AMRITA VISHWA VIDYAPEETHAM

NAME:SOWMYA K **DATE:22.12.2024**

ROLL NUMBER:CH.EN.EN.U4CYS22046 **COURSE CODE:20CYS311**

----

1. What is Hard Disk Forensics?

Hard disk forensics is the process of recovering, analyzing, and preserving data from a computer's hard drive for use as evidence in a legal investigation. It involves identifying, extracting, and documenting data, including deleted, hidden, or encrypted files.

2. What is an Image File?

An image file in digital forensics is a complete copy of a storage device's data, including all files, system areas, and unallocated space. It is used for analysis without altering the original data source.

3. What is Allocated and Unallocated Space?

- **Allocated Space:** Space on a storage device actively used to store data.
- **Unallocated Space:** Free space on a device not currently assigned to files, but it may contain remnants of deleted data.

4. What is Disk Cache and Disk Mirroring?

- **Disk Cache:** A portion of memory used to temporarily store frequently accessed data to improve read/write performance.
- **Disk Mirroring:** A data redundancy method where identical copies of data are maintained on two or more hard drives to ensure data availability.

5. What is a Forensic Image?

A forensic image is a bit-by-bit copy of a storage device that captures every byte of data, including deleted and hidden files, ensuring data integrity for forensic analysis.

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

The hash value of a hard disk is a unique cryptographic fingerprint (e.g., MD5 or SHA-256) of its contents, used to verify data integrity and ensure the evidence has not been tampered with.

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

- **Shadow Volume:** A hidden copy of files stored by the operating system for recovery purposes.
- **Shadow Copy:** A backup feature that creates snapshots of files or volumes at a specific point in time.
- **Swap Disk:** A portion of a hard drive used as virtual memory to extend the RAM when it is full.

8. What Tools Can Perform Hard Disk Forensics?

Popular tools for hard disk forensics include:

- EnCase
- FTK (Forensic Toolkit)
- Autopsy/Sleuth Kit
- X-Ways Forensics
- ProDiscover
- Magnet AXIOM
- Caine

9. What is Exif Metadata?

Exif metadata is embedded in image files and contains details such as:

- Camera settings (e.g., aperture, ISO).
- Date and time of capture.
- GPS location.
  It is crucial in forensic investigations to trace image origins or establish timelines.

10. What are Common Disk Image Formats?

- E01 (EnCase Evidence File)
- DD (Raw Disk Image)
- AFF (Advanced Forensic Format)
- ISO (CD/DVD Image)

11. What is Bit-by-Bit Copying?

Bit-by-bit copying creates an exact replica of a storage device by copying all sectors, including allocated, unallocated, and hidden areas, ensuring complete duplication of data for forensic analysis.

12. What is Cloning a Disk?

Cloning a disk involves creating an identical copy of a storage device, typically for backup or migration. Unlike forensic imaging, it may not capture deleted or hidden data.

13. What are the Latest Types of Storage Devices?

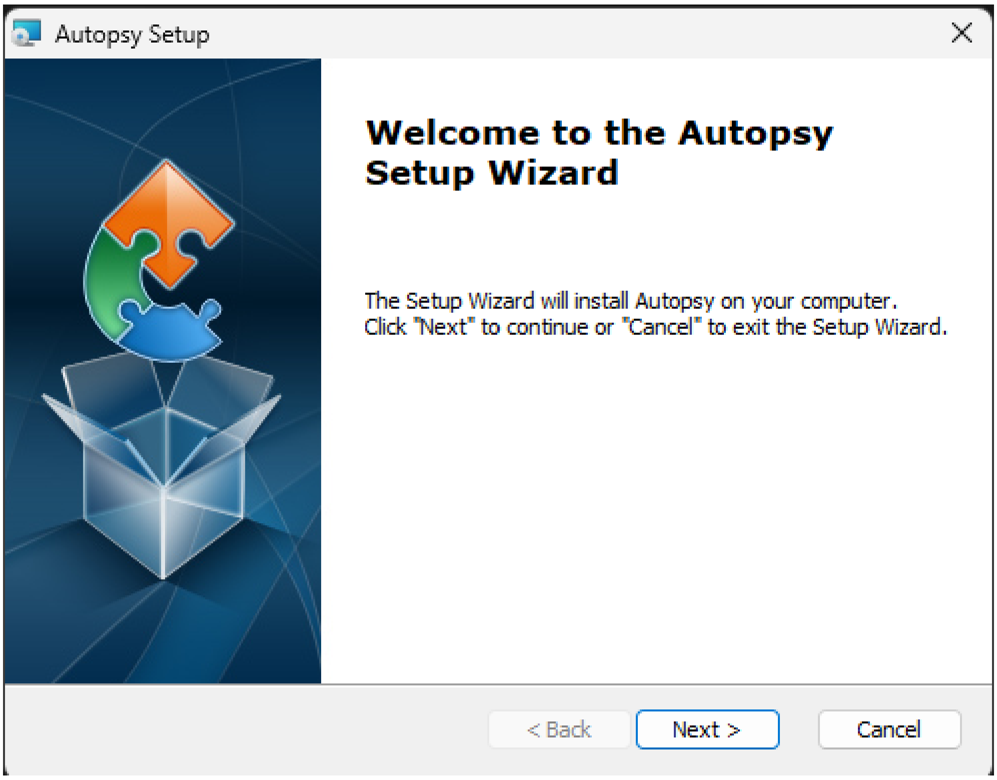
- Solid-State Drives (SSD)
- NVMe Drives
- Hybrid Drives (HDD + SSD)
- Cloud-Based Storage
- Flash Memory (e.g., USB drives, SD cards)
- Optane Memory

14. What is BitLocker Encryption?

BitLocker is a disk encryption feature in Windows that secures data by encrypting the entire drive, protecting it from unauthorized access in case of theft or loss. It requires a password or a recovery key to decrypt the data.

(ANALYSIS OF DATA SOURCE (LOCAL DISK) USING AUTOPSY

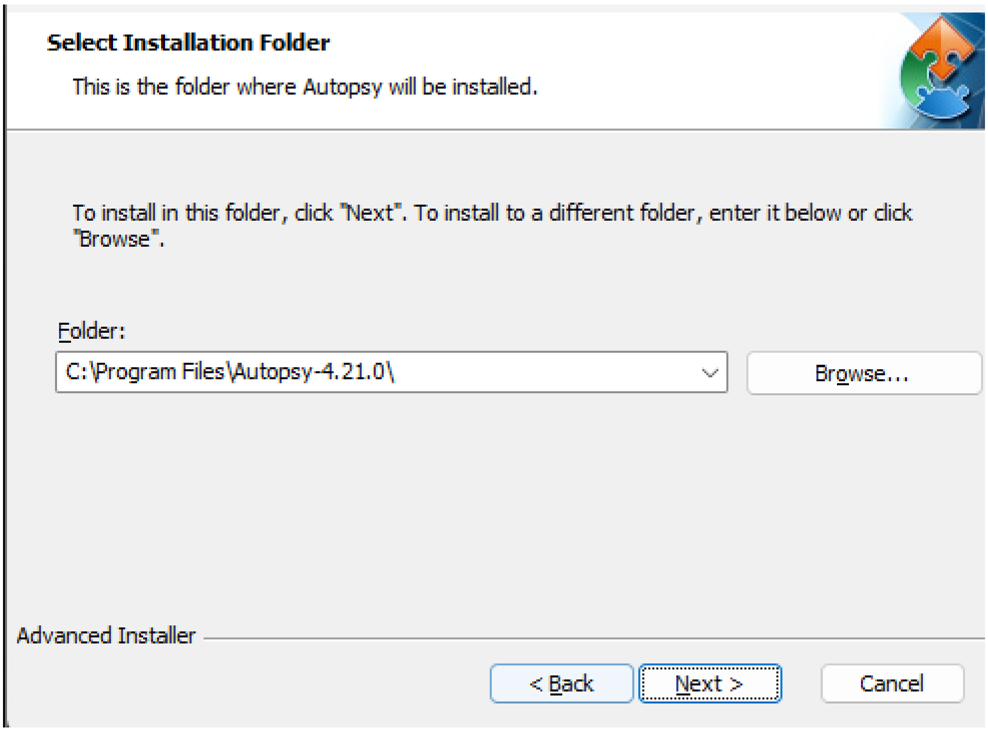
1.DOWNLOAD AUTOPSY:



Autopsy Setup

Welcome to the Autopsy Setup Wizard

The Setup Wizard will install Autopsy on your computer.
Click "Next" to continue or "Cancel" to exit the Setup Wizard.

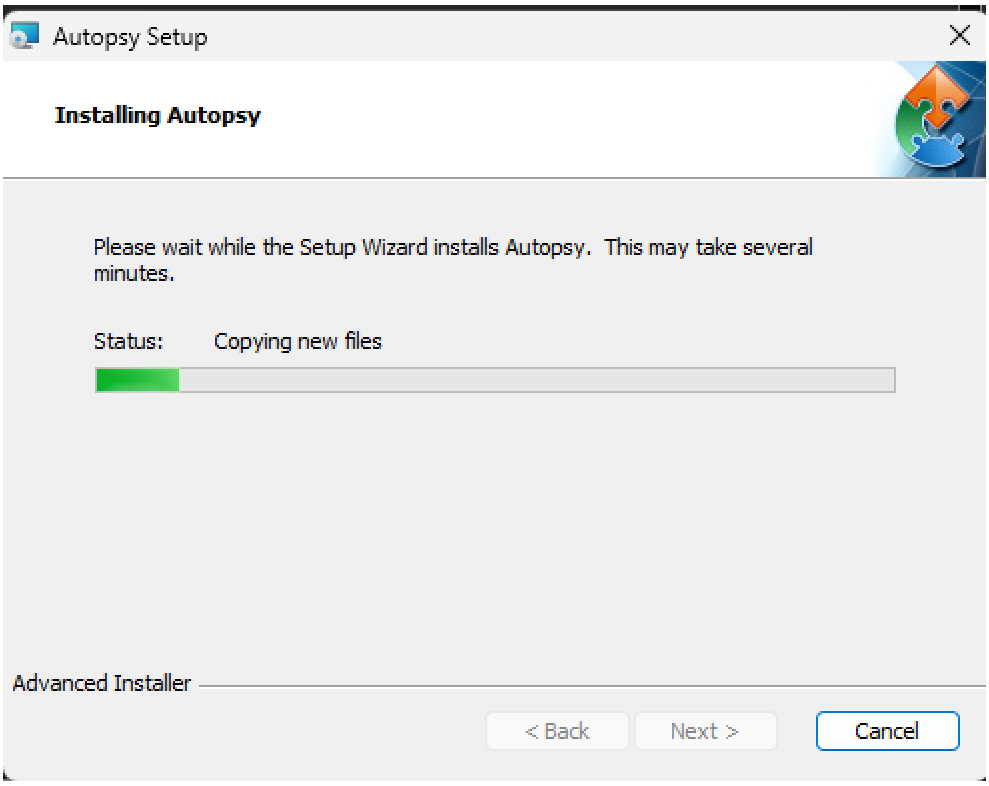


Select Installation Folder

This is the folder where Autopsy will be installed.

To install in this folder, click "Next". To install to a different folder, enter it below or click "Browse".

Folder: C:\Program Files\Autopsy-4.21.0\



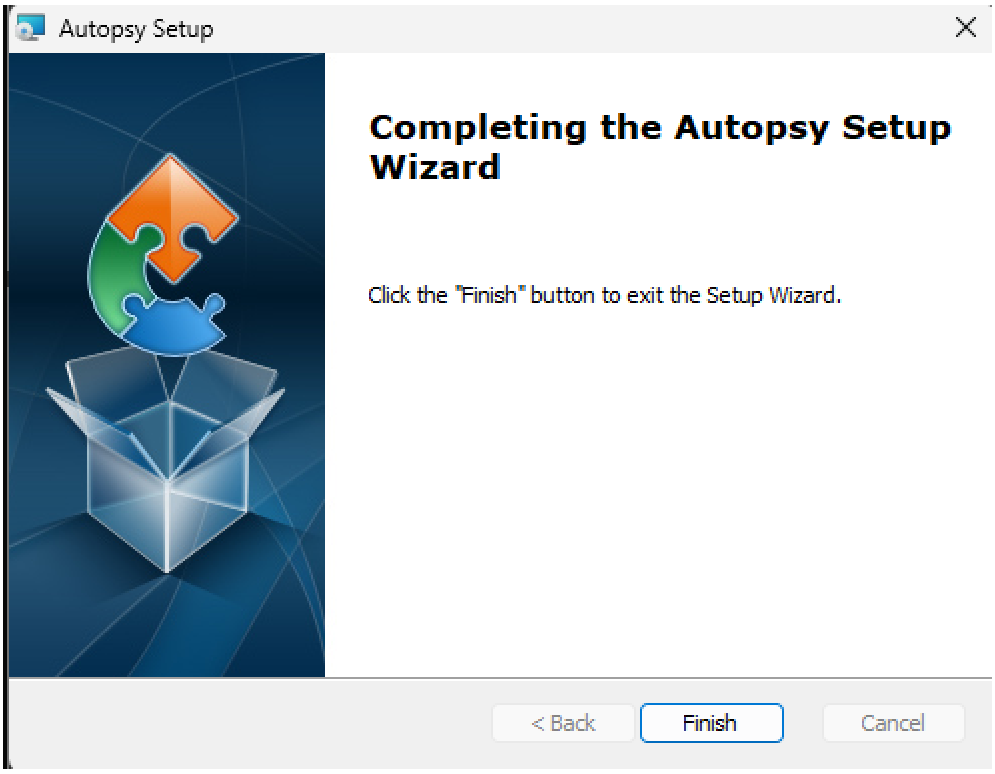
Autopsy Setup

Installing Autopsy

Please wait while the Setup Wizard installs Autopsy. This may take several minutes.

Status: Copying new files

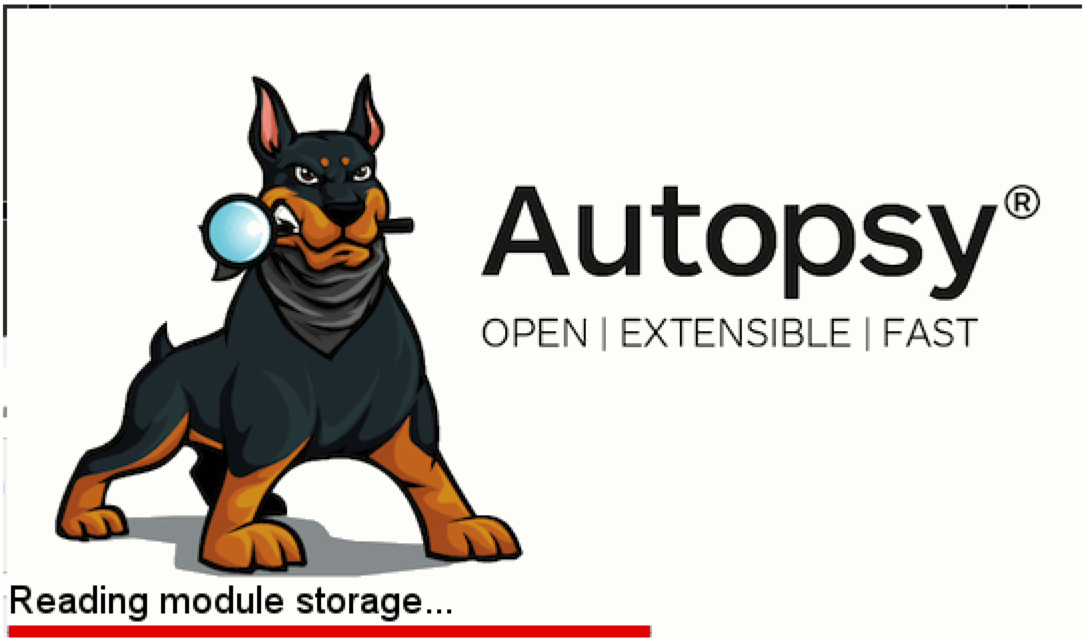
2.SETUP AUTOPSY



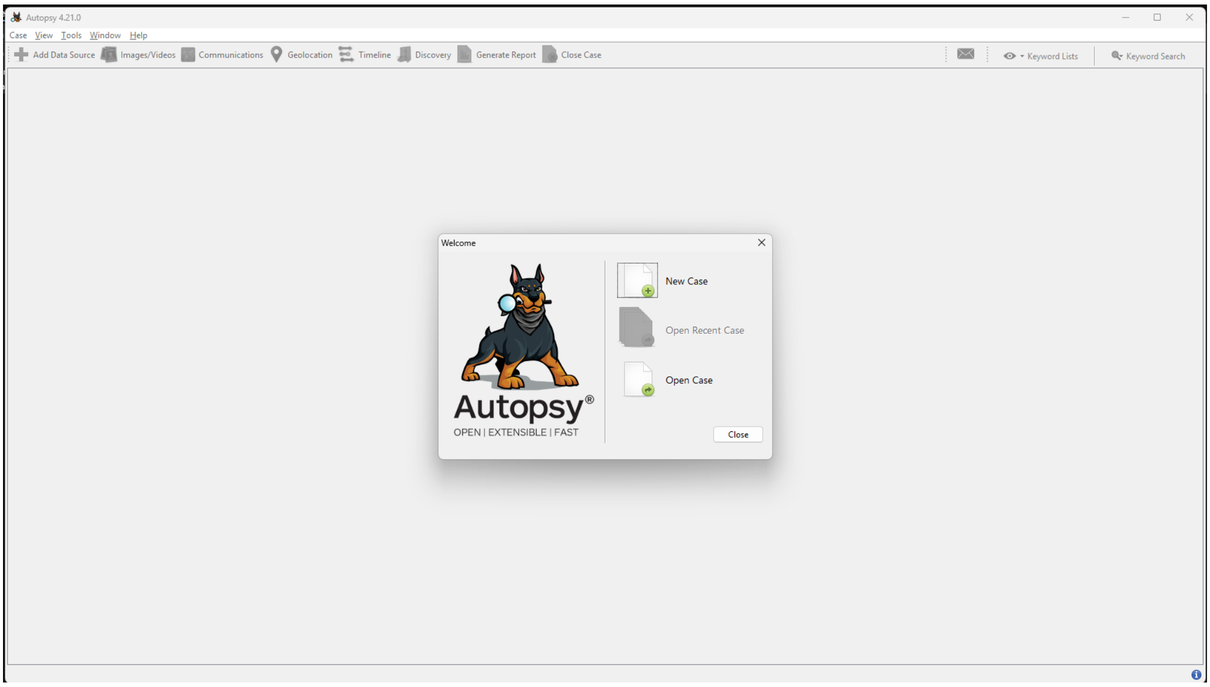
Autopsy Setup

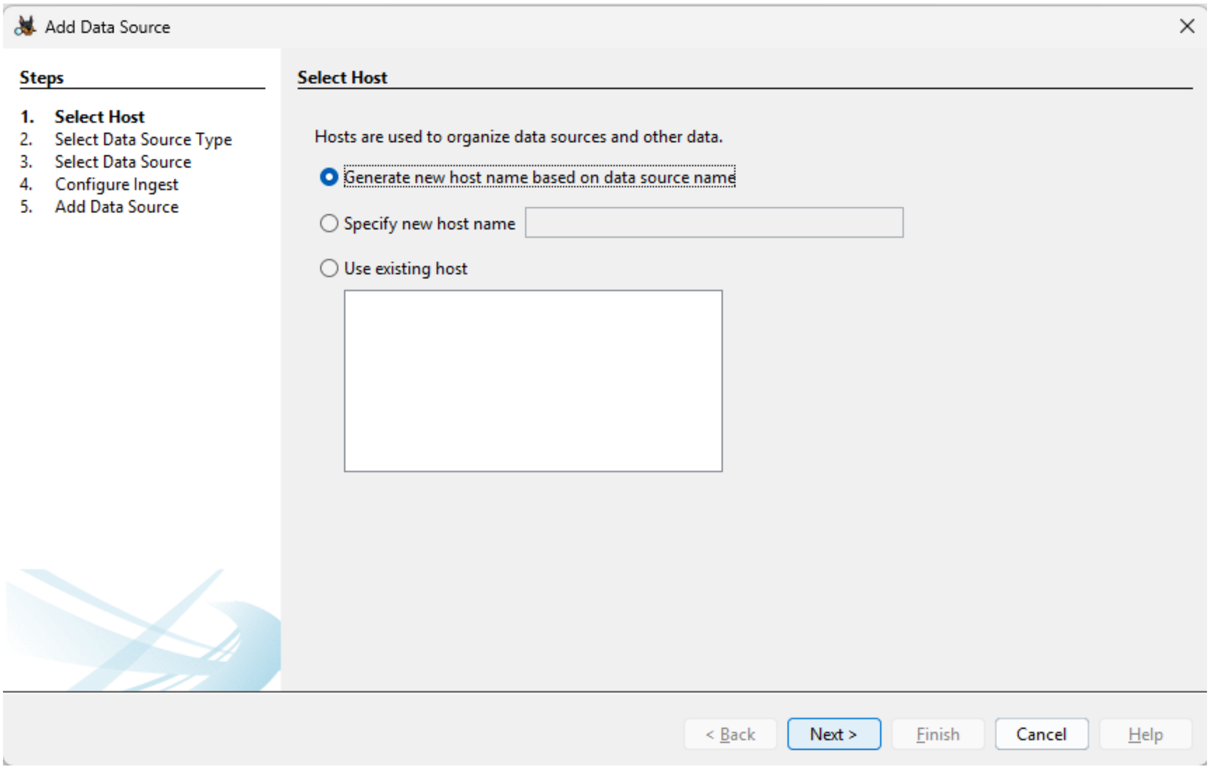
Completing the Autopsy Setup Wizard

Click the "Finish" button to exit the Setup Wizard.



3.ADD THE DATA SOURCE:





Add Data Source

Steps

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

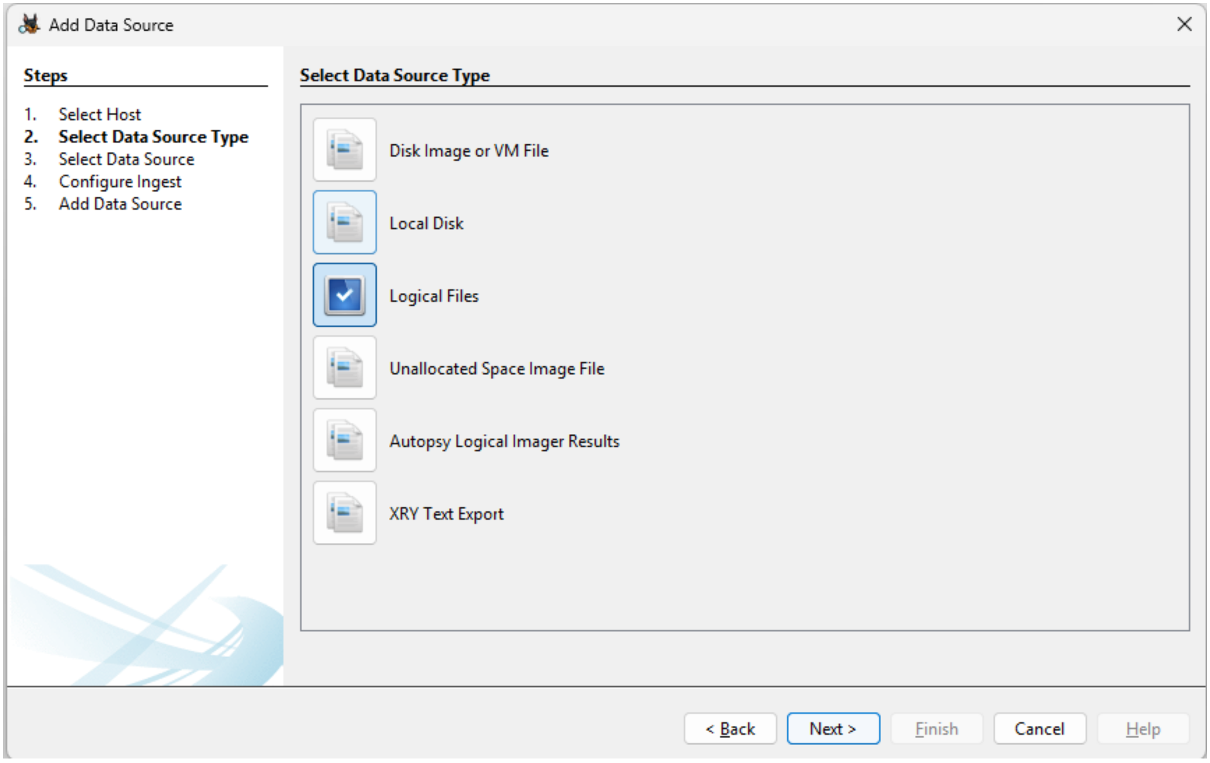
Select Host

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



Add Data Source

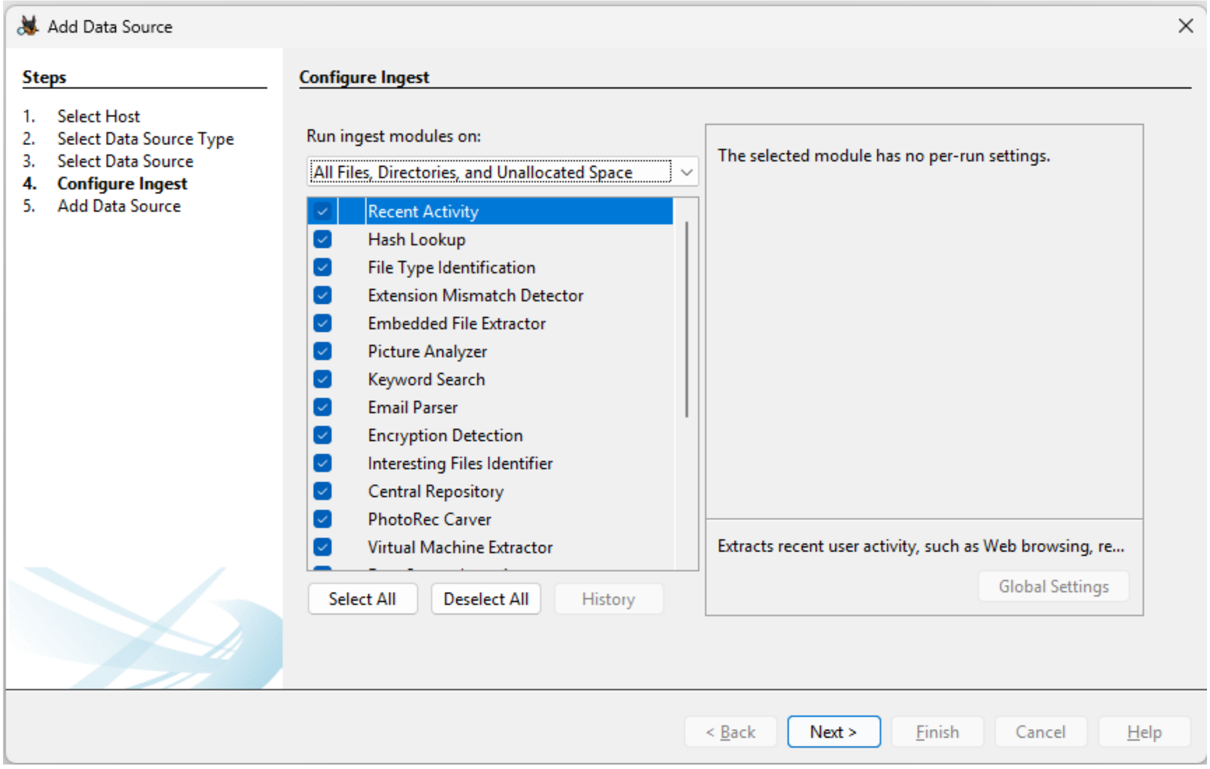
Steps

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
- Local Disk
- ✓ Logical Files
- Unallocated Space Image File
- Autopsy Logical Imager Results
- XRY Text Export

4.CONFIGURE INGEST MODULES



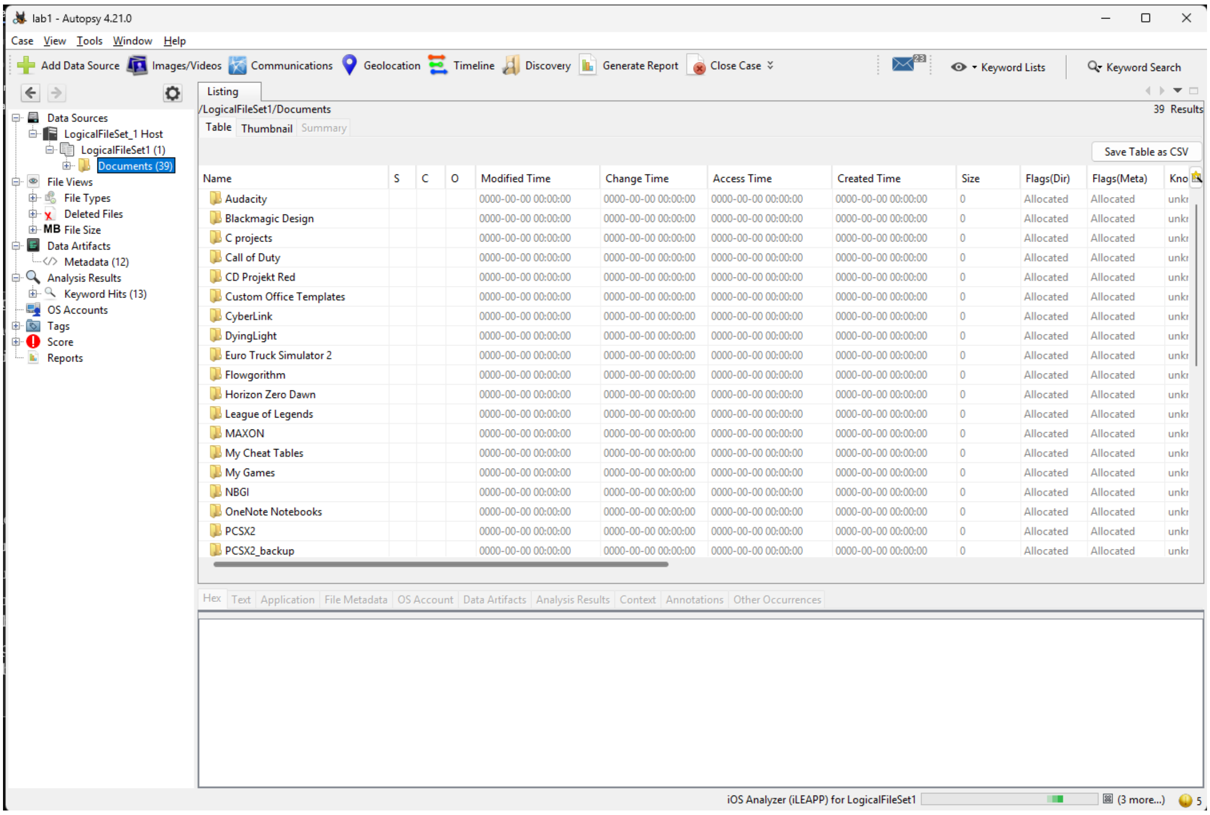
Run ingest modules on: All Files, Directories, and Unallocated Space

- ☑ 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

The selected module has no per-run settings.

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

5.GET THROUGH THE DATA SOURCE

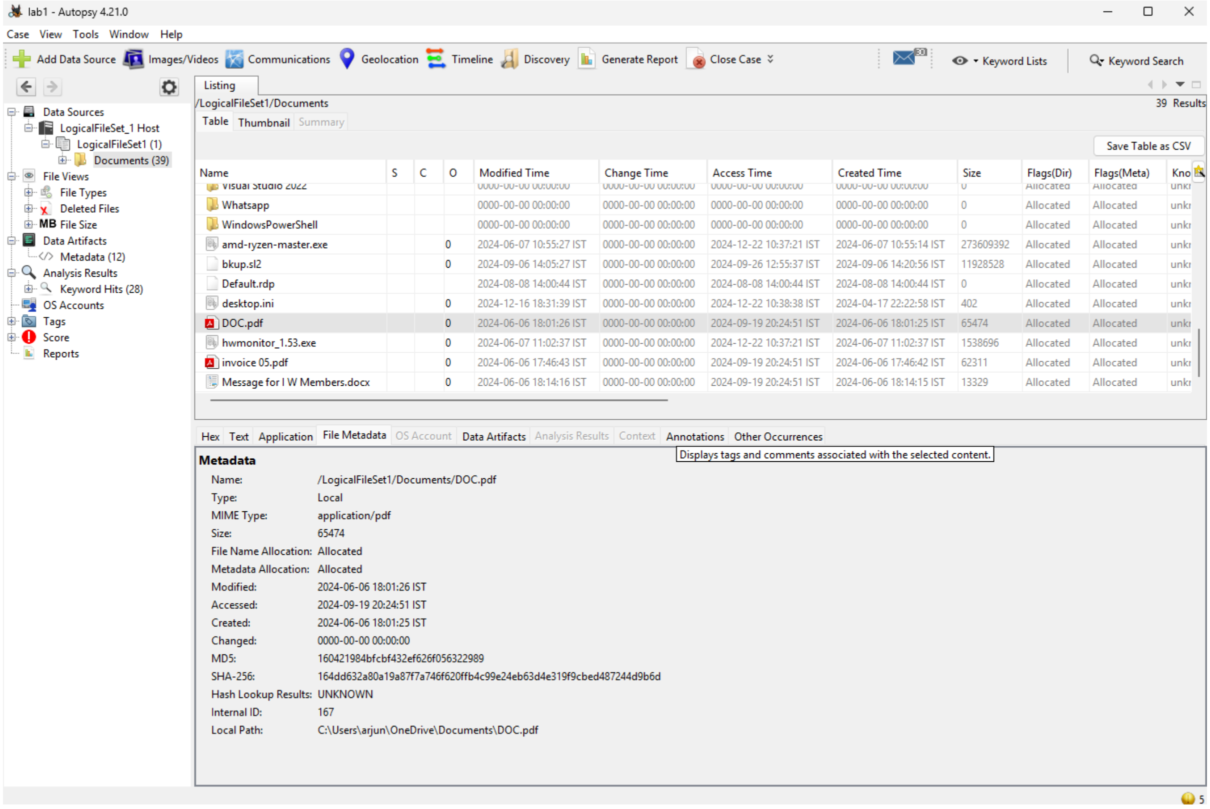


/LogicalFileSet1/Documents

39 Results

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Kno
Audacity				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unkr
Blackmagic Design				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unkr
C projects				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unkr
Call of Duty				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unkr
CD Projekt Red				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unkr
Custom Office Templates				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unkr
CyberLink				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unkr
DyingLight				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unkr
Euro Truck Simulator 2				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unkr
Flowgorithm				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unkr
Horizon Zero Dawn				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unkr
League of Legends				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unkr
MAXON				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unkr
My Cheat Tables				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unkr
My Games				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unkr
NBGI				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unkr
OneNote Notebooks				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unkr
PCSX2				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unkr
PCSX2_backup				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unkr

iOS Analyzer (iLEAPP) for LogicalFileSet1 (3 more...) 5



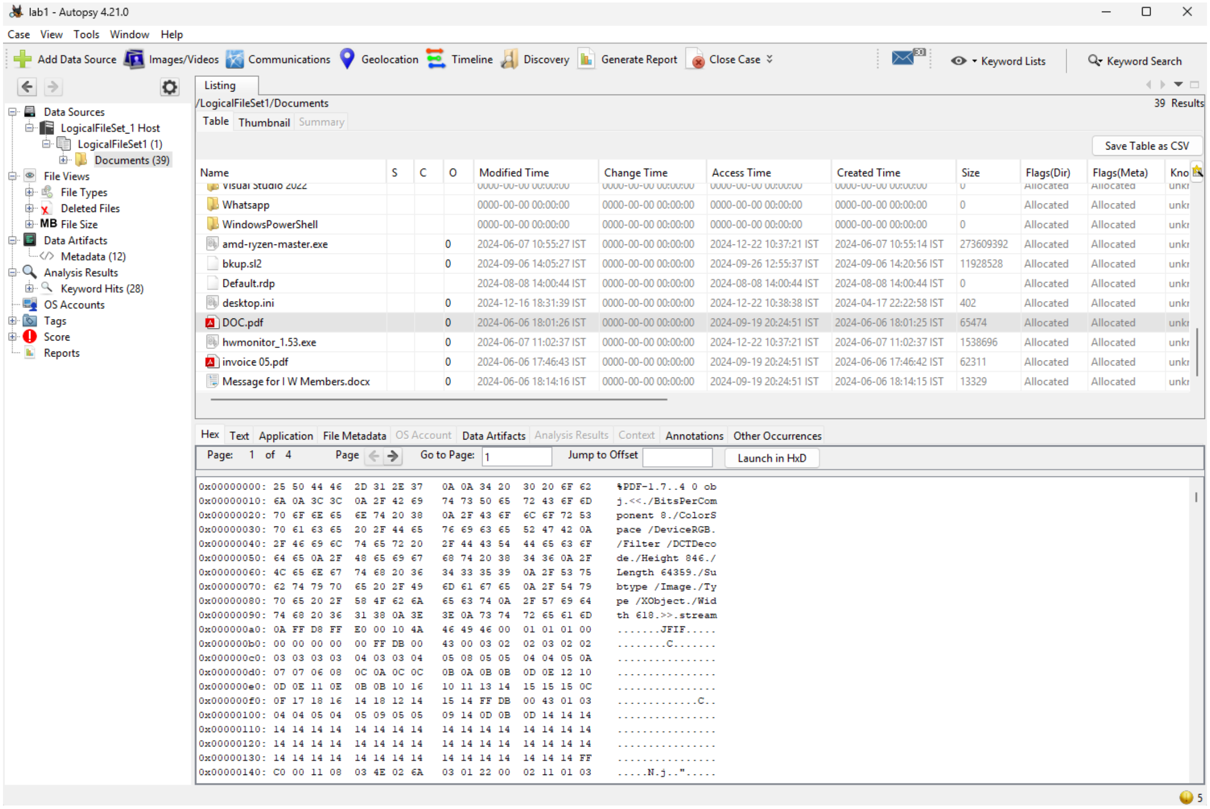
/LogicalFileSet1/Documents

39 Results

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Kno
Visual Studio 2022				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unk
Whatsapp				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unk
WindowsPowerShell				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unk
amd-ryzen-master.exe			0	2024-06-07 10:55:27 IST	0000-00-00 00:00:00	2024-12-22 10:37:21 IST	2024-06-07 10:55:14 IST	273609392	Allocated	Allocated	unk
bkup.sl2			0	2024-09-06 14:05:27 IST	0000-00-00 00:00:00	2024-09-26 12:55:37 IST	2024-09-06 14:20:56 IST	11928528	Allocated	Allocated	unk
Default.rdp				2024-08-08 14:00:44 IST	0000-00-00 00:00:00	2024-08-08 14:00:44 IST	2024-08-08 14:00:44 IST	0	Allocated	Allocated	unk
desktop.ini			0	2024-12-16 18:31:39 IST	0000-00-00 00:00:00	2024-12-22 10:38:38 IST	2024-04-17 22:22:58 IST	402	Allocated	Allocated	unk
DOC.pdf			0	2024-06-06 18:01:26 IST	0000-00-00 00:00:00	2024-09-19 20:24:51 IST	2024-06-06 18:01:25 IST	65474	Allocated	Allocated	unk
hwmonitor_1.53.exe			0	2024-06-07 11:02:37 IST	0000-00-00 00:00:00	2024-12-22 10:37:21 IST	2024-06-07 11:02:37 IST	1538696	Allocated	Allocated	unk
invoice 05.pdf			0	2024-06-06 17:46:43 IST	0000-00-00 00:00:00	2024-09-19 20:24:51 IST	2024-06-06 17:46:42 IST	62311	Allocated	Allocated	unk
Message for I W Members.docx			0	2024-06-06 18:14:16 IST	0000-00-00 00:00:00	2024-09-19 20:24:51 IST	2024-06-06 18:14:15 IST	13329	Allocated	Allocated	unk

Metadata

Name:	/LogicalFileSet1/Documents/DOC.pdf
Type:	Local
MIME Type:	application/pdf
Size:	65474
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2024-06-06 18:01:26 IST
Accessed:	2024-09-19 20:24:51 IST
Created:	2024-06-06 18:01:25 IST
Changed:	0000-00-00 00:00:00
MD5:	160421984bfcbf432ef626f056322989
SHA-256:	164dd632a80a19a87f7a746f620ffb4c99e24eb63d4e319f9cbed487244d9b6d
Hash Lookup Results:	UNKNOWN
Internal ID:	167
Local Path:	C:\Users\arjun\OneDrive\Documents\DOC.pdf



/LogicalFileSet1/Documents

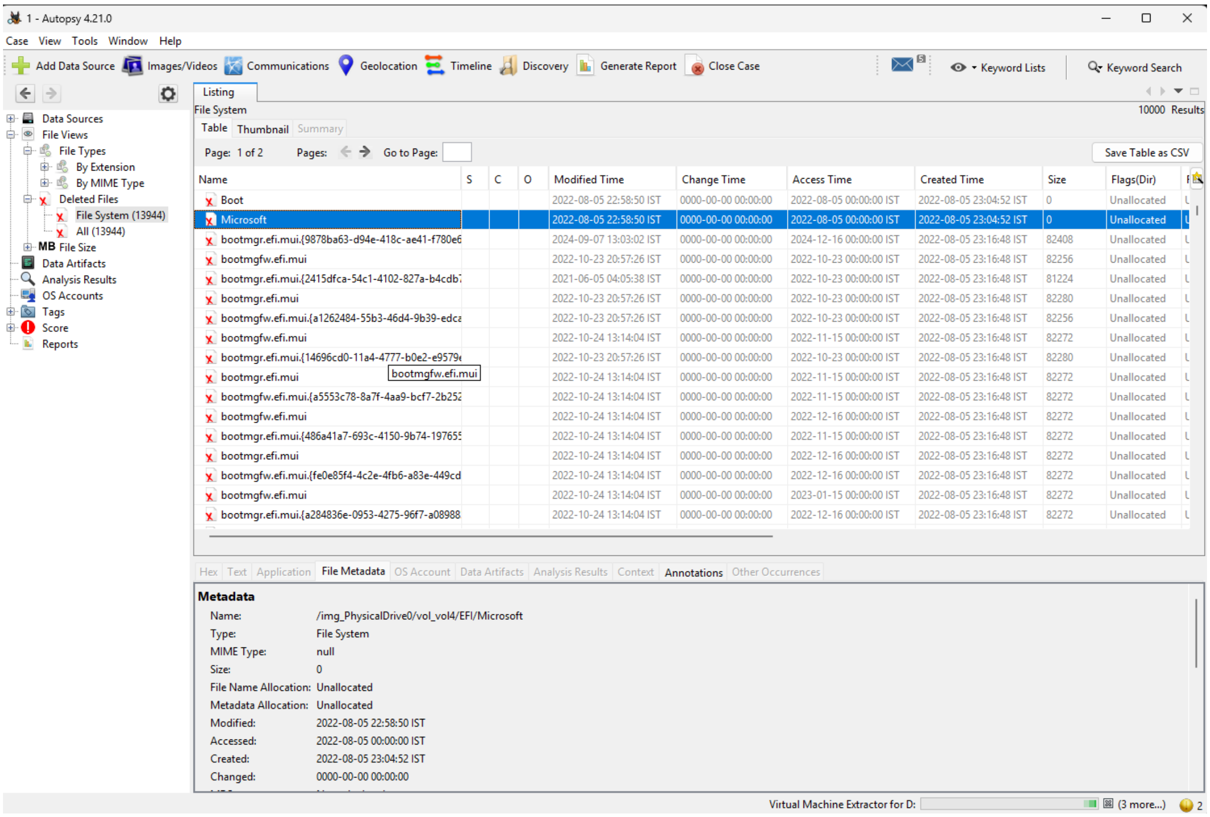
39 Results

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Kno
Visual Studio 2022				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unk
Whatsapp				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unk
WindowsPowerShell				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unk
amd-ryzen-master.exe			0	2024-06-07 10:55:27 IST	0000-00-00 00:00:00	2024-12-22 10:37:21 IST	2024-06-07 10:55:14 IST	273609392	Allocated	Allocated	unk
bkup.sl2			0	2024-09-06 14:05:27 IST	0000-00-00 00:00:00	2024-09-26 12:55:37 IST	2024-09-06 14:20:56 IST	11928528	Allocated	Allocated	unk
Default.rdp				2024-08-08 14:00:44 IST	0000-00-00 00:00:00	2024-08-08 14:00:44 IST	2024-08-08 14:00:44 IST	0	Allocated	Allocated	unk
desktop.ini			0	2024-12-16 18:31:39 IST	0000-00-00 00:00:00	2024-12-22 10:38:38 IST	2024-04-17 22:22:58 IST	402	Allocated	Allocated	unk
DOC.pdf			0	2024-06-06 18:01:26 IST	0000-00-00 00:00:00	2024-09-19 20:24:51 IST	2024-06-06 18:01:25 IST	65474	Allocated	Allocated	unk
hwmonitor_1.53.exe			0	2024-06-07 11:02:37 IST	0000-00-00 00:00:00	2024-12-22 10:37:21 IST	2024-06-07 11:02:37 IST	1538696	Allocated	Allocated	unk
invoice 05.pdf			0	2024-06-06 17:46:43 IST	0000-00-00 00:00:00	2024-09-19 20:24:51 IST	2024-06-06 17:46:42 IST	62311	Allocated	Allocated	unk
Message for I W Members.docx			0	2024-06-06 18:14:16 IST	0000-00-00 00:00:00	2024-09-19 20:24:51 IST	2024-06-06 18:14:15 IST	13329	Allocated	Allocated	unk

Page: 1 of 4 Page Go to Page: 1 Jump to Offset

```
0x00000000: 25 50 44 46  2D 31 2E 37   0A 0A 34 20  30 20 6F 62    %PDF-1.7..4 0 ob
0x00000010: 6A 0A 3C 3C  0A 2F 42 69   74 73 50 65  72 43 6F 6D    j.<<./BitsPerCom
0x00000020: 70 6F 6E 65  6E 74 20 38   0A 2F 43 6F  6C 6F 72 53    ponent 8./ColorS
0x00000030: 70 61 63 65  20 2F 44 65   76 69 63 65  52 47 42 0A    pace /DeviceRGB.
0x00000040: 2F 46 69 6C  74 65 72 20   2F 44 43 54  44 65 63 6F    /Filter /DCTDeco
0x00000050: 64 65 0A 2F  48 65 69 67   68 74 20 38  34 36 0A 2F    de./Height 846./
0x00000060: 4C 65 6E 67  74 68 20 36   34 33 35 39  0A 2F 53 75    Length 64359./Su
0x00000070: 62 74 79 70  65 20 2F 49   6D 61 67 65  0A 2F 54 79    btype /Image./Ty
0x00000080: 70 65 20 2F  58 4F 62 6A   65 63 74 0A  2F 57 69 64    pe /XObject./Wid
0x00000090: 74 68 20 36  31 38 0A 3E   3E 0A 73 74  72 65 61 6D    th 618.>>.stream
0x000000a0: 0A FF D8 FF  E0 00 10 4A   46 49 46 00  01 01 01 00    .......JFIF.....
0x000000b0: 00 00 00 00  00 FF DB 00   43 00 03 02  02 03 02 02    ........C.......
0x000000c0: 03 03 03 03  04 03 03 04   05 08 05 05  04 04 05 0A    ................
0x000000d0: 07 07 06 08  0C 0A 0C 0C   0B 0A 0B 0B  0D 0E 12 10    ................
0x000000e0: 0D 0E 11 0E  0B 0B 10 16   10 11 13 14  15 15 15 0C    ................
0x000000f0: 0F 17 18 16  14 18 12 14   15 14 FF DB  00 43 01 03    .............C..
0x00000100: 04 04 05 04  05 09 05 05   09 14 0D 0B  0D 14 14 14    ................
0x00000110: 14 14 14 14  14 14 14 14   14 14 14 14  14 14 14 14    ................
0x00000120: 14 14 14 14  14 14 14 14   14 14 14 14  14 14 14 14    ................
0x00000130: 14 14 14 14  14 14 14 14   14 14 14 14  14 14 14 FF    ................
0x00000140: C0 00 11 08  03 4E 02 6A   03 01 22 00  02 11 01 03    .....N.j..".....
```

6.UNALLOCATED,DELETED AND EXTRACTED CONTENTS



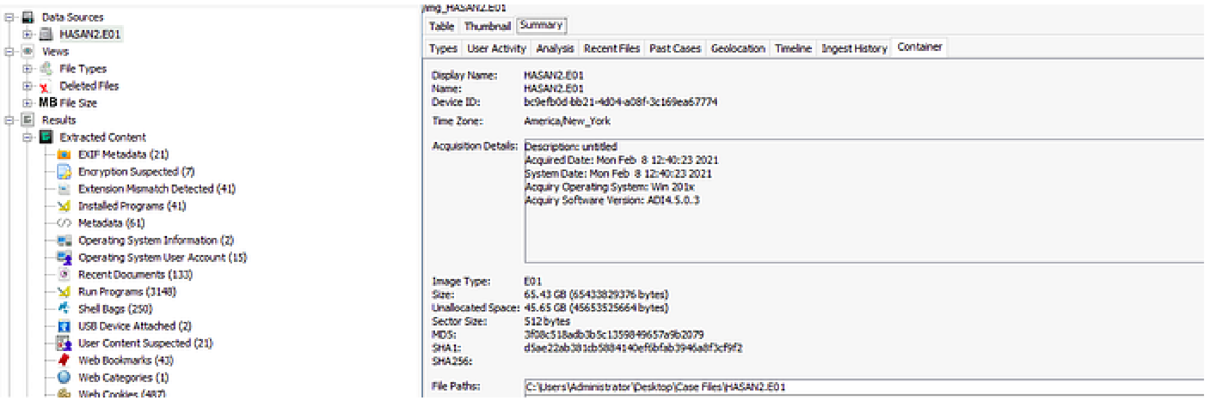
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)
Boot				2022-08-05 22:58:50 IST	0000-00-00 00:00:00	2022-08-05 00:00:00 IST	2022-08-05 23:04:52 IST	0	Unallocated
Microsoft				2022-08-05 22:58:50 IST	0000-00-00 00:00:00	2022-08-05 00:00:00 IST	2022-08-05 23:04:52 IST	0	Unallocated
bootmgr.efi.mui.{9878ba63-d94e-418c-ae41-f780e6				2024-09-07 13:03:02 IST	0000-00-00 00:00:00	2024-12-16 00:00:00 IST	2022-08-05 23:16:48 IST	82408	Unallocated
bootmgfw.efi.mui				2022-10-23 20:57:26 IST	0000-00-00 00:00:00	2022-10-23 00:00:00 IST	2022-08-05 23:16:48 IST	82256	Unallocated
bootmgr.efi.mui.{2415dfca-54c1-4102-827a-b4cdb7				2021-06-05 04:05:38 IST	0000-00-00 00:00:00	2022-10-23 00:00:00 IST	2022-08-05 23:16:48 IST	81224	Unallocated
bootmgr.efi.mui				2022-10-23 20:57:26 IST	0000-00-00 00:00:00	2022-10-23 00:00:00 IST	2022-08-05 23:16:48 IST	82280	Unallocated
bootmgfw.efi.mui.{a1262484-55b3-46d4-9b39-edca				2022-10-23 20:57:26 IST	0000-00-00 00:00:00	2022-10-23 00:00:00 IST	2022-08-05 23:16:48 IST	82256	Unallocated
bootmgfw.efi.mui				2022-10-24 13:14:04 IST	0000-00-00 00:00:00	2022-11-15 00:00:00 IST	2022-08-05 23:16:48 IST	82272	Unallocated
bootmgr.efi.mui.{14696cd0-11a4-4777-b0e2-e9579				2022-10-23 20:57:26 IST	0000-00-00 00:00:00	2022-10-23 00:00:00 IST	2022-08-05 23:16:48 IST	82280	Unallocated
bootmgr.efi.mui				2022-10-24 13:14:04 IST	0000-00-00 00:00:00	2022-11-15 00:00:00 IST	2022-08-05 23:16:48 IST	82272	Unallocated
bootmgfw.efi.mui.{a5553c78-8a7f-4aa9-bcf7-2b252				2022-10-24 13:14:04 IST	0000-00-00 00:00:00	2022-11-15 00:00:00 IST	2022-08-05 23:16:48 IST	82272	Unallocated
bootmgfw.efi.mui				2022-10-24 13:14:04 IST	0000-00-00 00:00:00	2022-12-16 00:00:00 IST	2022-08-05 23:16:48 IST	82272	Unallocated
bootmgr.efi.mui.{486a41a7-693c-4150-9b74-197655				2022-10-24 13:14:04 IST	0000-00-00 00:00:00	2022-11-15 00:00:00 IST	2022-08-05 23:16:48 IST	82272	Unallocated
bootmgr.efi.mui				2022-10-24 13:14:04 IST	0000-00-00 00:00:00	2022-12-16 00:00:00 IST	2022-08-05 23:16:48 IST	82272	Unallocated
bootmgfw.efi.mui.{fe0e85f4-4c2e-4fb6-a83e-449cd				2022-10-24 13:14:04 IST	0000-00-00 00:00:00	2022-12-16 00:00:00 IST	2022-08-05 23:16:48 IST	82272	Unallocated
bootmgfw.efi.mui				2022-10-24 13:14:04 IST	0000-00-00 00:00:00	2023-01-15 00:00:00 IST	2022-08-05 23:16:48 IST	82272	Unallocated
bootmgr.efi.mui.{a284836e-0953-4275-96f7-a08988				2022-10-24 13:14:04 IST	0000-00-00 00:00:00	2022-12-16 00:00:00 IST	2022-08-05 23:16:48 IST	82272	Unallocated

bootmgfw.efi.mui

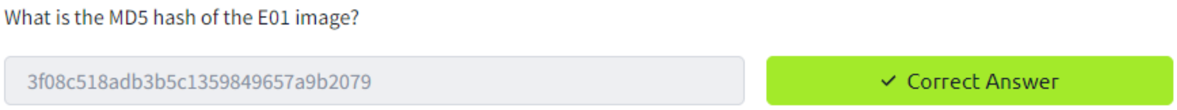
Metadata

Name: /img_PhysicalDrive0/vol_vol4/EFI/Microsoft
Type: File System
MIME Type: null
Size: 0
File Name Allocation: Unallocated
Metadata Allocation: Unallocated
Modified: 2022-08-05 22:58:50 IST
Accessed: 2022-08-05 00:00:00 IST
Created: 2022-08-05 23:04:52 IST
Changed: 0000-00-00 00:00:00

DISK ANALYSIS AND AUTOPSY USING TRYHACKME

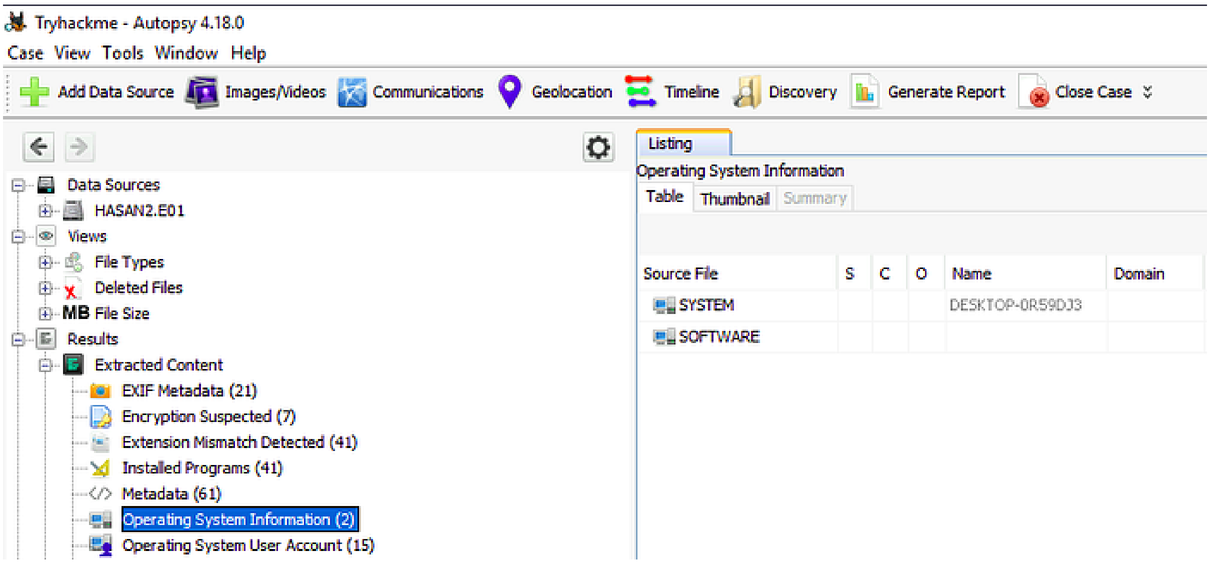


Display Name: HASAN2.E01
Name: HASAN2.E01
Device ID: bc9efb0d-bb21-4d04-a08f-3c169ea67774
Time Zone: America/New_York
Acquisition Details: Description: untitled
Acquired Date: Mon Feb 8 12:40:23 2021
System Date: Mon Feb 8 12:40:23 2021
Acquiry Operating System: Win 201x
Acquiry Software Version: ADI4.5.0.3
Image Type: E01
Size: 65.43 GB (65433829376 bytes)
Unallocated Space: 45.65 GB (45653525664 bytes)
Sector Size: 512 bytes
MD5: 3f08c518adb3b5c1359849657a9b2079
SHA1: d5ae22ab381cb5884140ef6bfab3946a8f3cf9f2
SHA256:
File Paths: C:\Users\Administrator\Desktop\Case Files\HASAN2.E01



What is the MD5 hash of the E01 image?

3f08c518adb3b5c1359849657a9b2079



Data Sources
HASAN2.E01
Views
File Types
Deleted Files
MB File Size
Results
Extracted Content
EXIF Metadata (21)
Encryption Suspected (7)
Extension Mismatch Detected (41)
Installed Programs (41)
Metadata (61)
Operating System Information (2)
Operating System User Account (15)

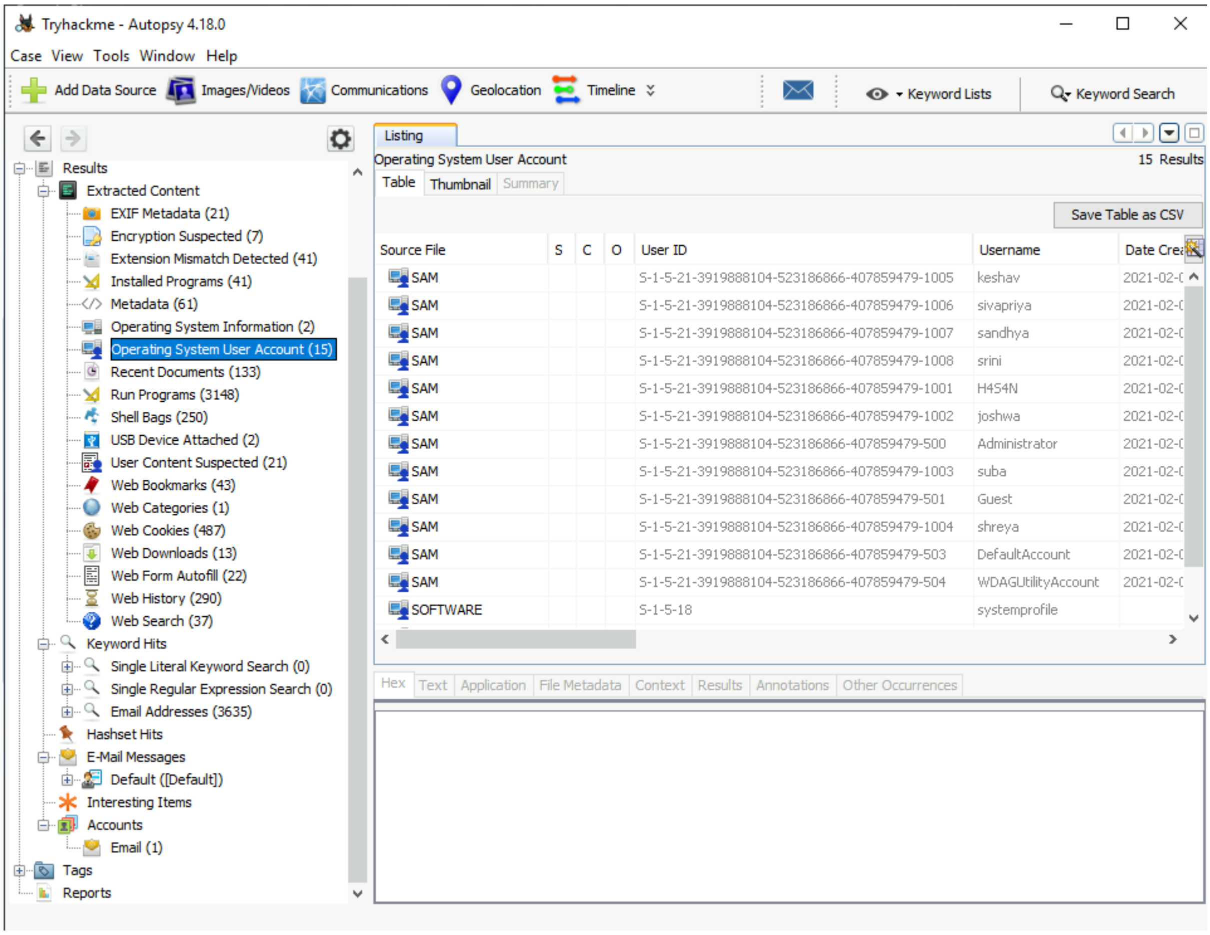
Operating System Information

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

What is the computer account name?

DESKTOP-0R59DJ3

✓ Correct Answer



Results
Extracted Content
EXIF Metadata (21)
Encryption Suspected (7)
Extension Mismatch Detected (41)
Installed Programs (41)
Metadata (61)
Operating System Information (2)
Operating System User Account (15)
Recent Documents (133)
Run Programs (3148)
Shell Bags (250)
USB Device Attached (2)
User Content Suspected (21)
Web Bookmarks (43)
Web Categories (1)
Web Cookies (487)
Web Downloads (13)
Web Form Autofill (22)
Web History (290)
Web Search (37)
Keyword Hits
Single Literal Keyword Search (0)
Single Regular Expression Search (0)
Email Addresses (3635)
Hashset Hits
E-Mail Messages
Default ([Default])
Interesting Items
Accounts
Email (1)
Tags
Reports

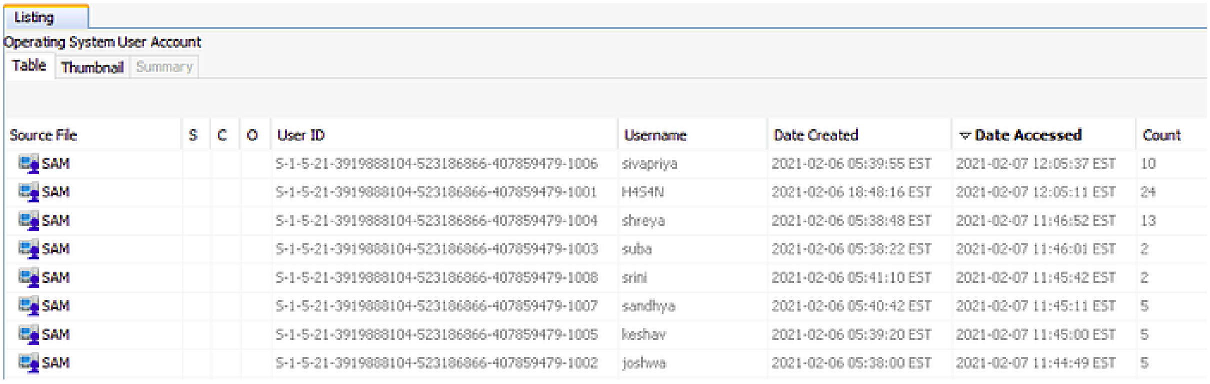
Operating System User Account 15 Results

Source File	S	C	O	User ID	Username	Date Cre
SAM				S-1-5-21-3919888104-523186866-407859479-1005	keshav	2021-02-(
SAM				S-1-5-21-3919888104-523186866-407859479-1006	sivapriya	2021-02-(
SAM				S-1-5-21-3919888104-523186866-407859479-1007	sandhya	2021-02-(
SAM				S-1-5-21-3919888104-523186866-407859479-1008	srini	2021-02-(
SAM				S-1-5-21-3919888104-523186866-407859479-1001	H4S4N	2021-02-(
SAM				S-1-5-21-3919888104-523186866-407859479-1002	joshwa	2021-02-(
SAM				S-1-5-21-3919888104-523186866-407859479-500	Administrator	2021-02-(
SAM				S-1-5-21-3919888104-523186866-407859479-1003	suba	2021-02-(
SAM				S-1-5-21-3919888104-523186866-407859479-501	Guest	2021-02-(
SAM				S-1-5-21-3919888104-523186866-407859479-1004	shreya	2021-02-(
SAM				S-1-5-21-3919888104-523186866-407859479-503	DefaultAccount	2021-02-(
SAM				S-1-5-21-3919888104-523186866-407859479-504	WDAGUtilityAccount	2021-02-(
SOFTWARE				S-1-5-18	systemprofile	

List all the user accounts. (alphabetical order)

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

✓ Correct Answer



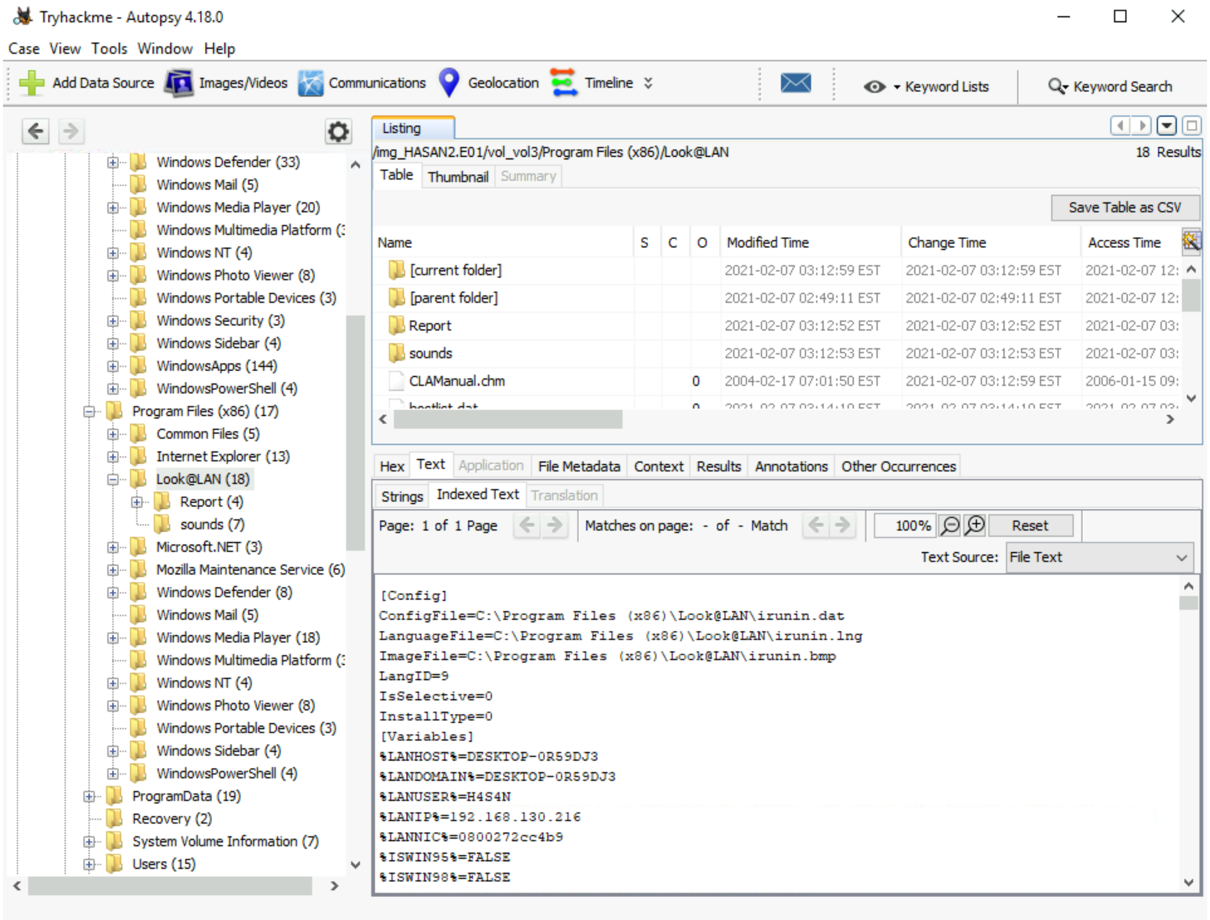
Operating System User Account

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	srini	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



/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:

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

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

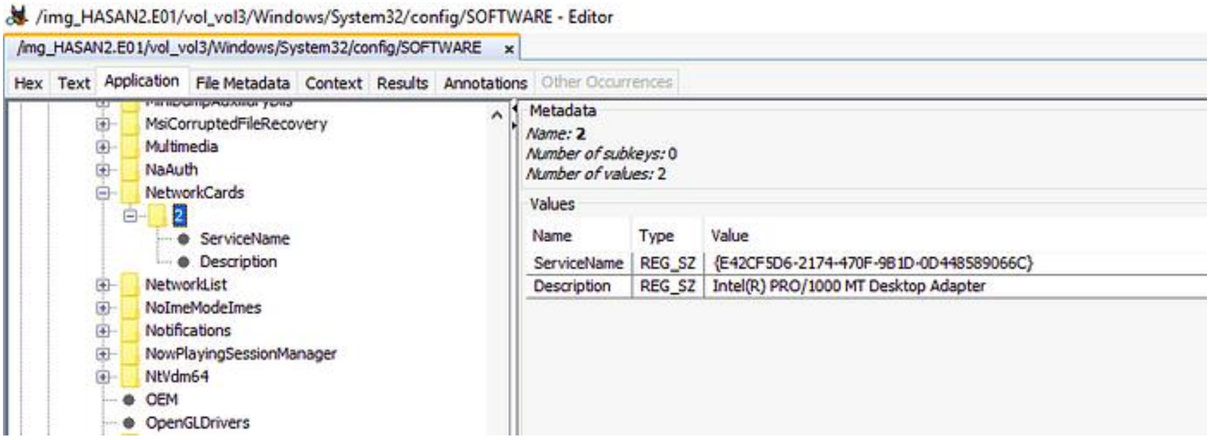
08-00-27-2c-c4-b9

✓ Correct Answer

What is the name of the network monitoring tool?

Look@LAN

✓ Correct Answer



Metadata

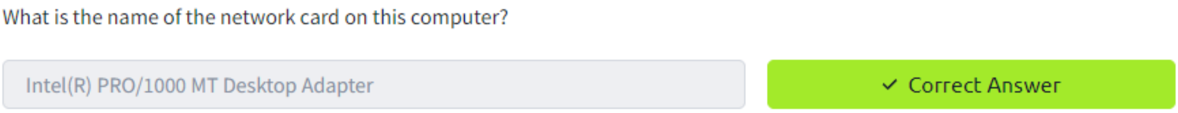
Name: **2**

Number of subkeys: 0

Number of values: 2

Values

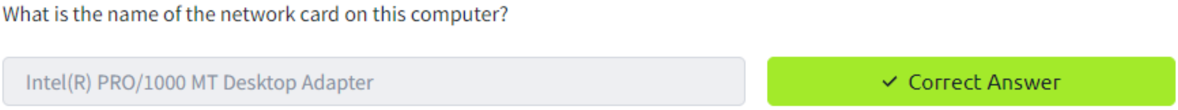
Name	Type	Value
ServiceName	REG_SZ	{E42CF5D6-2174-470F-9B1D-0D448589066C}
Description	REG_SZ	Intel(R) PRO/1000 MT Desktop Adapter



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

Intel(R) PRO/1000 MT Desktop Adapter

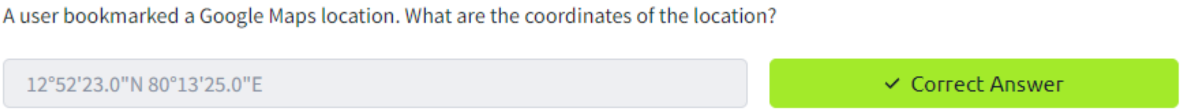
✓ Correct Answer



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

Intel(R) PRO/1000 MT Desktop Adapter

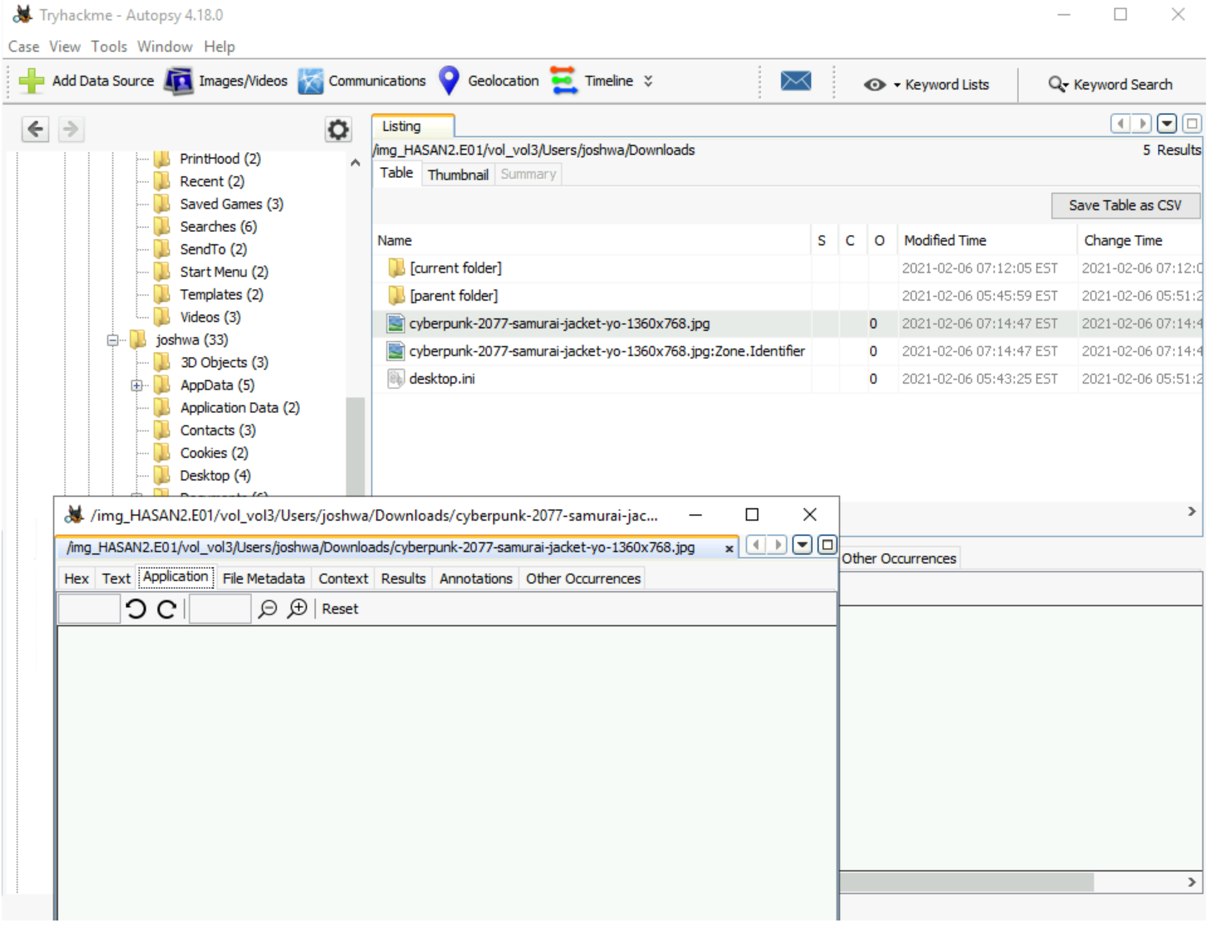
✓ Correct Answer



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



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

5 Results

Name	S	C	O	Modified Time	Change Time
[current folder]				2021-02-06 07:12:05 EST	2021-02-06 07:12:0
[parent folder]				2021-02-06 05:45:59 EST	2021-02-06 05:51:2
cyberpunk-2077-samurai-jacket-yo-1360x768.jpg			0	2021-02-06 07:14:47 EST	2021-02-06 07:14:4
cyberpunk-2077-samurai-jacket-yo-1360x768.jpg:Zone.Identifier			0	2021-02-06 07:14:47 EST	2021-02-06 07:14:4
desktop.ini			0	2021-02-06 05:43:25 EST	2021-02-06 05:51:2

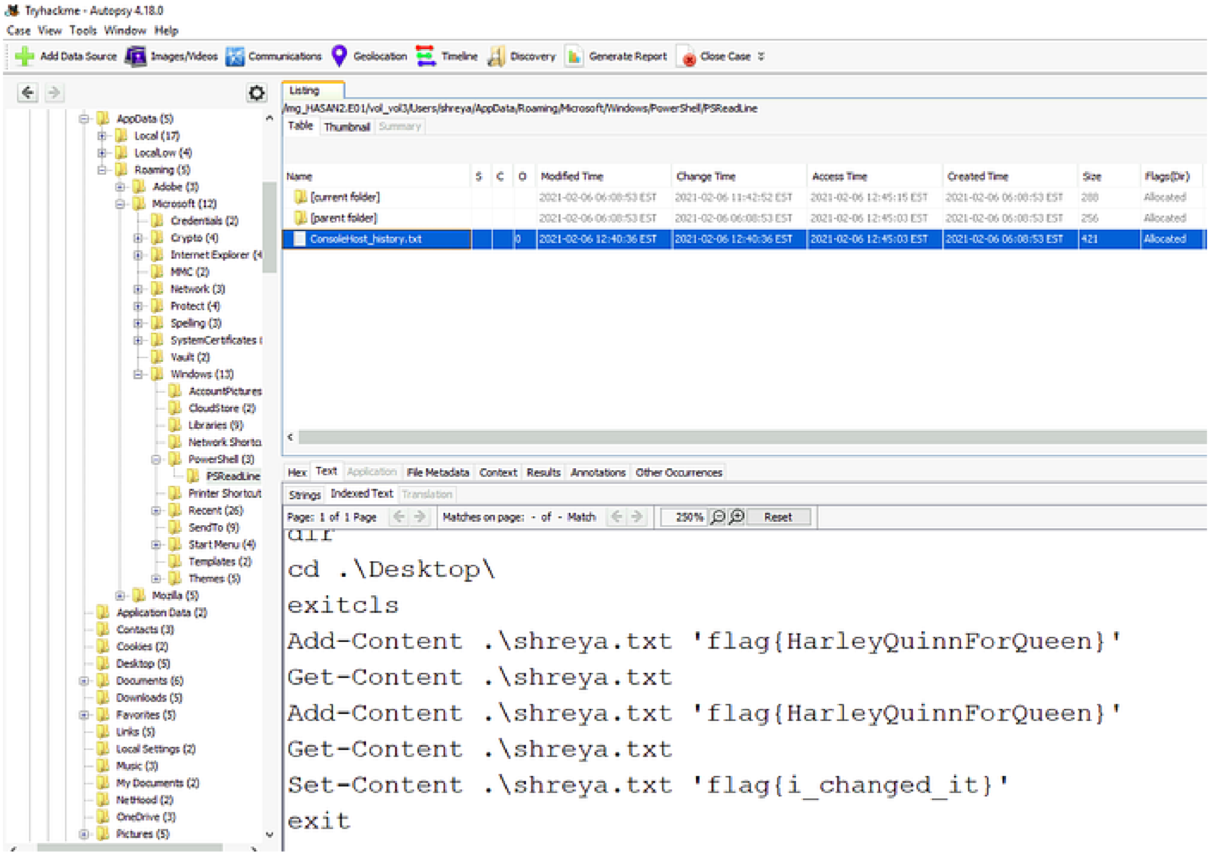
/img_HASAN2.E01/vol_vol3/Users/joshwa/Downloads/cyberpunk-2077-samurai-jac...

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

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

Anto Joshwa

✓ Correct Answer



/img_HASAN2.E01/vol_vol3/Users/shreya/AppData/Roaming/Microsoft/Windows/PowerShell/PSReadLine

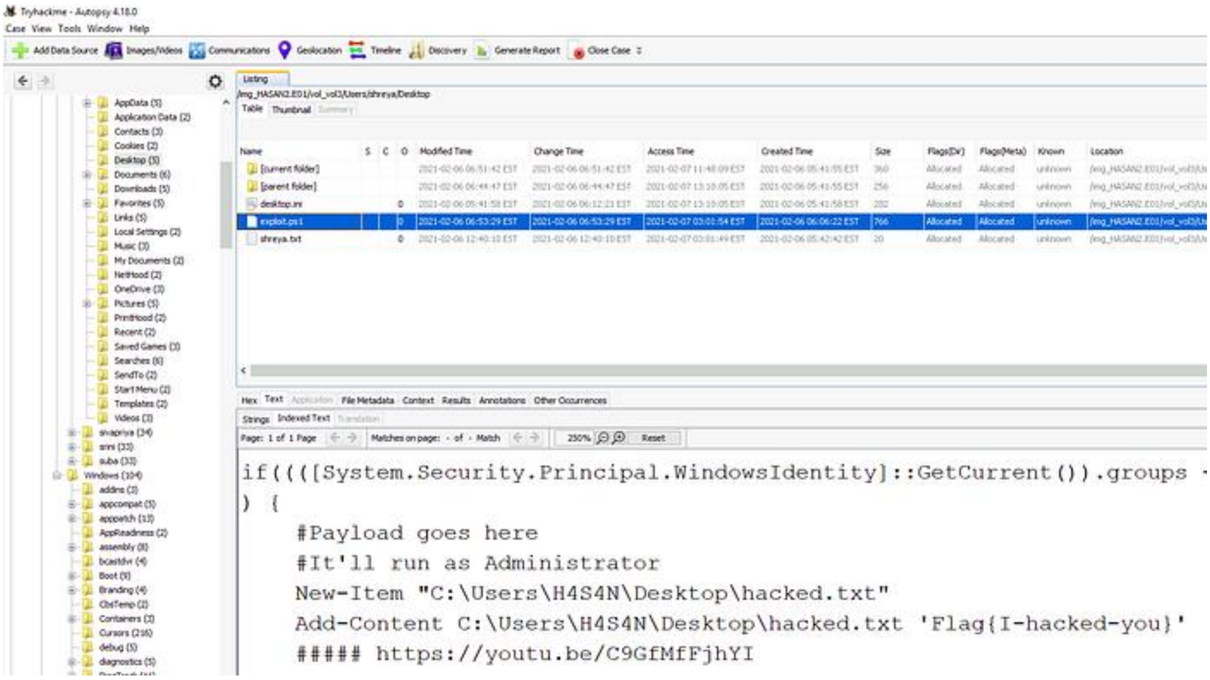
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)
[current folder]				2021-02-06 06:08:53 EST	2021-02-06 11:42:52 EST	2021-02-06 12:45:15 EST	2021-02-06 06:08:53 EST	288	Allocated
[parent folder]				2021-02-06 06:08:53 EST	2021-02-06 06:08:53 EST	2021-02-06 12:45:03 EST	2021-02-06 06:08:53 EST	256	Allocated
ConsoleHost_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 06:08:53 EST	421	Allocated

```
dir
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



/img_HASAN2.E01/vol_vol3/Users/shreya/Desktop

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	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/vol_vol3/Us
[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/vol_vol3/Us
desktop.ini			0	2021-02-06 05:41:58 EST	2021-02-06 06:12:23 EST	2021-02-07 13:10:05 EST	2021-02-06 05:41:58 EST	282	Allocated	Allocated	unknown	/img_HASAN2.E01/vol_vol3/Us
exploit.ps1			0	2021-02-06 06:53:29 EST	2021-02-06 06:53:29 EST	2021-02-07 03:01:54 EST	2021-02-06 06:06:22 EST	766	Allocated	Allocated	unknown	/img_HASAN2.E01/vol_vol3/Us
shreya.txt			0	2021-02-06 12:40:10 EST	2021-02-06 12:40:10 EST	2021-02-07 03:01:49 EST	2021-02-06 05:42:42 EST	20	Allocated	Allocated	unknown	/img_HASAN2.E01/vol_vol3/Us

```
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?

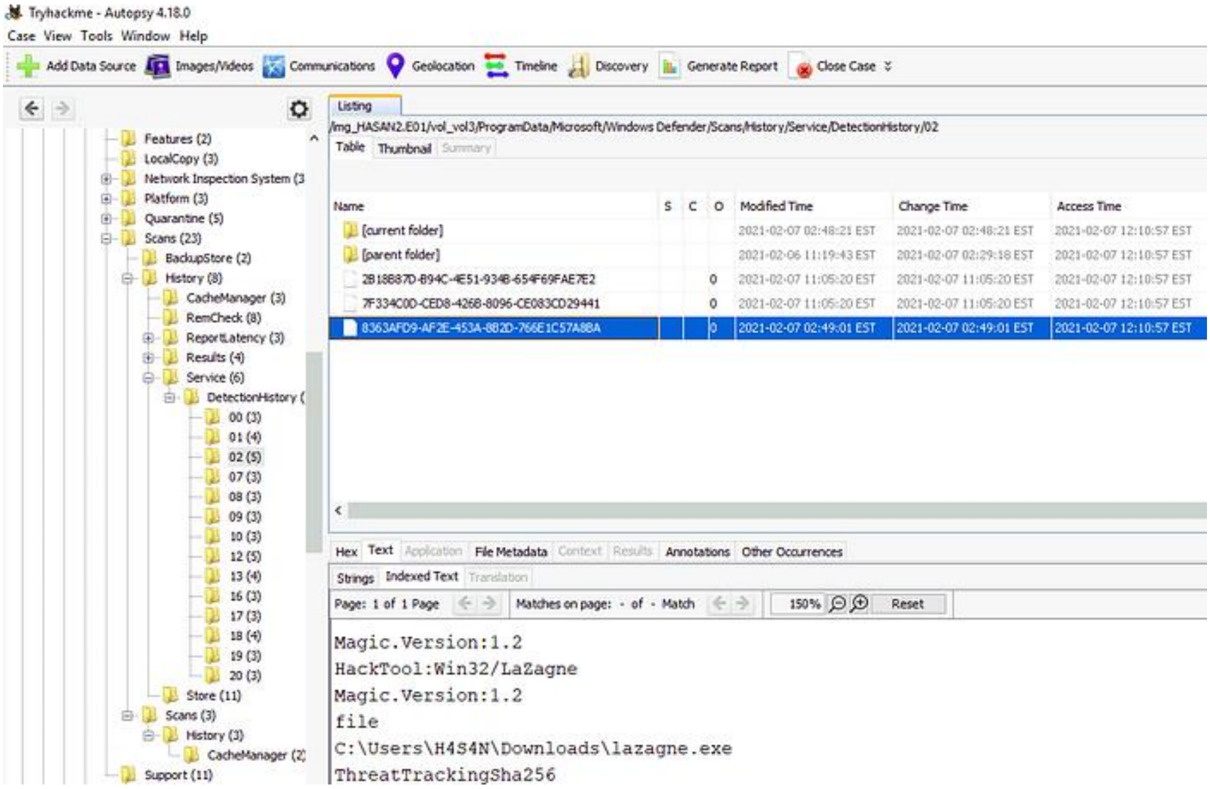
flag{I-hacked-you}

✓ Correct Answer

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



/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 02:29:18 EST	2021-02-07 12:10:57 EST
2B18887D-894C-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-766E1C57A8BA			0	2021-02-07 02:49:01 EST	2021-02-07 02:49:01 EST	2021-02-07 12:10:57 EST

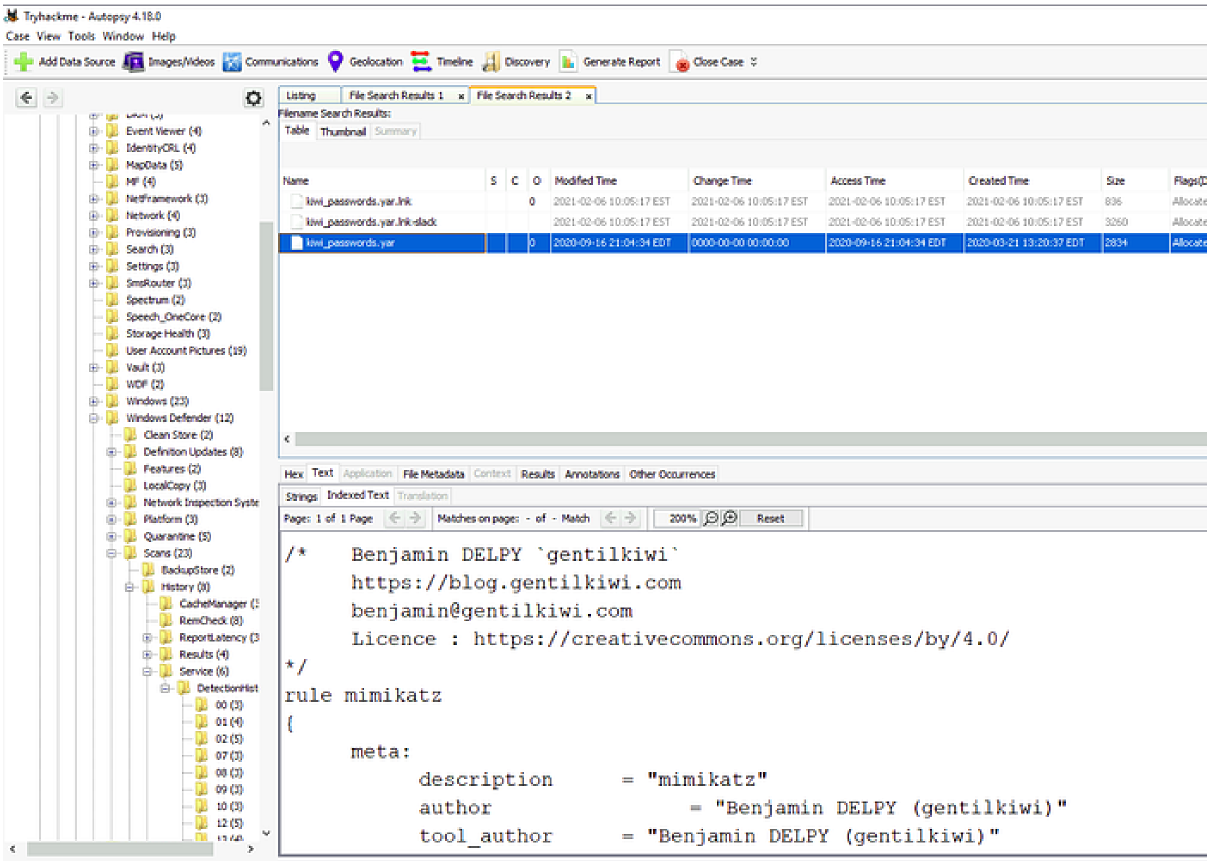
```
Magic.Version:1.2
HackTool:Win32/LaZagne
Magic.Version:1.2
file
C:\Users\H4S4N\Downloads\lazagne.exe
ThreatTrackingSha256
```

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



Filename Search Results:

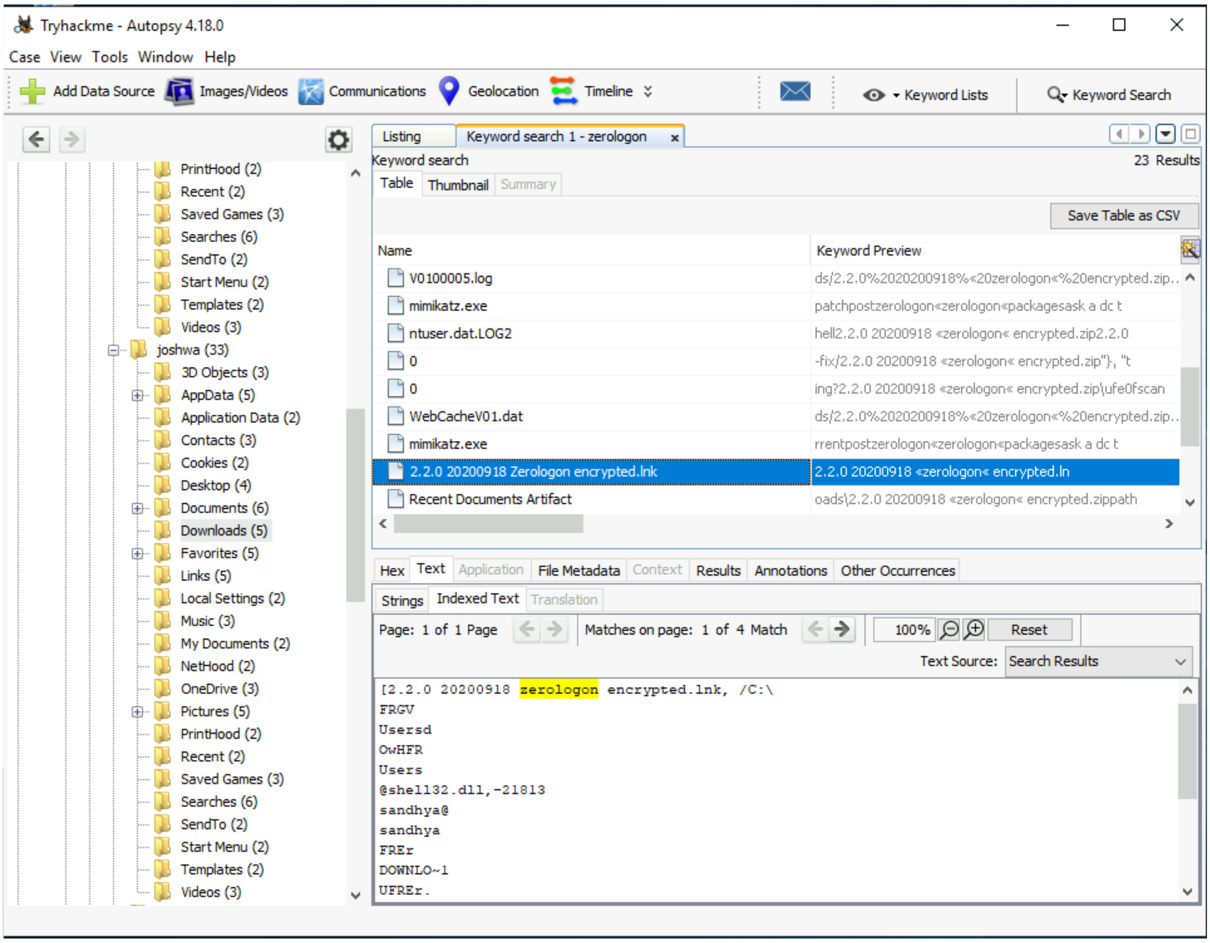
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(D
kiwi_passwords.yar.lnk			0	2021-02-06 10:05:17 EST	2021-02-06 10:05:17 EST	2021-02-06 10:05:17 EST	2021-02-06 10:05:17 EST	836	Allocate
kiwi_passwords.yar.lnk-slack				2021-02-06 10:05:17 EST	2021-02-06 10:05:17 EST	2021-02-06 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	2020-03-21 13:20:37 EDT	2834	Allocate

```
/*    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)

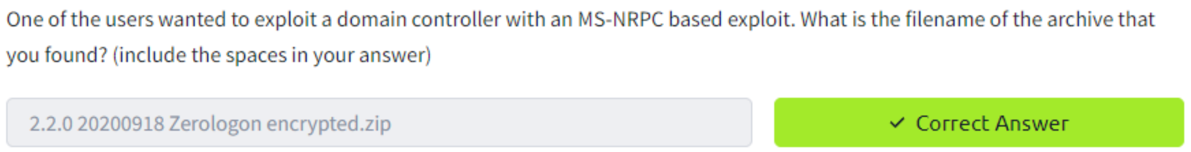
✓ Correct Answer



Keyword search — 23 Results

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

```
[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