

Practical No – 1

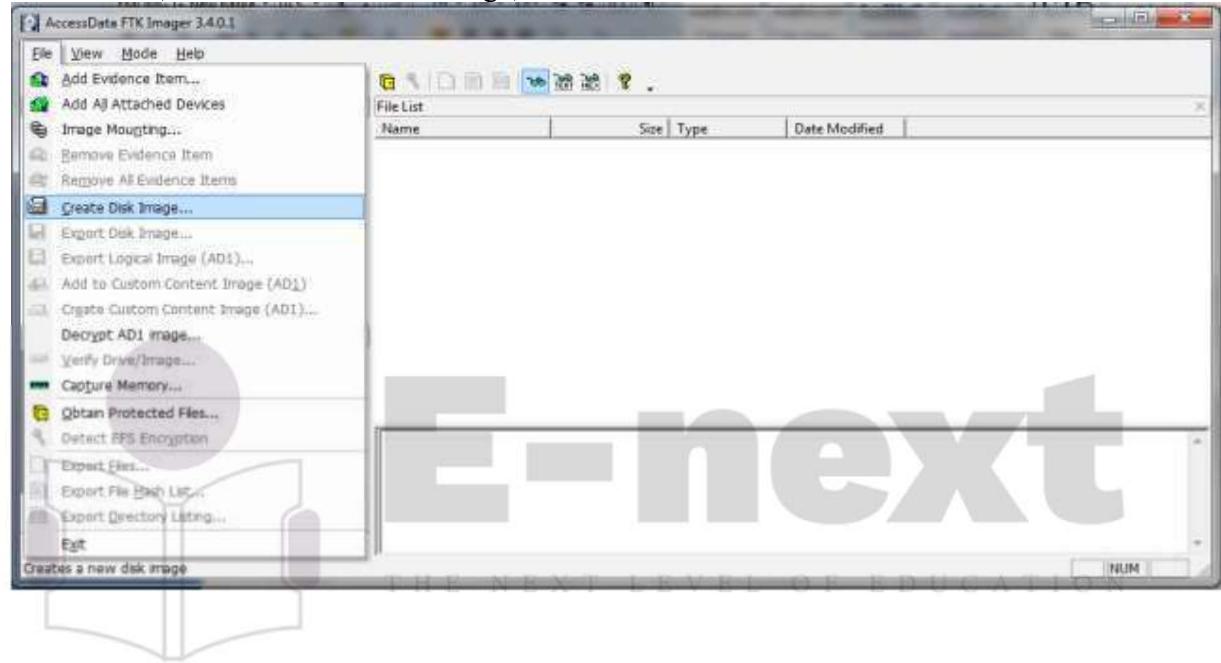
Aim: Creating a Forensic Image using FTK Imager/Encase Imager:

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

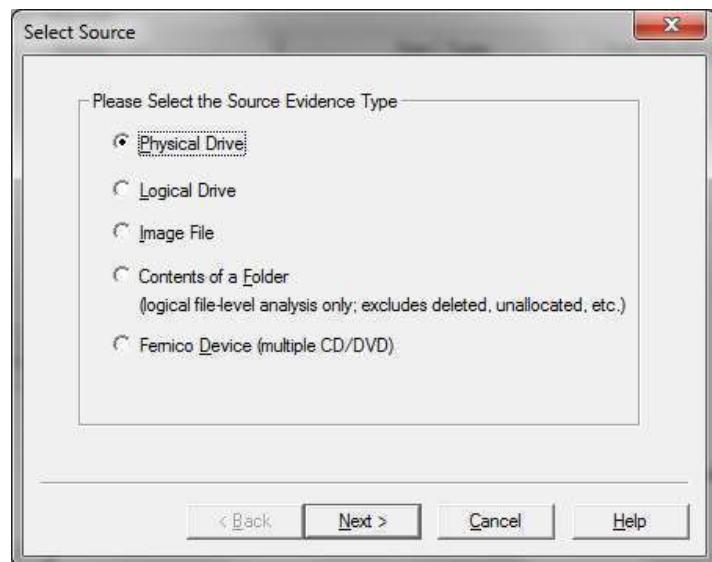
Steps:

Creating Forensic Image

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

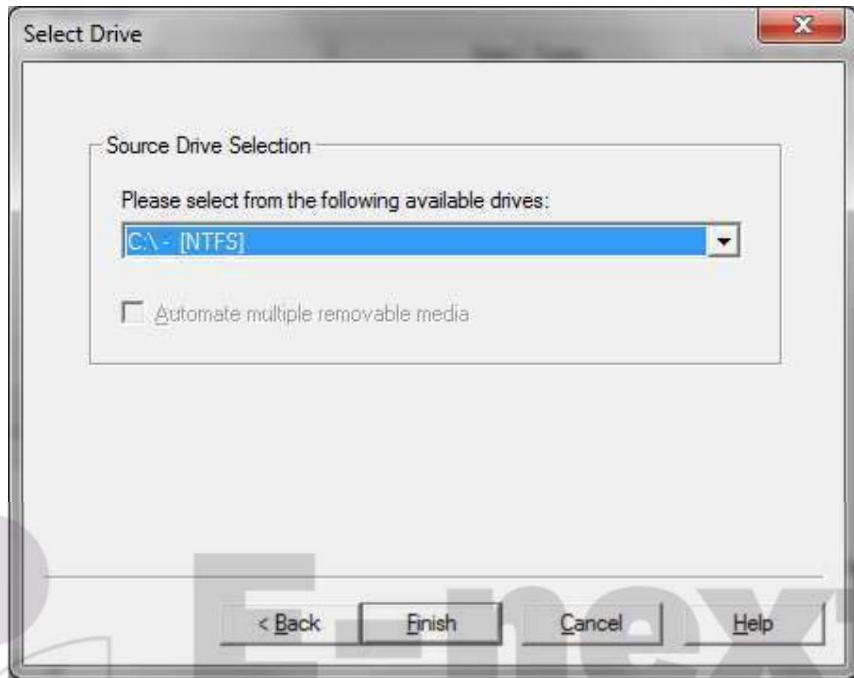


2. Select the source you want to make an image of and click Next.

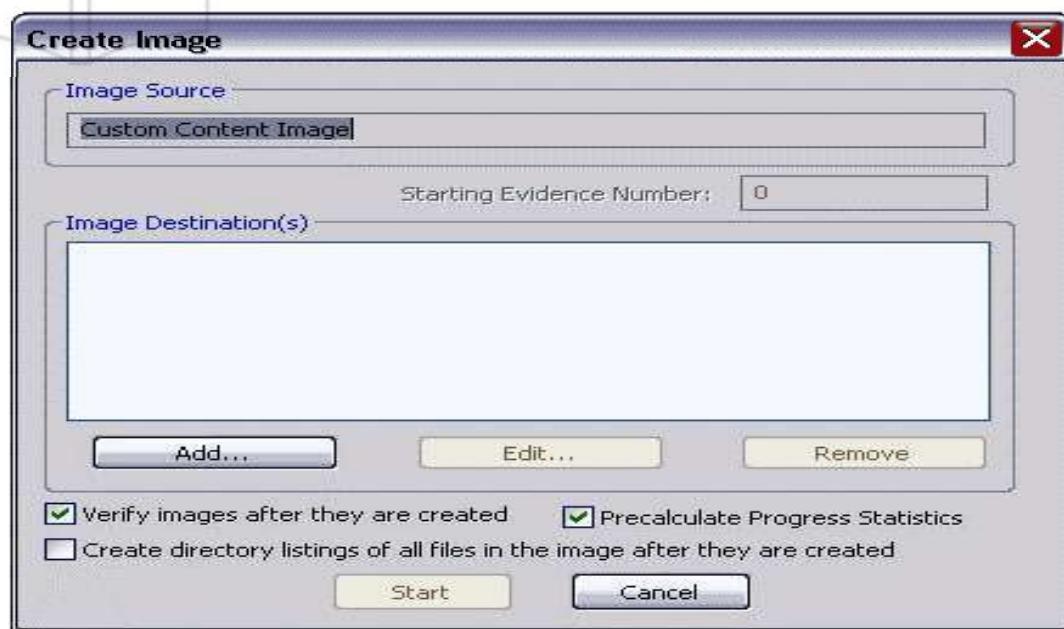


If you select Logical Drive to select a floppy or CD as a source, you can check the Automate multiple removable media box to create groups of images. Imager will automatically increment the case numbers with each image, and if something interrupts the process, you may assign case number manually.

3. Select the drive or browse to the source of the image you want, and then click Finish.



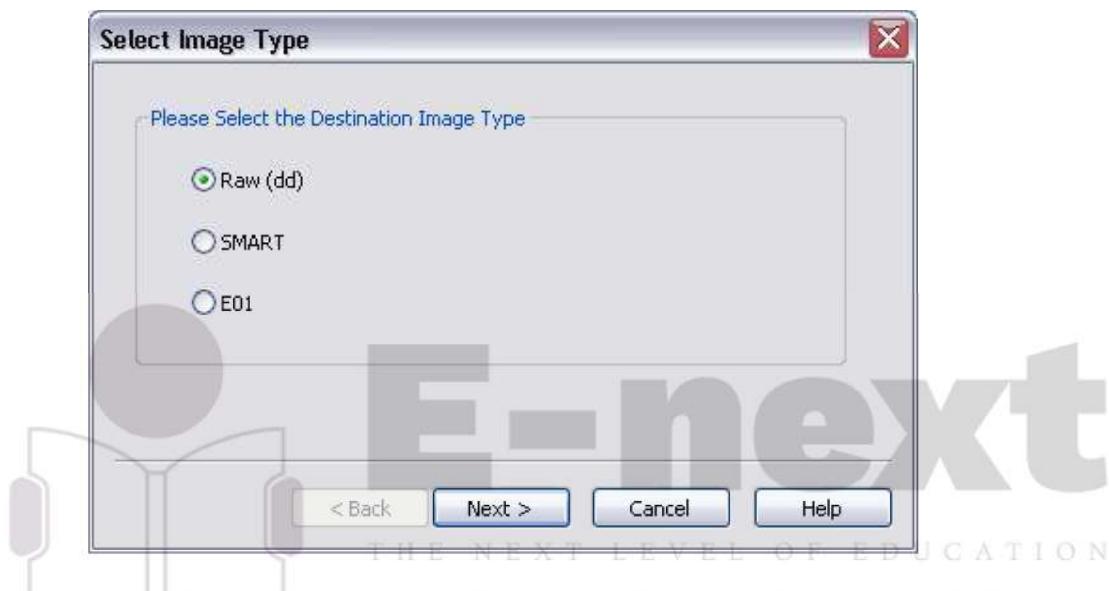
4. In the Create Image dialog, click Add.



- You can compare the stored hashes of your image content by checking the Verify images after they are created box. If a file doesn't have a hash, this option will generate one.
- You can list the entire contents of your images with path, creation dates, whether files were deleted, and other metadata. The list is saved in a tab-separated value format

5. Select the type of image you want to create, and then click Next.

Note: If you are creating an image of a CD or DVD, this step is skipped because all CD/DVD images are created in the IsoBuster CUE format.



The raw image type is not compressed. If you select the Raw (dd) type, be sure to have adequate space for the resulting image.

If you select SMART or E01 as the image type, complete the fields in the Evidence Item Information dialog, and click **Next**.

Raw (dd): This is the image format most commonly used by modern analysis tools. These raw file formatted images do not contain headers, metadata, or magic values. The raw format typically includes padding for any memory ranges that were intentionally skipped (i.e., device memory) or that could not be read by the acquisition tool, which helps maintain spatial integrity (relative offsets among data).

SMART: This file format is designed for Linux file systems. This format keeps the disk images as pure bitstreams with optional compression. The file consists of a standard 13-byte header followed by a series of sections. Each section includes its type string, a 64-bit offset to the next section, its 64-bit size, padding, and a CRC, in addition to actual data or comments, if applicable.

E01: this format is a proprietary format developed by Guidance Software's EnCase. This format compresses the image file. An image with this format starts with case information in the header and footer, which contains an MD5 hash of the entire bit stream. This case information contains the date and time of acquisition, examiner's name, special notes and an optional password.

AFF: Advance Forensic Format (AFF) was developed by Simson Garfinkel and Basis Technology. Its latest implementation is AFF4. The goal is to create a disk image format that

does not lock the user into a proprietary format that may prevent them from being able to properly analyze it.

6. 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.

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

8. In the Image Fragment Size field, specify the maximum size in MB for each fragment of the image file. The s01 format is limited by design to sizes between 1 MB and 2047 MB (2 GB). Compressed block pointers are 31-bit numbers (the high bit is a compressed flag), which limits the size of any one segment to two gigabytes.

Tip: If you want to transfer the image file to CD, accept the default fragment size of 650 MB.

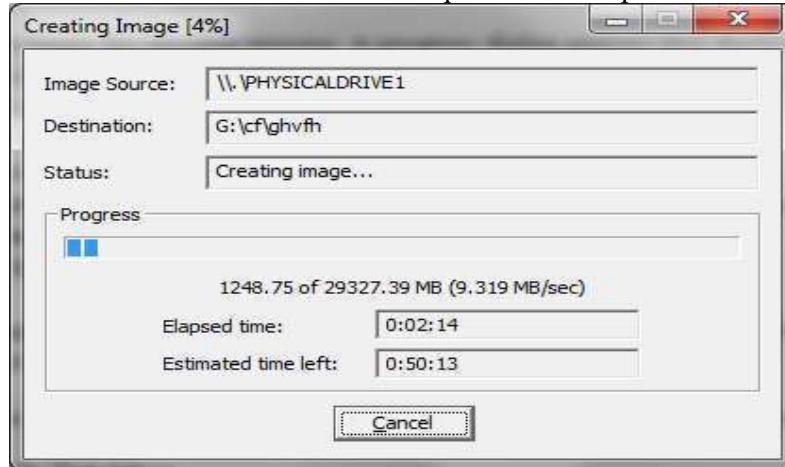
9. Click **Finish**. You return to the Create Image dialog.

10. To add another image destination (i.e., a different saved location or image file type), click **Add**, and repeat steps 5– 10. To make changes to an image destination, select the destination you want to change and click **Edit**.

To delete an image destination, select the destination and click **Remove**.

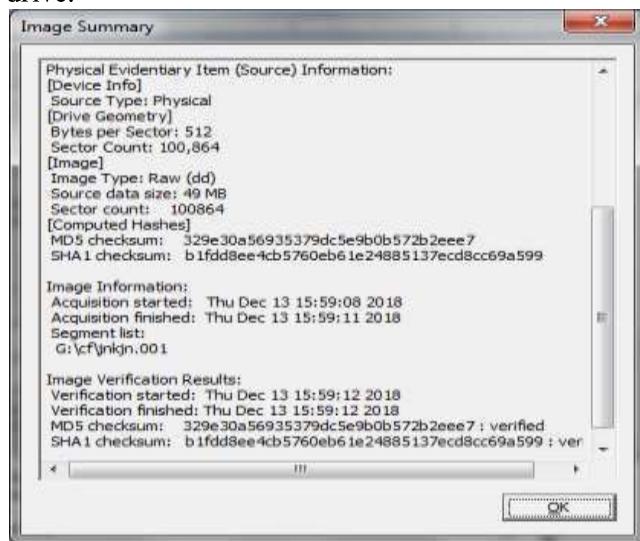
11. Click **Start** to begin the imaging process. A progress dialog appears that shows the following:

- The source that is being imaged
- The location where the image is being saved
- The status of the imaging process
- A graphical progress bar
- The amount of data in MB that has been copied and the total amount to be copied
- Elapsed time after the imaging process began
- Estimated time left until the process is complete



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

Note: This option is available only if you created an image file of a physical or logical drive.



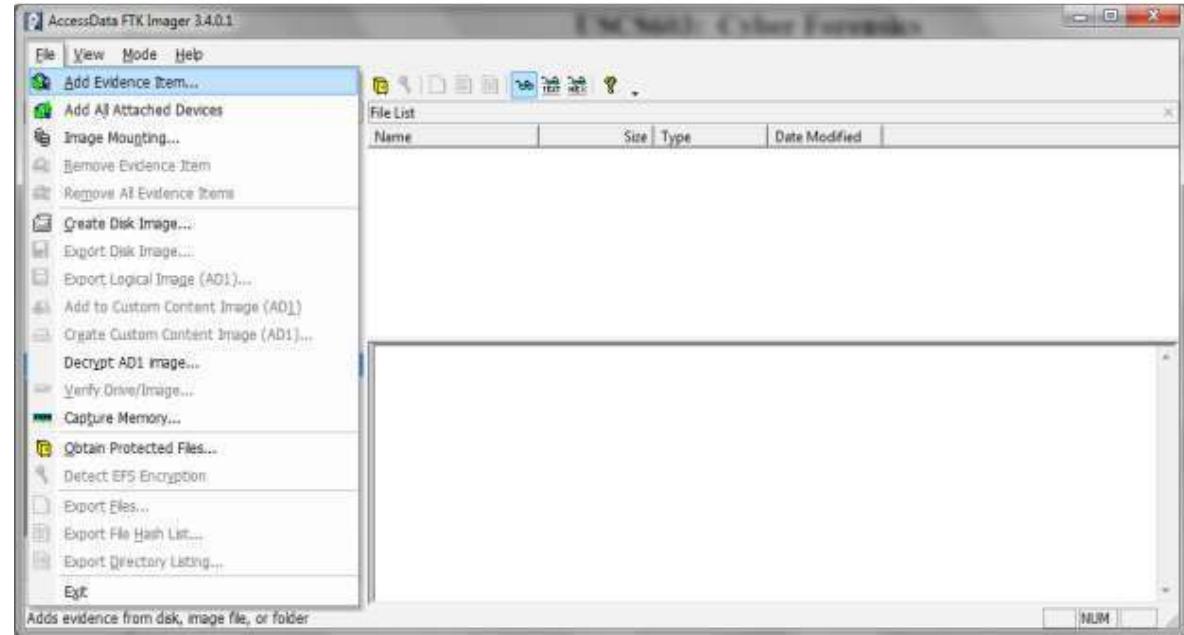
13. When finished, click **Close**

Note that the image file (*.001) as well as the image summary file from above (*.txt) have been saved onto the 'Drive'. The .001 extension may be left as is, or can be changed to .dd. The .001 extension is used due to the fact that many times the file to be imaged is very large and must be split into multiple chunks. In that case, you would have *.001, *.002, etc.

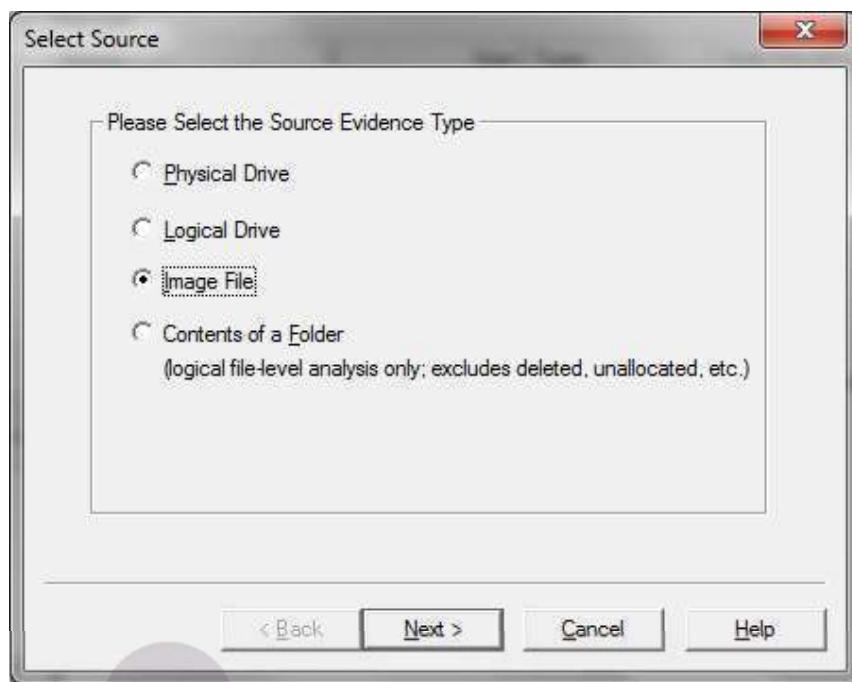
Analyze Forensic Image:

THE NEXT LEVEL OF EDUCATION

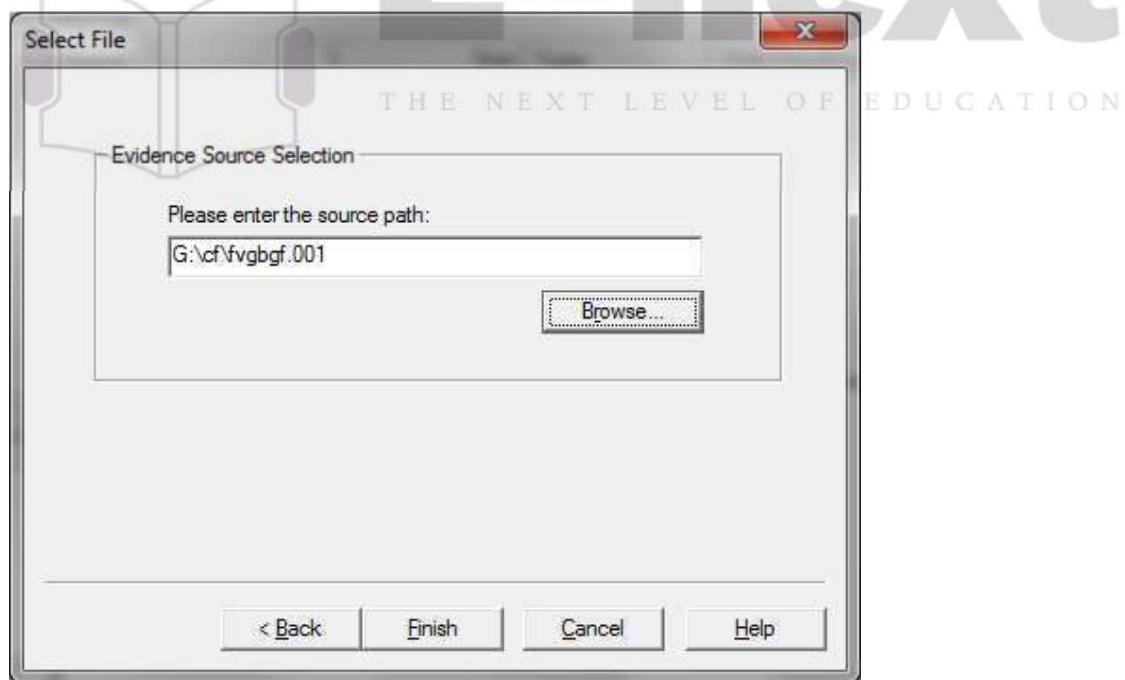
Click on Add Evidence Item to add evidence from disk, image file or folder.



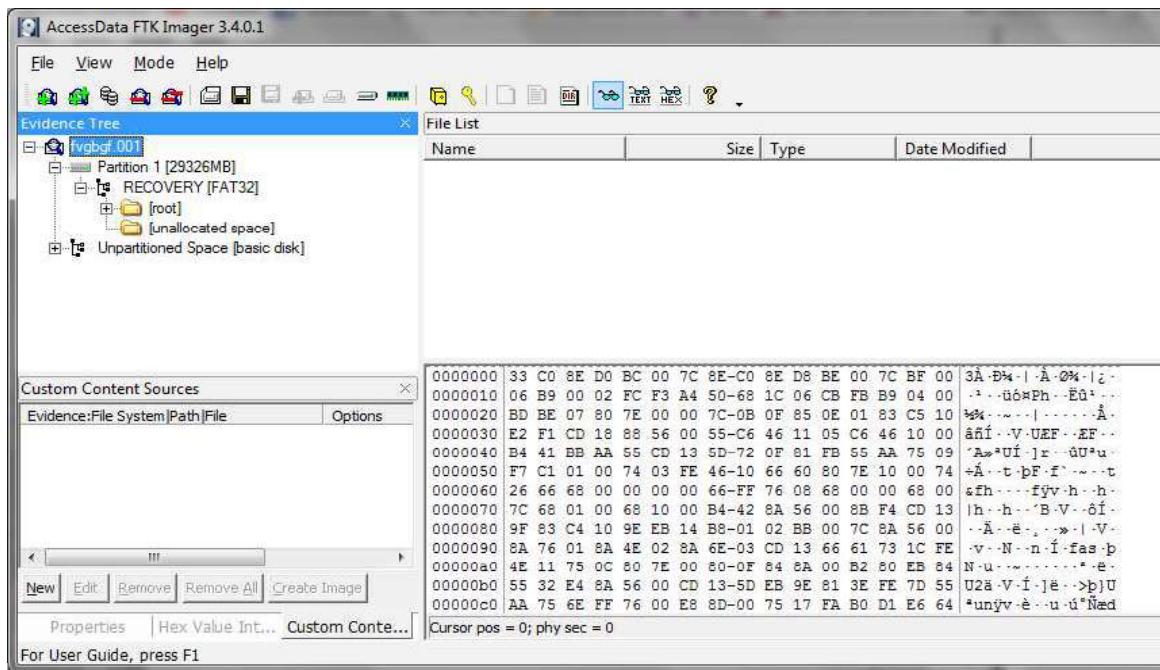
Now select the source evidence type as physical drive, logical drive or image file. We have selected image file and click on next.



Select virtual drive image & click on open option. Select the source path and click on finish.



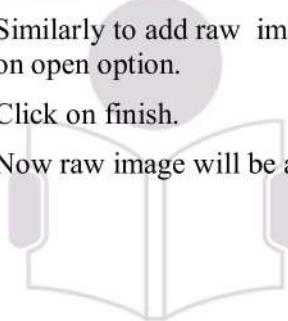
Now select Evidence Tree and analyze the virtual disk as physical disk.



Similarly to add raw image select again add evidence item and click on image file and click on open option.

Click on finish.

Now raw image will be added as physical drive to analyze.



Practical No – 2

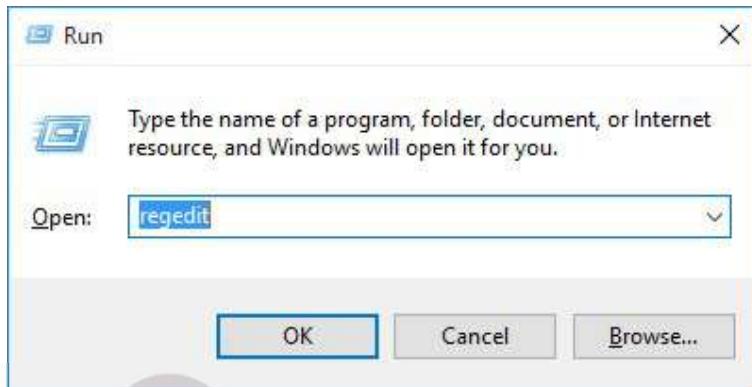
Aim: Data Acquisition:

- 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.

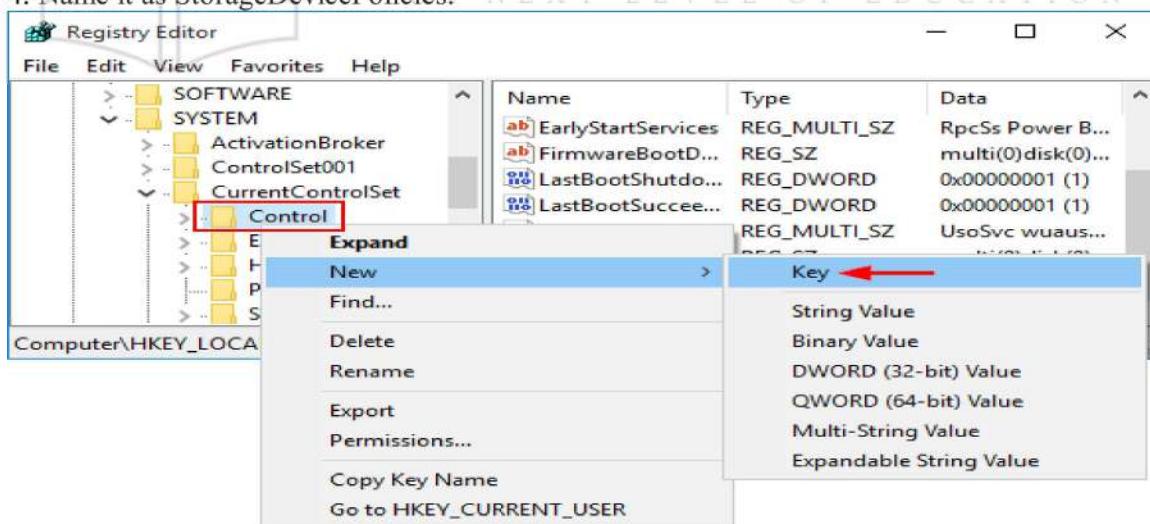


2. This will open the Registry Editor. Navigate to the following key:

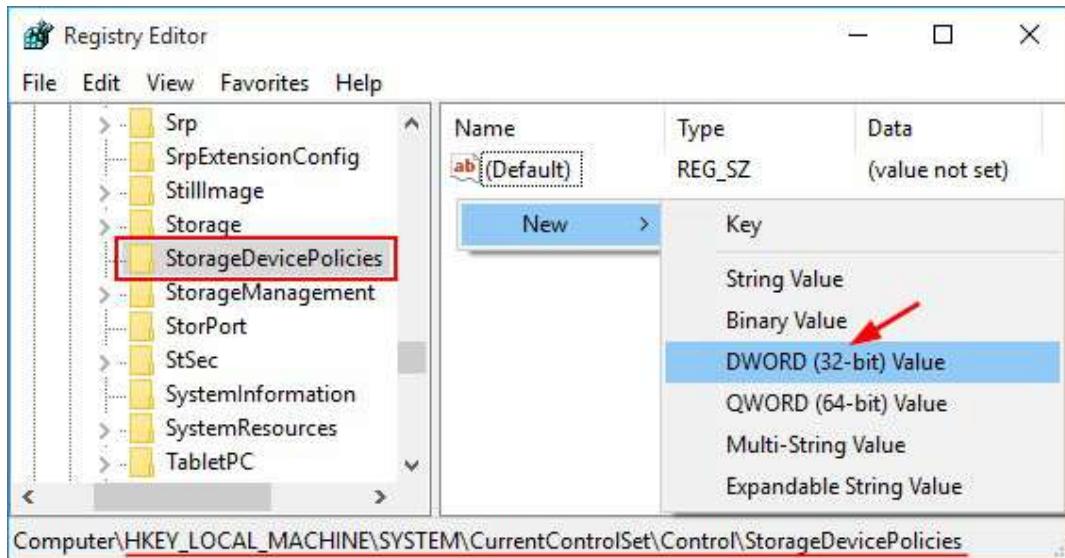
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control

3. Right-click on the Control key in the left pane, select New -> Key.

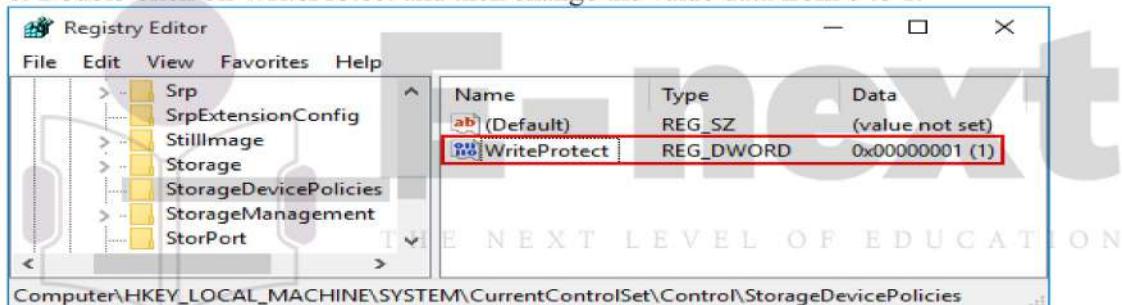
4. Name it as StorageDevicePolicies.



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.

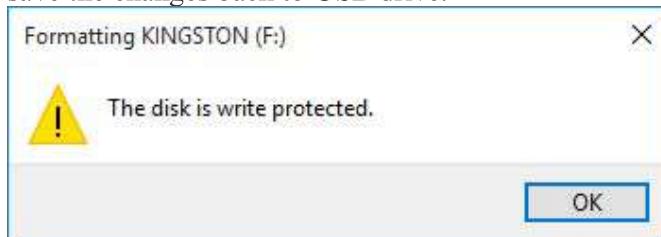


6. Double-click on WriteProtect and then change the value data from 0 to 1.



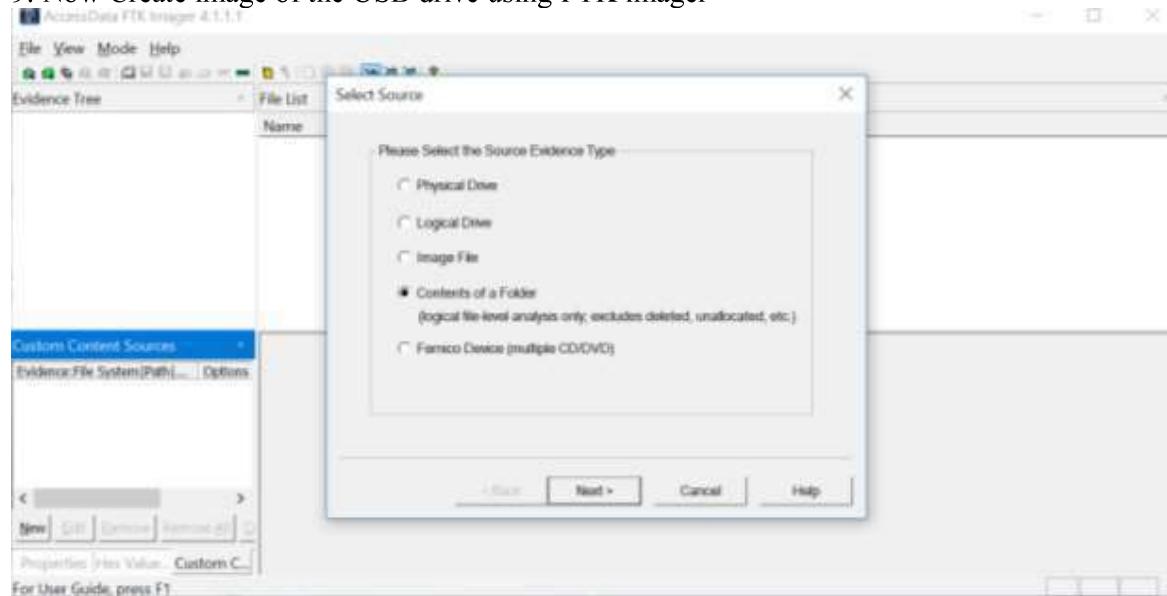
7. The new setting takes effect immediately. Every user who tries to copy / move data to USB devices or format USB drive will get the error message
“*The disk is write-protected*”.

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.



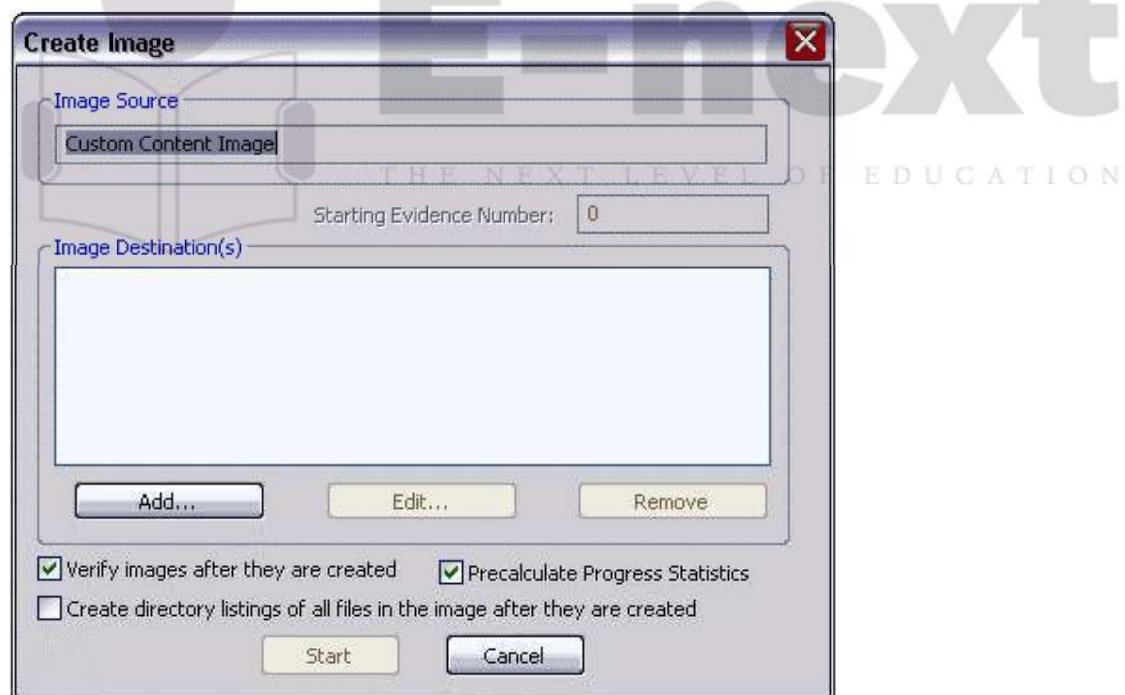
So this is how you can enable write protection to all connected USB drives. If you want to disable write protection at a later time, just open Registry Editor and set the WriteProtect value to 0.

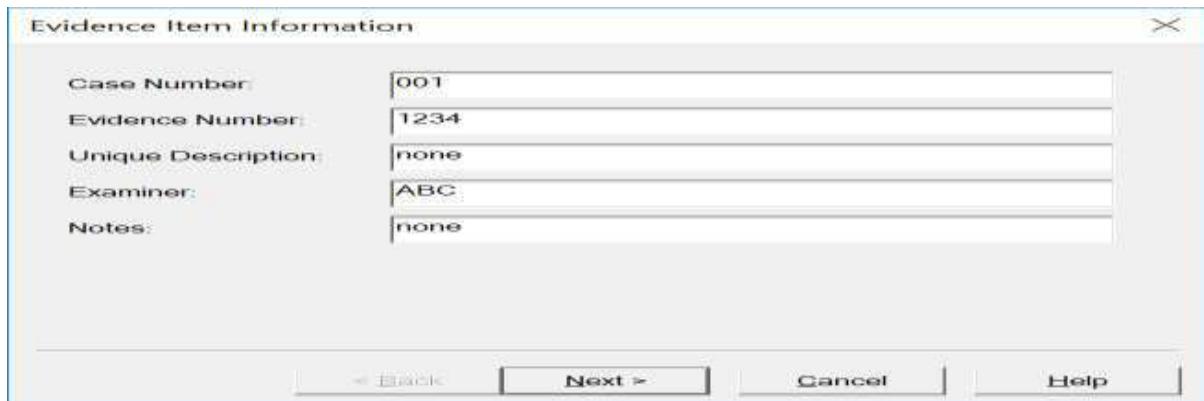
9. Now Create image of the USB drive using FTK imager



10. Select the USB drive folder by browsing and click next & Finish

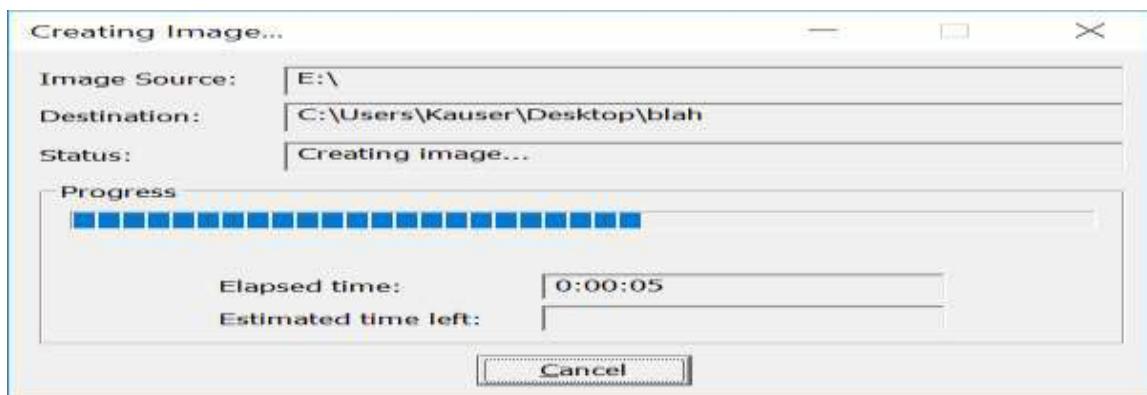
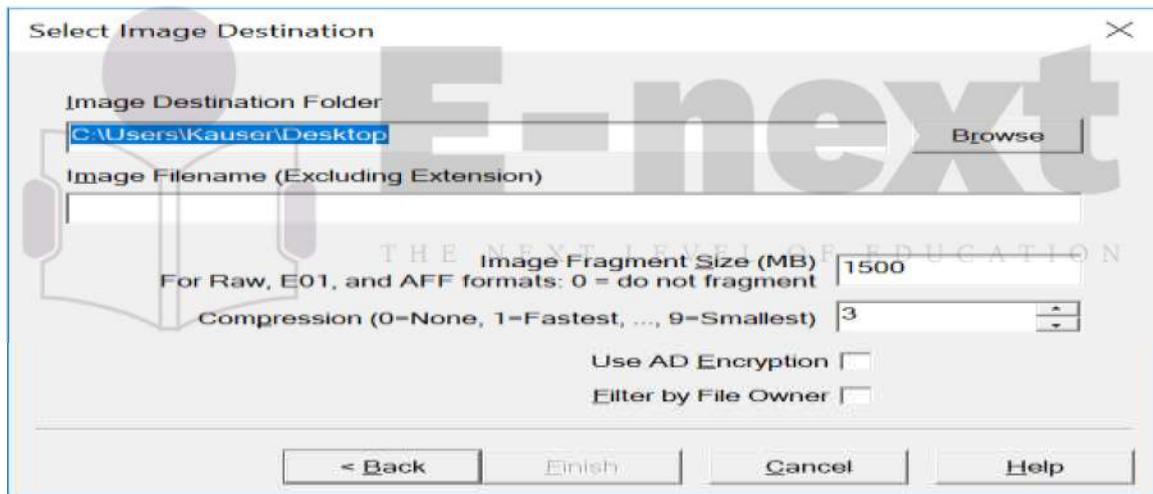
11. In the Create Image dialog, click Add.





- You can compare the stored hashes of your image content by checking the Verify images after they are created box. If a file doesn't have a hash, this option will generate one.
- You can list the entire contents of your images with path, creation dates, whether files were deleted, and other metadata. The list is saved in a tab-separated value format

Select the type of image you want to create, and then click Next



Practical No – 3

Aim: Forensics Case Study:

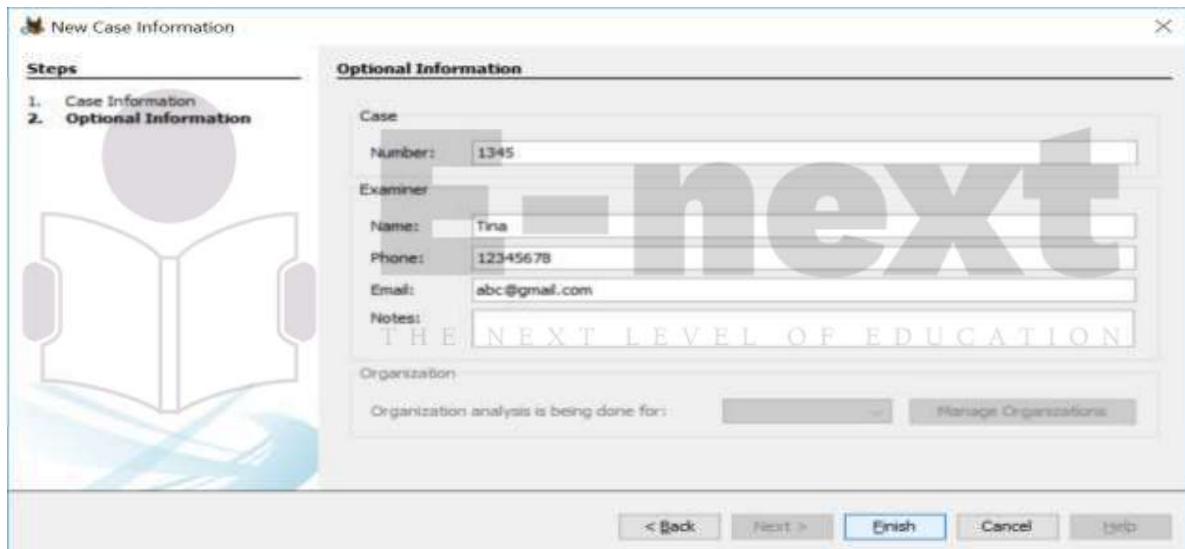
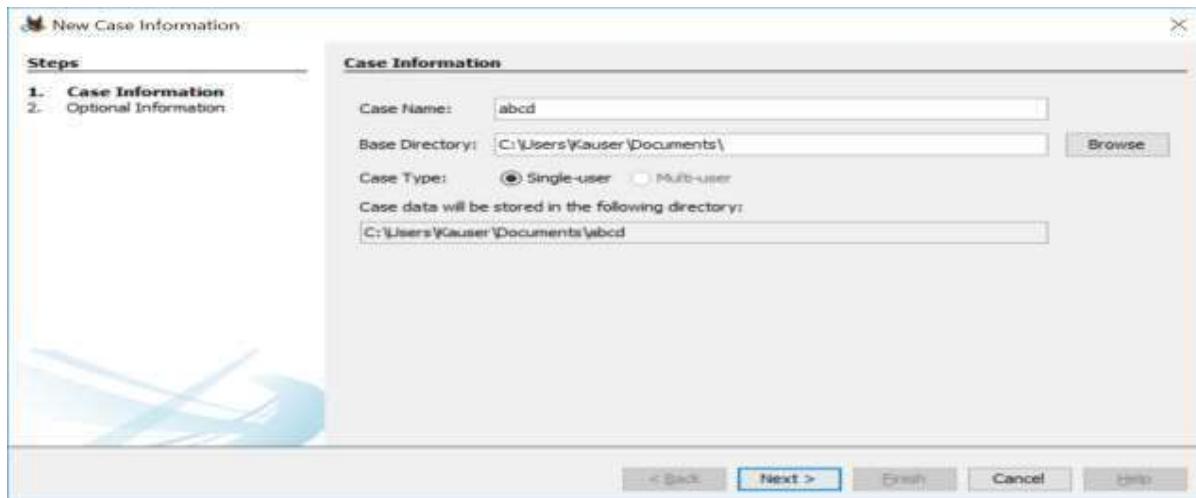
- Solve the Case study (image file) provide in lab using Autopsy

Steps:

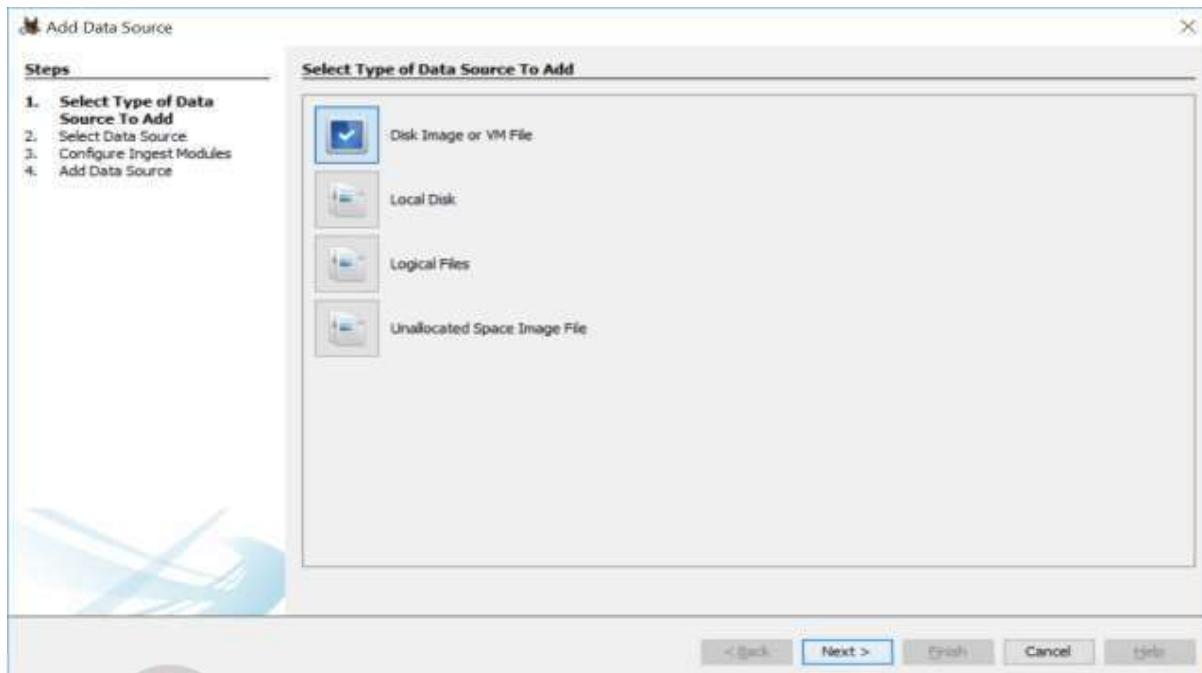
1. Start Autopsy



3. Enter Case Information and Base Directory & click on finish

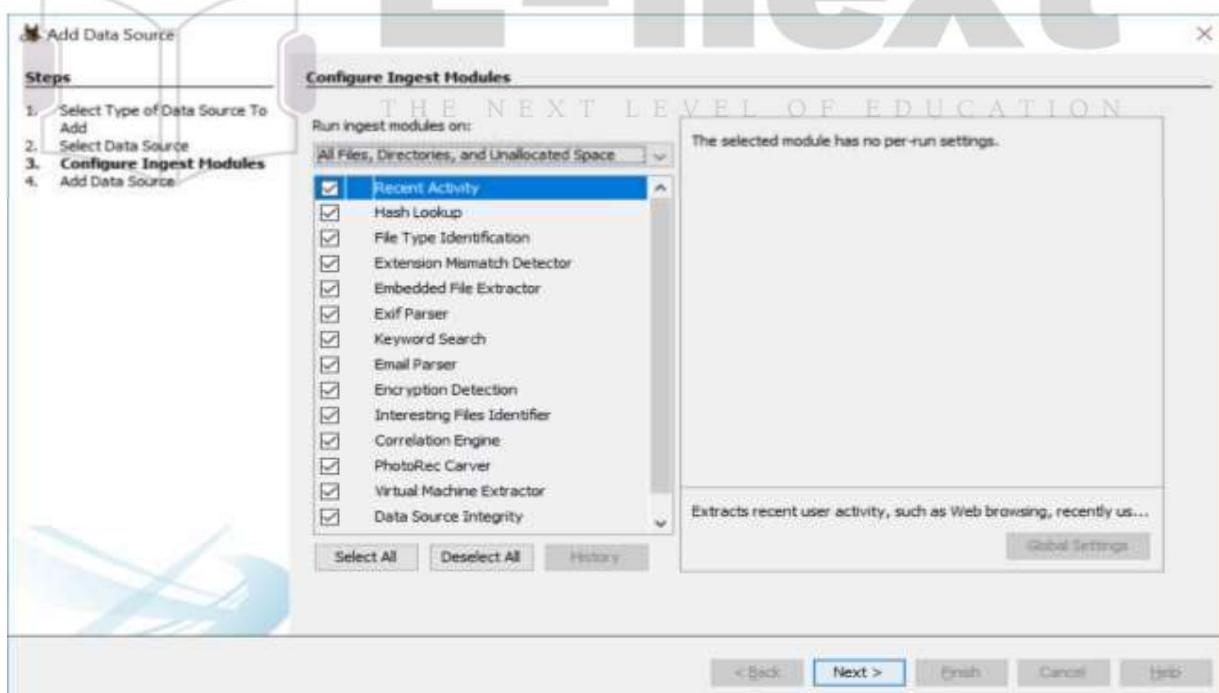


4. Select the type of Data Source that has to be added

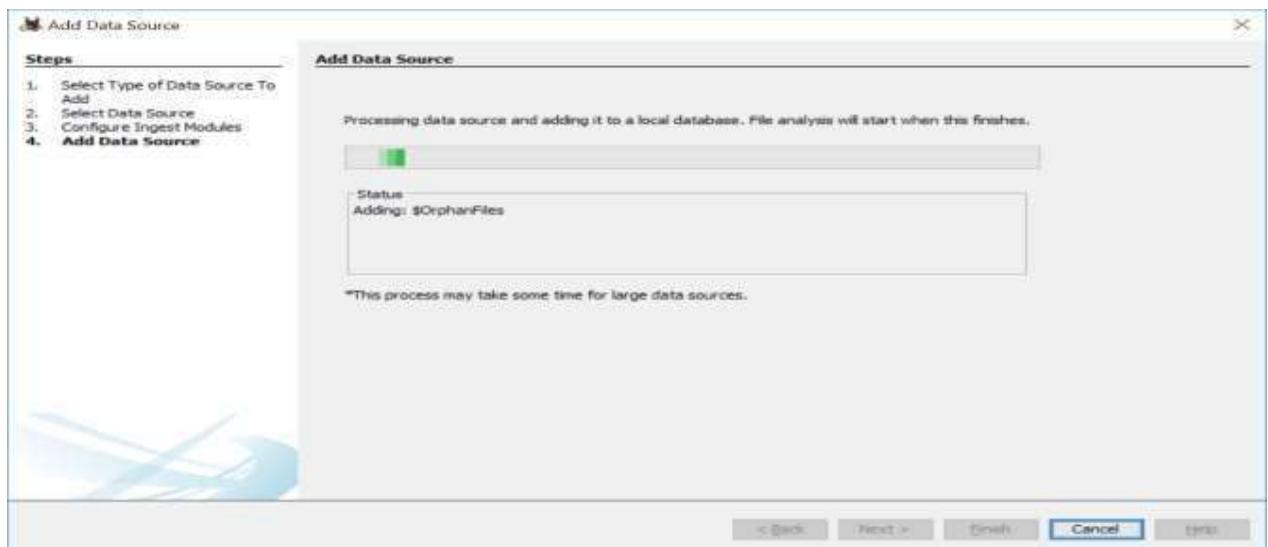


5. Select Data Source(here a previously made image file of a USB is selected)

6. Select all ingest modules



7. Wait for Data source to process and be added to local database. Click Finish



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



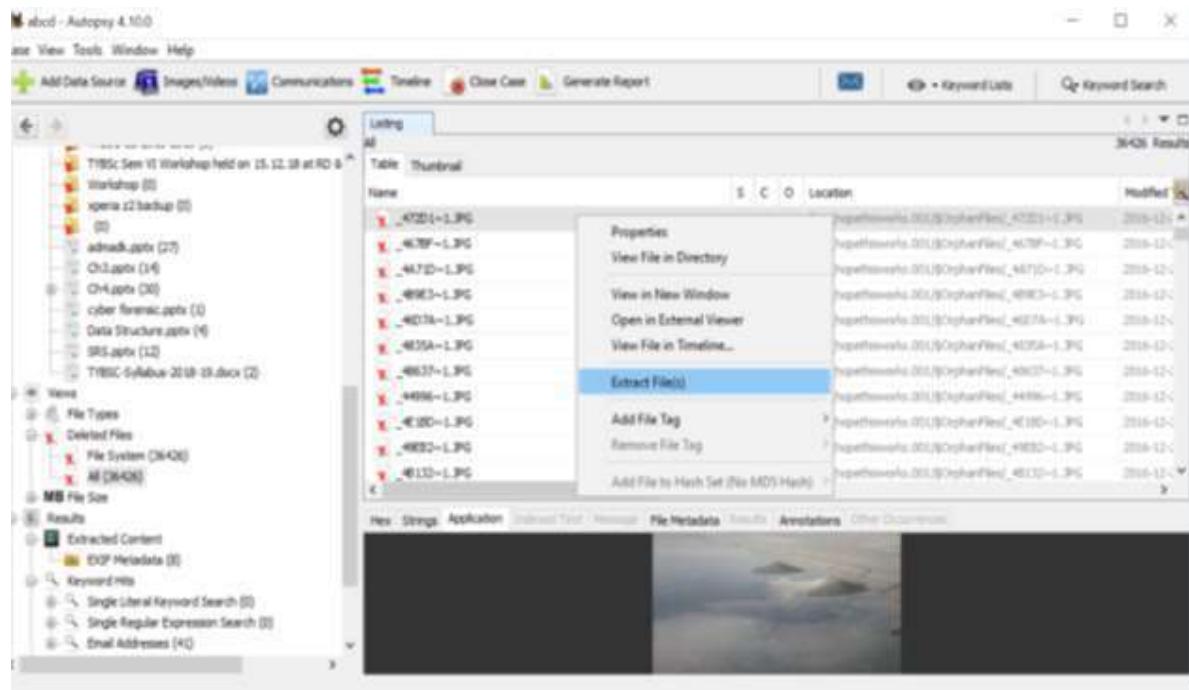
9. All files will appear in table tab select any file to see the data.

Name	S	C	O	Location	Modified Time
OrphanFiles				/img_hoopheworks.001//OrphanFiles	0000-00-00 00:00:00
IFAT1					0000-00-00 00:00:00
IFAT2					0000-00-00 00:00:00
ISBL					0000-00-00 00:00:00
Jhaloc				/img_hoopheworks.001//Jhaloc	2019-02-14 21:42:44 EST
_images					2019-01-15 17:04:14 EST
_ogg					2019-01-15 17:04:14 EST
_OST.DIR					2019-01-15 17:04:14 EST
Algo					2019-01-15 17:04:14 EST
Android					2019-01-15 17:04:14 EST
Bird.Box. 2018. WEBrip.x264-FGT					2019-01-15 17:04:14 EST
cyber					2019-01-15 17:04:14 EST
0396e9D-2e00-4b8e-880a-254239bc12E1					2019-01-15 17:04:14 EST
Data Structure					2019-01-15 17:04:14 EST
filestructure					2019-01-15 17:04:14 EST
logo print					2019-01-15 17:04:14 EST
New folder					2019-01-15 17:04:14 EST
Sem II					2019-01-15 17:04:14 EST
System Volume Information					2019-01-15 17:04:14 EST
TYBSC CS 2018-2019					2019-01-15 17:04:14 EST
TYBSC Sem VI Workshop held on 15.12.18 at RD S					2019-01-15 17:04:14 EST
Workshop					2019-01-15 17:04:14 EST
xpene x2 backup					2019-01-15 17:04:14 EST
(0)					2019-01-15 17:04:14 EST
adnadi.pptx					2019-01-15 17:04:14 EST
Ch3.pptx					2019-01-15 17:04:14 EST

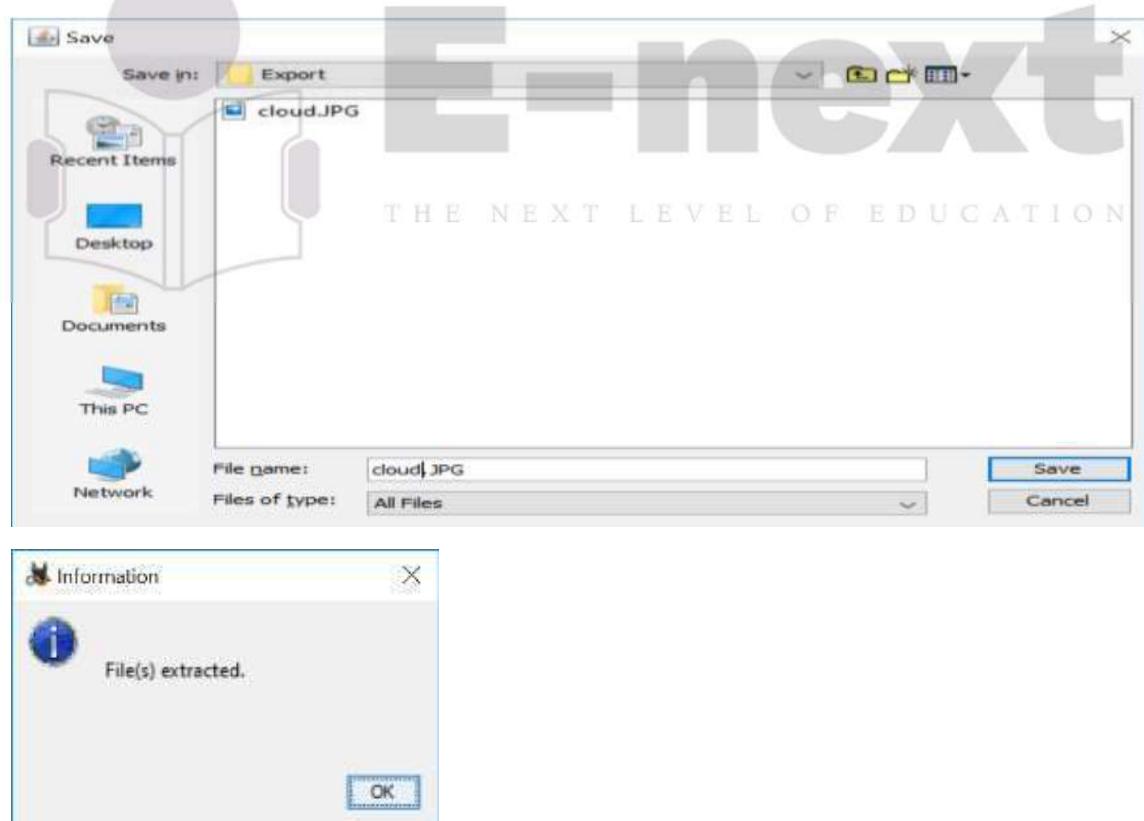
10. Expand the tree from left side panel to view the files and then expand the deleted files node

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.

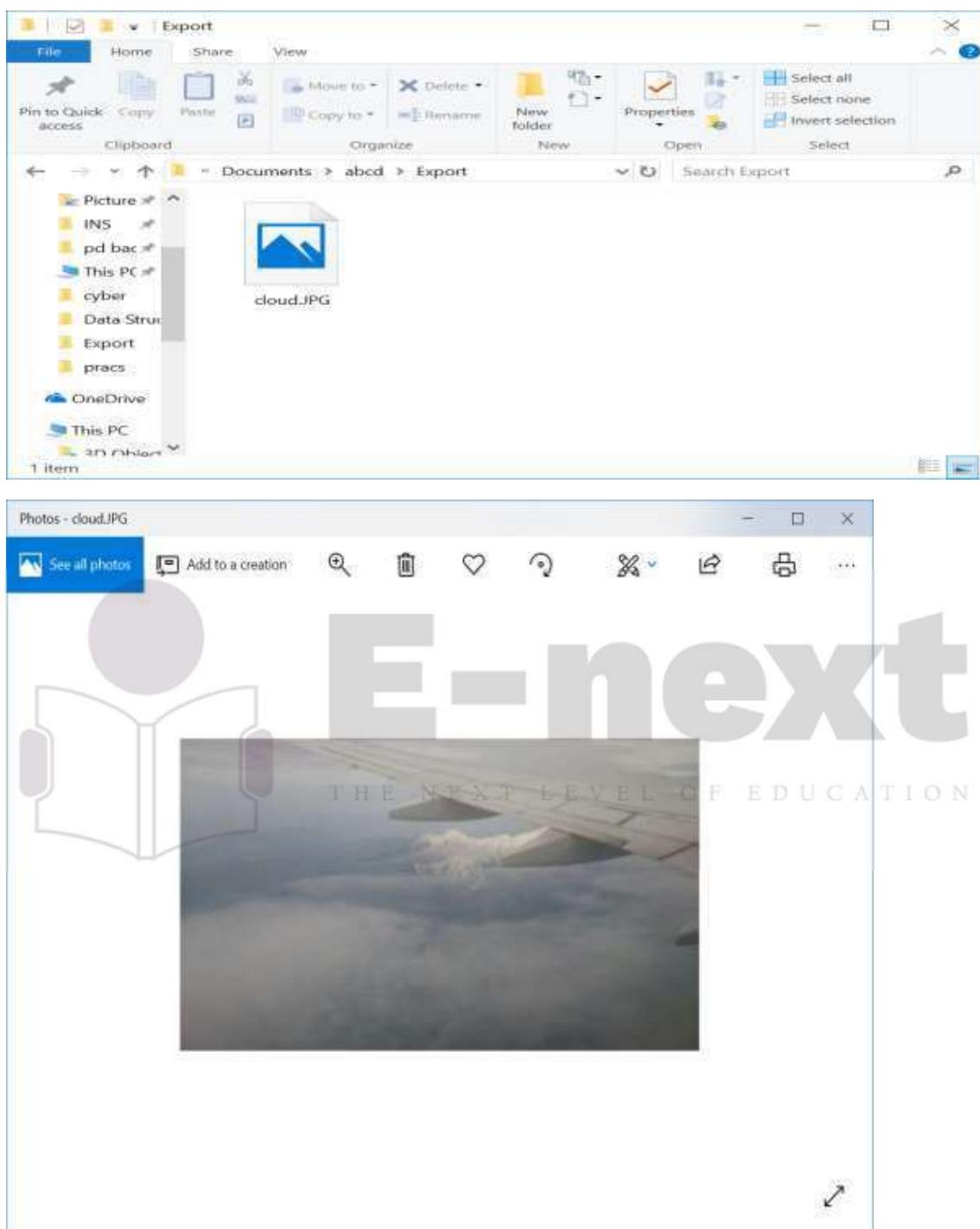
Name	S	C	O	Location	Modified
472D1~L.JPG				/img_hoopheworks.001//OrphanFiles/472D1~L.JPG	2019-12-~
467B~L.JPG				/img_hoopheworks.001//OrphanFiles/467B~L.JPG	2019-12-~
4A71D~L.JPG				/img_hoopheworks.001//OrphanFiles/4A71D~L.JPG	2019-12-~
4B1E5~L.JPG				/img_hoopheworks.001//OrphanFiles/4B1E5~L.JPG	2019-12-~
4B07A~L.JPG				/img_hoopheworks.001//OrphanFiles/4B07A~L.JPG	2019-12-~
4B35A~L.JPG				/img_hoopheworks.001//OrphanFiles/4B35A~L.JPG	2019-12-~
4B637~L.JPG				/img_hoopheworks.001//OrphanFiles/4B637~L.JPG	2019-12-~
44996~L.JPG				/img_hoopheworks.001//OrphanFiles/44996~L.JPG	2019-12-~
4E1BD~L.JPG				/img_hoopheworks.001//OrphanFiles/4E1BD~L.JPG	2019-12-~
49EB2~L.JPG				/img_hoopheworks.001//OrphanFiles/49EB2~L.JPG	2019-12-~
4B132~L.JPG				/img_hoopheworks.001//OrphanFiles/4B132~L.JPG	2019-12-~



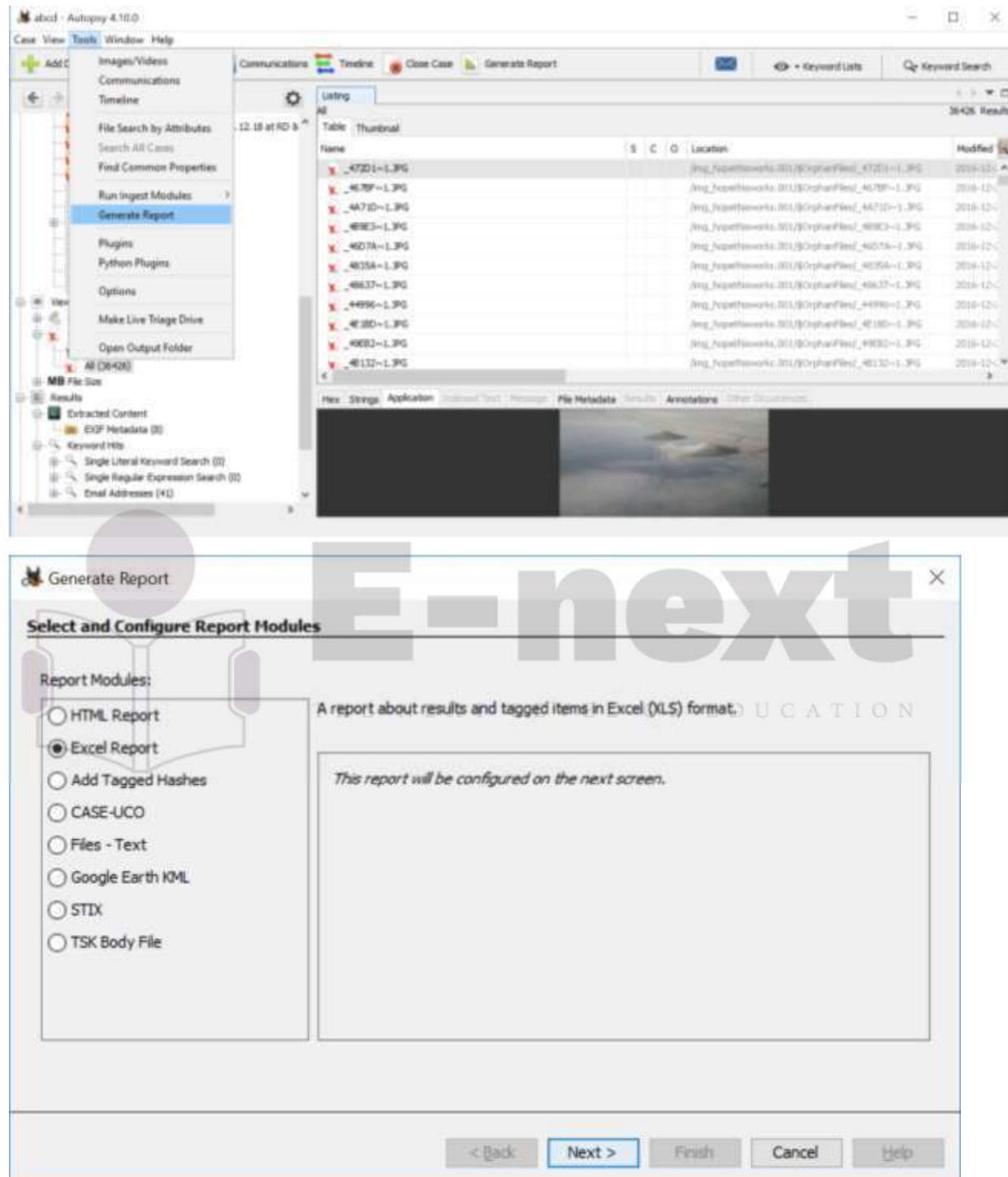
12. By default Export folder is choose to save the recovered file.



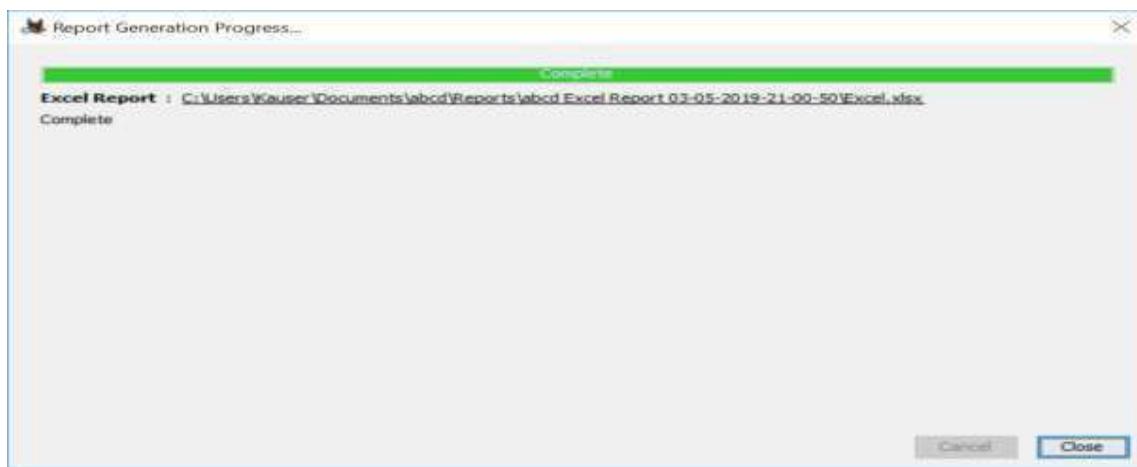
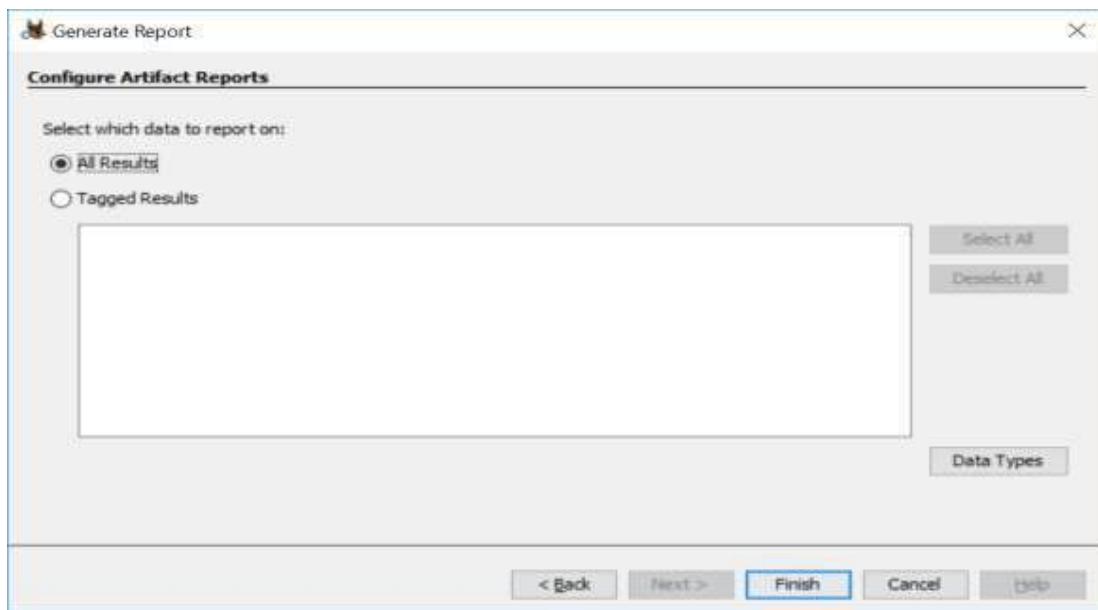
13. Now go to the Export Folder to view Recover file.



14. Click on Generate Report from autopsy window and Select the Excel format and click on next

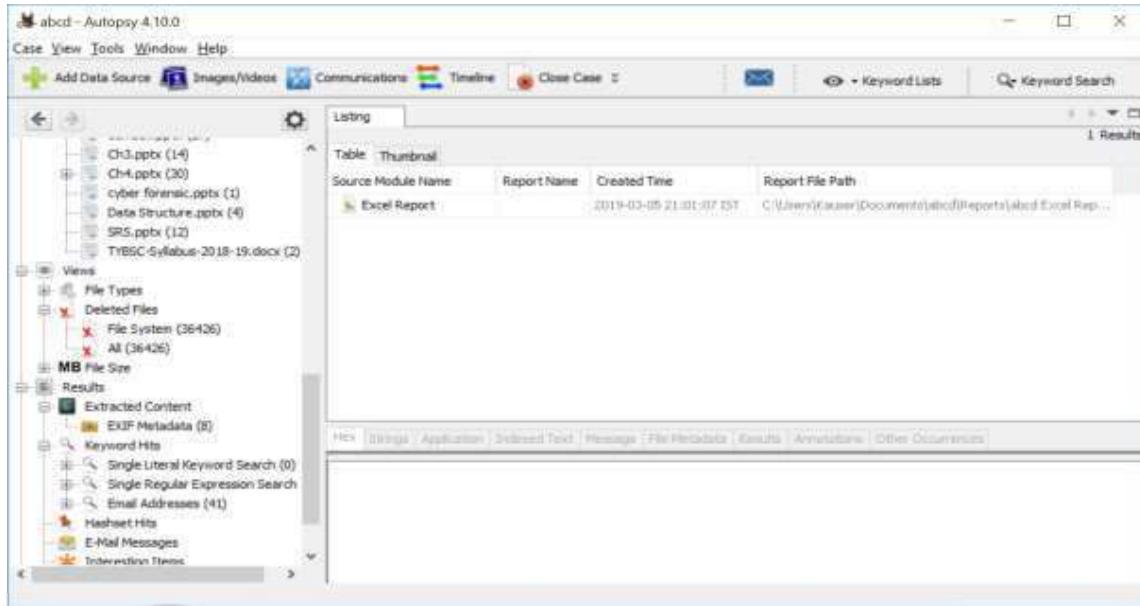


15. Click Finish after selecting All Results



Now Report is Generated So click on close Button, We can see the Report on Report Node.

Double click on the excel file and open it to view the report



THE NEXT LEVEL OF EDUCATION									
A1	B	C	D	E	F	G	H	I	J
1	Summary								
2									
3	Case Name:	abcd							
4	Case Number:	1345							
5	Examiner:	Tina							
6	Number of Images:	1							
7									
8									
9									
10									

A1	B	C	D	E	F	G
1	Date Taken	Device Manufacturer	Device Model	Latitude	Longitude	Altitude
2	2017-01-11 12:55:58 IST	Sony	D6502			/img_hopethisworks.001/KEAMANAN SISTEM INFORMASI MATERI 1.pdf
3	2017-01-11 15:14:48 IST	Sony	D6502			/img_hopethisworks.001/_883911C.tmp
4	2017-01-11 15:14:48 IST	Sony	D6502			/img_hopethisworks.001/_EE49B5C.tmp
5	2017-01-11 15:14:48 IST	Sony	D6502			/img_hopethisworks.001/_p18616.tmp
6	2017-01-11 15:14:48 IST	Sony	D6502			/img_hopethisworks.001/cyber forensic.pptx
7	2017-01-11 15:14:48 IST	Sony	D6502			/img_hopethisworks.001/cyber forensic.pptx
8	2017-01-11 15:14:48 IST	Sony	D6502			/img_hopethisworks.001/pptBA6C.tmp
9	2018-12-18 16:03:08 IST					/img_hopethisworks.001/admadv.pptx/image6.jpg
10						
11						
12						

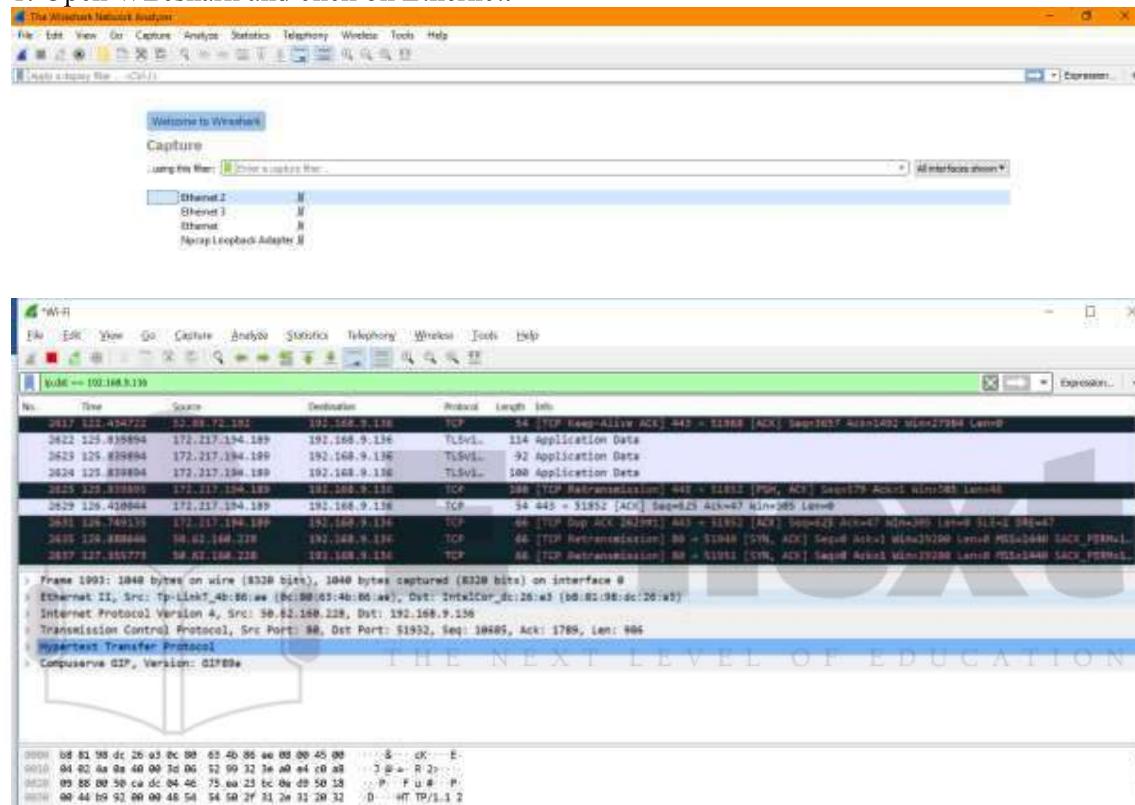
Practical No – 4

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

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

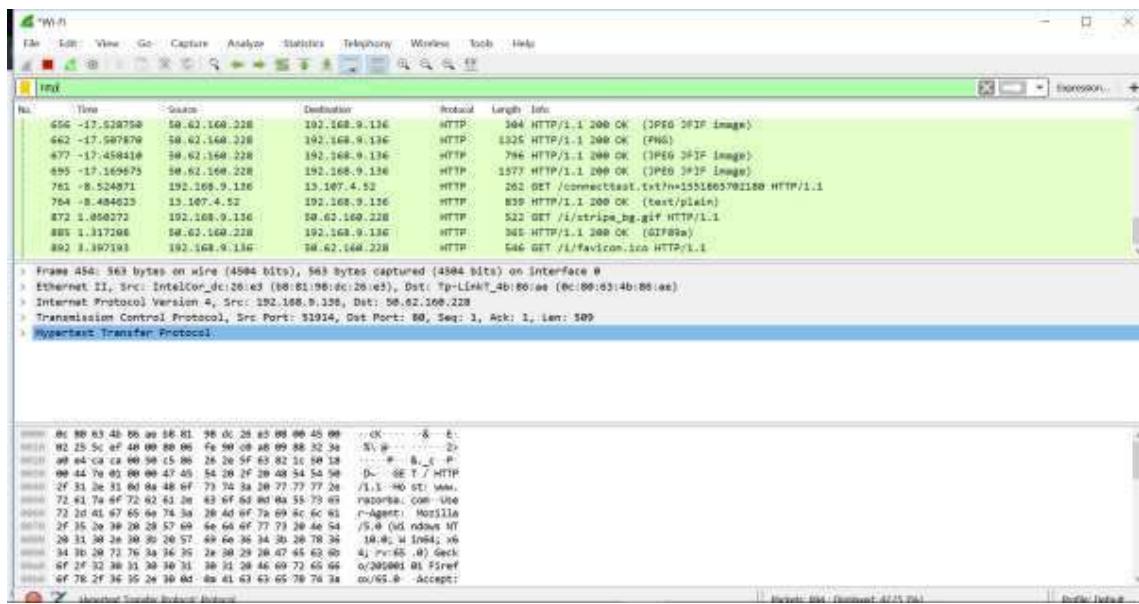
Steps:

1. Open Wireshark and click on Ethernet.

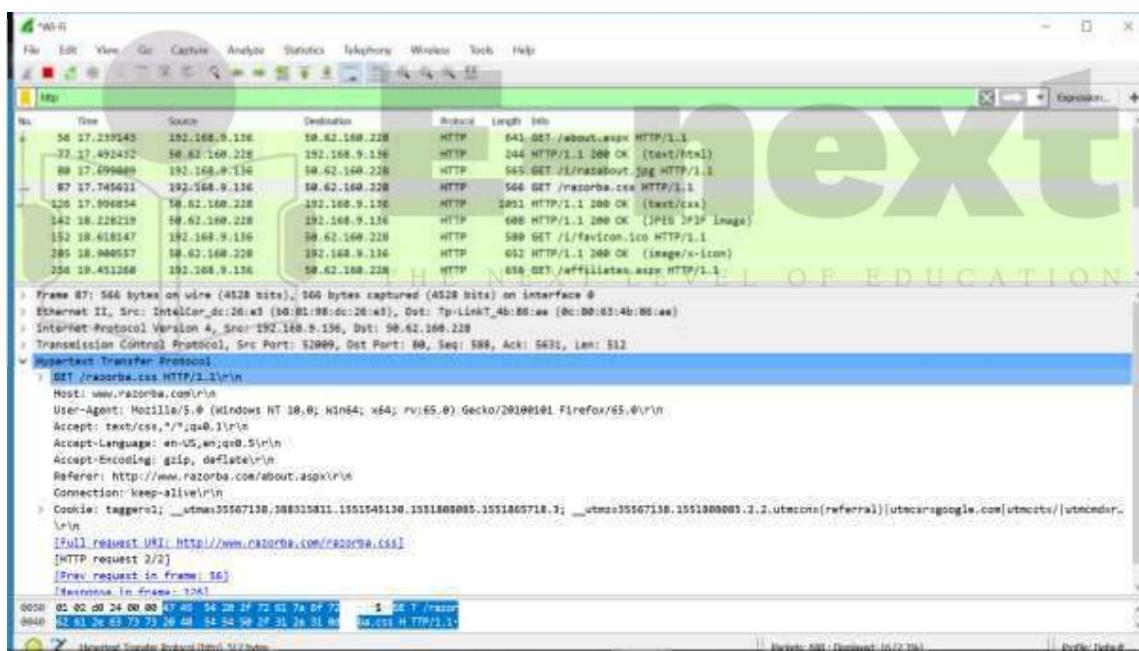


2. Now go on browser and open any unsecured website i.e www.razorba.com and perform some activity on the website.

3. Now come back to Wireshark and enter http in the search bar.



4. Now click on the get request and see the details.



Practical No – 5

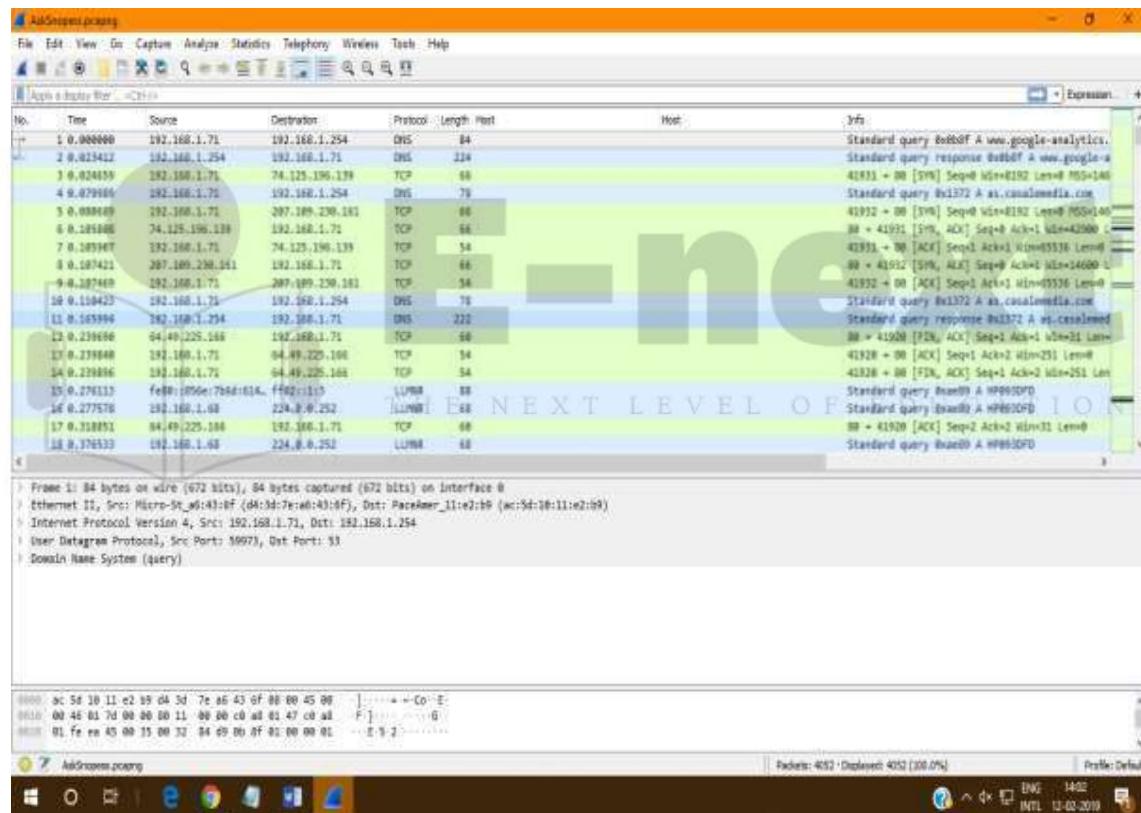
Aim: Analyze the packets provided in lab and solve the questions using Wireshark:

- What web server software is used by www.snopes.com?
 - About what cell phone problem is the client concerned?
 - According to Zillow, what instrument will Ryan learn to play?
 - How many web servers are running Apache?
 - What hosts (IP addresses) think that jokes are more entertaining when they are explained?

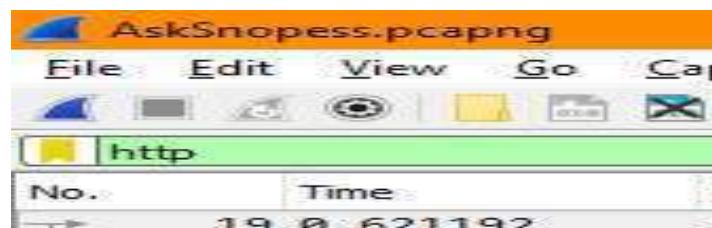
Steps:

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

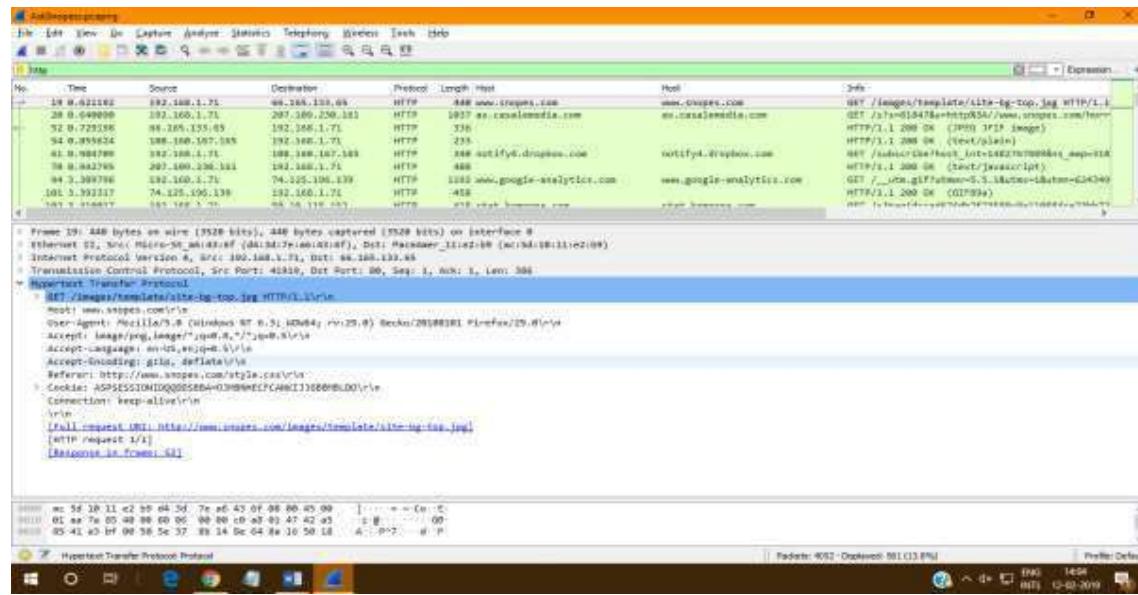
1. Open the AskSnopess file



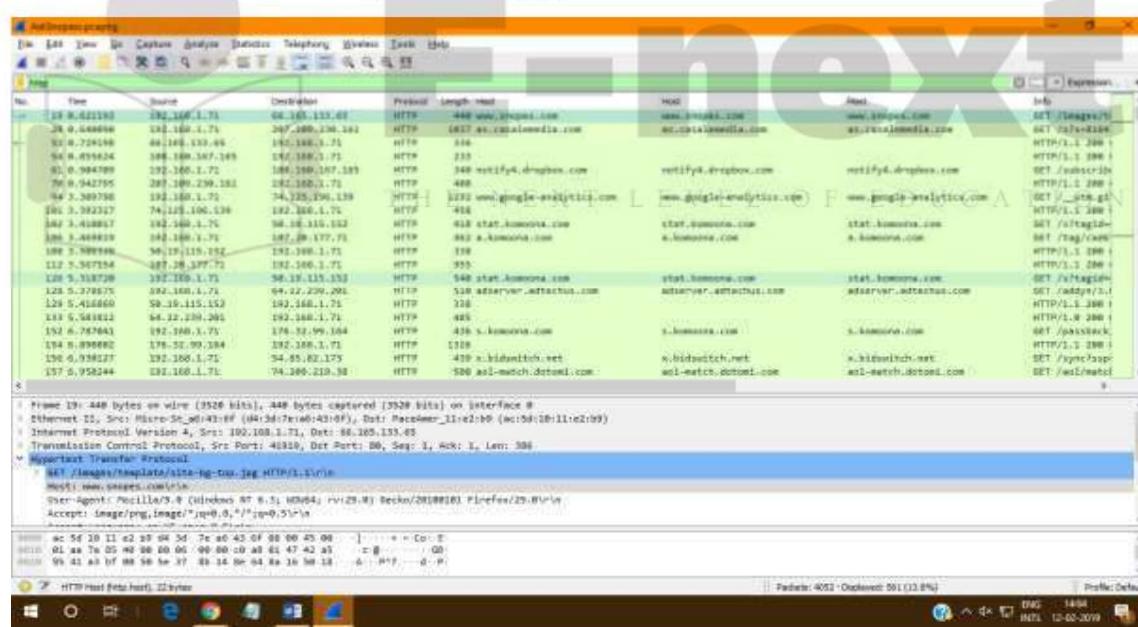
2. In the display filter type http.



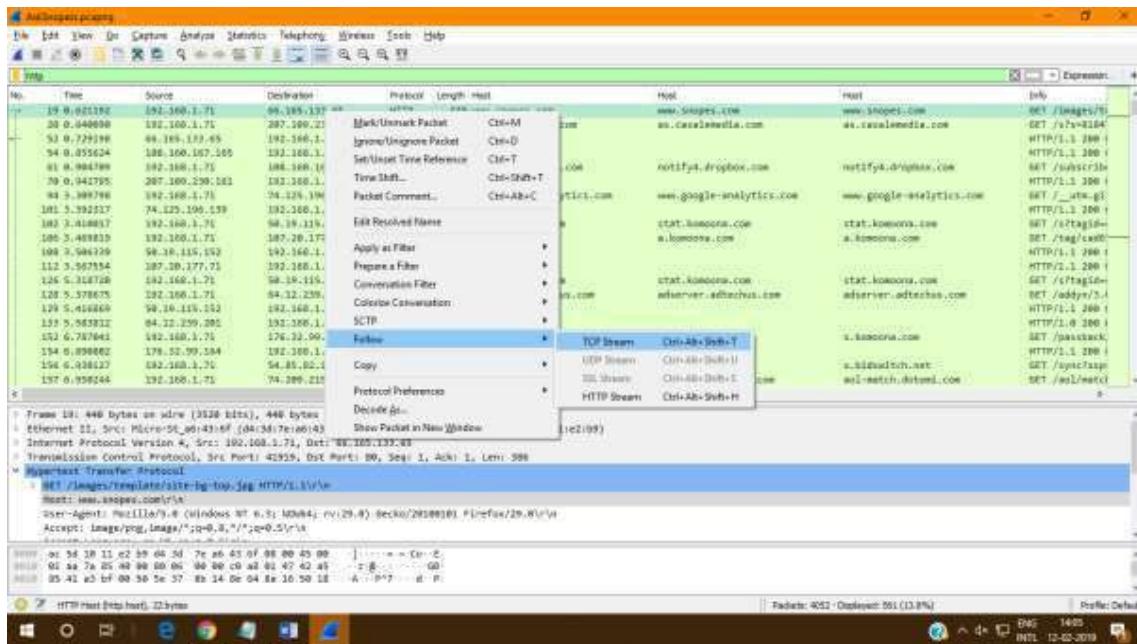
3. In the second panel expand the hypertext transfer protocol.



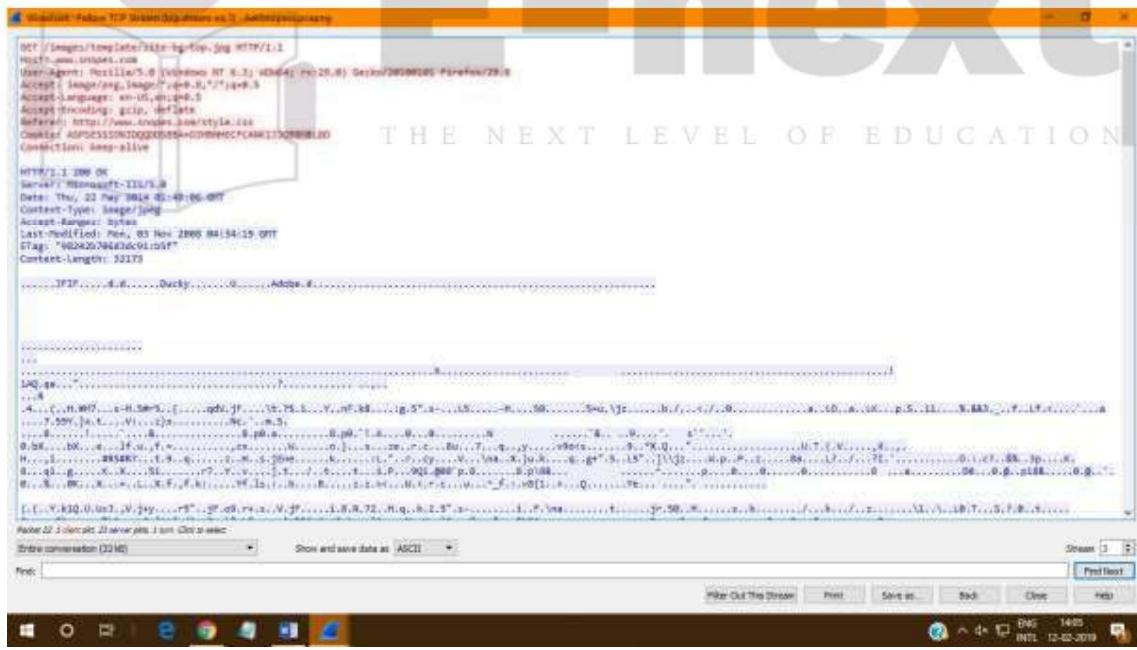
4. Click on the host name > right click> Apply as column



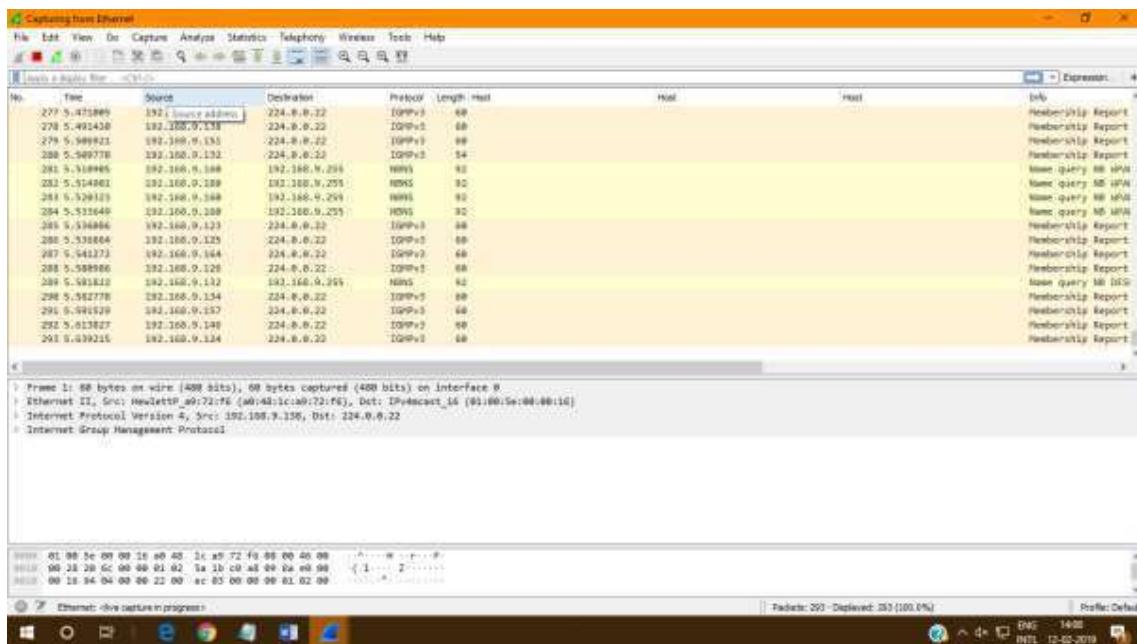
5. Click any of the http packet > right click> Follow> TCP Stream



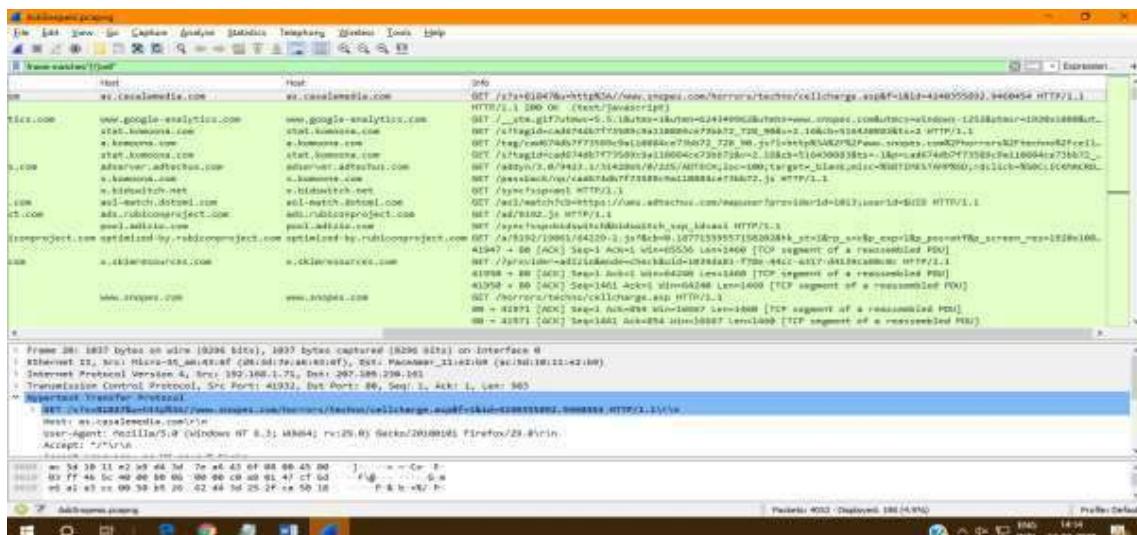
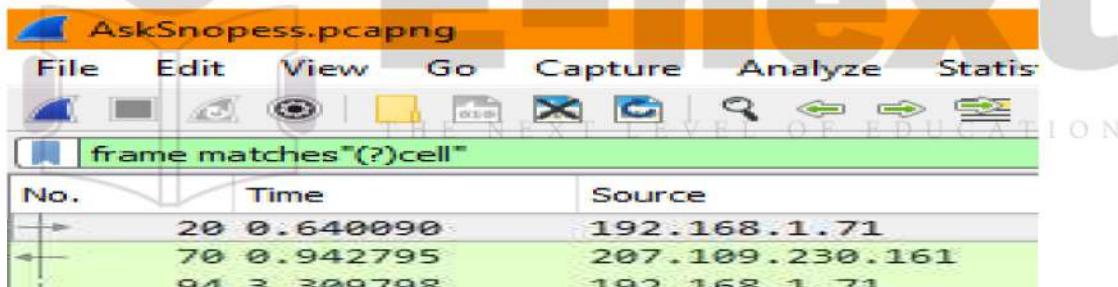
6. The webserver is Microsoft IIS/5.0



- About what cell phone problem is the client concerned?



1. In the display filter type frame matches"(?)cell".



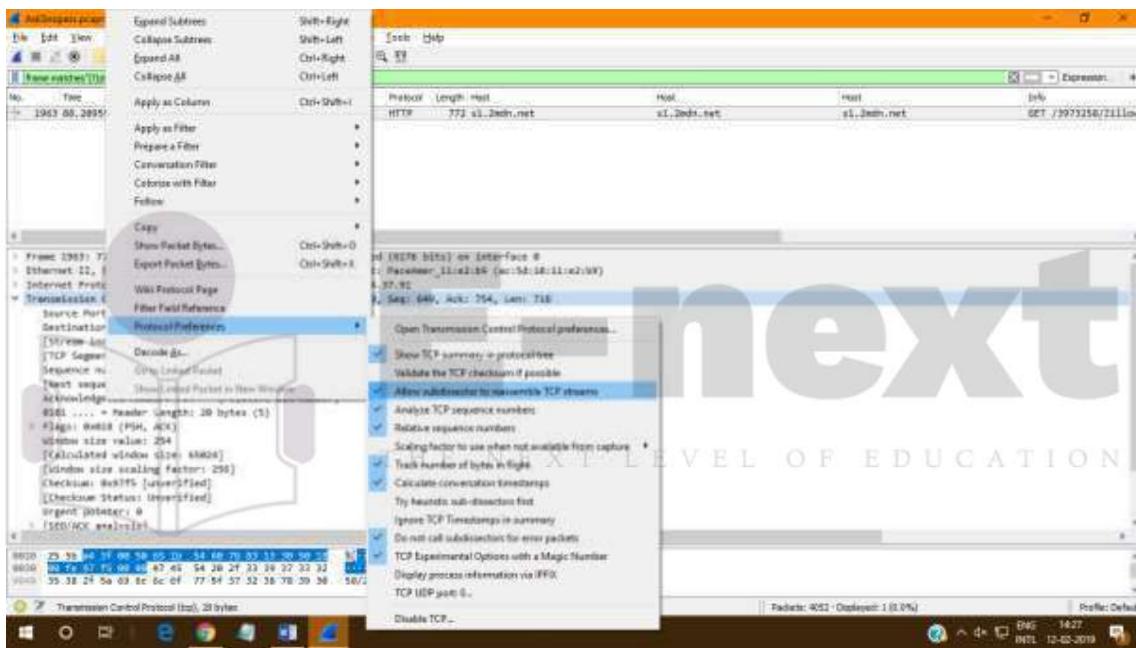
- According to Zillow, what instrument will Ryan learn to play?

1. In the display filter type frame matches"(?)zillow".

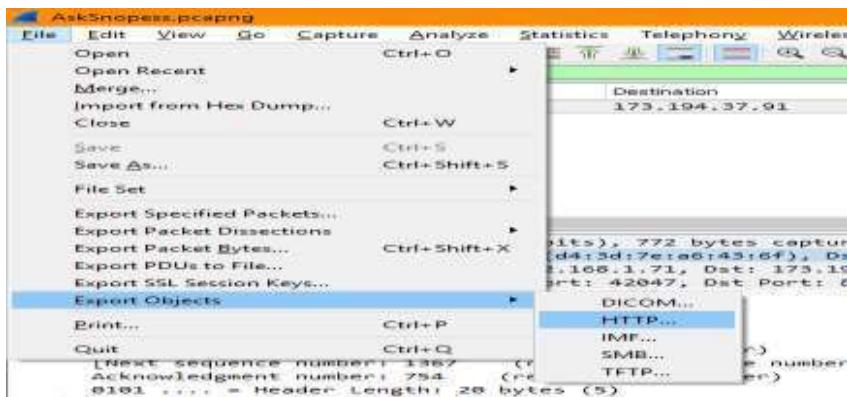


2. In the second tab expand the transmission control protocol.

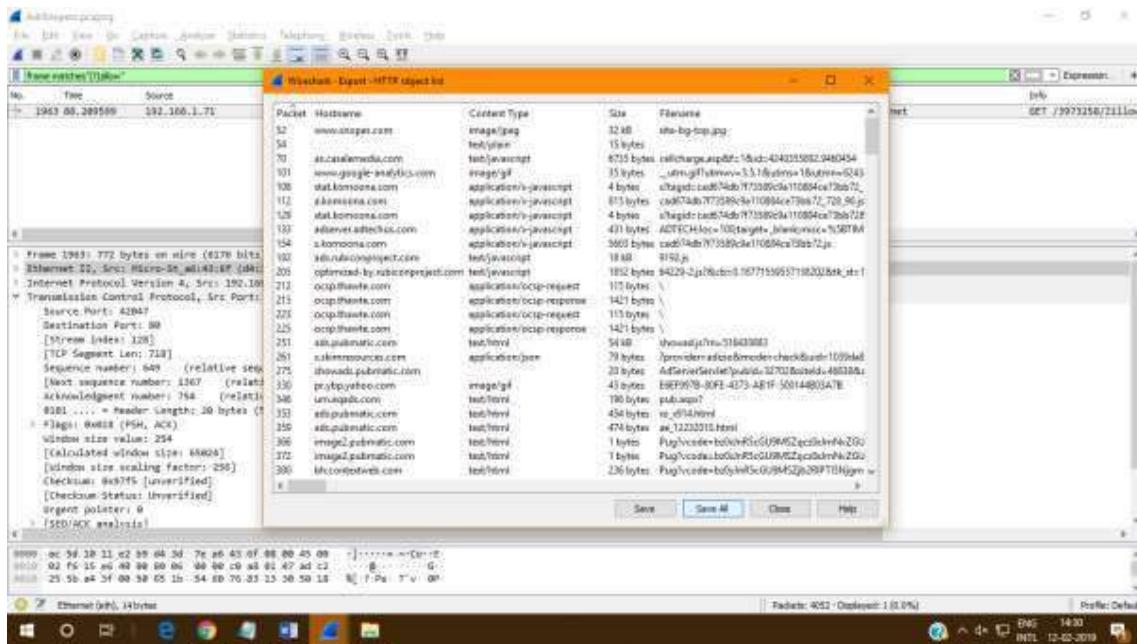
Right click on transmission control protocol > Protocol Preferences > Allow subdissector to reassemble TCP stream.



3. Click on file > Export objects > HTTP.



4. Click on Save all.

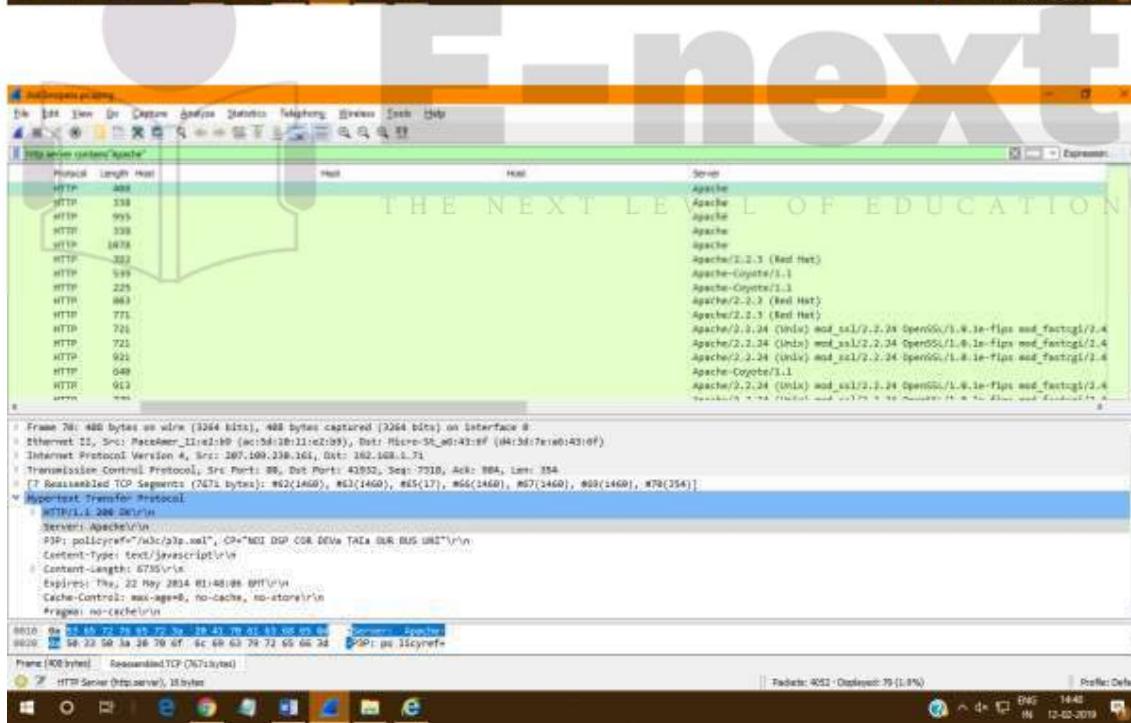
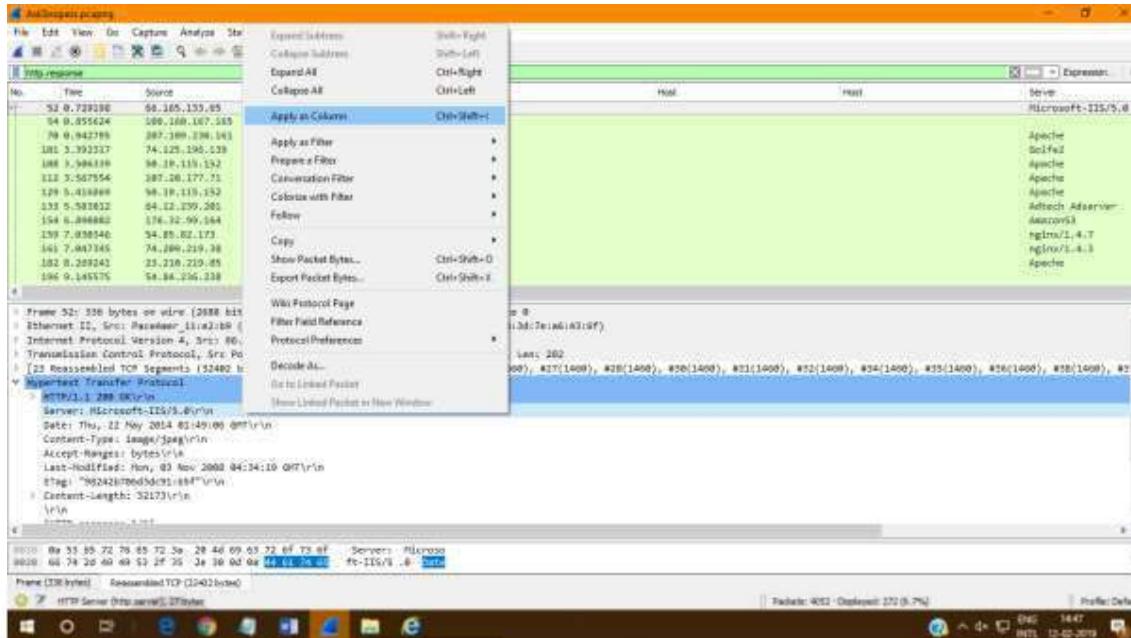


5. Run the saved file and you will get the result.

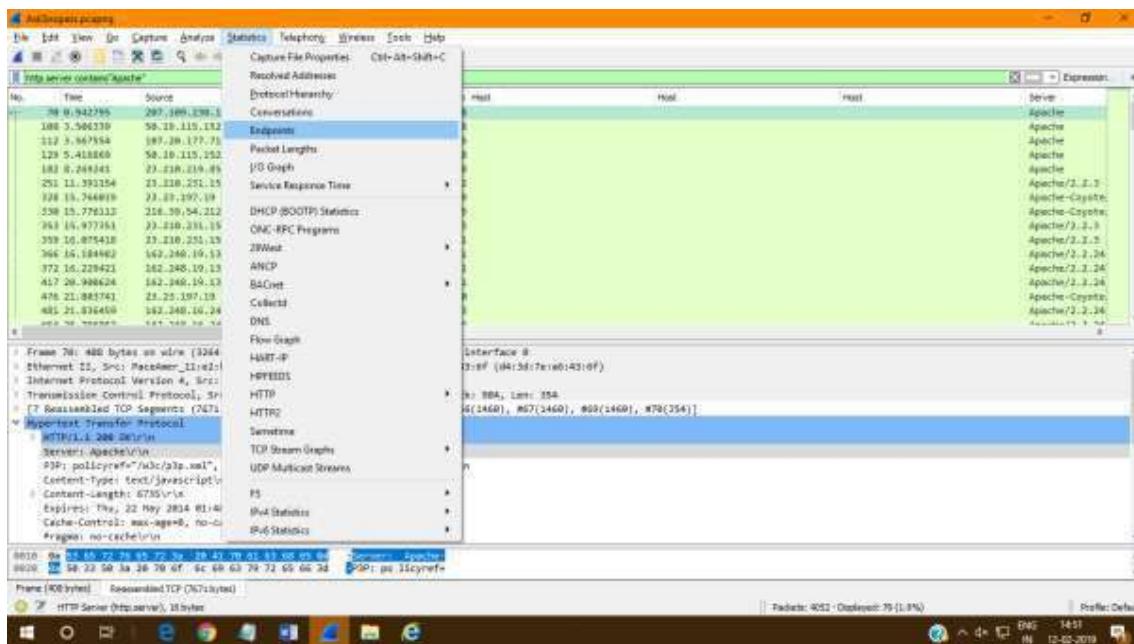


- How many web servers are running Apache?

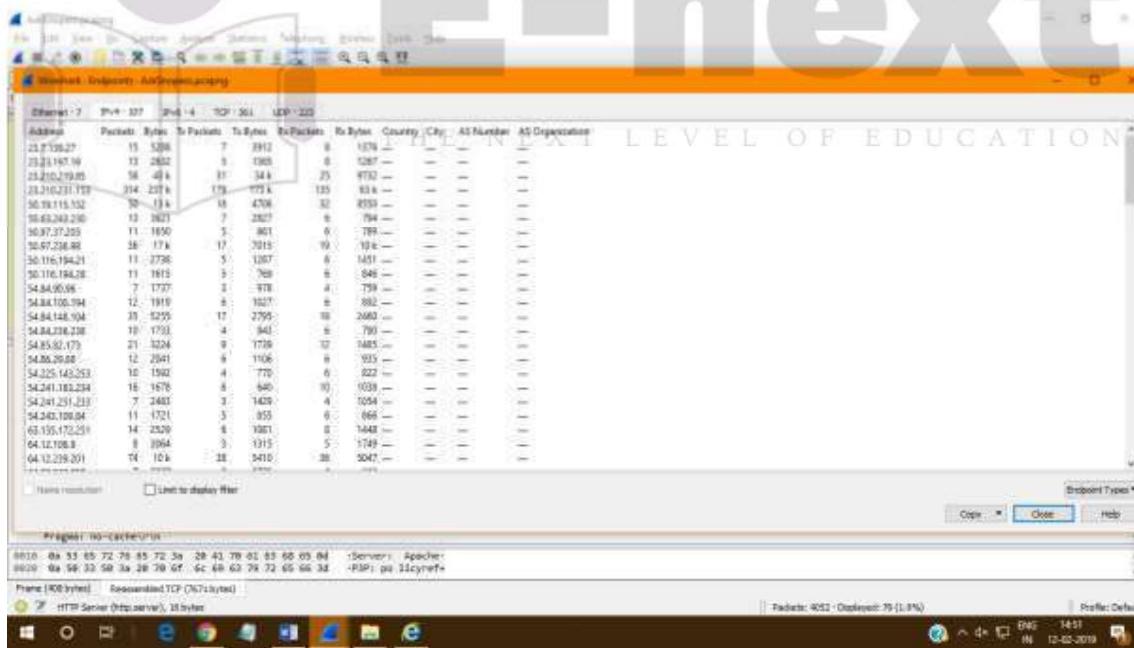
1. Right click on HTTP > Apply as column.



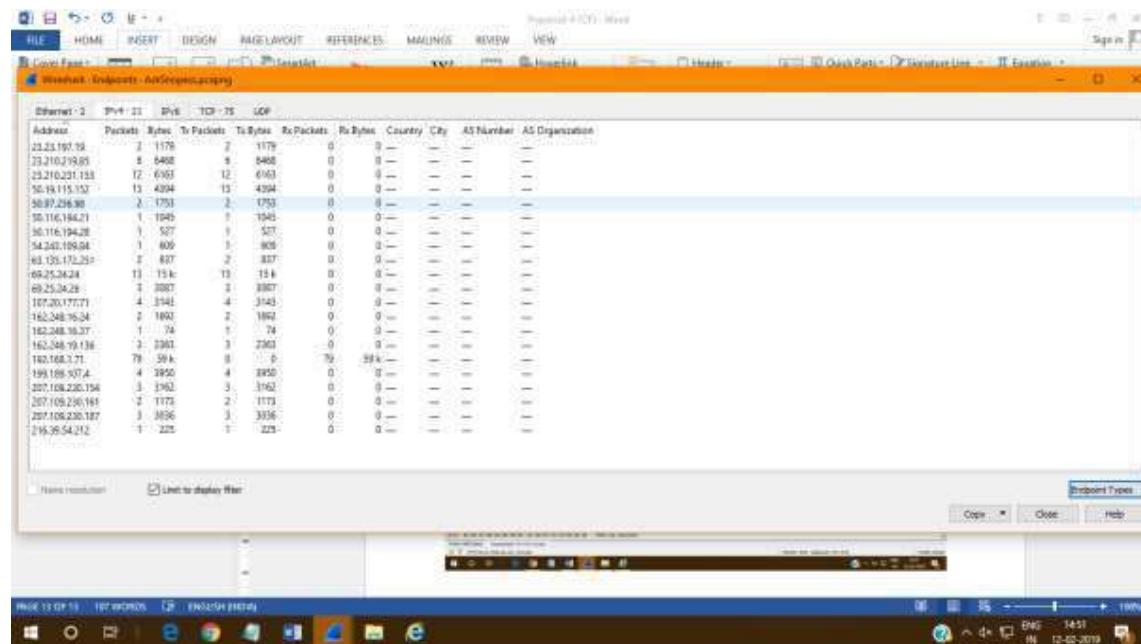
2. Click on Statistics > Endpoints.



3. Click the check box.

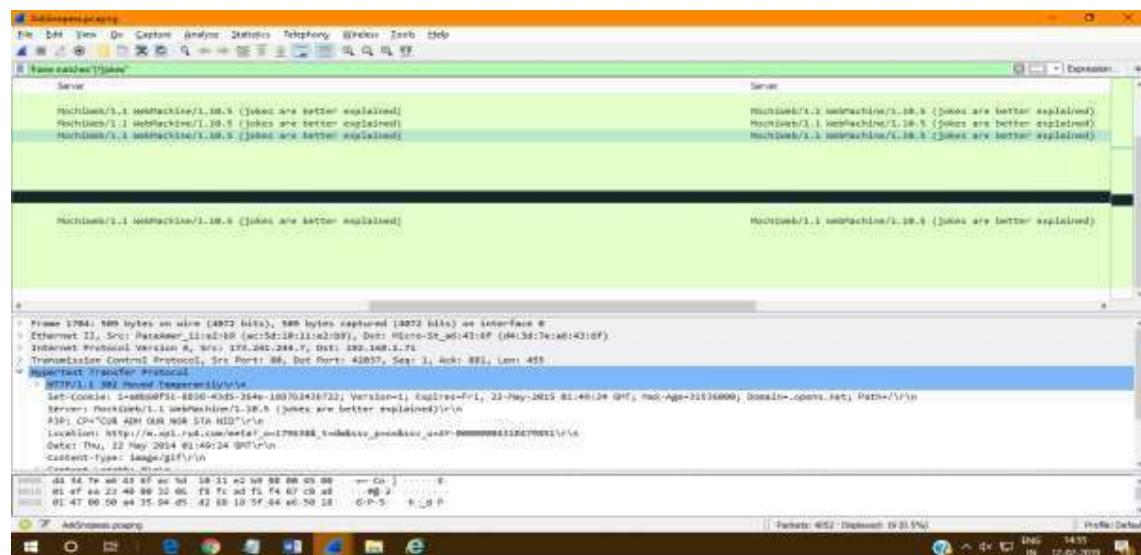


4. Beside IPv4 the number 21 shows that there are 21 web servers running on apache.



- What hosts (IP addresses) think that jokes are more entertaining when they are explained?

1. In the display filter type frame matches "(?)jokes".



Practical No – 6

Aim: Using Sysinternals tools for Network Tracking and Process Monitoring:

- Check Sysinternals tools
- Monitor Live Processes
- Capture RAM-Capture
- TCP/UDP packets
- Monitor Hard Disk
- Monitor Virtual Memory
- Monitor Cache Memory

Steps:

- 1) 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:

- File and Disk Utilities
- Networking Utilities
- Process Utilities
- Security Utilities
- System Information Utilities
- Miscellaneous Utilities

- 2) Monitor Live Processes (Tool: ProcMon)

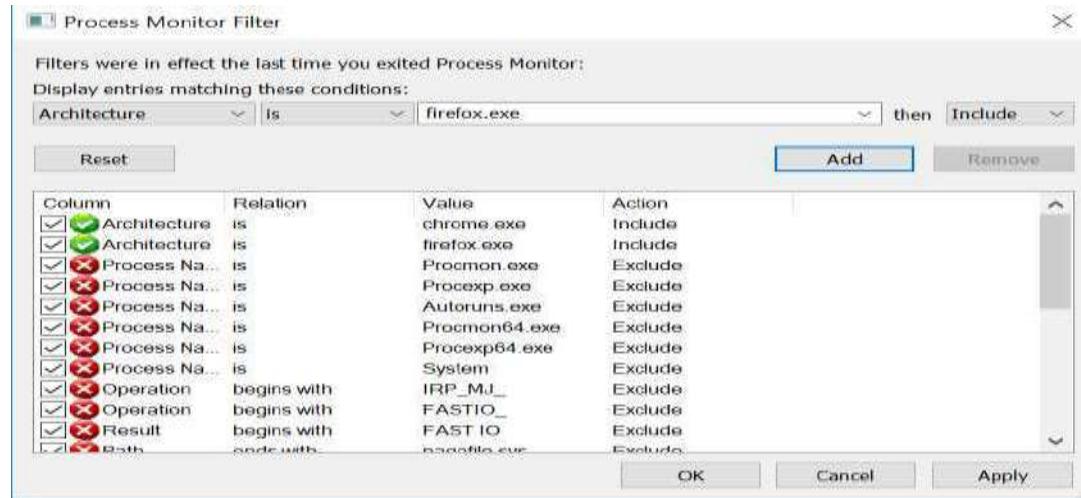


Process Monitor - Sysinternals: www.sysinternals.com

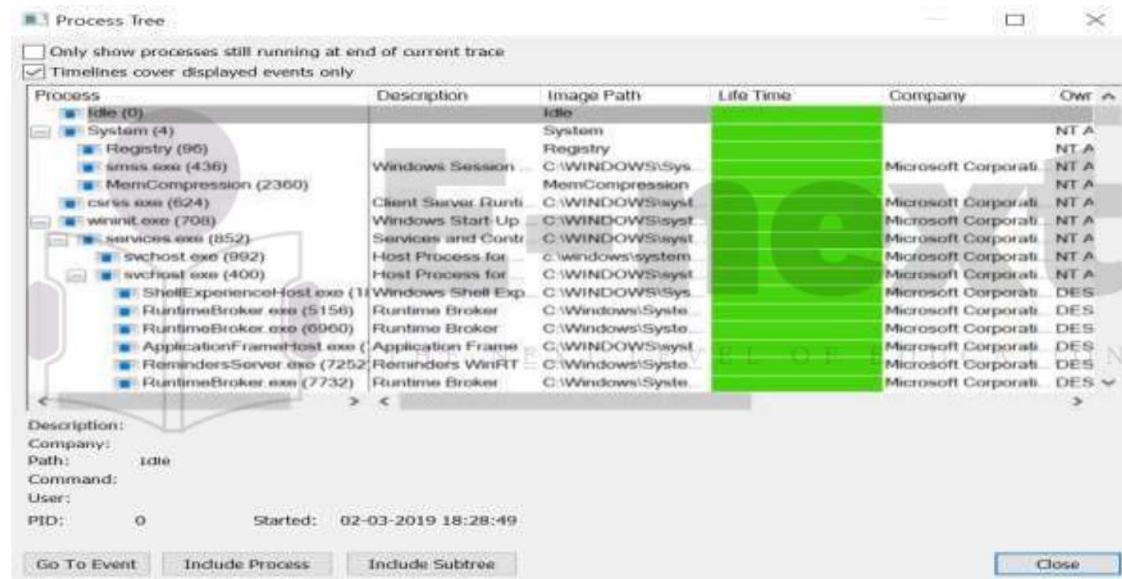
Time	Process Name	PID	Operation	Path
20:33:3...	Procmon64.exe	4120	RegQueryValue	HKLM\System\CurrentControlSet\Cont
20:33:3...	System	4	Thread Create	
20:33:3...	Procmon64.exe	4120	Thread Create	
20:33:3...	Procmon64.exe	4120	Thread Create	
20:33:3...	Procmon64.exe	4120	Thread Create	
20:33:3...	Procmon64.exe	4120	Thread Create	
20:33:3...	Procmon64.exe	4120	Thread Create	
20:33:3...	Procmon64.exe	4120	Thread Create	
20:33:3...	Procmon64.exe	4120	Thread Create	
20:33:3...	Procmon64.exe	4120	Thread Exit	
20:33:3...	ctfmon.exe	7048	RegQueryKey	HKCU
20:33:3...	ctfmon.exe	7048	RegOpenKey	HKCU\Software\Microsoft\Input\Setti

Showing 334641 of 338862 events (98%) Backed by virtual memory

Click on filter > Process monitor filter



Click on tools > Process tree

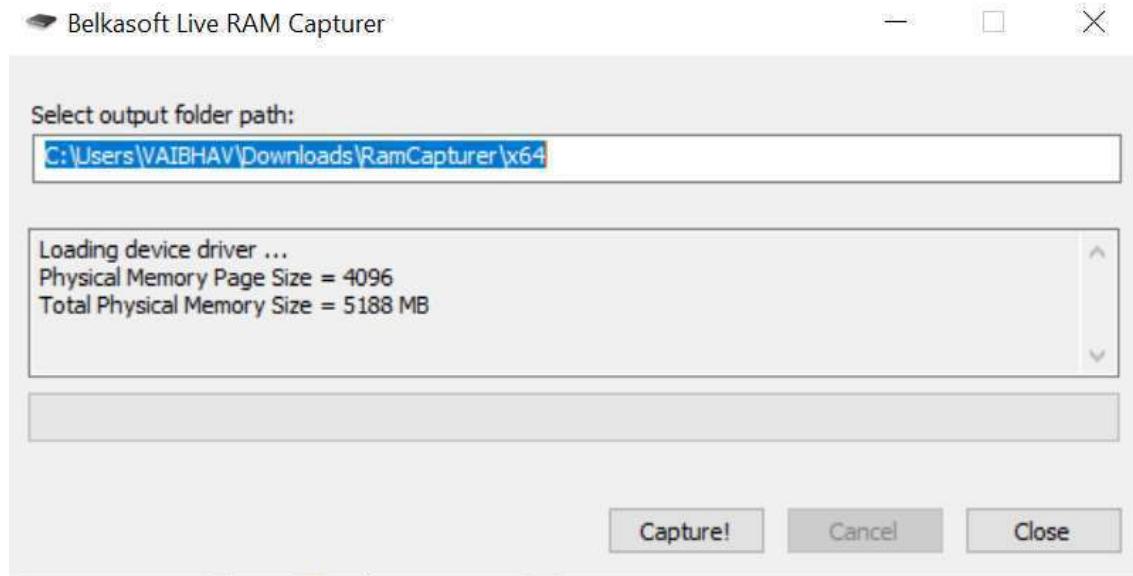


Click on filter > File summary

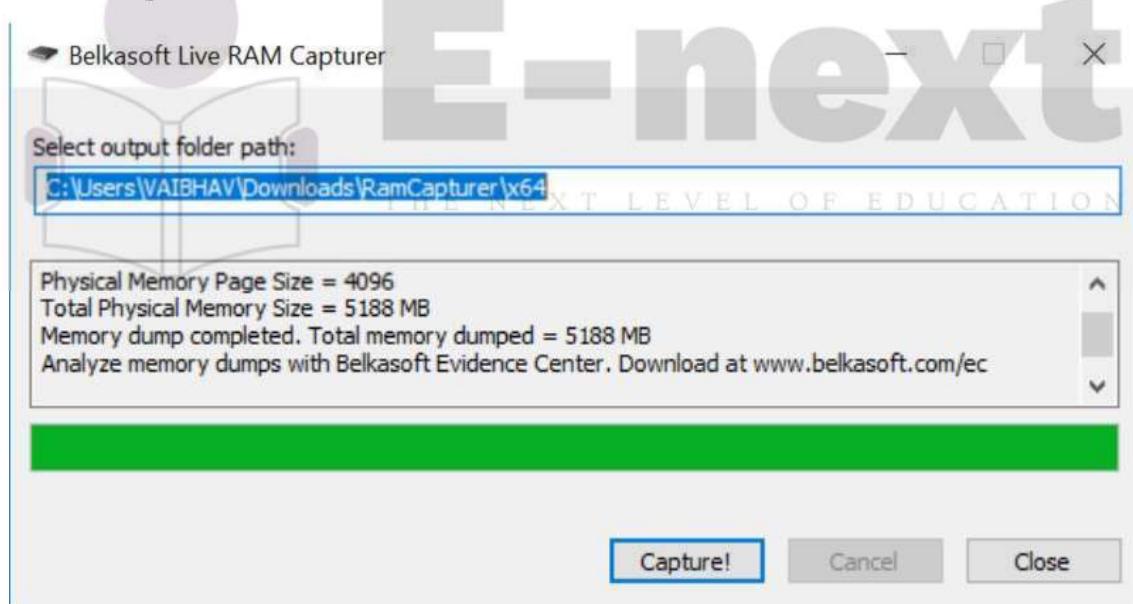
File Summary													
Files accessed during trace:													
By Path	By Folder	By Extension	File Time	Total Events	Opens	Closes	Reads	Writes	Read Byt..	Write Byt..	Get ACL	Set ACL	Other Path
10/14/2019 268301	48568	45477	7756	180	15685548	1776204	104	0	142673	<Total>	0	0	2374 C:\Windows\System32\svchost.exe
0.08652688	4652	759	759	1	0	32768	0	0	0	0	0	0	2 C:\Windows\System32\drivers\etc\serv...
0.03562811	4236	17	17	4183	0	2108081	0	0	0	0	0	0	682 C:\Windows\System32\UIAutomationC...
0.0402667	3562	128	128	2496	0	48464	0	0	0	0	0	0	1426 C:\Windows\System32\crypt32.dll
0.0457052	2848	474	473	1	0	32768	0	0	0	0	0	0	1421 C:\Windows\System32\msasn1.dll
0.0305297	2840	473	472	1	0	32768	0	0	0	0	0	0	1368 C:\Windows\System32\wintrust.dll
0.0291413	2728	454	454	0	0	0	0	0	0	0	0	0	1099 C:\Windows\System32\cryptui.dll
0.0256040	2725	543	543	0	0	0	0	0	0	0	0	0	1510 C:\Windows\System32\en-US\svchost...
0.0264369	2418	302	302	0	0	0	0	0	0	0	0	0	1063 C:\Windows\System32\spool.dll
0.0231385	2104	347	347	0	0	0	0	0	0	0	0	0	1005 C:\Windows\System32\PHLPAPI.DLL
0.02460511	2005	333	332	0	0	0	0	0	0	2	0	0	783 C:\Windows\System32\ntdll.dll
0.0225218	1943	387	386	0	0	0	0	0	0	0	0	0	

3) Capture RAM (Tool: RAMCapture)

Open the Ramcapture tool.



Click on capture.



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

Open the Tcpview tool.

Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State
[System Proc.]	0	TCP	desktop-fq9in	64289	bom07s11-in-f14...	https	TIME_WAIT
[System Proc.]	0	TCP	desktop-fq9in	64293	155.244.178.107...	https	TIME_WAIT
[System Proc.]	0	TCP	desktop-fq9in	64298	52.109.56.34	https	TIME_WAIT
epmd.exe	11016	TCP	DESKTOP-FTQ9ILN	4369	DESKTOP-FTQ9ILN	0	LISTENING
epmd.exe	11016	TCP	DESKTOP-FTQ9ILN	4369	localhost	51791	ESTABLISHED
epm.exe	11016	TCPv6	desktop-fq9in	4369	desktop-fq9in	0	LISTENING
erl.exe	7284	TCP	DESKTOP-FTQ9ILN	5984	DESKTOP-FTQ9ILN	0	LISTENING
erl.exe	7284	TCP	DESKTOP-FTQ9ILN	5986	DESKTOP-FTQ9ILN	0	LISTENING
erl.exe	7284	TCP	DESKTOP-FTQ9ILN	51790	DESKTOP-FTQ9ILN	0	LISTENING
erl.exe	7284	TCP	DESKTOP-FTQ9ILN	51791	localhost	4369	ESTABLISHED
firefox.exe	10952	TCP	DESKTOP-FTQ9ILN	50023	localhost	50024	ESTABLISHED
firefox.exe	10952	TCP	DESKTOP-FTQ9ILN	50024	localhost	50023	ESTABLISHED
firefox.exe	11480	TCP	DESKTOP-FTQ9ILN	50030	localhost	50031	ESTABLISHED
firefox.exe	11480	TCP	DESKTOP-FTQ9ILN	50031	localhost	50030	ESTABLISHED
firefox.exe	6524	TCP	DESKTOP-FTQ9ILN	50035	localhost	50036	ESTABLISHED
firefox.exe	6524	TCP	DESKTOP-FTQ9ILN	50036	localhost	50035	ESTABLISHED
firefox.exe	8484	TCP	DESKTOP-FTQ9ILN	50045	localhost	50046	ESTABLISHED
firefox.exe	8484	TCP	DESKTOP-FTQ9ILN	50046	localhost	50045	ESTABLISHED
firefox.exe	5504	TCP	DESKTOP-FTQ9ILN	50207	localhost	50208	ESTABLISHED
firefox.exe	5504	TCP	DESKTOP-FTQ9ILN	50208	localhost	50207	ESTABLISHED
firefox.exe	11236	TCP	DESKTOP-FTQ9ILN	50321	localhost	50322	ESTABLISHED
firefox.exe	11236	TCP	DESKTOP-FTQ9ILN	50322	localhost	50321	ESTABLISHED

Right click on any packet > whois

Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State
firefox.exe	11480	TCP	DESKTOP-FTQ9ILN	50031	localhost	50030	ESTABLISHED
firefox.exe	6524	TCP	DESKTOP-FTQ9ILN	50035	localhost	50036	ESTABLISHED
firefox.exe	6524	TCP	DESKTOP-FTQ9ILN	50036	localhost	50035	ESTABLISHED
firefox.exe	8484	TCP	DESKTOP-FTQ9ILN	50045	localhost	50046	ESTABLISHED
firefox.exe	8484	TCP	DESKTOP-FTQ9ILN	50046	localhost	50045	ESTABLISHED
firefox.exe	5504	TCP	DESKTOP-FTQ9ILN	50207	localhost	50208	ESTABLISHED
firefox.exe	5504	TCP	DESKTOP-FTQ9ILN	50208	localhost	50207	ESTABLISHED
firefox.exe	11236	TCP	DESKTOP-FTQ9ILN	50321	localhost	50322	ESTABLISHED
firefox.exe	11236	TCP	DESKTOP-FTQ9ILN	50322	localhost	50321	ESTABLISHED
mass.exe	872	TCPv6	desktop-fq9in	49865	DESKTOP-FTQ9ILN	0	LISTENING
node.exe	4428	TCP	desktop-fq9in	49865	Process Properties...	https	ESTABLISHED
node.exe	4428	TCP	desktop-fq9in	49865	End Process...	https	ESTABLISHED
services.exe	852	TCP	DESKTOP-FTQ9ILN	49865	Close Connection	N 0	LISTENING
services.exe	852	TCPv6	desktop-fq9in	49865	Whois...	Ctrl+W	LISTENING
SkypeApp.exe	7808	UDP	DESKTOP-FTQ9ILN	49865	Copy...	Ctrl+C	LISTENING
spoolsv.exe	13852	UDPv6	desktop-fq9in	49865			LISTENING
spoolsv.exe	13852	TCP	DESKTOP-FTQ9ILN	49865			LISTENING
svchost.exe	1084	TCP	DESKTOP-FTQ9ILN	espmap	DESKTOP-FTQ9ILN	0	LISTENING
svchost.exe	7100	TCP	DESKTOP-FTQ9ILN	5040	DESKTOP-FTQ9ILN	0	LISTENING
svchost.exe	1504	TCP	DESKTOP-FTQ9ILN	49866	DESKTOP-FTQ9ILN	0	LISTENING



OK

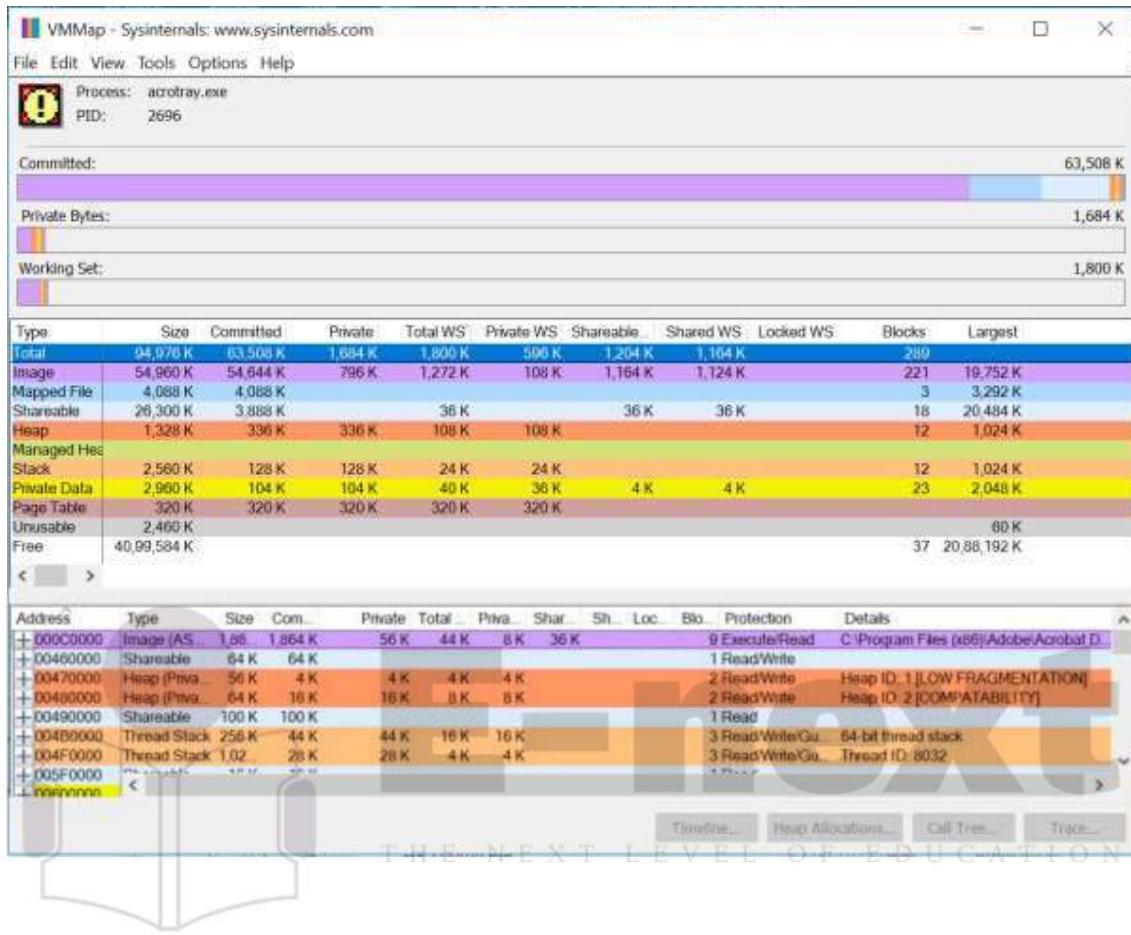
5) Monitor Hard Disk (Tool: DiskMon)

Open the Diskmon tool.

#	Time	Duration (s)	Disk	Request	Sector	Length
276	25.023239	0.00000000	0	Read	7024616	8
277	25.037334	0.00000000	0	Read	737624	8
278	25.037630	0.00000000	0	Read	7025104	8
279	25.059359	0.00000000	0	Read	255396480	128
280	25.081087	0.00000000	0	Read	7130184	8
281	25.100023	0.00000000	0	Read	6930184	8
282	25.106452	0.00000000	0	Read	6926312	8
283	25.118697	0.00000000	0	Read	7073128	8
284	25.118959	0.00000000	0	Read	7129992	8
285	25.129898	0.00000000	0	Read	6926512	8
286	25.130141	0.00000000	0	Read	737600	8
287	25.130330	0.00000000	0	Read	7132232	8
288	25.137335	0.00000000	0	Read	7132432	8
289	25.137633	0.00000000	0	Read	7130576	8
290	26.350045	0.00000000	0	Write	16671416	8
291	26.923136	0.00000000	0	Write	20504128	112
292	26.923376	0.00000000	0	Write	8724544	16
293	27.339871	0.00000000	0	Read	335710896	128

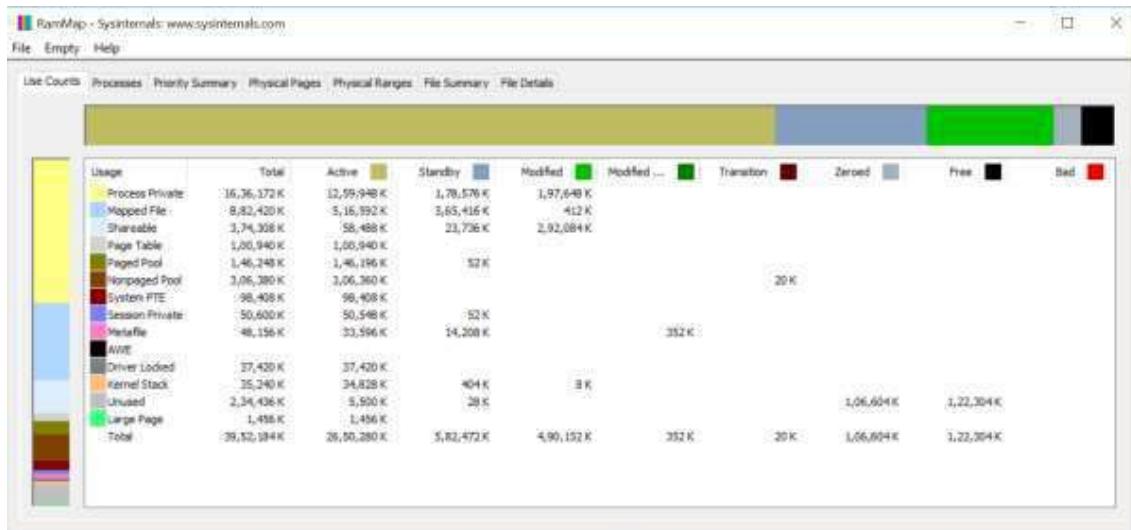
6) Monitor Virtual Memory (Tool: VMMap)

Open the VMMap tool.



7) Monitor Cache Memory (Tool: RAMMap)

Open the RAMMap tool.



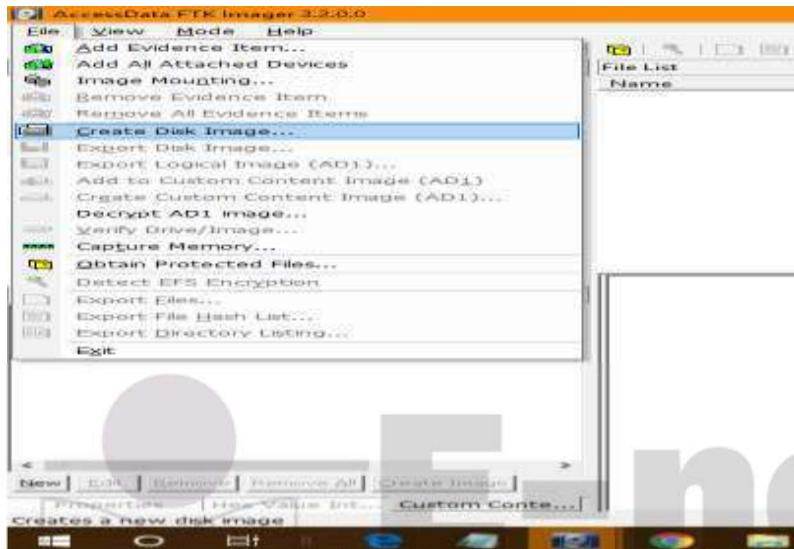
Practical No – 7

Aim: Recovering and Inspecting deleted files

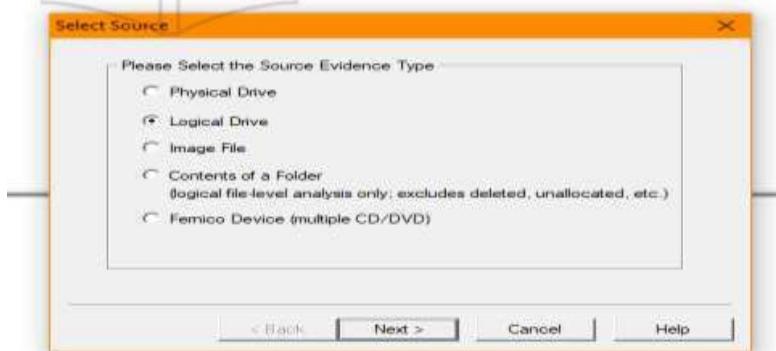
- Check for Deleted Files
- Recover the Deleted Files
- Analyzing and Inspecting the recovered files

Steps:

1. Open AccessData FTK Imager. Click on File > Create Disk Image.



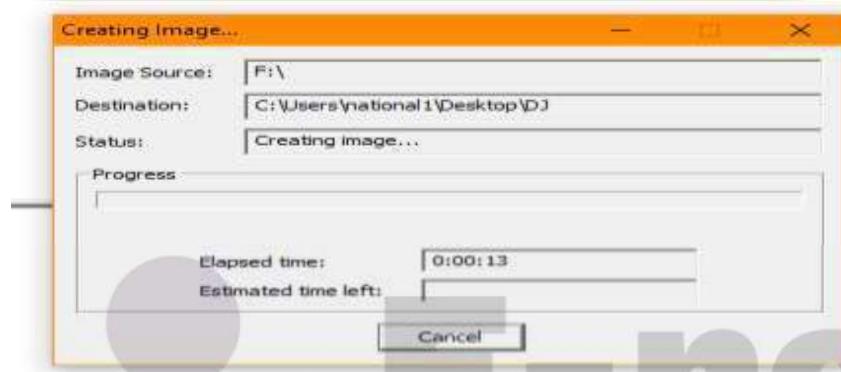
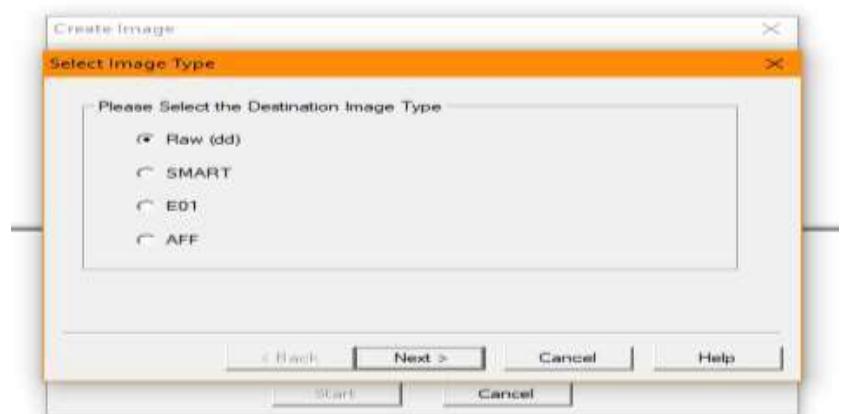
2. Type the destination path.
3. Click on Logical drive.



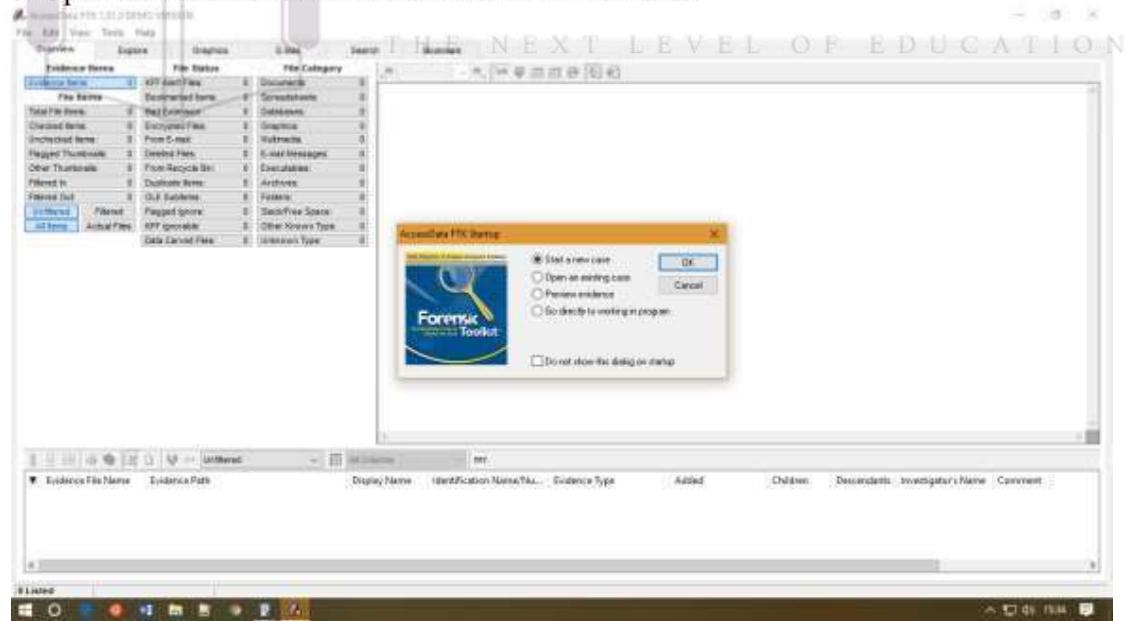
4. Click on Add > Browse.



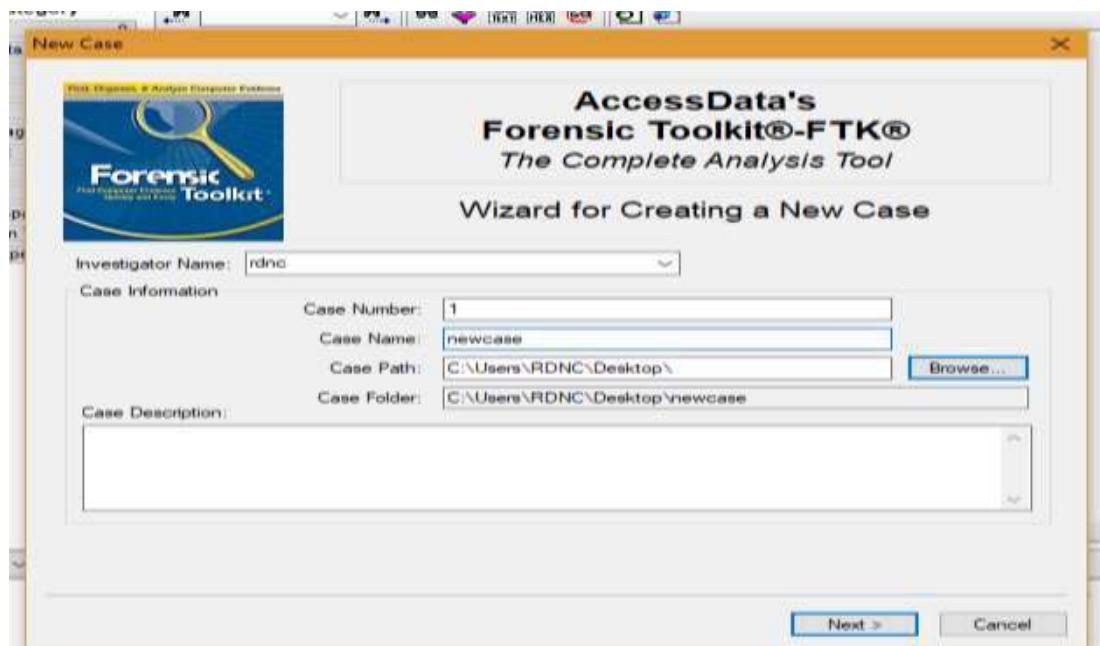
5. Select the type of data format and click next.



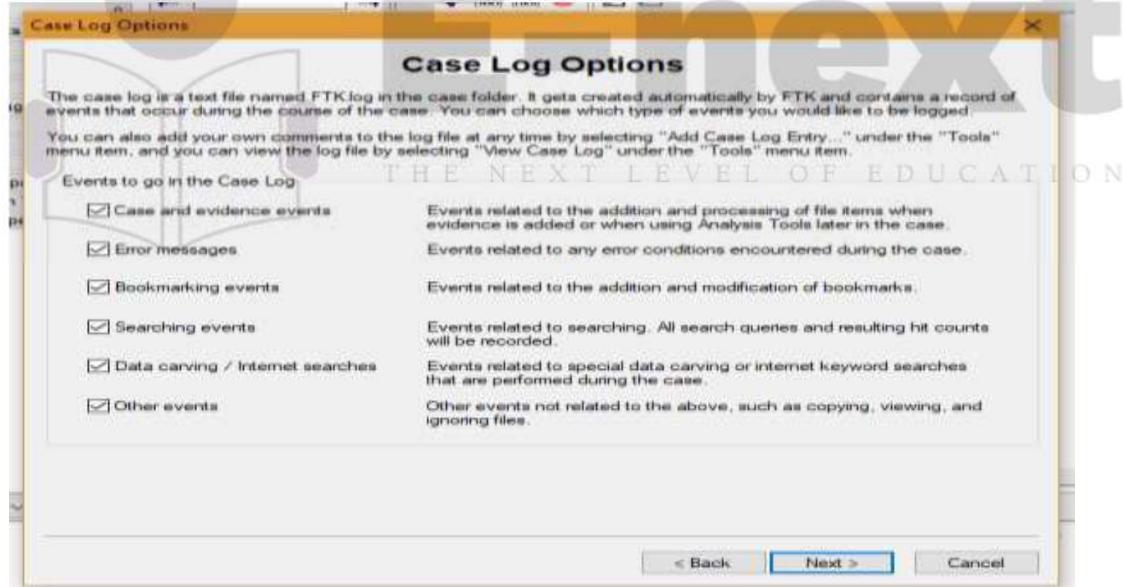
7. Open the Forensic toolkit and click on file > new case.



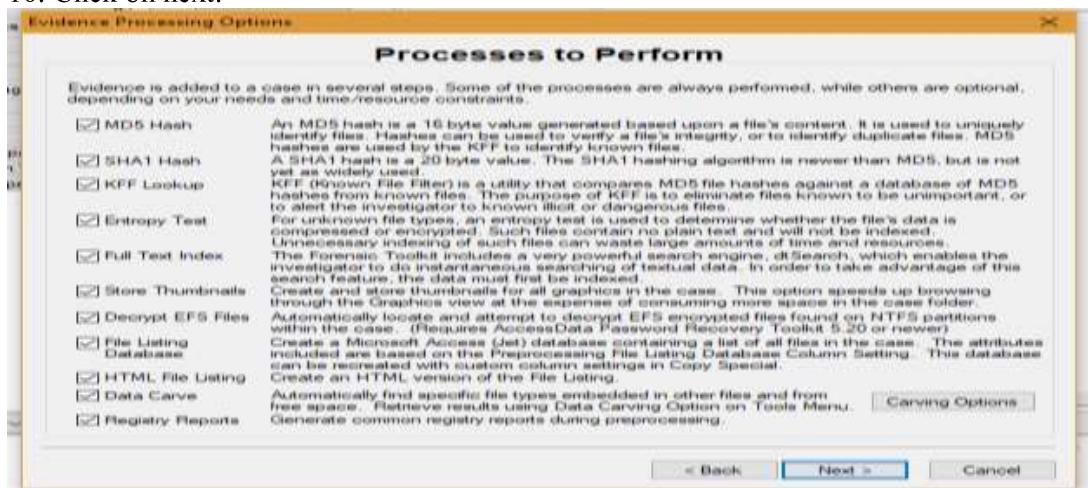
8. Enter the details and click on next.



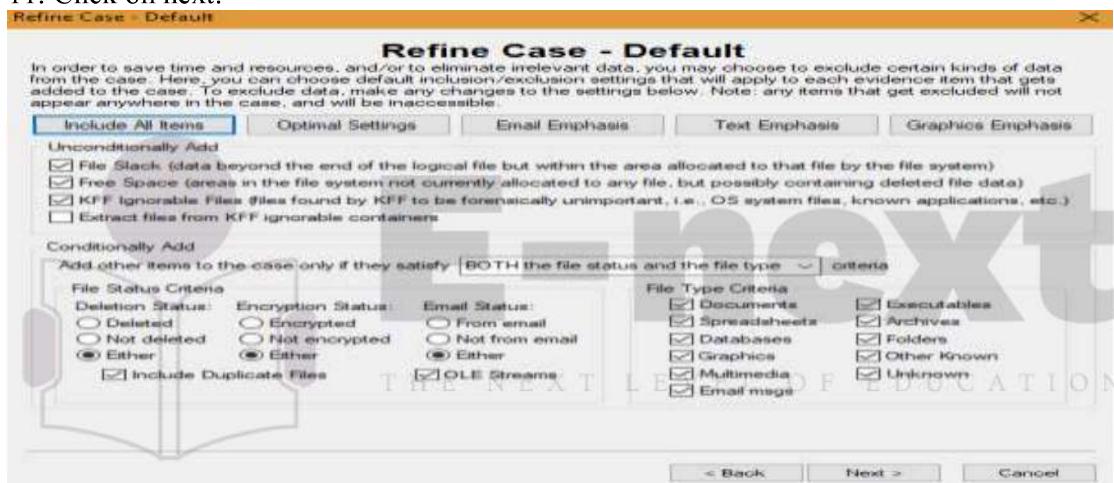
9. Click on next.



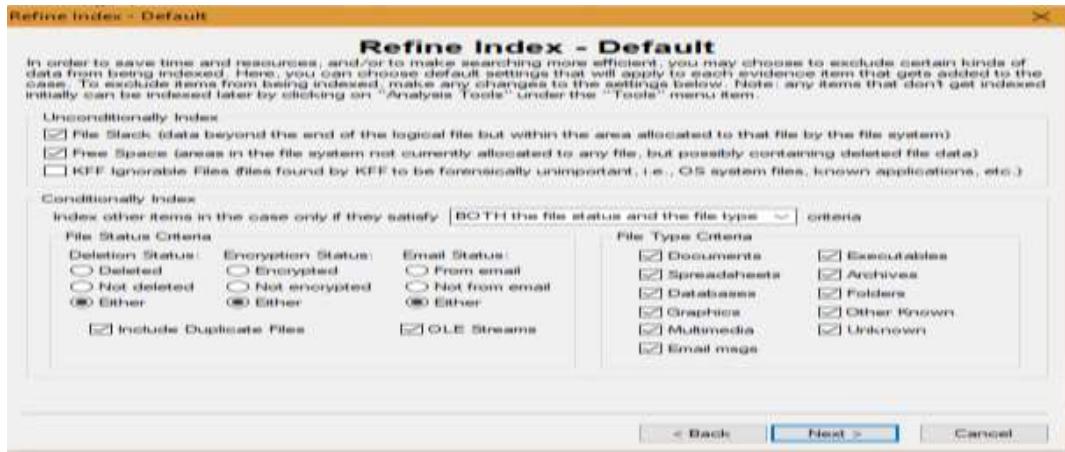
10. Click on next.



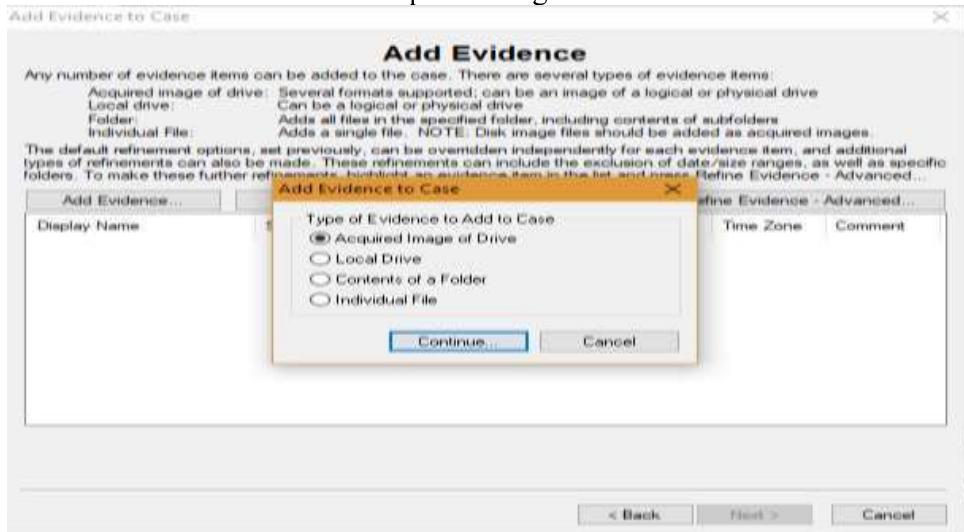
11. Click on next.



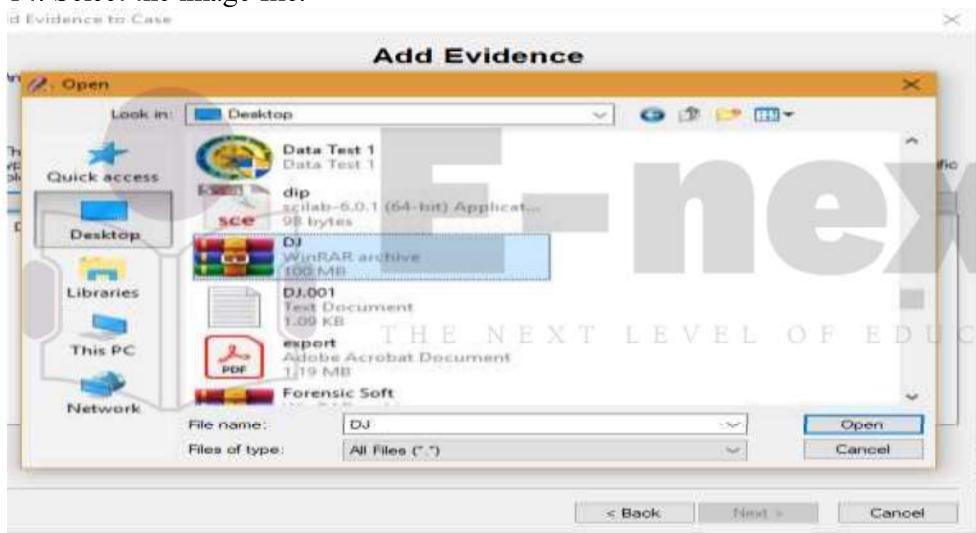
12. Click on next.



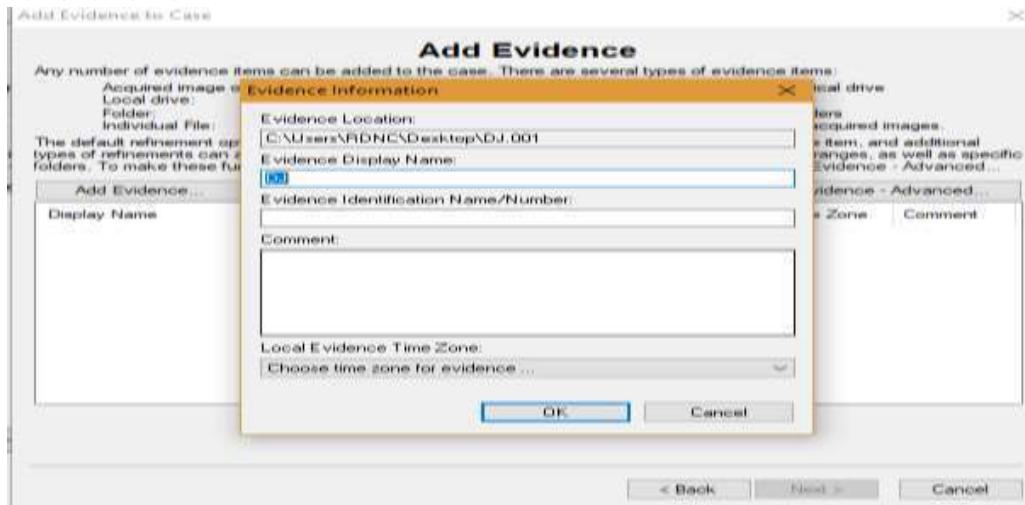
13. Click on Add Evidence > Acquired Image of Drive > Continue.



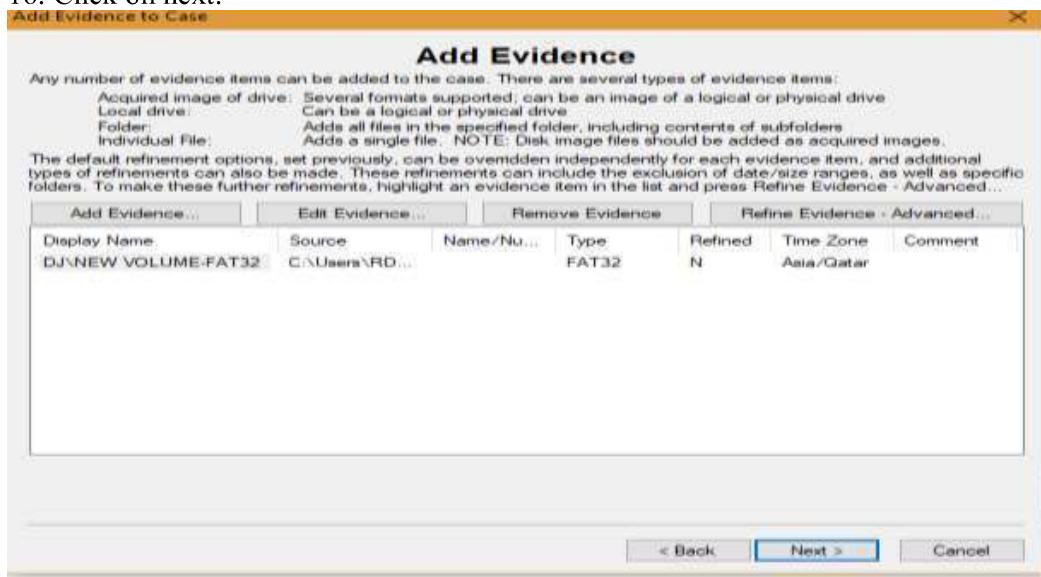
14. Select the image file.



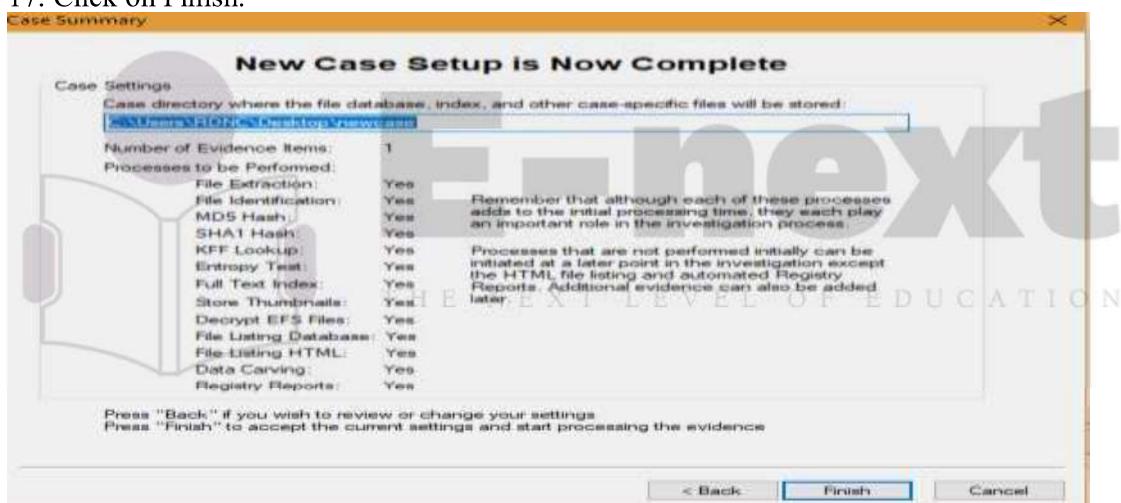
15. Click on OK.



16. Click on next.



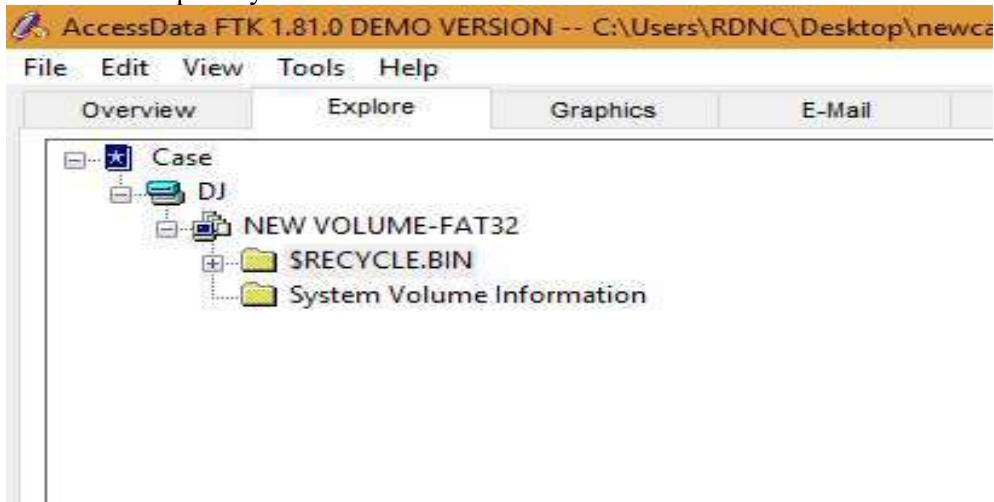
17. Click on Finish.



18. Files are being carving.



19. In the left panel you can see all the recovered files.

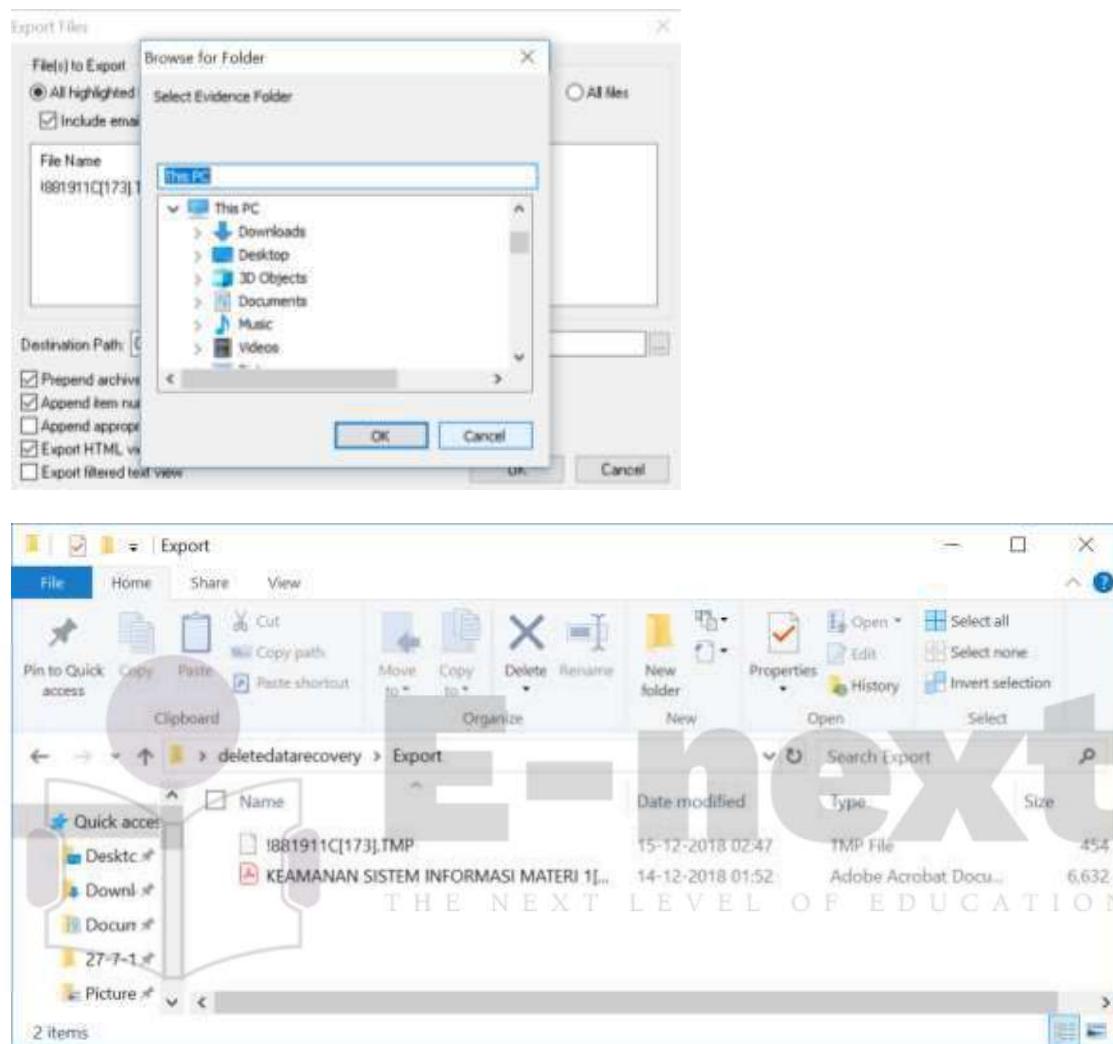


20. Click on the Deleted file tab-> Right click on any deleted file to export it

Evidence Items	File Status	File Category
4	KFF Alert Files: 0	Documents: 3830
	Bookmarked Items: 0	Spreadsheets: 0
5000	Bad Extension: 36	Databases: 0
0	Encrypted Files: 0	Graphics: 608
5000	From E-mail: 0	Multimedia: 4
0	Flagged Thumbnails: 0	E-mail Messages: 0
608	From Recycle Bin: 0	Executables: 0
5000	Duplicate Items: 2156	Archives: 1
0	OLE Subitems: 0	Folders: 33
0	Flagged Ignore: 0	Free/Space: 200
0	KFF Ignorable: 0	Other Known Type: 27
0	Data Carved Files: 0	Unknown Type: 217

Category	File Name	Subject	Cr Date	Mod Date
Documents	17A4521	Document	29-12-2018 09:23:12	21-12-2018 20:30:22
Documents	17B3971	Document	29-12-2018 09:23:12	21-12-2018 20:44:22
Graphics	17C3971	Document	15-12-2018 02:27:54	15-12-2018 02:47:02
TMP	17A2186D.TMP	Document	N/A	N/A
TMP	17C2186D.TMP	Document	15-12-2018 02:27:54	15-12-2018 02:50:30
PDF	17D.PDF	Document	08-12-2018 00:05:36	08-12-2018 00:05:38
TMP	17E1971C.TMP	Document	26-01-2019 10:45:26	26-01-2019 10:45:48

21. Browse and choose the destination folder to export the deleted file

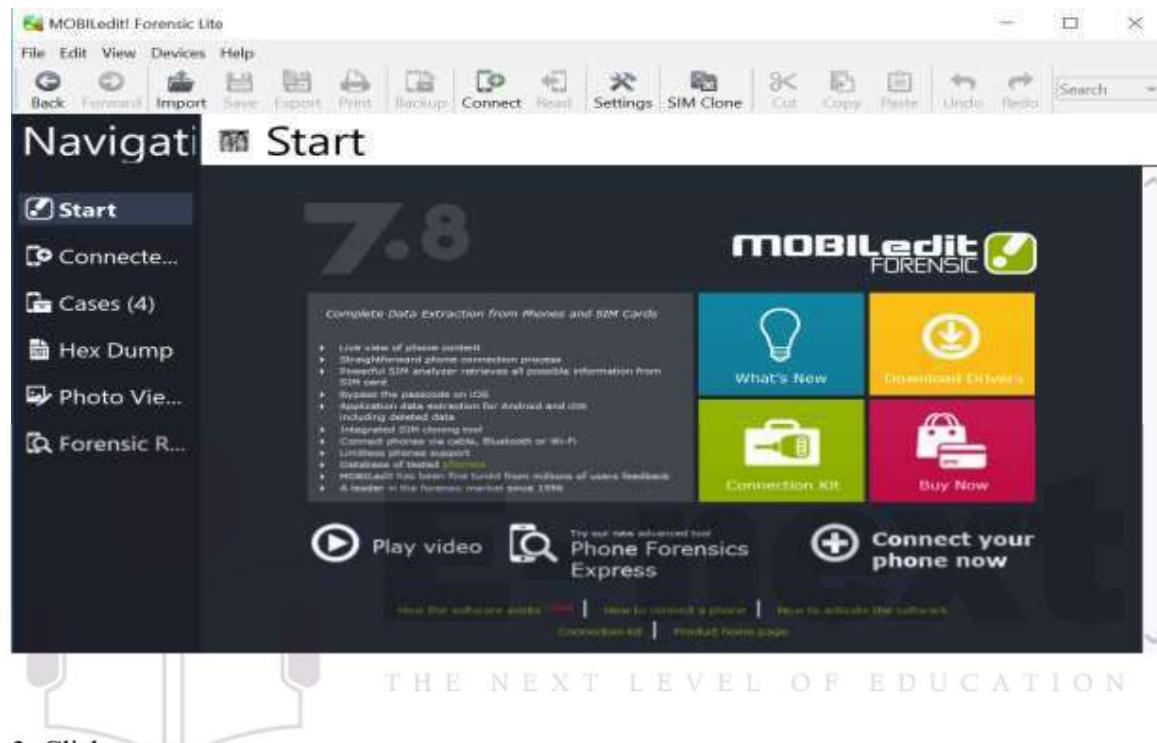


Practical No – 8

Aim: Acquisition of Cell phones and Mobile devices

Steps:

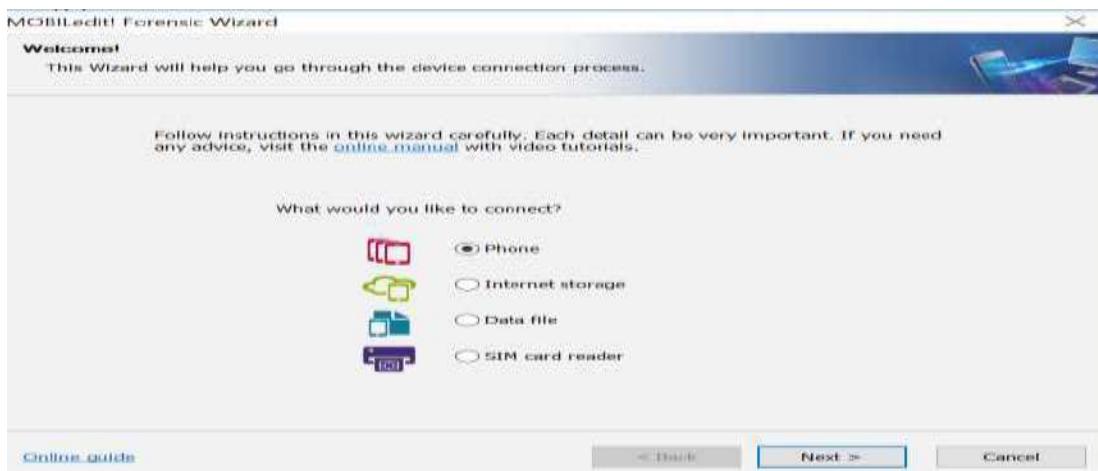
1. Download mobiledit forensic tool in mobile.
2. Open Mobiledit tool in PC.



3. Click on connect.



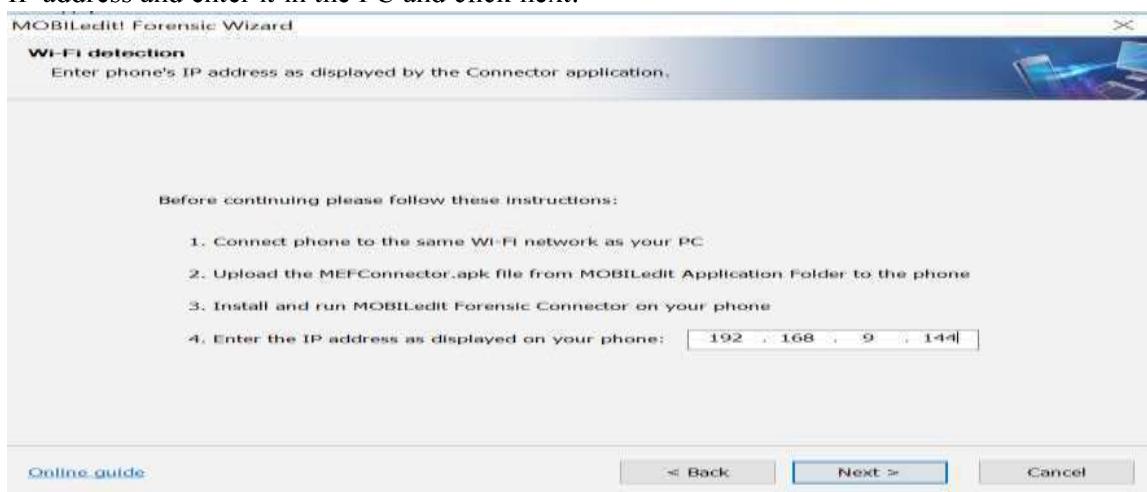
4. Connect your mobile device to the system. Click on phone > next.



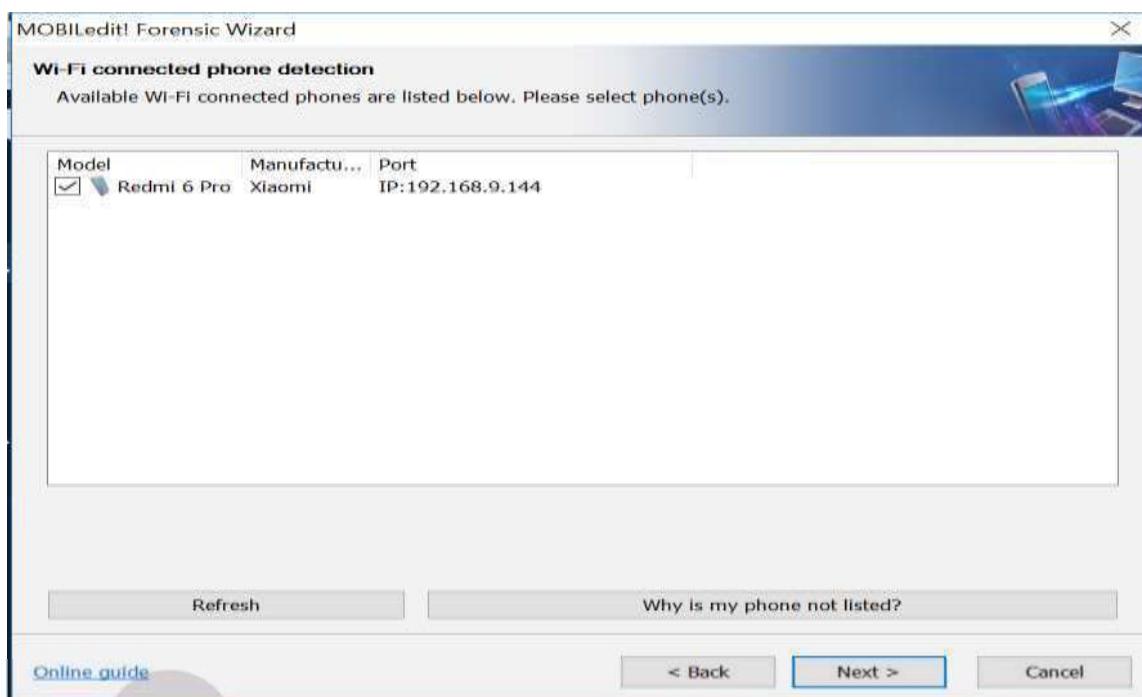
5. Click the connection



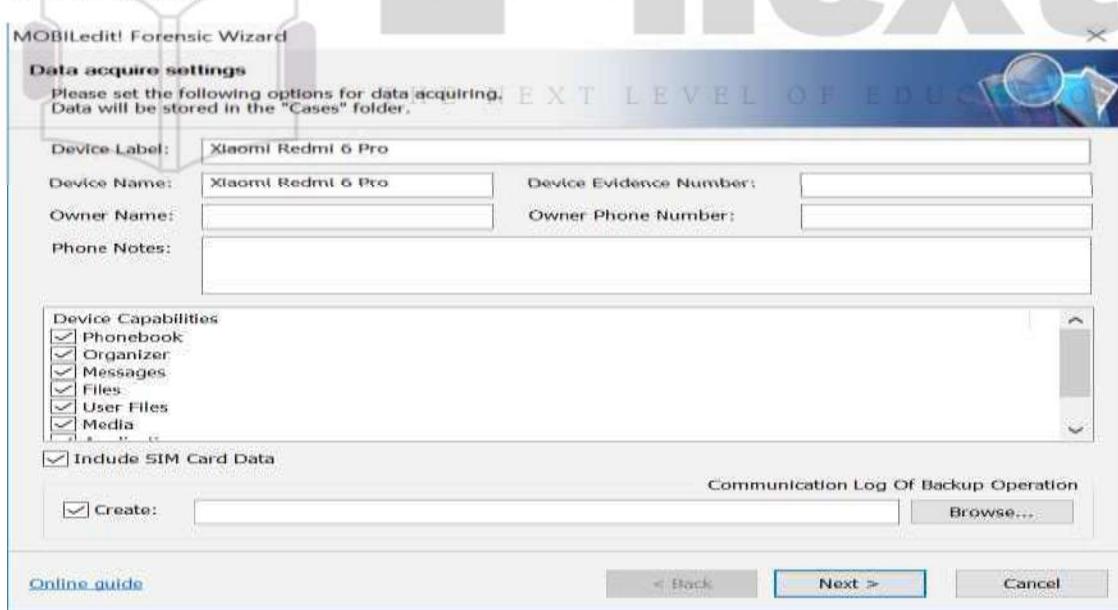
6. Open the mobiledit tool in phone and click on the type of connection (i.e Wifi) > Copy the IP address and enter it in the PC and click next.



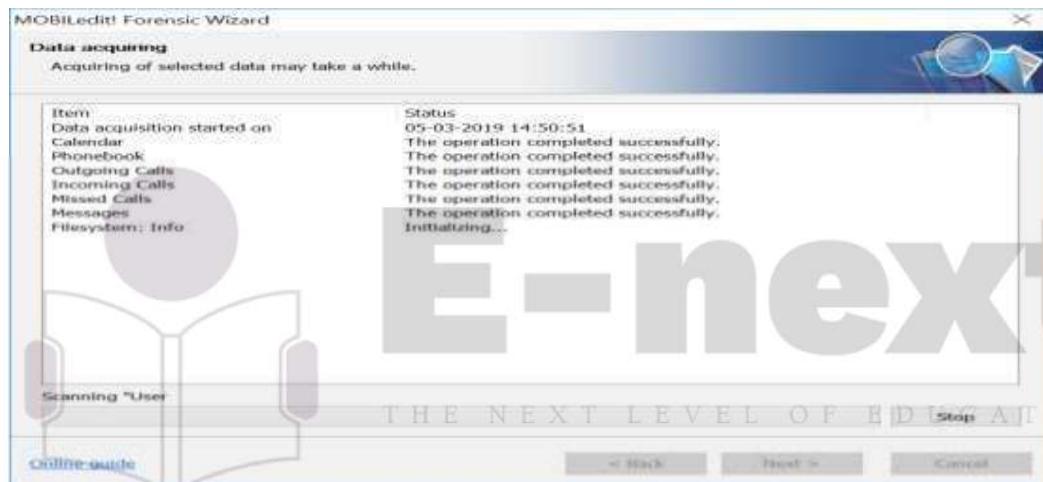
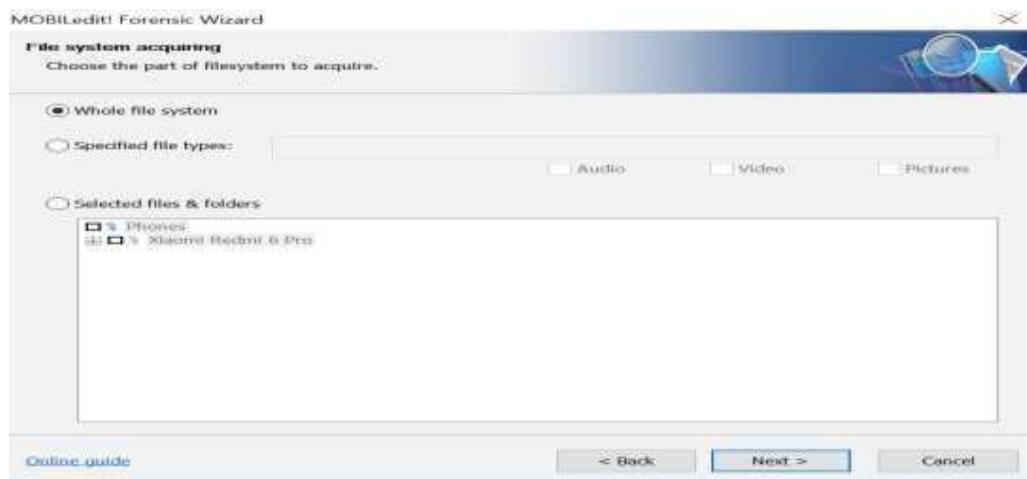
7. It shows the phone which is connected. Click on next.



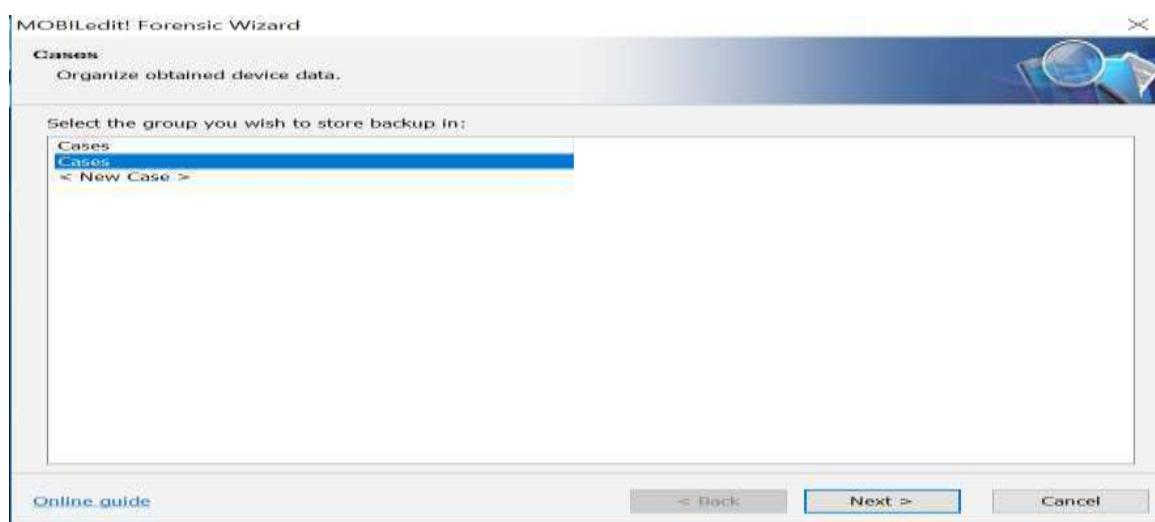
8. Click on next.



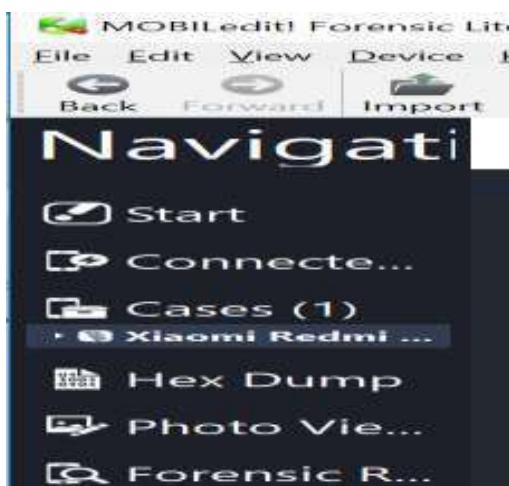
9. Click on whole system and click next.



10. Click on case and click next.



11. Click on your device in the left panel.



12. You can see all the files.

Name	Number
Ambulance	102
Fire	101
Jio-Complaint Helpline	198
Jio-General Helpline	199
Jio-Tele-verification Helpline	1977
Police	100
Railways	139

TX-SWIGGY
04-03-2019 01:23:59

VK-SWIGGY
04-03-2019 00:42:05

AD-ARWINF
03-03-2019 20:15:18

AX-MOJOPZ
03-03-2019 20:06:57

TX-CUREFT
03-03-2019 20:01:45

AD-LSKART
03-03-2019 14:17:48

AX-MOJOPZ
03-03-2019 20:06:57
Win Rs. 3,00,000 Paytm cash
Everyday just by playing games.
Install GameChamp app now!
<http://bit.ly/2VaTQh>

Practical No – 9

Aim: Email Forensics

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

Mail Service Providers

An email service provider (ESP) is a company that offers email marketing or bulk email services. An ESP may provide tracking information showing the status of email sent to each member of an address list. ESPs also often provide the ability to segment an address list into interest groups or categories, allowing the user to send targeted information to people who they believe will value the correspondence.

Here are nine features to look for when you select your business email service:

Spam Filter - Spam messages are a huge time waster. You don't want to spend your valuable time reading them. That's why you want an email service that has a system in place to detect and filter out inbox spam.

Reliability - Your business email provider needs to be up and running when you need it. Your email should always be available. Email downtime could result in lost or unhappy customers.

Integration - Some email services work well with other business tools such as calendars, and productivity suites. If your business relies heavily on such tools, consider an email package that integrates with the other tools you already use.

Security - With email hacks being a regular news item, you want your business email provider to offer strong measures to keep your accounts secure. You need to keep your messages safe and don't want any unauthorized use of your email account.

Ease of Use - As your business grows, more of your staff members need to create and use email accounts. Reduce staff training time by selecting an email service provider that's easy to use.

Archive Capabilities - The best business email providers provide a way for you to save, store, and organize your email messages and drafts. For many businesses, keeping an accurate and well-organized record of business communication is vital.

Advanced Features - When running a small business, advanced email features such as the ability to recall sent messages or schedule tasks within email can be important. Which advanced features are most important depends on your unique business needs.

Reputation - Your business email service provider needs to have a good reputation. Remember, your email address is one of the first pieces of information prospective clients see.

Storage - When selecting an email service provider, keep in mind the amount of storage space included with your account. You don't want to run out of space.

Types of Popular Email Service Providers are as follows:

1.Gmail:

One of the most popular and best email service providers, Gmail is used for personal and business communications alike. According to statistics reported by TechCrunch in 2016, over a billion people use Gmail.

Gmail has a good reputation and includes many advanced features such as the Undo Send feature and Email Forwarding. Since this service is owned by search engine giant, Google, naturally it includes a powerful search utility and filter system.

Google has also added strengthened security measures such as two-step verification and powerful spam filters to make it less likely that your account is hacked or that you receive junk messages. Finally, it integrates cleanly with popular productivity tools including Google Calendar and Google Docs.

2. Outlook

Microsoft's Outlook.com email provider is a strong option if you're looking for the best email provider. Statistics from Microsoft show that Outlook had over 400 million users in 2016.

This popular email package has the support and resources of tech giant Microsoft behind it. Outlook.com offers advanced features such as Clutter, which finds emails that are likely of low priority and separates them from your inbox. Another advanced Outlook.com feature is the ability to Undelete, or recover an email after you've accidentally discarded a message. Outlook integrates well with popular software including other Microsoft products.

3.iCloud Mail

iCloud email is a possible email choice if you frequently access your email package from your Apple mobile device. Apple employs several security features to make sure that your iCloud account is not compromised including two-step verification or two-factor authentication. There's also a spam filter.

4. Yahoo Mail

Yahoo! was one of the early Internet companies, dating back to 1994. Yahoo! Mail is popular with many users. In 2016, it was announced that the company was acquired by Verizon. Despite the recent changes to Yahoo! ownership, you can still sign up for a Yahoo! Mail account. Some Yahoo! Mail features you can benefit from if you choose it as your email provider include:

Auto deletion of Trash messages after 90 days

- Huge storage capacity (1 TB)
- Built-in web search tool, calendar, and notepad
- Spam filters and SSL encryption

5. AOL Mail

AOL is another early Internet company. In the 1980s the company was known as America Online. It was purchased by Verizon in 2015. The email component of the organization remains a popular and strong service that has earned its place on this list of the best email services.

Key AOL Mail features include advanced spam filters and virus protection. It's also known for the ability to personalize your email address with the MyAddress feature that lets you select your own email domain name.

6. Zoho Mail

Although Zoho Mail has several premium levels available, there is also a free level available that allows you to have up to 25 users. For many small businesses, this will be enough—so we have included the email service on our list of the best free email providers.

With the free level of Zoho Mail, you are limited to 5 GB of storage per user. It does include antivirus protection and spam filtering. This email service integrates with other Zoho productivity tools such as calendar, tasks, and notes.

THE NEXT LEVEL OF EDUCATION

Email Protocols

E-mail Protocols are set of rules that help the client to properly transmit the information to or from the mail server

The most commonly used Email protocols on the internet - POP3, IMAP and SMTP. Each one of them has specific function and way of work.

POP3

Post Office Protocol version 3 (POP3) is a standard mail protocol used to receive emails from a remote server to a local email client. POP3 allows you to download email messages on your local computer and read them even when you are offline. Note, that when you use POP3 to connect to your email account, messages are downloaded locally and removed from the email server. This means that if you access your account from multiple locations, that may not be the best option for you. On the other hand, if you use POP3, your messages are stored on your local computer, which reduces the space your email account uses on your web server.

By default, the POP3 protocol works on two ports:

Port 110 - this is the default POP3 non-encrypted port

Port 995 - this is the port you need to use if you want to connect using POP3 securely

IMAP

The Internet Message Access Protocol (IMAP) is a mail protocol used for accessing email on a remote web server from a local client. IMAP and POP3 are the two most commonly used Internet mail protocols for retrieving emails. Both protocols are supported by all modern email clients and web servers.

While the POP3 protocol assumes that your email is being accessed only from one application, IMAP allows simultaneous access by multiple clients. This is why IMAP is more suitable for you if you're going to access your email from different locations or if your messages are managed by multiple users.

By default, the IMAP protocol works on two ports:

Port 143 - this is the default IMAP non-encrypted port

Port 993 - this is the port you need to use if you want to connect using IMAP securely

SMTP

SMTP stands for Simple Mail Transfer Protocol. It was first proposed in 1982. It is a standard protocol used for sending e-mail efficiently and reliably over the internet. Simple Mail Transfer Protocol (SMTP) is the standard protocol for sending emails across the Internet.

By default, the SMTP protocol works on three ports:

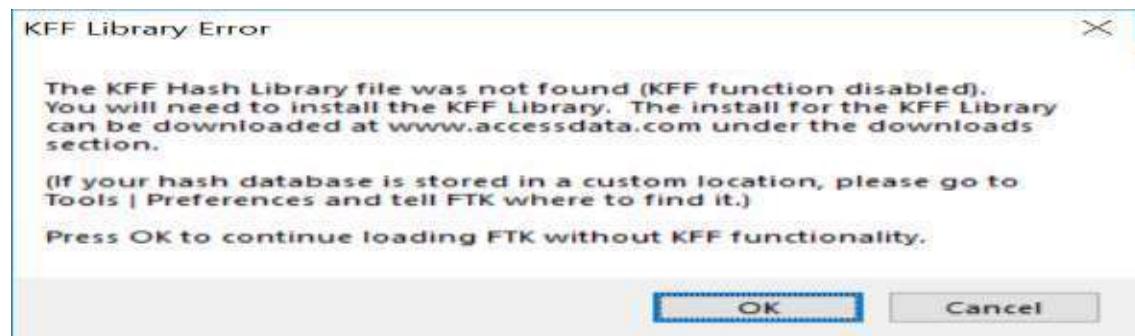
Port 25 - this is the default SMTP non-encrypted port

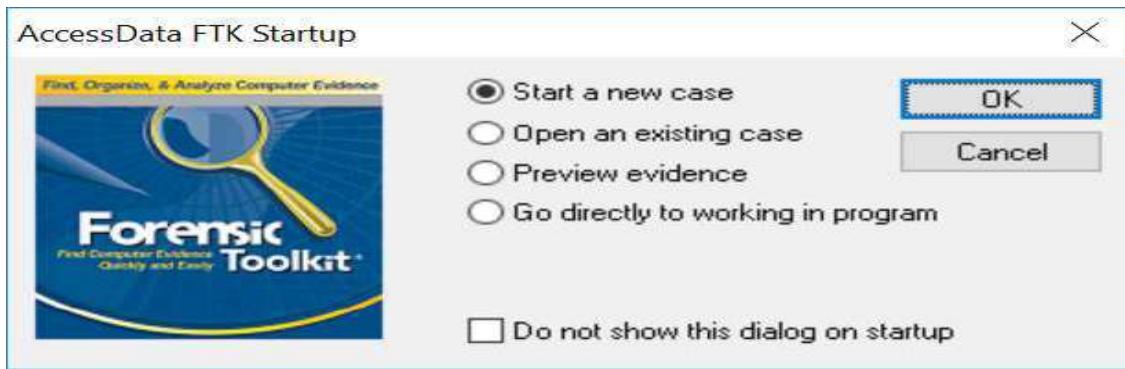
Port 2525 - this port is opened on all SiteGround servers in case port 25 is filtered (by your ISP for example) and you want to send non-encrypted emails with SMTP

Port 465 - this is the port used if you want to send messages using SMTP securely

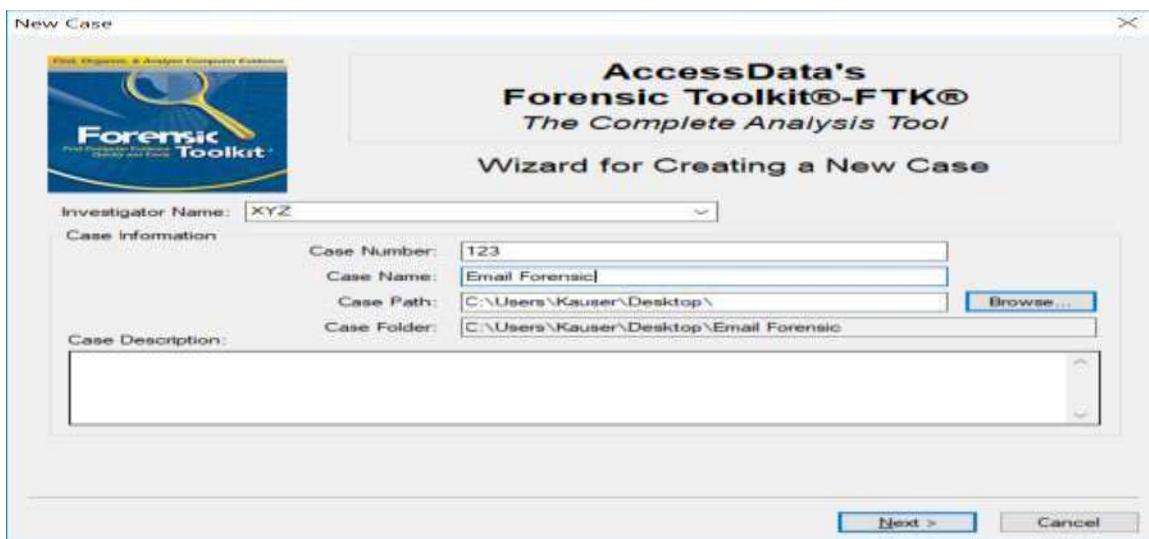
Recovering email using AccessData FTK:

1. Start AccessData FTK by right-clicking the AccessData FTK desktop icon, clicking Run as administrator, and clicking Continue in the UAC message box (if you're using Vista). If you're prompted with a warning message and/or notification (see Figure below), click OK as needed to continue. If asked whether you want to save the existing default case, click Yes.





2. When the AccessData FTK Startup dialog box opens, click Start a new case, and then click OK.
3. In the New Case dialog box, type your name for the investigator name, and type the case number and case name. Click Browse, navigate to and click your work folder, click OK, and then click Next.
4. In the Case Information dialog box, enter your investigator information, and then click Next.
5. Click Next until you reach the Refine Case - Default dialog box, shown in Figure below.
6. Click the Email Emphasis button, and then click Next.
7. Click Next until you reach the Add Evidence to Case dialog box, and then click the Add Evidence button.
8. In the Add Evidence to Case dialog box, click the Individual File option button (see Figure below), and then click Continue.
9. In the Select File dialog box, navigate to your work folder, click the Jim_shu's.pst file, and then click Open.
10. In the Evidence Information dialog box, click OK.



FTK Report Wizard - Case Information

Forensic Examiner Information

The following information will appear on the Case Information page of the report:

Agency/Company:	R D National		
Examiner's Name:	XYZ		
Address:	Linking Road,Mumbai		
Phone:	1234567	Fax:	12345
E-Mail:	xyz@gmail.com		
Comments:	none		

< Back Next > Cancel

Case Log Options

Case Log Options

The case log is a text file named FTK.log in the case folder. It gets created automatically by FTK and contains a record of events that occur during the course of the case. You can choose which type of events you would like to be logged.

You can also add your own comments to the log file at any time by selecting "Add Case Log Entry..." under the "Tools" menu item, and you can view the log file by selecting "View Case Log" under the "Tools" menu item.

Events to go in the Case Log	
<input checked="" type="checkbox"/> Case and evidence events	Events related to the addition and processing of file items when evidence is added or when using Analysis Tools later in the case.
<input checked="" type="checkbox"/> Error messages	Events related to any error conditions encountered during the case.
<input checked="" type="checkbox"/> Bookmarking events	Events related to the addition and modification of bookmarks.
<input checked="" type="checkbox"/> Searching events	Events related to searching. All search queries and resulting hit counts will be recorded.
<input checked="" type="checkbox"/> Data carving / Internet searches	Events related to special data carving or internet keyword searches that are performed during the case.
<input checked="" type="checkbox"/> Other events	Other events not related to the above, such as copying, viewing, and ignoring files.

< Back Next > Cancel

Evidence Processing Options

Processes to Perform

Evidence is added to a case in several steps. Some of the processes are always performed, while others are optional, depending on your needs and time/resource constraints.

<input checked="" type="checkbox"/> MD5 Hash	An MD5 hash is a 16 byte value generated based upon a file's content. It is used to uniquely identify files. Hashes can be used to verify a file's integrity, or to identify duplicate files. MD5 hashes are used by the KFF to identify known files.
<input checked="" type="checkbox"/> SHA1 Hash	A SHA1 hash is a 20 byte value. The SHA1 hashing algorithm is newer than MD5, but is not yet as widely used.
<input checked="" type="checkbox"/> KFF Lookup	KFF (Known File Filter) is a utility that compares MD5 file hashes against a database of MD5 hashes from known files. The purpose of KFF is to eliminate files known to be unimportant, or to alert the investigator to known illicit or dangerous files.
<input checked="" type="checkbox"/> Entropy Test	For unknown file types, an entropy test is used to determine whether the file's data is compressed or encrypted. Such files contain no plain text and will not be indexed. Unnecessary indexing of such files can waste large amounts of time and resources.
<input checked="" type="checkbox"/> Full Text Index	The Forensic Toolkit includes a very powerful search engine, dSearch, which enables the investigator to do instantaneous searching of textual data. In order to take advantage of this search feature, the data must first be indexed.
<input checked="" type="checkbox"/> Store Thumbnails	Create and store thumbnails for all graphics in the case. This option speeds up browsing through the Graphics view at the expense of consuming more space in the case folder.
<input checked="" type="checkbox"/> Decrypt EFS Files	Automatically locate and attempt to decrypt EFS encrypted files found on NTFS partitions within the case. (Requires AccessData Password Recovery Toolkit 5.20 or newer)
<input checked="" type="checkbox"/> File Listing Database	Create a Microsoft Access (Jet) database containing a list of all files in the case. The attributes included are based on the Preprocessing File Listing Database Column Setting. This database can be recreated with custom column settings in Copy Special.
<input checked="" type="checkbox"/> HTML File Listing	Create an HTML version of the File Listing.
<input checked="" type="checkbox"/> Data Carve	Automatically find specific file types embedded in other files and from free space. Retrieve results using Data Carving Option on Tools Menu.
<input checked="" type="checkbox"/> Registry Reports	Generate common registry reports during preprocessing.

< Back **Next >** Cancel

Refine Case - Default

Refine Case - Default

In order to save time and resources, and/or to eliminate irrelevant data, you may choose to exclude certain kinds of data from the case. Here, you can choose default inclusion/exclusion settings that will apply to each evidence item that gets added to the case. To exclude data, make any changes to the settings below. Note: any items that get excluded will not appear anywhere in the case, and will be inaccessible.

<input type="button" value="Include All Items"/>	<input type="button" value="Optimal Settings"/>	<input style="background-color: #0070C0; color: white; border: 1px solid #0070C0; padding: 2px 10px; border-radius: 5px; font-weight: bold; font-size: 10pt; text-decoration: none; text-align: center; margin-right: 10px;" type="button" value="Email Emphasis"/>	<input type="button" value="Text Emphasis"/>	<input type="button" value="Graphics Emphasis"/>												
<p>Unconditionally Add</p> <p><input type="checkbox"/> File Slack (data beyond the end of the logical file but within the area allocated to that file by the file system) <input type="checkbox"/> Free Space (areas in the file system not currently allocated to any file, but possibly containing deleted file data) <input type="checkbox"/> KFF Ignorable Files (files found by KFF to be forensically unimportant, i.e., OS system files, known applications, etc.) <input type="checkbox"/> Extract files from KFF ignorable containers</p> <p>Conditionally Add</p> <p>Add other items to the case only if they satisfy: BOTH the file status and the file type criteria</p> <table border="0"> <tbody> <tr> <td>File Status Criteria</td> <td>File Type Criteria</td> </tr> <tr> <td>Deletion Status: <input type="radio"/> Deleted <input type="radio"/> Not deleted <input type="radio"/> Either</td> <td>Encryption Status: <input type="radio"/> Encrypted <input type="radio"/> Not encrypted <input type="radio"/> Either</td> <td>Email Status: <input checked="" type="radio"/> From email <input type="radio"/> Not from email <input type="radio"/> Either</td> <td><input checked="" type="checkbox"/> Documents <input checked="" type="checkbox"/> Spreadsheets <input checked="" type="checkbox"/> Databases <input checked="" type="checkbox"/> Graphics <input checked="" type="checkbox"/> Multimedia <input checked="" type="checkbox"/> Email msgs</td> <td><input type="checkbox"/> Executables <input checked="" type="checkbox"/> Archives <input type="checkbox"/> Folders <input checked="" type="checkbox"/> Other Known <input checked="" type="checkbox"/> Unknown</td> </tr> <tr> <td><input type="checkbox"/> Include Duplicate Files</td> <td></td> <td><input type="checkbox"/> OLE Streams</td> <td></td> <td></td> </tr> </tbody> </table>					File Status Criteria	File Type Criteria	Deletion Status: <input type="radio"/> Deleted <input type="radio"/> Not deleted <input type="radio"/> Either	Encryption Status: <input type="radio"/> Encrypted <input type="radio"/> Not encrypted <input type="radio"/> Either	Email Status: <input checked="" type="radio"/> From email <input type="radio"/> Not from email <input type="radio"/> Either	<input checked="" type="checkbox"/> Documents <input checked="" type="checkbox"/> Spreadsheets <input checked="" type="checkbox"/> Databases <input checked="" type="checkbox"/> Graphics <input checked="" type="checkbox"/> Multimedia <input checked="" type="checkbox"/> Email msgs	<input type="checkbox"/> Executables <input checked="" type="checkbox"/> Archives <input type="checkbox"/> Folders <input checked="" type="checkbox"/> Other Known <input checked="" type="checkbox"/> Unknown	<input type="checkbox"/> Include Duplicate Files		<input type="checkbox"/> OLE Streams		
File Status Criteria	File Type Criteria															
Deletion Status: <input type="radio"/> Deleted <input type="radio"/> Not deleted <input type="radio"/> Either	Encryption Status: <input type="radio"/> Encrypted <input type="radio"/> Not encrypted <input type="radio"/> Either	Email Status: <input checked="" type="radio"/> From email <input type="radio"/> Not from email <input type="radio"/> Either	<input checked="" type="checkbox"/> Documents <input checked="" type="checkbox"/> Spreadsheets <input checked="" type="checkbox"/> Databases <input checked="" type="checkbox"/> Graphics <input checked="" type="checkbox"/> Multimedia <input checked="" type="checkbox"/> Email msgs	<input type="checkbox"/> Executables <input checked="" type="checkbox"/> Archives <input type="checkbox"/> Folders <input checked="" type="checkbox"/> Other Known <input checked="" type="checkbox"/> Unknown												
<input type="checkbox"/> Include Duplicate Files		<input type="checkbox"/> OLE Streams														

< Back **Next >** Cancel

Add Evidence to Case

Add Evidence

Any number of evidence items can be added to the case. There are several types of evidence items:

Acquired image of drive:
Local drive:
Folder:
Individual File:
The default refinement options, set previously, can be overridden independently for each evidence item, and additional types of refinements can also be made. These refinements can include the exclusion of date/size ranges, as well as specific folders. To make these further refinements, highlight an evidence item in the list and press Refine Evidence - Advanced...

Evidence Information

Evidence Location: C:\Users\Kauser\Desktop\cyber\pracs\Jim_shu's.pst
 Evidence Display Name: Jim_shu's
 Evidence Identification Name/Number: Jim Shu
 Comment: none

Local Evidence Time Zone: Choose time zone for evidence ...

OK Cancel

Add Evidence... Display Name

< Back Next > Cancel

Add Evidence to Case

Add Evidence

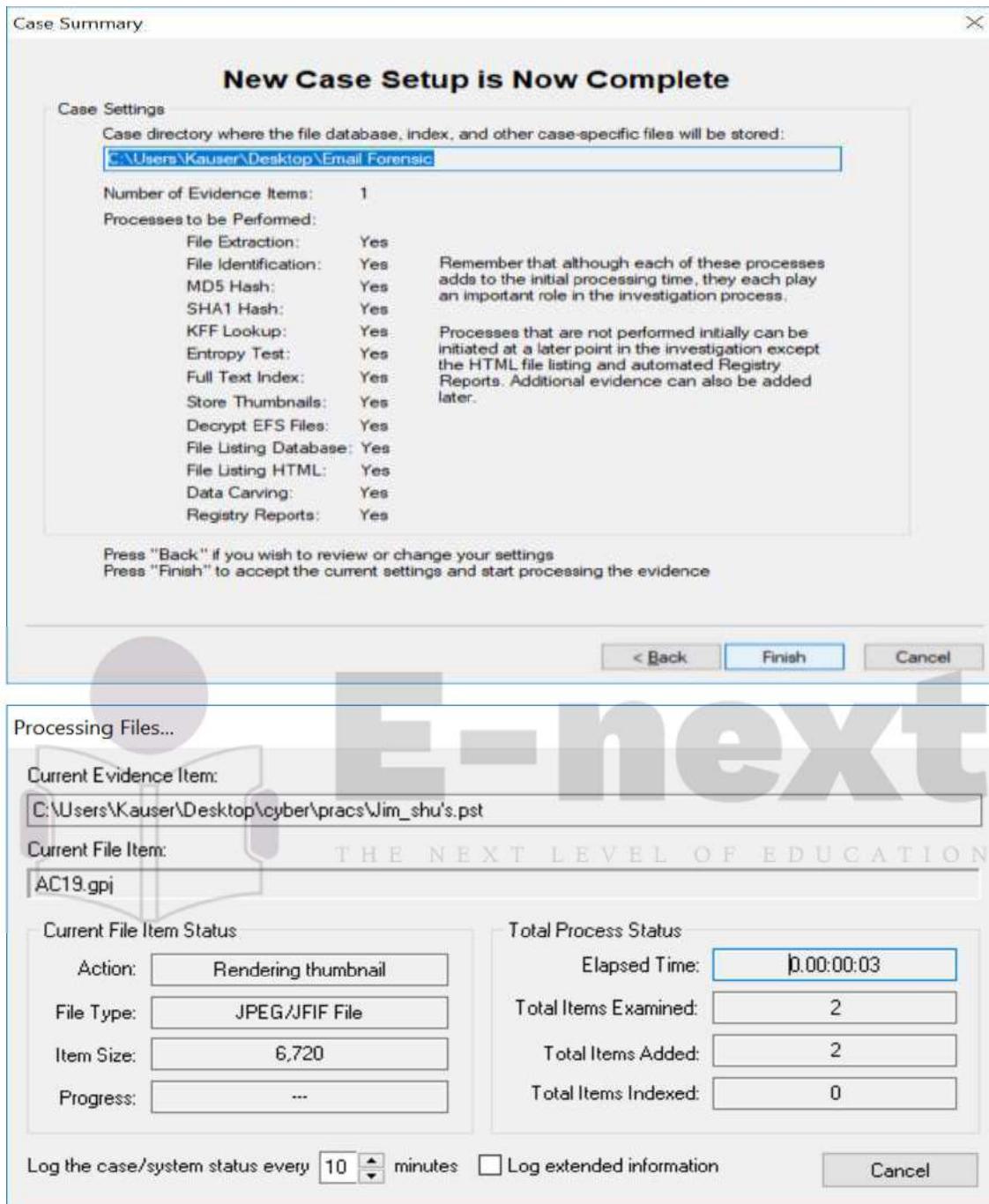
Any number of evidence items can be added to the case. There are several types of evidence items:

Acquired image of drive: Several formats supported, can be an image of a logical or physical drive
Local drive: Can be a logical or physical drive
Folder: Adds all files in the specified folder, including contents of subfolders
Individual File: Adds a single file. NOTE: Disk image files should be added as acquired images.

The default refinement options, set previously, can be overridden independently for each evidence item, and additional types of refinements can also be made. These refinements can include the exclusion of date/size ranges, as well as specific folders. To make these further refinements, highlight an evidence item in the list and press Refine Evidence - Advanced...

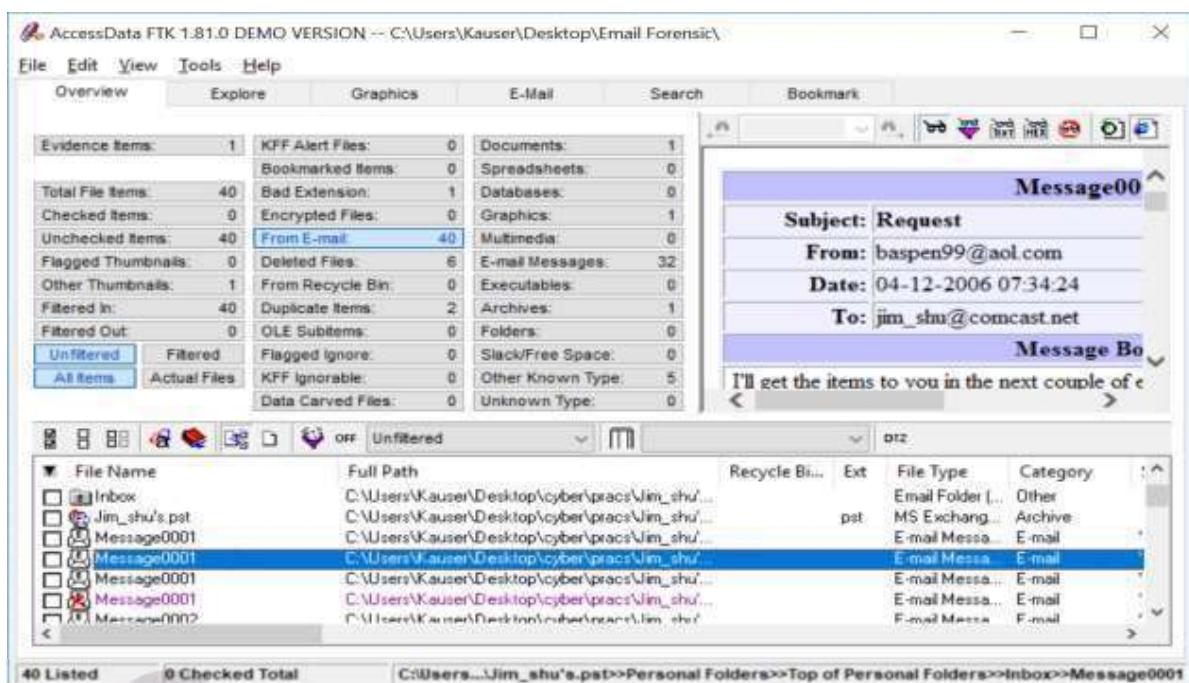
Add Evidence...	Edit Evidence...	Remove Evidence	Refine Evidence - Advanced...			
Display Name Jim_shu's	Source C:\Users\Kau...	Name/Nu... Jim Shu	Type Individual f...	Refined N	Time Zone N/A	Comment none

< Back Next > Cancel



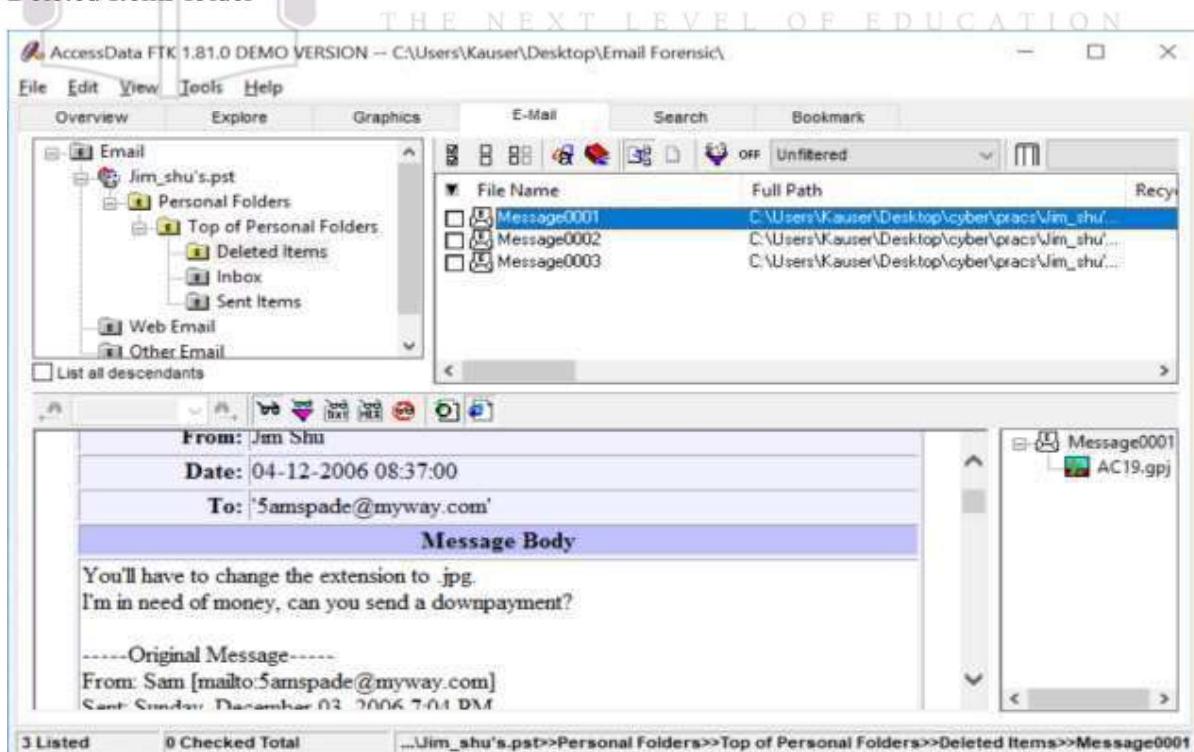
11. When the Add Evidence to Case dialog box opens, click Next. In the Case summary dialog box, click Finish.

12. 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 (see Figure below).

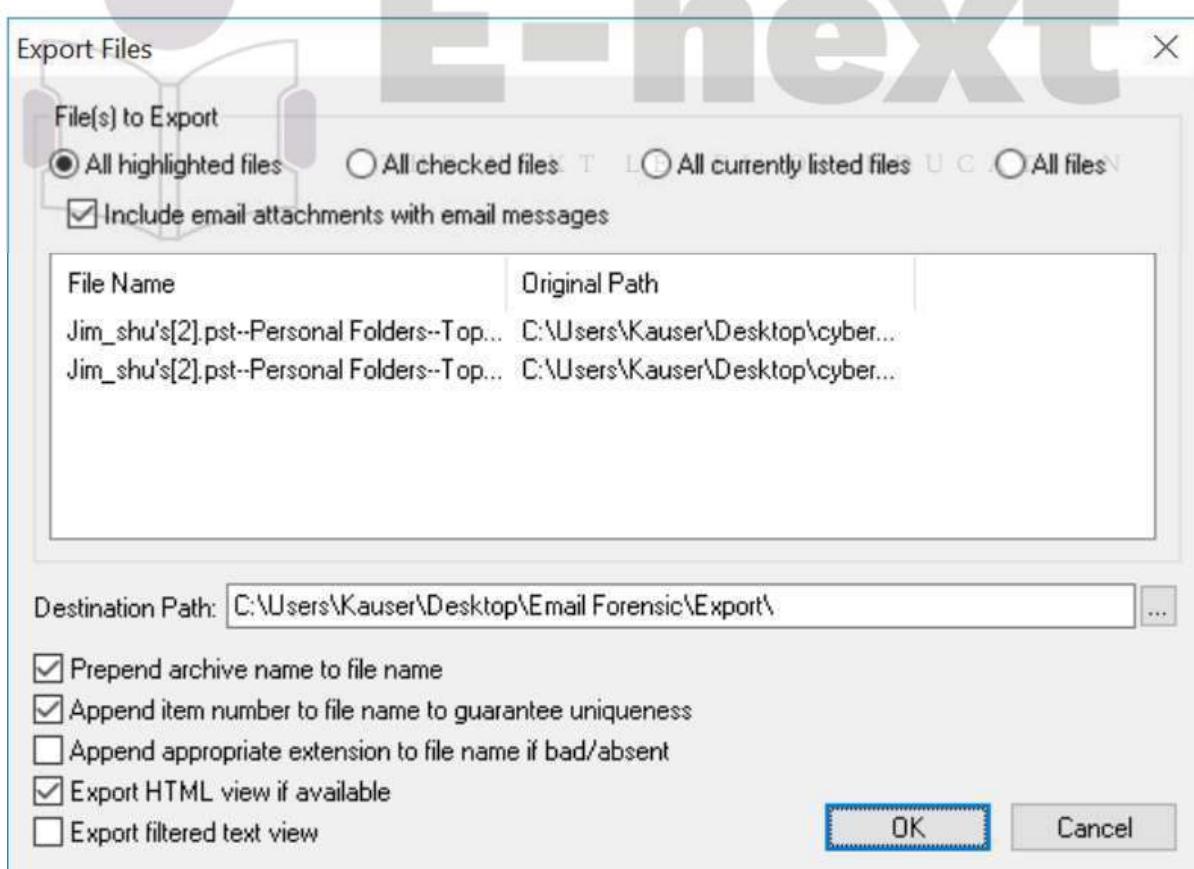
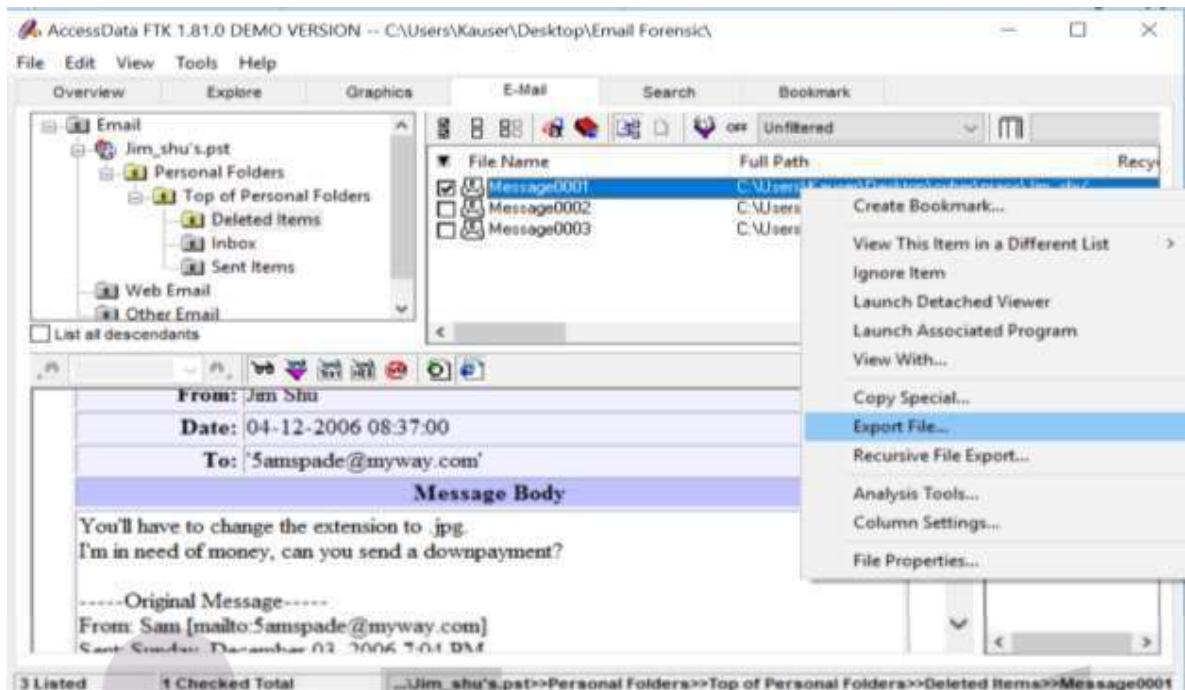


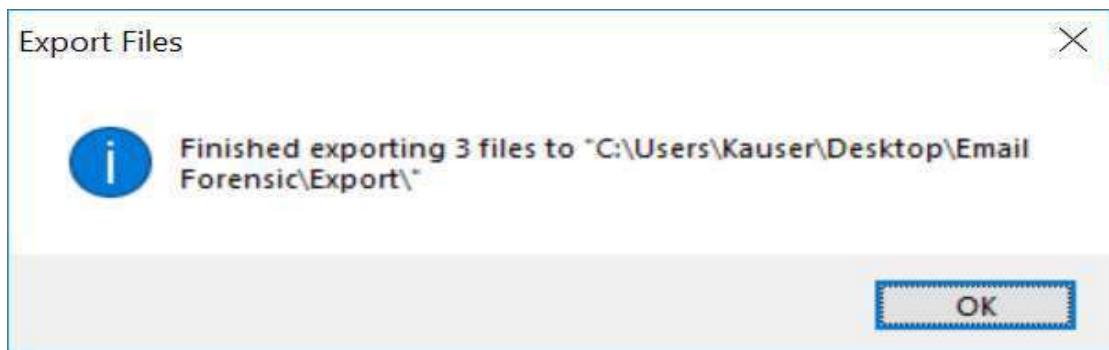
- For email recovery follow following steps:

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



2. Right-click Message0010 in the File List pane and click Export File. In the Export Files dialog box, click OK





3. Open the Export folder to view the Email Files, Open the HTML file in browser

Message0001

Subject:	RE: Bike spec's
From:	Jim Shu
Date:	04-12-2006 08:37:00
To:	'Samspade@myway.com'

Message Body

You'll have to change the extension to .jpg.
I'm in need of money, can you send a downpayment?

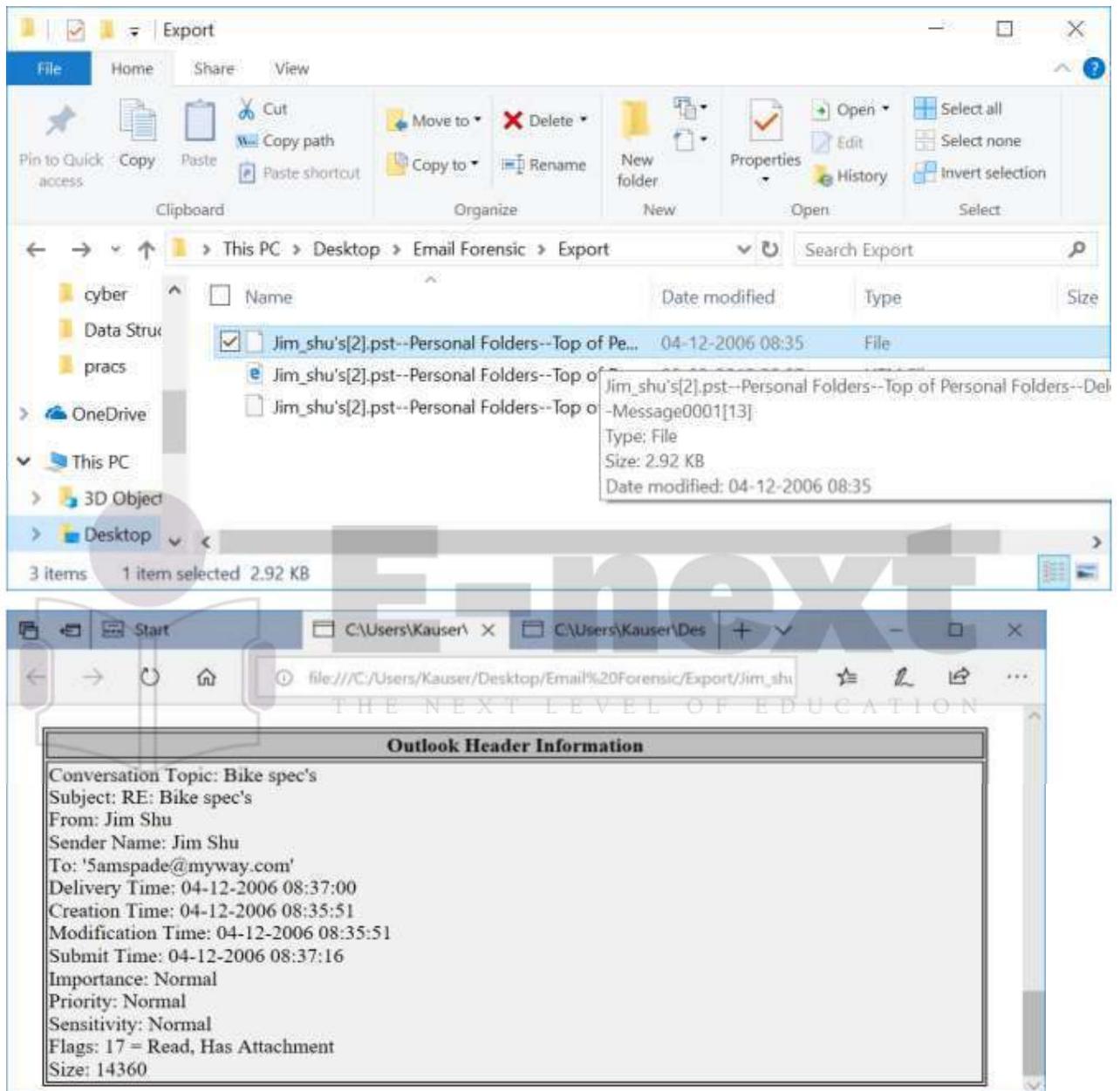
-----Original Message-----
 From: Sam [mailto:Samspade@myway.com]
 Sent: Sunday, December 03, 2006 7:04 PM
 To: Jim_shu@comcast.net
 Subject: RE: Bike spec's

I think I can raise another \$5 for you. Do you have something I can look at yet?

--- On Sun 12/03, Jim Shu <Jim_shu@comcast.net> wrote:

- For analyzing header follow following steps:

1. Right Click the file type and Rename it to HTML and open in browser to view header information



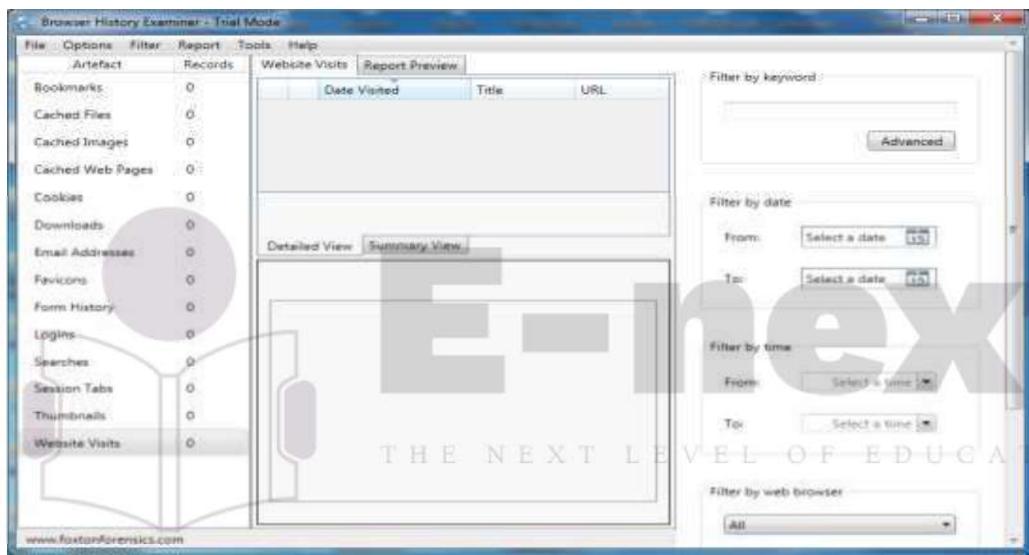
Practical No – 10

Aim: Web Browser Forensics

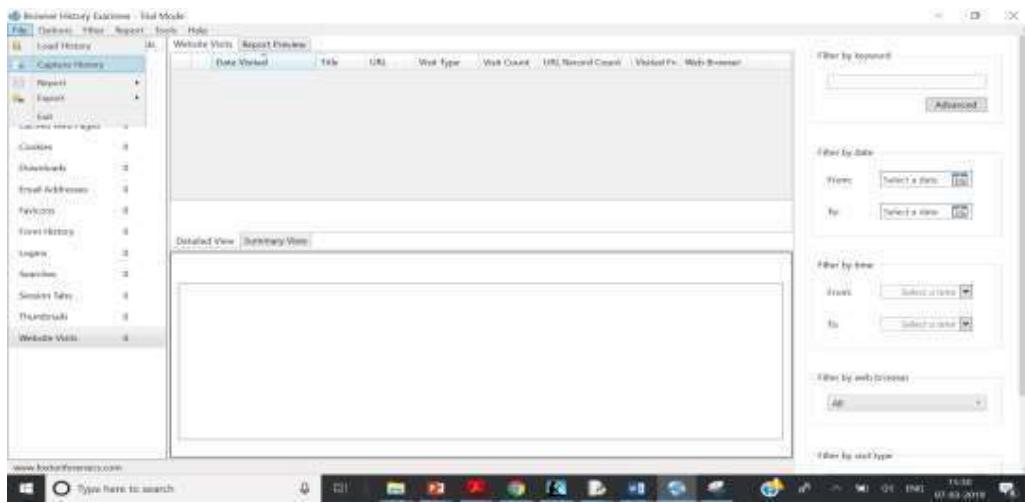
- Web Browser working
- Forensics activities on browser
- Cache / Cookies analysis
- Last Internet activity

Steps:

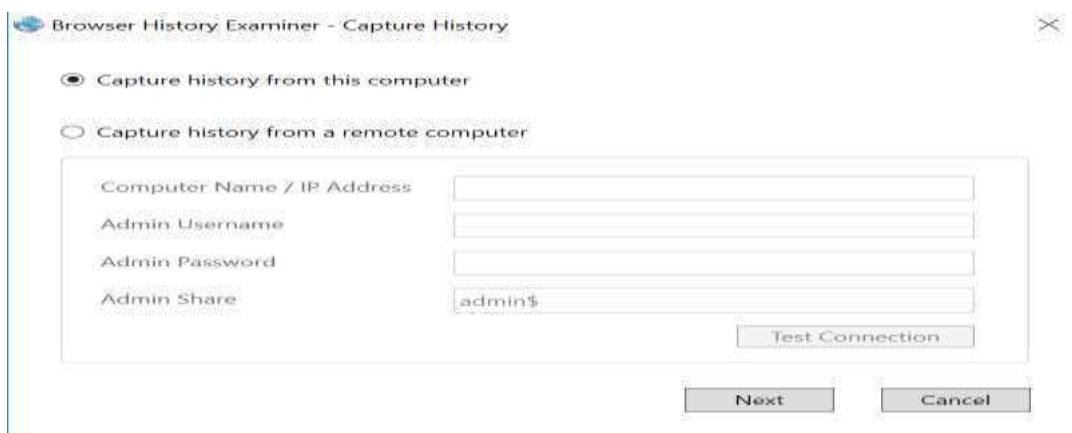
1. Open BrowserHistoryExaminer.



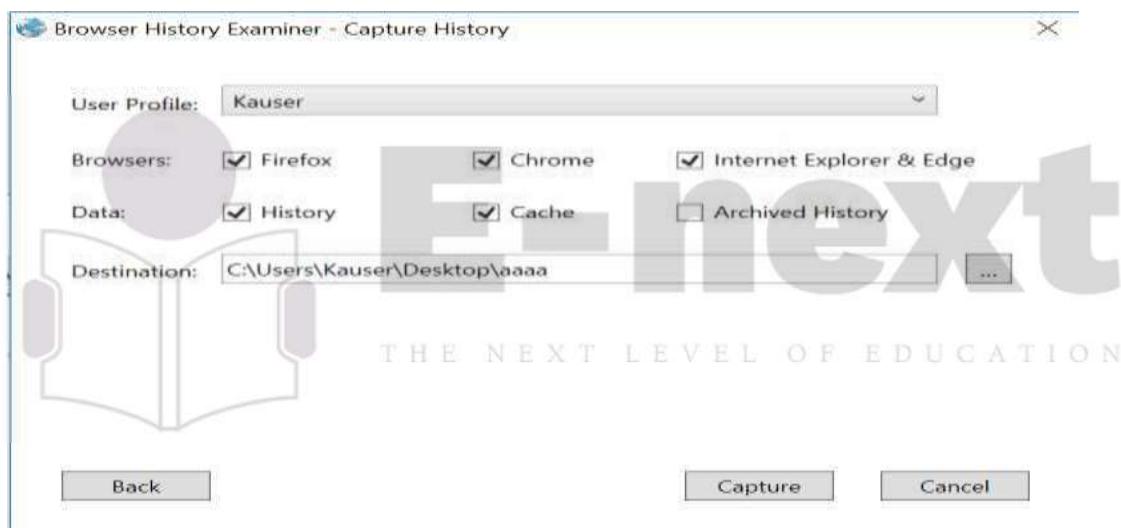
2. Click on file > Capture History.



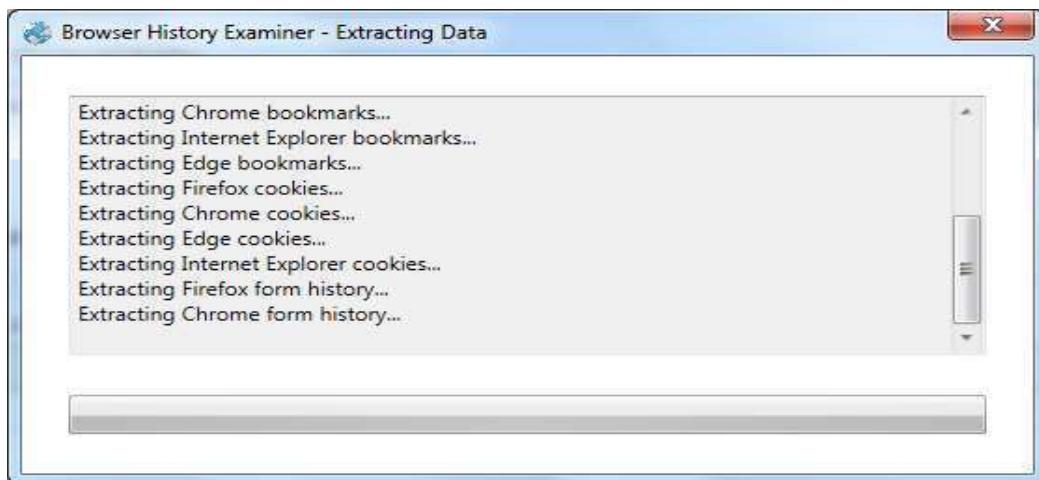
3. Select the capture folder and click on next.



4. Enter the destination to capture the data.



5. The History is been extracting.



6. The data has been retrieved.

File Options Filter Report Tools Help

Artifact Records

Website Visits Report Preview

Date Visited	Title	URL	Visit Type	Visit Count	URL Record Count	Visited By
06-03-2019 07:51:50	Browser History	https://www.firebaseio.com/	Link	1	1	https://www.firebaseio.com/
06-03-2019 07:51:48	Browser History	https://www.firebaseio.com/	Link	1	1	https://www.firebaseio.com/
06-03-2019 07:50:28	Home Legitify	https://legitify.com/	Link	1	1	https://legitify.com/
06-03-2019 07:50:28	Home Legitify	https://legitify.com/	Link	1	1	https://legitify.com/
06-03-2019 07:49:43	The Best Open	https://114.4.13.108/	Link	1	1	
06-03-2019 07:40:51	Open source bin	https://www.gutenberg.org/	Other	1	1	
06-02-2019 07:48:40	Browser History	https://www.firebaseio.com/	Other	2	2	https://www.firebaseio.com/
06-03-2019 07:48:35	Browser History	https://www.firebaseio.com/	Link	2	2	https://www.firebaseio.com/

Visiting 25/25 records

Filter by keyword: Advanced

From: To:

Filter by time: From: To:

Filter by web browser: All

Filter by visit type: All

Website Visit Count - 06-03-2019 to 06-03-2019

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

www.firebaseio.com

7. On the left panel click on bookmarks.

File Options Filter Report Tools Help

Artifact Records

Bookmarks Report Preview

Date Added	Last Modified	Title	URL	Web-Browser
06-01-2018 07:33:19		Format of Request to be	https://real.googleักษ	Chrome
06-01-2018 07:31:54		Format of Request to be	https://real.googleักษ	Chrome
14-12-2018 09:00:29		Welcome:	http://open.firebaseio.com/	Chrome
21-09-2018 01:16:56		Member Profile	https://114.4.13.108/	Chrome
30-01-2018 07:41:47	30-01-2018 07:41:47	Recent Tags	place_type:district:148	Firefox
30-01-2018 07:41:45	30-01-2018 07:41:47	Most Visited	place_type:district:148	Firefox
30-01-2018 07:41:44	30-01-2018 07:41:44	Getting Started	https://www.mozilla.org/	Firefox
30-01-2018 07:41:43	30-01-2018 07:41:43	Help and Tutorials	https://support.mozilla.org/	Firefox
30-01-2018 07:41:43	30-01-2018 07:41:43	Customize Firefox	https://www.mozilla.org/	Firefox
30-01-2018 07:41:43	30-01-2018 07:41:43	Get Involved	https://www.mozilla.org/	Firefox
30-01-2018 07:41:43	30-01-2018 07:41:43	About Us	https://www.mozilla.org/	Firefox
18-01-2018 07:25:20		UP Police Recruitment 21	https://www.recruitment	Chrome
06-10-2017 06:16:38		Redmi 4A (Grey, 16GB)	https://www.snapdeal.in/	Chrome
01-09-2017 07:37:45		MSI SWIFT	file:///C:/Users/akshay/Desktop/	Chrome
		Suggested Sites	https://explore.microsoft.com/	Internet Explorer
		Web Site Gallery	https://go.microsoft.com/	Internet Explorer

Visiting 18/18 records

Filter by keyword: Advanced

From: To:

Filter by time: From: To:

Filter by web browser: All

Filter:

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

www.firebaseio.com

8. On the left panel click on cached files.

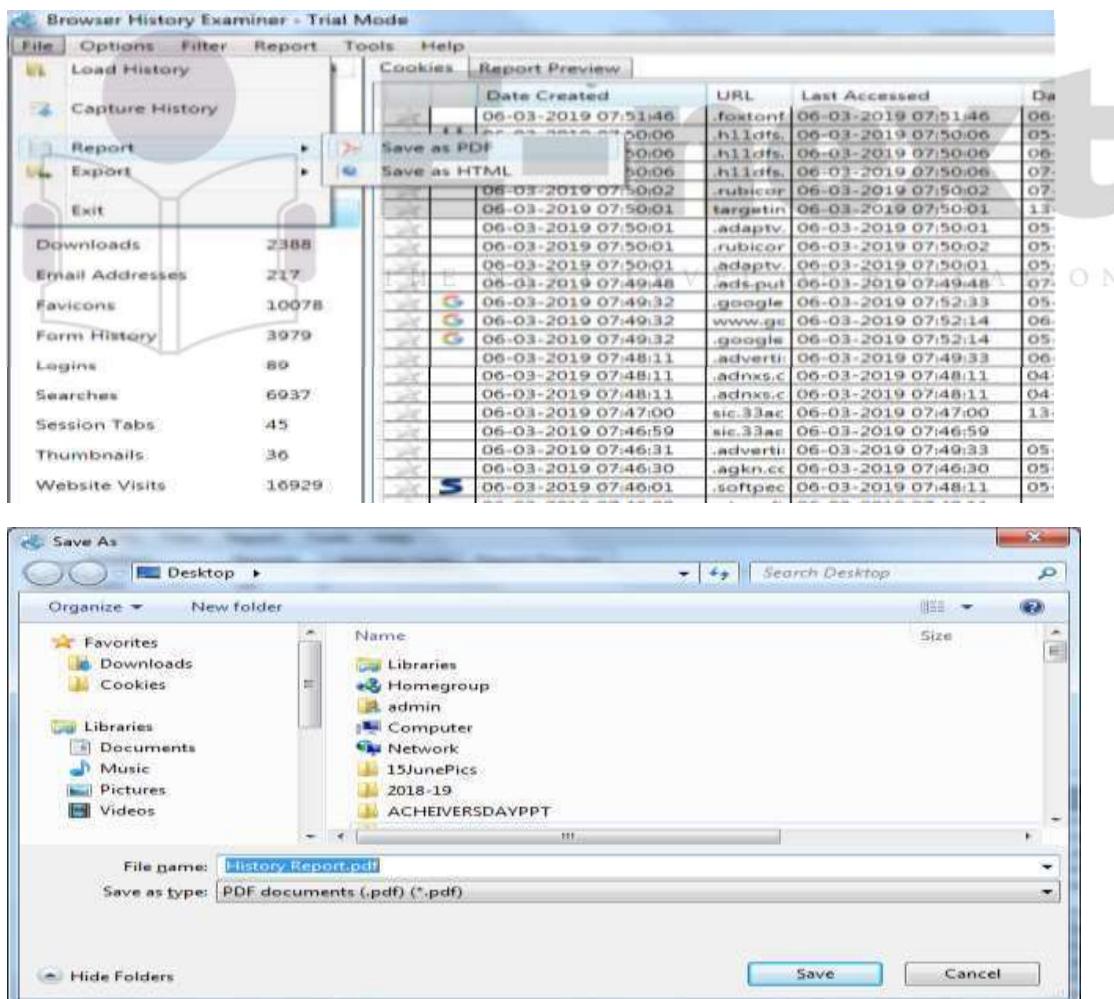
Content-Type	URL	Fetch Count	File Size (Bytes)	Web Browser
application/x-zip-compressed	https://excell.com	1	17897000	Chrome
application/x-octet-stream	https://excell.com	1	13736152	Internet Explorer
application/x-octet-stream	https://excell.com	1	11765280	Internet Explorer
application/pdf	https://www...	1	10882664	Chrome
application/x-octet-stream	https://excell.com	1	6262148	Internet Explorer
application/x-x509-ca-cert	https://osimba...	34	1082869	Internet Explorer
application/x-octet-stream	https://osimba...	1	2618664	Internet Explorer
application/x-octet-stream	https://osimba...	1	2612660	Internet Explorer
application/x-octet-stream	https://osimba...	1	2158676	Internet Explorer
application/x-octet-stream	https://osimba...	1	2158882	Internet Explorer
application/x-octet-stream	https://osimba...	1	2146972	Internet Explorer
application/x-octet-stream	https://osimba...	1	2063228	Internet Explorer
application/x-octet-stream	https://osimba...	1	2041280	Internet Explorer
application/x-octet-stream	https://osimba...	1	1968362	Internet Explorer
application/x-octet-stream	https://osimba...	1	1860481	Internet Explorer
application/x-octet-stream	https://osimba...	1	1783529	Internet Explorer
application/x-dwg		1	1725183	Chrome
application/x-octet-stream	https://osimba...	1	1734315	Internet Explorer
application/x-octet-stream	https://osimba...	1	1615643	Internet Explorer
application/x-octet-stream	https://osimba...	1	1588808	Internet Explorer
application/x-octet-stream	https://osimba...	1	1535347	Internet Explorer
application/x-octet-stream	https://osimba...	1	1406577	Internet Explorer
application/javascript	https://nl101...	1	1218968	Chrome
application/x-shockwave-flash	https://osimba...	1	1187006	Internet Explorer

9. On the left panel click on cached images.

Content-Type	URL	Fetch Count	File Size (Bytes)	Web Browser
image/jpeg	http://www.kataria...	1	2062228	Chrome
image/jpeg	http://www.kataria...	1	1871426	Chrome
image/jpeg	https://www.kataria...	1	10891920	Internet Explorer
image/jpeg	https://booksgaller...	1	2524010	Chrome
image/jpeg	http://www.kataria...	1	85974	Chrome
image/jpeg	https://www.kataria...	1	801862	Internet Explorer
image/jpeg	https://booksgaller...	1	693355	Internet Explorer
image/jpeg	http://www.kataria...	1	644068	Chrome
image/jpeg	http://www.kataria...	1	642181	Chrome
image/jpeg	http://digitalecorner...	1	611968	Internet Explorer
image/jpeg	http://osimba.m...	1	599252	Chrome
image/jpeg	https://www.kataria...	1	586784	Chrome

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: 06-03-2018 16:40
Created using: Browser History Examiner v1.3
Time zone: UTC, DST enabled
Date format: dd/mm/yyyy

Item Added	Last Modified	Title	URL	Web Browser
06-01-2018 07:31:19		~	https://www.google.com/search?rlz=1C1GCEU_enUS789US789&q=https://diggit.coop/+Hqg4tU2Mw&sa=U&pf=nZ	Chrome
06-01-2018 07:31:54		Format of Request to be part of the Advisory Panel for the National Conference - <mailto:kyle@diggit.co...	https://www.google.com/search?rlz=1C1GCEU_enUS789US789&q=https://diggit.coop/+Hqg4tU2Mw&sa=U&pf=nZ	Chrome
14-12-2018 06:00:25		Webmail	https://diggit.dreamhost.com/it_cms/	Chrome
21-08-2018 00:28:06		Header Password	https://www.sohu.com/nf/sohu_gm/sohucard/sohucardLogin.jsp	Chrome
30-01-2018 07:41:47	30-01-2018 07:41:47	Recent Tags	place.net/~kyle/1-14/newsletter/10	Firefox
30-01-2018 07:41:45	30-01-2018 07:41:47	Read Value	place.net/~kyle/newsletter/03	Firefox

Cached Files

Last Fetched	Content Type	URL	Fetch Count	File Size (Bytes)	Web Browser
		http://diggit.dreamhost.com/it_cms/cache/cachedimages/12.JPG	1	2138629	Internet Explorer
		http://diggit.dreamhost.com/it_cms/cache/cachedimages/8.JPG	1	2135881	Internet Explorer
		https://www.adobe.com/youid/account/curlykey/logo	1	2164671	Internet Explorer
		http://diggit.dreamhost.com/it_cms/cache/cachedimages/7.JPG	1	2063328	Internet Explorer
		http://diggit.dreamhost.com/it_cms/cache/cachedimages/2.JPG	1	201139	Internet Explorer
		http://diggit.dreamhost.com/it_cms/cache/cachedimages/9.JPG	1	1968362	Internet Explorer
		http://diggit.dreamhost.com/it_cms/cache/cachedimages/5.JPG	1	1860461	Internet Explorer

The screenshot shows the 'Browser History Examiner - Trial Mode' application interface. The left sidebar lists history types: Load History, Capture History, Report, Export, and Exit. Below this is a summary of history counts: Downloads (2388), Email Addresses (217), Favicons (10078), Form History (3979), Logins (89), Searches (6937), Session Tabs (45), Thumbnails (36), and Website Visits (16929). A central panel displays a 'Web Browser History Report' with a 'Created' date of 06-03-2019 14:38 and version Examiner v1.9. A context menu is open over the report, listing options: Export to Excel, Export to HTML, Export to CSV, Export to XML, and Export to Concordance Load File. The main pane shows a table with columns: Date Added, Last Modified, Title, and URL. The table contains several rows of browser history data.

Web Browser History Report					
		File	C:\Users\admin\Desktop\test_report.html		
06-10-2017 06:14:38		Padm 4A (Grey, 16GB)- Amazon.in: Electronics	https://www.amazon.in/Mi-Redmi-4A-Grey- 16GB/dp/B01PM7K078/ref=sr_1_8?__mk_in_IN=%E0%AF%8D=UTF8&q_	Chrome	
31-08-2017 07:37:43		MSc Sem II.pdf	file:///C:/Users/admin/Desktop/MSc%20Sem%20II.pdf	Chrome	
		Suggested Sites	https://leonline.microsoft.com/#esidice	Internet Explorer	
		Web Slicer Gallery	http://go.microsoft.com/fwlink/?LinkId=121315	Internet Explorer	