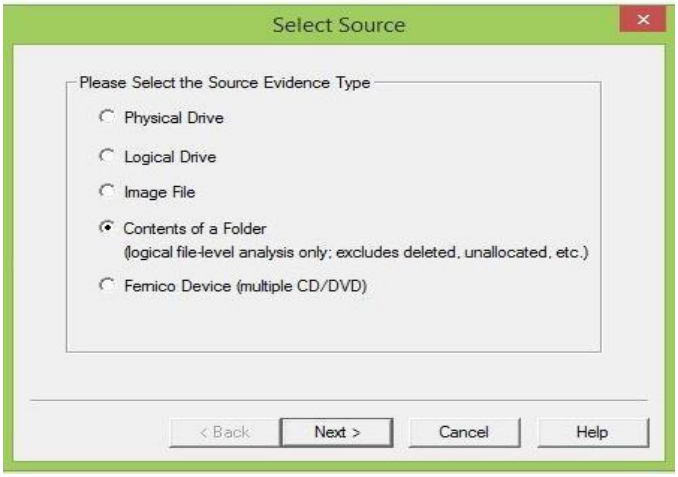
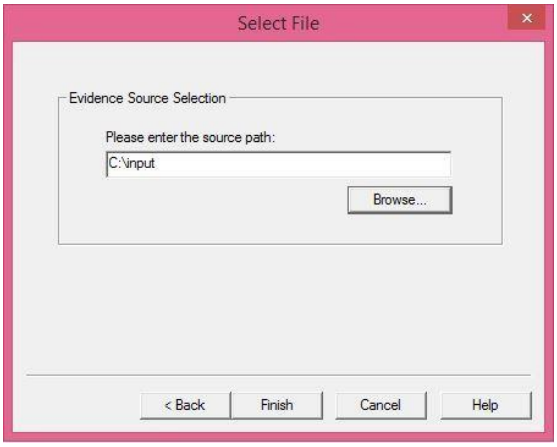
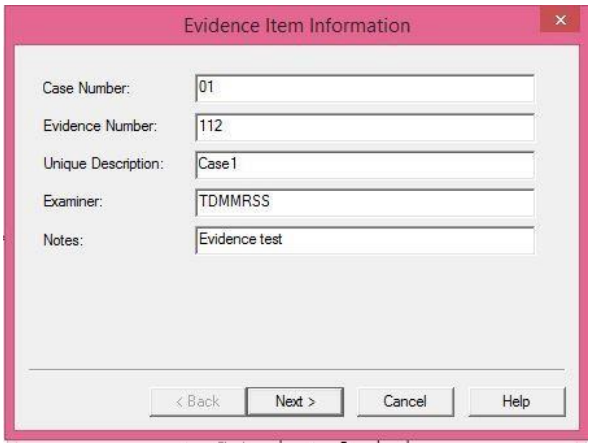
Practical No:1

Open →AccessData FTK Imager→File→create disk image→contents of a folder

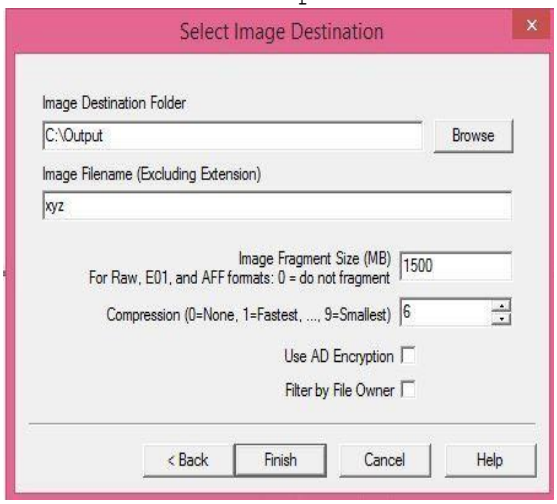


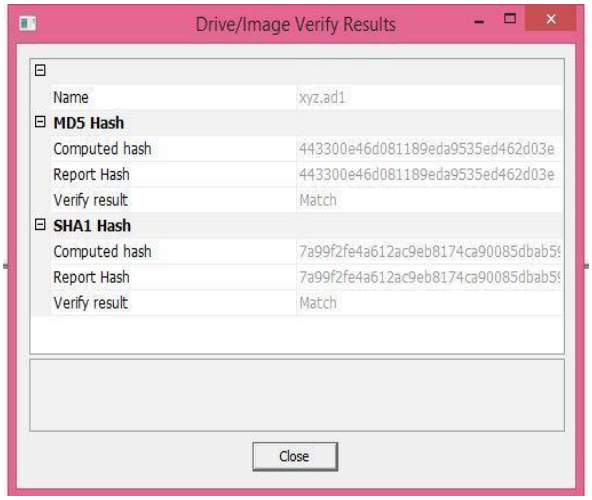
Create a file in C Drive name input →create a doc file ii2→ Browse the File → Finish



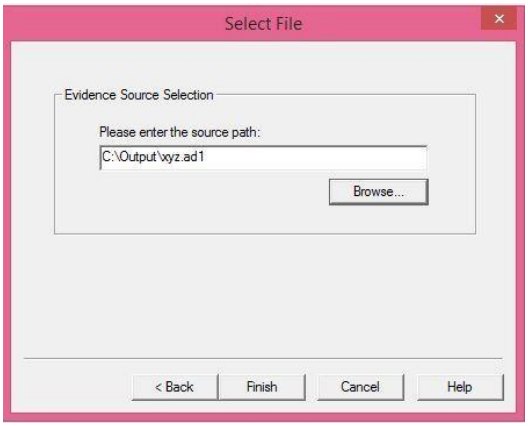


Create folder output2 in D drive→Select this as Destination→ Finish

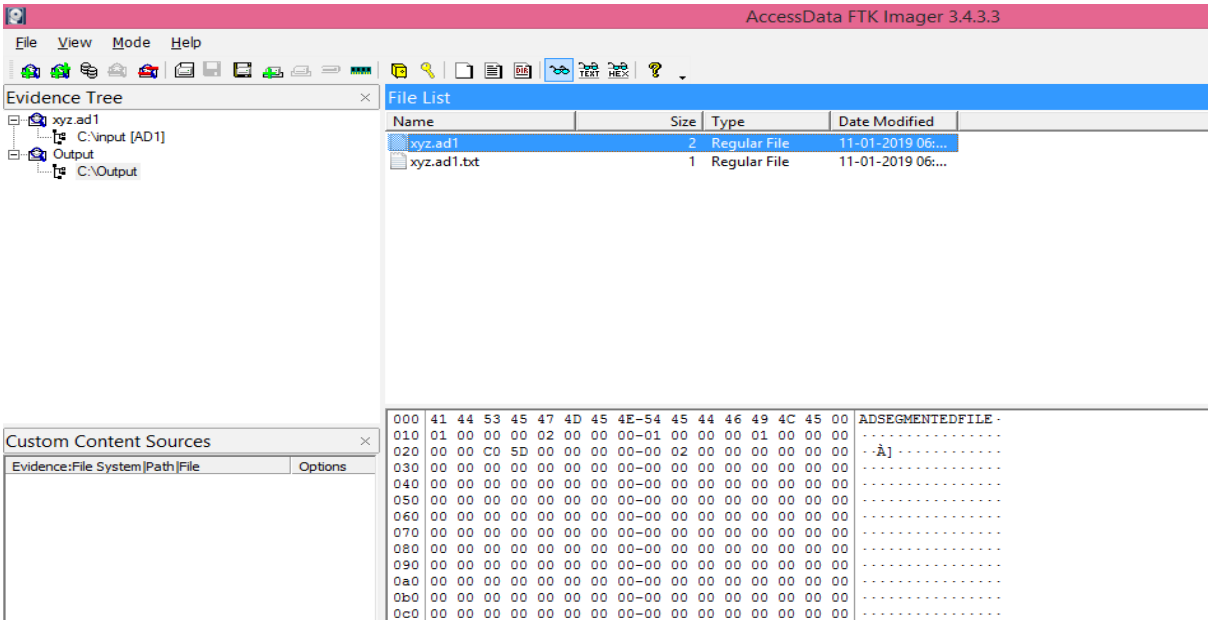


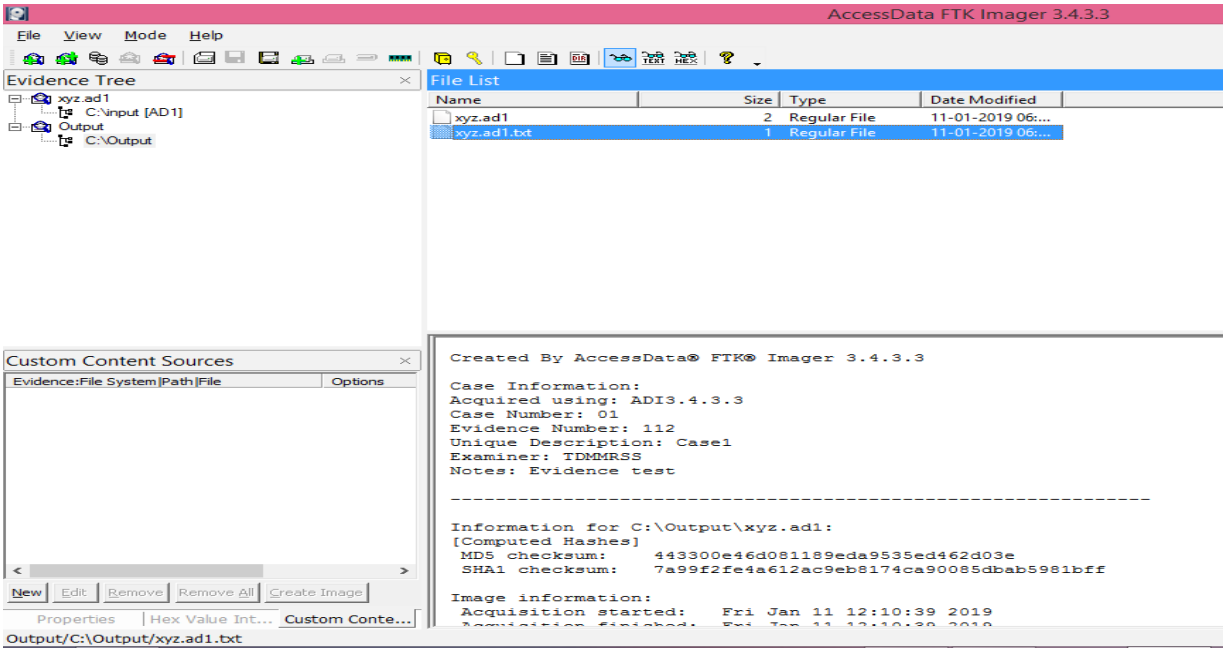


Add evidence item→image file→destination folder



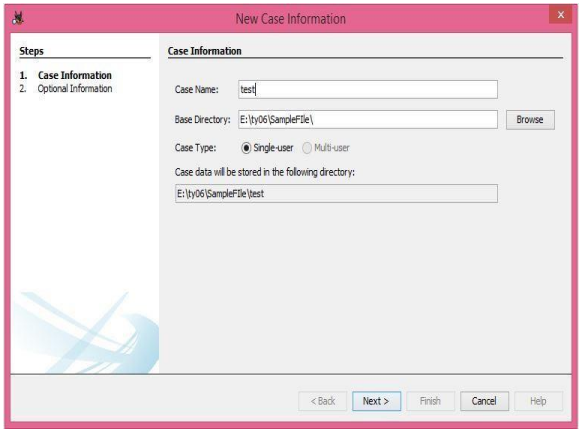
Output

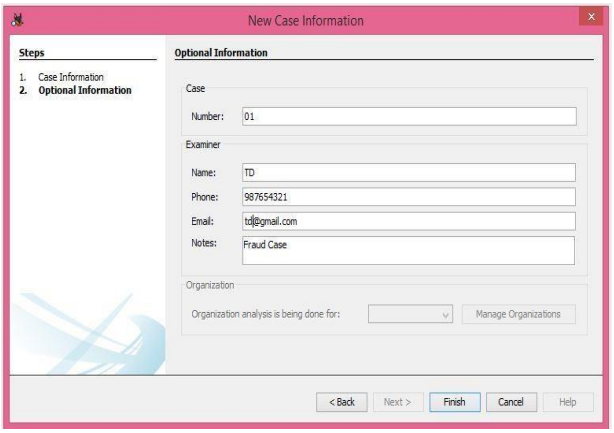




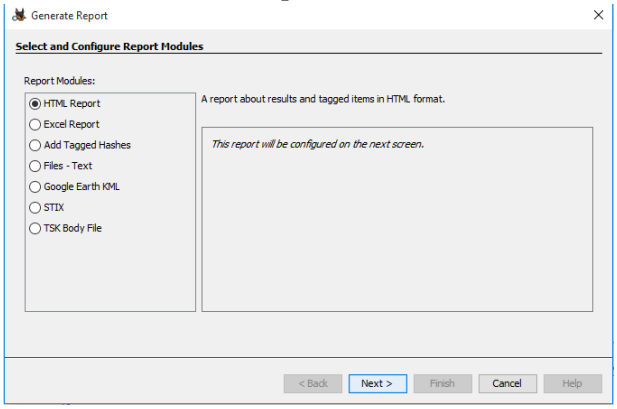
Practical No:3

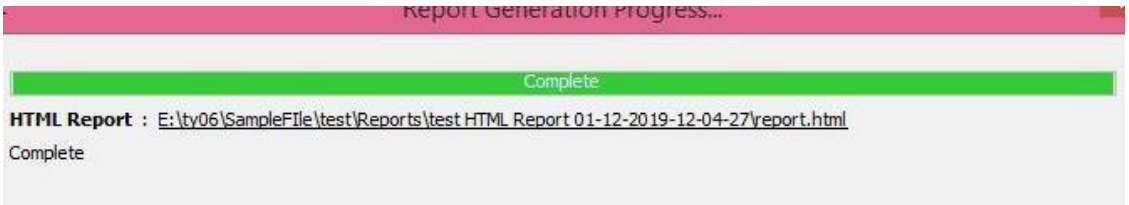
Open autopsy→ bin → File →new case→ you need a sample file→ Browse in directory
→ Fill the required information → Finish



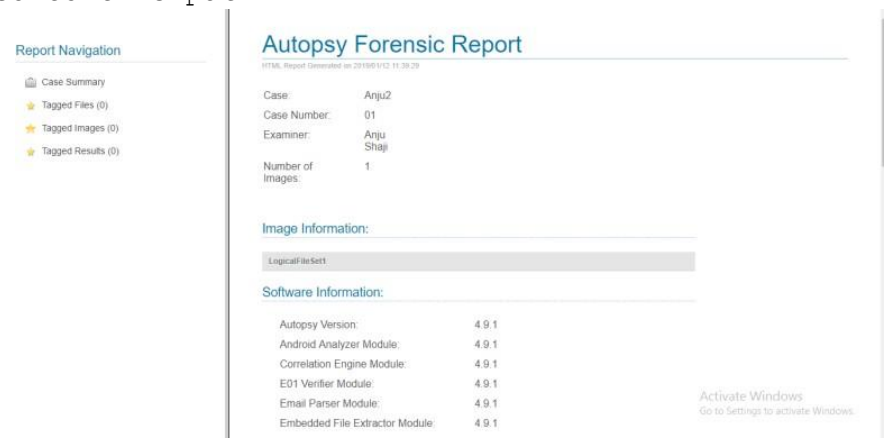


Select →Logical files→select sample file →add→ next →Finish
Then Generate Report→Click on Generate Report



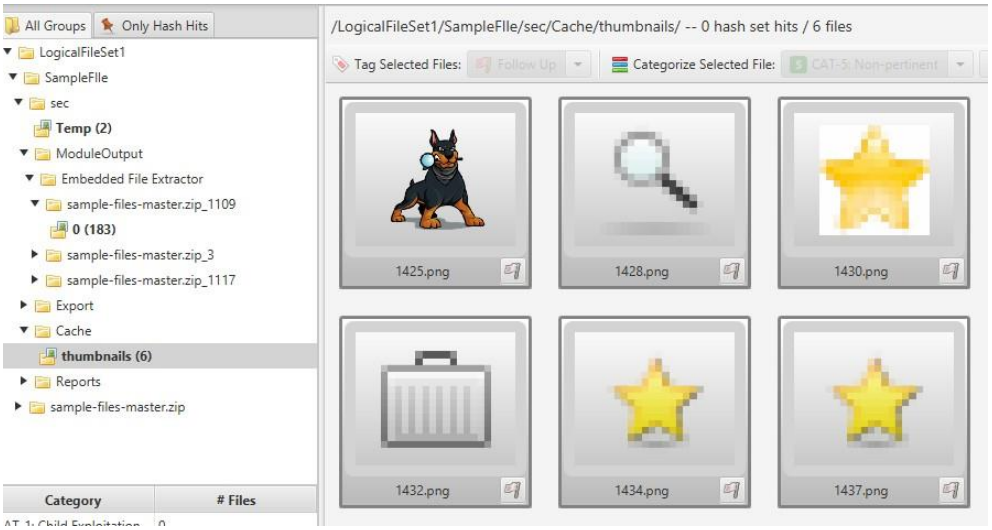


Go to this path



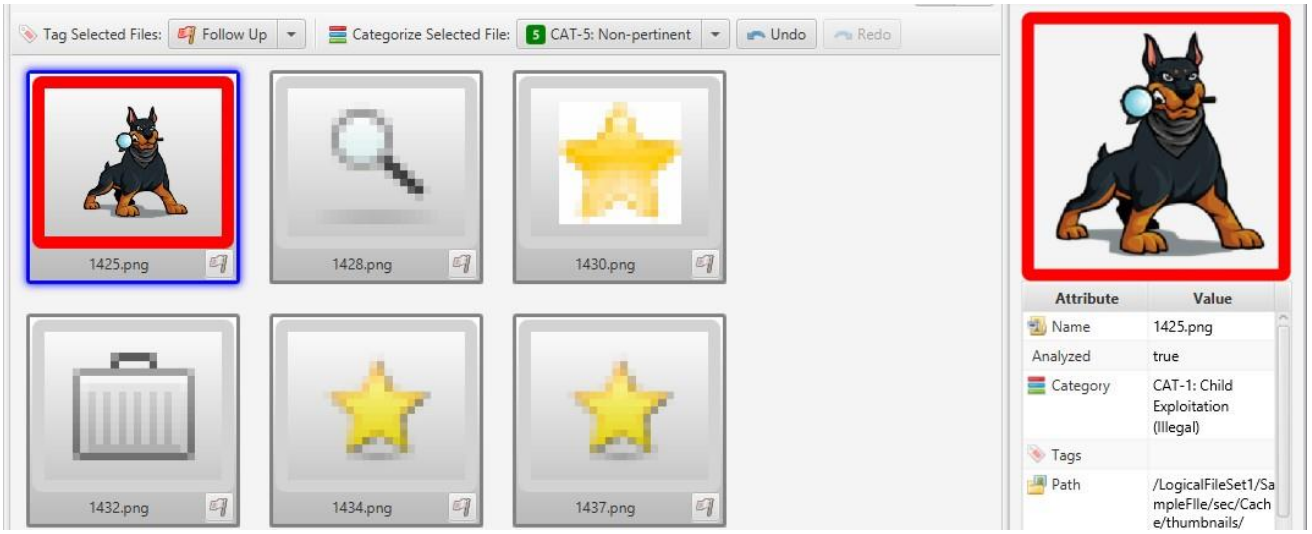
For image

Go to Image /gallery in menu → cache → thumbnails →pictures



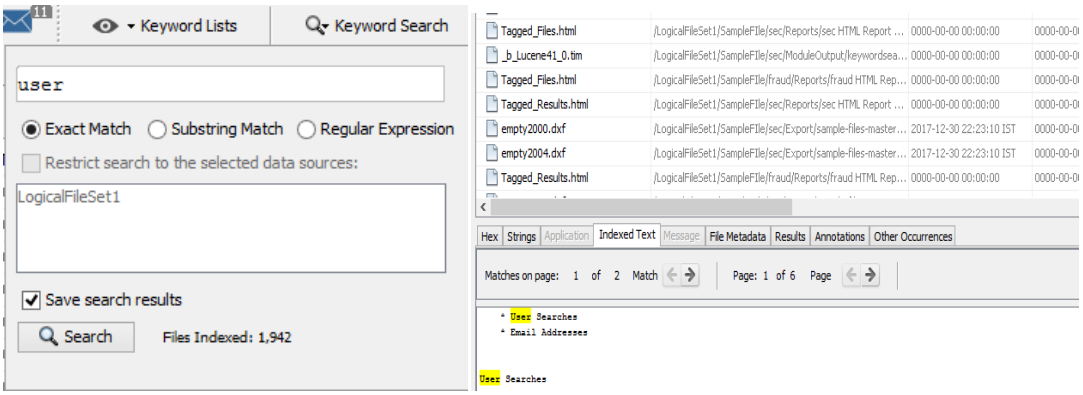
Right click on image →categorized

Output



For Keyword Search

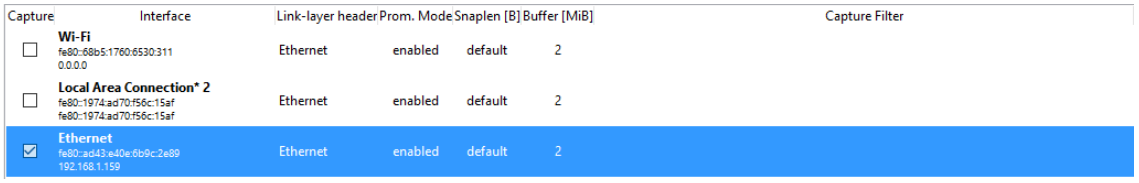
Select Keyword search at upper right corner →Type the word to search →



You can see the encrypted file with the search result

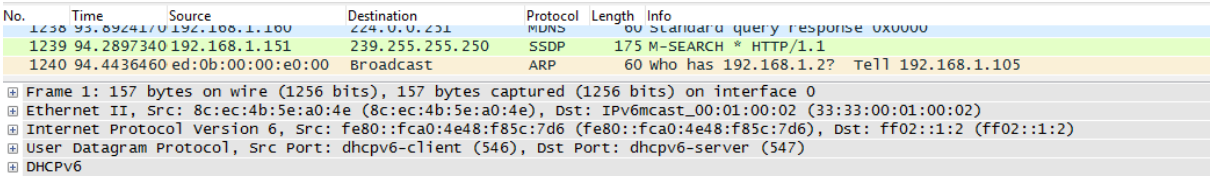
Practical No:4

Open wireshark → capture → interface →Ethernet



Capture	Interface	Link-layer header	Prom. Mode	Snaplen [B]	Buffer [MiB]	Capture Filter
☐	Wi-Fi fe80::68b5:1760:6530:311 0.0.0.0	Ethernet	enabled	default	2	
☐	Local Area Connection* 2 fe80::1974:ad70:f56c:15af fe80::1974:ad70:f56c:15af	Ethernet	enabled	default	2	
☑	Ethernet fe80::ad43:e40e:6b9c:2e89 192.168.1.159	Ethernet	enabled	default	2	

Capture Packets

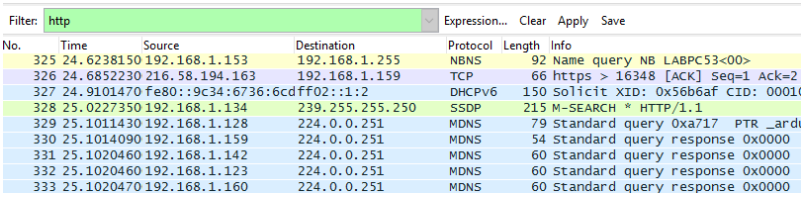


No.	Time	Source	Destination	Protocol	Length	Info
1238	93.8924170	192.168.1.160	224.0.0.251	MDNS	60	Standard query response 0x0000
1239	94.2897340	192.168.1.151	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
1240	94.4436460	ed:0b:00:00:e0:00	Broadcast	ARP	60	Who has 192.168.1.2? Tell 192.168.1.105

```
⊞ Frame 1: 157 bytes on wire (1256 bits), 157 bytes captured (1256 bits) on interface 0
⊞ Ethernet II, Src: 8c:ec:4b:5e:a0:4e (8c:ec:4b:5e:a0:4e), Dst: IPv6mcast_00:01:00:02 (33:33:00:01:00:02)
⊞ Internet Protocol Version 6, Src: fe80::fca0:4e48:f85c:7d6 (fe80::fca0:4e48:f85c:7d6), Dst: ff02::1:2 (ff02::1:2)
⊞ User Datagram Protocol, Src Port: dhcpv6-client (546), Dst Port: dhcpv6-server (547)
⊞ DHCPv6
```

Analyze the captured packets

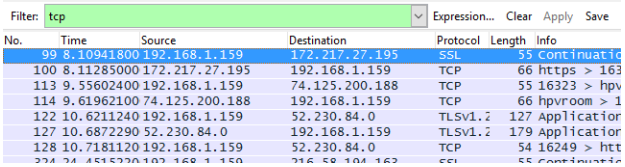
http



Filter: http

No.	Time	Source	Destination	Protocol	Length	Info
325	24.6238150	192.168.1.153	192.168.1.255	NBNS	92	Name query NB LABPC53<00>
326	24.6852230	216.58.194.163	192.168.1.159	TCP	66	https > 16348 [ACK] Seq=1 Ack=2
327	24.9101470	fe80::9c34:6736:6cd	ff02::1:2	DHCPv6	150	Solicit XID: 0x56b6af CID: 0001
328	25.0227350	192.168.1.134	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
329	25.1011430	192.168.1.128	224.0.0.251	MDNS	79	Standard query 0xa717 PTR _ard
330	25.1014090	192.168.1.159	224.0.0.251	MDNS	54	Standard query response 0x0000
331	25.1020460	192.168.1.142	224.0.0.251	MDNS	60	Standard query response 0x0000
332	25.1020460	192.168.1.123	224.0.0.251	MDNS	60	Standard query response 0x0000
333	25.1020470	192.168.1.160	224.0.0.251	MDNS	60	Standard query response 0x0000

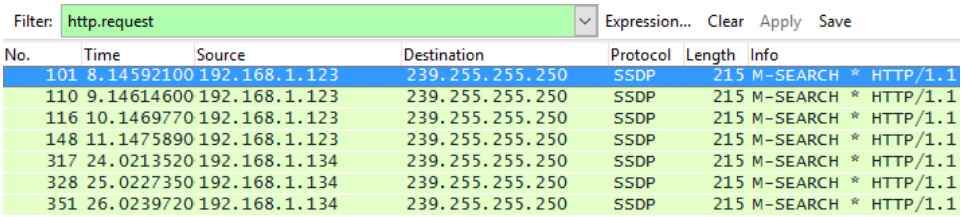
tcp



Filter: tcp

No.	Time	Source	Destination	Protocol	Length	Info
99	8.10941800	192.168.1.159	172.217.27.195	SSL	55	Continuatic
100	8.11285000	172.217.27.195	192.168.1.159	TCP	66	https > 163
113	9.55602400	192.168.1.159	74.125.200.188	TCP	55	16323 > hpv
114	9.61962100	74.125.200.188	192.168.1.159	TCP	66	hpvroom > 1
122	10.6211240	192.168.1.159	52.230.84.0	TLSv1.2	127	Applicatior
127	10.6872290	52.230.84.0	192.168.1.159	TLSv1.2	179	Applicatior
128	10.7181120	192.168.1.159	52.230.84.0	TCP	54	16249 > htt

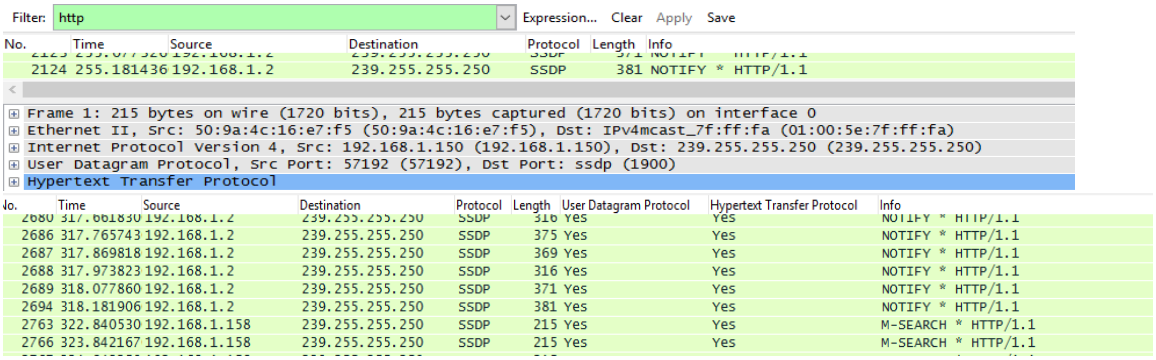
http.request



Filter: http.request

No.	Time	Source	Destination	Protocol	Length	Info
101	8.14592100	192.168.1.123	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
110	9.14614600	192.168.1.123	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
116	10.1469770	192.168.1.123	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
148	11.1475890	192.168.1.123	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
317	24.0213520	192.168.1.134	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
328	25.0227350	192.168.1.134	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
351	26.0239720	192.168.1.134	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1

Go to goggle→search anything→Go to wireshark →http→ Right click→apply as column



Filter: http

No.	Time	Source	Destination	Protocol	Length	User Datagram Protocol	Hypertext Transfer Protocol	Info
2124	255.181436	192.168.1.2	239.255.255.250	SSDP	381			NOTIFY * HTTP/1.1
2680	317.661830	192.168.1.2	239.255.255.250	SSDP	316	Yes	Yes	NOTIFY * HTTP/1.1
2686	317.765743	192.168.1.2	239.255.255.250	SSDP	375	Yes	Yes	NOTIFY * HTTP/1.1
2687	317.869818	192.168.1.2	239.255.255.250	SSDP	369	Yes	Yes	NOTIFY * HTTP/1.1
2688	317.973823	192.168.1.2	239.255.255.250	SSDP	316	Yes	Yes	NOTIFY * HTTP/1.1
2689	318.077860	192.168.1.2	239.255.255.250	SSDP	371	Yes	Yes	NOTIFY * HTTP/1.1
2694	318.181906	192.168.1.2	239.255.255.250	SSDP	381	Yes	Yes	NOTIFY * HTTP/1.1
2763	322.840530	192.168.1.158	239.255.255.250	SSDP	215	Yes	Yes	M-SEARCH * HTTP/1.1
2766	323.842167	192.168.1.158	239.255.255.250	SSDP	215	Yes	Yes	M-SEARCH * HTTP/1.1

```
⊞ Frame 1: 215 bytes on wire (1720 bits), 215 bytes captured (1720 bits) on interface 0
⊞ Ethernet II, Src: 50:9a:4c:16:e7:f5 (50:9a:4c:16:e7:f5), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
⊞ Internet Protocol Version 4, Src: 192.168.1.150 (192.168.1.150), Dst: 239.255.255.250 (239.255.255.250)
⊞ User Datagram Protocol, Src Port: 57192 (57192), Dst Port: ssdp (1900)
⊞ Hypertext Transfer Protocol
```

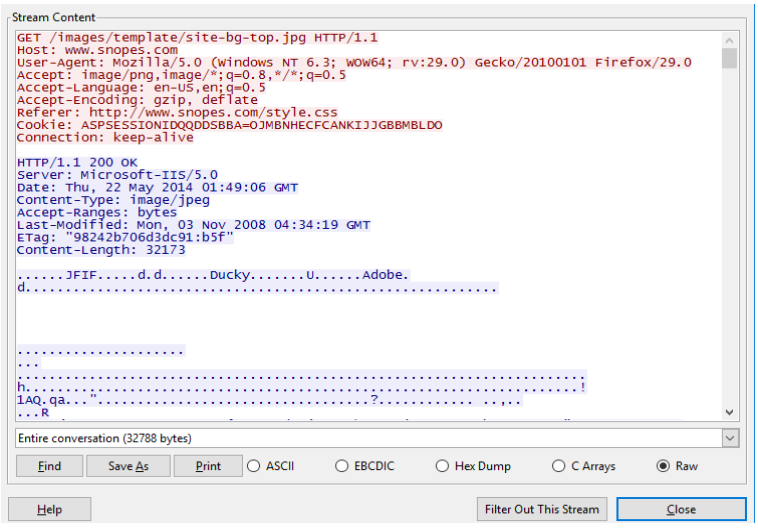
Practical No:5

1.What web server software is used by www.snopes.com?

Open Wireshark → file → open → Asksnopes.pcapng
Select any http → right click → Apply as Column

No.	Time	Source	Destination	Protocol	Length	Hypertext Transfer Pr
19	0.62119200	192.168.1.71	66.165.133.65	HTTP	440	Yes
22	0.71957600	66.165.133.65	192.168.1.71	TCP	1514	
23	0.72041500	66.165.133.65	192.168.1.71	TCP	1514	
24	0.72047200	192.168.1.71	66.165.133.65	TCP	54	
25	0.72122300	66.165.133.65	192.168.1.71	TCP	1514	
26	0.72199800	66.165.133.65	192.168.1.71	TCP	1514	
27	0.72200000	66.165.133.65	192.168.1.71	TCP	1514	
28	0.72200000	66.165.133.65	192.168.1.71	TCP	1514	
29	0.72206900	192.168.1.71	66.165.133.65	TCP	54	
30	0.72281200	66.165.133.65	192.168.1.71	TCP	1514	
31	0.72358100	66.165.133.65	192.168.1.71	TCP	1514	
32	0.72358200	66.165.133.65	192.168.1.71	TCP	1514	
33	0.72363700	192.168.1.71	66.165.133.65	TCP	54	
34	0.72438000	66.165.133.65	192.168.1.71	TCP	1514	
35	0.72438200	66.165.133.65	192.168.1.71	TCP	1514	

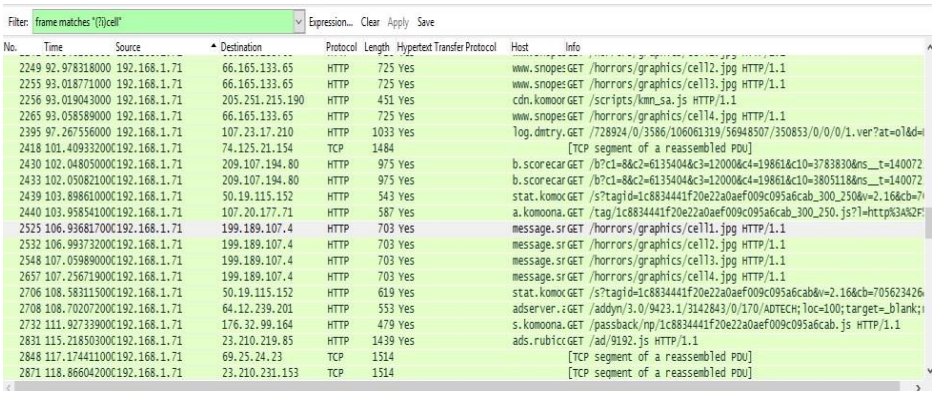
select http file → right click → follow TCP Stream



About what cell phone problem is the client concerned?

Client talking about cell so we search for cell keyword in whole packets.

frame.matches "(?i)cell



In the first HTTP request cell keyword is in URL and it was about cell phone charging issue.

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

frame.matches "(?i)zillow"

Filter: frame matches "(?i)zillow" Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Hypertext Transfer Protocol	Host	Info
1963	88.209599000	192.168.1.71	173.194.37.91	HTTP	772	Yes	s1.2mdn.ne	GET /3973258/Zillow_728x90_Rooms_Q4.swf HTTP/1.1

Open file → Export Object →HTTP → save All → select the folder to save

Packet num	Hostname	Content Type	Size	Filename
52	www.snopes.com	image/jpeg	32 kB	site-bg-top.jpg
54		text/plain	15 bytes	
70	as.casalemedia.com	text/javascript	6735 bytes	cellcharge.asp&f=1&id=4240355892.946045
101	www.google-analytics.com	image/gif	35 bytes	__utm.gif?utmwv=5.5.1&utms=1&utmn=6

Open the folder → search for the file name zillow → open with browser

How many web servers are running Apache?

http.response

Filter: http.response Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Host	Hypertext Transfer Protocol	Host	Host
22	0.719576000	66.165.133.65	192.168.1.71	HTTP	1514		Yes		
54	0.855624000	108.160.167.165	192.168.1.71	HTTP	233		Yes		
62	0.940186000	207.109.230.161	192.168.1.71	HTTP	1514		Yes		
101	3.392317000	74.125.196.139	192.168.1.71	HTTP	458		Yes		
108	3.506339000	50.19.115.152	192.168.1.71	HTTP	338		Yes		
112	3.567554000	107.20.177.71	192.168.1.71	HTTP	955		Yes		
129	5.416869000	50.19.115.152	192.168.1.71	HTTP	338		Yes		
132	5.582995000	64.12.239.201	192.168.1.71	HTTP	276		Yes		
153	6.889975000	176.32.99.164	192.168.1.71	HTTP	1514		Yes		
159	7.030346000	54.85.82.173	192.168.1.71	HTTP	681		Yes		
161	7.047345000	74.209.219.38	192.168.1.71	HTTP	303		Yes		
178	8.267658000	23.210.219.85	192.168.1.71	HTTP	1514		Yes		
196	9.145575000	54.84.236.238	192.168.1.71	HTTP	757		Yes		
202	9.621397000	69.25.24.23	192.168.1.71	HTTP	1514		Yes		

Select http → apply as column

http.server contains "Apache"

Filter: http.server contains "Apache" Expression... Clear Apply Save

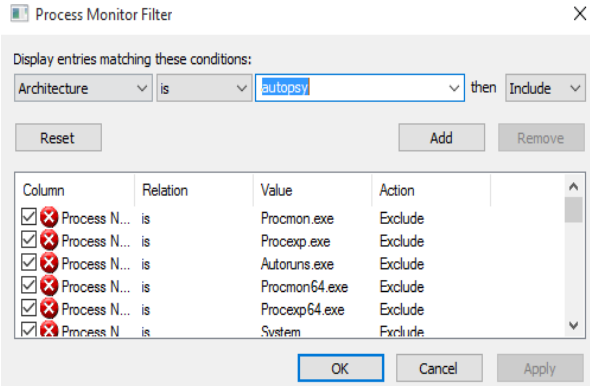
pertext Transfer Protocol	Host	Transmission Control Protocol	Hypertext Transfer Protocol	Server	Info
s		Yes	Yes	Apache	HTTP/1.1 200 OK (text/javascript)
s		Yes	Yes	Apache	HTTP/1.1 200 OK (application/x-javascript)
s		Yes	Yes	Apache	HTTP/1.1 200 OK (application/x-javascript)
s		Yes	Yes	Apache	HTTP/1.1 200 OK (application/x-javascript)
s		Yes	Yes	Apache	HTTP/1.1 200 OK (text/javascript)
s		Yes	Yes	Apache/2.2	HTTP/1.1 200 OK (text/html)
s		Yes	Yes	Apache	HTTP/1.1 200 OK [Malformed Packet]
s		Yes	Yes	Apache-Co	HTTP/1.1 302 Moved Temporarily
s		Yes	Yes	Apache-Co	HTTP/1.1 200 OK (GIF89a)
s		Yes	Yes	Apache/2.2	HTTP/1.1 200 OK (text/html)
s		Yes	Yes	Apache/2.2	HTTP/1.1 200 OK (text/html)
s		Yes	Yes	Apache/2.2	HTTP/1.1 200 OK (text/html)
s		Yes	Yes	Apache/2.2	HTTP/1.1 200 OK (text/html)

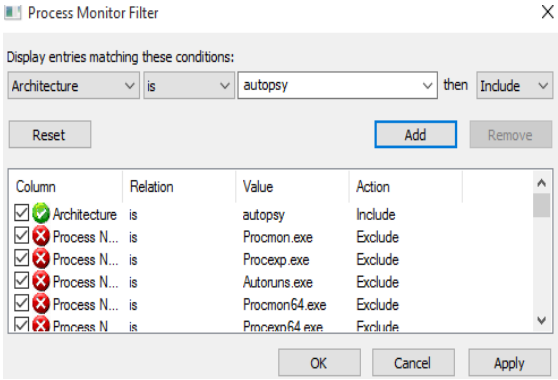
Practical No:6

1. Check Sysinternals tools

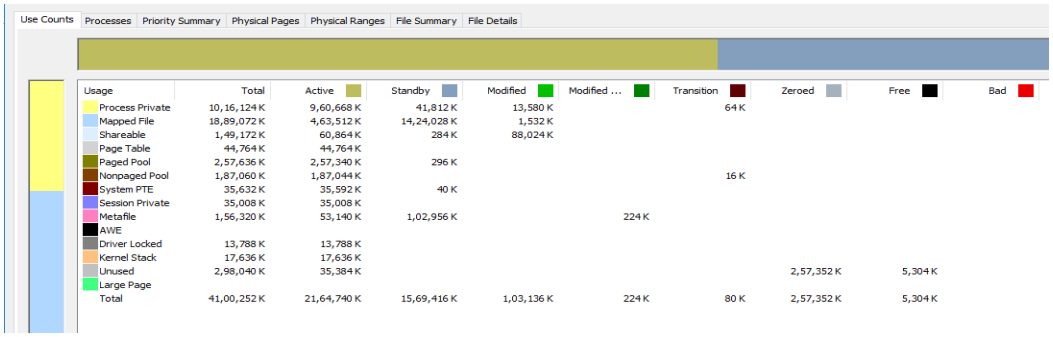
Google→sysinternal tools

2. Monitor Live Processes





3. Capture RAM



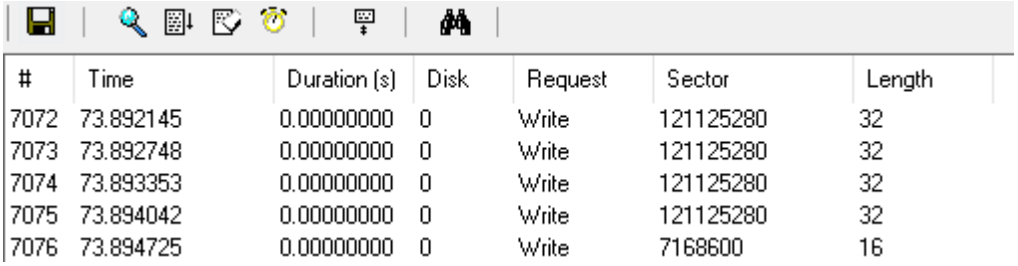
Usage	Total	Active	Standby	Modified	Modified ...	Transition	Zeroed	Free	Bad
Process Private	10,16,124 K	9,60,668 K	41,812 K	13,580 K		64 K			
Mapped File	18,89,072 K	4,63,512 K	14,24,028 K	1,532 K					
Shareable	1,49,172 K	60,864 K	284 K	88,024 K					
Page Table	44,764 K	44,764 K							
Paged Pool	2,57,636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

4. Capture TCP/UDP packets

Download TCPView

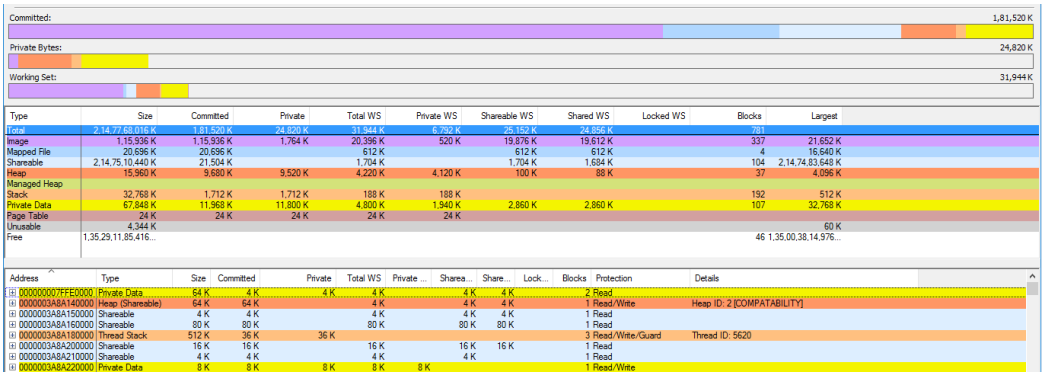
Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets	Sent Bytes	Rcvd Packets	Rcvd Bytes
chrome.exe	5808	TCP	desktop-vgrdiru	16323	sa-in-f188.1e100.net	5228	ESTABLISHED				
chrome.exe	5808	TCP	desktop-vgrdiru	16475	111.221.29.254	https	ESTABLISHED				
chrome.exe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

5. Monitor Hard Disk



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

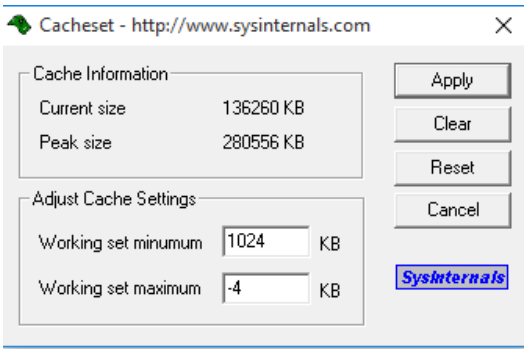
6. Monitor Virtual Memory



Type	Size	Committed	Private	Total WS	Private WS	Shareable WS	Shared WS	Locked WS	Blocks	Largest
Total	2,14,77,63,016 K	1,81,520 K	24,820 K	31,944 K	6,720 K	25,152 K	24,624 K		711	
Image	1,15,936 K	1,15,936 K	1,764 K	20,396 K	520 K	19,876 K	19,612 K		337	21,652 K
Mapped File	20,696 K	20,696 K		612 K		612 K	612 K		4	16,640 K
Shareable	2,14,75,10,440 K	21,504 K		1,704 K		1,704 K	1,684 K		104	2,14,74,83,648 K
Heap	15,960 K	9,680 K	9,520 K	4,220 K	4,120 K	100 K	88 K		37	4,096 K
Managed Heap										
Stack	32,768 K	1,712 K	1,712 K	188 K	188 K				192	512 K
Private Data	67,848 K	11,968 K	11,800 K	4,800 K	1,940 K	2,860 K	2,860 K		107	32,768 K
Page Table	24 K	24 K	24 K	24 K	24 K					
Unusable	4,344 K									60 K
Free	1,35,29,11,85,416...								46	1,35,00,38,14,976...

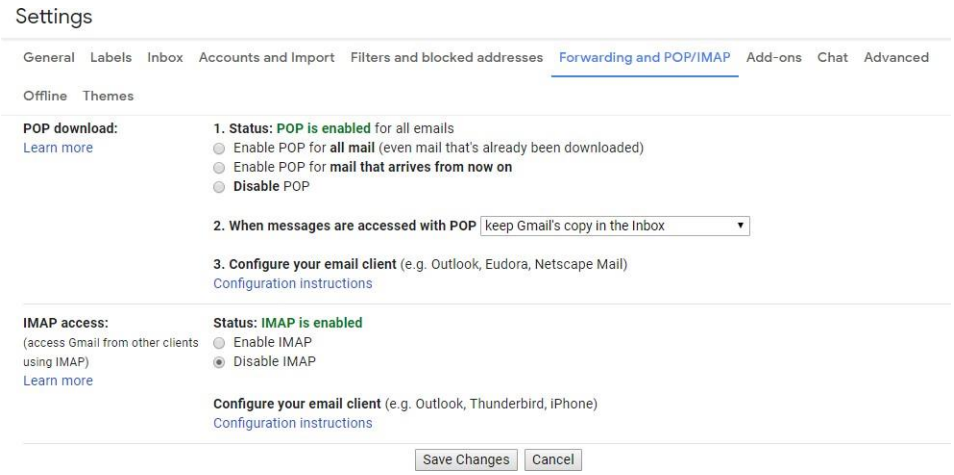
Address	Type	Size	Committed	Private	Total WS	Private ...	Sharea...	Share...	Lock...	Blocks	Protection	Details
000000007FFE0000	Private Data	64 K	4 K	4 K	4 K		4 K	4 K		2	Read	
0000003A8A140000	Heap (Shareable)	64 K	64 K		4 K		4 K	4 K		1	Read/Write	Heap ID: 2 [COMPATABILITY]
0000003A8A150000	Shareable	4 K	4 K		4 K		4 K	4 K		1	Read	
0000003A8A160000	Shareable	80 K	80 K		80 K		80 K	80 K		1	Read	
0000003A8A180000	Thread Stack	512 K	36 K	36 K						3	Read/Write/Guard	Thread ID: 5620
0000003A8A200000	Shareable	16 K	16 K		16 K		16 K	16 K		1	Read	
0000003A8A210000	Shareable	4 K	4 K		4 K		4 K			1	Read	
0000003A8A220000	Private Data	8 K	8 K	8 K	8 K	8 K				1	Read/Write	

7. Monitor Cache Memory



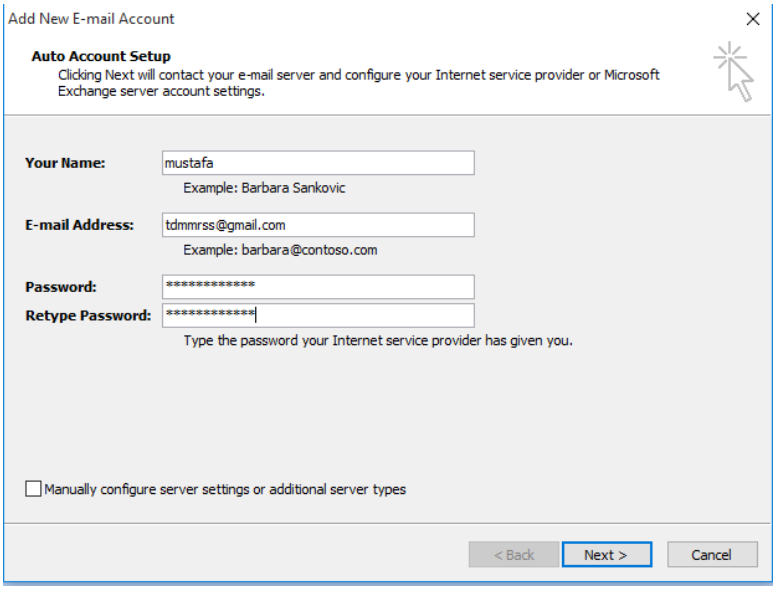
Practical No:9

Open gmail account → settings → Forwarding and POP/IMAP → Disable IMAP → Save

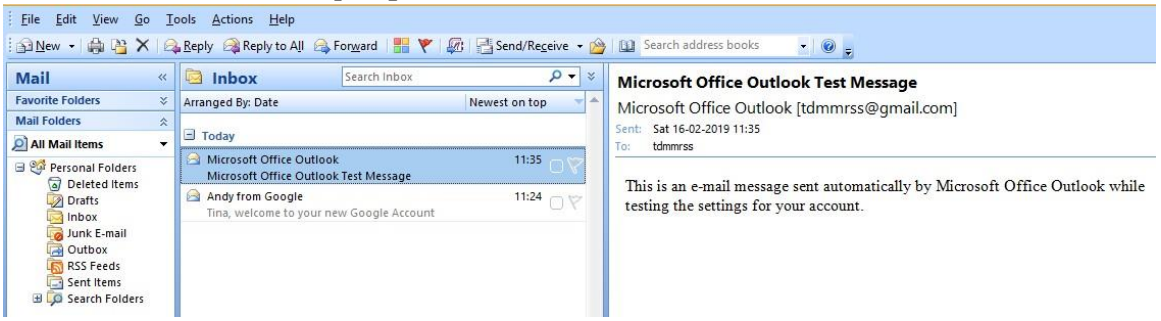


Recovering emails :-

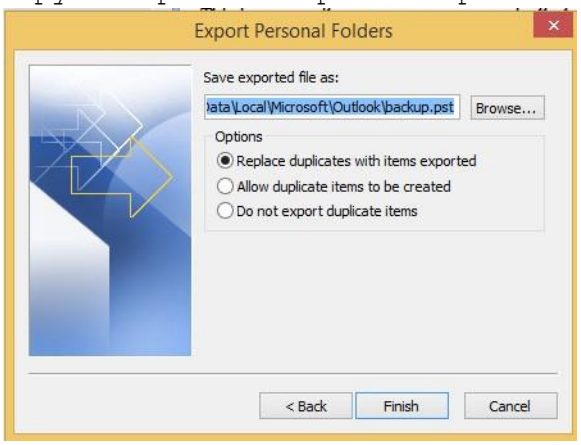
Create Outlook account with same gmail id → open Outlook 2017 → fill the information



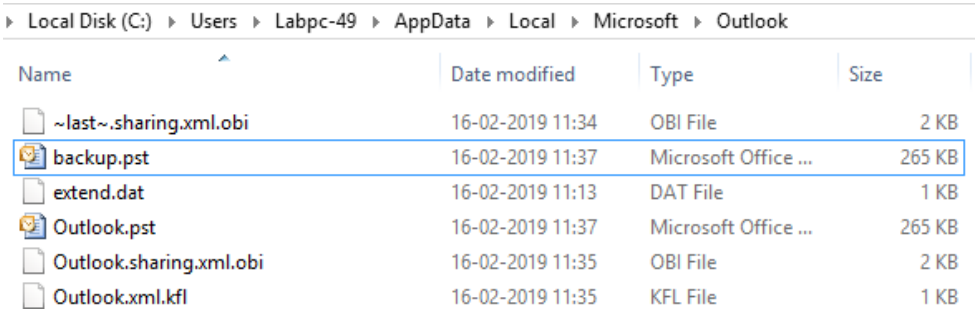
The screen will display



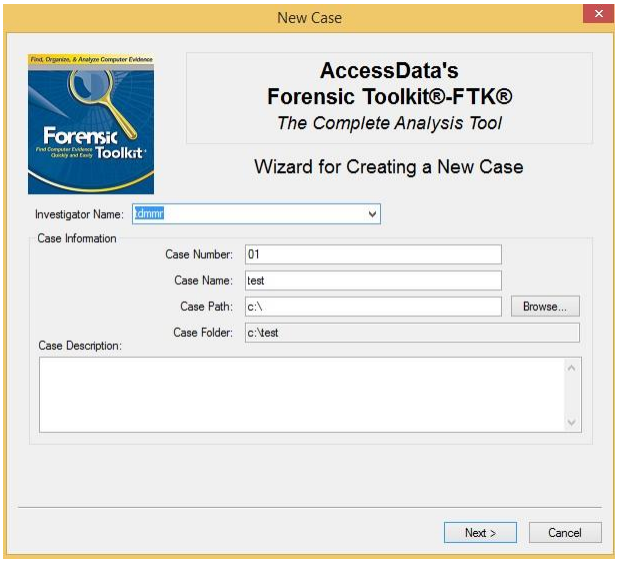
Go to File → Import and Export → Export to file → Personal Folder File(.pst) → Inbox
Copy the path → Replace duplicates with items exported



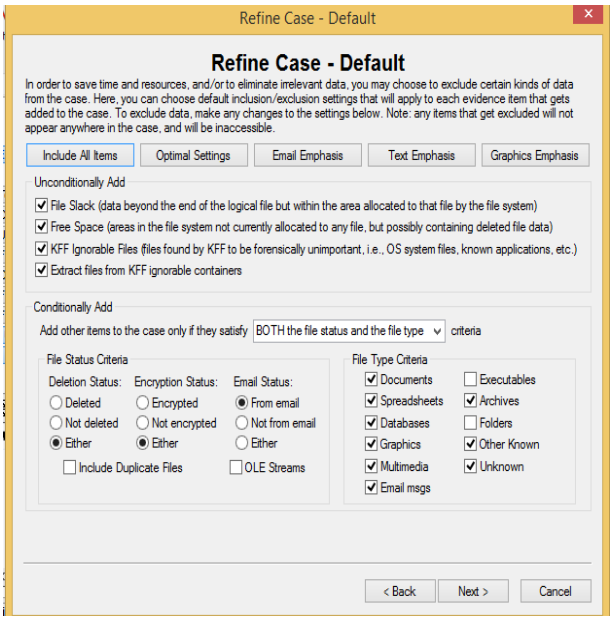
Browse to the path to see if the backup.pst file is created or not

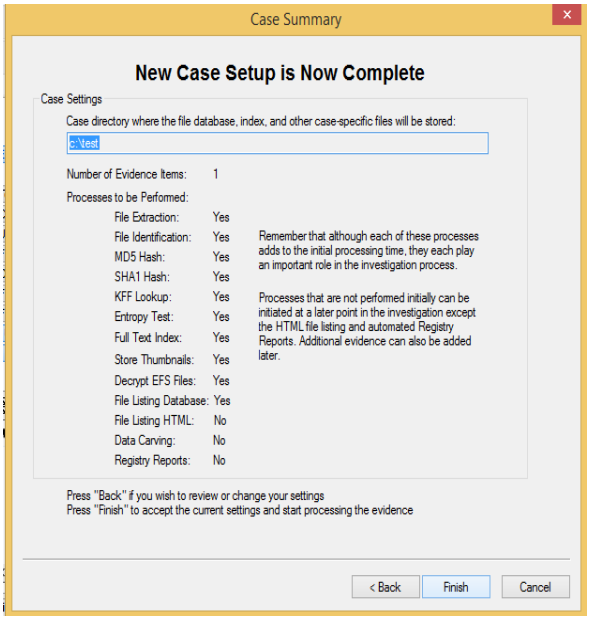


Open Forensic Toolkit 1.81(Run as Administrator) → start new case → fill the information

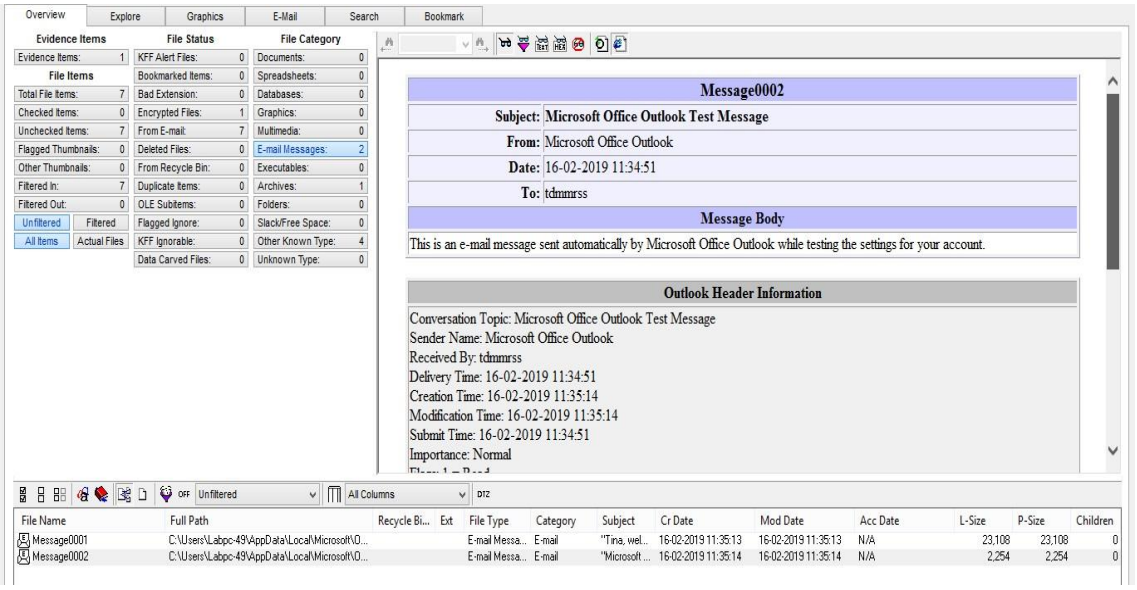


Select email emphasis → select all the checkboxes → Next → Add Evidence → Individual file → Browse the backup.pst file → Finish





Now open the E-mail Messages tab and select the E-mail you want to see the information

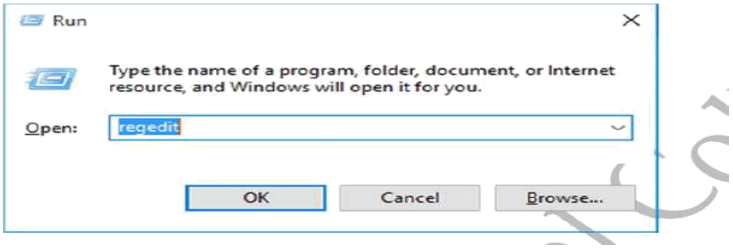


Practical No. 2

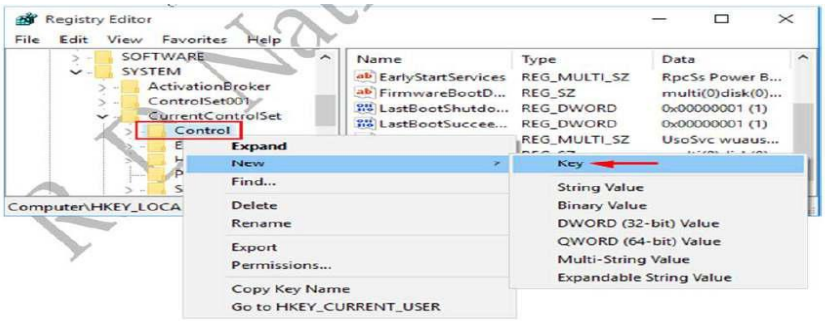
Aim: Data Acquisition:
- Perform data acquisition using:
- USB Write Blocker + FTK Imager

Steps:
Enable USB Write Block in Windows 10, 8 and 7 using registry

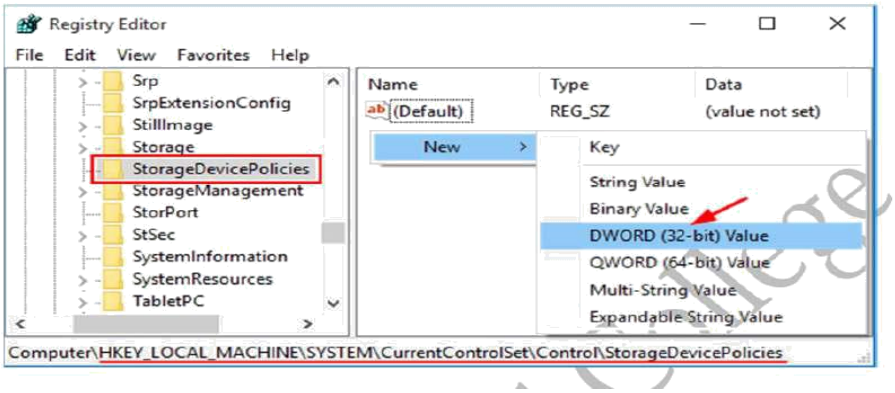
1. Press the Windows key + R to open the Run box. Type regedit and press Enter.



2. This will open the Registry Editor. Navigate to the following key:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control
3. Right-click on the Control key in the left pane, select New -> Key.
4. Name it as StorageDevicePolicies.

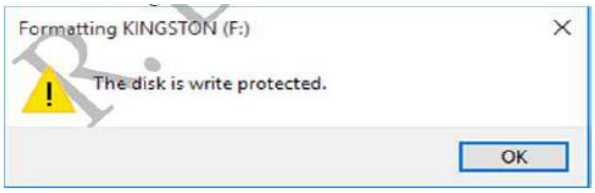


5. Select the StorageDevicePolicies key in the left pane, then right-click on any empty space
in the right pane and select New -> DWORD (32-bit) Value. Name it WriteProtect.

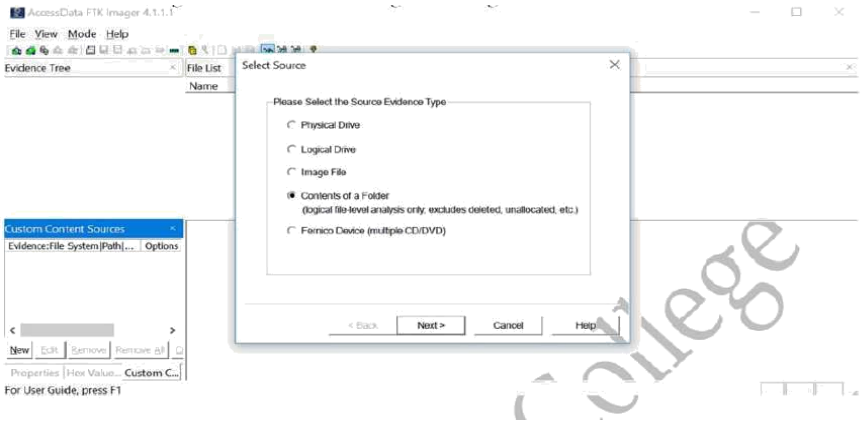


6. Double-click on WriteProtect and then change the value data from 0 to 1.

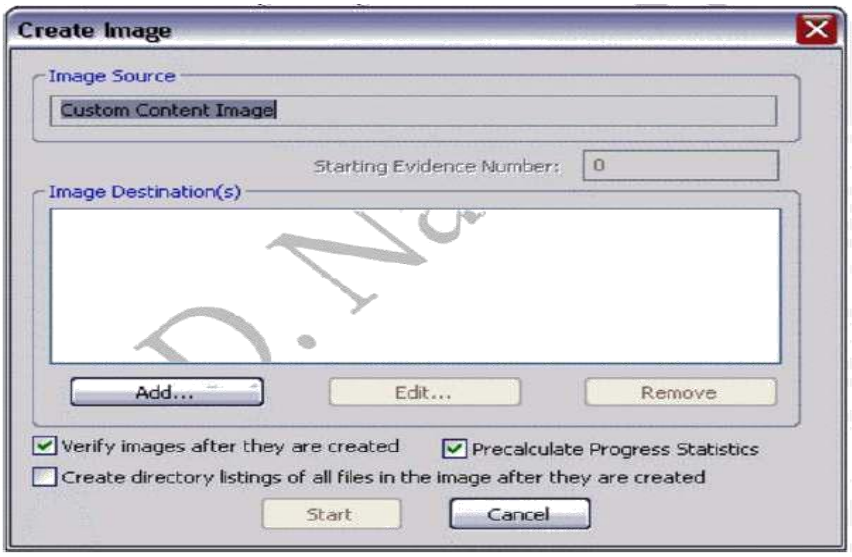
7. The new setting takes effect immediately. Every user who tries to copy / move data to USB
devices or format USB drive will get the error message
“The disk is write-protected”.
8. We can only open the file in the USB drive for reading, but it’s not allowed to modify and
save the changes back to USB drive.
So this is how you can enable write protection to all connected USB drives. If you want to
disable write protection at a later time, just open Registry Editor and set the WriteProtect
value to 0.



9.Now Create image of the USB drive using FTK imager



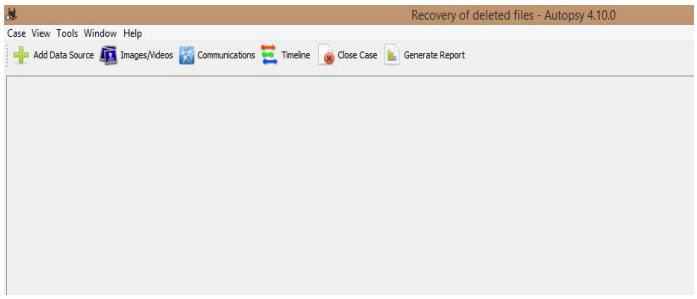
10. Select the USB drive folder by browsing and click next & Finish
11.In the Create Image dialog, click Add.



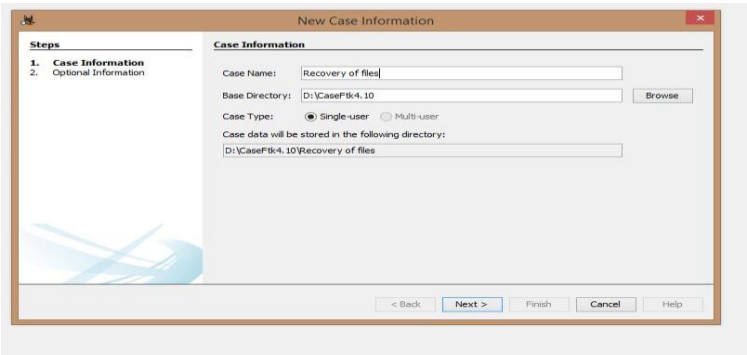
Practical No:7

To any query ple. Refer this video link :-
https://www.youtube.com/watch?v=UZo1wP_4GY

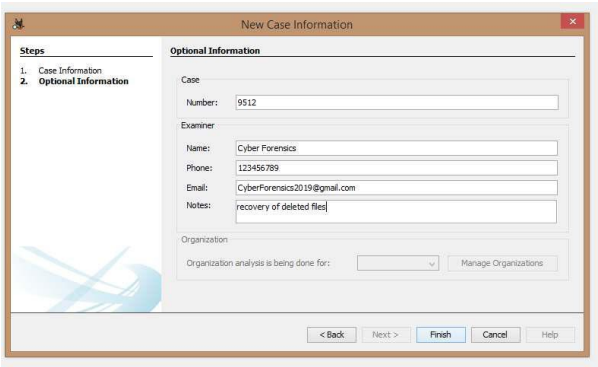
1.) Check for Deleted Files
Step1:-Create new case in autopsy (4.10.0)



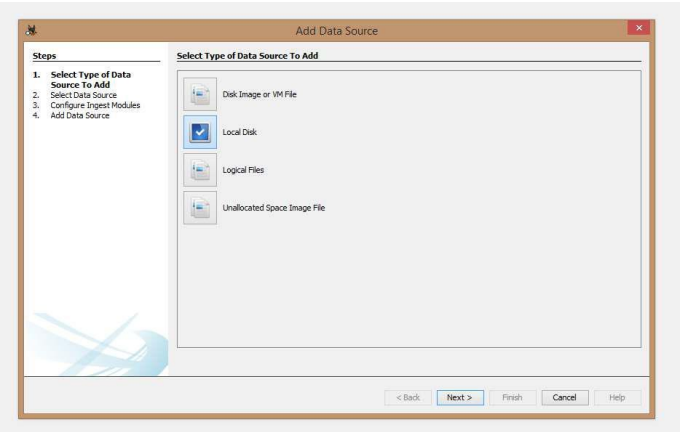
Provide new case detail



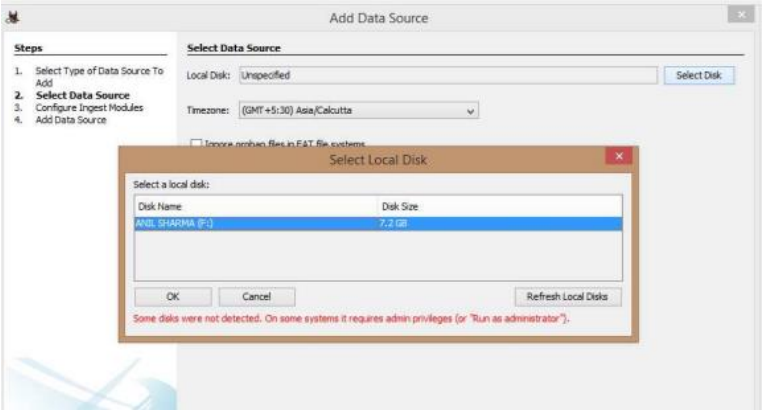
Click on next and provide other detail



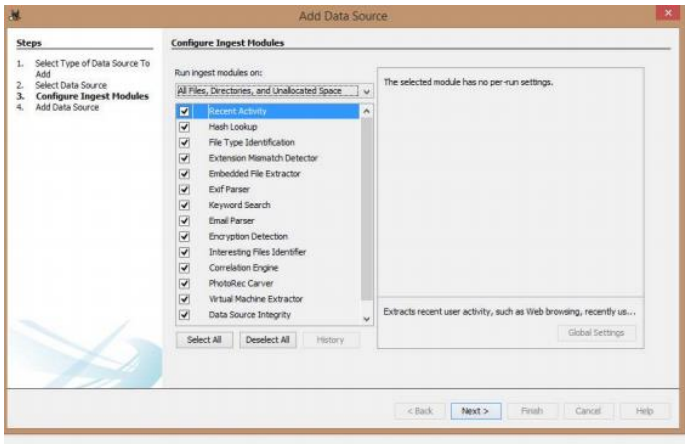
Click on finish



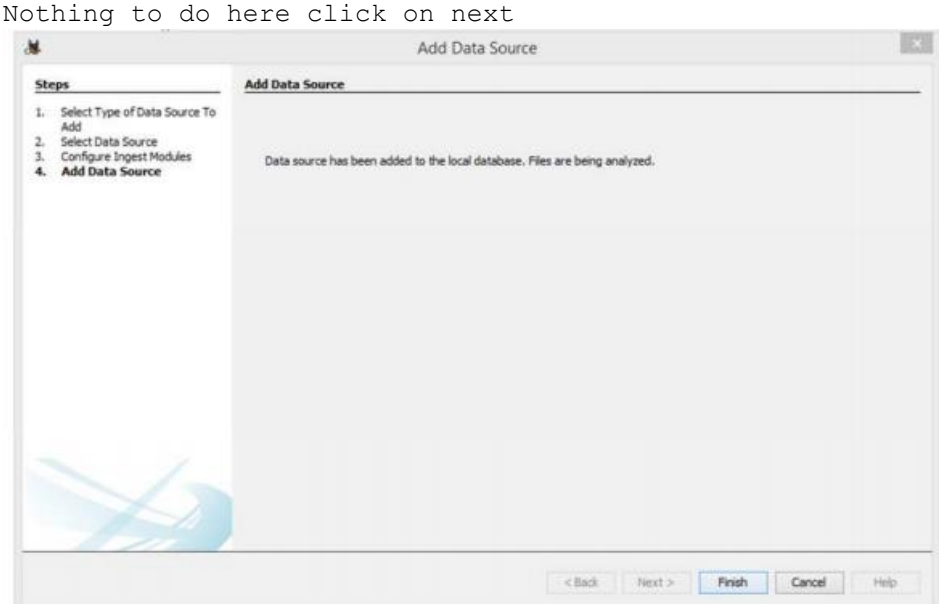
Choose type of data source as local disk(pen drive)



Choose your disk from select disk and click on ok

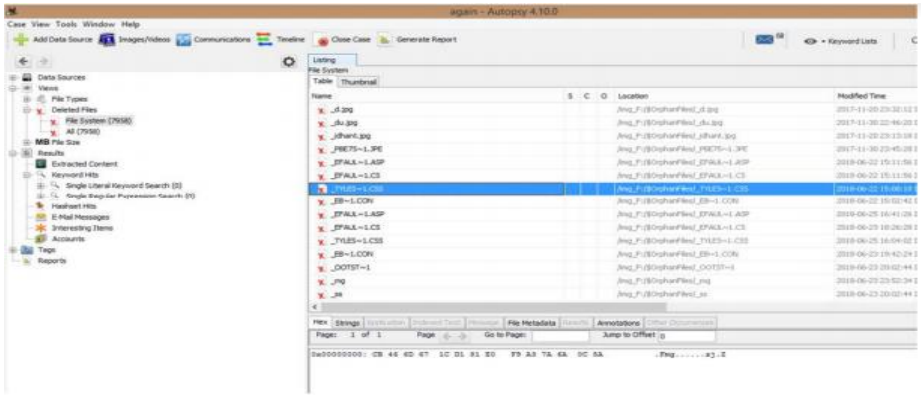


Nothing to do here click on next



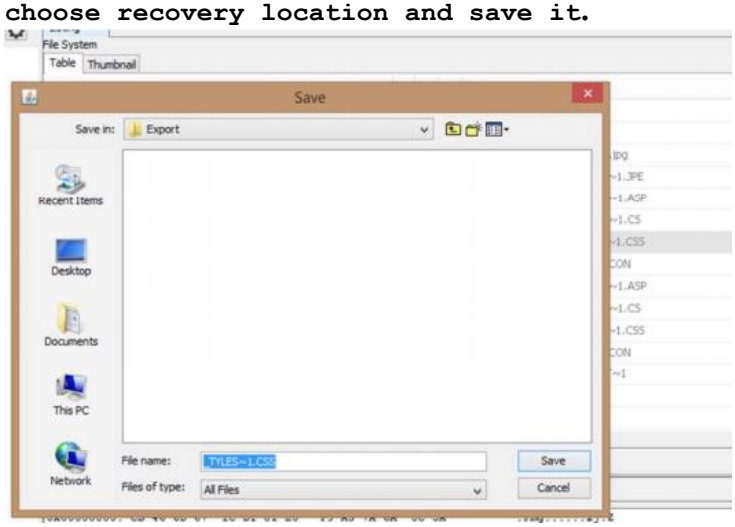
Click on finish

To see deleted files flow the path View→Deleted file→file system

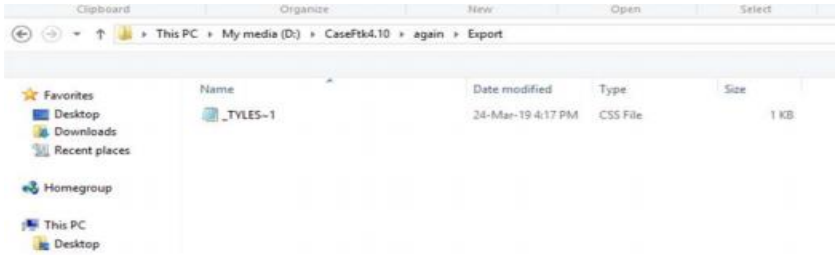


All Deleted files

To recover a file onlick on paticular file then right click export file choose recovery location and save it.



This is recover file



Practical No:8

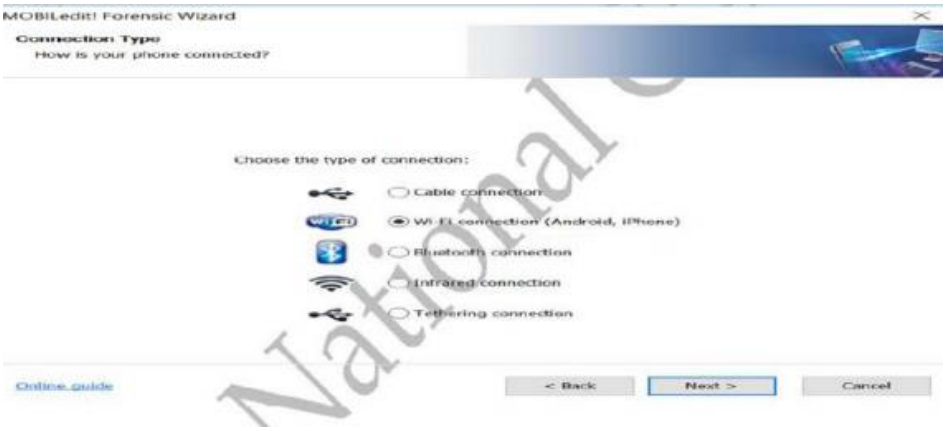
Steps:

1. **Download mobiledit forensic tool in mobile.**
2. **Open Mobiledit tool in PC.**

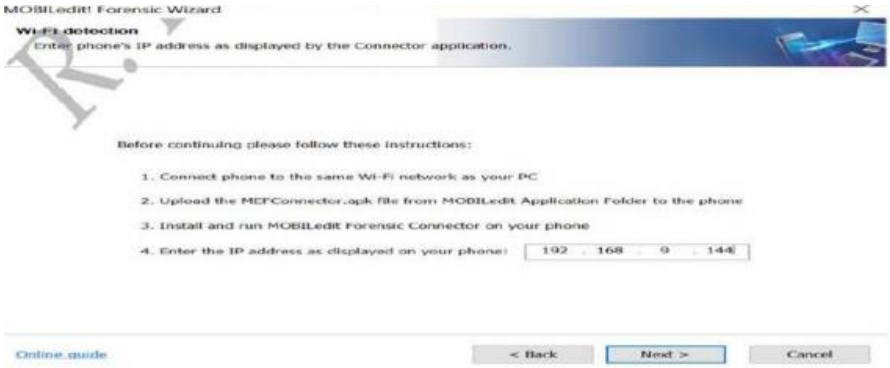
3.Click on connect.

4.Connect your mobile device to the system. Click on phone > next.

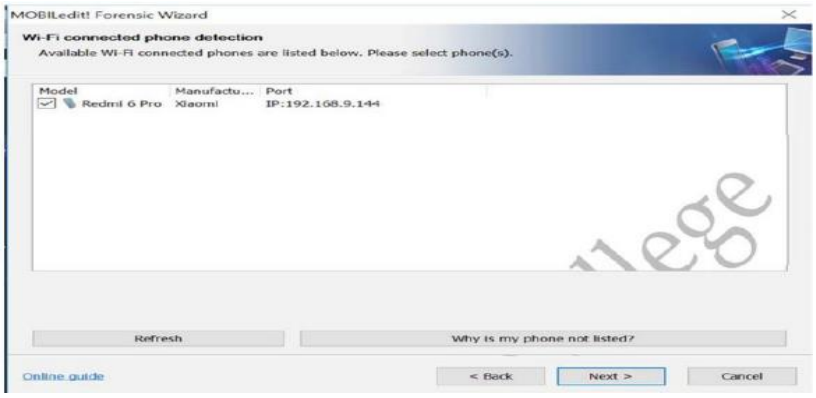
5.Click the connection



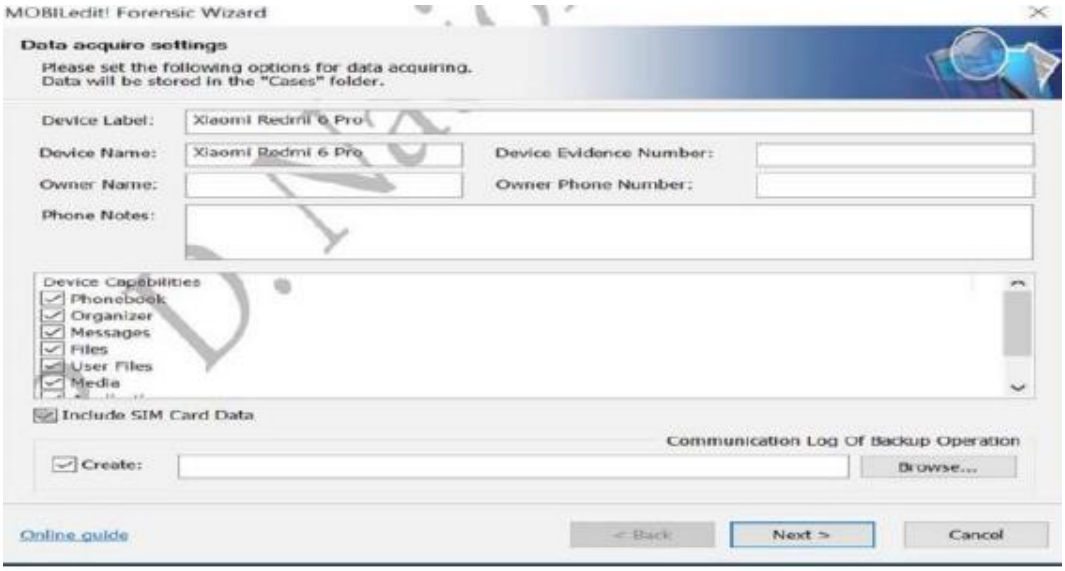
6. Open the mobiledit tool in phone and click on the type of connection (i.e Wifi) > Copy the
IP address and enter it in the PC and click next.



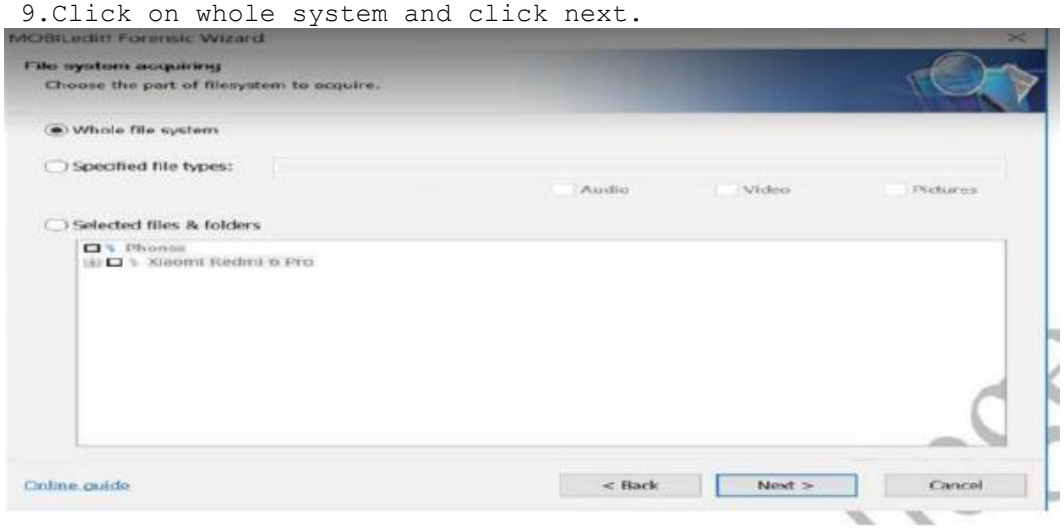
7.It shows the phone which is connected. Click on next.

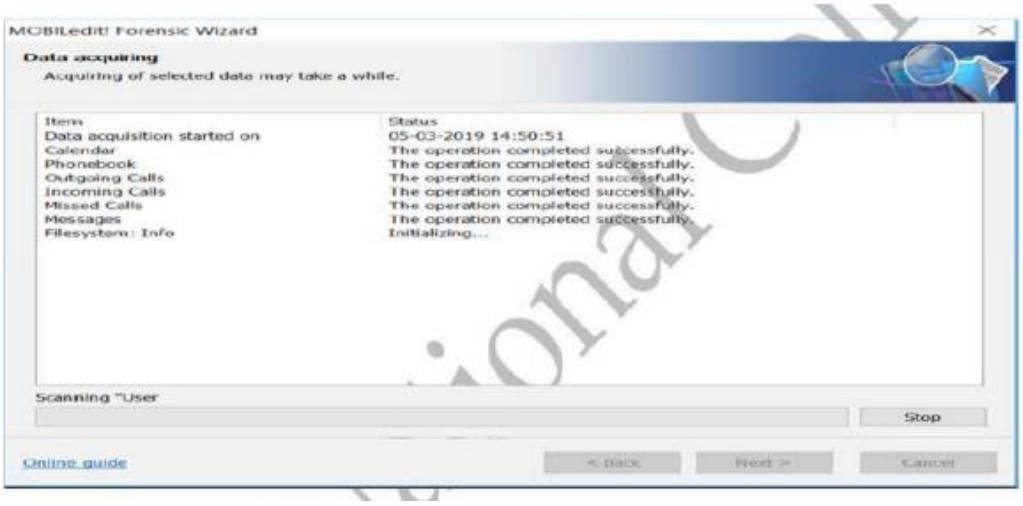


8.Click on next.

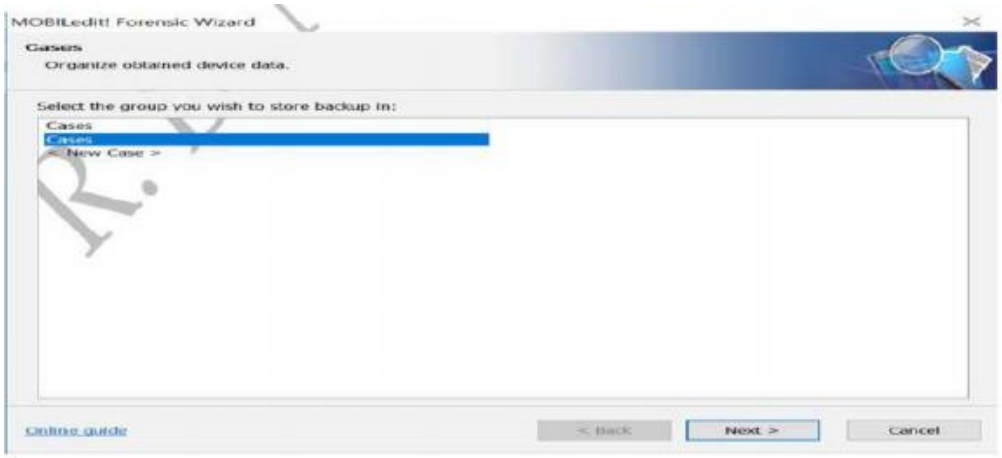


9.Click on whole system and click next.

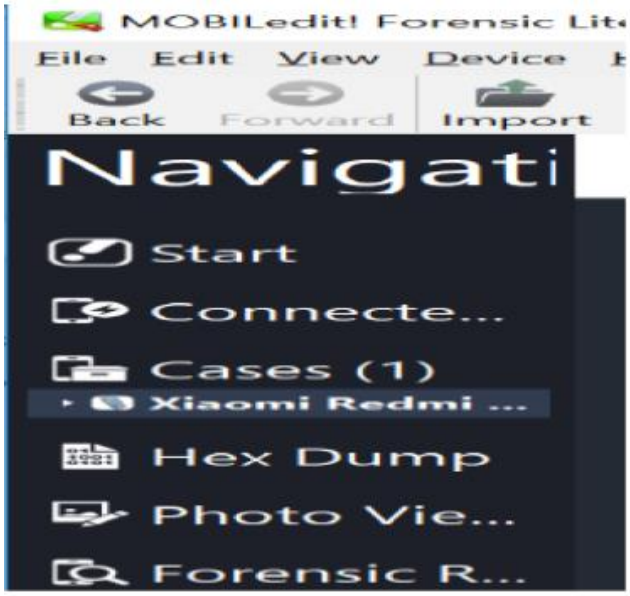




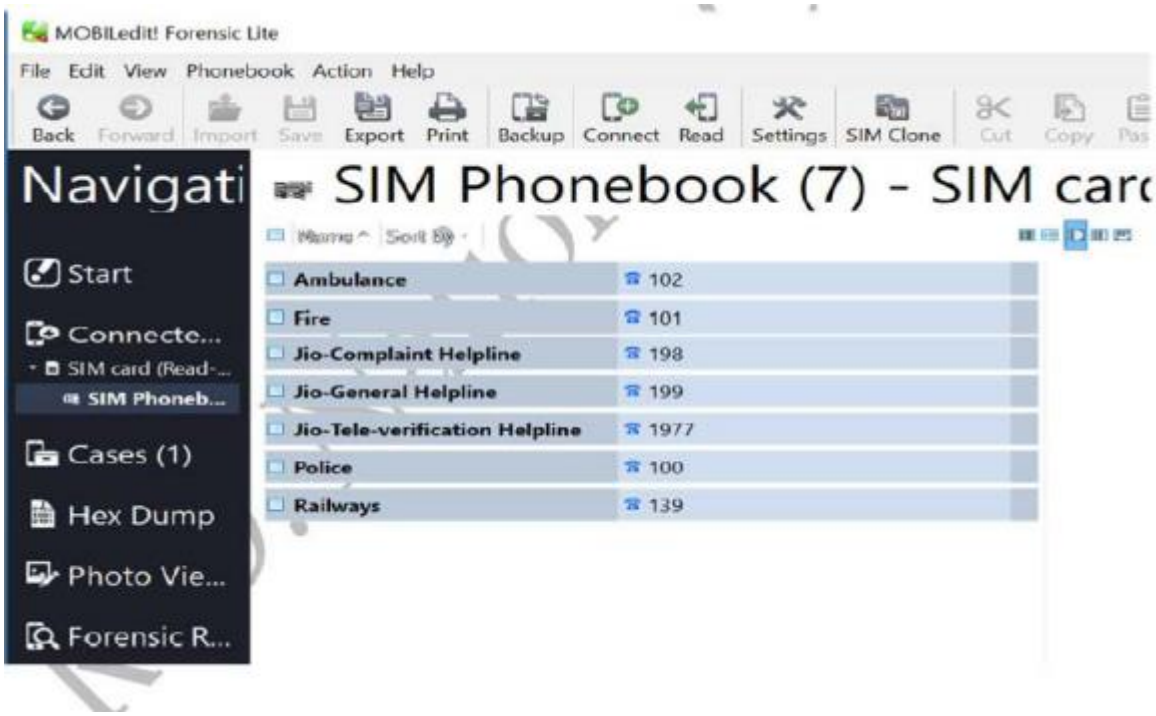
8. click on case and click next.



9. Click on your device in the left panel.



10. You can see all the files.

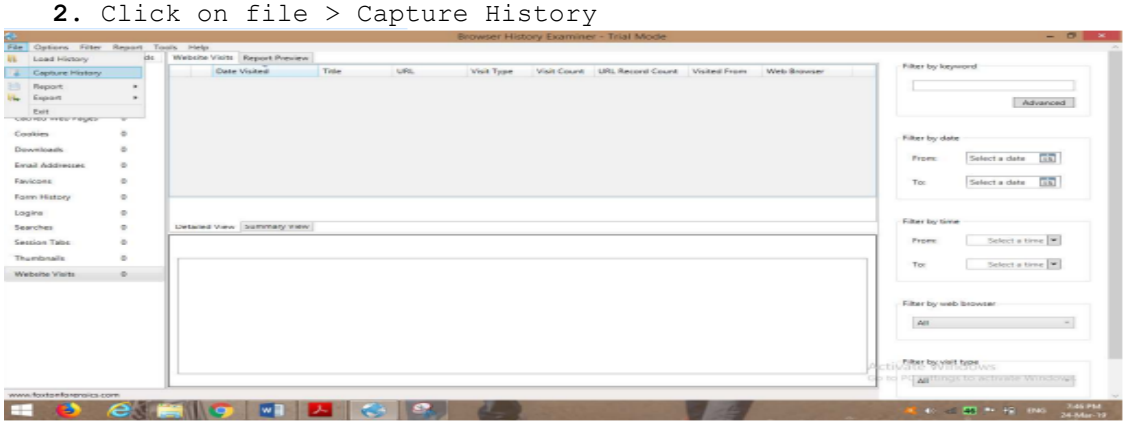


Practical No:10

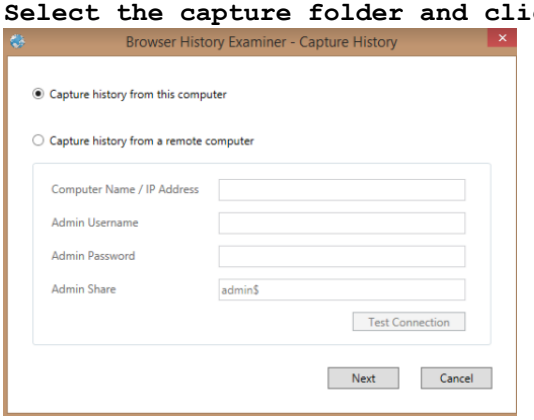
Steps:

1. **Open BrowserHistoryExaminer.**

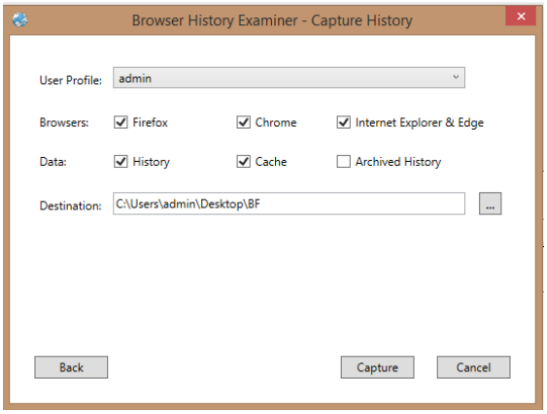
2. Click on file > Capture History



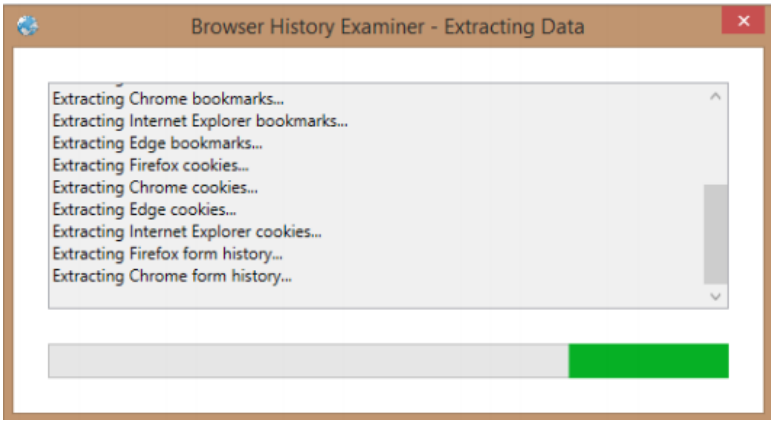
3. **Select the capture folder and click on next.**



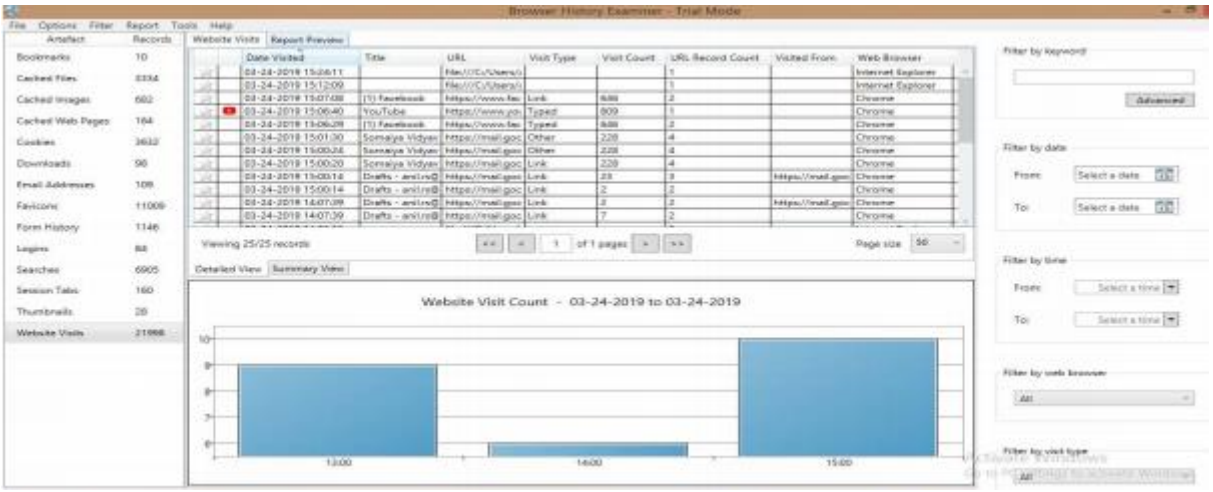
4. **Enter the destination to capture the data.**



5. **The History is been extracting.**

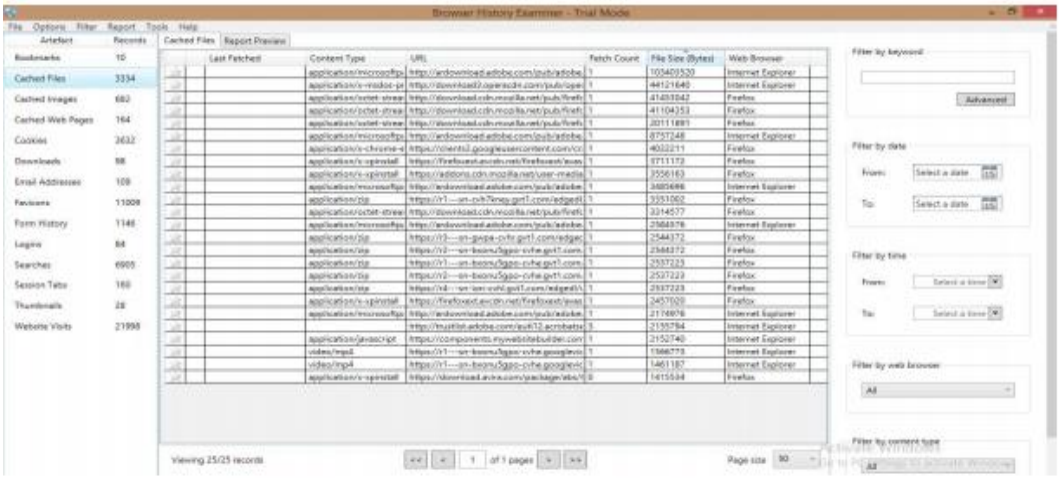


6. **The data has been retrieved.**

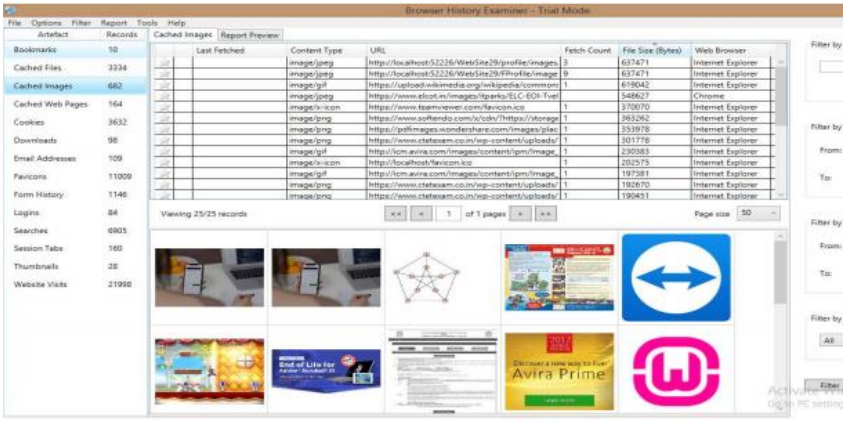


7. **On the left panel click on bookmarks.**

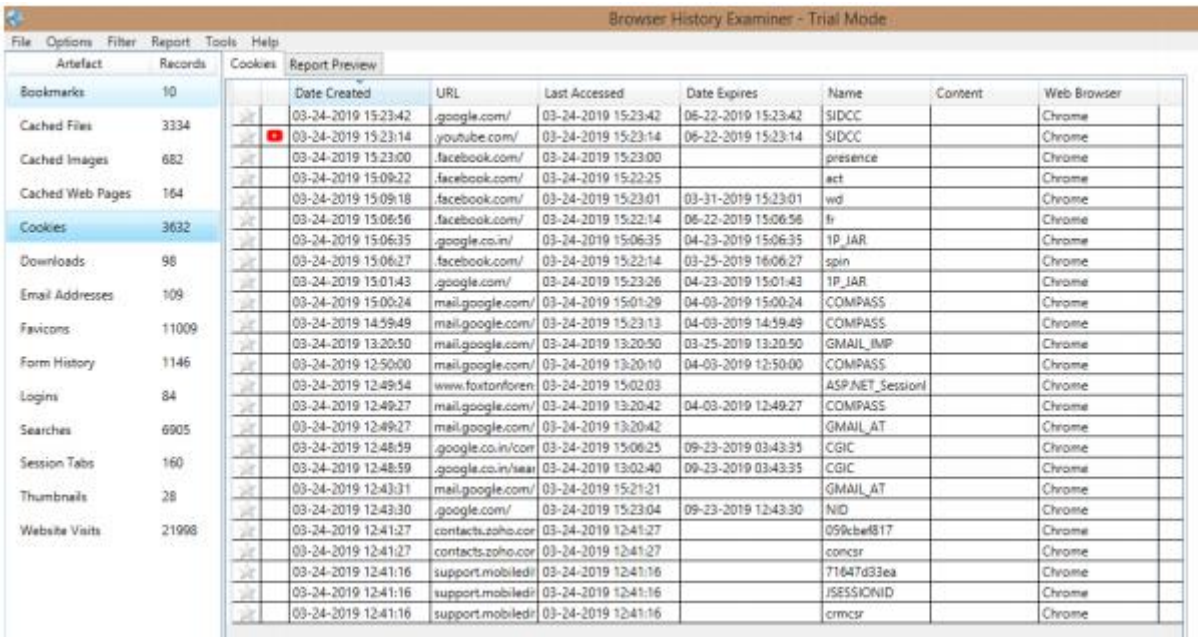
8. **On the left panel click on cached files**



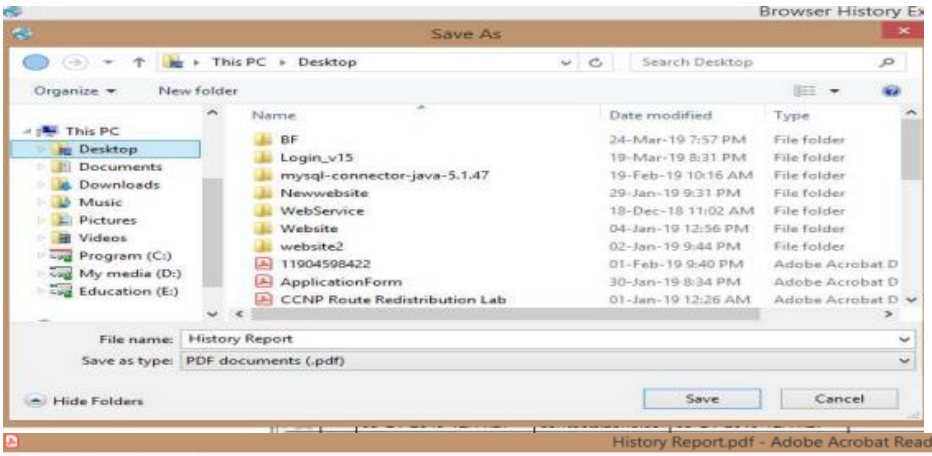
9. On the left panel click on cached images.

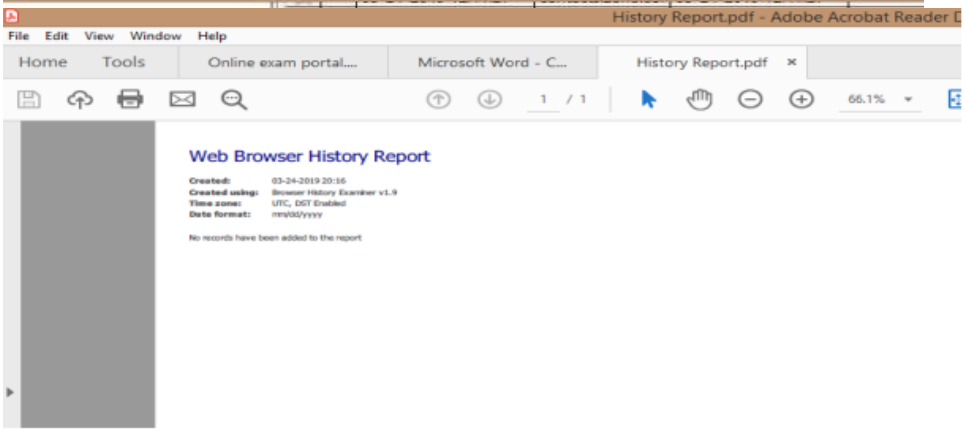


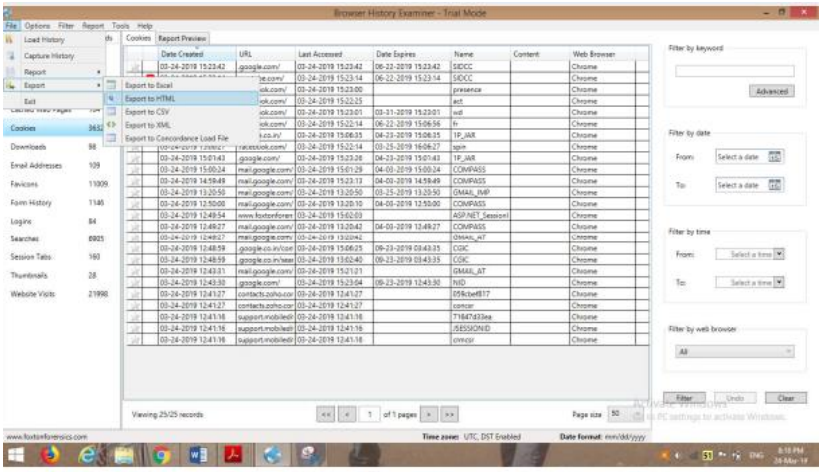
10. On the left panel click on cookies.



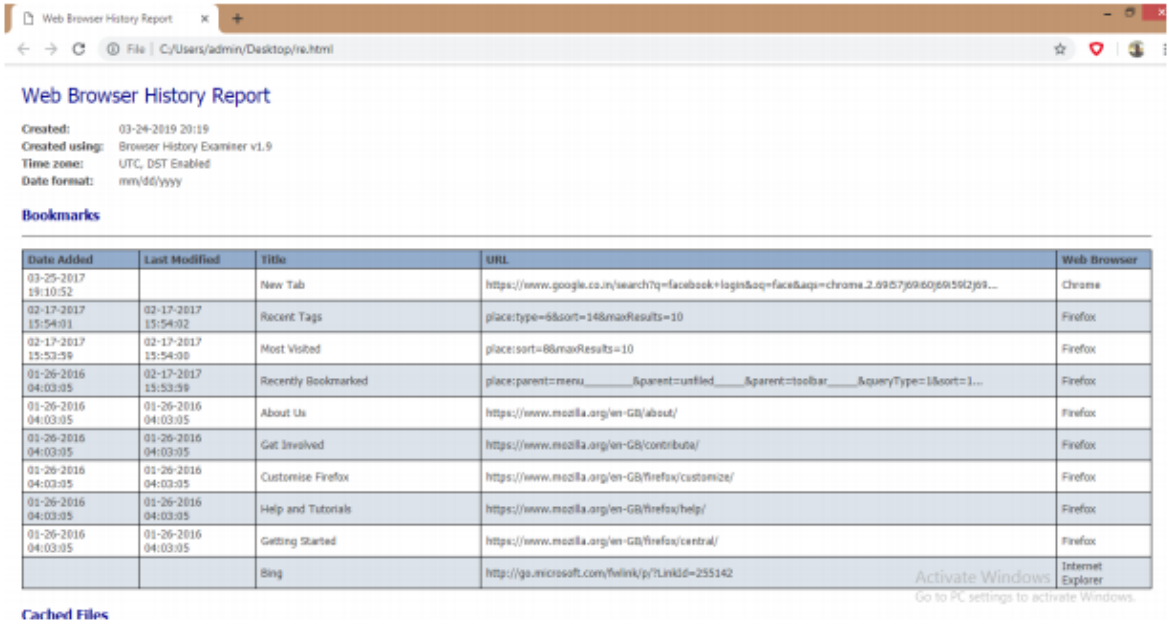
11.To Create Reports. Click on file > Report and save the report as pdf or html page.







Html file



Date Added	Last Modified	Title	URL	Web Browser
03-25-2017 19:10:52		New Tab	https://www.google.co.in/search?q=facebook+login&aq=face&aqs=chrome.2.69i57j69i60j69i59j0j69...	Chrome
02-17-2017 15:54:01	02-17-2017 15:54:02	Recent Tags	place:type=6&sort=14&maxResults=10	Firefox
02-17-2017 15:53:59	02-17-2017 15:54:00	Most Visited	place:sort=8&maxResults=10	Firefox
01-26-2016 04:03:05	02-17-2017 15:53:59	Recently Bookmarked	place:parent=menu_____&parent=unfiled_____&parent=toolbar_____&queryType=1&sort=1...	Firefox
01-26-2016 04:03:05	01-26-2016 04:03:05	About Us	https://www.mozilla.org/en-GB/about/	Firefox
01-26-2016 04:03:05	01-26-2016 04:03:05	Get Involved	https://www.mozilla.org/en-GB/contribute/	Firefox
01-26-2016 04:03:05	01-26-2016 04:03:05	Customise Firefox	https://www.mozilla.org/en-GB/firefox/customize/	Firefox
01-26-2016 04:03:05	01-26-2016 04:03:05	Help and Tutorials	https://www.mozilla.org/en-GB/firefox/help/	Firefox
01-26-2016 04:03:05	01-26-2016 04:03:05	Getting Started	https://www.mozilla.org/en-GB/firefox/central/	Firefox
		Bing	http://go.microsoft.com/fwlink/p/?LinkId=255142	Internet Explorer