Practical 1

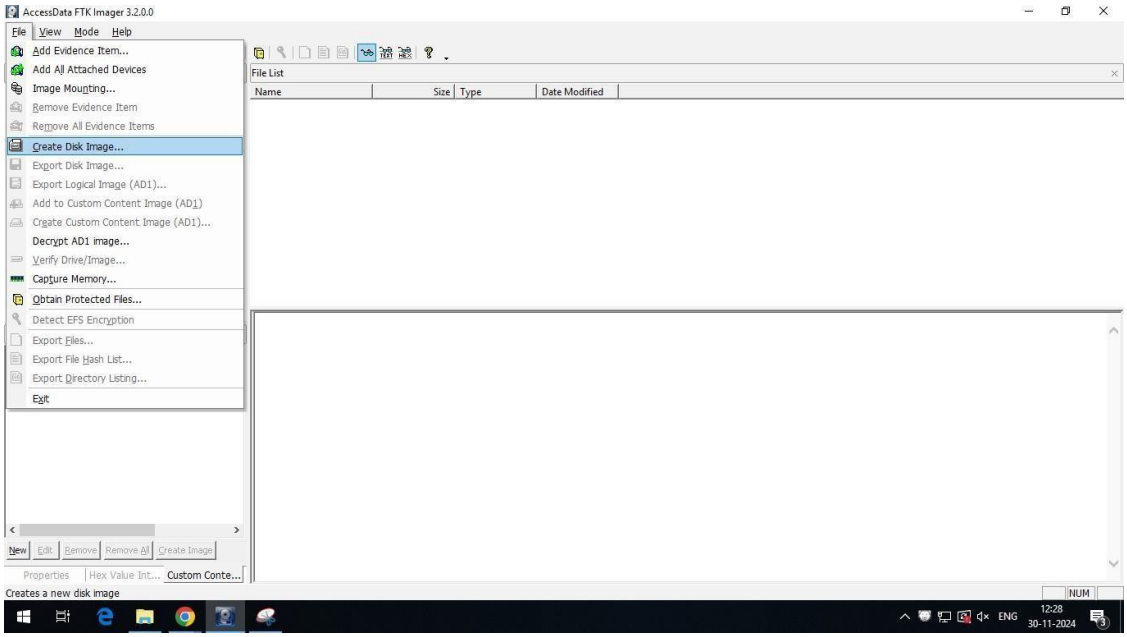
Date: 30-11-24

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

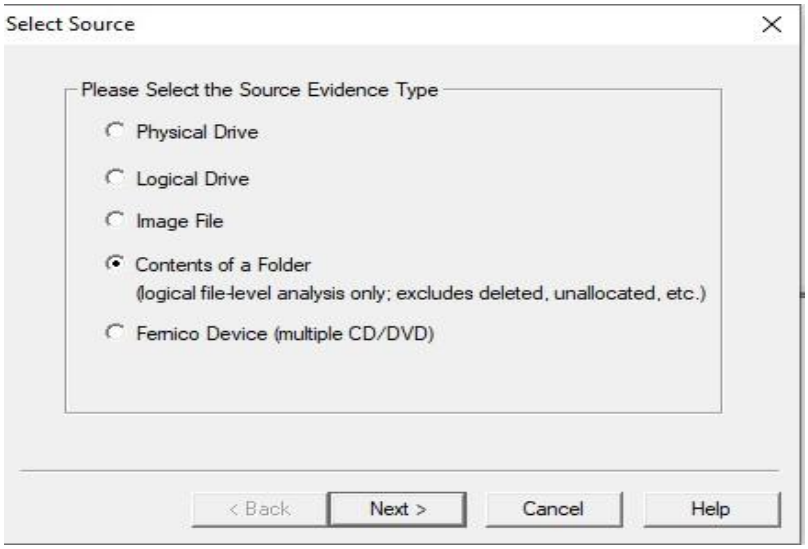
- Creating Forensic
- Check Integrity of Data
- Analyze Forensic Image

Creating Forensic:

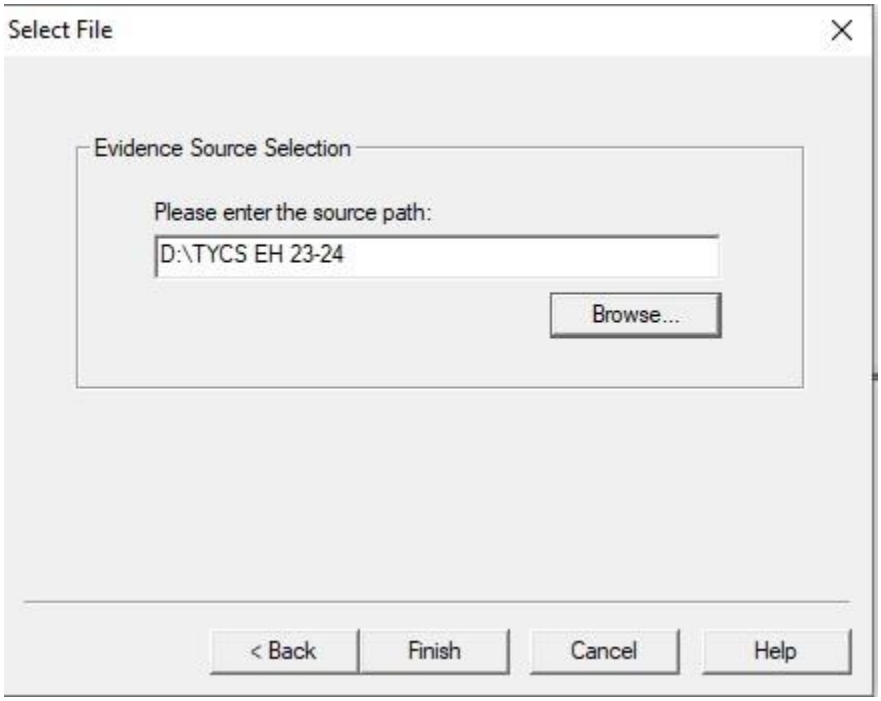
Step 1: Open AccessData FTK Imager, Click on File→Create Disk Image.



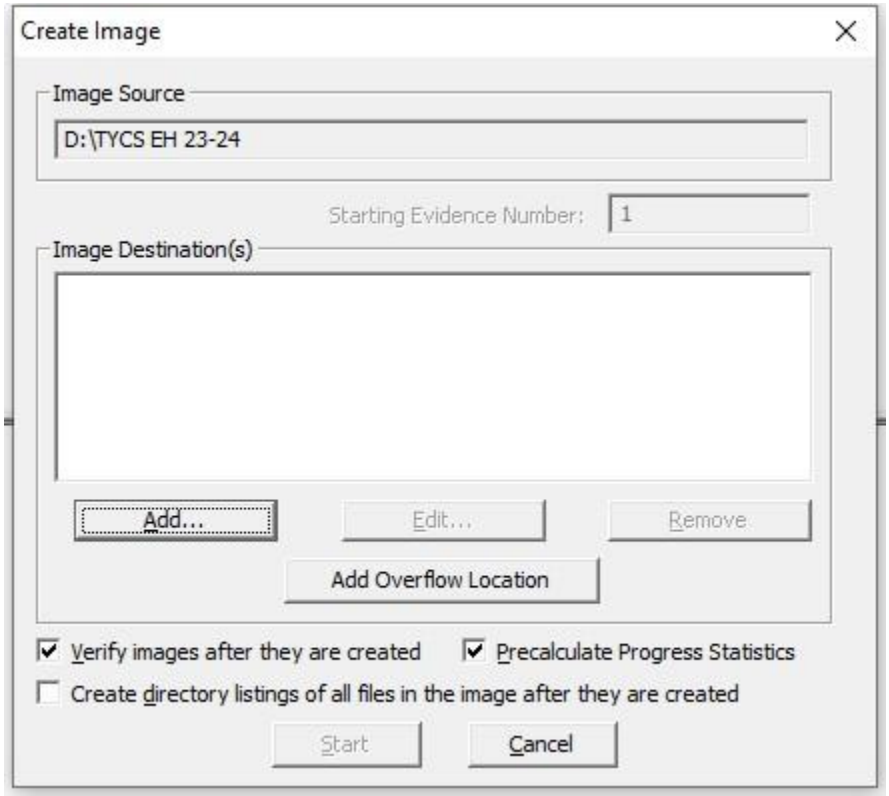
Step 2: From the "Select Source" Dialogbox select the option of "Contents of a folder". Click on Next.



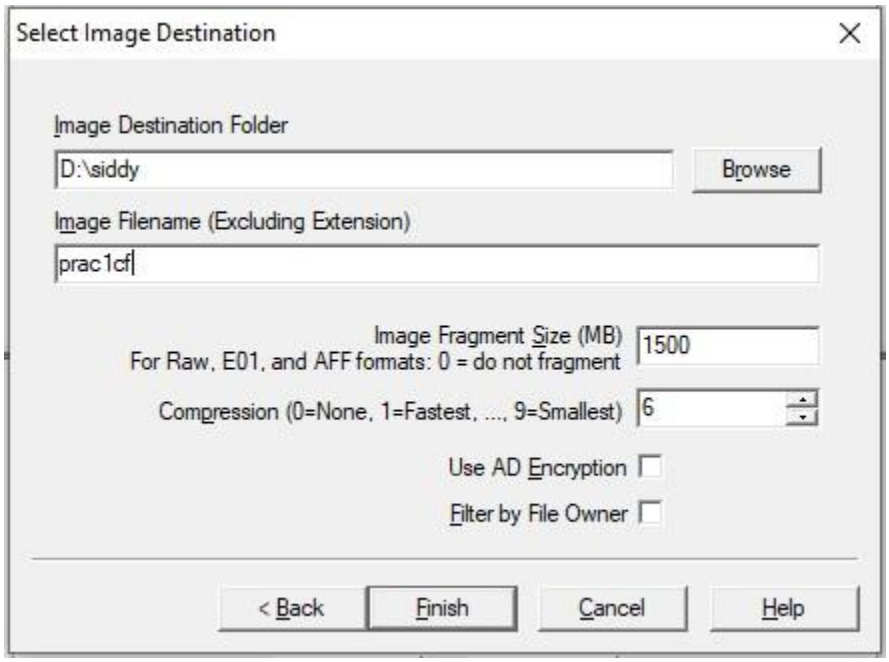
<u>Step 3:</u> Here browse and enter the source path of the file. Click on Finish.



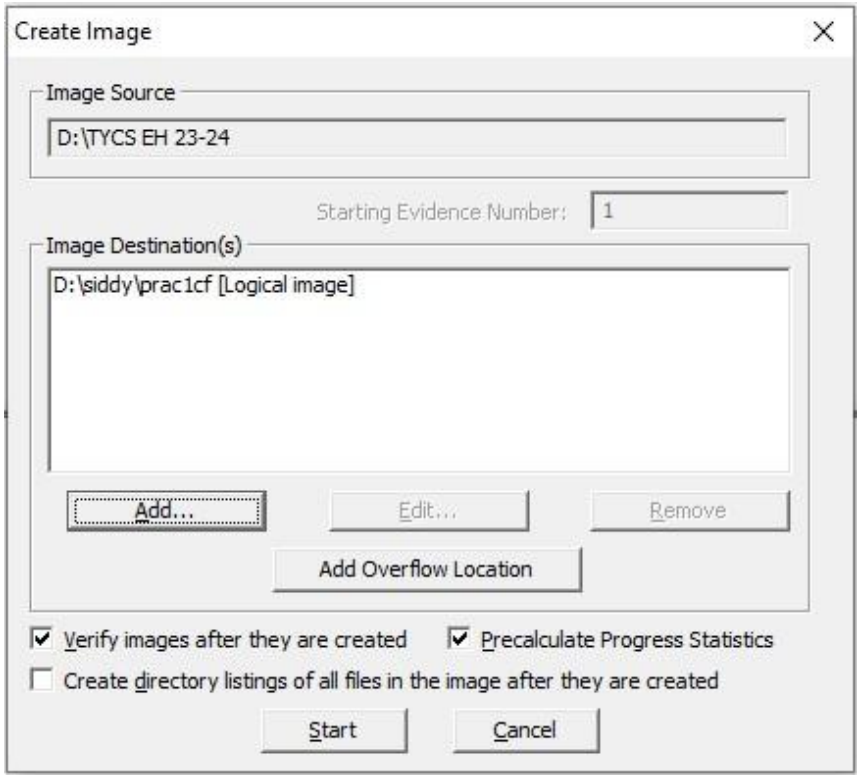
<u>Step 4:</u> Now click on the "Add" button and check the options of "Verify images after they are created" and "Precalculate progress statistics".



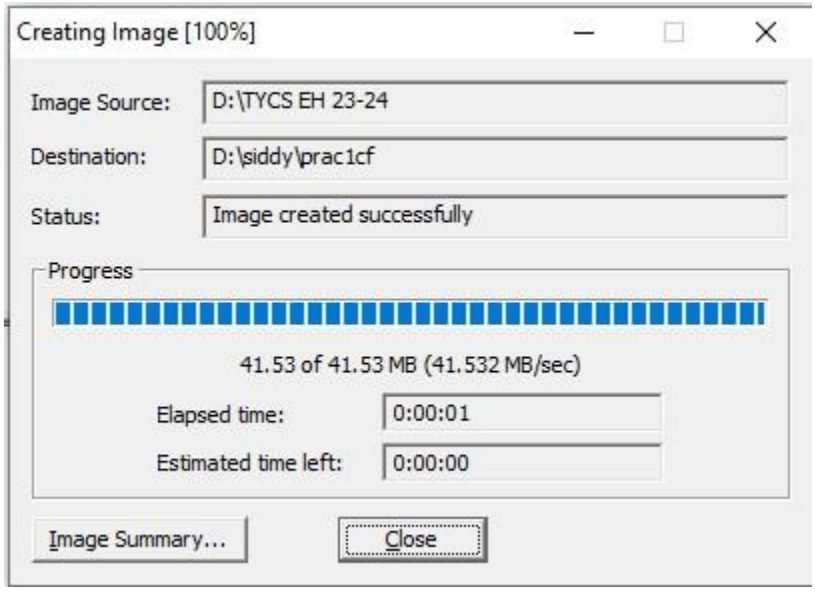
<u>Step 5:</u> After clicking on "Add" browse the "Image Destination Folder" and type the Image Filename. Click on Finish.



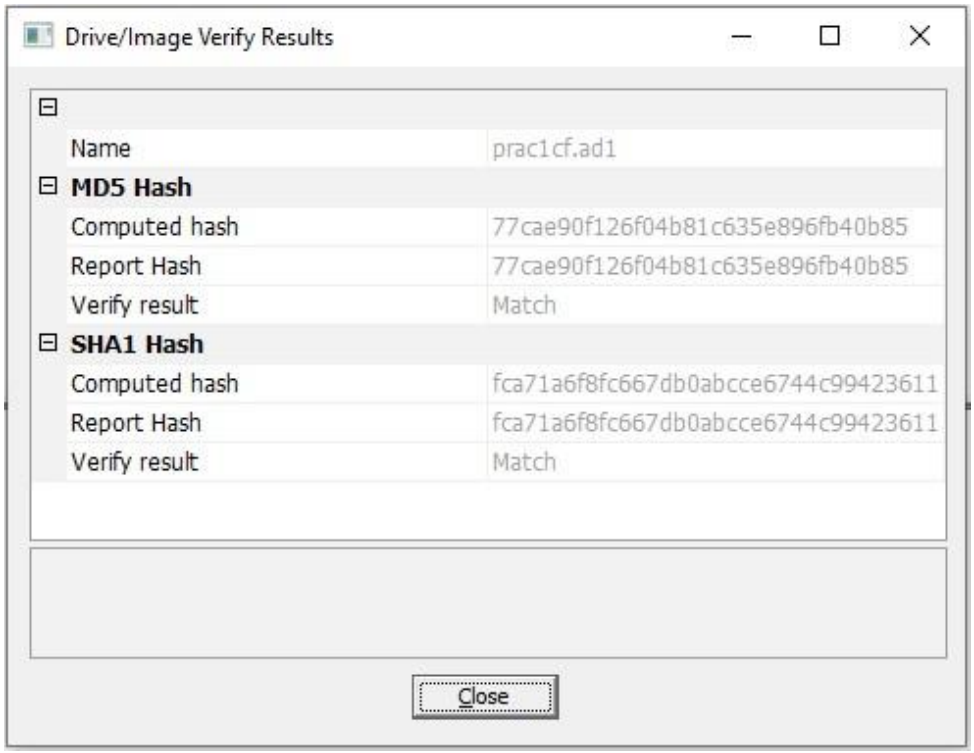
<u>Step 6:</u> Here we can see the Image Destination. Now click on "Start".



<u>Step 7:</u> Here the Image is being created. Proceed to click on "Image Summary" for the results.

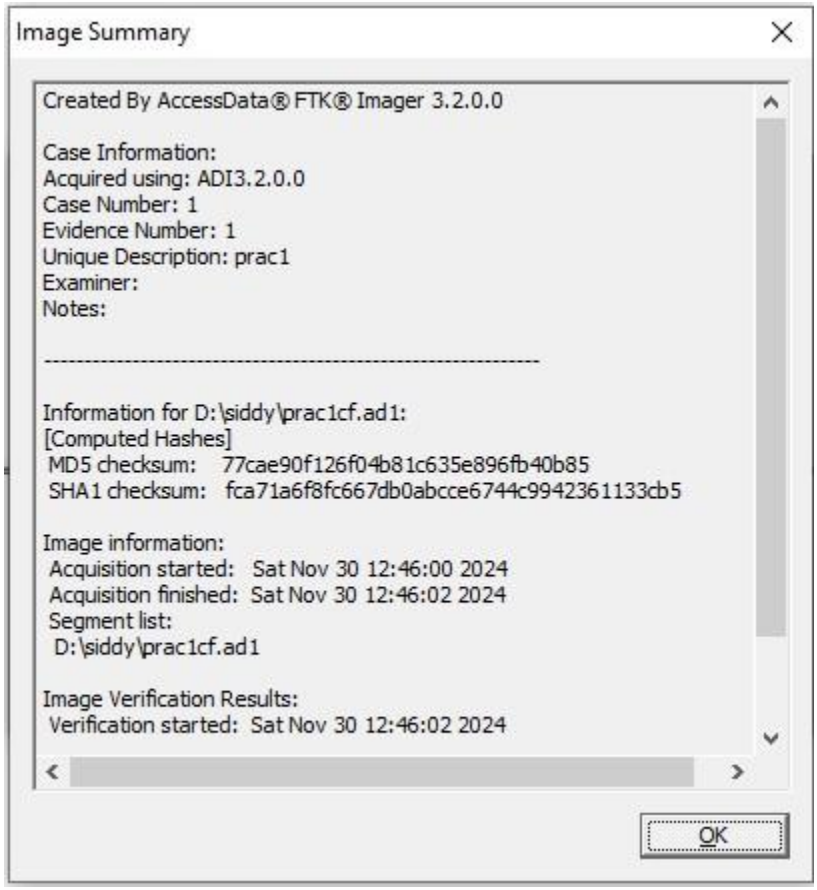


<u>Step 8:</u> Here we can see the Drive/Image Verify Results.

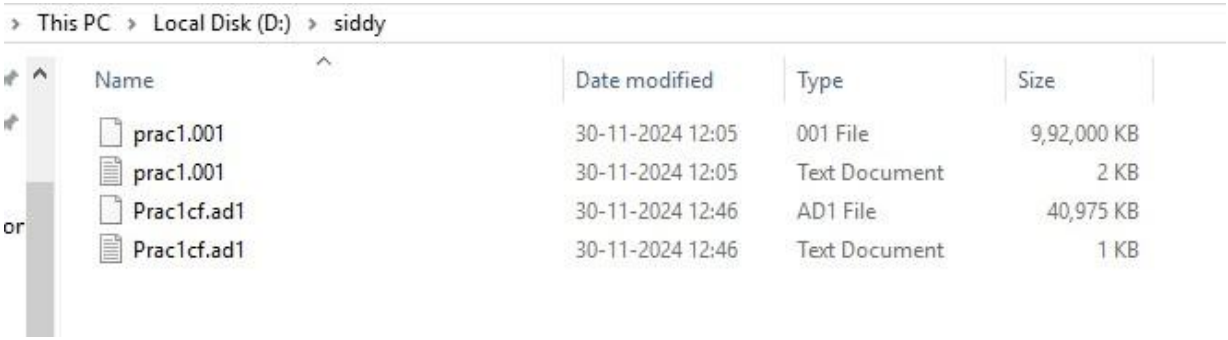


<u>Check Integrity of Data</u>

<u>Step 9:</u> Here we can see the whole summary of Image Verification Results.



<u>Step 10:</u> We can also check the Image Verification Summary in the folder where we have saved the file.



<u>Step 11:</u> Open the file "Prac1cf.ad1" from the folder which is a text document to see the summary of the image.

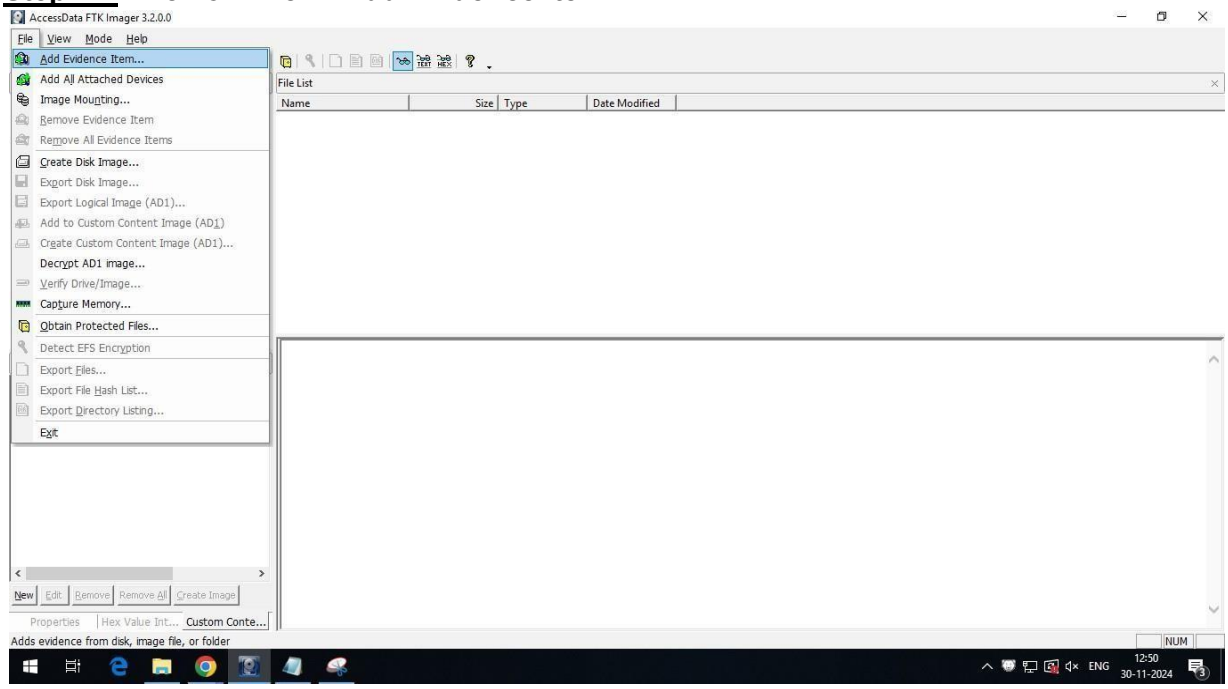
Prac1cf.ad1 - Notepad

File Edit Format View Help

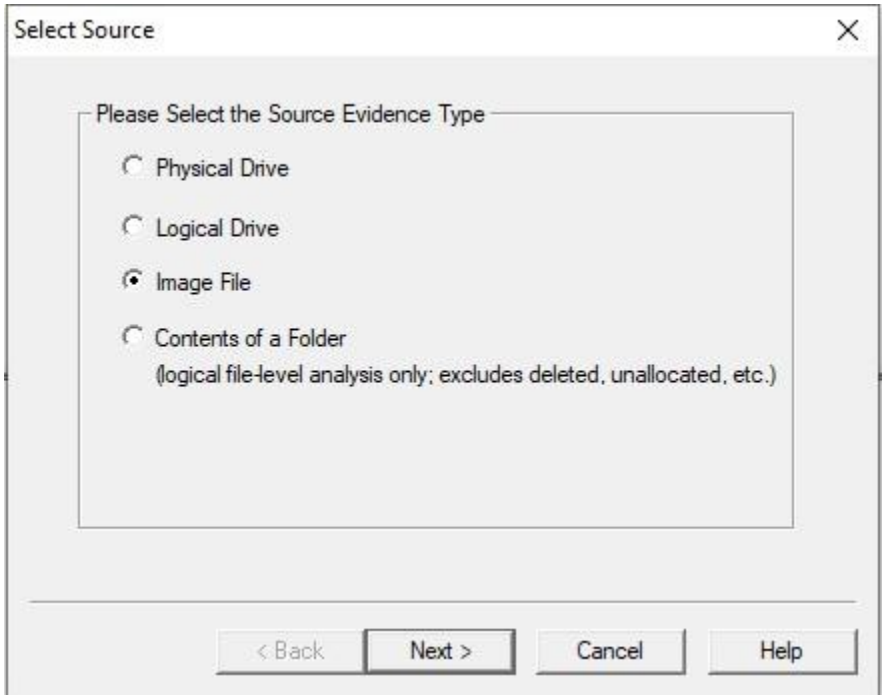
```
Created By AccessData® FTK® Imager 3.2.0.0

Case Information:
Acquired using: ADI3.2.0.0
Case Number: 1
Evidence Number: 1
Unique Description: prac1
Examiner:
Notes:

--------------------------------------------------------------

Information for D:\siddy\prac1cf.ad1:
[Computed Hashes]
 MD5 checksum:    77cae90f126f04b81c635e896fb40b85
 SHA1 checksum:   fca71a6f8fc667db0abcce6744c9942361133cb5

Image information:
 Acquisition started:   Sat Nov 30 12:46:00 2024
 Acquisition finished:  Sat Nov 30 12:46:02 2024
 Segment list:
  D:\siddy\prac1cf.ad1

Image Verification Results:
```

Analyze Forensic Image

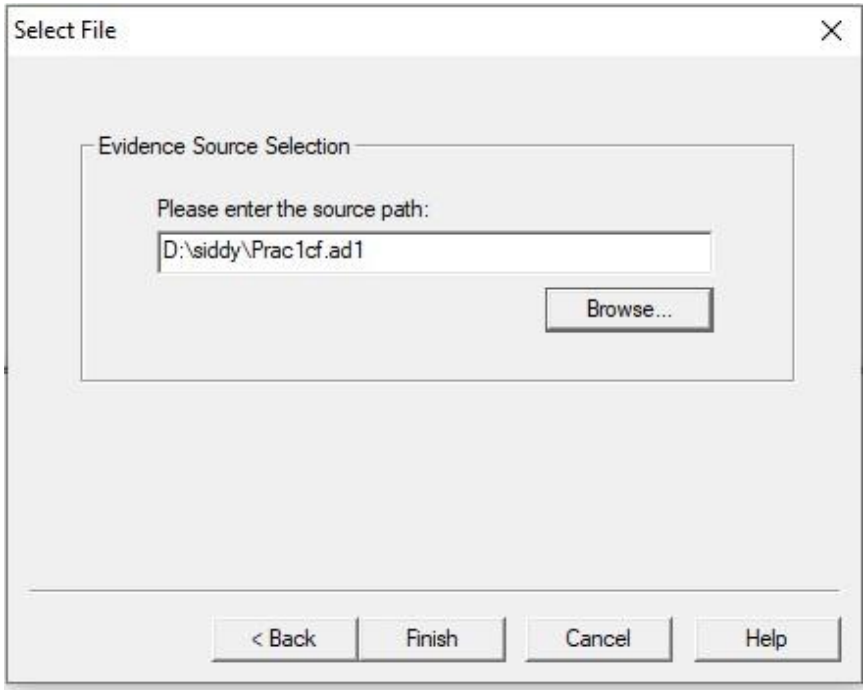
Step 12: Click on File→"Add Evidence Item".



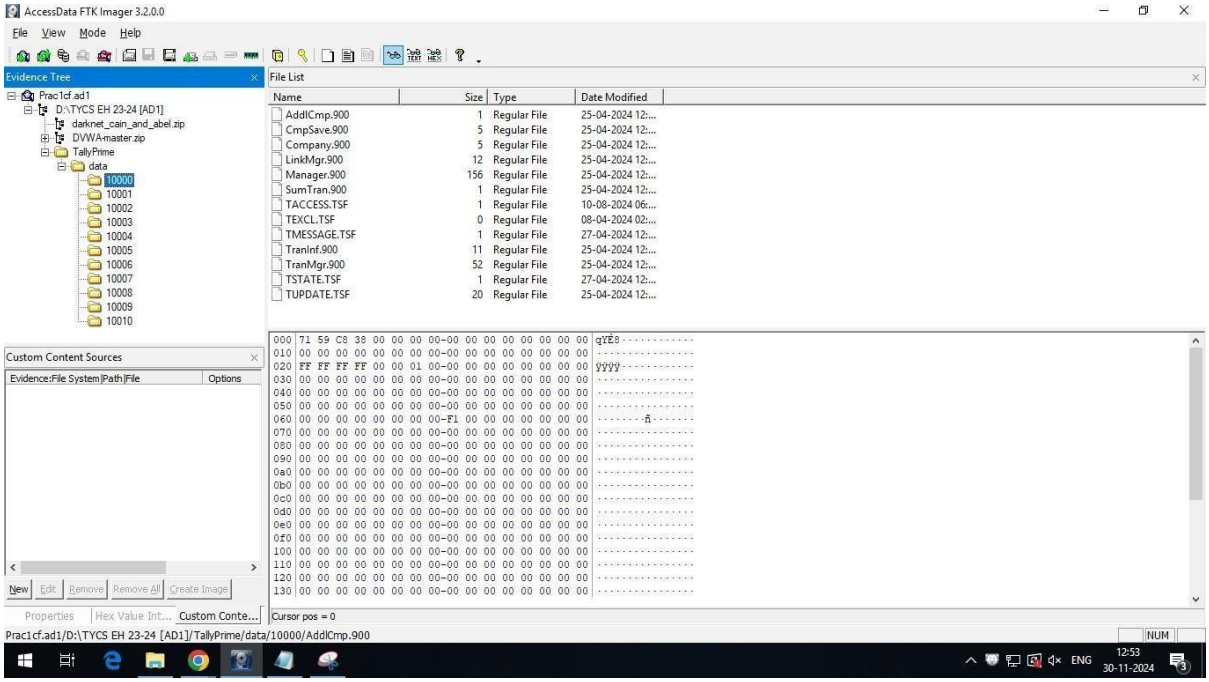
Step 13: Select the source evidence type→ Image File.



<u>Step 14:</u> Now browse the "Prac1cf.ad1" from the folder that we created. Click on "Finish".



<u>Step 15:</u> Here we can see the "Evidence Tree" to check the Analyzed result of the forensic Image.

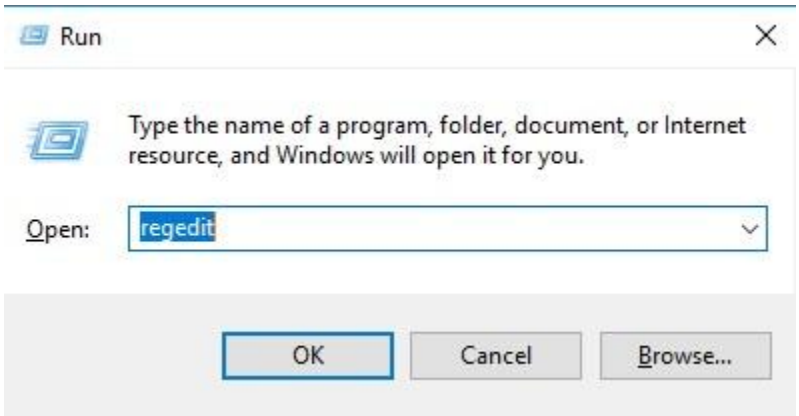

AccessData FTK Imager 3.2.0.0
File View Mode Help
Evidence Tree
Prac1cf.ad1
D:\TYCS EH 23-24 [AD1]
darknet_cain_and_abel.zip
DVWA-master.zip
TallyPrime
data
10000
10001
10002
10003
10004
10005
10006
10007
10008
10009
10010
File List
Name Size Type Date Modified
AddlCmp.900 1 Regular File 25-04-2024 12:...
CmpSave.900 5 Regular File 25-04-2024 12:...
Company.900 5 Regular File 25-04-2024 12:...
LinkMgr.900 12 Regular File 25-04-2024 12:...
Manager.900 156 Regular File 25-04-2024 12:...
SumTran.900 1 Regular File 25-04-2024 12:...
TACCESS.TSF 1 Regular File 10-08-2024 06:...
TEXCL.TSF 0 Regular File 08-04-2024 02:...
TMESSAGE.TSF 1 Regular File 27-04-2024 12:...
TranInf.900 11 Regular File 25-04-2024 12:...
TranMgr.900 52 Regular File 25-04-2024 12:...
TSTATE.TSF 1 Regular File 27-04-2024 12:...
TUPDATE.TSF 20 Regular File 25-04-2024 12:...
000 71 59 C8 38 00 00 00 00-00 00 00 00 00 00 00 00 qYÈ8
010 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
020 FF FF FF FF 00 00 01 00-00 00 00 00 00 00 00 00 ÿÿÿÿ
030 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
040 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
050 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
060 00 00 00 00 00 00 00 00-F1 00 00 00 00 00 00 00 ñ
070 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
080 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
090 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
0a0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
0b0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
0c0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
0d0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
0e0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
0f0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
100 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
110 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
120 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
130 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
Custom Content Sources
Evidence:File System|Path|File Options
New Edit Remove Remove All Create Image
Properties Hex Value Int... Custom Conte...
Cursor pos = 0
Prac1cf.ad1/D:\TYCS EH 23-24 [AD1]/TallyPrime/data/10000/AddlCmp.900
NUM
ENG
12:53
30-11-2024

Practical 2

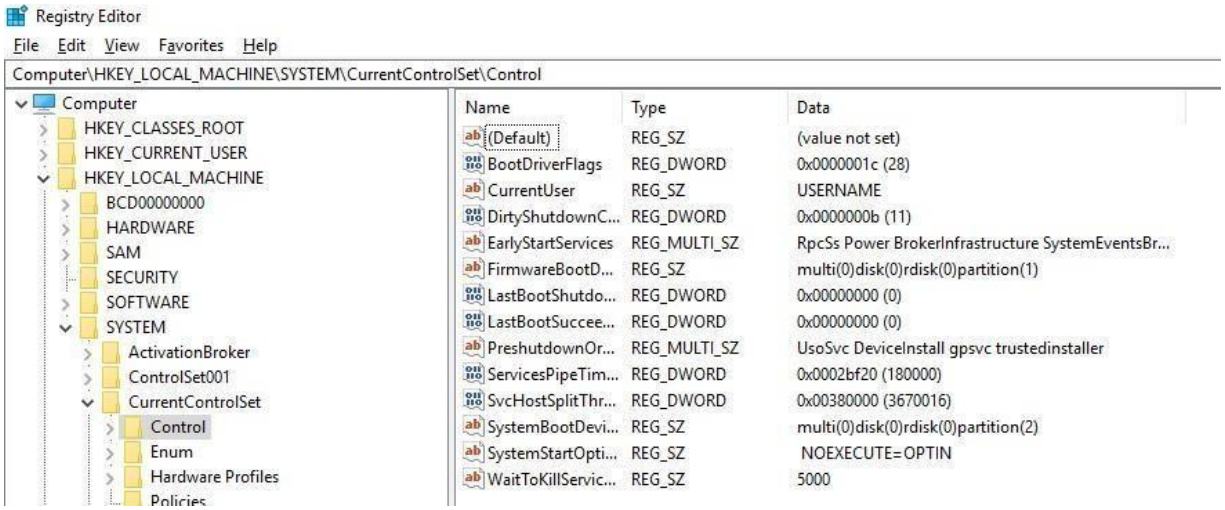
Date: 07-12-24

Aim: Data Acquisition:
Perform data acquisition using USB Writer Blocker + FTK Imager.

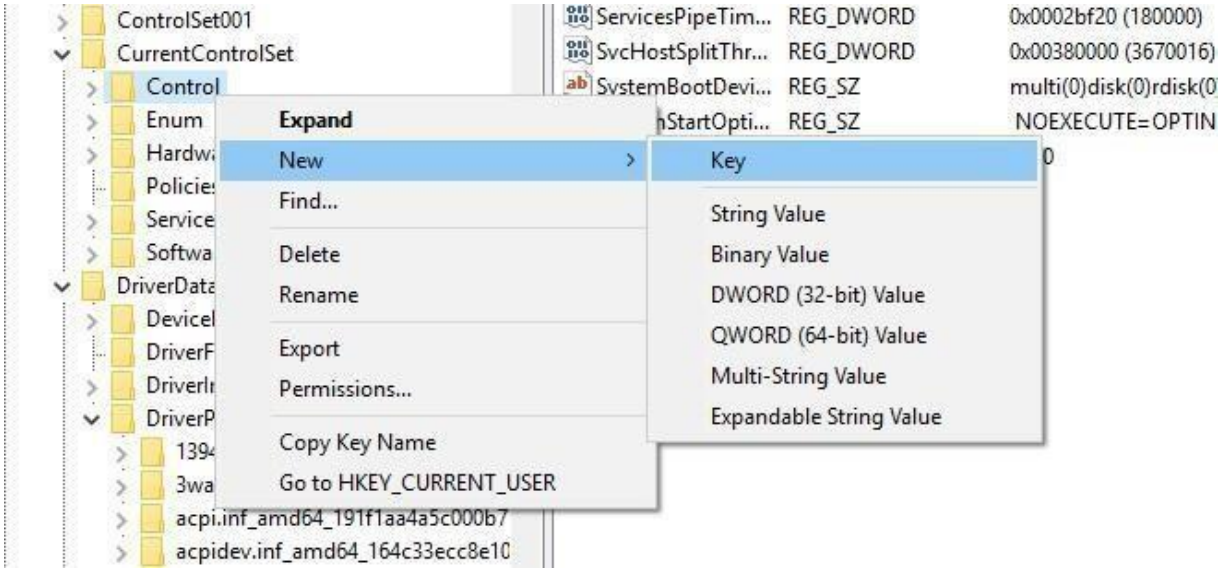
Step 1: Open the Run dialog box by using Windows+R and type "regedit".Click on Ok .



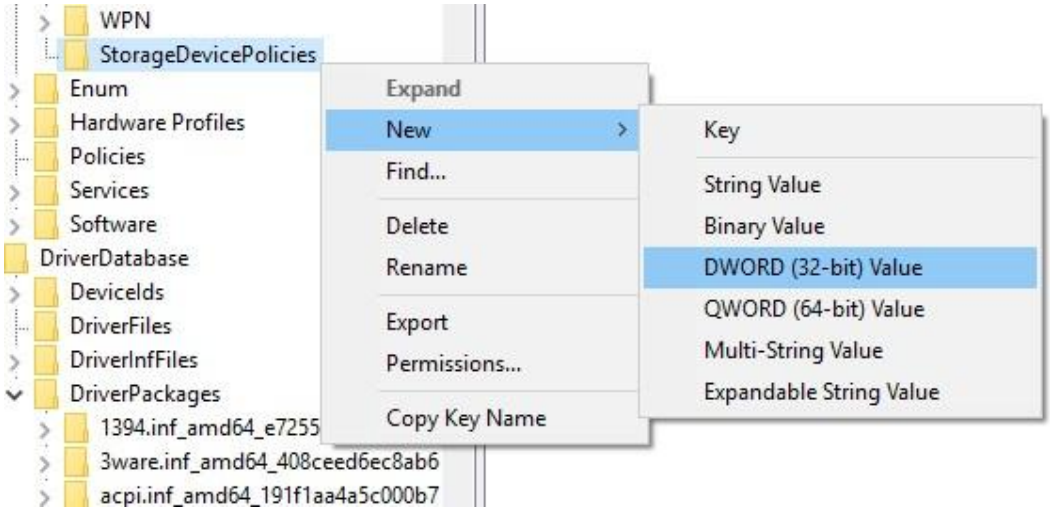
Step 2: A window like this will appear select
Computer → HKEY_LOCAL_MACHINE → SYSTEM → CurrentControlSet → Control.



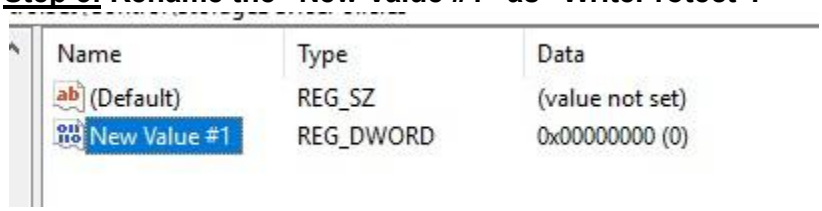
Step 3: Right Click on "Control".Select New → Key.



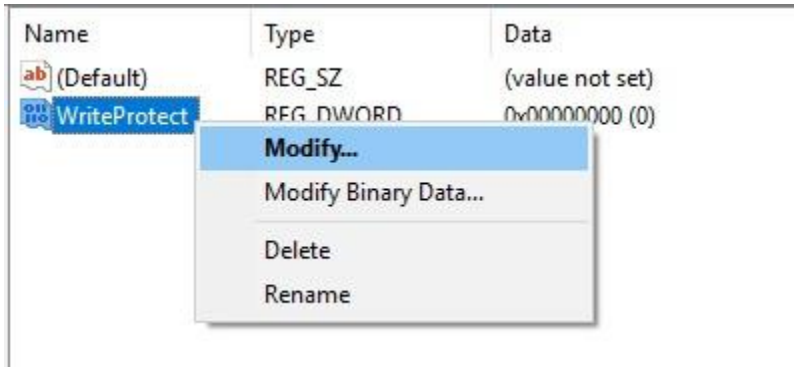
<u>Step 4:</u> Rename "New Key #1" as "StorageDevicePolicies" then right click on it select New→DWORD(32-bit)Value.



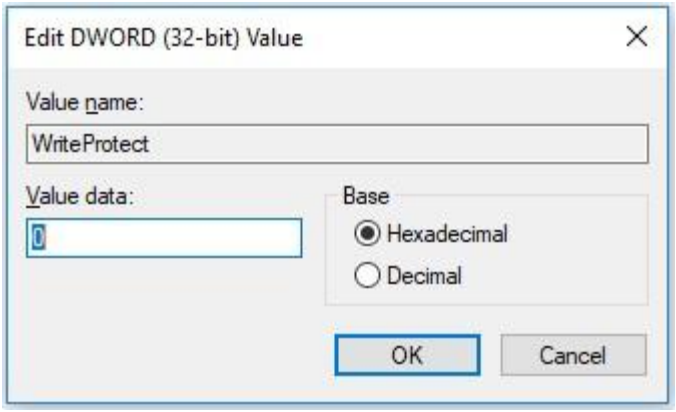
<u>Step 5:</u> Rename the "New Value #1" as "WriteProtect".

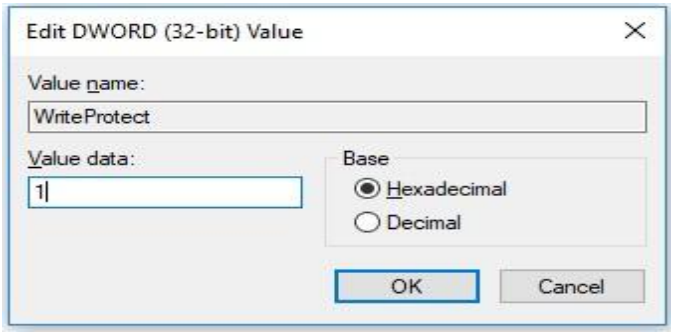


<u>Step 6:</u> Now right click on "WriteProtect" select the option of "Modify".

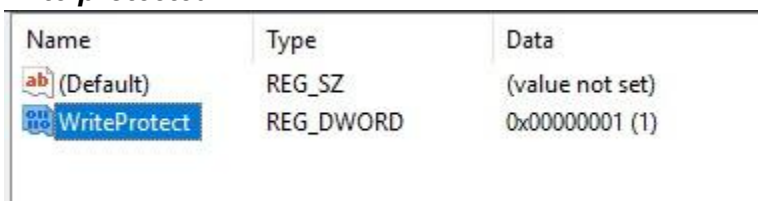


<u>Step 7:</u> Change the "Value data" into 1. Click on Ok.





<u>Step 8:</u> 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".*



<u>Step 9:</u> We can only open the file in the USB drive for reading,but it is not allowed to Modify and save the changes back to USB Drive.

<u>FTK Image:</u>

<u>Step 10:</u> Now create an image of the USB Driver using FTK Imager.

Following steps have to be performed for the same: ● Open AccessData FTK Imager, Click on File→Create Disk Image.

- **From the "Select Source" Dialogbox select the option of "Contents of a folder". Click on Next.**
- **Here browse and enter the source path of the file. Click on Finish.**
- **Now click on the "Add" button and check the options of "Verify images after they are created" and "Precalculate progress statistics".**
- **After clicking on "Add" browse the "Image Destination Folder" and type the Image Filename. Click on Finish. ● Here we can see the Image Destination. Now click on "Start".**
- **Here the Image is being created. Proceed to click on "Image Summary" for the results.**
- **Here we can see the Drive/Image Verify Results.**

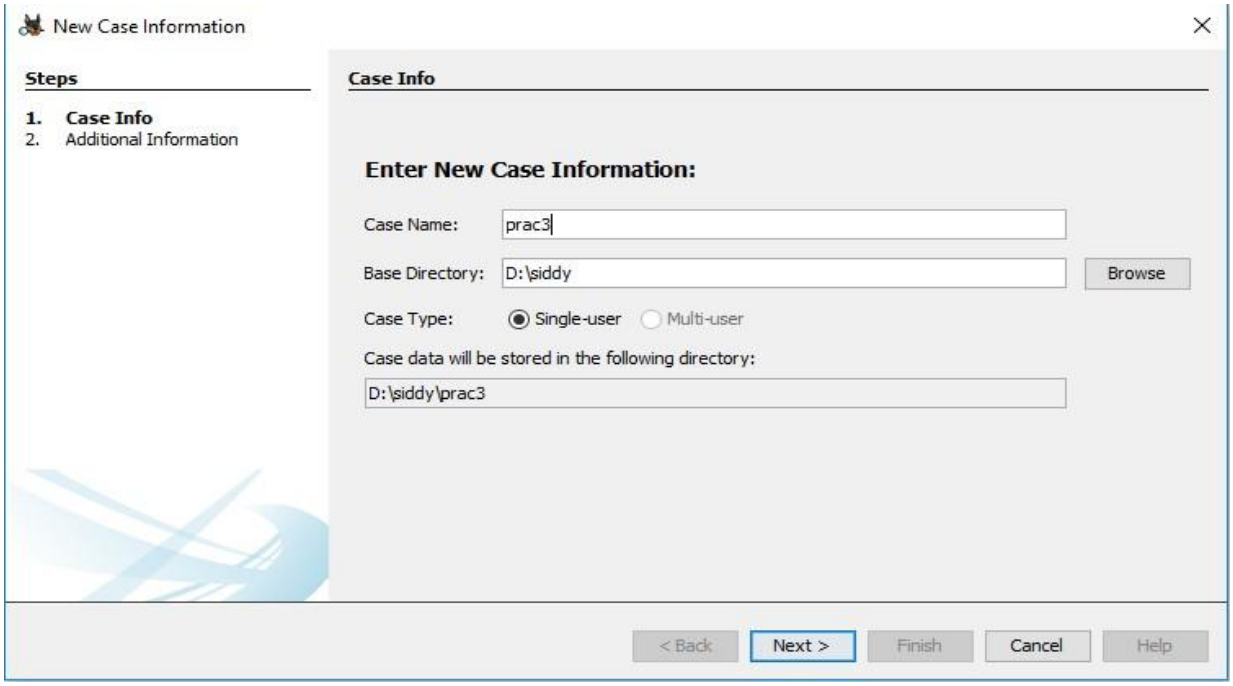
Practical 3

Date: 14-12-24

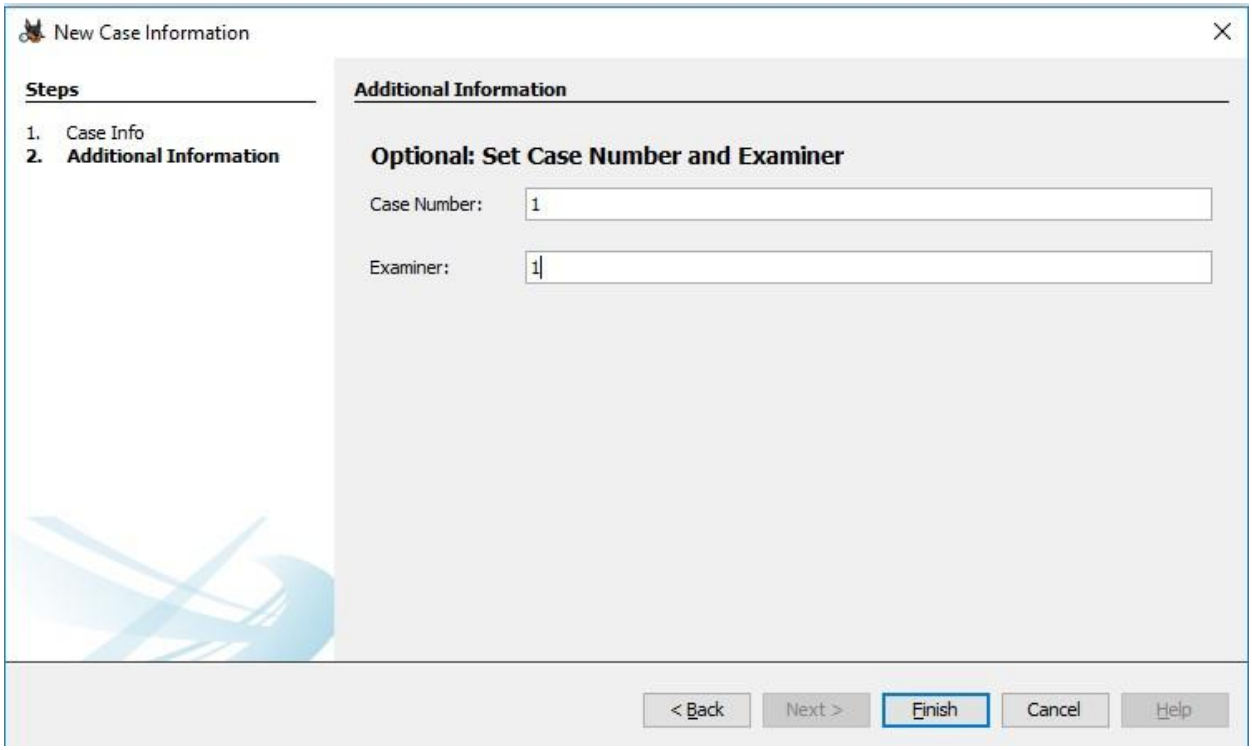
Aim: Forensic Case Study
Solve the Case Study (image file) provided in the lab using Autopsy.

Step 1: Open Autopsy and click on Create New Case.

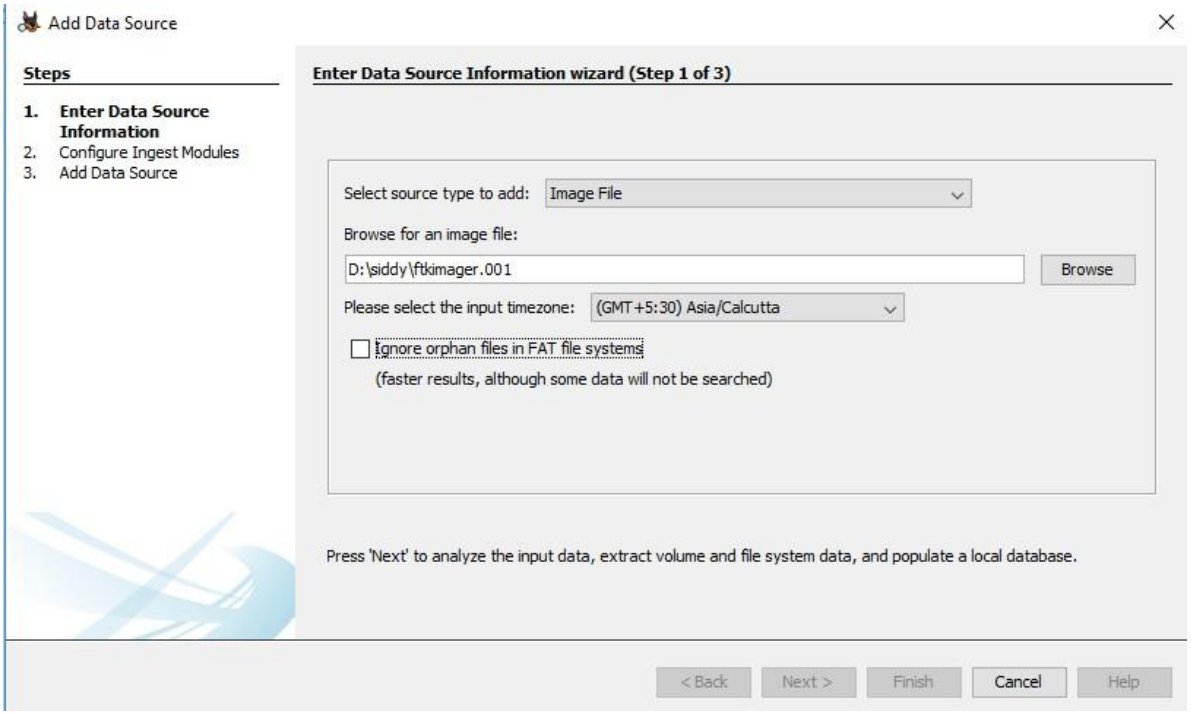
Step 2: Enter the details like "Case Name" and the "Base Directory" as follows. Click on next.



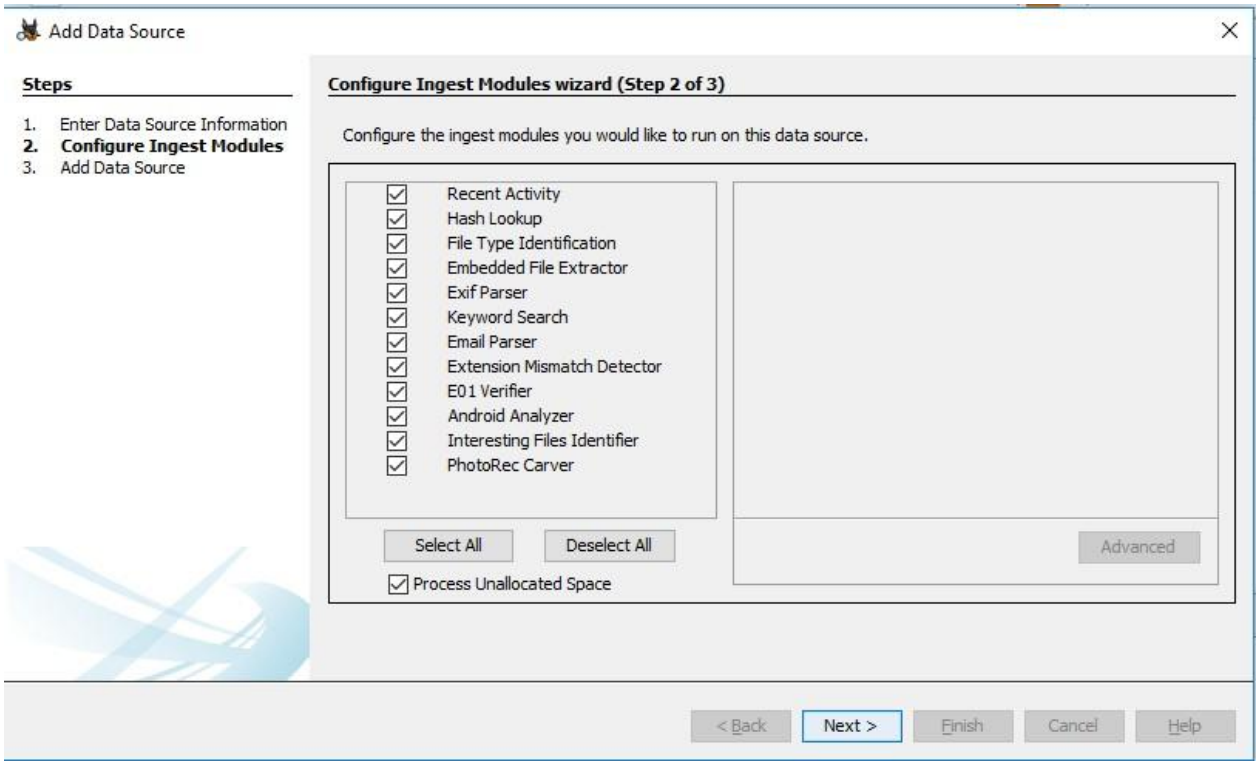
Step 3: Here set the Case Number and Examiner as follows.Click on Finish.S



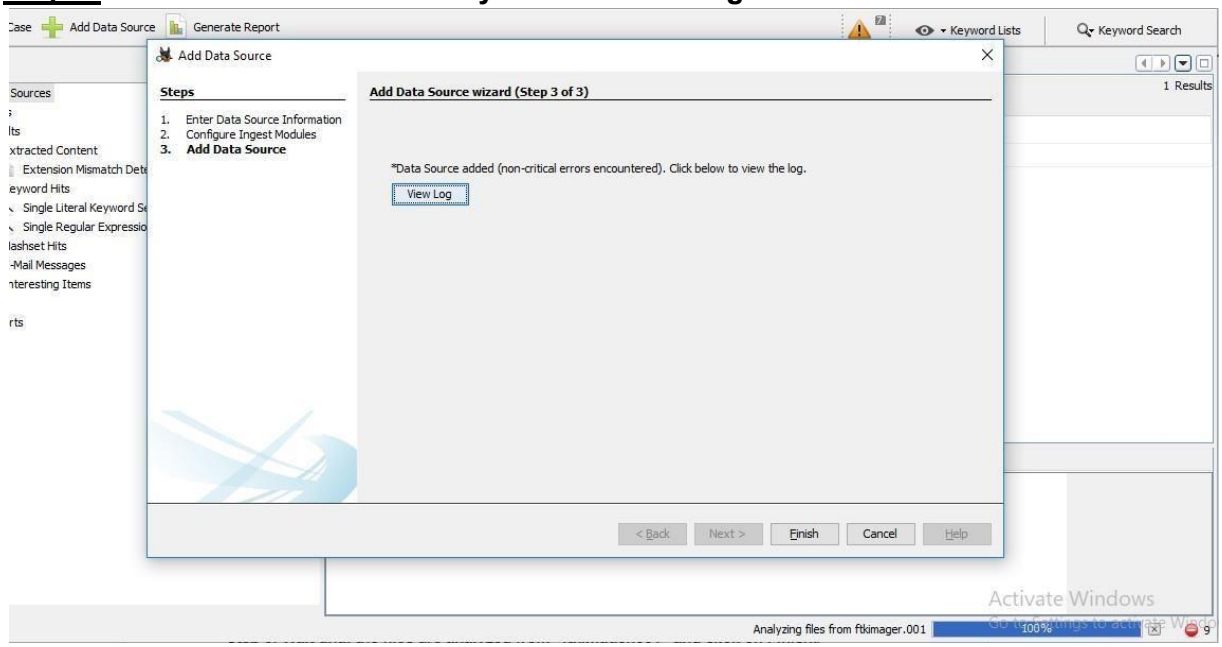
<u>Step 4:</u> Now Enter the Data Source and browse for the image file "ftkimager.001".Click on next.



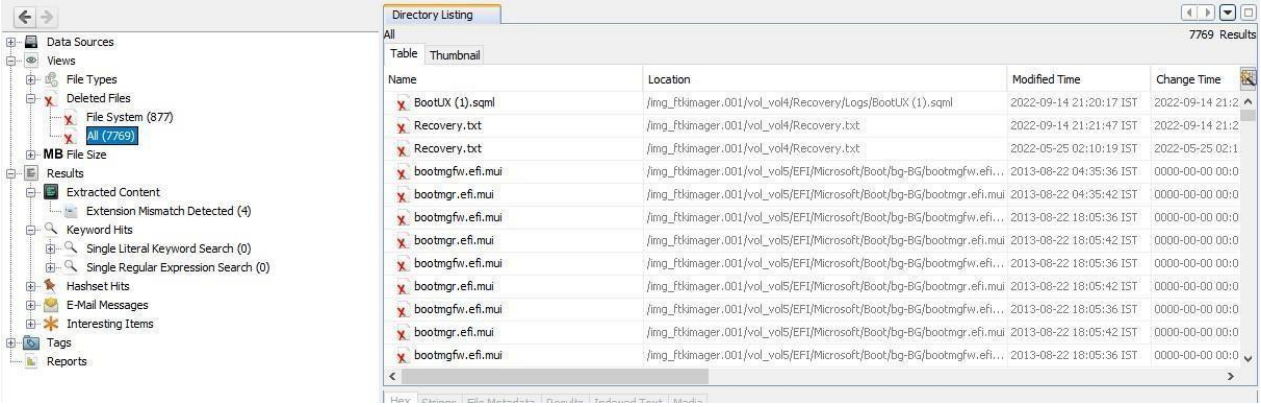
<u>Step 5:</u> Now select all the given checkboxes and click on next.



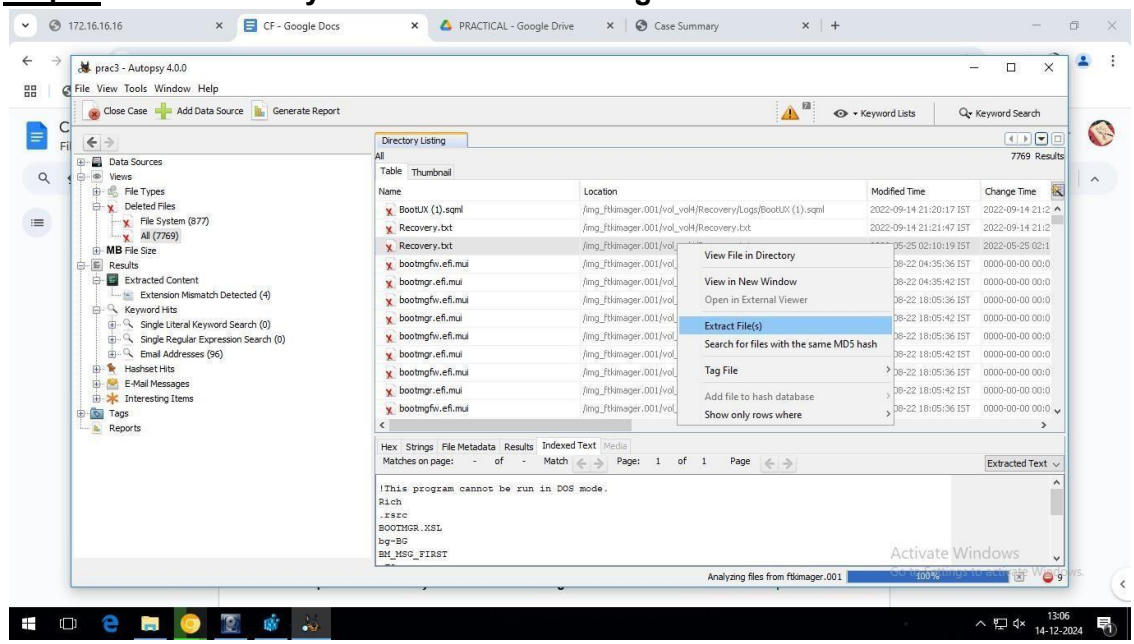
Step 6: **Wait until the files are analyzed from "ftkimager.001" and click on Finish.**



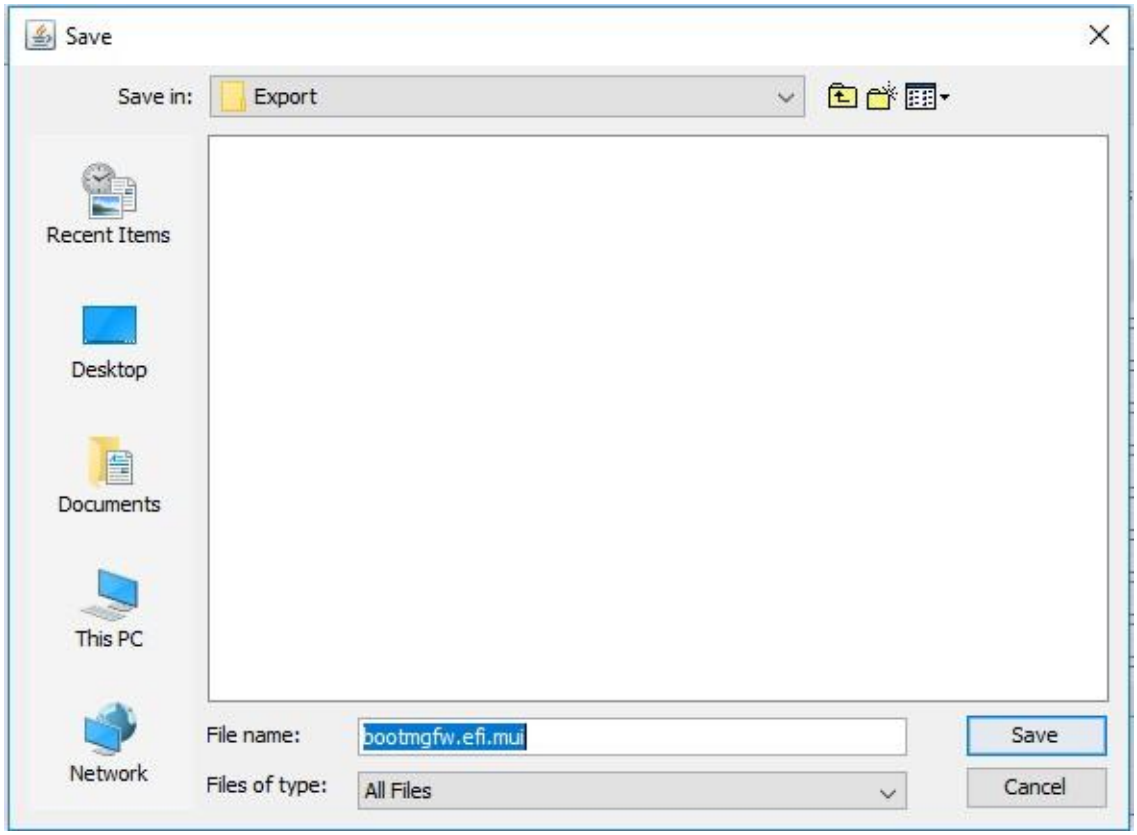
Step 7: **Now go to "Views" in the left pane and select Delete Files→All.The deleted files will be listed as shown below.**



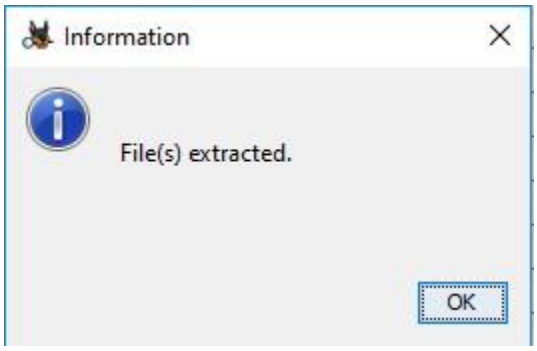
<u>Step 8:</u> Now select any one of the files then right click on it to select "Extract Files".



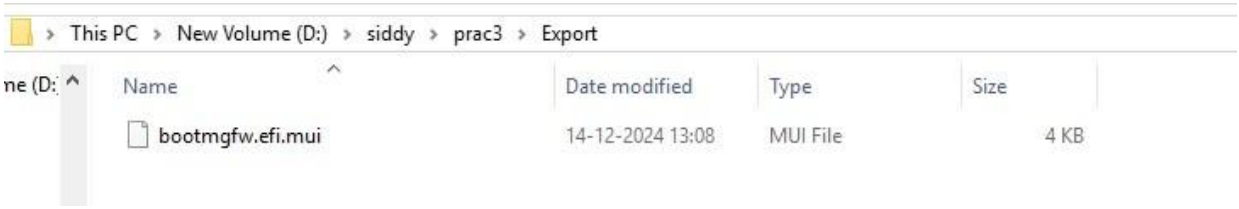
<u>Step 9:</u> Now save the Extracted File in the Export.



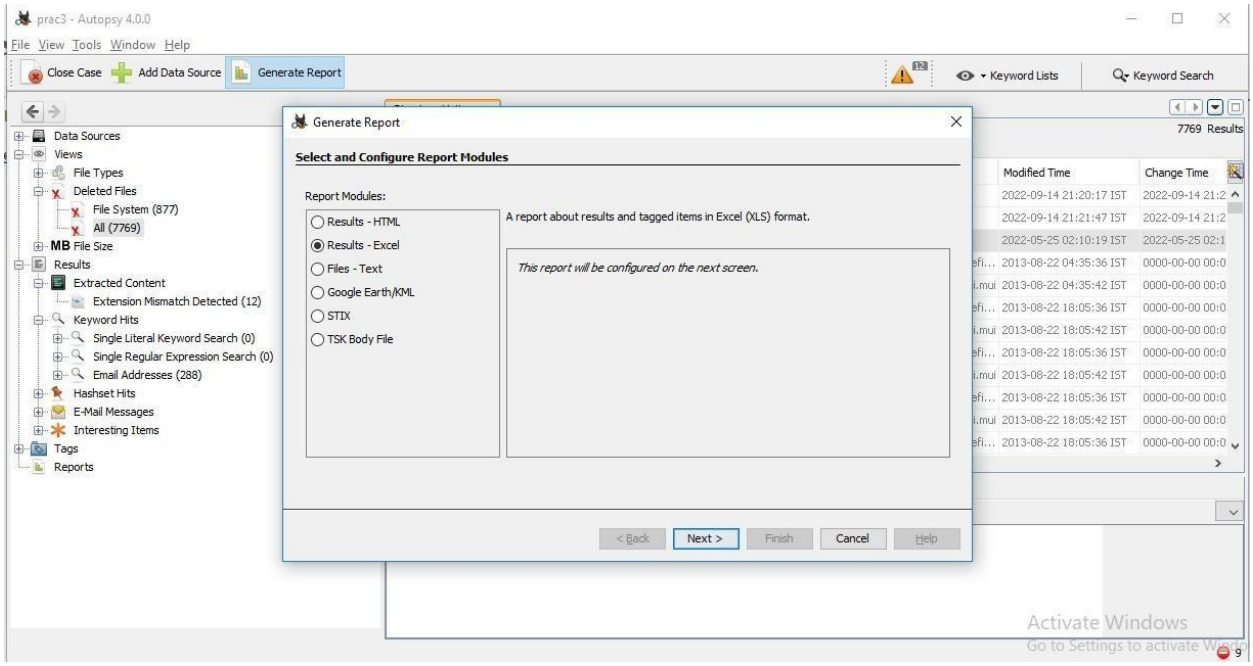
<u>Step 10:</u> The following window will appear which shows us that Files are extracted.



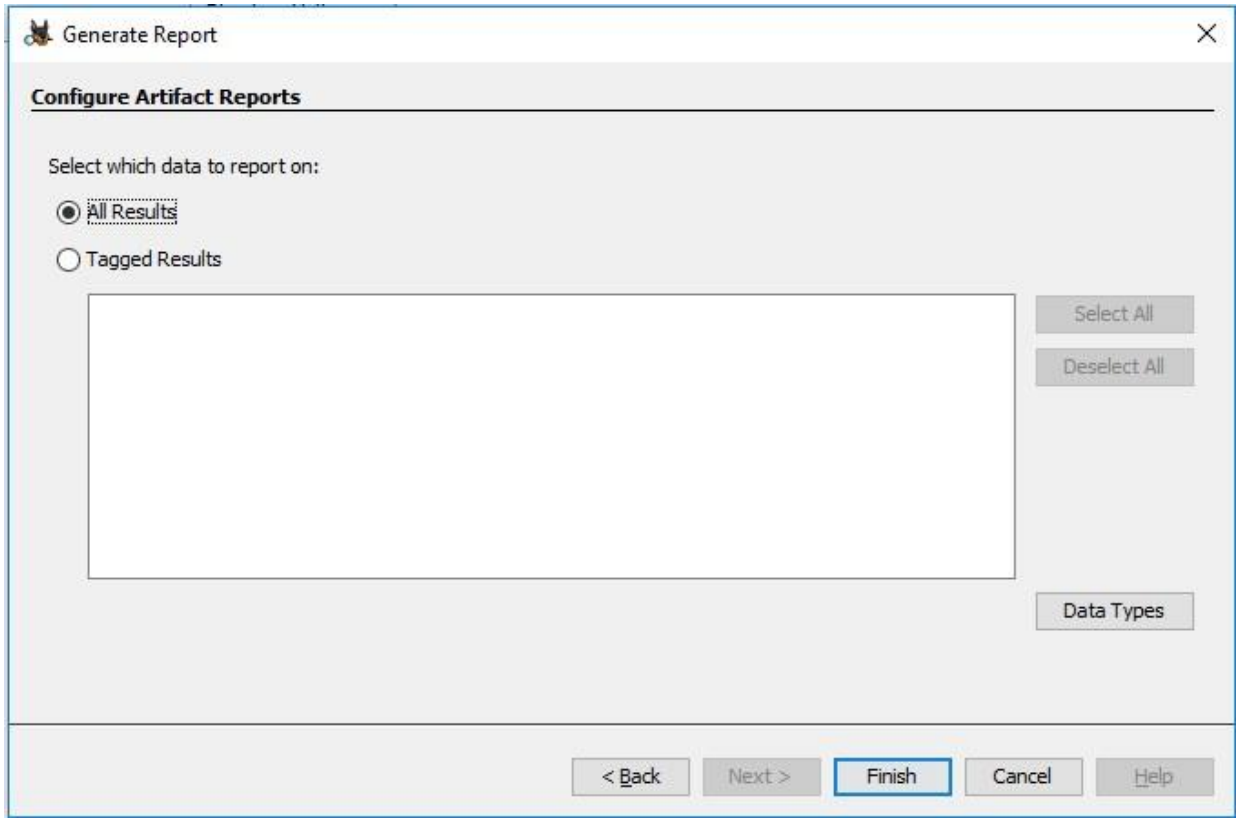
<u>Step 11:</u> We can see the deleted file in the "Export" folder as below.



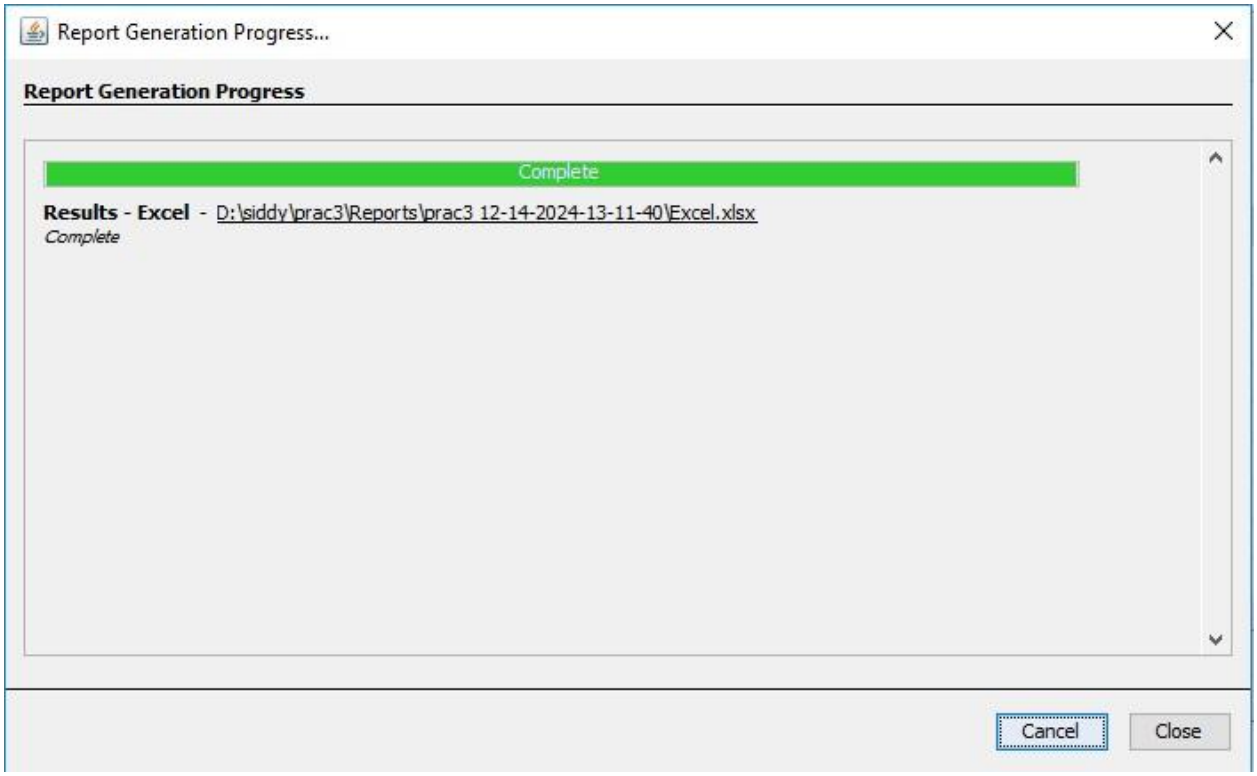
<u>Step 12:</u> Now click on the "Generate Report" seen in the top bar and select the option of Results-Excel.



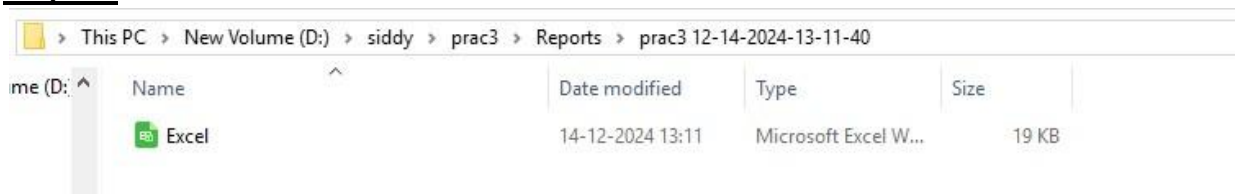
<u>Step 13:</u> Now click on Finish.



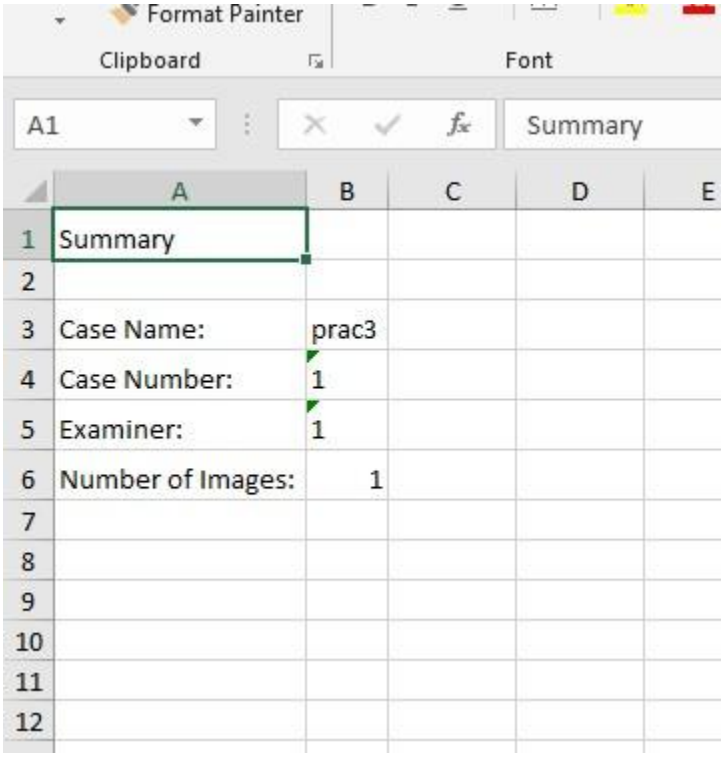
<u>Step 14:</u> We can see that the "Report Generation Process" is being completed.



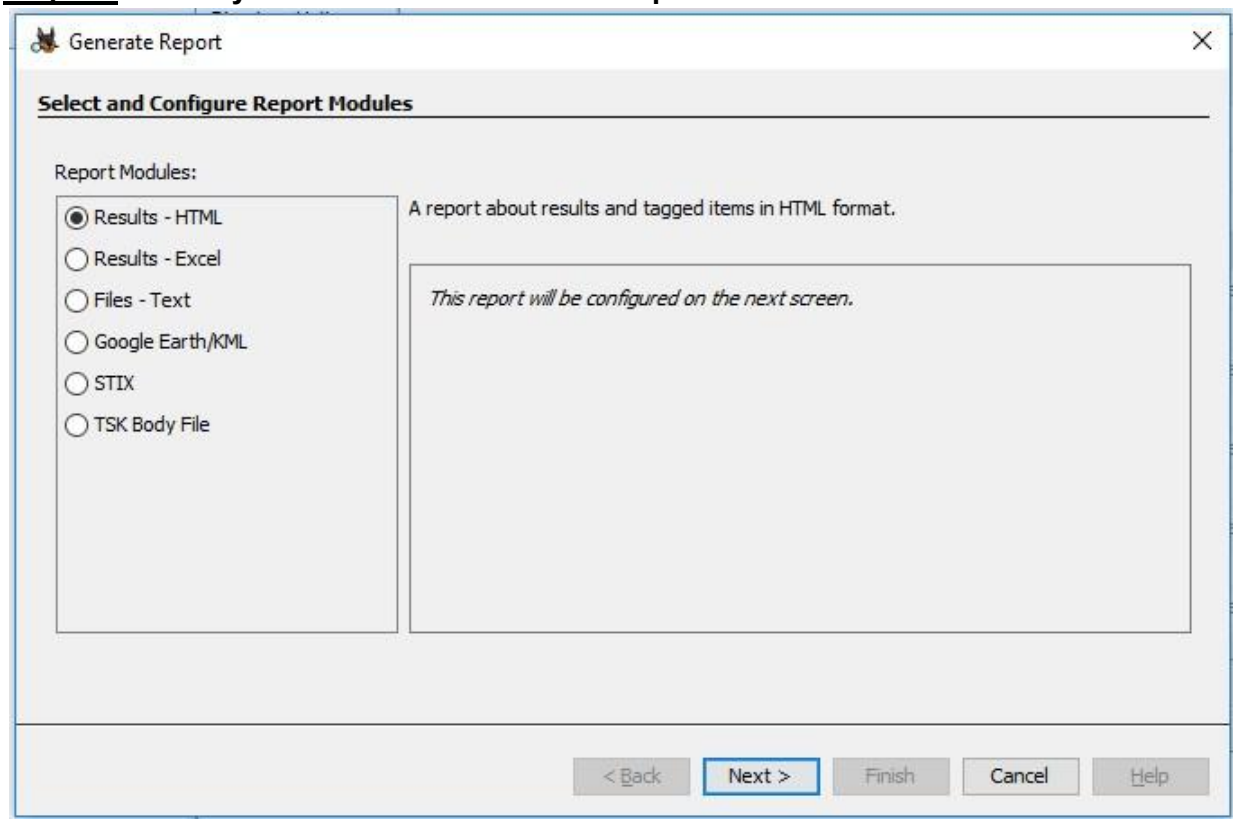
<u>Step 15:</u> The created Excel file will be shown in the Folder we created as below.



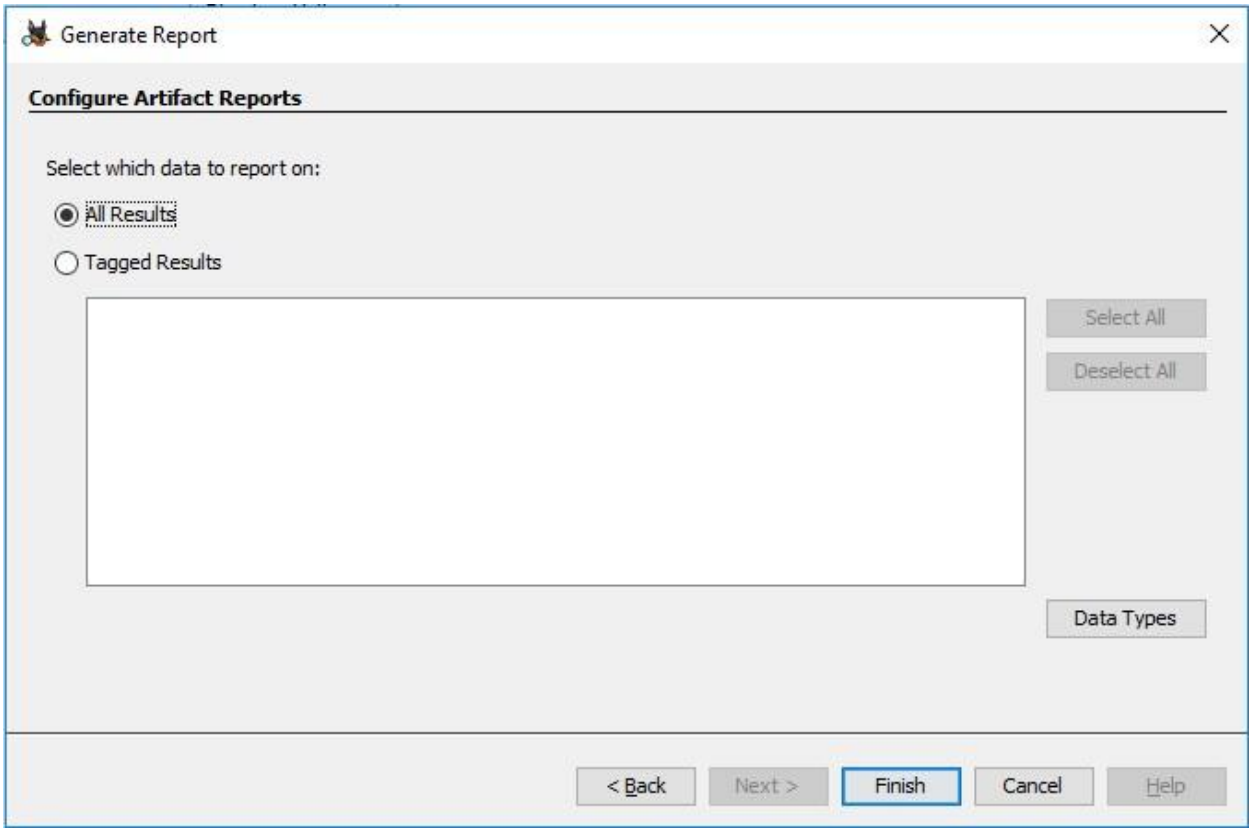
<u>Step 16:</u> Open the Excel file and the Summary of the Image file will be shown.



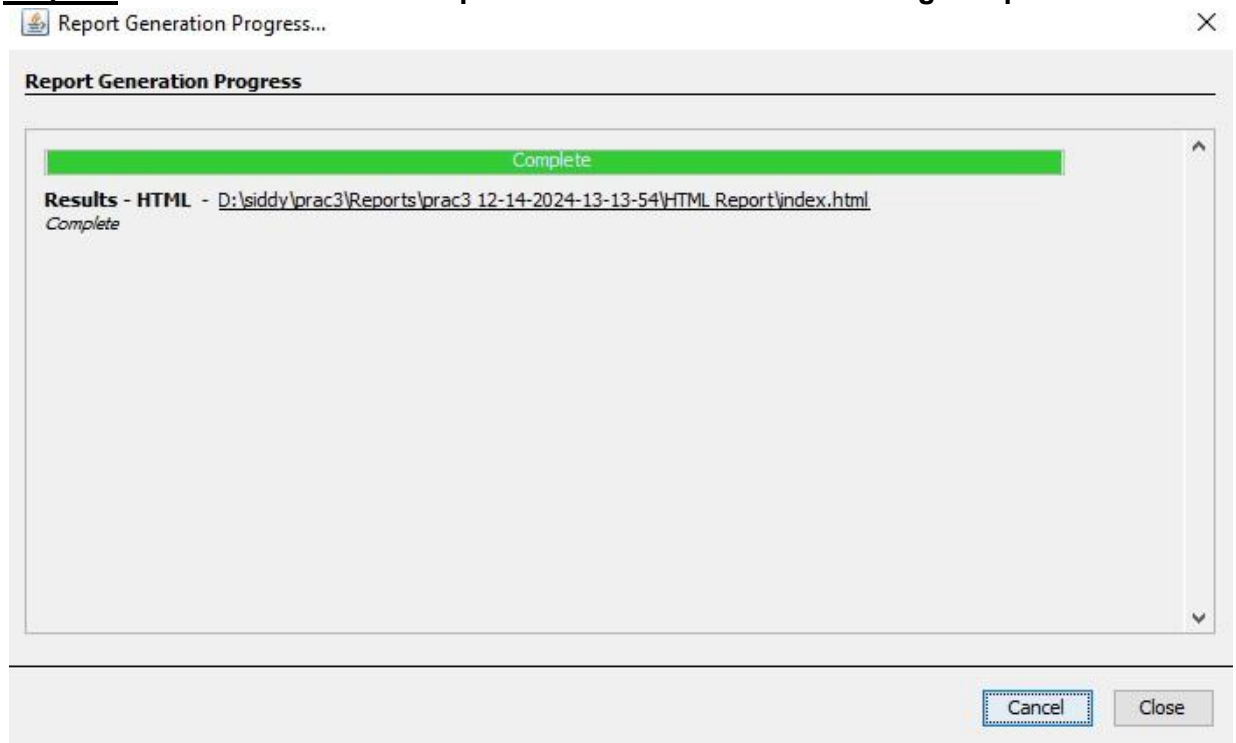
<u>Step 17:</u> Similarly select the "Results-HTML" option. Click on Next.



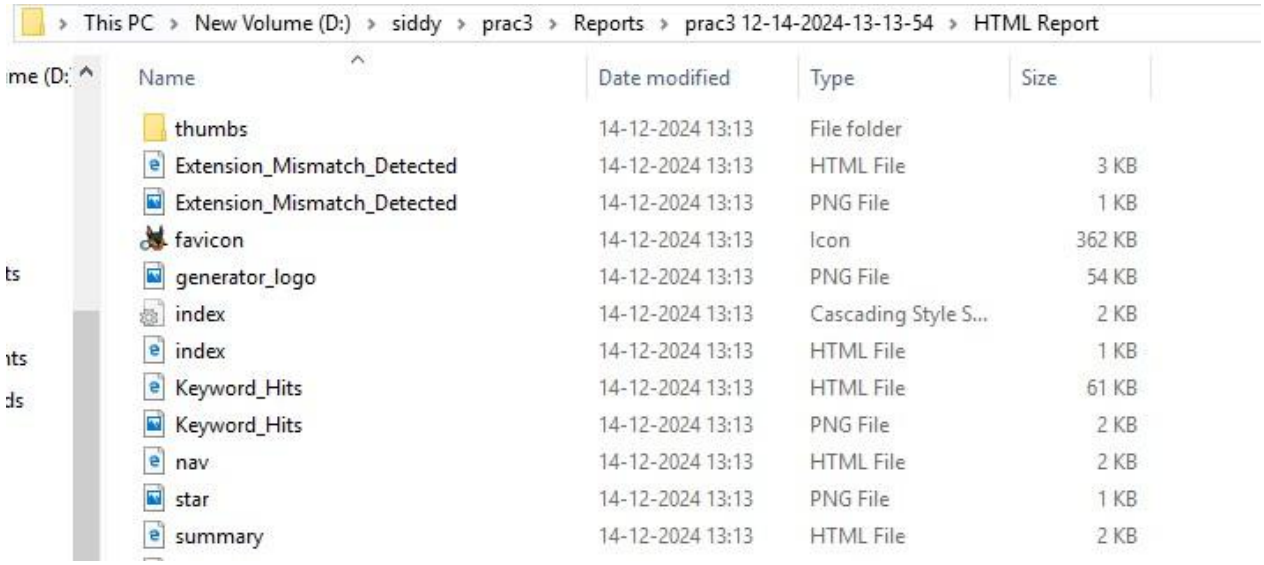
<u>Step 18:</u> Click on Finish.



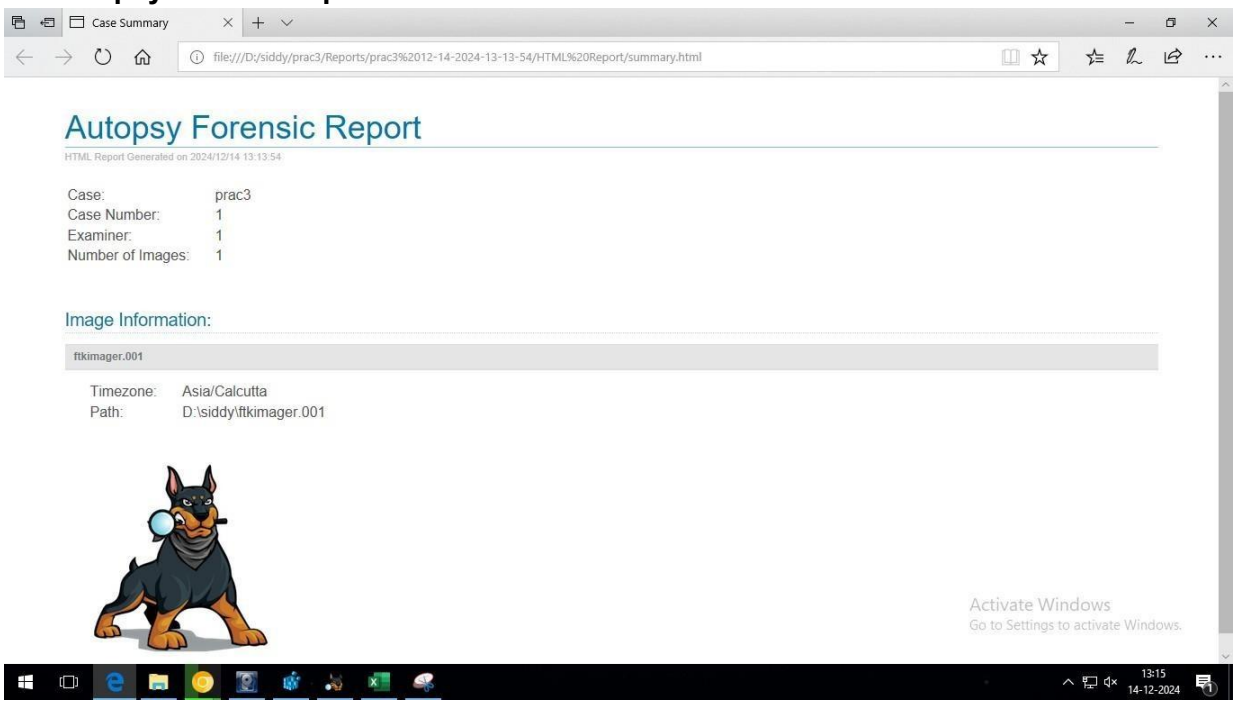
Step 19: **We can see that the "Report Generation Process" is being completed.**



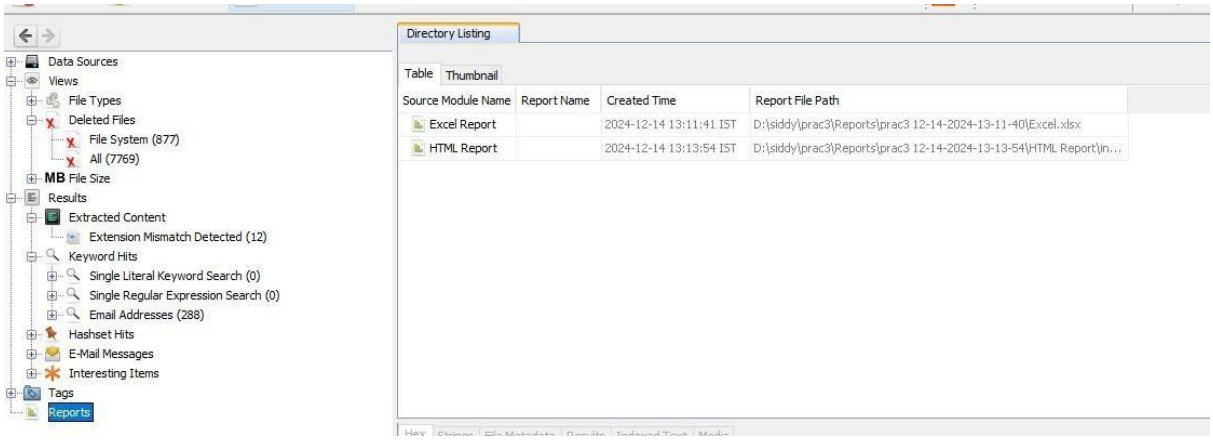
Step 20: **The "Results-HTML" report will be saved in the file we created as follows.**



<u>Step 21:</u> Click on summary html file and it will direct you to the browser window showing the autopsy forensic report.



<u>Step 22:</u> The Reports we created will be shown here which consist of Excel and HTML.


Data Sources
Views
File Types
Deleted Files
File System (877)
All (7769)
MB File Size
Results
Extracted Content
Extension Mismatch Detected (12)
Keyword Hits
Single Literal Keyword Search (0)
Single Regular Expression Search (0)
Email Addresses (288)
Hashset Hits
E-Mail Messages
Interesting Items
Tags
Reports
Directory Listing
Table
Thumbnail
Source Module Name
Report Name
Created Time
Report File Path
Excel Report
2024-12-14 13:11:41 IST
D:\siddy\prac3\Reports\prac3 12-14-2024-13-11-40\Excel.xlsx
HTML Report
2024-12-14 13:13:54 IST
D:\siddy\prac3\Reports\prac3 12-14-2024-13-13-54\HTML Report\in...

Practical 4

Date: 19-12-24

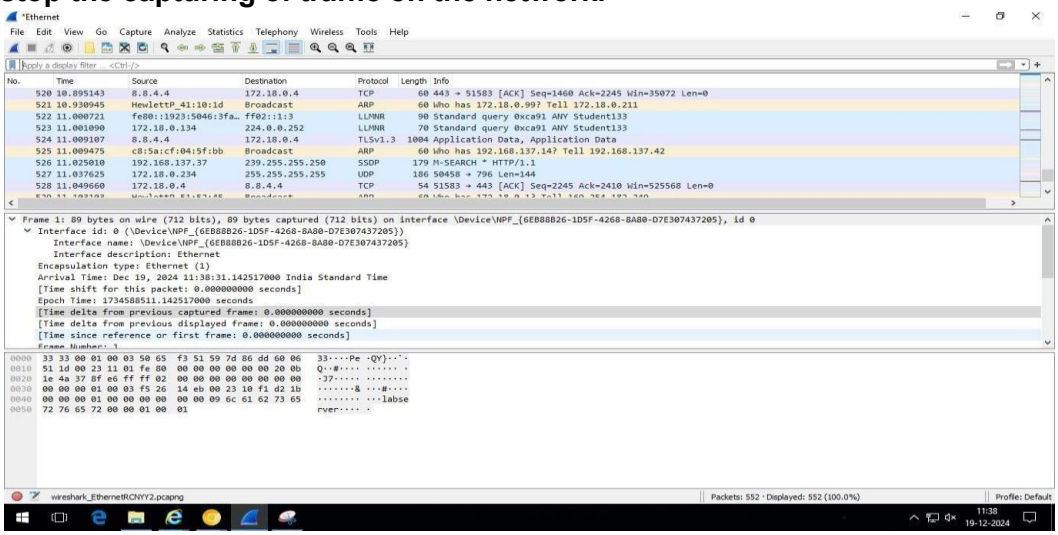
Aim: Capturing and analyzing network packets using Wireshark (Fundamentals):

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

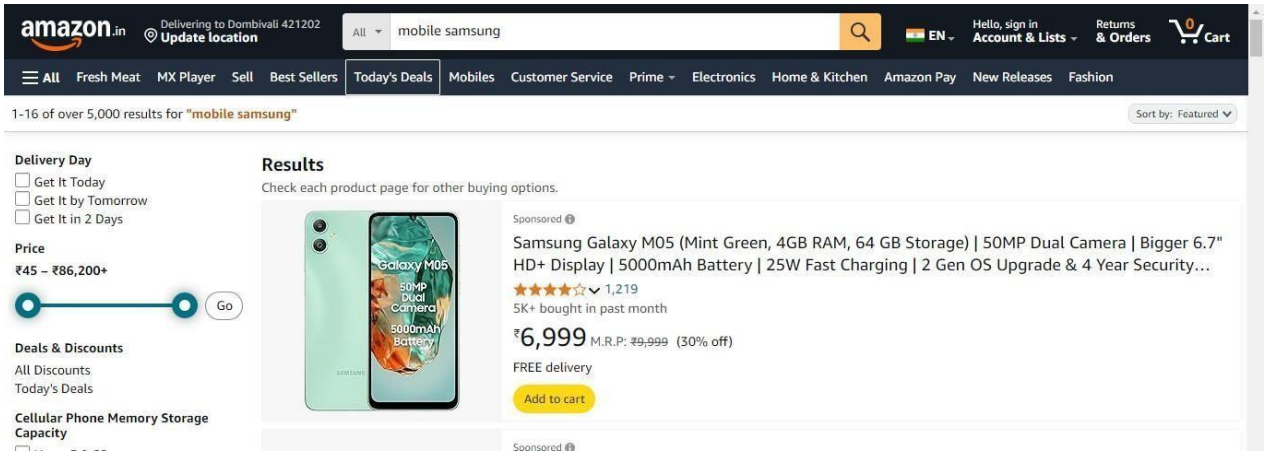
Step 1: Open Wireshark and click on Ethernet.

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

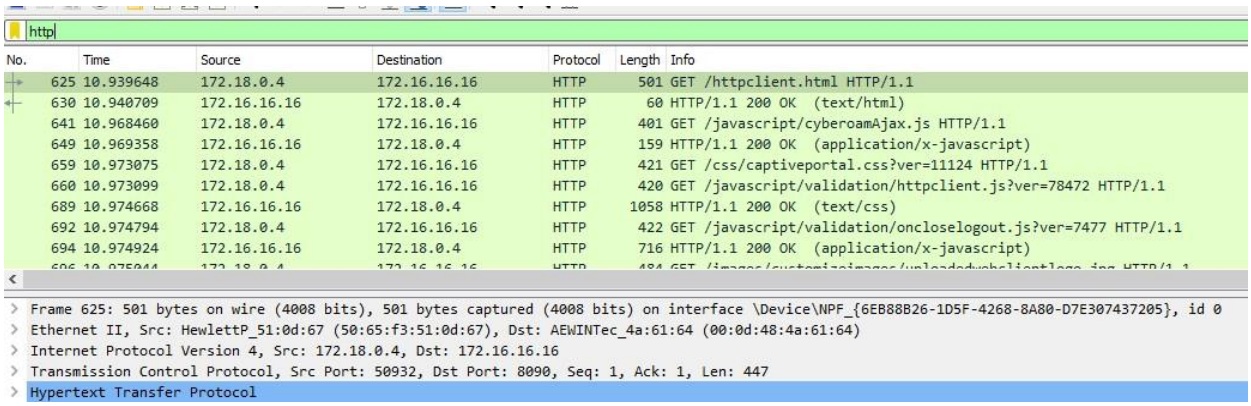
Step 2: The red box button "STOP" on the top left side of the window can be clicked to stop the capturing of traffic on the network.



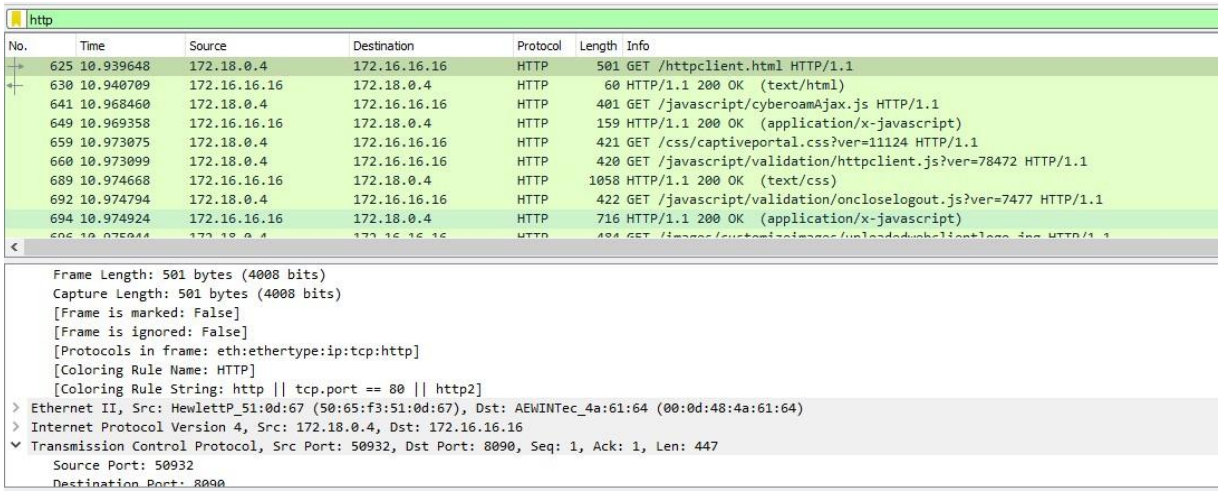
Step 3: Now go on browser and open any unsecured website i.e www.amazon.com and perform some activity on the website.



<u>Step 4:</u> Now come back to Wireshark and enter http in the search bar.

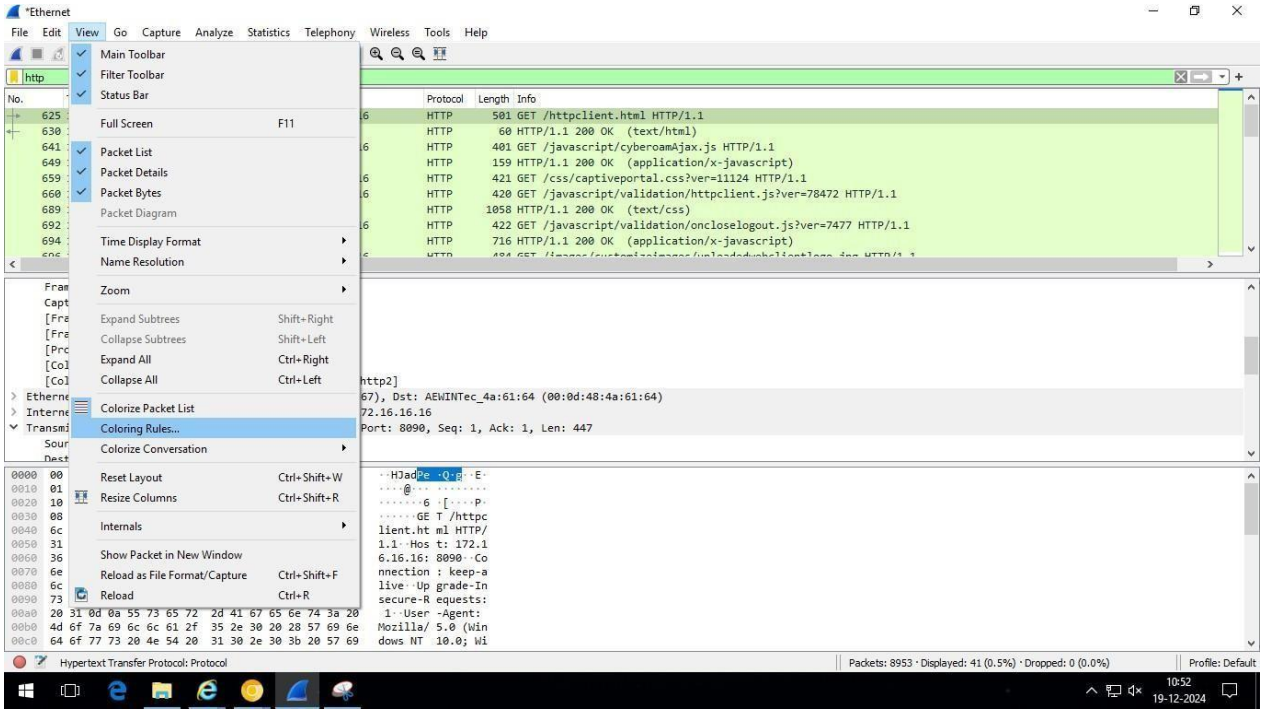


<u>Step 5:</u> Now click on the get request and see the details.

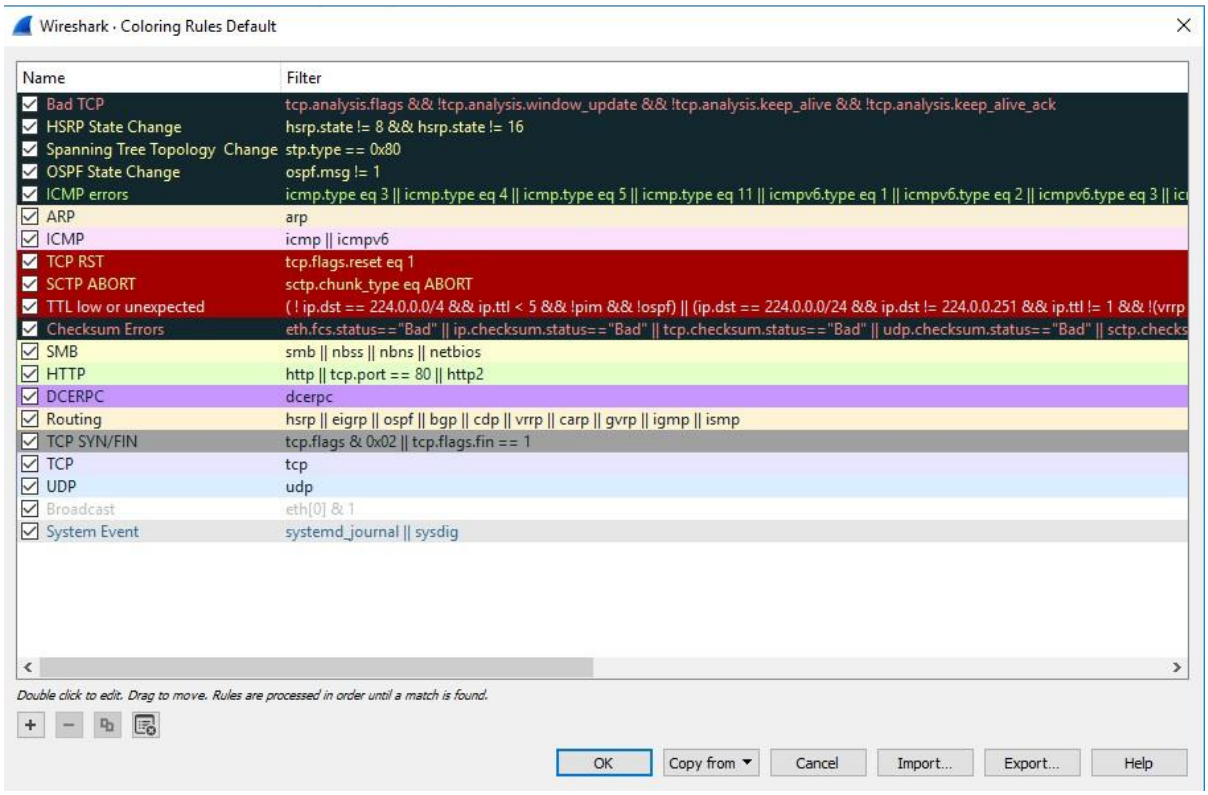


<u>Color Coding</u>

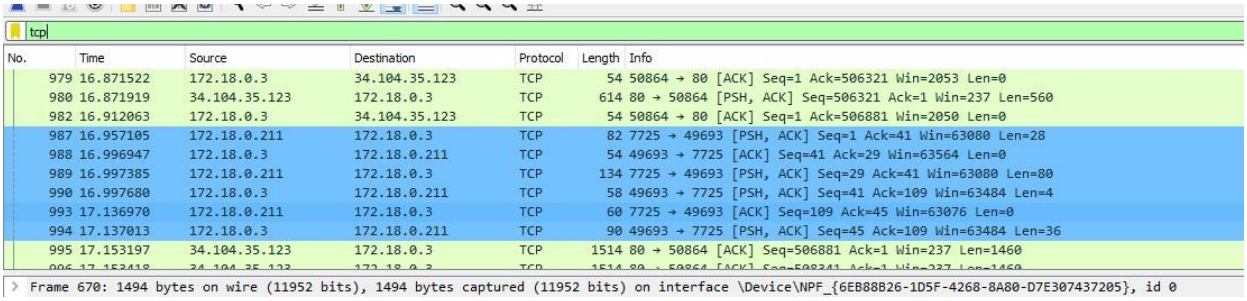
Different packets are seen highlighted in various different colors. This is Wireshark's way of displaying traffic to help you easily identify the types of it.



Default colors are:



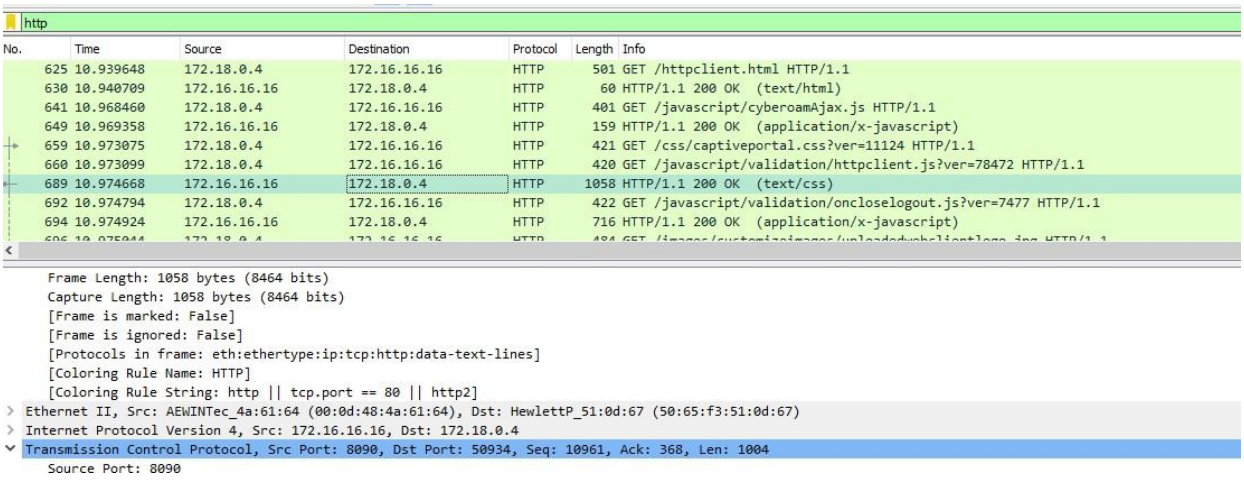
Click on the TCP packet and change the background color to any color (for eg: blue). It will appear as follows



tcp

No.	Time	Source	Destination	Protocol	Length	Info
979	16.871522	172.18.0.3	34.104.35.123	TCP	54	50864 → 80 [ACK] Seq=1 Ack=506321 Win=2053 Len=0
980	16.871919	34.104.35.123	172.18.0.3	TCP	614	80 → 50864 [PSH, ACK] Seq=506321 Ack=1 Win=237 Len=560
982	16.912063	172.18.0.3	34.104.35.123	TCP	54	50864 → 80 [ACK] Seq=1 Ack=506881 Win=2050 Len=0
987	16.957105	172.18.0.211	172.18.0.3	TCP	82	7725 → 49693 [PSH, ACK] Seq=1 Ack=41 Win=63080 Len=28
988	16.996947	172.18.0.3	172.18.0.211	TCP	54	49693 → 7725 [ACK] Seq=41 Ack=29 Win=63564 Len=0
989	16.997385	172.18.0.211	172.18.0.3	TCP	134	7725 → 49693 [PSH, ACK] Seq=29 Ack=41 Win=63080 Len=80
990	16.997680	172.18.0.3	172.18.0.211	TCP	58	49693 → 7725 [PSH, ACK] Seq=41 Ack=109 Win=63484 Len=4
993	17.136970	172.18.0.211	172.18.0.3	TCP	60	7725 → 49693 [ACK] Seq=109 Ack=45 Win=63076 Len=0
994	17.137013	172.18.0.3	172.18.0.211	TCP	90	49693 → 7725 [PSH, ACK] Seq=45 Ack=109 Win=63484 Len=36
995	17.153197	34.104.35.123	172.18.0.3	TCP	1514	80 → 50864 [ACK] Seq=506881 Ack=1 Win=237 Len=1460

> Frame 670: 1494 bytes on wire (11952 bits), 1494 bytes captured (11952 bits) on interface \Device\NPF_{6EB88B26-1D5F-4268-8A80-D7E307437205}, id 0



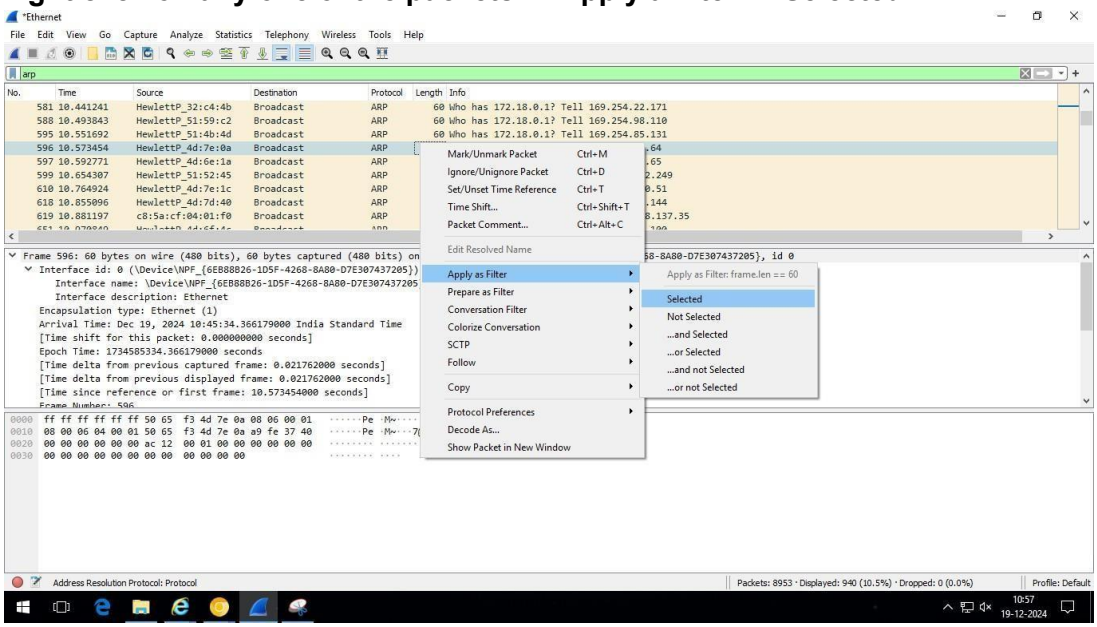
http

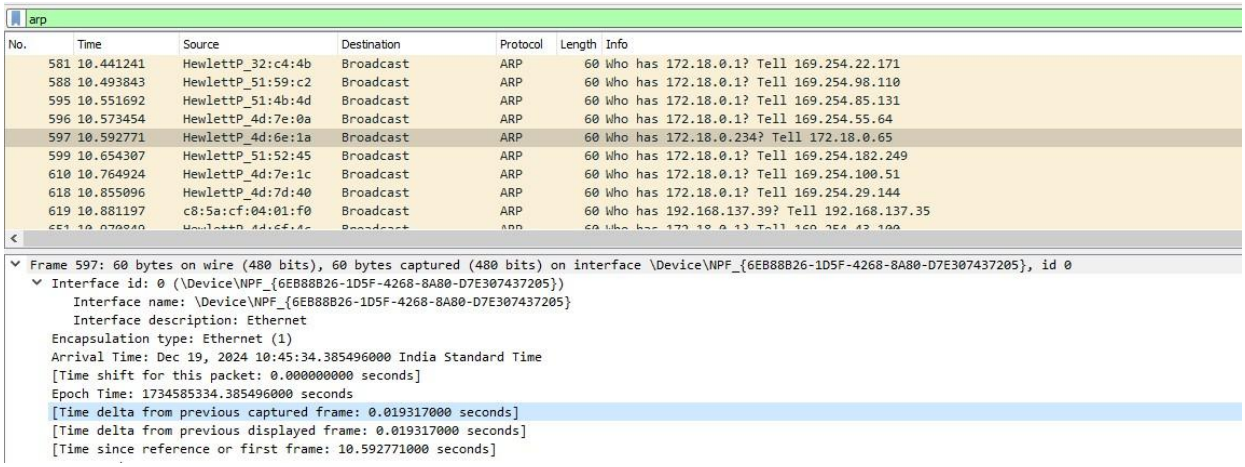
No.	Time	Source	Destination	Protocol	Length	Info
625	10.939648	172.18.0.4	172.16.16.16	HTTP	501	GET /httpclient.html HTTP/1.1
630	10.940709	172.16.16.16	172.18.0.4	HTTP	60	HTTP/1.1 200 OK (text/html)
641	10.968460	172.18.0.4	172.16.16.16	HTTP	401	GET /javascript/cyberoamAjax.js HTTP/1.1
649	10.969358	172.16.16.16	172.18.0.4	HTTP	159	HTTP/1.1 200 OK (application/x-javascript)
659	10.973075	172.18.0.4	172.16.16.16	HTTP	421	GET /css/captiveportal.css?ver=11124 HTTP/1.1
660	10.973099	172.18.0.4	172.16.16.16	HTTP	420	GET /javascript/validation/httpclient.js?ver=78472 HTTP/1.1
689	10.974668	172.16.16.16	172.18.0.4	HTTP	1058	HTTP/1.1 200 OK (text/css)
692	10.974794	172.18.0.4	172.16.16.16	HTTP	422	GET /javascript/validation/oncloselogout.js?ver=7477 HTTP/1.1
694	10.974924	172.16.16.16	172.18.0.4	HTTP	716	HTTP/1.1 200 OK (application/x-javascript)

```
    Frame Length: 1058 bytes (8464 bits)
    Capture Length: 1058 bytes (8464 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http:data-text-lines]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
> Ethernet II, Src: AEWINTec_4a:61:64 (00:0d:48:4a:61:64), Dst: HewlettP_51:0d:67 (50:65:f3:51:0d:67)
> Internet Protocol Version 4, Src: 172.16.16.16, Dst: 172.18.0.4
v Transmission Control Protocol, Src Port: 8090, Dst Port: 50934, Seq: 10961, Ack: 368, Len: 1004
    Source Port: 8090
```

Analyze the captured packets arp

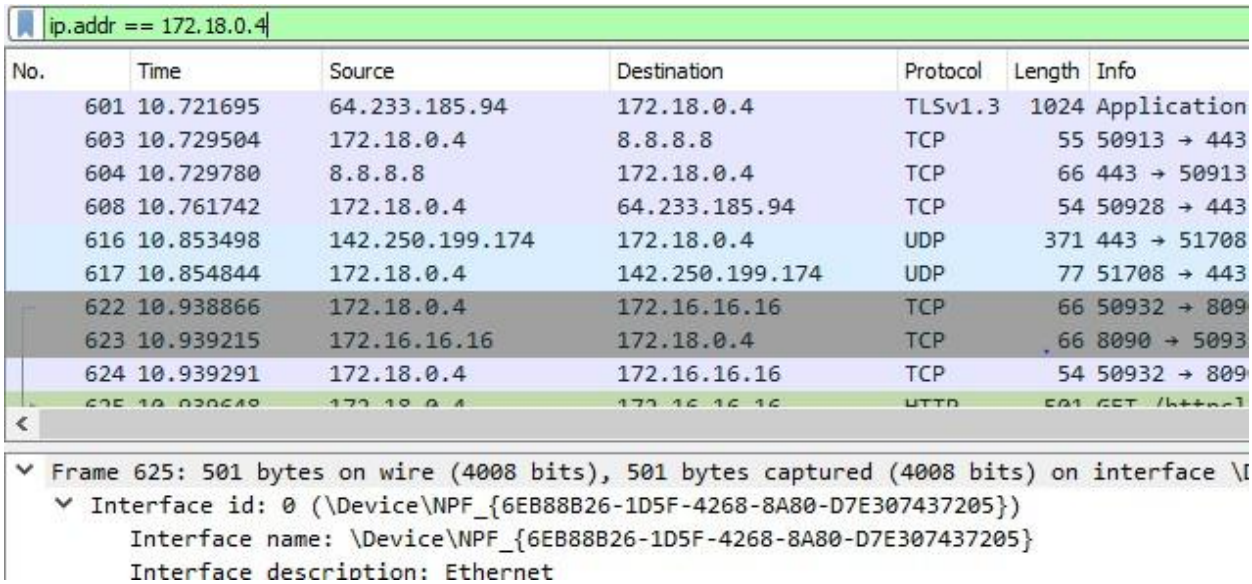
Right click on any one of the packets → Apply a filter → Selected



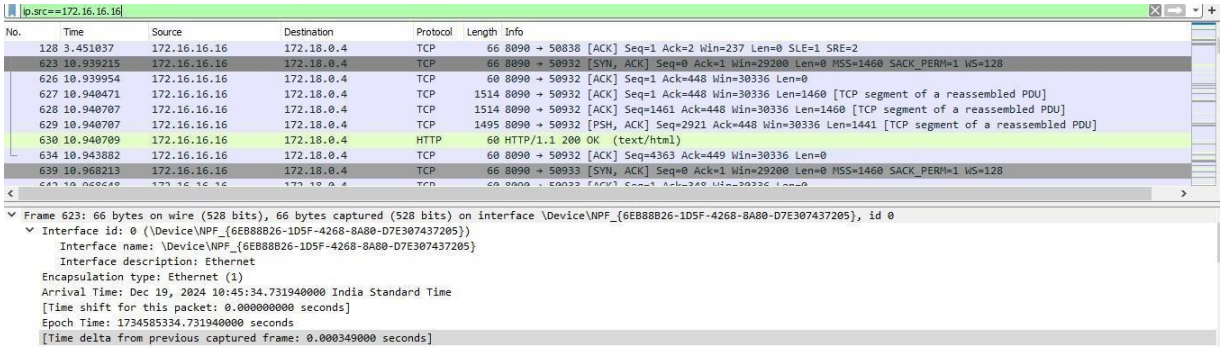


Display filter command

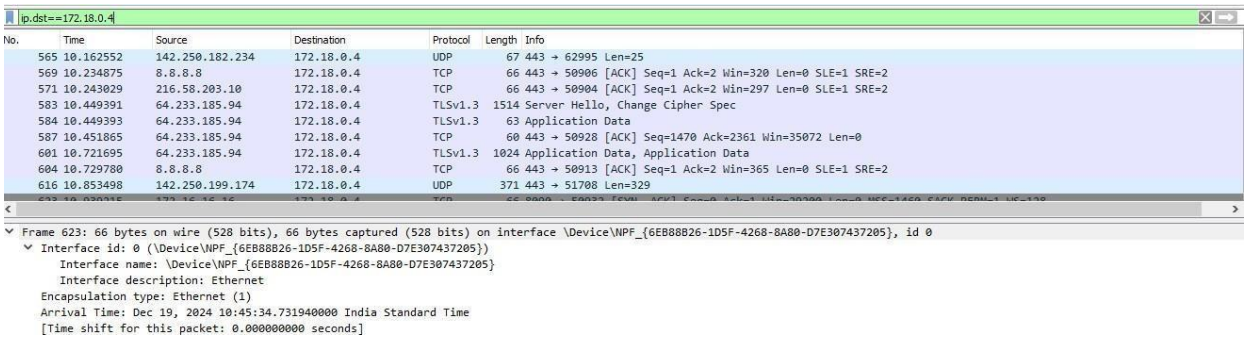
1. **Display packets based on specific IP addresses. ip.addr==172.18.0.4**



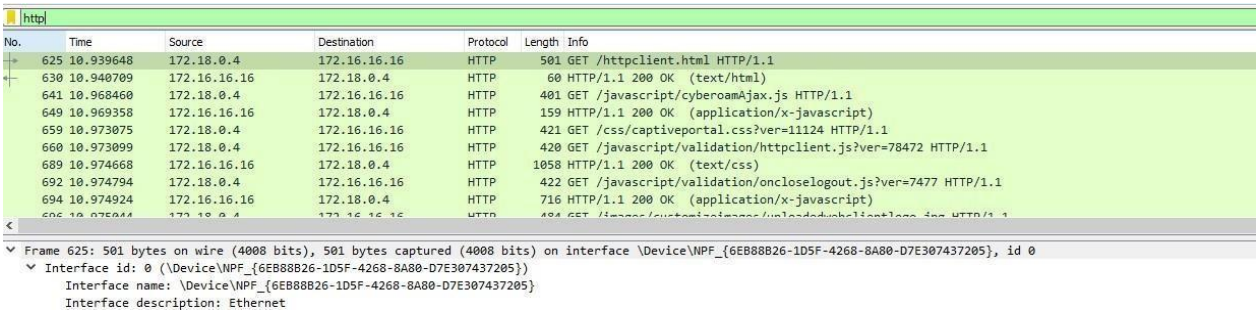
2. **Display packets which are coming from a specific IP address. ip.src==172.16.16.16**



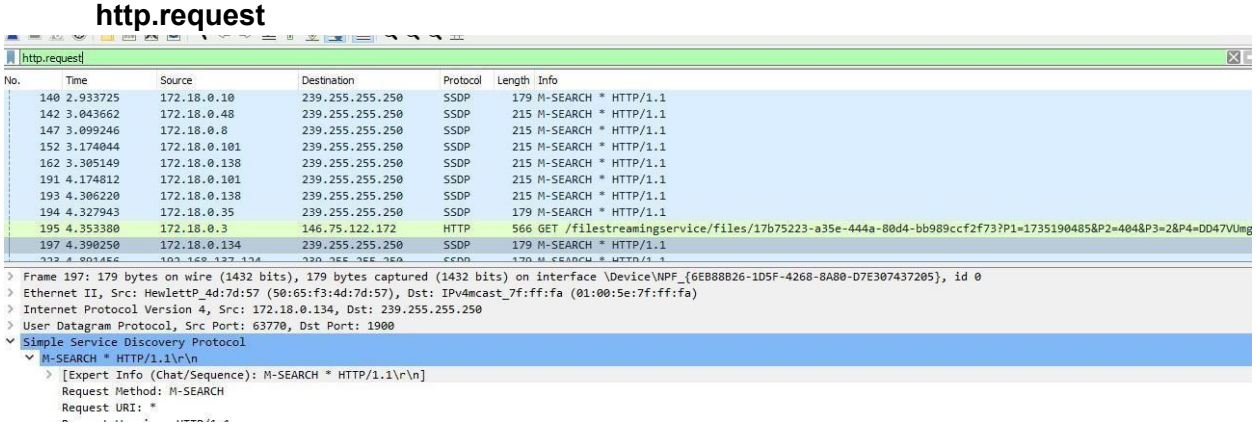
3. **Display packets which are coming from specific IP address destination. ip.dst==172.18.0.4**



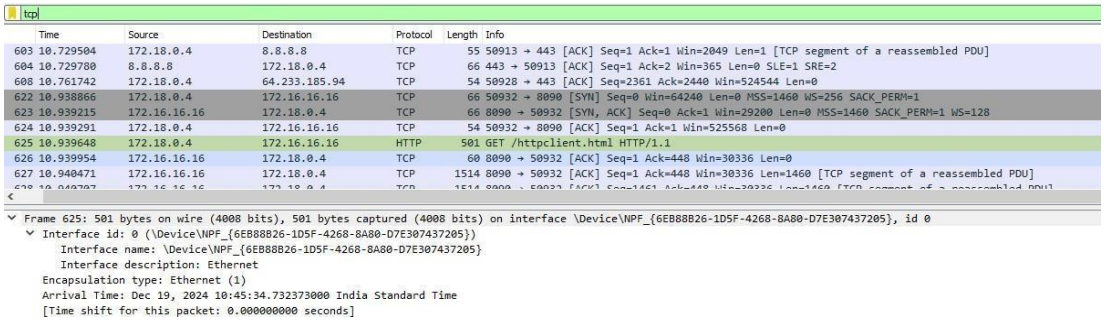
4. **Display packets which are having http as protocol. http**



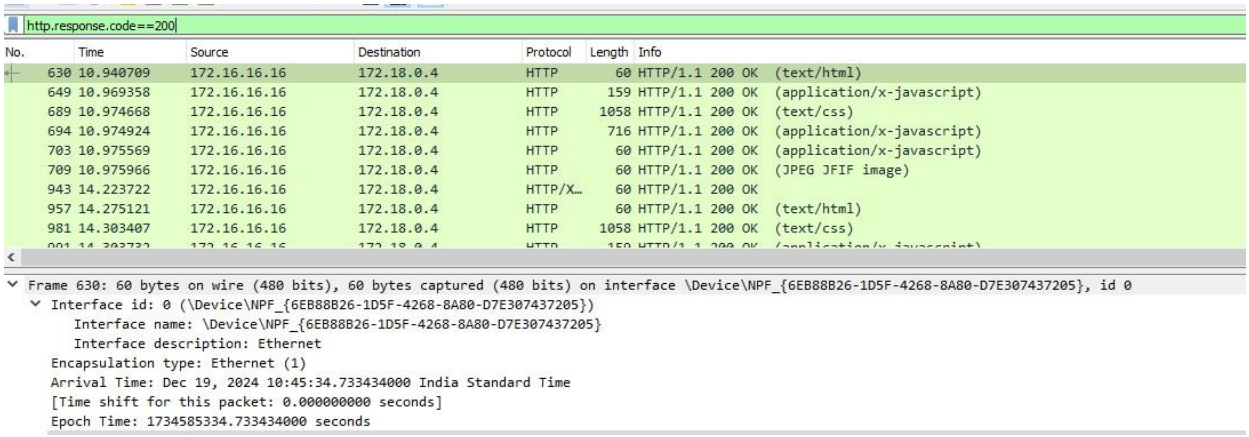
5. **Display packets which are using http request. http.request**



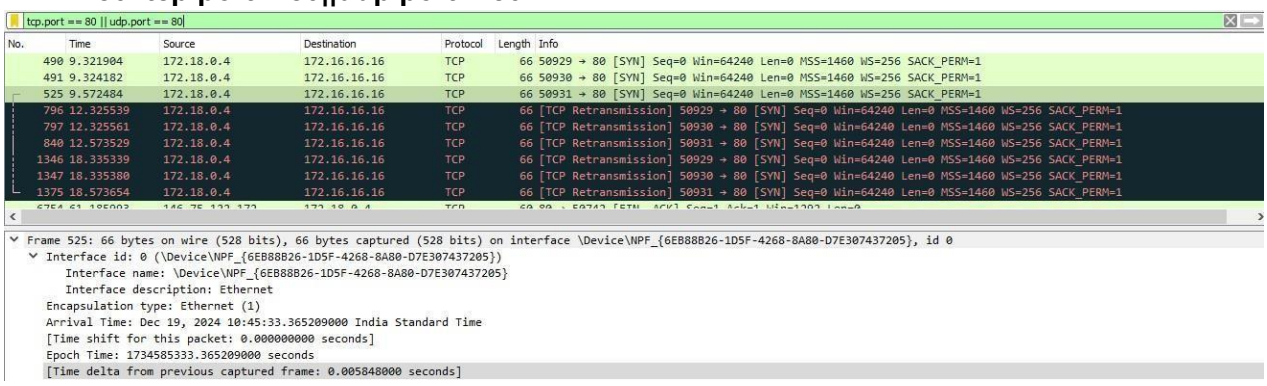
6. **Display packets which are using TCP protocol. tcp**



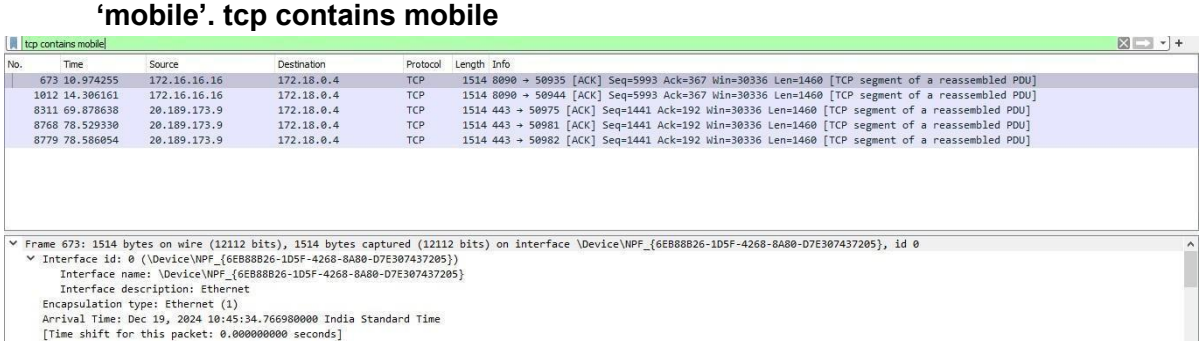
7. **Display packets having no error connecting to the server. http.response.code ==200**



8. **Display packets having port number 80. tcp.port==80||udp.port==80**



9. **Display packets which contain the keyword 'mobile'. tcp contains mobile**



Practical 5

Date: 21-12-24

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

What web server software is used by www.snopes.com?

About what cell phone problem is the client concerned about?

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

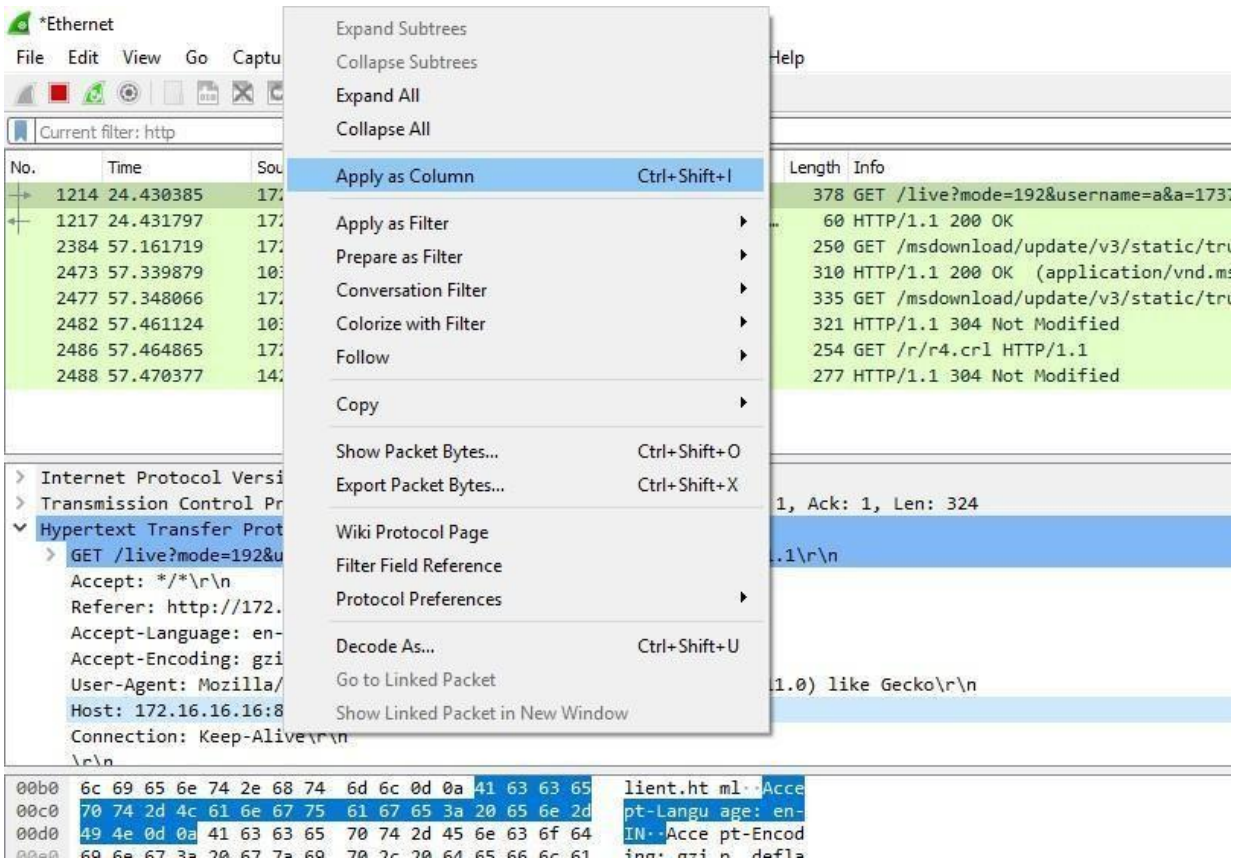
How many web servers are running in Apache?

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

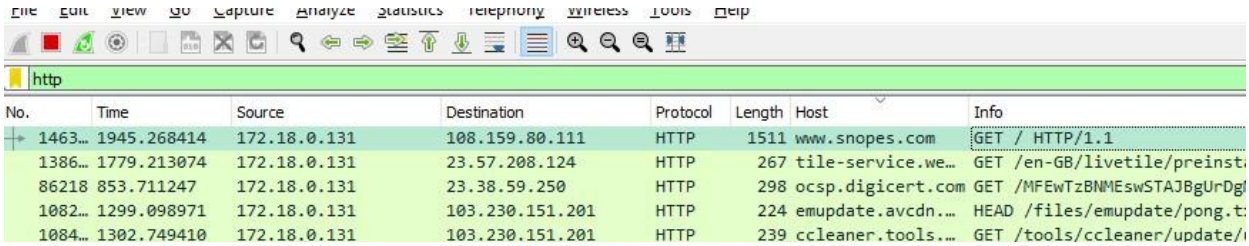
Steps:

1) What web server software is issued by www.snopes.com?

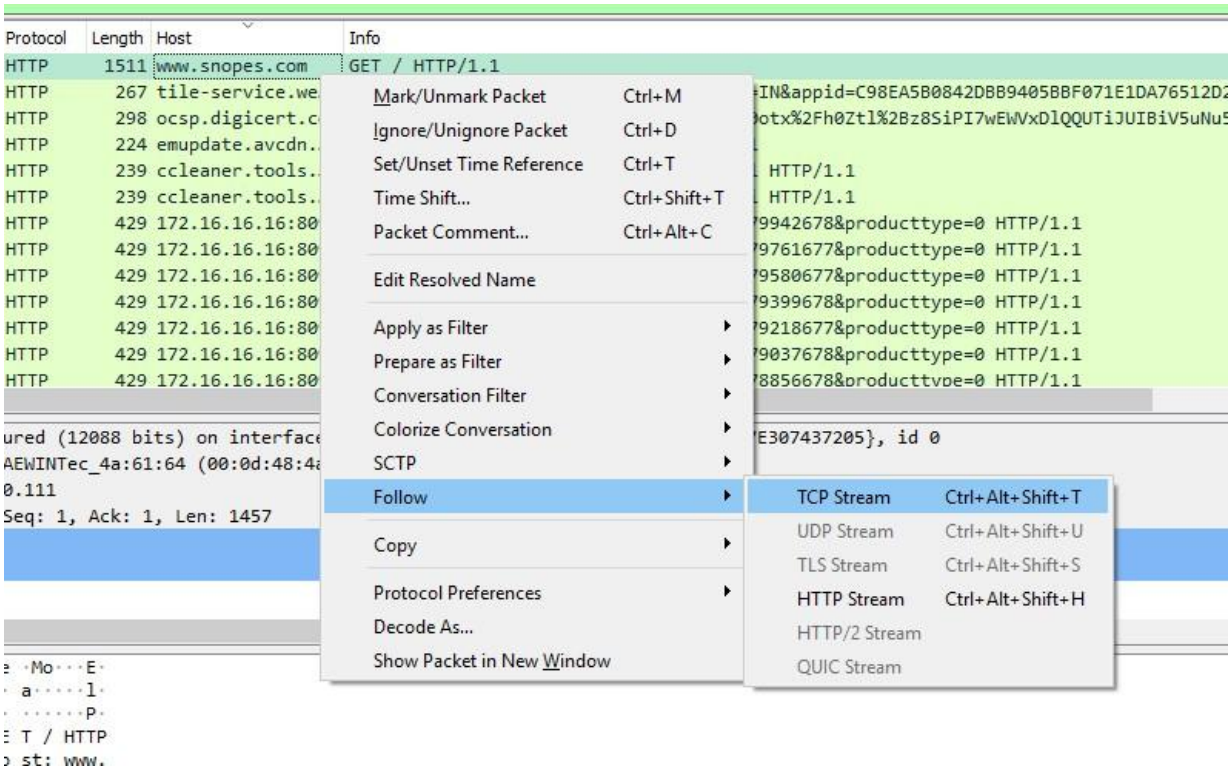
Analysis – The domain name be found from host header so we will set host header column where we will see all domain names. Select any HTTP request and expand the Hypertext Transfer Protocol then right click on Host header and then Apply as a Column.



Step 2: **Here we can see www.snopes.com in the host.**



Step 3: **Right click on the selected packet and then select Follow TCP stream.**



<u>Step 4:</u> Now we can see the web server name in server header as "CloudFront".

```
GET / HTTP/1.1
Host: www.snopes.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.6
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,ap
signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: _ga=GA1.1.1645644063.1737178243; _fbp=fb.1.1737178245683.355092851141826554; _tt_enable_cookie=1; _
L3EjMk4xIojo5LQ.tt.1; sharedid=2cc8191a-ecb8-41cd-89ce-d4681e91201d; sharedid_cst=SCwaLHgsZg%3D%3D;
newsletter_signup_promo=true; newsletter_signup_views=1; _lr_retry_request=true; _lr_env_src_ats=false; pbj
unifiedid=%7B%22TDID%22%3A%22d9a5c6f6-
e04d-4461-9a81-07f4ddcb98de%22%2C%22TDID_LOOKUP%22%3A%22TRUE%22%2C%22TDID_CREATED_AT%22%3A%222024-12-18T05%
pbjs-unifiedid_cst=SCwaLHgsZg%3D%3D;
FCNEC=%5B%5B%22AKsRol85nubYNM9O_mqlUuWnPsJP89fa173uPV1u9zWV1k5eTplKYBSbmtaXjDElyTmceFujhScDkFPyZhHTPEsR58de
IjdgZq_Qm4OwqqLzlUQav19-qWrlnBfXw1UK_m-R_NLk3EcXvXsQgA%3D%3D%22%5D%5D;
cto_bundle=owBvPl85dHltSU4lMkJRazg4MGtKaSUyQmlUenhSJTJGamZDNiUyQnpQRFk3cVB1OFJOMG9ZUTdmb2FjM3VkWjhGUklWJTJC
dklMQmElMkZvVEVITG9JN2hYcWJhQTV5dllhRVBCZHFPSllMRmFRcEh0RlhDakJtNSUyRmc0UE5CaCUyRkxzQTl0M0F0dkp5aTZER3VERVE
E; _ga_Q9SR89WW85=GS1.1.1737178243.1.1.1737179962.0.0.0

HTTP/1.1 301 Moved Permanently
Server: CloudFront
Date: Sat, 18 Jan 2025 05:59:38 GMT
Content-Type: text/html
Content-Length: 167
Connection: keep-alive
Location: https://www.snopes.com/
X-Cache: Redirect from cloudfront
Via: 1.1 e3fa108e9b3fe9d22878ae63261b1a56.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: BOM78-P6
X-Amz-Cf-Id: lJpaVY_Y7foDgQ8c5mYHrIH1NEoWJ0RM1diw_wwU68CvSiN5WhkT8Q==

<html>
<head><title>301 Moved Permanently</title></head>
<body>
<center><h1>301 Moved Permanently</h1></center>
<hr><center>CloudFront</center>
```

2) What cell phone problem is the client concerned about?

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

frame matches cell

No.	Time	Source	Destination	Protocol	Length	Host	Info
74319	204.924257	172.16.16.16	172.18.0.130	TCP	1514		8090 → 63761 [ACK] Seq=1461 Ack=448 Win=30336 Len=1460 [TCP segment of a reassembled
74320	204.924258	172.16.16.16	172.18.0.130	TCP	1495		8090 → 63761 [PSH, ACK] Seq=2921 Ack=448 Win=30336 Len=1441 [TCP segment of a reassem
74912	208.006737	172.16.16.16	172.18.0.130	TCP	1514		8090 → 63773 [ACK] Seq=1461 Ack=499 Win=30336 Len=1460 [TCP segment of a reassembled
74913	208.006739	172.16.16.16	172.18.0.130	TCP	1495		8090 → 63773 [PSH, ACK] Seq=2921 Ack=499 Win=30336 Len=1441 [TCP segment of a reassem
76703	227.429471	172.16.16.16	172.18.0.130	TCP	1514		8090 → 63787 [ACK] Seq=1461 Ack=448 Win=30336 Len=1460 [TCP segment of a reassembled
76704	227.429471	172.16.16.16	172.18.0.130	TCP	1495		8090 → 63787 [PSH, ACK] Seq=2921 Ack=448 Win=30336 Len=1441 [TCP segment of a reassem
76913	230.386448	172.16.16.16	172.18.0.130	TCP	1514		8090 → 63799 [ACK] Seq=1461 Ack=499 Win=30336 Len=1460 [TCP segment of a reassembled
76914	230.386449	172.16.16.16	172.18.0.130	TCP	1495		8090 → 63799 [PSH, ACK] Seq=2921 Ack=499 Win=30336 Len=1441 [TCP segment of a reassem
77257	238.606163	172.16.16.16	172.18.0.130	TCP	1514		8090 → 63808 [ACK] Seq=1461 Ack=448 Win=30336 Len=1460 [TCP segment of a reassembled

```
Transmission Control Protocol, Src Port: 8090, Dst Port: 63808, Seq: 2921, Ack: 448, Len: 1441
    Source Port: 8090
    Destination Port: 63808
    [Stream index: 128]
    [TCP Segment Len: 1441]
    Sequence Number: 2921    (relative sequence number)
    Sequence Number (raw): 2559079564
```