Practical No – 1

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

-Creating Forensic Image

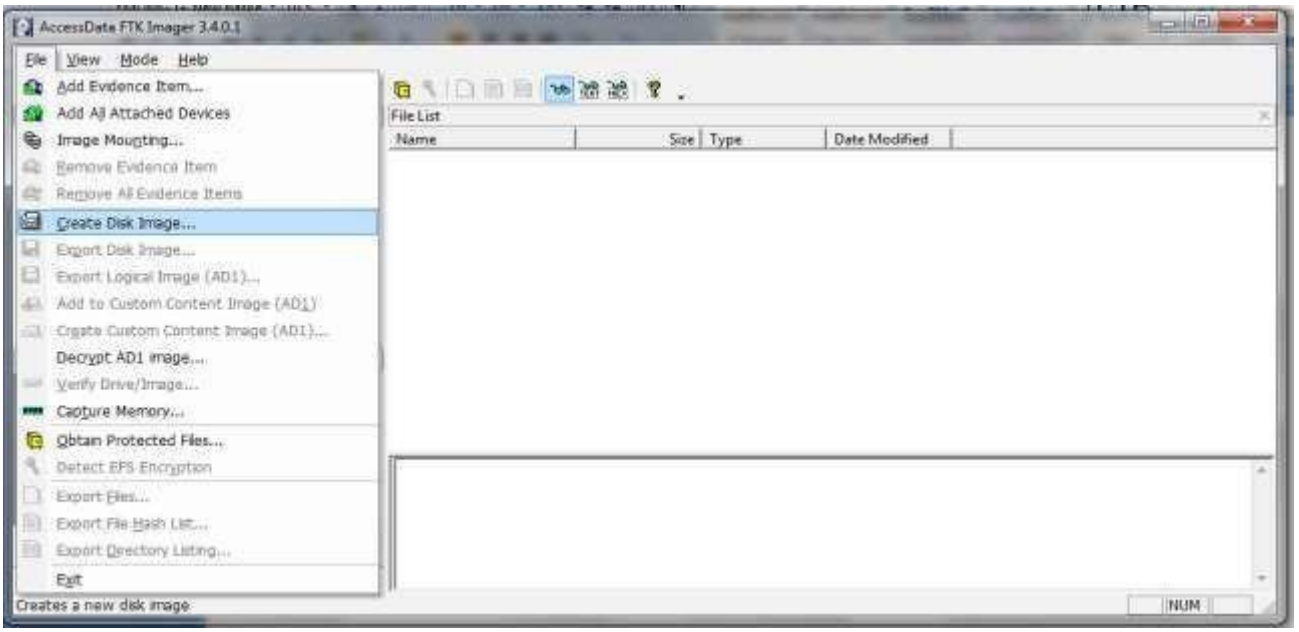
-Check Integrity of Data

-Analyze Forensic Image

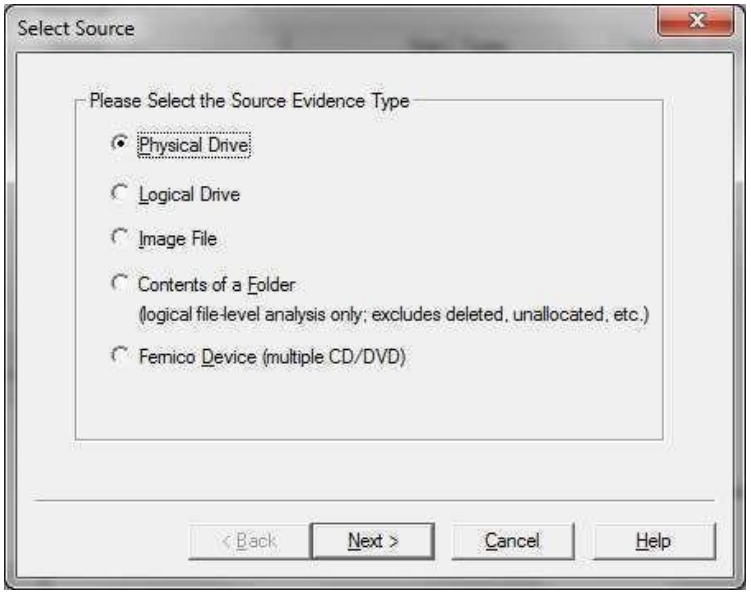
Steps:

Creating Forensic Image

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

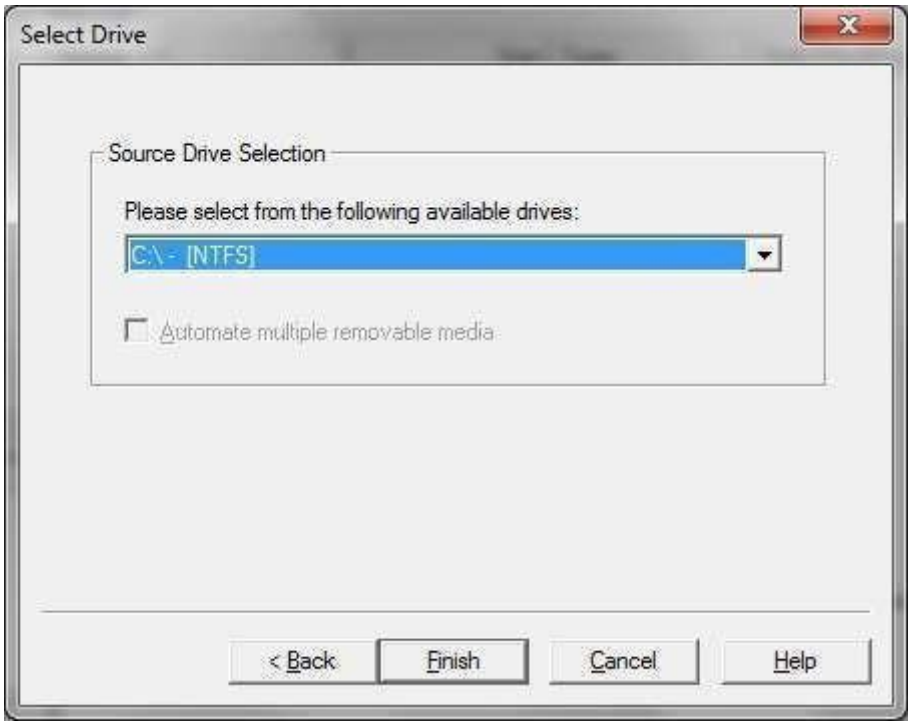


2. Select the source you want to make an image of and click Next.

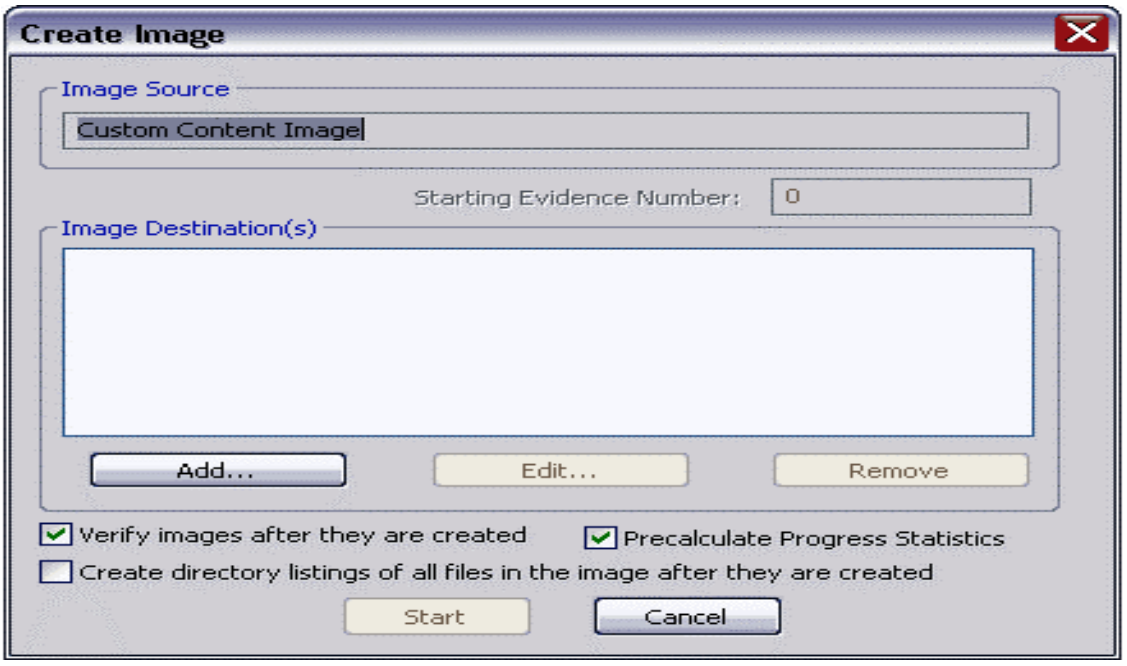


If you select Logical Drive to select a floppy or CD as a source, you can check the Automate multiple removable media box to create groups of images. Imager will automatically increment the case numbers with each image, and if something interrupts the process, you may assign case number manually.

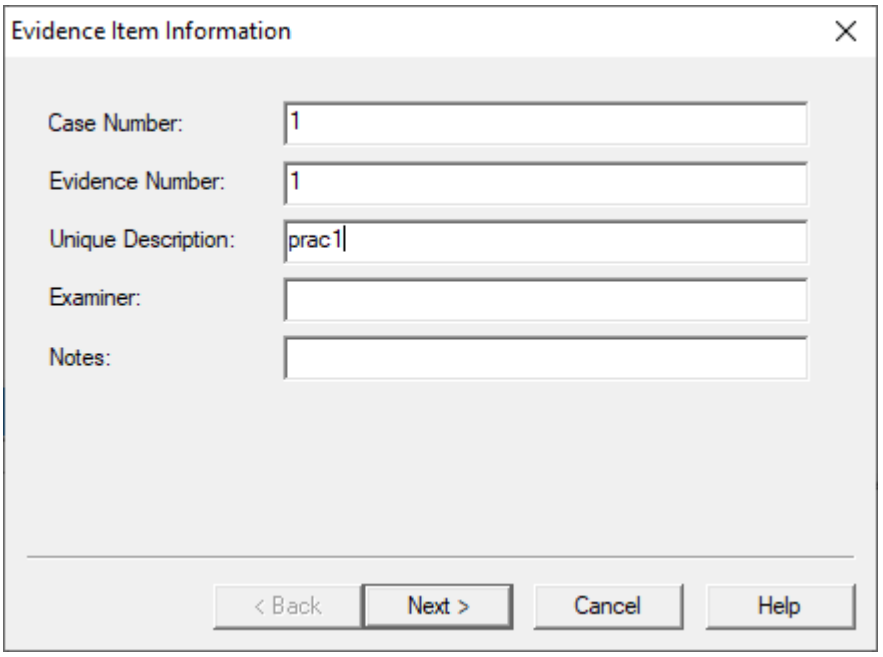
3. Select the drive or browse to the source of the image you want, and then click Finish.



4. In the Create Image dialog, click Add.

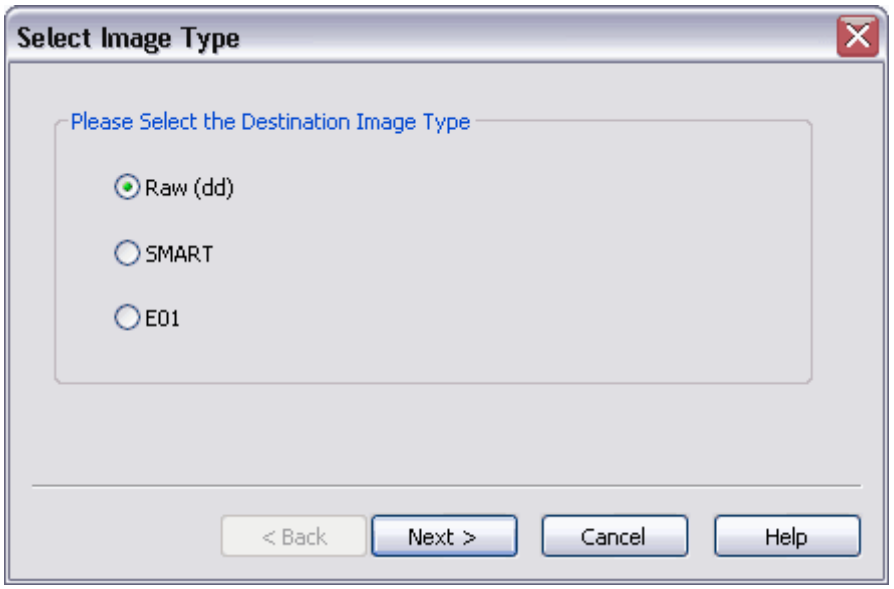


- You can compare the stored hashes of your image content by checking the Verify images after they are created box. If a file doesn't have a hash, this option will generate one.
- You can list the entire contents of your images with path, creation dates, whether files were deleted, and other metadata.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



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

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

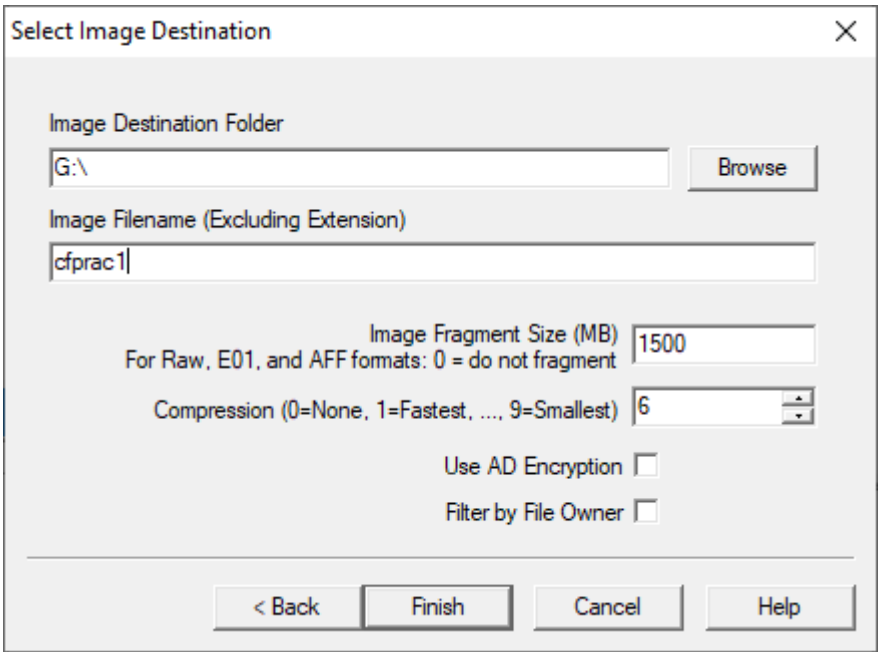


The raw image type is not compressed. If you select the Raw (dd) type, be sure to have adequate space for the resulting image.

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

Raw (dd): This is the image format most commonly used by modern analysis tools. These raw file formatted images do not contain headers, metadata, or magic values. The raw format typically includes padding for any memory ranges that were intentionally skipped (i.e.,

device memory) or that could not be read by the acquisition tool, which helps maintain spatial integrity (relative offsets among data).
SMART: This file format is designed for Linux file systems. This format keeps the disk images as pure bitstreams with optional compression. The file consists of a standard 13-byte header followed by a series of sections. Each section includes its type string, a 64-bit offset to the next section, its 64-bit size, padding, and a CRC, in addition to actual data or comments, if applicable.
E01: this format is a proprietary format developed by Guidance Software's EnCase. This format compresses the image file. An image with this format starts with case information in the header and footer, which contains an MD5 hash of the entire bit stream. This case information contains the date and time of acquisition, examiner's name, special notes and an optional password.
AFF: Advance Forensic Format (AFF) was developed by Simson Garfinkel and Basis Technology. Its latest implementation is AFF4. The goal is to create a disk image format that does not lock the user into a proprietary format that may prevent them from being able to properly analyze it.



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

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

7. In the Image Filename field, specify a name for the image file but do not specify a file extension.
8. In the Image Fragment Size field, specify the maximum size in MB for each fragment of the image file. The s01 format is limited by design to sizes between 1 MB and 2047 MB (2 GB). Compressed block pointers are 31- bit numbers (the high bit is a compressed flag), which limits the size of any one segment to two gigabytes.

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

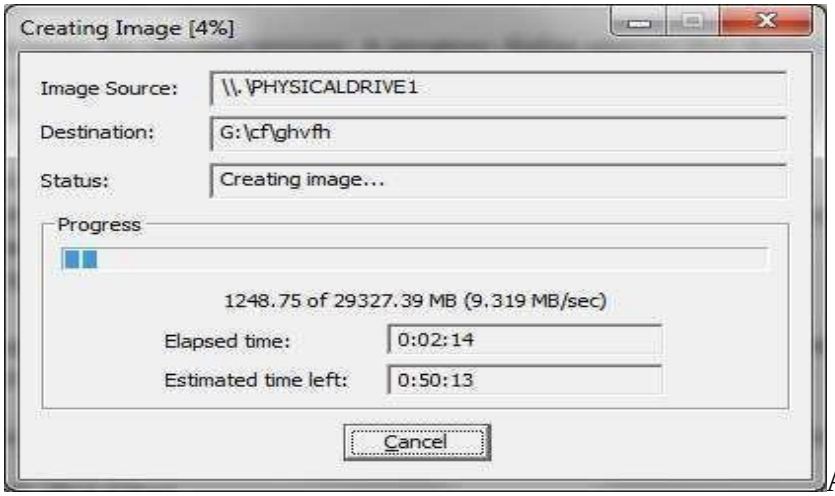
9. Click **Finish**. You return to the Create Image dialog.
10. To add another image destination (i.e., a different saved location or image file type),

click **Add**, and repeat steps 5– 10. To make changes to an image destination, select the destination you want to change and click **Edit.**

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

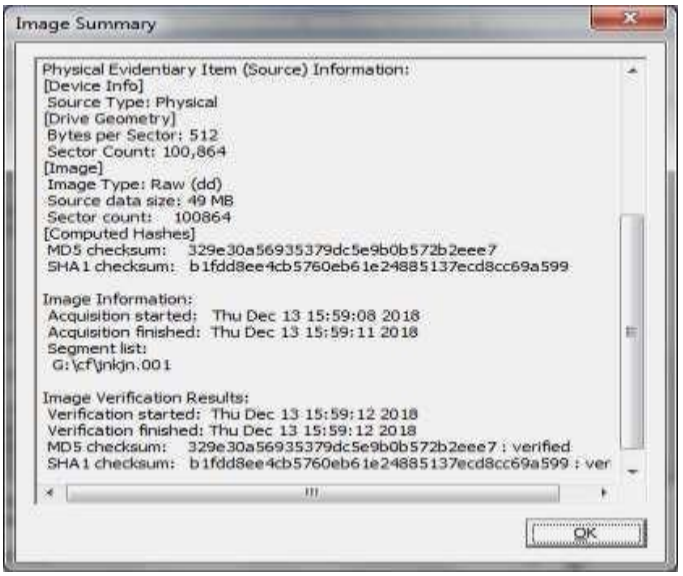
11. Click **Start** to begin the imaging process. A progress dialog appears that shows the following:

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



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

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

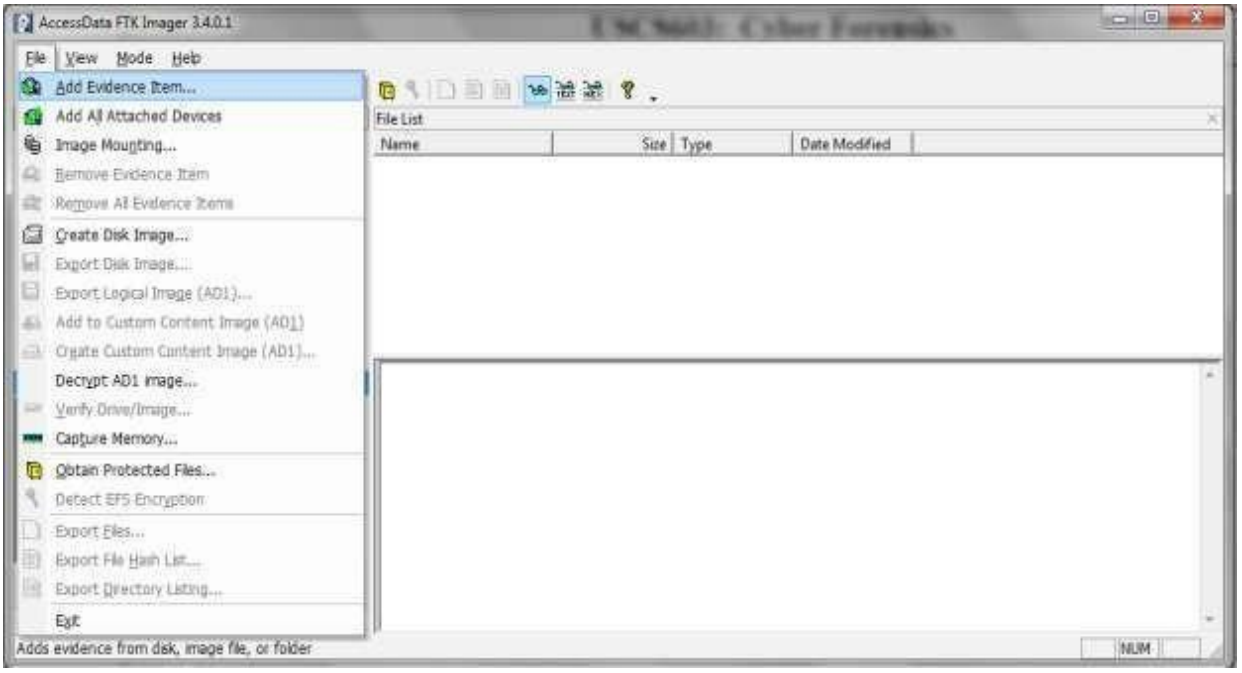


12. When finished, click **Close**

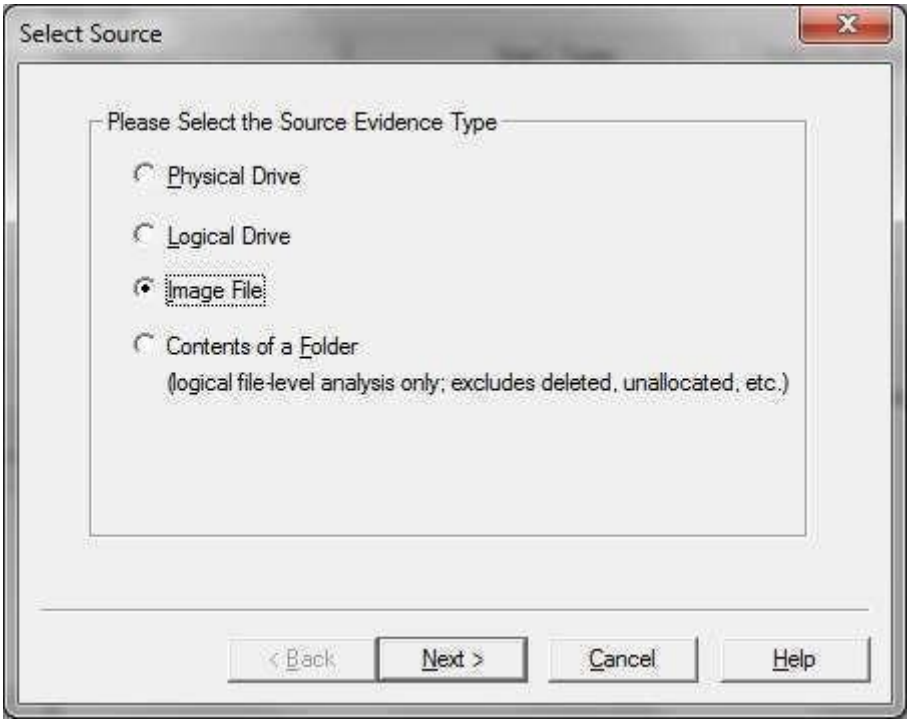
Note that the image file (*.001) as well as the image summary file from above (*.txt) have been saved onto the 'Drive'. The .001 extension may be left as is, or can be changed to .dd. The .001 extension is used due to the fact that many times the file to be imaged is very large and must be split into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

Analyze Forensic Image:

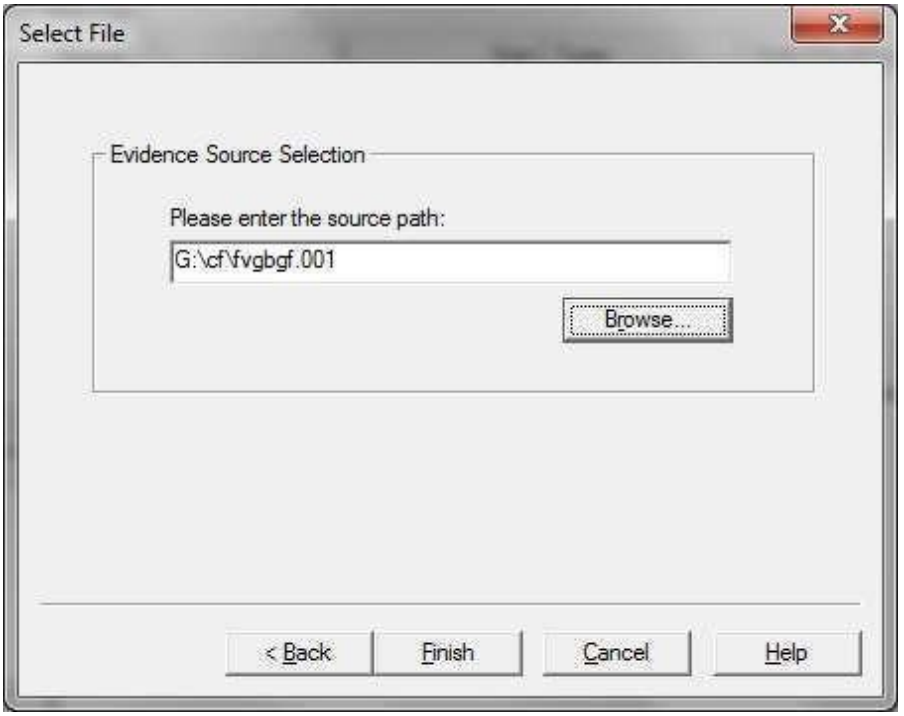
Click on Add Evidence Item to add evidence from disk, image file or folder.



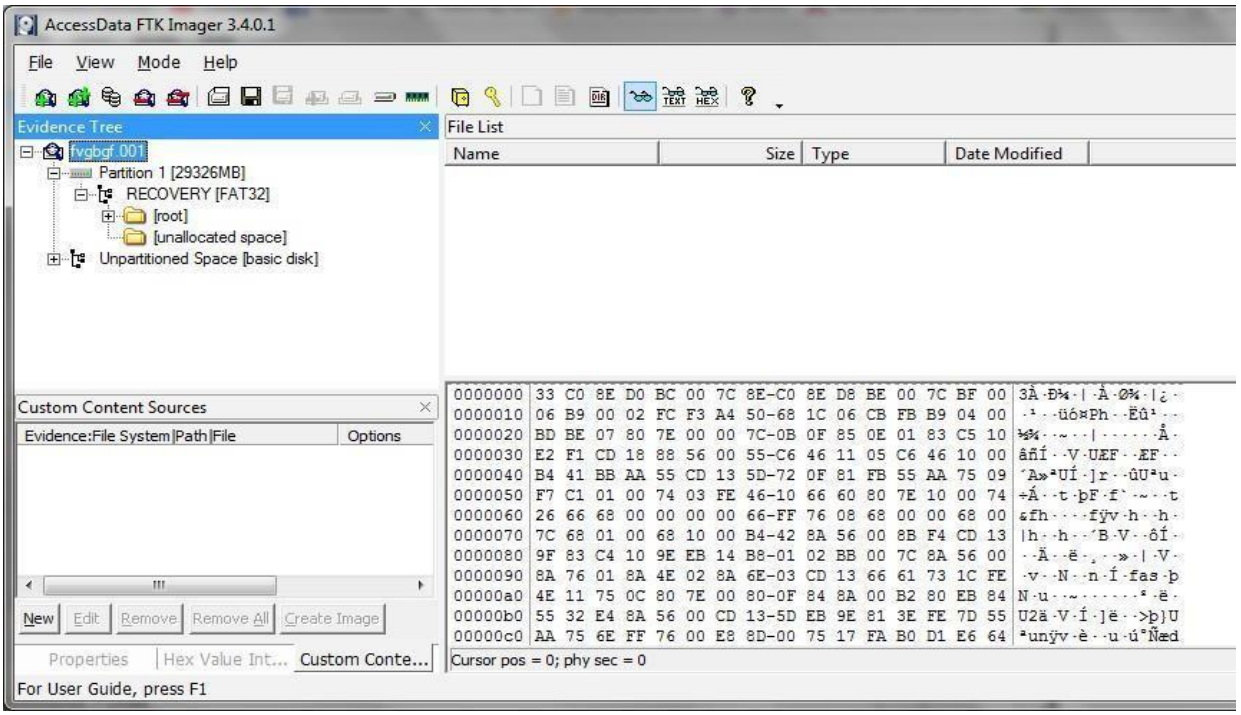
Now select the source evidence type as physical drive, logical drive or image file. We have selected image file and click on next.



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



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



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

Click on finish.

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

Practical No – 2

Aim: Data Acquisition:

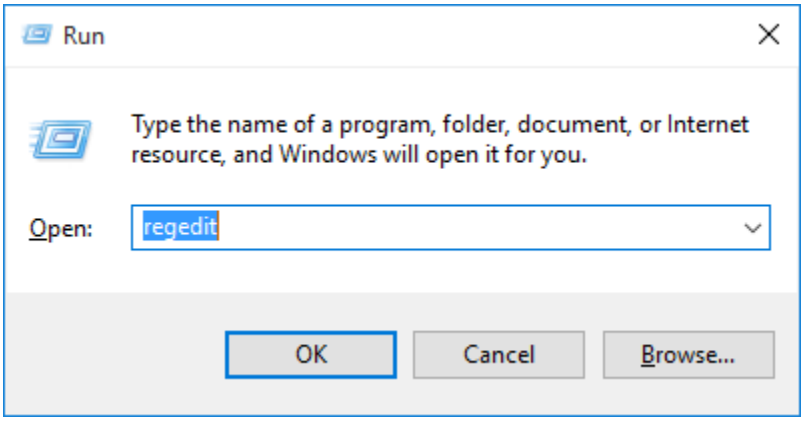
- Perform data acquisition using:

- USB Write Blocker + FTK Imager

Steps:

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

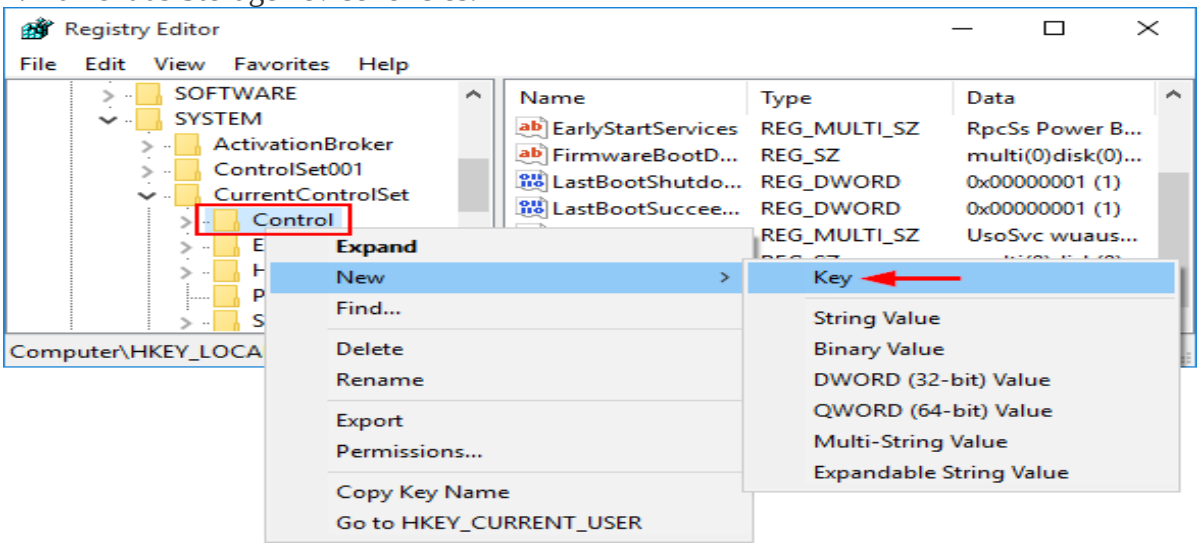
1. Press the Windows key + R to open the Run box. Type regedit and press Enter.



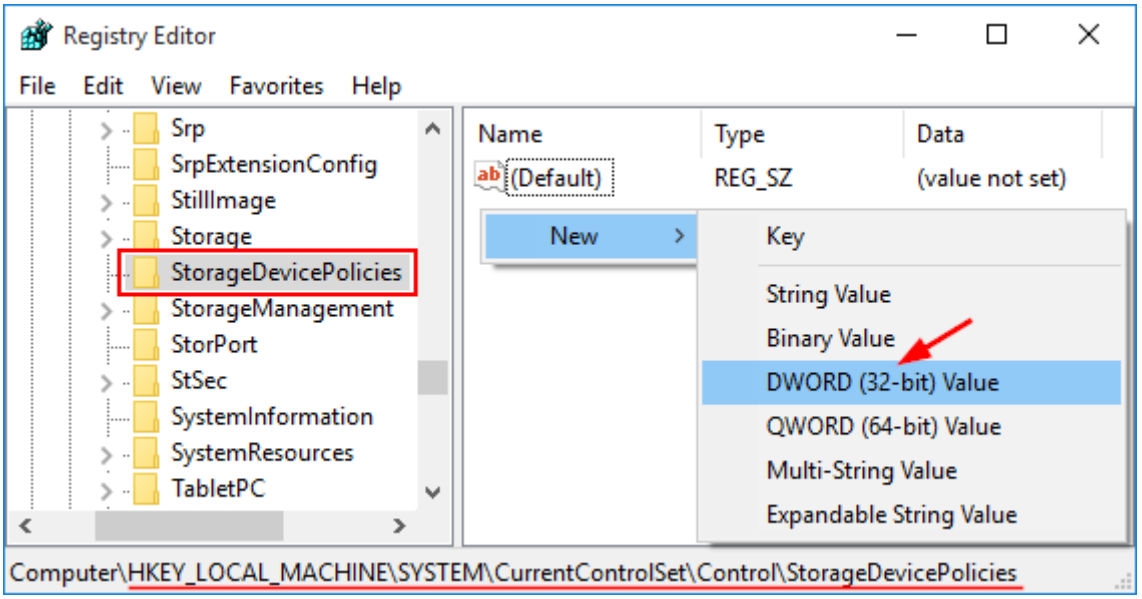
2. This will open the Registry Editor. Navigate to the following key:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control

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

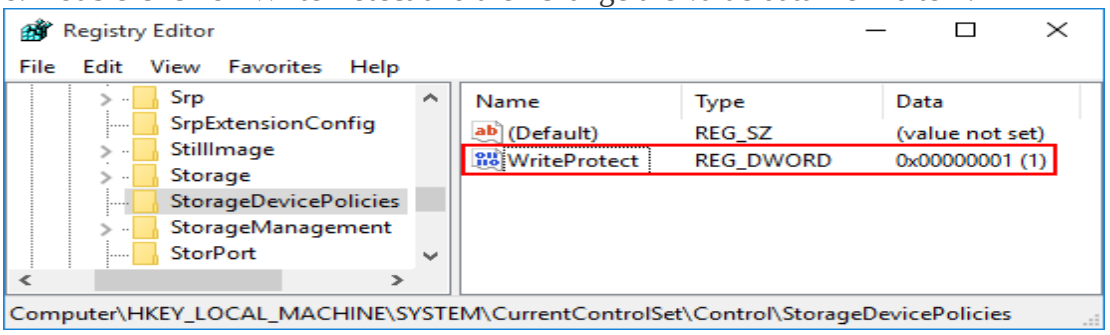
4. Name it as StorageDevicePolicies.



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

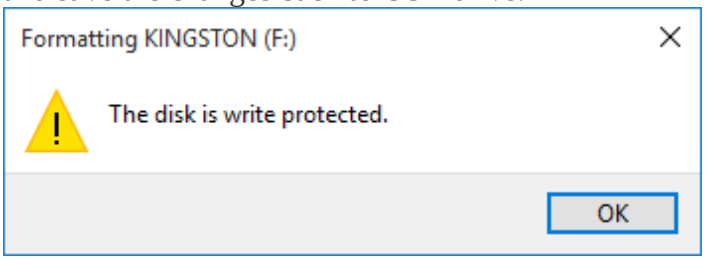


6. Double-click on WriteProtect and then change the value data from 0 to 1.



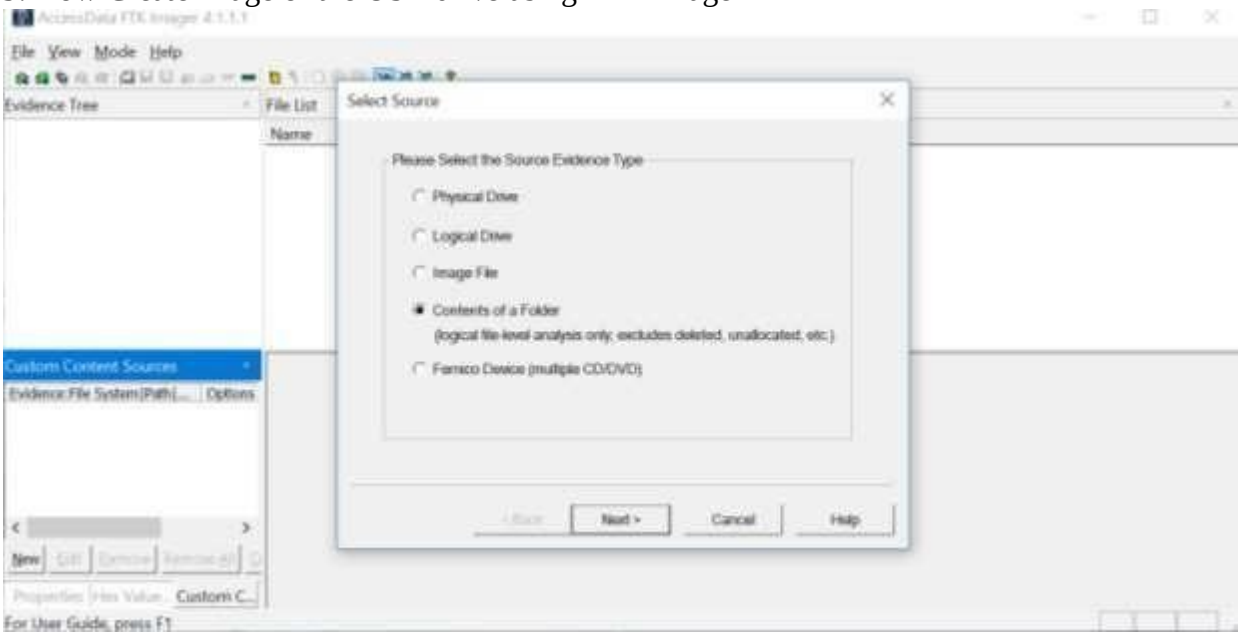
7. The new setting takes effect immediately. Every user who tries to copy / move data to USB devices or format USB drive will get the error message
"*The disk is write-protected*".

8. We can only open the file in the USB drive for reading, but it's not allowed to modify and save the changes back to USB drive.



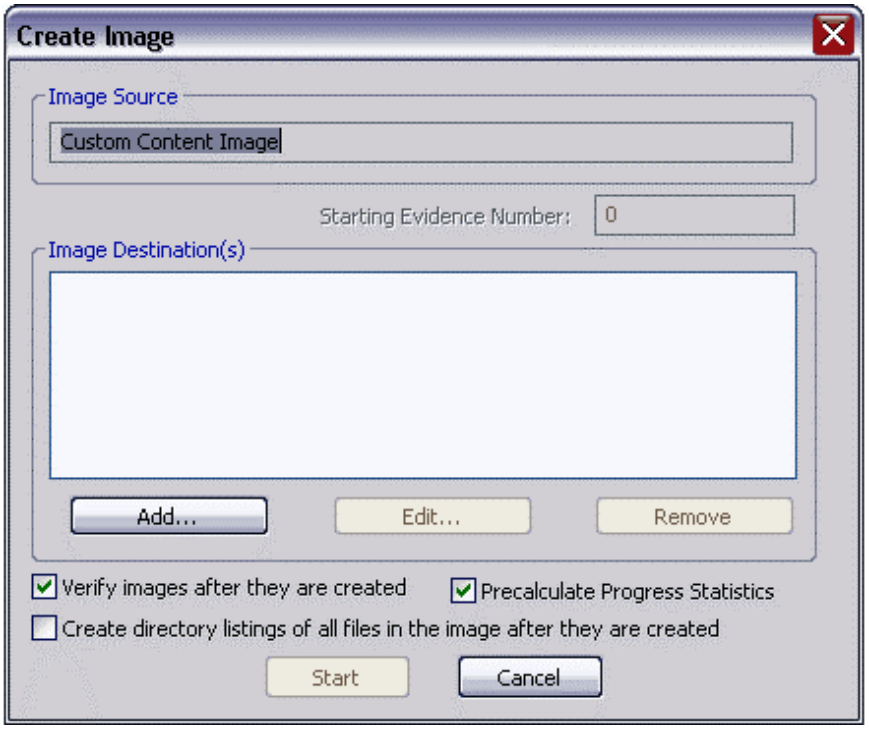
So this is how you can enable write protection to all connected USB drives. If you want to disable write protection at a later time, just open Registry Editor and set the WriteProtect value to 0.

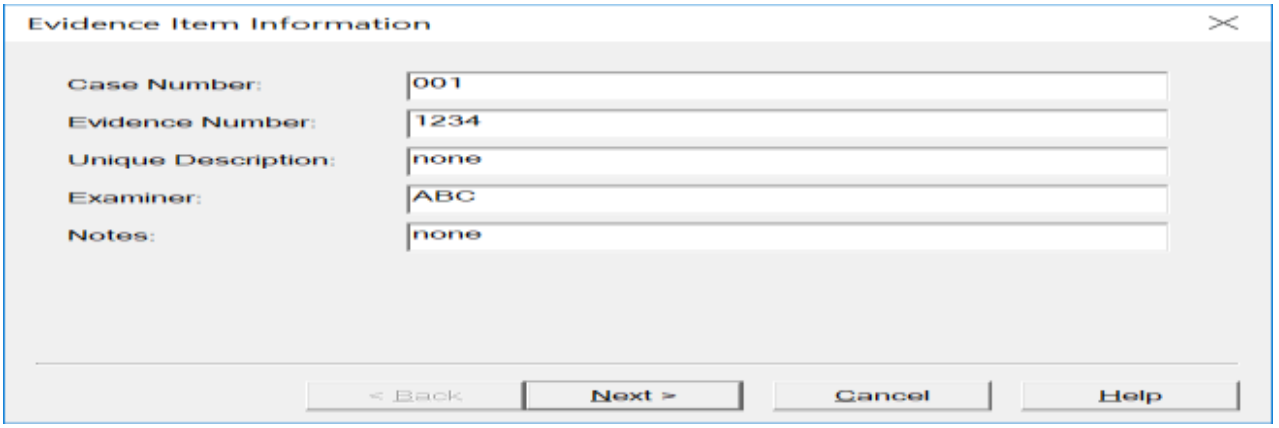
9. Now Create image of the USB drive using FTK imager



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

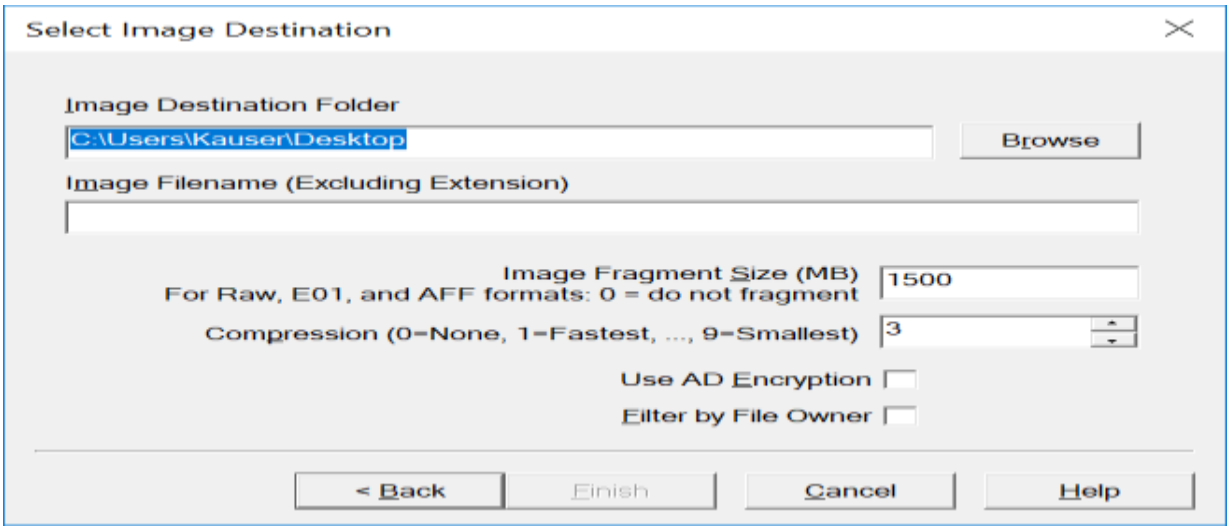
Finish 11.In the Create Image dialog, click Add.

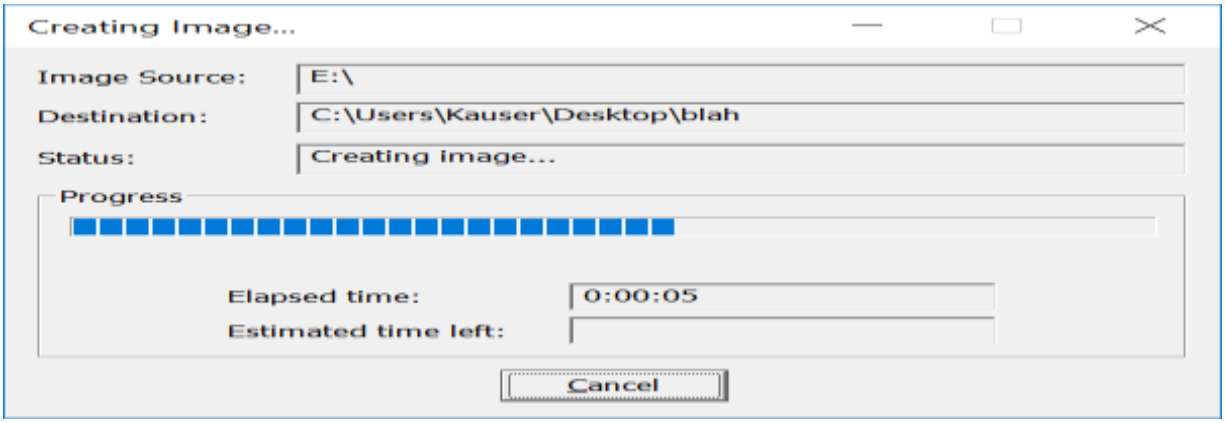




- You can compare the stored hashes of your image content by checking the Verify images after they are created box. If a file doesn't have a hash, this option will generate one.
- You can list the entire contents of your images with path, creation dates, whether files were deleted, and other metadata.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

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





Practical No – 3

Aim: Forensics Case Study:

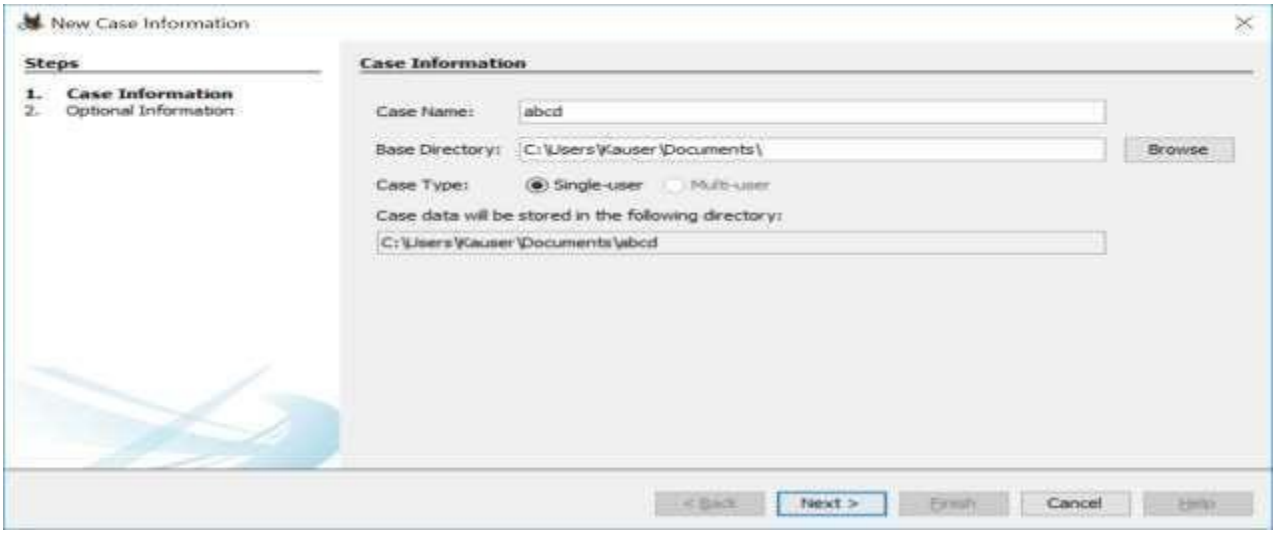
- Solve the Case study (image file) provide in lab using Autopsy

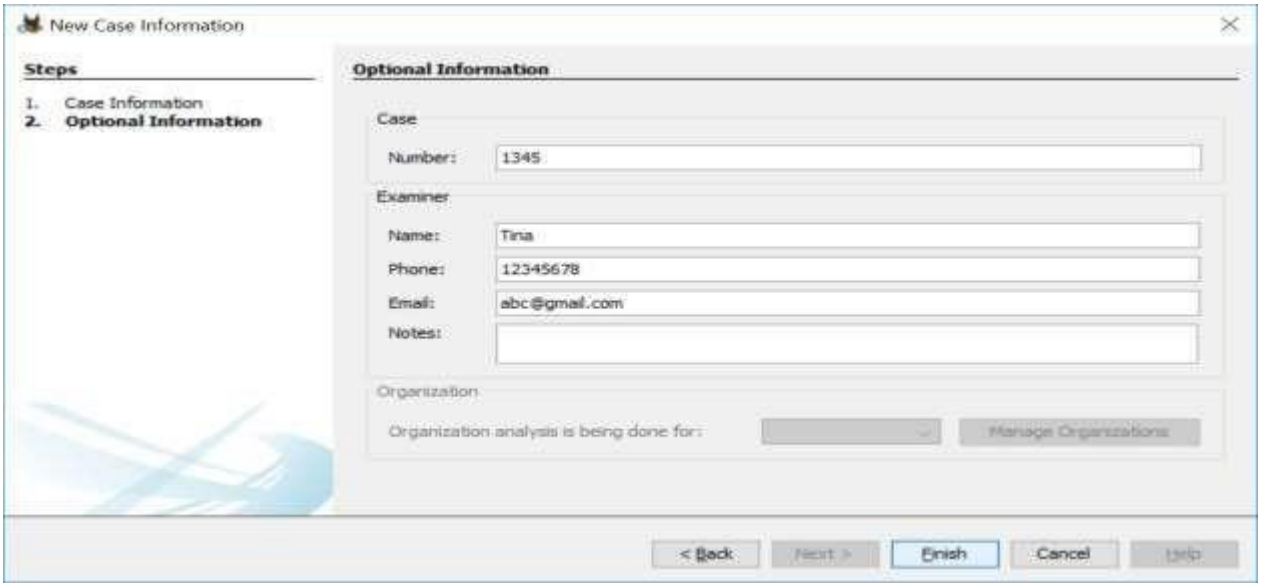
Steps:

1. Start Autopsy

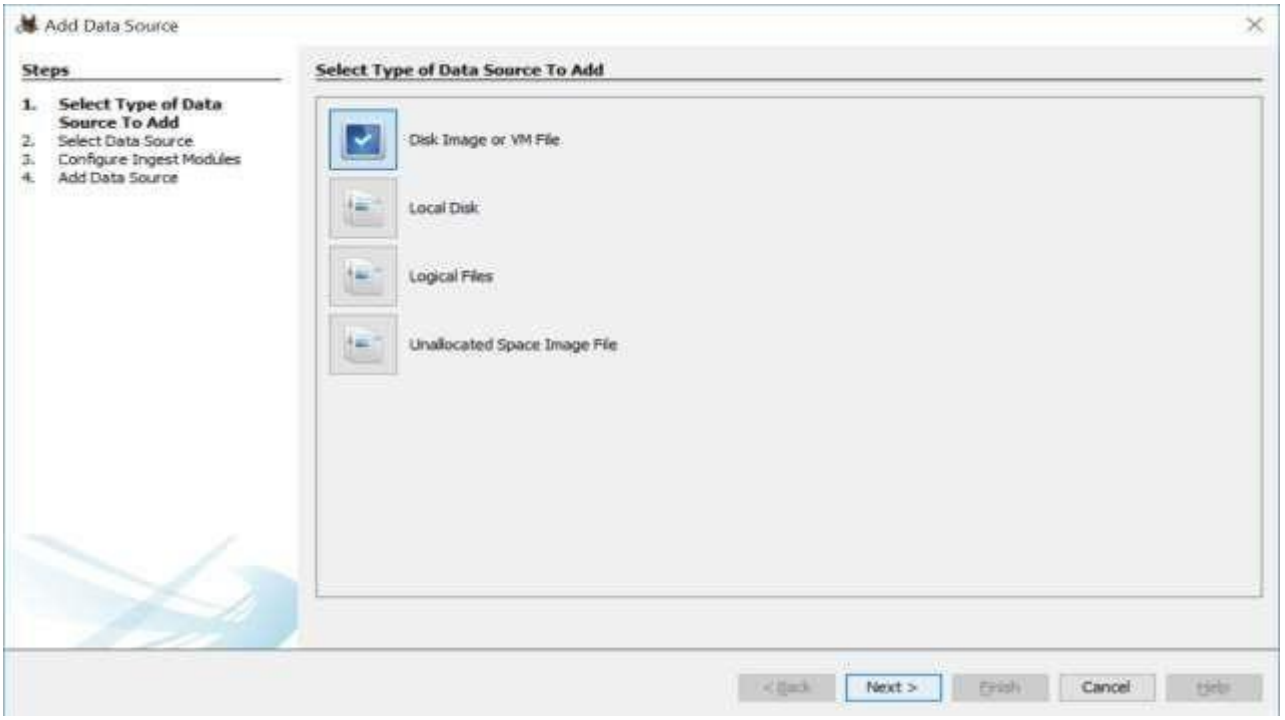
2. Select New Case

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



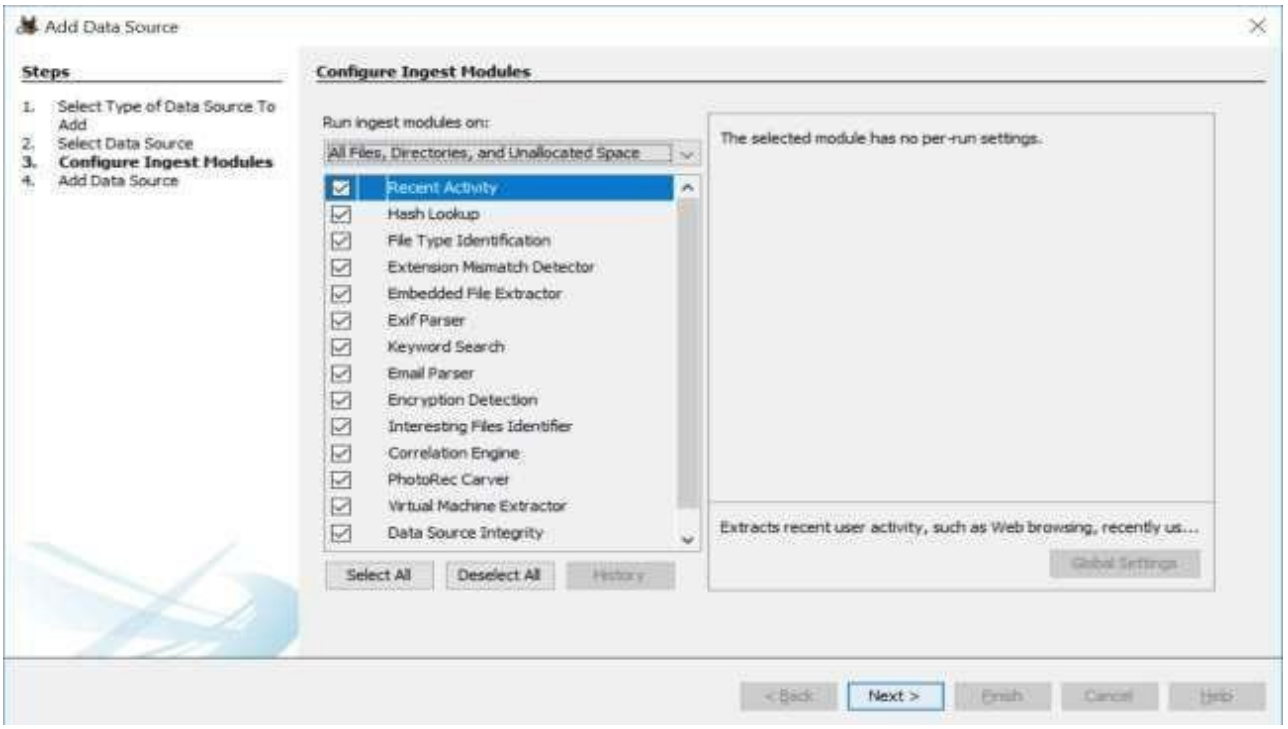


4. Select the type of Data Source that has to be added

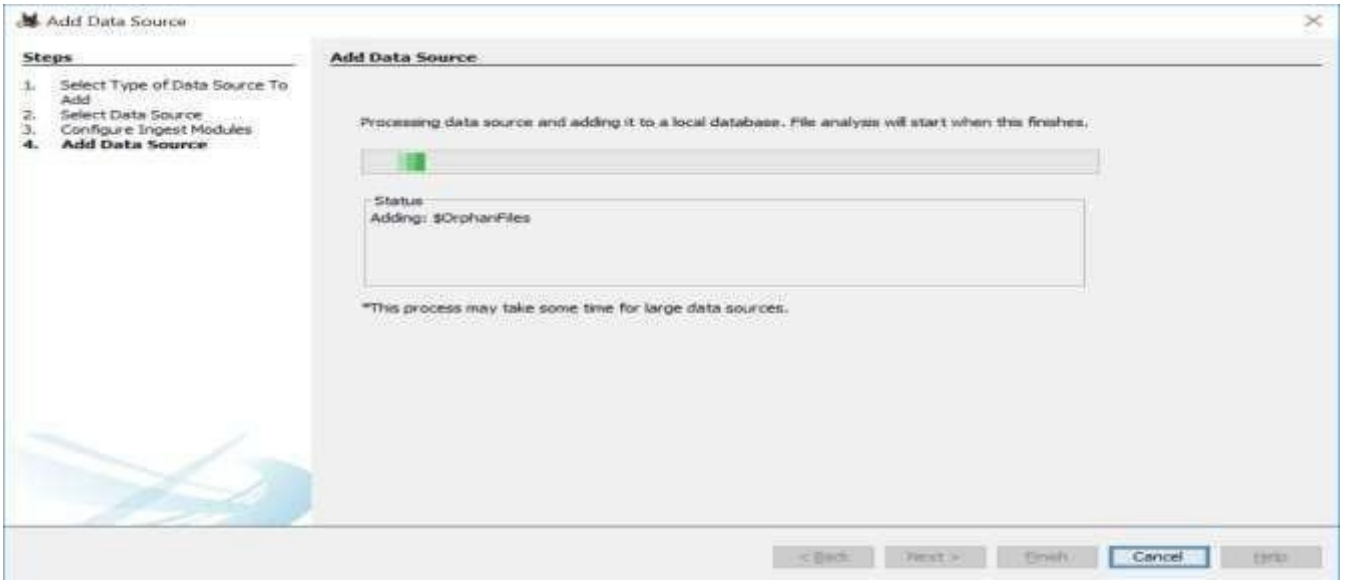


5. Select Data Source(here a previously made image file of a USB is selected)

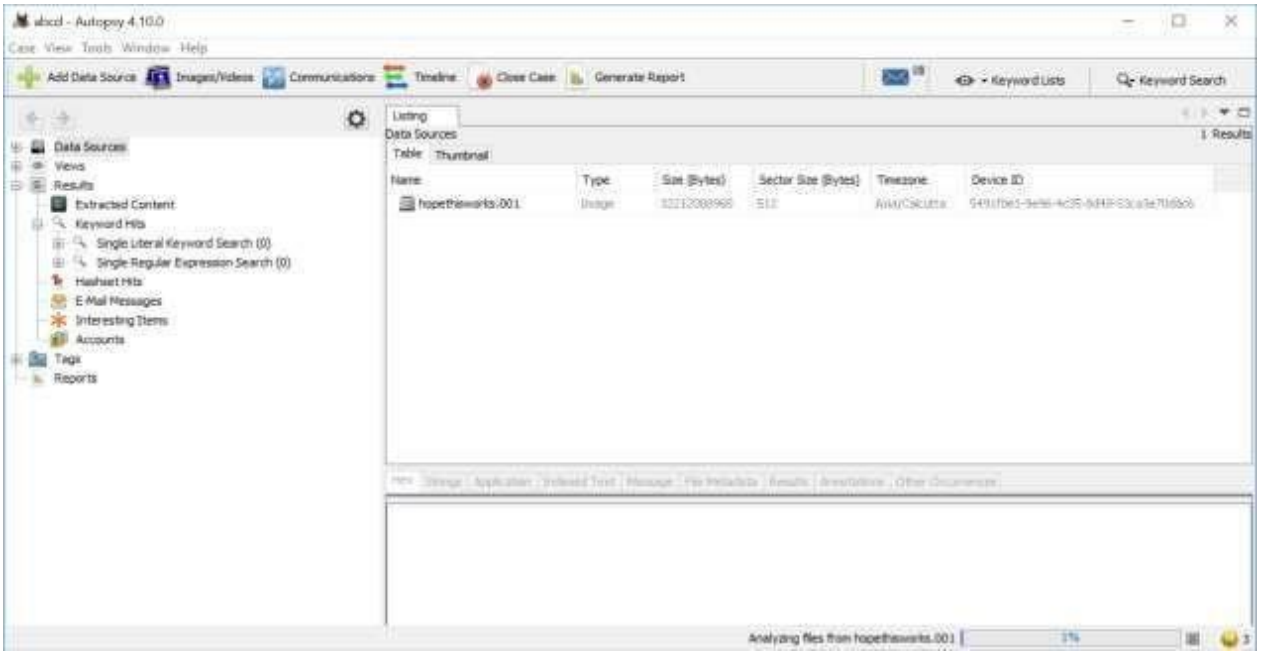
6. Select all ingest modules



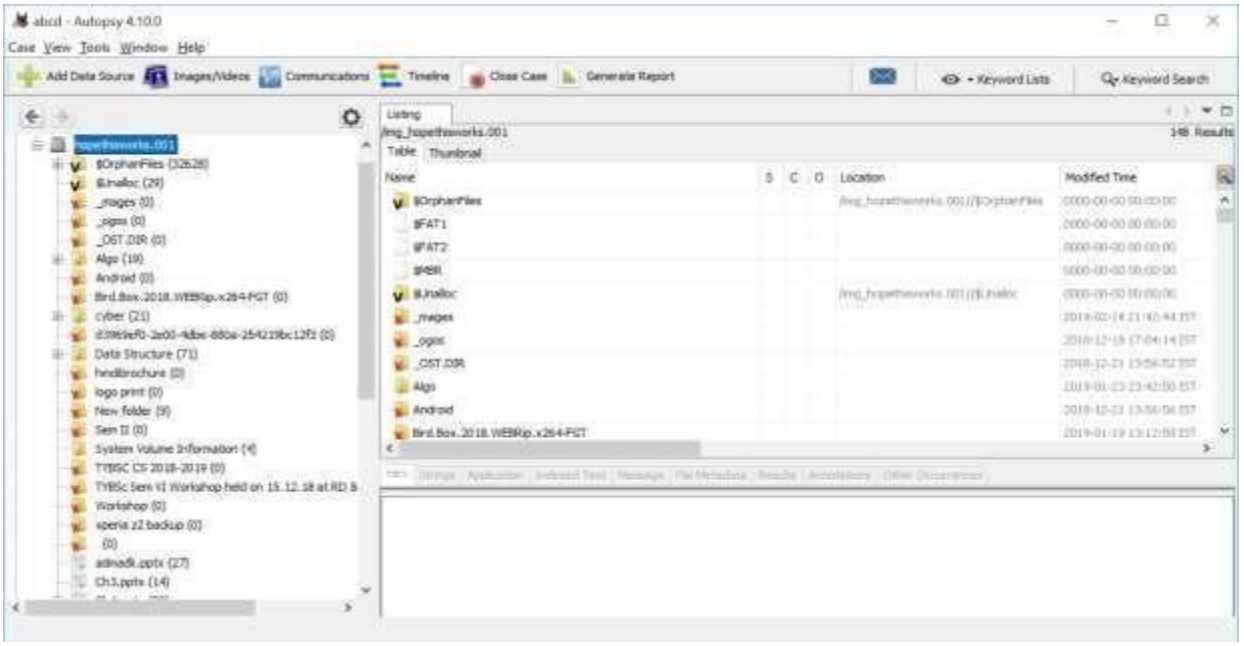
7.Wait for Data source to process and be added to local database. Click Finish



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

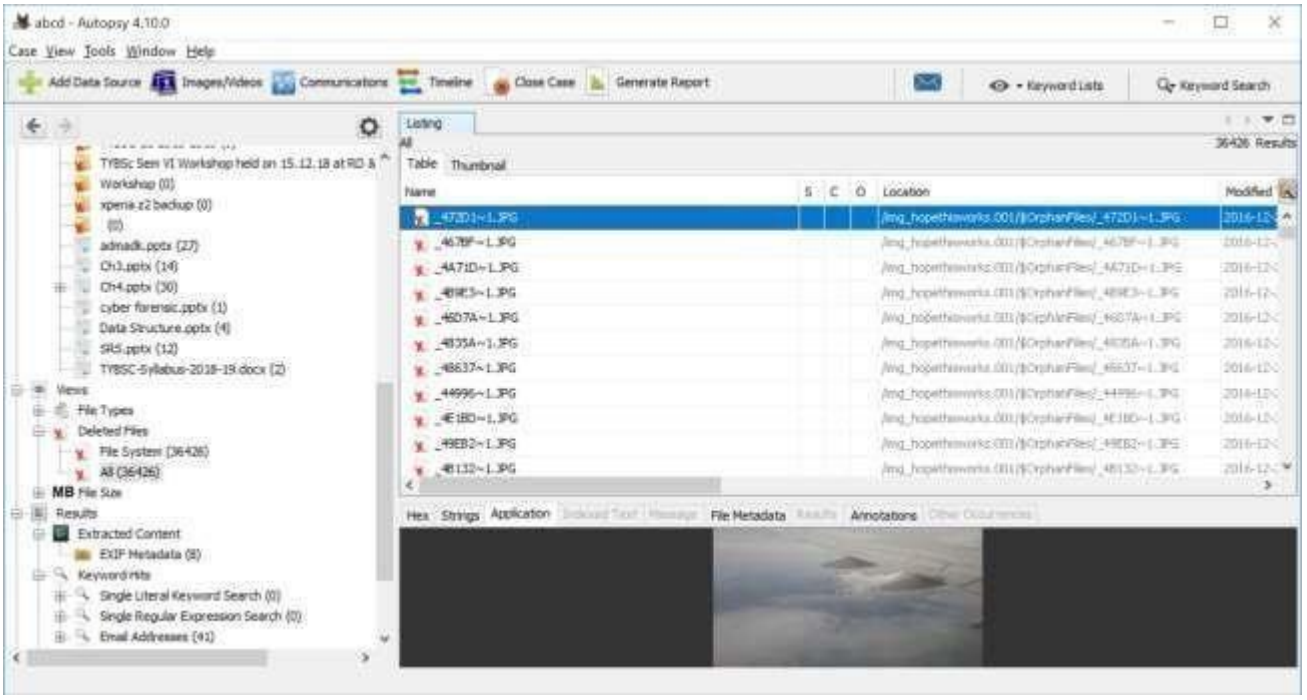


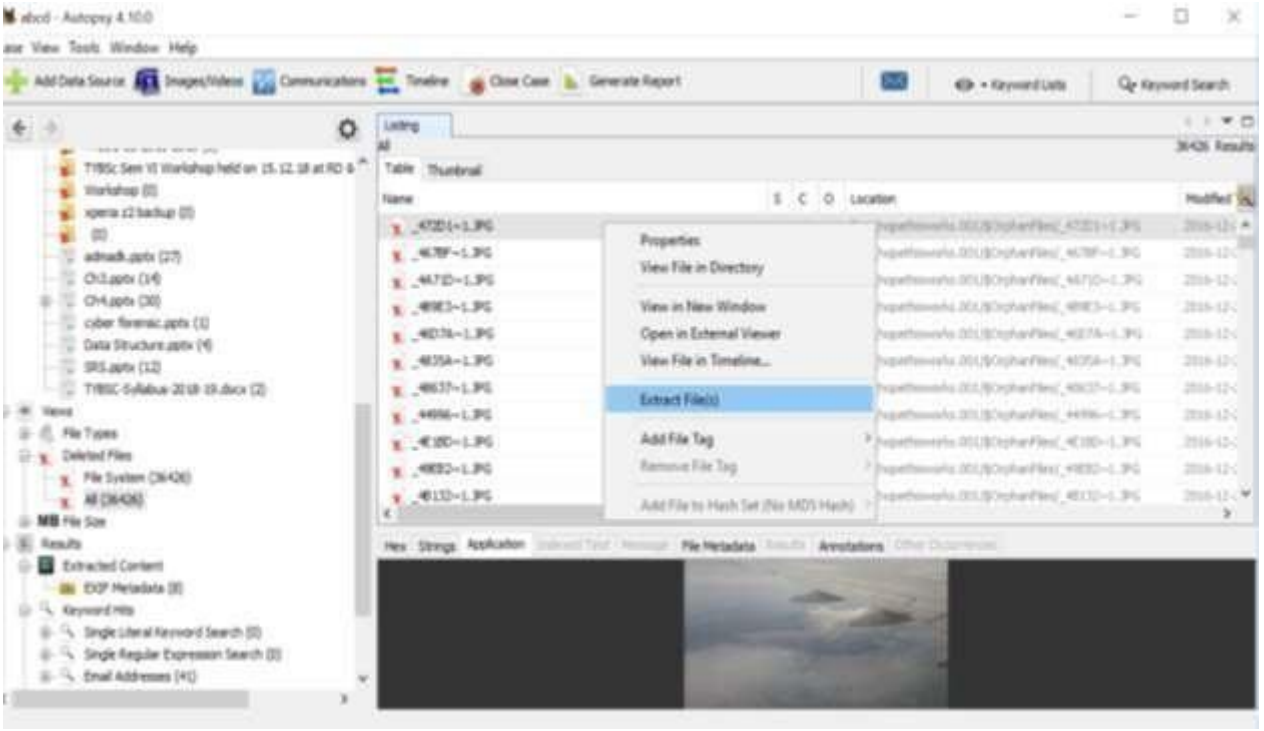
9. All files will appear in table tab select any file to see the data.



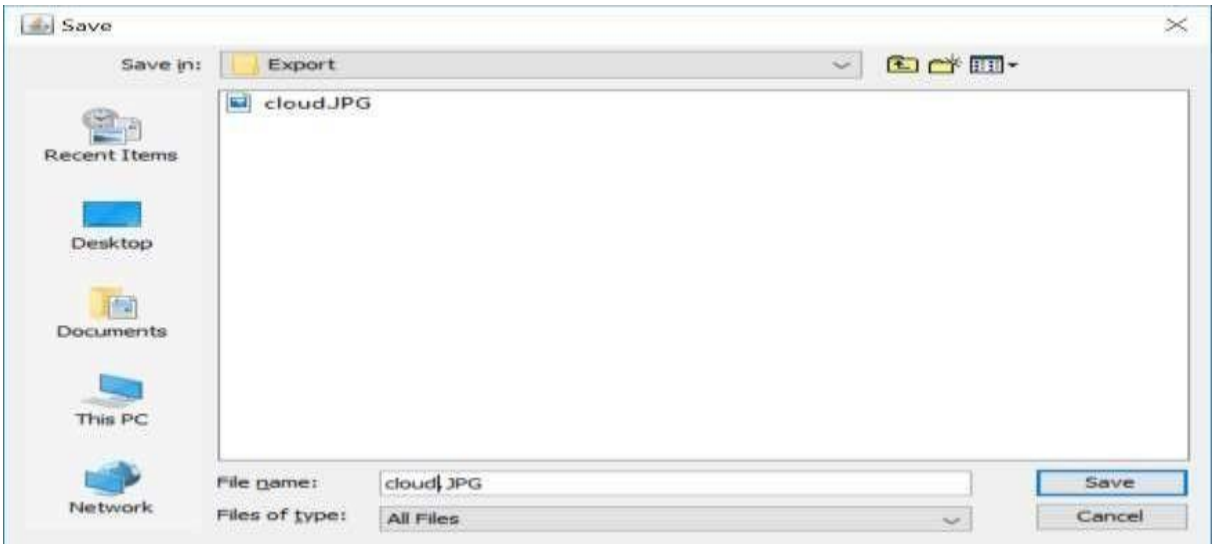
10. Expand the tree from left side panel to view the files and then expand the deleted files node

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

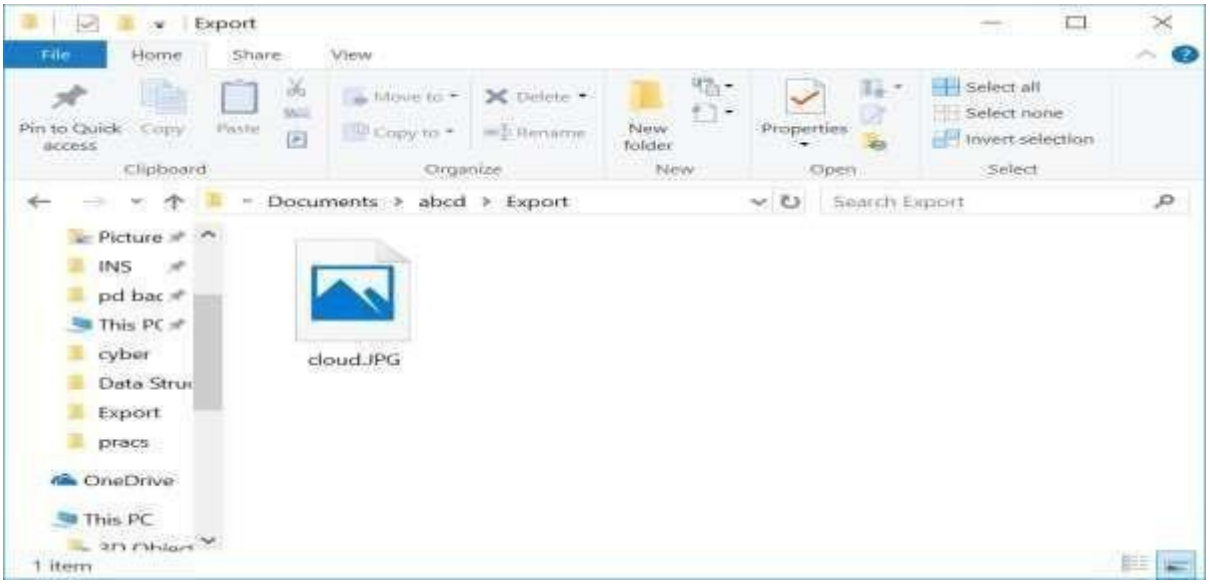


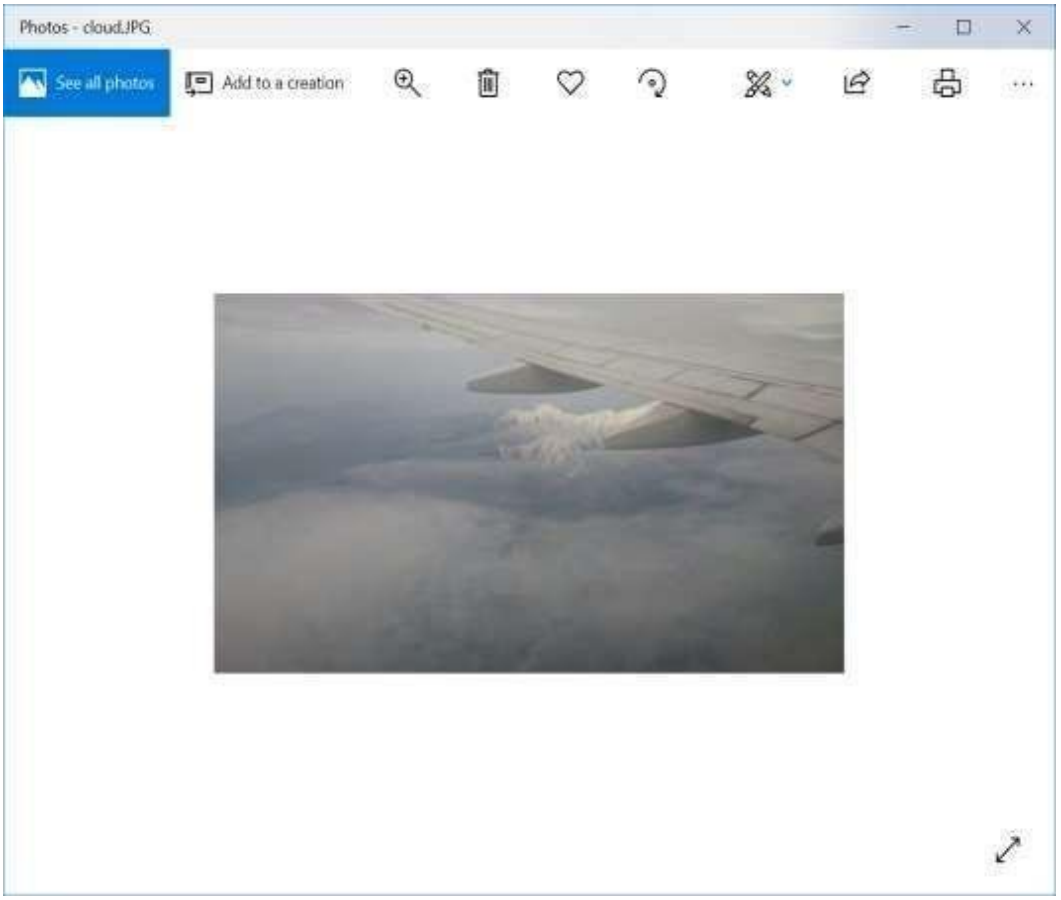


12. By default Export folder is choose to save the recovered file.

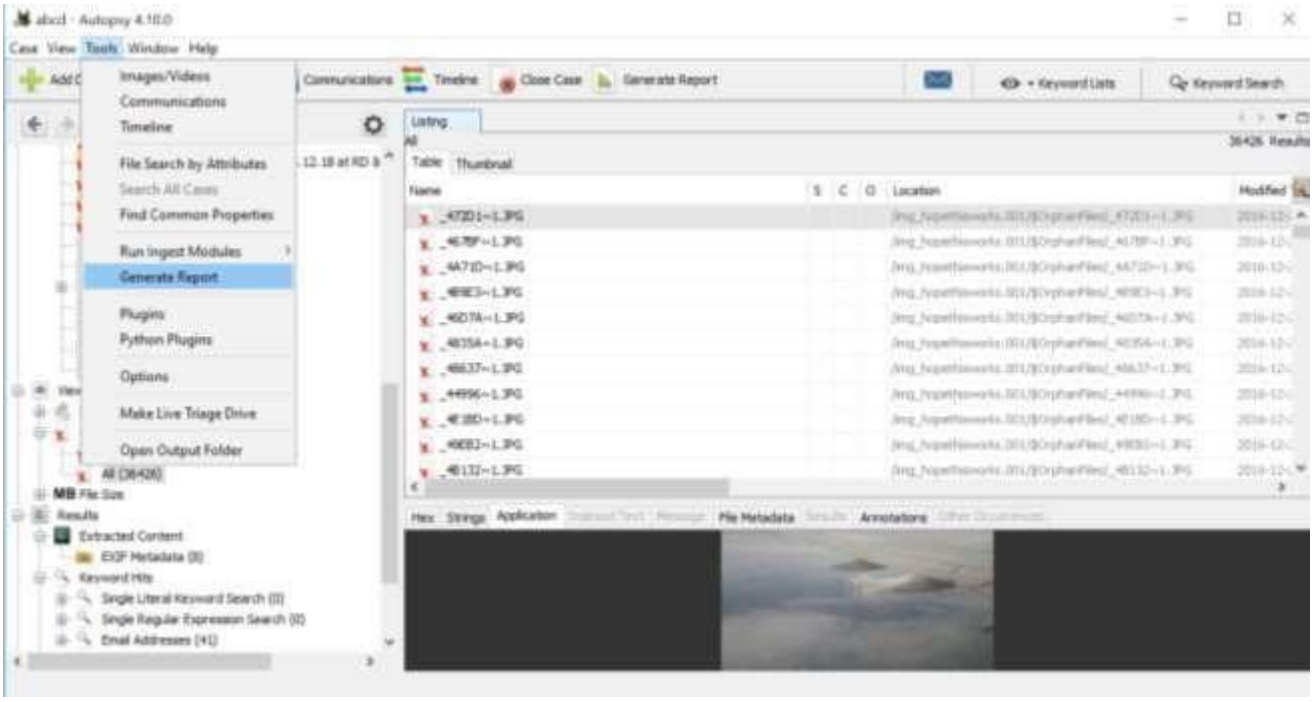


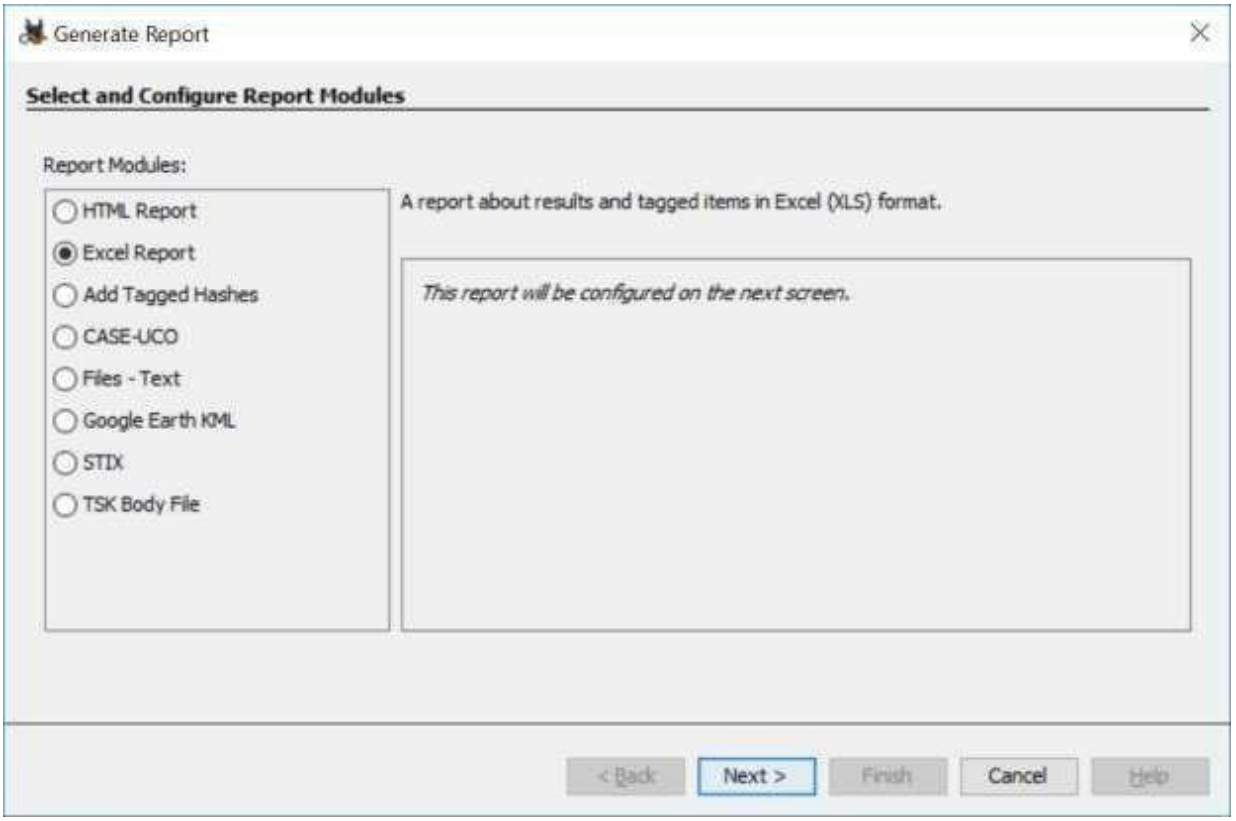
13. Now go to the Export Folder to view Recover file.



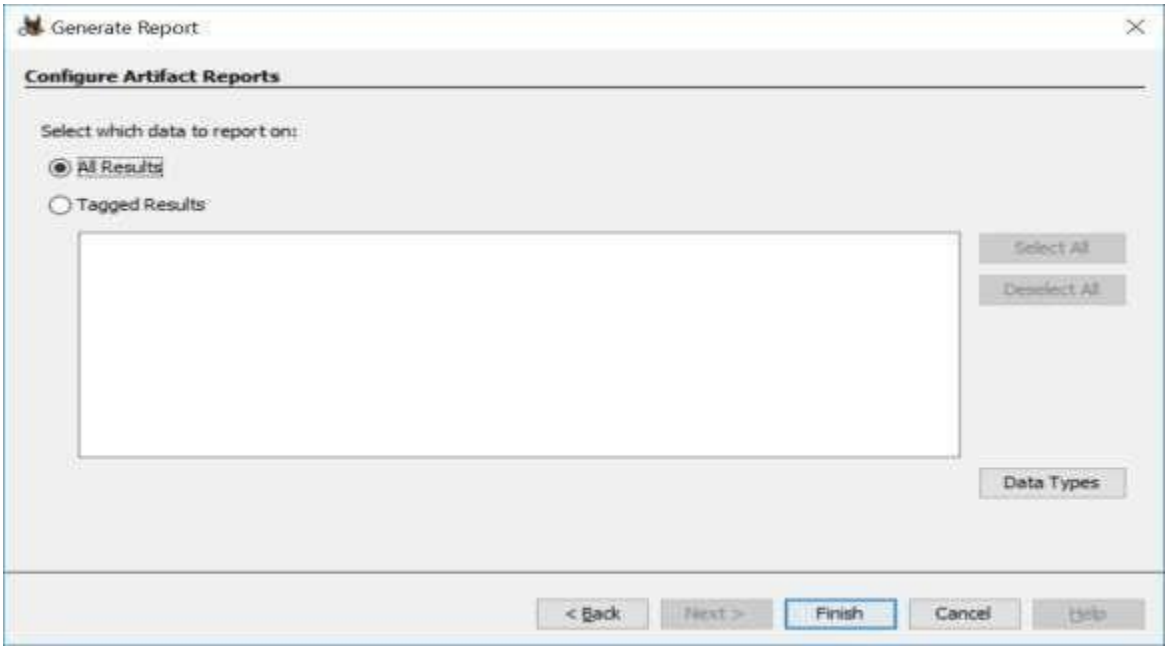


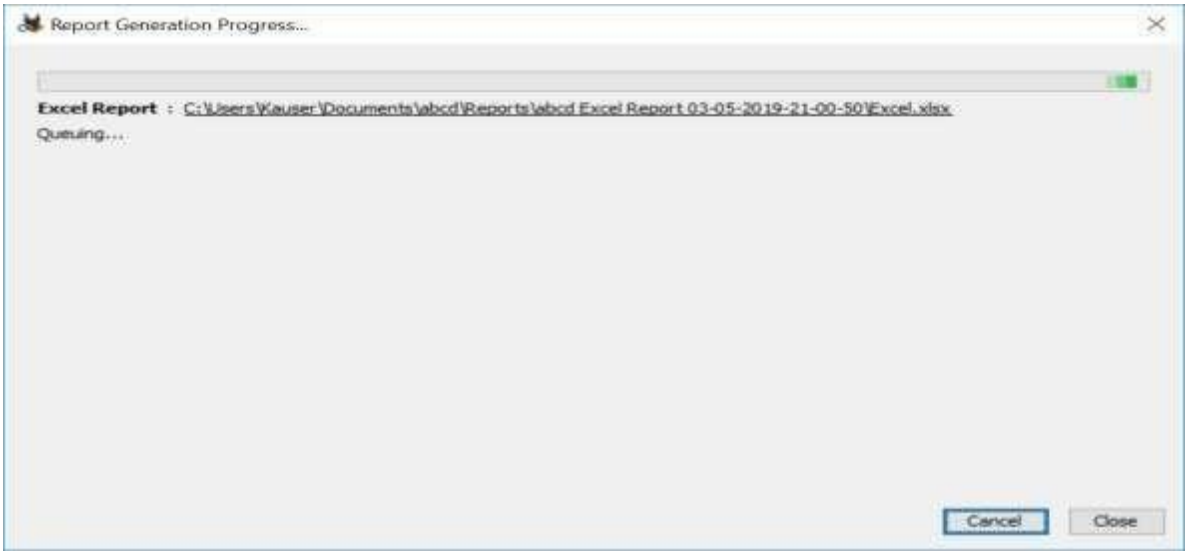
14. Click on Generate Report from autopsy window and Select the Excel format and click on next

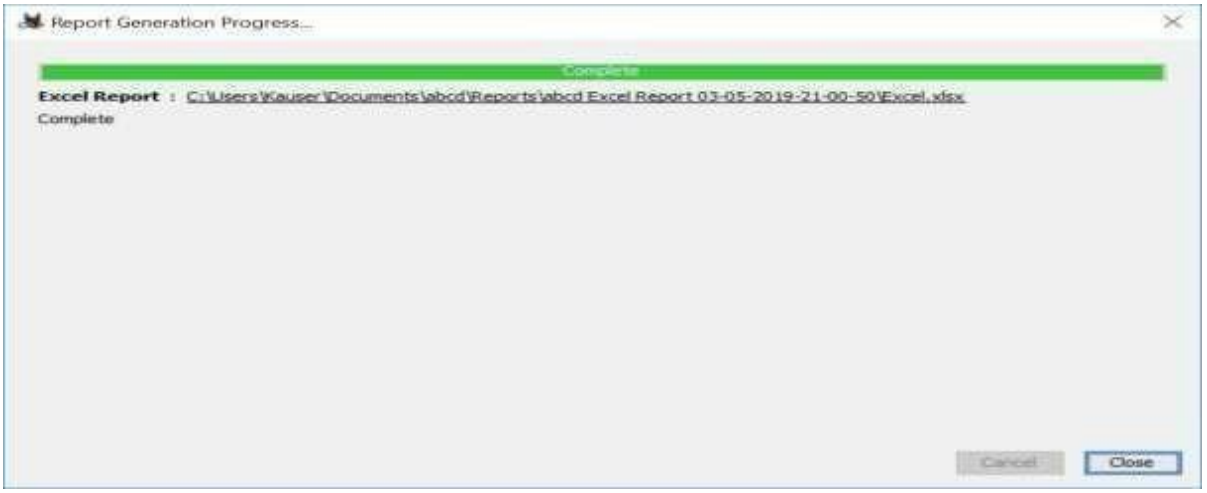




15. Click Finish after selecting All Results

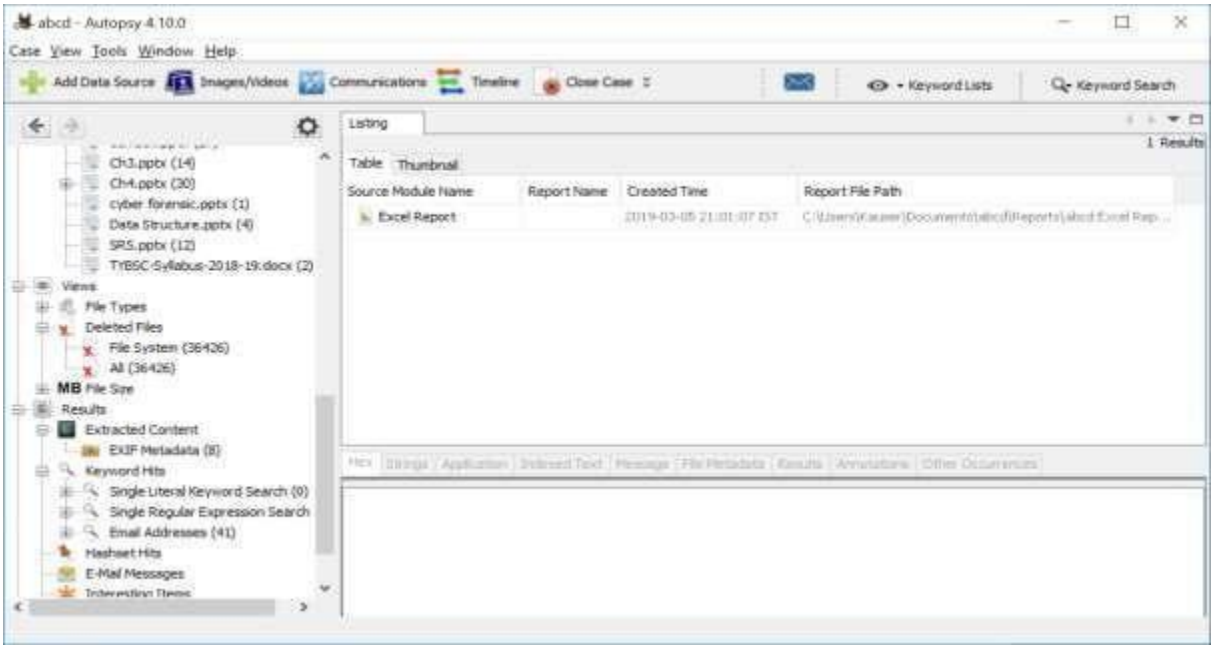


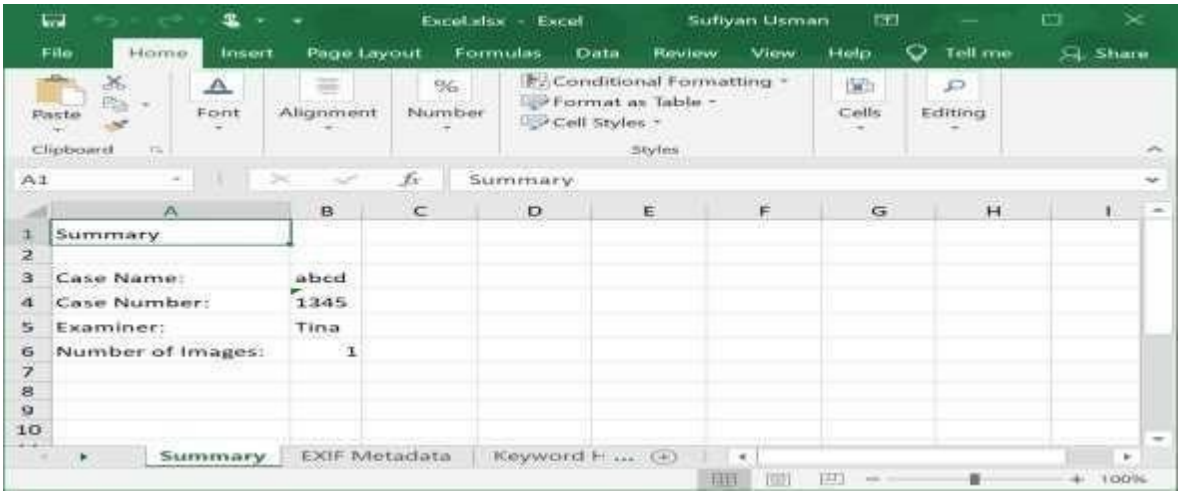


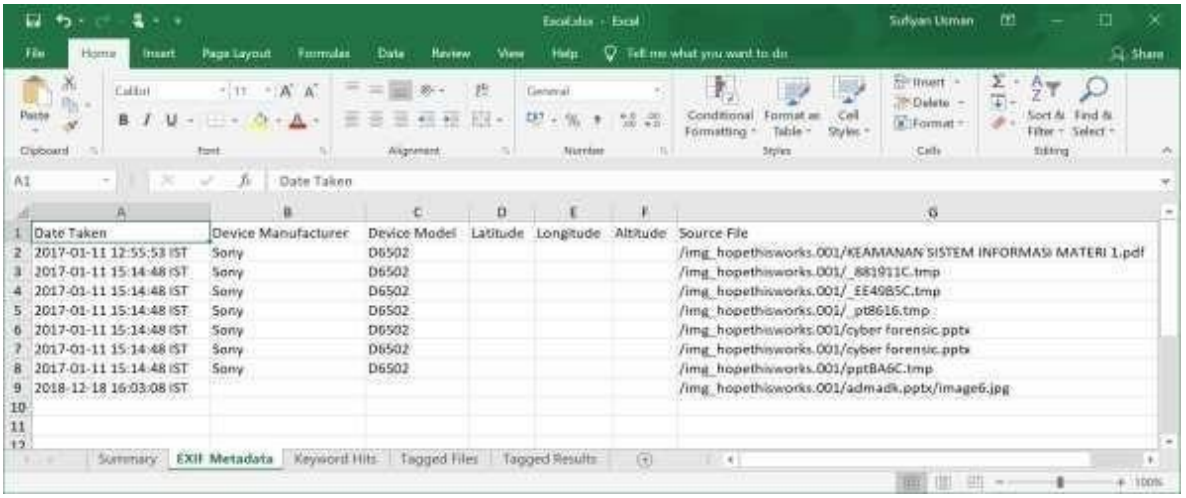


Now Report is Generated So click on close Button, We can see the Report on Report Node.

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







Practical No – 4

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

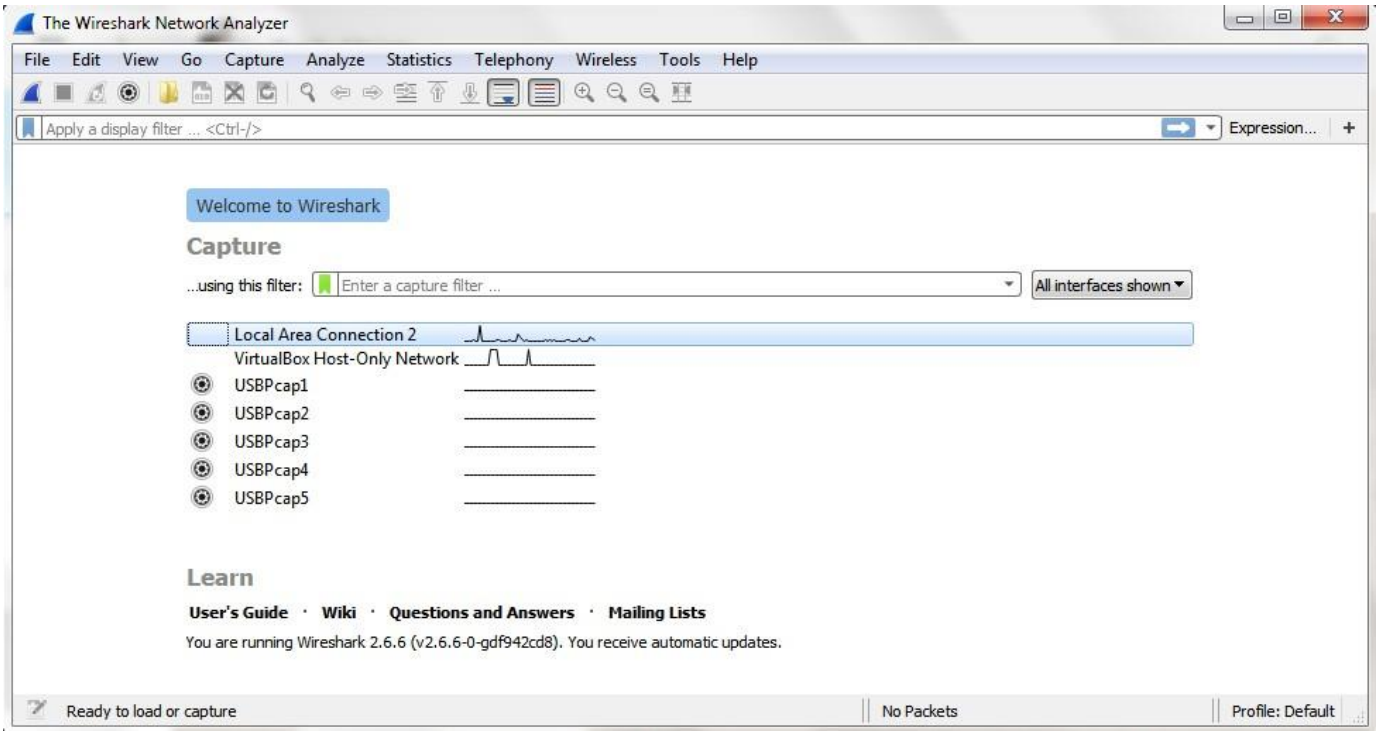
- **Identification the live network**
- **Capture Packets**
- **Analyze the captured packets**

Steps:

Capturing Packets

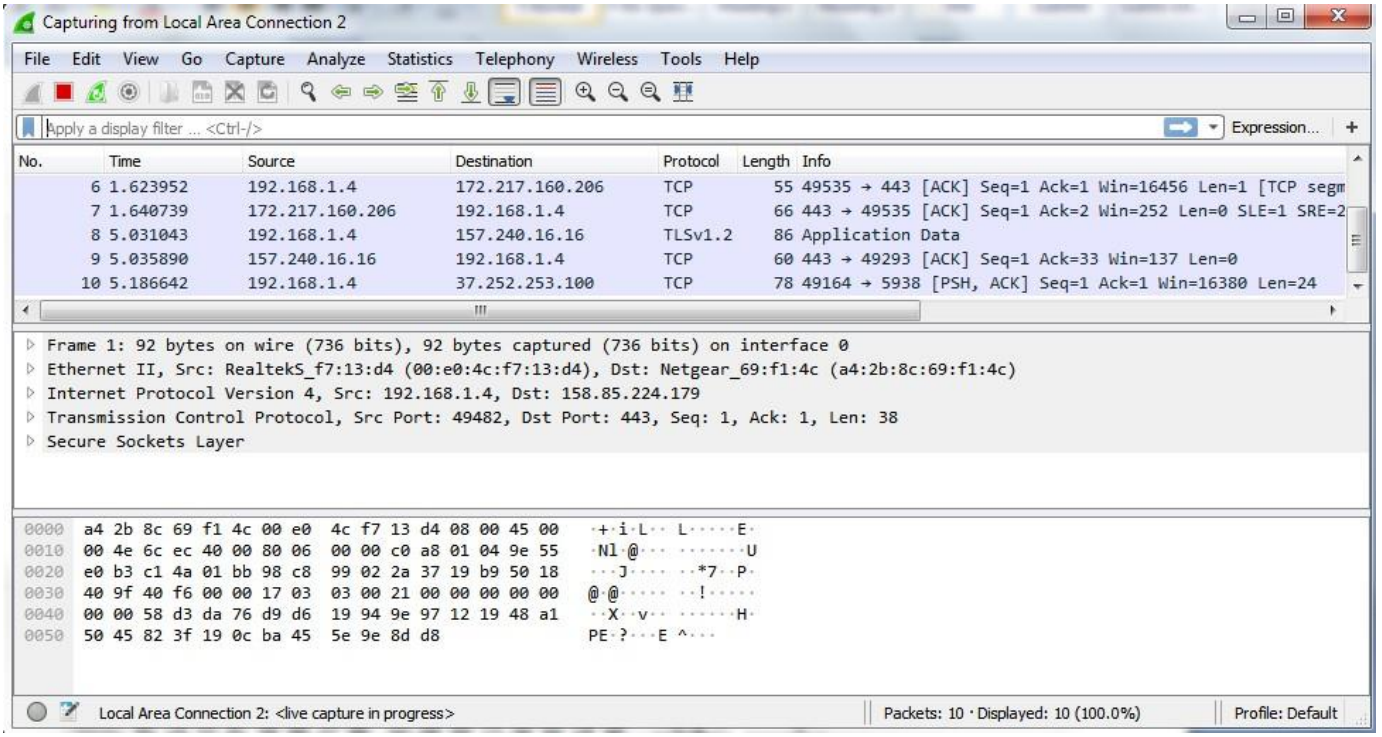
Capture traffic on your wireless network, click your wireless interface.
You can configure advanced features by clicking Capture > Options, but this isn't necessary for now.

1. Open Wireshark and click on Ethernet.



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".

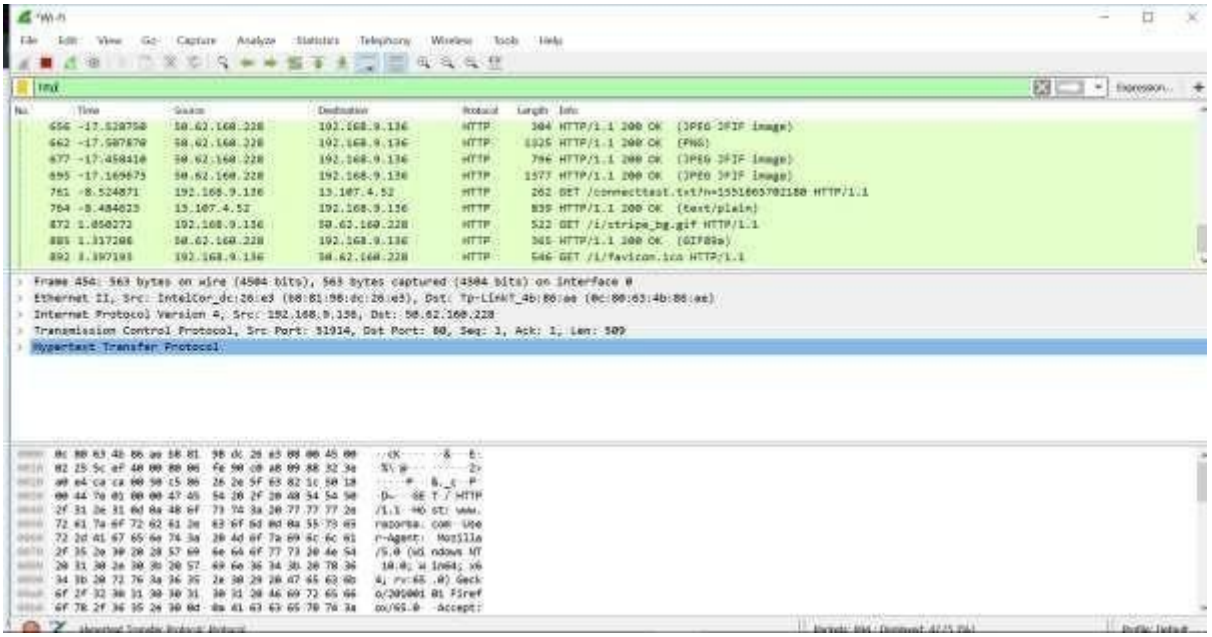


The red box button "STOP" on the top left side of the window can be clicked to stop the capturing of traffic on the network.

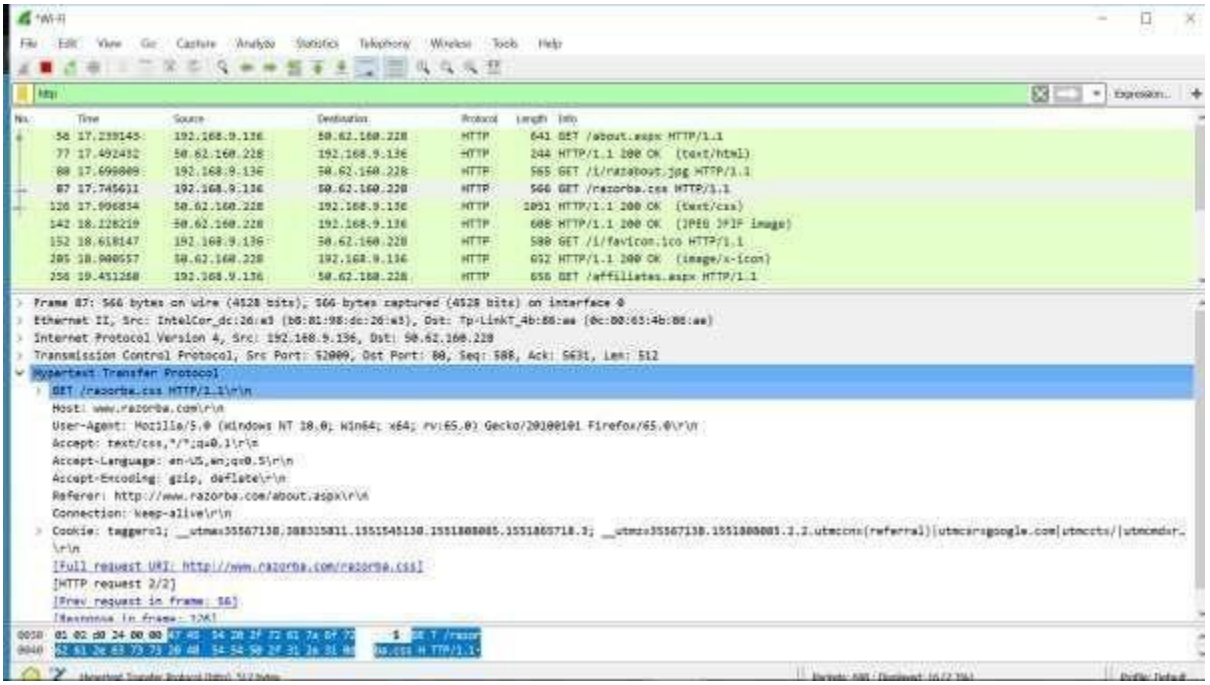
2. Now go on browser and open any unsecured website i.e www.razorba.com and

3. perform some activity on the website.

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



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



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:

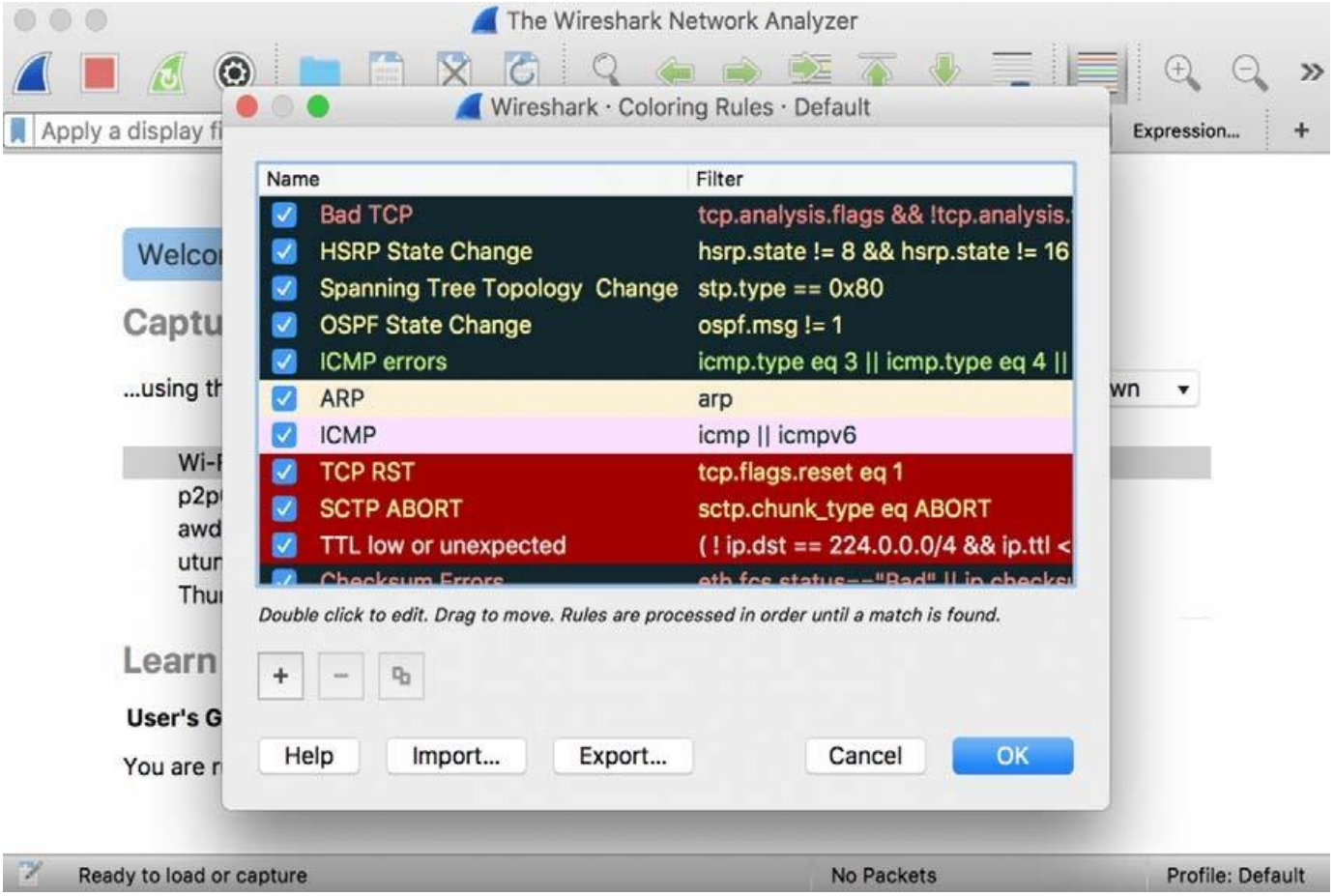
Light Purple color for TCP traffic Light

Blue color for UDP traffic

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

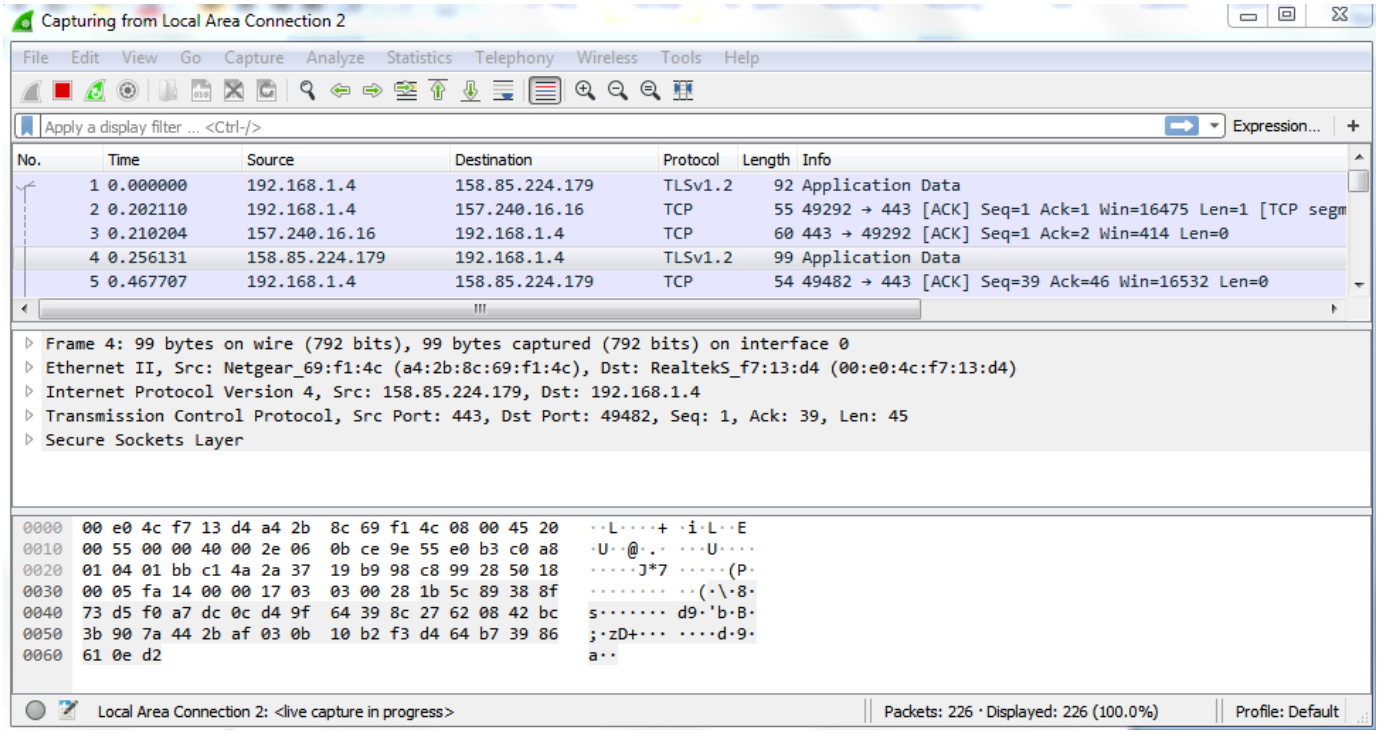
manner.

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.

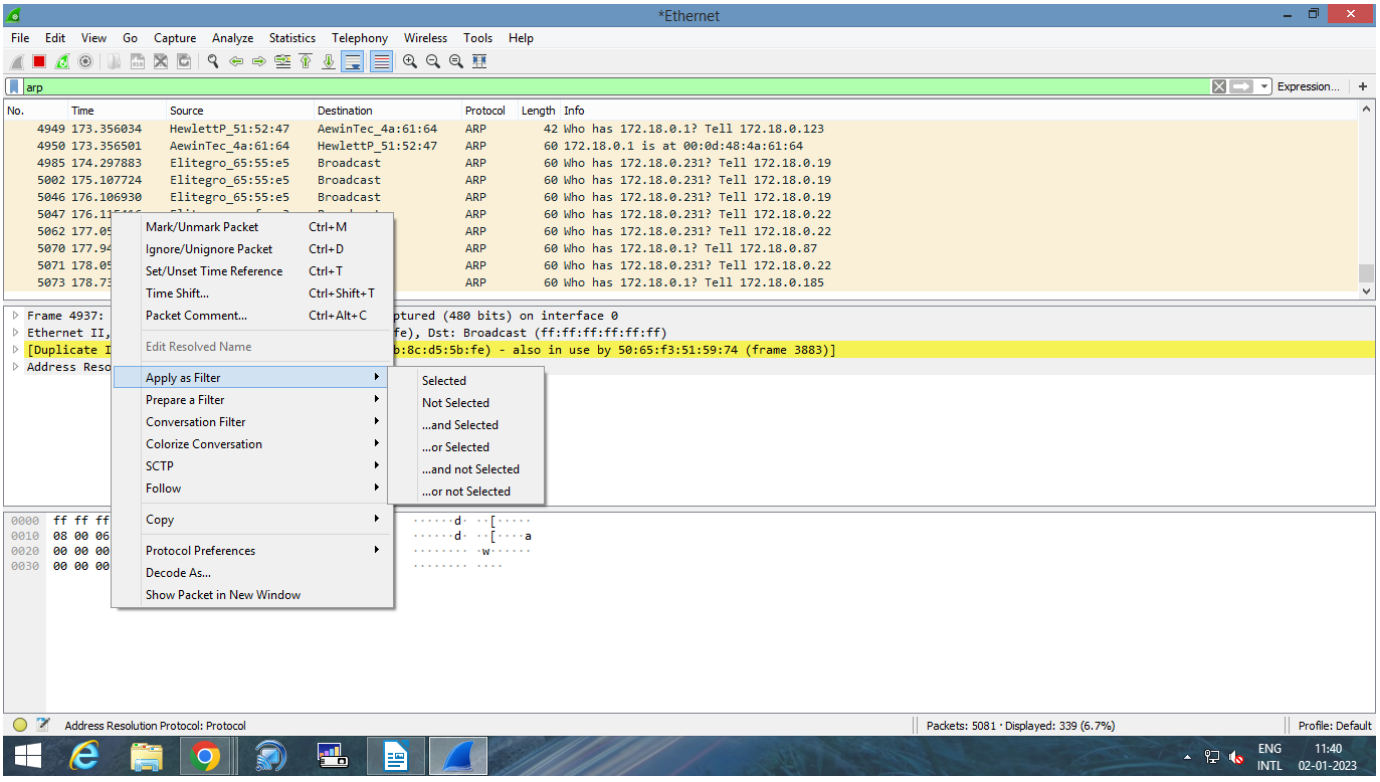


Analyze the captured Packets:

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



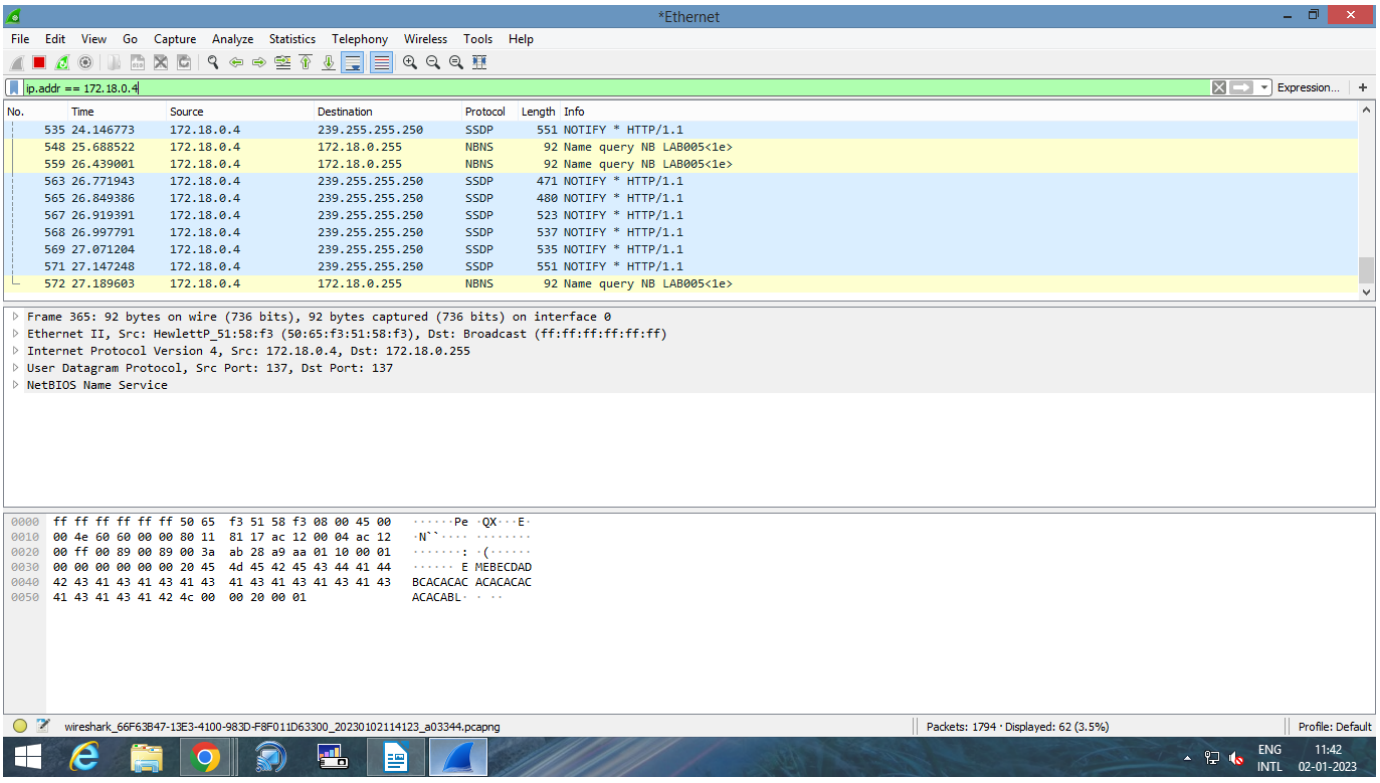
Filters can also be created from here. Right-click on one of any details. From the menu select Apply as Filter drop-down menu so filter based on it can be created.



Display filter command –

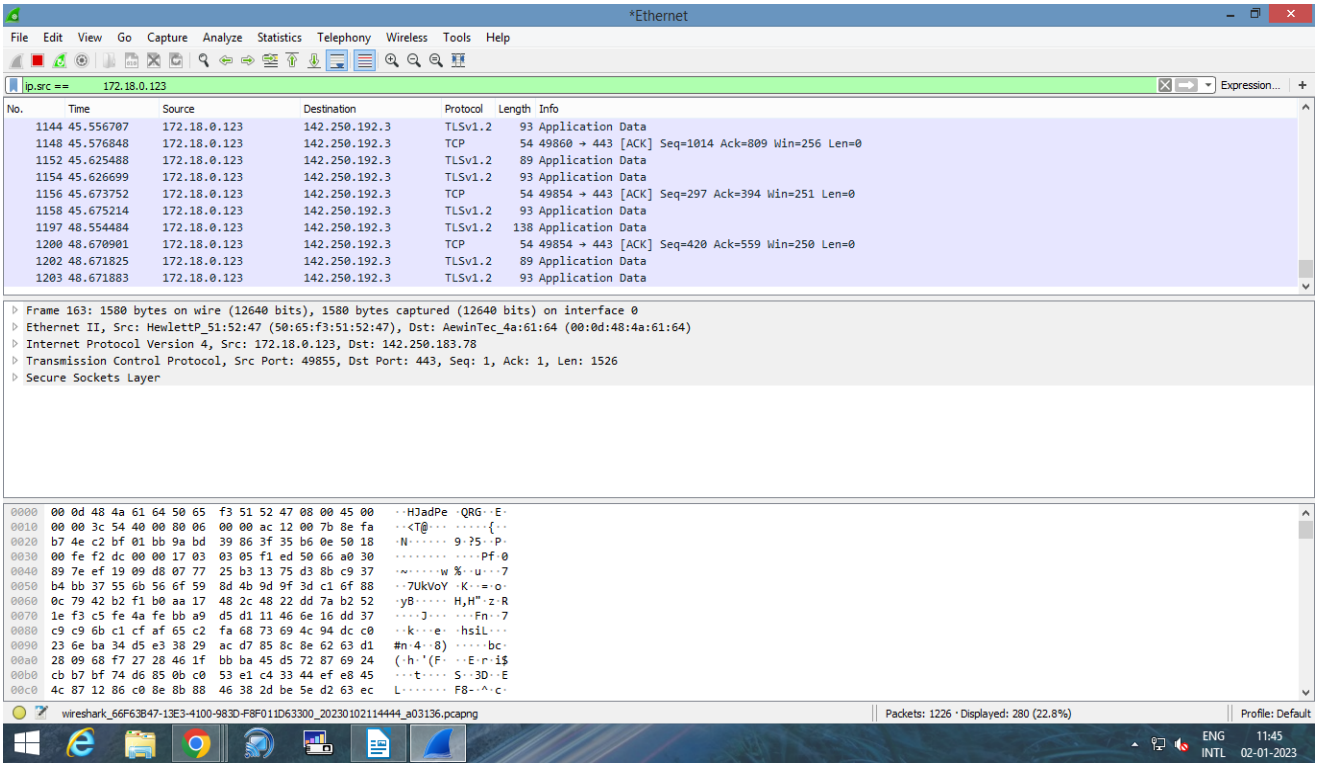
1. Display packets based on specific IP-address

ip.addr == 172.18.0.4



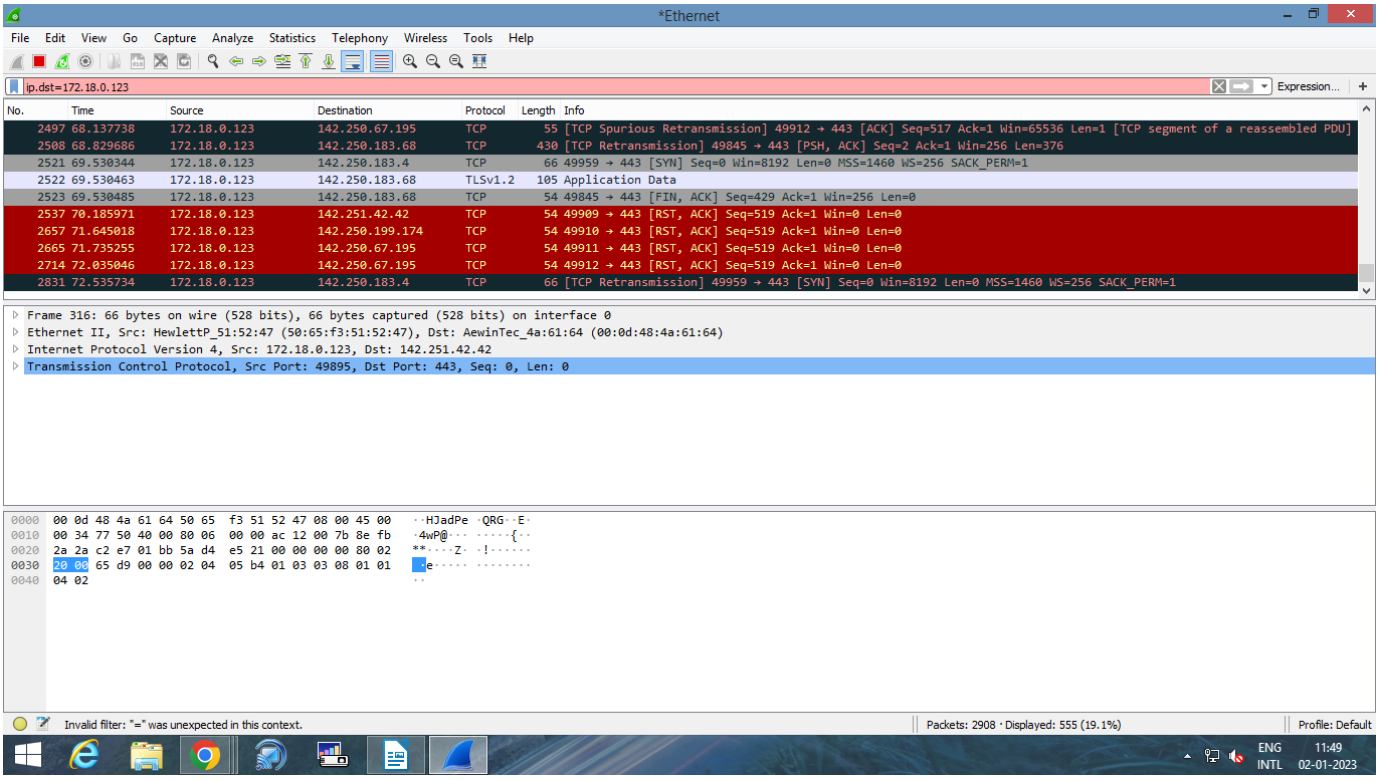
2. Display packets which are coming from specific IP-address

ip.src == 172.18.123



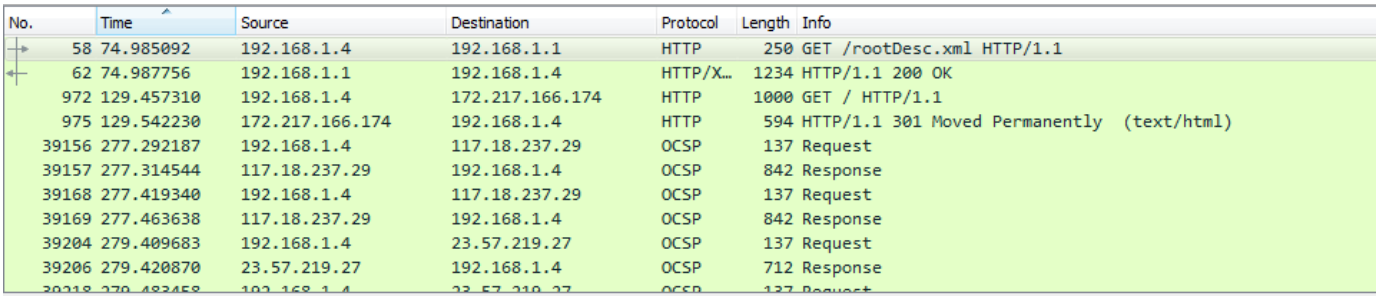
3. Display packets which are having specific IP-address destination

ip.dst == 172.18.0.123



4. Display packets which are using http protocol

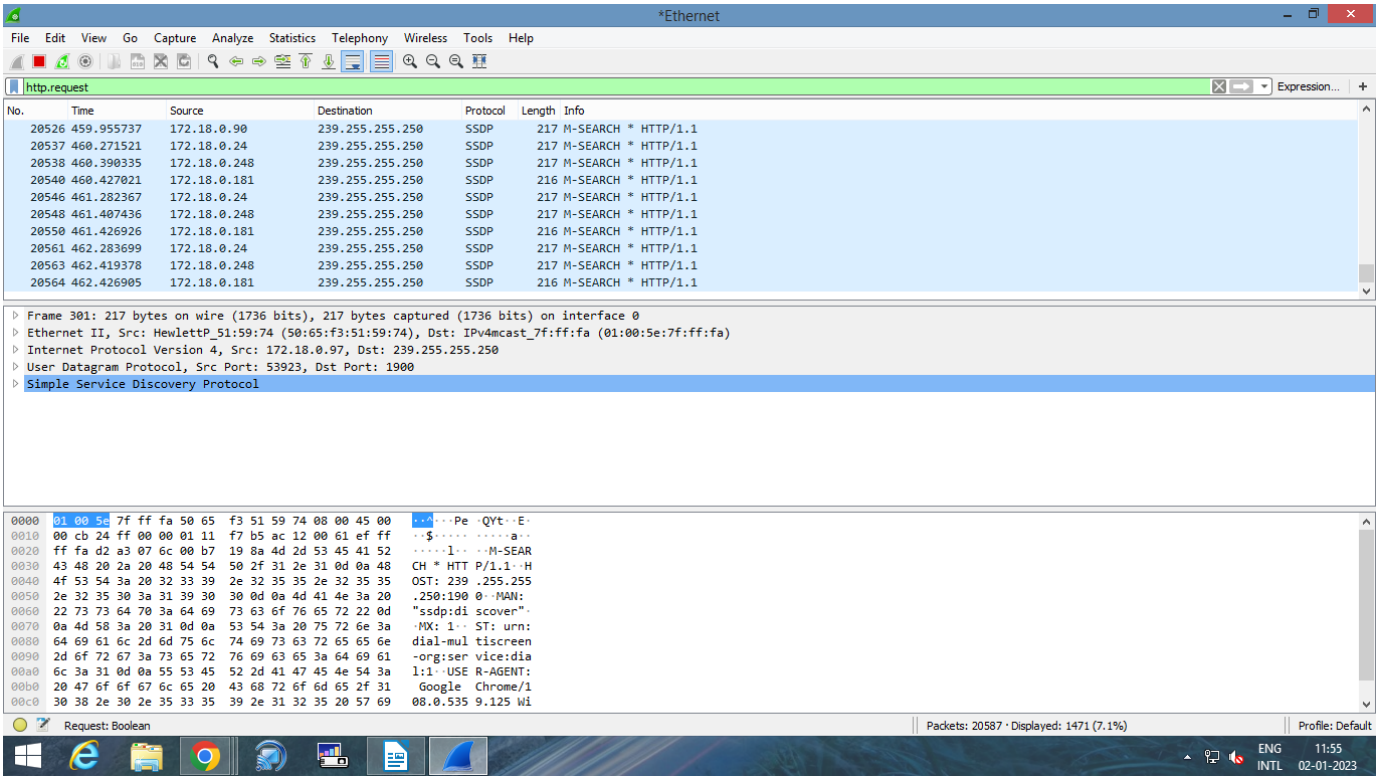
http



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

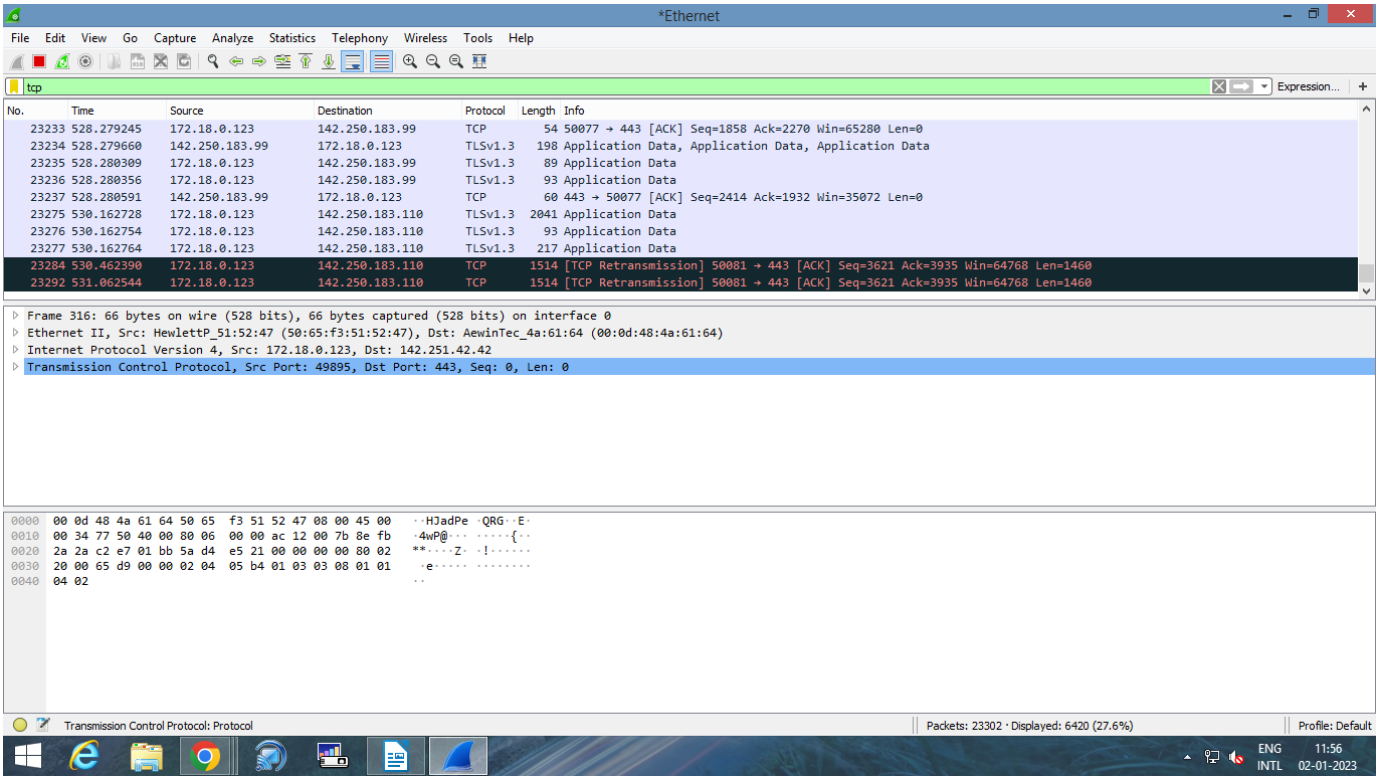
5. Display packets which are using http request

http.request



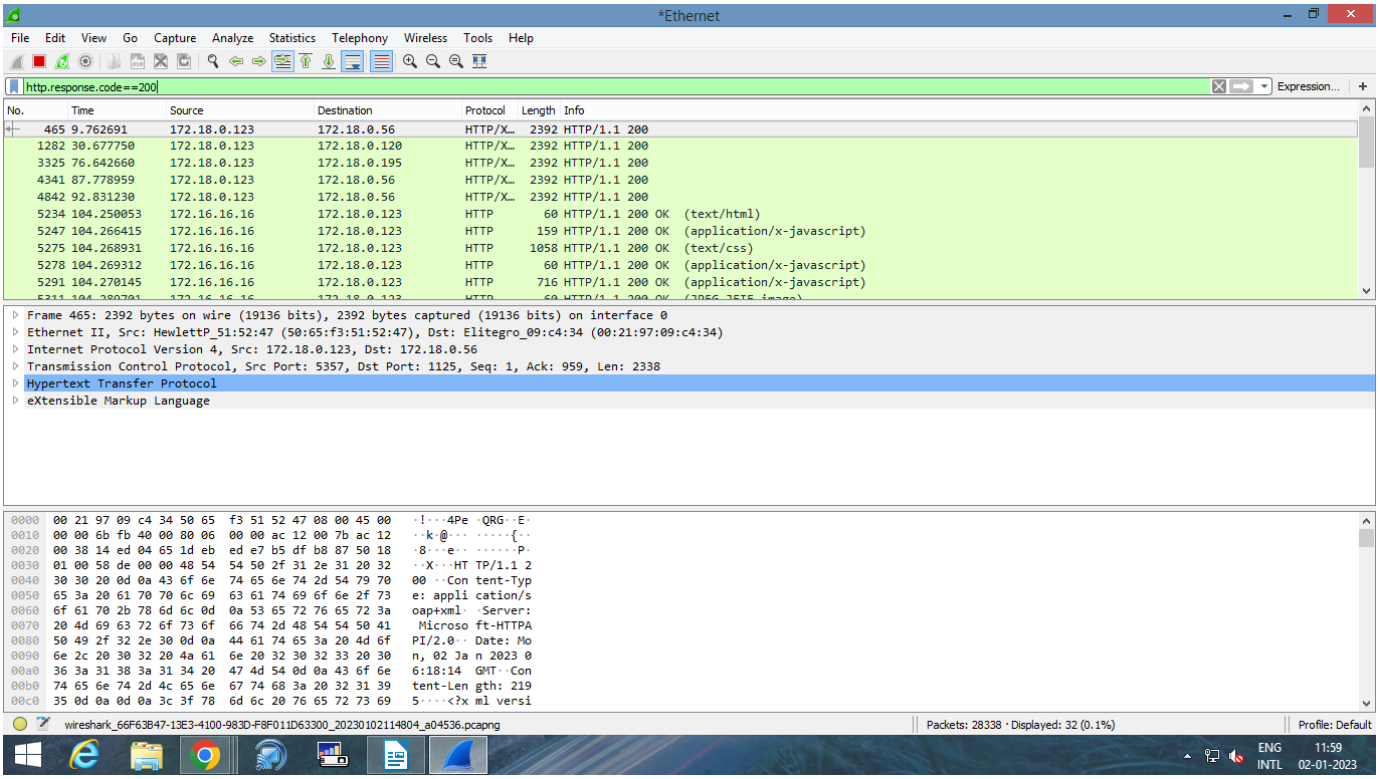
6. Display packets which are using TCP protocol

tcp



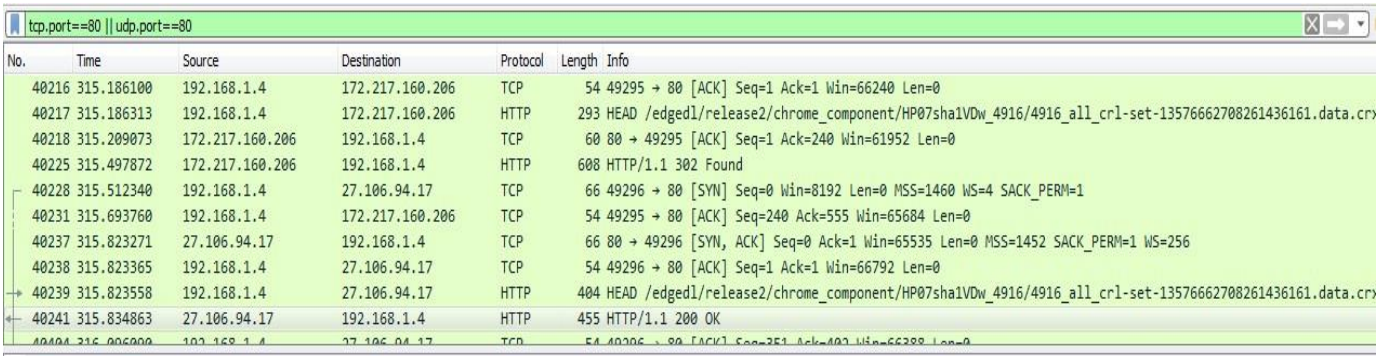
7. Display packets having no error connecting to server

http.response.code==200



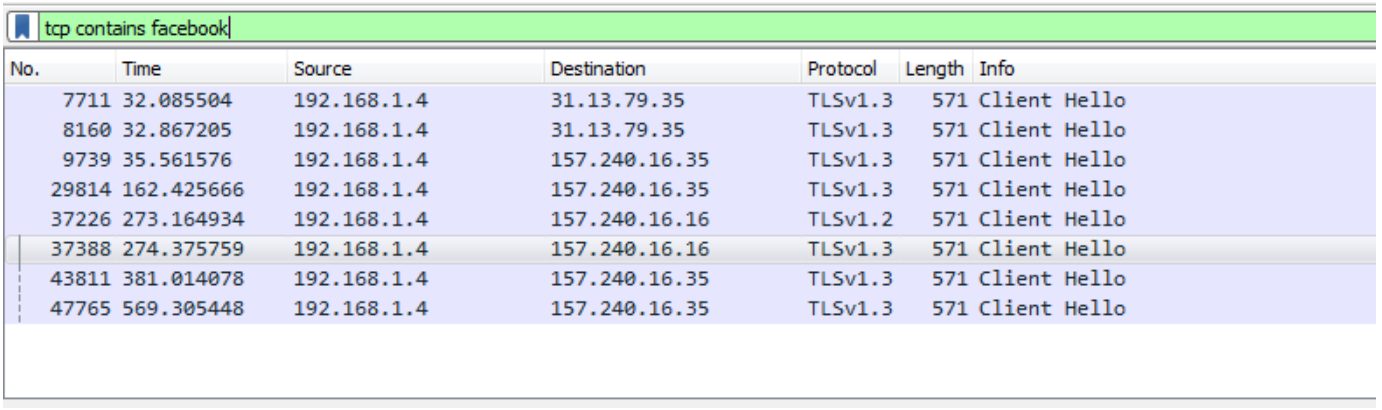
8. Display packets having port number 80

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



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

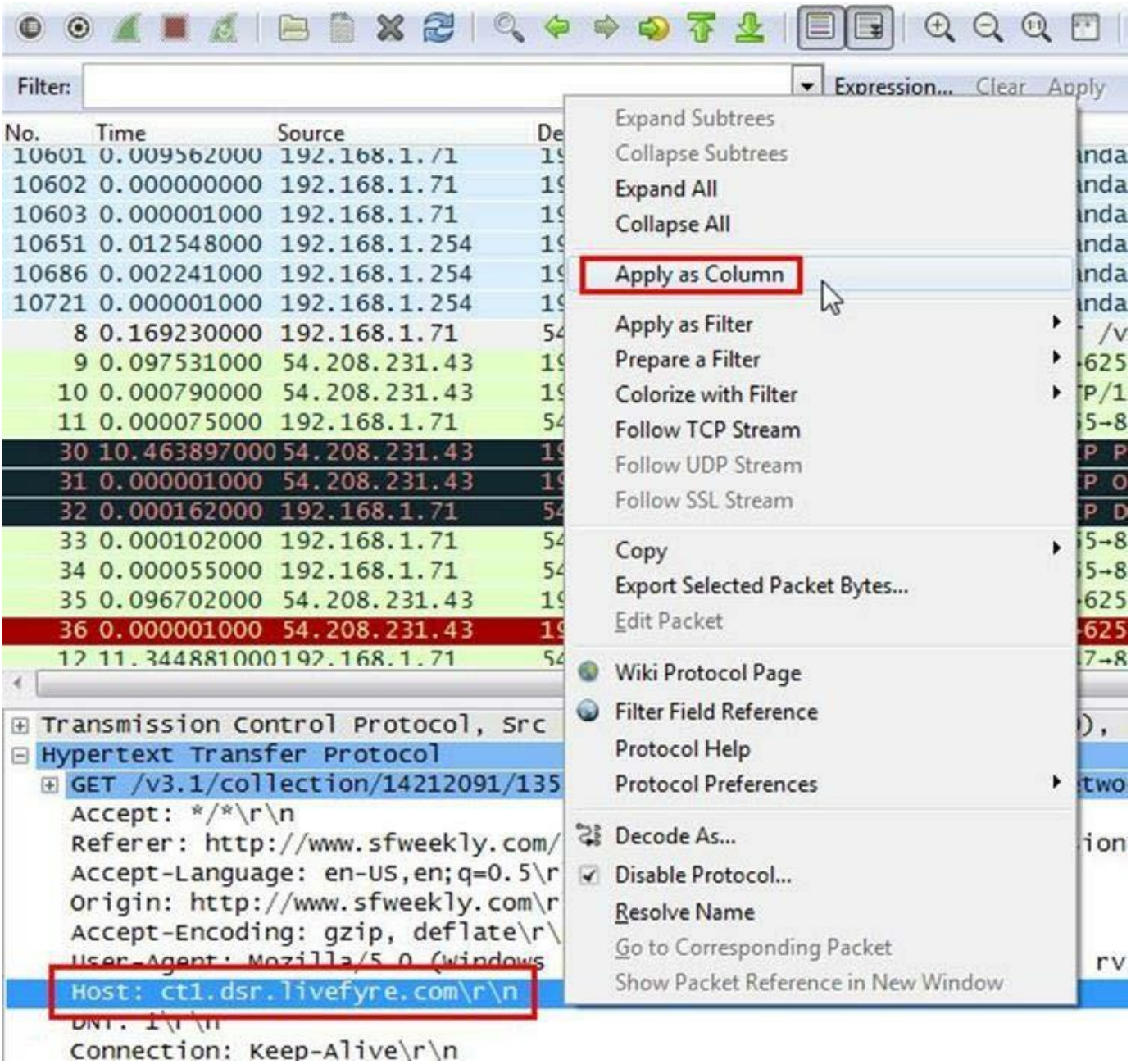
Practical No – 5

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

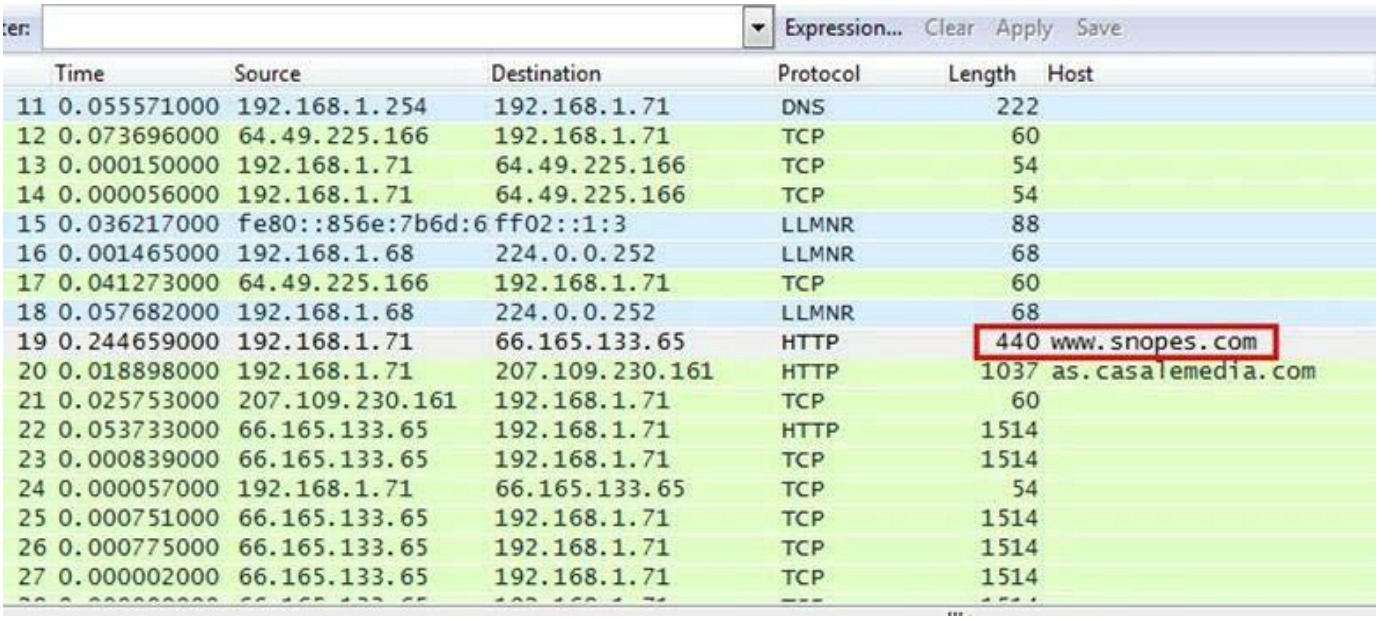
Steps:

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

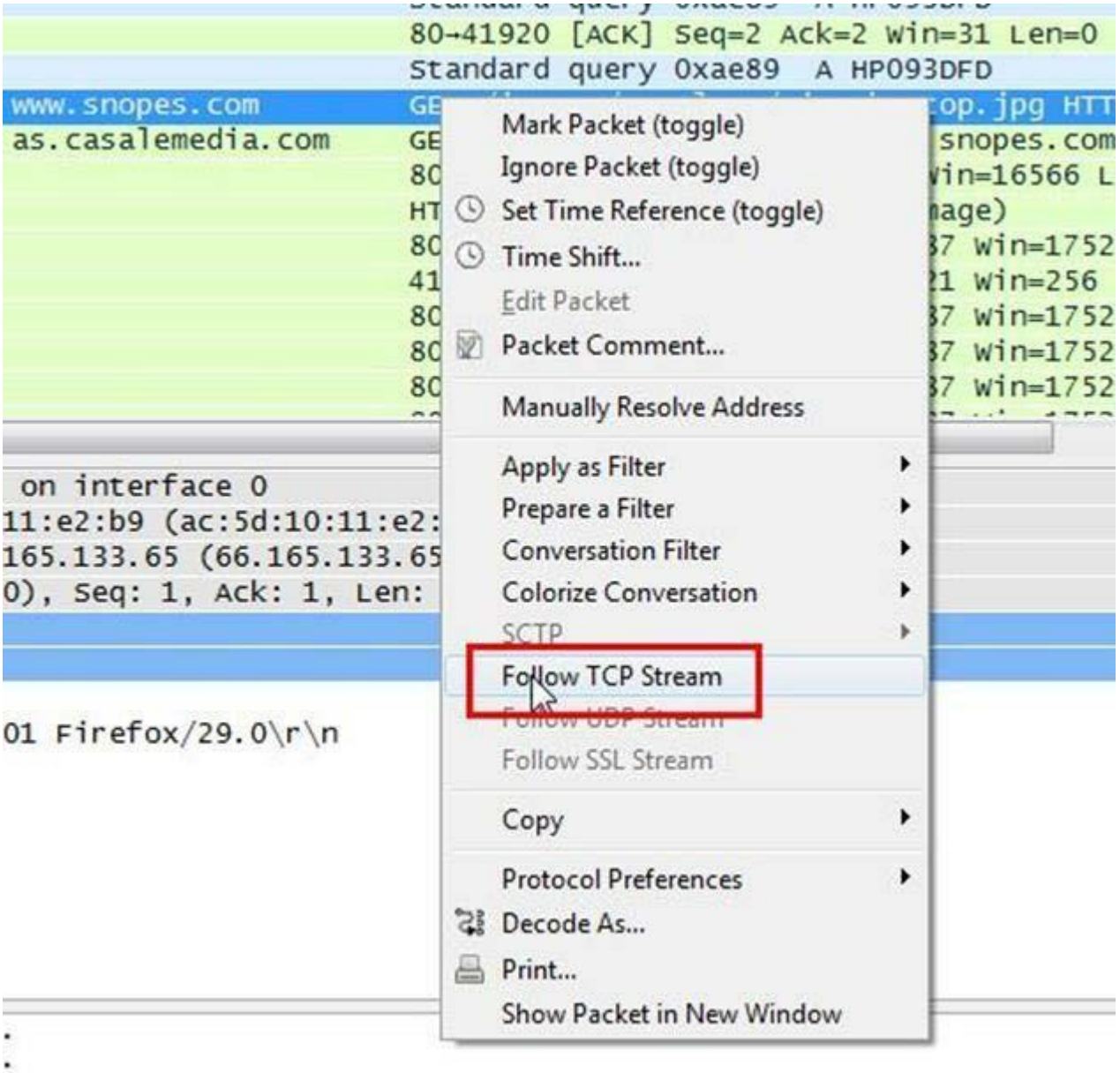
Analysis – The domain name be found from host header so we will set host header column where we will see all domain name. Select any HTTP request and expand the Hypertext Transfer Protocol then right click on Host header and then Apply as Column.



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



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

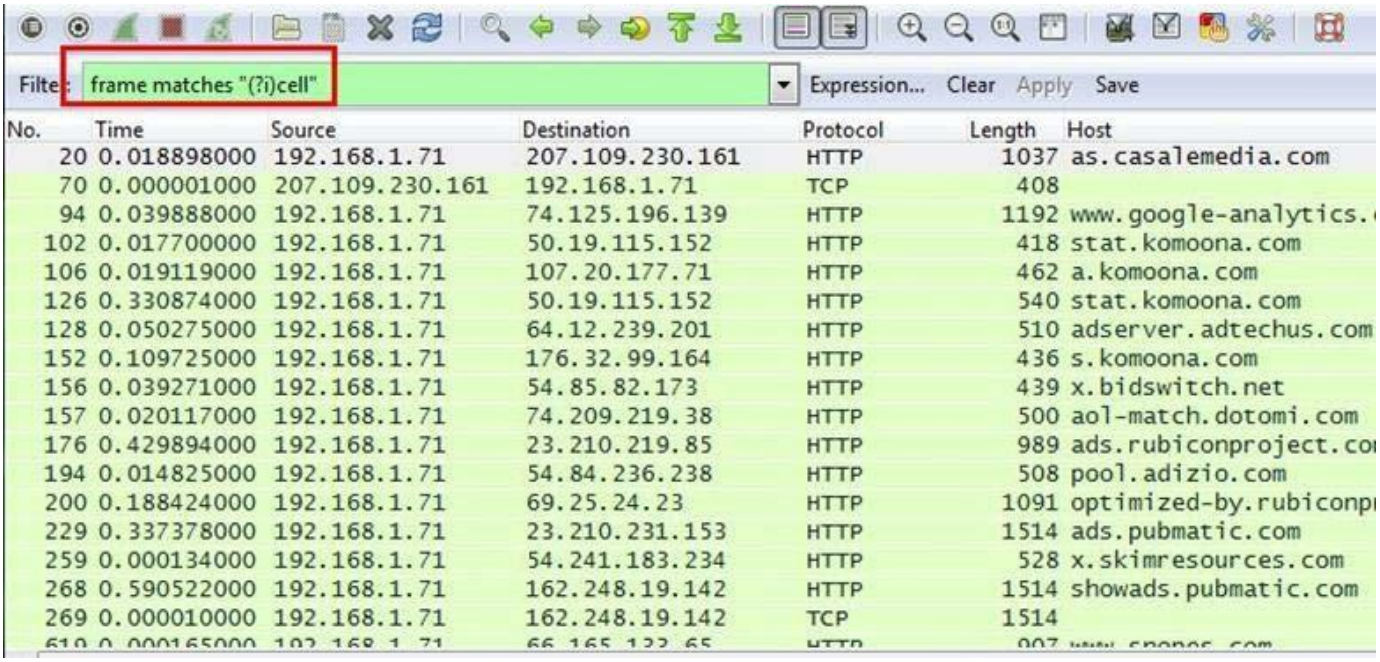


Now we can see the webserver name in server header it is Microsoft IIS 5.0

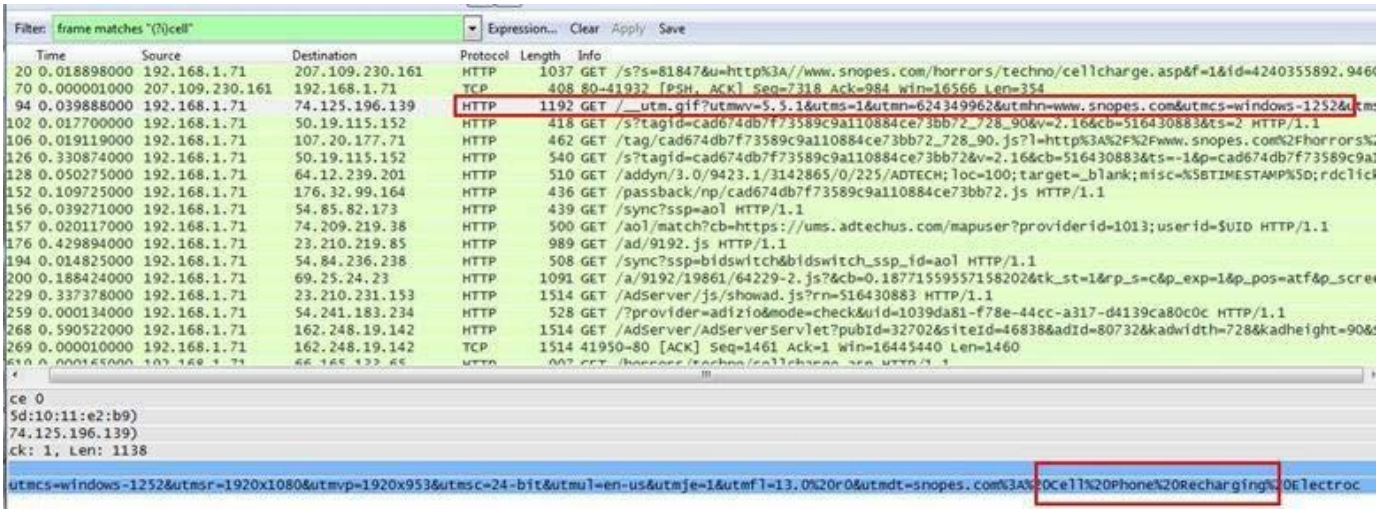
2.

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” or frame matches cell



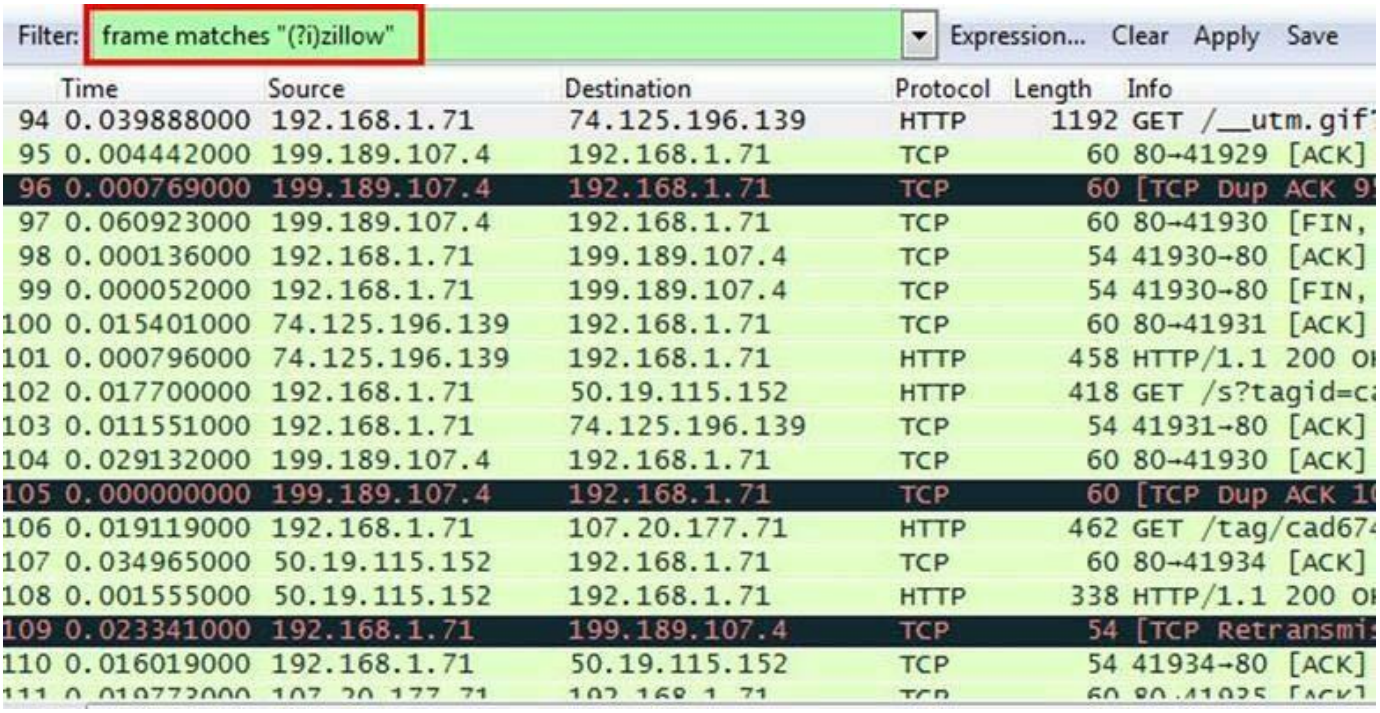
After applying the filter now, we will start to check every HTTP request. We noticed in the first HTTP request cell keyword is in URL and it was about cell phone charging issue.



3.

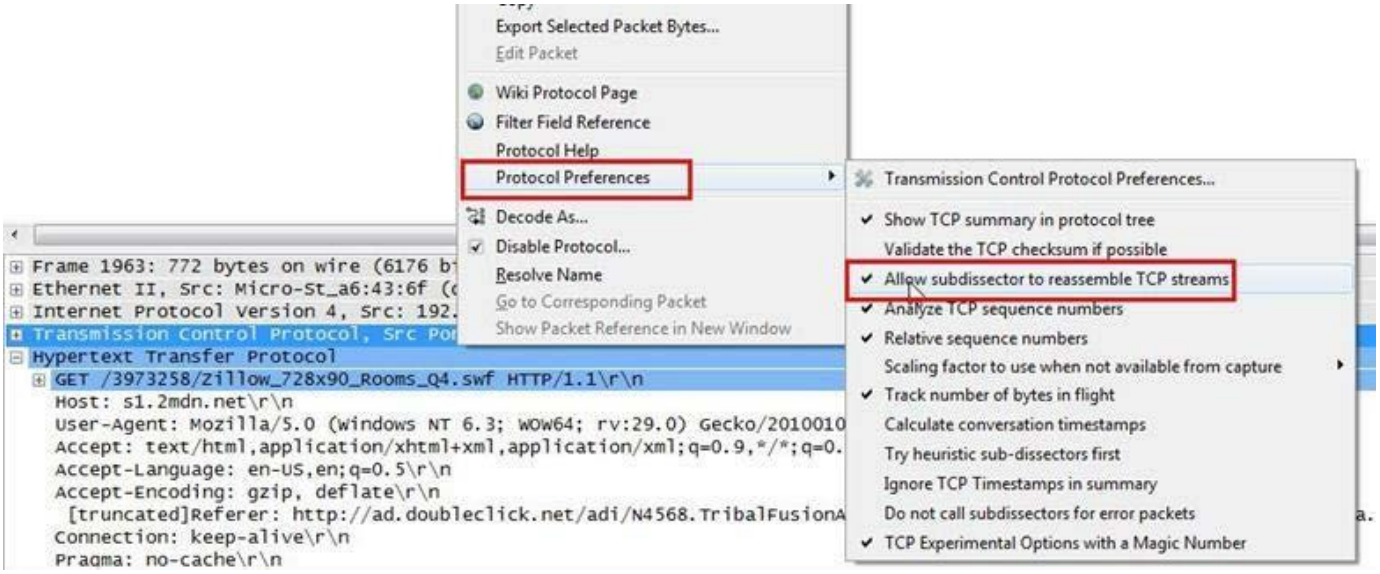
According to Zillow, what instrument will Ryan learn to play?

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

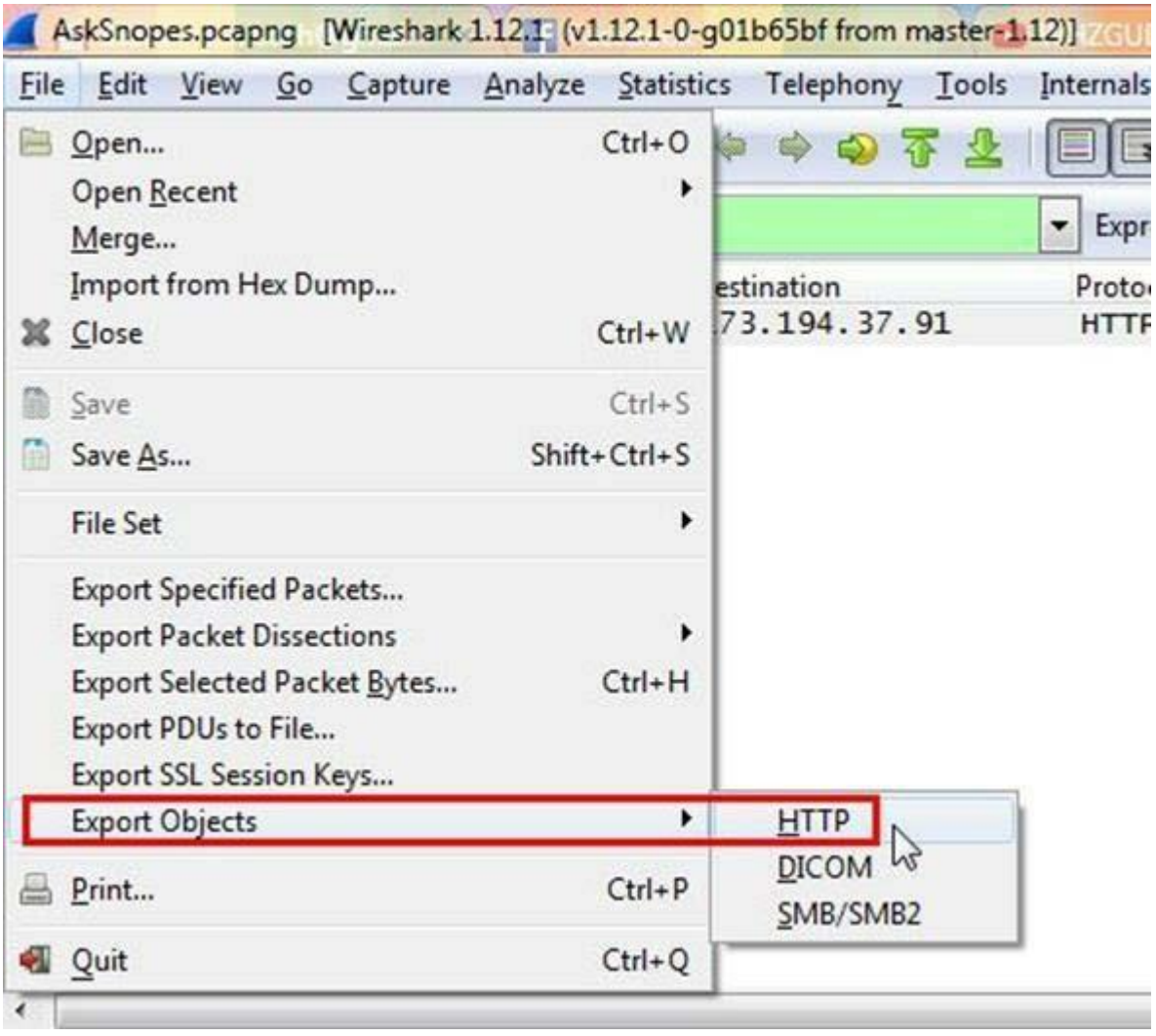


After applying the filter, we found only one packet with the Zillow keyword

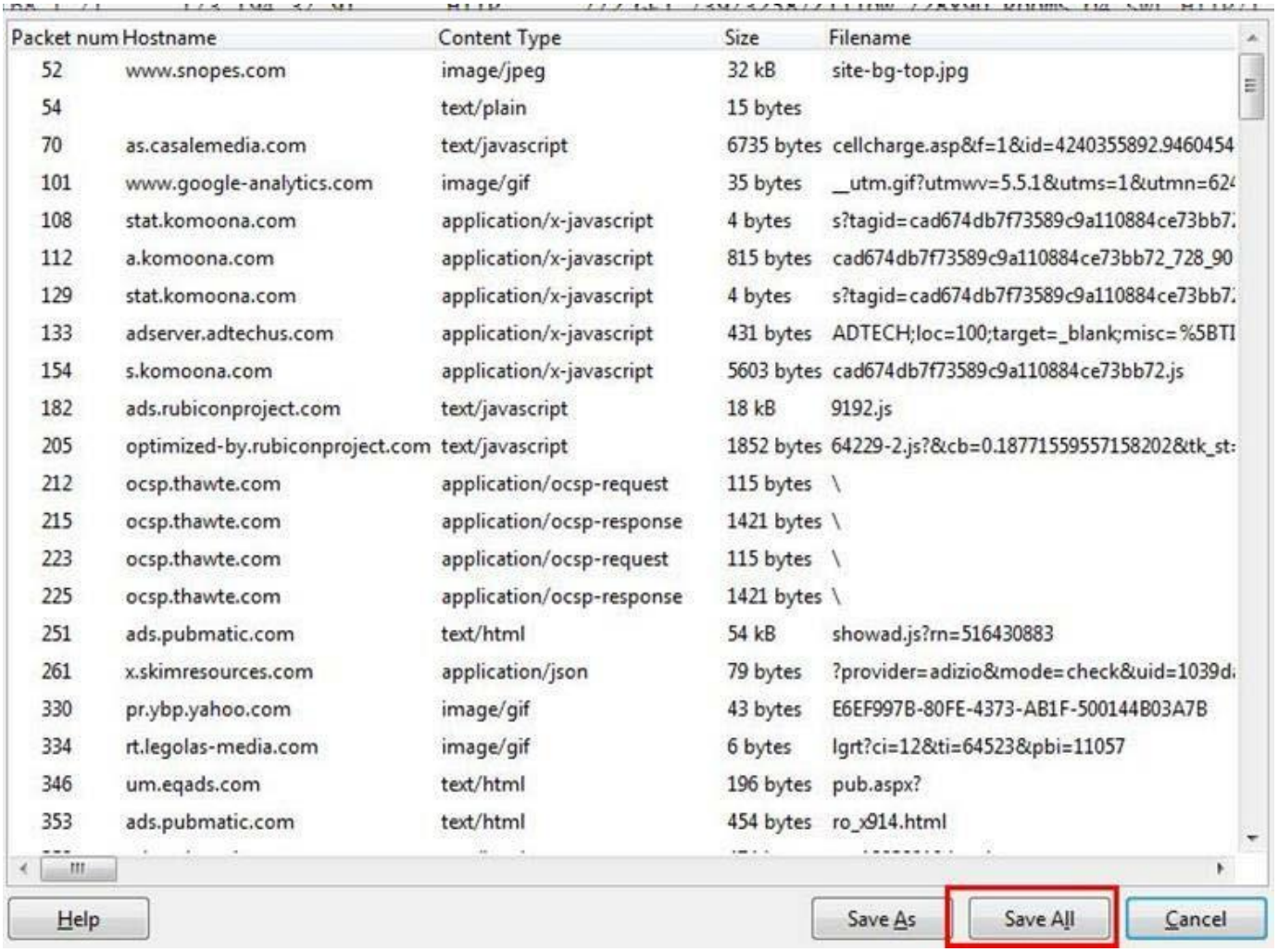
Select the packet and expand the Hypertext Transfer Protocol tab right click on it go to Protocol Preferences and check Allow subdissector to resemble TCP stream.



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



Click on save all.



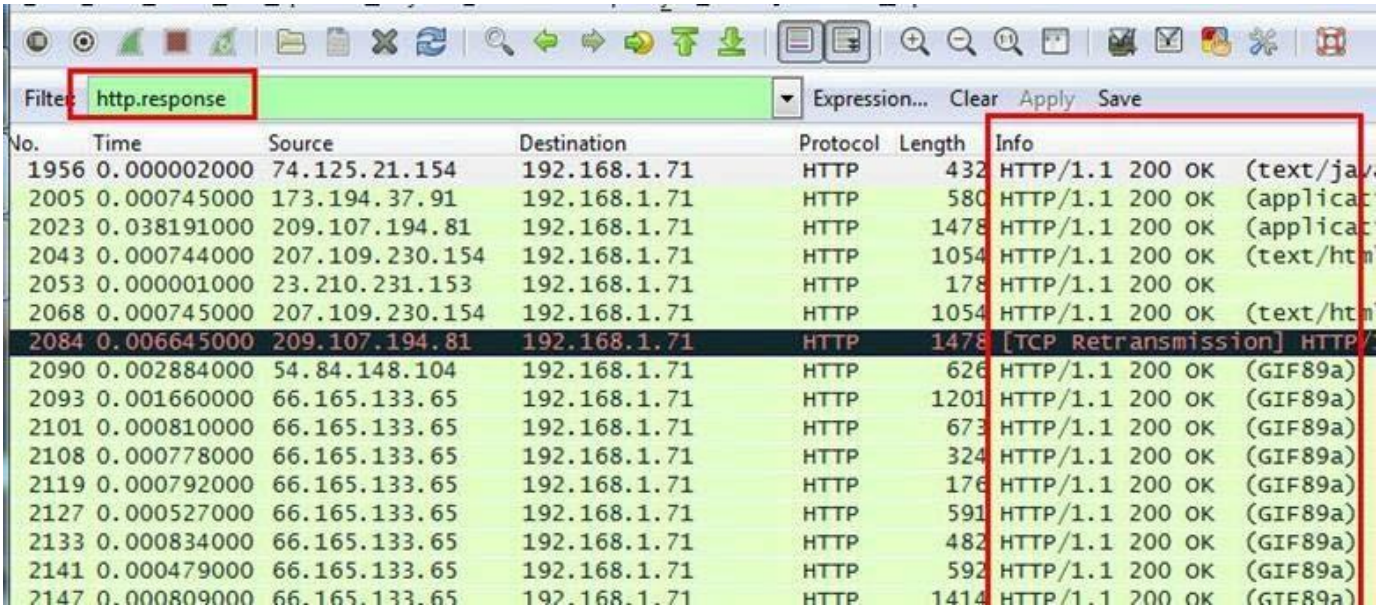
Packet num	Hostname	Content Type	Size	Filename
52	www.snopes.com	image/jpeg	32 kB	site-bg-top.jpg
54		text/plain	15 bytes	
70	as.casalemedia.com	text/javascript	6735 bytes	cellcharge.asp&f=1&id=4240355892.9460454
101	www.google-analytics.com	image/gif	35 bytes	__utm.gif?utmwv=5.5.1&utms=1&utmn=62
108	stat.komoona.com	application/x-javascript	4 bytes	s?tagid=cad674db7f73589c9a110884ce73bb7
112	a.komoona.com	application/x-javascript	815 bytes	cad674db7f73589c9a110884ce73bb72_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	cad674db7f73589c9a110884ce73bb72.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

Help Save As Save All Cancel

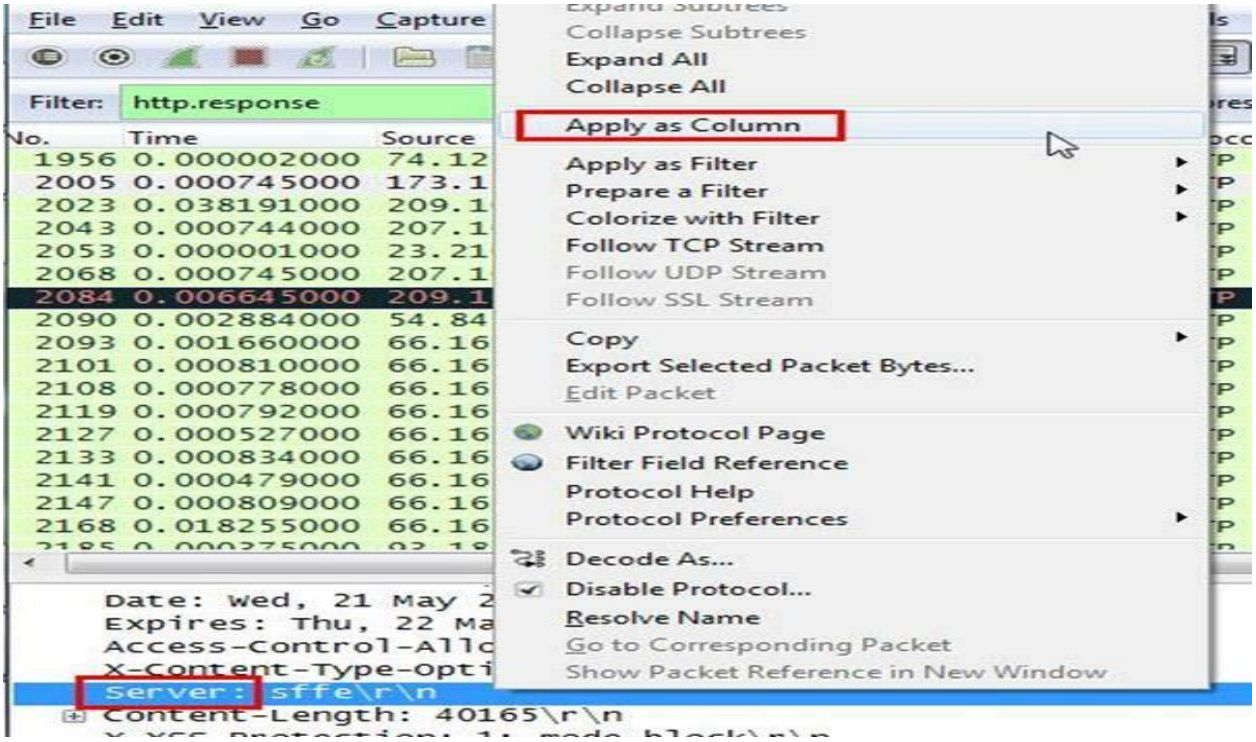
4.

How many web servers are running Apache?

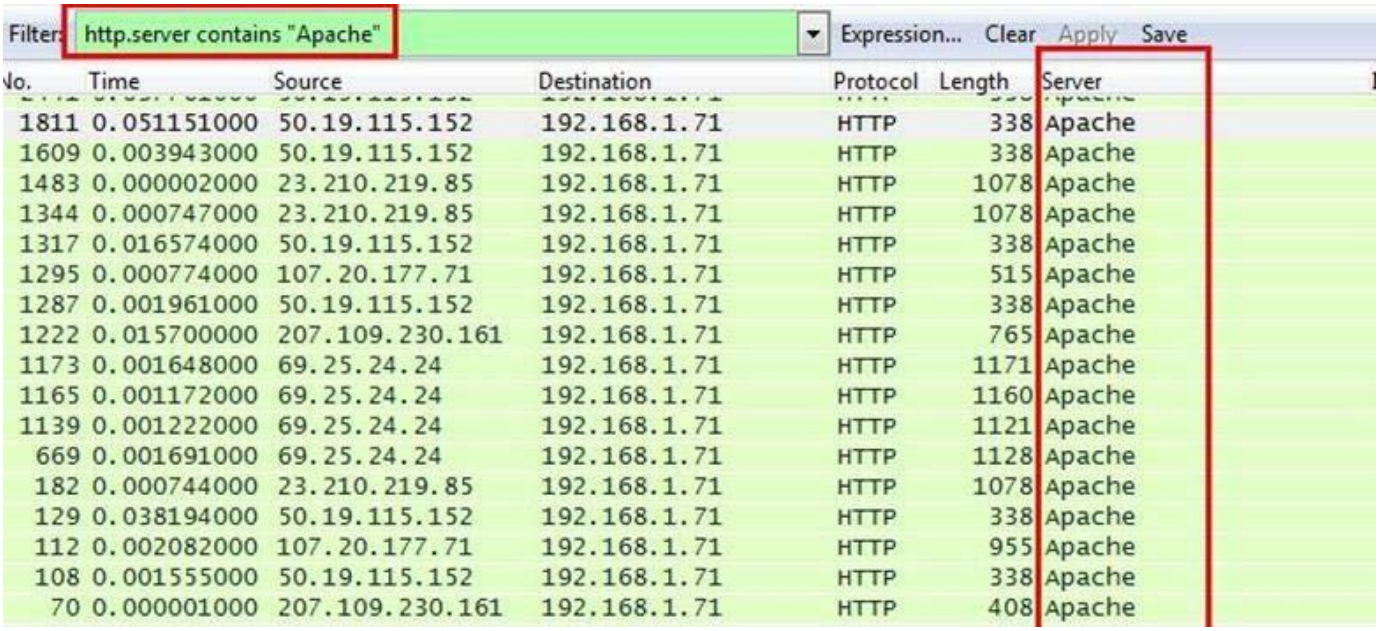
Analysis – The web server name can be retrieved from HTTP response header. So will apply filter http. response and we can see all http response packets.



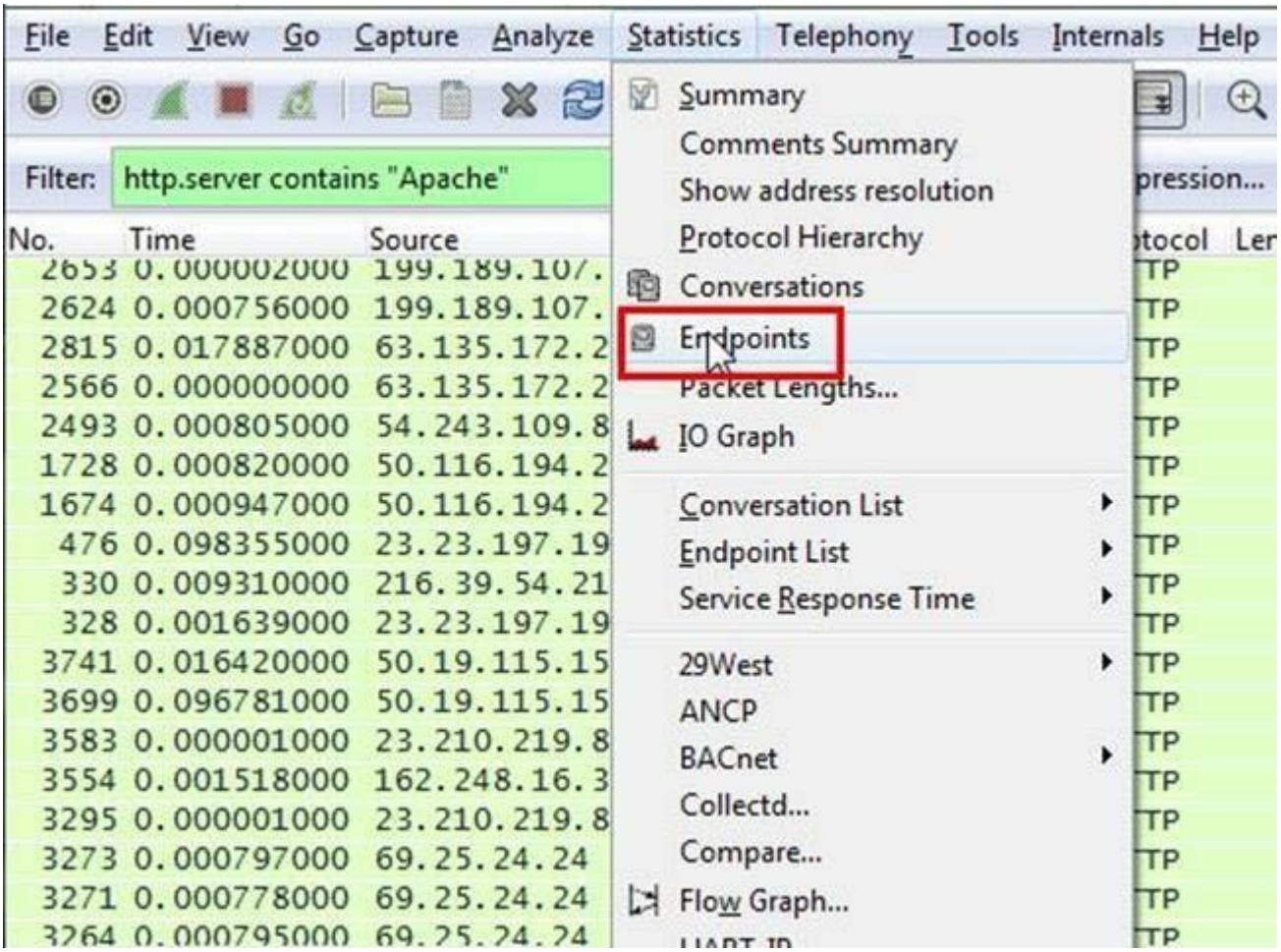
Now we will set the server header as column select any packet and right click on it then select Apply as Column.



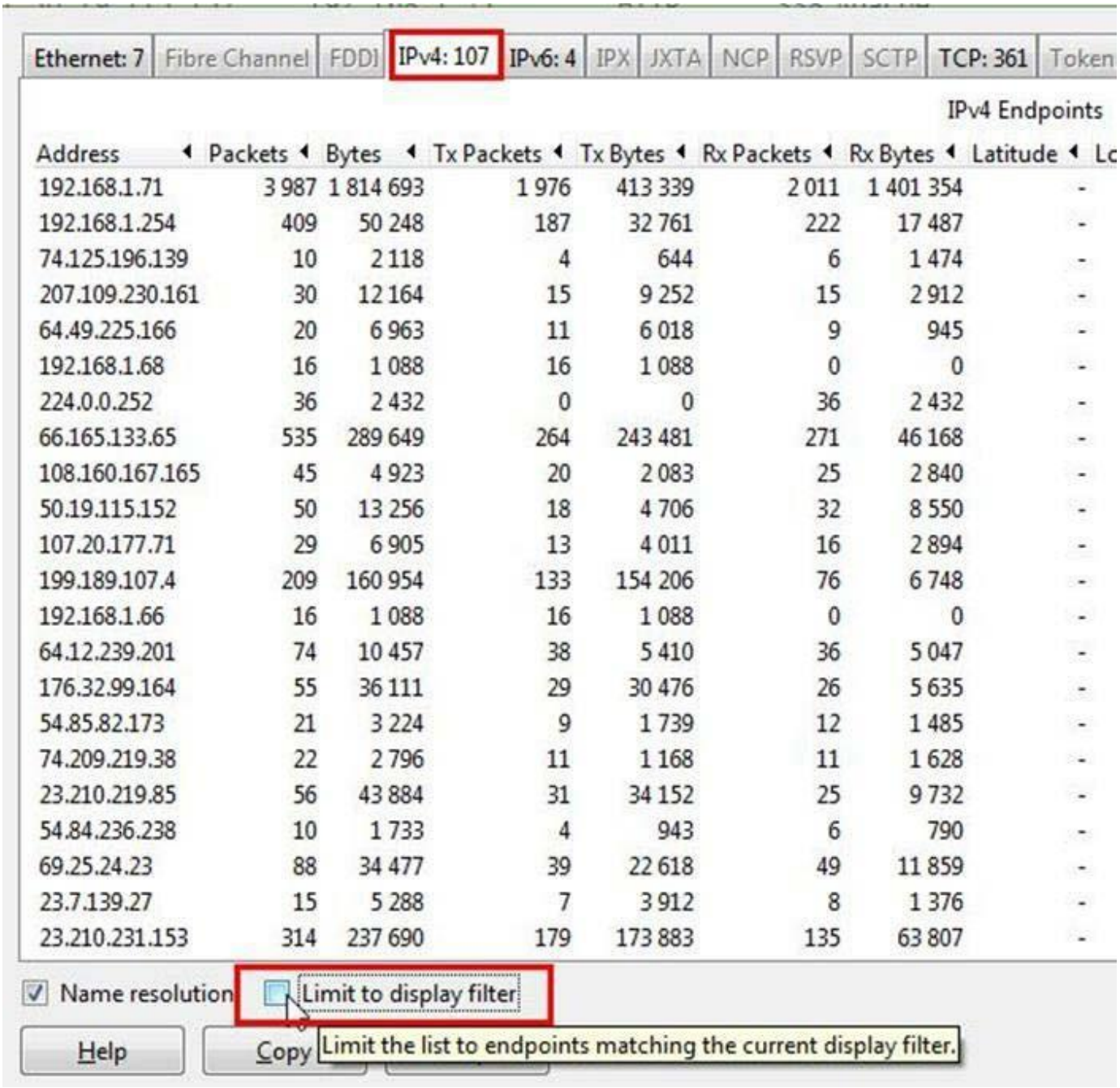
now we have to check how many Apache packets are there we can't count manually for each packet so we will apply another filter http.server contains "Apache"



After applying filter go to Statistics > Endpoints

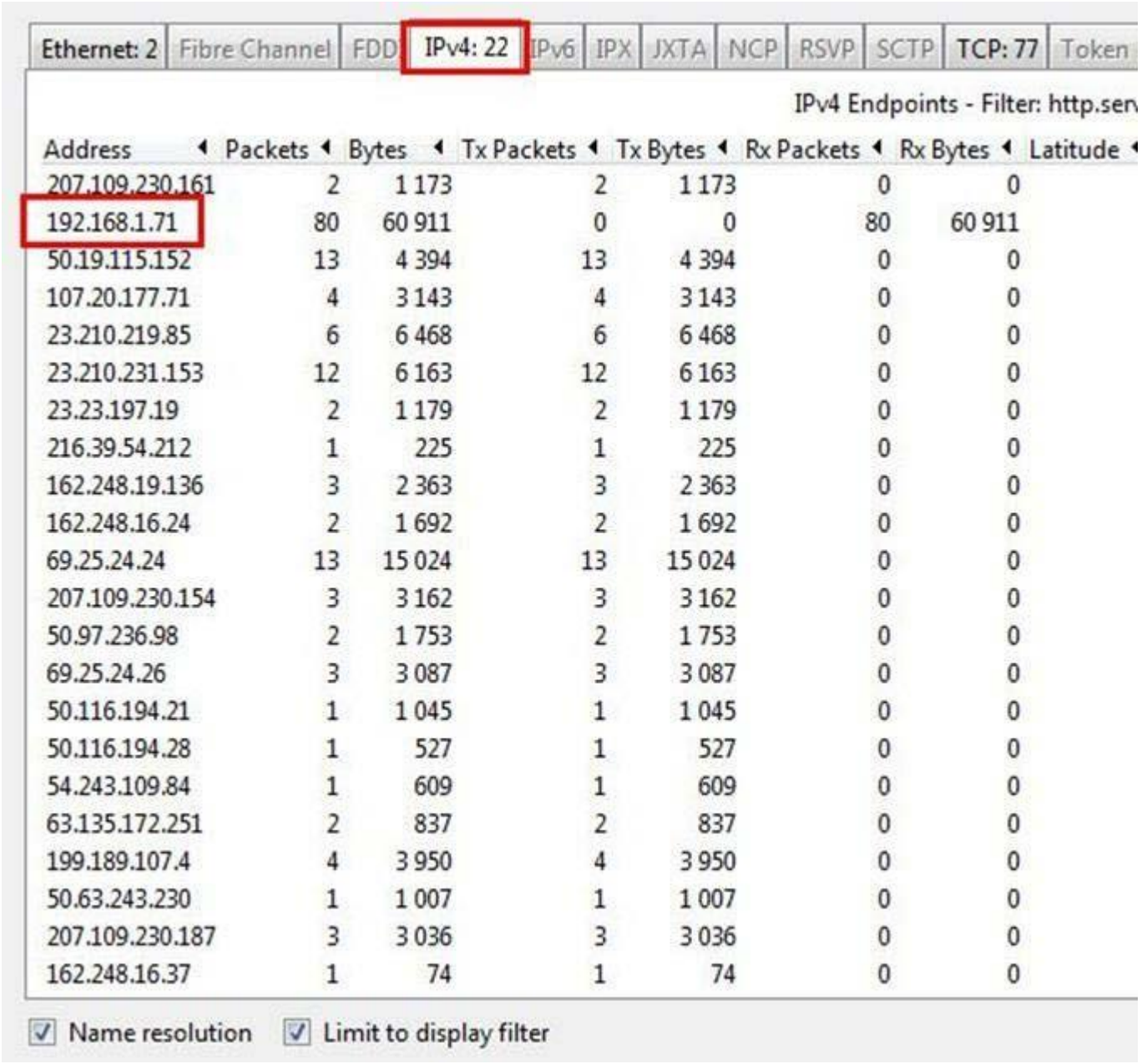


It will show all connections



Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Latitude	Lo
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.



Ethernet: 2 | Fibre Channel | FDD | IPv4: 22 | IPv6 | IPX | JXTA | NCP | RSVP | SCTP | TCP: 77 | Token

IPv4 Endpoints - Filter: http.ser

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Latitude
207.109.230.161	2	1 173	2	1 173	0	0	
192.168.1.71	80	60 911	0	0	80	60 911	
50.19.115.152	13	4 394	13	4 394	0	0	
107.20.177.71	4	3 143	4	3 143	0	0	
23.210.219.85	6	6 468	6	6 468	0	0	
23.210.231.153	12	6 163	12	6 163	0	0	
23.23.197.19	2	1 179	2	1 179	0	0	
216.39.54.212	1	225	1	225	0	0	
162.248.19.136	3	2 363	3	2 363	0	0	
162.248.16.24	2	1 692	2	1 692	0	0	
69.25.24.24	13	15 024	13	15 024	0	0	
207.109.230.154	3	3 162	3	3 162	0	0	
50.97.236.98	2	1 753	2	1 753	0	0	
69.25.24.26	3	3 087	3	3 087	0	0	
50.116.194.21	1	1 045	1	1 045	0	0	
50.116.194.28	1	527	1	527	0	0	
54.243.109.84	1	609	1	609	0	0	
63.135.172.251	2	837	2	837	0	0	
199.189.107.4	4	3 950	4	3 950	0	0	
50.63.243.230	1	1 007	1	1 007	0	0	
207.109.230.187	3	3 036	3	3 036	0	0	
162.248.16.37	1	74	1	74	0	0	

☑ Name resolution ☑ Limit to display filter

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

Practical No – 6

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

-Check Sysinternals tools

-Monitor Live Processes

-Capture RAM-Capture

-TCP/UDP packets

-Monitor Hard Disk

-Monitor Virtual Memory

-Monitor Cache Memory

Steps:

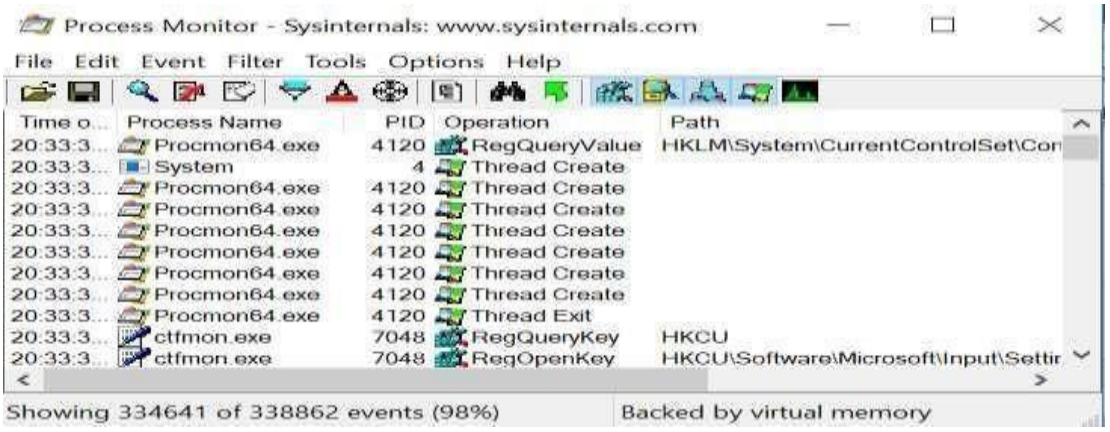
1) Check Sysinternals tools

Windows Sysinternals tools are utilities to manage, diagnose, troubleshoot, and monitor a Microsoft Windows environment

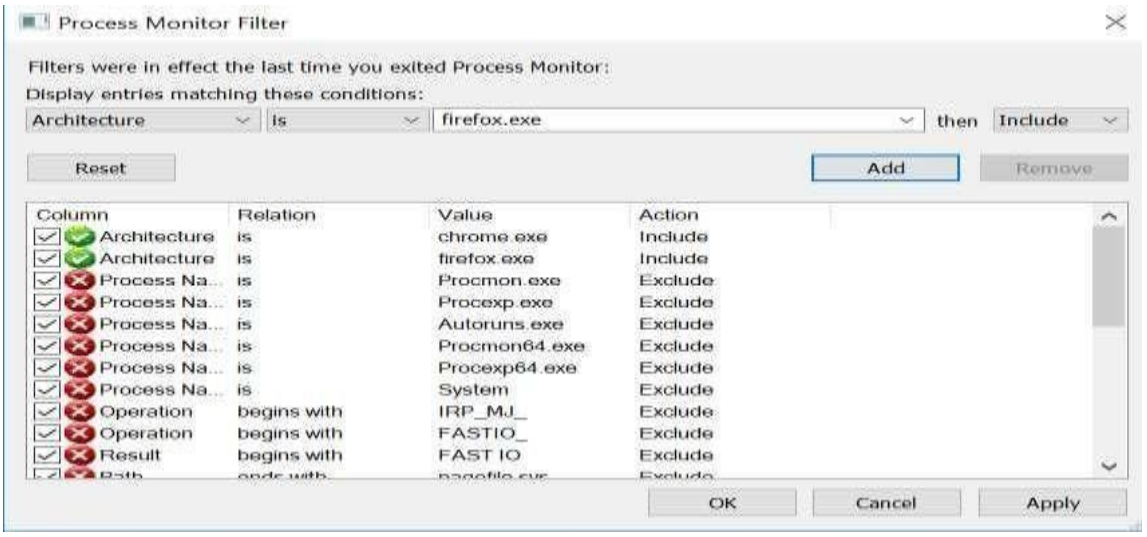
The following are the categories of Sysinternals Tools:

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

2) Monitor Live Processes (Tool: ProcMon)

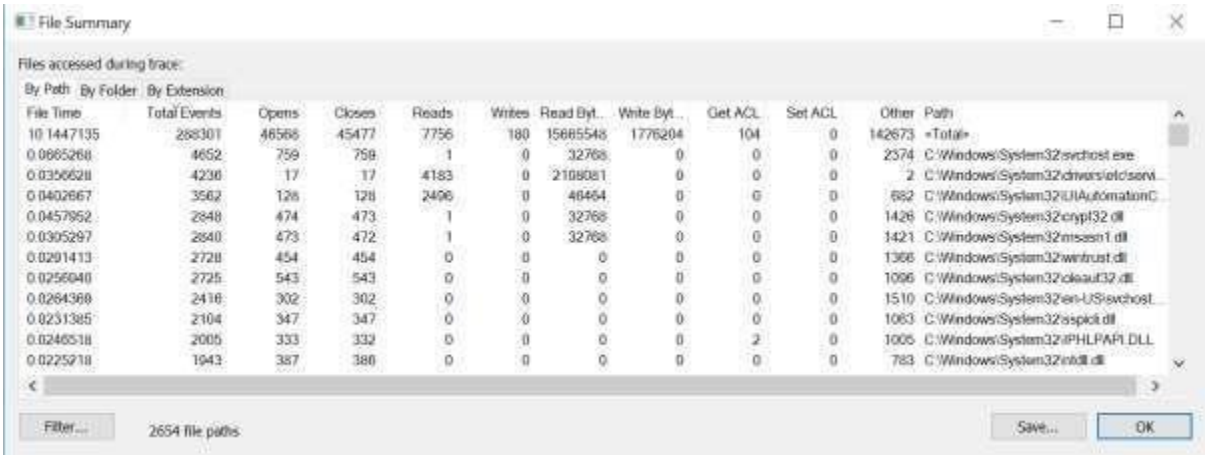


Click on filter > Process monitor filter



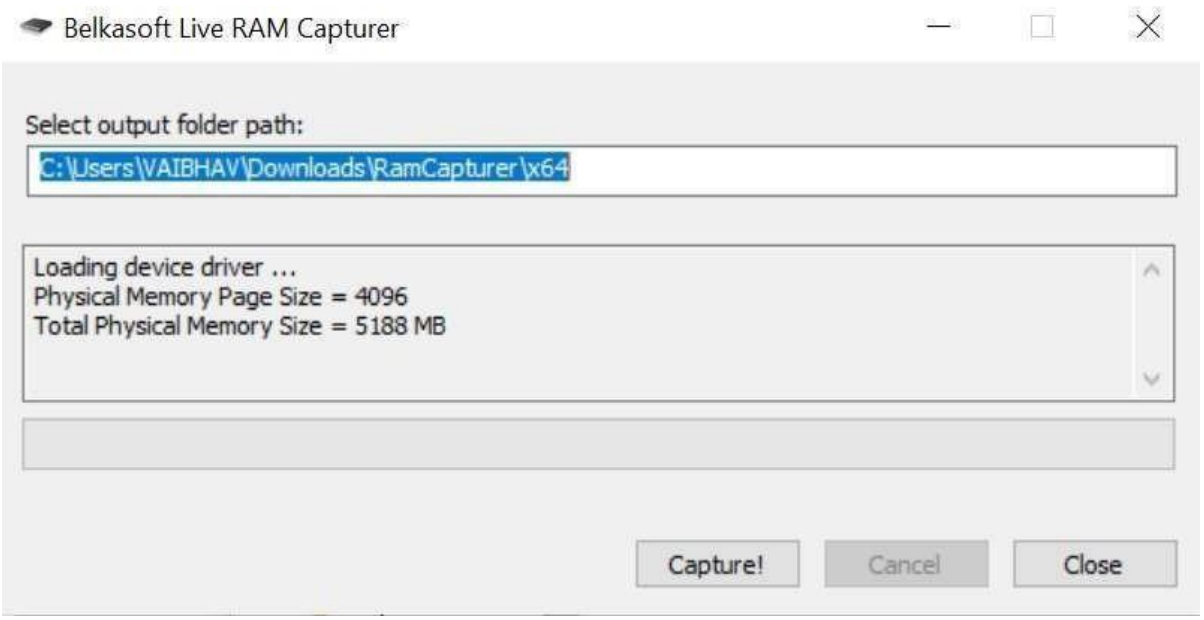
Click on tools > Process tree

Click on filter > File summary

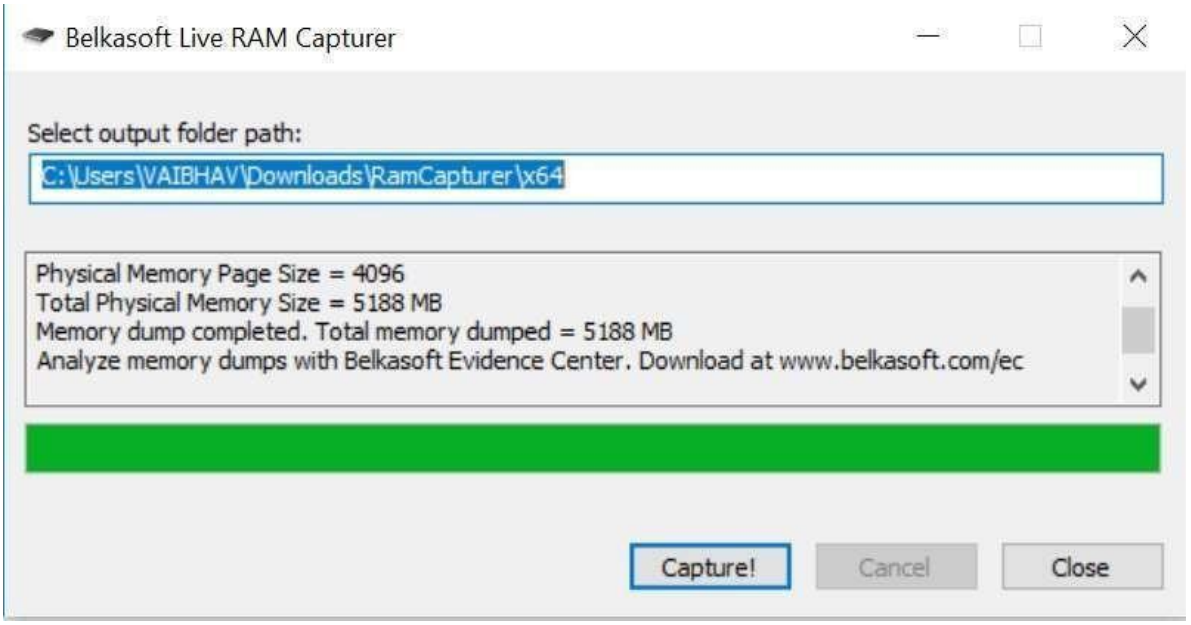


3) Capture RAM (Tool: RAMCapture)

Open the Ramcapture tool.

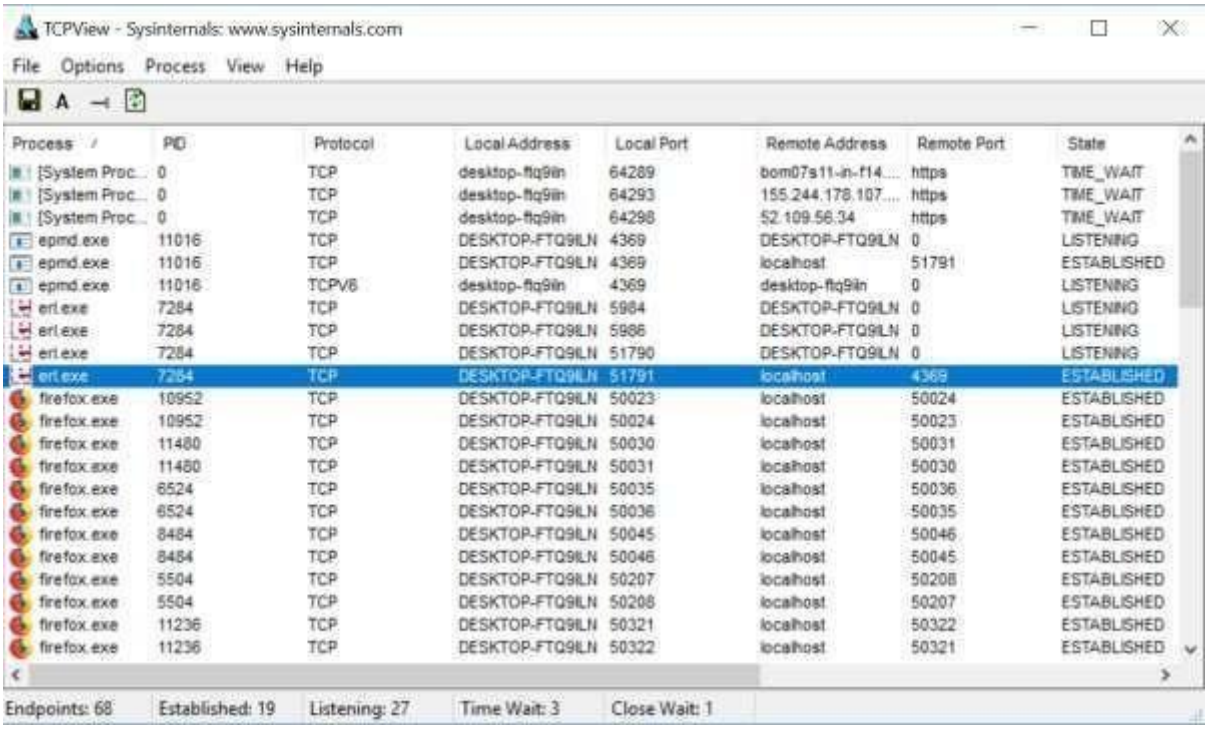


Click on capture.

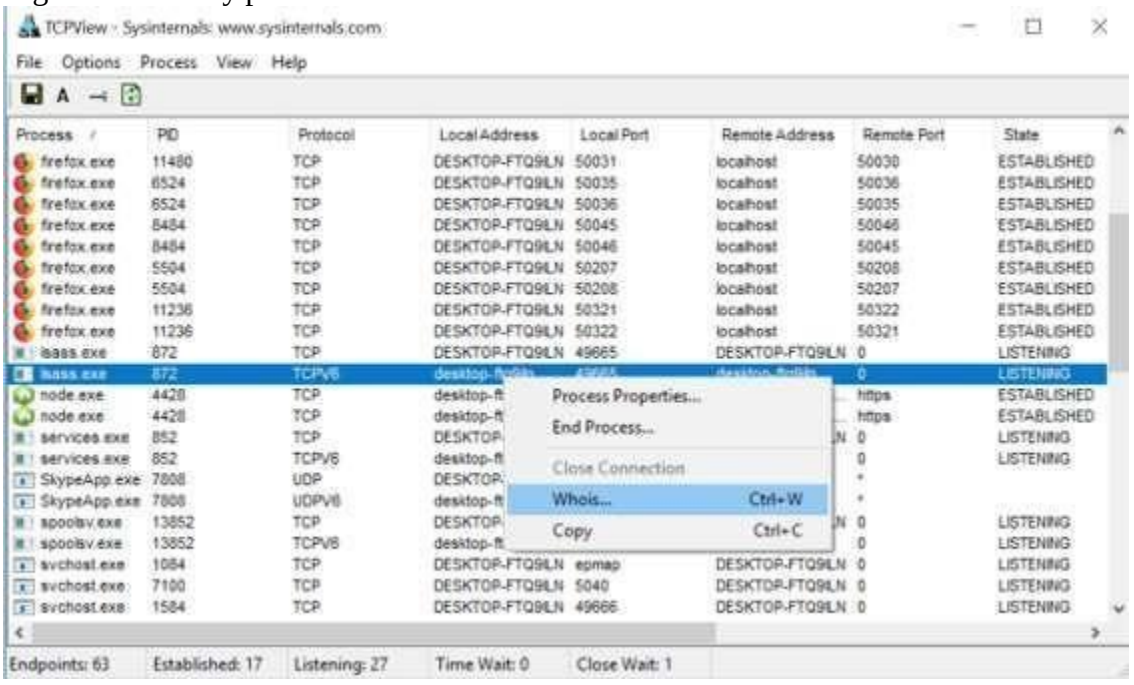


4) Capture TCP/UDP packets (Tool:

TcpView) Open the Tcpview tool.

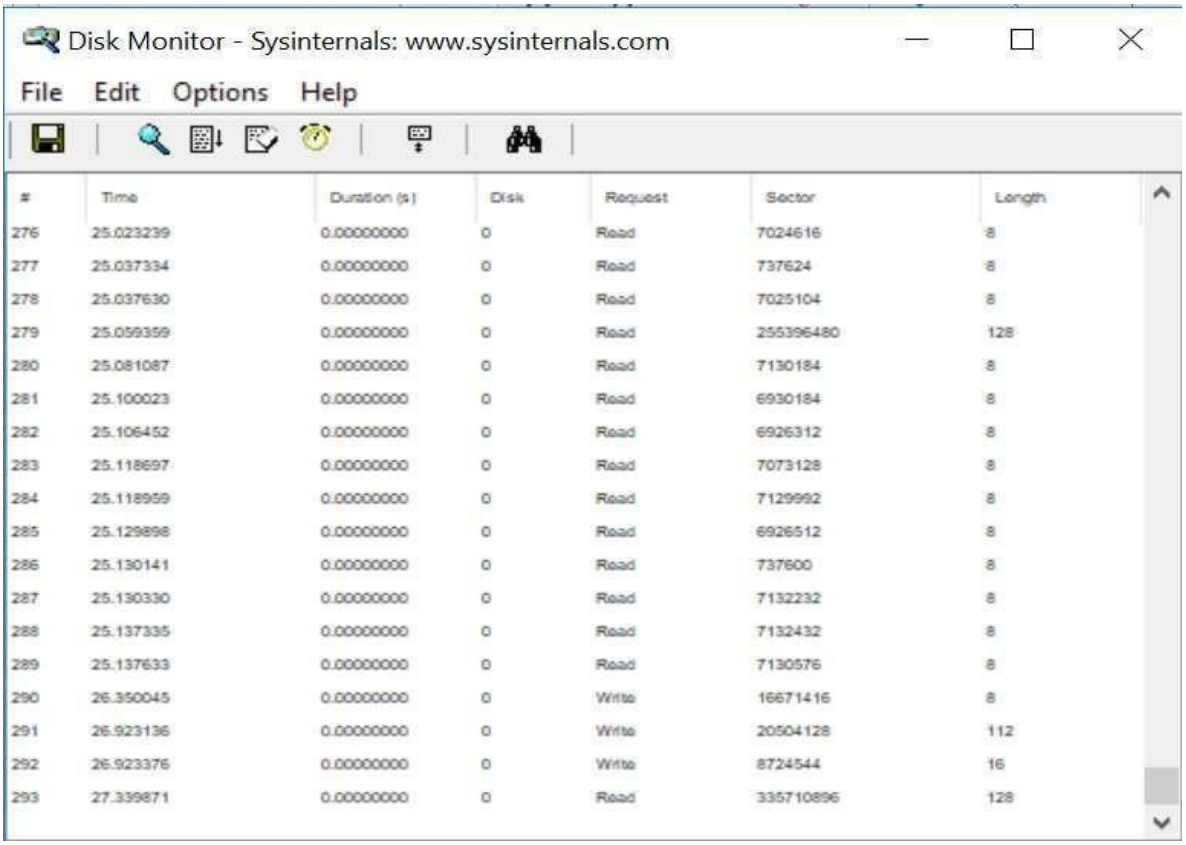


Right click on any packet > whois



5) Monitor Hard Disk (Tool: DiskMon)

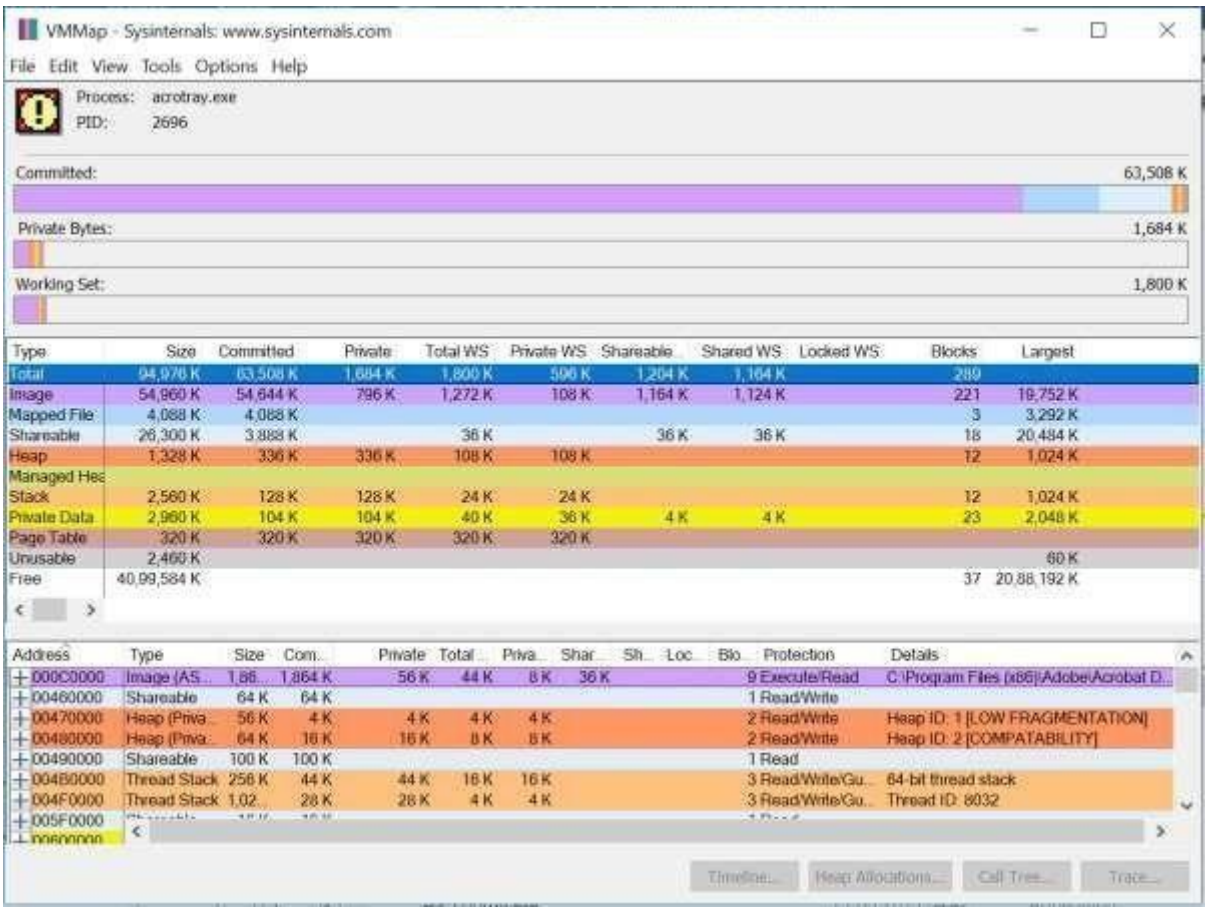
Open the Diskmon tool.



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

6) Monitor Virtual Memory (Tool: VMMap)

Open the VMMap tool.



7) Monitor Cache Memory (Tool:

RAMMap) Open the RAMMap tool.