Practical No – 6

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

-Check Sysinternals tools

-Monitor Live Processes

-Capture RAM-Capture

-TCP/UDP packets

-Monitor Hard Disk

-Monitor Virtual Memory

-Monitor Cache Memory

Steps:

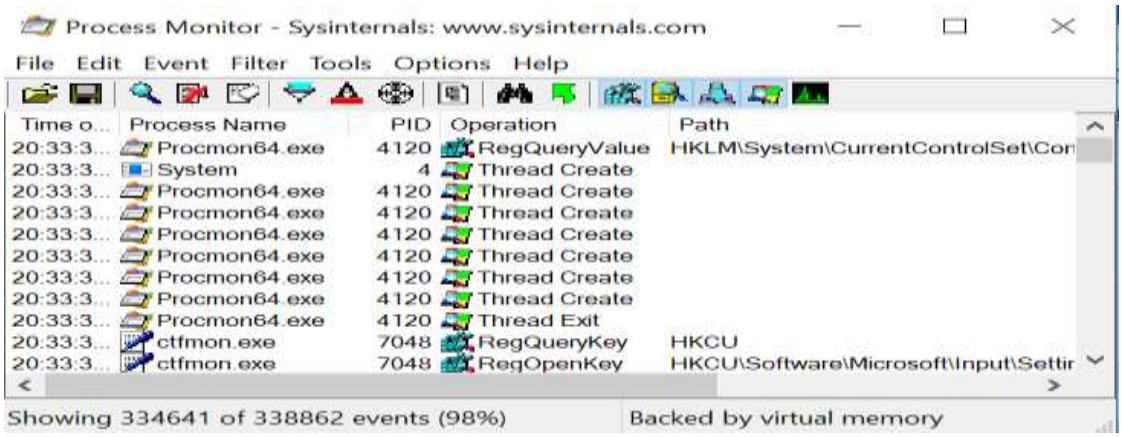
1) Check Sysinternals tools

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

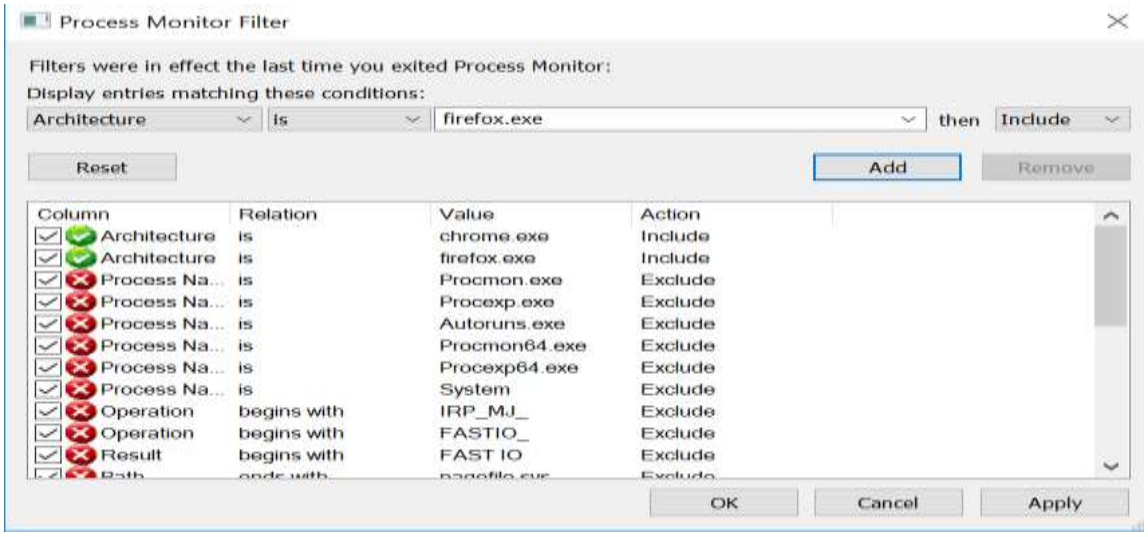
The following are the categories of Sysinternals Tools:

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

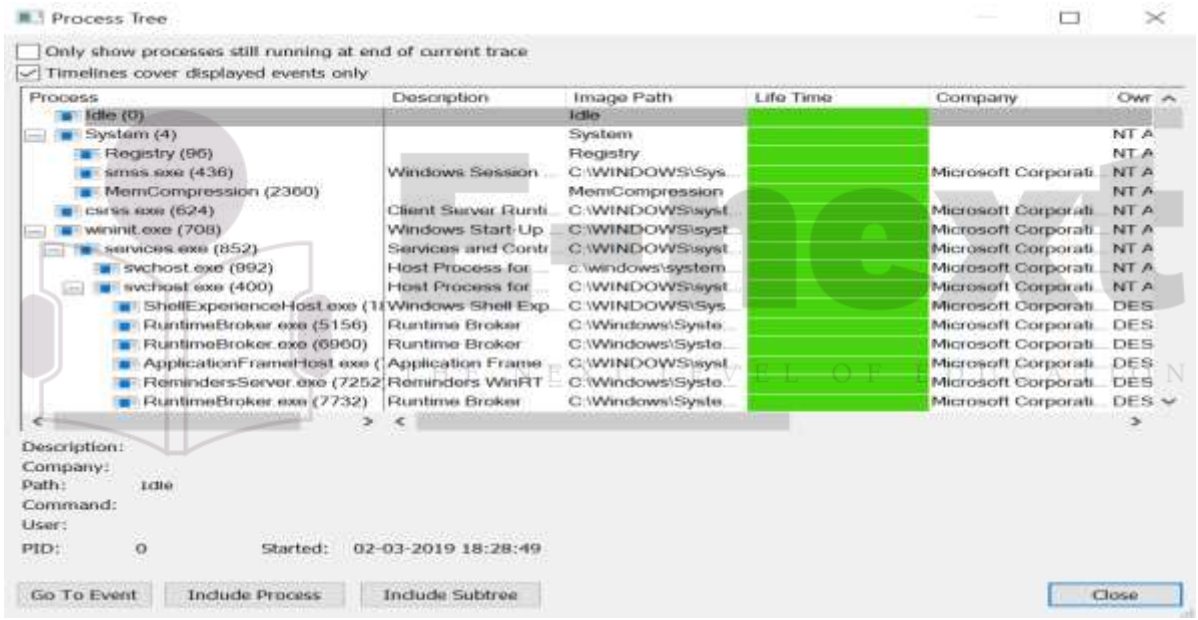
2) Monitor Live Processes (Tool: ProcMon)



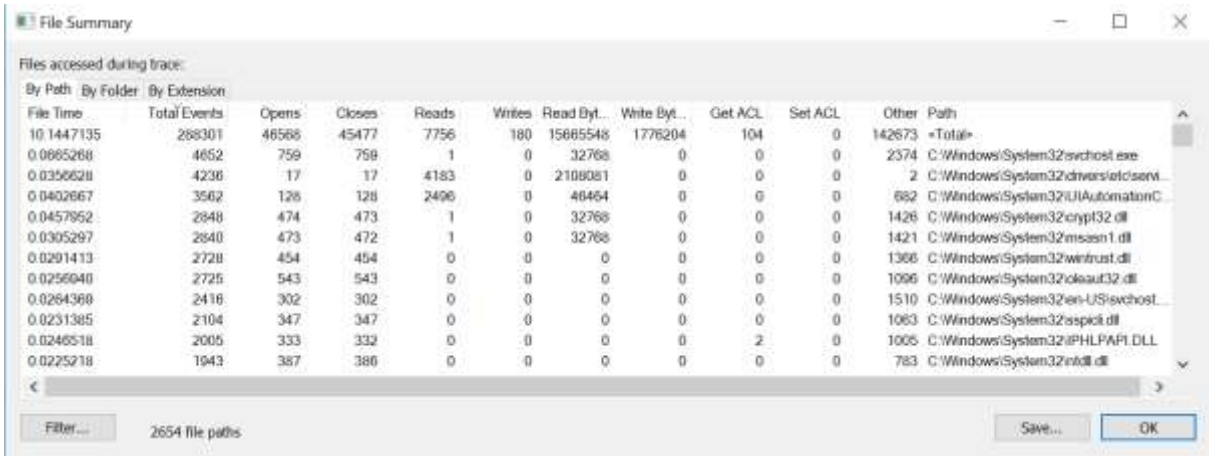
Click on filter > Process monitor filter



Click on tools > Process tree

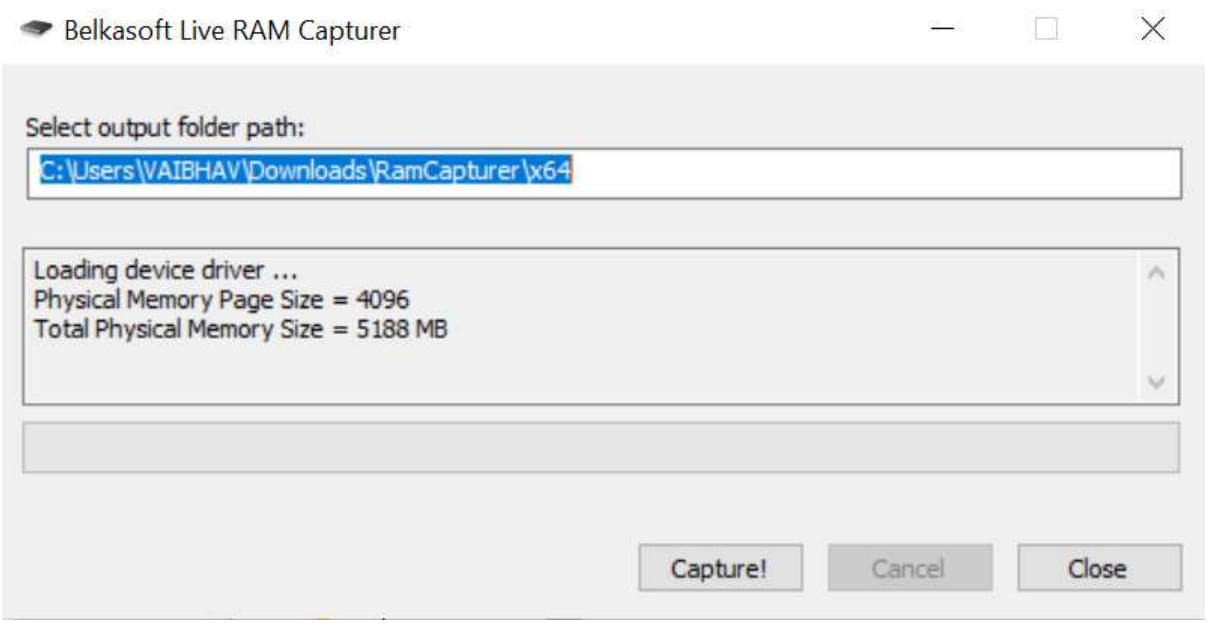


Click on filter > File summary

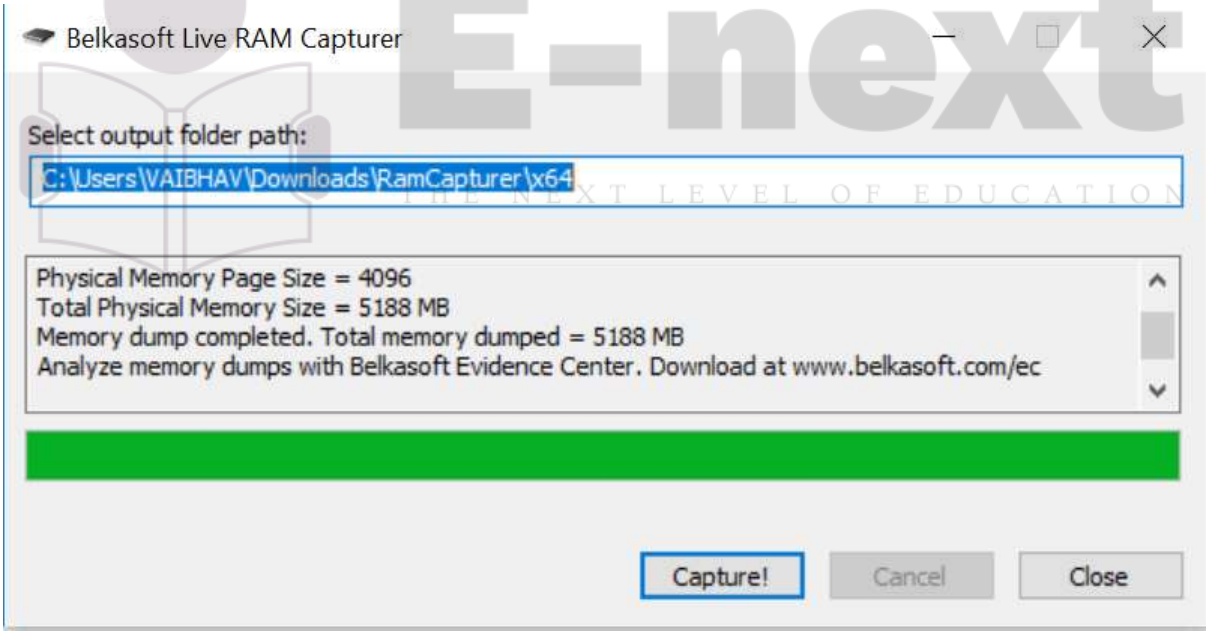


3) Capture RAM (Tool: RAMCapture)

Open the Ramcapture tool.

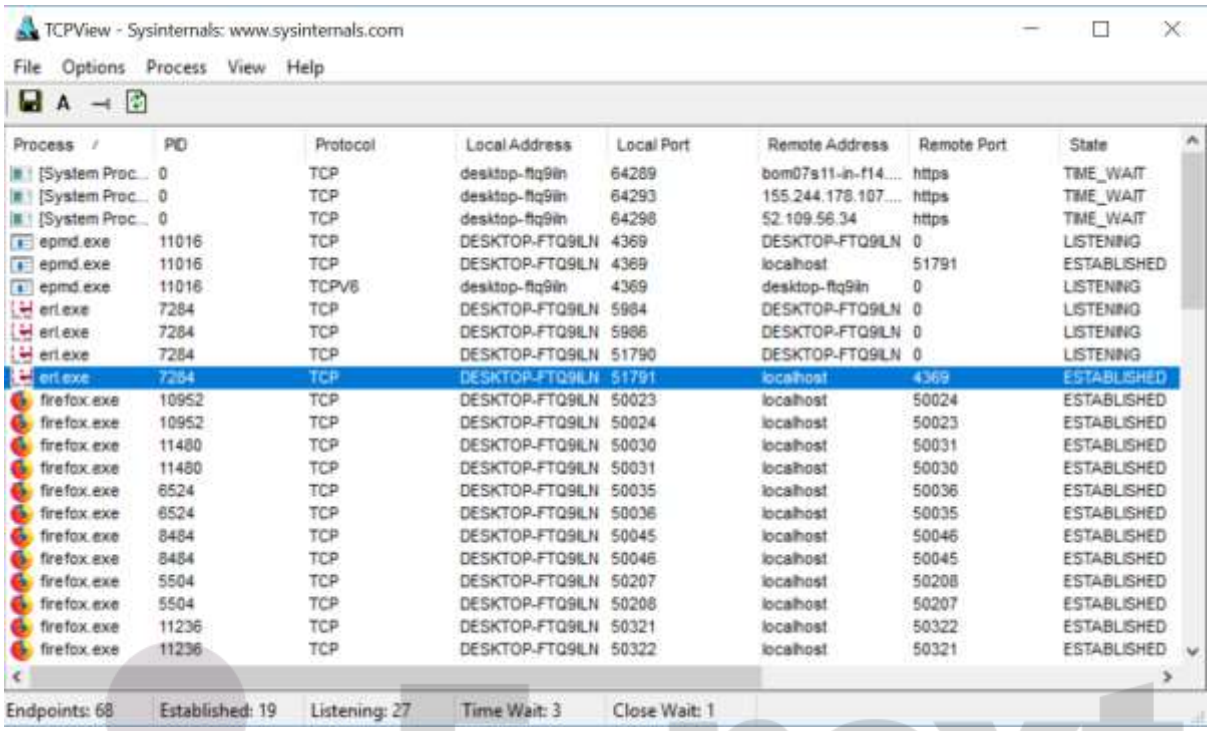


Click on capture.

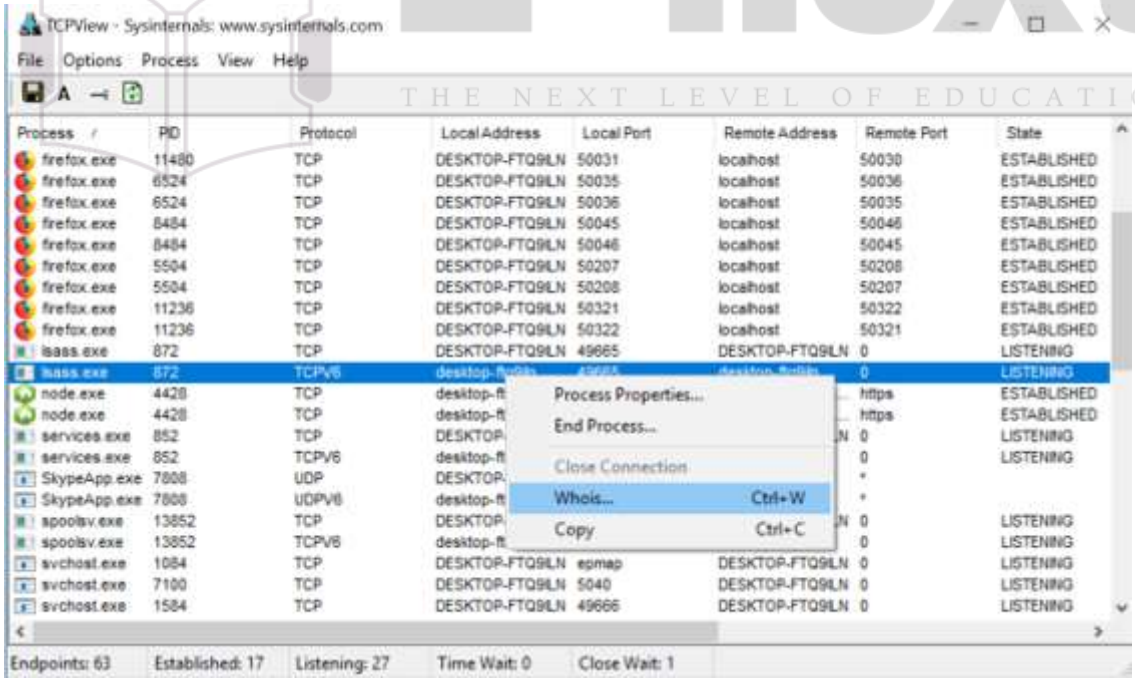


4) Capture TCP/UDP packets (Tool: TcpView)

Open the Tcpview tool.

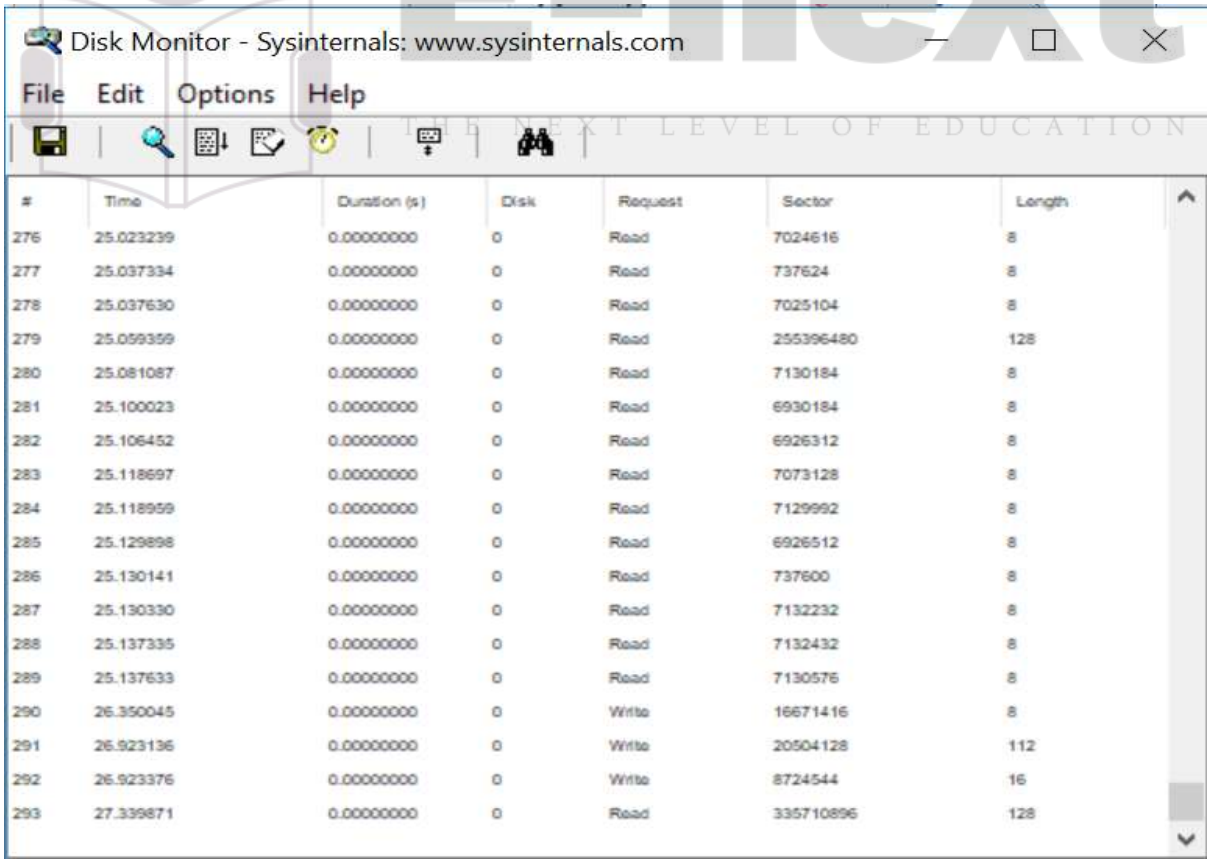


Right click on any packet > whois



5) Monitor Hard Disk (Tool: DiskMon)

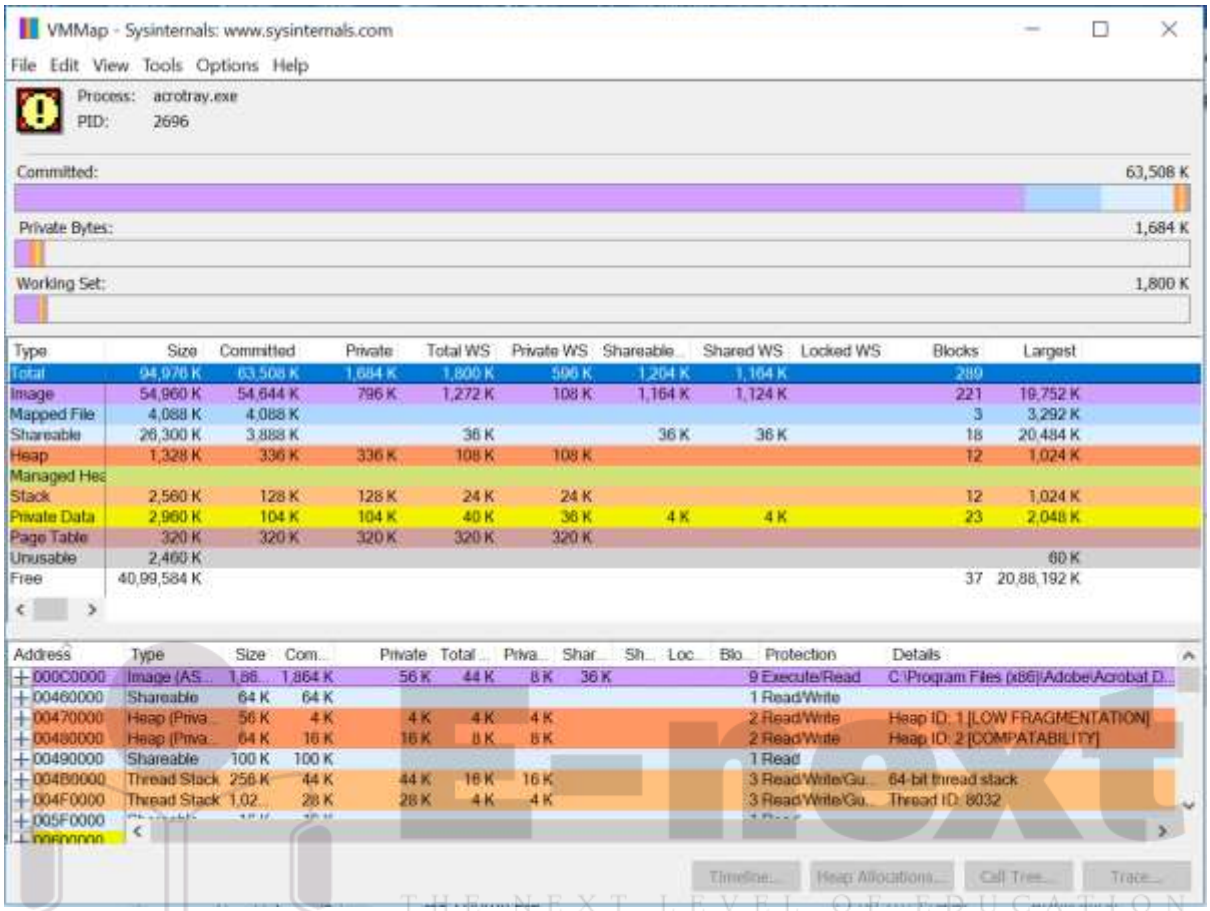
Open the Diskmon tool.



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

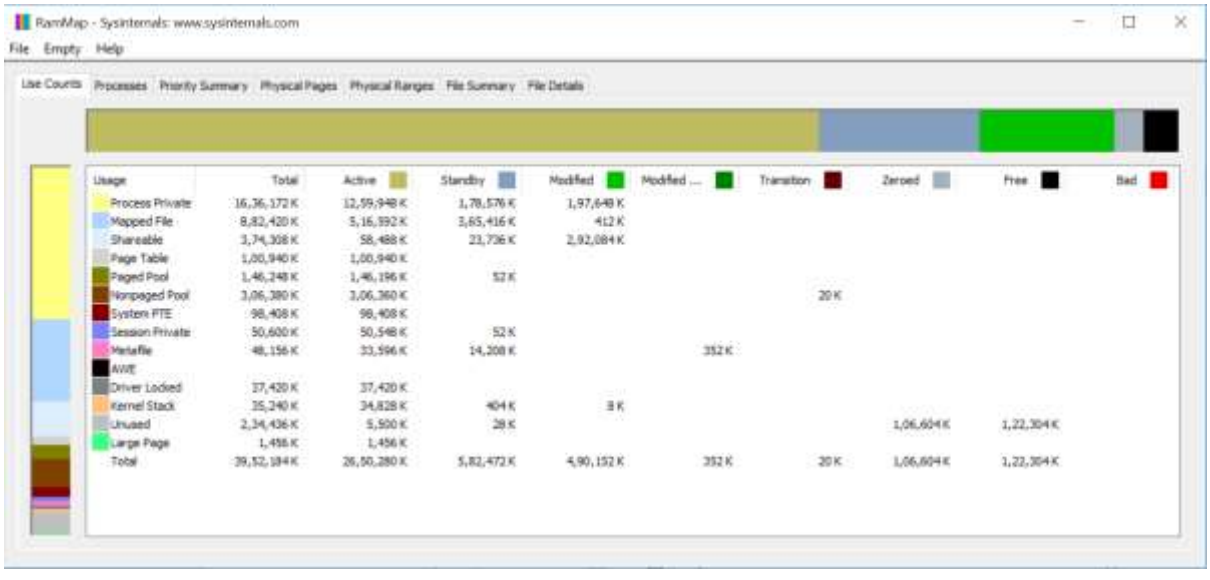
6) Monitor Virtual Memory (Tool: VMMap)

Open the VMMap tool.



7) Monitor Cache Memory (Tool: RAMMap)

Open the RAMMap tool.



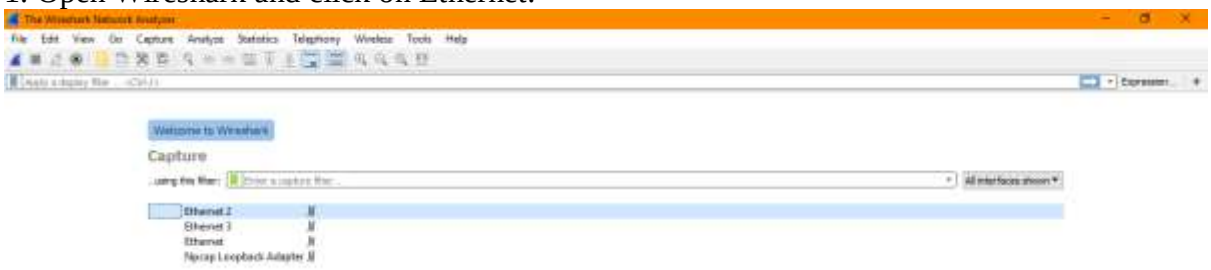
Practical No – 4

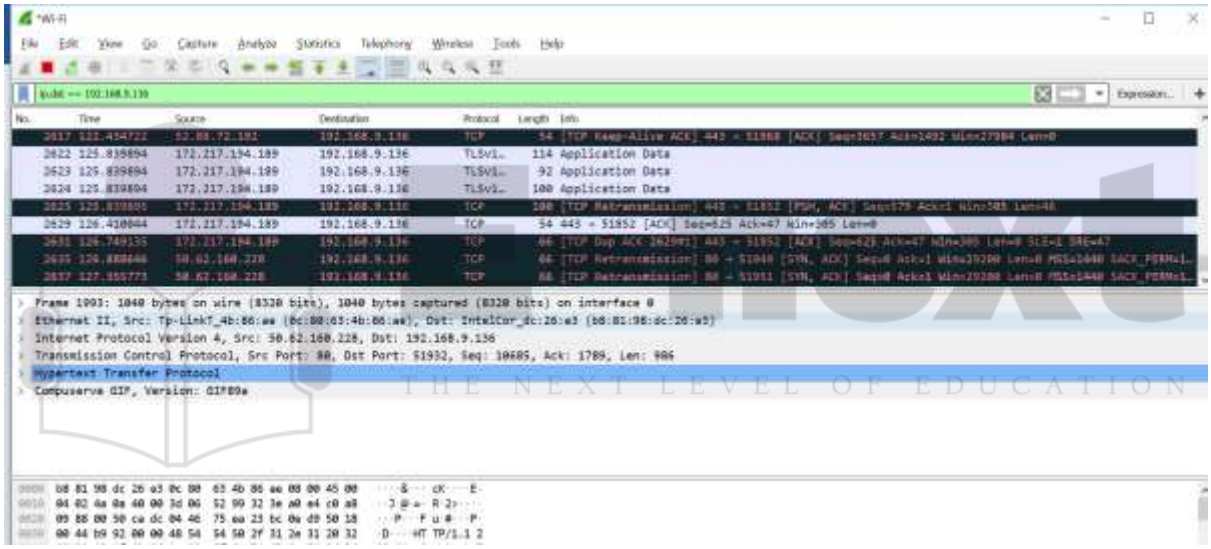
Aim: Capturing and analyzing network packets using Wireshark (Fundamentals):

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

Steps:

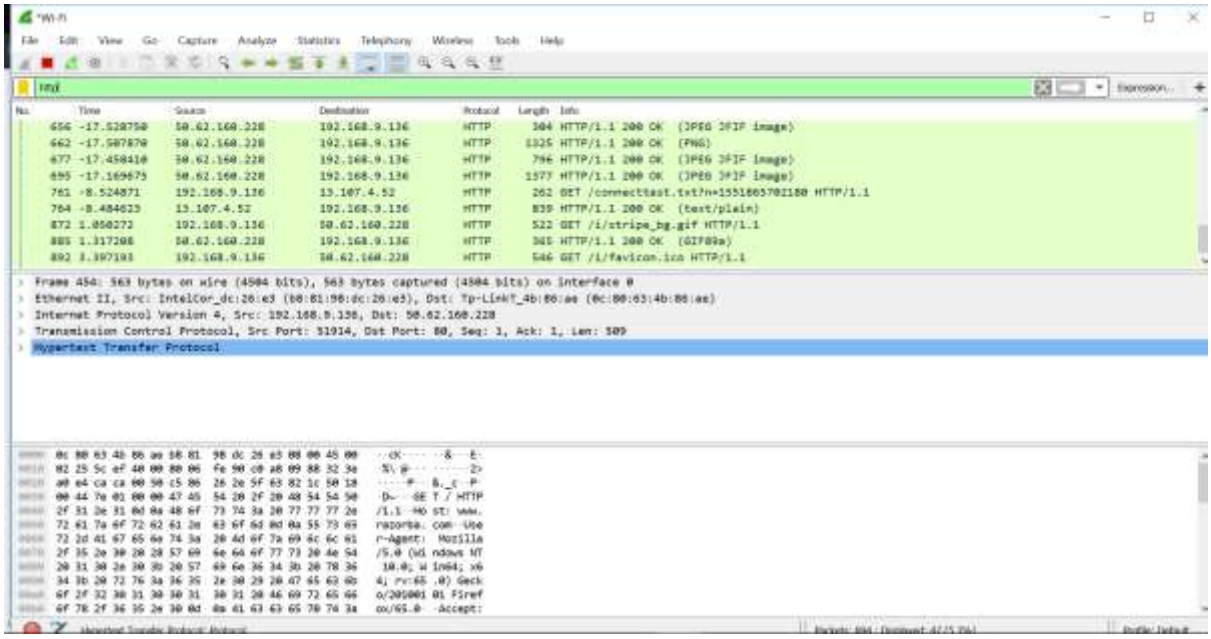
1. Open Wireshark and click on Ethernet.



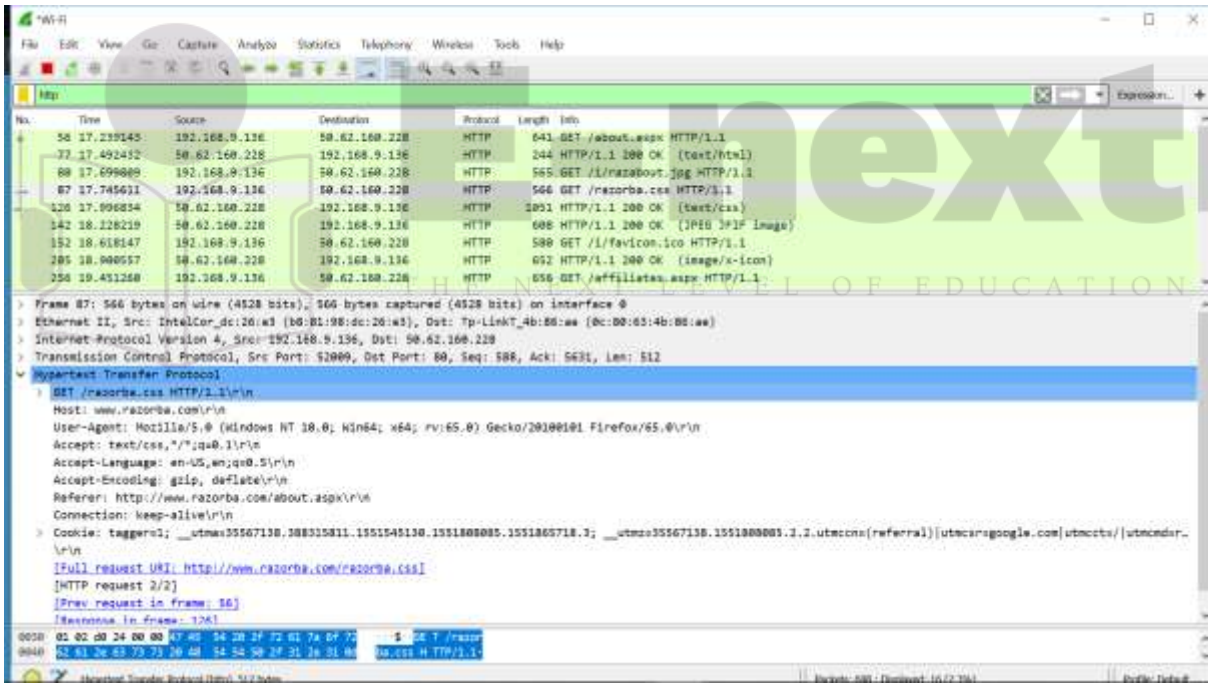


2. Now go on browser and open any unsecured website i.e www.razorba.com and perform some activity on the website.

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



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



Practical No – 3

Aim: Forensics Case Study:

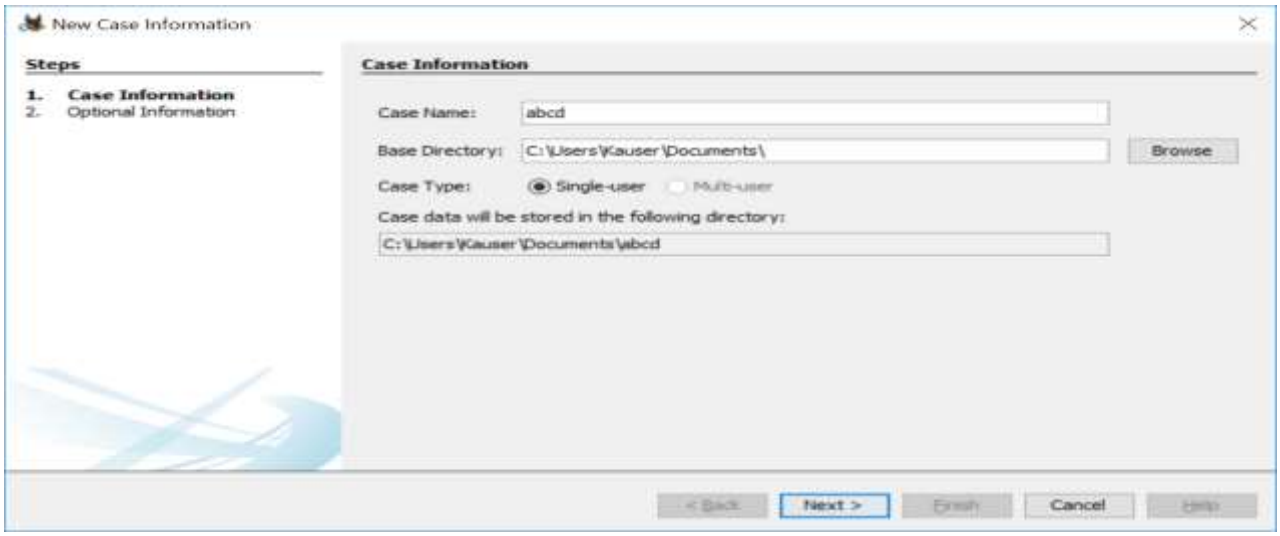
- Solve the Case study (image file) provide in lab using Autopsy

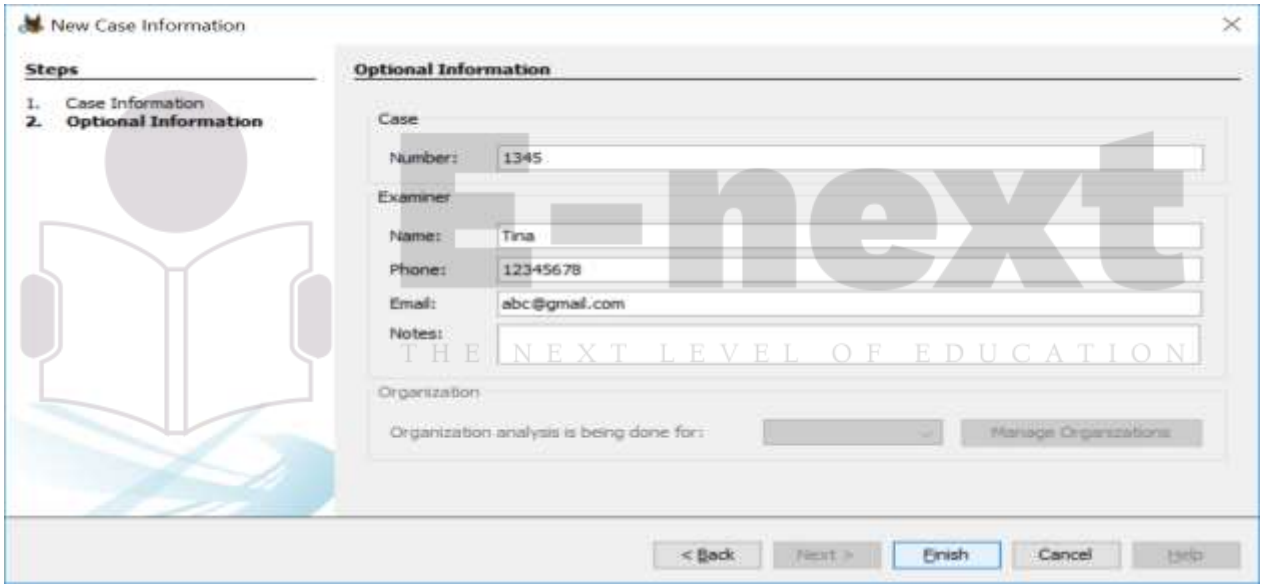
Steps:

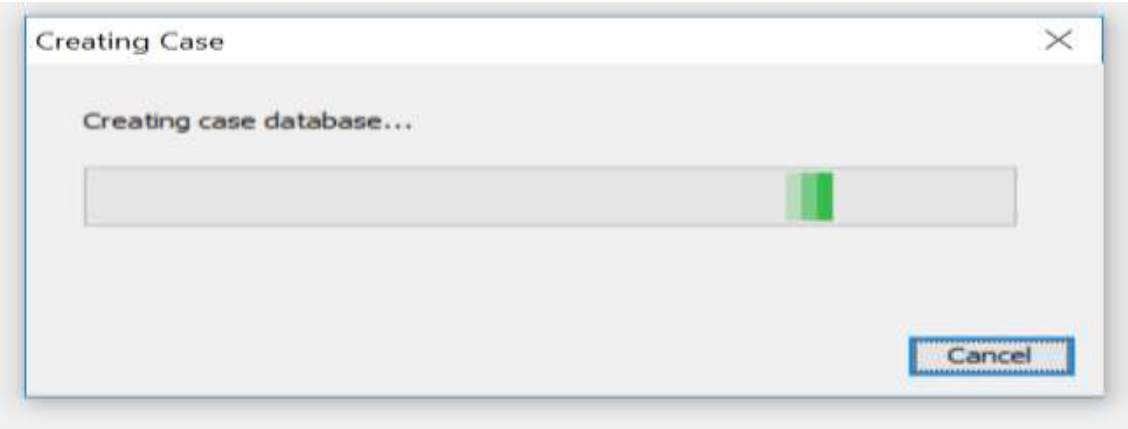
1. Start Autopsy

2. Select New Case

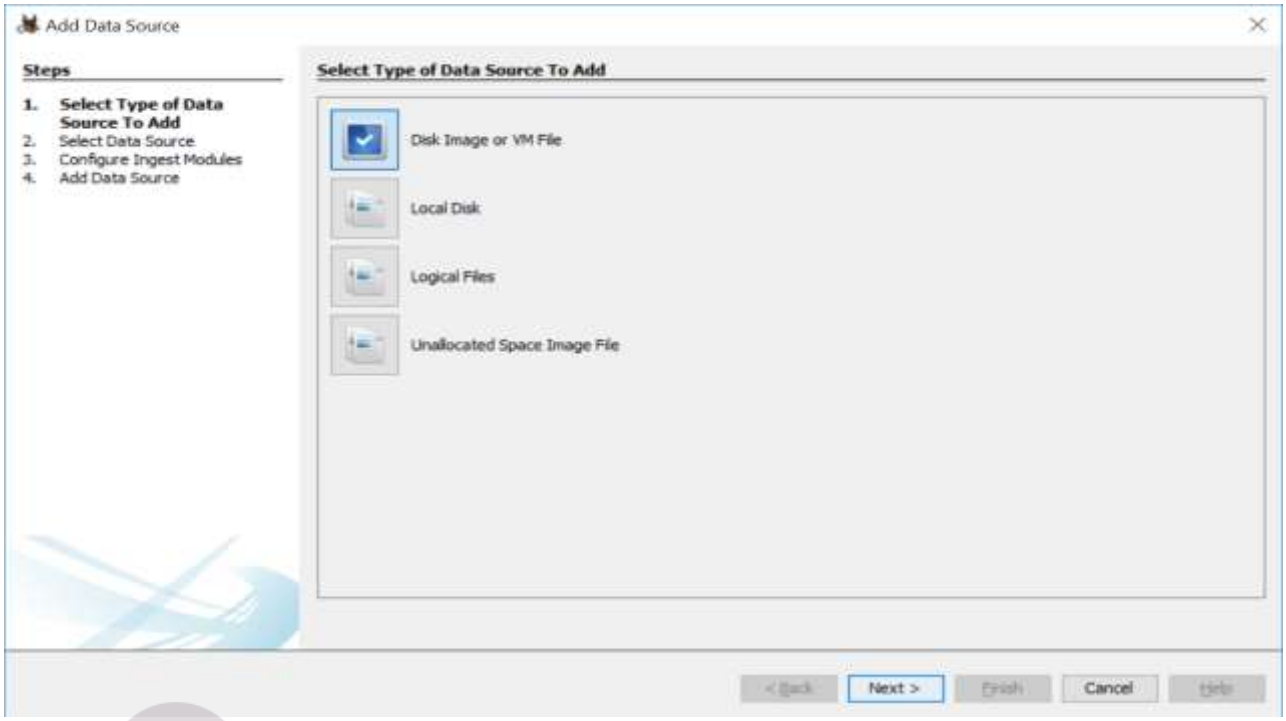
3. Enter Case Information and Base Directory & click on finish





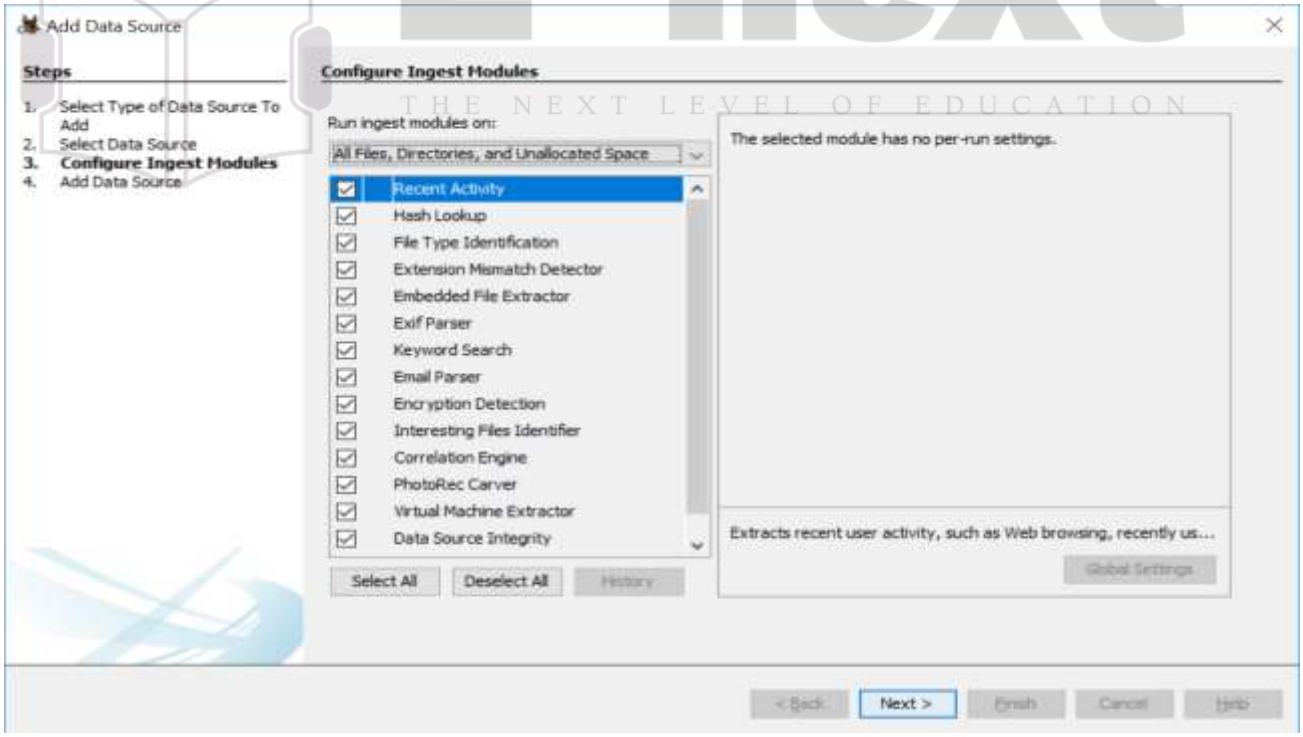


4. Select the type of Data Source that has to be added

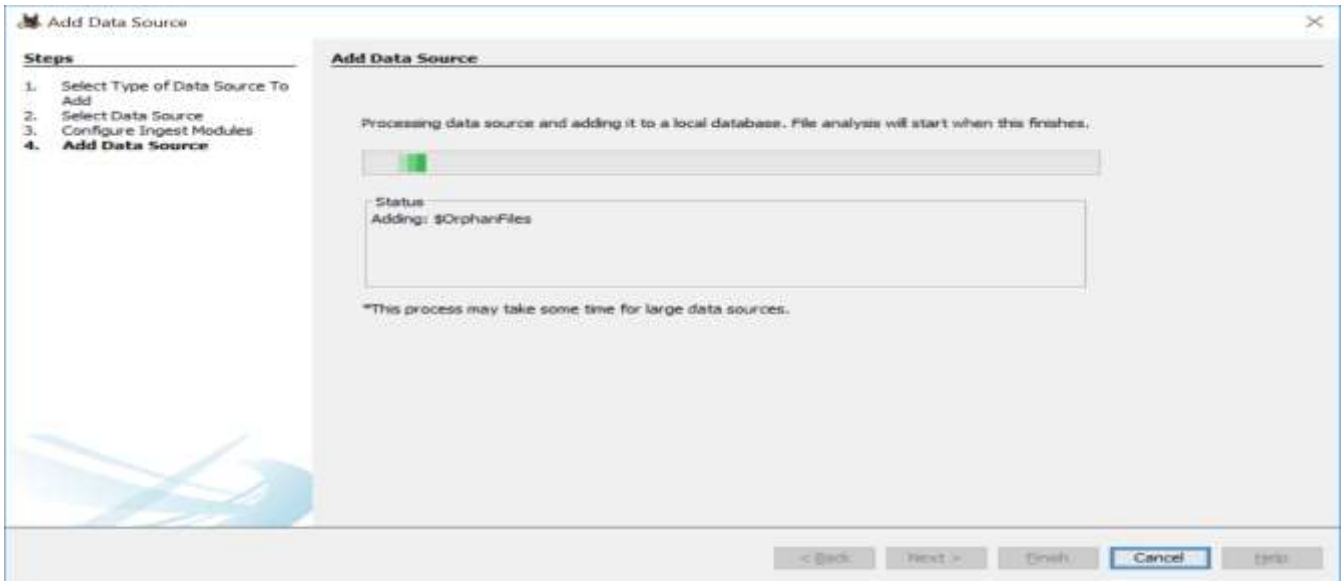


5. Select Data Source(here a previously made image file of a USB is selected)

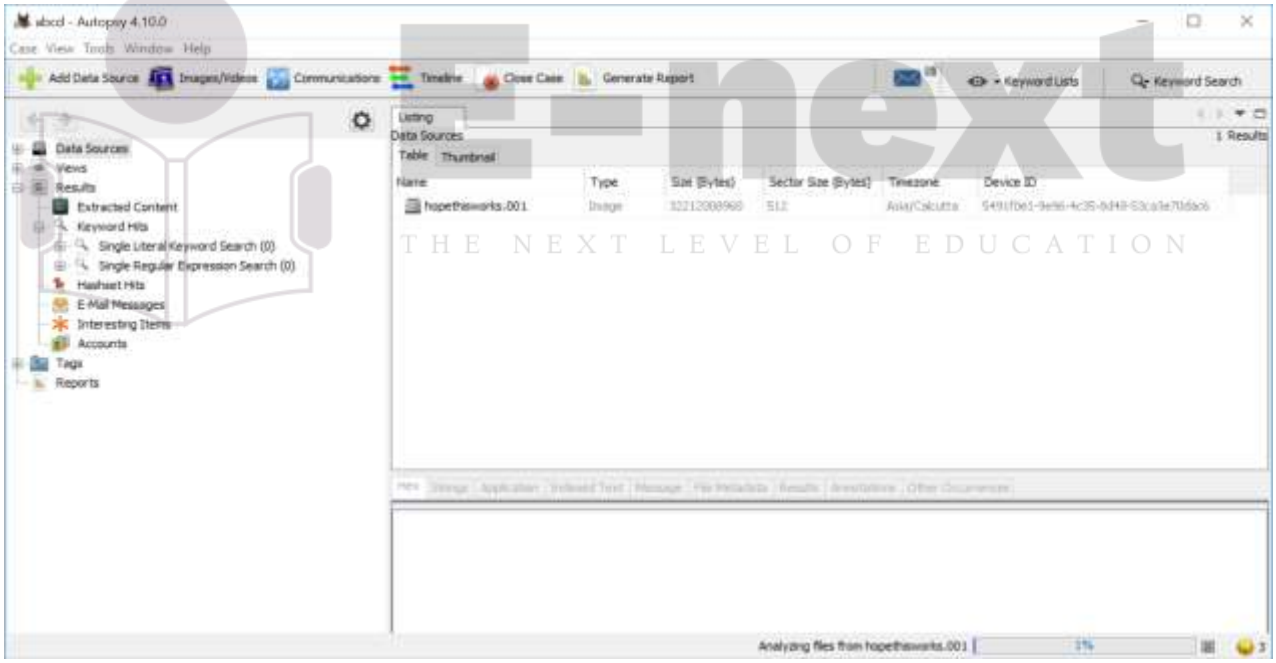
6. Select all ingest modules



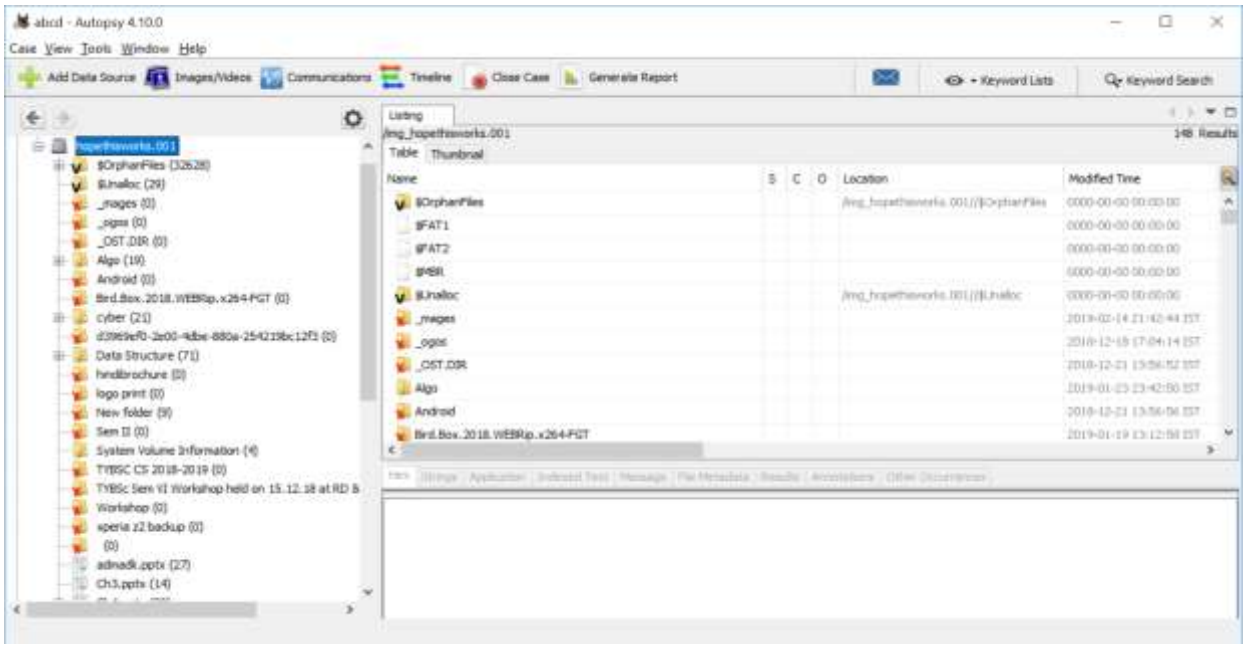
7.Wait for Data source to process and be added to local database. Click Finish



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

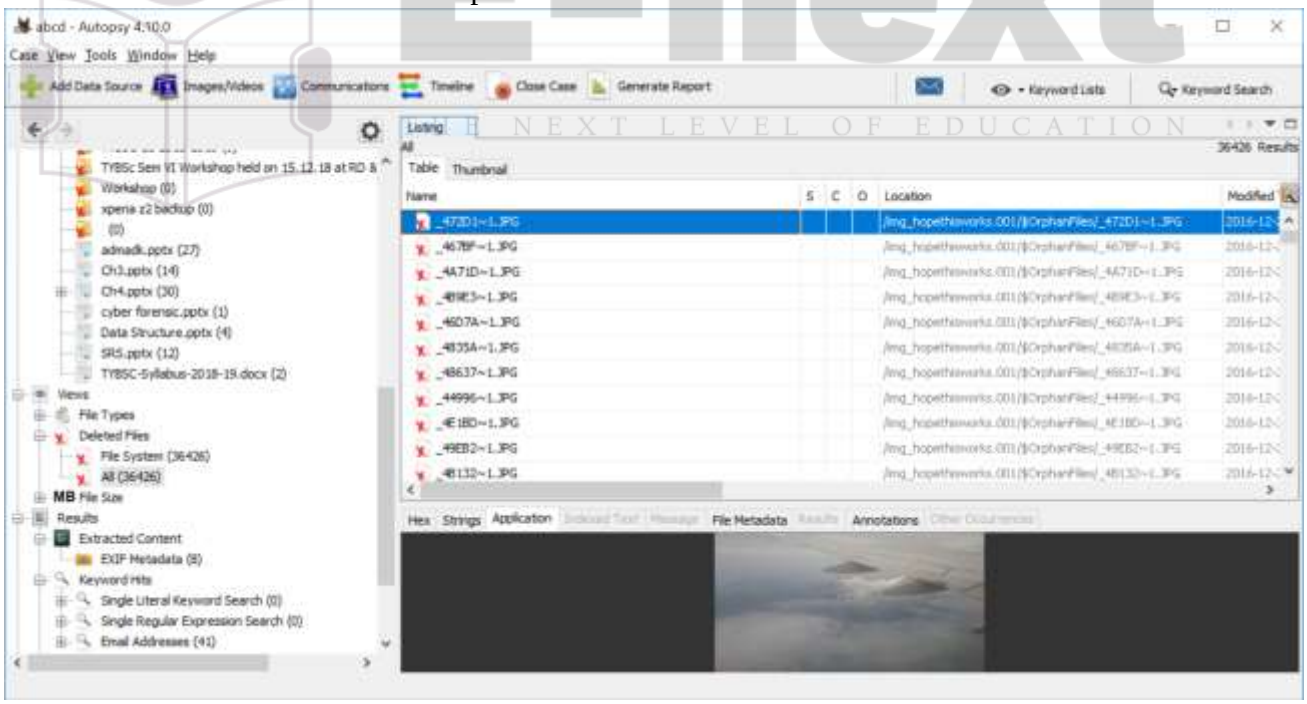


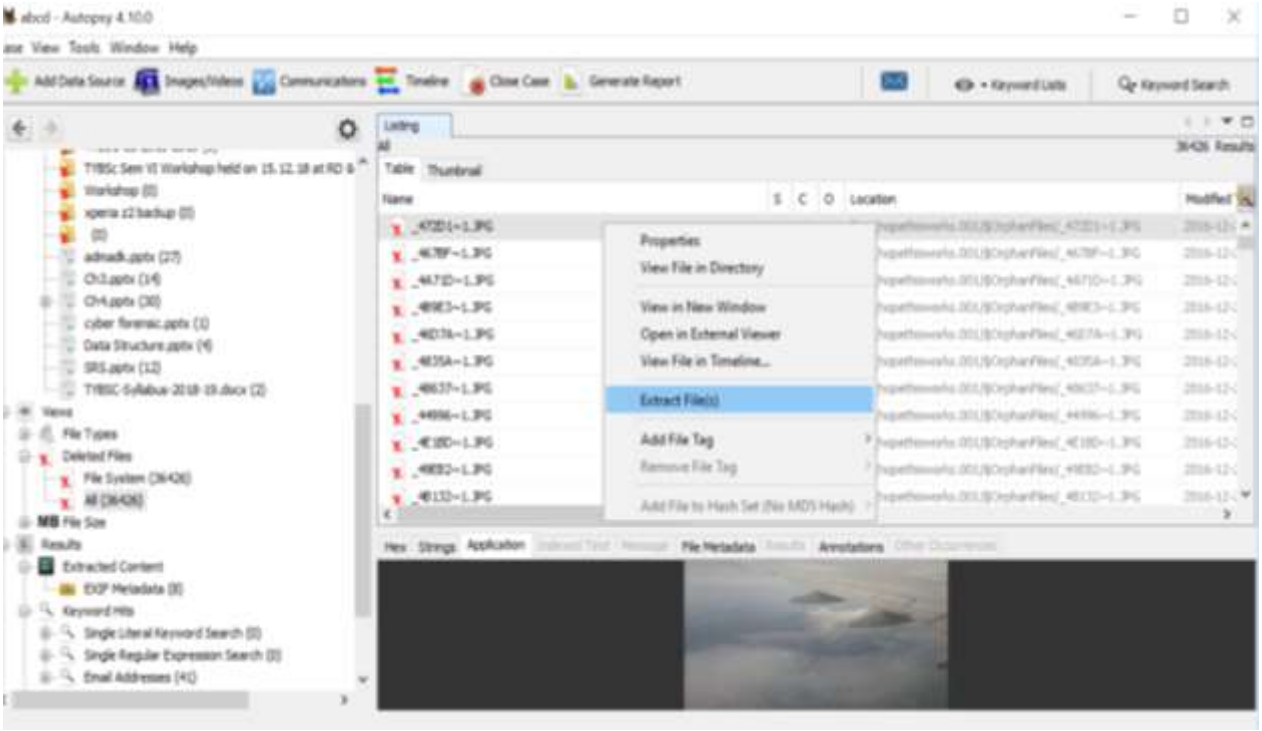
9. All files will appear in table tab select any file to see the data.



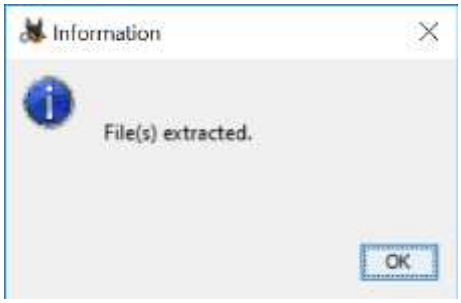
10. Expand the tree from left side panel to view the files and then expand the deleted files node

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

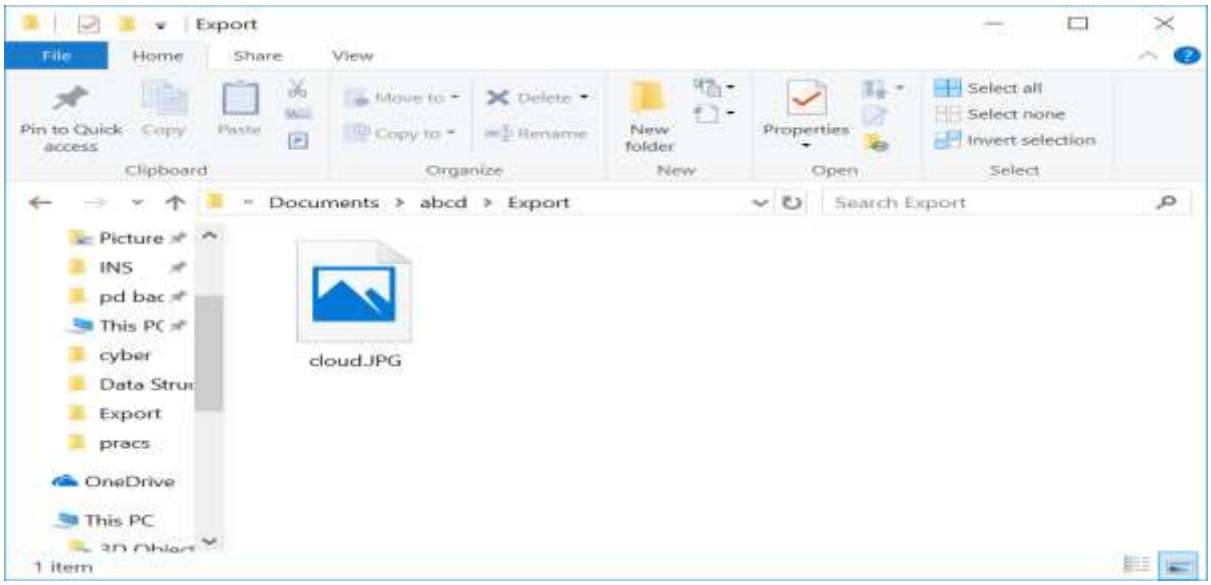


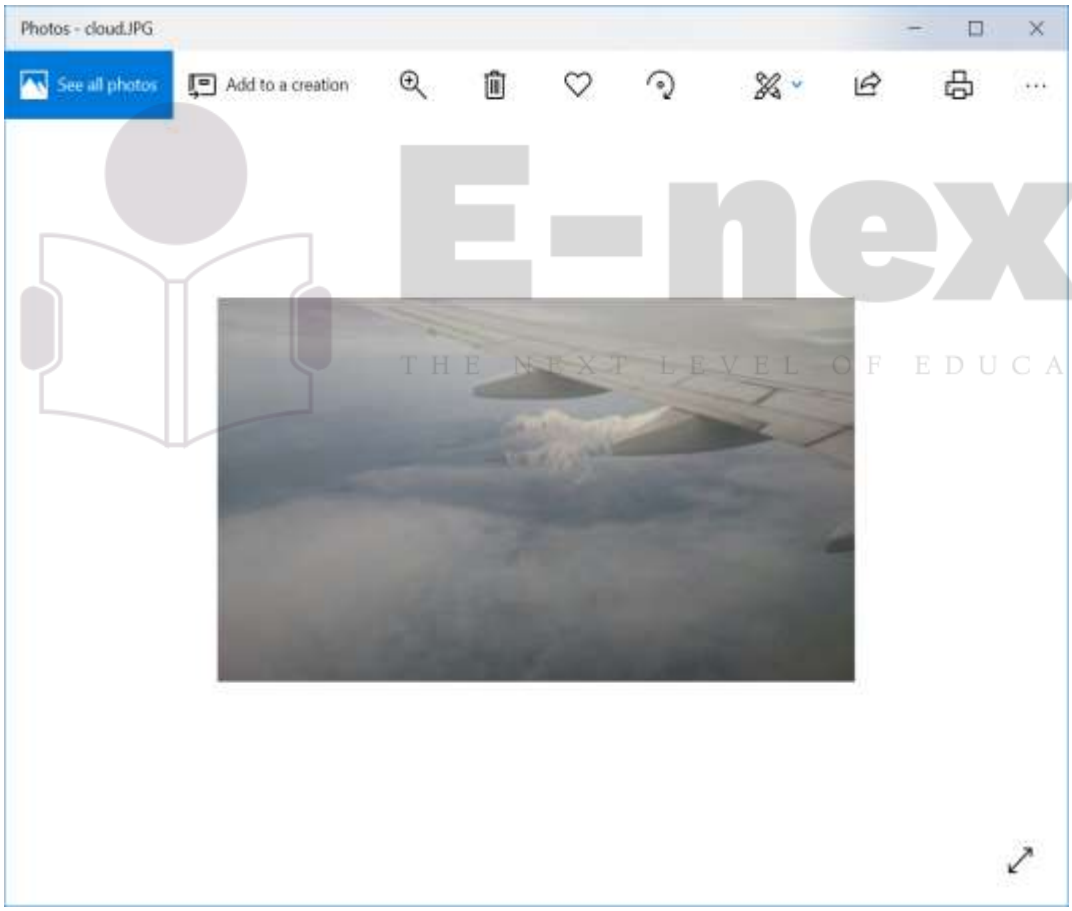


12. By default Export folder is choose to save the recovered file.

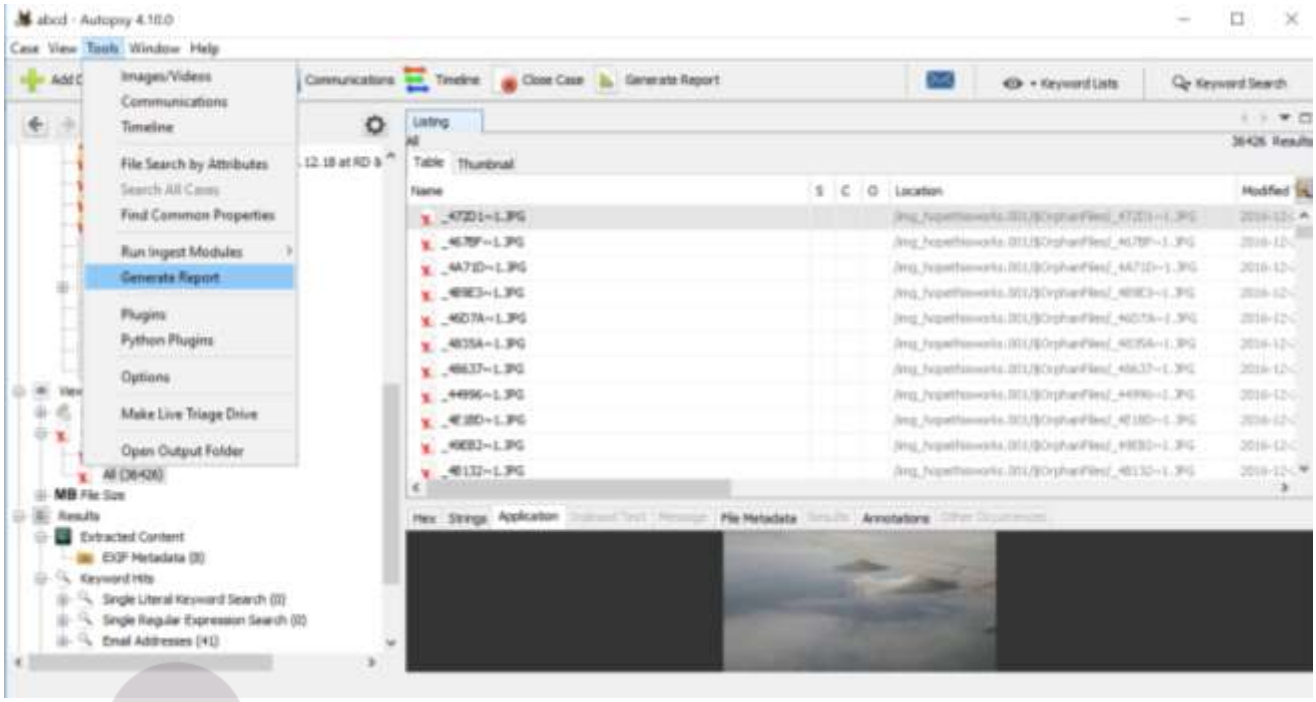


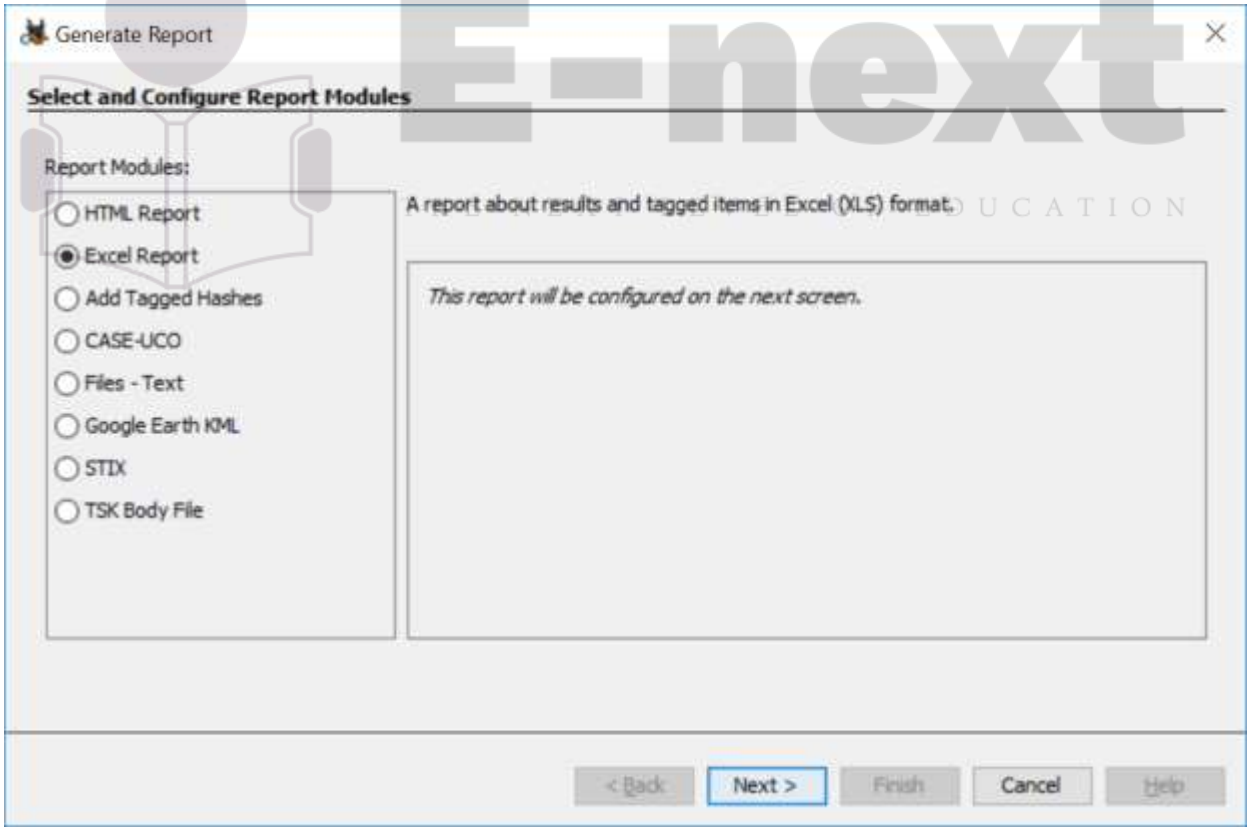
13. Now go to the Export Folder to view Recover file.



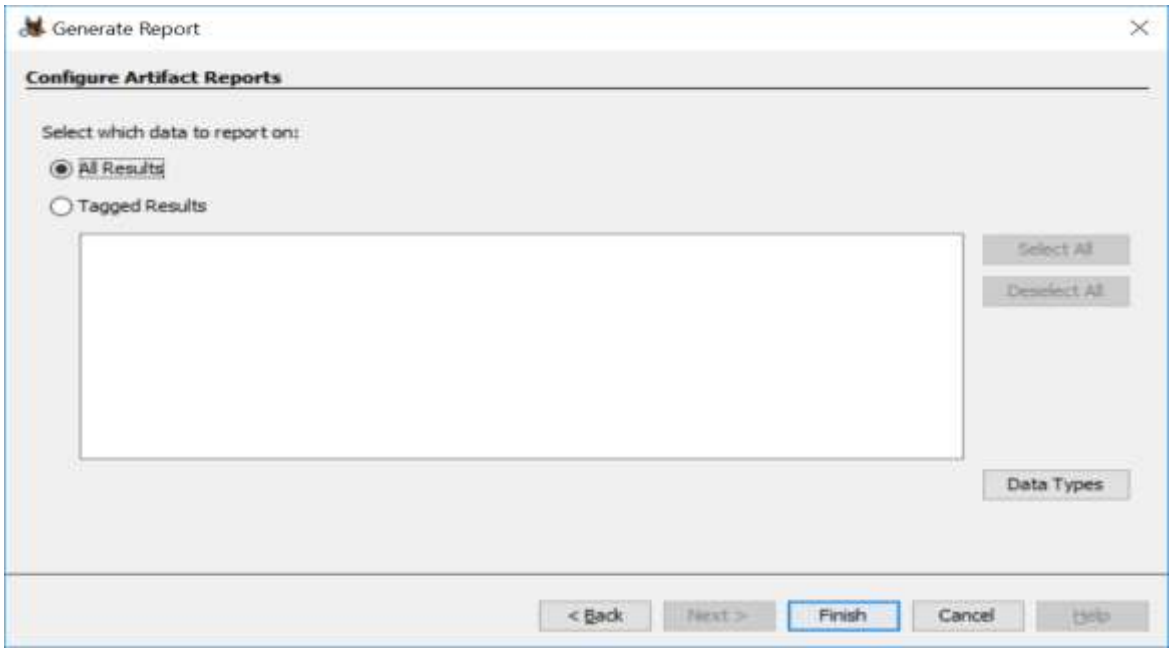


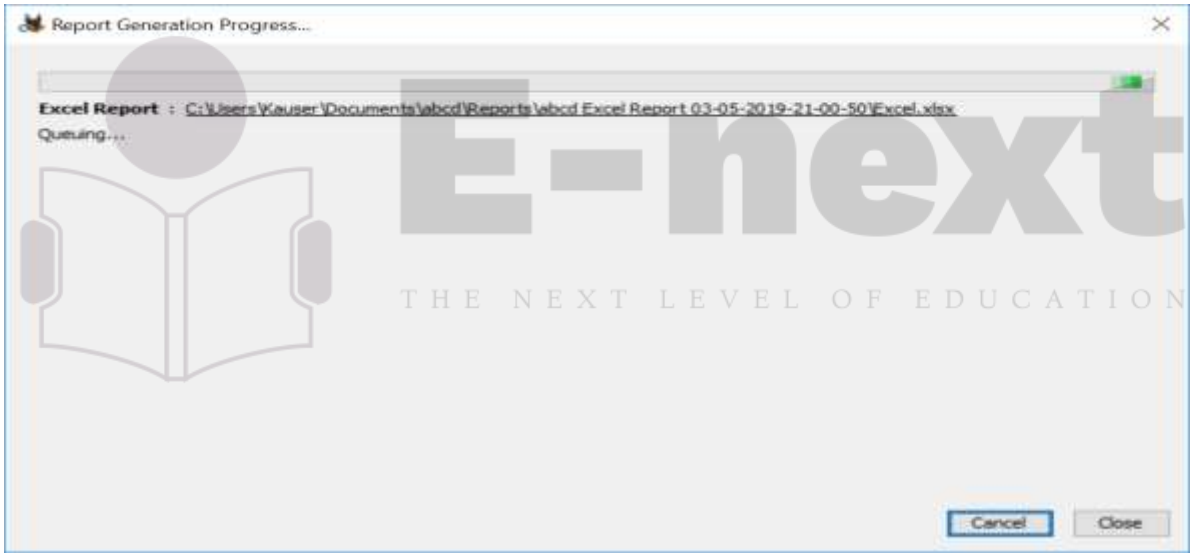
14. Click on Generate Report from autopsy window and Select the Excel format and click on next

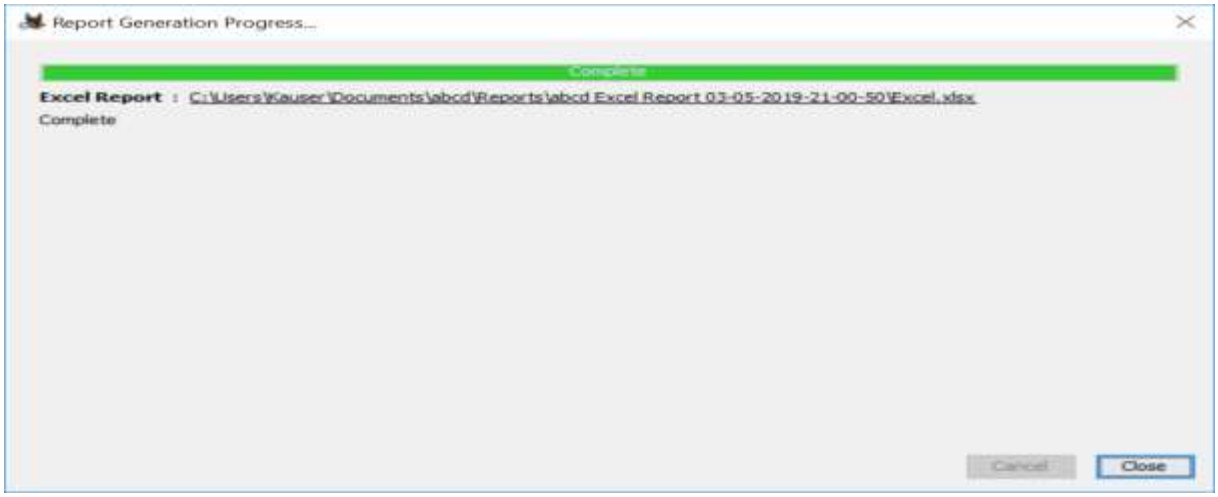




15. Click Finish after selecting All Results

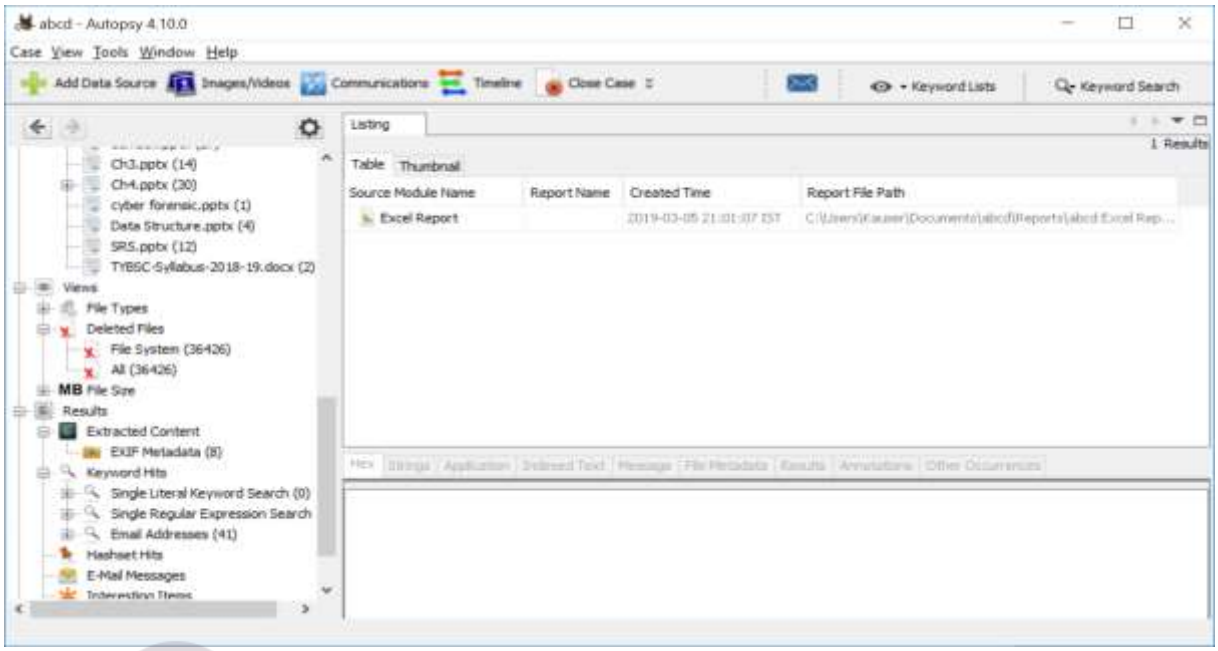


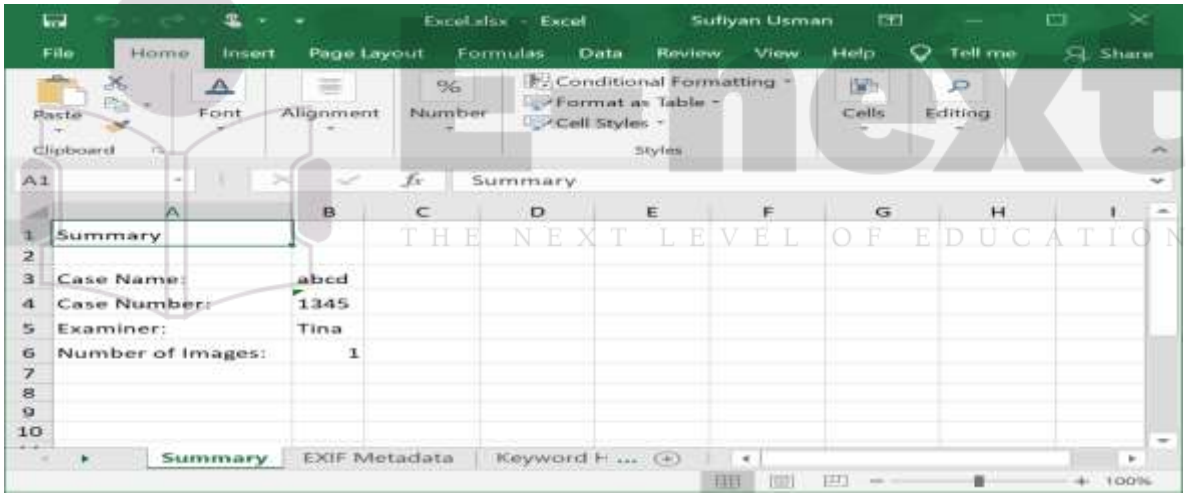


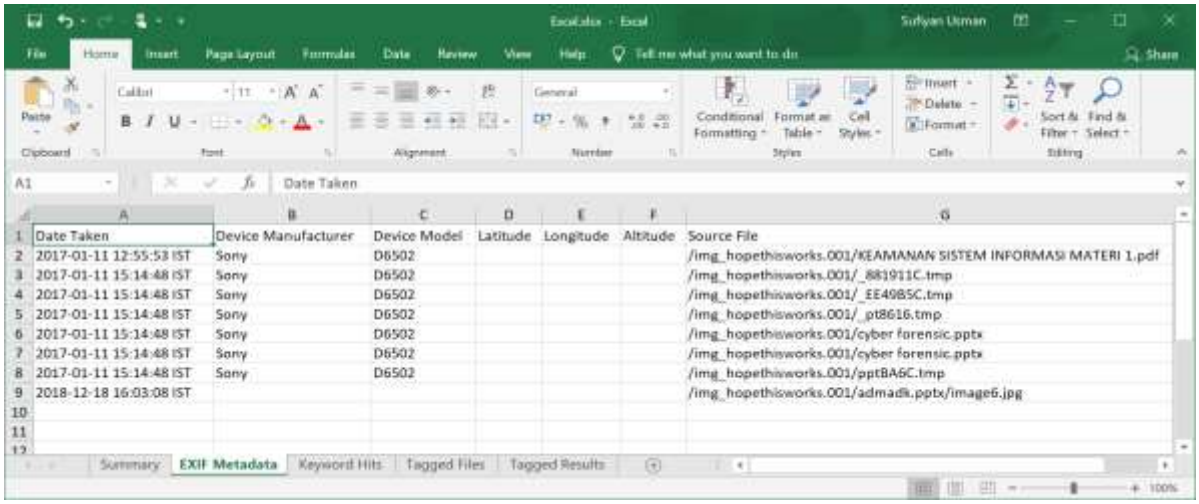


Now Report is Generated So click on close Button, We can see the Report on Report Node.

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







Practical No – 1

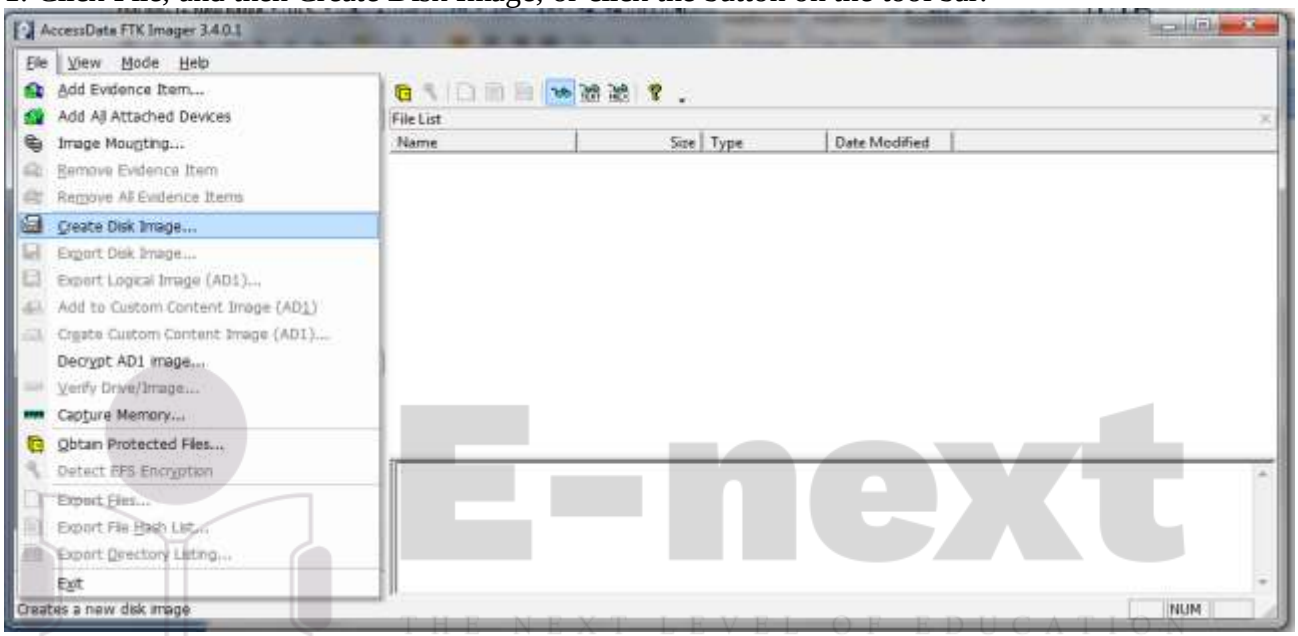
Aim: Creating a Forensic Image using FTK Imager/Encase Imager:

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

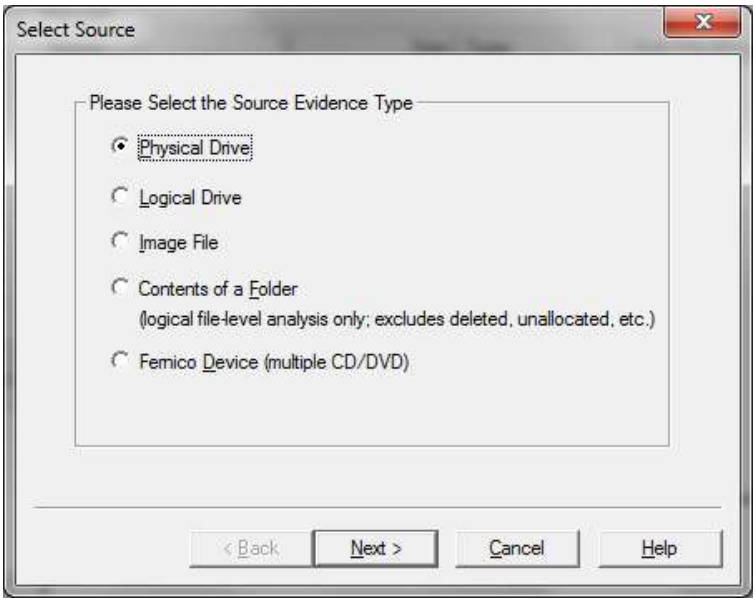
Steps:

Creating Forensic Image

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

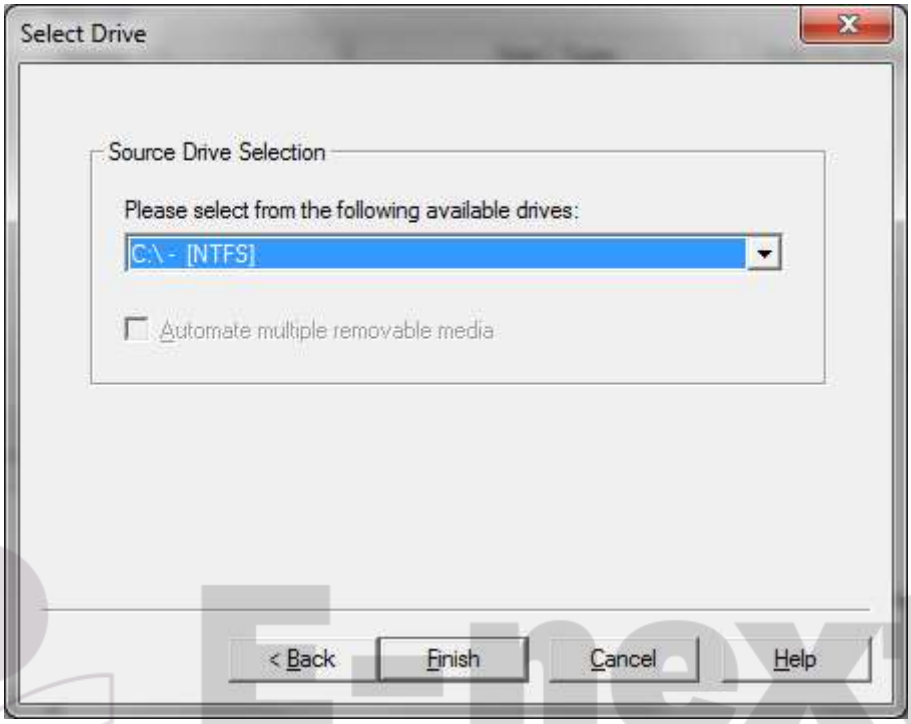


2. Select the source you want to make an image of and click Next.

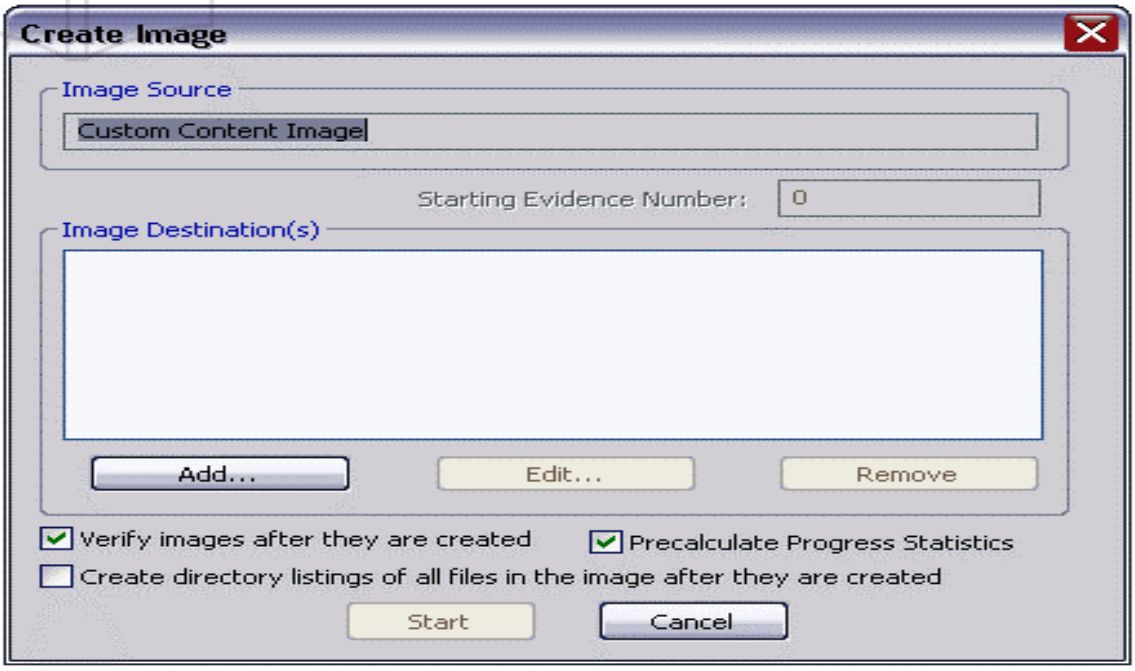


If you select Logical Drive to select a floppy or CD as a source, you can check the Automate multiple removable media box to create groups of images. Imager will automatically increment the case numbers with each image, and if something interrupts the process, you may assign case number manually.

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



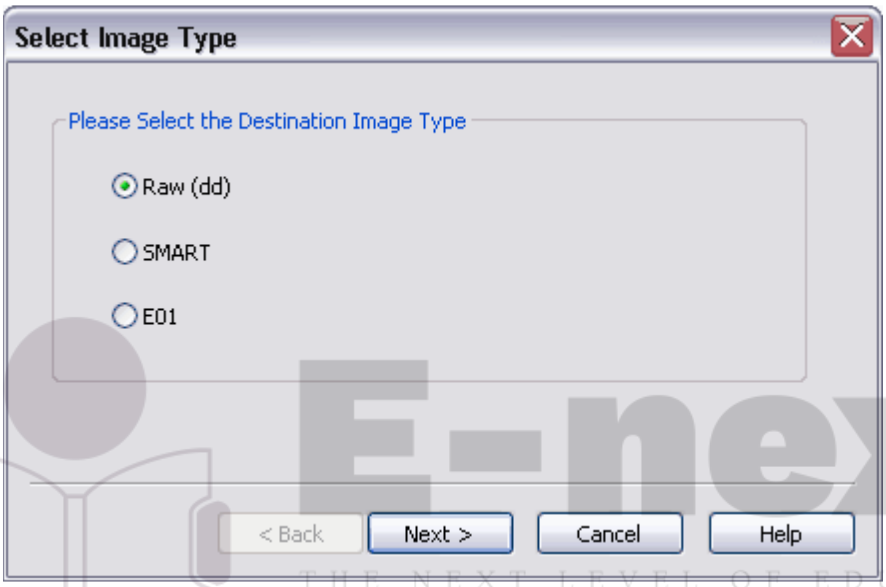
4. In the Create Image dialog, click Add.



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

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

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



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

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

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

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

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

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

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

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

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

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

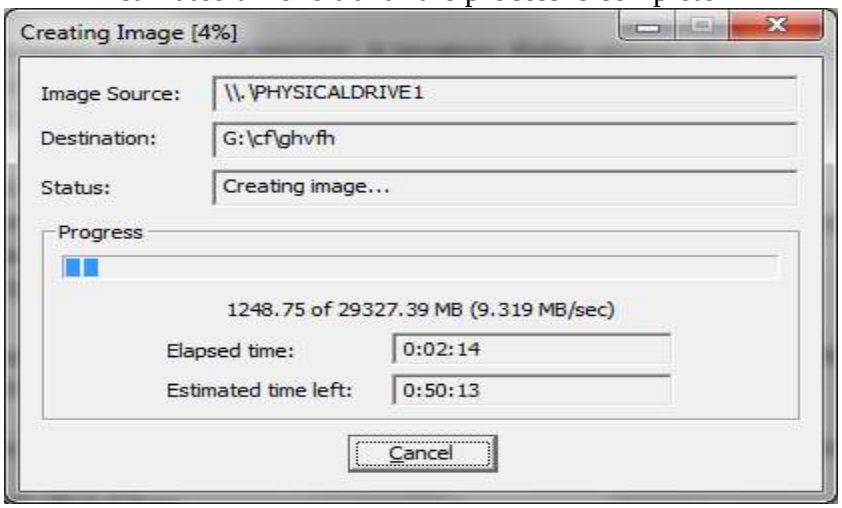
> **Tip:** If you want to transfer the image file to CD, accept the default fragment size of 650 MB.

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

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

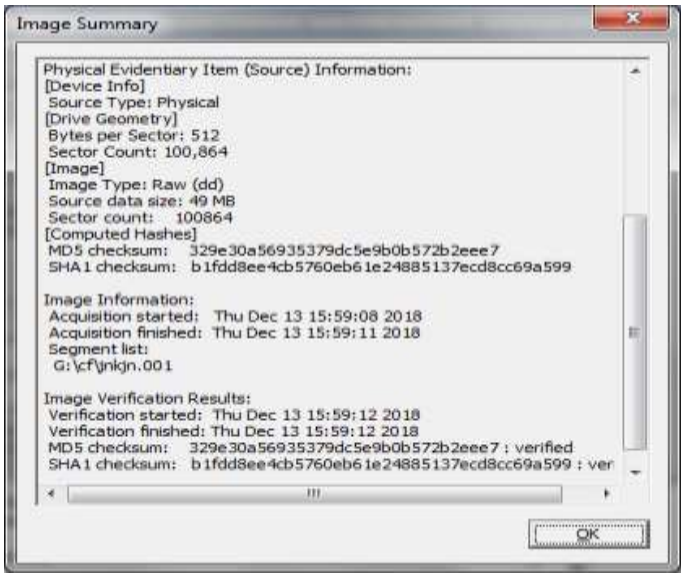
11. Click **Start** to begin the imaging process. A progress dialog appears that shows the following:

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



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

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

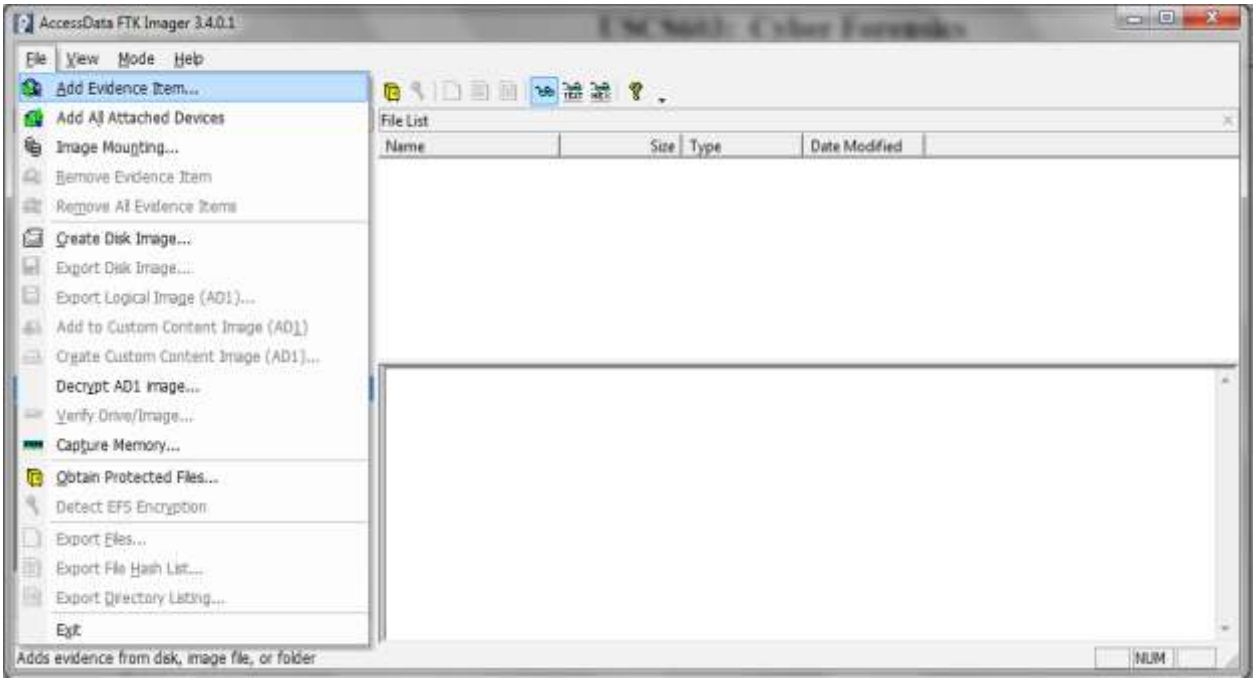


13. When finished, click **Close**

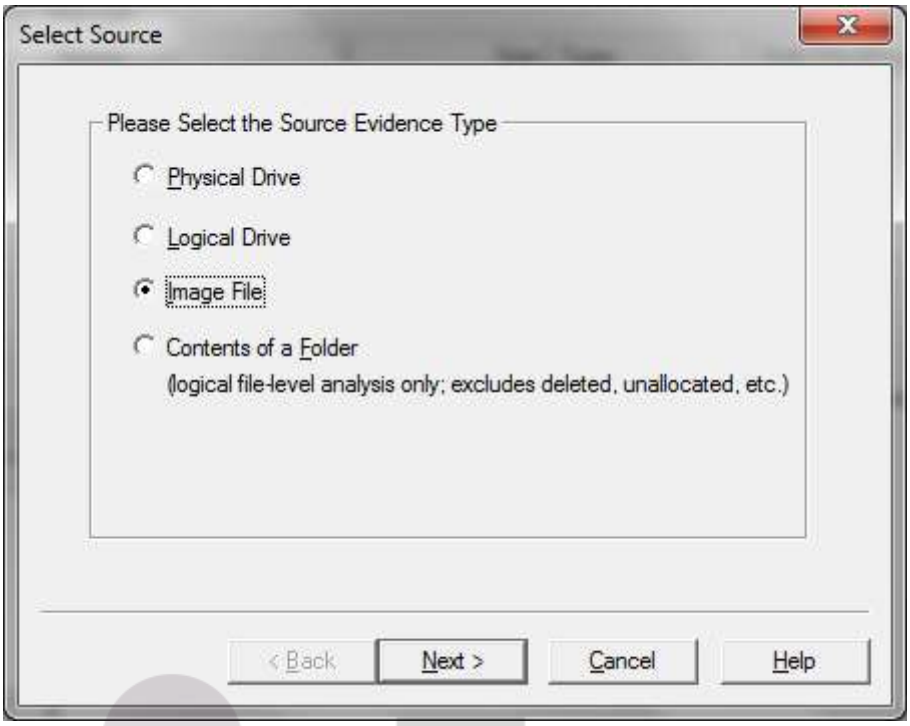
Note that the image file (*.001) as well as the image summary file from above (*.txt) have been saved onto the 'Drive'. The .001 extension may be left as is, or can be changed to .dd. The .001 extension is used due to the fact that many times the file to be imaged is very large and must be split into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

Analyze Forensic Image:

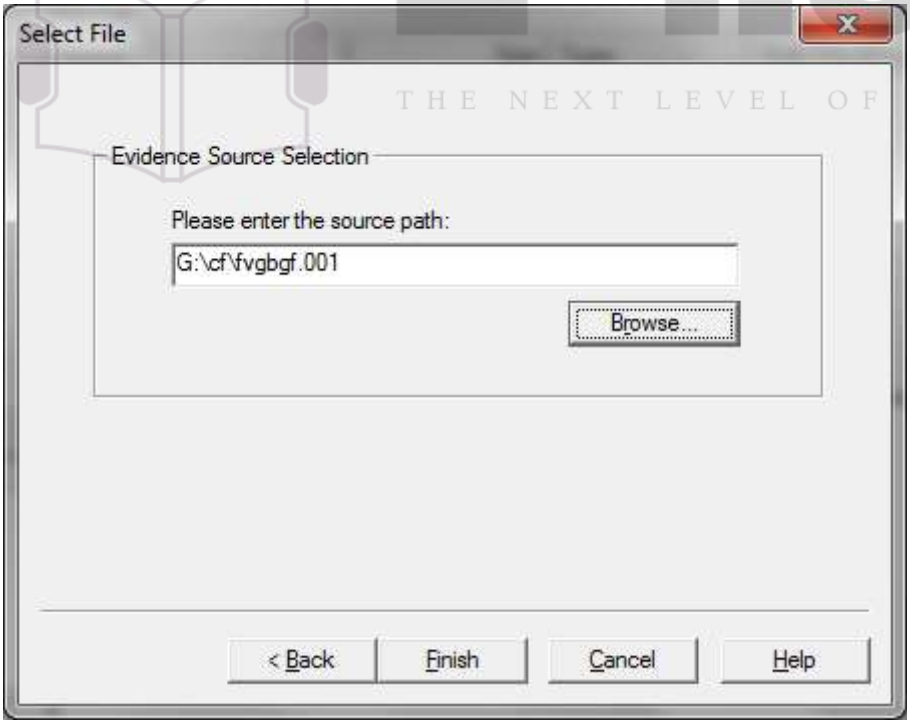
Click on Add Evidence Item to add evidence from disk, image file or folder.



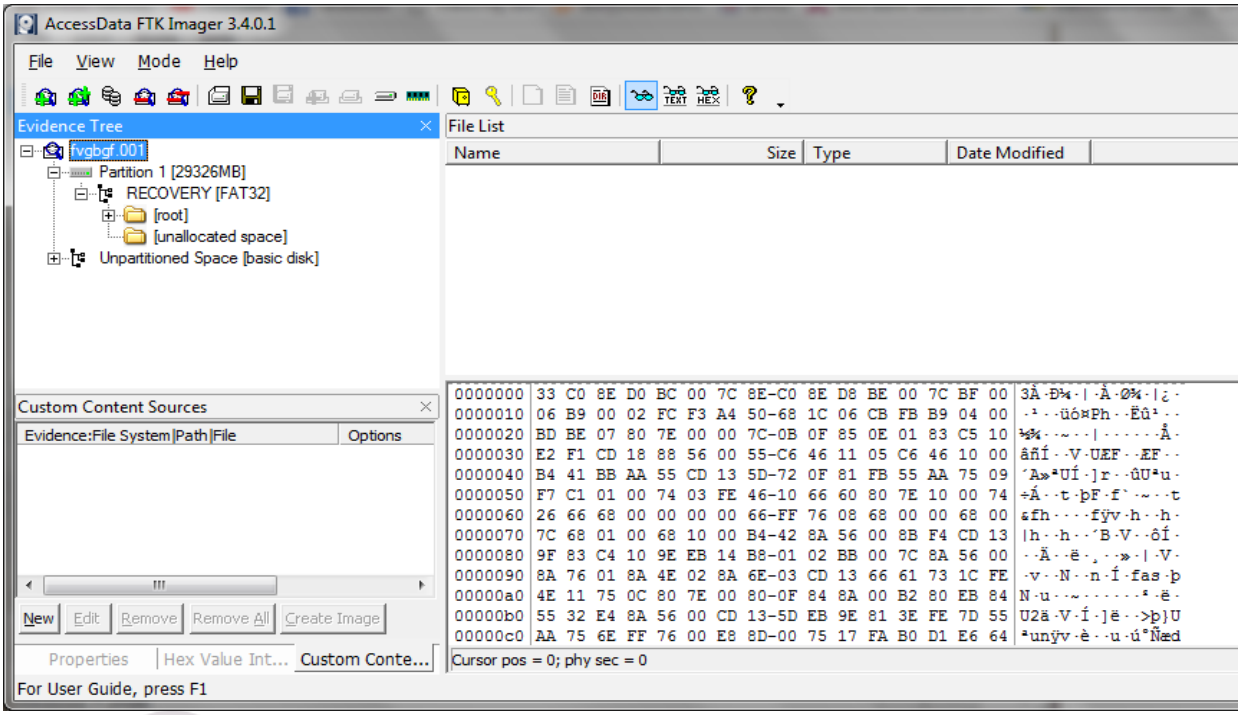
Now select the source evidence type as physical drive, logical drive or image file. We have selected image file and click on next.



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



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



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

Click on finish.

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

Practical No – 2

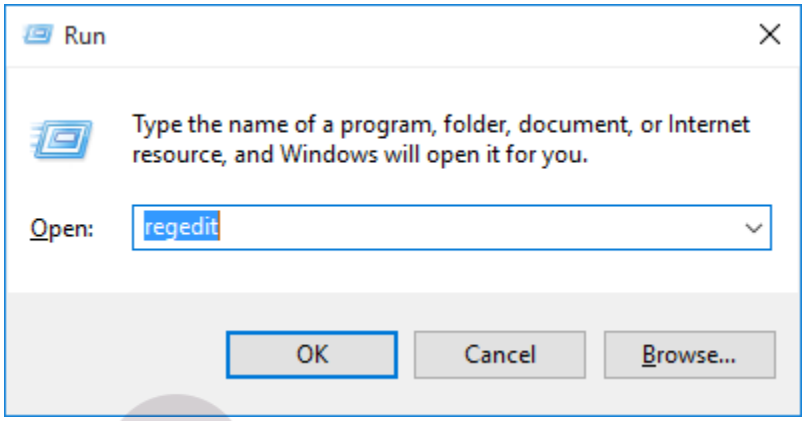
Aim: Data Acquisition:

- **Perform data acquisition using:**
- **USB Write Blocker + FTK Imager**

Steps:

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

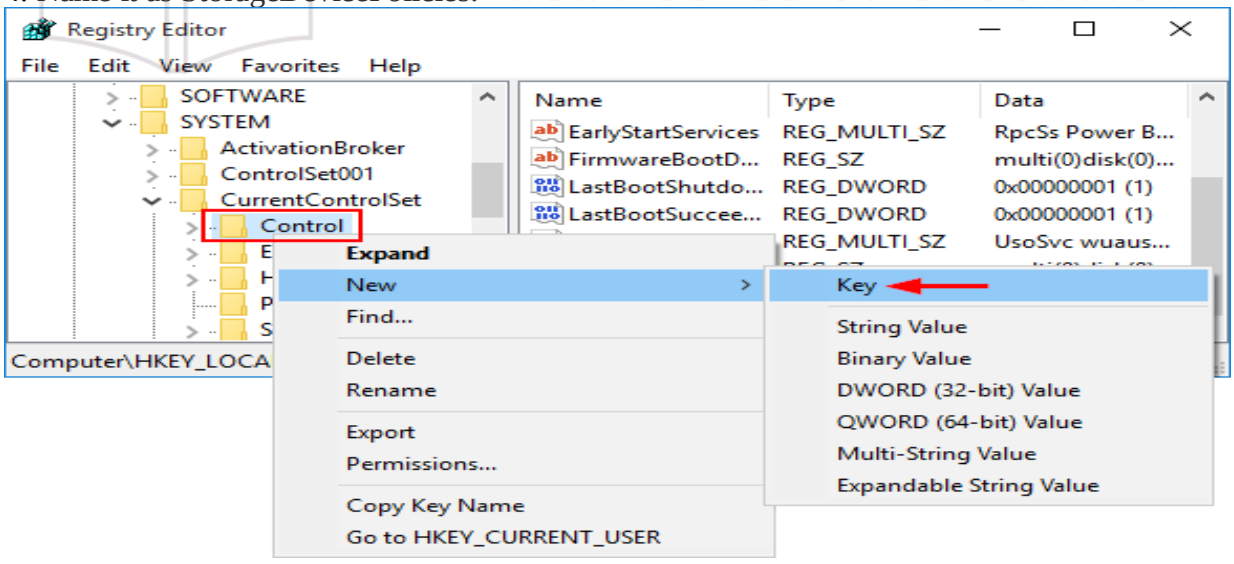
1. Press the Windows key + R to open the Run box. Type regedit and press Enter.



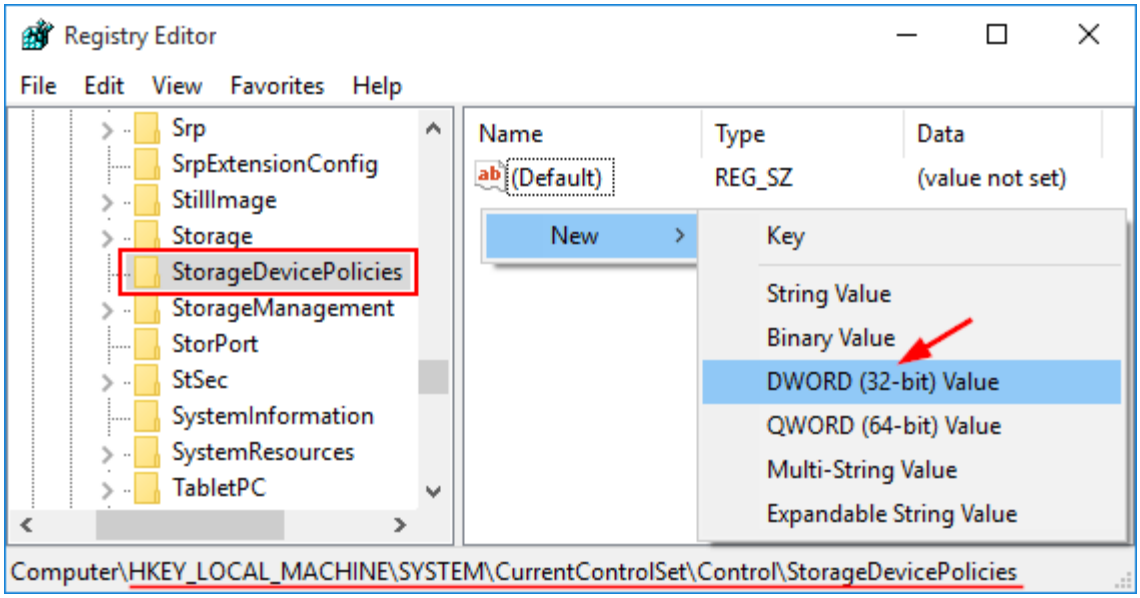
2. This will open the Registry Editor. Navigate to the following key:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control

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

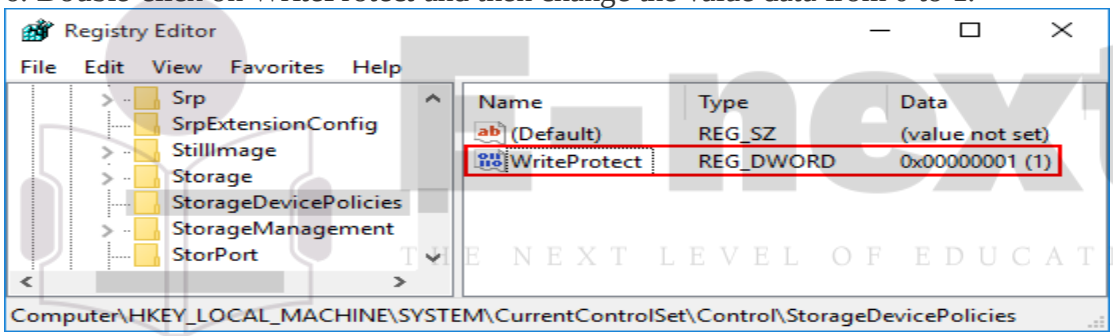
4. Name it as StorageDevicePolicies.



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

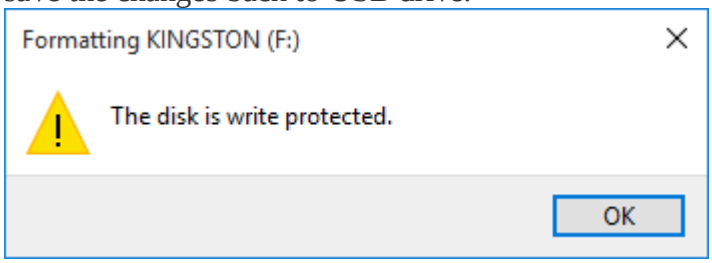


6. Double-click on WriteProtect and then change the value data from 0 to 1.



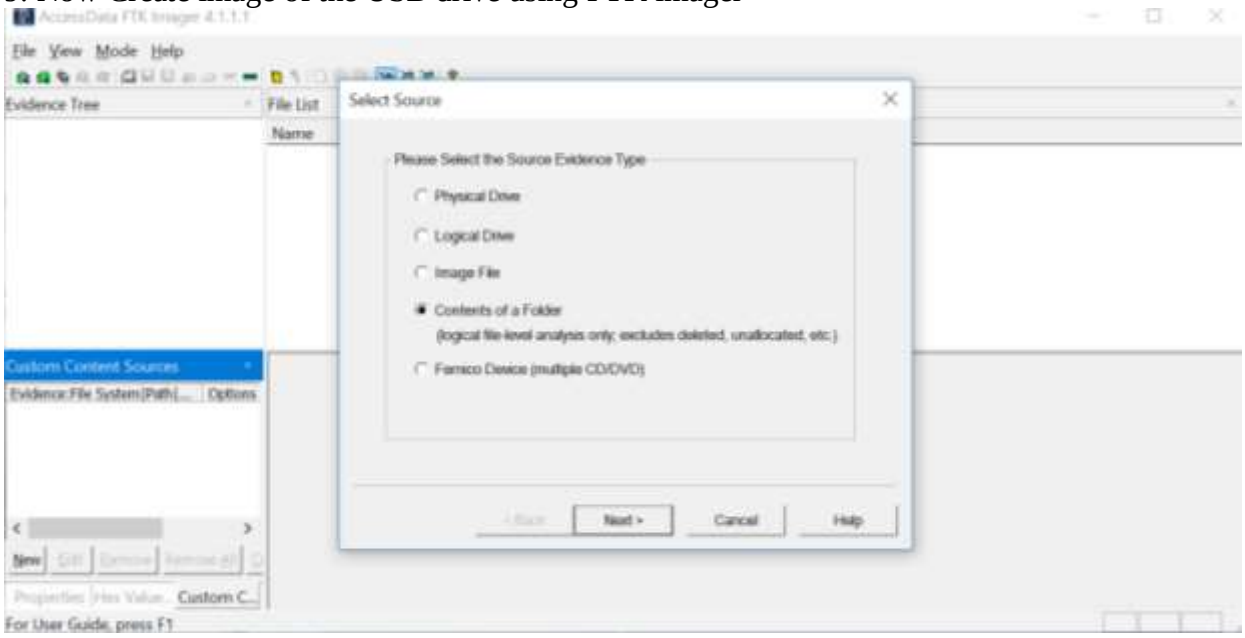
7. The new setting takes effect immediately. Every user who tries to copy / move data to USB devices or format USB drive will get the error message
"*The disk is write-protected*".

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



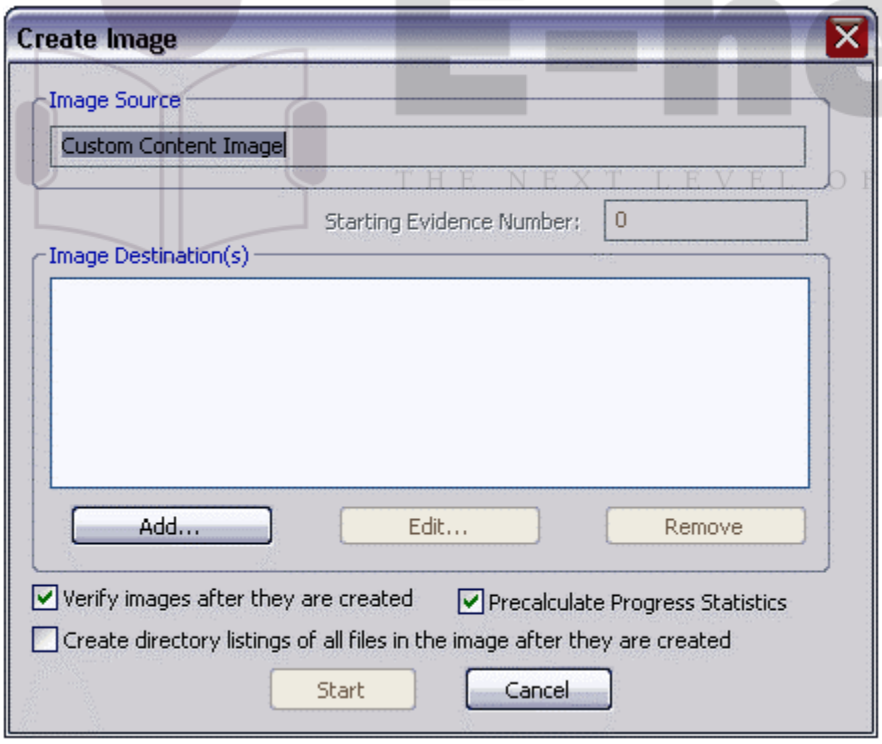
So this is how you can enable write protection to all connected USB drives. If you want to disable write protection at a later time, just open Registry Editor and set the WriteProtect value to 0.

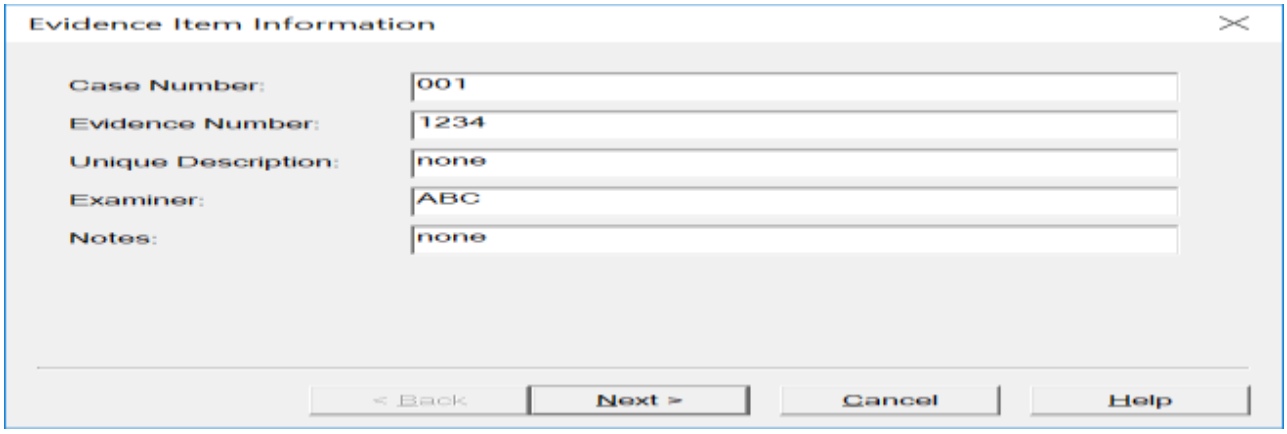
9. Now Create image of the USB drive using FTK imager



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

11.In the Create Image dialog, click Add.





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

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