

Practical 1

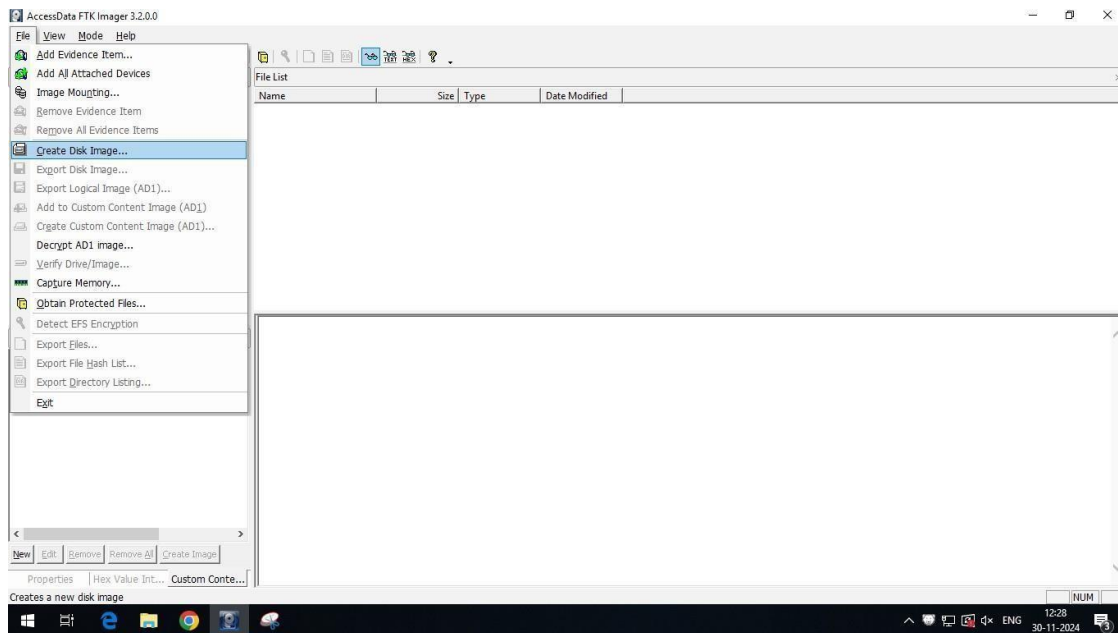
Date: 30-11-24

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

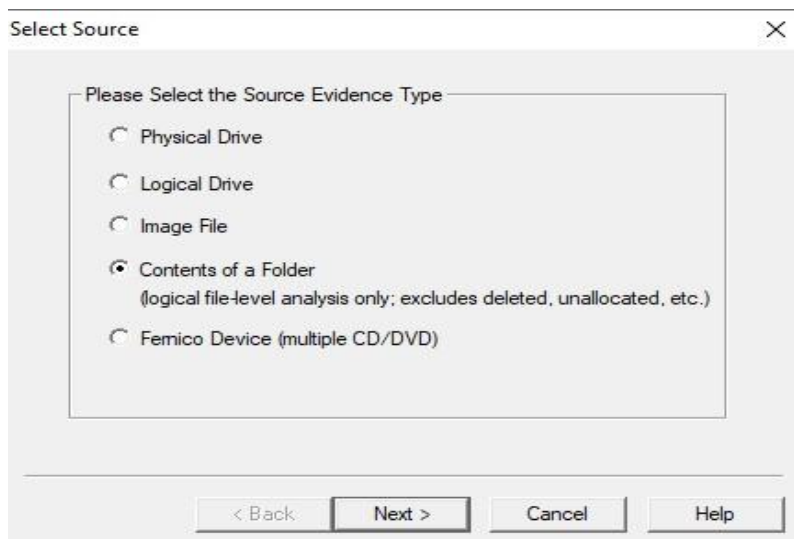
- Creating Forensic
- Check Integrity of Data
- Analyze Forensic Image

Creating Forensic:

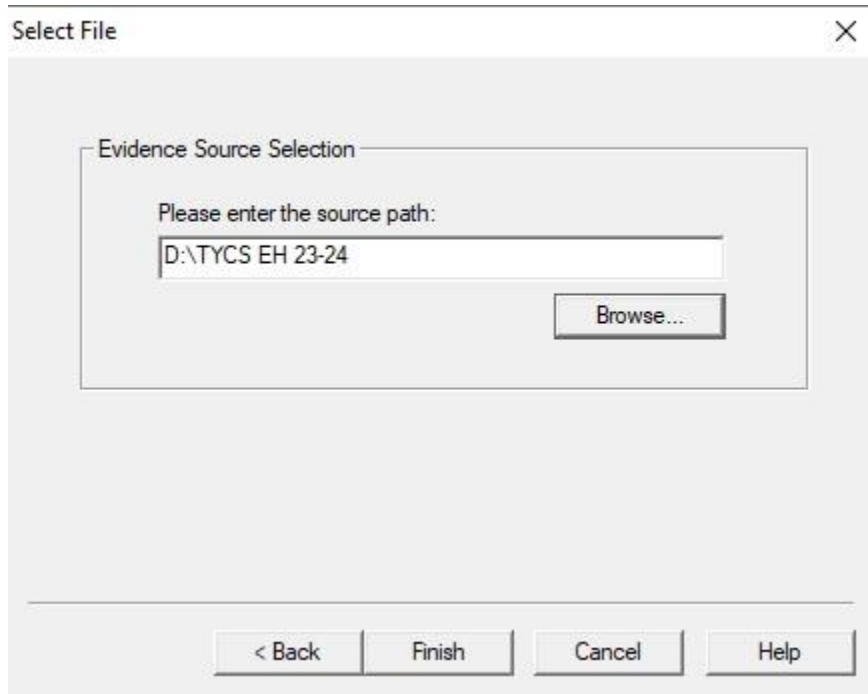
Step 1: Open AccessData FTK Imager, Click on File→Create Disk Image.



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

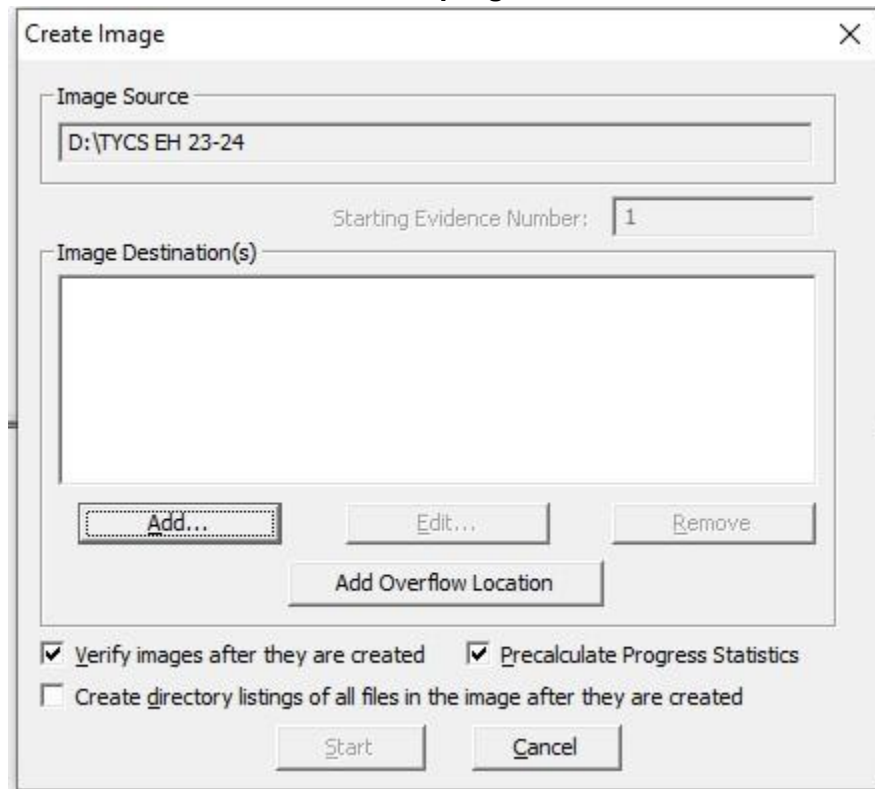


Step 3: Here browse and enter the source path of the file. Click on Finish.



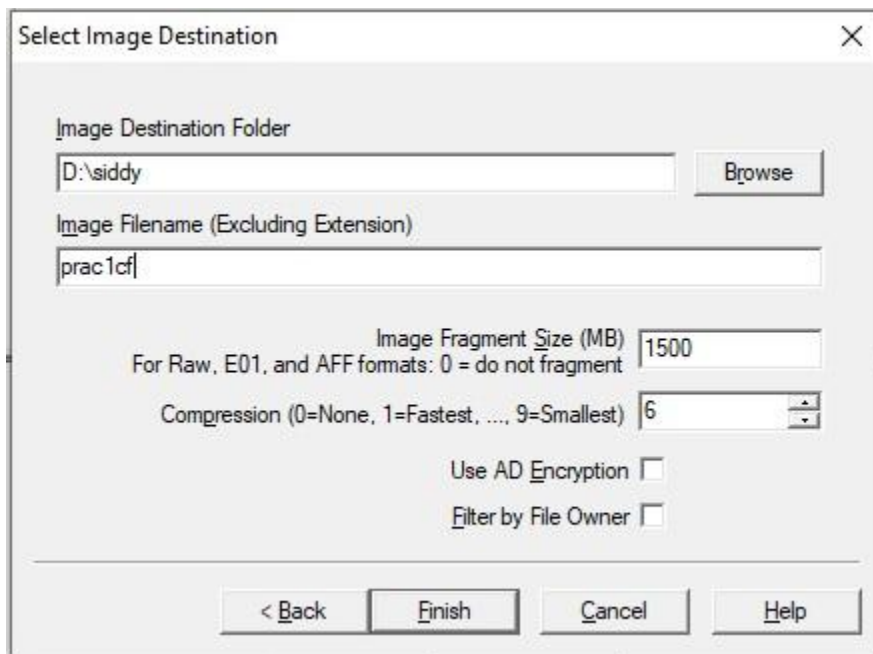
The "Select File" dialog box has a title bar with a close button (X). Inside, there is a section titled "Evidence Source Selection". Below this title, it says "Please enter the source path:". A text input field contains the path "D:\TYCS EH 23-24". To the right of the input field is a "Browse..." button. At the bottom of the dialog, there are four buttons: "< Back", "Finish", "Cancel", and "Help".

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



The "Create Image" dialog box has a title bar with a close button (X). It contains several sections: "Image Source" with a text field containing "D:\TYCS EH 23-24"; "Starting Evidence Number:" with a text field containing "1"; and "Image Destination(s)" with a large empty list box. Below the list box are three buttons: "Add..." (highlighted with a dashed border), "Edit...", and "Remove". Below these is a button labeled "Add Overflow Location". At the bottom, there are three checkboxes: "☒ Verify images after they are created", "☒ Precalculate Progress Statistics", and "☐ Create directory listings of all files in the image after they are created". At the very bottom are "Start" and "Cancel" buttons.

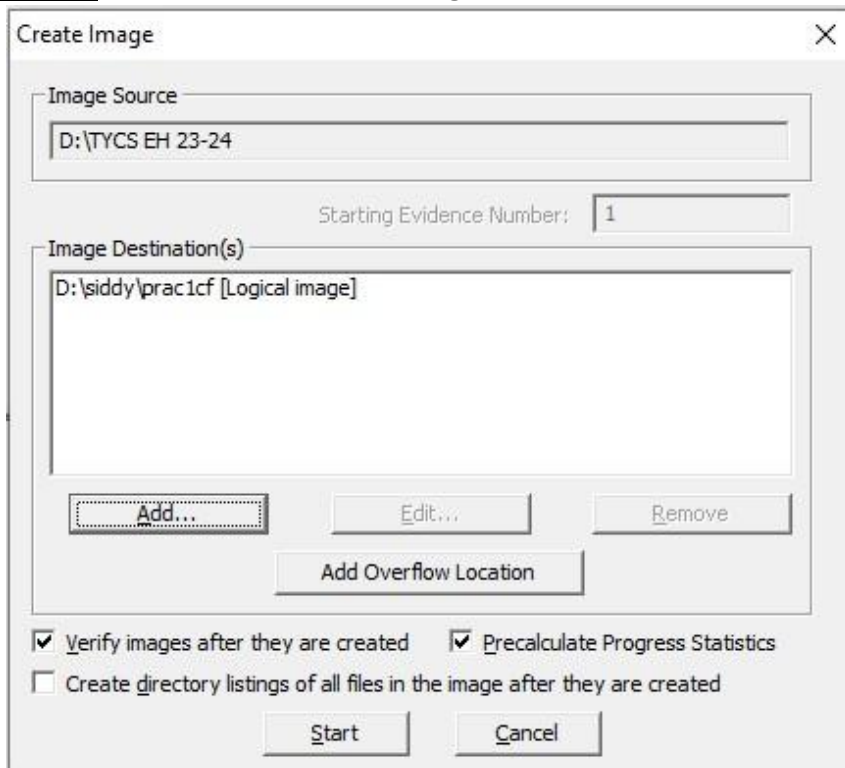
Step 5: After clicking on “Add” browse the “Image Destination Folder” and type the Image Filename. Click on Finish.



The "Select Image Destination" dialog box contains the following fields and controls:

- Image Destination Folder:** A text box containing "D:\siddy" with a "Browse" button to its right.
- Image Filename (Excluding Extension):** A text box containing "prac1cf".
- Image Fragment Size (MB):** A text box containing "1500". Below it, a note reads: "For Raw, E01, and AFF formats: 0 = do not fragment".
- Compression:** A dropdown menu showing "6". Below it, a note reads: "(0=None, 1=Fastest, ..., 9=Smallest)".
- Use AD Encryption:** An unchecked checkbox.
- Filter by File Owner:** An unchecked checkbox.
- Buttons:** "< Back", "Finish", "Cancel", and "Help" are located at the bottom.

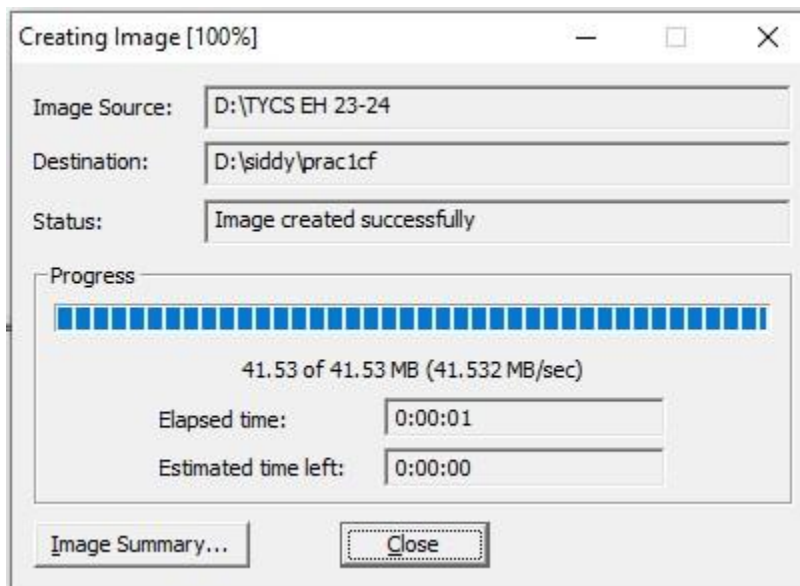
Step 6: Here we can see the Image Destination. Now click on “Start”.



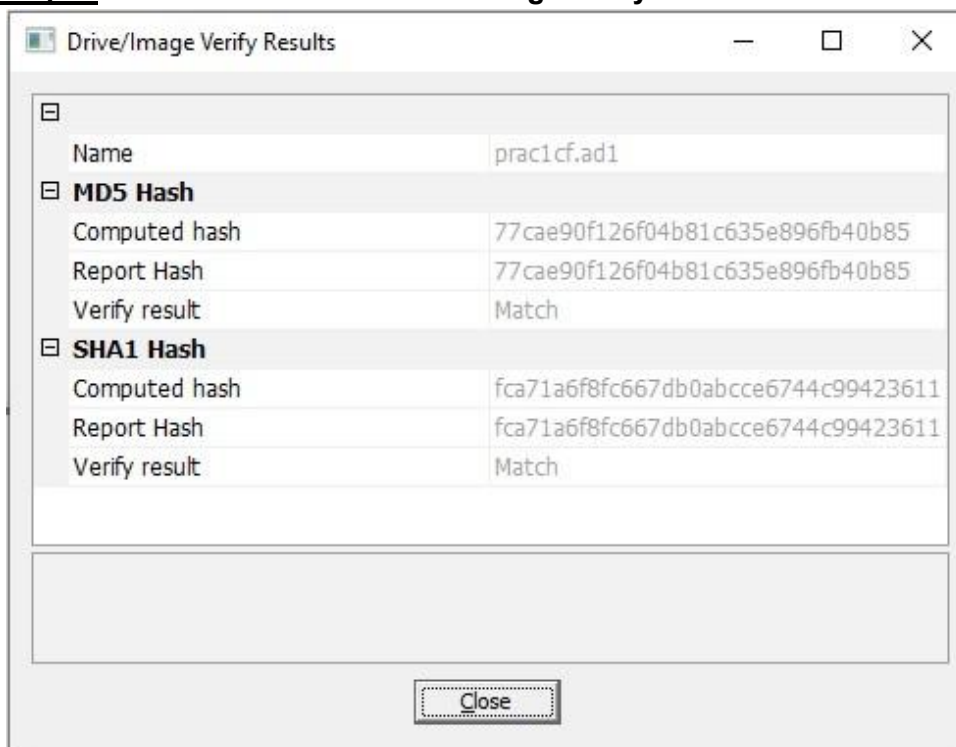
The "Create Image" dialog box contains the following fields and controls:

- Image Source:** A text box containing "D:\TYCS EH 23-24".
- Starting Evidence Number:** A text box containing "1".
- Image Destination(s):** A list box containing "D:\siddy\prac1cf [Logical image]".
- Buttons:** "Add...", "Edit...", "Remove", and "Add Overflow Location" are located below the list box.
- Checkboxes:**
 - ☒ Verify images after they are created
 - ☒ Precalculate Progress Statistics
 - ☐ Create directory listings of all files in the image after they are created
- Buttons:** "Start" and "Cancel" are located at the bottom.

Step 7: Here the Image is being created. Proceed to click on “Image Summary” for the results.

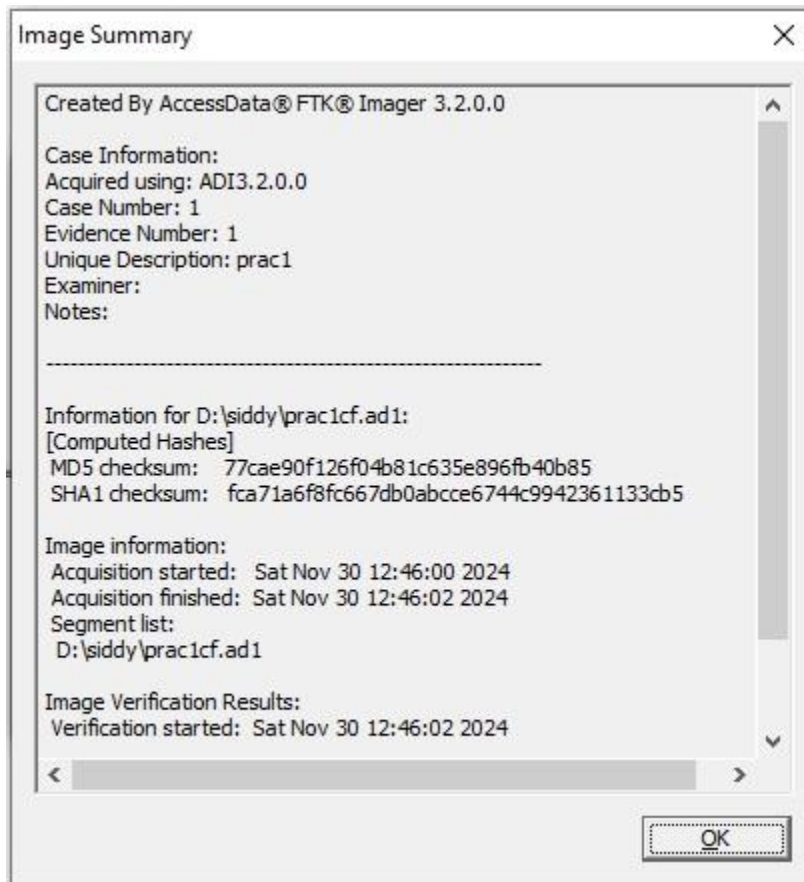


Step 8: Here we can see the Drive/Image Verify Results.



Check Integrity of Data

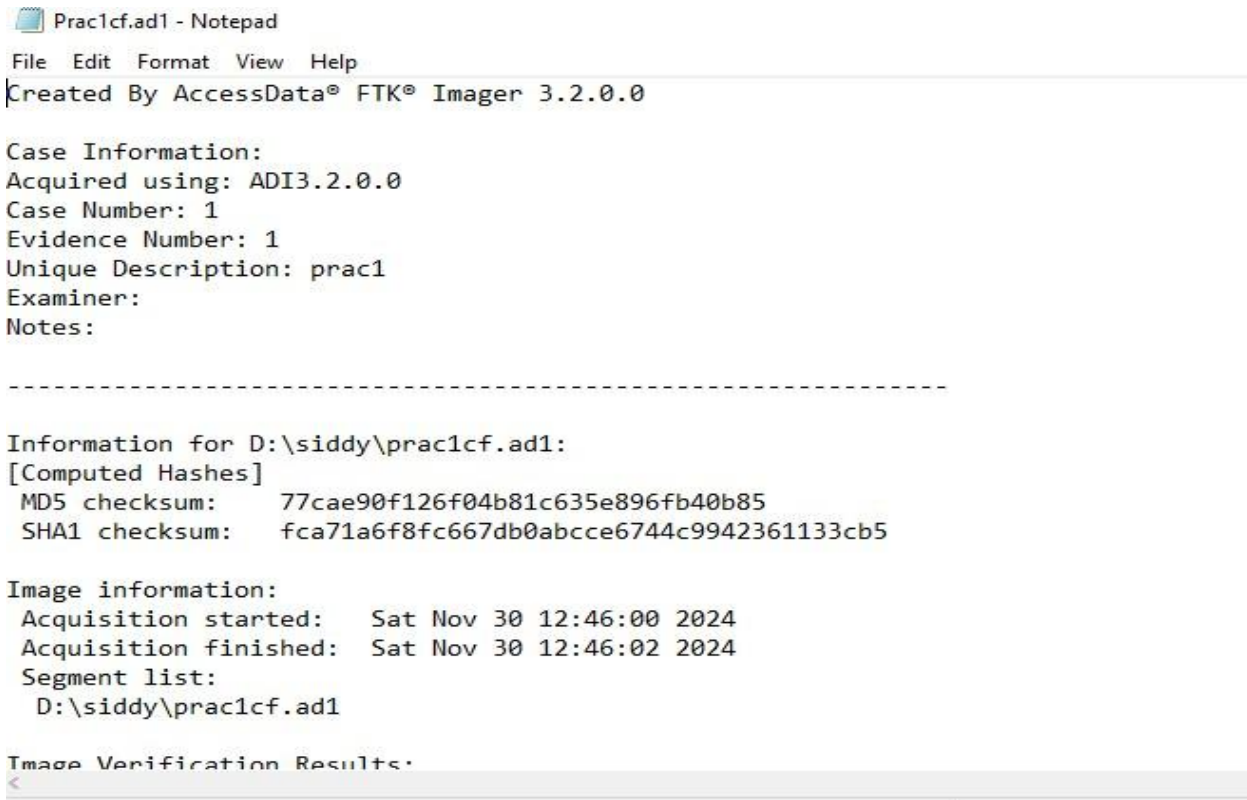
Step 9: Here we can see the whole summary of Image Verification Results.



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

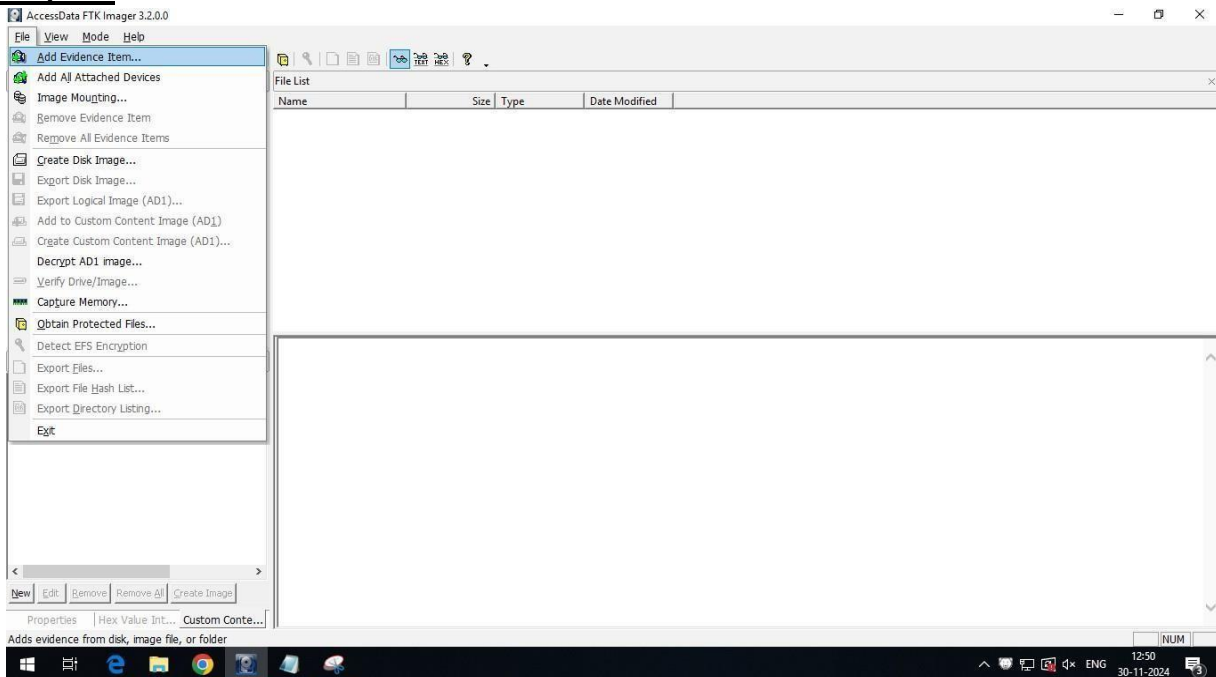
This PC > Local Disk (D:) > siddy				
	Name	Date modified	Type	Size
	prac1.001	30-11-2024 12:05	001 File	9,92,000 KB
	prac1.001	30-11-2024 12:05	Text Document	2 KB
	Prac1cf.ad1	30-11-2024 12:46	AD1 File	40,975 KB
	Prac1cf.ad1	30-11-2024 12:46	Text Document	1 KB

Step 11: Open the file “Prac1cf.ad1” from the folder which is a text document to see the summary of the image.

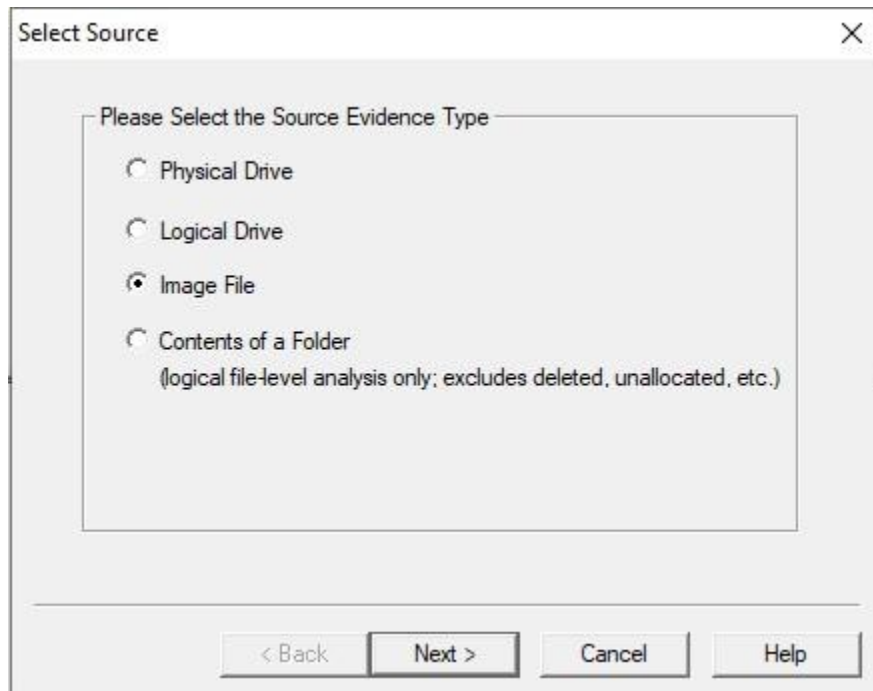


Analyze Forensic Image

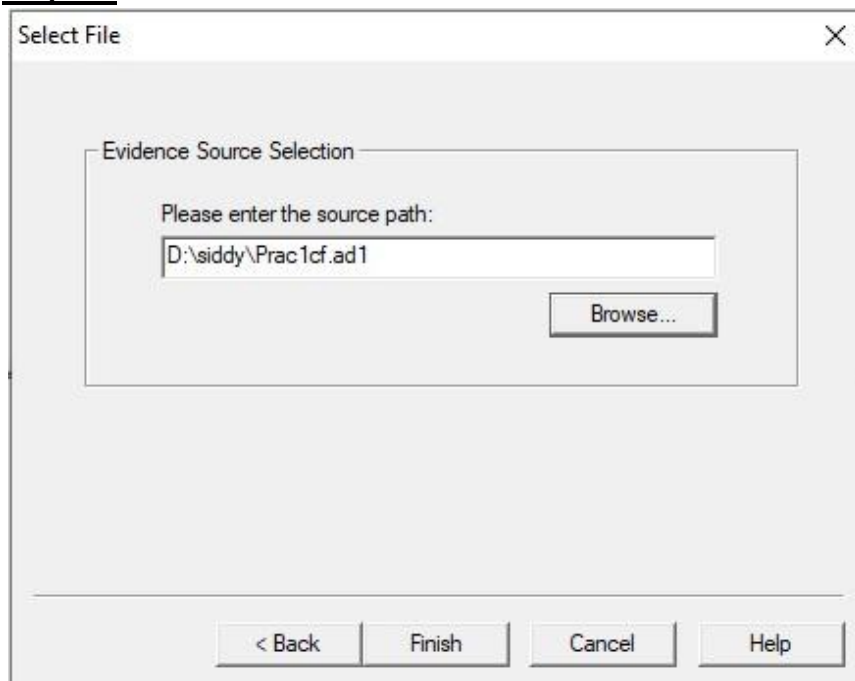
Step 12: Click on File→“Add Evidence Item”.



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



Step 14: Now browse the “Prac1cf.ad1” from the folder that we created. Click on “Finish”.



Step 15: Here we can see the “Evidence Tree” to check the Analyzed result of the forensic Image.

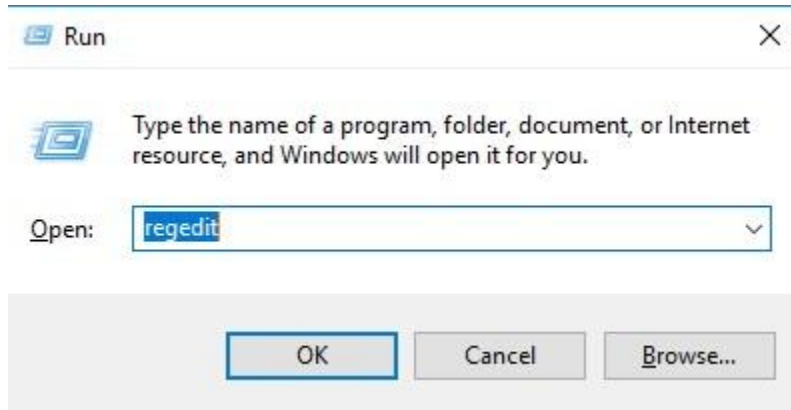
Practical 2

Date: 07-12-24

Aim: Data Acquisition:

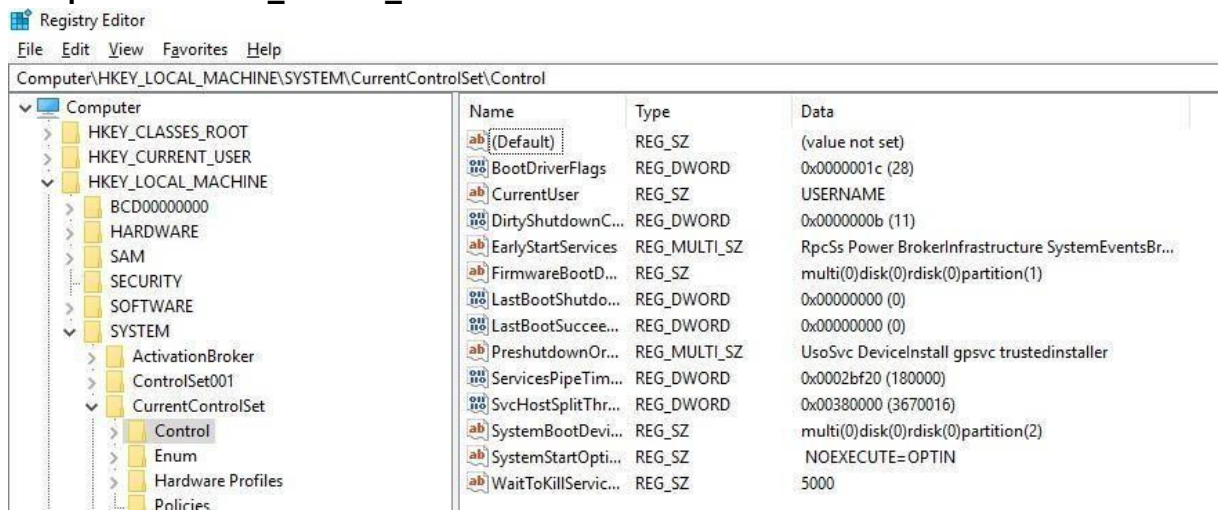
Perform data acquisition using USB Writer Blocker + FTK Imager.

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

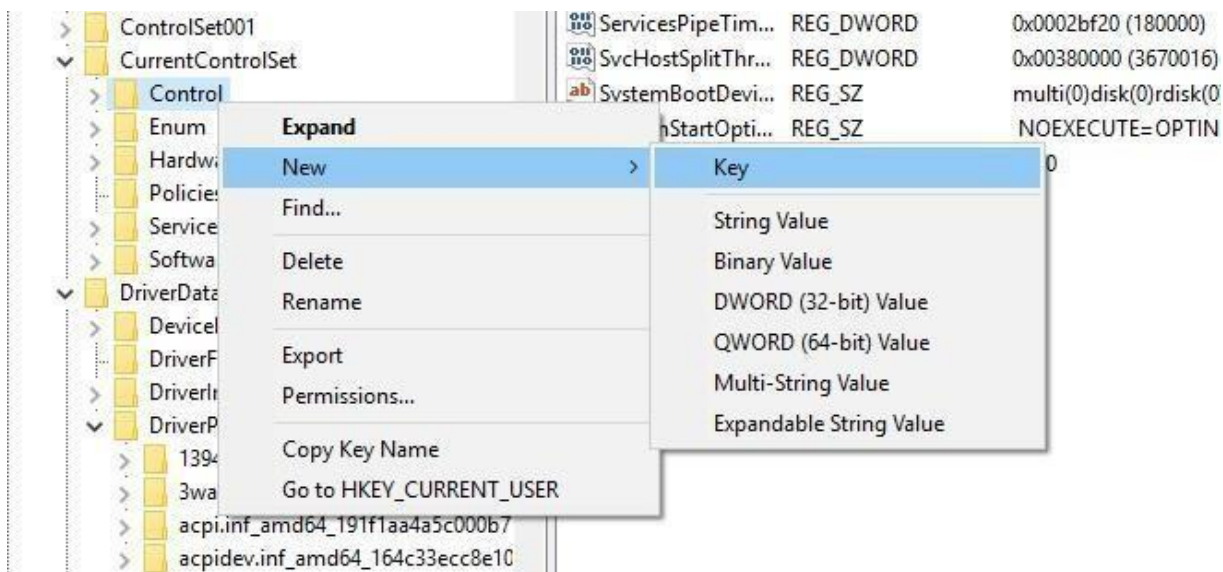


Step 2: A window like this will appear select

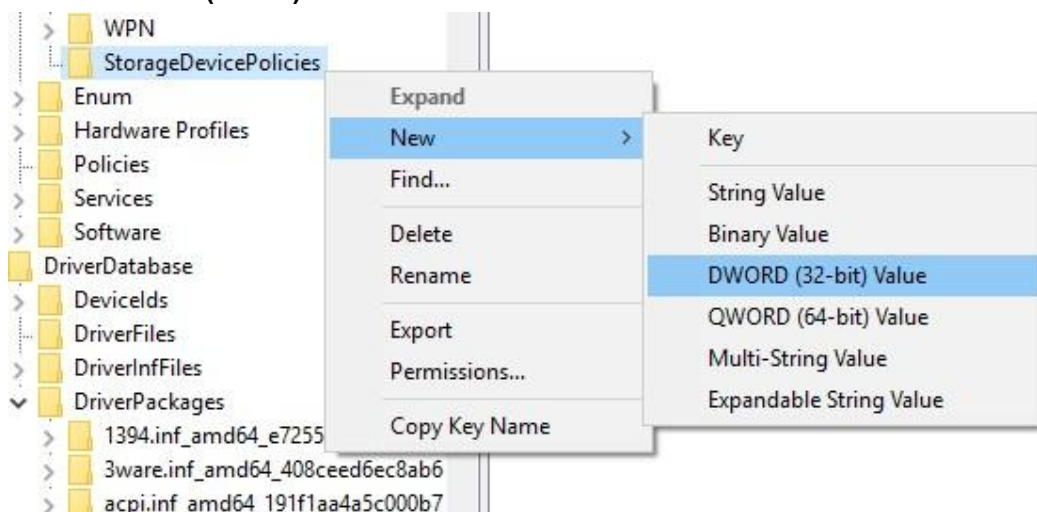
Computer → HKEY_LOCAL_MACHINE → SYSTEM → CurrentControlSet → Control.



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



Step 4: Rename “New Key #1” as “StorageDevicePolicies” then right click on it select New→DWORD(32-bit)Value.



Step 5: Rename the “New Value #1” as “WriteProtect”.

Name	Type	Data
(Default)	REG_SZ	(value not set)
New Value #1	REG_DWORD	0x00000000 (0)

Step 6: Now right click on “WriteProtect” select the option of “Modify”.

Name	Type	Data
(Default)	REG_SZ	(value not set)
WriteProtect	REG_DWORD	0x00000000 (0)

Modify...

Modify Binary Data...

Delete

Rename

Step 7: Change the “Value data” into 1. Click on Ok.

Edit DWORD (32-bit) Value

Value name:

WriteProtect

Value data:

0

Base

☒ Hexadecimal

☐ Decimal

OK
Cancel

Edit DWORD (32-bit) Value

Value name:

WriteProtect

Value data:

1

Base

☒ Hexadecimal

☐ Decimal

OK
Cancel

Step 8: 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*”.

Name	Type	Data
(Default)	REG_SZ	(value not set)
WriteProtect	REG_DWORD	0x00000001 (1)

Step 9: 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.

FTK Image:

Step 10: 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

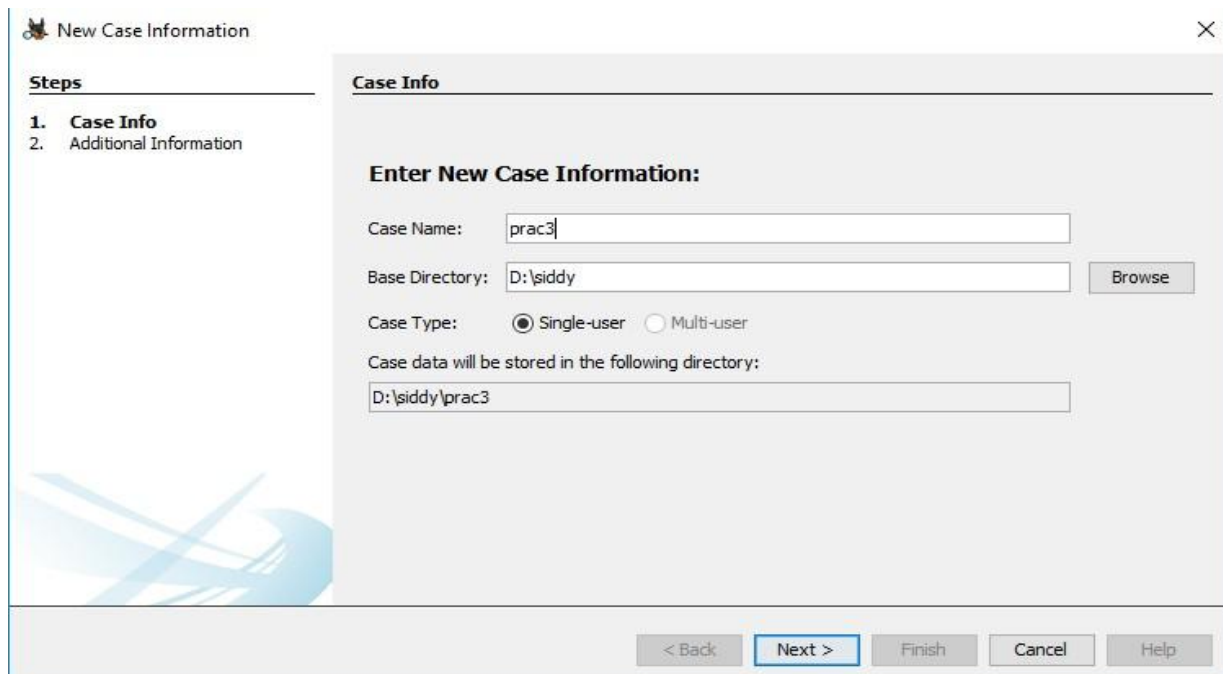
Aim: Forensic Case Study

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.

The image shows the 'New Case Information' dialog box. On the left, there is a 'Steps' list with two items: '1. Case Info' and '2. Additional Information'. The 'Case Info' section is active. It contains the following fields: 'Case Name' with the value 'prac3', 'Base Directory' with the value 'D:\siddy', and 'Case Type' with 'Single-user' selected. Below these fields, it says 'Case data will be stored in the following directory:' followed by the path 'D:\siddy\prac3'. There is a 'Browse' button next to the 'Base Directory' field. At the bottom, there are five buttons: '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'. The 'Next >' button is highlighted.

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

New Case Information

Steps

1. Case Info
2. **Additional Information**

Additional Information

Optional: Set Case Number and Examiner

Case Number:

Examiner:

< Back Next > **Finish** Cancel Help

Step 4: Now Enter the Data Source and browse for the image file “ftkimager.001”.Click on next.

Add Data Source

Steps

1. **Enter Data Source Information**
2. Configure Ingest Modules
3. Add Data Source

Enter Data Source Information wizard (Step 1 of 3)

Select source type to add:

Browse for an image file:

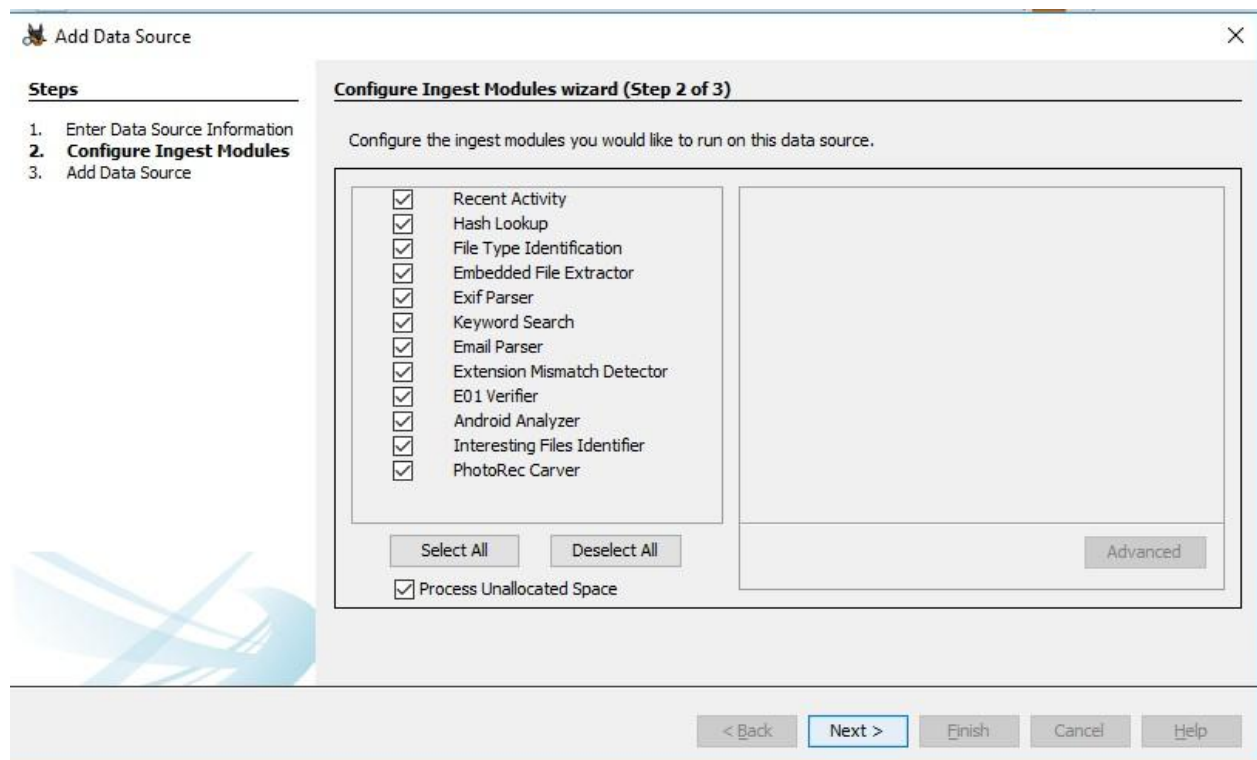
Please select the input timezone:

☐ ignore orphan files in FAT file systems
(faster results, although some data will not be searched)

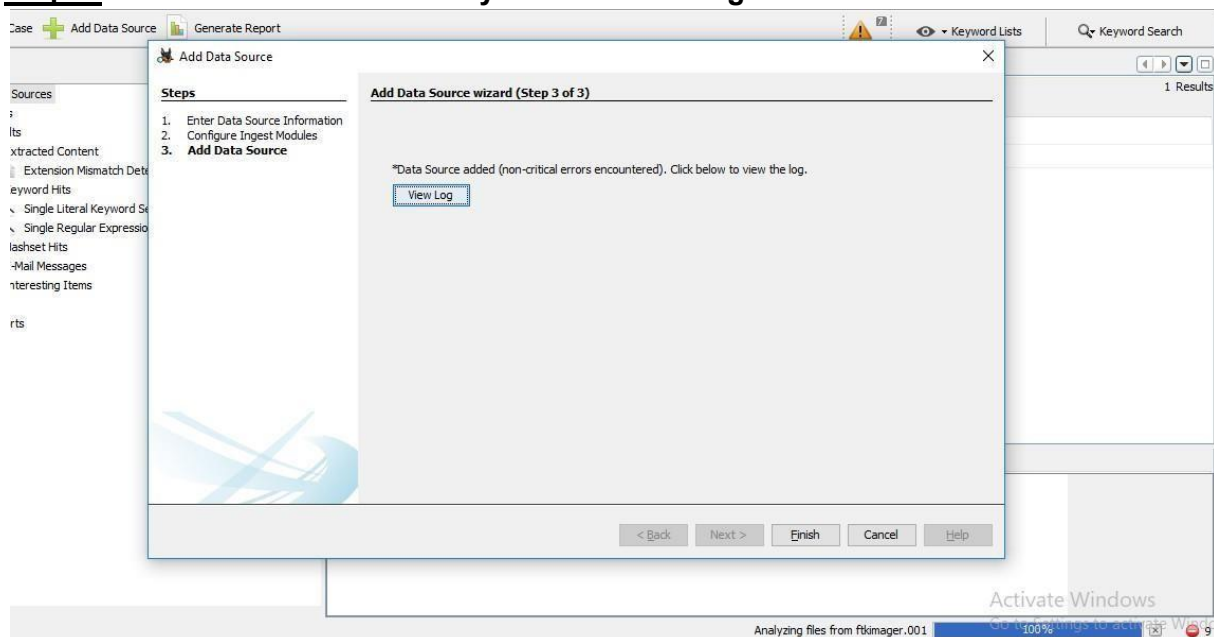
Press 'Next' to analyze the input data, extract volume and file system data, and populate a local database.

< Back Next > Finish Cancel Help

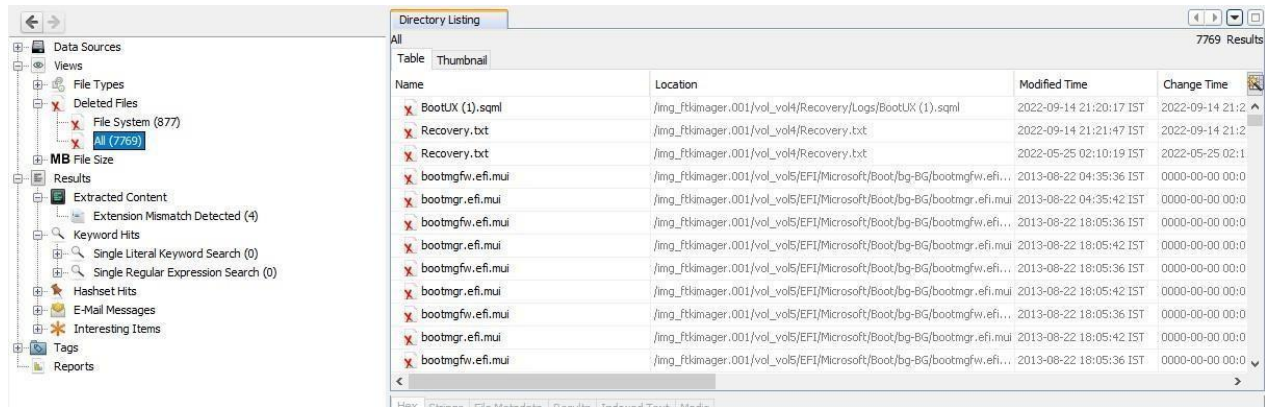
Step 5: Now select all the given checkboxes and click on next.



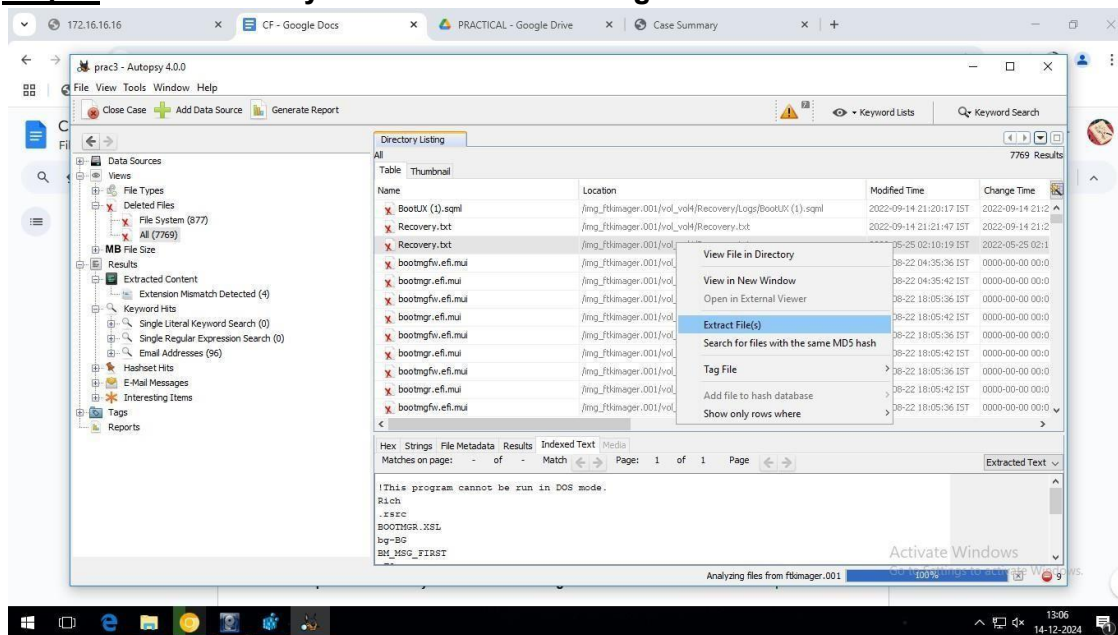
Step 6: Wait until the files are analyzed from “ftkimager.001” and click on Finish.



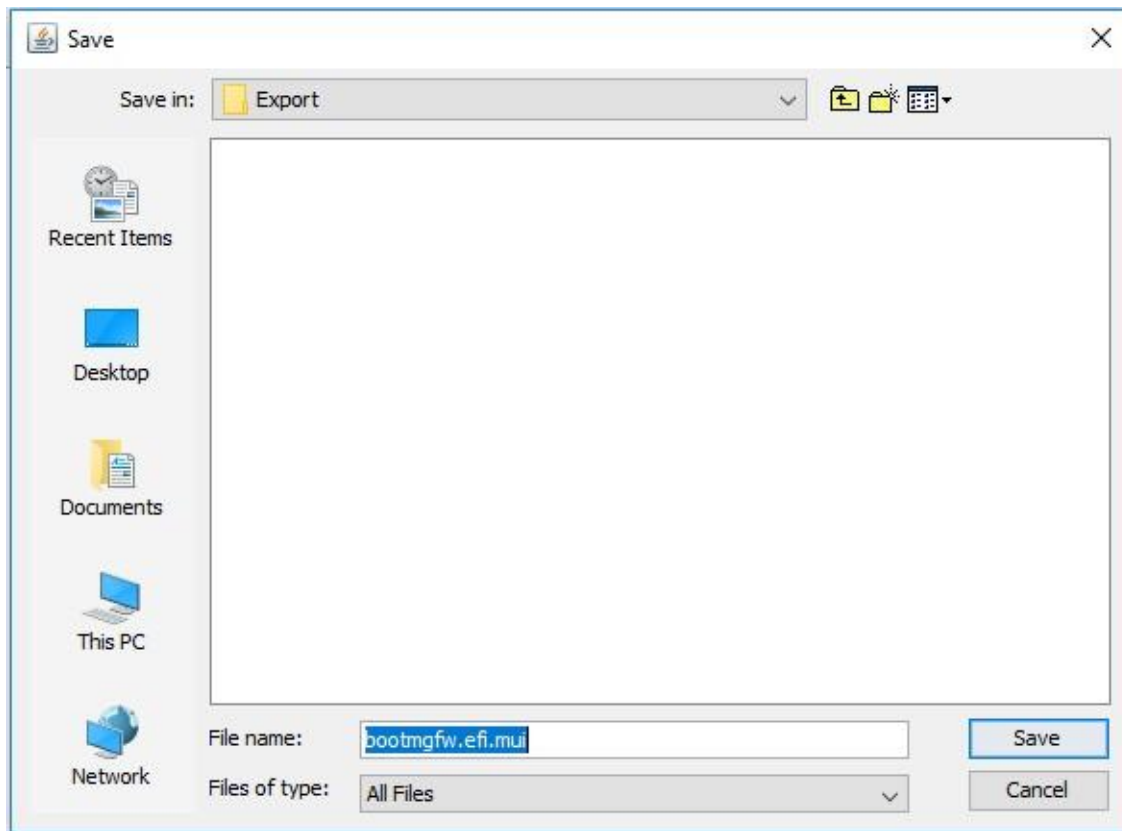
Step 7: Now go to “Views” in the left pane and select Delete Files→All. The deleted files will be listed as shown below.



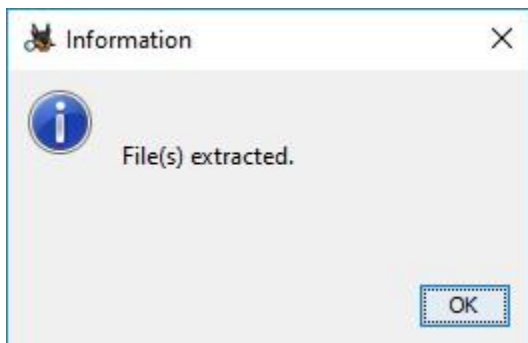
Step 8: Now select any one of the files then right click on it to select “Extract Files”.



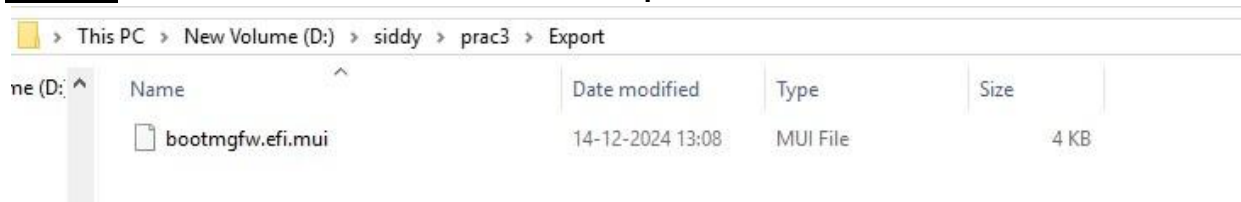
Step 9: Now save the Extracted File in the Export.



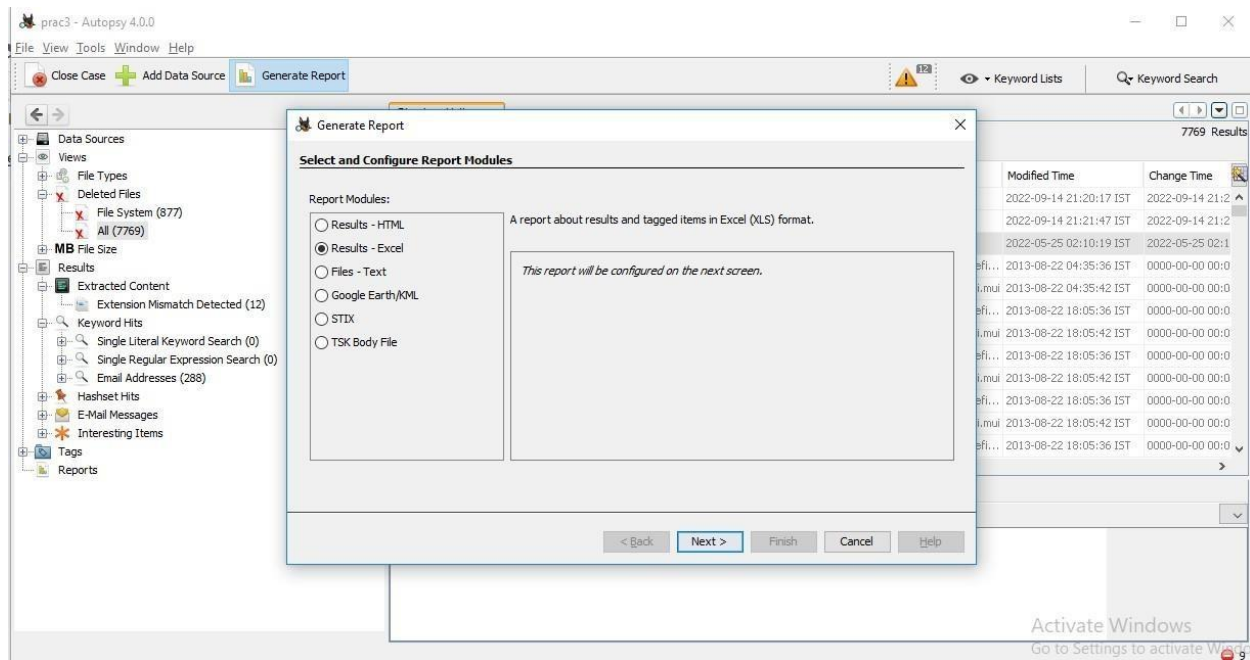
Step 10: The following window will appear which shows us that Files are extracted.



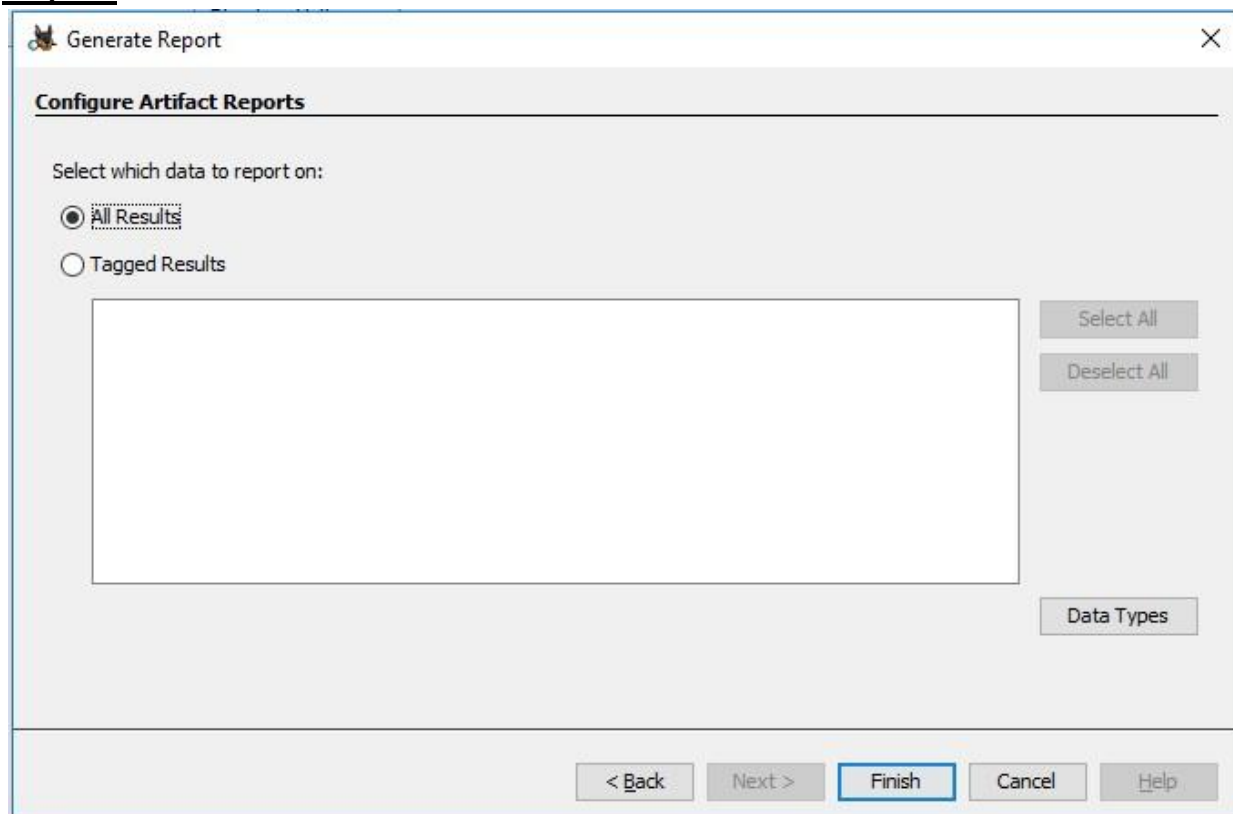
Step 11: We can see the deleted file in the “Export” folder as below.



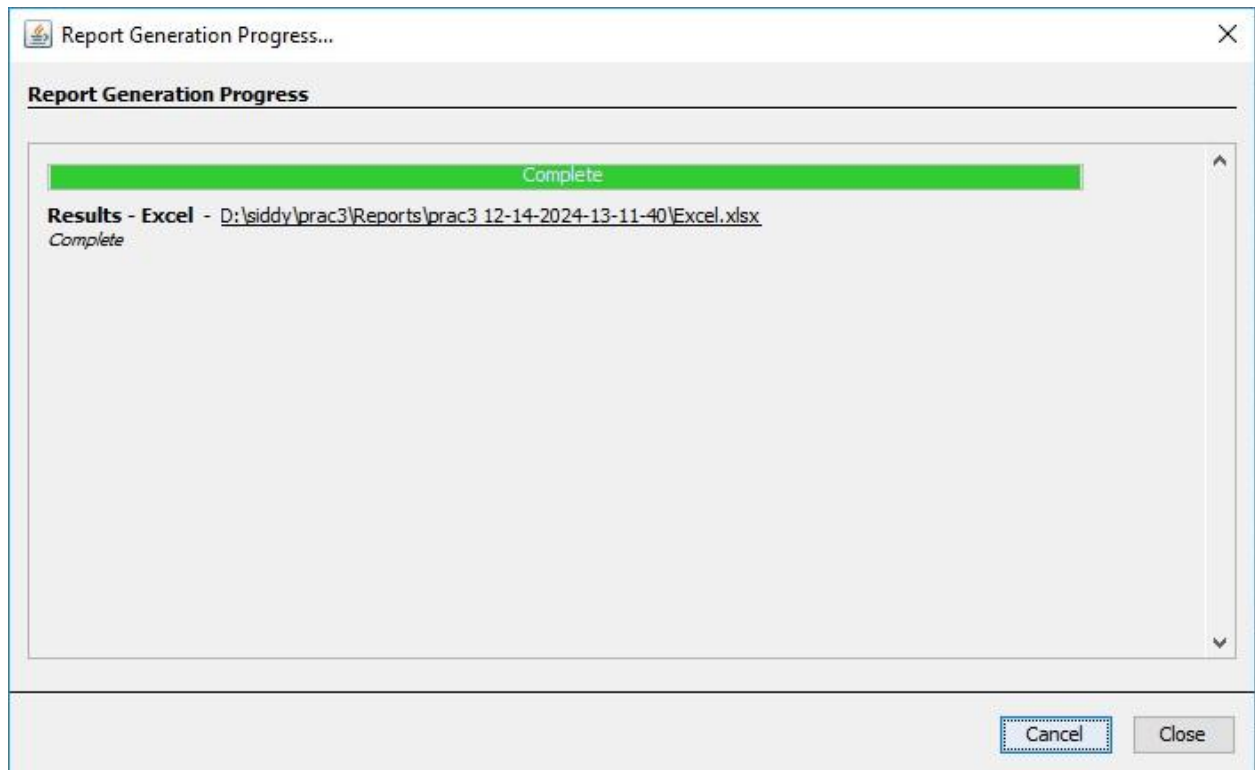
Step 12: Now click on the “Generate Report” seen in the top bar and select the option of Results-Excel.



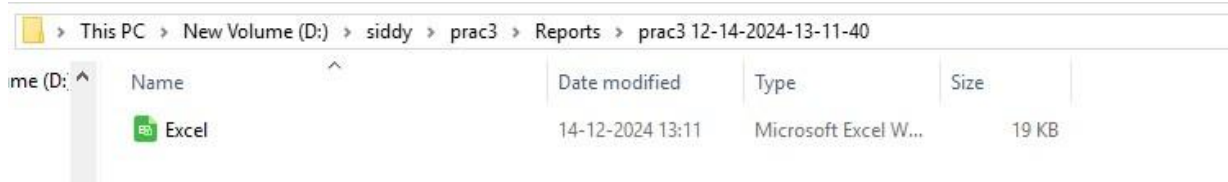
Step 13: Now click on Finish.



Step 14: We can see that the “Report Generation Process” is being completed.



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



Step 16: Open the Excel file and the Summary of the Image file will be shown.

Format Painter					
Clipboard			Font		
A1					Summary
	A	B	C	D	E
1	Summary				
2					
3	Case Name:	prac3			
4	Case Number:	1			
5	Examiner:	1			
6	Number of Images:	1			
7					
8					
9					
10					
11					
12					

Step 17: Similarly select the “Results-HTML” option. Click on Next.

Generate Report

Select and Configure Report Modules

Report Modules:

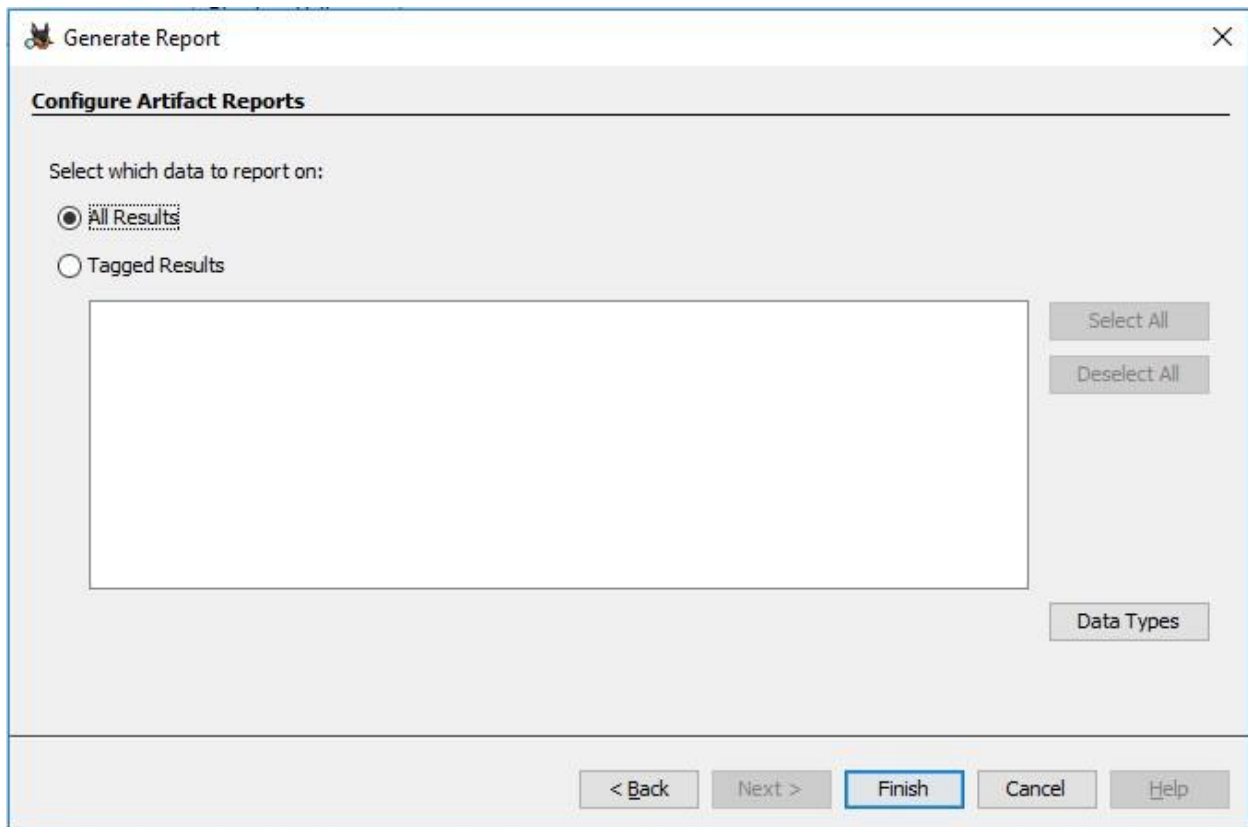
- ☒ Results - HTML
- ☐ Results - Excel
- ☐ Files - Text
- ☐ Google Earth/KML
- ☐ STIX
- ☐ TSK Body File

A report about results and tagged items in HTML format.

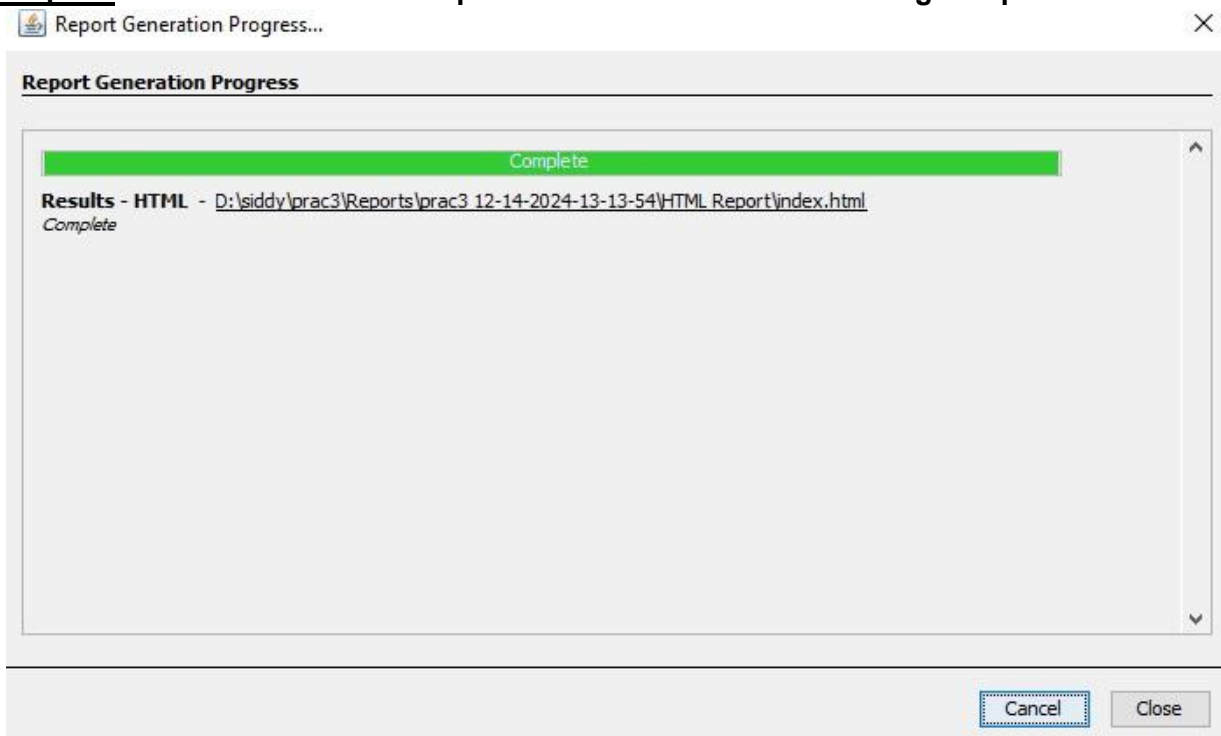
This report will be configured on the next screen.

< Back
Next >
Finish
Cancel
Help

Step 18: 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.

This PC > New Volume (D:) > sidddy > prac3 > Reports > prac3 12-14-2024-13-13-54 > HTML Report					
Name	Date modified	Type	Size		
thumbs	14-12-2024 13:13	File folder			
Extension_Mismatch_Detected	14-12-2024 13:13	HTML File	3 KB		
Extension_Mismatch_Detected	14-12-2024 13:13	PNG File	1 KB		
favicon	14-12-2024 13:13	Icon	362 KB		
generator_logo	14-12-2024 13:13	PNG File	54 KB		
index	14-12-2024 13:13	Cascading Style S...	2 KB		
index	14-12-2024 13:13	HTML File	1 KB		
Keyword_Hits	14-12-2024 13:13	HTML File	61 KB		
Keyword_Hits	14-12-2024 13:13	PNG File	2 KB		
nav	14-12-2024 13:13	HTML File	2 KB		
star	14-12-2024 13:13	PNG File	1 KB		
summary	14-12-2024 13:13	HTML File	2 KB		

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

The screenshot shows a web browser window with the address bar displaying the file path: `file:///D:/sidddy/prac3/Reports/prac3%2012-14-2024-13-13-54/HTML%20Report/summary.html`. The page title is "Autopsy Forensic Report". Below the title, it says "HTML Report Generated on 2024/12/14 13:13:54".

The report content includes the following details:

- Case: prac3
- Case Number: 1
- Examiner: 1
- Number of Images: 1

Under the "Image Information:" section, there is a table with one entry:

ftkimager.001	
Timezone:	Asia/Calcutta
Path:	D:\sidddy\ftkimager.001

Below the table is a cartoon illustration of a Doberman Pinscher. In the bottom right corner, there is a watermark that says "Activate Windows Go to Settings to activate Windows." The Windows taskbar is visible at the bottom of the screen.

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

Practical 4

Date: 19-12-24

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

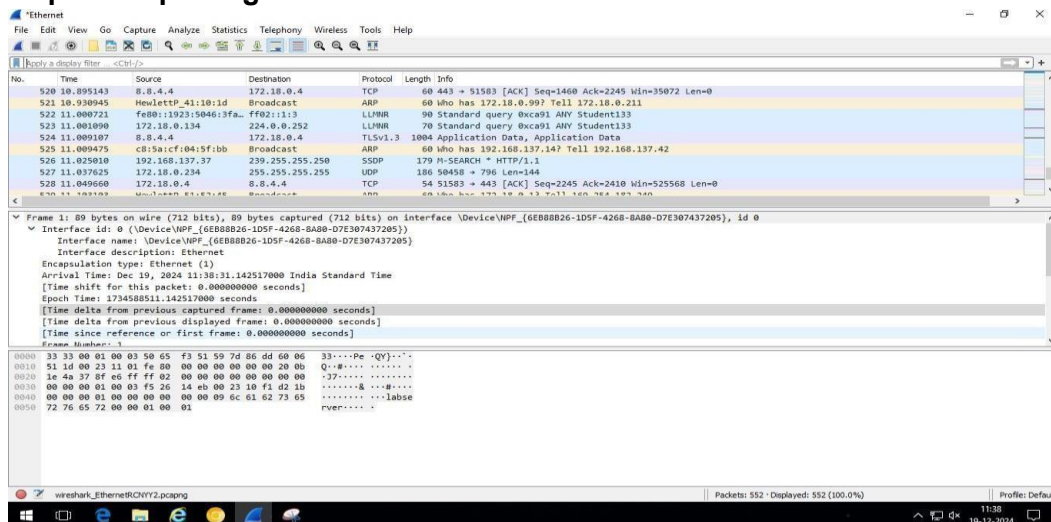
- Identification the live network
- Capture Packets
- Analyze the captured packets

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.

amazon.in Delivering to Dombivali 421202 [Update location](#) All mobile samsung

1-16 of over 5,000 results for "mobile samsung" [Sort by: Featured](#)

Delivery Day

- ☐ Get It Today
- ☐ Get It by Tomorrow
- ☐ Get It in 2 Days

Price

₹45 - ₹86,200+ [Go](#)

Deals & Discounts

All Discounts
Today's Deals

Cellular Phone Memory Storage Capacity

Results

Check each product page for other buying options.

Sponsored

Samsung Galaxy M05 (Mint Green, 4GB RAM, 64 GB Storage) | 50MP Dual Camera | Bigger 6.7" HD+ Display | 5000mAh Battery | 25W Fast Charging | 2 Gen OS Upgrade & 4 Year Security...

★★★★☆ 1,219
5K+ bought in past month

₹6,999 M.R.P: ₹9,999 (30% off)

FREE delivery

[Add to cart](#)

Sponsored

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

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)
696	10.975044	172.18.0.4	172.16.16.16	HTTP	404	GET /images/customimages/unloadedhttpClientLogo.jpg HTTP/1.1

> Frame 625: 501 bytes on wire (4008 bits), 501 bytes captured (4008 bits) on interface \Device\NPF_{6E888B26-1D5F-4268-8A80-D7E307437205}, id 0
> Ethernet II, Src: HewlettP_51:0d:67 (50:65:f3:51:0d:67), Dst: AEWIntec_4a:61:64 (00:0d:48:4a:61:64)
> Internet Protocol Version 4, Src: 172.18.0.4, Dst: 172.16.16.16
> Transmission Control Protocol, Src Port: 50932, Dst Port: 8090, Seq: 1, Ack: 1, Len: 447
> **Hypertext Transfer Protocol**

Step 5: Now click on the get request and see the details.

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)
696	10.975044	172.18.0.4	172.16.16.16	HTTP	404	GET /images/customimages/unloadedhttpClientLogo.jpg HTTP/1.1

Frame Length: 501 bytes (4008 bits)
Capture Length: 501 bytes (4008 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:tcp:http]
[Coloring Rule Name: HTTP]
[Coloring Rule String: http || tcp.port == 80 || http2]
> Ethernet II, Src: HewlettP_51:0d:67 (50:65:f3:51:0d:67), Dst: AEWIntec_4a:61:64 (00:0d:48:4a:61:64)
> Internet Protocol Version 4, Src: 172.18.0.4, Dst: 172.16.16.16
▼ Transmission Control Protocol, Src Port: 50932, Dst Port: 8090, Seq: 1, Ack: 1, Len: 447
Source Port: 50932
Destination Port: 8090

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.

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)
696	10.975044	172.18.0.4	172.16.16.16	HTTP	484	GET /images/favicon.ico HTTP/1.1

```

    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
✓ Transmission Control Protocol, Src Port: 8090, Dst Port: 50934, Seq: 10961, Ack: 368, Len: 1004
  Source Port: 8090

```

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

The screenshot shows the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains icons for opening files, saving, zooming, and other standard functions. The main display area is divided into three panes: the packet list, the packet details, and the packet bytes.

The packet list pane shows a list of captured packets. The selected packet is an ARP request (No. 581) from 10.441.241 to the broadcast address (255.255.255.255). The packet details pane shows the structure of the selected packet, including the Ethernet II header and the ARP section. The packet bytes pane shows the raw data of the packet.

A context menu is open over the packet list, showing various actions that can be performed on the selected packet. The menu options include:

- Mark/Unmark Packet (Ctrl+M)
- Ignore/Unignore Packet (Ctrl+D)
- Set/Unset Time Reference (Ctrl+T)
- Time Shift... (Ctrl+Shift+T)
- Packet Comment... (Ctrl+Alt+C)
- Edit Resolved Name
- Apply as Filter (selected)
- Prepare as Filter
- Conversation Filter
- Colonize Conversation
- SCTP
- Follow
- Copy
- Protocol Preferences
- Decode As...
- Show Packet in New Window

No.	Time	Source	Destination	Protocol	Length	Info
581	10.441241	HewlettP_32:c4:4b	Broadcast	ARP	60	Who has 172.18.0.1? Tell 169.254.22.171
588	10.493843	HewlettP_51:59:c2	Broadcast	ARP	60	Who has 172.18.0.1? Tell 169.254.98.110
595	10.551692	HewlettP_51:4b:4d	Broadcast	ARP	60	Who has 172.18.0.1? Tell 169.254.85.131
596	10.573454	HewlettP_4d:7e:0a	Broadcast	ARP	60	Who has 172.18.0.1? Tell 169.254.55.64
597	10.592771	HewlettP_4d:6e:1a	Broadcast	ARP	60	Who has 172.18.0.234? Tell 172.18.0.65
599	10.654307	HewlettP_51:52:45	Broadcast	ARP	60	Who has 172.18.0.1? Tell 169.254.182.249
610	10.764924	HewlettP_4d:7e:1c	Broadcast	ARP	60	Who has 172.18.0.1? Tell 169.254.100.51
618	10.855096	HewlettP_4d:7d:40	Broadcast	ARP	60	Who has 172.18.0.1? Tell 169.254.29.144
619	10.881197	c8:5a:cf:04:01:f0	Broadcast	ARP	60	Who has 192.168.137.39? Tell 192.168.137.35
621	10.928820	HewlettP_4d:6f:1e	Broadcast	ARP	60	Who has 172.18.0.1? Tell 169.254.43.100

Frame 597: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{6EB88B26-1D5F-4268-8A80-D7E307437205}, id 0

Interface id: 0 (\Device\NPF_{6EB88B26-1D5F-4268-8A80-D7E307437205})

Interface name: \Device\NPF_{6EB88B26-1D5F-4268-8A80-D7E307437205}

Interface description: Ethernet

Encapsulation type: Ethernet (1)

Arrival Time: Dec 19, 2024 10:45:34.385496000 India Standard Time

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1734585334.385496000 seconds

[Time delta from previous captured frame: 0.019317000 seconds]

[Time delta from previous displayed frame: 0.019317000 seconds]

[Time since reference or first frame: 10.592771000 seconds]

Display filter command

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

No.	Time	Source	Destination	Protocol	Length	Info
601	10.721695	64.233.185.94	172.18.0.4	TLSv1.3	1024	Application
603	10.729504	172.18.0.4	8.8.8.8	TCP	55	50913 → 443
604	10.729780	8.8.8.8	172.18.0.4	TCP	66	443 → 50913
608	10.761742	172.18.0.4	64.233.185.94	TCP	54	50928 → 443
616	10.853498	142.250.199.174	172.18.0.4	UDP	371	443 → 51708
617	10.854844	172.18.0.4	142.250.199.174	UDP	77	51708 → 443
622	10.938866	172.18.0.4	172.16.16.16	TCP	66	50932 → 809
623	10.939215	172.16.16.16	172.18.0.4	TCP	66	8090 → 5093
624	10.939291	172.18.0.4	172.16.16.16	TCP	54	50932 → 809
625	10.939548	172.18.0.4	172.16.16.16	HTTP	501	GET /b+...-1

Frame 625: 501 bytes on wire (4008 bits), 501 bytes captured (4008 bits) on interface \Device\NPF_{6EB88B26-1D5F-4268-8A80-D7E307437205}, id 0

Interface id: 0 (\Device\NPF_{6EB88B26-1D5F-4268-8A80-D7E307437205})

Interface name: \Device\NPF_{6EB88B26-1D5F-4268-8A80-D7E307437205}

Interface description: Ethernet

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

No.	Time	Source	Destination	Protocol	Length	Info
128	3.451037	172.16.16.16	172.18.0.4	TCP	66	8090 → 50838 [ACK] Seq=1 Ack=2 Win=237 Len=0 SLE=1 SRE=2
623	10.939215	172.16.16.16	172.18.0.4	TCP	66	8090 → 50932 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
626	10.939954	172.16.16.16	172.18.0.4	TCP	60	8090 → 50932 [ACK] Seq=1 Ack=448 Win=30336 Len=0
627	10.940471	172.16.16.16	172.18.0.4	TCP	1514	8090 → 50932 [ACK] Seq=1 Ack=448 Win=30336 Len=1460 [TCP segment of a reassembled PDU]
628	10.940707	172.16.16.16	172.18.0.4	TCP	1514	8090 → 50932 [ACK] Seq=1461 Ack=448 Win=30336 Len=1460 [TCP segment of a reassembled PDU]
629	10.940707	172.16.16.16	172.18.0.4	TCP	1495	8090 → 50932 [PSH, ACK] Seq=2921 Ack=448 Win=30336 Len=1441 [TCP segment of a reassembled PDU]
630	10.940709	172.16.16.16	172.18.0.4	HTTP	60	HTTP/1.1 200 OK (text/html)
634	10.943882	172.16.16.16	172.18.0.4	TCP	60	8090 → 50932 [ACK] Seq=4363 Ack=449 Win=30336 Len=0
639	10.968213	172.16.16.16	172.18.0.4	TCP	66	8090 → 50933 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128

Frame 623: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{6EB88B26-1D5F-4268-8A80-D7E307437205}, id 0

Interface id: 0 (\Device\NPF_{6EB88B26-1D5F-4268-8A80-D7E307437205})

Interface name: \Device\NPF_{6EB88B26-1D5F-4268-8A80-D7E307437205}

Interface description: Ethernet

Encapsulation type: Ethernet (1)

Arrival Time: Dec 19, 2024 10:45:34.731940000 India Standard Time

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1734585334.731940000 seconds

[Time delta from previous captured frame: 0.000349000 seconds]

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

No.	Time	Source	Destination	Protocol	Length	Info
565	10.162552	142.250.182.234	172.18.0.4	UDP	67	443 → 62995 Len=25
569	10.234875	8.8.8.8	172.18.0.4	TCP	66	443 → 50906 [ACK] Seq=1 Ack=2 Win=320 Len=0 SLE=1 SRE=2
571	10.243029	216.58.203.10	172.18.0.4	TCP	66	443 → 50904 [ACK] Seq=1 Ack=2 Win=297 Len=0 SLE=1 SRE=2
583	10.449391	64.233.185.94	172.18.0.4	TLSv1.3	1514	Server Hello, Change Cipher Spec
584	10.449393	64.233.185.94	172.18.0.4	TLSv1.3	63	Application Data
587	10.451865	64.233.185.94	172.18.0.4	TCP	60	443 → 50928 [ACK] Seq=1470 Ack=2361 Win=35072 Len=0
601	10.721695	64.233.185.94	172.18.0.4	TLSv1.3	1024	Application Data, Application Data
604	10.729700	8.8.8.8	172.18.0.4	TCP	66	443 → 50913 [ACK] Seq=1 Ack=2 Win=365 Len=0 SLE=1 SRE=2
616	10.853498	142.250.199.174	172.18.0.4	UDP	371	443 → 51708 Len=329

Frame 623: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{6EB88B26-1D5F-4268-8A80-D7E307437205}, id 0

Interface id: 0 (\Device\NPF_{6EB88B26-1D5F-4268-8A80-D7E307437205})

Interface name: \Device\NPF_{6EB88B26-1D5F-4268-8A80-D7E307437205}

Interface description: Ethernet

Encapsulation type: Ethernet (1)

Arrival Time: Dec 19, 2024 10:45:34.731940000 India Standard Time

[Time shift for this packet: 0.000000000 seconds]

4. Display packets which are having http as protocol. 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=74777 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 625: 501 bytes on wire (4008 bits), 501 bytes captured (4008 bits) on interface \Device\NPF_{6EB88B26-1D5F-4268-8A80-D7E307437205}, id 0

Interface id: 0 (\Device\NPF_{6EB88B26-1D5F-4268-8A80-D7E307437205})

Interface name: \Device\NPF_{6EB88B26-1D5F-4268-8A80-D7E307437205}

Interface description: Ethernet

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

No.	Time	Source	Destination	Protocol	Length	Info
140	2.933725	172.18.0.10	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
142	3.043662	172.18.0.48	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
147	3.089246	172.18.0.8	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
152	3.174044	172.18.0.101	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
162	3.305149	172.18.0.138	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
191	4.174812	172.18.0.101	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
193	4.306220	172.18.0.138	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
194	4.327943	172.18.0.35	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
195	4.353380	172.18.0.3	146.75.122.172	HTTP	566	GET /filestreamingservice/files/17b75223-a35e-444a-80d4-bb989cccf2f73?P1=1735190485&P2=404&P3=2&P4=DD47VUm
197	4.390250	172.18.0.134	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1

Frame 197: 179 bytes on wire (1432 bits), 179 bytes captured (1432 bits) on interface \Device\NPF_{6EB88B26-1D5F-4268-8A80-D7E307437205}, id 0

Ethernet II, Src: Hewlett-Packard 50:65:f3:4d:7d:57, Dst: IPv4multicast 01:00:5e:7f:ff:fa (01:00:5e:7f:ff:fa)

Internet Protocol Version 4, Src: 172.18.0.134, Dst: 239.255.255.250

User Datagram Protocol, Src Port: 63770, Dst Port: 1900

Simple Service Discovery Protocol

M-SEARCH * HTTP/1.1\r\n

[Expert Info (Chat/Sequence): M-SEARCH * HTTP/1.1\r\n]

Request Method: M-SEARCH

Request URI: *

6. Display packets which are using TCP protocol. tcp

tcp					
Time	Source	Destination	Protocol	Length	Info
603 10.729504	172.18.0.4	8.8.8.8	TCP	55	50913 → 443 [ACK] Seq=1 Ack=1 Win=2049 Len=1 [TCP segment of a reassembled PDU]
604 10.729780	8.8.8.8	172.18.0.4	TCP	66	443 → 50913 [ACK] Seq=1 Ack=2 Win=365 Len=0 SLE=1 SRE=2
608 10.761742	172.18.0.4	64.233.185.94	TCP	54	50928 → 443 [ACK] Seq=2361 Ack=2440 Win=524544 Len=0
622 10.938866	172.18.0.4	172.16.16.16	TCP	66	50932 → 8090 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
623 10.939215	172.16.16.16	172.18.0.4	TCP	66	8090 → 50932 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
624 10.939291	172.18.0.4	172.16.16.16	TCP	54	50932 → 8090 [ACK] Seq=1 Ack=1 Win=525568 Len=0
625 10.939648	172.18.0.4	172.16.16.16	HTTP	501	GET /httpclient.html HTTP/1.1
626 10.939954	172.16.16.16	172.18.0.4	TCP	60	8090 → 50932 [ACK] Seq=1 Ack=448 Win=30336 Len=0
627 10.940471	172.16.16.16	172.18.0.4	TCP	1514	8090 → 50932 [ACK] Seq=1 Ack=448 Win=30336 Len=1460 [TCP segment of a reassembled PDU]
628 10.940737	172.16.16.16	172.18.0.4	TCP	1514	8090 → 50932 [ACK] Seq=1 Ack=448 Win=30336 Len=1460 [TCP segment of a reassembled PDU]

< Frame 625: 501 bytes on wire (4008 bits), 501 bytes captured (4008 bits) on interface \Device\NPF_{6EB88B26-1D5F-4268-8A80-D7E307437205}, id 0

Interface id: 0 (\Device\NPF_{6EB88B26-1D5F-4268-8A80-D7E307437205})

Interface name: \Device\NPF_{6EB88B26-1D5F-4268-8A80-D7E307437205}

Interface description: Ethernet

Encapsulation type: Ethernet (1)

Arrival Time: Dec 19, 2024 10:45:34.732370000 India Standard Time

[Time shift for this packet: 0.000000000 seconds]

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

http.response.code==200						
No.	Time	Source	Destination	Protocol	Length	Info
630	10.940709	172.16.16.16	172.18.0.4	HTTP	60	HTTP/1.1 200 OK (text/html)
649	10.969358	172.16.16.16	172.18.0.4	HTTP	159	HTTP/1.1 200 OK (application/x-javascript)
689	10.974668	172.16.16.16	172.18.0.4	HTTP	1058	HTTP/1.1 200 OK (text/css)
694	10.974924	172.16.16.16	172.18.0.4	HTTP	716	HTTP/1.1 200 OK (application/x-javascript)
703	10.975569	172.16.16.16	172.18.0.4	HTTP	60	HTTP/1.1 200 OK (application/x-javascript)
709	10.975966	172.16.16.16	172.18.0.4	HTTP	60	HTTP/1.1 200 OK (JPEG JFIF image)
943	14.223722	172.16.16.16	172.18.0.4	HTTP/X...	60	HTTP/1.1 200 OK
957	14.275121	172.16.16.16	172.18.0.4	HTTP	60	HTTP/1.1 200 OK (text/html)
981	14.303407	172.16.16.16	172.18.0.4	HTTP	1058	HTTP/1.1 200 OK (text/css)
991	14.303733	172.16.16.16	172.18.0.4	HTTP	150	HTTP/1.1 200 OK (application/x-javascript)

Frame 630: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{6EB88B26-1D5F-4268-8A80-D7E307437205}, id 0
 Interface id: 0 (\Device\NPF_{6EB88B26-1D5F-4268-8A80-D7E307437205})
 Interface name: \Device\NPF_{6EB88B26-1D5F-4268-8A80-D7E307437205}
 Interface description: Ethernet
 Encapsulation type: Ethernet (1)
 Arrival Time: Dec 19, 2024 10:45:34.733434000 India Standard Time
 [Time shift for this packet: 0.000000000 seconds]
 Epoch Time: 1734585334.733434000 seconds

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

tcp.port == 80 udp.port == 80						
No.	Time	Source	Destination	Protocol	Length	Info
490	9.321904	172.18.0.4	172.16.16.16	TCP	66	50929 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
491	9.324182	172.18.0.4	172.16.16.16	TCP	66	50930 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
525	9.572484	172.18.0.4	172.16.16.16	TCP	66	50931 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
796	12.325539	172.18.0.4	172.16.16.16	TCP	66	[TCP Retransmission] 50929 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
797	12.325561	172.18.0.4	172.16.16.16	TCP	66	[TCP Retransmission] 50930 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
840	12.573529	172.18.0.4	172.16.16.16	TCP	66	[TCP Retransmission] 50931 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
1346	18.335339	172.18.0.4	172.16.16.16	TCP	66	[TCP Retransmission] 50929 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
1347	18.335380	172.18.0.4	172.16.16.16	TCP	66	[TCP Retransmission] 50930 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
1375	18.573654	172.18.0.4	172.16.16.16	TCP	66	[TCP Retransmission] 50931 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1

Frame 525: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{6EB88B26-1D5F-4268-8A80-D7E307437205}, id 0
 Interface id: 0 (\Device\NPF_{6EB88B26-1D5F-4268-8A80-D7E307437205})
 Interface name: \Device\NPF_{6EB88B26-1D5F-4268-8A80-D7E307437205}
 Interface description: Ethernet
 Encapsulation type: Ethernet (1)
 Arrival Time: Dec 19, 2024 10:45:33.365209000 India Standard Time
 [Time shift for this packet: 0.000000000 seconds]
 Epoch Time: 1734585333.365209000 seconds
 [Time delta from previous captured frame: 0.005848000 seconds]

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

tcp contains mobile						
No.	Time	Source	Destination	Protocol	Length	Info
673	10.974255	172.16.16.16	172.18.0.4	TCP	1514	8090 → 50935 [ACK] Seq=5993 Ack=367 Win=30336 Len=1460 [TCP segment of a reassembled PDU]
1012	14.306161	172.16.16.16	172.18.0.4	TCP	1514	8090 → 50944 [ACK] Seq=5993 Ack=367 Win=30336 Len=1460 [TCP segment of a reassembled PDU]
8311	69.878638	20.189.173.9	172.18.0.4	TCP	1514	443 → 50975 [ACK] Seq=1441 Ack=192 Win=30336 Len=1460 [TCP segment of a reassembled PDU]
8768	78.529330	20.189.173.9	172.18.0.4	TCP	1514	443 → 50981 [ACK] Seq=1441 Ack=192 Win=30336 Len=1460 [TCP segment of a reassembled PDU]
8779	78.586054	20.189.173.9	172.18.0.4	TCP	1514	443 → 50982 [ACK] Seq=1441 Ack=192 Win=30336 Len=1460 [TCP segment of a reassembled PDU]

Frame 673: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF_{6EB88B26-1D5F-4268-8A80-D7E307437205}, id 0
 Interface id: 0 (\Device\NPF_{6EB88B26-1D5F-4268-8A80-D7E307437205})
 Interface name: \Device\NPF_{6EB88B26-1D5F-4268-8A80-D7E307437205}
 Interface description: Ethernet
 Encapsulation type: Ethernet (1)
 Arrival Time: Dec 19, 2024 10:45:34.766900000 India Standard Time
 [Time shift for this packet: 0.000000000 seconds]

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?

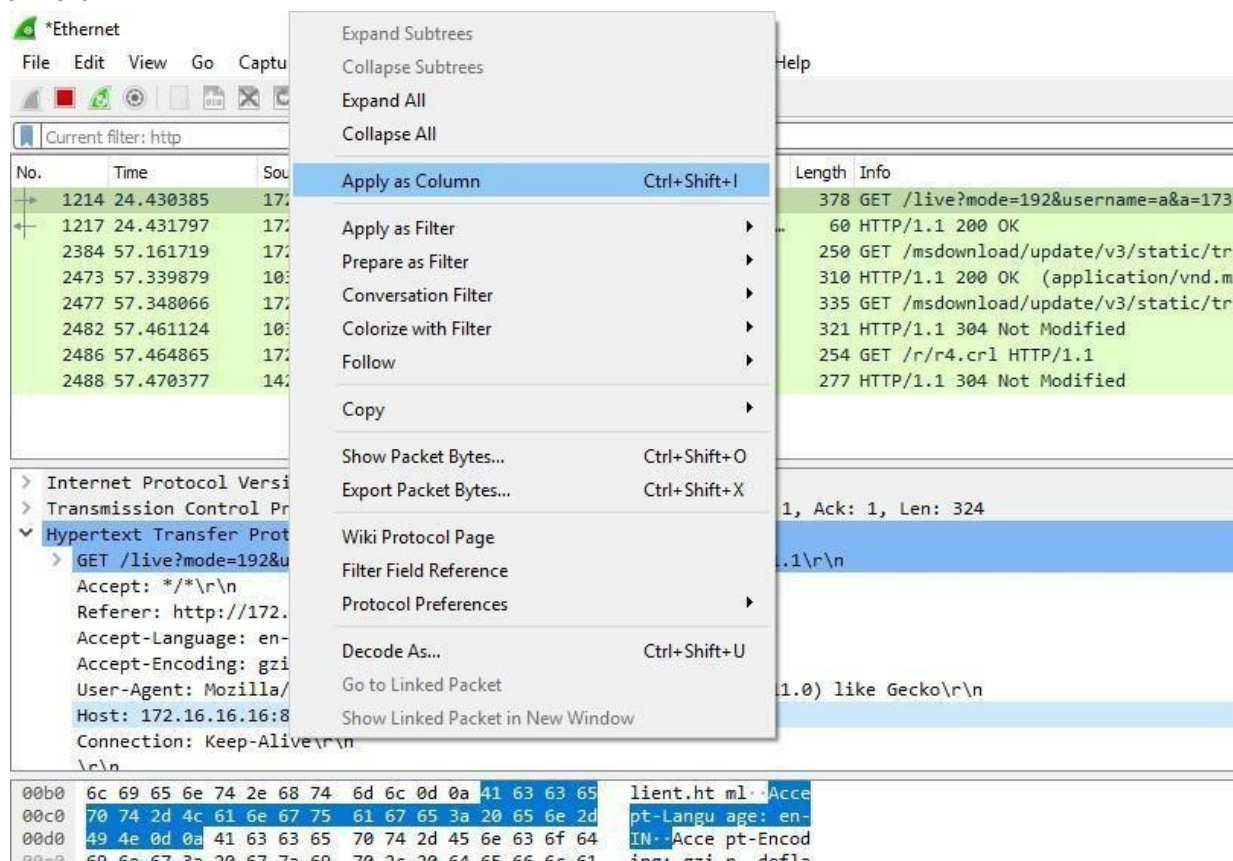
What hosts (IP addresses) think that jokes are more entertaining when they are

Explained?

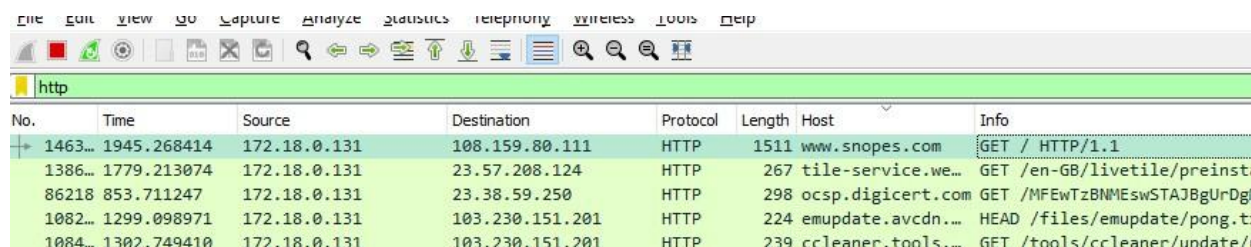
Steps:

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.


```
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: l3paVY_Y7foDgQ8c5mYHrIH1NEoWJ0RM1diw_wwU68CvSiN5WhkT8Q==
```

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

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

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 reassembled
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 reassembled
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 reassembled
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 reassembled
77257	238.600163	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