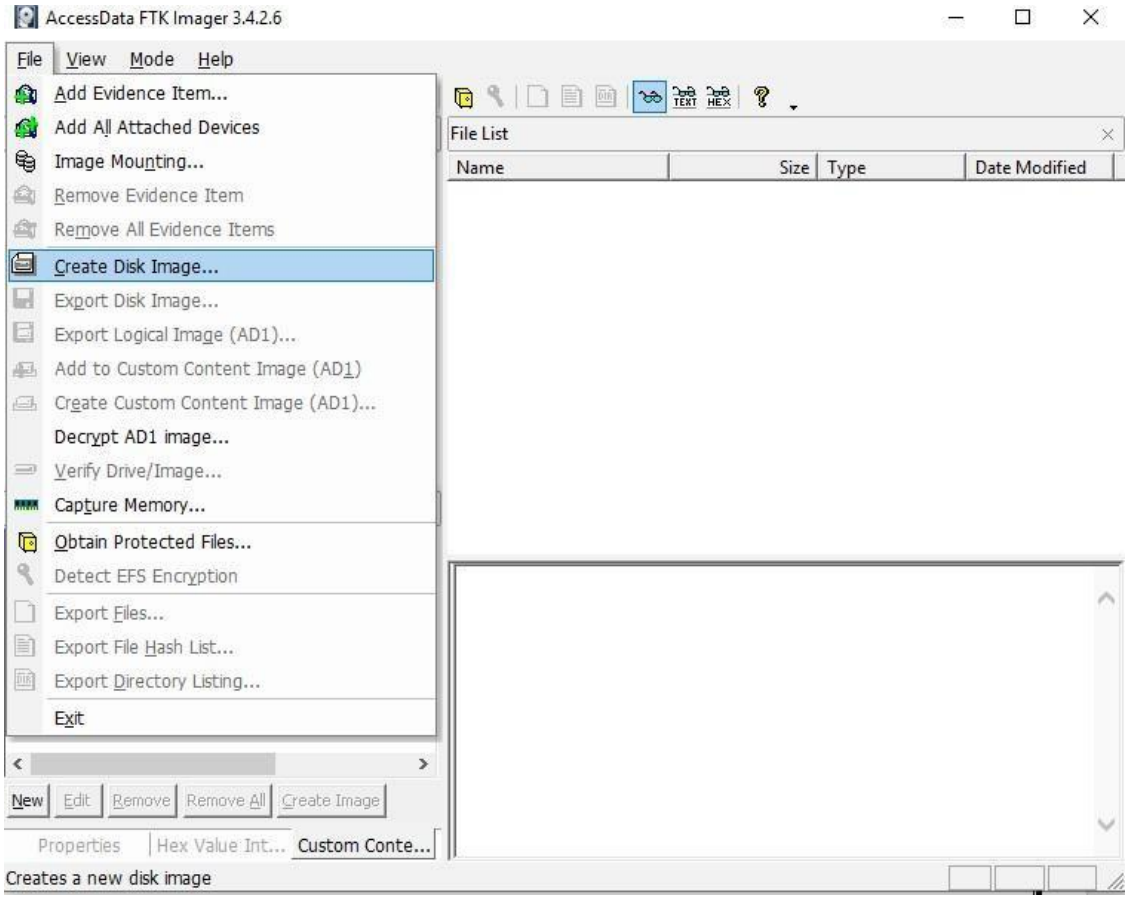
PRACTICAL 1

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

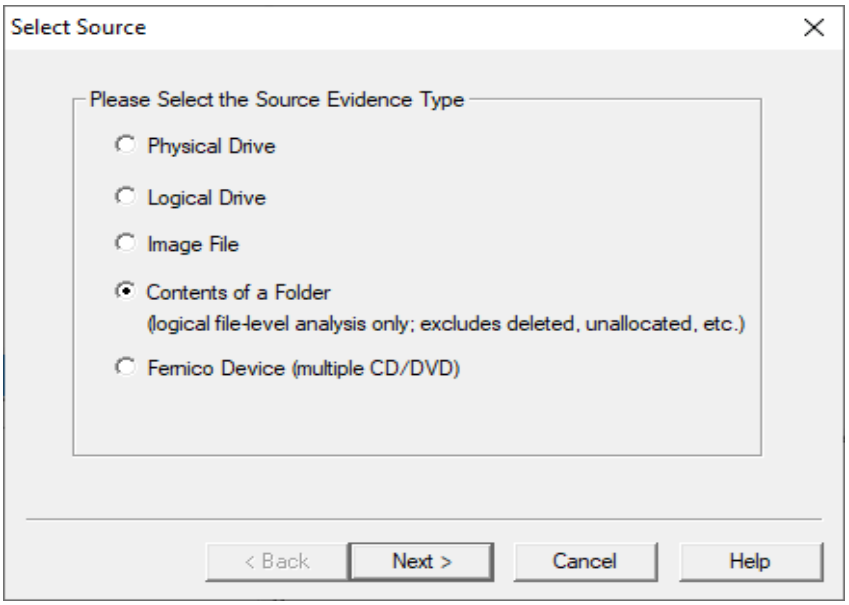
- Creating Forensic Image
- Check Integrity of Data
- Analyze Forensic Image

- Creating Forensic Image

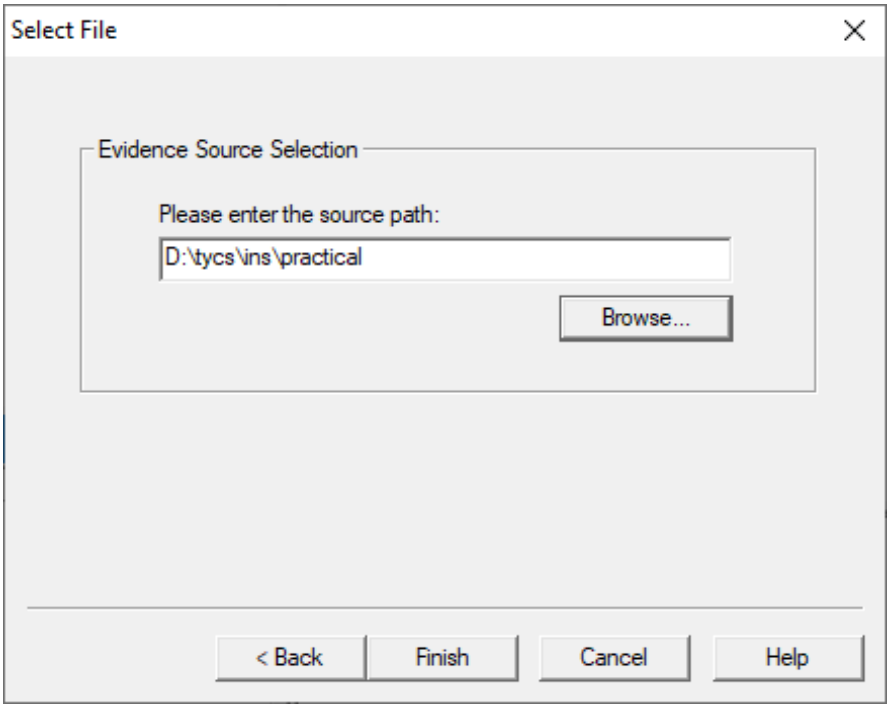
1. Click File, and then Create Disk Image, or click the button on the tool bar.



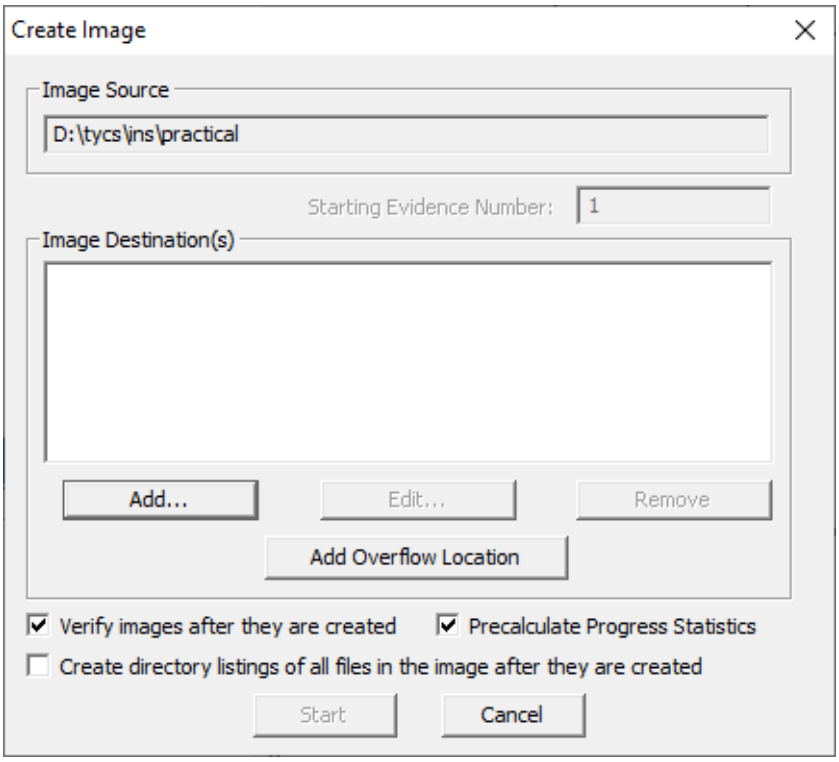
2. Select the source evidence type you want to make an image of and click Next.

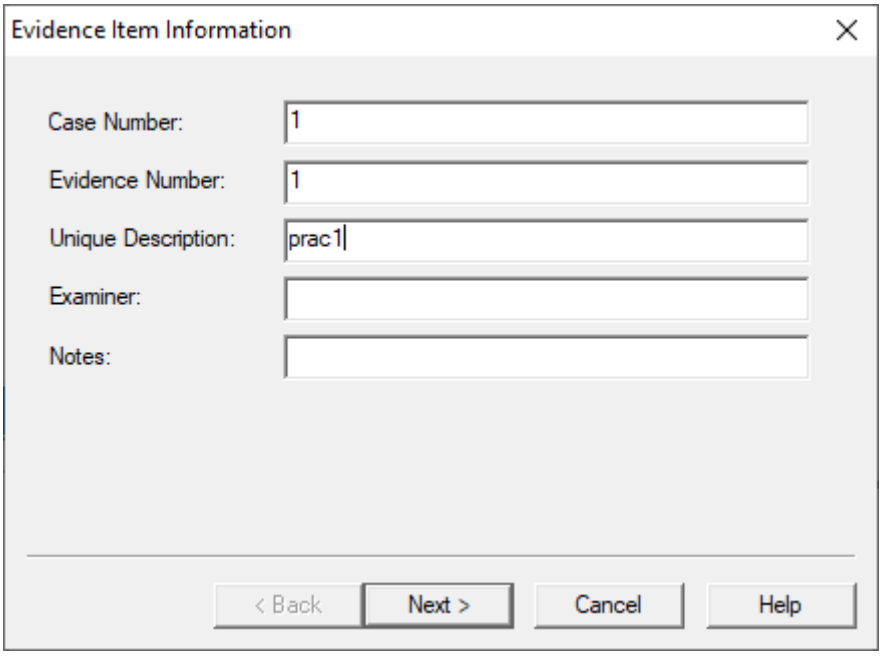


3. Select the source evidence file with path.



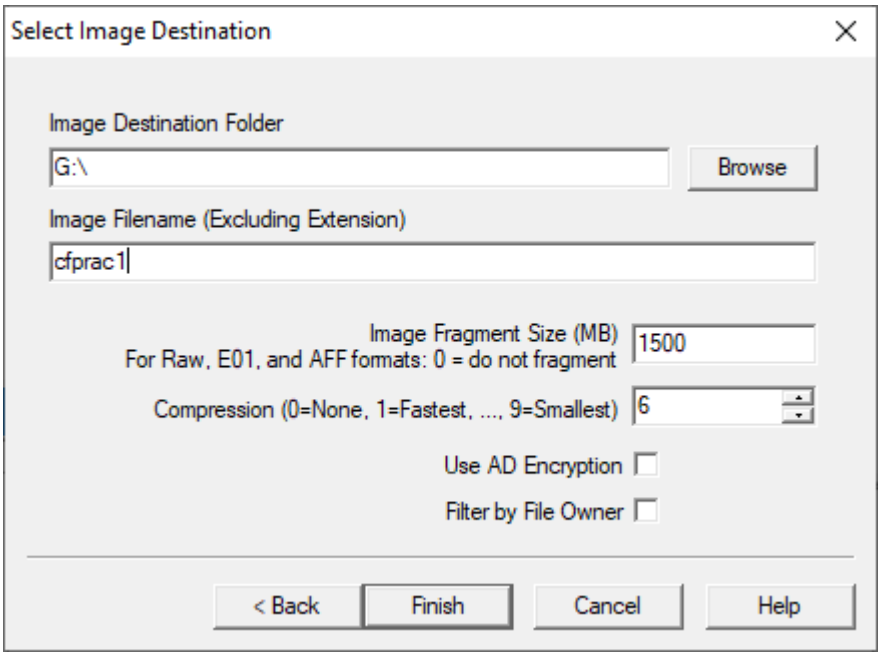
Click on “add” to add image destination



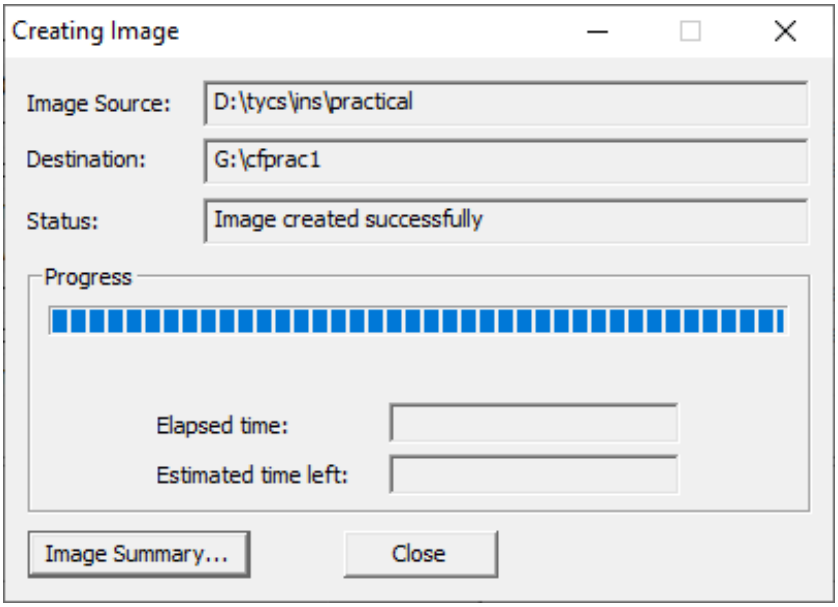


4. In the Image Destination Folder field, type the location path where you want to save the image file, or click **Browse** to find to the desired location.

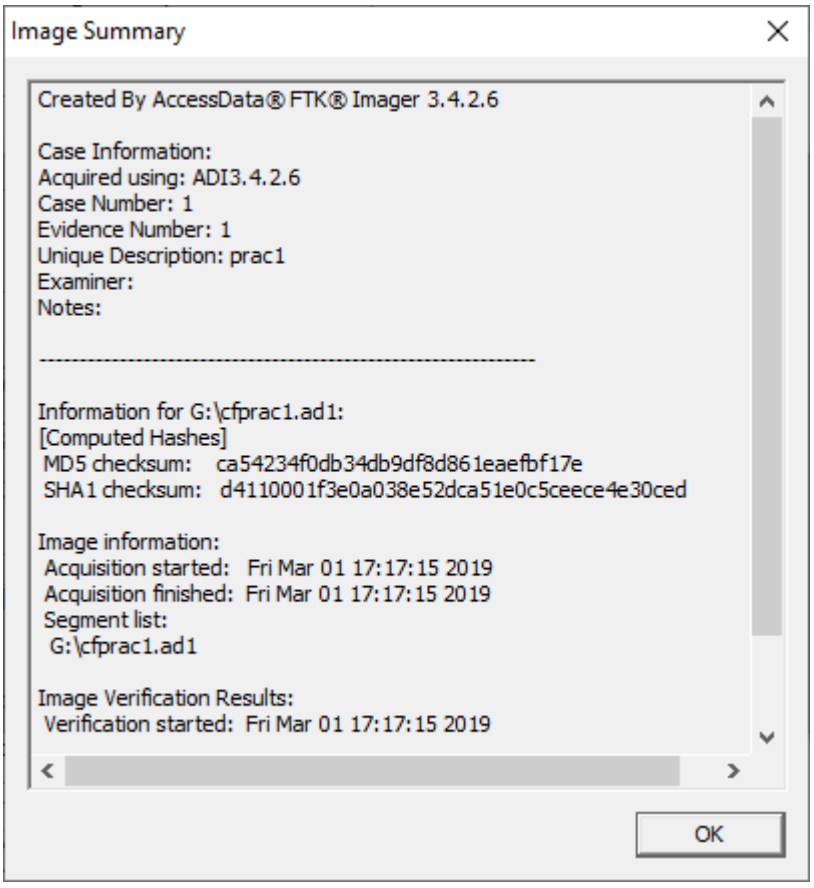
Note: If the destination folder you select is on a drive that does not have sufficient free space to store the entire image file, FTK Imager prompts for a new destination folder when all available space has been used in the first location.In the Image Filename field, specify a name for the image file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



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

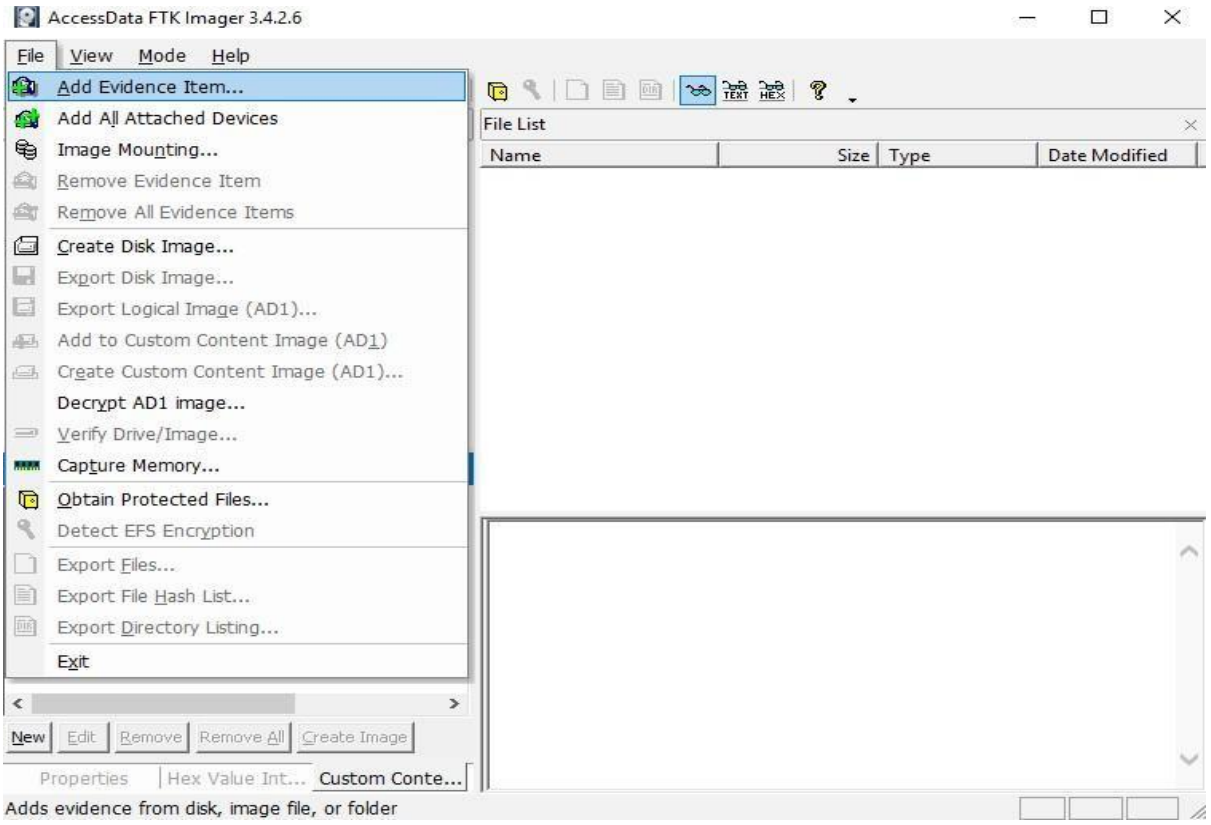


6. After the images are successfully created, click Image Summary to view detailed file information, including MD5 and SHA1 checksums.

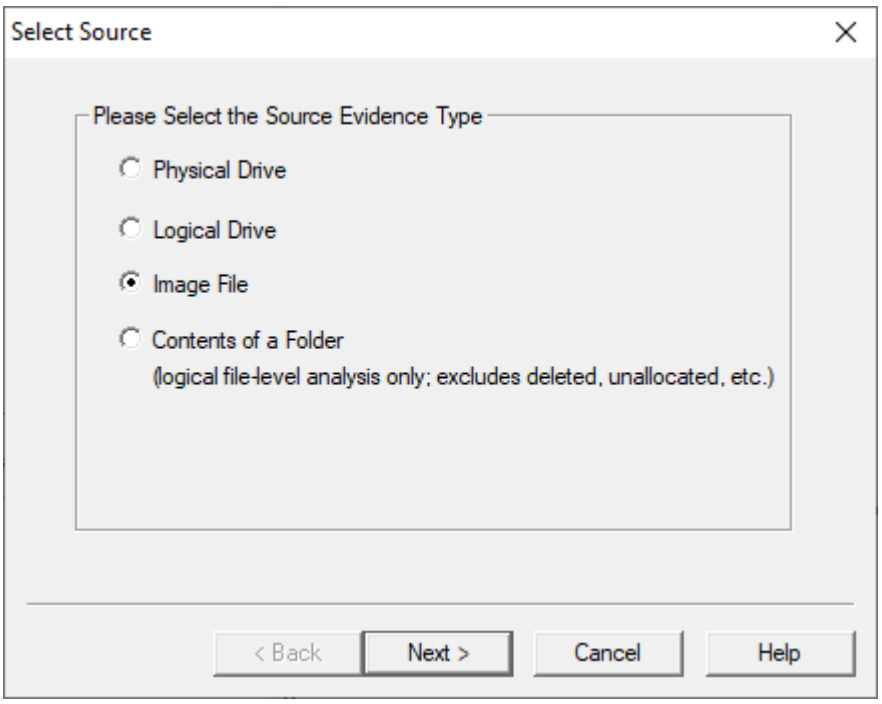


Analyze Forensic Image:

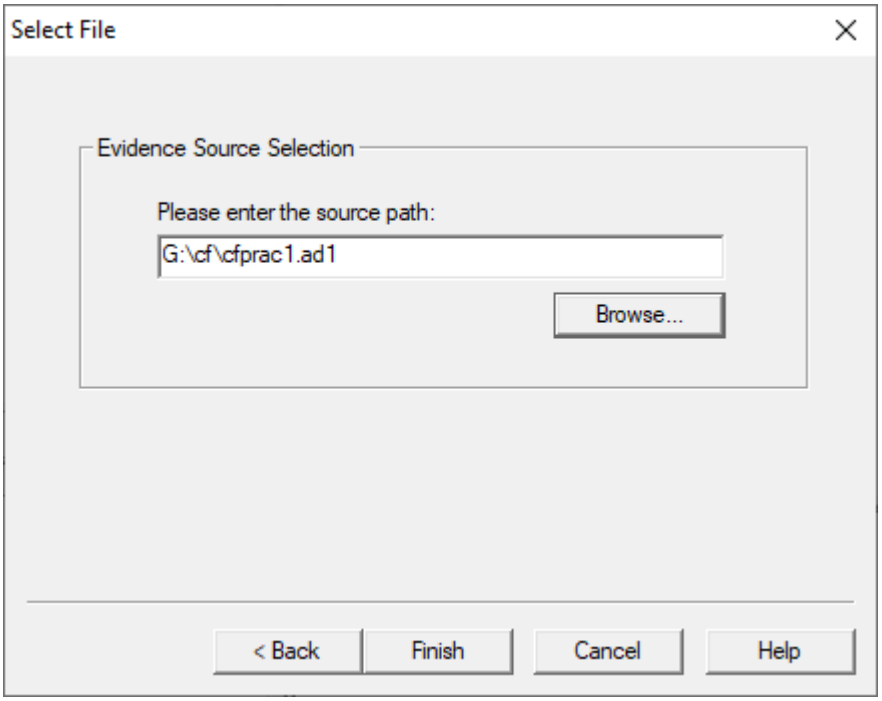
Click on Add Evidence Item to add evidence from disk, image file or folder.



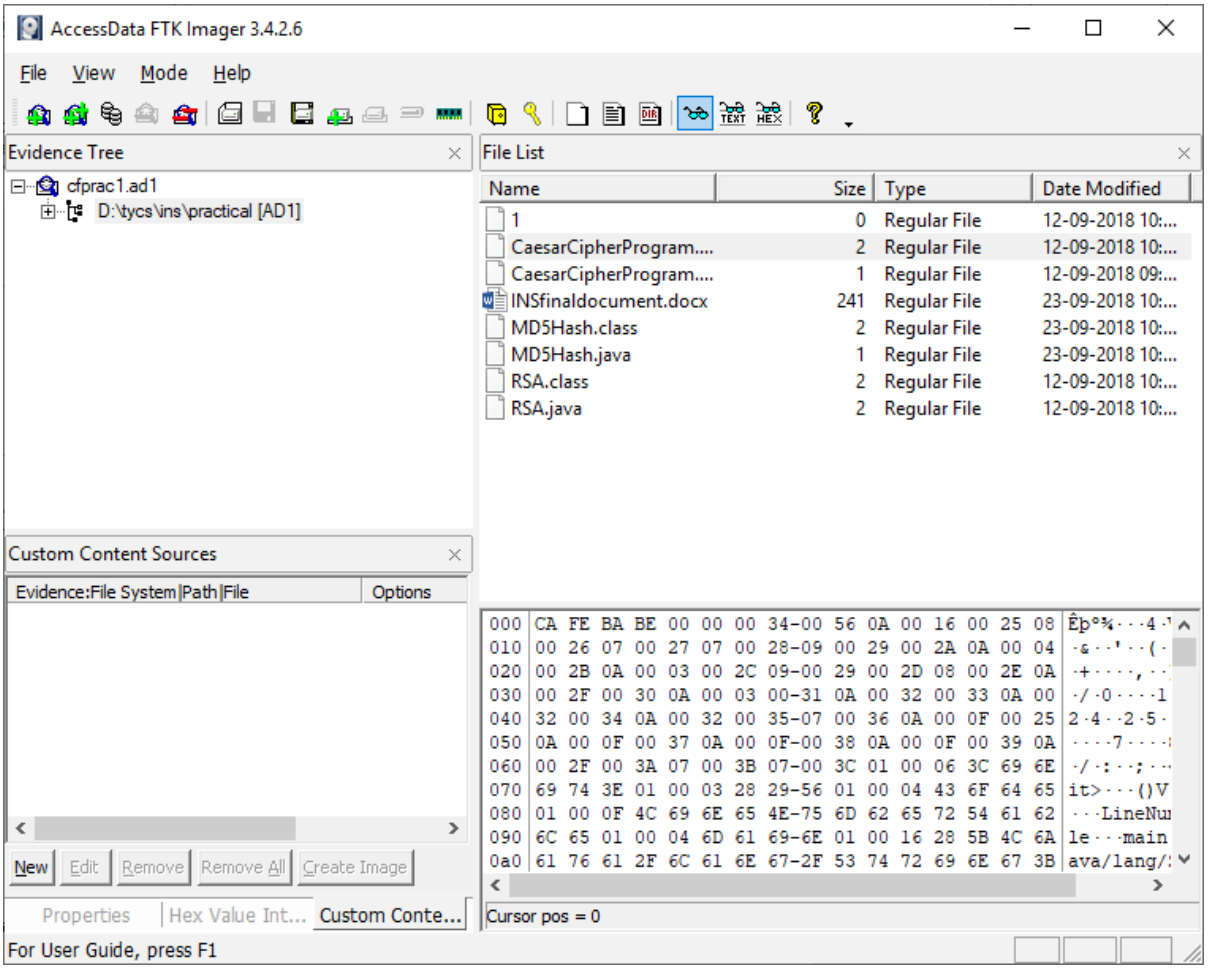
Now select the source evidence type as image file.



Open the created evidence image file



Now select Evidence Tree and analyze the image file .



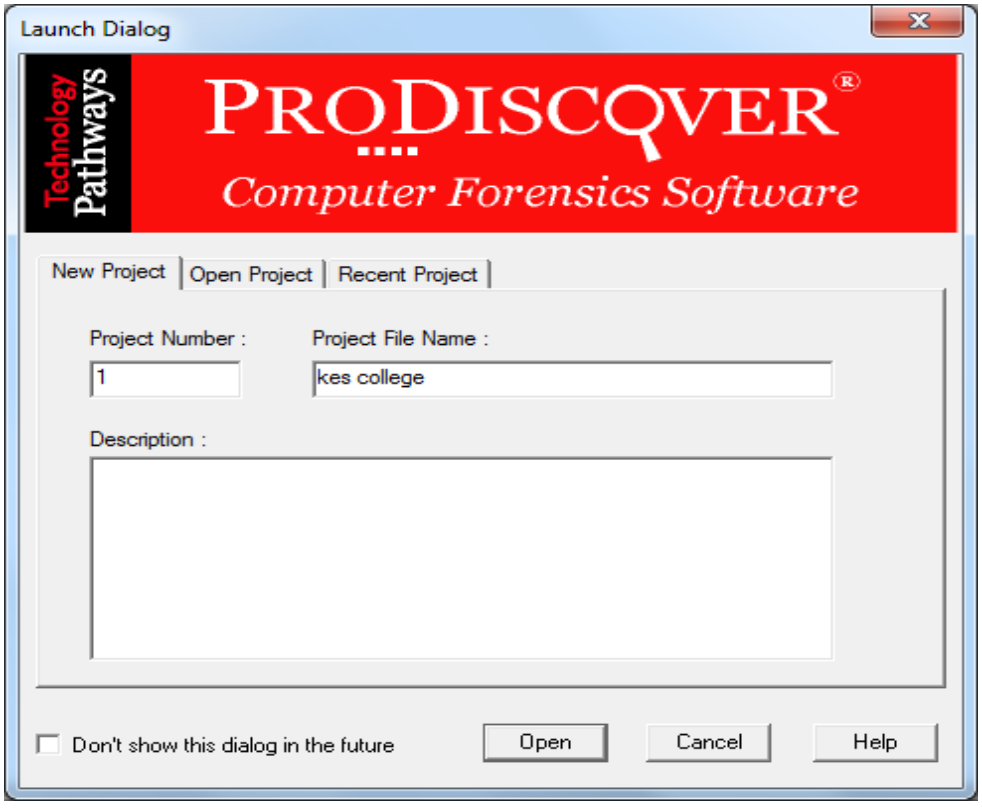
PRACTICAL 2

Aim: Data Acquisition:

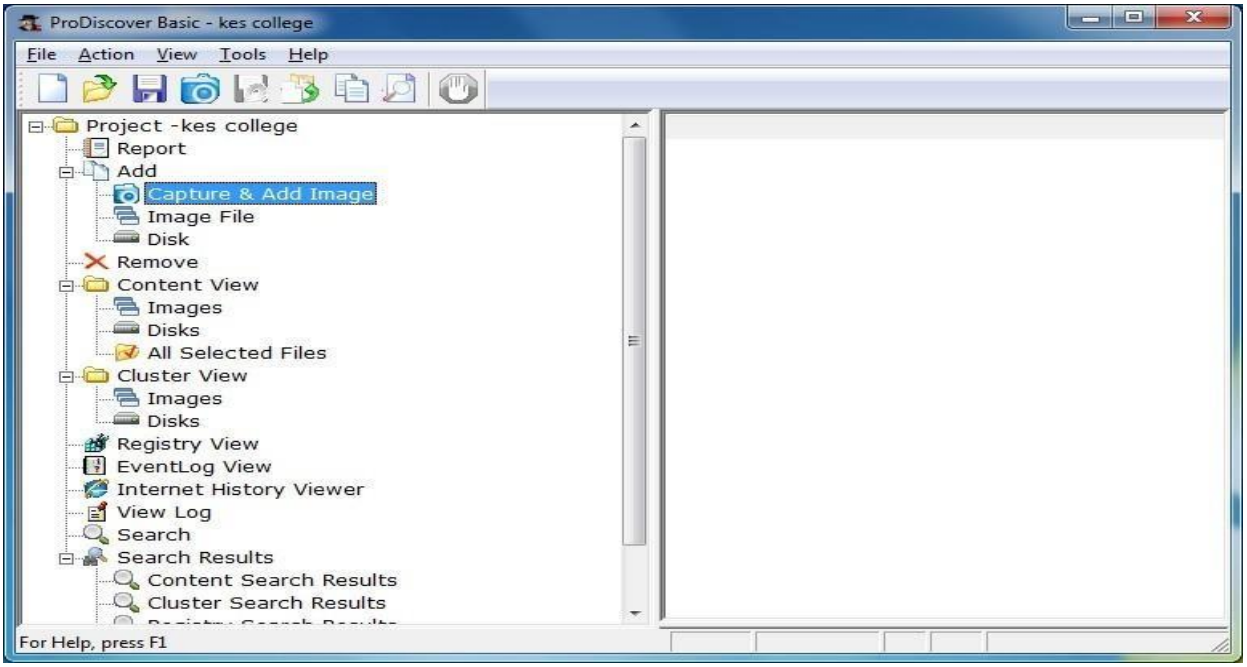
- Perform data acquisition using:
- USB Write Blocker + FTK Imager

Steps:

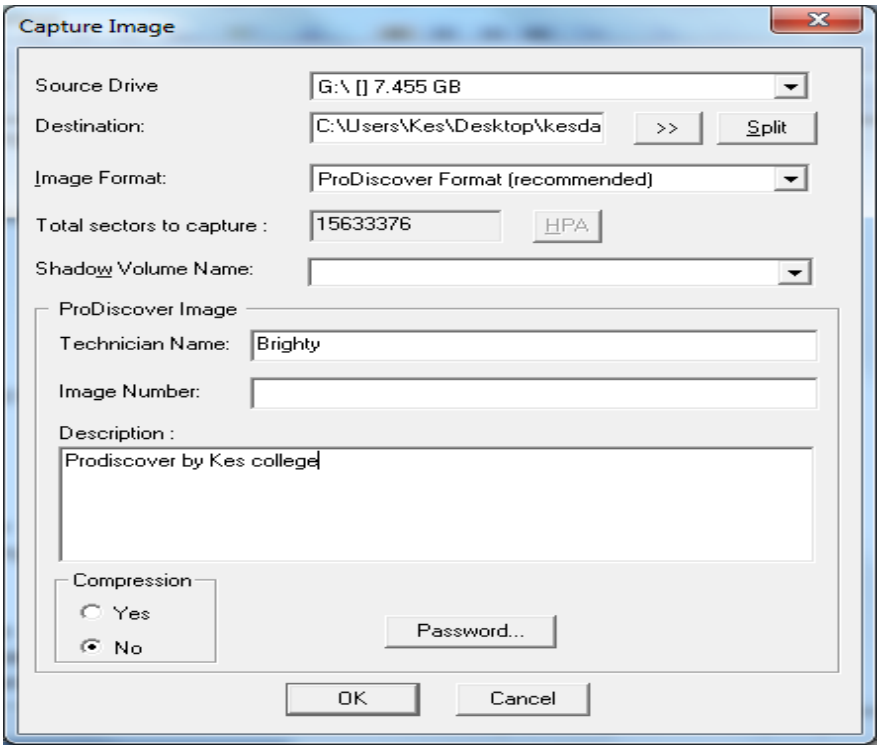
Step 1: First Open Prodiscover Basic and start with new case.



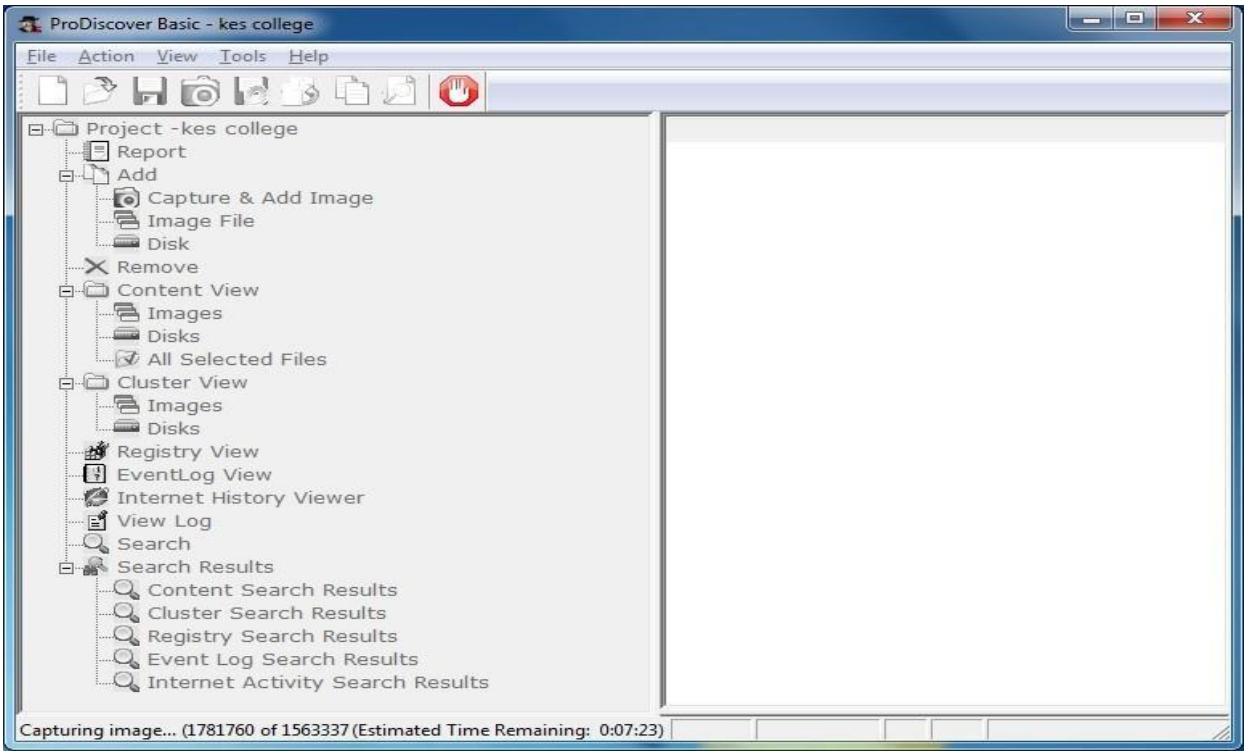
Step 2: The created project appears in left pane and select add>capture & add image.

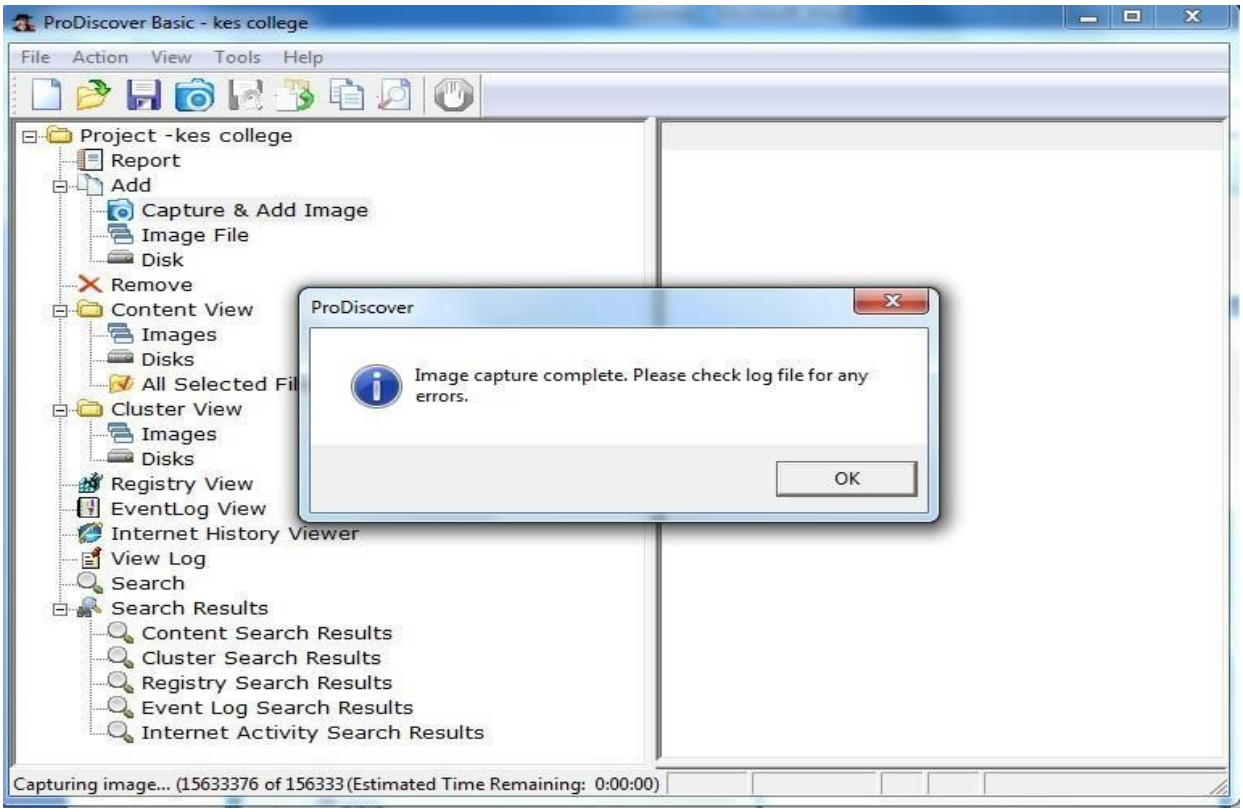


Step 3: fill the details as below. And click ok.

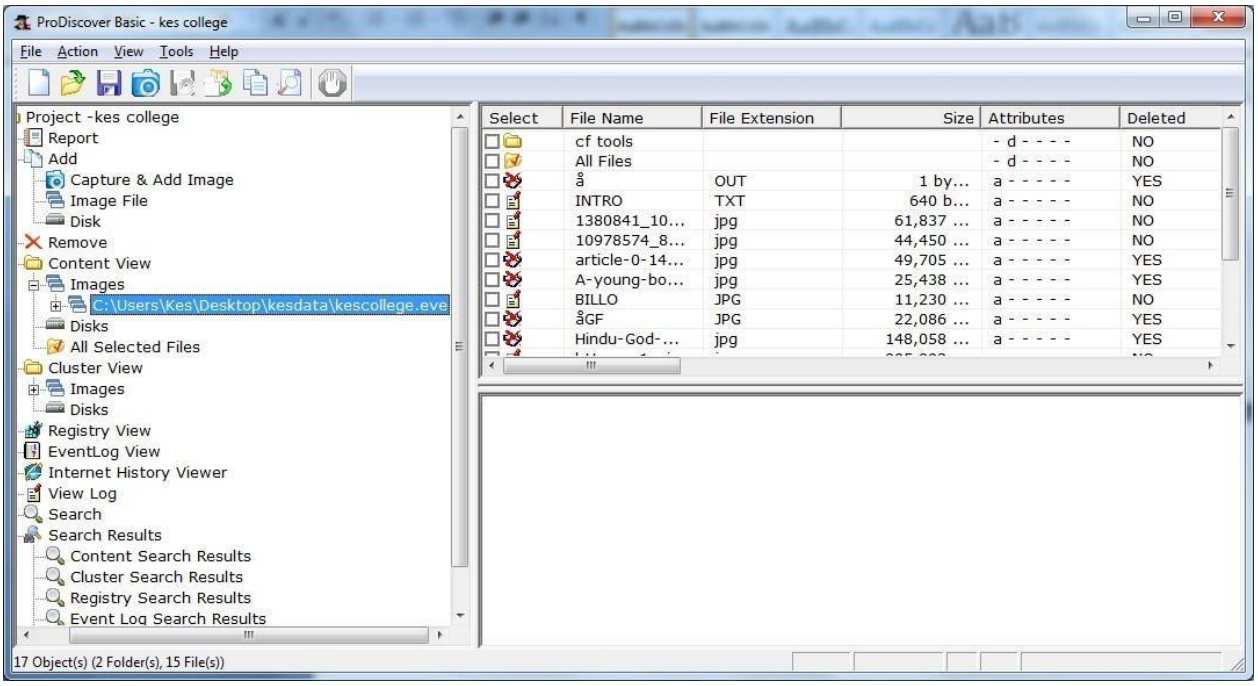


Step 4: capturing of image starts.



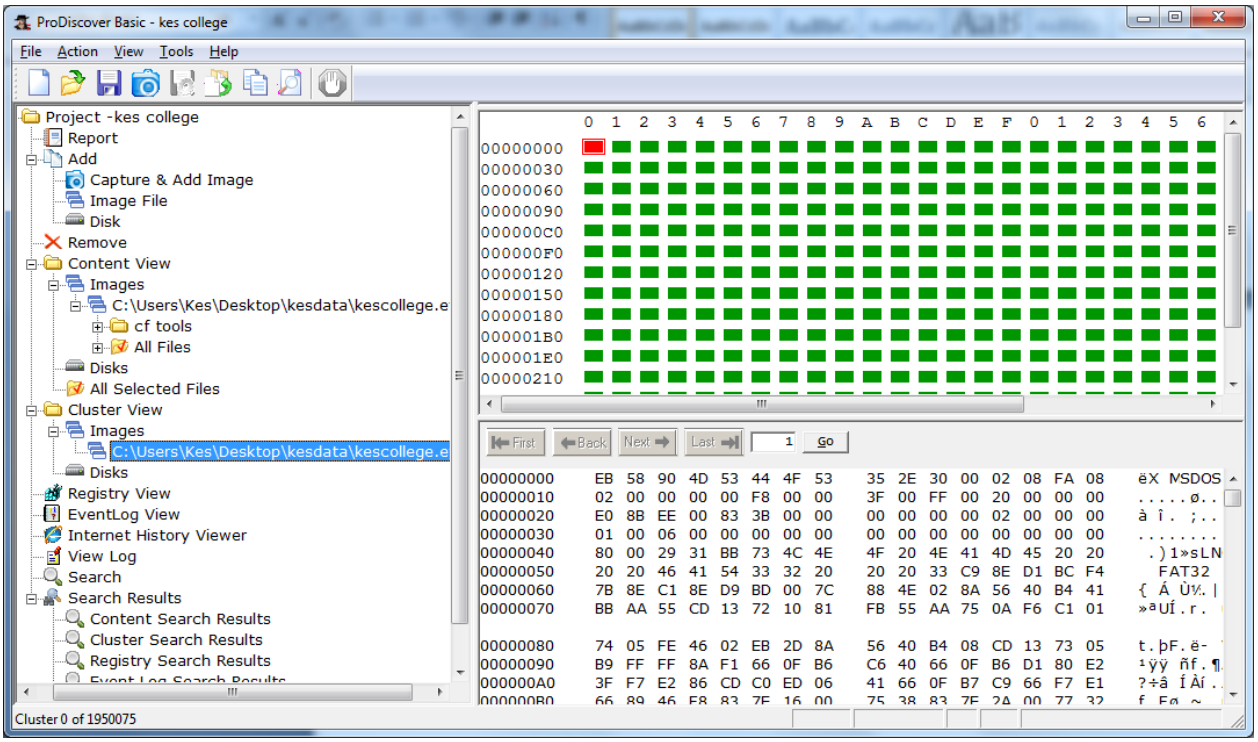


Step 5: Open the image created, go to Add > Images in left pane.

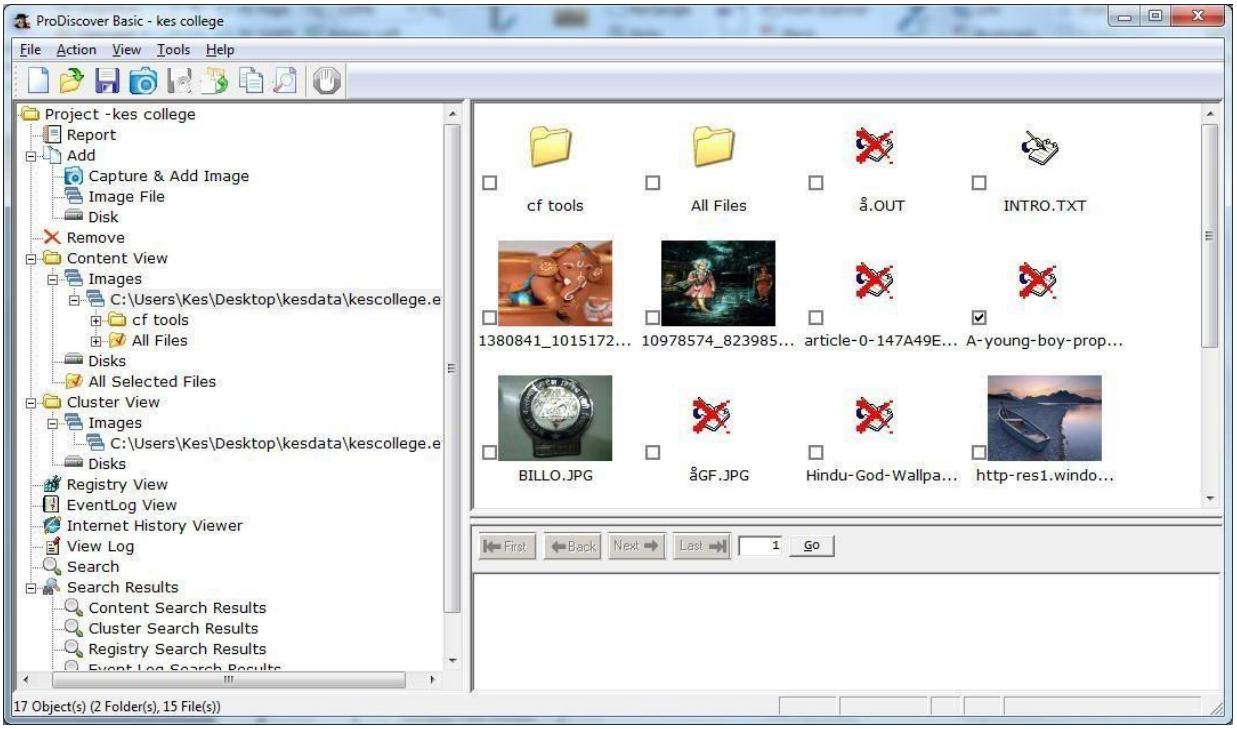


Step 6: Click on any File and type a comment.

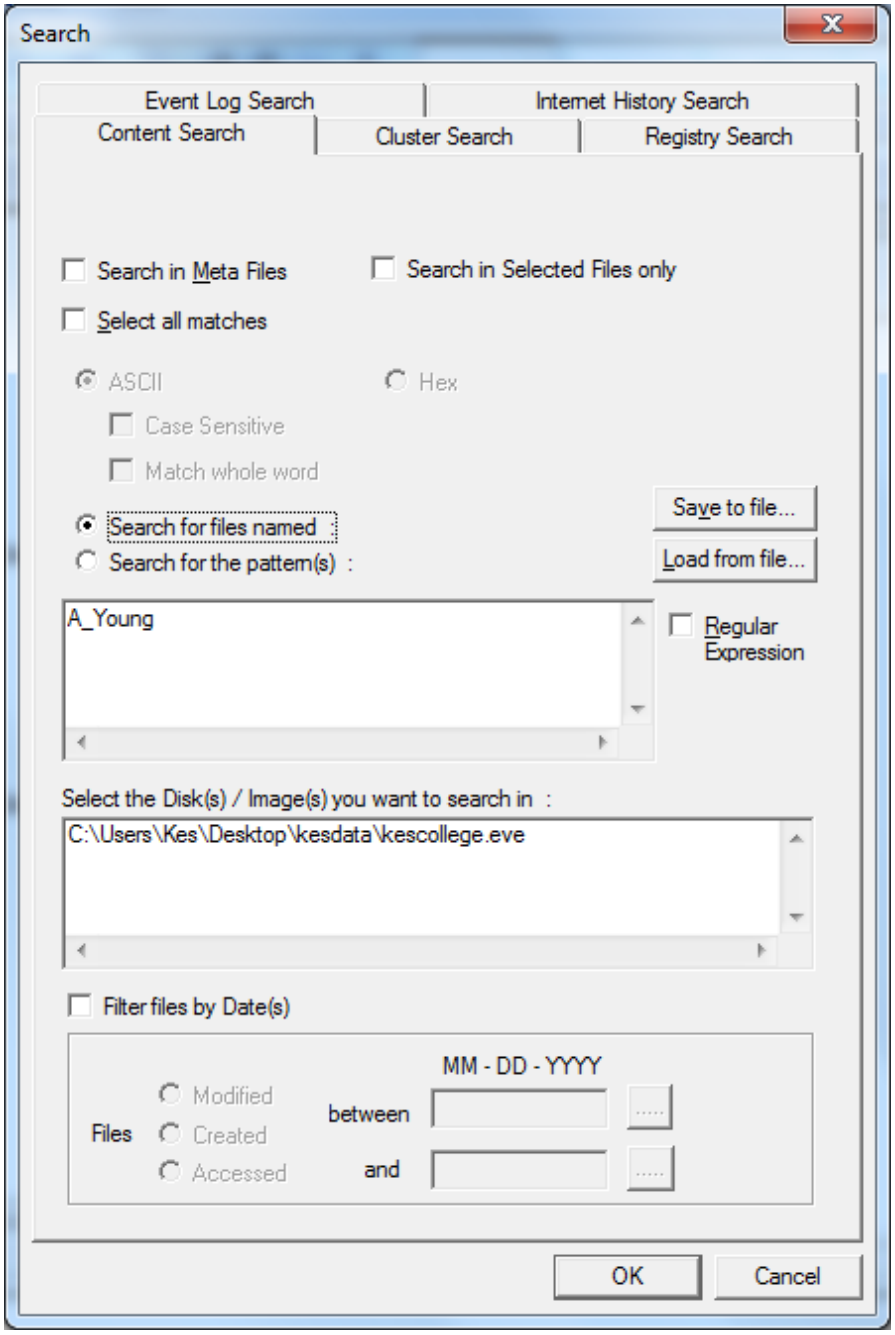
Step 7 : the cluster view is seen from the cluster view in left panel.



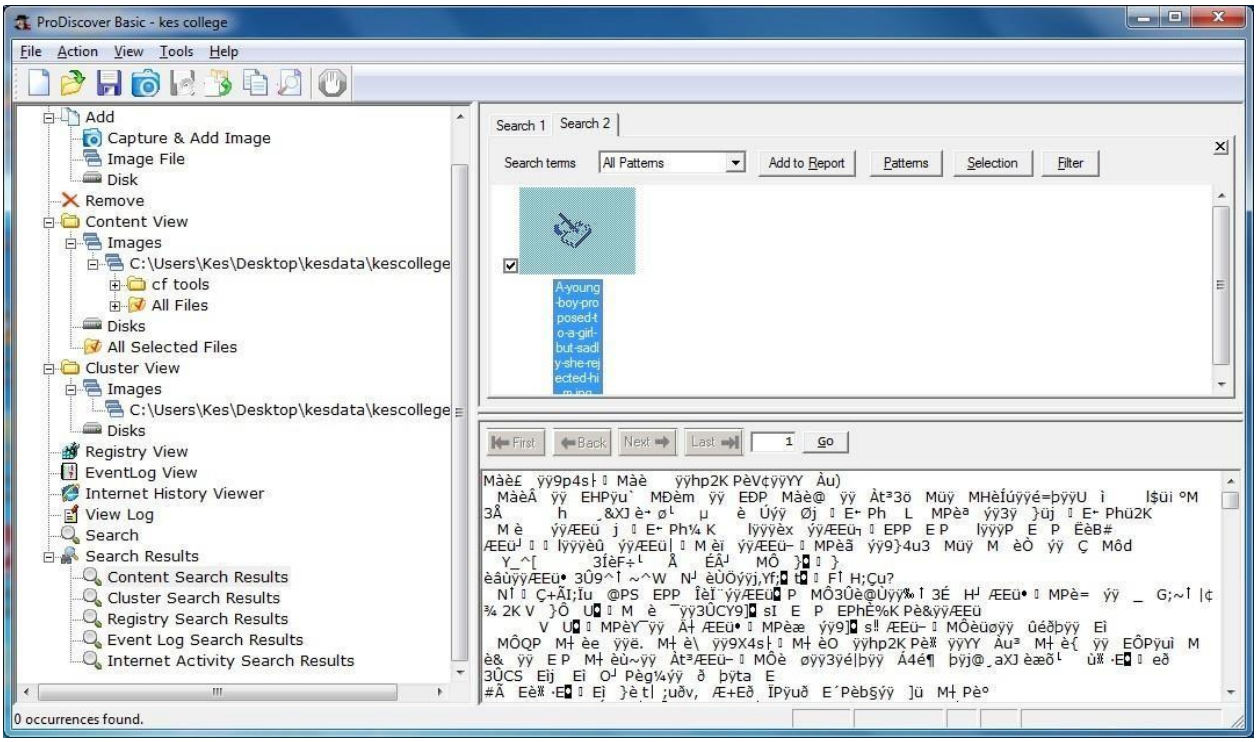
Step 8 : We can also view gallery view by Right Click.



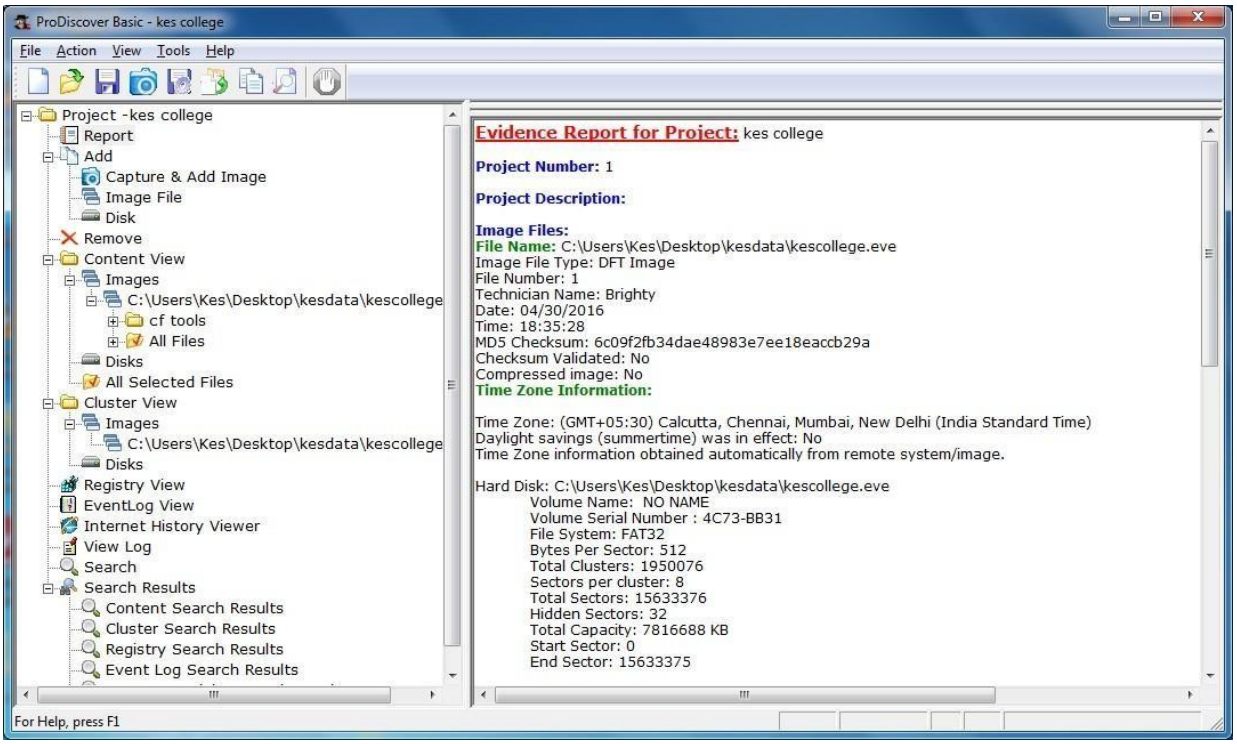
Step 9: Keyword search. Click on Search in left pane and Enter the file name to be searched in the image created.

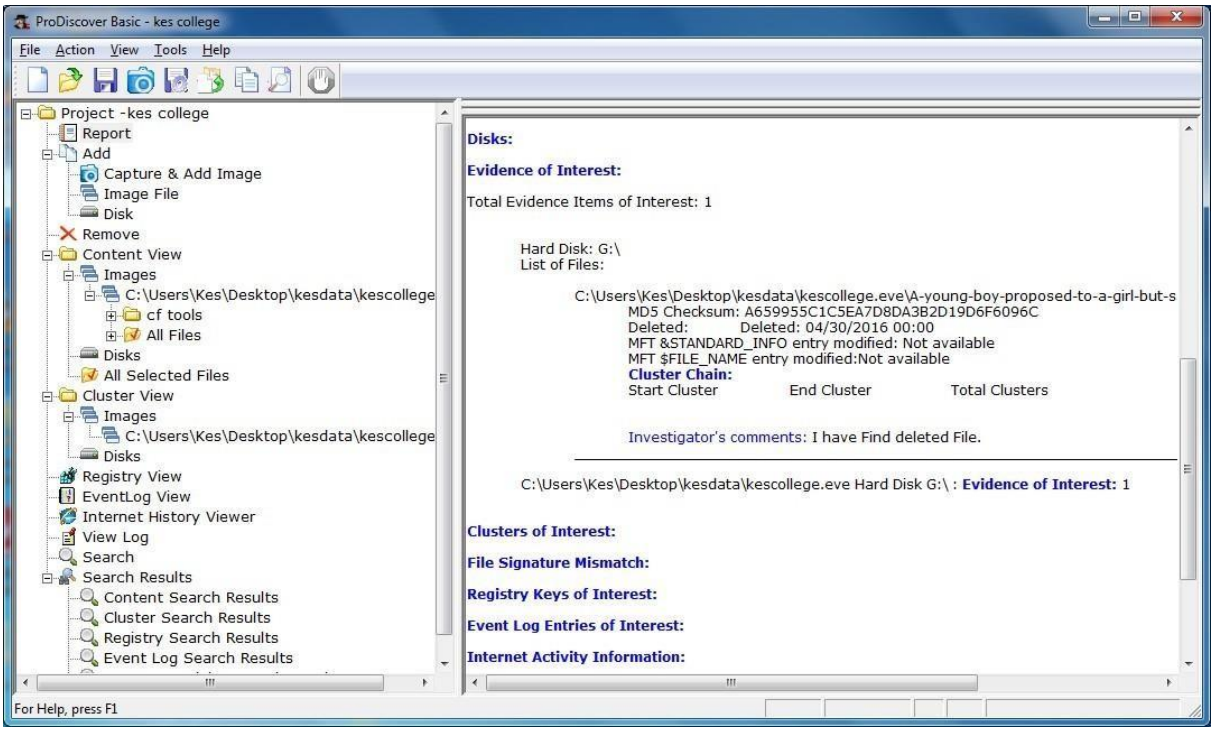


Step 10 : Output of Keyword search.



Step 11 : Click on View>Report.




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

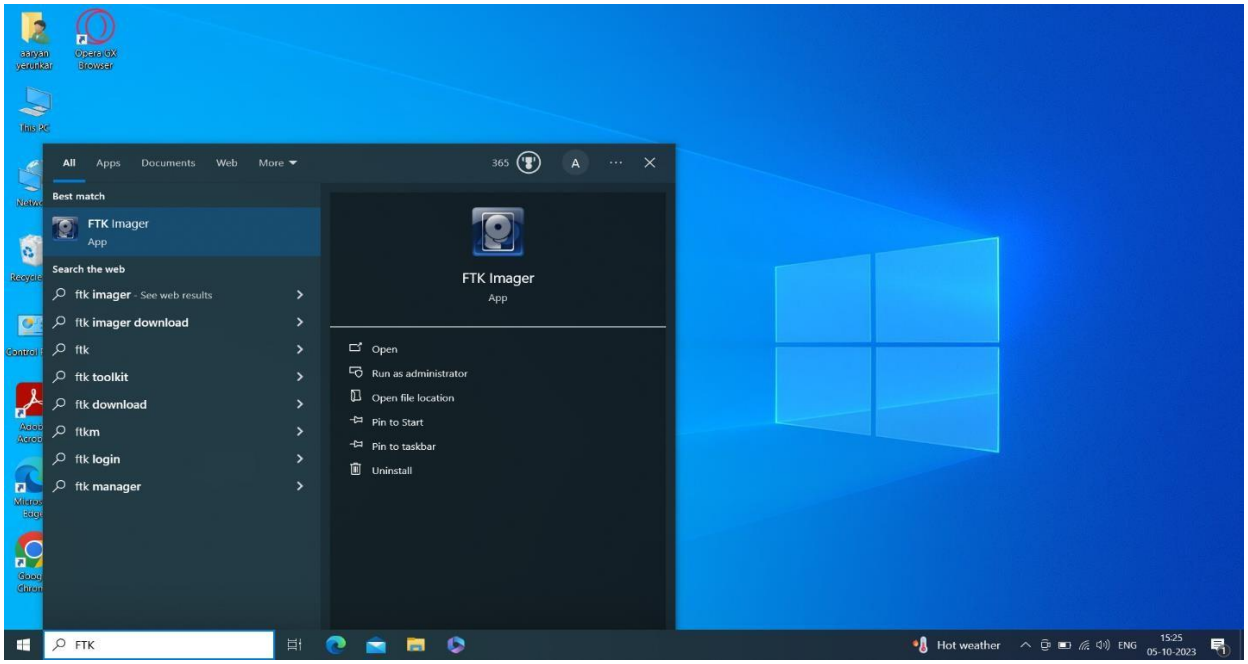
PRACTICAL 3

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

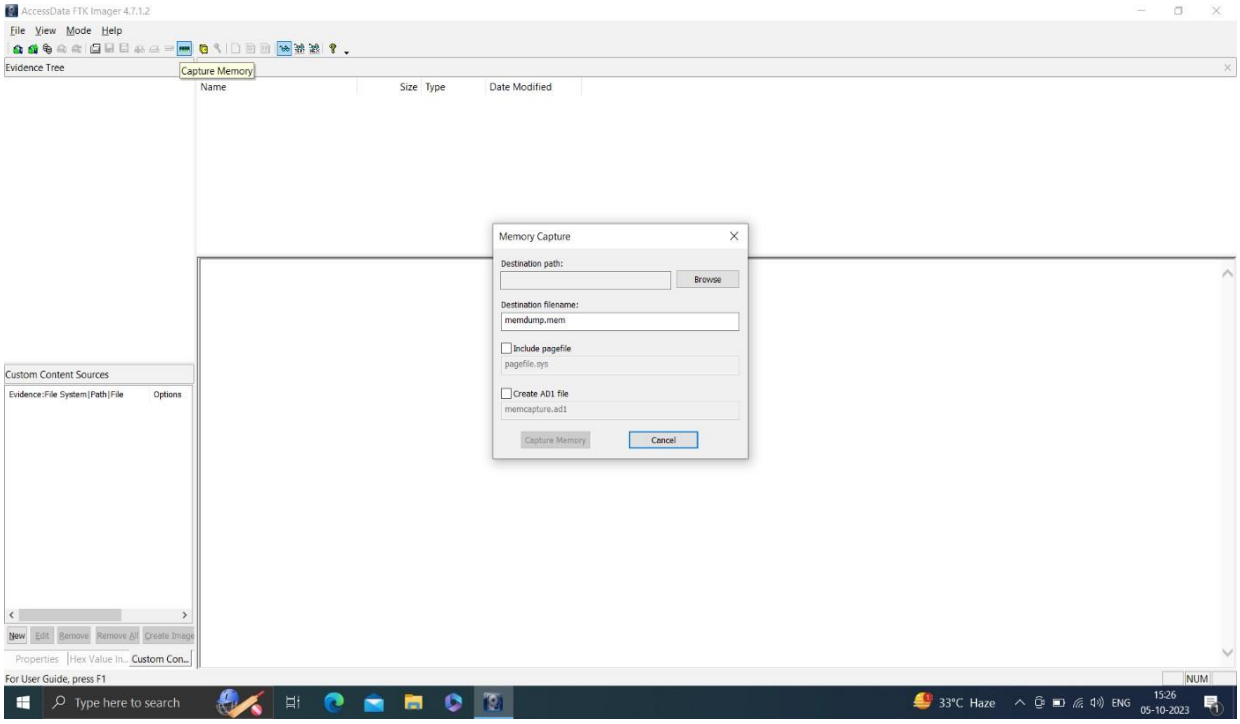
- Capture The Memory Dump By Using AccessData FTK Imager
- Analyze The Memory Dump (.MEM File)

Steps:-

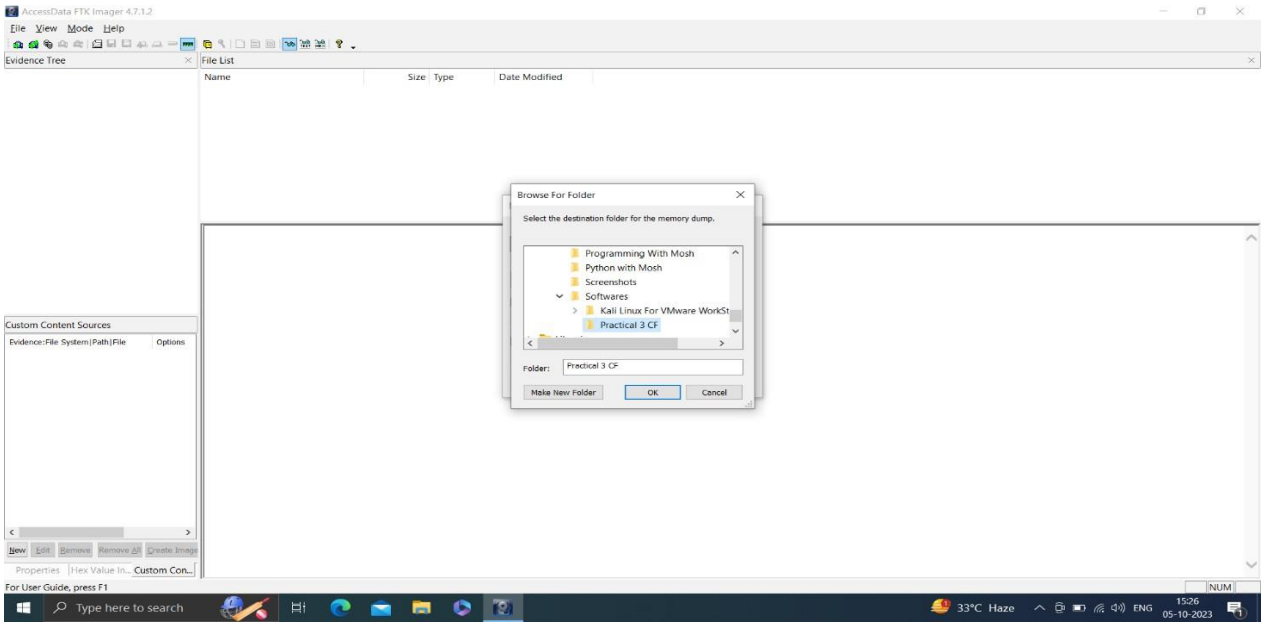
1) On Your Computer Open AccessData FTK Imager



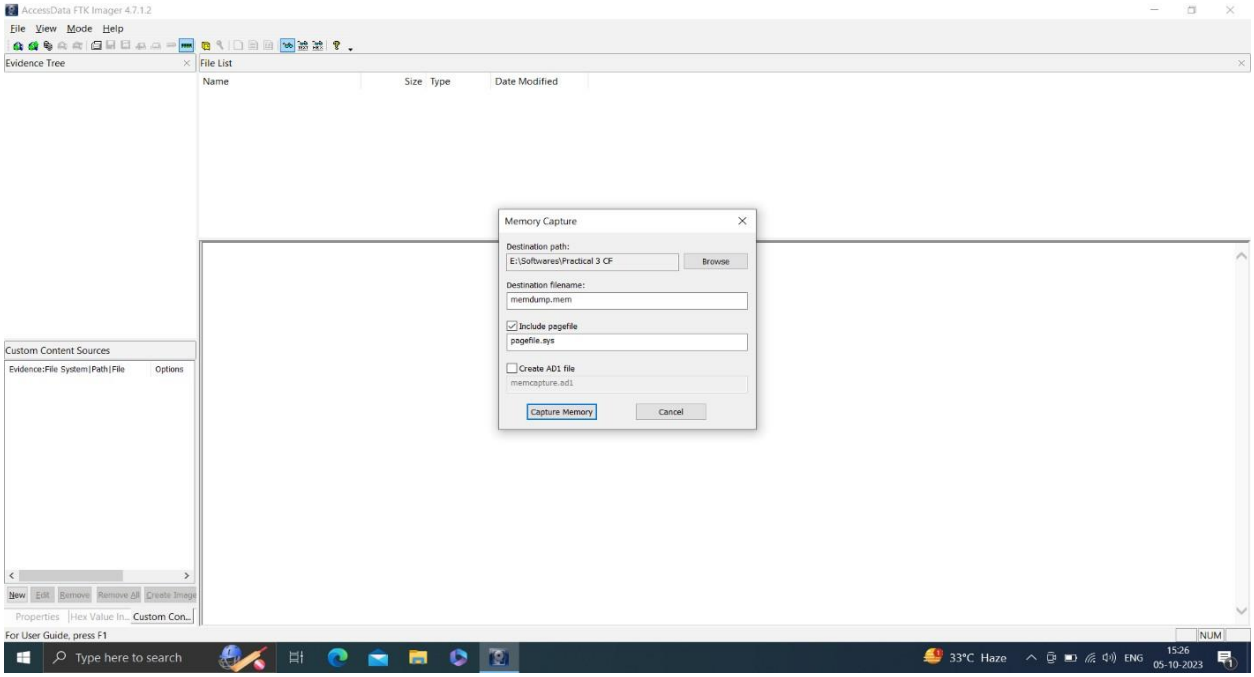
2) Now To Capture Memory Dump Click on ‘Capture Memory ’ Icon



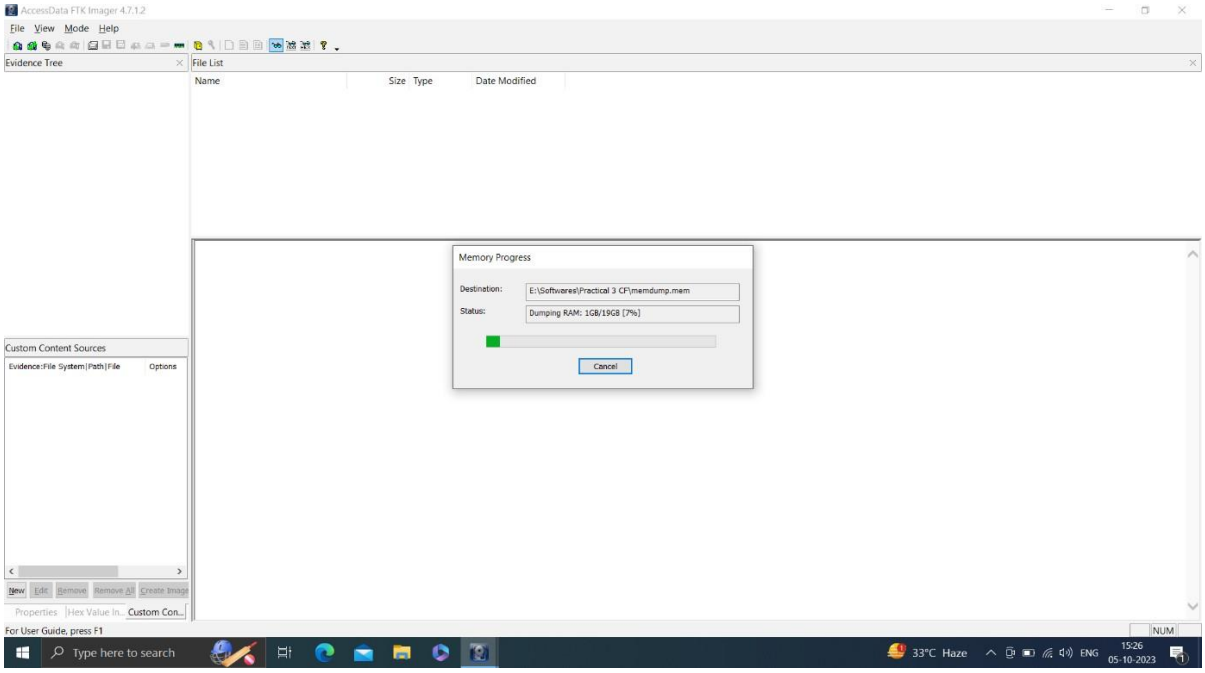
3) Browse The Destination Path



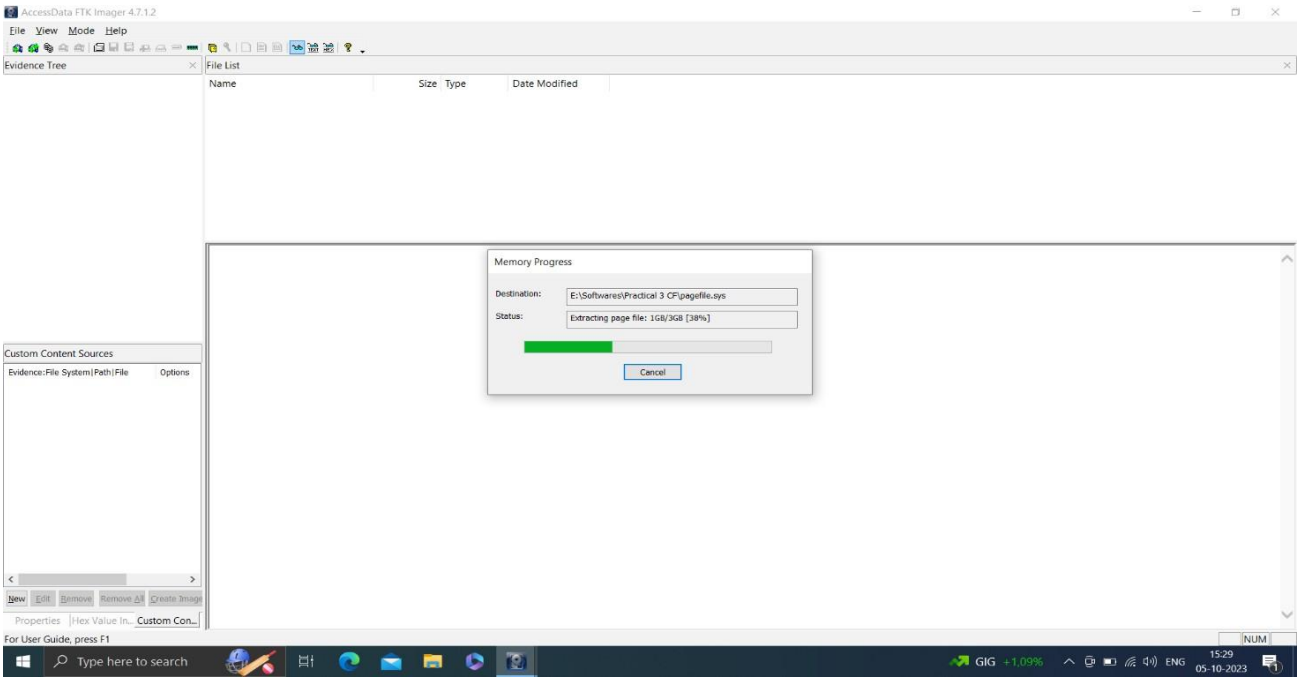
4) Now Click on ‘Include Page File’



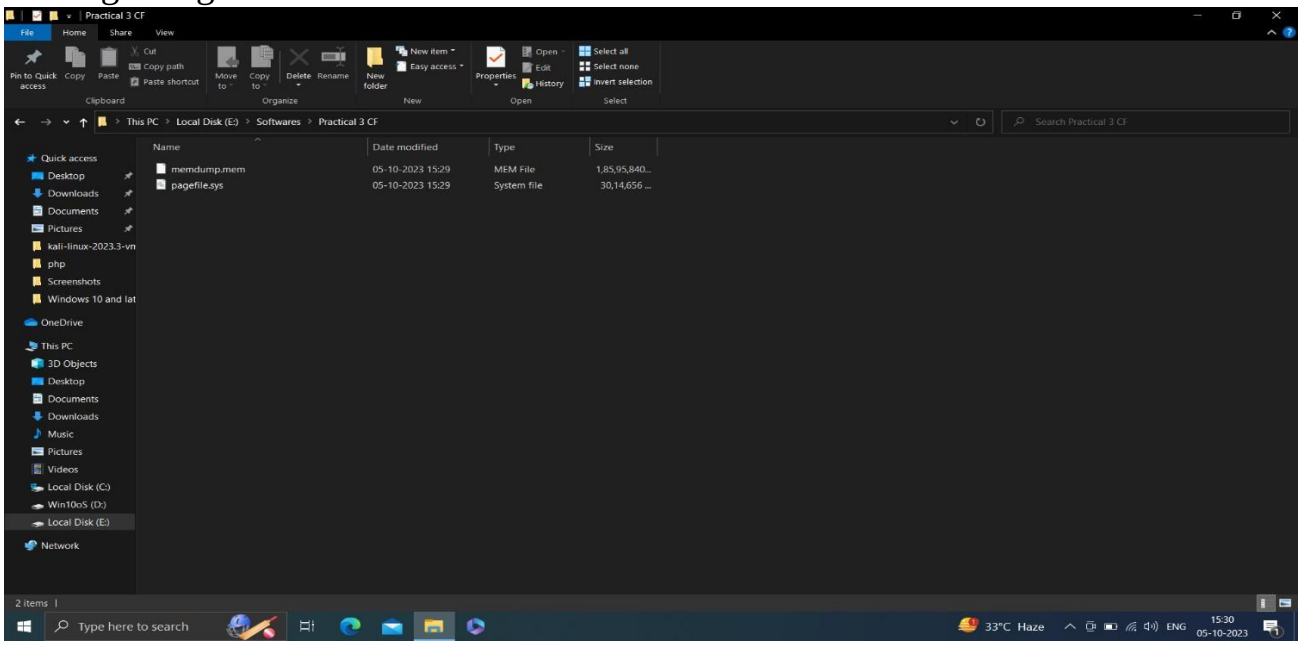
5) Click on Capture Memory to Capture the Memory Dump



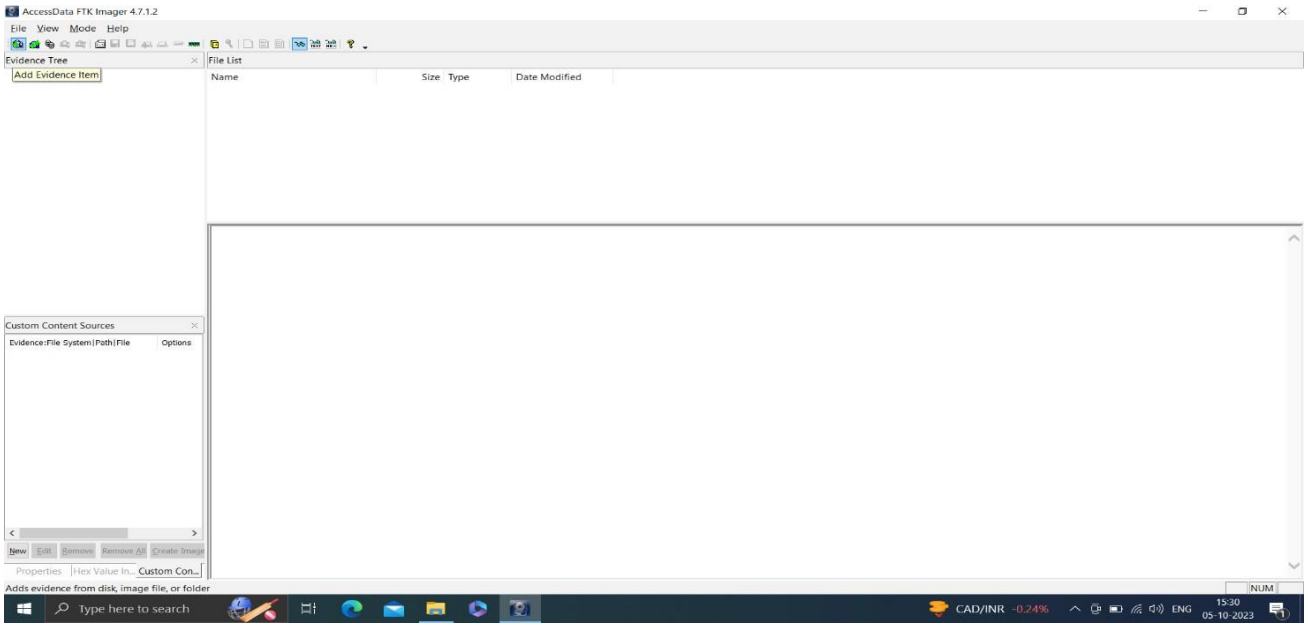
It will Also Extract Page File



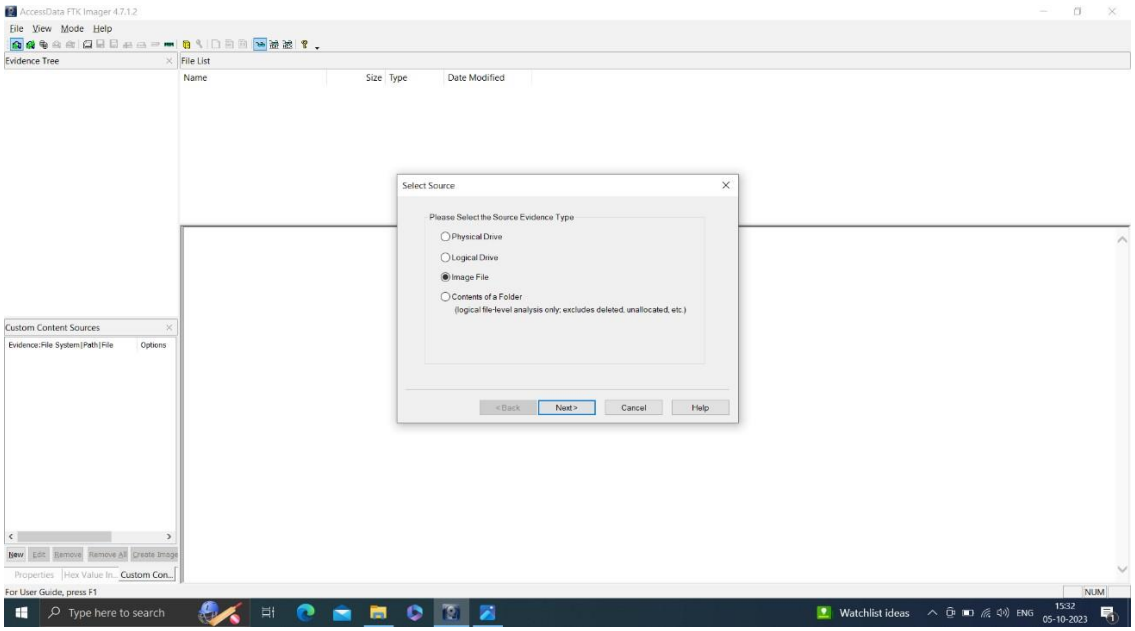
6) So After That The Files Will be Displayed In Destination Folder Which You Selected at the Beginning



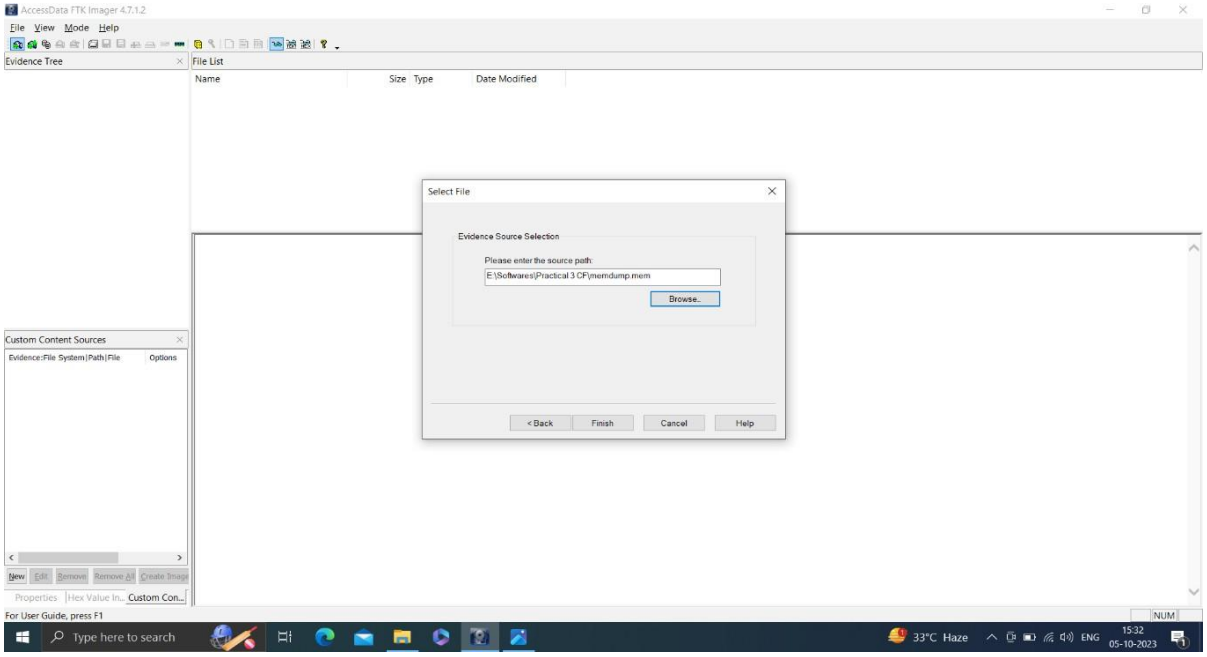
7) Now To Analyze The Memory Dump Click on ‘Add Evidence Item’ Icon



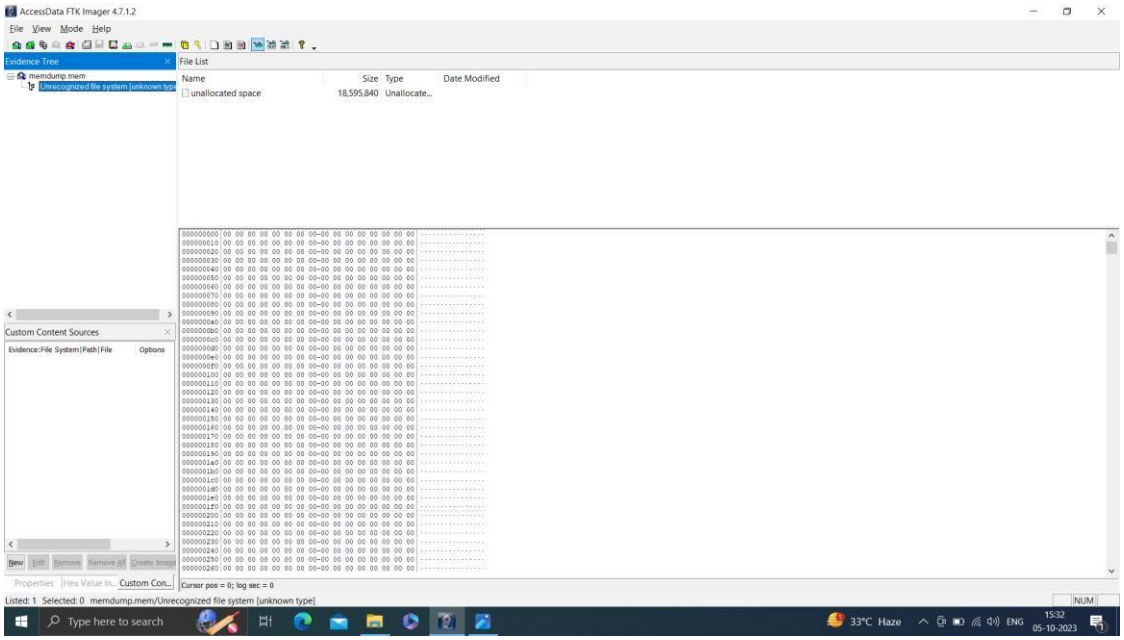
8) Select Source Type ‘Image File’ as Shown In Below Image



9) Browse the Source Path where The Evidence is Stored



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



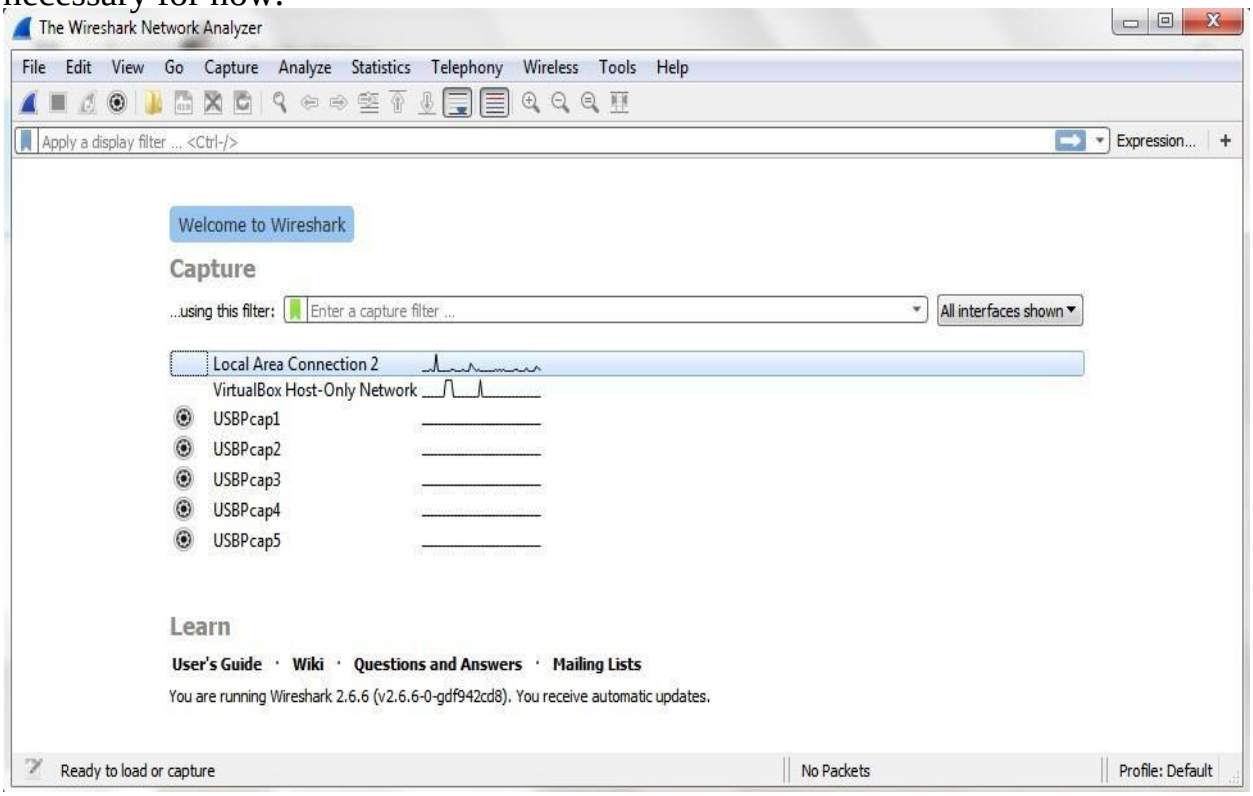
PRACTICAL 4

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

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

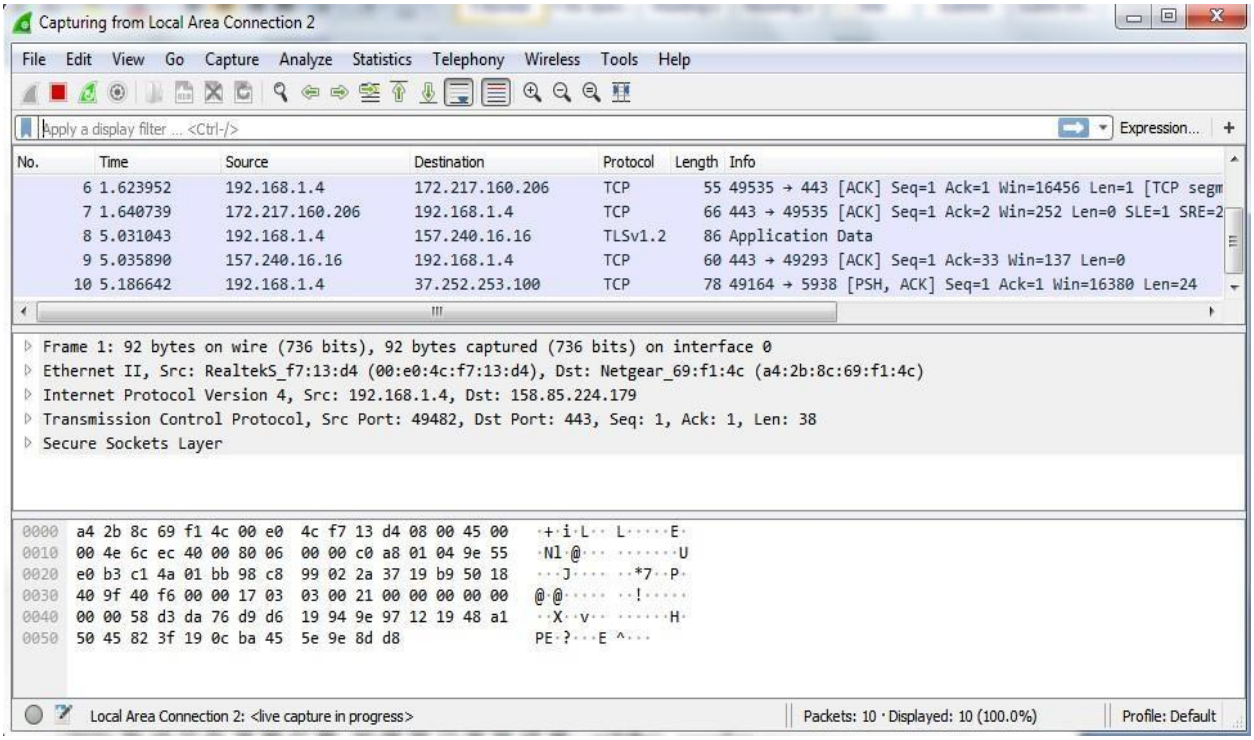
Capturing Packets

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

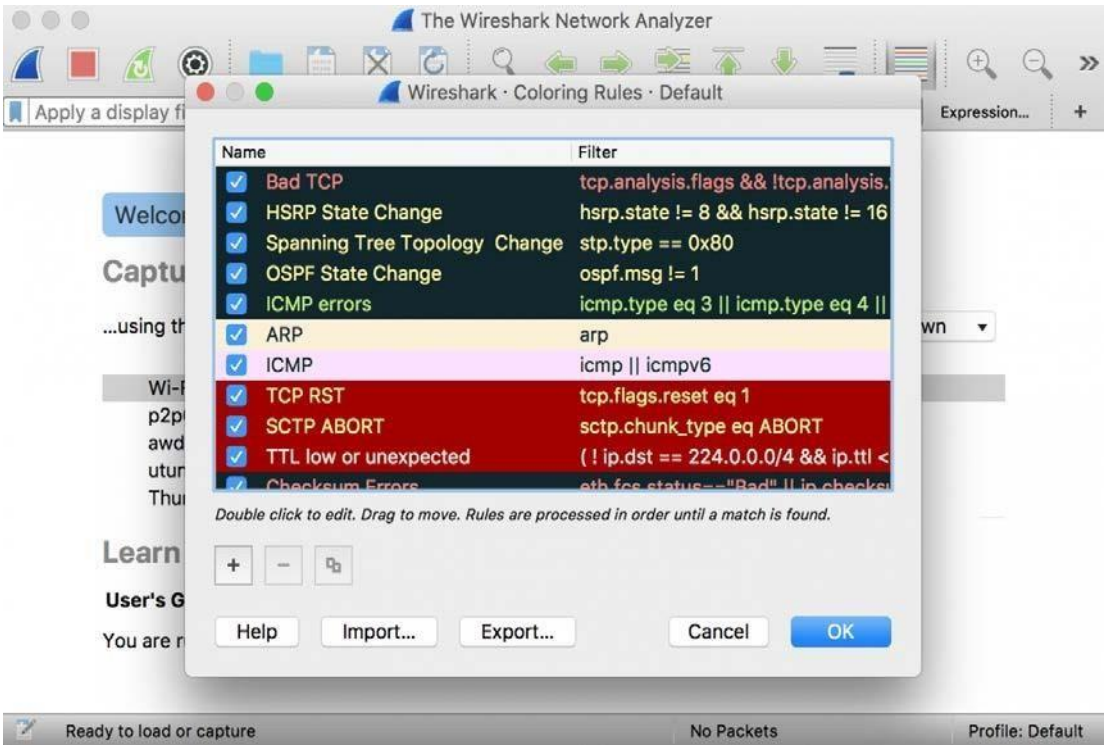
Different packets are seen highlighted in various different colors. This is Wireshark's way of displaying traffic to help you easily identify the types of it. Default colors are:

Light Purple color for TCP traffic

Light Blue color for UDP traffic

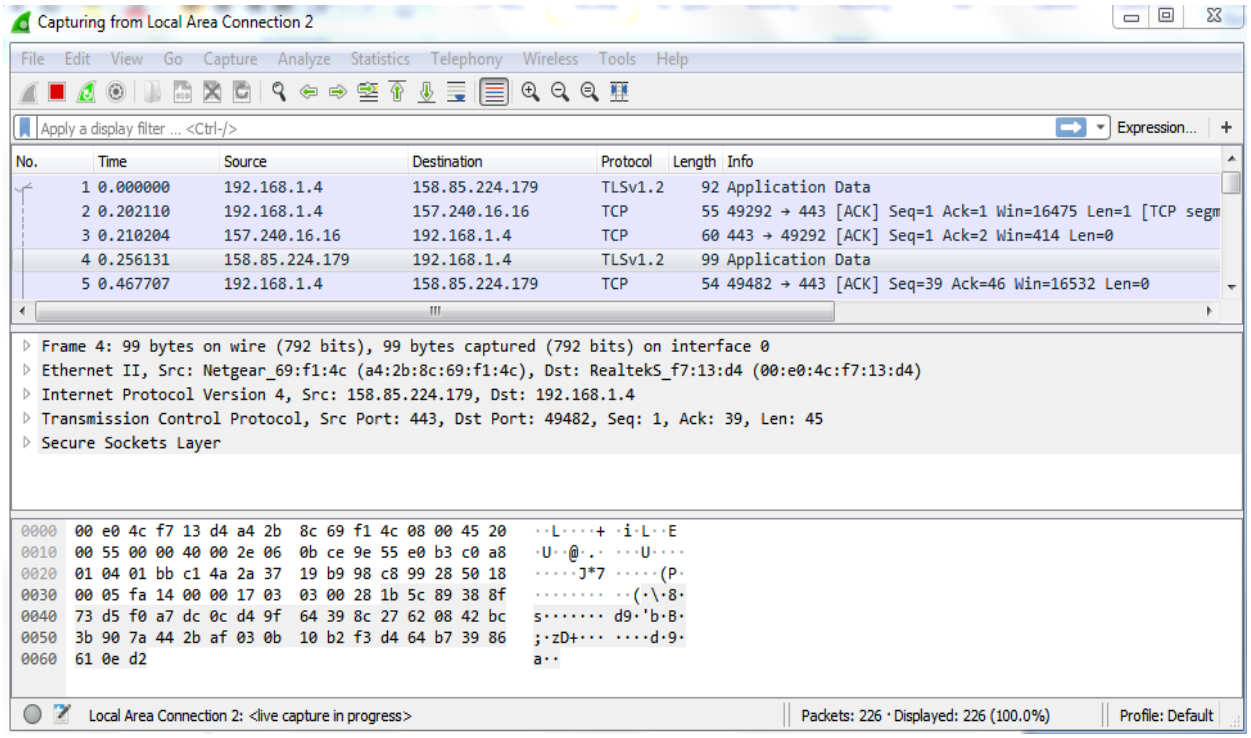
Black color identifies packets with errors – example these packets are delivered in an unordered manner.

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.

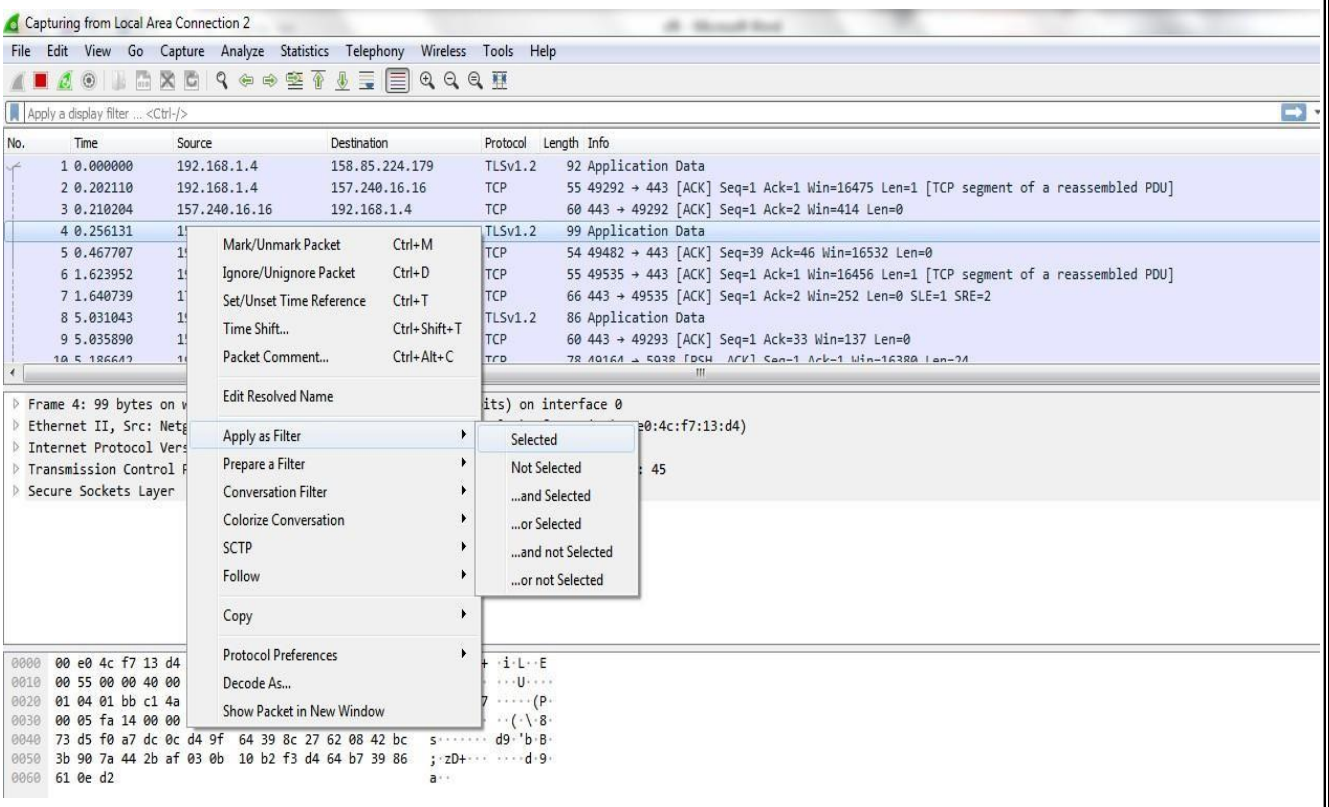


Analyze the captured Packets:

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

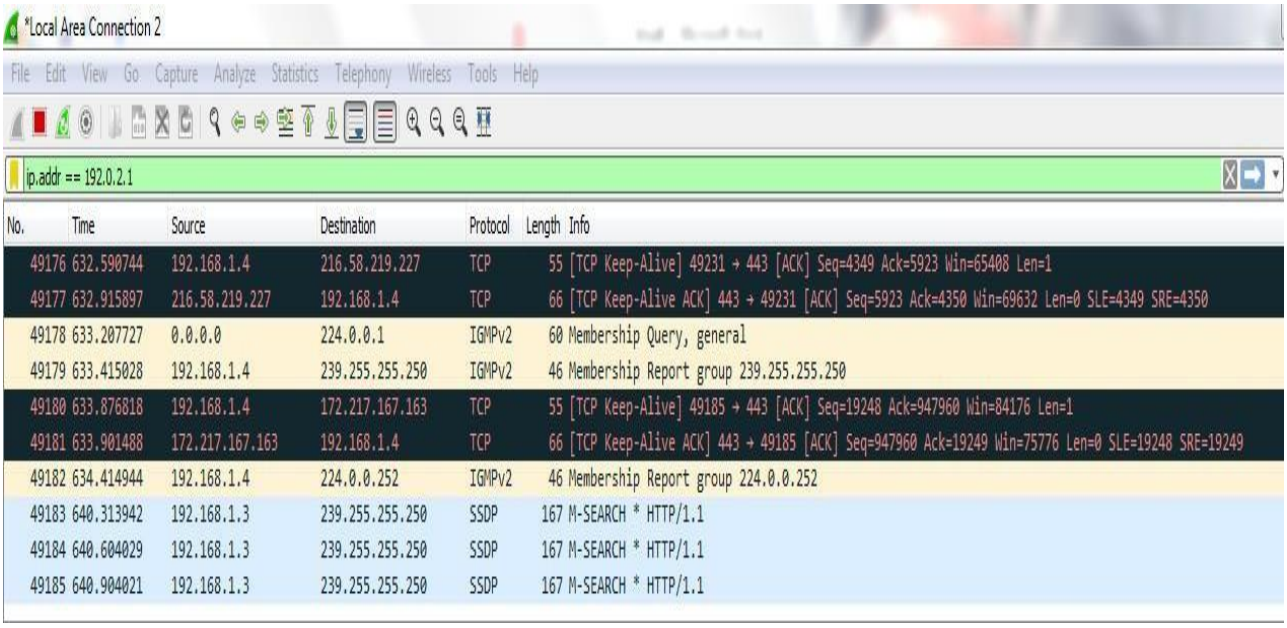


Filters can also be created from here. Right-click on one of any details. From the menu select Apply as Filter drop-down menu so filter based on it can be created.

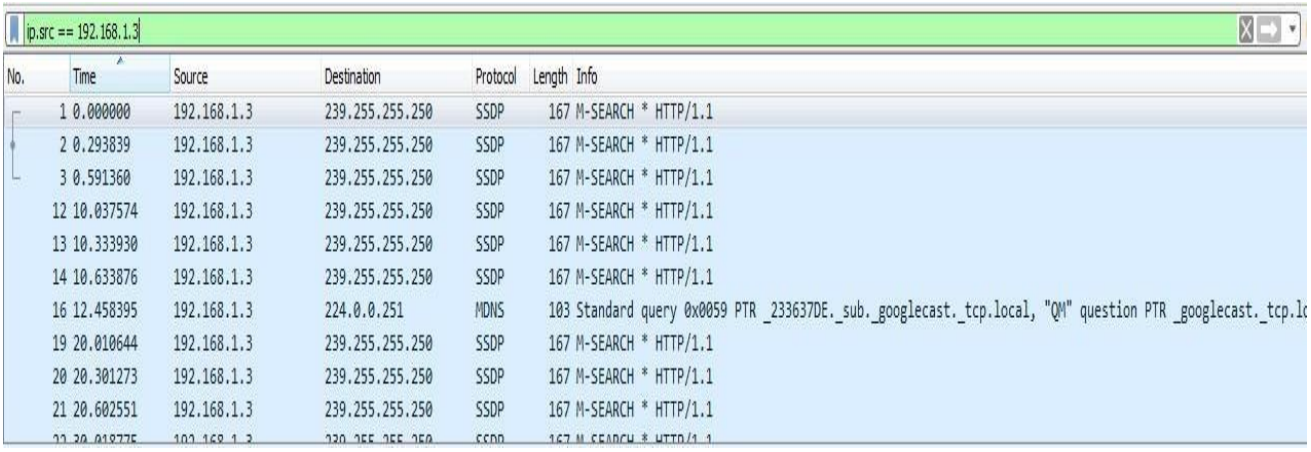


Display filter command –

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



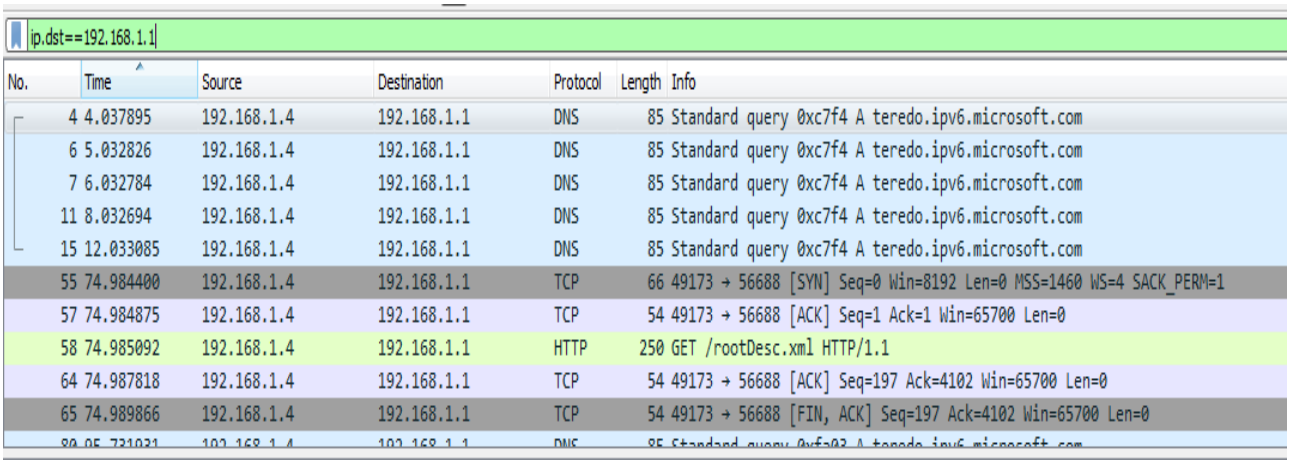
2. Display packets which are coming from specific IP-address
   - ip.src == 192.168.1.3



ip.src == 192.168.1.3

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

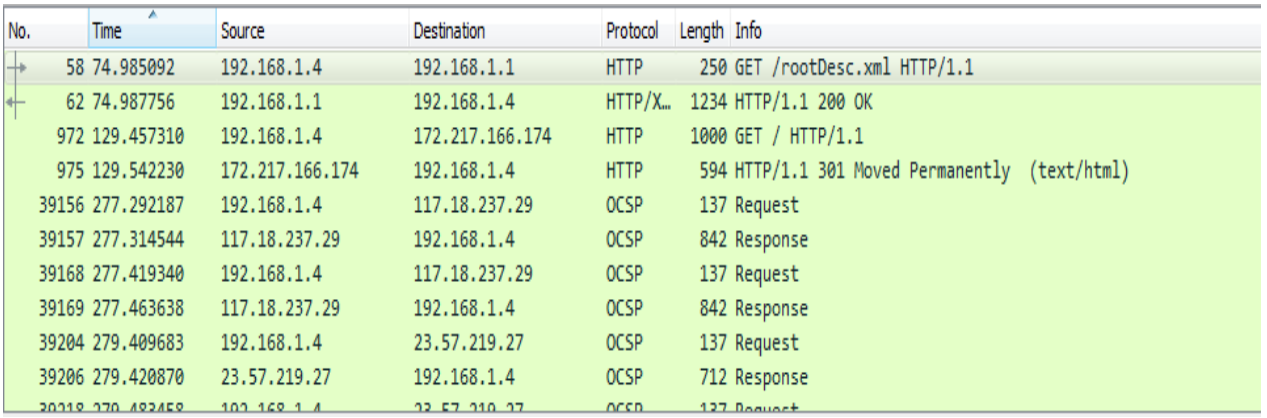
3. Display packets which are having specific IP-address destination
   - ip.dst == 192.168.1.1



ip.dst==192.168.1.1

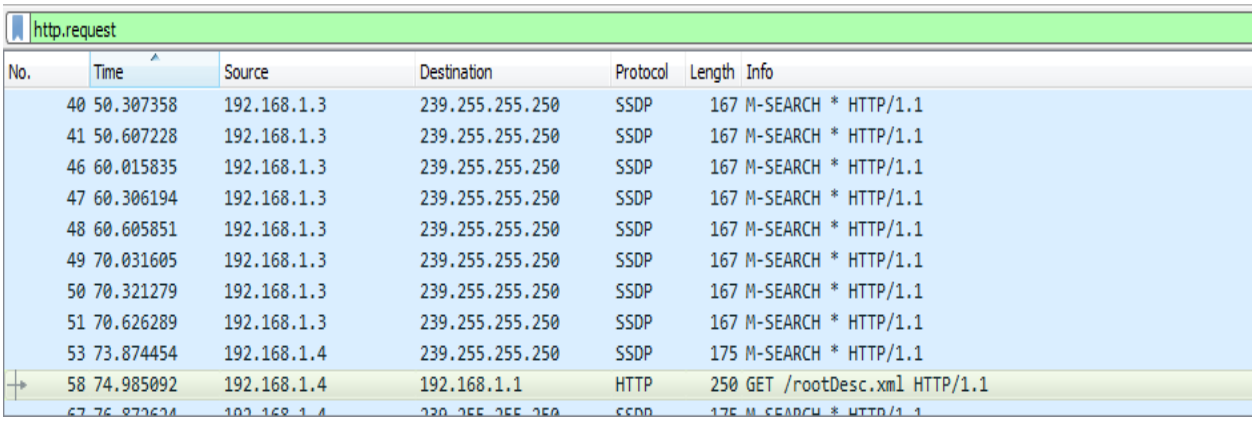
No.	Time	Source	Destination	Protocol	Length	Info
4	4.037895	192.168.1.4	192.168.1.1	DNS	85	Standard query 0xc7f4 A teredo.ipv6.microsoft.com
6	5.032826	192.168.1.4	192.168.1.1	DNS	85	Standard query 0xc7f4 A teredo.ipv6.microsoft.com
7	6.032784	192.168.1.4	192.168.1.1	DNS	85	Standard query 0xc7f4 A teredo.ipv6.microsoft.com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

4. Display packets which are using http protocol
   - http



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

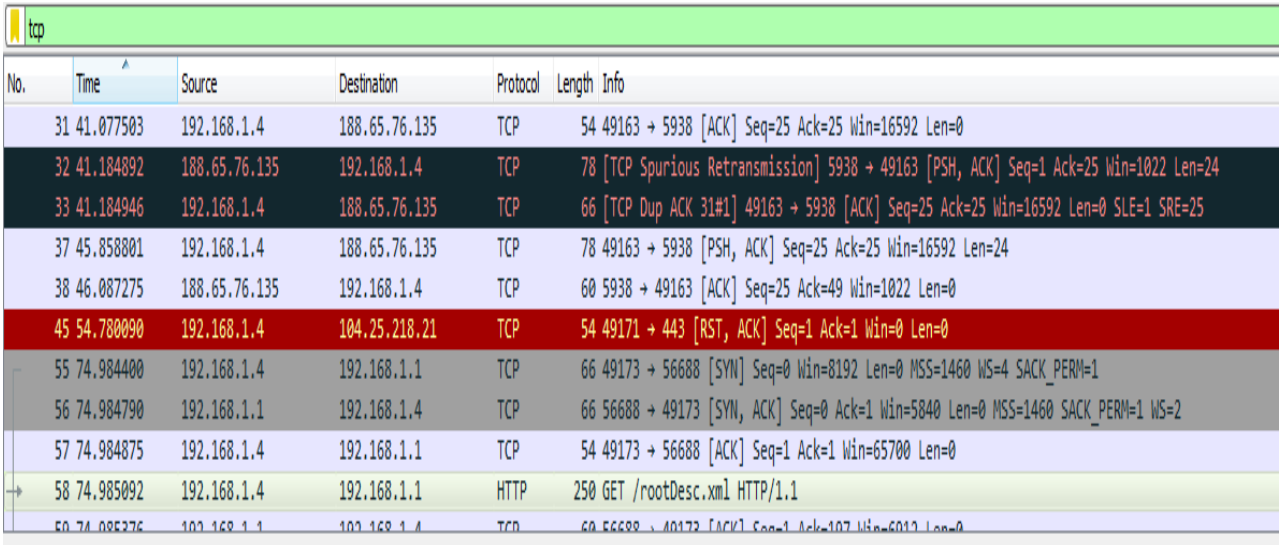
5. Display packets which are using http request
   - http.request



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

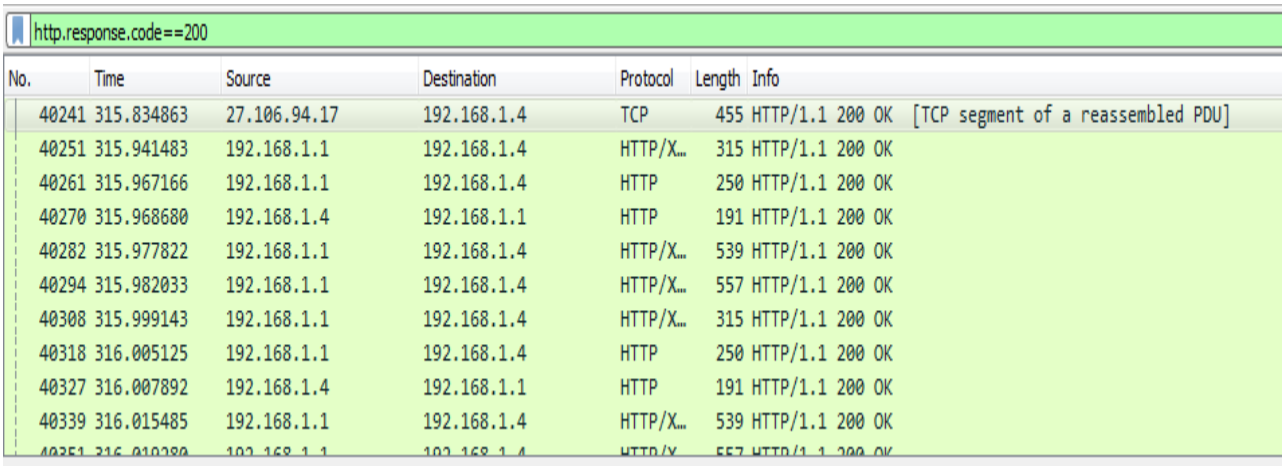
6. Display packets which are using TCP protocol
   - tcp



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=16592 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

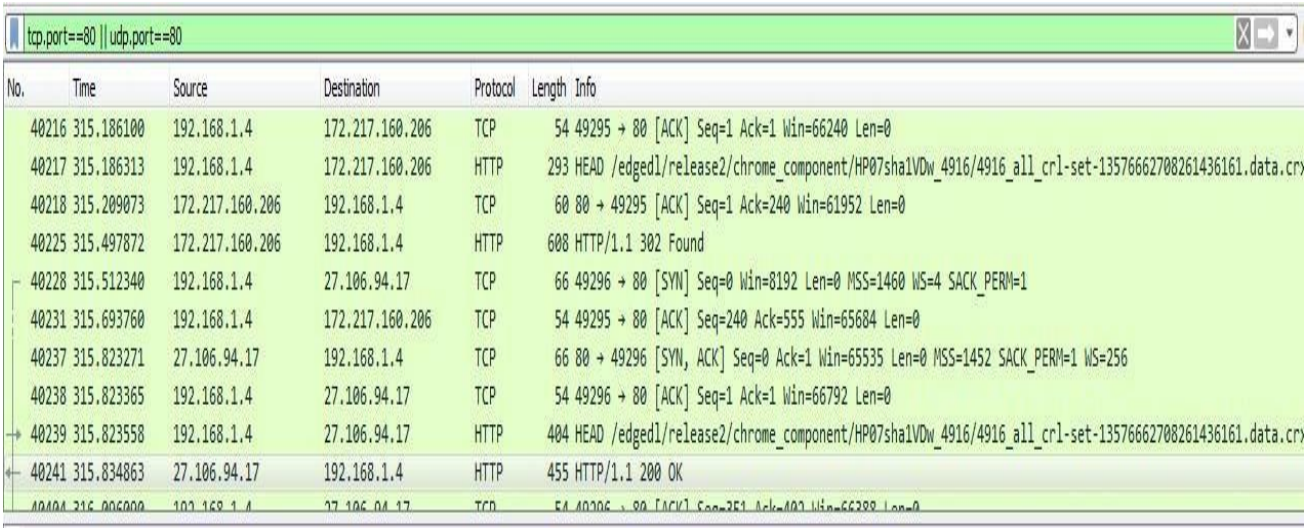
7. Display packets having no error connecting to server
   - http.response.code==200



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

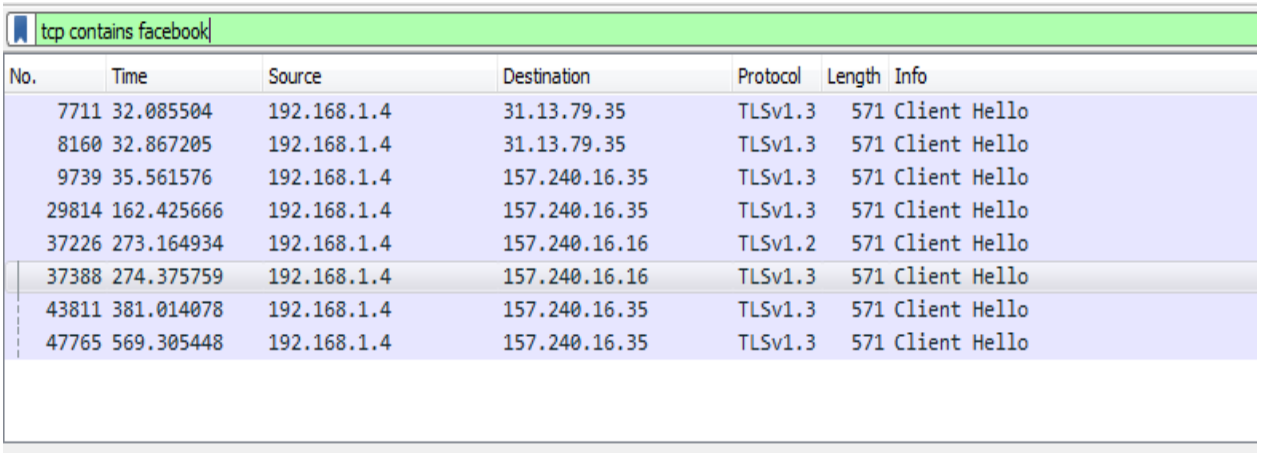
8. Display packets having port number 80
    - tcp.port==80 || udp.port==80



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 /edgedl/release2/chrome_component/HP07sha1VDw_4916/4916_all_crl-set-13576662708261436161.data.cry
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 /edgedl/release2/chrome_component/HP07sha1VDw_4916/4916_all_crl-set-13576662708261436161.data.cry
40241	315.834863	27.106.94.17	192.168.1.4	HTTP	455	HTTP/1.1 200 OK

9. Display packets which that 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:

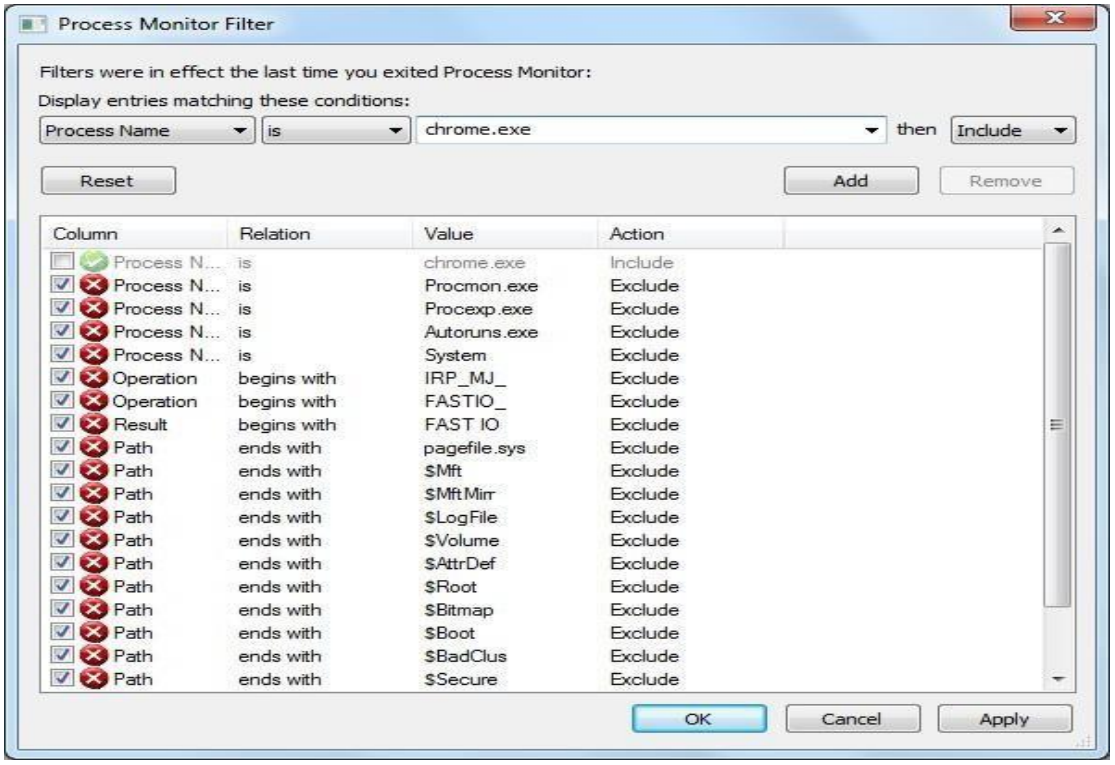
1. File and Disk Utilities
2. Networking Utilities
3. Process Utilities
4. Security Utilities
5. System Information Utilities
6. Miscellaneous Utilities

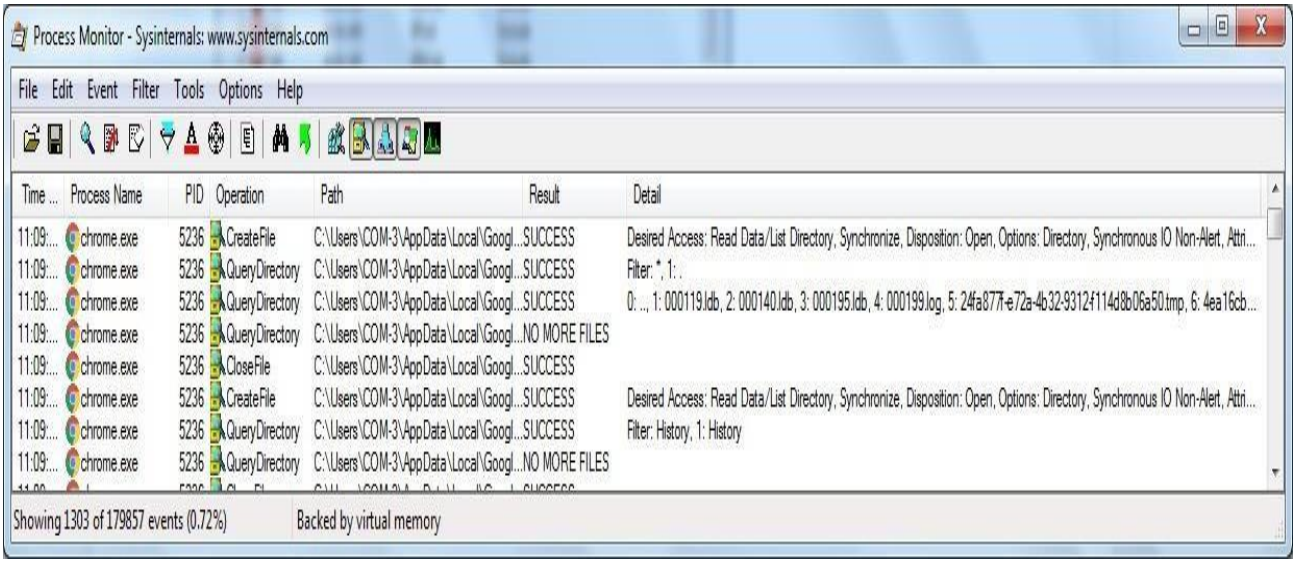
- **Monitor Live Processes : (Tool: ProcMon)**

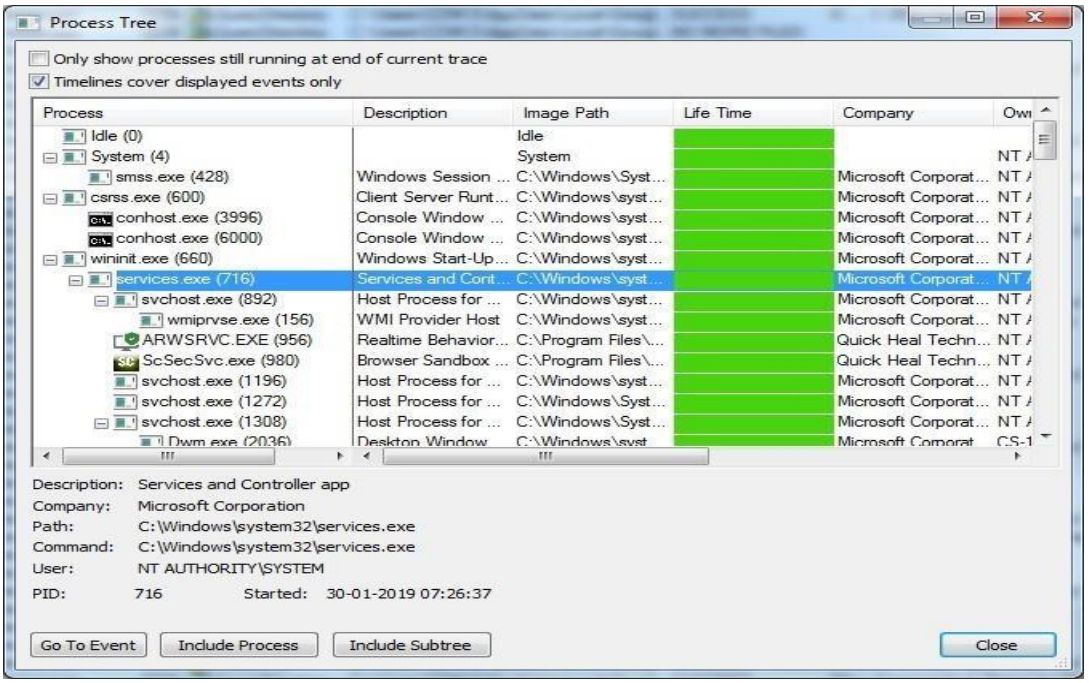
To Do:

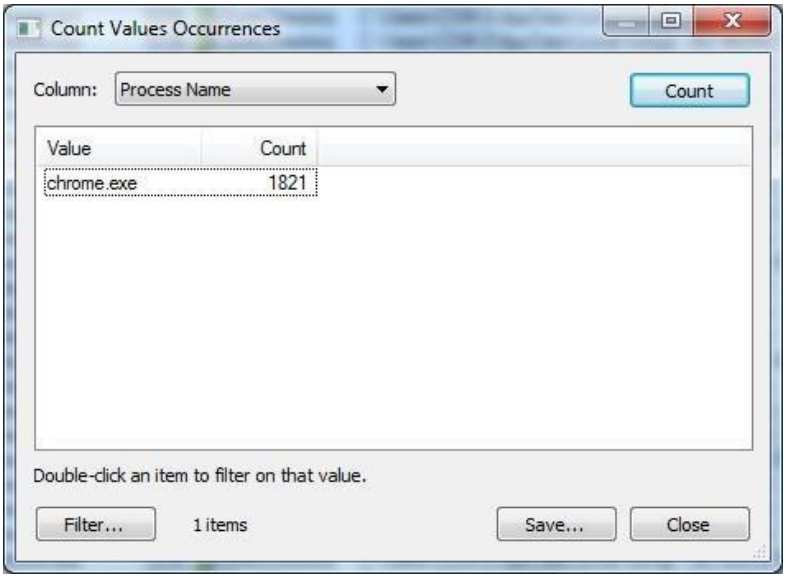
1. Filter (Process Name or PID or Architecture, etc)
2. Process Tree
3. Process Activity Summary
4. Count Occurrences

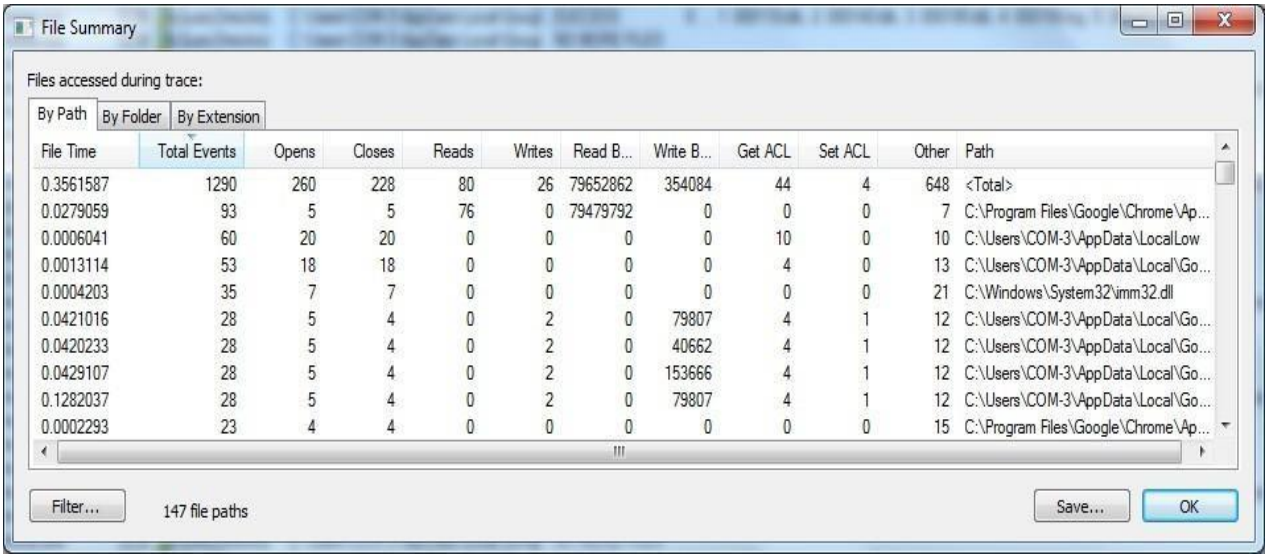
Output:


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


Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Time ... Process Name PID Operation Path Result Detail
11:09:... chrome.exe 5236 CreateFile C:\Users\COM-3\AppData\Local\Googl...SUCCESS Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Attri...
11:09:... chrome.exe 5236 QueryDirectory C:\Users\COM-3\AppData\Local\Googl...SUCCESS Filter: *, 1: .
11:09:... chrome.exe 5236 QueryDirectory C:\Users\COM-3\AppData\Local\Googl...SUCCESS 0: .., 1: 000119.ldb, 2: 000140.ldb, 3: 000195.ldb, 4: 000199.log, 5: 24fa877f-e72a-4b32-9312-f114d8b06a50.tmp, 6: 4ea16cb...
11:09:... chrome.exe 5236 QueryDirectory C:\Users\COM-3\AppData\Local\Googl...NO MORE FILES
11:09:... chrome.exe 5236 CloseFile C:\Users\COM-3\AppData\Local\Googl...SUCCESS
11:09:... chrome.exe 5236 CreateFile C:\Users\COM-3\AppData\Local\Googl...SUCCESS Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Attri...
11:09:... chrome.exe 5236 QueryDirectory C:\Users\COM-3\AppData\Local\Googl...SUCCESS Filter: History, 1: History
11:09:... chrome.exe 5236 QueryDirectory C:\Users\COM-3\AppData\Local\Googl...NO MORE FILES
Showing 1303 of 179857 events (0.72%)
Backed by virtual memory


Process Tree
Only show processes still running at end of current trace
Timelines cover displayed events only
Process
Description
Image Path
Life Time
Company
Idle (0)
System (4)
smss.exe (428)
csrss.exe (600)
conhost.exe (3996)
conhost.exe (6000)
wininit.exe (660)
services.exe (716)
svchost.exe (892)
wmiprvse.exe (156)
ARWSRVC.EXE (956)
ScSecSvc.exe (980)
svchost.exe (1196)
svchost.exe (1272)
svchost.exe (1308)
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

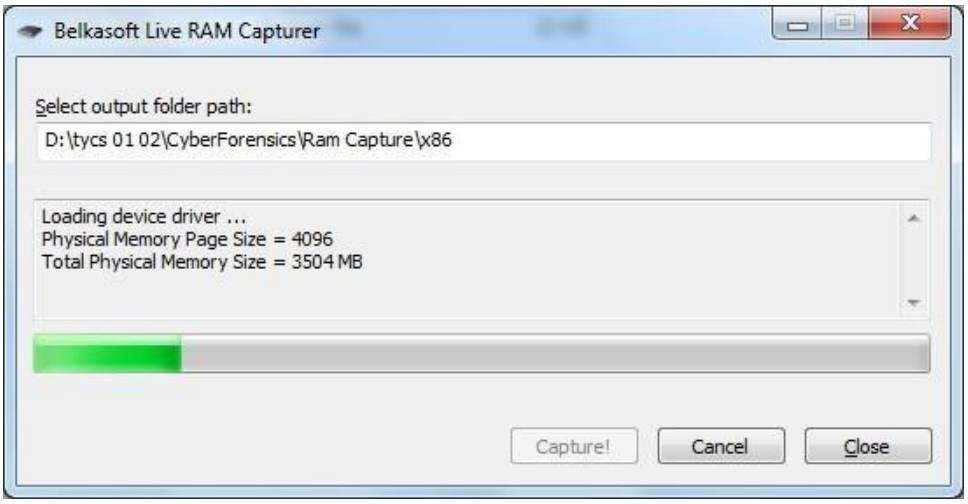

File Summary
Files accessed during trace:
By Path
By Folder
By Extension
File Time
Total Events
Opens
Closes
Reads
Writes
Read B...
Write B...
Get ACL
Set ACL
Other
Path
0.3561587 1290 260 228 80 26 79652862 354084 44 4 648 <Total>
0.0279059 93 5 5 76 0 79479792 0 0 0 7 C:\Program Files\Google\Chrome\Ap...
0.0006041 60 20 20 0 0 0 0 10 0 10 C:\Users\COM-3\AppData\LocalLow
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

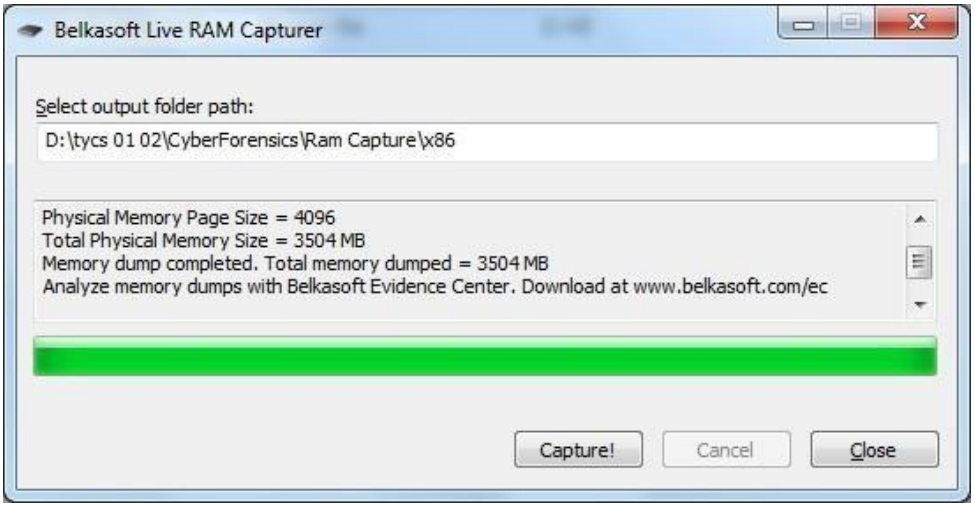
- **Capture RAM (Tool: RAMCapture)**

To Do:

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

Output:



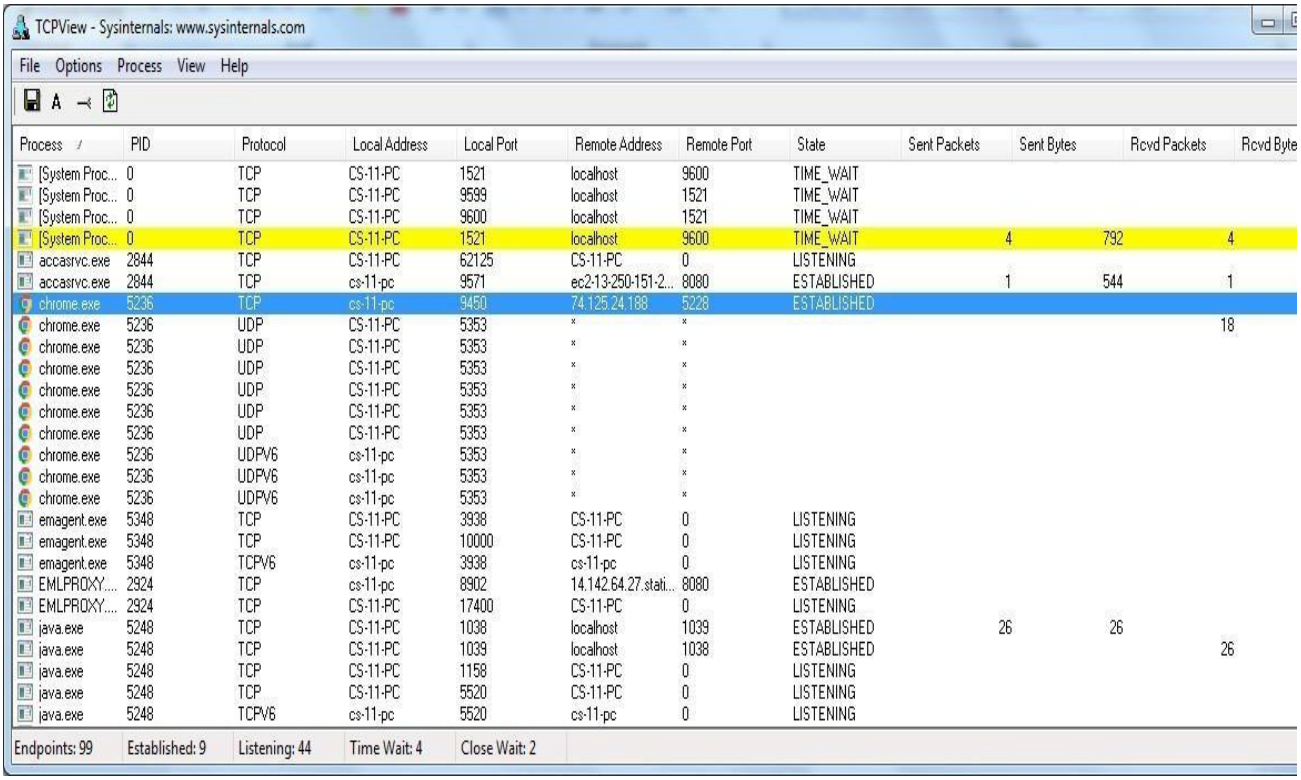


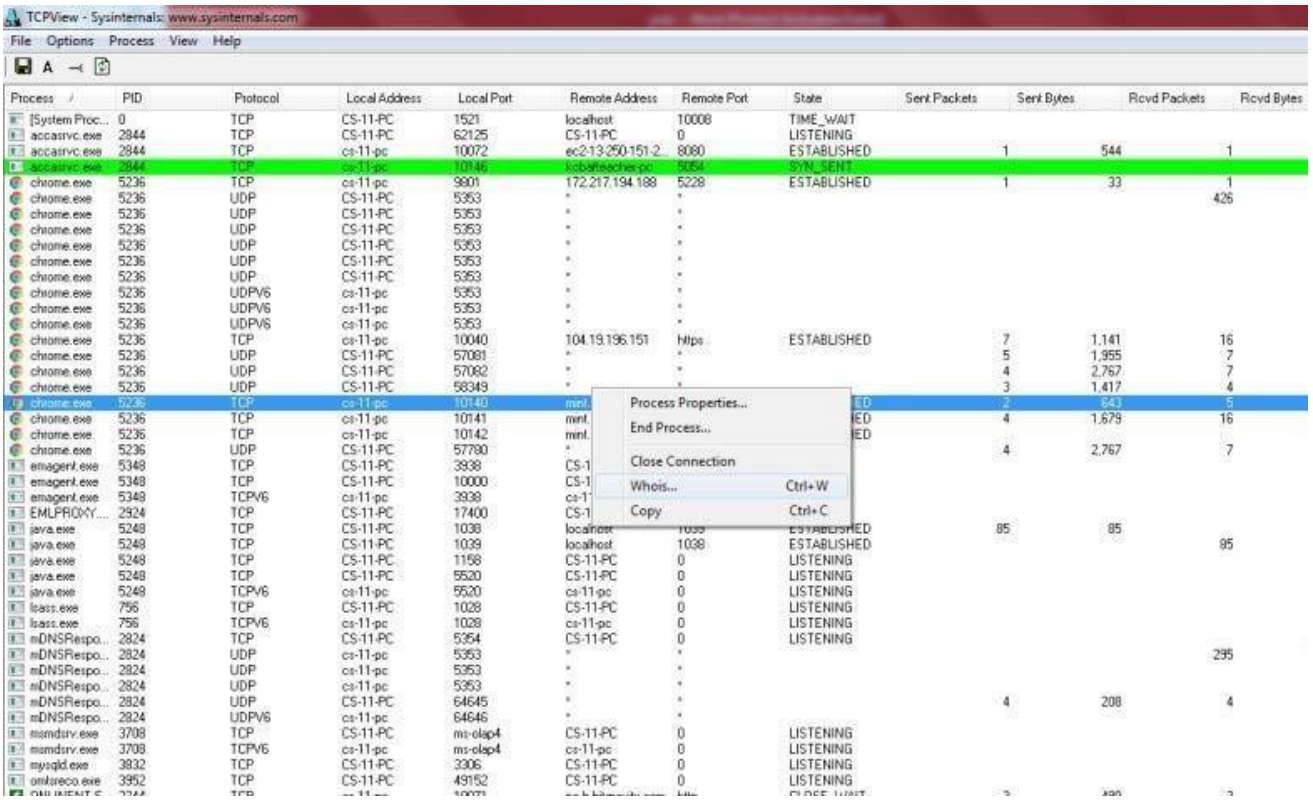
- **Capture TCP/UDP packets (Tool: TcpView) :**

To Do: 1. Save to .txt file.

2. Whois

Output:




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 Properties...
End Process...
Close Connection
Whois... Ctrl+W
Copy Ctrl+C

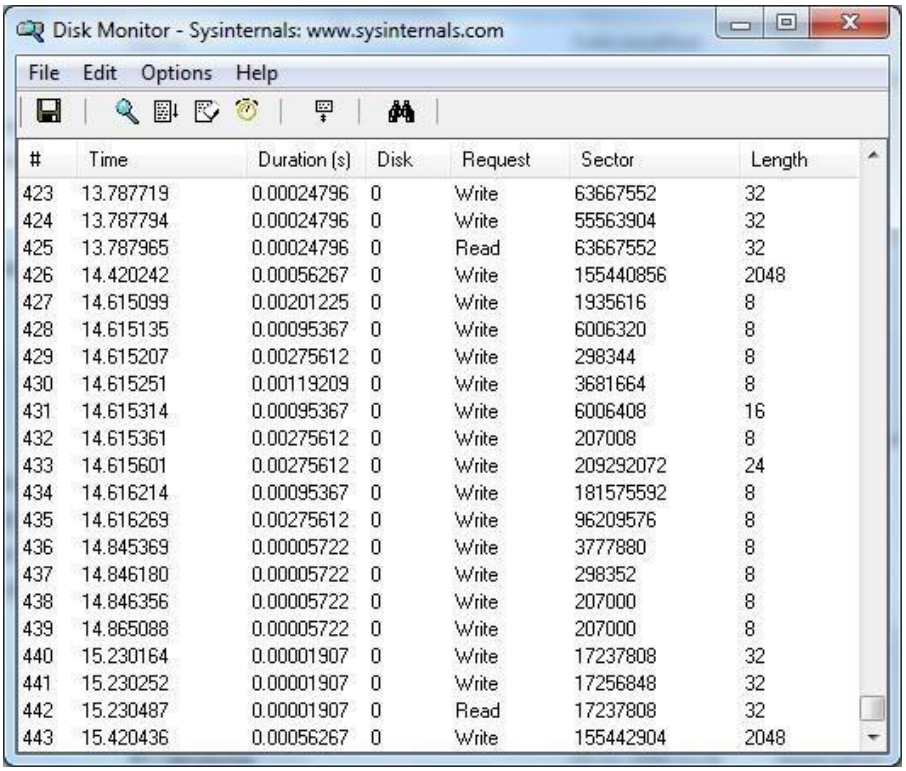

mint.whois.com
Domain ID: 809888_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.PublicDomainRegistry.com
Registrar URL: http://www.publicdomainregistry.com
Updated Date: 2018-05-02T13:14:37Z
Creation Date: 1995-04-11T04:00:00Z
Registry Expiry Date: 2028-04-12T04:00:00Z
Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com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

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

To Do:

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

Output :



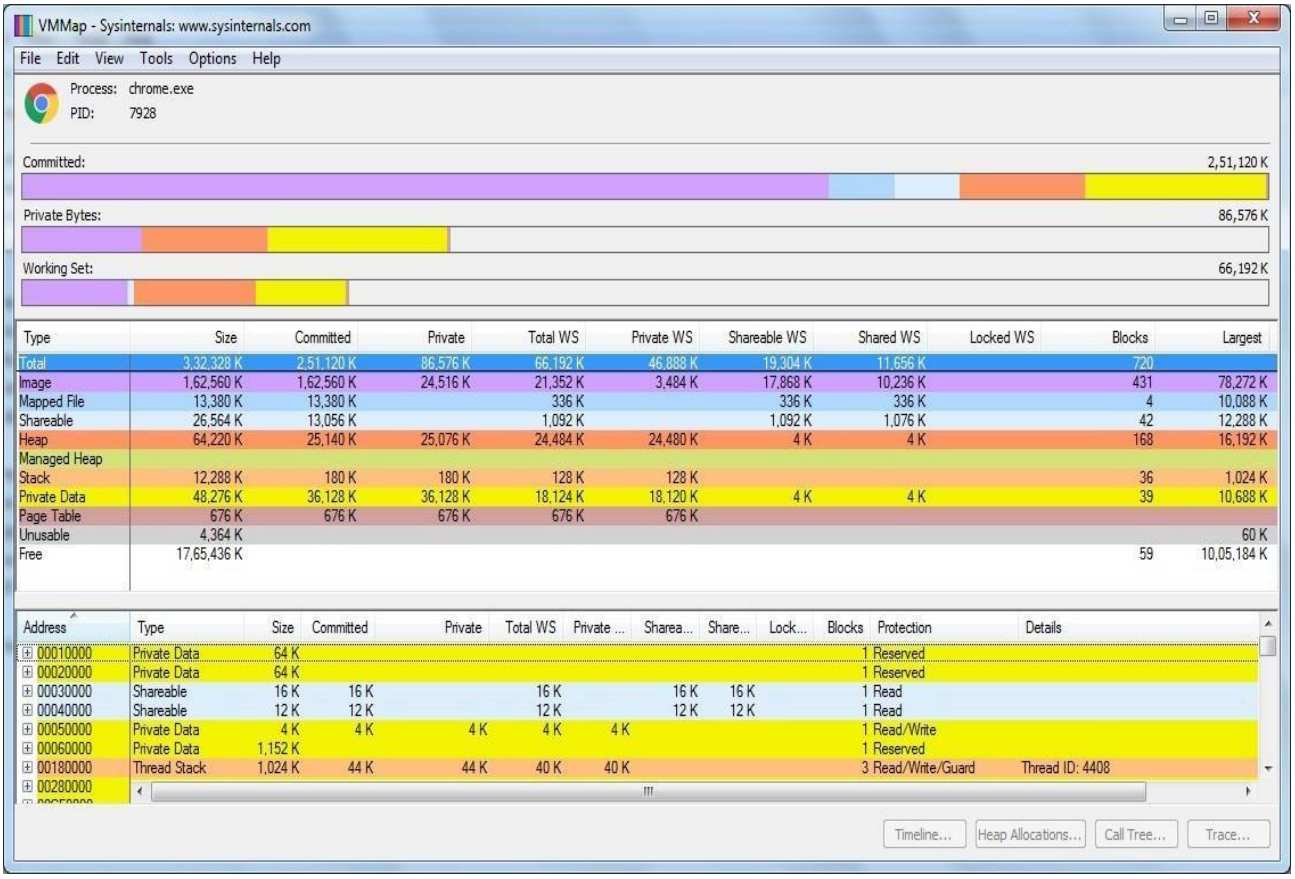
#	Time	Duration (s)	Disk	Request	Sector	Length
423	13.787719	0.00024796	0	Write	63667552	32
424	13.787794	0.00024796	0	Write	55563904	32
425	13.787965	0.00024796	0	Read	63667552	32
426	14.420242	0.00056267	0	Write	155440856	2048
427	14.615099	0.00201225	0	Write	1935616	8
428	14.615135	0.00095367	0	Write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

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

To Do:

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

Output :

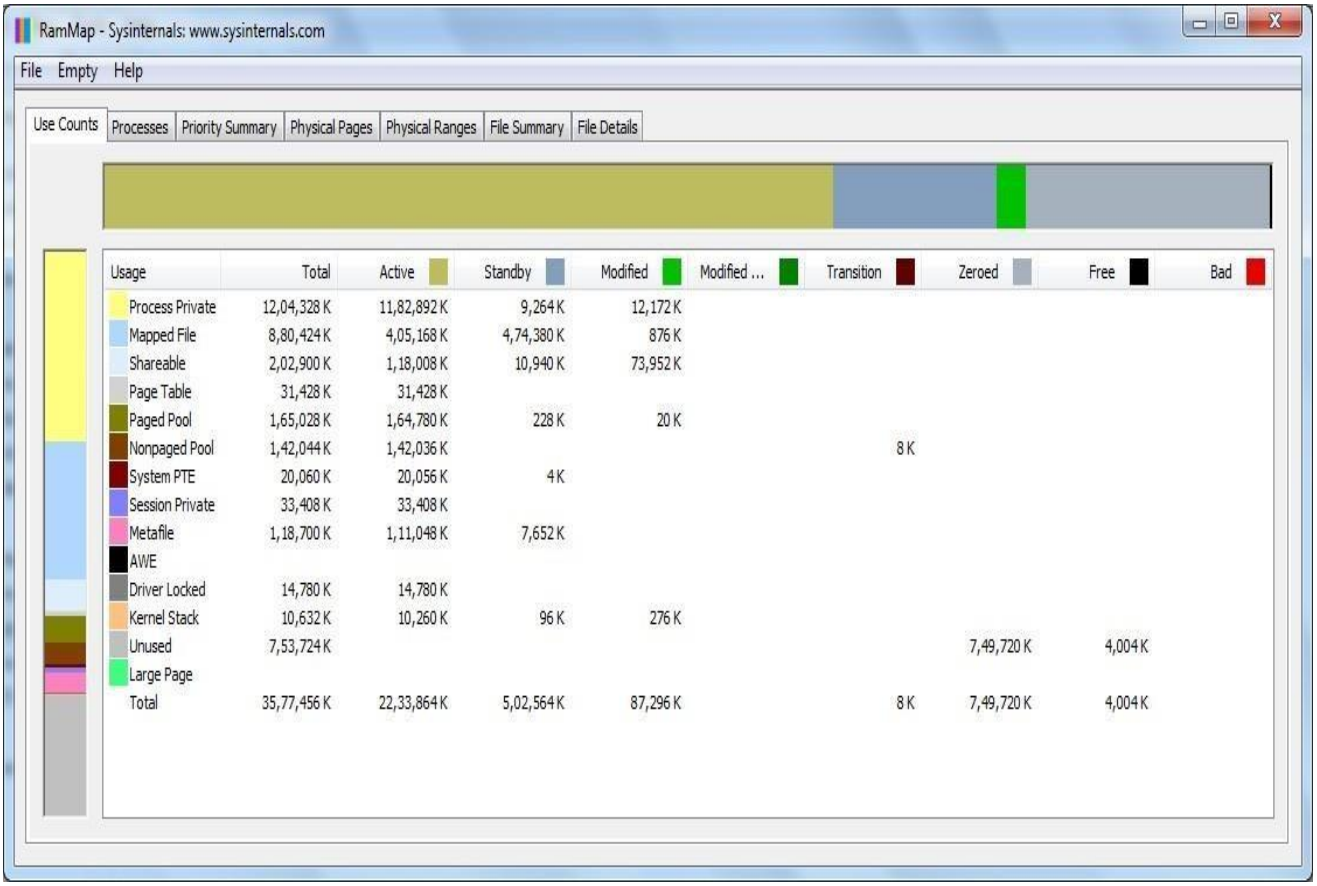


- **Monitor Cache Memory**
  (Tool: RAMMap)

TO DO :

1. Save to .RMP file.

Output:



PRACTICAL 6

AIM : - Recovering and Inspecting deleted files

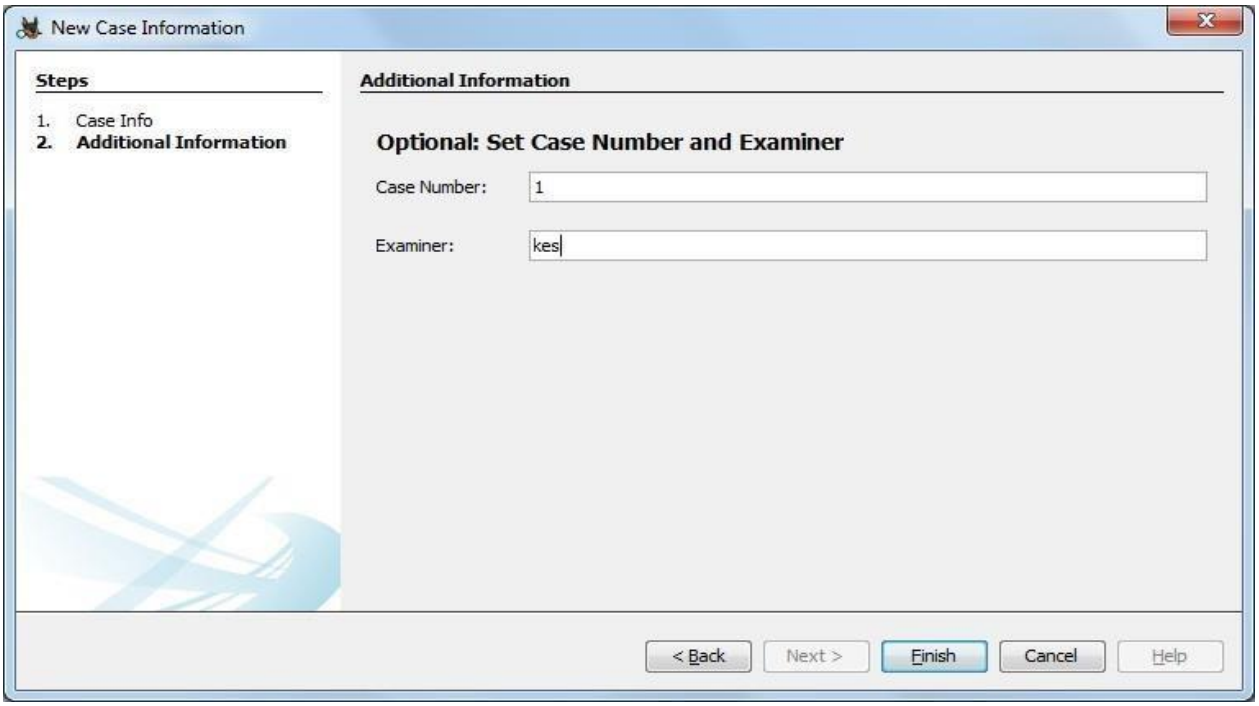
- Check for Deleted Files
- Recover the Deleted Files
-Analyzing and Inspecting the recovered files

Step 1: Start Autopsy from Desktop.

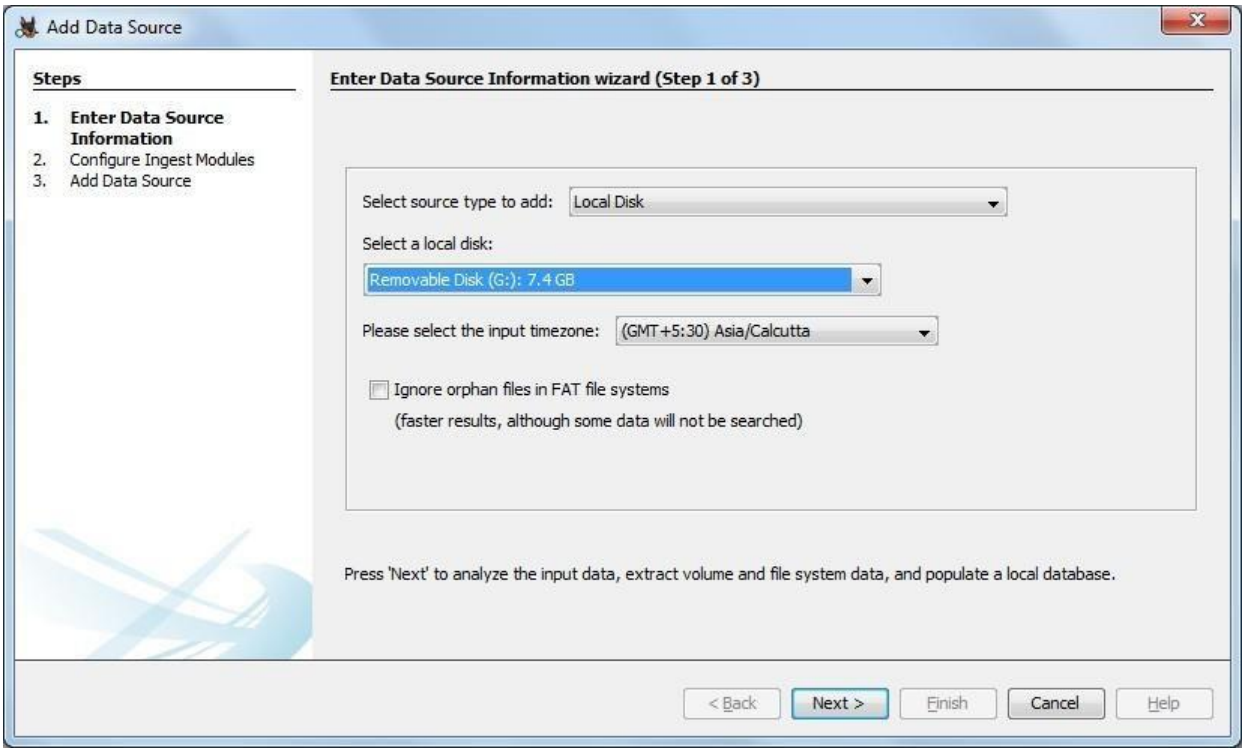
Step 2: Now create on New Case.

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

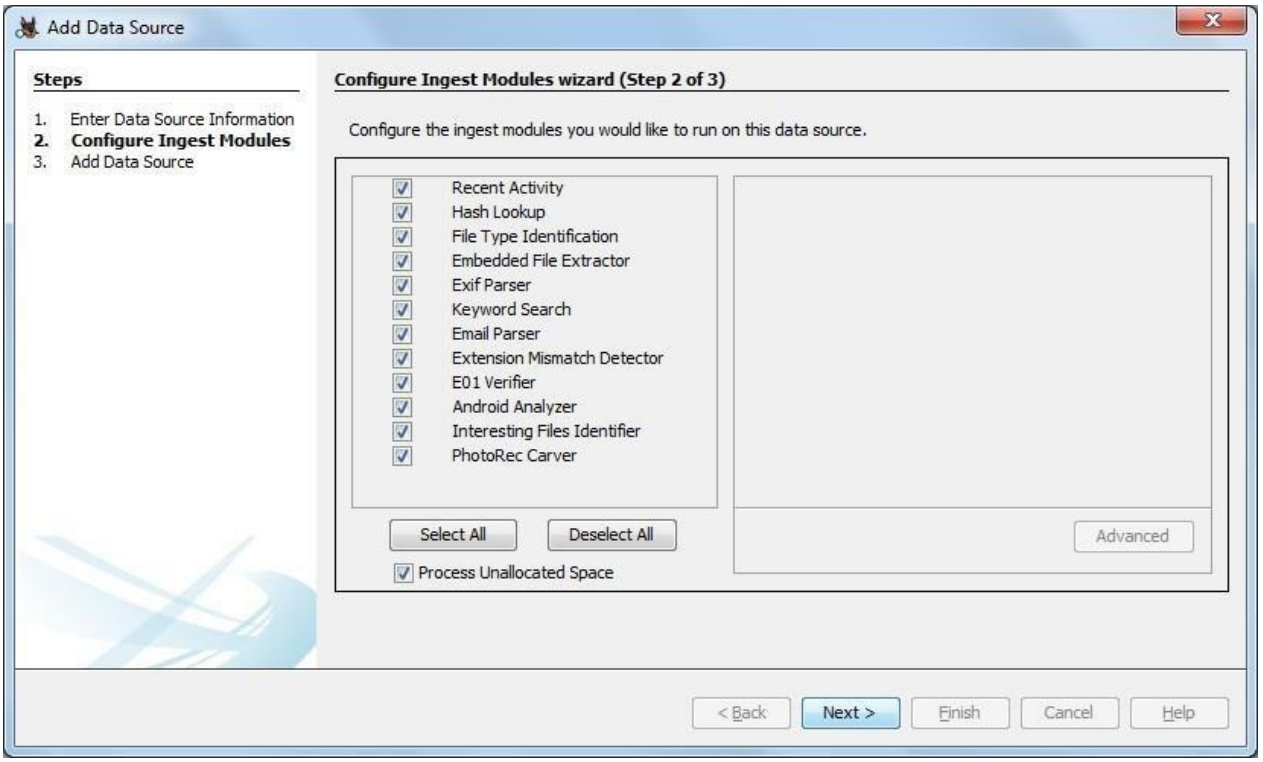
Step 4: Enter the additional Information and click on Finish.



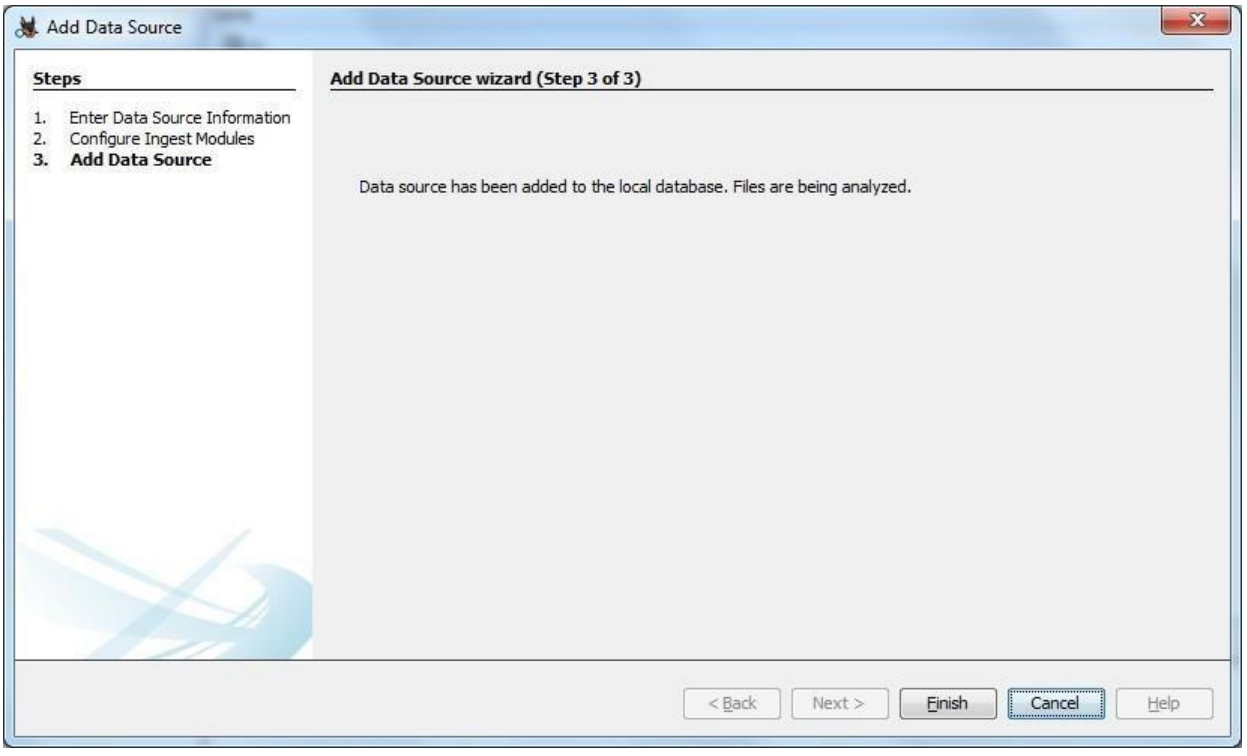
Step 5: Now Select Source Type as Local disk and Select Local disk form drop down list and click on Next.



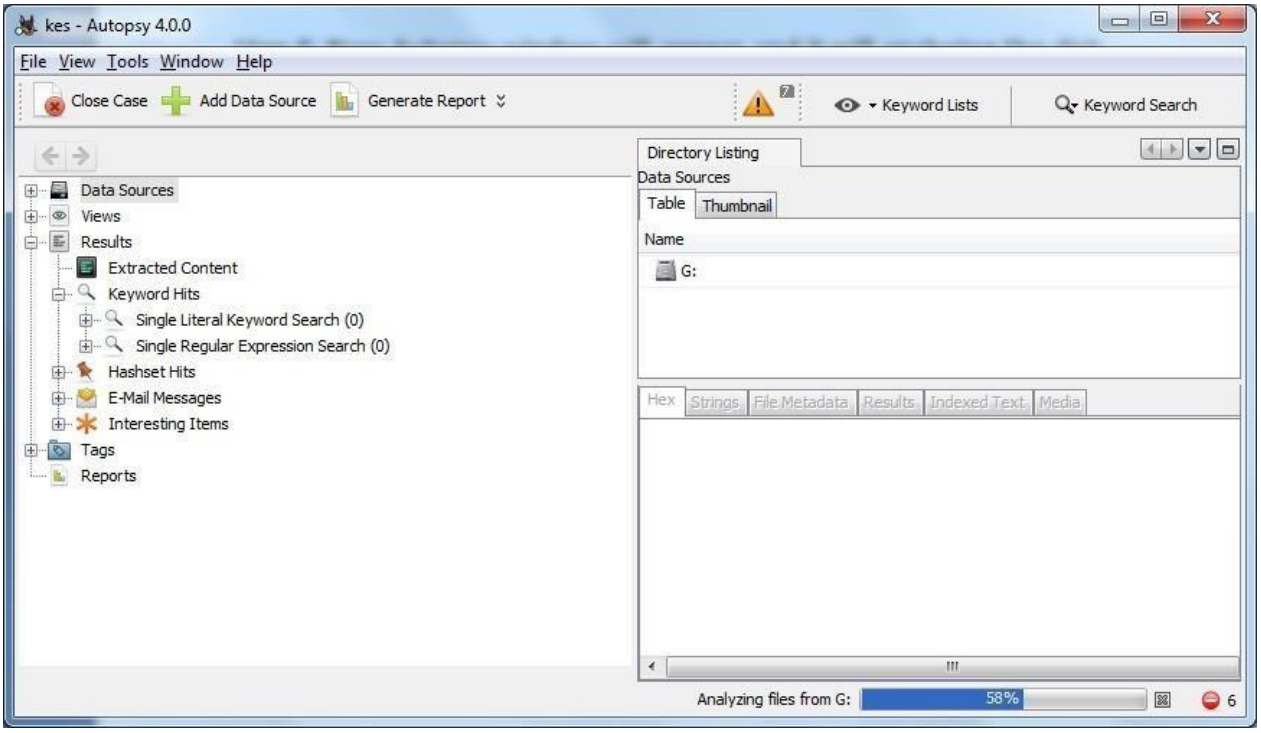
Step 6: Click on Next Button.



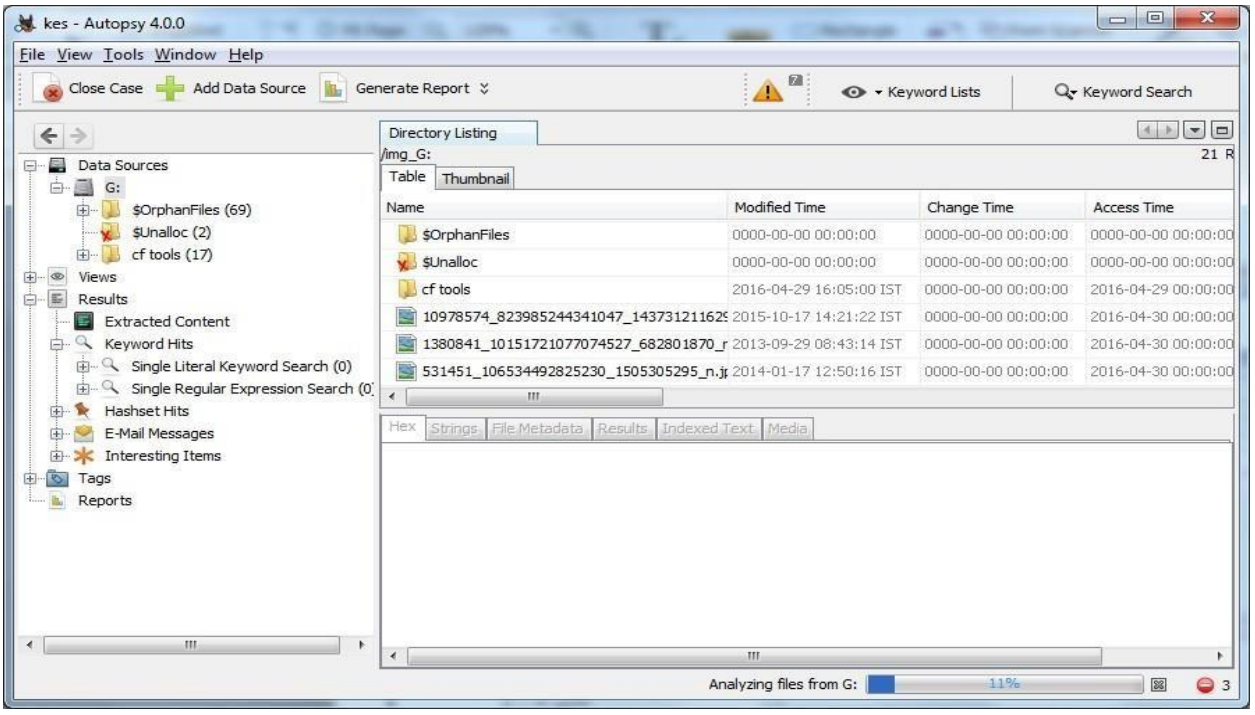
Step 7: Now click On Finish.



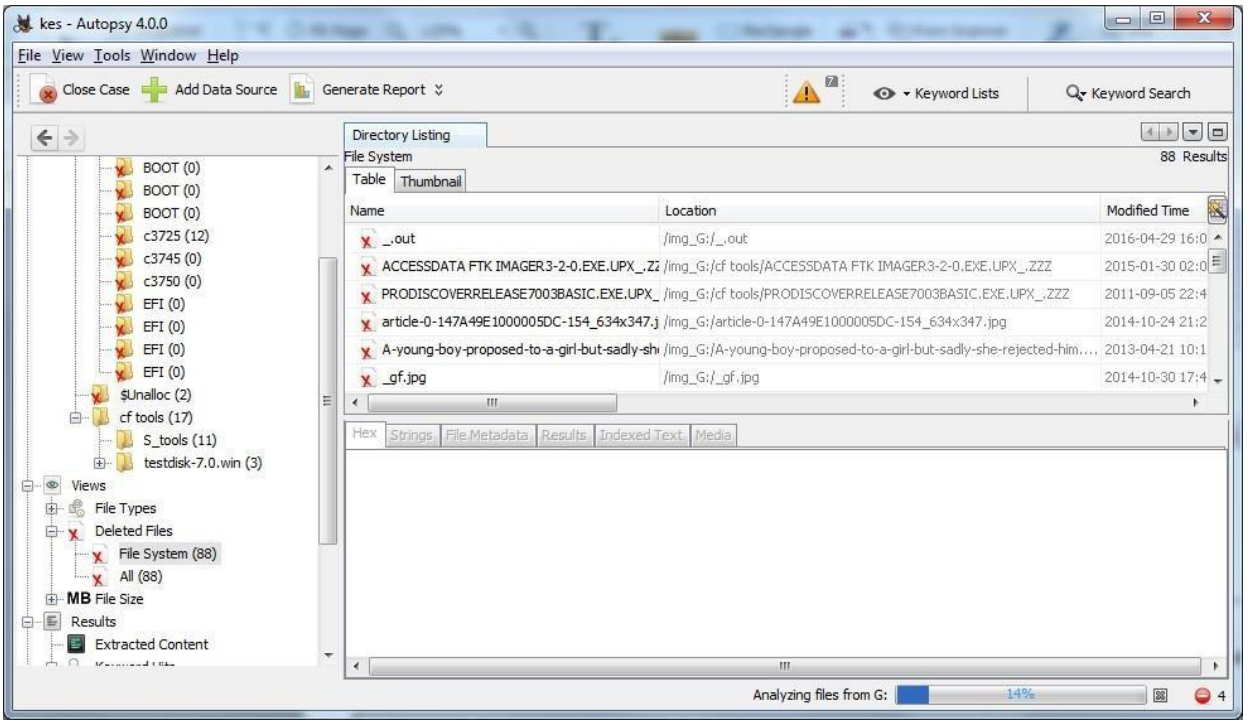
Step 8: Now Autopsy window will appear and it will analyzing the disk that we have selected.



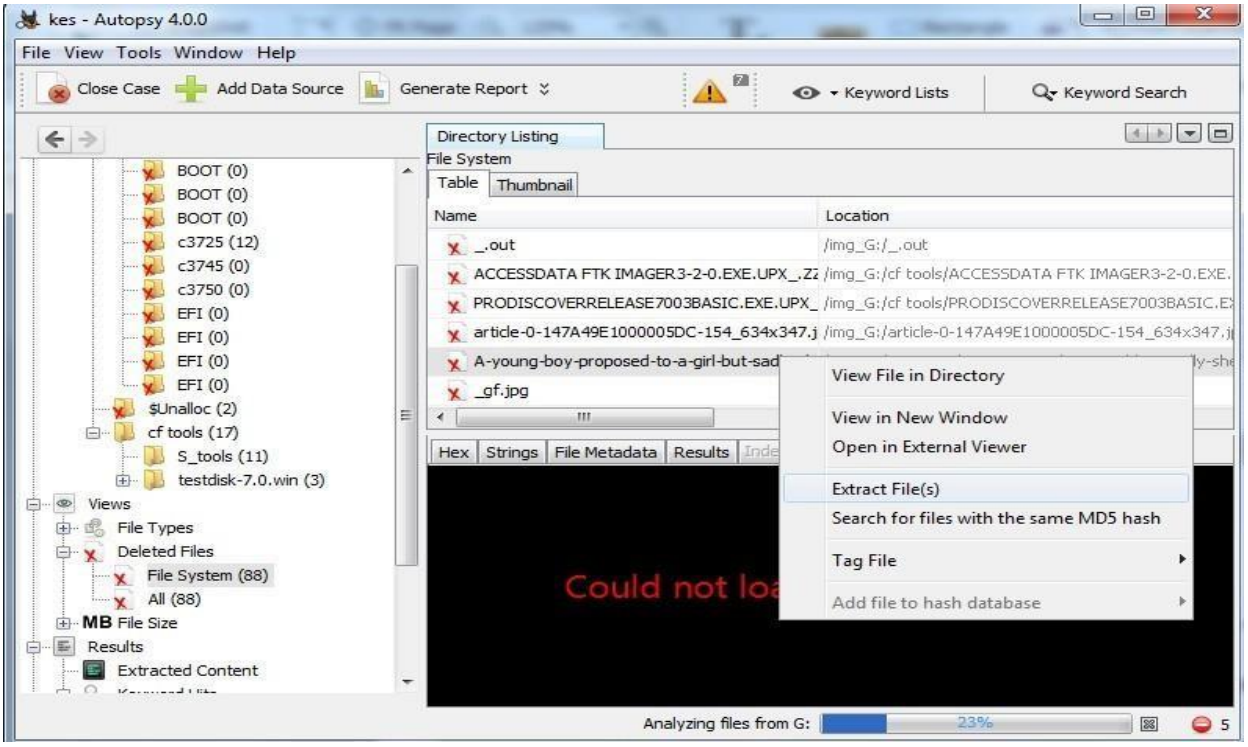
Step 9: All files will appear in table tab select any file to see the data.



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



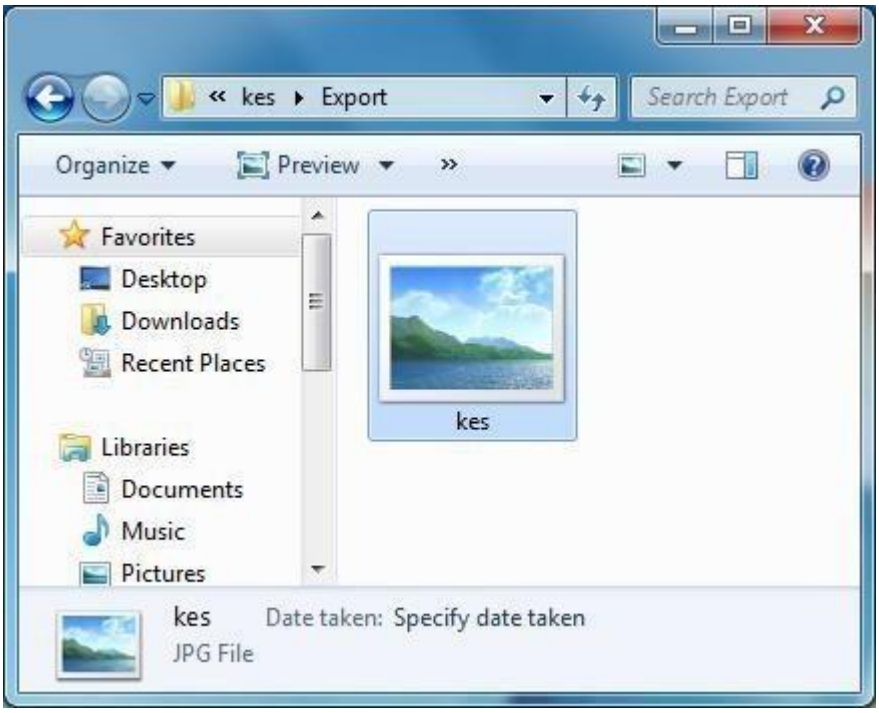
Step 11: To recover the file, go to view node-> Deleted Files node , here select any file and right click on it than select Extract Files option.



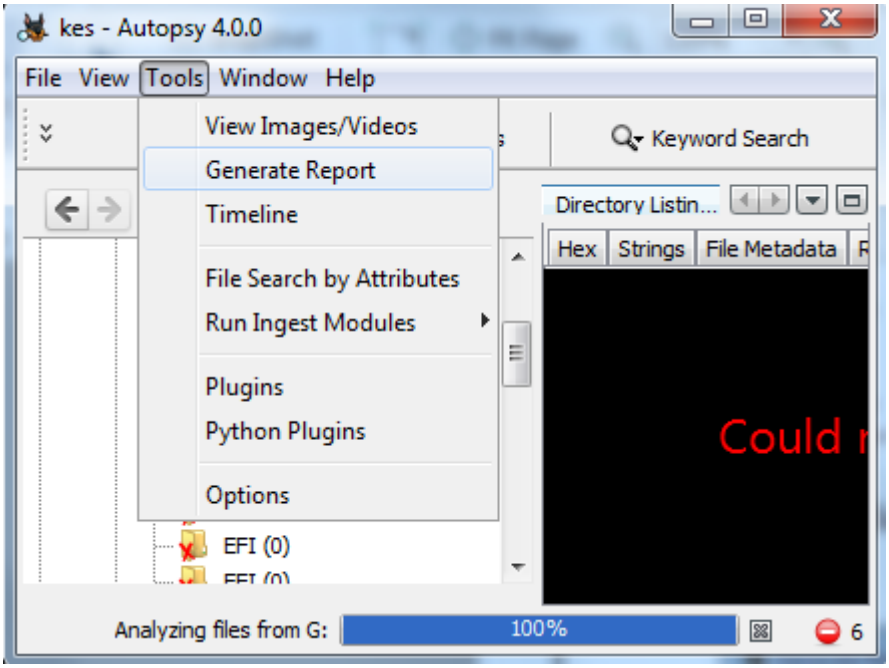
Step 12: By default Export folder is choose to save the recovered file.

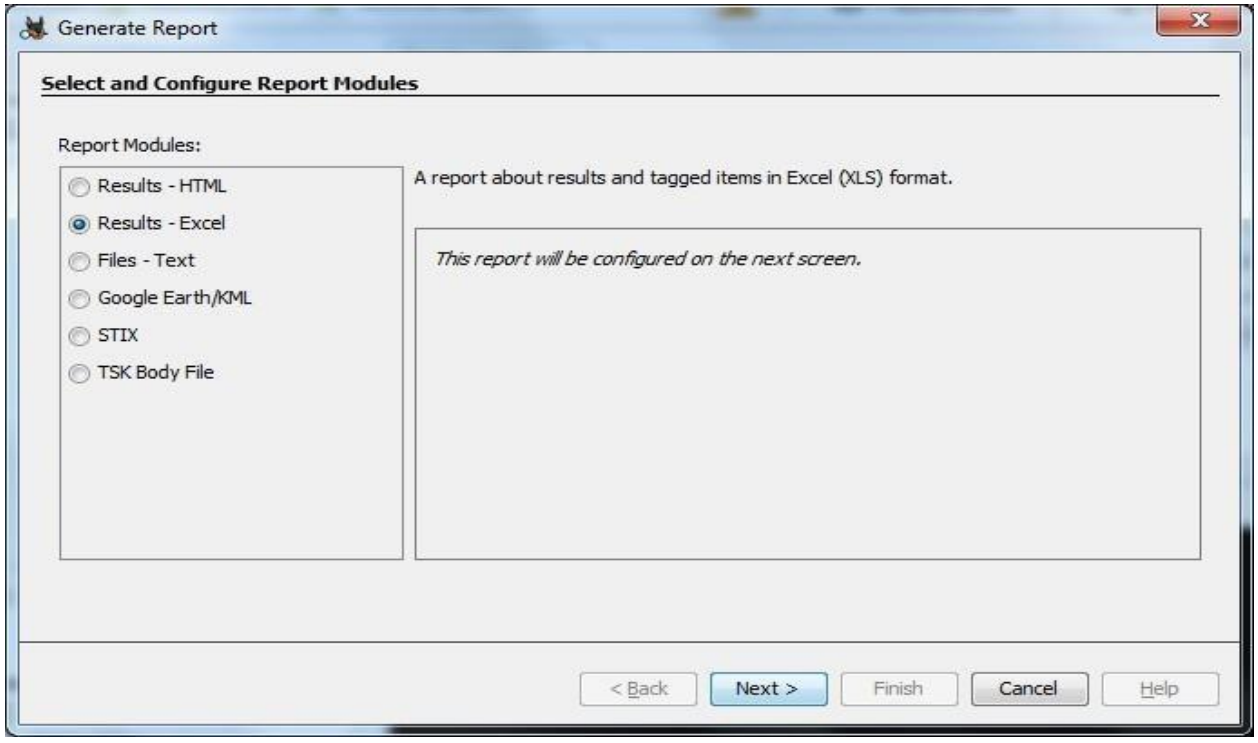
Sep 13 : Now Click on Ok.

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

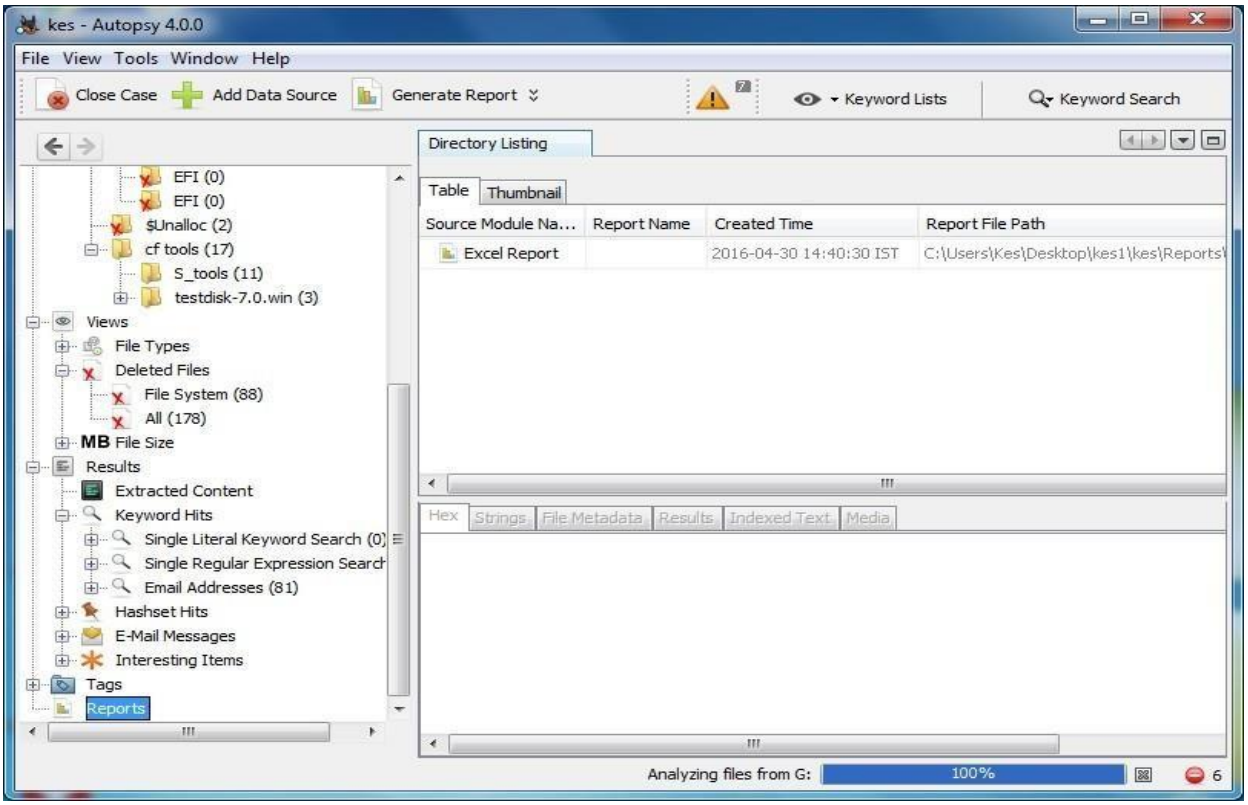


Step 15: Click on Generate Report from autopsy window and Select the Excel format and click on next.

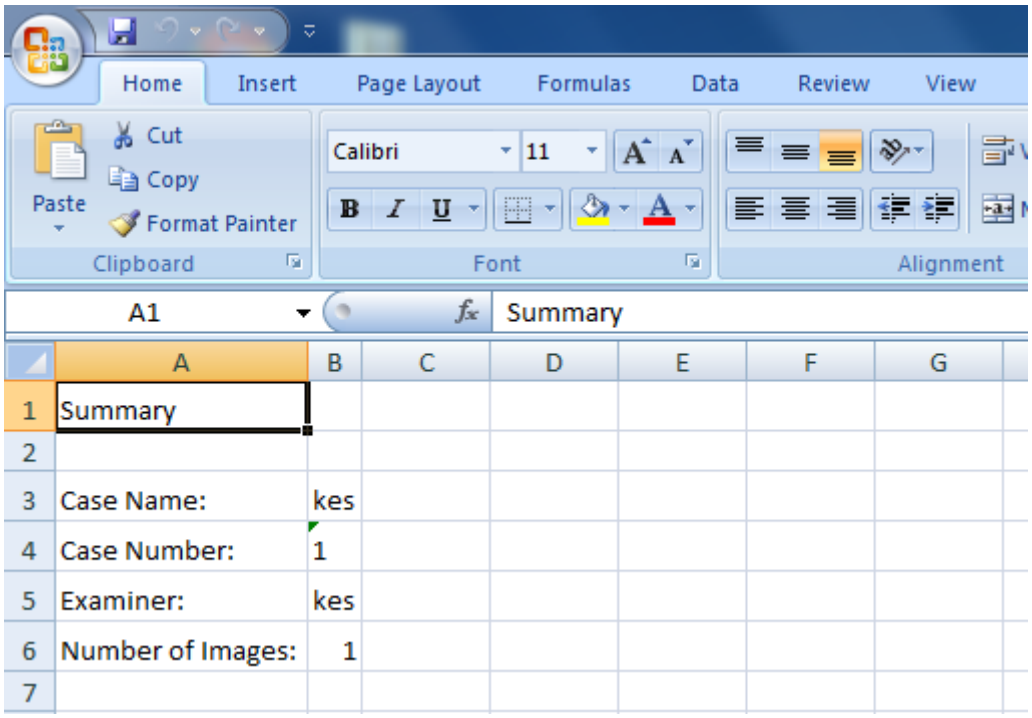




Step 16: Now Report is Generated So click on close Button .we can see the Report on Report Node.



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



Practical 7

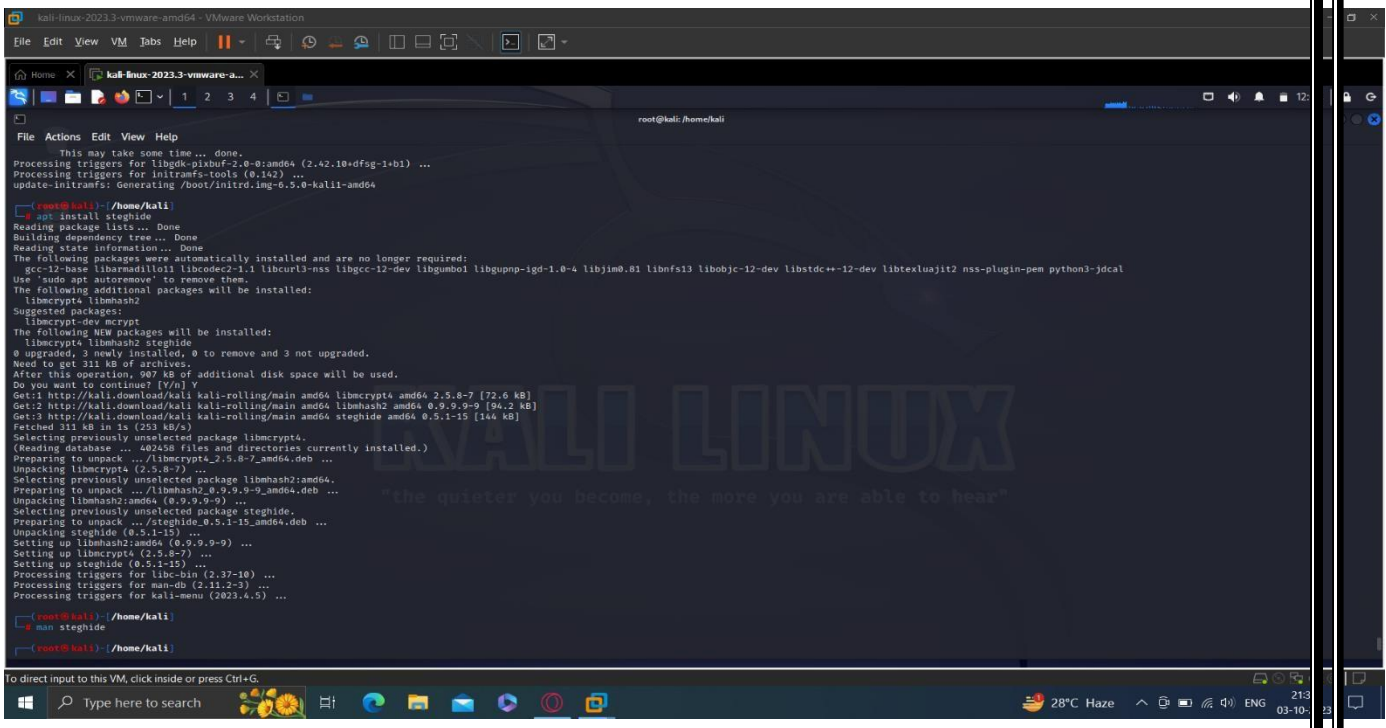
Aim : - Steganography Detection

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

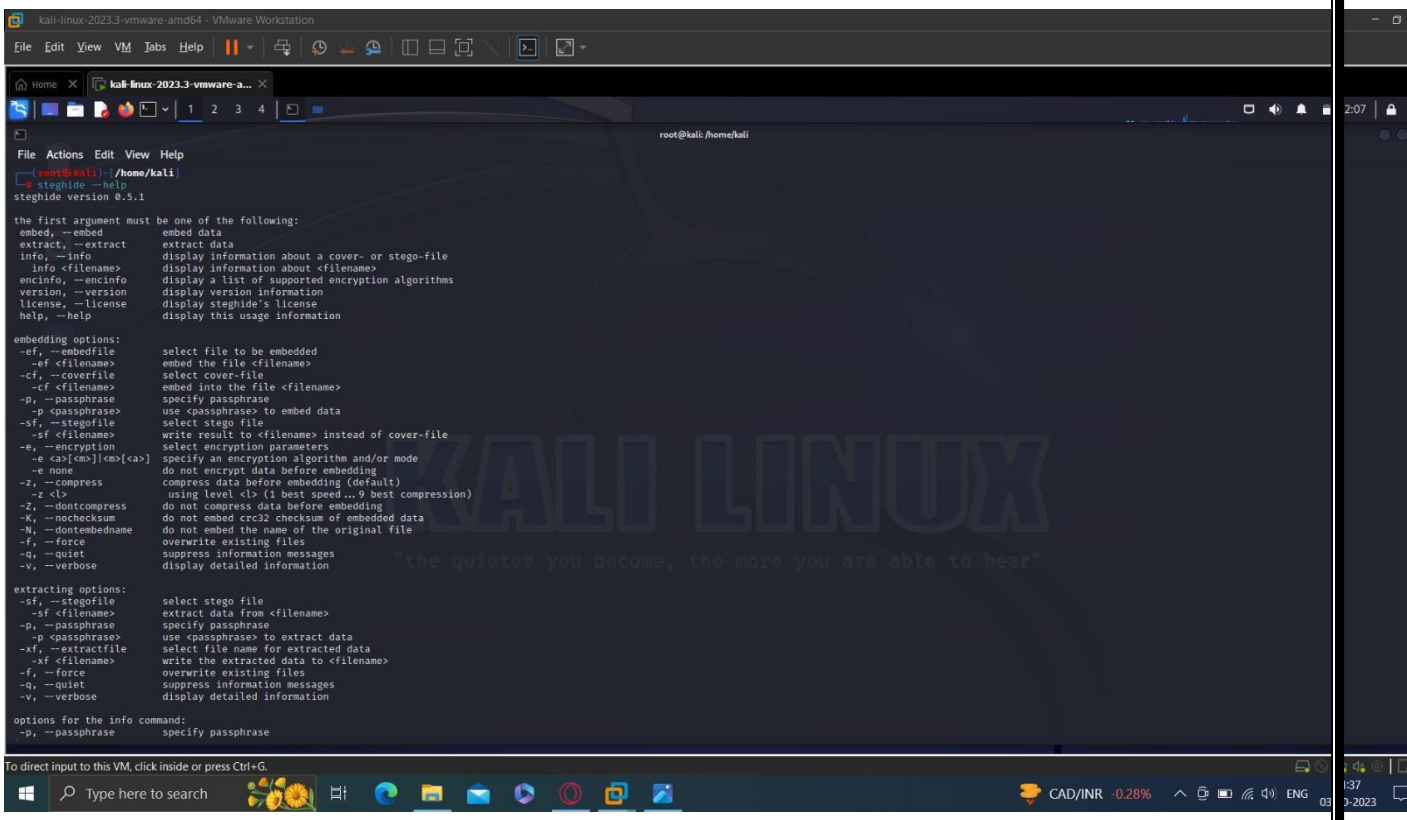
Steps:-

1) Intsall Steghide Tool On Linux

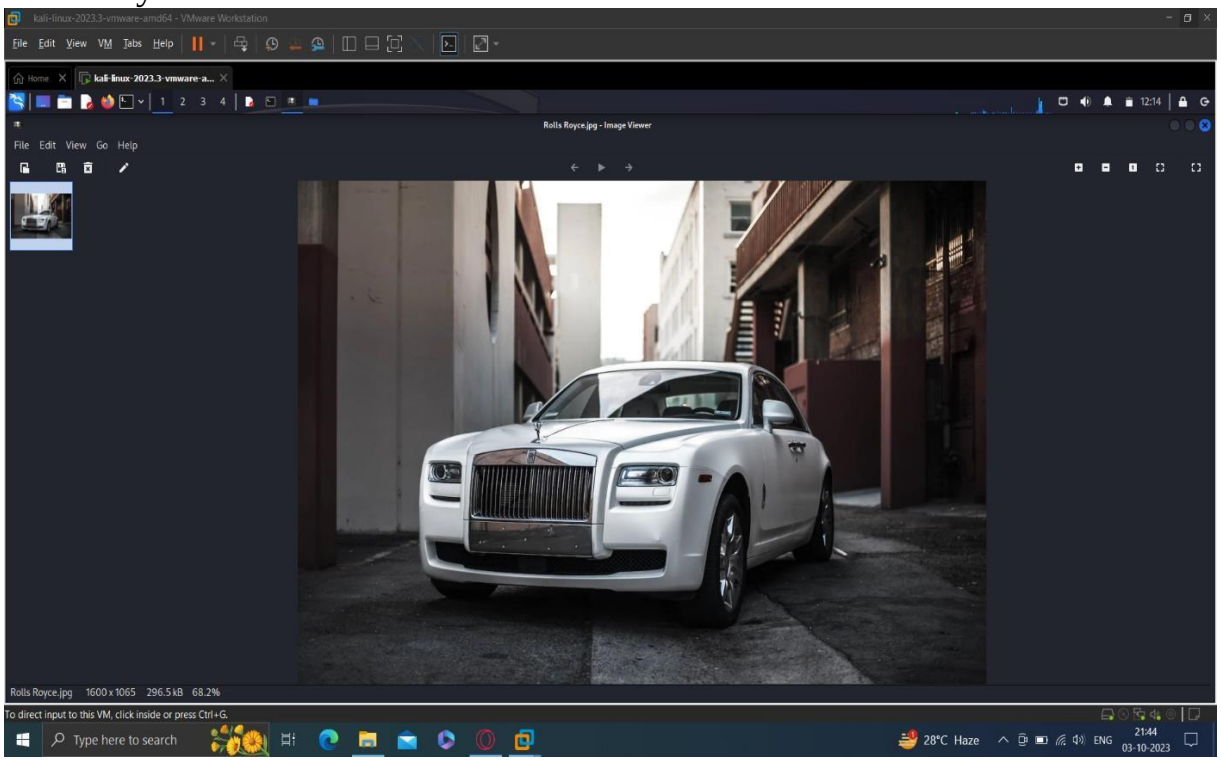


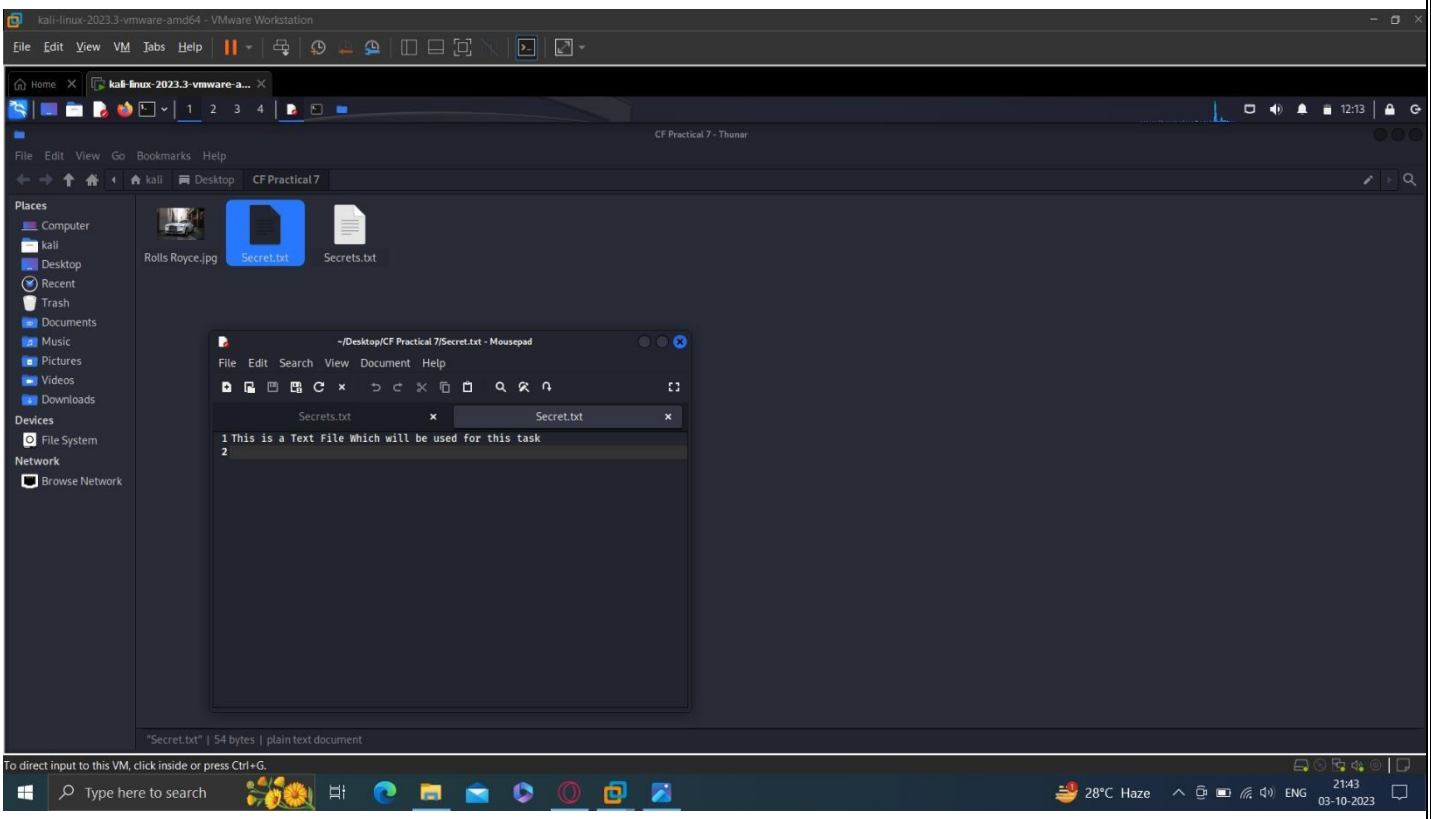
Command :- apt Install Steghide

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



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

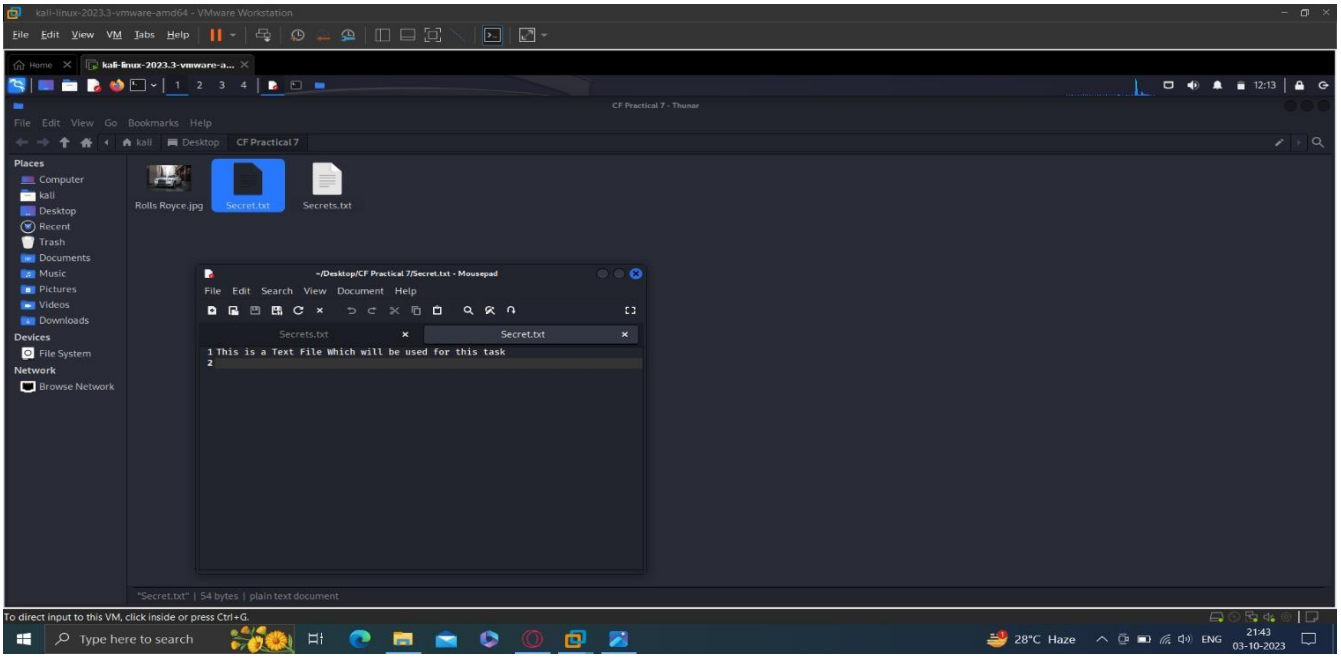
```
┌──(root㉿kali)-[/home/kali]
└─# steghide embed -ef '/home/kali/Desktop/CF Practical 7/Secret.txt'  -cf '/home/kali/Desktop/CF Practical 7/Rolls Royce.jpg' -p abcd1234
embedding "/home/kali/Desktop/CF Practical 7/Secret.txt" in "/home/kali/Desktop/CF Practical 7/Rolls Royce.jpg"... done
```

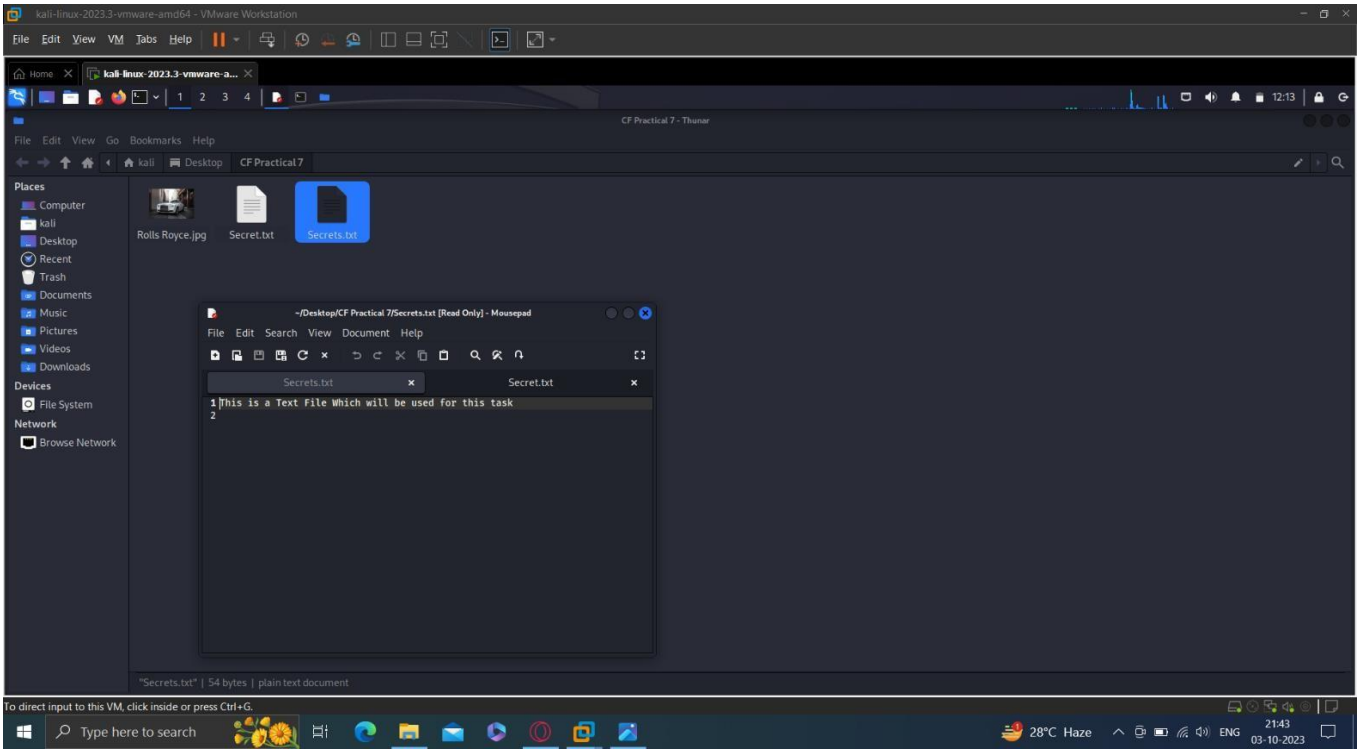
To Do this use the above command
Here -ef means embed File which is the File to be Embeded i.e the txt file from which we want to hide the text in the Image and -cf means cover file i.e the file in which we want to hide the text

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.t t'
wrote extracted data to "/home/kali/Desktop/CF Practical 7/Secrets.txt".
```

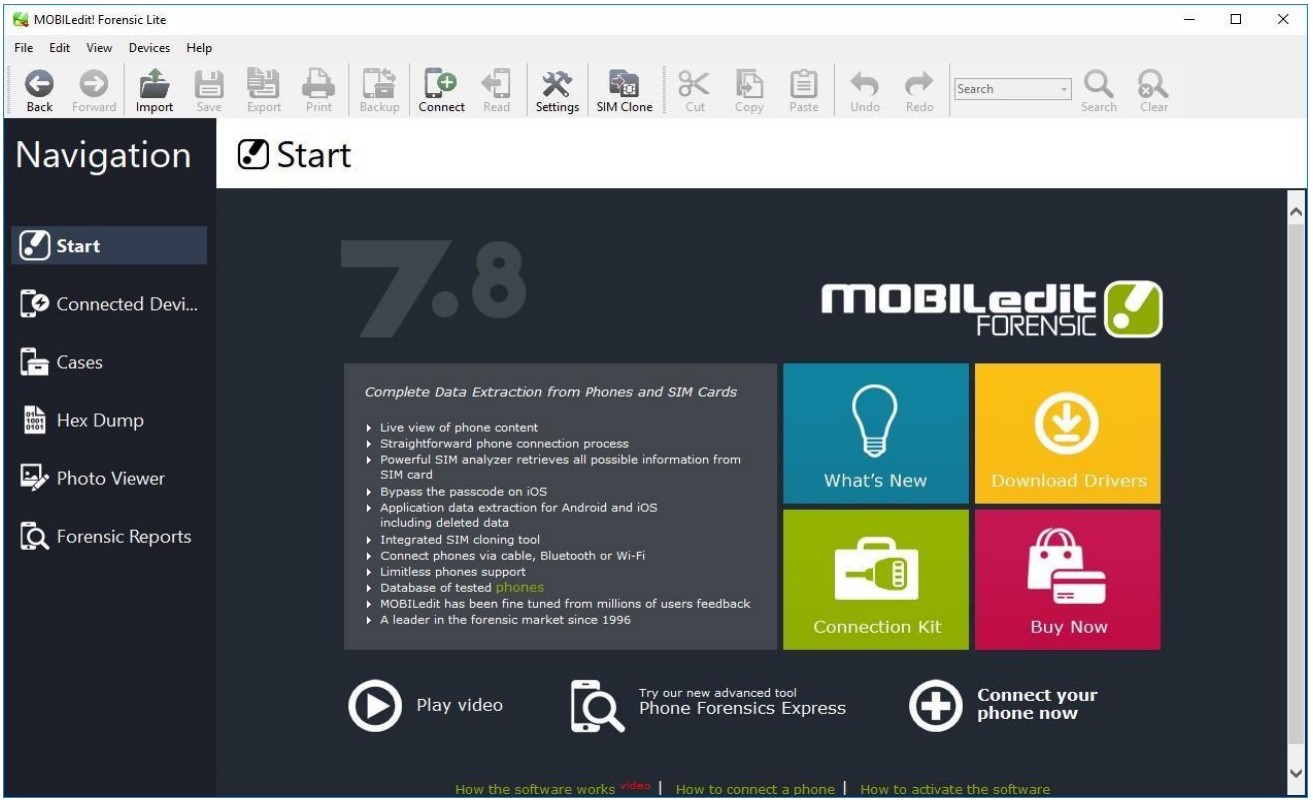
To do this use Above Command
Here -sf Means Stego File i.e the File From which we want to extract the Hidden data and -xf means extractfile i.e the File in which the Hidden Data Will be Extracted

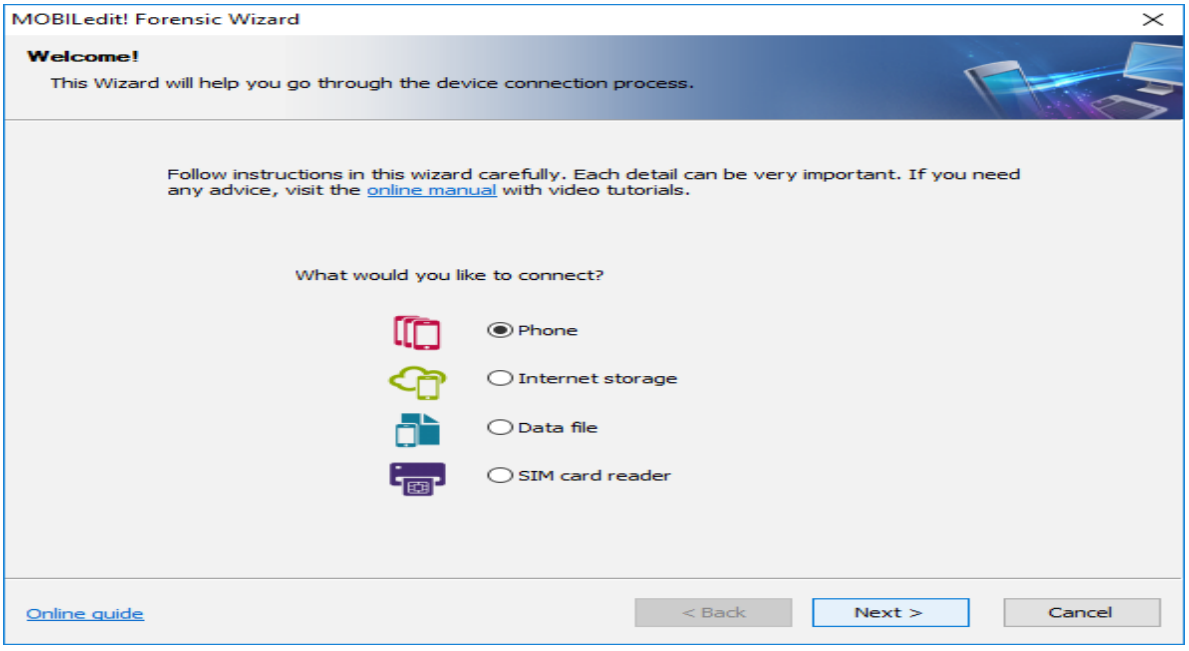

kali-linux-2023.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
CF Practical 7 - Thunar
File Edit View Go Bookmarks Help
kali Desktop CF Practical 7
Places
Computer
kali
Desktop
Recent
Trash
Documents
Music
Pictures
Videos
Downloads
Devices
File System
Network
Browse Network
Rolls Royce.jpg
Secret.txt
Secrets.txt
~/Desktop/CF Practical 7/Secret.txt - Mousepad
File Edit Search View Document Help
Secrets.txt
Secret.txt
1 This is a Text File Which will be used for this task
2
"Secret.txt" | 54 bytes | plain text document
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
28°C Haze
ENG
21:43
03-10-2023

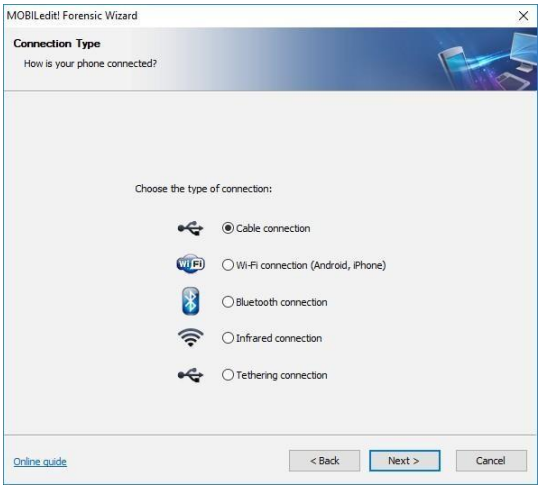

kali-linux-2023.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
CF Practical 7 - Thunar
File Edit View Go Bookmarks Help
kali Desktop CF Practical 7
Places
Computer
kali
Desktop
Recent
Trash
Documents
Music
Pictures
Videos
Downloads
Devices
File System
Network
Browse Network
Rolls Royce.jpg
Secret.txt
Secrets.txt
~/Desktop/CF Practical 7/Secrets.txt [Read Only] - Mousepad
File Edit Search View Document Help
Secrets.txt
Secret.txt
1 This is a Text File Which will be used for this task
2
"Secrets.txt" | 54 bytes | plain text document
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
28°C Haze
ENG
21:43
03-10-2023

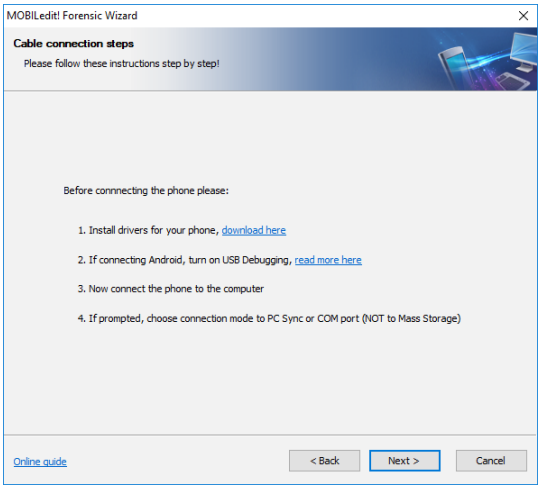
PRACTICAL 8

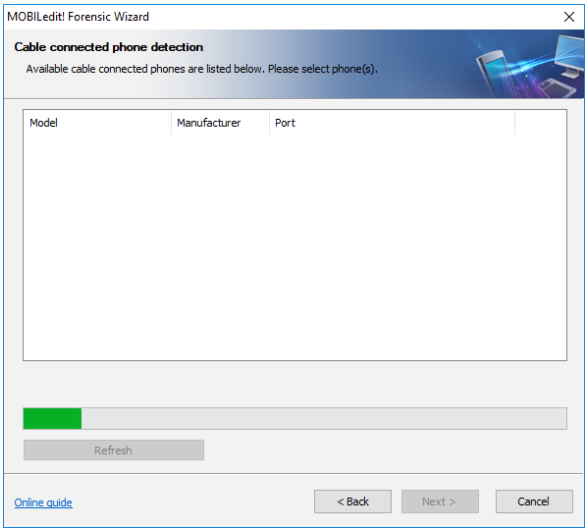
Aim :- Acquisition of Cell phones and Mobile devices .

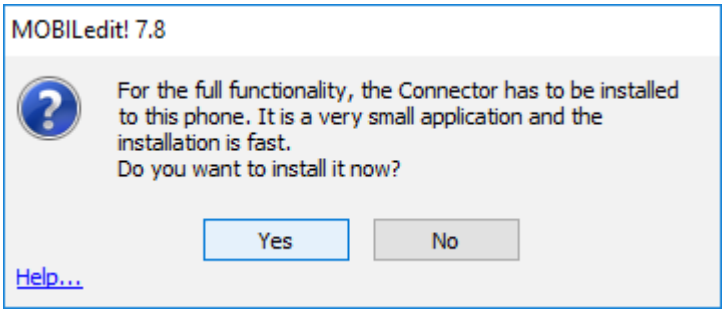


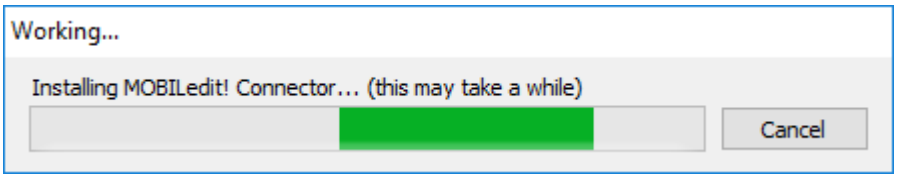


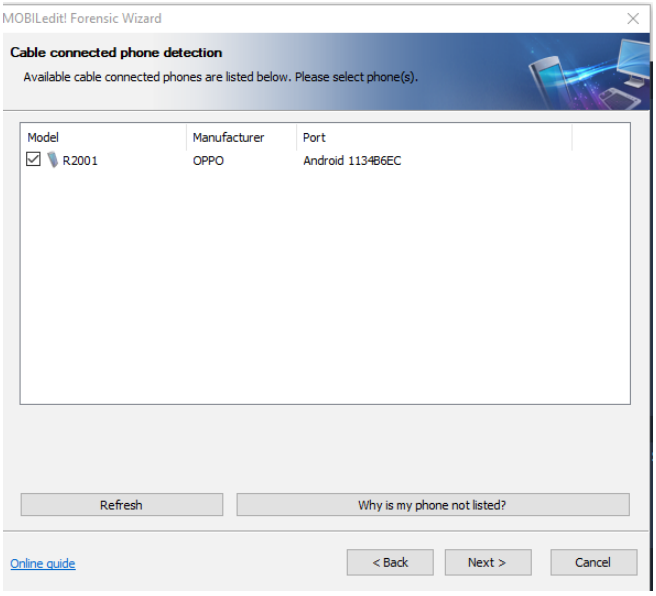

MOBILedit! Forensic Wizard
Connection Type
How is your phone connected?
Choose the type of connection:
Cable connection
Wi-Fi connection (Android, iPhone)
Bluetooth connection
Infrared connection
Tethering connection
Online guide
< Back
Next >
Cancel

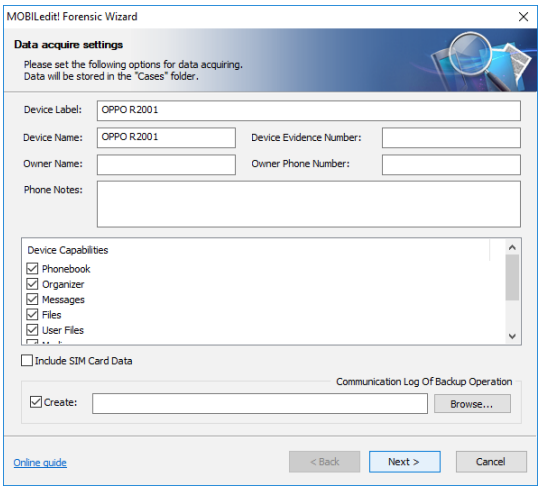

MOBILedit! Forensic Wizard
Cable connection steps
Please follow these instructions step by step!
Before connnecting the phone please:
1. Install drivers for your phone, download here
2. If connecting Android, turn on USB Debugging, read more here
3. Now connect the phone to the computer
4. If prompted,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

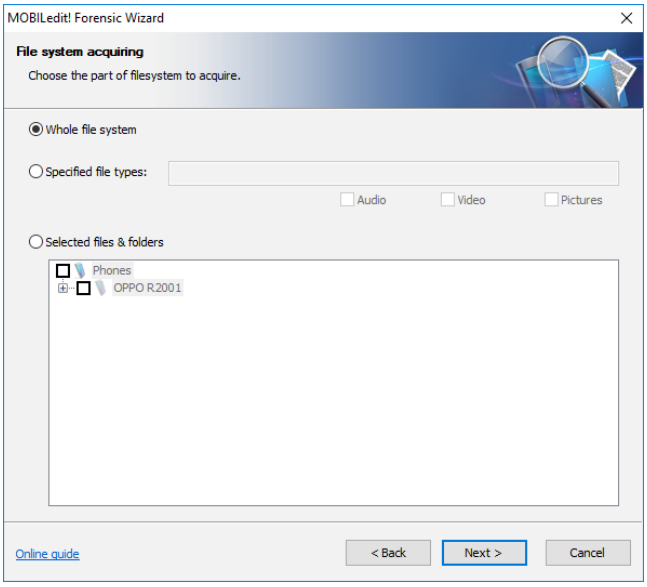

MOBILedit! Forensic Wizard
Cable connected phone detection
Available cable connected phones are listed below. Please select phone(s).
Model
Manufacturer
Port
Refresh
Online guide
< Back
Next >
Cancel

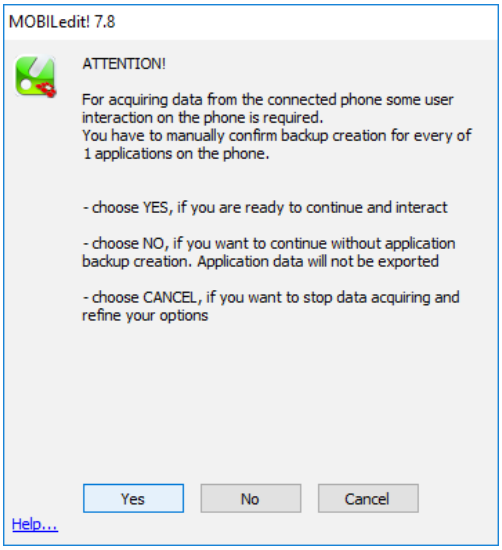

MOBILedit! 7.8
For the full functionality, the Connector has to be installed to this phone. It is a very small application and the installation is fast.
Do you want to install it now?
Yes
No
Help...

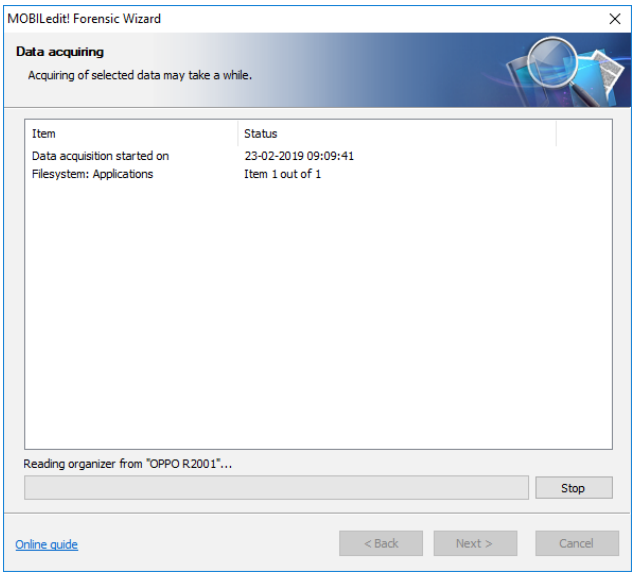

Working...
Installing MOBILedit! Connector... (this may take a while)
Cancel

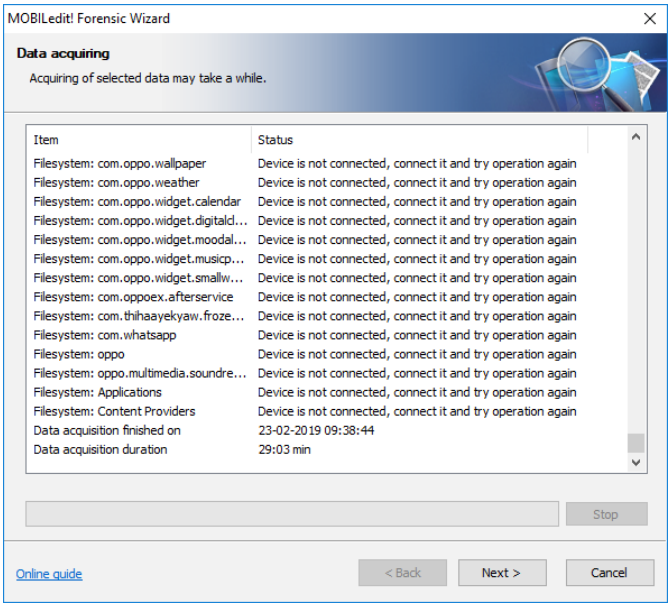

MOBILedit! Forensic Wizard
Cable connected phone detection
Available cable connected phones are listed below. Please select phone(s).
Model
Manufacturer
Port
R2001
OPPO
Android 1134B6EC
Refresh
Why is my phone not listed?
Online guide
< Back
Next >
Cancel

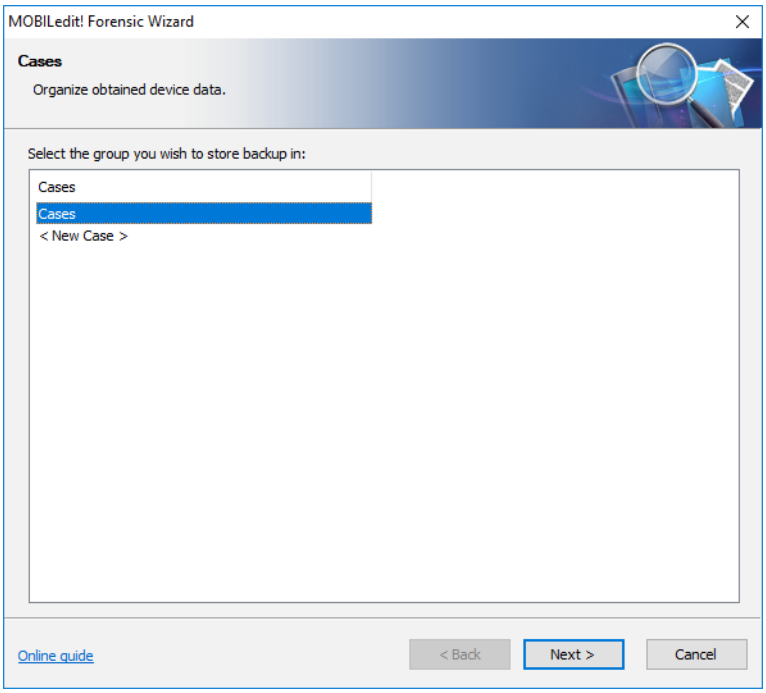

MOBILedit! Forensic Wizard
Data acquire settings
Please set the following options for data acquiring.
Data will be stored in the "Cases" folder.
Device Label:
OPPO R2001
Device Name:
OPPO R2001
Device Evidence Number:
Owner Name:
Owner Phone Number:
Phone Notes:
Device Capabilities
Phonebook
Organizer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

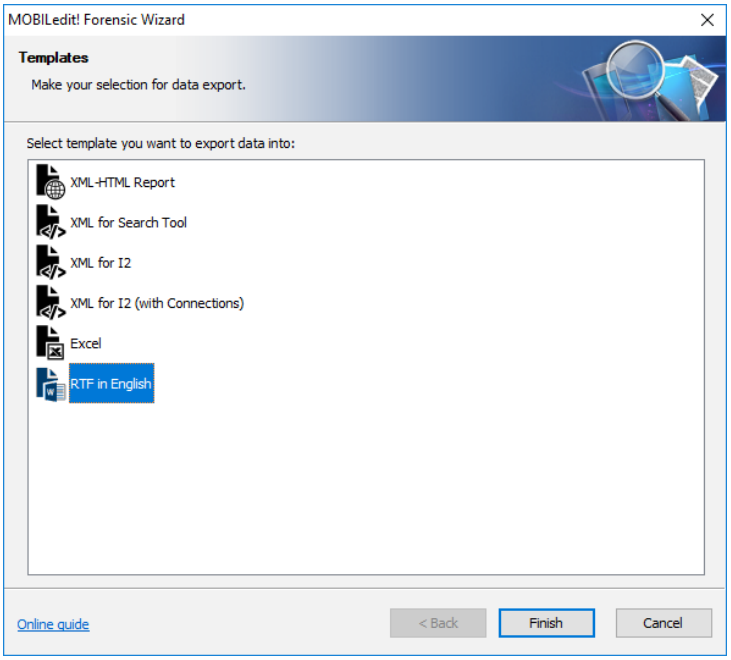

MOBILedit! Forensic Wizard
File system acquiring
Choose the part of filesystem to acquire.
Whole file system
Specified file types:
Audio
Video
Pictures
Selected files & folders
Phones
OPPO R2001
Online guide
< Back
Next >
Cancel

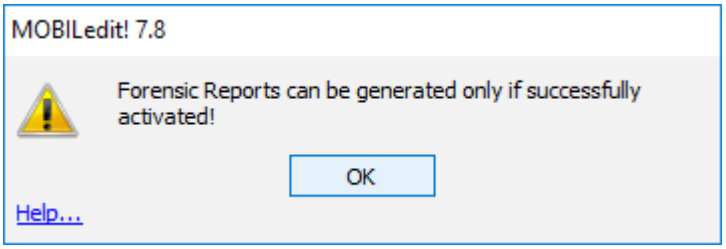

MOBILedit! 7.8
ATTENTION!
For acquiring data from the connected phone some user interaction on the phone is required.
You have to manually confirm backup creation for every of 1 applications on the phone.
- choose YES, if you are ready to continue and interact
- choose NO, if you want to continue without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

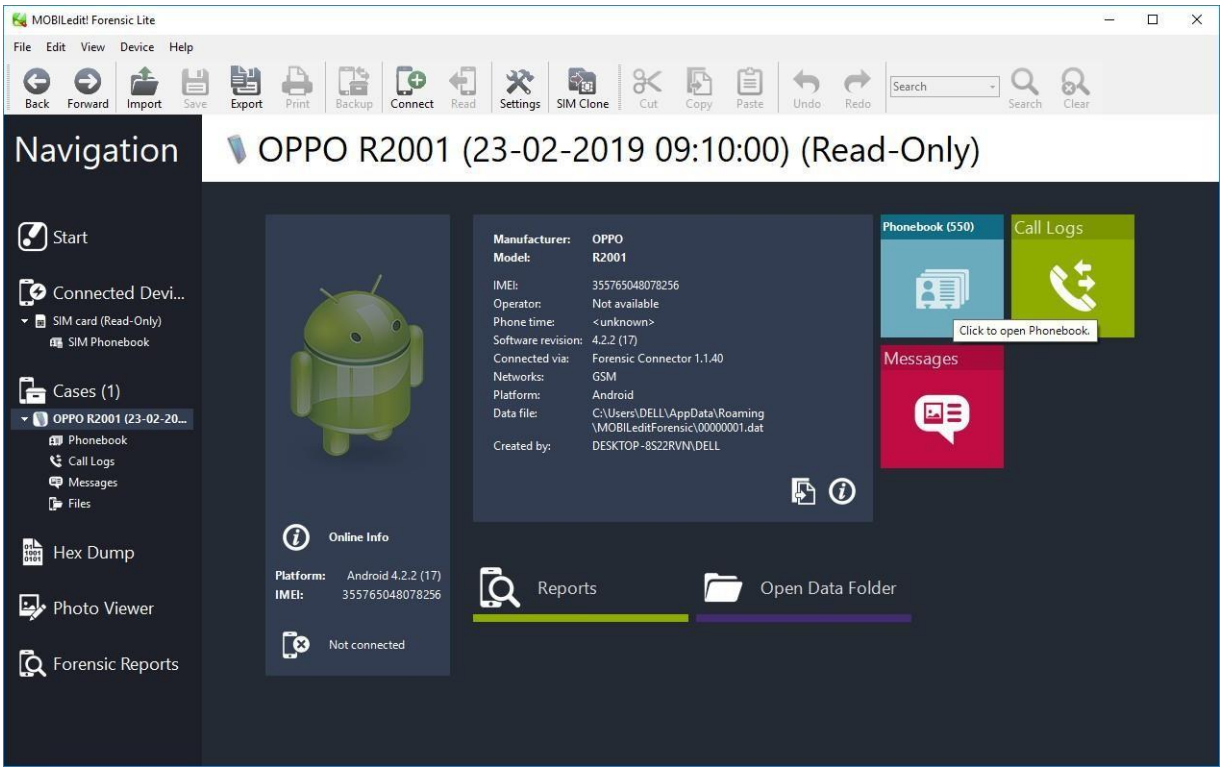

MOBILedit! Forensic Wizard
Data acquiring
Acquiring of selected data may take a while.
Item
Status
Data acquisition started on
23-02-2019 09:09:41
Filesystem: Applications
Item 1 out of 1
Reading organizer from "OPPO R2001"...
Stop
Online guide
< Back
Next >
Cancel

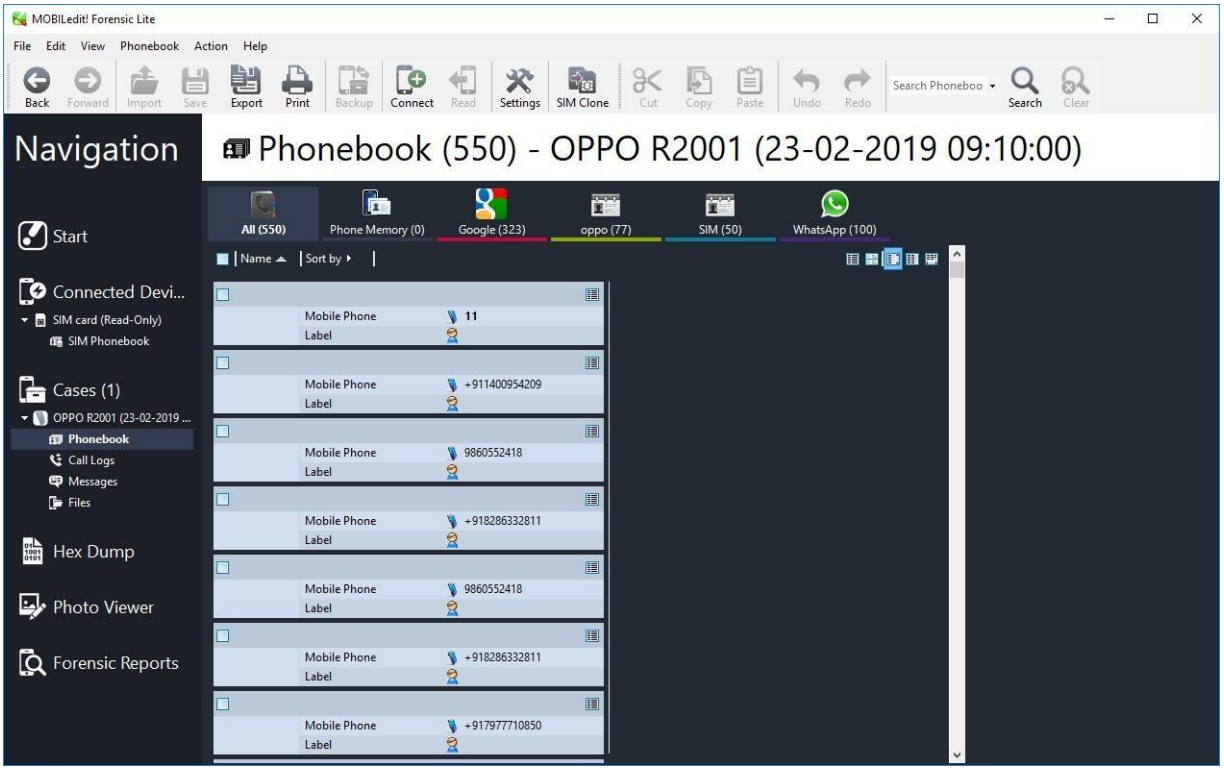

MOBILedit! Forensic Wizard
Data acquiring
Acquiring of selected data may take a while.
Item
Status
Filesystem: com.oppo.wallpaper
Device is not connected, connect it and try operation again
Filesystem: com.oppo.weather
Device is not connected, connect it and try operation again
Filesystem: com.oppo.widget.calendar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

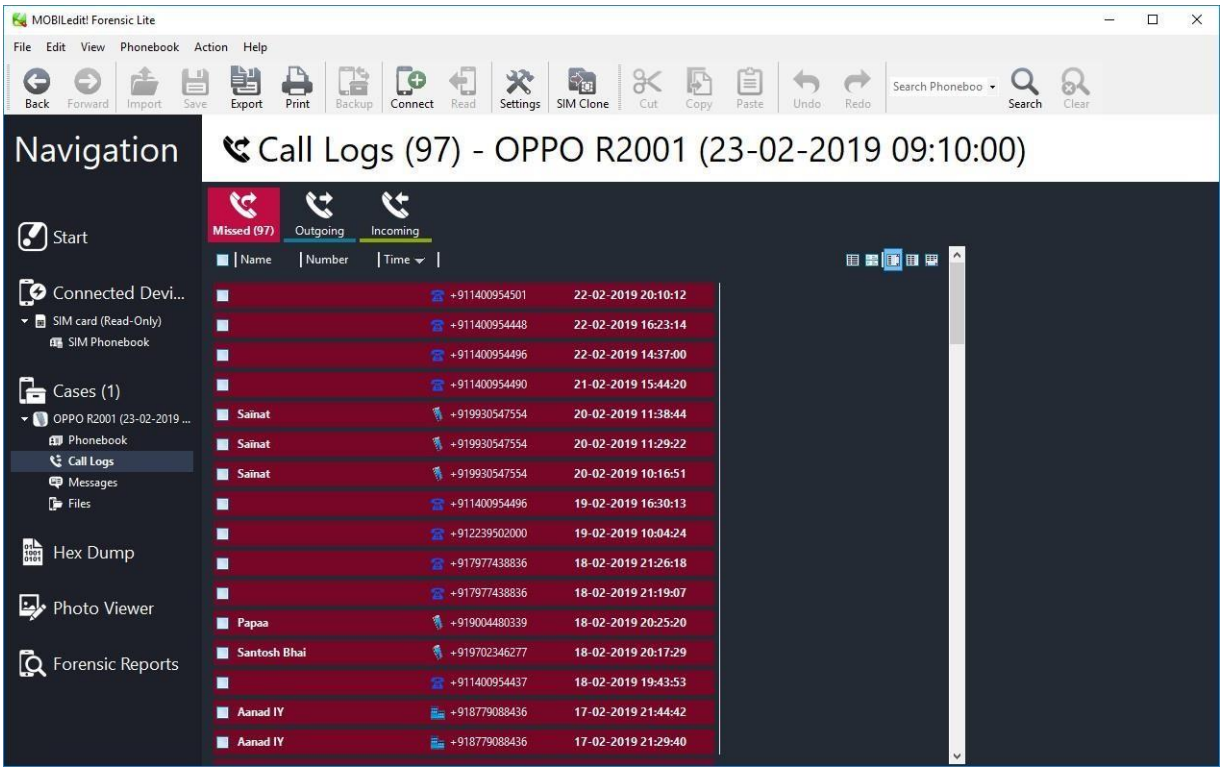

MOBILedit! Forensic Wizard
Cases
Organize obtained device data.
Select the group you wish to store backup in:
Cases
Cases
< New Case >
Online guide
< Back
Next >
Cancel

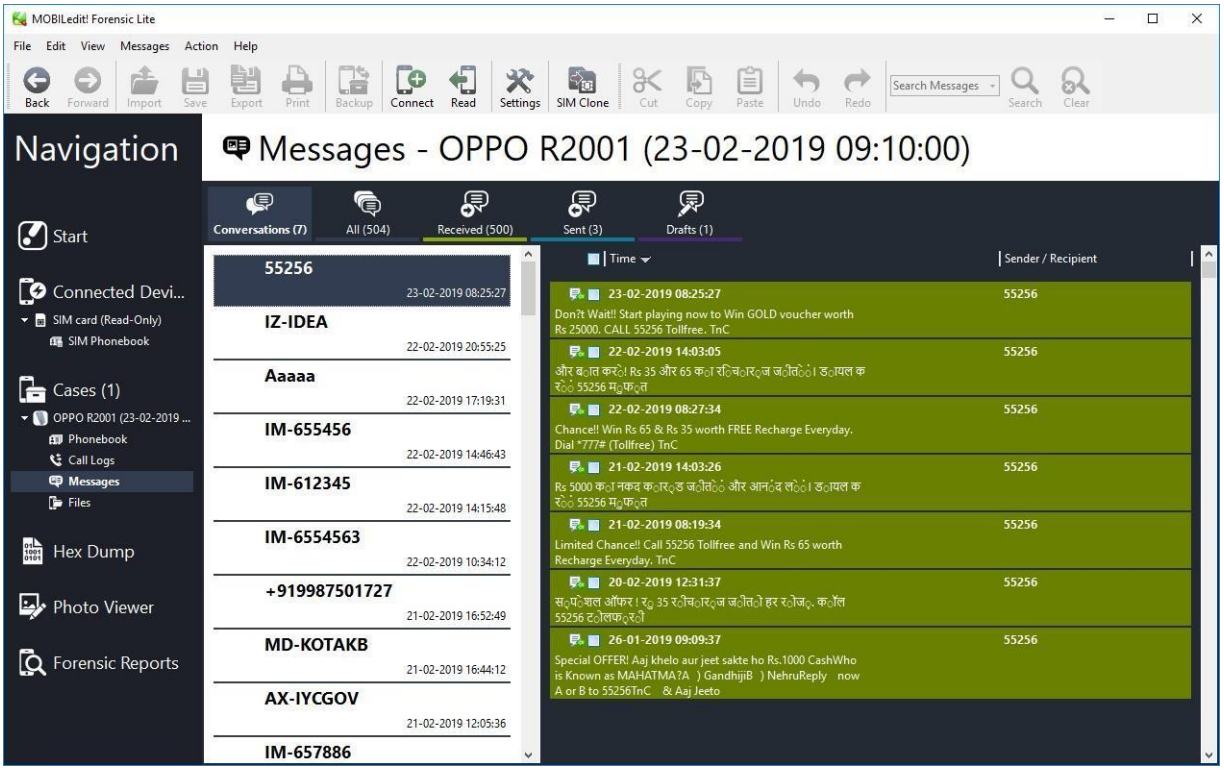

MOBILedit! Forensic Wizard
Templates
Make your selection for data export.
Select template you want to export data into:
XML-HTML Report
XML for Search Tool
XML for I2
XML for I2 (with Connections)
Excel
RTF in English
Online guide
< Back
Finish
Cancel


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


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


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


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


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

PRACTICAL 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.

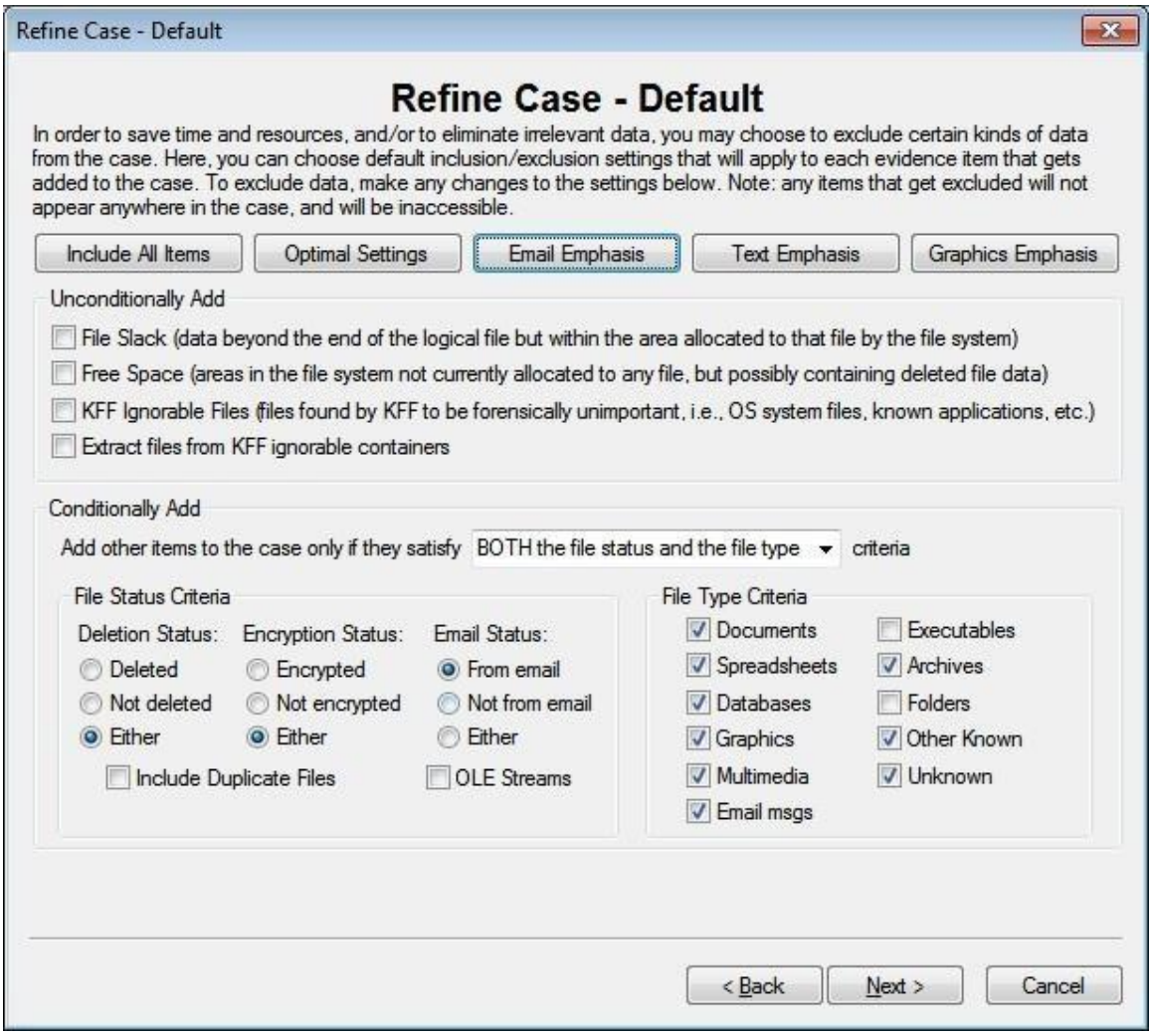
Martha asked her CIO, to have an IT employee copy the Outlook .pst file from

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.

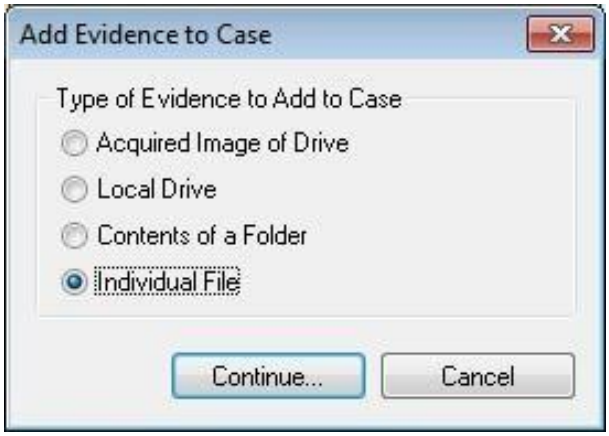
Recovering Email

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

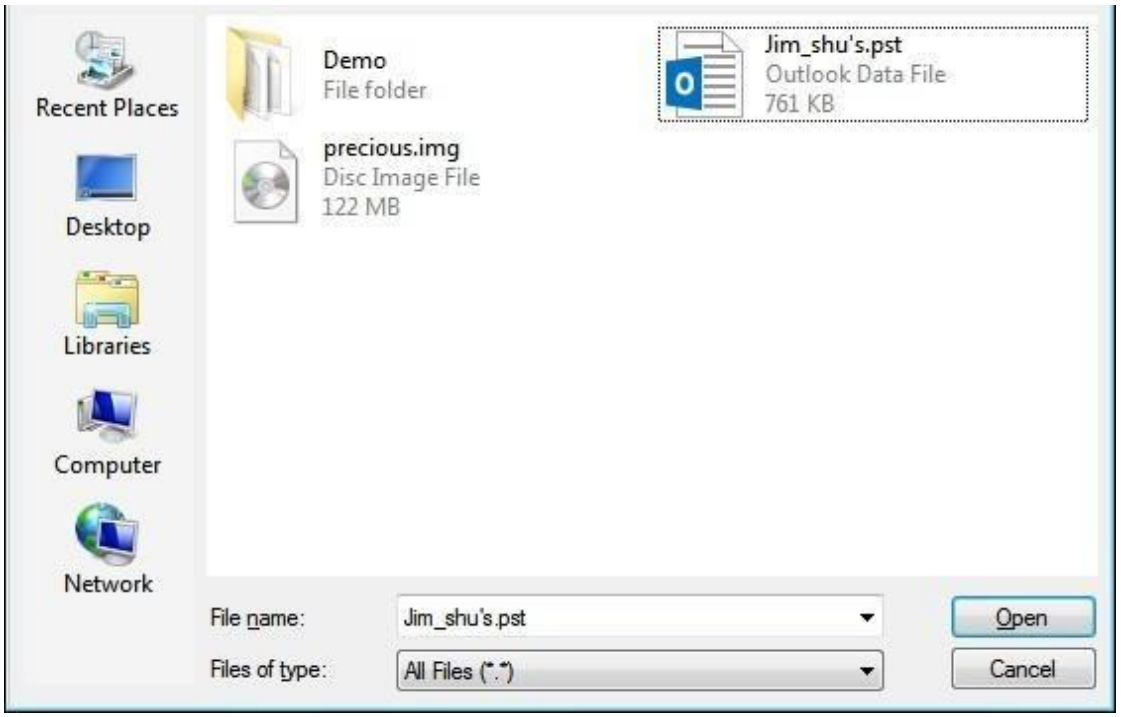


Click **Next** until you reach the **Add Evidence to Case** dialog box, and then click the **Add Evidence** button.

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

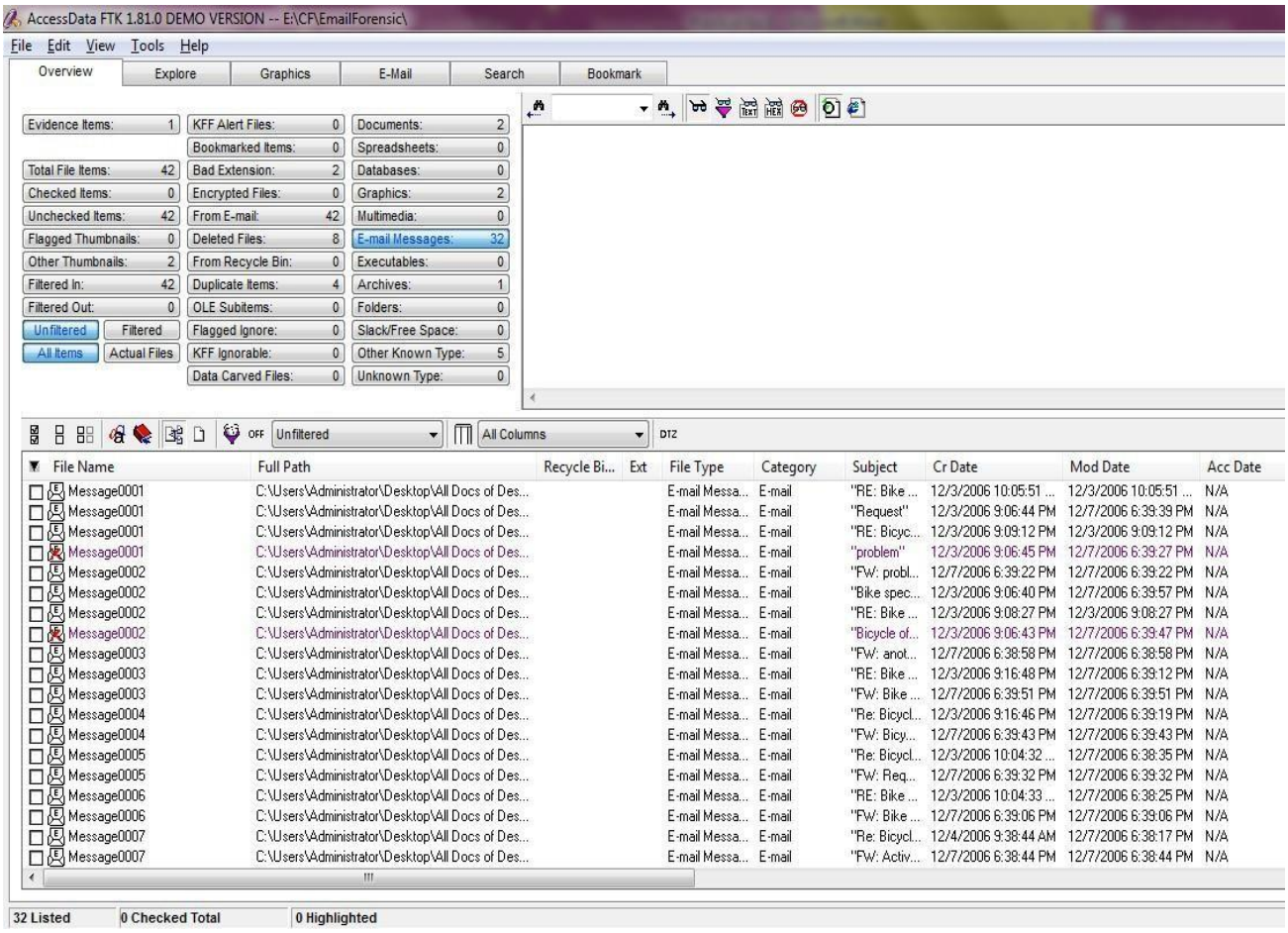


In the **Select File** dialog box, navigate to your work folder, click the **Jim_shu's.pst file**, and then click **Open**.



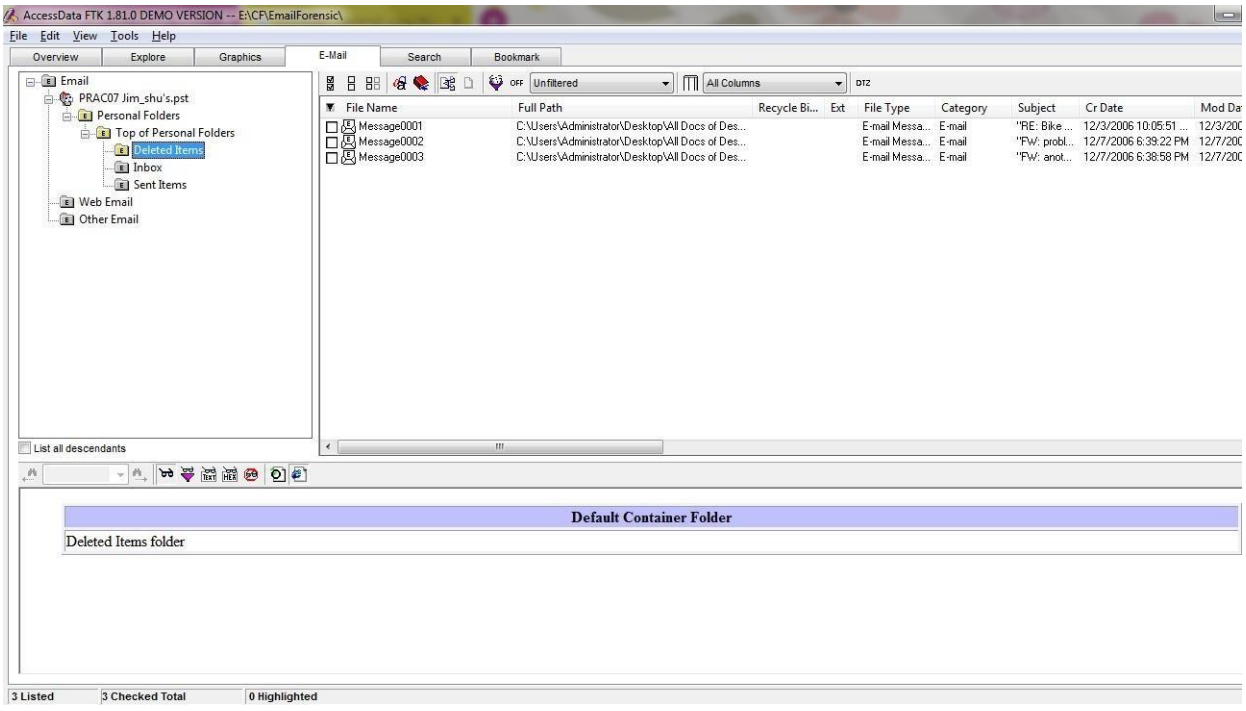
When the **Add Evidence to Case** dialog box opens, click **Next**. In the **Case summary** dialog box, click **Finish**.

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



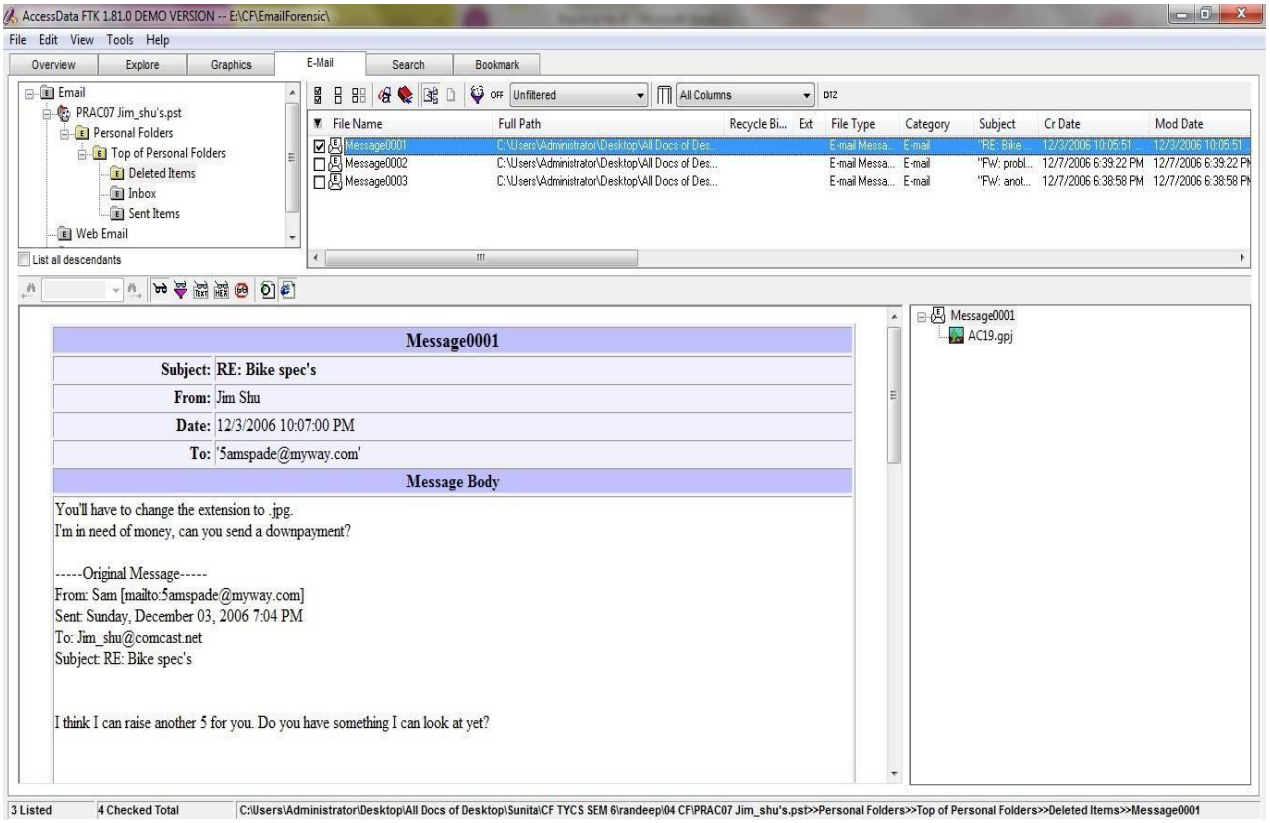
For email recovery follow following steps:

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



Select any message say Message0001 right click and select option Launch.

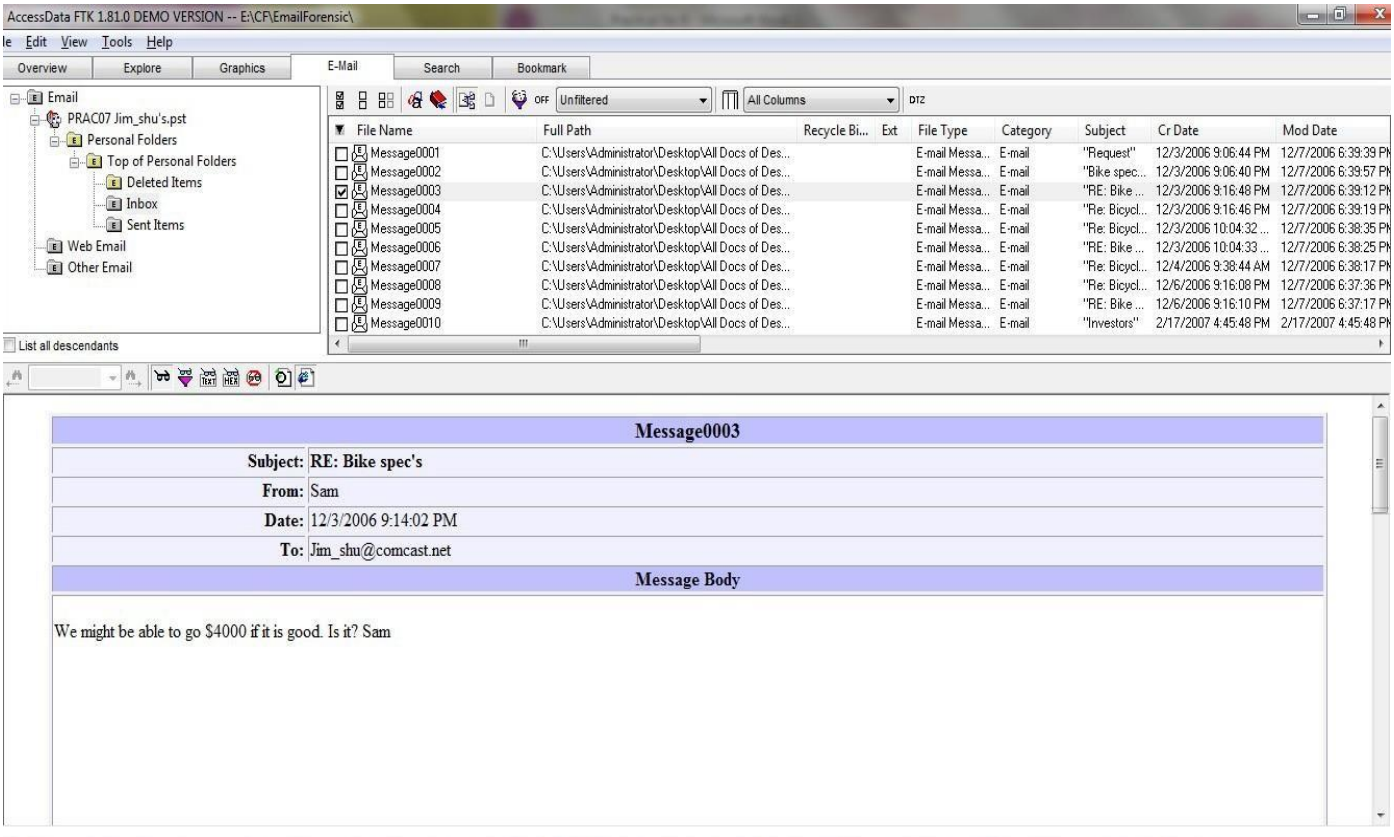
Detached Viewer and you can see detail of deleted message.



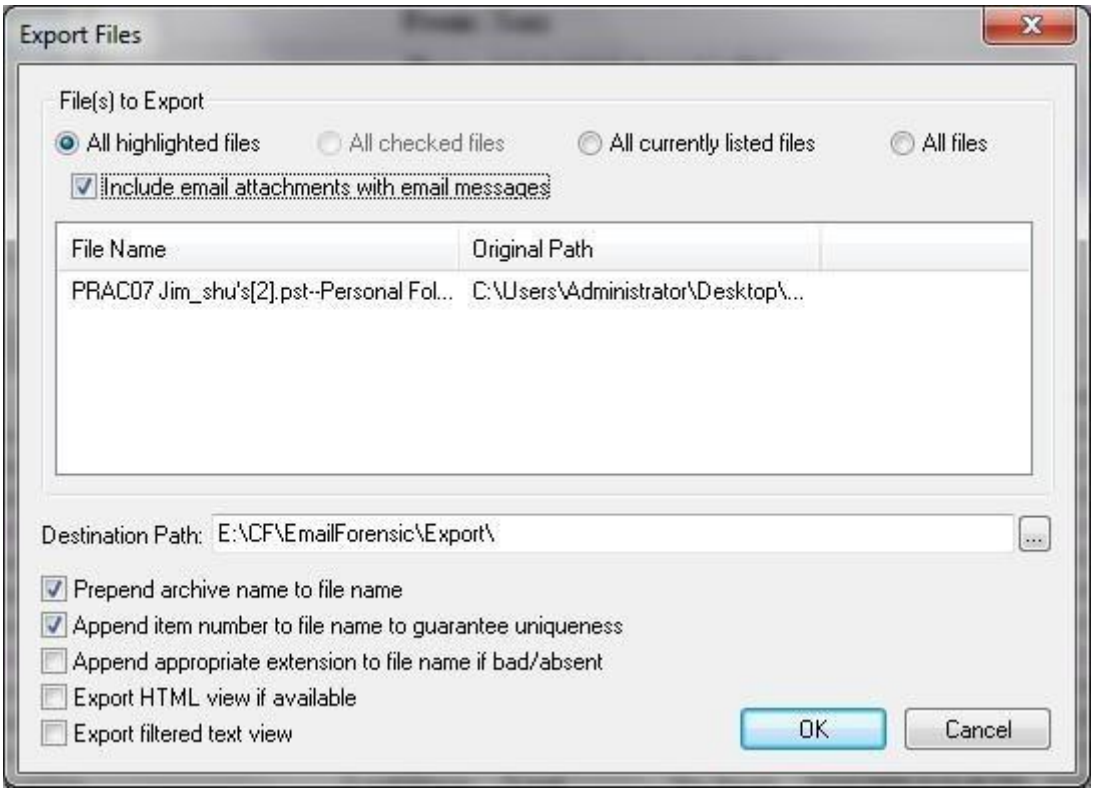
For analyzing header follow following steps:

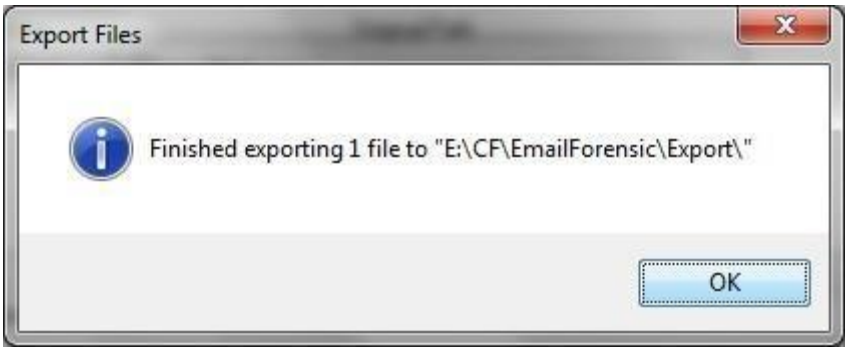
Click the **E-Mail** tab. In the tree view, click to expand all folders, and then click the **Inbox** folder.

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

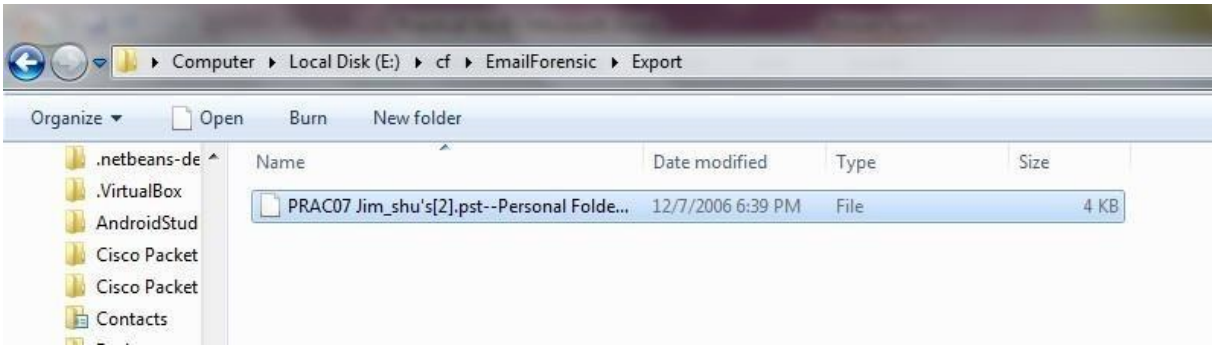


Right-click on any message say Message0003 in the File List pane and click Export File. In the Export Files dialog box, click OK.

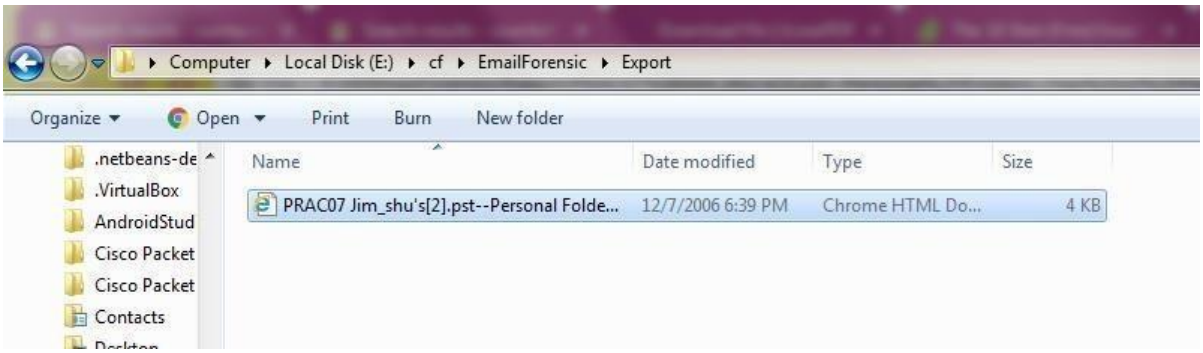




FTK saves exported files in the HTML format with no extension.



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



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

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 mprdmxin.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 [24.18.24.230] by mprdmailfe3.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: 5amspade@myway.com From: "Sam"<5amspade@myway.com> MIME-Version: 1.0 X-Sender: 5amspade@myway.com X-Mailer: PHP Content-Type: text/plain; charset="US-ASCII" Content-Transfer-Encoding: 7bit Message-Id: <20061204021414.63B6067669@mprdmxin.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: 5amspade@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:5amspade@myway.com] Sent: Sunday, December 03, 2006 5:40 PMTo: jim_shu@comcast.netSubject: Bike spec'sDo 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

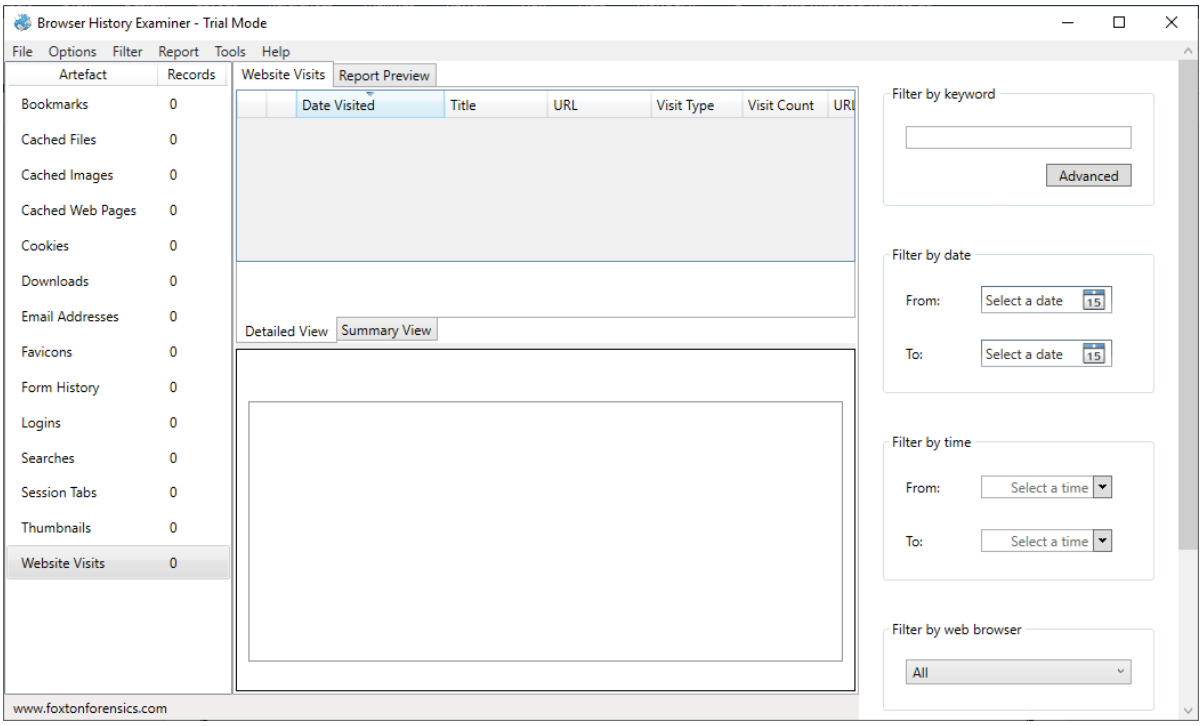
-Forensics activities on browser

-Cache / Cookies analysis

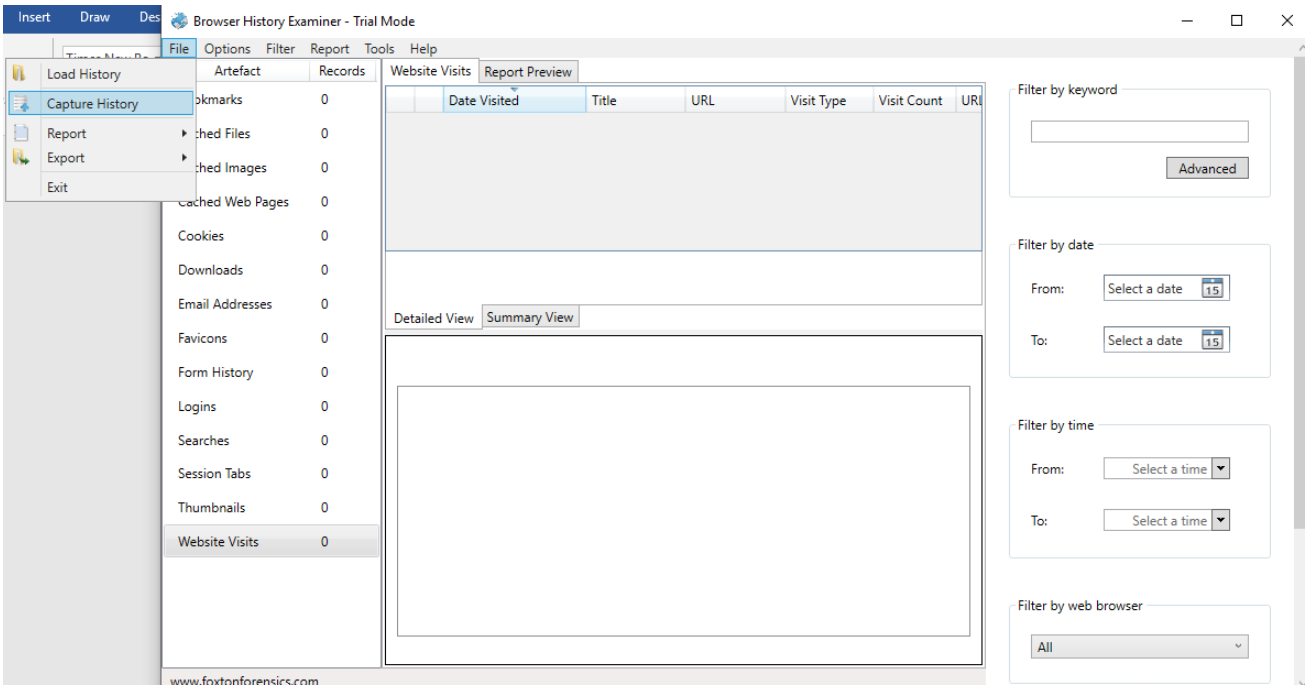
-Last Internet activity

Steps:

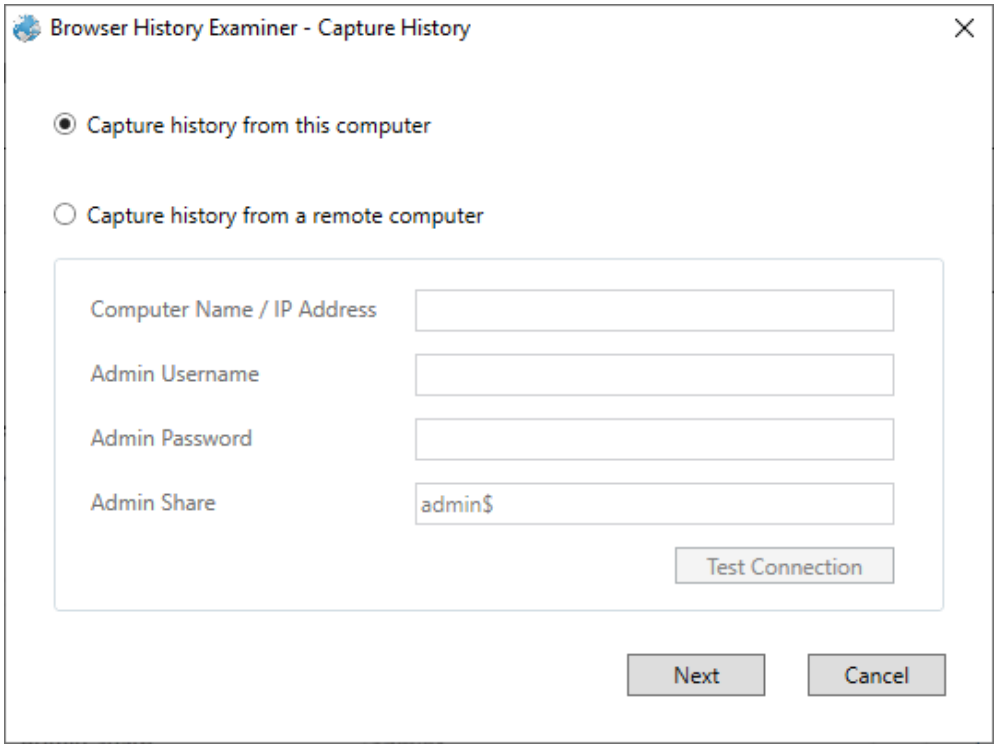
1. Open BrowserHistoryExaminer.



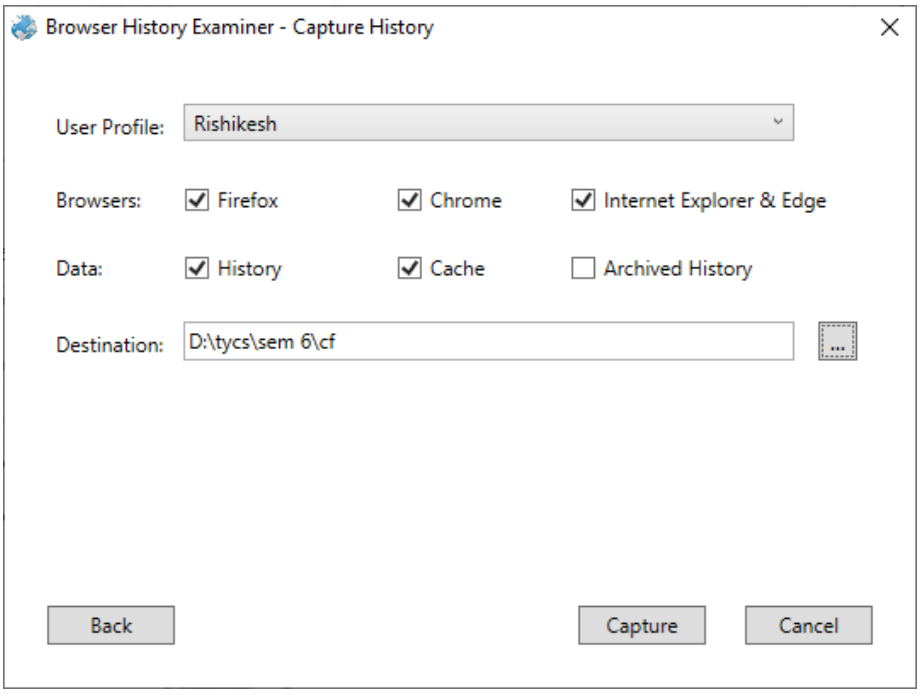
2. Click on file > Capture History



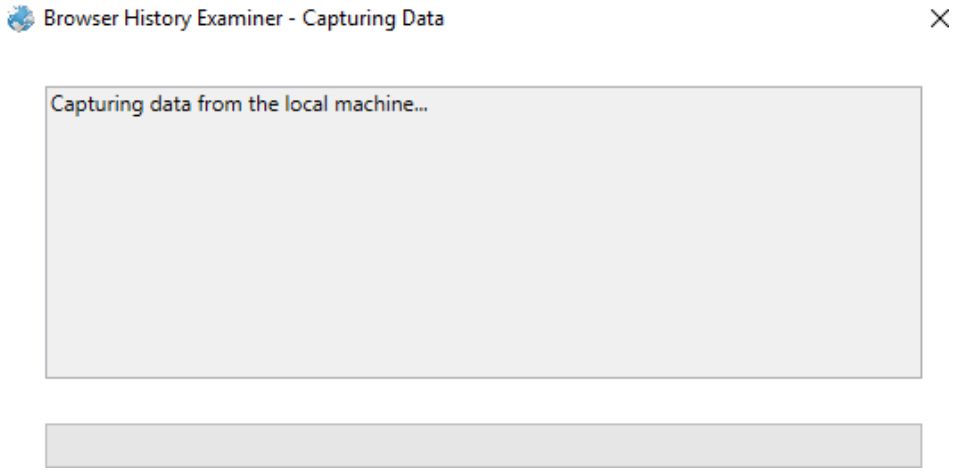
3. Select the capture folder and click on next.

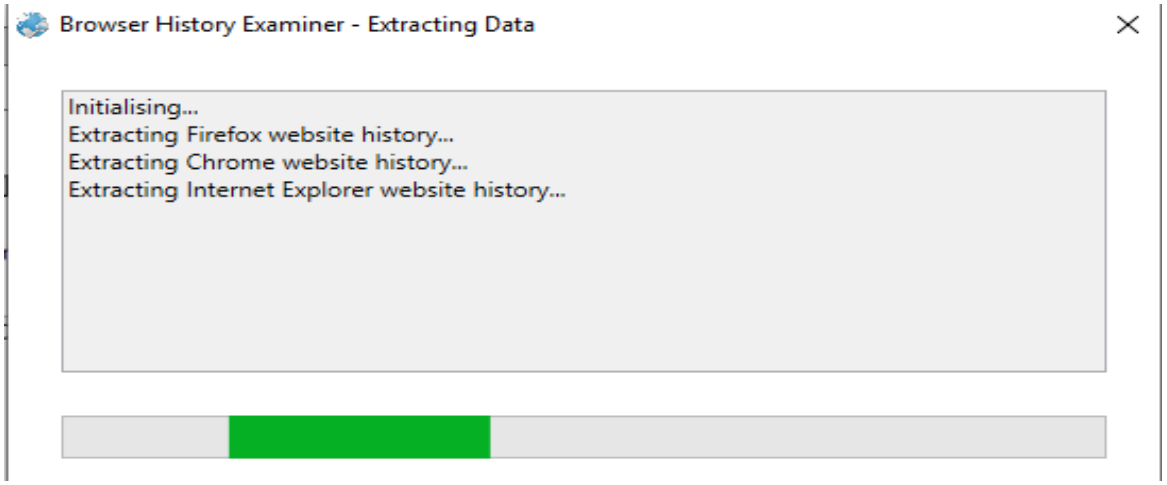


4. Enter the destination to capture the data.

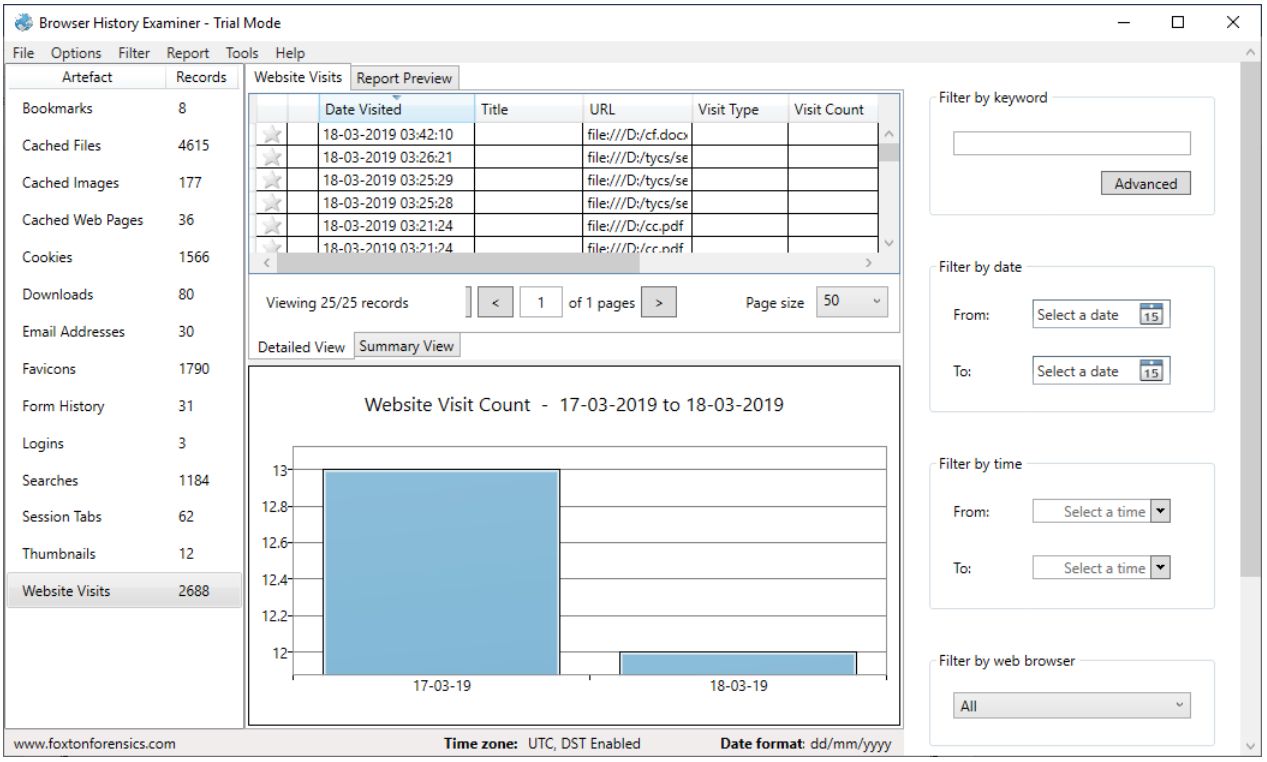


5. The History is been extracting.

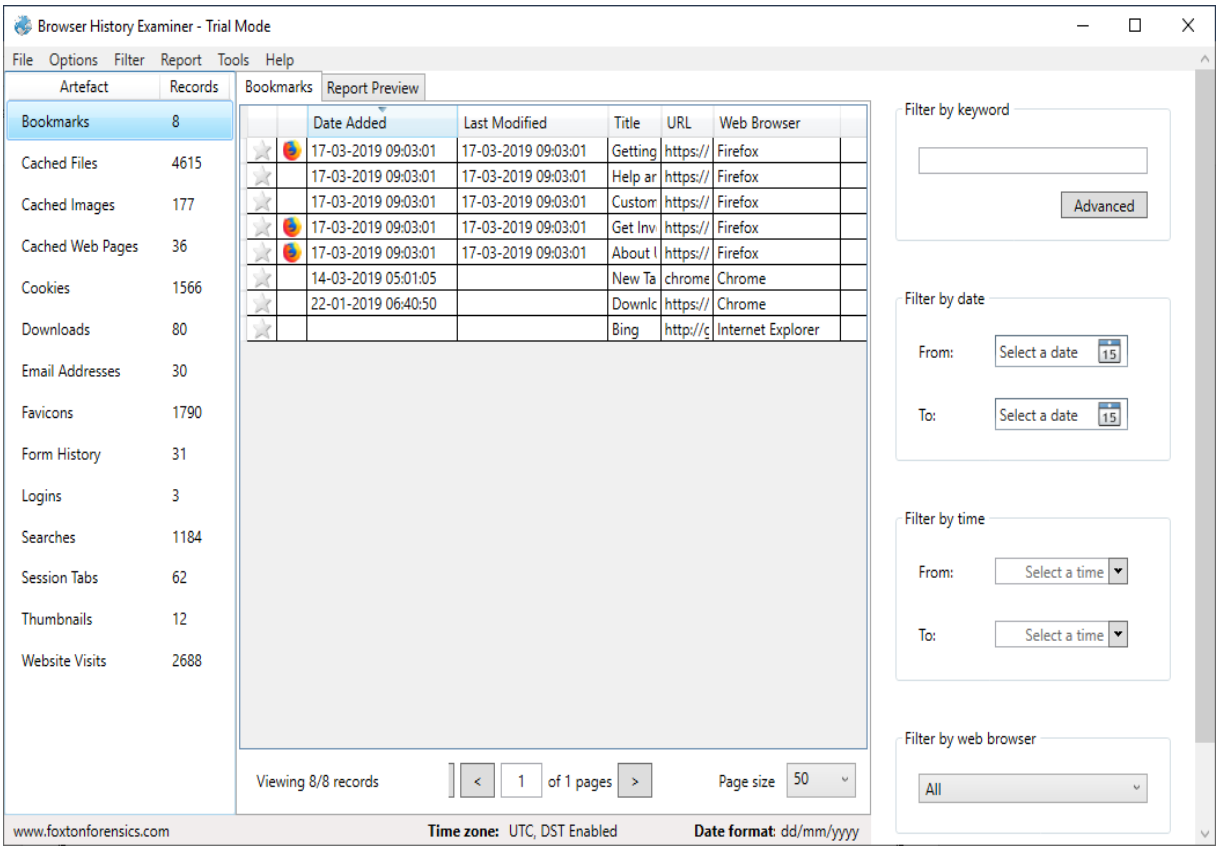




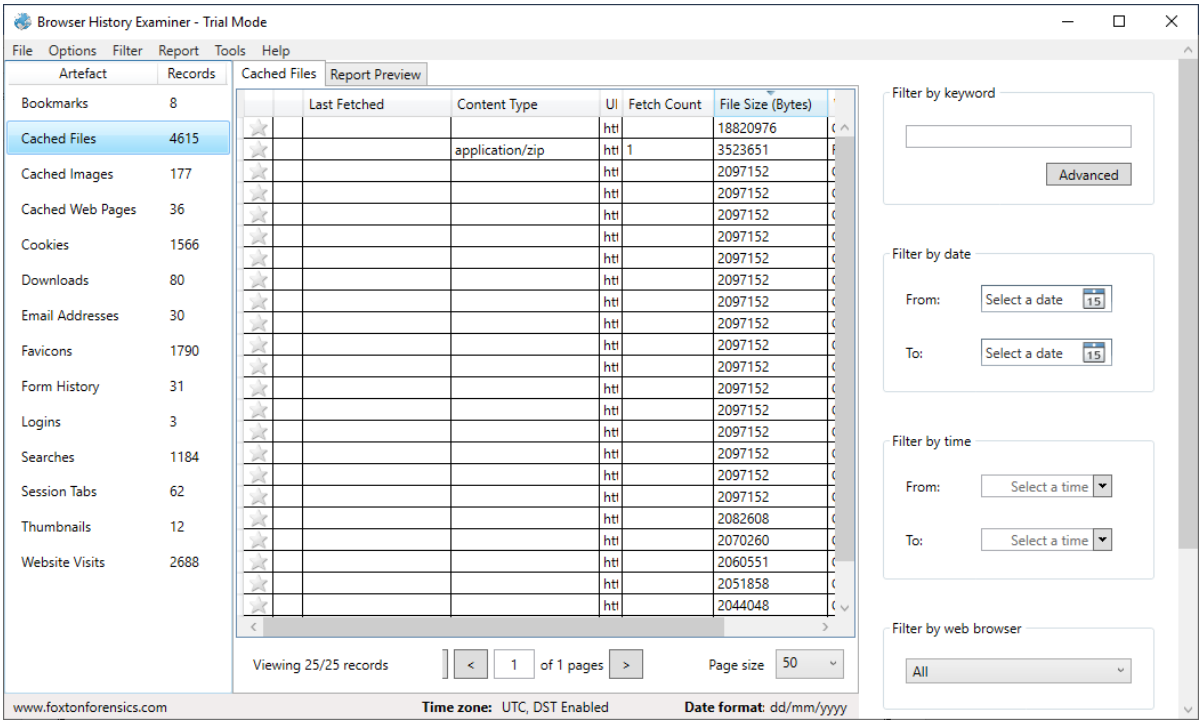
6. The data has been retrieved.



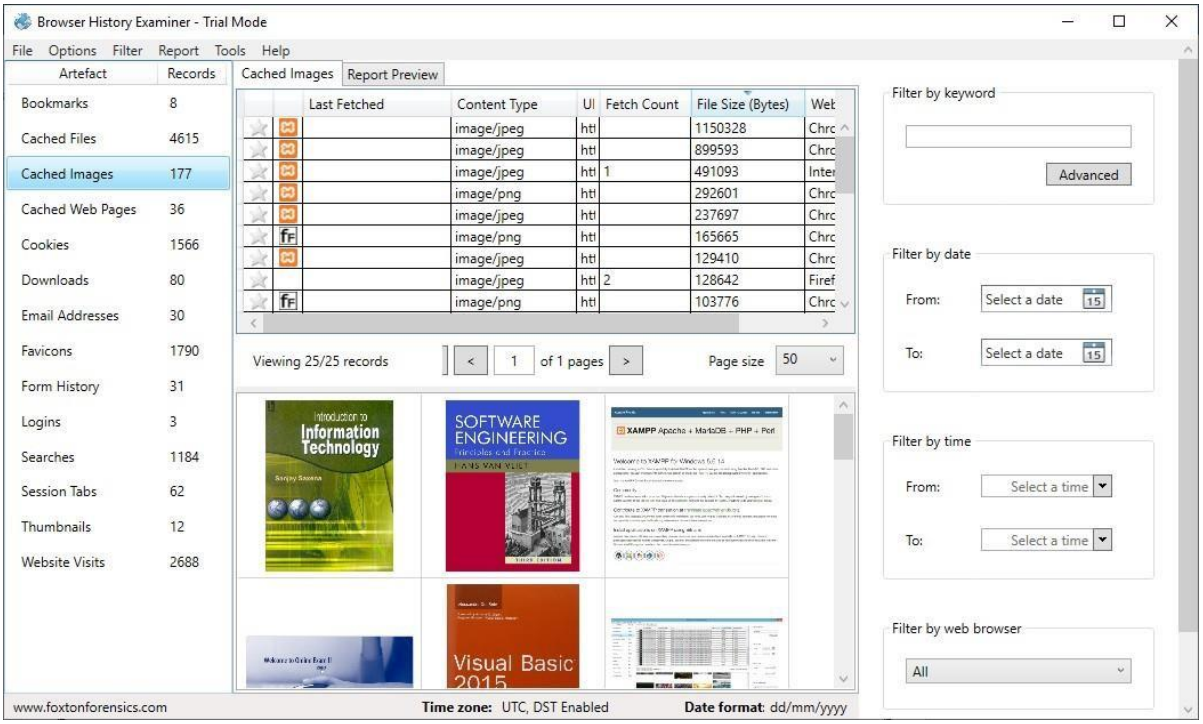
7. On the left panel click on bookmarks.



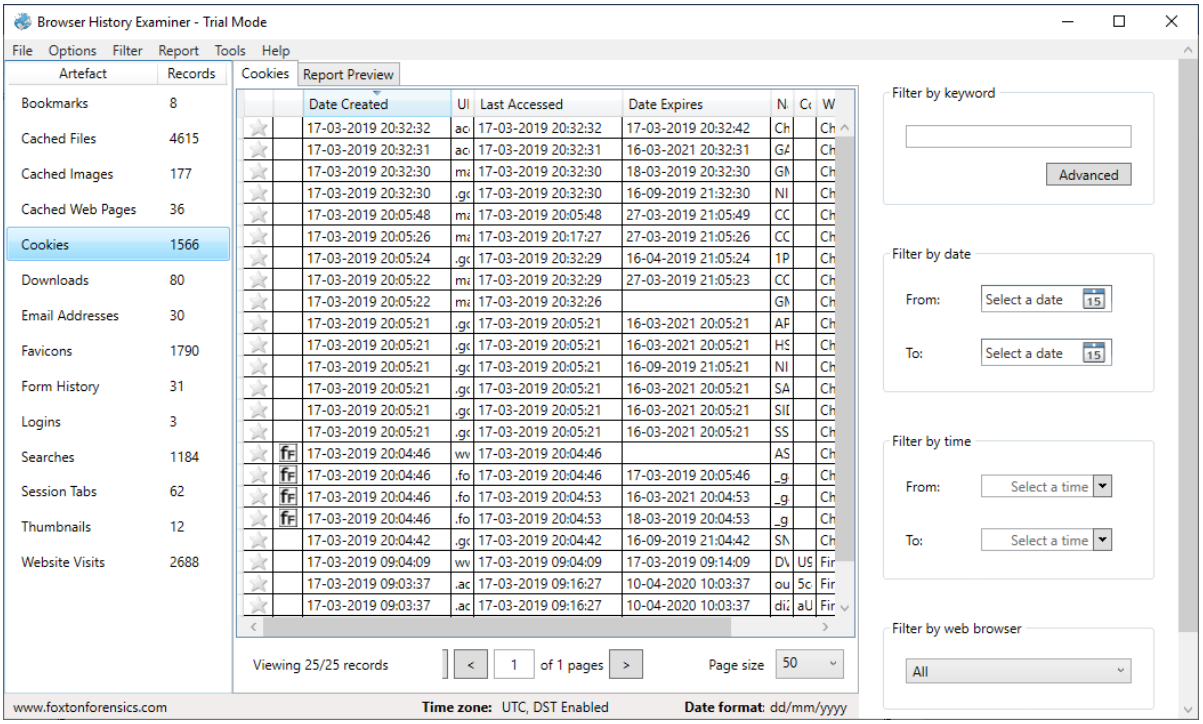
8. On the left panel click on cached files.



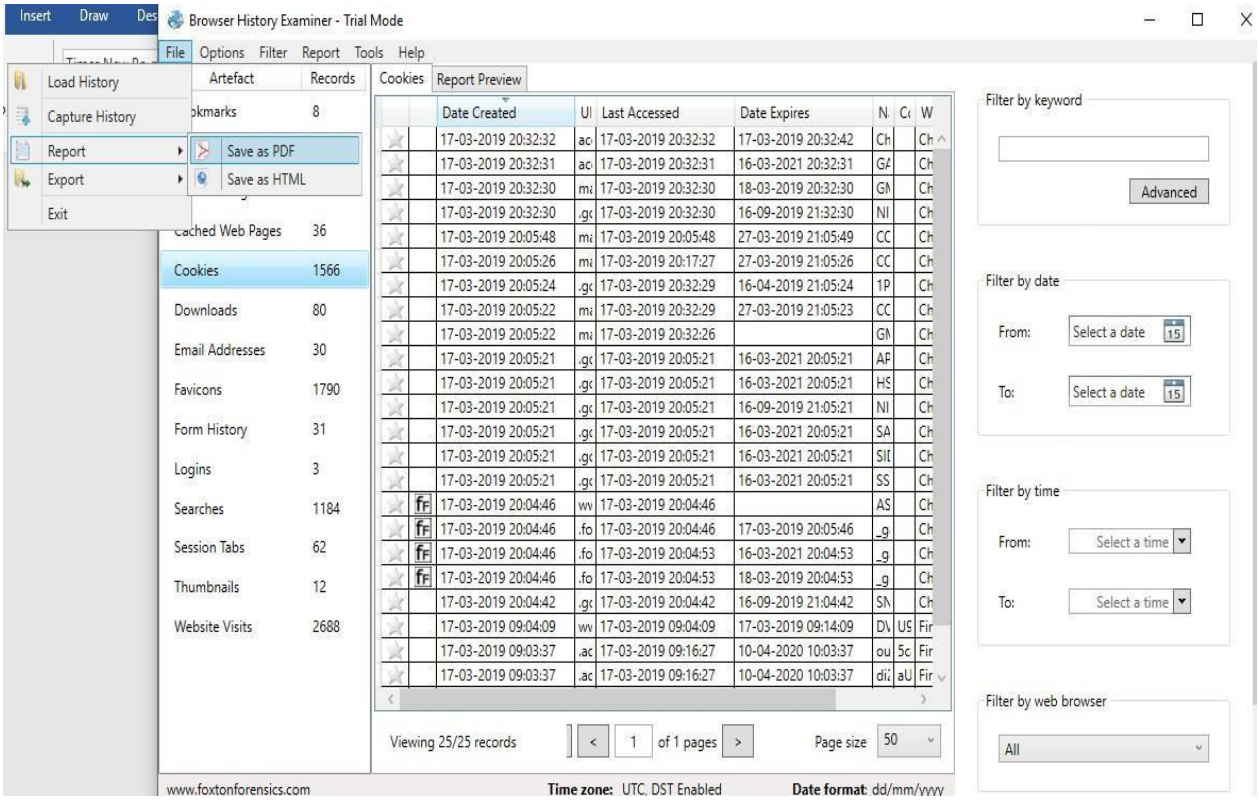
9. On the left panel click on cached images.

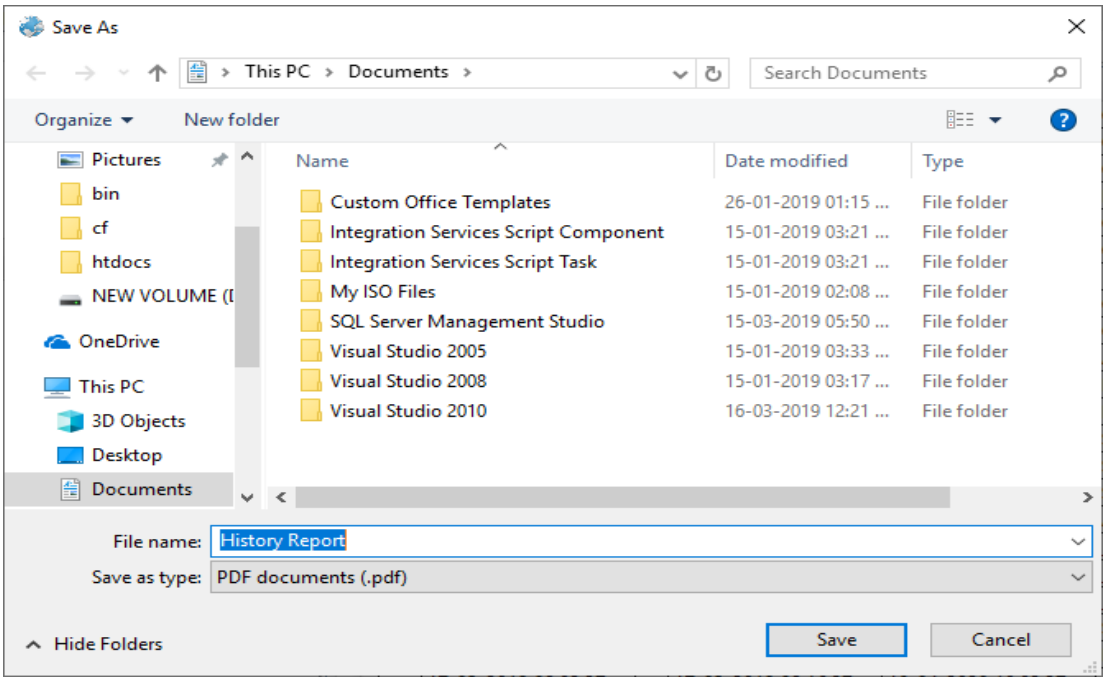


10. On the left panel click on cookies.



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





Web Browser History Report

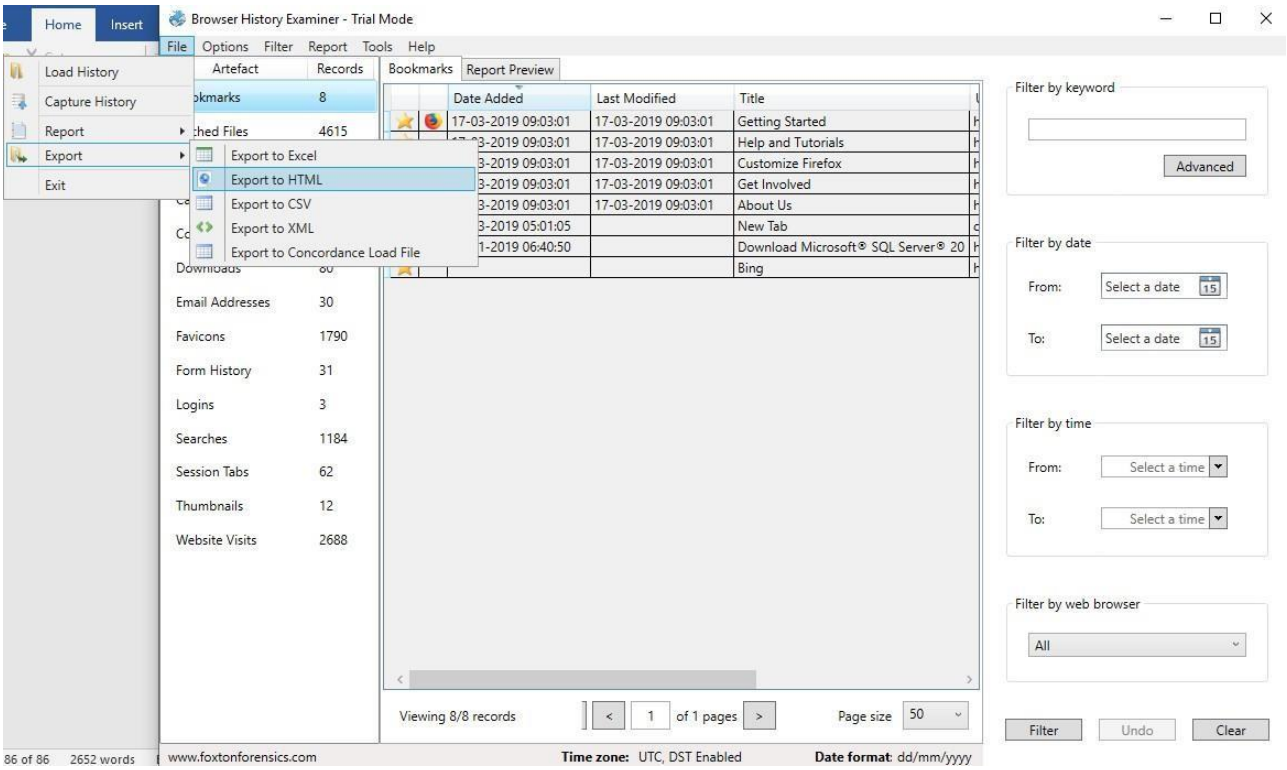
Created: 18-03-2019 09:36
Created using: Browser History Examiner v1.9
Time zone: UTC, DST Enabled
Date format: dd/mm/yyyy

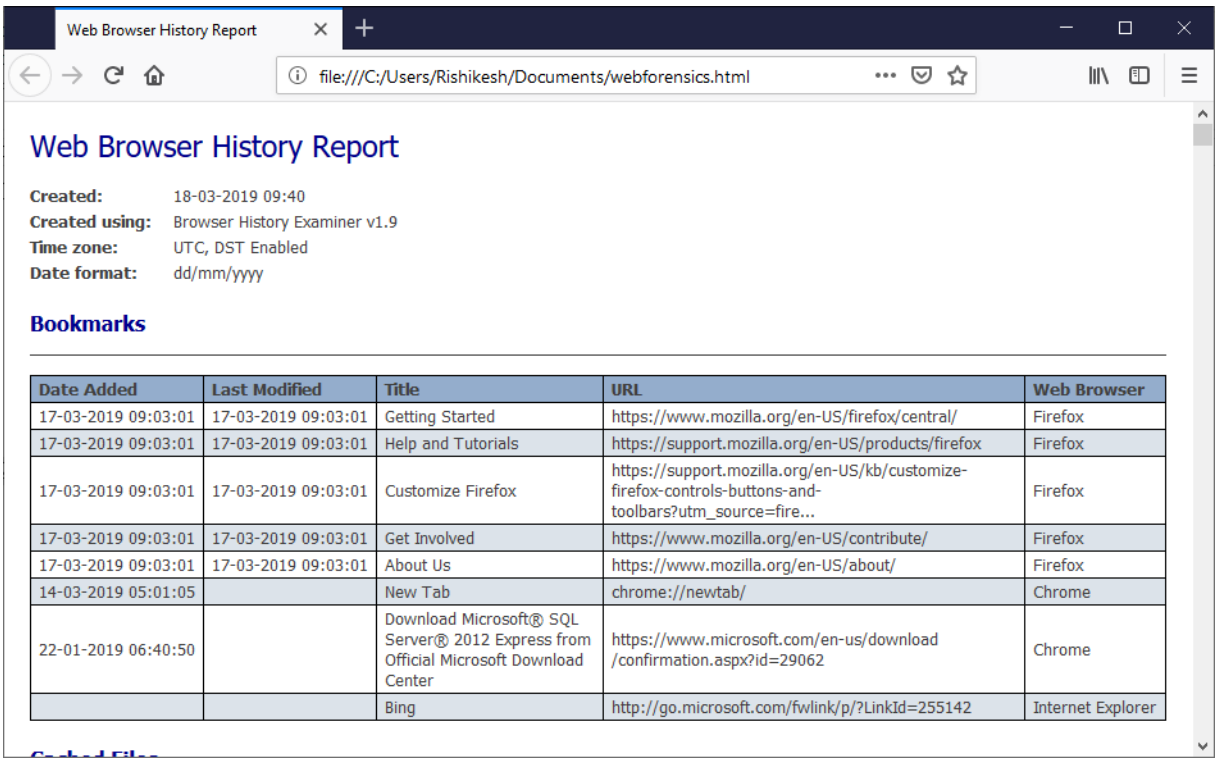
Bookmarks

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

Cached Files

Last Fetched	Content Type	URL	Fetch Count	File Size (Bytes)	Web Browser
		https://mail-attachment.googleusercontent.com/attachment/u/0/?ui=2&ik=5c151dfa36&attid=0.1&a...		18820976	Chrome
	application/zip	https://r4---sn-4p8xoxu-cvhe.gvt1.com/edgedl/widevine-cdm/4.10.1146.0-win-x64.zip?cms_redirect=yes&a...	1	3523651	Firefox
		https://r3---sn-4p8xoxu-cvhe.googlevideo.com/videoplayback?ei=uYyLXNeQA4ei1Ab4h7K4Cg&dur=152.733...		2097152	Chrome
		https://r3---sn-4p8xoxu-cvhe.googlevideo.com/videoplayback?ei=uYyLXNeQA4ei1Ab4h7K4Cg&dur=152.733...		2097152	Chrome
		https://r3---sn-4p8xoxu-cvhe.googlevideo.com/videoplayback?ei=uYyLXNeQA4ei1Ab4h7K4Cg&dur=152.733...		2097152	Chrome





Web Browser History Report

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

Bookmarks

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