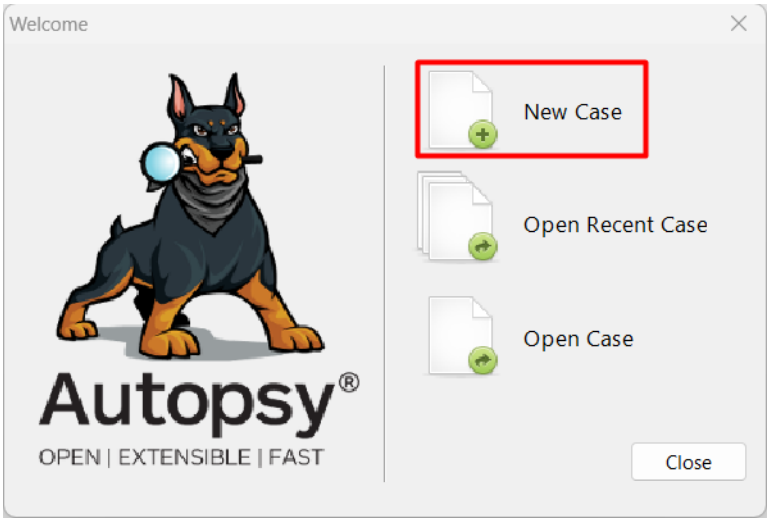
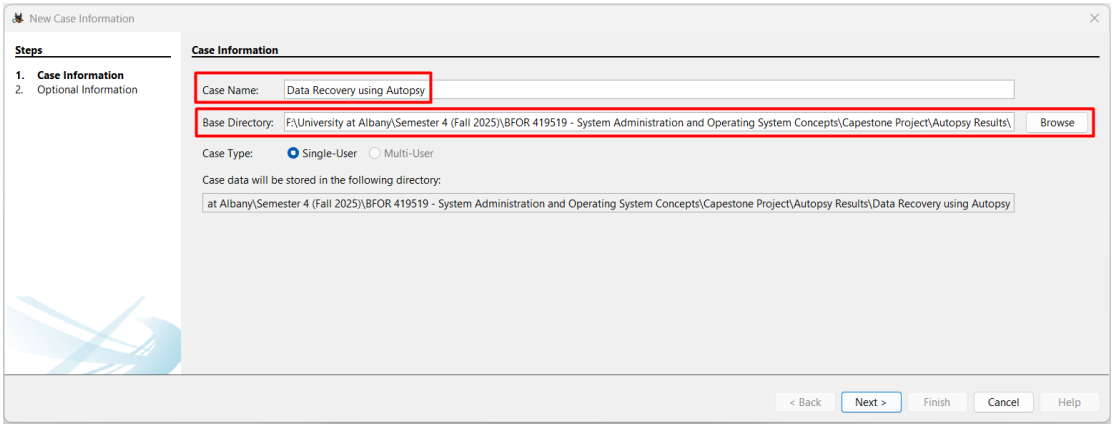
Autopsy Configuration

Open Autopsy & Case Setup

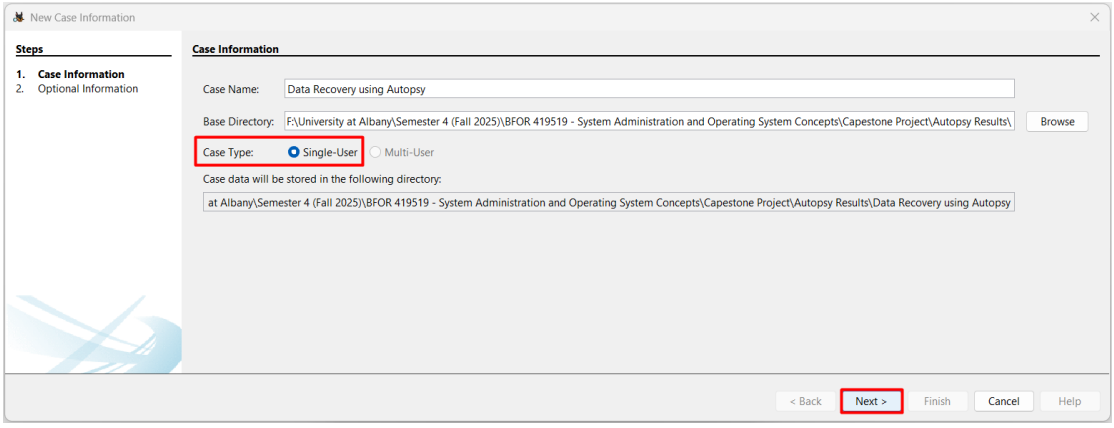
1. Now start autopsy, click New Case button in the welcome window.



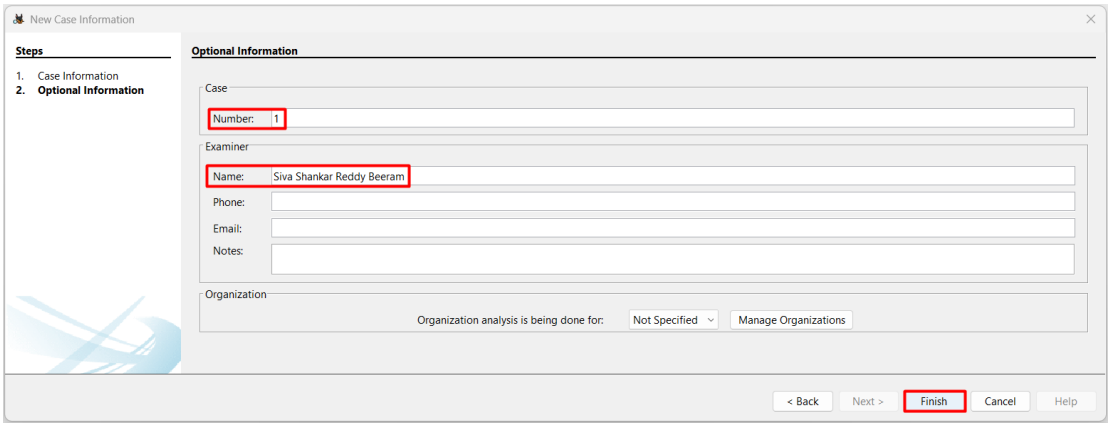
2. In the New Case Information window, enter Data Recovery using Autopsy in the Case Name text box and click Browse next to the Base Directory text box. Navigate to and click your Work folder.



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

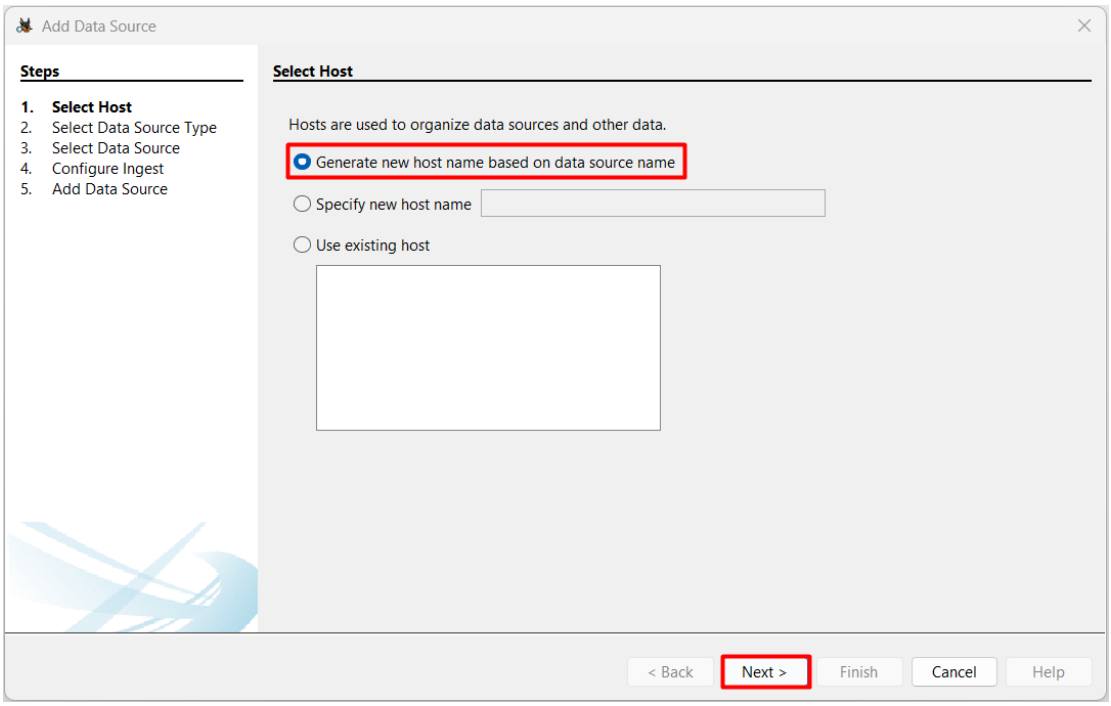


4. Now in the Optional Information window, type ‘1’ in the Case Number text box and your full name in the Name text box in the Examiner section and Click Finish.

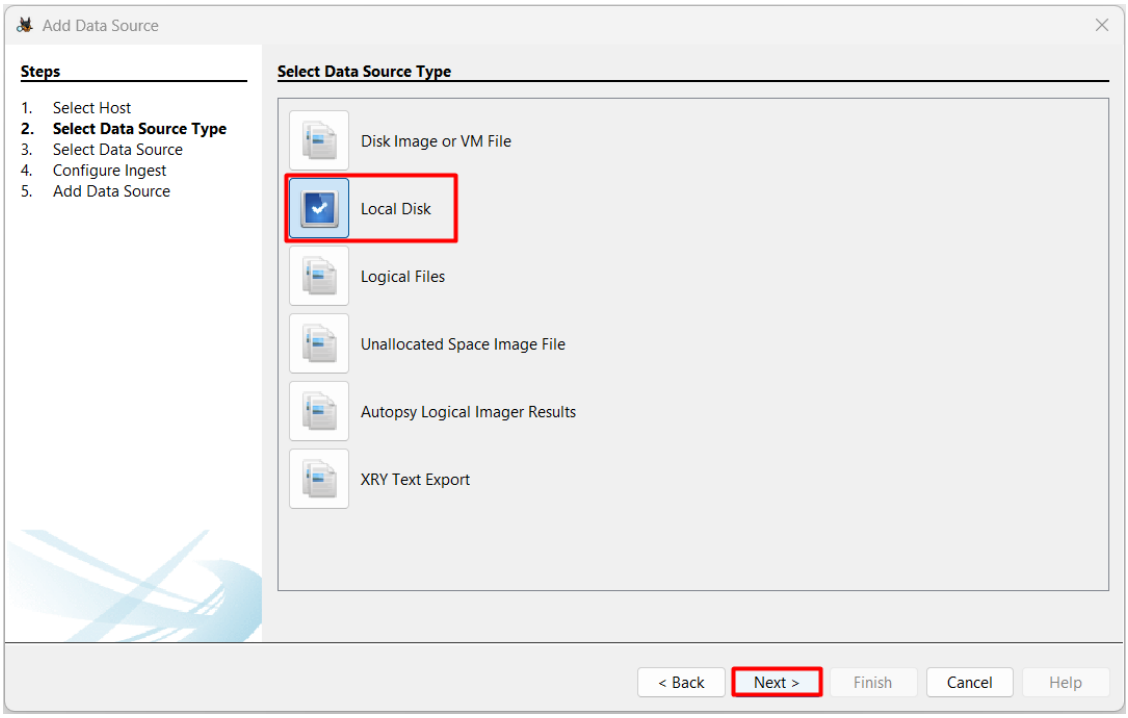


ADD Data Source

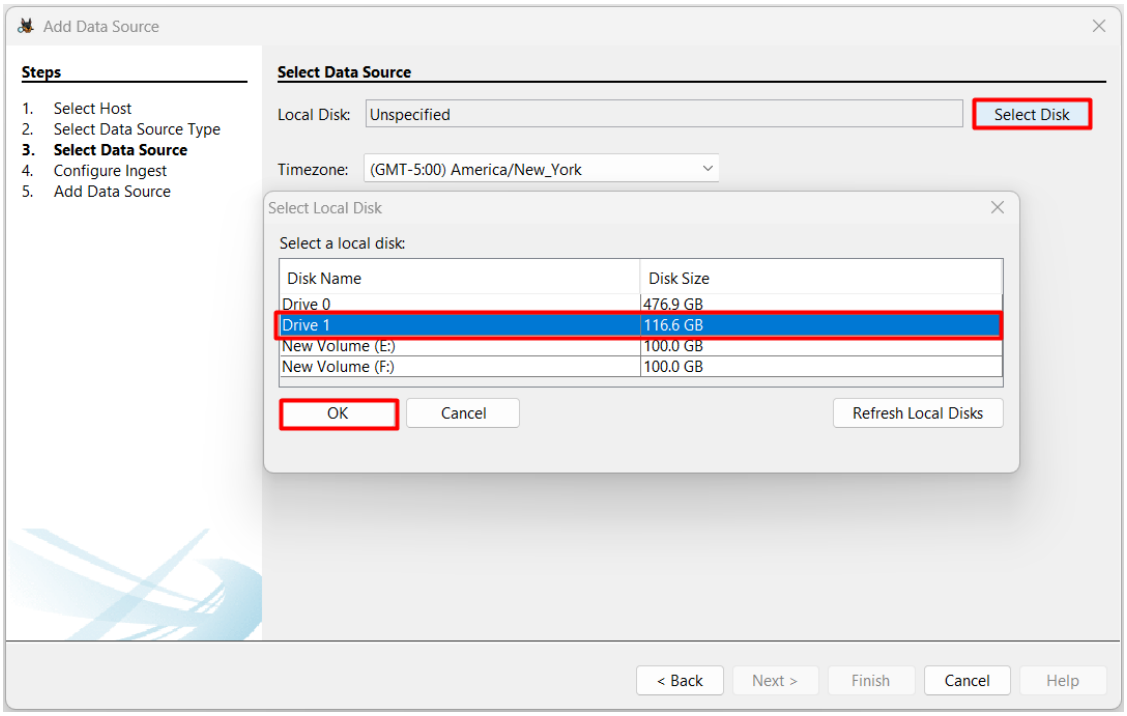
1. Select the option Generate new host name based on data source name in the select host step and click next to move to next step.



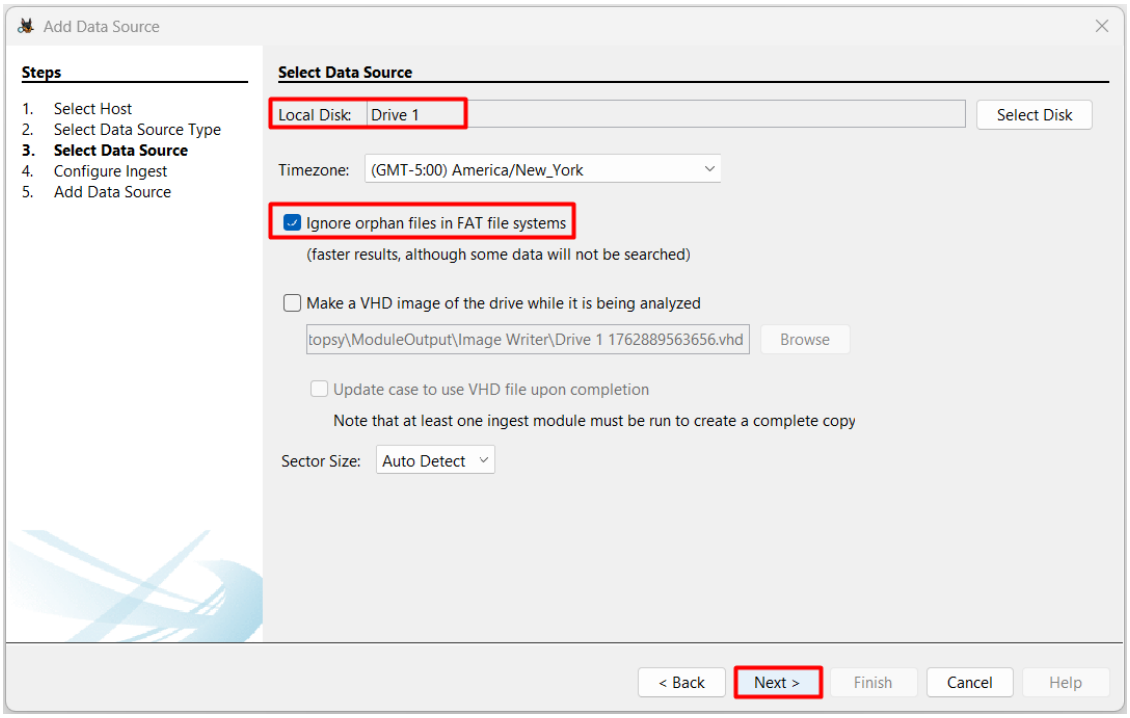
2. Now click on Local Disk button in the Select Type of Data Source to Add area of the Add Data Source window.



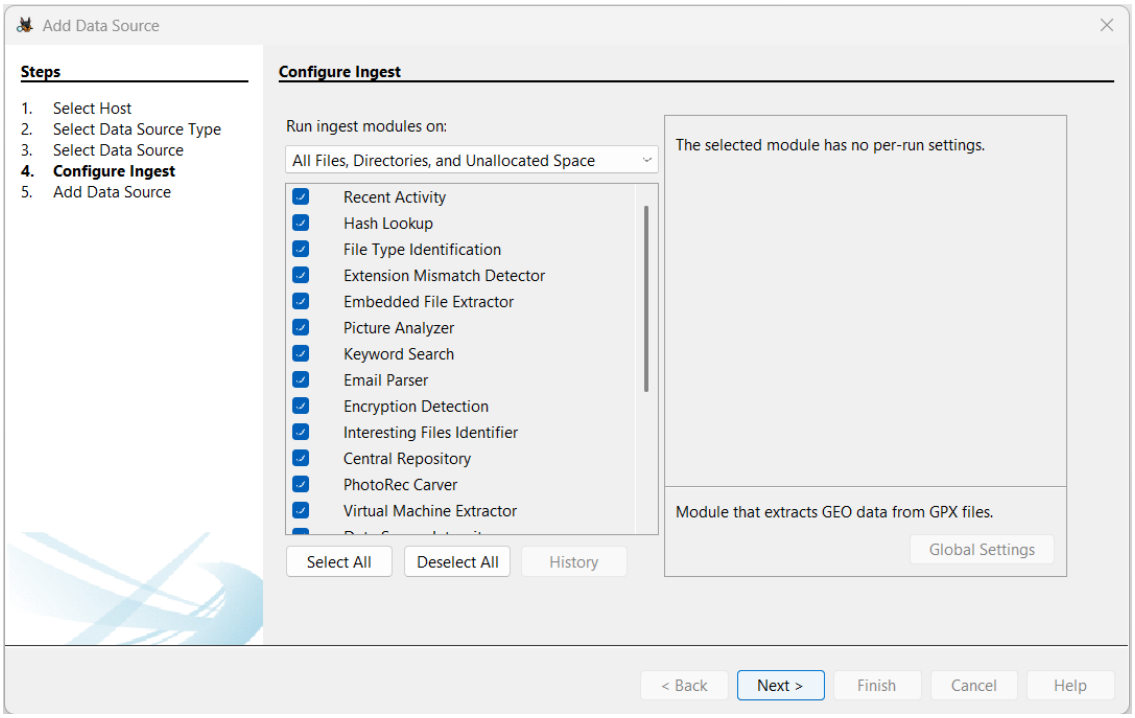
3. In the Select Data Source pane, click Select Disk and now choose Drive 1 (which is USB Drive used for this capstone project), now click ok.



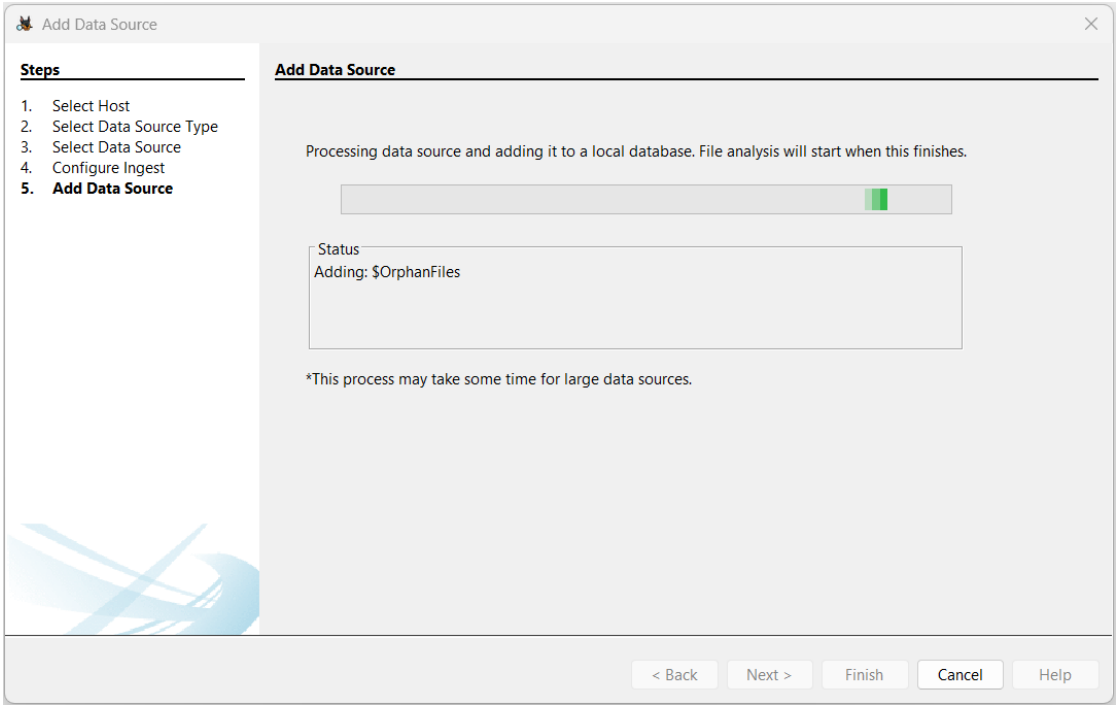
4. Now we can see the USD Drive (Drive 1) is selected and now check the box Ignore Orphan files in FAT file systems for fast results and click next.



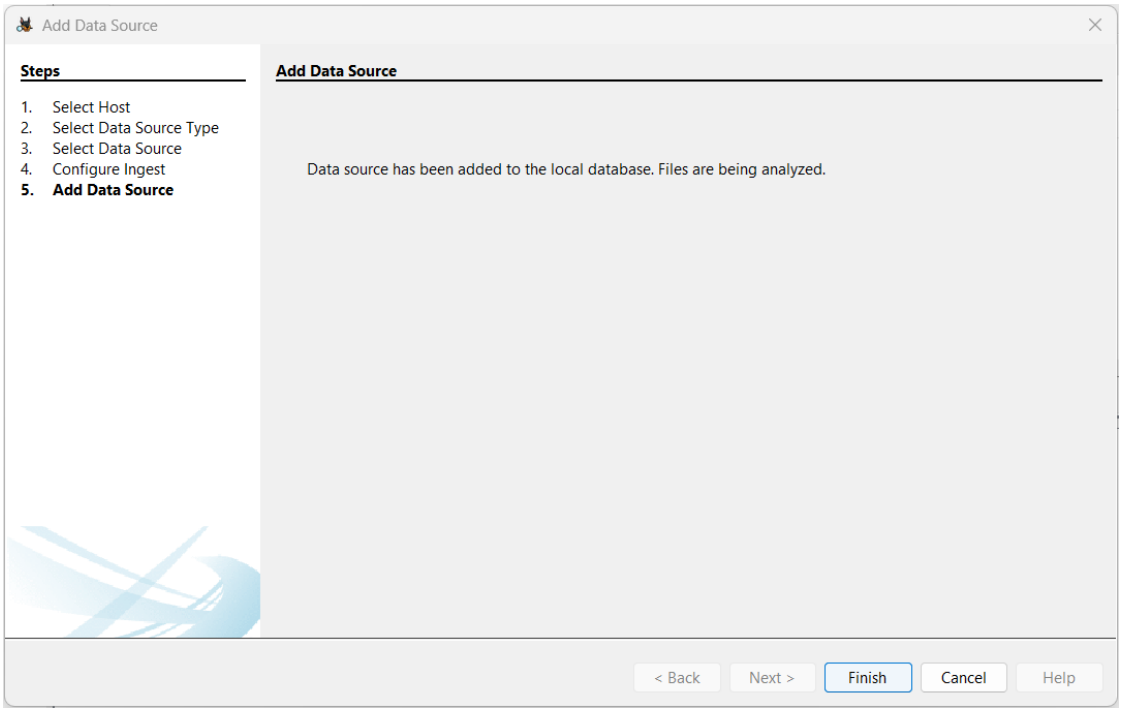
5. In the Configure Ingest area of the Add Data Source window, enable modules such as “File Type Identification” and “Carve Files.” This ensures deleted file recovery and scans for both file system entries and raw fragments.



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

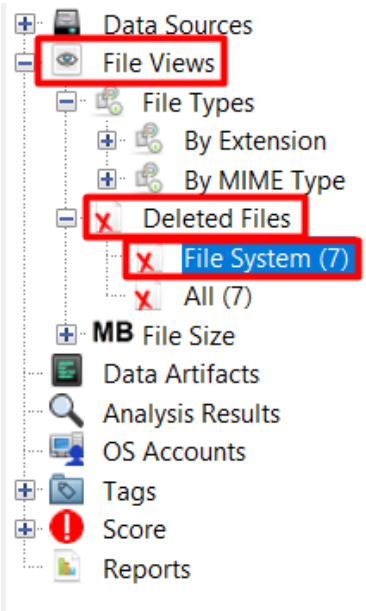


7. Once the data is analysed successfully, we can see a successful message confirming that data has added.

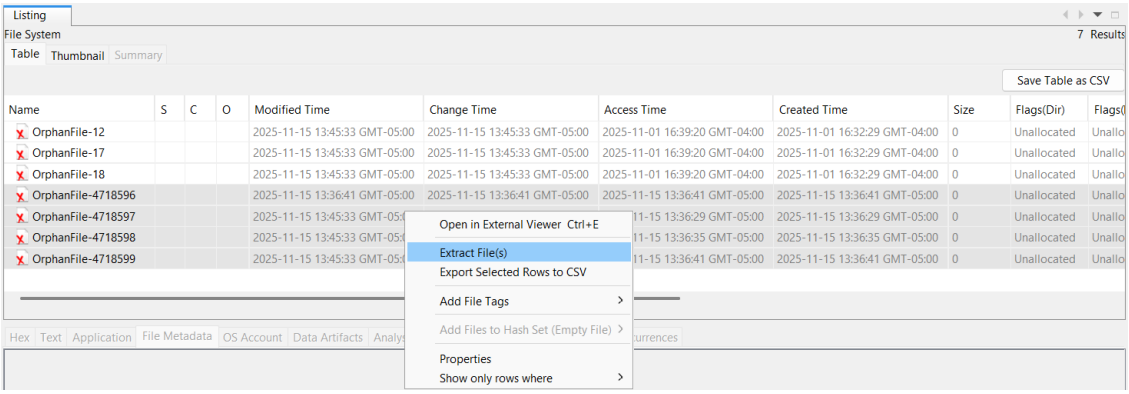


Browsing and Recovering Deleted Files

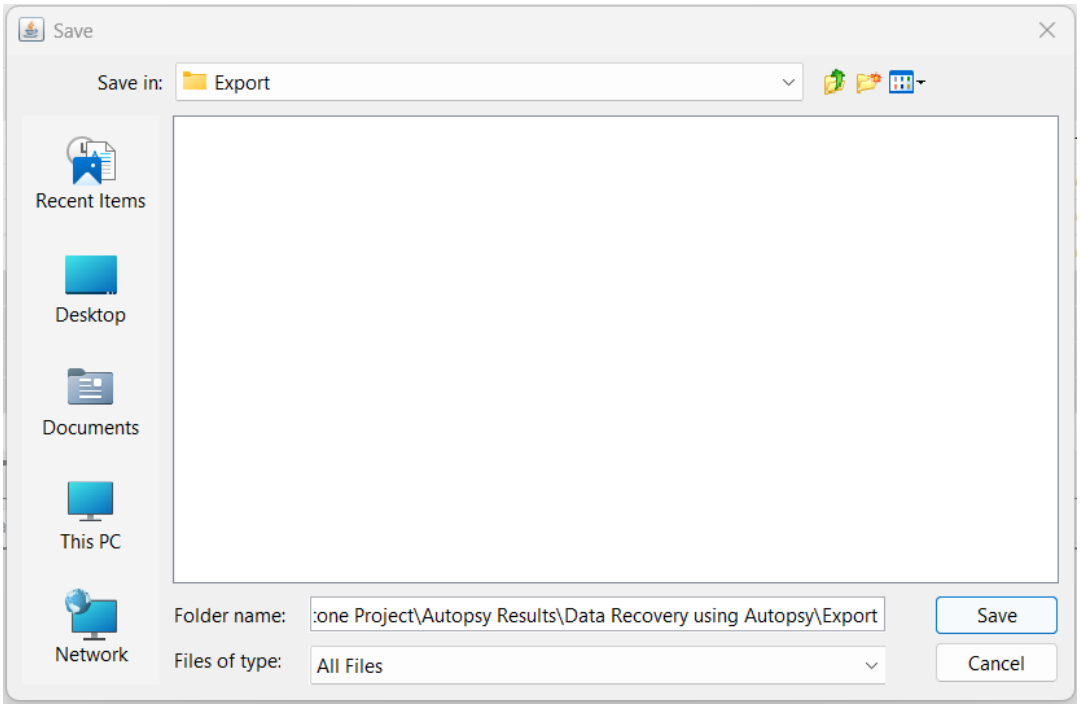
1. Now in the Tree viewer panel (on the left-hand side), Expand “Files Views” > “Deleted Files”



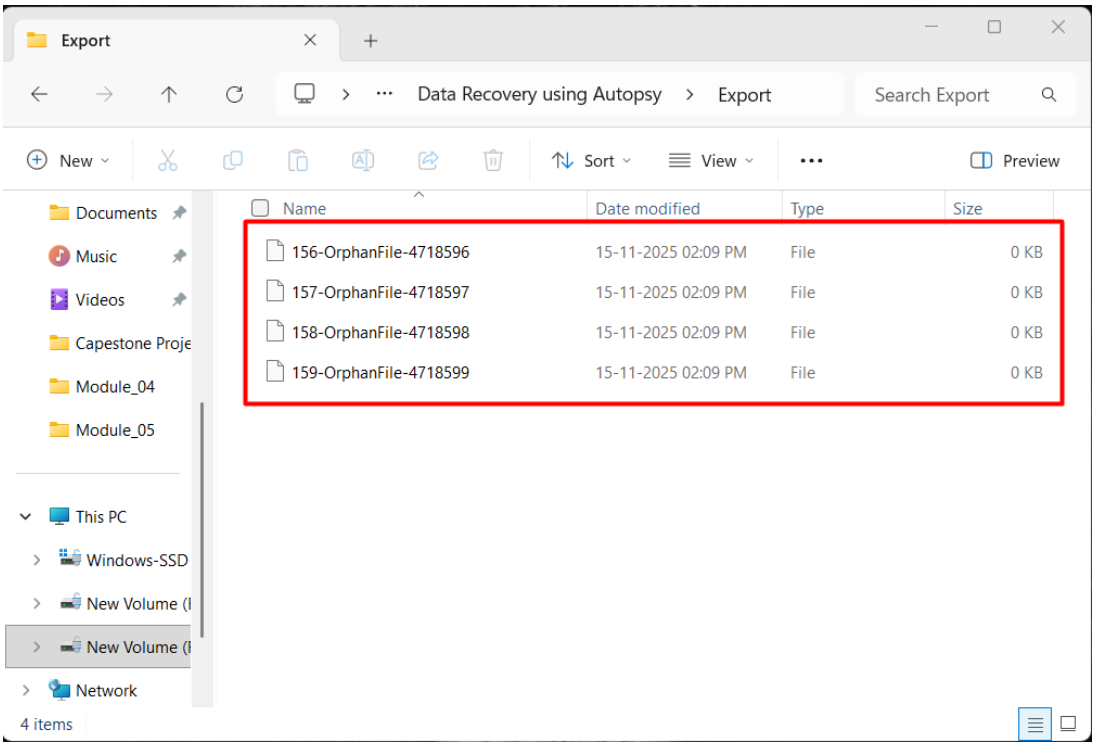
2. In the Result Viewer pane (on the right-hand side), click on the files that we want to recover and now click Extract Files.



Click Save.



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 using Autopsy\Export.



Track Recovery Time

Event	Start Time	End Time
Case Opened	**13:46:34.767**	-
Case Closed	-	**14:12:22.358**
Ingest Job Attempt	13:49:21.781	13:49:24.208 (Cancelled/Finished)