

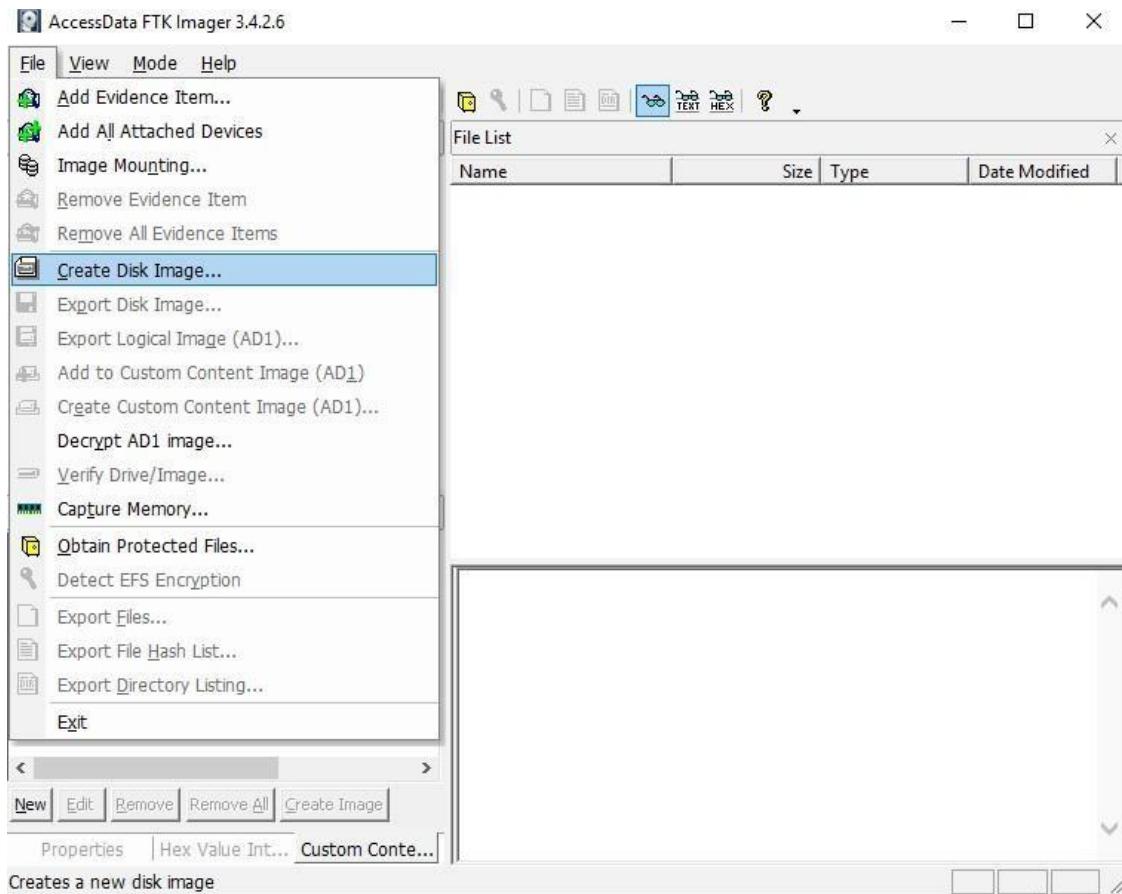
## **PRACTICAL 1**

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

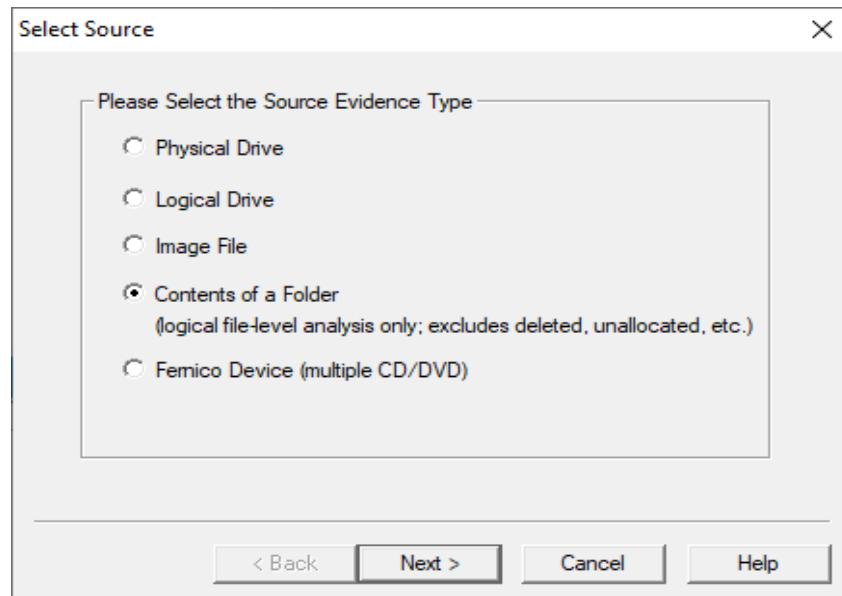
- Creating Forensic Image
- Check Integrity of Data
- Analyze Forensic Image

### ➤ Creating Forensic Image

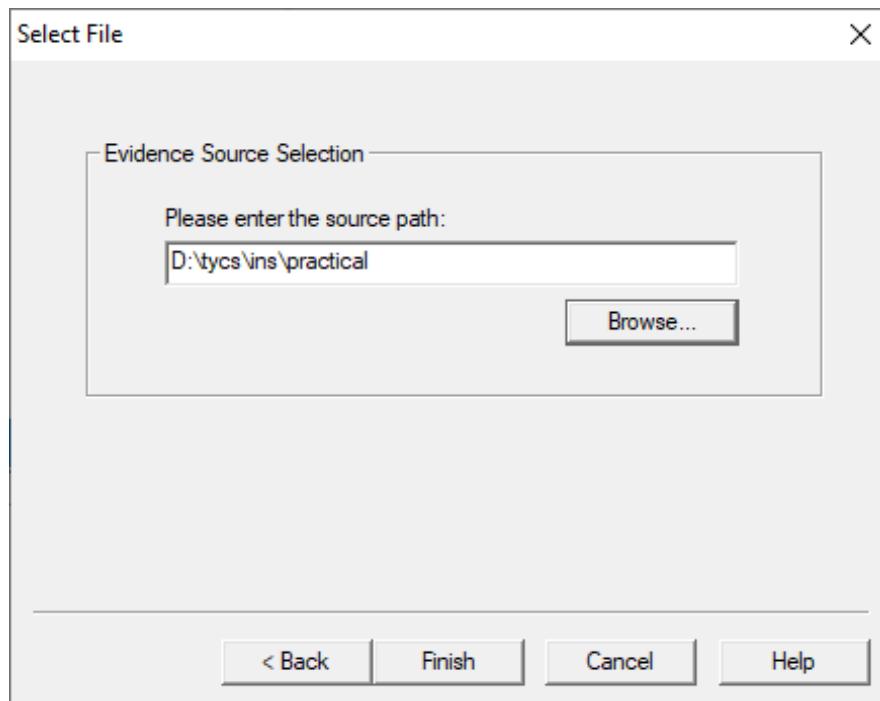
1. Click File, and then Create Disk Image, or click the button on the tool bar.



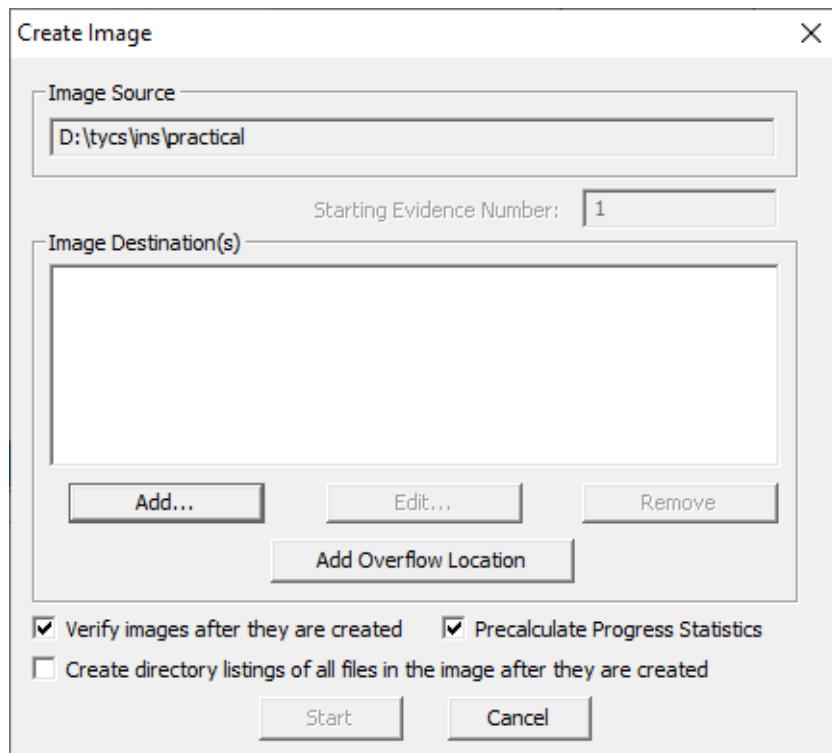
2. Select the source evidence type you want to make an image of and click Next.



3. Select the source evidence file with path.



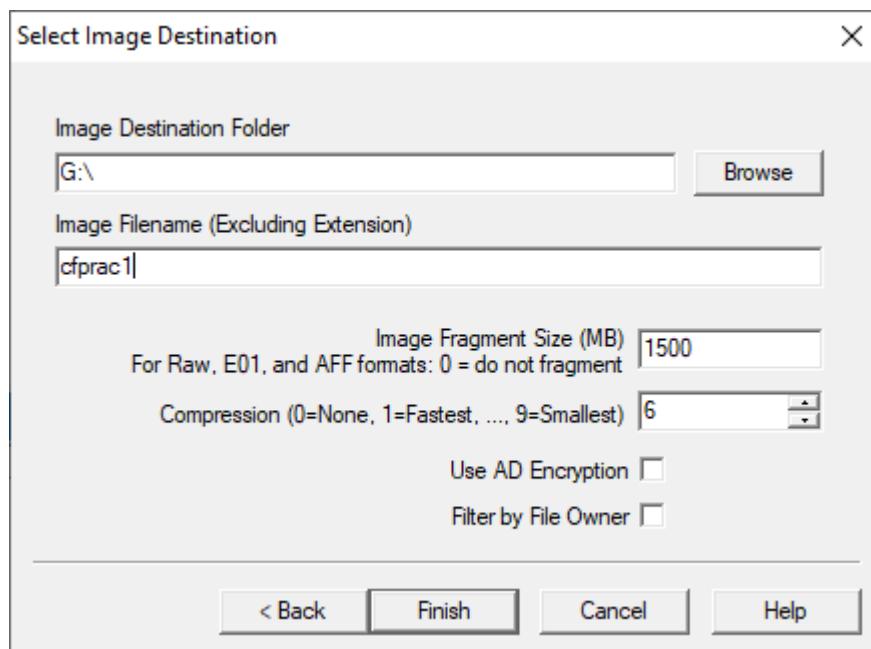
Click on “add” to add image destination



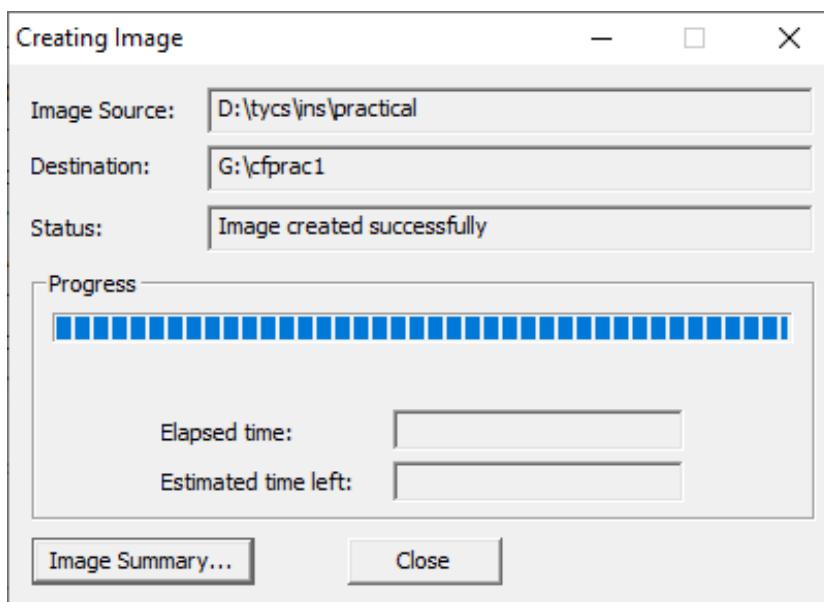
The 'Evidence Item Information' dialog box is shown. It contains fields for 'Case Number' (1), 'Evidence Number' (1), 'Unique Description' (prac1), 'Examiner' (empty), and 'Notes' (empty). At the bottom are buttons for '< Back', 'Next >', 'Cancel', and 'Help'.

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.

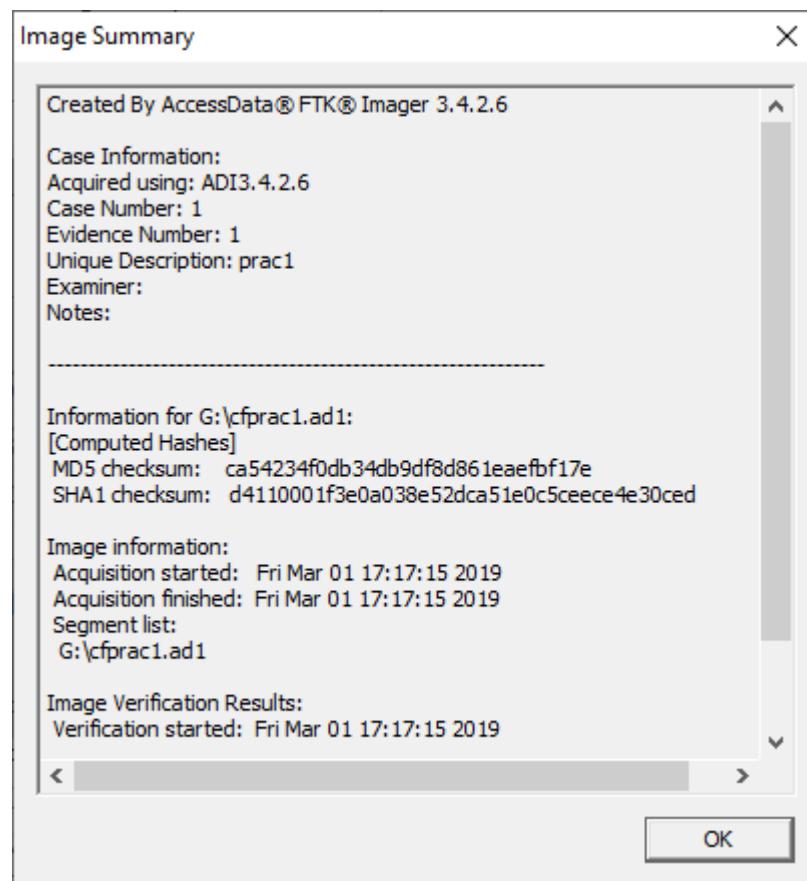
**Note:** If the destination folder you select is on a drive that does not have sufficient free space to store the entire image file, FTK Imager prompts for a new destination folder when all available space has been used in the first location. In the Image Filename field, specify a name for the image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



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

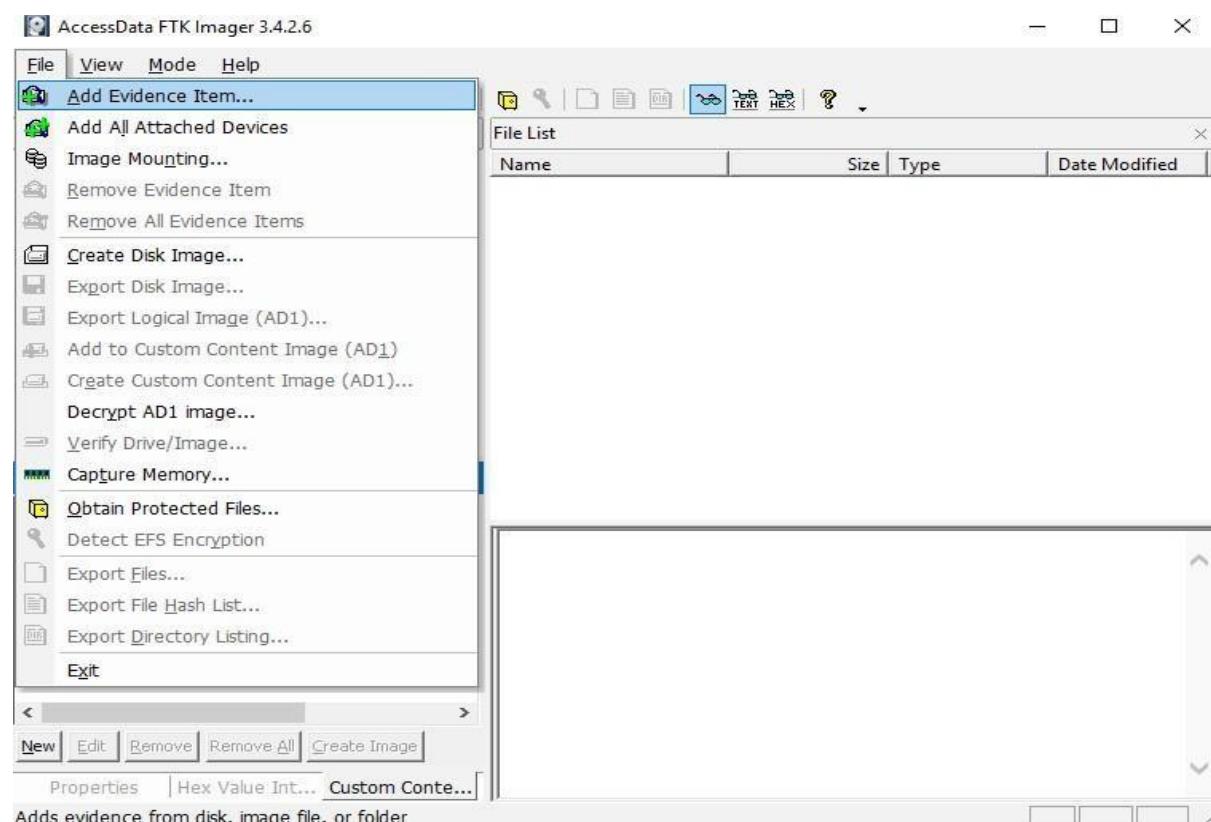


6. After the images are successfully created, click Image Summary to view detailed file information, including MD5 and SHA1 checksums.

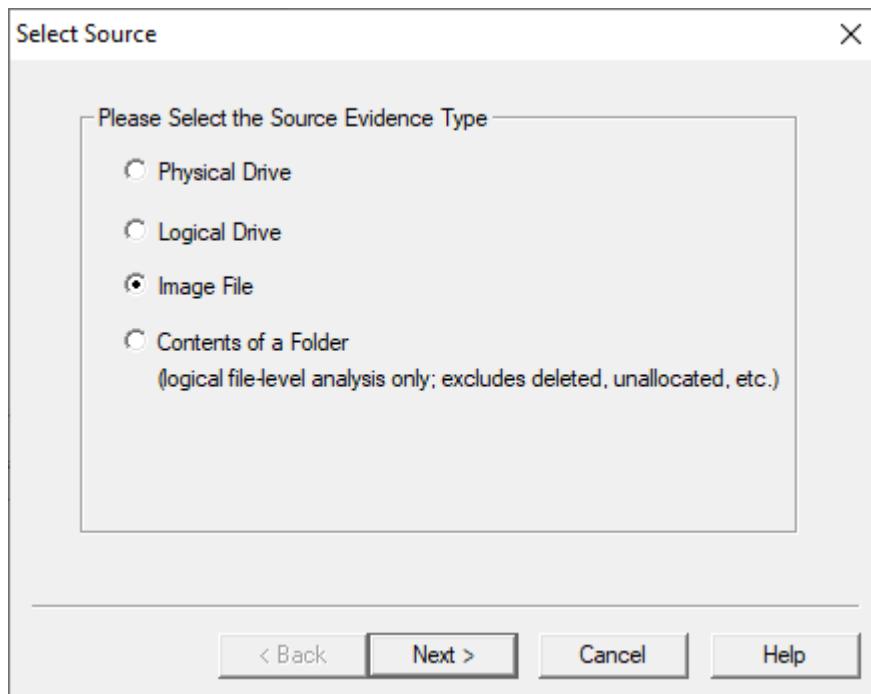


## Analyze Forensic Image:

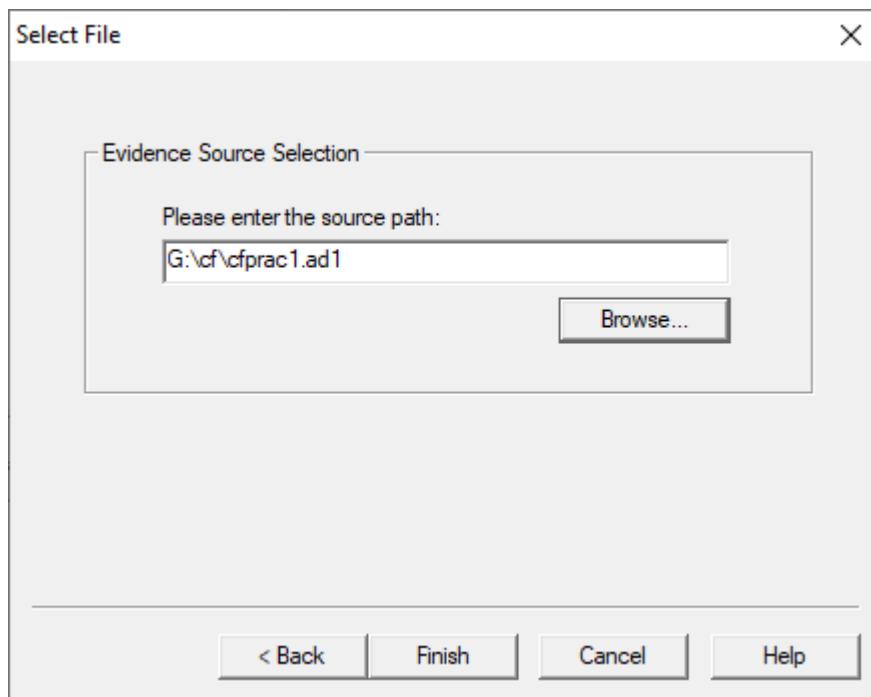
Click on Add Evidence Item to add evidence from disk, image file or folder.



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: cfprac1.ad1, which contains 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 such as 1 (Regular File, 0 bytes, 12-09-2018), CaesarCipherProgram.... (Regular File, 2 bytes, 12-09-2018), CaesarCipherProgram.... (Regular File, 1 byte, 12-09-2018), INSfinaldocument.docx (Regular File, 241 bytes, 23-09-2018), MD5Hash.class (Regular File, 2 bytes, 23-09-2018), MD5Hash.java (Regular File, 1 byte, 23-09-2018), RSA.class (Regular File, 2 bytes, 12-09-2018), and RSA.java (Regular File, 2 bytes, 12-09-2018). Below these panes is the Custom Content Sources pane, which lists Evidence: File System | Path | File and provides options for New, Edit, Remove, Remove All, and Create Image. At the bottom, there are tabs for Properties, Hex Value Int..., Custom Conte..., and a note to press F1 for the User Guide. A status bar at the bottom indicates Cursor pos = 0.

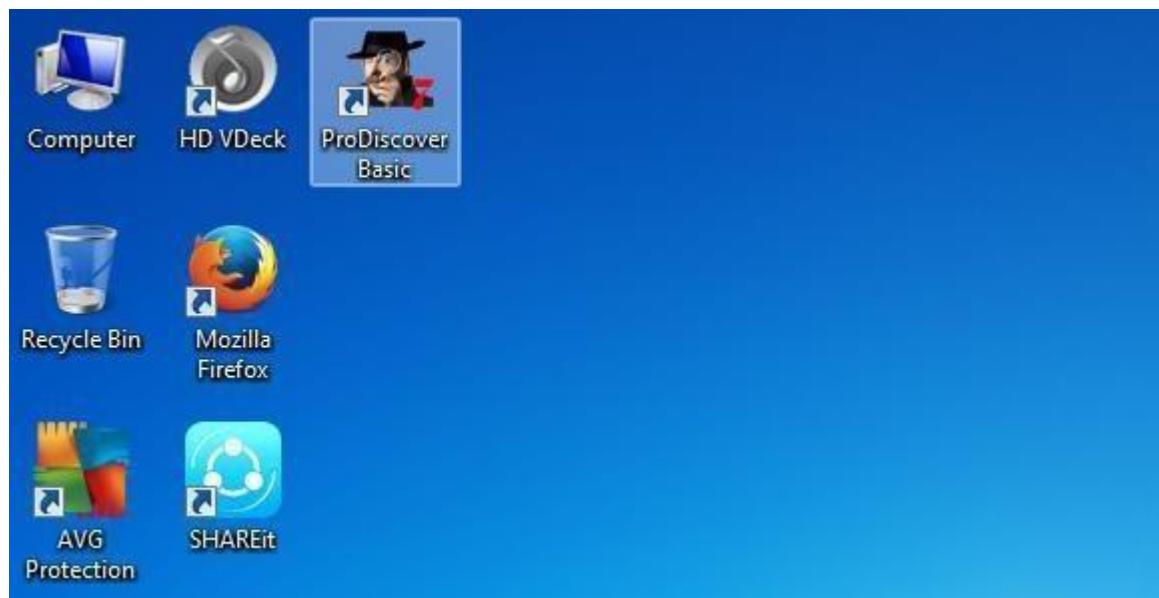
## PRACTICAL 2

Aim: Data Acquisition:

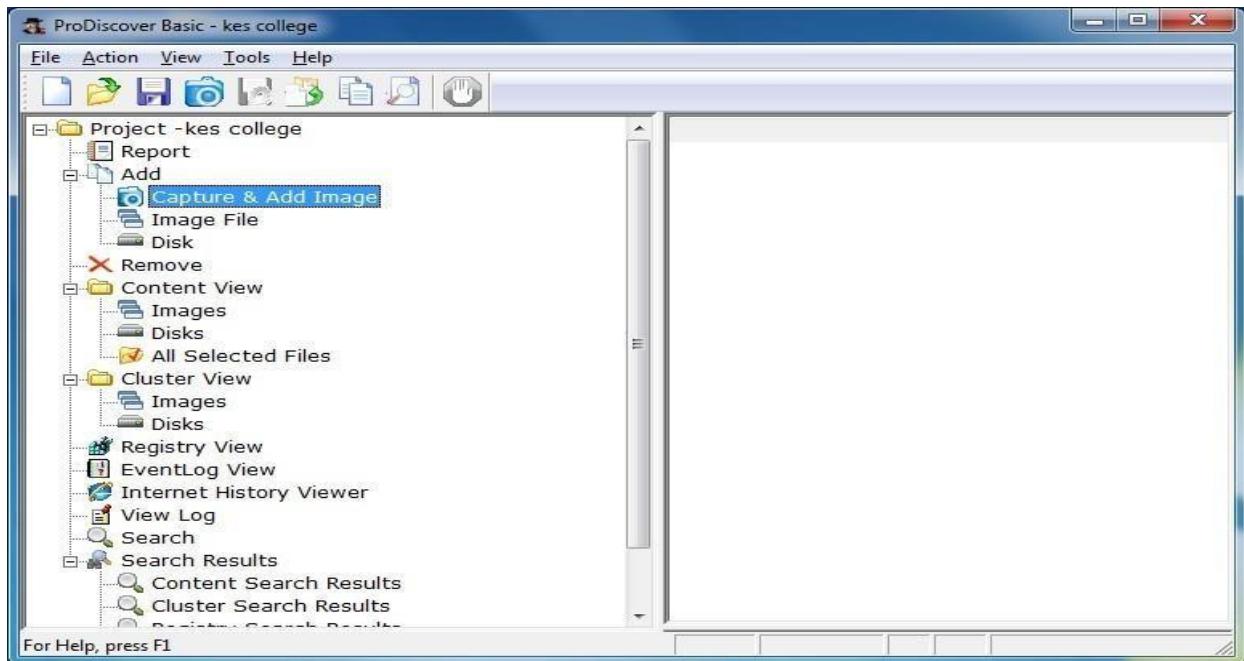
- Perform data acquisition using:
- USB Write Blocker + FTK Imager

Steps:

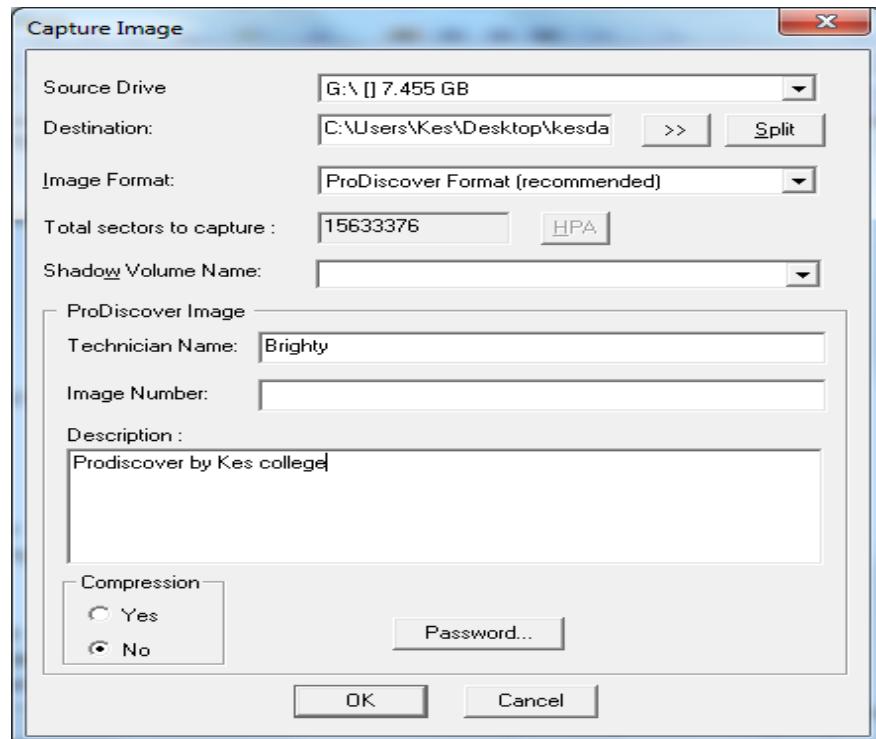
Step 1: First Open Prodiscover Basic and start with new case.



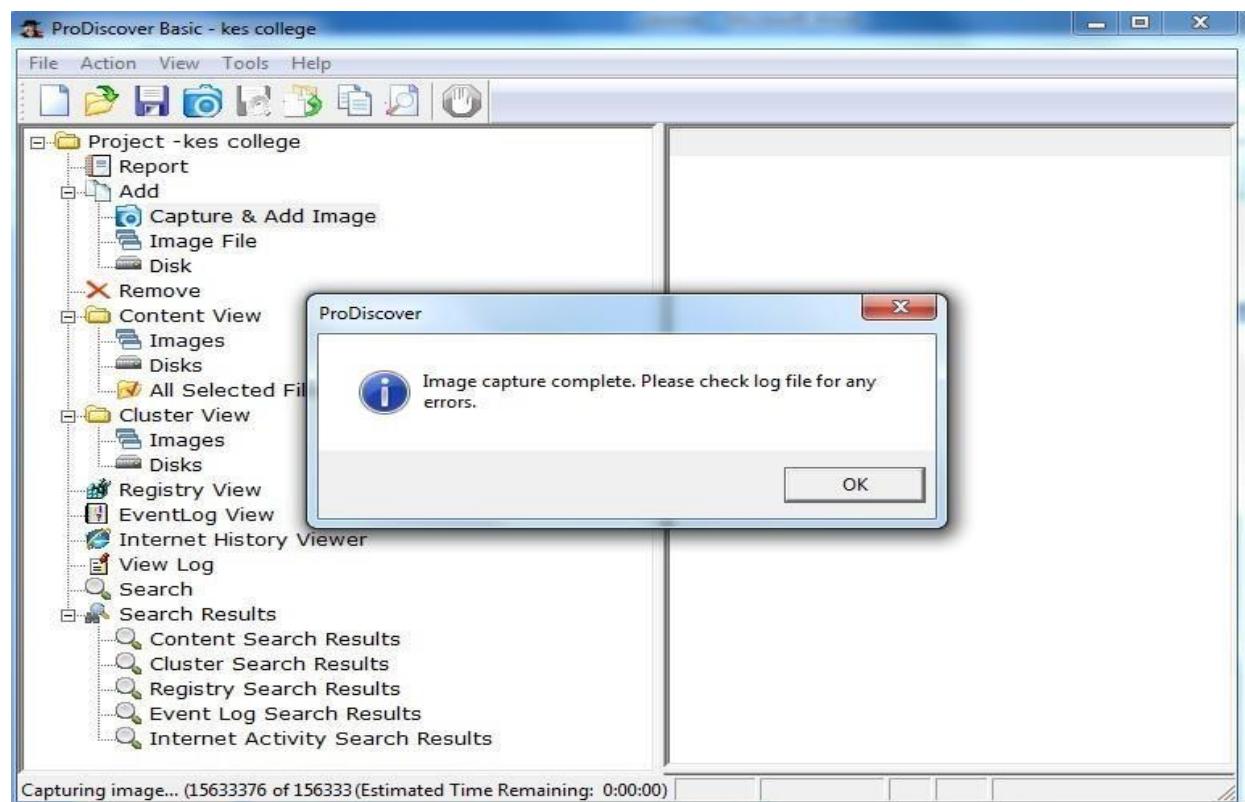
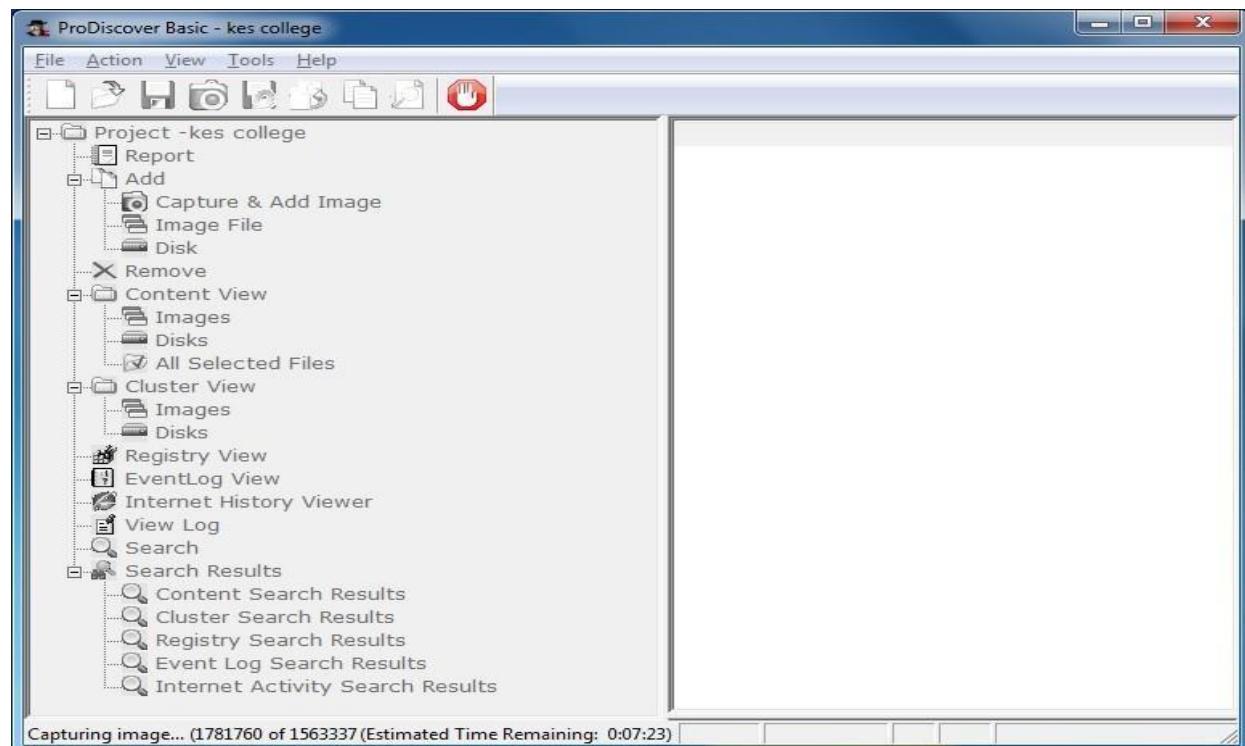
Step 2: The created project appears in left pane and select add>capture & add image.



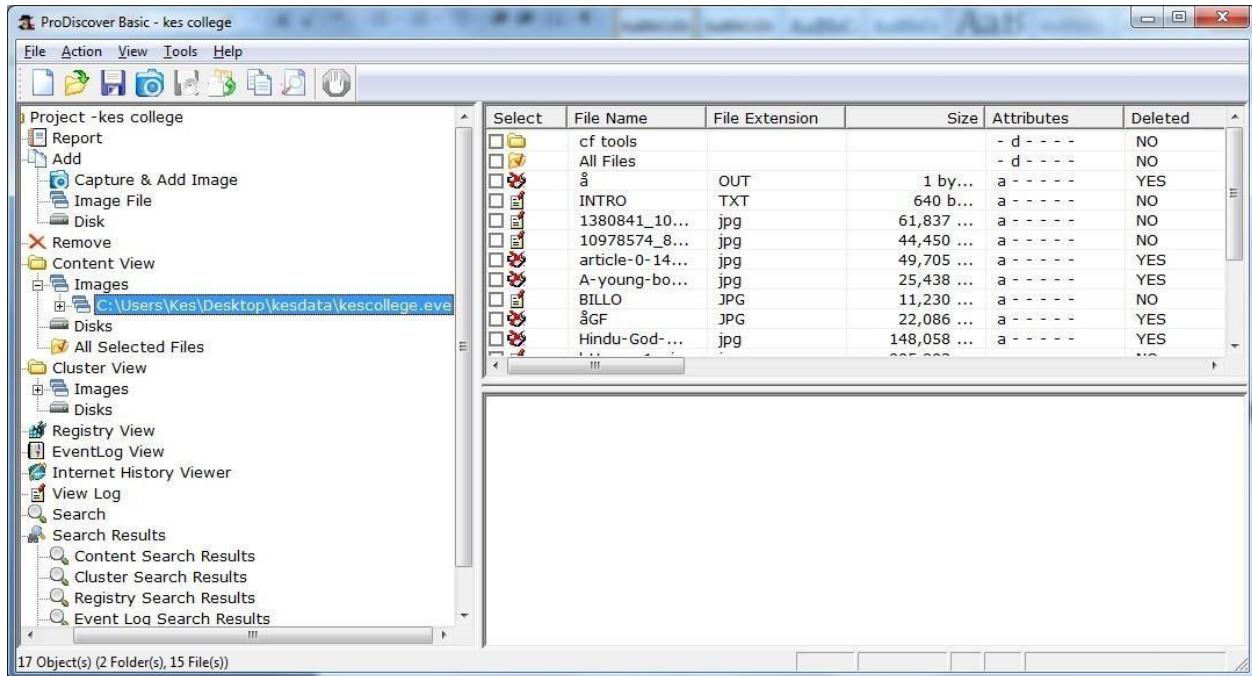
Step 3: fill the details as below. And click ok.



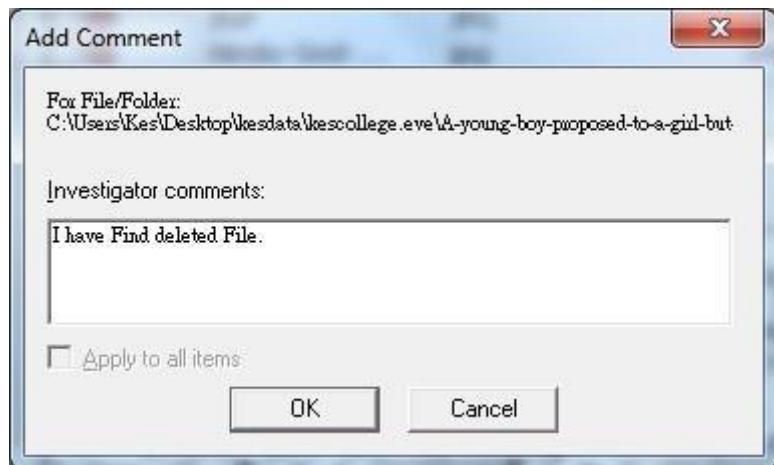
## Step 4: capturing of image starts.



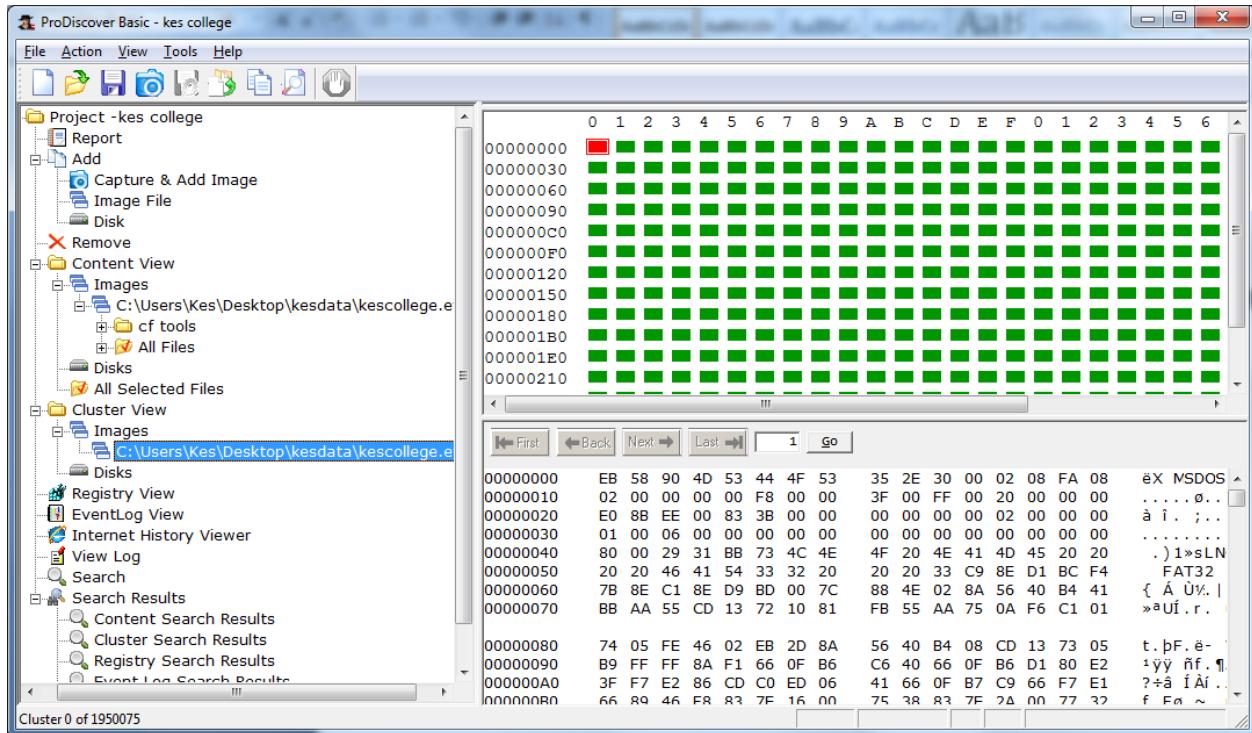
Step 5: Open the image created, go to Add > Images in left pane.



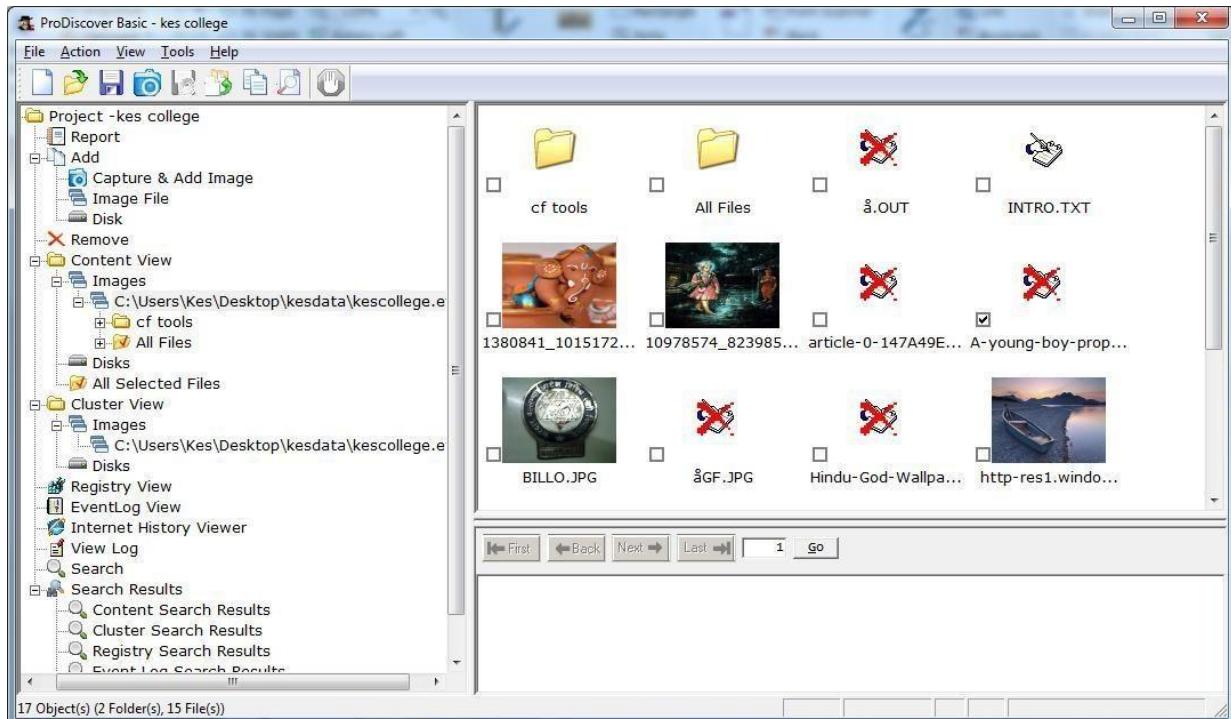
Step 6: Click on any File and type a comment.



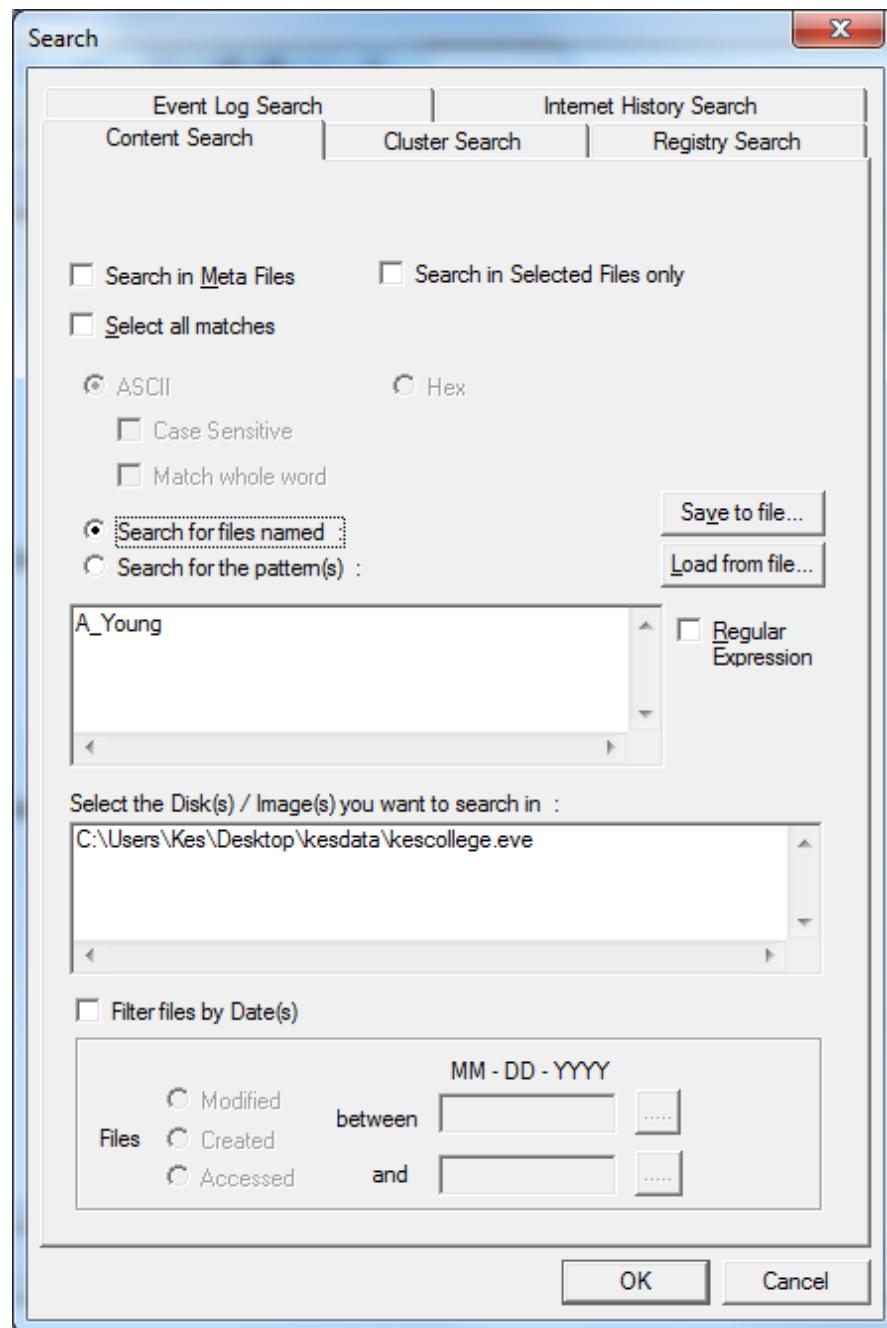
Step 7 : the cluster view is seen from the cluster view in left panel.



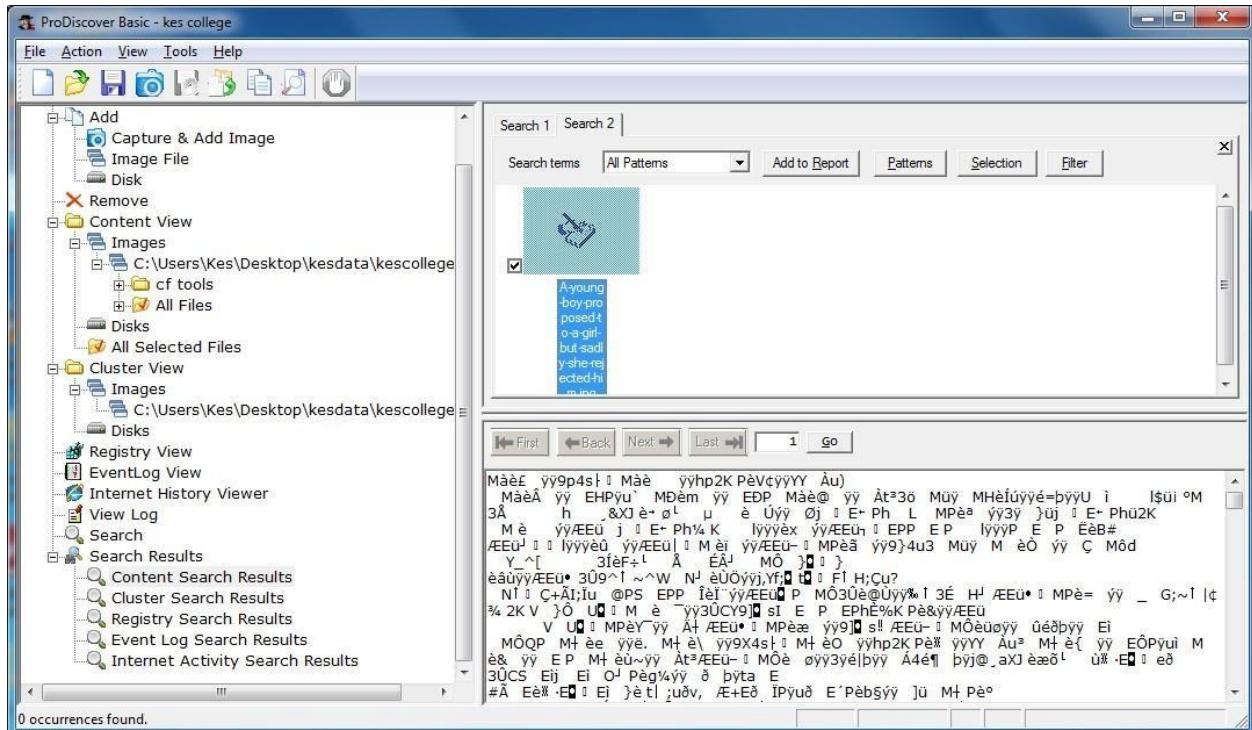
Step 8 : We can also view gallery view by Right Click.



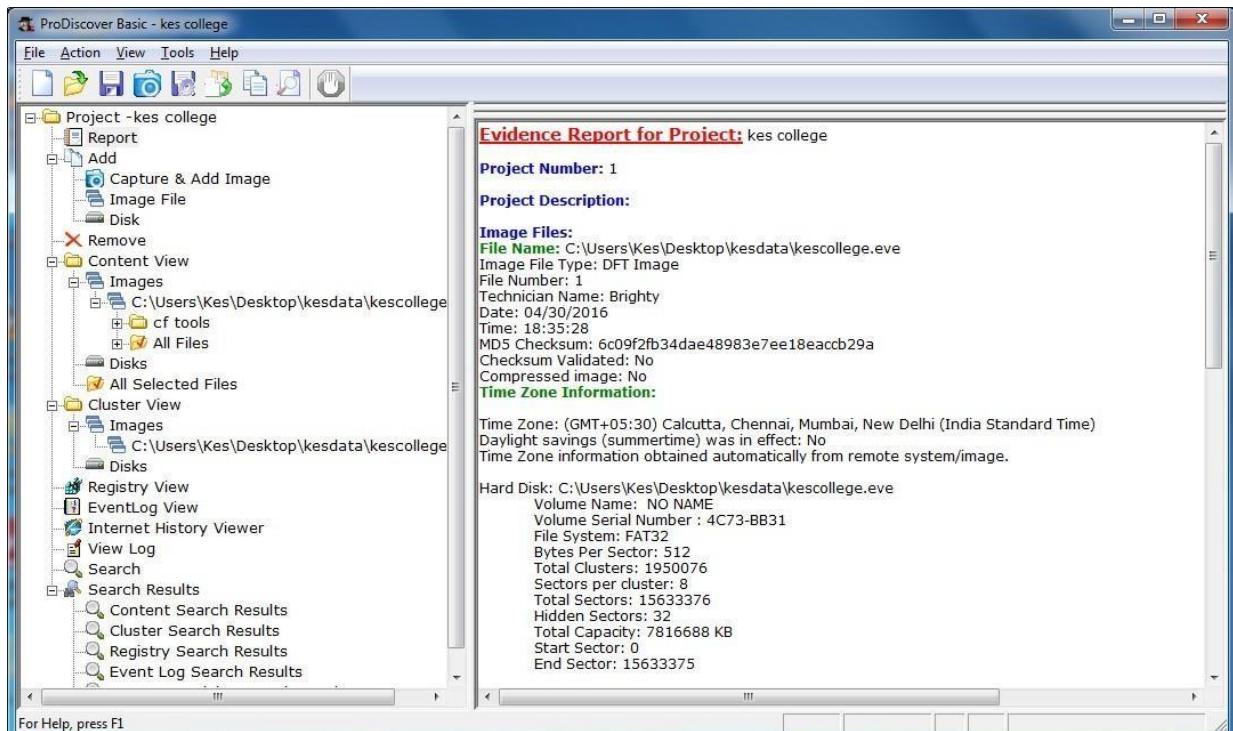
Step 9: Keyword search. Click on Search in left pane and Enter the file name to be searched in the image created.

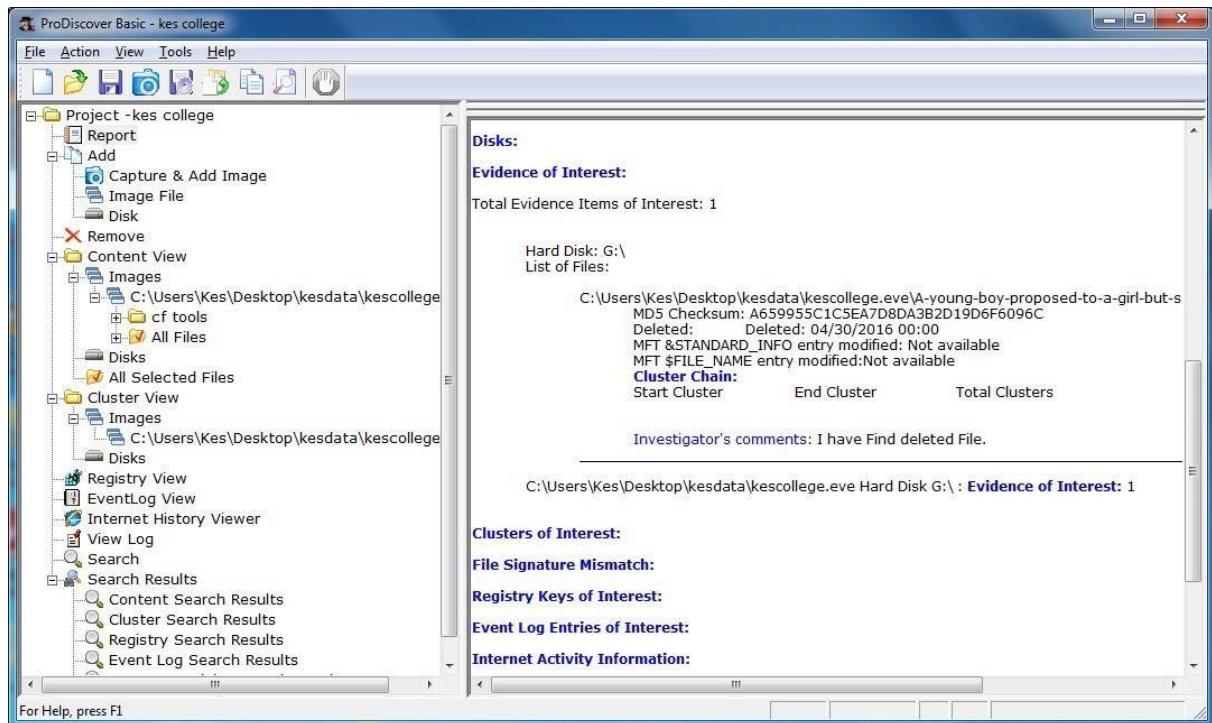


## Step 10 : Output of Keyword search.



## Step 11 : Click on View>Report.





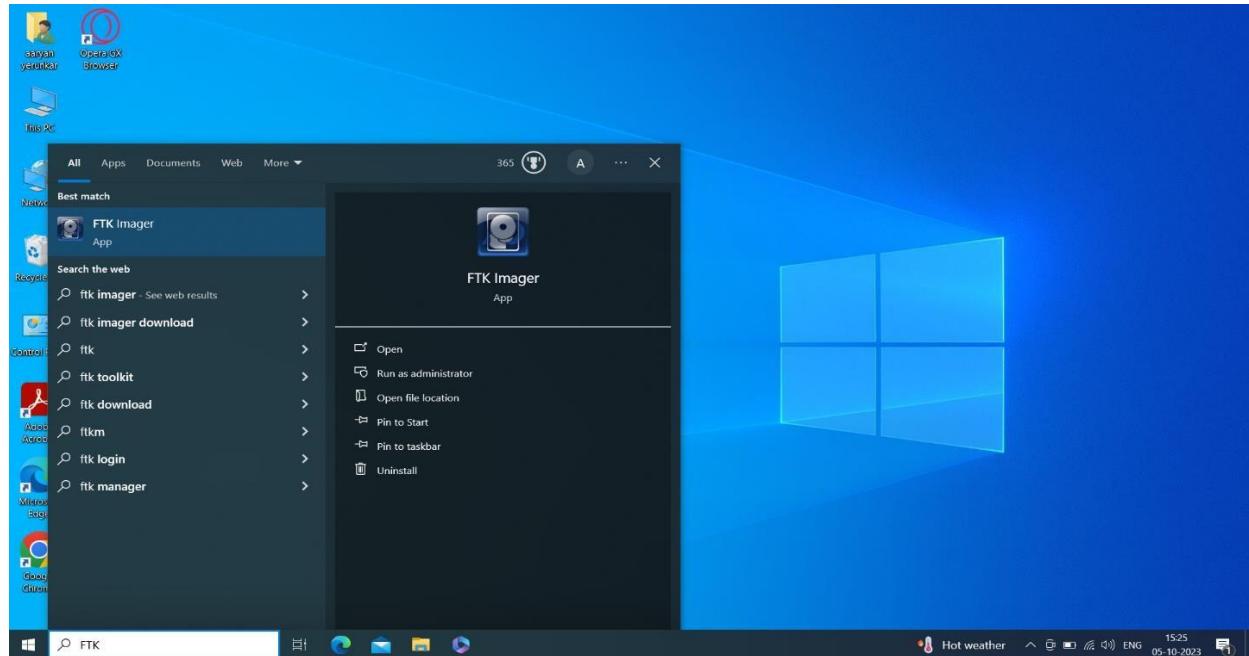
## PRACTICAL 3

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

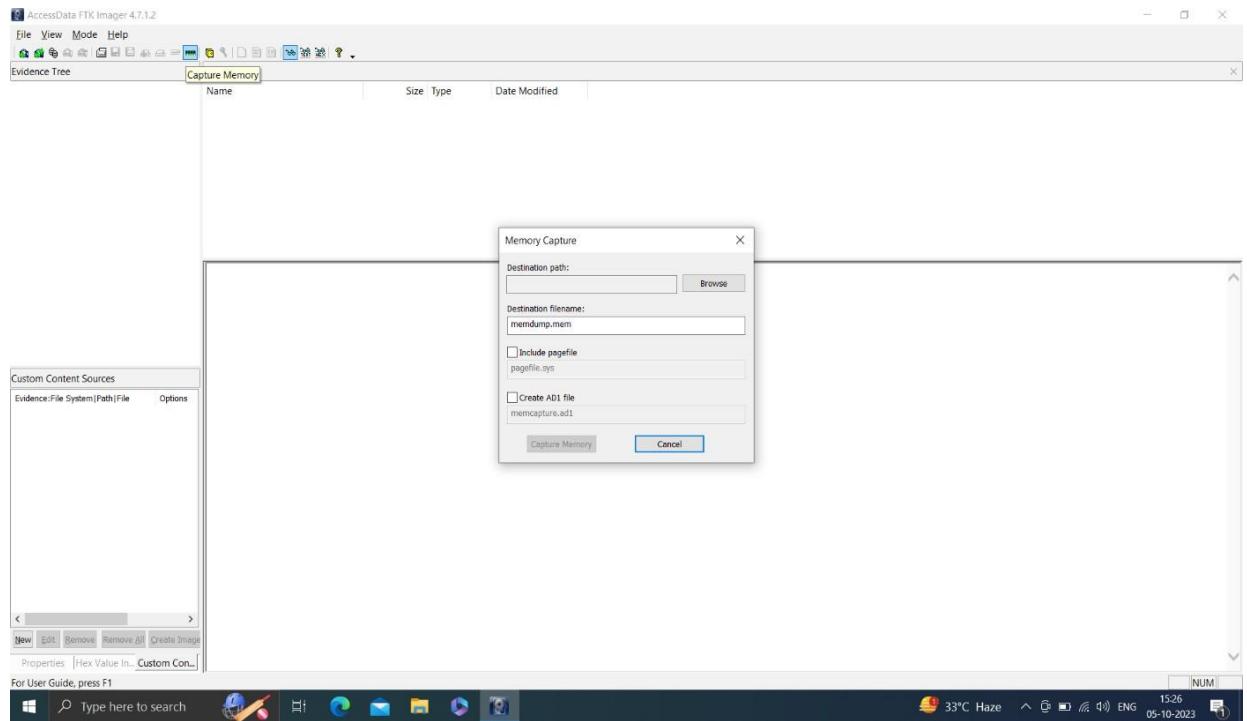
- Capture The Memory Dump By Using AccessData FTK Imager
- Analyze The Memory Dump (.MEM File)

**Steps:-**

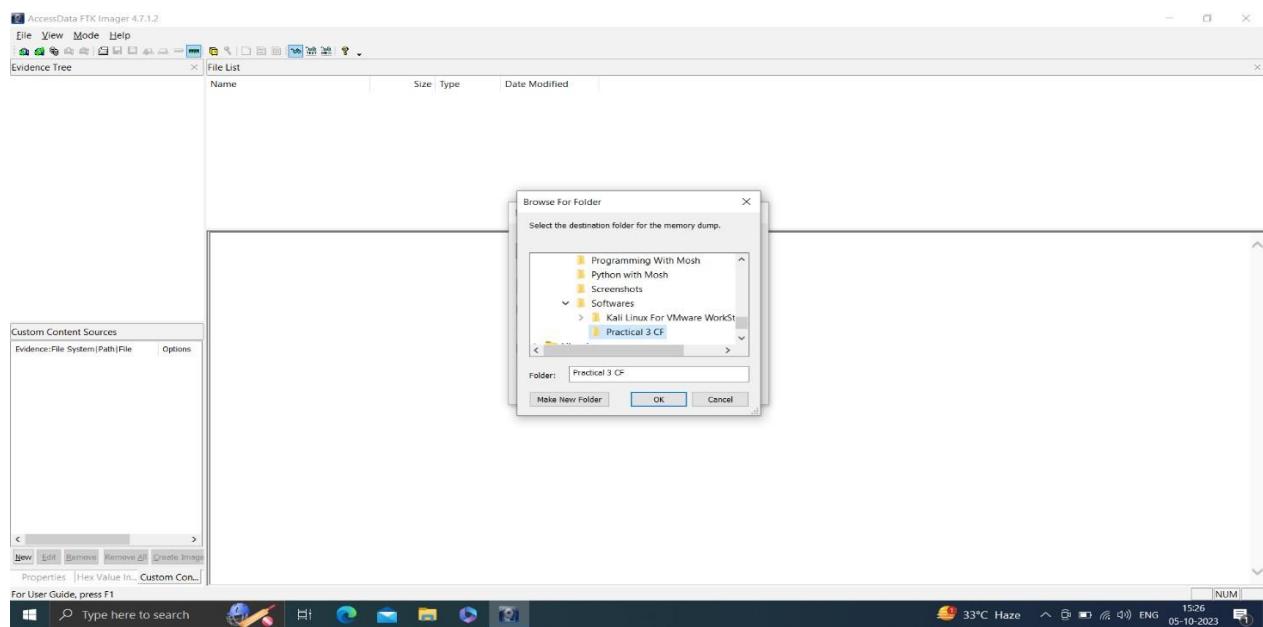
1) On Your Computer Open AccessData FTK Imager



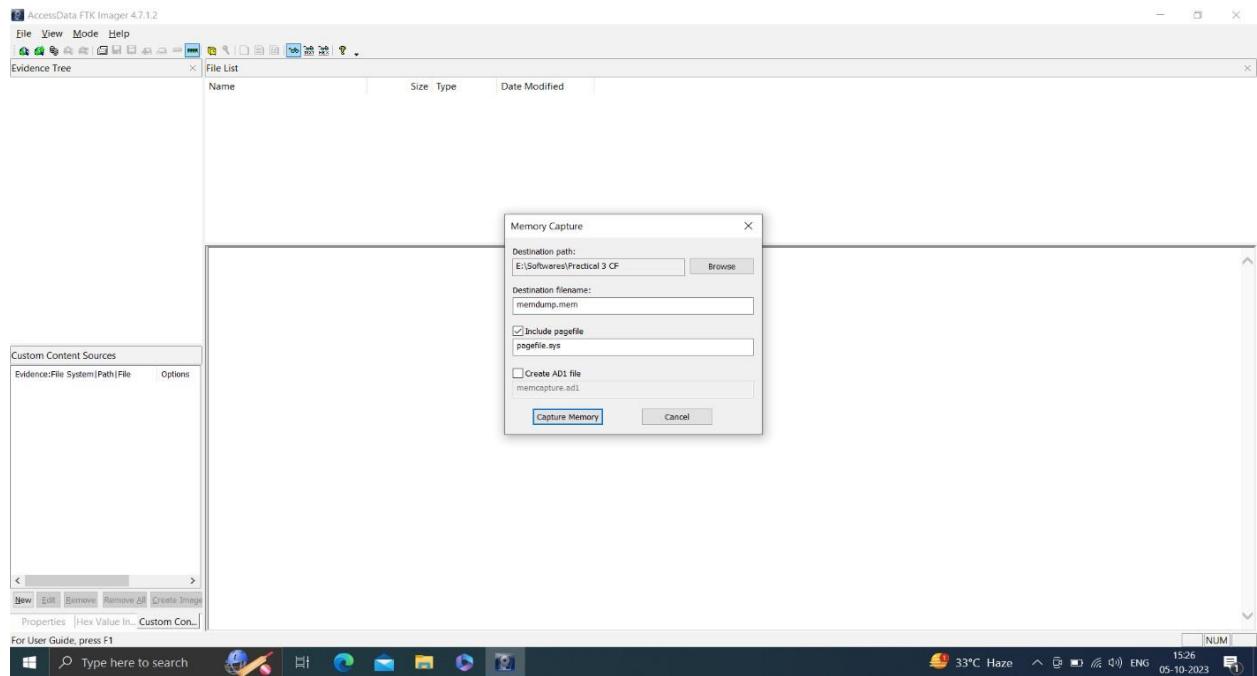
## 2) Now To Capture Memory Dump Click on ‘Capture Memory’ Icon



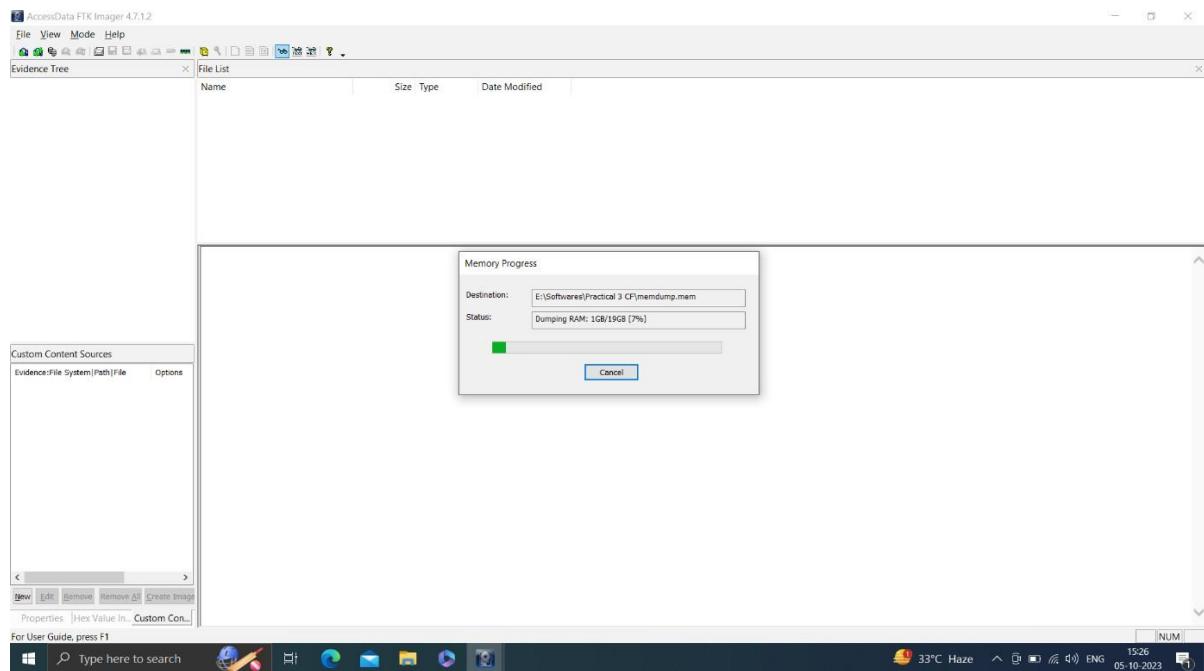
## 3) Browse The Destination Path



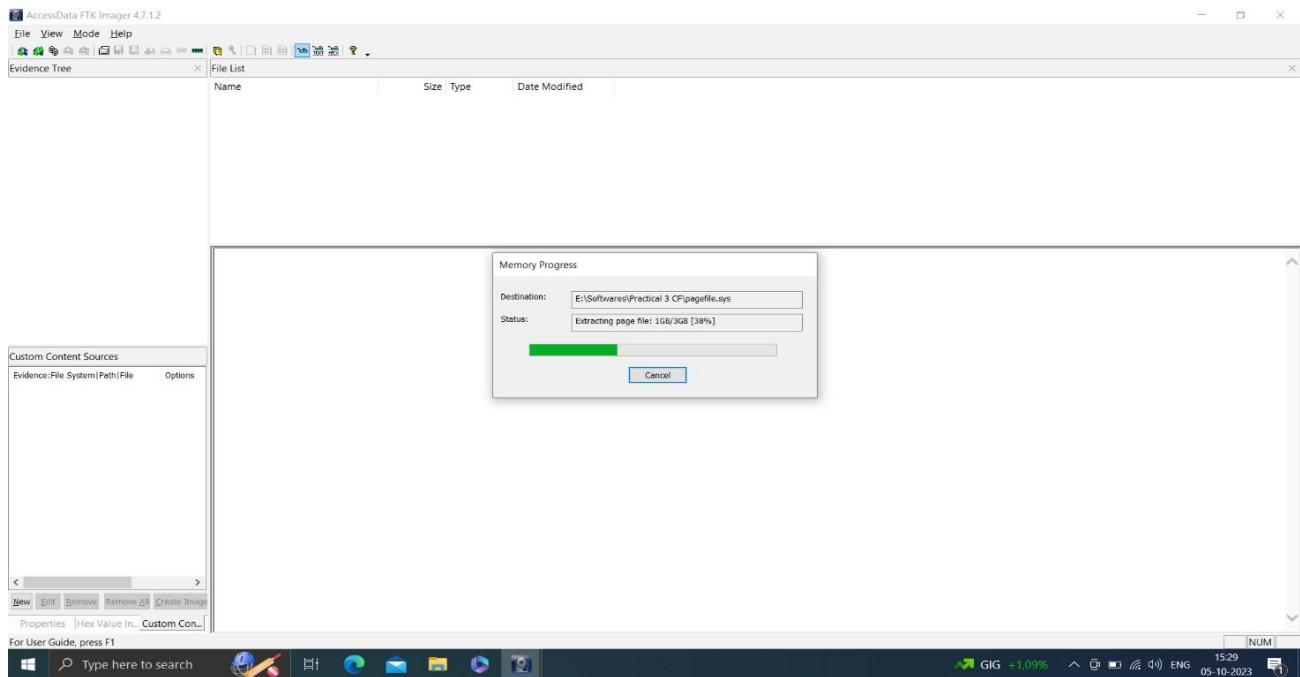
4) Now Click on ‘Include Page File’



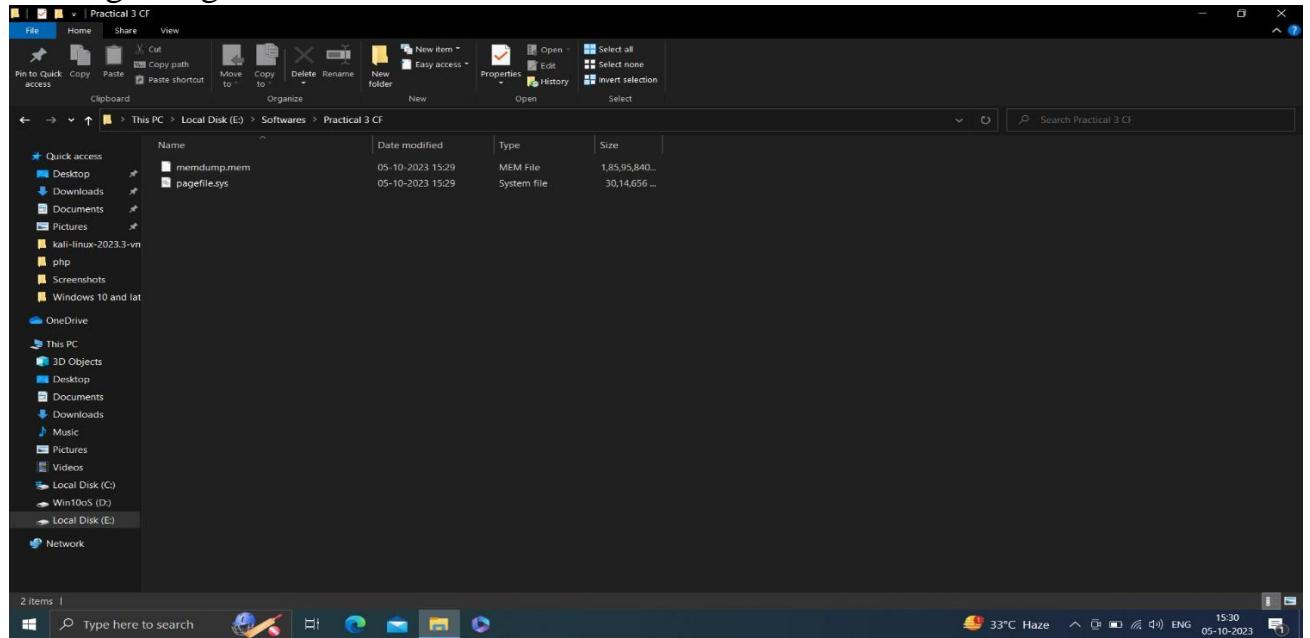
5) Click on Capture Memory to Capture the Memory Dump



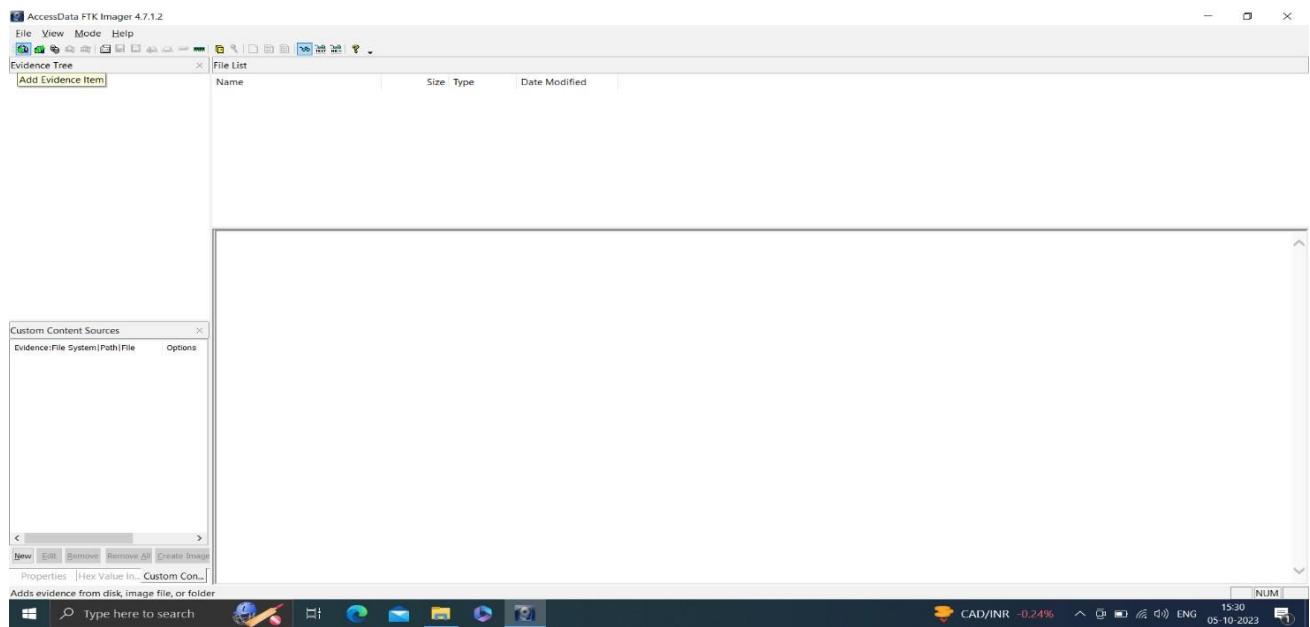
## It will Also Extract Page File



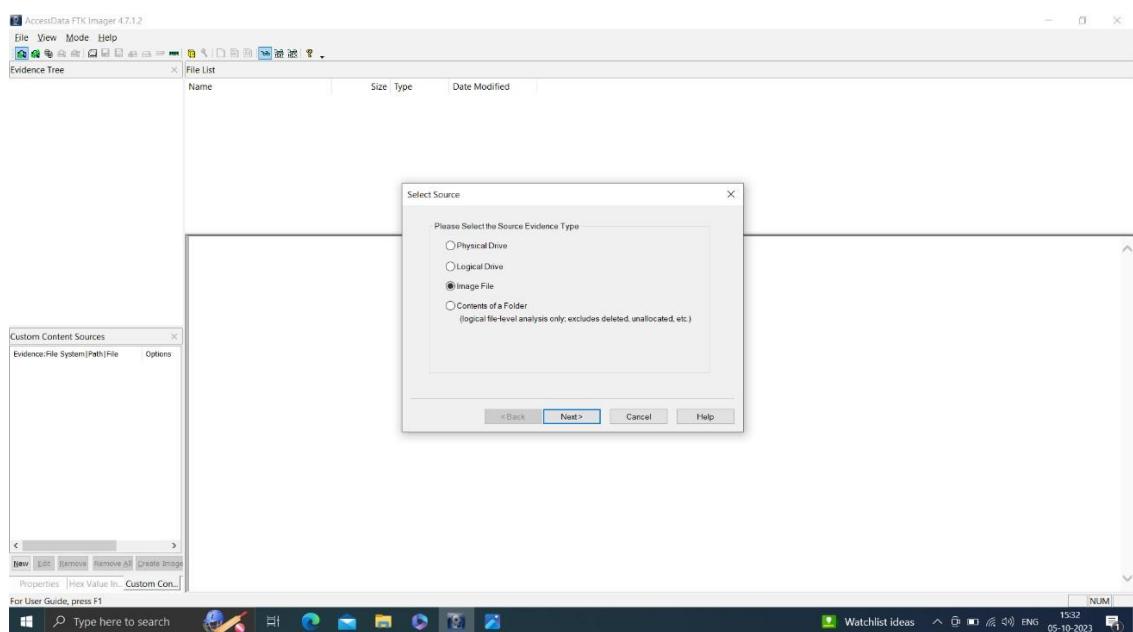
- 6) So After That The Files Will be Displayed In Destination Folder Which You Selected at the Beginning



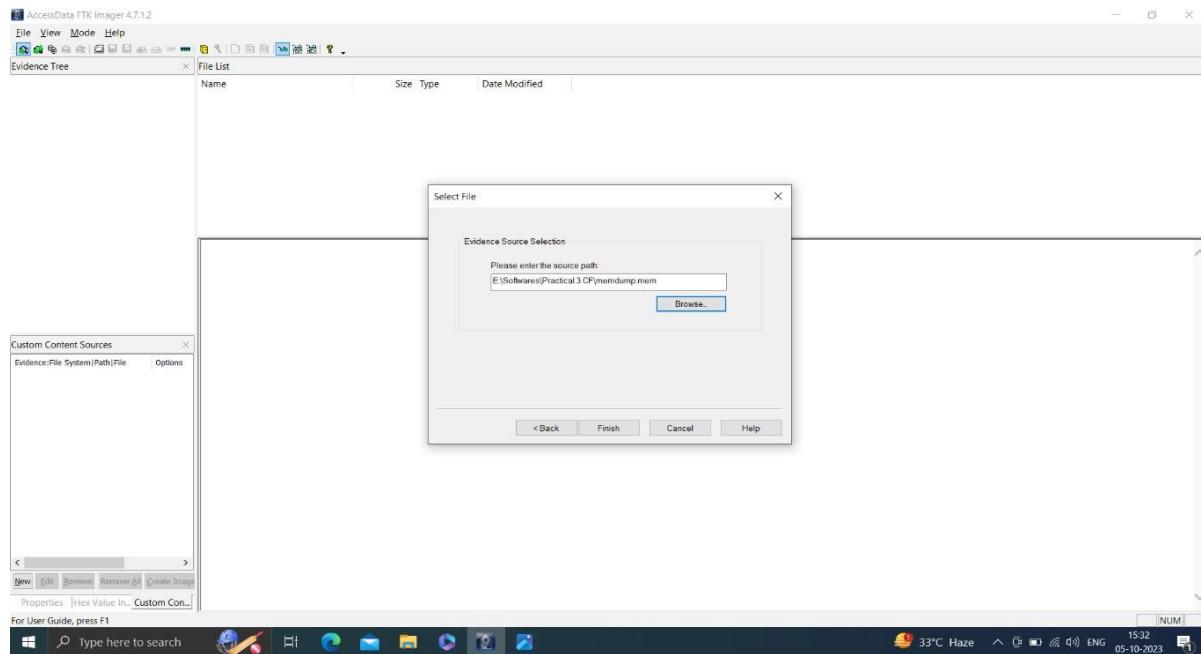
7) Now To Analyze The Memory Dump Click on ‘Add Evidence Item’ Icon



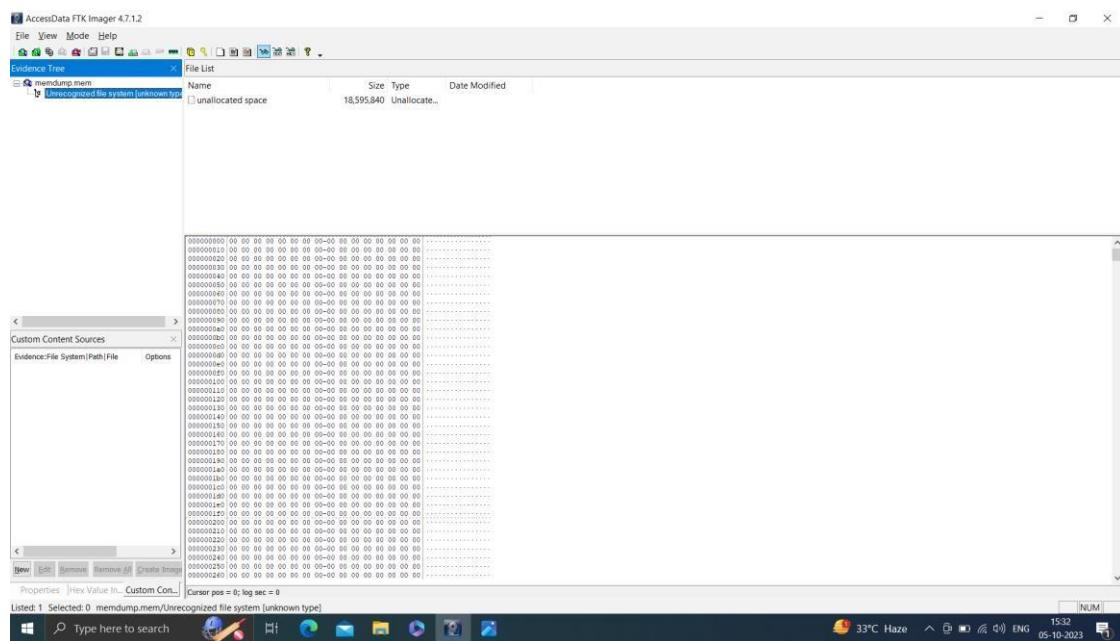
8) Select Source Type ‘Image File’ as Shown In Below Image



## 9) Browse the Source Path where The Evidence is Stored



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



## PRACTICAL 4

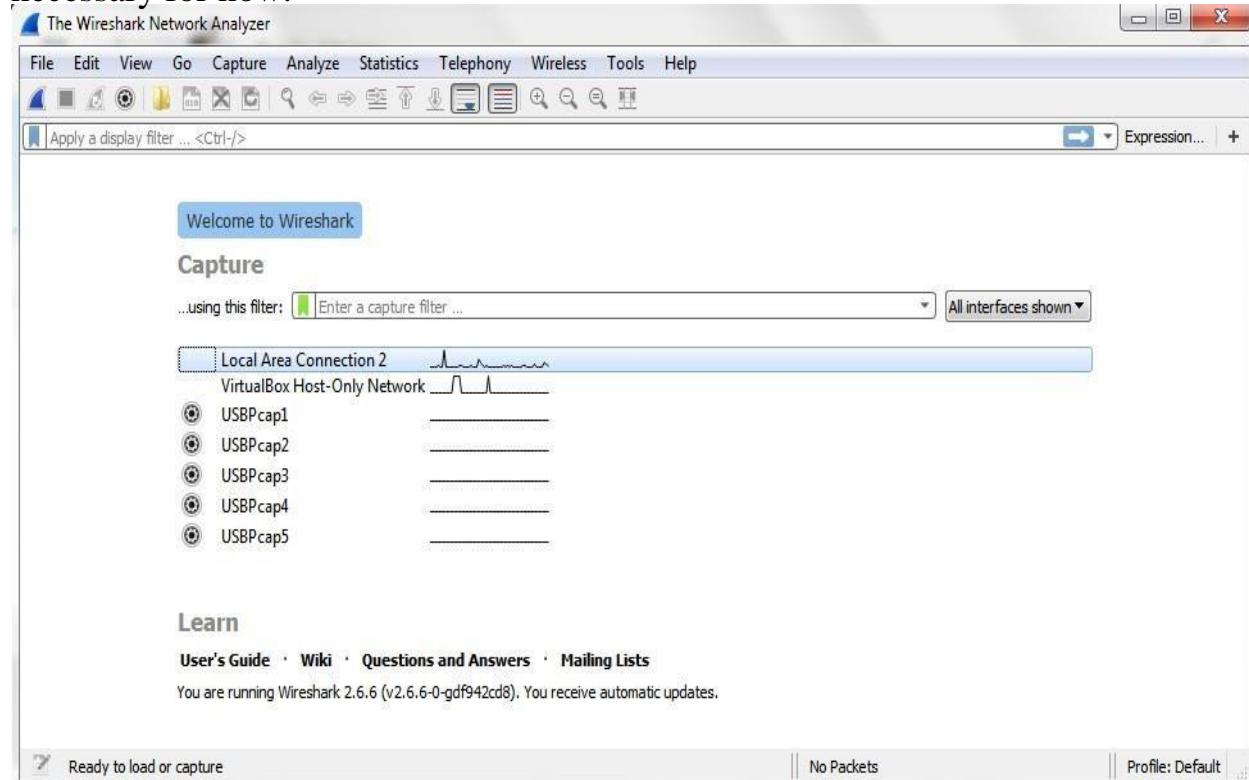
AIM : Capturing and analyzing network packets using Wireshark (Fundamentals) :

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

### Capturing Packets

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

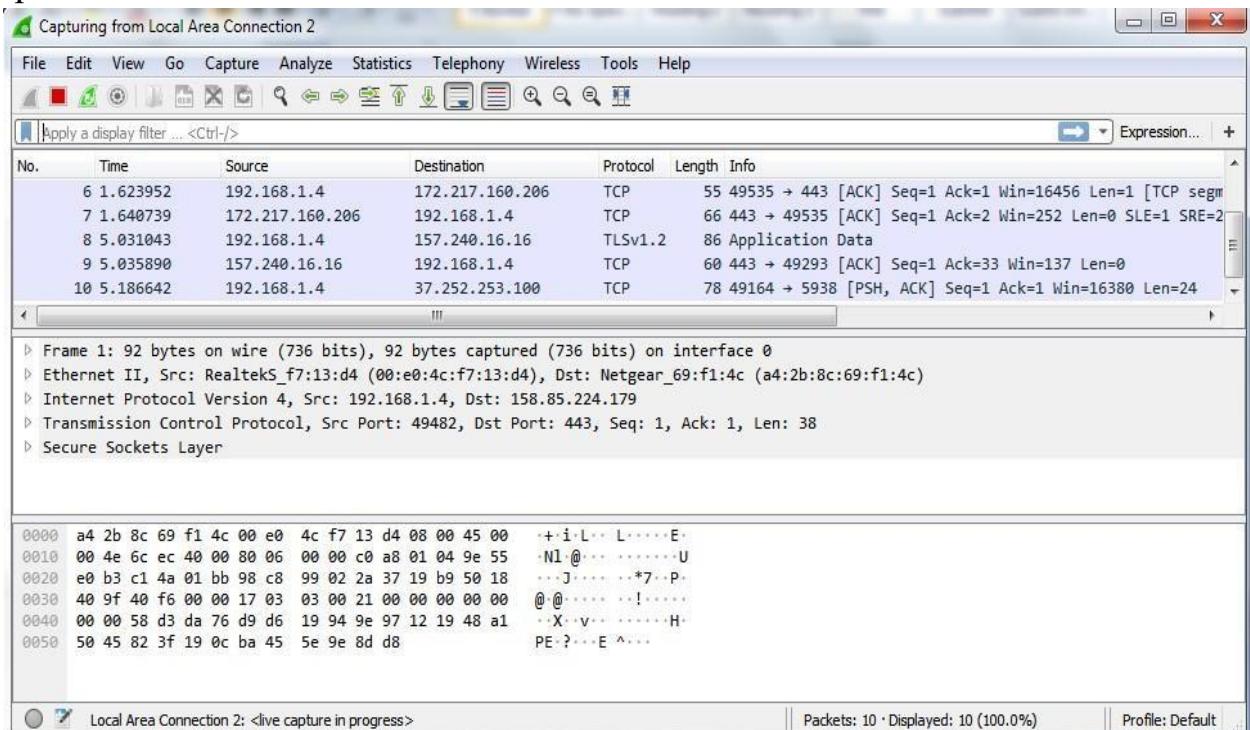
You can configure advanced features by clicking Capture > Options, but this isn't necessary for now.



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

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

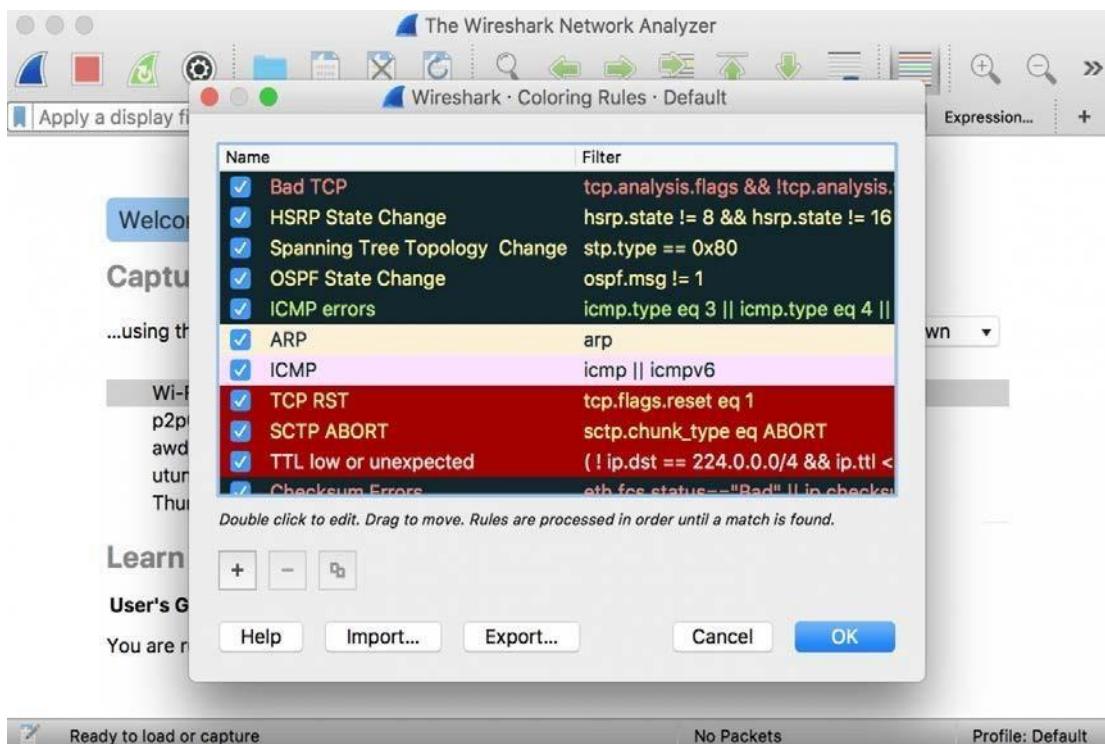
Different packets are seen highlighted in various different colors. This is Wireshark’s way of displaying traffic to help you easily identify the types of it. Default colors are:

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.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.4	158.85.224.179	TLSv1.2	92	Application Data
2	0.202110	192.168.1.4	157.240.16.16	TCP	55	49292 → 443 [ACK] Seq=1 Ack=1 Win=16475 Len=1 [TCP segment part 1 of 1]
3	0.210204	157.240.16.16	192.168.1.4	TCP	60	443 → 49292 [ACK] Seq=1 Ack=2 Win=414 Len=0
4	0.256131	158.85.224.179	192.168.1.4	TLSv1.2	99	Application Data
5	0.467707	192.168.1.4	158.85.224.179	TCP	54	49482 → 443 [ACK] Seq=39 Ack=46 Win=16532 Len=0

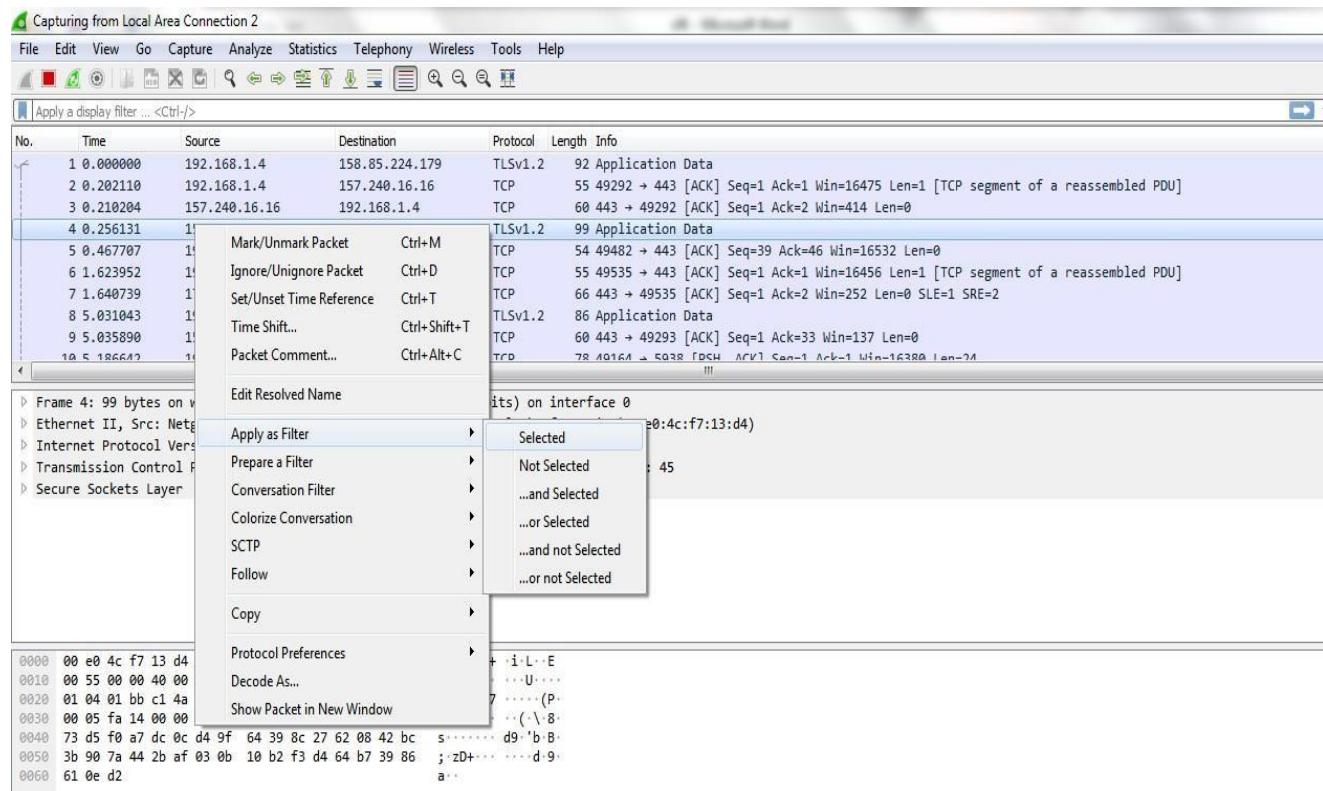
Frame 4: 99 bytes on wire (792 bits), 99 bytes captured (792 bits) on interface 0  
 Ethernet II, Src: Netgear\_69:f1:4c (a4:2b:8c:69:f1:4c), Dst: RealtekS\_f7:13:d4 (00:e0:4c:f7:13:d4)  
 Internet Protocol Version 4, Src: 158.85.224.179, Dst: 192.168.1.4  
 Transmission Control Protocol, Src Port: 443, Dst Port: 49482, Seq: 1, Ack: 39, Len: 45  
 Secure Sockets Layer

```

0000  00 e0 4c f7 13 d4 a4 2b  8c 69 f1 4c 08 00 45 20  ..L....+ .i·L·E
0010  00 55 00 00 40 00 2e 06  0b ce 9e 55 e0 b3 c0 a8  .U· @... ..U....
0020  01 04 01 bb c1 4a 2a 37  19 b9 98 c8 99 28 50 18  .....J*7 .....(P.
0030  00 05 fa 14 00 00 17 03  03 00 28 1b 5c 89 38 8f  .........(.\.8.
0040  73 d5 f0 a7 dc 0c d4 9f  64 39 8c 27 62 08 42 bc  s..... d9.'b.B.
0050  3b 90 7a 44 2b af 03 0b  10 b2 f3 d4 64 b7 39 86  ;·zD+.....d.9.
0060  61 0e d2          a...

```

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 SLE=4349 SRE=4350
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 SLE=19248 SRE=19249
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, "QNAME" 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	20.919775	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	05.721024	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	279.421459	192.168.1.4	23.57.219.27	OCSP	127	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 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
59	74.085276	192.168.1.1	104.25.218.21	TCP	60	56688 → 49173 [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	316.010280	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`

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
	101.169.1.1	17.106.94.17		TCP	54	Ack=1006 + 80 [ACK] Seq=251 Ack=101 Win=66280 Len=0

## 9. Display packets which contains keyword facebook

➤ `tcp contains 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 :- 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:

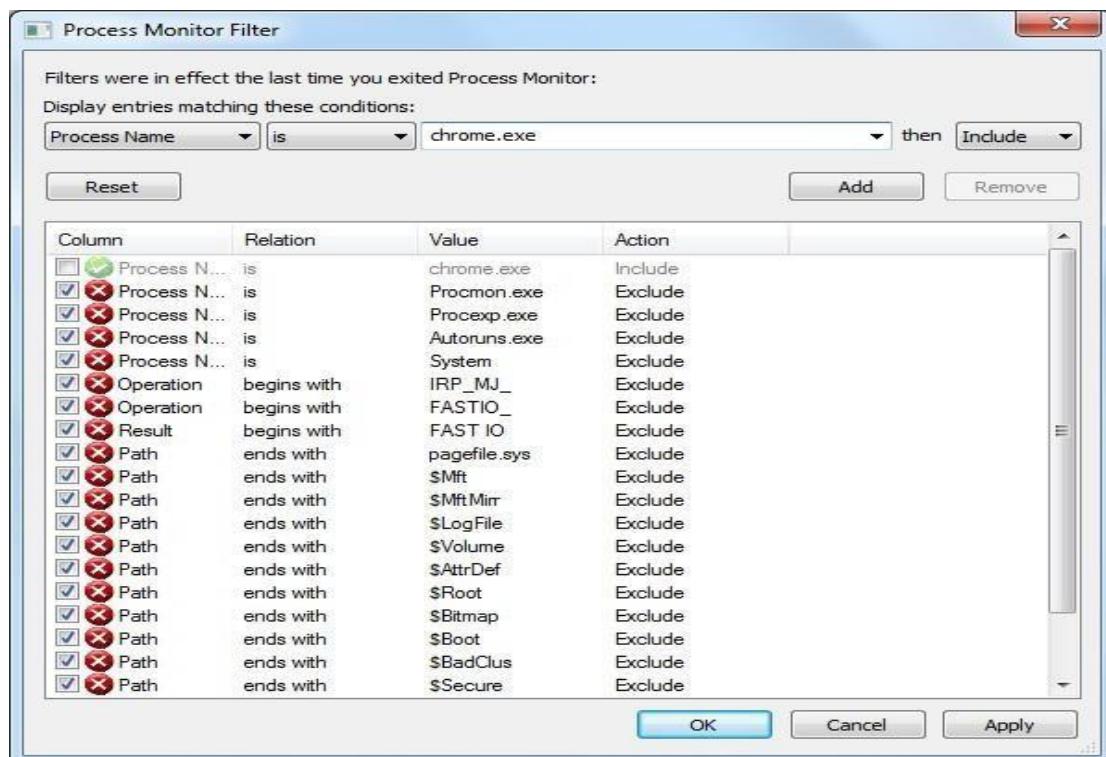
1. File and Disk Utilities
2. Networking Utilities
3. Process Utilities
4. Security Utilities
5. System Information Utilities
6. Miscellaneous Utilities

➤ **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:



The screenshot shows the main Process Monitor window titled 'Process Monitor - Sysinternals: www.sysinternals.com'. The menu bar includes File, Edit, Event, Filter, Tools, Options, and Help. The toolbar contains various icons for file operations. The main pane displays a table of events. The columns are: Time ..., Process Name, PID, Operation, Path, Result, and Detail. The table shows several events for the process 'chrome.exe' with PID 5236. The operations include CreateFile, QueryDirectory, and CloseFile. The paths are mostly within the directory 'C:\Users\COM-3\AppData\Local\Google\Chrome\User Data\Default'. The results are mostly 'SUCCESS'. The details column provides more information about the operations, such as 'Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Attr...' and file names like '000119ldb', '000140ldb', '000195ldb', '000199log', '24fa877-e72a-4b32-9312-f114d8b06a50tmp', and '4ea16cb...'. The status at the bottom indicates 'Showing 1303 of 179857 events (0.72%)' and 'Backed by virtual memory'.

Time ...	Process Name	PID	Operation	Path	Result	Detail
11:09...	chrome.exe	5236	CreateFile	C:\Users\COM-3\AppData\Local\Google\Chrome\User Data\Default\1000119ldb	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Attr...
11:09...	chrome.exe	5236	QueryDirectory	C:\Users\COM-3\AppData\Local\Google\Chrome\User Data\Default\1000140ldb	SUCCESS	Filter: *, 1: 000119ldb, 2: 000140ldb, 3: 000195ldb, 4: 000199log, 5: 24fa877-e72a-4b32-9312-f114d8b06a50tmp, 6: 4ea16cb...
11:09...	chrome.exe	5236	QueryDirectory	C:\Users\COM-3\AppData\Local\Google\Chrome\User Data\Default\1000195ldb	SUCCESS	0: ..., 1: 000119ldb, 2: 000140ldb, 3: 000195ldb, 4: 000199log, 5: 24fa877-e72a-4b32-9312-f114d8b06a50tmp, 6: 4ea16cb...
11:09...	chrome.exe	5236	QueryDirectory	C:\Users\COM-3\AppData\Local\Google\Chrome\User Data\Default\1000199log	NO MORE FILES	
11:09...	chrome.exe	5236	CloseFile	C:\Users\COM-3\AppData\Local\Google\Chrome\User Data\Default\1000199log	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Attr...
11:09...	chrome.exe	5236	CreateFile	C:\Users\COM-3\AppData\Local\Google\Chrome\User Data\Default\1000199log	SUCCESS	Filter: History, 1: History
11:09...	chrome.exe	5236	QueryDirectory	C:\Users\COM-3\AppData\Local\Google\Chrome\User Data\Default\1000199log	SUCCESS	Filter: History, 1: History
11:09...	chrome.exe	5236	QueryDirectory	C:\Users\COM-3\AppData\Local\Google\Chrome\User Data\Default\1000199log	NO MORE FILES	

**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			Microsoft Corporation	NT AUTHORITY\SYSTEM
cers.exe (600)	Client Server Run...	C:\Windows\system...		Microsoft Corporation	NT AUTHORITY\SYSTEM
conhost.exe (3996)	Console Window ...	C:\Windows\system...		Microsoft Corporation	NT AUTHORITY\SYSTEM
conhost.exe (6000)	Console Window ...	C:\Windows\system...		Microsoft Corporation	NT AUTHORITY\SYSTEM
wininit.exe (660)	Windows Start-Up ...	C:\Windows\system...		Microsoft Corporation	NT AUTHORITY\SYSTEM
services.exe (716)	Services and Cont...	C:\Windows\system...		Microsoft Corporation	NT AUTHORITY\SYSTEM
svchost.exe (892)	Host Process for ...	C:\Windows\system...		Microsoft Corporation	NT AUTHORITY\SYSTEM
wmiprvse.exe (156)	WMI Provider Host	C:\Windows\system...		Microsoft Corporation	NT AUTHORITY\SYSTEM
ARWSRVC.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\system...		Microsoft Corporation	NT AUTHORITY\SYSTEM
svchost.exe (1272)	Host Process for ...	C:\Windows\system...		Microsoft Corporation	NT AUTHORITY\SYSTEM
svchost.exe (1308)	Host Process for ...	C:\Windows\system...		Microsoft Corporation	NT AUTHORITY\SYSTEM
Dwm.exe (2036)	Desktop Window	C:\Windows\system...		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...

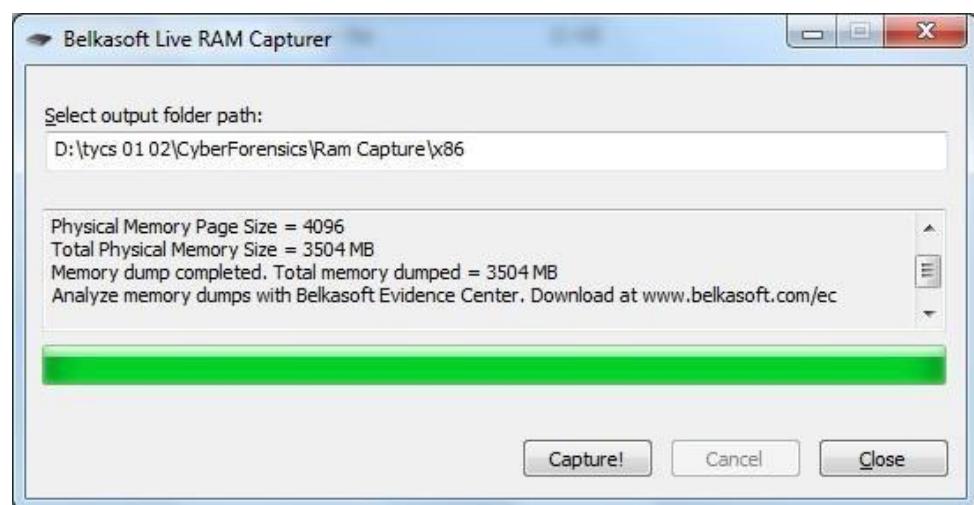
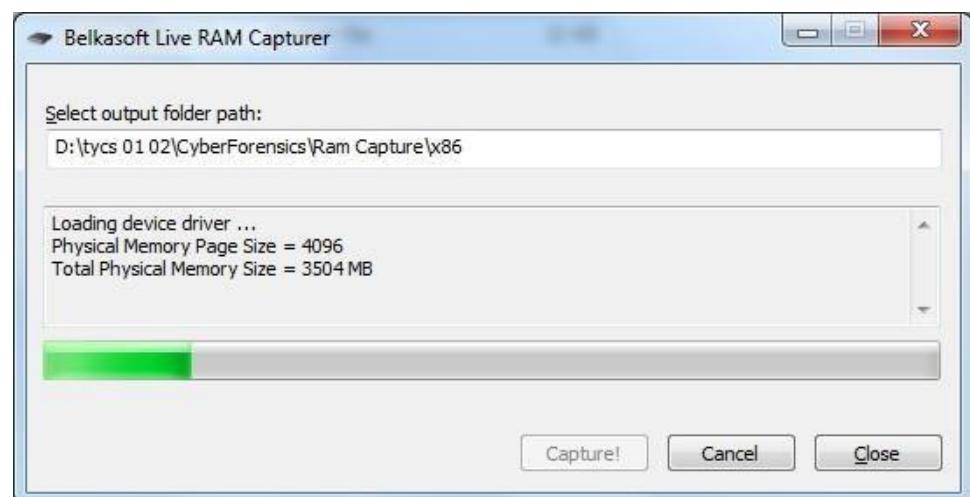
[Filter...](#) 147 file paths [Save...](#) [OK](#)

## ➤ Capture RAM (Tool: RAMCapture)

### To Do:

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

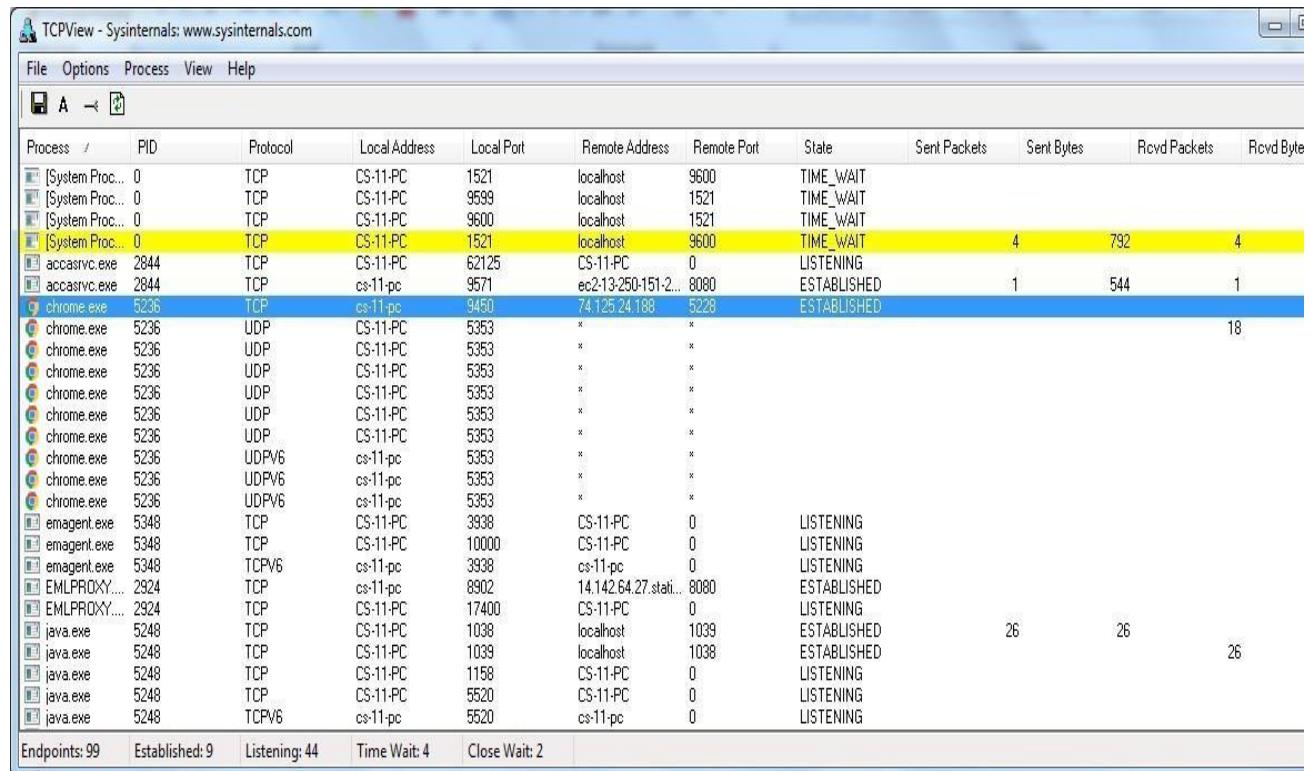
### Output:



➤ Capture TCP/UDP packets (Tool: TcpView) :

- To Do: 1. Save to .txt file.  
2. Whois

**Output:**



The screenshot shows the TCPView application interface with a list of network connections. The columns in the table are: Process / PID, Protocol, Local Address, Local Port, Remote Address, Remote Port, State, Sent Packets, Sent Bytes, Rcvd Packets, and Rcvd Byte. The table lists various processes like System Proc., accasvc.exe, chrome.exe, emagent.exe, EMLPROXY..., and java.exe, along with their respective connection details. The chrome.exe process (PID 5236) is highlighted in yellow, indicating it is the current focus.

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	
accasvc.exe 2844	TCP	CS-11-PC	62125	CS-11-PC	0	LISTENING				
accasvc.exe 2844	TCP	cs-11-pc	9571	ec2-13-250-151-2...	8080	ESTABLISHED	1	544	1	
chrome.exe 5236	TCP	cs-11-pc	9450	74.125.24.188	5228	ESTABLISHED				18
chrome.exe 5236	UDP	CS-11-PC	5353	*	*					
chrome.exe 5236	UDP	CS-11-PC	5353	*	*					
chrome.exe 5236	UDP	CS-11-PC	5353	*	*					
chrome.exe 5236	UDP	CS-11-PC	5353	*	*					
chrome.exe 5236	UDP	CS-11-PC	5353	*	*					
chrome.exe 5236	UDP	CS-11-PC	5353	*	*					
chrome.exe 5236	UDPV6	cs-11-pc	5353	*	*					
chrome.exe 5236	UDPV6	cs-11-pc	5353	*	*					
chrome.exe 5236	UDPV6	cs-11-pc	5353	*	*					
emagent.exe 5348	TCP	CS-11-PC	3938	CS-11-PC	0	LISTENING				
emagent.exe 5348	TCP	CS-11-PC	10000	CS-11-PC	0	LISTENING				
emagent.exe 5348	TCPV6	cs-11-pc	3938	cs-11-pc	0	LISTENING				
EMLPROXY.... 2924	TCP	cs-11-pc	8902	14.142.64.27.static	8080	ESTABLISHED				
EMLPROXY.... 2924	TCP	CS-11-PC	17400	CS-11-PC	0	LISTENING				
java.exe 5248	TCP	CS-11-PC	1038	localhost	1039	ESTABLISHED	26	26		
java.exe 5248	TCP	CS-11-PC	1039	localhost	1038	ESTABLISHED				26
java.exe 5248	TCP	CS-11-PC	1158	CS-11-PC	0	LISTENING				
java.exe 5248	TCP	CS-11-PC	5520	CS-11-PC	0	LISTENING				
java.exe 5248	TCPV6	cs-11-pc	5520	cs-11-pc	0	LISTENING				

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

Process /	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets	Sent Bytes	Rcvd Packets	Rcvd Bytes
[System Proc... 0	0	TCP	CS-11-PC	1521	localhost	10008	TIME_WAIT				
[accsvc.exe 2844	2844	TCP	CS-11-PC	62125	CS-11-PC	0	LISTENING				
[accsvc.exe 2844	2844	TCP	cs-11-pc	10072	ec2-13-250-151-2	8080	ESTABLISHED	1	544	1	
[accsvc.exe 2844	2844	TCP	cs-11-pc	10146	lobby.techno-pc	5054	SYN_SENT				
chrome.exe 5236	5236	TCP	cs-11-pc	9801	172.217.194.188	5228	ESTABLISHED	1	33	1	426
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	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	TCP	cs-11-pc	10040	104.19.196.151	Https	ESTABLISHED	7	1,141	16	
chrome.exe 5236	5236	UDP	CS-11-PC	57081	*	*		5	1,955	7	
chrome.exe 5236	5236	UDP	CS-11-PC	57082	*	*		4	2,767	7	
chrome.exe 5236	5236	UDP	CS-11-PC	58349	*	*		3	1,417	4	
chrome.exe 5236	5236	TCP	cs-11-pc	10140	mint.	Process Properties...	ED	2	643	5	
chrome.exe 5236	5236	TCP	cs-11-pc	10141	mint.	End Process...	ED	4	1,679	16	
chrome.exe 5236	5236	TCP	cs-11-pc	10142	mint.	Close Connection	ED	4	2,767	7	
chromer.exe 5348	5348	TCP	CS-11-PC	3938	CS-1						
chromer.exe 5348	5348	TCP	CS-11-PC	10000	CS-1	Whois...	Ctrl+W				
chromer.exe 5348	5348	TCPV6	ca-11-pc	3938	CS-1	Copy	Ctrl+C				
EMLPROXY... 2924	2924	TCP	CS-11-PC	17400	CS-1						
java.exe 5249	5249	TCP	CS-11-PC	1038	localhost	1038	ESTABLISHED	85	85		85
java.exe 5249	5249	TCP	CS-11-PC	1039	localhost	1038	ESTABLISHED				
java.exe 5249	5249	TCP	CS-11-PC	1158	CS-11-PC	0	LISTENING				
java.exe 5249	5249	TCP	CS-11-PC	5520	CS-11-PC	0	LISTENING				
java.exe 5249	5249	TCPV6	ca-11-pc	5520	ca-11-pc	0	LISTENING				
last.exe 756	756	TCP	CS-11-PC	1028	CS-11-PC	0	LISTENING				
last.exe 756	756	TCPV6	ca-11-pc	1028	ca-11-pc	0	LISTENING				
ndNSRespo... 2824	2824	TCP	CS-11-PC	5354	CS-11-PC	0	LISTENING				295
ndNSRespo... 2824	2824	UDP	ca-11-pc	5353	*	*					
ndNSRespo... 2824	2824	UDP	ca-11-pc	5353	*	*					
ndNSRespo... 2824	2824	UDP	ca-11-pc	5353	*	*					
ndNSRespo... 2824	2824	UDP	ca-11-pc	64645	*	*		4	208	4	
ndNSRespo... 2824	2824	UDPV6	ca-11-pc	64646	*	*					
nsmdrv.exe 3708	3708	TCP	CS-11-PC	ms-dsdp4	CS-11-PC	0	LISTENING				
nsmdrv.exe 3708	3708	TCPV6	ca-11-pc	ms-dsdp4	ca-11-pc	0	LISTENING				
mysqld.exe 3832	3832	TCP	CS-11-PC	3306	CS-11-PC	0	LISTENING				
omtreco.exe 3952	3952	TCP	CS-11-PC	49152	CS-11-PC	0	LISTENING				
outlook.c... 7724	7724	TCP	-- 11 --	49152	-- 11 --	49152	CLOSE_WAIT				

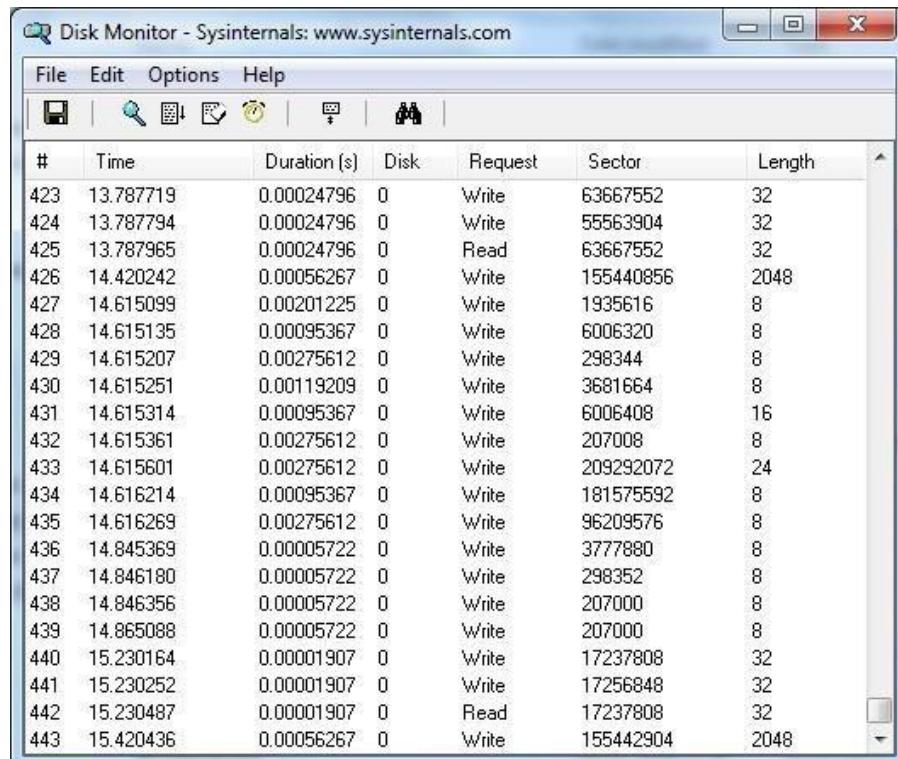


➤ **Monitor Hard Disk (Tool: DiskMon) :**

**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 data grid displaying disk operations. The columns are labeled #, Time, Duration (s), Disk, Request, Sector, and Length. The data grid contains approximately 40 rows of log entries, showing various write and read requests with their corresponding times, durations, disk numbers, request types, sector addresses, and lengths.

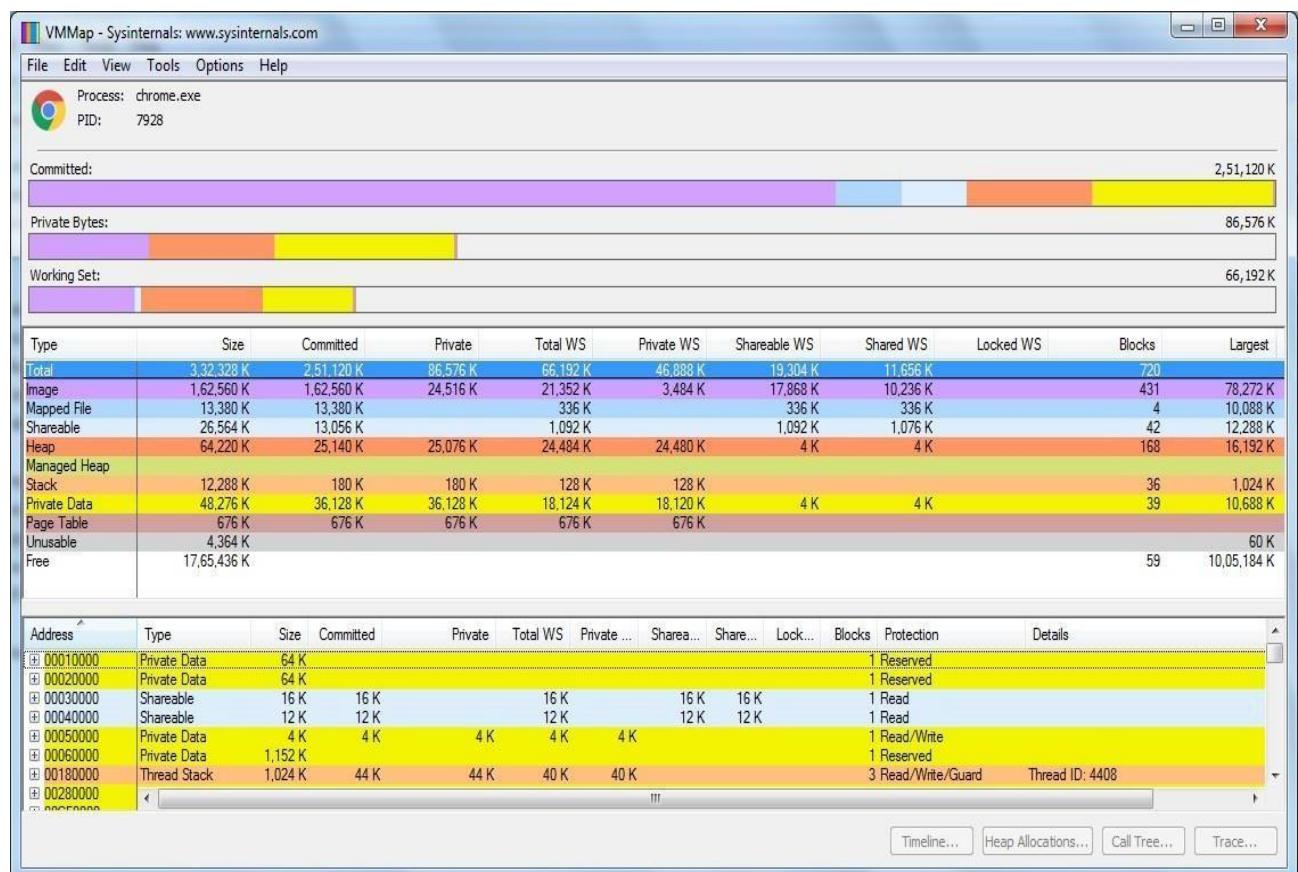
#	Time	Duration (s)	Disk	Request	Sector	Length
423	13.787719	0.00024796	0	Write	63667552	32
424	13.787794	0.00024796	0	Write	55563904	32
425	13.787965	0.00024796	0	Read	63667552	32
426	14.420242	0.00056267	0	Write	155440856	2048
427	14.615099	0.00201225	0	Write	1935616	8
428	14.615135	0.00095367	0	Write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

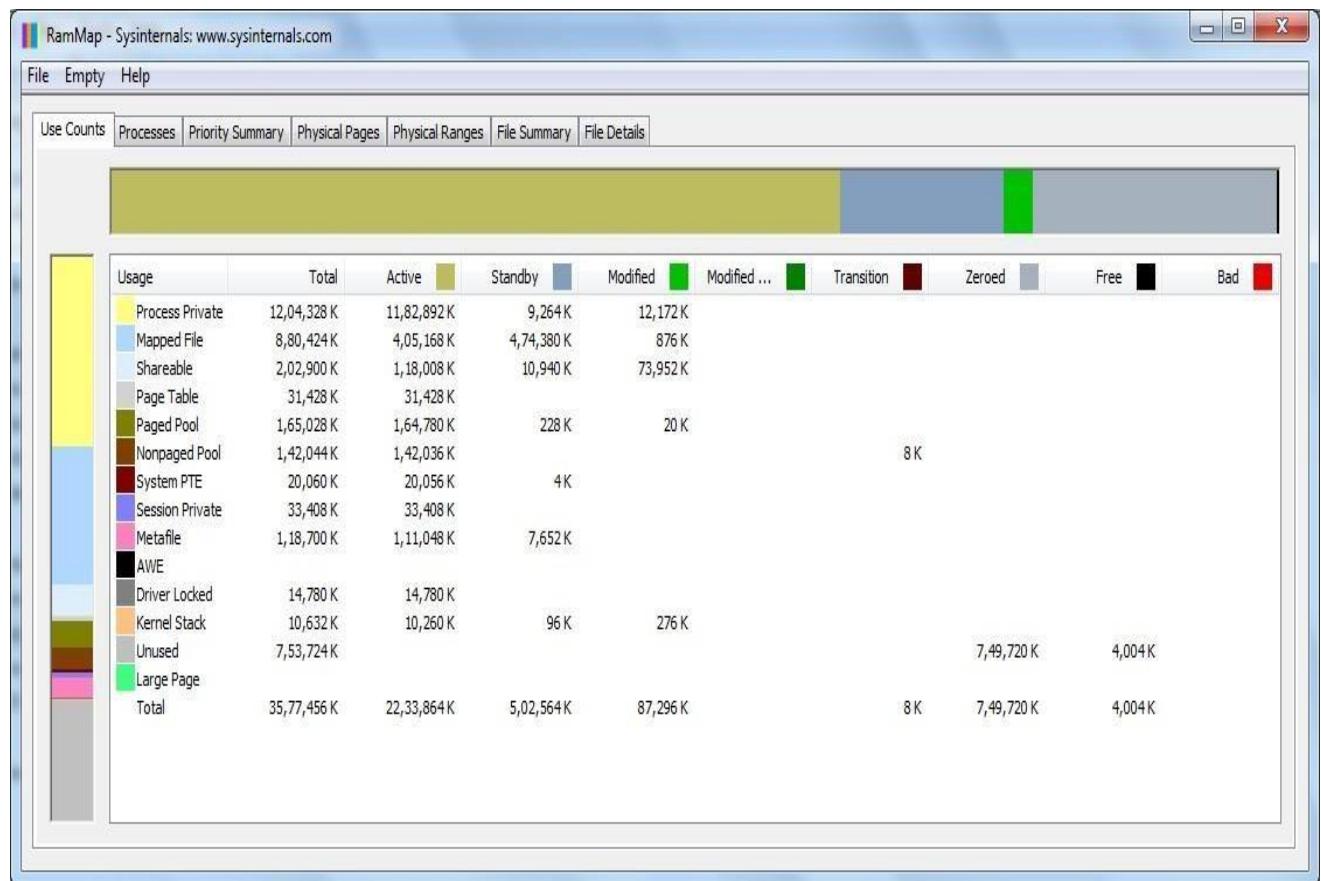


➤ **Monitor Cache Memory**  
**(Tool: RAMMap)**

**TO DO :**

1. Save to .RMP file.

**Output:**



## **PRACTICAL 6**

**AIM : - Recovering and Inspecting deleted files**

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

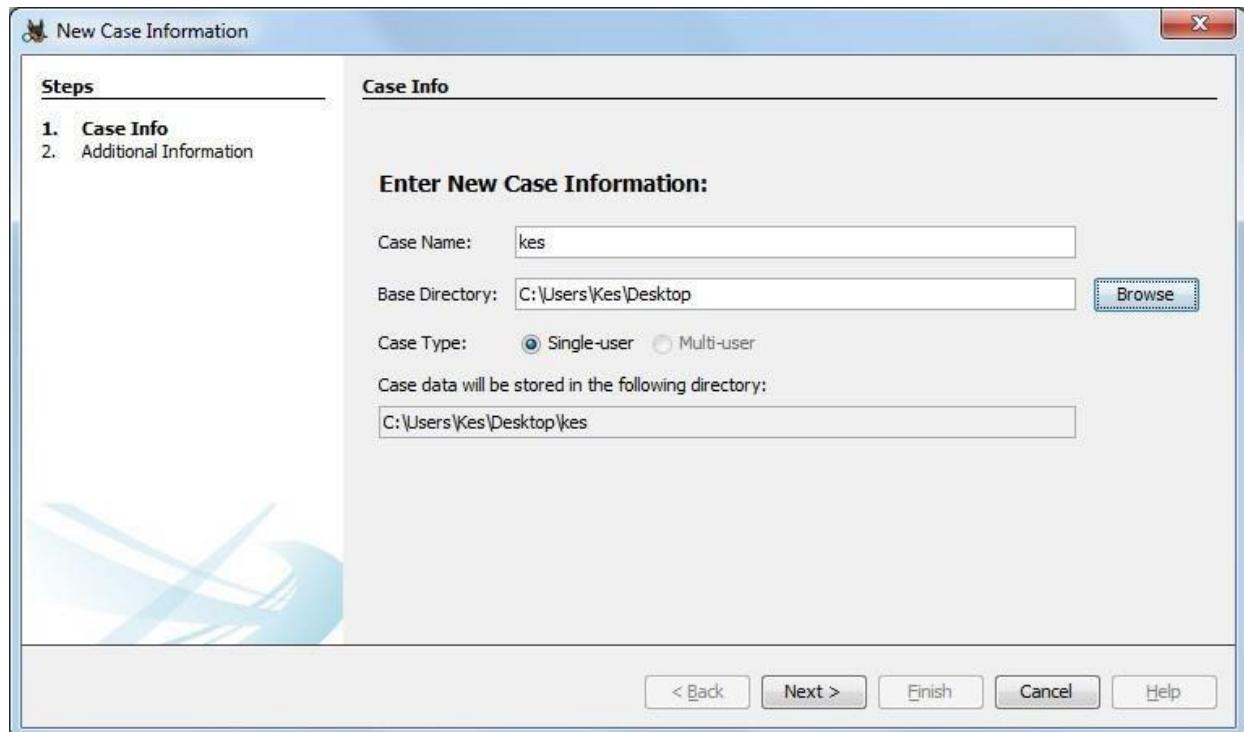
**Step 1: Start Autopsy from Desktop.**



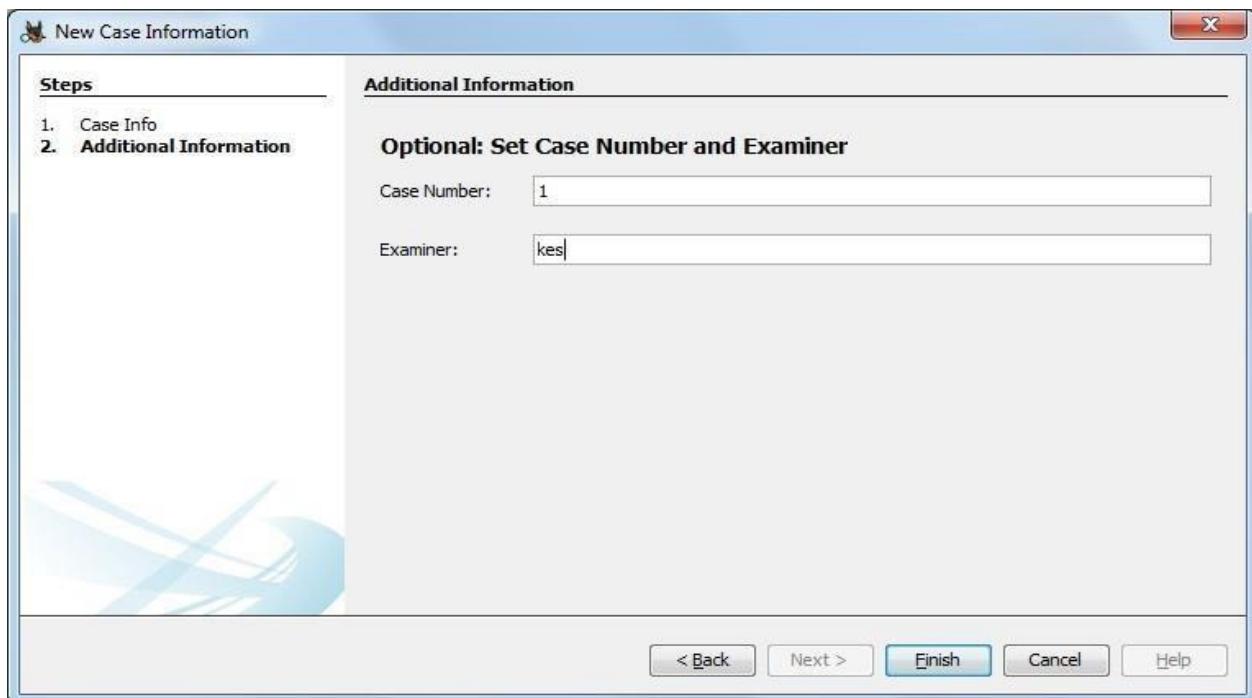
Step 2: Now create on New Case.



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



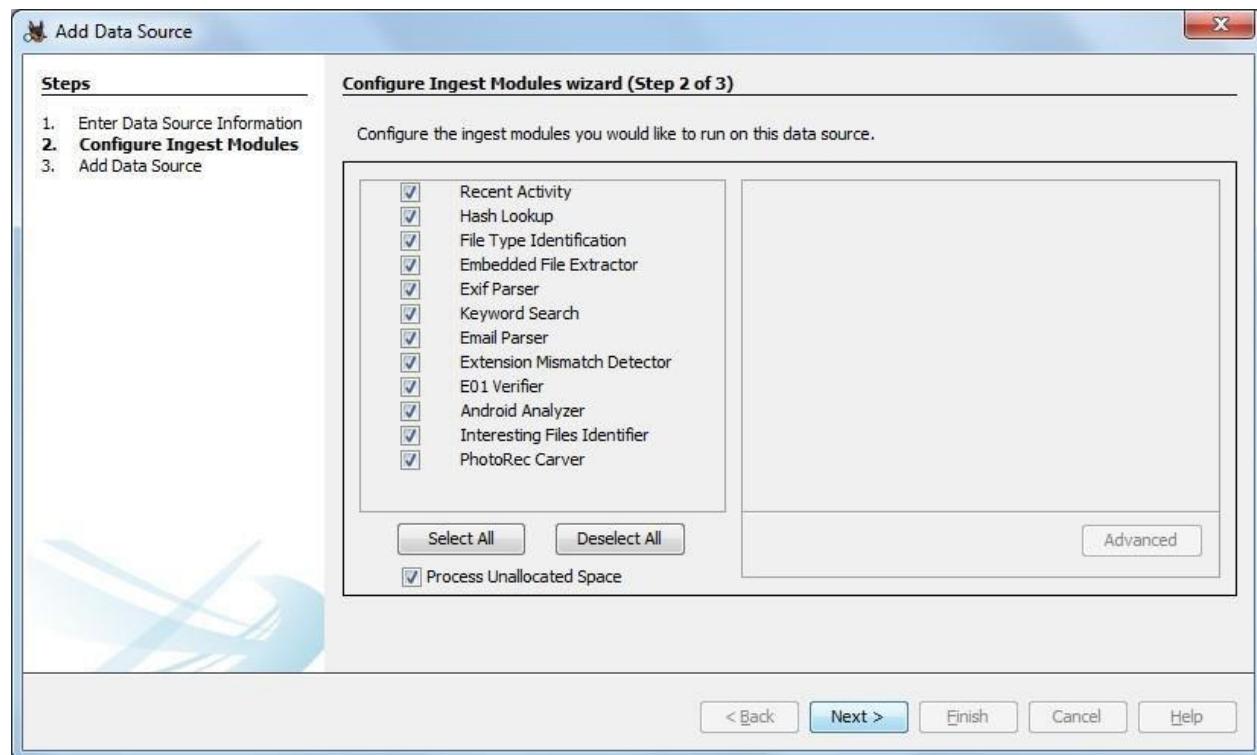
Step 4: Enter the additional Information and click on Finish.



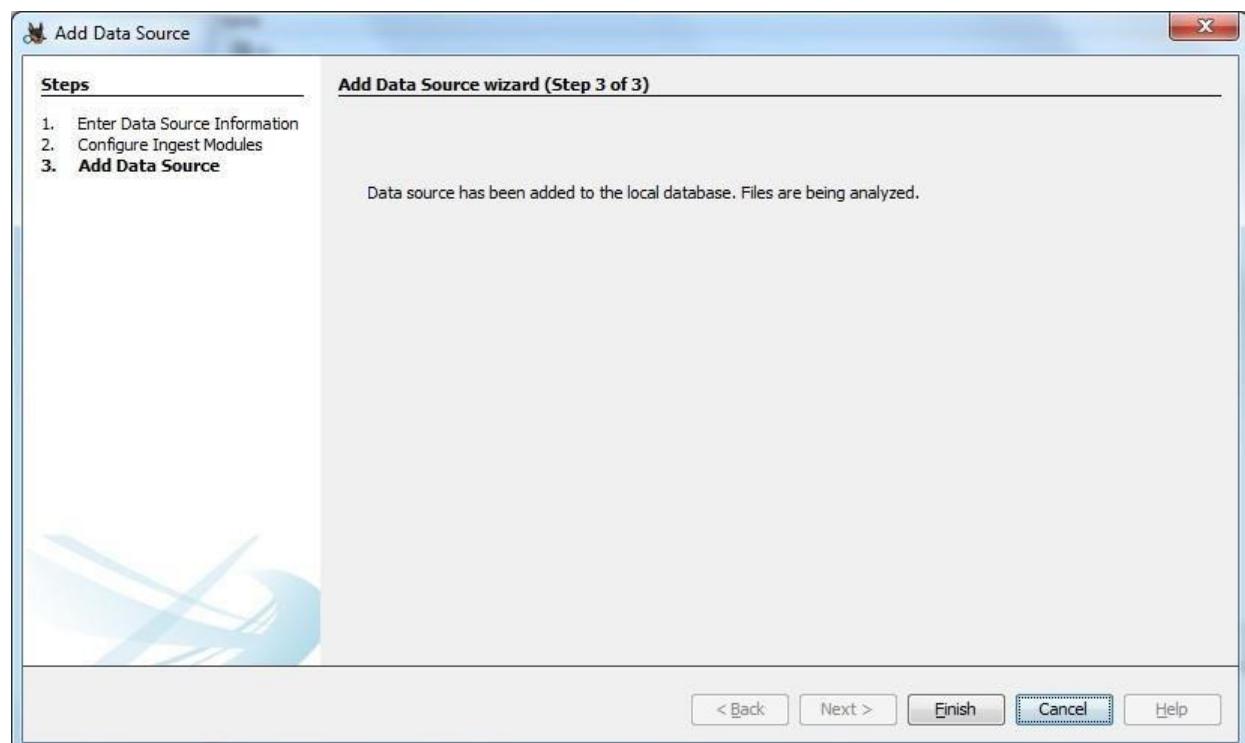
Step 5: Now Select Source Type as Local disk and Select Local disk form drop down list and click on Next.



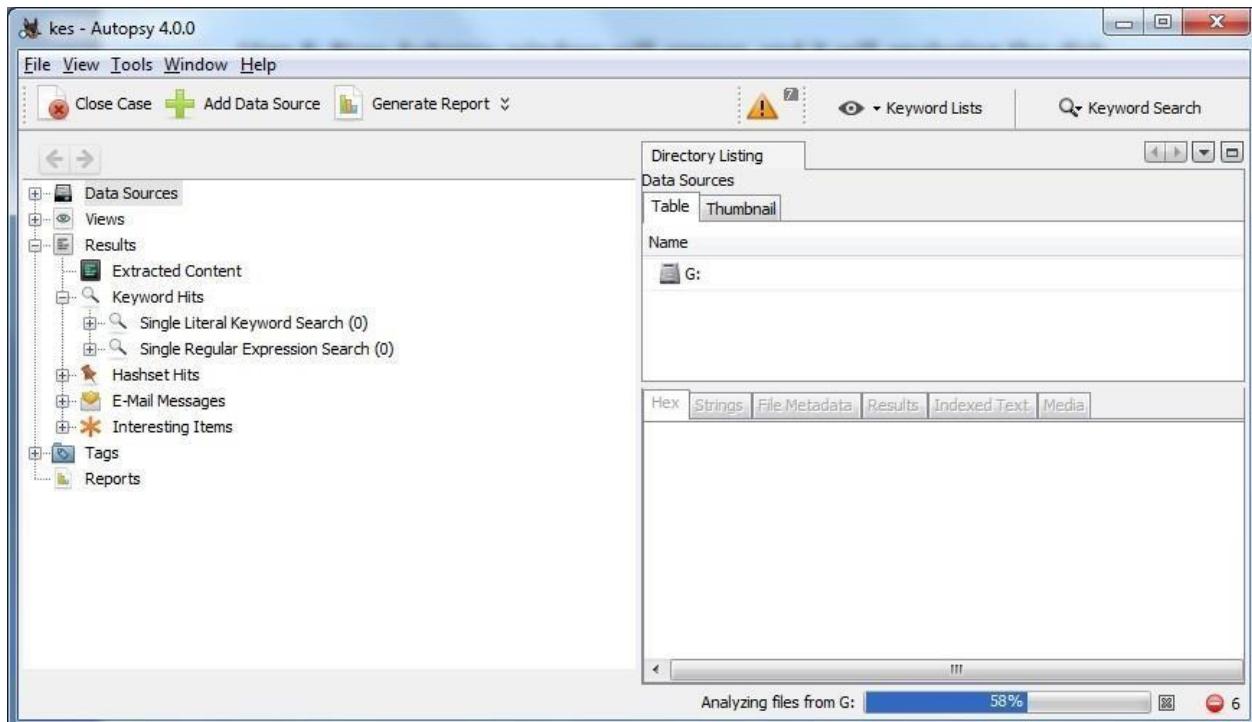
## Step 6: Click on Next Button.



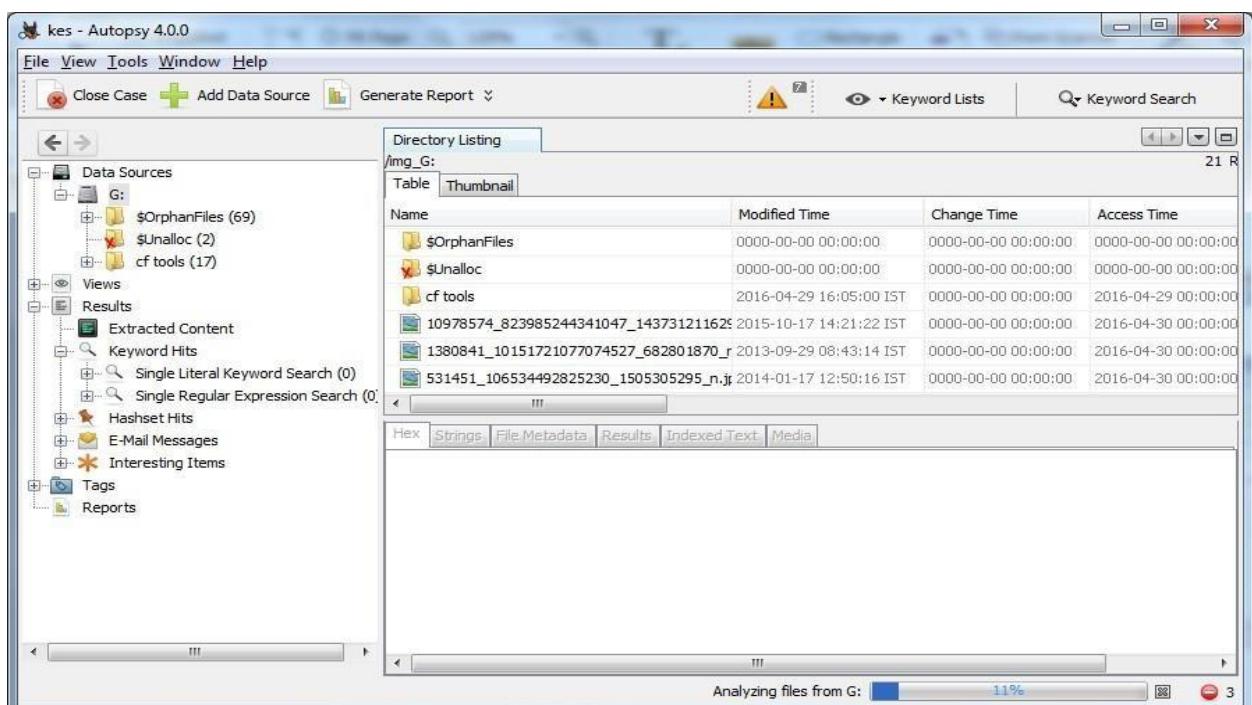
## Step 7: Now click On Finish.



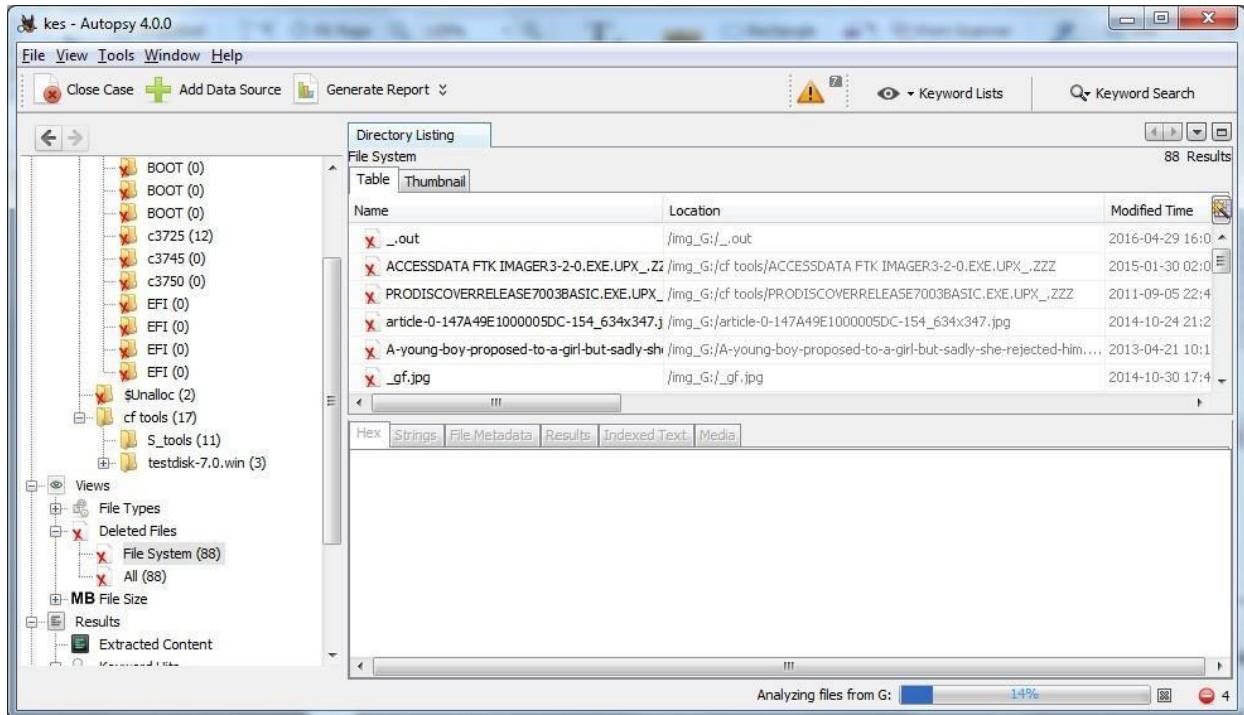
Step 8: Now Autopsy window will appear and it will analyzing the disk that we have selected.



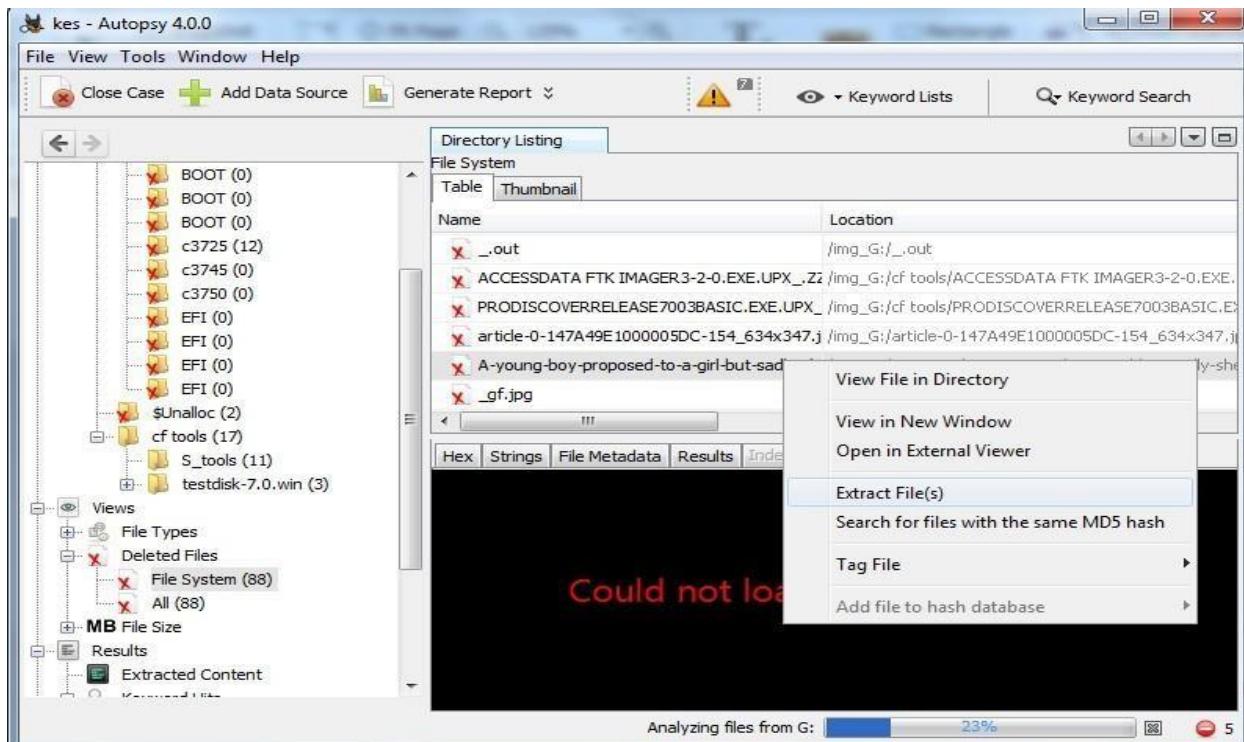
Step 9: All files will appear in table tab select any file to see the data.



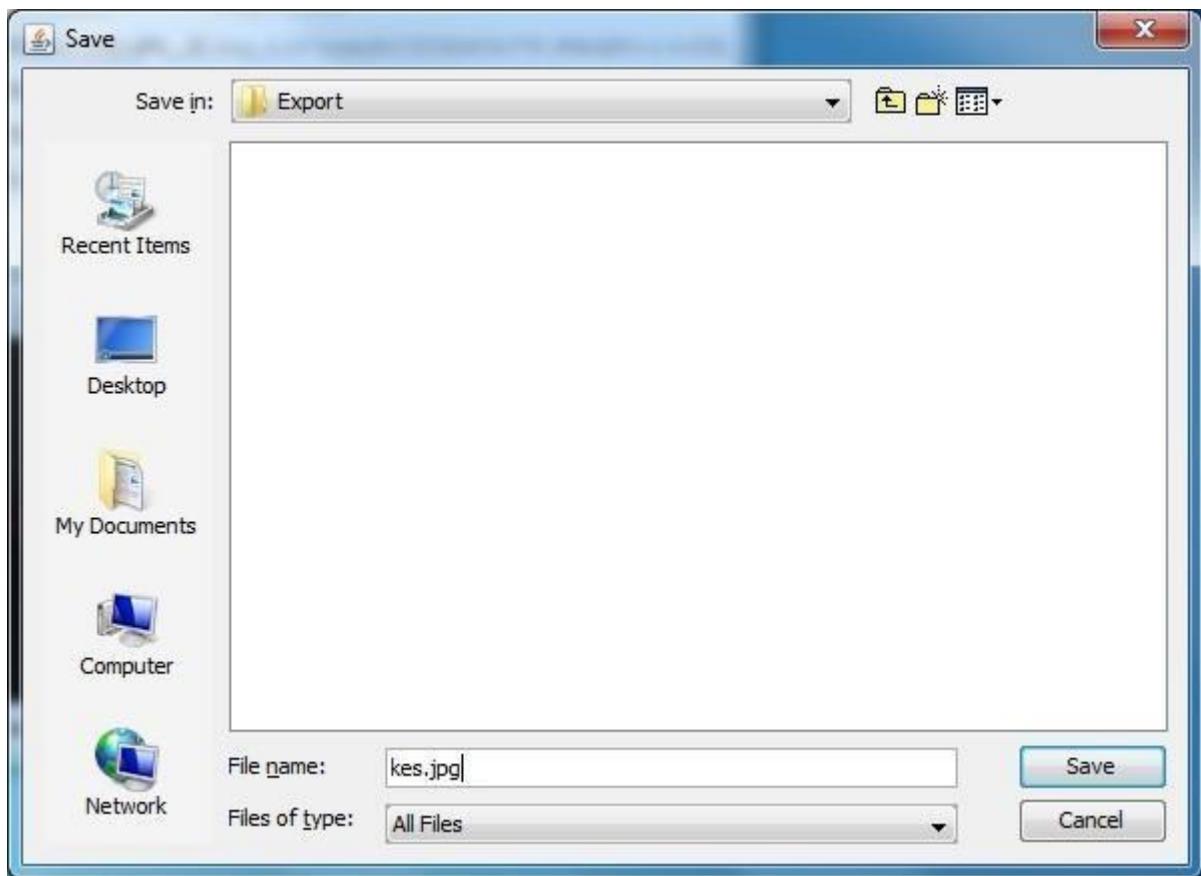
Step 10: Expand the tree from left side panel to view the document files.



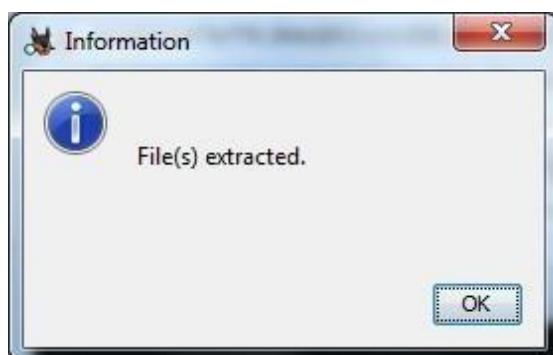
Step 11: To recover the file, go to view node-> Deleted Files node , here select any file and right click on it than select Extract Files option.



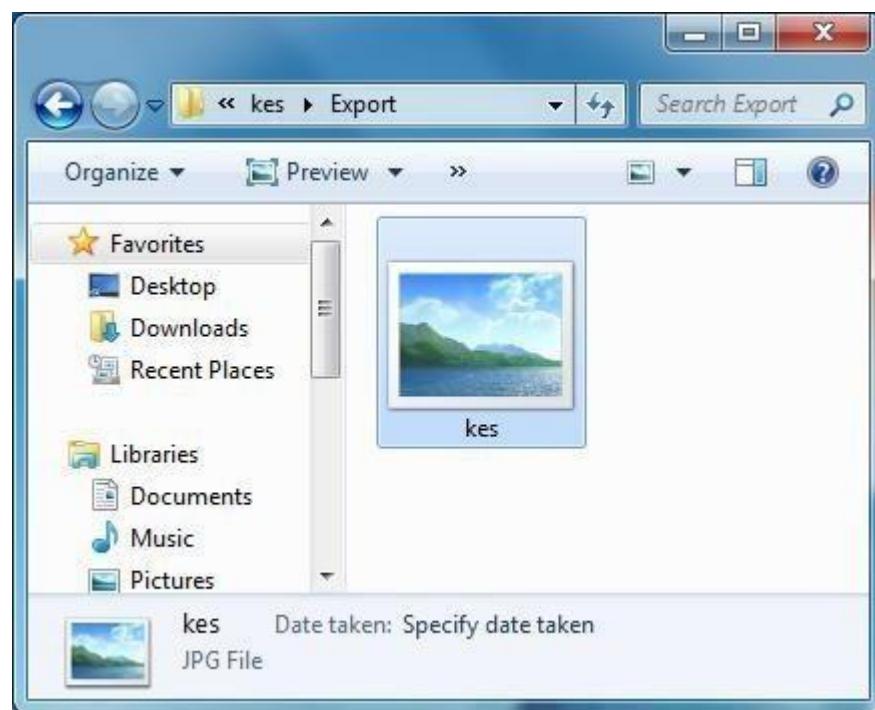
Step 12: By default Export folder is choose to save the recovered file.



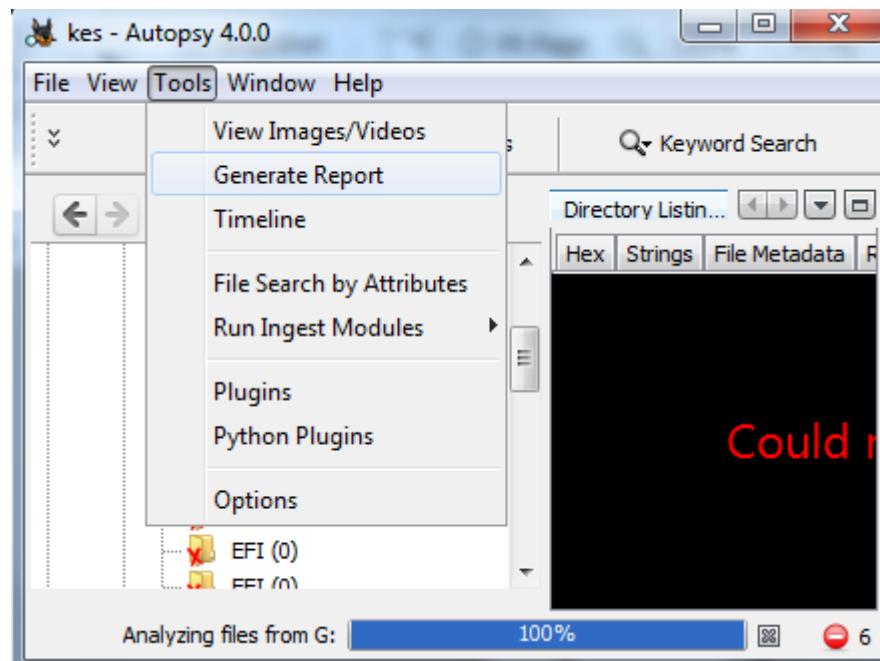
Sep 13 : Now Click on Ok.

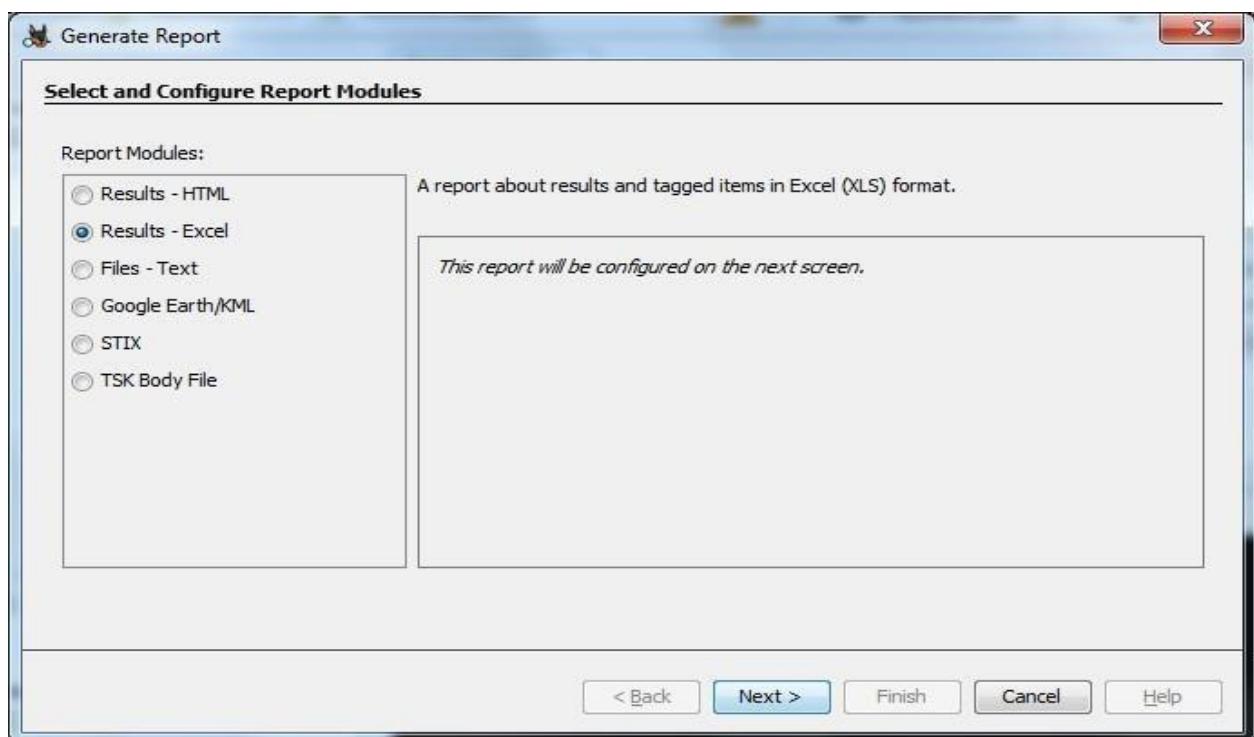


Step 14: Now go to the Export Folder to view Recover file.

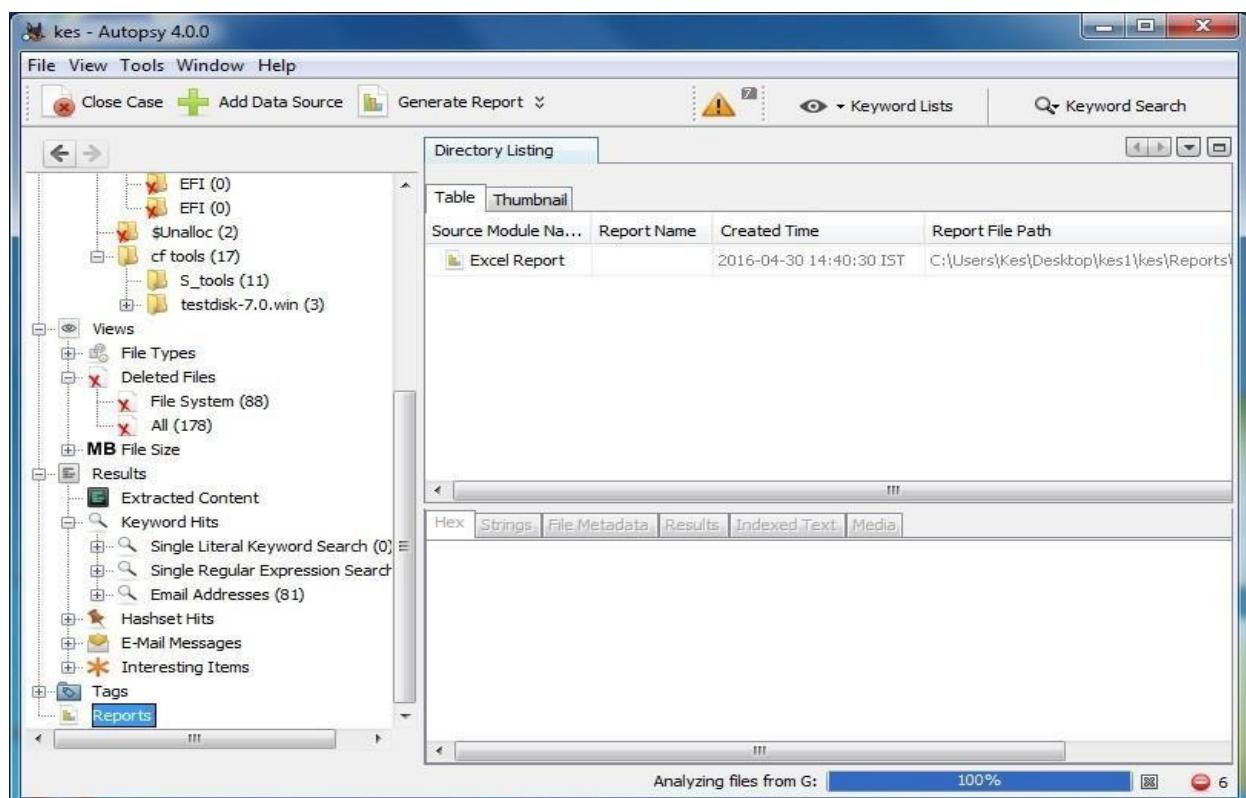


Step 15: Click on Generate Report from autopsy window and Select the Excel format and click on next.

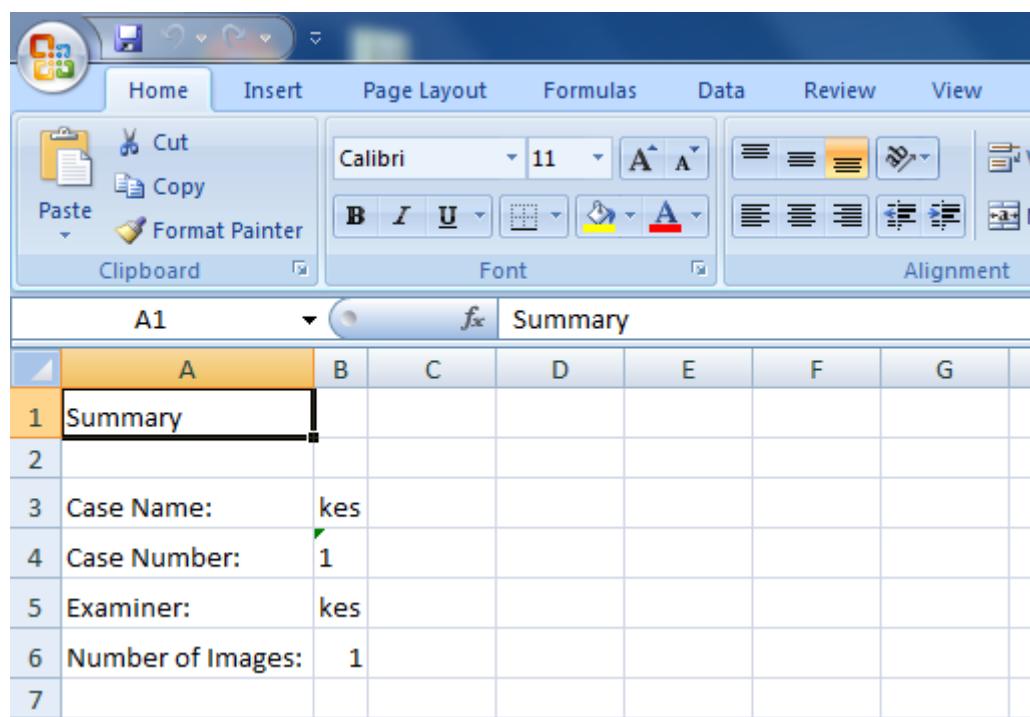




Step 16: Now Report is Generated So click on close Button .we can see the Report on Report Node.



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



A screenshot of Microsoft Excel showing a summary report. The ribbon tabs are Home, Insert, Page Layout, Formulas, Data, Review, and View. The Font group shows Calibri 11pt. The Alignment group shows center alignment. The active cell is A1, which contains the text "Summary". Row 1 contains the header "Summary". Rows 2 through 6 contain data: Case Name: kes, Case Number: 1, Examiner: kes, and Number of Images: 1. Row 7 is empty.

	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 7**

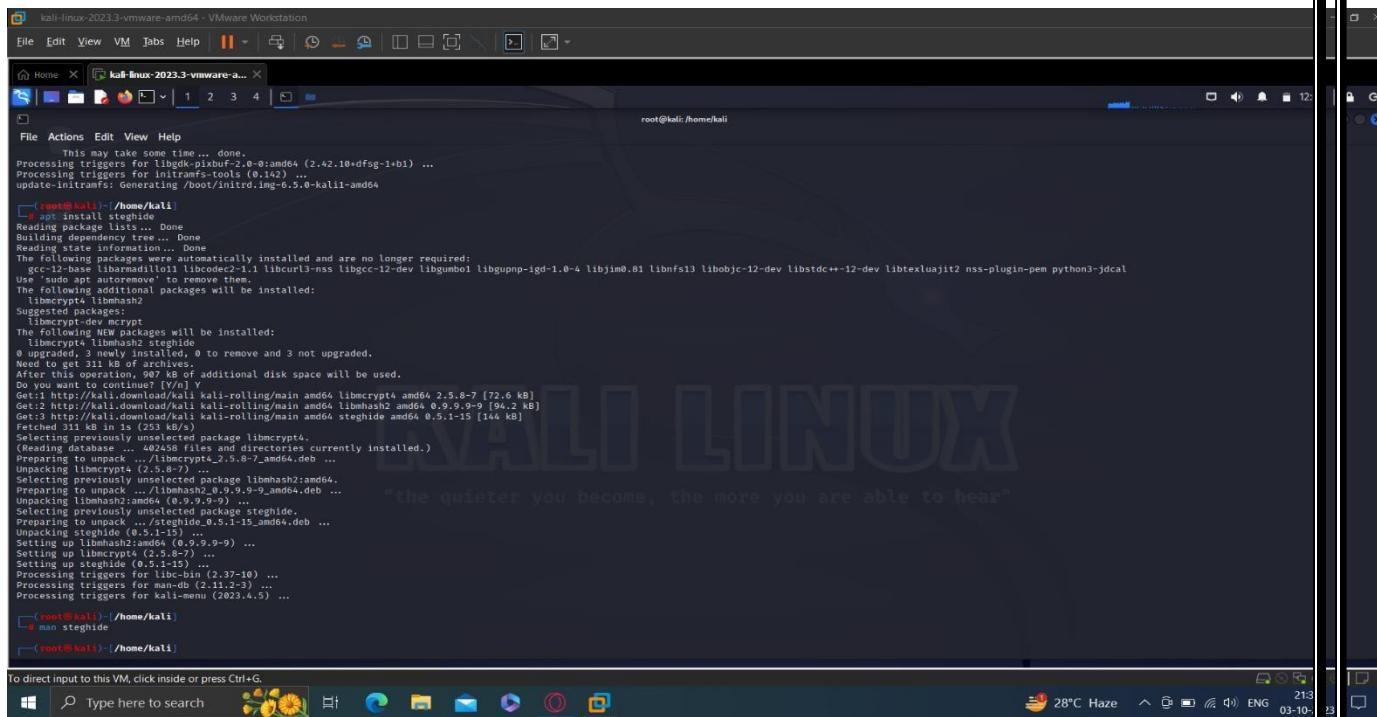
Aim : - Steganography Detection

*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

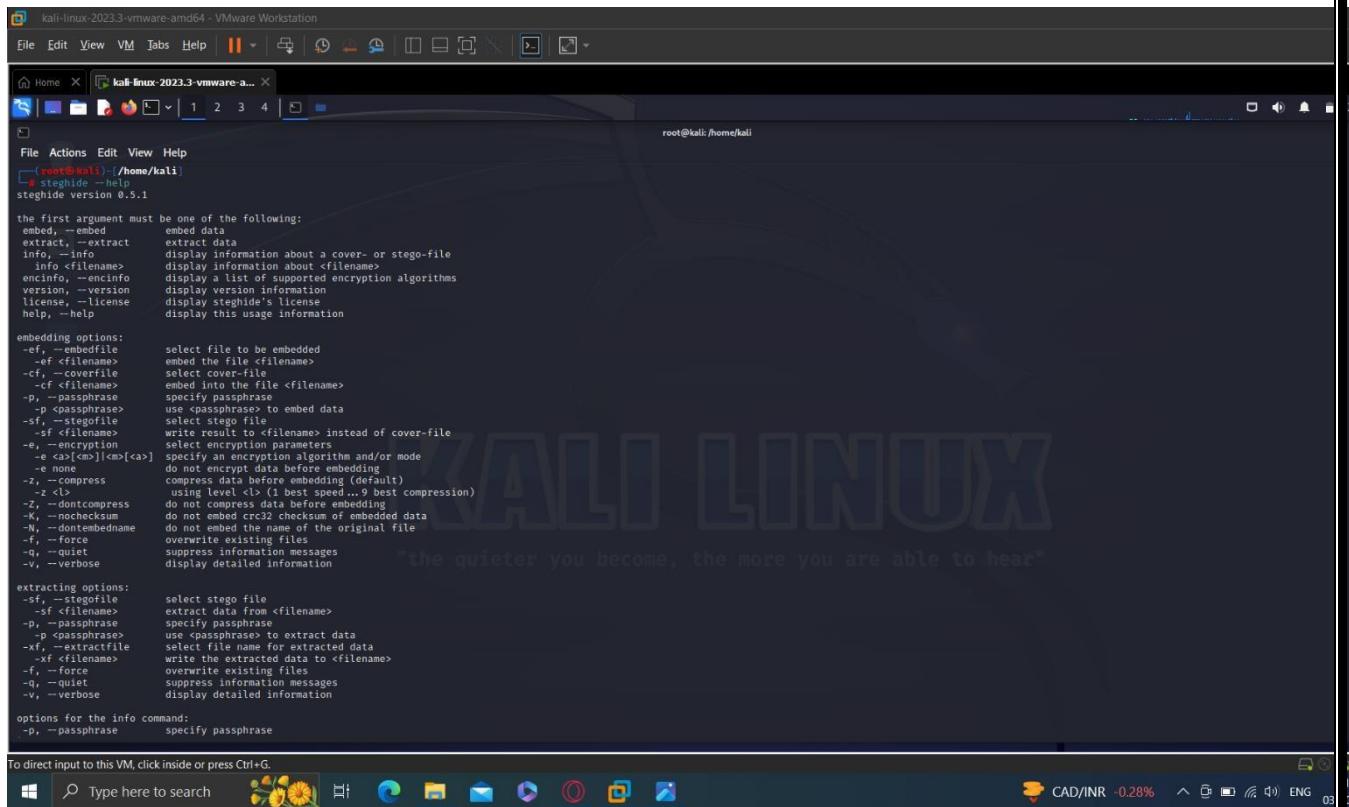


The screenshot shows a terminal window in a Kali Linux VM. The user is at the root prompt (root@kali). They type 'apt install steghide' and press Enter. The terminal displays the package manager's output, showing the download and installation of the steghide package and its dependencies. The terminal window has a dark background with light-colored text. At the bottom, there's a taskbar with various icons and system status information.

```
root@kali:~/home/kali
[1]# 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 libcodec2-1.1 libcurl3-nss libcryptopp-1.0-4 libgumbo1 libgupnp-igd-1.0-4 libjim0.81 libnfs13 libobjc-12-dev libstdc++-12-dev libtexlua1j2 nss-plugin-pem python3-jdcal
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  libmcrypt4 libmhash
Suggested packages:
  libmcrypt4-mcrypt
The following packages will be installed:
  libmcrypt4 libmhash2 steghide
0 upgraded, 3 newly installed, 0 to remove and 3 not upgraded.
Need to get 331 kB of archives.
After this operation, approximately 8 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://kali.download/kali kali-rolling/main amd64 libmcrypt4 amd64 2.5.8-7 [72.6 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 libmhash2 amd64 0.9.9.9-9 [94.2 kB]
Get:3 http://kali.download/kali kali-rolling/main amd64 steghide amd64 0.5.1-15 [114 kB]
Fetched 311 kB in 1s (253 kB/s)
Selecting previously unselected package libmcrypt4.
(Reading database ... 402458 files and directories currently installed.)
Unpacking libmcrypt4 (2.5.8-7) ...
Selecting previously unselected 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 libmcrypt4 (2.5.8-7) ...
Setting up libmhash2:amd64 (0.9.9.9-9) ...
Setting up steghide (0.5.1-15) ...
processing triggers for libc-bin (2.37-0ubuntu0.2) ...
processing triggers for man-db (2.11.2-3) ...
processing triggers for kali-menu (2023.4.0) ...
[1]# man steghide
[1]#
```

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 --help
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
-f <filename>, --filename <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

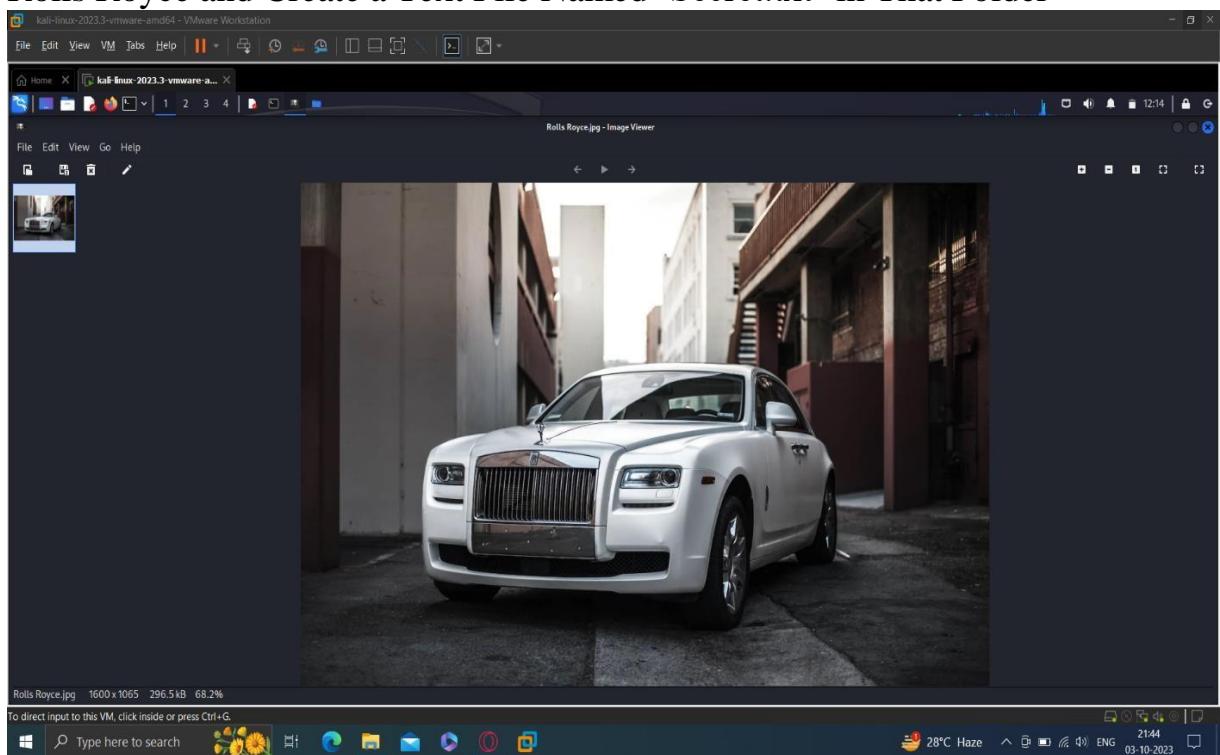
embedding options:
-ef, --embedfile    select file to be embedded
-o <filename>       embed the file <filename>
-cf <filename>      select cover-file
-p, --passphrase    embed into the file <filename>
-p <passphrase>     specify passphrase
-sf <stegofile>    select stego-file
-of <filename>      write result to <filename> instead of cover-file
-e, --encryption    select encryption parameters
-a <a>[<m>]<n>[<a>]  specify an encryption algorithm and/or mode
-n, --none           do not encrypt data before embedding
-z, --compress      compress data before embedding (default)
-x <level>          using level <l> (1 best speed...9 best compression)
-Z, --dontcompress  do not compress data before embedding
-N, --nochecksum    do not embed md5 checksum of embedded data
-N, --nointembedname do not embed the name of the original file
-f, --force          overwrite existing files
-q, --quiet          suppress information messages
-v, --verbose        display detailed information

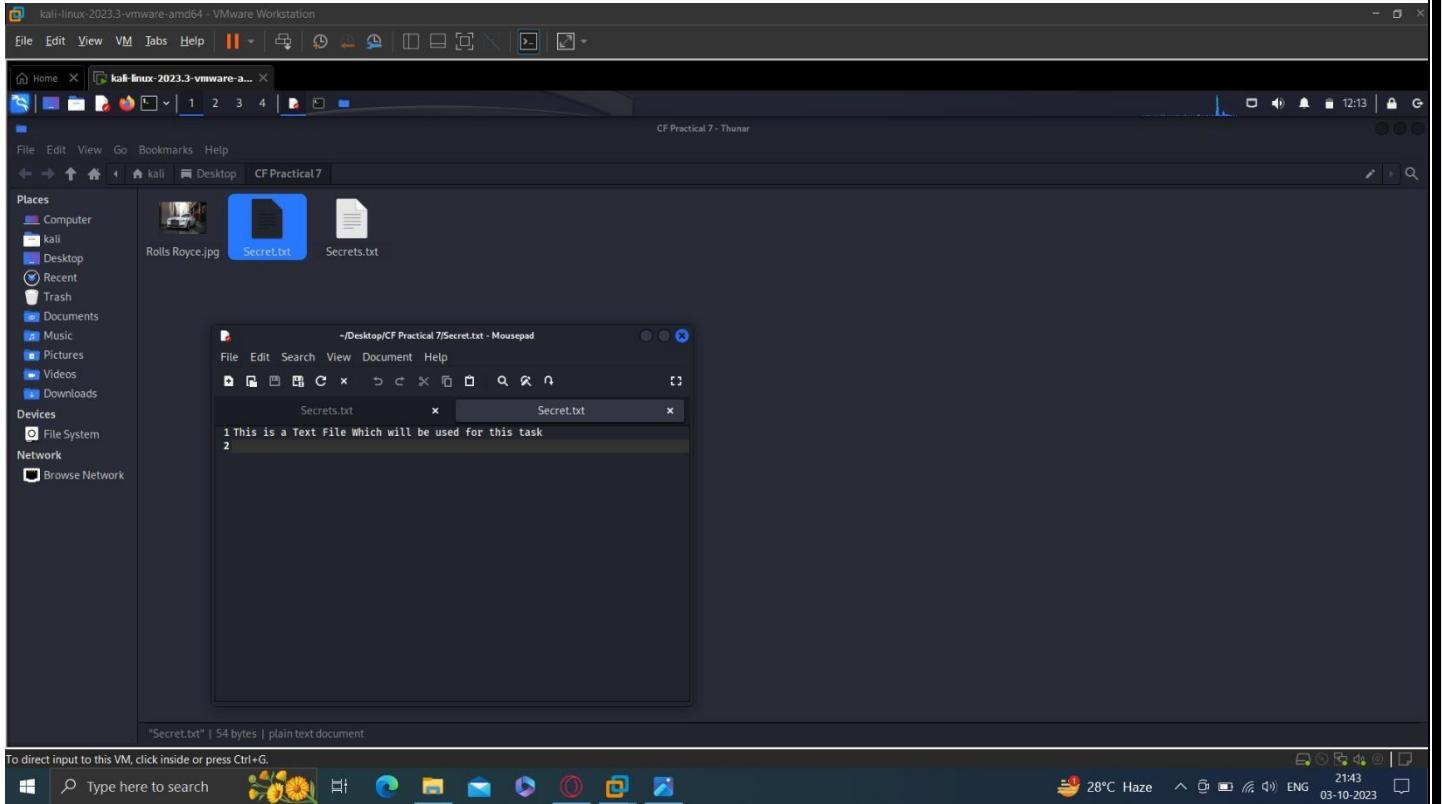
extracting options:
-sf <stegofile>    select stego-file
-xf <filename>      extract data from <filename>
-p, --passphrase    specify passphrase
-p <passphrase>     use <passphrase> to extract data
-xf, --extractfile  select file name for extracted data
-xf <filename>      write extracted data to <filename>
-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]# 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

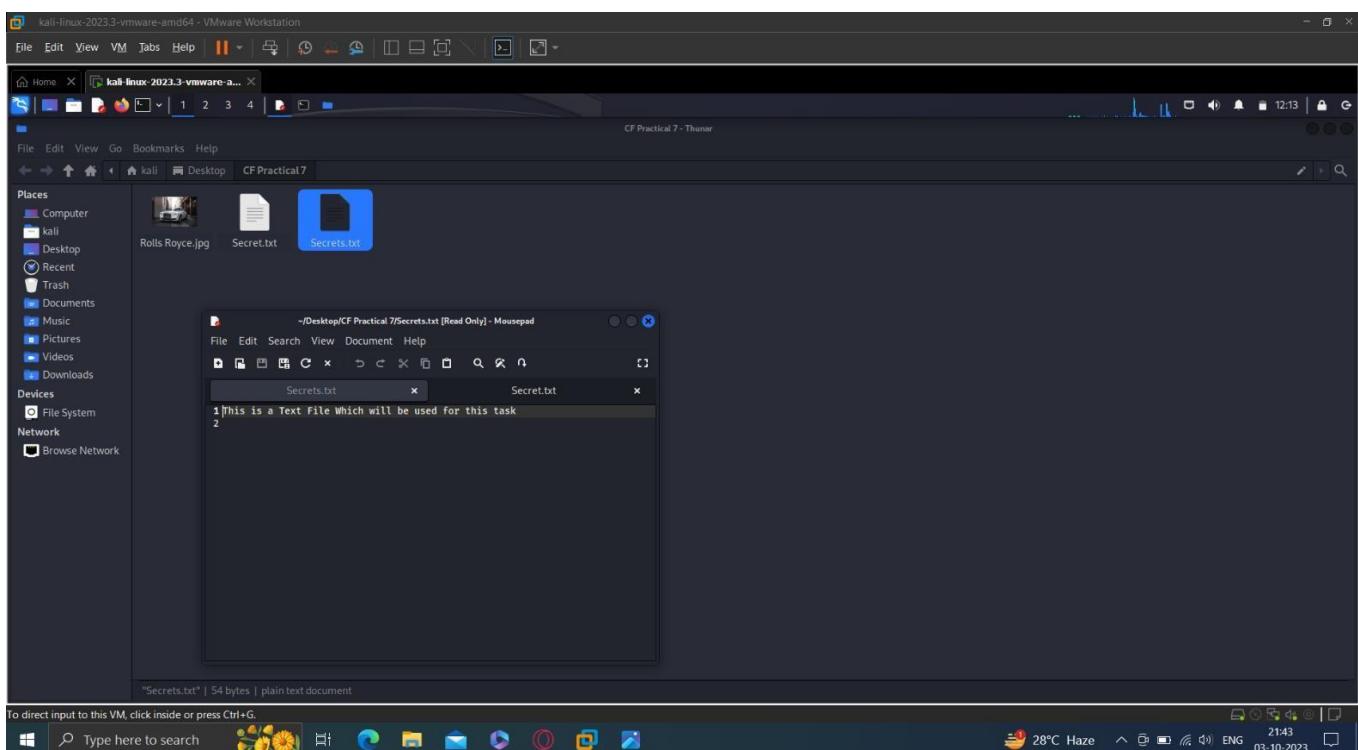
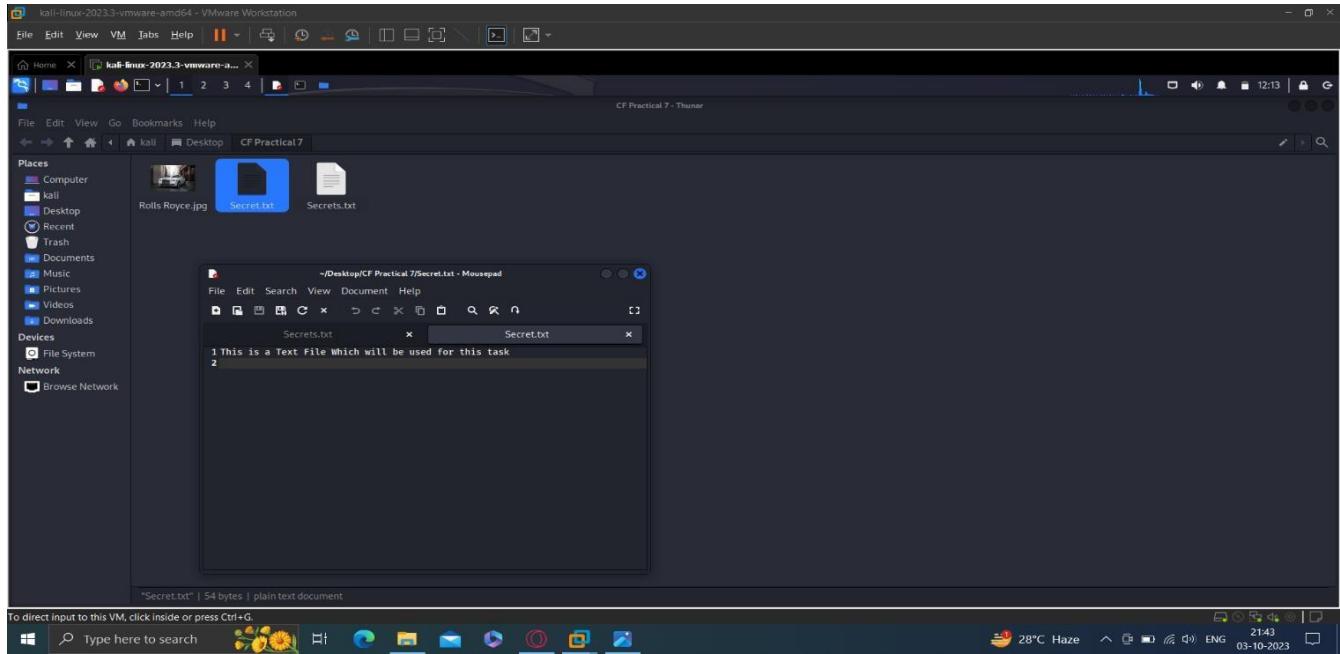
Here -ef means embed File which is the File to be Embedded i.e the txt file from which we want to hide the text in the Image and -cf means cover file i.e the file in which we want to hide the text

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

```
[root@kali]# 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".
```

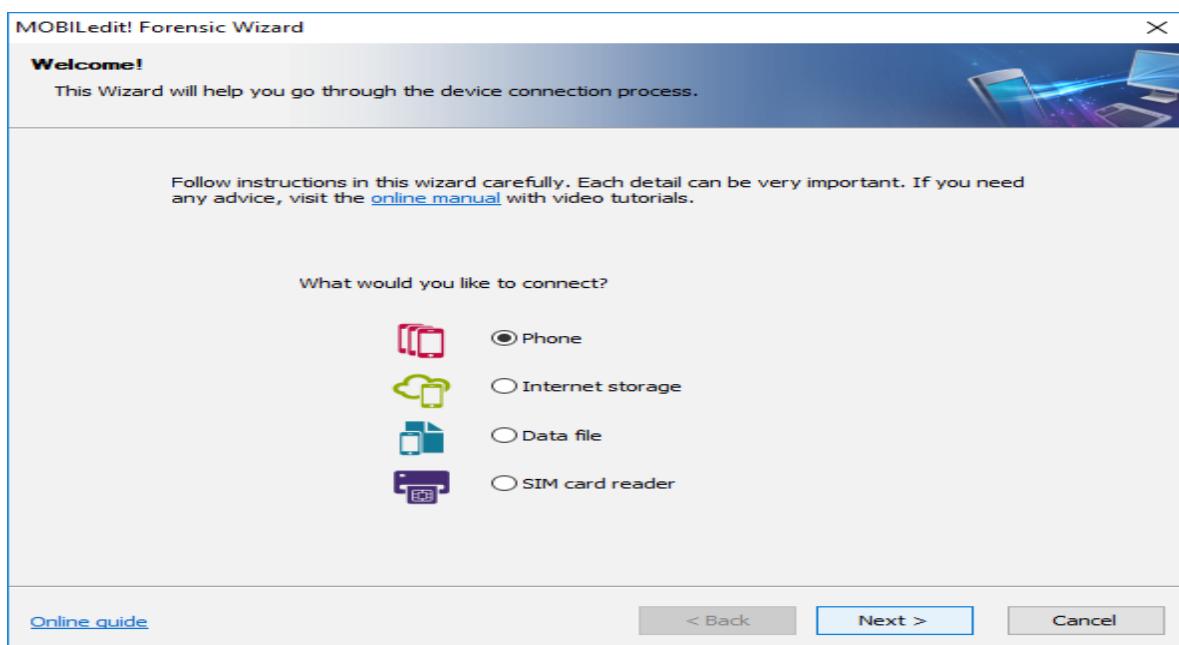
To do this use Above Command

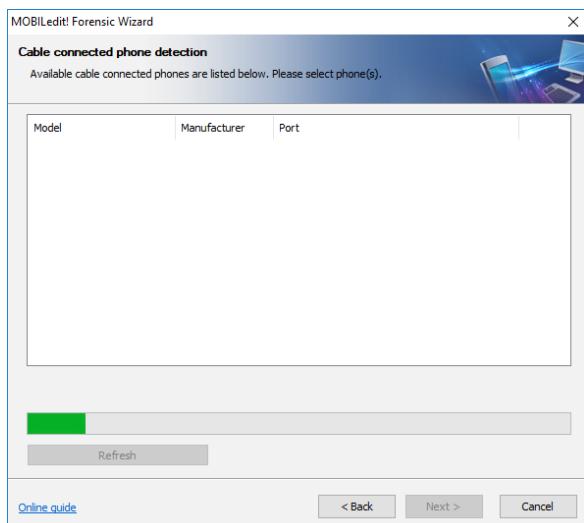
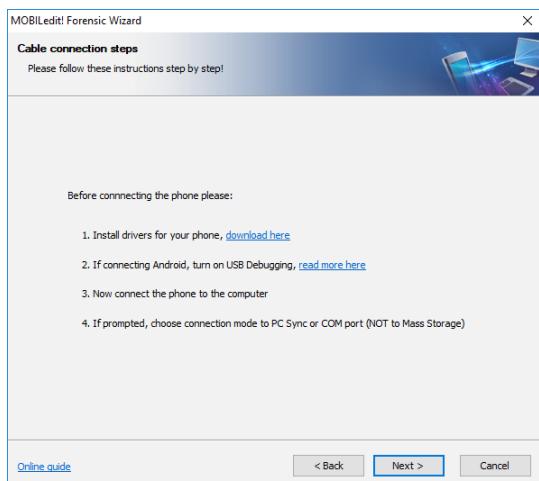
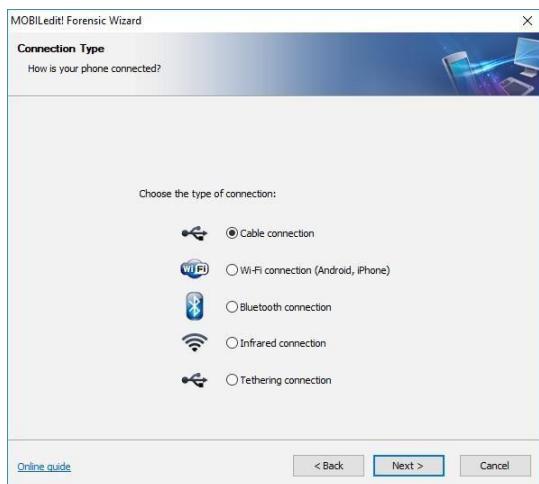
Here -sf Means Stego File i.e the File From which we want to extract the Hidden data and -xf means extractfile i.e the File in which the Hidden Data Will be Extracted

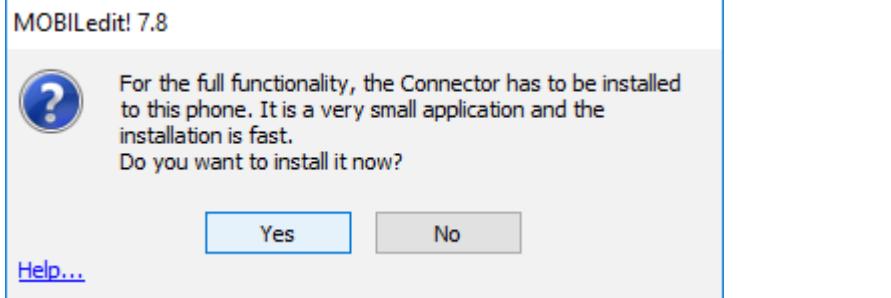


## PRACTICAL 8

Aim :- Acquisition of Cell phones and Mobile devices .







Working...

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

Cancel

MOBILedit! Forensic Wizard

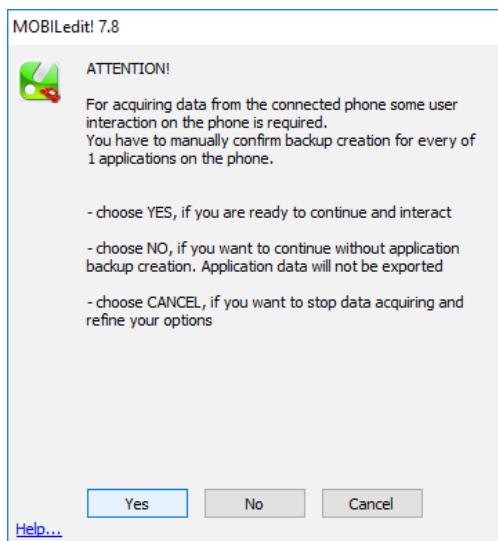
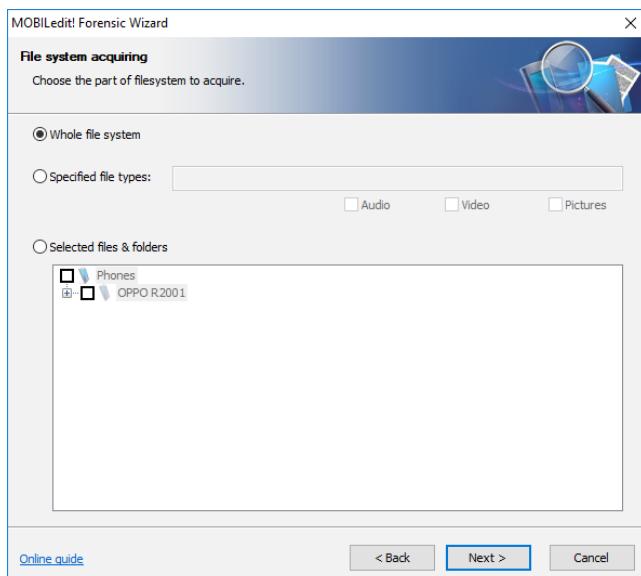
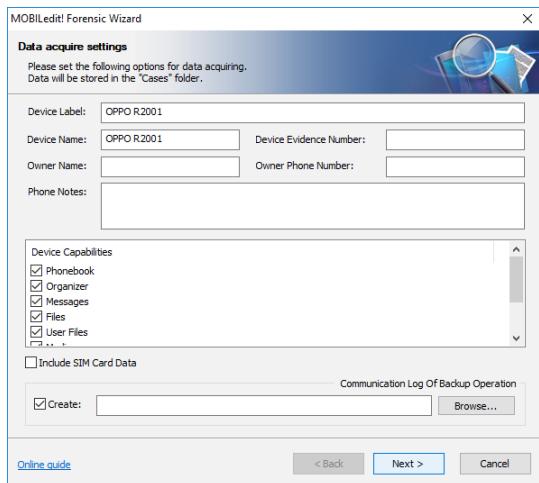
Cable connected phone detection

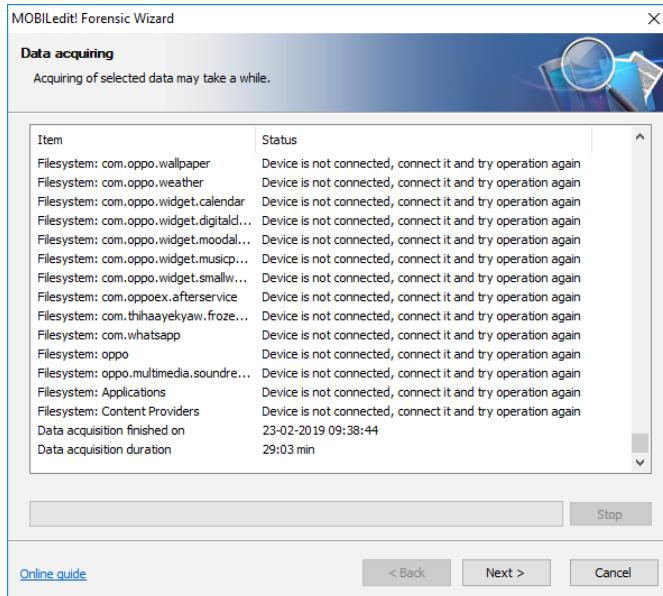
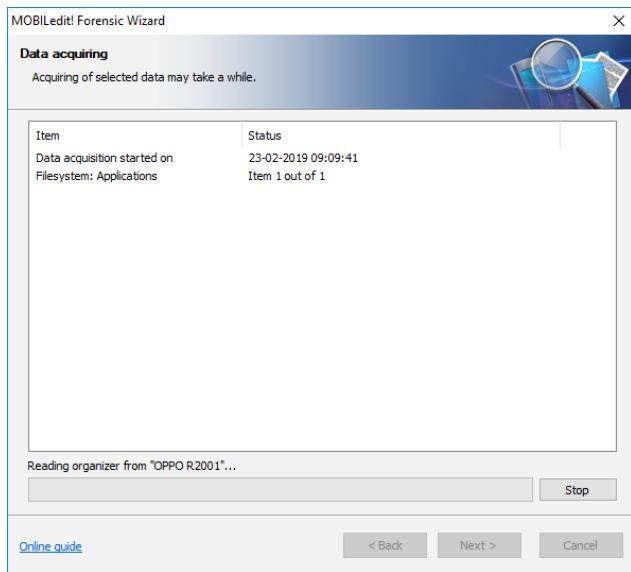
Available cable connected phones are listed below. Please select phone(s).

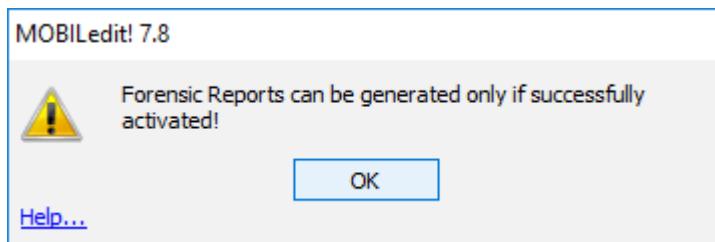
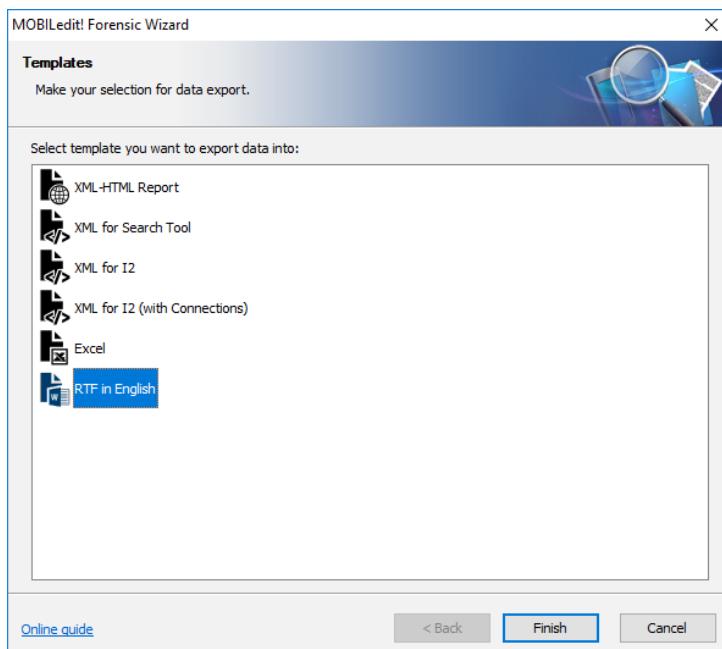
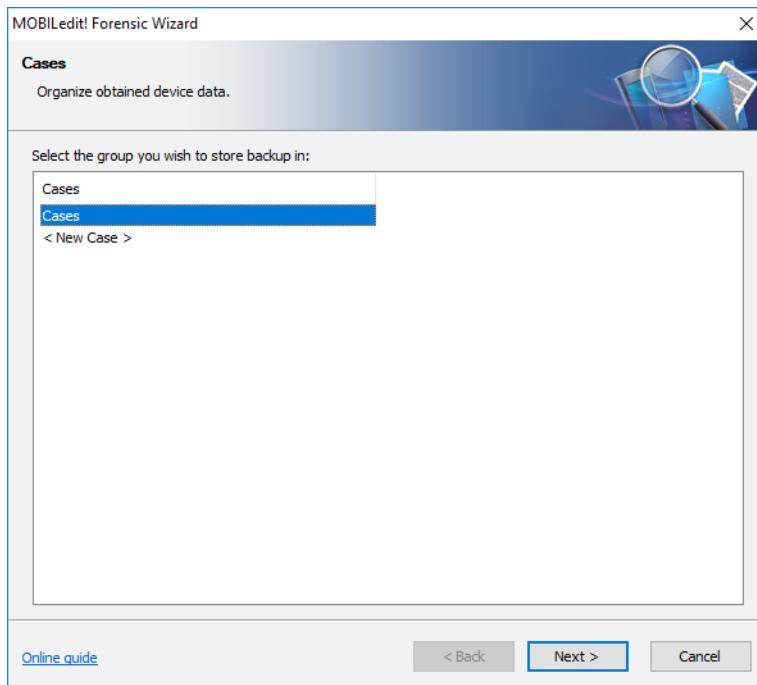
Model	Manufacturer	Port
<input checked="" type="checkbox"/> R2001	OPPO	Android 1134B6EC

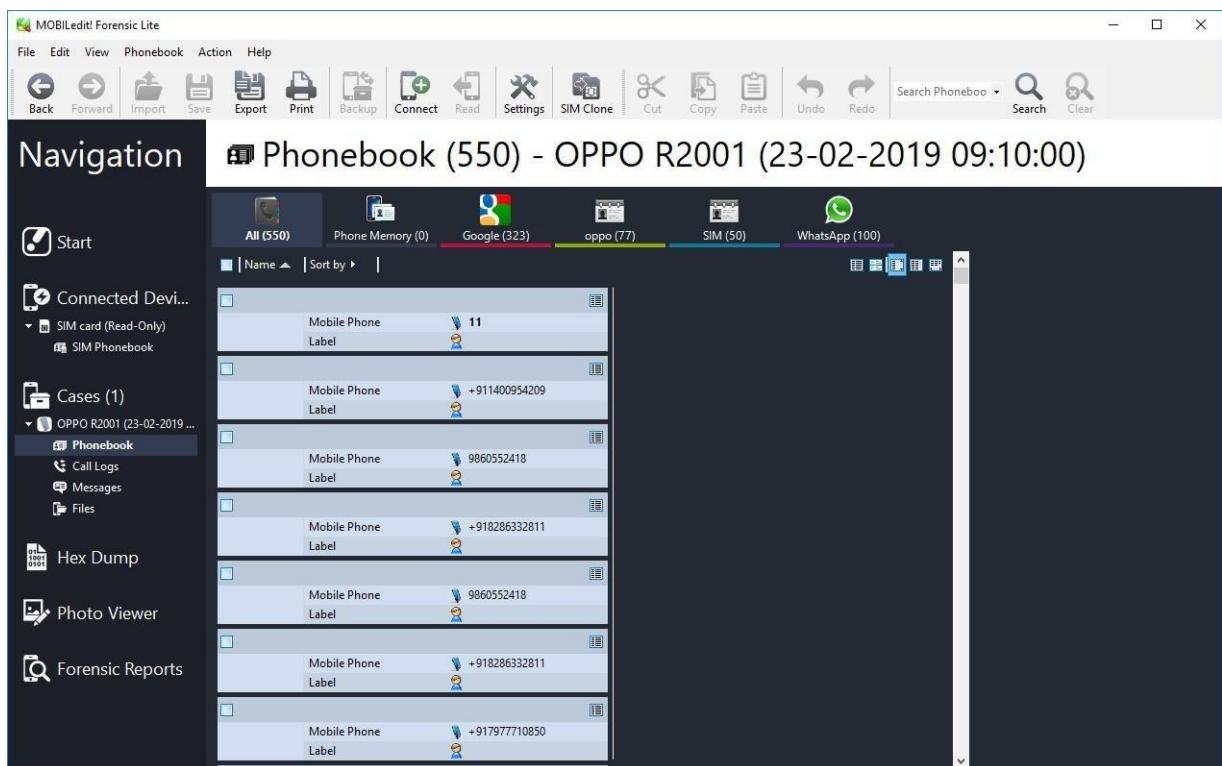
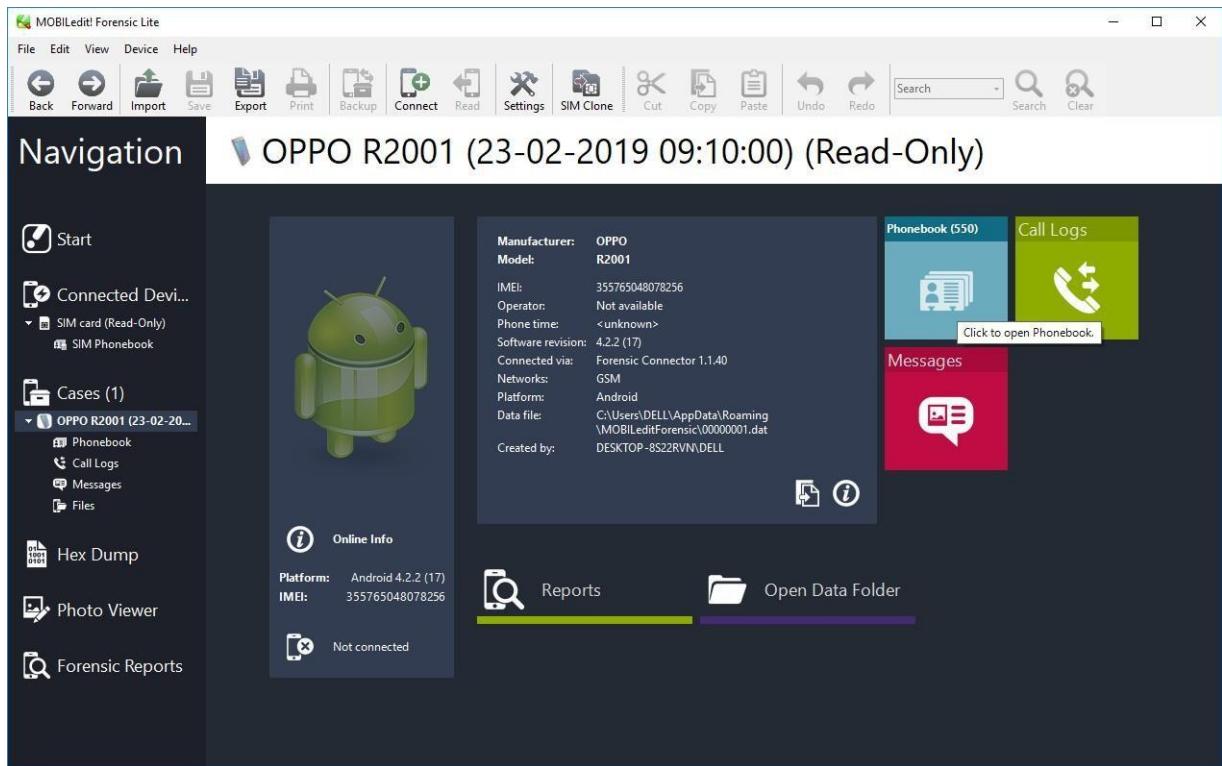
Refresh      Why is my phone not listed?

Online guide      < Back      Next >      Cancel









**Navigation**

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

Name	Number	Date	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 IV	+918779088436	17-02-2019	21:44:42
Aanad IV	+918779088436	17-02-2019	21:29:40

**Navigation**

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

Conversation	Date	Time	Recipient
55256	23-02-2019	08:25:27	55256
IZ-IDEA	22-02-2019	20:55:25	55256
Aaaaa	22-02-2019	17:19:31	55256
IM-655456	22-02-2019	14:46:43	55256
IM-612345	22-02-2019	14:15:48	55256
IM-6554563	22-02-2019	10:34:12	55256
+919987501727	21-02-2019	16:52:49	55256
MD-KOTAKB	21-02-2019	16:44:12	55256
AX-IYCGOV	21-02-2019	12:05:36	55256
IM-657886			55256

## **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.

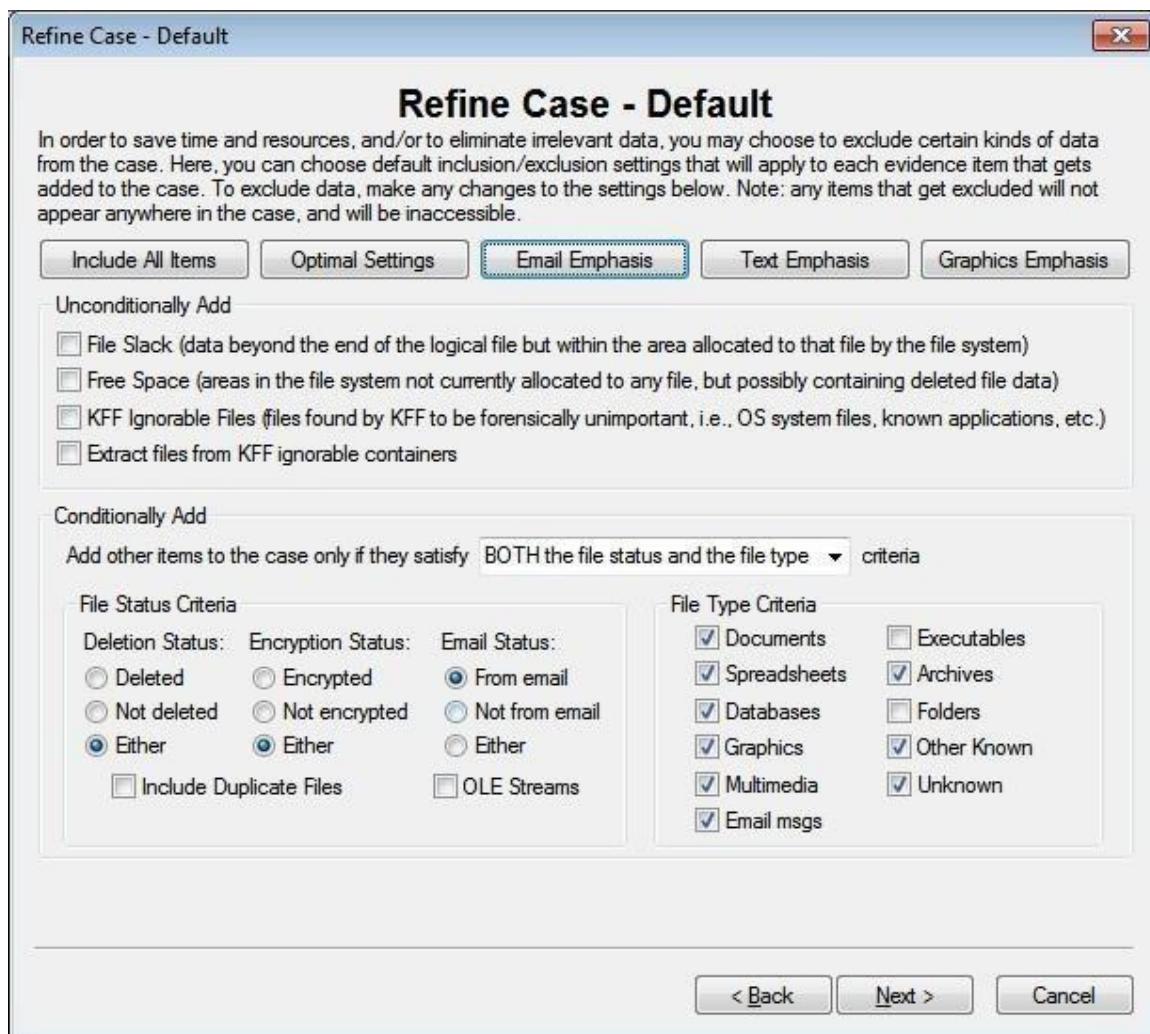
Martha asked her CIO, to have an IT employee copy the Outlook .pst file from Jim Shu's old computer to a USB drive.

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**

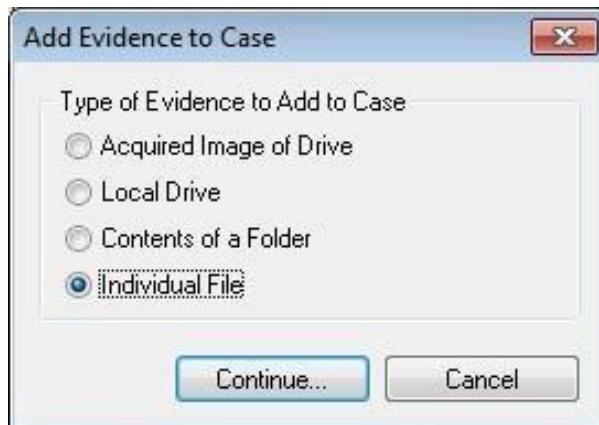
Start AccessData FTK and click **Start a new case**, then click **OK**. Click **Next** until you reach the **Refine Case - Default** dialog box Click the **Email Emphasis** button , and then click **Next** .

---

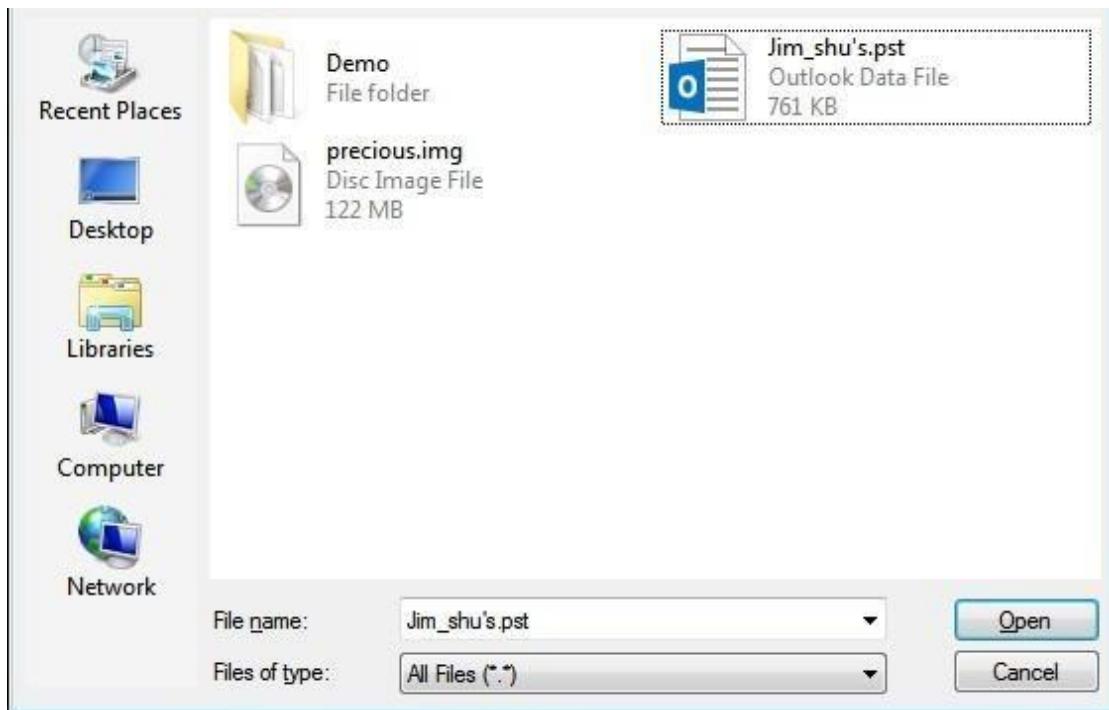


Click **Next** until you reach the **Add Evidence to Case** dialog box, and then click the **Add Evidence** button.

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:\CP\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
<b>Unfiltered</b>	<b>Filtered</b>	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: Bicyc..."	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: Bicyc..."	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:\CP\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 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
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

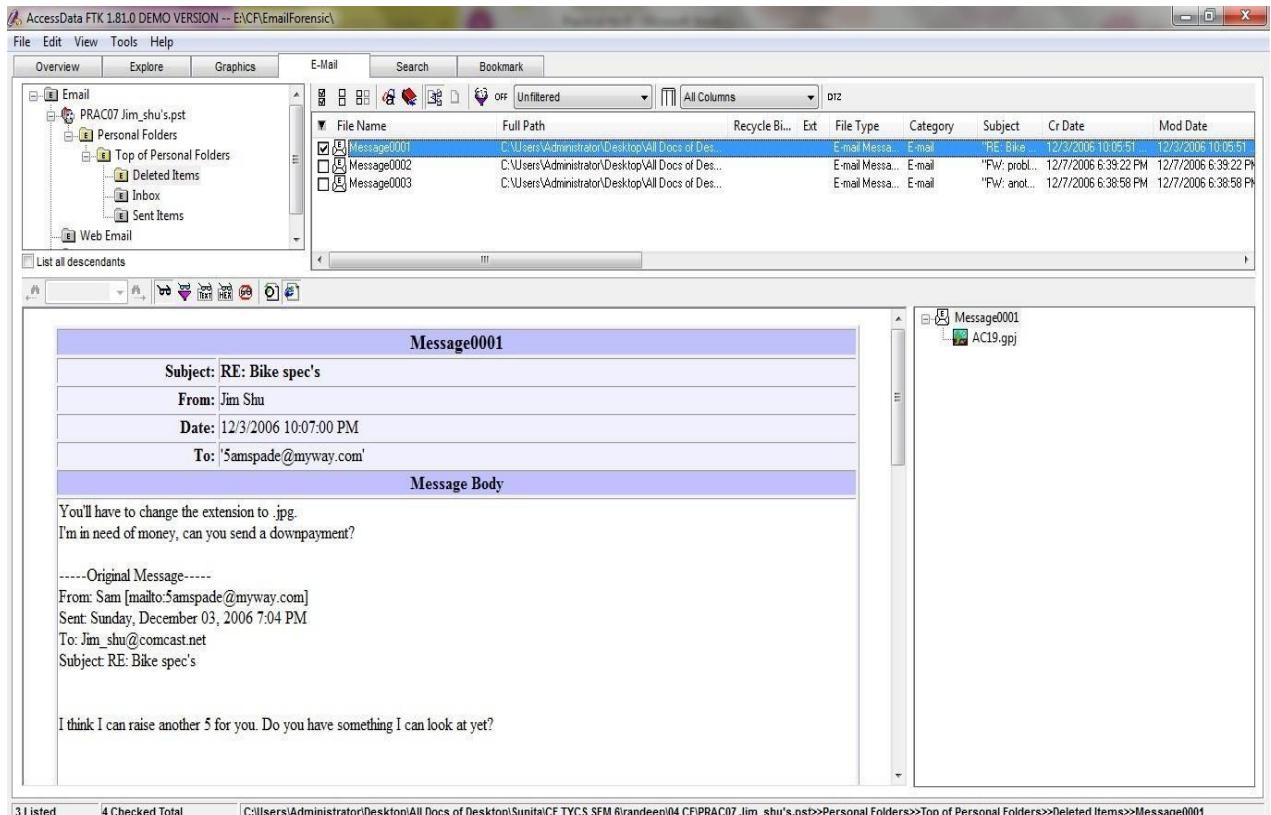
Default Container Folder

Deleted Items folder

3 Listed 3 Checked Total 0 Highlighted

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: Bicycl..."	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: Bicycl..."	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: Bicycl..."	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: Bicycl..."	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

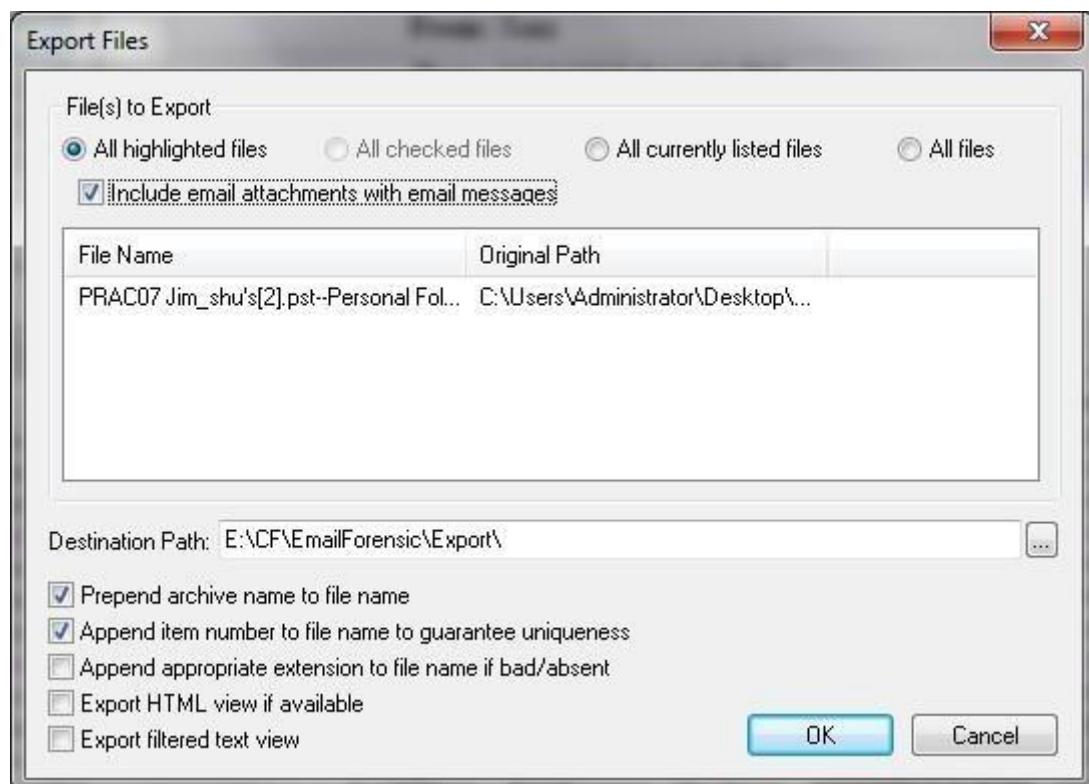
Message0003

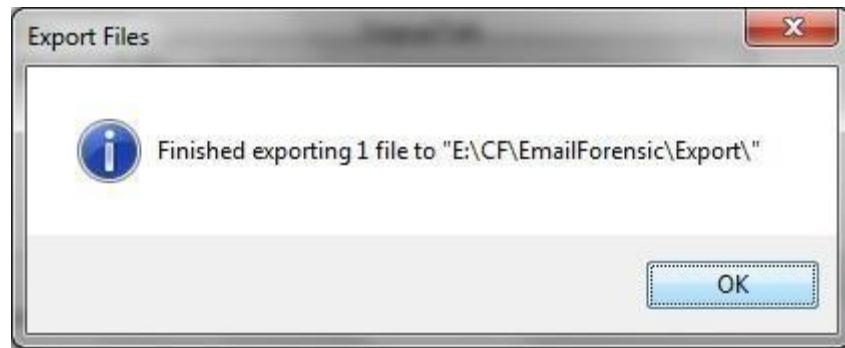
Subject: RE: Bike spec's  
 From: Sam  
 Date: 12/3/2006 9:14:02 PM  
 To: Jim\_shu@comcast.net

Message Body

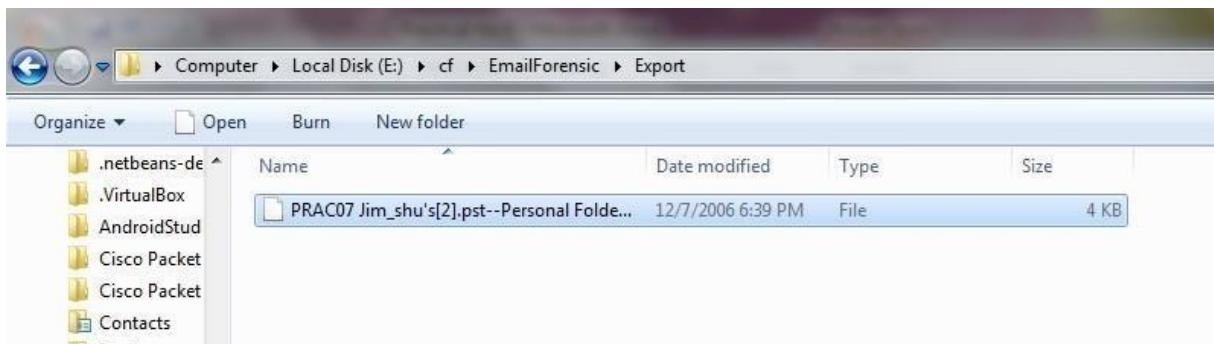
We might be able to go \$4000 if it is good. Is it? Sam

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

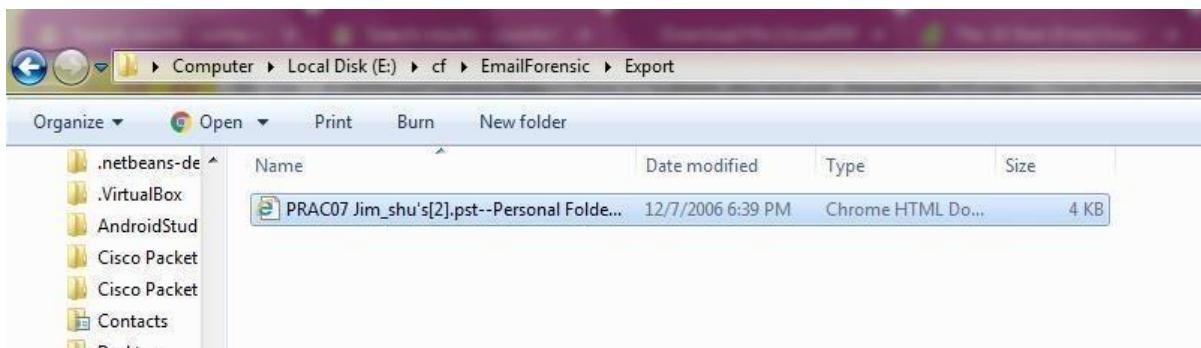




FTK saves exported files in the HTML format with no extension.



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.excitemail.com[207.159.120.55](untrusted sender)) by alnrmxc23.comcast.net (alnrmxc23) with ESMTP id <20061204021402a2300190t3e>; 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 mprdmailfe3.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

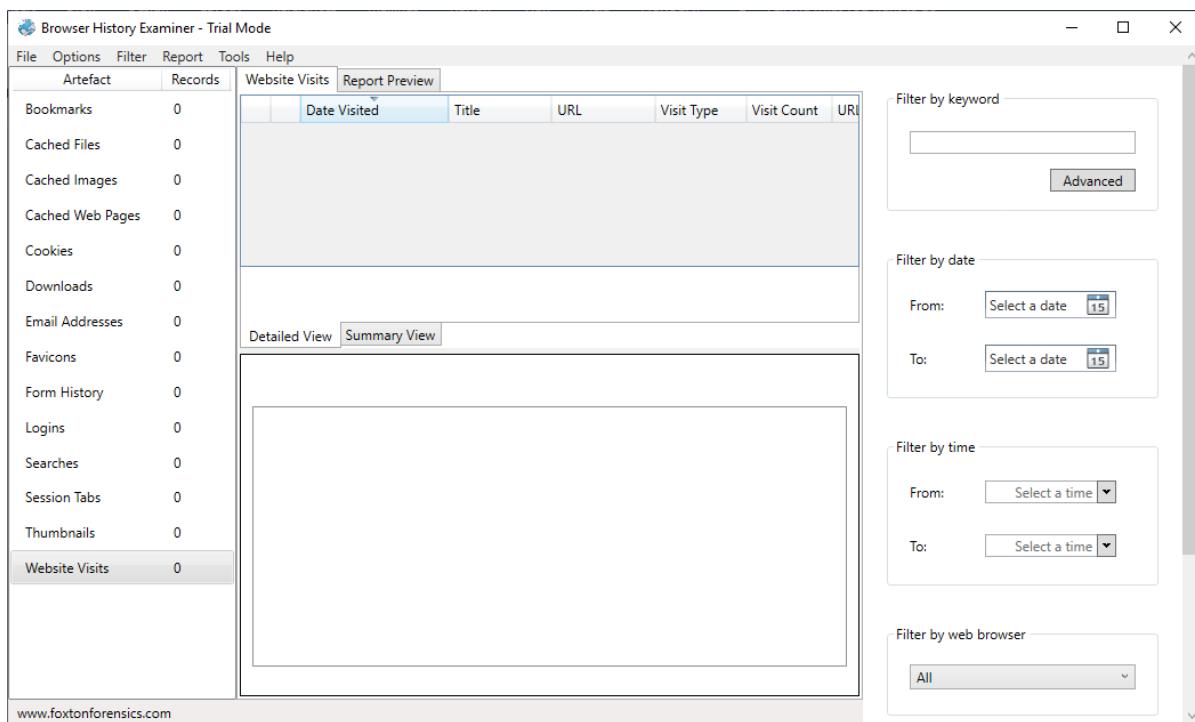
## **PRACTICAL 10**

Aim: Web Browser Forensics .

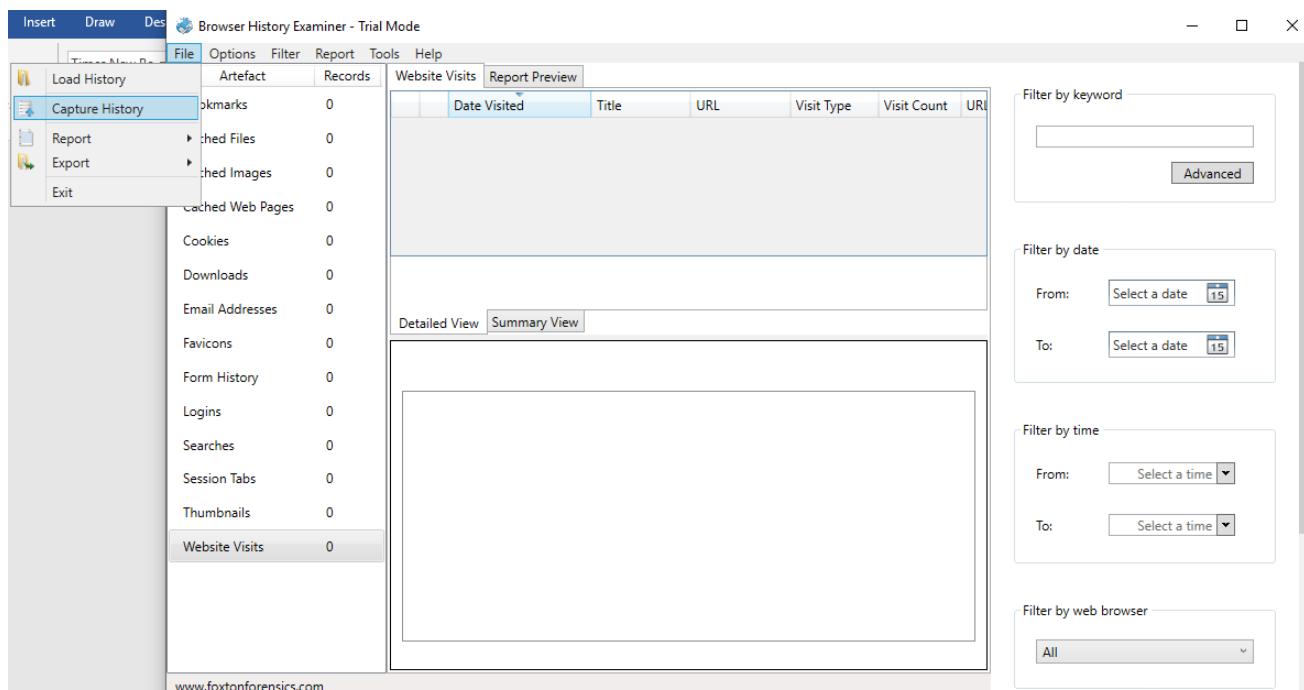
- Web Browser working
- Forensics activities on browser
- Cache / Cookies analysis
- Last Internet activity

### **Steps:**

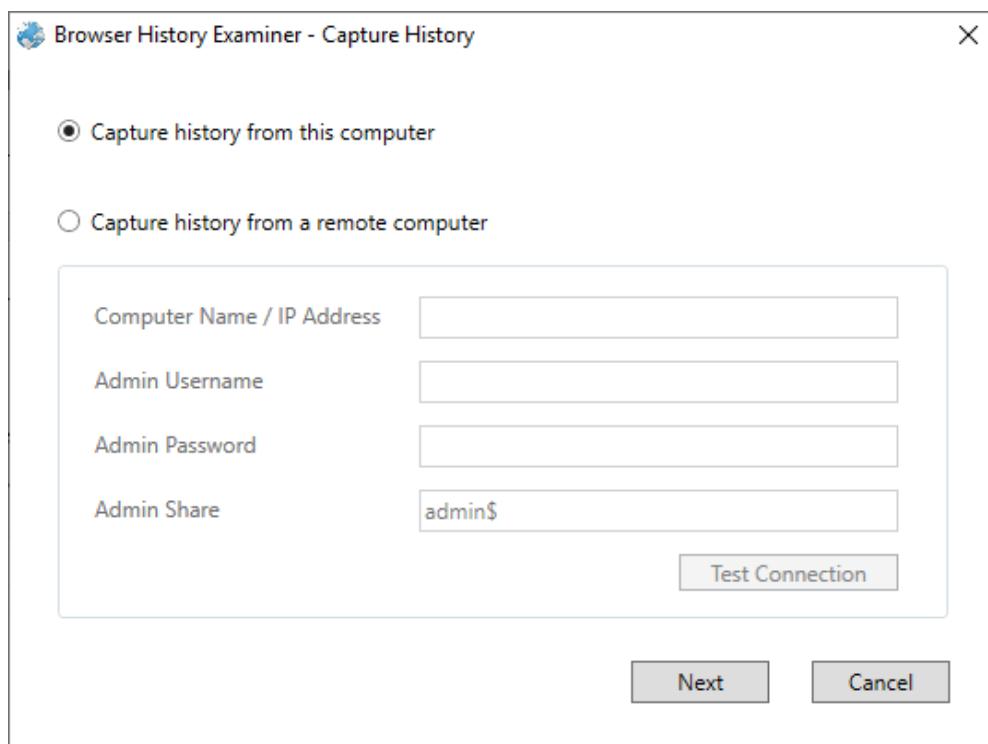
1. Open BrowserHistoryExaminer.



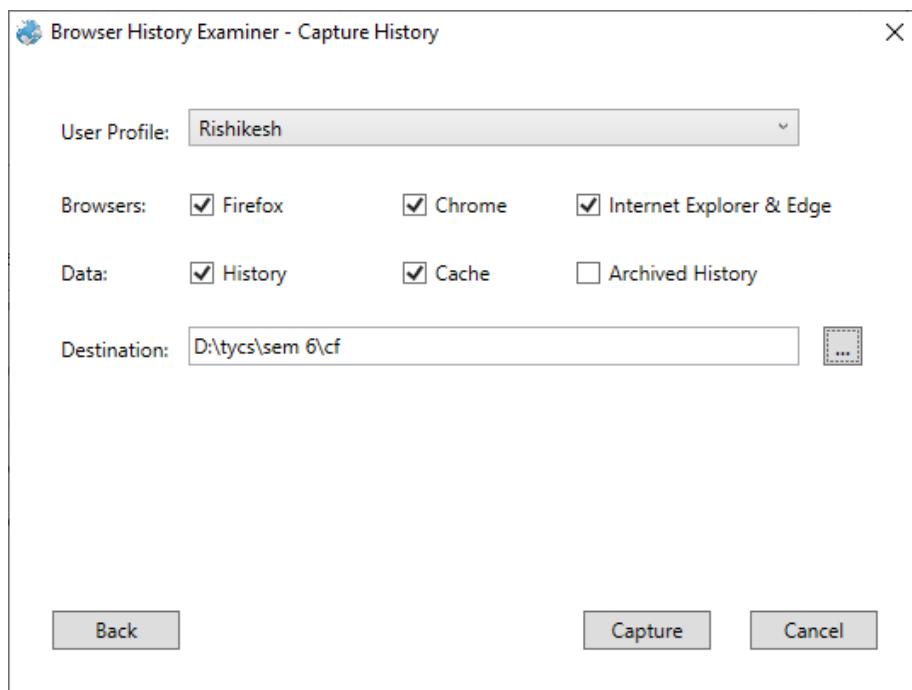
2. Click on file > Capture History



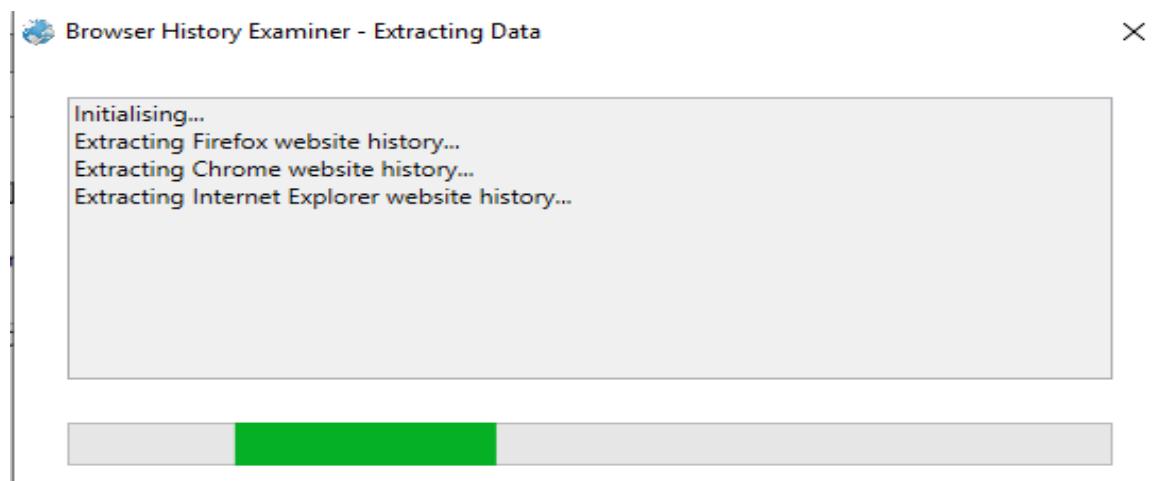
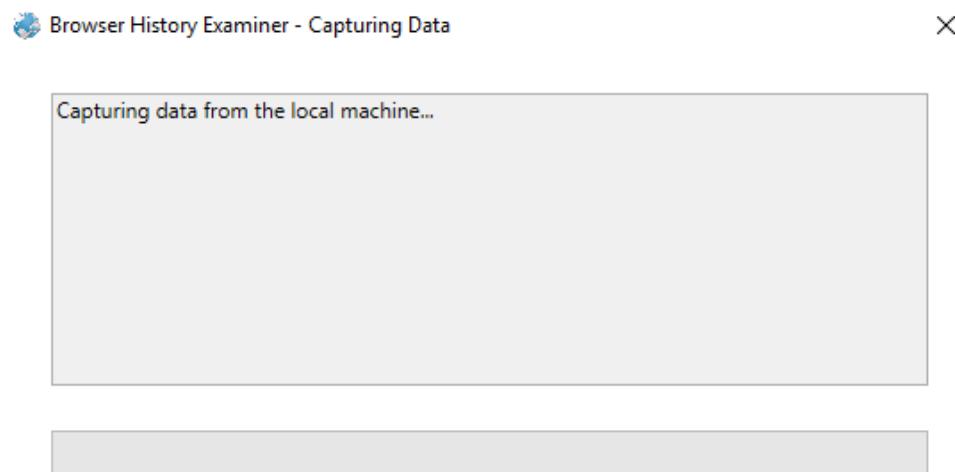
3. Select the capture folder and click on next.



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.nof		

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.

The screenshot shows the 'Browser History Examiner - Trial Mode' application window. The left sidebar lists various history types 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 'Cached Files' tab is currently selected. The main pane displays a table of cached files with columns: Last Fetched, Content Type, UI, Fetch Count, File Size (Bytes), and Web. The table contains 25 records. The first few rows show entries like 'application/zip' with a fetch count of 1 and file sizes ranging from 3523651 to 18820976 bytes. The interface includes a filter section on the right for keyword, date, time, and web browser, and navigation controls at the bottom.

9. On the left panel click on cached images.

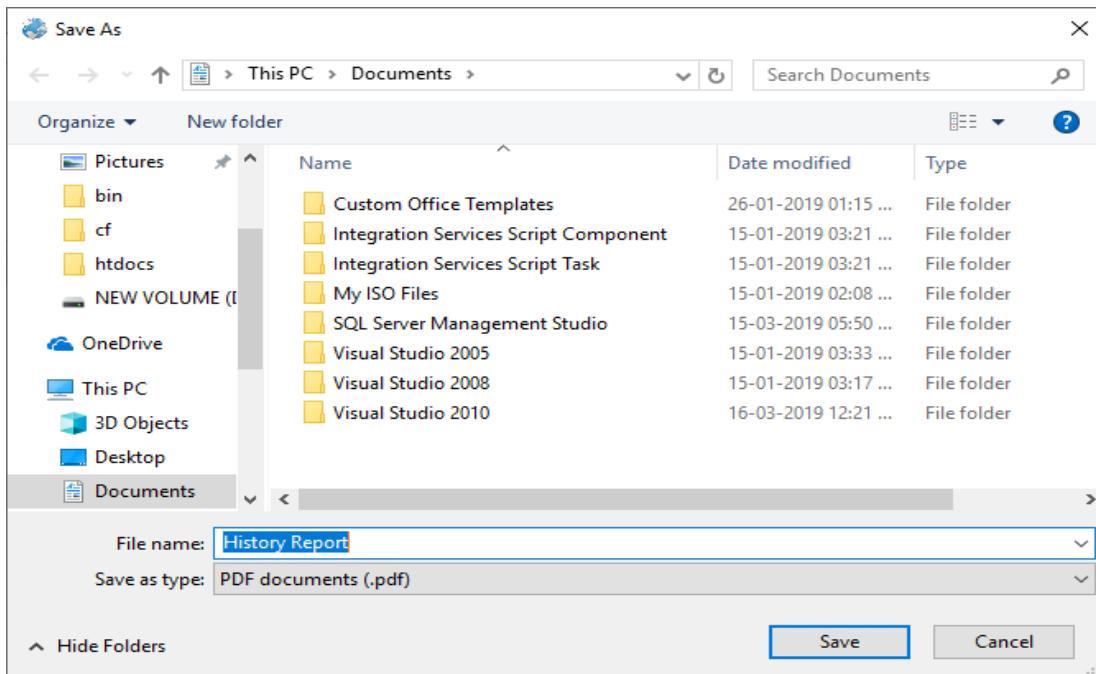
The screenshot shows the 'Browser History Examiner - Trial Mode' application window. The left sidebar lists various history types with their counts. The 'Cached Images' tab is currently selected. The main pane displays a table of cached images with columns: Last Fetched, Content Type, UI, Fetch Count, File Size (Bytes), and Web. The table contains 25 records. The first few rows show images with content types like 'image/jpeg' and 'image/png', fetch counts of 1 or 2, and file sizes ranging from 491093 to 1150328 bytes. Below the table, several thumbnail previews of the cached images are displayed. The interface includes a filter section on the right for keyword, date, time, and web browser, and navigation controls at the bottom.

10. On the left panel click on cookies.

	Date Created	UI	Last Accessed	Date Expires	N	C	W
17-03-2019 20:32:32	ac	17-03-2019 20:32:32	17-03-2019 20:32:42	Ch	Ch		
17-03-2019 20:32:31	ac	17-03-2019 20:32:31	16-03-2021 20:32:31	GA	Ch		
17-03-2019 20:32:30	mi	17-03-2019 20:32:30	18-03-2019 20:32:30	GM	Ch		
17-03-2019 20:32:30	.gc	17-03-2019 20:32:30	16-09-2019 21:32:30	NI	Ch		
17-03-2019 20:05:48	mi	17-03-2019 20:05:48	27-03-2019 21:05:49	CC	Ch		
17-03-2019 20:05:26	mi	17-03-2019 20:17:27	27-03-2019 21:05:26	CC	Ch		
17-03-2019 20:05:24	.gc	17-03-2019 20:32:29	16-04-2019 21:05:24	IP	Ch		
17-03-2019 20:05:22	mi	17-03-2019 20:32:29	27-03-2019 21:05:23	CC	Ch		
17-03-2019 20:05:22	mi	17-03-2019 20:32:26		GM	Ch		
17-03-2019 20:05:21	.gc	17-03-2019 20:05:21	16-03-2021 20:05:21	AP	Ch		
17-03-2019 20:05:21	.gc	17-03-2019 20:05:21	16-03-2021 20:05:21	HS	Ch		
17-03-2019 20:05:21	.gc	17-03-2019 20:05:21	16-09-2019 21:05:21	NI	Ch		
17-03-2019 20:05:21	.gc	17-03-2019 20:05:21	16-03-2021 20:05:21	SA	Ch		
17-03-2019 20:05:21	.gc	17-03-2019 20:05:21	16-03-2021 20:05:21	SIL	Ch		
17-03-2019 20:05:21	.gc	17-03-2019 20:05:21	16-03-2021 20:05:21	SS	Ch		
17-03-2019 20:04:46	wv	17-03-2019 20:04:46		AS	Ch		
17-03-2019 20:04:46	.fo	17-03-2019 20:04:46	17-03-2019 20:05:46	_g	Ch		
17-03-2019 20:04:46	.fo	17-03-2019 20:04:53	16-03-2021 20:04:53	_g	Ch		
17-03-2019 20:04:46	.fo	17-03-2019 20:04:53	18-03-2019 20:04:53	_g	Ch		
17-03-2019 20:04:42	.gc	17-03-2019 20:04:42	16-09-2019 21:04:42	SN	Ch		
17-03-2019 09:04:09	wv	17-03-2019 09:04:09	17-03-2019 09:14:09	DV	US	Fir	
17-03-2019 09:03:37	.ac	17-03-2019 09:16:27	10-04-2020 10:03:37	ou	5c	Fir	
17-03-2019 09:03:37	.ac	17-03-2019 09:16:27	10-04-2020 10:03:37	di	aU	Fir	v

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

	Date Created	UI	Last Accessed	Date Expires	N	C	W
17-03-2019 20:32:32	ac	17-03-2019 20:32:32	17-03-2019 20:32:42	Ch	Ch		
17-03-2019 20:32:31	ac	17-03-2019 20:32:31	16-03-2021 20:32:31	GA	Ch		
17-03-2019 20:32:30	mi	17-03-2019 20:32:30	18-03-2019 20:32:30	GM	Ch		
17-03-2019 20:32:30	.gc	17-03-2019 20:32:30	16-09-2019 21:32:30	NI	Ch		
17-03-2019 20:05:48	mi	17-03-2019 20:05:48	27-03-2019 21:05:49	CC	Ch		
17-03-2019 20:05:26	mi	17-03-2019 20:17:27	27-03-2019 21:05:26	CC	Ch		
17-03-2019 20:05:24	.gc	17-03-2019 20:32:29	16-04-2019 21:05:24	IP	Ch		
17-03-2019 20:05:22	mi	17-03-2019 20:32:29	27-03-2019 21:05:23	CC	Ch		
17-03-2019 20:05:22	mi	17-03-2019 20:32:26		GM	Ch		
17-03-2019 20:05:21	.gc	17-03-2019 20:05:21	16-03-2021 20:05:21	AP	Ch		
17-03-2019 20:05:21	.gc	17-03-2019 20:05:21	16-03-2021 20:05:21	HS	Ch		
17-03-2019 20:05:21	.gc	17-03-2019 20:05:21	16-09-2019 21:05:21	NI	Ch		
17-03-2019 20:05:21	.gc	17-03-2019 20:05:21	16-03-2021 20:05:21	SA	Ch		
17-03-2019 20:05:21	.gc	17-03-2019 20:05:21	16-03-2021 20:05:21	SIL	Ch		
17-03-2019 20:05:21	.gc	17-03-2019 20:05:21	16-03-2021 20:05:21	SS	Ch		
17-03-2019 20:04:46	wv	17-03-2019 20:04:46		AS	Ch		
17-03-2019 20:04:46	.fo	17-03-2019 20:04:46	17-03-2019 20:05:46	_g	Ch		
17-03-2019 20:04:46	.fo	17-03-2019 20:04:53	16-03-2021 20:04:53	_g	Ch		
17-03-2019 20:04:46	.fo	17-03-2019 20:04:53	18-03-2019 20:04:53	_g	Ch		
17-03-2019 20:04:42	.gc	17-03-2019 20:04:42	16-09-2019 21:04:42	SN	Ch		
17-03-2019 09:04:09	wv	17-03-2019 09:04:09	17-03-2019 09:14:09	DV	US	Fir	
17-03-2019 09:03:37	.ac	17-03-2019 09:16:27	10-04-2020 10:03:37	ou	5c	Fir	
17-03-2019 09:03:37	.ac	17-03-2019 09:16:27	10-04-2020 10:03:37	di	aU	Fir	v



## 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/?ui=2&ik=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=uYLNNeQAei1Ab4h7K4Cg&dur=152.733...		2097152	Chrome
		https://r3-sn-4p8xoxu-cvhe.googlevideo.com/videoplayback?ei=uYLNNeOA4ei1Ab4h7K4Co&dur=152.733...		2097152	Chrome
		https://r3-sn-4p8xoxu-cvhe.googlevideo.com/videoplayback?ei=uYLNNeOA4ei1Ab4h7K4Co&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			Date Added	Last Modified
Export	Export to Excel		17-03-2019 09:03:01	17-03-2019 09:03:01
	Export to HTML		17-03-2019 09:03:01	17-03-2019 09:03:01
	Export to CSV		17-03-2019 09:03:01	17-03-2019 09:03:01
	Export to XML		17-03-2019 09:03:01	17-03-2019 09:03:01
	Export to Concordance Load File		17-03-2019 09:03:01	17-03-2019 09:03:01
	Downloads	80	17-03-2019 09:03:01	17-03-2019 09:03:01
	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

Filter 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

