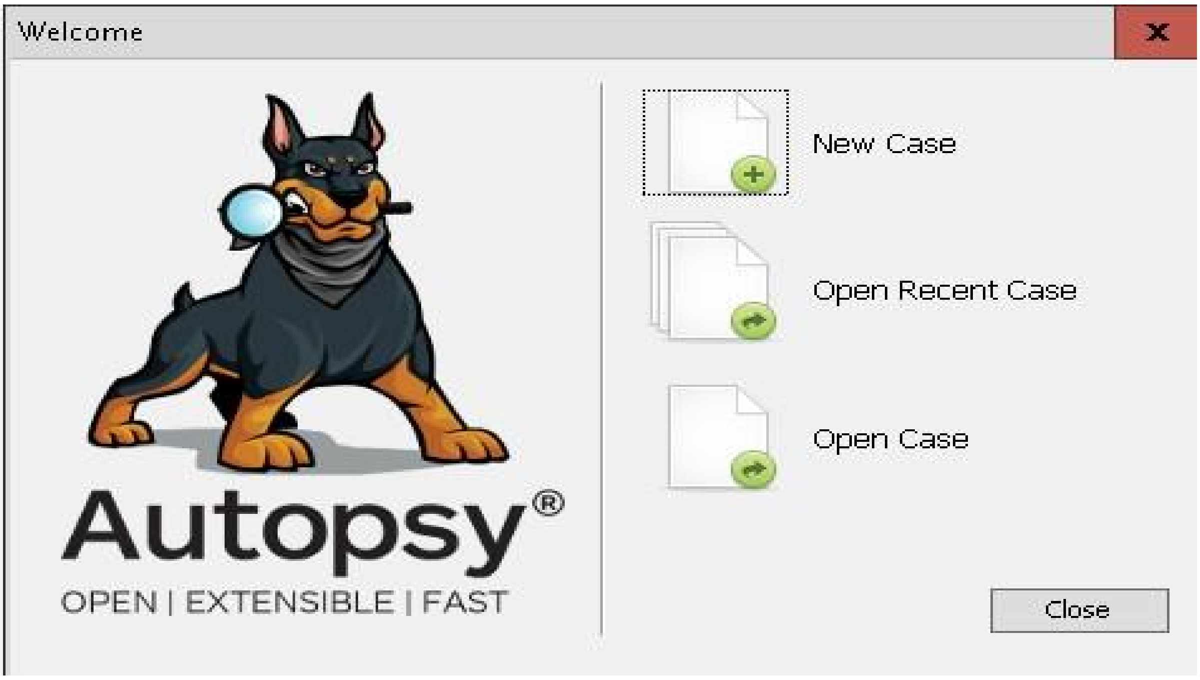
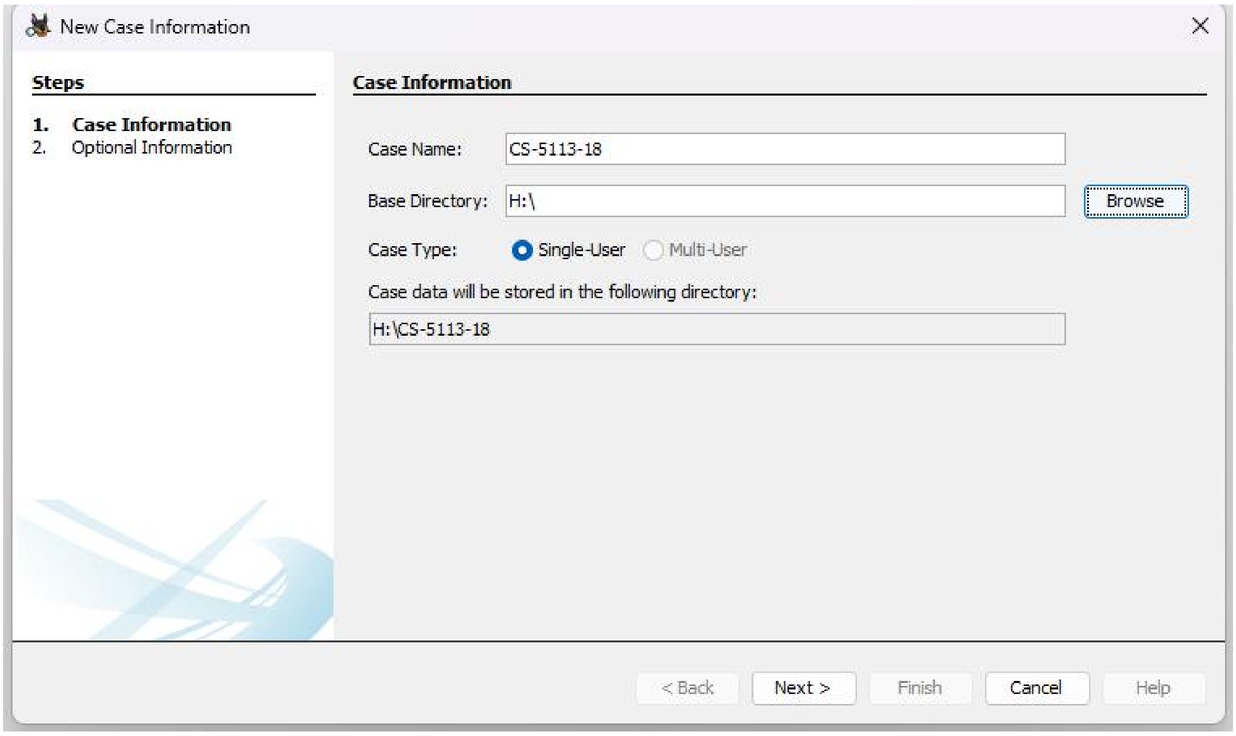
Title: Forensic Case Study: Solve the Case Study (ImageFile) provided in lab using Encase Investigator or Autopsy.

Step 1: Open Autopsy and Create a New Case.



Step 2: Enter Case Name and Base Directory where case will be stored.



Case Name: CS-5113-18

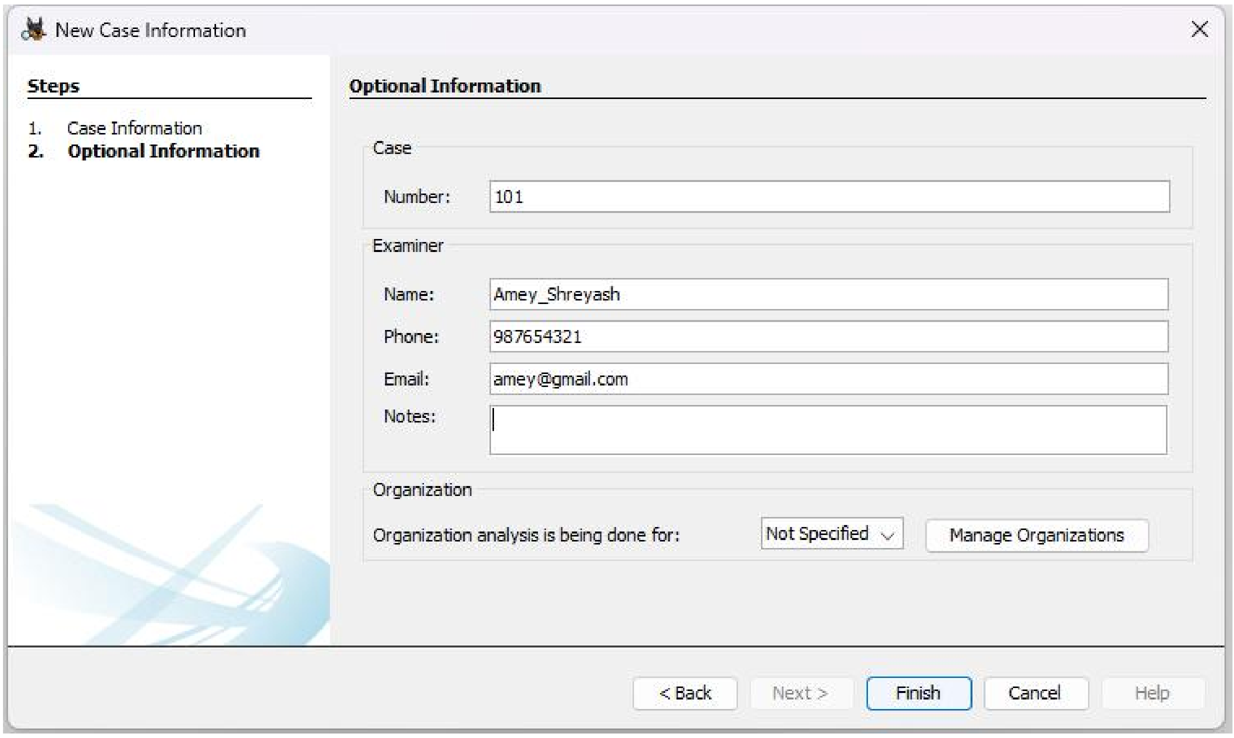
Base Directory: H:\

Case Type: ● Single-User ○ Multi-User

Case data will be stored in the following directory:

H:\CS-5113-18

Step 3: Enter other details and Click on Finish.



New Case Information

Steps

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

Optional Information

Case

Number: 101

Examiner

Name: Amey_Shreyash

Phone: 987654321

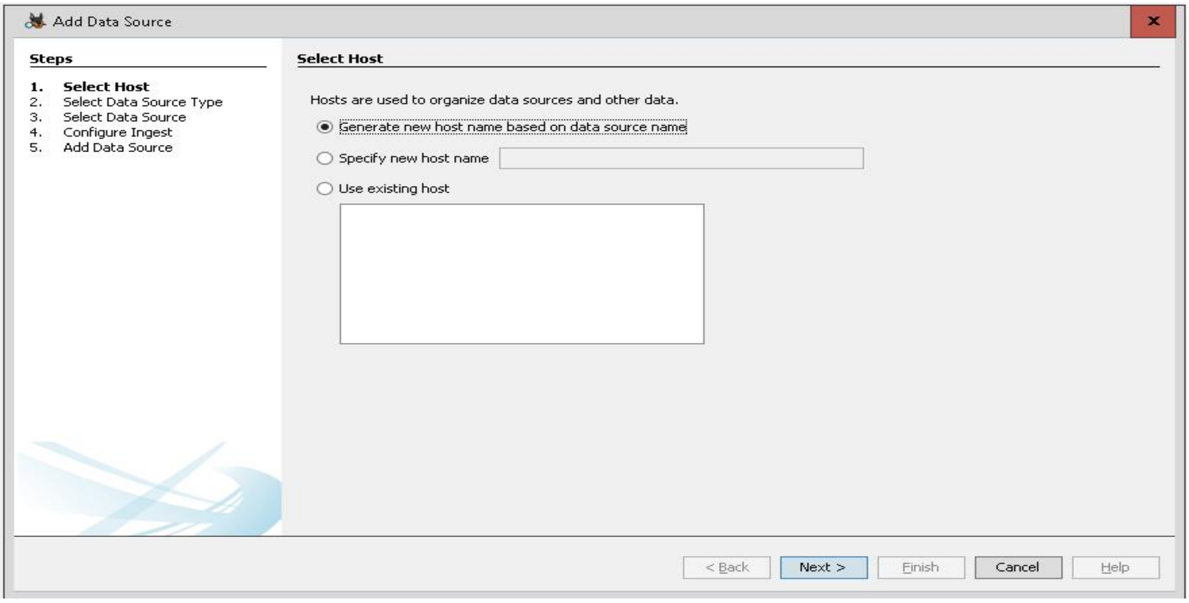
Email: amey@gmail.com

Notes:

Organization

Organization analysis is being done for: Not Specified

Step 4: Add Data Source on which Case Study is to be done.



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

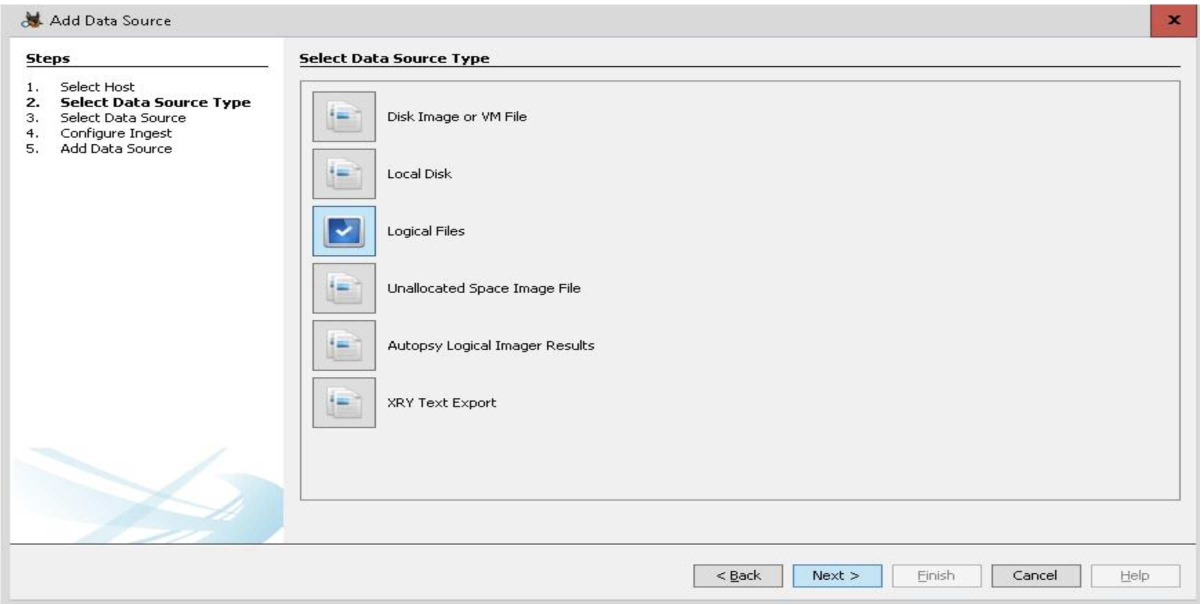
Hosts are used to organize data sources and other data.

● Generate new host name based on data source name

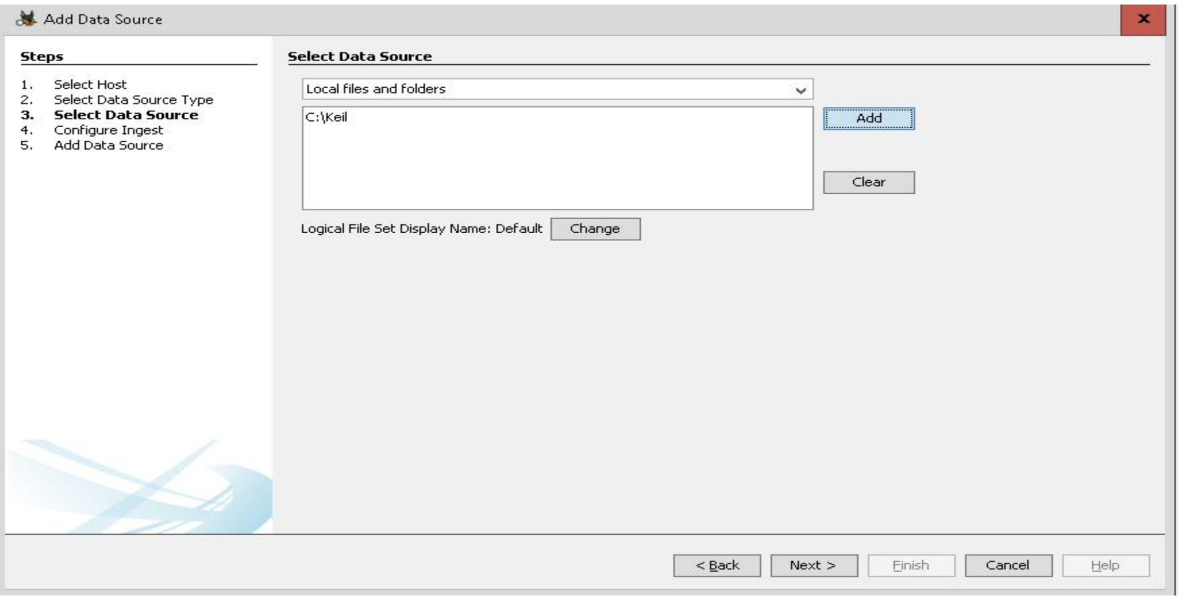
○ Specify new host name

○ Use existing host

Step 5: Add Data Source Type and Select Local Disk for entire Disk or Logical files for a particular file or folder. Select Logical Files in our Case.



Step 6: Select the Disk and Click on Finish.

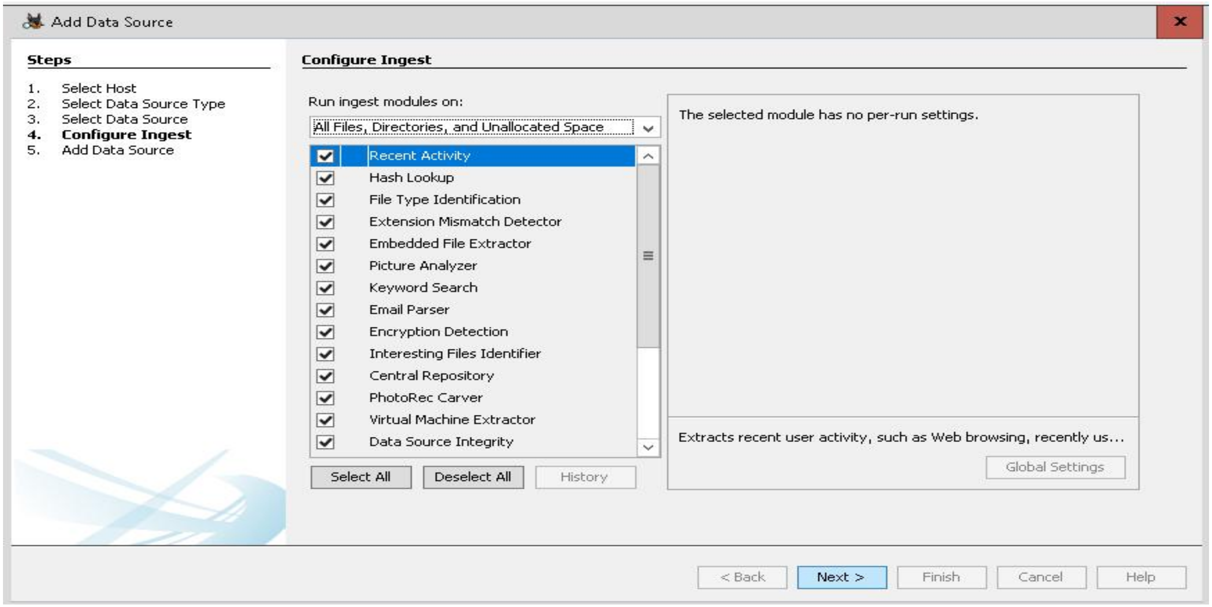


Local files and folders

C:\Keil

Logical File Set Display Name: Default

Step 7: Select different operations to be performed on the disk and Click on Next.



Steps

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

Configure Ingest

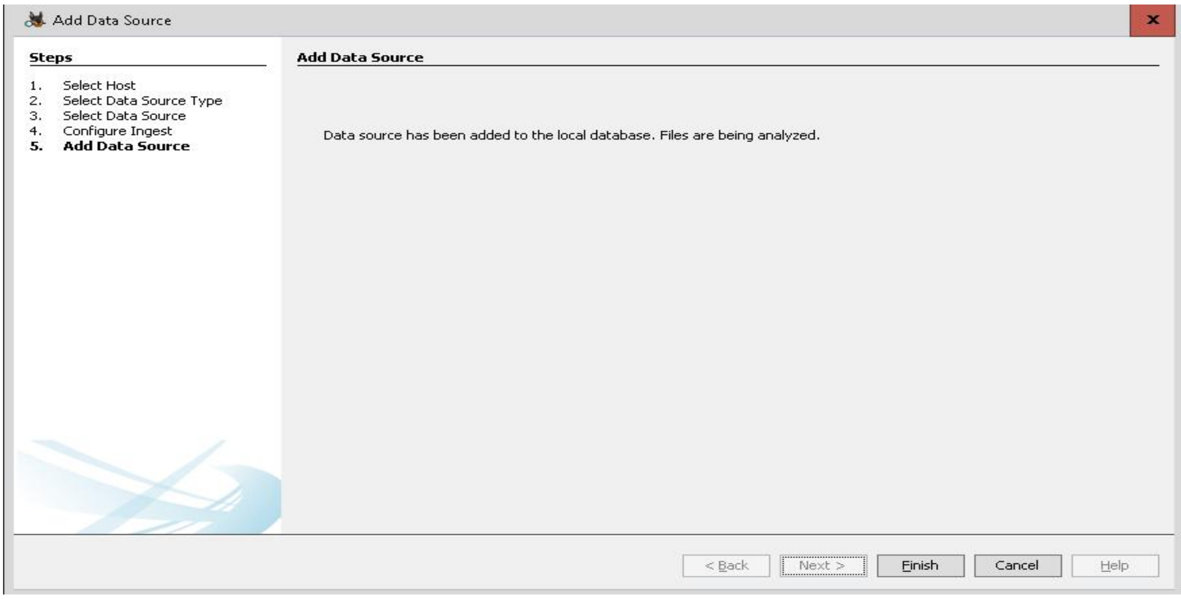
Run ingest modules on: All Files, Directories, and Unallocated Space

- ☑ 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
- ☑ Data Source Integrity

The selected module has no per-run settings.

Extracts recent user activity, such as Web browsing, recently us...

Step 8: Click on Finish.



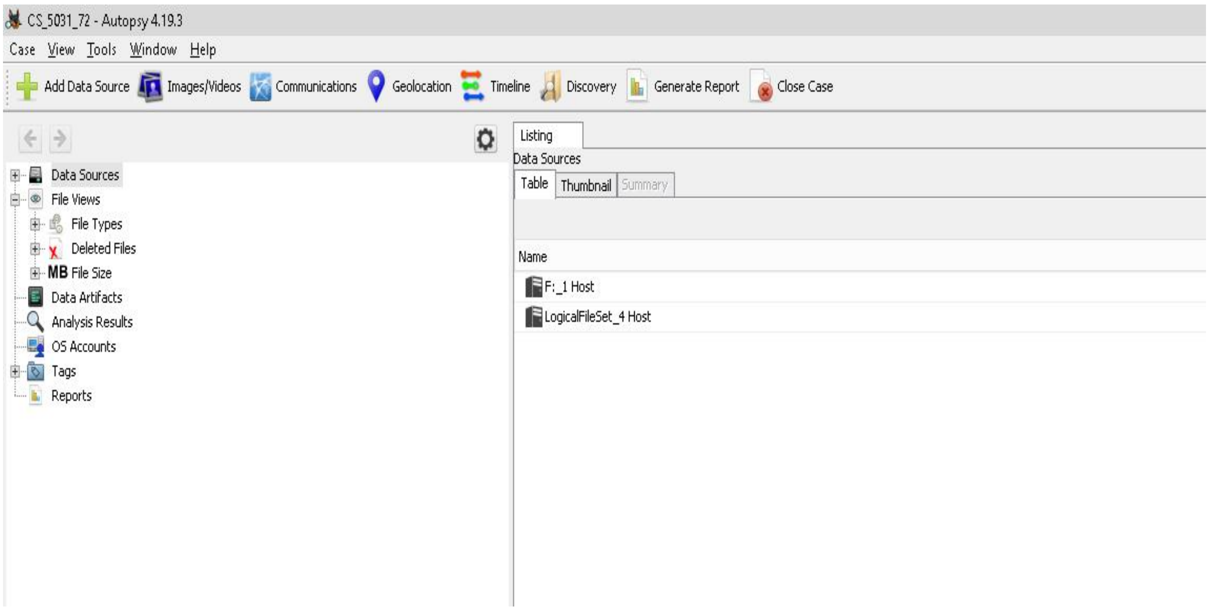
Steps

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

Add Data Source

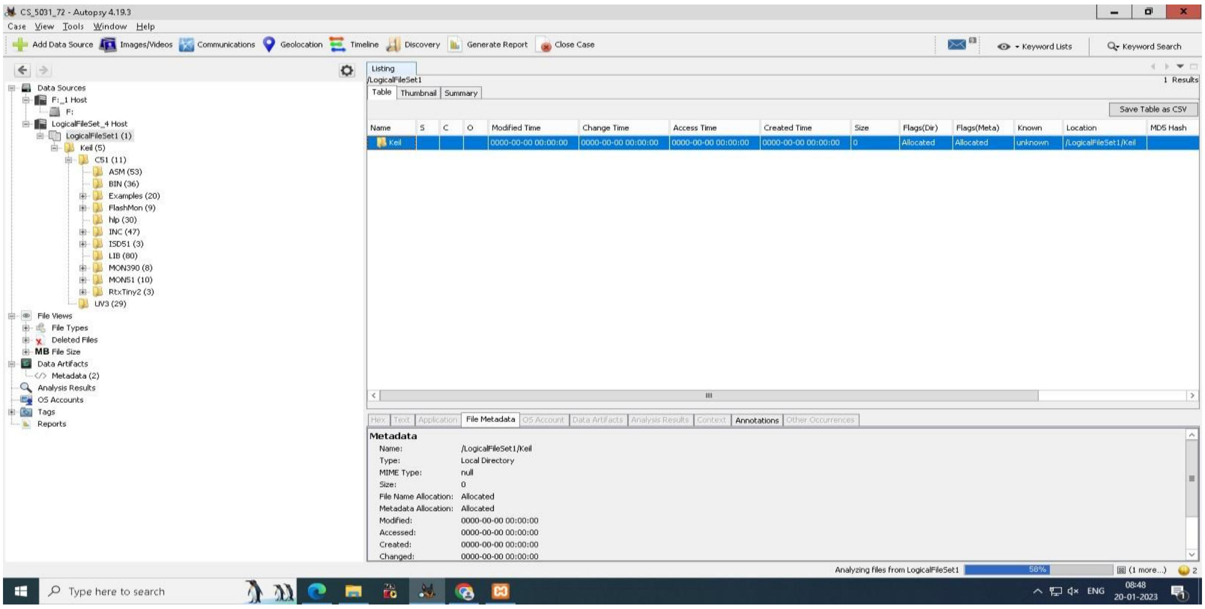
Data source has been added to the local database. Files are being analyzed.

Step 9: You can see all the files including deleted files and all details regarding the files.



Data Sources

Name
F:_1 Host
LogicalFileSet_4 Host

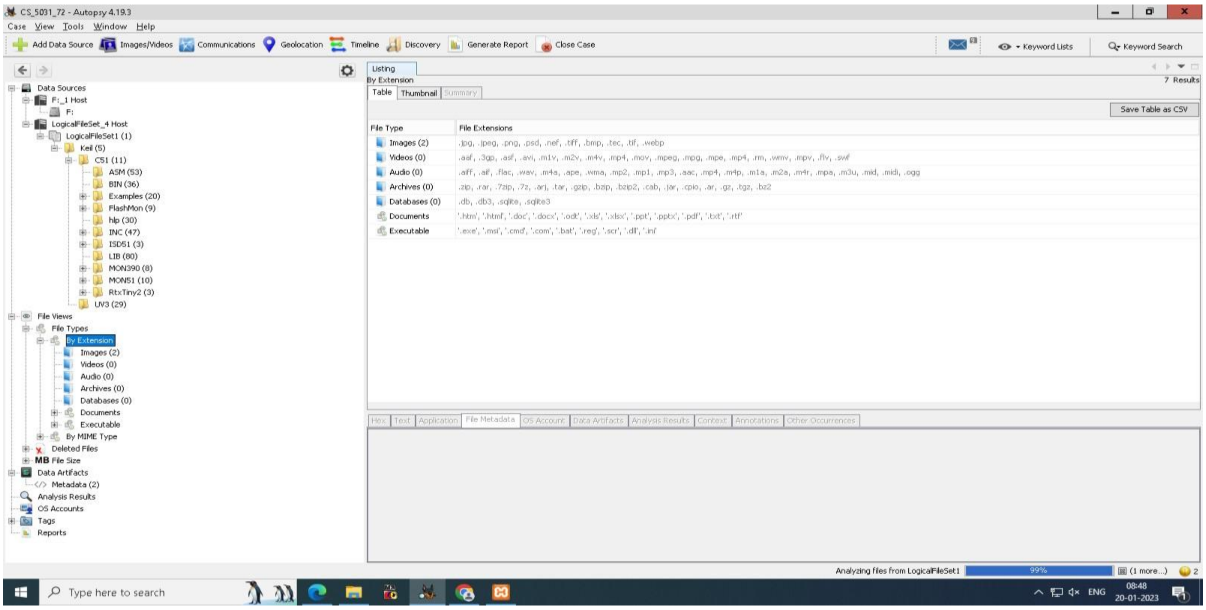


/LogicalFileSet1 1 Results

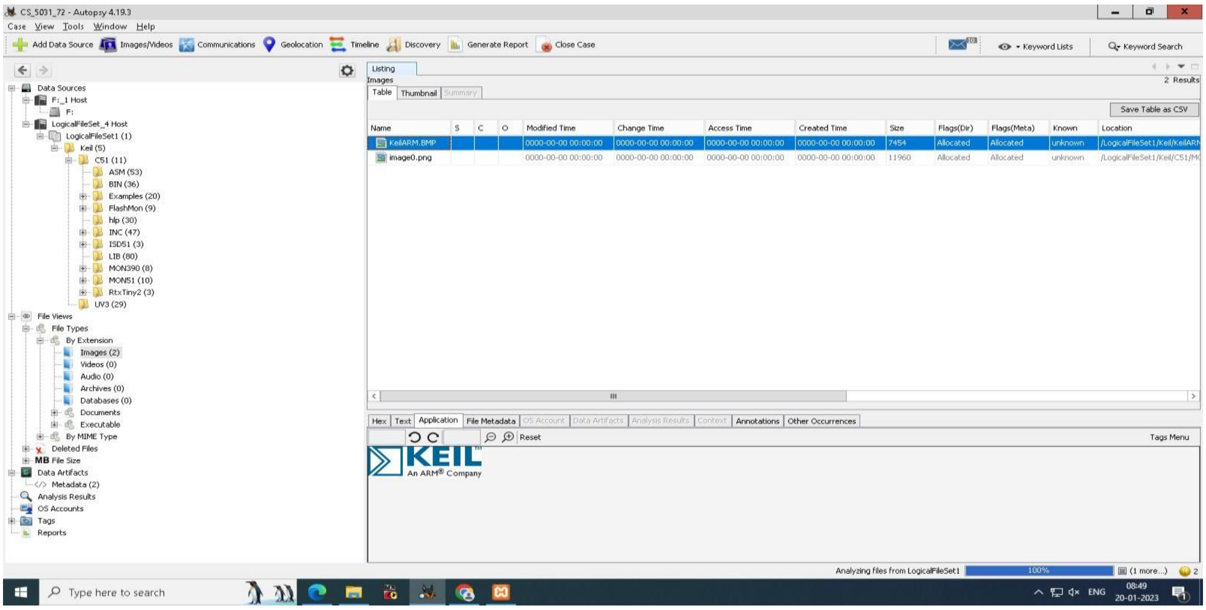
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location	MD5 Hash
Keil				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/Keil	

Metadata

Name:	/LogicalFileSet1/Keil
Type:	Local Directory
MIME Type:	null
Size:	0
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
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



File Type	File Extensions
Images (2)	.jpg, .jpeg, .png, .psd, .nef, .tiff, .bmp, .tec, .tif, .webp
Videos (0)	.aaf, .3gp, .asf, .avi, .m1v, .m2v, .m4v, .mp4, .mov, .mpeg, .mpg, .mpe, .mp4, .rm, .wmv, .mpv, .flv, .swf
Audio (0)	.aiff, .aif, .flac, .wav, .m4a, .ape, .wma, .mp2, .mp1, .mp3, .aac, .mp4, .m4p, .m1a, .m2a, .m4r, .mpa, .m3u, .mid, .midi, .ogg
Archives (0)	.zip, .rar, .7zip, .7z, .arj, .tar, .gzip, .bzip, .bzip2, .cab, .jar, .cpio, .ar, .gz, .tgz, .bz2
Databases (0)	.db, .db3, .sqlite, .sqlite3
Documents	'.htm', '.html', '.doc', '.docx', '.odt', '.xls', '.xlsx', '.ppt', '.pptx', '.pdf', '.txt', '.rtf'
Executable	'.exe', '.msi', '.cmd', '.com', '.bat', '.reg', '.scr', '.dll', '.ini'



Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
KeilARM.BMP				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	7454	Allocated	Allocated	unknown	/LogicalFileSet1/Keil/KeilARN
image0.png				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	11960	Allocated	Allocated	unknown	/LogicalFileSet1/Keil/C51/MC