**Index**

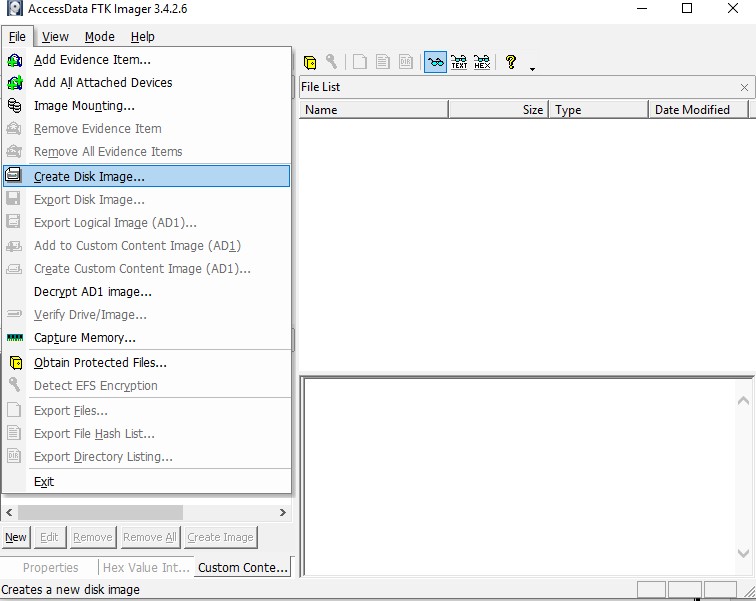
|  |  |  |  |
| --- | --- | --- | --- |
| **Sr.No** | **Date** | **Title** | **Sign** |
| Pract 1 |  | Creating a Forensic Image using FTK Imager/Encase  Imager: Creating Forensic Image, Check Integrity of Data, Analyze Forensic Image |  |
| Pract 2 |  | Data Acquisition: Perform data acquisition using:,  USB Write Blocker + FTK Imager |  |
| Pract 3 |  | Forensics Case Study: Solve the Case study (image file) provide in lab using Encase Investigator or Autopsy. |  |
| Pract 4 |  | Capturing and analyzing network packets using Wireshark(Fundamentals): Identification the live network, Capture Packets, Analyze the captured packets |  |
| Pract 6 |  | Using Sysinternals tools for Network Tracking and  Process Monitoring: Check Sysinternalstools, Monitor Live Processes, Capture RAM, Capture TCP/UDP packets, Monitor Hard Disk, Monitor Virtual Memory, Monitor Cache Memory |  |

# PRACTICAL 1

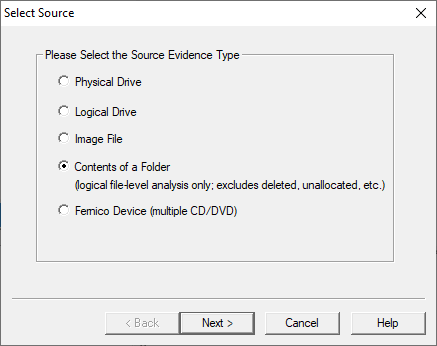
Aim : Creating a Forensic Image using FTK Imager/Encase Imager :

* Creating ForensicImage
* Check Integrity ofData
* Analyze ForensicImage
  + - Creating ForensicImage

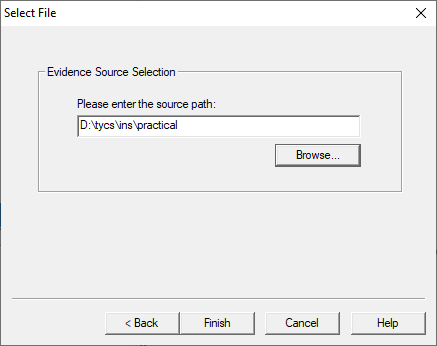
1. Click File, and then Create Disk Image, or click the button on the toolbar.



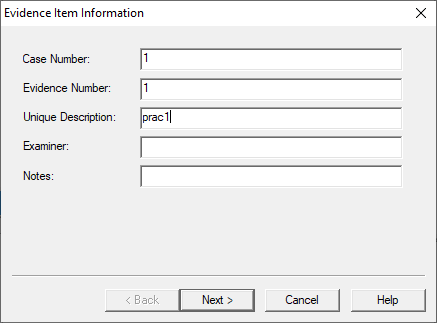
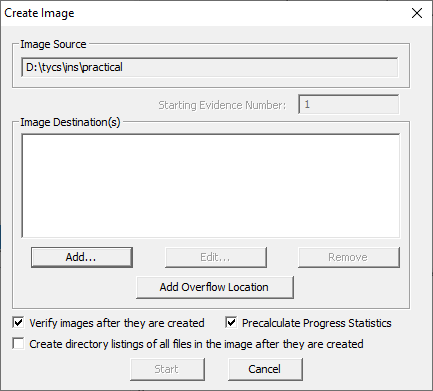
1. Select the source evidence type you want to make an image of and clickNext.



1. Select the source evidence file with path.

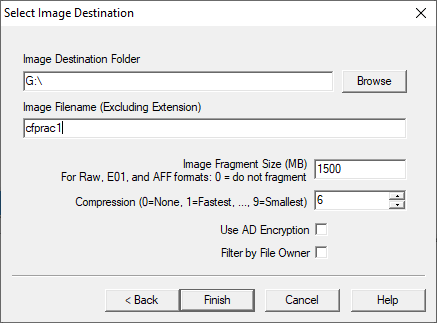


Click on “add” to add image destination

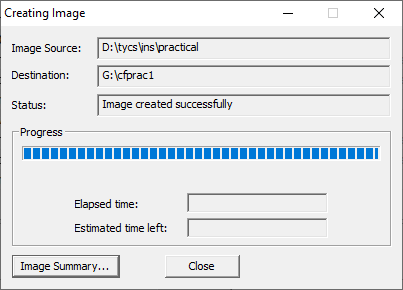


1. In the Image Destination Folder field, type the location path where youwanttosavetheimagefile,orclick**Browse**tofindtothedesired location.

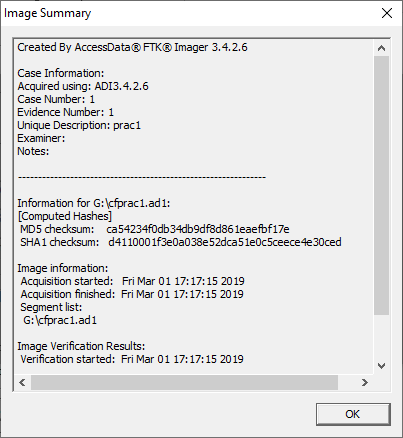
**Note:** If the destination folder you select is on a drive that does not have sufficientfreespacetostoretheentireimagefile,FTKImagerpromptsfor anewdestinationfolderwhenallavailablespacehasbeenusedinthefirst location.IntheImageFilenamefield,specifyanamefortheimagefilebut do not specify a fileextension.



1. After adding the image destination path click on finish and start the imageprocessing.

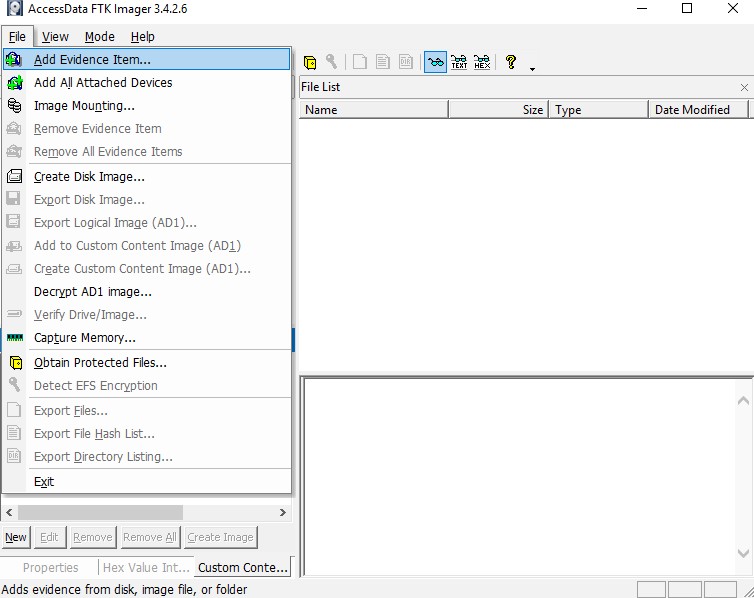


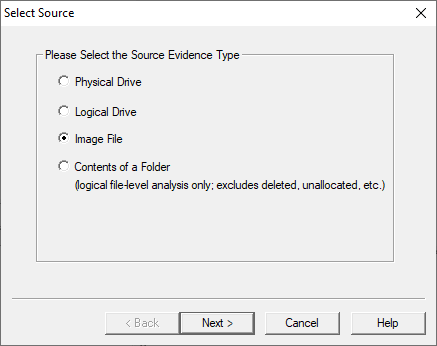
1. After the images are successfully created, click Image Summary to view detailed file information, including MD5 and SHA1 checksums.



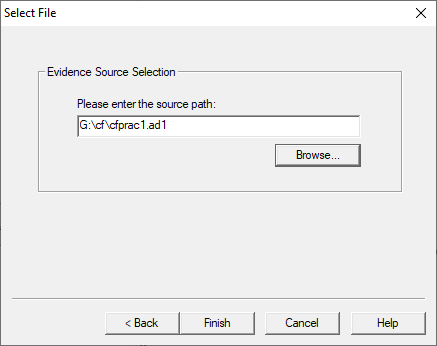
## Analyze Forensic Image:

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

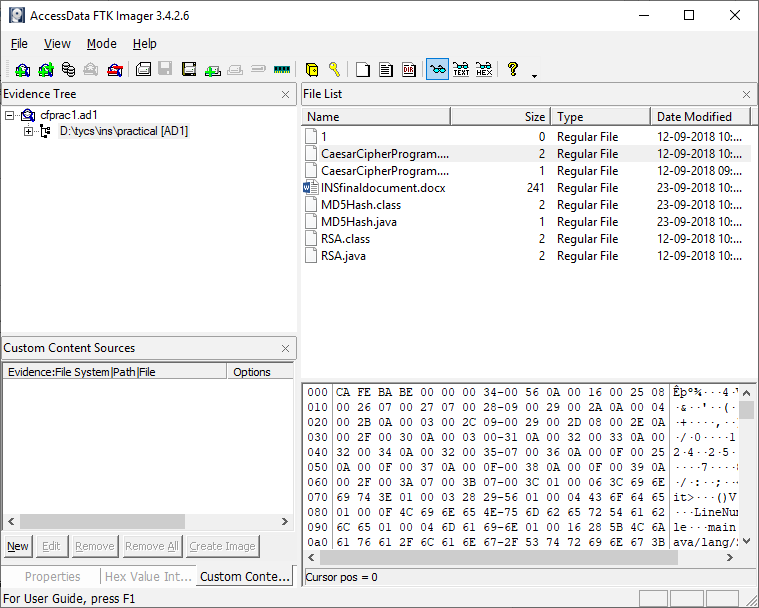


Now select the source evidence type as image file.

Open the created evidence image file



Now select Evidence Tree and analyze the image file .



# PRACTICAL 2

Aim: Data Acquisition:

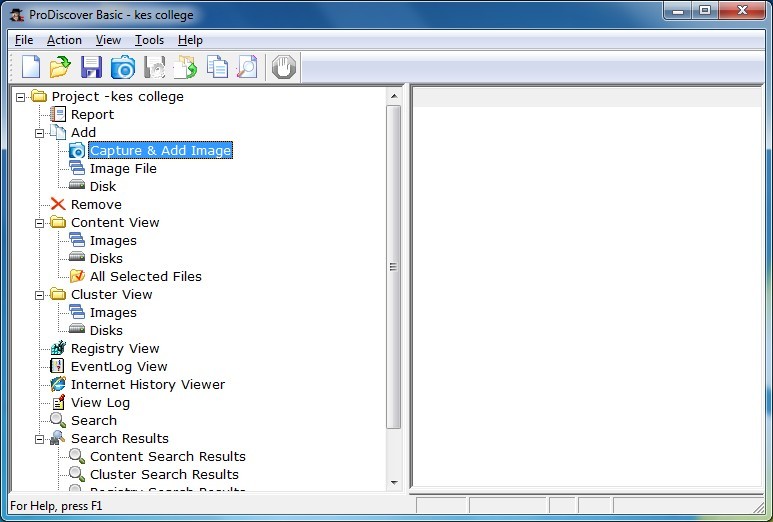
* Perform data acquisitionusing:
* USB Write Blocker + FTKImager

## Steps:

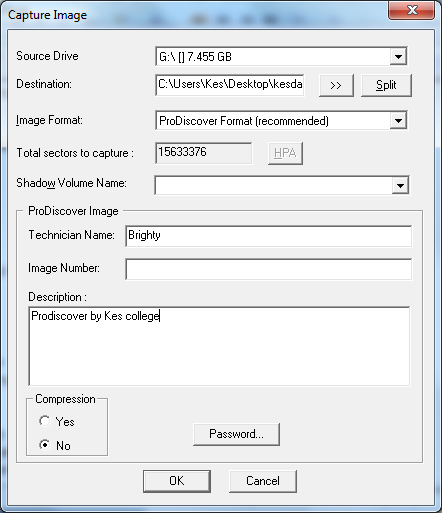
Step 1: First Open Prodiscover Basic and start with new case.



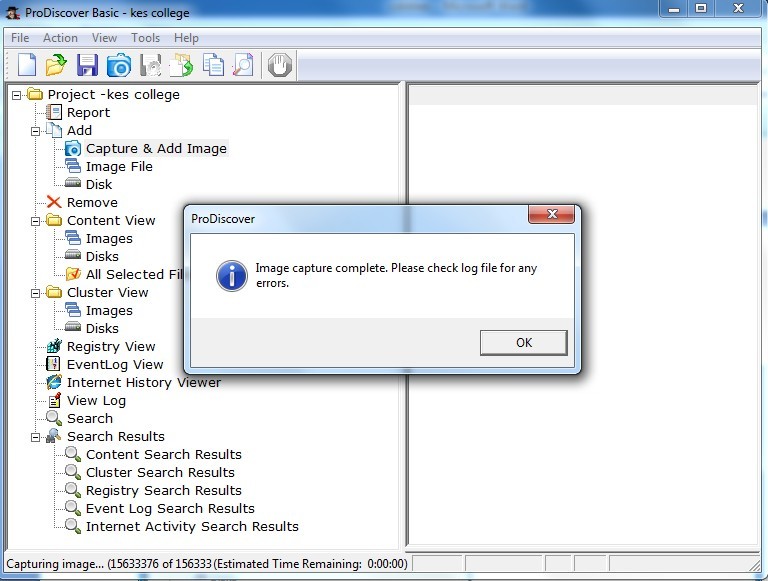
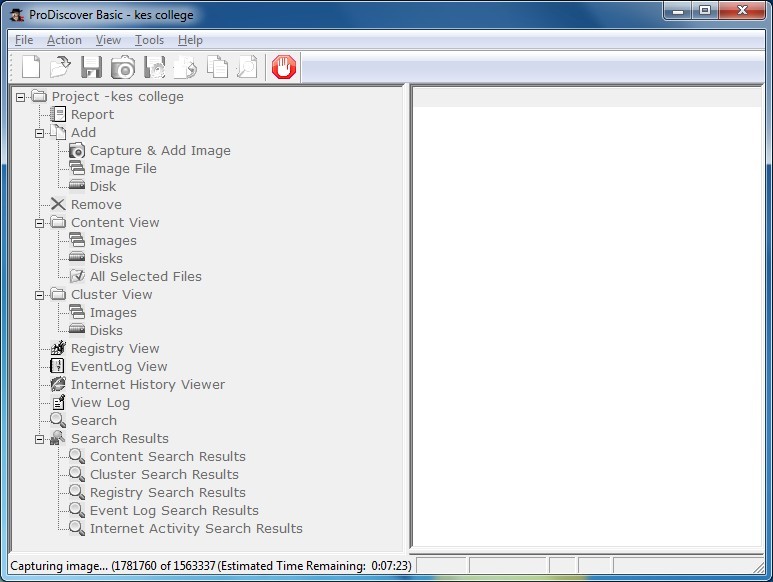
Step 2: The created project appears in left pane and select add>capture & add image.



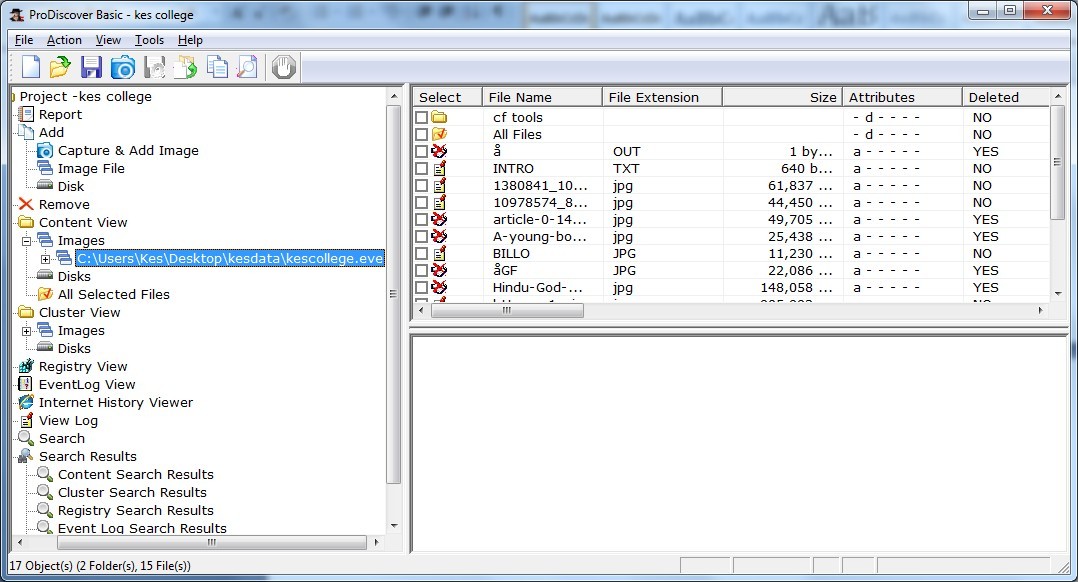
Step 3: fill the details as below. And click ok.



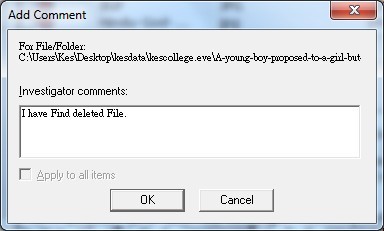
Step 4: capturing of image starts.



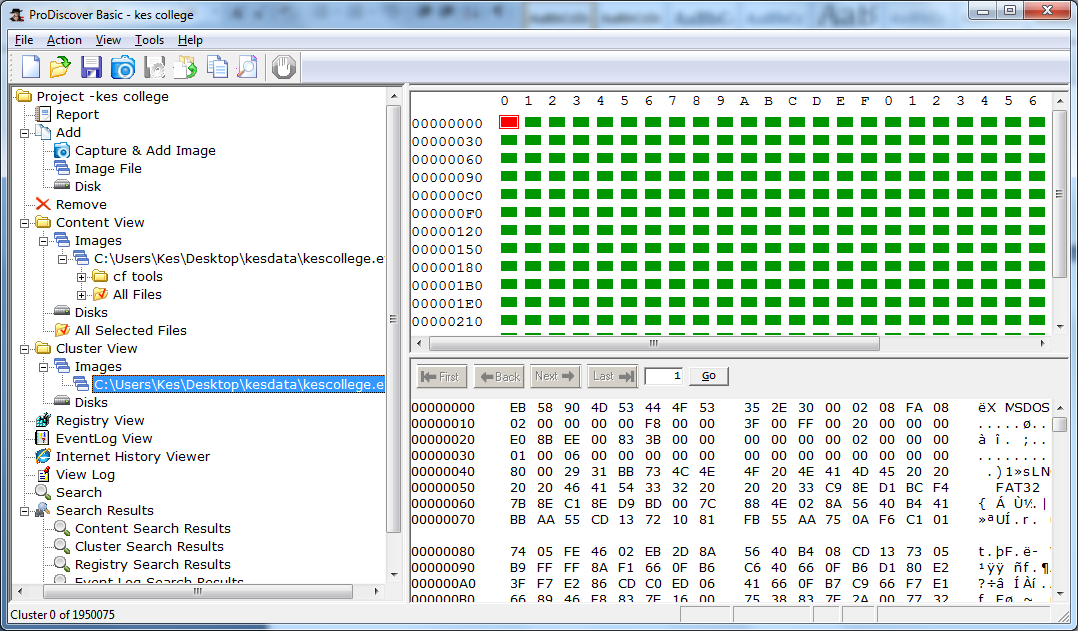
Step 5: Open the image created, go to Add > Images in left pane.



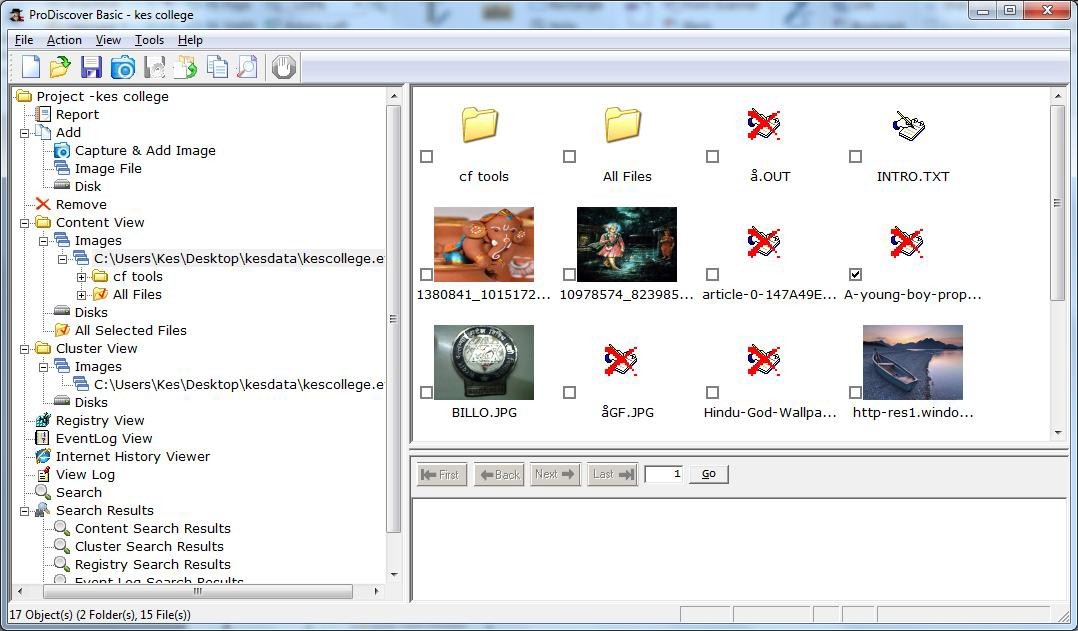
Step 6: Click on any File and type a comment.



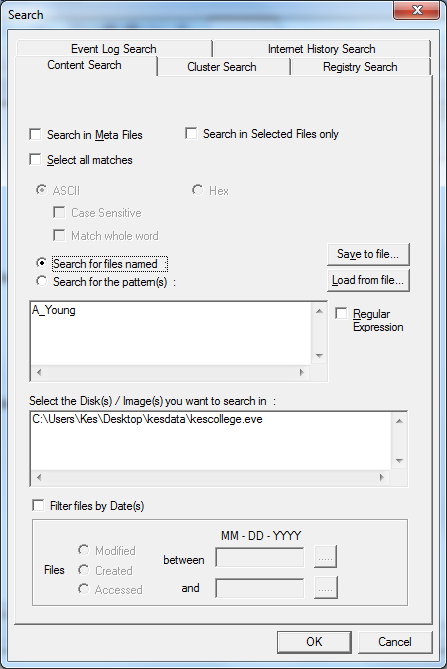
Step 7 : the cluster view is seen from the cluster view in left panel.



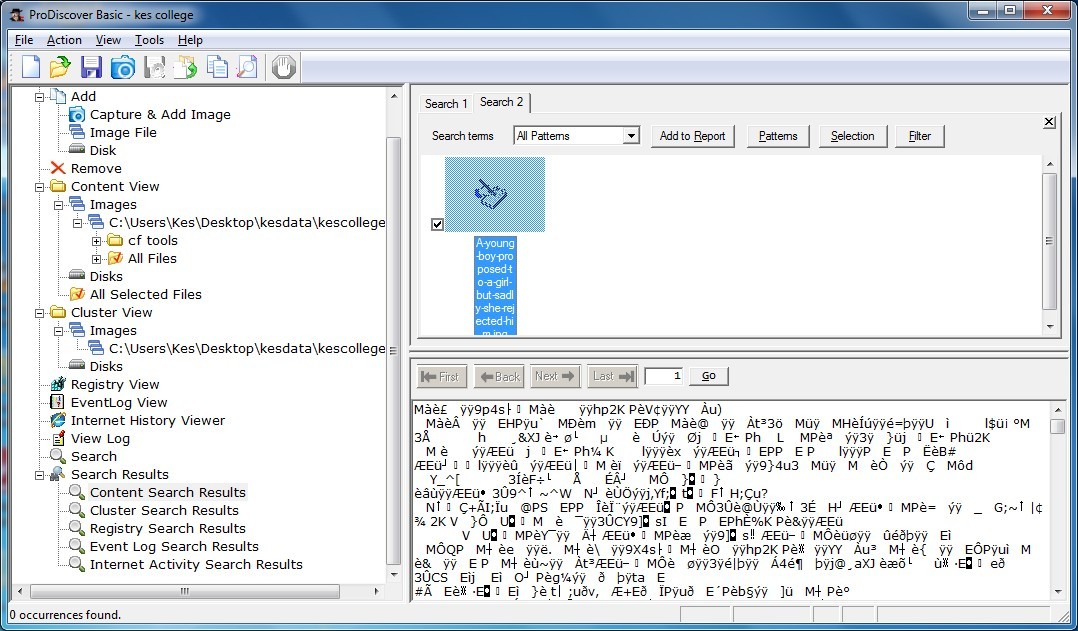
Step 8 : We can also view gallery view by Right Click.



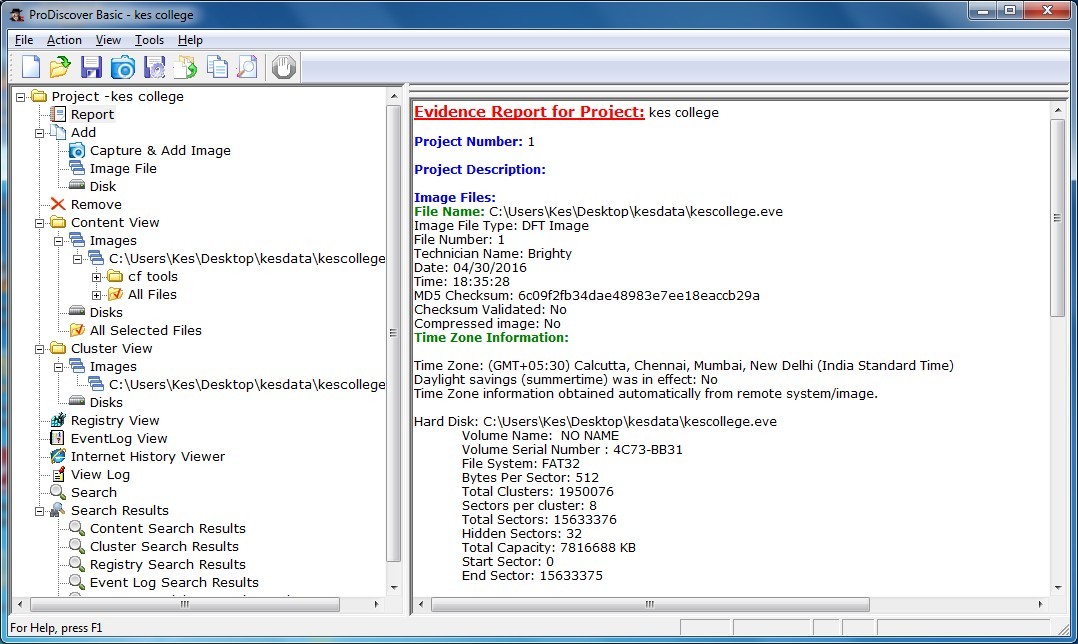
Step 9: Keyword search. Click on Search in left pane and Enter the file name to be searched in the image created.

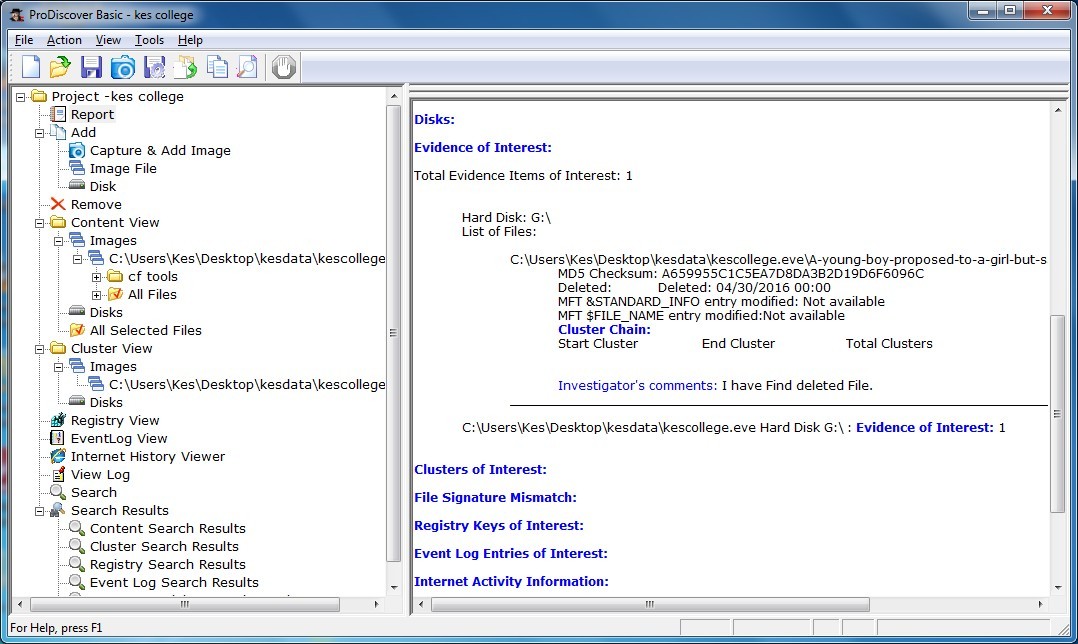


Step 10 : Output of Keyword search.



Step 11 : Click on View>Report.





# PRACTICAL 3

AIM :- Forensics Case Study : Solve the Case study (image file) provide in lab using Encase Investigator or Autopsy .

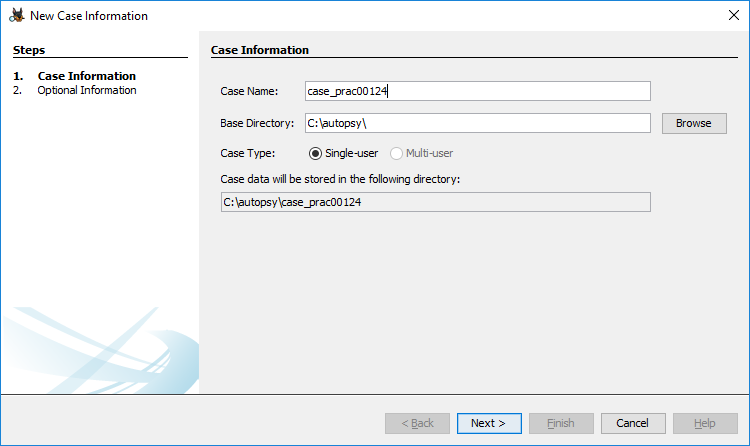
Step 1 : Open Autopsy



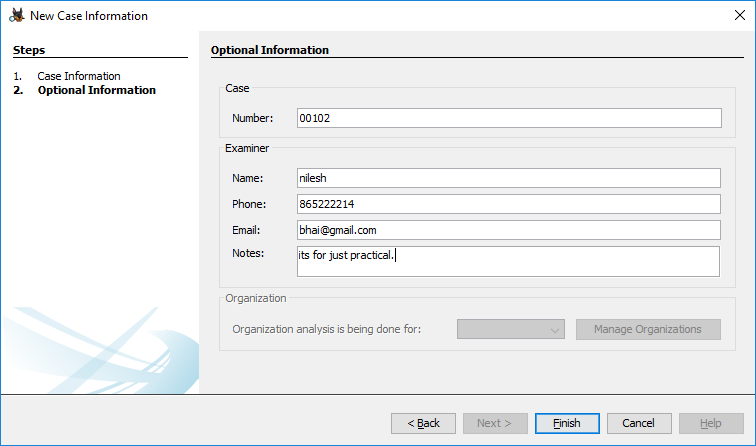
Step 2 : Click on new case



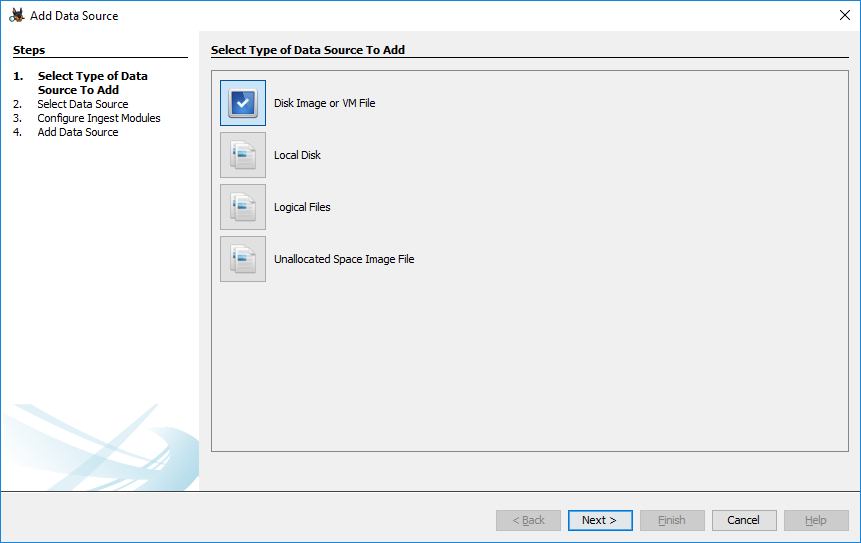
Step 3 : Enter details regarding the case and click on next button.



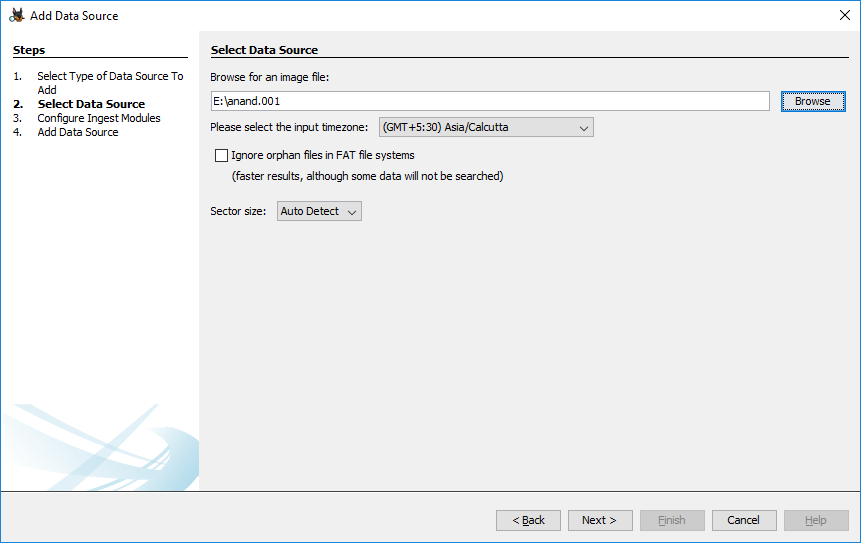
Step 4 : Enter further details and click on next button



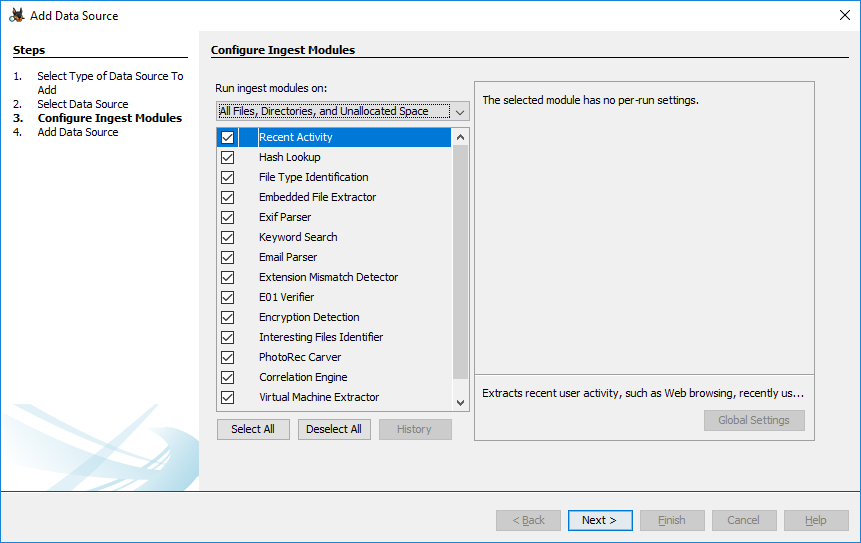
Step 5 : Now here we have to select Type of data source to add , in our case disk image or VM file and click on next



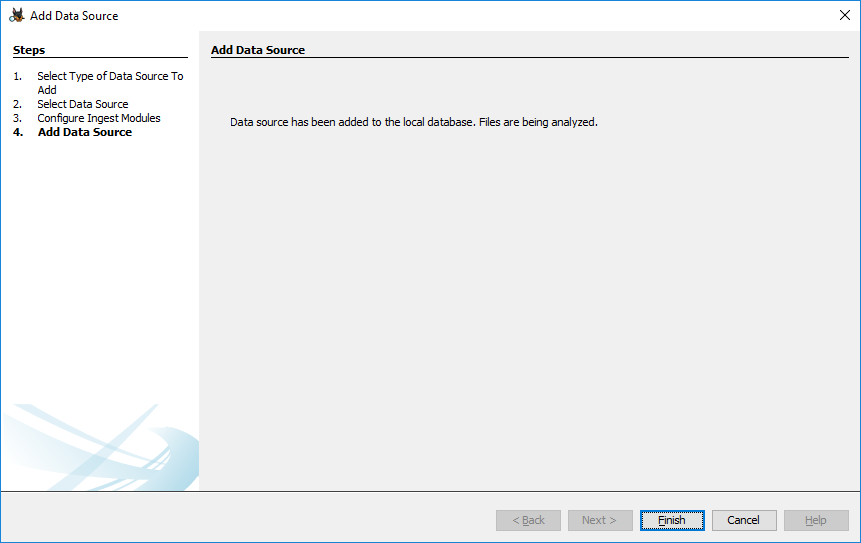
Step 6 : Now we have to select image file and click on next button



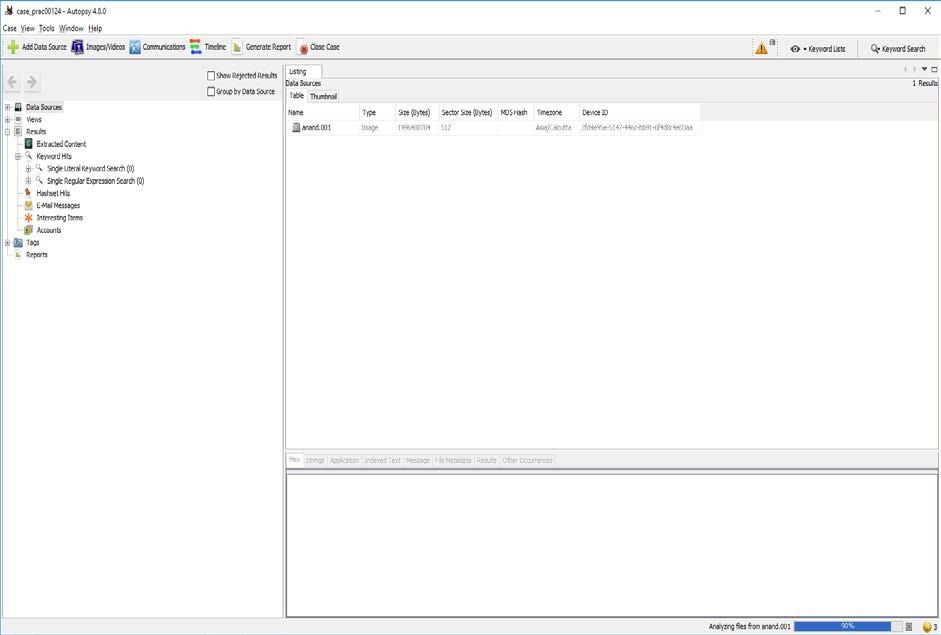
Step 7 : Now click on select all in order to Run ingest modules on: and click on next.



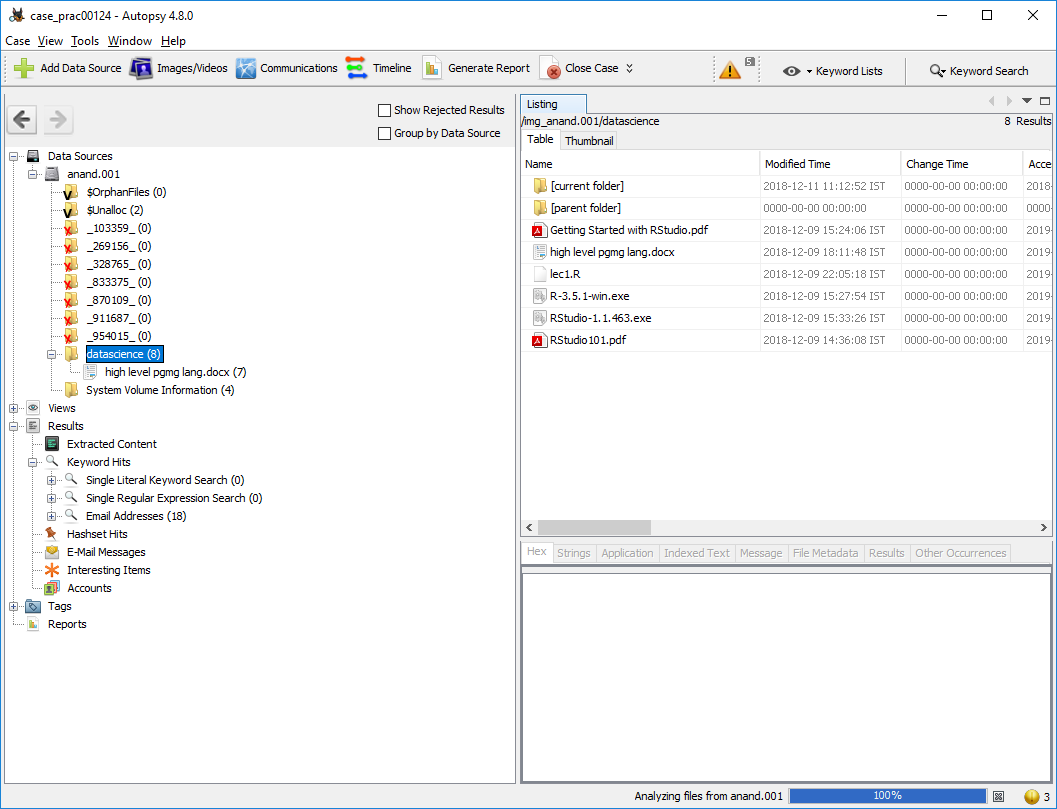
Step 8 : Now click on finish



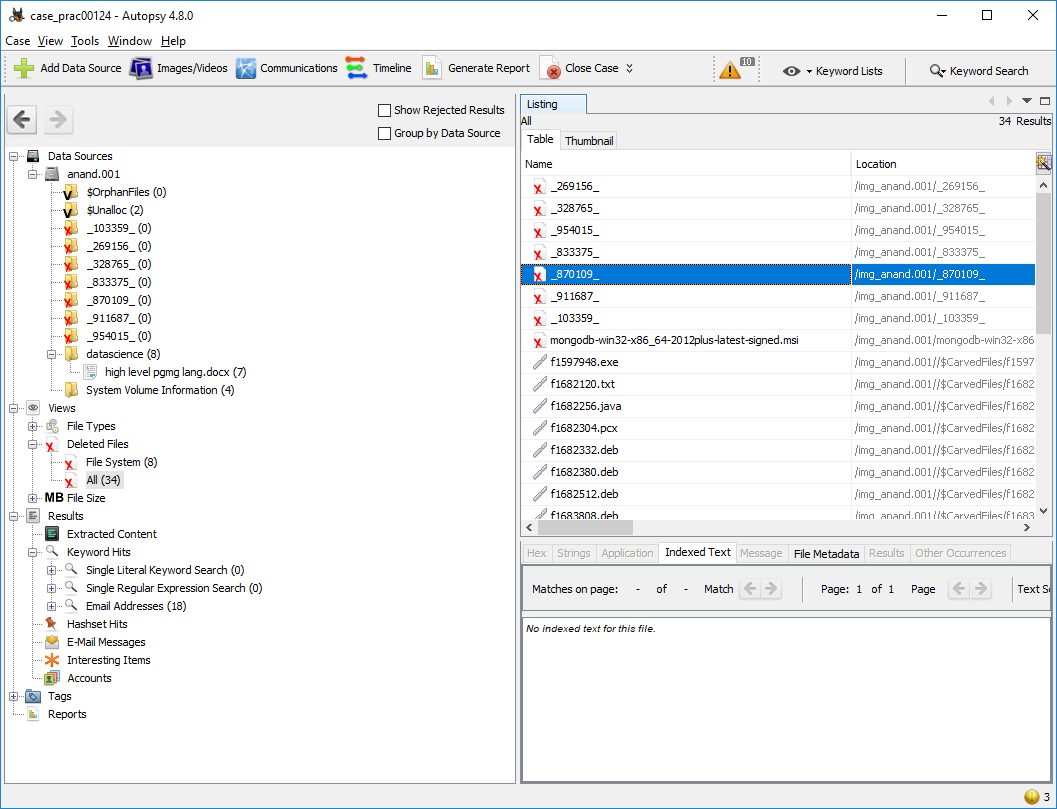
Step 9 : Now Autopsy window will appear and it will analyse the disk that we have selected .



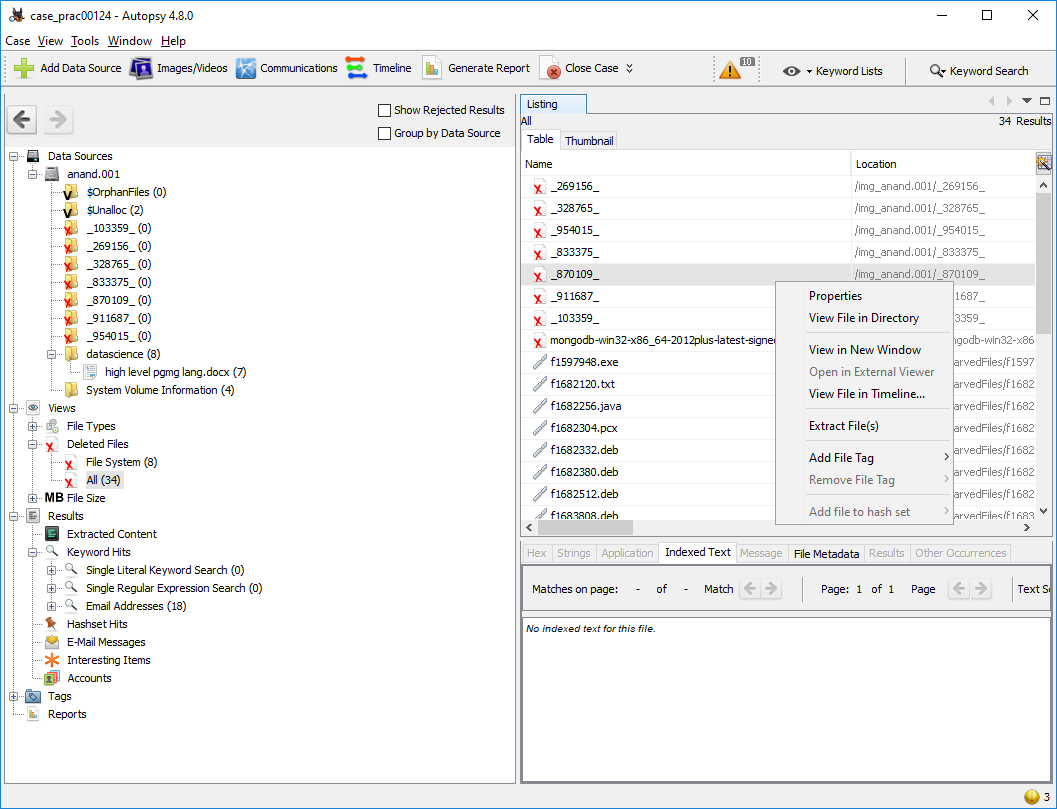
Step 10 : All image files appears in the Table tab. Select any file to see the data



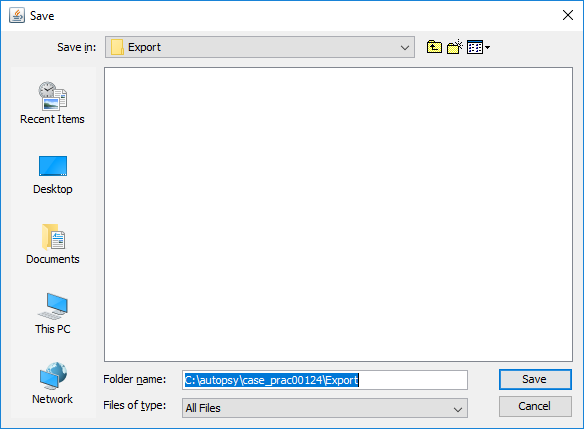
Step 11 :Expand the tree from left side panel to view the document files.



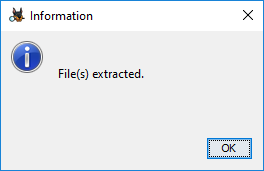
Step 12 : To recover the files , go to view code  Deleted files node , here select any file and right click on it then select Extract files option



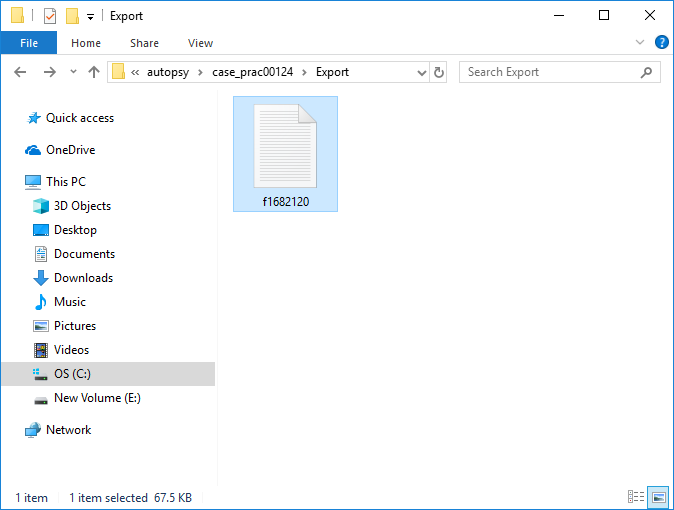
Step 12: Select Path where you want to save extracted file and click on save .



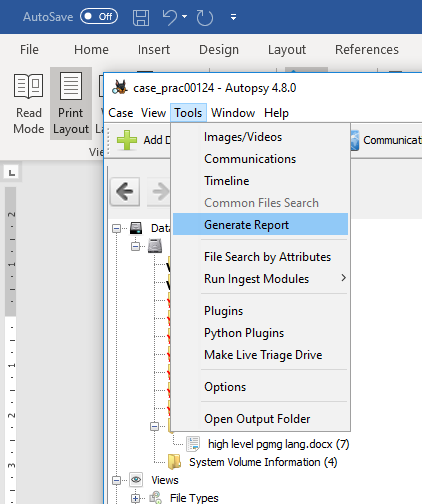
Step 13 : Now click on OK



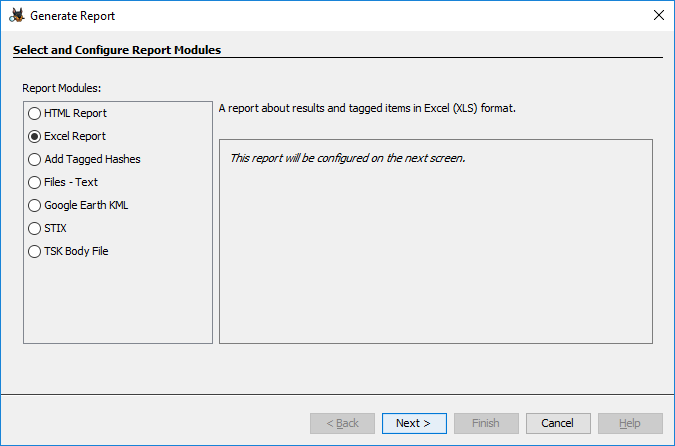
Step 14 : Now go to C:\autopsy\case\_prac00124\Export folder to see recover file



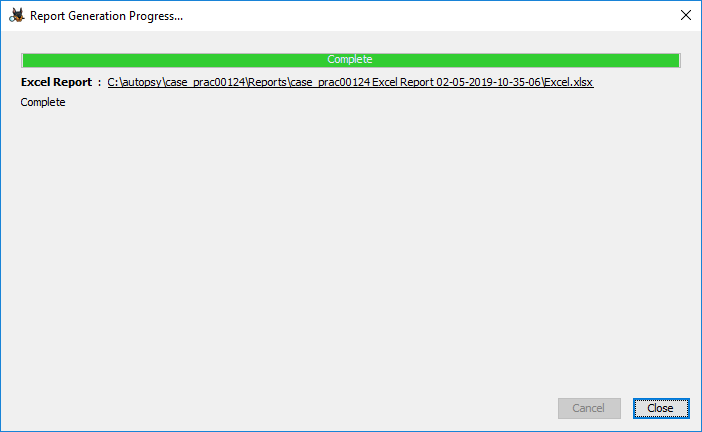
Step 15 : Click on generate report from Autopsy window and select the Excel format and click on next



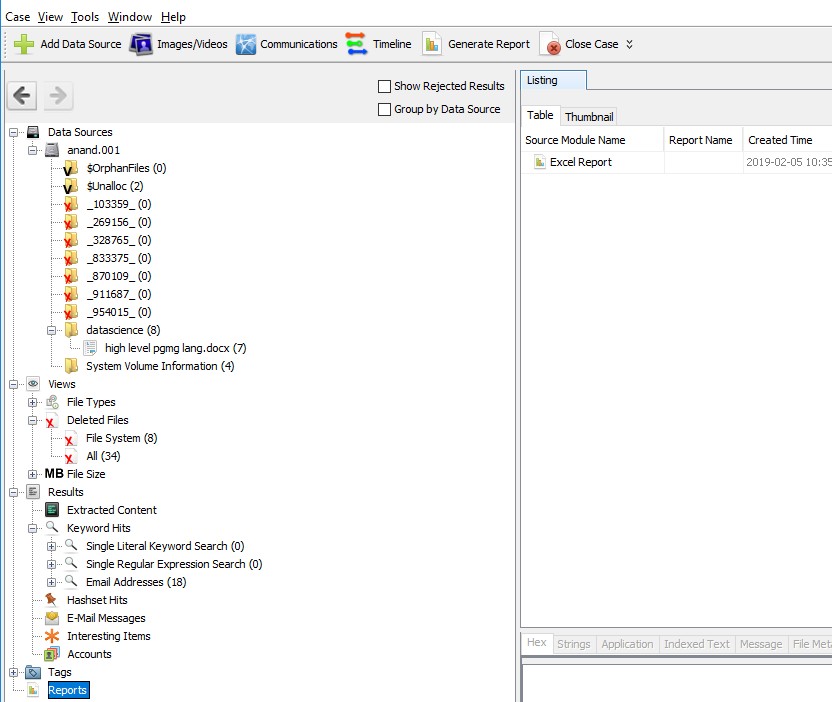
Step 16 : This window will appear



Step 17 : Now report is generated so click on close button. We can see the Report on Report Node



Step 18 : Click on report



# PRACTICAL 4

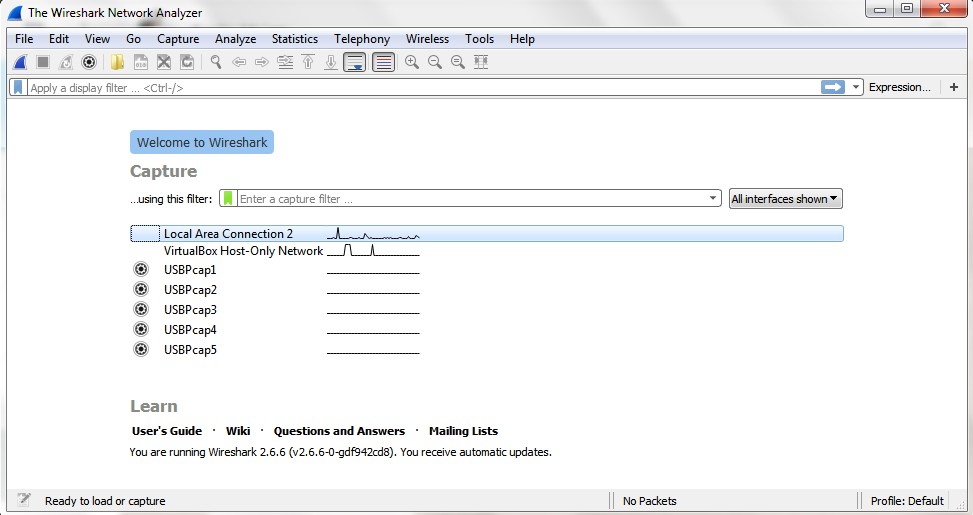
AIM : Capturing and analyzing network packets using Wireshark(Fundamentals):

* Identification the livenetwork
* CapturePackets
* Analyze the capturedpackets

## Capturing Packets

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

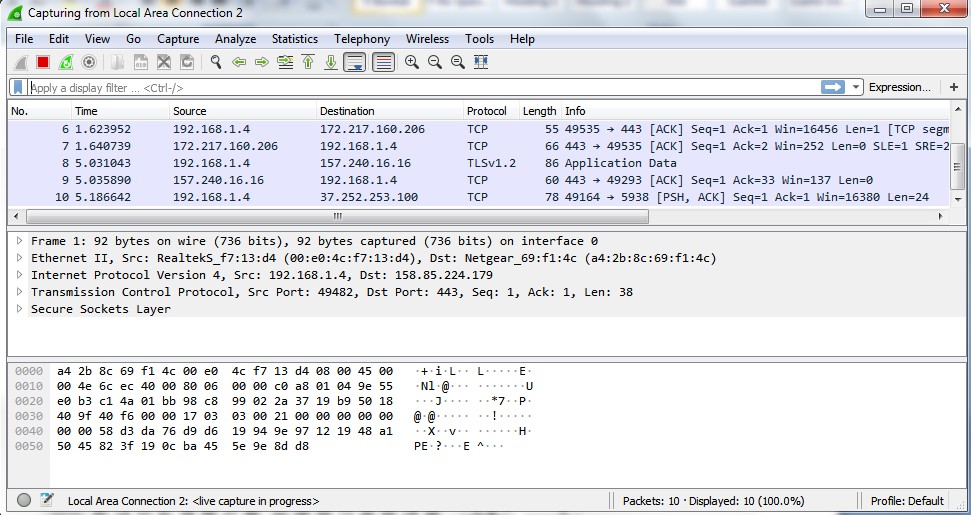
YoucanconfigureadvancedfeaturesbyclickingCapture>Options,butthisisn’t necessary fornow.



As soon as you single-click on your network interface’s name, you can see how the packets are working in real-time. Wireshark will capture all the packets going in and out of our systems.

Promiscuous mode is the mode in which you can see all the packets from other systems on the network and not only the packets send or received from your network adapter. Promiscuous mode is enabled by default. To check if this mode is enabled, go to Capture and Select Options. Under this window check, if the

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



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

## Color Coding

Different packets are seen highlighted in various colors. This is Wireshark’s way of displaying traffic to help you easily identify the types of it. Default colors are:

Light Purple color for TCP traffic Light Blue color for UDP traffic

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

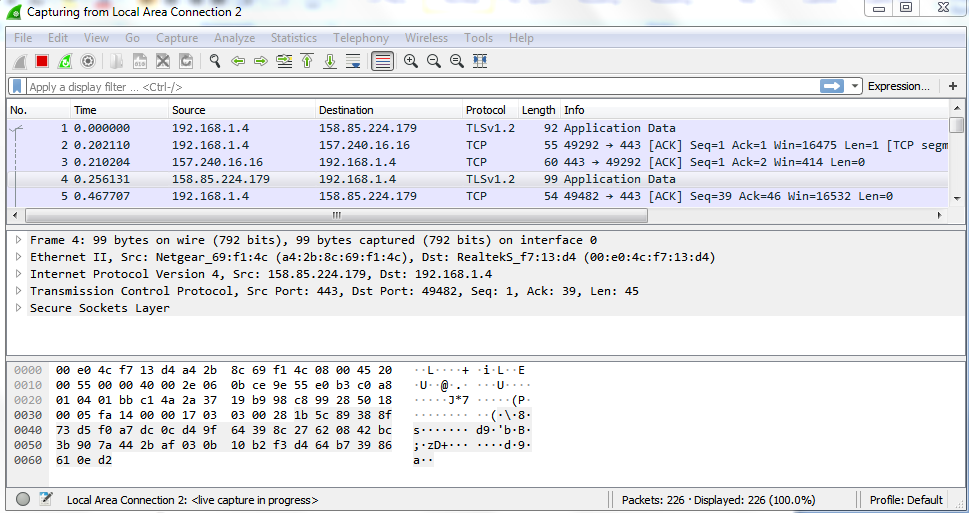
To check the color coding rules click on View and select Coloring Rules. These color coding rules can be customized and modified to fit your needs.

Graphical user interface, text, application

Description automatically generated

## Analyze the captured Packets:

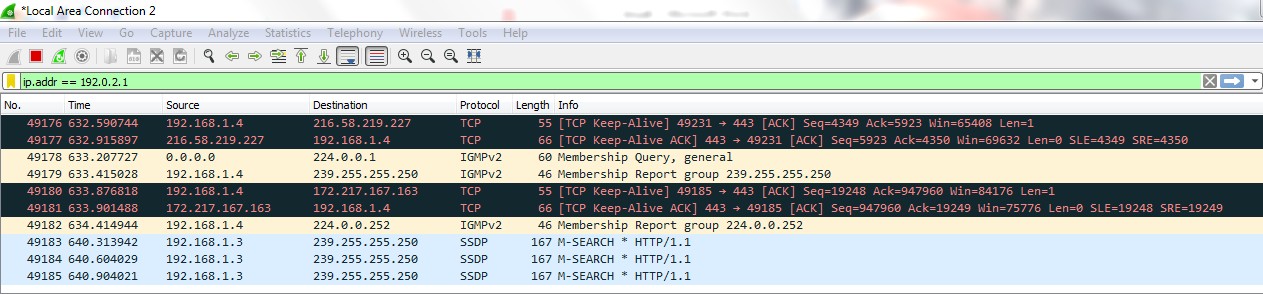
First of all, click on a packet and select it. Now, you can scroll down to view all its details.



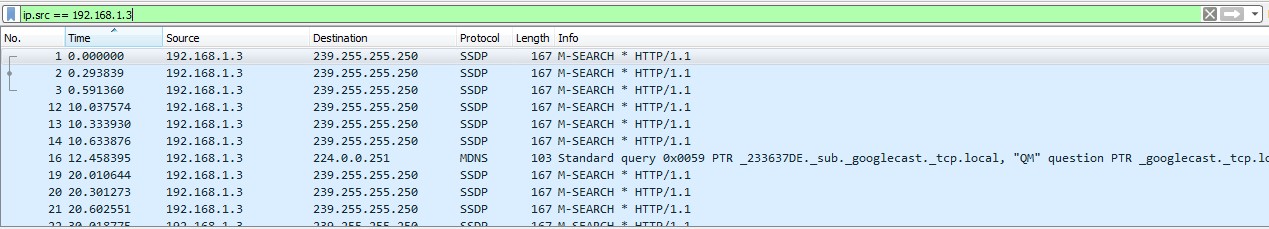
Filters can also be created from here. Right-click on one of any details. From the menu select Apply as Filter drop-down menu so filter based on it can be created.

## Display filter command –

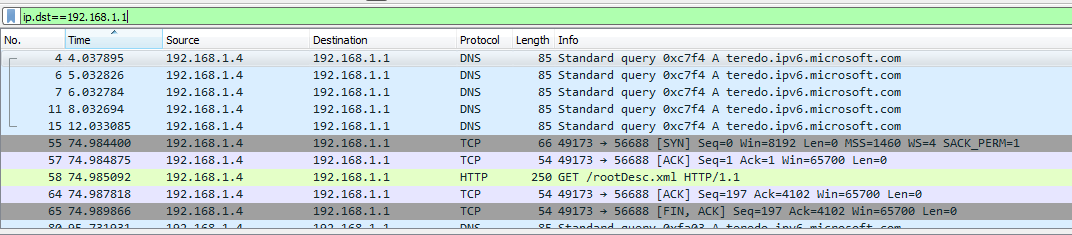
1. Display packets based on specificIP-address
   * ip.addr ==192.0.2.1



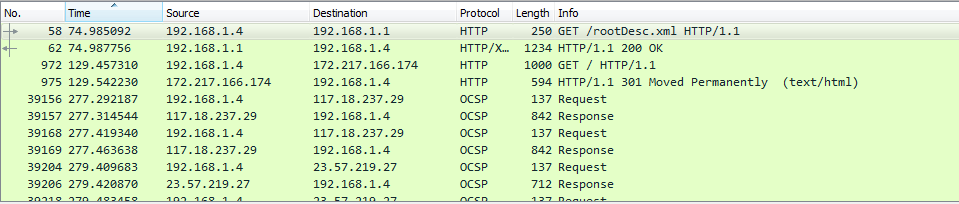
1. isplay packets which are coming from specificIP-address
   * ip.src ==192.168.1.3



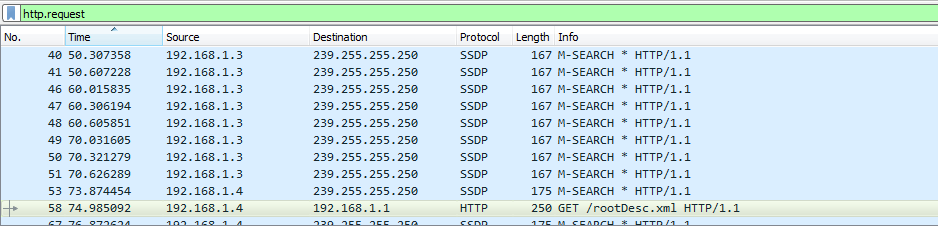
1. Display packets which are having specific IP-addressdestination
   * ip.dst ==192.168.1.1



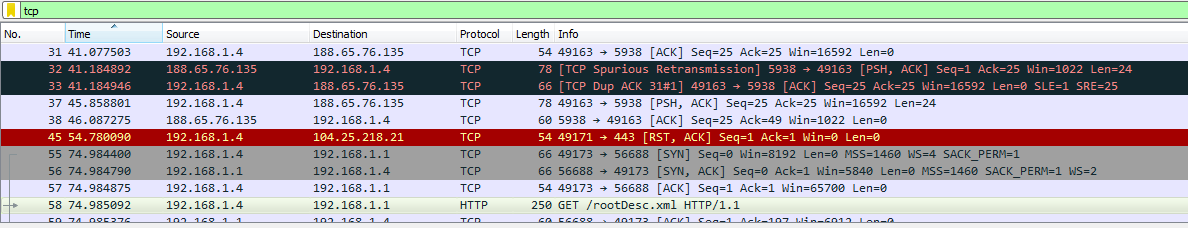
1. Display packets which are using httpprotocol
   * http



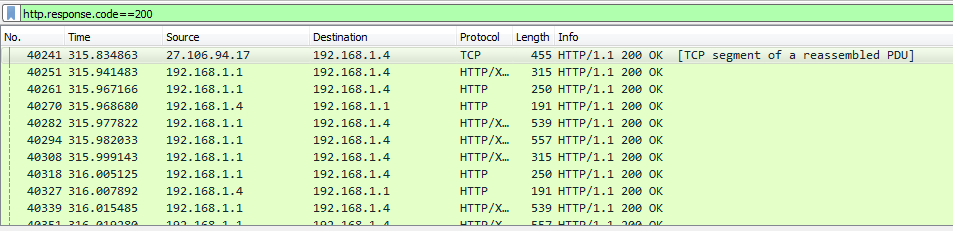
1. Display packets which are using httprequest
   * http.request



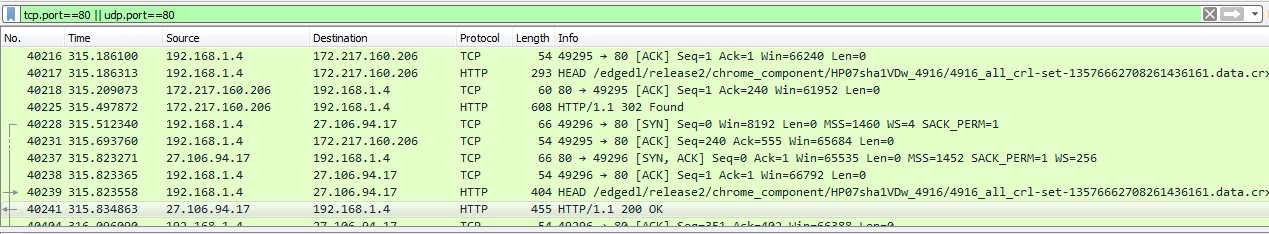
1. Display packets which are using TCPprotocol
   * tcp



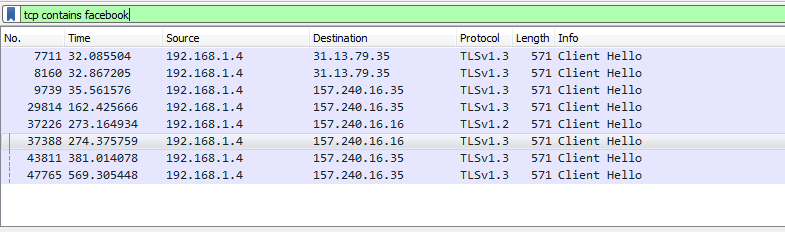
1. Display packets having no error connecting toserver
   * http.response.code==200



1. Display packets having port number80
   * tcp.port==80 ||udp.port==80



1. Display packets which that contains keywordfacebook
   * tcp containsfacebook



# PRACTICAL 6

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

* Check Sysinternalstools
* Monitor LiveProcesses
* CaptureRAM
* Capture TCP/UDP packets
* Monitor HardDisk
* Monitor VirtualMemory
* Monitor CacheMemory
  + **Check Sysinternalstools :**Windows Sysinternals tools are utilities to manage, diagnose, troubleshoot, and monitor a Microsoft Windows environment.

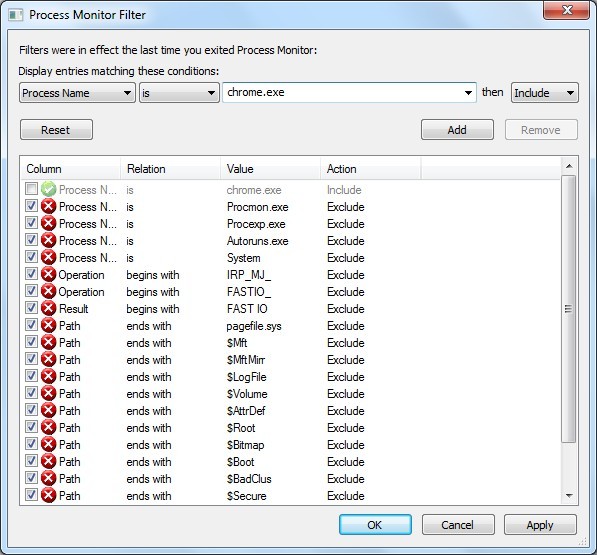
The following are the categories of Sysinternals Tools:

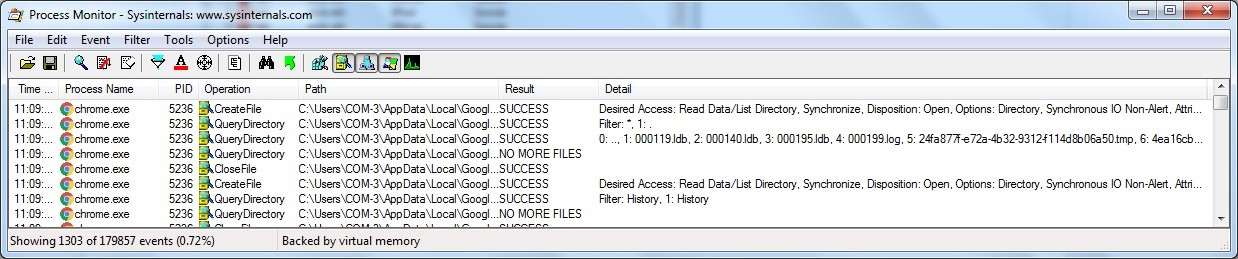
* 1. File and DiskUtilities
  2. NetworkingUtilities
  3. ProcessUtilities
  4. SecurityUtilities
  5. System InformationUtilities
  6. MiscellaneousUtilities

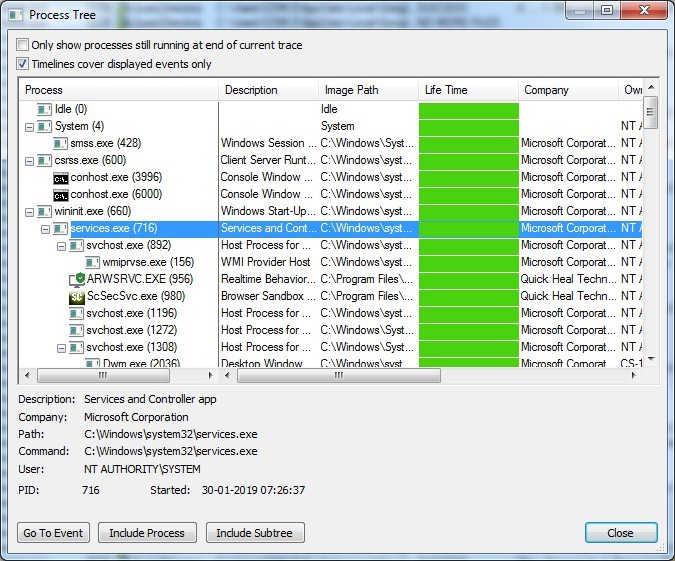
## Monitor Live Processes : (Tool: ProcMon) ToDo:

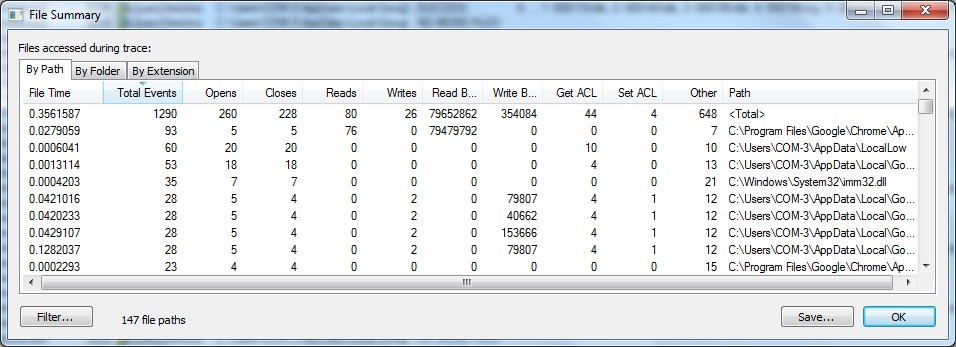
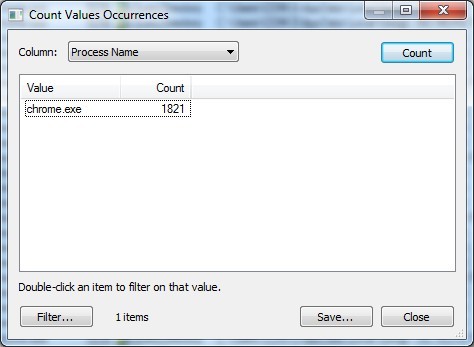
1. Filter (Process Name or PID or Architecture,etc)
2. ProcessTree
3. Process ActivitySummary
4. CountOccurrences

## Output:







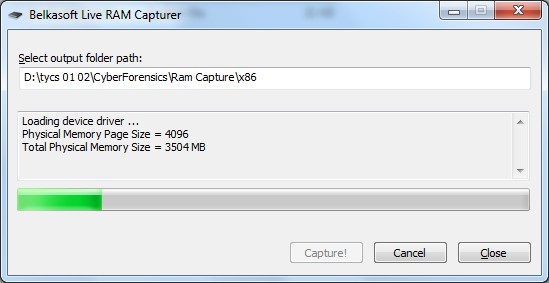


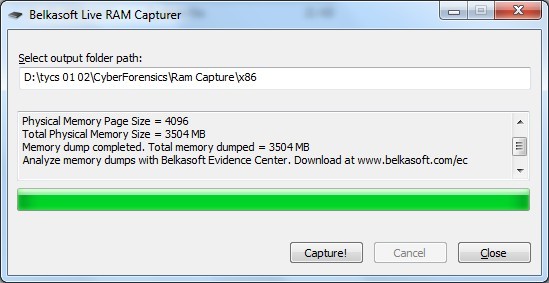
* + **Capture RAM (Tool:RAMCapture)**

**To Do:**

* 1. Click Capture
  2. Creates a .mem file of the system memory (RAM)utilized.

## Output:



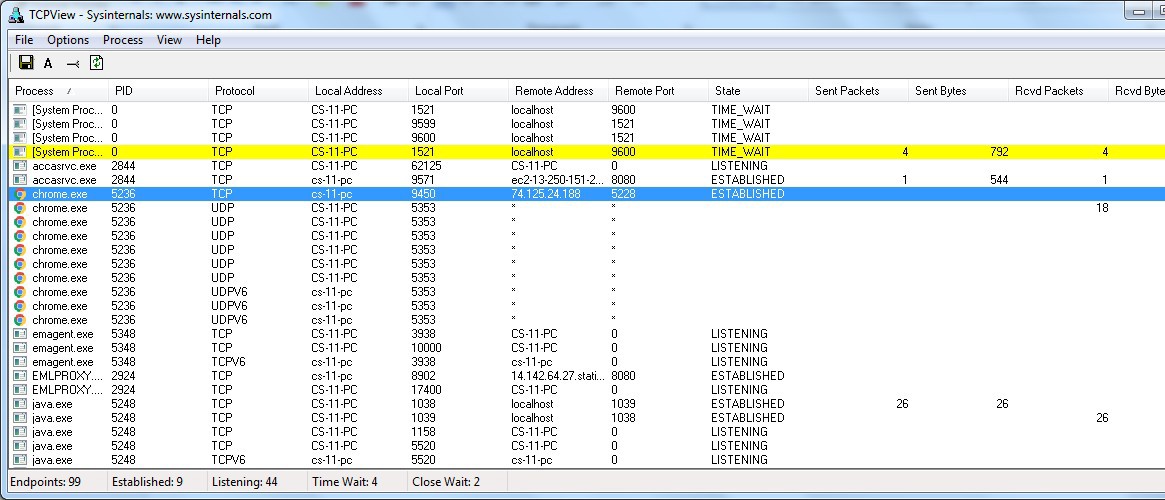


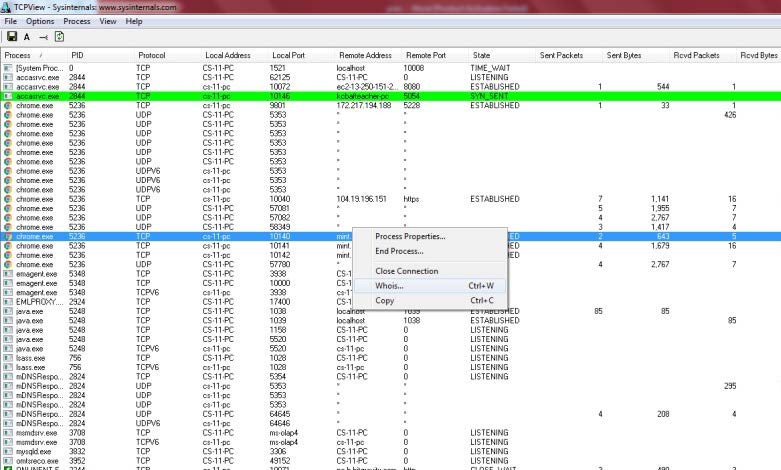
* + **Capture TCP/UDP packets (Tool: TcpView):**

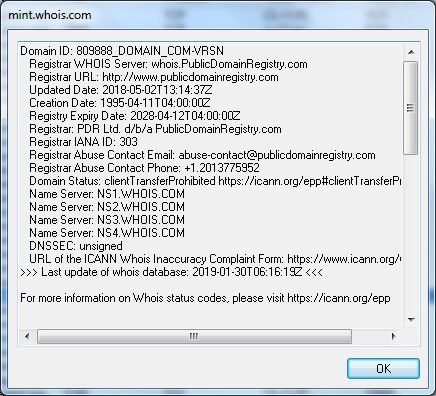
**ToDo:**1. Save to .txtfile.

2.Whois

## Output:





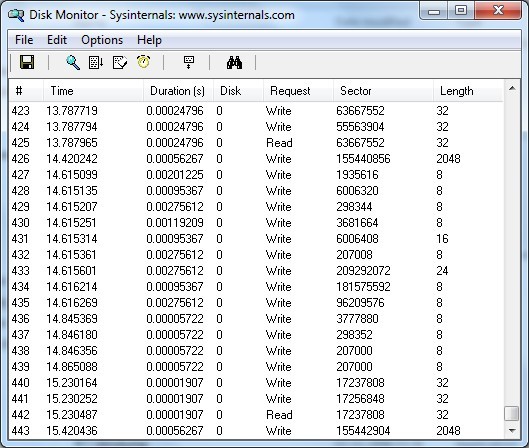


* + **Monitor Hard Disk (Tool: DiskMon):**

**To Do:**

1. Save to .logfile.
2. Check operations performed in the disk as per time and sectorsaffected.

## Output :

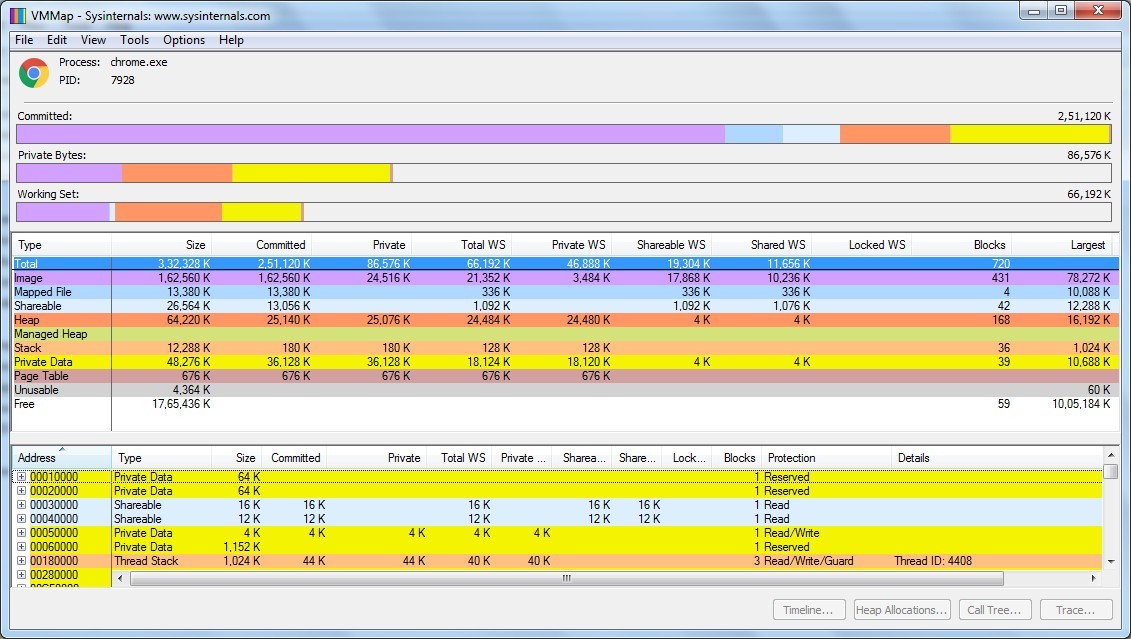


* + **Monitor Virtual Memory ( Tool : VMMAP):**

**To Do:**

1. Options – Show Free & UnusableRegions
2. File-> Select Process e.g.chrome.exe
3. Save to .mmpfile.

## Output :



* + **Monitor Cache Memory (Tool:RAMMap)**

**TO DO :**

* 1. Save to .RMPfile.

## Output:

