

Amrita Vishwa Vidyapeetham

CYBER-FORENSICS

Sub Code: 20CYS311

Name: ARAVINDHAN.K

Roll No: CH.EN.U4CYS22001

Date: 22-12-2024

Lab Record

Questions:

1) **What is Hard Disk Forensics?**

Hard disk forensics involves the retrieval, examination, and safeguarding of data from storage media for investigative objectives. It ensures the originality of data while identifying concealed, erased, or encrypted files for legal purposes.

2) What is an Image File?

An image file digitally represents visual content, such as pictures or graphics, saved in formats like PNG or JPEG. In forensics, it can also mean a disk image, which is an exact duplicate of a storage device.

3) What is Allocated and Unallocated Space?

Allocated space stores active and accessible data, whereas unallocated space contains unused sections of a drive, often holding fragments of deleted data.

4) What is Disk Cache and Disk Mirroring?

A disk cache temporarily holds frequently used data to boost performance during read/write operations. Disk mirroring creates exact duplicates of data across multiple drives to ensure reliability and protect against data loss.

5) What is a Forensic Image?

A forensic image is an exact sector-by-sector copy of a storage device, including inactive areas and unused space, to ensure no data is altered during the investigation.

6) What is the Hash Value of a Hard Disk?

A hash value is a unique identifier created using hashing algorithms like SHA or MD5, ensuring data authenticity. Even the slightest modification changes the hash.

7) What is Shadow Volume, Shadow Copy, and Swap Disk?

Shadow volumes and shadow copies enable snapshots of files or drives for restoration. A swap disk uses disk storage to expand the system's virtual memory.

8) What Tools Can Perform Hard Disk Forensics?

Software like Autopsy, EnCase, Sleuth Kit, and FTK Imager can recover files, create drive images, and analyze digital storage for investigative work.

9) What is Exif Metadata?

Exif metadata, embedded in image files, contains details like camera settings, timestamps, and GPS data, which are valuable in investigations.

10) What are Common Disk Image Formats?

Popular disk image formats include DD (raw data), E01 (EnCase format), and AFF (Advanced Forensic Format), used for forensic purposes.

11) What is Bit-by-Bit Copying?

Bit-by-bit copying duplicates all data on a storage device, including hidden and unused areas, to ensure a complete replica.

12) What is Cloning a Disk?

Disk cloning creates a full replica of a drive, including its partitions and boot information, often for backup or forensic use.

13)What are the Latest Types of Storage Devices?

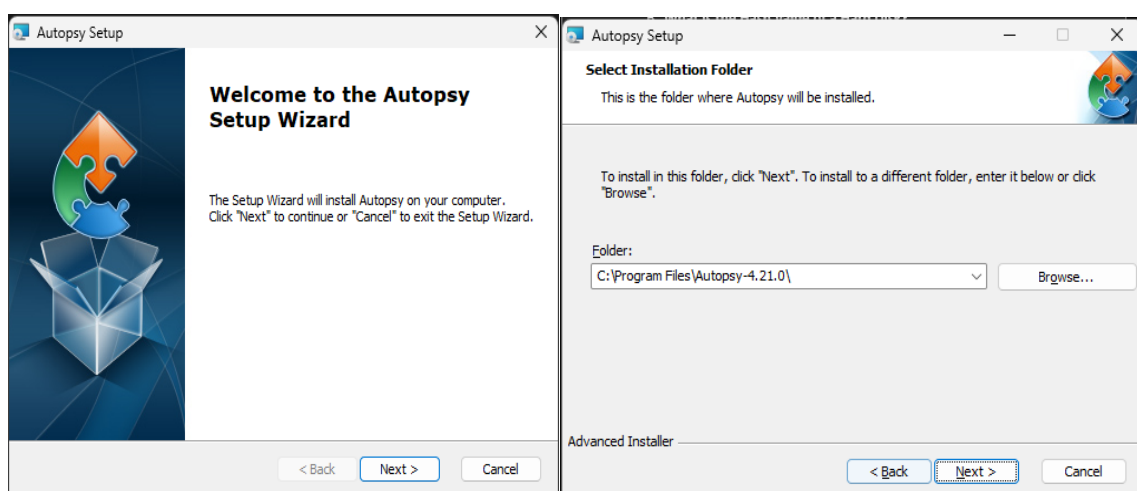
Recent storage technologies include SSDs for speed, NVMe drives for ultra-fast access, and 3D NAND for increased storage capacity.

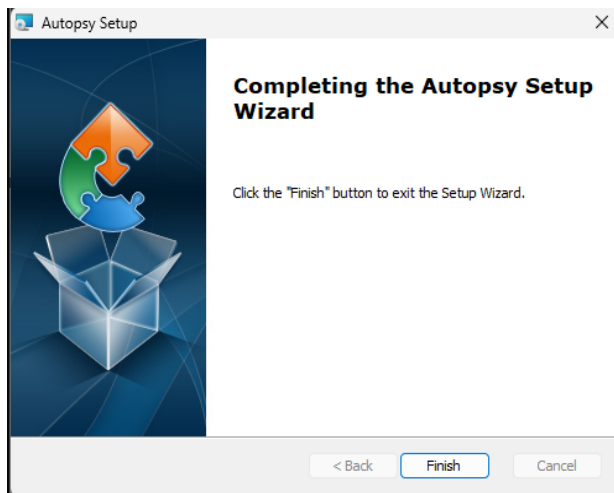
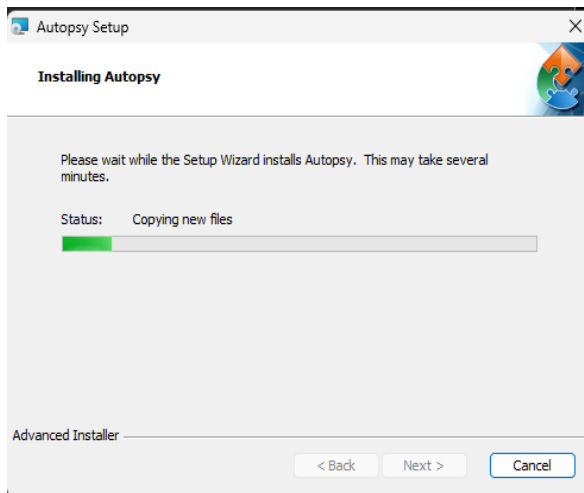
14)What is BitLocker Encryption?

BitLocker is a Windows security feature that encrypts an entire drive, ensuring data remains secure against unauthorized access through advanced encryption methods.

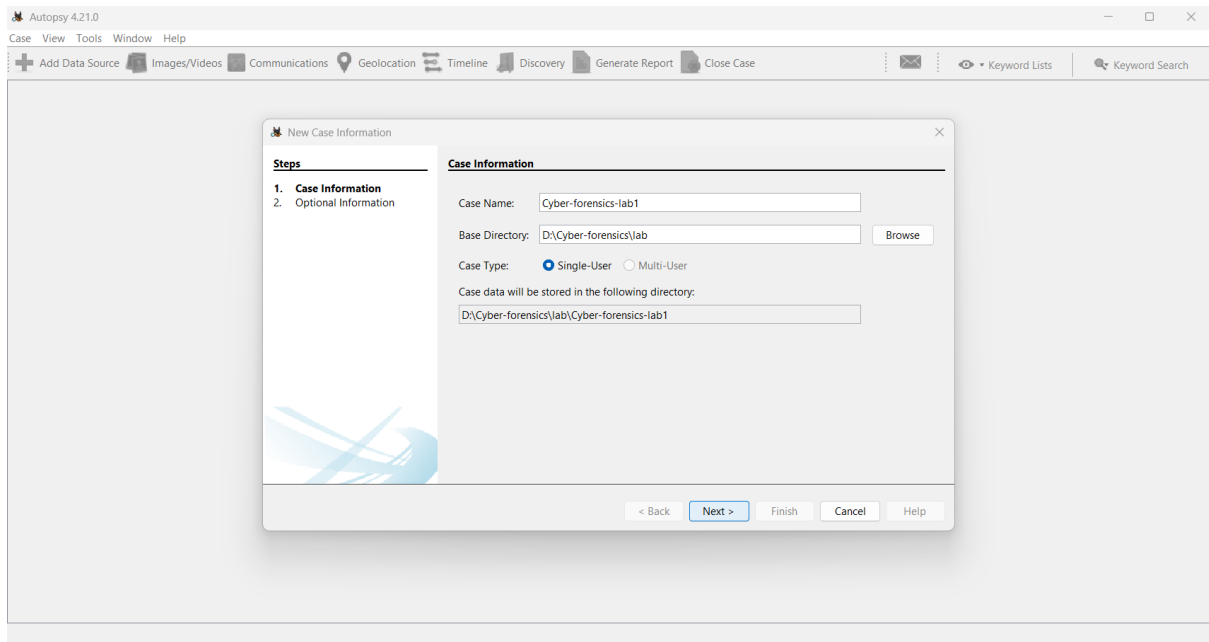
Experiment – 1 (Analysis of Data source (Local Disk) using Autopsy Screenshots

Step 1: Download Autopsy and Start





Step 2: Create a new case and add a data source like below

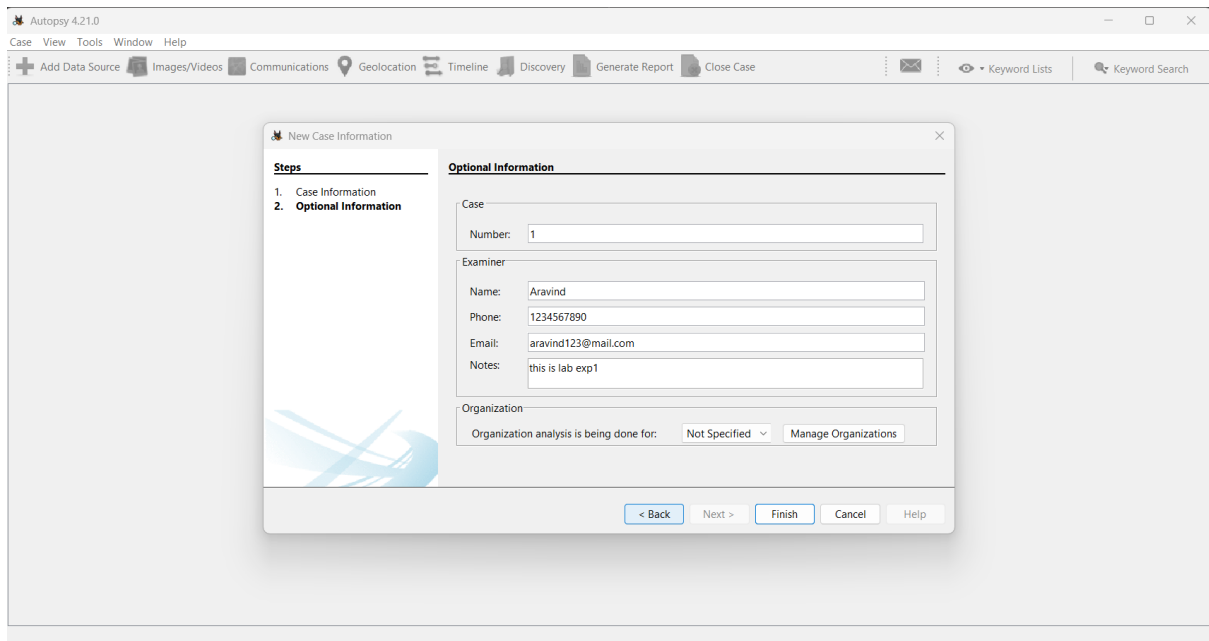


The screenshot shows the Autopsy 4.21.0 application window. The 'New Case Information' dialog box is open, displaying the 'Case Information' tab. The 'Steps' panel on the left shows '1. Case Information' and '2. Optional Information'. The 'Case Information' tab contains the following fields:

- Case Name:
- Base Directory:
- Case Type: ☒ Single-User ☐ Multi-User
- Case data will be stored in the following directory:

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

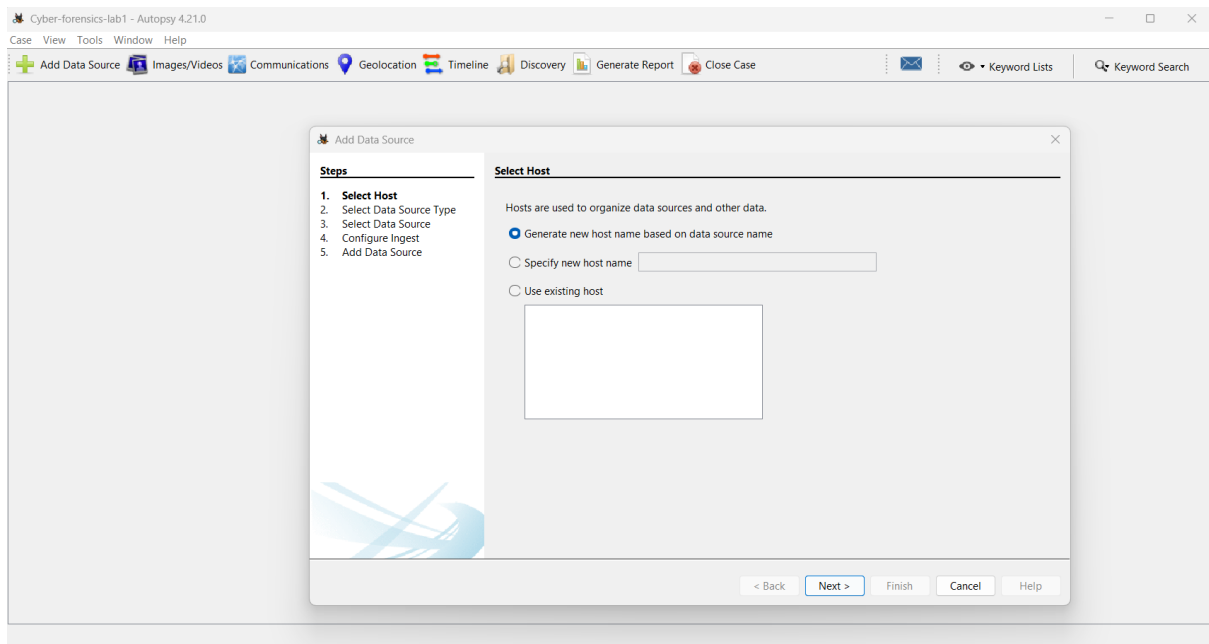
Fill the details and give finish.



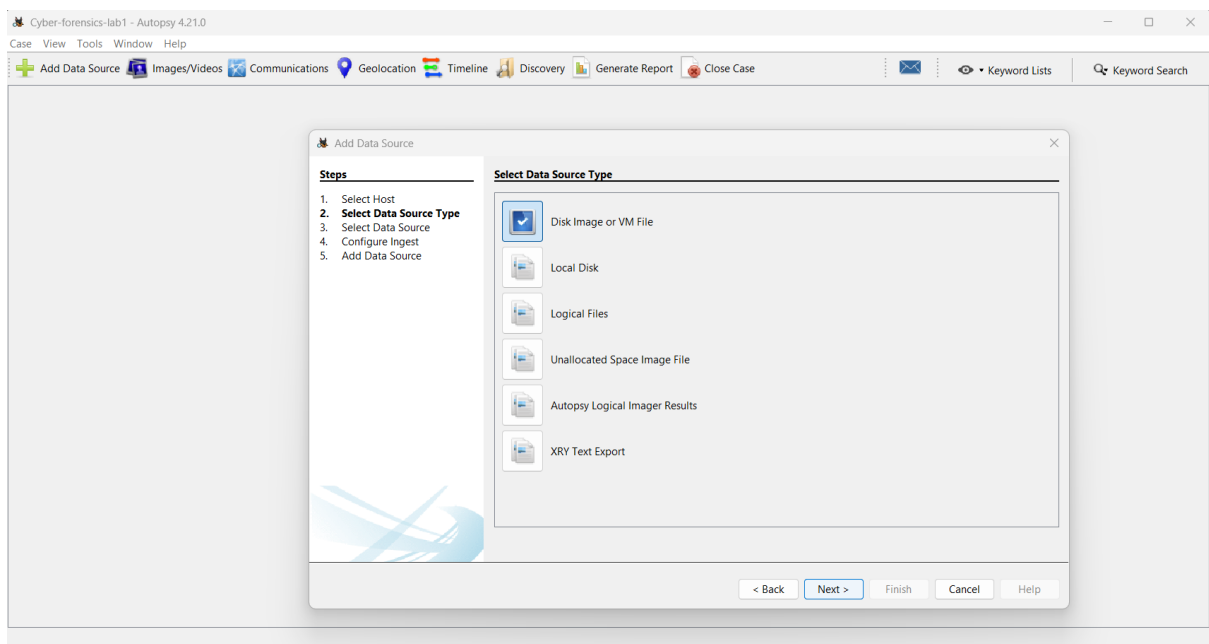
The screenshot shows the Autopsy 4.21.0 application window. The 'New Case Information' dialog box is open, displaying the 'Optional Information' tab. The 'Steps' panel on the left shows '1. Case Information' and '2. Optional Information'. The 'Optional Information' tab contains the following fields:

- Case Number:
- Examiner:
 - Name:
 - Phone:
 - Email:
 - Notes:
- Organization:
 - Organization analysis is being done for:

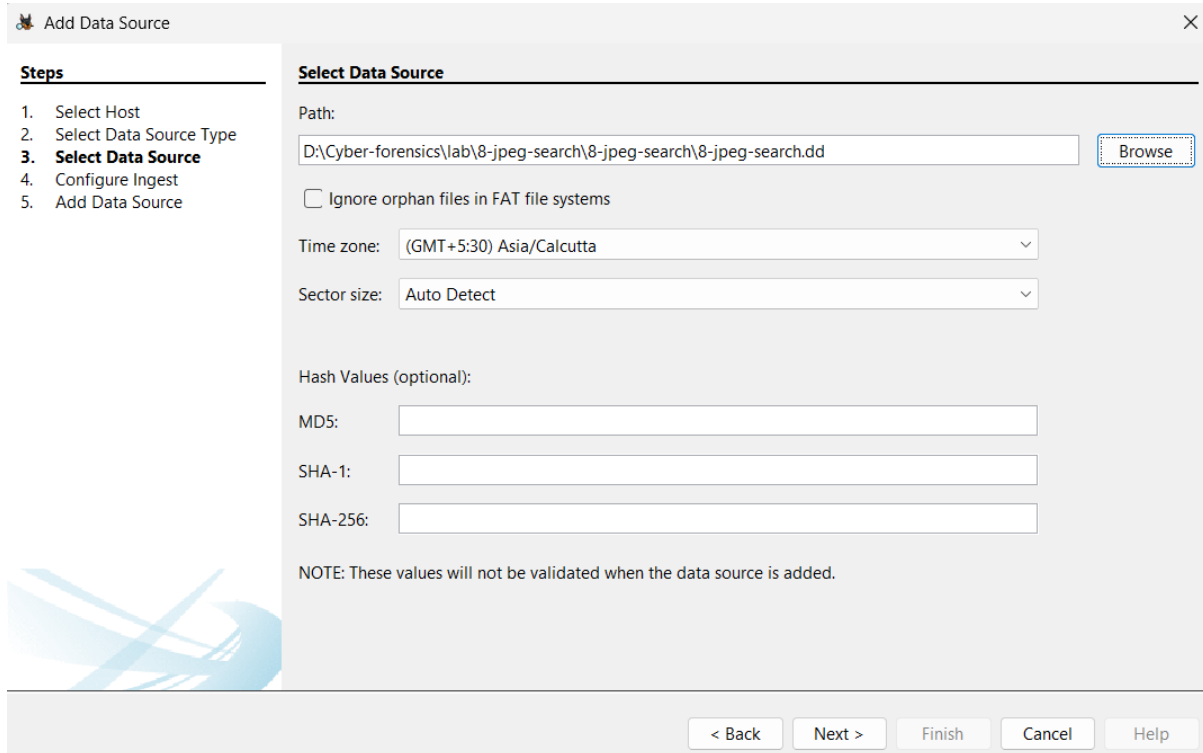
At the bottom of the dialog box, there are buttons: < Back, Next >, Finish, Cancel, and Help.



Click disk image or vm file option(coz I have a disk file)



Add the disk file in the path.(like I did)



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

Path:

☐ Ignore orphan files in FAT file systems

Time zone:

Sector size:

Hash Values (optional):

MD5:

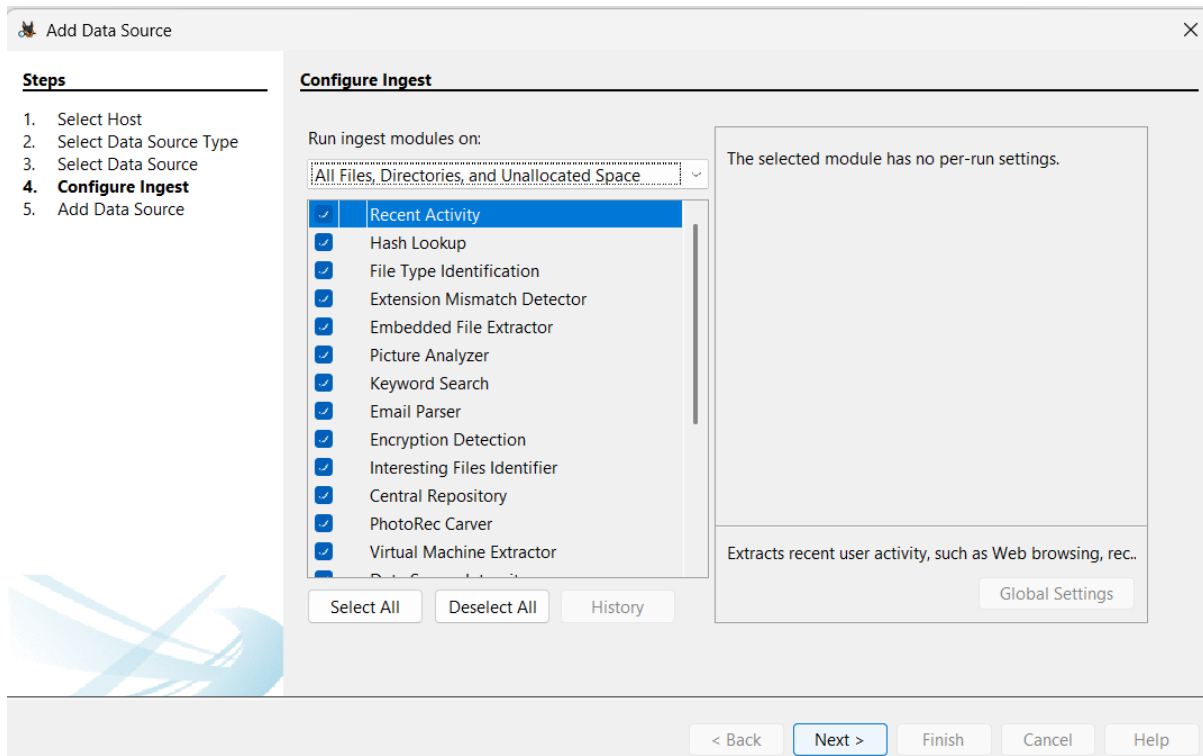
SHA-1:

SHA-256:

NOTE: These values will not be validated when the data source is added.

< Back Next > Finish Cancel Help

Configure the ingest .



Add Data Source

Steps

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

Configure Ingest

Run ingest modules on:

- ☒ Recent Activity
- ☒ Hash Lookup
- ☒ File Type Identification
- ☒ Extension Mismatch Detector
- ☒ Embedded File Extractor
- ☒ Picture Analyzer
- ☒ Keyword Search
- ☒ Email Parser
- ☒ Encryption Detection
- ☒ Interesting Files Identifier
- ☒ Central Repository
- ☒ PhotoRec Carver
- ☒ Virtual Machine Extractor

Select All Deselect All History

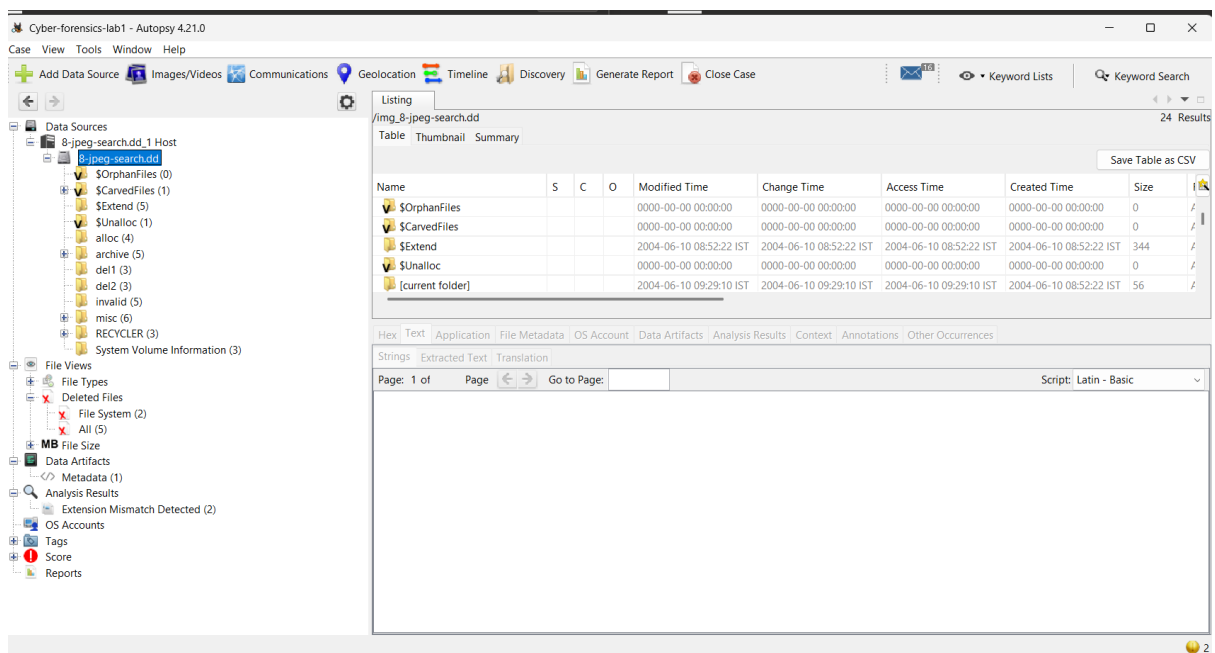
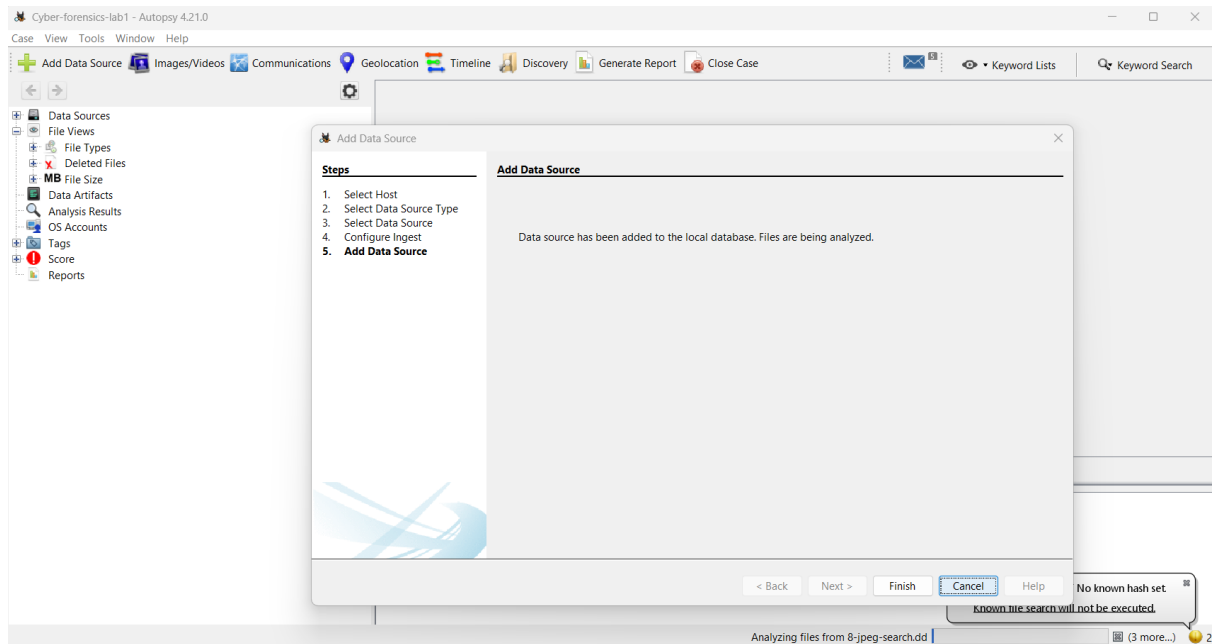
The selected module has no per-run settings.

Extracts recent user activity, such as Web browsing, rec..

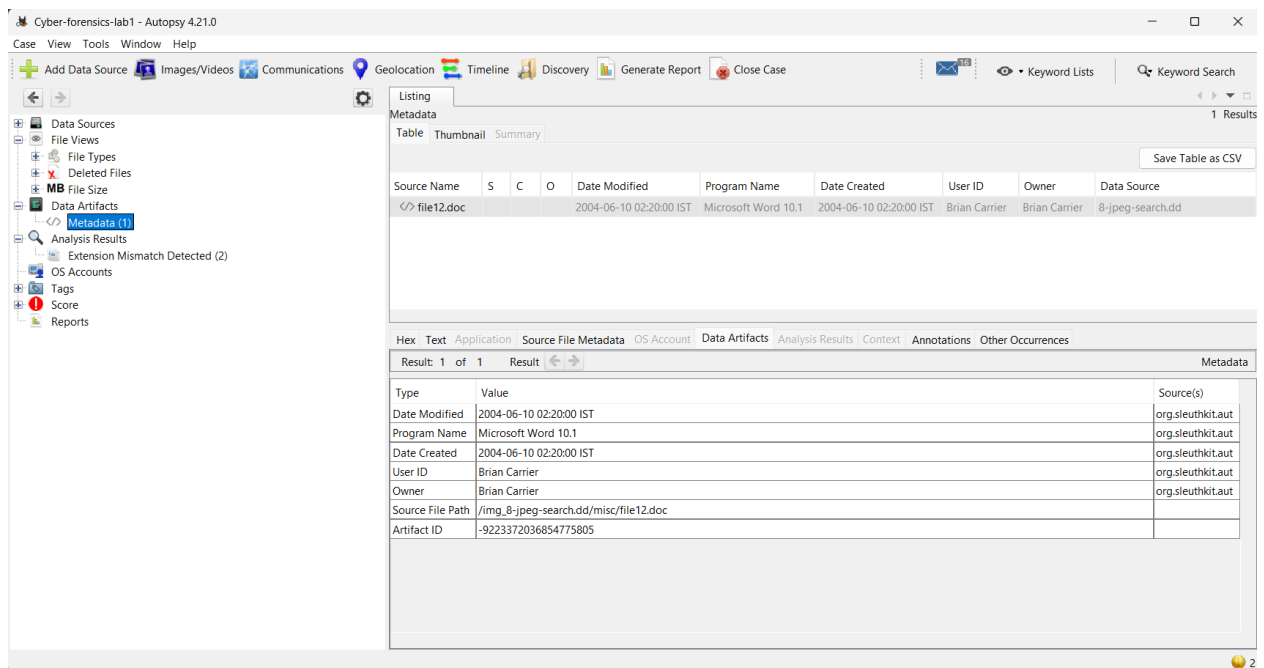
Global Settings

< Back **Next >** Finish Cancel Help

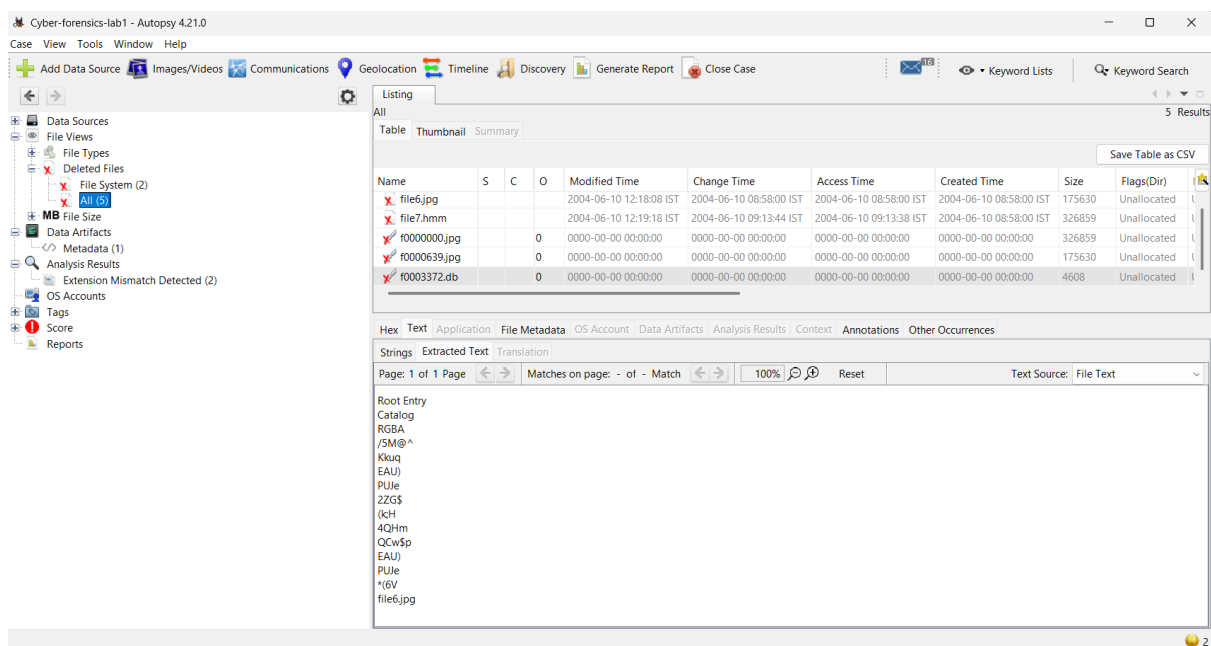
After some time the analysis will be over



We can generate report or view the deleted files etc suffs.



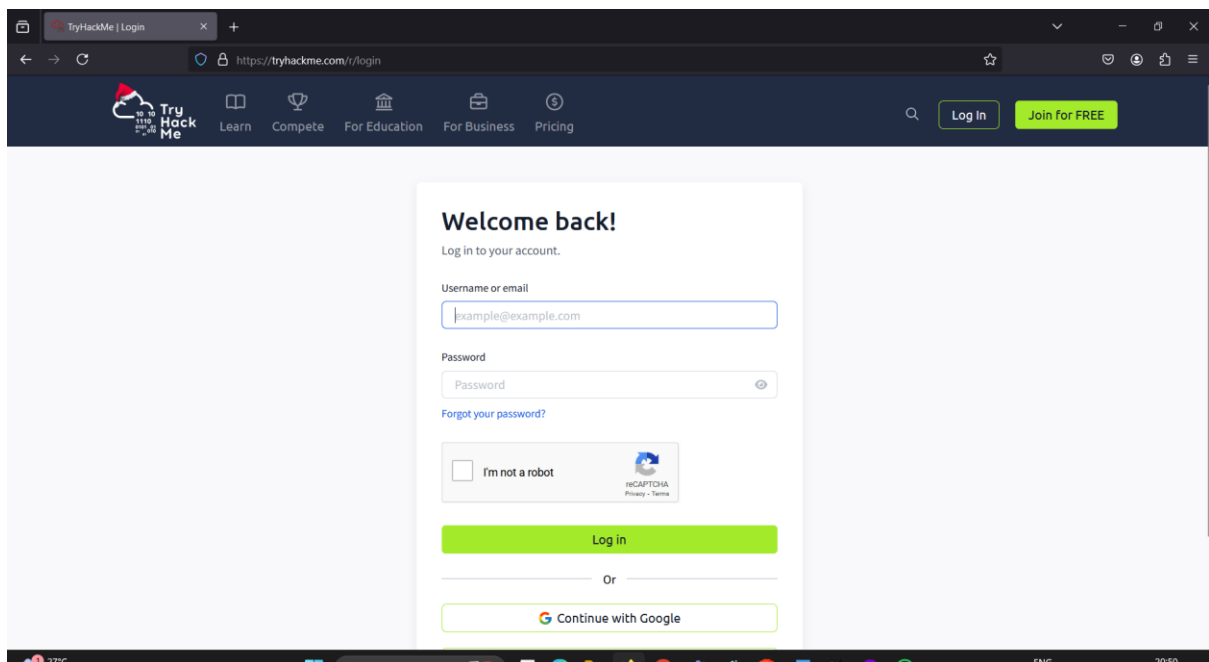
We can see the file file12.doc and its meta data etc



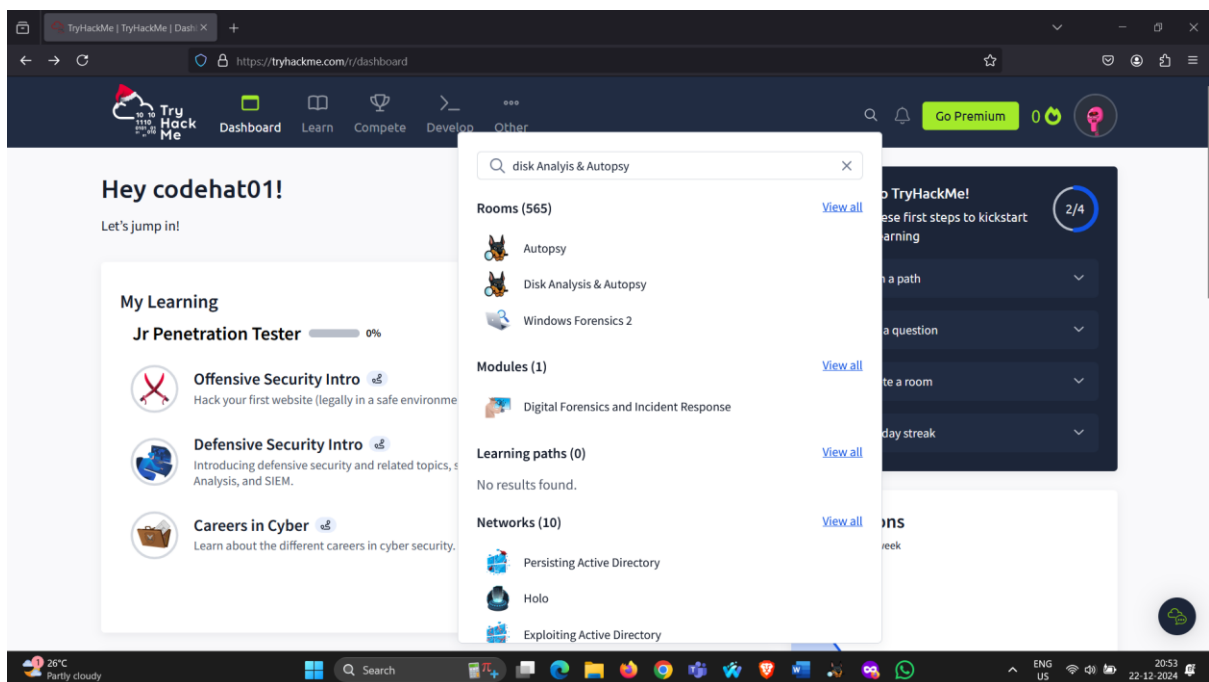
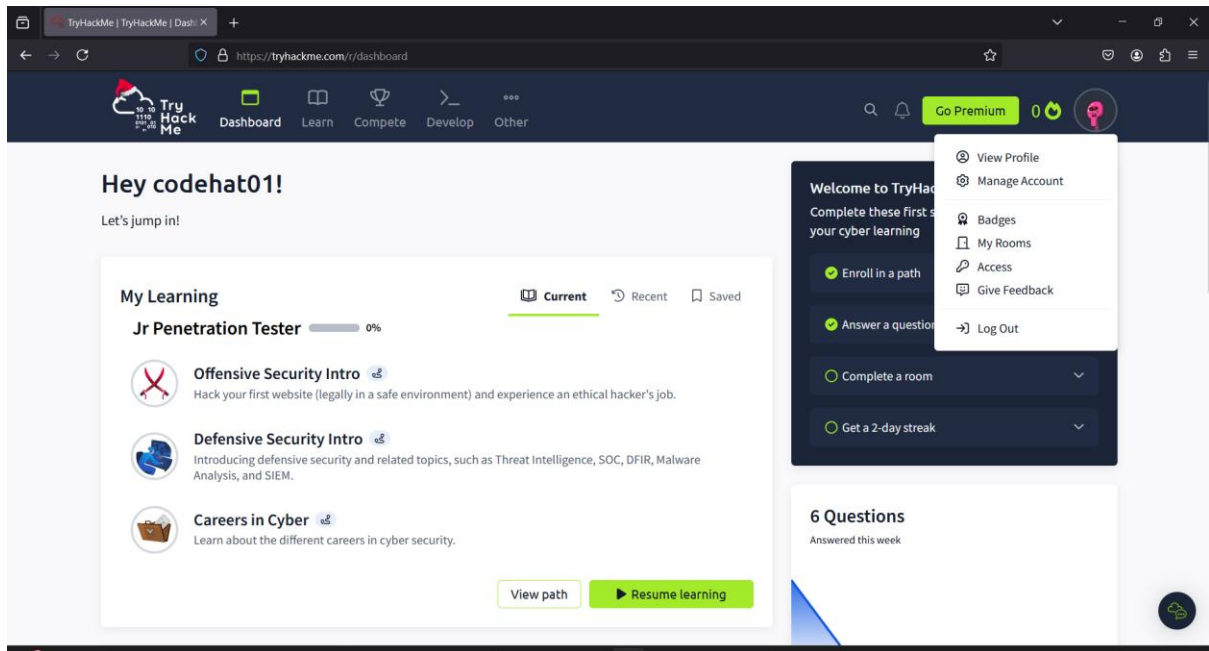
Finally we can see the deleted file and we can retrieve it and save it and if needed we can generate report too by click generate option above.

Experiment 2: Disk Analysis and Autopsy using TryHackMe

Step1:login to tryhackme first



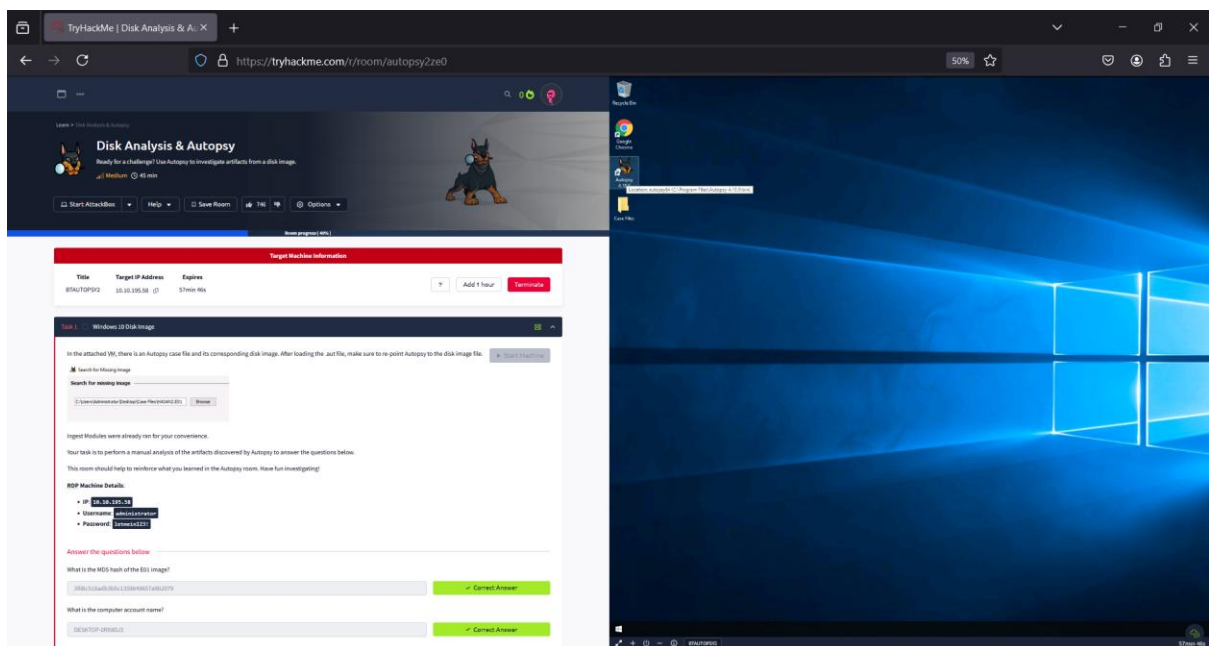
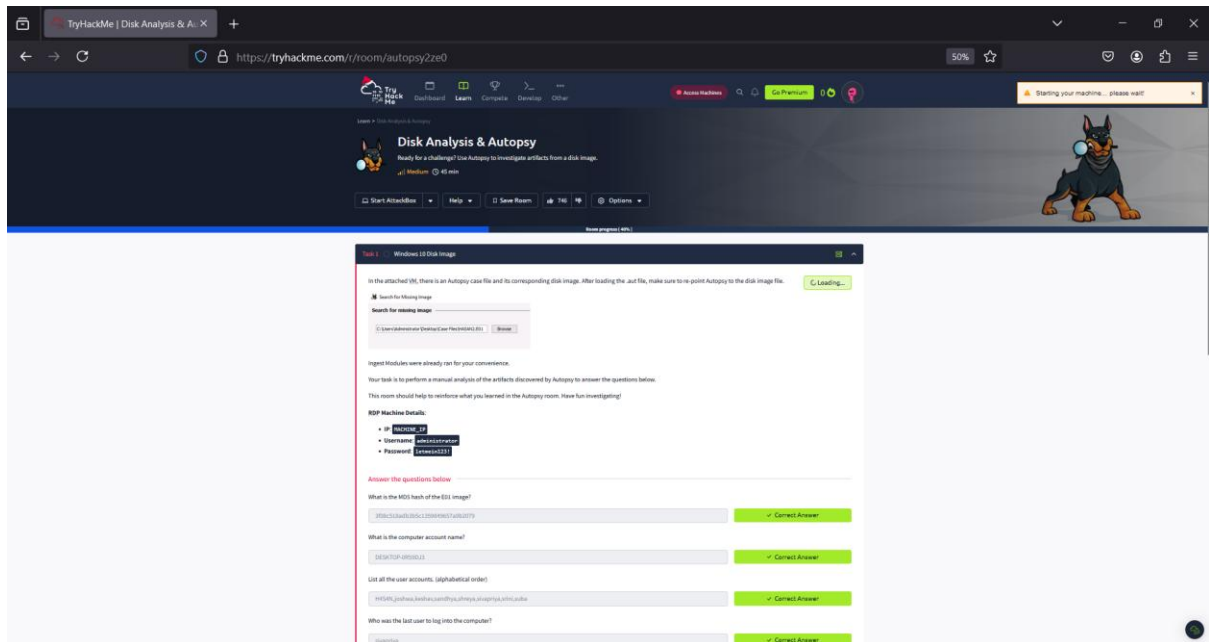
After logged in search for the “DISK Analysis & Autopsy”

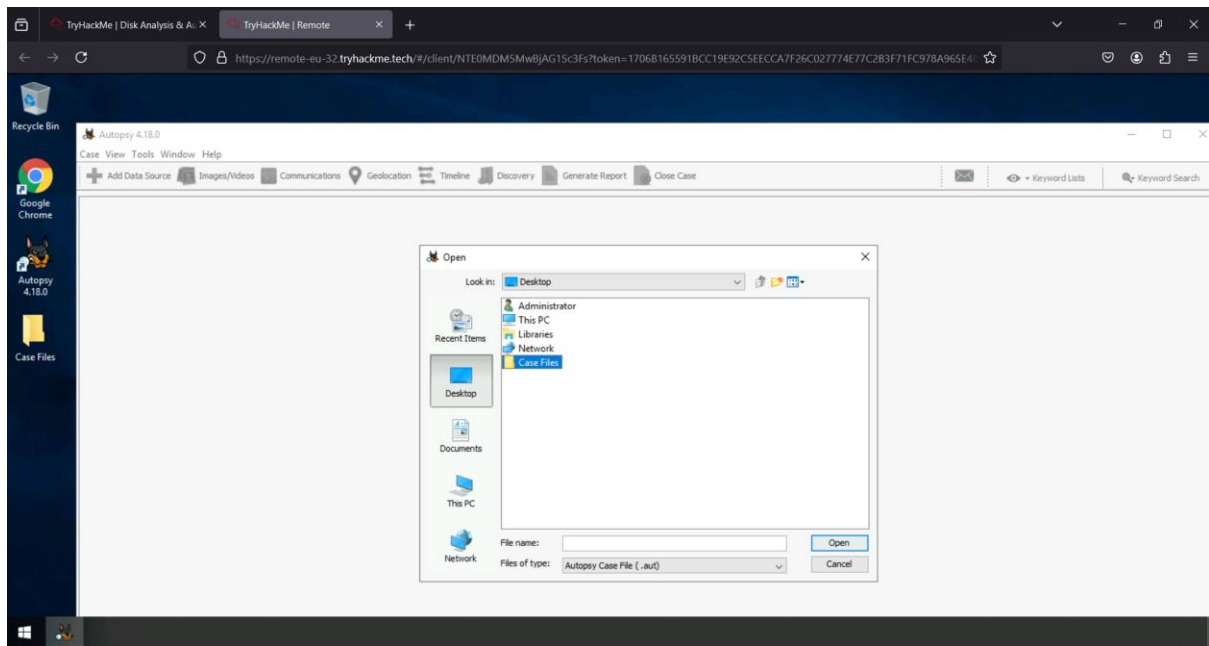


[Link to room](#)

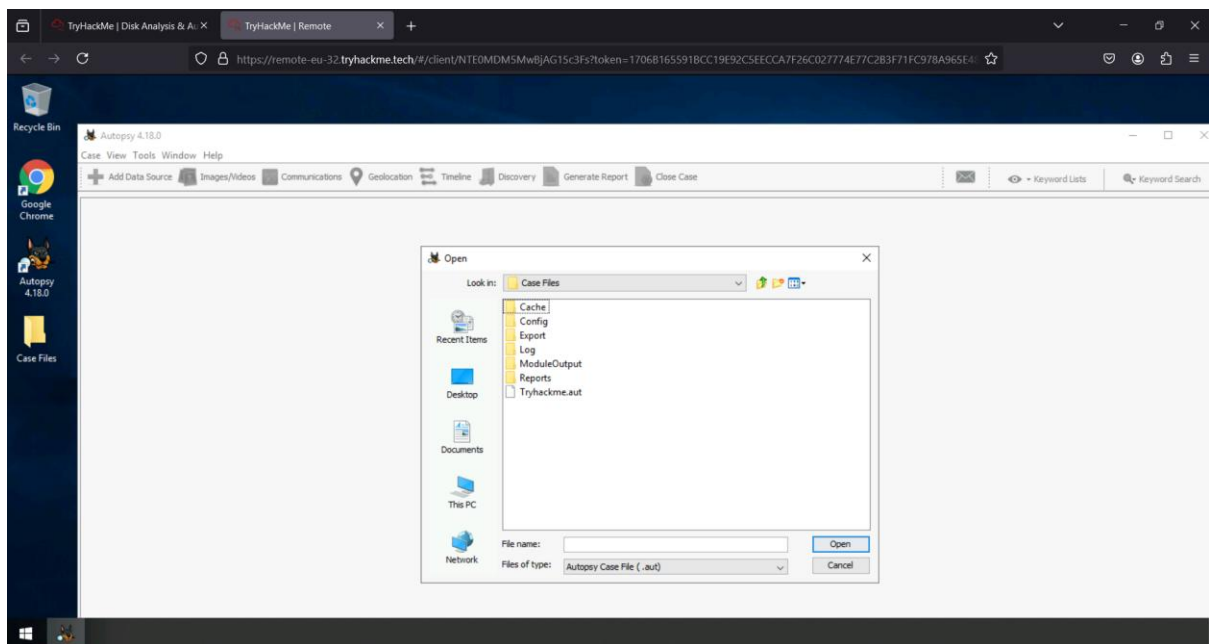
Start the machine

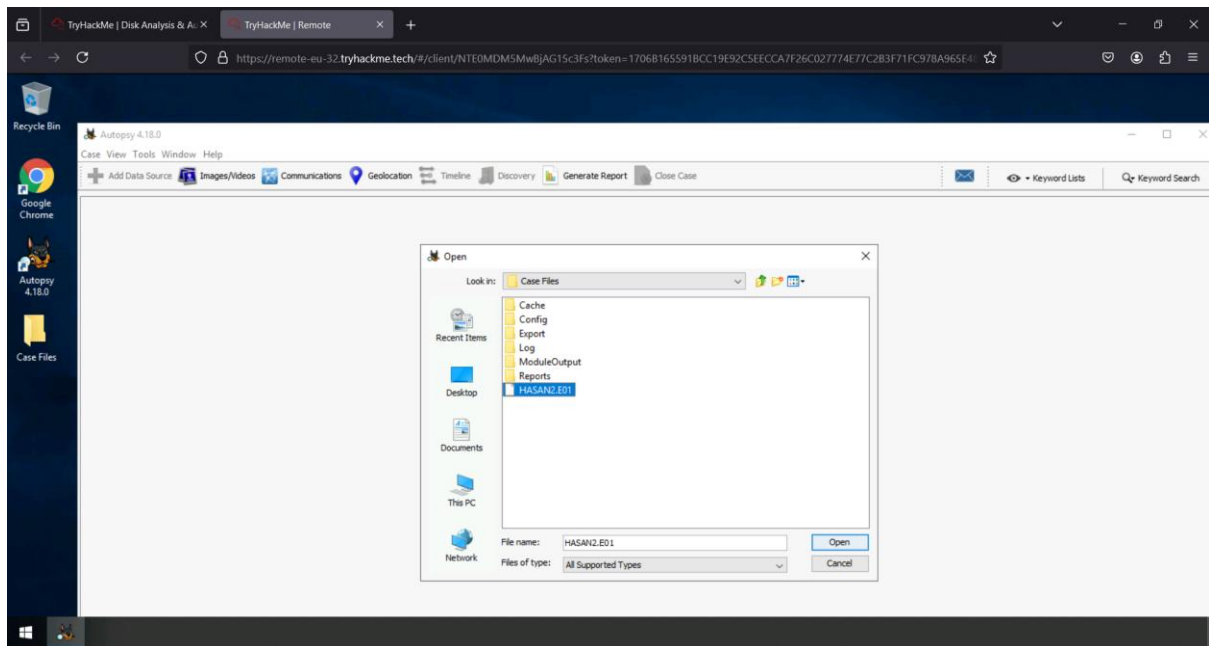
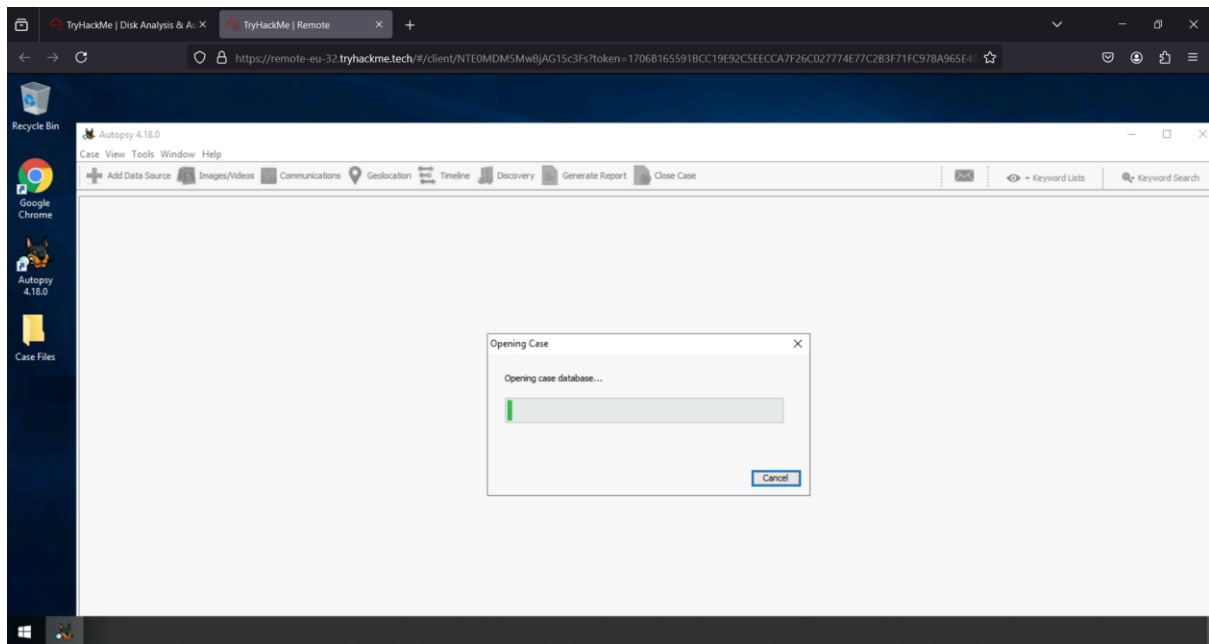
And solve the challenge



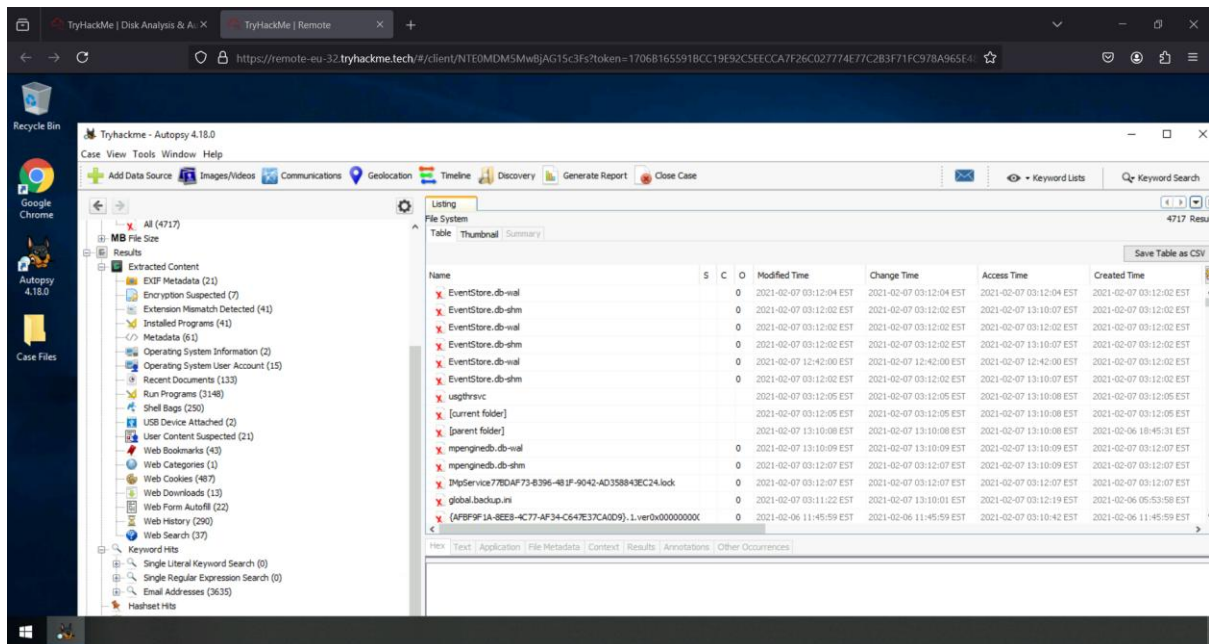
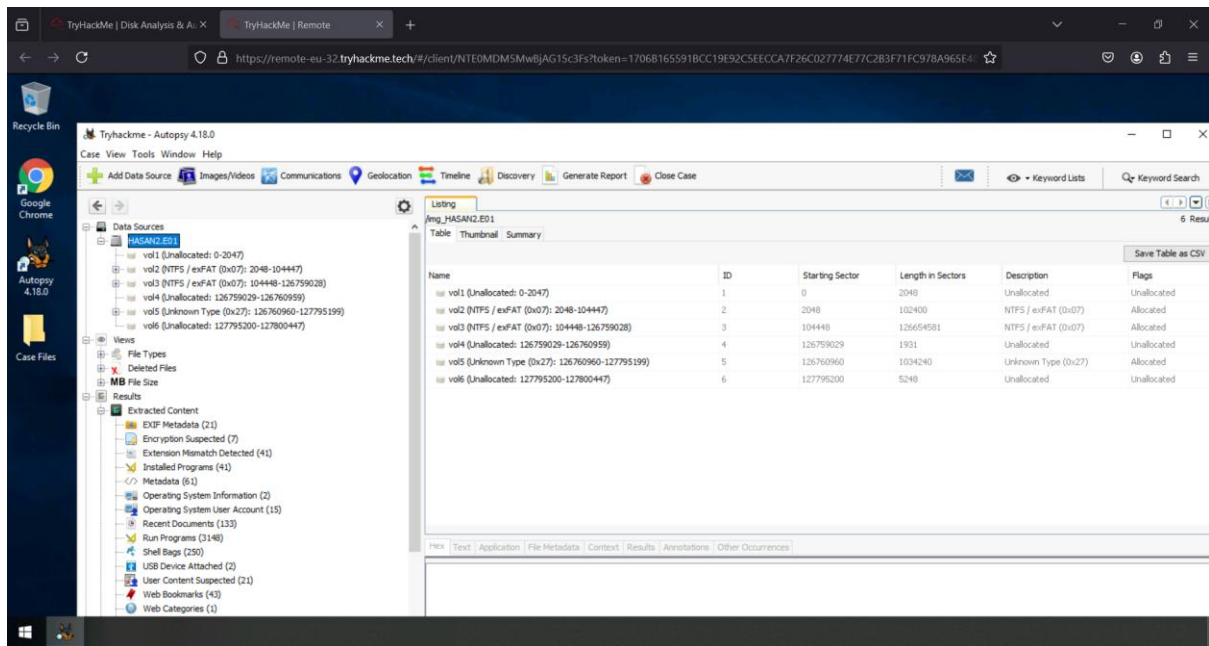


In that case files the is file named Tryhackme.aut open that file and solve the questions.





It will ask for a missing file we need to select this HASAN2.E01



In the left side we can see the extracted content in that we can find more clues to solve this questions start solving

Open the autopsy app in that machine and solve the challenge and answer the questions

Question 1)

The screenshot shows the Autopsy 4.18.0 interface. On the left, the 'Data Sources' pane shows 'HASAN2.E01' under 'Views'. The 'Results' pane shows 'Extracted Content' with various categories like EXIF Metadata, Encryption Suspected, etc. The main pane shows the 'Summary' tab for 'HASAN2.E01'.

Types	User Activity	Analysis	Recent Files	Past Cases	Geolocation	Timeline	Ingest History	Container
Display Name: HASAN2.E01 Name: HASAN2.E01 Device ID: bc9efb0d-bb21-4d04-a08f-3c169ea67774 Time Zone: America/New_York								
Acquisition Details: Description: untitled Acquired Date: Mon Feb 8 12:40:23 2021 System Date: Mon Feb 8 12:40:23 2021 Acquiry Operating System: Win 201x Acquiry Software Version: AD14.5.0.3								
Image Type: E01 Size: 65.43 GB (65433829376 bytes) Unallocated Space: 45.65 GB (45653525664 bytes) Sector Size: 512 bytes MD5: 3f08c518adb3b5c1359849657a9b2079 SHA1: d5ec22ab301db5004140efbfab7946a8f3cf9f2 SHA256:								
File Paths: C:\Users\Administrator\Desktop\Case Files\HASAN2.E01								

What is the MD5 hash of the E01 image?

3f08c518adb3b5c1359849657a9b2079

✓ Correct Answer

Question 2)

The screenshot shows the Autopsy 4.18.0 interface. On the left, the 'Data Sources' pane shows 'HASAN2.E01' under 'Views'. The 'Results' pane shows 'Extracted Content' with various categories like EXIF Metadata, Encryption Suspected, etc. The main pane shows the 'Listing' tab for 'Operating System Information'.

Source File	S	C	O	Name	Domain
SYSTEM				DESKTOP-0R59DJ3	
SOFTWARE					

What is the computer account name?

DESKTOP-0R59DJ3

✓ Correct Answer

Question 3)

The screenshot shows the Autopsy 4.18.0 interface. On the left, the 'Results' pane is expanded to 'Operating System User Account (15)'. The main pane displays a table of user accounts.

Source File	S	C	O	User ID	Username	Date Created
SAM				S-1-5-21-3919888104-523186866-407859479-1005	keshav	2021-02-06 05:39:20 EST
SAM				S-1-5-21-3919888104-523186866-407859479-1006	sivapriya	2021-02-06 05:39:55 EST
SAM				S-1-5-21-3919888104-523186866-407859479-1007	sandhya	2021-02-06 05:40:42 EST
SAM				S-1-5-21-3919888104-523186866-407859479-1008	sriini	2021-02-06 05:41:10 EST
SAM				S-1-5-21-3919888104-523186866-407859479-1001	H4S4N	2021-02-06 18:48:16 EST
SAM				S-1-5-21-3919888104-523186866-407859479-1002	joshwa	2021-02-06 05:38:00 EST
SAM				S-1-5-21-3919888104-523186866-407859479-500	Administrator	2021-02-06 05:39:20 EST
SAM				S-1-5-21-3919888104-523186866-407859479-1003	suba	2021-02-06 05:38:22 EST
SAM				S-1-5-21-3919888104-523186866-407859479-501	Guest	2021-02-06 05:39:55 EST
SAM				S-1-5-21-3919888104-523186866-407859479-1004	shreya	2021-02-06 05:38:48 EST
SAM				S-1-5-21-3919888104-523186866-407859479-503	DefaultAccount	2021-02-06 05:39:20 EST
SAM				S-1-5-21-3919888104-523186866-407859479-504	WDAGUtilityAccount	2021-02-06 05:39:20 EST
SOFTWARE				S-1-5-18	systemprofile	

List all the user accounts. (alphabetical order)

H4S4N,joshwa,keshav,sandhya,shreya,sivapriya,sriini,suba

✓ Correct Answer

Question 4)

The screenshot shows the Autopsy 4.18.0 interface. The 'Operating System User Account' listing is displayed with additional columns for 'Date Accessed' and 'Count'.

Source File	S	C	O	User ID	Username	Date Created	Date Accessed	Count
SAM				S-1-5-21-3919888104-523186866-407859479-1006	sivapriya	2021-02-06 05:39:55 EST	2021-02-07 12:05:37 EST	10
SAM				S-1-5-21-3919888104-523186866-407859479-1001	H4S4N	2021-02-06 18:48:16 EST	2021-02-07 12:05:11 EST	24
SAM				S-1-5-21-3919888104-523186866-407859479-1004	shreya	2021-02-06 05:38:48 EST	2021-02-07 11:46:52 EST	13
SAM				S-1-5-21-3919888104-523186866-407859479-1003	suba	2021-02-06 05:38:22 EST	2021-02-07 11:46:01 EST	2
SAM				S-1-5-21-3919888104-523186866-407859479-1008	sriini	2021-02-06 05:41:10 EST	2021-02-07 11:45:42 EST	2
SAM				S-1-5-21-3919888104-523186866-407859479-1007	sandhya	2021-02-06 05:40:42 EST	2021-02-07 11:45:11 EST	5
SAM				S-1-5-21-3919888104-523186866-407859479-1005	keshav	2021-02-06 05:39:20 EST	2021-02-07 11:45:00 EST	5
SAM				S-1-5-21-3919888104-523186866-407859479-1002	joshwa	2021-02-06 05:38:00 EST	2021-02-07 11:44:49 EST	5

Who was the last user to log into the computer?

sivapriya

✓ Correct Answer

Question 5)

Tryhackme - Autopsy 4.18.0

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Keyword Lists Keyword Search

Listing

/img_HASAN2.E01/vol_vol3/Program Files (x86)/Look@LAN 18 Results

Name	S	C	O	Modified Time	Change Time	Access Time
[current folder]				2021-02-07 03:12:59 EST	2021-02-07 03:12:59 EST	2021-02-07 12:...
[parent folder]				2021-02-07 02:49:11 EST	2021-02-07 02:49:11 EST	2021-02-07 12:...
Report				2021-02-07 03:12:52 EST	2021-02-07 03:12:52 EST	2021-02-07 03:...
sounds				2021-02-07 03:12:53 EST	2021-02-07 03:12:53 EST	2021-02-07 03:...
CLAManual.chm			0	2004-02-17 07:01:50 EST	2021-02-07 03:12:59 EST	2006-01-15 09:...
Look@LAN.dat			0	2021-02-07 03:14:10 EST	2021-02-07 03:14:10 EST	2021-02-07 03:...

Hex Text Application File Metadata Context Results Annotations Other Occurrences

Strings Indexed Text Translation

Page: 1 of 1 Page Matches on page: - of - Match 100% Reset

Text Source: File Text

```
[Config]
ConfigFile=C:\Program Files (x86)\Look@LAN\irunin.dat
LanguageFile=C:\Program Files (x86)\Look@LAN\irunin.lng
ImageFile=C:\Program Files (x86)\Look@LAN\irunin.bmp
LangID=9
IsSelective=0
InstallType=0
[Variables]
%LANHOST%=DESKTOP-0R59DJ3
%LANDOMAIN%=DESKTOP-0R59DJ3
%LANUSER%=H4S4N
%LANIP%=192.168.130.216
%LANNIC%=0800272cc4b9
%ISWIN95%=FALSE
%ISWIN98%=FALSE
```

What was the IP address of the computer?

192.168.130.216

✓ Correct Answer

Question 6)

What was the MAC address of the computer? (XX-XX-XX-XX-XX-XX)

08-00-27-2c-c4-b9

✓ Correct Answer

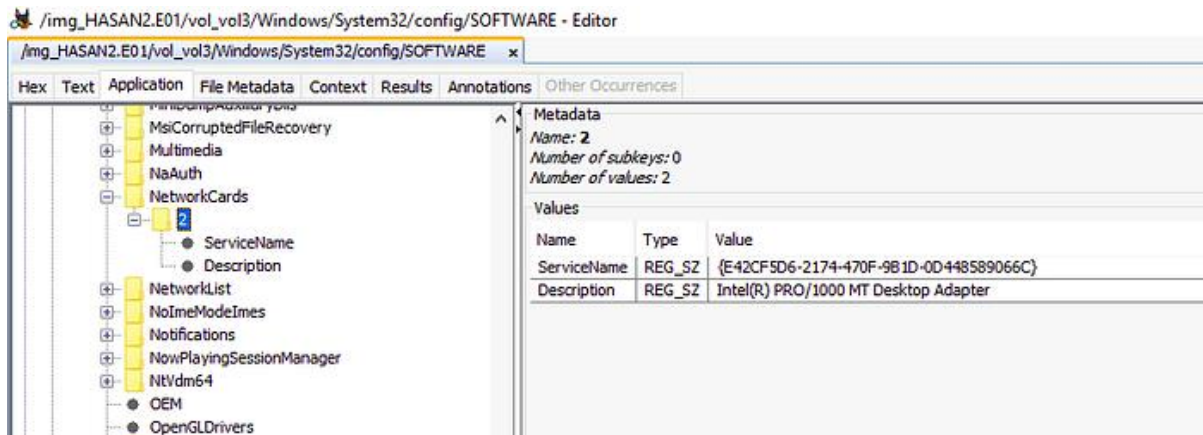
Question 7)

What is the name of the network monitoring tool?

Look@LAN

✓ Correct Answer

Question 8)

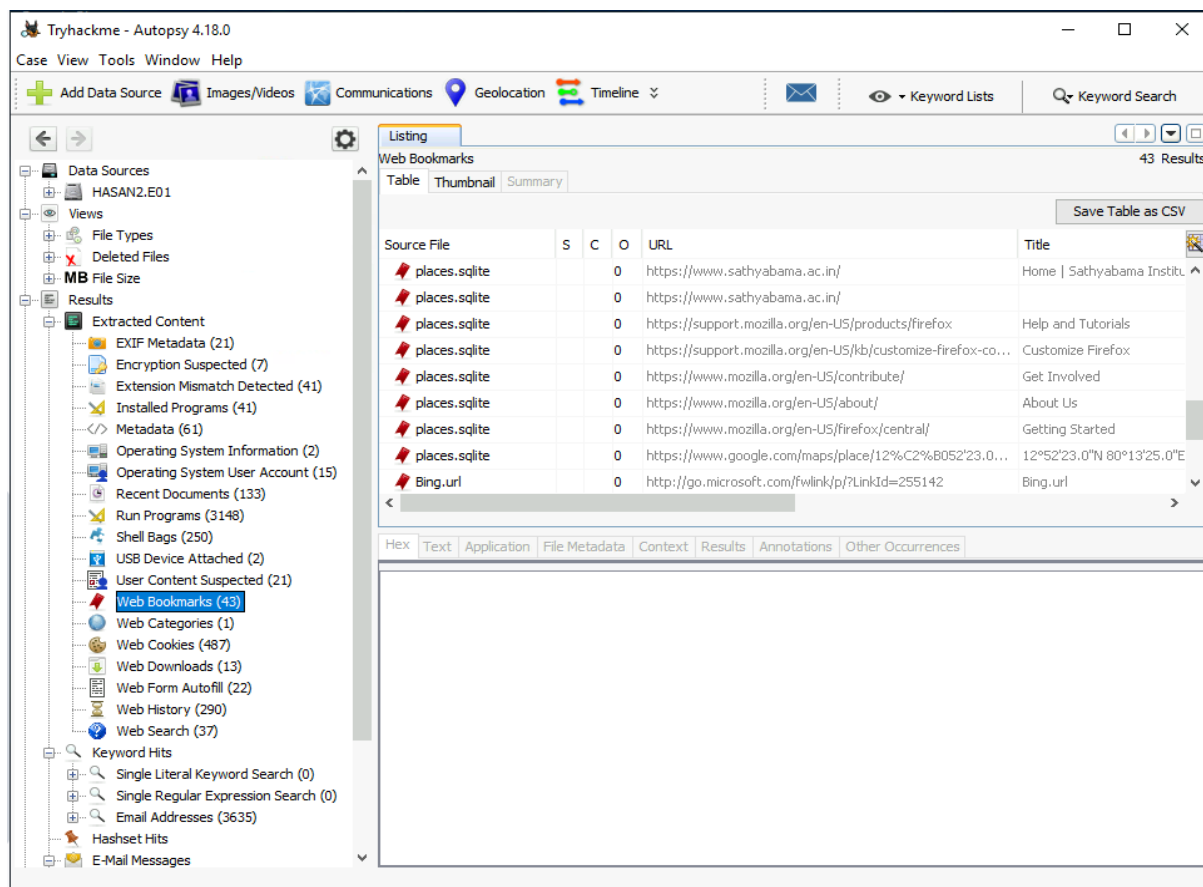


What is the name of the network card on this computer?

Intel(R) PRO/1000 MT Desktop Adapter

✓ Correct Answer

Question 9)



A user bookmarked a Google Maps location. What are the coordinates of the location?

12°52'23.0"N 80°13'25.0"E

✓ Correct Answer

Question 10)

Tryhackme - Autopsy 4.18.0

Case View Tools Window Help

+ Add Data Source Images/Videos Communications Geolocation Timeline Keyword Lists Keyword Search

Listing

/img_HASAN2.E01/vol_vol3/Users/joshwa/Downloads 5 Results

Table Thumbnail Summary Save Table as CSV

Name	S	C	O	Modified Time	Change Time
[current folder]				2021-02-06 07:12:05 EST	2021-02-06 07:12:05 EST
[parent folder]				2021-02-06 05:45:59 EST	2021-02-06 05:51:25 EST
cyberpunk-2077-samurai-jacket-yo-1360x768.jpg			0	2021-02-06 07:14:47 EST	2021-02-06 07:14:47 EST
cyberpunk-2077-samurai-jacket-yo-1360x768.jpg:Zone.Identifier			0	2021-02-06 07:14:47 EST	2021-02-06 07:14:47 EST
desktop.ini			0	2021-02-06 05:43:25 EST	2021-02-06 05:51:25 EST

/img_HASAN2.E01/vol_vol3/Users/joshwa/Downloads/cyberpunk-2077-samurai-jacket-yo-1360x768.jpg

Hex Text Application File Metadata Context Results Annotations Other Occurrences

Reset

Other Occurrences

A user has his full name printed on his desktop wallpaper. What is the user's full name?

Anto Joshua

✓ Correct Answer

Question 11)

TryHackme - Autopsy 4.18.0
Case View Tools Window Help
Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

Listing
img_HASAN2.E01/vol3/Users/shreya/AppData/Roaming/Microsoft/Windows/PowerShell/PSReadLine

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dr)
[current folder]				2021-02-06 06:00:53 EST	2021-02-06 11:42:52 EST	2021-02-06 12:45:15 EST	2021-02-06 06:00:53 EST	288	Allocated
[parent folder]				2021-02-06 06:00:53 EST	2021-02-06 06:00:53 EST	2021-02-06 12:45:03 EST	2021-02-06 06:00:53 EST	256	Allocated
Consolertst_history.txt			0	2021-02-06 12:40:36 EST	2021-02-06 12:40:36 EST	2021-02-06 12:45:03 EST	2021-02-06 06:00:53 EST	421	Allocated

Hex Text Application File Metadata Context Results Annotations Other Occurrences

Saves Indexed Text Translation

Pages: 1 of 1 Page Matches on page: - of - Match 250% Reset

```
cd .\Desktop\  
exitcls  
Add-Content .\shreya.txt 'flag{HarleyQuinnForQueen}'  
Get-Content .\shreya.txt  
Add-Content .\shreya.txt 'flag{HarleyQuinnForQueen}'  
Get-Content .\shreya.txt  
Set-Content .\shreya.txt 'flag{i_changed_it}'  
exit
```

A user had a file on her desktop. It had a flag but she changed the flag using PowerShell. What was the first flag?

flag{HarleyQuinnForQueen}

✓ Correct Answer

Question 12)

TryHackme - Autopsy 4.18.0
Case View Tools Window Help
Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

Listing
img_HASAN2.E01/vol3/Users/shreya/Desktop

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dr)	Flags(Meta)	Known	Location
[current folder]				2021-02-06 06:51:42 EST	2021-02-06 06:51:42 EST	2021-02-07 11:48:09 EST	2021-02-06 05:41:55 EST	360	Allocated	Allocated	unknown	img_HASAN2.E01/vol3/Users/shreya/Desktop
[parent folder]				2021-02-06 06:44:47 EST	2021-02-06 06:44:47 EST	2021-02-07 13:10:05 EST	2021-02-06 05:41:55 EST	256	Allocated	Allocated	unknown	img_HASAN2.E01/vol3/Users/shreya/Desktop
desktop.txt			0	2021-02-06 05:41:58 EST	2021-02-06 05:41:58 EST	2021-02-07 13:10:05 EST	2021-02-06 05:41:58 EST	382	Allocated	Allocated	unknown	img_HASAN2.E01/vol3/Users/shreya/Desktop
shreya.txt			0	2021-02-06 06:53:29 EST	2021-02-06 06:53:29 EST	2021-02-07 02:01:54 EST	2021-02-06 06:06:22 EST	764	Allocated	Allocated	unknown	img_HASAN2.E01/vol3/Users/shreya/Desktop

Hex Text Application File Metadata Context Results Annotations Other Occurrences

Saves Indexed Text Translation

Pages: 1 of 1 Page Matches on page: - of - Match 250% Reset

```
if((([System.Security.Principal.WindowsIdentity]::GetCurrent()).groups -  
) {  
    #Payload goes here  
    #It'll run as Administrator  
    New-Item "C:\Users\H4S4N\Desktop\hacked.txt"  
    Add-Content C:\Users\H4S4N\Desktop\hacked.txt 'Flag{I-hacked-you}'  
    ##### https://youtu.be/C9GFmfFjhYI
```


The same user found an exploit to escalate privileges on the computer. What was the message to the device owner?

flag{I-hacked-you}

✓ Correct Answer

Question 13)

Tryhackme - Autopsy 4.18.0

Case View Tools Window Help

Autopsy 4.18.0 interface showing the file system view of a Windows user's Downloads folder.

Left sidebar (File System):

- Support (11)
- Windows NT (4)
- Windows Security Health (4)
- WinMSIPC (3)
- WwanSvc (4)
- Microsoft OneDrive (3)
- Mozilla (5)
- Package Cache (14)
- Packages (10)
- regid.1991-06.com.microsoft (3)
- SoftwareDistribution (2)
- ssh (2)
- Start Menu (2)
- Templates (2)
- USOPrivate (3)
- USOShare (3)
- WindowsHolographicDevices (3)
- Recovery (2)
- System Volume Information (7)
- Users (15)
- All Users (2)
- Default (28)
- Default User (2)
- H4S4N (34)

Right pane (Listing):

Path: /img_HASAN2.E01/vol_vol3/Users/H4S4N/Downloads

Name	S	C	O	Modified Time	CI
[current folder]				2021-02-07 02:49:01 EST	2C
[parent folder]				2021-02-06 18:51:57 EST	2C
0or1.jpg			0	2020-10-01 14:17:08 EDT	2C
desktop.ini			0	2021-02-06 18:49:17 EST	2C
lsetup250.exe			0	2021-02-07 02:47:16 EST	2C
mimikatz_trunk.zip			0	2021-02-06 09:56:28 EST	2C
mimikatz_trunk.zip:Zone.Identifier			0	2021-02-06 09:56:28 EST	2C
python-3.9.1-amd64.exe			0	2021-02-06 10:27:17 EST	2C
wallpapersden-com-mr-robot-season-4-7500x3708.jpg			0	2021-02-06 11:42:50 EST	2C
wallpapersden-com-mr-robot-season-4-7500x3708.jpg:Zone.Ident			0	2021-02-06 11:42:50 EST	2C

Tryhackme - Autopsy 4.18.0

Case View Tools Window Help

Autopsy 4.18.0 interface showing the file system view of a Windows user's Downloads folder.

Left sidebar (File System):

- Features (2)
- LocalCopy (3)
- Network Inspection System (3)
- Platform (3)
- Quarantine (5)
- Scans (23)
- BackupStore (2)
- History (8)
- CacheManager (3)
- RemCheck (8)
- ReportLatency (3)
- Results (4)
- Service (6)
- DetectionHistory (11)
- 00 (3)
- 01 (4)
- 02 (5)
- 07 (3)
- 08 (3)
- 09 (3)
- 10 (3)
- 12 (5)
- 13 (4)
- 16 (3)
- 17 (3)
- 18 (4)
- 19 (3)
- 20 (3)
- Store (11)
- Scans (3)
- History (3)
- CacheManager (2)
- Support (11)

Right pane (Listing):

Path: /img_HASAN2.E01/vol_vol3/ProgramData/Microsoft/Windows Defender/Scans/History/Service/DetectionHistory/02

Name	S	C	O	Modified Time	Change Time	Access Time
[current folder]				2021-02-07 02:48:21 EST	2021-02-07 02:48:21 EST	2021-02-07 12:10:57 EST
[parent folder]				2021-02-06 11:19:43 EST	2021-02-07 02:29:38 EST	2021-02-07 12:10:57 EST
2B18837D-B94C-4E51-934B-654F69FAE7E2			0	2021-02-07 11:05:20 EST	2021-02-07 11:05:20 EST	2021-02-07 12:10:57 EST
7F334C0D-CED8-4268-8096-CE083CD29441			0	2021-02-07 11:05:20 EST	2021-02-07 11:05:20 EST	2021-02-07 12:10:57 EST
8363AFD9-AF2E-453A-882D-766E1C57A88A			0	2021-02-07 02:49:01 EST	2021-02-07 02:49:01 EST	2021-02-07 12:10:57 EST

Bottom pane (Strings):

Page: 1 of 1 Page

Matches on page: - of - Match

150%

Reset

Strings: Indexed Text Translation

Magic.Version:1.2
HackTool:Win32/LaZagne
Magic.Version:1.2
file
C:\Users\H4S4N\Downloads\lazagne.exe
ThreatTrackingSha256

2 hack tools focused on passwords were found in the system. What are the names of these tools? (alphabetical order)

Lazagne,Mimikatz

✓ Correct Answer

🔍 Hint

Question 14)

The screenshot shows the Autopsy 4.18.0 interface. On the left, a file tree is visible. The main pane displays 'File Search Results 1' and 'File Search Results 2'. The search results table shows three files:

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags
kiwi_passwords.yar.lnk			0	2021-02-06 10:05:17 EST	2021-02-06 10:05:17 EST	2021-02-06 10:05:17 EST	2021-02-06 10:05:17 EST	836	Allocate
kiwi_passwords.yar.lnk.slack				2021-02-06 10:05:17 EST	2021-02-06 10:05:17 EST	2021-02-06 10:05:17 EST	2021-02-06 10:05:17 EST	3260	Allocate
kiwi_passwords.yar			0	2020-09-16 21:04:34 EDT	0000-00-00 00:00:00	2020-09-16 21:04:34 EDT	2020-09-21 13:20:37 EDT	3834	Allocate

The 'kiwi_passwords.yar' file is selected. The bottom pane shows the YARA file content:

```
/* Benjamin DELPY `gentilkiwi`  
https://blog.gentilkiwi.com  
benjamin@gentilkiwi.com  
Licence : https://creativecommons.org/licenses/by/4.0/  
*/  
rule mimikatz  
{  
  meta:  
    description      = "mimikatz"  
    author            = "Benjamin DELPY (gentilkiwi)"  
    tool_author       = "Benjamin DELPY (gentilkiwi)"
```

There is a YARA file on the computer. Inspect the file. What is the name of the author?

Benjamin DELPY (gentilkiwi)

✓ Correct Answer

Question 15)

The screenshot shows the Tryhackme - Autopsy 4.18.0 interface. On the left is a file tree with various folders like 'PrintHood (2)', 'Recent (2)', 'Saved Games (3)', etc. The main pane displays a 'Keyword search 1 - zerologon' window with 23 results. The results are shown in a table with columns 'Name' and 'Keyword Preview'. The file '2.2.0 20200918 Zerologon encrypted.lnk' is selected and highlighted in blue. Below the table, the 'Text' tab is active, showing the contents of the selected file. The text includes a list of users: 'FRGV', 'Usersd', 'OwHFR', 'Users', '@shell32.dll, -21813', 'sandhya@', 'sandhya', 'FREr', 'DOWNLO~1', and 'UFREr.'.

Name	Keyword Preview
V0100005.log	ds/2.2.0%2020200918%«20zerologon«%20encrypted.zip..
mimikatz.exe	patchpostzerologon«zerologon«packagesask a dc t
ntuser.dat.LOG2	hell2.2.0 20200918 «zerologon« encrypted.zip2.2.0
0	-fix/2.2.0 20200918 «zerologon« encrypted.zip", "t
0	ing?2.2.0 20200918 «zerologon« encrypted.zip\ufe0fscan
WebCacheV01.dat	ds/2.2.0%2020200918%«20zerologon«%20encrypted.zip..
mimikatz.exe	rrentpostzerologon«zerologon«packagesask a dc t
2.2.0 20200918 Zerologon encrypted.lnk	2.2.0 20200918 «zerologon« encrypted.ln
Recent Documents Artifact	oads{2.2.0 20200918 «zerologon« encrypted.zippath

Page: 1 of 1 Page | Matches on page: 1 of 4 Match | 100% | Reset

Text Source: Search Results

```
{2.2.0 20200918 zerologon encrypted.lnk, /C:\
FRGV
Usersd
OwHFR
Users
@shell32.dll, -21813
sandhya@
sandhya
FREr
DOWNLO~1
UFREr.
```

One of the users wanted to exploit a domain controller with an MS-NRPC based exploit. What is the filename of the archive that you found? (include the spaces in your answer)

2.2.0 20200918 Zerologon encrypted.zip

✓ Correct Answer

After submission:

