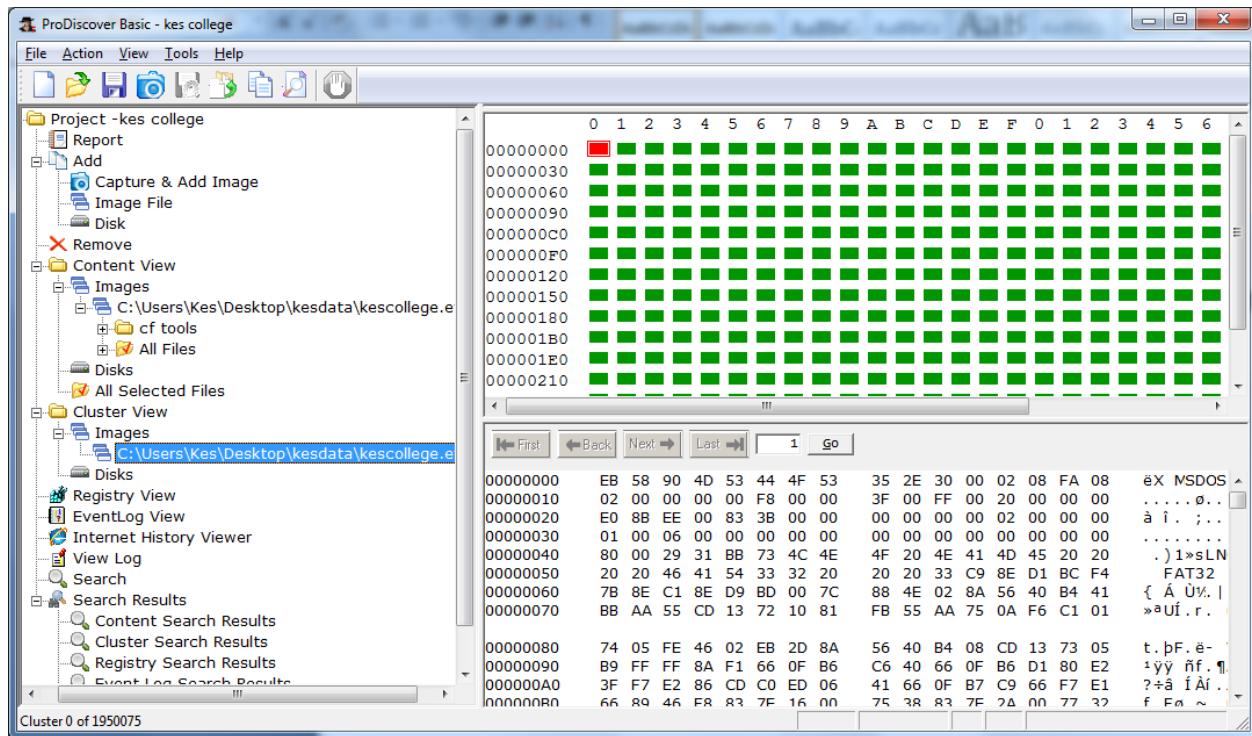
Step 5: Open the image created, go to Add > Images in left pane.



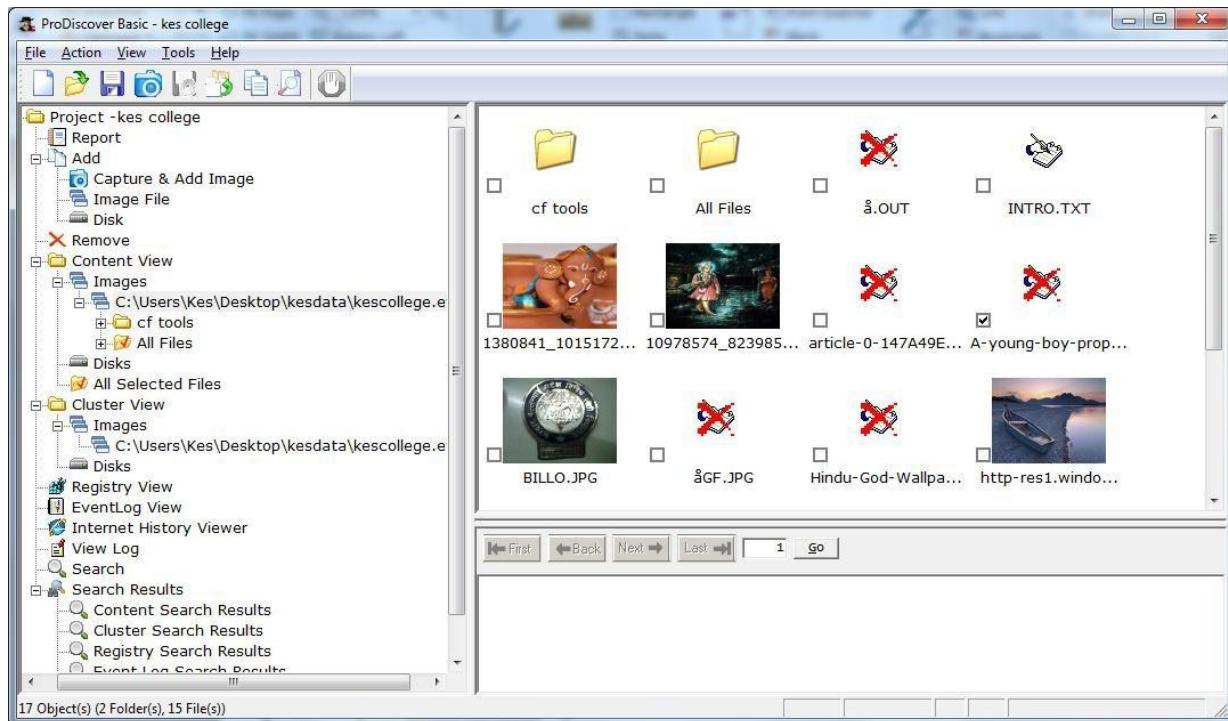
Step 6: Click on any File and type a comment.



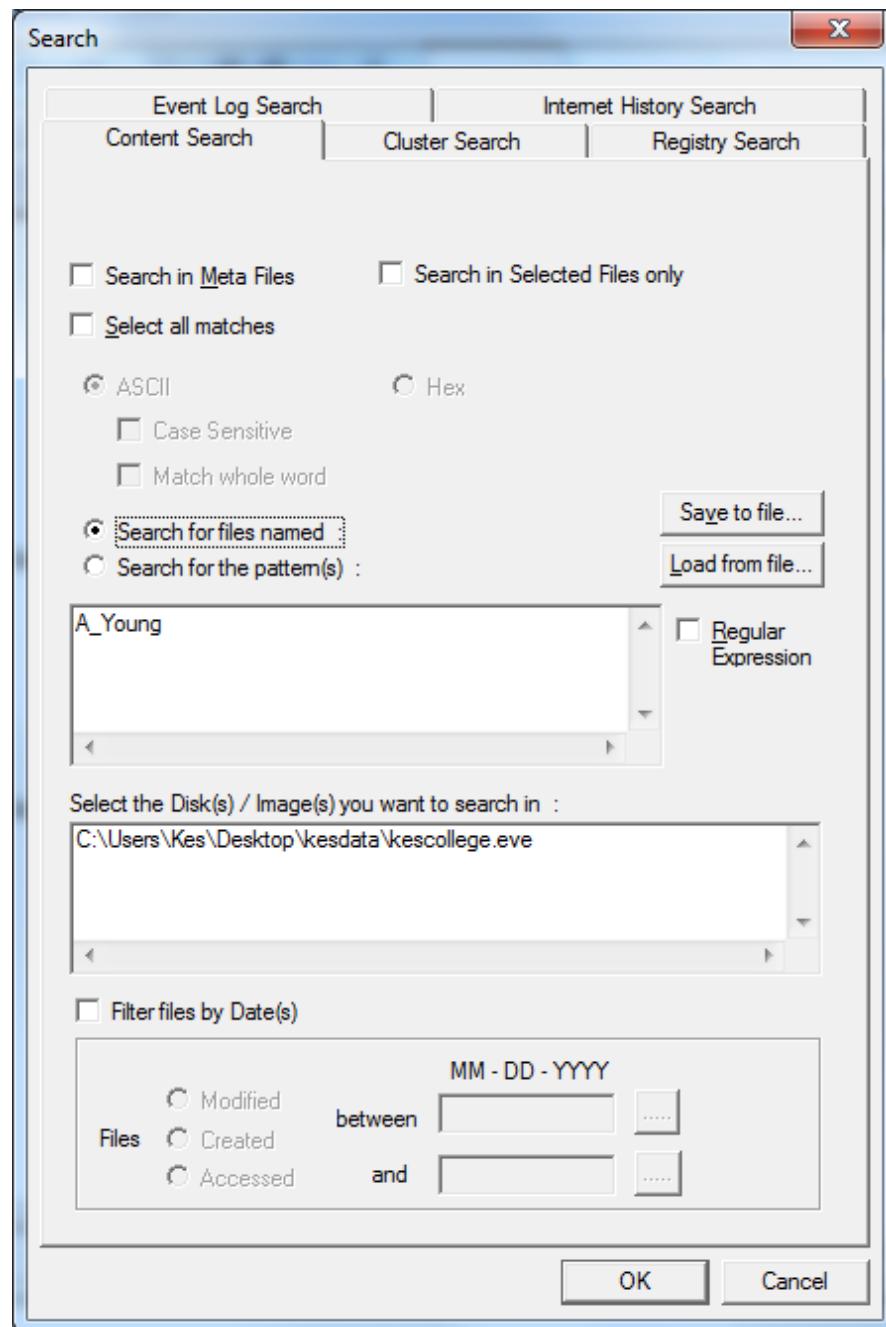
Step 7 : the cluster view is seen from the cluster view in left panel.



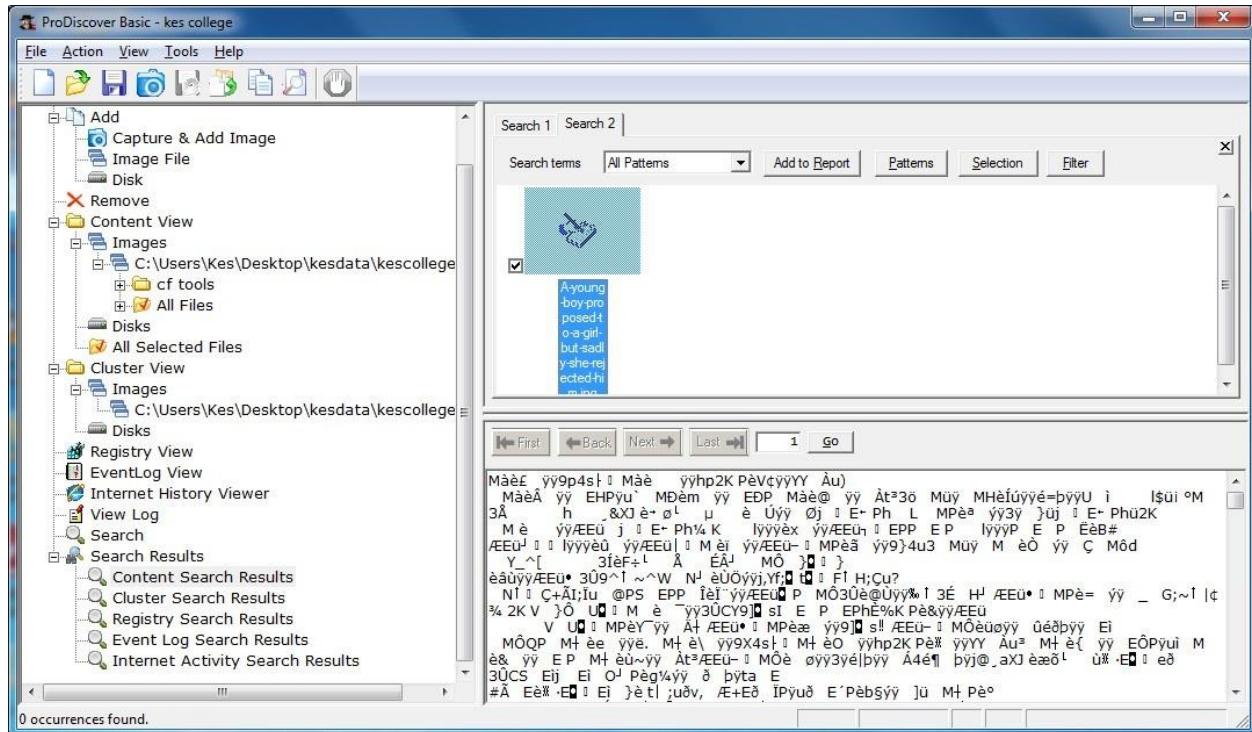
Step 8 : We can also view gallery view by Right Click.



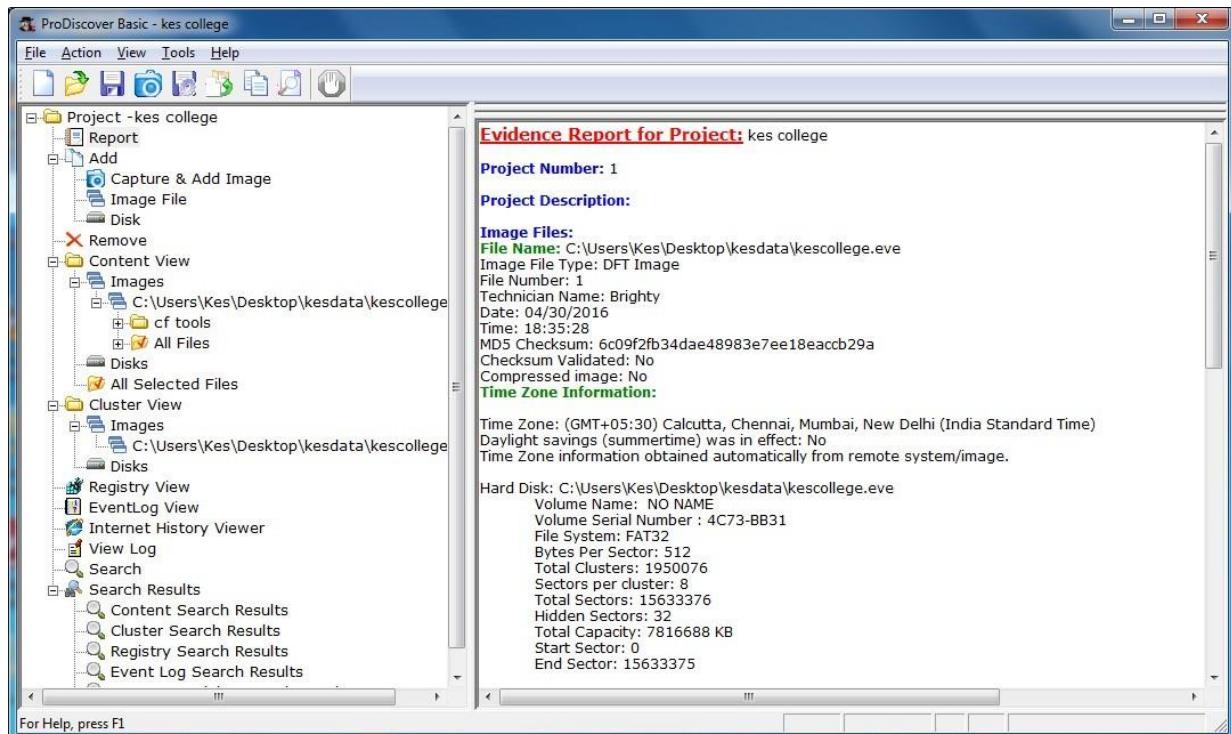
Step 9: Keyword search. Click on Search in left pane and Enter the file name to be searched in the image created.

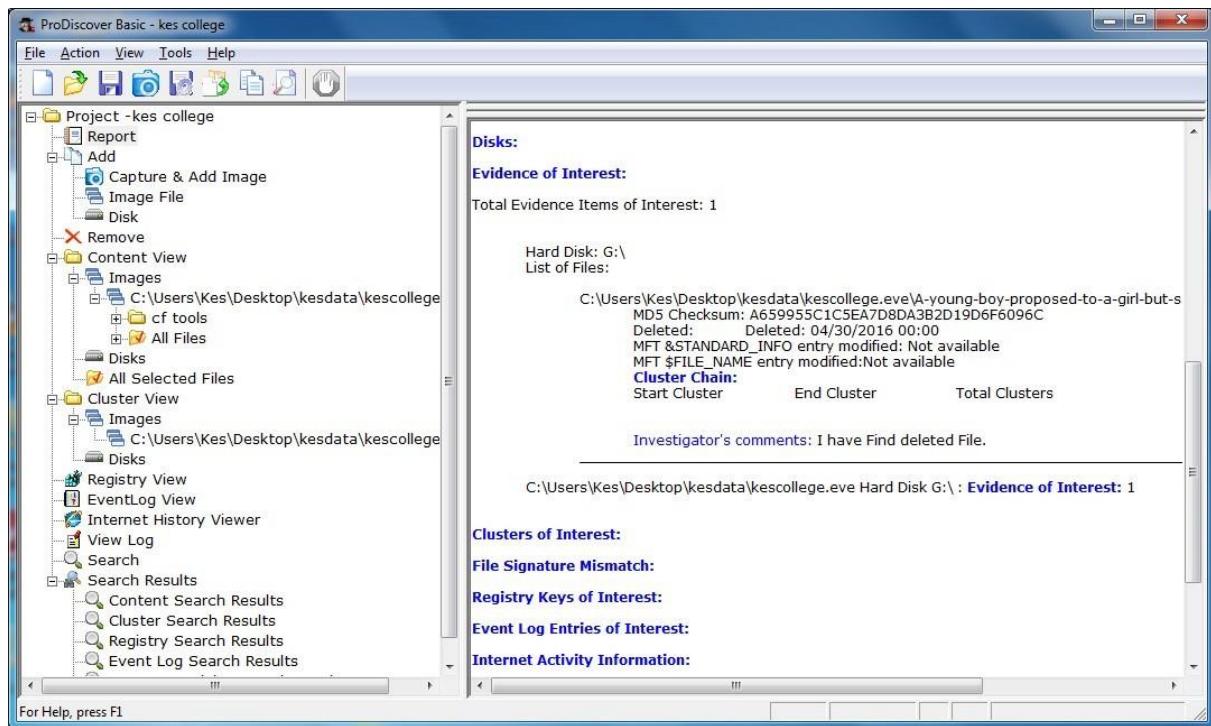


Step 10 : Output of Keyword search.



Step 11 : Click on View>Report.





PRACTICAL 3

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

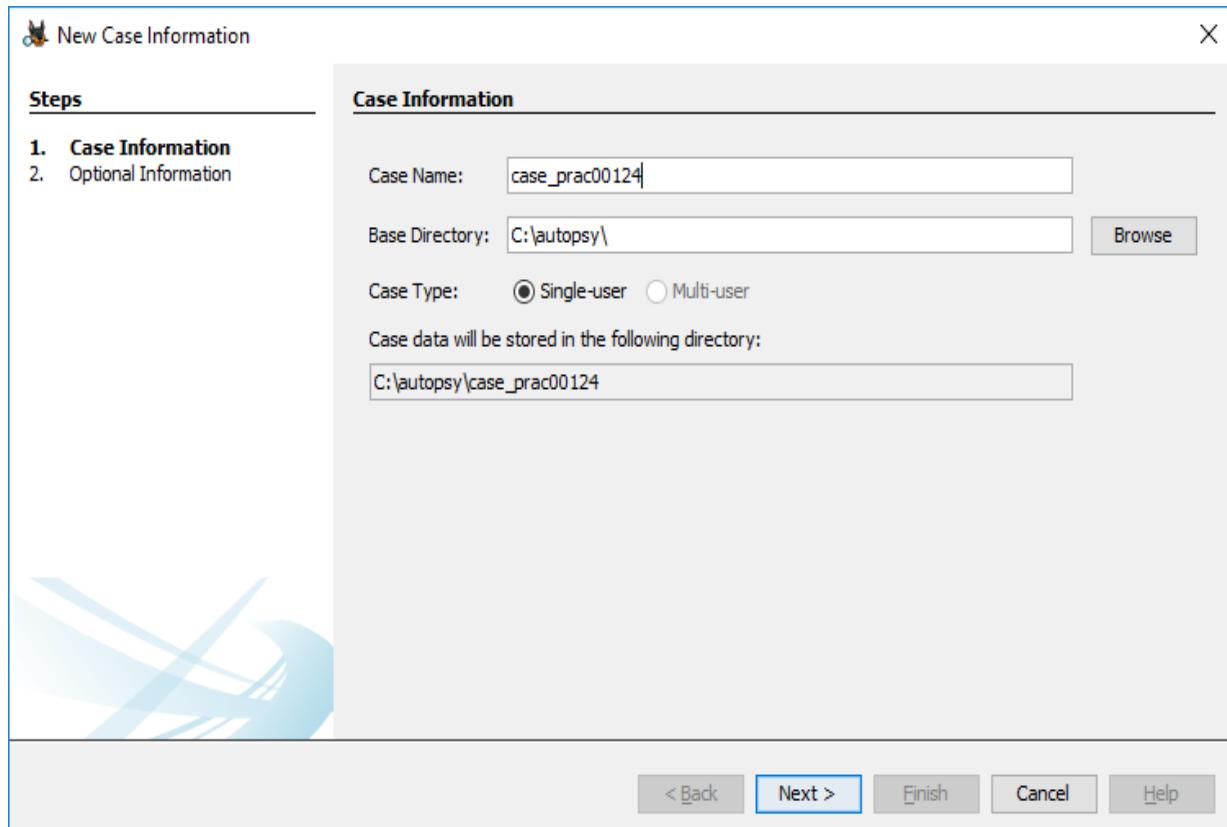
Step 1 : Open Autopsy



Step 2 : Click on new case



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



New Case Information

Steps

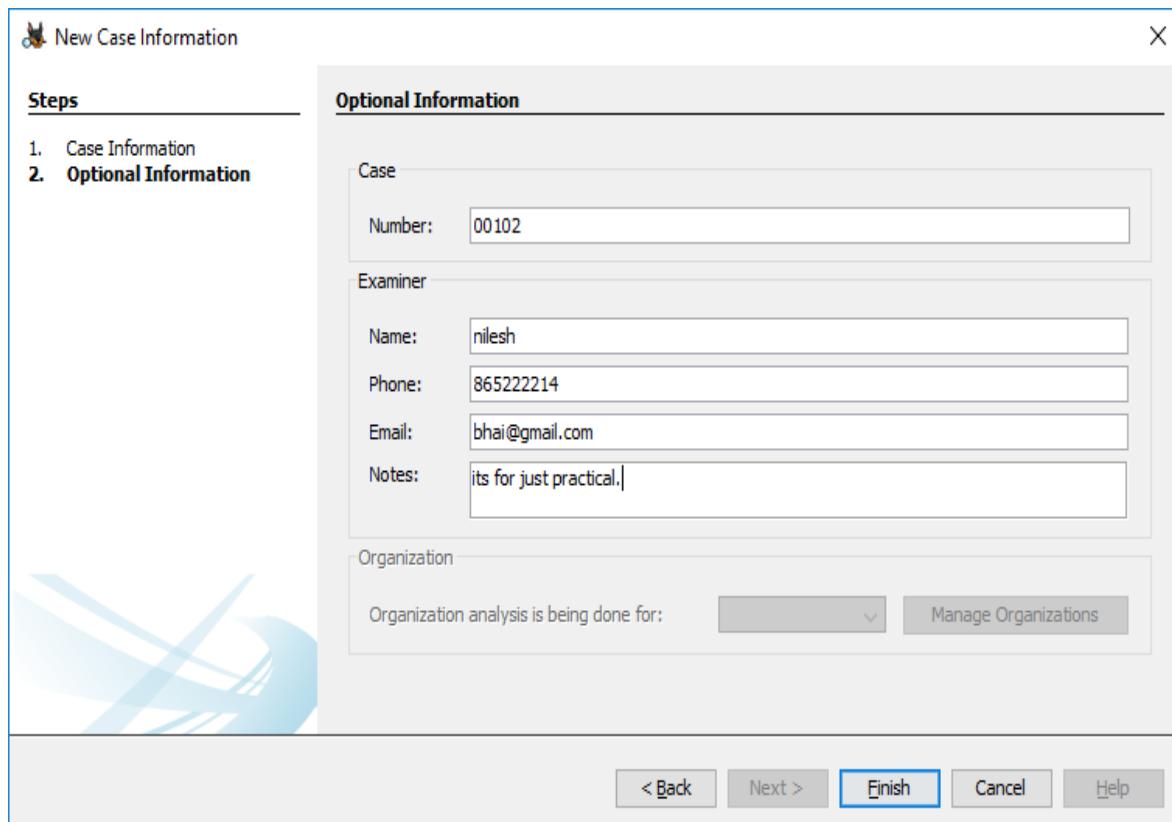
1. Case Information
2. Optional Information

Case Information

Case Name: Base Directory: Case Type: Single-user Multi-user
Case data will be stored in the following directory:

< Back

Step 4 : Enter further details and click on next button



New Case Information

Steps

1. Case Information
2. Optional Information

Optional Information

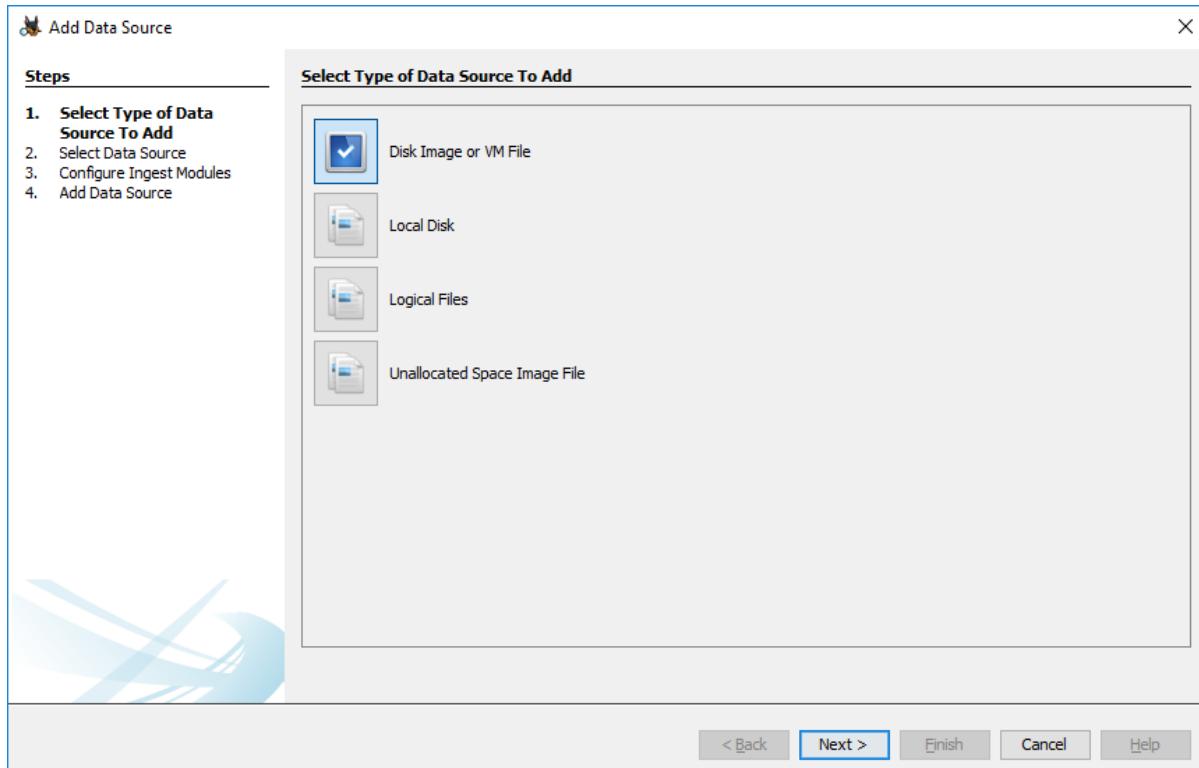
Case
Number:

Examiner
Name:
Phone:
Email:
Notes:

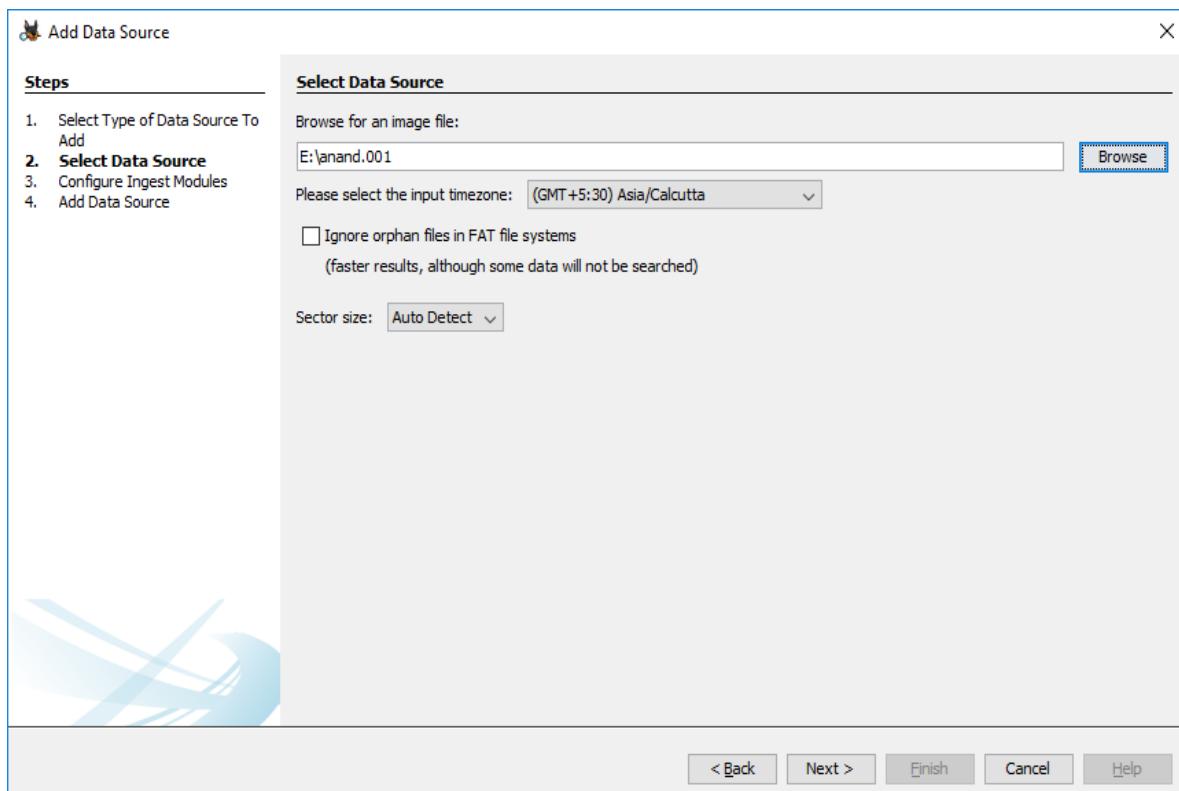
Organization
Organization analysis is being done for:

< Back

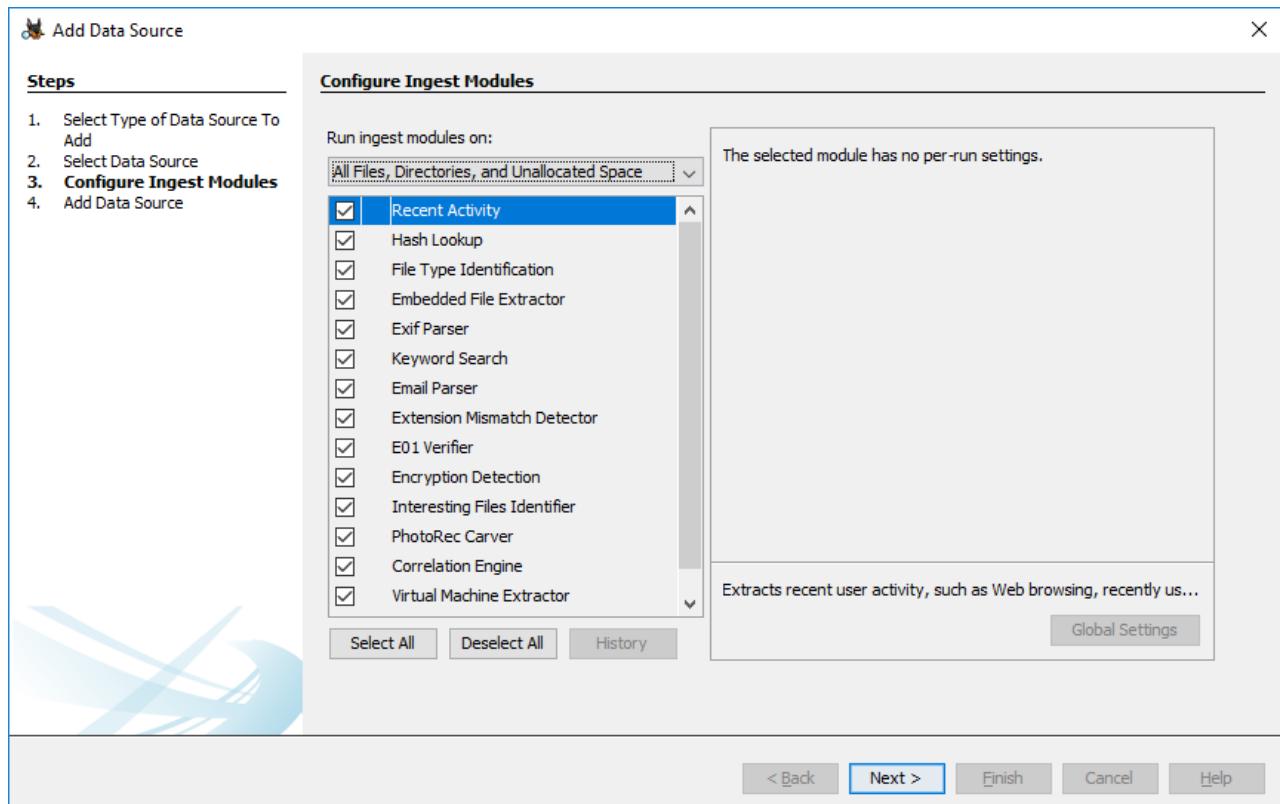
Step 5 : Now here we have to select Type of data source to add , in our case disk image or VM file and click on next



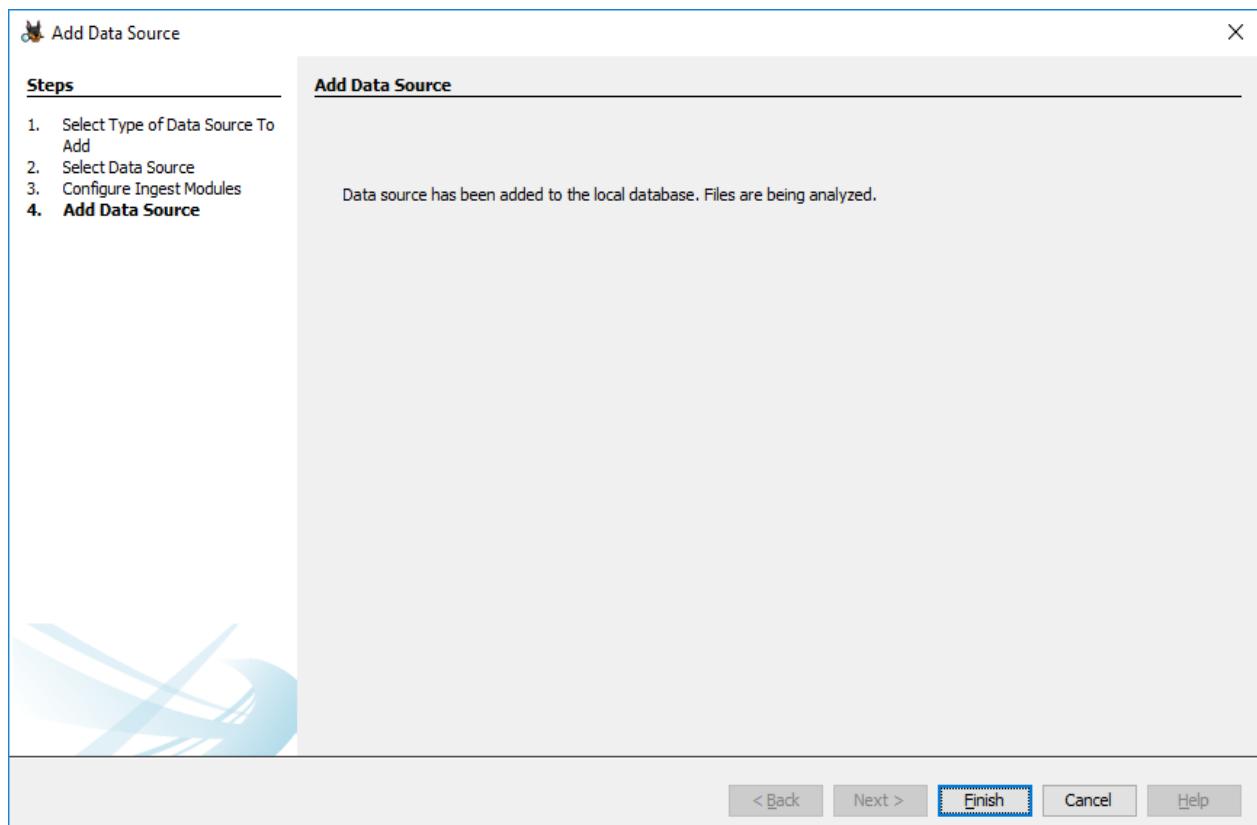
Step 6 : Now we have to select image file and click on next button



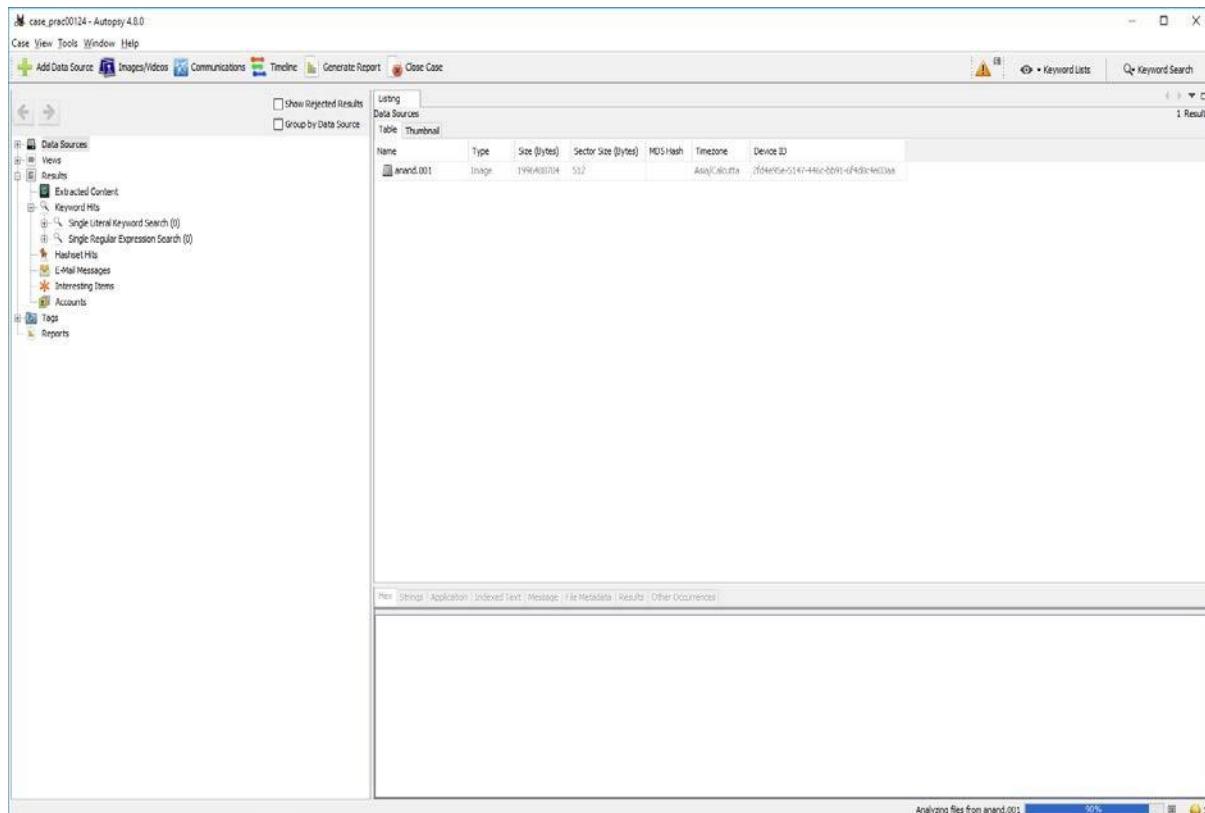
Step 7 : Now click on select all in order to Run ingest modules on: and click on next.



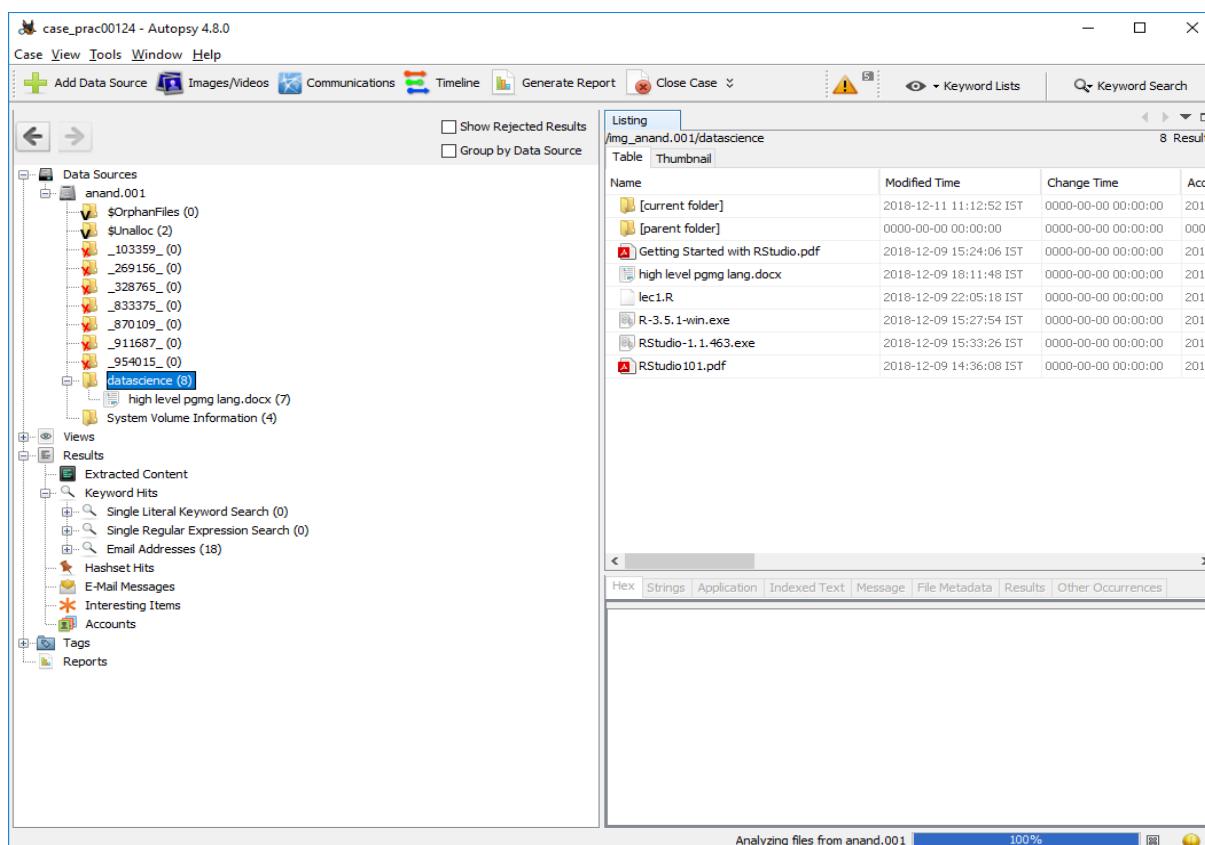
Step 8 : Now click on finish



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



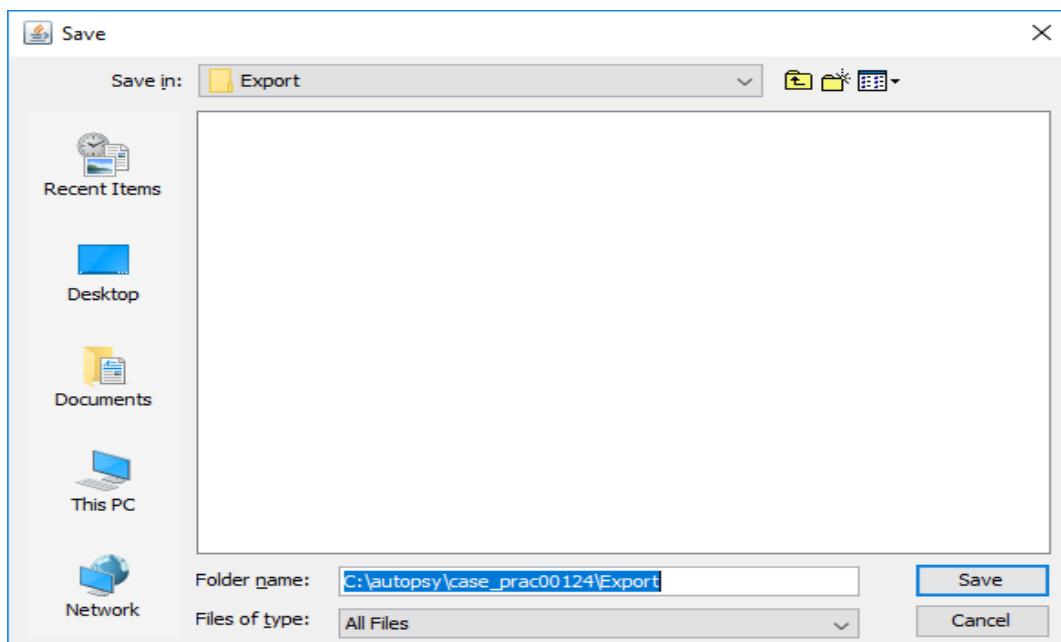
Step 11 : Expand the tree from left side panel to view the document files.

The screenshot shows the Autopsy 4.8.0 interface. The left sidebar displays a hierarchical tree of data sources and results. Under 'Data Sources', 'anand.001' is expanded, showing various file types like '\$OrphanFiles', '\$Unalloc', and several deleted files represented by red X icons. Other data sources listed include 'datascience (8)' which contains a file named 'high level pgmg lang.docx'. The 'Deleted Files' node under 'Views' has 8 items. The 'Results' section includes 'Extracted Content', 'Keyword Hits' (with sub-options for Single Literal Keyword Search, Single Regular Expression Search, and Email Addresses), and 'Interesting Items' (with sub-options for HashSet Hits, E-Mail Messages, and Accounts). The main pane on the right is titled 'Listing' and shows a table of recovered files. The table has two columns: 'Name' and 'Location'. The 'Name' column lists file names such as '_269156_', '_328765_', '_954015_', '_833375_', '_870109_ (selected)', '_911687_', '_103359_', 'mongodb-win32-x86_64-2012plus-latest-signed.msi', 'f1597948.exe', 'f1682120.txt', 'f1682256.java', 'f1682304.pcx', 'f1682332.deb', 'f1682380.deb', 'f1682512.deb', and 'f1682808.rph'. The 'Location' column shows their paths within the recovered structure. Below the table are tabs for Hex, Strings, Application, Indexed Text (which is selected), Message, File Metadata, Results, and Other Occurrences. The indexed text area below the tabs displays the message 'No indexed text for this file.'

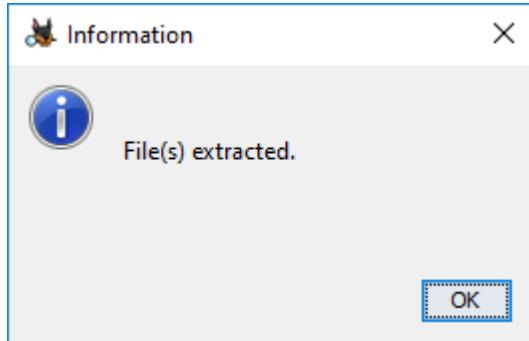
Step 12 : To recover the files , go to view code → Deleted files node , here select any file and right click on it then select Extract files option

The screenshot shows the Autopsy 4.8.0 interface. The left sidebar contains a tree view of data sources, views, and results. The main pane displays a list of extracted files under the 'Listing' tab. The table has columns for Name and Location. A context menu is open over a file named 'f1682332.deb'. The menu options include Properties, View File in Directory, View in New Window, Open in External Viewer, View File in Timeline..., Extract File(s), Add File Tag, Remove File Tag, and Add file to hash set. At the bottom of the main pane, there are tabs for Hex, Strings, Application, Indexed Text, Message, File Metadata, Results, and Other Occurrences. The 'Indexed Text' tab is selected, showing the message 'No indexed text for this file.'

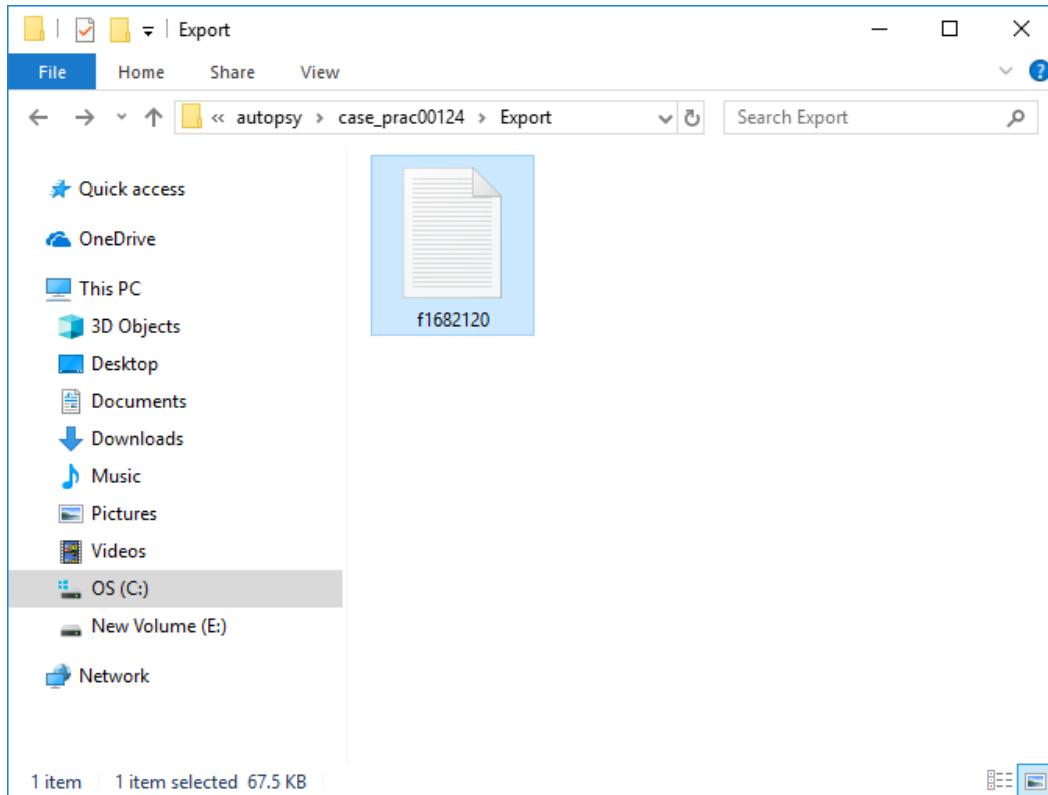
Step 12: Select Path where you want to save extracted file and click on save .



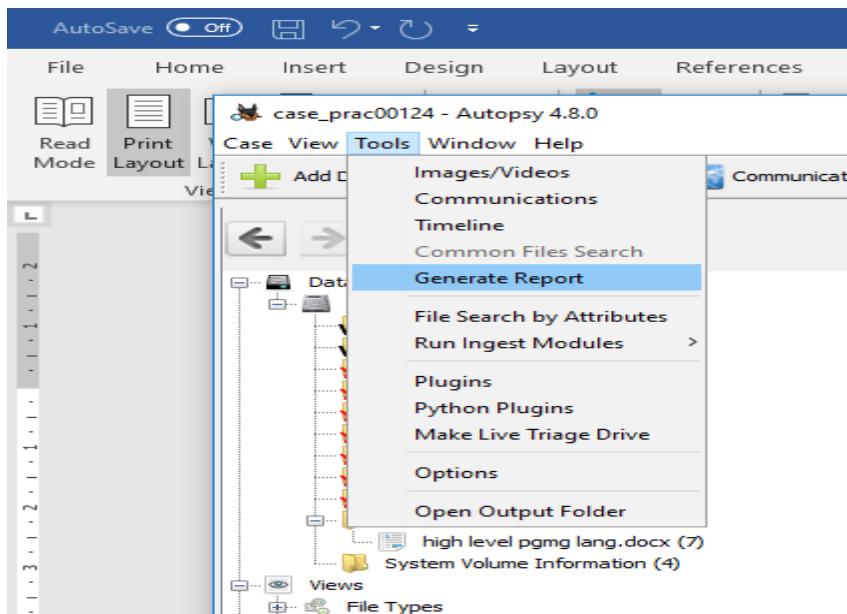
Step 13 : Now click on OK



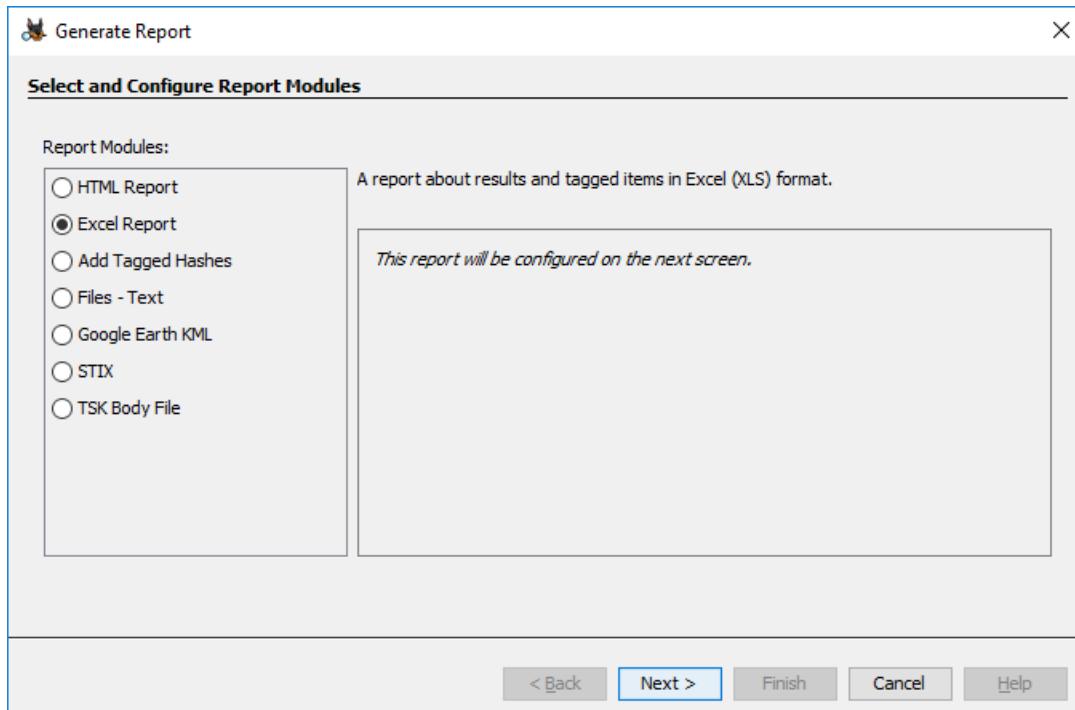
Step 14 : Now go to C:\autopsy\case_prac00124\Export folder to see recover file



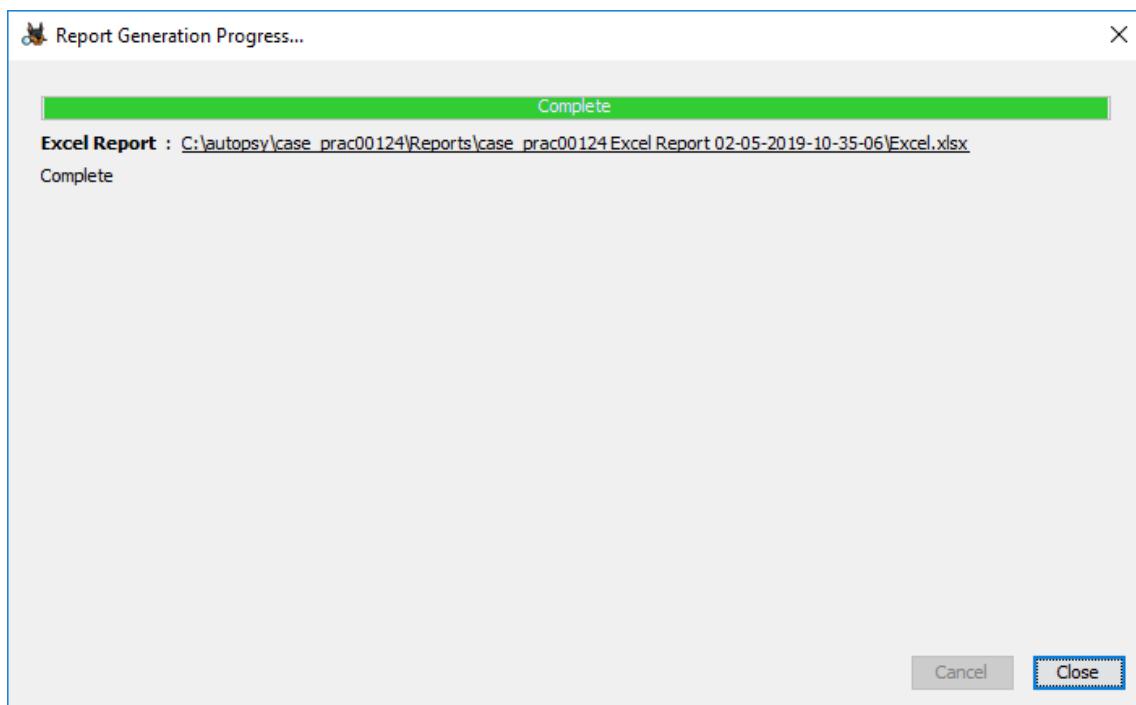
Step 15 : Click on generate report from Autopsy window and select the Excel format and click on next



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

Case View Tools Window Help

Add Data Source Images/Videos Communications Timeline Generate Report Close Case

Listing

Source Module Name	Report Name	Created Time
Excel Report		2019-02-05 10:35

Data Sources

- anand.001
 - \$OrphanFiles (0)
 - \$Unalloc (2)
 - _103359_ (0)
 - _269156_ (0)
 - _328765_ (0)
 - _833375_ (0)
 - _870109_ (0)
 - _911687_ (0)
 - _954015_ (0)
 - datascience (8)
 - high level pgmg lang.docx (7)
 - System Volume Information (4)

Views

- File Types
 - Deleted Files
 - File System (8)
 - All (34)
- MB File Size

Results

- Extracted Content
- Keyword Hits
 - Single Literal Keyword Search (0)
 - Single Regular Expression Search (0)
 - Email Addresses (18)
- Hashset Hits
- E-Mail Messages
- Interesting Items
- Accounts

Tags

Reports

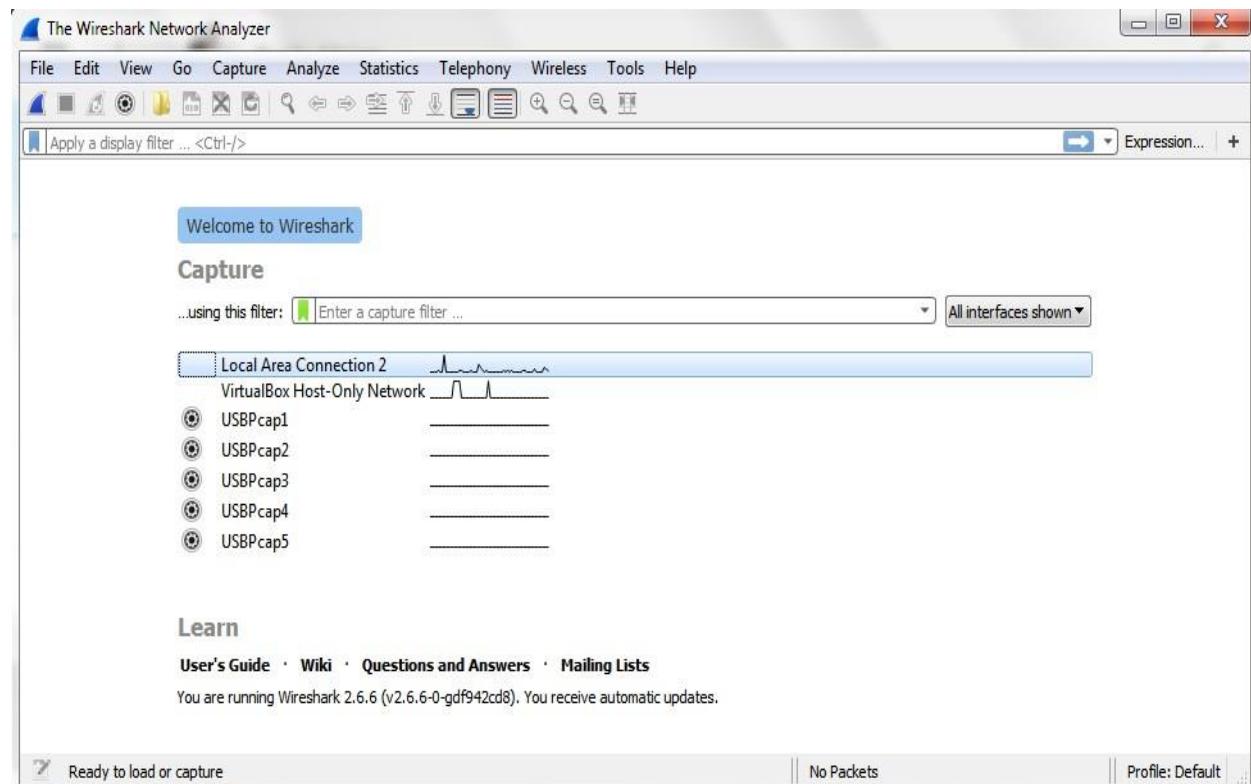
PRACTICAL 4

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

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

Capturing Packets

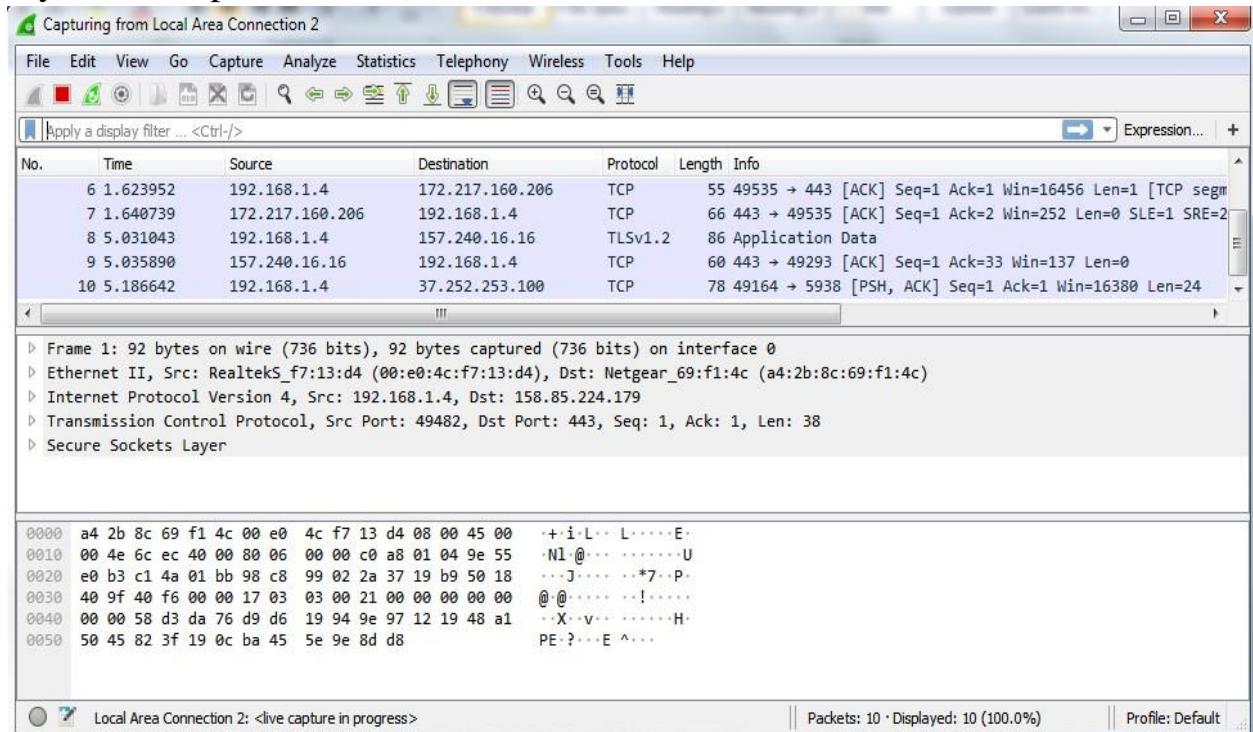
Capture traffic on your wireless network, click your wireless interface. You can configure advanced features by clicking Capture > Options, but this isn't necessary for now.



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

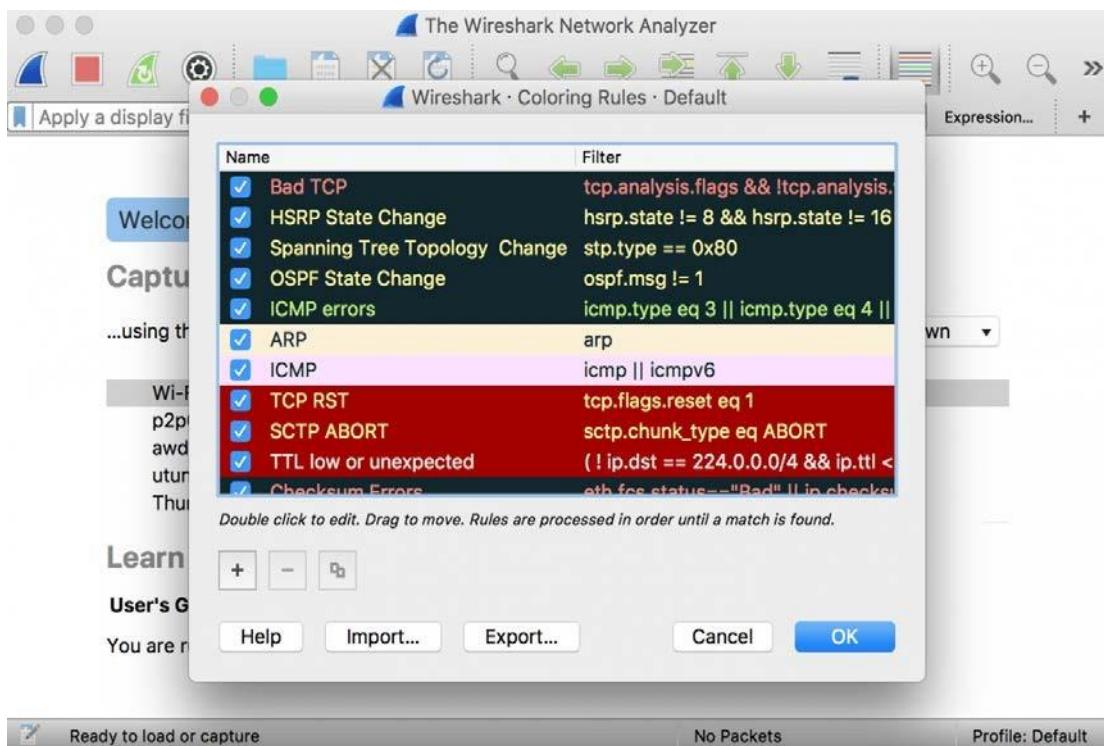
Different packets are seen highlighted in various different colors. This is Wireshark’s way of displaying traffic to help you easily identify the types of it. Default colors are:

Light Purple color for TCP traffic

Light Blue color for UDP traffic

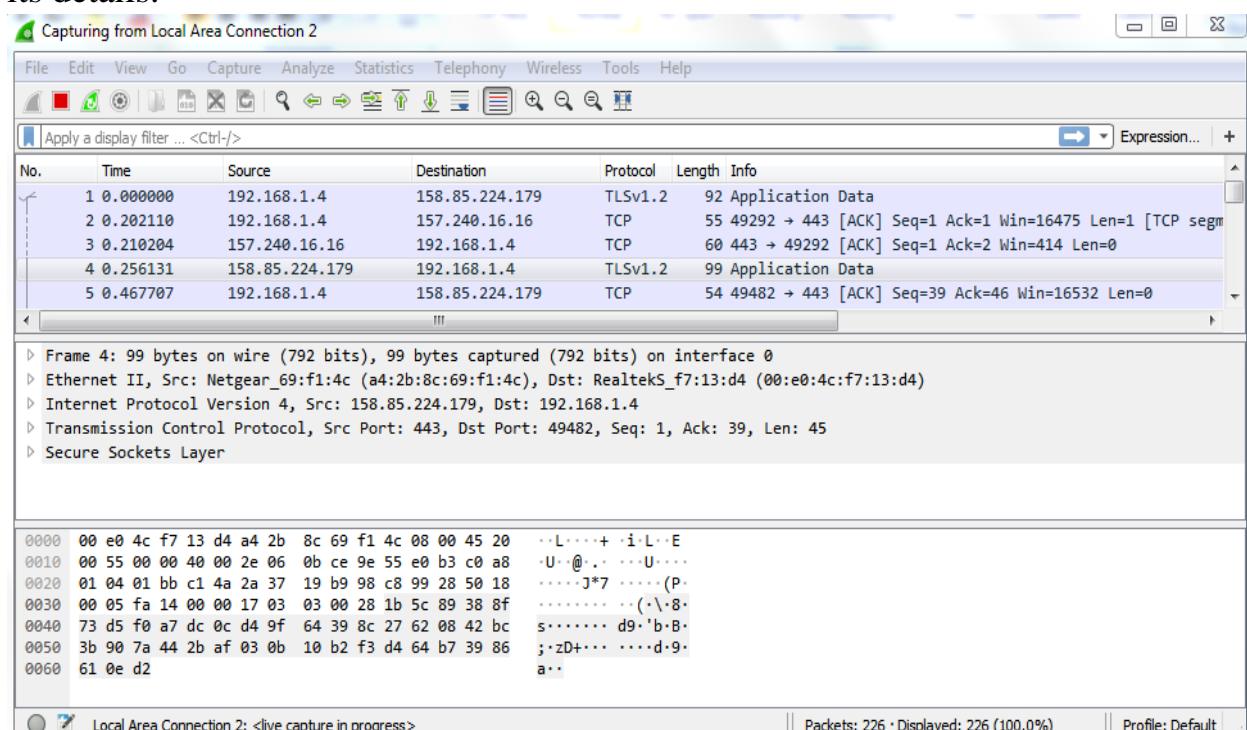
Black color identifies packets with errors – example these packets are delivered in an unordered manner.

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.

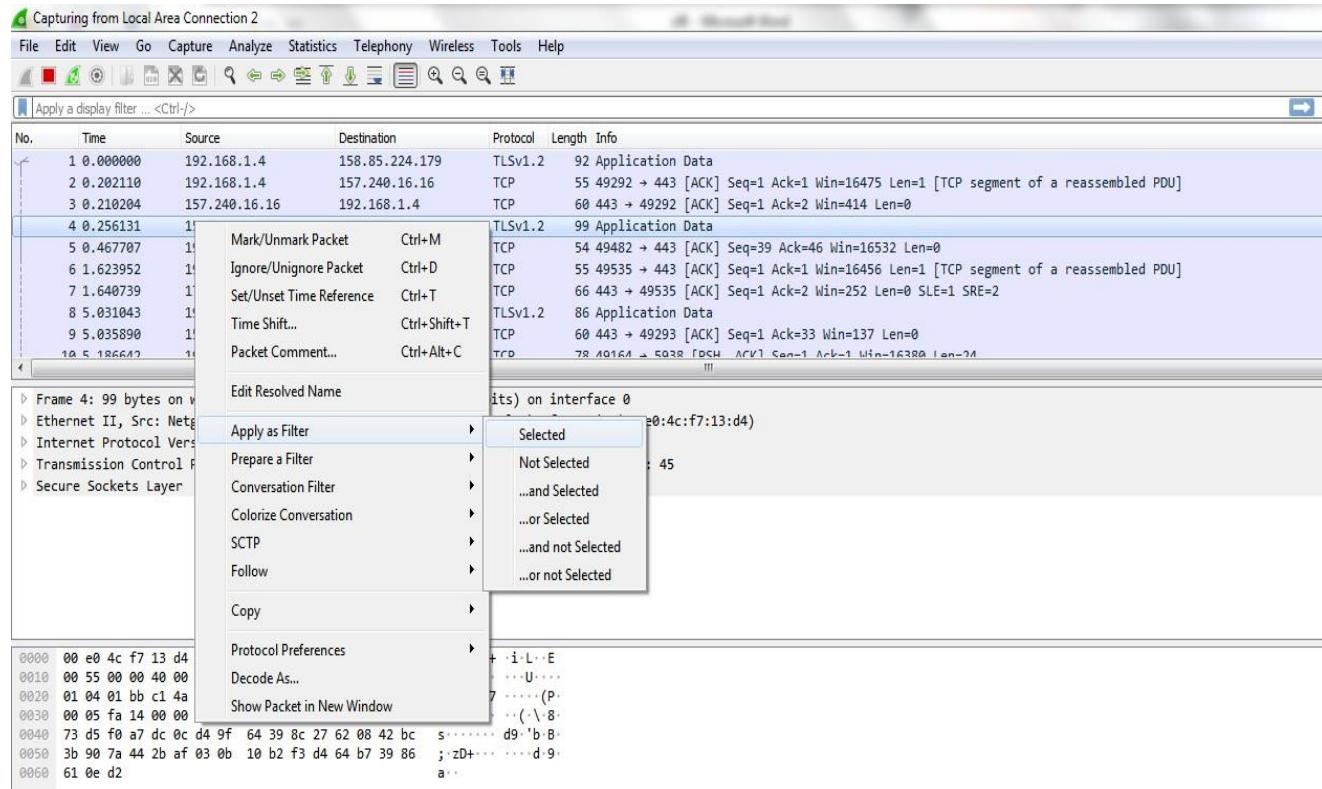


Analyze the captured Packets:

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

No.	Time	Source	Destination	Protocol	Length	Info
49176	632.590744	192.168.1.4	216.58.219.227	TCP	55	[TCP Keep-Alive] 49231 → 443 [ACK] Seq=4349 Ack=5923 Win=65408 Len=1
49177	632.915897	216.58.219.227	192.168.1.4	TCP	66	[TCP Keep-Alive ACK] 443 → 49231 [ACK] Seq=5923 Ack=4350 Win=69632 Len=0 SRE=4349
49178	633.207727	0.0.0.0	224.0.0.1	IGMPv2	60	Membership Query, general
49179	633.415028	192.168.1.4	239.255.255.250	IGMPv2	46	Membership Report group 239.255.255.250
49180	633.876818	192.168.1.4	172.217.167.163	TCP	55	[TCP Keep-Alive] 49185 → 443 [ACK] Seq=19248 Ack=947960 Win=84176 Len=1
49181	633.901488	172.217.167.163	192.168.1.4	TCP	66	[TCP Keep-Alive ACK] 443 → 49185 [ACK] Seq=947960 Ack=19249 Win=75776 Len=0 SRE=19248
49182	634.414944	192.168.1.4	224.0.0.252	IGMPv2	46	Membership Report group 224.0.0.252
49183	640.313942	192.168.1.3	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
49184	640.604029	192.168.1.3	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
49185	640.904021	192.168.1.3	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1

2. Display packets which are coming from specific IP-address
 ➤ 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
22	20.918775	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

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
90	05.721021	192.168.1.4	192.168.1.1	DNS	85	Standard query 0xc7f4 A teredo.ipv6.microsoft.com

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
39210	279.420870	192.168.1.4	23.57.219.27	OCSP	137	Request

5. Display packets which are using http request

- http.request

No.	Time	Source	Destination	Protocol	Length	Info
40	50.307358	192.168.1.3	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
41	50.607228	192.168.1.3	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
46	60.015835	192.168.1.3	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
47	60.306194	192.168.1.3	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
48	60.605851	192.168.1.3	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
49	70.031605	192.168.1.3	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
50	70.321279	192.168.1.3	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
51	70.626289	192.168.1.3	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
53	73.874454	192.168.1.4	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
→ 58	74.985092	192.168.1.4	192.168.1.1	HTTP	250	GET /rootDesc.xml HTTP/1.1
67	76.972624	192.168.1.4	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1

6. Display packets which are using TCP protocol

- tcp

No.	Time	Source	Destination	Protocol	Length	Info
31	41.077503	192.168.1.4	188.65.76.135	TCP	54	49163 → 5938 [ACK] Seq=25 Ack=25 Win=16592 Len=0
32	41.184892	188.65.76.135	192.168.1.4	TCP	78	[TCP Spurious Retransmission] 5938 → 49163 [PSH, ACK] Seq=1 Ack=25 Win=1022 Len=24
33	41.184946	192.168.1.4	188.65.76.135	TCP	66	[TCP Dup ACK 31#1] 49163 → 5938 [ACK] Seq=25 Ack=25 Win=0 Len=0 SLE=1 SRE=25
37	45.858801	192.168.1.4	188.65.76.135	TCP	78	49163 → 5938 [PSH, ACK] Seq=25 Ack=25 Win=16592 Len=24
38	46.087275	188.65.76.135	192.168.1.4	TCP	60	5938 → 49163 [ACK] Seq=25 Ack=49 Win=1022 Len=0
45	54.780090	192.168.1.4	104.25.218.21	TCP	54	49171 → 443 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
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
56	74.984790	192.168.1.1	192.168.1.4	TCP	66	56688 → 49173 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1 WS=2
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
60	74.985276	192.168.1.1	104.25.218.21	TCP	60	56688 → 104.25.218.21 [ACK] Seq=1 Ack=107 Win=6011 Len=0

7. Display packets having no error connecting to server

- http.response.code==200

No.	Time	Source	Destination	Protocol	Length	Info
40241	315.834863	27.106.94.17	192.168.1.4	TCP	455	HTTP/1.1 200 OK [TCP segment of a reassembled PDU]
40251	315.941483	192.168.1.1	192.168.1.4	HTTP/X...	315	HTTP/1.1 200 OK
40261	315.967166	192.168.1.1	192.168.1.4	HTTP	250	HTTP/1.1 200 OK
40270	315.968680	192.168.1.4	192.168.1.1	HTTP	191	HTTP/1.1 200 OK
40282	315.977822	192.168.1.1	192.168.1.4	HTTP/X...	539	HTTP/1.1 200 OK
40294	315.982033	192.168.1.1	192.168.1.4	HTTP/X...	557	HTTP/1.1 200 OK
40308	315.999143	192.168.1.1	192.168.1.4	HTTP/X...	315	HTTP/1.1 200 OK
40318	316.005125	192.168.1.1	192.168.1.4	HTTP	250	HTTP/1.1 200 OK
40327	316.007892	192.168.1.4	192.168.1.1	HTTP	191	HTTP/1.1 200 OK
40339	316.015485	192.168.1.1	192.168.1.4	HTTP/X...	539	HTTP/1.1 200 OK
40351	316.010290	192.168.1.1	192.168.1.1	HTTP/X...	557	HTTP/1.1 200 OK

8. Display packets having port number 80

➤ `tcp.port==80 || udp.port==80`

No.	Time	Source	Destination	Protocol	Length	Info
40216	315.186100	192.168.1.4	172.217.160.206	TCP	54	49295 → 80 [ACK] Seq=1 Ack=1 Win=66240 Len=0
40217	315.186313	192.168.1.4	172.217.160.206	HTTP	293	HEAD /edged1/release2/chrome_component/Hp07sha1Vdw_4916/4916_all_crl-set-13576662708261436161.data.crx
40218	315.209073	172.217.160.206	192.168.1.4	TCP	60	80 → 49295 [ACK] Seq=1 Ack=240 Win=61952 Len=0
40225	315.497872	172.217.160.206	192.168.1.4	HTTP	608	HTTP/1.1 302 Found
40228	315.512340	192.168.1.4	27.106.94.17	TCP	66	49296 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
40231	315.693760	192.168.1.4	172.217.160.206	TCP	54	49295 → 80 [ACK] Seq=240 Ack=555 Win=65684 Len=0
40237	315.823271	27.106.94.17	192.168.1.4	TCP	66	80 → 49296 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1452 SACK_PERM=1 WS=256
40238	315.823365	192.168.1.4	27.106.94.17	TCP	54	49296 → 80 [ACK] Seq=1 Ack=1 Win=66792 Len=0
40239	315.823558	192.168.1.4	27.106.94.17	HTTP	404	HEAD /edged1/release2/chrome_component/Hp07sha1Vdw_4916/4916_all_crl-set-13576662708261436161.data.crx
40241	315.834863	27.106.94.17	192.168.1.4	HTTP	455	HTTP/1.1 200 OK
40404	216.006000	10.1.169.1.1	27.106.94.17	TCP	54	49296 → 80 [ACK] Seq=251 Ack=101 Win=66280 Len=0

9. Display packets which contains keyword facebook

➤ `tcp contains facebook`

No.	Time	Source	Destination	Protocol	Length	Info
7711	32.085504	192.168.1.4	31.13.79.35	TLSv1.3	571	Client Hello
8160	32.867205	192.168.1.4	31.13.79.35	TLSv1.3	571	Client Hello
9739	35.561576	192.168.1.4	157.240.16.35	TLSv1.3	571	Client Hello
29814	162.425666	192.168.1.4	157.240.16.35	TLSv1.3	571	Client Hello
37226	273.164934	192.168.1.4	157.240.16.16	TLSv1.2	571	Client Hello
37388	274.375759	192.168.1.4	157.240.16.16	TLSv1.3	571	Client Hello
43811	381.014078	192.168.1.4	157.240.16.35	TLSv1.3	571	Client Hello
47765	569.305448	192.168.1.4	157.240.16.35	TLSv1.3	571	Client Hello

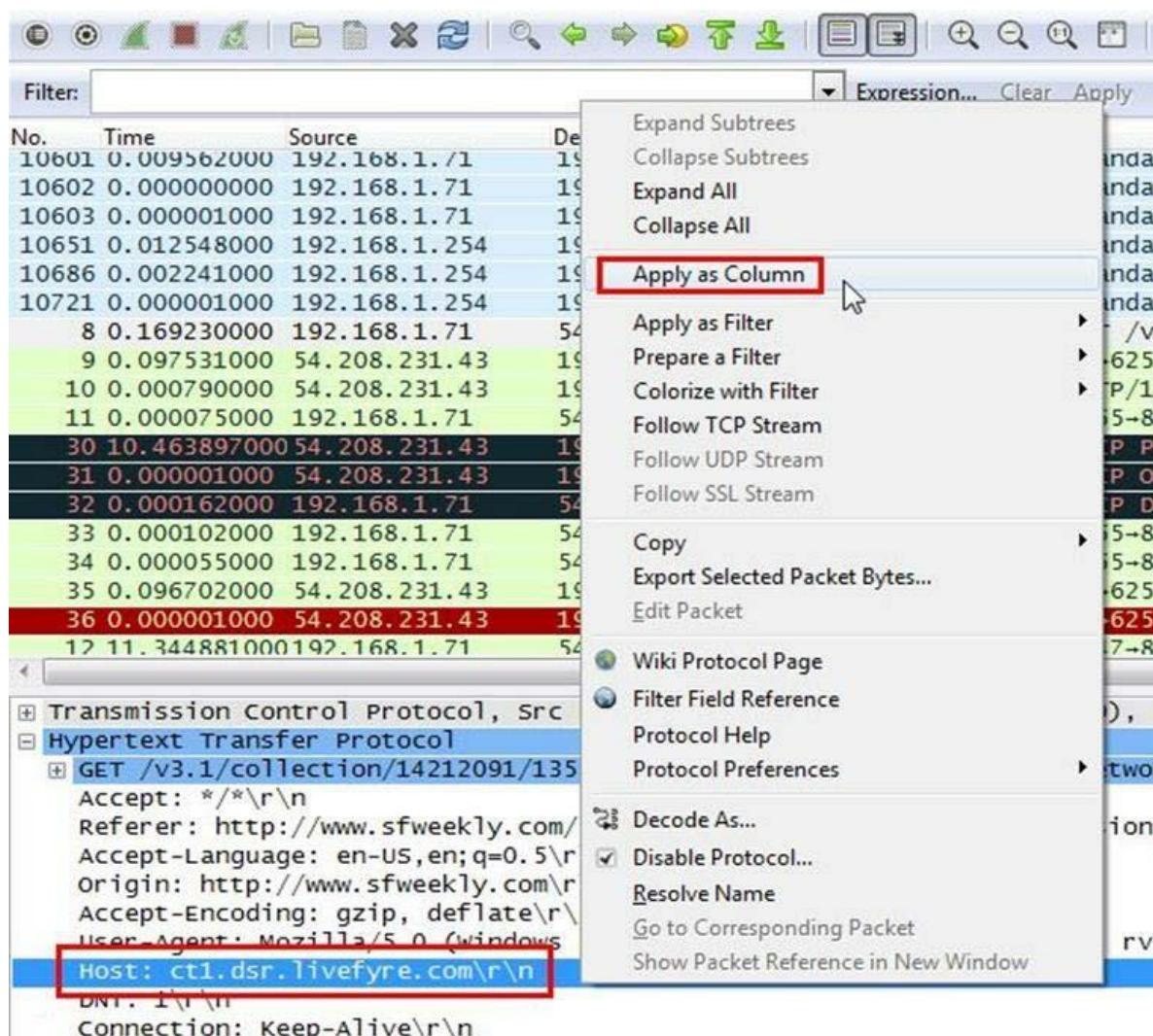
PRACTICAL 5

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?

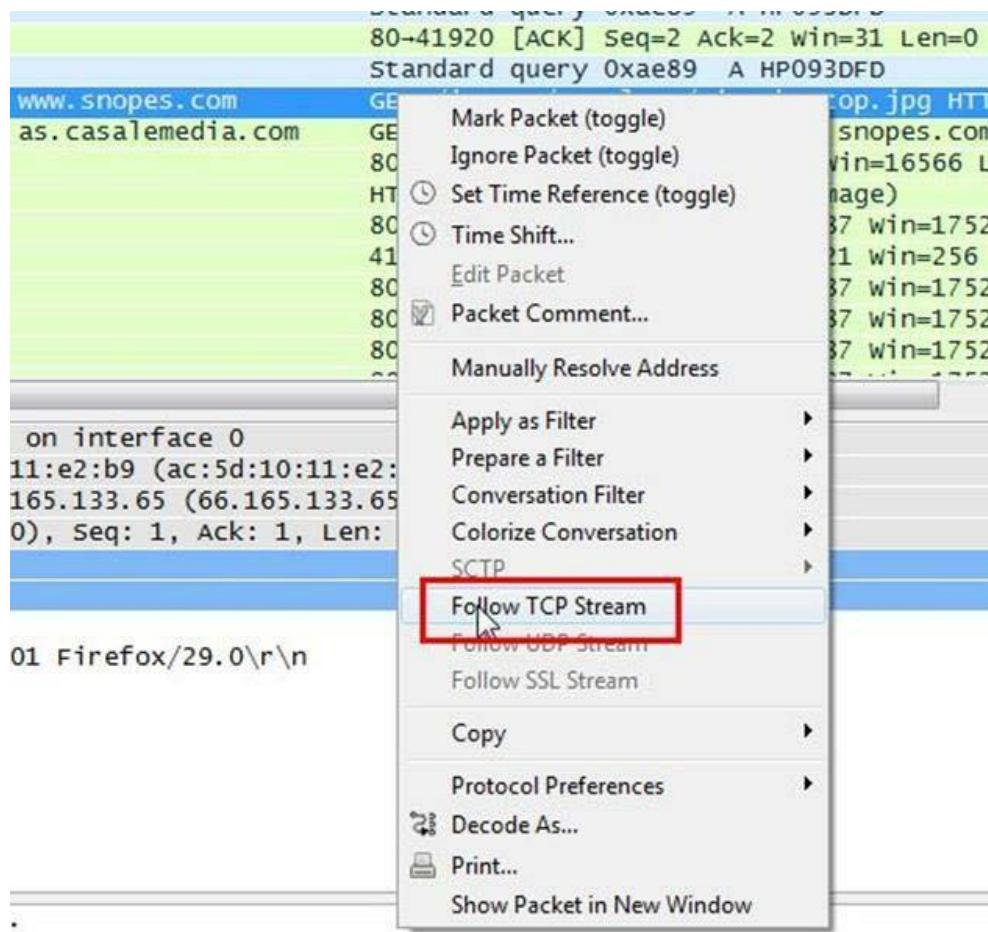
Analysis – The domain name be found from host header so we will set host header column where we will see all domain name. Select any HTTP request and expand the Hypertext Transfer Protocol then right click on Host header and then Apply as Column.



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

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

Stream Content

```

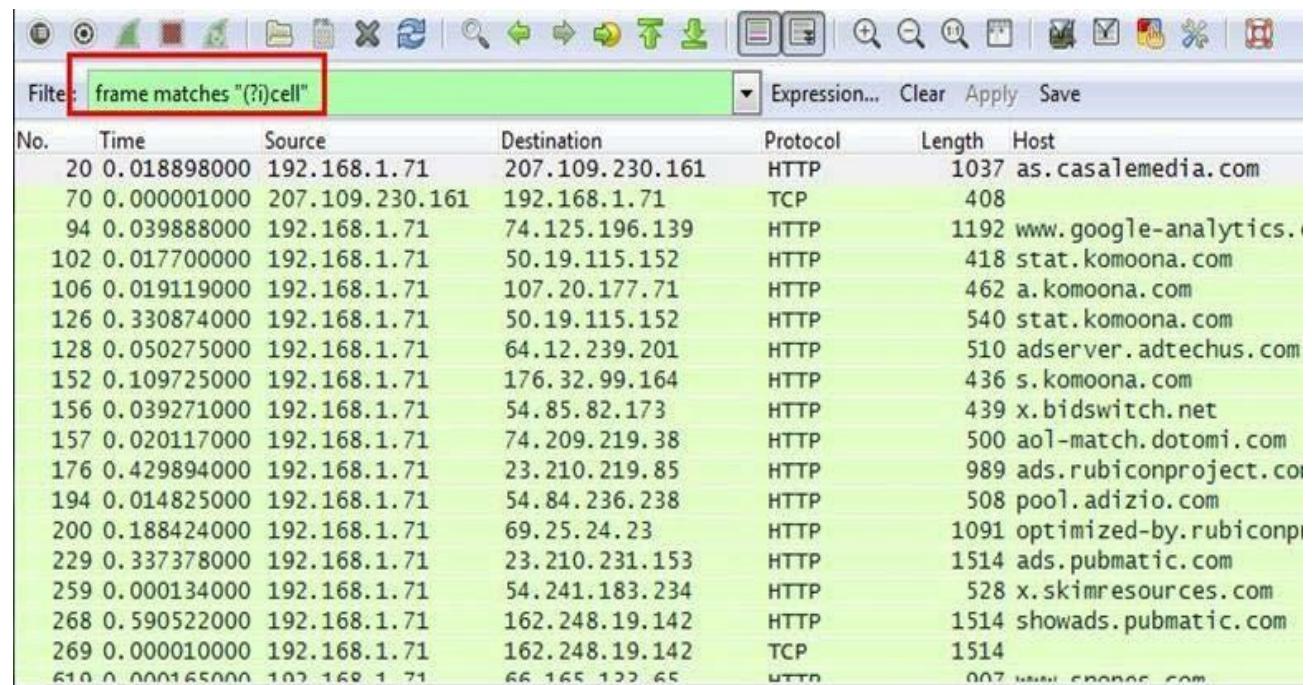
GET /images/template/site-bg-top.jpg HTTP/1.1
Host: www.snopes.com
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:29.0) Gecko/20100101 Firefox/29.0
Accept: image/png,image/*;q=0.8,*/*;q=0.5
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.snopes.com/style.css
Cookie: ASPSESSIONIDQQQDSBBA=OJMBNHECFCANKIJJGBBMBLDO
Connection: keep-alive

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

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

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”



The screenshot shows the Wireshark interface with a packet list. A search bar at the top contains the expression "frame matches '(?! cell'". The packet list below shows various network interactions, with the first few entries matching the search criteria.

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	
610	0.000165000	192.168.1.71	66.165.122.65	HTTP	907	www.snopes.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"						
				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=7318 Ack=984 Win=16566 Len=354
94 0.039888000	192.168.1.71	74.125.196.139		HTTP	1192	GET /__utm.gif?utmwv=5.3.1&utmn=624349962&utmhn=www.snopes.com&utmcs=windows-1252&utm
102 0.017700000	192.168.1.71	50.19.115.152		HTTP	418	GET /?tagid=cad64dbf73589c9a110884ce73bb72_728_90.js?l=http%3A%2F%2Fwww.snopes.com%2Fhorrors%
106 0.019119000	192.168.1.71	107.20.177.71		HTTP	462	GET /tag/cad674dbf73589c9a110884ce73bb72_728_90.js?l=http%3A%2F%2Fwww.snopes.com%2Fhorrors%
126 0.330874000	192.168.1.71	50.19.115.152		HTTP	540	GET /?tagid=cad674dbf73589c9a110884ce73bb72&v=2.16&cb=516430883&ts=-1&p=cad674dbf73589c9a1
128 0.050272500	192.168.1.71	64.12.239.201		HTTP	510	GET /addy/n/3/0/9423.1/3142865/0/225/ADTECH; loc=100; target=_blank; misc=\$5BTIMESTAMP\$50; rdclic
152 0.109725000	192.168.1.71	176.32.99.164		HTTP	436	GET /passback/np/cad674dbf73589c9a110884ce73bb72.js HTTP/1.1
156 0.039271000	192.168.1.71	54.85.82.173		HTTP	439	GET /sync?ssp=aol HTTP/1.1
157 0.020117000	192.168.1.71	74.209.219.38		HTTP	500	GET /aol/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=bidsswitch&bidsswitch_ssp_id=aol HTTP/1.1
200 0.188424000	192.168.1.71	69.25.24.23		HTTP	1092	GET /a/9192/19861/64229-2.js?&cb=0.18771559557158202&tk_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	1514	GET /AdServer/js/showad.js?rn=516430883 HTTP/1.1
259 0.000134000	192.168.1.71	54.241.183.234		HTTP	528	GET /?provider=adizio&mode=check&uid=1039da81-f78e-44cc-a317-d4139ca80c0c HTTP/1.1
268 0.590522000	192.168.1.71	162.248.19.142		HTTP	1514	GET /AdServer/AdServerServlet?pubId=32702&siteId=46838&adId=80732&kadwidth=728&kadheight=90&
269 0.000001000	192.168.1.71	162.248.19.142		TCP	1514	41950->80 [ACK] Seq=1461 Ack=1 Win=16445440 Len=1460
610 0.000045000	107.20.177.71	66.169.122.66		HTTP	007	GET /wwwes/techno/cellcharge.htm HTTP/1.1

ce 0
Sd:10:11:e2:b9
74.125.196.139
ck: 1, Len: 1138

utmcs=windows-1252&utmsr=1920x1080&utmvp=1920x953&utmvc=24-bit&utmul=en-us&utmje=1&utmfl=13.%20r0&utmdt=snopes.com%3A%20cell%20Phone%20recharging%20Electro

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

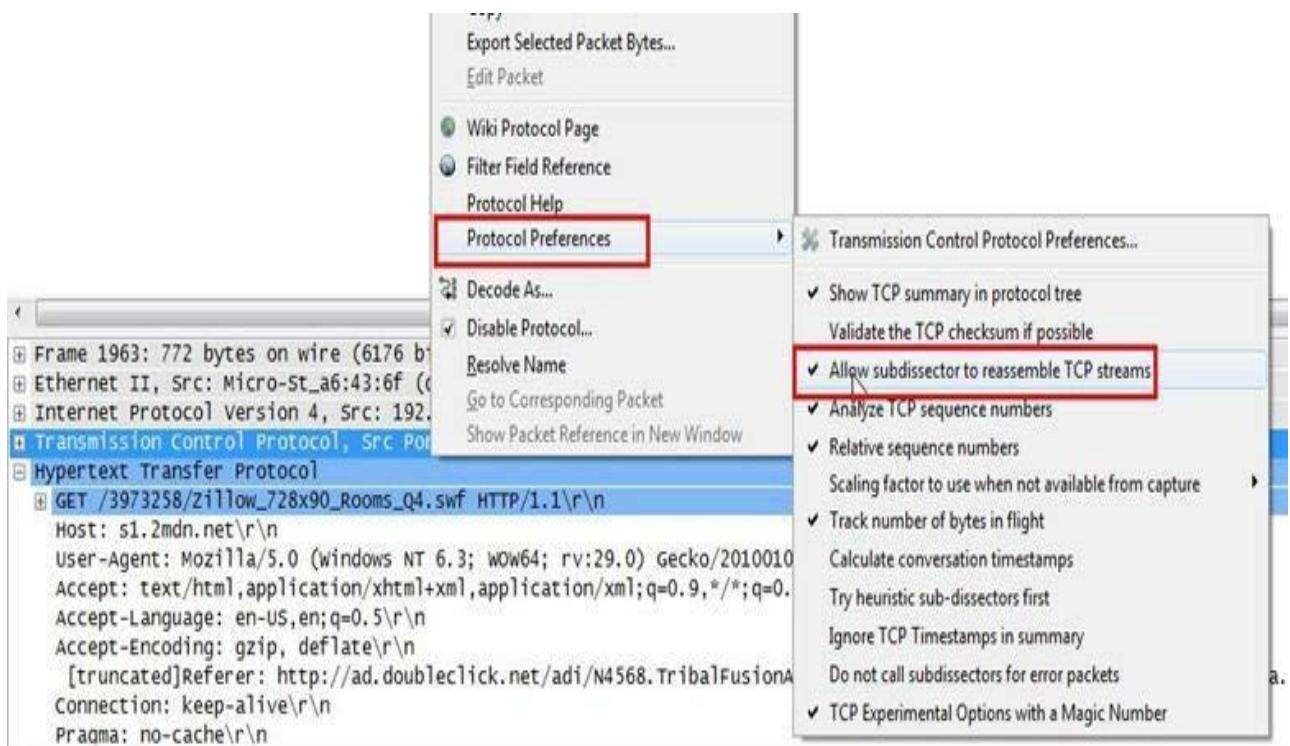
Analysis – As we did in the last challenge, we will apply a regular express filter for the Zillow keyword. Apply frame matched “(?) zillow”

Filter: frame matches "(?)zillow"						
				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 /?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 0.010773000	107.20.177.71	107.169.1.71		TCP	60	80->41935 [ACK]

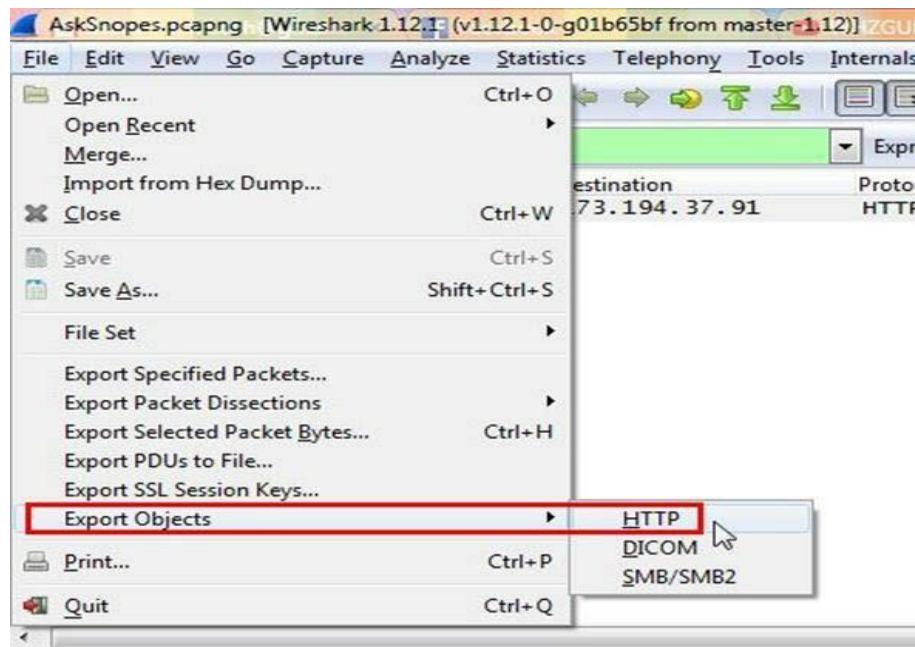
After applying the filter, we found only one packet with the Zillow keyword



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.



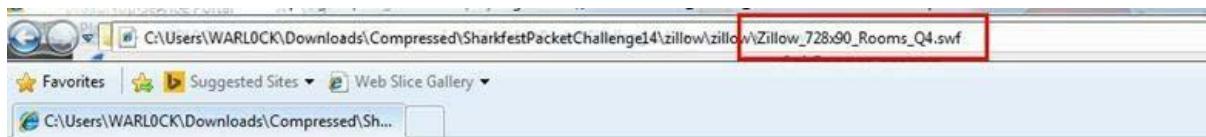
Now go to file and select Export Objects > HTTP. It will save all objects from the packet.



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=cad674db7f73589c9a110884ce73bb72_728_90
112	a.komoona.com	application/x-javascript	815 bytes	cad674db7f73589c9a110884ce73bb72_728_90
129	stat.komoona.com	application/x-javascript	4 bytes	s?tagid=cad674db7f73589c9a110884ce73bb72_728_90
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&tkt_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-500144B03A78
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_914.html

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.

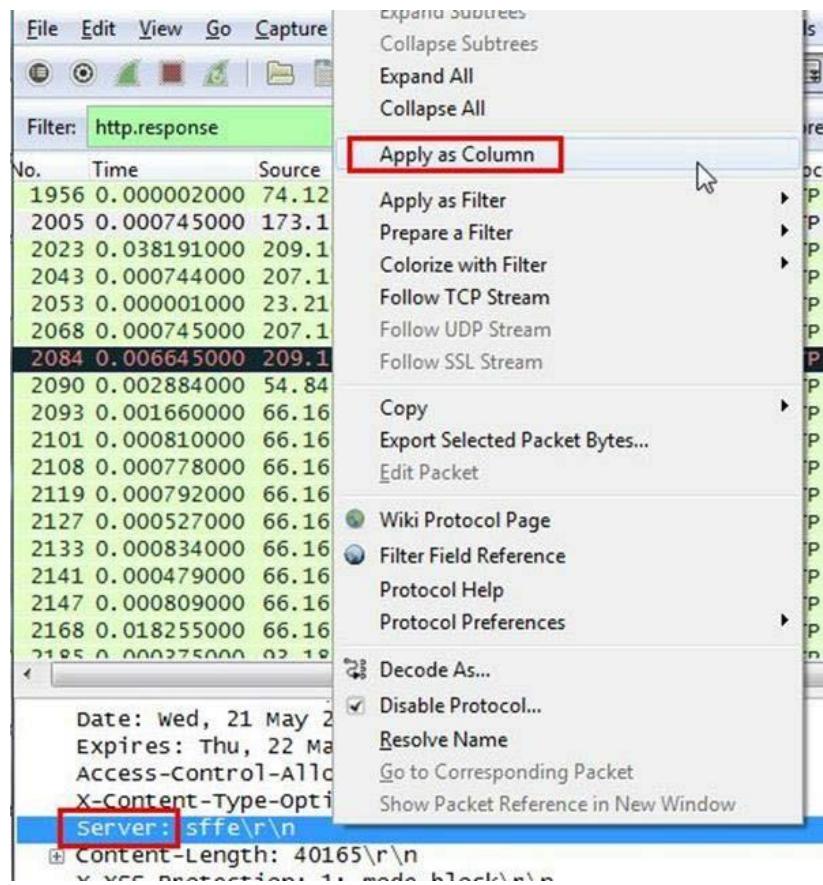


4. How many web servers are running Apache?

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.

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/java)
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

The screenshot shows the Wireshark interface with a green header bar containing the filter: "http.server contains \"Apache\"". Below the header is a table of network packets. To the right of the table is the "Statistics" menu, which is currently open. The "Endpoints" option is highlighted with a red box. Other options in the menu include "Summary", "Comments Summary", "Show address resolution", "Protocol Hierarchy", "Conversations", "Packet Lengths...", "IO Graph", "Conversation List", "Endpoint List", "Service Response Time", "29West", "ANCP", "BACnet", "Collectd...", "Compare...", and "Flow Graph...".

It will show all connections

Ethernet: 7	Fibre Channel	FDDI	IPv4: 107	IPv6: 4	IPX	JXTA	NCP	RSVP	SCTP	TCP: 361	Token
IPv4 Endpoints											
Address	↓ Packets	↓ Bytes	↓ Tx Packets	↓ Tx Bytes	↓ Rx Packets	↓ Rx Bytes	↓ Latitude	↓ Lc			
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	-	-	-	-	-
<input checked="" type="checkbox"/> Name resolution	<input type="checkbox"/>	Limit to display filter									
Help Copy Limit the list to endpoints matching the current 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: 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	↓ Interface	↓ Source	↓ Destination
207.109.230.161	2	1 173	2	1 173	0	0	0	0	0	0	0
192.168.1.71	80	60 911	0	0	80	60 911	0	0	0	0	0
50.19.115.152	13	4 394	13	4 394	0	0	0	0	0	0	0
107.20.177.71	4	3 143	4	3 143	0	0	0	0	0	0	0
23.210.219.85	6	6 468	6	6 468	0	0	0	0	0	0	0
23.210.231.153	12	6 163	12	6 163	0	0	0	0	0	0	0
23.23.197.19	2	1 179	2	1 179	0	0	0	0	0	0	0
216.39.54.212	1	225	1	225	0	0	0	0	0	0	0
162.248.19.136	3	2 363	3	2 363	0	0	0	0	0	0	0
162.248.16.24	2	1 692	2	1 692	0	0	0	0	0	0	0
69.25.24.24	13	15 024	13	15 024	0	0	0	0	0	0	0
207.109.230.154	3	3 162	3	3 162	0	0	0	0	0	0	0
50.97.236.98	2	1 753	2	1 753	0	0	0	0	0	0	0
69.25.24.26	3	3 087	3	3 087	0	0	0	0	0	0	0
50.116.194.21	1	1 045	1	1 045	0	0	0	0	0	0	0
50.116.194.28	1	527	1	527	0	0	0	0	0	0	0
54.243.109.84	1	609	1	609	0	0	0	0	0	0	0
63.135.172.251	2	837	2	837	0	0	0	0	0	0	0
199.189.107.4	4	3 950	4	3 950	0	0	0	0	0	0	0
50.63.243.230	1	1 007	1	1 007	0	0	0	0	0	0	0
207.109.230.187	3	3 036	3	3 036	0	0	0	0	0	0	0
162.248.16.37	1	74	1	74	0	0	0	0	0	0	0

Name resolution Limit to 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:

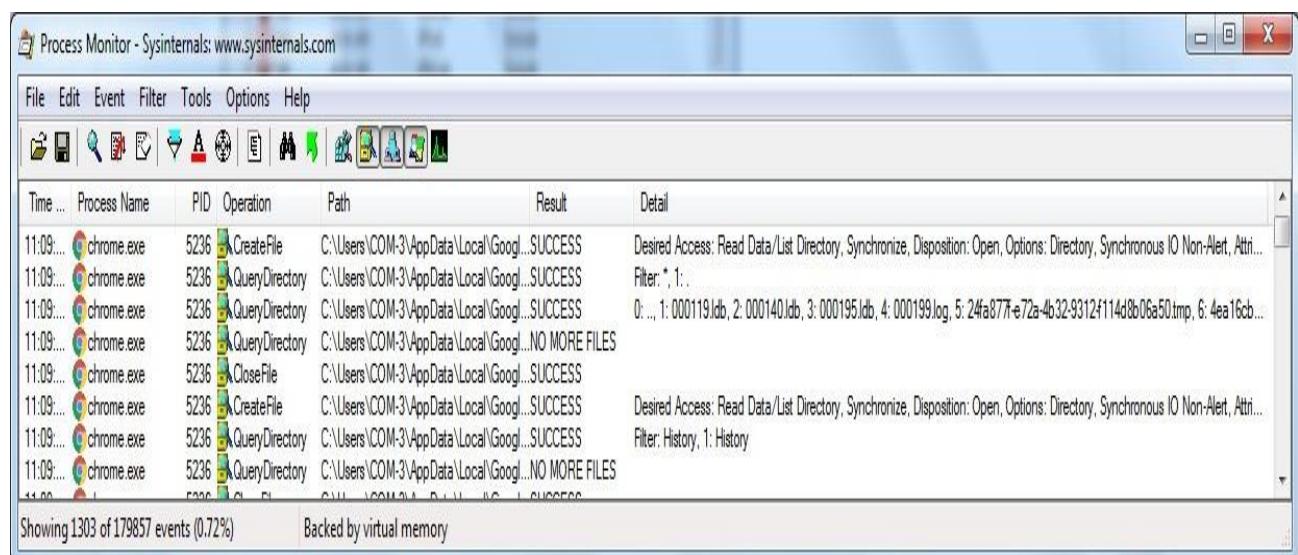
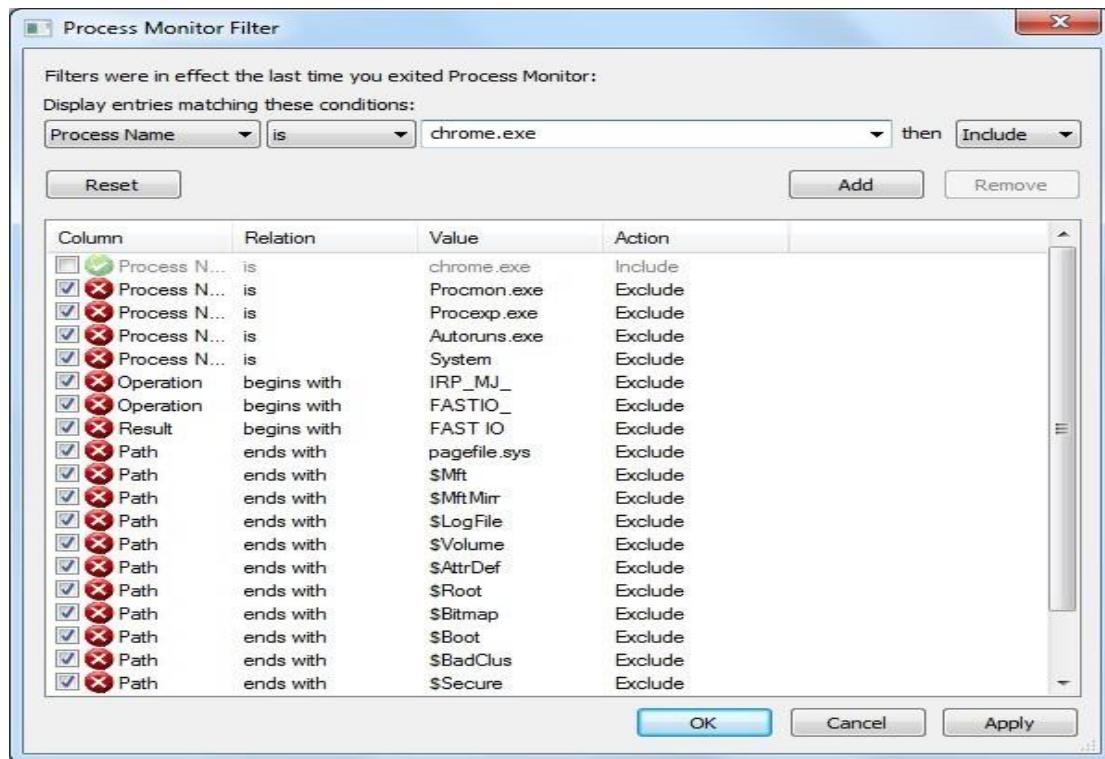
1. File and Disk Utilities
2. Networking Utilities
3. Process Utilities
4. Security Utilities
5. System Information Utilities
6. Miscellaneous Utilities

➤ **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 Tree

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

Process	Description	Image Path	Life Time	Company	Owner
Idle (0)	Idle	System			NT AUTHORITY\SYSTEM
System (4)	Windows Session ...	C:\Windows\System...		Microsoft Corporation	NT AUTHORITY\SYSTEM
smss.exe (428)	System	C:\Windows\system...		Microsoft Corporation	NT AUTHORITY\SYSTEM
cers.exe (600)	Client Server Run...	C:\Windows\sys...		Microsoft Corporation	NT AUTHORITY\SYSTEM
cnhost.exe (3996)	Console Window ...	C:\Windows\sys...		Microsoft Corporation	NT AUTHORITY\SYSTEM
cnhost.exe (6000)	Console Window ...	C:\Windows\sys...		Microsoft Corporation	NT AUTHORITY\SYSTEM
wininit.exe (660)	Windows Start-Up ...	C:\Windows\sys...		Microsoft Corporation	NT AUTHORITY\SYSTEM
services.exe (716)	Services and Cont...	C:\Windows\sys...		Microsoft Corporation	NT AUTHORITY\SYSTEM
svchost.exe (892)	Host Process for ...	C:\Windows\sys...		Microsoft Corporation	NT AUTHORITY\SYSTEM
wmiprvse.exe (156)	WMI Provider Host	C:\Windows\sys...		Microsoft Corporation	NT AUTHORITY\SYSTEM
ARWSRVCE.EXE (956)	Realtime Behavior...	C:\Program Files\...		Quick Heal Techn...	NT AUTHORITY\SYSTEM
ScSecSvc.exe (980)	Browser Sandbox ...	C:\Program Files\...		Quick Heal Techn...	NT AUTHORITY\SYSTEM
svchost.exe (1196)	Host Process for ...	C:\Windows\sys...		Microsoft Corporation	NT AUTHORITY\SYSTEM
svchost.exe (1272)	Host Process for ...	C:\Windows\sys...		Microsoft Corporation	NT AUTHORITY\SYSTEM
svchost.exe (1308)	Host Process for ...	C:\Windows\sys...		Microsoft Corporation	NT AUTHORITY\SYSTEM
Dwm.exe (2036)	Desktop Window	C:\Windows\sys...		Microsoft Corporation	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](#)

Count Values Occurrences

Column: **Process Name** [Count](#)

Value	Count
chrome.exe	1821

Double-click an item to filter on that value.

[Filter...](#) 1 items [Save...](#) [Close](#)

File Summary

Files accessed during trace:

[By Path](#) [By Folder](#) [By Extension](#)

File Time	Total Events	Opens	Closes	Reads	Writes	Read B...	Write B...	Get ACL	Set ACL	Other	Path
0.3561587	1290	260	228	80	26	79652862	354084	44	4	648	<Total>
0.0279059	93	5	5	76	0	79479792	0	0	0	7	C:\Program Files\Google\Chrome\Ap...
0.0006041	60	20	20	0	0	0	0	10	0	10	C:\Users\COM-3\AppData\Local\Low...
0.0013114	53	18	18	0	0	0	0	4	0	13	C:\Users\COM-3\AppData\Local\Go...
0.0004203	35	7	7	0	0	0	0	0	0	21	C:\Windows\System32\imm32.dll
0.0421016	28	5	4	0	2	0	79807	4	1	12	C:\Users\COM-3\AppData\Local\Go...
0.0420233	28	5	4	0	2	0	40662	4	1	12	C:\Users\COM-3\AppData\Local\Go...
0.0429107	28	5	4	0	2	0	153666	4	1	12	C:\Users\COM-3\AppData\Local\Go...
0.1282037	28	5	4	0	2	0	79807	4	1	12	C:\Users\COM-3\AppData\Local\Go...
0.0002293	23	4	4	0	0	0	0	0	0	15	C:\Program Files\Google\Chrome\Ap...

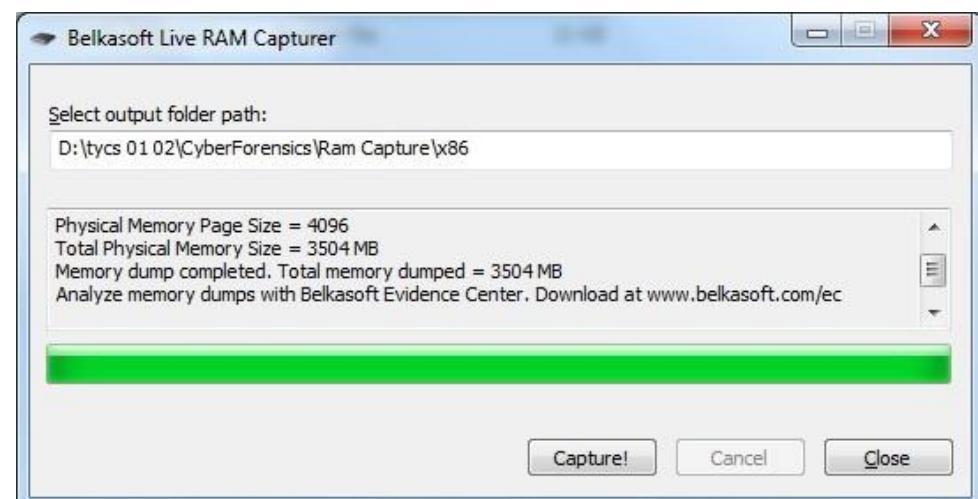
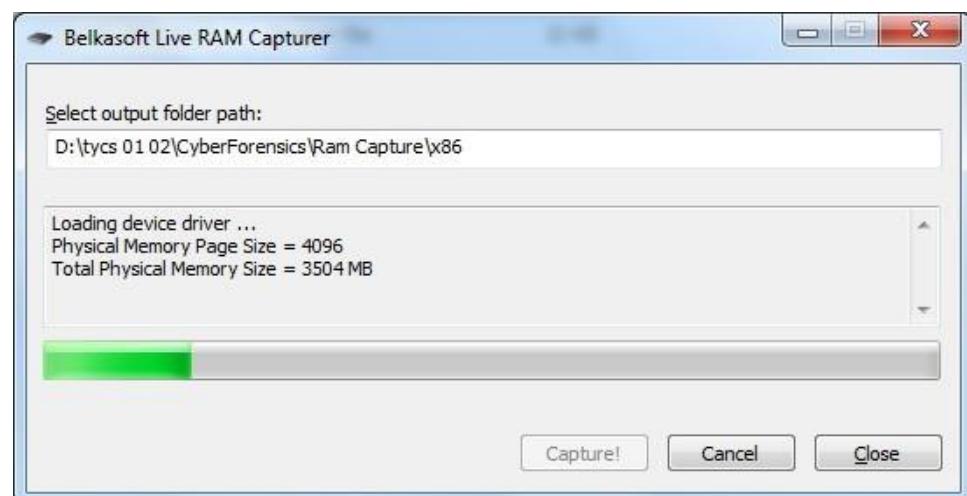
[Filter...](#) 147 file paths [Save...](#) [OK](#)

➤ **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 Byte
[System Proc... 0		TCP	CS-11-PC	1521	localhost	9600	TIME_WAIT				
[System Proc... 0		TCP	CS-11-PC	9599	localhost	1521	TIME_WAIT				
[System Proc... 0		TCP	CS-11-PC	9600	localhost	1521	TIME_WAIT				
[System Proc... 0		TCP	CS-11-PC	1521	localhost	9600	TIME_WAIT	4	792	4	
accasrvc.exe 2844		TCP	CS-11-PC	62125	CS-11-PC	0	LISTENING				
accasrvc.exe 2844		TCP	cs-11-pc	9571	ec2-13-250-151-2...	8080	ESTABLISHED	1	544	1	
chrome.exe 5236	5236	TCP	cs-11-pc	9450	74.125.24.188	5228	ESTABLISHED				18
chrome.exe 5236	5236	UDP	CS-11-PC	5353	*	*					
chrome.exe 5236	5236	UDP	CS-11-PC	5353	*	*					
chrome.exe 5236	5236	UDP	CS-11-PC	5353	*	*					
chrome.exe 5236	5236	UDP	CS-11-PC	5353	*	*					
chrome.exe 5236	5236	UDP	CS-11-PC	5353	*	*					
chrome.exe 5236	5236	UDP	CS-11-PC	5353	*	*					
chrome.exe 5236	5236	UDPV6	cs-11-pc	5353	*	*					
chrome.exe 5236	5236	UDPV6	cs-11-pc	5353	*	*					
chrome.exe 5236	5236	UDPV6	cs-11-pc	5353	*	*					
emagent.exe 5348	5348	TCP	CS-11-PC	3938	CS-11-PC	0	LISTENING				
emagent.exe 5348	5348	TCP	CS-11-PC	10000	CS-11-PC	0	LISTENING				
emagent.exe 5348	5348	TCPV6	cs-11-pc	3938	cs-11-pc	0	LISTENING				
EMLPROXY.... 2924	2924	TCP	cs-11-pc	8902	14.142.64.27.stat... 8080		ESTABLISHED				
EMLPROXY.... 2924	2924	TCP	CS-11-PC	17400	CS-11-PC	0	LISTENING				
java.exe 5248	5248	TCP	CS-11-PC	1038	localhost	1039	ESTABLISHED	26	26		
java.exe 5248	5248	TCP	CS-11-PC	1039	localhost	1038	ESTABLISHED				26
java.exe 5248	5248	TCP	CS-11-PC	1158	CS-11-PC	0	LISTENING				
java.exe 5248	5248	TCP	CS-11-PC	5520	CS-11-PC	0	LISTENING				
java.exe 5248	5248	TCPV6	cs-11-pc	5520	cs-11-pc	0	LISTENING				

TCPView - Sysinternals: www.sysinternals.com

File Options Process View Help

Process /	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets	Sent Bytes	Rcvd Packets	Rcvd Bytes
System Proc...	0	TCP	CS-11-PC	1521	localhost	10008	TIME_WAIT				
accsvc.exe	2844	TCP	CS-11-PC	62125	CS-11-PC	0	LISTENING				
accsvc.exe	2844	TCP	cs-11-pc	10072	ec2-13-250-151-2	8080	ESTABLISHED	1	544	1	
accsvc.exe	2844	TCP	cs-11-pc	10146	82.24.100.123	5054	SYN_SENT				
chrome.exe	5236	TCP	cs-11-pc	9801	172.217.194.188	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	UDPV6	cs-11-pc	5353	*	*					
chrome.exe	5236	UDPV6	cs-11-pc	5353	*	*					
chrome.exe	5236	UDPV6	cs-11-pc	5353	*	*					
chrome.exe	5236	TCP	cs-11-pc	10040	104.19.196.151	Https	ESTABLISHED	7	1,141	16	
chrome.exe	5236	UDP	CS-11-PC	57081	*	*					
chrome.exe	5236	UDP	CS-11-PC	57082	*	*					
chrome.exe	5236	UDP	CS-11-PC	58349	*	*					
chrome.exe	5236	TCP	cs-11-pc	10140	mint.	mint.	Process Properties...	ED	2	843	5
chrome.exe	5236	TCP	cs-11-pc	10141	mint.	mint.	End Process...	ED	4	1,679	16
chrome.exe	5236	TCP	cs-11-pc	10142	mint.	mint.	Close Connection	ED	4	2,767	7
chrome.exe	5236	UDP	CS-11-PC	57790	*	*					
emager.exe	5348	TCP	CS-11-PC	3938	CS-1	CS-1	Whois...	Ctrl+W			
emager.exe	5348	TCP	CS-11-PC	10000	CS-1	CS-1	Copy	Ctrl+C			
EMLPROXY...	2924	TCP	CS-11-PC	17400	CS-1	CS-1					
java.exe	5249	TCP	CS-11-PC	1038	localhost	1038	LISTENING	ED	85	85	85
java.exe	5249	TCP	CS-11-PC	1039	localhost	1038	ESTABLISHED				
java.exe	5249	TCP	CS-11-PC	1158	CS-11-PC	0	LISTENING				
java.exe	5249	TCP	CS-11-PC	5520	CS-11-PC	0	LISTENING				
java.exe	5249	TCPPV6	cs-11-pc	5520	cs-11-pc	0	LISTENING				
bast.exe	756	TCP	CS-11-PC	1028	CS-11-PC	0	LISTENING				
bast.exe	756	TCPPV6	cs-11-pc	1028	cs-11-pc	0	LISTENING				
dnDNSRespo...	2824	TCP	CS-11-PC	5354	CS-11-PC	0	LISTENING				235
dnDNSRespo...	2824	UDP	cs-11-pc	5353	*	*					
dnDNSRespo...	2824	UDP	cs-11-pc	5353	*	*					
dnDNSRespo...	2824	UDP	cs-11-pc	5353	*	*					
dnDNSRespo...	2824	UDP	cs-11-pc	64645	*	*					
dnDNSRespo...	2824	UDPV6	cs-11-pc	64646	*	*					
msndrv.exe	3708	TCP	CS-11-PC	ms-olap4	CS-11-PC	0	LISTENING				
msndrv.exe	3708	TCPPV6	cs-11-pc	ms-olap4	cs-11-pc	0	LISTENING				
mysqld.exe	3832	TCP	CS-11-PC	3306	CS-11-PC	0	LISTENING				
omtreco.exe	3952	TCP	CS-11-PC	49152	CS-11-PC	0	LISTENING				
outlook.exe	7744	TCP	-- 11 --	49152	-- 11 --	49152	CLOSE_WAIT	ED	200	200	200

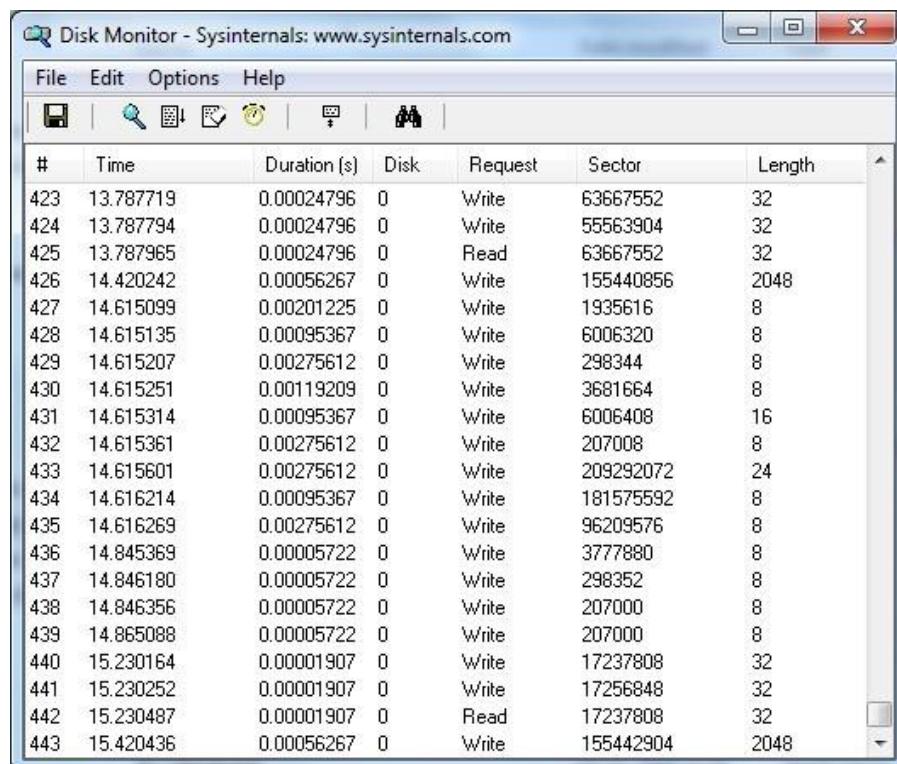


➤ **Monitor Hard Disk (Tool: DiskMon) :**

To Do:

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

Output :



The screenshot shows the 'Disk Monitor' application window from Sysinternals. The window title is 'Disk Monitor - Sysinternals: www.sysinternals.com'. The menu bar includes File, Edit, Options, and Help. Below the menu is a toolbar with icons for search, refresh, and other functions. The main area is a table displaying disk operations:

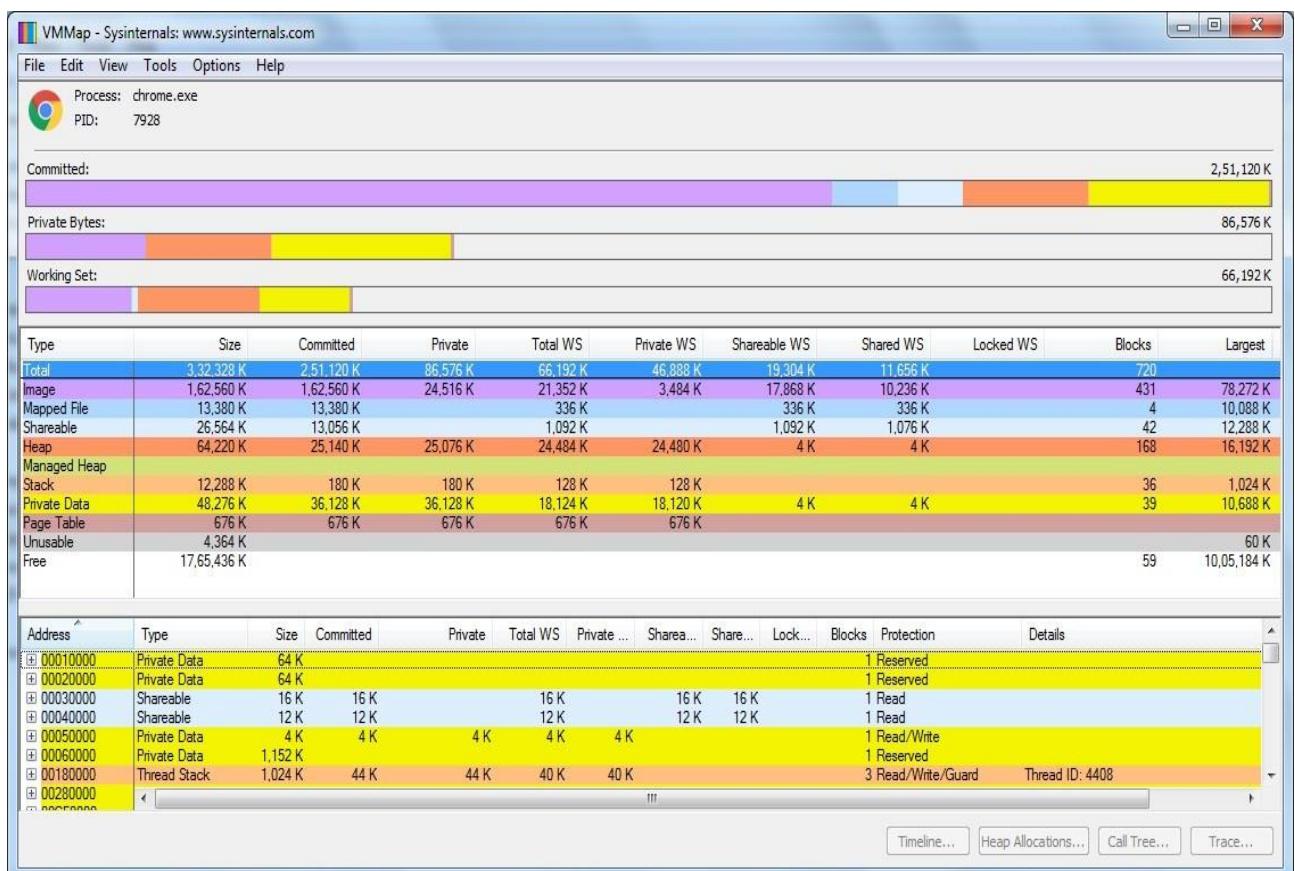
#	Time	Duration (s)	Disk	Request	Sector	Length
423	13.787719	0.00024796	0	Write	63667552	32
424	13.787794	0.00024796	0	Write	55563904	32
425	13.787965	0.00024796	0	Read	63667552	32
426	14.420242	0.00056267	0	Write	155440856	2048
427	14.615099	0.00201225	0	Write	1935616	8
428	14.615135	0.00095367	0	Write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

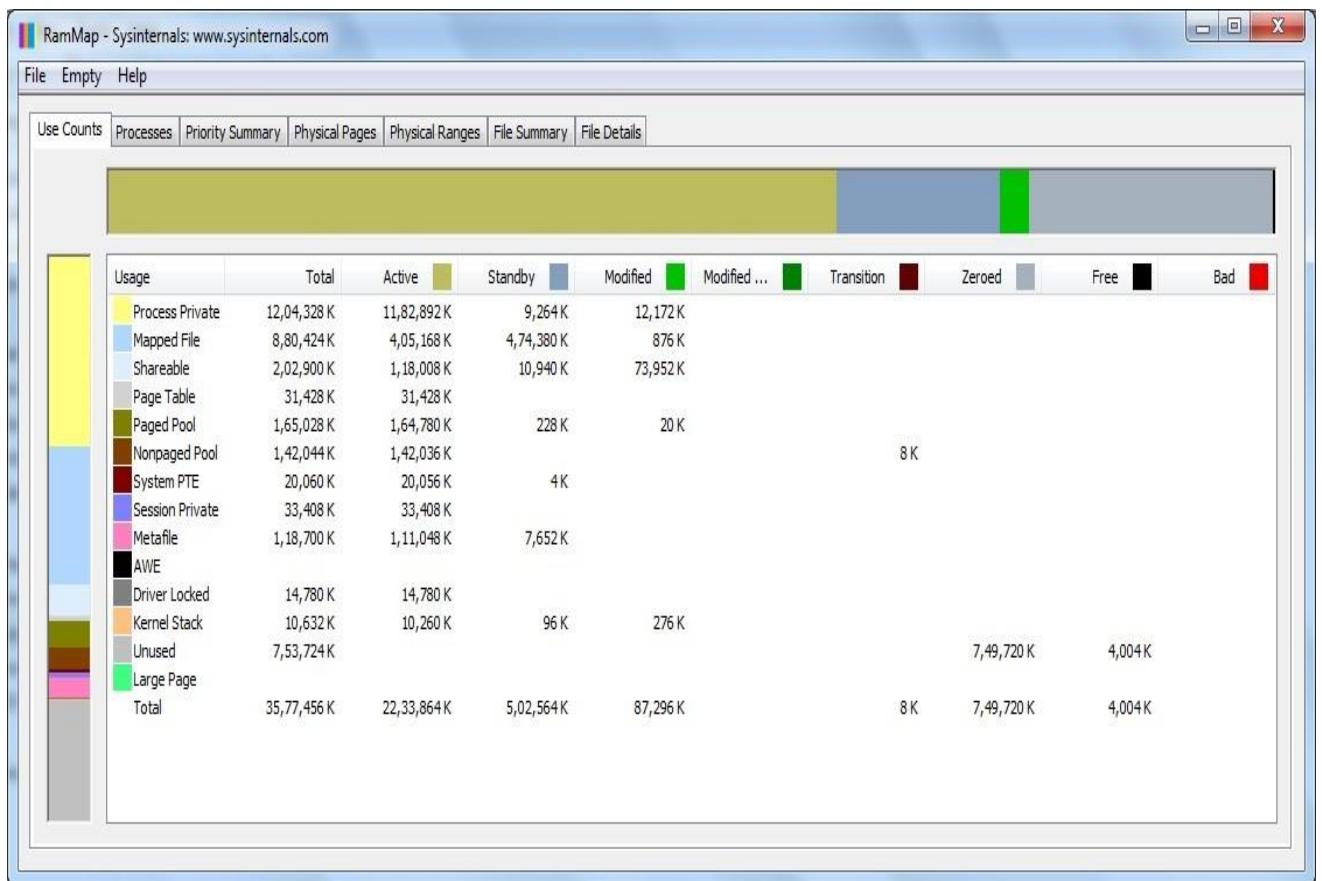


➤ **Monitor Cache Memory**
(Tool: RAMMap)

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

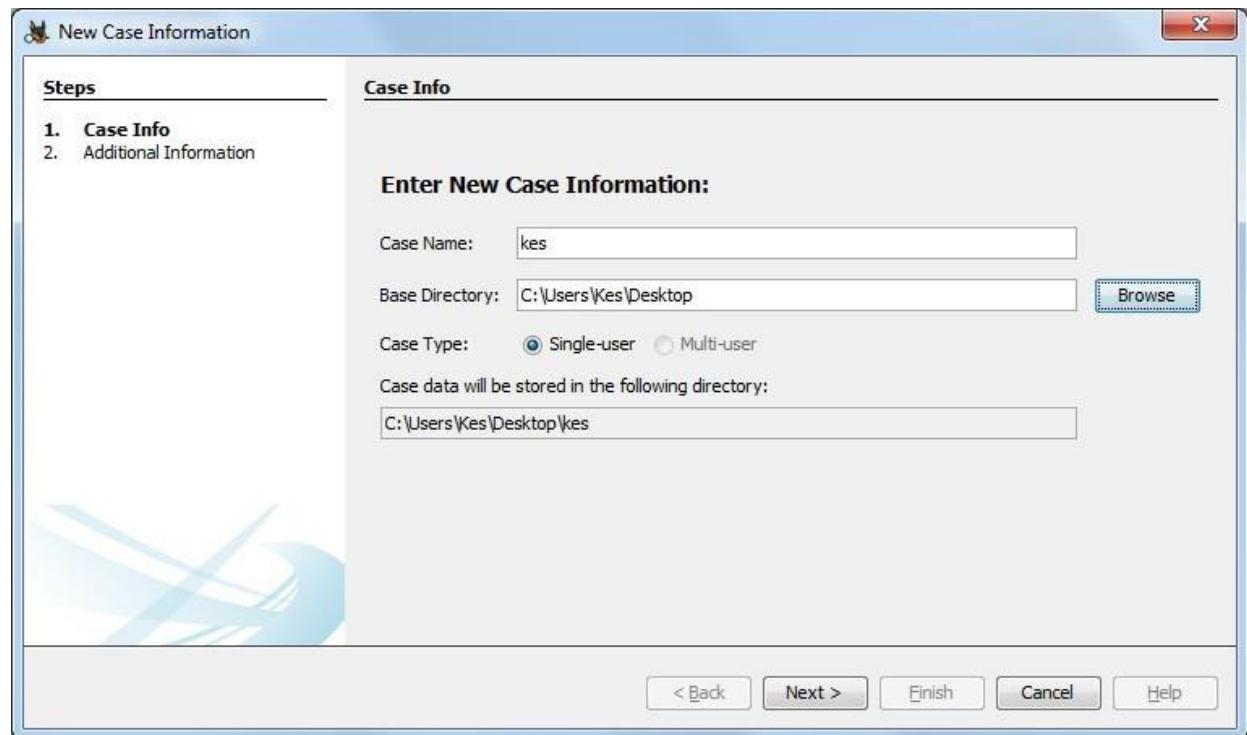
Step 1: Start Autopsy from Desktop.



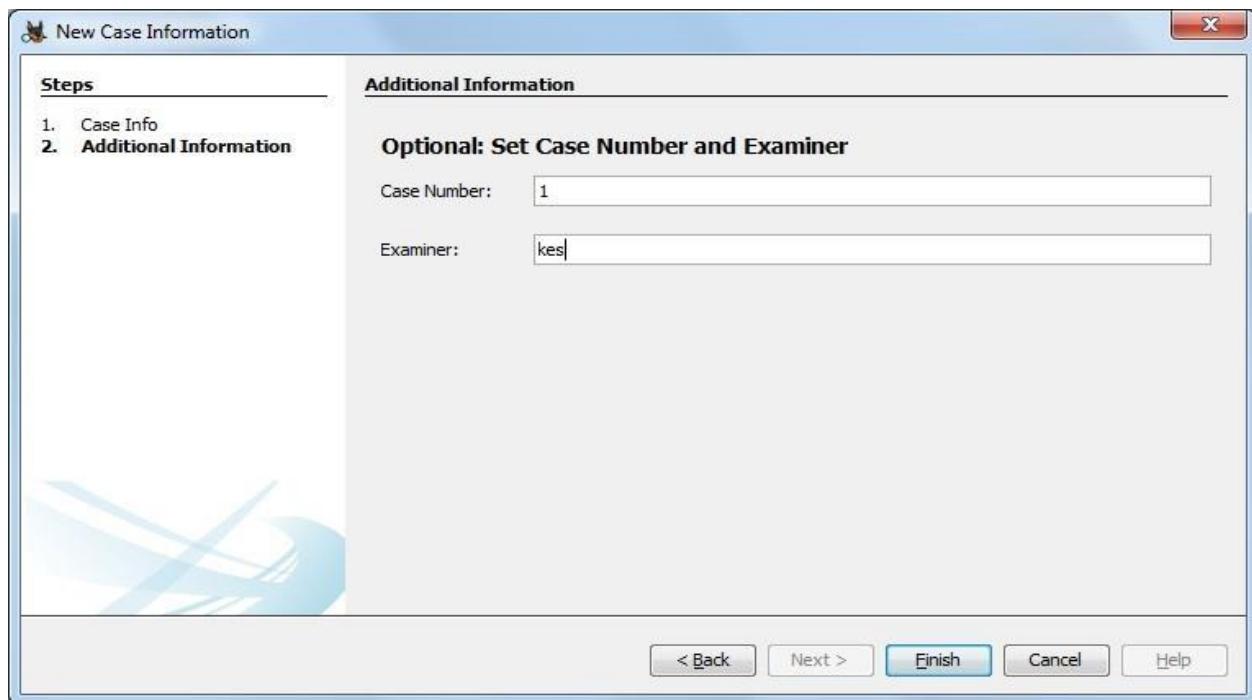
Step 2: Now create on New Case.



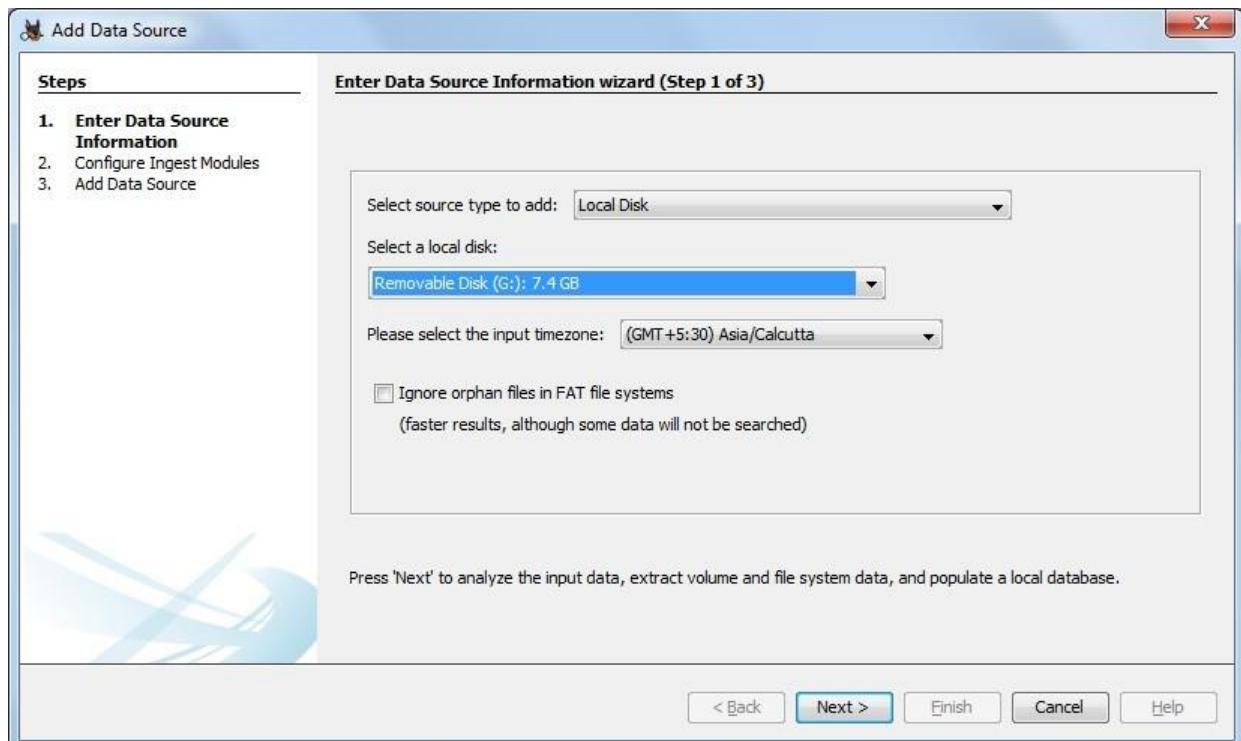
Step 3: Enter the New case Information and click on Next Button.



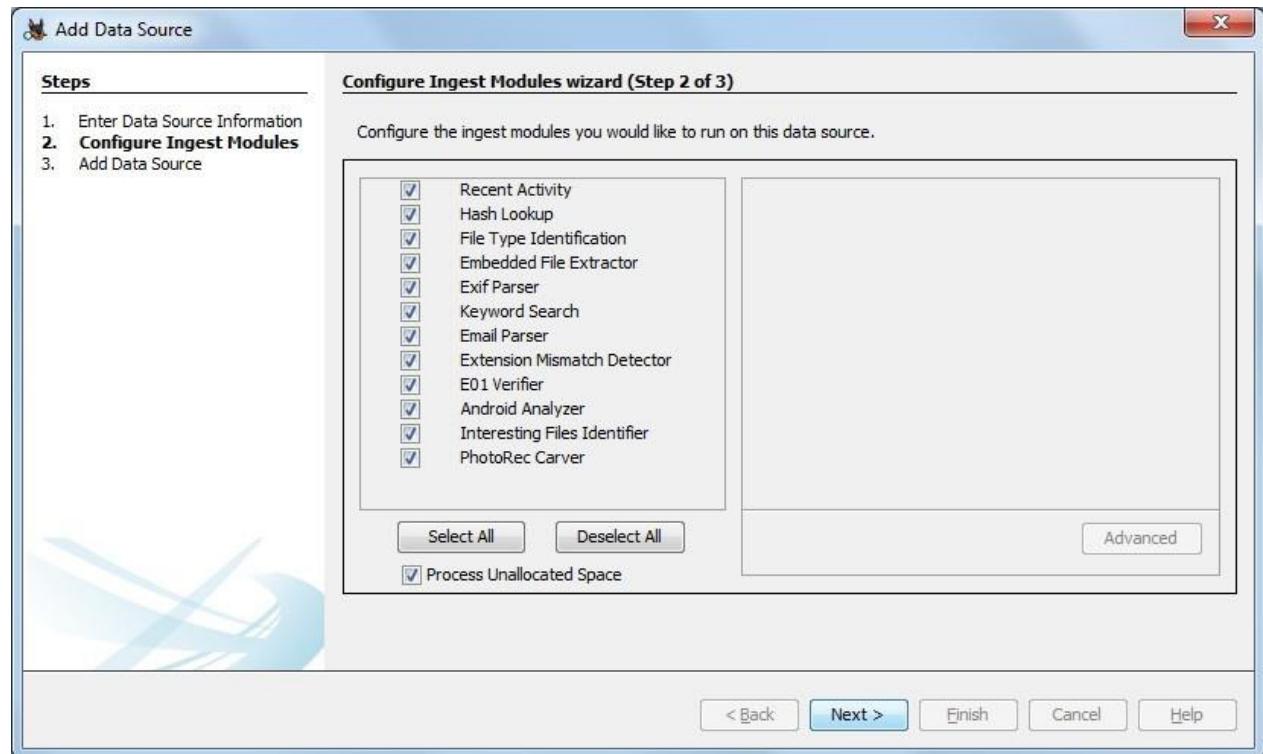
Step 4: Enter the additional Information and click on Finish.



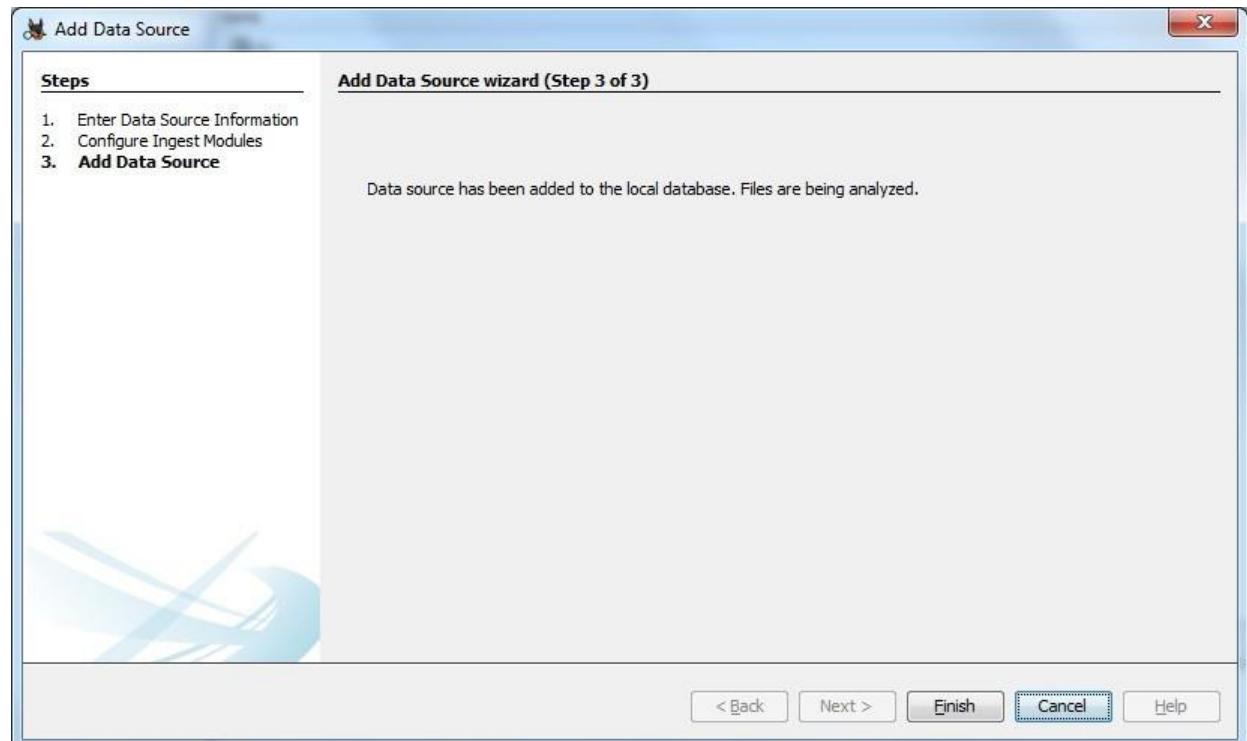
Step 5: Now Select Source Type as Local disk and Select Local disk form drop down list and click on Next.



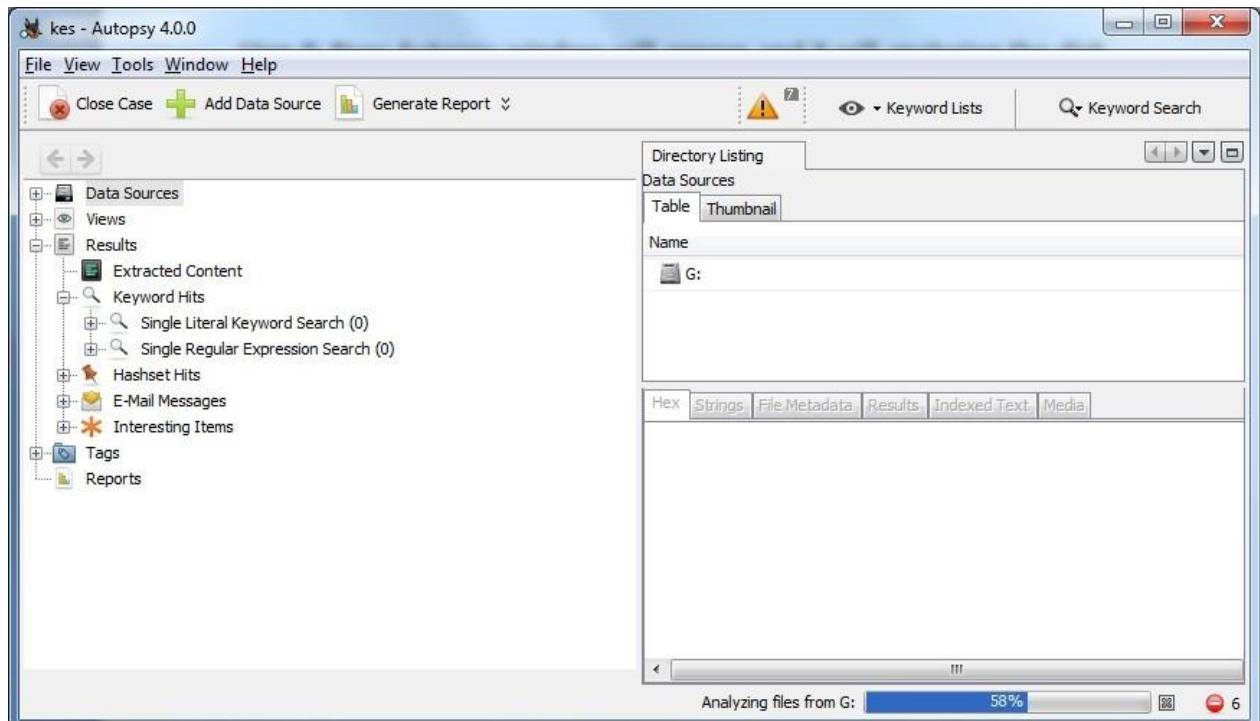
Step 6: Click on Next Button.



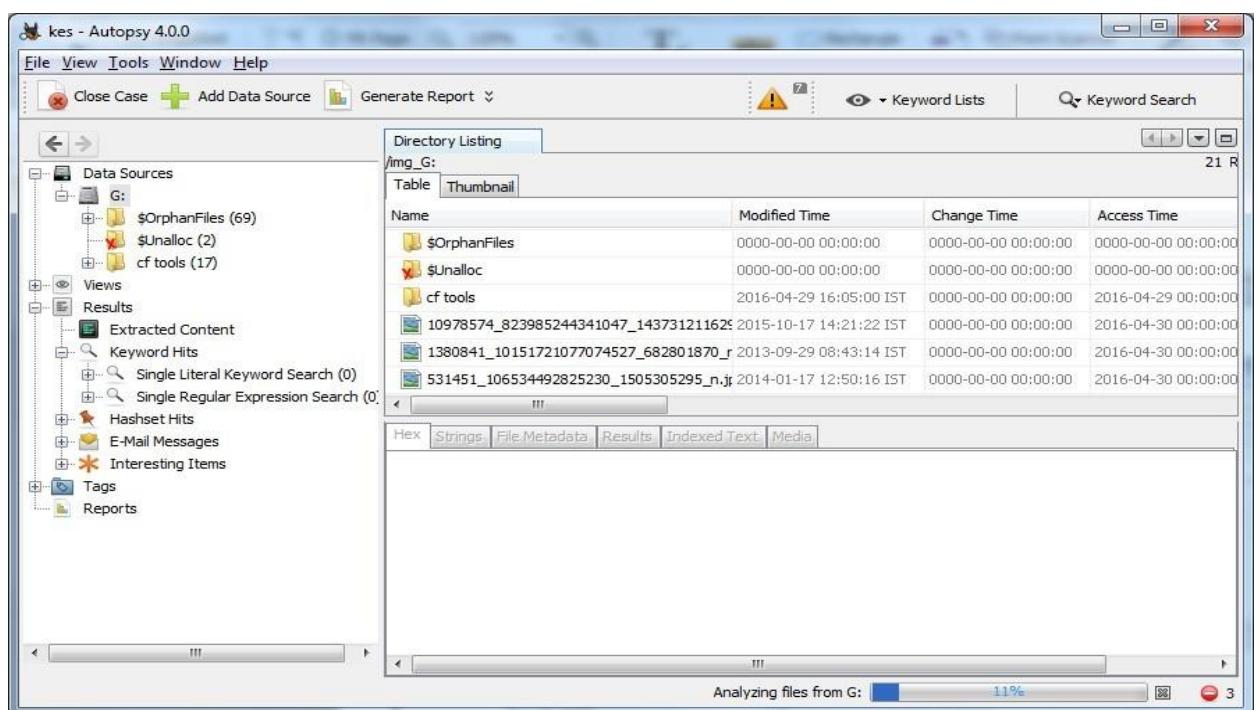
Step 7: Now click On Finish.



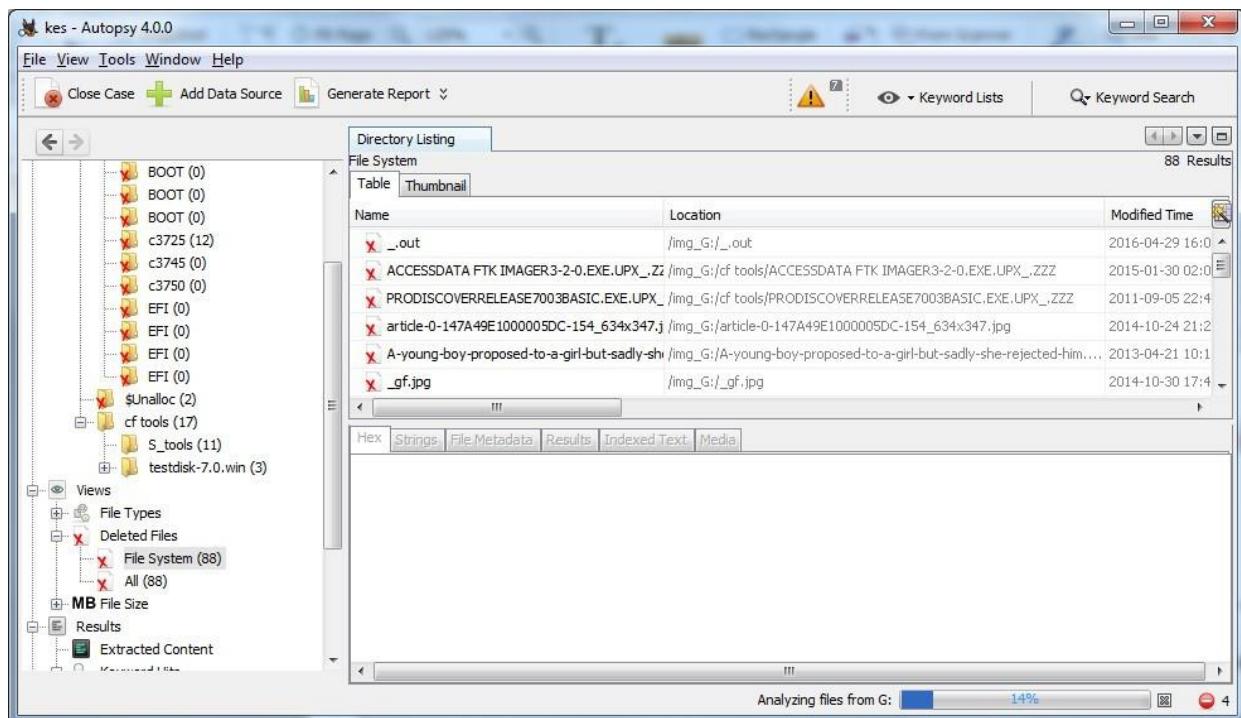
Step 8: Now Autopsy window will appear and it will analyzing the disk that we have selected.



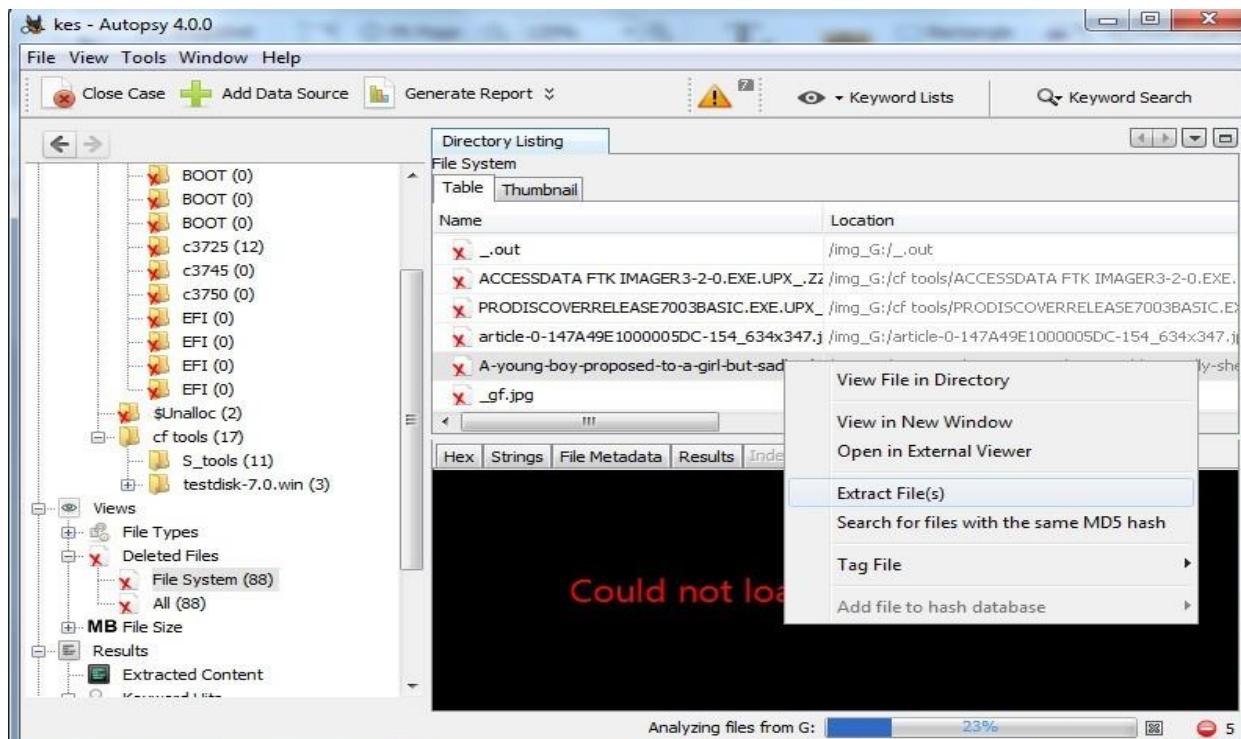
Step 9: All files will appear in table tab select any file to see the data.



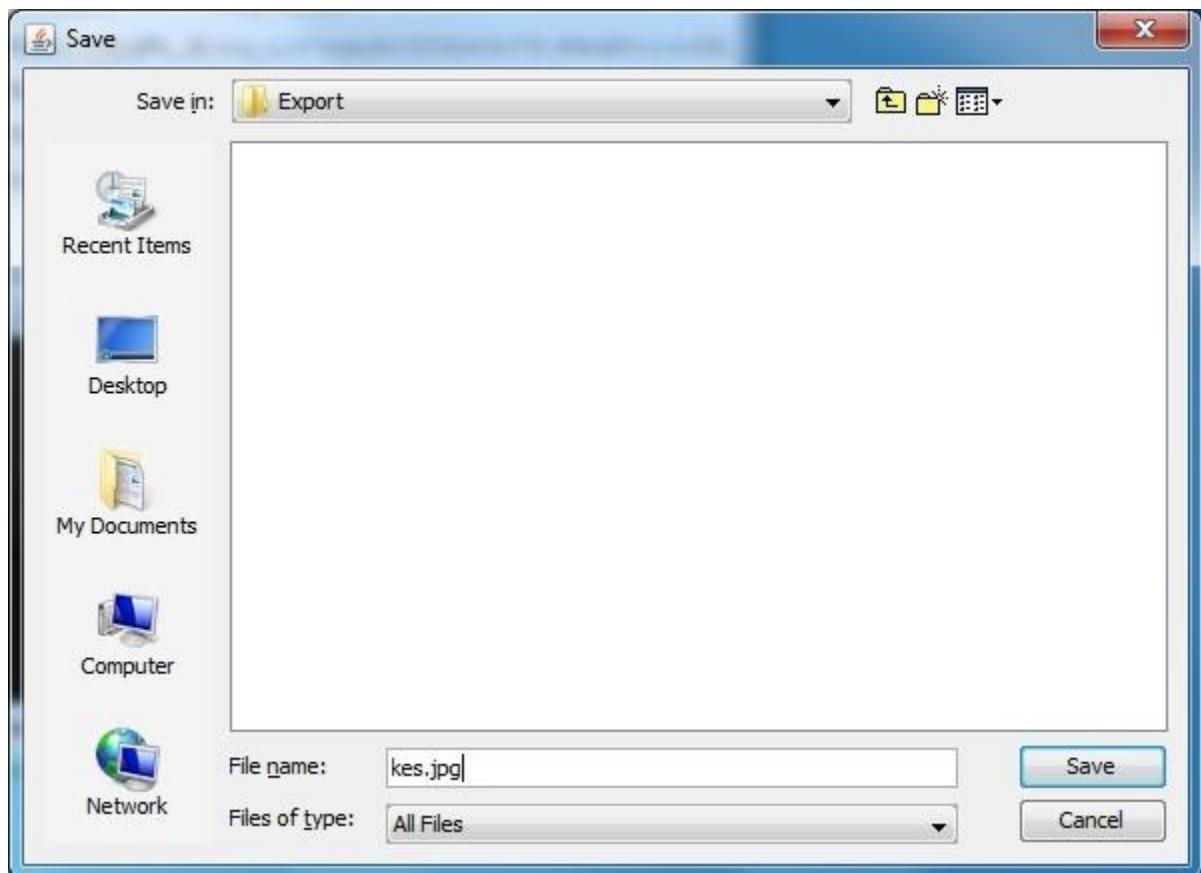
Step 10: Expand the tree from left side panel to view the document files.



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.



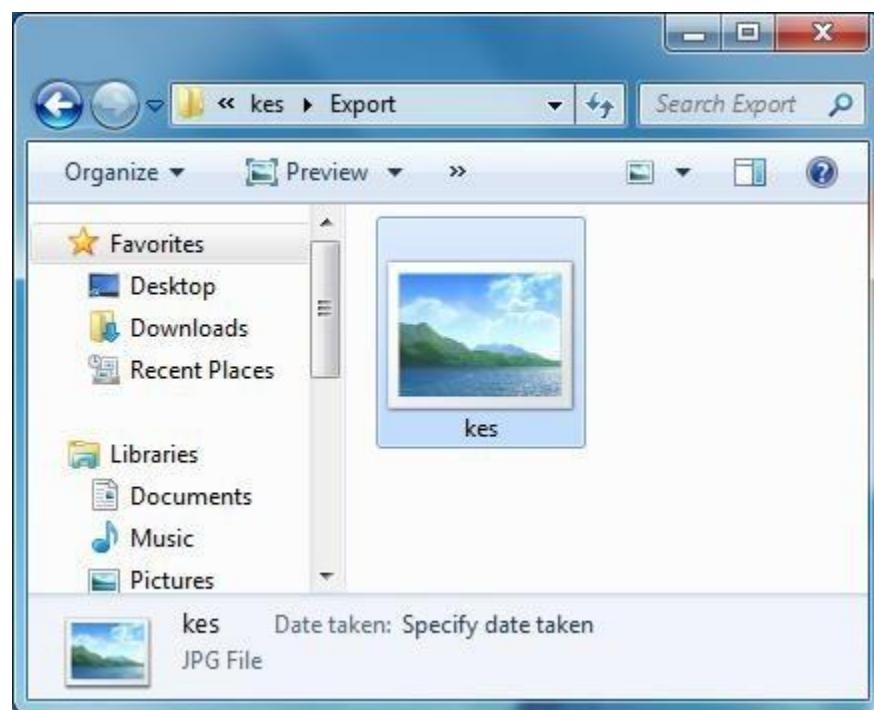
Step 12: By default Export folder is choose to save the recovered file.



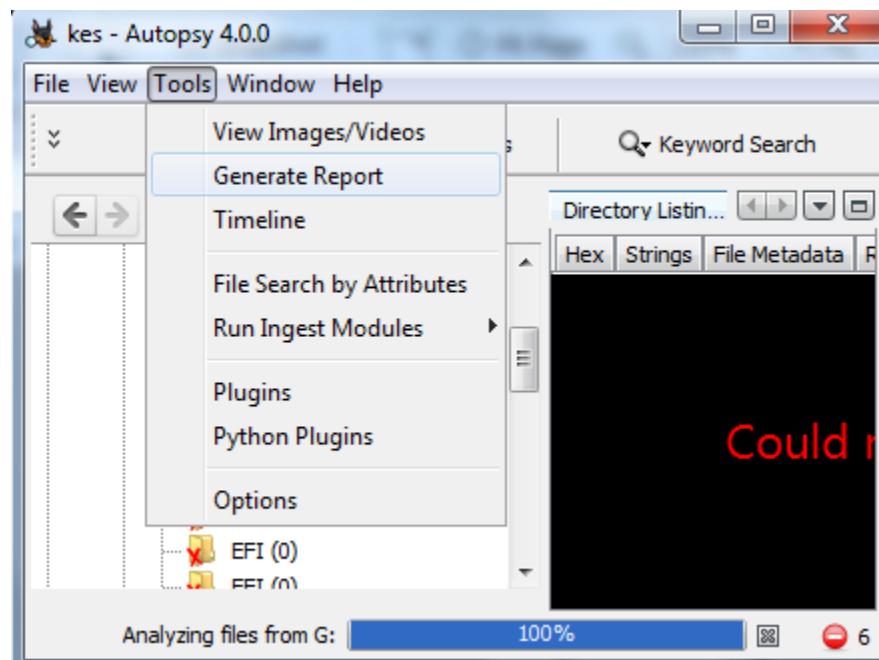
Sep 13 : Now Click on Ok.

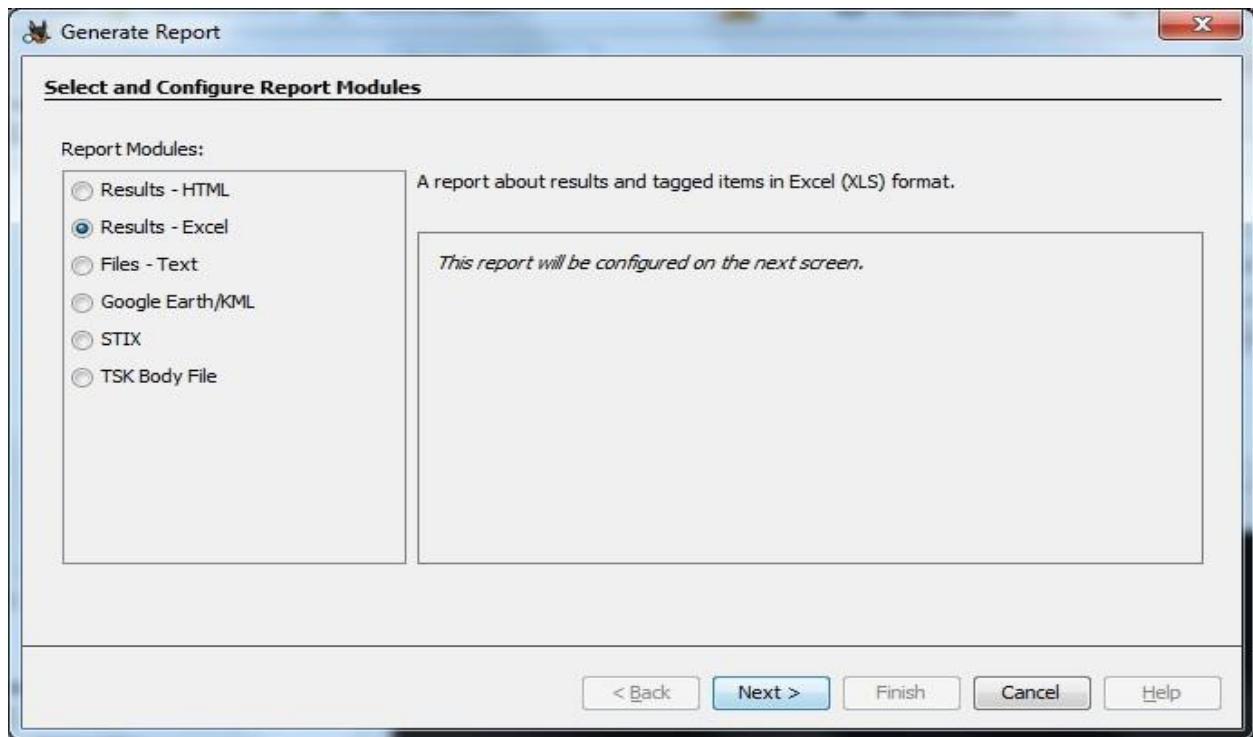


Step 14: Now go to the Export Folder to view Recover file.

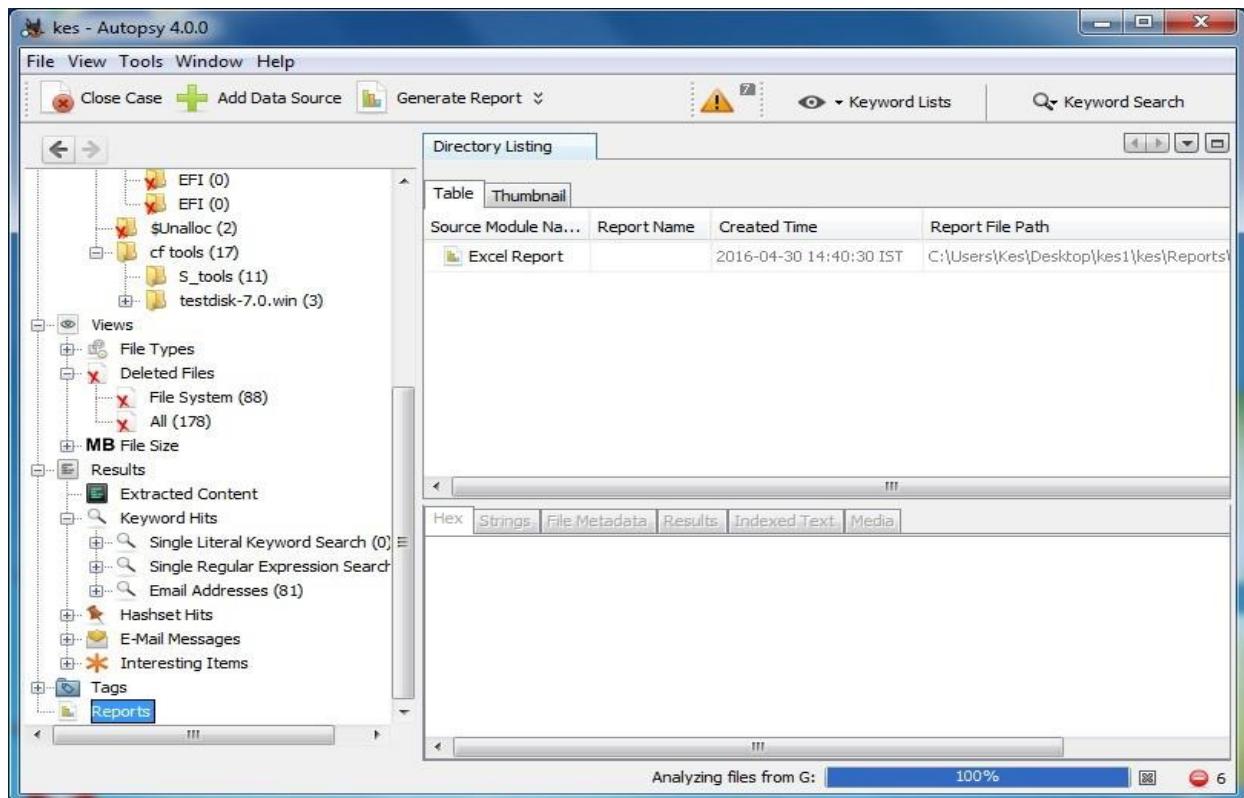


Step 15: Click on Generate Report from autopsy window and Select the Excel format and click on next.

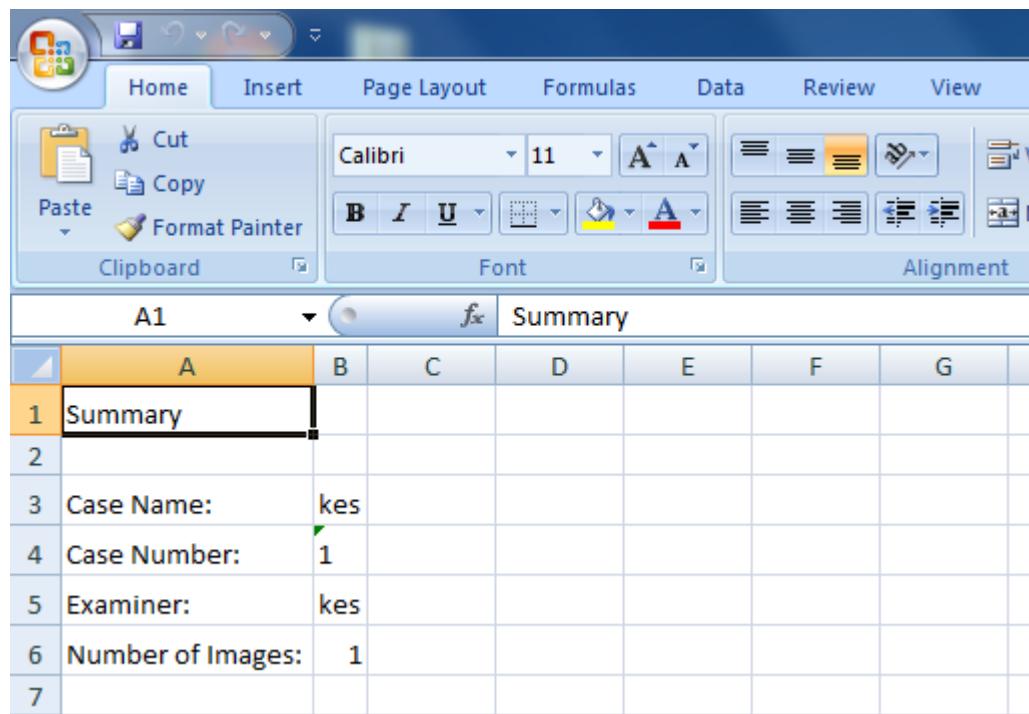




Step 16: Now Report is Generated So click on close Button .we can see the Report on Report Node.



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

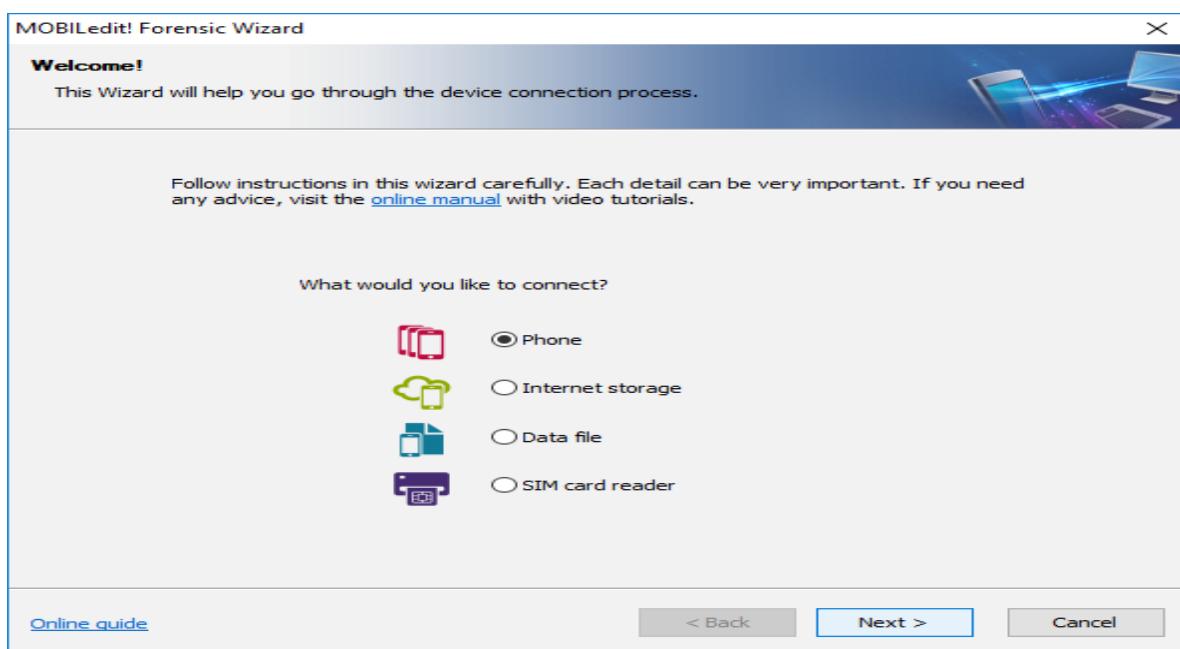
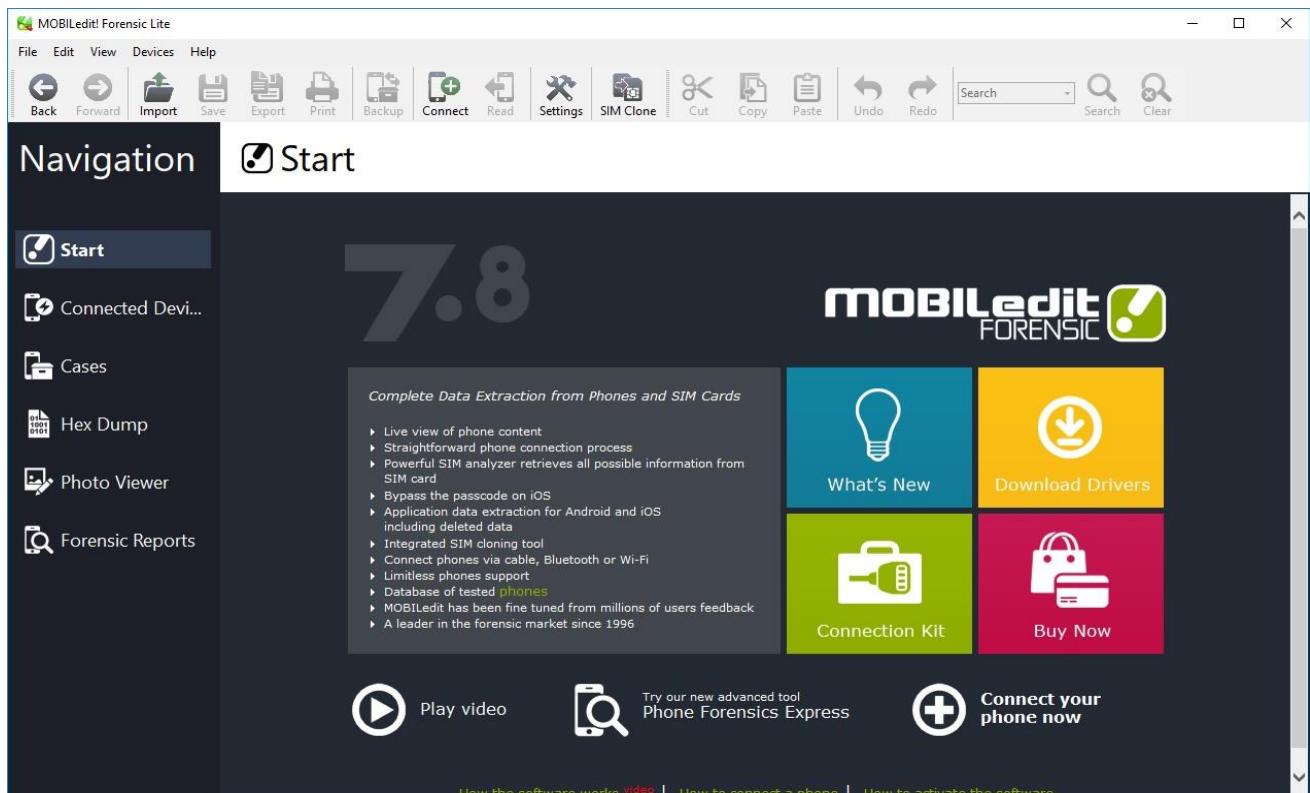


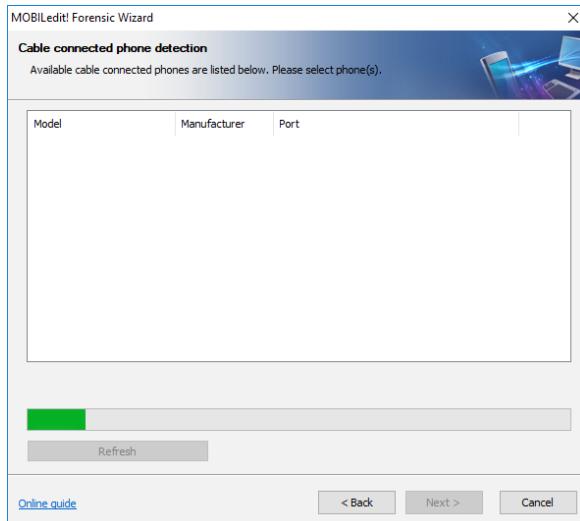
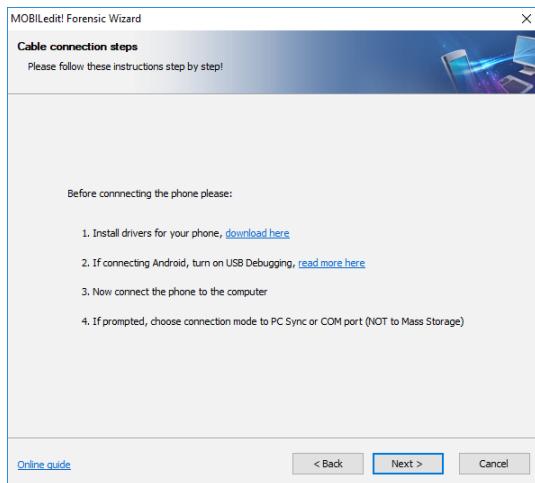
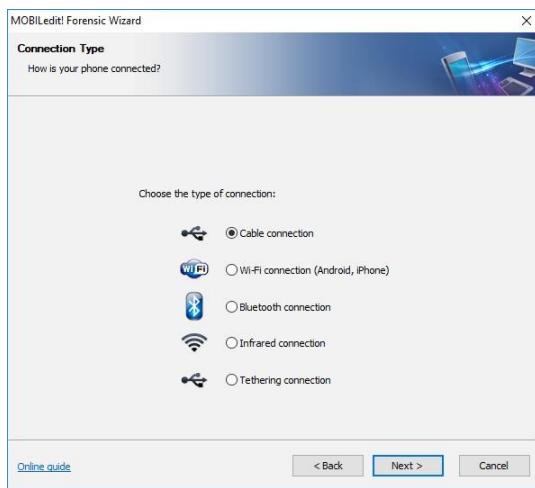
A screenshot of a Microsoft Excel spreadsheet titled "Summary". The spreadsheet contains the following data:

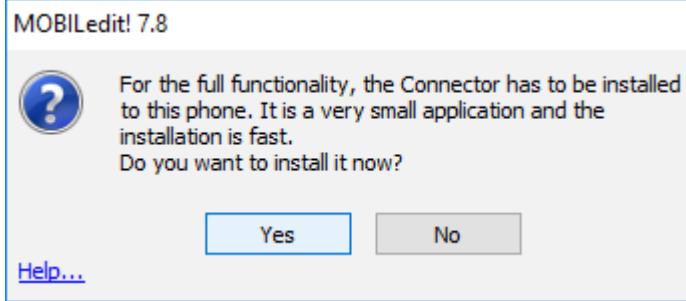
	A	B	C	D	E	F	G
1	Summary						
2							
3	Case Name:	kes					
4	Case Number:	1					
5	Examiner:	kes					
6	Number of Images:	1					
7							

PRACTICAL 8

Aim :- Acquisition of Cell phones and Mobile devices .







Working...

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

Cancel

MOBILedit! Forensic Wizard

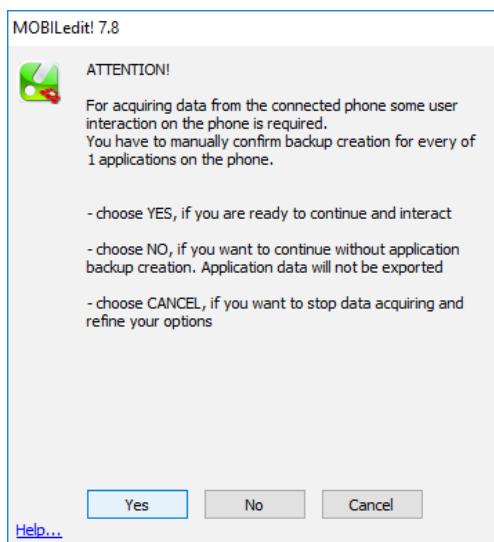
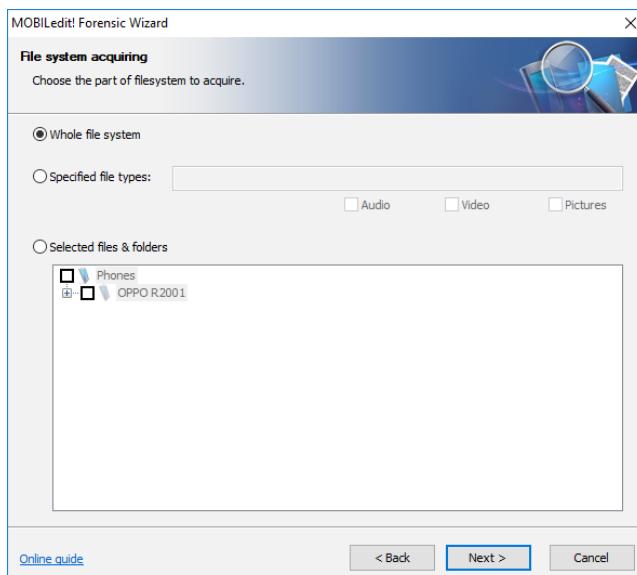
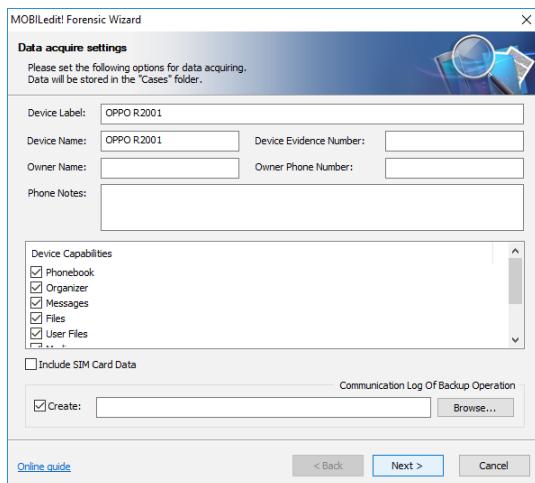
Cable connected phone detection

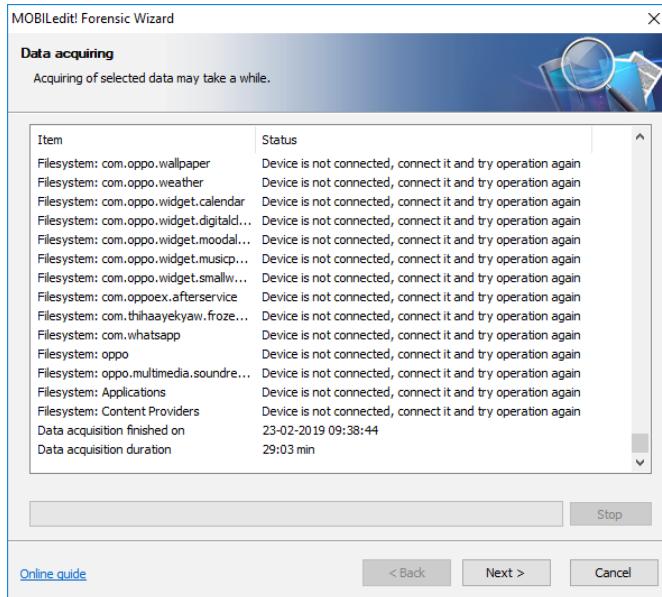
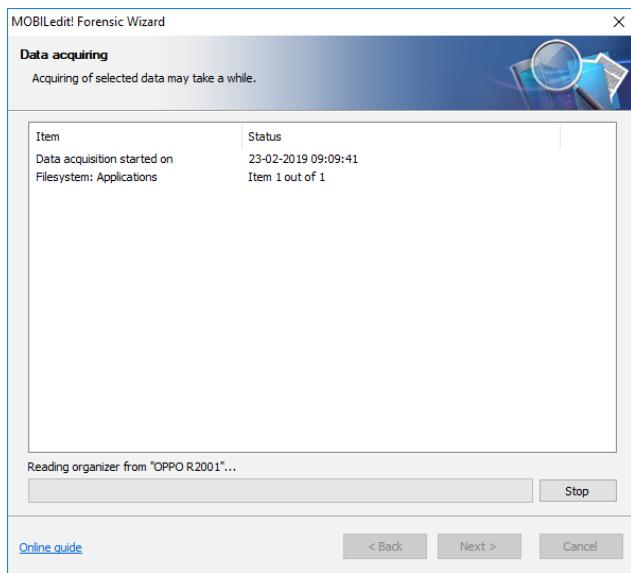
Available cable connected phones are listed below. Please select phone(s).

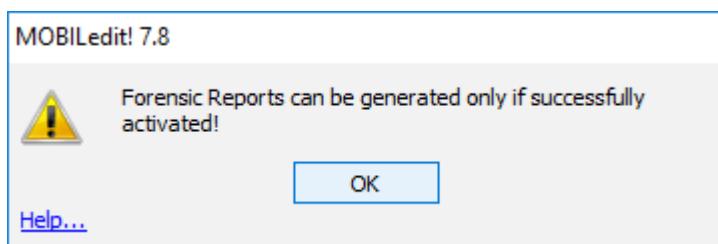
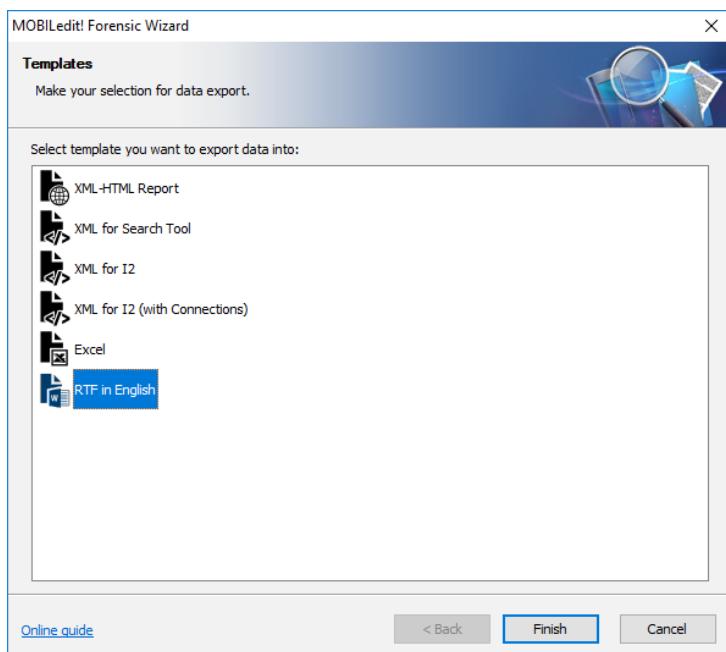
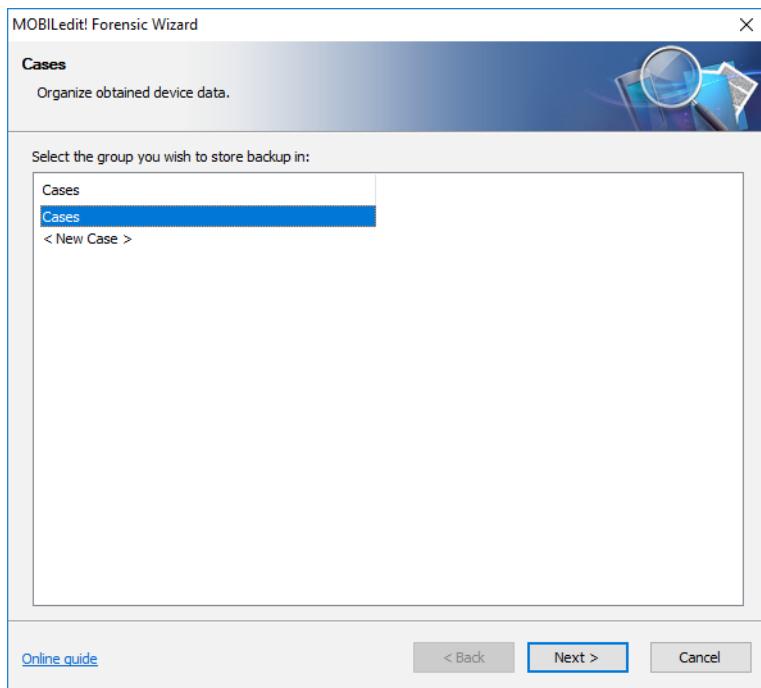
Model	Manufacturer	Port
<input checked="" type="checkbox"/> R2001	OPPO	Android 1134B6EC

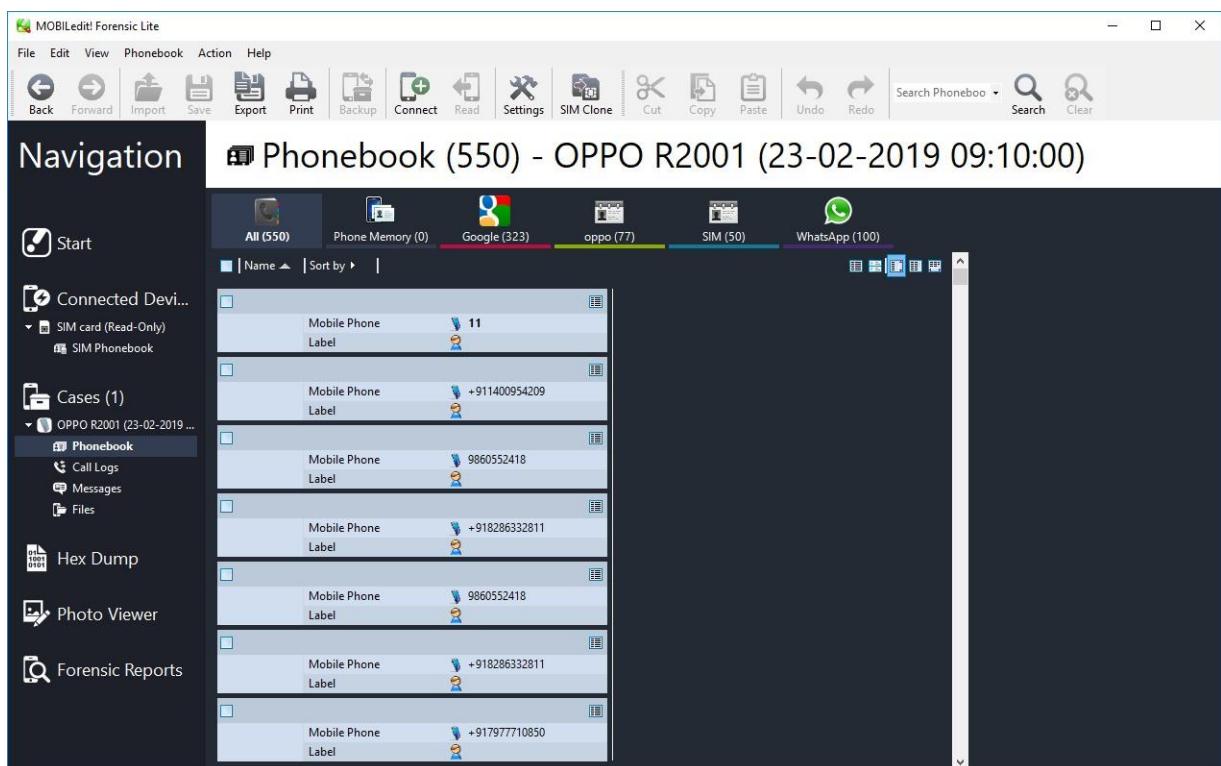
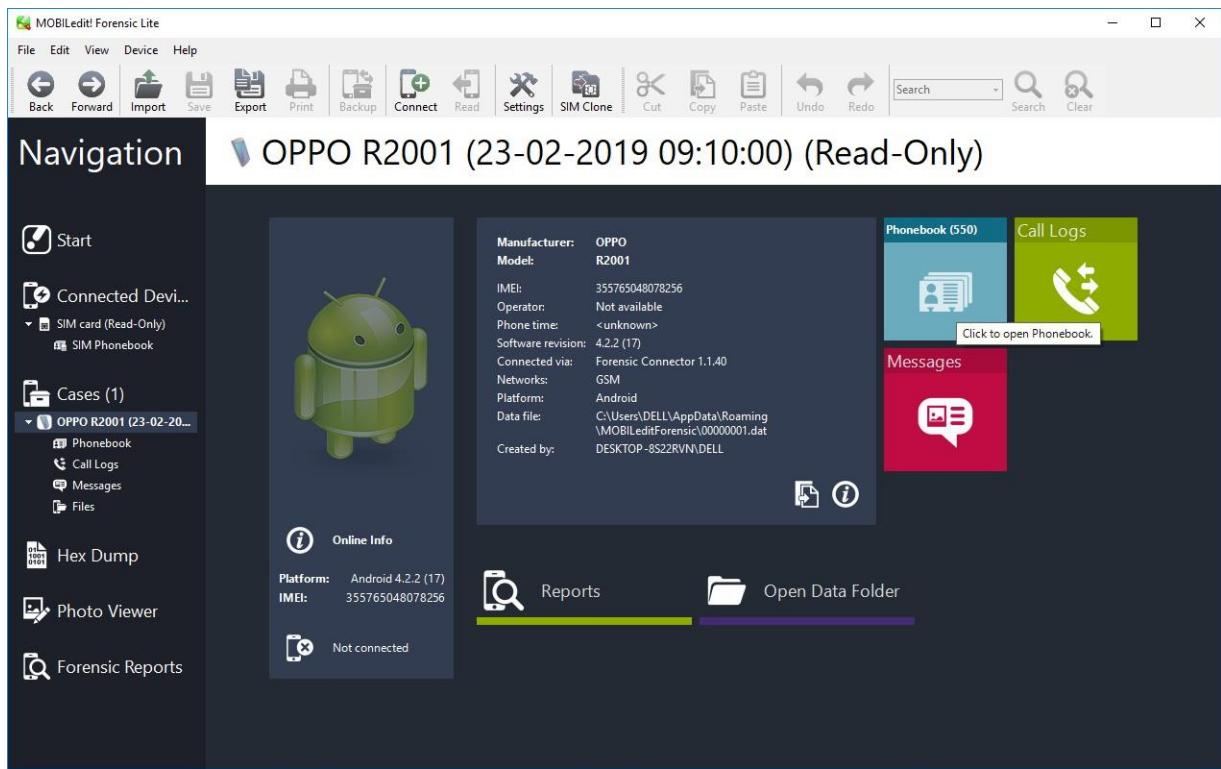
Refresh Why is my phone not listed?

[Online guide](#) < Back Next > Cancel









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

- 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

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

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
Sainat	+91993047554	20-02-2019 11:38:44
Sainat	+919930547554	20-02-2019 11:29:22
Sainat	+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

- 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

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

Conversations (7)	All (504)	Received (500)	Sent (3)	Drafts (1)
Time				
Sender / Recipient				
55256	23-02-2019 08:25:27			55256
IZ-IDEA	22-02-2019 20:55:25	Don't Wait!! Start playing now to Win GOLD voucher worth Rs 25000. CALL 55256 Tollfree. TnC		55256
Aaaaa	22-02-2019 17:19:31	और कॉल करें Rs 35 और 65 का रोचास जीतें। डायल करें 55256 मुफ्त		55256
IM-655456	22-02-2019 14:46:43	Chance!! Win Rs 65 & Rs 35 worth FREE Recharge Everyday. Dial 7777 (Tollfree) TnC		55256
IM-612345	22-02-2019 14:15:48	Rs 5000 का नवद कोरक जीतें और आनंद लें। डायल करें 55256 मुफ्त		55256
IM-6554563	22-02-2019 10:34:12	Limited Chance!! Call 55256 Tollfree and Win Rs 65 worth Recharge Everyday. TnC		55256
+919987501727	21-02-2019 16:52:49	Special OFFER! Aaj khelo aur jeet sakte ho Rs.1000 CashWho is Known as MAHATMATA?) GandhijiB NehruReply now A or B to 55256TnC & Aaj Jeeto		55256
MD-KOTAKB	21-02-2019 16:44:12			55256
AX-IYCGOV	21-02-2019 12:05:36			55256
IM-657886				

PRACTICAL 9

Aim :- Email Forensics

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

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

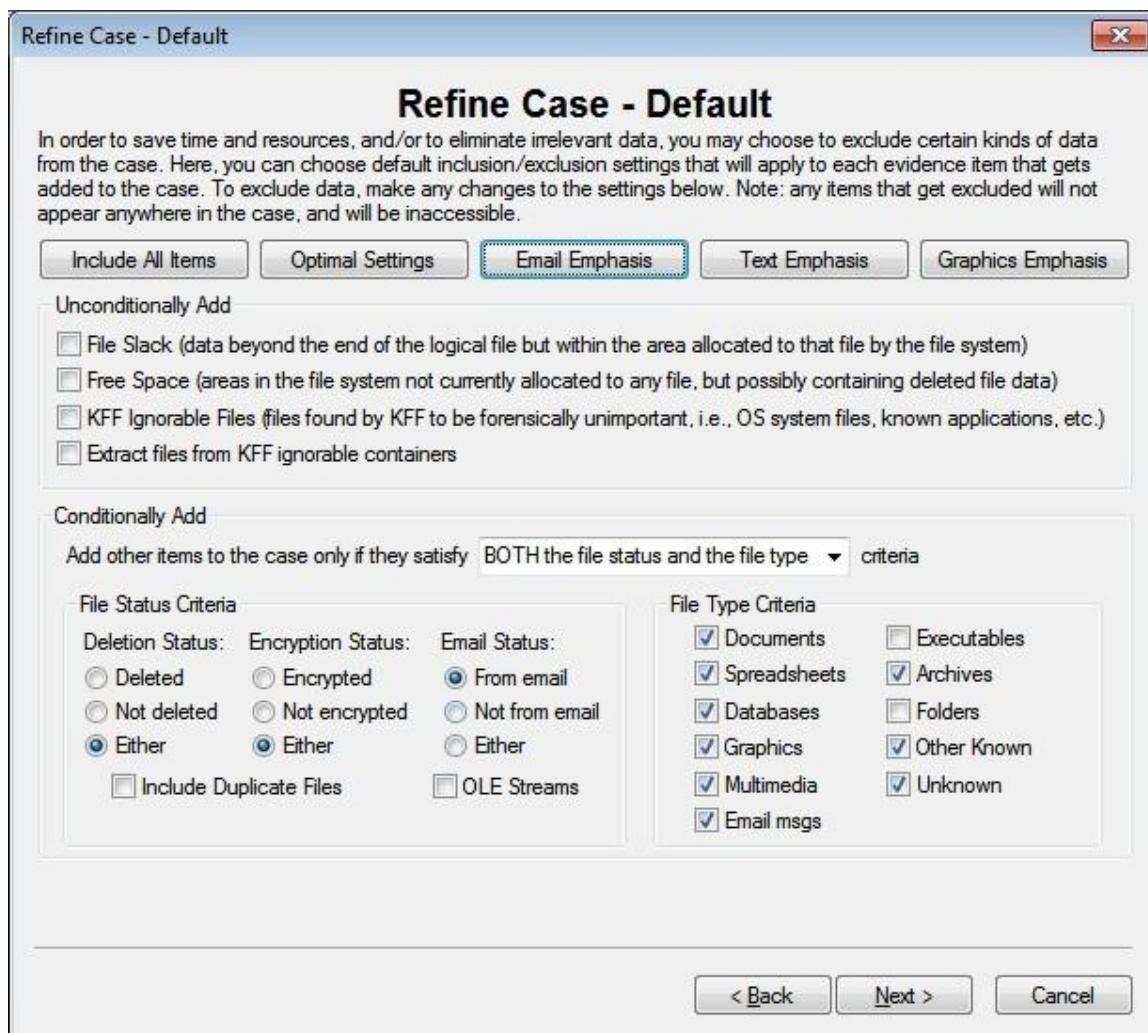
Because of Jim's responses to a poor performance review, the CEO of Superior Bicycles, Martha Dax, suspects he might have obtained sensitive information about the company's business model that he's leaking to a competitor.

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.

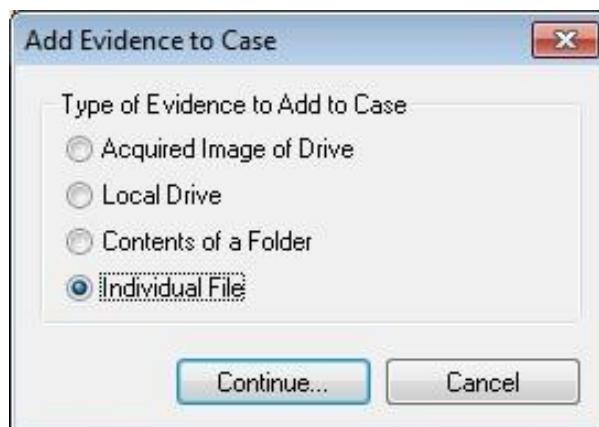
Recovering Email

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** .

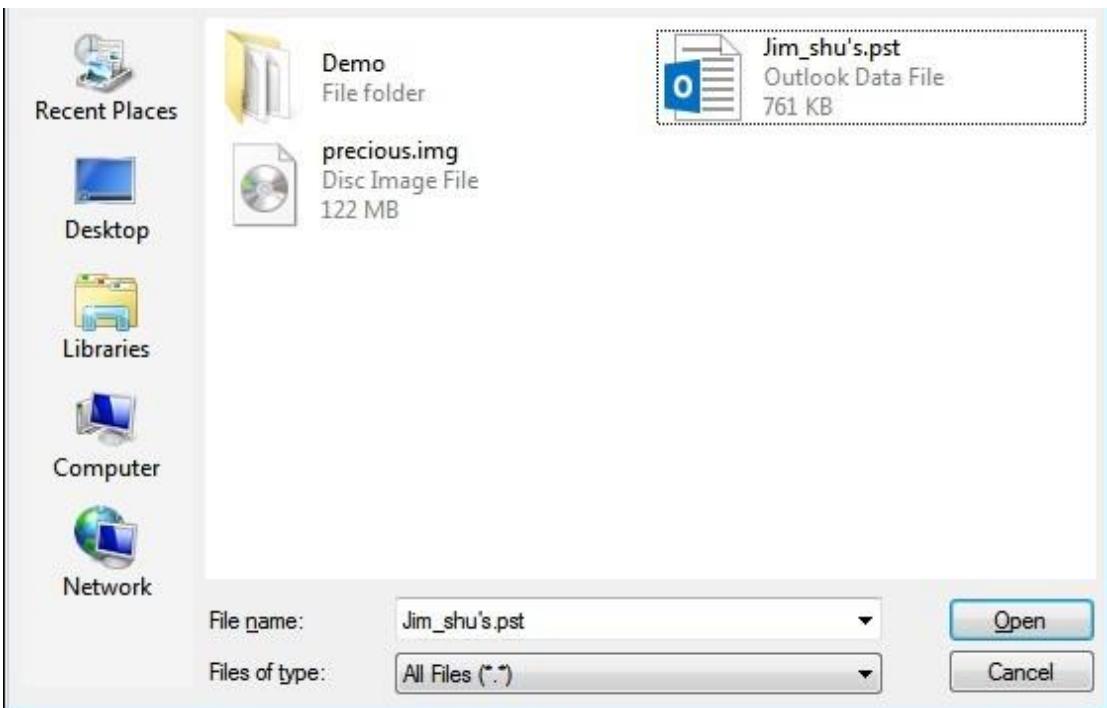


Click **Next** until you reach the **Add Evidence to Case** dialog box, and then click the **Add Evidence** button.

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.

AccessData FTK 1.81.0 DEMO VERSION -- E:\CF\EmailForensic\

File Edit View Tools Help

Overview Explore Graphics E-Mail Search Bookmark

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

File Name Full Path Recycle Bi... Ext File Type Category Subject Cr Date Mod Date Acc Date

Message0001	C:\Users\Administrator\Desktop\All Docs of Des...			E-mail Messa...	E-mail	"RE: Bike ...	12/3/2006 10:05:51 ...	12/3/2006 10:05:51 ...	N/A
Message0001	C:\Users\Administrator\Desktop\All Docs of Des...			E-mail Messa...	E-mail	"Request"	12/3/2006 9:06:44 PM	12/7/2006 6:39:39 PM	N/A
Message0001	C:\Users\Administrator\Desktop\All Docs of Des...			E-mail Messa...	E-mail	"RE: Bicyc..."	12/3/2006 9:09:12 PM	12/3/2006 9:09:12 PM	N/A
Message0001	C:\Users\Administrator\Desktop\All Docs of Des...			E-mail Messa...	E-mail	"problem"	12/3/2006 9:06:45 PM	12/7/2006 6:39:27 PM	N/A
Message0002	C:\Users\Administrator\Desktop\All Docs of Des...			E-mail Messa...	E-mail	"FW: probl..."	12/7/2006 6:39:22 PM	12/7/2006 6:39:22 PM	N/A
Message0002	C:\Users\Administrator\Desktop\All Docs of Des...			E-mail Messa...	E-mail	"Bike spec..."	12/3/2006 9:06:40 PM	12/7/2006 6:39:57 PM	N/A
Message0002	C:\Users\Administrator\Desktop\All Docs of Des...			E-mail Messa...	E-mail	"RE: Bike ..."	12/3/2006 9:08:27 PM	12/3/2006 9:08:27 PM	N/A
Message0002	C:\Users\Administrator\Desktop\All Docs of Des...			E-mail Messa...	E-mail	"Bicycle of..."	12/3/2006 9:06:43 PM	12/7/2006 6:39:47 PM	N/A
Message0003	C:\Users\Administrator\Desktop\All Docs of Des...			E-mail Messa...	E-mail	"FW: anot..."	12/7/2006 6:38:58 PM	12/7/2006 6:38:58 PM	N/A
Message0003	C:\Users\Administrator\Desktop\All Docs of Des...			E-mail Messa...	E-mail	"RE: Bike ..."	12/3/2006 9:16:48 PM	12/7/2006 6:39:12 PM	N/A
Message0003	C:\Users\Administrator\Desktop\All Docs of Des...			E-mail Messa...	E-mail	"FW: Bike ..."	12/7/2006 6:39:51 PM	12/7/2006 6:39:51 PM	N/A
Message0004	C:\Users\Administrator\Desktop\All Docs of Des...			E-mail Messa...	E-mail	"Re: Bicycl..."	12/3/2006 9:16:46 PM	12/7/2006 6:39:19 PM	N/A
Message0004	C:\Users\Administrator\Desktop\All Docs of Des...			E-mail Messa...	E-mail	"FW: Bicy..."	12/7/2006 6:39:43 PM	12/7/2006 6:39:43 PM	N/A
Message0005	C:\Users\Administrator\Desktop\All Docs of Des...			E-mail Messa...	E-mail	"Re: Bicycl..."	12/3/2006 10:04:32 ...	12/7/2006 6:38:35 PM	N/A
Message0005	C:\Users\Administrator\Desktop\All Docs of Des...			E-mail Messa...	E-mail	"FW: Req..."	12/7/2006 6:39:32 PM	12/7/2006 6:39:32 PM	N/A
Message0006	C:\Users\Administrator\Desktop\All Docs of Des...			E-mail Messa...	E-mail	"RE: Bike ..."	12/3/2006 10:04:33 ...	12/7/2006 6:38:25 PM	N/A
Message0006	C:\Users\Administrator\Desktop\All Docs of Des...			E-mail Messa...	E-mail	"FW: Bike ..."	12/7/2006 6:39:06 PM	12/7/2006 6:39:06 PM	N/A
Message0007	C:\Users\Administrator\Desktop\All Docs of Des...			E-mail Messa...	E-mail	"Re: Bicycl..."	12/4/2006 9:38:44 AM	12/7/2006 6:38:17 PM	N/A
Message0007	C:\Users\Administrator\Desktop\All Docs of Des...			E-mail Messa...	E-mail	"FW: Activ..."	12/7/2006 6:38:44 PM	12/7/2006 6:38:44 PM	N/A

32 Listed 0 Checked Total 0 Highlighted

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.

AccessData FTK 1.81.0 DEMO VERSION -- E:\CF\EmailForensic\

File Edit View Tools Help

Overview Explore Graphics E-Mail Search Bookmark

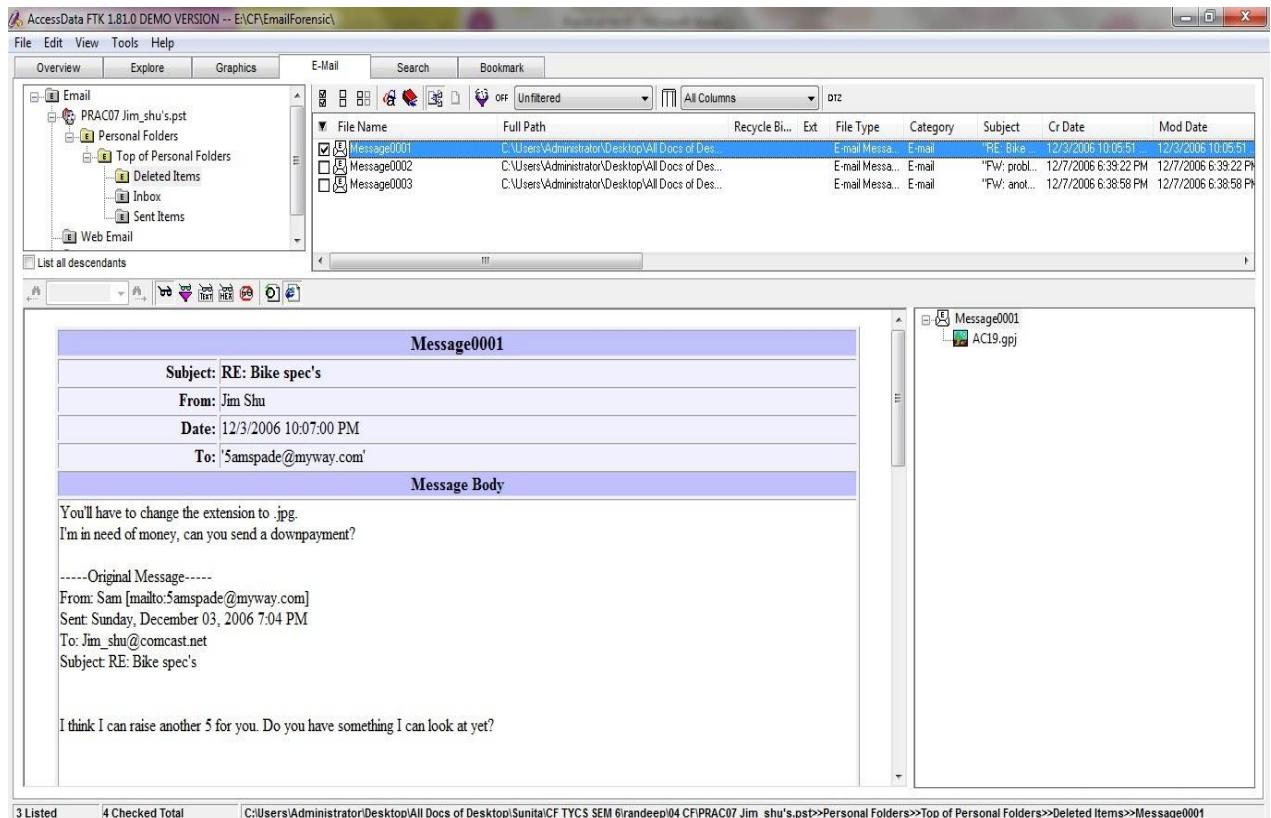
File Name Full Path Recycle Bi... Ext File Type Category Subject Cr Date Mod Da

Message0001	C:\Users\Administrator\Desktop\All Docs of Des...			E-mail Messa...	E-mail	"RE: Bike ..."	12/3/2006 10:05:51 ...	12/3/2006
Message0002	C:\Users\Administrator\Desktop\All Docs of Des...			E-mail Messa...	E-mail	"FW: probl..."	12/7/2006 6:39:22 PM	12/7/2006
Message0003	C:\Users\Administrator\Desktop\All Docs of Des...			E-mail Messa...	E-mail	"FW: anot..."	12/7/2006 6:38:58 PM	12/7/2006

File Name Full Path Recycle Bi... Ext File Type Category Subject Cr Date Mod Da

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**.

AccessData FTK 1.81.0 DEMO VERSION - E:\CF\EmailForensic\

File Edit View Tools Help

Overview Explore Graphics E-Mail Search Bookmark

Email PRAC07 Jim_shu's.pst

- Personal Folders
 - Top of Personal Folders
 - Deleted Items
 - Inbox
 - Sent Items
- Web Email
- Other Email

List all descendants

File Name Full Path Recycle Bi... Ext File Type Category Subject Cr Date Mod Date

File Name	Full Path	Recycle Bi...	Ext	File Type	Category	Subject	Cr Date	Mod Date
Message0001	C:\Users\Administrator\Desktop\All Docs of Des...			E-mail Messa...	E-mail	"Request"	12/3/2006 9:06:44 PM	12/7/2006 6:39:39 PM
Message0002	C:\Users\Administrator\Desktop\All Docs of Des...			E-mail Messa...	E-mail	"Bike spec..."	12/3/2006 9:06:40 PM	12/7/2006 6:39:57 PM
Message0003	C:\Users\Administrator\Desktop\All Docs of Des...			E-mail Messa...	E-mail	"RE: Bike ..."	12/3/2006 9:16:48 PM	12/7/2006 6:39:12 PM
Message0004	C:\Users\Administrator\Desktop\All Docs of Des...			E-mail Messa...	E-mail	"Re: Cycl..."	12/3/2006 9:16:46 PM	12/7/2006 6:39:19 PM
Message0005	C:\Users\Administrator\Desktop\All Docs of Des...			E-mail Messa...	E-mail	"Re: Cycl..."	12/3/2006 10:04:32...	12/7/2006 6:38:35 PM
Message0006	C:\Users\Administrator\Desktop\All Docs of Des...			E-mail Messa...	E-mail	"RE: Bike ..."	12/3/2006 10:04:33...	12/7/2006 6:38:25 PM
Message0007	C:\Users\Administrator\Desktop\All Docs of Des...			E-mail Messa...	E-mail	"Re: Cycl..."	12/4/2006 9:38:44 AM	12/7/2006 6:38:17 PM
Message0008	C:\Users\Administrator\Desktop\All Docs of Des...			E-mail Messa...	E-mail	"Re: Cycl..."	12/6/2006 9:16:08 PM	12/7/2006 6:37:36 PM
Message0009	C:\Users\Administrator\Desktop\All Docs of Des...			E-mail Messa...	E-mail	"RE: Bike ..."	12/6/2006 9:16:10 PM	12/7/2006 6:37:17 PM
Message0010	C:\Users\Administrator\Desktop\All Docs of Des...			E-mail Messa...	E-mail	"Investors"	2/17/2007 4:45:48 PM	2/17/2007 4:45:48 PM

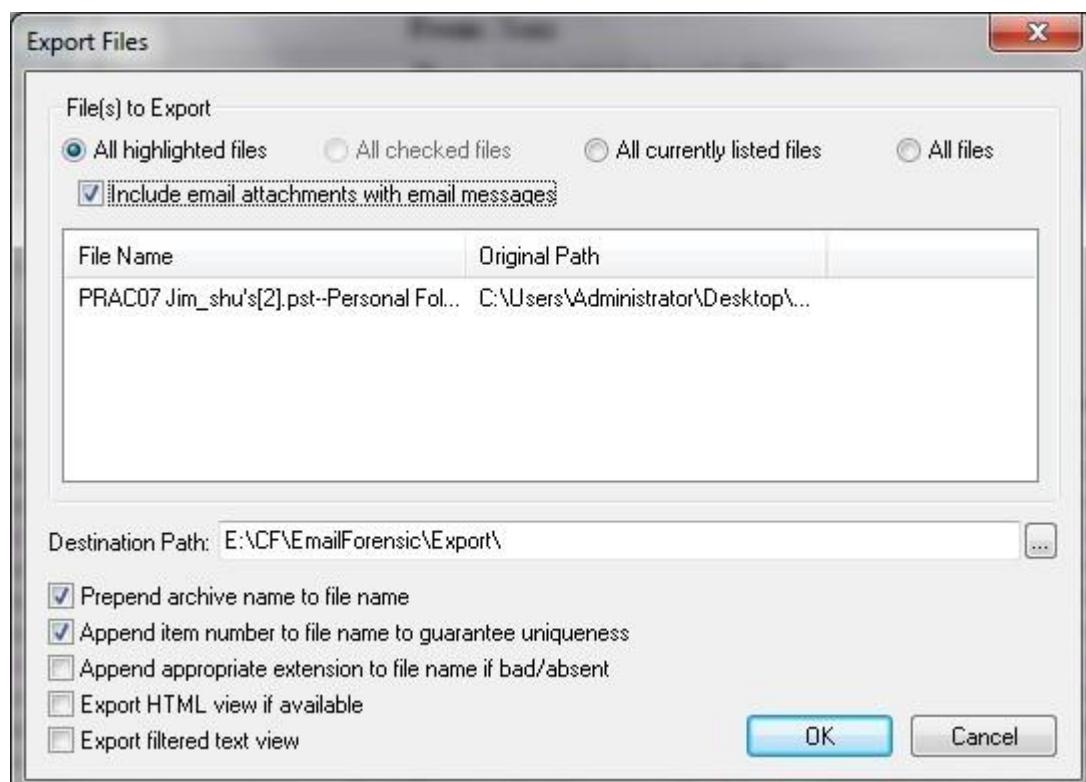
Message0003

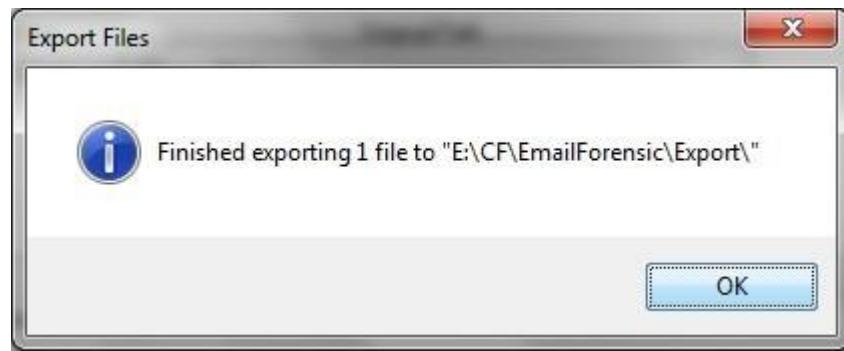
Subject: RE: Bike spec's
 From: Sam
 Date: 12/3/2006 9:14:02 PM
 To: Jim_shu@comcast.net

Message Body

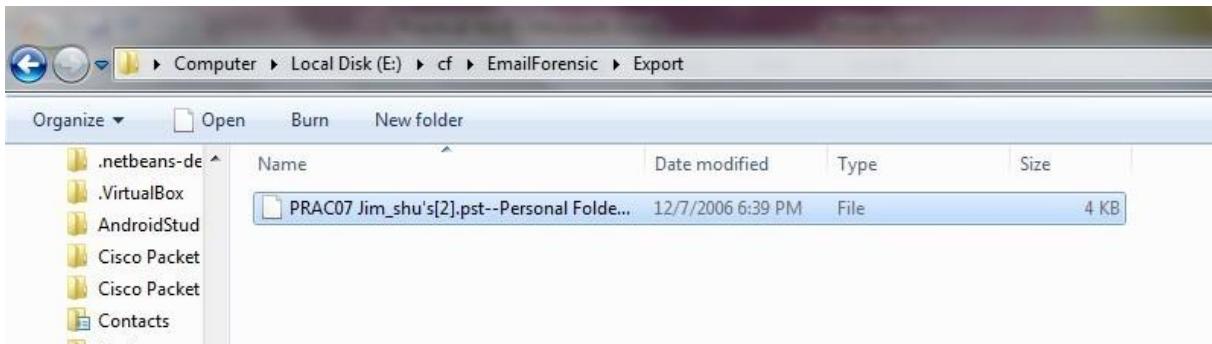
We might be able to go \$4000 if it is good. Is it? Sam

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

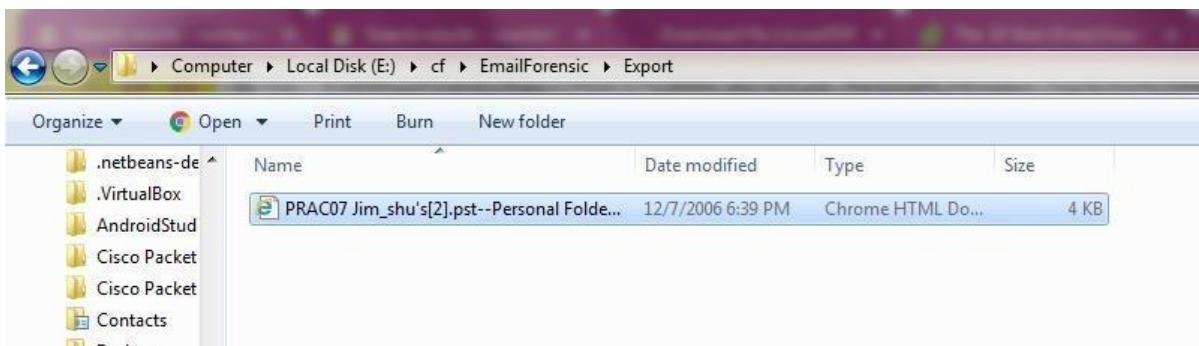




FTK saves exported files in the HTML format with no extension.



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.



Conversation Topic: Bike spec's Sender Name: Sam Received By: Jim Shu Delivery Time: 12/3/2006 9:14:02 PM Creation Time: 12/3/2006 9:16:48 PM Modification Time: 12/7/2006 6:39:12 PM Submit Time: 12/3/2006 9:14:14 PM Flags: 1 = Read Size: 6456 Received: from myway.com (nn1.excitenetwork.com[207.159.120.55](untrusted sender)) by alnrmxc23.comcast.net (alnrmxc23) with ESMTP id <20061204021402a2300i90t3e>; Mon, 4 Dec 2006 02:14:02 +0000 X-Originating-IP: [207.159.120.55] Received: by mprdmixin.myway.com (Postfix, from userid 110) id 63B6067669; Sun, 3 Dec 2006 21:14:14 -0500 (EST) To: Jim_shu@comcast.net Subject: RE: Bike spec's Received: from [24.18.24.250] by mprdmilfe3.nwk.myway.com via HTTP; Sun, 03 Dec 2006 21:14:14 EST X-AntiAbuse: This header was added to track abuse, please include it with any abuse report X-AntiAbuse: ID=f869dfbea97fe07b9eab2f865d19b540 Reply-to: Samspade@myway.com From: "Sam" <Samspade@myway.com> MIME-Version: 1.0 X-Sender: Samspade@myway.com X-Mailer: PHP Content-Type: text/plain; charset="US-ASCII" Content-Transfer-Encoding: 7bit Message-Id: <20061204021414.63B6067669@mprdmixin.myway.com> Date: Sun, 3 Dec 2006 21:14:14 -0500 (EST) We might be able to go \$4000 if it is good. Is it? Sam --- On Sun 12/03, Jim Shu <Jim_shu@comcast.net> wrote: From: Jim Shu [mailto: Jim_shu@comcast.net] To: Samspade@myway.com Date: Sun, 3 Dec 2006 18:09:06 -0800 Subject: RE: Bike spec's How much are you willing to pay me to get these plans to you? Jim-----Original Message-----From: Sam [mailto: Samspade@myway.com] Sent: Sunday, December 03, 2006 5:40 PM To: Jim_shu@comcast.net Subject: Bike spec's Do you have them yet? I've got people in Asia ready to duplicate them? Sam _____ No banners. No pop-ups. No kidding. Make My Way your home on the Web - http://www.myway.com _____ No banners. No pop-ups. No kidding. Make My Way your home on the Web - http://www.myway.com

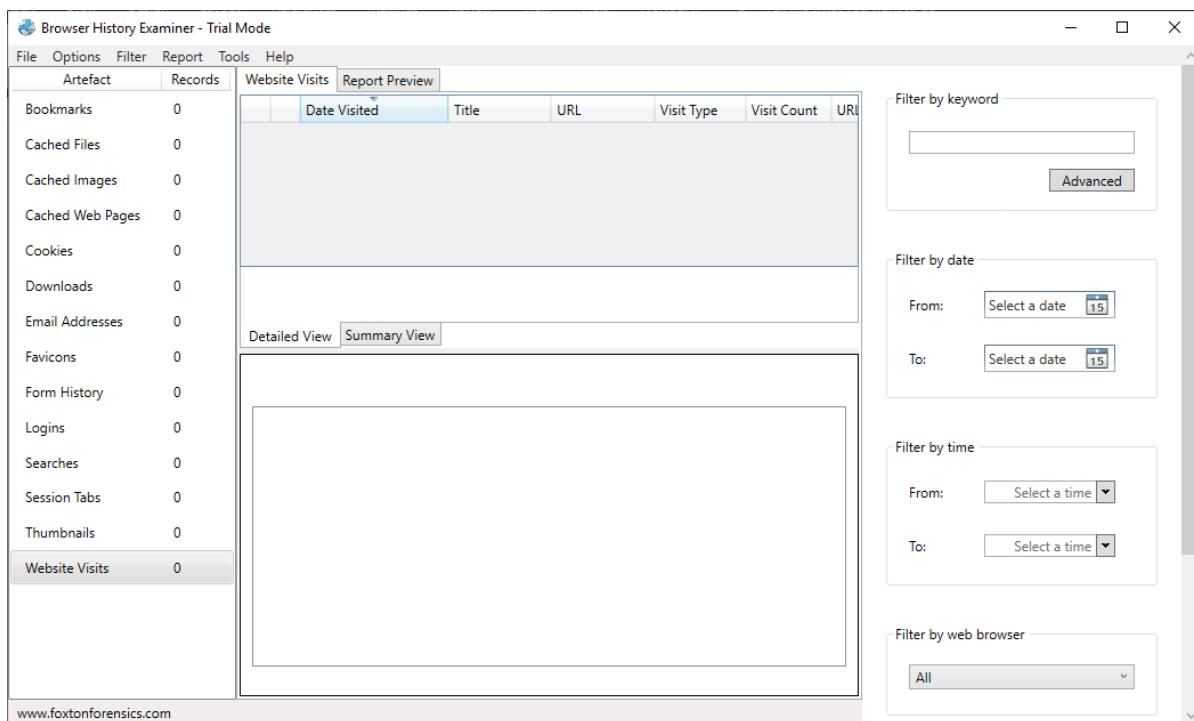
PRACTICAL 10

Aim: Web Browser Forensics .

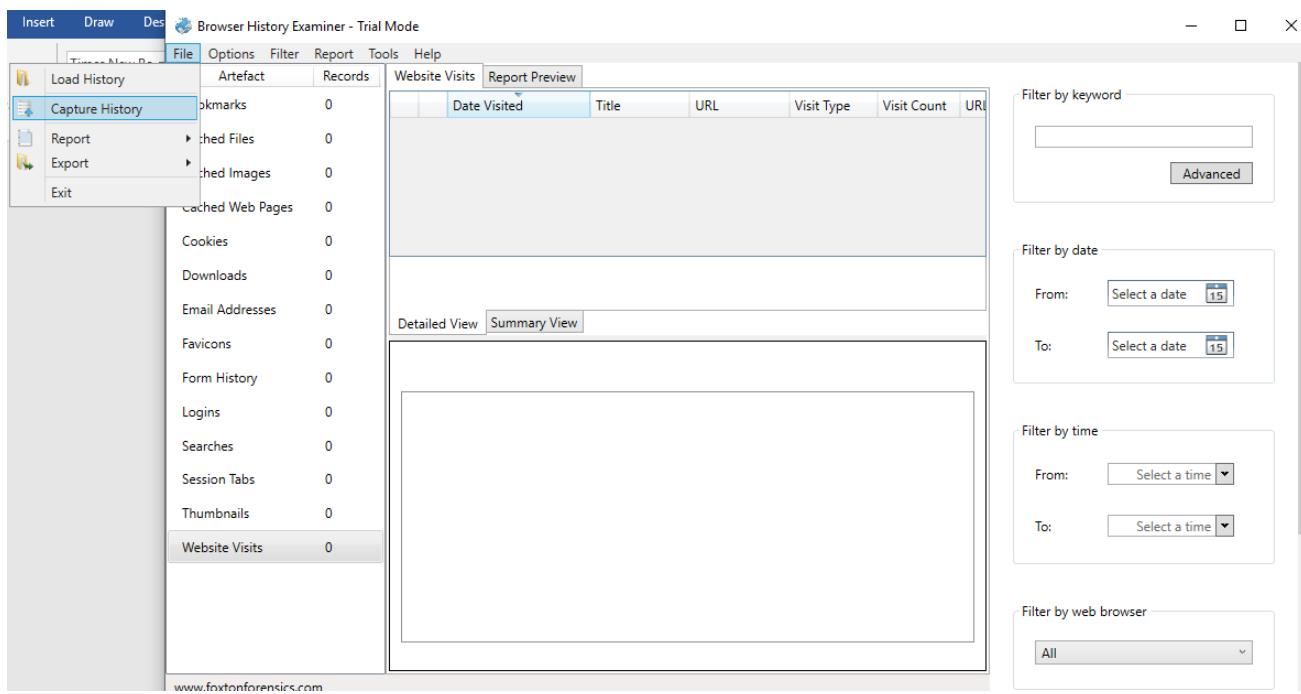
- Web Browser working
- Forensics activities on browser
- Cache / Cookies analysis
- Last Internet activity

Steps:

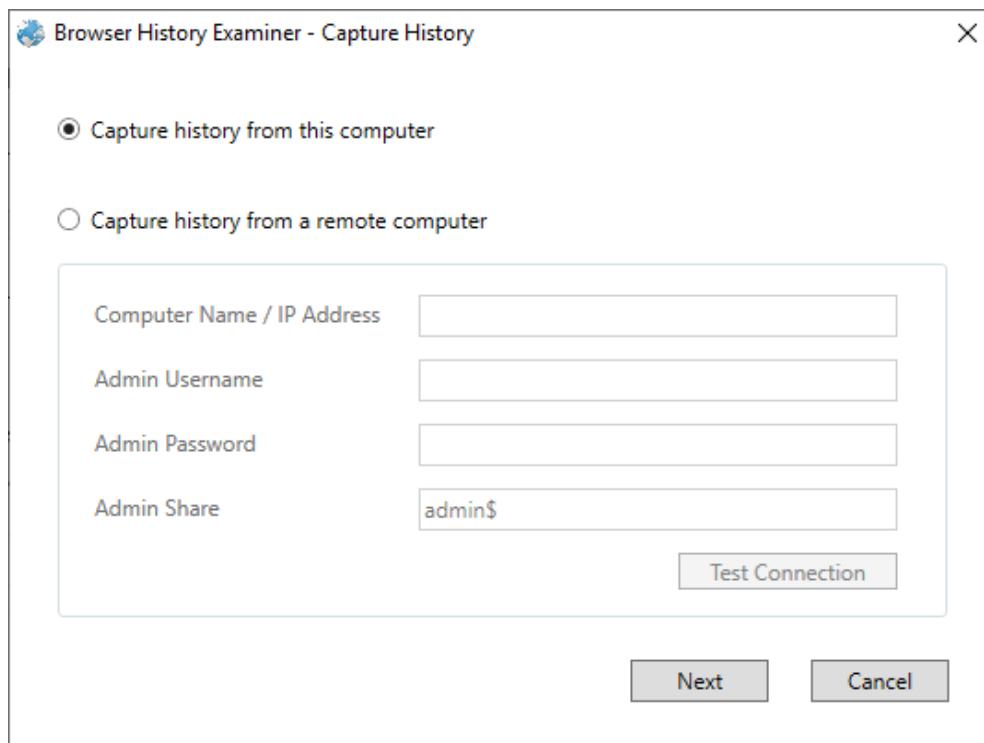
1. Open BrowserHistoryExaminer.



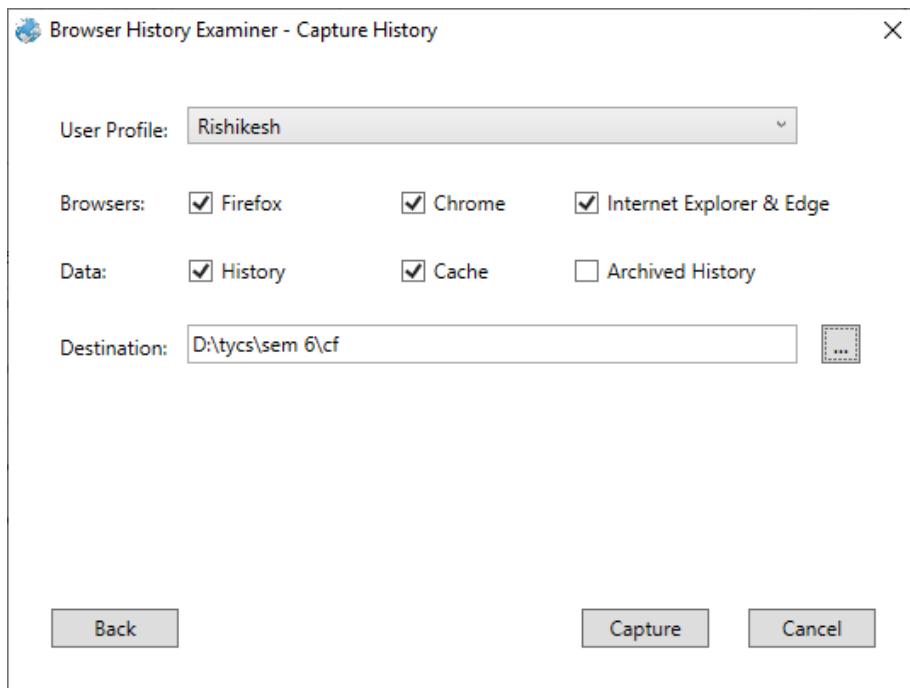
2. Click on file > Capture History



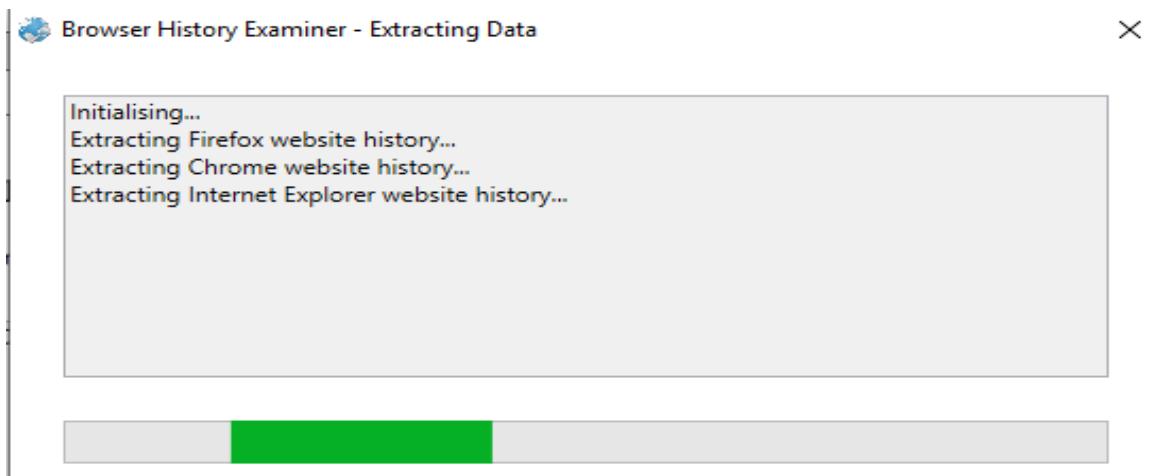
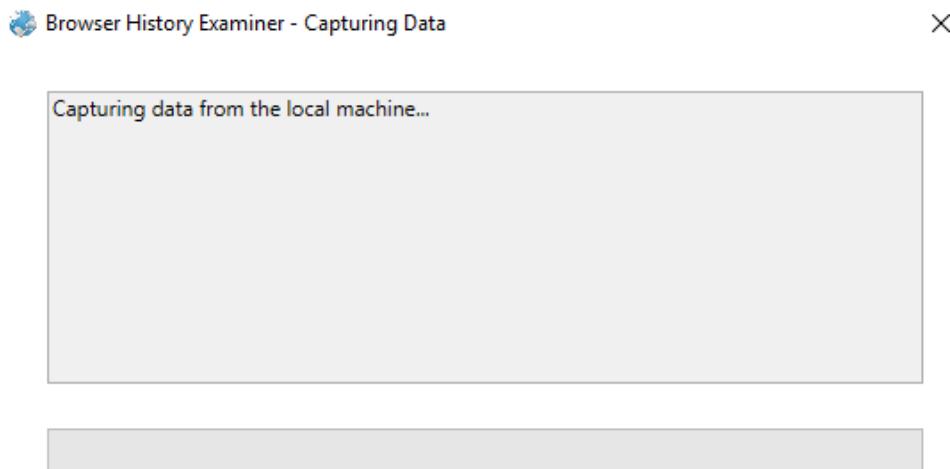
3. Select the capture folder and click on next.



4. Enter the destination to capture the data.



5. The History is been extracting.



6. The data has been retrieved.

The screenshot shows the 'Browser History Examiner - Trial Mode' application window. The left panel lists various artifacts with their counts: Bookmarks (8), Cached Files (4615), Cached Images (177), Cached Web Pages (36), Cookies (1566), Downloads (80), Email Addresses (30), Favicons (1790), Form History (31), Logins (3), Searches (1184), Session Tabs (62), Thumbnails (12), and Website Visits (2688). The 'Website Visits' tab is selected, displaying a table of visit records:

	Date Visited	Title	URL	Visit Type	Visit Count
★	18-03-2019 03:42:10		file:///D:/cf.docx		
★	18-03-2019 03:26:21		file:///D:/tycs/se		
★	18-03-2019 03:25:29		file:///D:/tycs/se		
★	18-03-2019 03:25:28		file:///D:/tycs/se		
★	18-03-2019 03:21:24		file:///D:/cc.pdf		
★	18-03-2019 03:21:24		file:///D:/cc.pdf		

Below the table, it says 'Viewing 25/25 records'. To the right, there are four filter panels: 'Filter by keyword', 'Filter by date', 'Filter by time', and 'Filter by web browser'. The 'Filter by keyword' panel contains a text input and an 'Advanced' button. The 'Filter by date' panel has 'From' and 'To' fields set to 'Select a date 15'. The 'Filter by time' panel has 'From' and 'To' fields set to 'Select a time'. The 'Filter by web browser' panel has a dropdown set to 'All'.

7. On the left panel click on bookmarks.

The screenshot shows the 'Browser History Examiner - Trial Mode' application window. The left panel lists various artifacts with their counts, identical to the previous screenshot. The 'Bookmarks' tab is selected, displaying a table of bookmark records:

	Date Added	Last Modified	Title	URL	Web Browser
★	17-03-2019 09:03:01	17-03-2019 09:03:01	Getting	https://	Firefox
★	17-03-2019 09:03:01	17-03-2019 09:03:01	Help ar	https://	Firefox
★	17-03-2019 09:03:01	17-03-2019 09:03:01	Custom	https://	Firefox
★	17-03-2019 09:03:01	17-03-2019 09:03:01	Get Inv	https://	Firefox
★	17-03-2019 09:03:01	17-03-2019 09:03:01	About l	https://	Firefox
★	14-03-2019 05:01:05		New Ta	chrome	Chrome
★	22-01-2019 06:40:50		Downlc	https://	Chrome
★			Bing	http://c	Internet Explorer

Below the table, it says 'Viewing 8/8 records'. To the right, there are four filter panels: 'Filter by keyword', 'Filter by date', 'Filter by time', and 'Filter by web browser'. The 'Filter by keyword' panel contains a text input and an 'Advanced' button. The 'Filter by date' panel has 'From' and 'To' fields set to 'Select a date 15'. The 'Filter by time' panel has 'From' and 'To' fields set to 'Select a time'. The 'Filter by web browser' panel has a dropdown set to 'All'.

8. On the left panel click on cached files.

Artefact	Records
Bookmarks	8
Cached Files	4615
Cached Images	177
Cached Web Pages	36
Cookies	1566
Downloads	80
Email Addresses	30
Favicons	1790
Form History	31
Logins	3
Searches	1184
Session Tabs	62
thumbnails	12
Website Visits	2688

Viewing 25/25 records Page size: 50

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

9. On the left panel click on cached images.

Artefact	Records
Bookmarks	8
Cached Files	4615
Cached Images	177
Cached Web Pages	36
Cookies	1566
Downloads	80
Email Addresses	30
Favicons	1790
Form History	31
Logins	3
Searches	1184
Session Tabs	62
thumbnails	12
Website Visits	2688

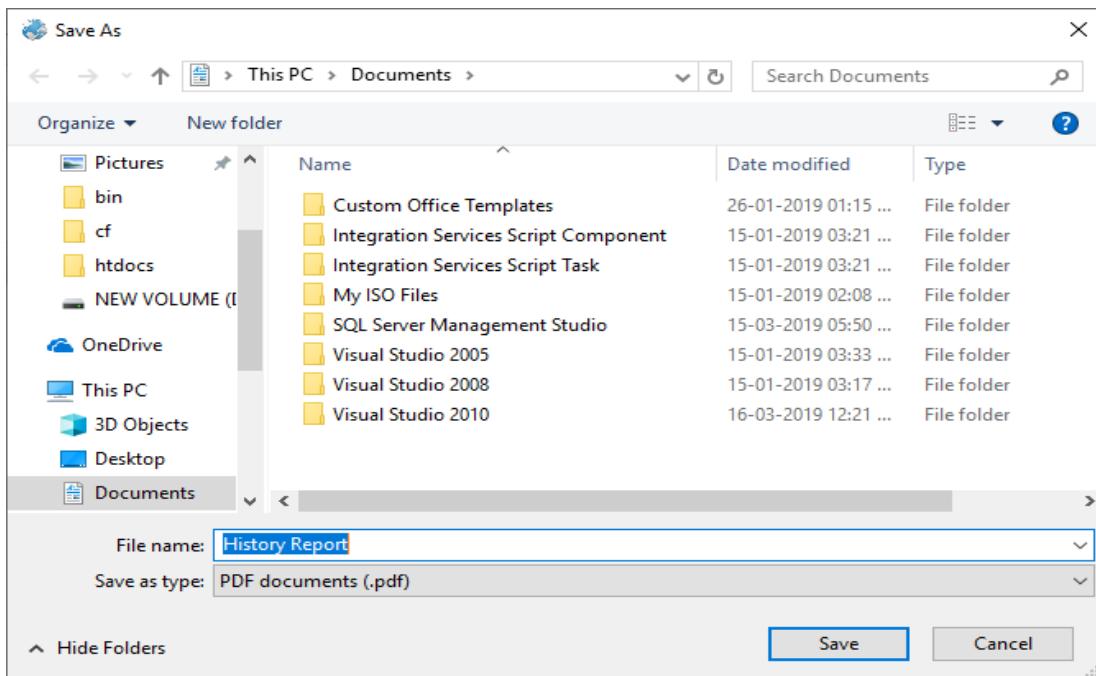
Viewing 25/25 records Page size: 50

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

10. On the left panel click on cookies.

Artefact	Records	Cookies	Report Preview
Bookmarks	8		
Cached Files	4615		
Cached Images	177		
Cached Web Pages	36		
Cookies	1566		
Downloads	80		
Email Addresses	30		
Favicons	1790		
Form History	31		
Logins	3		
Searches	1184		
Session Tabs	62		
thumbnails	12		
Website Visits	2688		

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/?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/?u=2&k=5c151dfa36&attid=0.18a...		18820976	Chrome
	application/zip	https://r3-sn-4p8xoxu-cvhe.googlevideo.com/edged/widevine-cdm4.10.1146.0-win-x64.zip?cms_redirect=yes&a...	1	3523651	Firefox
		https://r3-sn-4p8xoxu-cvhe.googlevideo.com/videoplayback?ei=uYLNNeQA4eiIAb4h7K4Cg&dur=152.733...		2097152	Chrome
		https://r3-sn-4p8xoxu-cvhe.googlevideo.com/videoplayback?ei=uYLNNeQA4eiIAb4h7K4Cg&dur=152.733...		2097152	Chrome
		https://r3-sn-4p8xoxu-cvhe.googlevideo.com/videoplayback?ei=uYLNNeOA4eiIAb4h7K4Co&dur=152.733...		2097152	Chrome

Browser History Examiner - Trial Mode

File Options Filter Report Tools Help

	Artefact	Records	Bookmarks	Report Preview
Load History	Bookmarks	8		
Capture History	Downloaded Files	4615		
Report	Export to Excel			
Export	Export to HTML			
	Export to CSV			
	Export to XML			
	Export to Concordance Load File			
Downloads				
Email Addresses	30			
Favicons	1790			
Form History	31			
Logins	3			
Searches	1184			
Session Tabs	62			
Thumbnails	12			
Website Visits	2688			

Filter by keyword Advanced

Filter by date From: To:

Filter by time From: To:

Filter by web browser All Undo Clear

Viewing 8/8 records | < | 1 | of 1 pages | > | Page size: 50 |

86 of 86 2652 words | www.foxtonforensics.com Time zone: UTC, DST Enabled Date format: dd/mm/yyyy

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/?LinkId=255142	Internet Explorer

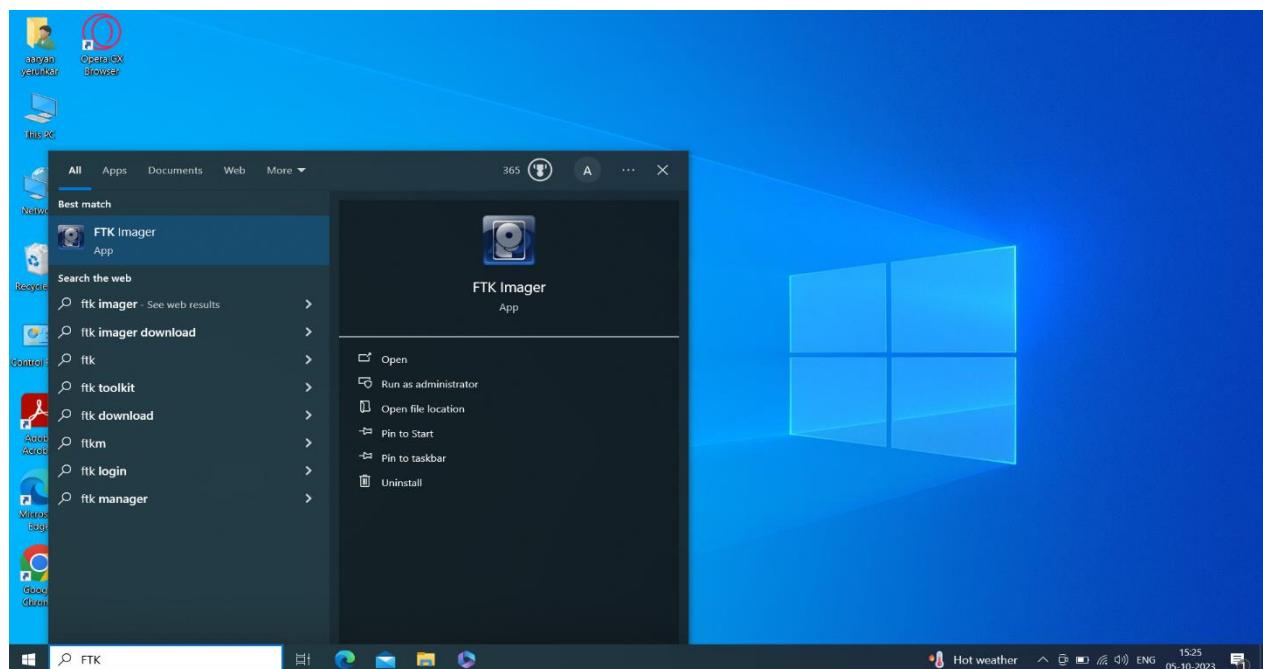
Practical 11

Aim :- Analyze The Memory Dump Of a Running Computer System

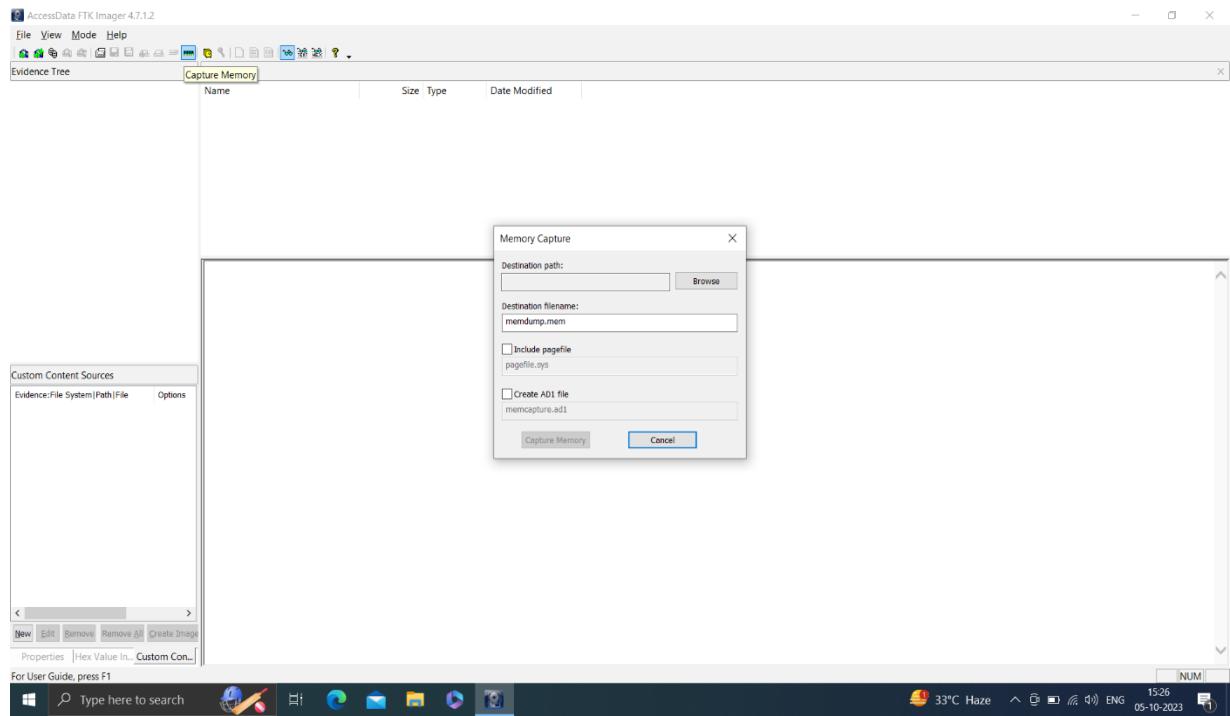
- Capture The Memory Dump By Using AccessData FTK Imager
- Analyze The Memory Dump (.MEM File)

Steps:-

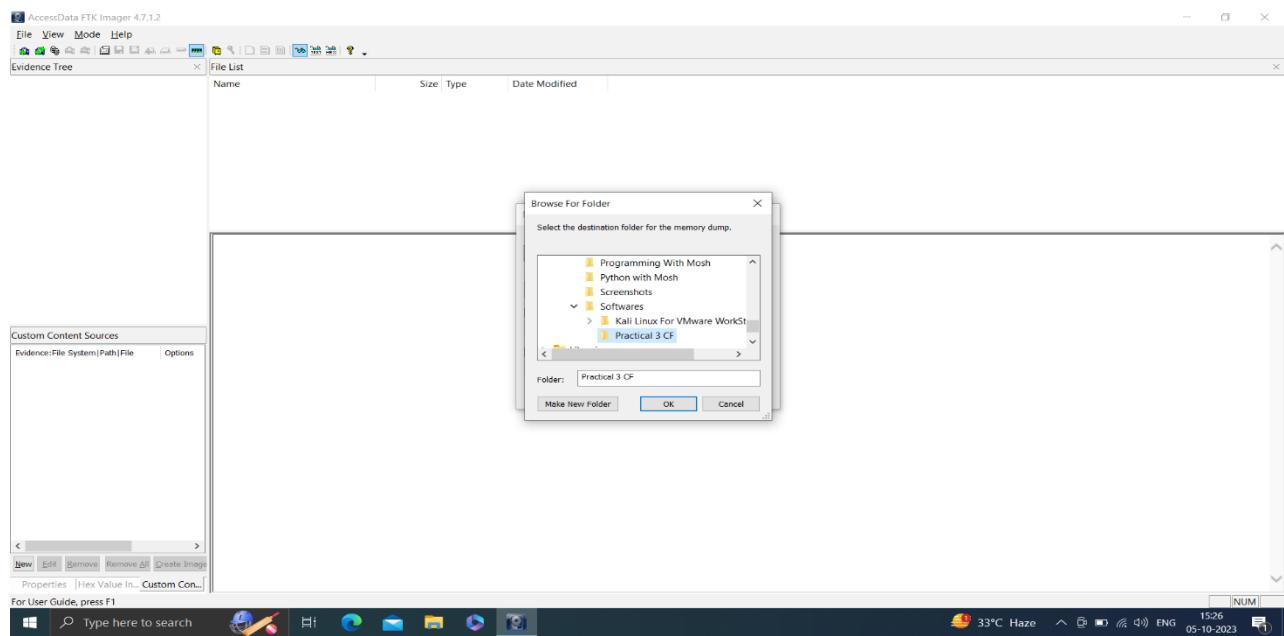
1) On Your Computer Open AccessData FTK Imager



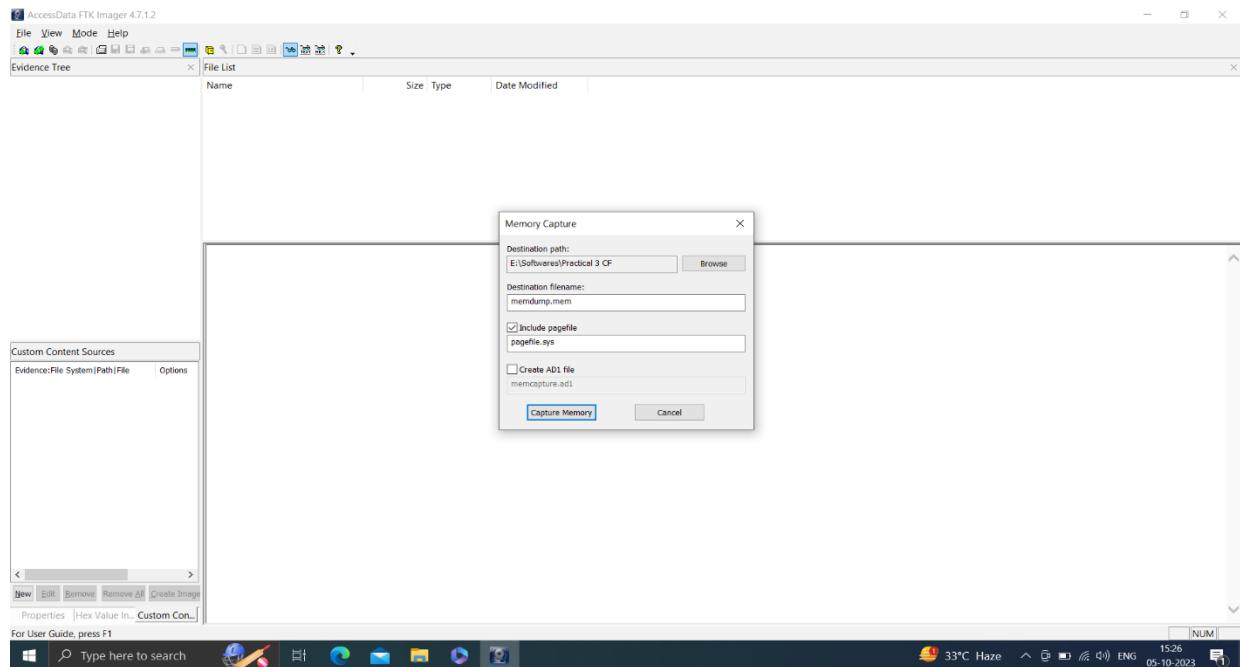
2) Now To Capture Memory Dump Click on ‘Capture Memory’ Icon



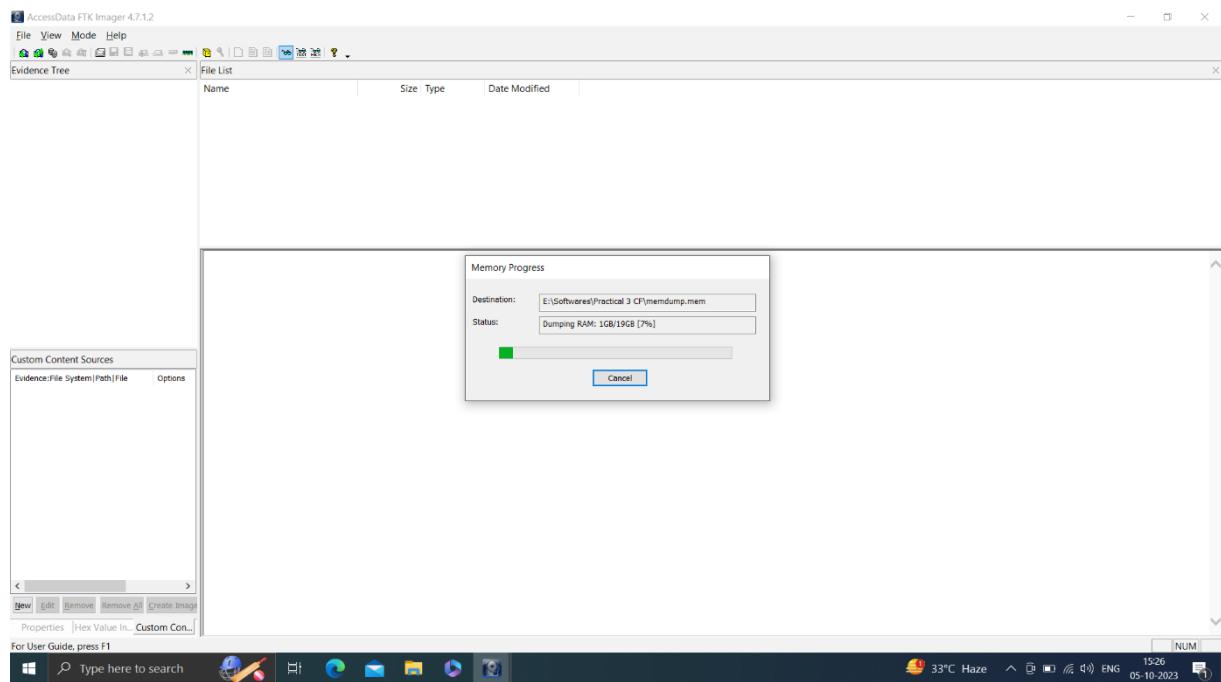
3) Browse The Destination Path



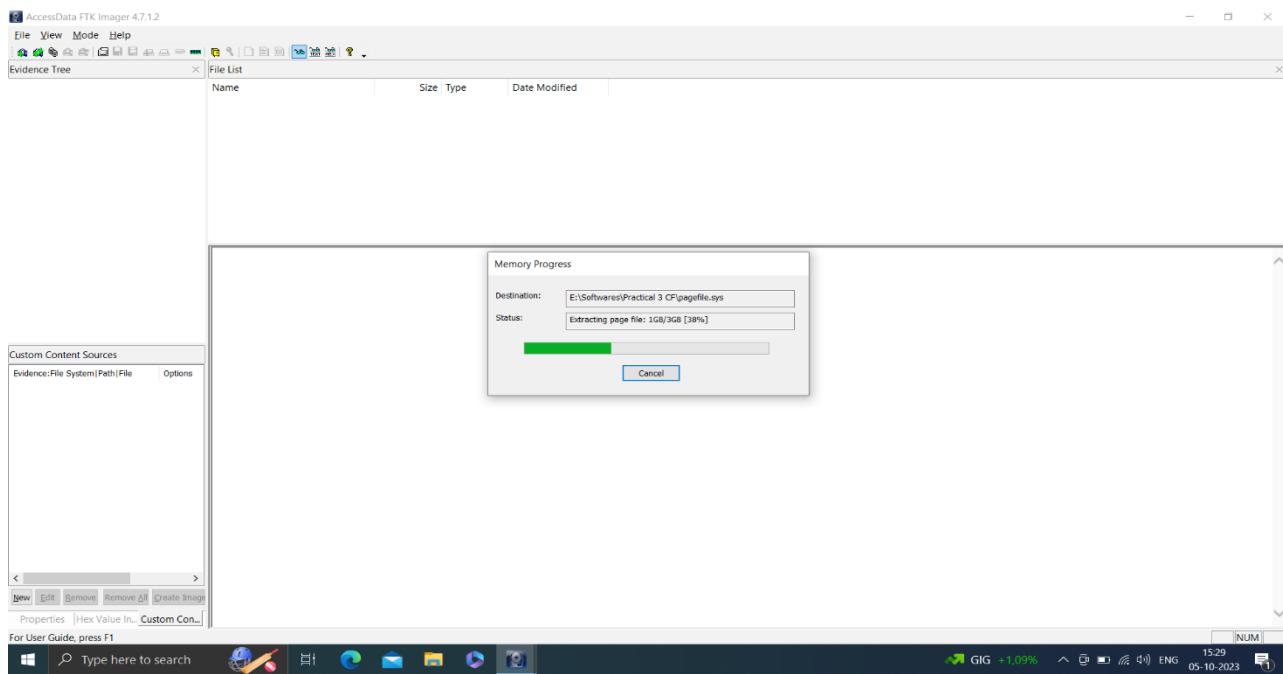
4) Now Click on ‘Include Page File’



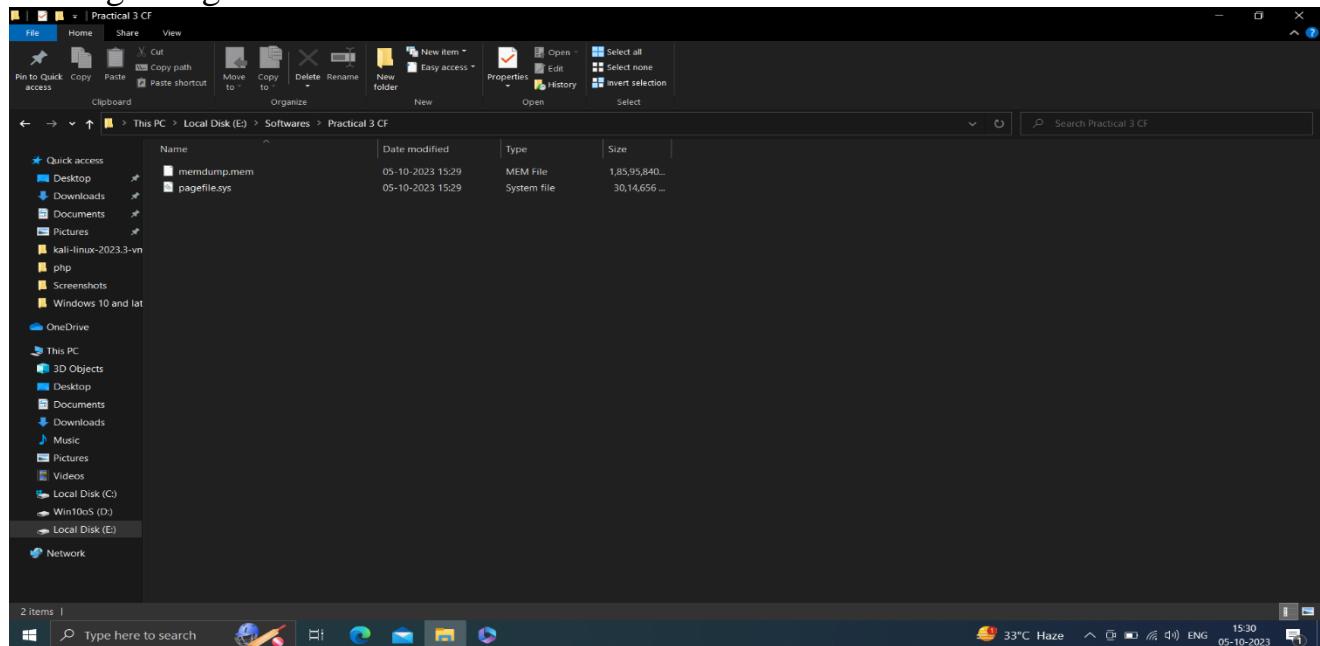
5) Click on Capture Memory to Capture the Memory Dump



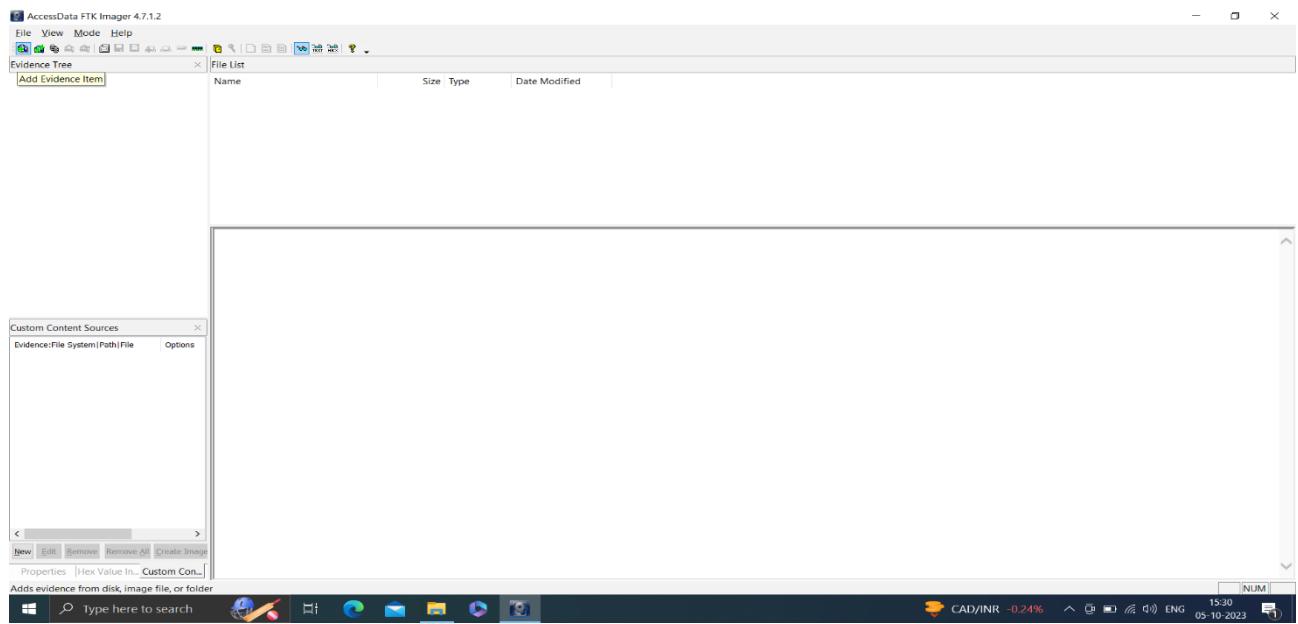
It will Also Extract Page File



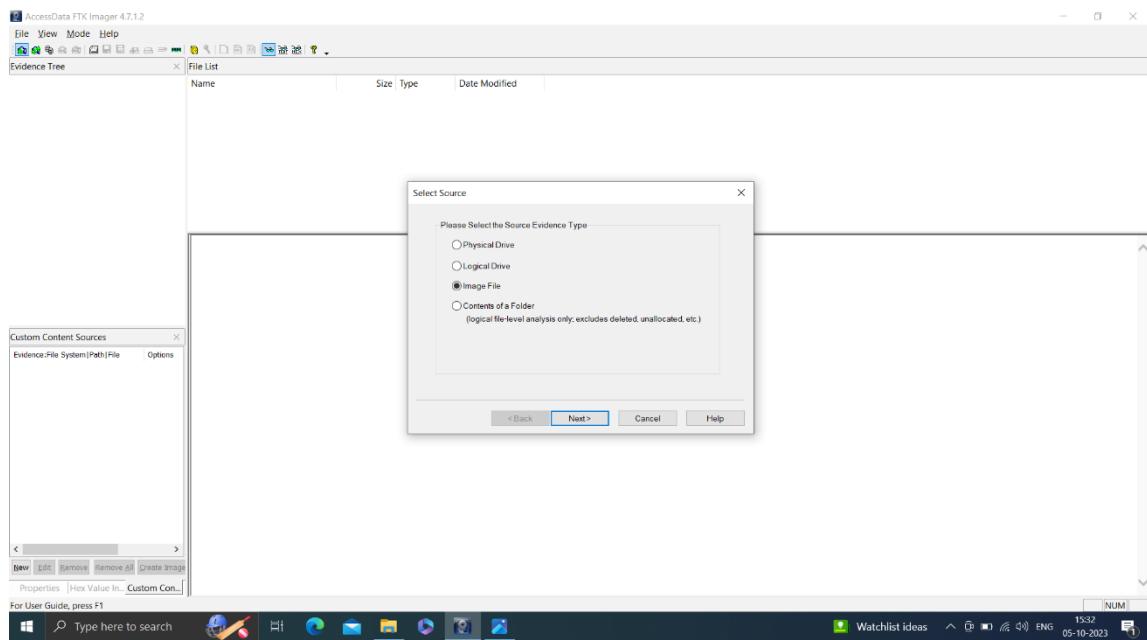
- 6) So After That The Files Will be Displayed In Destination Folder Which You Selected at the Beginning



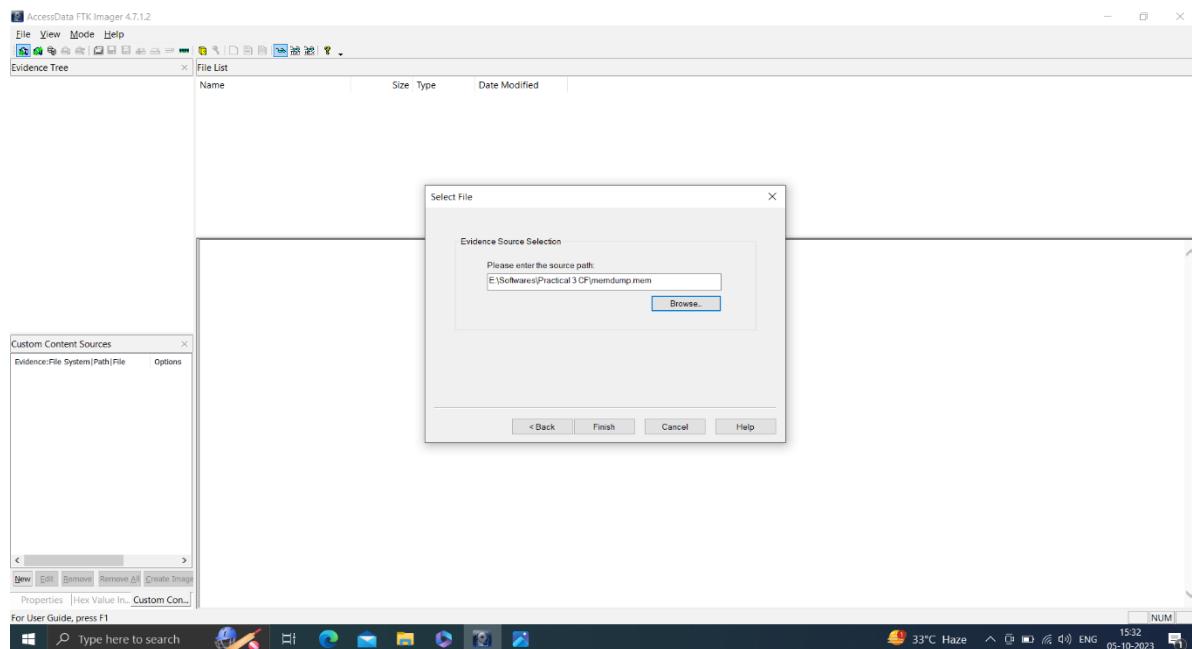
7) Now To Analyze The Memory Dump Click on ‘Add Evidence Item’ Icon



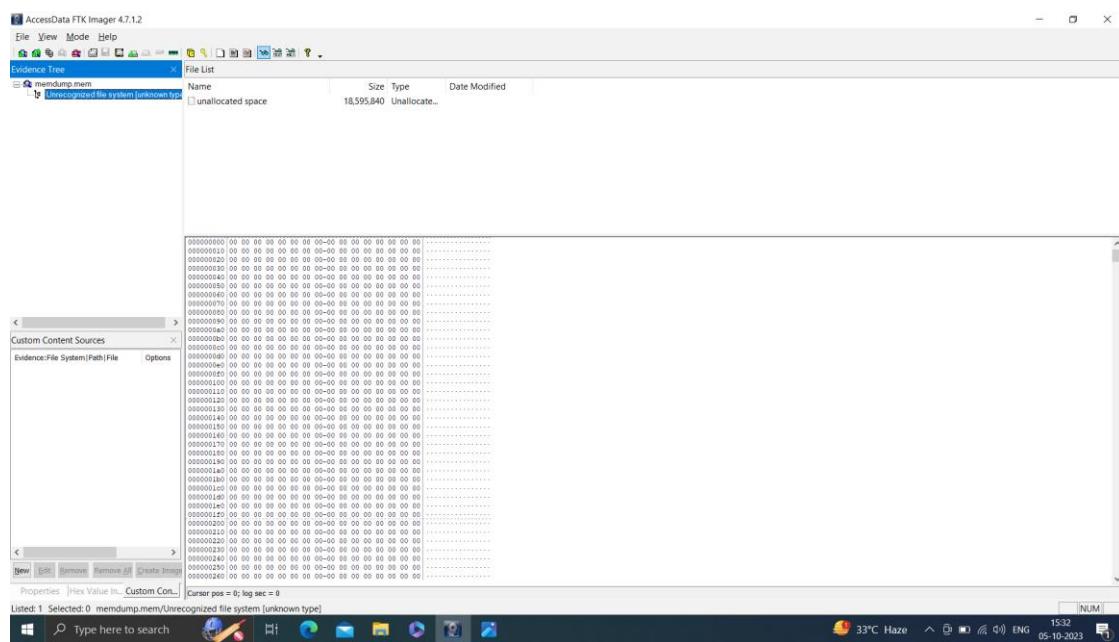
8) Select Source Type ‘Image File’ as Shown In Below Image



9) Browse the Source Path where The Evidence is Stored



10) Then Click on Finish and The Memory Dump Will be analyzed



Practical 12

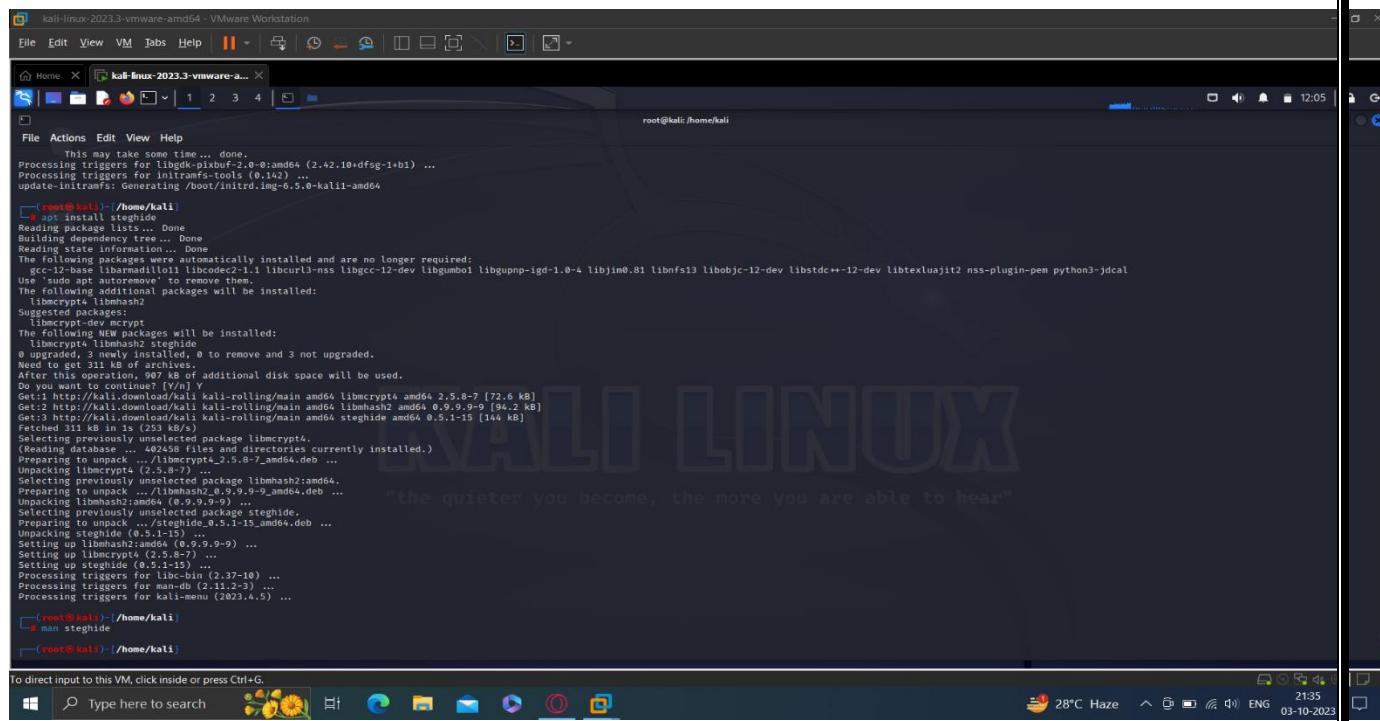
Aim : - Steganography Detection

Requirements :-

- VMware WorkStation Pro 17 Should be Installed
- In VMware WorkStation Virtual Machine of Kali Linux Should be Installed
As we are Going to Perform this on Kali Linux

Steps:-

1) Intsall Steghide Tool On Linux



The screenshot shows a terminal window titled "kali-linux-2023.3-vmware-amd64 - VMware Workstation". The terminal is running as root, indicated by the prompt "(root@kali:~)". The user is executing the command "apt install steghide". The output of the command shows the package manager processing dependencies, installing new packages like libmcrypt4 and libmhash2, and updating existing ones like libmcrypt4. The terminal also displays a watermark for "KALI LINUX" and the slogan "the quieter you become, the more you are able to hear".

```
This may take some time ... done.  
Processing triggers for libgdk-pixbuf2.0-0:amd64 (2.42.10+dfsg-1+b1) ...  
Processing triggers for initramfs-tools (0.142) ...  
update-initramfs: Generating /boot/initrd.img-6.5.0-kali1-amd64  
  
(root@kali:~/home/kali)  
# apt install steghide  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
The following packages were automatically installed and are no longer required:  
  gcc-12-base libarmadillo1 libcurl3-nss libgcc-12-dev libgumbo1 libgupnp-igd-1.0-4 libjemalloc1 libnfs13 libobjc-12-dev libstdc++-12-dev libtxluiajit2 nss-plugin-pem python3-jdcal  
Use 'sudo apt autoremove' to remove them.  
The following additional packages will be installed:  
  libmcrypt4 libmhash2  
Suggested packages:  
  libmcrypt4 libmhash2 steghide  
  0 upgraded, 0 newly installed, 0 to remove and 3 not upgraded.  
Need to get 311 kB of archives.  
After this operation, 907 kB of additional disk space will be used.  
Do you want to continue? [Y/n] Y  
Get:1 http://http://kali.download/kali kali-rolling/main amd64 libmcrypt4 amd64 2.5.8-7 [72.6 kB]  
Get:2 http://http://kali.download/kali kali-rolling/main amd64 libmhash2 amd64 0.9.9.9-9 [94.2 kB]  
Get:3 http://http://kali.download/kali kali-rolling/main amd64 steghide amd64 0.5.1-15 [144 kB]  
Fetched 311 kB in 1s (253 kB/s)  
Setting up libmcrypt4 (2.5.8-7) ...  
Setting up libmhash2:amd64 (0.9.9.9-9) ...  
Unpacking libmcrypt4 (2.5.8-7) ...  
Selecting previously unpacked package libmhash2:amd64.  
Preparing to unpack .../libmhash2_0.9.9.9-9_amd64.deb ...  
Unpacking libmhash2:amd64 (0.9.9.9-9) ...  
Selecting previously unselected package steghide.  
Preparing to unpack .../steghide_0.5.1-15_amd64.deb ...  
Unpacking steghide (0.5.1-15) ...  
Setting up libmhash2:amd64 (0.9.9.9-9) ...  
Setting up libmcrypt4 (2.5.8-7) ...  
Setting up libmhash2:amd64 (0.9.9.9-9) ...  
Processing triggers for libc-bin (2.37-10) ...  
Processing triggers for man-db (2.11.2-3) ...  
Processing triggers for kali-menu (2023.4.5) ...  
  
(root@kali:~/home/kali)  
# man steghide  
# (root@kali:~/home/kali)
```

Command :- apt Install Steghide

2) Now After Installing Steghide Give Command ‘steghide -- help’ This will display all the Commands Used in this Tool



```

root@kali:~/home/kali
steghide version 0.5.1

The first argument must be one of the following:
embed, --embed      embed data
extract, --extract  extract data
info, --info        display information about a cover- or stego-file
info <filename>   display information about <filename>
encinfo, --encinfo  display a list of supported encryption algorithms
version, --version   display version information
license, --license   display steghide's license
help, --help        display this usage information

embedding options:
-eF, --embedfile    select file to be embedded
-eF <filename>     embed the file <filename>
-cF, --coverfile    select cover-file
-cF <filename>     embed into the file <filename>
-p, --passphrase    specify passphrase
-p <passphrase>    use <passphrase> to embed data
-sf, --stegofile    select stego file
-sf <filename>     write result to <filename> instead of cover-file
-e, --encryption    select encryption parameters
-e <a>[<b>]<c>[<d>]<e>[<f>]  specify an encryption algorithm and/or mode
-e none            do not encrypt data before embedding
-z, --compress      compress data before embedding (default)
-z <n>              compress data (<n> = 1 for best compression)
-Z, --dontcompress  do not compress data before embedding
-K, --nochecksum    do not embed crc32 checksum of embedded data
-N, --dontembedname do not embed the name of the original file
-f, --force         overwrite existing files
-q, --quiet         suppress information messages
-v, --verbose       display detailed information

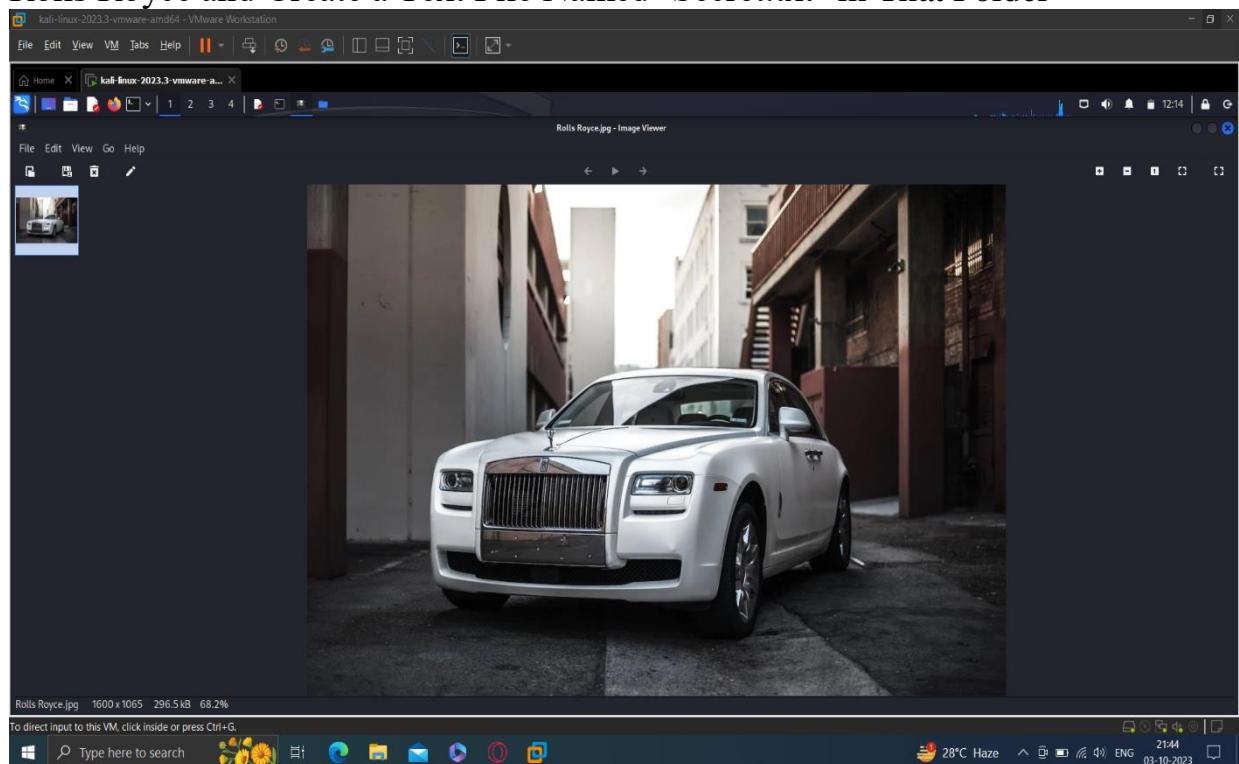
extracting options:
-sf, --stegofile    select stego file
-sf <filename>     extract data from <filename>
-p, --passphrase    specify passphrase
-p <passphrase>    use <passphrase> to extract data
-xF, --extractfile  select file to extract data
-xF <filename>     write the extracted data to <filename>
-f, --force         overwrite existing files
-q, --quiet         suppress information messages
-v, --verbose       display detailed information

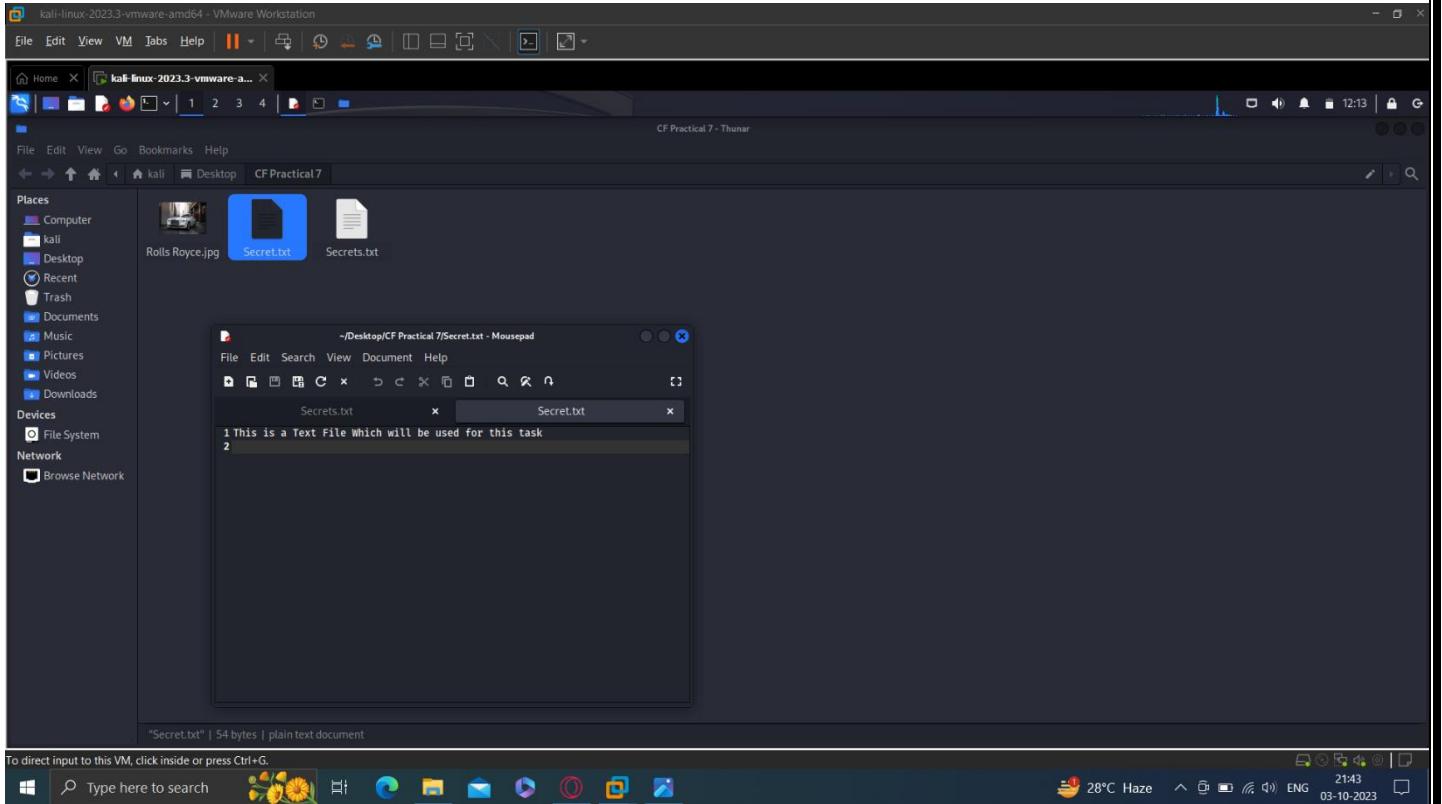
options for the info command:
-p, --passphrase    specify passphrase

```

To direct input to this VM, click inside or press Ctrl+G.

- 3) Now Create a Folder named ‘CF Practical 7’ On Desktop and Download A Image of Rolls Royce and Create a Text File Named ‘Secret.txt’ in That Folder





4) Now Hide the Text in secret.txt file in Rolls Royce image

```
(root㉿kali)-[~/home/kali]
# steghide embed -ef '/home/kali/Desktop/CF Practical 7/Secret.txt' -cf '/home/kali/Desktop/CF Practical 7/Rolls Royce.jpg' -p abcd1234
embedding "/home/kali/Desktop/CF Practical 7/Secret.txt" in "/home/kali/Desktop/CF Practical 7/Rolls Royce.jpg" ... done
```

To Do this use the above command

Here -ef means embed File which is the File to be Embedded i.e the txt file from which we want to hide the text in the Image and -cf means cover file i.e the file in which we want to hide the text

5) Now Extract the hidden text in the Rolls Royce Image

```
(root㉿kali)-[~/home/kali]
# steghide extract -sf '/home/kali/Desktop/CF Practical 7/Rolls Royce.jpg' -p abcd1234 -xf '/home/kali/Desktop/CF Practical 7/Secrets.txt'.
wrote extracted data to "/home/kali/Desktop/CF Practical 7/Secrets.txt".
```

To do this use Above Command

Here -sf Means Stego File i.e the File From which we want to extract the Hidden data and -xf means extractfile i.e the File in which the Hidden Data Will be Extracted

