

Practical No – 1

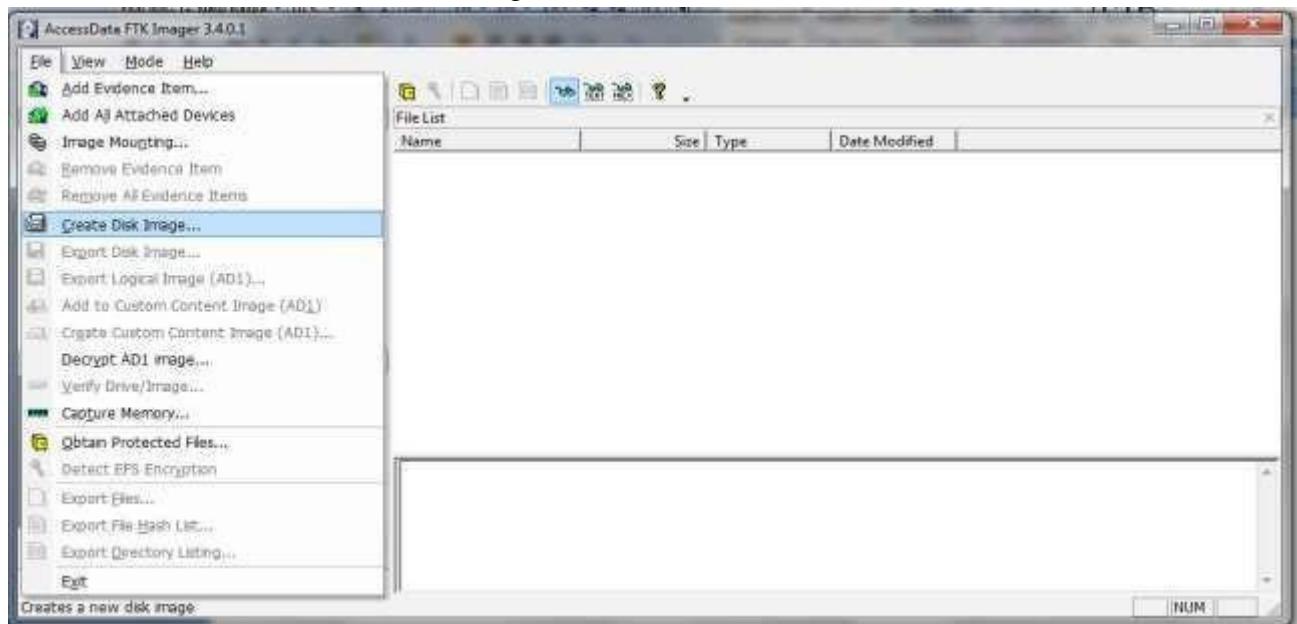
Aim: Creating a Forensic Image using FTK Imager/Encase Imager:

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

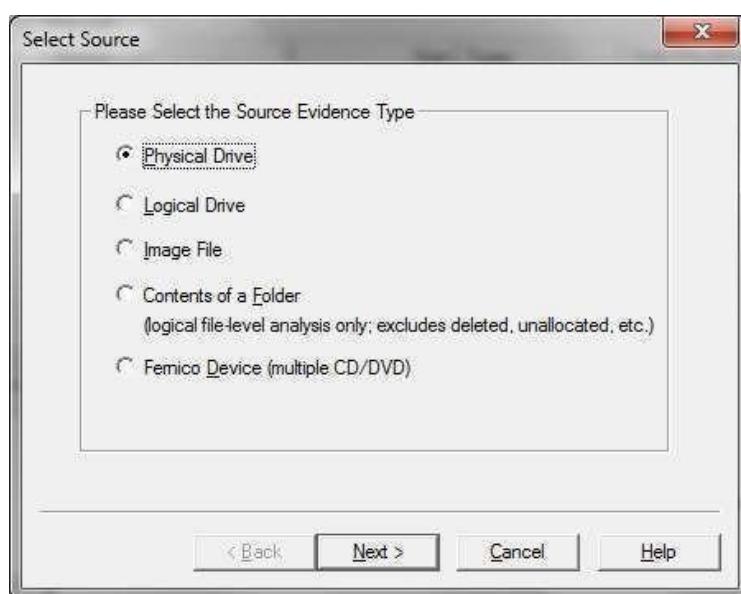
Steps:

Creating Forensic Image

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

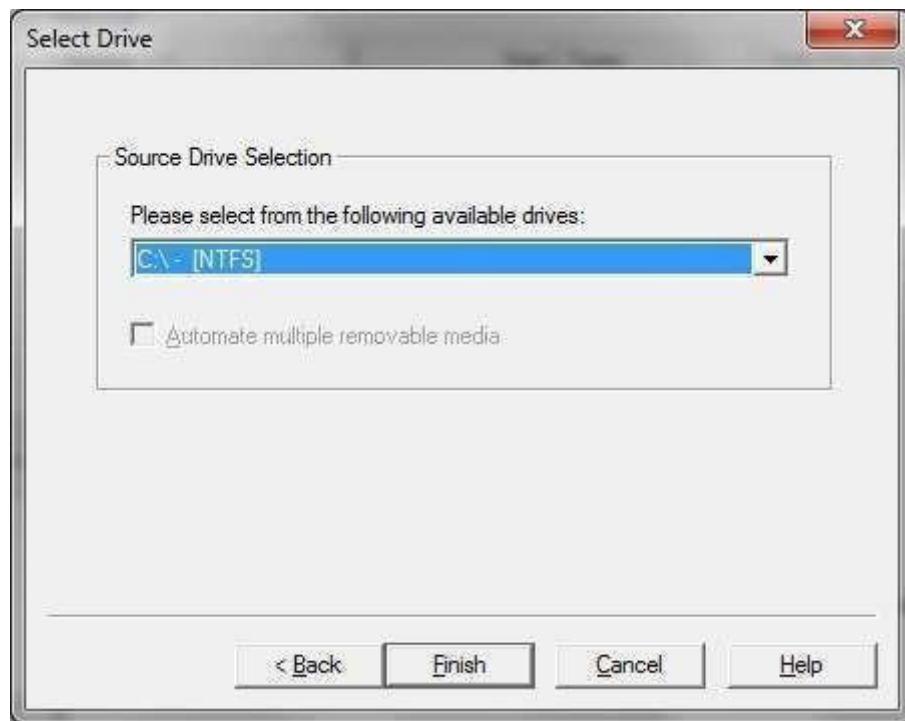


2. Select the source you want to make an image of and click Next.

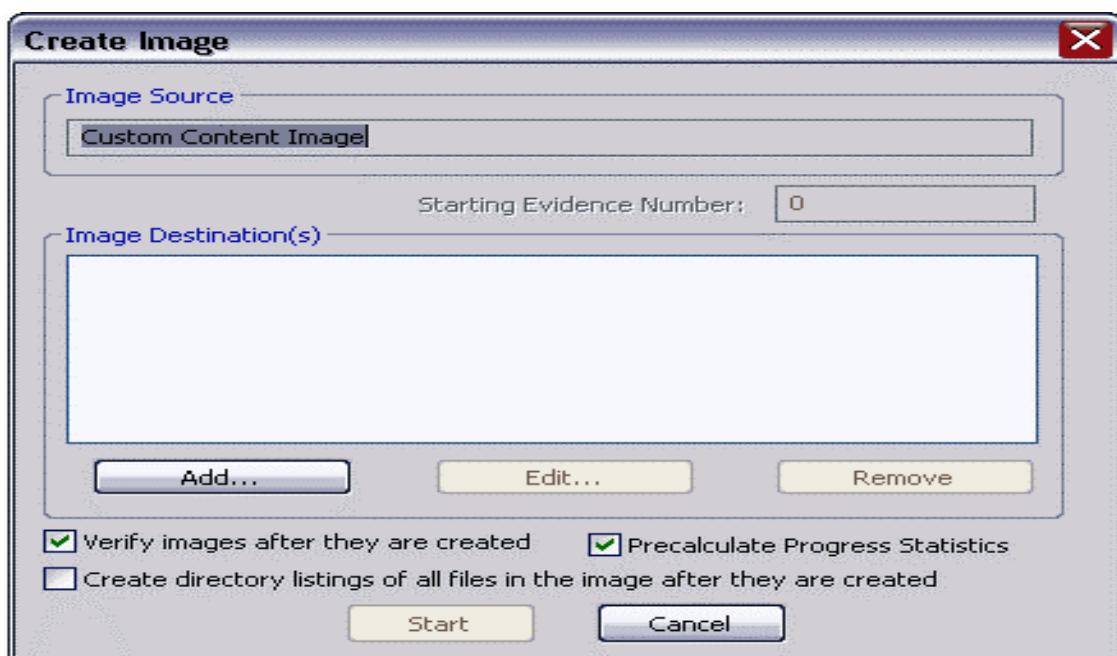


If you select Logical Drive to select a floppy or CD as a source, you can check the Automate multiple removable media box to create groups of images. Imager will automatically increment the case numbers with each image, and if something interrupts the process, you may assign case number manually.

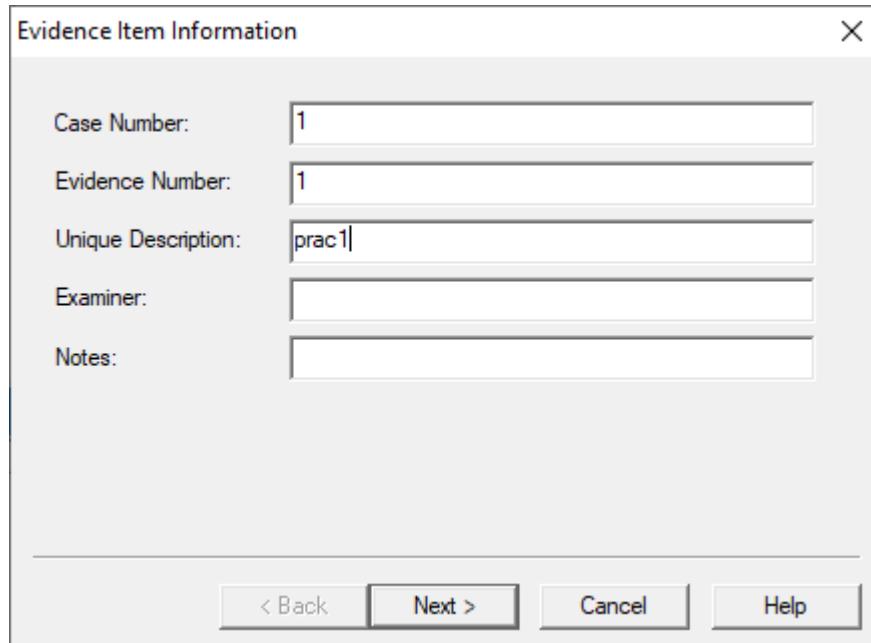
3. Select the drive or browse to the source of the image you want, and then click Finish.



4. In the Create Image dialog, click Add.

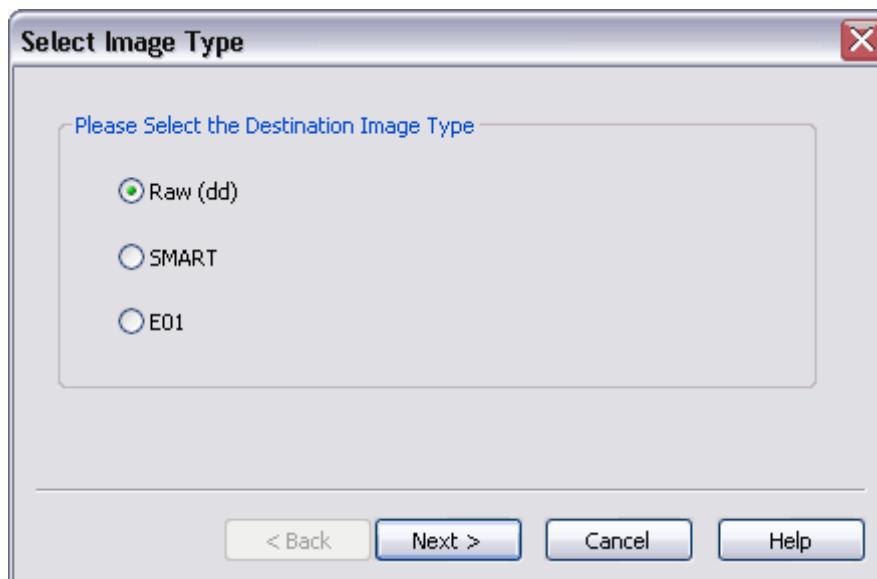


- You can compare the stored hashes of your image content by checking the Verify images after they are created box. If a file doesn't have a hash, this option will generate one.
- You can list the entire contents of your images with path, creation dates, whether files were deleted, and other metadata.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

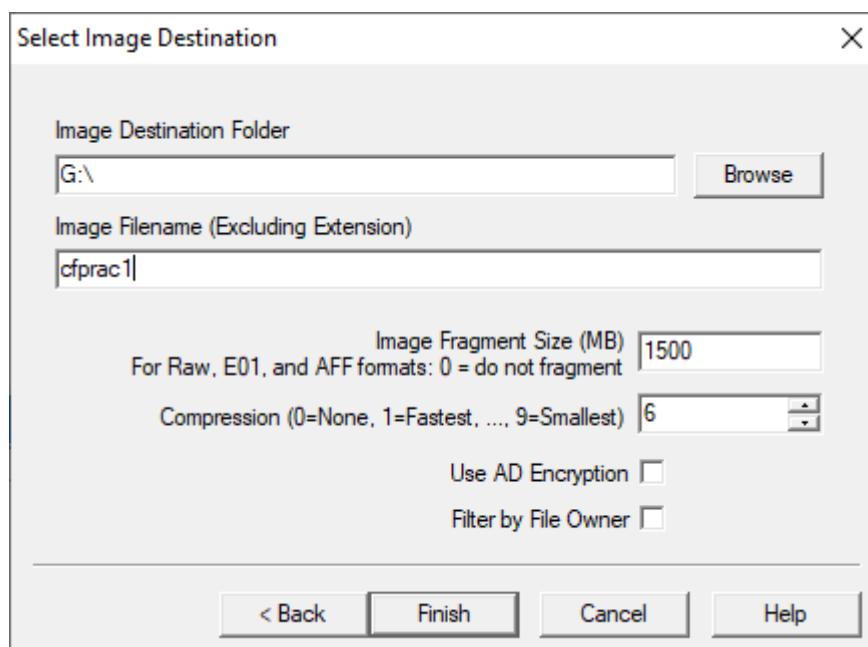
Raw (dd): This is the image format most commonly used by modern analysis tools. These raw file formatted images do not contain headers, metadata, or magic values. The raw format typically includes padding for any memory ranges that were intentionally skipped (i.e.,

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.

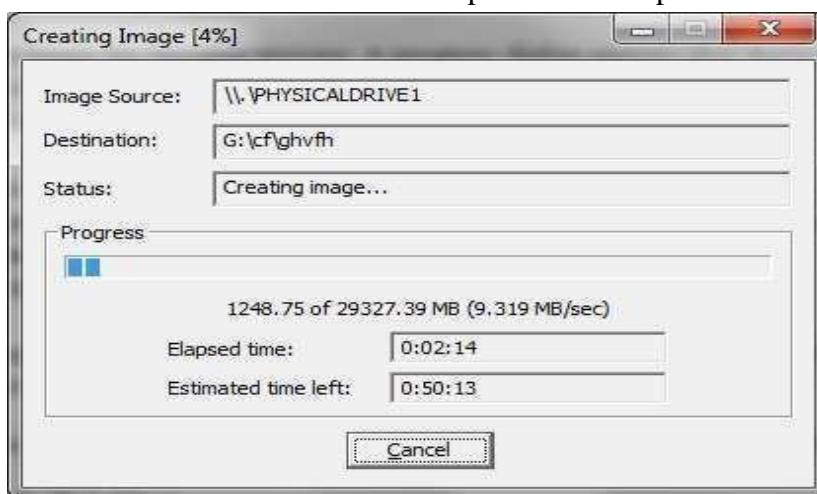
10. To add another image destination (i.e., a different saved location or image file type),

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**.

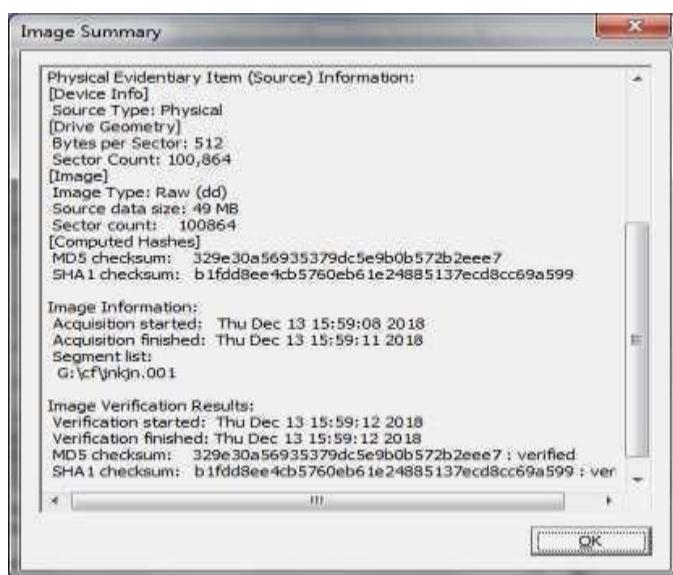
11. Click **Start** to begin the imaging process. A progress dialog appears that shows the following:

- 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.

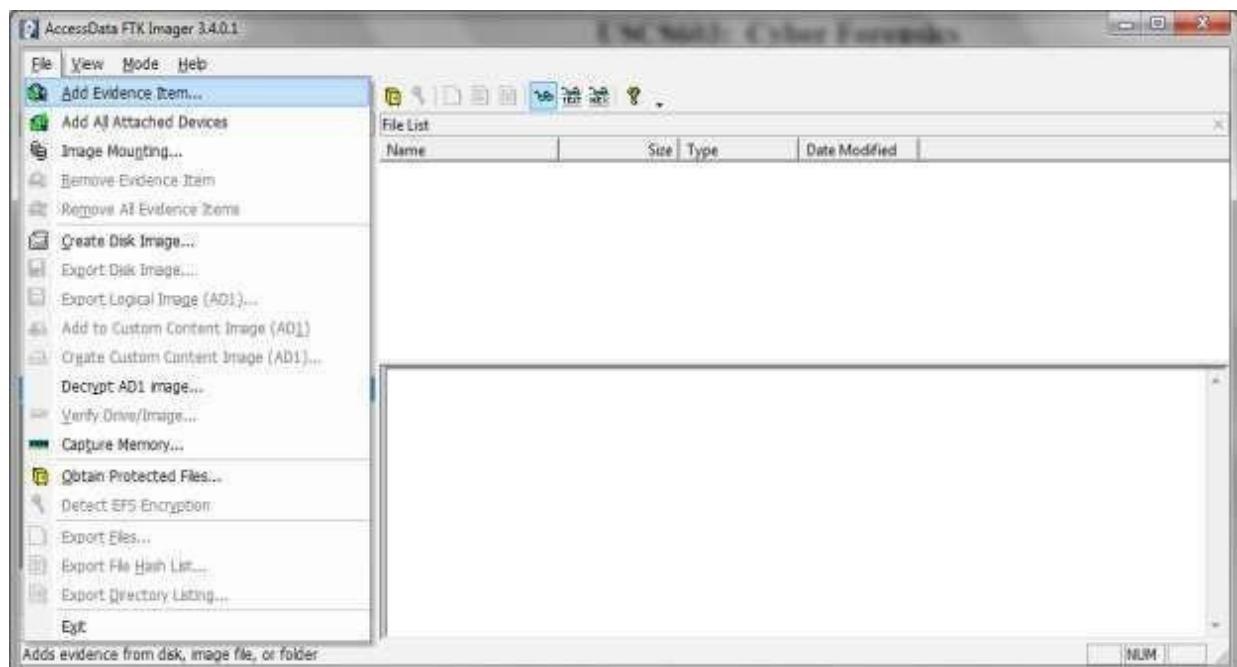


12. When finished, click **Close**

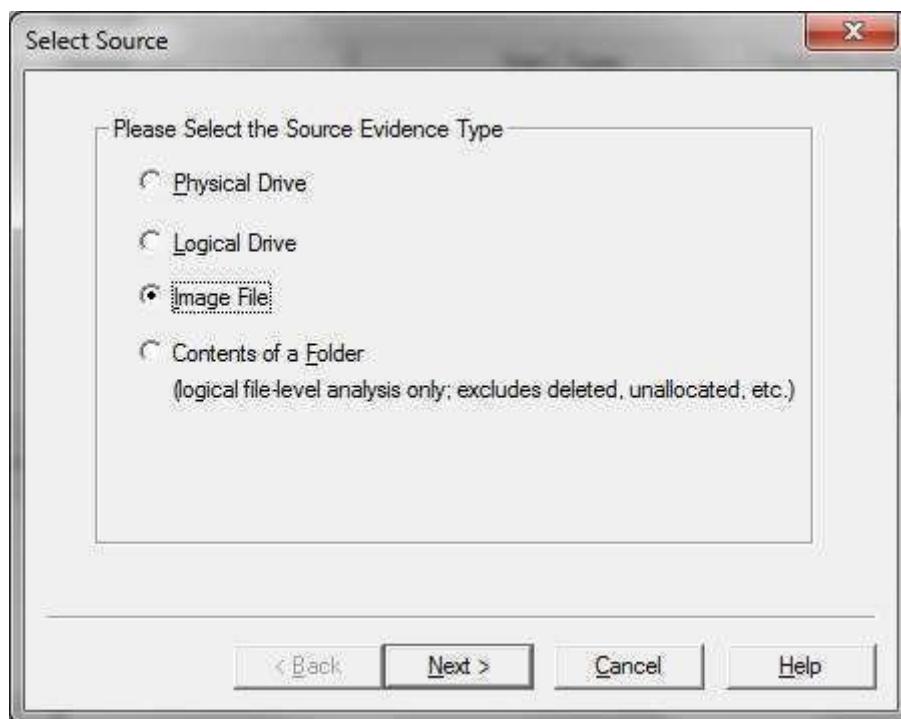
Note that the image file (*.001) as well as the image summary file from above (*.txt) have been saved onto the ‘Drive’. The .001 extension may be left as is, or can be changed to .dd. The .001 extension is used due to the fact that many times the file to be imaged is very large and must be split into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

Analyze Forensic Image:

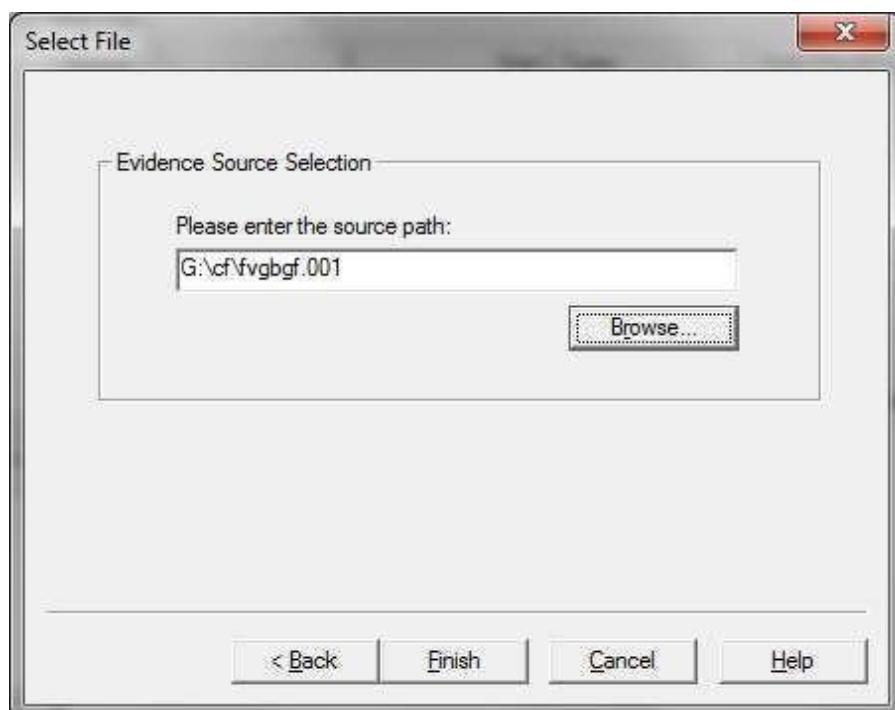
Click on Add Evidence Item to add evidence from disk, image file or folder.



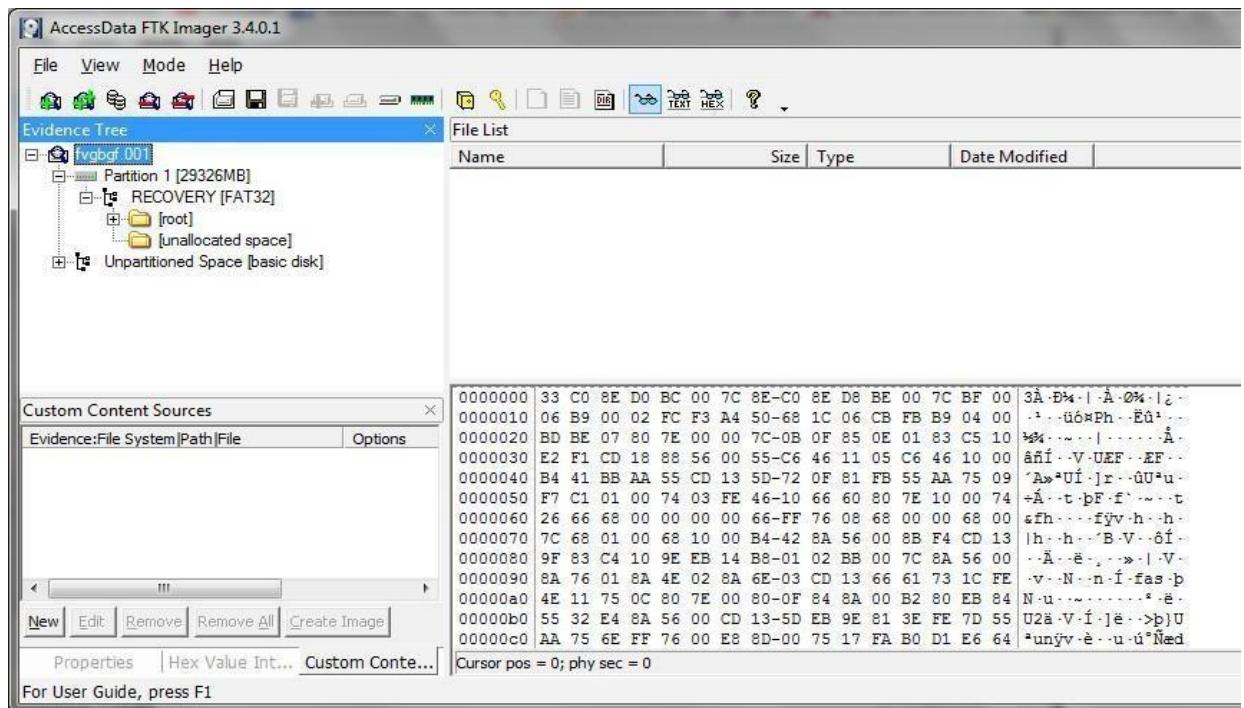
Now select the source evidence type as physical drive, logical drive or image file. We have selected image file and click on next.



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

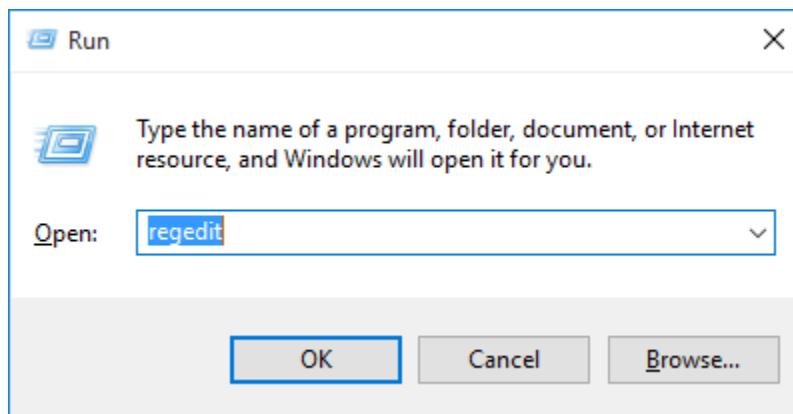
Aim: Data Acquisition:

- 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.

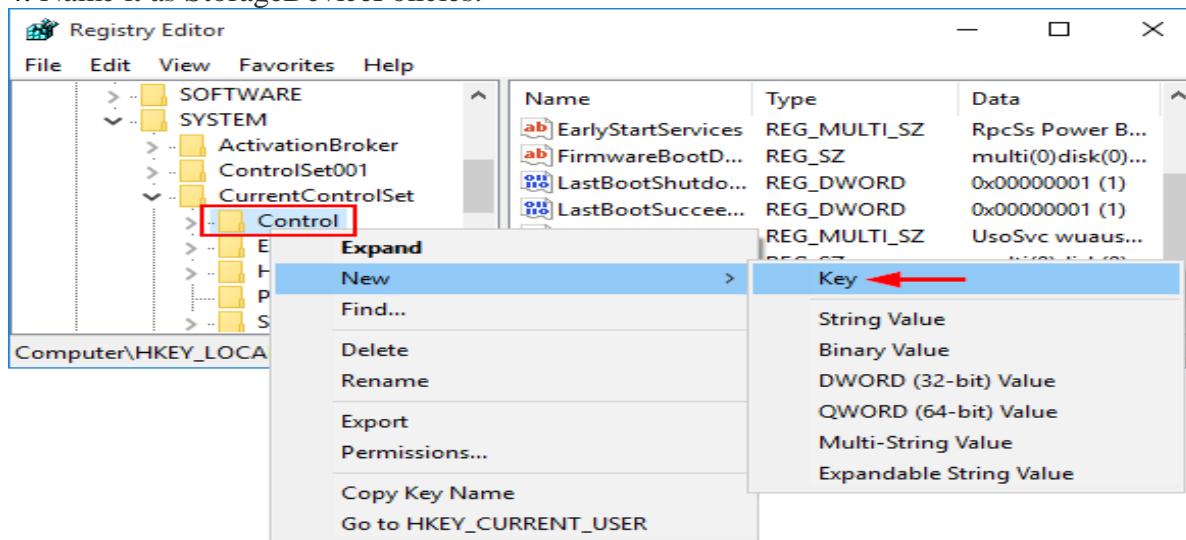


2. This will open the Registry Editor. Navigate to the following key:

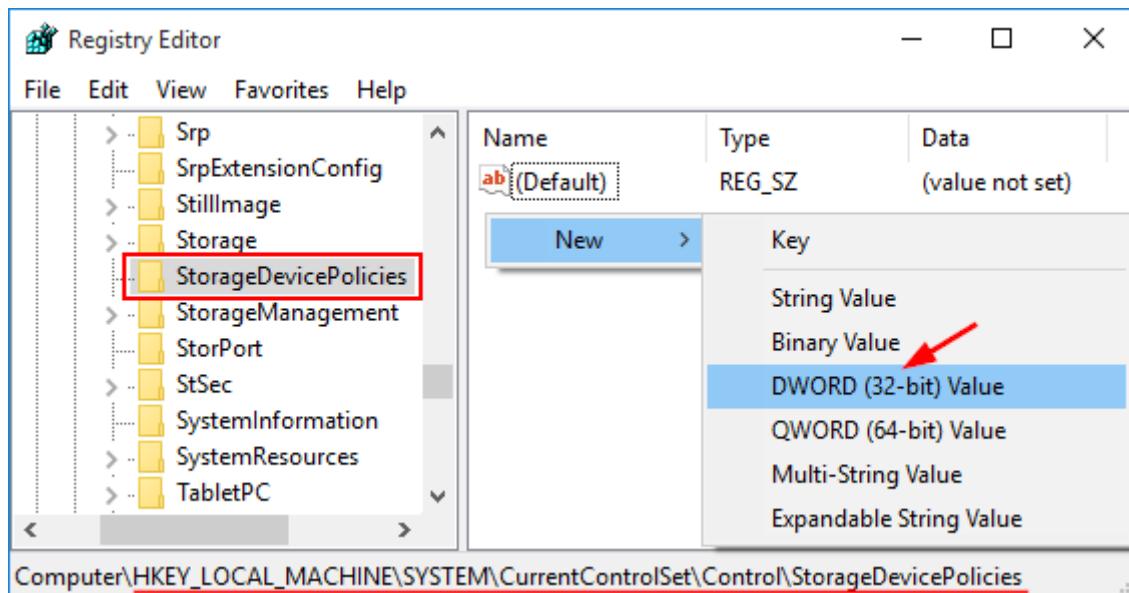
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control

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

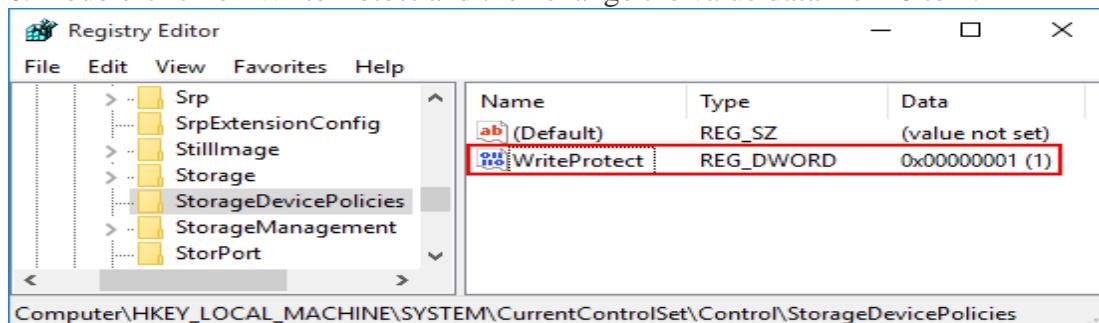
4. Name it as StorageDevicePolicies.



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.

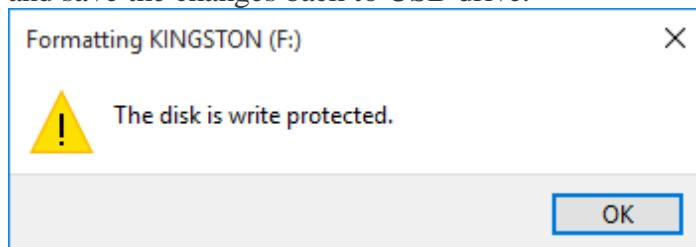


6. Double-click on WriteProtect and then change the value data from 0 to 1.



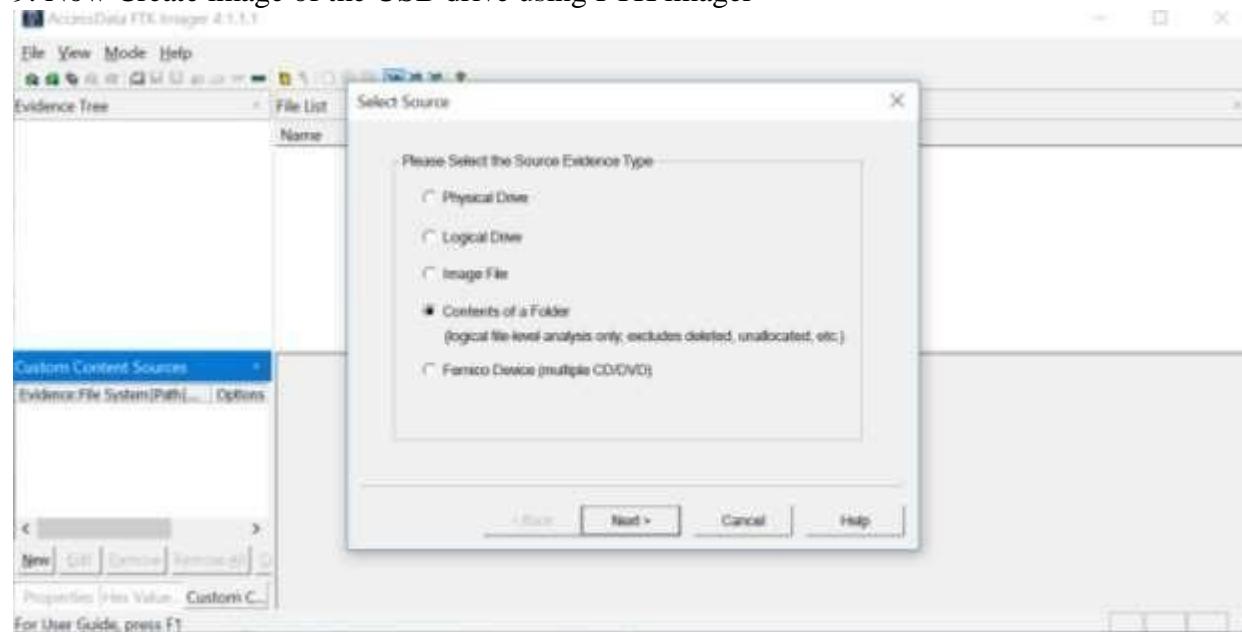
7. The new setting takes effect immediately. Every user who tries to copy / move data to USB devices or format USB drive will get the error message “The disk is write-protected”.

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.



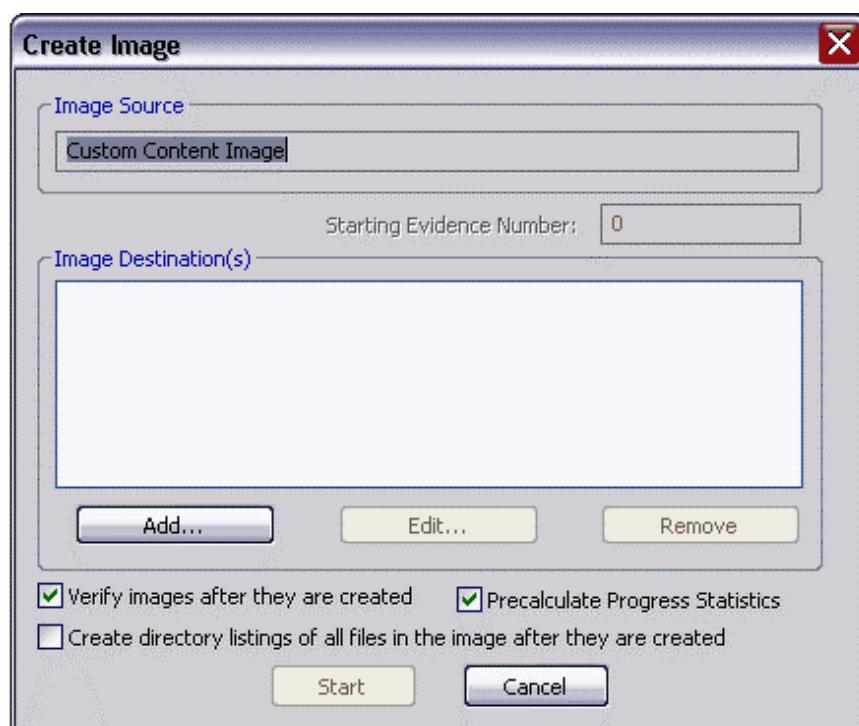
So this is how you can enable write protection to all connected USB drives. If you want to disable write protection at a later time, just open Registry Editor and set the WriteProtect value to 0.

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.



Evidence Item Information

Case Number:	001
Evidence Number:	1234
Unique Description:	none
Examiner:	ABC
Notes:	none

[**< Back**](#) [**Next >**](#) [**Cancel**](#) [**Help**](#)

- 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

Select Image Destination

Image Destination Folder	<input type="text" value="C:\Users\Kauser\Desktop"/>	Browse
Image Filename (Excluding Extension)		
<input type="text"/> Image Fragment Size (MB) <input type="text" value="1500"/> <small>For Raw, E01, and AFF formats: 0 = do not fragment</small> Compression (0=None, 1=Fastest, ..., 9=Smallest) <input type="text" value="3"/> <input type="checkbox"/> Use AD Encryption <input type="checkbox"/> Filter by File Owner		
< Back	Finish	Cancel
Help		

Creating Image...

Image Source:	<input type="text" value="E:\\"/> <small>(FAT, NTFS, exFAT, HFS+, ext2, ext3, ext4, ext5, ext6, ext7, ext8, ext9, ext10, ext11, ext12, ext13, ext14, ext15, ext16, ext17, ext18, ext19, ext20, ext21, ext22, ext23, ext24, ext25, ext26, ext27, ext28, ext29, ext30, ext31, ext32, ext33, ext34, ext35, ext36, ext37, ext38, ext39, ext40, ext41, ext42, ext43, ext44, ext45, ext46, ext47, ext48, ext49, ext50, ext51, ext52, ext53, ext54, ext55, ext56, ext57, ext58, ext59, ext60, ext61, ext62, ext63, ext64, ext65, ext66, ext67, ext68, ext69, ext70, ext71, ext72, ext73, ext74, ext75, ext76, ext77, ext78, ext79, ext80, ext81, ext82, ext83, ext84, ext85, ext86, ext87, ext88, ext89, ext90, ext91, ext92, ext93, ext94, ext95, ext96, ext97, ext98, ext99, ext100, ext101, ext102, ext103, ext104, ext105, ext106, ext107, ext108, ext109, ext110, ext111, ext112, ext113, ext114, ext115, ext116, ext117, ext118, ext119, ext120, ext121, ext122, ext123, ext124, ext125, ext126, ext127, ext128, ext129, ext130, ext131, ext132, ext133, ext134, ext135, ext136, ext137, ext138, ext139, ext140, ext141, ext142, ext143, ext144, ext145, ext146, ext147, ext148, ext149, ext150, ext151, ext152, ext153, ext154, ext155, ext156, ext157, ext158, ext159, ext160, ext161, ext162, ext163, ext164, ext165, ext166, ext167, ext168, ext169, ext170, ext171, ext172, ext173, ext174, ext175, ext176, ext177, ext178, ext179, ext180, ext181, ext182, ext183, ext184, ext185, ext186, ext187, ext188, ext189, ext190, ext191, ext192, ext193, ext194, ext195, ext196, ext197, ext198, ext199, ext200, ext201, ext202, ext203, ext204, ext205, ext206, ext207, ext208, ext209, ext210, ext211, ext212, ext213, ext214, ext215, ext216, ext217, ext218, ext219, ext220, ext221, ext222, ext223, ext224, ext225, ext226, ext227, ext228, ext229, ext2210, ext2211, ext2212, ext2213, ext2214, ext2215, ext2216, ext2217, ext2218, ext2219, ext22100, ext22101, ext22102, ext22103, ext22104, ext22105, ext22106, ext22107, ext22108, ext22109, ext22110, ext22111, ext22112, ext22113, ext22114, ext22115, ext22116, ext22117, ext22118, ext22119, ext221100, ext221101, ext221102, ext221103, ext221104, ext221105, ext221106, ext221107, ext221108, ext221109, ext221110, ext221111, ext221112, ext221113, ext221114, ext221115, ext221116, ext221117, ext221118, ext221119, ext2211100, ext2211101, ext2211102, ext2211103, ext2211104, ext2211105, ext2211106, ext2211107, ext2211108, ext2211109, ext2211110, ext2211111, ext2211112, ext2211113, ext2211114, ext2211115, ext2211116, ext2211117, ext2211118, ext2211119, ext22111100, ext22111101, ext22111102, ext22111103, ext22111104, ext22111105, ext22111106, ext22111107, ext22111108, ext22111109, ext22111110, ext22111111, ext22111112, ext22111113, ext22111114, ext22111115, ext22111116, ext22111117, ext22111118, ext22111119, ext221111100, ext221111101, ext221111102, ext221111103, ext221111104, ext221111105, ext221111106, ext221111107, ext221111108, ext221111109, ext221111110, ext221111111, ext221111112, ext221111113, ext221111114, ext221111115, ext221111116, ext221111117, ext221111118, ext221111119, ext2211111100, ext2211111101, ext2211111102, ext2211111103, ext2211111104, ext2211111105, ext2211111106, ext2211111107, ext2211111108, ext2211111109, ext2211111110, ext2211111111, ext2211111112, ext2211111113, ext2211111114, ext2211111115, ext2211111116, ext2211111117, ext2211111118, ext2211111119, ext22111111100, ext22111111101, ext22111111102, ext22111111103, ext22111111104, ext22111111105, ext22111111106, ext22111111107, ext22111111108, ext22111111109, ext22111111110, ext22111111111, ext22111111112, ext22111111113, ext22111111114, ext22111111115, ext22111111116, ext22111111117, ext22111111118, ext22111111119, ext221111111100, ext221111111101, ext221111111102, ext221111111103, ext221111111104, ext221111111105, ext221111111106, ext221111111107, ext221111111108, ext221111111109, ext221111111110, ext221111111111, ext221111111112, ext221111111113, ext221111111114, ext221111111115, ext221111111116, ext221111111117, ext221111111118, ext221111111119, ext2211111111100, ext2211111111101, ext2211111111102, ext2211111111103, ext2211111111104, ext2211111111105, ext2211111111106, ext2211111111107, ext2211111111108, ext2211111111109, ext2211111111110, ext2211111111111, ext2211111111112, ext2211111111113, ext2211111111114, ext2211111111115, ext2211111111116, ext2211111111117, ext2211111111118, ext2211111111119, ext22111111111100, ext22111111111101, ext22111111111102, ext22111111111103, ext22111111111104, ext22111111111105, ext22111111111106, ext22111111111107, ext22111111111108, ext22111111111109, ext22111111111110, ext22111111111111, ext22111111111112, ext22111111111113, ext22111111111114, ext22111111111115, ext22111111111116, ext22111111111117, ext22111111111118, ext22111111111119, ext221111111111100, ext221111111111101, ext221111111111102, ext221111111111103, ext221111111111104, ext221111111111105, ext221111111111106, ext221111111111107, ext221111111111108, ext221111111111109, ext221111111111110, ext221111111111111, ext221111111111112, ext221111111111113, ext221111111111114, ext221111111111115, ext221111111111116, ext221111111111117, ext221111111111118, ext221111111111119, ext2211111111111100, ext2211111111111101, ext2211111111111102, ext2211111111111103, ext2211111111111104, ext2211111111111105, ext2211111111111106, ext2211111111111107, ext2211111111111108, ext2211111111111109, ext2211111111111110, ext2211111111111111, ext2211111111111112, ext2211111111111113, ext2211111111111114, ext2211111111111115, ext2211111111111116, ext2211111111111117, ext2211111111111118, ext2211111111111119, ext22111111111111100, ext22111111111111101, ext22111111111111102, ext22111111111111103, ext22111111111111104, ext22111111111111105, ext22111111111111106, ext22111111111111107, ext22111111111111108, ext22111111111111109, ext22111111111111110, ext22111111111111111, ext22111111111111112, ext22111111111111113, ext22111111111111114, ext22111111111111115, ext22111111111111116, ext22111111111111117, ext22111111111111118, ext22111111111111119, ext221111111111111100, ext221111111111111101, ext221111111111111102, ext221111111111111103, ext221111111111111104, ext221111111111111105, ext221111111111111106, ext221111111111111107, ext221111111111111108, ext221111111111111109, ext221111111111111110, ext221111111111111111, ext221111111111111112, ext221111111111111113, ext221111111111111114, ext221111111111111115, ext221111111111111116, ext221111111111111117, ext221111111111111118, ext221111111111111119, ext2211111111111111100, ext2211111111111111101, ext2211111111111111102, ext2211111111111111103, ext2211111111111111104, ext2211111111111111105, ext2211111111111111106, ext2211111111111111107, ext2211111111111111108, ext2211111111111111109, ext2211111111111111110, ext2211111111111111111, ext2211111111111111112, ext2211111111111111113, ext2211111111111111114, ext2211111111111111115, ext2211111111111111116, ext2211111111111111117, ext2211111111111111118, ext2211111111111111119, ext22111111111111111100, ext22111111111111111101, ext22111111111111111102, ext22111111111111111103, ext22111111111111111104, ext22111111111111111105, ext22111111111111111106, ext22111111111111111107, ext22111111111111111108, ext22111111111111111109, ext22111111111111111110, ext22111111111111111111, ext22111111111111111112, ext22111111111111111113, ext22111111111111111114, ext22111111111111111115, ext22111111111111111116, ext22111111111111111117, ext22111111111111111118, ext22111111111111111119, ext221111111111111111100, ext221111111111111111101, ext221111111111111111102, ext221111111111111111103, ext221111111111111111104, ext221111111111111111105, ext221111111111111111106, ext221111111111111111107, ext221111111111111111108, ext221111111111111111109, ext221111111111111111110, ext221111111111111111111, ext221111111111111111112, ext221111111111111111113, ext221111111111111111114, ext221111111111111111115, ext221111111111111111116, ext221111111111111111117, ext221111111111111111118, ext221111111111111111119, ext2211111111111111111100, ext2211111111111111111101, ext2211111111111111111102, ext2211111111111111111103, ext2211111111111111111104, ext2211111111111111111105, ext2211111111111111111106, ext2211111111111111111107, ext2211111111111111111108, ext2211111111111111111109, ext2211111111111111111110, ext2211111111111111111111, ext2211111111111111111112, ext2211111111111111111113, ext2211111111111111111114, ext2211111111111111111115, ext2211111111111111111116, ext2211111111111111111117, ext2211111111111111111118, ext2211111111111111111119, ext22111111111111111111100, ext22111111111111111111101, ext22111111111111111111102, ext22111111111111111111103, ext22111111111111111111104, ext22111111111111111111105, ext22111111111111111111106, ext22111111111111111111107, ext22111111111111111111108, ext22111111111111111111109, ext22111111111111111111110, ext22111111111111111111111, ext22111111111111111111112, ext22111111111111111111113, ext22111111111111111111114, ext22111111111111111111115, ext22111111111111111111116, ext22111111111111111111117, ext22111111111111111111118, ext22111111111111111111119, ext221111111111111111111100, ext221111111111111111111101, ext221111111111111111111102, ext221111111111111111111103, ext221111111111111111111104, ext221111111111111111111105, ext221111111111111111111106, ext221111111111111111111107, ext221111111111111111111108, ext221111111111111111111109, ext221111111111111111111110, ext221111111111111111111111, ext221111111111111111111112, ext221111111111111111111113, ext221111111111111111111114, ext221111111111111111111115, ext221111111111111111111116, ext221111111111111111111117, ext221111111111111111111118, ext221111111111111111111119, ext2211111111111111111111100, ext2211111111111111111111101, ext2211111111111111111111102, ext2211111111111111111111103, ext2211111111111111111111104, ext2211111111111111111111105, ext2211111111111111111111106, ext2211111111111111111111107, ext2211111111111111111111108, ext2211111111111111111111109, ext2211111111111111111111110, ext2211111111111111111111111, ext2211111111111111111111112, ext2211111111111111111111113, ext2211111111111111111111114, ext2211111111111111111111115, ext2211111111111111111111116, ext2211111111111111111111117, ext2211111111111111111111118, ext2211111111111111111111119, ext22111111111111111111111100, ext22111111111111111111111101, ext22111111111111111111111102, ext22111111111111111111111103, ext22111111111111111111111104, ext22111111111111111111111105, ext22111111111111111111111106, ext22111111111111111111111107, ext22111111111111111111111108, ext22111111111111111111111109, ext22111111111111111111111110, ext22111111111111111111111111, ext22111111111111111111111112, ext22111111111111111111111113, ext22111111111111111111111114, ext22111111111111111111111115, ext22111111111111111111111116, ext22111111111111111111111117, ext22111111111111111111111118, ext22111111111111111111111119, ext221111111111111111111111100, ext221111111111111111111111101, ext221111111111111111111111102, ext221111111111111111111111103, ext221111111111111111111111104, ext221111111111111111111111105, ext221111111111111111111111106, ext221111111111111111111111107, ext221111111111111111111111108, ext221111111111111111111111109, ext221111111111111111111111110, ext221111111111111111111111111, ext221111111111111111111111112, ext221111111111111111111111113, ext221111111111111111111111114, ext221111111111111111111111115, ext221111111111111111111111116, ext221111111111111111111111117, ext221111111111111111111111118, ext221111111111111111111111119, ext2211111111111111111111111100, ext2211111111111111111111111101, ext2211111111111111111111111102, ext2211111111111111111111111103, ext2211111111111111111111111104, ext2211111111111111111111111105, ext2211111111111111111111111106, ext2211111111111111111111111107, ext2211111111111111111111111108, ext2211111111111111111111111109, ext2211111111111111111111111110, ext2211111111111111111111111111, ext2211111111111111111111111112, ext2211111111111111111111111113, ext2211111111111111111111111114, ext2211111111111111111111111115, ext2211111111111111111111111116, ext2211111111111111111111111117, ext2211111111111111111111111118, ext2211111111111111111111111119, ext22111111111111111111111111100, ext22111111111111111111111111101, ext22111111111111111111111111102, ext22111111111111111111111111103, ext22111111111111111111111111104, ext22111111111111111111111111105, ext22111111111111111111111111106, ext22111111111111111111111111107, ext22111111111111111111111111108, ext22111111111111111111111111109, ext22111111111111111</small>
---------------	---

Practical No – 3**Aim: Forensics Case Study:**

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

Steps:

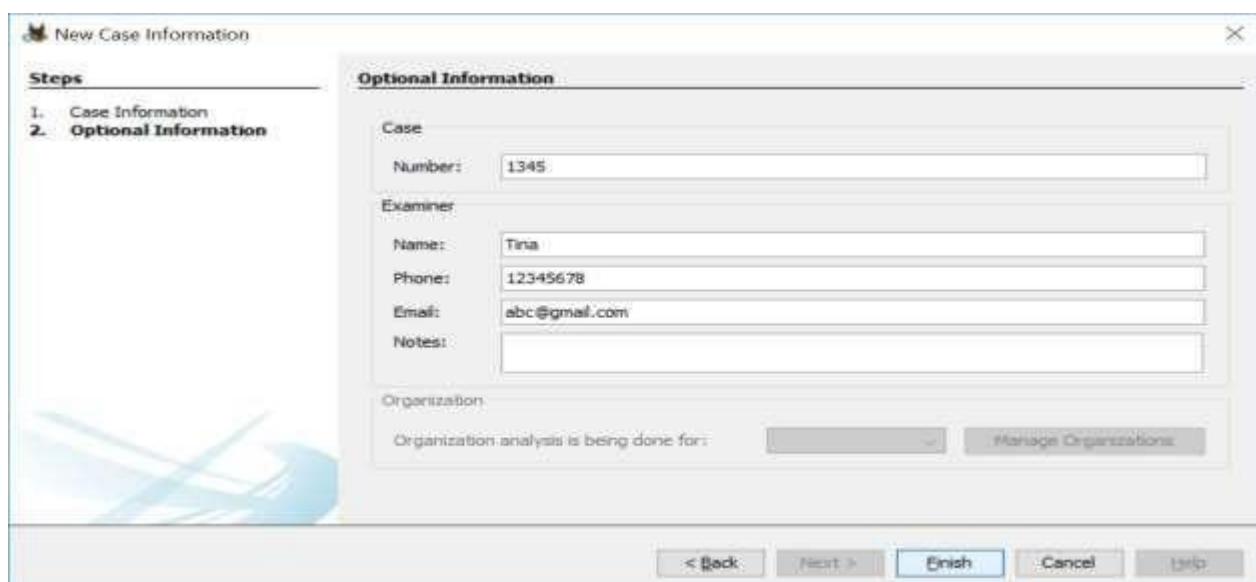
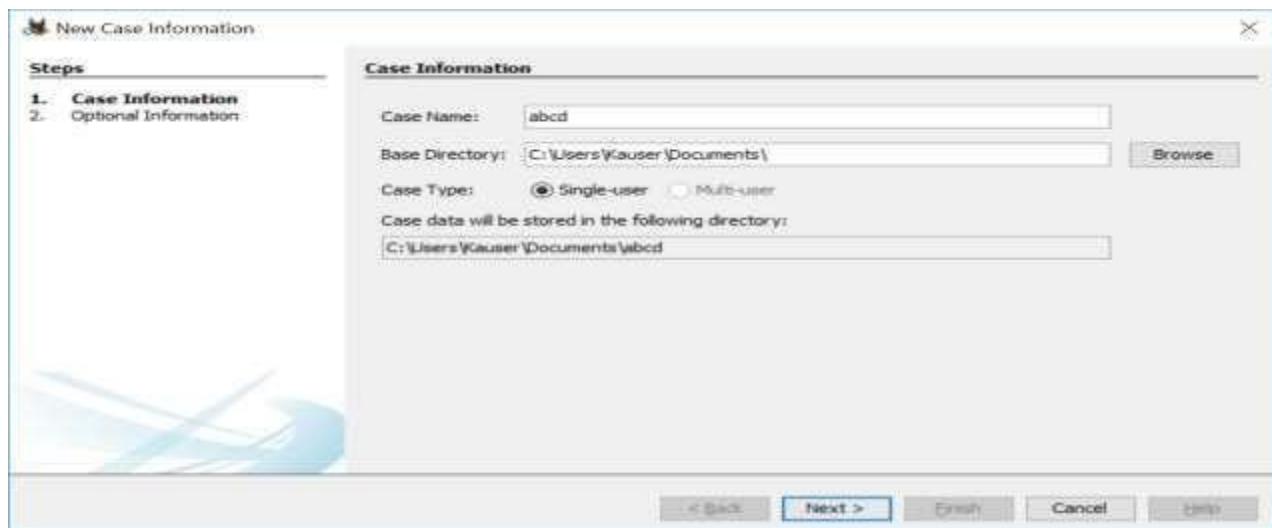
1. Start Autopsy



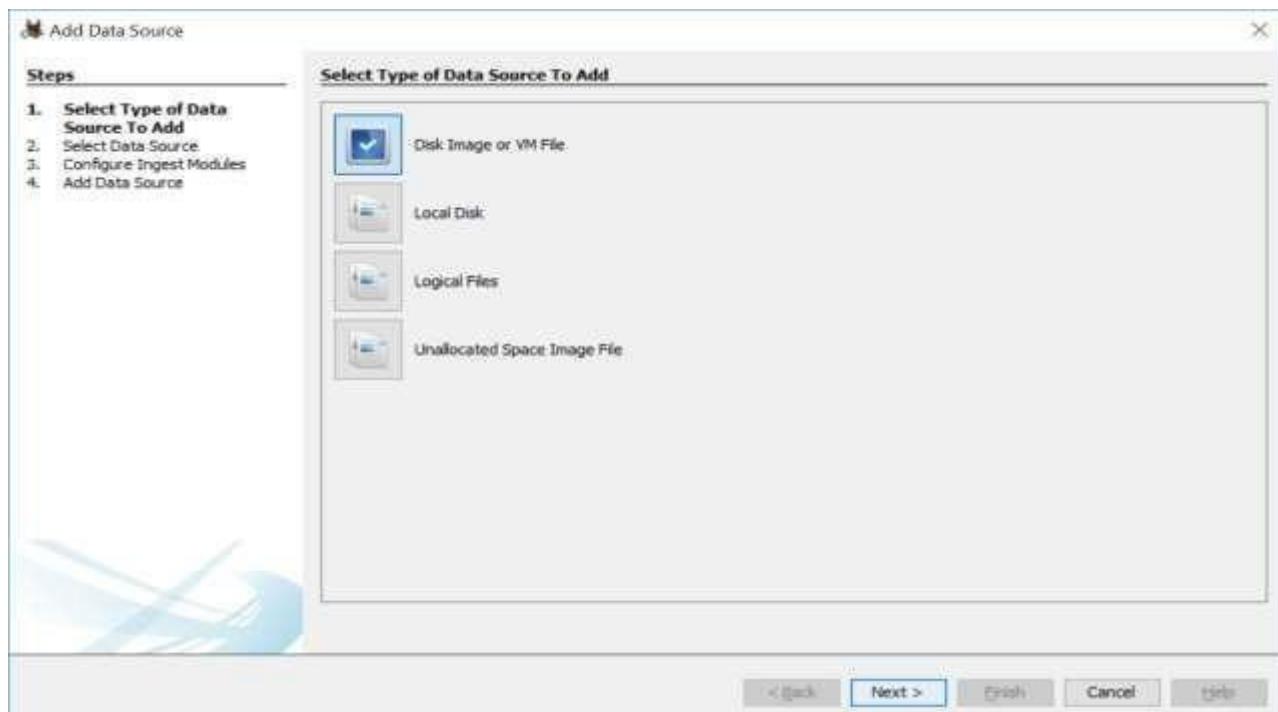
2. Select New Case



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

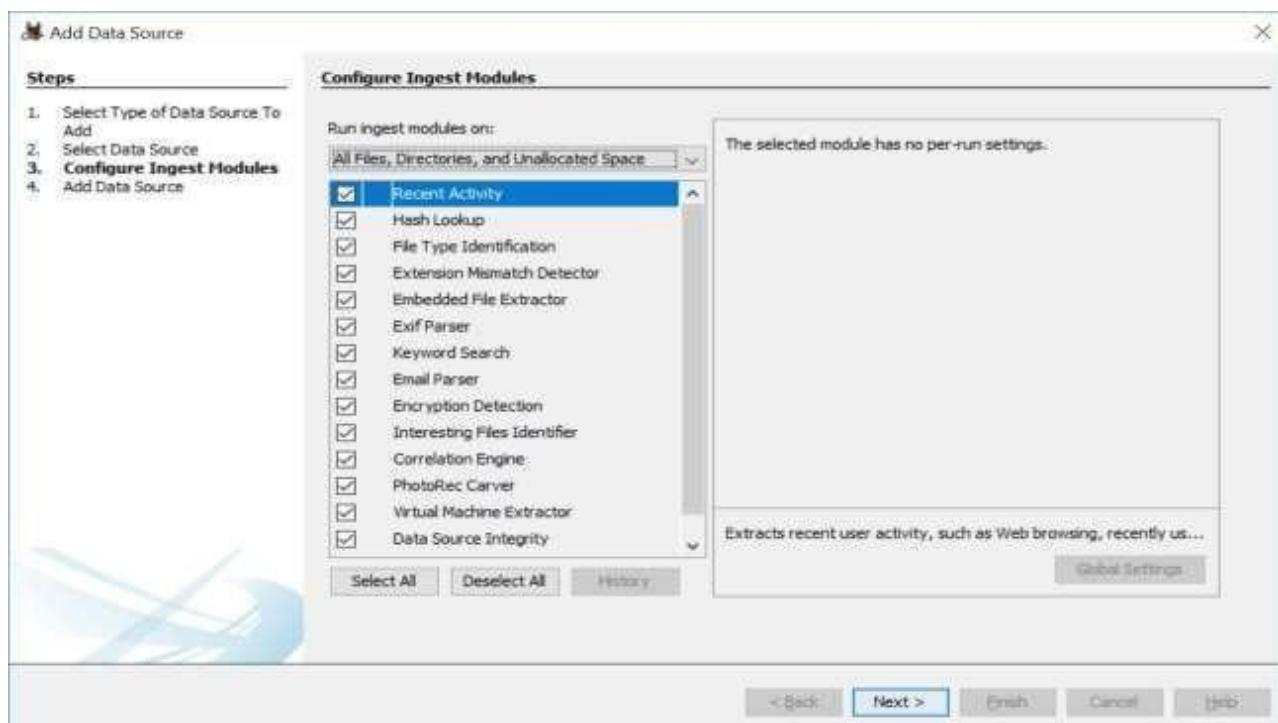


4. Select the type of Data Source that has to be added

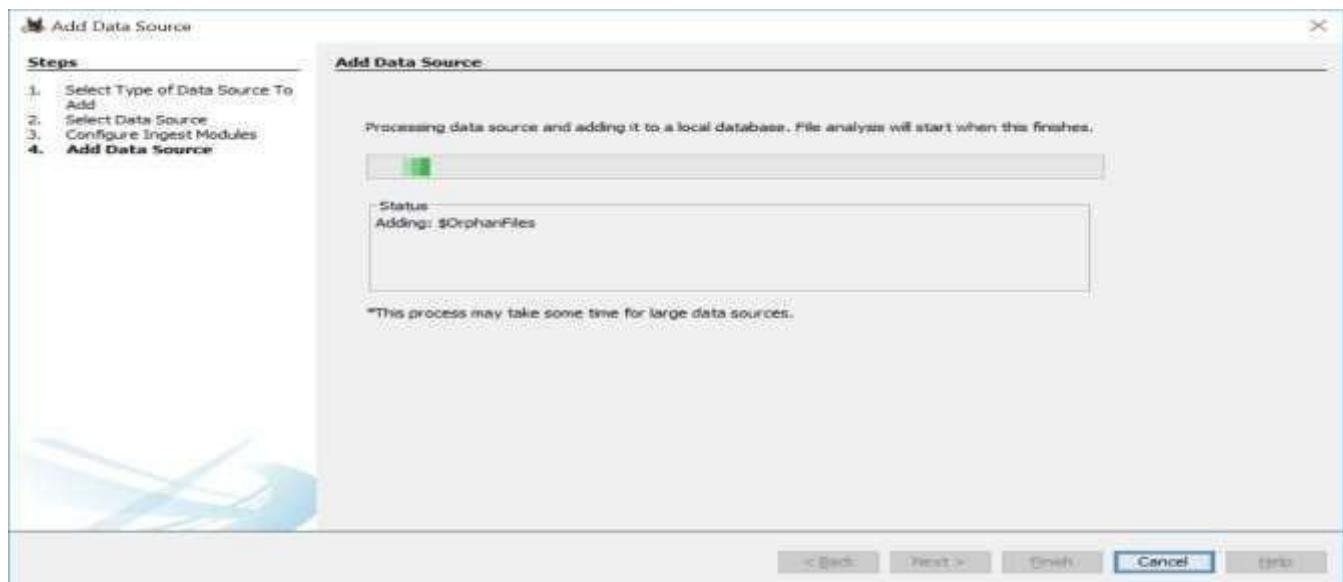


5. Select Data Source(here a previously made image file of a USB is selected)

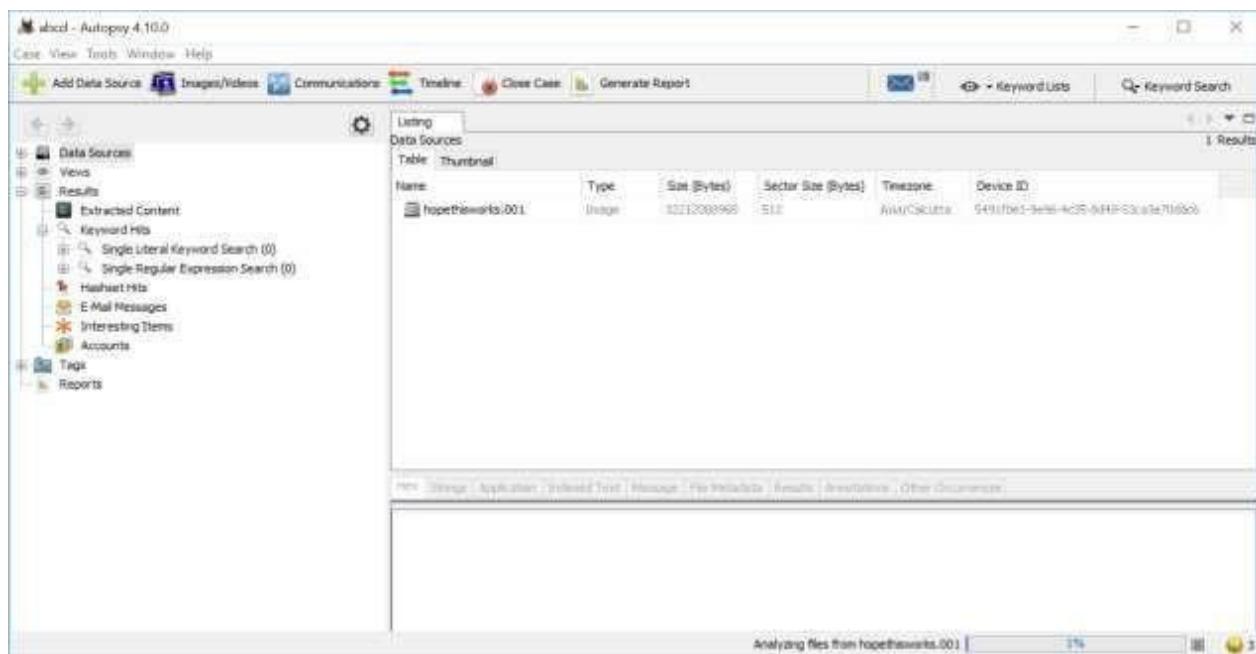
6. Select all ingest modules



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



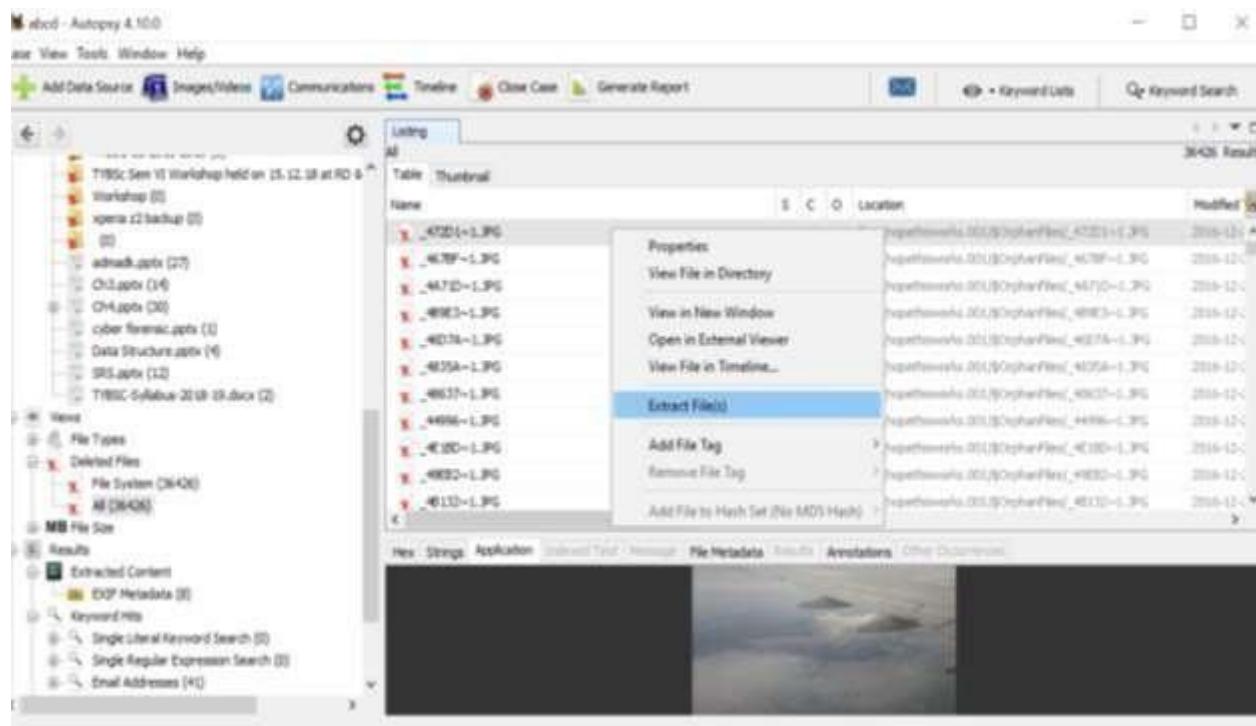
9. All files will appear in table tab select any file to see the data.

Name	S	C	O	Location	Modified Time
OrphanFiles				/img_hopeithworks.001//OrphanFile	2000-01-01 00:00:00
IFAT1				/img_hopeithworks.001//IFAT1	2000-01-01 00:00:00
IFAT2				/img_hopeithworks.001//IFAT2	2000-01-01 00:00:00
gpart				/img_hopeithworks.001//gpart	2000-01-01 00:00:00
Deleted Files				/img_hopeithworks.001//Deleted	2018-01-01 00:00:00
_images				/img_hopeithworks.001//_images	2018-01-01 14:21:44 EST
_ogg				/img_hopeithworks.001//ogg	2018-12-21 15:56:57 EST
_OST.DIR				/img_hopeithworks.001//_OST.DIR	2018-01-23 23:42:50 EST
Algo				/img_hopeithworks.001//Algo	2018-12-21 13:56:08 EST
Android				/img_hopeithworks.001//Android	2018-12-21 13:56:08 EST
Bird.Box.2018.WBRIp.x264-FGT				/img_hopeithworks.001//Bird.Box.2018.WBRIp.x264-FGT	2019-01-19 13:12:01 EST
cyber				/img_hopeithworks.001//cyber	2018-12-18 17:04:14 EST
d3mef0-2e05-adbe-88aa-254239bc12f1				/img_hopeithworks.001//d3mef0-2e05-adbe-88aa-254239bc12f1	2018-01-23 15:56:57 EST
Data Structure (71)				/img_hopeithworks.001//Data Structure	2018-01-23 23:42:50 EST
headstructure (0)				/img_hopeithworks.001//headstructure	2018-01-23 23:42:50 EST
logo print (0)				/img_hopeithworks.001//logo print	2018-01-23 23:42:50 EST
New folder (9)				/img_hopeithworks.001//New folder	2018-01-23 23:42:50 EST
Sem II (0)				/img_hopeithworks.001//Sem II	2018-01-23 23:42:50 EST
System Volume Information (4)				/img_hopeithworks.001//System Volume Information	2018-01-23 23:42:50 EST
TBSC CS 2018-2019 (0)				/img_hopeithworks.001//TBSC CS 2018-2019	2018-01-23 23:42:50 EST
TBSC Sem VI Workshop held on 15.12.18 at RD 5				/img_hopeithworks.001//TBSC Sem VI Workshop held on 15.12.18 at RD 5	2018-01-23 23:42:50 EST
Workshop (0)				/img_hopeithworks.001//Workshop	2018-01-23 23:42:50 EST
xperie z2 backup (0)				/img_hopeithworks.001//xperie z2 backup	2018-01-23 23:42:50 EST
(0)				/img_hopeithworks.001//(0)	2018-01-23 23:42:50 EST
admark.pptx (27)				/img_hopeithworks.001//admark.pptx	2018-12-18 14:21:44 EST
Ch3.pptx (14)				/img_hopeithworks.001//Ch3.pptx	2018-12-18 14:21:44 EST
Ch4.pptx (30)				/img_hopeithworks.001//Ch4.pptx	2018-12-18 14:21:44 EST
cyber forensic.pptx (1)				/img_hopeithworks.001//cyber forensic.pptx	2018-12-18 14:21:44 EST
Data Structure (4)				/img_hopeithworks.001//Data Structure	2018-12-18 14:21:44 EST
GR5.pptx (12)				/img_hopeithworks.001//GR5.pptx	2018-12-18 14:21:44 EST
TBSC syllabus-2018-19.docx (2)				/img_hopeithworks.001//TBSC syllabus-2018-19.docx	2018-12-18 14:21:44 EST

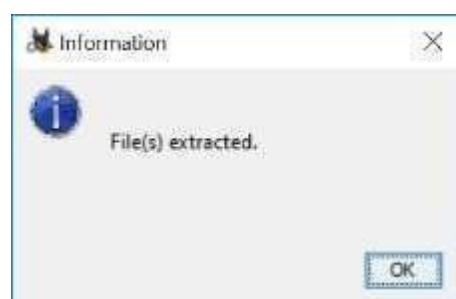
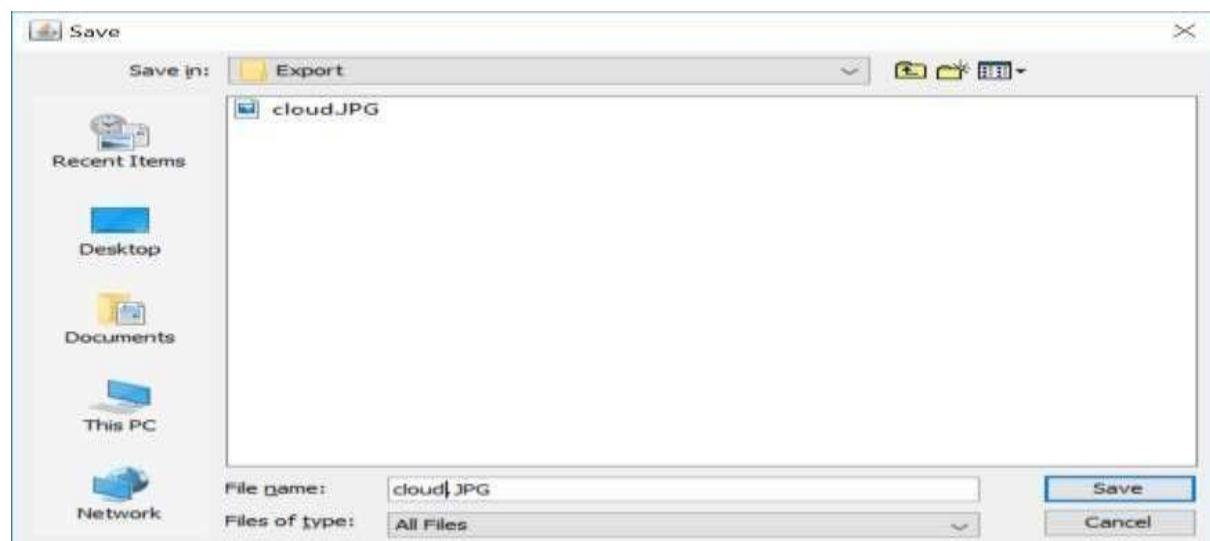
10. Expand the tree from left side panel to view the files and then expand the deleted files node

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

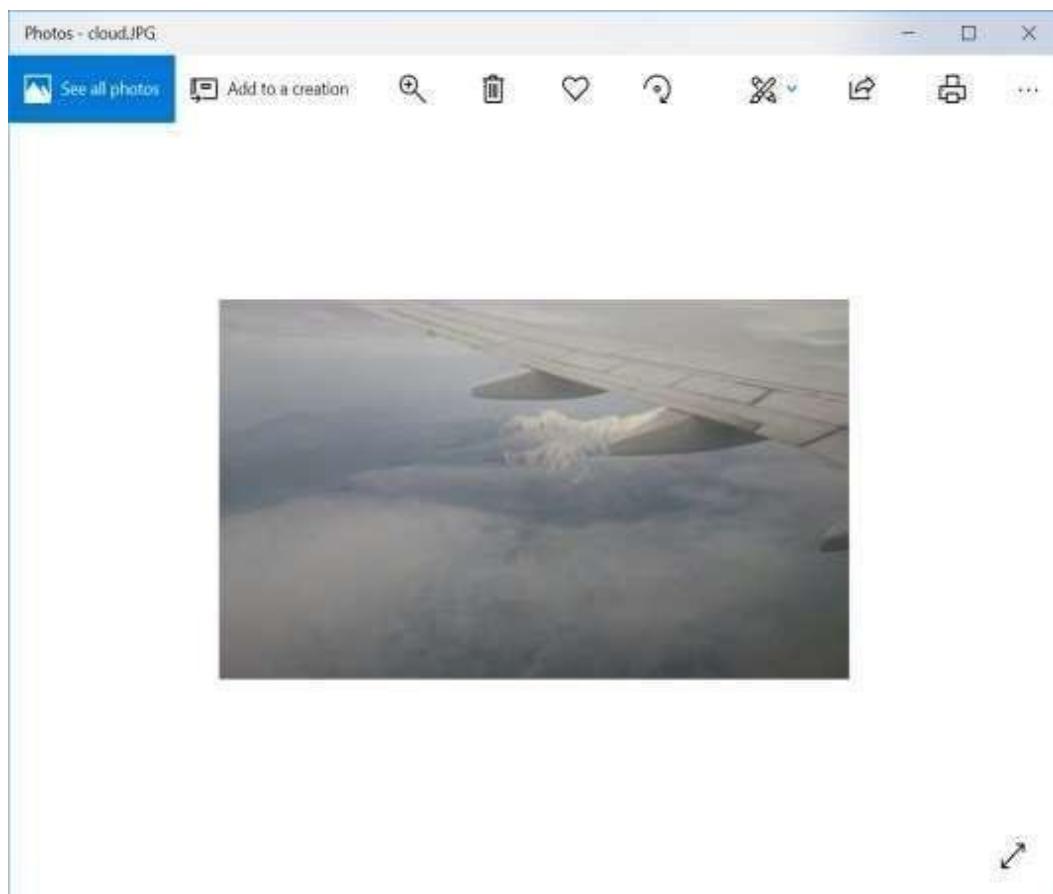
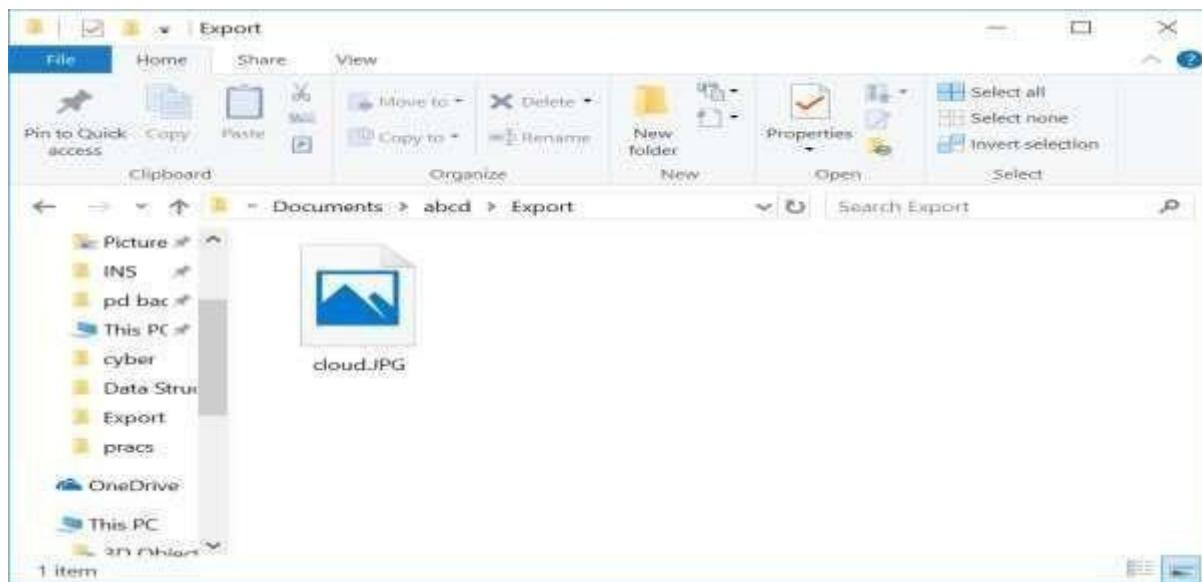
Name	S	C	O	Location	Modified
_472D1~1.JPG				/img_hopeithworks.001//OrphanFile/_472D1~1.JPG	2018-12-
_4678F~1.JPG				/img_hopeithworks.001//OrphanFile/_4678F~1.JPG	2018-12-
_4A71D~1.JPG				/img_hopeithworks.001//OrphanFile/_4A71D~1.JPG	2018-12-
_4B1E3~1.JPG				/img_hopeithworks.001//OrphanFile/_4B1E3~1.JPG	2018-12-
_4B07A~1.JPG				/img_hopeithworks.001//OrphanFile/_4B07A~1.JPG	2018-12-
_4B35A~1.JPG				/img_hopeithworks.001//OrphanFile/_4B35A~1.JPG	2018-12-
_4B837~1.JPG				/img_hopeithworks.001//OrphanFile/_4B837~1.JPG	2018-12-
_44996~1.JPG				/img_hopeithworks.001//OrphanFile/_44996~1.JPG	2018-12-
_4E1BD~1.JPG				/img_hopeithworks.001//OrphanFile/_4E1BD~1.JPG	2018-12-
_49EB2~1.JPG				/img_hopeithworks.001//OrphanFile/_49EB2~1.JPG	2018-12-
_4B132~1.JPG				/img_hopeithworks.001//OrphanFile/_4B132~1.JPG	2018-12-



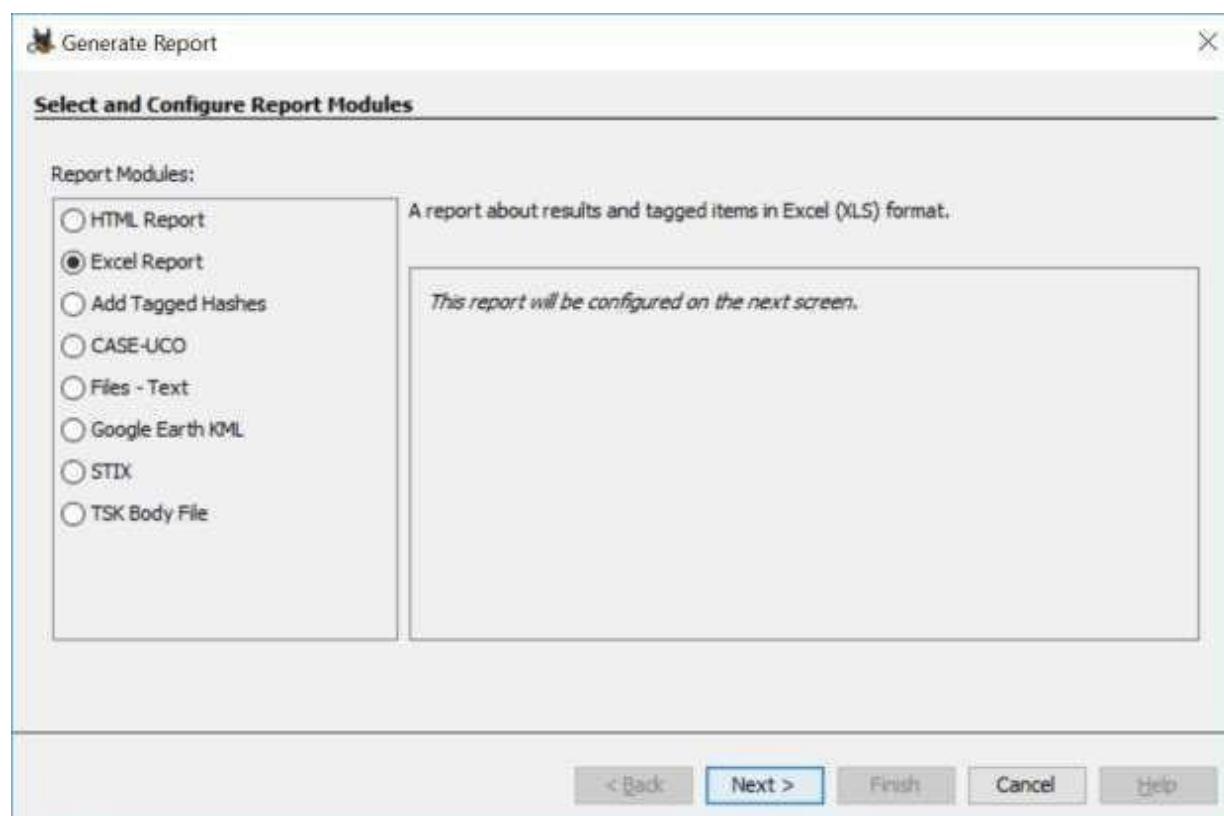
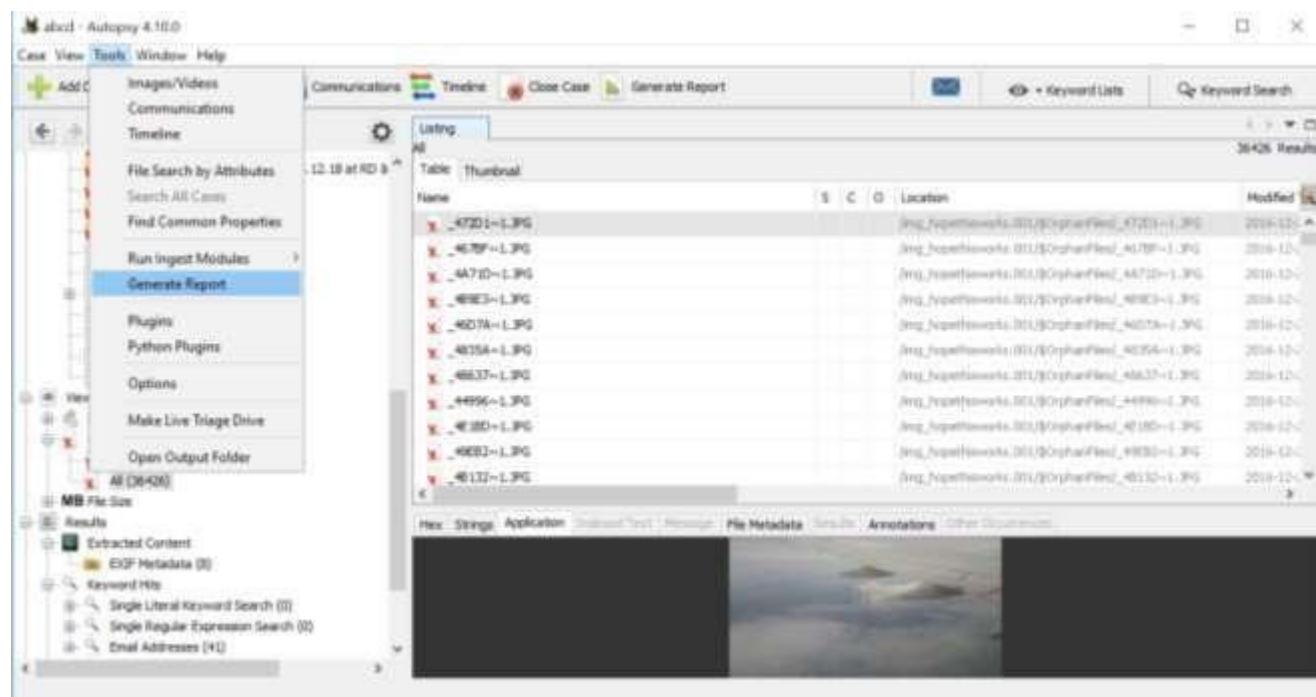
12. By default Export folder is choose to save the recovered file.



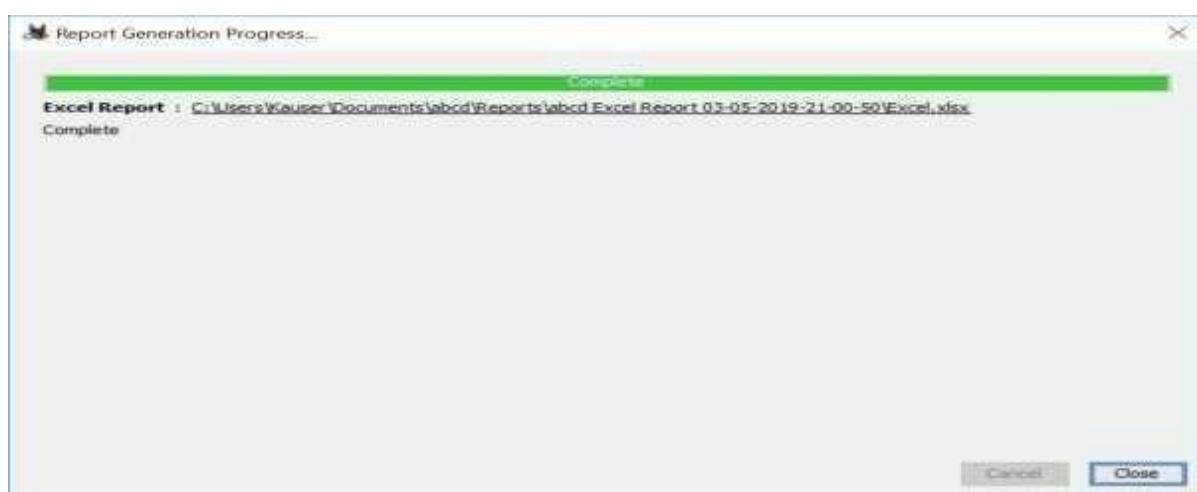
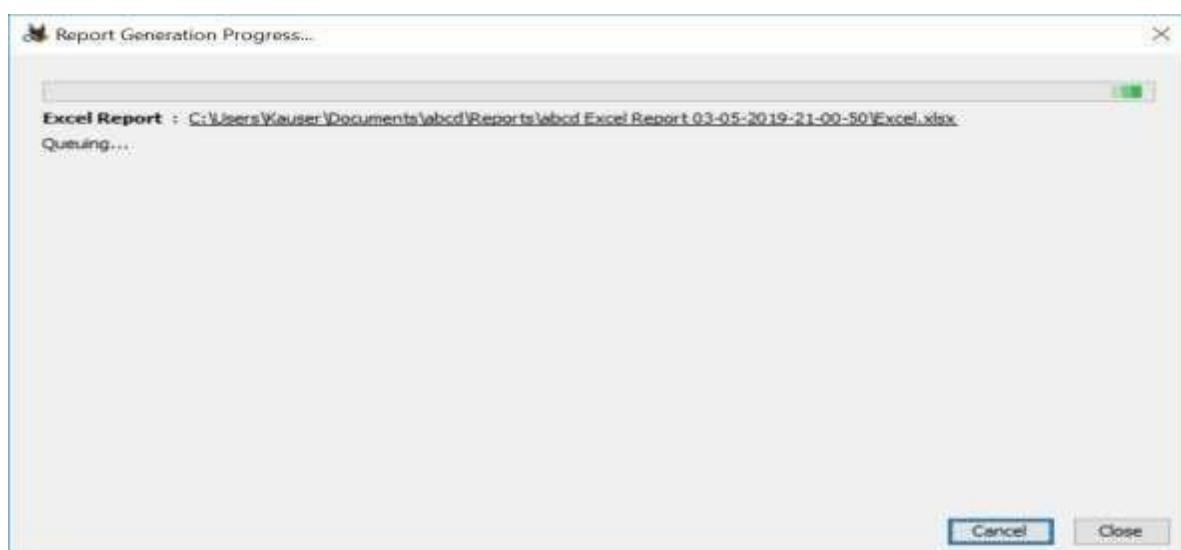
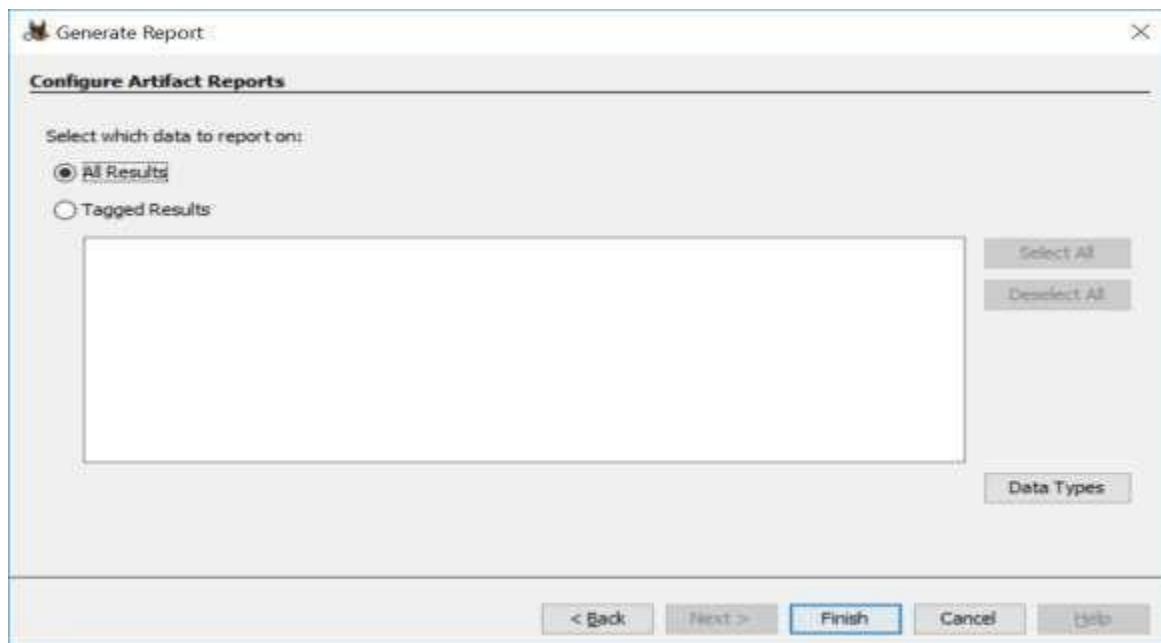
13. Now go to the Export Folder to view Recover file.



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

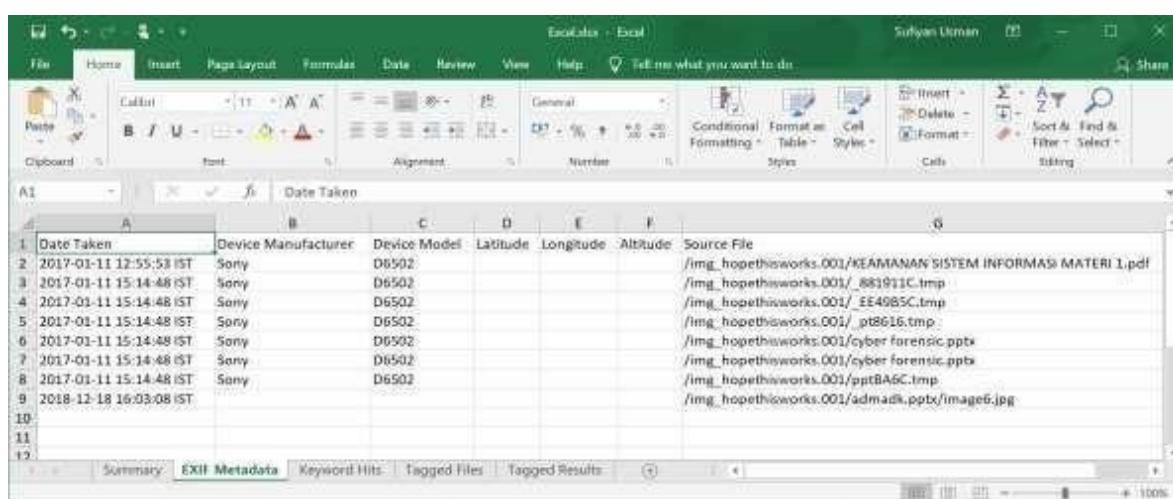
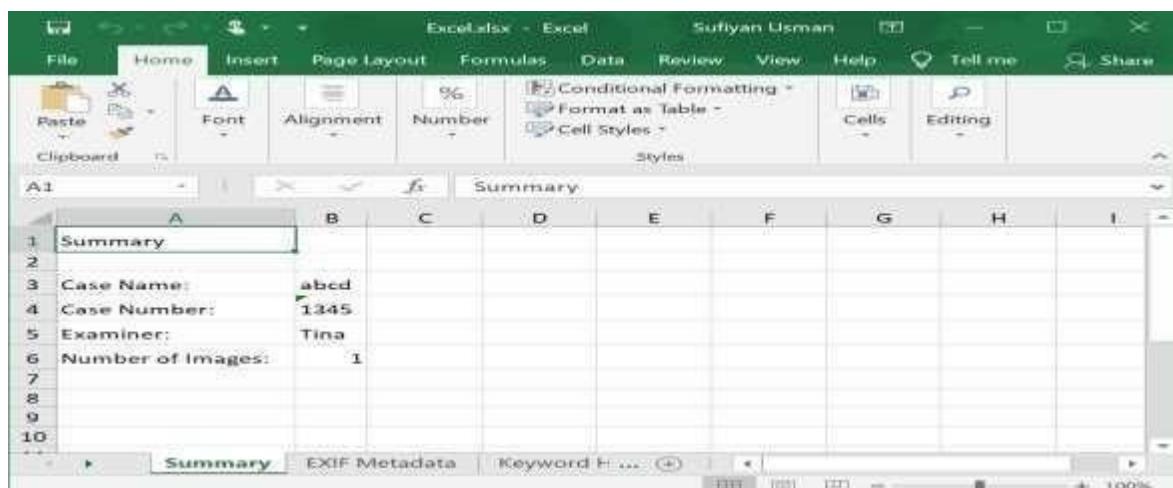
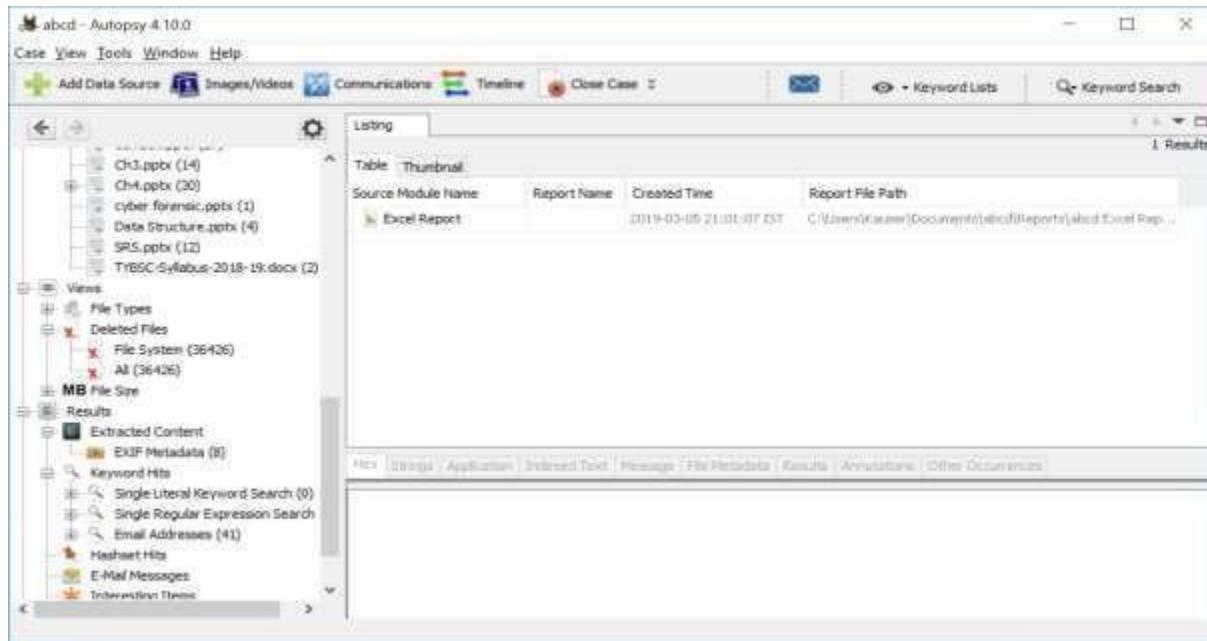


15. Click Finish after selecting All Results



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

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



Practical No – 4

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

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

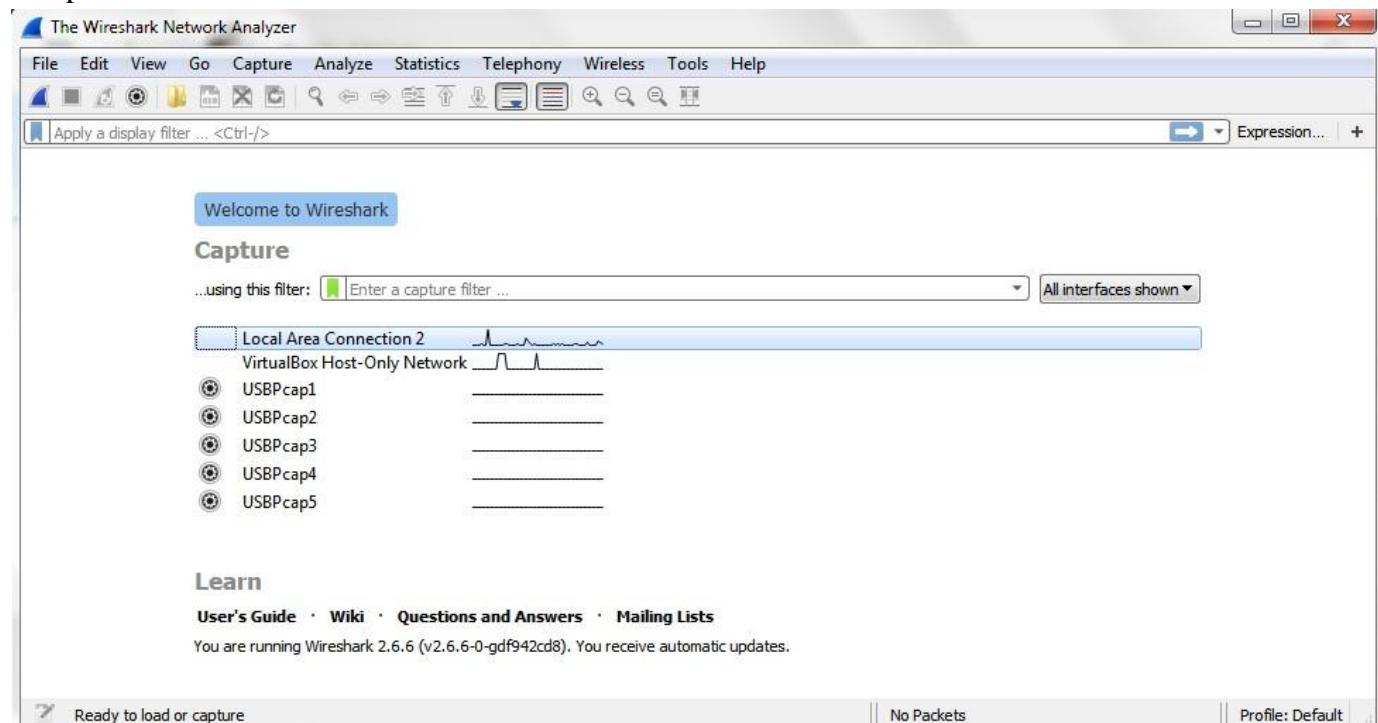
Steps:

Capturing Packets

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

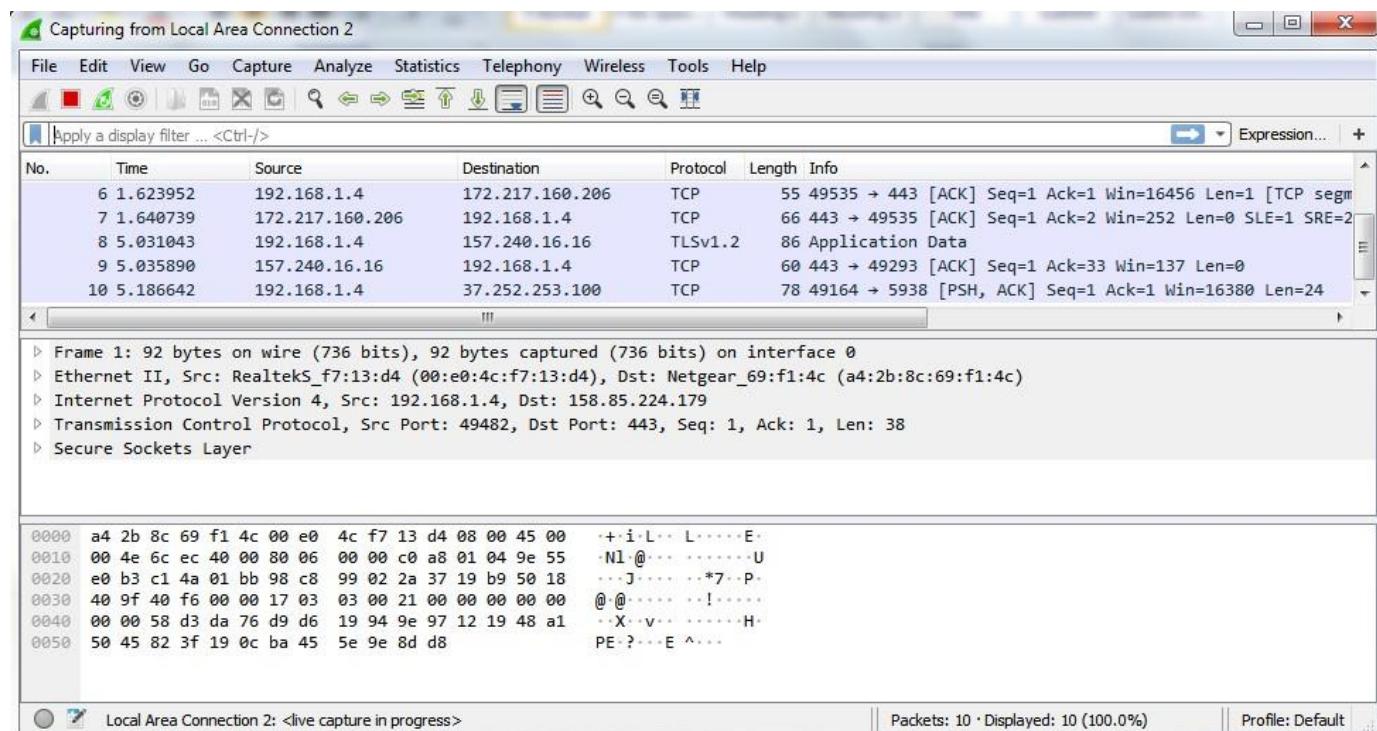
You can configure advanced features by clicking Capture > Options, but this isn't necessary for now.

1. Open Wireshark and click on Ethernet.

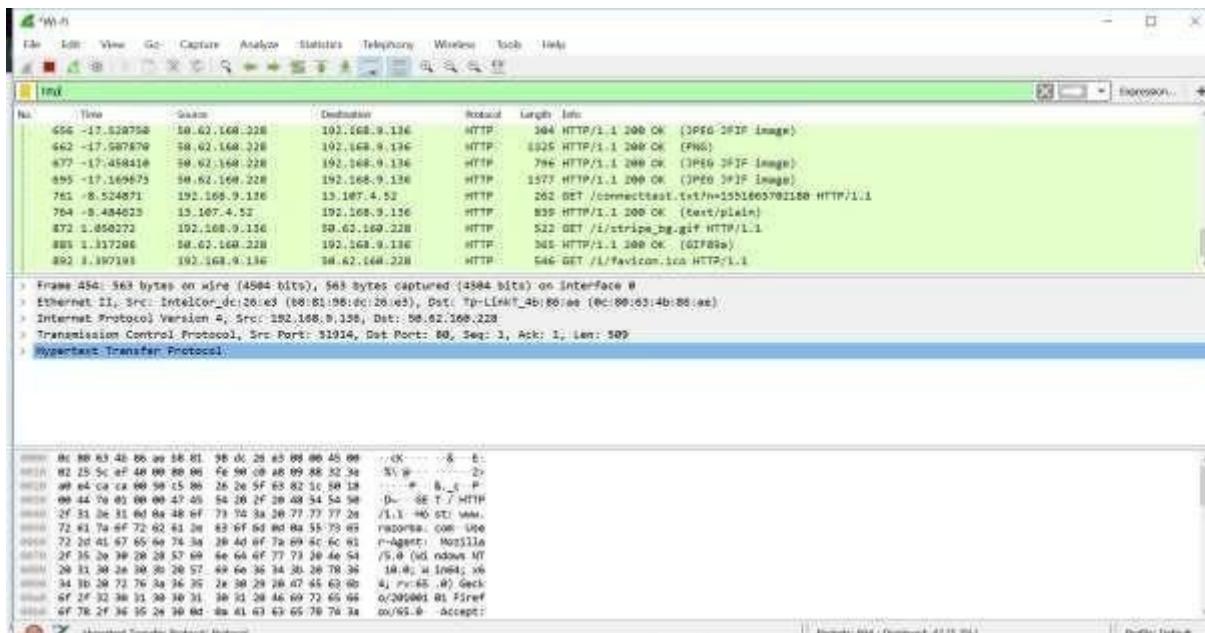


As soon as you single-click on your network interface's name, you can see how the packets are working in real time. Wireshark will capture all the packets going in and out of our systems. Promiscuous mode is the mode in which you can see all the packets from other systems on the network and not only 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

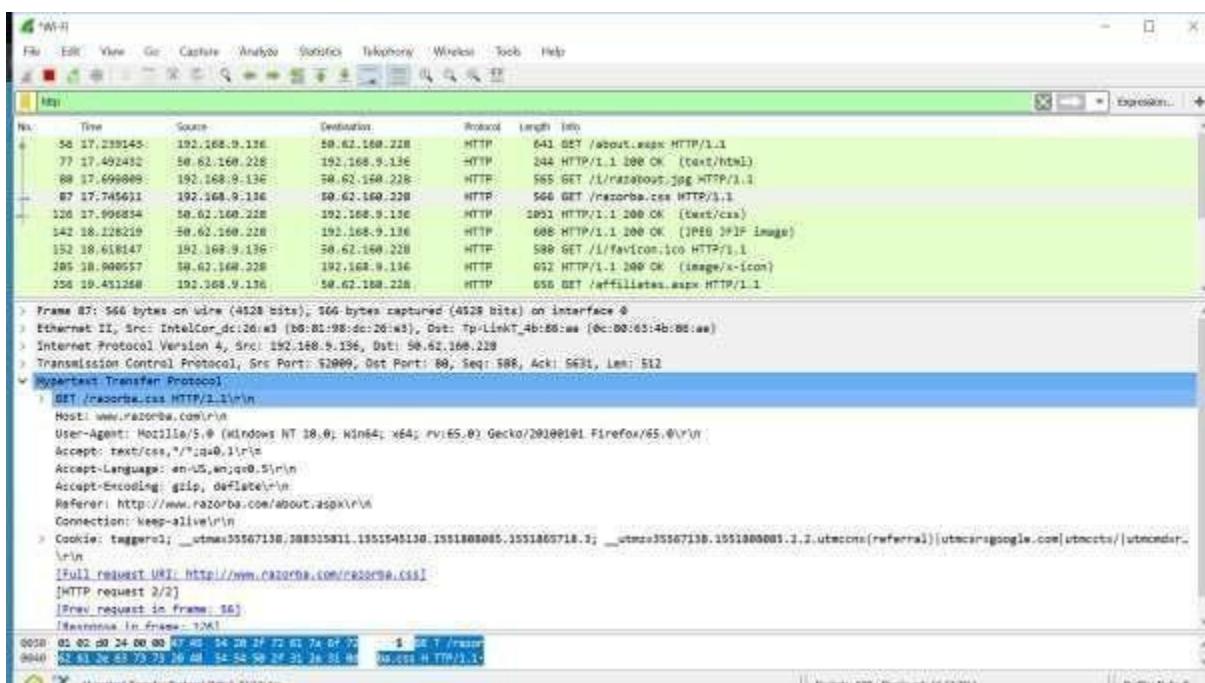
checkbox is selected and activated at the bottom of the window. The checkbox says “Enable promiscuous mode on all interfaces”.



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:

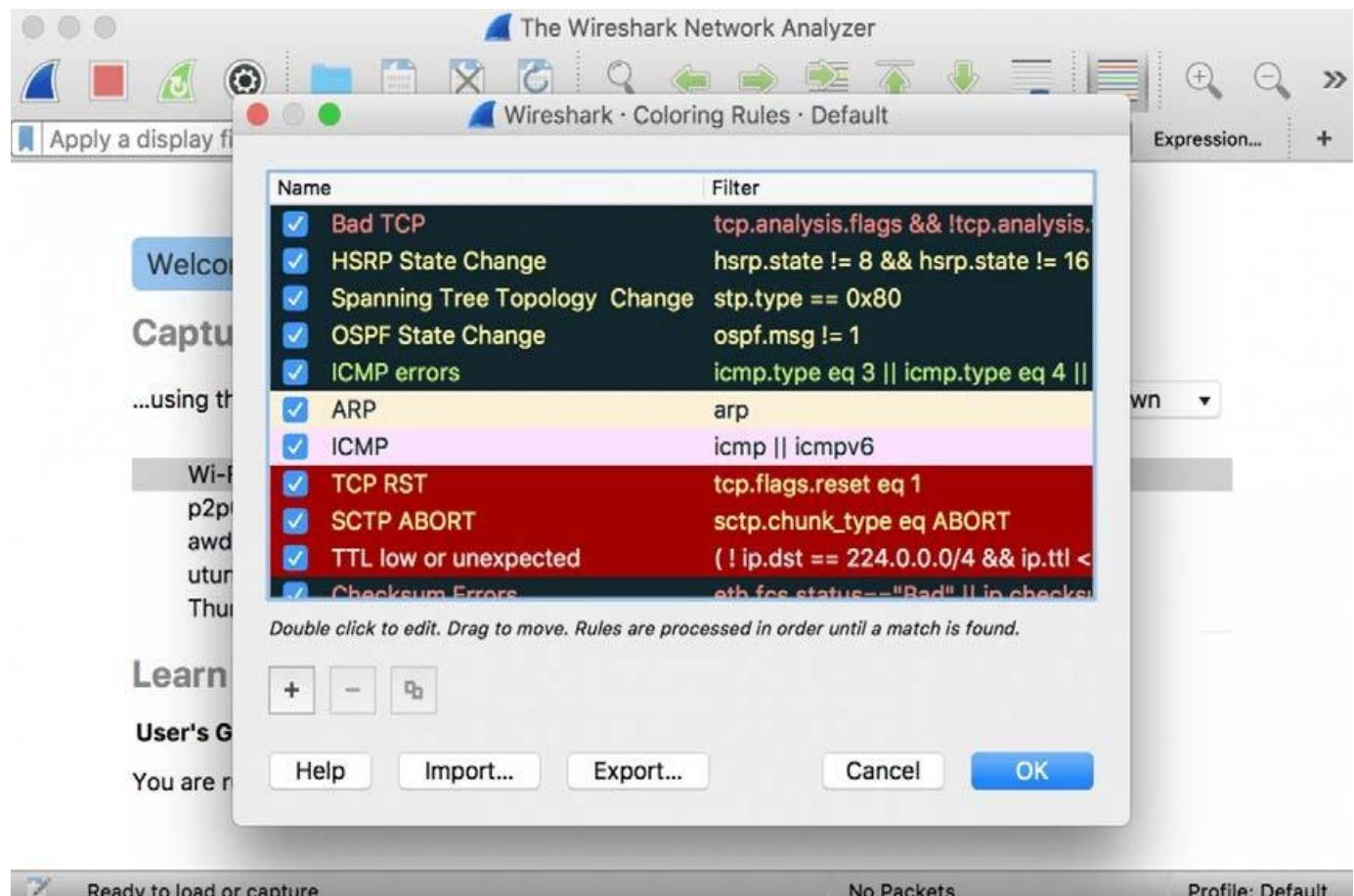
Light Purple color for TCP traffic

Blue color for UDP traffic

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

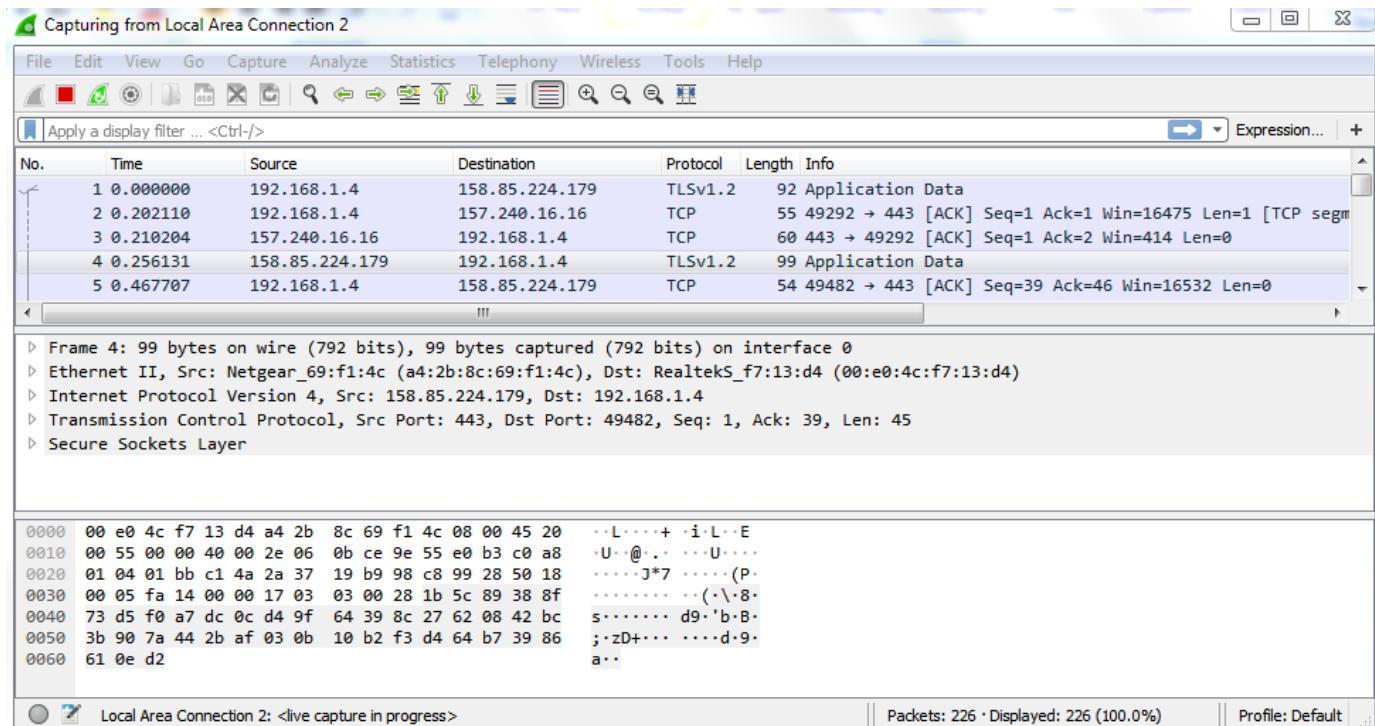
manner.

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.

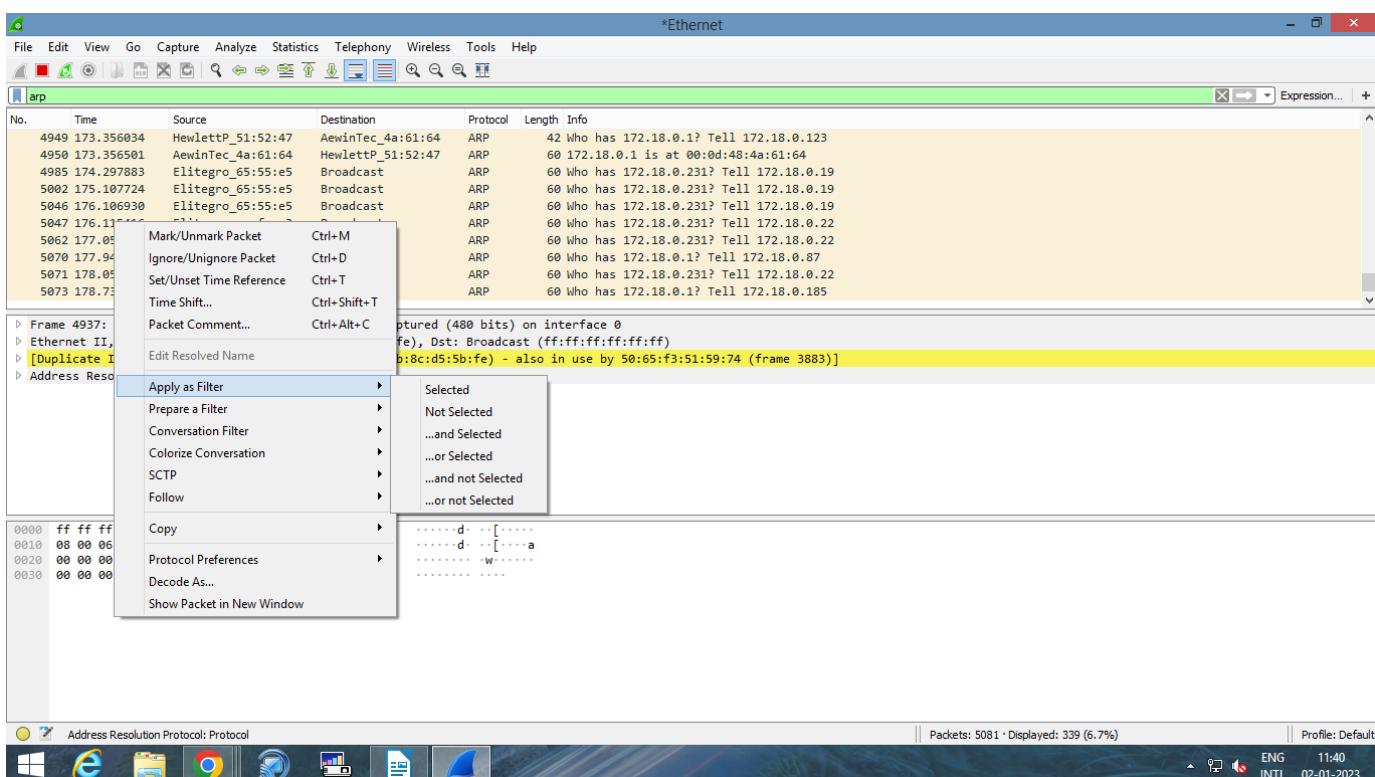


Analyze the captured Packets:

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



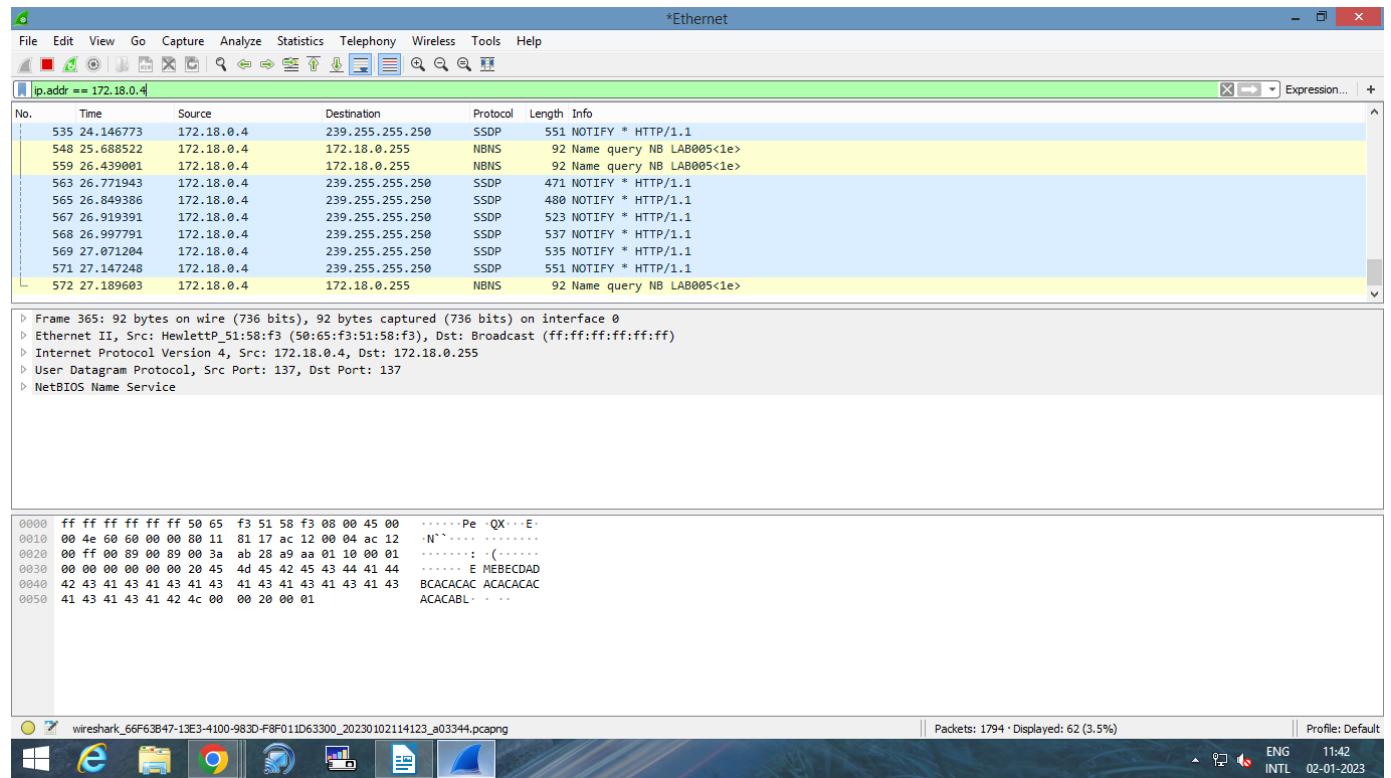
Filters can also be created from here. Right-click on one of any details. From the menu select Apply as Filter drop-down menu so filter based on it can be created.



Display filter command –

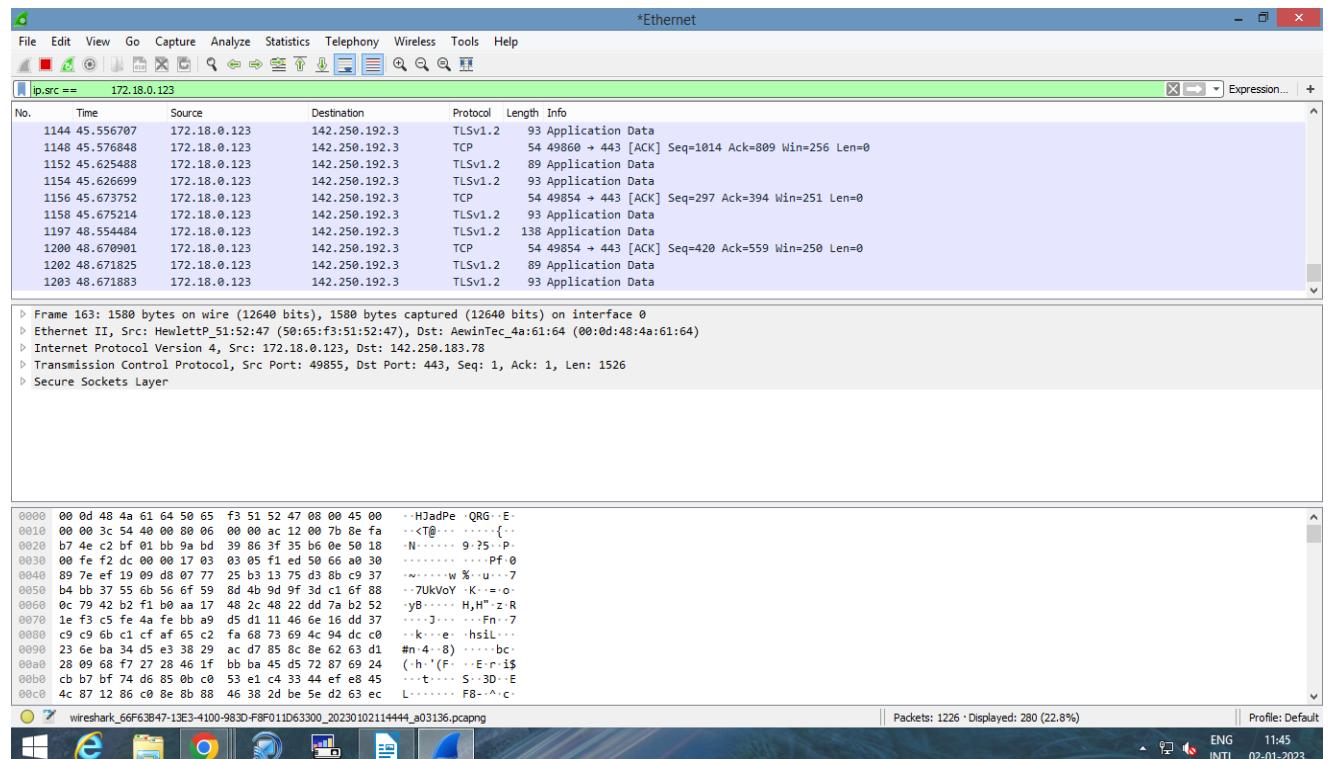
1. Display packets based on specific IP-address

`ip.addr == 172.18.0.4`



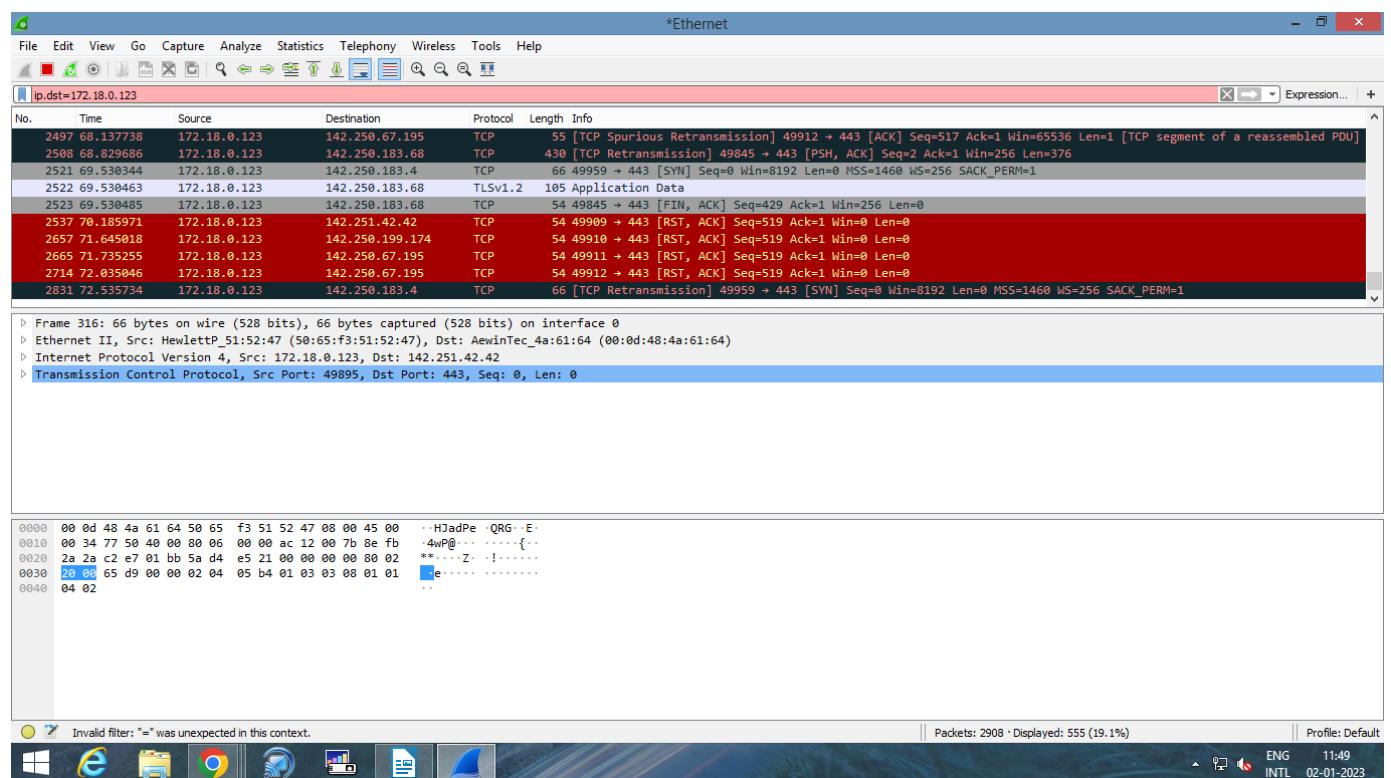
2. Display packets which are coming from specific IP-address

`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
39218	279.483458	192.168.1.4	23.57.219.27	OCSP	137	Request

5. Display packets which are using http request

http.request

*Ethernet						
No.	Time	Source	Destination	Protocol	Length	Info
20526	459.955737	172.18.0.90	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
20537	460.271521	172.18.0.24	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
20538	460.390335	172.18.0.248	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
20540	460.427021	172.18.0.181	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
20546	461.282367	172.18.0.24	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
20548	461.407436	172.18.0.248	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
20550	461.426926	172.18.0.181	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
20561	462.283699	172.18.0.24	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
20563	462.419378	172.18.0.248	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
20564	462.426905	172.18.0.181	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1

Frame 301: 217 bytes on wire (1736 bits), 217 bytes captured (1736 bits) on interface 0

Ethernet II, Src: HewlettP_51:59:74 (50:65:f3:51:59:74), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)

Internet Protocol Version 4, Src: 172.18.0.97, Dst: 239.255.255.250

User Datagram Protocol, Src Port: 53923, Dst Port: 1900

Simple Service Discovery Protocol

0000	01 00 54 7f ff fa 50 65 f3 51 59 74 08 00 45 00	...Pe .QYt: E-
0010	00 cb 24 ff 00 00 01 11 f7 b5 ac 12 00 61 ff ff	...\$a..
0020	ff fa d2 a3 07 6c 00 b7 19 8a 4d 2d 53 45 41 52	...l... M-SEAR
0030	43 48 20 2a 20 48 54 54 58 2f 31 2e 31 0d 0a 48	CH * HTT P/1.1..H
0040	47 53 54 3a 20 32 33 39 2e 32 35 2e 32 35 35	OST: 239 .255.255
0050	2e 32 35 38 3a 31 39 38 30 0d 0a 4d 41 4a 3a 20	.250:190 0 ..MAN:
0060	22 73 73 64 70 3a 64 69 73 6f 76 65 72 22 0d	"ssdp:discover".
0070	0a 4d 58 3a 20 31 0d 0a 53 54 3a 26 75 72 6e 3a	MX: 1.. ST: urn:
0080	64 69 61 6c 2d 6d 75 6c 74 69 73 63 72 65 66	dial-mul tiscreen
0090	2d 6f 72 67 73 65 72 6c 43 68 72 6f 6d 65 2f 31	-org:ser vice:dia
00a0	6c 3a 31 0d 0a 55 53 45 52 2d 41 47 45 4e 54 3a	1:1- USE R-AGENT:
00b0	20 47 6f 67 6c 65 20 43 68 72 6f 6d 65 2f 31	Google Chrome/1
00c0	30 38 2e 30 2e 35 33 35 39 2e 31 32 35 20 57 69	08.0.535 9.125 Wi

Packets: 20587 · Displayed: 1471 (7.1%)

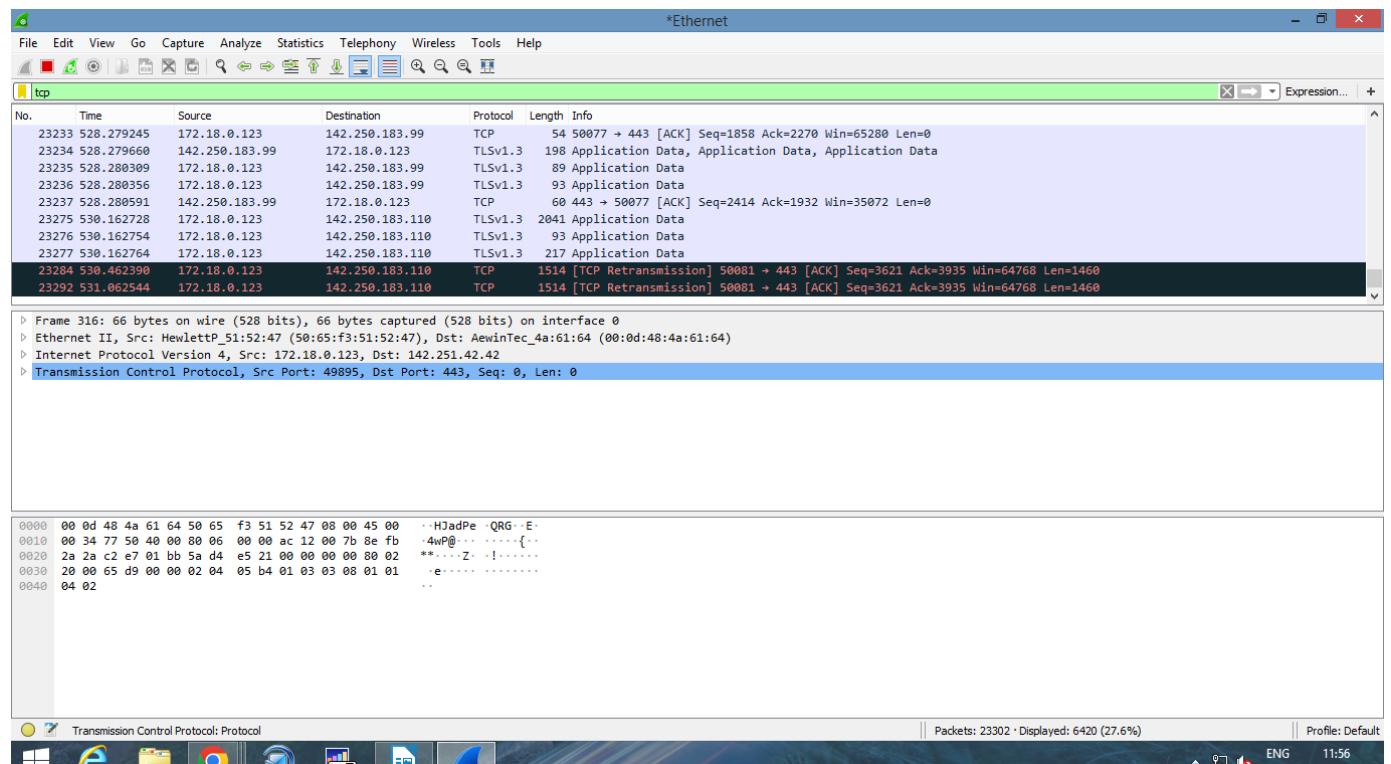
Profile: Default

Request: Boolean

ENG 11:55
INTL 02-01-2023

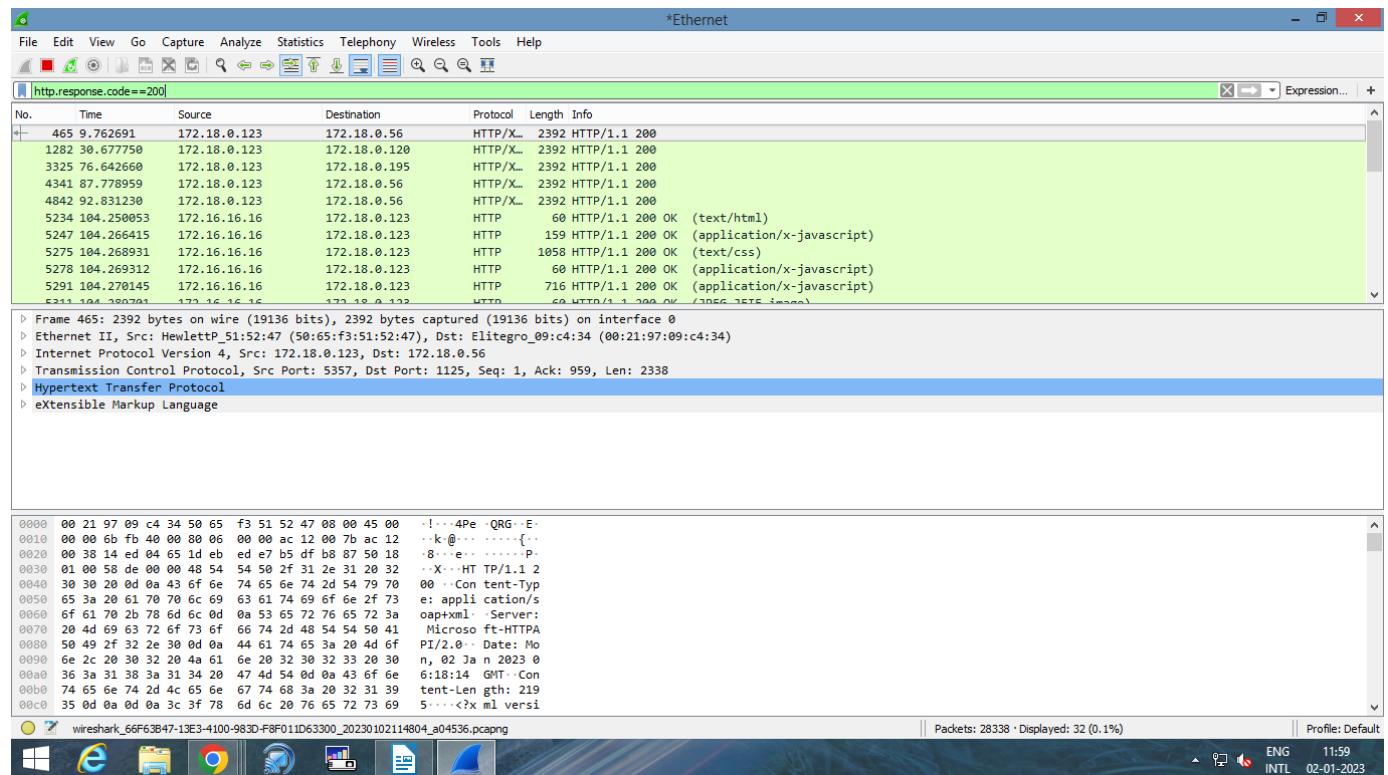
6. Display packets which are using TCP protocol

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 80

No.	Time	Source	Destination	Protocol	Length	Info
40216	315.186100	192.168.1.4	172.217.160.206	TCP	54	49295 → 80 [ACK] Seq=1 Ack=1 Win=66240 Len=0
40217	315.186313	192.168.1.4	172.217.160.206	HTTP	293	HEAD /edgedl/release2/chrome_component/H07sha1Vdw_4916/4916_all_crl-set-13576662708261436161.data.cr
40218	315.209073	172.217.160.206	192.168.1.4	TCP	60	80 → 49295 [ACK] Seq=1 Ack=240 Win=61952 Len=0
40225	315.497872	172.217.160.206	192.168.1.4	HTTP	608	HTTP/1.1 302 Found
40228	315.512340	192.168.1.4	27.106.94.17	TCP	66	49296 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
40231	315.693760	192.168.1.4	172.217.160.206	TCP	54	49295 → 80 [ACK] Seq=240 Ack=555 Win=65684 Len=0
40237	315.823271	27.106.94.17	192.168.1.4	TCP	66	80 → 49296 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1452 SACK_PERM=1 WS=256
40238	315.823365	192.168.1.4	27.106.94.17	TCP	54	49296 → 80 [ACK] Seq=1 Ack=1 Win=66792 Len=0
40239	315.823558	192.168.1.4	27.106.94.17	HTTP	404	HEAD /edgedl/release2/chrome_component/H07sha1Vdw_4916/4916_all_crl-set-13576662708261436161.data.cr
40241	315.834863	27.106.94.17	192.168.1.4	HTTP	455	HTTP/1.1 200 OK
40244	315.906000	192.168.1.4	27.106.94.17	TCP	54	49296 → 80 [ACK] Seq=251 Ack=102 Win=66288 Len=0

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.

The screenshot shows a Wireshark interface with a list of network packets on the left and a detailed view of a selected packet on the right. A context menu is open over the selected packet (No. 36), specifically over the 'Host' header. The menu has several options, with 'Apply as Column' being the one highlighted by a red box. Another red box highlights the 'Host' header value in the packet details pane.

No.	Time	Source	Dest
10601	0.009562000	192.168.1.1	192.168.1.71
10602	0.000000000	192.168.1.71	192.168.1.1
10603	0.000001000	192.168.1.71	192.168.1.1
10651	0.012548000	192.168.1.254	192.168.1.1
10686	0.002241000	192.168.1.254	192.168.1.1
10721	0.000001000	192.168.1.254	192.168.1.1
8	0.169230000	192.168.1.71	54.208.231.43
9	0.097531000	54.208.231.43	192.168.1.71
10	0.000790000	54.208.231.43	192.168.1.71
11	0.000075000	192.168.1.71	54.208.231.43
30	10.463897000	54.208.231.43	192.168.1.71
31	0.000001000	54.208.231.43	192.168.1.71
32	0.000162000	192.168.1.71	54.208.231.43
33	0.000102000	192.168.1.71	54.208.231.43
34	0.000055000	192.168.1.71	54.208.231.43
35	0.096702000	54.208.231.43	192.168.1.71
36	0.000001000	54.208.231.43	192.168.1.71
12	11.344881000	192.168.1.71	54.208.231.43

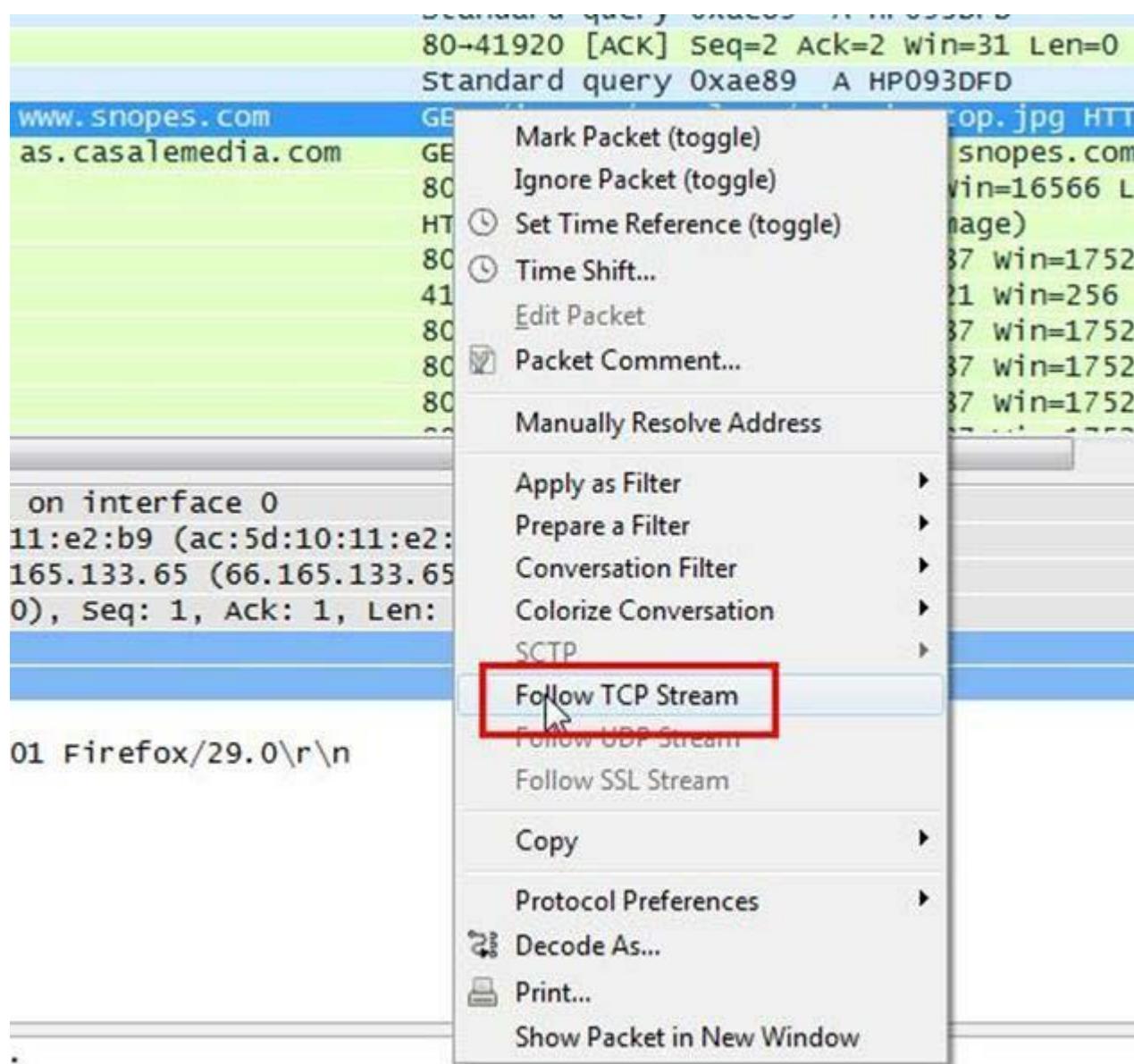
Protocol Tree:

- Transmission Control Protocol, Src Port: 54254 (54.208.231.43), Dst Port: 80 (192.168.1.71)
- Hypertext Transfer Protocol
 - GET /v3.1/collection/14212091/135
 - Accept: */*\r\n
 - Referer: http://www.sfweekly.com/
 - Accept-Language: en-US,en;q=0.5\r\n
 - Origin: http://www.sfweekly.com\r\n
 - Accept-Encoding: gzip, deflate\r\n
 - User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.138 Safari/537.36
 - Host: ct1.ds...livefyre.com\r\n
 - DNT: 1\r\n
 - Connection: Keep-Alive\r\n

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

```
Stream Content
GET /images/template/site-bg-top.jpg HTTP/1.1
Host: www.snopes.com
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:29.0) Gecko/2
Accept: image/png,image/*;q=0.8,*/*;q=0.5
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.snopes.com/style.css
Cookie: ASPSESSIONIDQQDDSBBA=OJMBNHECFANCANKIJJGBBMBLDO
Connection: keep-alive

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

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

2.

About what cell phone problem is the client concerned?

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

Filter: frame matches "(?)cell"

No.	Time	Source	Destination	Protocol	Length	Host
20	0.018898000	192.168.1.71	207.109.230.161	HTTP	1037	as.casalemedia.com
70	0.000001000	207.109.230.161	192.168.1.71	TCP	408	
94	0.039888000	192.168.1.71	74.125.196.139	HTTP	1192	www.google-analytics.com
102	0.017700000	192.168.1.71	50.19.115.152	HTTP	418	stat.komoona.com
106	0.019119000	192.168.1.71	107.20.177.71	HTTP	462	a.komoona.com
126	0.330874000	192.168.1.71	50.19.115.152	HTTP	540	stat.komoona.com
128	0.050275000	192.168.1.71	64.12.239.201	HTTP	510	adserver.adtechus.com
152	0.109725000	192.168.1.71	176.32.99.164	HTTP	436	s.komoona.com
156	0.039271000	192.168.1.71	54.85.82.173	HTTP	439	x.bidswitch.net
157	0.020117000	192.168.1.71	74.209.219.38	HTTP	500	aol-match.dotomi.com
176	0.429894000	192.168.1.71	23.210.219.85	HTTP	989	ads.rubiconproject.com
194	0.014825000	192.168.1.71	54.84.236.238	HTTP	508	pool.adizio.com
200	0.188424000	192.168.1.71	69.25.24.23	HTTP	1091	optimized-by.rubiconproject.com
229	0.337378000	192.168.1.71	23.210.231.153	HTTP	1514	ads.pubmatic.com
259	0.000134000	192.168.1.71	54.241.183.234	HTTP	528	x.skimresources.com
268	0.590522000	192.168.1.71	162.248.19.142	HTTP	1514	showads.pubmatic.com
269	0.000010000	192.168.1.71	162.248.19.142	TCP	1514	
510	0.000165000	192.168.1.71	66.165.122.65	HTTP	907	www.snopes.com

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

Filter: frame matches "(?)cell"

Time	Source	Destination	Protocol	Length	Info
20 0.018898000	192.168.1.71	207.109.230.161	HTTP	1037	/s?s=81847&u=http%3A//www.snopes.com/horrors/techno/cellcharge.asp&f=1&id=4240355892,946
70 0.000001000	207.109.230.161	192.168.1.71	TCP	408	80-[ACK] Seq=7318 Ack=984 Win=16566 Len=354
94 0.039888000	192.168.1.71	74.125.196.139	HTTP	1192	GET /_utm.gif?utmw=5.5.1&utms=1&utmhn=www.snopes.com&utmcn=windows-1252&utm
102 0.017700000	192.168.1.71	50.19.115.152	HTTP	418	GET /s?tagId=cad674dbf73589c9a110884ce3bb72_728_90&w=2.16&cb=516430883&t=2 HTTP/1.1
106 0.019119000	192.168.1.71	107.20.177.71	HTTP	462	GET /tag/cad674dbf73589c9a110884ce3bb72_728_90.jstl=http%3A%2F%2Fwww.snopes.com%2Fhorrors%
126 0.330874000	192.168.1.71	50.19.115.152	HTTP	540	GET /s?tagId=cad674dbf73589c9a110884ce3bb72v=2.16&cb=516430883&t=-1&p=Cad674dbf73589c9a1
128 0.050275000	192.168.1.71	64.12.239.201	HTTP	510	GET /addyn/3.0/9423.1/3142865/0/225/ADTECH;loc=100;target=_blank;misc=%5BTIMESTAMP%50;rdclci
152 0.109725000	192.168.1.71	176.32.99.164	HTTP	436	GET /passback/np/cad674dbf73589c9a110884ce3bb72.js HTTP/1.1
156 0.039271000	192.168.1.71	54.85.82.173	HTTP	439	GET /sync?ssp=aol HTTP/1.1
157 0.020117000	192.168.1.71	74.209.219.38	HTTP	500	GET /aol/match?cb=https://ums.adtechus.com/mapuser?providerId=1013;userId=\$UID HTTP/1.1
176 0.429894000	192.168.1.71	23.210.219.85	HTTP	989	GET /ad/9192.js HTTP/1.1
194 0.014825000	192.168.1.71	54.84.236.238	HTTP	508	GET /sync?ssp=bidswitch&bidswitch_ssp_id=aol HTTP/1.1
200 0.188424000	192.168.1.71	69.25.24.23	HTTP	1091	GET /a/9192/19861/64229-2.js?&cb=0.18771559557158202&tk_st=1&r_p_s=c&p_exp=1&p_pos=atf&p_scre
229 0.337378000	192.168.1.71	23.210.231.153	HTTP	1514	GET /Adserver/js/showad.js?rn=516430883 HTTP/1.1
259 0.000134000	192.168.1.71	54.241.183.234	HTTP	528	GET /?provider=adizio&mode=check&uid=1039da81-f78e-44cc-a317-d4139ca80c0c HTTP/1.1
268 0.590522000	192.168.1.71	162.248.19.142	HTTP	1514	GET /Adserver/AdvertiserServlet?pubId=32702&siteId=46838&adId=80732&kadwidth=728&kadheight=90&
269 0.000010000	192.168.1.71	162.248.19.142	TCP	1514	41950-80-[ACK] Seq=1461 Ack=1 Win=16445440 Len=1460
510 0.000165000	192.168.1.71	66.165.122.65	HTTP	907	GET https://techno.cellcharge.com HTTP/1.1

3.

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

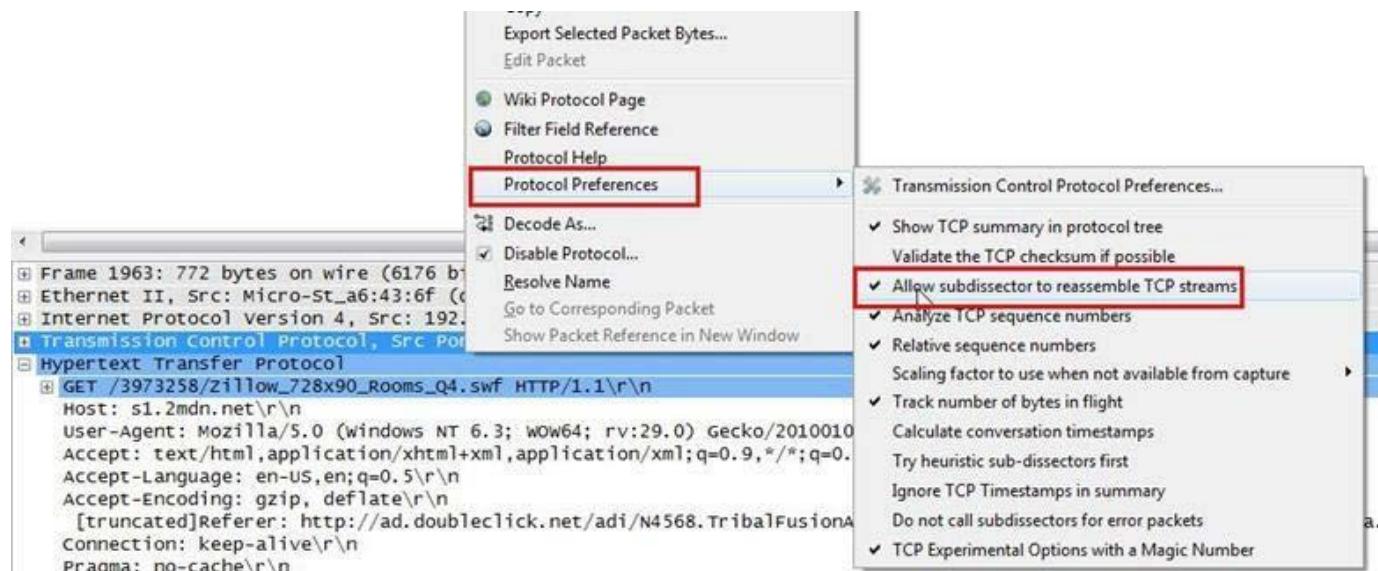
Analysis – As we did in the last challenge, we will apply a regular express filter for the Zillow keyword. Apply frame matched “(?) zillow” or frame matches zillow

Filter: frame matches "(?i)zillow"							▼	Expression...	Clear	Apply	Save
No.	Time	Source	Destination	Protocol	Length	Info					
94	0.039888000	192.168.1.71	74.125.196.139	HTTP	1192	GET /__utm.gif					
95	0.004442000	199.189.107.4	192.168.1.71	TCP	60	80->41929 [ACK]					
96	0.000769000	199.189.107.4	192.168.1.71	TCP	60	[TCP Dup ACK 9]					
97	0.060923000	199.189.107.4	192.168.1.71	TCP	60	80->41930 [FIN,					
98	0.000136000	192.168.1.71	199.189.107.4	TCP	54	41930->80 [ACK]					
99	0.000052000	192.168.1.71	199.189.107.4	TCP	54	41930->80 [FIN,					
100	0.015401000	74.125.196.139	192.168.1.71	TCP	60	80->41931 [ACK]					
101	0.000796000	74.125.196.139	192.168.1.71	HTTP	458	HTTP/1.1 200 OK					
102	0.017700000	192.168.1.71	50.19.115.152	HTTP	418	GET /s?tagid=c					
103	0.011551000	192.168.1.71	74.125.196.139	TCP	54	41931->80 [ACK]					
104	0.029132000	199.189.107.4	192.168.1.71	TCP	60	80->41930 [ACK]					
105	0.000000000	199.189.107.4	192.168.1.71	TCP	60	[TCP Dup ACK 10]					
106	0.019119000	192.168.1.71	107.20.177.71	HTTP	462	GET /tag/cad674					
107	0.034965000	50.19.115.152	192.168.1.71	TCP	60	80->41934 [ACK]					
108	0.001555000	50.19.115.152	192.168.1.71	HTTP	338	HTTP/1.1 200 OK					
109	0.023341000	192.168.1.71	199.189.107.4	TCP	54	[TCP Retransmission]					
110	0.016019000	192.168.1.71	50.19.115.152	TCP	54	41934->80 [ACK]					
111	0.010772000	107.20.177.71	107.168.1.71	TCP	60	80->41935 [ACK]					

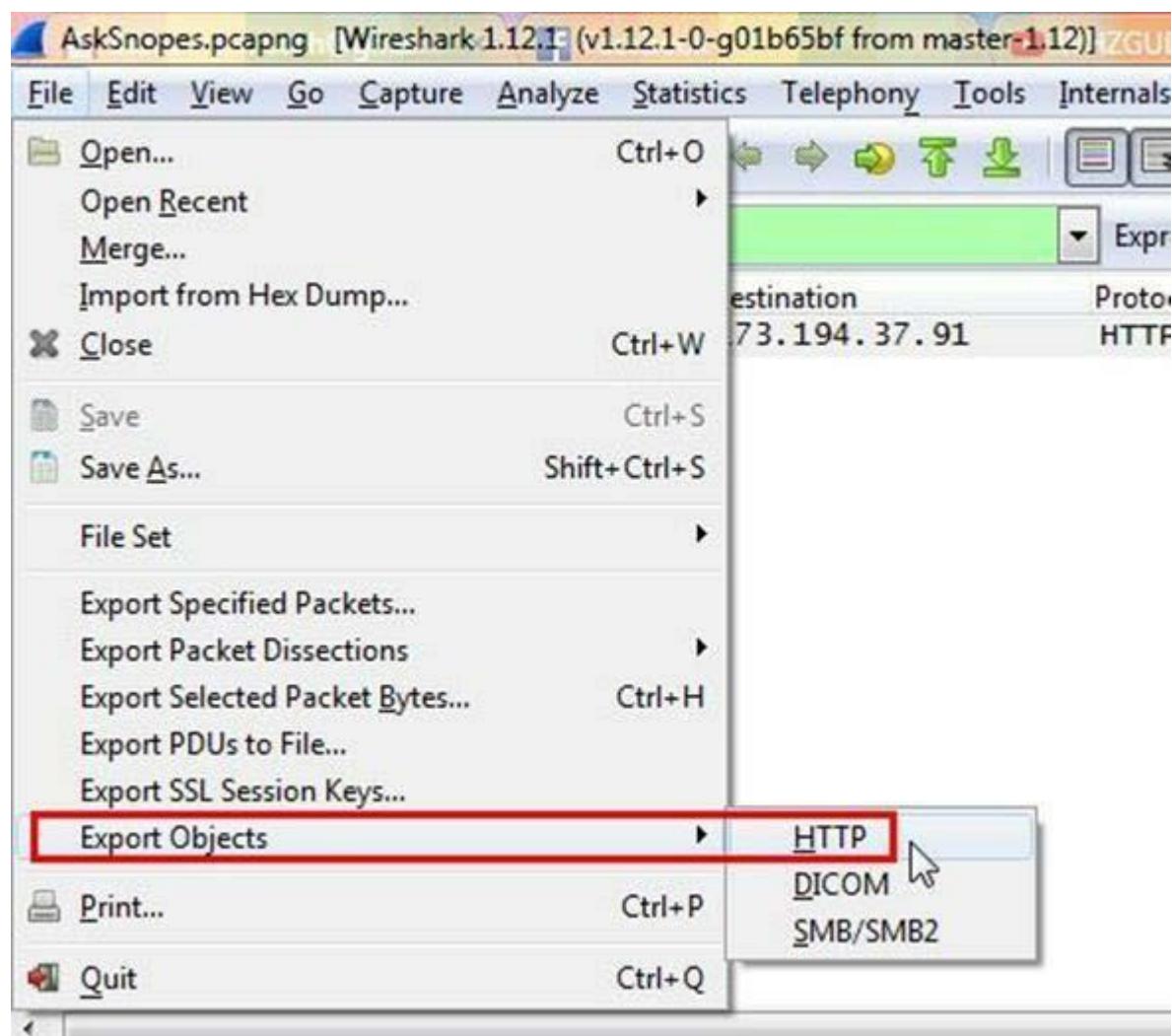
After applying the filter, we found only one packet with the Zillow keyword

Filter: frame matches "(?i)zillow"							▼	Expression...	Clear	Apply	Save
No.	Time	Source	Destination	Protocol	Length	Info					
1963	0.604769000	192.168.1.71	173.194.37.91	HTTP	772	GET /3973258/zillow_728x90_Rooms_Q4.swf	HTTP/1.1				

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=624
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	Igrt?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

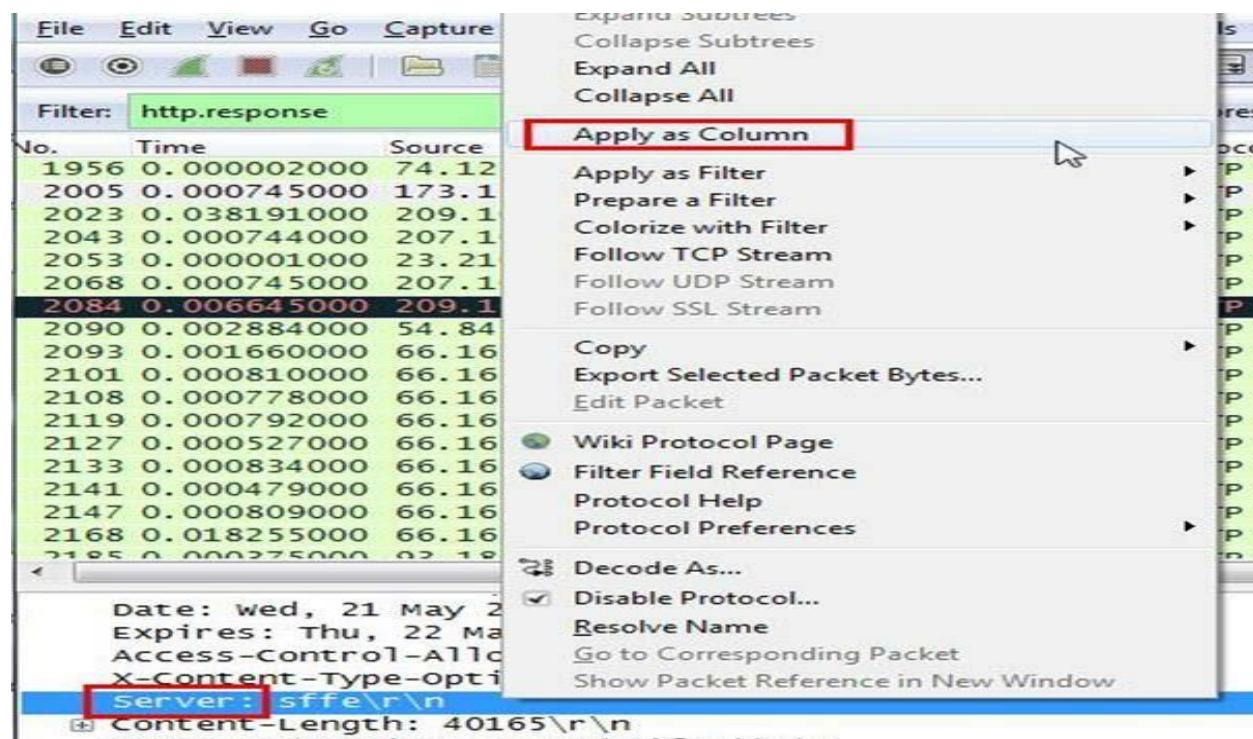
Cancel

How many web servers are running Apache?

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

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

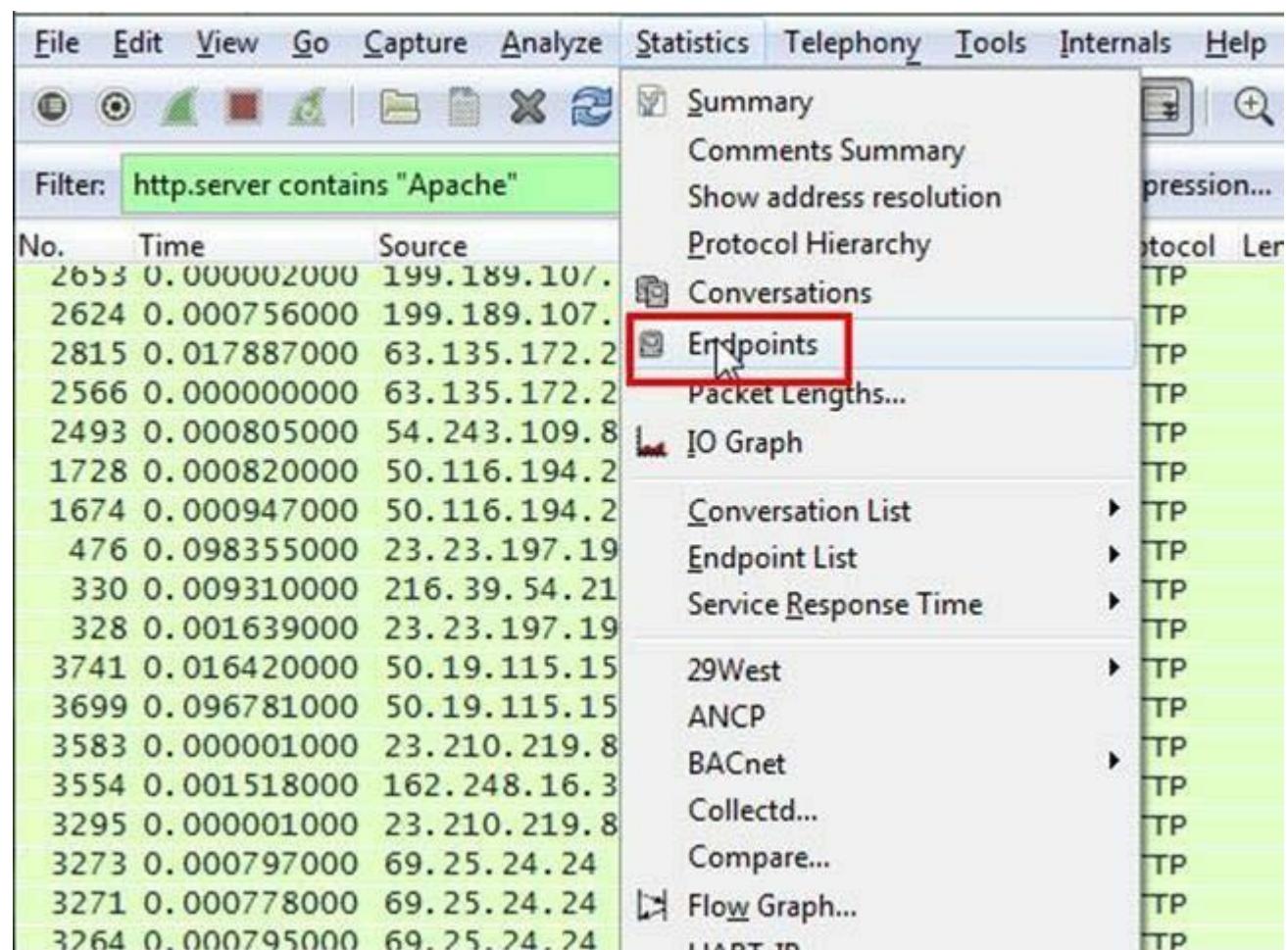
Now we will set the server header as column select any packet and right click on it then select Apply as Column.



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

Filter: http.server contains "Apache"							Expression...	Clear	Apply	Save
No.	Time	Source	Destination	Protocol	Length	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 connections

Ethernet: 7	Fibre Channel	FDDI	IPv4: 107	IPv6: 4	IPX	JXTA	NCP	RSVP	SCTP	TCP: 361	Token
IPv4 Endpoints											
Address	◀ Packets	◀ Bytes	◀ Tx Packets	◀ Tx Bytes	◀ Rx Packets	◀ Rx Bytes	◀ Latitude	◀ Loc	◀	◀	◀
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	-	-	-	-	-

Name resolution Limit to display filter

 Limit the list to endpoints matching the current display filter.

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

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)

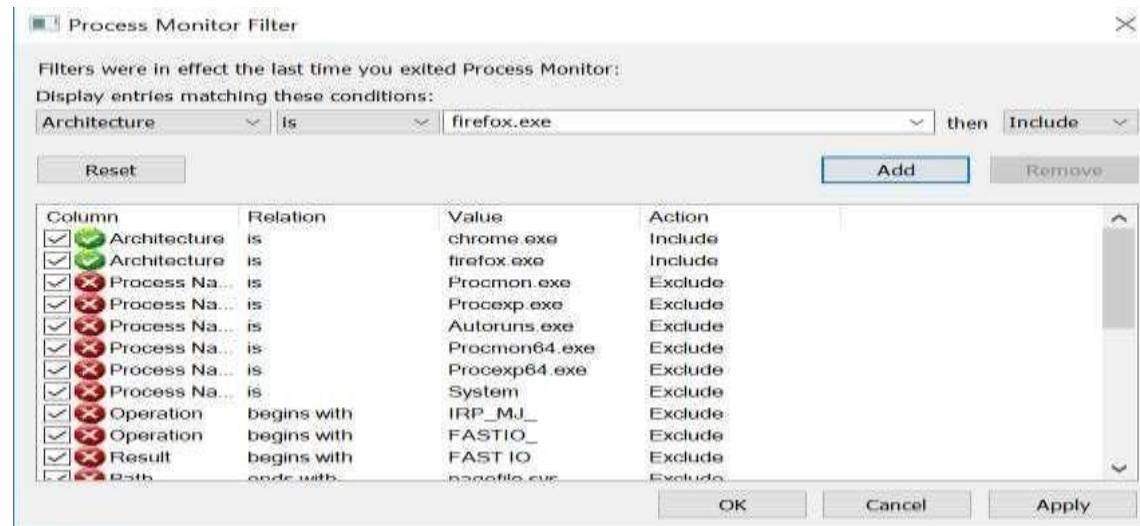


The screenshot shows the Process Monitor interface with the following details:

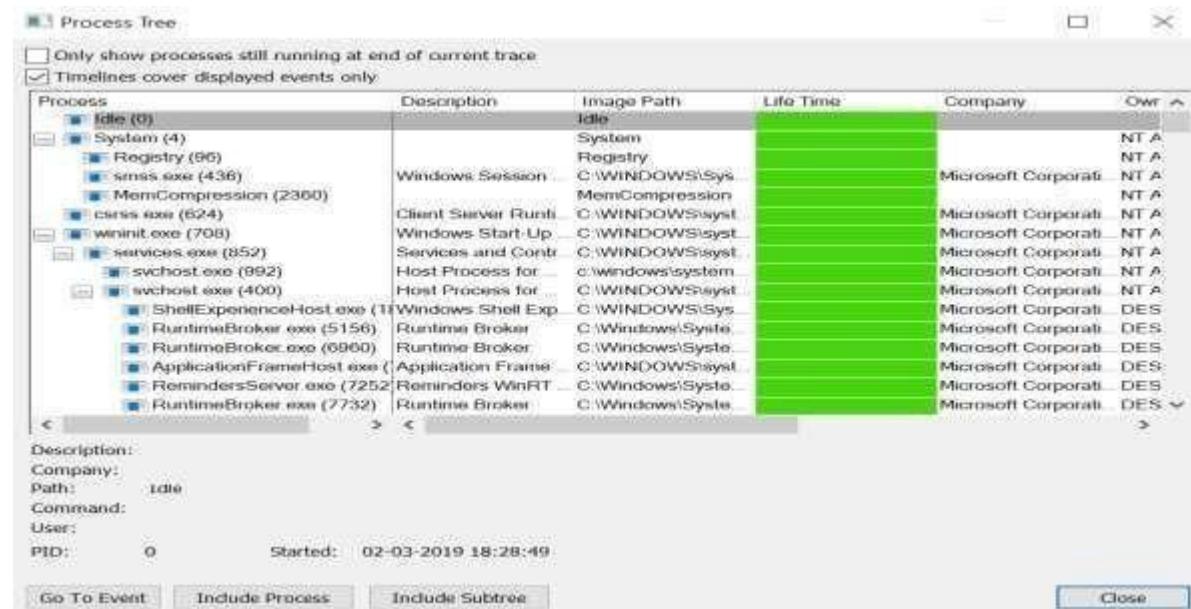
Time	Process Name	PID	Operation	Path
20:33:3...	Procmon64.exe	4120	RegQueryValue	HKLM\System\CurrentControlSet\Cont...
20:33:3...	System	4	Thread Create	
20:33:3...	Procmon64.exe	4120	Thread Create	
20:33:3...	Procmon64.exe	4120	Thread Create	
20:33:3...	Procmon64.exe	4120	Thread Create	
20:33:3...	Procmon64.exe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

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

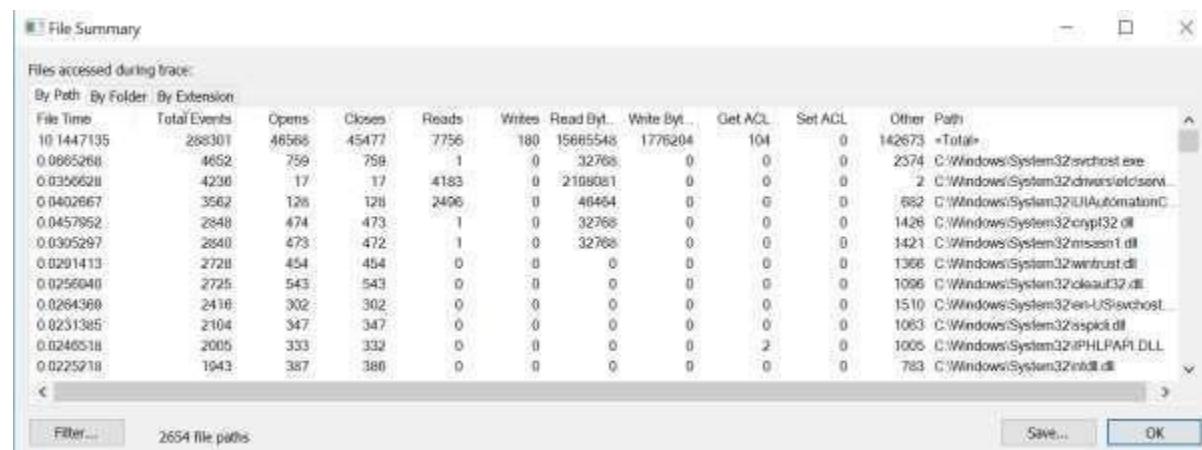
Click on filter > Process monitor filter



Click on tools > Process tree

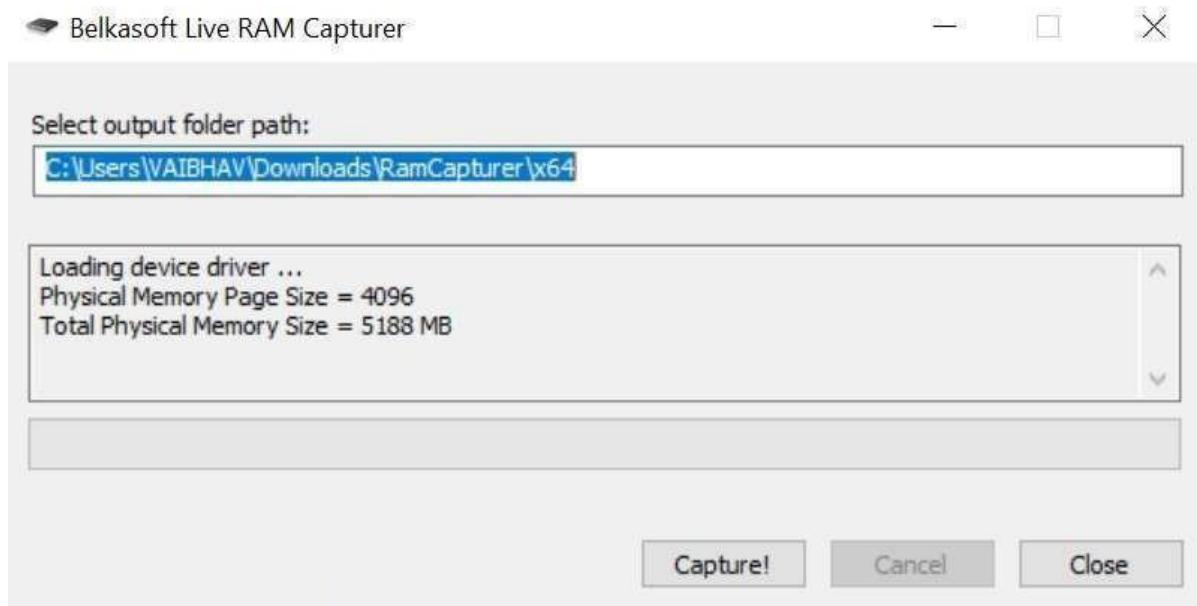


Click on filter > File summary

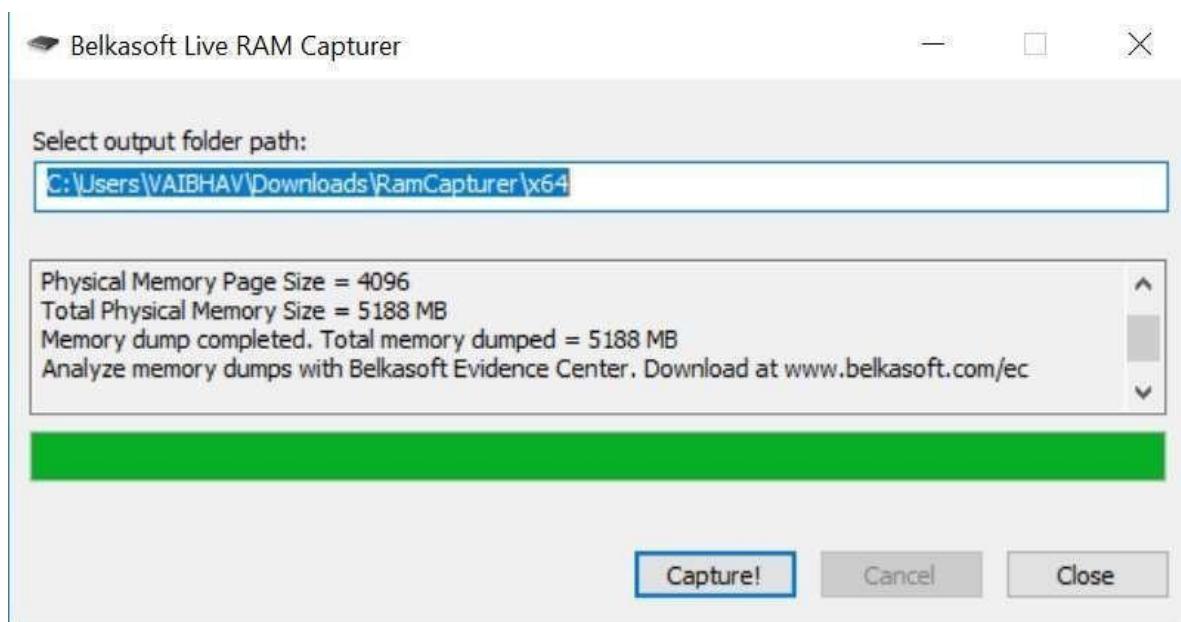


3) Capture RAM (Tool: RAMCapture)

Open the Ramcapture tool.



Click on capture.



4) Capture TCP/UDP packets (Tool:

TcpView) Open the Tcpview tool.

Process	/	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State
[System Proc]	0	0	TCP	desktop-ftq9ln	64289	bom07s11-in-f14...	https	TIME_WAIT
[System Proc]	0	0	TCP	desktop-ftq9ln	64293	155.244.178.107...	https	TIME_WAIT
[System Proc]	0	0	TCP	desktop-ftq9ln	64298	52.109.56.34	https	TIME_WAIT
epmd.exe	11016	11016	TCP	DESKTOP-FTQ9LN	4369	DESKTOP-FTQ9LN	0	LISTENING
epmd.exe	11016	11016	TCP	DESKTOP-FTQ9LN	4369	localhost	51791	ESTABLISHED
epmd.exe	11016	11016	TCPV6	desktop-ftq9ln	4369	desktop-ftq9ln	0	LISTENING
erl.exe	7284	7284	TCP	DESKTOP-FTQ9LN	5984	DESKTOP-FTQ9LN	0	LISTENING
erl.exe	7284	7284	TCP	DESKTOP-FTQ9LN	5986	DESKTOP-FTQ9LN	0	LISTENING
erl.exe	7284	7284	TCP	DESKTOP-FTQ9LN	51790	DESKTOP-FTQ9LN	0	LISTENING
erl.exe	7284	7284	TCP	DESKTOP-FTQ9LN	51791	localhost	4369	ESTABLISHED
firefox.exe	10952	10952	TCP	DESKTOP-FTQ9LN	50023	localhost	50024	ESTABLISHED
firefox.exe	10952	10952	TCP	DESKTOP-FTQ9LN	50024	localhost	50023	ESTABLISHED
firefox.exe	11480	11480	TCP	DESKTOP-FTQ9LN	50030	localhost	50031	ESTABLISHED
firefox.exe	11480	11480	TCP	DESKTOP-FTQ9LN	50031	localhost	50030	ESTABLISHED
firefox.exe	6524	6524	TCP	DESKTOP-FTQ9LN	50035	localhost	50036	ESTABLISHED
firefox.exe	6524	6524	TCP	DESKTOP-FTQ9LN	50036	localhost	50035	ESTABLISHED
firefox.exe	8484	8484	TCP	DESKTOP-FTQ9LN	50045	localhost	50046	ESTABLISHED
firefox.exe	8484	8484	TCP	DESKTOP-FTQ9LN	50046	localhost	50045	ESTABLISHED
firefox.exe	5504	5504	TCP	DESKTOP-FTQ9LN	50207	localhost	50208	ESTABLISHED
firefox.exe	5504	5504	TCP	DESKTOP-FTQ9LN	50208	localhost	50207	ESTABLISHED
firefox.exe	11236	11236	TCP	DESKTOP-FTQ9LN	50321	localhost	50322	ESTABLISHED
firefox.exe	11236	11236	TCP	DESKTOP-FTQ9LN	50322	localhost	50321	ESTABLISHED

Right click on any packet > whois

Process	/	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State
firefox.exe	11480	11480	TCP	DESKTOP-FTQ9LN	50031	localhost	50030	ESTABLISHED
firefox.exe	6524	6524	TCP	DESKTOP-FTQ9LN	50035	localhost	50036	ESTABLISHED
firefox.exe	6524	6524	TCP	DESKTOP-FTQ9LN	50036	localhost	50035	ESTABLISHED
firefox.exe	8484	8484	TCP	DESKTOP-FTQ9LN	50045	localhost	50046	ESTABLISHED
firefox.exe	8484	8484	TCP	DESKTOP-FTQ9LN	50046	localhost	50045	ESTABLISHED
firefox.exe	5504	5504	TCP	DESKTOP-FTQ9LN	50207	localhost	50208	ESTABLISHED
firefox.exe	5504	5504	TCP	DESKTOP-FTQ9LN	50208	localhost	50207	ESTABLISHED
firefox.exe	11236	11236	TCP	DESKTOP-FTQ9LN	50321	localhost	50322	ESTABLISHED
firefox.exe	11236	11236	TCP	DESKTOP-FTQ9LN	50322	localhost	50321	ESTABLISHED
bass.exe	872	872	TCPV6	desktop-ftq9ln	49665	DESKTOP-FTQ9LN	0	LISTENING
node.exe	4420	4420	TCP	desktop-ft	Process Properties...			
node.exe	4420	4420	TCP	desktop-ft	End Process...			
services.exe	852	852	TCP	DESKTOP-				
services.exe	852	852	TCPV6	desktop-ft	Close Connection			
SkypeApp.exe	7608	7608	UDP	DESKTOP-				
SkypeApp.exe	7608	7608	UDPV6	desktop-ft	Whois...	Ctrl+W		
spoolsv.exe	13852	13852	TCP	DESKTOP-				
spoolsv.exe	13852	13852	TCPV6	desktop-ft	Copy	Ctrl+C		
svchost.exe	1054	1054	TCP	DESKTOP-FTQ9LN	49665	DESKTOP-FTQ9LN	0	LISTENING
svchost.exe	7100	7100	TCP	DESKTOP-FTQ9LN	5040	DESKTOP-FTQ9LN	0	LISTENING
svchost.exe	1584	1584	TCP	DESKTOP-FTQ9LN	49666	DESKTOP-FTQ9LN	0	LISTENING



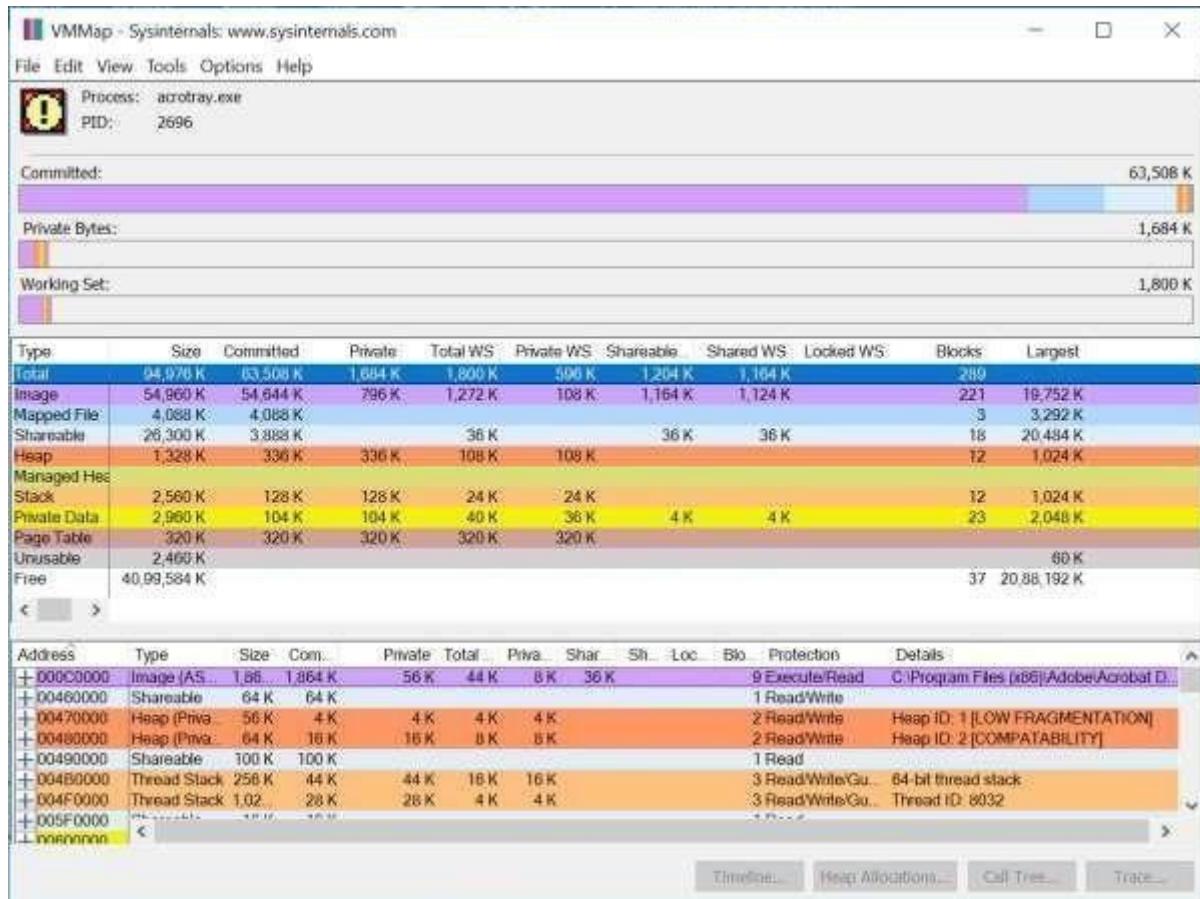
5) Monitor Hard Disk (Tool: DiskMon)

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.

