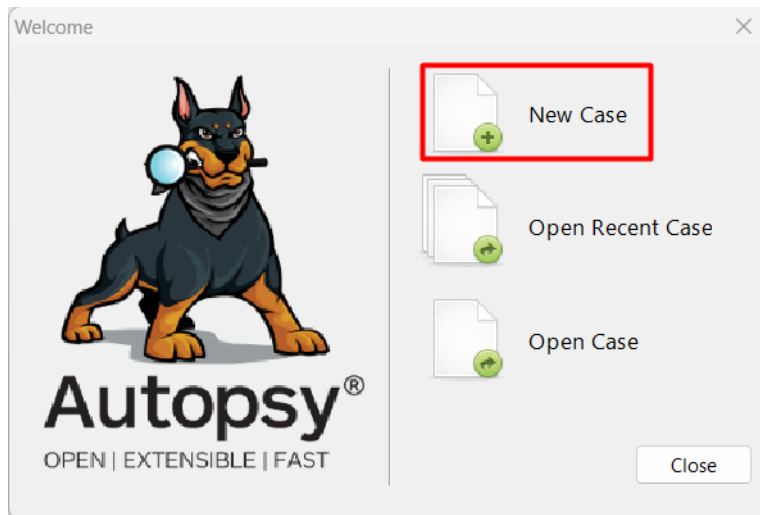


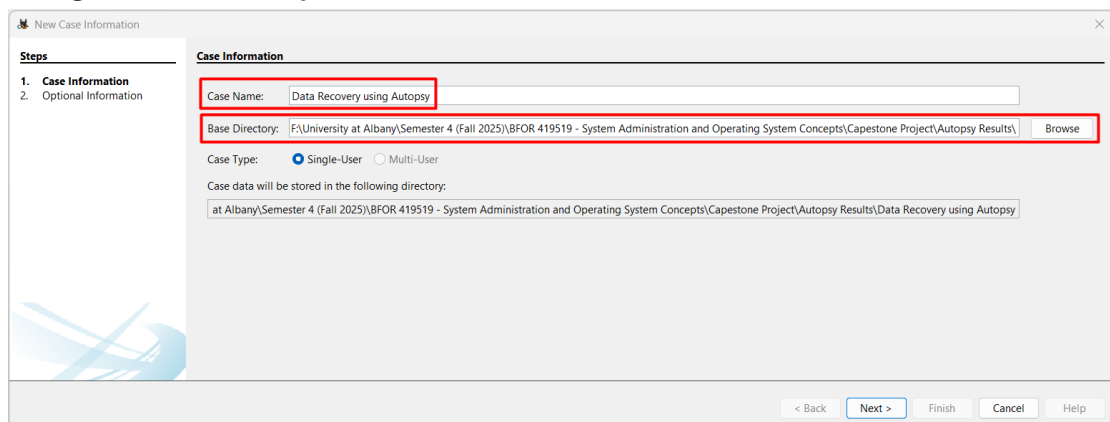
Autopsy Configuration

Open Autopsy & Case Setup

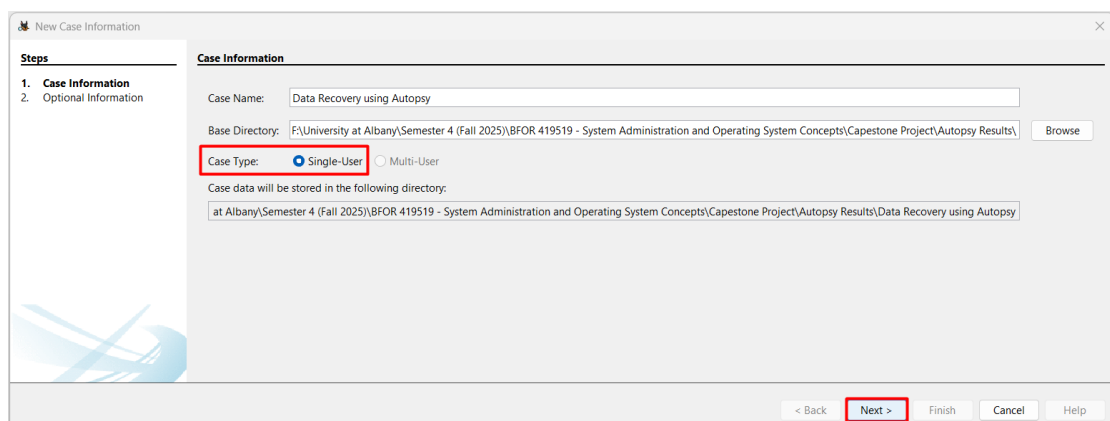
1. Now start autopsy, click New Case button in the welcome window.



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.



- 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.

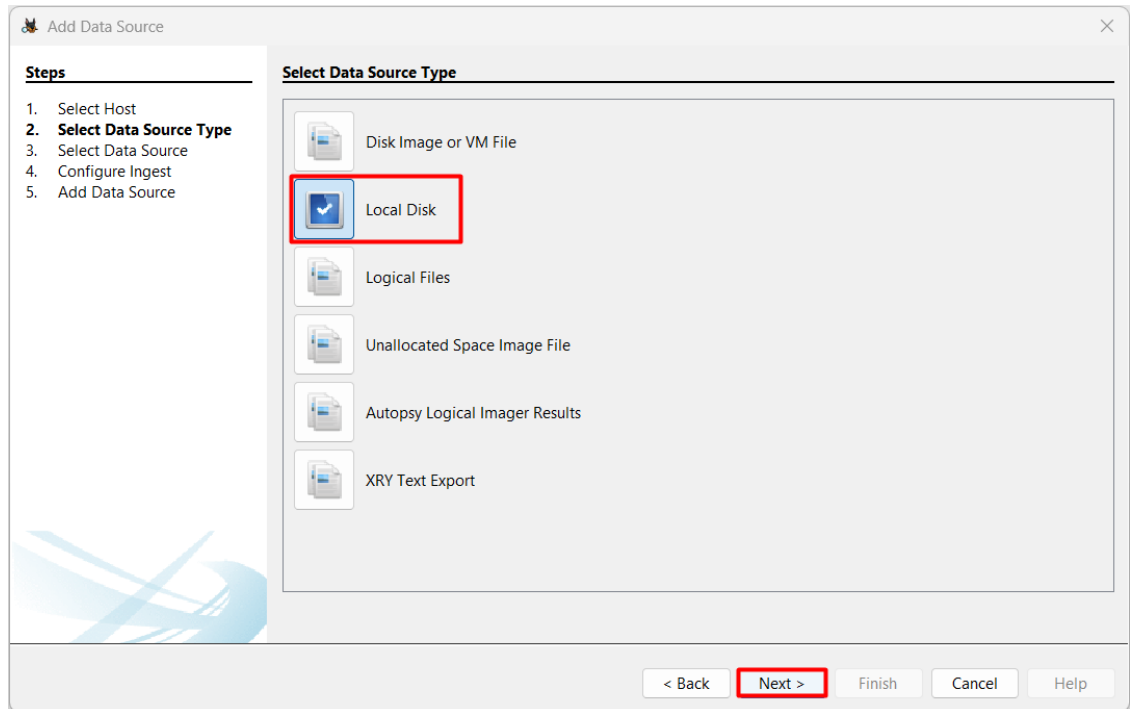
The screenshot shows the 'New Case Information' window with the 'Optional Information' tab selected. The 'Case' section has a 'Number' field containing '1'. The 'Examiner' section has a 'Name' field containing 'Siva Shankar Reddy Beeram'. The 'Organization' section has a dropdown menu set to 'Not Specified' and a 'Manage Organizations' button. The 'Steps' sidebar on the left shows '1. Case Information' and '2. Optional Information'. The bottom navigation bar includes '< Back', 'Next >', 'Finish', 'Cancel', and 'Help' buttons.

ADD Data Source

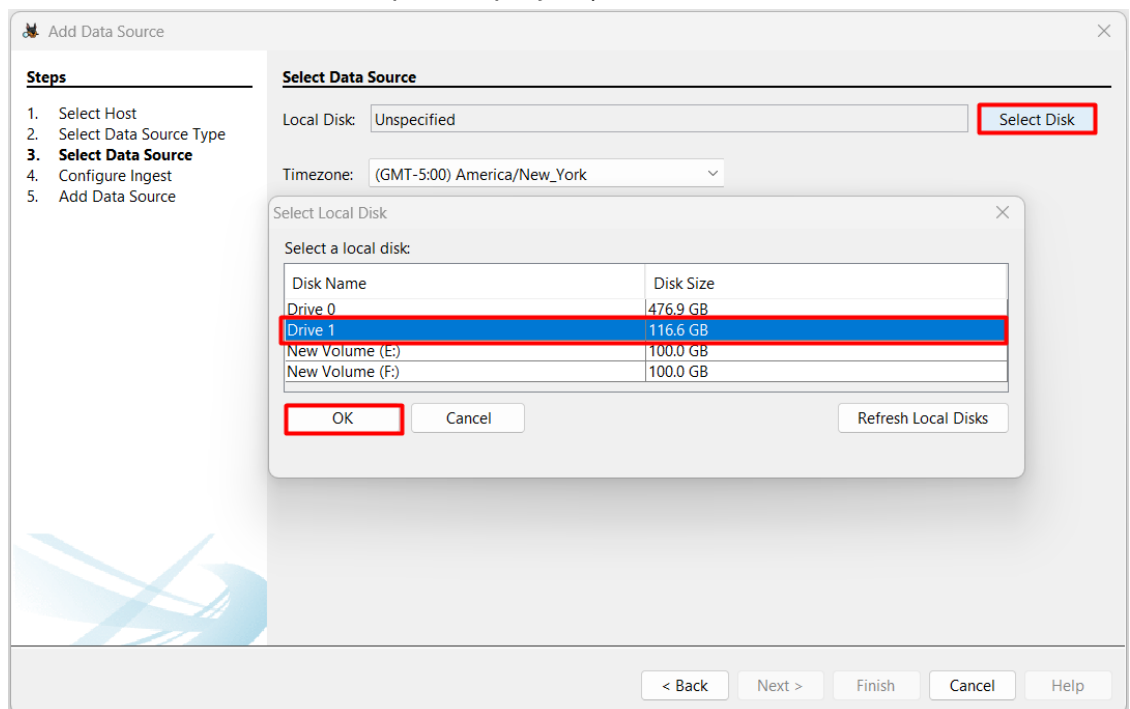
- Select the option Generate new host name based on data source name in the select host step and click next to move to next step.

The screenshot shows the 'Add Data Source' window with the 'Select Host' tab selected. The 'Steps' sidebar on the left shows '1. Select Host', '2. Select Data Source Type', '3. Select Data Source', '4. Configure Ingest', and '5. Add Data Source'. The 'Select Host' section has a heading 'Hosts are used to organize data sources and other data.' and three radio button options: 'Generate new host name based on data source name' (selected), 'Specify new host name', and 'Use existing host'. The bottom navigation bar includes '< Back', 'Next >', 'Finish', 'Cancel', and 'Help' buttons.

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.



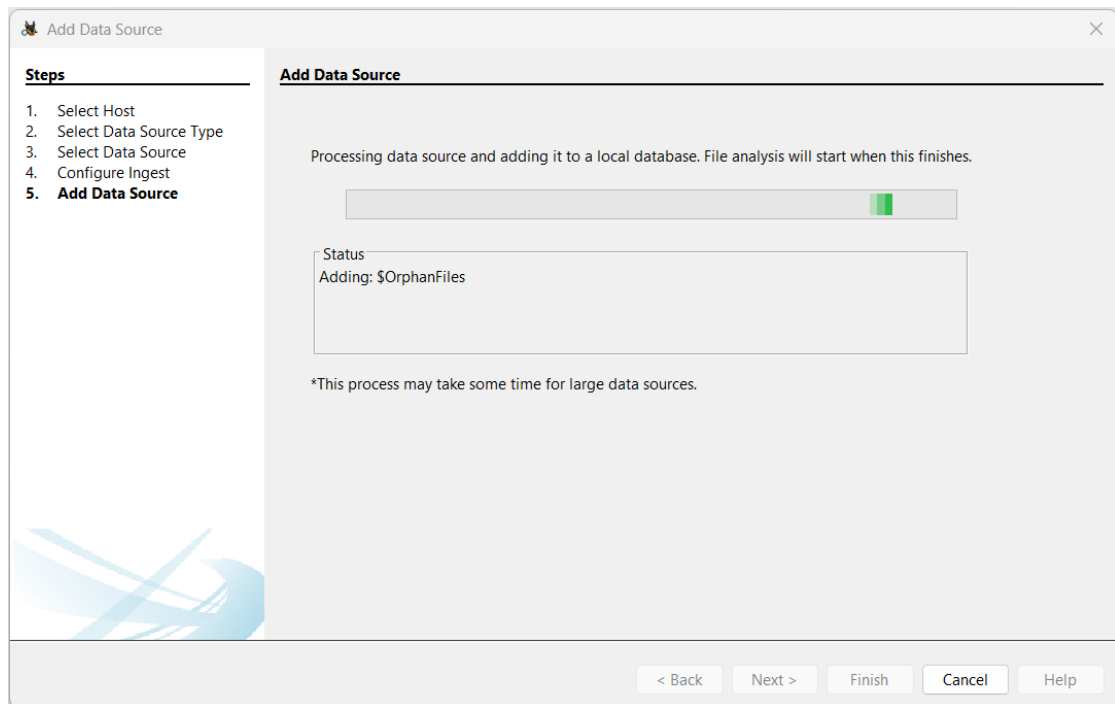
4. Now we can see the USD Drive (Drive 1) is selected and now check the box Ignore Orphan files in FAT file systems for fast results and click next.

The screenshot shows the 'Add Data Source' window with the 'Select Data Source' tab active. On the left, a 'Steps' list shows '3. Select Data Source' as the current step. The main area has 'Local Disk: Drive 1' selected in a dropdown, with a 'Select Disk' button to its right. Below this, the 'Timezone' is set to '(GMT-5:00) America/New_York'. A checkbox labeled 'Ignore orphan files in FAT file systems' is checked and highlighted with a red box; a note below it says '(faster results, although some data will not be searched)'. There is an unchecked checkbox for 'Make a VHD image of the drive while it is being analyzed' with a text field containing 'topsy\ModuleOutput\Image Writer\Drive 1 1762889563656.vhd' and a 'Browse' button. Below that is an unchecked checkbox for 'Update case to use VHD file upon completion' and a note: 'Note that at least one ingest module must be run to create a complete copy'. The 'Sector Size' is set to 'Auto Detect'. At the bottom, navigation buttons include '< Back', 'Next >' (highlighted with a red box), 'Finish', 'Cancel', and 'Help'.

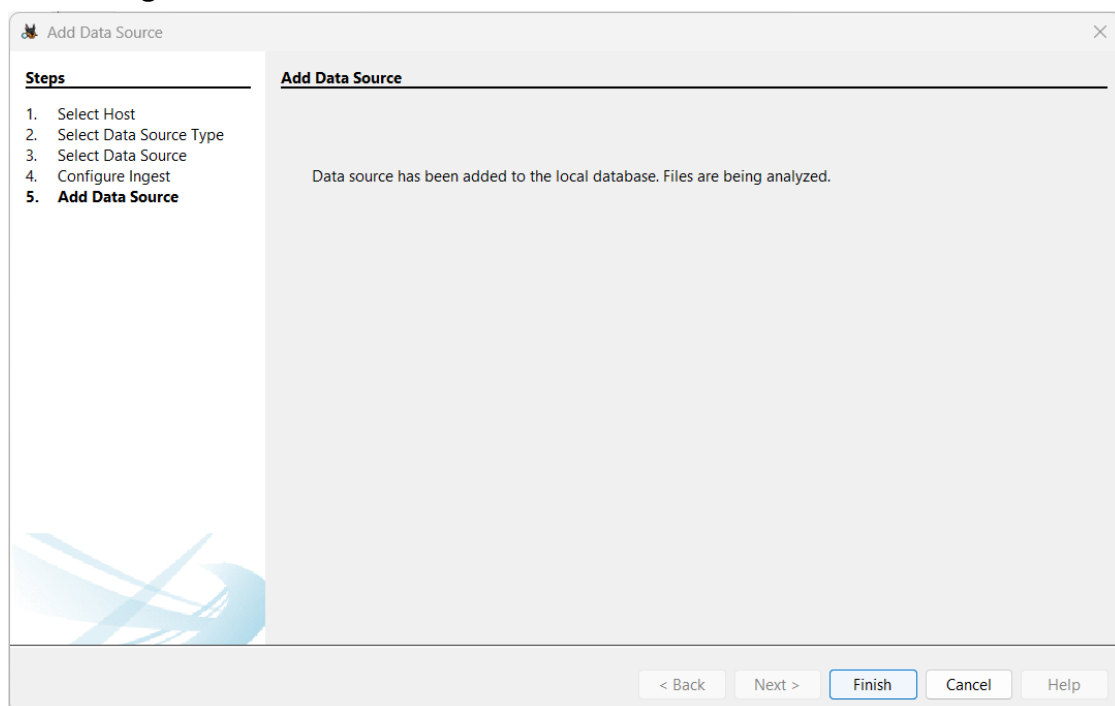
5. In the Configure Ingest area of the Add Data Source window, enable modules such as “File Type Identification” and “Carve Files.” This ensures deleted file recovery and scans for both file system entries and raw fragments.

The screenshot shows the 'Add Data Source' window with the 'Configure Ingest' tab active. The 'Steps' list on the left shows '4. Configure Ingest' as the current step. The main area has a dropdown for 'Run ingest modules on:' set to 'All Files, Directories, and Unallocated Space'. Below this is a list of modules with checkboxes, all of which are checked: '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', and 'Virtual Machine Extractor'. At the bottom of this list are buttons for 'Select All', 'Deselect All', and 'History'. To the right of the module list is a text box that says 'The selected module has no per-run settings.' and another section that says 'Module that extracts GEO data from GPX files.' with a 'Global Settings' button. At the bottom of the window, navigation buttons include '< Back', 'Next >' (highlighted with a blue box), 'Finish', 'Cancel', and 'Help'.

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

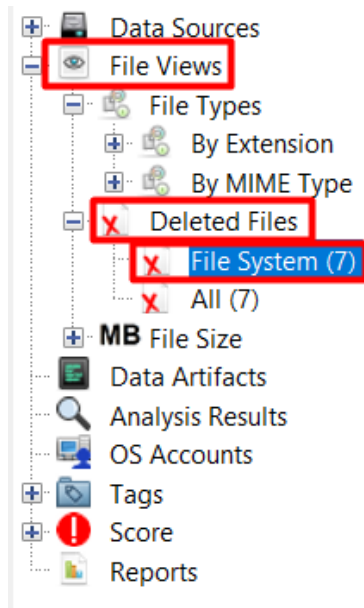


7. Once the data is analysed successfully, we can see a successful message confirming that data has added.

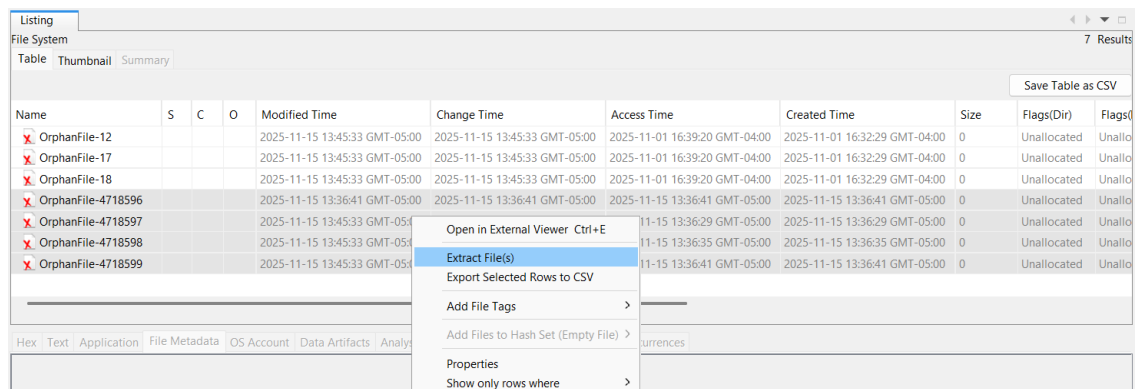


Browsing and Recovering Deleted Files

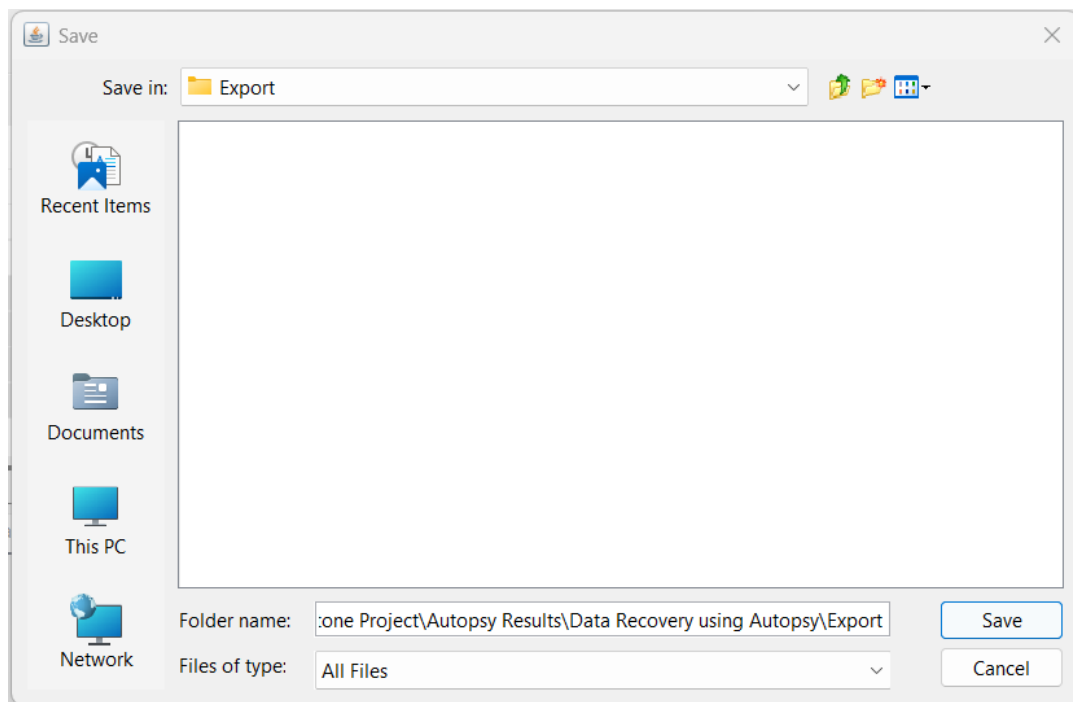
1. Now in the Tree viewer panel (on the left-hand side), Expand “Files Views” > “Deleted Files”



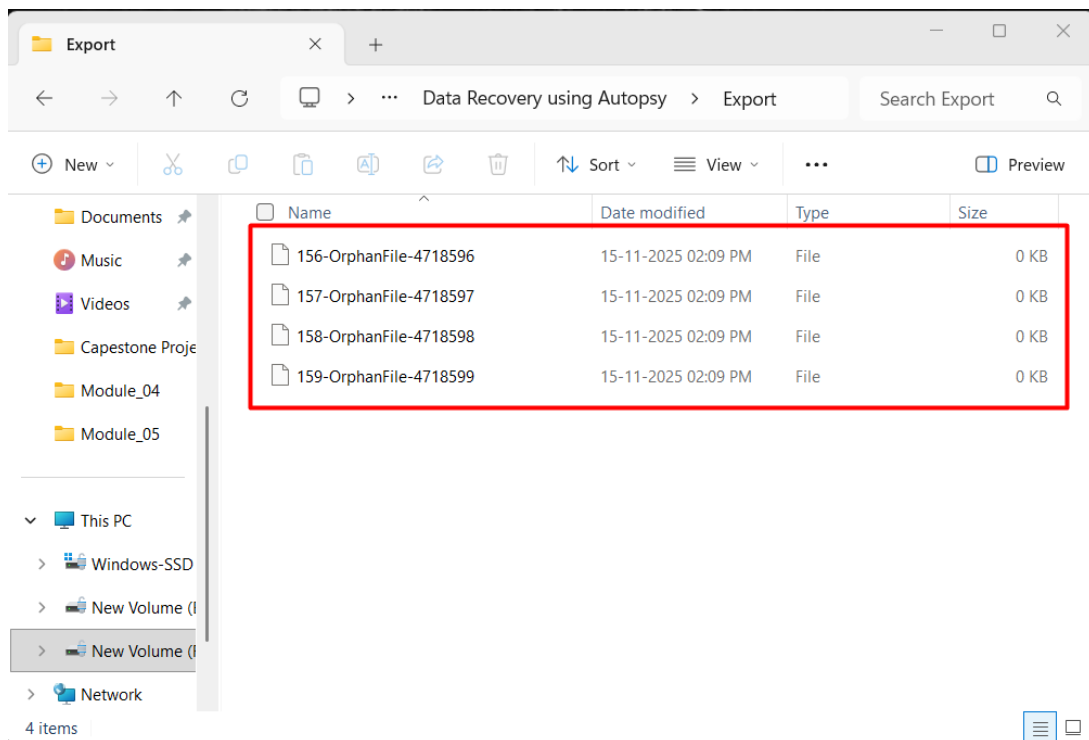
2. In the Result Viewer pane (on the right-hand side), click on the files that we want to recover and now click Extract Files.



Click Save.



- 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)