

University Of Mumbai
Institute of Distance & Open Learning



PRACTICAL JOURNAL IN PAPER-II

CYBER FORENSICS

SUBMITTED BY

**DEVANG VIJAY DESHMUKH APPLICATION ID: 137062 SEAT NO:
0103557**

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY PART-II

ACADEMIC YEAR 2021-2022

**INSTITUTE OF DISTANCE AND OPEN LEARNING
IDOL BUILDING, VIDYANAGARI,
SANTACRUZ (EAST), MUMBAI-400 098**

**CONDUCTED AT
RIZVI COLLEGE OF ARTS, SCIENCE AND COMMERCE
BANDRA (W), MUMBAI 400050**

University of Mumbai
Institute of Distance & Open Learning



Dr.Shankar Dayal Sharama Bhavan, Kalina,
Vidanagari, Santacruz (E), Mumbai-400 098.

Certificate

This is to certify that

Mr. **DEVANG VIJAY DESHMUKH** Application ID: **137062**,
Seat No: **0103557** from Rizvi College of Arts, Science and Commerce
Bandra(W), Mumbai 400050 has successfully completed all the practical
of Paper **II** titled **CYBER FORENSICS** for M.sc (IT) Part II in the
academic year 2021-2022.

Section I _____

Section II _____

MSc (IT) Co-ordinator, IDOL

External Examiner

INDEX

PRACTICAL NO	TITLE
1	Creating Image of an Evidence(Logical / physical drive)
2	Creating an Image of content of folder from system
3	Analyse and investigate the image file provided in Autopsy
4	Capture and Analyse the network Packets
5	Investigate the packets provided in Wireshark
6	Perform Network packet analyse and process monitoring
7	Investigate the Mobile Device
8	Investigate Email File Given
9	Browser Forensic
10	Perform Stegnography

PRACTICAL 1

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

- **Creating Forensic Image**
- **Check Integrity of Data**
- **Analyse Forensic Image**
-

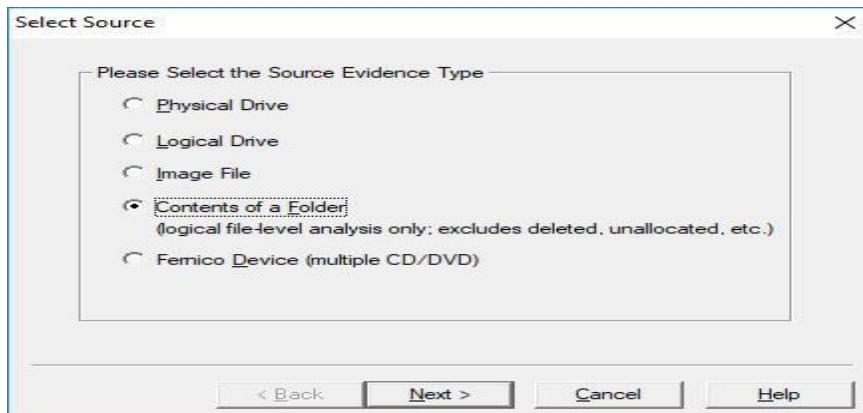
FTK Imager allows you to make several different types of forensic images. In addition, drive content and hash lists can be exported.

a) Creating Forensic Image

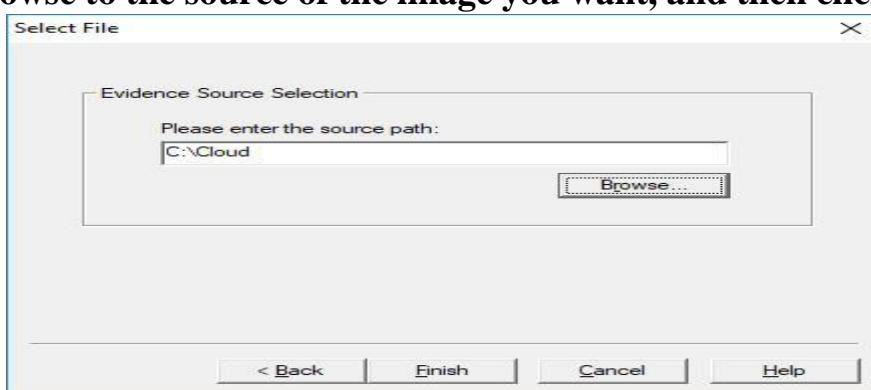
FTK Imager allows you to write an image file to a single destination or to simultaneously write multiple image files to multiple destinations using the same source data or drive.

To create a forensic image

- 1. Click File > Create Disk Image.**
- 2. In the Select Source dialog box, select the source you want to make an image of.**



- 3. Click Next.**
- 4. Click Yes**
- 5. Browse to the source of the image you want, and then click Finish.**

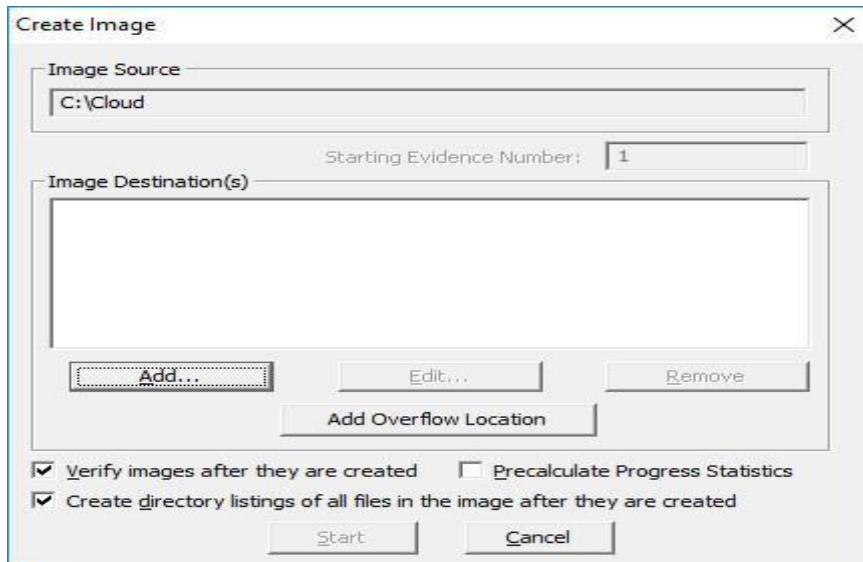


6. In the Create Image dialog,

6.a. 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.

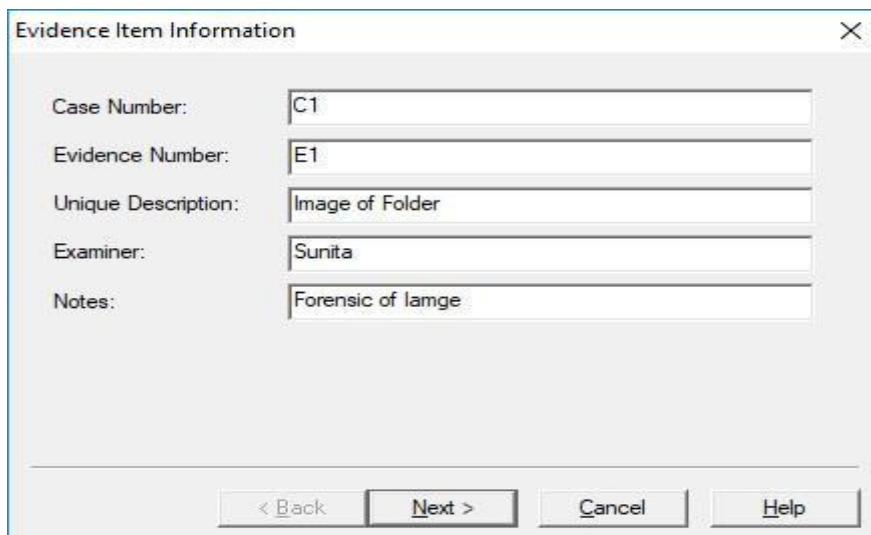
6.b. List the entire contents of your images with path, creation dates, whether files were deleted, and other metadata. The list is saved in tab-separated value (.CSV) format.

6.c. click Add.



7. Click Next.

8. Specify Evidence Item Information. All Evidence Item Information is optional, but it is helpful to have the information easily accessible in case it is called into question at any time after creation



9. Click Next.

10. In the Image Destination Folder field Click Browse to find and select the desired location.

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

12.a.Specify the Image fragment Size:

Default Image Fragment Size = 1500 MB

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.

12.b. Select the compression level to use.

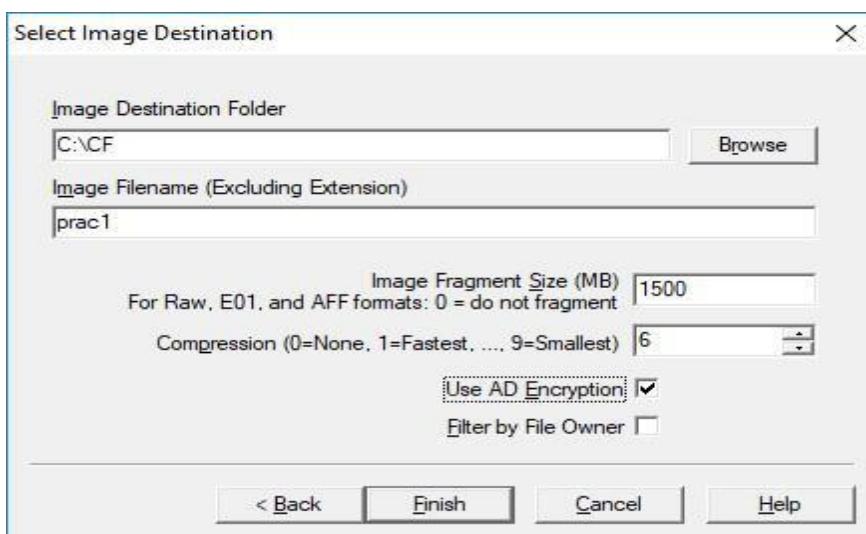
0=No Compression

1=Fastest, Least Compression (faster, and also slightly smaller than a 0-compression file)

9=Slowest, Most Compression (smallest file, slowest to create).

Numbers between 1 and 9 produce an image with varying levels of compression to speed ratio.

13. To encrypt the new image with AD Encryption, mark the Use AD Encryption box.



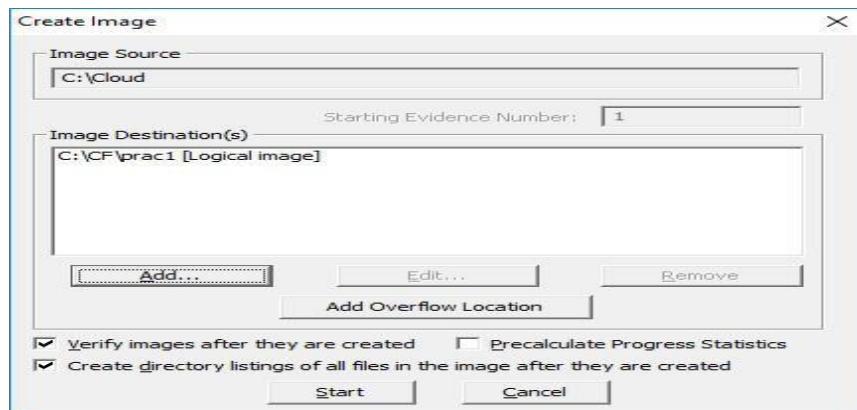
14. When AD Encryption is selected, you can choose between encrypting with a password, or encrypting with a certificate.



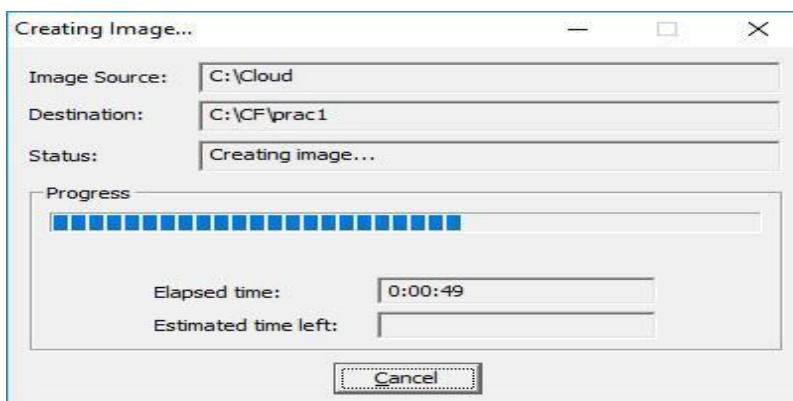
15. When encryption selections are made, click OK to save selections and return to the Create Image dialog.

16. To add another image destination (i.e., a different saved location or image file type), click Add, and repeat steps

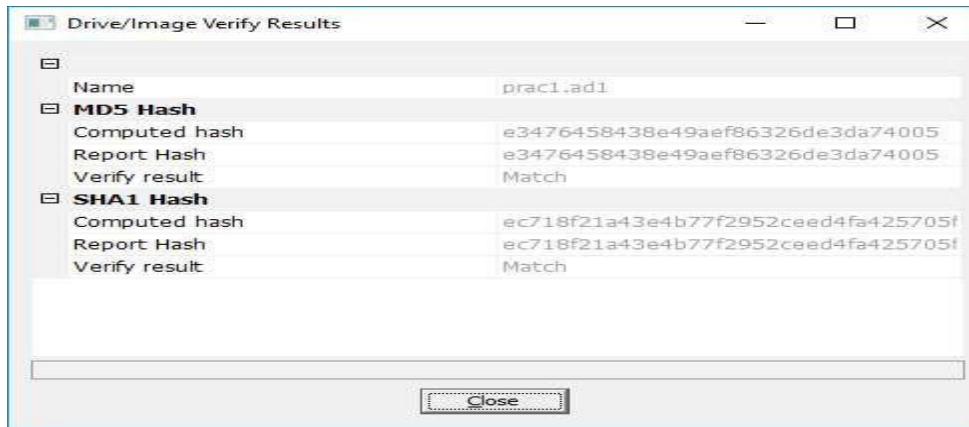
17. Click Start to begin the imaging process.



18. A progress dialog appears that shows the following

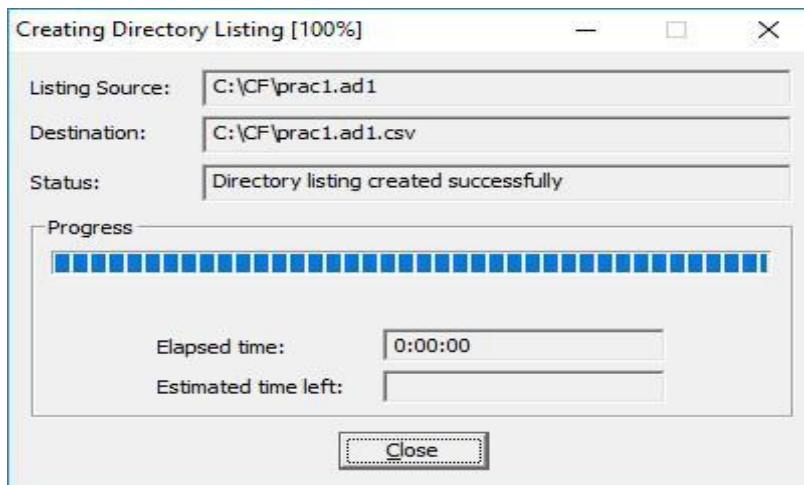


19. After the images are successfully created, the Drive/Image Verify Results box shows detailed image information, including MD5 and SHA1 check sums, and bad sectors.

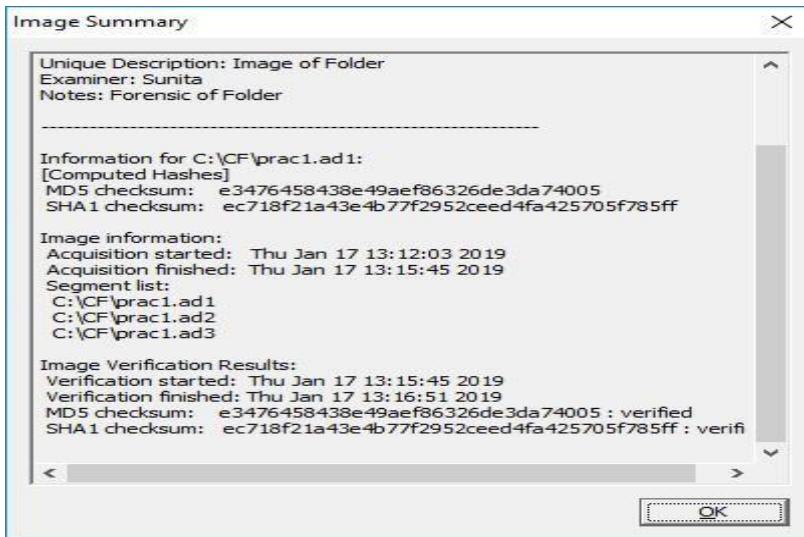


20. Click on Close to close the Drive/Image Verify Results box

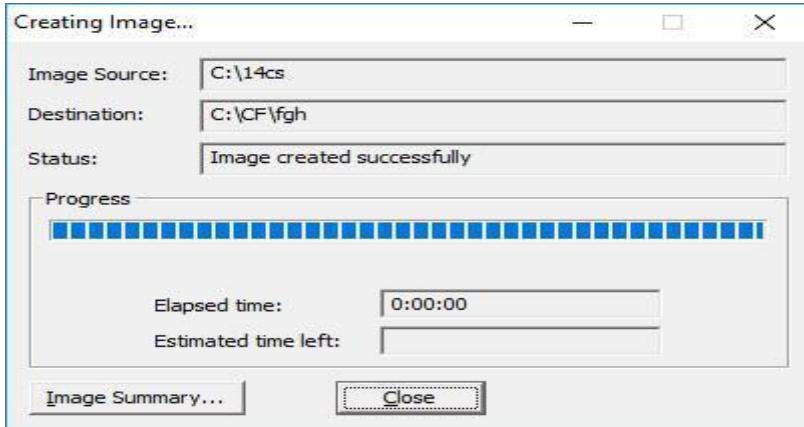
21. Click on Close to close the Creating Directory Listing dialog



22. Click Image Summary to close the Image Summary. The Image Summary also includes the data you entered in the Evidence Item Information dialog.



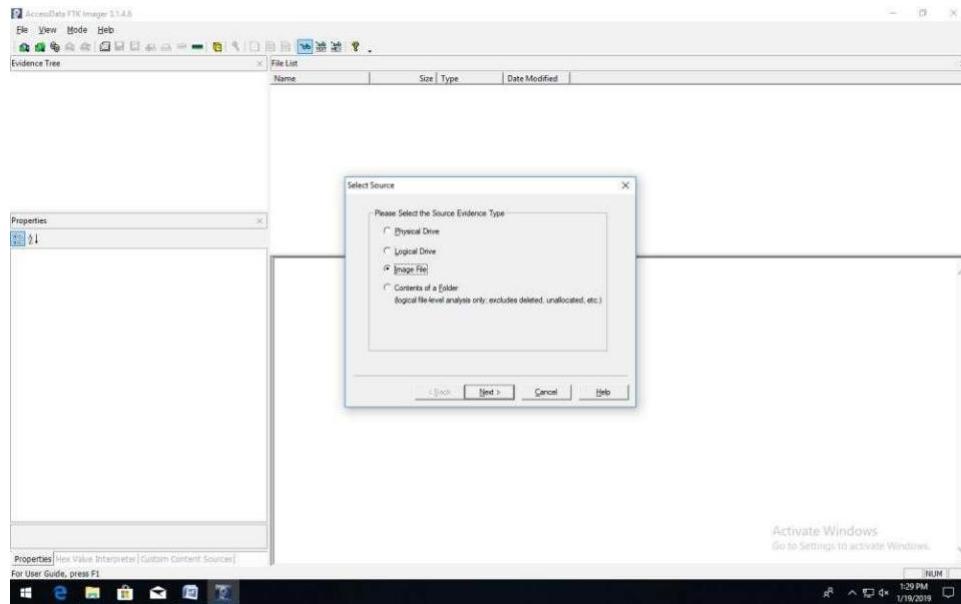
23. Click Close to exit back to Imager.



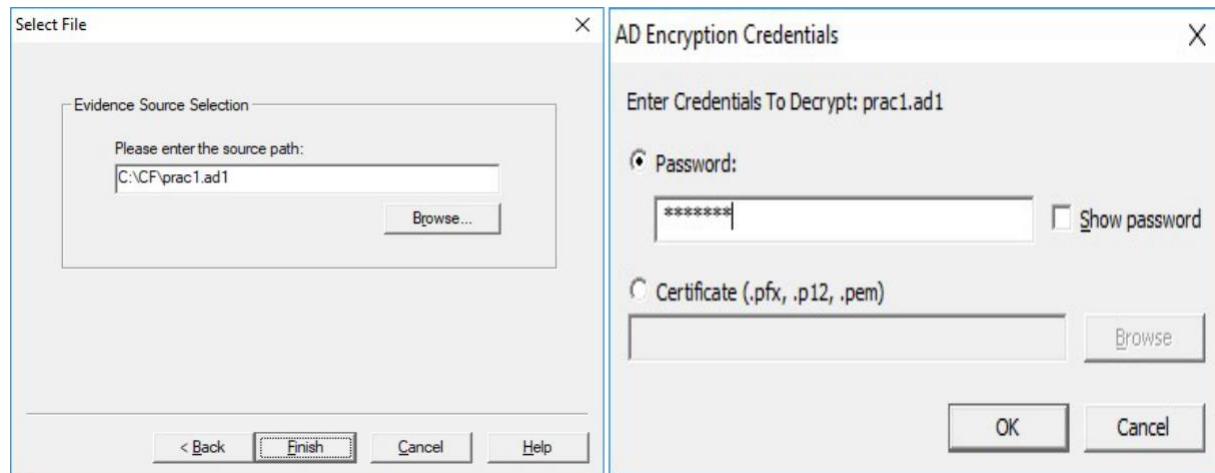
b) Check Integrity of Data

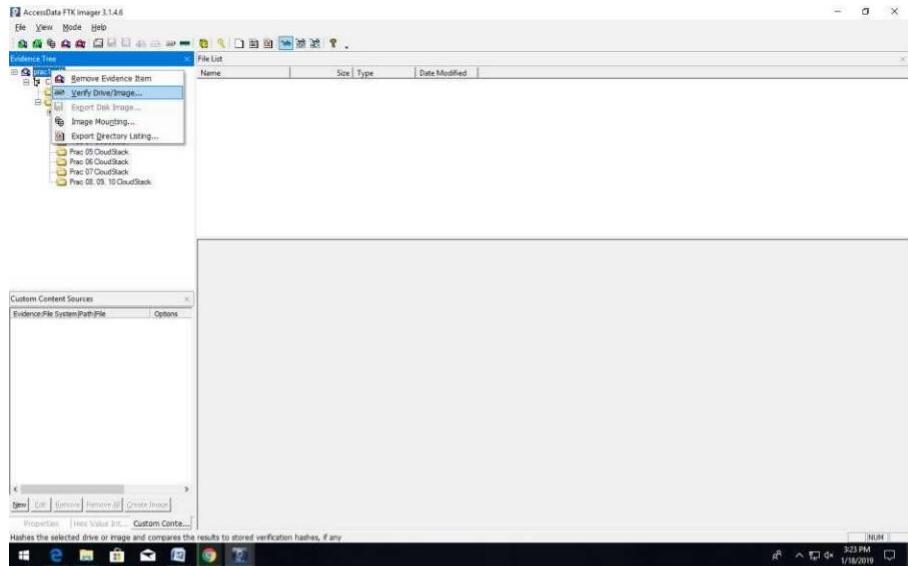
Hashing is the process of generating a unique value based on a file's contents. This value can then be used to prove that a copy of a file has not been altered in any way from the original file. It is computationally infeasible for an altered file to generate the same hash number as the original version of that file. The Export File Hash List feature in FTK Imager uses the MD5 and SHA1 hash algorithms to generate hash numbers for files.

Go to File->Add Evidence Item..->Select Option as Image File



Browse your image file->Click on Finish button-> enter password and Click on Ok button

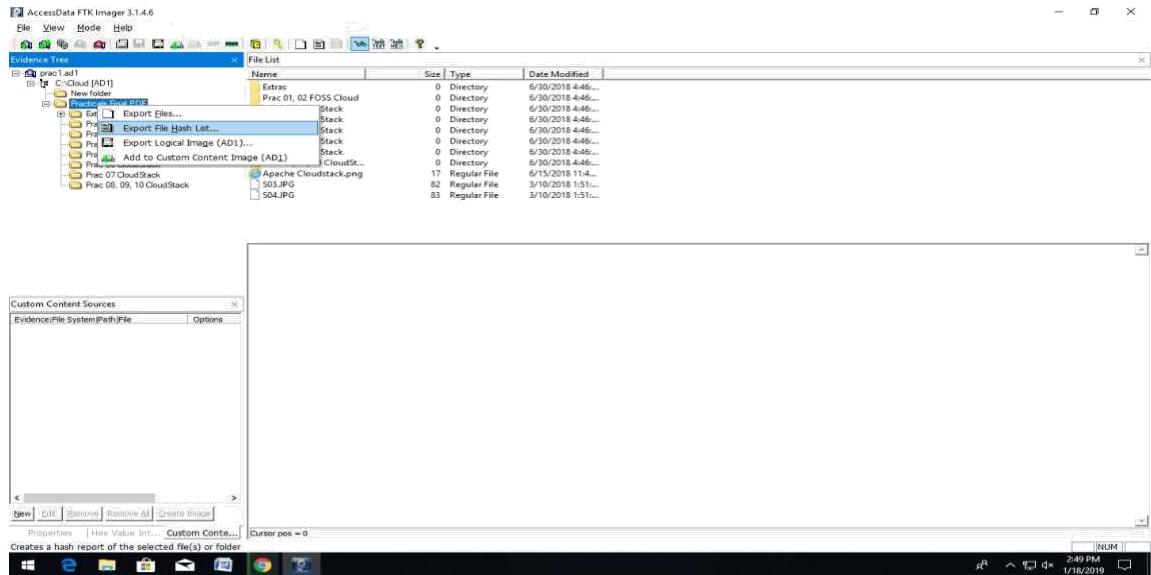




Drive/Image Verify Results	
□	Name
	prac1.ad1
□	MD5 Hash
Computed hash	e3476458438e49aef86326de3da74005
Report Hash	e3476458438e49aef86326de3da74005
Verify result	Match
□	SHA1 Hash
Computed hash	ec718f21a43e4b77f2952ceed4fa425705f
Report Hash	ec718f21a43e4b77f2952ceed4fa425705f
Verify result	Match
Close	

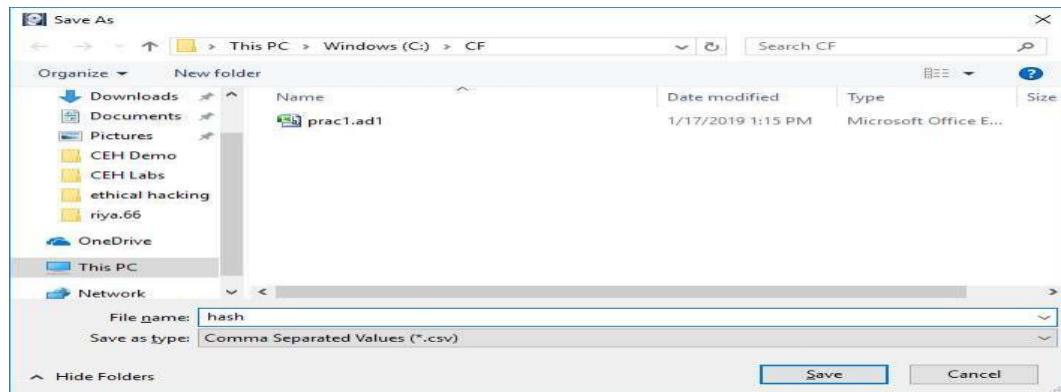
To generate and export hash values to a list

1. In the Evidence Tree, select the folder that contains the objects you want to hash. The object's contents are displayed in the File List.
2. In the File List, select the folders or files you want to hash. If you select a folder, all the files contained in the folder and its sub folders are hashed.
3. Click File > Export File Hash List



4. In the Save As dialog, type a name for the file hash list in the File Name field.

5. Click Save.

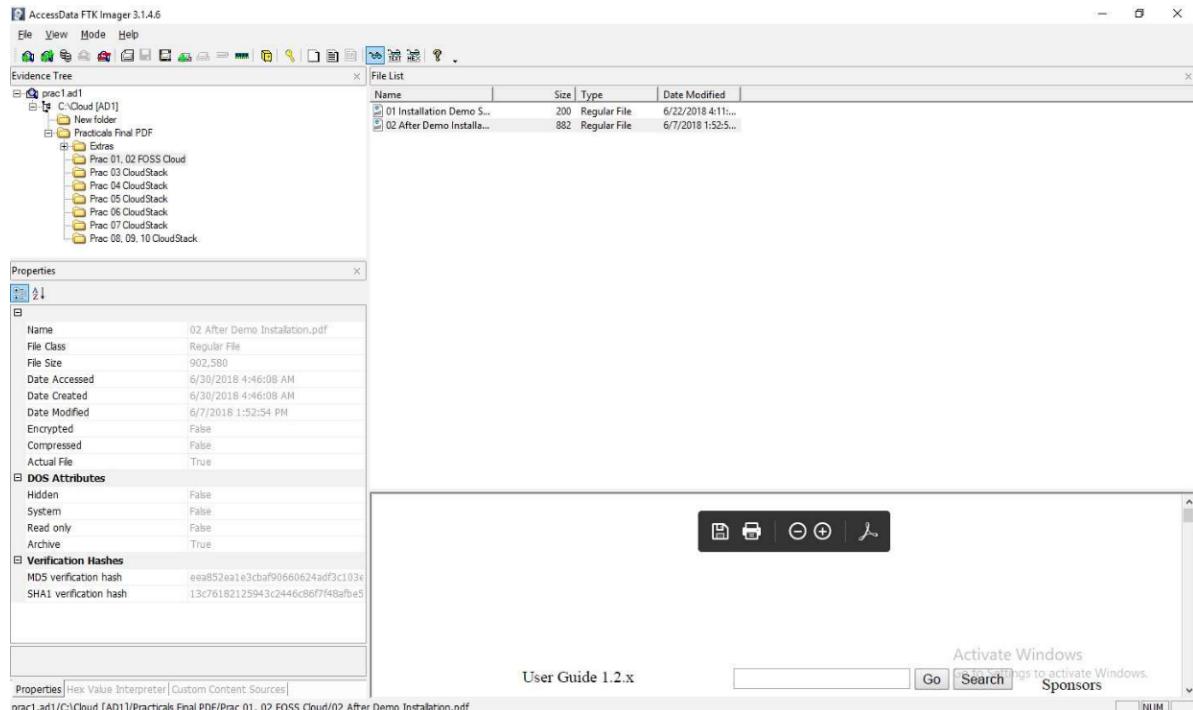


The hash list is saved as a file of comma-separated values (*.CSV).

	A	B	C
1	MDS	SHA1	fileNames
2	53108117dbb0b08c79ec1c29625c9e5	86ad921998f57af71e76151ffad52681c3d9a69	prac1.ad1\c1\Cloud\AD1\Practicals Final PDF\Apache Cloudstack.pdf
3	0ff3e3b3c75fb40f696171b921a7fe7b6	521d4ea6eae608987519d477adfe754606777	prac1.ad1\c1\Cloud\AD1\Practicals Final PDF\extras\01 CloudStack Documentation.pdf
4	ed39aa4744f4ab12b48e0845140241	01b601008ae2c153dc0cb1d771cd9e09141	prac1.ad1\c1\Cloud\AD1\Practicals Final PDF\extras\02 CloudStack Installation.pdf
5	5543ce4e8008a41f2e6e12099c02fc	970a2ebd18704d1bbc5977944e031a1ef8c	prac1.ad1\c1\Cloud\AD1\Practicals Final PDF\extras\03 CloudStack Administration.pdf
6	63012654474a21a97fa310966472ba	79a1c7175e92d48f1ce8248195ddc7a77302ce0	prac1.ad1\c1\Cloud\AD1\Practicals Final PDF\extras\04 CloudStack Release Notes.pdf
7	4b1979dadeabfb7a0f1c11e4da3a0f	669k17420a1d58ff0d1f50ah3911264d4ff9e1	prac1.ad1\c1\Cloud\AD1\Practicals Final PDF\extras\05 DevCloud - Apache Cloudstack - Apache Software Foundation.pdf
8	da034e588905e3e003f12a2df0359d	e6e1733961bf93178709309aca14114c136	prac1.ad1\c1\Cloud\AD1\Practicals Final PDF\extras\06 Setting up a CloudStack dev environment on Windows - Apache Cloudstack - Apache Software Foundation.pdf
9	19e2374734528e52b056760b145	bff1526671a077250dc8b60878227	prac1.ad1\c1\Cloud\AD1\Practicals Final PDF\extras\07 Quick Installation Guide for CentOS 6 [Up2014] Apache CloudStack Installation Documentation.pdf
10	13e2c92301d0e04252b01561670799e	ea7b010bb023417f4ff5fb1d0ad62006516	prac1.ad1\c1\Cloud\AD1\Practicals Final PDF\extras\New folder\0 PRAC 4 Working with Virtual Machines [U+2014] Apache CloudStack Administration.pdf
11	63a0c92000f31e837029c5abc1	d317c35861ac039601820a62e20f7fb4a0d208	prac1.ad1\c1\Cloud\AD1\Practicals Final PDF\extras\New folder\0 PRAC 5 A.pdf
12	6c72e2162628cf78a126249097b67e8	aac40424284104065170fa548ee1a08cca	prac1.ad1\c1\Cloud\AD1\Practicals Final PDF\extras\New folder\0 PRAC 5B How To Configure SSH Key-Based Authentication on a Linux System [U+2014] Apache CloudStack Administration.pdf
13	f3b18688f0512a93de981c10cc20d8	7b9ef34cc14d61399e67499f1cc538ff9e4bb	prac1.ad1\c1\Cloud\AD1\Practicals Final PDF\extras\New folder\0 PRAC 8 Managing the Cloud [U+2014] Apache CloudStack Administration.pdf
14	3f4903d161958b26c45003f9f6a0e	91b727353b7f27272a0e179e111c4a6a854b	prac1.ad1\c1\Cloud\AD1\Practicals Final PDF\extras\New folder\0 PRAC 8.8 Managing CPU sockets - Apache Cloudstack - Apache Software Foundation.pdf
15	4ec5f2ed763a9358e34bd0b02671e0d	db0ec5f2c0ab11116171b639b08ce27300f	prac1.ad1\c1\Cloud\AD1\Practicals Final PDF\extras\New folder\0 PRAC 9.10Managing the Cloud [U+2014] Apache CloudStack Administration.pdf
16	95a6b79c77250dc8b60878227	f151661b1756780d0b7300f79300079195	prac1.ad1\c1\Cloud\AD1\Practicals Final PDF\extras\New folder\1. Installing from Source - 80 Recipes for Apache CloudStack [Book].pdf
17	950be8c3502906601600d82d727e0f	83cb677e319499a6e015097946952e2020e	prac1.ad1\c1\Cloud\AD1\Practicals Final PDF\extras\New folder\Activeneon Team Blog - Devcloud Image Customization.pdf
18	3b02246aa0c2b0f1c92617e4fe1f6	4d4a01791d6a751403e74d99f1cc538ff9e4bb	prac1.ad1\c1\Cloud\AD1\Practicals Final PDF\extras\New folder\How to test Apache CloudStack 4.2 on your local machine - LeaseWeb lab.pdf
19	12883770a033808ea1c065762	c08ed732d035e93a46a76737269ff1e06f	prac1.ad1\c1\Cloud\AD1\Practicals Final PDF\extras\New folder\P1_LeaseWebLab.pdf
20	eadd4f8485127feffb7a958df195	de6529295572e6762fb0fe5f3fc1b149	prac1.ad1\c1\Cloud\AD1\Practicals Final PDF\extras\New folder\P3_P.pdf
21	0635e8093a0a5353e6fa21ab6ff48d6	49c128371065516612d1150ee0338394705e2	prac1.ad1\c1\Cloud\AD1\Practicals Final PDF\extras\New folder\P4_P6.pdf
22	41f9994745917304054e3906571706	b6c16170a870d805731613360a9e0d5678e8	prac1.ad1\c1\Cloud\AD1\Practicals Final PDF\extras\New folder\Rohit Yadav - DevCloud for CloudStack Development.pdf
23	20d0ca227a4c10324e4354862717c	9e12324022176530729177f57253897908	prac1.ad1\c1\Cloud\AD1\Practicals Final PDF\extras\Prac 01_02 FOSS Cloud\01 Installation Demo System - FOSS-Cloud.pdf
24	ea8522e1e1cb95660632ad43c103e	13c76182125943c2446e6874fa0f5a5e169	prac1.ad1\c1\Cloud\AD1\Practicals Final PDF\extras\Prac 01_02 FOSS Cloud\02 After Demo Installation.pdf
25	045813950f01530276f97c48fd7d529	06293439c4f56344e725976708533d0675528483c	prac1.ad1\c1\Cloud\AD1\Practicals Final PDF\extras\Prac 03 CloudStack\03 Prac 3.pdf
26	6513d1e5699446c903948c39f198	81b52a86608a4e12b6bf70956396d5ab0	prac1.ad1\c1\Cloud\AD1\Practicals Final PDF\extras\Prac 04 Cloud 4.pdf
27	0b304ce8807e7b3c46cb0fa0b742b	250bb10b450f4a5081bc500f72851996582	prac1.ad1\c1\Cloud\AD1\Practicals Final PDF\extras\Prac 05 CloudStack\05 Prac 5A.pdf
28	57ec15cd8b944c4cb9393a9b7e	862fde1a9e93ec015252a9f180e90aa8d93e60756	prac1.ad1\c1\Cloud\AD1\Practicals Final PDF\extras\Prac 06 CloudStack\06 Prac 5B.pdf
29	60ead1fc167fb08c5d9995f435e	044012bc1f552ca9f9d180e90aa8d93e60756	prac1.ad1\c1\Cloud\AD1\Practicals Final PDF\extras\Prac 07 CloudStack\07 Prac 6.pdf
30	9ea96345c154873370298ca25	236f575545e8374a565d653131f7209e	prac1.ad1\c1\Cloud\AD1\Practicals Final PDF\extras\Prac 07 CloudStack\07 Prac 7.pdf
31	9420a613eed62z9d1a32778489	b6fde386a3e662f2b05f257eef1d6fa8	prac1.ad1\c1\Cloud\AD1\Practicals Final PDF\extras\Prac 08, 09, 10 CloudStack\09 Prac 08, 09, 10.pdf
32	675521a0f5987b7199nhhh9c7ea7	90ab87f1f991ad510e99b30904d46878053b	prac1.ad1\c1\Cloud\AD1\Practicals Final PDF\extras\Prac 09,10.pdf

c) Analyze Forensic Image

- a. Open Image using Add Evidence Item Option.
- b. Select any folder from Evidence Tree.
- c. Files will be displayed in File List
- d. Select any File and you can view Properties of file in Properties Box



PRACTICAL 2

Aim: Creating an Image of content of folder from system

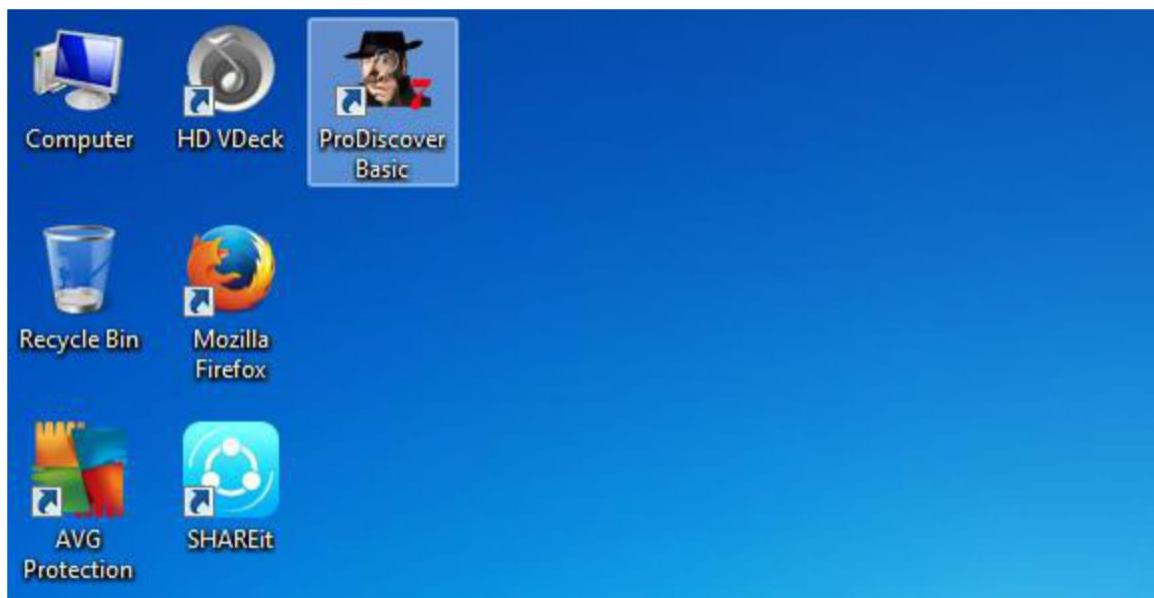
Data Acquisition:

Perform data acquisition using:

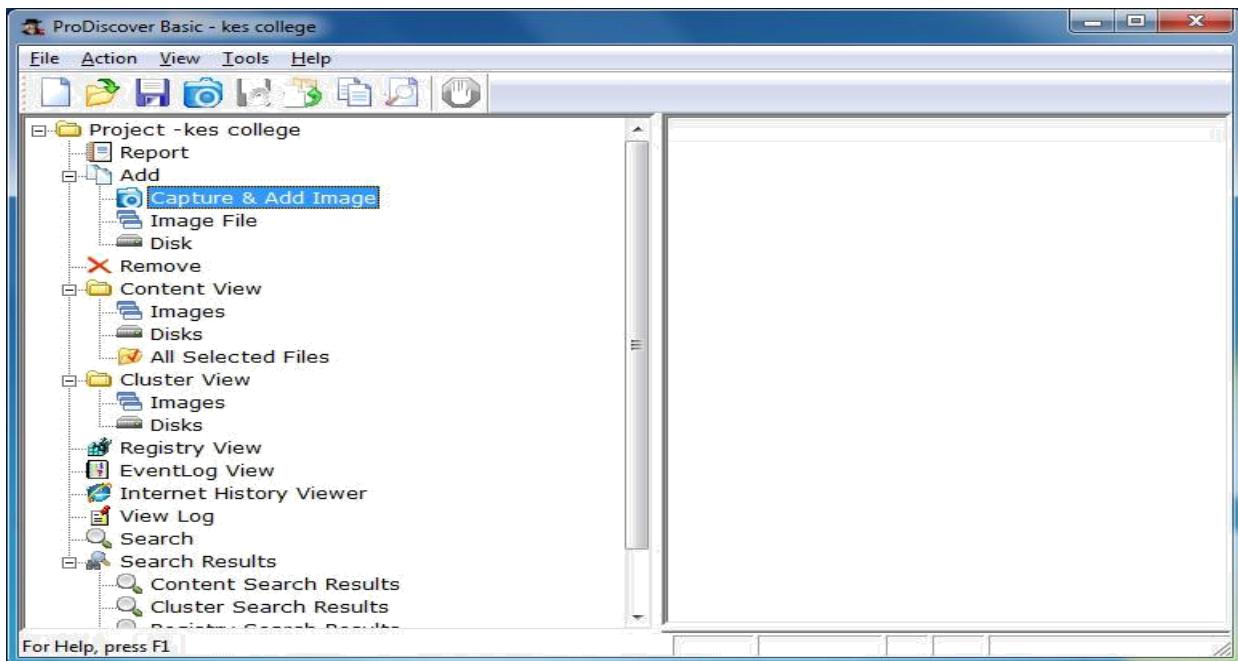
USB Write Blocker + FTK Imager

Steps:

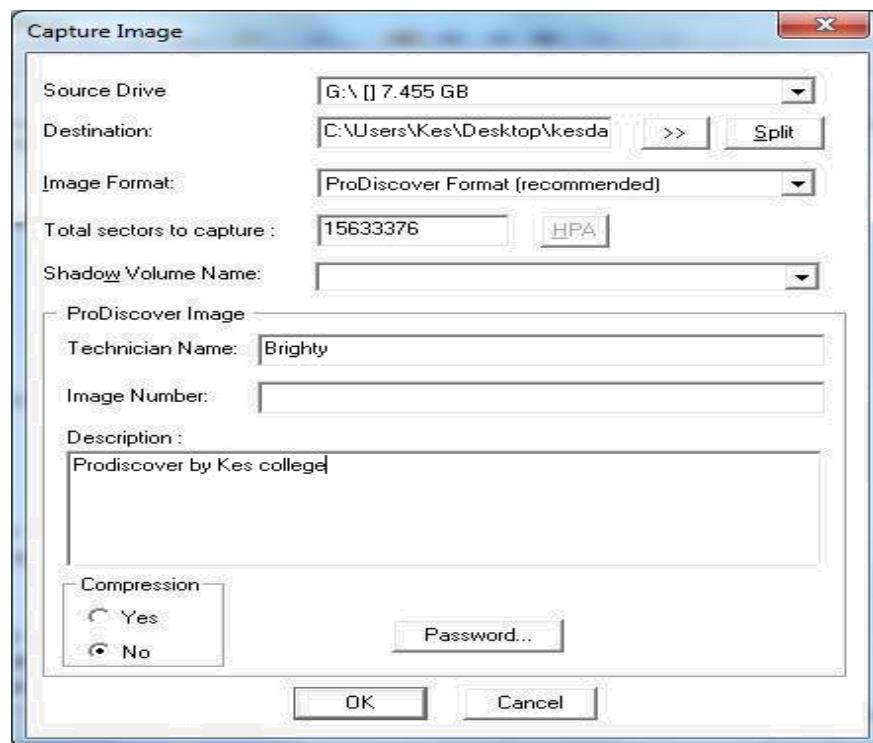
Step 1: First Open Prodiscover Basic and start with new case.



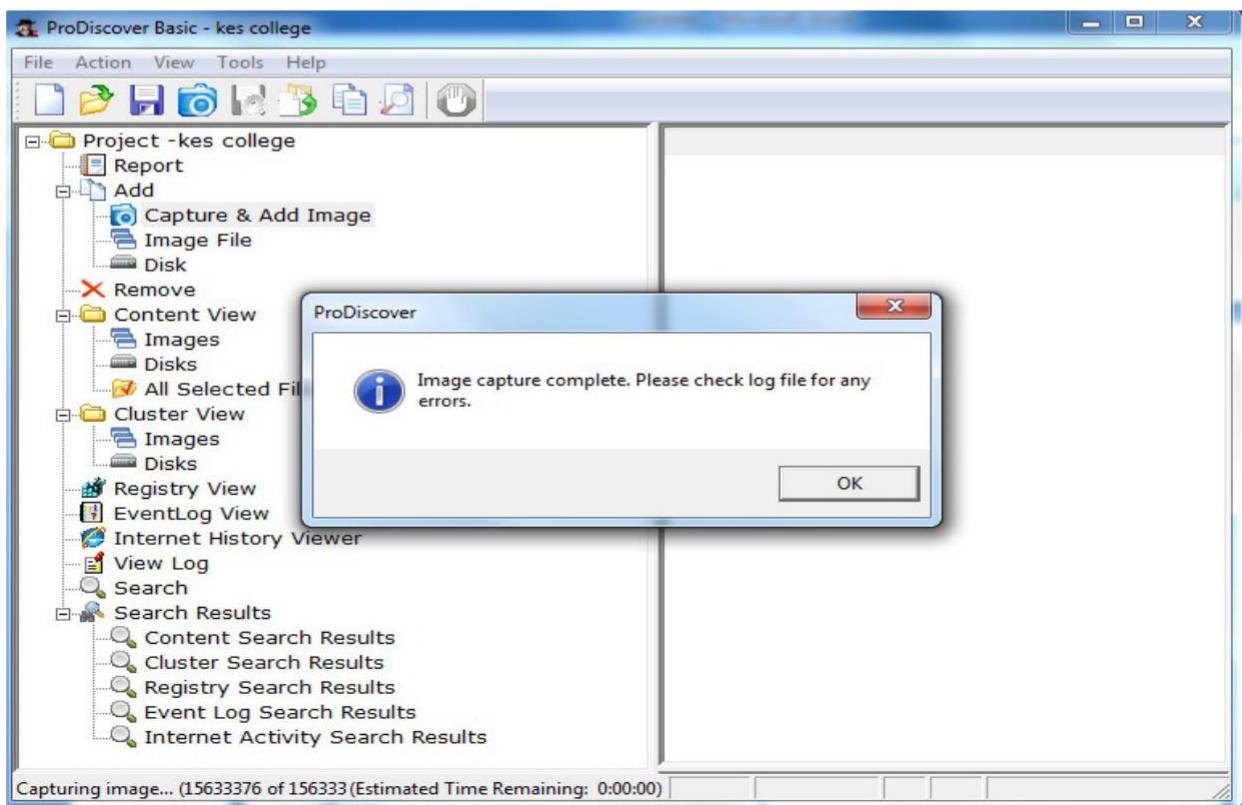
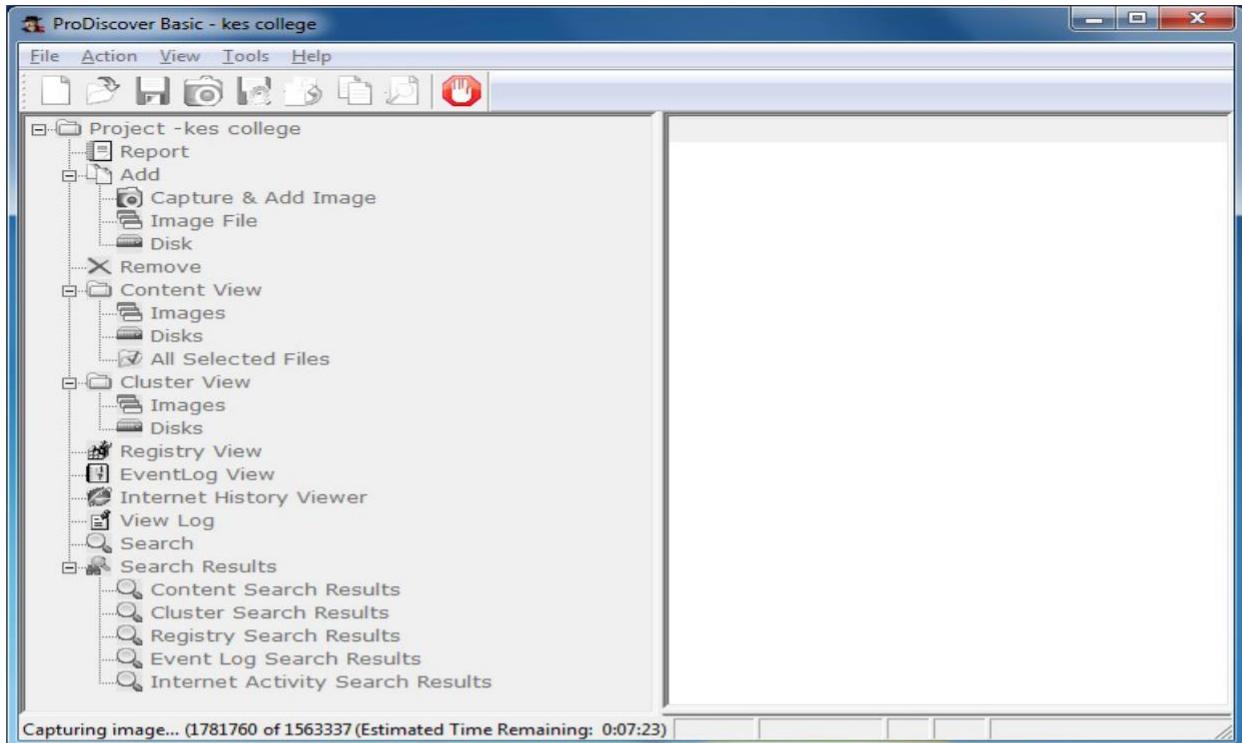
Step 2: The created project appears in left pane and select add>capture & add image.



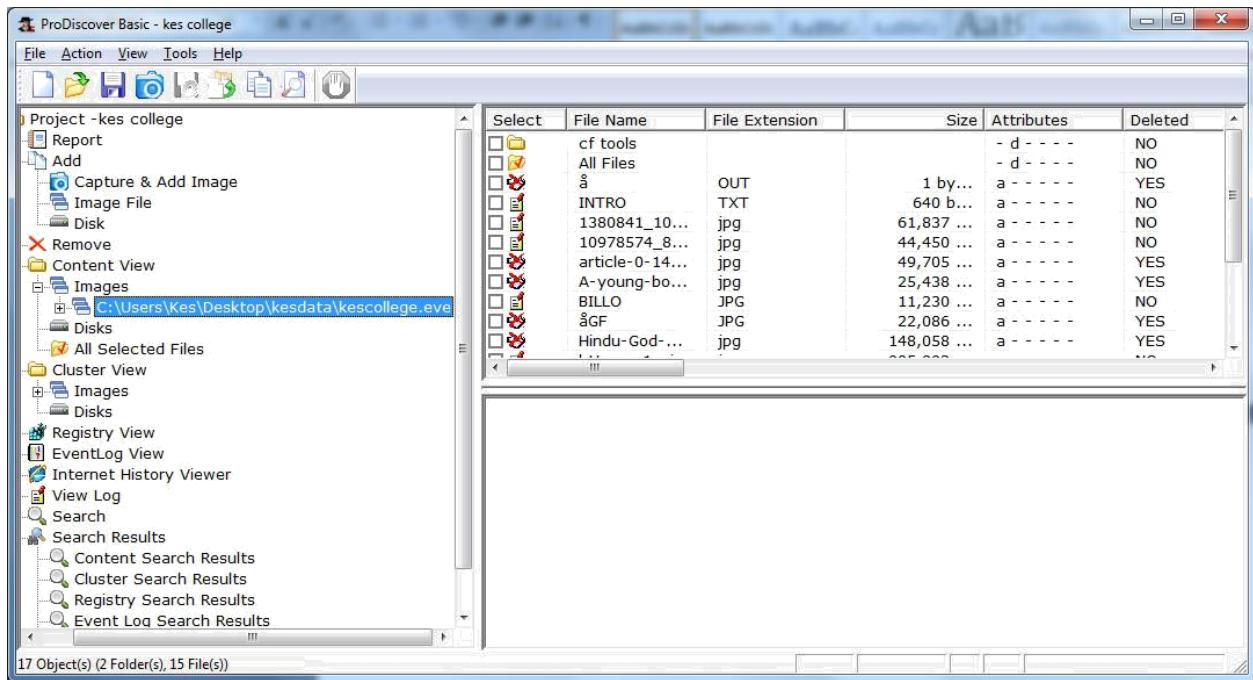
Step 3: fill the details as below. And click ok.



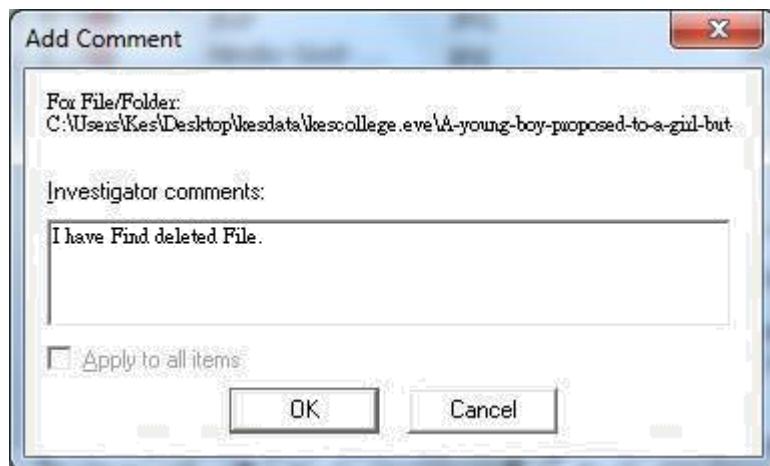
Step 4: capturing of image starts.



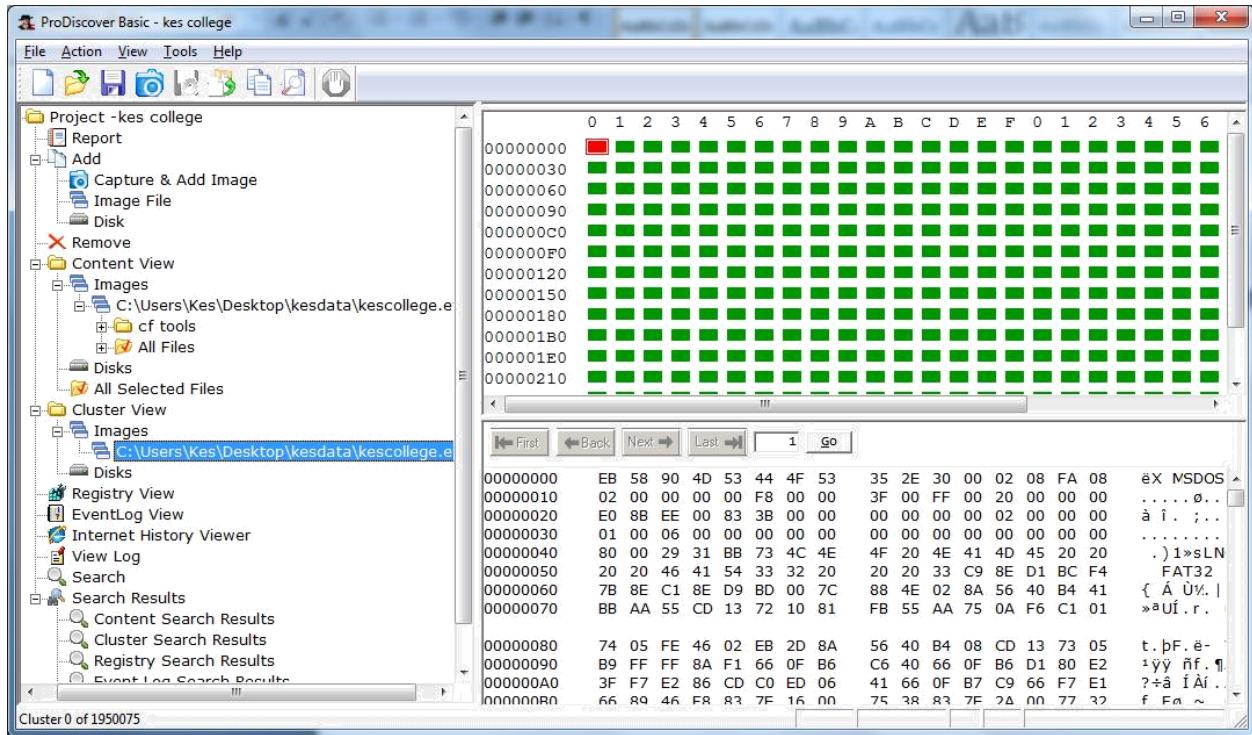
Step 5: Open the image created, go to Add > Images in left pane.



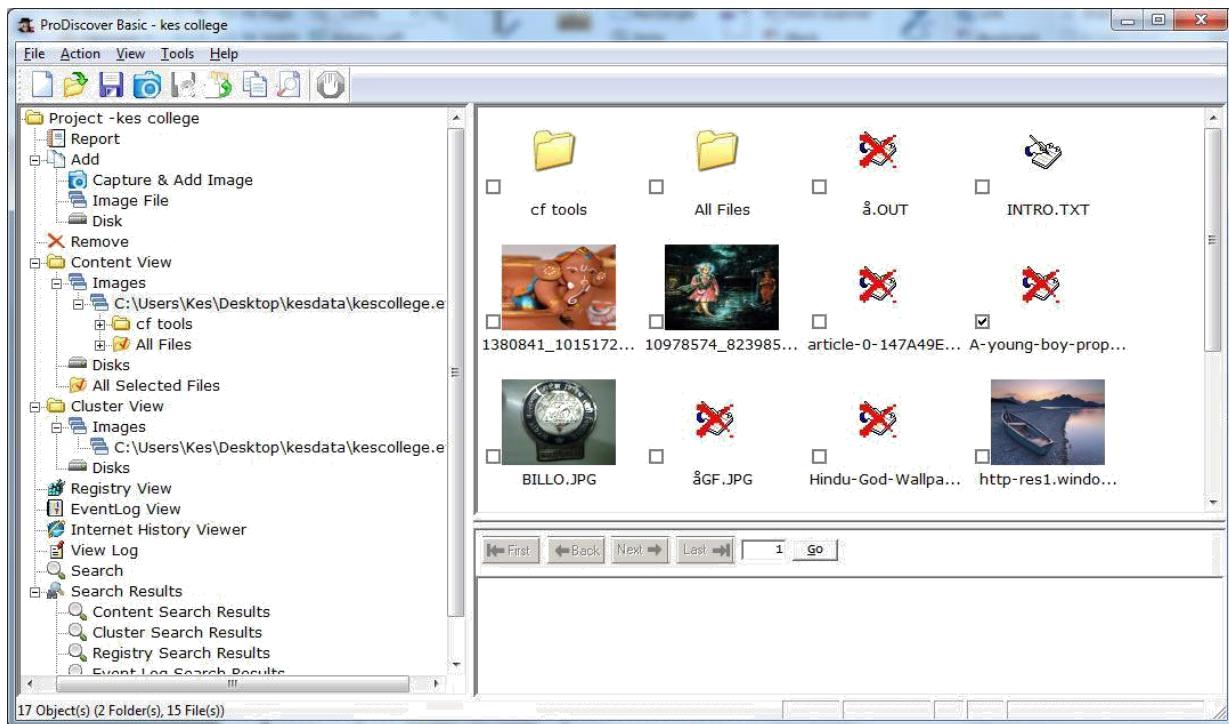
Step 6: Click on any File and type a comment.



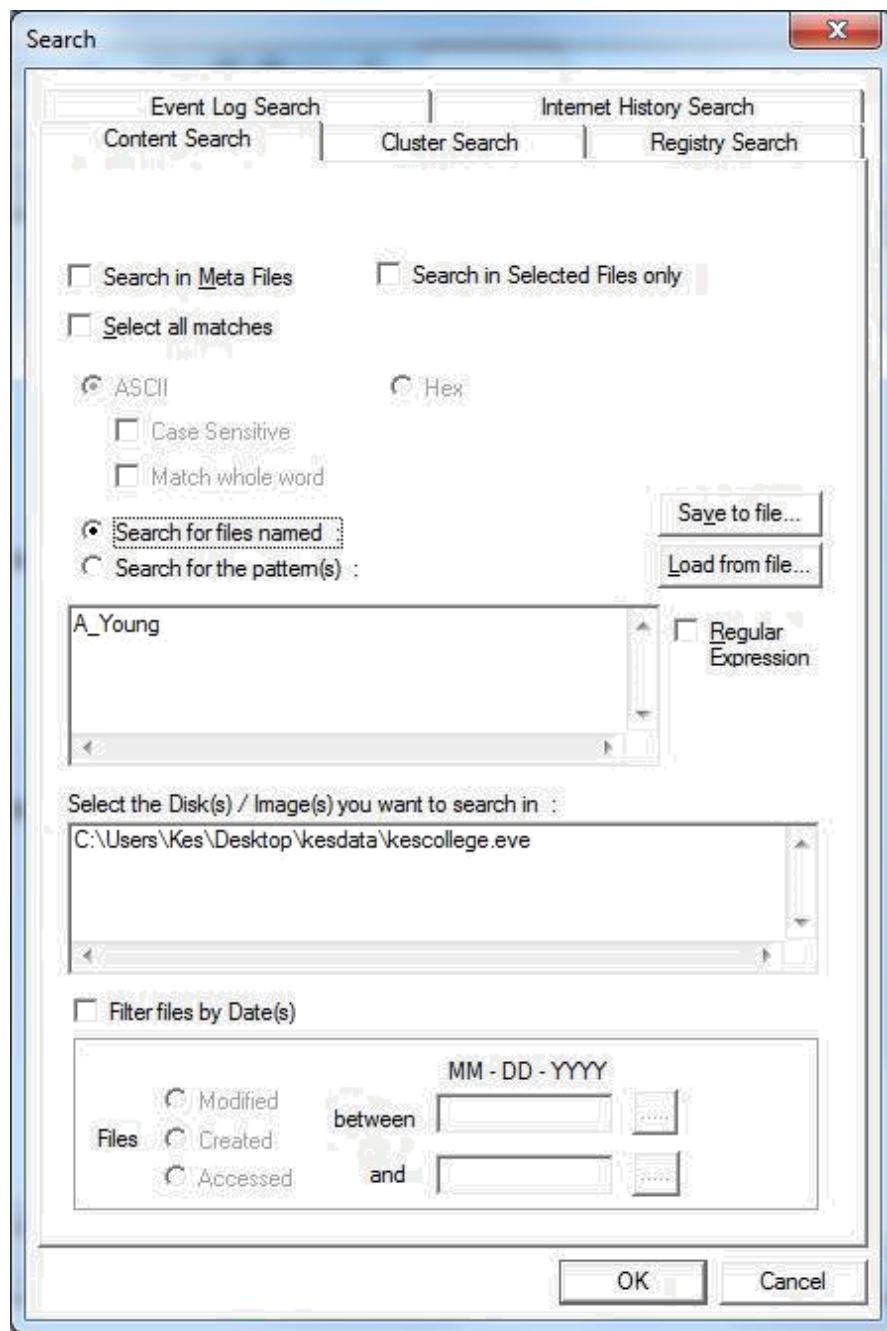
Step 7 : the cluster view is seen from the cluster view in left panel.



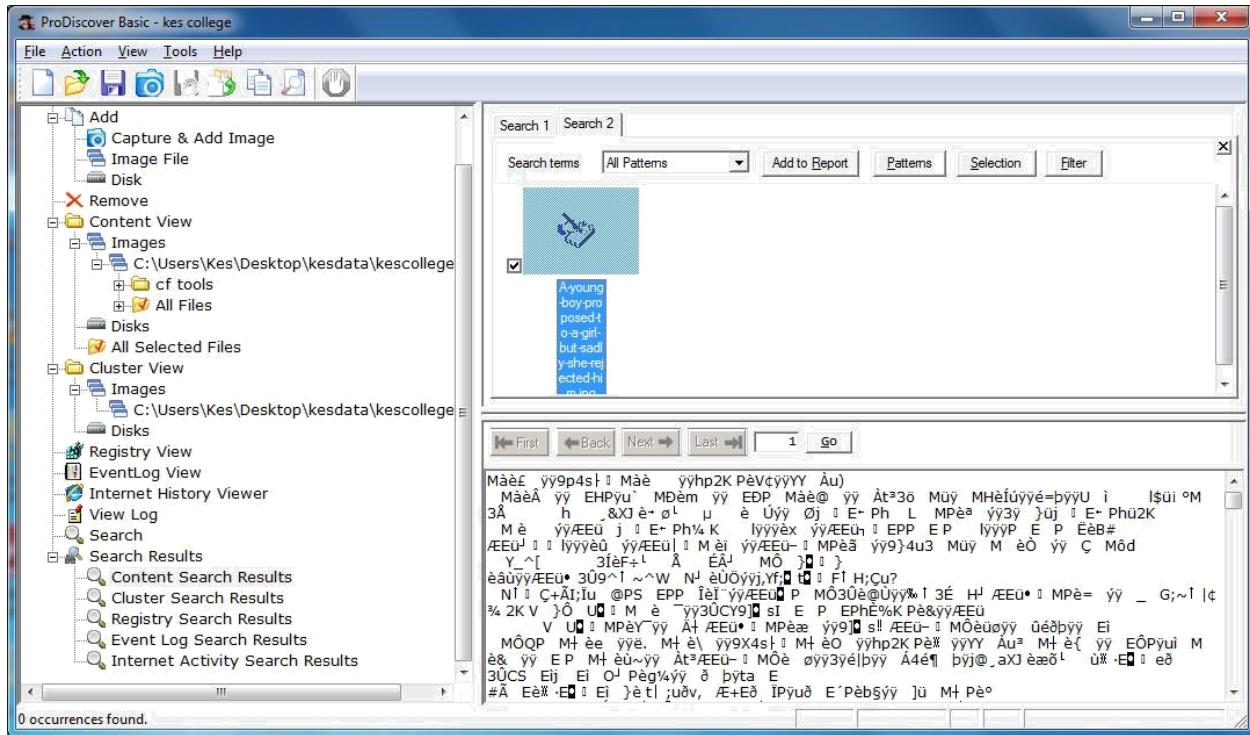
Step 8 : We can also view gallery view by Right Click.



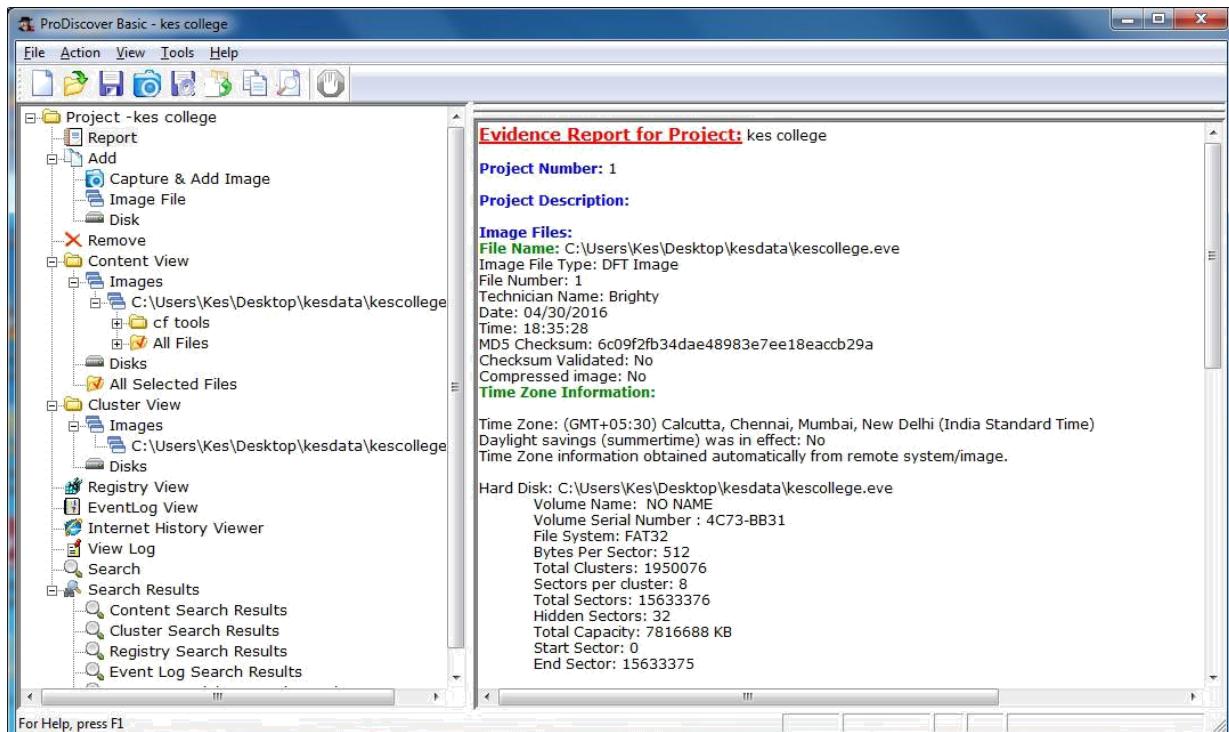
Step 9: Keyword search. Click on Search in left pane and Enter the file name to be searched in the image created.

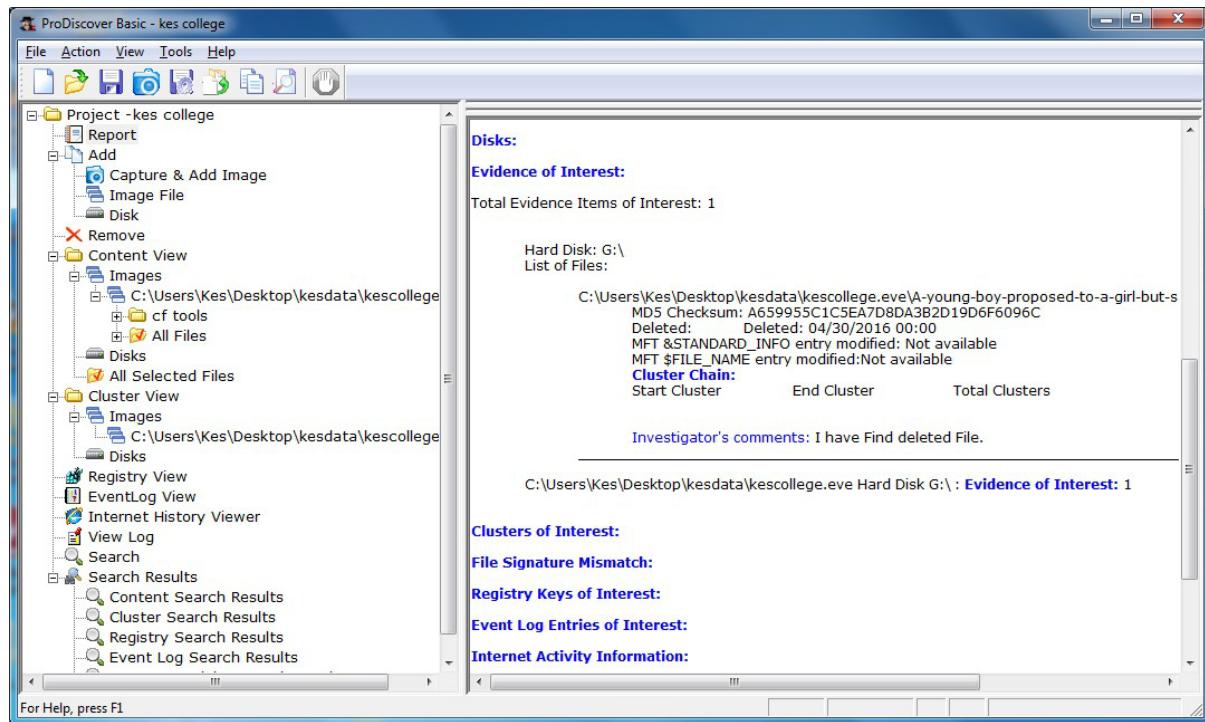


Step 10 : Output of Keyword search.



Step 11 : Click on View>Report.





PRACTICAL 3

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

Step 1: Open Autopsy



Step 2 : Click on new case



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

New Case Information

Steps

1. Case Information
2. Optional Information

Case Information

Case Name:

Base Directory:

Case Type: Single-user Multi-user

Case data will be stored in the following directory:

< Back Finish Cancel Help

Step 4 : Enter further details and click on next button

New Case Information

Steps

1. Case Information
2. Optional Information

Optional Information

Case

Number:

Examiner

Name:

Phone:

Email:

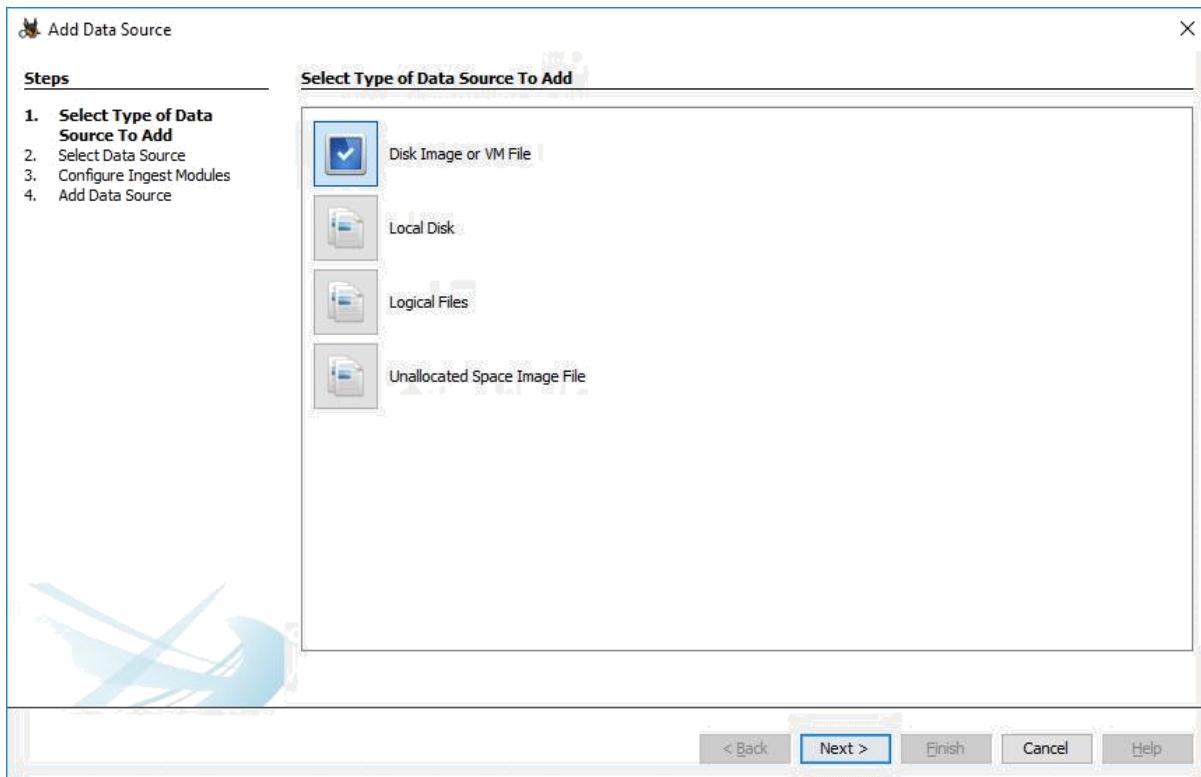
Notes:

Organization

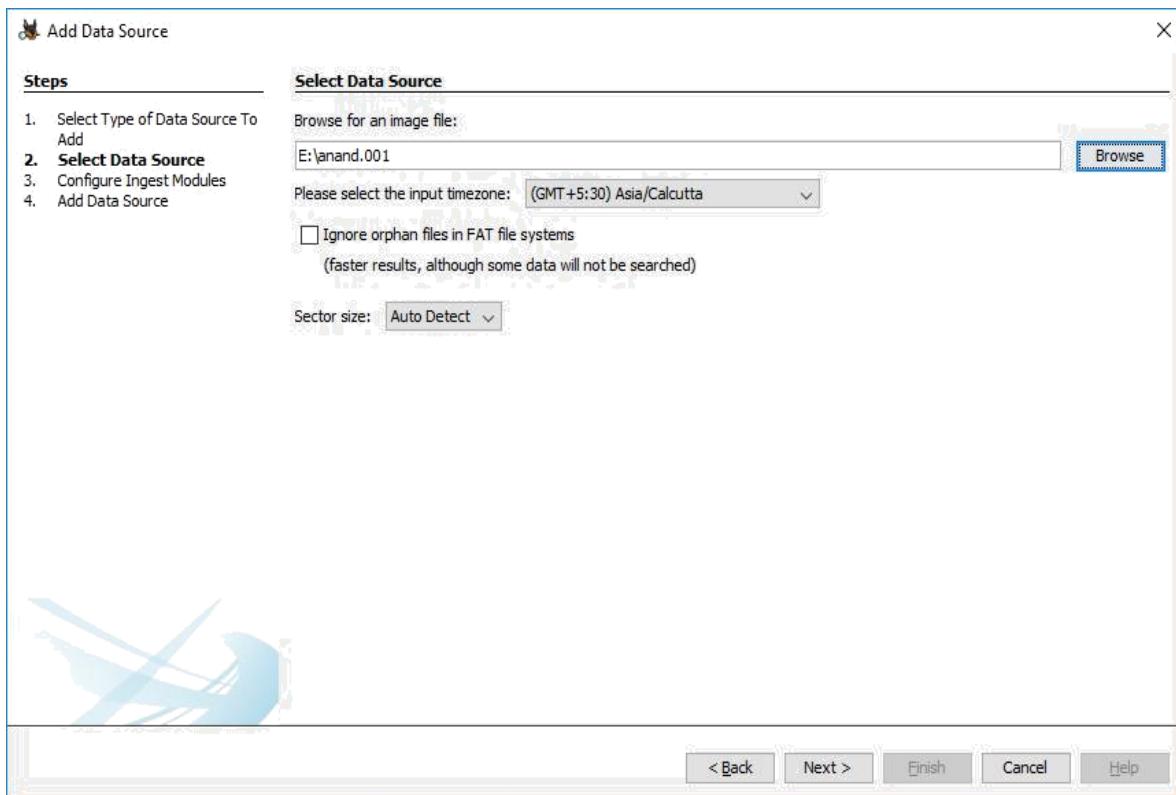
Organization analysis is being done for: Manage Organizations

< Back Finish Cancel Help

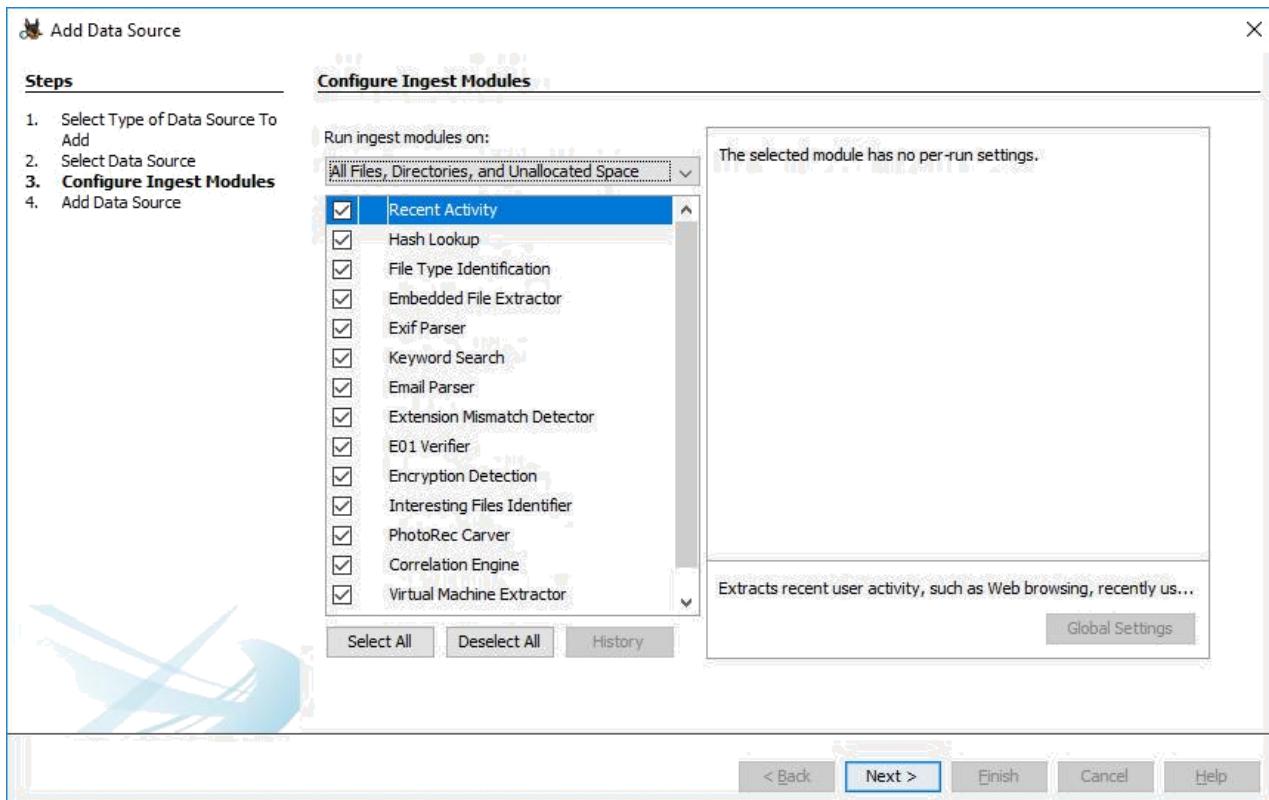
Step 5 : Now here we have to select Type of data source to add , in our case disk image or VM file and click on next



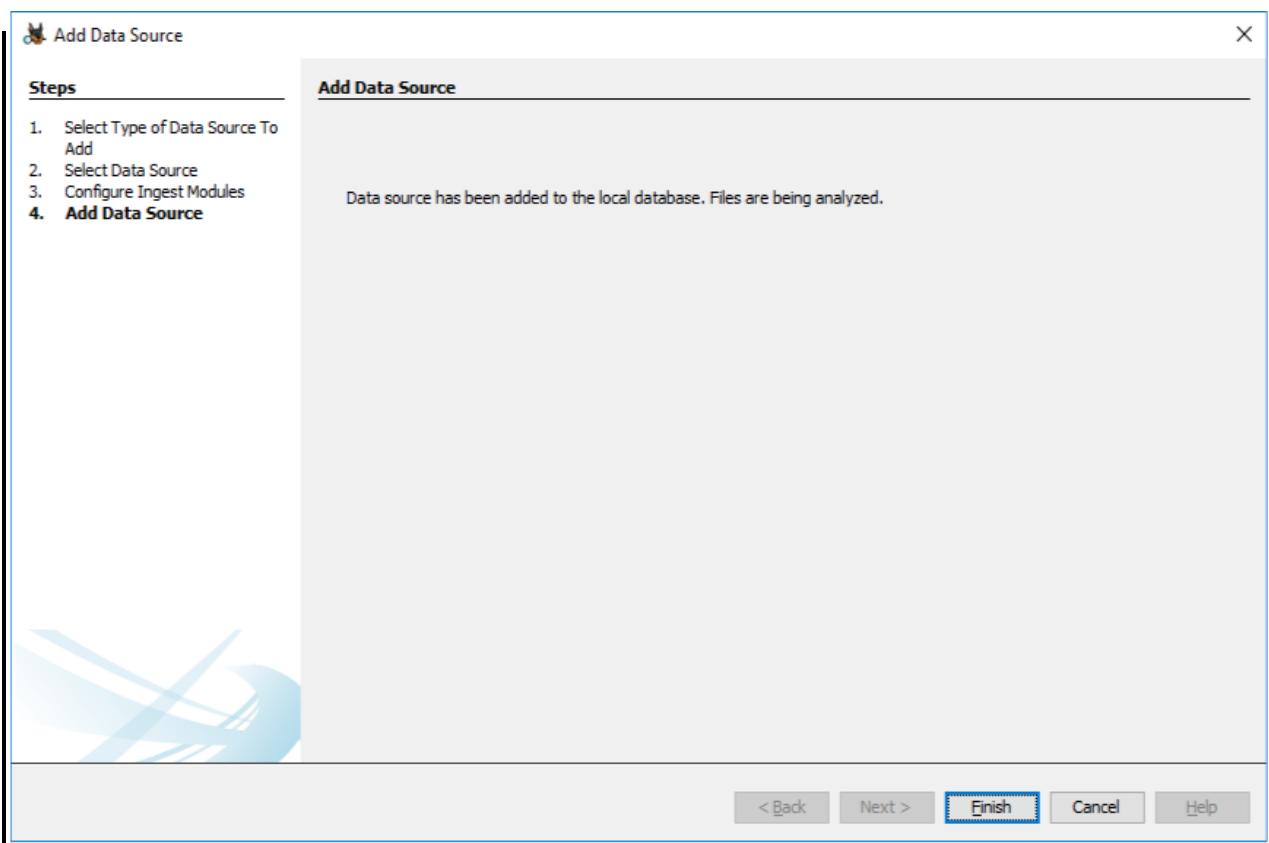
Step 6 : Now we have to select image file and click on next button



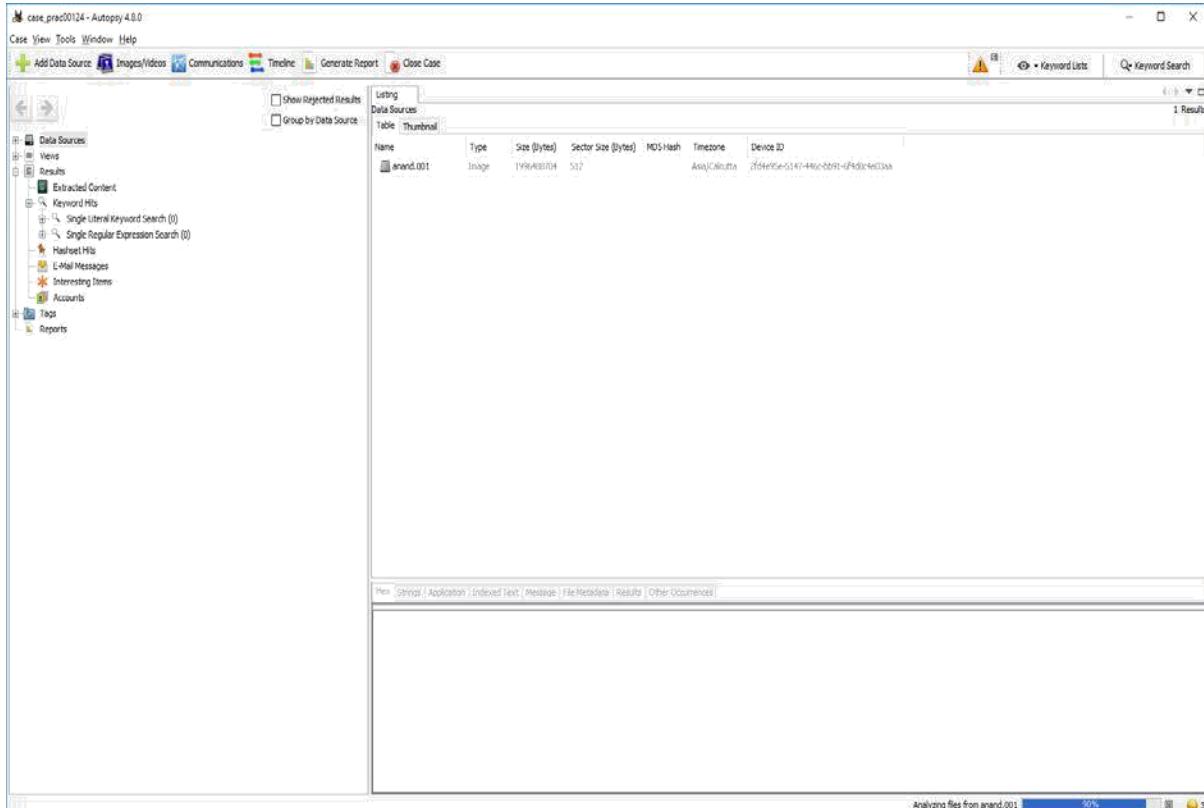
Step 7 : Now click on select all in order to Run ingest modules on: and click on next.



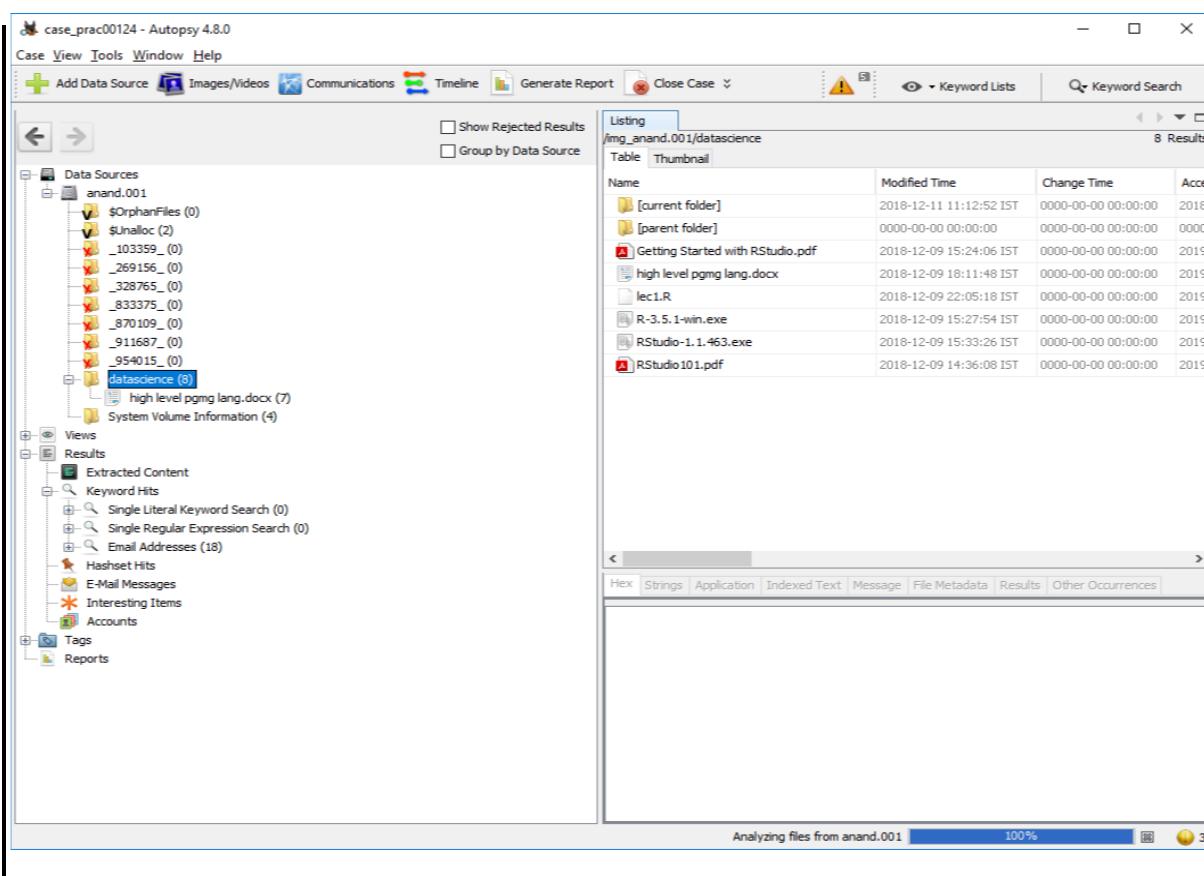
Step 8 : Now click on finish



Step 9 : Now Autopsy window will appear and it will analyse the disk that we have selected .



Step 10 : All image files appears in the Table tab. Select any file to see the data



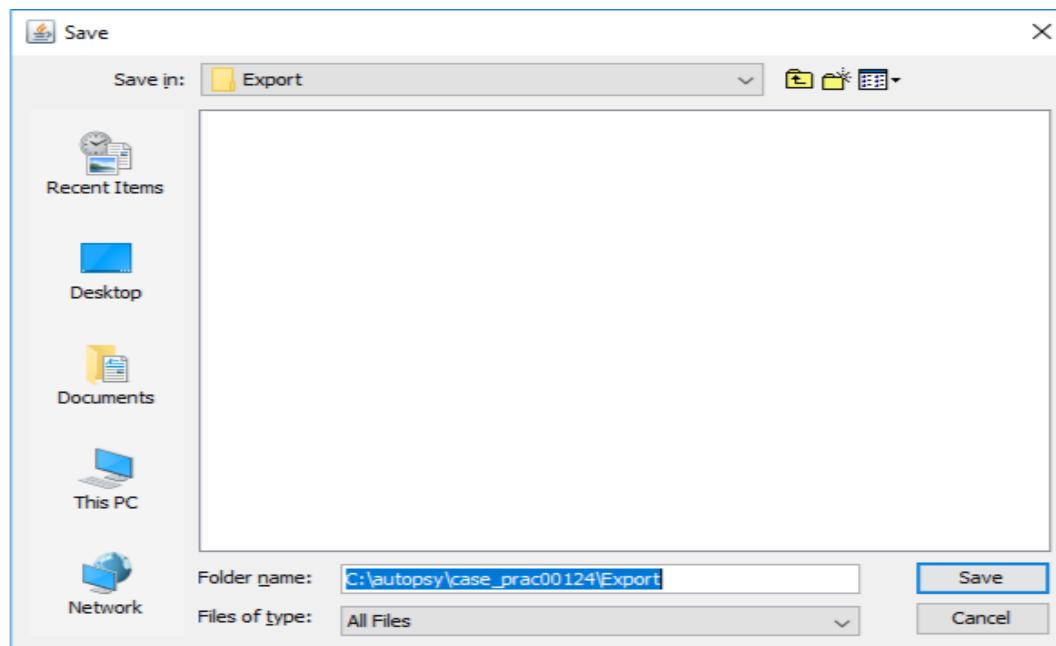
Step 11 : Expand the tree from left side panel to view the document files.

The screenshot shows the Autopsy 4.8.0 interface with the title bar "case_prac00124 - Autopsy 4.8.0". The menu bar includes Case, View, Tools, Window, Help, and several icons for Add Data Source, Images/Videos, Communications, Timeline, Generate Report, Close Case, Keyword Lists, and Keyword Search. The left sidebar contains a tree view with nodes for Data Sources (anand.001), Views (File Types, Deleted Files, MB File Size), Results (Extracted Content, Keyword Hits, Single Literal Keyword Search, Single Regular Expression Search, Email Addresses, HashSet Hits, E-Mail Messages, Interesting Items, Accounts), Tags, and Reports. The main pane is titled "Listing" and shows a table of file results. The table has columns for Name and Location. A specific file, "870109", is selected and highlighted in blue. The table lists various files including ".269156", ".328765", ".954015", ".833375", ".911687", ".103359", "mongodb-win32-x86_64-2012plus-signed.msi", "f1597948.exe", "f1682120.txt", "f1682256.java", "f1682304.pcx", "f1682332.deb", "f1682380.deb", "f1682512.deb", and "f1683808.deb". Below the table, there are tabs for Hex, Strings, Application, Indexed Text, Message, File Metadata, Results, and Other Occurrences. The Indexed Text tab is active, showing the message "No indexed text for this file." The status bar at the bottom right shows a yellow circle with the number 3.

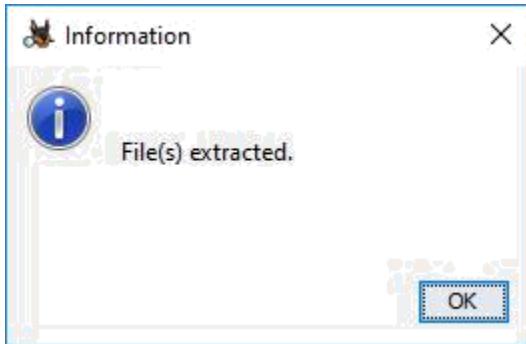
Step 12 : To recover the files , go to view code → Deleted files node , here select any file and right click on it then select Extract files option

The screenshot shows the Autopsy 4.8.0 interface. The left sidebar contains navigation links such as Data Sources, Views, MB File Size, Results, Tags, and Reports. The main area displays a listing of files from the 'anand.001' data source. The listing table has columns for Name and Location. A context menu is open over a file named 'f1682120.txt'. The menu options include Properties, View File in Directory, View in New Window, Open in External Viewer, View File in Timeline..., Extract File(s), Add File Tag, Remove File Tag, and Add file to hash set. The 'Indexed Text' tab is selected in the bottom panel, which shows the text 'No indexed text for this file.'

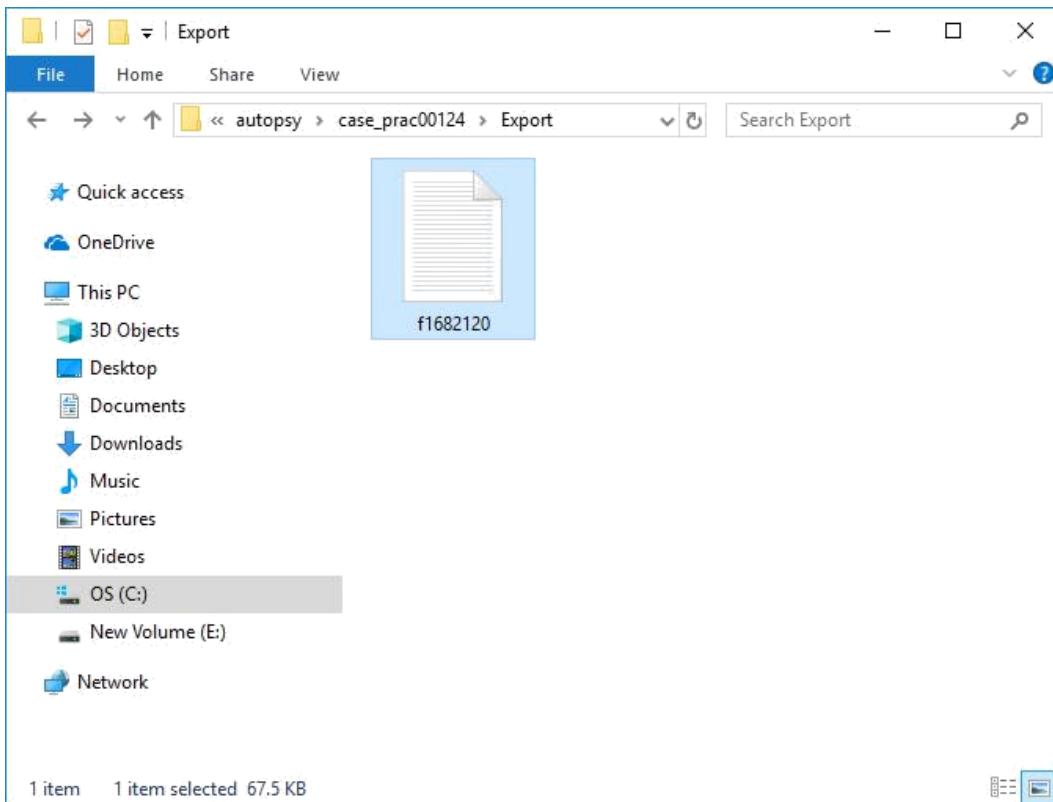
Step 12: Select Path where you want to save extracted file and click on save .



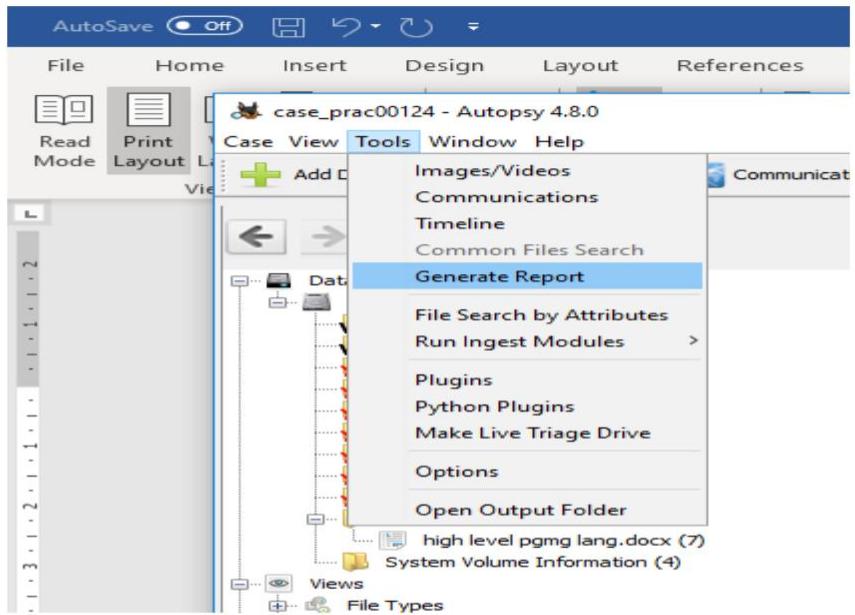
Step 13 : Now click on OK



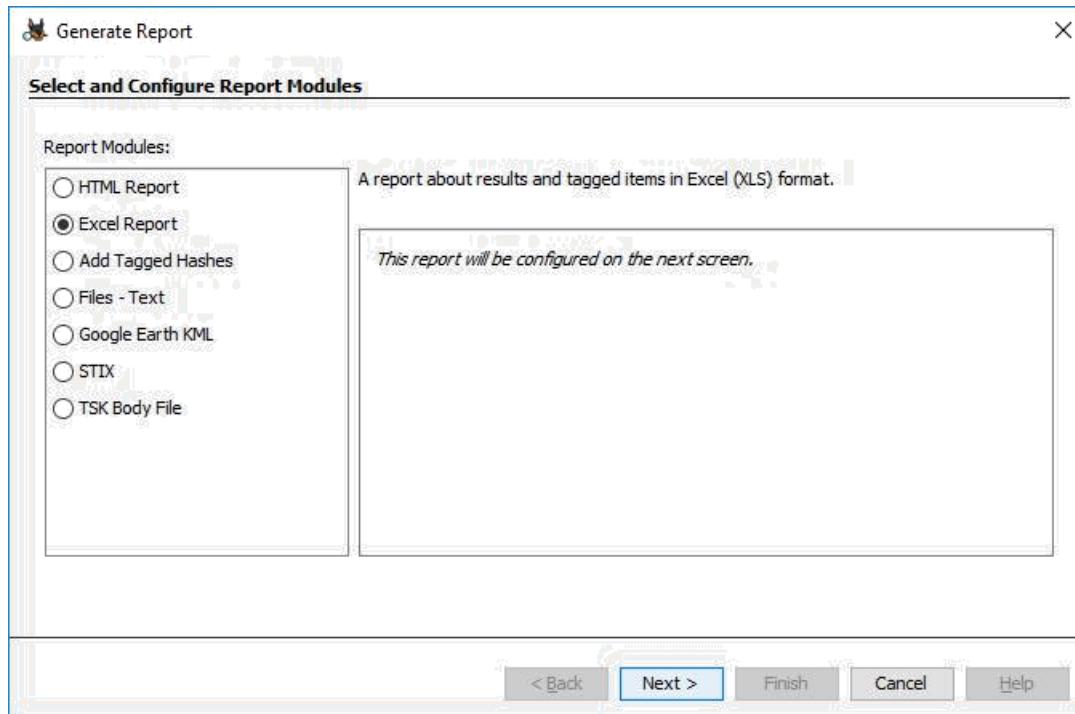
Step 14 : Now go to C:\autopsy\case_prac00124\Export folder to see recover file



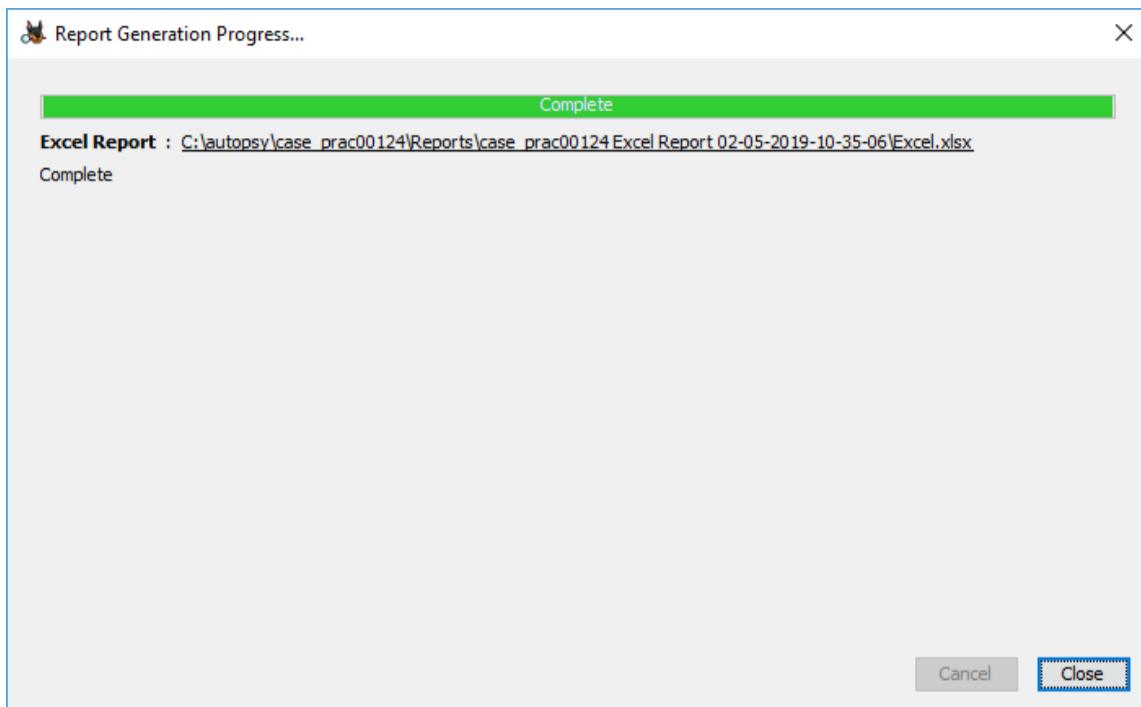
Step 15 : Click on generate report from Autopsy window and select the Excel format and click on next



Step 16 : This window will appear



Step 17 : Now report is generated so click on close button. We can see the Report on Report Node



Step 18 : Click on report

The screenshot shows the Autopsy digital forensics tool interface. The menu bar includes Case, View, Tools, Window, Help. The toolbar has icons for Add Data Source, Images/Videos, Communications, Timeline, Generate Report, and Close Case. The left sidebar navigation includes Data Sources, Views, Results, and Tags. The main pane displays a "Listing" table with the following data:

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

At the bottom, tabs for Hex, Strings, Application, Indexed Text, Message, and File Meta are visible.

PRACTICAL 4

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

Identification the live network

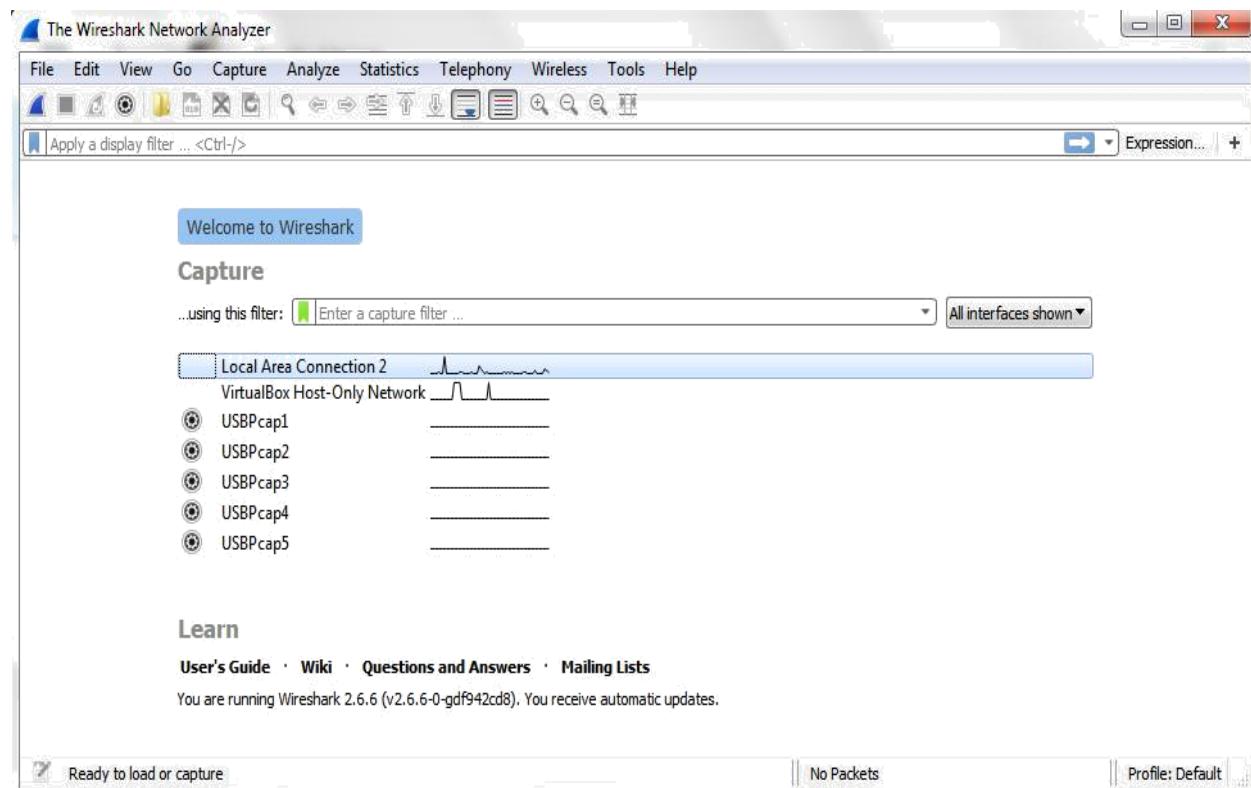
Capture Packets

Analyze the captured packets

Capturing Packets

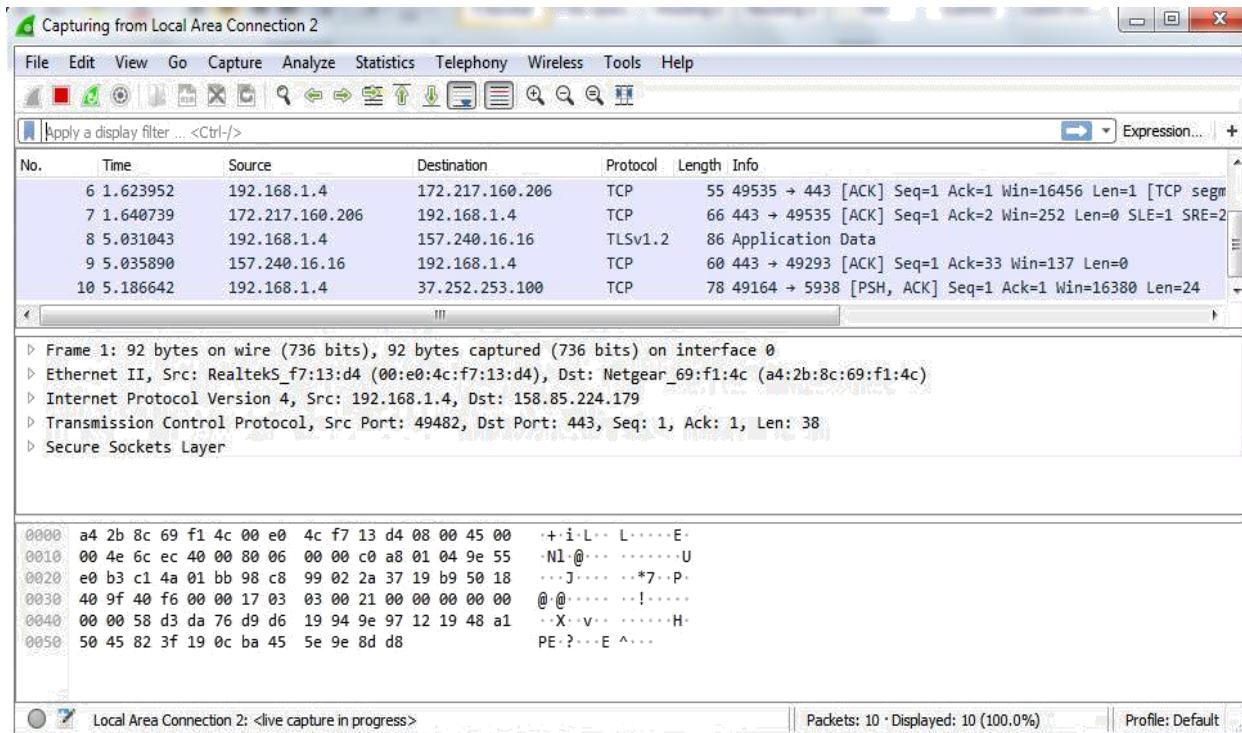
Capture traffic on your wireless network, click your wireless interface.

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



As soon as you single-click on your network interface's name, you can see how the packets are working in real time. Wireshark will capture all the packets going in and out of our systems.

Promiscuous mode is the mode in which you can see all the packets from other systems on the network and not only the packets send or received from your network adapter. Promiscuous mode is enabled by default. To check if this mode is enabled, go to Capture and Select Options. Under this window check, if the checkbox is selected and activated at the bottom of the window. The checkbox says “Enable promiscuous mode on all interfaces”.



The red box button “STOP” on the top left side of the window can be clicked to stop the capturing of traffic on the network.

Color Coding

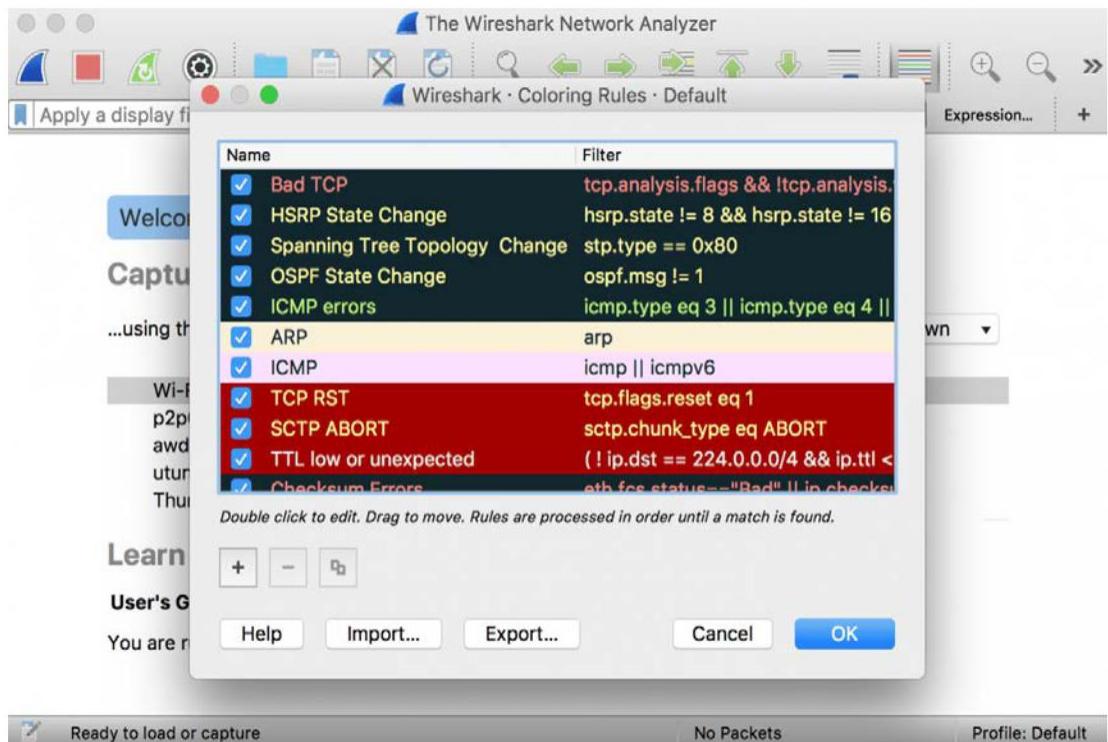
Different packets are seen highlighted in various different colors. This is Wireshark’s way of displaying traffic to help you easily identify the types of it. Default colors are:

Light Purple color for TCP traffic

Light Blue color for UDP traffic

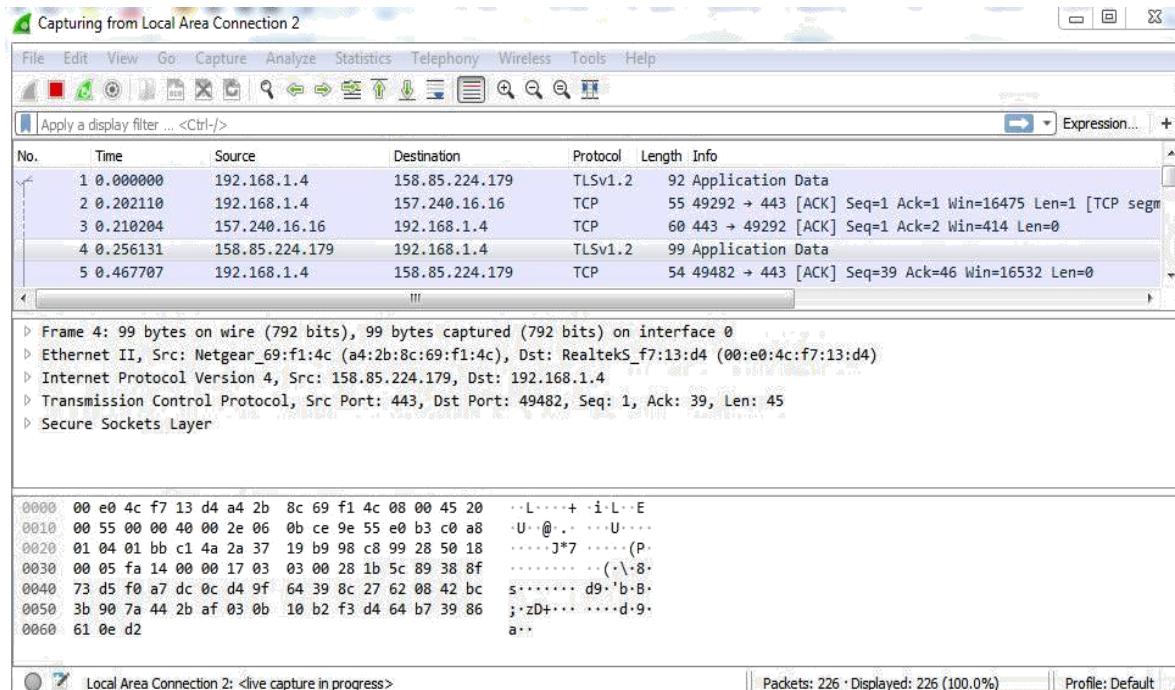
Black color identifies packets with errors – example these packets are delivered in an unordered manner.

To check the color coding rules click on View and select Coloring Rules. These color coding rules can be customized and modified to fit your needs.

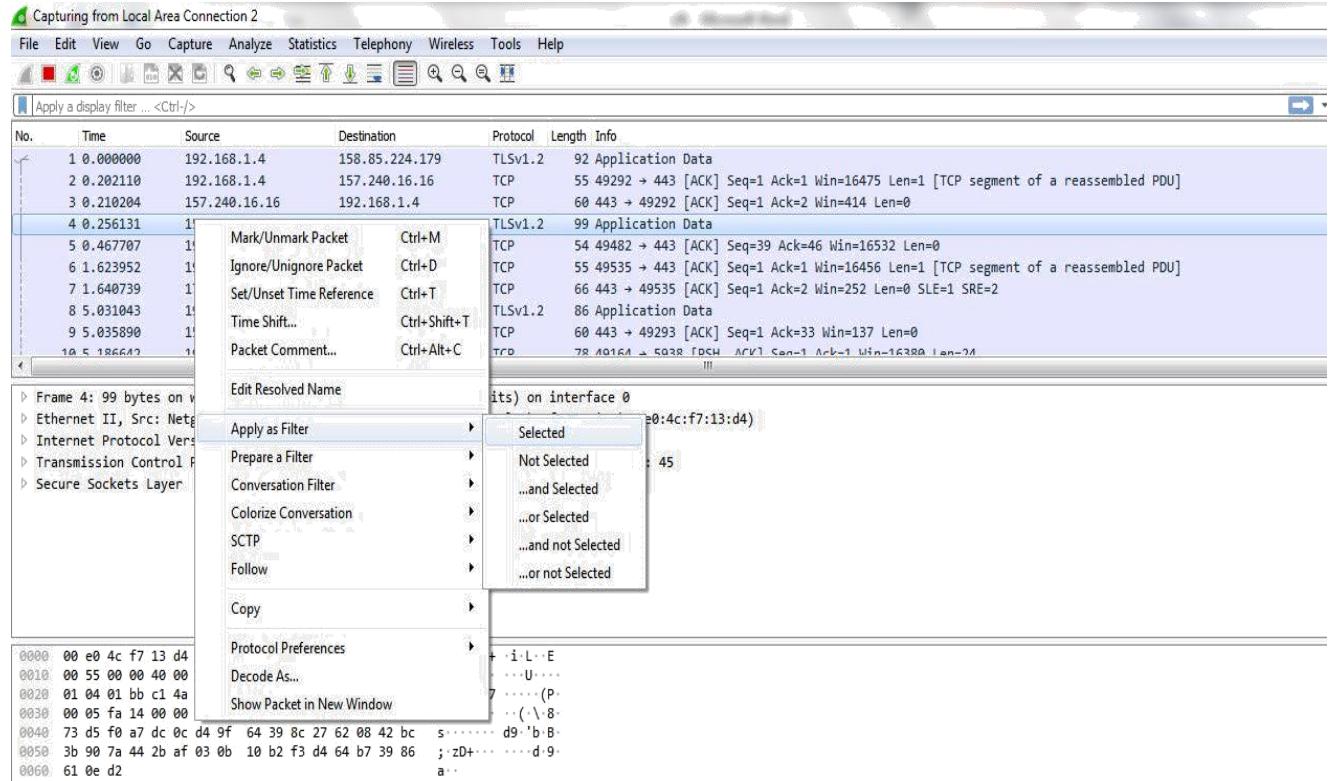


Analyze the captured Packets:

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



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



Display filter command –

1. Display packets based on specific IP-address

`ip.addr == 192.0.2.1`

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

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

ip.src == 192.168.1.3

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.3	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
2	0.293839	192.168.1.3	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
3	0.591360	192.168.1.3	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
12	10.037574	192.168.1.3	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
13	10.333930	192.168.1.3	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
14	10.633876	192.168.1.3	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
16	12.458395	192.168.1.3	224.0.0.251	MDNS	103	Standard query 0x0059 PTR _233637DE._sub._googlecast._tcp.local, "QM" question PTR _googlecast._tcp.lo
19	20.010644	192.168.1.3	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
20	20.301273	192.168.1.3	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
21	20.602551	192.168.1.3	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
22	20.619775	192.168.1.3	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1

3. Display packets which are having specific IP-address destination

ip.dst == 192.168.1.1

No.	Time	Source	Destination	Protocol	Length	Info
4	4.037895	192.168.1.4	192.168.1.1	DNS	85	Standard query 0xc7f4 A teredo.ipv6.microsoft.com
6	5.032826	192.168.1.4	192.168.1.1	DNS	85	Standard query 0xc7f4 A teredo.ipv6.microsoft.com
7	6.032784	192.168.1.4	192.168.1.1	DNS	85	Standard query 0xc7f4 A teredo.ipv6.microsoft.com
11	8.032694	192.168.1.4	192.168.1.1	DNS	85	Standard query 0xc7f4 A teredo.ipv6.microsoft.com
15	12.033085	192.168.1.4	192.168.1.1	DNS	85	Standard query 0xc7f4 A teredo.ipv6.microsoft.com
55	74.984400	192.168.1.4	192.168.1.1	TCP	66	49173 → 56688 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
57	74.984875	192.168.1.4	192.168.1.1	TCP	54	49173 → 56688 [ACK] Seq=1 Ack=1 Win=65700 Len=0
58	74.985092	192.168.1.4	192.168.1.1	HTTP	250	GET /rootDesc.xml HTTP/1.1
64	74.987818	192.168.1.4	192.168.1.1	TCP	54	49173 → 56688 [ACK] Seq=197 Ack=4102 Win=65700 Len=0
65	74.989866	192.168.1.4	192.168.1.1	TCP	54	49173 → 56688 [FIN, ACK] Seq=197 Ack=4102 Win=65700 Len=0
80	0E.721021	192.168.1.4	192.168.1.1	DNS	0	Standard query Buf=02 A teredo.ipv6.microsoft.com

4. Display packets which are using http protocol http

No.	Time	Source	Destination	Protocol	Length	Info
58	74.985092	192.168.1.4	192.168.1.1	HTTP	250	GET /rootDesc.xml HTTP/1.1
62	74.987756	192.168.1.1	192.168.1.4	HTTP/X...	1234	HTTP/1.1 200 OK
972	129.457310	192.168.1.4	172.217.166.174	HTTP	1000	GET / HTTP/1.1
975	129.542230	172.217.166.174	192.168.1.4	HTTP	594	HTTP/1.1 301 Moved Permanently (text/html)
39156	277.292187	192.168.1.4	117.18.237.29	OCSP	137	Request
39157	277.314544	117.18.237.29	192.168.1.4	OCSP	842	Response
39168	277.419340	192.168.1.4	117.18.237.29	OCSP	137	Request
39169	277.463638	117.18.237.29	192.168.1.4	OCSP	842	Response
39204	279.409683	192.168.1.4	23.57.219.27	OCSP	137	Request
39206	279.420870	23.57.219.27	192.168.1.4	OCSP	712	Response
39219	279.483458	192.168.1.4	23.57.219.27	OCSP	137	Request

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

No.	Time	Source	Destination	Protocol	Length	Info
40	50.307358	192.168.1.3	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
41	50.607228	192.168.1.3	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
46	60.015835	192.168.1.3	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
47	60.306194	192.168.1.3	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
48	60.605851	192.168.1.3	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
49	70.031605	192.168.1.3	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
50	70.321279	192.168.1.3	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
51	70.626289	192.168.1.3	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
53	73.874454	192.168.1.4	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
58	74.985092	192.168.1.4	192.168.1.1	HTTP	250	GET /rootDesc.xml HTTP/1.1
59	74.985092	192.168.1.4	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1

6. Display packets which are using TCP protocol tcp

No.	Time	Source	Destination	Protocol	Length	Info
31	41.077503	192.168.1.4	188.65.76.135	TCP	54	49163 → 5938 [ACK] Seq=25 Ack=25 Win=16592 Len=0
32	41.184894	188.65.76.135	192.168.1.4	TCP	78	[TCP Spurious Retransmission] 5938 → 49163 [PSH, ACK] Seq=1 Ack=25 Win=1022 Len=24
33	41.184946	192.168.1.4	188.65.76.135	TCP	66	[TCP Dup ACK 3181] 49163 → 5938 [ACK] Seq=25 Ack=25 Win=16592 Len=0 SRE=25
37	45.858801	192.168.1.4	188.65.76.135	TCP	78	49163 → 5938 [PSH, ACK] Seq=25 Ack=25 Win=16592 Len=24
38	46.087275	188.65.76.135	192.168.1.4	TCP	60	5938 → 49163 [ACK] Seq=25 Ack=49 Win=1022 Len=0
45	54.780090	192.168.1.4	104.25.218.21	TCP	54	49171 → 443 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
55	74.984400	192.168.1.4	192.168.1.1	TCP	66	49173 → 56688 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
56	74.984790	192.168.1.1	192.168.1.4	TCP	66	56688 → 49173 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1 WS=2
57	74.984875	192.168.1.4	192.168.1.1	TCP	54	49173 → 56688 [ACK] Seq=1 Ack=1 Win=65700 Len=0
58	74.985092	192.168.1.4	192.168.1.1	HTTP	250	GET /rootDesc.xml HTTP/1.1
59	74.985092	192.168.1.1	102.168.1.4	TCP	60	56688 → 102.168.1.4 [ACK] Seq=1 Ack=107 Win=65700 Len=0

7. Display packets having no error connecting to server

http.response.code==200

No.	Time	Source	Destination	Protocol	Length	Info
40241	315.834863	27.106.94.17	192.168.1.4	TCP	455	HTTP/1.1 200 OK [TCP segment of a reassembled PDU]
40251	315.941483	192.168.1.1	192.168.1.4	HTTP/X...	315	HTTP/1.1 200 OK
40261	315.967166	192.168.1.1	192.168.1.4	HTTP	250	HTTP/1.1 200 OK
40270	315.968680	192.168.1.4	192.168.1.1	HTTP	191	HTTP/1.1 200 OK
40282	315.977822	192.168.1.1	192.168.1.4	HTTP/X...	539	HTTP/1.1 200 OK
40294	315.982033	192.168.1.1	192.168.1.4	HTTP/X...	557	HTTP/1.1 200 OK
40308	315.999143	192.168.1.1	192.168.1.4	HTTP/X...	315	HTTP/1.1 200 OK
40318	316.005125	192.168.1.1	192.168.1.4	HTTP	250	HTTP/1.1 200 OK
40327	316.007892	192.168.1.4	192.168.1.1	HTTP	191	HTTP/1.1 200 OK
40339	316.015485	192.168.1.1	192.168.1.4	HTTP/X...	539	HTTP/1.1 200 OK
40351	316.016280	192.168.1.1	192.168.1.4	HTTP/X...	557	HTTP/1.1 200 OK

8. Display packets having port number 80

tcp.port==80 || udp.port==80

No.	Time	Source	Destination	Protocol	Length	Info
40216	315.186100	192.168.1.4	172.217.160.206	TCP	54	49296 → 80 [ACK] Seq=1 Ack=1 Win=66240 Len=0
40217	315.186313	192.168.1.4	172.217.160.206	HTTP	293	HEAD /edged1/release2/chrome_component/Hp07sha1Vdw_4916/4916_all_crl-set-13576662708261436161.data.crx3 HTTP/1...
40218	315.209073	172.217.160.206	192.168.1.4	TCP	60	80 → 49295 [ACK] Seq=1 Ack=240 Win=61952 Len=0
40225	315.497872	172.217.160.206	192.168.1.4	HTTP	608	HTTP/1.1 302 Found
40228	315.512340	192.168.1.4	27.106.94.17	TCP	66	49296 → 80 [SYN] Seq=0 Win=8192 MSS=1460 WS=4 SACK_PERM=1
40231	315.693760	192.168.1.4	172.217.160.206	TCP	54	49295 → 80 [ACK] Seq=240 Ack=555 Win=65684 Len=0
40237	315.823271	27.106.94.17	192.168.1.4	TCP	66	80 → 49296 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1452 SACK_PERM=1 WS=256
40238	315.823365	192.168.1.4	27.106.94.17	TCP	54	49296 → 80 [ACK] Seq=1 Ack=1 Win=66792 Len=0
40239	315.823550	192.168.1.4	27.106.94.17	HTTP	404	HEAD /edged1/release2/chrome_component/Hp07sha1Vdw_4916/4916_all_crl-set-13576662708261436161.data.crx3?cms_red...
40241	315.834863	27.106.94.17	192.168.1.4	HTTP	455	HTTP/1.1 200 OK

9.Display packets which that contains keyword facebook tcp contains facebook

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

PRACTICAL 5

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

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

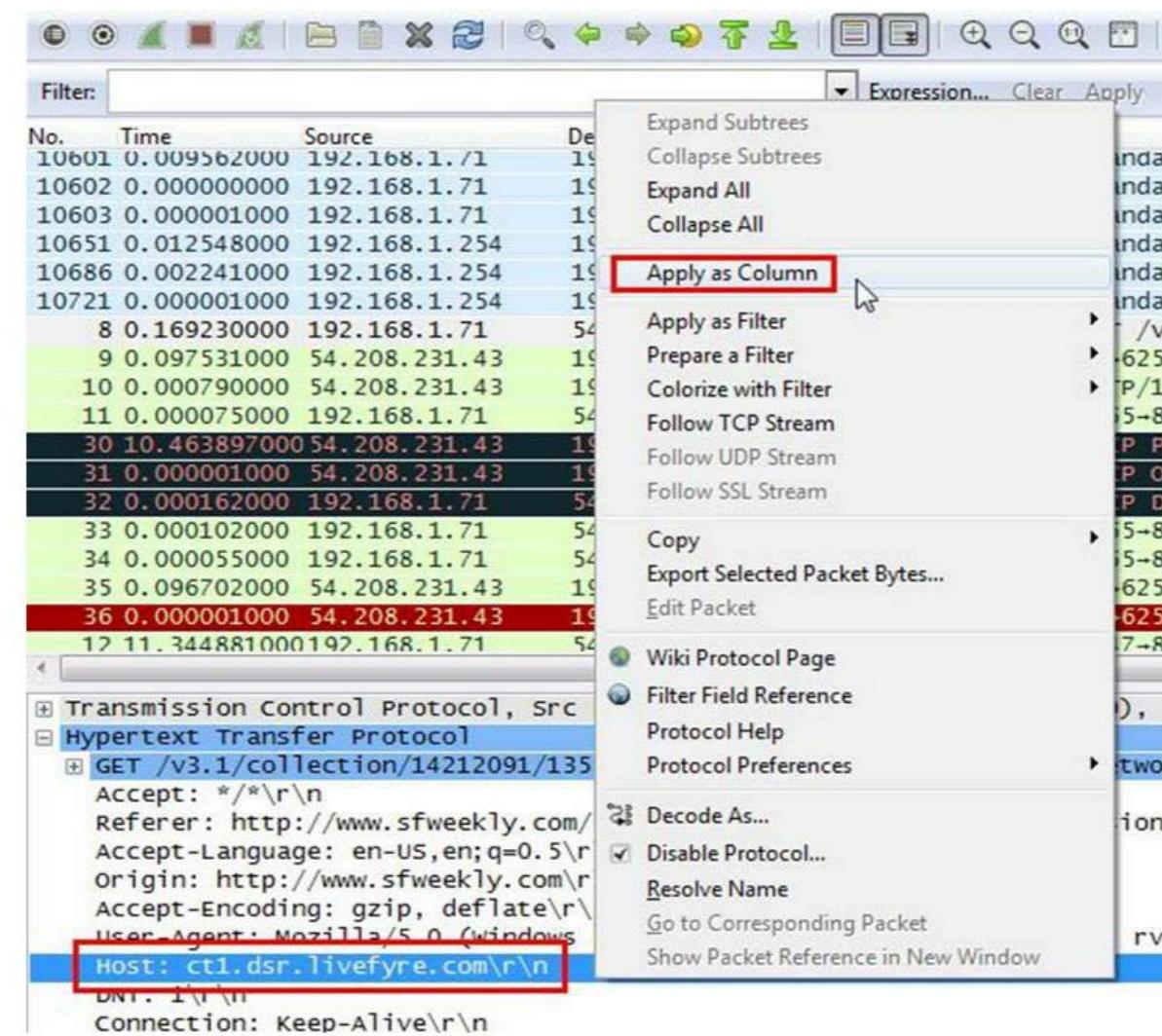
About what cell phone problem is the client concerned?

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

How many web servers are running Apache?

What web server software issued by www.snopes.com?

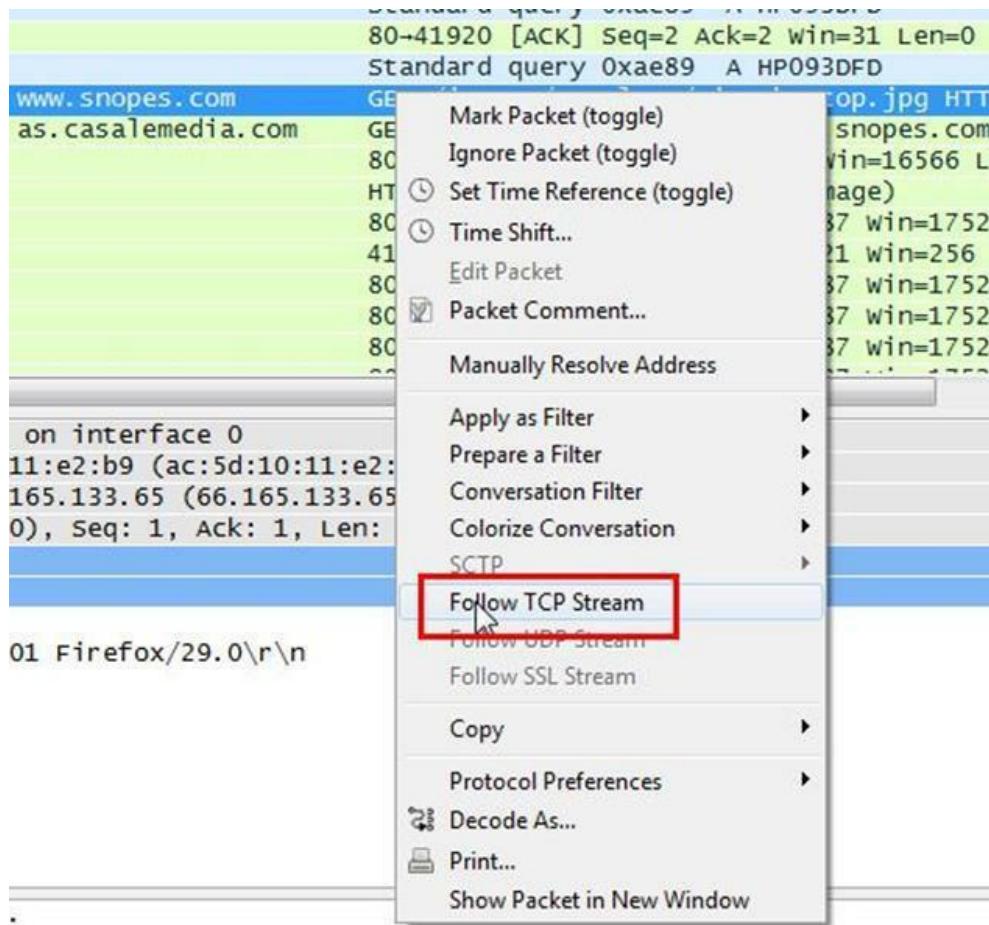
Analysis – The domain name be found from host header so we will set host header column where we will see all domain name. Select any HTTP request and expand the Hypertext Transfer Protocol then right click on Host header and then Apply as Column.



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

Time	Source	Destination	Protocol	Length	Host
11 0.055571000	192.168.1.254	192.168.1.71	DNS	222	
12 0.073696000	64.49.225.166	192.168.1.71	TCP	60	
13 0.000150000	192.168.1.71	64.49.225.166	TCP	54	
14 0.000056000	192.168.1.71	64.49.225.166	TCP	54	
15 0.036217000	fe80::856e:7b6d:6ff02::1:3		LLMNR	88	
16 0.001465000	192.168.1.68	224.0.0.252	LLMNR	68	
17 0.041273000	64.49.225.166	192.168.1.71	TCP	60	
18 0.057682000	192.168.1.68	224.0.0.252	LLMNR	68	
19 0.244659000	192.168.1.71	66.165.133.65	HTTP	440	www.snopes.com
20 0.018898000	192.168.1.71	207.109.230.161	HTTP	1037	as.casalemedia.com
21 0.025753000	207.109.230.161	192.168.1.71	TCP	60	
22 0.053733000	66.165.133.65	192.168.1.71	HTTP	1514	
23 0.000839000	66.165.133.65	192.168.1.71	TCP	1514	
24 0.000057000	192.168.1.71	66.165.133.65	TCP	54	
25 0.000751000	66.165.133.65	192.168.1.71	TCP	1514	
26 0.000775000	66.165.133.65	192.168.1.71	TCP	1514	
27 0.000002000	66.165.133.65	192.168.1.71	TCP	1514	

Right click on the selected packet and then select Follow TCP stream.



Now we can see the webserver name in server header it is Microsoft IIS 5.0

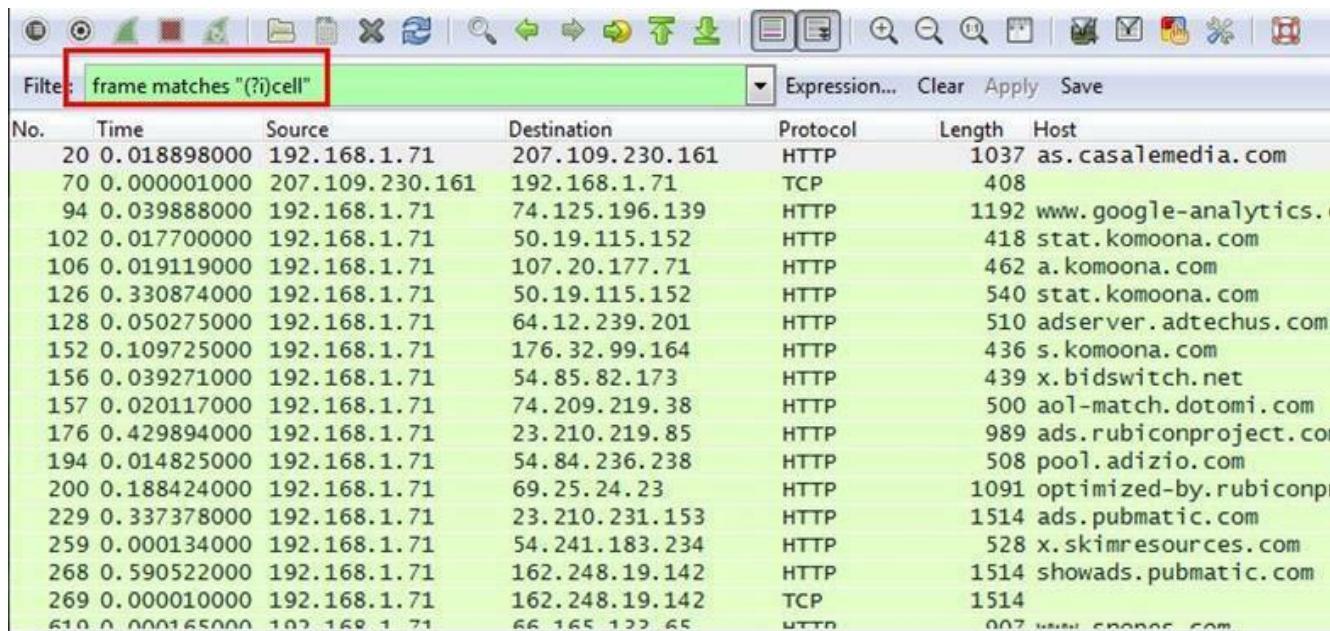
```
Stream Content
GET /images/template/site-bg-top.jpg HTTP/1.1
Host: www.snopes.com
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:29.0) Gecko/20100101 Firefox/29.0
Accept: image/png,image/*;q=0.8,*/*;q=0.5
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.snopes.com/style.css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

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

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

2. About what cell phone problem is the client concerned?

Analysis – Client talking about cell so we search for cell keyword in whole packets. We will use regular express for searching the cell keyword. Apply frame matches “(?! cell”



Frame List						
No.	Time	Source	Destination	Protocol	Length	Host
20	0.018898000	192.168.1.71	207.109.230.161	HTTP	1037	as.casalemedia.com
70	0.000001000	207.109.230.161	192.168.1.71	TCP	408	
94	0.039888000	192.168.1.71	74.125.196.139	HTTP	1192	www.google-analytics.com
102	0.017700000	192.168.1.71	50.19.115.152	HTTP	418	stat.komoona.com
106	0.0191119000	192.168.1.71	107.20.177.71	HTTP	462	a.komoona.com
126	0.330874000	192.168.1.71	50.19.115.152	HTTP	540	stat.komoona.com
128	0.050275000	192.168.1.71	64.12.239.201	HTTP	510	adserver.adtechus.com
152	0.109725000	192.168.1.71	176.32.99.164	HTTP	436	s.komoona.com
156	0.039271000	192.168.1.71	54.85.82.173	HTTP	439	x.bidswitch.net
157	0.0201117000	192.168.1.71	74.209.219.38	HTTP	500	aol-match.dotomi.com
176	0.429894000	192.168.1.71	23.210.219.85	HTTP	989	ads.rubiconproject.com
194	0.014825000	192.168.1.71	54.84.236.238	HTTP	508	pool.adizio.com
200	0.188424000	192.168.1.71	69.25.24.23	HTTP	1091	optimized-by.rubiconproject.com
229	0.337378000	192.168.1.71	23.210.231.153	HTTP	1514	ads.pubmatic.com
259	0.000134000	192.168.1.71	54.241.183.234	HTTP	528	x.skimresources.com
268	0.590522000	192.168.1.71	162.248.19.142	HTTP	1514	showads.pubmatic.com
269	0.000010000	192.168.1.71	162.248.19.142	TCP	1514	
610	0.000165000	192.168.1.71	66.165.122.65	HTTP	607	www.snopes.com

After applying the filter now, we will start to check every HTTP request. We noticed in the first HTTP request cell keyword is in URL and it was about cell phone charging issue.

Filter: frame matches "(?)cell"						
Time	Source	Destination	Protocol	Length	Info	
20 0.018898000	192.168.1.71	207.109.230.161	HTTP	1037	GET /s?5=81847&u=http%3A//www.snopes.com/horrors/techno/cellcharge.asp&f=1&id=4240355892.9460	
70 0.000001000	207.109.230.161	192.168.1.71	TCP	408	80-41932 [PSH, ACK] Seq=7318 Ack=984 Win=16566 Len=354	
94 0.039888000	192.168.1.71	74.125.196.139	HTTP	1192	GET /__utm.gif?utmwv=5.5.1&utmcn=1&utm-624349962&utmhn=www.snopes.com&utmcs=windows-1252&utm	
102 0.017700000	192.168.1.71	50.19.115.152	HTTP	418	GET /s?tagid=cad674db7f73589c9a110884ce73bb72_728_90&v=2.16&cb=516430883&ts=2 HTTP/1.1	
106 0.019119000	192.168.1.71	107.20.177.71	HTTP	462	GET /tag/cad674db7f73589c9a110884ce73bb72_728_90.js?l=http%3A%2F%2Fwww.snopes.com%2Fhorrors%2	
126 0.330874000	192.168.1.71	50.19.115.152	HTTP	540	GET /s?tagid=cad674db7f73589c9a110884ce73bb72&v=2.16&cb=516430883&ts=1&p=cad674db7f73589c9a1	
128 0.050275000	192.168.1.71	64.12.239.201	HTTP	510	GET /addyn/3.0/9423.1/3142865/0/225/ADTECH;loc=100;target=_blank;misc=%5BTIMESTAMP%50;rdclick	
152 0.109725000	192.168.1.71	176.32.99.164	HTTP	436	GET /passback/np/cad674db7f73589c9a110884ce73bb72.js HTTP/1.1	
156 0.039271000	192.168.1.71	54.85.82.173	HTTP	439	GET /sync?ssp=aol HTTP/1.1	
157 0.020117000	192.168.1.71	74.209.219.38	HTTP	500	GET /ao1/match?cb=https://ums.adtechus.com/mapuser?providerid=1013;userid=\$UID HTTP/1.1	
176 0.429894000	192.168.1.71	23.210.219.85	HTTP	989	GET /ad/9192.js HTTP/1.1	
194 0.014825000	192.168.1.71	54.84.236.238	HTTP	508	GET /sync?ssp=bidsswitchbidsswitch_ssp_id=aol HTTP/1.1	
200 0.188424000	192.168.1.71	69.25.24.23	HTTP	1091	GET /a/9192/1986/64229-2.js?cb=0.18771559557158202&tk_st=l&rp_s=c&p_exp=1&p_pos=atf&p_scree	
229 0.337378000	192.168.1.71	23.210.231.153	HTTP	1514	GET /AdServer/ja/showad.js?rn=516430883 HTTP/1.1	
259 0.000134000	192.168.1.71	54.241.183.234	HTTP	528	GET /?provider=ad1210&mode=check&uid=1039da81-f78e-44cc-a317-d4139ca80c0c HTTP/1.1	
268 0.590522000	192.168.1.71	162.248.19.142	HTTP	1514	GET /AdServer/AdvertiserServlet?pubid=32702&siteid=46838&adid=80732&kadwidth=728&kadheight=90&	
269 0.000010000	192.168.1.71	162.248.19.142	TCP	1514	41950-80 [ACK] Seq=1461 Ack=1 win=16445440 Len=1460	
610 0.000165000	192.168.1.71	66.165.132.46	HTTP	007	GET /techno/cellcharge.asp HTTP/1.1	
					ce 0	
					Sd:10:11:e2:b9)	
					74.125.196.139)	
					ck: 1, Len: 1138	
					utmcn=windows-1252&utmrv=1920x1080&utmvp=1920x953&utmcs=24-bit&utmul=en-us&utmje=1&utmfl=13.0%20r0&utmdt=snopes.com%3A%20Cell%20Phone%20Recharging%20Electroc	
					.0/r/n	

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

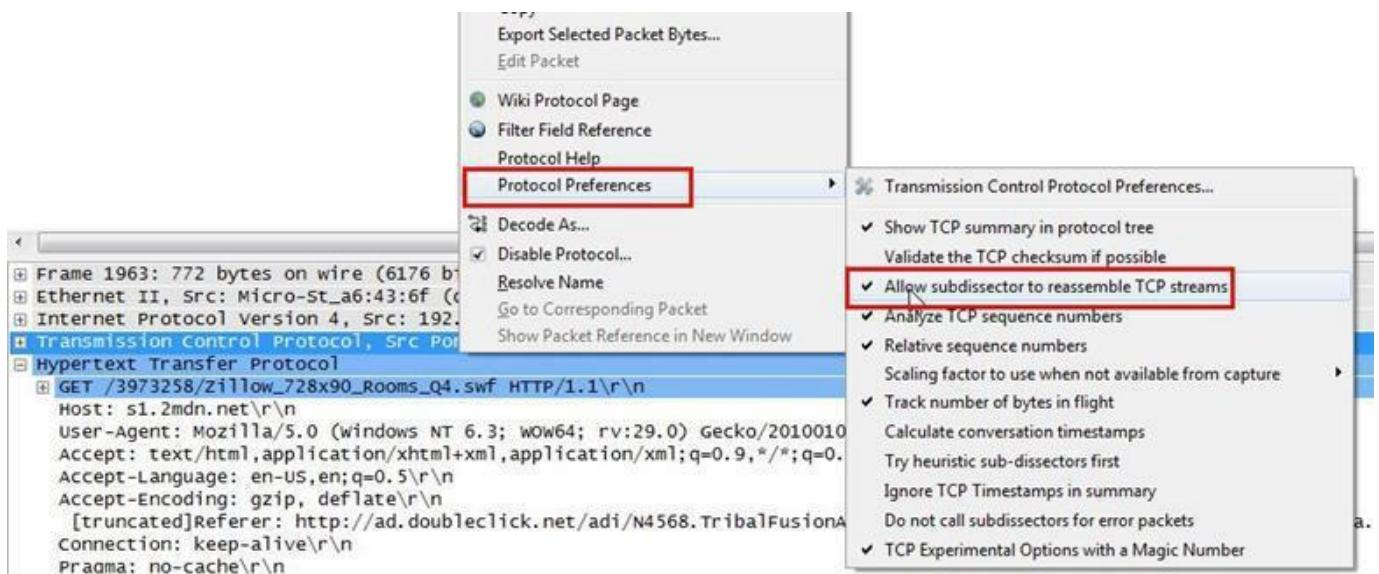
Analysis – As we did in the last challenge, we will apply a regular express filter for the Zillow keyword. Apply frame matched “(?) zillow”

Filter: frame matches "(?)zillow"						
Time	Source	Destination	Protocol	Length	Info	
94 0.039888000	192.168.1.71	74.125.196.139	HTTP	1192	GET /__utm.gif	
95 0.004442000	199.189.107.4	192.168.1.71	TCP	60	80-41929 [ACK]	
96 0.000769000	199.189.107.4	192.168.1.71	TCP	60	[TCP Dup ACK 9]	
97 0.060923000	199.189.107.4	192.168.1.71	TCP	60	80-41930 [FIN,	
98 0.000136000	192.168.1.71	199.189.107.4	TCP	54	41930->80 [ACK]	
99 0.000052000	192.168.1.71	199.189.107.4	TCP	54	41930->80 [FIN,	
100 0.015401000	74.125.196.139	192.168.1.71	TCP	60	80-41931 [ACK]	
101 0.000796000	74.125.196.139	192.168.1.71	HTTP	458	HTTP/1.1 200 OK	
102 0.017700000	192.168.1.71	50.19.115.152	HTTP	418	GET /s?tagid=c	
103 0.011551000	192.168.1.71	74.125.196.139	TCP	54	41931->80 [ACK]	
104 0.029132000	199.189.107.4	192.168.1.71	TCP	60	80-41930 [ACK]	
105 0.000000000	199.189.107.4	192.168.1.71	TCP	60	[TCP Dup ACK 10]	
106 0.019119000	192.168.1.71	107.20.177.71	HTTP	462	GET /tag/cad674	
107 0.034965000	50.19.115.152	192.168.1.71	TCP	60	80-41934 [ACK]	
108 0.001555000	50.19.115.152	192.168.1.71	HTTP	338	HTTP/1.1 200 OK	
109 0.023341000	192.168.1.71	199.189.107.4	TCP	54	[TCP Retransmis	
110 0.016019000	192.168.1.71	50.19.115.152	TCP	54	41934->80 [ACK]	
111 0.010773000	107.20.177.71	107.168.1.71	TCP	60	80-41935 [ACK]	

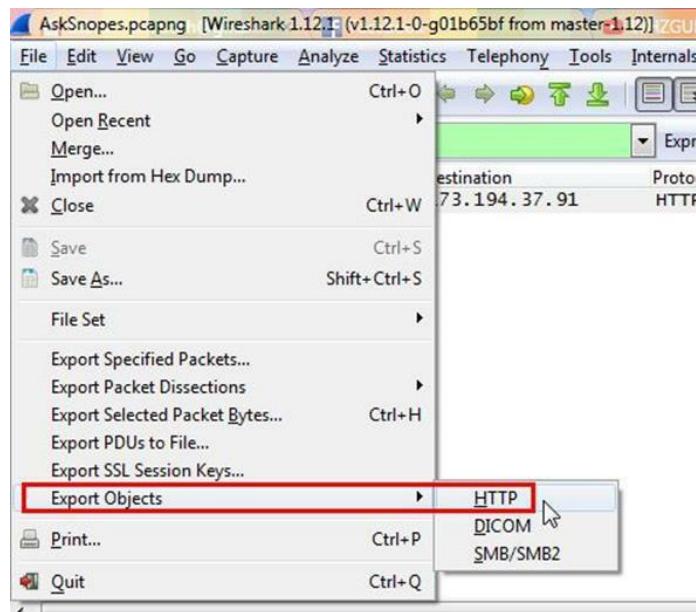
After applying the filter, we found only one packet with the Zillow keyword



Select the packet and expand the Hypertext Transfer Protocol tab right click on it go to Protocol Preferences and check Allow subdissector to reassemble TCP stream.



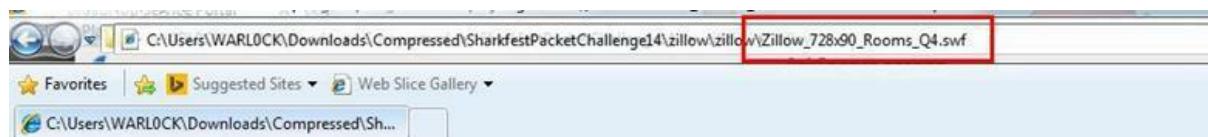
Now go to file and select Export Objects > HTTP. It will save all objects from the packet.



Click on save all.

Packet num	Hostname	Content Type	Size	Filename
52	www.snopes.com	image/jpeg	32 kB	site-bg-top.jpg
54		text/plain	15 bytes	
70	as.casalemedia.com	text/javascript	6735 bytes	cellcharge.asp&f=1&id=4240355892.9460454
101	www.google-analytics.com	image/gif	35 bytes	_utm.gif?utmwv=5.5.1&utms=1&utmn=624
108	stat.komoona.com	application/x-javascript	4 bytes	s?tagid=cad674db7f73589c9a110884ce73bb7:
112	a.komoona.com	application/x-javascript	815 bytes	cad674db7f73589c9a110884ce73bb7_728_90
129	stat.komoona.com	application/x-javascript	4 bytes	s?tagid=cad674db7f73589c9a110884ce73bb7:
133	adserver.adtechus.com	application/x-javascript	431 bytes	ADTECH;loc=100;target=_blank;misc=%5BTI
154	s.komoona.com	application/x-javascript	5603 bytes	cad674db7f73589c9a110884ce73bb7.js
182	ads.rubiconproject.com	text/javascript	18 kB	9192.js
205	optimized-by.rubiconproject.com	text/javascript	1852 bytes	64229-2.js?&cb=0.18771559557158202&tk_st:
212	ocsp.thawte.com	application/ocsp-request	115 bytes	\
215	ocsp.thawte.com	application/ocsp-response	1421 bytes	\
223	ocsp.thawte.com	application/ocsp-request	115 bytes	\
225	ocsp.thawte.com	application/ocsp-response	1421 bytes	\
251	ads.pubmatic.com	text/html	54 kB	showad.js?rn=516430883
261	x.skimresources.com	application/json	79 bytes	?provider=adizio&mode=check&uid=1039d
330	pr.ybp.yahoo.com	image/gif	43 bytes	E6EF997B-80FE-4373-AB1F-500144B03A7B
334	rt.legolas-media.com	image/gif	6 bytes	lgrt?ci=12&ti=64523&pbi=11057
346	um.eqads.com	text/html	196 bytes	pub.aspx?
353	ads.pubmatic.com	text/html	454 bytes	ro_x914.html

After saving all files in a directory and we found a swf file with name Zillow.
After opening the flash file, we saw that Zillow was trying to learn saxophone.

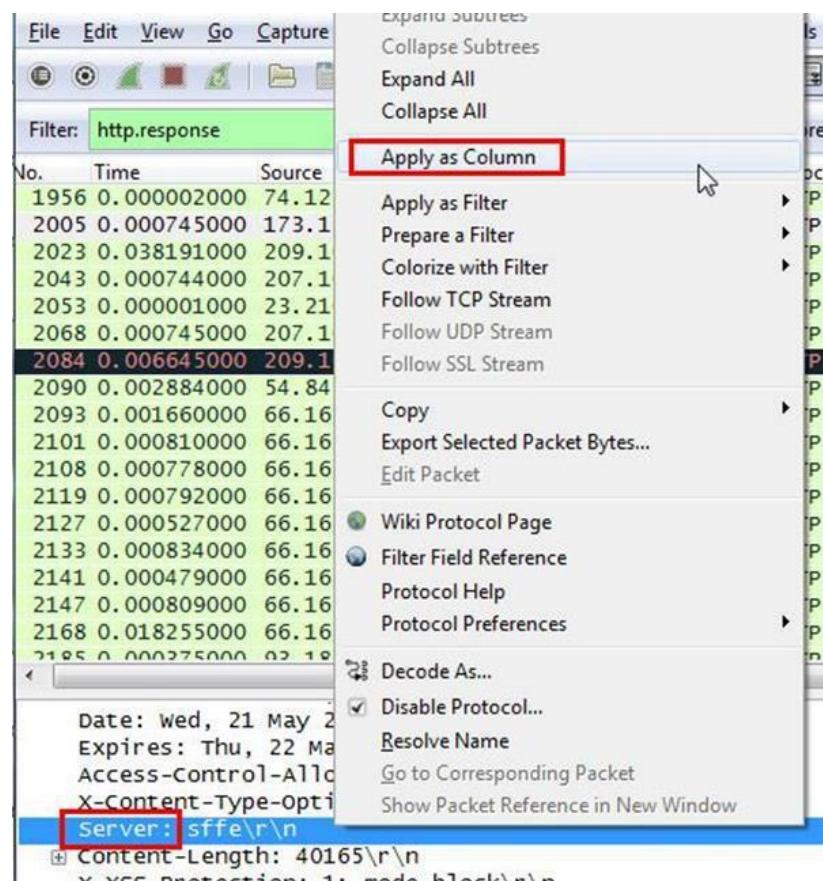


4. How many web servers are running Apache?

Analysis – The web server name can be retrieved from HTTP response header. So will apply filter http. response and we can see all http response packets.

No.	Time	Source	Destination	Protocol	Length	Info
1956	0.000002000	74.125.21.154	192.168.1.71	HTTP	432	HTTP/1.1 200 OK (text/javascript)
2005	0.000745000	173.194.37.91	192.168.1.71	HTTP	580	HTTP/1.1 200 OK (application/javascript)
2023	0.038191000	209.107.194.81	192.168.1.71	HTTP	1478	HTTP/1.1 200 OK (application/javascript)
2043	0.000744000	207.109.230.154	192.168.1.71	HTTP	1054	HTTP/1.1 200 OK (text/html)
2053	0.000001000	23.210.231.153	192.168.1.71	HTTP	178	HTTP/1.1 200 OK (text/html)
2068	0.000745000	207.109.230.154	192.168.1.71	HTTP	1054	HTTP/1.1 200 OK (text/html)
2084	0.006645000	209.107.194.81	192.168.1.71	HTTP	1478	[TCP Retransmission] HTTP/1.1 200 OK (text/html)
2090	0.002884000	54.84.148.104	192.168.1.71	HTTP	626	HTTP/1.1 200 OK (GIF89a)
2093	0.001660000	66.165.133.65	192.168.1.71	HTTP	1201	HTTP/1.1 200 OK (GIF89a)
2101	0.000810000	66.165.133.65	192.168.1.71	HTTP	673	HTTP/1.1 200 OK (GIF89a)
2108	0.000778000	66.165.133.65	192.168.1.71	HTTP	324	HTTP/1.1 200 OK (GIF89a)
2119	0.000792000	66.165.133.65	192.168.1.71	HTTP	176	HTTP/1.1 200 OK (GIF89a)
2127	0.000527000	66.165.133.65	192.168.1.71	HTTP	591	HTTP/1.1 200 OK (GIF89a)
2133	0.000834000	66.165.133.65	192.168.1.71	HTTP	482	HTTP/1.1 200 OK (GIF89a)
2141	0.000479000	66.165.133.65	192.168.1.71	HTTP	592	HTTP/1.1 200 OK (GIF89a)
2147	0.000809000	66.165.133.65	192.168.1.71	HTTP	1414	HTTP/1.1 200 OK (GIF89a)

Now we will set the server header as column select any packet and right click on it then select Apply as Column.



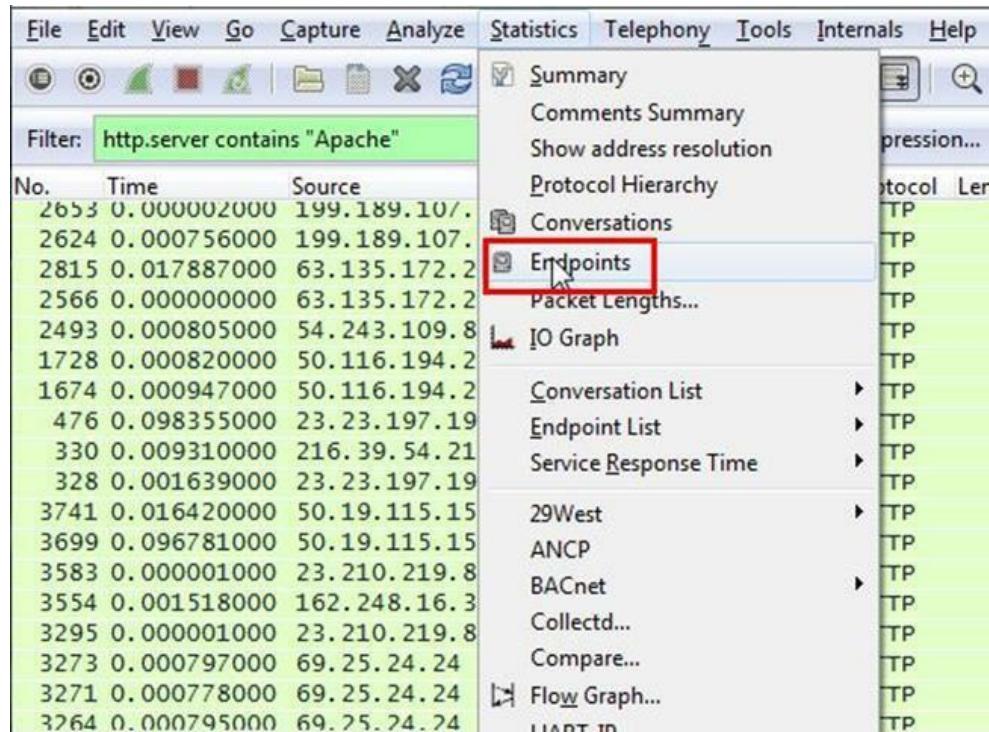
Now can see the server column where all server name is showing.

Destination	Protocol	Length	Server	Info
192.168.1.71	HTTP	828	sffe	HTTP/1.1 200 OK (JPEG JFIF image)
192.168.1.71	HTTP	580	sffe	HTTP/1.1 200 OK (application/x-shockwave-flash)
192.168.1.71	HTTP	807	sffe	HTTP/1.1 200 OK (text/javascript)
192.168.1.71	HTTP	463	sffe	HTTP/1.1 200 OK (text/javascript)
192.168.1.71	HTTP	959	radiumone/1.2	HTTP/1.1 200 OK (GIF89a)
192.168.1.71	HTTP	525	radiumone/1.2	HTTP/1.1 200 OK (text/html)
192.168.1.71	HTTP	875	post/2.0	HTTP/1.1 200 OK (application/x-javascript)
192.168.1.71	OCSP	829	ocsp_responder	response
192.168.1.71	HTTP	1159	nginx/1.5.3	HTTP/1.1 302 Found
192.168.1.71	HTTP	1092	nginx/1.5.3	HTTP/1.1 302 Found
192.168.1.71	HTTP	626	nginx/1.4.7	HTTP/1.1 200 OK (GIF89a)
192.168.1.71	HTTP	685	nginx/1.4.7	HTTP/1.1 302 Moved Temporarily
192.168.1.71	HTTP	626	nginx/1.4.7	HTTP/1.1 200 OK (GIF89a)
192.168.1.71	HTTP	626	nginx/1.4.7	HTTP/1.1 200 OK (GIF89a)
192.168.1.71	HTTP	681	nginx/1.4.7	HTTP/1.1 302 Moved Temporarily
192.168.1.71	HTTP	323	nginx/1.4.3	[TCP out-of-order] HTTP/1.1 302 Found
192.168.1.71	HTTP	303	nginx/1.4.3	HTTP/1.1 302 Found
192.168.1.71	HTTP	225	nginx/1.2.0	HTTP/1.1 200 OK (application/x-javascript)

Now we have to check how many Apache packets are there we can't count manually for each packet so we will apply another filter http.server contains "Apache"

Filter:	http.server contains "Apache"	Expression...	Clear	Apply	Save
No.	Time	Source	Destination	Protocol	Length
1811	0.051151000	50.19.115.152	192.168.1.71	HTTP	338
1609	0.003943000	50.19.115.152	192.168.1.71	HTTP	338
1483	0.000002000	23.210.219.85	192.168.1.71	HTTP	1078
1344	0.000747000	23.210.219.85	192.168.1.71	HTTP	1078
1317	0.016574000	50.19.115.152	192.168.1.71	HTTP	338
1295	0.000774000	107.20.177.71	192.168.1.71	HTTP	515
1287	0.001961000	50.19.115.152	192.168.1.71	HTTP	338
1222	0.015700000	207.109.230.161	192.168.1.71	HTTP	765
1173	0.001648000	69.25.24.24	192.168.1.71	HTTP	1171
1165	0.001172000	69.25.24.24	192.168.1.71	HTTP	1160
1139	0.001222000	69.25.24.24	192.168.1.71	HTTP	1121
669	0.001691000	69.25.24.24	192.168.1.71	HTTP	1128
182	0.000744000	23.210.219.85	192.168.1.71	HTTP	1078
129	0.038194000	50.19.115.152	192.168.1.71	HTTP	338
112	0.002082000	107.20.177.71	192.168.1.71	HTTP	955
108	0.001555000	50.19.115.152	192.168.1.71	HTTP	338
70	0.000001000	207.109.230.161	192.168.1.71	HTTP	408

After applying filter go to Statistics > Endpoints



It will show all connections

IPv4 Endpoints										
Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Latitude	Longitude	Altitude	Traffic
192.168.1.71	3 987	1 814 693	1 976	413 339	2 011	1 401 354	-	-	-	-
192.168.1.254	409	50 248	187	32 761	222	17 487	-	-	-	-
74.125.196.139	10	2 118	4	644	6	1 474	-	-	-	-
207.109.230.161	30	12 164	15	9 252	15	2 912	-	-	-	-
64.49.225.166	20	6 963	11	6 018	9	945	-	-	-	-
192.168.1.68	16	1 088	16	1 088	0	0	-	-	-	-
224.0.0.252	36	2 432	0	0	36	2 432	-	-	-	-
66.165.133.65	535	289 649	264	243 481	271	46 168	-	-	-	-
108.160.167.165	45	4 923	20	2 083	25	2 840	-	-	-	-
50.19.115.152	50	13 256	18	4 706	32	8 550	-	-	-	-
107.20.177.71	29	6 905	13	4 011	16	2 894	-	-	-	-
199.189.107.4	209	160 954	133	154 206	76	6 748	-	-	-	-
192.168.1.66	16	1 088	16	1 088	0	0	-	-	-	-
64.12.239.201	74	10 457	38	5 410	36	5 047	-	-	-	-
176.32.99.164	55	36 111	29	30 476	26	5 635	-	-	-	-
54.85.82.173	21	3 224	9	1 739	12	1 485	-	-	-	-
74.209.219.38	22	2 796	11	1 168	11	1 628	-	-	-	-
23.210.219.85	56	43 884	31	34 152	25	9 732	-	-	-	-
54.84.236.238	10	1 733	4	943	6	790	-	-	-	-
69.25.24.23	88	34 477	39	22 618	49	11 859	-	-	-	-
23.7.139.27	15	5 288	7	3 912	8	1 376	-	-	-	-
23.210.231.153	314	237 690	179	173 883	135	63 807	-	-	-	-

Check the limit to display filter then it will show the actual Apache connections. Now there are showing 22 connections but will exclude 192.168.1.71 because it is client's IP not a server IP so there are actual 21 Apache servers.

Ethernet: 2	Fibre Channel	FDD	IPv4: 22	IPv6	IPX	JXTA	NCP	RSVP	SCTP	TCP: 77	Token
IPv4 Endpoints - Filter: http.send											
Address	► Packets	► Bytes	► Tx Packets	► Tx Bytes	► Rx Packets	► Rx Bytes	► Latitude	► Longitude	►	►	►
207.109.230.161	2	1 173	2	1 173	0	0	0	0	0	0	0
192.168.1.71	80	60 911	0	0	80	60 911	0	0	0	0	0
50.19.115.152	13	4 394	13	4 394	0	0	0	0	0	0	0
107.20.177.71	4	3 143	4	3 143	0	0	0	0	0	0	0
23.210.219.85	6	6 468	6	6 468	0	0	0	0	0	0	0
23.210.231.153	12	6 163	12	6 163	0	0	0	0	0	0	0
23.23.197.19	2	1 179	2	1 179	0	0	0	0	0	0	0
216.39.54.212	1	225	1	225	0	0	0	0	0	0	0
162.248.19.136	3	2 363	3	2 363	0	0	0	0	0	0	0
162.248.16.24	2	1 692	2	1 692	0	0	0	0	0	0	0
69.25.24.24	13	15 024	13	15 024	0	0	0	0	0	0	0
207.109.230.154	3	3 162	3	3 162	0	0	0	0	0	0	0
50.97.236.98	2	1 753	2	1 753	0	0	0	0	0	0	0
69.25.24.26	3	3 087	3	3 087	0	0	0	0	0	0	0
50.116.194.21	1	1 045	1	1 045	0	0	0	0	0	0	0
50.116.194.28	1	527	1	527	0	0	0	0	0	0	0
54.243.109.84	1	609	1	609	0	0	0	0	0	0	0
63.135.172.251	2	837	2	837	0	0	0	0	0	0	0
199.189.107.4	4	3 950	4	3 950	0	0	0	0	0	0	0
50.63.243.230	1	1 007	1	1 007	0	0	0	0	0	0	0
207.109.230.187	3	3 036	3	3 036	0	0	0	0	0	0	0
162.248.16.37	1	74	1	74	0	0	0	0	0	0	0

Name resolution Limit to display filter

CONCLUSION: We have successfully analyzed the packets provided and solved the questions using wireshark.

PRACTICAL 6

AIM: Using Sysinternals tools for Network Tracking and Process Monitoring

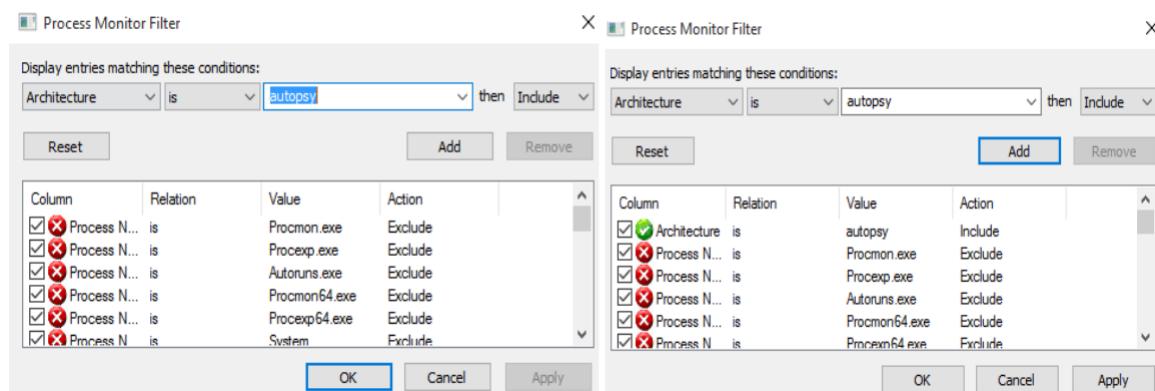
1. Check Sysinternals tools

→ Google sysinternal tools

2. Monitor Live Processes

Process Monitor is an advanced monitoring tool for Windows that shows real-time file system, Registry and process/thread activity. It combines the features of two legacy Sysinternals utilities, *Filemon* and *Regmon*, and adds an extensive list of enhancements including rich and non-destructive filtering, comprehensive event properties such session IDs and user names, reliable process information, full thread stacks with integrated symbol support for each operation, simultaneous logging to a file, and much more. Its uniquely powerful features will make Process Monitor a core utility in your system troubleshooting and malware hunting toolkit.

Sysinternal → procmon



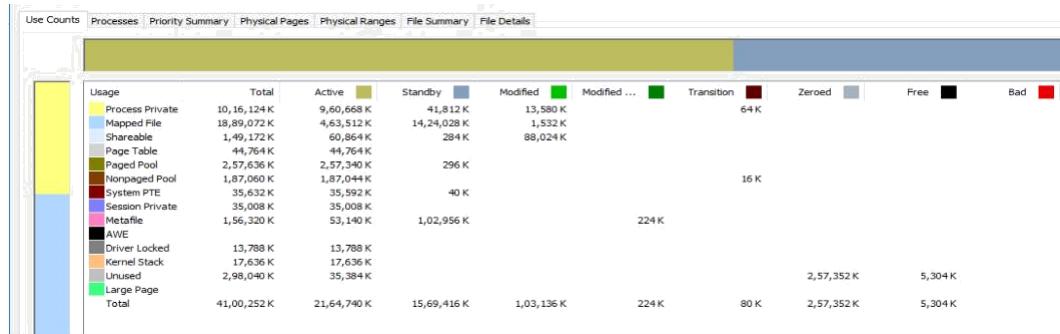
3. Capture RAM

RAMMap is an advanced physical memory usage analysis utility for Windows Vista and higher. It presents usage information in different ways on its several different tabs:

- Use Counts:* usage summary by type and paging list
- Processes:* process working set sizes
- Priority Summary:* prioritized standby list sizes
- Physical Pages:* per-page use for all physical memory
- Physical Ranges:* physical memory addresses
- File Summary:* file data in RAM by file
- File Details:* individual physical pages by file

Use RAMMap to gain understanding of the way Windows manages memory, to analyze application memory usage, or to answer specific questions about how RAM is being allocated. RAMMap's refresh feature enables you to update the display and it includes support for saving and loading memory snapshots.

STEPS sysinternal → RAMMap



4.Capture TCP/UDP packets

TCPView is a Windows program that will show you detailed listings of all TCP and UDP endpoints on your system, including the local and remote addresses and state of TCP connections. On Windows Server 2008, Vista, and XP, TCPView also reports the name of the process that owns the endpoint. TCPView provides a more informative and conveniently presented subset of the Netstat program that ships with Windows. The TCPView download includes Tcpvcon, a command-line version with the same functionality.

Using TCPView

When you start TCPView it will enumerate all active TCP and UDP endpoints, resolving all IP addresses to their domain name versions. You can use a toolbar button or menu item to toggle the display of resolved names. On Windows XP systems, TCPView shows the name of the process that owns each endpoint. By default, TCPView updates every second, but you can use the **Options|Refresh Rate** menu item to change the rate. Endpoints that change state from one update to the next are highlighted in yellow; those that are deleted are shown in red, and new endpoints are shown in green. You can close established TCP/IP connections (those labeled with a state of ESTABLISHED) by selecting **File|Close Connections**, or by right-clicking on a connection and choosing **Close Connections** from the resulting context menu. You can save TCPView's output window to a file using the **Save** menu item.

Using Tcpvcon

Tcpvcon usage is similar to that of the built-in Windows netstat utility:

Usage: tcpvcon [-a] [-c] [-n] [process name or PID]

Parameter Description

-a Show all endpoints (default is to show established TCP connections).

-c Print output as CSV.

-n Don't resolve addresses.

STEPS

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-vgrdu...	16323	sam+118.1e100.net	5228	ESTABLISHED				
chrome.exe	5808	TCP	desktop-vgrdu...	16375	111.101.23.22...	https	ESTABLISHED				
chrome.exe	5808	TCP	desktop-vgrdu...	16477	172.21.10.157	http	ESTABLISHED				
chrome.exe	5808	TCP	desktop-vgrdu...	16495	bom+0511-in+141...	https	ESTABLISHED				
chrome.exe	5808	TCP	desktop-vgrdu...	16501	bom+0715-in+101...	https	ESTABLISHED				
chrome.exe	5808	TCP	desktop-vgrdu...	16520	40.72.226.250	https	ESTABLISHED	1	3,090	1	436
chrome.exe	5808	TCP	desktop-vgrdu...	16525	151.101.36.133	https	ESTABLISHED				
chrome.exe	5808	TCP	desktop-vgrdu...	16528	52.162.216.193	https	ESTABLISHED				
chrome.exe	5808	TCP	desktop-vgrdu...	16529	52.162.216.193	https	ESTABLISHED				
chrome.exe	5808	TCP	desktop-vgrdu...	16530	52.162.216.193	https	ESTABLISHED				
chrome.exe	5808	UDP	DESKTOP-VGRDI...	5363	*	*				33	695
chrome.exe	5808	UDP	DESKTOP-VGRDI...	5363	*	*					
chrome.exe	5808	UDP	DESKTOP-VGRDI...	5363	*	*					
chrome.exe	5808	UDPv6	[0:0:0:0:0:0]	5363	*	*					
chrome.exe	5808	UDPv6	[0:0:0:0:0:0]	5363	*	*					
explorer.exe	3248	TCP	desktop-vgrdu...	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]	1540	[0:0:0:0:0:0]	0	LISTENING				
mysqld.exe	2280	TCP	DESKTOP-VGRDI...	3086	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]	1544	[0:0:0:0:0:0]	0	LISTENING				
services.exe	772	TCP	DESKTOP-VGRDI...	1545	DESKTOP-VGRDI...	0	LISTENING	1	414	1	202
services.exe	772	TCPv6	[0:0:0:0:0:0]	1545	[0:0:0:0:0:0]	0	LISTENING				
smokey.exe	1722	TCP	DESKTOP-VGRDI...	1539	DESKTOP-VGRDI...	0	LISTENING				
spoolsv.exe	1772	TCPv6	[0:0:0:0:0:0]	1539	[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-vgrdu...	ssdp	*	*					
svchost.exe	1152	UDP	DESKTOP-VGRDI...	ws-discovery	*	*					
svchost.exe	1152	UDP	DESKTOP-VGRDI...	ws-discovery	*	*					
svchost.exe	1328	UDP	DESKTOP-VGRDI...	5533	*	*				11	132
svchost.exe	326	UDP	DESKTOP-VGRDI...	5544	*	*				33	695
svchost.exe	1152	UDP	DESKTOP-VGRDI...	5517	*	*					
svchost.exe	1152	UDP	desktop-vgrdu...	57748	*	*					
svchost.exe	1152	UDP	DESKTOP-VGRDI...	57749	*	*					
svchost.exe	940	TCPv6	[0:0:0:0:0:0]	epmap	[0:0:0:0:0:0]	0	LISTENING				
svchost.exe	1144	TCPv6	[0:0:0:0:0:0]	1537	[0:0:0:0:0:0]	0	LISTENING				
svchost.exe	336	TCPv6	[0:0:0:0:0:0]	1538	[0:0:0:0:0:0]	0	LISTENING				
svchost.exe	1136	UDPv6	[0:0:0:0:0:0]	123	*	*					
svchost.exe	1152	UDPv6	[0:0:0:0:0:0]	1090	*	*					

Activate Windows
Go to Settings to activate Windc

5. Monitor Hard Disk

DiskMon is an application that logs and displays all hard disk activity on a Windows system. You can also minimize *DiskMon* to your system tray where it acts as a disk light, presenting a green icon when there is disk-read activity and a red icon when there is disk-write activity.

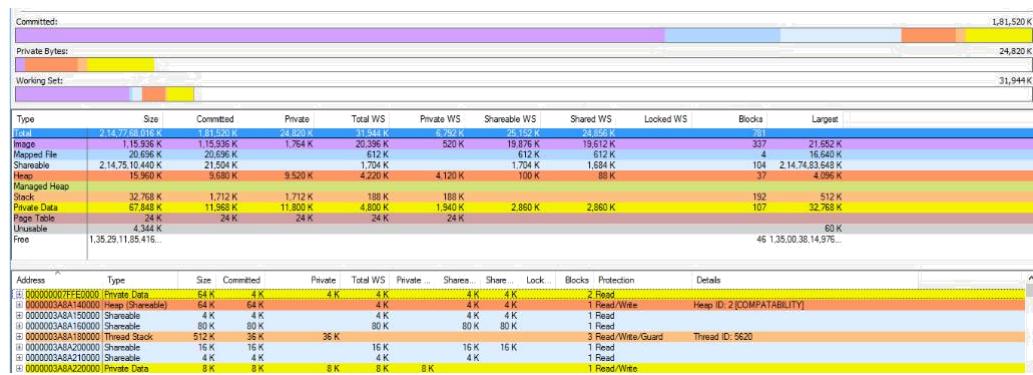
→ Download DiskMon Run as administrator

#	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

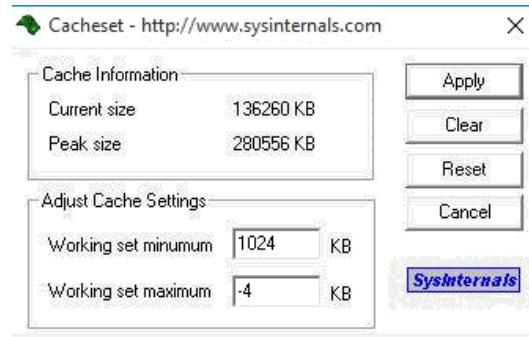
VMMMap is a process virtual and physical memory analysis utility. It shows a breakdown of a process's committed virtual memory types as well as the amount of physical memory (working set) assigned by the operating system to those types. Besides graphical representations of memory usage, VMMMap also shows summary information and a detailed process memory map. Powerful filtering and refresh capabilities allow you to identify the sources of process memory usage and the memory cost of application features

→
sysinternals → VMMMap



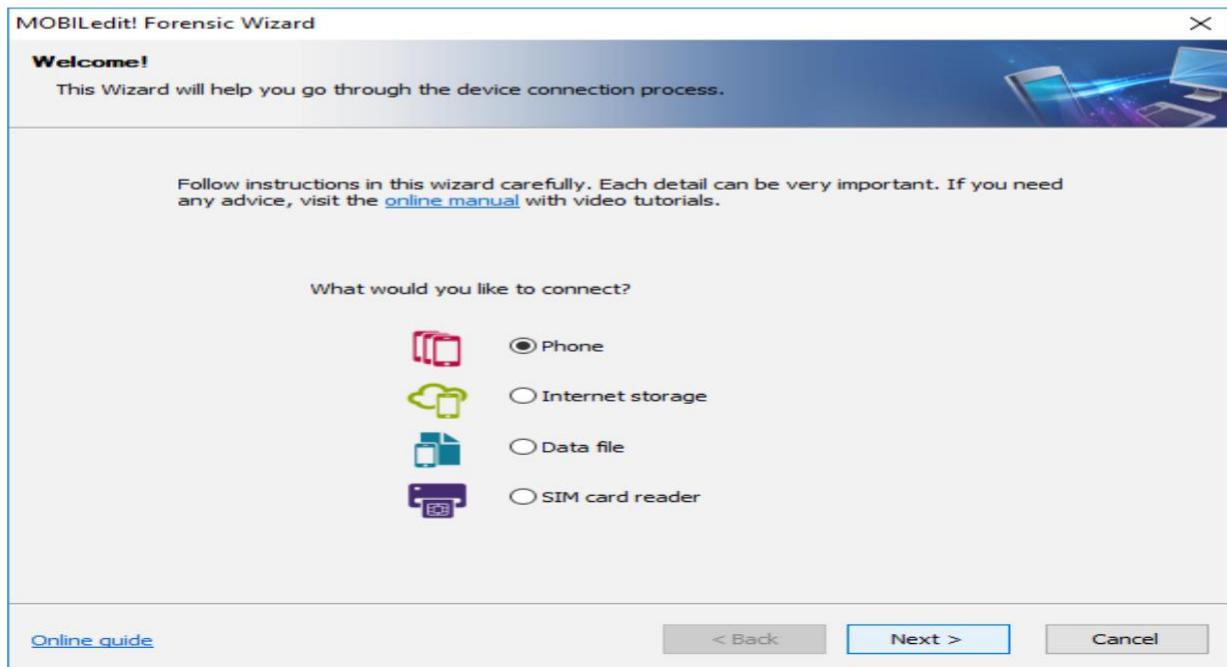
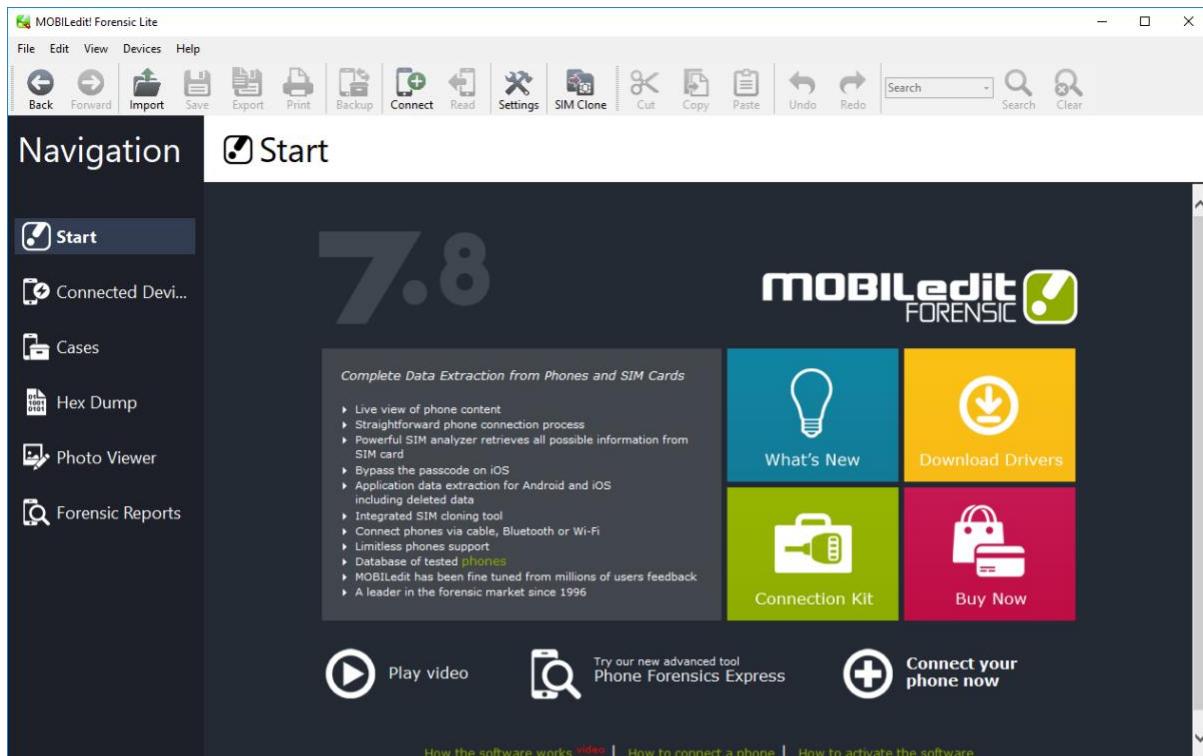
7.Monitor Cache Memory

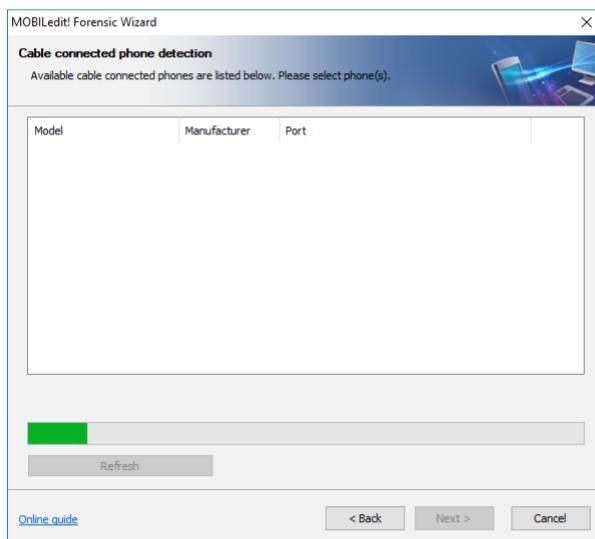
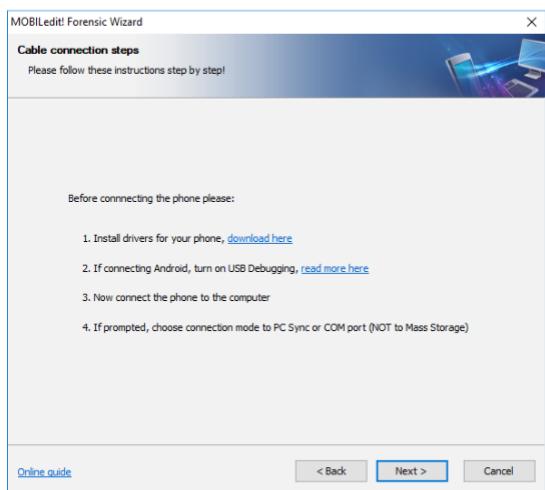
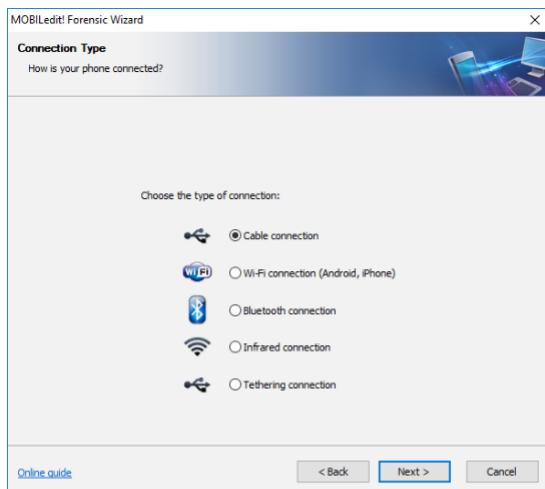
CacheSet is an applet that allows you to manipulate the working-set parameters of the system file cache. Unlike CacheMan, *CacheSet* runs on all versions of NT and will work without modifications on new Service Pack releases. In addition to providing you the ability to control the minimum and maximum working set sizes, it also allows you to reset the Cache's working set, forcing it to grow as necessary from a minimal starting point. Also unlike CacheMan, changes made with *CacheSet* have an immediate effect on the size of the Cache.

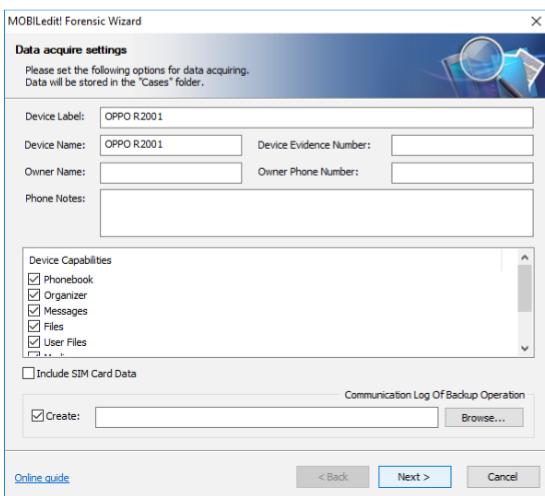
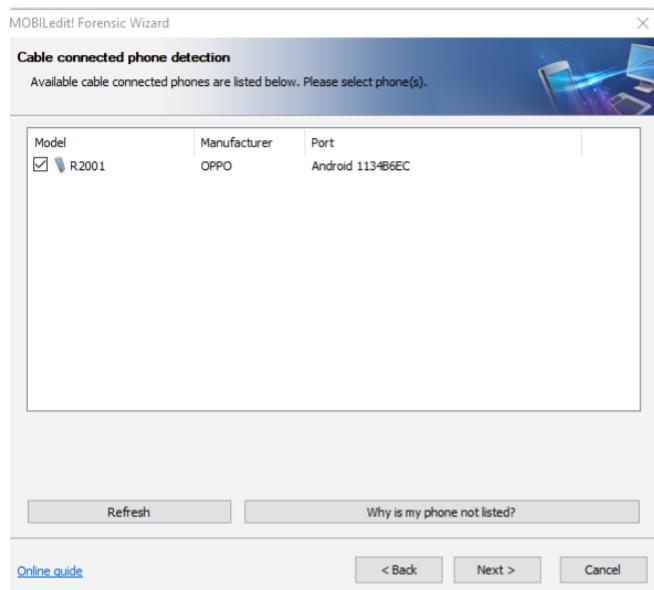
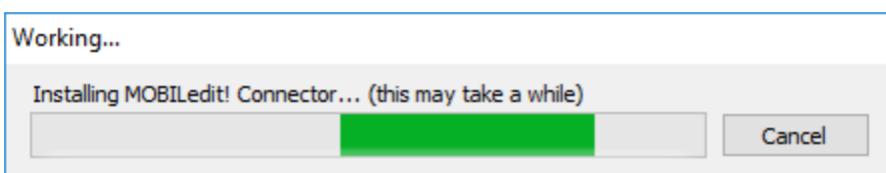
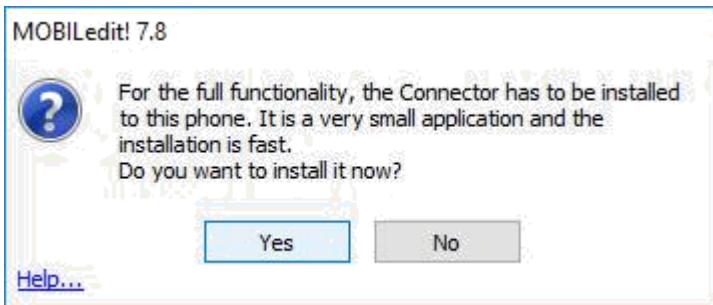


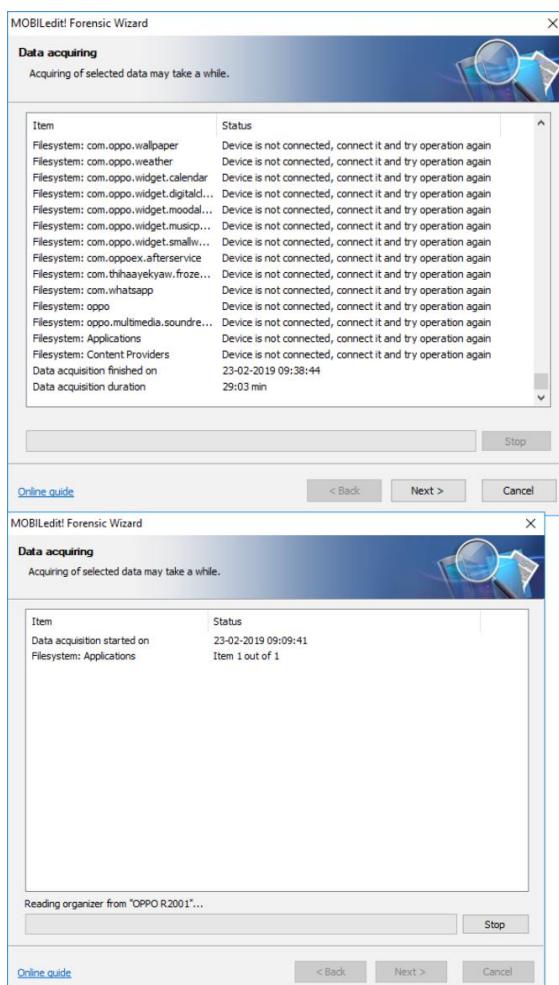
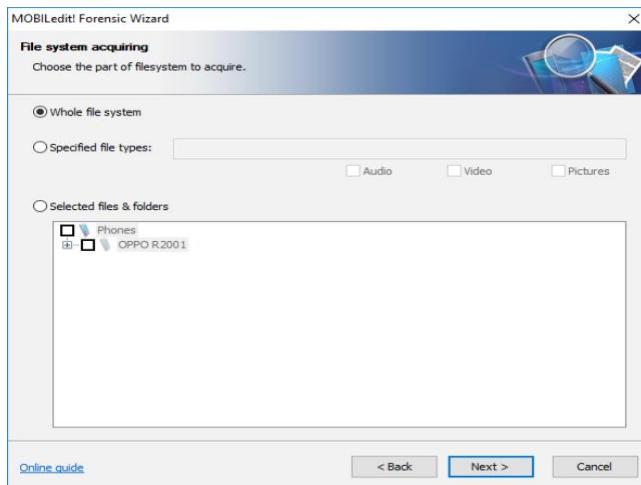
PRACTICAL 7

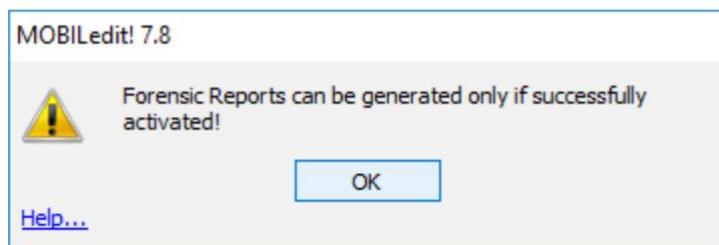
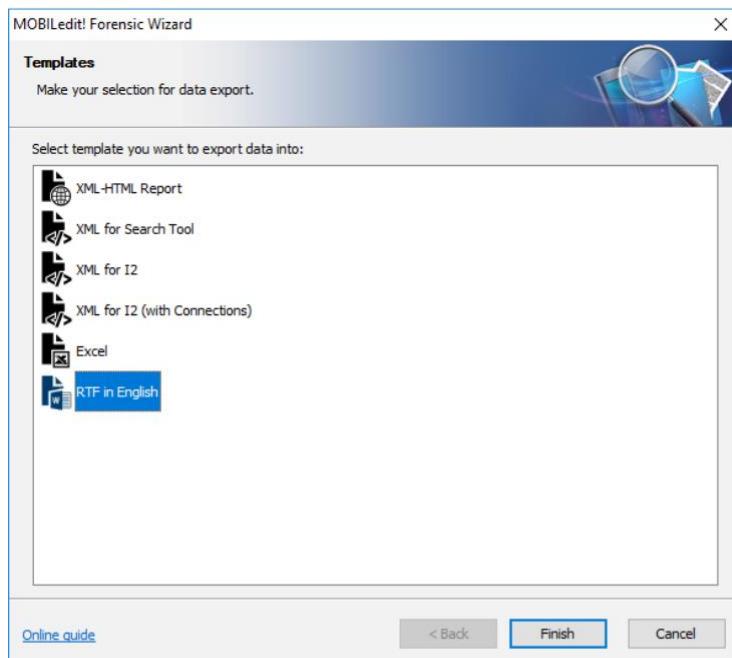
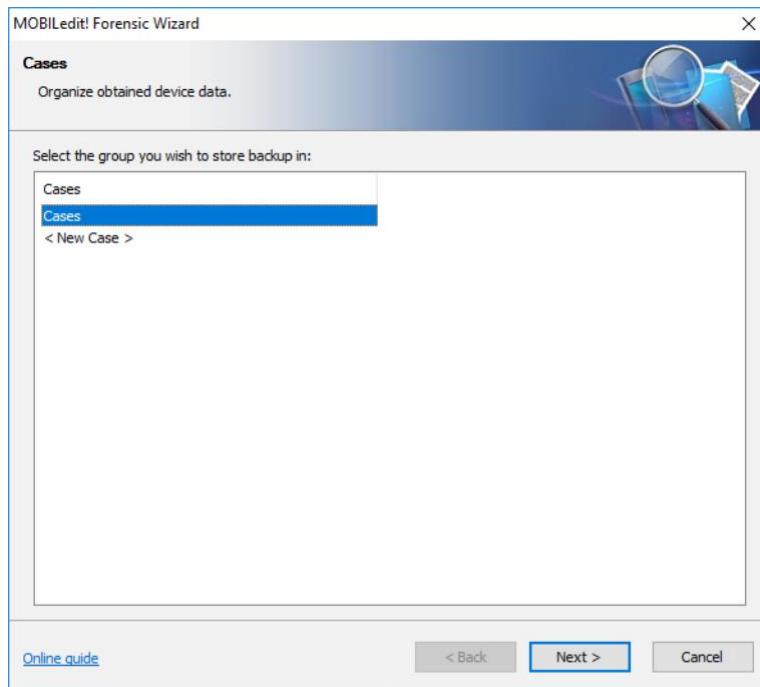
AIM: Investigate the Mobile Device.

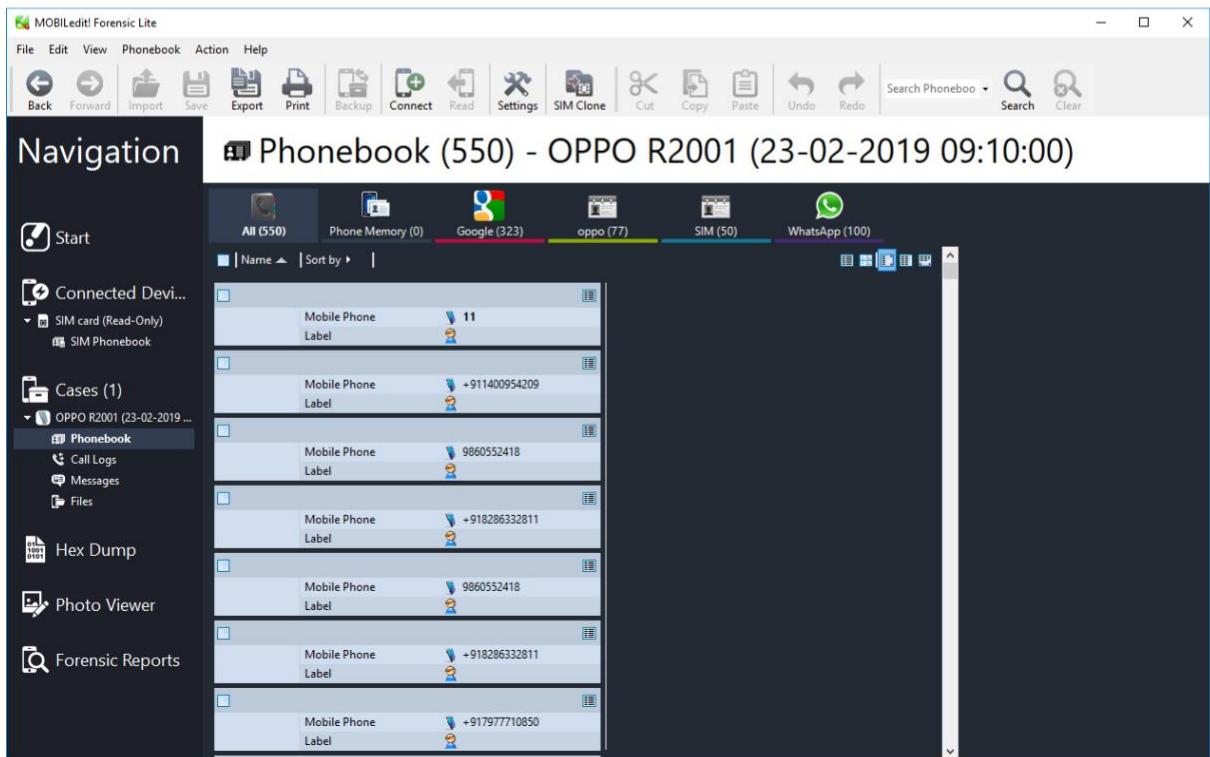
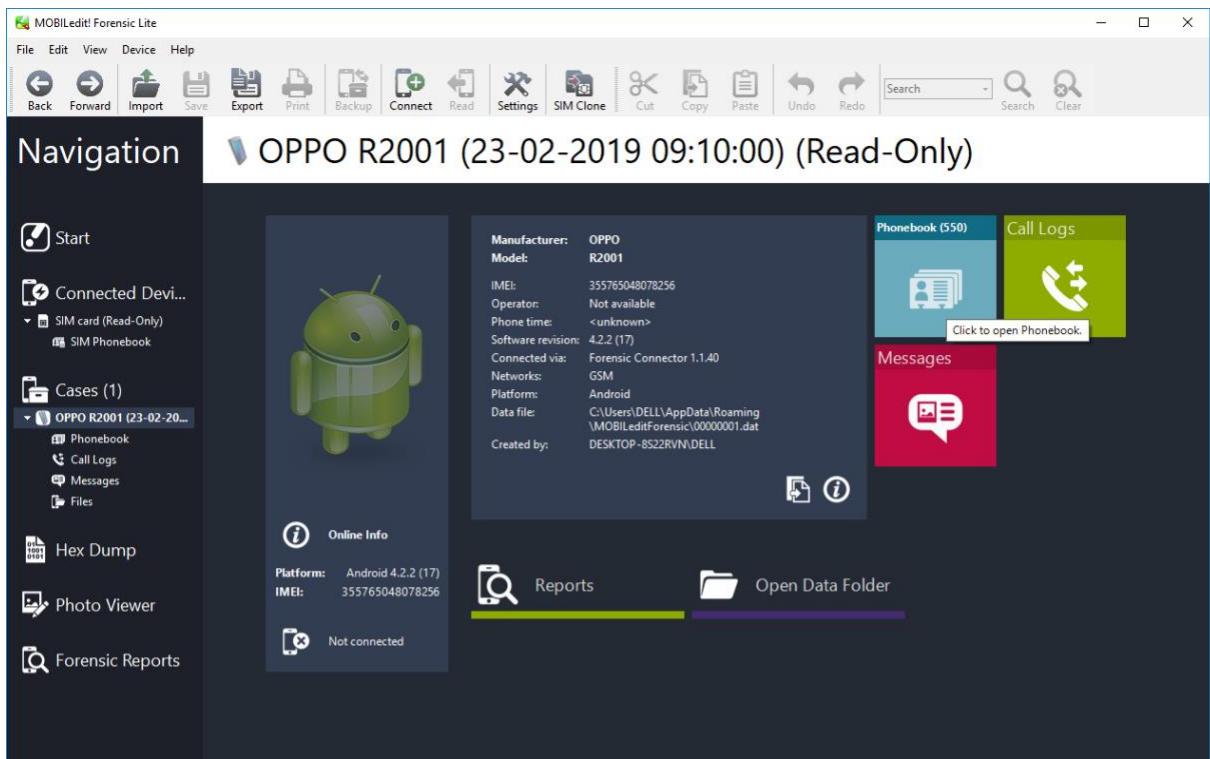












MOBILedit! Forensic Lite

File Edit View Phonebook Action Help

Back Forward Import Save Export Print Backup Connect Read Settings SIM Clone Cut Copy Paste Undo Redo Search Phoneboo Search Clear

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

Start Connected Devi... Cases (1) OPPO R2001 (23-02-2019 ...) Phonebook Call Logs Messages Files Hex Dump Photo Viewer Forensic Reports

Missed (97) Outgoing Incoming

Name	Number	Date
	+911400954501	22-02-2019 20:10:12
	+911400954448	22-02-2019 16:23:14
	+911400954496	22-02-2019 14:37:00
	+911400954490	21-02-2019 15:44:20
Sainat	+919930547554	20-02-2019 11:38:44
Sainat	+919930547554	20-02-2019 11:29:22
Sainat	+919930547554	20-02-2019 10:16:51
	+911400954496	19-02-2019 16:30:13
	+912239502000	19-02-2019 10:04:24
	+917977438886	18-02-2019 21:26:18
	+917977438886	18-02-2019 21:19:07
Papaa	+919004480339	18-02-2019 20:25:20
Santosh Bhai	+919702346277	18-02-2019 20:17:29
	+911400954437	18-02-2019 19:43:53
Aanad IY	+918779088436	17-02-2019 21:44:42
Aanad IY	+918779088436	17-02-2019 21:29:40

MOBILedit! Forensic Lite

File Edit View Messages Action Help

Back Forward Import Save Export Print Backup Connect Read Settings SIM Clone Cut Copy Paste Undo Redo Search Messages Search Clear

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

Start Connected Devi... Cases (1) OPPO R2001 (23-02-2019 ...) Phonebook Call Logs Messages Files Hex Dump Photo Viewer Forensic Reports

Conversations (7) All (504) Received (500) Sent (3) Drafts (1)

Time	Sender / Recipient
23-02-2019 08:25:27	55256
Don't Wait!! Start playing now to Win GOLD voucher worth Rs 25000. CALL 55256 Tollfree. TnC	
22-02-2019 14:03:05	55256
ओर कॉल करो Re 35 और 65 का राइवर्स्ट्रज जीतो। डायल 55256 मुफ्त	
22-02-2019 08:27:34	55256
Chance!! Win Rs 65 & Rs 35 worth FREE Recharge Everyday. Dial *77# (Tollfree) TnC	
21-02-2019 14:03:26	55256
Rs 5000 का नवक कॉर्ट जीतो। और आनंद लें। डायल 55256 मुफ्त	
21-02-2019 08:19:34	55256
Limited Chance!! Call 55256 Tollfree and Win Rs 65 worth Recharge Everyday. TnC	
20-02-2019 12:31:37	55256
संघर्ष ऑफर ! ₹ 35 रोज़े, ₹ 35 जीतो हर रोज़, कहाँले 55256 दोलफुरो	
26-01-2019 09:09:37	55256
Special OFFER! Aaj khelo aur jeet sakte ho Rs.1000 CashWho is Known as MAHATMATA) GandhijiB) NehruReply now A or B to 55256TnC & Aaj Jeeto	

PRACTICAL 8

AIM: Investigate Email File Given.

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

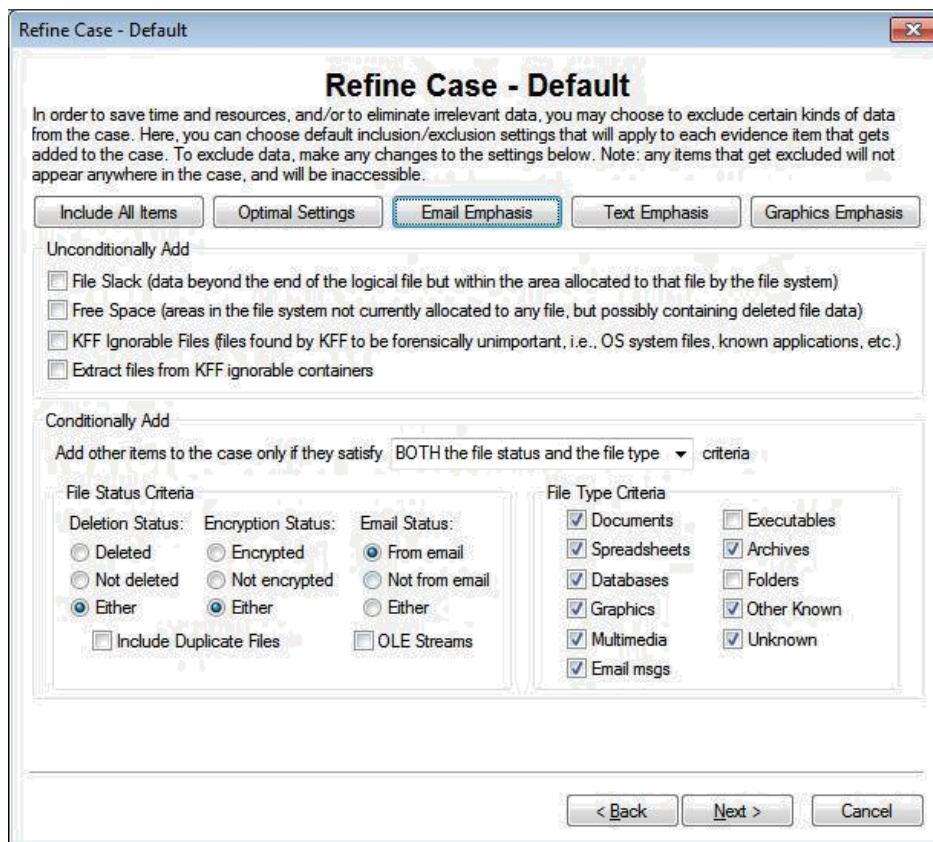
Because of Jim's responses to a poor performance review, the CEO of Superior Bicycles, Martha Dax, suspects he might have obtained sensitive information about the company's business model that he's leaking to a competitor.

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

To process this investigation, we need to examine the Jim_shu.pst file, locate the message, and export it for further analysis of its header to see how Jim might have received it.

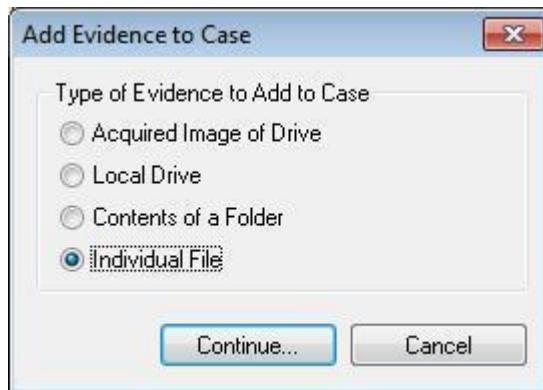
Recovering Email

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

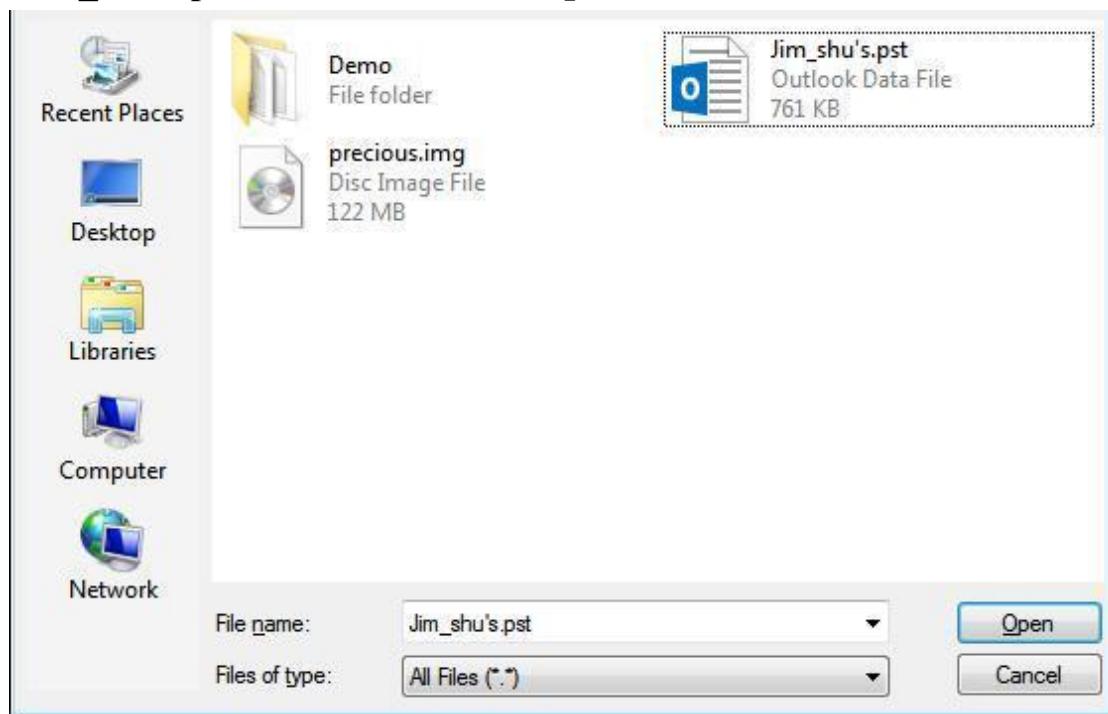


Click **Next** until you reach the **Add Evidence to Case** dialog box, and then click the **Add Evidence** button.

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



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



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

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

For email recovery follow following steps:

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

Select any message say Message0001 right click and select option Launch Detached Viewer and you can see detail of deleted message.

The screenshot shows the AccessData FTK 1.81.0 interface. The left pane displays a tree view of email folders, including 'PRAC07 Jim_shu's.pst' and its sub-folders like 'Deleted Items'. The right pane shows a list of messages with columns for File Name, Full Path, Recycle Bin, Ext, File Type, Category, Subject, Cr Date, and Mod Date. A message titled 'Message0001' is selected. Below the list is a preview pane for 'Message0001' showing the message header and body. The message header includes:

Subject: RE: Bike spec's
From: Jim Shu
Date: 12/3/2006 10:07:00 PM
To: 5ampsade@myway.com'

The message body contains:

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:5ampsade@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?

For analyzing header follow following steps:

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

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

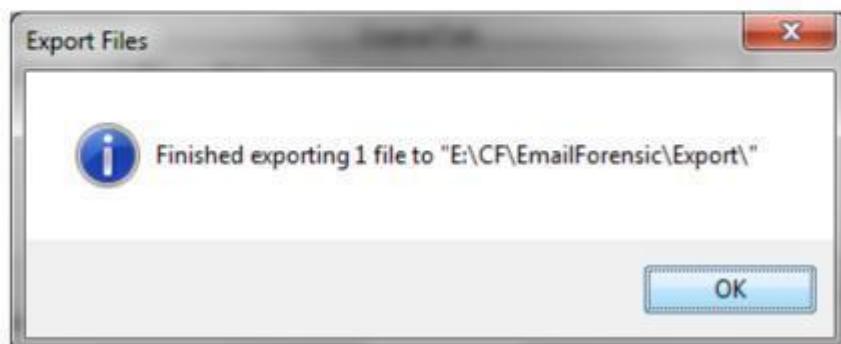
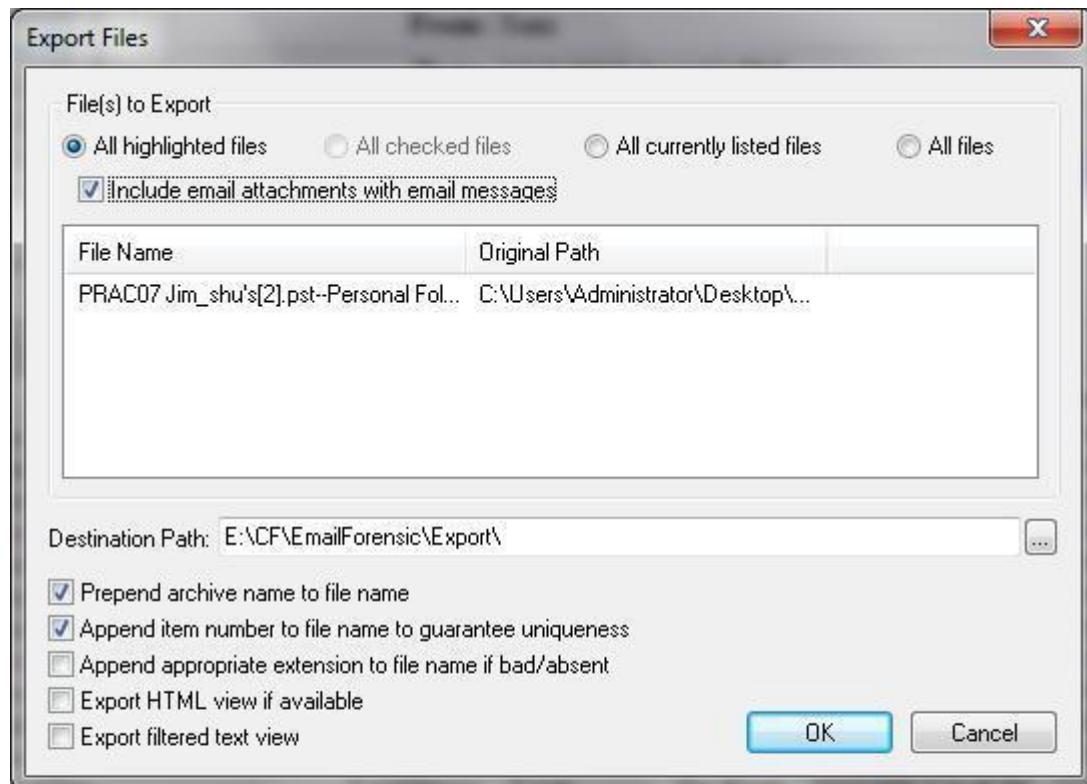
The screenshot shows the AccessData FTK 1.81.0 interface. The left pane displays a tree view of email folders, including 'PRAC07 Jim_shu's.pst' and its sub-folders like 'Deleted Items'. The right pane shows a list of messages with columns for File Name, Full Path, Recycle Bin, Ext, File Type, Category, Subject, Cr Date, and Mod Date. A message titled 'Message0003' is selected. Below the list is a preview pane for 'Message0003' showing the message header and body. The message header includes:

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

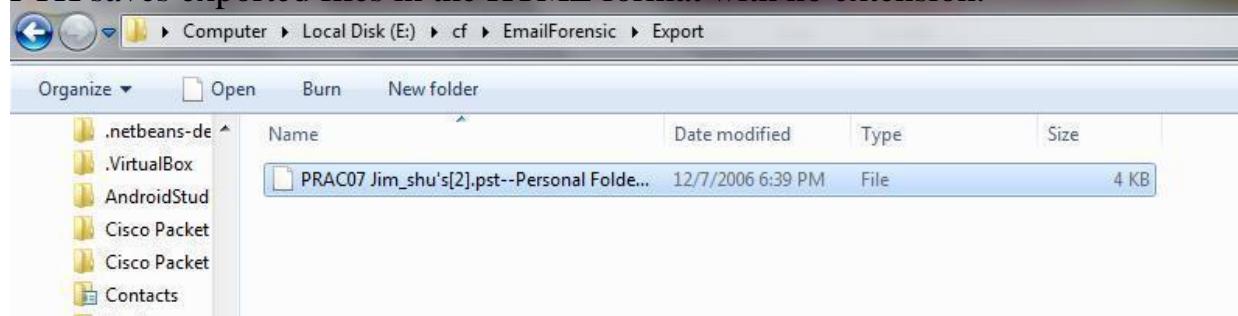
The message body contains:

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

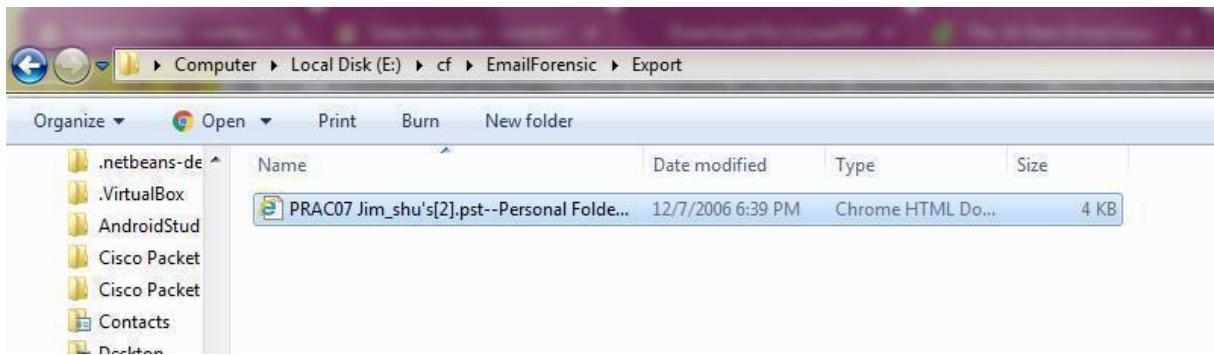
Right-click on any message say Message0003 in the File List pane and click Export File. In the Export Files dialog box, click OK.



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



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



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



Conversation Topic: Bike spec's Sender Name: Sam Received By: Jim Shu Delivery Time: 12/3/2006 9:14:02 PM Creation Time: 12/3/2006 9:16:48 PM Modification Time: 12/7/2006 6:39:12 PM Submit Time: 12/3/2006 9:14:14 PM Flags: 1 = Read Size: 6456 Received: from myway.com (mnl.excitennetwork.com[207.159.120.55](untrusted sender)) by alnrmxc23.comcast.net (alnrmxc23) with ESMTP id <20061204021402.2300190f3e>; Mon, 4 Dec 2006 02:14:02 +0000 X-Originating-IP: [207.159.120.55] Received: by mprrdmxin.myway.com (Postfix, from userid 110) id 63B6067669; Sun, 3 Dec 2006 21:14:14 -0500 (EST) To: Jim_shu@comcast.net Subject: RE: Bike spec's Received: from [24.18.24.250] by mprrdmmailfe3.nwk.myway.com via HTTP; Sun, 3 Dec 2006 21:14:14 EST X-AntiAbuse: This header was added to track abuse, please include it with any abuse report X-AntiAbuse: ID = f869dfbea97fe07b9eab2f865d19b540 Reply-to: 5amspade@myway.com From: "Sam" <5amspade@myway.com> MIME-Version: 1.0 X-Sender: 5amspade@myway.com X-Mailer: PHP Content-Type: text/plain; charset="US-ASCII" Content-Transfer-Encoding: 7bit Message-Id: <20061204021414.63B6067669@mprrdmxin.myway.com> Date: Sun, 3 Dec 2006 21:14:14 -0500 (EST) We might be able to go \$4000 if it is good. Is it? Sam --- On Sun 12/03, Jim Shu <Jim_shu@comcast.net> wrote: From: Jim Shu [mailto: Jim_shu@comcast.net] To: 5amspade@myway.com Date: Sun, 3 Dec 2006 18:09:06 -0800 Subject: RE: Bike spec's How much are you willing to pay me to get these plans to you? Jim---Original Message---From: Sam [mailto: 5amspade@myway.com] Sent: Sunday, December 03, 2006 5:40 PM To: jim_shu@comcast.net Subject: Bike spec's Do you have them yet? I've got people in Asia ready to duplicate them? Sam _____ No banners. No pop-ups. No kidding. Make My Way your home on the Web - http://www.myway.com _____ No banners. No pop-ups. No kidding. Make My Way your home on the Web - http://www.myway.com'

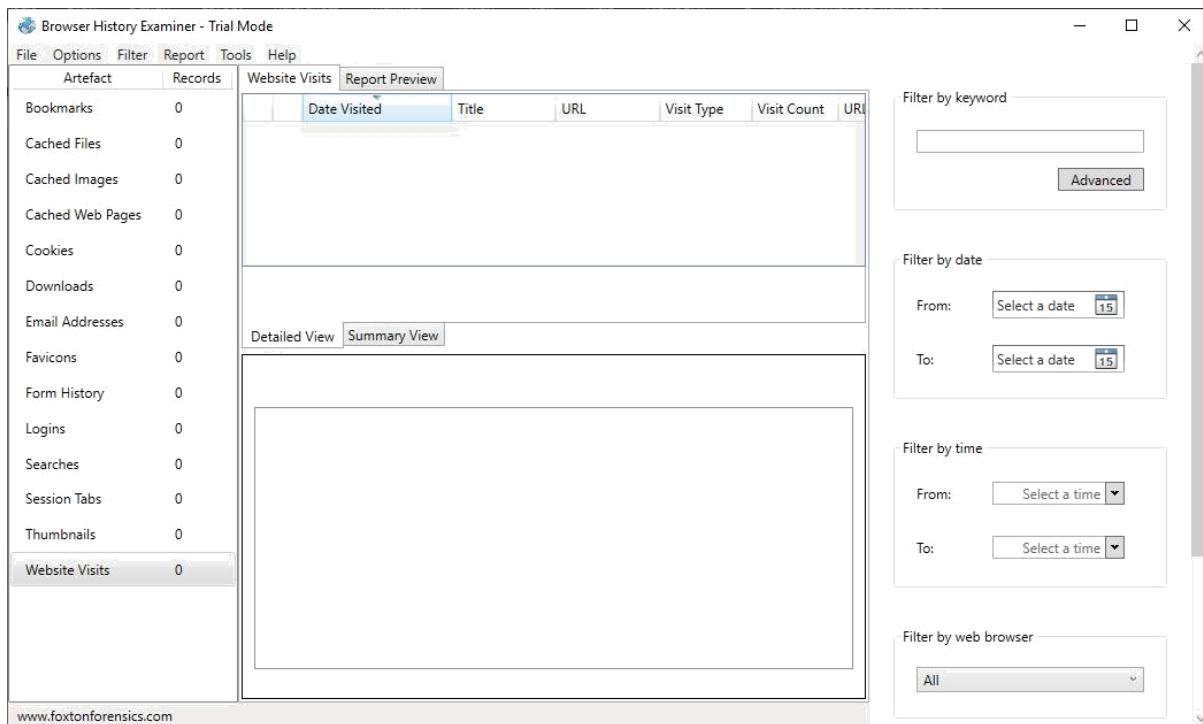
PRACTICAL 9

Aim: Web Browser Forensics .

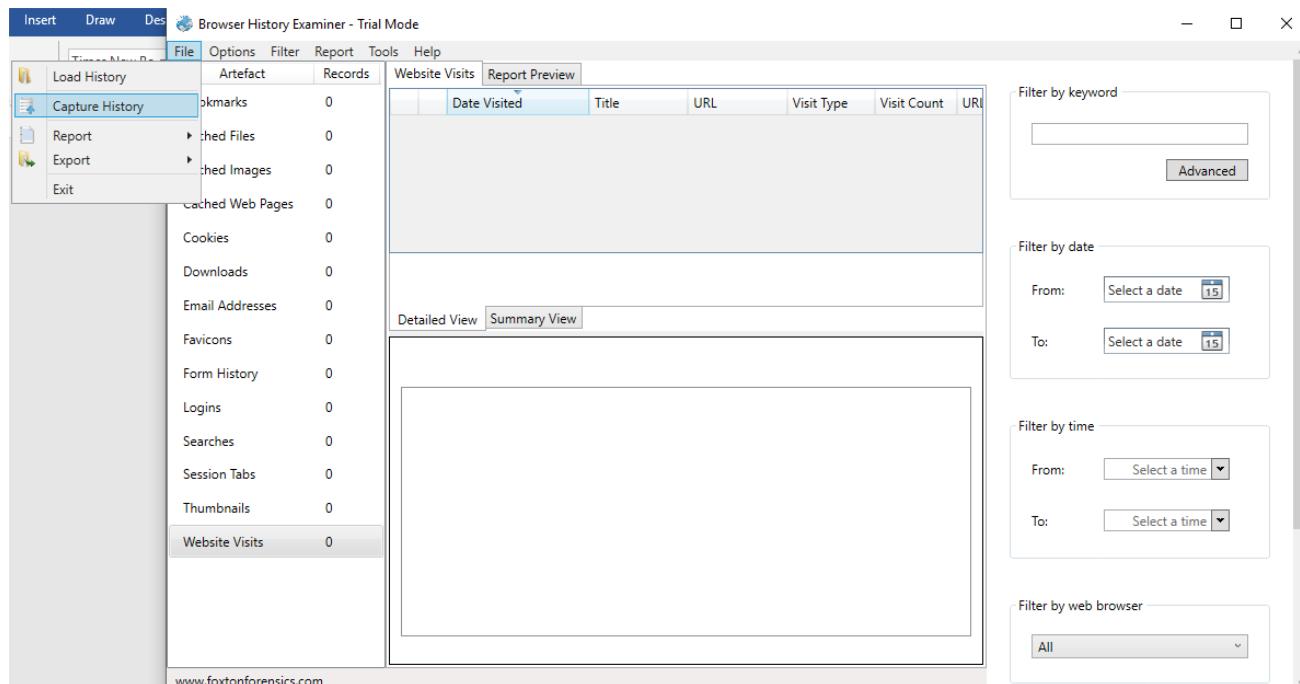
- Web Browser working
- Forensics activities on browser
- Cache / Cookies analysis
- Last Internet activity

Steps:

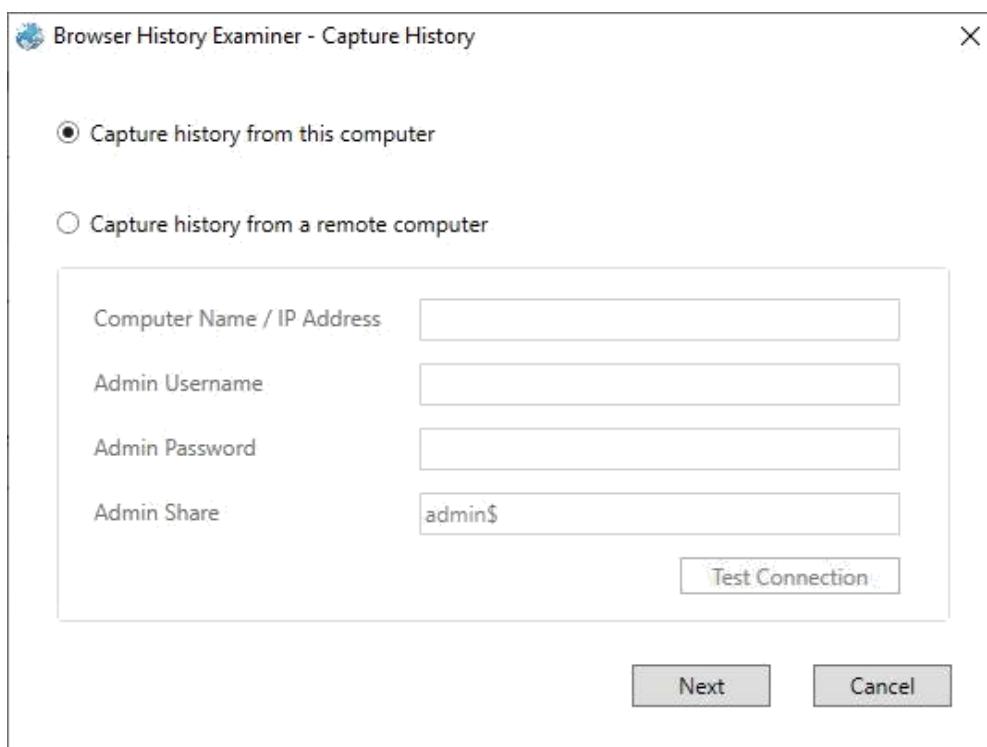
1. Open BrowserHistoryExaminer.



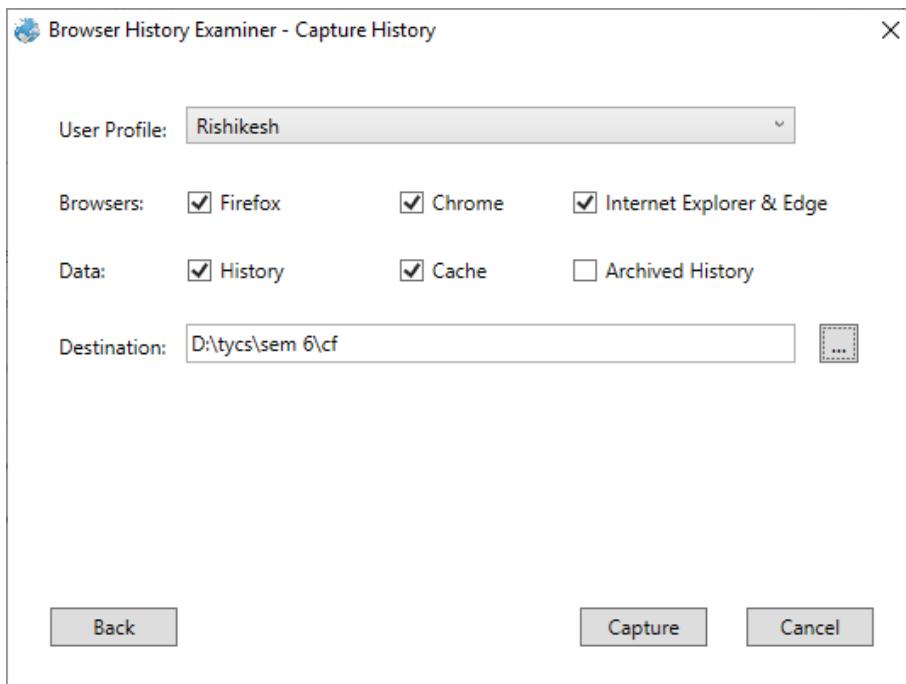
2. Click on file > Capture History



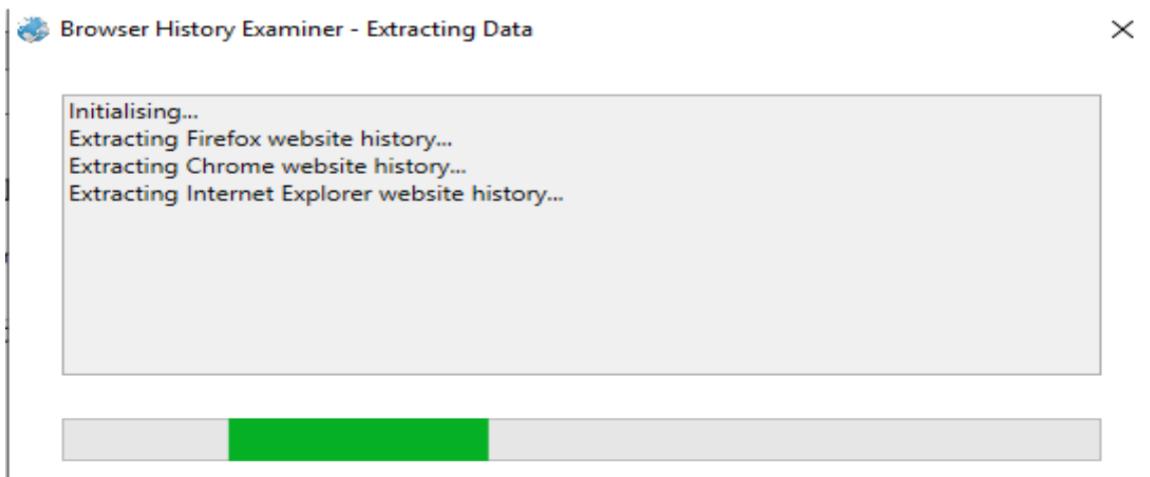
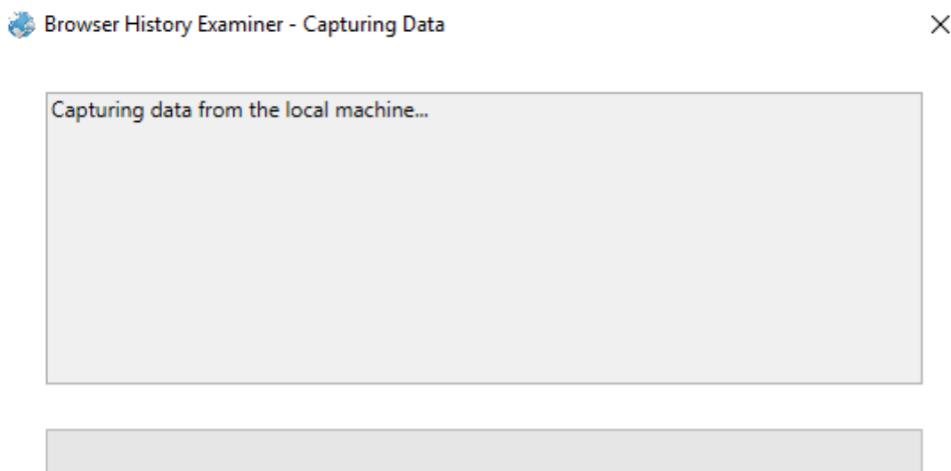
3. Select the capture folder and click on next.



4. Enter the destination to capture the data.



5. The History is been extracting.



6. The data has been retrieved.

Screenshot of Browser History Examiner - Trial Mode showing the 'Website Visits' report preview. The left panel lists artifacts with counts: Bookmarks (8), Cached Files (4615), Cached Images (177), Cached Web Pages (36), Cookies (1566), Downloads (80), Email Addresses (30), Favicons (1790), Form History (31), Logins (3), Searches (1184), Session Tabs (62), Thumbnails (12), and Website Visits (2688). The main area displays a table of website visits from March 17, 2019, to March 18, 2019, with columns for Date Visited, Title, URL, Visit Type, and Visit Count. A summary chart titled 'Website Visit Count - 17-03-2019 to 18-03-2019' shows visit counts for each hour. Filter options for keyword, date, time, and web browser are available on the right.

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

7. On the left panel click on bookmarks.

Screenshot of Browser History Examiner - Trial Mode showing the 'Bookmarks' report preview. The left panel lists artifacts with counts, including Bookmarks (8), which is highlighted. The main area displays a table of bookmarks with columns for Date Added, Last Modified, Title, URL, and Web Browser. A summary chart titled 'Website Visit Count - 17-03-2019 to 18-03-2019' is also present. Filter options for keyword, date, time, and web browser are available on the right.

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

8. On the left panel click on cached files.

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

Viewing 25/25 records < > 1 of 1 pages Page size 50

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

9. On the left panel click on cached images.

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

Viewing 25/25 records < > 1 of 1 pages Page size 50

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

10. On the left panel click on cookies.

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

Viewing 25/25 records < > 1 of 1 pages Page size 50

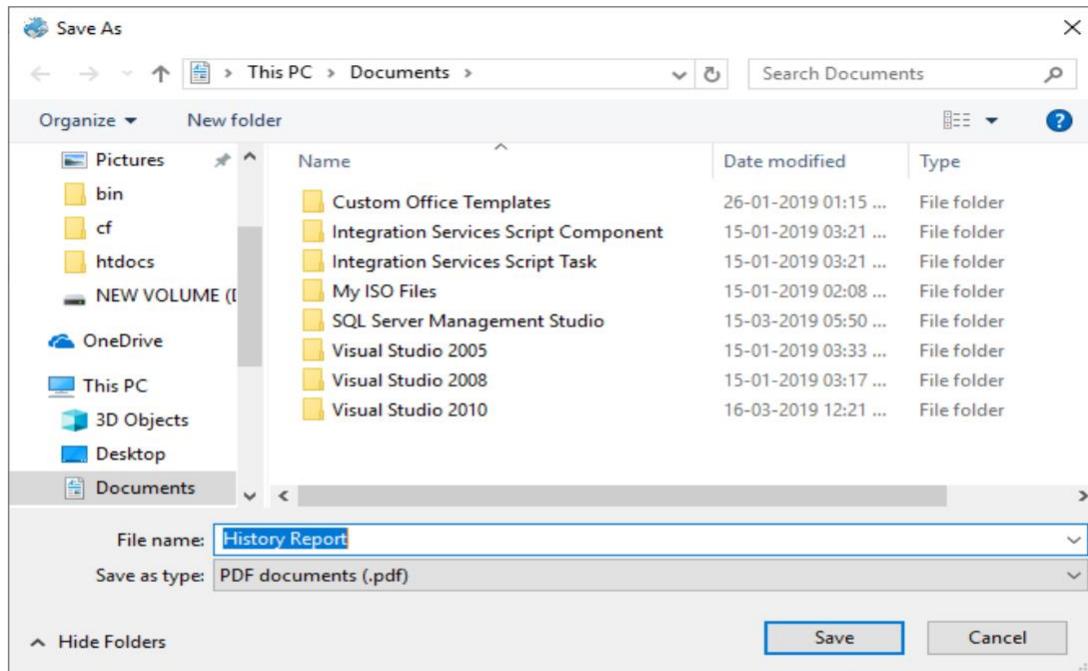
Time zone: UTC, DST Enabled Date format: dd/mm/yyyy

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

Artefact	Records	Cookies	Report Preview
Load History	8		
Capture History			
Report			
Save as PDF			
Save as HTML			
Export			
Exit			
Cached Web Pages	36		
Cookies	1566		
Downloads	80		
Email Addresses	30		
Favicons	1790		
Form History	31		
Logins	3		
Searches	1184		
Session Tabs	62		
Thumbnails	12		
Website Visits	2688		

Viewing 25/25 records < > 1 of 1 pages Page size 50

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



Web Browser History Report

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

Bookmarks

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

Cached Files

Last Fetched	Content Type	URL	Fetch Count	File Size (Bytes)	Web Browser
		https://mail-attachment.googleusercontent.com/attachment/u/0/?ui=2&ik=5c151dfa368attid=0.18a...		18820976	Chrome
	application/zip	https://r4---sn-4pb8xoxu-cvhe.gvt1.com/edgedj/widevine-cdm4.10.1146.0-win-x64.zip?cm_redirect=yes&a...	1	3523651	Firefox
		https://r3---sn-4pb8xoxu-cvhe.googlevideo.com/videoplayback?ei=uYlXNeQA4ei1Ab4h7K4Cg&dur=152.733...		2097152	Chrome
		https://r3---sn-4pb8xoxu-cvhe.googlevideo.com/videoplayback?ei=uYlXNeQA4ei1Ab4h7K4Cg&dur=152.733...		2097152	Chrome
		https://r3---sn-4pb8xoxu-cvhe.googlevideo.com/videoplayback?ei=uYlXNeQA4ei1Ab4h7K4Cg&dur=152.733...		2097152	Chrome

Browser History Examiner - Trial Mode

File Options Filter Report Tools Help

Bookmarks

Date Added	Last Modified	Title
17-03-2019 09:03:01	17-03-2019 09:03:01	Getting Started
17-03-2019 09:03:01	17-03-2019 09:03:01	Help and Tutorials
17-03-2019 09:03:01	17-03-2019 09:03:01	Customize Firefox
17-03-2019 09:03:01	17-03-2019 09:03:01	Get Involved
17-03-2019 09:03:01	17-03-2019 09:03:01	About Us
17-03-2019 09:03:01	17-03-2019 09:03:01	New Tab
22-01-2019 06:40:50		Download Microsoft® SQL Server® 2012 Express from Official Microsoft Download Center
		Bing

Export

- Export to Excel
- Export to HTML**
- Export to CSV
- Export to XML
- Export to Concordance Load File

Downloads

Email Addresses	30
Favicons	1790
Form History	31
Logins	3
Searches	1184
Session Tabs	62
thumbnails	12
Website Visits	2688

Viewing 8/8 records | Page size: 50 | Filter | Undo | Clear

Web Browser History Report

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

Bookmarks

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

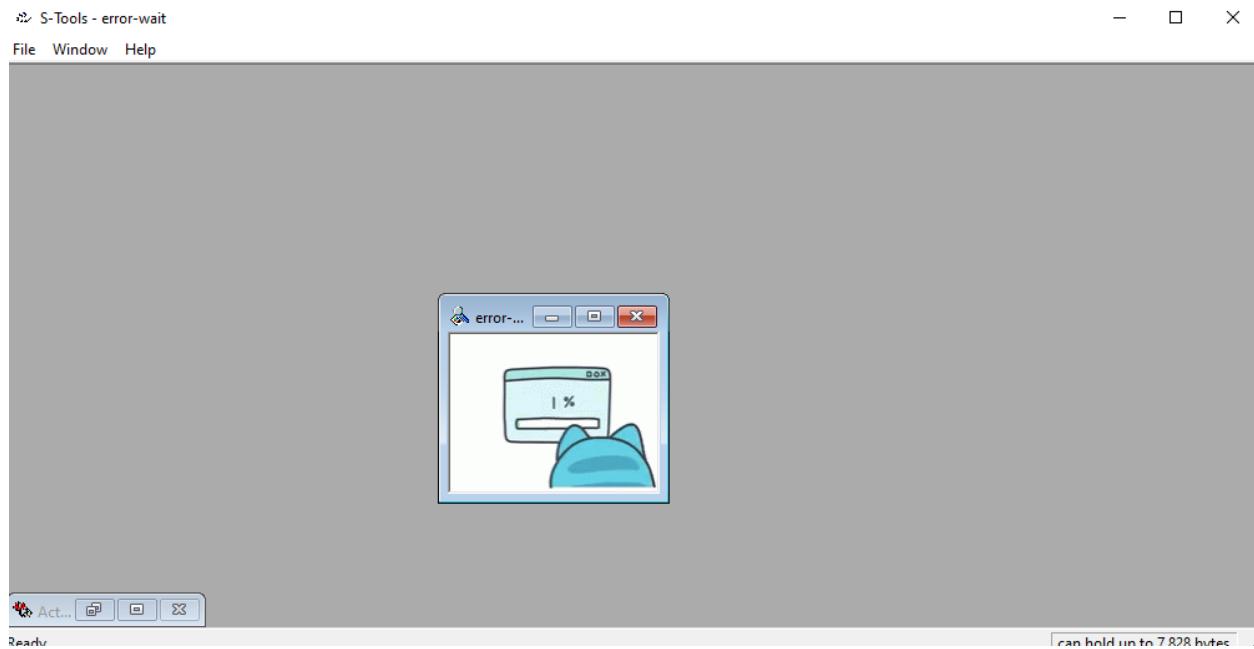
PRACTICAL 10

A.Using Steganography Tools [S-Tools]

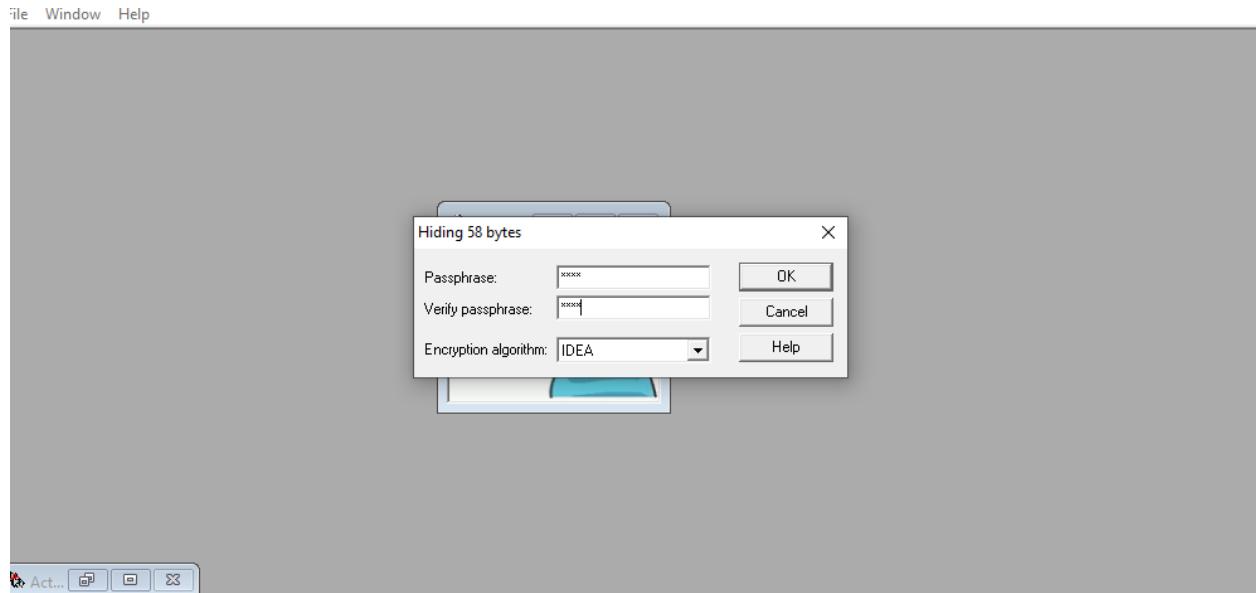
Step 1: The dark gray background area is used for dropping the image or sound files into.



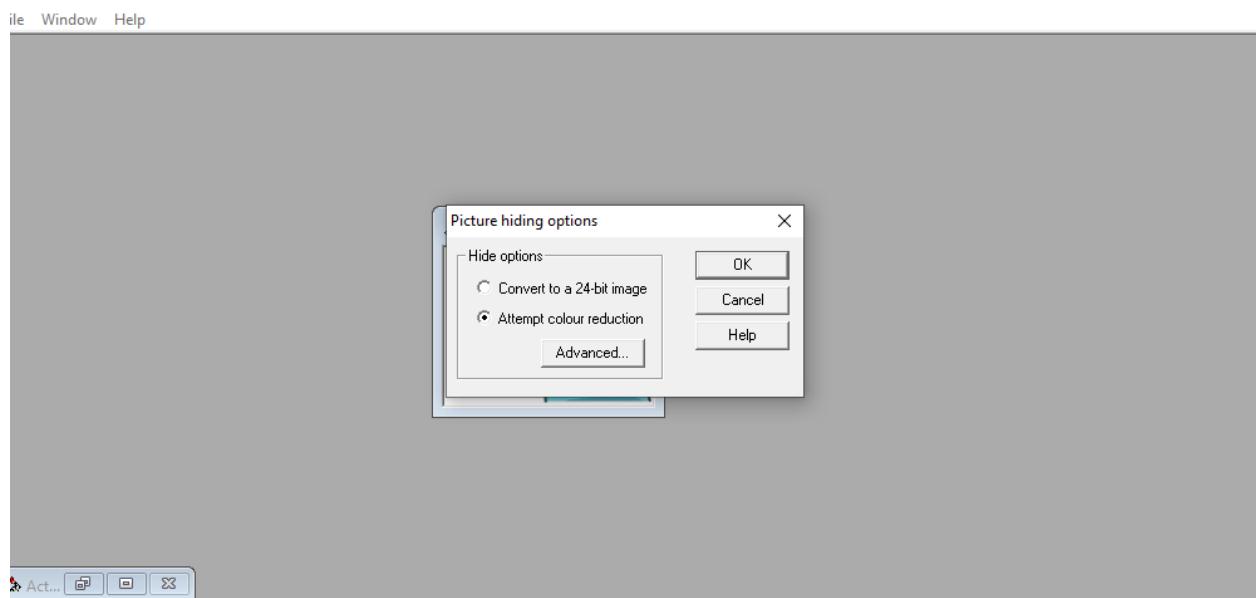
Step 2: After opening S-Tools (S-Tools.exe) and Windows Explorer, drag Cover File.gif into the main working area of S-Tools



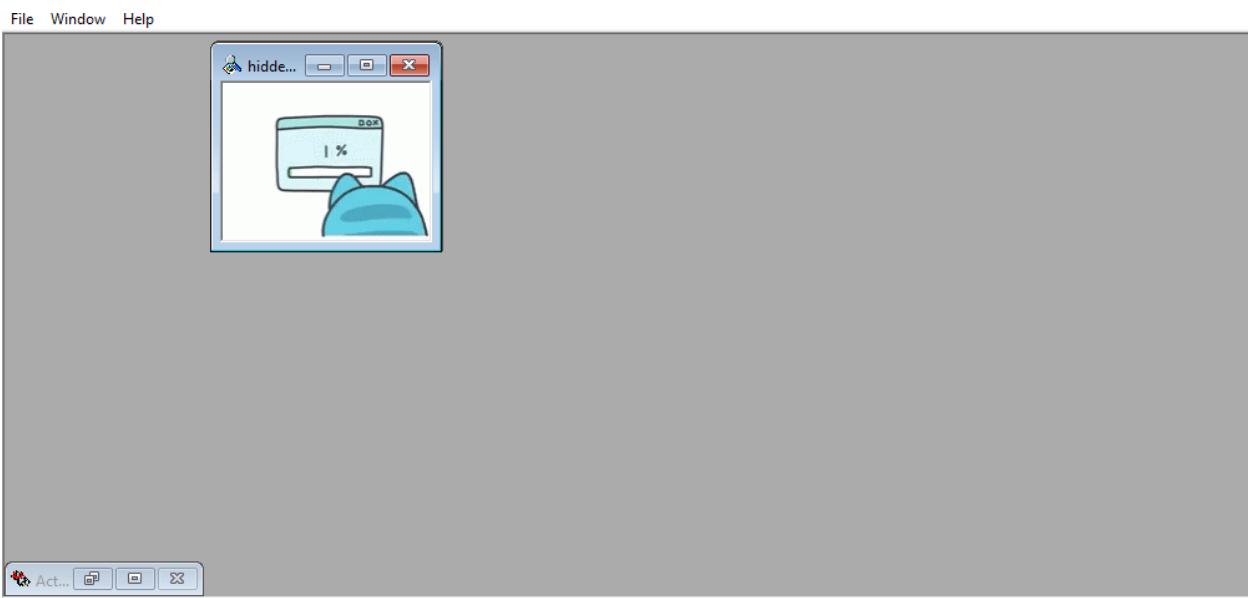
Step 3: The pass phrase is used in generating the pseudorandom number that is used to insert the bits into the cover file. S-Tools gives a choice between IDEA, DES, TripleDES, and MDC encryption algorithms



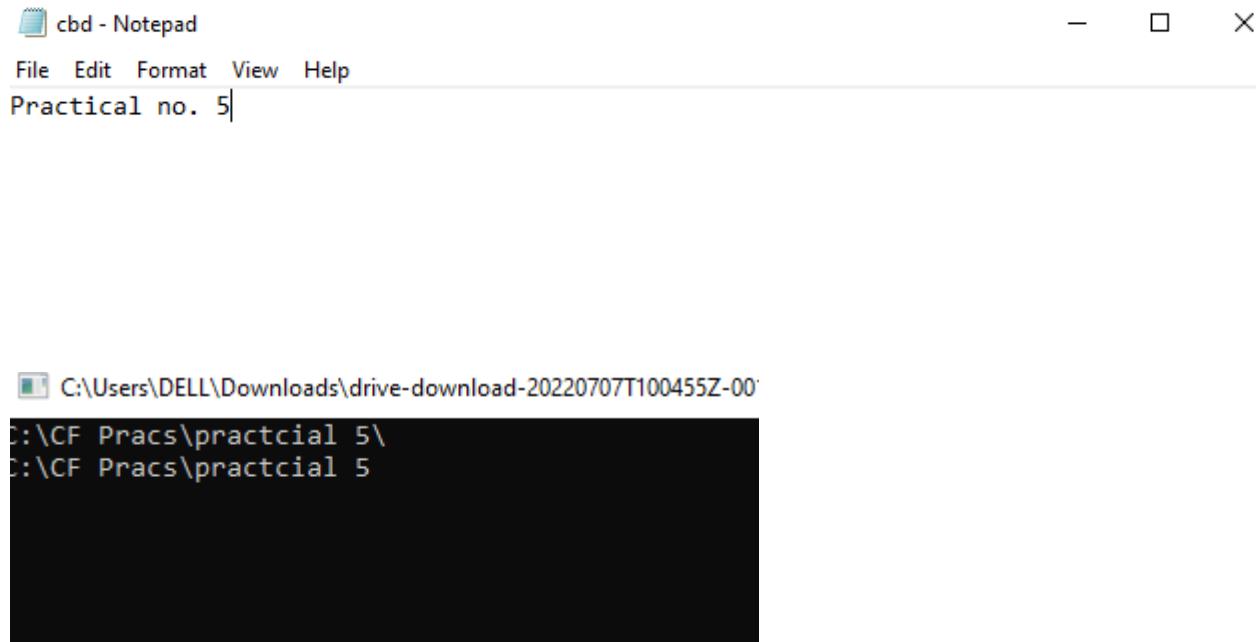
Step 4: To have S-Tools process the GIF file, a dialog box prompts for choices to be made



Step 5 : When S-Tools finishes inserting the data, the output image will display with the marker "hidden data" at the top

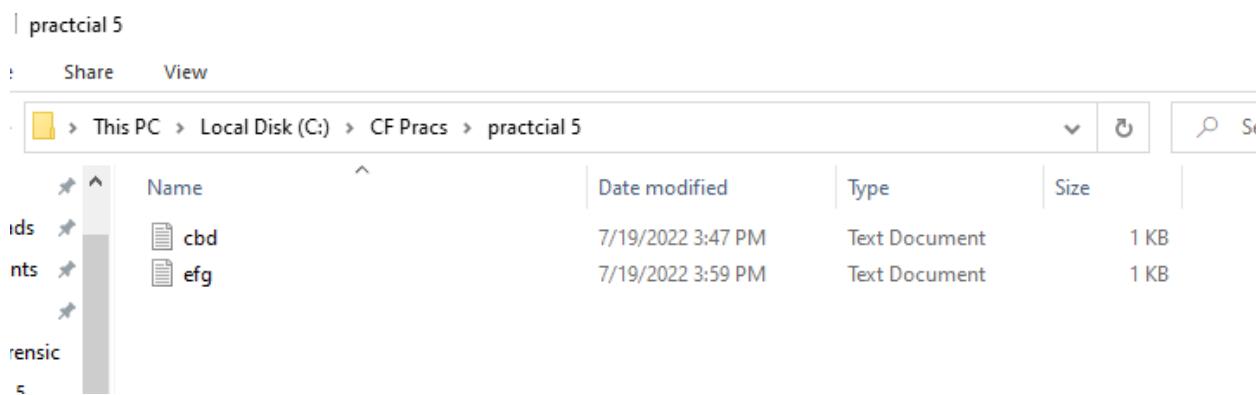


B. Using Whitespace Stegnography tool SNOW



```
snow -C -m "MessageToHide" -p "Password" "InputTextFile" "OutputTextFile"
```

```
C:\Users\DELL\Downloads\drive-download-20220707T100455Z-001\SNOW.EXE
C:\CF Pracs\practical 5>snow -C -m "Practical number 5 " -p "kaushal" cbd.txt efg.txt
Compressed by 35.67%
Message exceeded available space by approximately 788.54%
An extra 4 lines were added.
```



```
C:\Users\DELL\Downloads\drive-download-20220707T100455Z-001\SNOW.EXE
C:\CF Pracs\practical 5>snow -C -p "kaushal" efg.txt
Practical number 5
C:\CF Pracs\practical>
C:\CF Pracs\practical>
```