

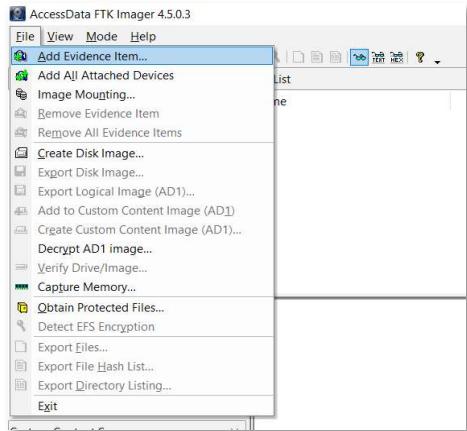
TOPIC
Practical 1 : Creating a Forensic Image using FTK Imager/Encase Image: - Creating Forensic Image (not to be done) - Analyze Forensic Image - Check Integrity of Data
Practical 2: Data Acquisition: Extract Images, Text files from RECYCLER and unallocated space using FTK Imager
Practical 3: Forensics Case Study: - Solve the Case study (image file) using Autopsy
Practical 4: Capturing and analyzing network packets using Wireshark
Practical 5: Using Sysinternals tools for Network Tracking and Process Monitoring
Practical 6: Recovering and inspecting deleted files
Practical 7: Email Forensics
Practical 8: Web Browser Forensics

Practical 1

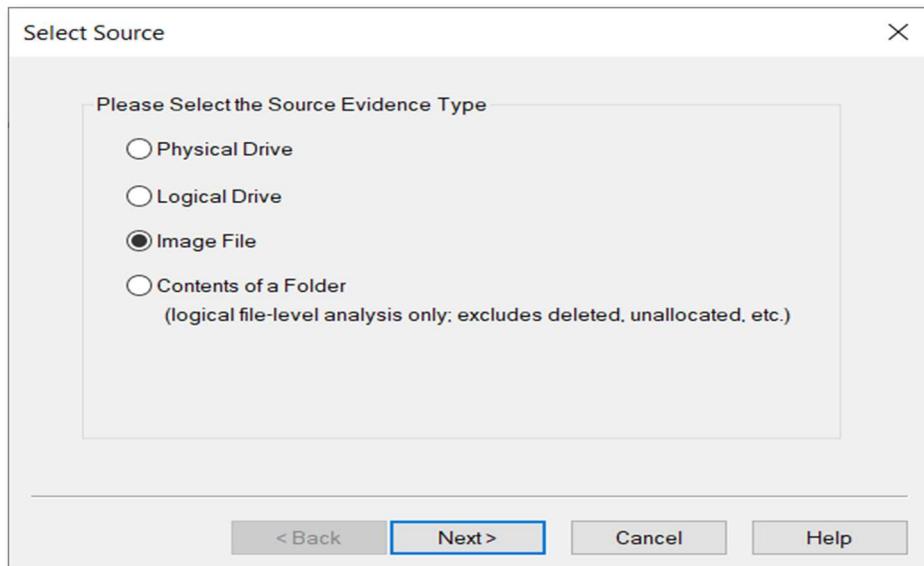
- a) **Creating Forensic Images FTK**
(not to be performed precious.img is provided)

b) Analyze Forensic Image: (to be performed on precious.img)

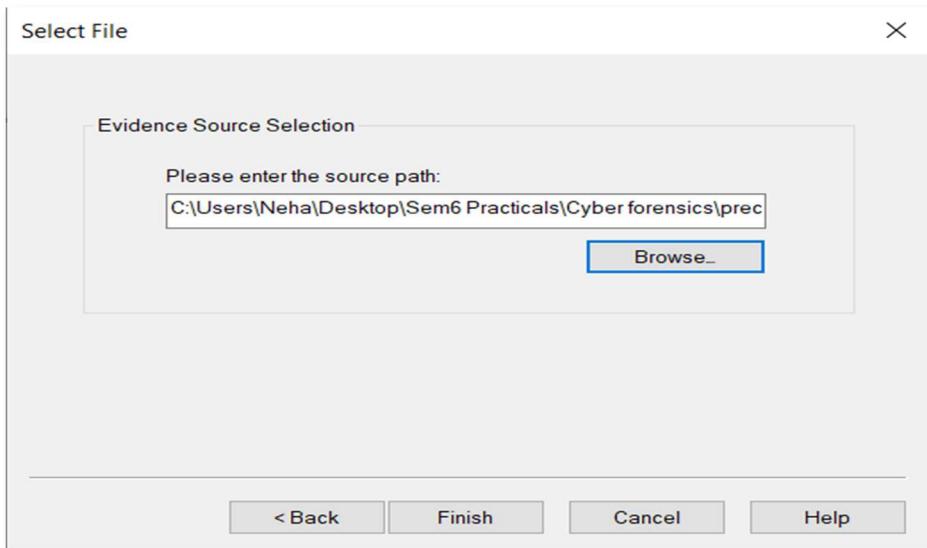
1. Click on Add Evidence Item to add evidence from disk, image file or folder.



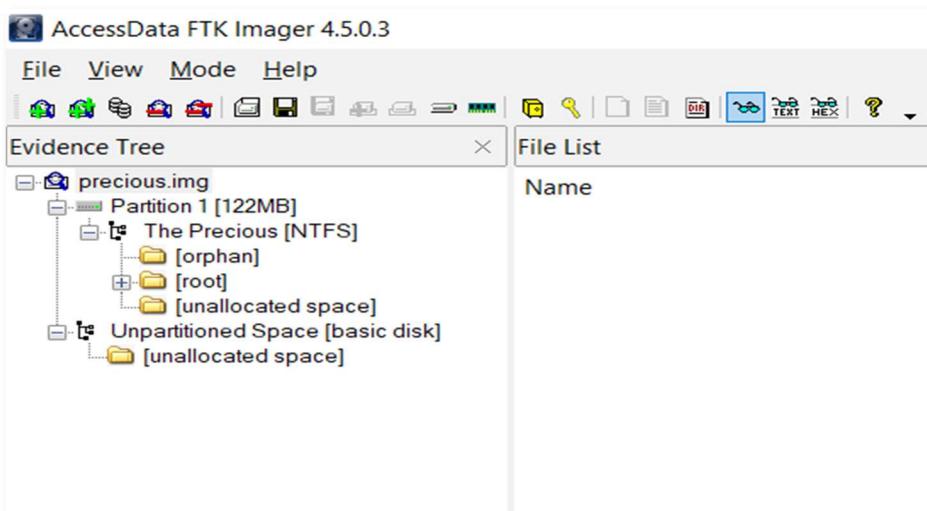
2. Now select the source evidence type as physical drive, logical drive or image file. We have selected image file and click on next.



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



4. Now select Evidence Tree and analyze the virtual disk as physical disk.



5. Here we can analyze disk image by noticing these items:

In the left pane, a tree-structured list of the contents of C drive appears

- **RECYCLER** contains files in the recycle bin

html file from RECYCLER

The screenshot shows the AccessData FTK Imager interface. The left pane displays a tree view of the evidence file 'previous.img' containing 'Partition 1 [122MB]'. Inside 'Partition 1' are several folders like 'The Precious [NTFS]', 'orphans', 'root', 's\$BadClus', 's\$Extend', 's\$Secure', 'Documents and Settings', 'Instruction Materials', 'My Music', 'My Shared Folder', 'Program Files', 'RECYCLER', and 'Windows'. The 'RECYCLER' folder is expanded, showing files like 'Dd1.exe', 'Dd3.htm', 'Dd5.exe', 'Dd6.jpg', 'Dd7.jpg', 'desktop.ini', 'Info2', '\$130', '\$130', and 'Info2'. The right pane shows a 'File List' table with columns for Name, Size, Type, and Date Modified. A large black rectangular area covers the main workspace, containing a survey titled 'Which Lord of the Rings character are you most like? Take this test and see! This test is undergoing a few updates etc. Please be patient.' Below this are three sections of questions with multiple-choice answers:

- What is the weapon of your choice?**
 - A Long Handled Sword
 - A Dirk for hand-to-hand combat
 - A Giant Axe
 - A Bow and Arrow
 - My Bare Hands Are Fine
 - You're Kidding! I'd ruuuuuuun!!
 - I'd Use Magic.
- What do you like to do in your spare time?**
 - Read a good book
 - Go out for a walk
 - Cook
 - Play sports
 - Play chess
- What kind of food do you like?**
 - Anything goes
 - A light meal is best. Something like fruit or a sandwich.
 - Something filling, like steak.
 - Rich food is nice, like chocolate.

At the bottom of the survey area, it says 'When you go to a mall, where's the first place you'd go?' with options: 'Electronics Store'.

Image file from RECYCLER

AccessData FTK Imager 4.5.0.3

Evidence Tree

File List

Name	Size	Type	Date Modified
\$130	4	NTFS Index...	1/1/2005 7:05:31 PM
\$130	4	Regular File	1/3/2005 8:15:02 PM
Dct1.exe	879	Regular File	6/20/2003 12:15:16...
Dct3.htm	14	Regular File	12/29/2004 11:36:5...
Dct5.exe	876	Regular File	6/15/2003 7:21:50...
Dct1.jpg	76	Regular File	12/21/2004 9:10:14...
Dct7.jpg	14	Regular File	1/2/2005 7:38:11 PM
desktop.ini	1	Regular File	12/30/2005 10:01:1...
Info2	6	Regular File	12/30/2004 10:21:5...

Custom Content Sources

Evidence File System Path: /Re

Properties Hex Value In: Custom Con...



PDF file from document & settings folder

AccessData FTK Imager 4.5.0.3

Evidence Tree

File List

Name	Size	Type	Date Modified
DEMO 1.pdf	42	Regular File	5/26/2005 9:56:26 ...
DEMO 2.pdf	54	Regular File	5/26/2005 9:56:31 ...

AccessData Training - Demo Image Request

Page 1 of 1

Home Products Training Resellers Support Company

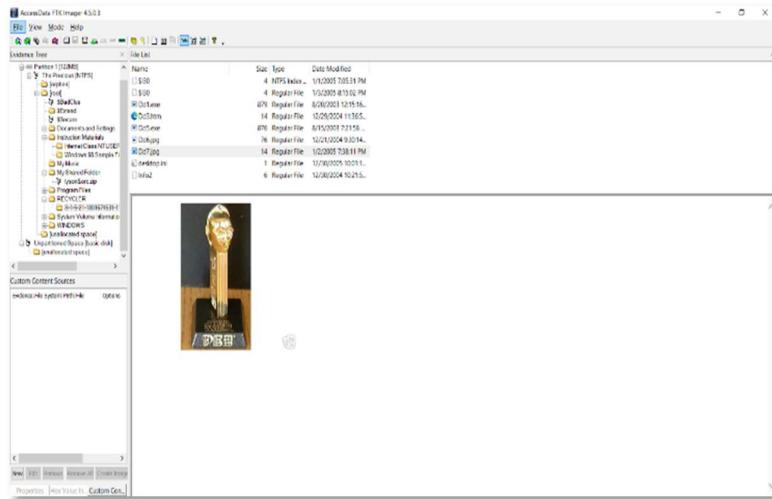
AccessData Training



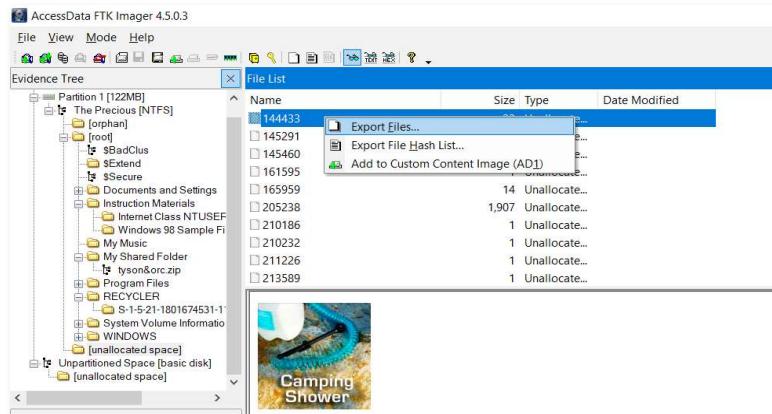
c) Extract Images, Text files from RECYCLER and unallocated space using FTK Imager

1. View Deleted File(s) in the Recycler.

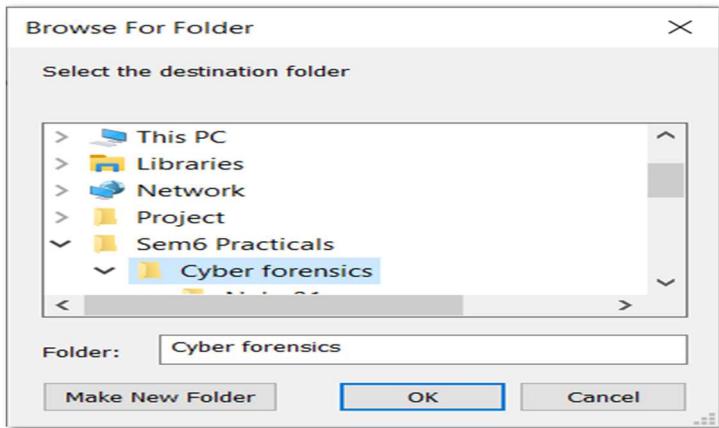
Navigate to RECYCLER --> RECYCLER SUBDIR Click on the jpg file if it exists.



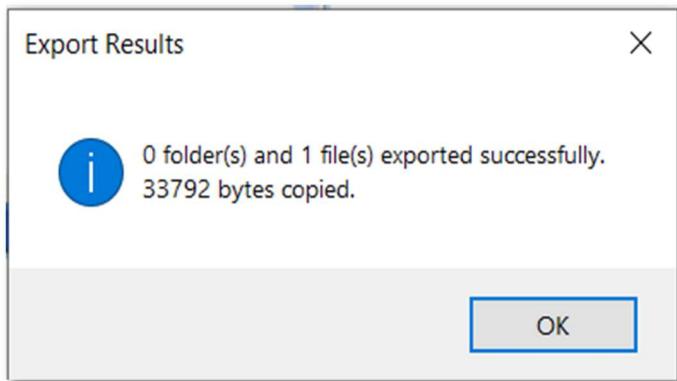
2. Recover deleted image using option Export File. Right Click on the file that contains the picture Select Export Files



3. Select the destination folder. Click the OK Button.



4. Export Results Click the OK Button

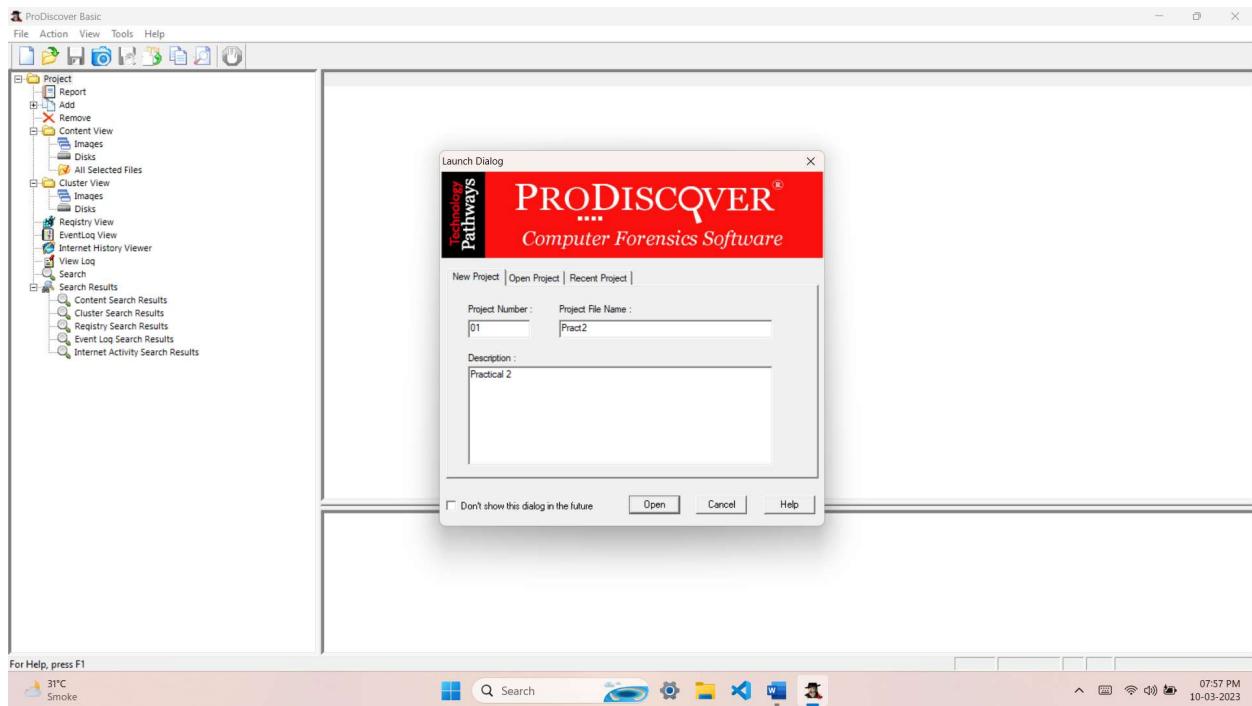


Practical 2

AIM: Perform data acquisition using: ProDiscover

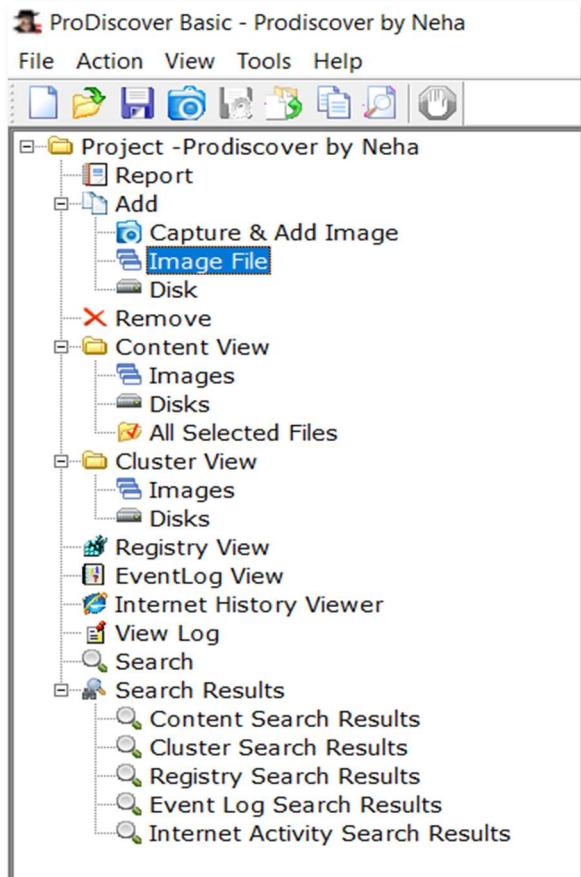
Steps:

1. First Open Prodiscover Basic and start with new case

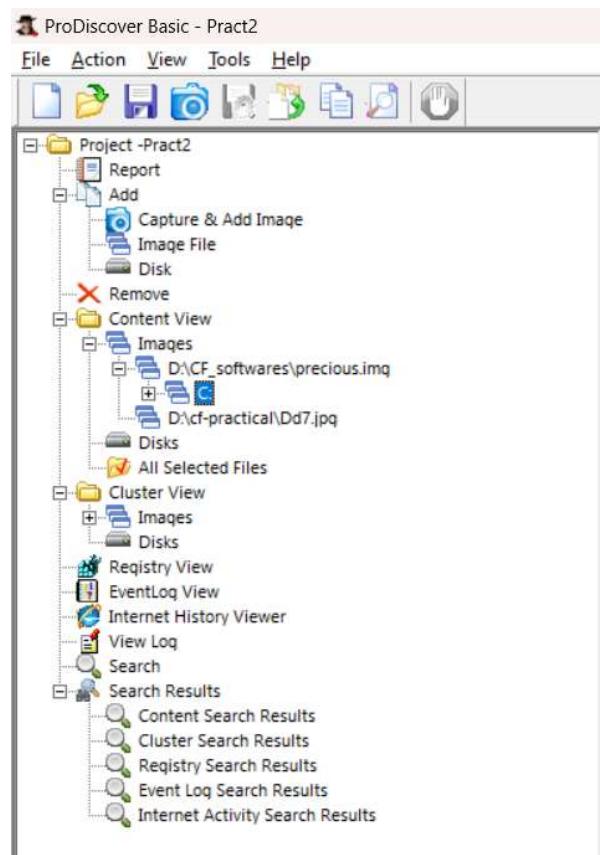


2. created project appears in left pane and select add>image file

Add precious.img file and previously recovered jpg file



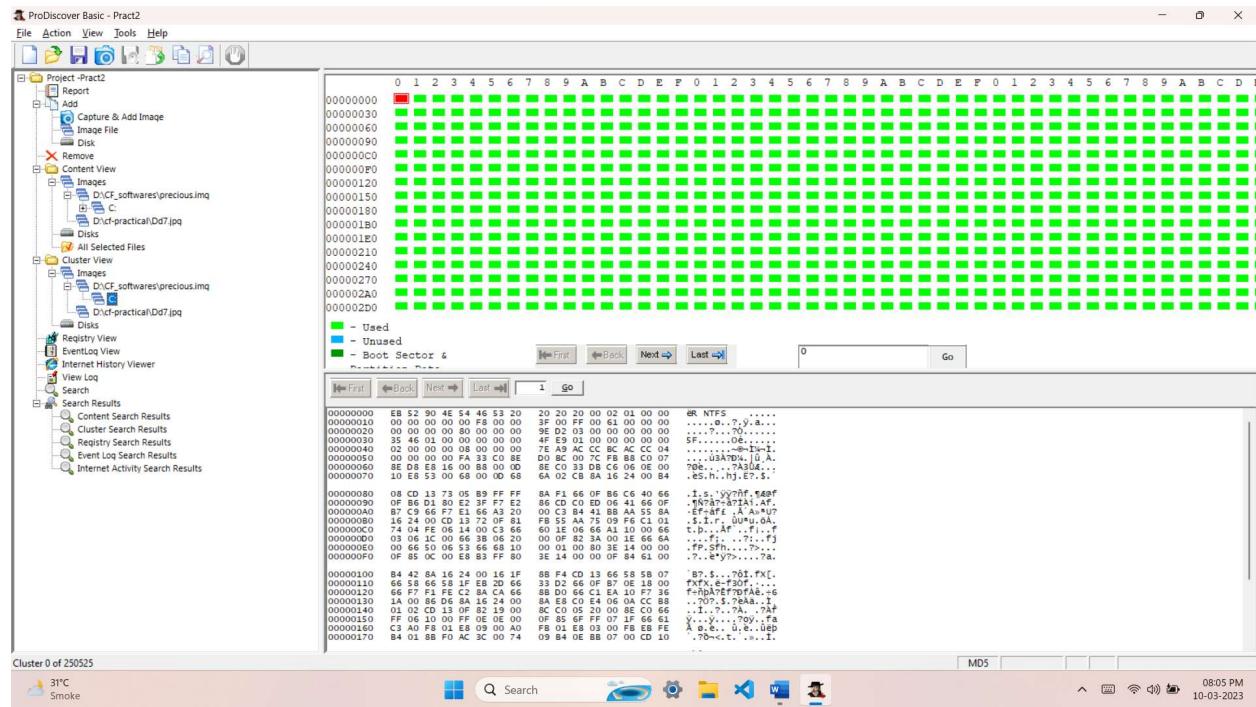
3. Open the image exported, go to Content View > Images in left pane.



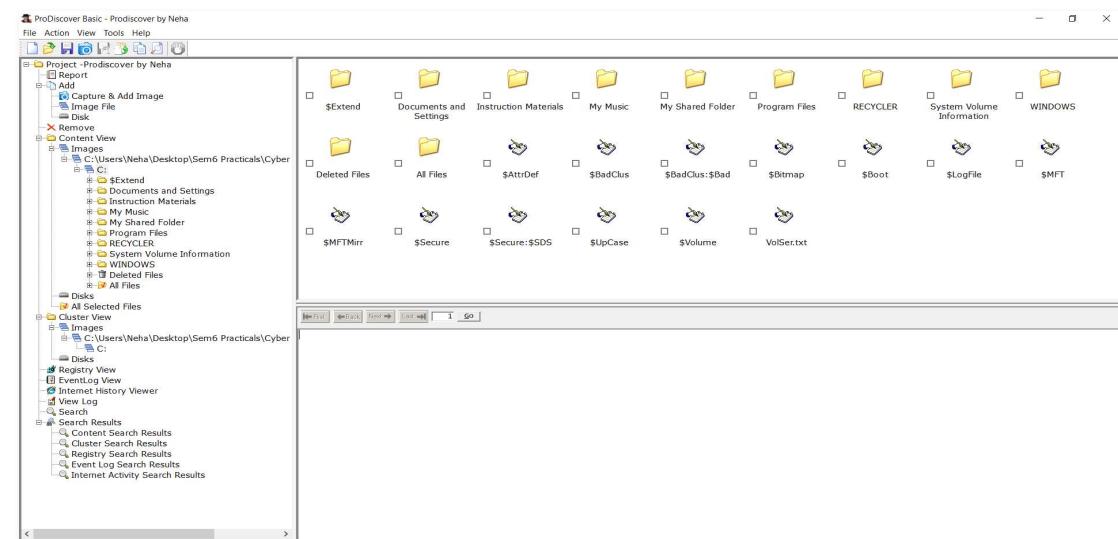
4. Click on any File and type a comment.

Select	File Name	File Extension	Size	Attributes	Deleted	Created Date	Modified Date	Accessed Date	Parent Folder
	\$Extend			--META--	NO	01/02/2005 00:12	01/02/2005 00:12	01/02/2005 00:12	D:\CF_softwares\precious
	Documents and Setti...			--d----	NO	01/02/2005 00:18	01/02/2005 00:20	12/31/2004 10:53	D:\CF_softwares\precious
	Instruction Materials			--d----	NO	01/02/2005 00:20	01/03/2004 02:10	12/31/2004 10:53	D:\CF_softwares\precious
	My Music			--d----	NO	01/02/2005 00:20	01/02/2005 00:20	12/31/2004 10:53	D:\CF_softwares\precious
	My Shared Folder			--d----	NO	01/02/2005 00:20	01/03/2004 01:32	12/31/2004 10:53	D:\CF_softwares\precious
	Program Files			--d----	NO	01/02/2005 00:20	01/02/2005 00:20	12/31/2004 10:53	D:\CF_softwares\precious
	RECYCLER			--d----	NO	01/02/2005 00:20	01/02/2005 00:20	12/31/2004 10:53	D:\CF_softwares\precious
	System Volume Infor...			--d----	NO	01/02/2005 00:18	01/02/2005 00:18	12/31/2004 10:53	D:\CF_softwares\precious
	WINDOWS			--d----	NO	01/02/2005 00:18	01/02/2005 00:18	12/31/2004 10:53	D:\CF_softwares\precious
	Deleted Files			--d----	NO	01/01/1970 05:30	01/01/1970 05:30	01/01/1970 05:30	D:\CF_softwares\precious
	\$AttrDef			--d----	NO	01/02/2005 00:12	01/02/2005 00:12	01/02/2005 00:12	D:\CF_softwares\precious
	\$BadClus			--d----	NO	01/02/2005 00:12	01/02/2005 00:12	01/02/2005 00:12	D:\CF_softwares\precious
	\$BadClus\$Bad			--d----	NO	01/02/2005 00:12	01/02/2005 00:12	01/02/2005 00:12	D:\CF softwares\precious
	\$Bitmap		36,000 bytes	--META--	NO	01/02/2005 00:12	01/02/2005 00:12	01/02/2005 00:12	D:\CF softwares\precious
	\$Boot			--d----	NO	01/02/2005 00:12	01/02/2005 00:12	01/02/2005 00:12	D:\CF softwares\precious
	\$LogFile			--d----	NO	01/02/2005 00:12	01/02/2005 00:12	01/02/2005 00:12	D:\CF softwares\precious
	\$MFT			--d----	NO	01/02/2005 00:12	01/02/2005 00:12	01/02/2005 00:12	D:\CF softwares\precious
	\$MFTMirr			--d----	NO	01/02/2005 00:12	01/02/2005 00:12	01/02/2005 00:12	D:\CF softwares\precious
	\$Secure			--d----	NO	01/01/1970 05:30	01/01/1970 05:30	01/01/1970 05:30	D:\CF softwares\precious

5. in the sidebar click o cluster view is seen from the cluster view in left panel.



6. We can also view gallery view by going view > gallery view.

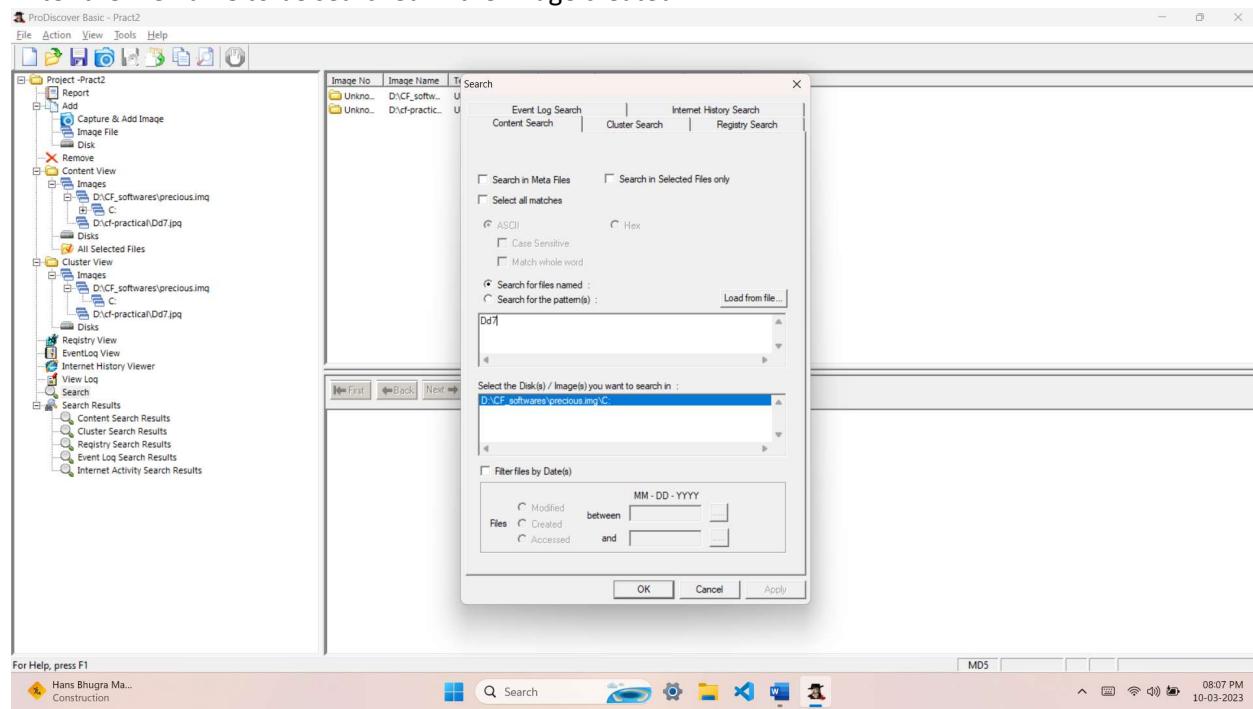


7. Keyword search.

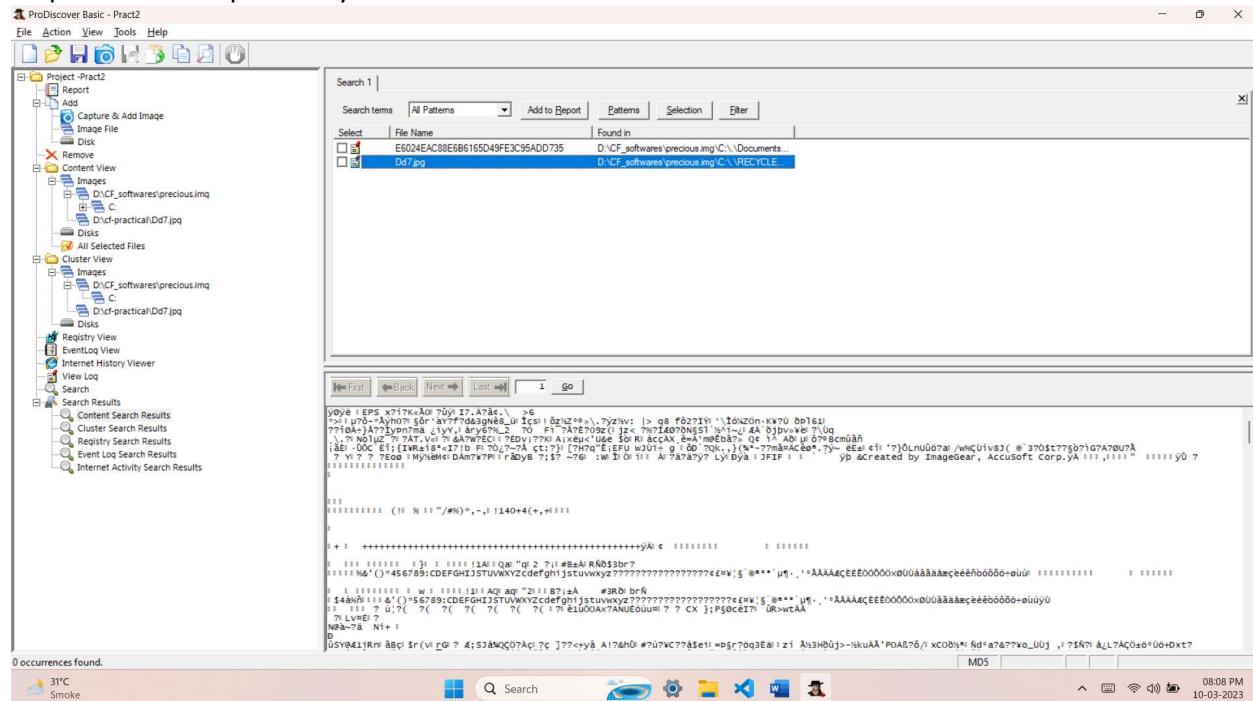
Click on Search in left pane and

Select click on **search for files named**

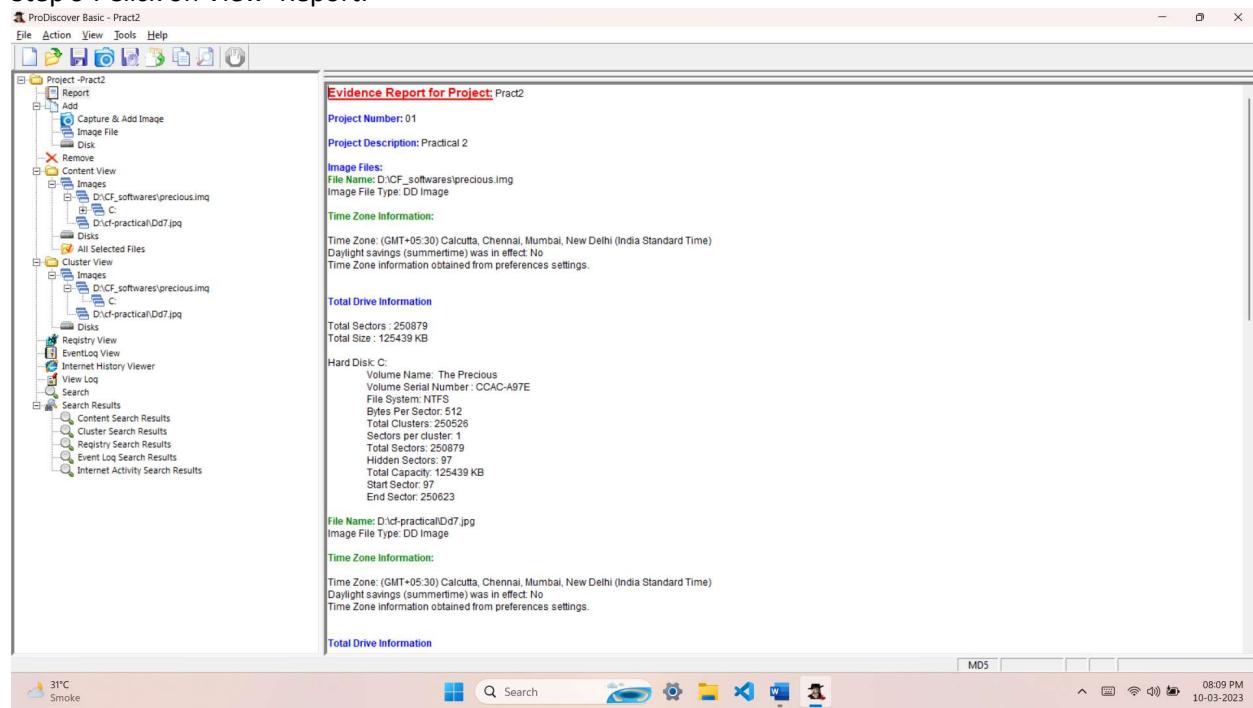
Enter the file name to be searched in the image created.



Step 8: Select Output of Keyword search.



Step 9 : Click on View>Report.



Practical 3

AIM: Forensics Case Study: - Solve the Case study (image file) using Autopsy

1. To create a case, Select new case



2. You will need to supply it with the name of the case and a directory to store the case results into.

The image shows the 'New Case Information' dialog box. On the left, a sidebar titled 'Steps' indicates that step 1, 'Case Information', is selected. Step 2, 'Optional Information', is also listed. The main area is titled 'Case Information'. It contains the following fields:

- 'Case Name:' input field containing 'Neha01'
- 'Base Directory:' input field containing 'C:\Users\Neha\Desktop\Sem6 Practicals\Cyber forensics\' with a 'Browse' button next to it
- 'Case Type:' radio buttons for 'Single-User' (selected) and 'Multi-User'
- A note below the base directory field stating 'Case data will be stored in the following directory:' followed by an input field containing 'C:\Users\Neha\Desktop\Sem6 Practicals\Cyber forensics\Neha01'

At the bottom of the dialog box, there are buttons for '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'.

You can optionally provide case numbers and other details

New Case Information

Steps

- Case Information
- Optional Information**

Optional Information

Case

Number: 01

Examiner

Name: Neha

Phone: 855*****

Email: np@gmail.com

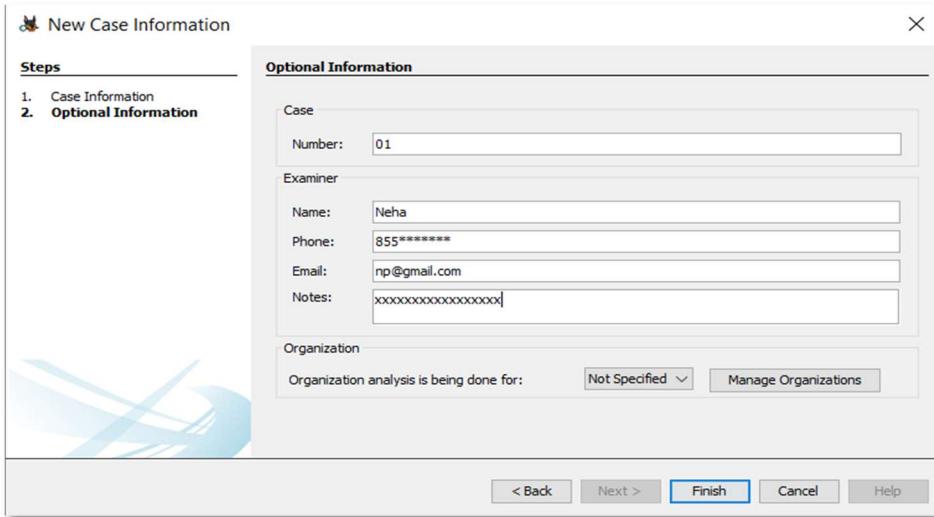
Notes: xxxxxxxxxxxxxxxxx

Organization

Organization analysis is being done for: Not Specified

Manage Organizations

< Back Next > Finish Cancel Help



After adding case information it will automatically redirect to add data source wizard Click on next

Add Data Source

Steps

- Select Host
- Select Data Source Type
- Select Data Source
- Configure Ingest
- Add Data Source

Select Host

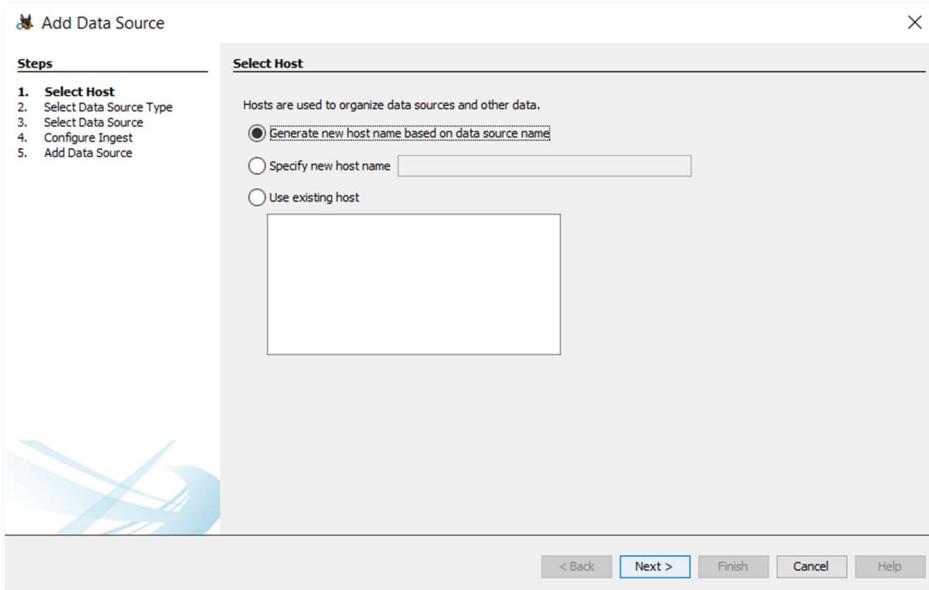
Hosts are used to organize data sources and other data.

Generate new host name based on data source name

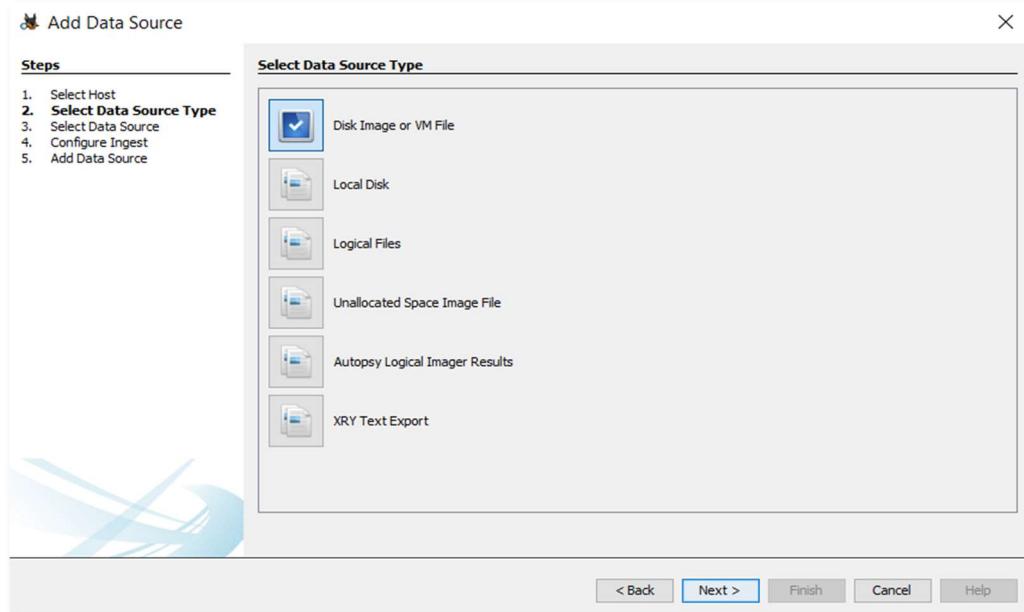
Specify new host name

Use existing host

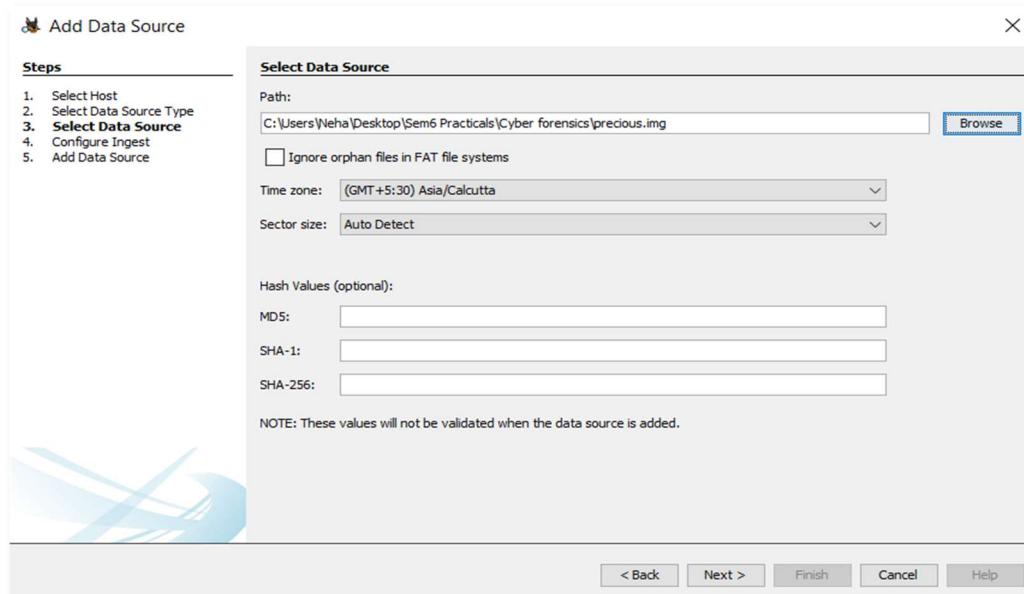
< Back Next > Finish Cancel Help



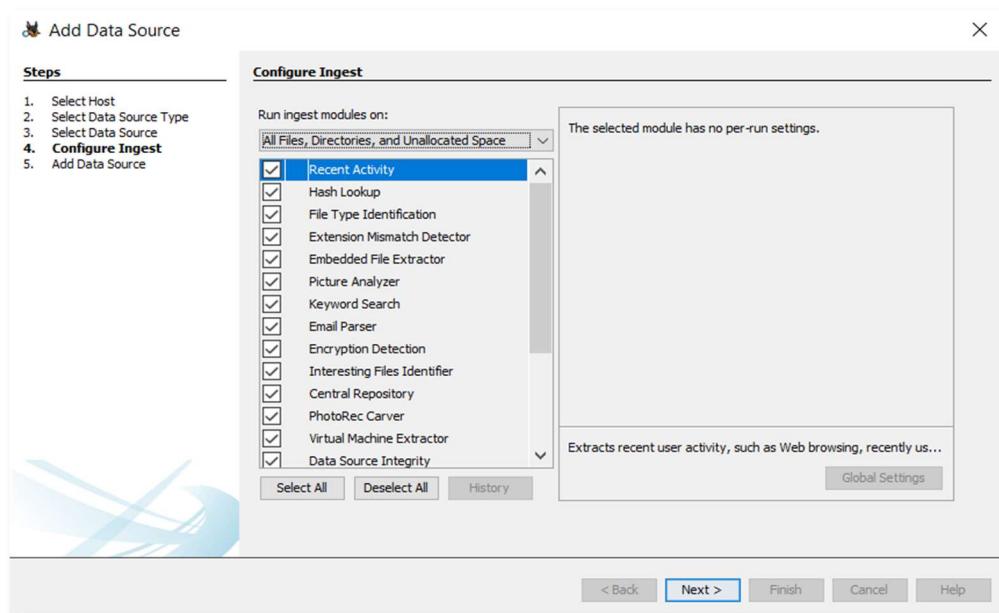
You will need to choose the type of input data source to add image.
Click on disk image or VM file then click on next



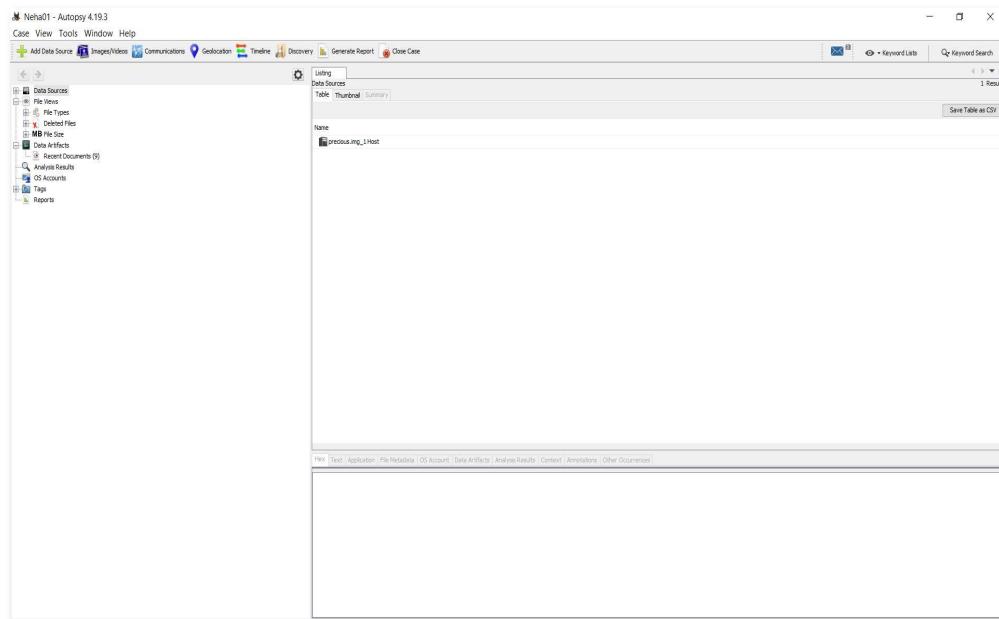
Next, supply it with the location of the source to add.



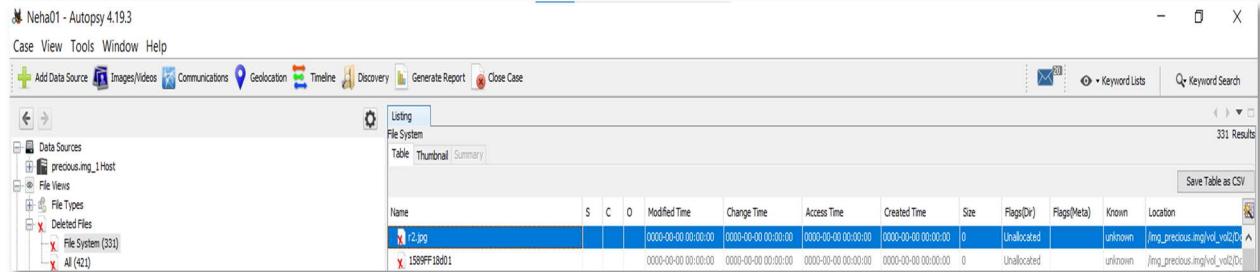
Click on next and finish



Autopsy will start to analyze these data sources and add them to the case and internal database



Click on deleted files < file system select first image



You can see metadata of image file

Metadata	
Name:	/img_precious.img/vol_vol2/Documents and Settings/Bilbo Baggins/My Documents/Pez Pix/r2.jpg
Type:	File System
MIME Type:	application/octet-stream
Size:	0
File Name Allocation:	Unallocated
Metadata Allocation:	
Modified:	0000-00-00 00:00:00
Accessed:	0000-00-00 00:00:00
Created:	0000-00-00 00:00:00
Changed:	0000-00-00 00:00:00
MD5:	d41d8cd98f00b204e9800998ecf8427e
SHA-256:	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
Hash Lookup Results:	UNKNOWN
Internal ID:	1000

Click on html report

 Generate Report X

Select and Configure Report Modules

Report Modules:

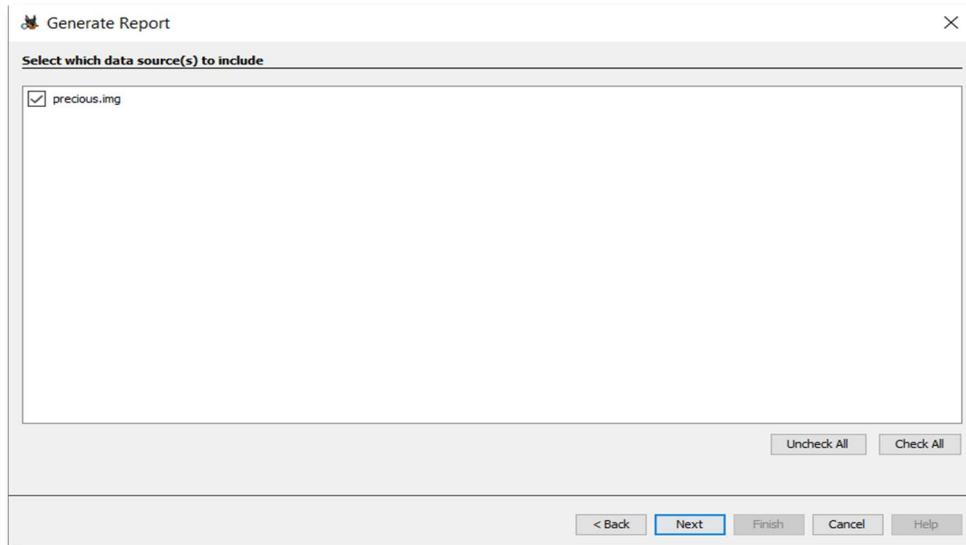
- HTML Report
- Excel Report
- Files - Text
- Data Source Summary Report
- Save Tagged Hashes
- Extract Unique Words
- TSK Body File
- Google Earth KML
- CASE-UCO
- Portable Case

A report about results and tagged items in HTML format.

Header:	<input type="text" value="neha"/>
Footer:	<input type="text"/>

< Back Next > Finish Cancel Help

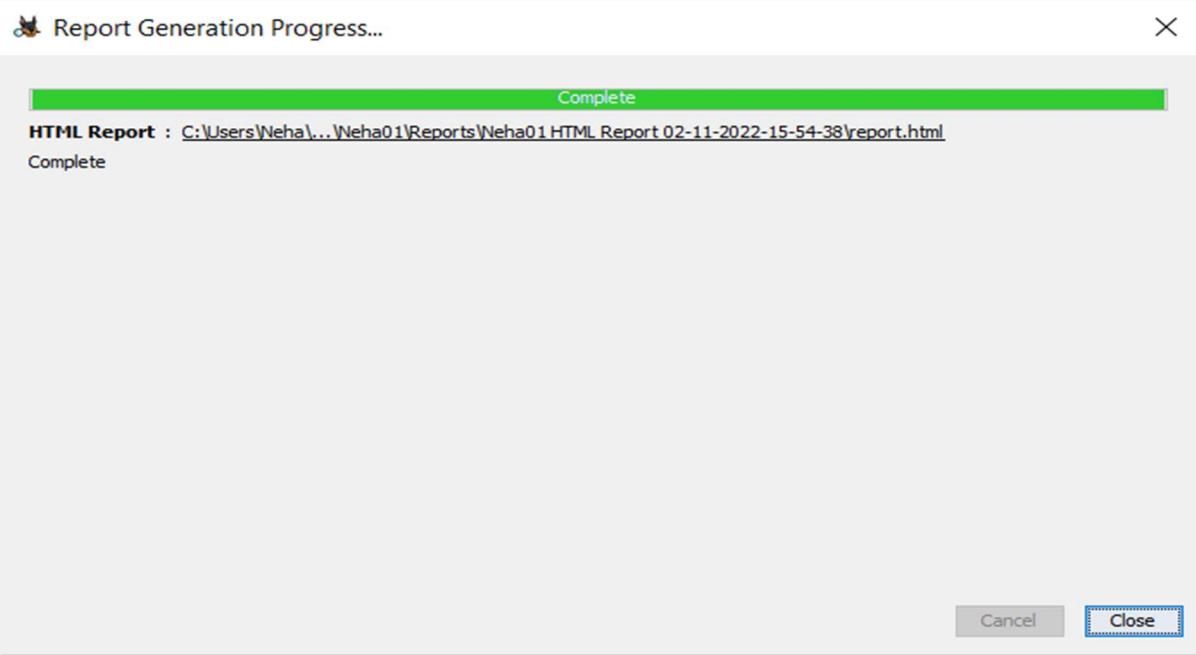
click on check box then click on next



Click on all results radio button



Html report is generated click on link it will redirect to browser



Report Navigation

- Case Summary
 - Accounts, Email (38)
 - Data Source Usage (1)
 - E-Mail Messages (65)
 - Encryption Detected (4)
 - Extension Mismatch Detected (22)
 - Installed Programs (61)
 - Keyword Hits (603)
 - Metadata (8)
 - Operating System Information (2)
 - Recent Documents (17)
 - Remote Drive (1)
 - Shell Bags (294)
 - Tagged Files (0)
 - Tagged Images (0)
 - Tagged Results (0)
 - USB Device Attached (19)
 - Web Bookmarks (24)
 - Web Categories (5)

Autopsy Forensic Report

Printed: Friday, October 01, 2022 11:54:28

Case: Neha01
Case Number: 01
Number of data sources: 1
In case:
Notes: x0000000000000000
Examiner: Neha

neha

Image Information:

previous.img

Timezone: Asia/Calcutta
Path: C:\Users\Neha\Desktop\Sem6 Practical\Cyber forensics\previous.img

Software Information:

Autopsy Version:	4.19.3
Android Analyzer Module:	4.19.3
Android Analyzer (aEAPP) Module:	4.19.3

Practical 4

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

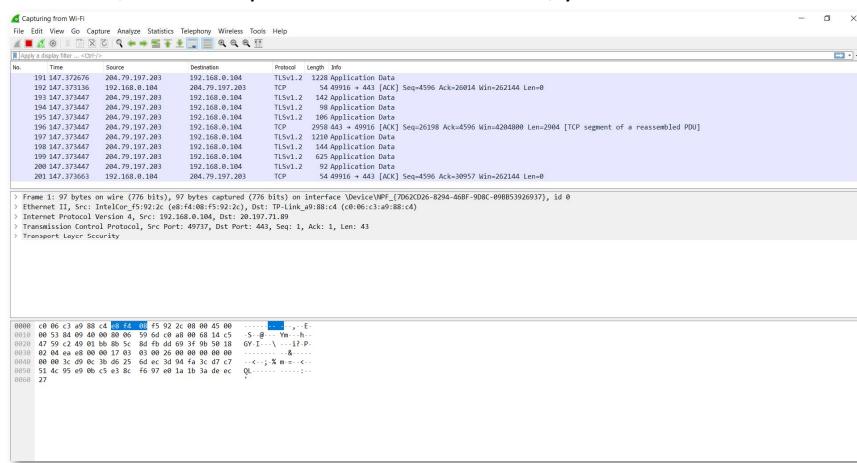
- Identification the live network
- Capture Packets
- Analyze the captured packets

Capturing Packets

Select wifi/Ethernet

Analyze the captured Packets:

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



Display filter command –

1. ip.addr ==192.168.0.1 (change ip based on current scenario)

Wi-Fi						
No.	Time	Source	Destination	Protocol	Length	Info
ip.addr ==192.168.0.1						
15	30.750202	192.168.0.104	192.168.0.1	UDP	70	51312 → 2054 Len=28
16	30.751282	192.168.0.1	192.168.0.104	ICMP	98	Destination unreachable (Port unreachable)
53	90.764857	192.168.0.104	192.168.0.1	UDP	70	51314 → 2054 Len=28
54	90.767810	192.168.0.1	192.168.0.104	ICMP	98	Destination unreachable (Port unreachable)
56	95.354540	192.168.0.1	239.255.255.250	SSDP	459	NOTIFY * HTTP/1.1
57	95.359549	192.168.0.1	239.255.255.250	SSDP	468	NOTIFY * HTTP/1.1
58	95.457547	192.168.0.1	239.255.255.250	SSDP	527	NOTIFY * HTTP/1.1
59	95.464231	192.168.0.1	239.255.255.250	SSDP	521	NOTIFY * HTTP/1.1
60	95.468383	192.168.0.1	239.255.255.250	SSDP	459	NOTIFY * HTTP/1.1
61	95.472865	192.168.0.1	239.255.255.250	SSDP	468	NOTIFY * HTTP/1.1
62	95.475266	192.168.0.1	239.255.255.250	SSDP	531	NOTIFY * HTTP/1.1
63	95.482235	192.168.0.1	239.255.255.250	SSDP	523	NOTIFY * HTTP/1.1
64	95.487316	192.168.0.1	239.255.255.250	SSDP	468	NOTIFY * HTTP/1.1
65	95.489974	192.168.0.1	239.255.255.250	SSDP	507	NOTIFY * HTTP/1.1

2. ip.src ==192.168.0.1 (change ip based on current scenario)

Wi-Fi						
No.	Time	Source	Destination	Protocol	Length	Info
ip.src ==192.168.0.1						
16	30.751282	192.168.0.1	192.168.0.104	ICMP	98	Destination unreachable (Port unreachable)
54	90.767810	192.168.0.1	192.168.0.104	ICMP	98	Destination unreachable (Port unreachable)
56	95.354540	192.168.0.1	239.255.255.250	SSDP	459	NOTIFY * HTTP/1.1
57	95.359549	192.168.0.1	239.255.255.250	SSDP	468	NOTIFY * HTTP/1.1
58	95.457547	192.168.0.1	239.255.255.250	SSDP	527	NOTIFY * HTTP/1.1
59	95.464231	192.168.0.1	239.255.255.250	SSDP	521	NOTIFY * HTTP/1.1
60	95.468383	192.168.0.1	239.255.255.250	SSDP	459	NOTIFY * HTTP/1.1
61	95.472865	192.168.0.1	239.255.255.250	SSDP	468	NOTIFY * HTTP/1.1
62	95.475266	192.168.0.1	239.255.255.250	SSDP	531	NOTIFY * HTTP/1.1
63	95.482235	192.168.0.1	239.255.255.250	SSDP	523	NOTIFY * HTTP/1.1
64	95.487316	192.168.0.1	239.255.255.250	SSDP	468	NOTIFY * HTTP/1.1
65	95.489974	192.168.0.1	239.255.255.250	SSDP	507	NOTIFY * HTTP/1.1

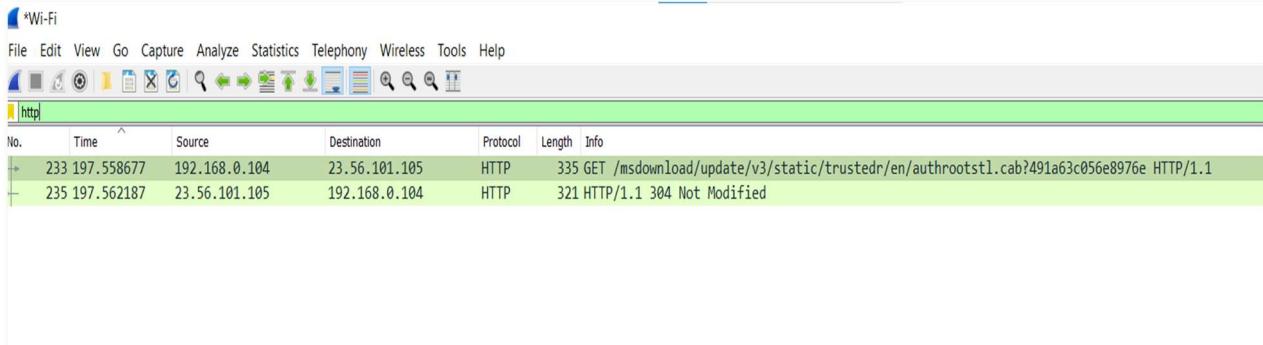
> Frame 16: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface \Device\NPF_{7062CD26-8294-46BF-9D8C-09BB53926937}, id 0
> Ethernet II, Src: TP-Link_a9:88:c4 (e0:06:c3:a9:88:c4), Dst: IntelCor_f5:92:2c (e8:f4:08:f5:92:2c)
> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.104
> Internet Control Message Protocol
> Data (28 bytes)

3. ip.dst ==192.168.0.104 (change ip based on current scenario)

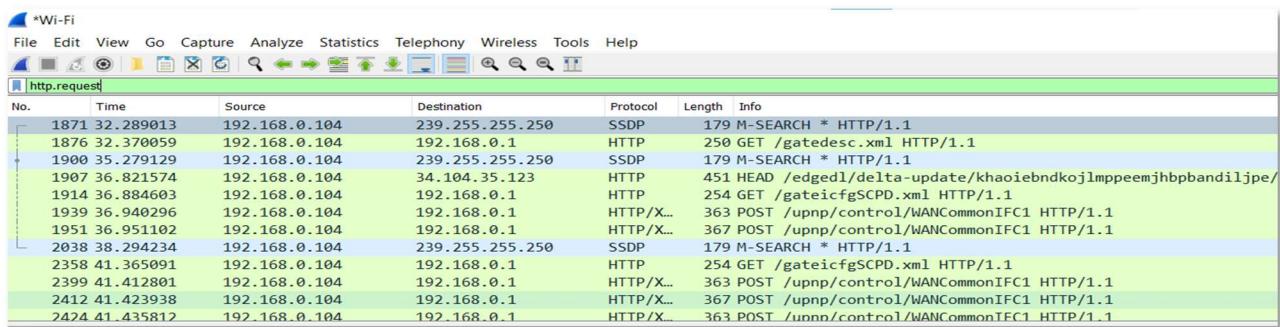
Wi-Fi						
No.	Time	Source	Destination	Protocol	Length	Info
ip.dst ==192.168.0.104						
30	41.917967	46.4.107.149	192.168.0.104	TCP	54	[TCP Keep-Alive] 80 → 49691 [ACK] Seq=1 Ack=1 Win=501 Len=0
33	45.085808	20.197.71.89	192.168.0.104	TLSv1.2	228	Application Data
35	52.254204	46.4.107.149	192.168.0.104	TCP	54	[TCP Keep-Alive] 80 → 49691 [ACK] Seq=1 Ack=1 Win=501 Len=0
39	62.583580	46.4.107.149	192.168.0.104	TCP	54	[TCP Keep-Alive] 80 → 49691 [ACK] Seq=1 Ack=1 Win=501 Len=0
41	72.926086	46.4.107.149	192.168.0.104	TCP	54	[TCP Keep-Alive] 80 → 49691 [ACK] Seq=1 Ack=1 Win=501 Len=0
44	76.002039	46.4.107.149	192.168.0.104	TCP	66	[TCP Keep-Alive ACK] 80 → 49691 [ACK] Seq=2 Ack=1 Win=501 Len=0 SLE=0
45	86.139766	46.4.107.149	192.168.0.104	TCP	54	[TCP Keep-Alive] 80 → 49691 [ACK] Seq=1 Ack=1 Win=501 Len=0
51	90.102965	20.197.71.89	192.168.0.104	TLSv1.2	228	Application Data
54	90.767810	192.168.0.1	192.168.0.104	ICMP	98	Destination unreachable (Port unreachable)
68	96.478672	46.4.107.149	192.168.0.104	TCP	54	[TCP Keep-Alive] 80 → 49691 [ACK] Seq=1 Ack=1 Win=501 Len=0
72	106.823343	46.4.107.149	192.168.0.104	TCP	54	[TCP Keep-Alive] 80 → 49691 [ACK] Seq=1 Ack=1 Win=501 Len=0
74	117.163517	46.4.107.149	192.168.0.104	TCP	54	[TCP Keep-Alive] 80 → 49691 [ACK] Seq=1 Ack=1 Win=501 Len=0

> Frame 2: 228 bytes on wire (1824 bits), 228 bytes captured (1824 bits) on interface \Device\NPF_{7062CD26-8294-46BF-9D8C-09BB53926937}, id 0
> Ethernet II, Src: TP-Link_a9:88:c4 (e0:06:c3:a9:88:c4), Dst: IntelCor_f5:92:2c (e8:f4:08:f5:92:2c)
> Internet Protocol Version 4, Src: 20.197.71.89, Dst: 192.168.0.104
> Transmission Control Protocol, Src Port: 443, Dst Port: 49737, Seq: 1, Ack: 44, Len: 174
> Transport Layer Security

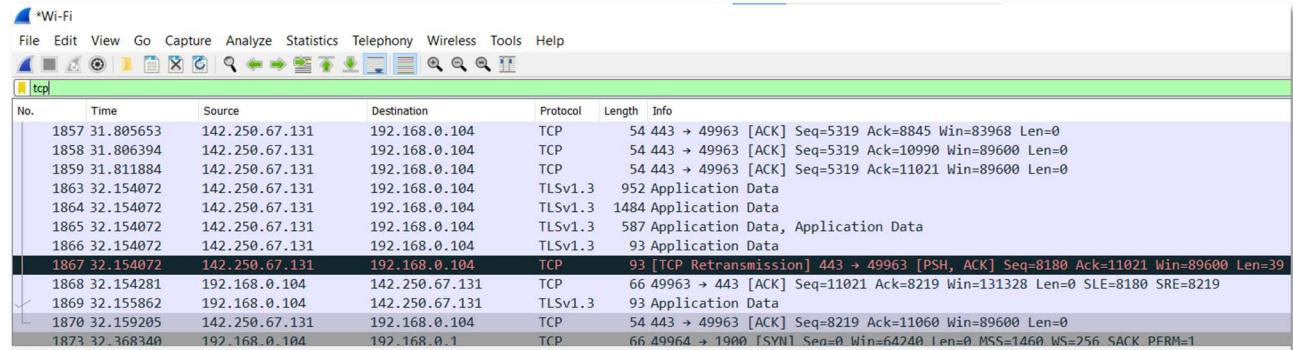
4. http (start recording and search for http website and visit any website which is of http)



5. http.request



6. Tcp



7. http.response.code==200

*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http.response.code==200

No.	Time	Source	Destination	Protocol	Length	Info
1872	32.311965	192.168.0.1	192.168.0.104	SSDP	527	HTTP/1.1 200 OK
1881	32.373085	192.168.0.1	192.168.0.104	HTTP/X...	513	HTTP/1.1 200 OK
1901	35.283313	192.168.0.1	192.168.0.104	SSDP	527	HTTP/1.1 200 OK
1909	36.828902	34.104.35.123	192.168.0.104	TCP	603	HTTP/1.1 200 OK [TCP segment of a reassembled PDU]
1918	36.887829	192.168.0.1	192.168.0.104	HTTP/X...	1309	HTTP/1.1 200 OK
1927	36.928158	192.168.0.1	192.168.0.104	HTTP	293	HTTP/1.1 200 OK
1943	36.946229	192.168.0.1	192.168.0.104	HTTP/X...	389	HTTP/1.1 200 OK
1955	36.957213	192.168.0.1	192.168.0.104	HTTP/X...	406	HTTP/1.1 200 OK
1961	36.979455	192.168.0.104	192.168.0.1	HTTP	179	HTTP/1.1 200 OK
2039	38.299180	192.168.0.1	192.168.0.104	SSDP	527	HTTP/1.1 200 OK
2371	41.370751	192.168.0.1	192.168.0.104	HTTP/X...	1309	HTTP/1.1 200 OK
2386	41.401610	192.168.0.1	192.168.0.104	HTTP	293	HTTP/1.1 200 OK

8. tcp.port==80 | udp.port==80

*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.port==80 | udp.port==80

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	46.4.107.149	192.168.0.104	TCP	54	80 → 49691 [ACK] Seq=1 Ack=1 Win=501 Len=0
2	0.000133	192.168.0.104	46.4.107.149	TCP	54	[TCP ACKed unseen segment] 49691 → 80 [ACK] Seq=1 Ack=2 Win=514 Len=0
117	10.329034	46.4.107.149	192.168.0.104	TCP	54	[TCP Dup ACK #1] 80 → 49691 [ACK] Seq=1 Ack=1 Win=501 Len=0
118	10.329177	192.168.0.104	46.4.107.149	TCP	54	[TCP Dup ACK #1] [TCP ACKed unseen segment] 49691 → 80 [ACK] Seq=1 Ack=2 Win=514 Len=0
1522	20.685274	46.4.107.149	192.168.0.104	TCP	54	[TCP Dup ACK #2] 80 → 49691 [ACK] Seq=1 Ack=1 Win=501 Len=0
1523	20.685479	192.168.0.104	46.4.107.149	TCP	54	[TCP Dup ACK #2] [TCP ACKed unseen segment] 49691 → 80 [ACK] Seq=1 Ack=2 Win=514 Len=0
1786	31.028147	46.4.107.149	192.168.0.104	TCP	54	[TCP Dup ACK #3] 80 → 49691 [ACK] Seq=1 Ack=1 Win=501 Len=0
1787	31.028343	192.168.0.104	46.4.107.149	TCP	54	[TCP Dup ACK #3] [TCP ACKed unseen segment] 49691 → 80 [ACK] Seq=1 Ack=2 Win=514 Len=0
1885	33.876410	192.168.0.104	46.4.107.149	TCP	55	[TCP Keep-Alive] [TCP ACKed unseen segment] 49691 → 80 [ACK] Seq=0 Ack=2 Win=514 Len=1
1886	34.202028	46.4.107.149	192.168.0.104	TCP	66	[TCP Previous segment not captured] 80 → 49691 [ACK] Seq=2 Ack=1 Win=501 Len=0 SLE=0 SRE=1
1904	36.817454	192.168.0.104	34.104.35.123	TCP	66	49968 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
1905	36.821166	34.104.35.123	192.168.0.104	TCP	66	80 → 49968 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1452 SACK_PERM=1 WS=256

9. Go to facebook.com

tcp and frame contains "facebook.com"
tcp and frame contains "facebook"

*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp and frame contains "facebook.com"

No.	Time	Source	Destination	Protocol	Length	Info
2672	16.842609	2401:4900:172d:a58c...	2a03:2880:f06d:10:f...	TLSv1.3	591	Client Hello
2798	17.143641	2401:4900:172d:a58c...	2a03:2880:f06d:10:f...	TCP	591	[TCP Retransmission] 24933 → 443 [PSH, ACK] Seq=1 Ack=1 Win=66048 Len=517
2864	17.286091	192.168.208.84	157.240.228.19	TLSv1.3	571	Client Hello
3217	17.925439	192.168.208.84	157.240.228.15	TLSv1.3	571	Client Hello
3965	22.149423	2401:4900:172d:a58c...	2a03:2880:f06d:10:f...	TLSv1.3	591	Client Hello

Practical 5

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

- Monitor LiveProcesses
- CaptureRAM
- Capture TCP/UDP packets
- Monitor HardDisk
- Monitor VirtualMemory
- Monitor CacheMemory

Monitor Live Processes : (Tool: ProcMon) ToDo:

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

Filter (Process Name or PID or Architecture)

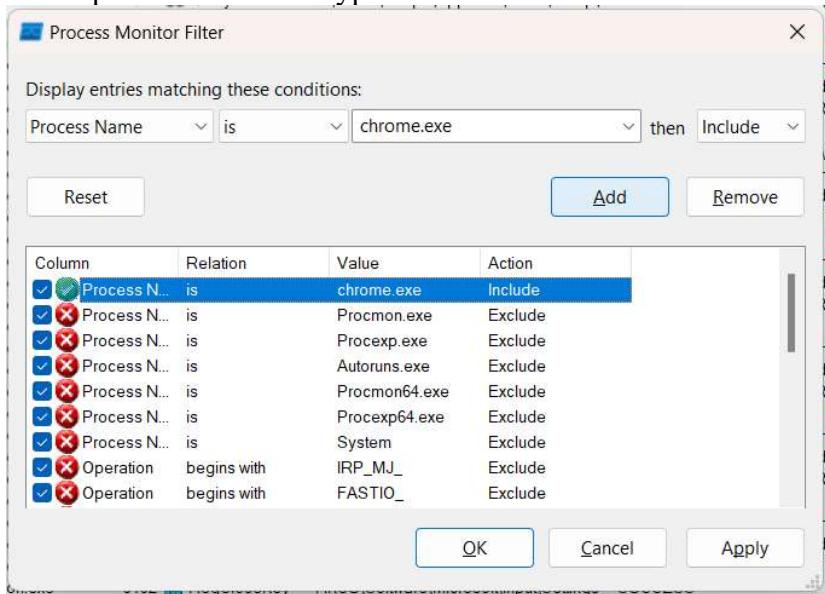
Open chrome and go to any website to start the process

Click on filter or Ctrl + L

The screenshot shows the Process Monitor interface with the title bar "Process Monitor - Sysinternals: www.sysinternals.com". The menu bar includes File, Edit, Event, Filter, Tools, Options, and Help. Below the menu is a toolbar with various icons for file operations and monitoring. A status bar at the bottom indicates "Showing 39797 of 312499 events (12%) Backed by virtual memory".

Time o...	Process Name	Filter (Ctrl+L) on	Path	Result	Detail
08:06:22...	IIsass.exe	1020	QueryNameInfo... C:\Users\deepta\AppData\Local\Temp\...	SUCCESS	Name: \Users\dee...
08:06:22...	IIsass.exe	1028	QueryNameInfo... C:\Users\deepta\AppData\Local\Temp\...	SUCCESS	Name: \Users\dee...
08:06:22...	SearchIndexer...	7892	FileSystemCont... C:	SUCCESS	Control: FSCTL_RE...
08:06:22...	SearchIndexer...	7892	FileSystemCont... C:	SUCCESS	Control: FSCTL_RE...
08:06:22...	ctfmon.exe	9192	RegQueryKey HKLM	SUCCESS	Query: HandleTag...
d08:06:22...	ctfmon.exe	9192	RegOpenKey HKLM\Software\Microsoft\Input\Locales\...	SUCCESS	Desired Access: R...
08:06:22...	ctfmon.exe	9192	RegQueryValue HKLM\SOFTWARE\Microsoft\Input\Loca...	SUCCESS	Type: REG_DWO...
1108:06:22...	ctfmon.exe	9192	RegCloseKey HKLM\SOFTWARE\Microsoft\Input\Loca...	SUCCESS	
08:06:22...	ctfmon.exe	9192	QueryNameInfo... C:\Users\deepta\AppData\Local\Temp\...	SUCCESS	Name: \Users\dee...
08:06:22...	ctfmon.exe	9192	RegQueryKey HKCU	SUCCESS	Query: HandleTag...
08:06:22...	ctfmon.exe	9192	RegOpenKey HKCU\SOFTWARE\Microsoft\Input\Setti...	SUCCESS	Desired Access: R...
08:06:22...	ctfmon.exe	9192	RegQueryValue HKCU\Software\Microsoft\input\Settings\...	NAME NOT FOUND Length: 16	
08:06:22...	ctfmon.exe	9192	RegCloseKey HKCU\Software\Microsoft\input\Settings	SUCCESS	
08:06:22...	ctfmon.exe	9192	RegQueryKey HKLM	SUCCESS	
08:06:22...	ctfmon.exe	9192	RegOpenKey HKLM\Software\Microsoft\Input\Setti...	SUCCESS	Desired Access: R...
08:06:22...	ctfmon.exe	9192	RegQueryValue HKLM\SOFTWARE\Microsoft\Input\Setti...	SUCCESS	Type: REG_DWO...
08:06:22...	ctfmon.exe	9192	RegCloseKey HKLM\SOFTWARE\Microsoft\Input\Setti...	SUCCESS	
a08:06:22...	ctfmon.exe	9192	RegQueryKey HKCU	SUCCESS	Query: HandleTag...
08:06:22...	ctfmon.exe	9192	RegOpenKey HKCU\Software\Microsoft\input\TypingIn...	SUCCESS	Desired Access: R...
08:06:22...	ctfmon.exe	9192	RegQueryValue HKCU\Software\Microsoft\input\TypingIn...	SUCCESS	Type: REG_BINAR...
08:06:22...	ctfmon.exe	9192	RegCloseKey HKCU\Software\Microsoft\input\TypingIn...	SUCCESS	
08:06:22...	ctfmon.exe	9192	RegQueryKey HKCU	SUCCESS	Query: HandleTag...
08:06:22...	ctfmon.exe	9192	RegCreateKey HKCU\Software\Microsoft\input\TypingIn...	SUCCESS	Desired Access: W...
08:06:22...	ctfmon.exe	9192	RegSetValue HKCU\Software\Microsoft\input\TypingIn...	SUCCESS	Type: REG_BINAR...
08:06:22...	ctfmon.exe	9192	RegCloseKey HKCU\Software\Microsoft\input\TypingIn...	SUCCESS	
08:06:22...	ctfmon.exe	9192	RegQueryKey HKCU	SUCCESS	Query: HandleTag...
08:06:22...	ctfmon.exe	9192	RegOpenKey HKCU\Software\Microsoft\input\Setti...	SUCCESS	Desired Access: R...
08:06:22...	ctfmon.exe	9192	RegQueryValue HKCU\Software\Microsoft\input\Settings\...	NAME NOT FOUND Length: 16	
08:06:22...	ctfmon.exe	9192	RegCloseKey HKCU\Software\Microsoft\input\Settings	SUCCESS	
08:06:22...	ctfmon.exe	9192	RegQueryKey HKLM	SUCCESS	Query: HandleTag...
08:06:22...	ctfmon.exe	9192	RegOpenKey HKLM\Software\Microsoft\input\Setti...	SUCCESS	Desired Access: R...
08:06:22...	ctfmon.exe	9192	RegQueryValue HKLM\SOFTWARE\Microsoft\input\Setti...	NAME NOT FOUND Length: 16	

Select process name and type chrome.exe



ProcessTree

Select Process Tree

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time... Process Name PID Operation Process Tree lh Result Detail

08:06:22...	chrome.exe	6712	UDP Send	HEWLETT-I3-PACKARD:56675->born0...	SUCCESS	Length: 33, seqnum...
08:06:22...	chrome.exe	6712	UDP Receive	HEWLETT-I3-PACKARD:56675->born0...	SUCCESS	Length: 29, seqnum...
08:06:25...	chrome.exe	14984	Thread Exit		SUCCESS	Thread ID: 1736, U...
08:06:25...	chrome.exe	14984	Thread Exit		SUCCESS	Thread ID: 15568, ...
08:06:26...	chrome.exe	6712	Thread Exit		SUCCESS	Thread ID: 11924, ...
08:06:27...	chrome.exe	6948	Thread Exit		SUCCESS	Thread ID: 5952, U...
08:06:29...	chrome.exe	6712	UDP Send	HEWLETT-I3-PACKARD:56675->born0...	SUCCESS	Length: 33, seqnum...
08:06:29...	chrome.exe	6712	UDP Receive	HEWLETT-I3-PACKARD:56675->born0...	SUCCESS	Length: 29, seqnum...
08:06:32...	chrome.exe	14984	ReadFile	C:\Users\deepa\AppData\Local\Google...	END OF FILE	Offset 9216, Length...
08:06:32...	chrome.exe	14984	FlushBuffersFile	C:\Users\deepa\AppData\Local\Google...	SUCCESS	Offset 0, Length: 12
08:06:32...	chrome.exe	14984	WriteFile	C:\Users\deepa\AppData\Local\Google...	SUCCESS	Offset 0, Length: 40...
08:06:32...	chrome.exe	14984	FlushBuffersFile	C:\Users\deepa\AppData\Local\Google...	SUCCESS	Offset 32768, Length...
08:06:32...	chrome.exe	14984	WriteFile	C:\Users\deepa\AppData\Local\Google...	SUCCESS	Offset 45056, Length...
08:06:32...	chrome.exe	14984	FlushBuffersFile	C:\Users\deepa\AppData\Local\Google...	SUCCESS	Offset 32768, Length...
08:06:32...	chrome.exe	14984	WriteFile	C:\Users\deepa\AppData\Local\Google...	SUCCESS	Offset 45056, Length...
08:06:32...	chrome.exe	14984	SetEndOfFileInf	C:\Users\deepa\AppData\Local\Google...	SUCCESS	EndOfFile: 0
08:06:32...	chrome.exe	14984	SetAllocationInf	C:\Users\deepa\AppData\Local\Google...	SUCCESS	AllocationSize: 0
08:06:32...	chrome.exe	14984	FlushBuffersFile	C:\Users\deepa\AppData\Local\Google...	SUCCESS	Offset: -1, Length: 7
08:06:32...	chrome.exe	14984	WriteFile	C:\Users\deepa\AppData\Local\Google...	SUCCESS	Desired Access: R...
08:06:32...	chrome.exe	14984	RegOpenKey	HKEY\Software\Microsoft\Windows\Tabl...	SUCCESS	Offset: -1, Length: 162
08:06:32...	chrome.exe	14984	WriteFile	C:\Users\deepa\AppData\Local\Google...	SUCCESS	Type: REG_DWO...
08:06:32...	chrome.exe	14984	RegQueryValue	HKEY\Software\Microsoft\Windows\...	SUCCESS	Desired Access: R...
08:06:32...	chrome.exe	14984	RegCloseKey	HKEY\Software\Microsoft\Windows\...	SUCCESS	Type: REG_DWO...
08:06:32...	chrome.exe	14984	RegOpenKey	HKEY\Software\Microsoft\Windows\Tabl...	SUCCESS	Desired Access: R...
08:06:32...	chrome.exe	14984	RegQueryValue	HKEY\Software\Microsoft\Windows\...	SUCCESS	Type: REG_DWO...
08:06:32...	chrome.exe	14984	RegCloseKey	HKEY\Software\Microsoft\Windows\...	SUCCESS	Desired Access: R...
08:06:32...	chrome.exe	14984	RegOpenKey	HKEY\Software\Microsoft\Windows\Tabl...	SUCCESS	Type: REG_DWO...
08:06:32...	chrome.exe	14984	RegQueryValue	HKEY\Software\Microsoft\Windows\...	SUCCESS	Desired Access: R...
08:06:32...	chrome.exe	14984	RegCloseKey	HKEY\Software\Microsoft\Windows\...	SUCCESS	Type: REG_DWO...
Showing 1642759 of 3264960 events (50%) Backed by virtual memory						
Process	Description	Image Path	Life Time	Company	Owner	
WinLogon.exe (15896)	Windows Logon A...	C:\WINDOWS\Sys...		Microsoft Corporati...	NT AUTHORITY...	
fontdrvhost.exe (13924)	Usermode Font Dr...	C:\WINDOWS\Sys...		Microsoft Corporati...	Font Driver H...	
dwm.exe (2968)	Desktop Window ...	C:\WINDOWS\Sys...		Microsoft Corporati...	Window Man...	
Explorer.EXE (6968)	Windows Explorer	C:\WINDOWS\Exp...		Microsoft Corporati...	HEWLETT-I3	
SecurityHealthStray.exe (1444)	Windows Security ...	C:\Windows\Syste...		Microsoft Corporati...	HEWLETT-I3	
RtkAudUService64.exe (4308)	Realtek HD Audio ...	C:\Windows\Syste...		Realtek Semicond...	HEWLETT-I3	
WINWORD.EXE (1552)	Microsoft Word	C:\Program Files\...		Microsoft Corporati...	HEWLETT-I3	
ai.exe (15036)	Artificial Intelligenc...	C:\Program Files\...		Microsoft Corporati...	HEWLETT-I3	
chrome.exe (14984)	Google Chrome	C:\Program Files\...		Google LLC	HEWLETT-I3	
chrome.exe (12360)	Google Chrome	C:\Program Files\...		Google LLC	HEWLETT-I3	
chrome.exe (13124)	Google Chrome	C:\Program Files\...		Google LLC	HEWLETT-I3	
chrome.exe (6712)	Google Chrome	C:\Program Files\...		Google LLC	HEWLETT-I3	
chrome.exe (14440)	Google Chrome	C:\Program Files\...		Google LLC	HEWLETT-I3	
chrome.exe (5976)	Google Chrome	C:\Program Files\...		Google LLC	HEWLETT-I3	
chrome.exe (10084)	Google Chrome	C:\Program Files\...		Google LLC	HEWLETT-I3	
chrome.exe (13740)	Google Chrome	C:\Program Files\...		Google LLC	HEWLETT-I3	
chrome.exe (9372)	Google Chrome	C:\Program Files\...		Google LLC	HEWLETT-I3	
chrome.exe (10996)	Google Chrome	C:\Program Files\...		Google LLC	HEWLETT-I3	
chrome.exe (12916)	Google Chrome	C:\Program Files\...		Google LLC	HEWLETT-I3	
chrome.exe (6948)	Google Chrome	C:\Program Files\...		Google LLC	HEWLETT-I3	

Process ActivitySummary

Only select show profiling events and it will show summary

Time ...	Process Name	PID	Operation	Path	Result	Detail
08:06:22...	chrome.exe	14984	Process Profiling		SUCCESS	User Time: 9.70312...
08:06:22...	chrome.exe	12360	Process Profiling		SUCCESS	User Time: 0.01562...
08:06:22...	chrome.exe	13124	Process Profiling		SUCCESS	User Time: 2.98437...
08:06:22...	chrome.exe	6712	Process Profiling		SUCCESS	User Time: 1.56250...
08:06:22...	chrome.exe	14440	Process Profiling		SUCCESS	User Time: 0.04687...
08:06:22...	chrome.exe	5976	Process Profiling		SUCCESS	User Time: 0.09375...
08:06:22...	chrome.exe	10084	Process Profiling		SUCCESS	User Time: 0.04687...
08:06:22...	chrome.exe	13740	Process Profiling		SUCCESS	User Time: 0.09375...
08:06:22...	chrome.exe	9372	Process Profiling		SUCCESS	User Time: 0.06250...
08:06:22...	chrome.exe	10996	Process Profiling		SUCCESS	User Time: 0.10937...
08:06:22...	chrome.exe	12916	Process Profiling		SUCCESS	User Time: 0.10937...
08:06:22...	chrome.exe	6948	Process Profiling		SUCCESS	User Time: 14.1718...
08:06:22...	chrome.exe	10304	Process Profiling		SUCCESS	User Time: 0.00000...
08:06:22...	chrome.exe	9580	Process Profiling		SUCCESS	User Time: 0.01562...
08:06:23...	chrome.exe	14984	Process Profiling		SUCCESS	User Time: 9.70312...
08:06:23...	chrome.exe	12360	Process Profiling		SUCCESS	User Time: 0.01562...
08:06:23...	chrome.exe	13124	Process Profiling		SUCCESS	User Time: 2.98437...
08:06:23...	chrome.exe	6712	Process Profiling		SUCCESS	User Time: 1.56250...
08:06:23...	chrome.exe	14440	Process Profiling		SUCCESS	User Time: 0.04687...
08:06:23...	chrome.exe	5976	Process Profiling		SUCCESS	User Time: 0.09375...
08:06:23...	chrome.exe	10084	Process Profiling		SUCCESS	User Time: 0.04687...
08:06:23...	chrome.exe	13740	Process Profiling		SUCCESS	User Time: 0.09375...
08:06:23...	chrome.exe	9372	Process Profiling		SUCCESS	User Time: 0.06250...
08:06:23...	chrome.exe	10996	Process Profiling		SUCCESS	User Time: 0.10937...
08:06:23...	chrome.exe	12916	Process Profiling		SUCCESS	User Time: 0.10937...
08:06:23...	chrome.exe	6948	Process Profiling		SUCCESS	User Time: 14.1718...
08:06:23...	chrome.exe	10304	Process Profiling		SUCCESS	User Time: 0.00000...
08:06:23...	chrome.exe	9580	Process Profiling		SUCCESS	User Time: 0.01562...
08:06:24...	chrome.exe	14984	Process Profiling		SUCCESS	User Time: 9.70312...
08:06:24...	chrome.exe	12360	Process Profiling		SUCCESS	User Time: 0.01562...
08:06:24...	chrome.exe	13124	Process Profiling		SUCCESS	User Time: 2.98437...
08:06:24...	chrome.exe	6712	Process Profiling		SUCCESS	User Time: 1.56250...

Count Occurrences

Tools > Count Occurrence

Select Process Name

Column:	Process Name	Count
Value	Count	49059

Double-click an item to filter on that value.

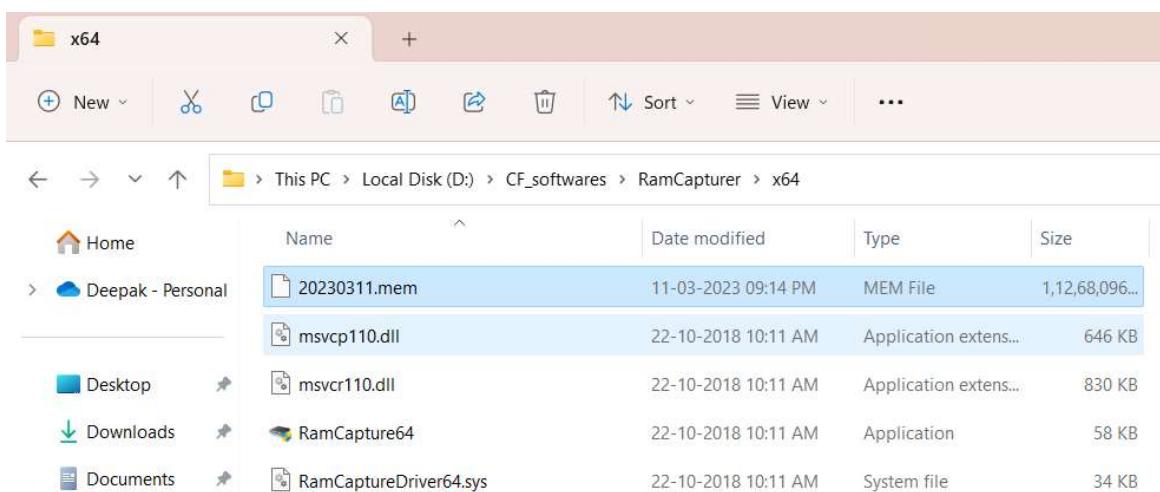
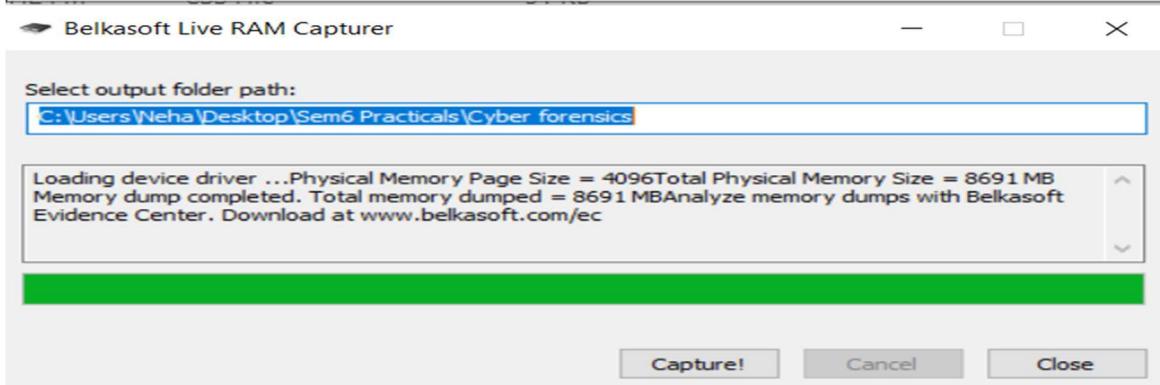
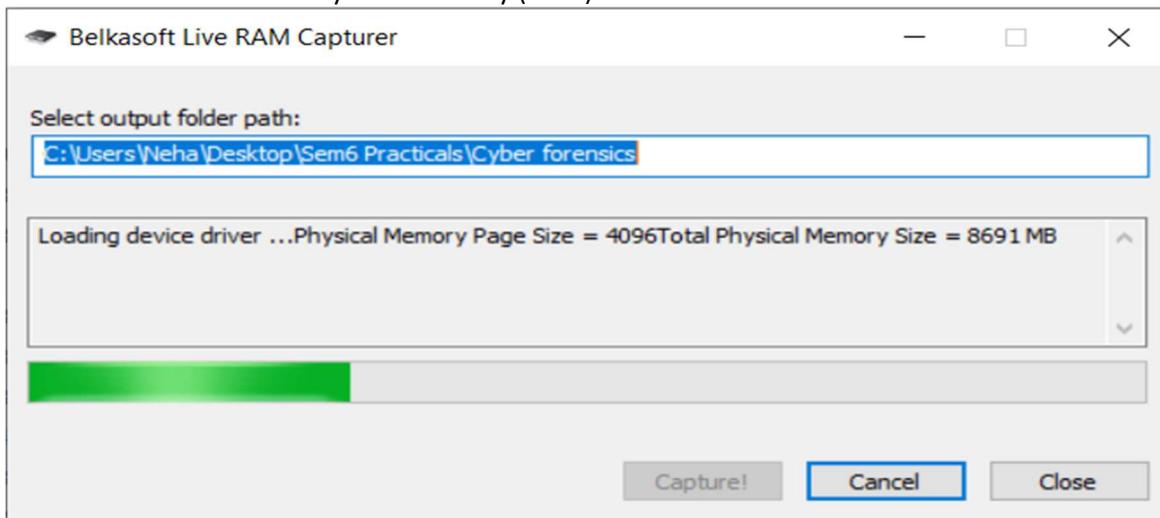
Filter... 1 items Save... Close

Capture RAM (Tool:RAMCapture)

To Do:

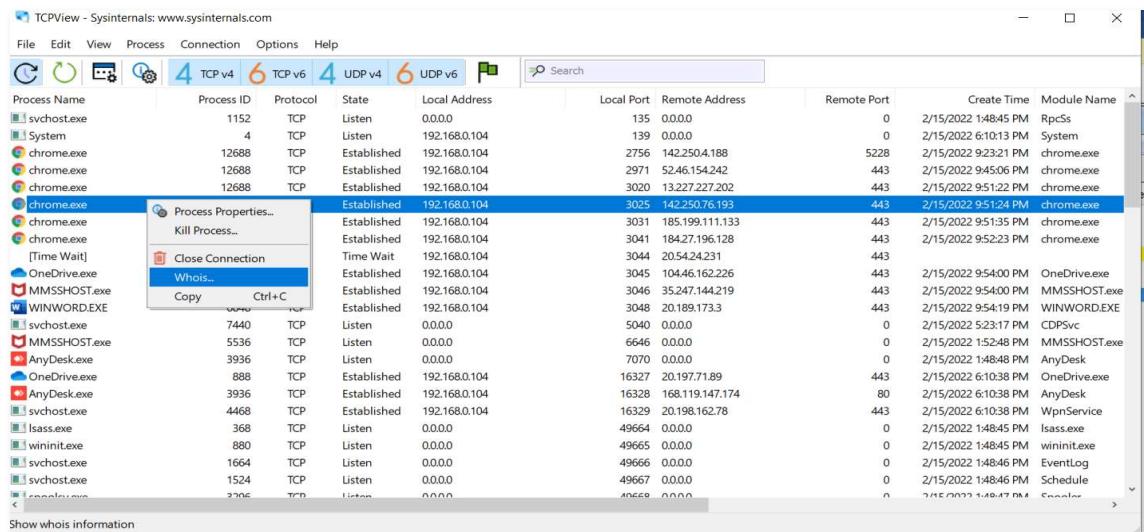
Click Capture

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



Capture TCP/UDP packets (Tool: TcpView):

To Do: Save to .txtfile. as Whois



Show whois information

Whois: a184-27-196-128.deploy.static.akamaitechnologies.com

Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferPr ^ Copy

Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdatePro

Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProt

Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferF

Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdatePr

Name Server: AX0.AKAMAISTREAM.NET

Name Server: AX1.AKAMAISTREAM.NET

Name Server: AX2.AKAMAISTREAM.NET

Name Server: AX3.AKAMAISTREAM.NET

Name Server: NS2-32.AKAMAISTREAM.NET

Name Server: NS3-32.AKAMAISTREAM.NET

Name Server: NS6-32.AKAMAISTREAM.NET

Name Server: P5.AKAMAISTREAM.NET

Name Server: P6.AKAMAISTREAM.NET

Name Server: P7.AKAMAISTREAM.NET

Name Server: P8.AKAMAISTREAM.NET

DNSSEC: unsigned

URL of the ICANN Whois Inaccuracy Complaint Form: <https://www.icann.org/wi>

>>> Last update of whois database: 2022-02-15T08:21:27Z <<<

For more information on Whois status codes, please visit <https://icann.org/epp>

OK

Monitor Hard Disk (Tool: DiskMon): To Do:

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

Disk Monitor - Sysinternals: www.sysinternals.com

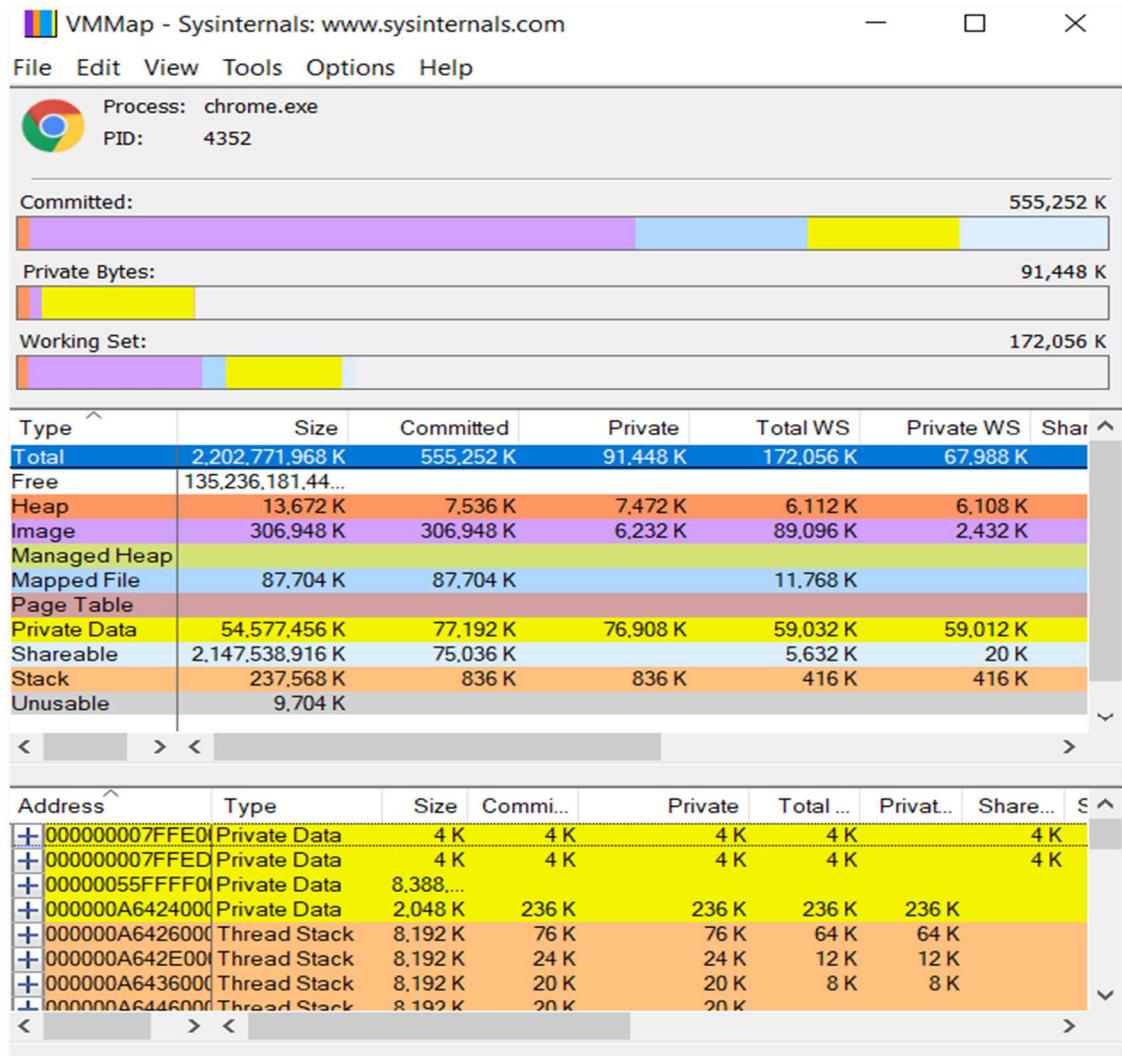
File Edit Options Help

#	Time	Duration (s)	Disk	Request	Sector	Length
948	40.004640	0.00000000	0	Write	1235736	8
949	40.004758	0.00000000	0	Write	201423472	8
950	40.004866	0.00000000	0	Write	35400384	8
951	40.005006	0.00000000	0	Write	83604912	8
952	40.005126	0.00000000	0	Write	16731432	8
953	40.005245	0.00000000	0	Read	16731432	32
954	40.005371	0.00000000	0	Write	213181532	32
955	40.005495	0.00000000	0	Write	212493200	32
956	40.005618	0.00000000	0	Write	134159352	8
957	40.005629	0.00000000	0	Write	612000	16
958	40.005646	0.00000000	0	Write	590656	8
959	40.005653	0.00000000	0	Write	709398	8
960	40.005663	0.00000000	0	Write	145247472	24
961	40.005671	0.00000000	0	Write	729504	8
962	40.005687	0.00000000	0	Write	729588	16
963	40.005702	0.00000000	0	Write	1847088	8
964	40.005707	0.00000000	0	Write	1846736	8
965	40.005717	0.00000000	0	Write	1846480	16
966	40.005715	0.00000000	0	Write	1846598	8
967	40.005742	0.00000000	0	Write	1846312	8
968	40.005750	0.00000000	0	Write	1846396	8
969	40.005765	0.00000000	0	Write	66504336	8
970	40.005757	0.00000000	0	Write	1341624	8
971	40.005782	0.00000000	0	Write	87075704	8
972	40.005800	0.00000000	0	Write	1846326	8
973	40.005806	0.00000000	0	Write	3175984	8
974	40.005820	0.00000000	0	Write	2108440	8
975	40.005832	0.00000000	0	Write	1795736	8
976	40.005839	0.00000000	0	Write	1795792	8
977	40.005846	0.00000000	0	Write	26957480	8
978	40.005838	0.00000000	0	Write	28970300	8
979	40.005891	0.00000000	0	Write	28970280	8
980	40.005891	0.00000000	0	Write	28970520	8
981	40.005904	0.00000000	0	Write	28971432	8
982	40.005916	0.00000000	0	Write	91438456	8
983	40.005926	0.00000000	0	Write	1007000	16
984	40.005925	0.00000000	0	Write	1007048	8
985	40.005941	0.00000000	0	Write	26982192	8
986	40.005974	0.00000000	0	Write	147631976	8
987	40.005964	0.00000000	0	Write	117534944	8
988	40.005974	0.00000000	0	Write	117535008	8
989	40.005985	0.00000000	0	Write	63397120	8
990	40.005980	0.00000000	0	Write	63397280	8
991	40.010144	0.00000000	0	Write	659349	8
992	40.380838	0.00000000	0	Read	14548240	64
993	41.343143	0.00000000	0	Write	65383104	8

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

To Do:

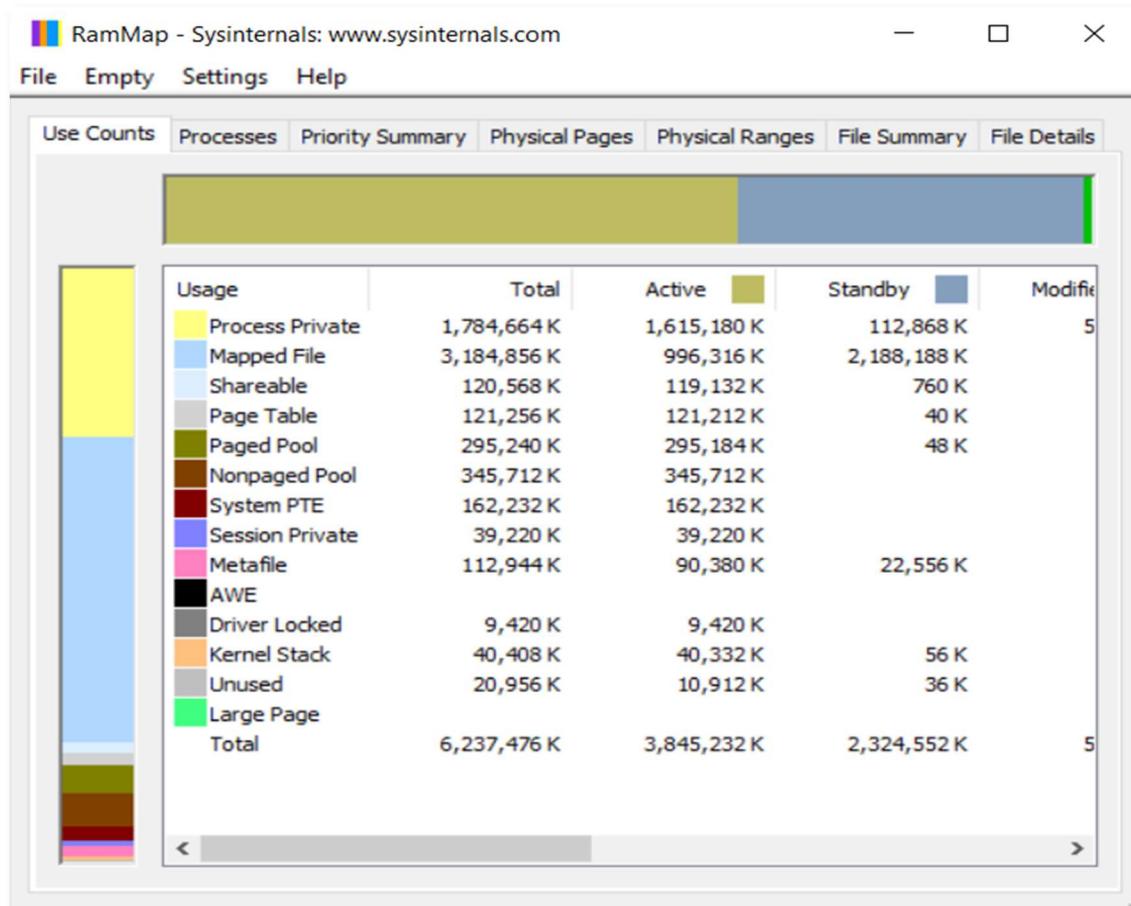
e.g.chrome.exe Save to .mmpfile.



Monitor Cache Memory

(Tool:RAMMap) TO DO :

1. Save to .RMPfile.



Practical 6

AIM: Recovering and Inspecting deleted files

- Check for Deleted Files
- Recover the Deleted Files
- Analyzing and Inspecting the recovered files

Step 1 start autopsy from desktop Now create on New Case.



Step 2: Enter the New case Information and click on Next Button.

A screenshot of the 'New Case Information' dialog box. On the left, there is a sidebar titled 'Steps' with two items: 'Case Information' (which is currently selected and highlighted in blue) and 'Optional Information'. The main panel is titled 'Case Information'. It contains the following fields:

- 'Case Name:' input field containing 'Neha02'.
- 'Base Directory:' input field containing 'C:\Users\Neha\Desktop\Sem6 Practicals\Cyber forensics\' with a 'Browse' button to its right.
- 'Case Type:' radio buttons for 'Single-User' (selected, indicated by a green dot) and 'Multi-User'.
- A note below the radio buttons stating 'Case data will be stored in the following directory:' followed by an input field containing 'C:\Users\Neha\Desktop\Sem6 Practicals\Cyber forensics\Neha02'.

At the bottom of the dialog box are several buttons: '< Back' (disabled), 'Next >' (highlighted in blue), 'Finish' (disabled), 'Cancel' (disabled), and 'Help'.

Step 3: Enter the additional Information and click on Finish.

New Case Information

Steps

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

Optional Information

Case

Number: 02

Examiner

Name: Neha

Phone: 855*****

Email: np@gmail.com

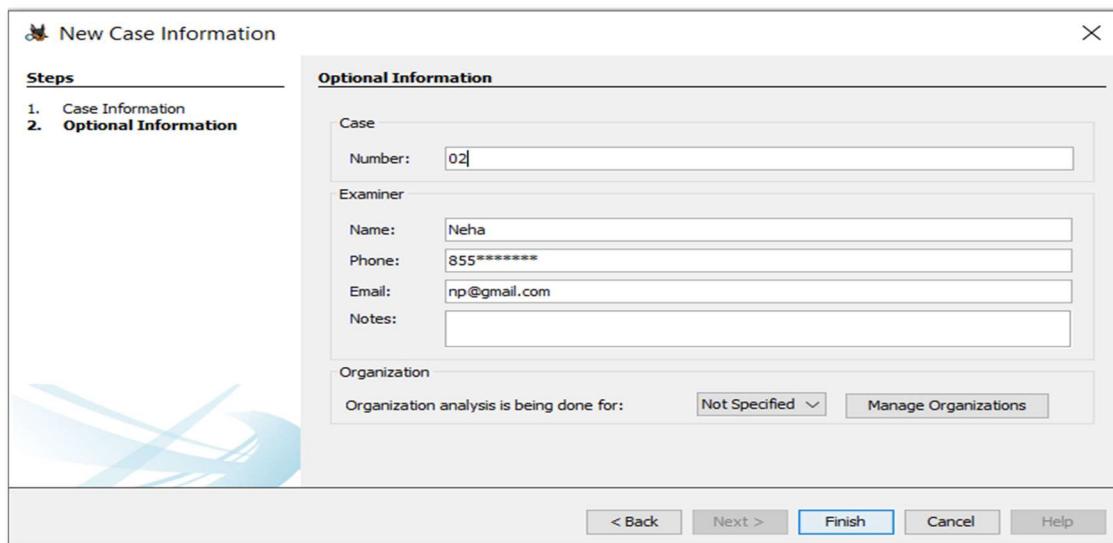
Notes:

Organization

Organization analysis is being done for: Not Specified

Manage Organizations

< Back Next > Finish Cancel Help



Step 4: Now Select Source Type as Local disk and Select Local disk form drop down list and click on Next.

Add Data Source

Steps

1. Select Host
2. **Select Data Source Type**
3. Select Data Source
4. Configure Ingest
5. Add Data Source

Select Data Source Type

Disk Image or VM File (selected)

Local Disk

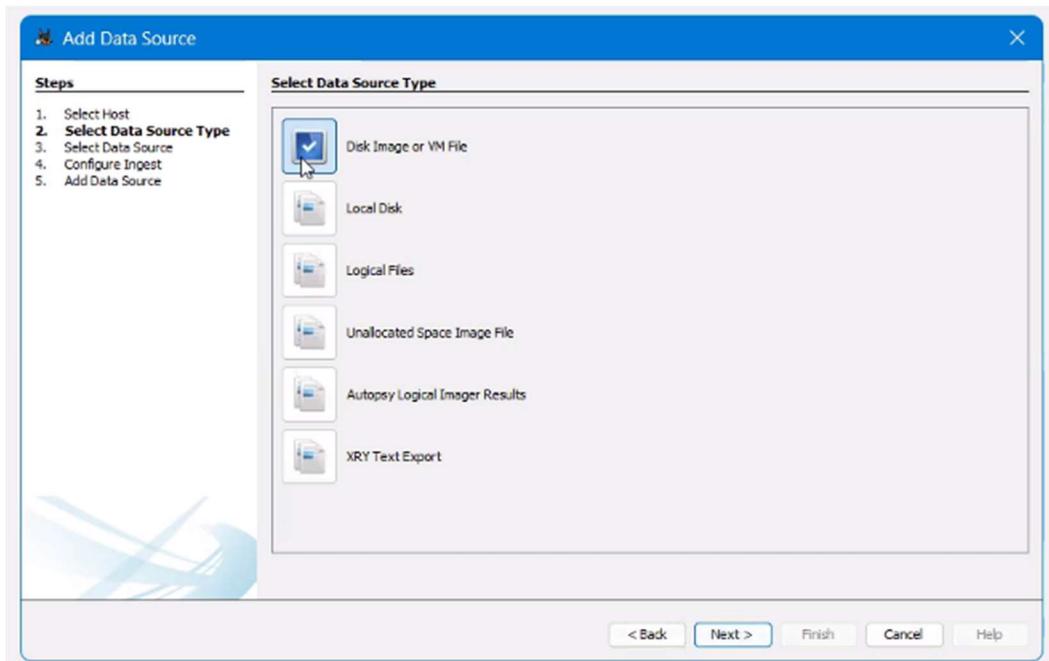
Logical Files

Unallocated Space Image File

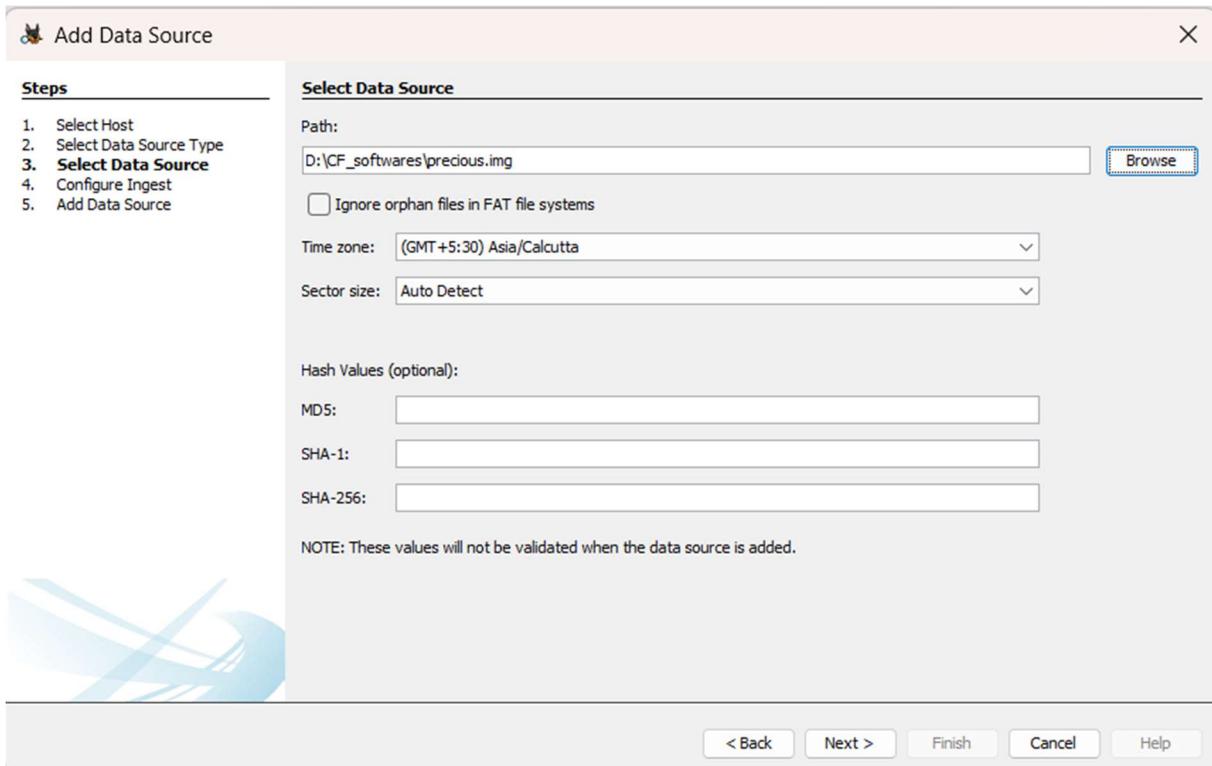
Autopsy Logical Imager Results

XRY Text Export

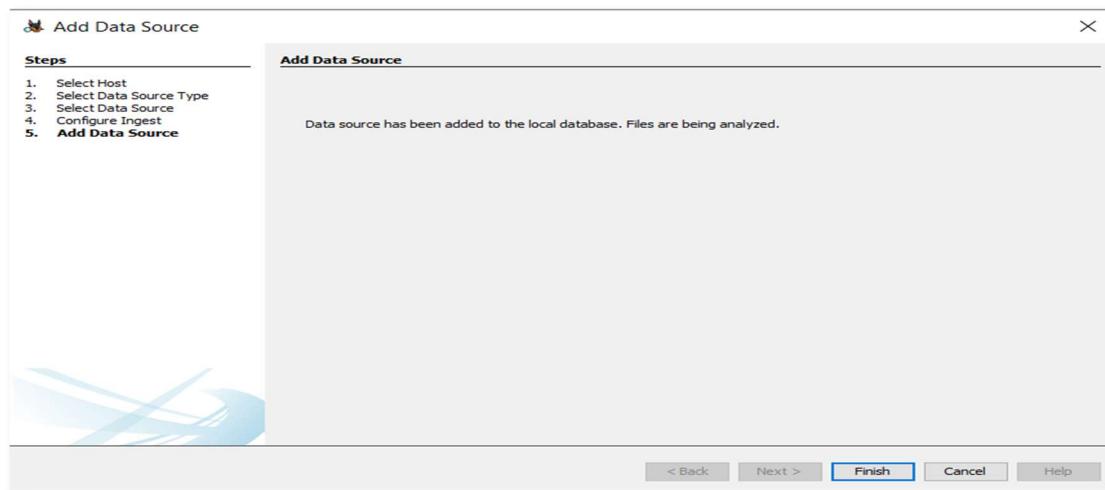
< Back Next > Finish Cancel Help



Step 5: add precious.img



Step 6: Now click On Finish.



Step 7: Now Autopsy window will appear and it will analyzing the disk that we have selected.

Step 8: All files will appear in table tab select any file to see the data.

Step 9: Expand the tree from left side panel to view the document files.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
x Thumbs.db				2004-12-31 04:43:38 IST	2004-12-31 04:43:38 IST	2004-12-31 11:10:07 IST	2005-01-02 00:18:40 IST	9216	Unallocated	Unallocated	Unknown	[img:precious]
x 0601_top03[1].jpg				2005-12-31 00:34:04 IST	2004-12-31 22:23:37 IST	2004-12-31 10:54:51 IST	2005-01-02 00:19:17 IST	5069	Unallocated	Unallocated	Unknown	[img:precious]
x 0601_search[1].jpg				2005-12-31 00:34:04 IST	2004-12-31 22:23:37 IST	2004-12-31 10:54:59 IST	2005-01-02 00:19:17 IST	1911	Unallocated	Unallocated	Unknown	[img:precious]
x __4x15[1].gif				2005-01-07 03:35:58 IST	2004-12-31 11:03:54 IST	2004-12-31 11:03:54 IST	2005-01-02 00:19:07 IST	76	Unallocated	Unallocated	Unknown	[img:precious]
x yellow[1].g				2004-12-31 04:39:26 IST	2004-12-31 22:22:40 IST	2004-12-31 09:07:16 IST	2005-01-02 00:21:21 IST	44	Unallocated	Unallocated	Unknown	[img:precious]
x yellow[2].g				2004-12-31 04:41:54 IST	2004-12-31 22:22:45 IST	2004-12-31 11:03:32 IST	2005-01-02 00:19:17 IST	44	Unallocated	Unallocated	Unknown	[img:precious]
x i1[1].g				2005-01-07 03:57:57 IST	2004-12-31 22:22:49 IST	2004-12-31 11:04:09 IST	2005-01-02 00:19:07 IST	43	Unallocated	Unallocated	Unknown	[img:precious]
x 2.jpg				2000-09-00 00:00:00	2000-09-00 00:00:00	2000-09-00 00:00:00	2000-09-00 00:00:00	0	Unallocated	Unallocated	Unknown	[img:precious]
x 1989FF18D01				2000-09-00 00:00:00	2000-09-00 00:00:00	2000-09-00 00:00:00	2000-09-00 00:00:00	0	Unallocated	Unallocated	Unknown	[img:precious]
x 24F79C0D01				2000-09-00 00:00:00	2000-09-00 00:00:00	2000-09-00 00:00:00	2000-09-00 00:00:00	0	Unallocated	Unallocated	Unknown	[img:precious]
x A38E630B01				2000-09-00 00:00:00	2000-09-00 00:00:00	2000-09-00 00:00:00	2000-09-00 00:00:00	0	Unallocated	Unallocated	Unknown	[img:precious]
x 4D72AE5601				2000-09-00 00:00:00	2000-09-00 00:00:00	2000-09-00 00:00:00	2000-09-00 00:00:00	0	Unallocated	Unallocated	Unknown	[img:precious]
x 5842775001				2000-09-00 00:00:00	2000-09-00 00:00:00	2000-09-00 00:00:00	2000-09-00 00:00:00	0	Unallocated	Unallocated	Unknown	[img:precious]
x 629#A3A4B01				2000-09-00 00:00:00	2000-09-00 00:00:00	2000-09-00 00:00:00	2000-09-00 00:00:00	0	Unallocated	Unallocated	Unknown	[img:precious]
x 780568A401				2000-09-00 00:00:00	2000-09-00 00:00:00	2000-09-00 00:00:00	2000-09-00 00:00:00	0	Unallocated	Unallocated	Unknown	[img:precious]
x 8AA1BC2201				2000-09-00 00:00:00	2000-09-00 00:00:00	2000-09-00 00:00:00	2000-09-00 00:00:00	0	Unallocated	Unallocated	Unknown	[img:precious]
x 8A1D0F9D01				2000-09-00 00:00:00	2000-09-00 00:00:00	2000-09-00 00:00:00	2000-09-00 00:00:00	0	Unallocated	Unallocated	Unknown	[img:precious]
x A58B2723001				2000-09-00 00:00:00	2000-09-00 00:00:00	2000-09-00 00:00:00	2000-09-00 00:00:00	0	Unallocated	Unallocated	Unknown	[img:precious]
x 897C0342001				2000-09-00 00:00:00	2000-09-00 00:00:00	2000-09-00 00:00:00	2000-09-00 00:00:00	0	Unallocated	Unallocated	Unknown	[img:precious]
x C6991A0C0B01				2000-09-00 00:00:00	2000-09-00 00:00:00	2000-09-00 00:00:00	2000-09-00 00:00:00	0	Unallocated	Unallocated	Unknown	[img:precious]
x D28A8E9F001				2000-09-00 00:00:00	2000-09-00 00:00:00	2000-09-00 00:00:00	2000-09-00 00:00:00	0	Unallocated	Unallocated	Unknown	[img:precious]
x DCC98A8501				2000-09-00 00:00:00	2000-09-00 00:00:00	2000-09-00 00:00:00	2000-09-00 00:00:00	0	Unallocated	Unallocated	Unknown	[img:precious]

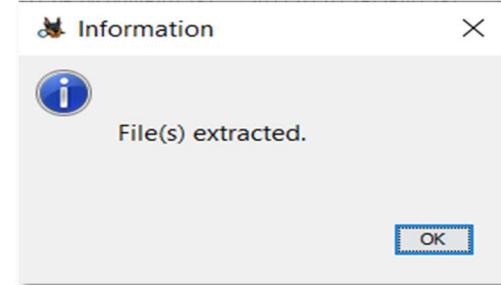
Step 10: To recover the file, go to Deleted Files > File System , here select any file and right click on it than select Extract Files option.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
x Thumbs.db				2004-12-31 04:43:38 IST	2004-12-31 04:43:38 IST	2004-12-31 11:10:07 IST	2005-01-02 00:18:40 IST	9216	Unallocated	Unallocated	Unknown	[img:precious]
x 0601_top03[1].jpg				2005-12-31 00:34:04 IST	2004-12-31 22:23:37 IST	2004-12-31 10:54:51 IST	2005-01-02 00:19:17 IST	5069	Unallocated	Unallocated	Unknown	[img:precious]
x 0601_search[1].jpg				2005-12-31 00:34:04 IST	2004-12-31 22:23:37 IST	2004-12-31 10:54:59 IST	2005-01-02 00:19:17 IST	1911	Unallocated	Unallocated	Unknown	[img:precious]
x __4x15[1].gif				2005-01-07 03:35:58 IST	2004-12-31 11:03:54 IST	2004-12-31 11:03:54 IST	2005-01-02 00:19:07 IST	76	Unallocated	Unallocated	Unknown	[img:precious]
x yellow[1].g				2004-12-31 04:41:54 IST	2004-12-31 22:22:45 IST	2004-12-31 11:03:32 IST	2005-01-02 00:19:17 IST	44	Unallocated	Unallocated	Unknown	[img:precious]
x yellow[2].g				2005-01-07 03:57:57 IST	2004-12-31 22:22:49 IST	2004-12-31 11:04:09 IST	2005-01-02 00:19:07 IST	43	Unallocated	Unallocated	Unknown	[img:precious]
x 2.jpg				2000-09-00 00:00:00	2000-09-00 00:00:00	2000-09-00 00:00:00	2000-09-00 00:00:00	0	Unallocated	Unallocated	Unknown	[img:precious]
x 1989FF18D01				2000-09-00 00:00:00	2000-09-00 00:00:00	2000-09-00 00:00:00	2000-09-00 00:00:00	0	Unallocated	Unallocated	Unknown	[img:precious]
x 24F79C0D01				2000-09-00 00:00:00	2000-09-00 00:00:00	2000-09-00 00:00:00	2000-09-00 00:00:00	0	Unallocated	Unallocated	Unknown	[img:precious]
x A38E630B01				2000-09-00 00:00:00	2000-09-00 00:00:00	2000-09-00 00:00:00	2000-09-00 00:00:00	0	Unallocated	Unallocated	Unknown	[img:precious]
x 629#A3A4B01				2000-09-00 00:00:00	2000-09-00 00:00:00	2000-09-00 00:00:00	2000-09-00 00:00:00	0	Unallocated	Unallocated	Unknown	[img:precious]
x 780568A401				2000-09-00 00:00:00	2000-09-00 00:00:00	2000-09-00 00:00:00	2000-09-00 00:00:00	0	Unallocated	Unallocated	Unknown	[img:precious]
x 8AA1BC2201				2000-09-00 00:00:00	2000-09-00 00:00:00	2000-09-00 00:00:00	2000-09-00 00:00:00	0	Unallocated	Unallocated	Unknown	[img:precious]
x 8A1D0F9D01				2000-09-00 00:00:00	2000-09-00 00:00:00	2000-09-00 00:00:00	2000-09-00 00:00:00	0	Unallocated	Unallocated	Unknown	[img:precious]
x A58B2723001				2000-09-00 00:00:00	2000-09-00 00:00:00	2000-09-00 00:00:00	2000-09-00 00:00:00	0	Unallocated	Unallocated	Unknown	[img:precious]
x 897C0342001				2000-09-00 00:00:00	2000-09-00 00:00:00	2000-09-00 00:00:00	2000-09-00 00:00:00	0	Unallocated	Unallocated	Unknown	[img:precious]
x C6991A0C0B01				2000-09-00 00:00:00	2000-09-00 00:00:00	2000-09-00 00:00:00	2000-09-00 00:00:00	0	Unallocated	Unallocated	Unknown	[img:precious]
x D28A8E9F001				2000-09-00 00:00:00	2000-09-00 00:00:00	2000-09-00 00:00:00	2000-09-00 00:00:00	0	Unallocated	Unallocated	Unknown	[img:precious]
x DCC98A8501				2000-09-00 00:00:00	2000-09-00 00:00:00	2000-09-00 00:00:00	2000-09-00 00:00:00	0	Unallocated	Unallocated	Unknown	[img:precious]

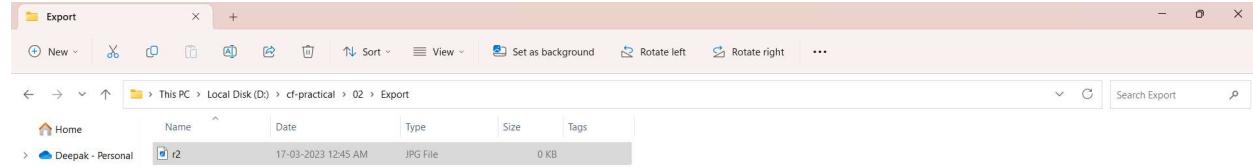
Step 11: By default Export folder is choose to save the recovered file.

The screenshot shows the Autopsy interface with the 'File System' tab selected. The left sidebar shows various data sources, including 'img_precious.img_1.Hist' and 'File Virus'. The main area displays a table of recovered files with columns for Name, S, C, O, Modified Time, Change Time, Access Time, Created Time, Size, Flags(Dir), Flags(Meta), Known, and Location. A 'Save' dialog is overlaid on the interface, prompting to save the file to the 'Export' folder, with 'Desktop' selected as the save location.

Step 12 : Now Click on Ok.



Step 13: Now go to the Export Folder to view Recovered file.



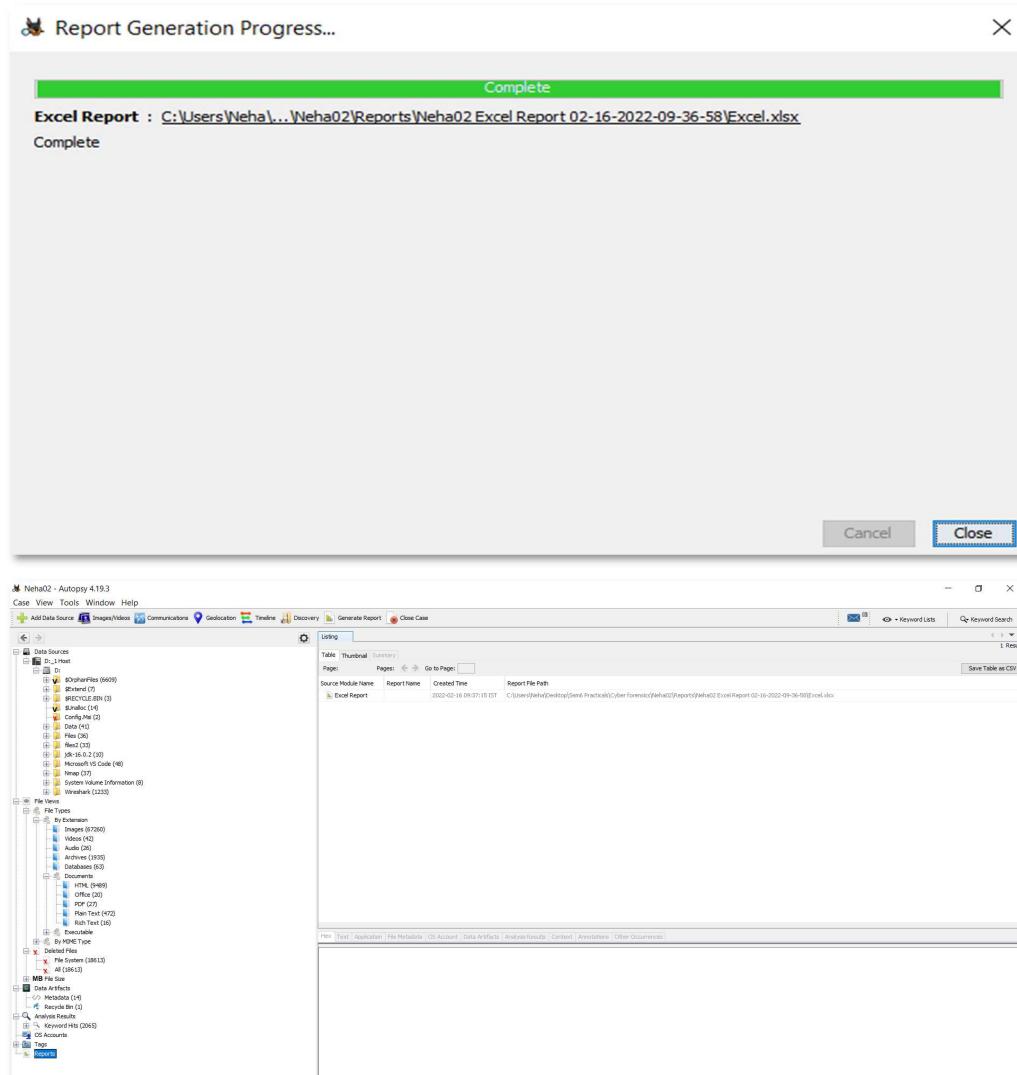
Step 14: Click on Generate Report from autopsy window and Select the Excel format and click on next.

The screenshot shows the autopsy tool's main interface. The menu bar at the top includes 'Case', 'View', 'Tools', 'Window', and 'Help'. The 'Tools' menu is open, and 'Generate Report' is highlighted. The main pane displays a table titled 'File System' with columns for Name, S, C, O, Modified Time, Change Time, Access Time, Created Time, Size, Flag(DR), Flag(Meta), Known, and Location. The table lists numerous files and folders, many of which are marked as 'Unlocated' or have specific paths like 'Img_D:\[REDACTED]'. A status bar at the bottom right indicates '10000 Results'.

The screenshot shows the 'Generate Report' configuration dialog. At the top, it says 'Select and Configure Report Modules'. Below this, there is a section titled 'Report Modules:' with a list of options. The 'Excel Report' option is selected, indicated by a checked radio button. To the right of this list is a text area containing the message: 'A report about results and tagged items in Excel (XLS) format.' Below this text area is another message: 'This report will be configured on the next screen.' At the bottom of the dialog are several buttons: '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'.

- HTML Report
- Excel Report
- Files - Text
- Data Source Summary Report
- Save Tagged Hashes
- Extract Unique Words
- TSK Body File
- Google Earth KML
- CASE-UCO
- Portable Case

Step 15: Now Report is Generated So click on close Button .we can see the Report on Report Node.



Step 17: Now open the Report folder and Open Excel File.

	A1		X	✓	fx	Summary
1	Summary					
2						
3	Case Name:					Neha02
4	Case Number:					02
5	Number of data sources in case:					1
6	Examiner:					Neha
7						

Practical 7

AIM: Email Forensics –

1. Mail Service Providers

Step 1 : Find MX Record.

MX records points a domain's incoming email provider responsible for processing those messages.

- a) Go to <http://www.misk.com/tools/> # dns
- b) Enter your domain name.
- c) Press Enter on your keyboard. A list of all dns records for the name will appear.
- d) Copy the Ip address of A

The screenshot shows the Misk DNS lookup interface. At the top, there is a navigation bar with the Misk logo, a search bar containing 'google.com', and links for 'Cart - Empty', 'Support', 'Control Panel', and 'LOGIN'. Below the search bar, it displays 'YOUR IP ADDRESS' as 103.87.28.158. The main content area has tabs for 'DNS LOOKUP' (which is selected), 'WHOIS', and 'TRACEROUTE'. Under the 'DNS LOOKUP' tab, the results for 'google.com' are listed. The results table includes columns for 'Time' (e.g., 5 minutes, 1 hour), 'Type' (e.g., A, AAAA, MX, TXT), and 'Value'. The results are as follows:

Time	Type	Value
5 minutes	A	142.251.45.14
5 minutes	AAAA	2607:fbb0:4004:83e::200e
10 minutes	MX	aspmx.l.google.com (10)
10 minutes	MX	alt1.aspmx.l.google.com (20)
10 minutes	MX	alt2.aspmx.l.google.com (30)
10 minutes	MX	alt3.aspmx.l.google.com (40)
10 minutes	MX	alt4.aspmx.l.google.com (50)
1 hour	TXT	google-site-verification=TV9-DBe4R80X4v0M4U_bd_J9cpOJM0nikft0jAgjmsQ
1 hour	TXT	facebook-domain-verification=22rm551cu4k0ab0bxsw536tlds4h95
1 hour	TXT	docsign=1b0a6754-49b1-4db5-8540-d2c12664b289
1 hour	TXT	google-site-verification=wD8N71JTNTkezJ49svvVVV48f8_9xveREV4oB-0Hf5o
1 hour	TXT	v=spf1 include:_spf.google.com ~all
1 hour	TXT	apple-domain-verification=30afflBcvSuDV2PLX
1 hour	TXT	MS=E4A68B9AB2BB9670BCE15412F62916164C0B20BB
1 hour	TXT	docsign=05958488-4752-4ef2-95eb-aa7ba8a3bd0e
1 hour	TXT	globalsign-smime-dv=CDYX+XFHUw2wml6/Gb8+59BsH31KzUr6c1l2BPvqKX8=

Below the results, there is a section for 'DMARC (p=reject)' which lists authoritative nameservers: ns2.google.com, ns1.google.com, ns3.google.com, and ns4.google.com.

2. IP WHOIS:

- a) Go the same site select whois and enter the copied hostname.
- b) Press enter on your keyboard.
- c) The IP address whois record will appear.

The screenshot shows the MISK web interface. At the top, there is a navigation bar with links for Domains, Essentials, Email, Support, Control Panel, and a LOGIN button. On the right side of the header, it says "Cart - Empty" and "YOUR IP ADDRESS 103.87.28.158". Below the header, there is a search bar containing the IP address "142.251.45.14". A message below the search bar says "Enter a domain name to view its whois record (ownership, registrar, expiration, etc.). Enter an ip address to view its internet service provider." There are three buttons at the bottom of this section: "DNS LOOKUP", "WHOIS" (which is highlighted in blue), and "TRACEROUTE". The main content area displays the WHOIS response for the IP address 142.251.45.14. The response includes a copyright notice from ARIN and detailed network information:

```
NetRange: 142.250.0.0 - 142.251.255.255
CIDR: 142.250.0.0/15
NetName: GOOGLE
NetHandle: NET-142-250-0-0-1
Parent: NET142 (NET-142-0-0-0-0)
NetType: Direct Allocation
OriginAS: AS15169
Organization: Google LLC (GOGL)
RegDate: 2012-05-24
Updated: 2012-05-24
Ref: https://rdap.arin.net/registry/ip/142.250.0.0
```

3. Email protocols –

- a) On your computer, open Gmail.
- b) In the top right corner, click settings.
- c) Click on forwarding and POP/IMAP tab
- d) Now you can see that which protocol your email is using. Here it is using POP and IMAPs

Settings

General Labels Inbox Accounts and Import Filters and Blocked Addresses **Forwarding and POP/IMAP** Add-ons Chat and Meet Advanced Offline Themes

Forwarding: [Learn more](#) [Add a forwarding address](#)

Tip: You can also forward only some of your mail by creating a filter!

POP download: [Learn more](#)

1. Status: **POP is disabled**
 Enable POP for all mail
 Enable POP for mail that arrives from now on

2. When messages are accessed with POP: **keep Gmail's copy in the Inbox**

3. Configure your email client (e.g. Outlook, Eudora, Netscape Mail)
[Configuration Instructions](#)

IMAP access: (access Gmail from other clients using IMAP) [Learn more](#)

Status: **IMAP is enabled**
 Enable IMAP
 Disable IMAP

When I mark a message in IMAP as deleted:
 Auto-Expunge on - Immediately update the server. (default)
 Auto-Expunge off - Wait for the client to update the server.

When a message is marked as deleted and expunged from the last visible IMAP folder:
 Archive the message (default)
 Move the message to the Trash
 Immediately delete the message forever

Folder size limits
 Do not limit the number of messages in an IMAP folder (default)
 Limit IMAP folders to contain no more than this many messages: **1,000**

Configure your email client (e.g. Outlook, Thunderbird, iPhone)
[Configuration Instructions](#)

[Save Changes](#) [Cancel](#)

4. Analyzing email headers.

- Open the email you want to analyze the header for.
- Next to reply, click on the three dots.
- Click show original.
- Click on copy to clipboard.

Message ID	<2023031110401.30806958.107003@sailthru.com>
Created on:	11 March 2023 at 21:34 (Delivered after 2 seconds)
From:	TechCrunch <newsletter@techcrunch.com> Using sailthru.com
To:	deepakpadhi90058@gmail.com
Subject:	Startups Weekly - Silicon Valley Bank's collapse is a human story
SPF:	PASS with IP 163.47.180.40 Learn more
DKIM:	'PASS' with domain techcrunch.com Learn more
DMARC:	'PASS' Learn more

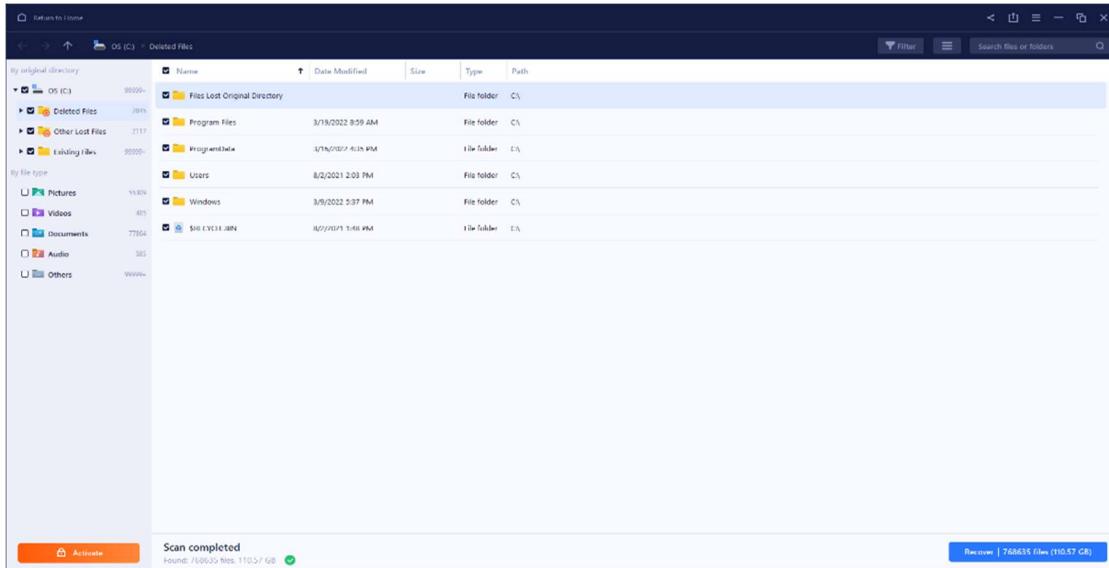
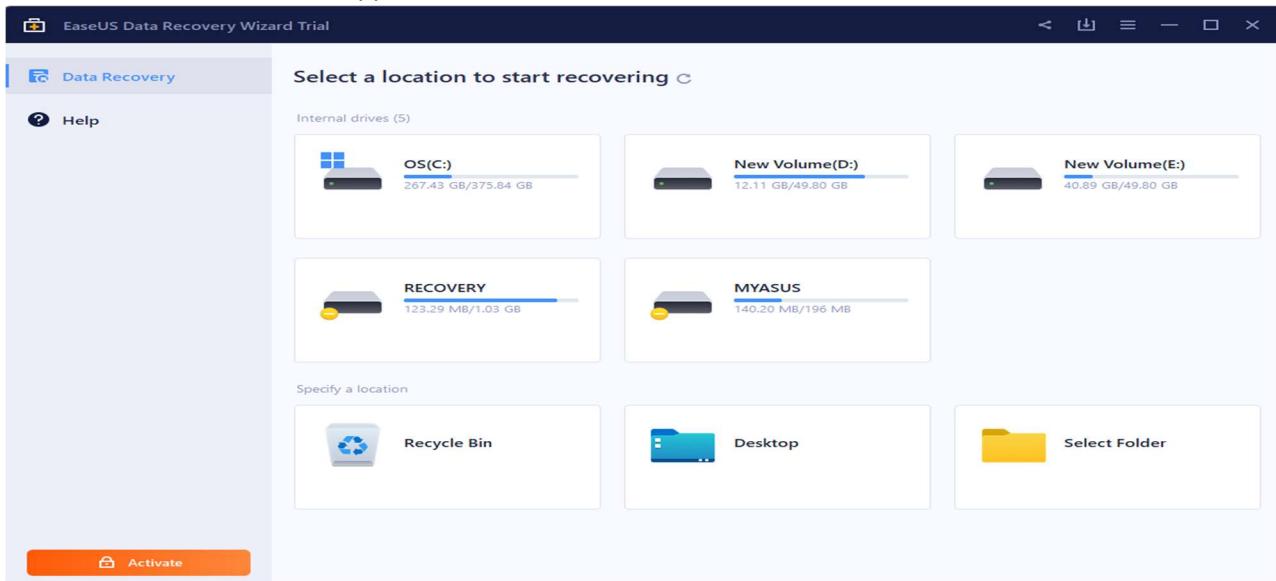
Download original Copy to clipboard

- Open the message header tool. (<http://toolbox.googleapps.com/messageheader>)
- Paste the header the paste box.
- Then click on analyse the above header.

MessageId	2023031110401.30806958.107003@sailthru.com
Created at:	3/11/2023, 9:34:01 PM GMT+5:30 (Delivered after 3 sec)
From:	TechCrunch <newsletter@techcrunch.com> Using sailthru.com
To:	deepakpadhi90058@gmail.com
Subject:	Startups Weekly - Silicon Valley Bank's collapse is a human story
SPF:	pass with IP 163.47.180.40 Learn more
DKIM:	pass with domain pmta.sailthru.com Learn more
DMARC:	pass Learn more

5. Recovering emails –

1. To recover the emails here we are using EaseUS recovery tools.
Run the email recovery software.
 2. Click on scan to let the software scan and find the lost emails.
- Step 2:
1. Find the lost emails .
 2. Deleted files: If you accidentally delete the email files, they will appear.
 3. Lost files: All lost files will appear here.



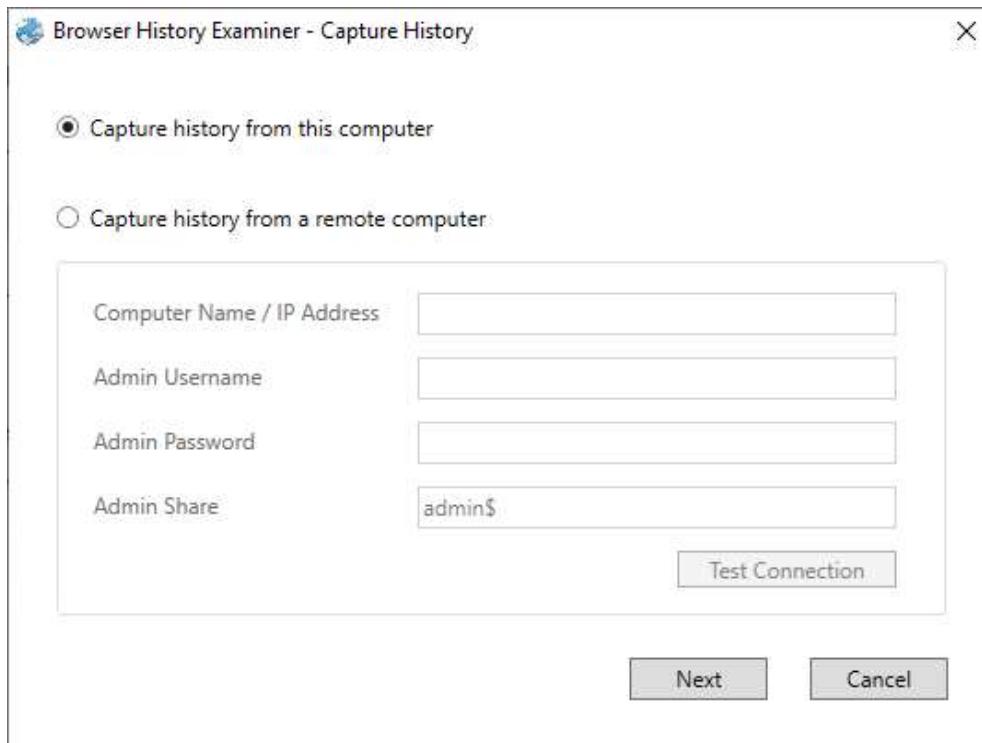
Practical 8

Aim: Web Browser Forensics .

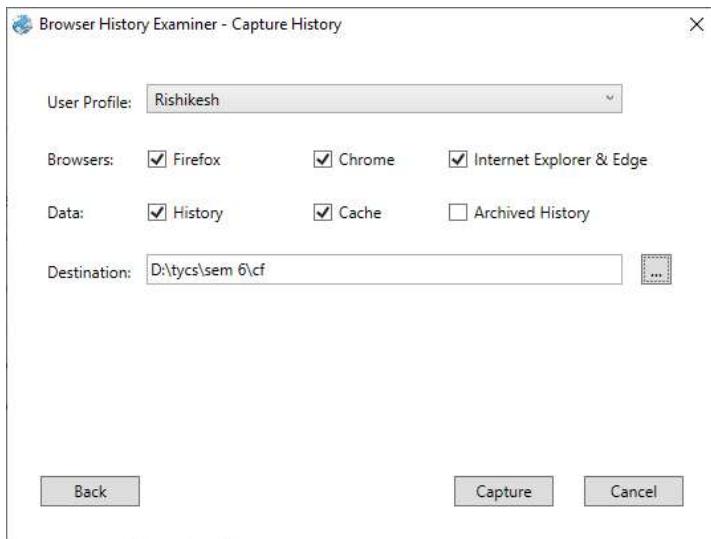
- Web Browser working
- Forensics activities on browser
- Cache / Cookies analysis
- Last Internet activity

Steps:

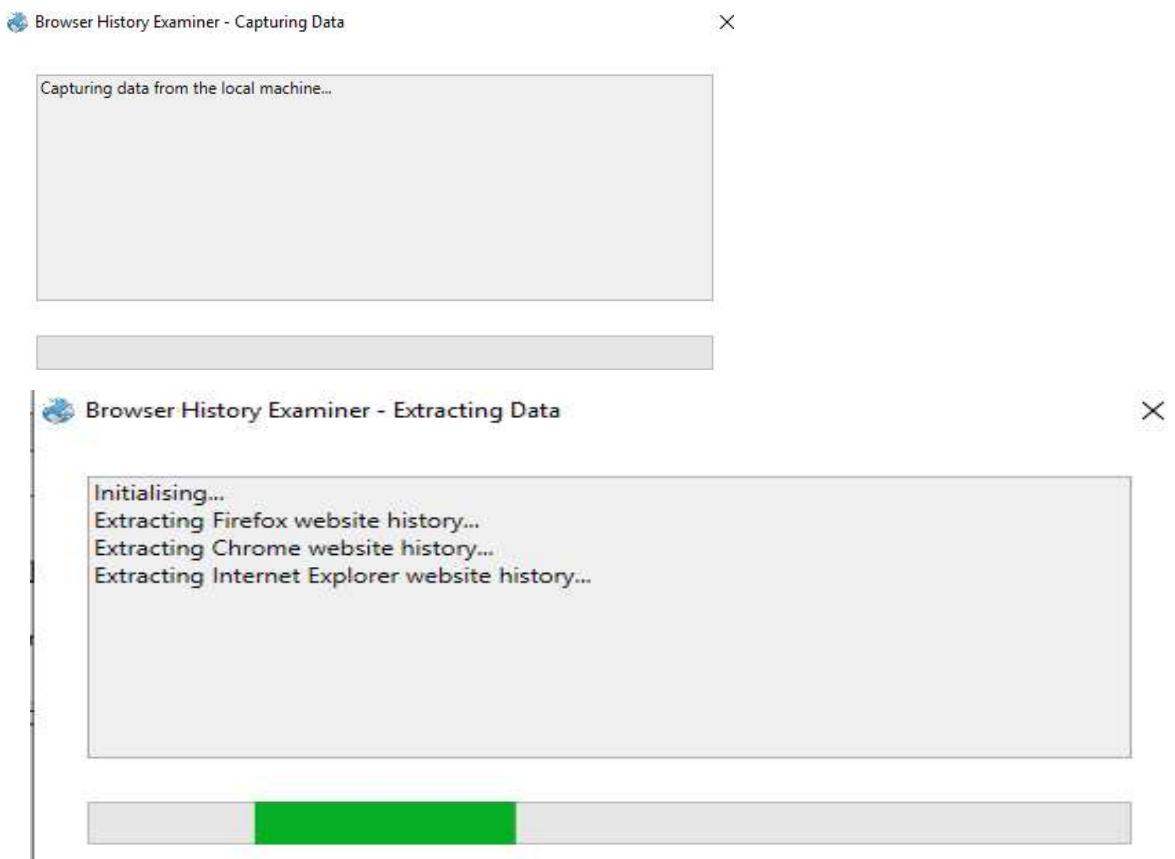
1. Download and install BrowserHistoryExaminer.
2. Open BrowserHistoryExaminer.
3. Click on continue trail
4. Click on Capture history
5. Select the default.



Enter the destination path to capture the data.



Follow the onscreen directions
The History is been extracting.



The data has been retrieved.

Browser History Examiner - Trial Mode

Artefact Records

	Date Visited	Title	URL	Visit Type	Visit Count
18-03-2019 03:42:10			file:///D:/cf.docx		
18-03-2019 03:26:21			file:///D:/tycs/se		
18-03-2019 03:25:29			file:///D:/tycs/se		
18-03-2019 03:25:28			file:///D:/tycs/se		
18-03-2019 03:21:24			file:///D:/cc.pdf		
18-03-2019 03:21:24			file:///D:/cc.pdf		

Viewing 25/25 records | < 1 of 1 pages > Page size 50

Detailed View **Summary View**

Website Visit Count - 17-03-2019 to 18-03-2019

Time zone: UTC, DST Enabled Date format: dd/mm/yyyy

On the left panel click on bookmarks.

Browser History Examiner - Trial Mode

Artefact Records

	Date Added	Last Modified	Title	URL	Web Browser
17-03-2019 09:03:01	17-03-2019 09:03:01	Getting	https://	Firefox	
17-03-2019 09:03:01	17-03-2019 09:03:01	Help ar	https://	Firefox	
17-03-2019 09:03:01	17-03-2019 09:03:01	Custom	https://	Firefox	
17-03-2019 09:03:01	17-03-2019 09:03:01	Get Inv	https://	Firefox	
17-03-2019 09:03:01	17-03-2019 09:03:01	About	https://	Firefox	
	14-03-2019 05:01:05		New Ta	Chrome	
	22-01-2019 06:40:50		Downl	https://	Chrome
			Bing	http://	Internet Explorer

Viewing 8/8 records | < 1 of 1 pages > Page size 50

Filter by keyword **Advanced**

Filter by date From: Select a date 15 To: Select a date 15

Filter by time From: Select a time To: Select a time

Filter by web browser All

Time zone: UTC, DST Enabled Date format: dd/mm/yyyy

On the left panel click on cached files.

The screenshot shows the 'Browser History Examiner - Trial Mode' application window. The left sidebar lists various artifacts with their counts: Bookmarks (8), Cached Files (4615), Cached Images (177), Cached Web Pages (36), Cookies (1566), Downloads (80), Email Addresses (30), Favicons (1790), Form History (31), Logins (3), Searches (1184), Session Tabs (62), Thumbnails (12), and Website Visits (2688). The 'Cached Files' tab is selected, displaying a table with columns: Last Fetched, Content Type, UI, Fetch Count, File Size (Bytes), and Web. The table contains several rows of data, with the first row showing a file size of 18820976 bytes. On the right side of the window, there are four filter panels: 'Filter by keyword' (with a search input and 'Advanced' button), 'Filter by date' (with 'From' and 'To' date pickers), 'Filter by time' (with 'From' and 'To' time pickers), and 'Filter by web browser' (with a dropdown menu set to 'All'). At the bottom, status information includes 'www.foxtonforensics.com', 'Time zone: UTC, DST Enabled', and 'Date format: dd/mm/yyyy'.

On the left panel click on cached images.

The screenshot shows the 'Browser History Examiner - Trial Mode' application window. The left sidebar lists various artifacts with their counts: Bookmarks (8), Cached Files (4615), Cached Images (177), Cached Web Pages (36), Cookies (1566), Downloads (80), Email Addresses (30), Favicons (1790), Form History (31), Logins (3), Searches (1184), Session Tabs (62), Thumbnails (12), and Website Visits (2688). The 'Cached Images' tab is selected, displaying a table with columns: Last Fetched, Content Type, UI, Fetch Count, File Size (Bytes), and Web. The table contains several rows of data, with the first row showing a file size of 1150328 bytes. Below the table, five thumbnail images are displayed: 'Introduction to Information Technology', 'SOFTWARE ENGINEERING', 'XAMPP Apache + MySQL + PHP + Perl', 'Visual Basic 2015', and 'Microsoft Office Excel 2013'. On the right side of the window, there are four filter panels: 'Filter by keyword' (with a search input and 'Advanced' button), 'Filter by date' (with 'From' and 'To' date pickers), 'Filter by time' (with 'From' and 'To' time pickers), and 'Filter by web browser' (with a dropdown menu set to 'All'). At the bottom, status information includes 'www.foxtonforensics.com', 'Time zone: UTC, DST Enabled', and 'Date format: dd/mm/yyyy'.

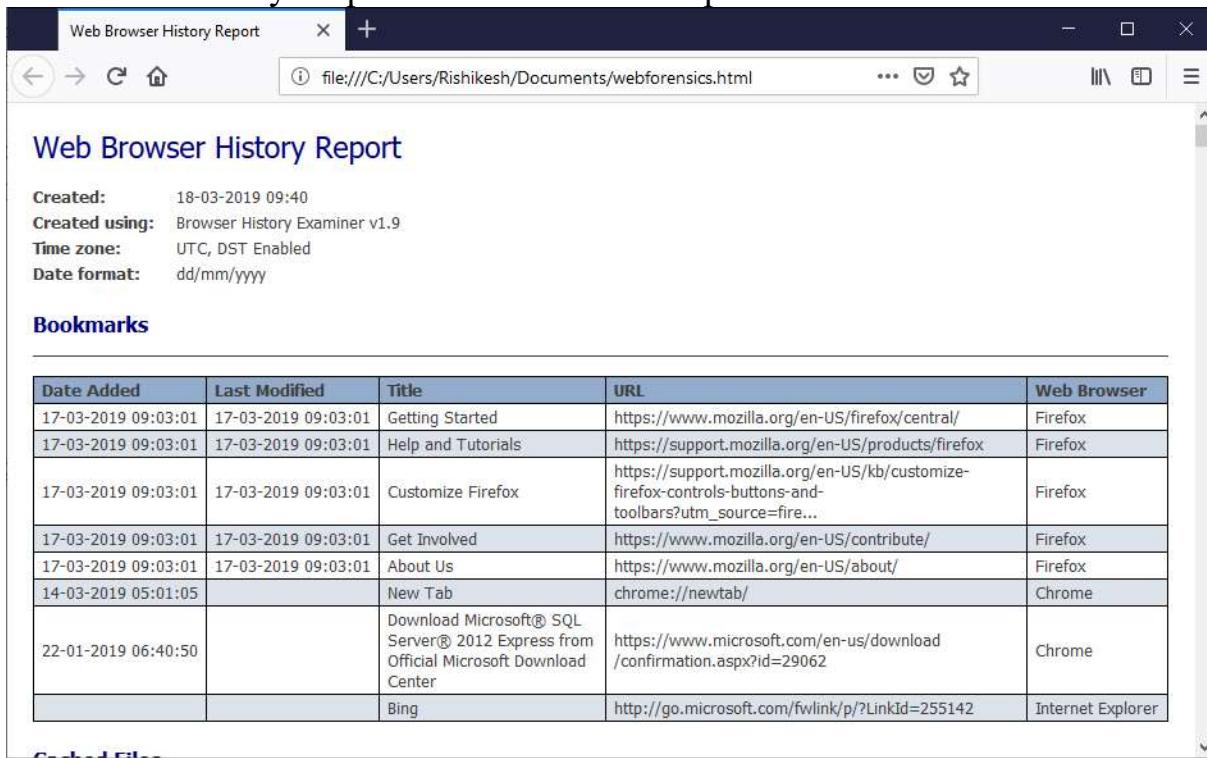
On the left panel click on cookies.

The screenshot shows the 'Report Preview' tab selected in the top navigation bar. The main pane displays a table of cookie data with columns: Date Created, UI, Last Accessed, Date Expires, N, Cr, and W. The table lists 1566 cookies. The left sidebar shows categories like Bookmarks, Cached Files, Cached Images, Cached Web Pages, Cookies, Downloads, Email Addresses, Favicons, Form History, Logins, Searches, Session Tabs, Thumbnails, and Website Visits. The 'Cookies' category is highlighted. On the right side, there are four filter panels: 'Filter by keyword', 'Filter by date' (From: Select a date [15], To: Select a date [15]), 'Filter by time' (From: Select a time [dropdown], To: Select a time [dropdown]), and 'Filter by web browser' (All [dropdown]). At the bottom, it says 'Viewing 25/25 records' and 'Page size 50'.

To Create Reports. Click on file > Export and save the report as html page.

The screenshot shows the 'File' menu open, with 'Export' selected. Under 'Export', there are options: Export to Excel, Export to HTML (which is highlighted), Export to CSV, Export to XML, Export to Concordance Load File, and Downloads. The left sidebar shows the same categories as the previous screenshot. On the right, the filter panels are identical to the first screenshot. At the bottom, it says 'Viewing 8/8 records' and 'Page size 50'.

Save the file into your preferred location and open it



The screenshot shows a web browser window titled "Web Browser History Report". The address bar displays the URL "file:///C:/Users/Rishikesh/Documents/webforensics.html". The main content area is titled "Web Browser History Report" and contains the following information:

Created: 18-03-2019 09:40
Created using: Browser History Examiner v1.9
Time zone: UTC, DST Enabled
Date format: dd/mm/yyyy

Bookmarks

Date Added	Last Modified	Title	URL	Web Browser
17-03-2019 09:03:01	17-03-2019 09:03:01	Getting Started	https://www.mozilla.org/en-US/firefox/central/	Firefox
17-03-2019 09:03:01	17-03-2019 09:03:01	Help and Tutorials	https://support.mozilla.org/en-US/products/firefox	Firefox
17-03-2019 09:03:01	17-03-2019 09:03:01	Customize Firefox	https://support.mozilla.org/en-US/kb/customize-firefox-controls-buttons-and-toolbars?utm_source=fire...	Firefox
17-03-2019 09:03:01	17-03-2019 09:03:01	Get Involved	https://www.mozilla.org/en-US/contribute/	Firefox
17-03-2019 09:03:01	17-03-2019 09:03:01	About Us	https://www.mozilla.org/en-US/about/	Firefox
14-03-2019 05:01:05		New Tab	chrome://newtab/	Chrome
22-01-2019 06:40:50		Download Microsoft® SQL Server® 2012 Express from Official Microsoft Download Center	https://www.microsoft.com/en-us/download/confirmation.aspx?id=29062	Chrome
		Bing	http://go.microsoft.com/fwlink/p/?LinkId=255142	Internet Explorer