



**S.I.W.S**

**N.R SWAMY COLLEGE OF COMMERCE AND ECONOMICS AND  
SMT.THIRUMALAI COLLEGE OF SCIENCE.**

**CYBER FORENSICS**

**JAISWAR ROHIT MANOJ**

**T.Y.Bsc.C.S**

**ROLL NO:39041**

**Year 2022-2023**

**S.I.W.S****N.R SWAMY COLLEGE OF COMMERCE AND ECONOMICS  
AND****SMT. THIRUMALAI COLLEGE OF SCIENCE**Plot No.337, Major R. Parmeshwaran Marg, Sewree Wadala Estate,  
Wadala, Mumbai-400 031.**T.Y.B.Sc.(Computer Science)  
Semester VI****CERTIFICATE**

Class: \_\_\_\_\_

University Seat No.: \_\_\_\_\_

Roll No.: \_\_\_\_\_

This is to certify that the experiments entered in this journal is the work of  
Mr./Ms. \_\_\_\_\_ in the Computer Science Department of S.I.W.S  
Degree College during the year 2022 – 2023.

\_\_\_\_\_  
Teacher-In-Charge\_\_\_\_\_  
Co-Ordinator\_\_\_\_\_  
Internal Examiner\_\_\_\_\_  
External Examiner

Date: \_\_\_\_\_

**College Stamp**

## INDEX

SR.NO	DATE	TITLE	PAGE NO	SIGN
1		<b>PRACTICAL NO 1</b> Creating a Forensic Image using FTK Imager/Encase Imager: -Creating Forensic Image -Check Integrity of Data -Analyze Forensic Image		
2		<b>PRACTICAL NO 2</b> Data Acquisition: Perform data acquisition using: USB Write Blocker + FTK Imager		
3		<b>PRACTICAL NO 3</b> Forensic Case Study: -Solve the Case study(image file) provide in lab using Autopsy		
4		<b>PRACTICAL NO 4</b> Capturing and analzing network packets using wireshark(Fundamentals): -Identification the live network -Capture Packets Analyze the Captured packets		
5		<b>PRACTICAL NO 5</b> Analyze the packets provided in lab and solve the questions using Wireshark:		
6		<b>PRACTICAL NO 6</b> 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		
7		<b>PRACTICAL NO 7</b> Recovering and Inspecting deleted files -Check for Deleted Files -Recover the Deleted Files -Analyzing and Inspecting the recovered files		
8		<b>PRACTICAL NO 8</b> Acquisition of Cell phones and Mobile		

## PRACTICAL NO 1

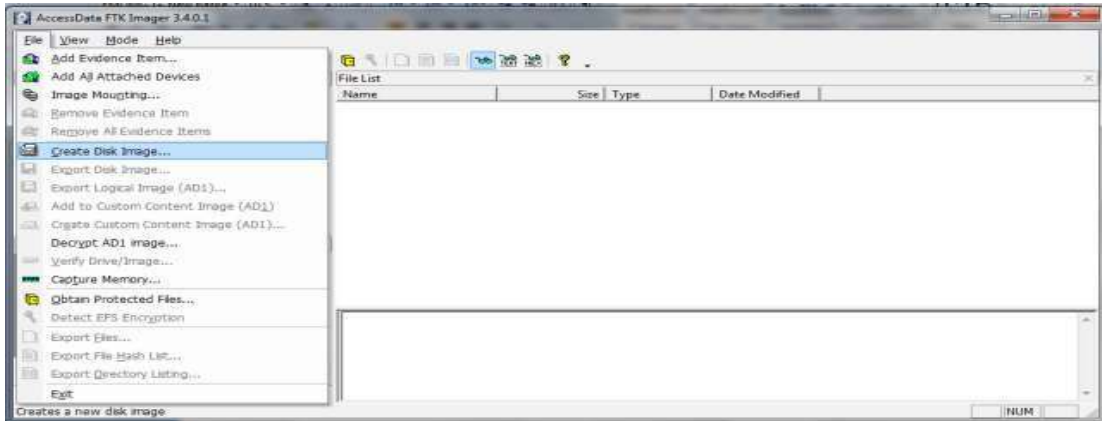
**Aim: Creating a Forensic Image using FTK Imager/Encase Imager:**

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

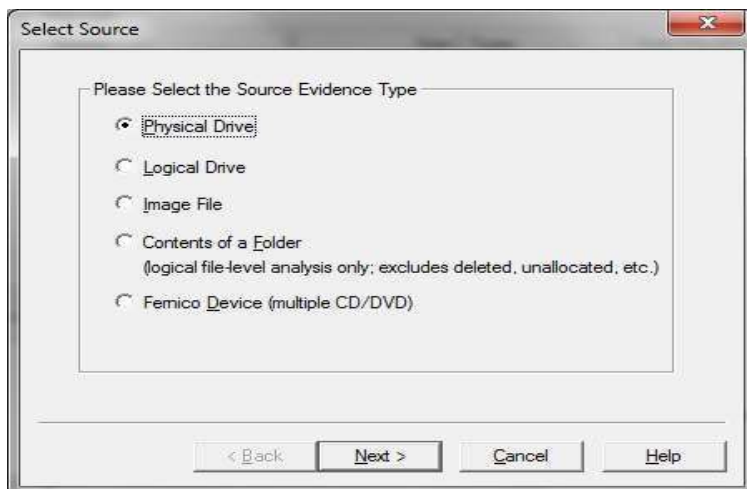
### Steps:

#### Creating Forensic Image

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

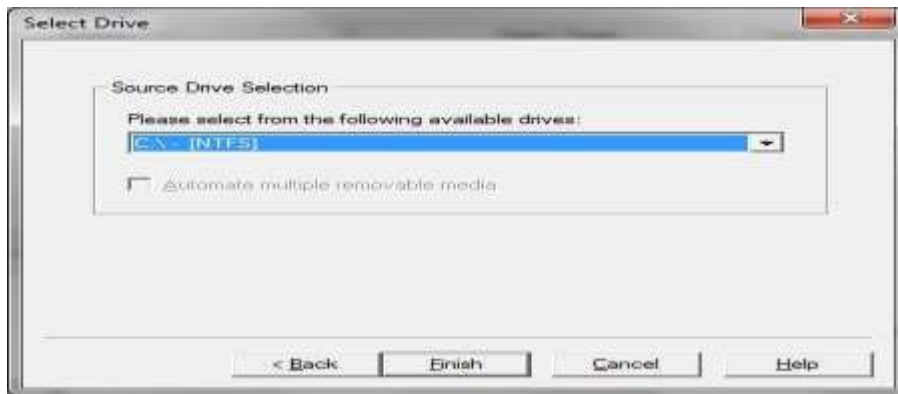


2. Select the source you want to make an image of and click Next.

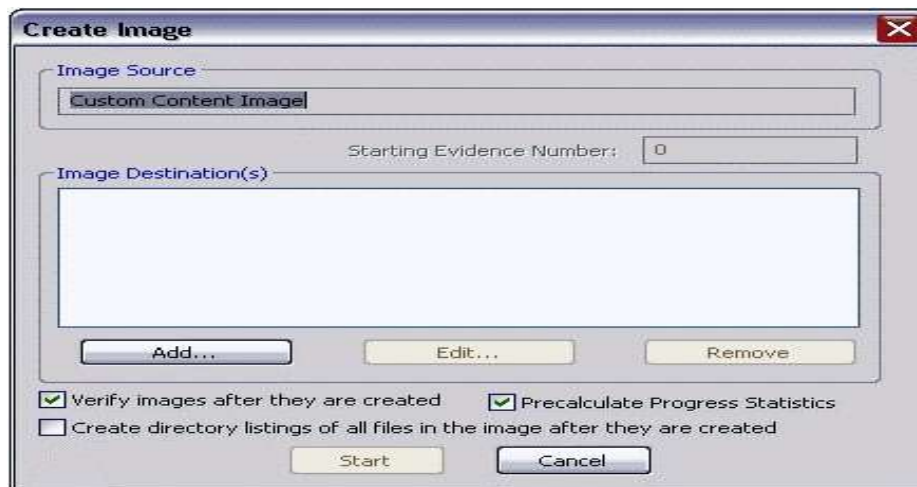


If you select Logical Drive to select a floppy or CD as a source, you can check the Automate multiple removable media box to create groups of images. Imager will automatically increment the case numbers with each image, and if something interrupts the process, you may assign case number manually.

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



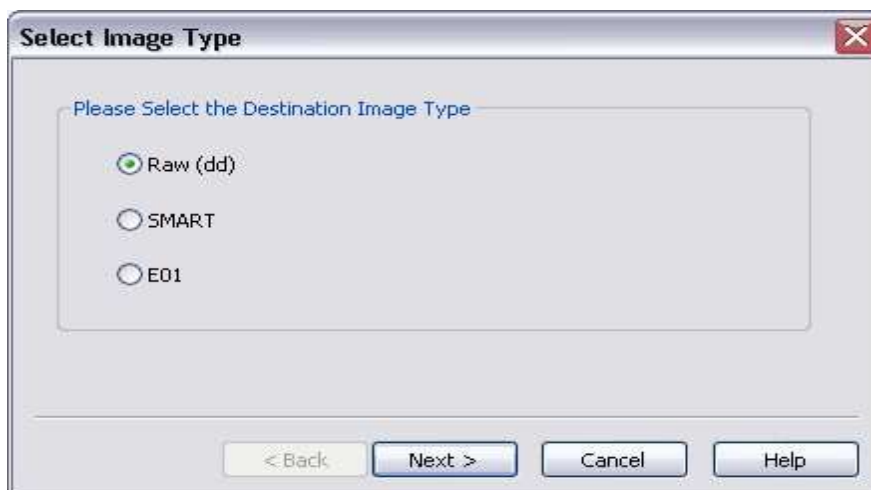
3. In the Create Image dialog, click Add.



- 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

4. 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.

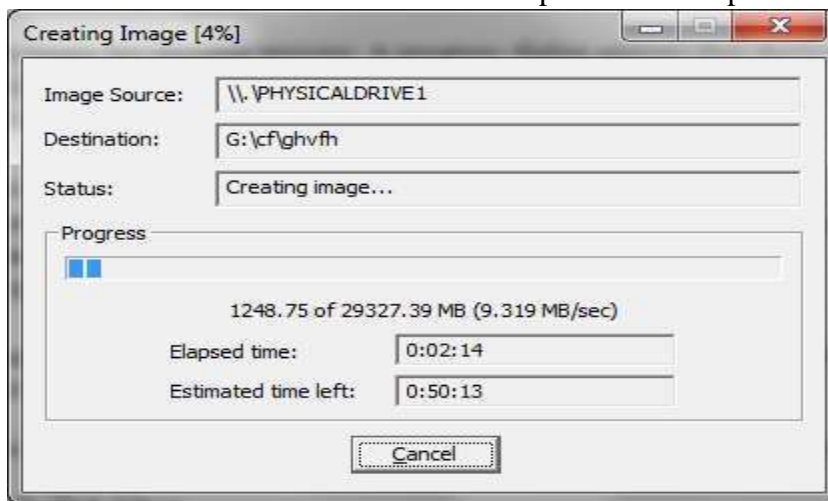
9. Click **Finish**. You return to the Create Image dialog.

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**.

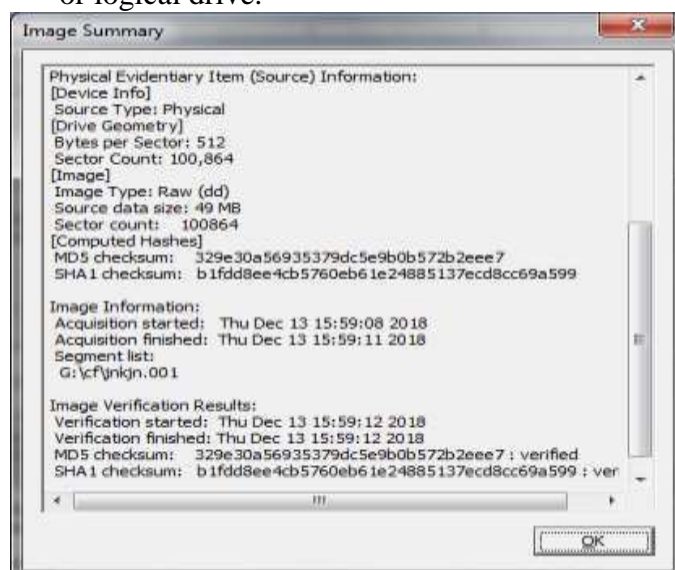
11. Click **Start** to begin the imaging process. A progress dialog appears that shows the following:

- 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.

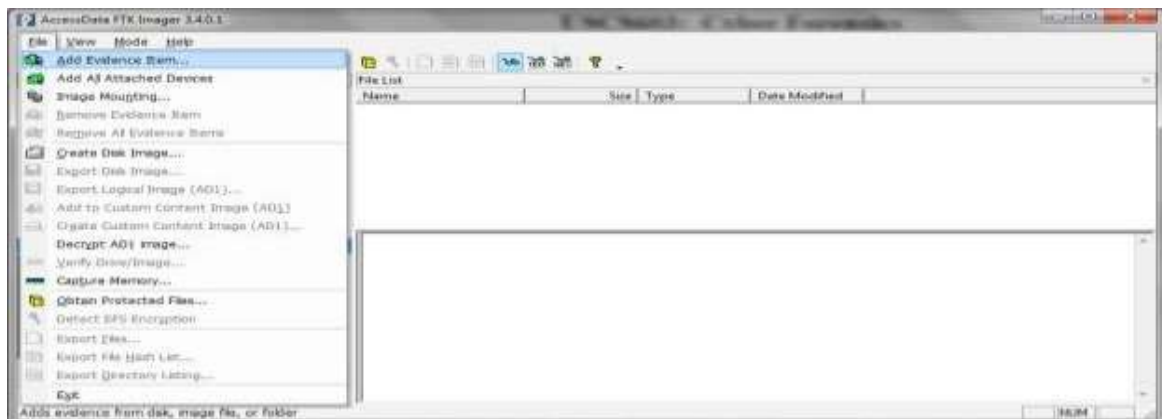


13. When finished, click **Close**

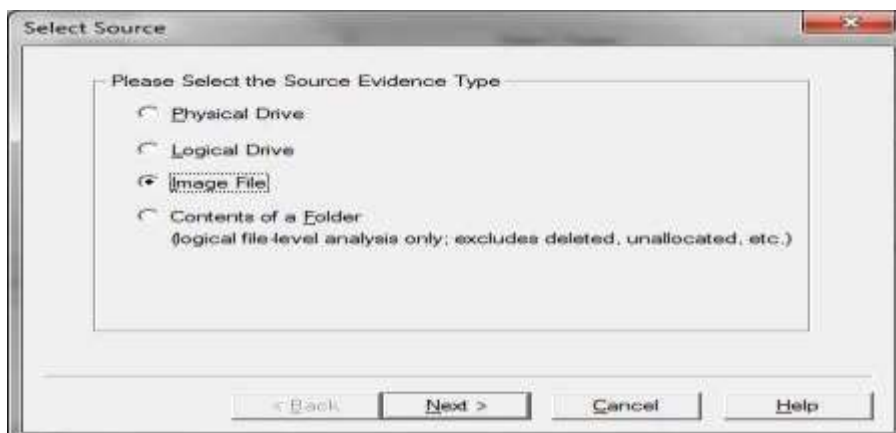
Note that the image file (\*.001) as well as the image summary file from above (\*.txt) have been saved onto the 'Drive'. The .001 extension may be left as is, or can be changed to .dd. The .001 extension is used due to the fact that many times the file to be imaged is very large and must be split into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

### Analyze Forensic Image:

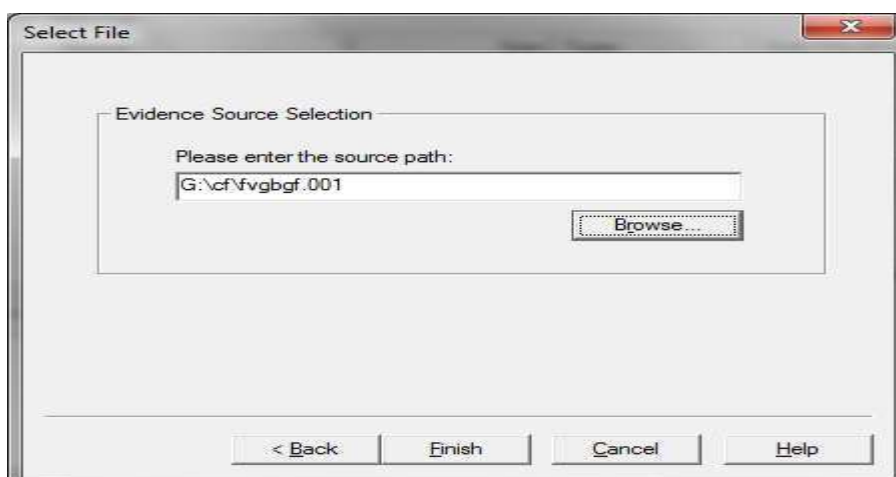
Click on Add Evidence Item to add evidence from disk, image file or folder.



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.





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

9

## PRACTICAL NO 2

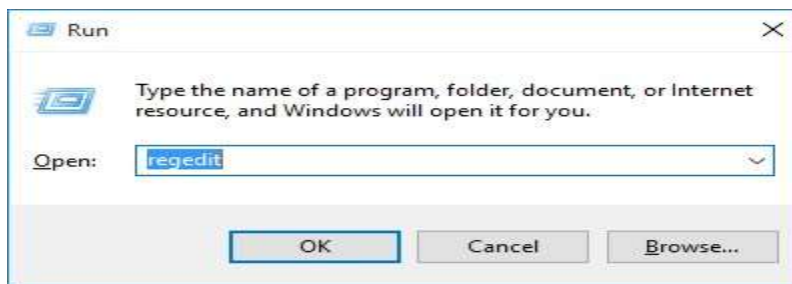
### Aim: Data Acquisition:

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

### Steps:

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

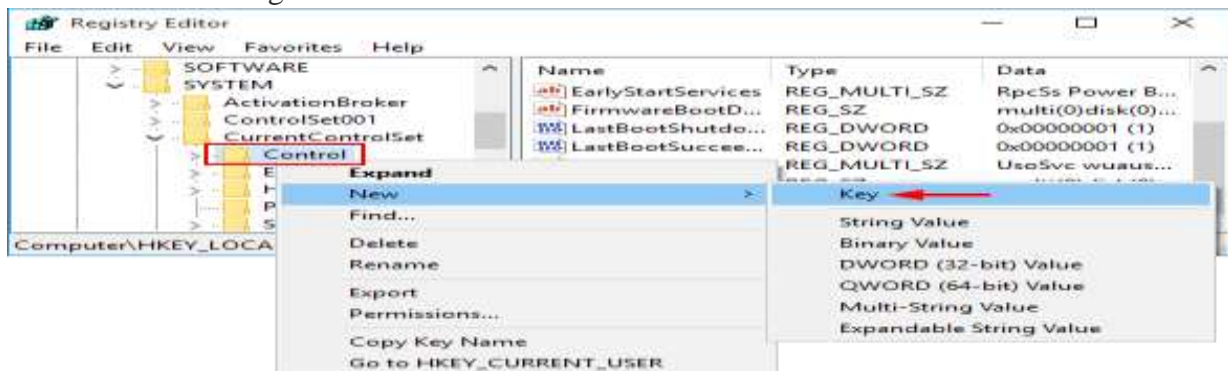
1. Press the Windows key + R to open the Run box. Type regedit and press Enter.



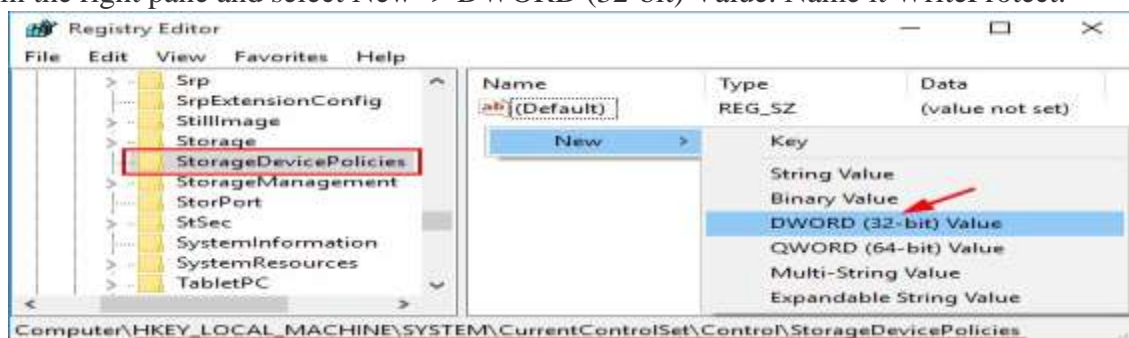
2. This will open the Registry Editor. Navigate to the following key: HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control

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

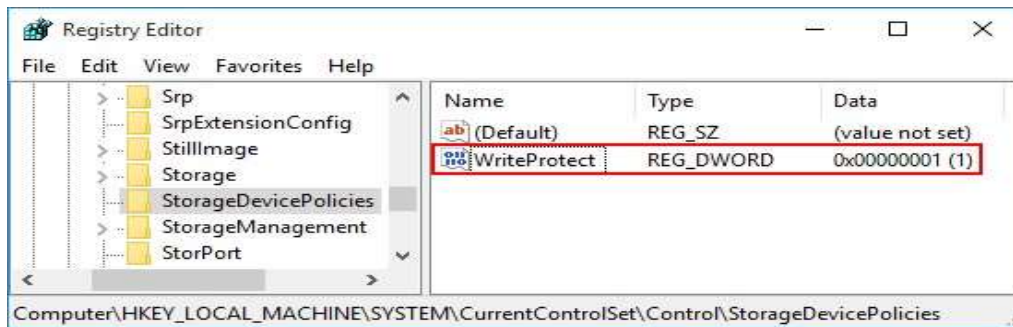
4. Name it as StorageDevicePolicies.



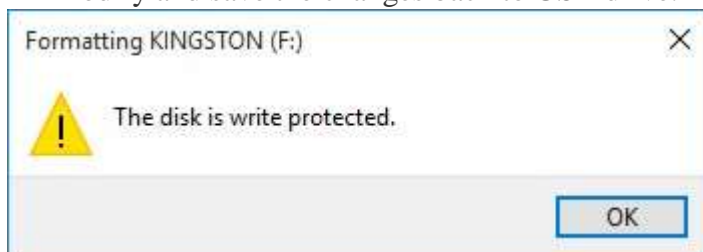
5. Select the StorageDevicePolicies key in the left pane, then right-click on any empty space in the right pane and select New -> DWORD (32-bit) Value. Name it WriteProtect.



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

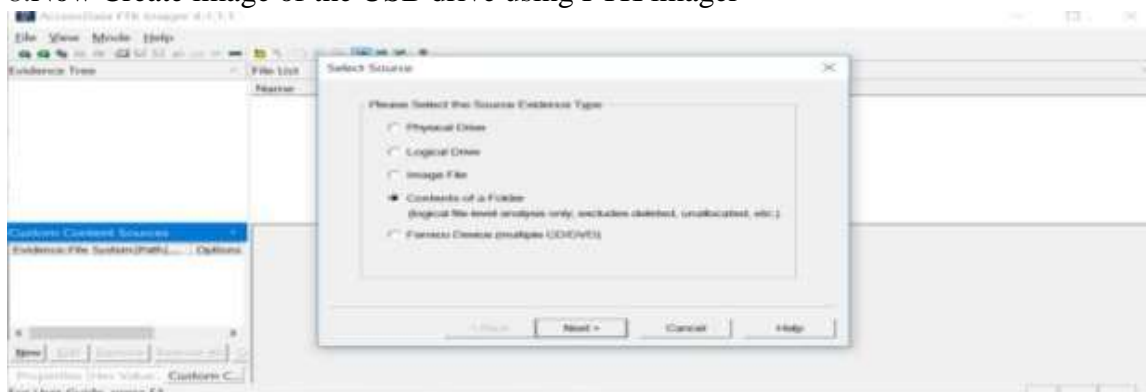


6. The new setting takes effect immediately. Every user who tries to copy / move data to USB devices or format USB drive will get the error message “*The disk is write-protected*”.
7. We can only open the file in the USB drive for reading, but it’s not allowed to modify and save the changes back to USB drive.



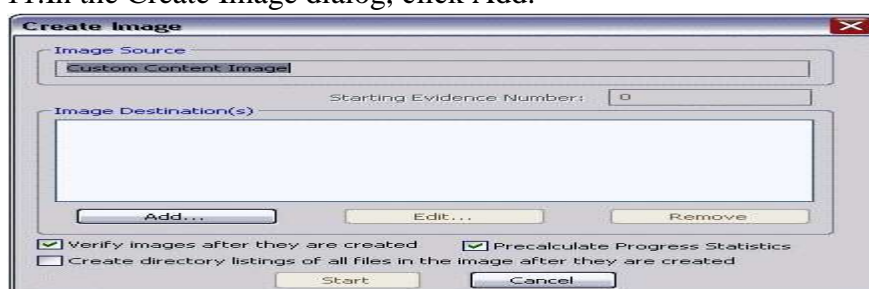
So this is how you can enable write protection to all connected USB drives. If you want to disable write protection at a later time, just open Registry Editor and set the WriteProtect value to 0.

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



8. 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

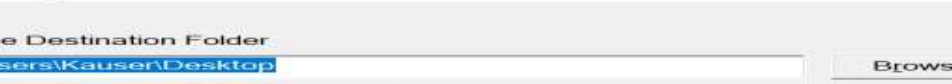
Next >

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  
C:\Users\Kausen\Desktop Browse

Image Filename (Excluding Extension)

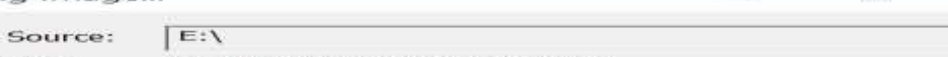
Image Fragment Size (MB)  
For Raw, E01, and AFF formats: 0 = do not fragment 1500

Compression (0=None, 1=Fastest, ..., 9=Smallest) 3

Use AD Encryption ☐

Filter by File Owner ☐

< Back Finish Cancel Help



Creating Image...

Image Source: E:\

Destination: C:\Users\Kausar\Desktop\blah

Status: Creating image...

Progress

Elapsed time: 0:00:05

Estimated time left:

Cancel

**Conclusion:** The above program has been executed successfully.

## PRACTICAL NO 3

### Aim: Forensics Case Study:

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

### Steps:

1. Start Autopsy

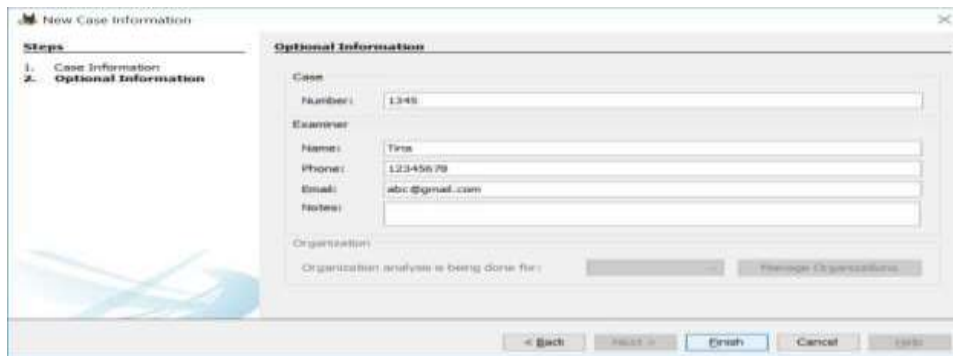


2. Select New Case



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





**New Case Information**

**Steps**

1. Case Information
2. **Optional Information**

**Optional Information**

Case Number: 1345

Examiner Name: Tina

Phone: 12345678

Email: abc@gmail.com

Notes:

Organization: Organization analysis is being done for:

< Back Next > Finish Cancel Help

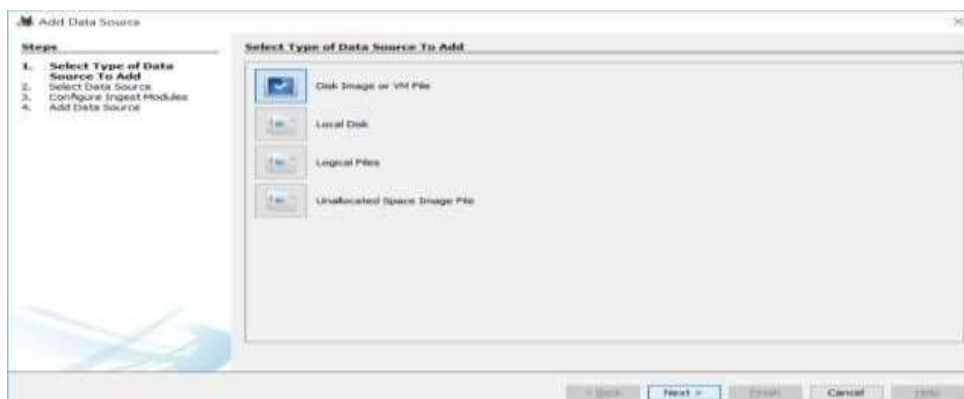


**Creating Case**

Creating case database...

Cancel

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



**Add Data Source**

**Steps**

1. **Select Type of Data Source To Add**
2. Select Data Source
3. Configure Ingest Modules
4. Add Data Source

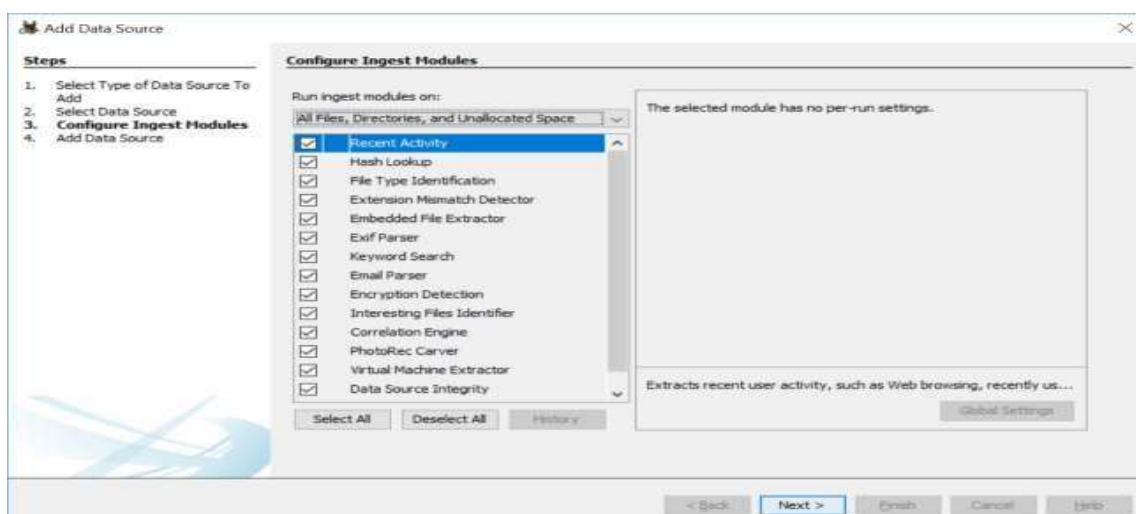
**Select Type of Data Source To Add**

- ☒ Disk Image or VM File
- ☐ Local Disk
- ☐ Logical Files
- ☐ Unallocated Space Image File

< Back Next > Finish Cancel Help

5. Select Data Source( here a previously made image file of a USB is selected) 6.

Select all ingest modules



**Add Data Source**

**Steps**

1. Select Type of Data Source To Add
2. Select Data Source
3. **Configure Ingest Modules**
4. Add Data Source

**Configure Ingest Modules**

Run ingest modules on: All Files, Directories, and Unallocated Space

- ☒ Recent Activity
- ☒ Hash Lookup
- ☒ File Type Identification
- ☒ Extension Mismatch Detector
- ☒ Embedded File Extractor
- ☒ Exif Parser
- ☒ Keyword Search
- ☒ Email Parser
- ☒ Encryption Detection
- ☒ Interesting Files Identifier
- ☒ Correlation Engine
- ☒ PhotoRec Carver
- ☒ Virtual Machine Extractor
- ☒ Data Source Integrity

Select All Deselect All History

The selected module has no per-run settings.

Extracts recent user activity, such as Web browsing, recently us...

Global Settings

< Back Next > Finish Cancel Help



**Steps**

1. Select Type of Data Source To Add
2. Select Data Source
3. Configure Import Modules
4. **Add Data Source**

**Add Data Source**

Processing data source and adding it to a local database. File analysis will start when this finishes.

10%

Status:  
Adding: \$OrphanFiles

\*This process may take some time for large data sources.

Back Next Cancel OK

Autopsy 4.10.0

File View Tools Window Help

Add Data Source Images/Video Communications Timeline Close Case Generate Report

Keyword List Keyword Search

Learning

Data Sources

Table 1 (Sorted)

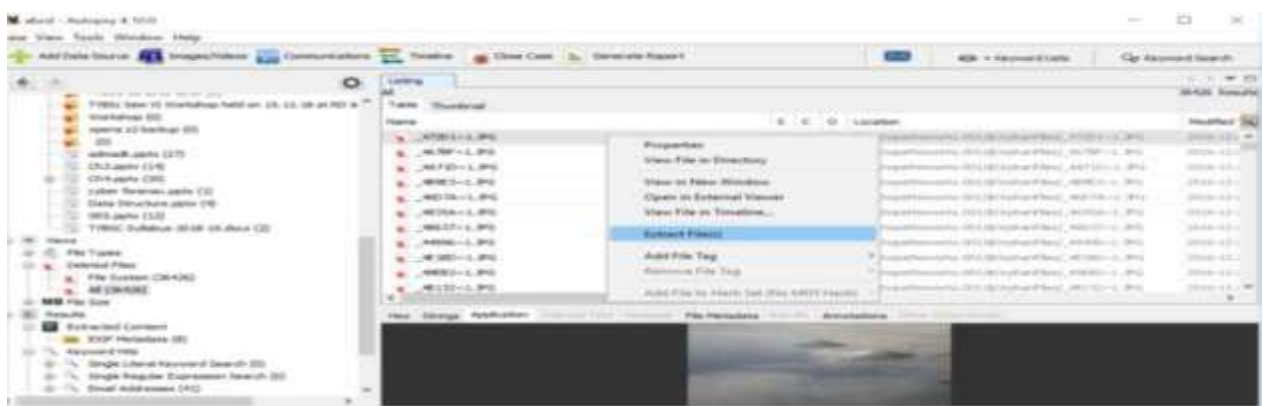
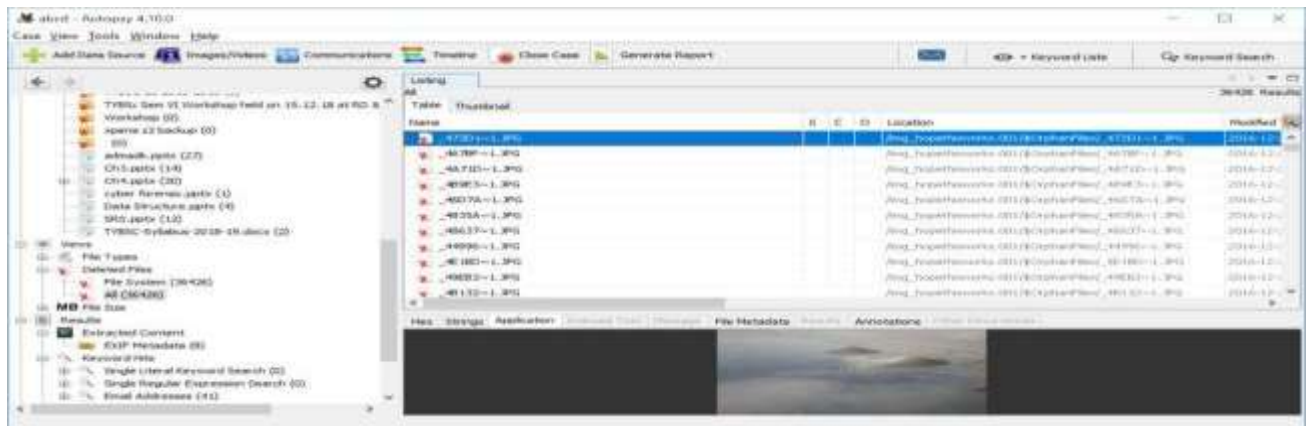
Name	Type	Size (Bytes)	Sector Size (Bytes)	Timestamp	Device ID
hoperhworks.001	Image	322,028,960	4096	Aug 27, 2014 14:16	947076c3-9090-4c08-b09f-79a3a7630a3c

File Sources | Extracted Files | Metadata | File Previews | Results | Examinations | (2000 Images Loaded)

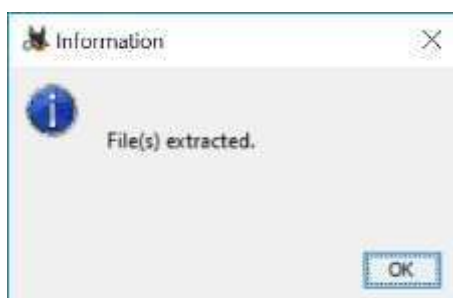
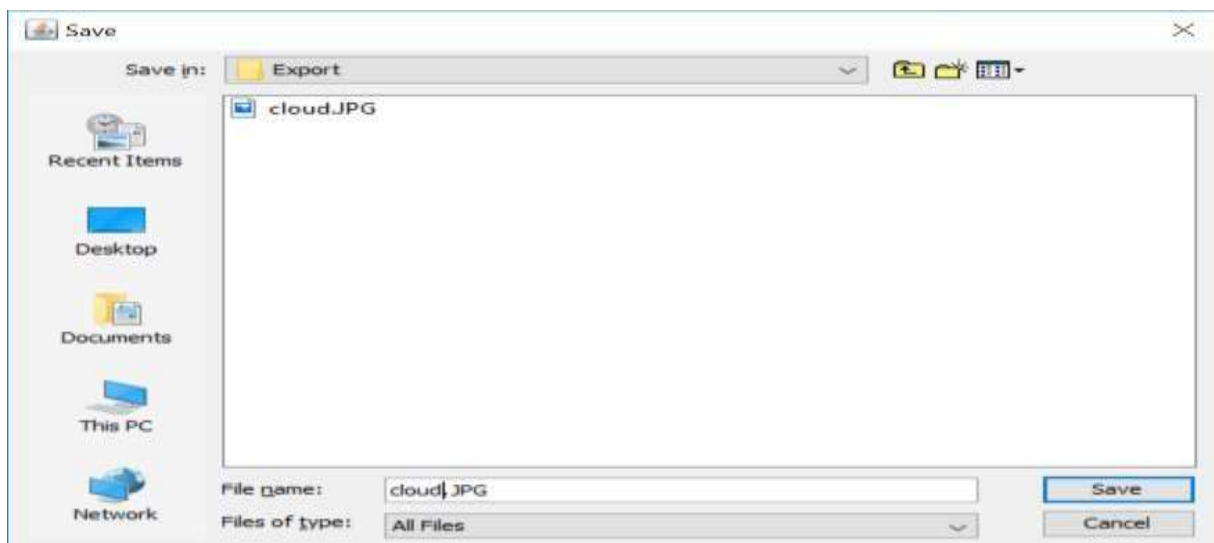
Analyzing files from hoperhworks.001

[illegible]

- 15

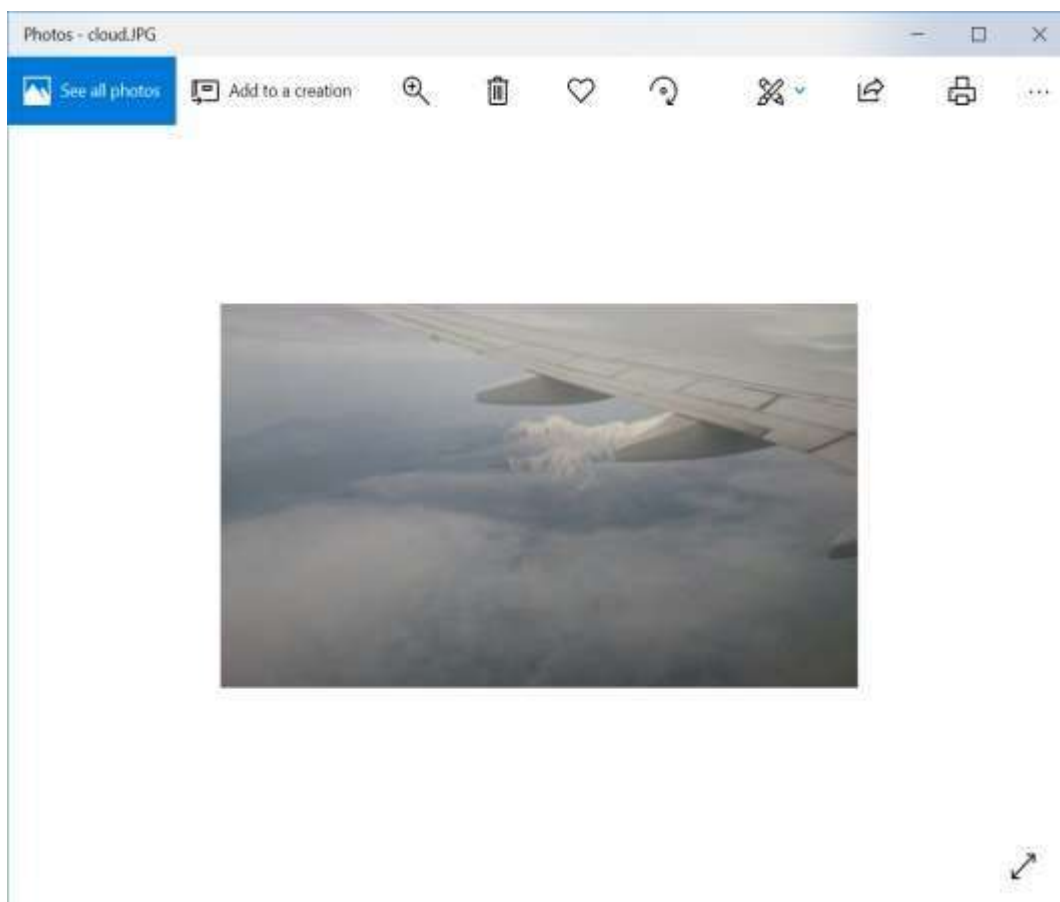
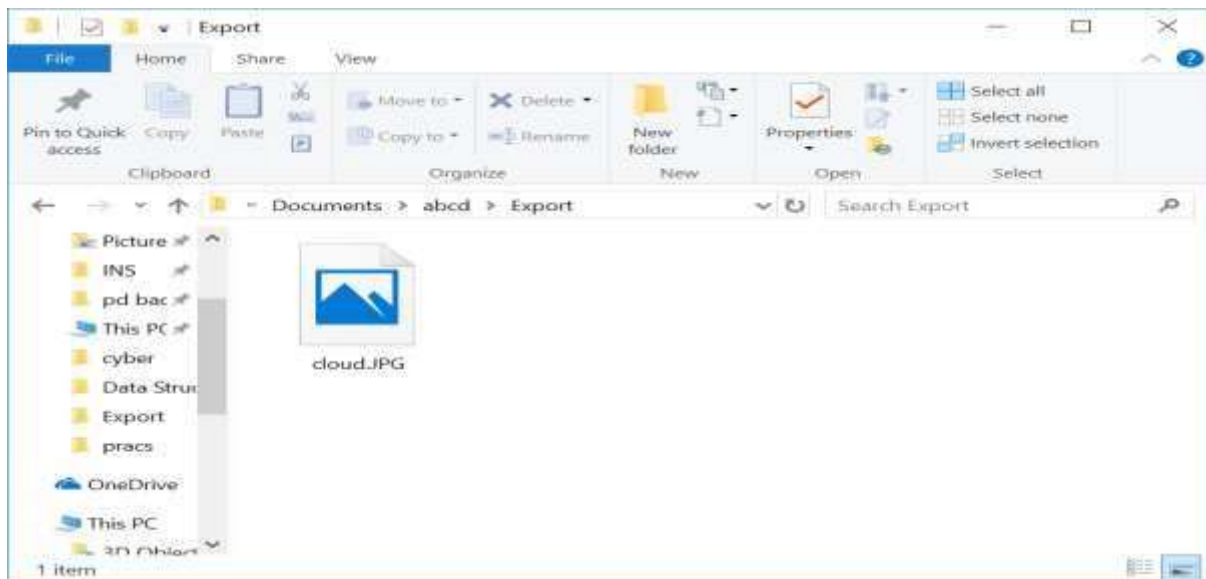


10. By default Export folder is choose to save the recovered file.

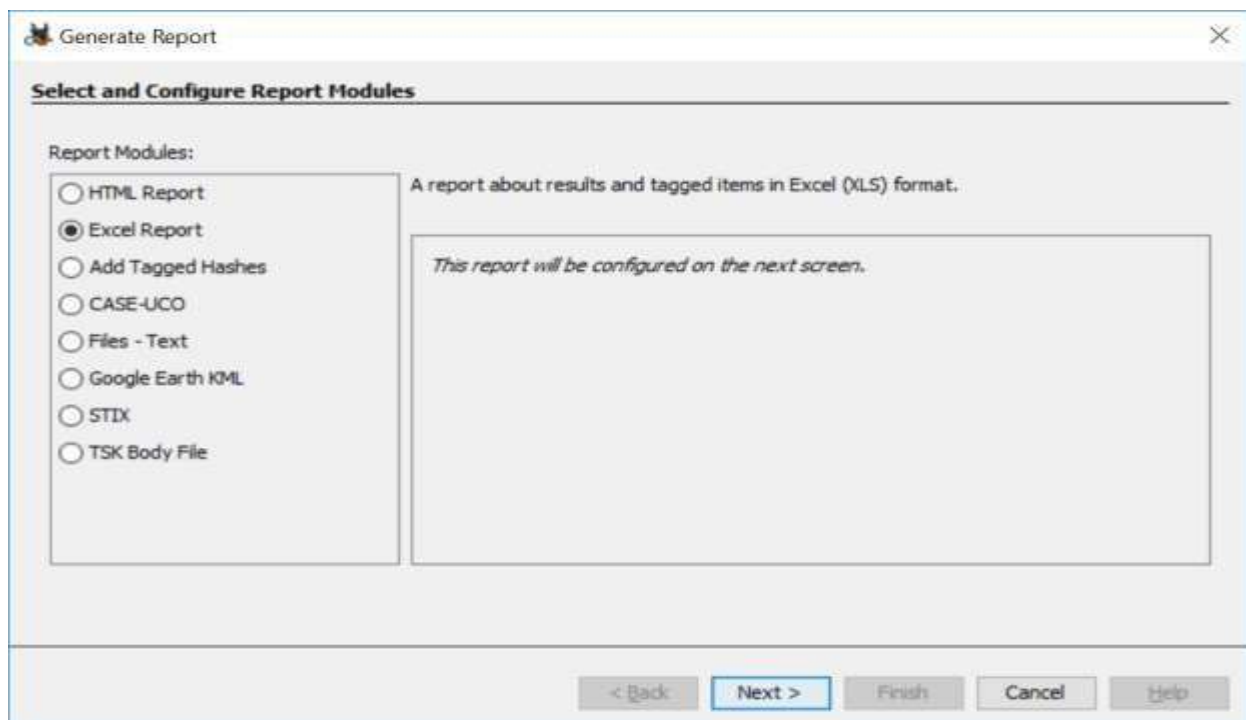
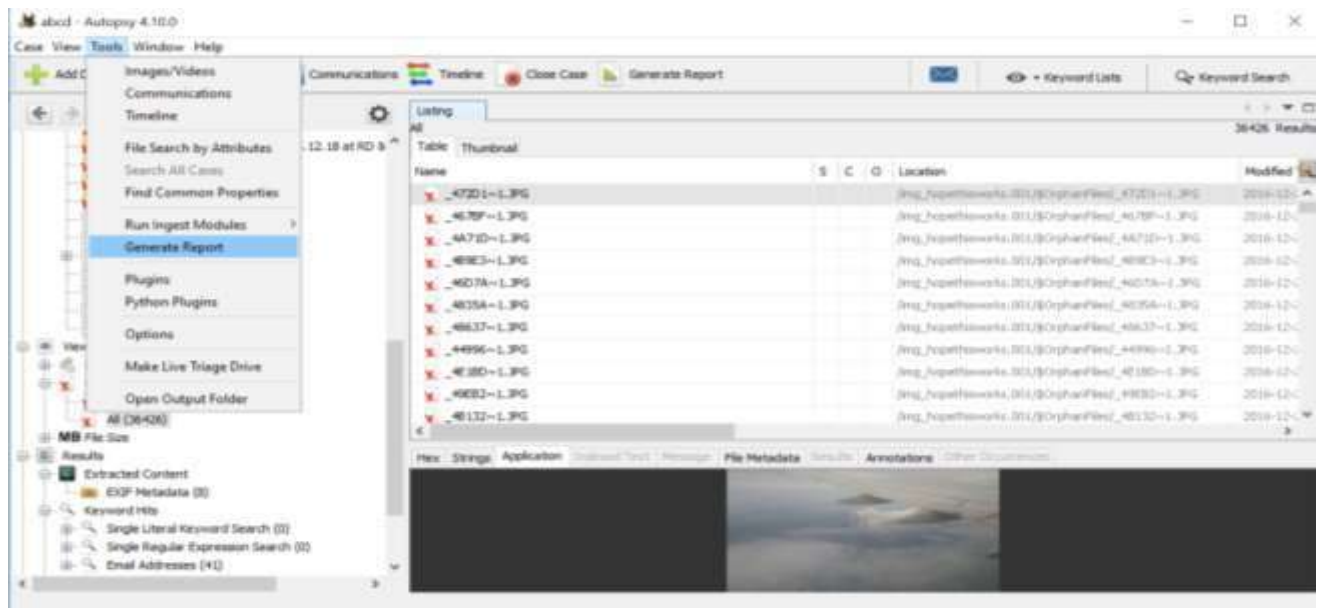




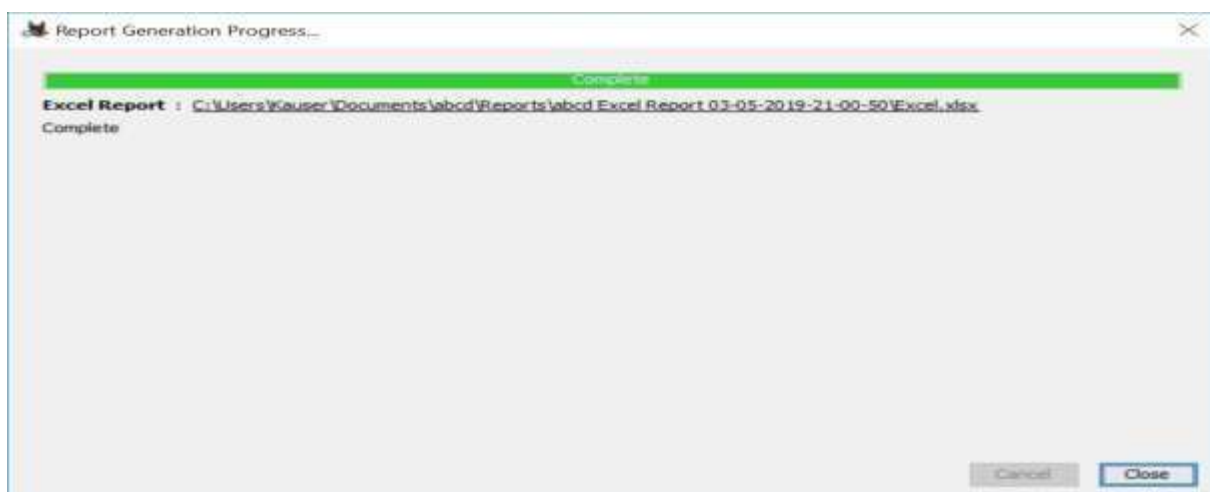
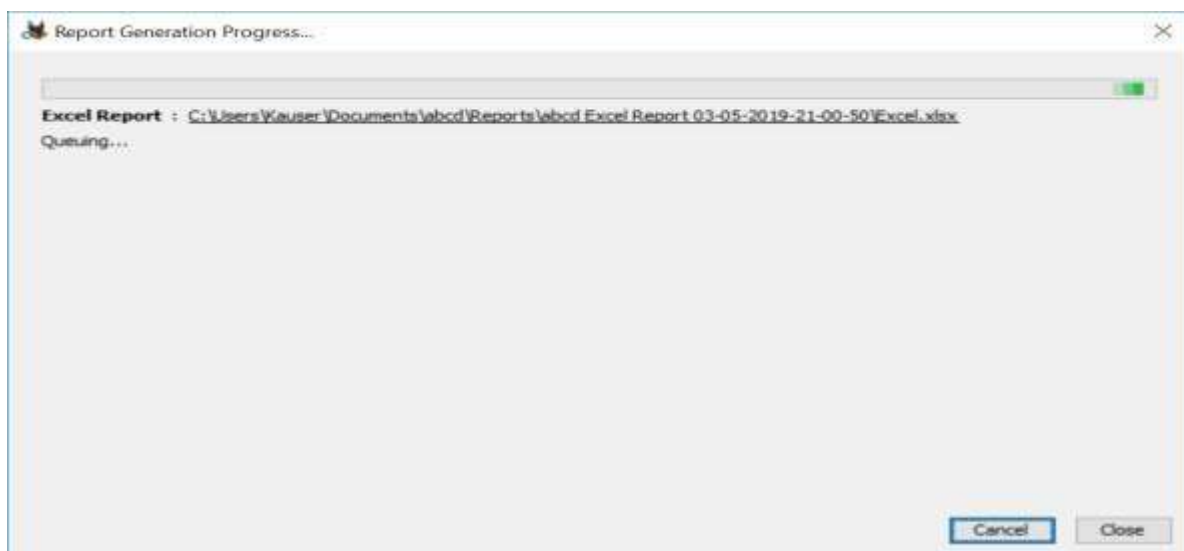
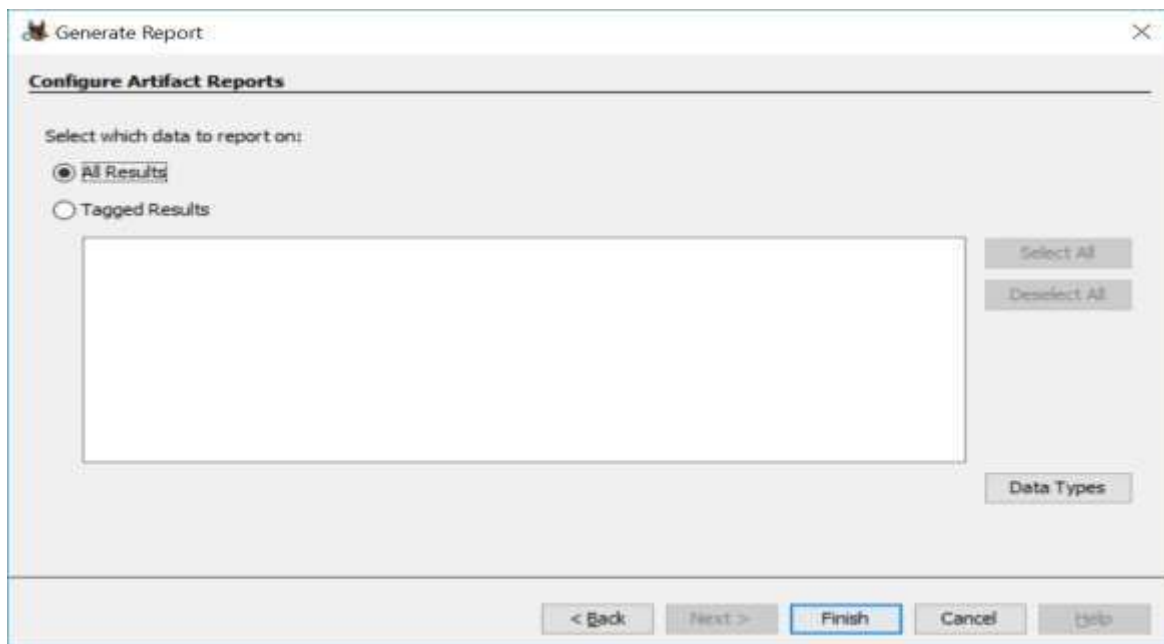
11. Now go to the Export Folder to view Recover file.



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

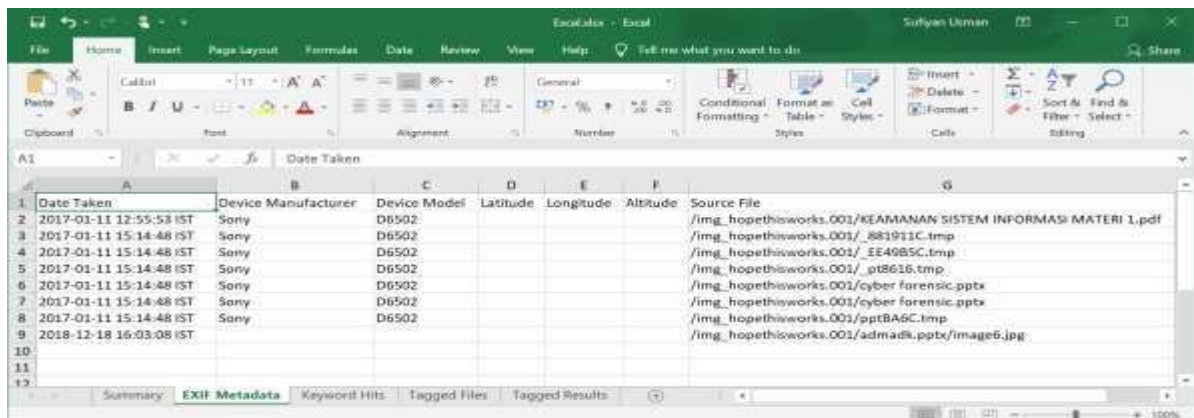
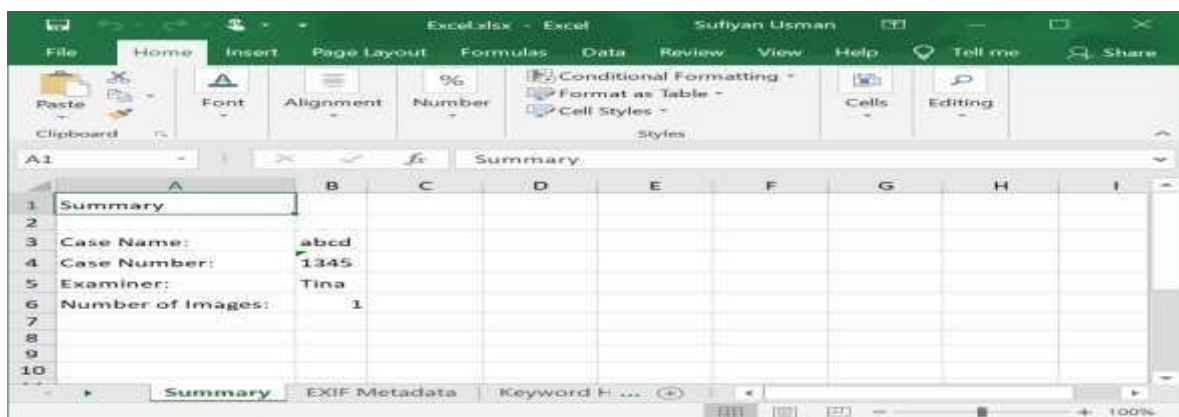
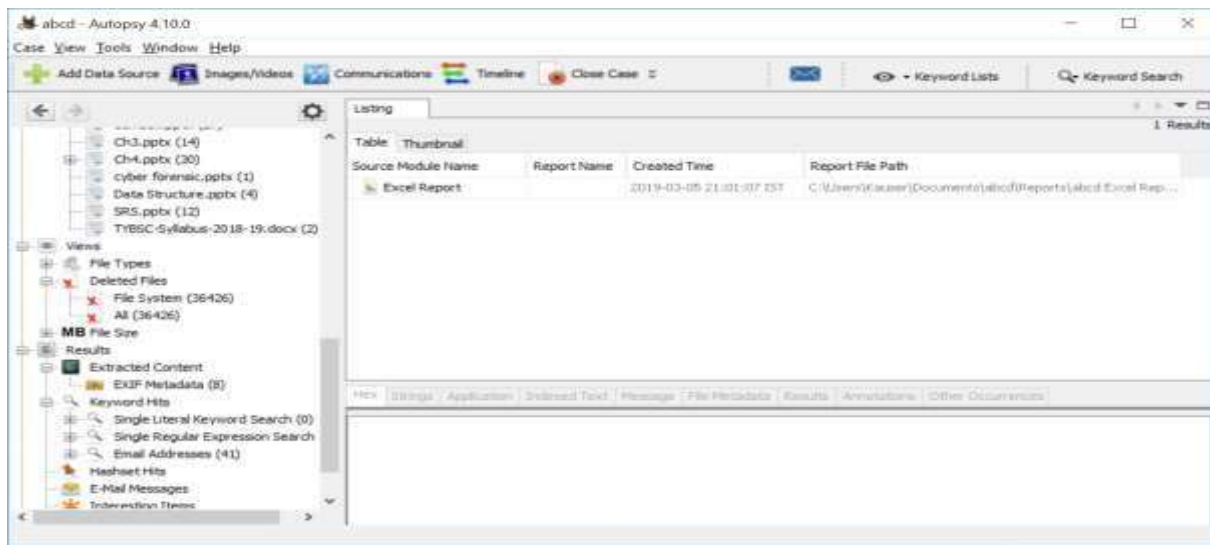


13. Click Finish after selecting All Results



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



**Conclusion:** The above program has been executed successfully

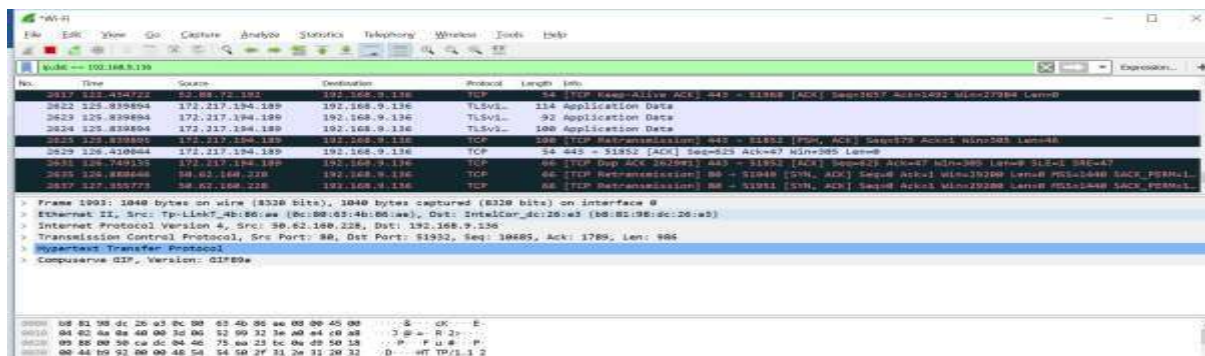
## PRACTICAL NO 4

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

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

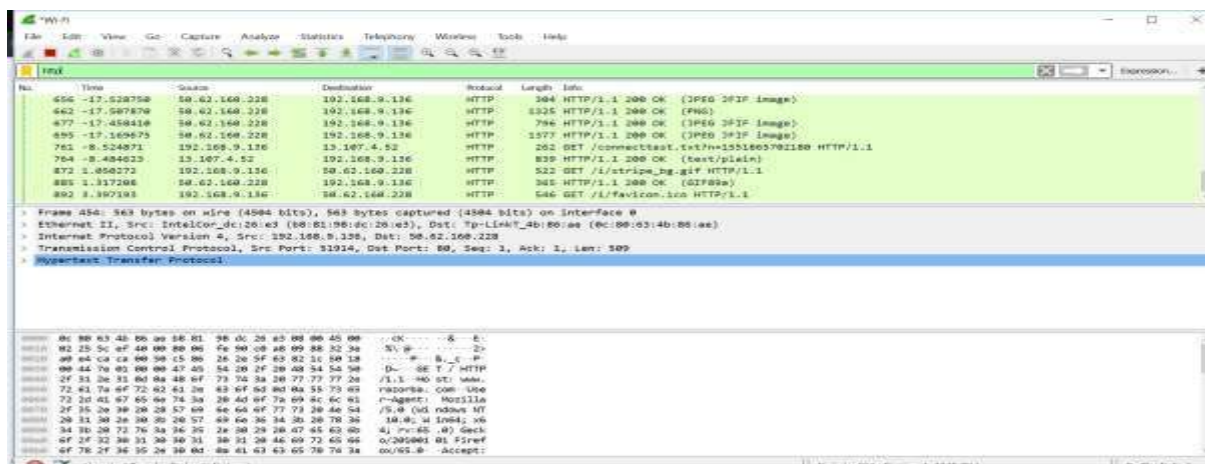
#### Steps:

1. Open Wireshark and click on Ethernet.

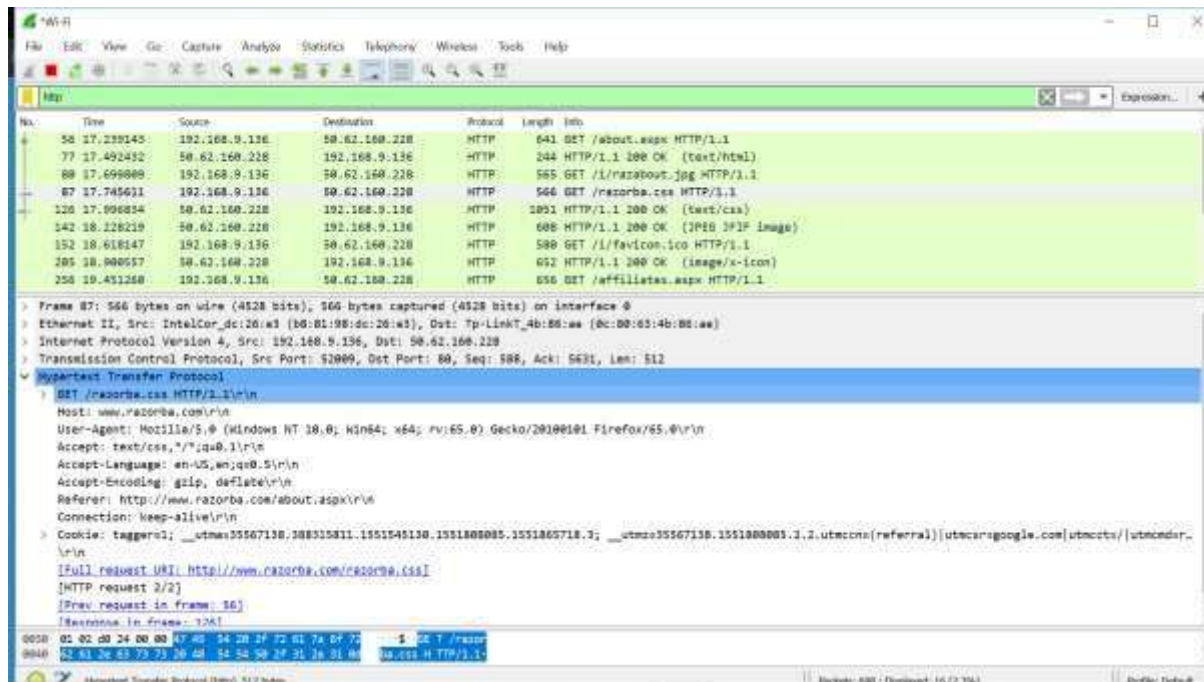


2. Now go on browser and open any unsecured website i.e www.razorba.com and perform some activity on the website.

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



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



**Conclusion:** The above program has been executed successfully.



## PRACTICAL NO 5

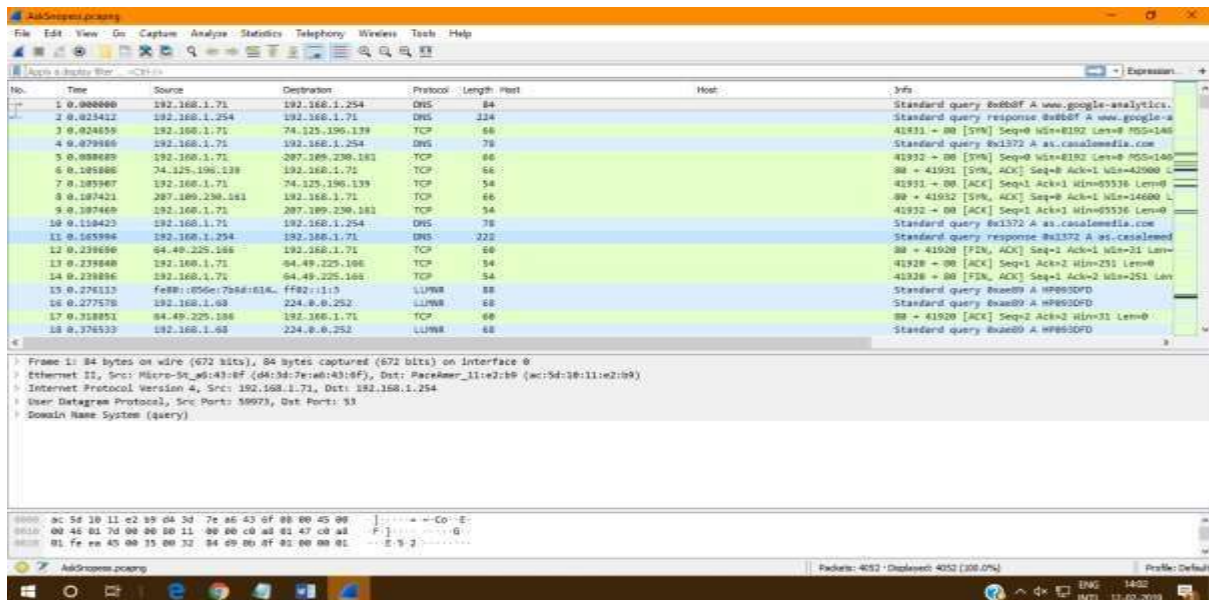
**Aim:** Analyze the packets provided in lab and solve the questions using Wireshark:

- What web server software is used by [www.snopes.com](http://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:**

- What web server software is used by [www.snopes.com](http://www.snopes.com)?

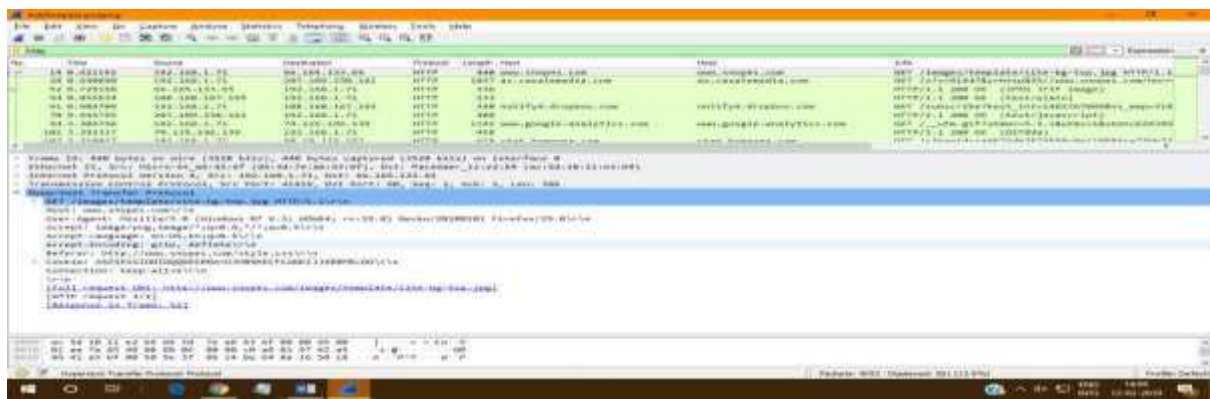
1. Open the AskSnopess file



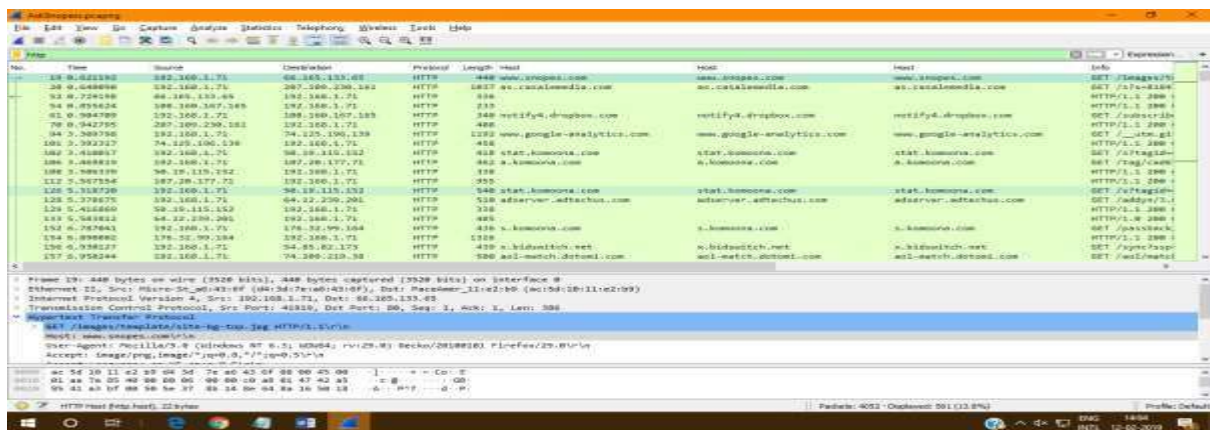
2. In the display filter type http.



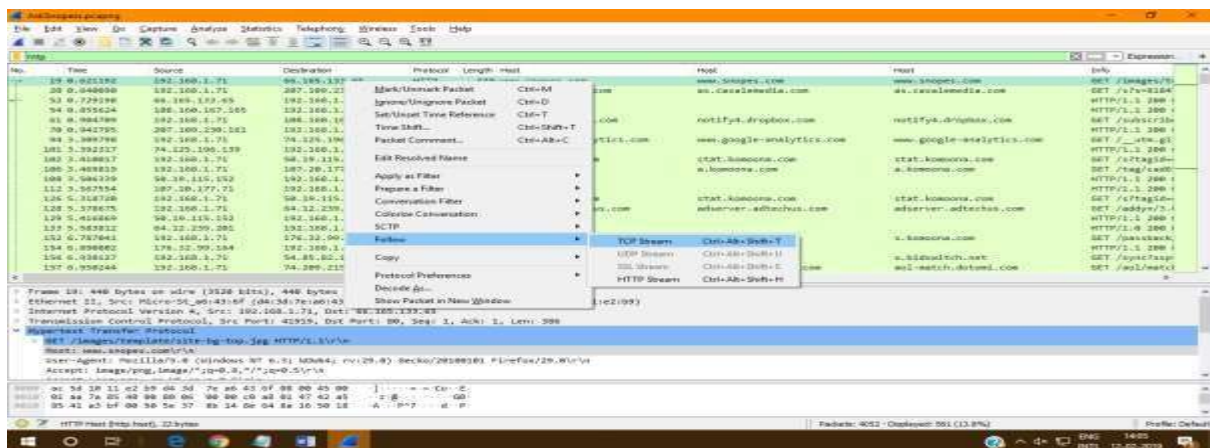
3. In the second panel expand the hypertext transfer protocol.



4. Click on the host name > right click> Apply as column

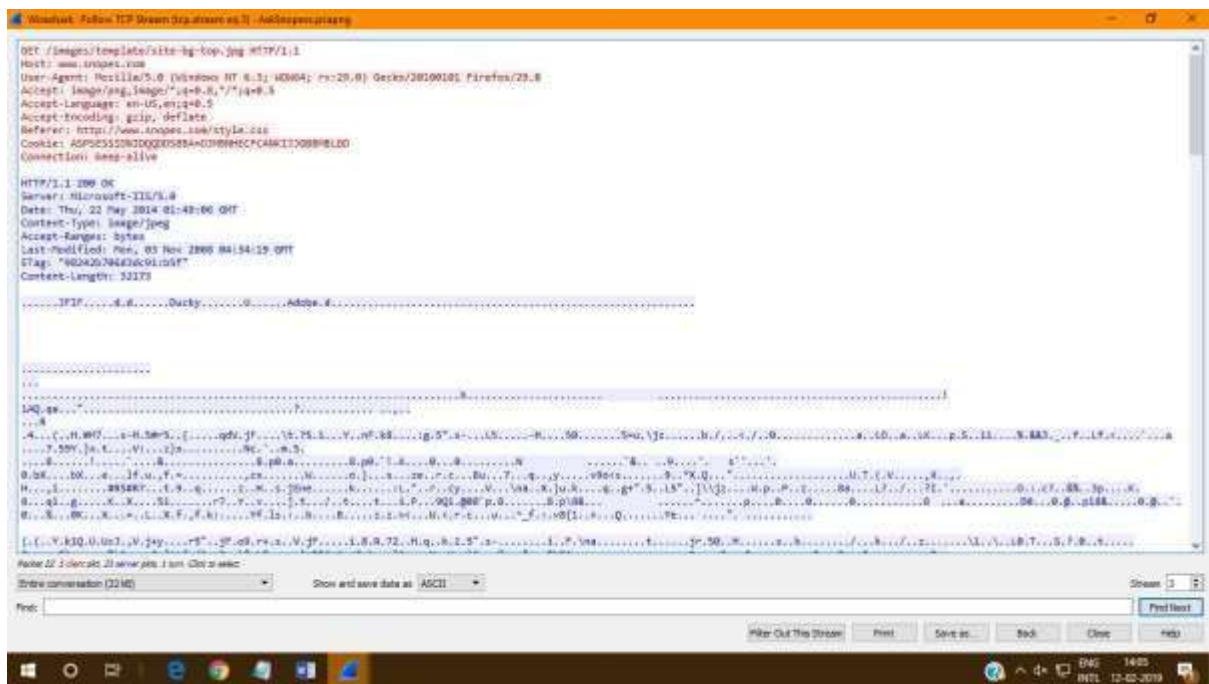


5. Click any of the http packet > right click> Follow> TCP Stream

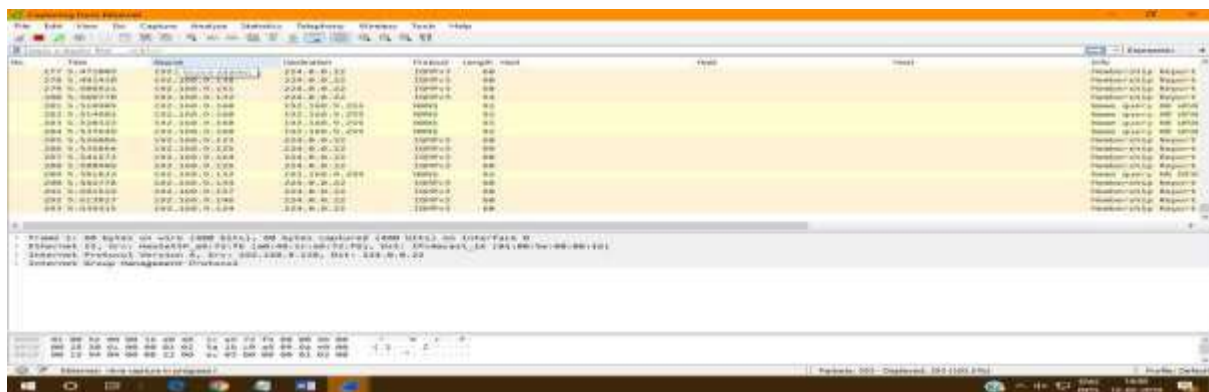


6. The webserver is Microsoft IIS/5.0

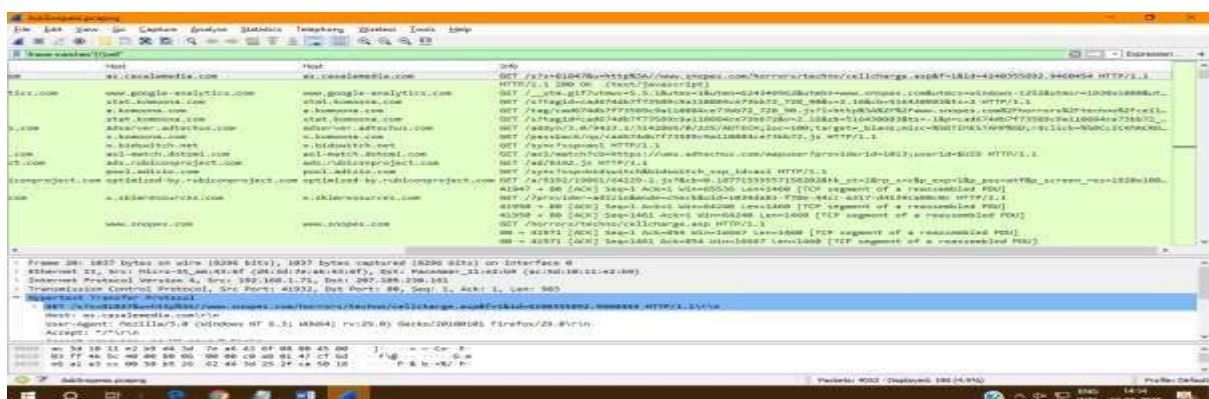
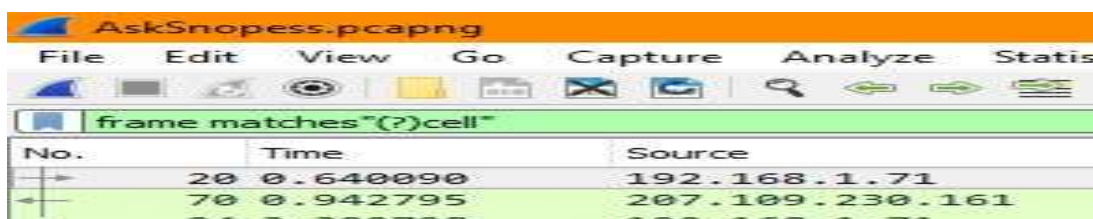




➤ About what cell phone problem is the client concerned?



1. In the display filter type frame matches"(?)cell".



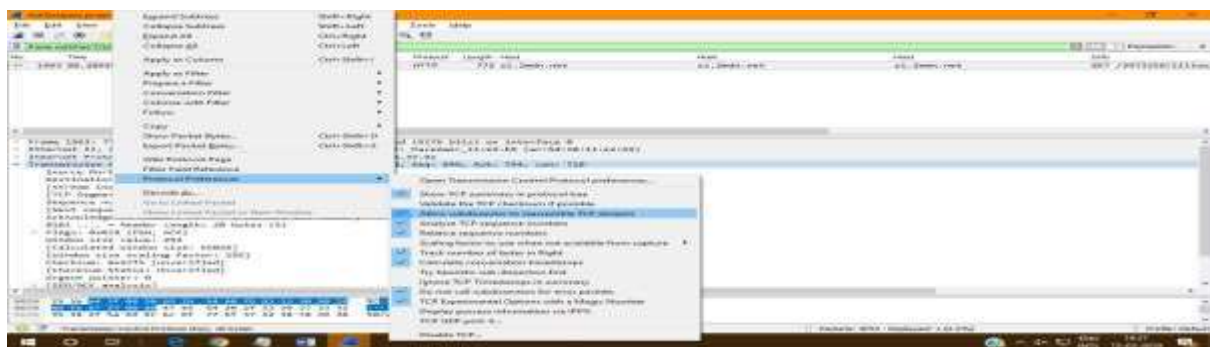
➤ According to Zillow, what instrument will Ryan learn to play?

1. In the display filter type frame matches"(?)zillow".

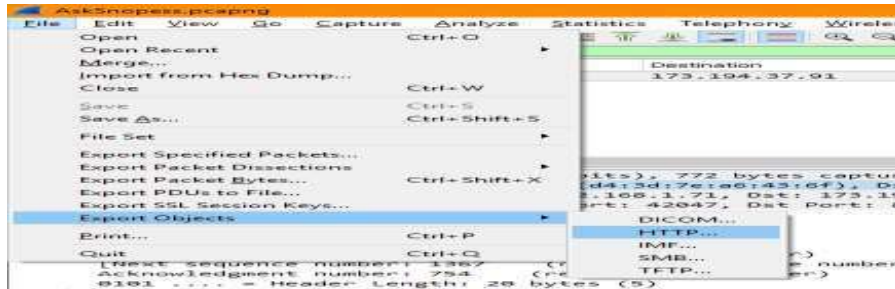


2. In the second tab expand the transmission control protocol.

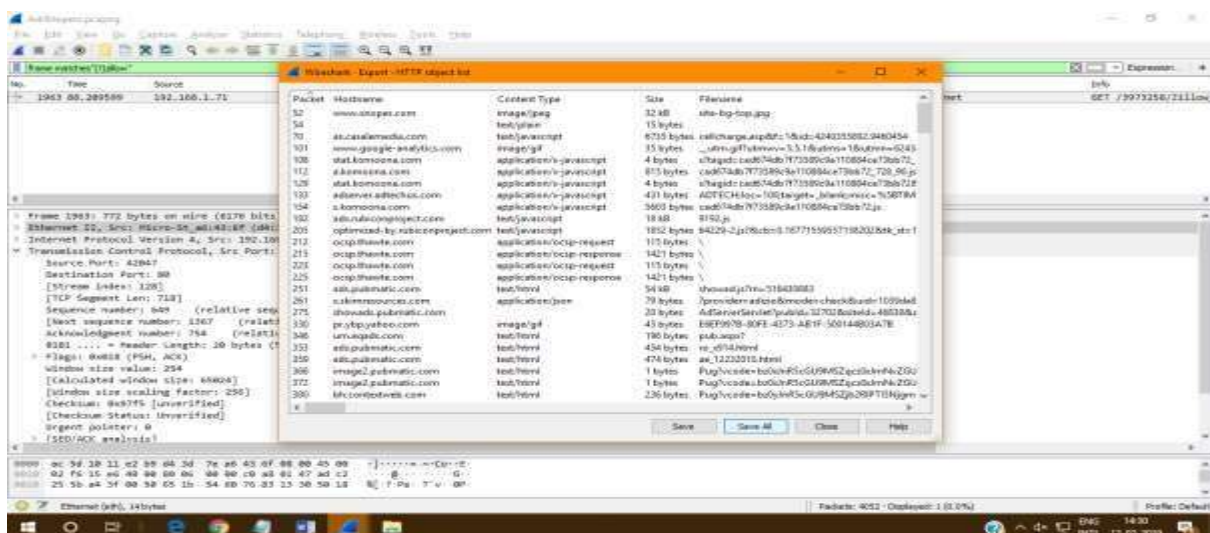
Right click on transmission control protocol > Protocol Preferences > Allow subdissector to reassemble TCP stream.



3. Click on file > Export objects > HTTP.



4. Click on Save all.

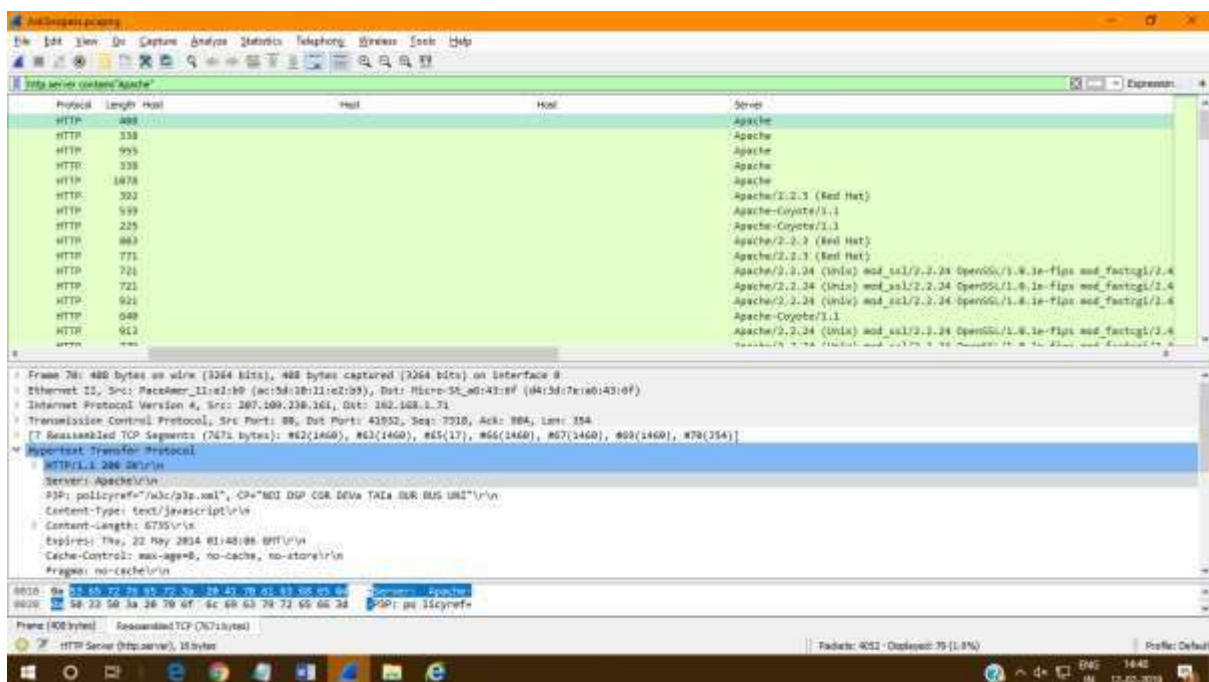
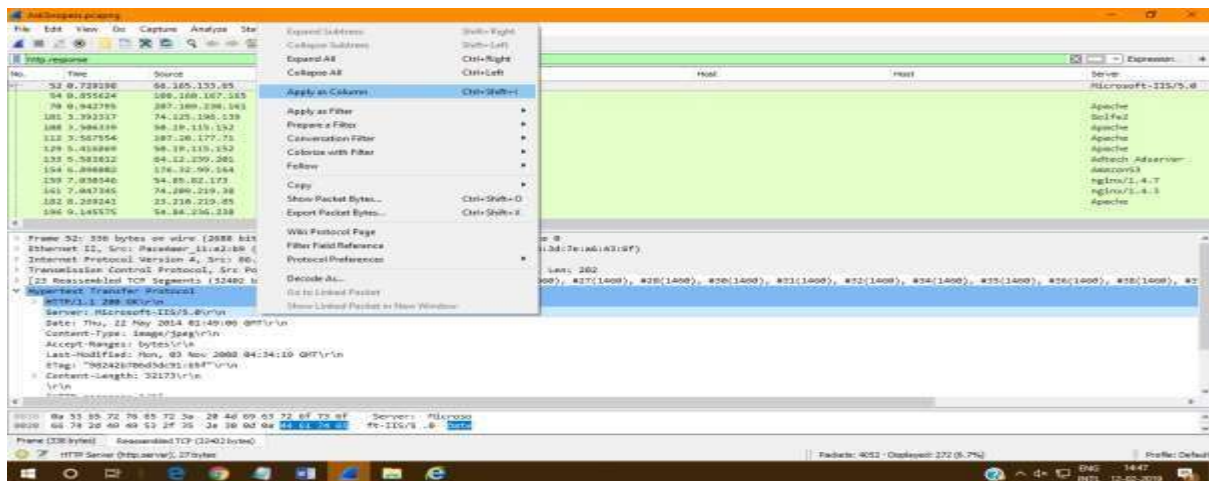


- Run the saved file and you will get the result.



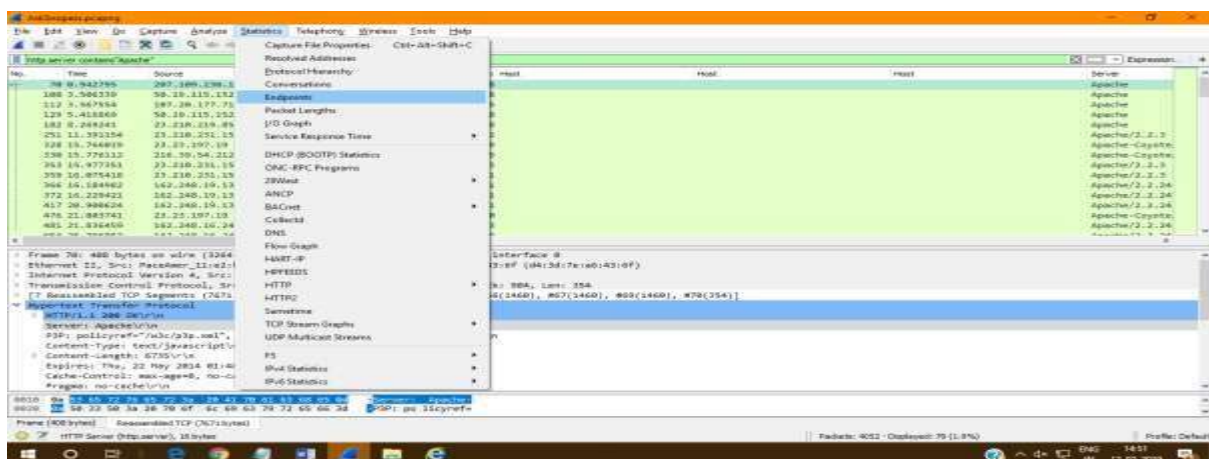
- How many web servers are running Apache?

- Right click on HTTP > Apply as column.

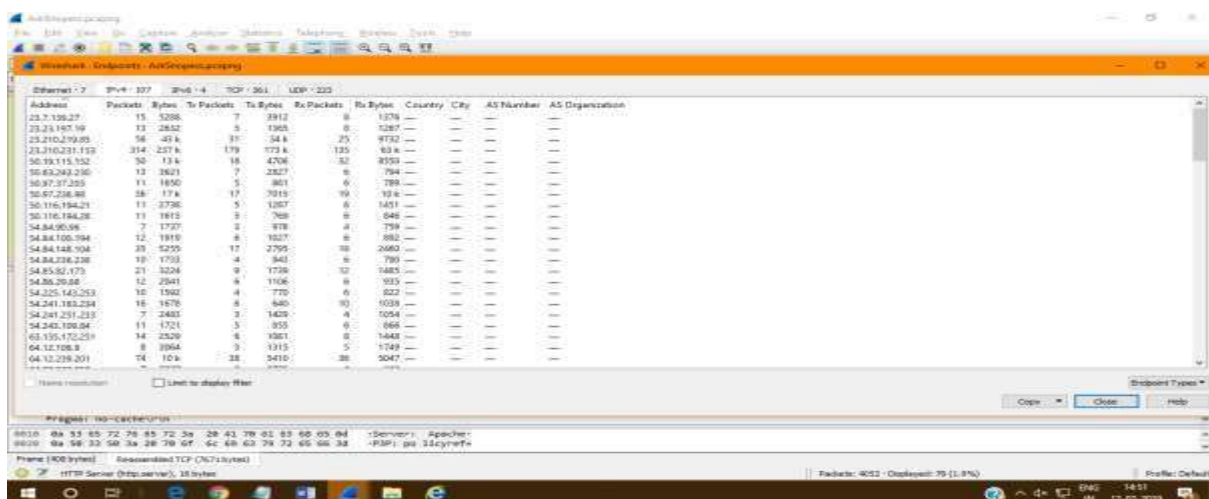




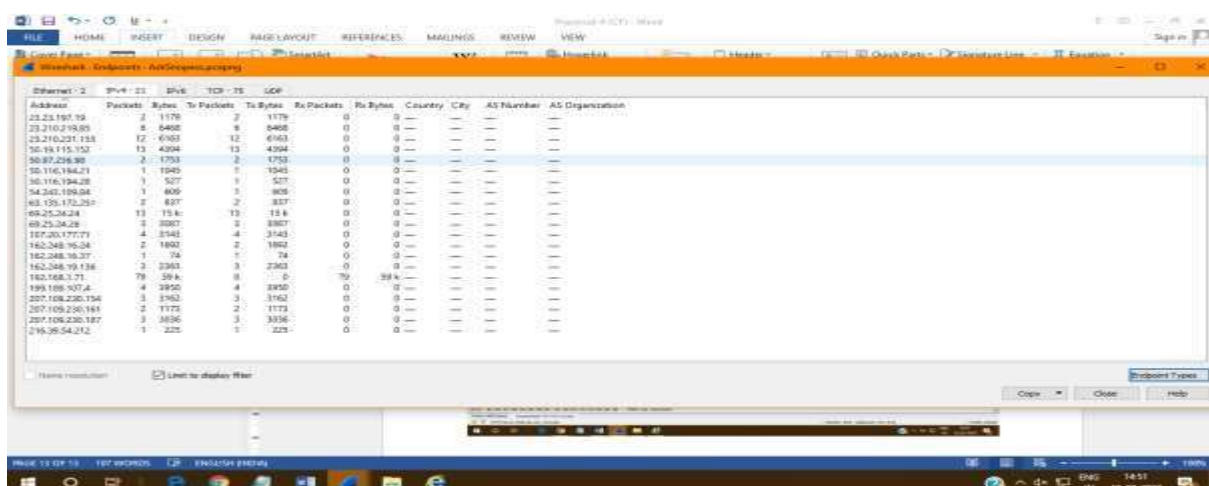
## 2. Click on Statistics > Endpoints.



## 3. Click the check box.

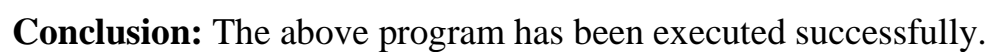


## 4. Beside IPv4 the number 21 shows that there are 21 web servers running on apache.



➤ What hosts (IP addresses) think that jokes are more entertaining when they are explained?

## 1. In the display filter type frame matches "(?)jokes".



## 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

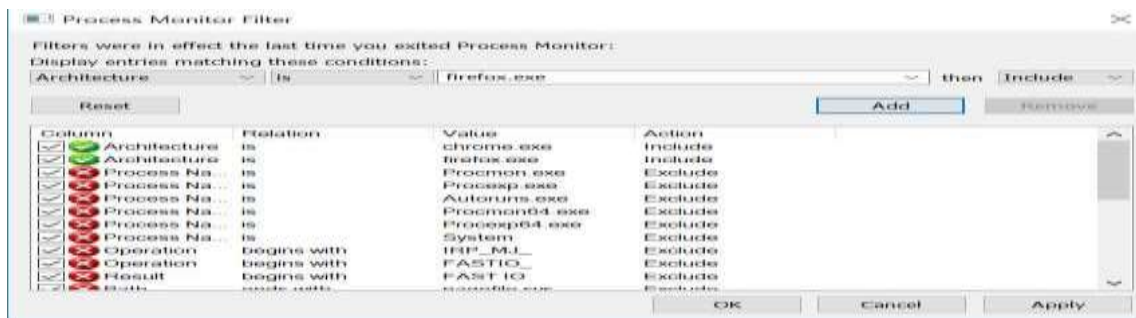
The following are the categories of Sysinternals Tools:

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

2) Monitor Live Processes (Tool: ProcMon)



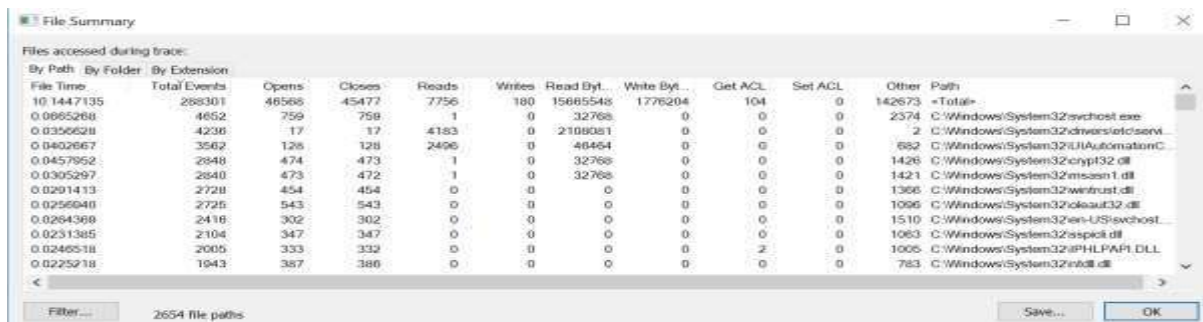
Click on filter > Process monitor filter



Click on tools > Process tree

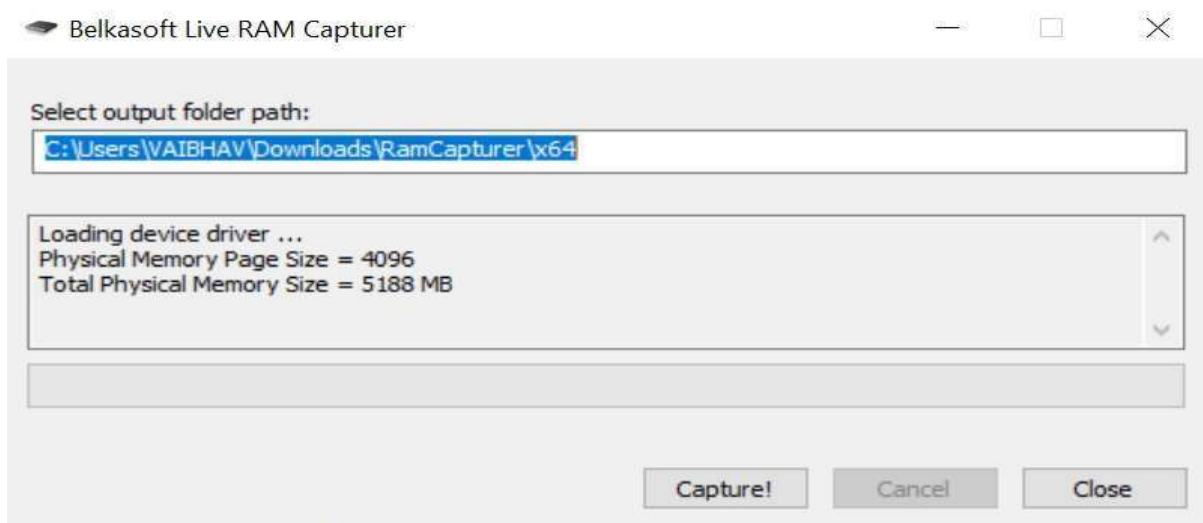


Click on filter > File summary



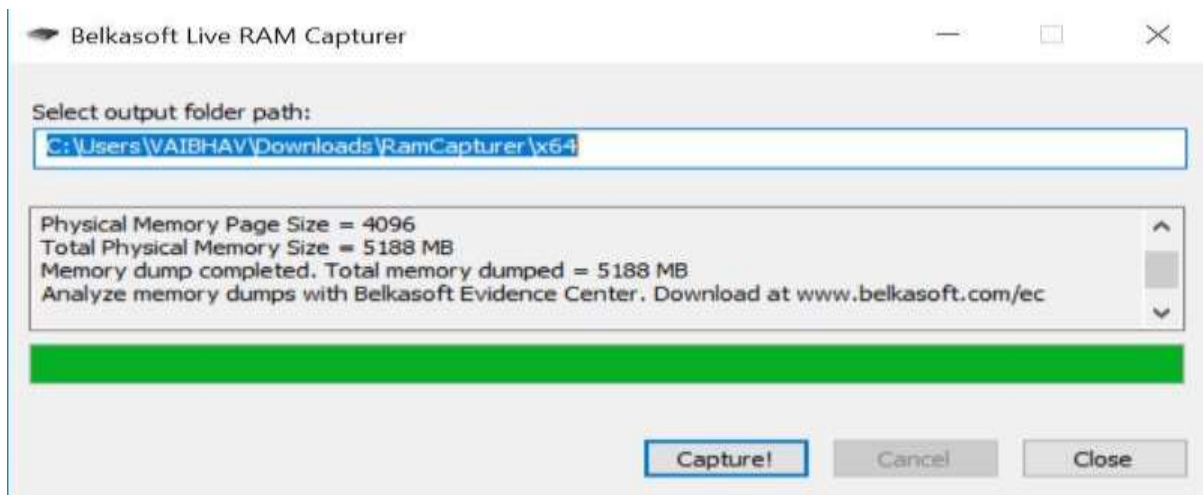
### 3) Capture RAM (Tool: RAMCapture)

Open the Ramcapture tool.

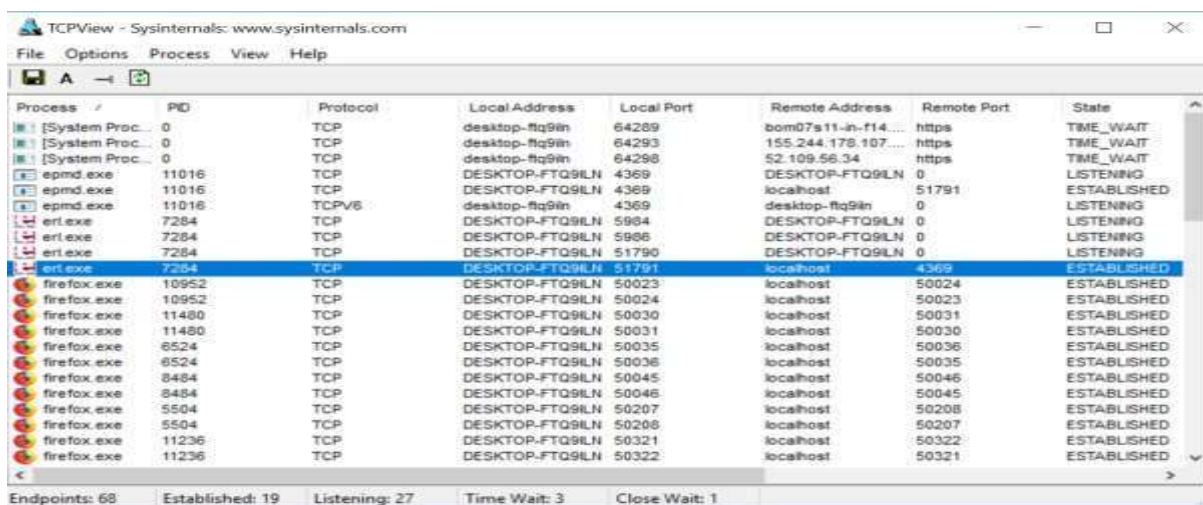


Click on capture.

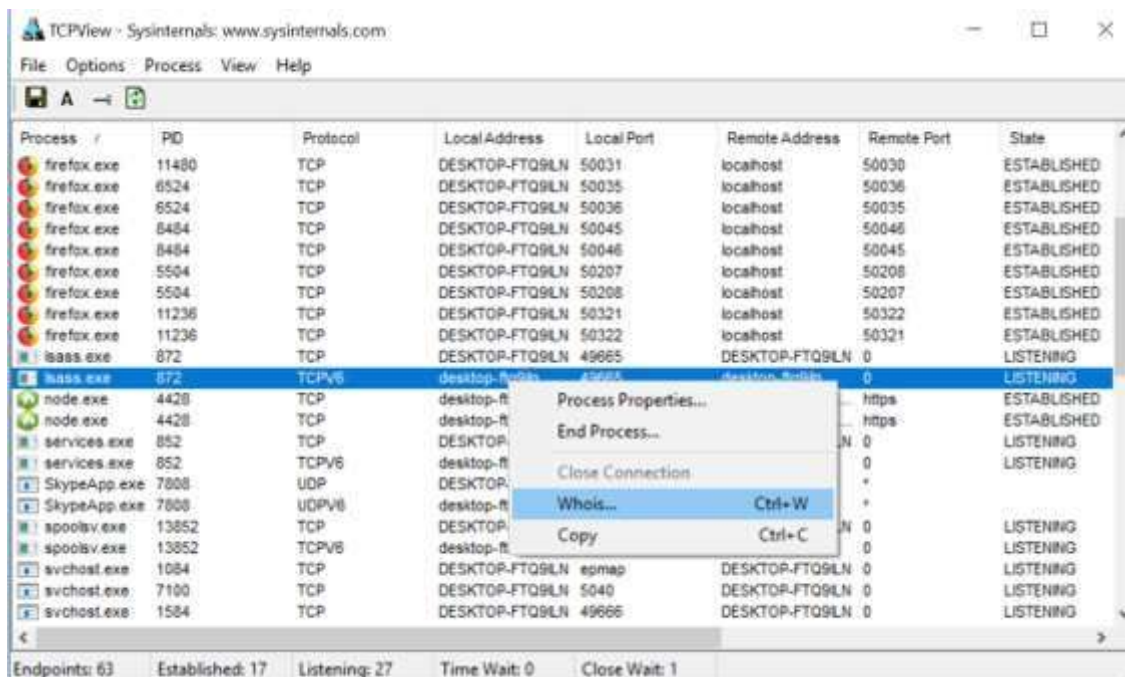




4) Capture TCP/UDP packets (Tool: TcpView) Open the Tcpview tool.



Right click on any packet > whois

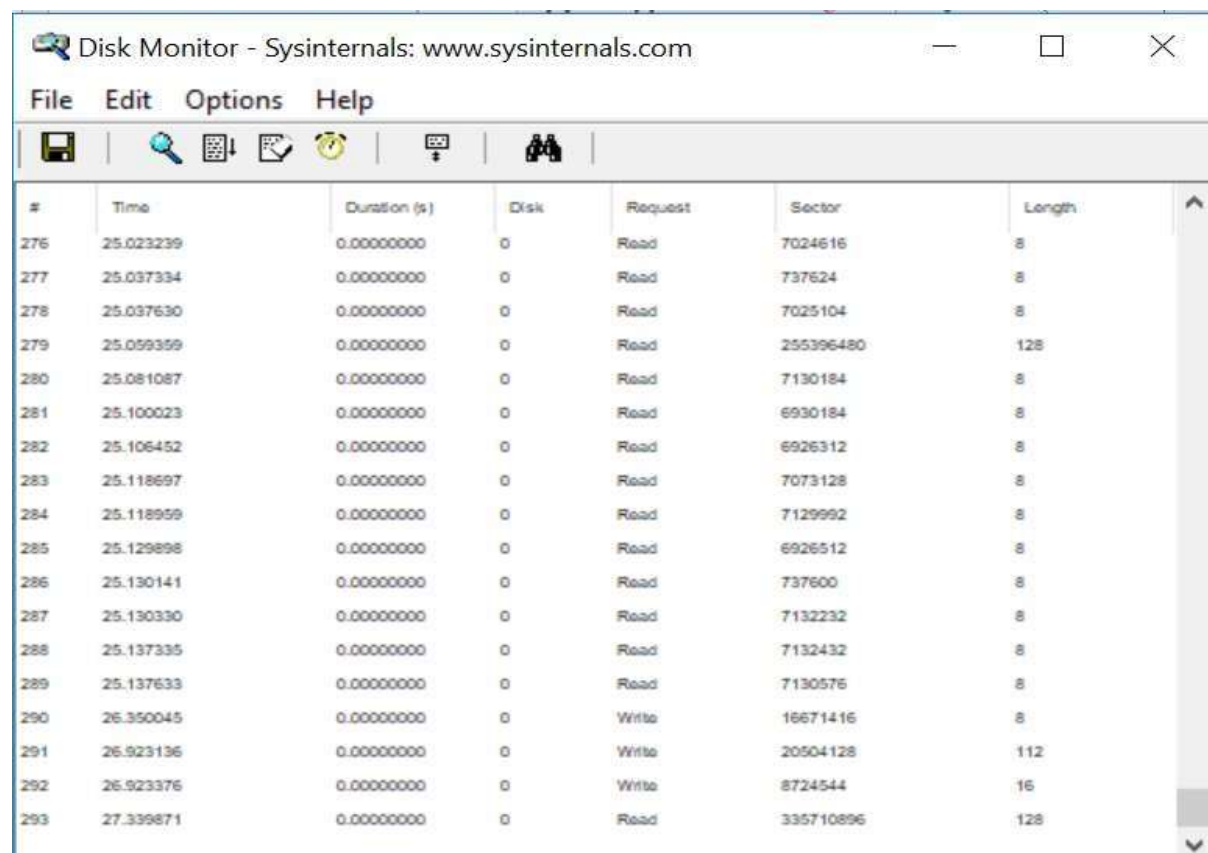




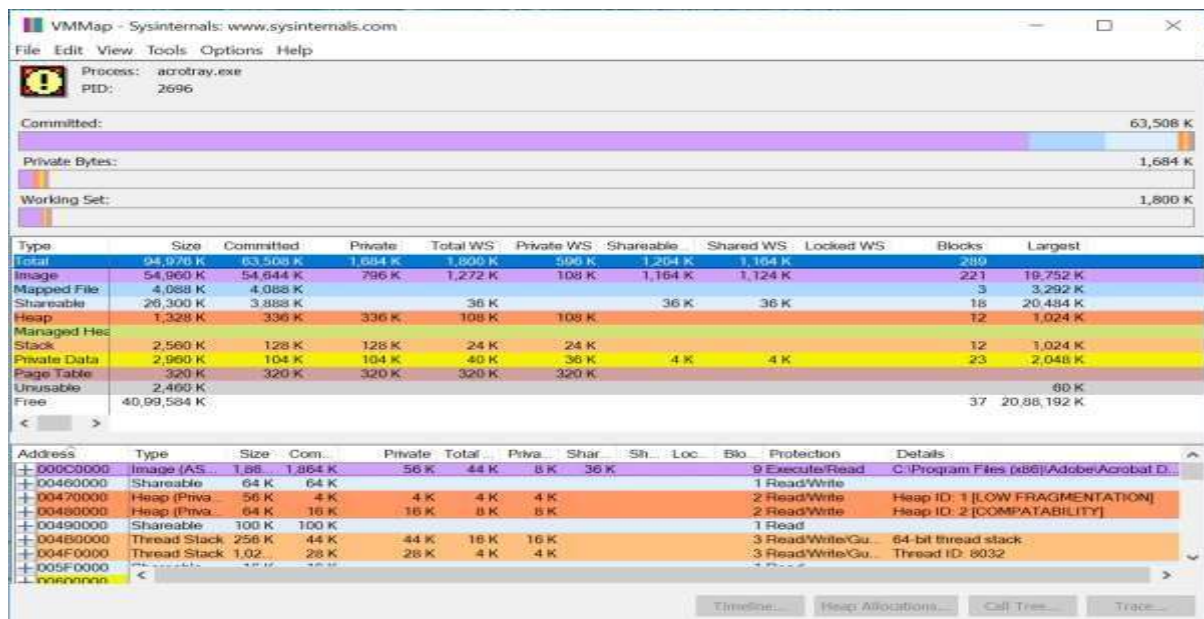


### 5) Monitor Hard Disk (Tool: DiskMon)

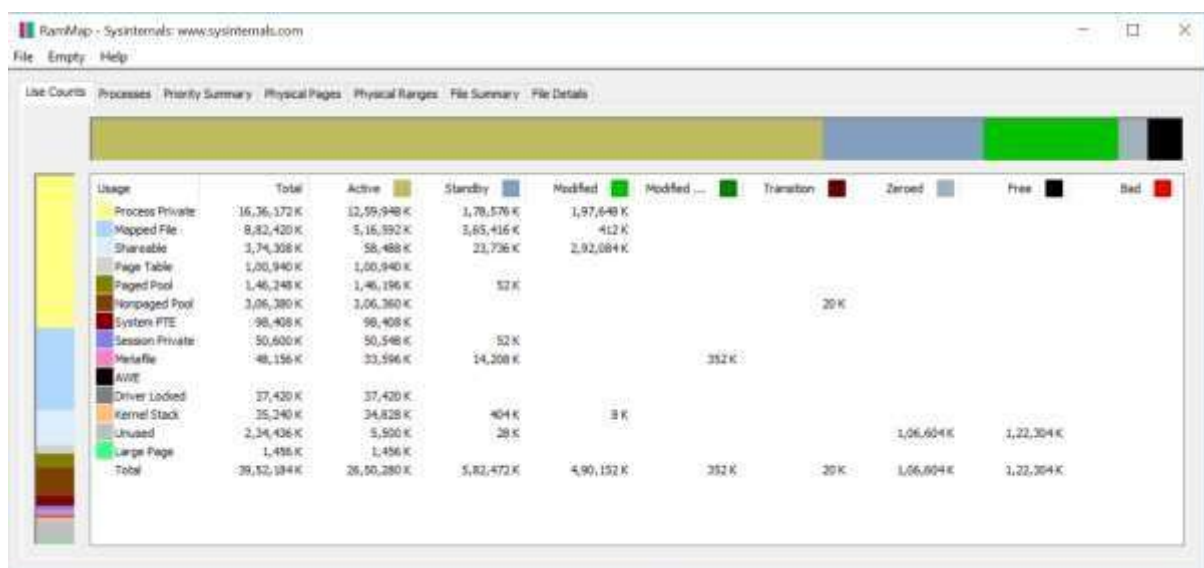
Open the Diskmon tool.



6) Monitor Virtual Memory (Tool:  
VMMMap) Open the VMMMap tool.



7) Monitor Cache Memory (Tool:  
RAMMap) Open the RAMMap tool.



**Conclusion:** The above program has been executed successfully.

## PRACTICAL NO 7

**Aim: Recovering and Inspecting deleted files**

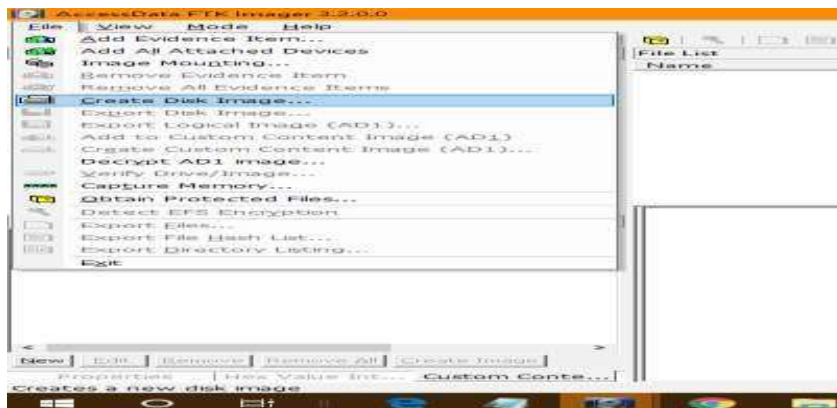
**-Check for Deleted Files**

**-Recover the Deleted Files**

**-Analyzing and Inspecting the recovered files**

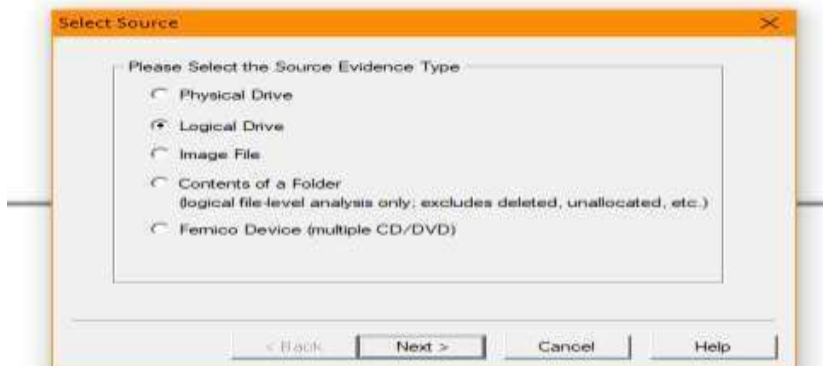
**Steps:**

1. Open AccessData FTK Imager. Click on File > Create Disk Image.

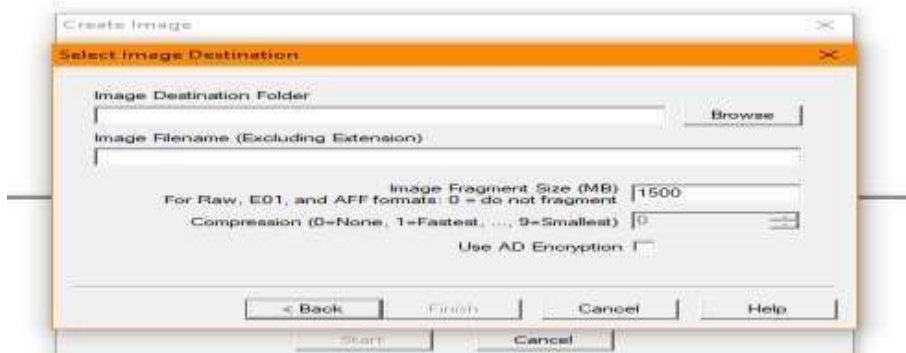


2. Type the destination path.

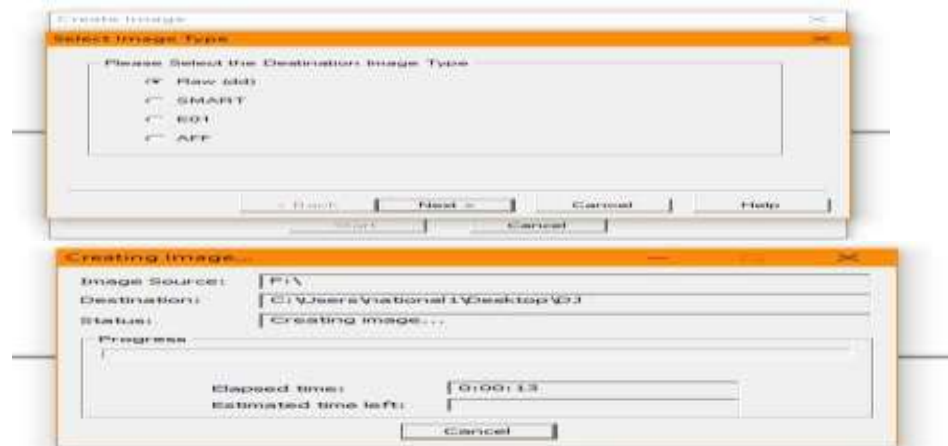
3. Click on Logical drive.



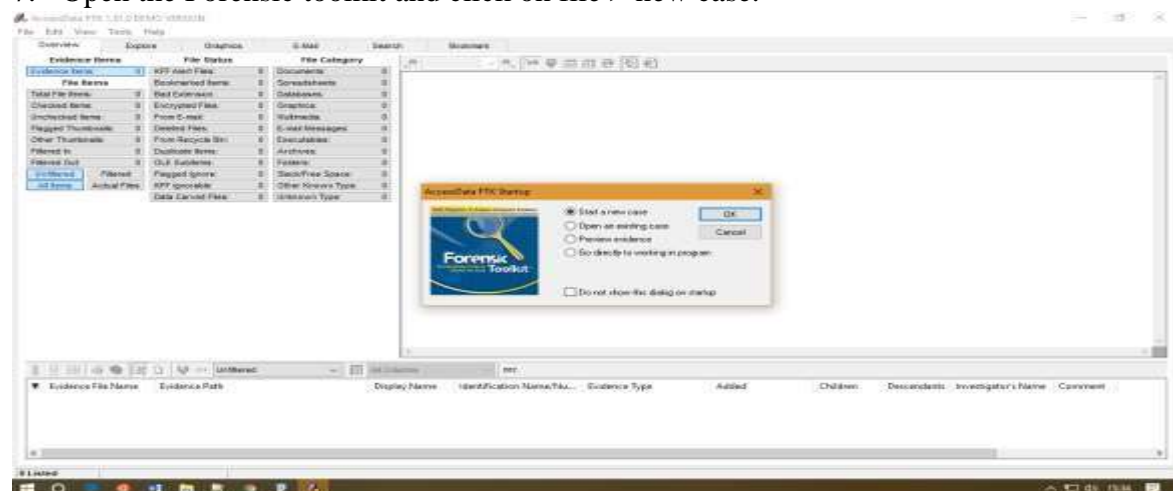
4. Click on Add > Browse.



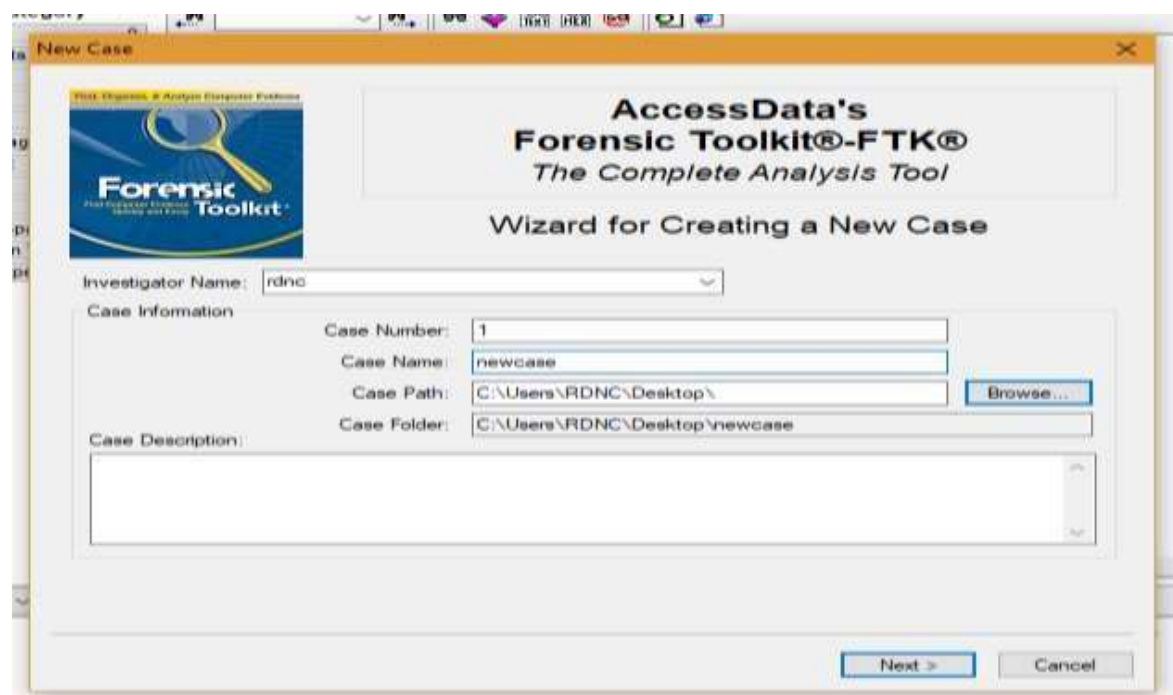
5. Select the type of data format and click next.



7. Open the Forensic toolkit and click on file > new case.

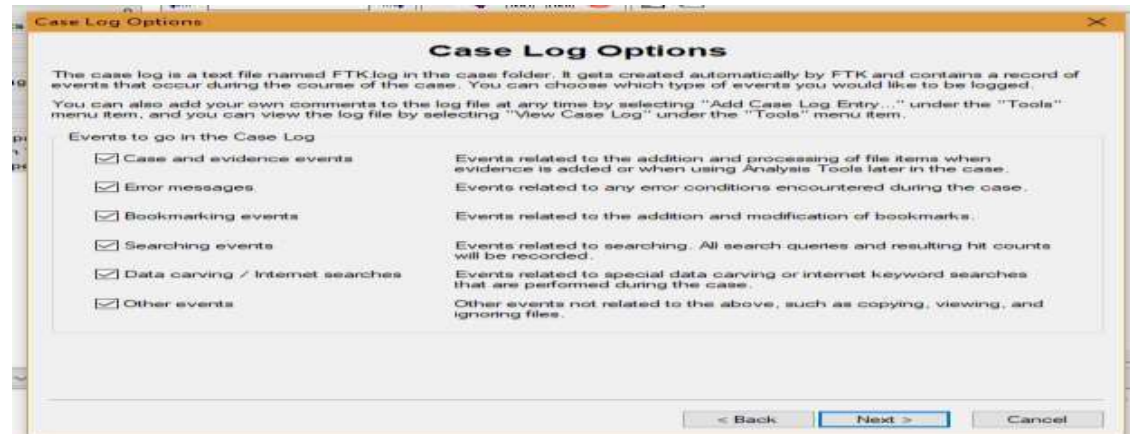


8. Enter the details and click on next.

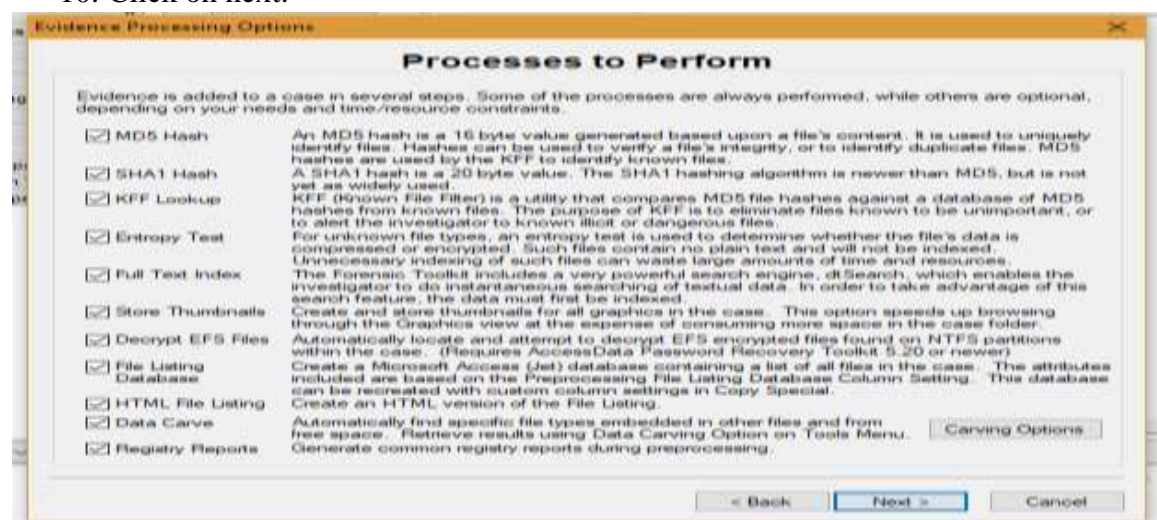




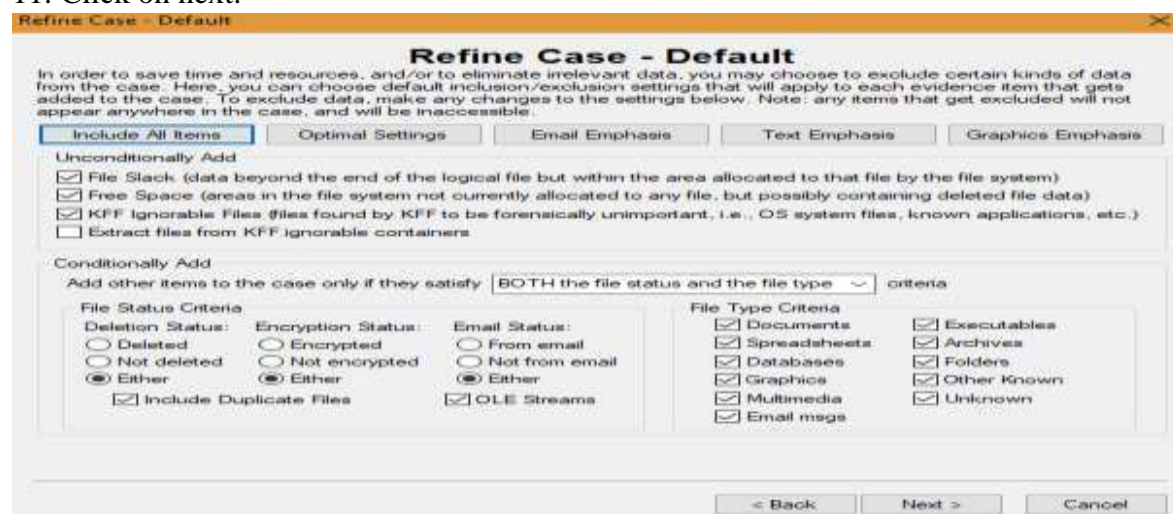
## 9. Click on next.



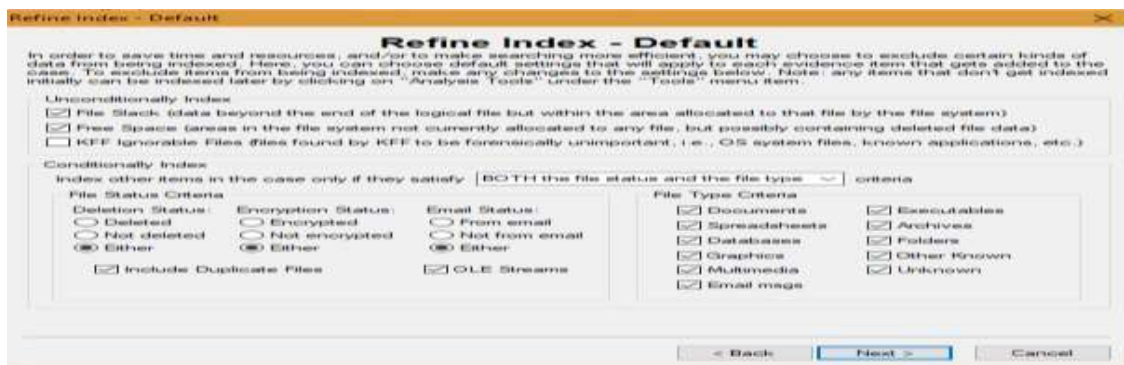
## 10. Click on next.



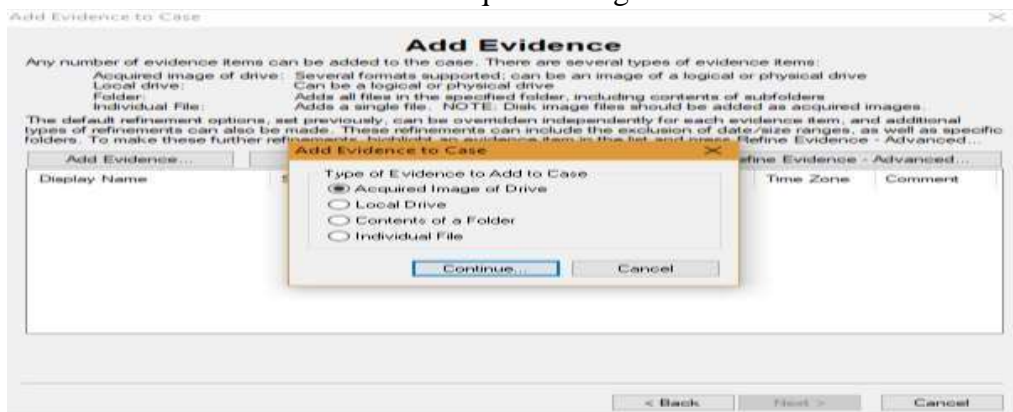
## 11. Click on next.



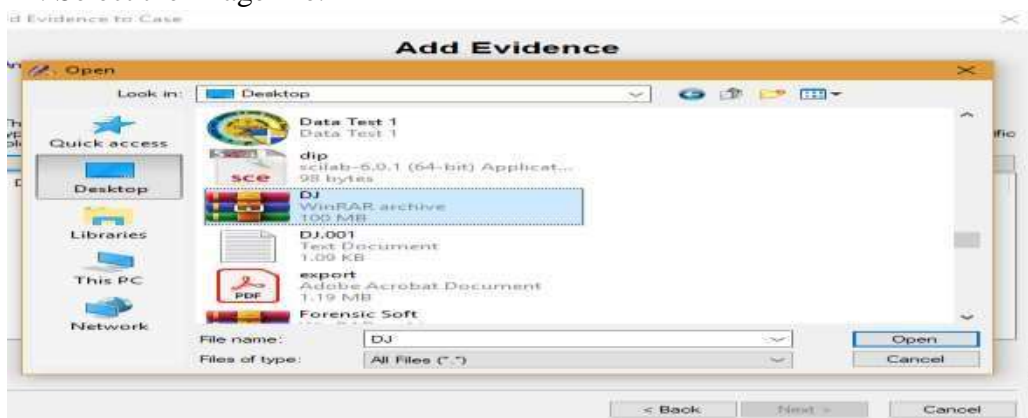
## 12. Click on next.



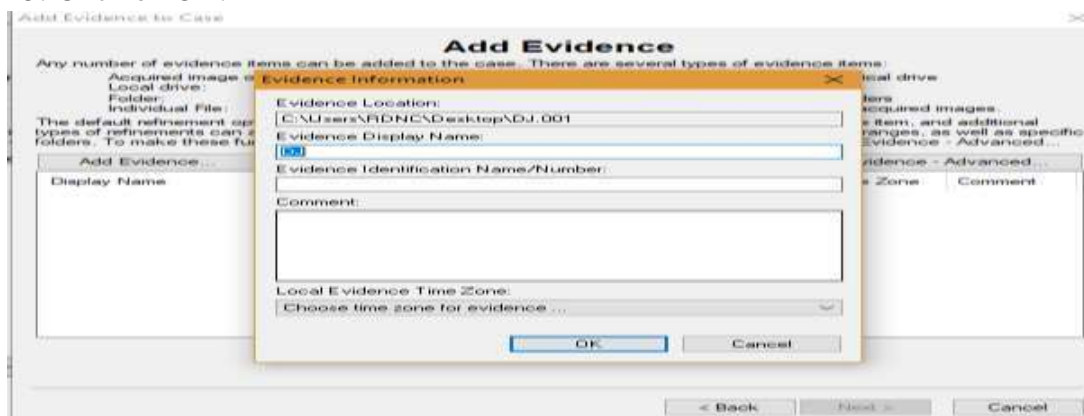
13. Click on Add Evidence > Acquired Image of Drive > Continue.



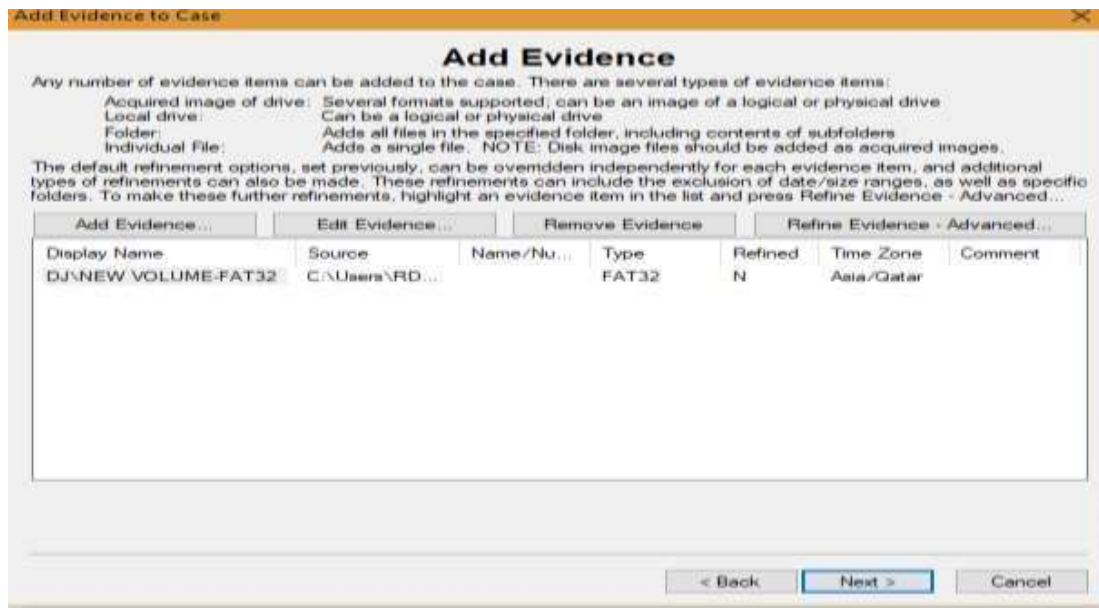
14. Select the image file.



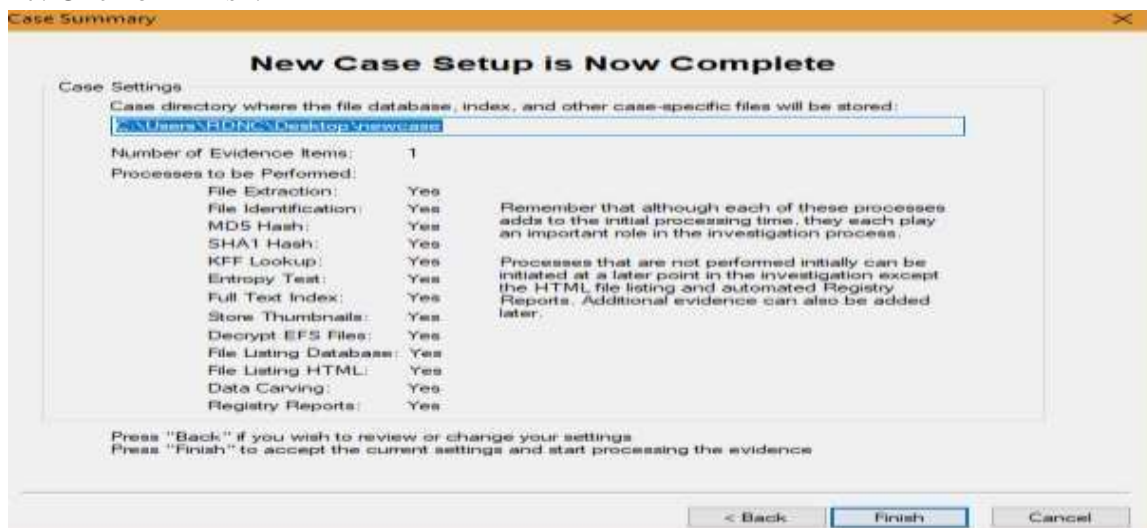
15. Click on OK.



16. Click on next.



17. Click on Finish.

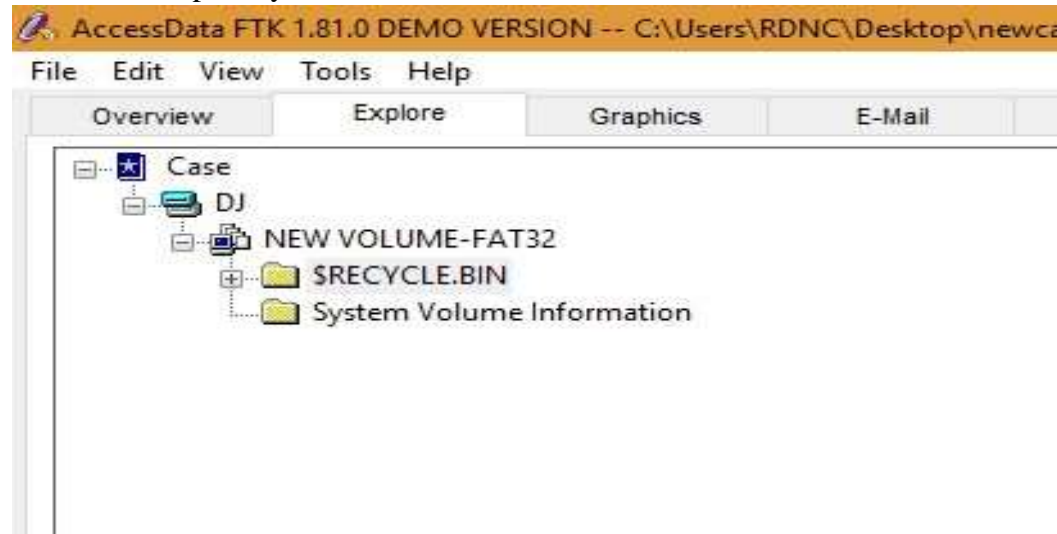


18. Files are being carving.

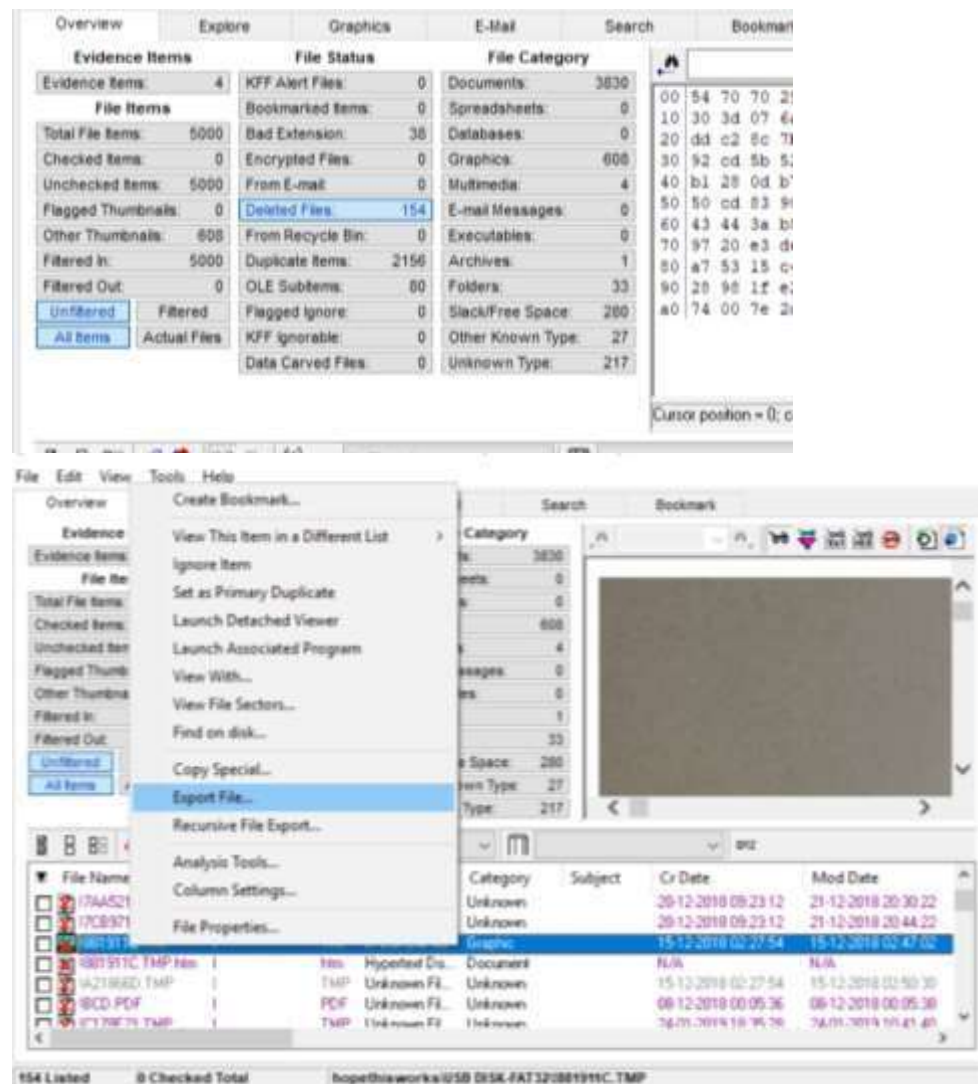




19. In the left panel you can see all the recovered files.

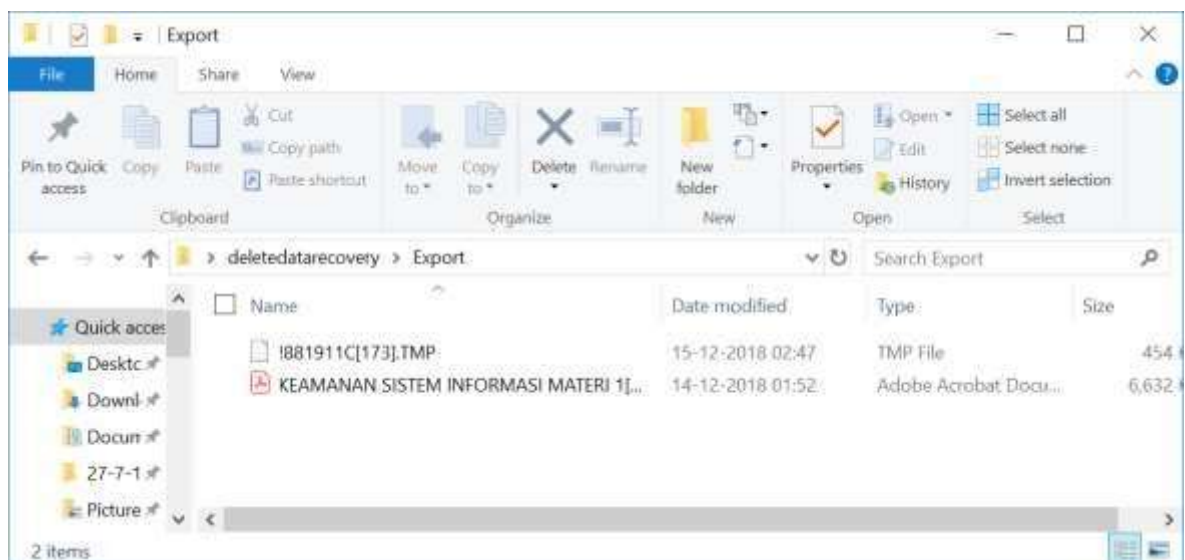
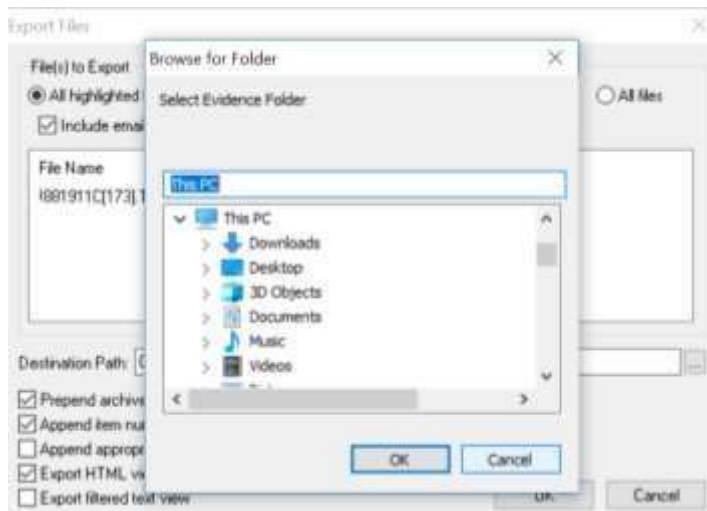


20. Click on the Deleted file tab-> Right click on any deleted file to export it





21. Browse and choose the destination folder to export the deleted file



**Conclusion:** The above program has been executed successfully.

## PRACTICAL NO 8

**Aim: Acquisition of Cell phones and Mobile**

**devices Steps:**

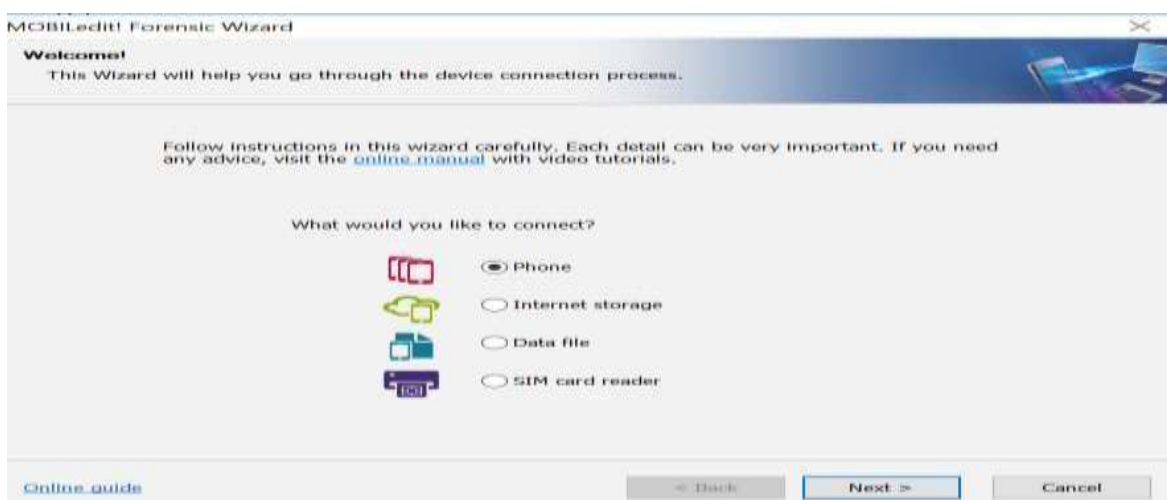
1. Download mobiledit forensic tool in mobile.
2. Open Mobiledit tool in PC.



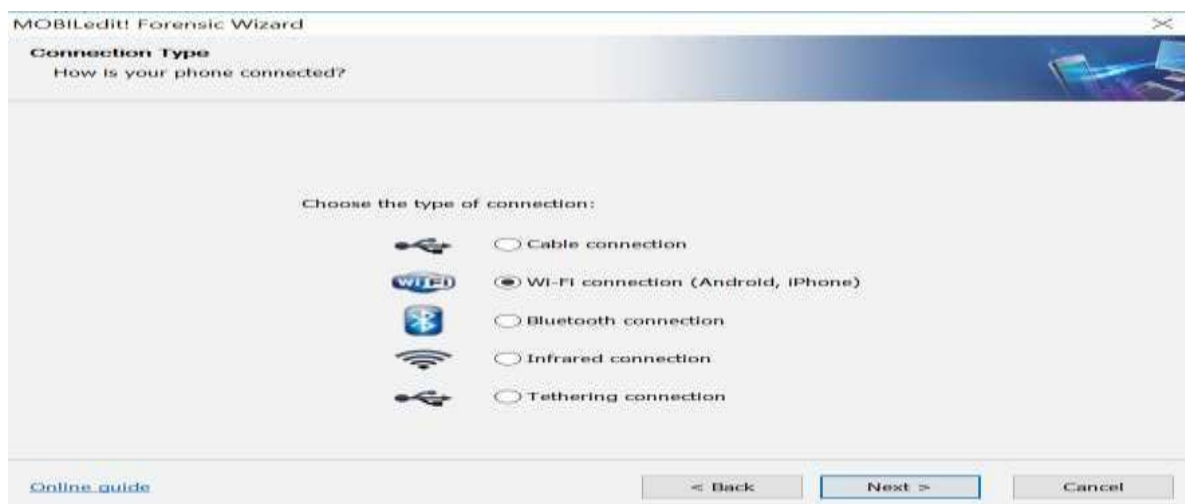
3. Click on connect.



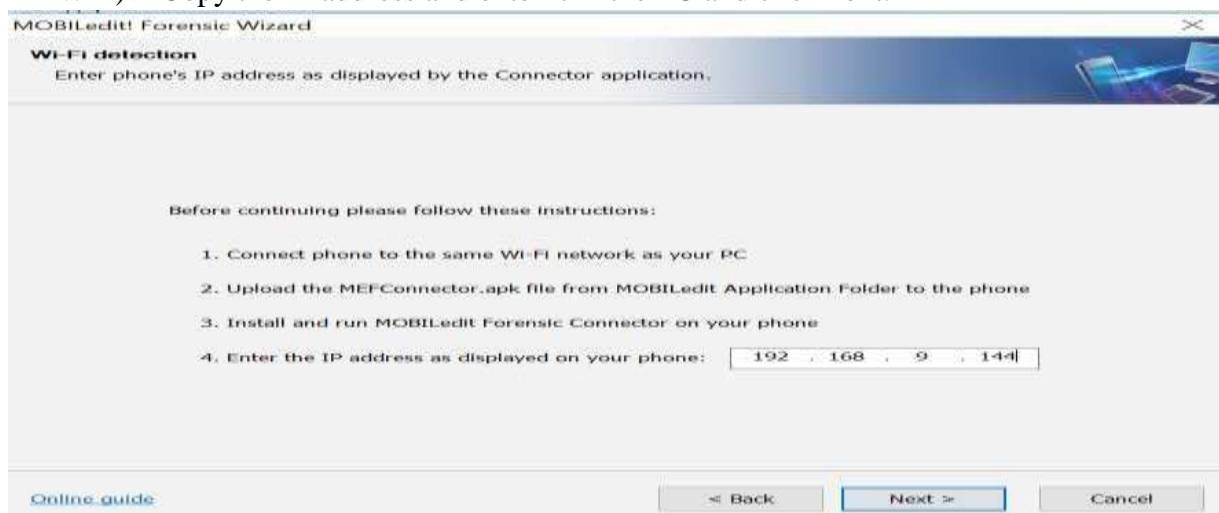
4. Connect your mobile device to the system. Click on phone > next.



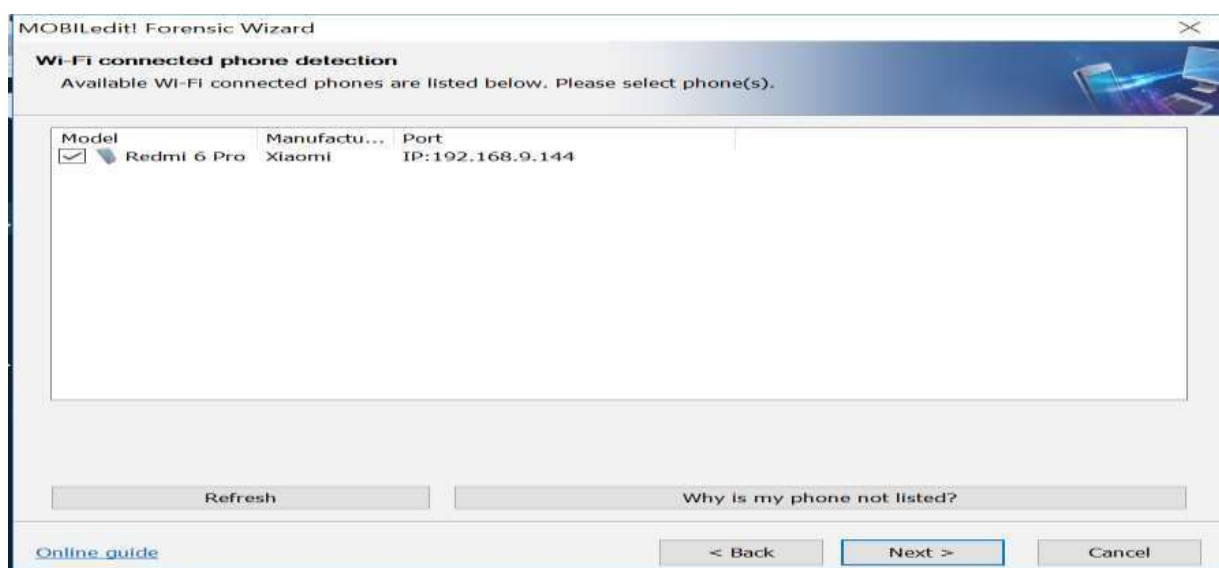
## 5. Click the connection



## 6. Open the mobiledit tool in phone and click on the type of connection (i.e Wifi) &gt; Copy the IP address and enter it in the PC and click next.



## 7. It shows the phone which is connected. Click on next.



8. Click on next.

MOBILedit! Forensic Wizard

**Data acquire settings**  
Please set the following options for data acquiring.  
Data will be stored in the "Cases" folder.

Device Label:

Device Name:  Device Evidence Number:

Owner Name:  Owner Phone Number:

Phone Notes:

Device Capabilities

- ☒ Phonebook
- ☒ Organizer
- ☒ Messages
- ☒ Files
- ☒ User Files
- ☒ Media

☒ Include SIM Card Data

Communication Log Of Backup Operation

☒ Create:

[Online guide](#)

9. Click on whole system and click next.

MOBILedit! Forensic Wizard

**File system acquiring**  
Choose the part of filesystem to acquire.

☒ Whole file system

☐ Specified file types:  ☐ Audio ☐ Video ☐ Pictures

☐ Selected files & folders

☒ Phones

☒ Xiaomi Redmi 6 Pro

[Online guide](#)

MOBILedit! Forensic Wizard

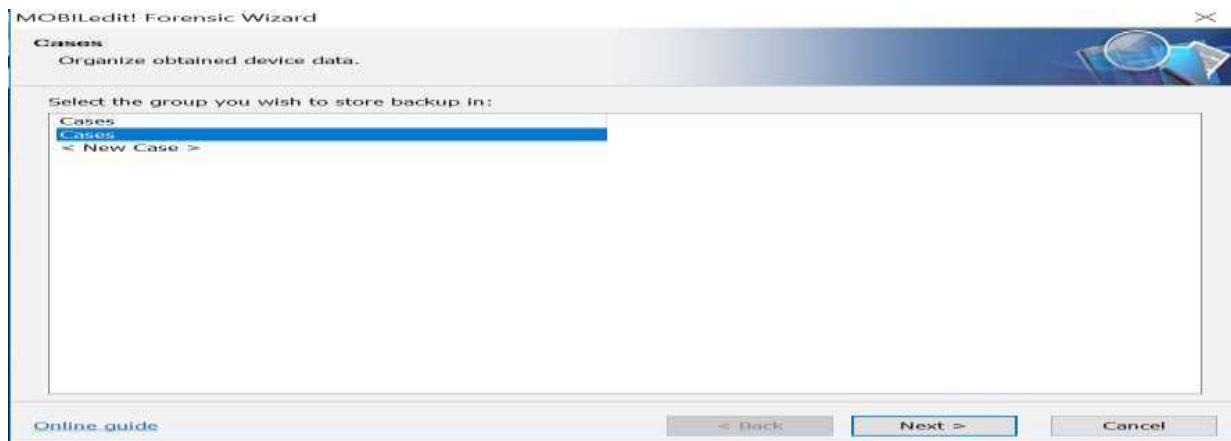
**Data acquiring**  
Acquiring of selected data may take a while.

Item	Status
Data acquisition started on	05-03-2019 14:50:51
Calendar	The operation completed successfully.
Phonebook	The operation completed successfully.
Outgoing Calls	The operation completed successfully.
Incoming Calls	The operation completed successfully.
Missed Calls	The operation completed successfully.
Messages	The operation completed successfully.
Filesystem: Info	Initializing...

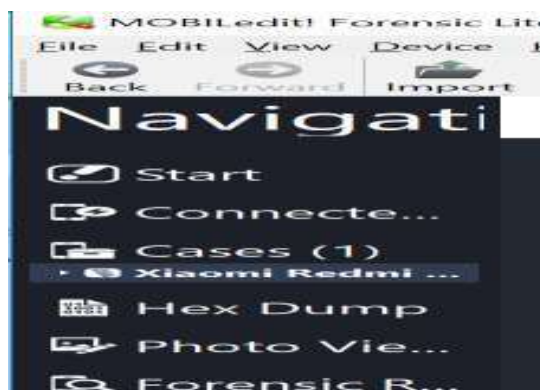
Scanning "User":

[Online guide](#)

10. Click on case and click next.



11. Click on your device in the left panel.



12. You can see all the files.



**Conclusion:** The above program has been executed successfully.