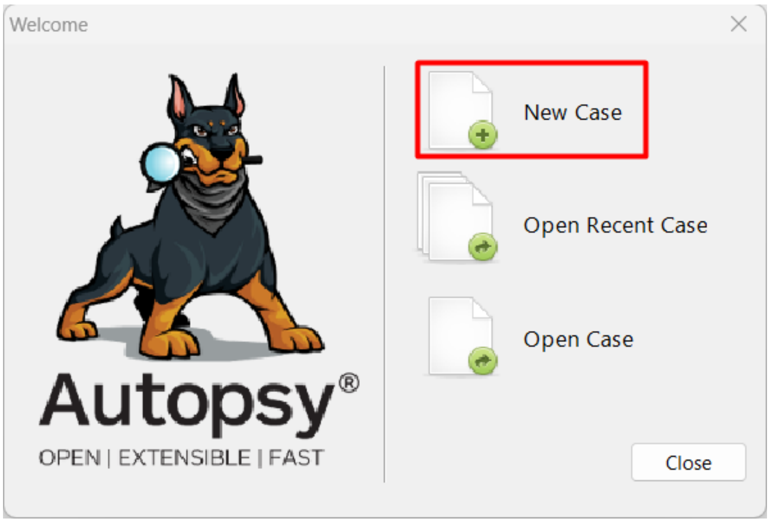
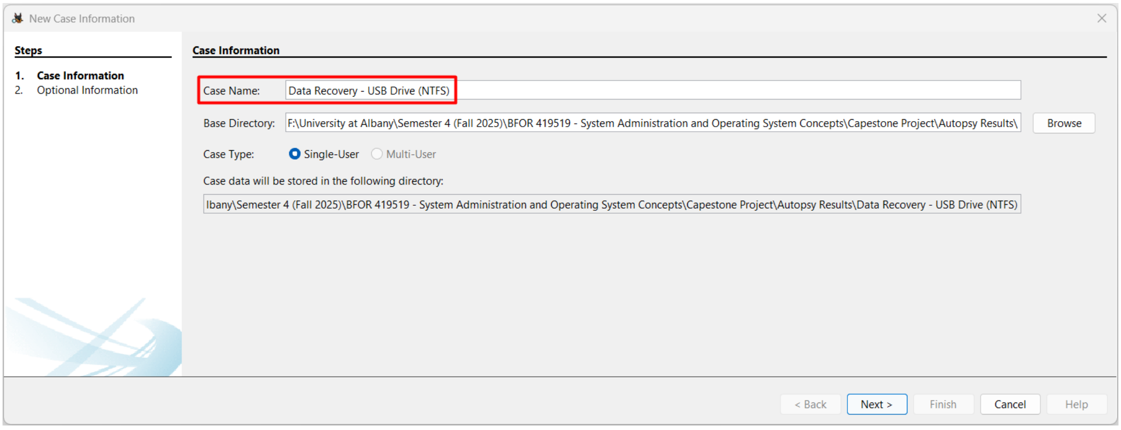
Autopsy Configuration

Open Autopsy & Case Setup

1. Now start autopsy, click New Case button in the welcome window.



2. In the New Case Information window, enter Data Recovery – USB Drive (NTFS) in the Case Name text box and click Browse next to the Base Directory text box. Navigate to and click your Work folder.



New Case Information

Steps

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

Case Information

Case Name: Data Recovery - USB Drive (NTFS)

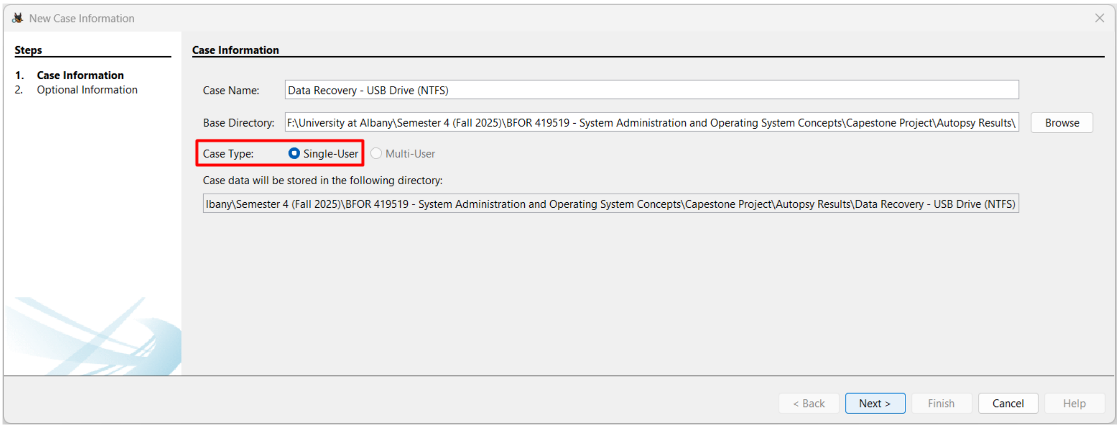
Base Directory: F:\University at Albany\Semester 4 (Fall 2025)\BFOR 419519 - System Administration and Operating System Concepts\Capestone Project\Autopsy Results\

Case Type: ● Single-User ○ Multi-User

Case data will be stored in the following directory:

lbany\Semester 4 (Fall 2025)\BFOR 419519 - System Administration and Operating System Concepts\Capestone Project\Autopsy Results\Data Recovery - USB Drive (NTFS)

3. Make sure the Single-User option button is selected for Case Type and then click Next.



New Case Information

Steps

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

Case Information

Case Name: Data Recovery - USB Drive (NTFS)

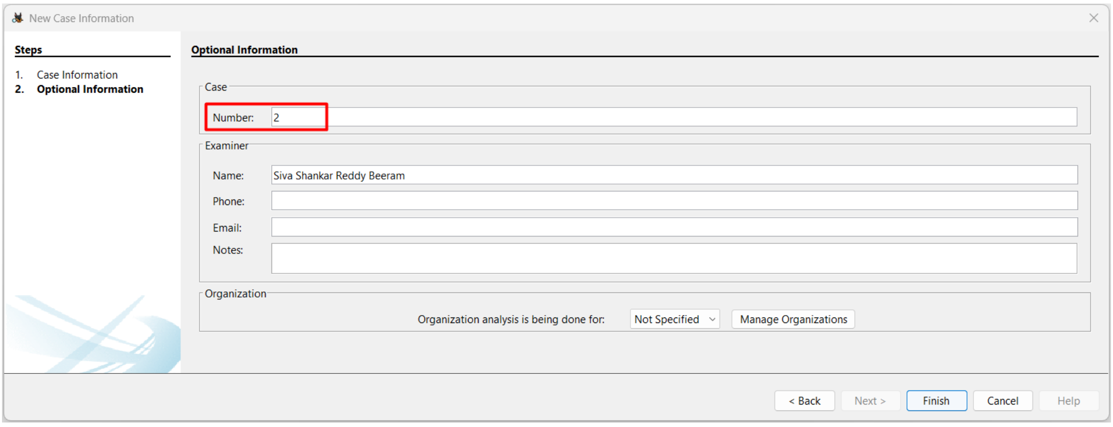
Base Directory: F:\University at Albany\Semester 4 (Fall 2025)\BFOR 419519 - System Administration and Operating System Concepts\Capestone Project\Autopsy Results\

Case Type: ● Single-User ○ Multi-User

Case data will be stored in the following directory:

lbany\Semester 4 (Fall 2025)\BFOR 419519 - System Administration and Operating System Concepts\Capestone Project\Autopsy Results\Data Recovery - USB Drive (NTFS)

4. Now in the Optional Information window, type '1' in the Case Number text box and your full name in the Name text box in the Examiner section and Click Finish.



New Case Information

Steps

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

Optional Information

Case

Number: 2

Examiner

Name: Siva Shankar Reddy Beeram

Phone:

Email:

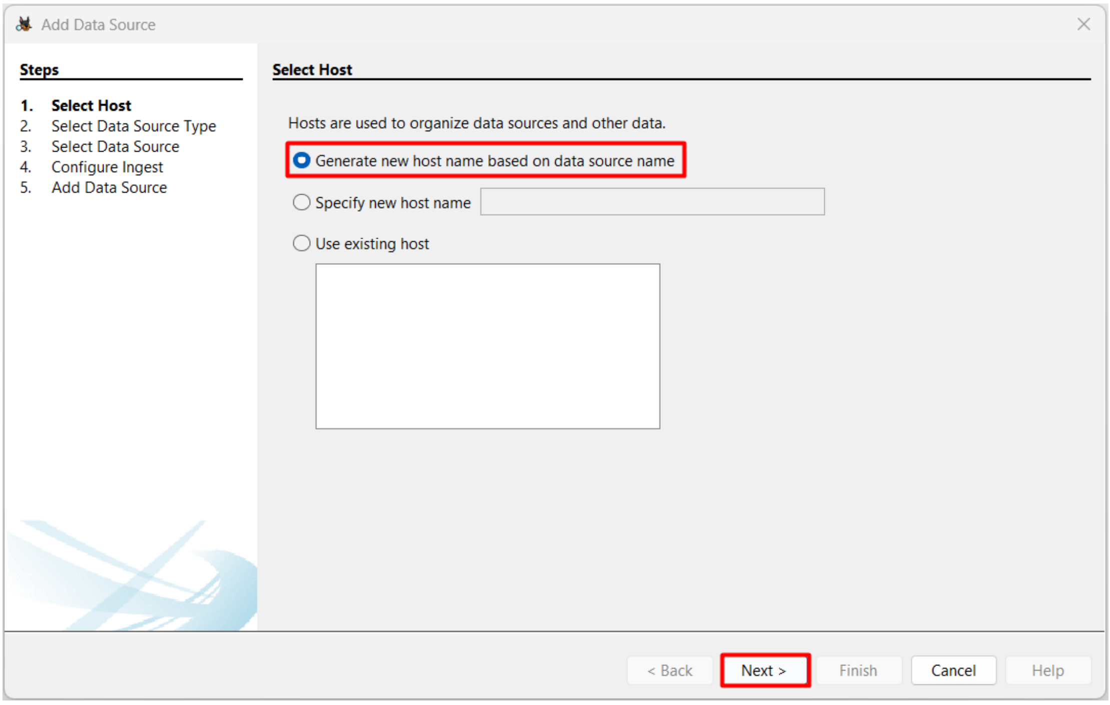
Notes:

Organization

Organization analysis is being done for: Not Specified

ADD Data Source

1. Select the option Generate new host name based on data source name in the select host step and click next to move to next step.



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

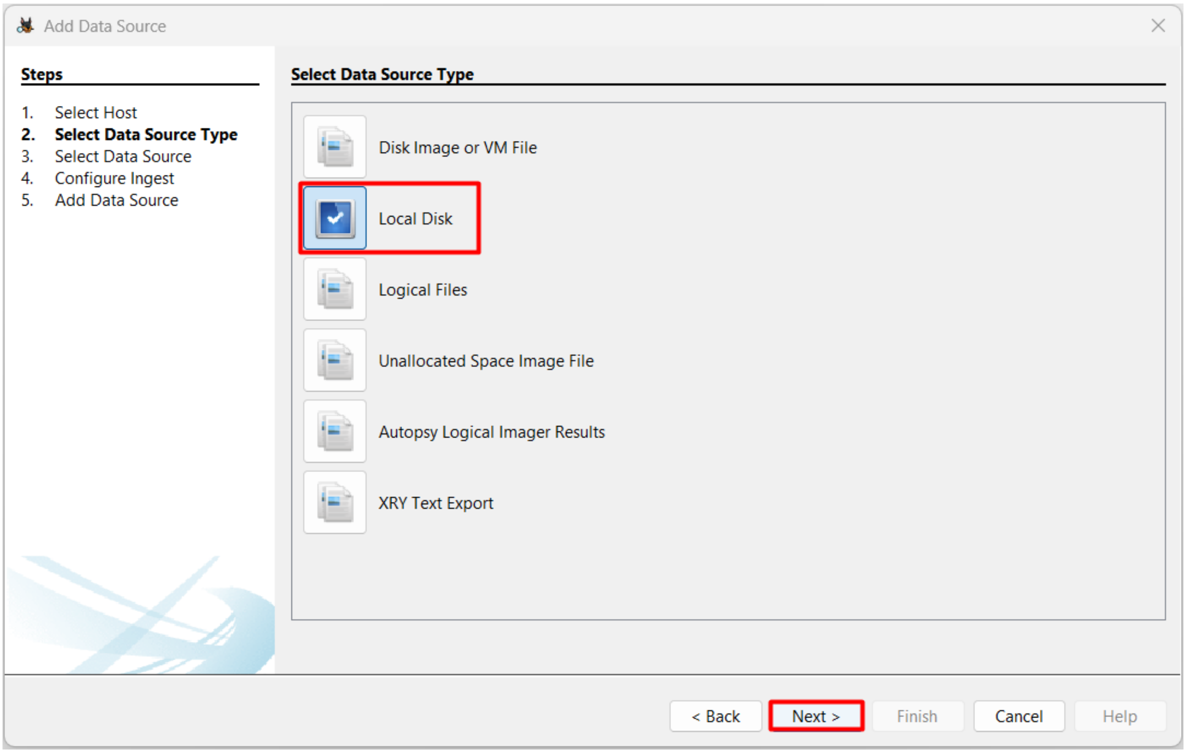
Hosts are used to organize data sources and other data.

● Generate new host name based on data source name

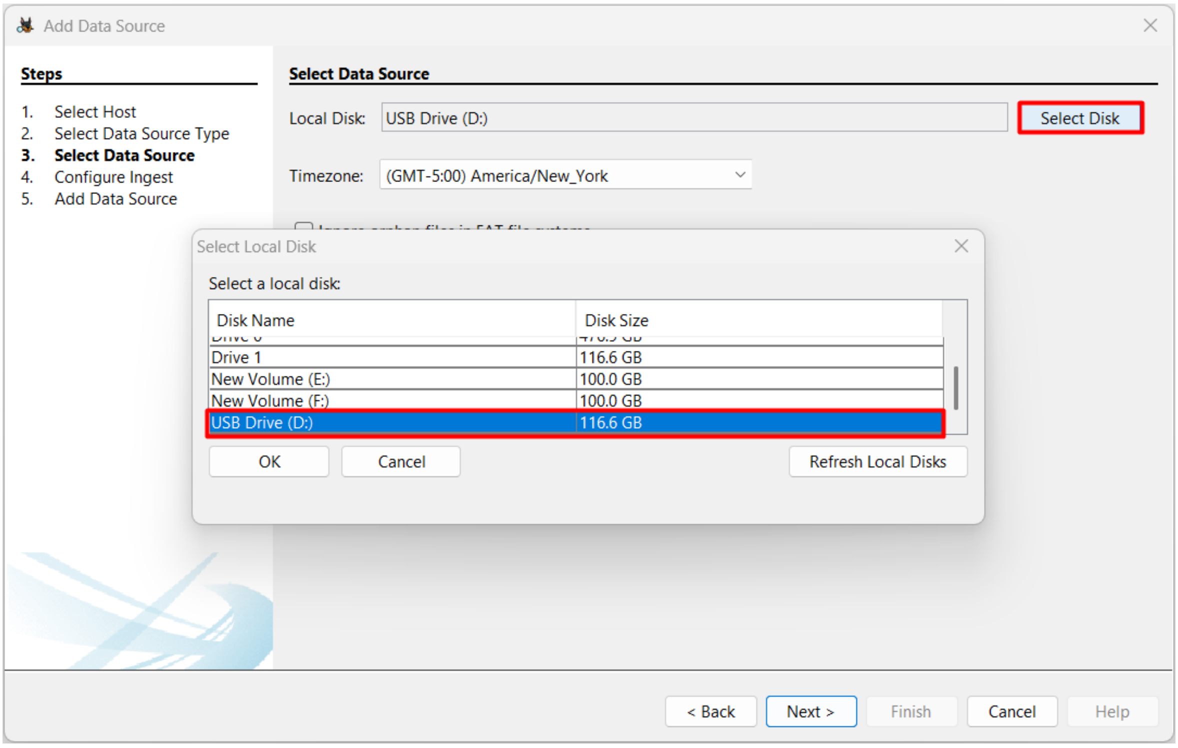
○ Specify new host name

○ Use existing host

2. Now click on Local Disk button in the Select Type of Data Source to Add area of the Add Data Source window.



3. In the Select Data Source pane, click Select Disk and now choose USB Drive, now click ok.



Local Disk: USB Drive (D:)

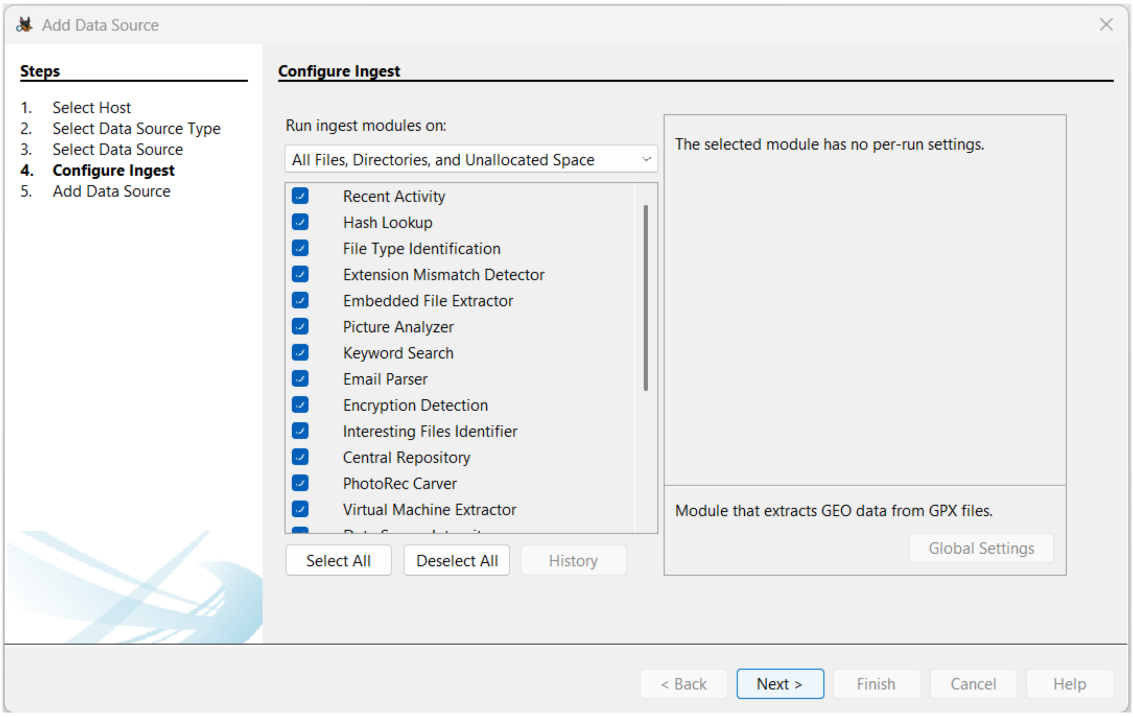
Timezone: (GMT-5:00) America/New_York

Select a local disk:

Disk Name	Disk Size
Drive 1	116.6 GB
New Volume (E:)	100.0 GB
New Volume (F:)	100.0 GB
USB Drive (D:)	116.6 GB

4. In the Configure Ingest area of the Add Data Source window, enable modules such as "File Type Identification" and "Carve Files." This ensures deleted file

recovery and scans for both file system entries and raw fragments.



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:

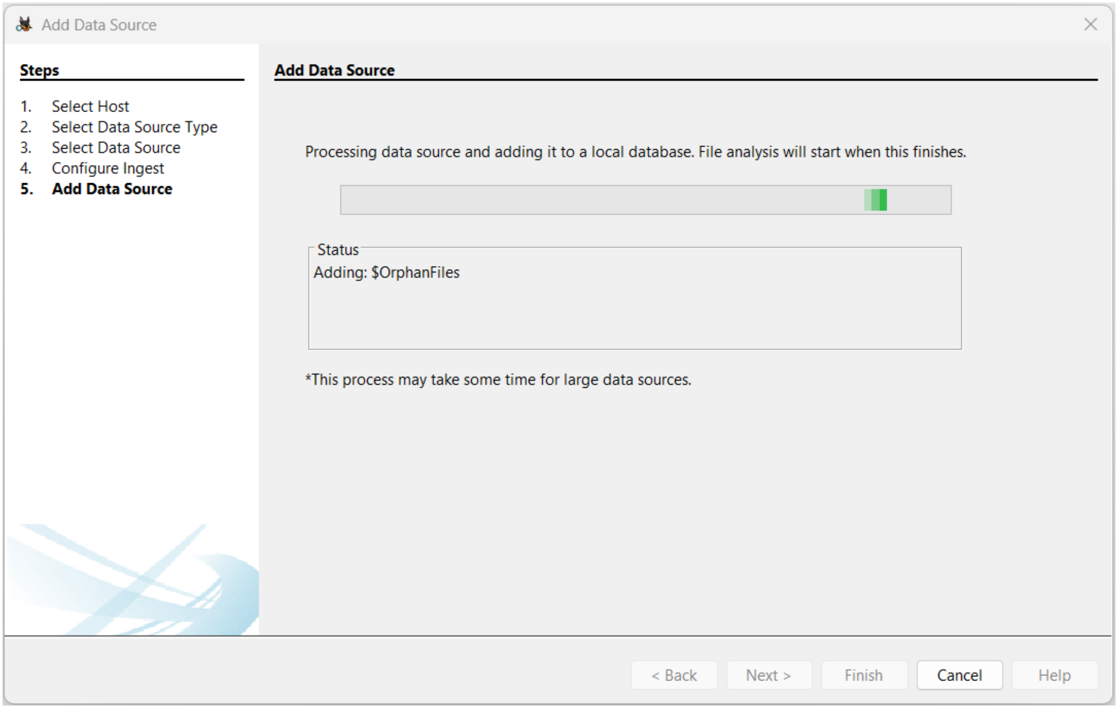
All Files, Directories, and Unallocated Space

- ☑ 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.

Module that extracts GEO data from GPX files.

5. We can see the data is being analysed. Autopsy scans all content, including unallocated space, to find and attempt recovery of deleted files.



Add Data Source

Steps

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

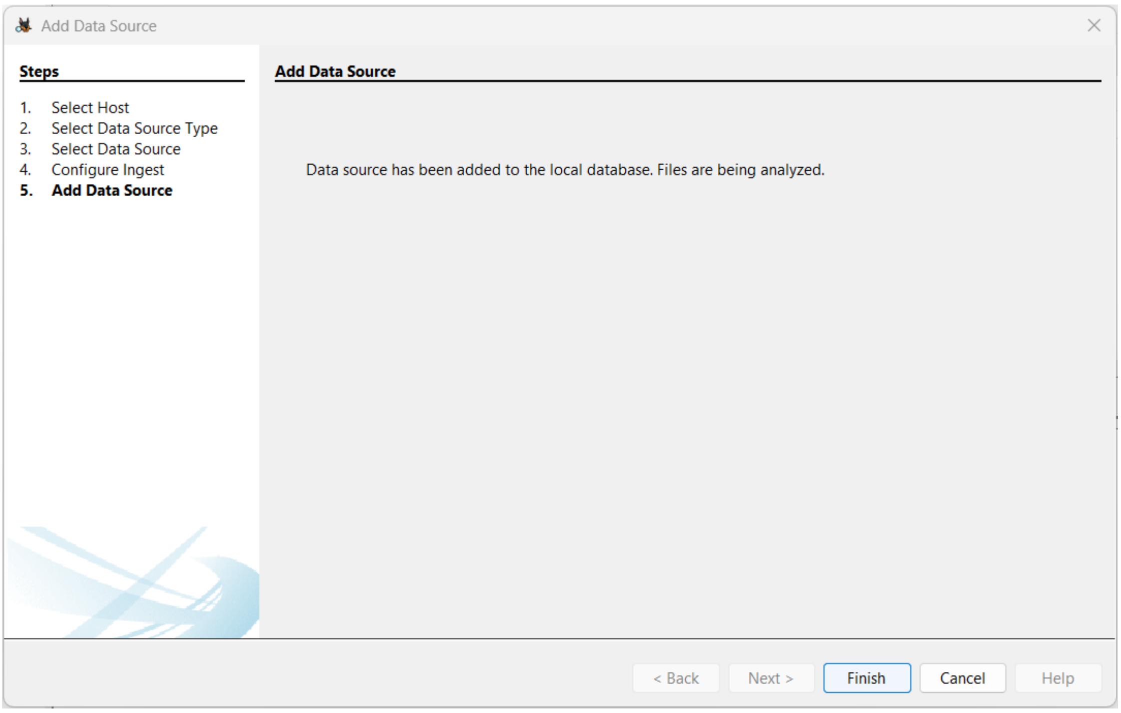
Add Data Source

Processing data source and adding it to a local database. File analysis will start when this finishes.

Status
Adding: $OrphanFiles

*This process may take some time for large data sources.

6. Once the data is analysed successfully, we can see a successful message confirming that data has added.



Add Data Source

Steps

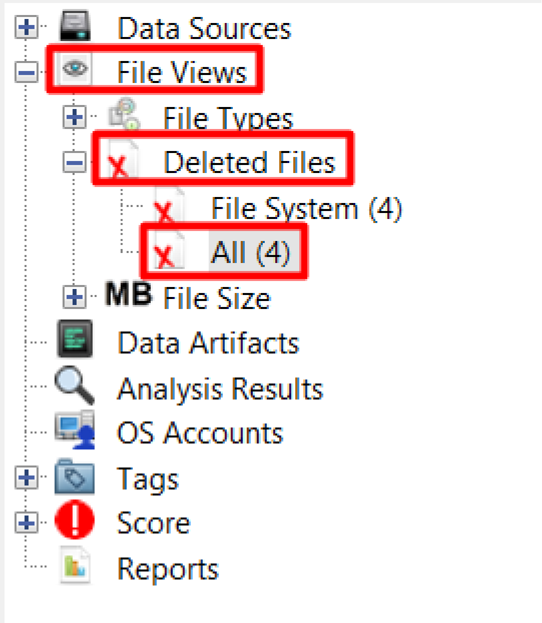
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. **Add Data Source**

Add Data Source

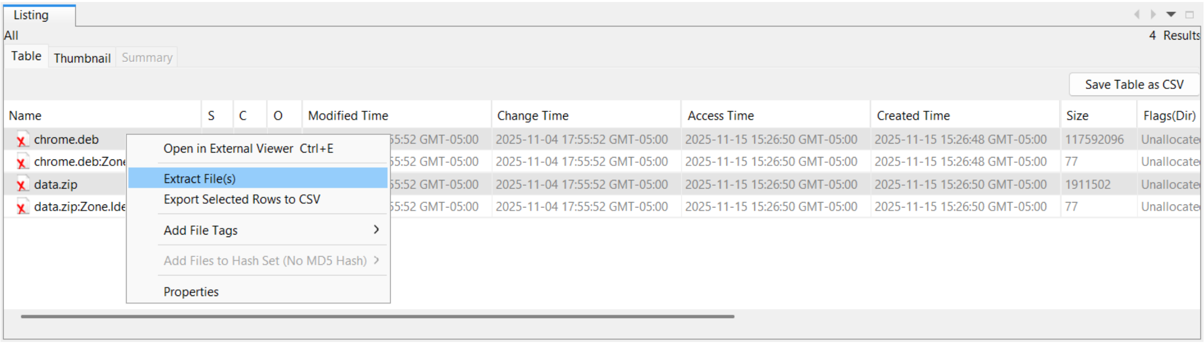
Data source has been added to the local database. Files are being analyzed.

Browsing and Recovering Deleted Files

1. Now in the Tree viewer panel (on the left-hand side), Expand “Files Views” > “Deleted Files”

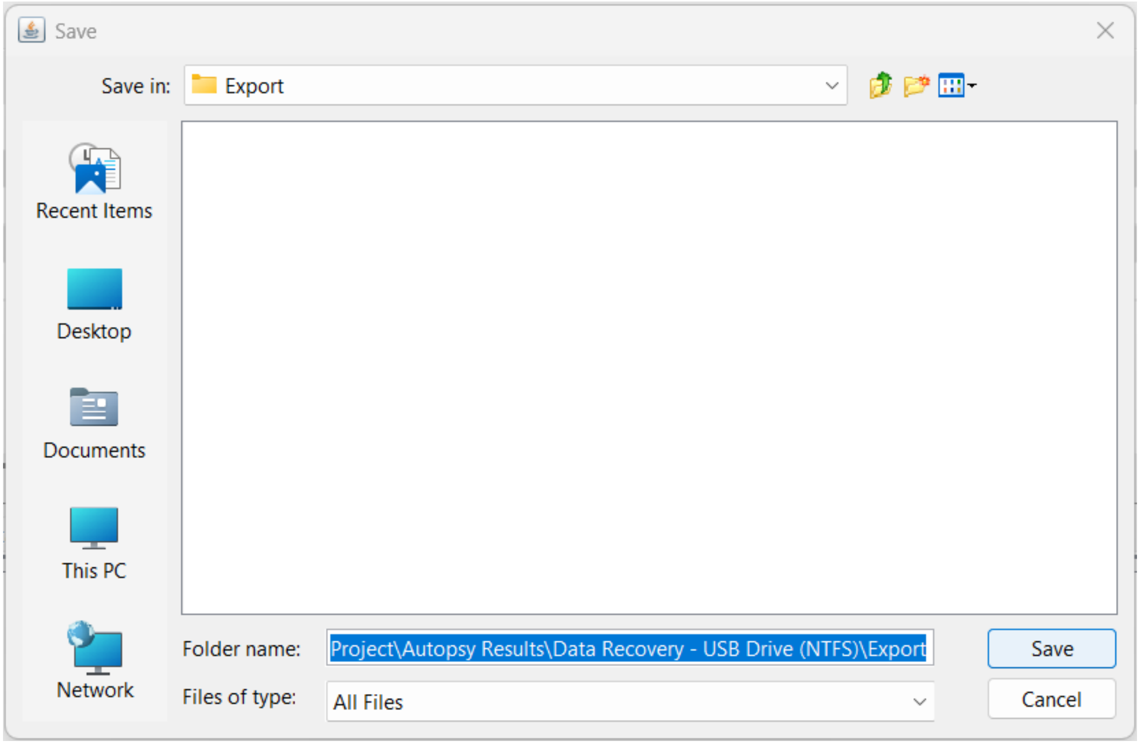


2. In the Result Viewer pane (on the right-hand side), click on the files that we want to recover and now click Extract Files.



Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)
chrome.deb				5:52 GMT-05:00	2025-11-04 17:55:52 GMT-05:00	2025-11-15 15:26:50 GMT-05:00	2025-11-15 15:26:48 GMT-05:00	117592096	Unallocate
chrome.deb:Zon				5:52 GMT-05:00	2025-11-04 17:55:52 GMT-05:00	2025-11-15 15:26:50 GMT-05:00	2025-11-15 15:26:48 GMT-05:00	77	Unallocate
data.zip				5:52 GMT-05:00	2025-11-04 17:55:52 GMT-05:00	2025-11-15 15:26:50 GMT-05:00	2025-11-15 15:26:50 GMT-05:00	1911502	Unallocate
data.zip:Zone.Ide				5:52 GMT-05:00	2025-11-04 17:55:52 GMT-05:00	2025-11-15 15:26:50 GMT-05:00	2025-11-15 15:26:50 GMT-05:00	77	Unallocate

Click Save.

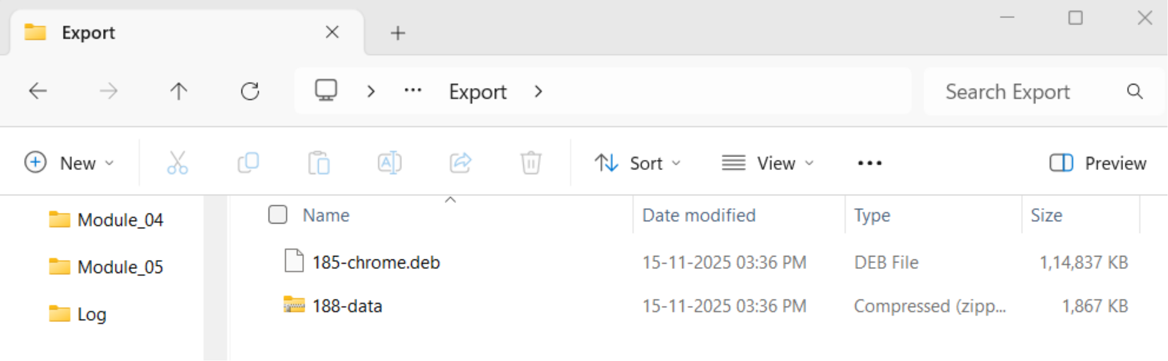


Save in: Export

Folder name: Project\Autopsy Results\Data Recovery - USB Drive (NTFS)\Export

Files of type: All Files

3. Now Using File Explorer, navigate to the Autopsy Export folder, which will be located under your Work folder at F:\University at Albany\Semester 4 (Fall 2025)\BFOR 419519 - System Administration and Operating System Concepts\Capestone Project\Autopsy Results\Data Recovery - USB Drive (NTFS)\Export.



Name	Date modified	Type	Size
185-chrome.deb	15-11-2025 03:36 PM	DEB File	1,14,837 KB
188-data	15-11-2025 03:36 PM	Compressed (zipp...	1,867 KB

Track Recovery Time

Event	Timestamp	Action / Context
Case Opened	**2025-11-15 15:30:03.748**	Start of the later, shorter session.
Case Closed	**2025-11-15 15:39:07.285**	End of the later session.