Assessment No. 01

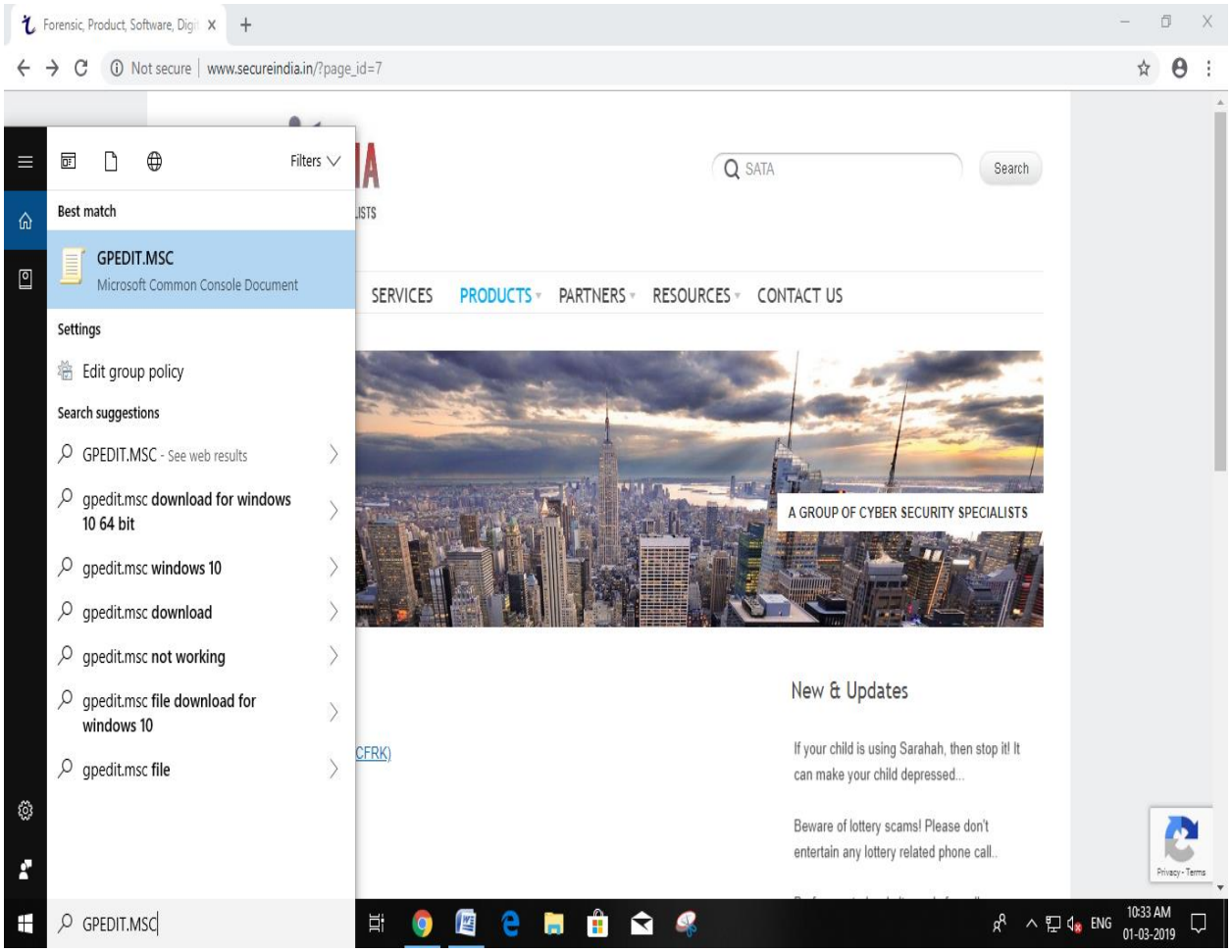
AIM: Perform Data Acquisition using:

(1) USB write blocker + Encase Imager
(2) SATA Write Blocker + Encase Image
(3) Falcon Imaging Device

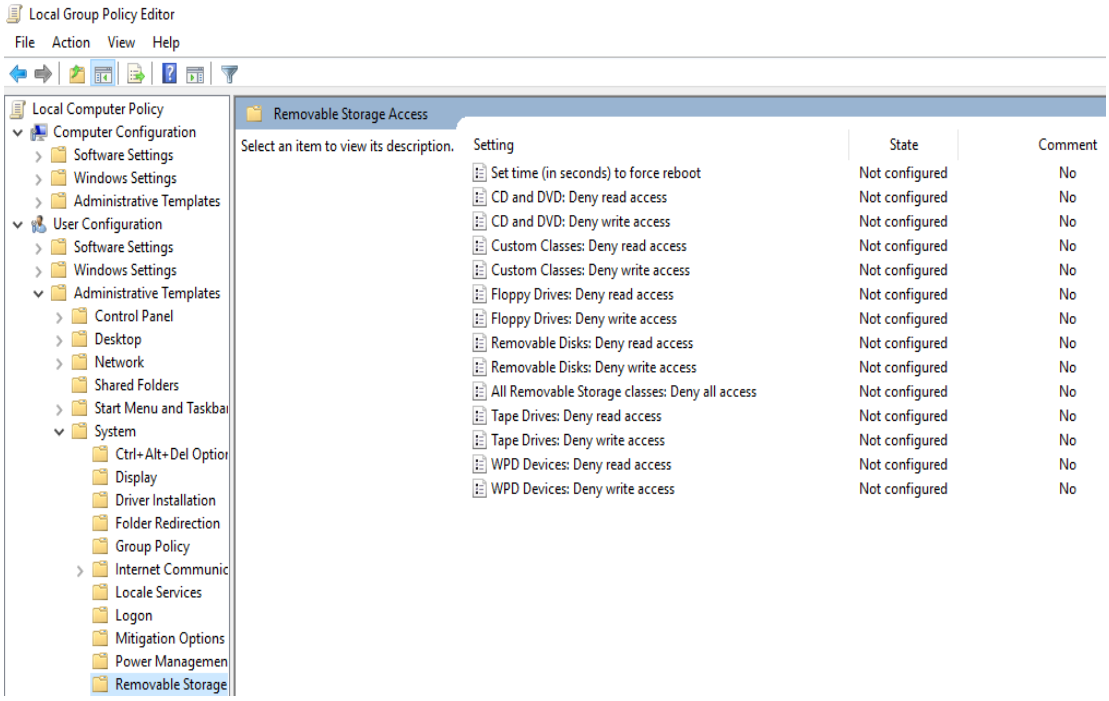
PROCEDURE AND OUTPUT:

(1)USB write blocker + Encase Imager

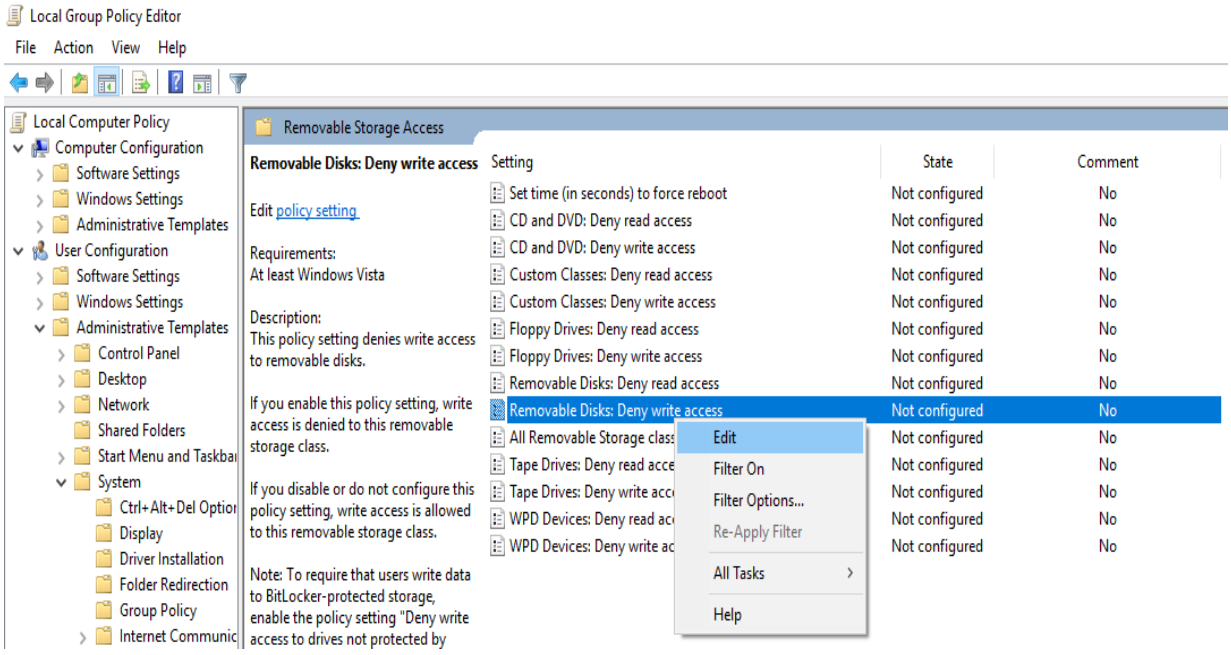
STEP 1: Open gpedit.msc file



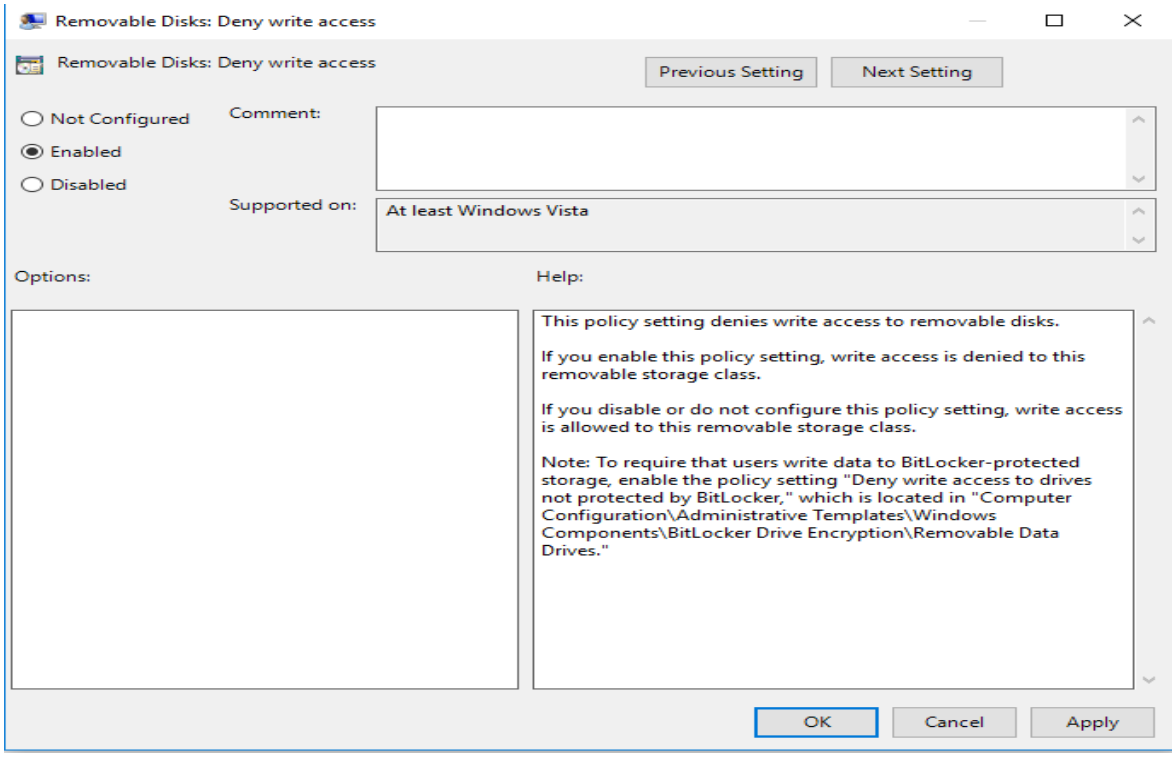
STEP 2: Go to User Configuration → Administrative Templates → System → Removable Storage Access



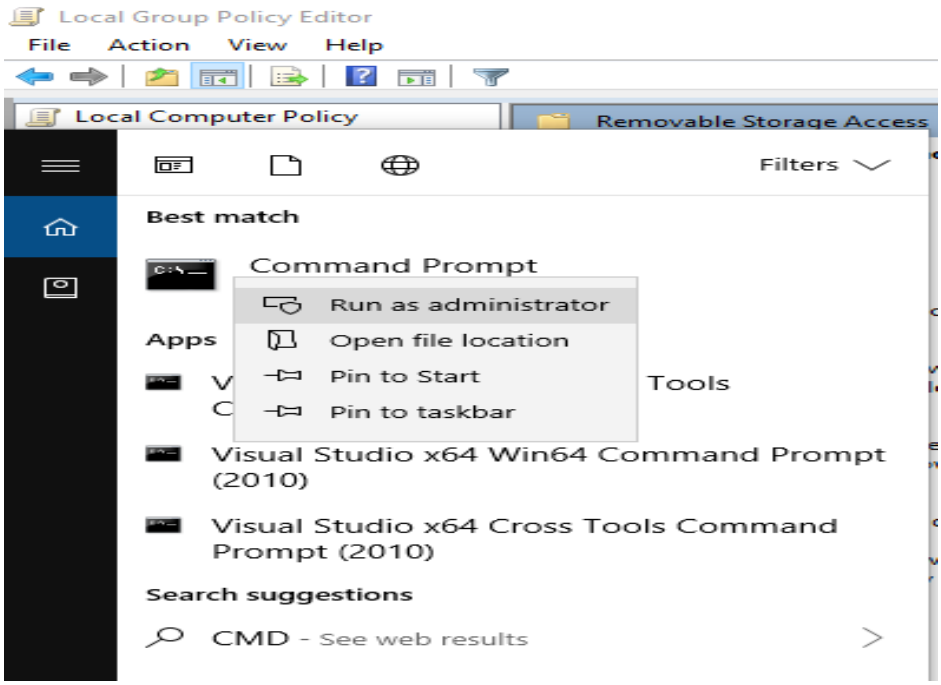
STEP 3: Right Click on the Removable Disks: Deny write access and press Edit.



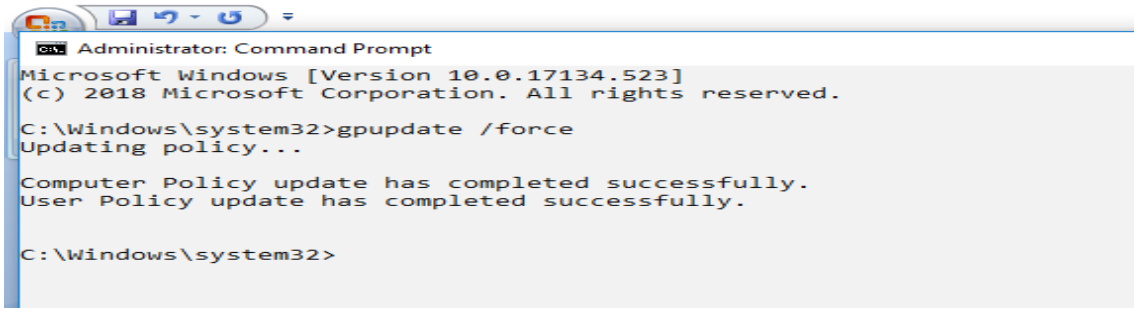
STEP 4: Now select the option 'Enabled' → Click on Apply → Now on OK



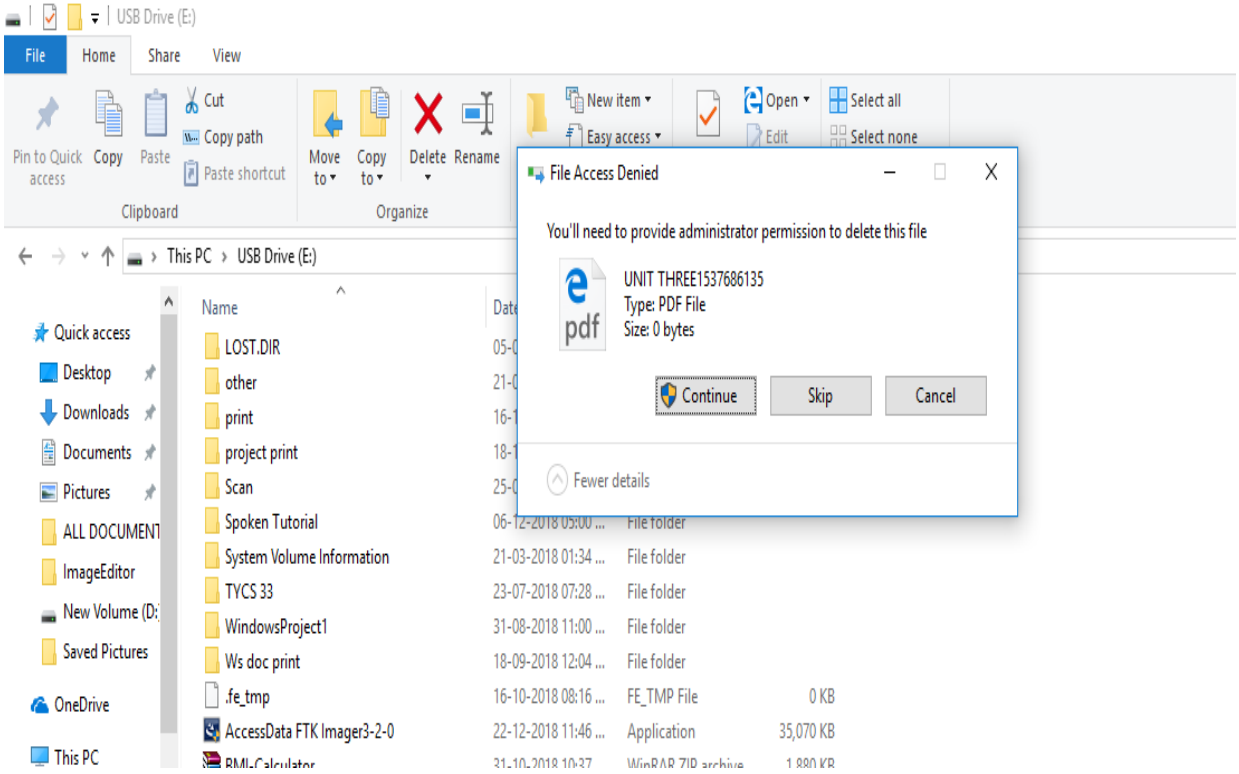
STEP 5: Open cmd in administrator mode.



STEP 6: Type command on cmd “gpupdate /force”.



STEP 7: Now Insert Removable Drive(Pen Drive) →open the removable drive through file manager → Try to delete one file.



(2) SATA Write Blocker + Encase Image

- **HISTORY:-**

SATA was announced in 2000[3] in order to provide several advantages over the earlier PATA interface such as reduced cable size and cost (seven conductors instead of 40 or 80), native hot swapping, faster data transfer through higher signaling rates, and more efficient transfer through an (optional) I/O queuing protocol.

- **FEATURES:-**

- **Hot plug**

The Serial ATA Spec requires SATA device hot plugging; that is, devices that meet the specification are capable of insertion / removal of a device into / from a backplane connector (combined signal and power) that has power on. After insertion, the device initializes and then operates normally. Depending upon the operating system the host may also initialize resulting in a hot swap. The powered host or devices are not necessarily in a quiescent state.

- **Advanced Host Controller Interface**

Advanced Host Controller Interface (AHCI) is an open host controller interface published and used by Intel, which has become a de facto standard. It allows the use of advanced features of SATA such as hotplug and native command queuing (NCQ).

- **VERSIONS OF SATA:-**

(1) SATA revision 1.0 (1.5 Gbit/s, 150 MB/s, Serial ATA-150)

Revision 1.0a was released on January 7, 2003. First-generation SATA interfaces, now known as SATA 1.5 Gbit/s, communicate at a rate of 1.5 Gbit/s,[b] and do not support Native Command Queuing (NCQ).

(2) SATA revision 2.0 (3 Gbit/s, 300 MB/s, Serial ATA-300)

SATA revision 2.0 was released in April 2004, introducing Native Command Queuing (NCQ). It is backward compatible with SATA 1.5 Gbit/s

(3) SATA revision 2.5

Announced in August 2005, SATA revision 2.5 consolidated the specification to a single document

(4) SATA revision 2.6

Announced in February 2007, SATA revision 2.6 introduced the following features

- **Slimline connector.**
- **Micro connector (initially for 1.8" HDD).**

- **FUNCTIONALITY**

- Write blockers are devices that allow acquisition of information on a drive without creating the possibility of accidentally damaging the drive contents.
- They do this by allowing read commands to pass but by blocking write commands, hence their name.
- The **Read Write UltraBlock USB 3.0 IDE-SATA** is used to write data to an IDE or SATA hard drive.
- The USB 3.0 family of portable forensic bridges offer faster imaging speeds, reliable performance, and an easy to use USB 3.0 host computer connection.
- We offer an UltraBlock USB 3.0 IDE/SATA pre-configured for read/write operation.
- It's available in a yellow case so that you can easily distinguish a pre-configured read/write device from a read-only device.
- It offers forensic examiners the case of use, reliability, and imaging speed necessary to image today's larger and faster hard-disk drives - in both lab or field environments.
- Serial ATA (SATA, abbreviated from Serial AT Attachment)[2] is a computer bus interface that connects host bus adapters to mass storage devices such as hard disk drives, optical drives, and solid-state drives. Serial ATA succeeded the earlier Parallel ATA (PATA) standard to become the predominant interface for storage devices.

(3) Falcon Imaging Device

- Write-blocking on source ports ensures data integrity.

- The fastest forensic duplicator on the market – Images at up to 20 GB/min.
- Performs up to five tasks at once.
- Image multiple sources to multiple destinations and perform secure wipes concurrently.
- No ongoing license fees. Once you own the device, it can be used in perpetuity.

FEATURES:

1) **Extremely Fast Imaging**
   The Falcon is the fastest forensic imaging solution available, achieving speeds of 20GB/min*. The Falcon meets future hard drive speed improvements with SAS/SATA-3 6GB/s maximum rated speed of 37GB/min.
2) **Multiple Image Formats**
   The Falcon images and verifies to the following formats: native or mirror copy, dd image, e01, ex01 and file-based copy. e01 and ex01 feature user-selectable compression levels and the Falcon supports SHA1, SHA256 or MD5 authentication.
3) **Multiple Imaging Ports**
   Write-protected source ports include:
   2 SAS/SATA
   1 USB 3.0 (can be converted to SATA using an optional USB to SATA adapter)
   1 Firewire
   1 SCSI (using the SCSI Module Option)
   Destination ports include:
   2 SAS/SATA
   2 USB 3.0 (can be converted to SATA using an optional USB to SATA adapter)
   1 Firewire
   1 SCSI (using the SCSI Module Option)
4) **A Gigabit Ethernet port** for network connectivity is built-in. An optional PCI express card interface (for new/future technologies such as Thunderbolt) is planned for future availability.In addition the unit includes a USB 3.0 device port for drive preview and two USB 2.0 host ports
5) **Multi-task**
   Improve efficiency and shorten the evidence collection process with the ability to wipe one destination drive while imaging to another simultaneously, or image from multiple source drives to multiple destinations. Perform up to five tasks concurrently.
6) **Web-based User Interface**
   An easy to use and intuitive interface allows you to connect to the Falcon from a web browser and manage all operations remotely. The browser features automatic page scaling for iPad type devices.

7) **Broad Interface Support**
   Built-in support for SAS/SATA/USB/Firewire storage devices. Supports 1.8″/2.5″/3.5″ IDE and 1.8″ IDE ZIF and microSATA interfaces with adapters included with Falcon. Optional adapters are available for eSATA, mSATA and flash drives.
8) **Wipe**

Wipe up to DoD specifications or use Secure Erase to erase drives.

9) **Image to External Storage Device**

The Falcon allows you to image to an external storage device such as a NAS, using the Gigabit Ethernet port, USB 3.0 or via the SAS/SATA connection.

10) **SCSI Module Option**

The SCSI Module Option expands the capability of the Forensic Falcon by providing support for imaging from and to SCSI hard drives. The Module connects seamlessly to the Falcon and provides 1 write-protected SCSI source port and 1 SCSI destination port. All Falcon features supported with this module.

CONCLUSION: Thus we have performed Data Acquisition Successfully.

Assessment No. 02

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

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:

1. File and Disk Utilities

2. Networking Utilities

3. Process Utilities

4. Security Utilities

5. System Information Utilities

6. Miscellaneous Utilities

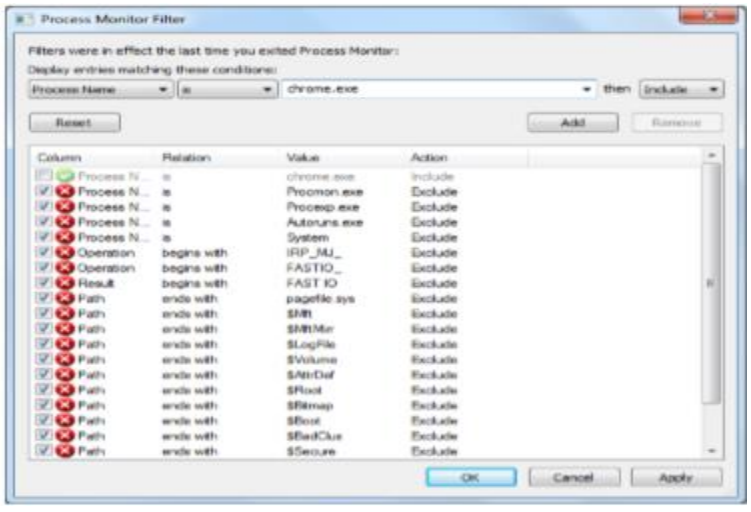
2. Monitor Live Processes (Tool: ProcMon).

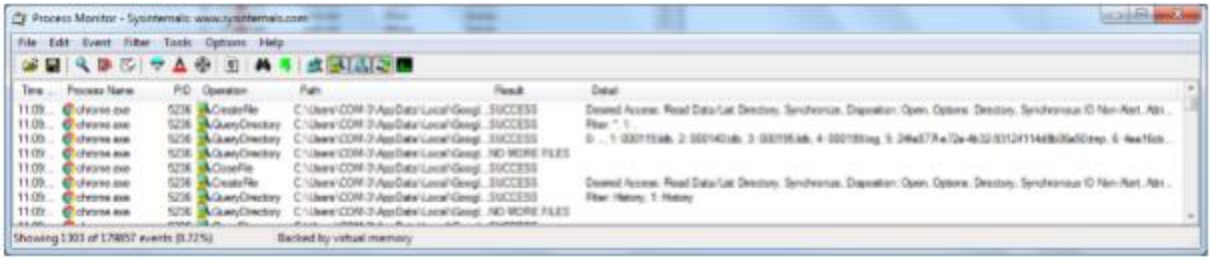
1. Filter (Process Name or PID or Architecture, etc)

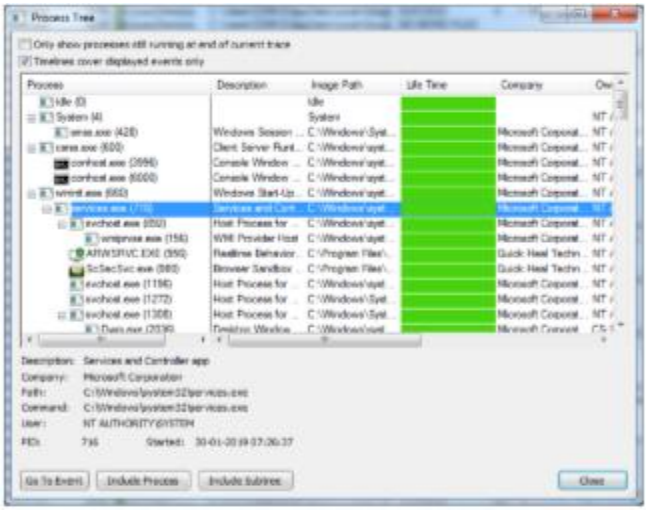
2. Process Tree

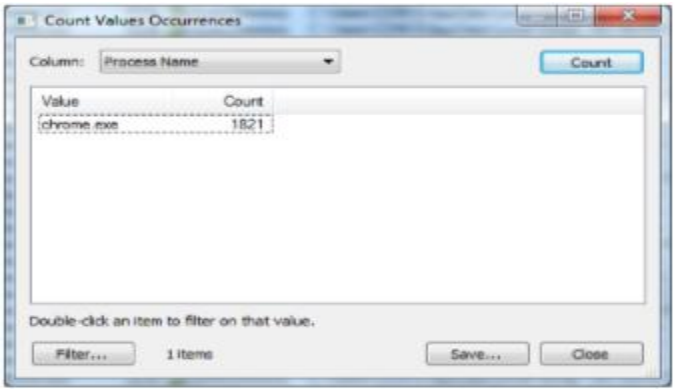
3. Process Activity Summary

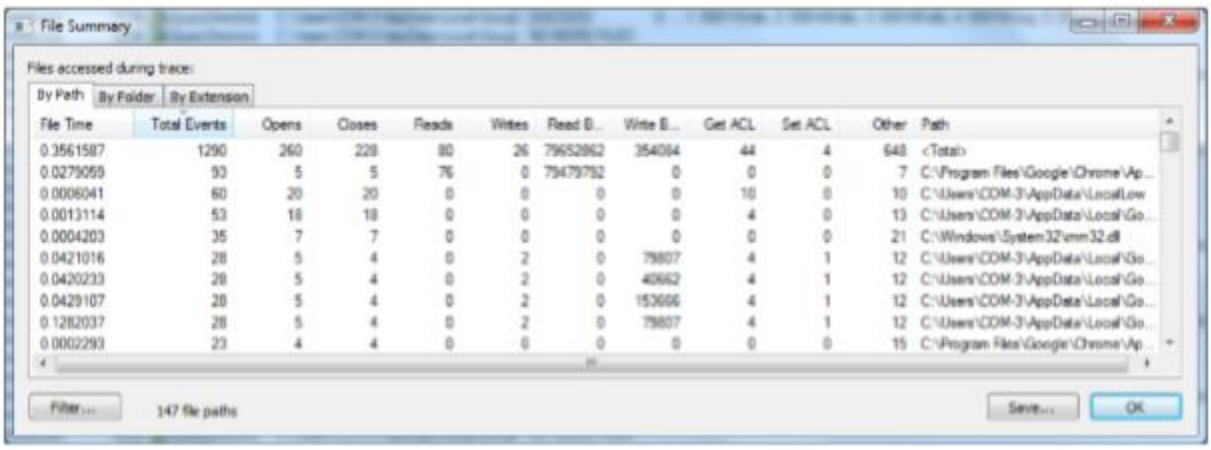
4. Count Occurrences




Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Time ... Process Name PID Operation Path Result Detail


Process Tree
Only show processes still running at end of current trace
Timelines cover displayed events only
Process Description Image Path Life Time Company
Description: Services and Controller app
Company: Microsoft Corporation
Path:
Command:
User:
PID: 716 Started:
Go To Event
Include Process
Include Subtree
Close


Count Values Occurrences
Column: Process Name
Count
Value Count
chrome.exe 1821
Double-click an item to filter on that value.
Filter...
1 items
Save...
Close

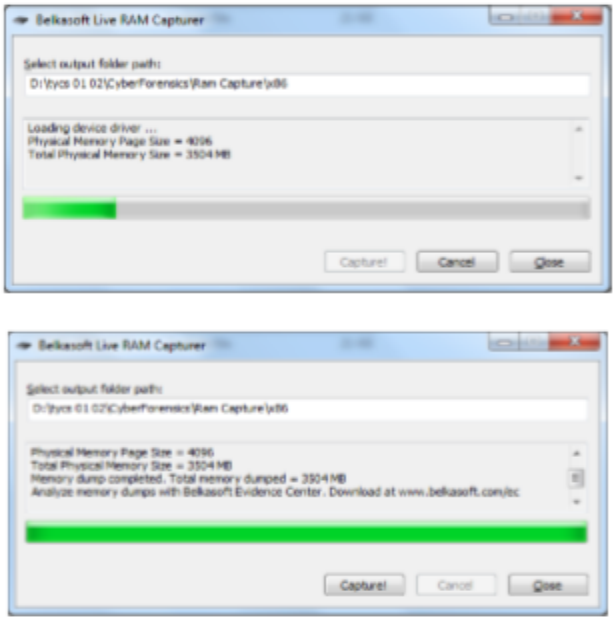

File Summary
Files accessed during trace:
By Path By Folder By Extension
File Time Total Events Opens Closes Reads Writes Read B... Write B... Get ACL Set ACL Other Path
0.3561587 1290 260 228 80 26 79652862 354084 44 4 648 <Total>
0.0279059 93 5 5 76 0 79479752 0 0 0 7 C:\Program Files\Google\Chrome\Ap...
0.0006041 60 20 20 0 0 0 0 10 0 10 C:\Users\COM-3\AppData\LocalLow
0.0013114 53 18 18 0 0 0 0 4 0 13 C:\Users\COM-3\AppData\Local\Go...
0.0004203 35 7 7 0 0 0 0 0 0 21 C:\Windows\System32\mm32.dll
0.0421016 28 5 4 0 2 0 79807 4 1 12 C:\Users\COM-3\AppData\Local\Go...
0.0420233 28 5 4 0 2 0 40662 4 1 12 C:\Users\COM-3\AppData\Local\Go...
0.0429107 28 5 4 0 2 0 153666 4 1 12 C:\Users\COM-3\AppData\Local\Go...
0.1282037 28 5 4 0 2 0 79807 4 1 12 C:\Users\COM-3\AppData\Local\Go...
0.0002293 23 4 4 0 0 0 0 0 0 15 C:\Program Files\Google\Chrome\Ap...
Filter...
147 file paths
Save...
OK

3. Capture RAM (Tool: RAMCapture)

1. Click Capture

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

Output:

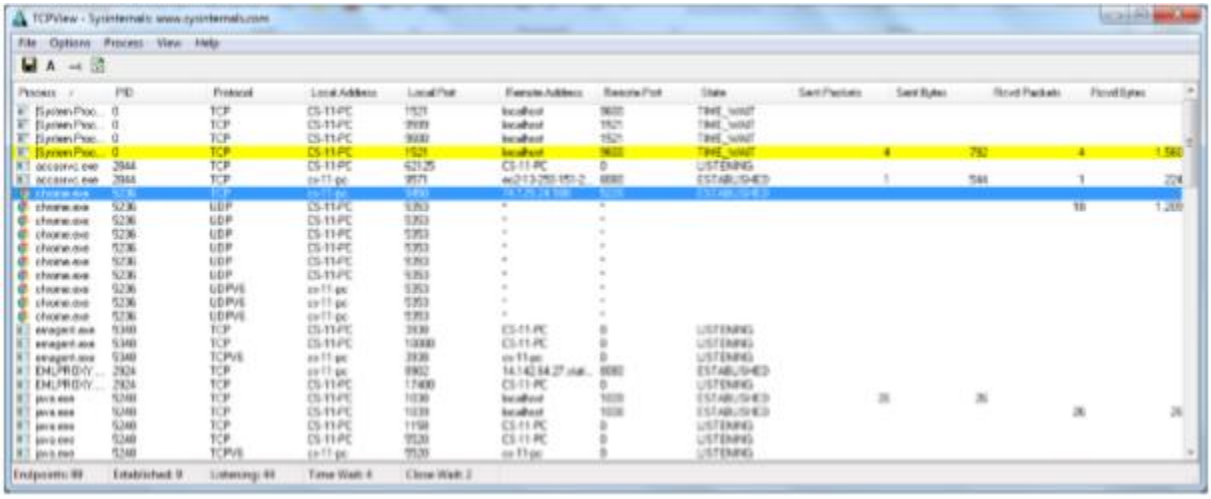


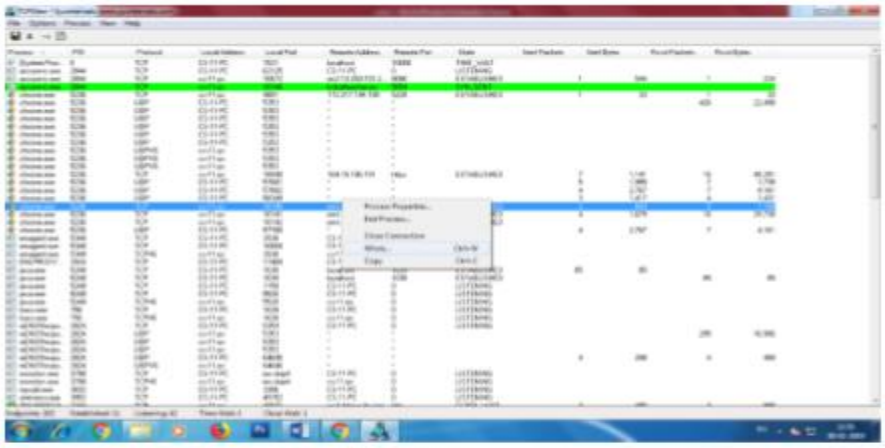
4. Capture TCP/UDP packets (Tool: TcpView)

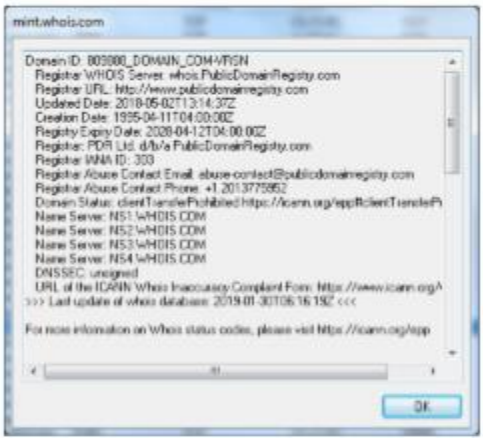
1. Save to .txt file.

2. Whois

Output:



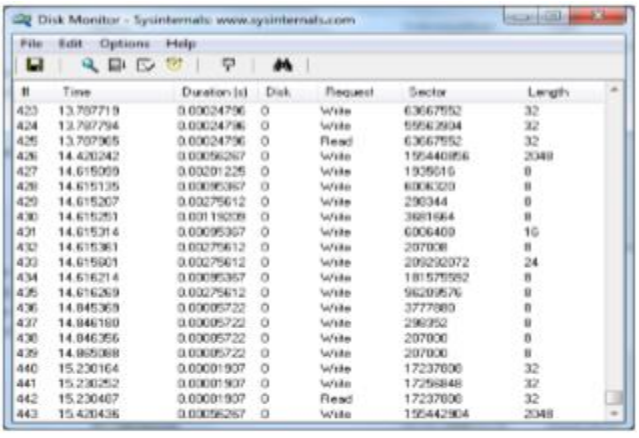




5. Monitor Hard Disk (Tool: DiskMon)

1. Save to .log file.

2. Check operations performed in the disk as per time and sectors affected.



Conclusion: Thus we have successfully studied Network Tracking and Process Monitoring.

Assessment No. 03

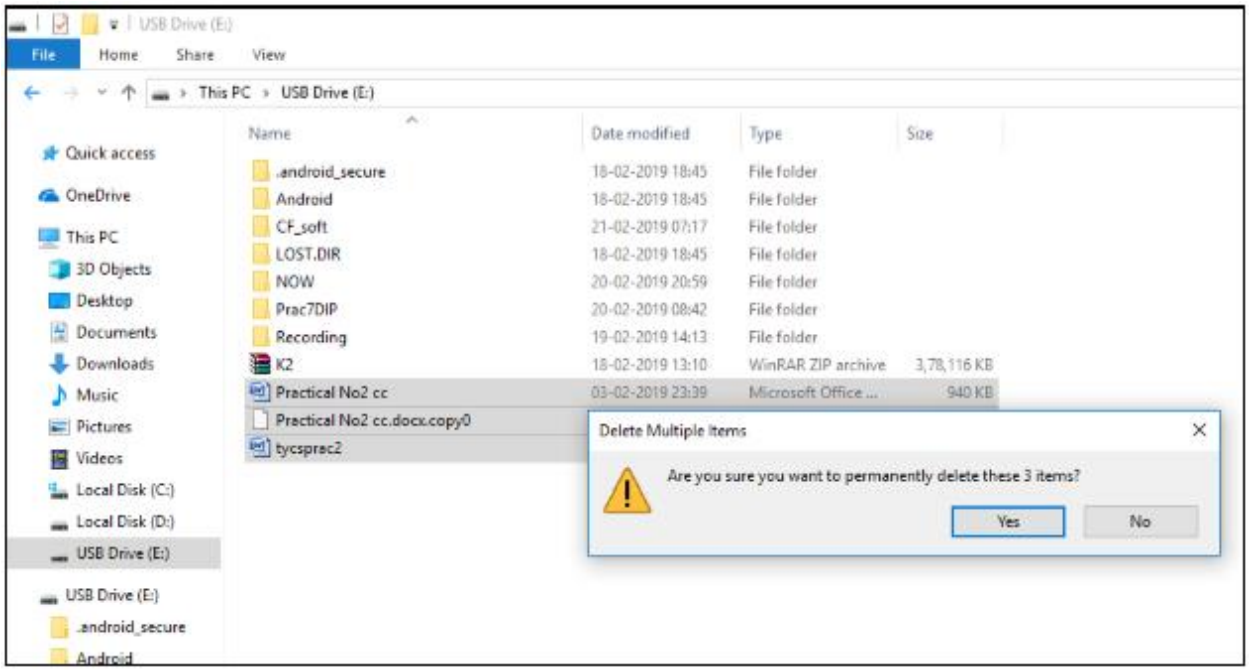
AIM: To recover deleted file using FTK.

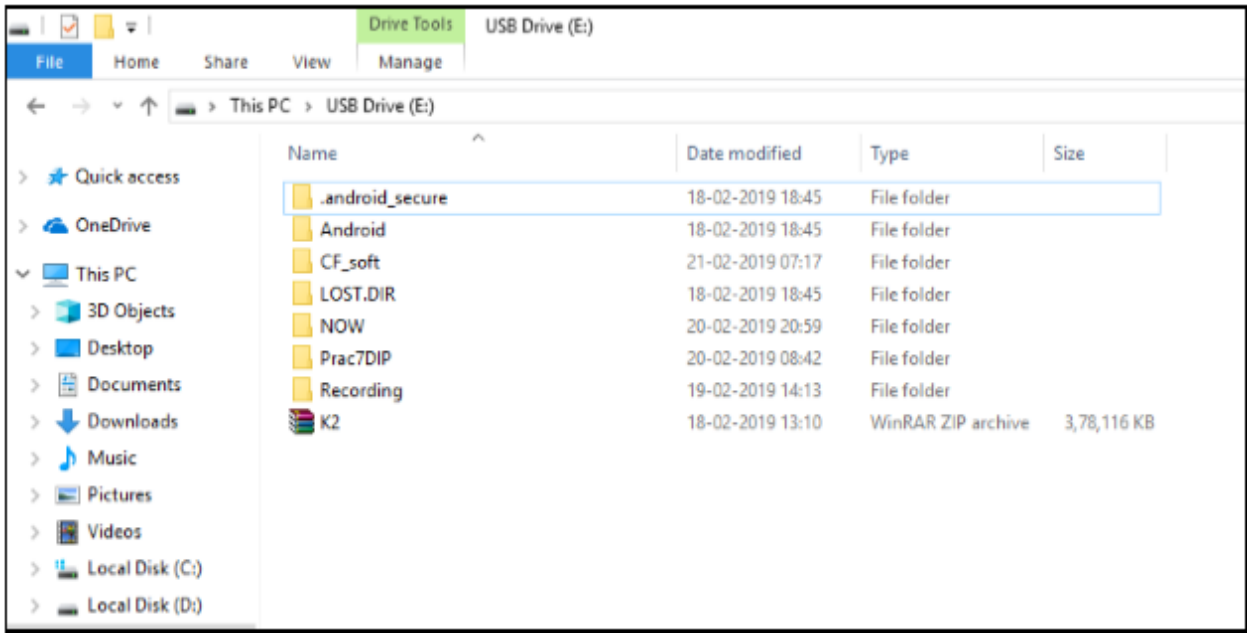
Steps:

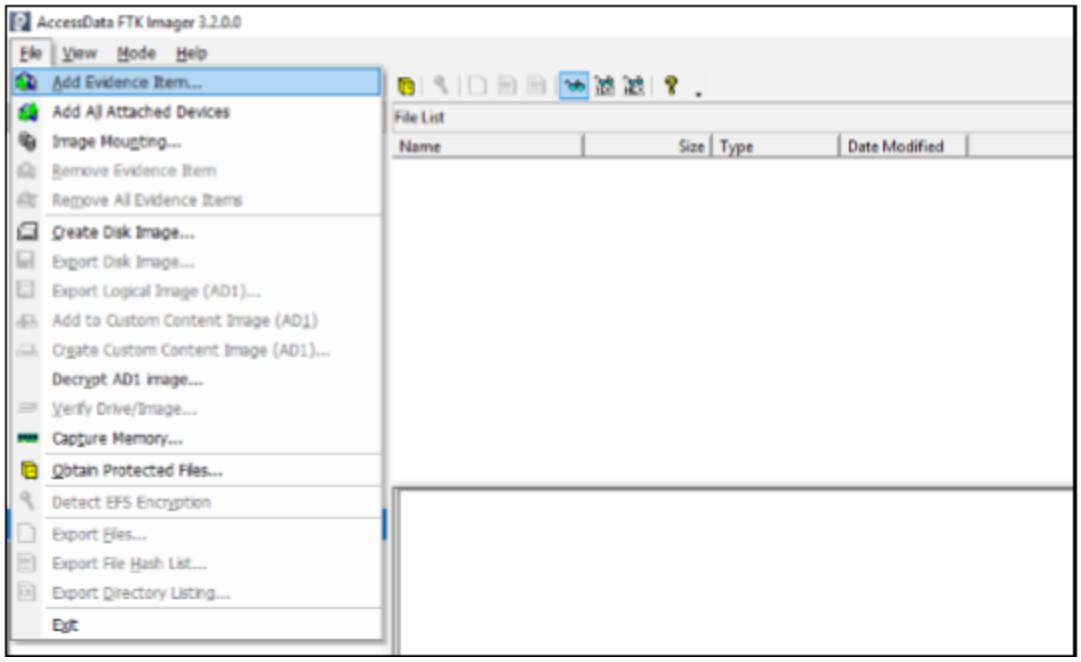
1. Insert the USB Drive in the Computer.

2. Delete folder from the drive.

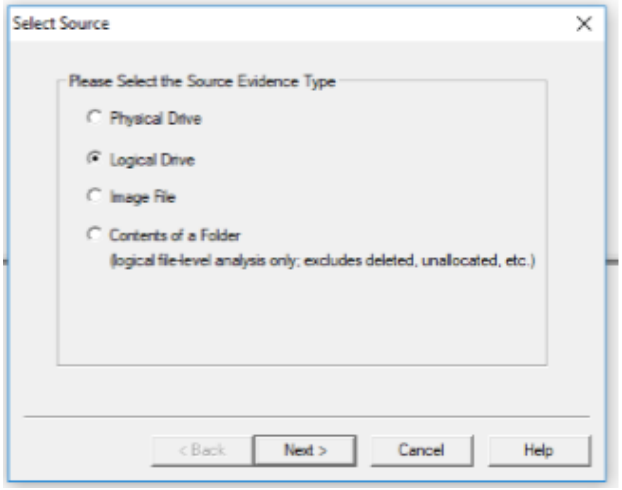
3. Open Access Data FTK Imager > File > Add Evidence Item.

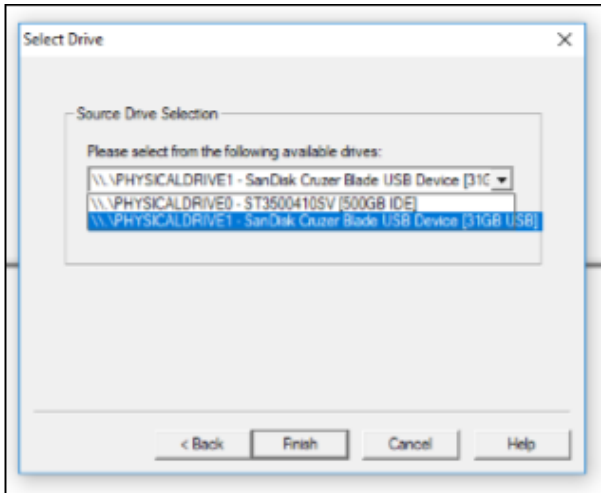




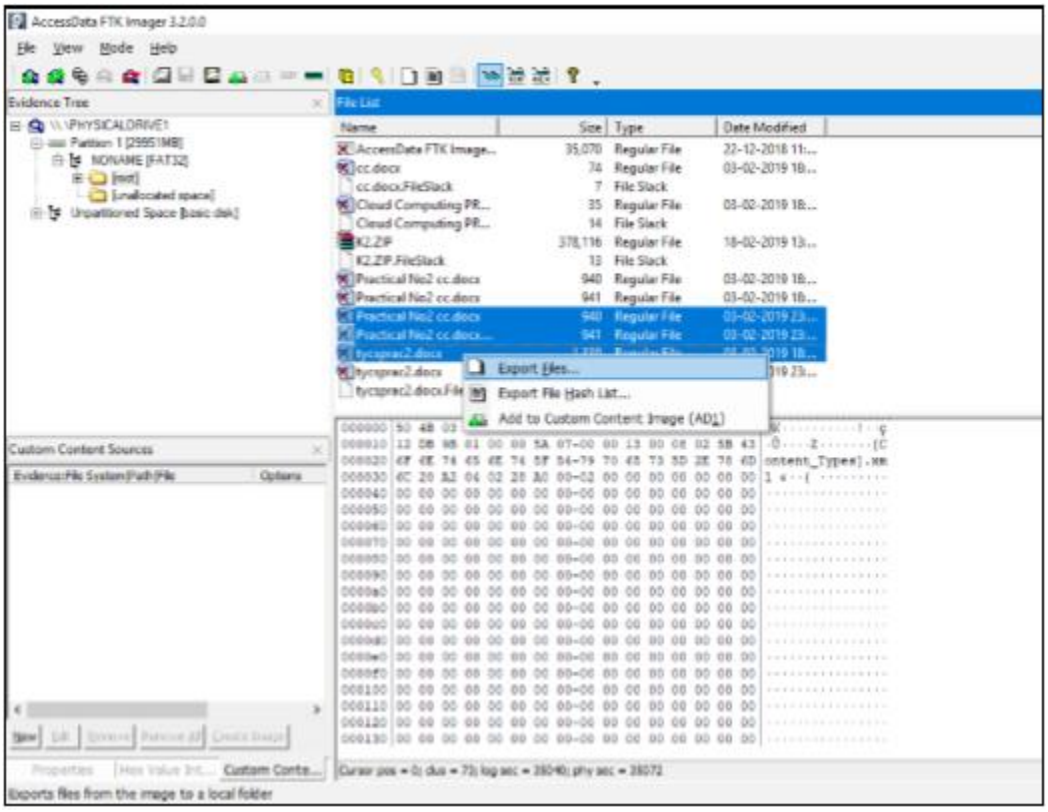


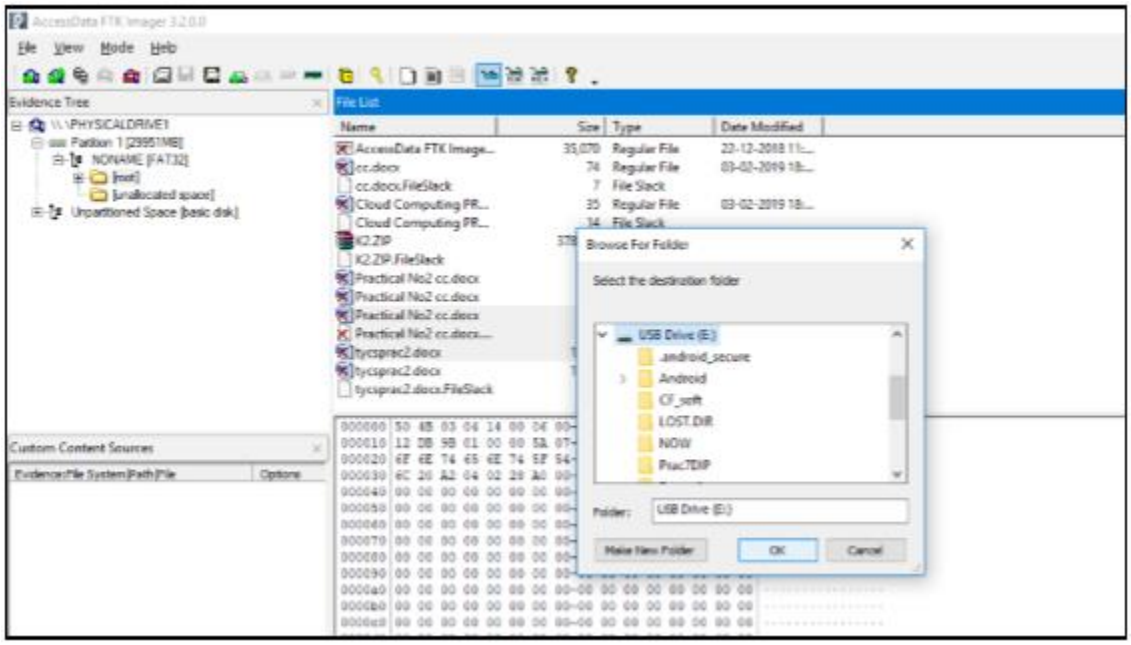
4. Select Logical Drive.

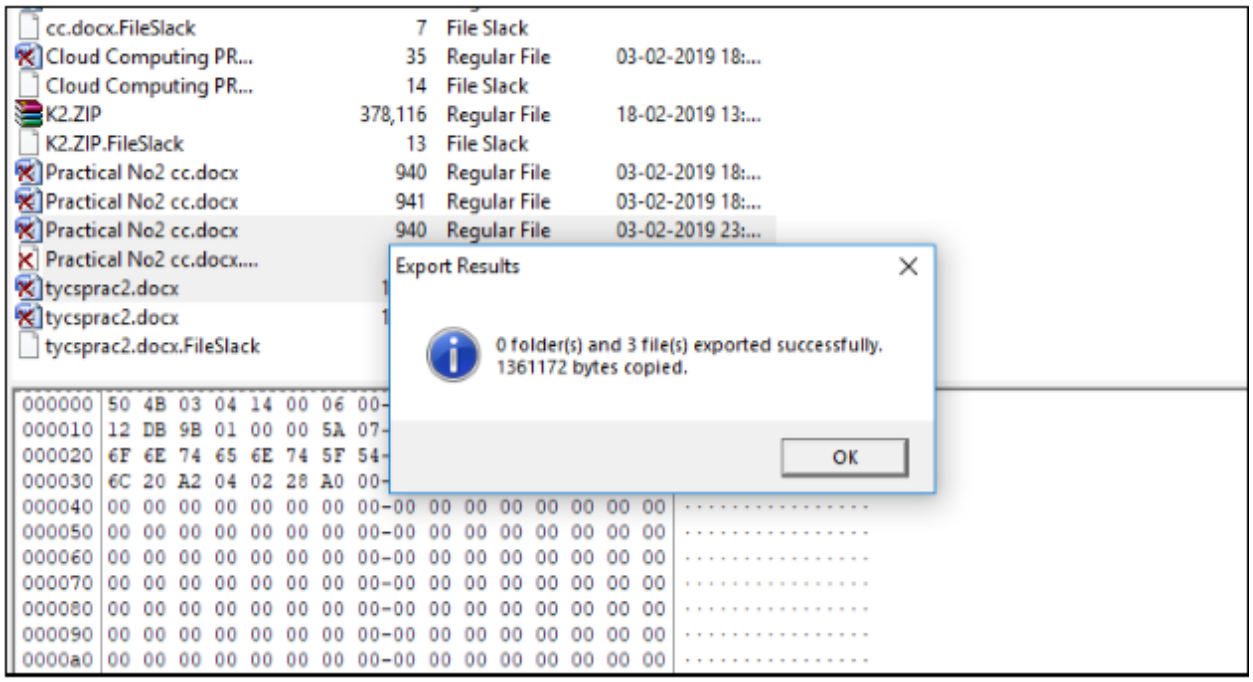


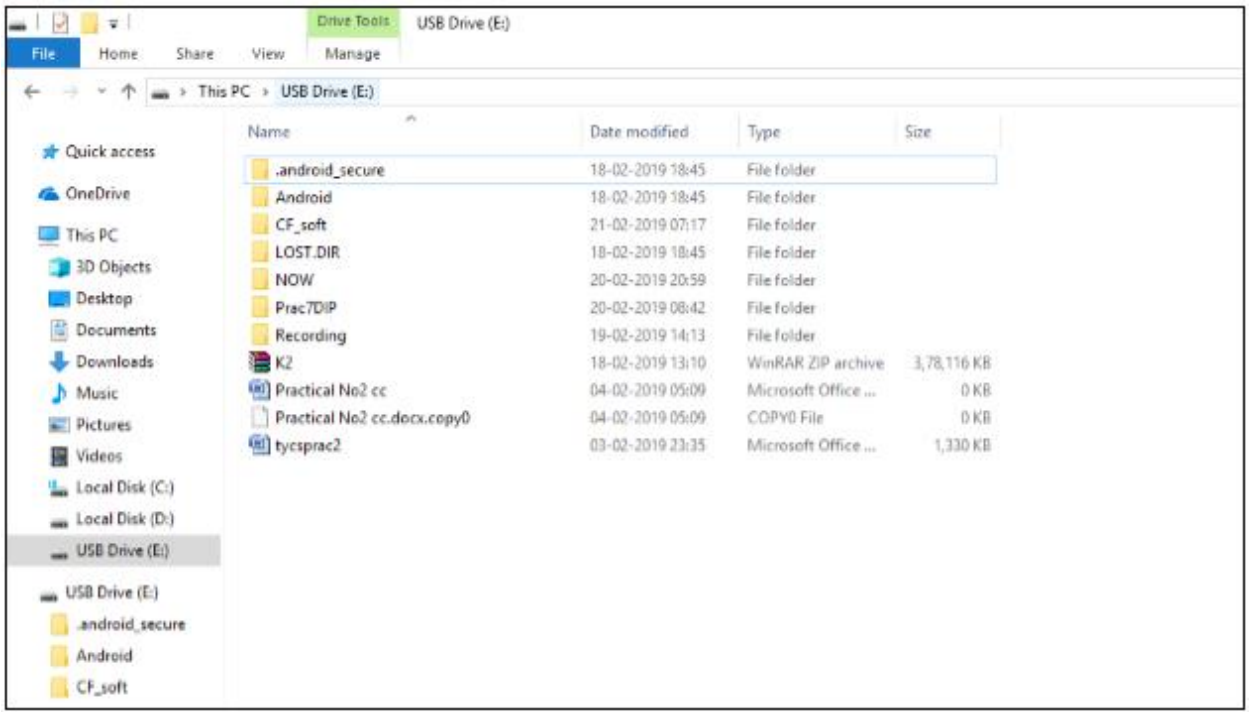


5. Right Click on the File > Export Files > Select the source to Copy > OK









Conclusion: Thus the deleted files were recovered successfully.

Assessment No. 04

AIM: Email Forensics

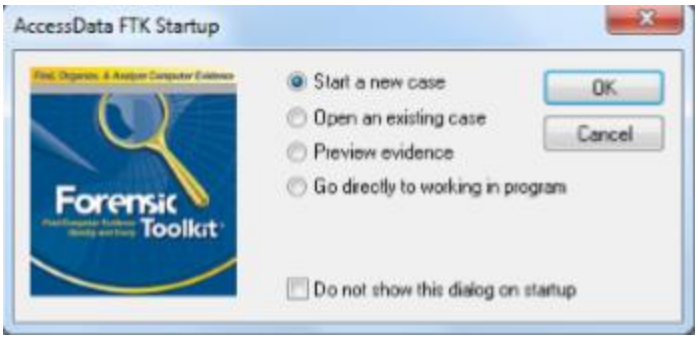
- Mail Service Providers

- Email protocols

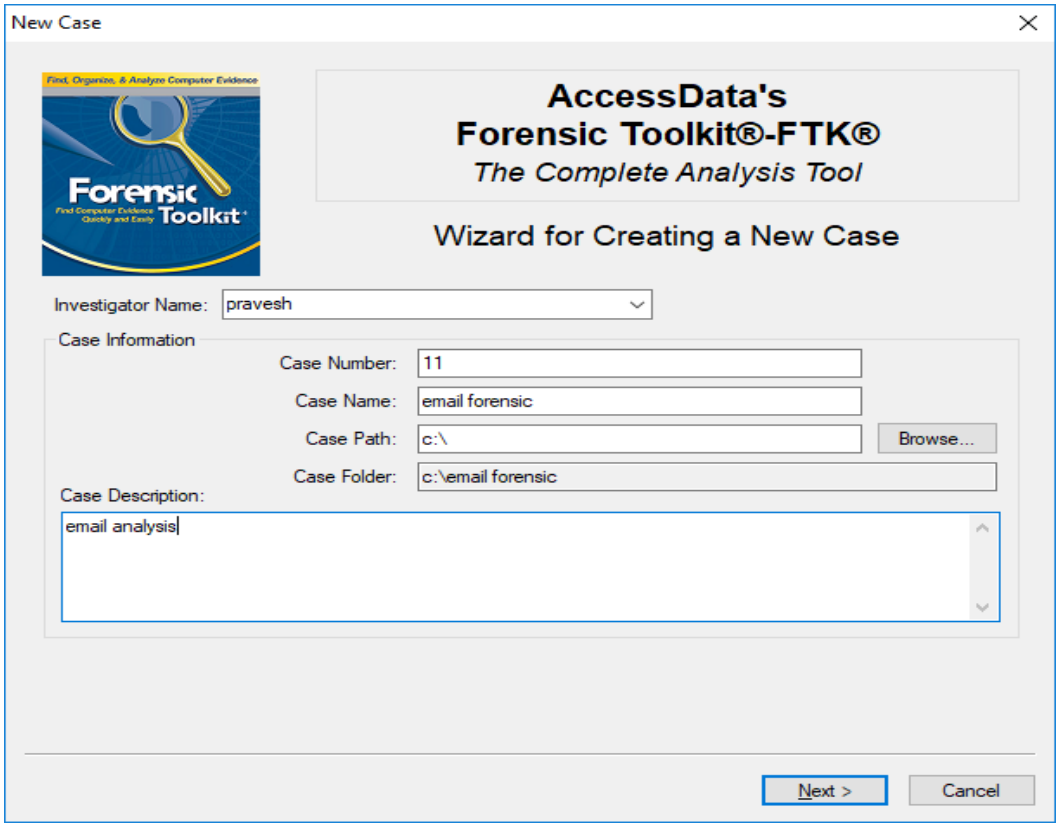
- Recovering emails

- Analyzing email header

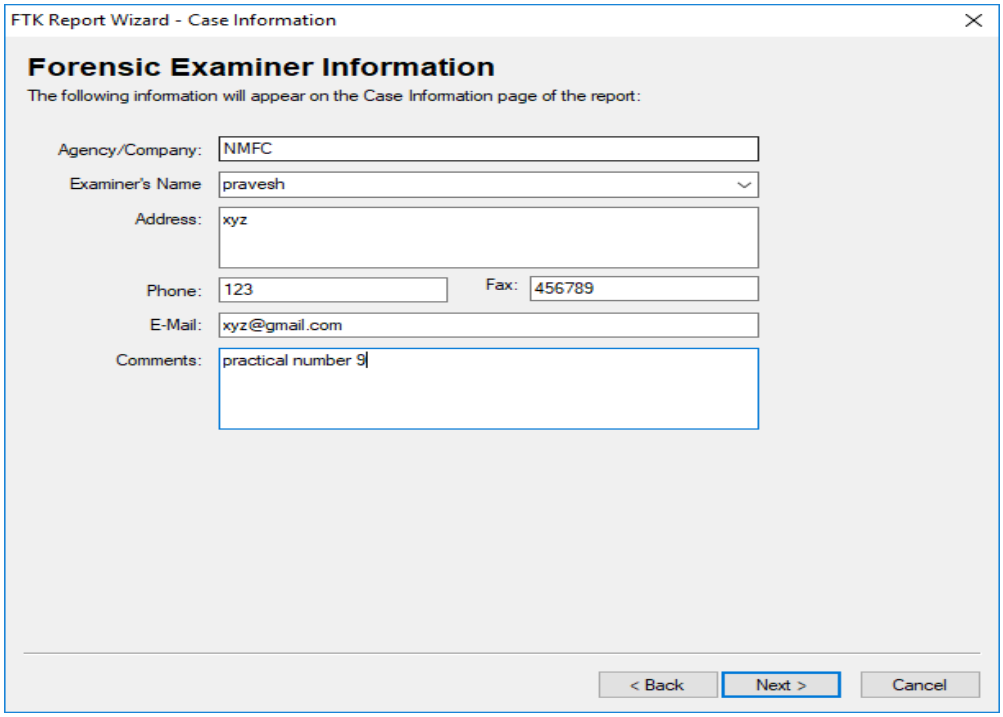
STEP 1: Select menu Start new Case



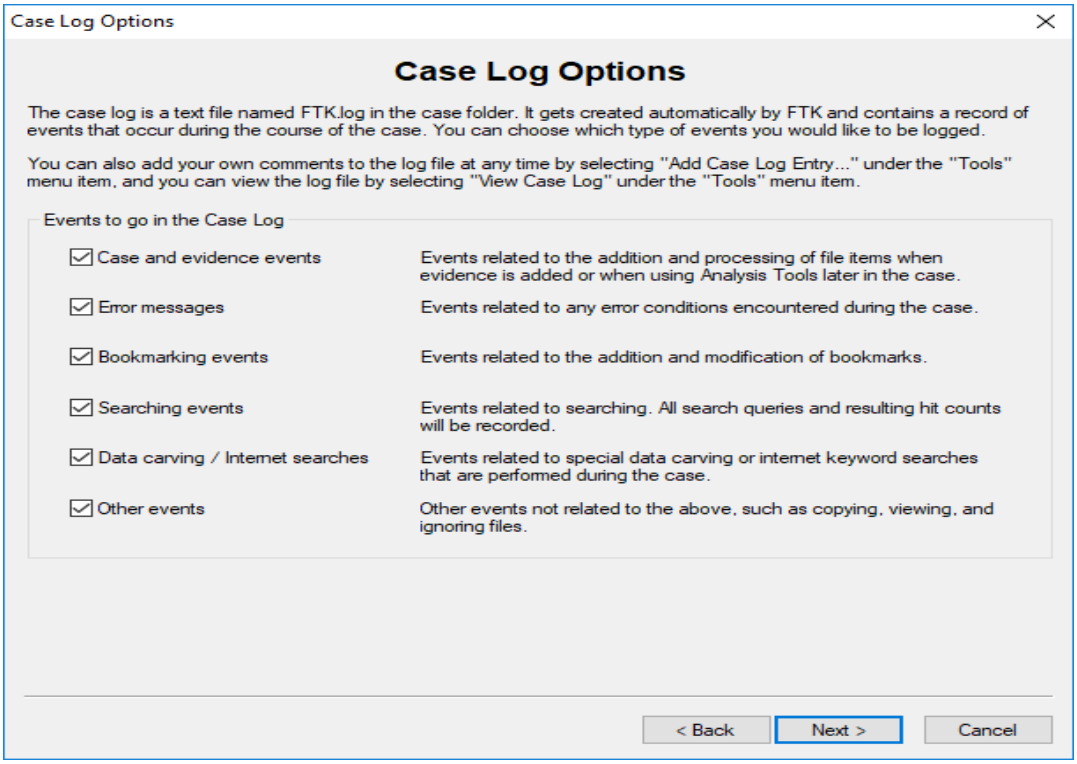
Step 02: Provide details for Case.



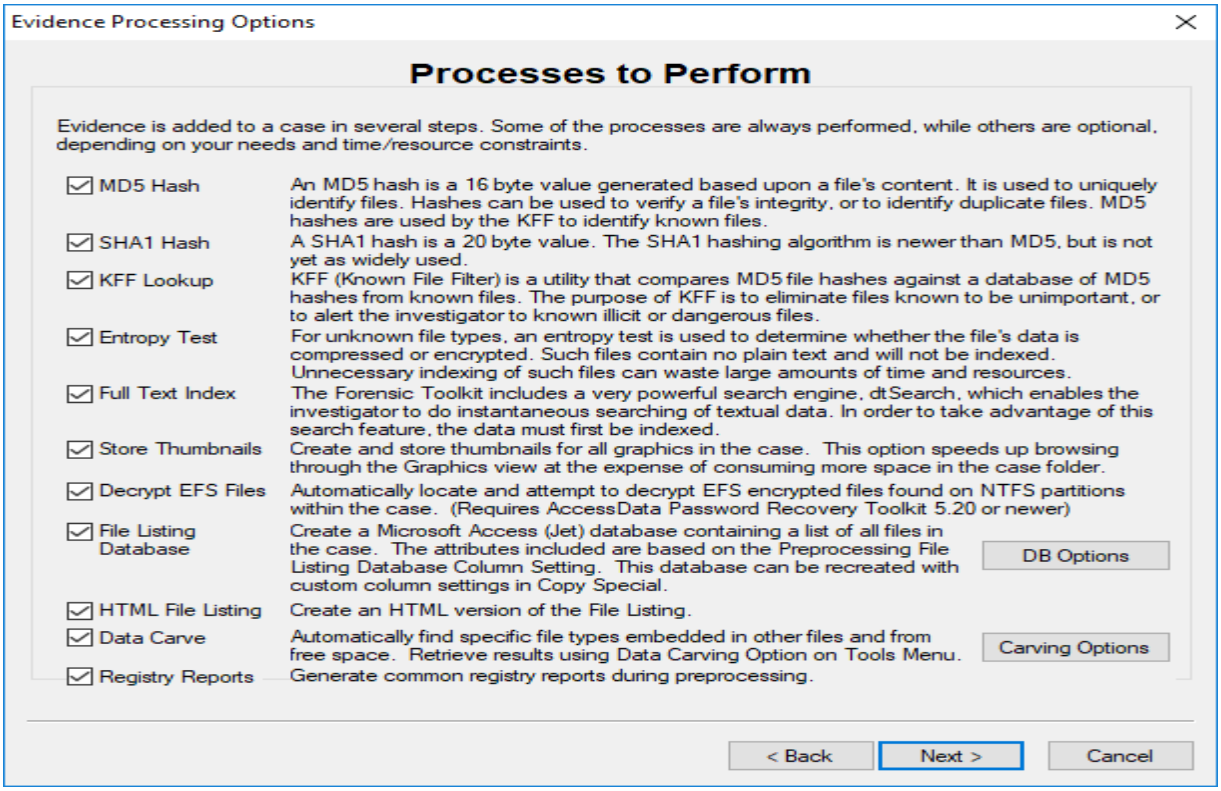
Step 03: Provide details for Case Examiner



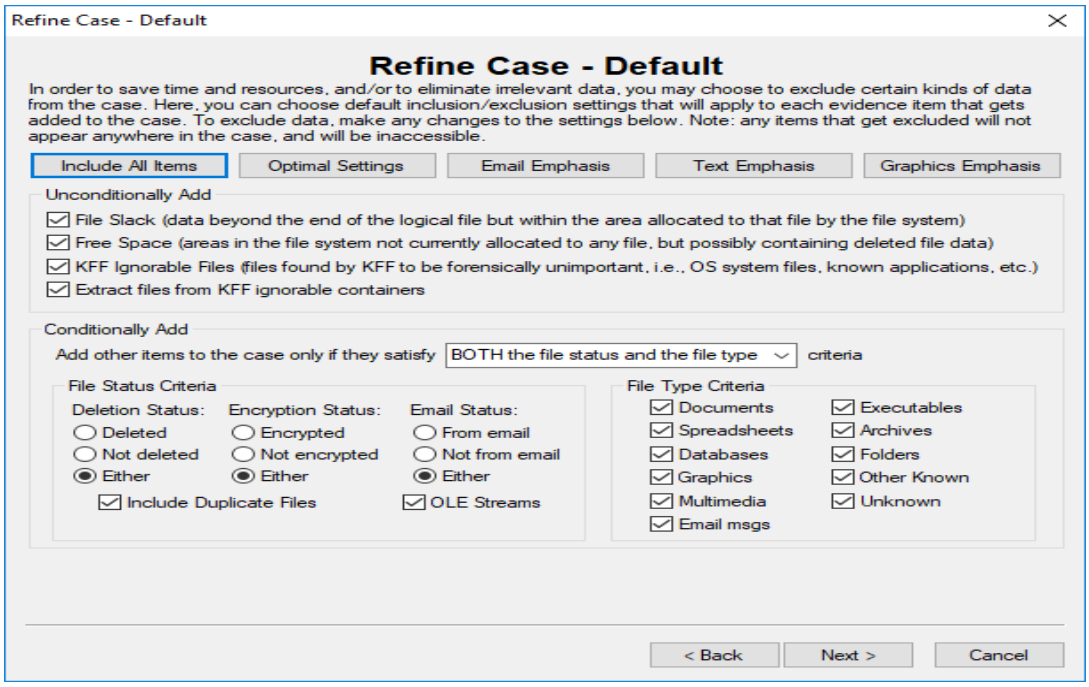
Step 04: Select all options and click on Next



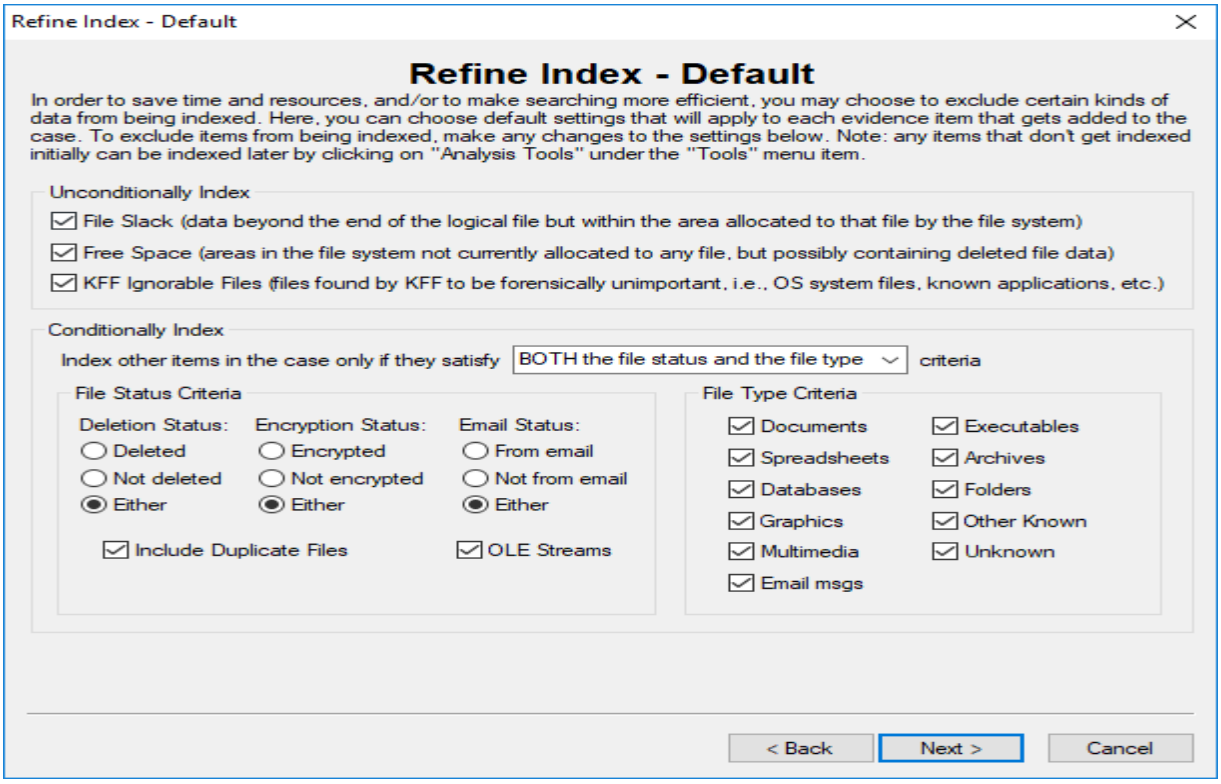
Step 05: Select all options and click on Next.



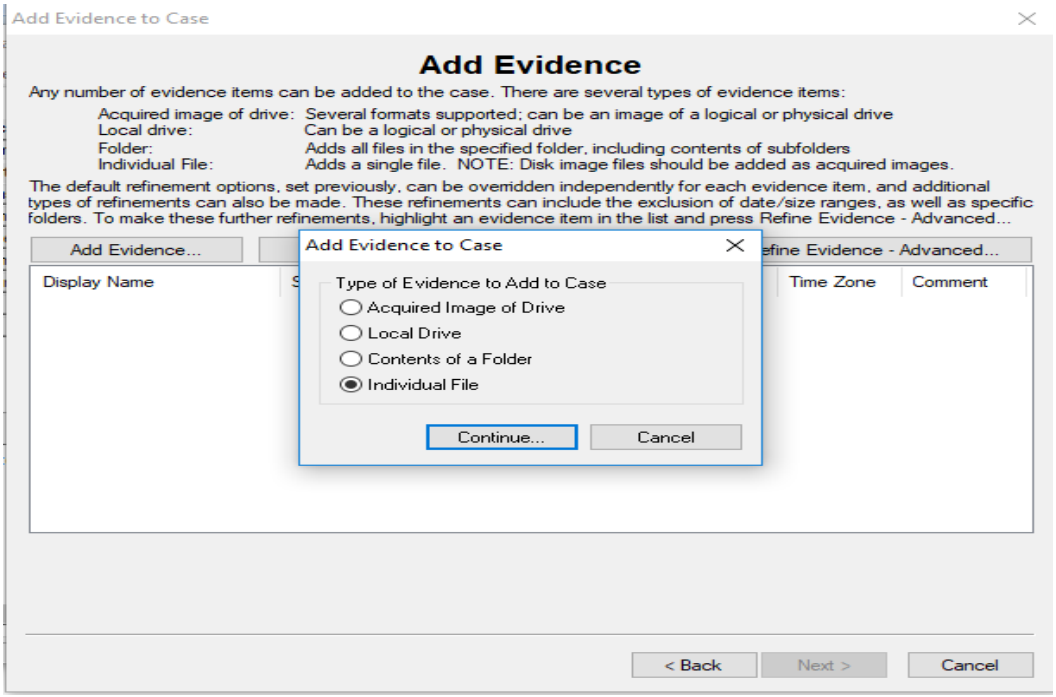
Step 06: Click on Include all Items.



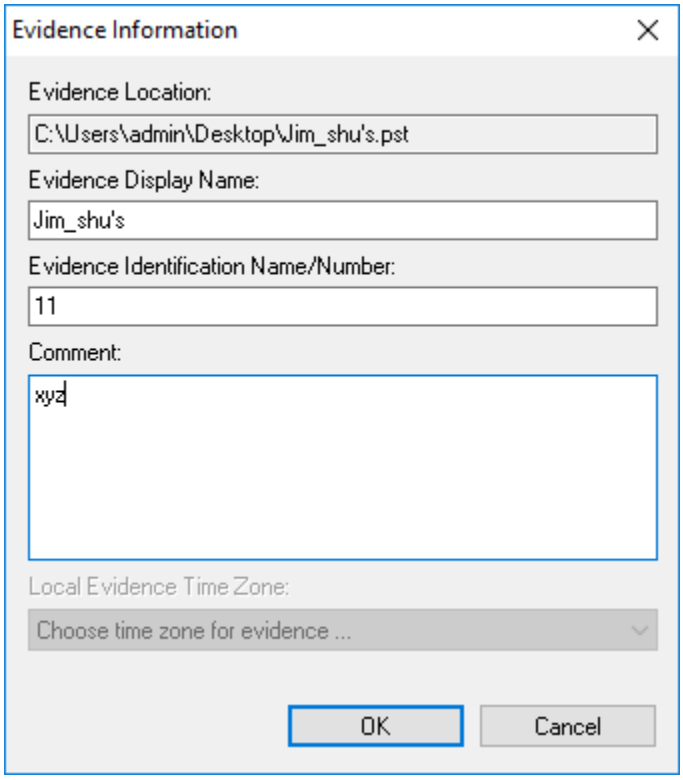
Step 07: Select all Options.



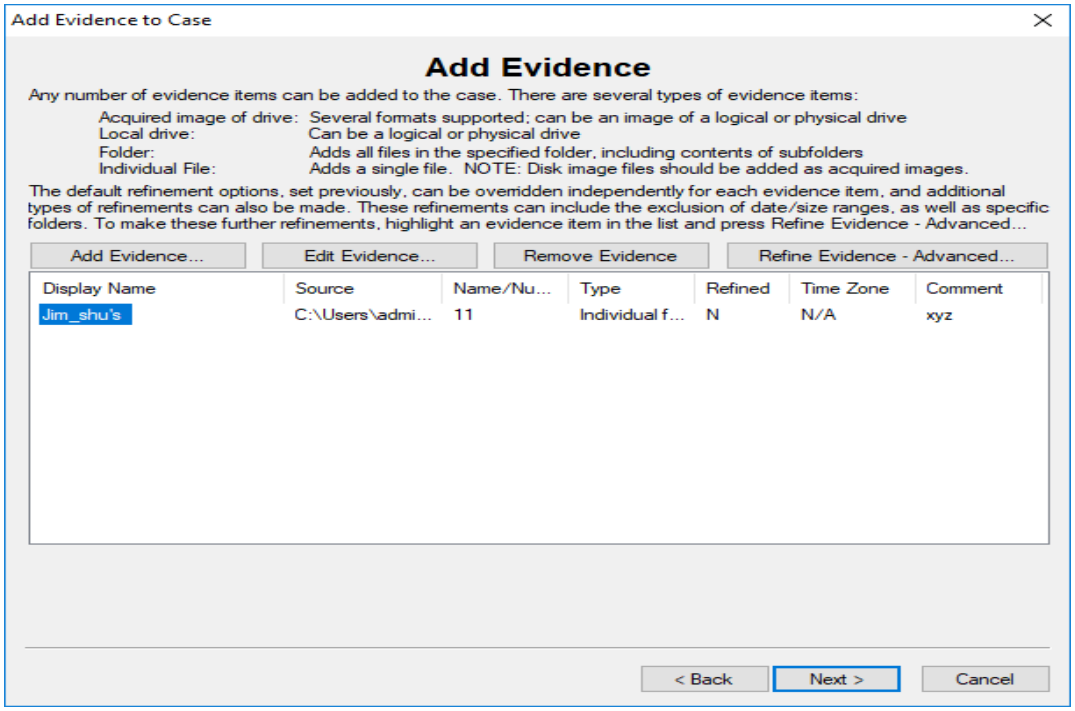
Step 08: Add Evidence to the Case by selecting Individual File.



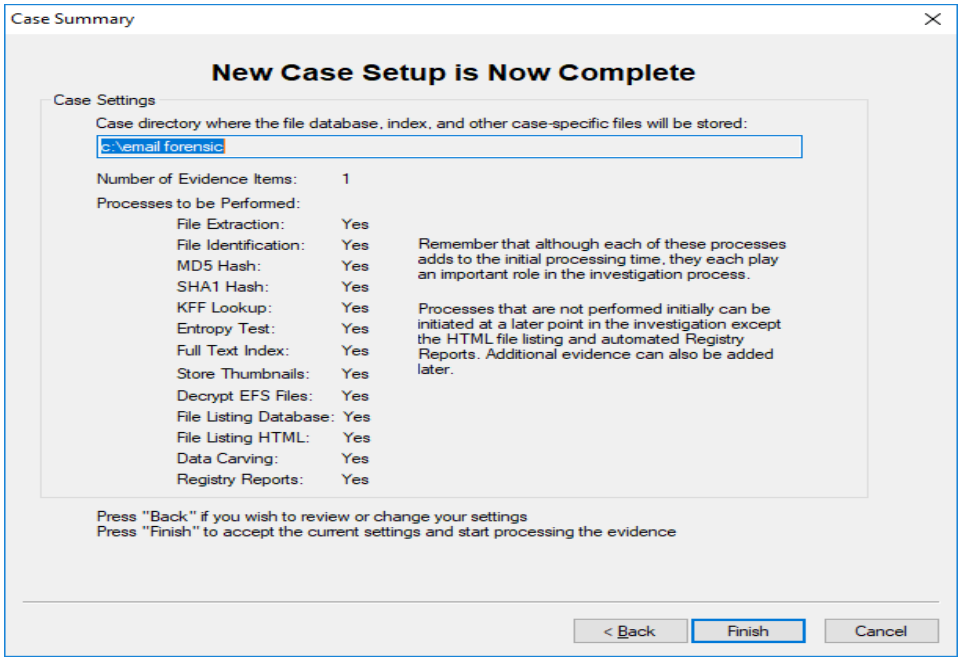
Step 9: Provide details for Evidence Information.



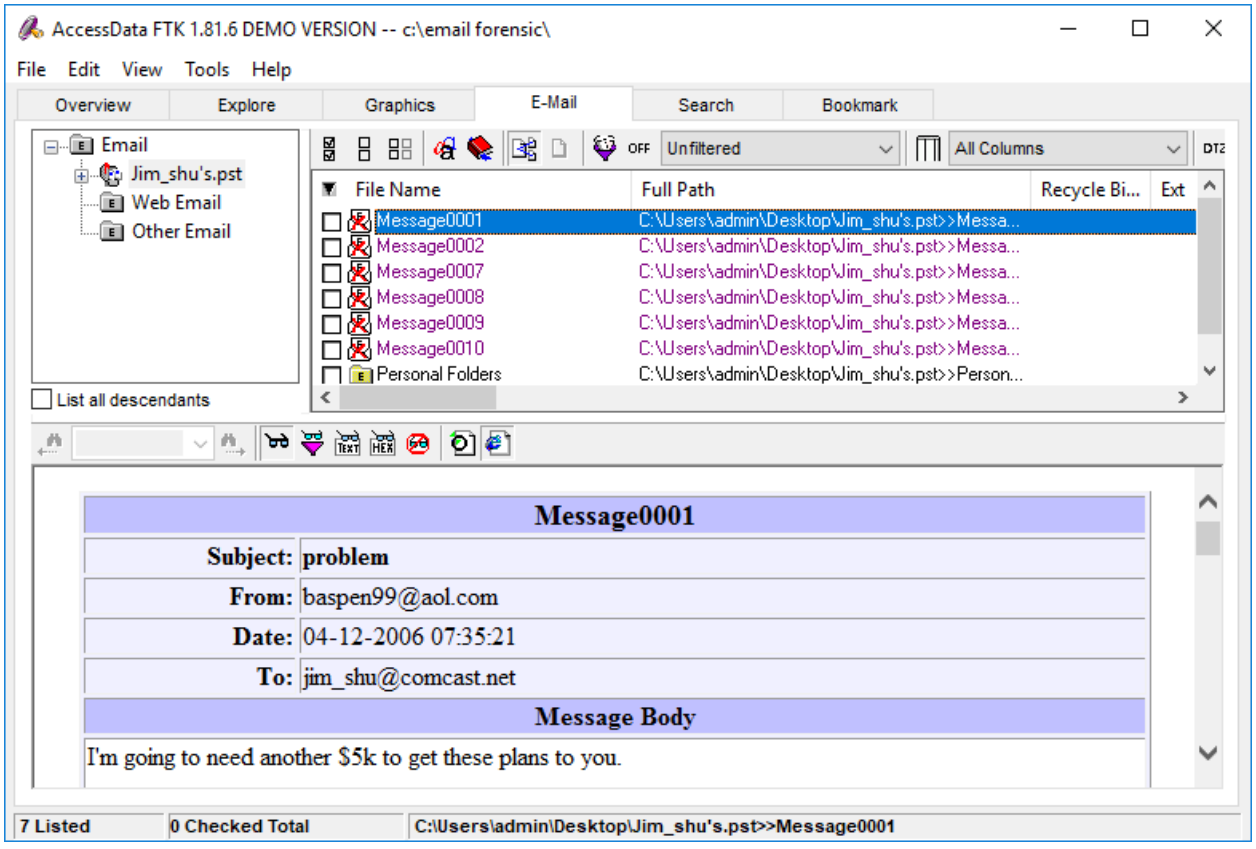
Step 10: Add the Evidence to the case.



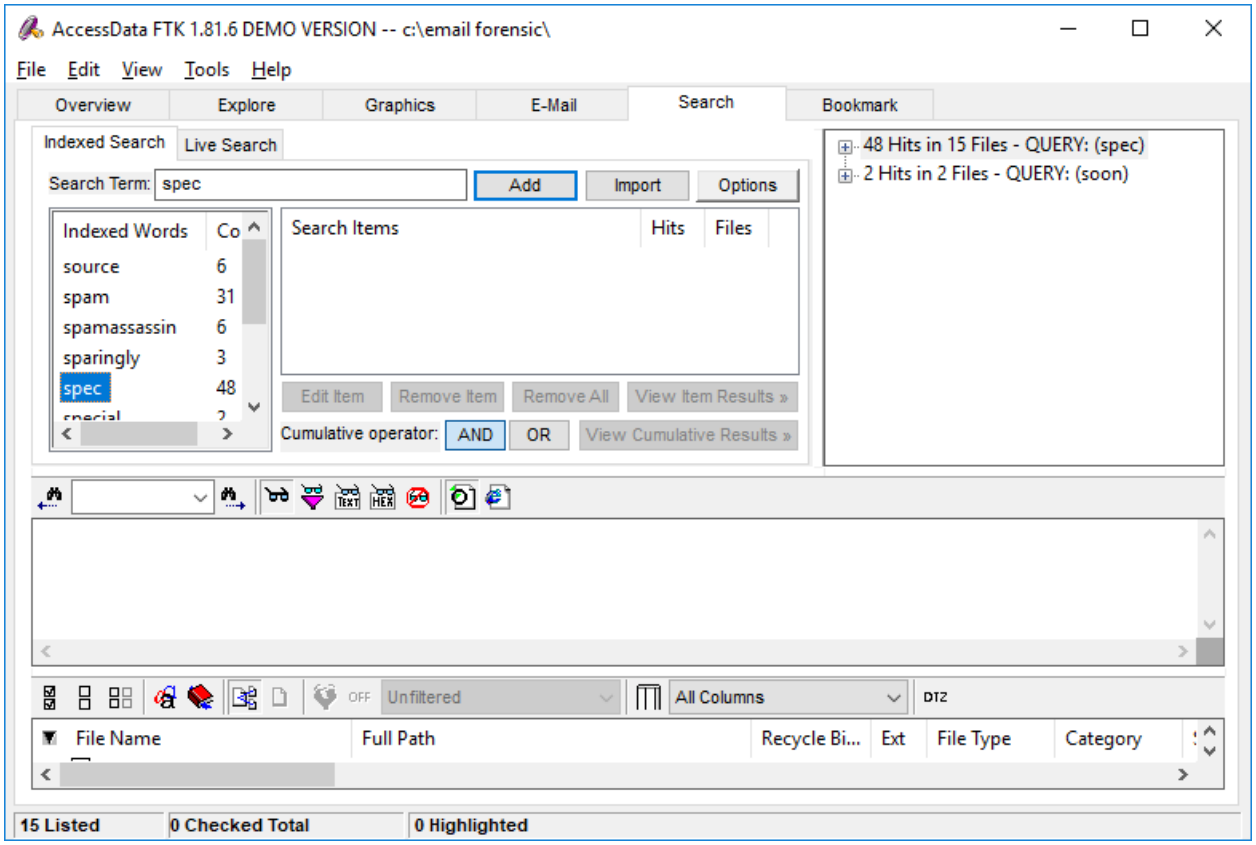
Step 11: Case Summary will be display.



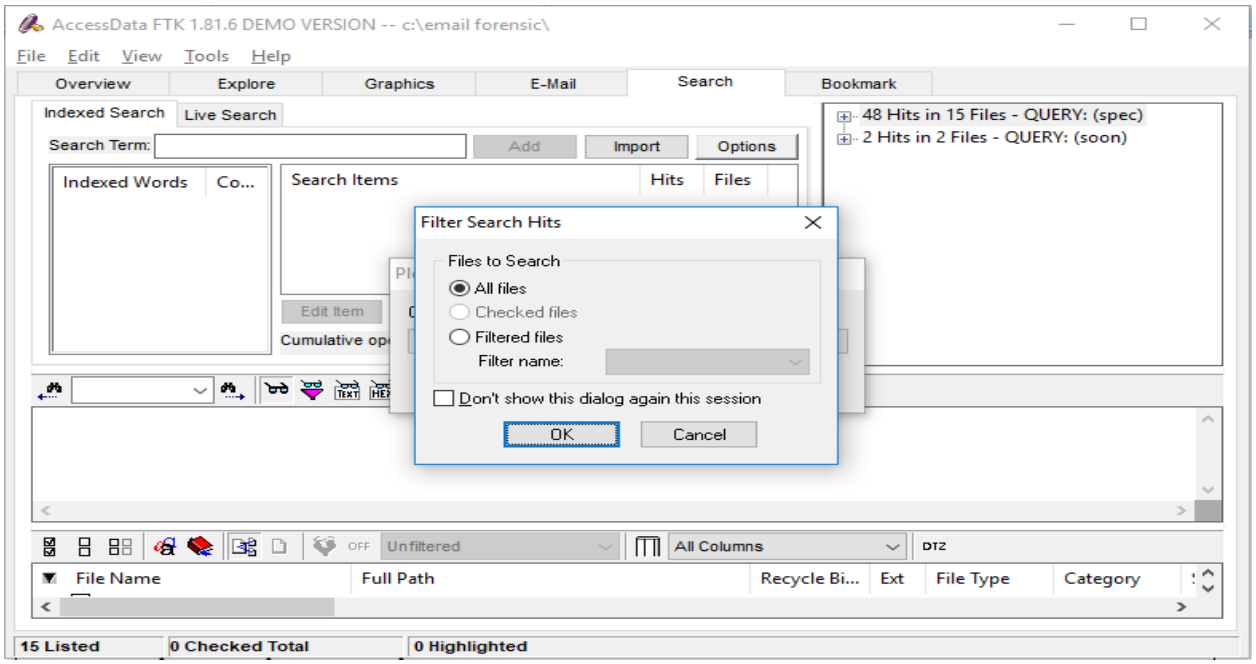
Step 12: Select any message, display will be shown.



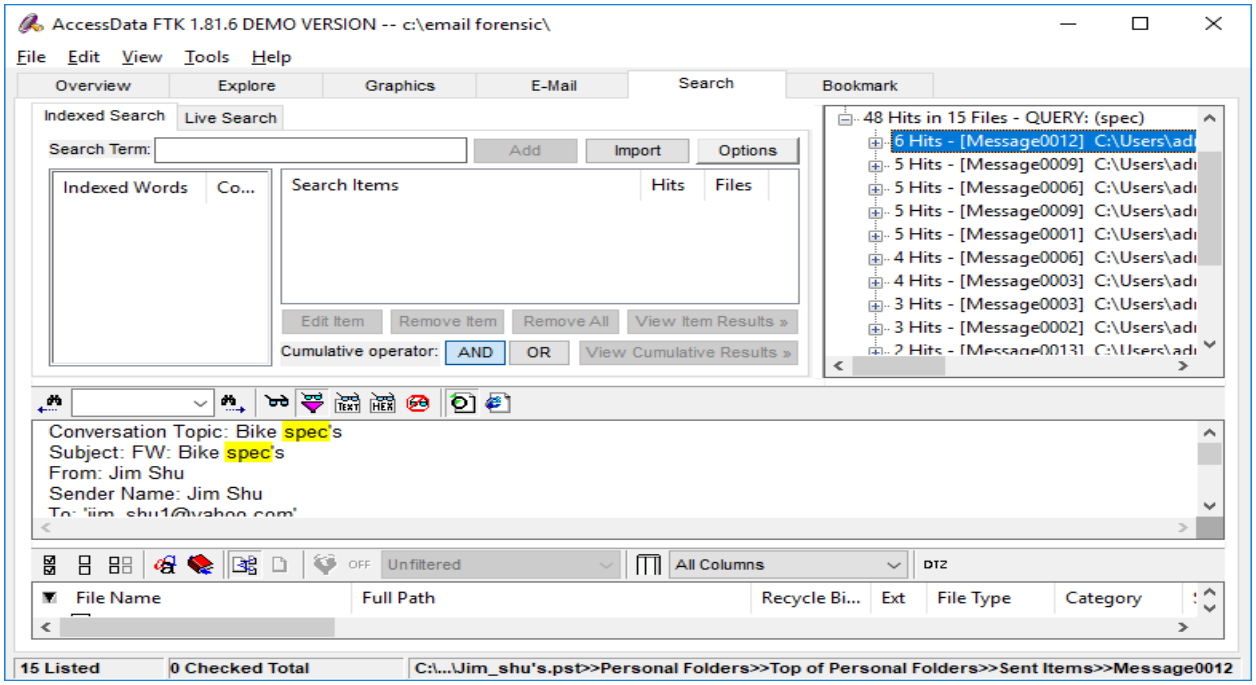
Step 13: Provide search item and click on Add.



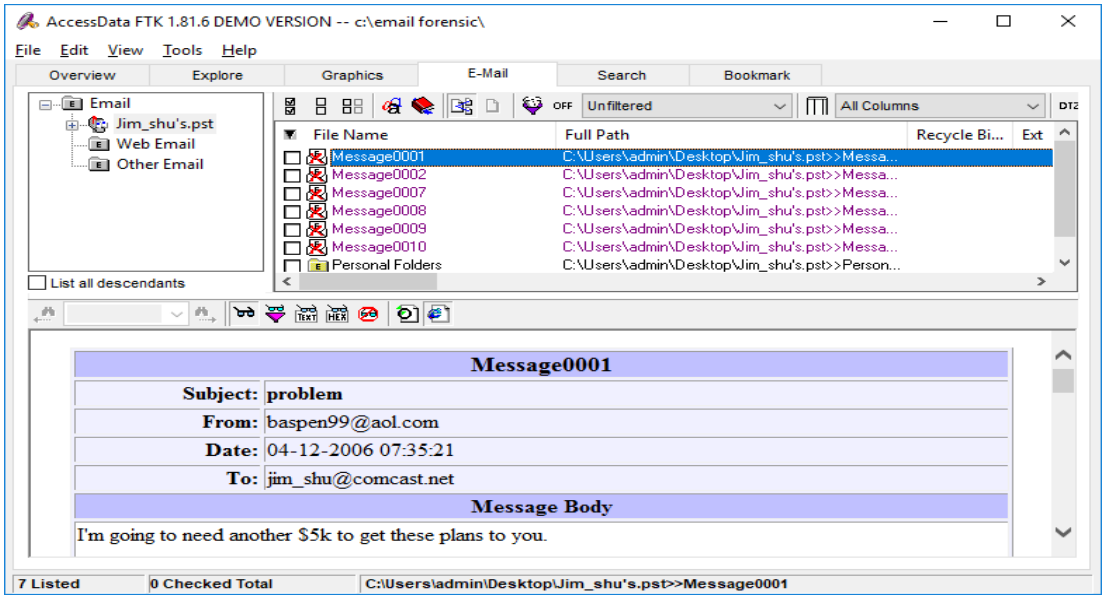
Step 14: Click filter to search.



Step 15: Keyword will be searched and displayed.



Step 16: Exporting will be finished



Conclusion: Thus we have performed email forensic successfully.

Assessment No. 05

Aim: Web Browser Forensics

1. Web Browser working
2. Forensics activities on browser
3. Cache/ cookies analysis
4. Last internet activity

Theory:

1. **Web Browser working:**

Architecture of a Browser: The browser's main functionality is to fetch the files from the server and to display them on the screen. It basically displays html files containing images, PDF, videos, flashes, etc in an ordered layout. A browser is a group of structured codes that performs plenty of tasks to display a webpage on the screen. These codes are separated in to different components according to their tasks performed. The structure of a browser is shown in the below image.

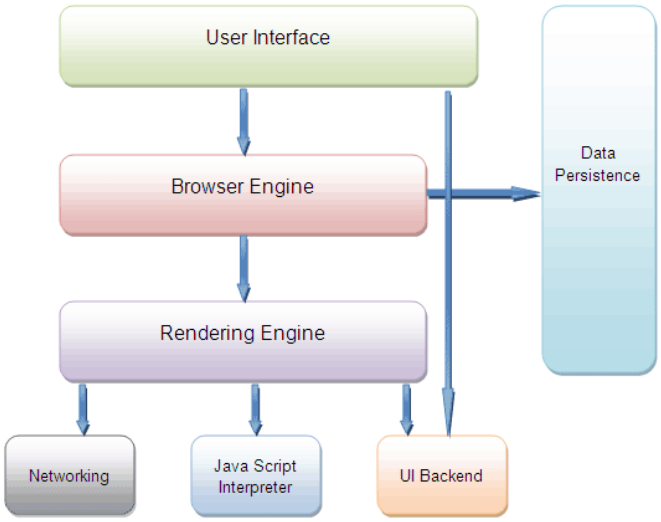


Fig. 2: Block Diagram Showing Web Browser Architecture

How Browsers work?

World Wide Web works on the client-server model. A user computer works as a client which can receive and send data to the server. When a web page is requested by a user, the browser contacts the requested server (where the website is stored) and by fetching and interpreting the requested files, it displays the web page on the computer screen.

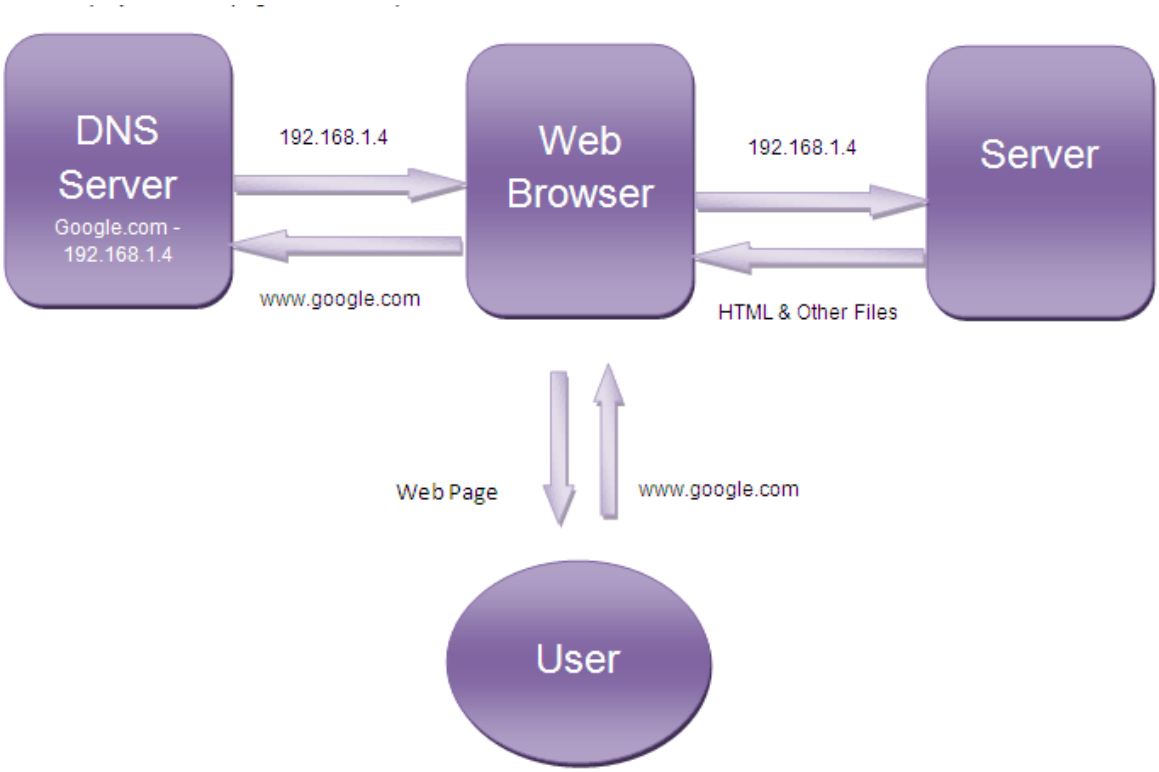


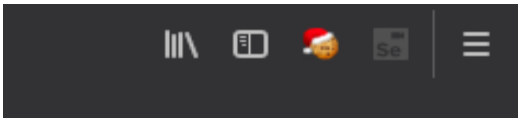
Fig. 3: Simple Block Diagram Showing Working of Web Browser

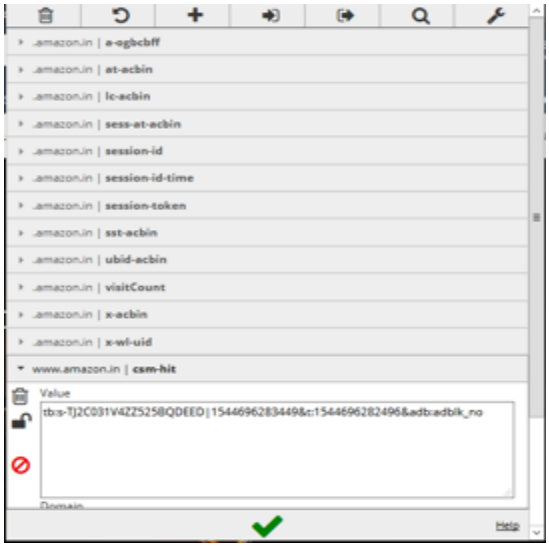
2. **Forensics activities on browser:**
   Both criminals as well as investigators use internet. Web browser is used by criminals to collect or inquire information for a new crime technique, to conceal his/her crime. Every moment criminal leaves the traces on computer while using web browser. This proof is found in the browser history, temporary files, index.dat, cookies, download files, unallocated space and the cache etc. In this paper, we studied major tools used for web browser analysis. Also, we compare them and find out its benefits and limitations.

Example Session Impersonation using Firefox:

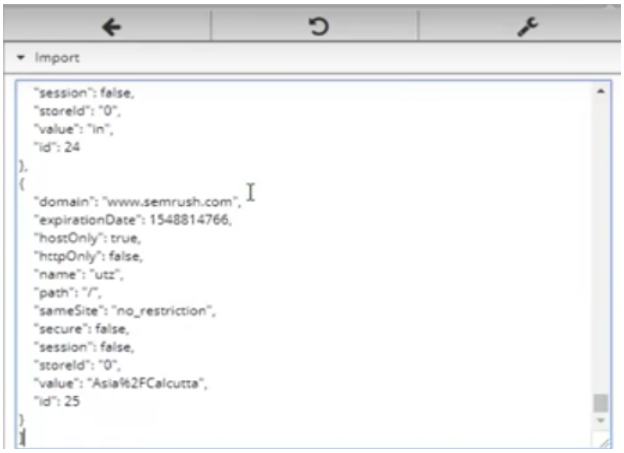
STEPS:

1. Open FireFox
2. Go to Tools > Addons > Extension
3. Search and install EditThisCookie or Cookie Import/Export or any other Cookie tool
4. Then Click on Cookie extension to get cookie
5. Open a Website and Login and then click on export cookie





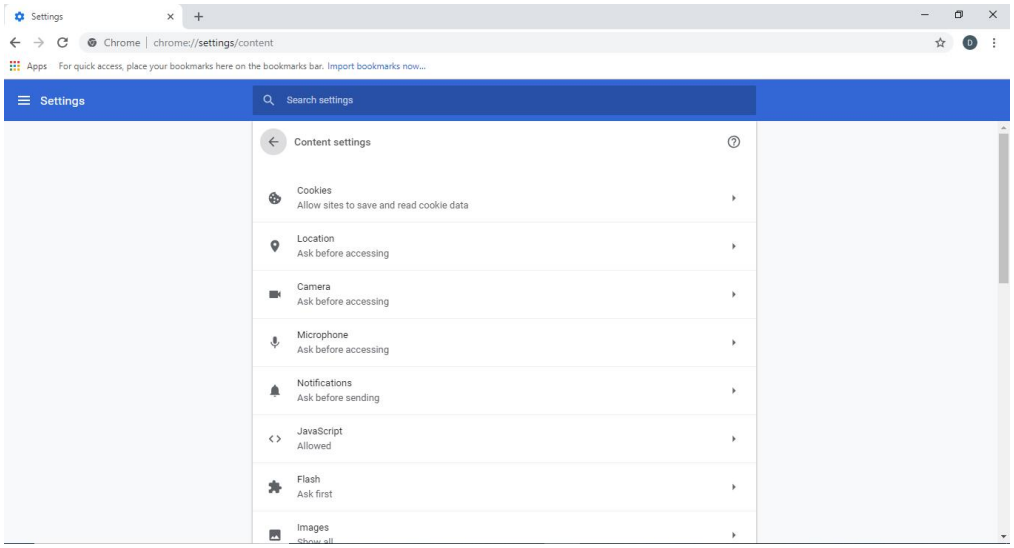
Paste the cookie in the tool which you have exported and click on green tick



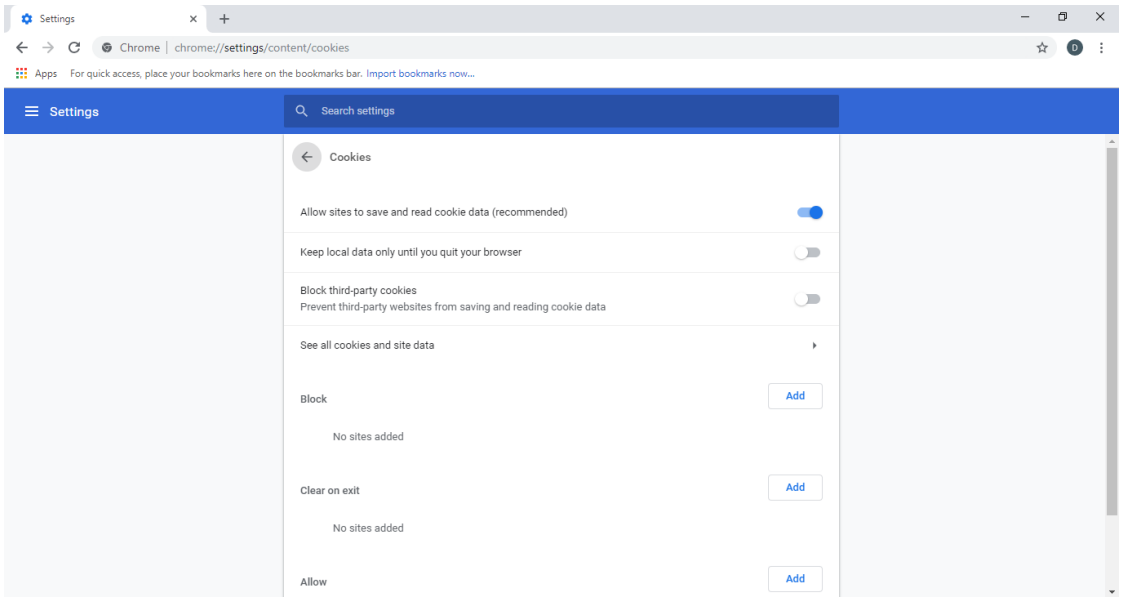
3. **Cache/ cookies analysis**

Chrome

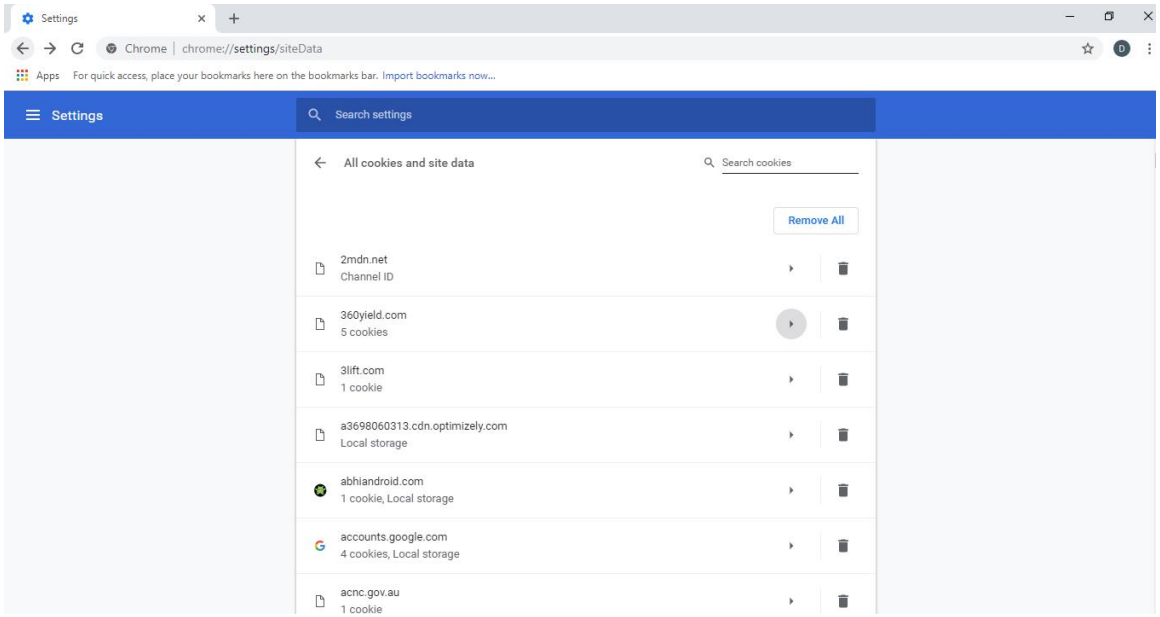
1. Select Settings from the top menu of the browser.
2. At the bottom of the page, click Show advanced settings
3. Under Privacy, select Content settings

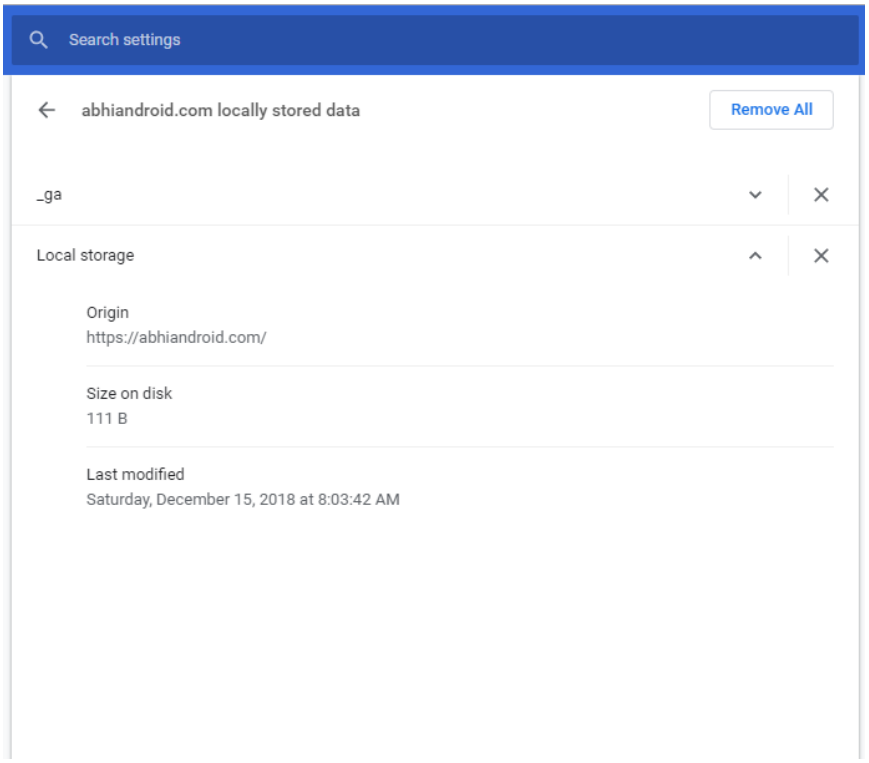


4. To manage cookie settings, check or uncheck the options under “Cookies”.



5. To view or remove individual cookies, click All cookies and site data...



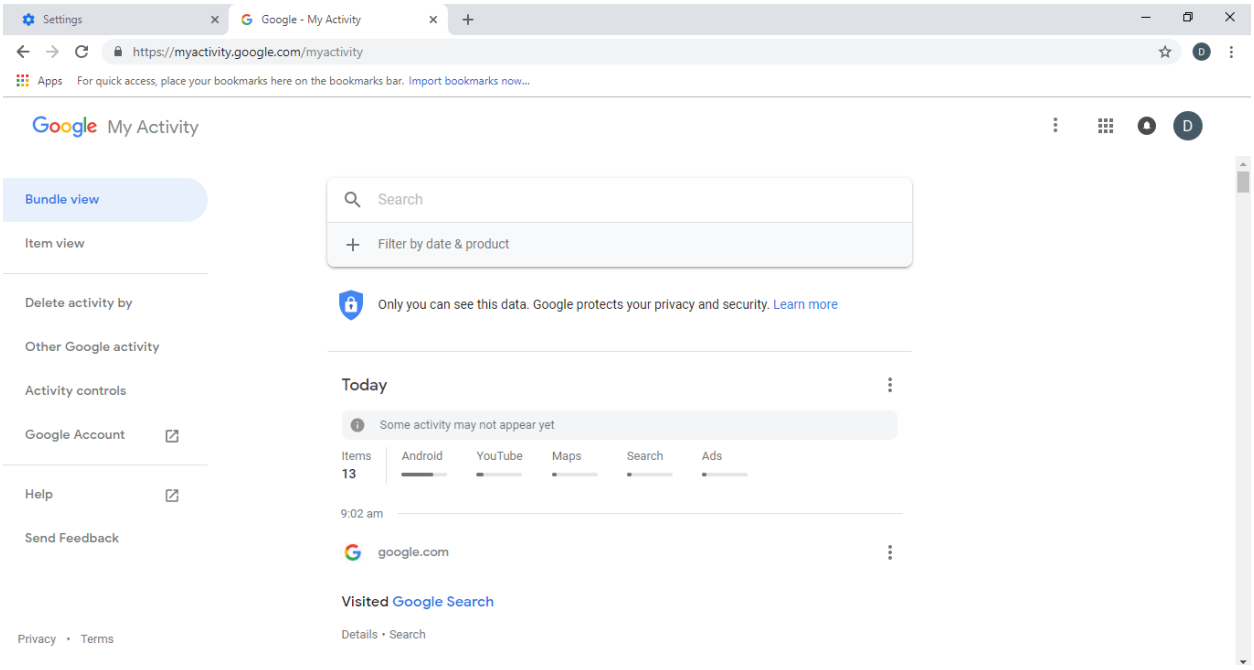


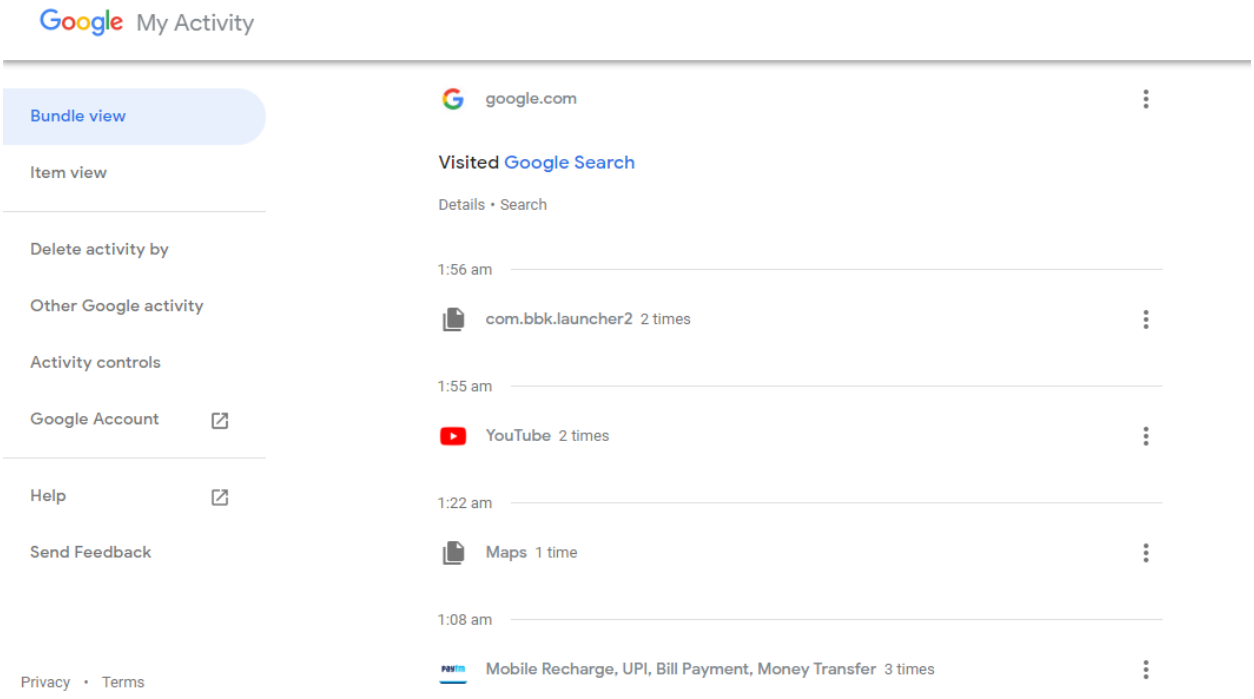
4. Last internet activity:

Method 1: 1.To check the last internet activity enter the URL:

https://myactivity.google.com/myactivity

2. You will get the activities you performed.





Method 2:

1. Open Chrome
2. At the top right, click More
3. Click History > History
4. You can see all the past activities.

Conclusion: Thus we have successfully studied web browsing forensics.

Assessment No. 06

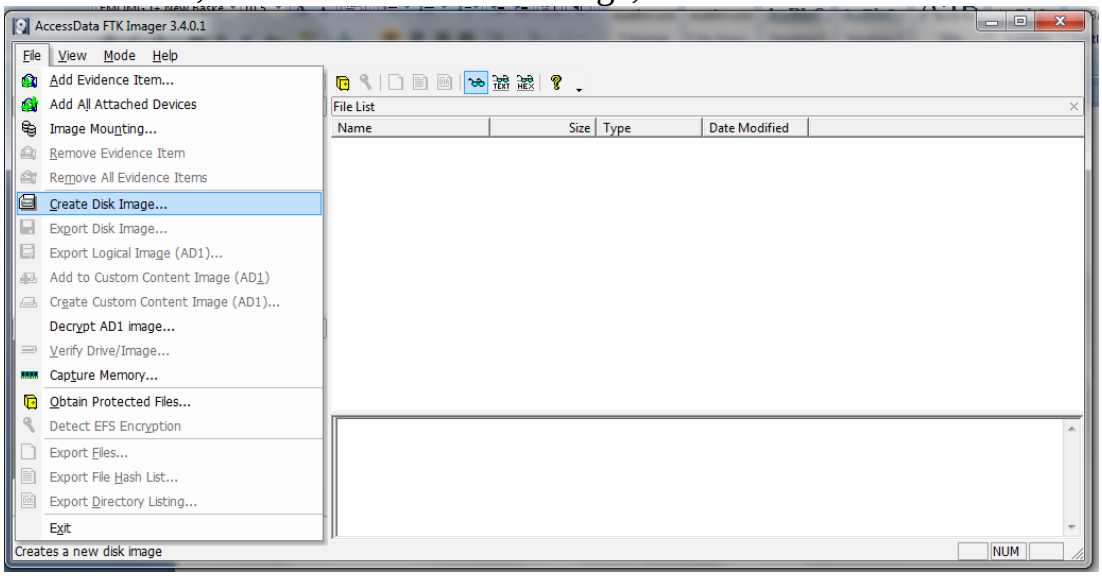
AIM: Creating Forensic Images FTK.

1. Create a copy of Image.
2. Check Integrity of Image.
3. Analyze the Image.

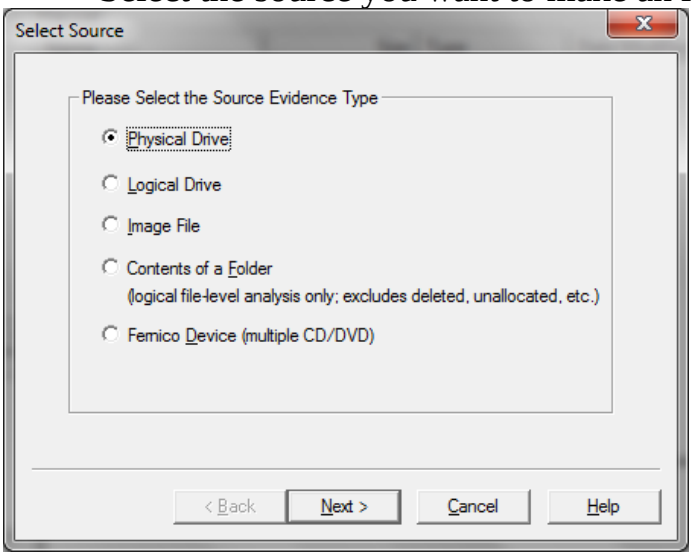
Description: Imager allows you to write an image file to a single destination or to simultaneously write multiple image files to multiple destinations.

- To create a forensic image:

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

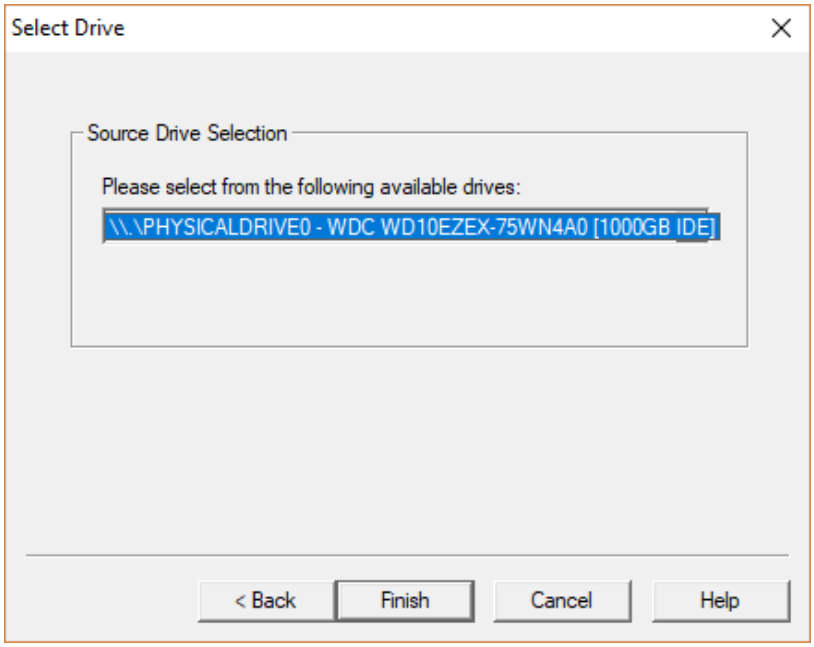


- Select the source you want to make an image of and click Next.

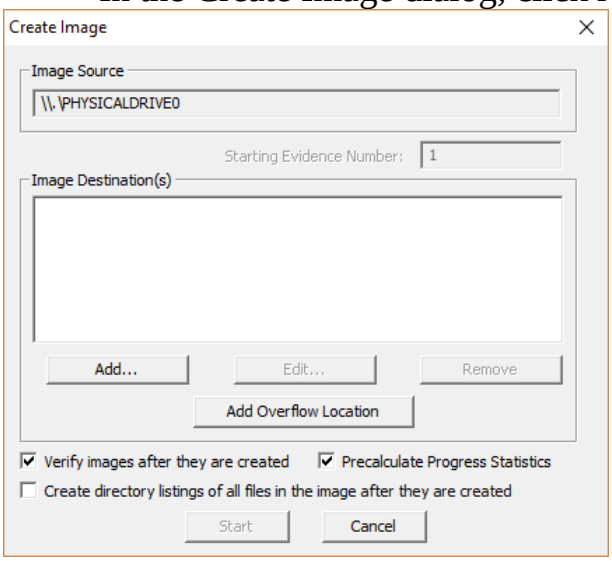


If you select Logical Drive to select a floppy or CD as a source, you can check the Automate multiple removable media box to create groups of images. Imager will automatically increment the case numbers with each image, and if something interrupts the process, you may assign case number manually.

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



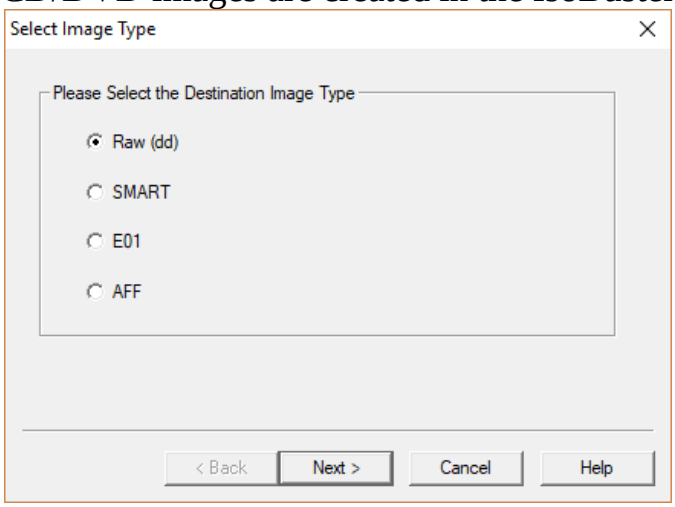
- In the Create Image dialog, click Add.



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.

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.

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

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

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

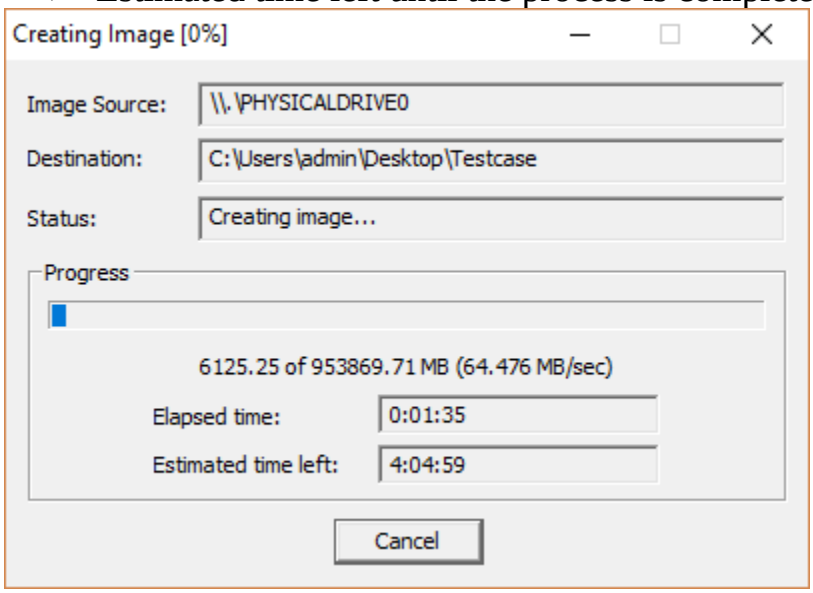
In the Image Fragment Size field, specify the maximum size in MB for each fragment of the image file. The s01 format is limited by design to sizes between 1 MB and 2047 MB (2 GB). Compressed block pointers are 31- bit numbers (the high bit is a compressed flag), which limits the size of any one segment to two gigabytes. Tip: If you want to transfer the image file to CD, accept the default fragment size of 650 MB.

- Click Finish. You return to the Create Image dialog.

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.

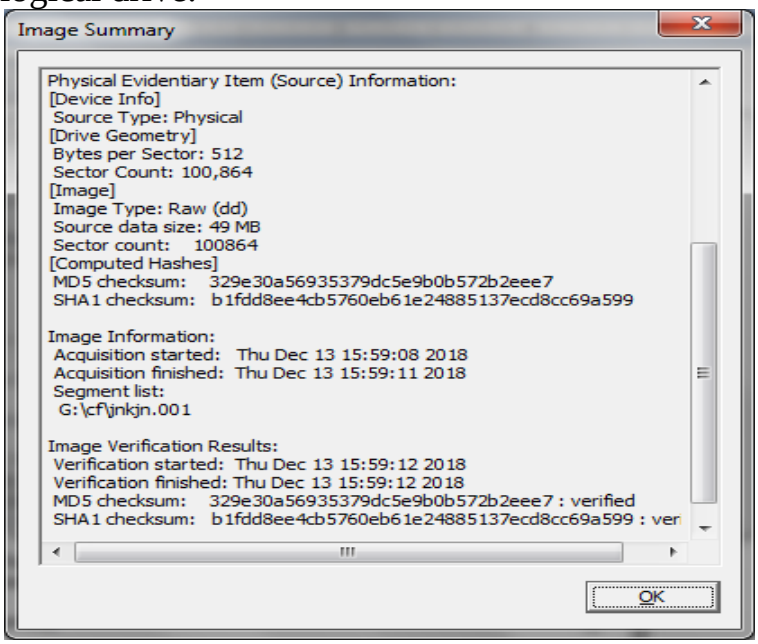
- Click Start to begin the imaging process. A progress dialog appears that shows the following:
  - The source that is being imaged
  - The location where the image is being saved
  - The status of the imaging process
  - A graphical progress bar

- 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.

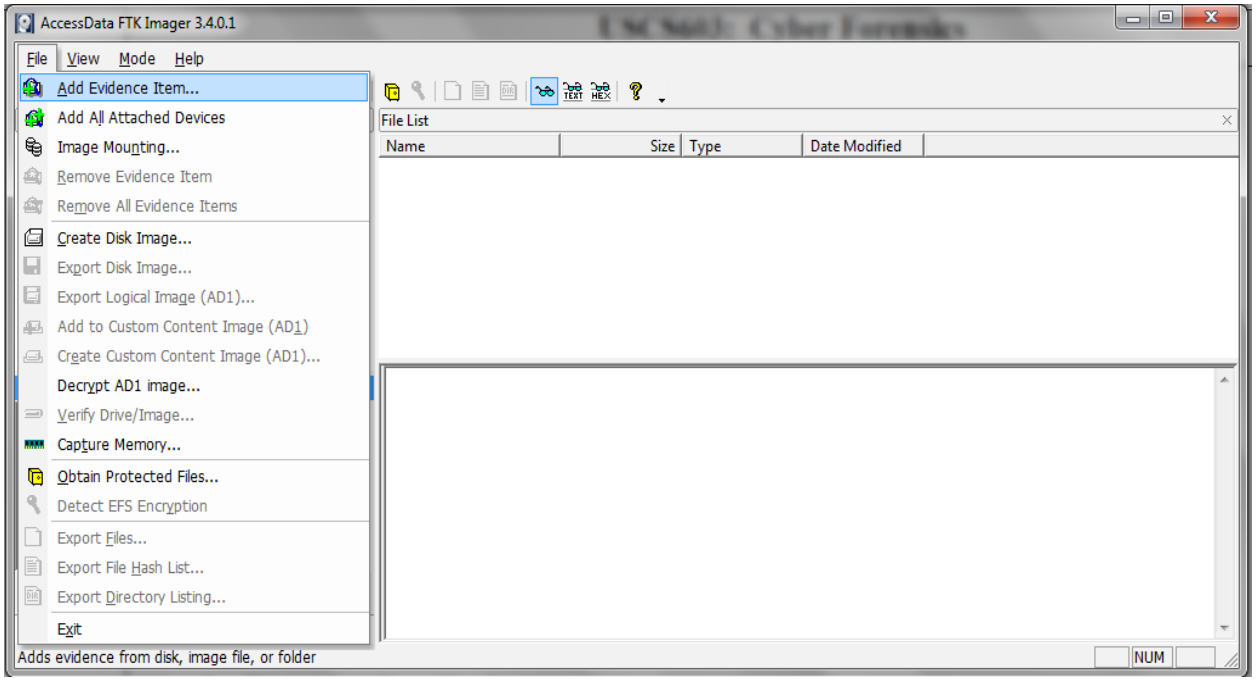
Note: This option is available only if you created an image file of a physical or logical drive.



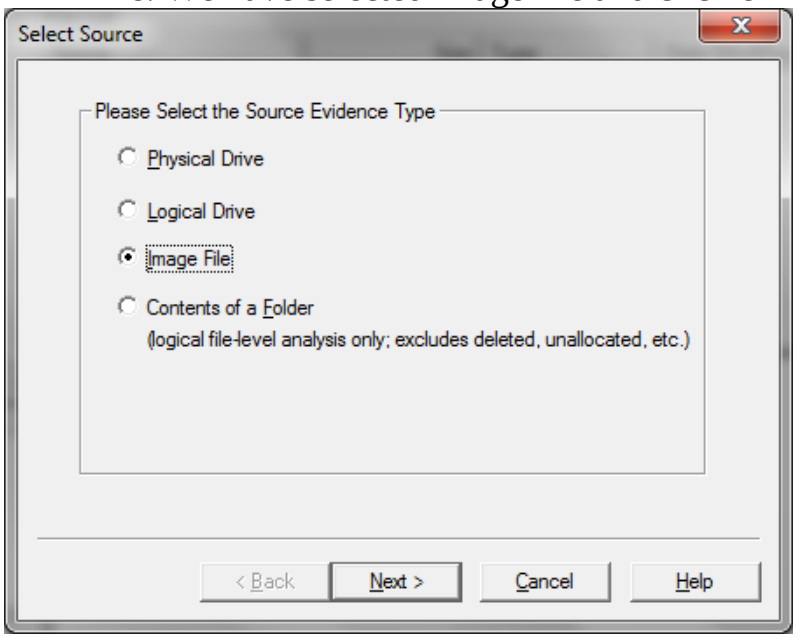
- When finished, click Close

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.

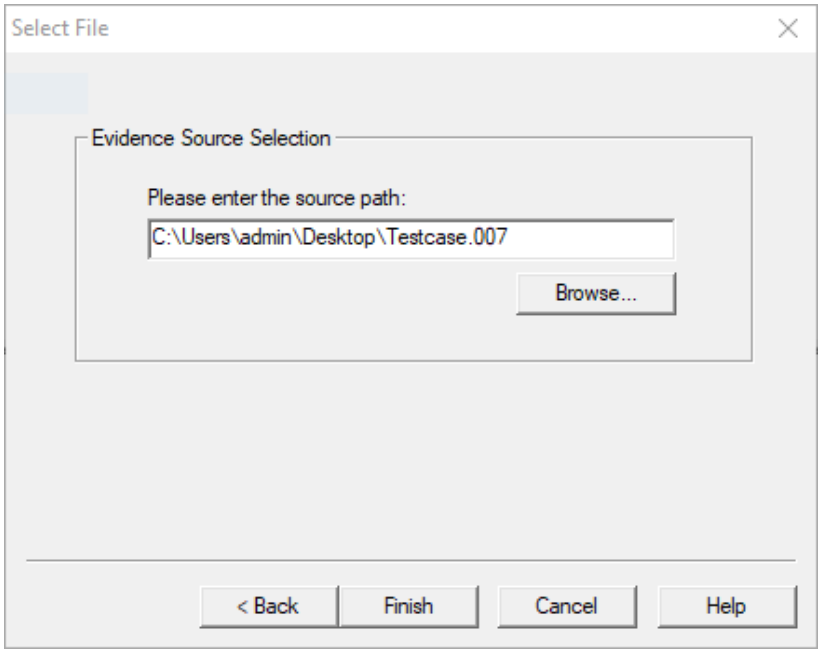
- Analyze Forensic Image:
- Click on Add Evidence Item to add evidence from disk, image file or folder.



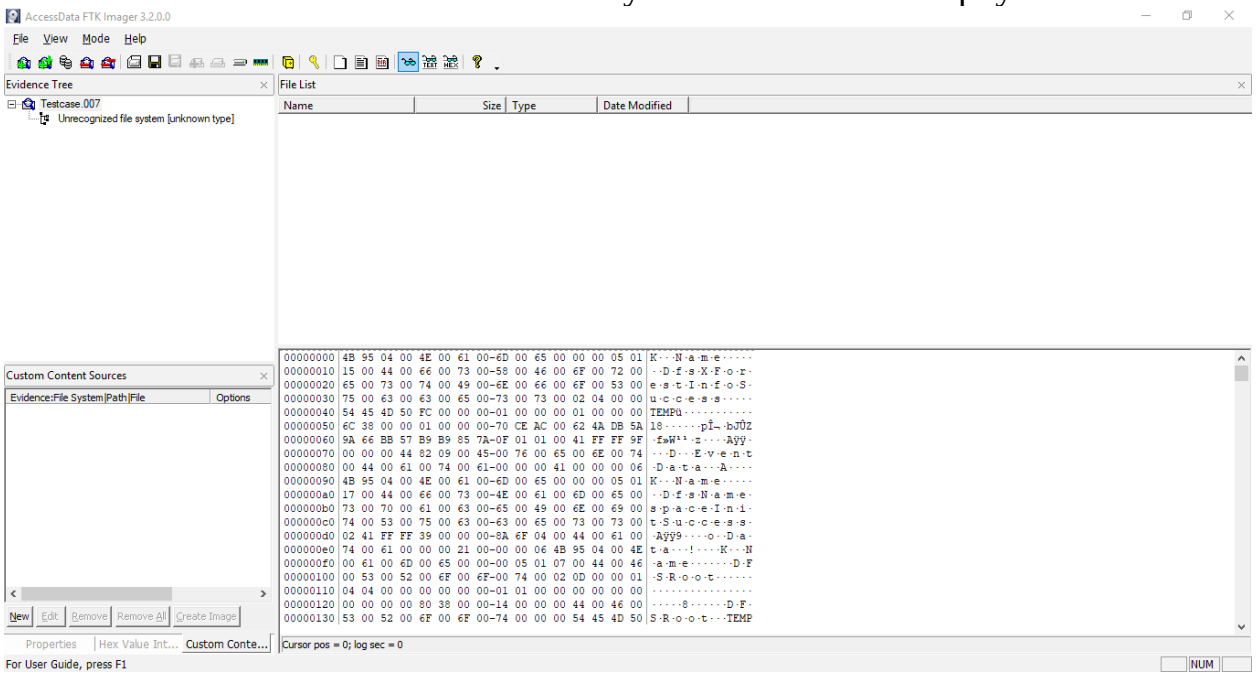
- Now select the source evidence type as physical drive, logical drive or image file. We have selected image file and click on next.



- 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.

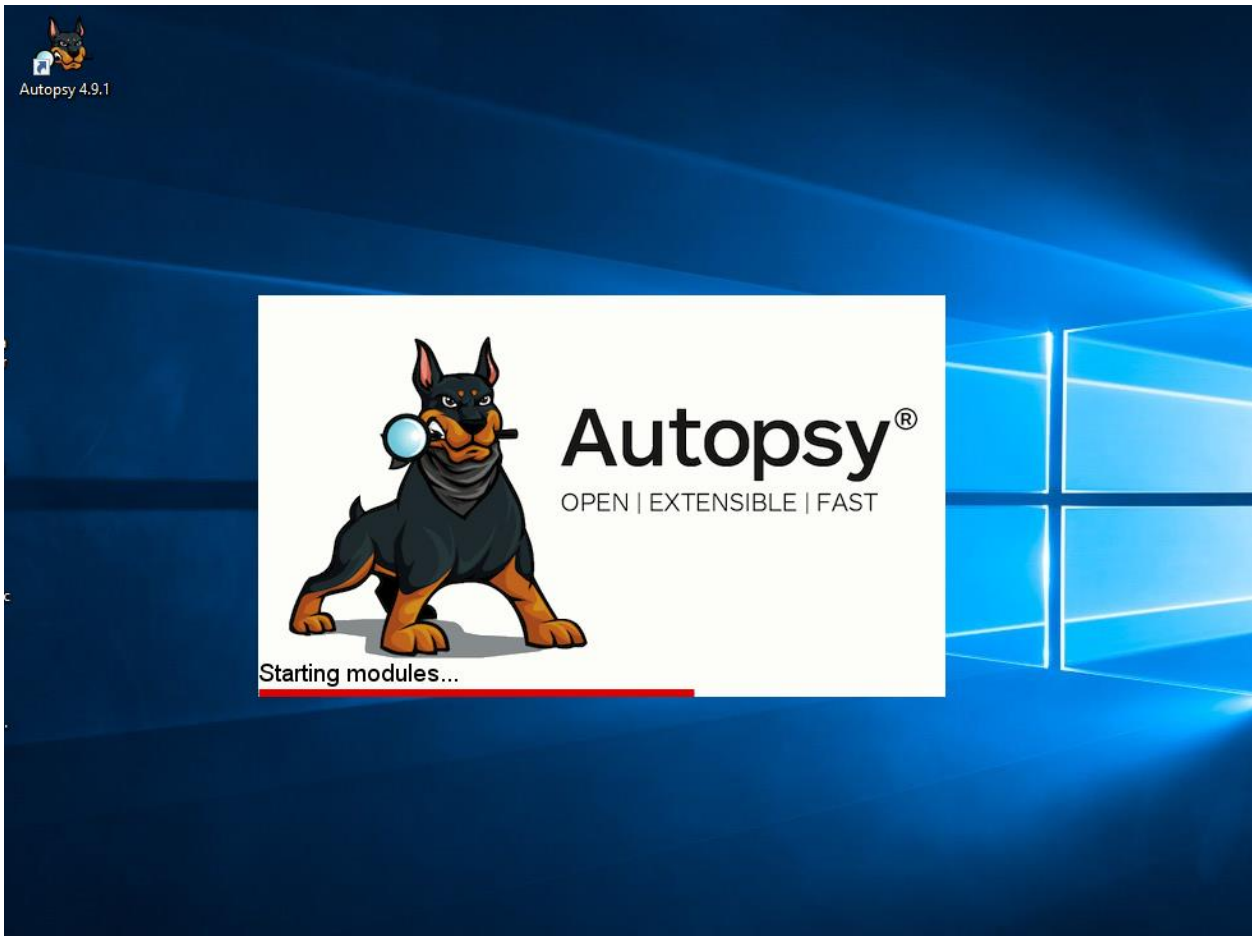
Conclusion: Now you have successfully added raw image as physical drive to analyze.

Assessment No. 07

Forensic Case Study

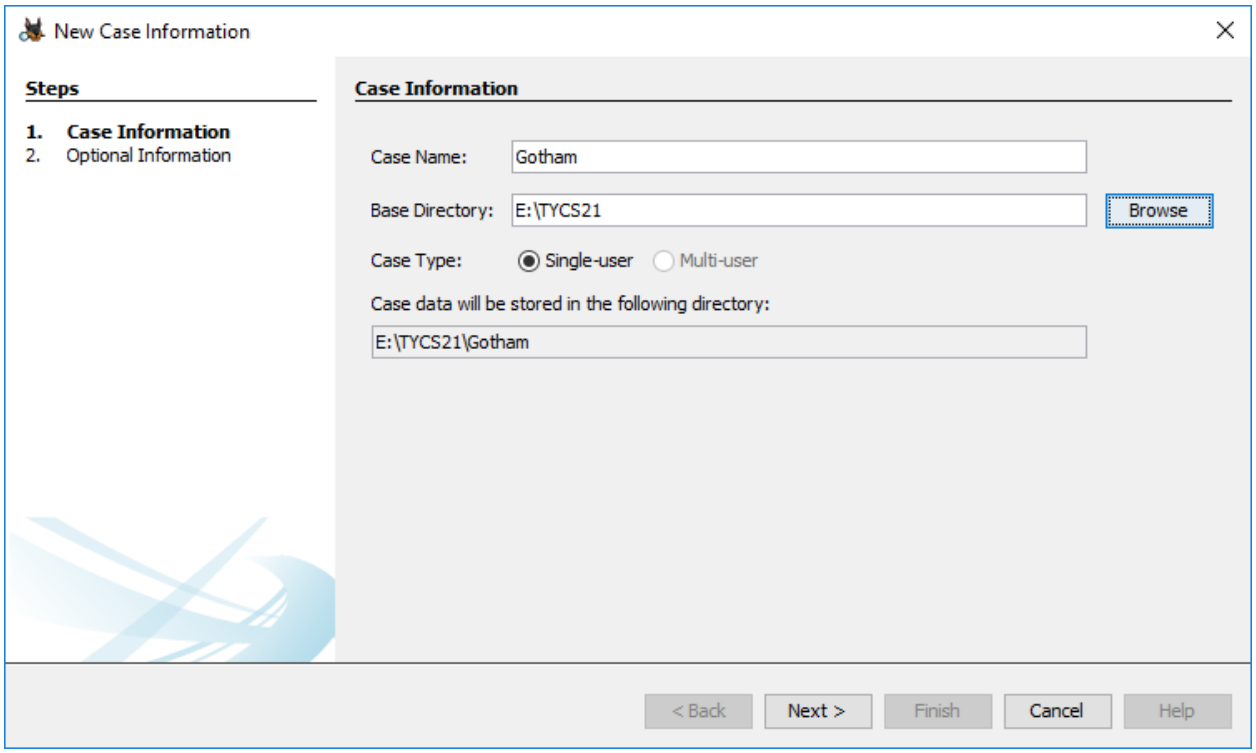
Aim: Solve the case study (Image File) provided in lab using Encase Imager or Autopsy.

Step 1: Start Autopsy from Desktop.

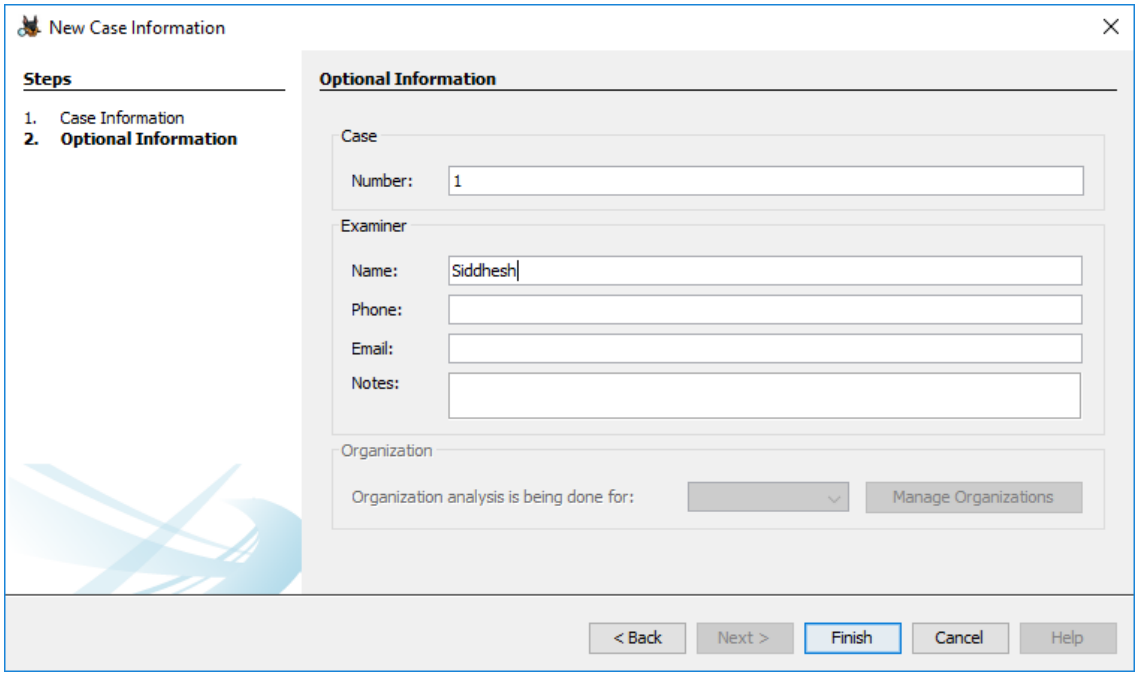


Step 2: Now Create on New Case

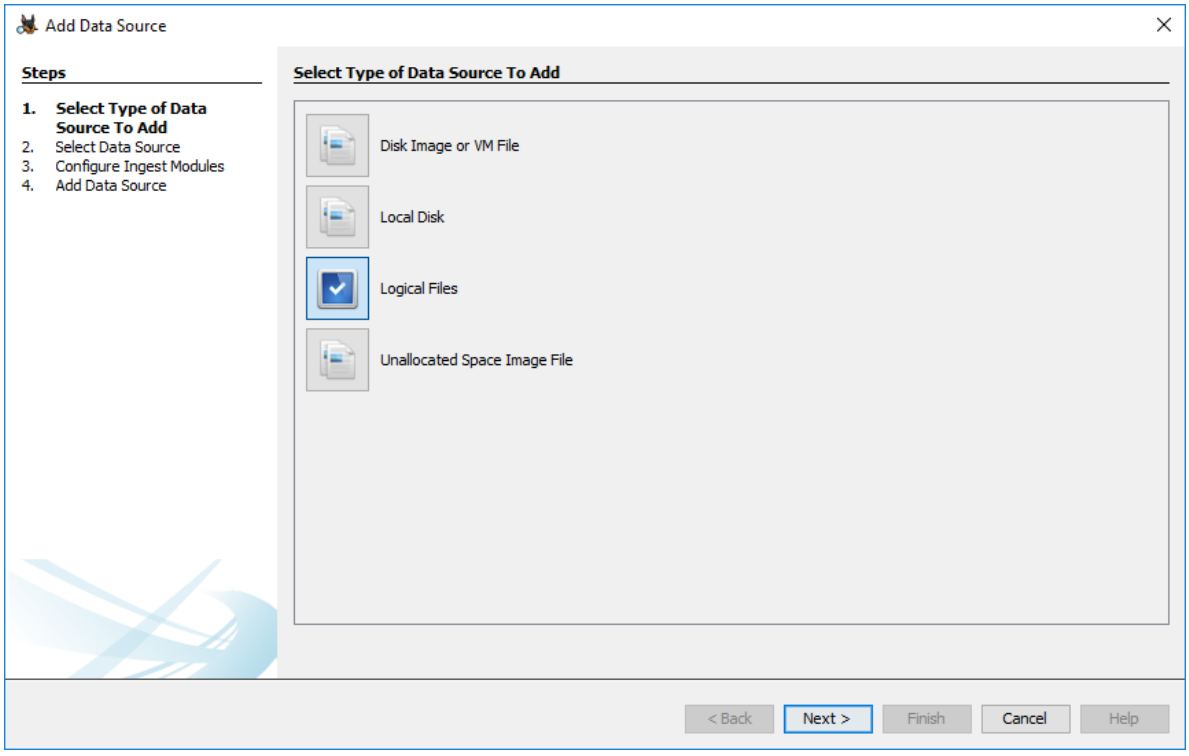
Step 3: Enter the New case information and Click on Next button.

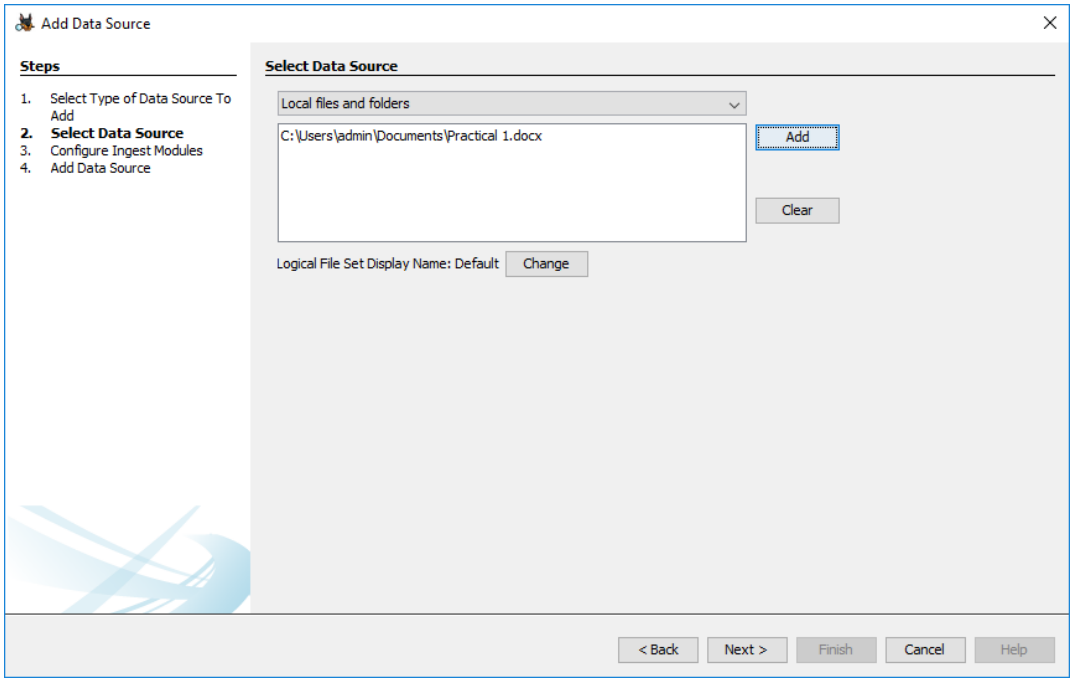


Step 4: Enter the additional information and click on Finish.

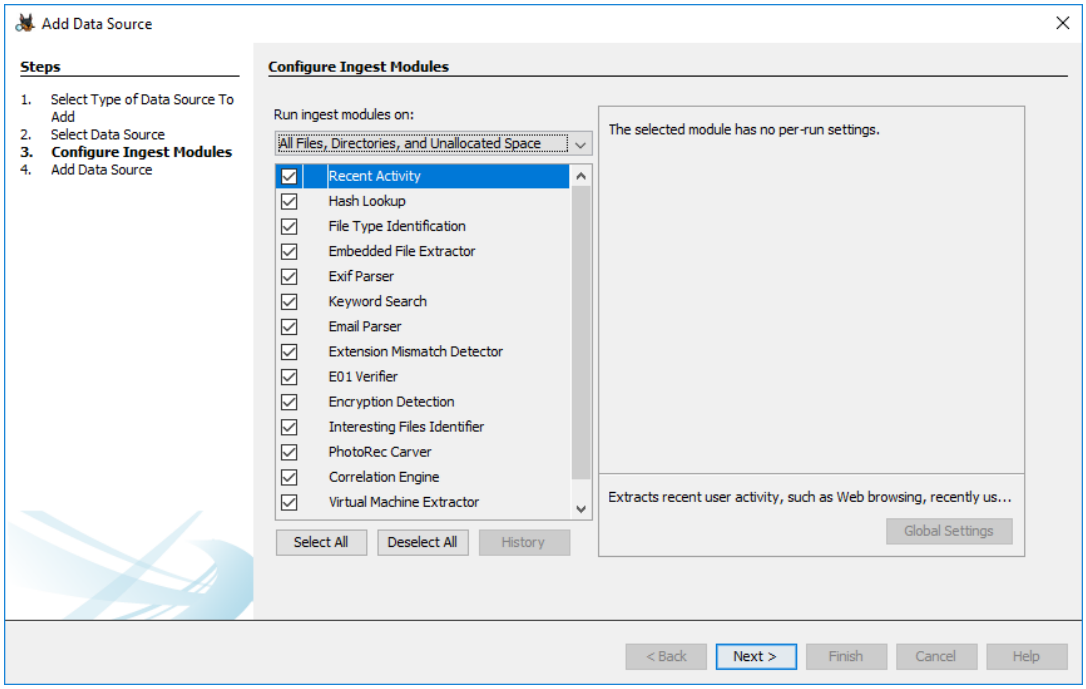


Step 5: Now Select Source Type as Local disk and Select Local disk form drop down list and click on Next.

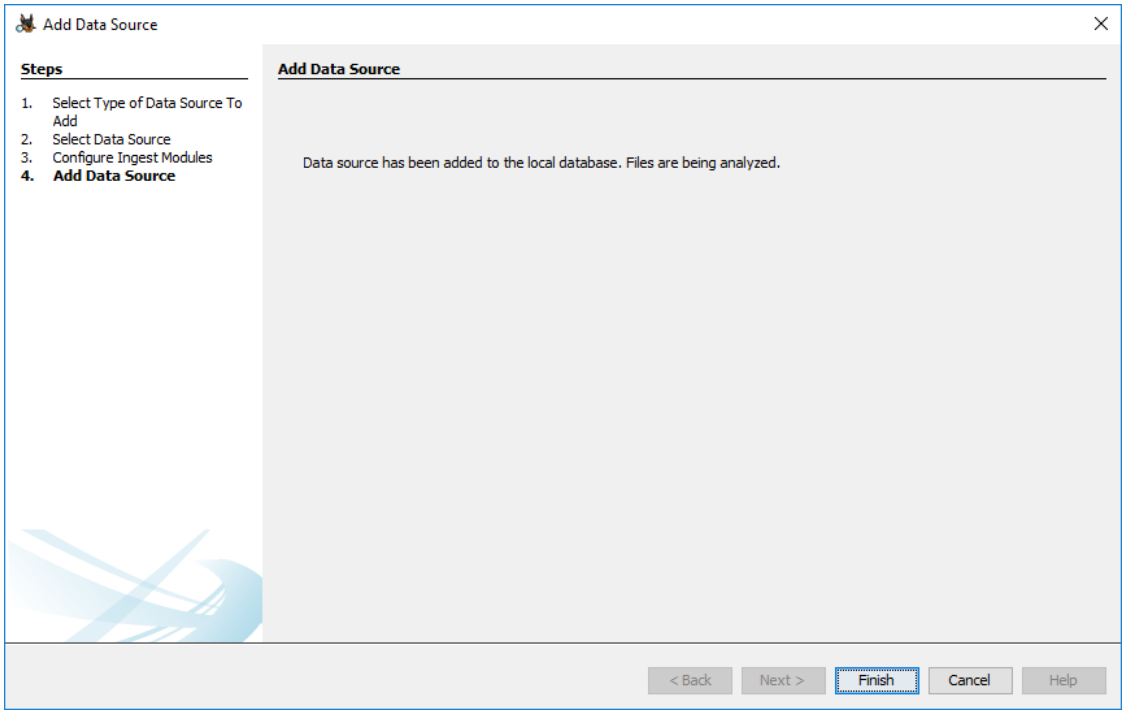


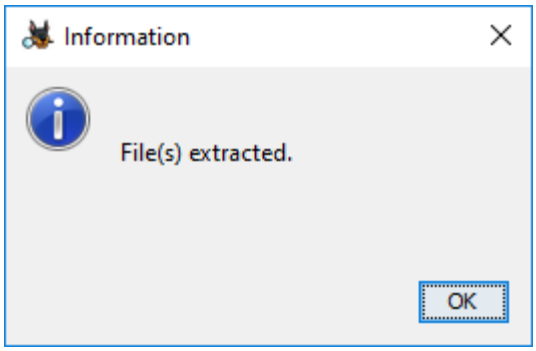


Step 6: Click on Next Button.

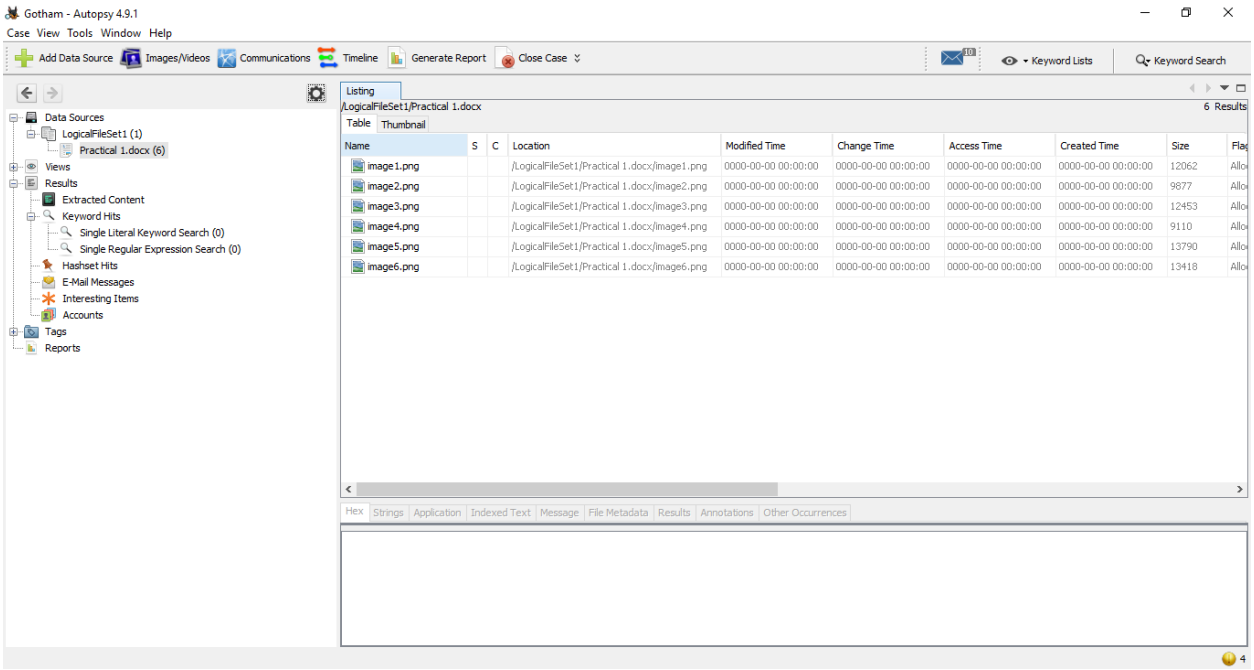


Step 7: Now click On Finish.

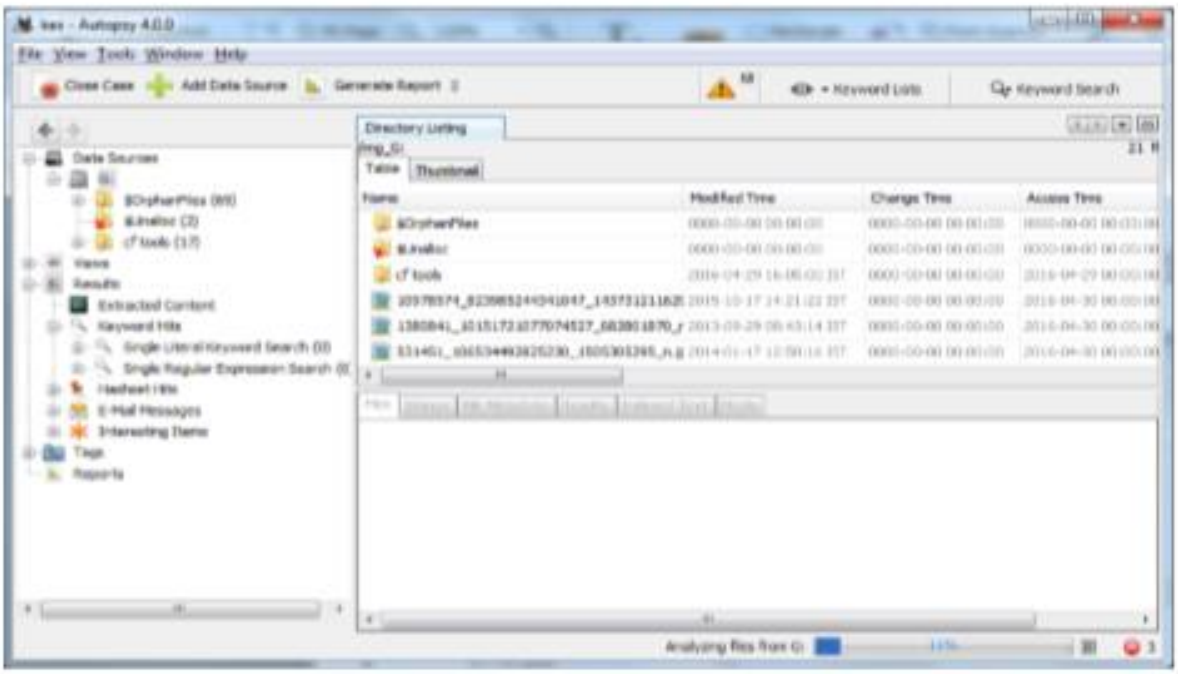




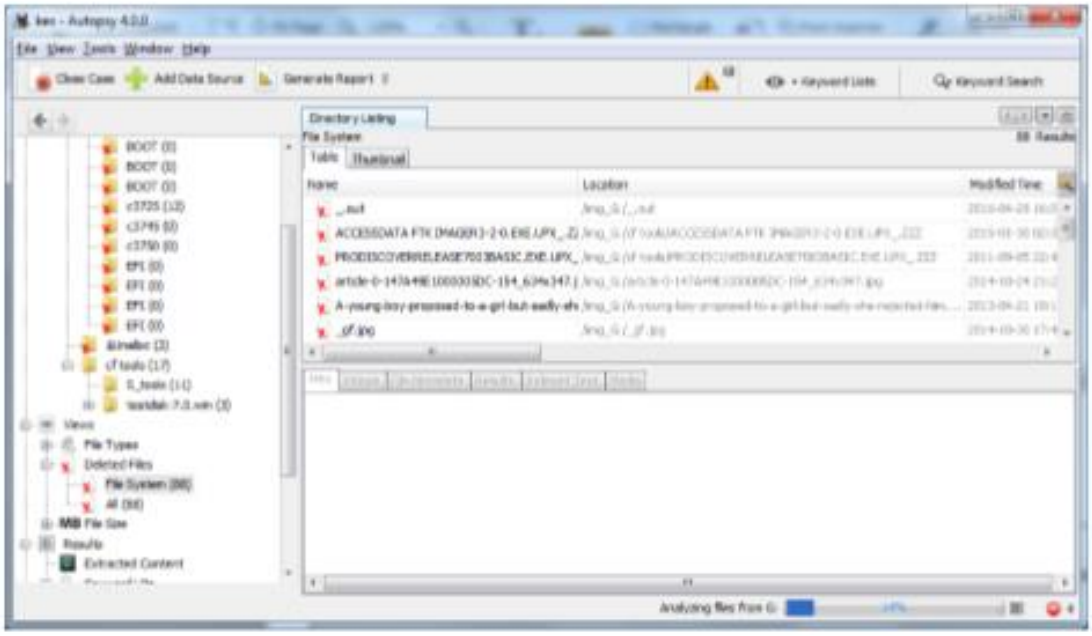
Step 8: Now Autopsy window will appear and it will analyzing the disk that we have selected.



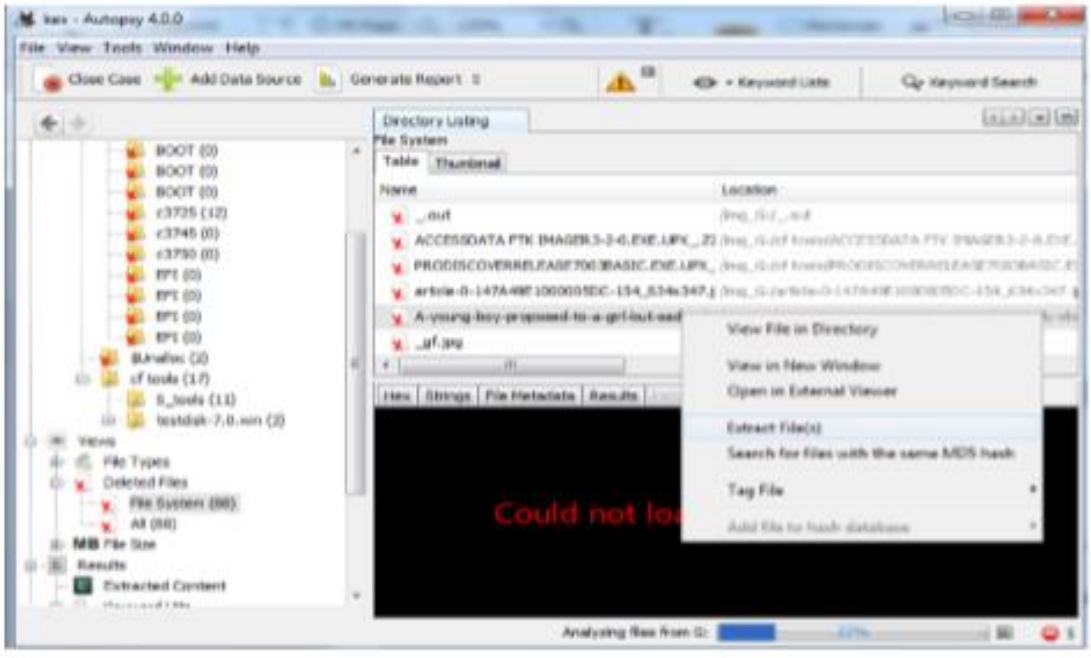
Step 9: All files will appear in table tab select any file to see the data.



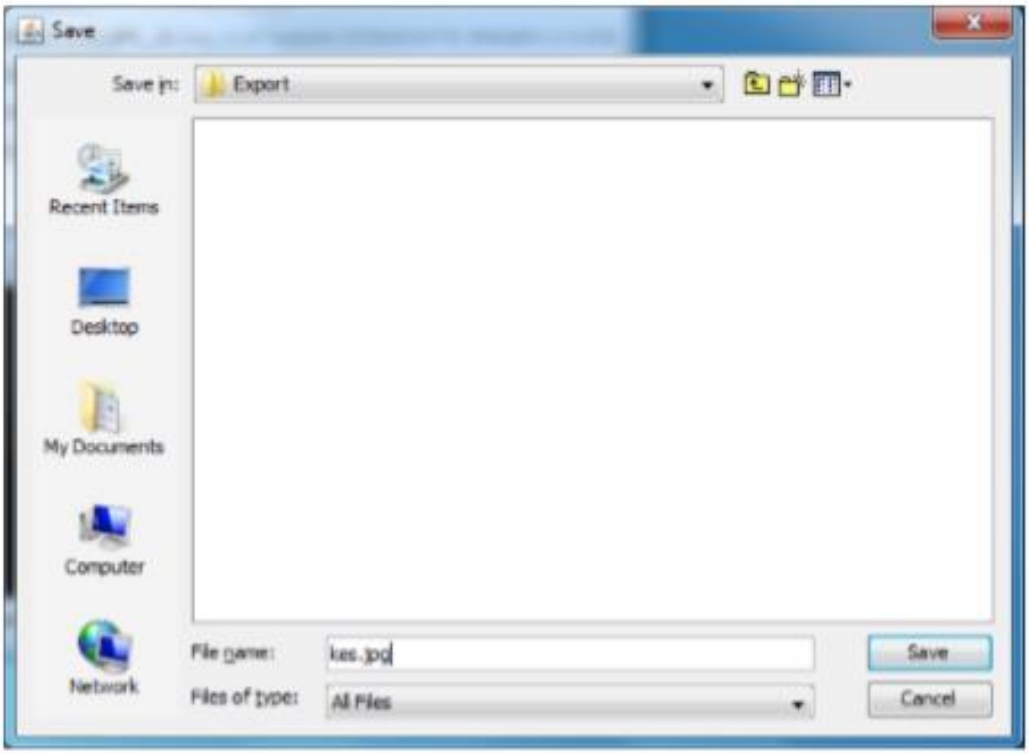
Step 10:Expand the tree from left side panel to view the document files.



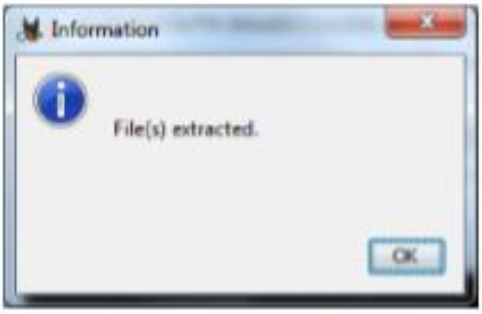
Step 11: To recover the file, go to view node-> Deleted Files node , here select any file and right click on it than select Extract Files option.



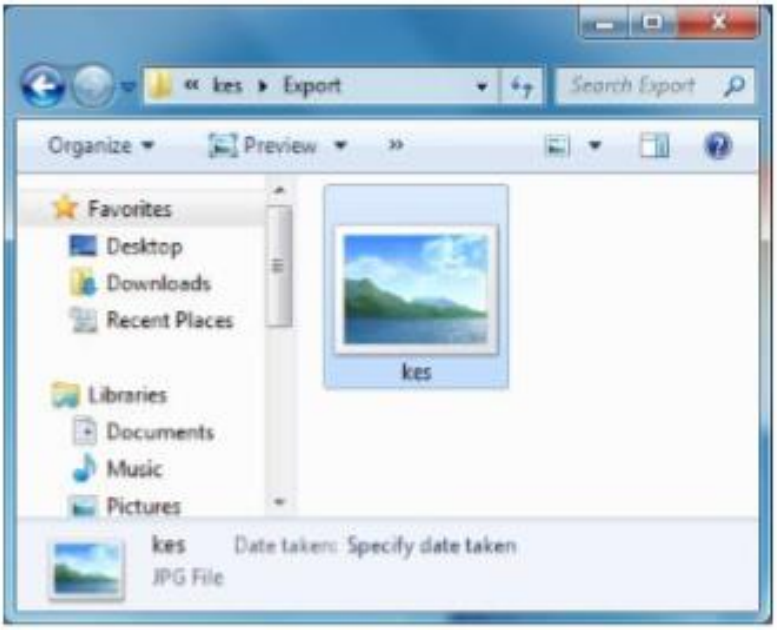
Step 12: By default Export folder is choose to save the recovered file.



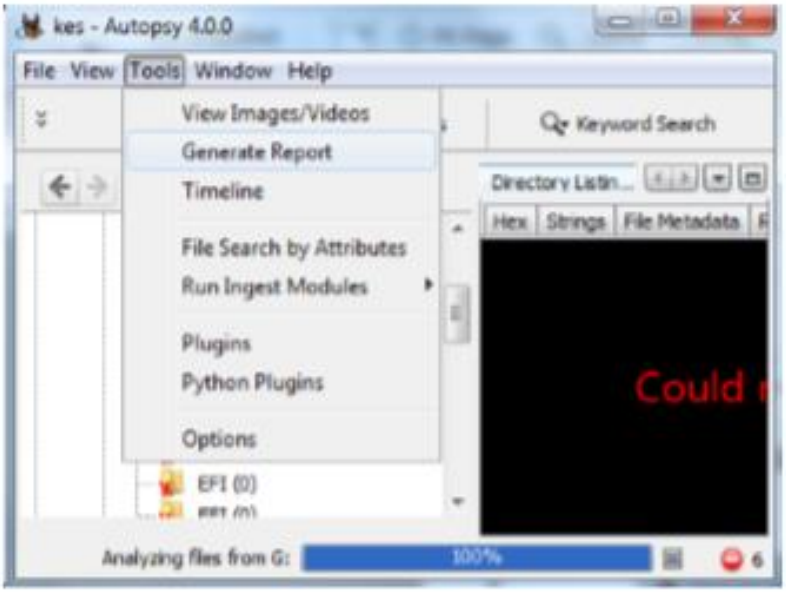
Sep 13 : Now Click on Ok.



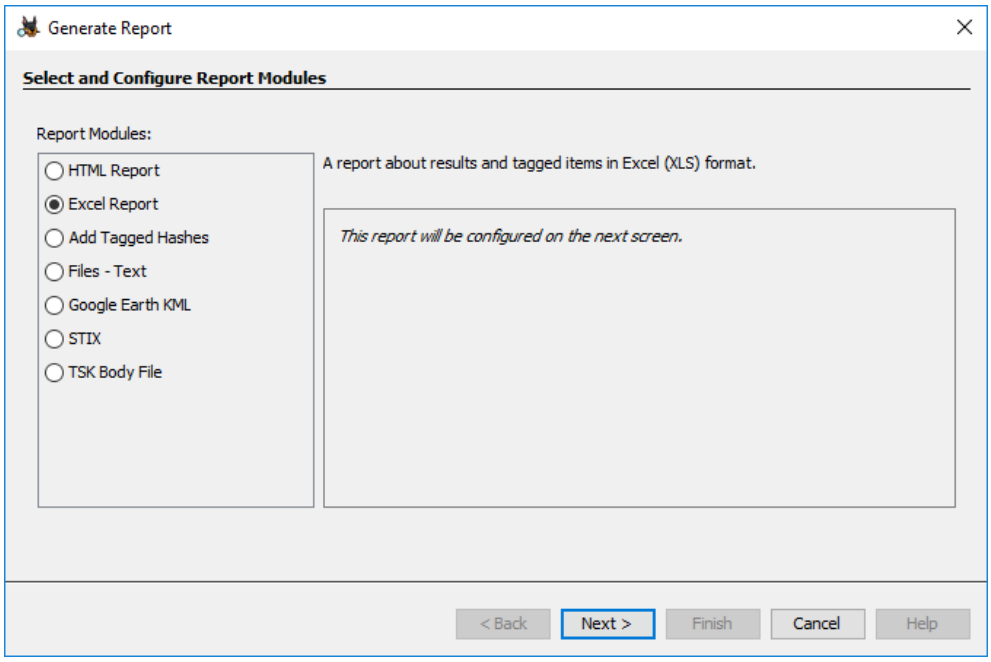
Step 14: Now go to the Export Folder to view Recover file.

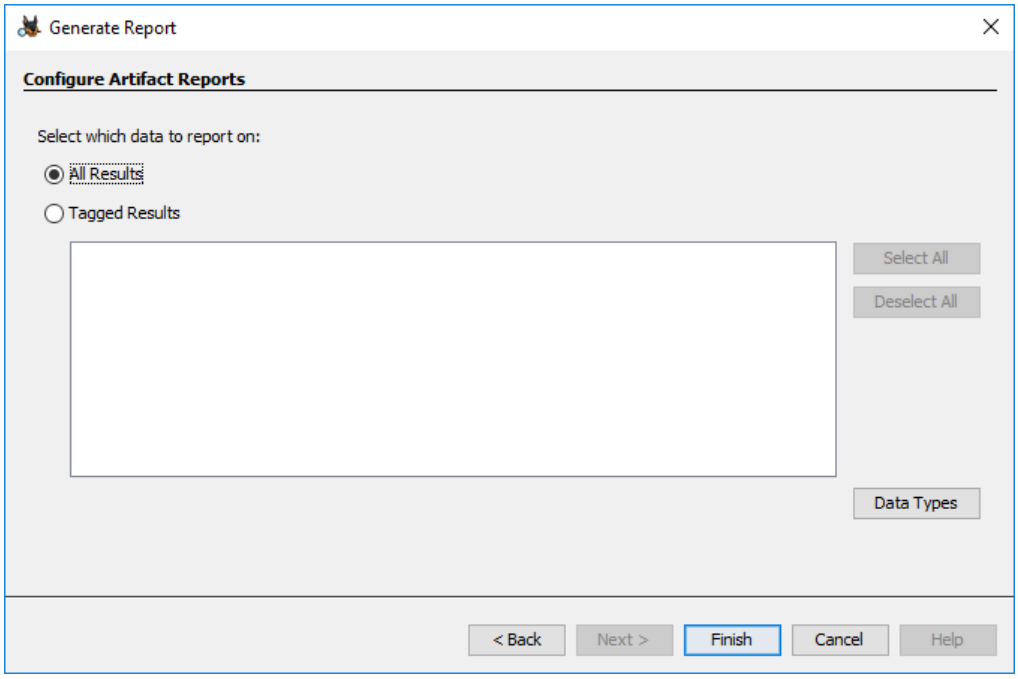


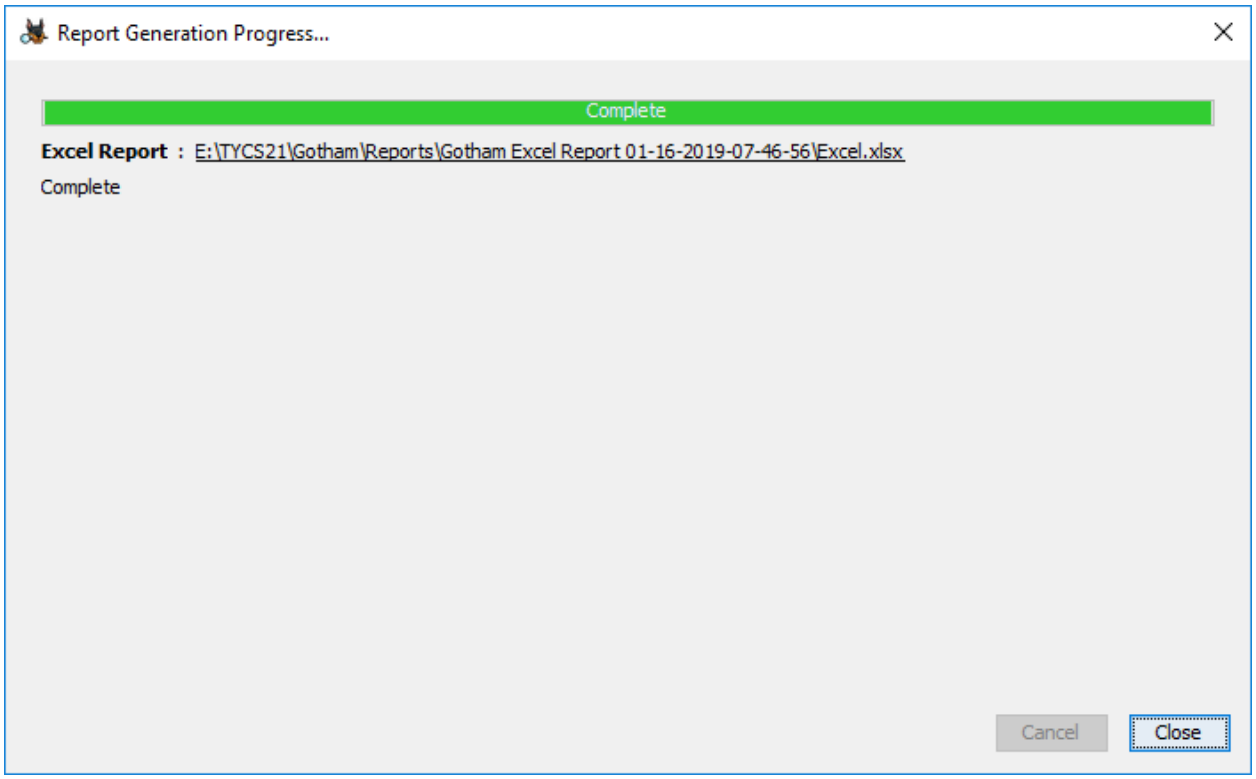
Step 15: Click on Generate Report from autopsy window and Select the Excel format and click on next.



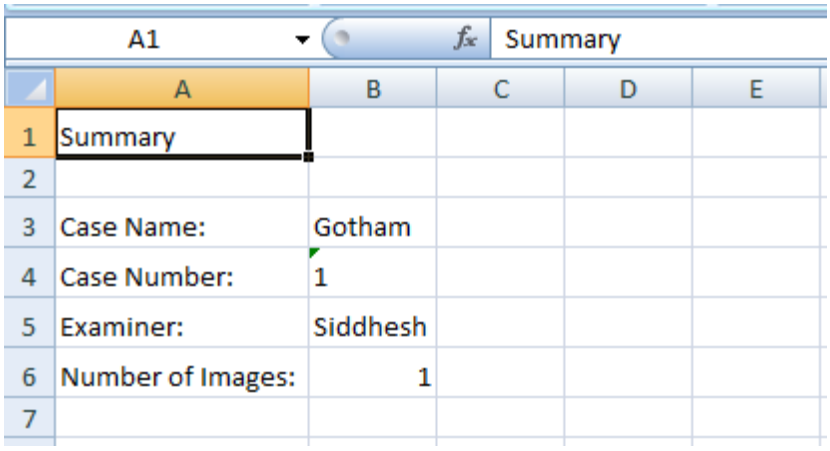
Step 16: Now Report is generated So click on close Button .we can see the Report on Report Node.







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



Conclusion: Here we have successfully completed case study (image file) using Autopsy application.

Assessment No. 08

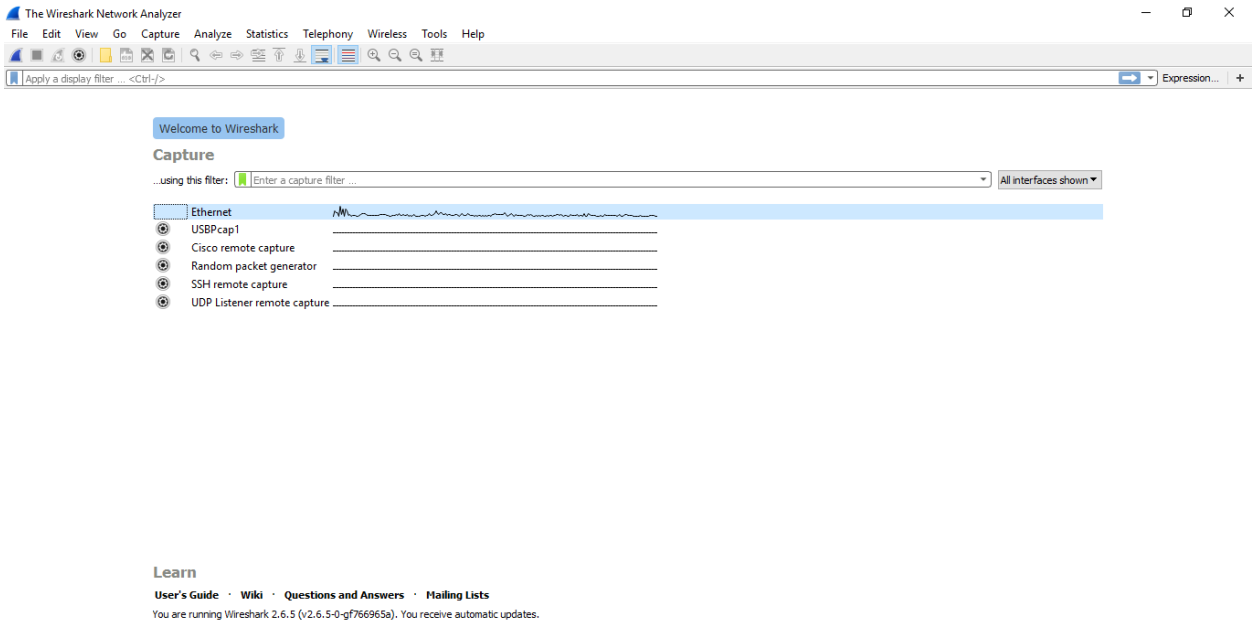
AIM: Use Wireshark (Sniffer) to capture network traffic and analyze.

THEORY:

Wireshark, a network analysis tool formerly known as Ethereal, captures packets in real time and display them in human-readable format. Wireshark includes filters, color coding, and other features that let you dig deep into network traffic and inspect individual packets.

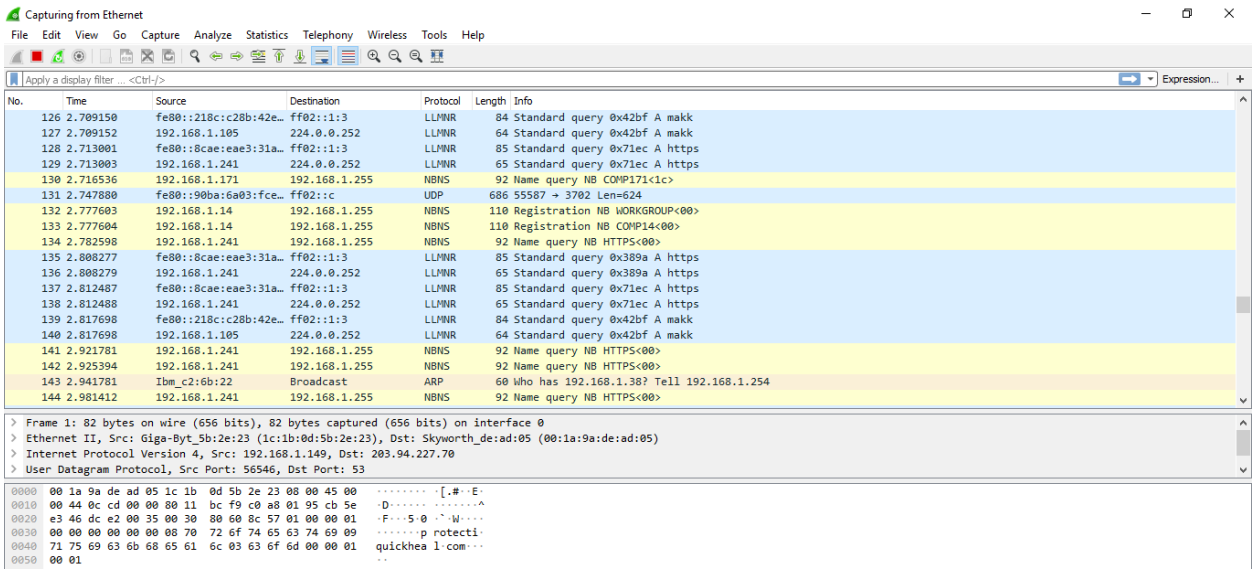
Capturing Packets

After downloading and installing Wireshark, you can launch it and double-click the name of a network interface under Capture to start capturing packets on that interface. For example, if you want to 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.

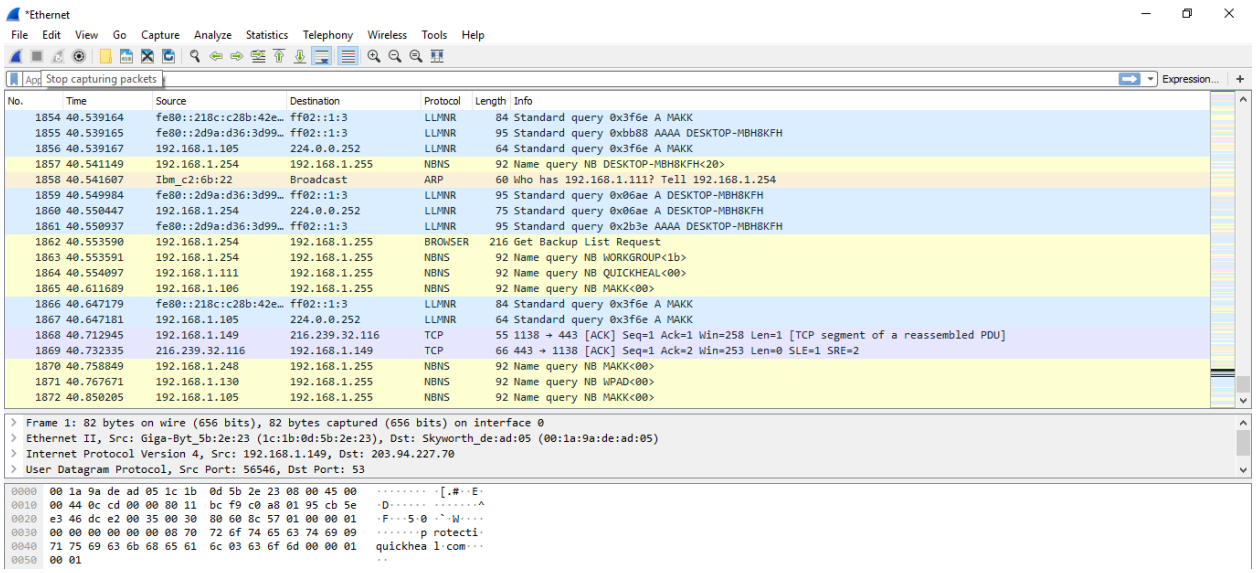


As soon as you click the interface's name, you'll see the packets start to appear in real time. Wireshark captures each packet sent to or from your system.

If you have promiscuous mode enabled—it's enabled by default—you'll also see all the other packets on the network instead of only packets addressed to your network adapter. To check if promiscuous mode is enabled, click Capture > Options and verify the "Enable promiscuous mode on all interfaces" checkbox is activated at the bottom of this window.



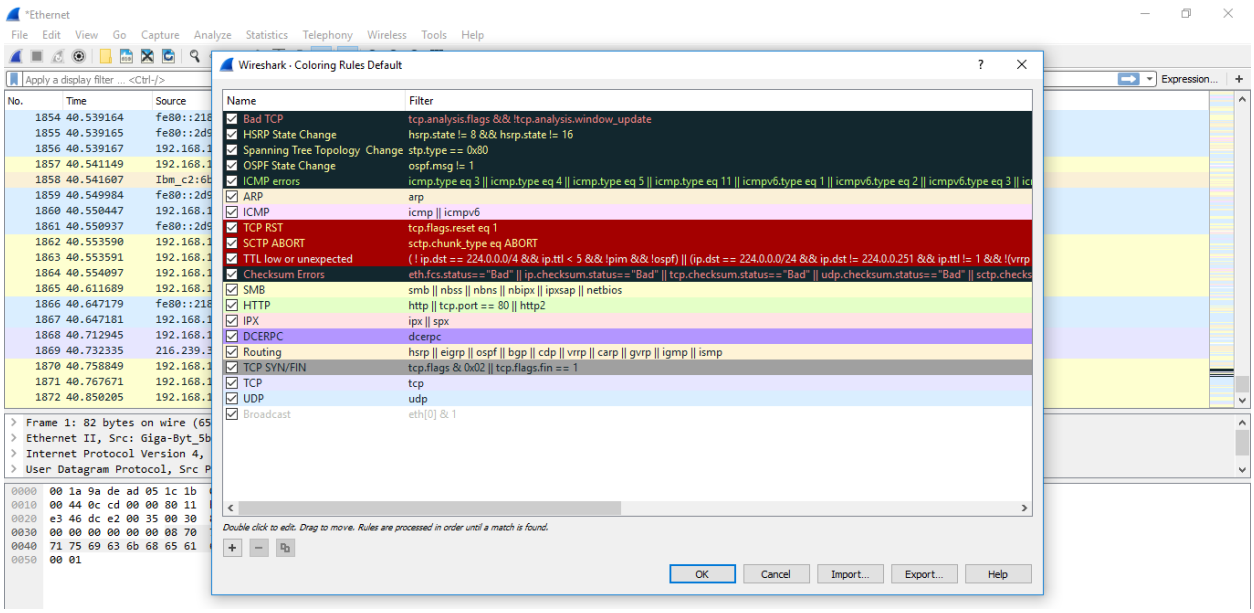
Click the red “Stop” button near the top left corner of the window when you want to stop capturing traffic.



Color Coding

You’ll probably see packets highlighted in a variety of different colors. Wireshark uses colors to help you identify the types of traffic at a glance. By default, light purple is TCP traffic, light blue is UDP traffic, and black identifies packets with errors—for example, they could have been delivered out of order.

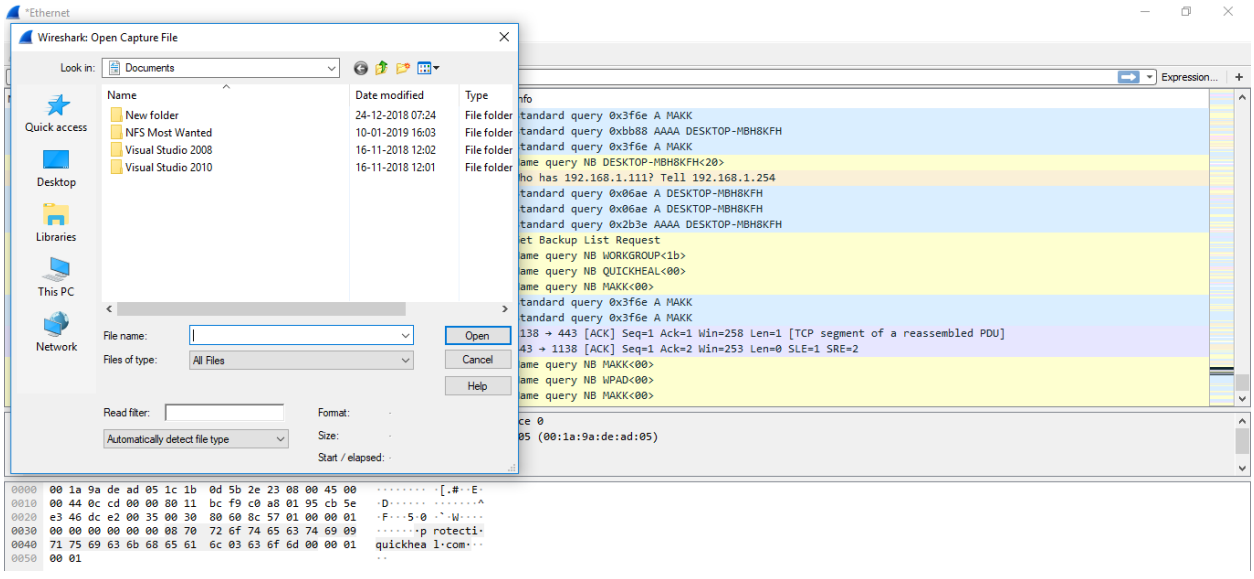
To view exactly what the color codes mean, click View > Coloring Rules. You can also customize and modify the coloring rules from here, if you like.



Sample Captures

If there's nothing interesting on your own network to inspect, Wireshark's wiki has you covered. The wiki contains a page of sample capture files that you can load and inspect. Click File > Open in Wireshark and browse for your downloaded file to open one.

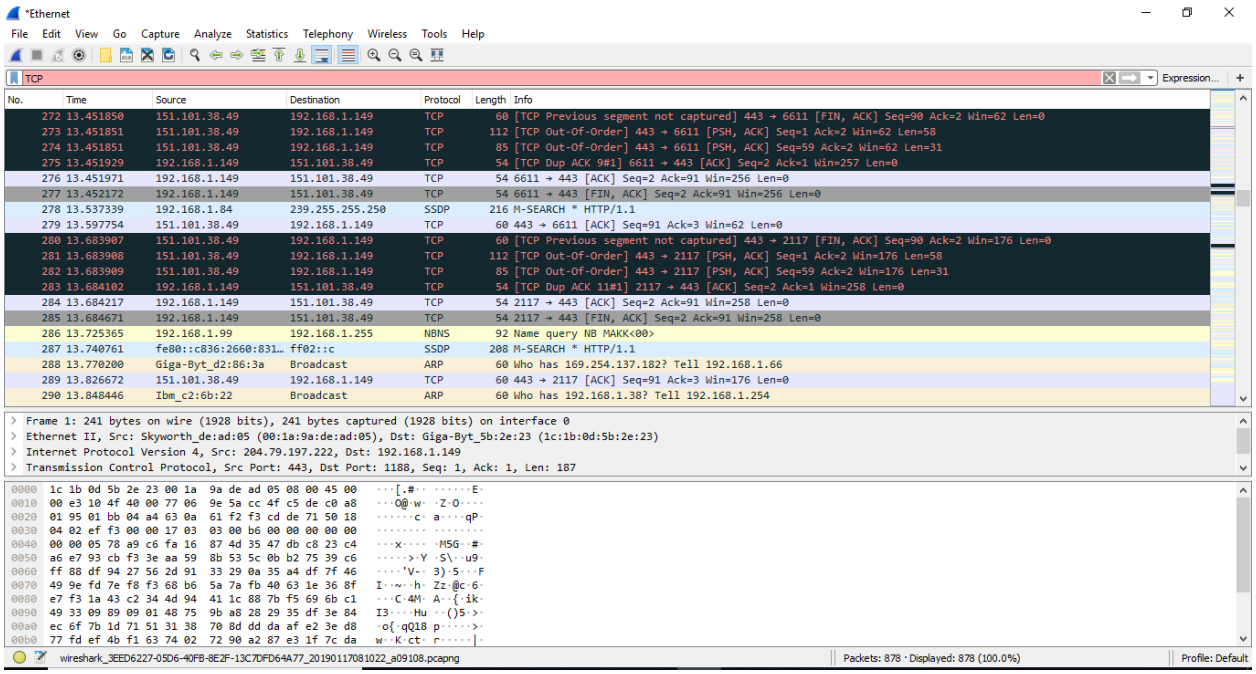
You can also save your own captures in Wireshark and open them later. Click File > Save to save your captured packets.



Filtering Packets

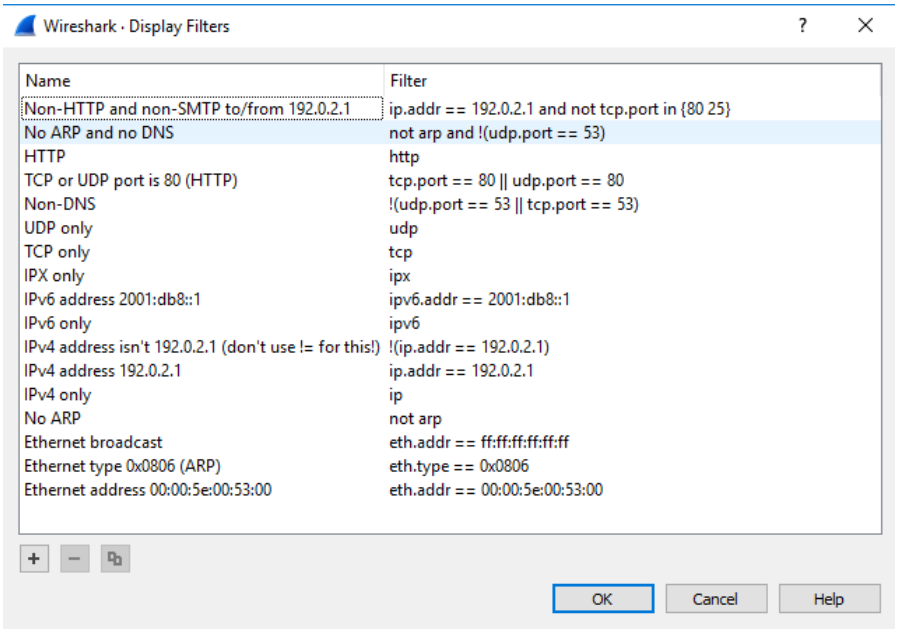
If you're trying to inspect something specific, such as the traffic a program sends when phoning home, it helps to close down all other applications using the network so you can narrow down the traffic. Still, you'll likely have a large amount of packets to sift through. That's where Wireshark's filters come in.

The most basic way to apply a filter is by typing it into the filter box at the top of the window and clicking Apply (or pressing Enter). For example, type "dns" and you'll see only DNS packets. When you start typing, Wireshark will help you autocomplete your filter.



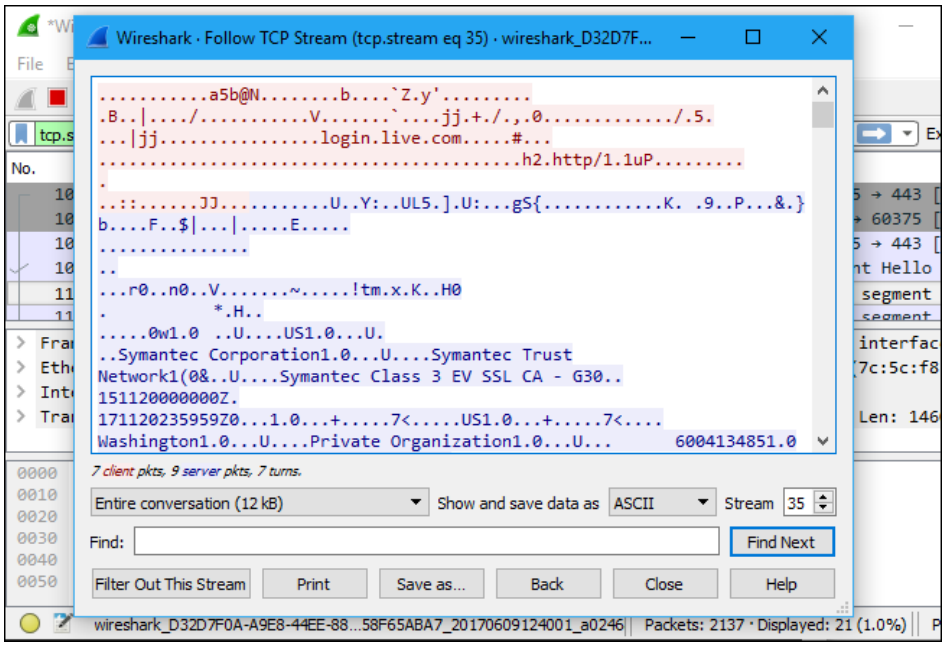
You can also click Analyze > Display Filters to choose a filter from among the default filters included in Wireshark. From here, you can add your own custom filters and save them to easily access them in the future.

For more information on Wireshark's display filtering language, read the Building display filter expressions page in the official Wireshark documentation.

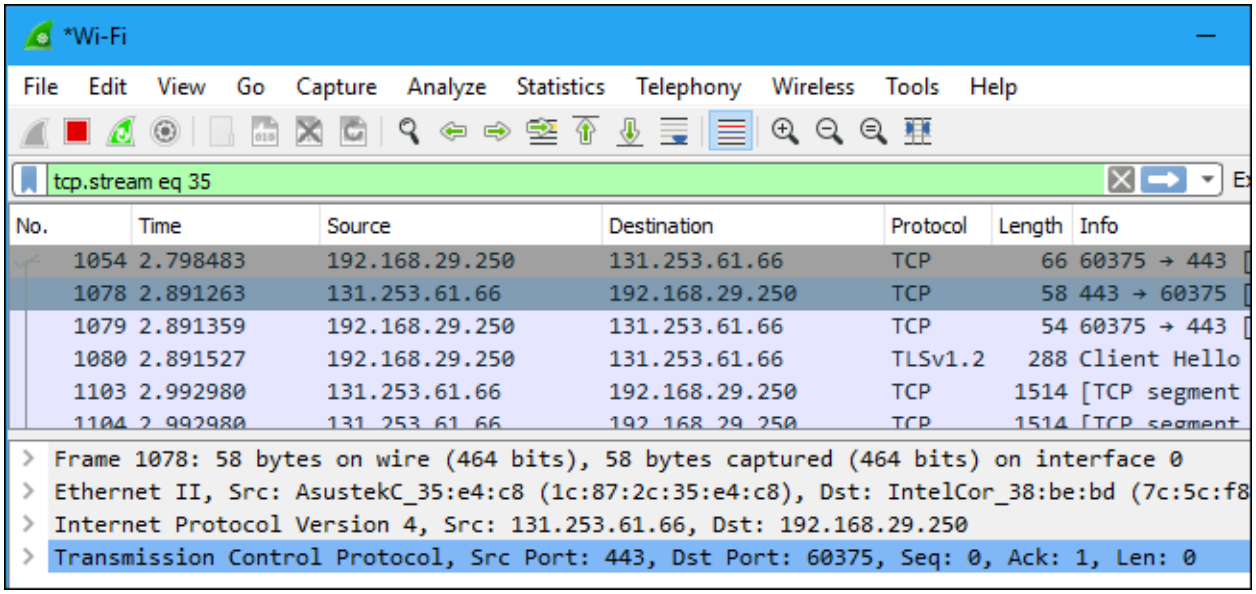


Another interesting thing you can do is right-click a packet and select Follow > TCP Stream.

You'll see the full TCP conversation between the client and the server. You can also click other protocols in the Follow menu to see the full conversations for other protocols, if applicable.

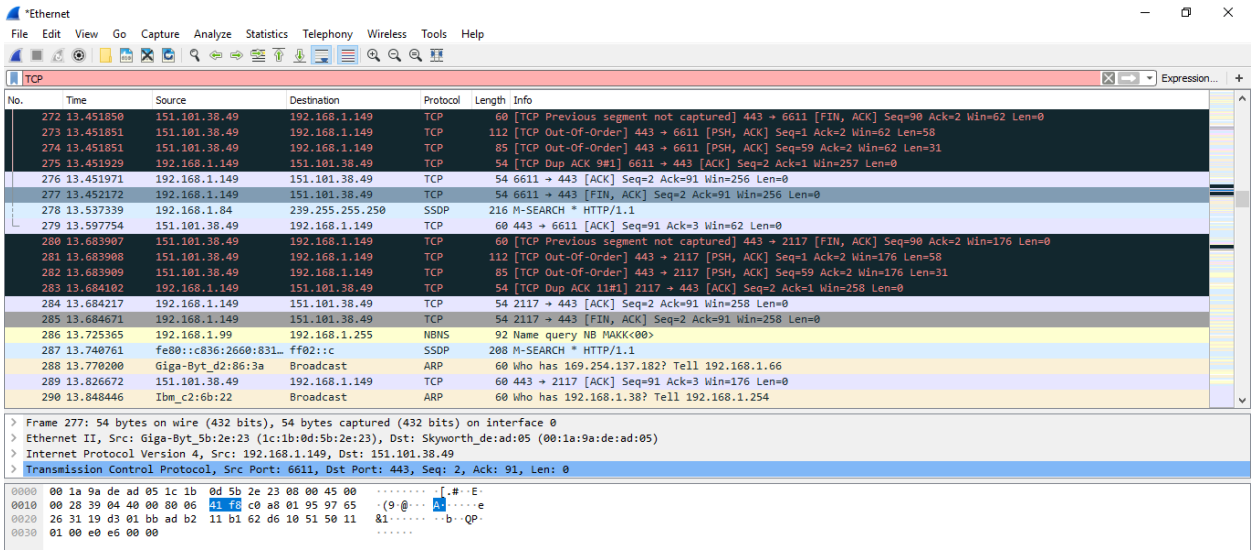


Close the window and you'll find a filter has been applied automatically. Wireshark is showing you the packets that make up the conversation.

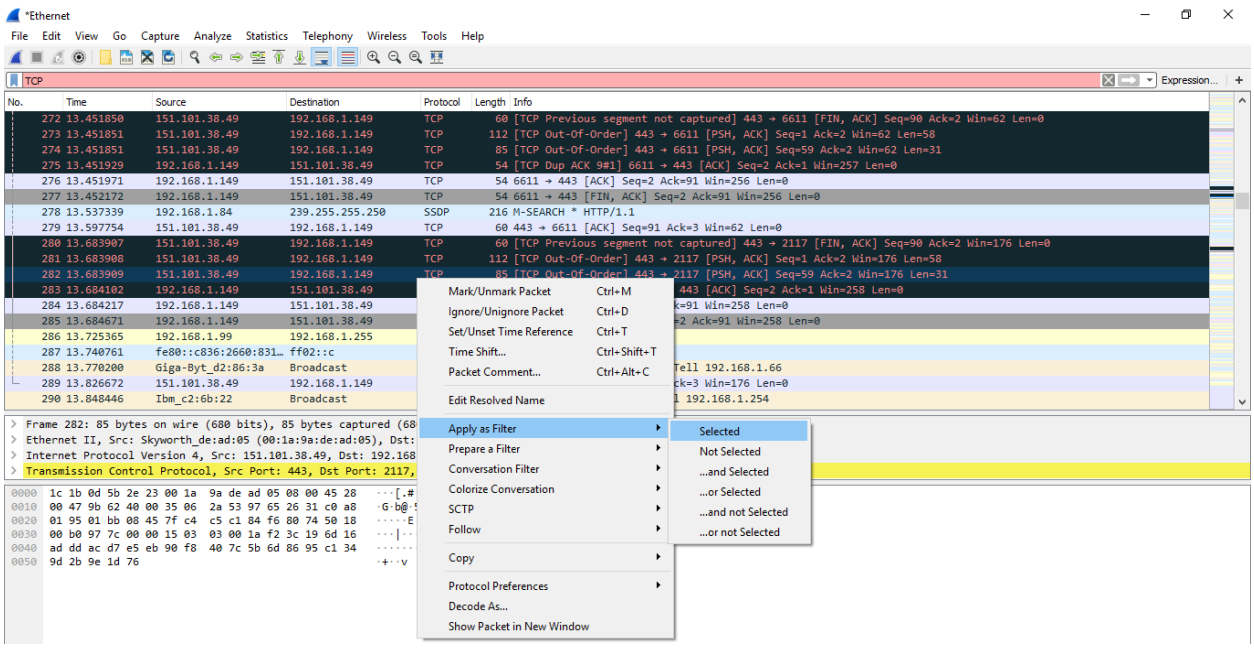


Inspecting Packets

Click a packet to select it and you can dig down to view its details



You can also create filters from here — just right-click one of the details and use the Apply as Filter submenu to create a filter based on it.



Wireshark is an extremely powerful tool, and this tutorial is just scratching the surface of what you can do with it. Professionals use it to debug network protocol implementations, examine security problems and inspect network protocol internals.

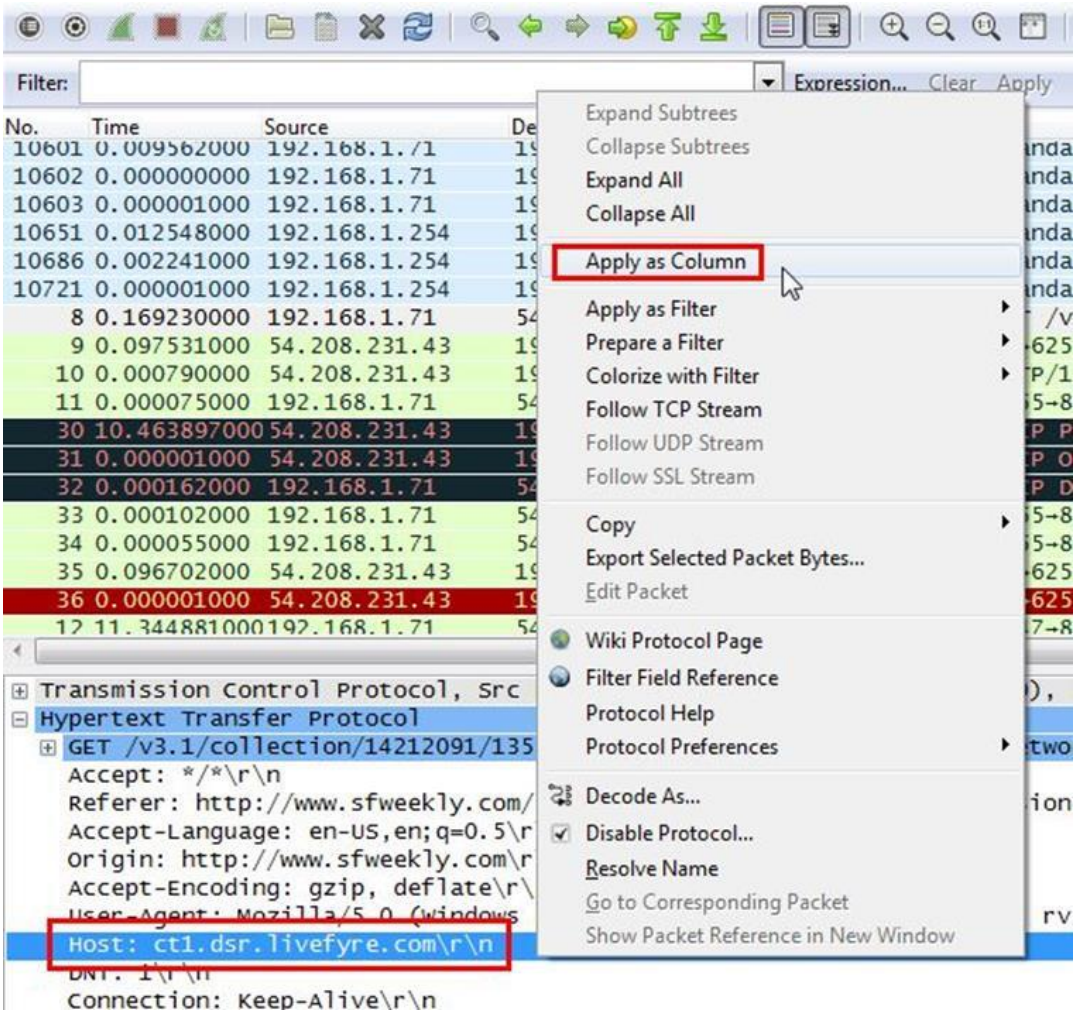
CONCLUSION: We have captured and analyzed network packets using Wireshark.

Assessment No. 09

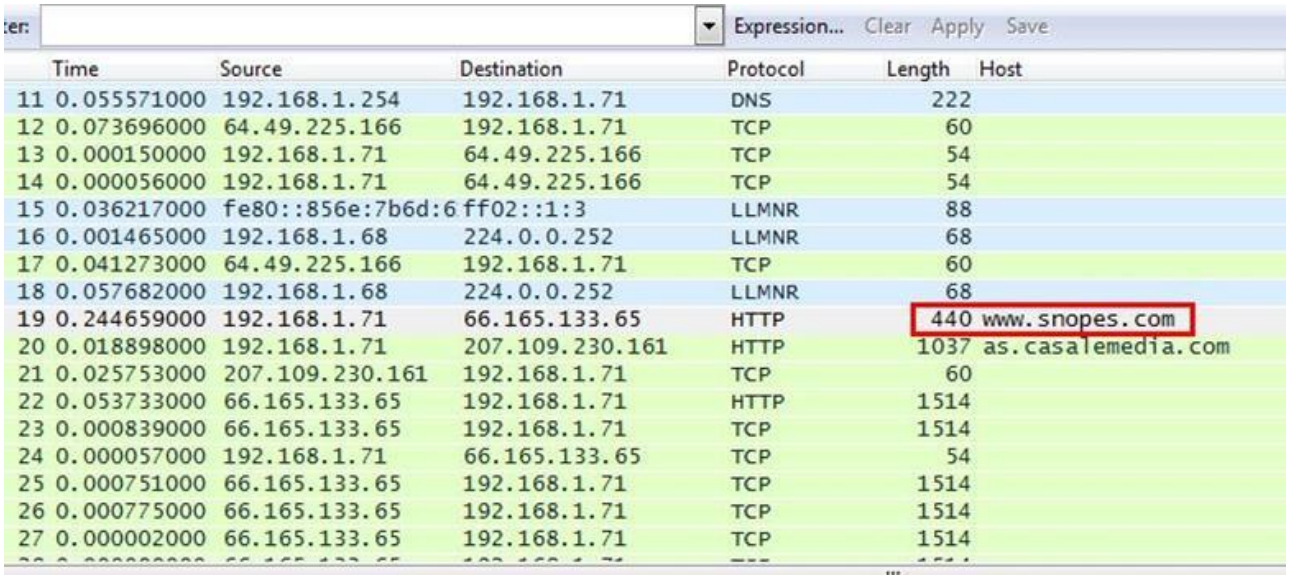
Aim: Analyze the packets provided in lab and solve the questions using Wireshark.

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.

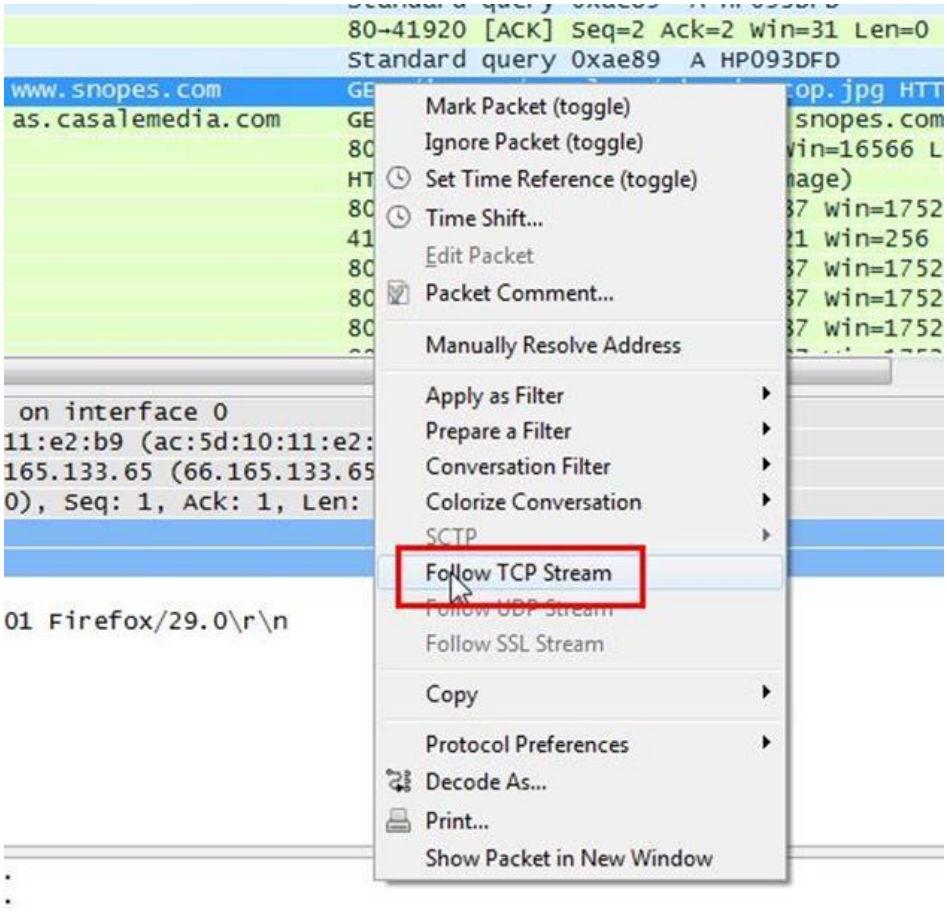


Now we can see our host www.snopes.com in host column.



	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:6	ff02::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	

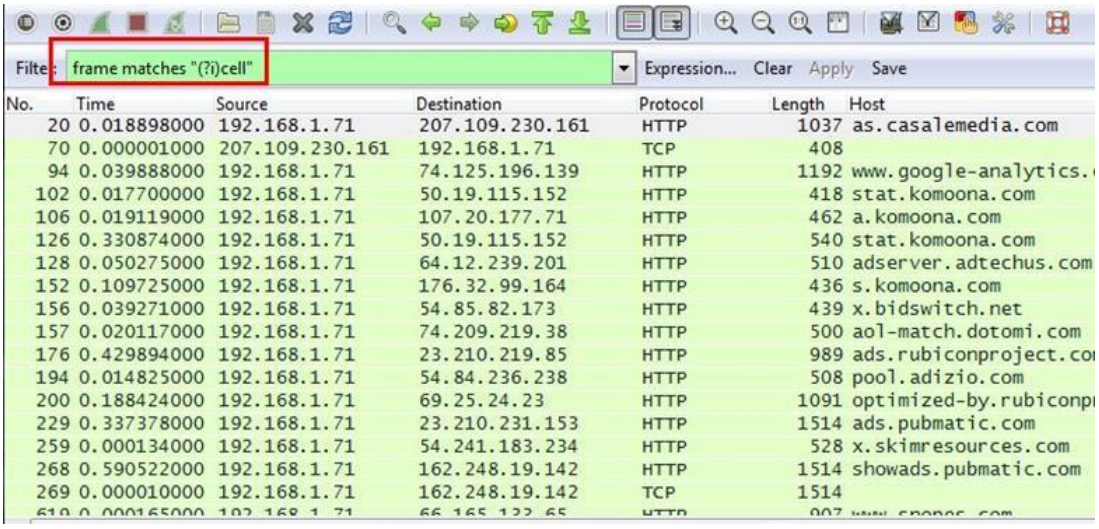
Right click on the selected packet and then select Follow TCP stream.



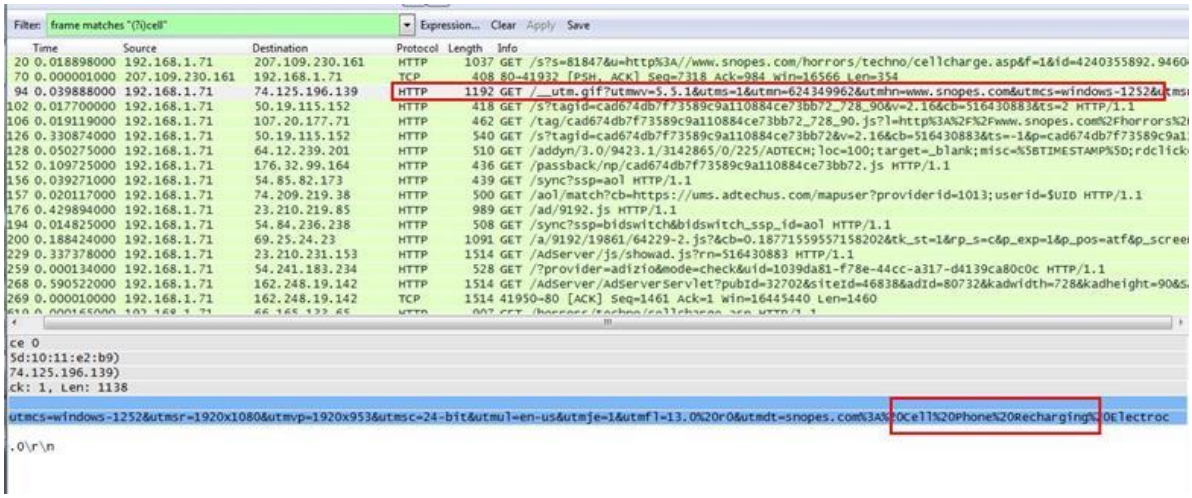
Now we can see the webserver name in server header it is Microsoft IIS 5.0

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"

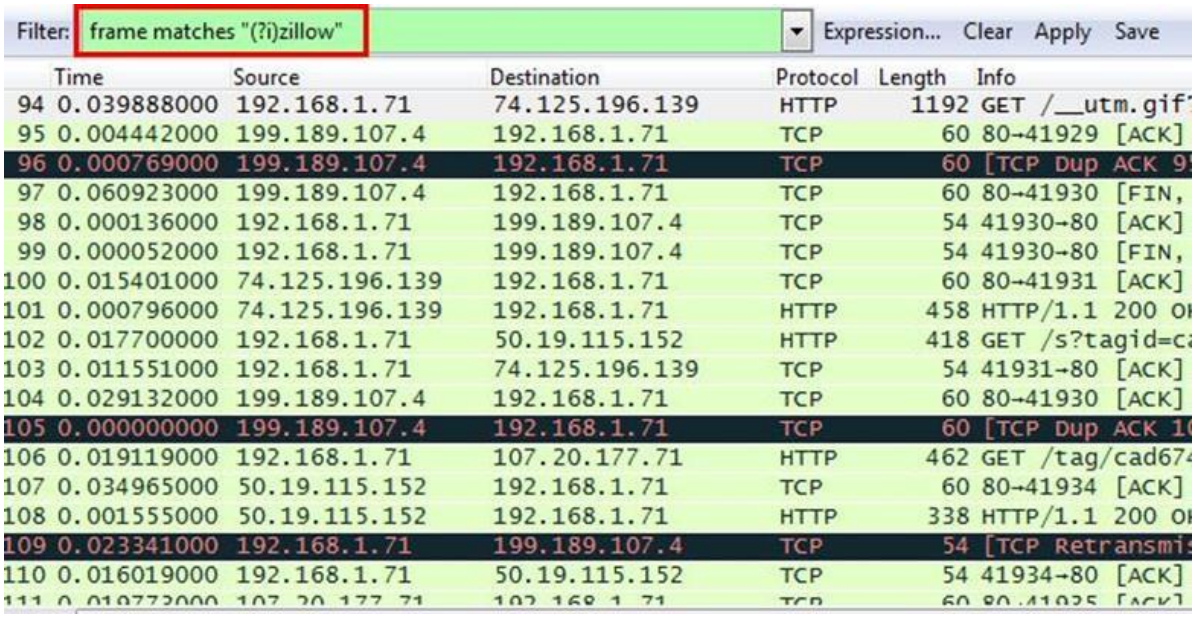


After applying the filter now, we will start to check every HTTP request. We noticed in the first HTTP request cell keyword is in URL and it was about cell phone charging issue.



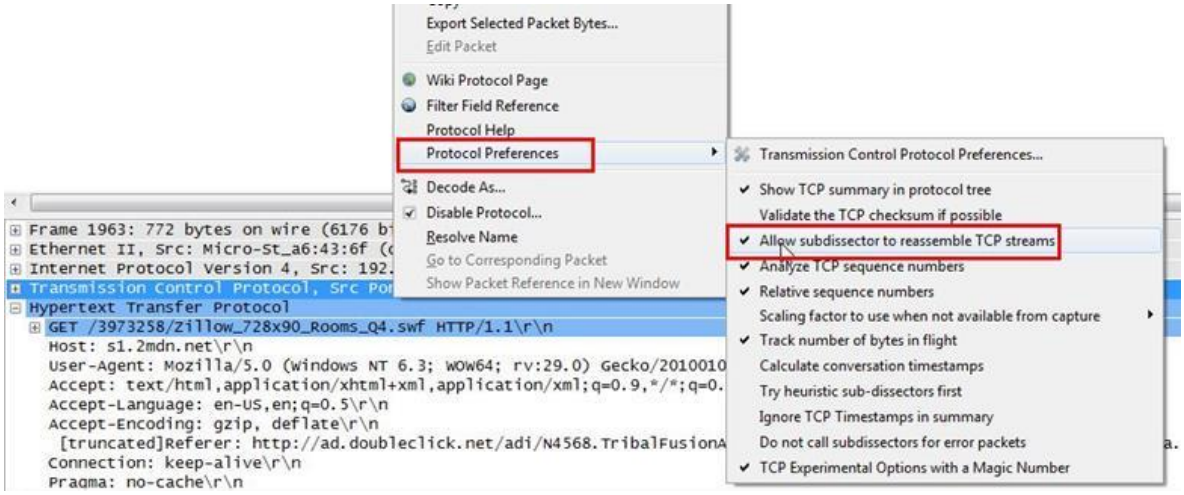
3. According to Zillow, what instrument will Ryan learn to play?

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

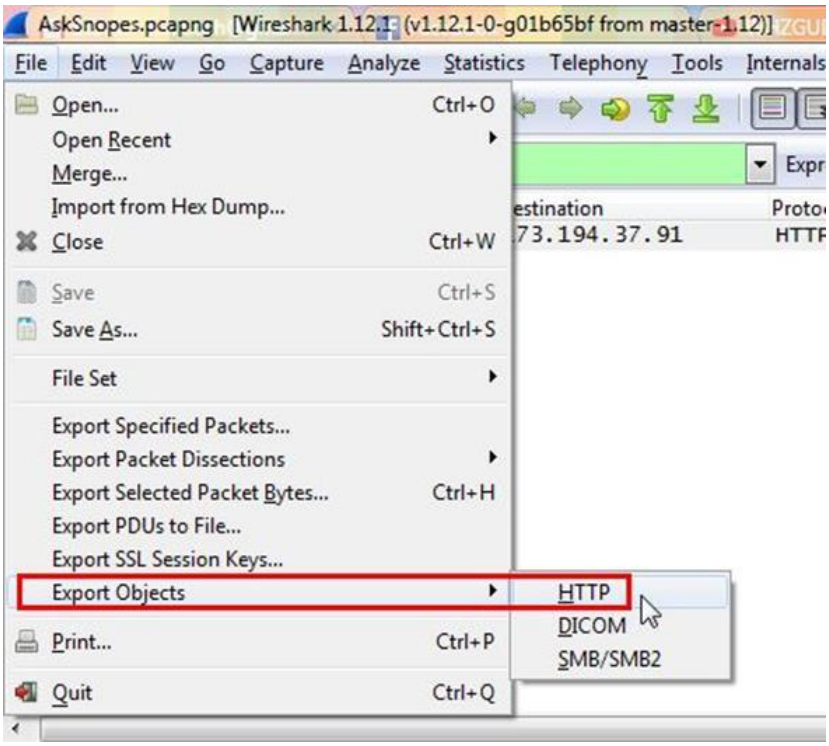


After applying the filter, we found only one packet with the Zillow keyword

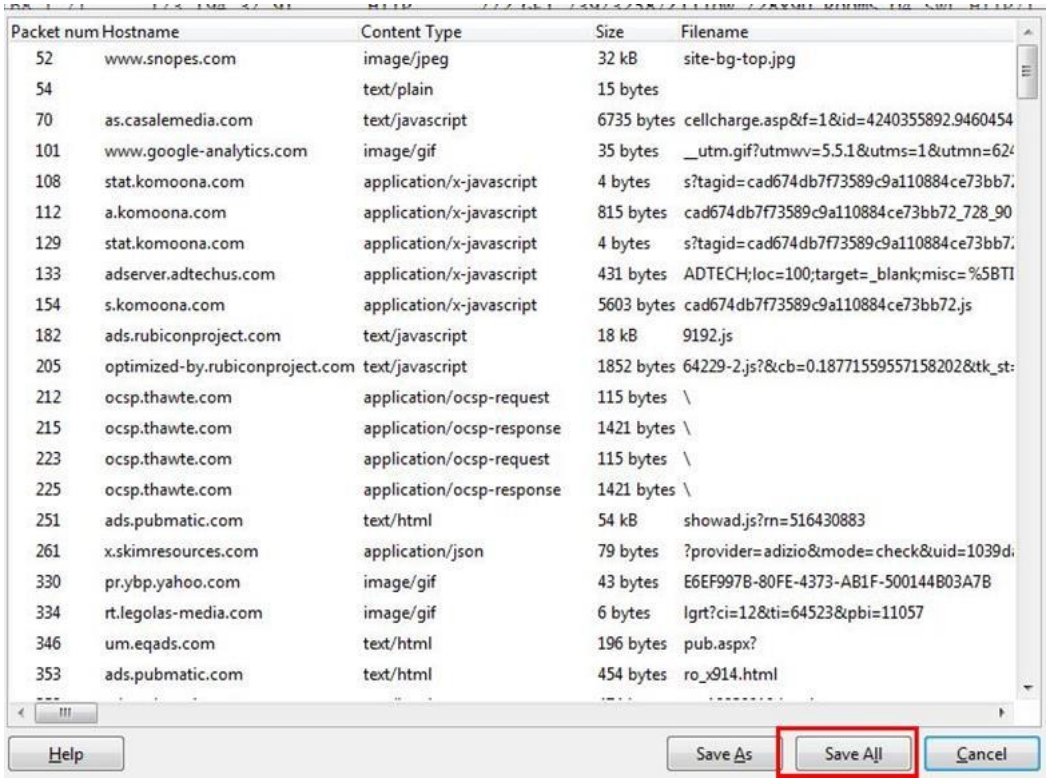
Select the packet and expand the Hypertext Transfer Protocol tab right click on it go to Protocol Preferences and check Allow subdissector to resemble TCP stream.



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



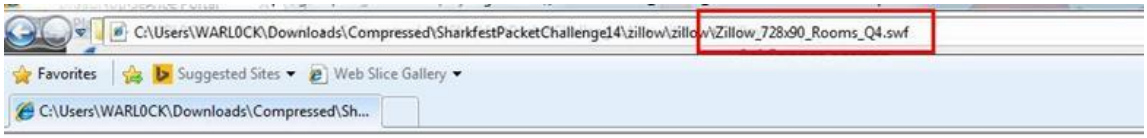
Click on save all.



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

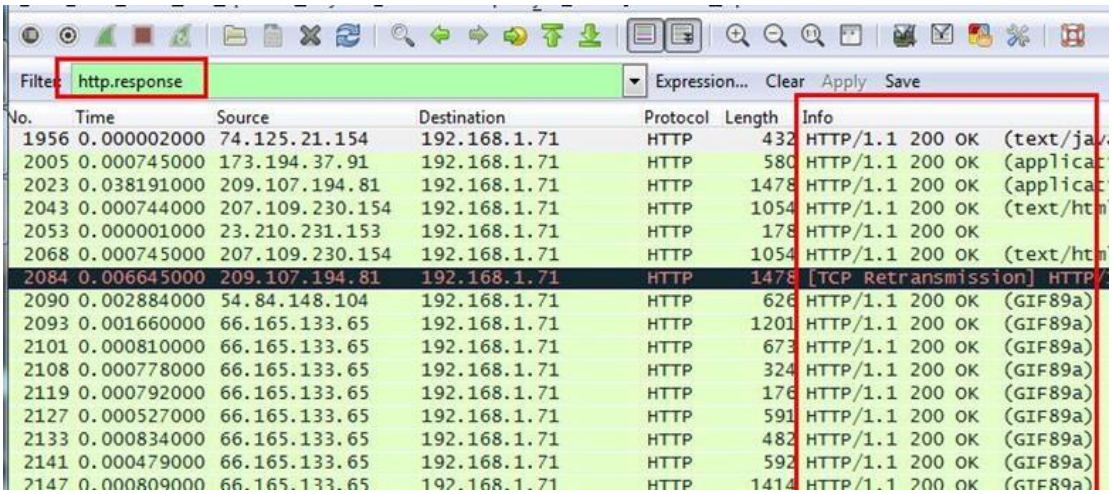
Help | Save As | Save All | Cancel

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.

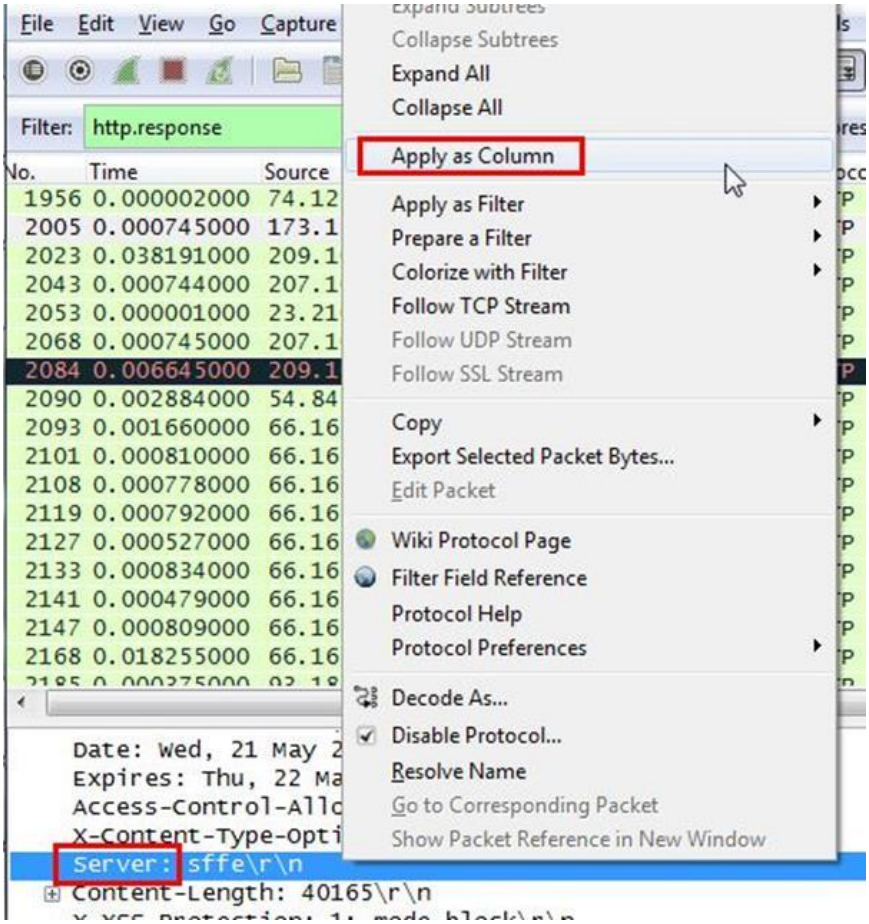


4. How many web servers are running Apache?

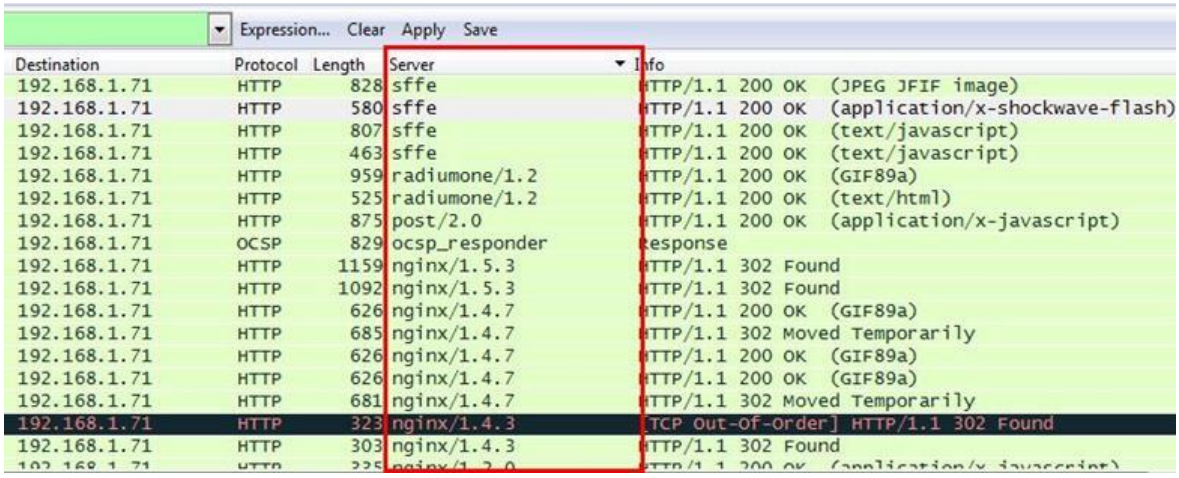
Analysis – The web server name can be retrieved from HTTP response header. So will apply filter http.response and we can see all http response packets.



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

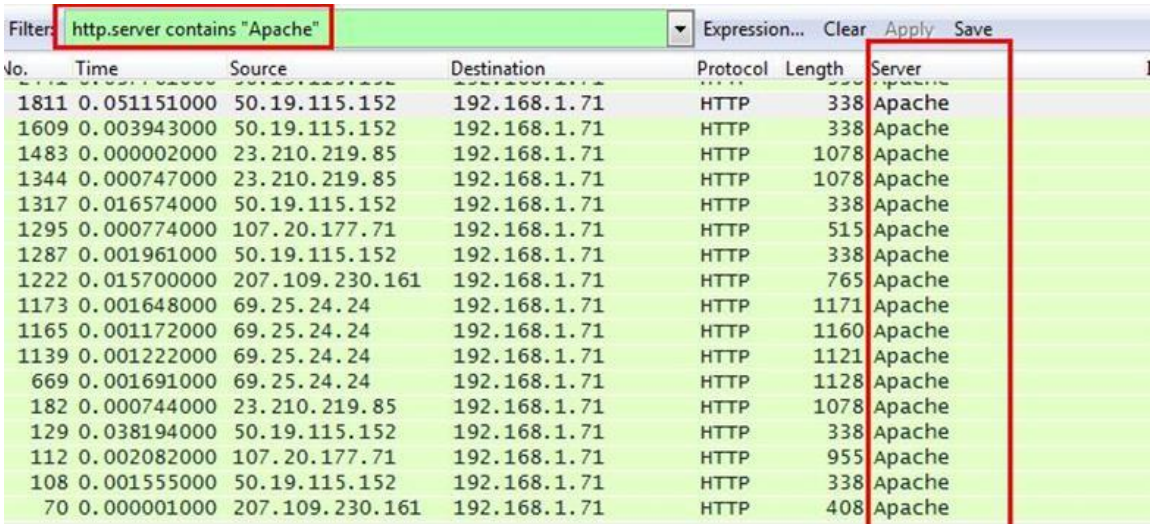


Now can see the server column where all server name is showing.



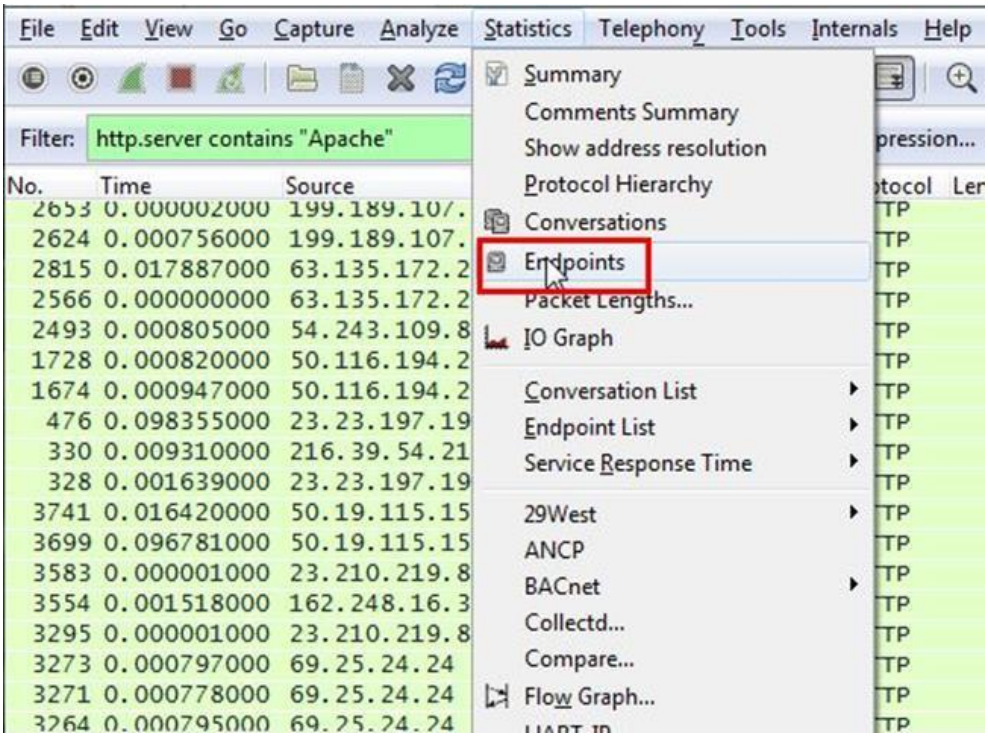
Destination	Protocol	Length	Server	Info
192.168.1.71	HTTP	828	sffe	HTTP/1.1 200 OK (JPEG JFIF image)
192.168.1.71	HTTP	580	sffe	HTTP/1.1 200 OK (application/x-shockwave-flash)
192.168.1.71	HTTP	807	sffe	HTTP/1.1 200 OK (text/javascript)
192.168.1.71	HTTP	463	sffe	HTTP/1.1 200 OK (text/javascript)
192.168.1.71	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

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"

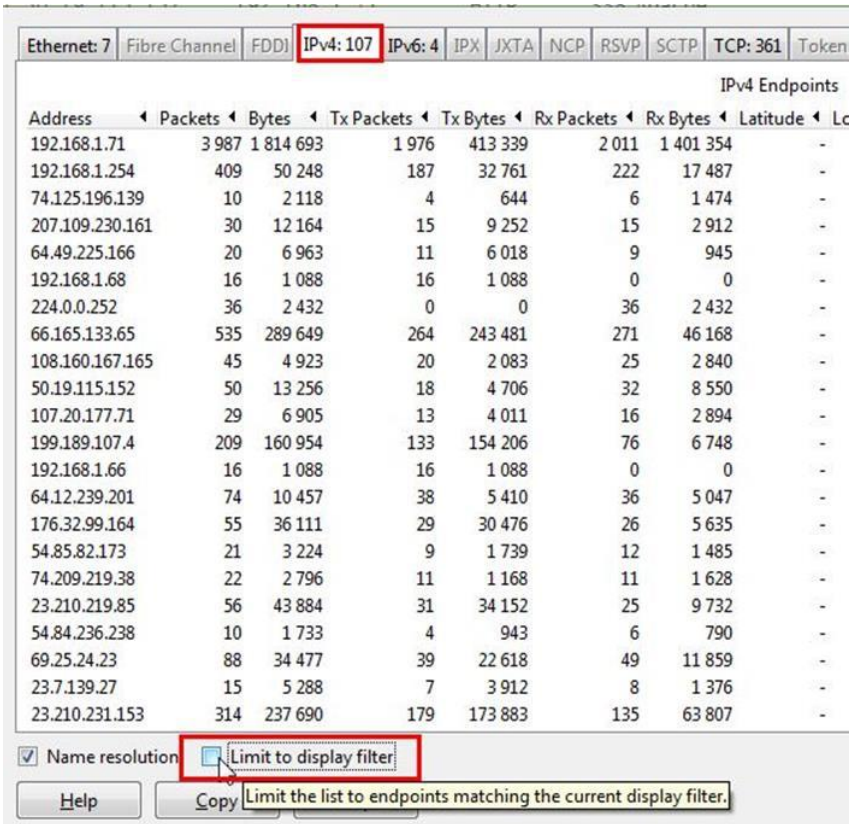


No.	Time	Source	Destination	Protocol	Length	Server
1811	0.051151000	50.19.115.152	192.168.1.71	HTTP	338	Apache
1609	0.003943000	50.19.115.152	192.168.1.71	HTTP	338	Apache
1483	0.000002000	23.210.219.85	192.168.1.71	HTTP	1078	Apache
1344	0.000747000	23.210.219.85	192.168.1.71	HTTP	1078	Apache
1317	0.016574000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

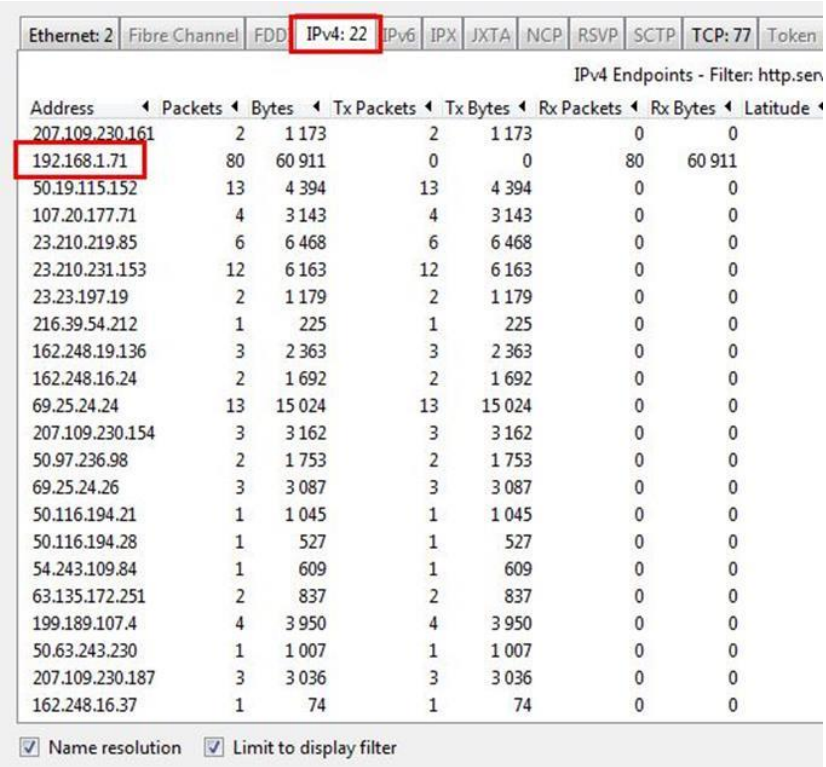
After applying filter go to Statistics > Endpoints



It will show all connection



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 | FDDI | 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 analyze the provided packets and solved the questions given using Wireshark.