**Practical No. 1**

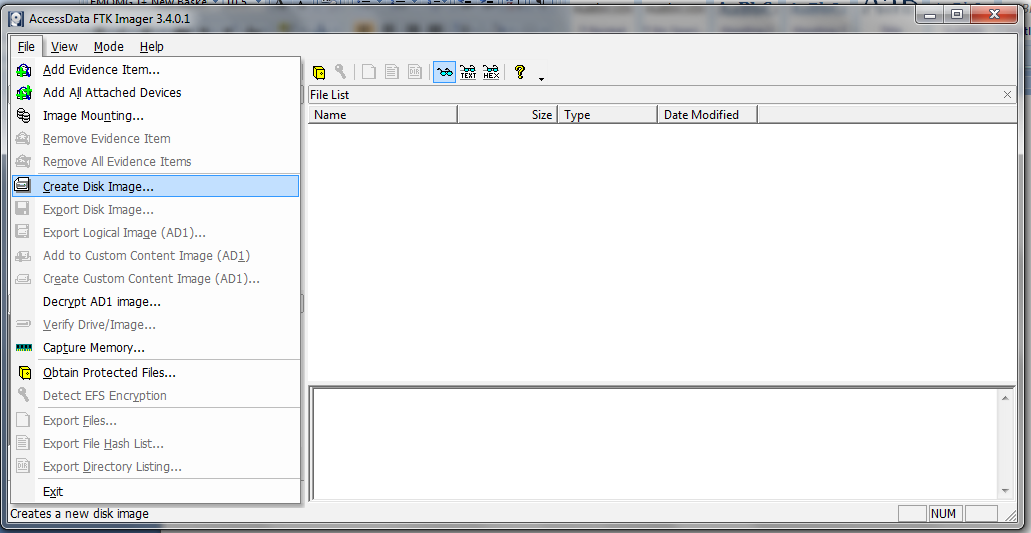
**Aim :-** Creating a Forensic Image using FTK Imager/Encase Imager

1. **Creating Forensic Images FTK :**

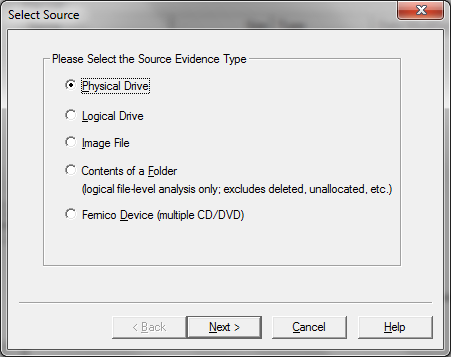
Imager allows you to write an image file to a single destination or to simultaneously write multiple image files to multiple destinations.

To create a forensic image:

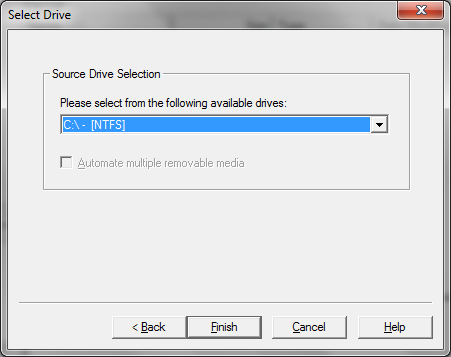
1. Click File, and then Create Disk Image, or click the button on the tool bar.



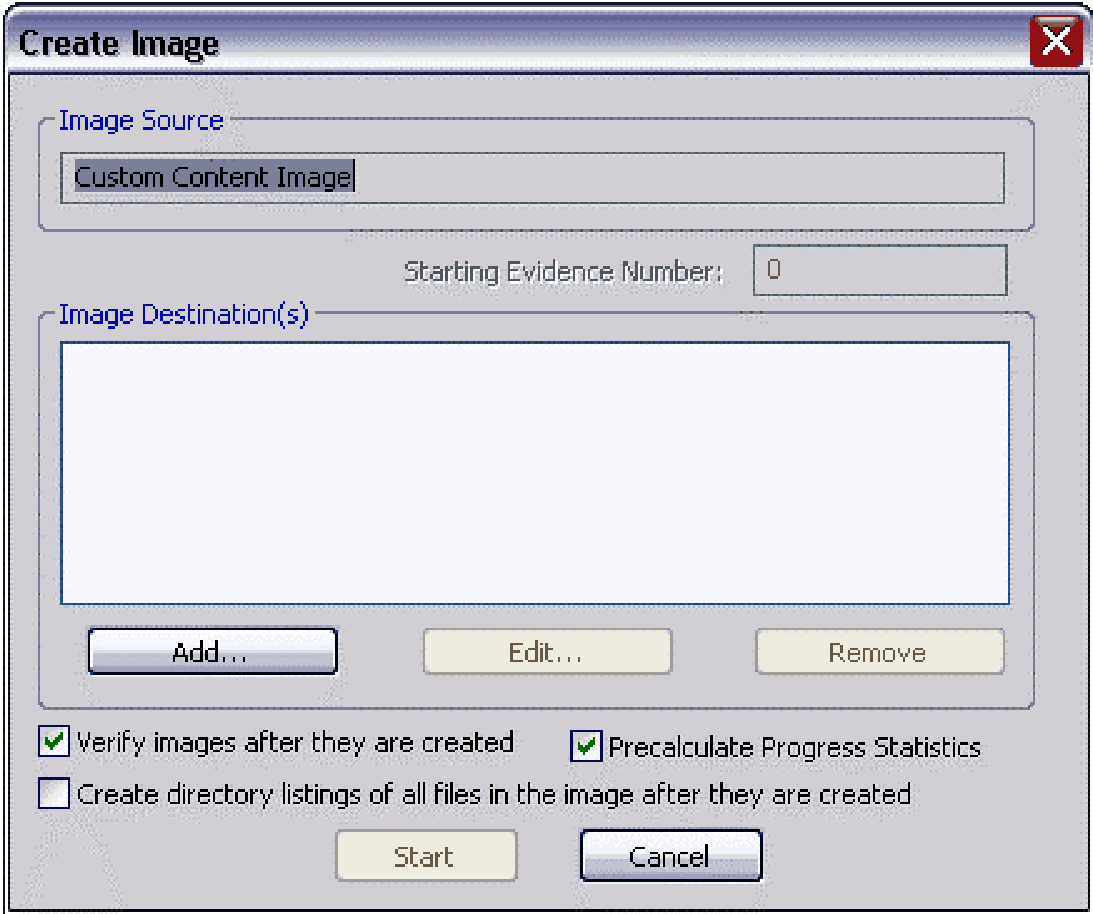
2. Select the source you want to make an image of and click Next.



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

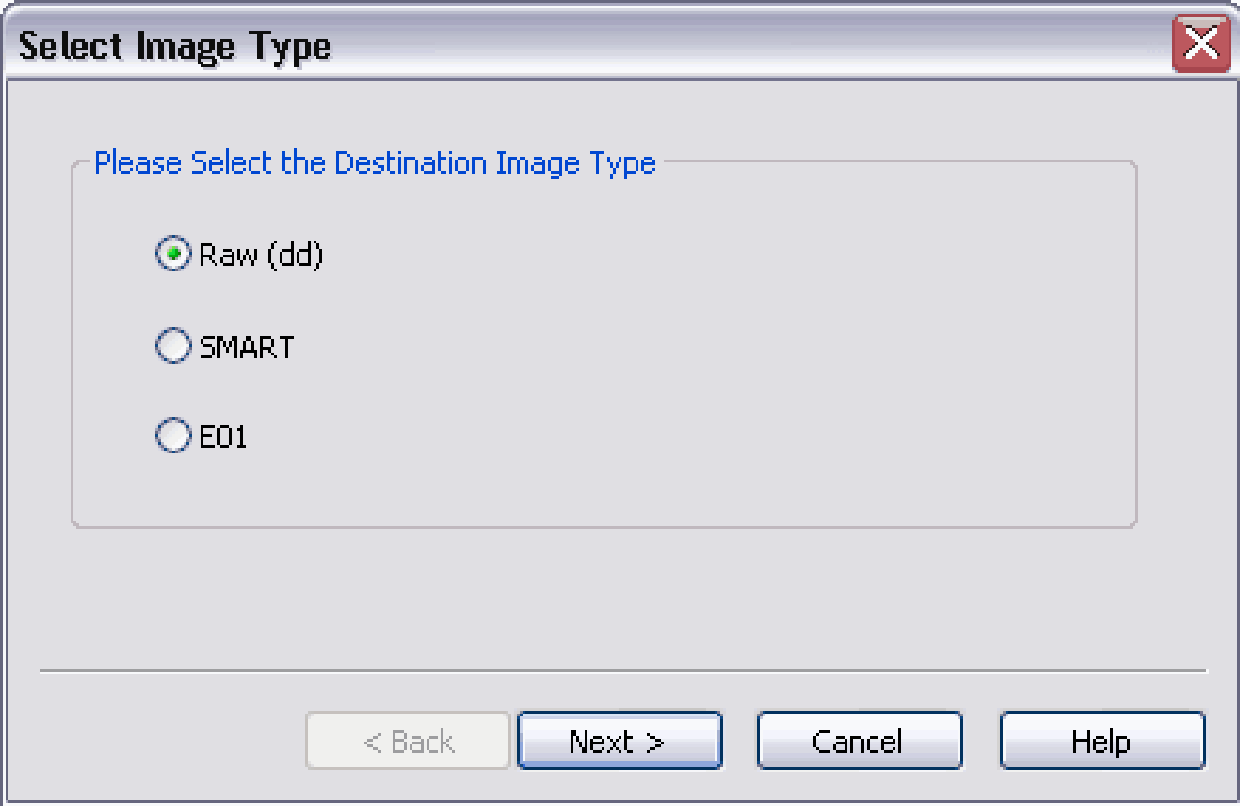


1. In the Create Image dialog, click Add.

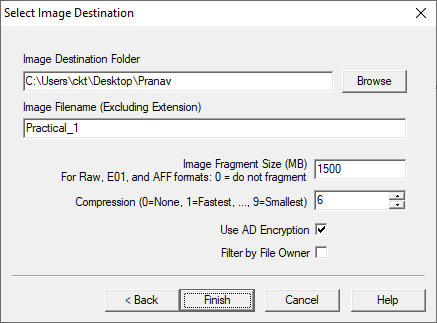


1. Select the type of image you want to create, and then click Next.

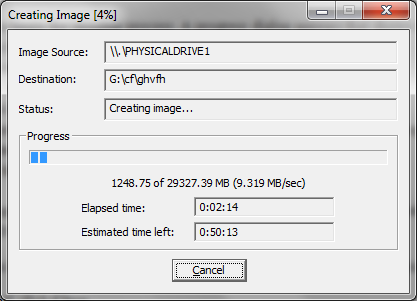
**Note:** If you are creating an image of a CD or DVD, this step is skipped because all CD/DVD images are created in the IsoBuster CUE format.



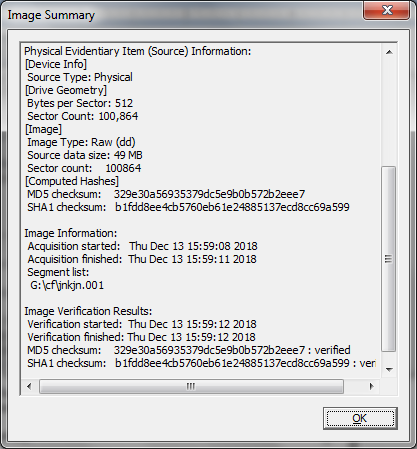
1. In the Image Destination Folder field, type the location path where you want to save the image file, or click **Browse** to find to the desired location.



1. In the Image Filename field, specify a name for the image file but do not specify a file extension.
2. 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.
3. Click **Finish**. You return to the Create Image dialog.
4. 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.**
5. 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



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

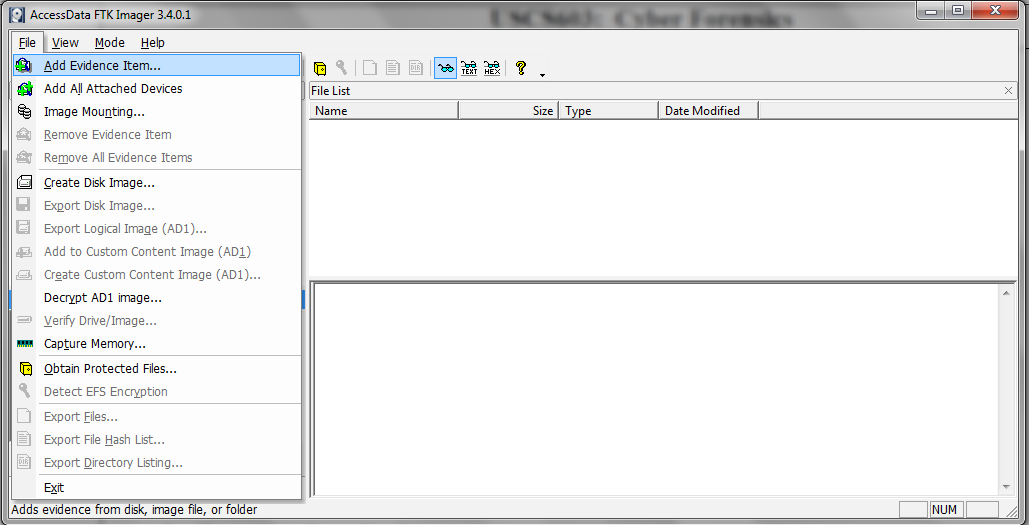


1. When finished, click **Close**

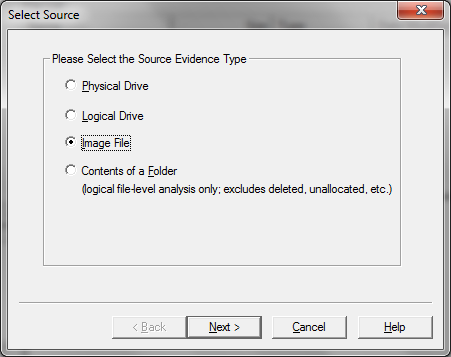
**Practical No. 2**

**Aim:** Analyze Forensic Image

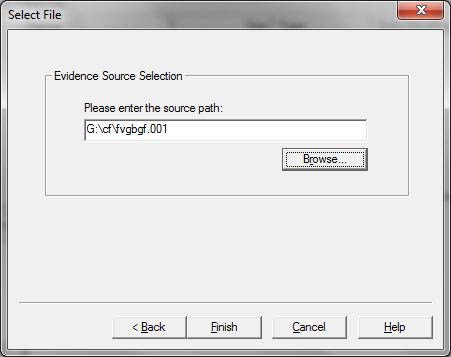
1. Click on Add Evidence Item to add evidence from disk, image file or folder.



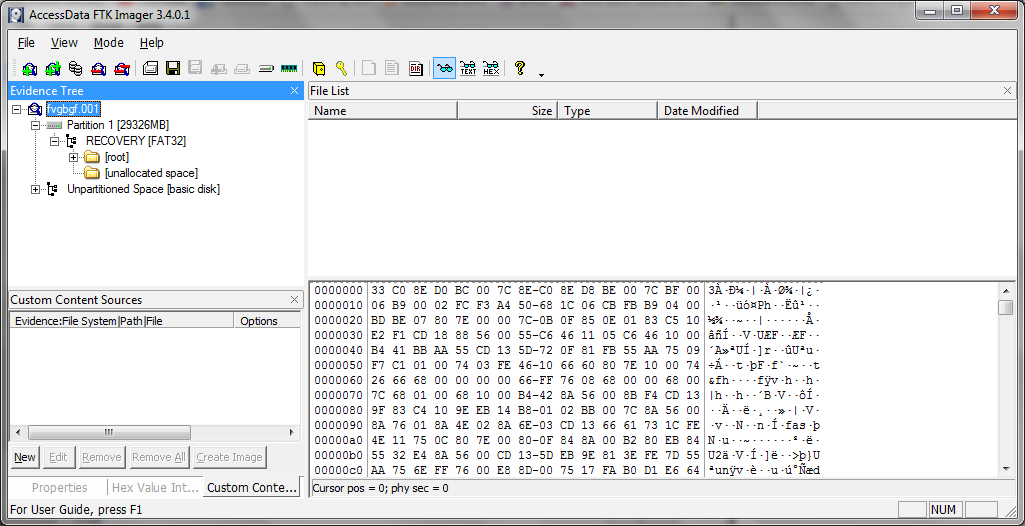
1. Now select the source evidence type as physical drive, logical drive or image file. We have selected image file and click on next.



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



1. 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.

1. Click on finish.
2. Now raw images will be added as a physical drive to analyze.

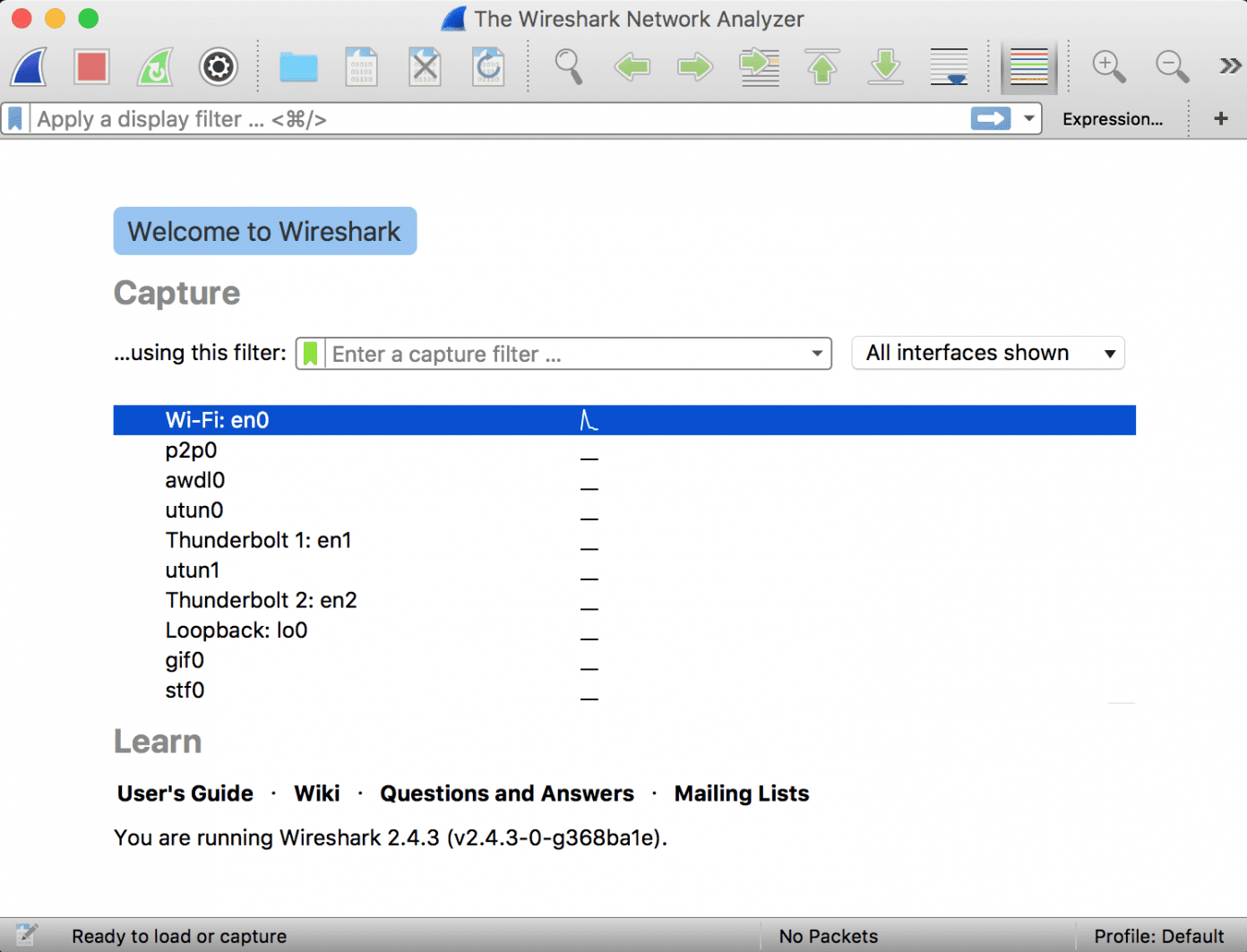
**Practical No. 4**

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

1. **Capturing Packets :**

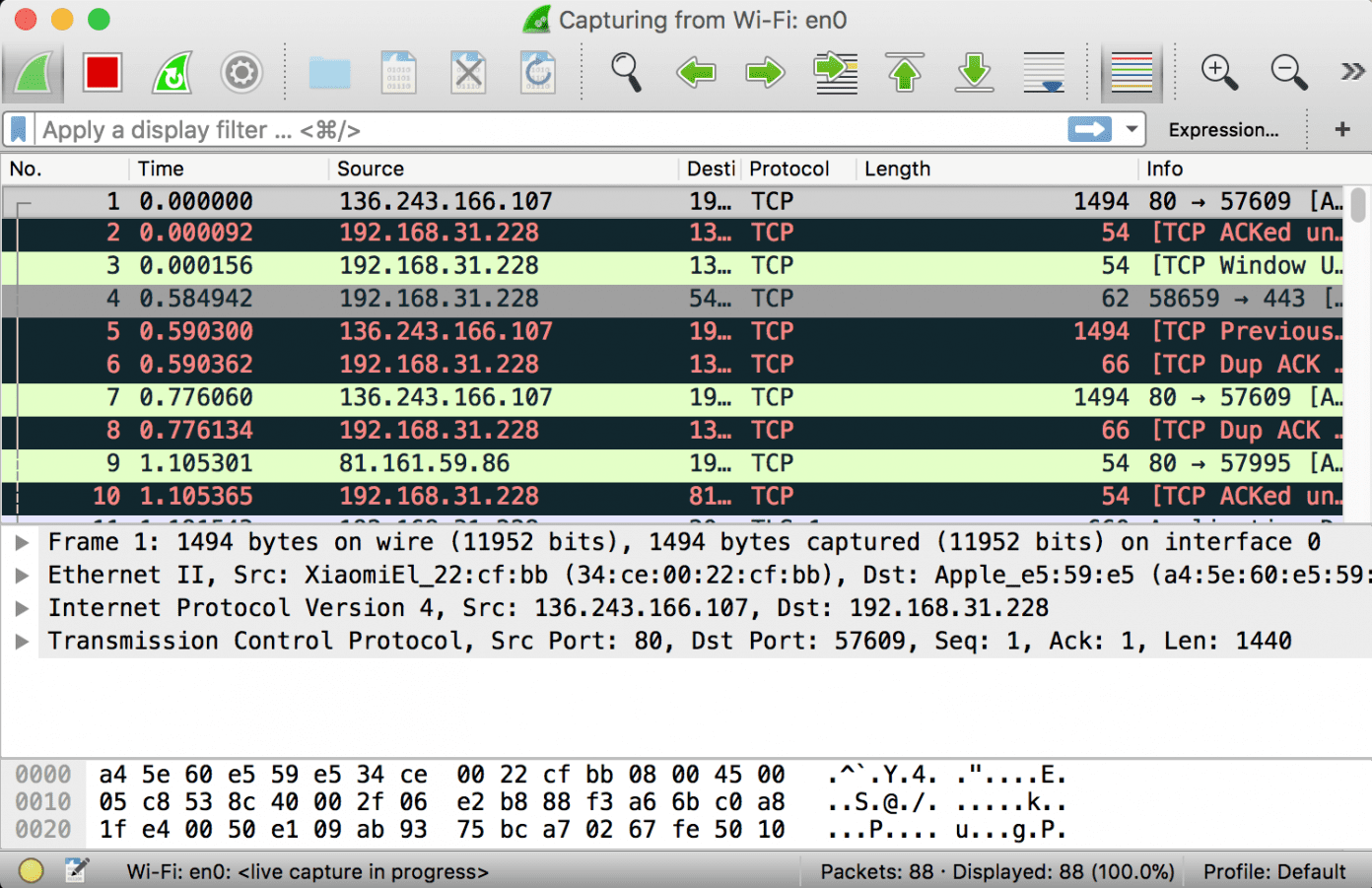
Capture traffic on your wireless network, click your wireless interface.

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



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.

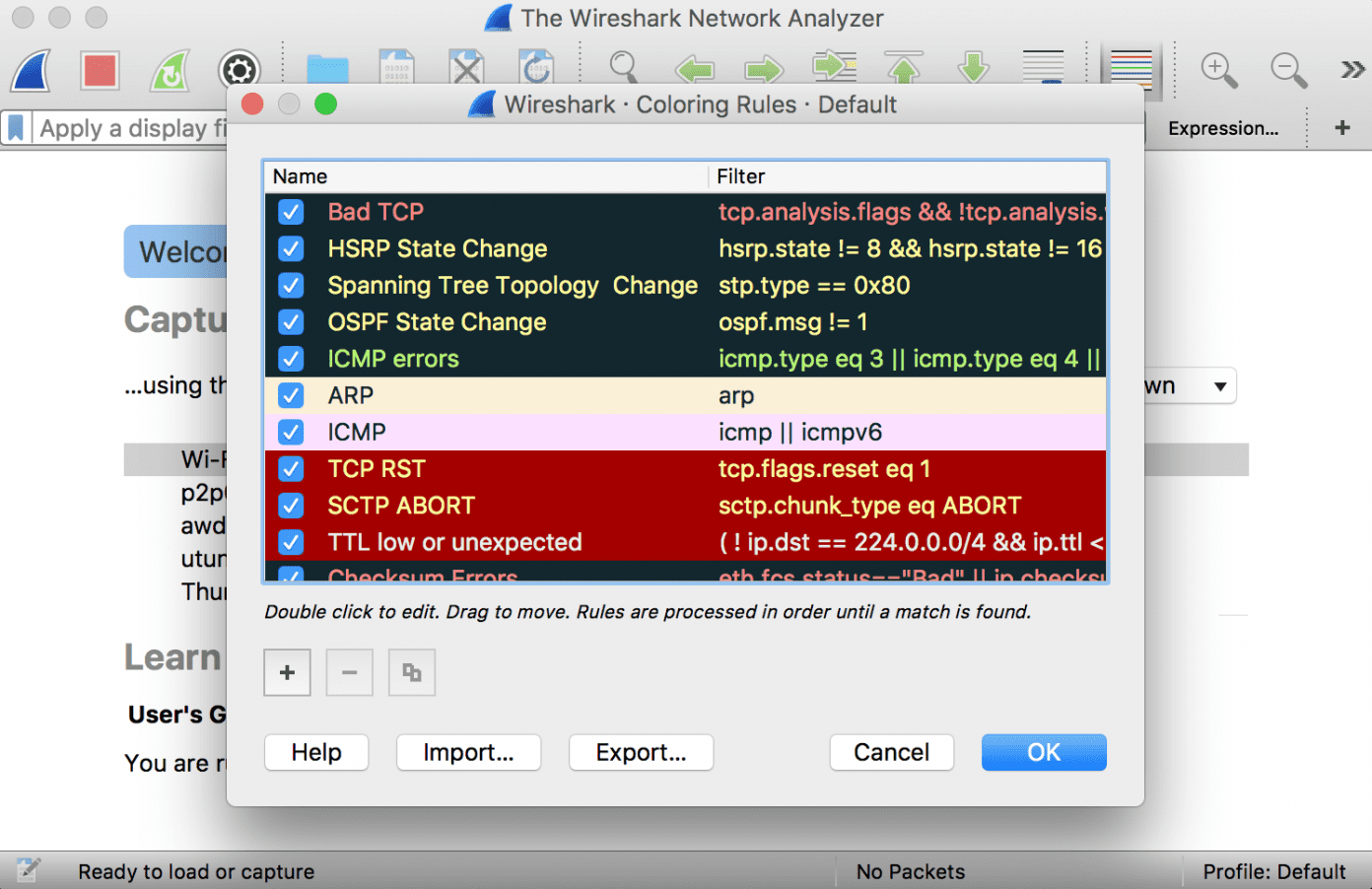
1. **Color Coding :**

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:

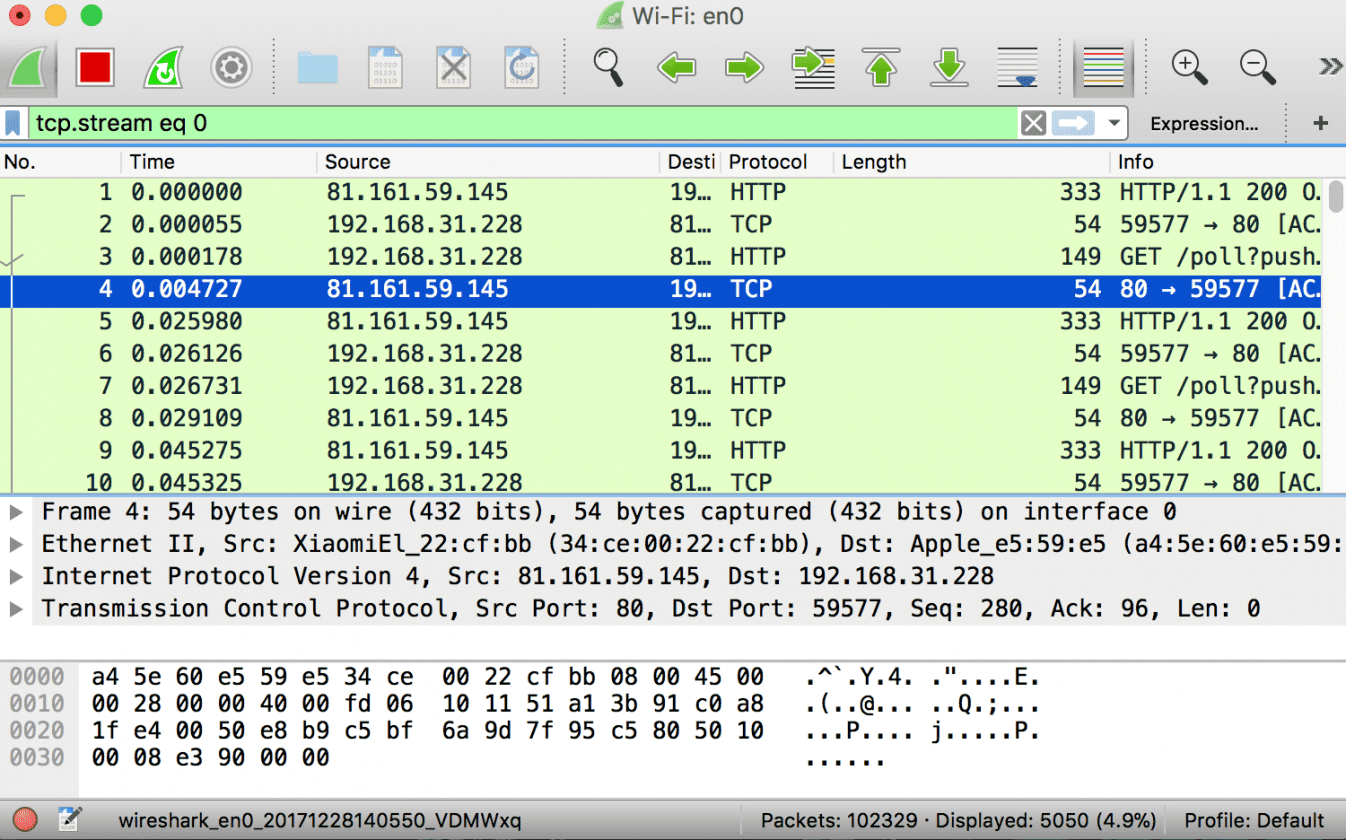
* Light Purple color for TCP traffic
* Light Blue color for UDP traffic
* Black color identifies packets with errors – example these packets are delivered in an unordered manner.

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.

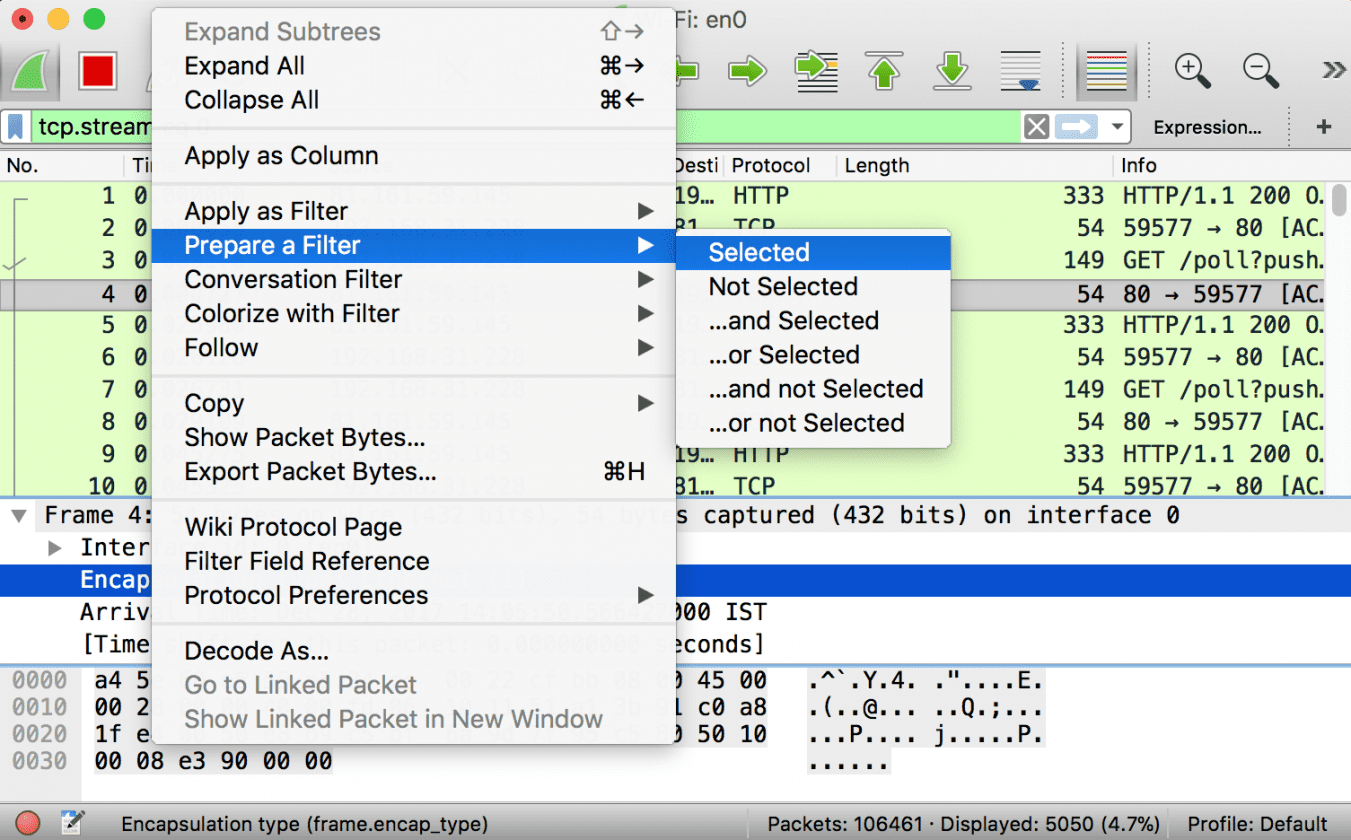


1. **Analyze the captured Packets:**

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.



**Practical No. 5**

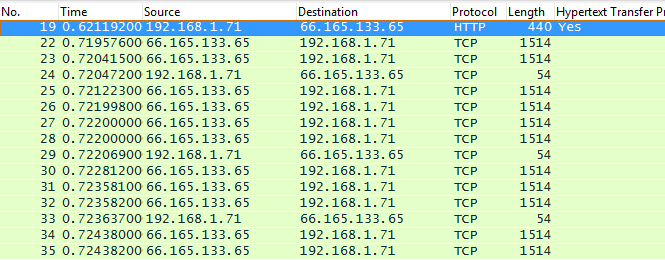
**Aim:-** Analyze the packets provided in lab and solve the questions using Wireshark :

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

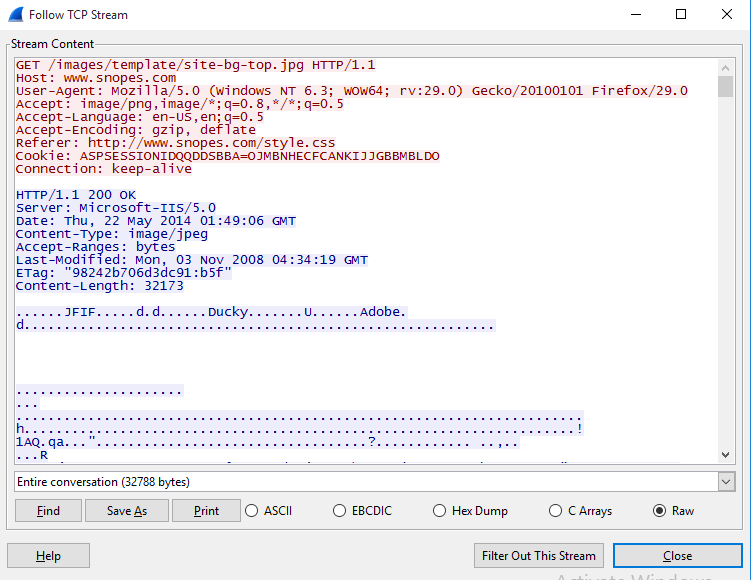
The domain name be found from host header so we will set host header column where we will see all domain name

Open Wireshark 🡪 file 🡪 open 🡪 Asksnopes.pcapng

Select any http 🡪 right click 🡪 Apply as Column



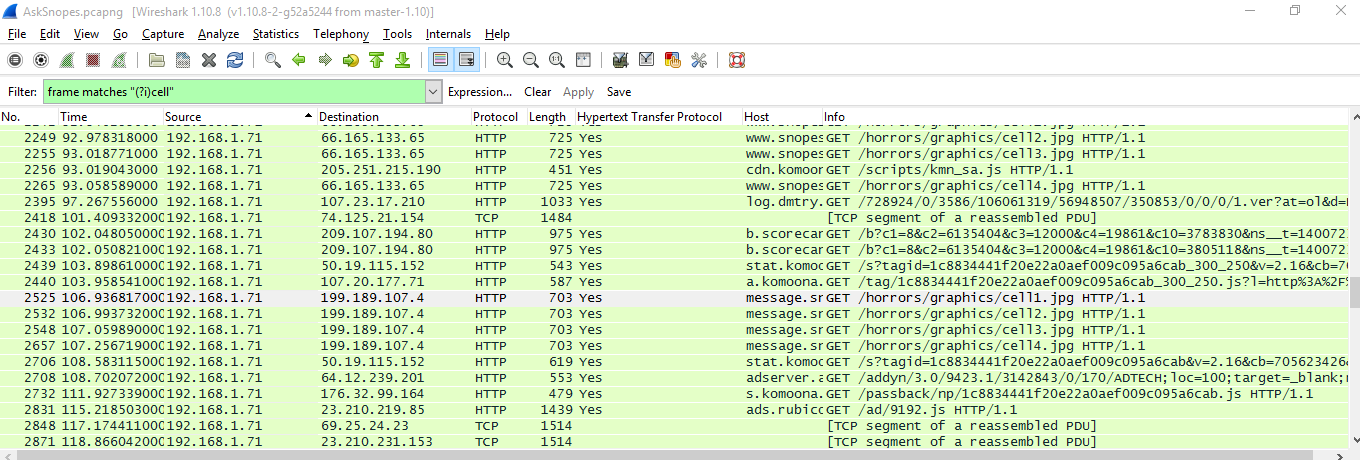
select http file 🡪 right click 🡪 follow TCP Stream



1. **About what cell phone problem is the client concerned?**

Client talking about cell so we search for cell keyword in whole packets.

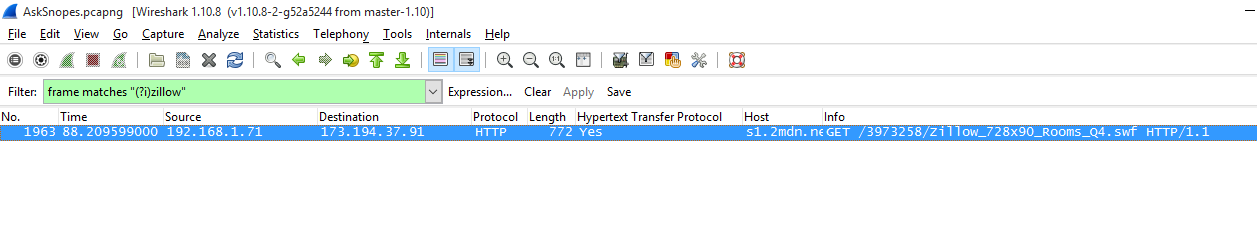
frame.matches “(?i)cell

****

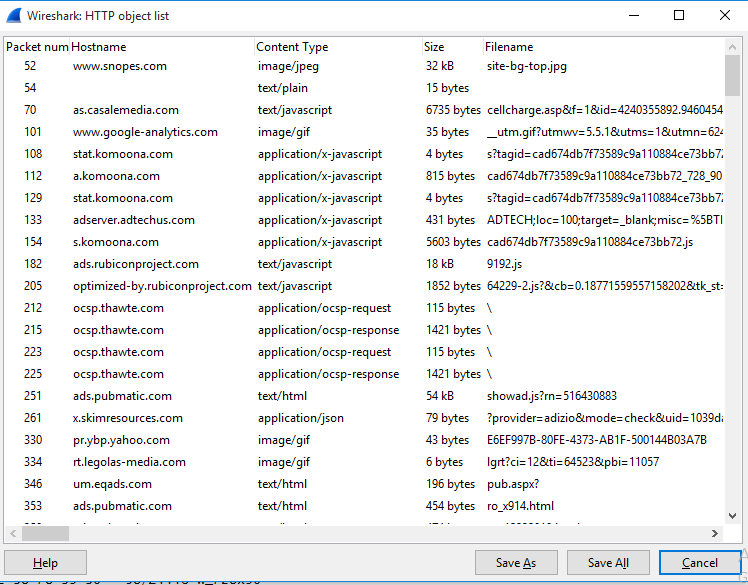
In the first HTTP request cell keyword is in URL and it was about cell phone charging issue.

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

frame.matches “(?i)zillow”

****

Open file 🡪 Export Object 🡪 HTTP 🡪 save All 🡪 select the folder to save

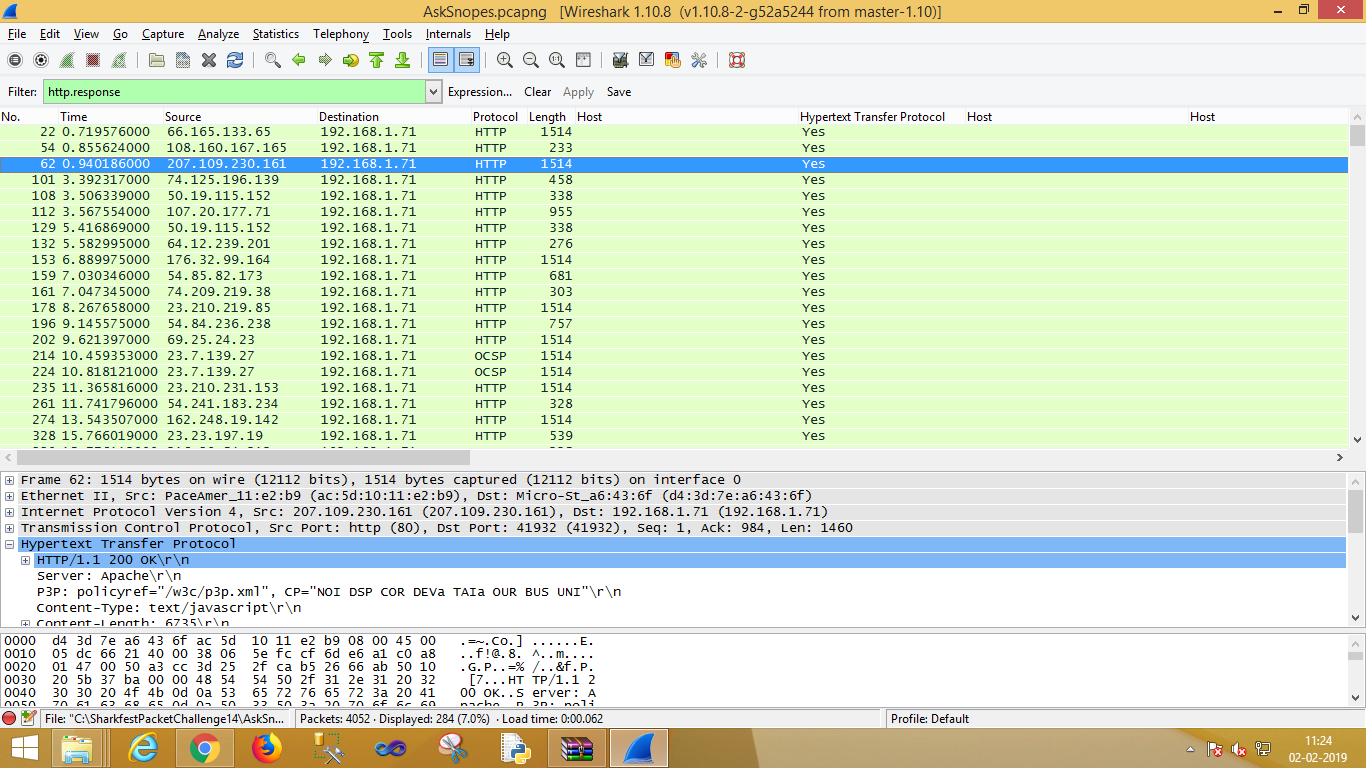


Open the folder 🡪 search for the file name zillow 🡪 open with browser



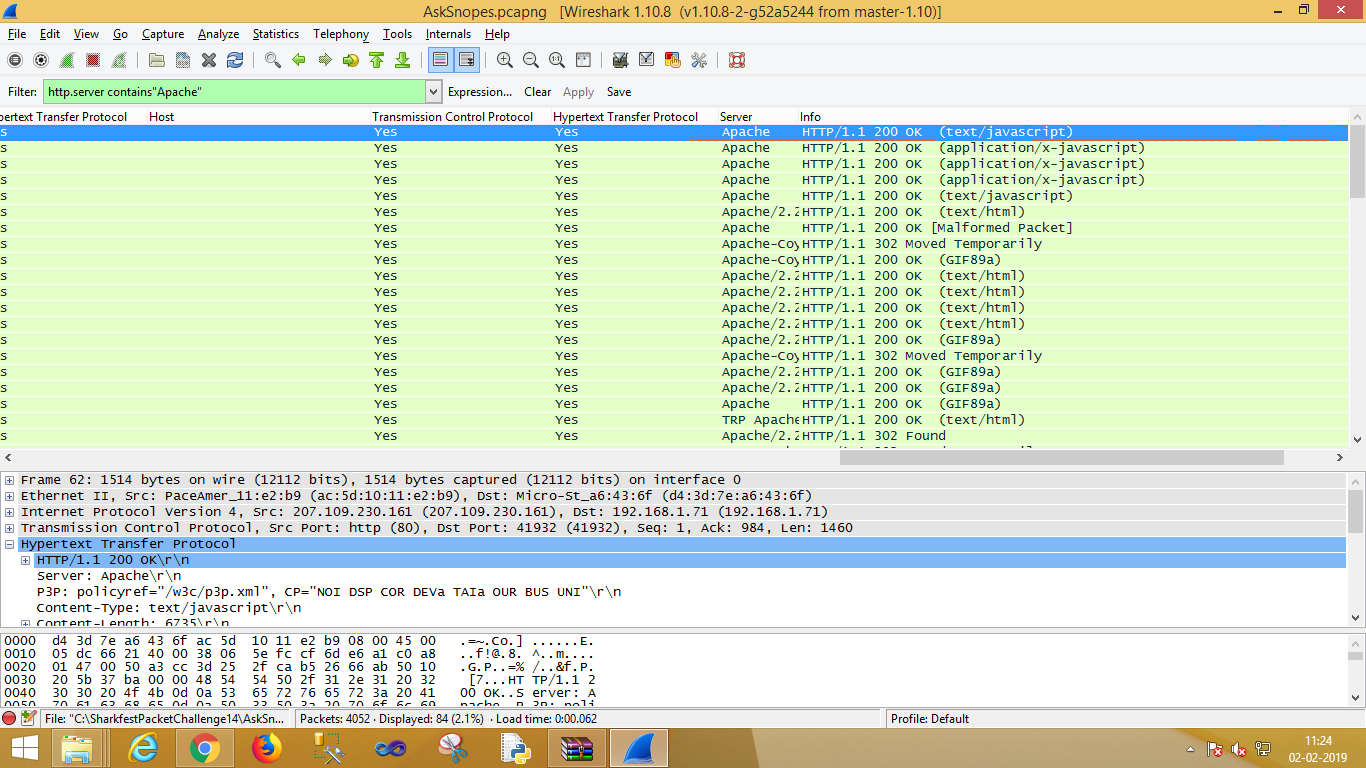
1. **How many web servers are running Apache?**

http.response

****

Select http 🡪 apply as column

http.server contains “Apache”

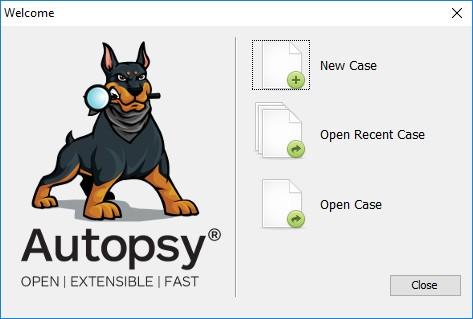
****

**Practical No. 6**

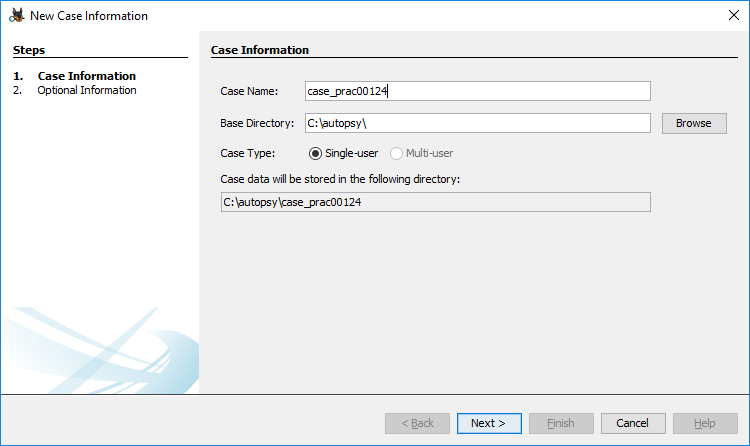
**Aim:-** Forensics Case Study: Solve the Case study (image file) provide in lab using Encase Investigator or Autopsy

**Step 1: Open Autopsy**

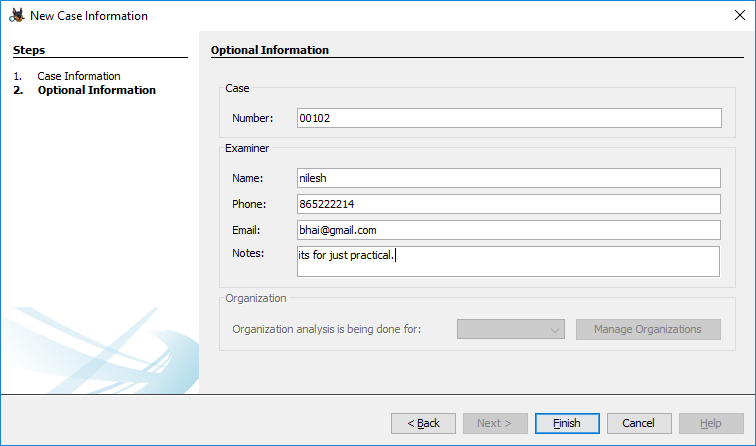
**Step 2: Click on new case**



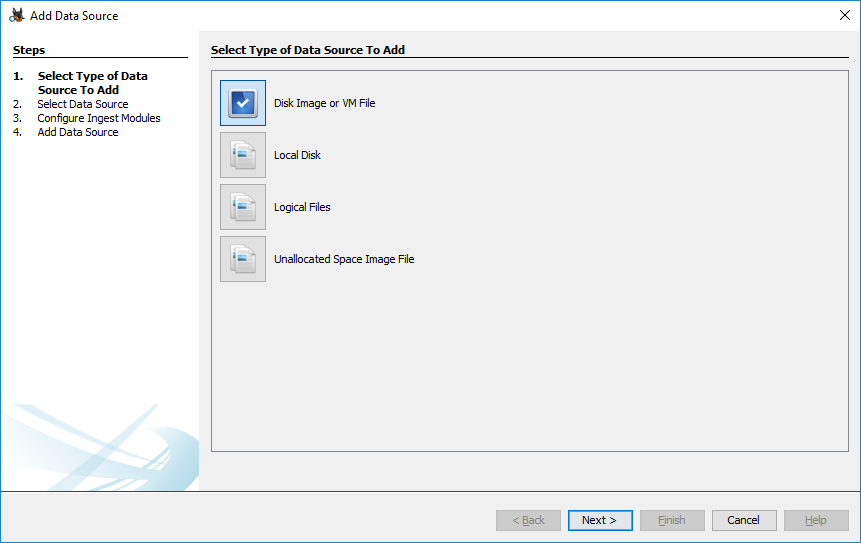
**Step 3: Enter details regarding the case and click on next button.**



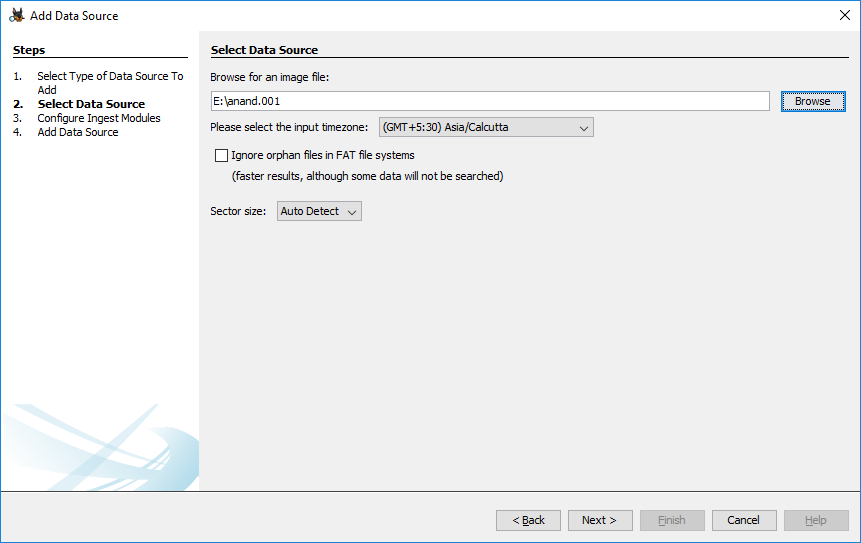
**Step 4: Enter further details and click on next button**



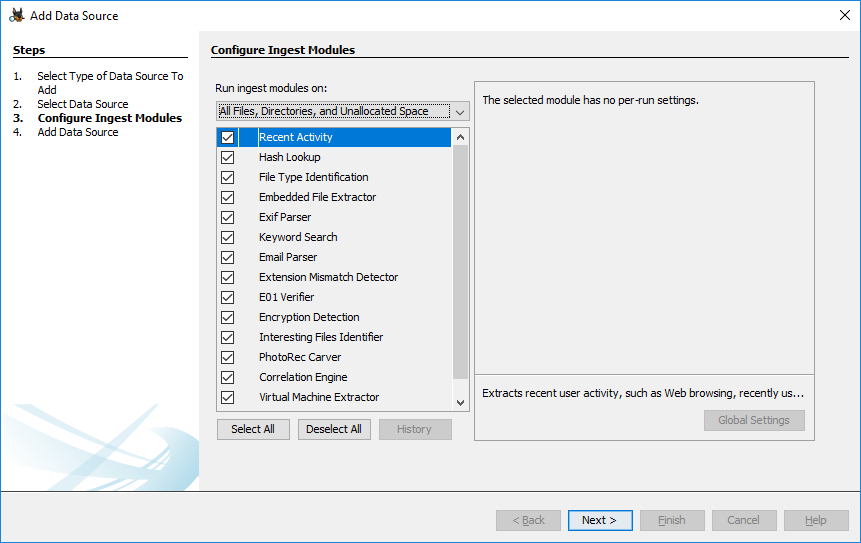
**Step 5: Now here we have to select Type of data source to add , in our case disk image or VM file and click on next**



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

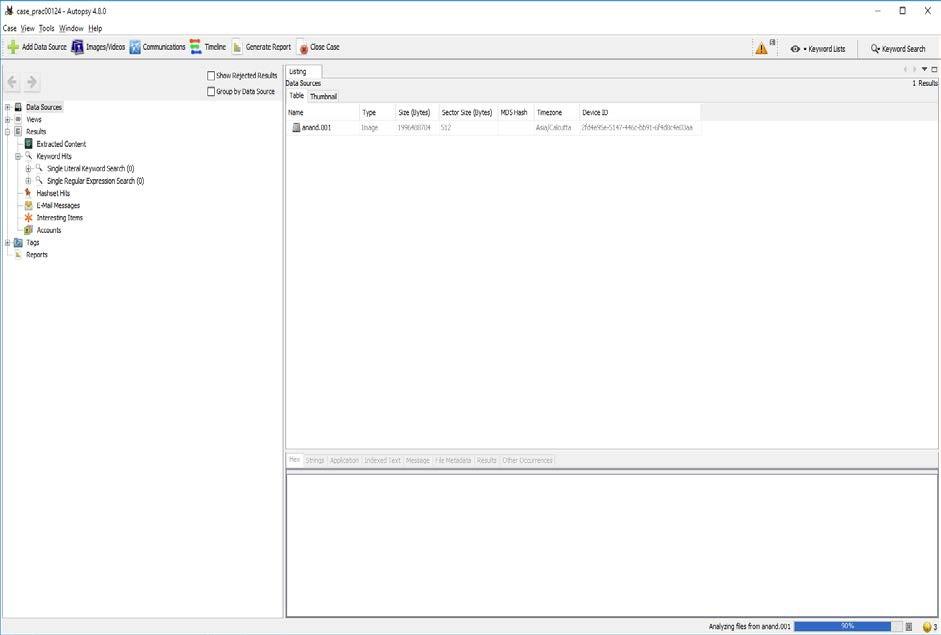


**Step 7: Now click on select all in order to Run ingest modules on: and click on next**.

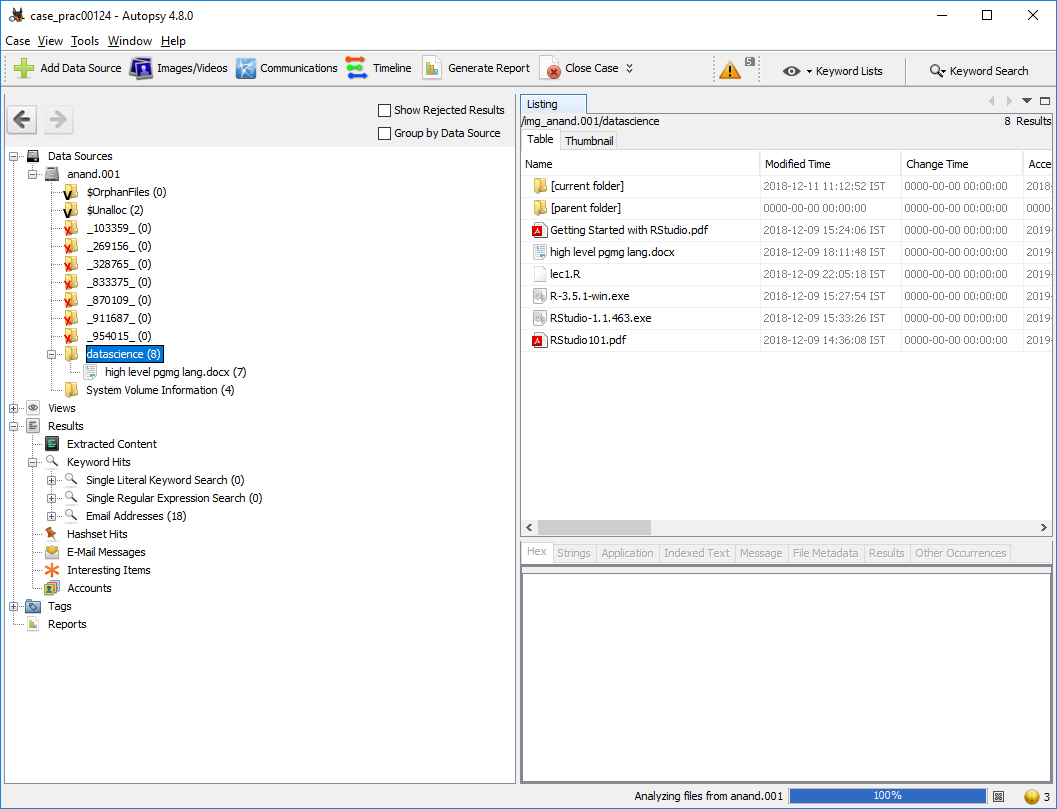


**Step 8: Now click on finish**

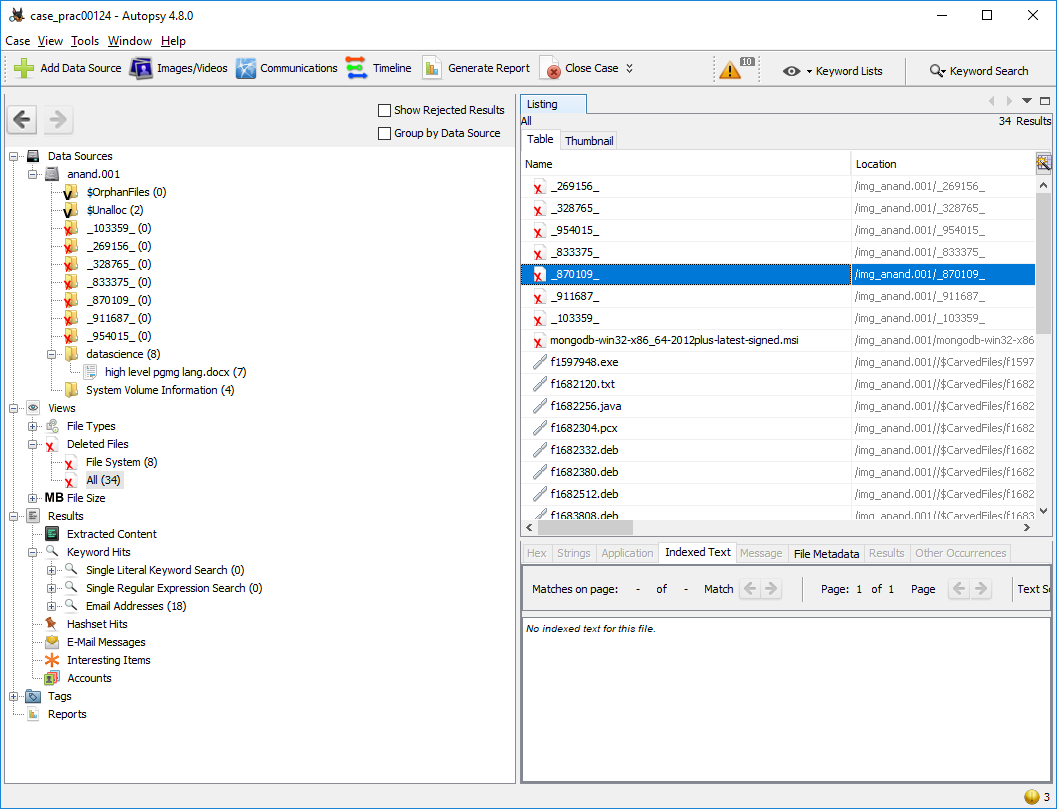
**Step 9: Now Autopsy window will appear and it will analyse the disk that we have selected .**



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



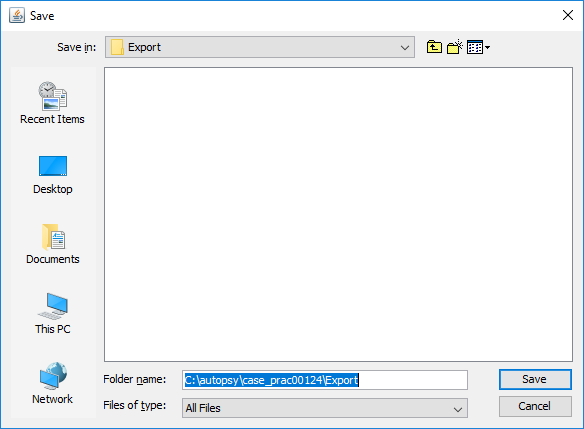
**Step 11: Expand the tree from left side panel to view the document files.**



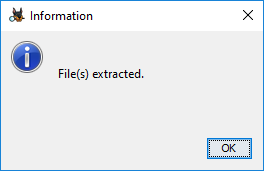
**Step 12: To recover the files , go to view code 🡪 Deleted files node , here select any file and right click on it then select Extract files option**



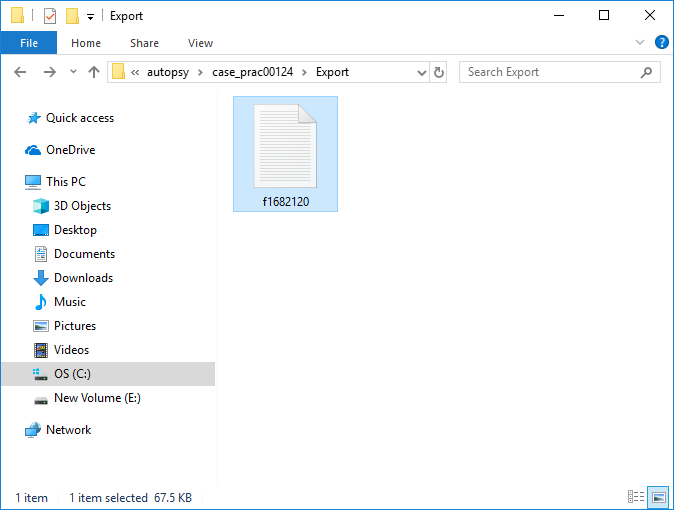
**Step 13: Select Path where you want to save extracted file and click on save .**



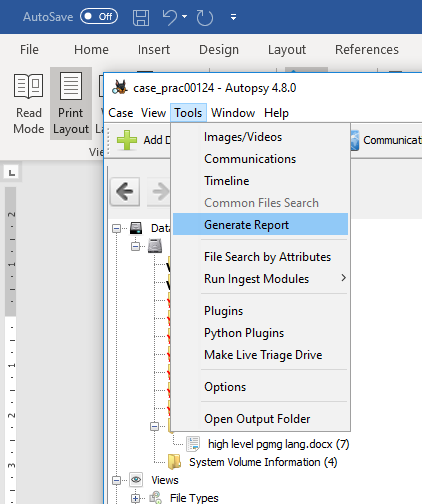
**Step 14 : Now click on OK**



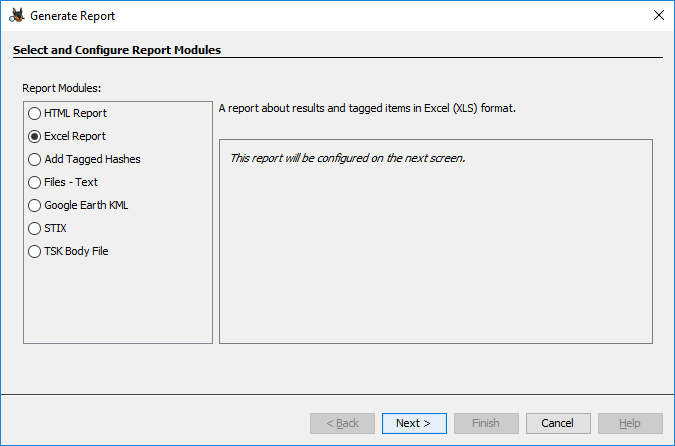
**Step 15 : Now go to C:\autopsy\case\_prac00124\Export folder to see recover file**



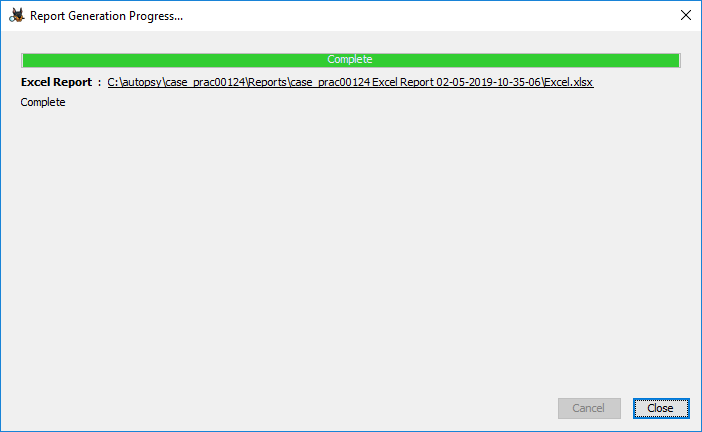
**Step 16 : Click on generate report from Autopsy window and select the Excel format and click on next**



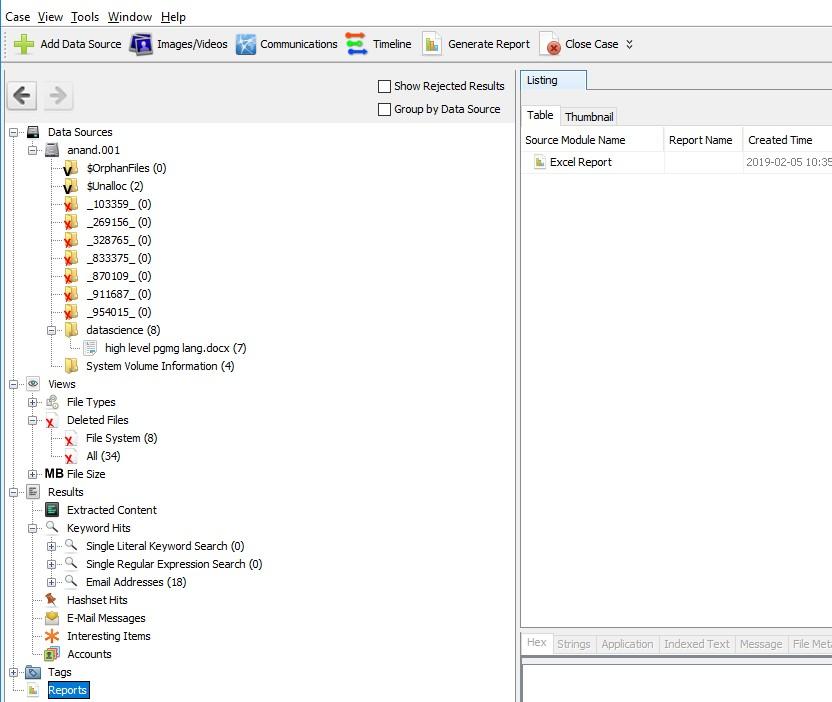
**Step 17 : This window will appear**



**Step 18 : Now report is generated so click on close button. We can see the Report on Report Node**



**Step 19 : Click on report**



**Practical No. 8**

**Aim :-** Using Sysinternals tools for Process Monitoring

* + - 1. **Monitor Live Processes : (Tool: ProcMon)**

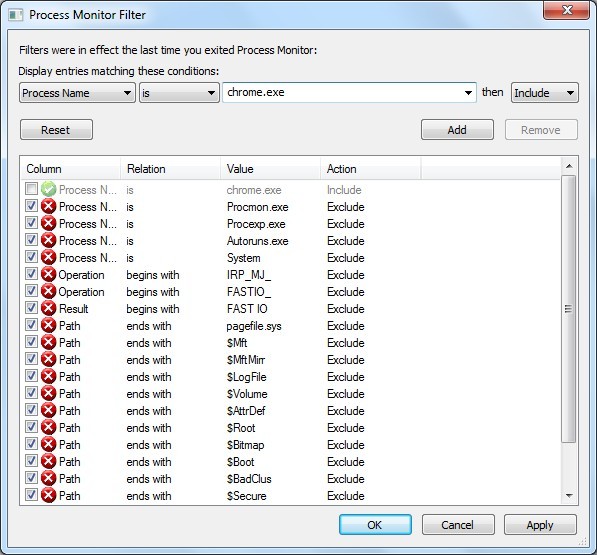
To Do:

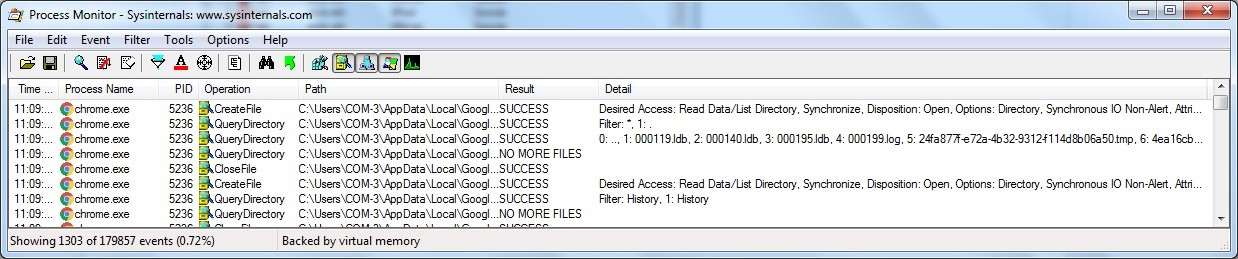
Filter (Process Name or PID or Architecture, etc)

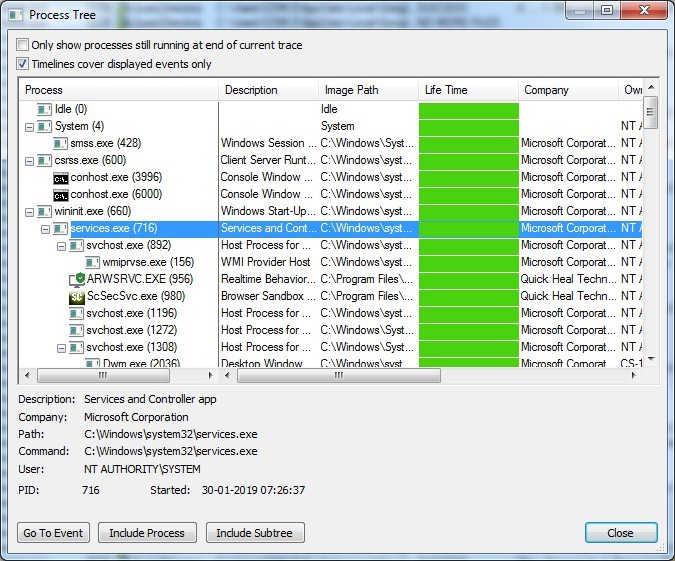
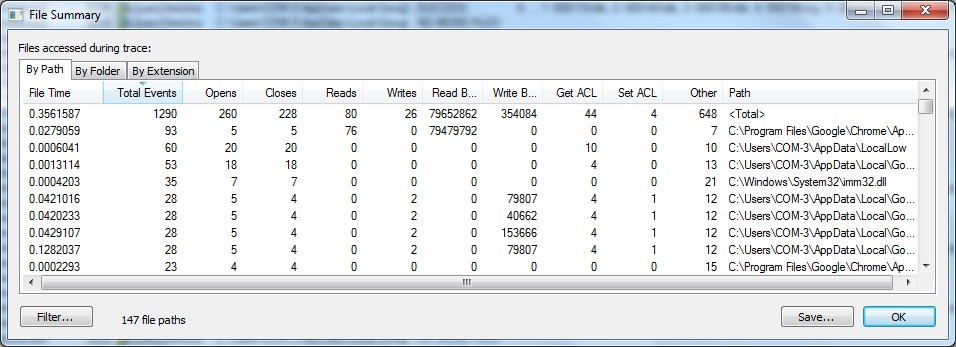
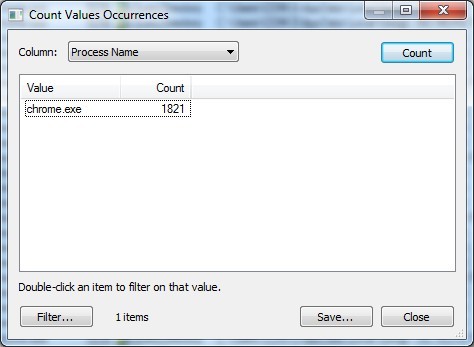
Process Tree

Process Activity Summary Count Occurrences

**Output**





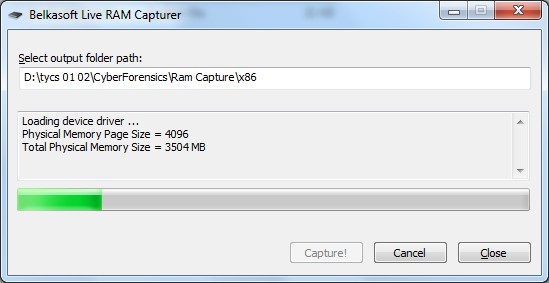


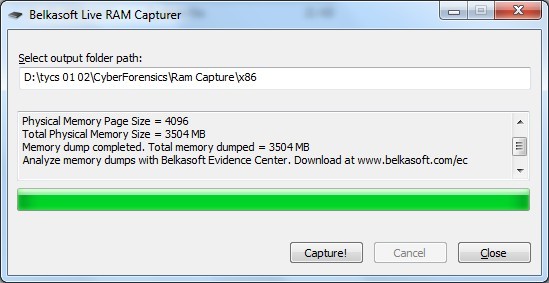
* + - 1. **Capture RAM (Tool: RAMCapture)**

Click Capture

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

**Output**





**Practical No. 9**

**Aim:** Network Tracking using Sysinternals tools

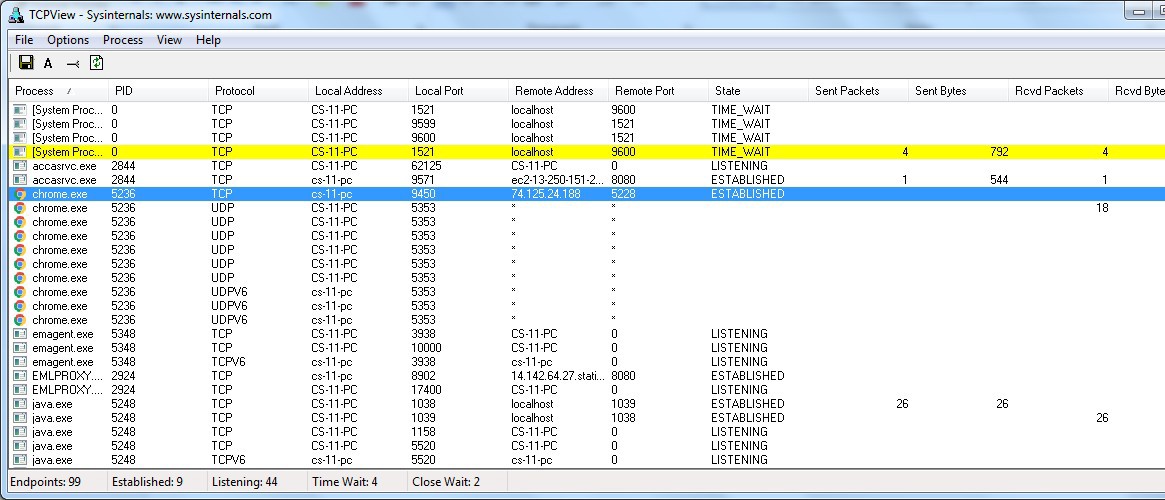
**Capture TCP/UDP packets (Tool: TcpView) :**

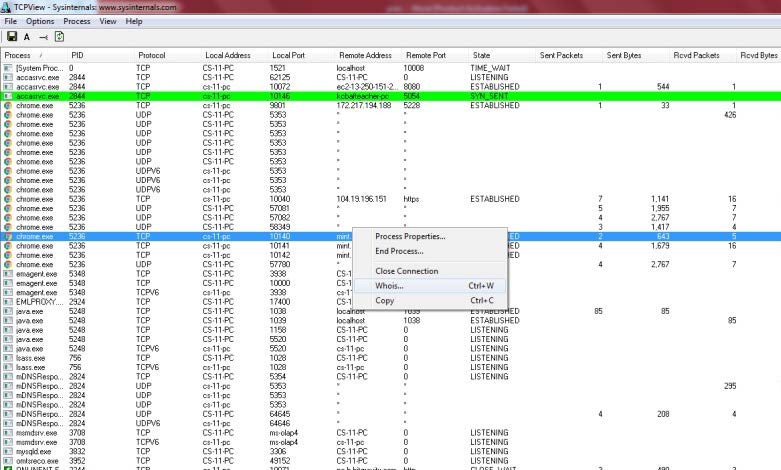
To Do:

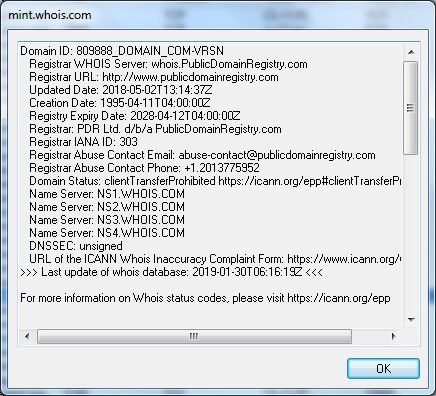
1.Save to .txt file.

2. Whois

**Output:**







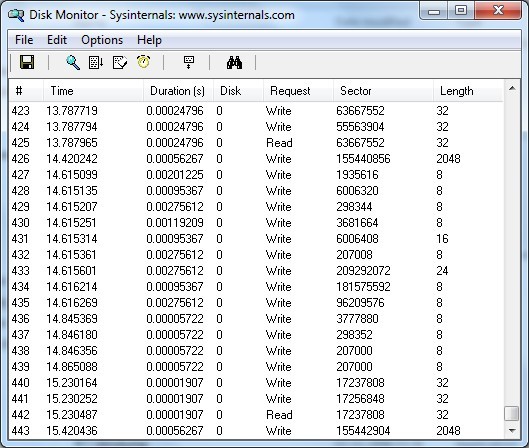
**Monitor Hard Disk (Tool: DiskMon) :**

To Do:

Save to .log file.

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

**Output :**



* + - 1. **Monitor Virtual Memory ( Tool : VMMAP) :**

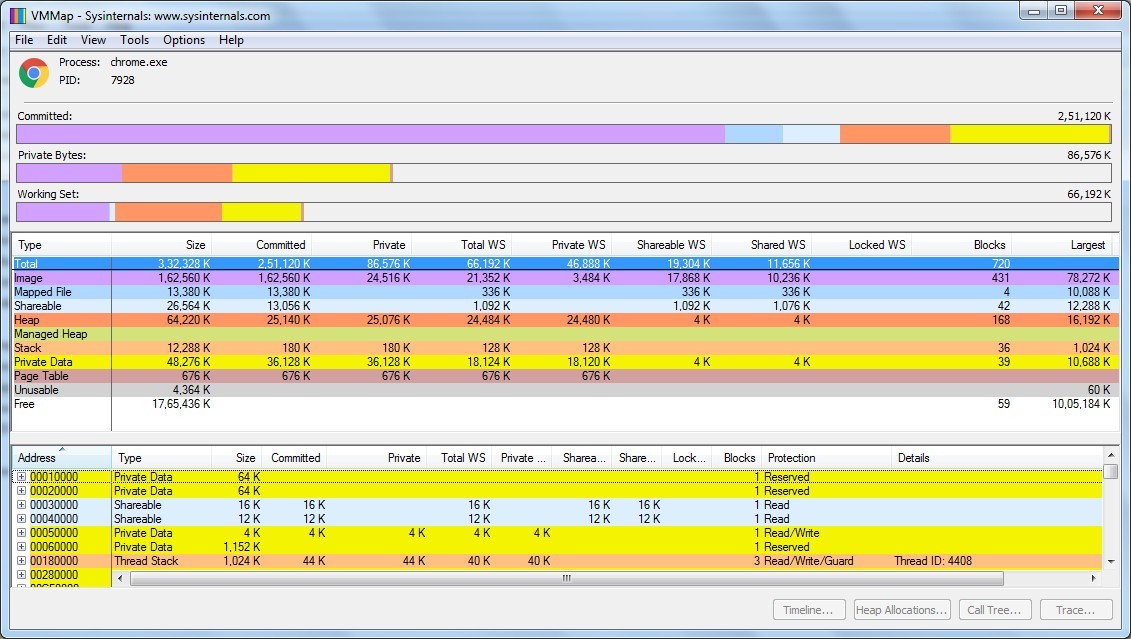
To Do:

Options – Show Free & Unusable Regions

File-> Select Process e.g. chrome.exe

Save to .mmp file.

**Output :**



1. **Monitor Cache Memory (Tool: RAMMap)**

TO DO :

Save to .RMP file.

**Output:**

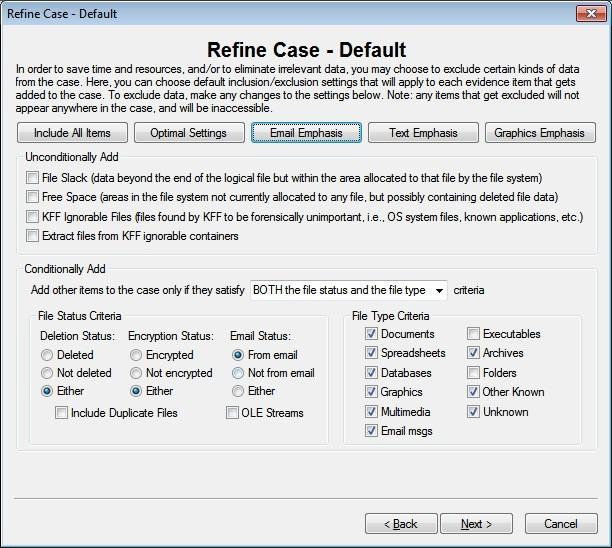
**Practical No. 11**

**Aim:-** Email Forensics

* Mail Service Providers
* Email protocols
* Recovering emails

**Code:**

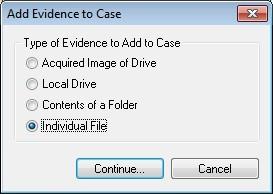
Start AccessData FTK and click **Start a new case**, then click **OK**. Click **Next** until you reach the **Refine Case - Default** dialog box Click the **Email Emphasis** button, and then click Next



Click **Next** until you reach the **Add Evidence to Case** dialog box, and then click the **Add Evidence** button.

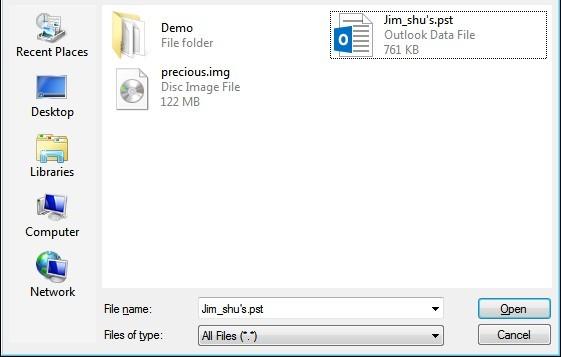
In the Add Evidence to Case dialog box, click the **Individual File**

option button, and then click **Continue**.

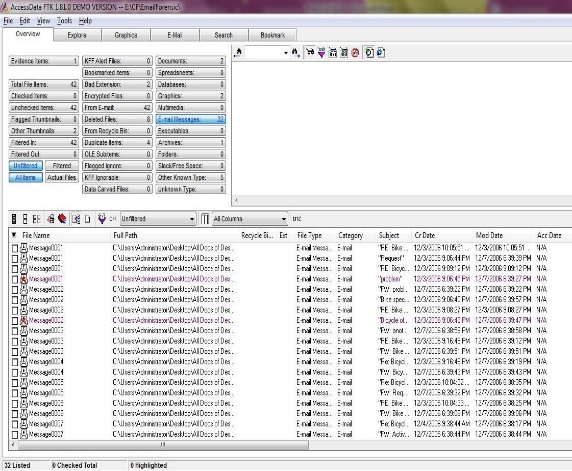


In the **Select File** dialog box, navigate to your work folder, click the

**Jim\_shu’s.pst file**, and then click **Open**.

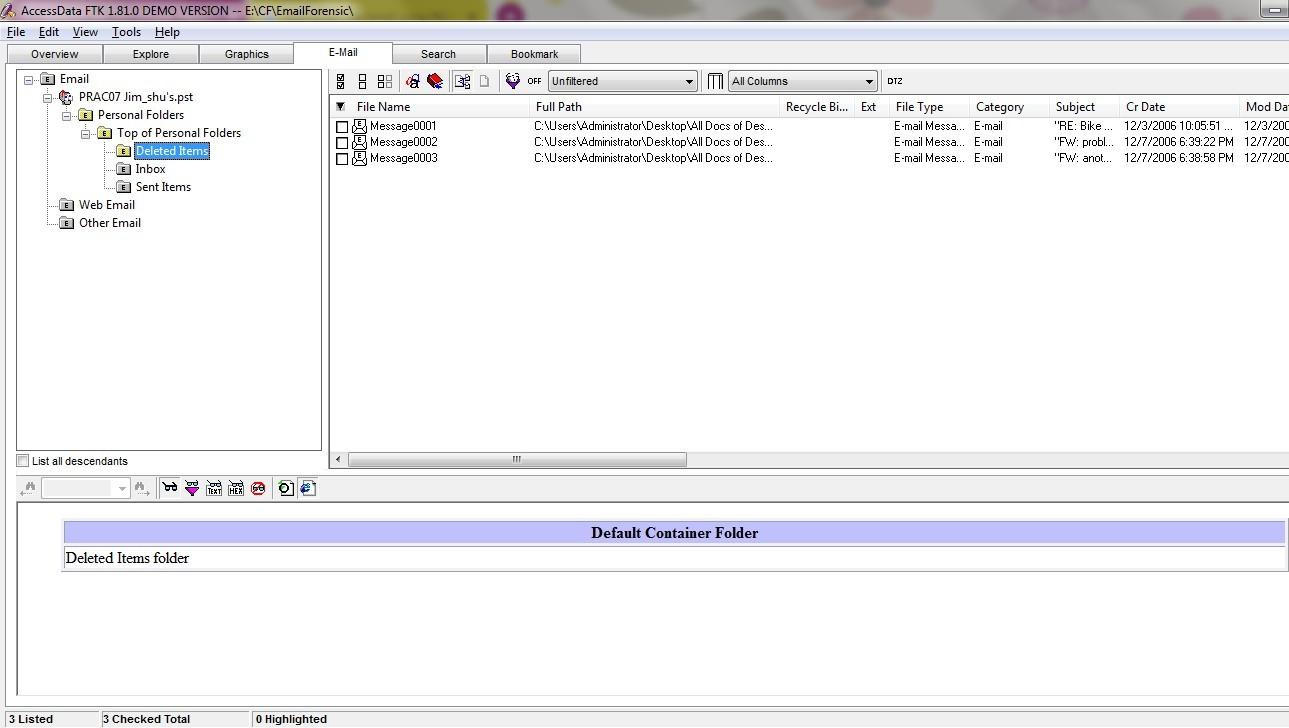


When the **Add Evidence to Case** dialog box opens, click **Next**. In the **Case summary** dialog box, click **Finish**.When FTK finishes processing the file, in the main FTK window, click the **E- mail Messages** button, and then click the **Full Path** column header to sort the records.

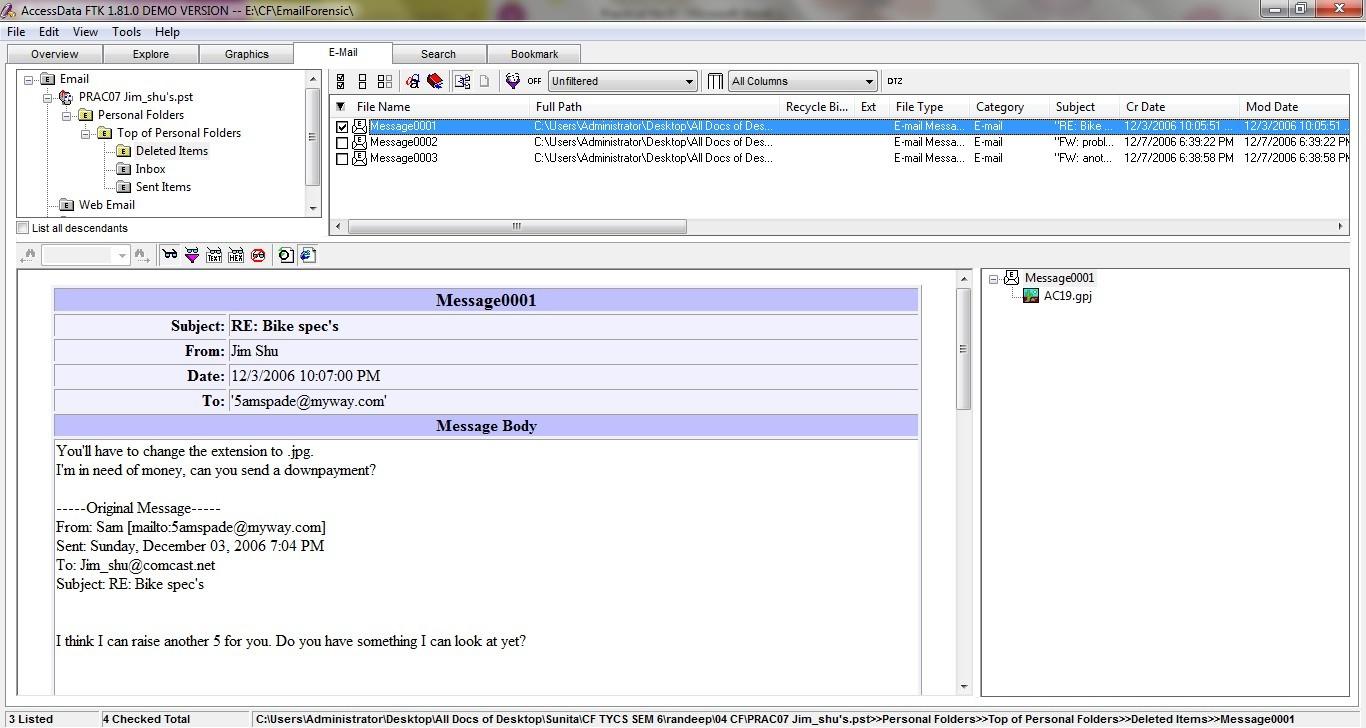


For email recovery follow following steps:

Click the **E-Mail** tab. In the tree view, click to expand all folders, and then click the **Deleted items folder**

.

Select any message say Message0001 right click and select option Launch. Detached Viewer and you can see detail of deleted message.



**Practical No. 12**

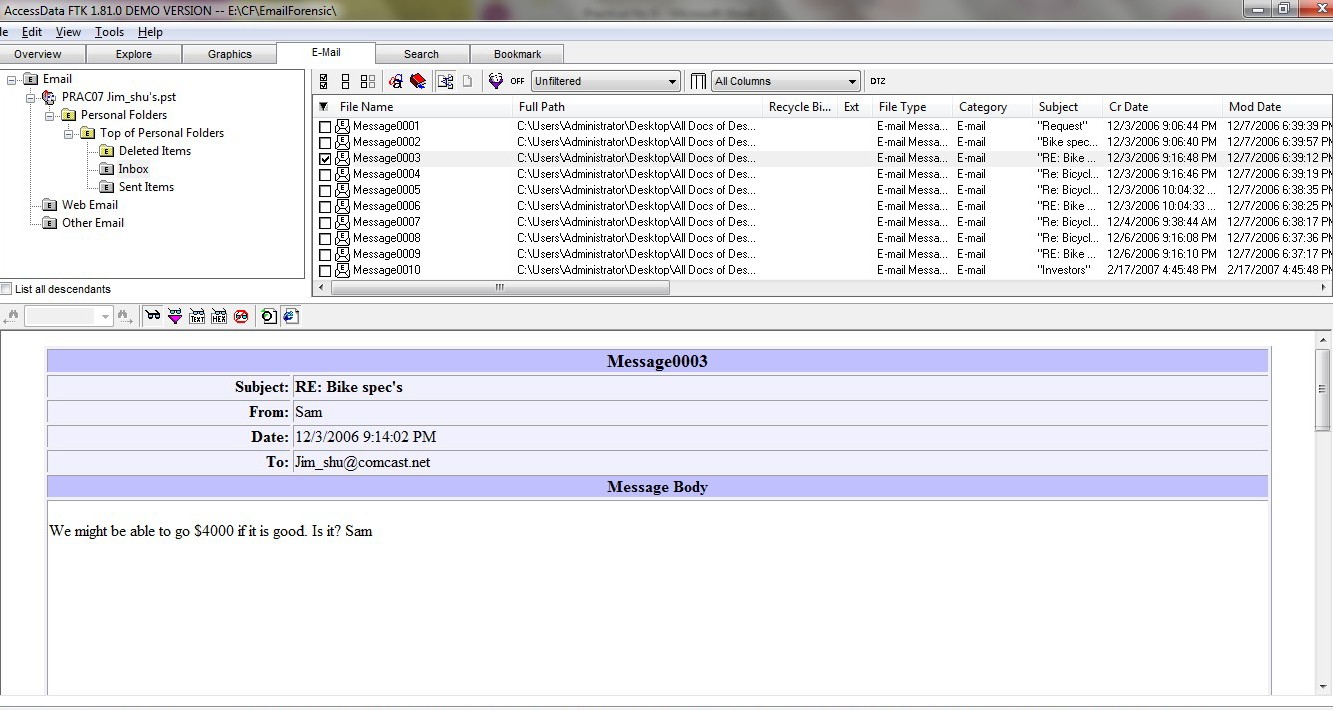
**Aim:** Analyzing email header

For analyzing header follow following:

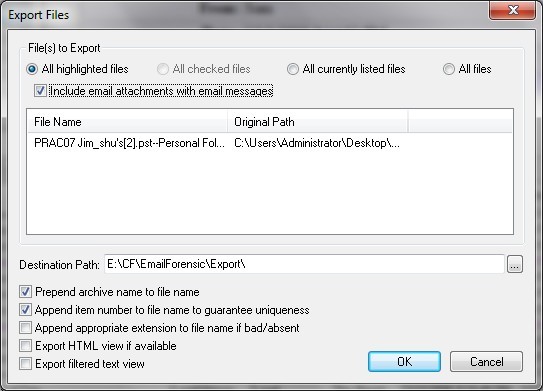
Steps:

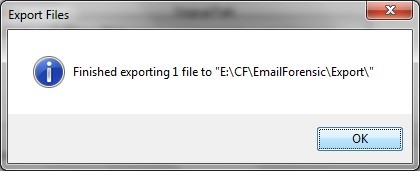
Click the **E-Mail** tab. In the tree view, click to expand all folders, and then click the **Inbox** folder.

In the File List pane at the upper right, click Message0003; as shown in the pane at the bottom, it’s from **Sam** and is addressed to [**Jim\_shu@comcast.net.**](mailto:martha.dax@superiorbicycles.biz)

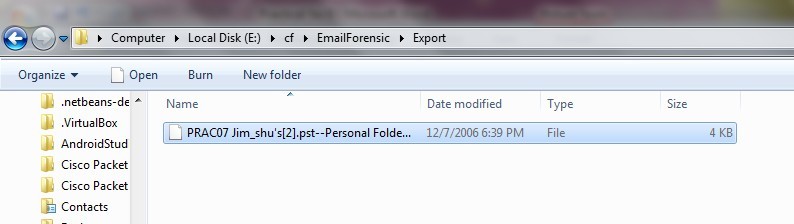


Right-click on any message say Message0003 in the File List pane and click Export File. In the Export Files dialog box, click OK.

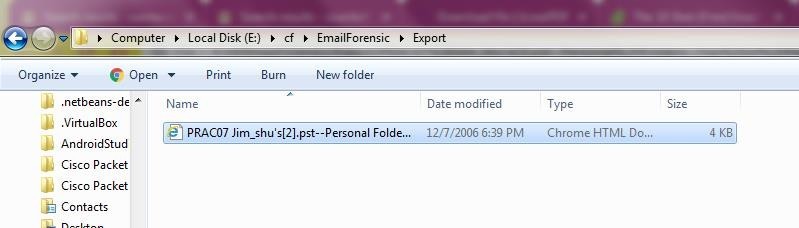




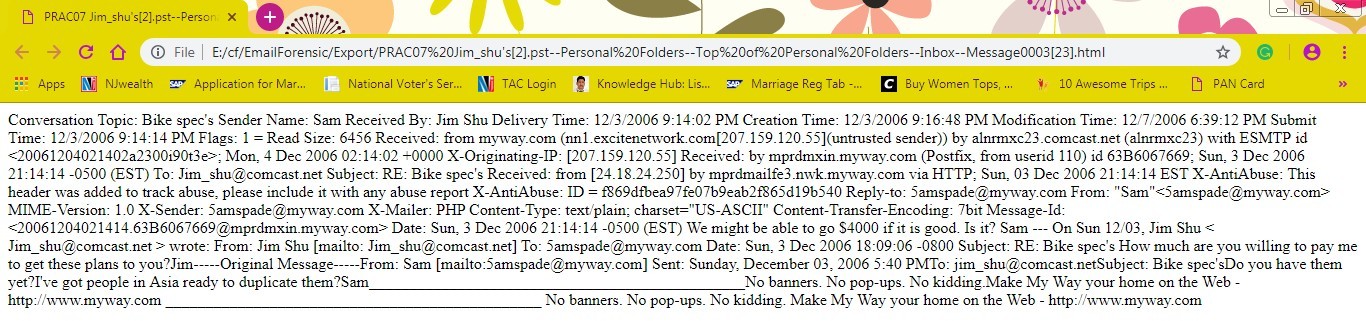
FTK saves exported files in the HTML format with no extension.



Right-click the Message0003 file and click Rename. Type Message0003.html and press Enter.



Double-click Message0003.html to view it in a Web browser.



**Practical No. 13**

**Aim:** Web Browser Forensics

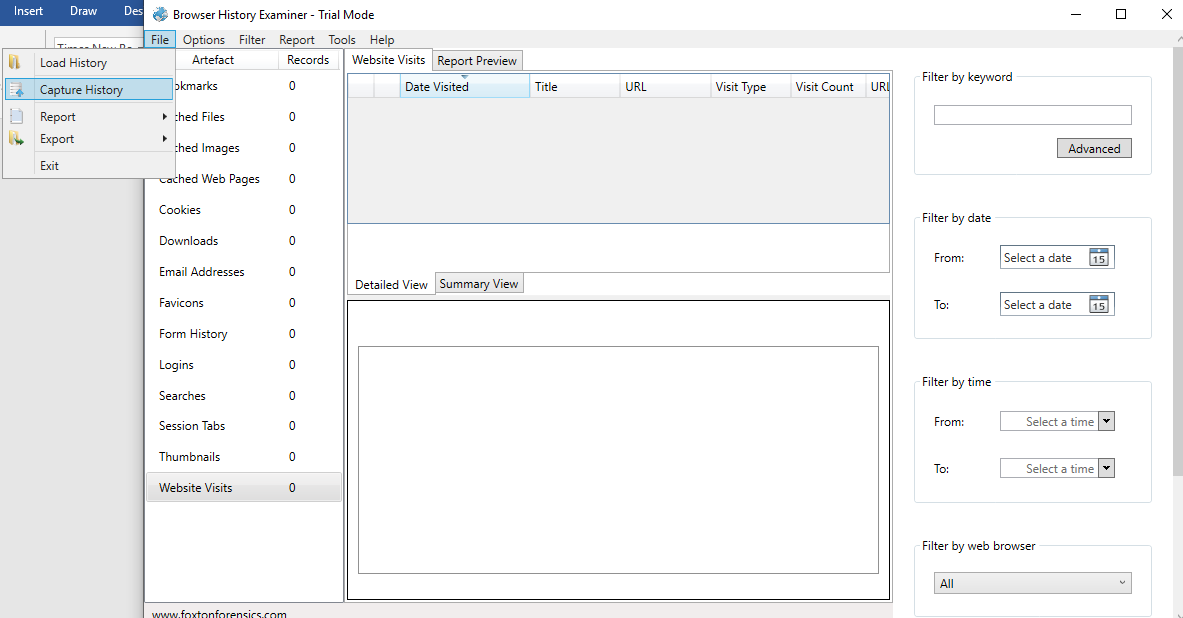
* Web Browser working
* -Forensics activities on browser
* -Cache / Cookies analysis
* -Last Internet activity

**Steps:**

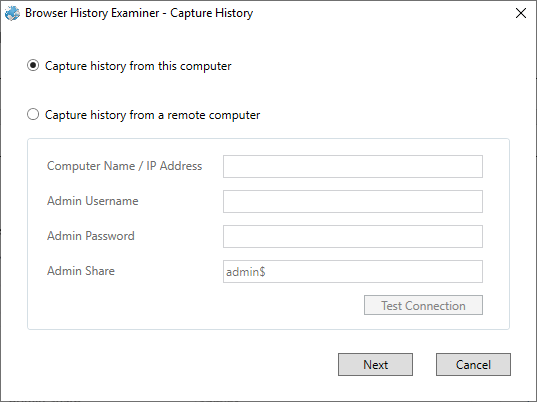
**Open BrowserHistoryExaminer.**



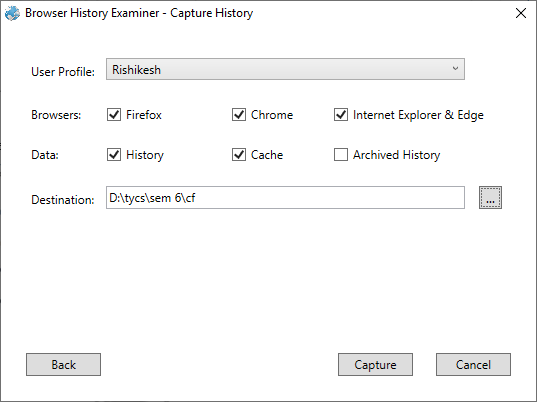
Click on file > Capture History



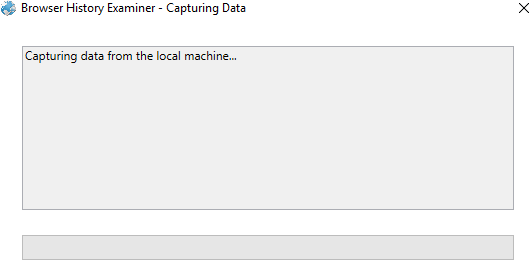
Select the capture folder and click on next.

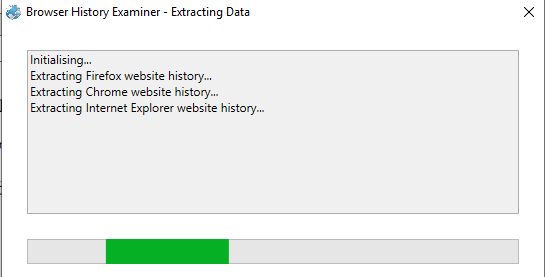


Enter the destination to capture the data.

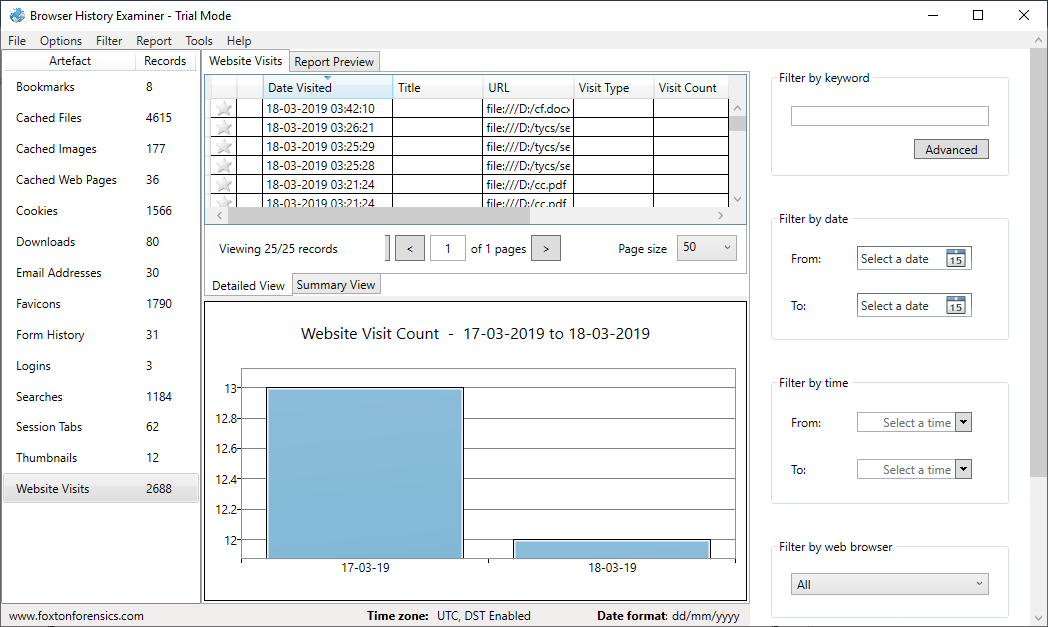


The History is been extracting.

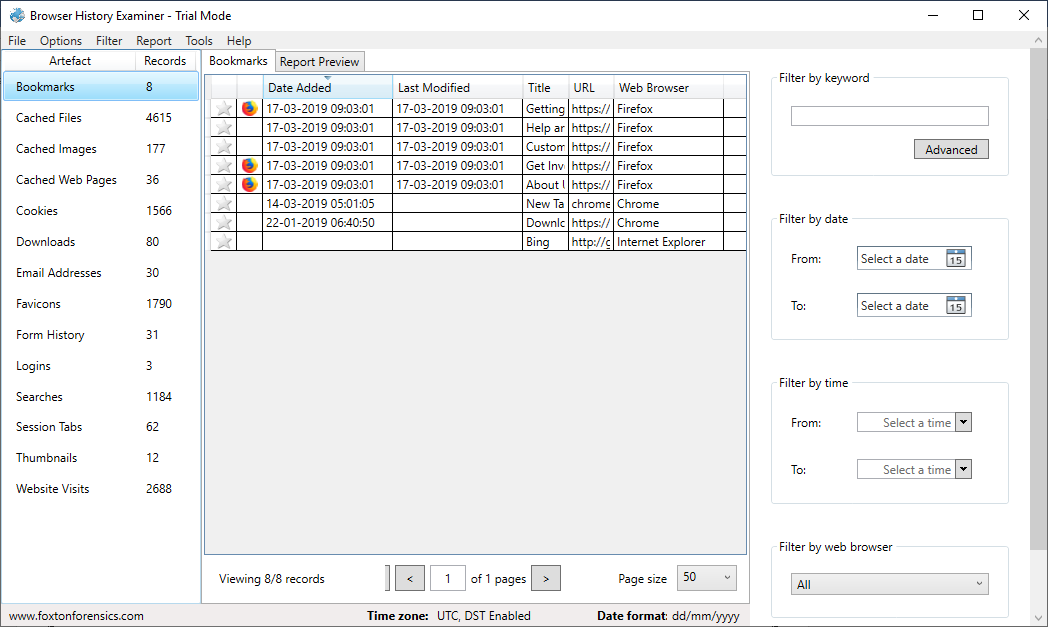




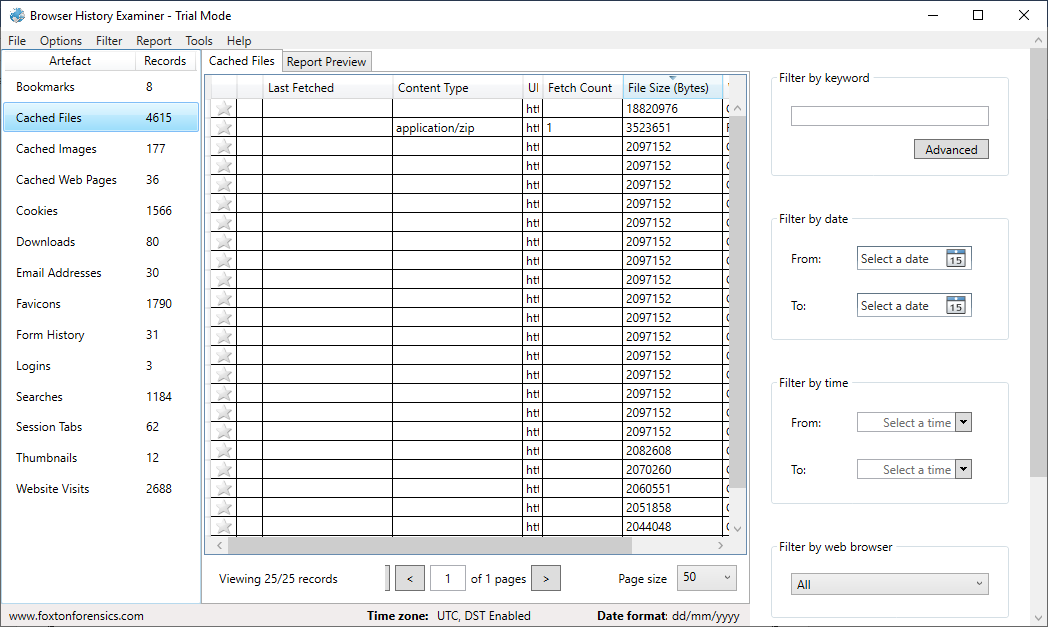
The data has been retrieved.



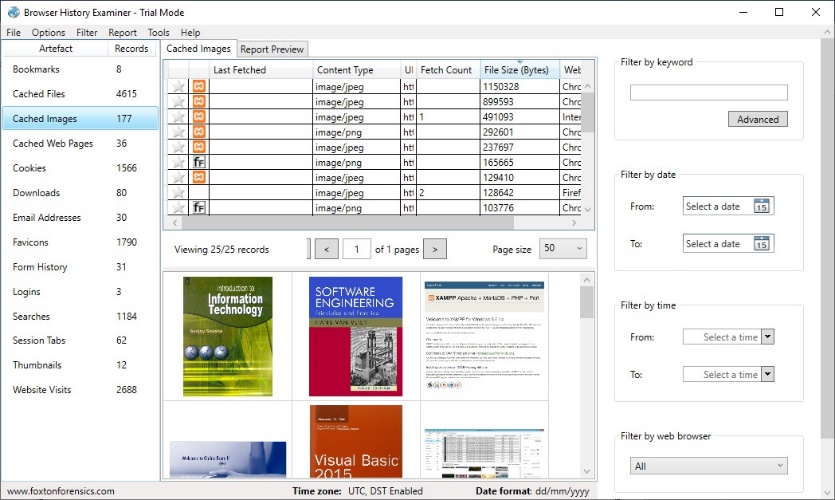
On the left panel click on bookmarks.



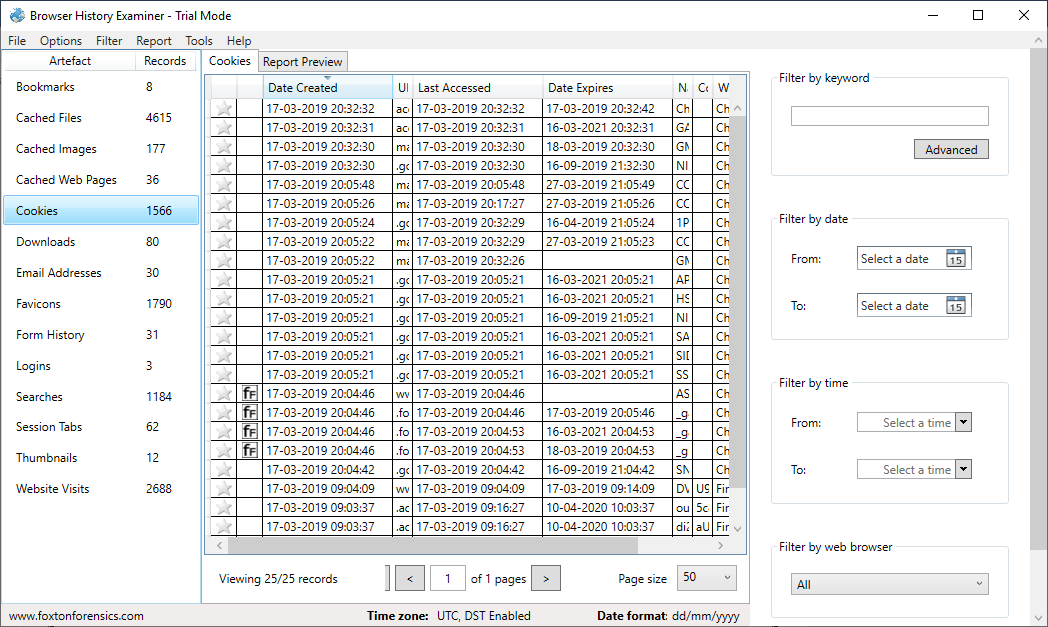
On the left panel click on cached files.



On the left panel click on cached images.



On the left panel click on cookies.



To Create Reports. Click on file > Report and save the report as pdf or html page.

