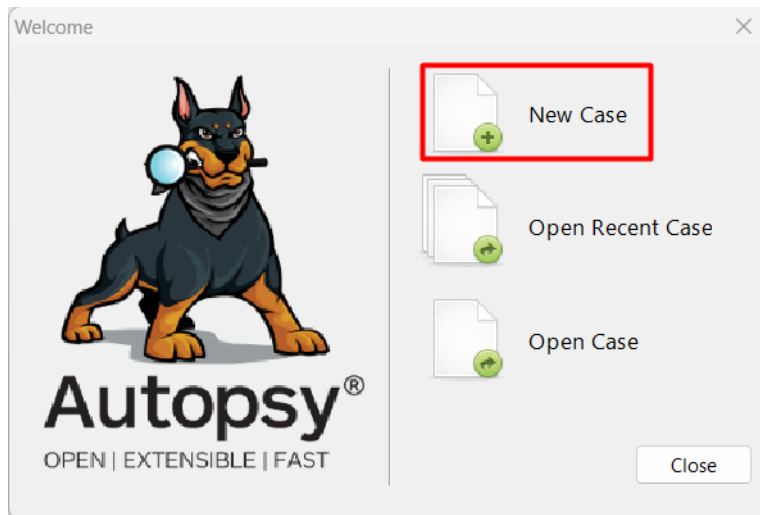


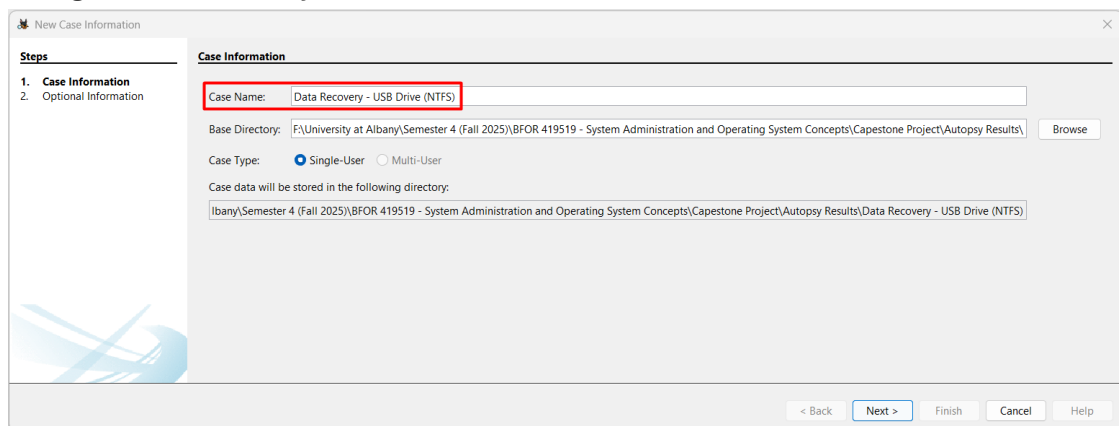
Autopsy Configuration

Open Autopsy & Case Setup

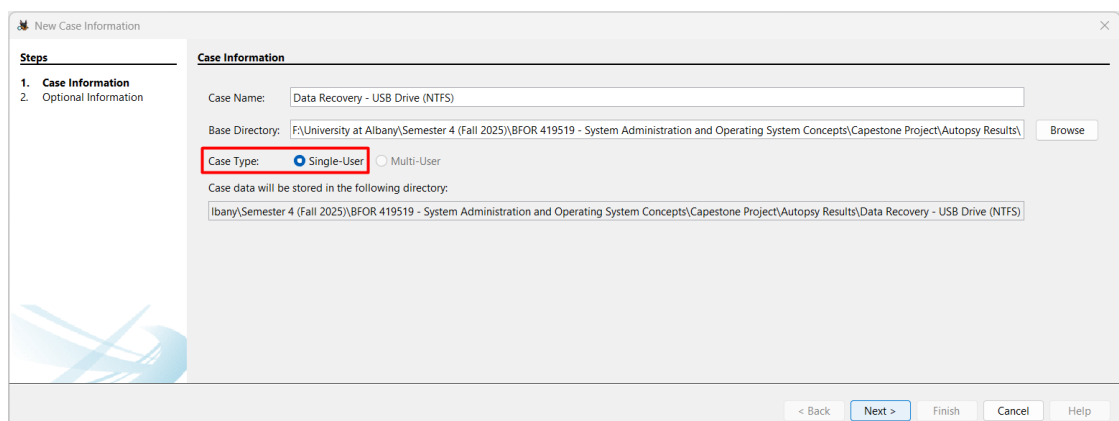
1. Now start autopsy, click New Case button in the welcome window.



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.



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



- 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.

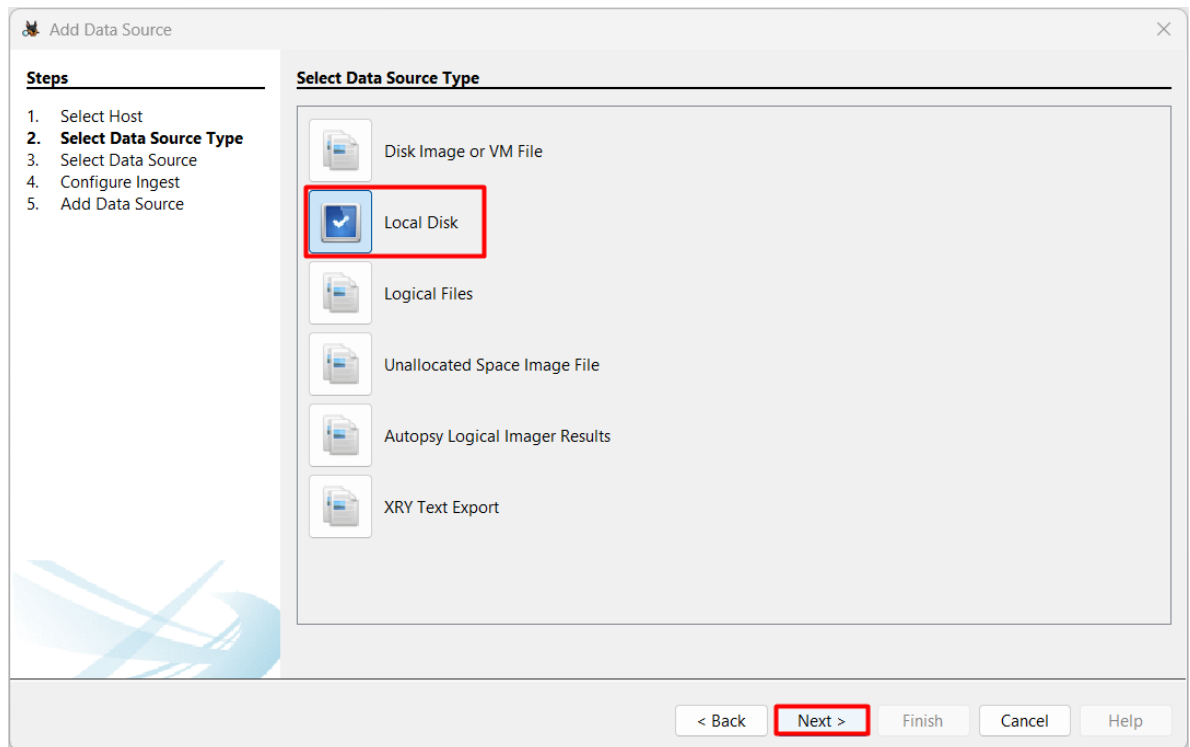
The screenshot shows the 'New Case Information' window with the 'Optional Information' tab selected. On the left, a 'Steps' sidebar lists '1. Case Information' and '2. Optional Information'. The main area contains several sections: 'Case' with a 'Number' field containing '2' (highlighted with a red box); 'Examiner' with fields for 'Name' (containing 'Siva Shankar Reddy Beeram'), 'Phone', 'Email', and 'Notes'; and 'Organization' with a dropdown menu set to 'Not Specified' and a 'Manage Organizations' button. At the bottom right, there are buttons for '< Back', 'Next >', 'Finish' (highlighted with a blue border), 'Cancel', and 'Help'.

ADD Data Source

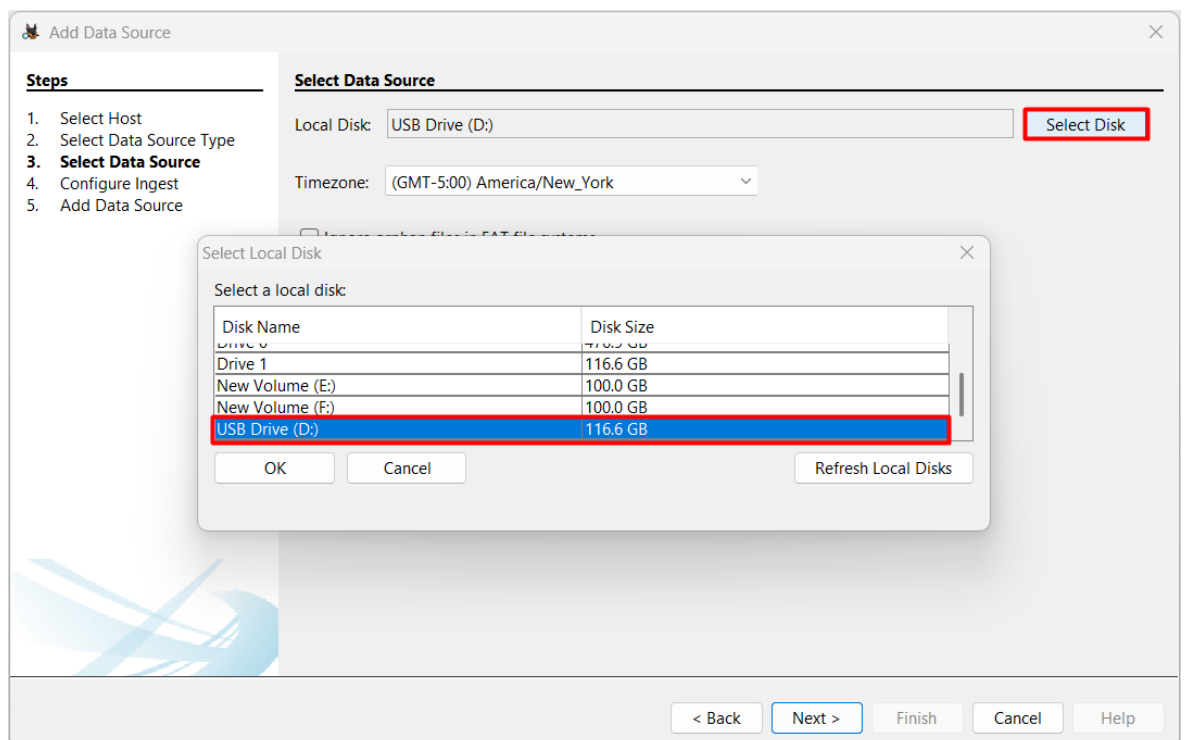
- Select the option Generate new host name based on data source name in the select host step and click next to move to next step.

The screenshot shows the 'Add Data Source' window with the 'Select Host' tab selected. On the left, a 'Steps' sidebar lists five steps: '1. Select Host', '2. Select Data Source Type', '3. Select Data Source', '4. Configure Ingest', and '5. Add Data Source'. The main area has a heading 'Select Host' and a sub-heading 'Hosts are used to organize data sources and other data.' Below this, there are two radio button options: 'Generate new host name based on data source name' (which is selected and highlighted with a red box) and 'Specify new host name' (with an adjacent text field). Below these options is a large empty rectangular box. At the bottom right, there are buttons for '< Back', 'Next >' (highlighted with a red box), 'Finish', 'Cancel', and 'Help'.

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

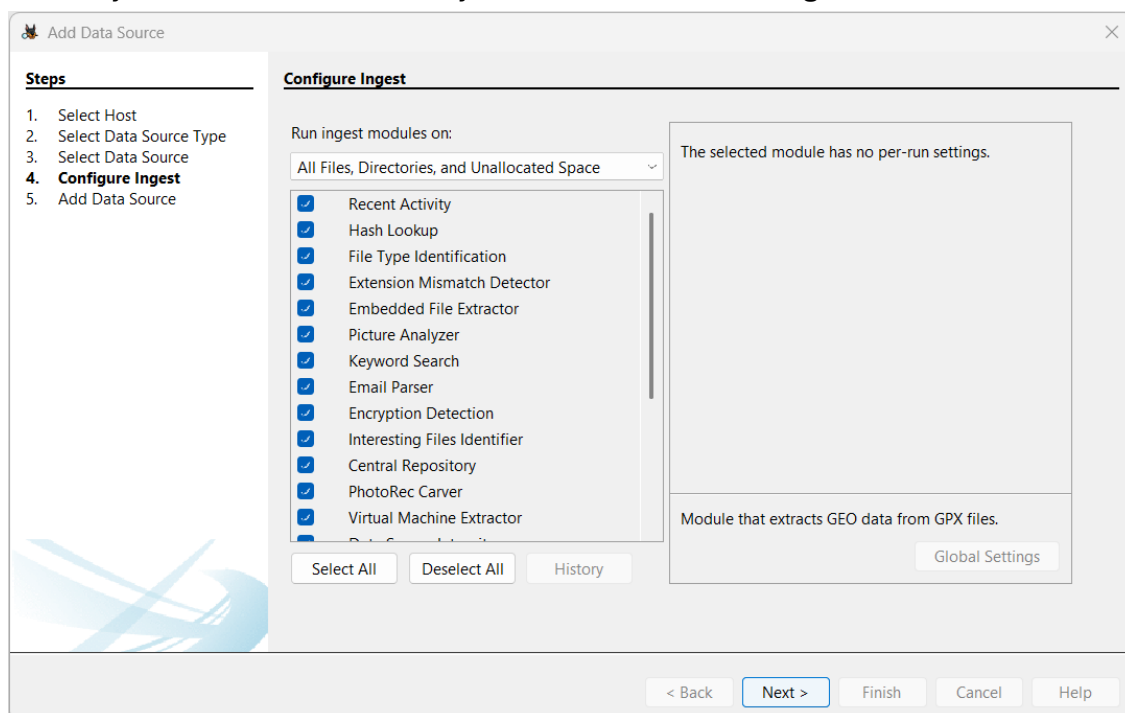


3. In the Select Data Source pane, click Select Disk and now choose USB Drive, now click ok.

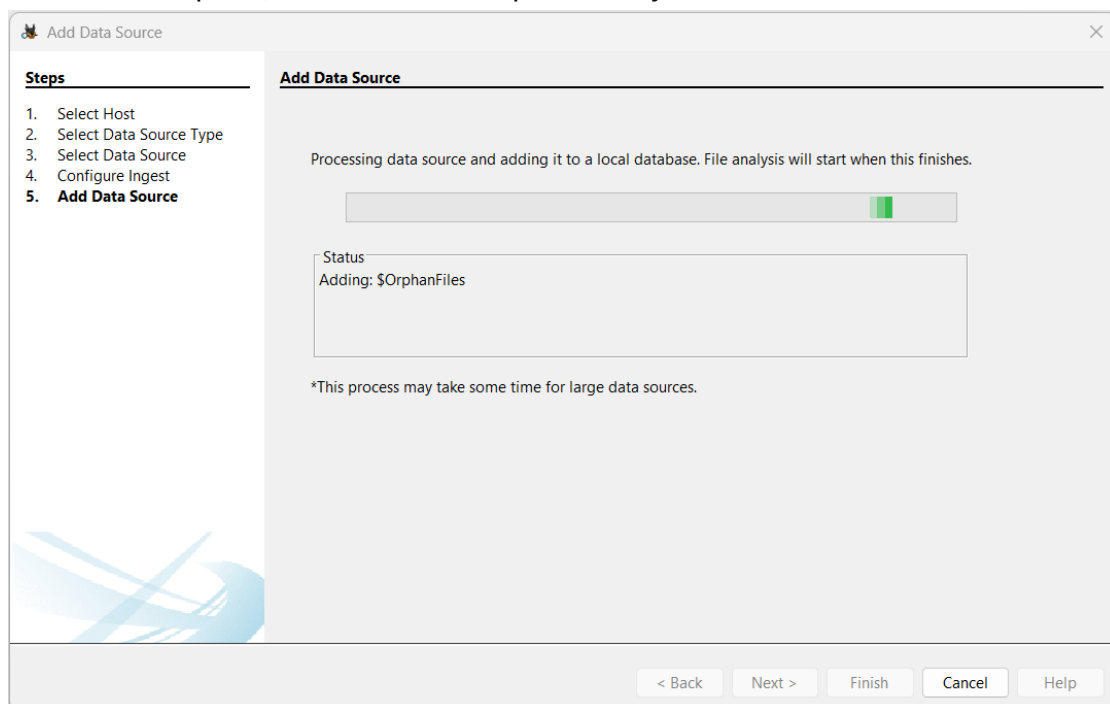


4. In the Configure Ingest area of the Add Data Source window, enable modules such as “File Type Identification” and “Carve Files.” This ensures deleted file

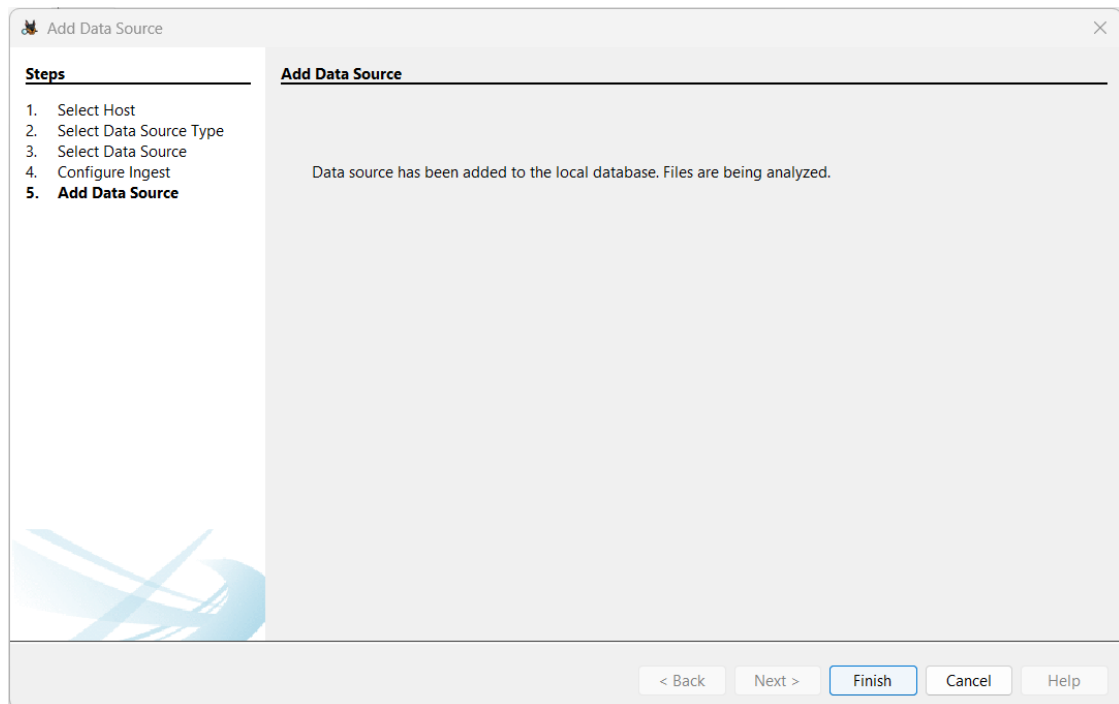
recovery and scans for both file system entries and raw fragments.



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

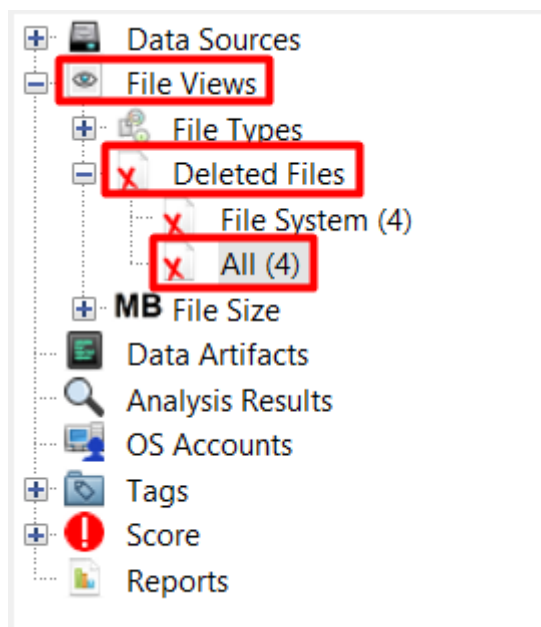


6. Once the data is analysed successfully, we can see a successful message confirming that data has added.



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.

Listing

All 4 Results

Table Thumbnail Summary

Save Table as CSV

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)
chrome.deb	X			2025-11-04 17:55:52 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	Unallocated
chrome.deb:Zone	X			2025-11-04 17:55:52 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	Unallocated
data.zip	X			2025-11-04 17:55:52 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	Unallocated
data.zip:ZoneIde	X			2025-11-04 17:55:52 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	Unallocated

Open in External Viewer Ctrl+E

Extract File(s)

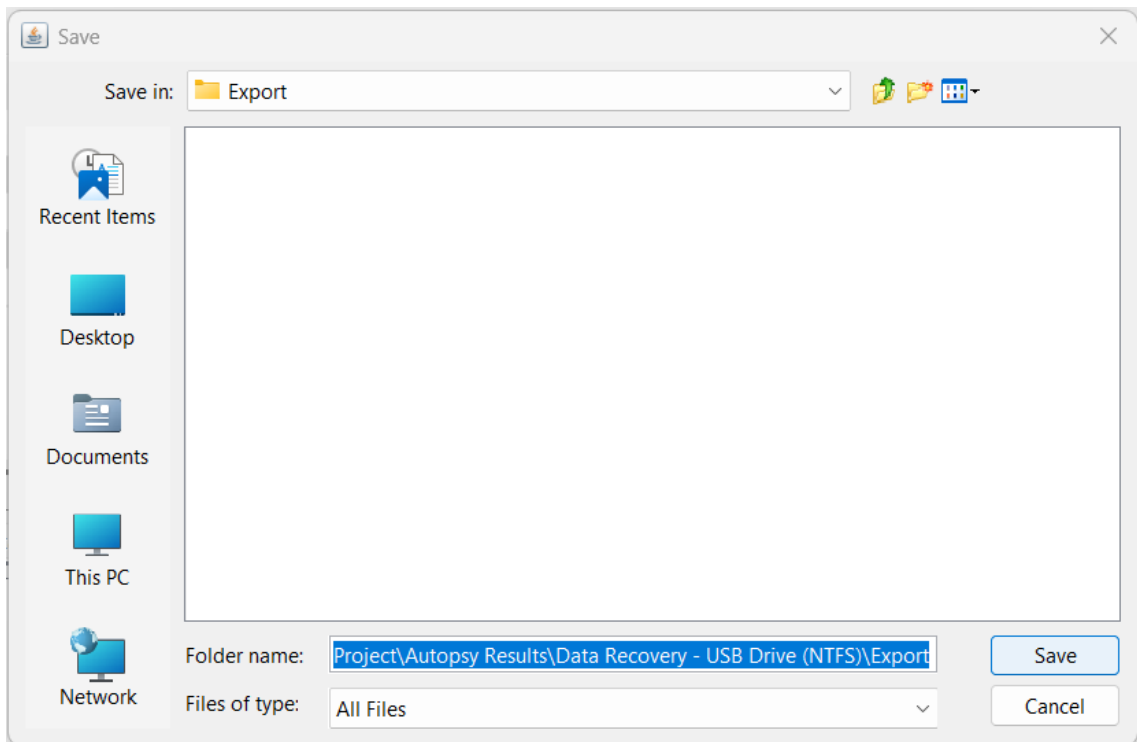
Export Selected Rows to CSV

Add File Tags

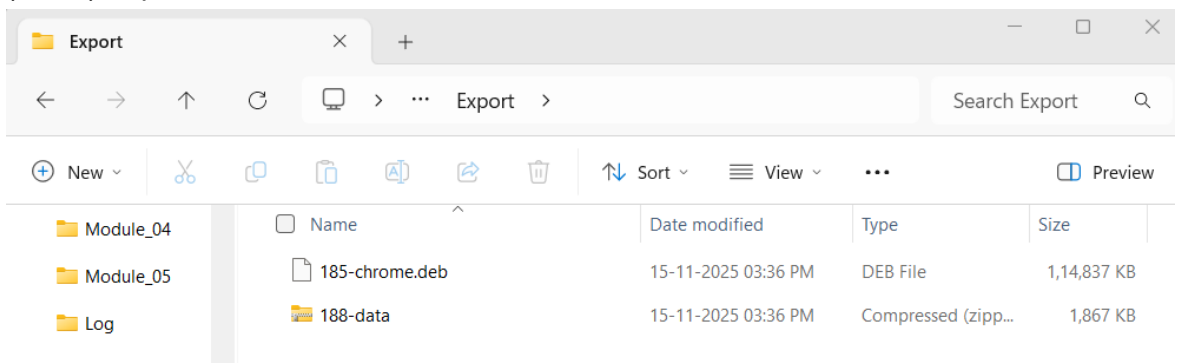
Add Files to Hash Set (No MD5 Hash)

Properties

Click Save.



- 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.



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.