

# EXP 4: Using-the-Autopsy-retrieve-the-deleted-files

---

## AIM:

---

To install Autopsy software on windows operating system and analyse the file and folder configuration.

## EQUIPMENT REQUIRED:

---

- Hardware: Personal Computer (PC)

Register Number:212223100035  
Name: Muhammad Afshan A



## DESIGN STEPS:

---

### 1. Copy Files to the Virtual Disk

- Open File Explorer → Go to the new drive ( E: ), where the folder created in the New Virtual Disk
- Create a new folder or use the entire disk and then copy **images or files** into it.

### 2. Delete the Files

- Select any one or two images → Press **Delete**.
- Empty the **Recycle Bin** to permanently delete them.

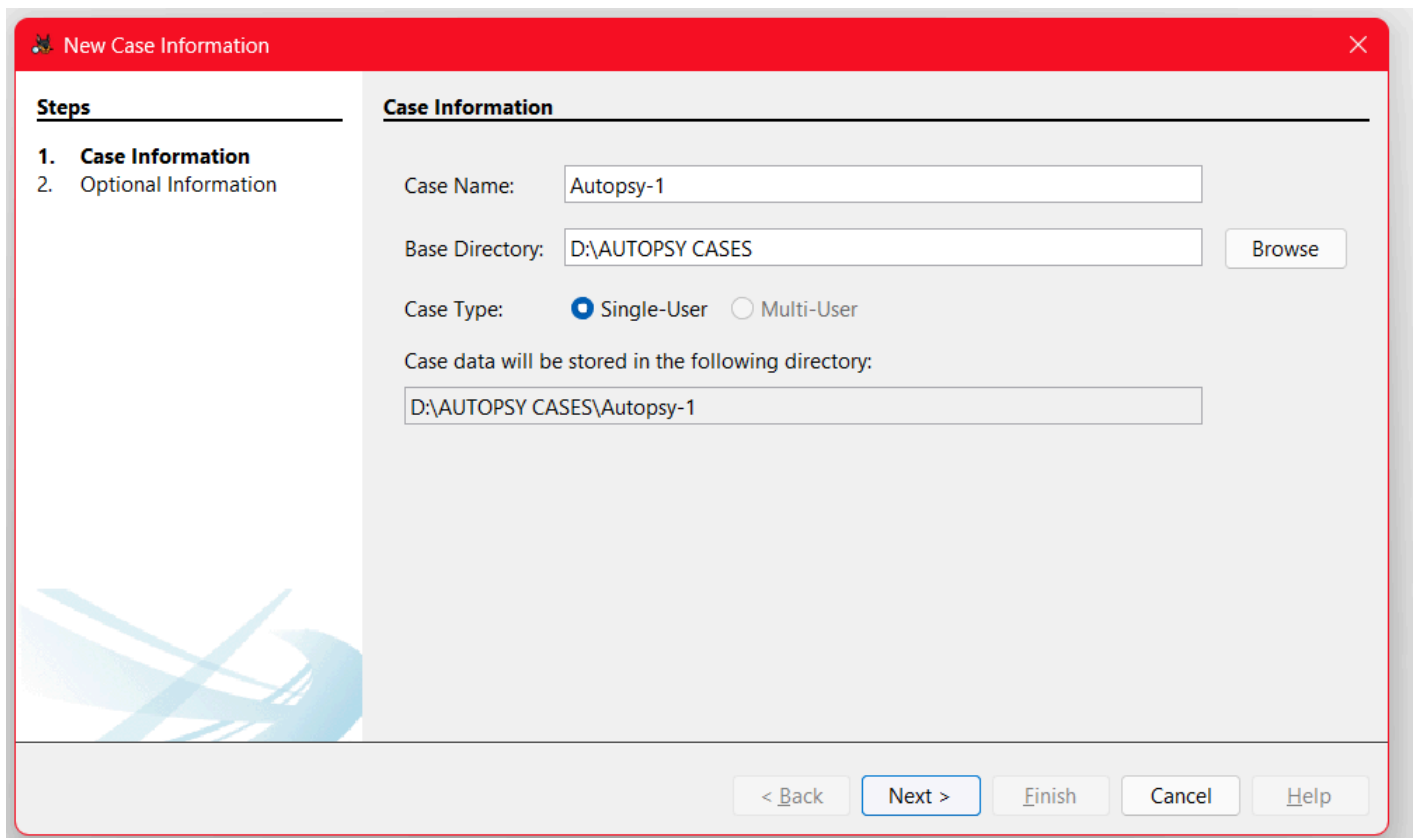
### 3. Recover Deleted Files Using Autopsy

#### Open Autopsy & Create a New Case

- Launch **Autopsy** and Run as a administrator
- Click **Create New Case**.

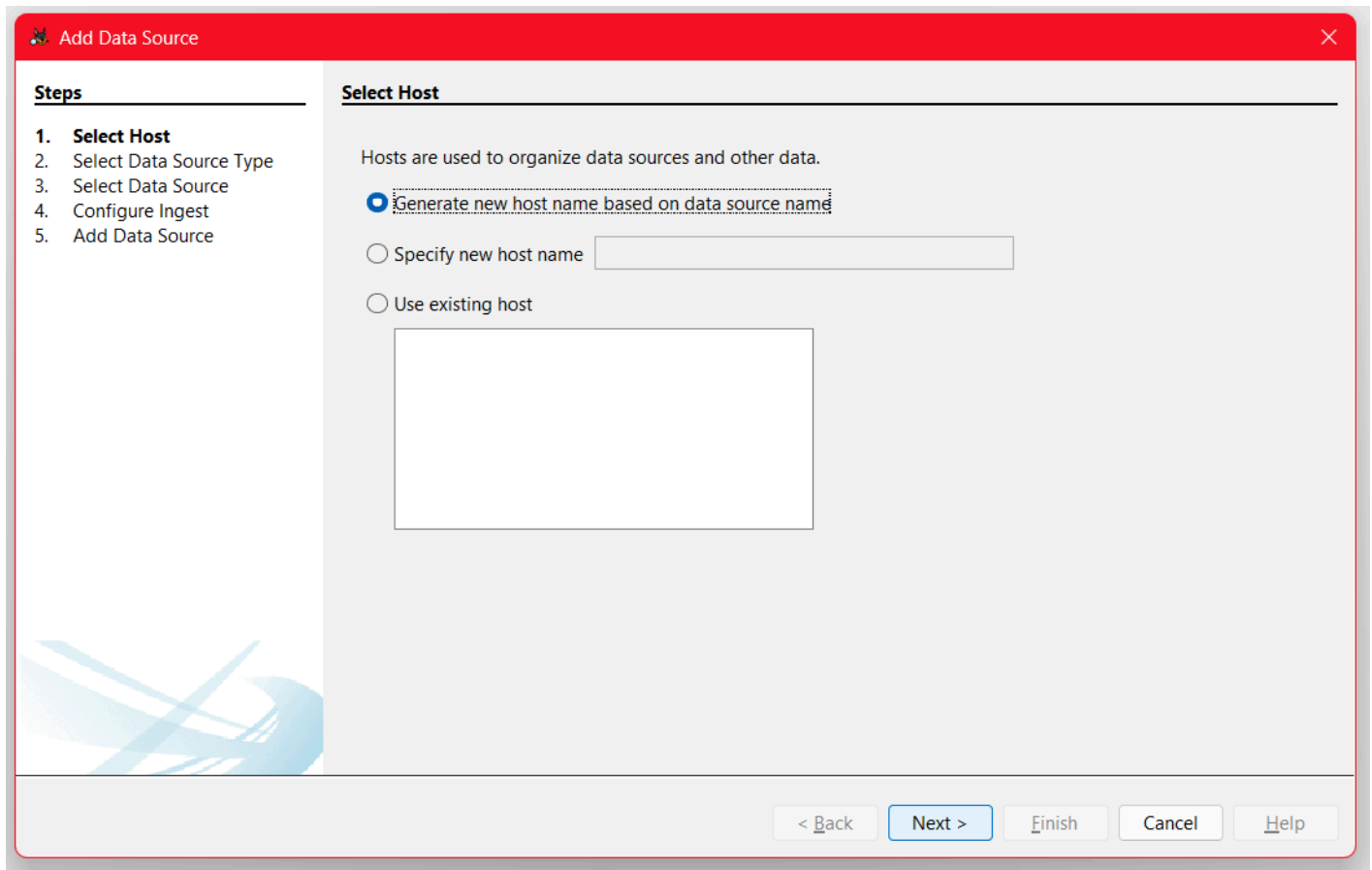


- Enter a **Case Name** (e.g., Autopsy-1 ).
- Choose a **Case Folder** location.
- Click **Next** → Click **Finish**.

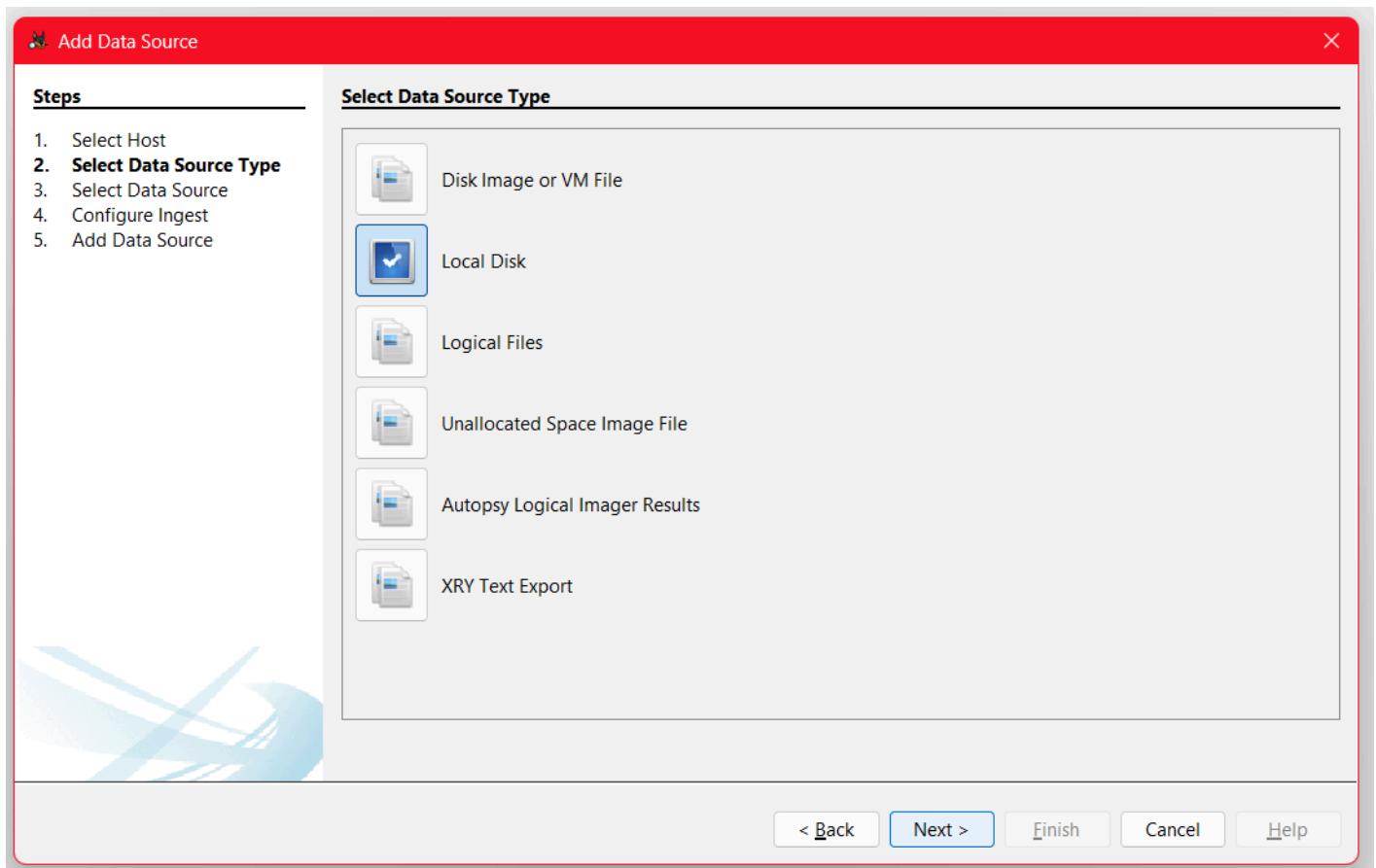
The image shows the 'New Case Information' dialog box. The title bar is red and contains the text 'New Case Information' and a close button (X). The dialog is divided into two main sections. On the left, under the heading 'Steps', there is a list: '1. Case Information' and '2. Optional Information'. The right section, titled 'Case Information', contains several input fields and buttons. The 'Case Name' field has 'Autopsy-1' entered. The 'Base Directory' field has 'D:\AUTOPSY CASES' entered, with a 'Browse' button to its right. The 'Case Type' section has two radio buttons: 'Single-User' (which is selected) and 'Multi-User'. Below this, a text label says 'Case data will be stored in the following directory:', followed by a text field containing 'D:\AUTOPSY CASES\Autopsy-1'. At the bottom of the dialog, there are five buttons: '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'. The 'Next >' button is highlighted with a blue border.

## Add the Virtual Disk as an Evidence Source

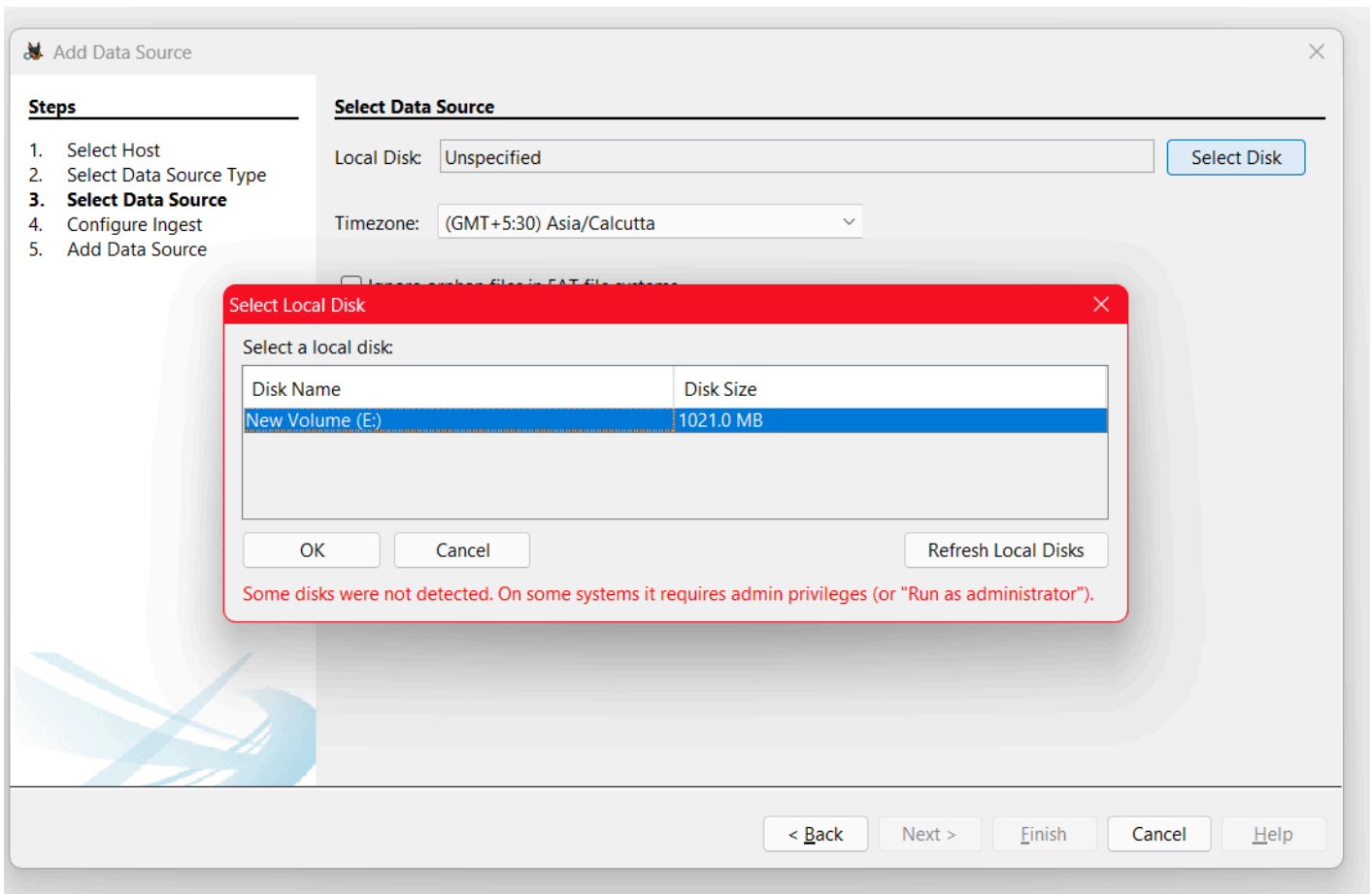
- Click Add Data Source → Select Host



- Select Local Disk → next



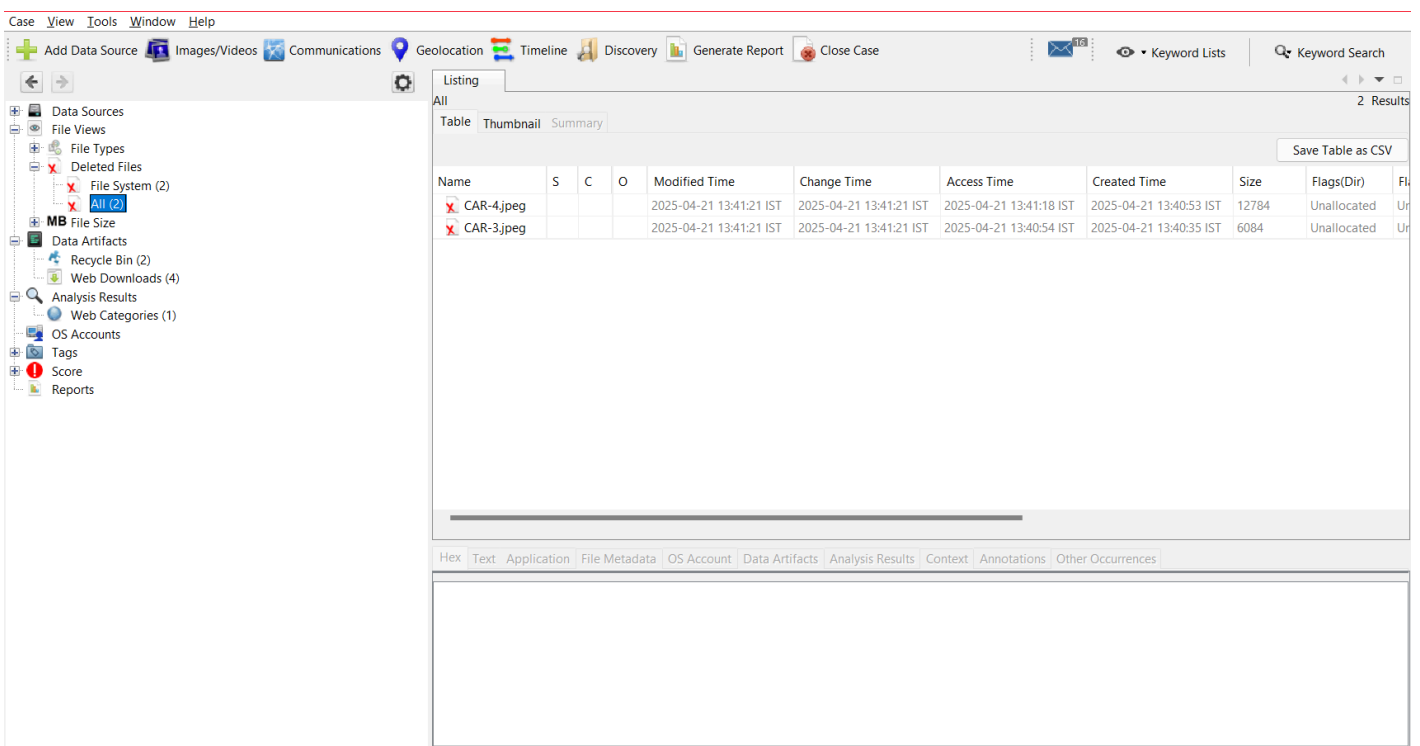
- Select Disk → Choose the VHD drive ( New Volume(E:))



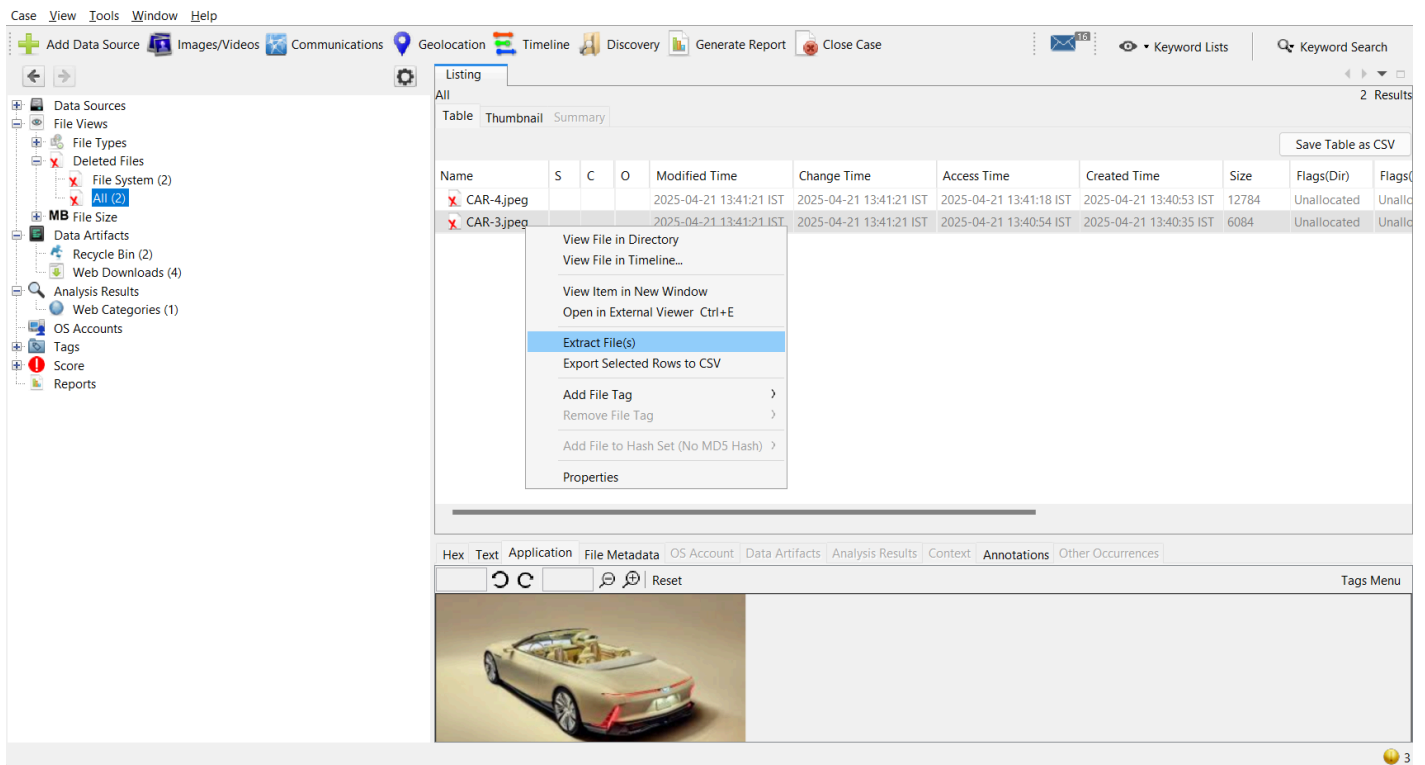
- Click **Next** → Keep default settings → Click **Finish**.
- Wait for Autopsy to process the disk.

## Recover Deleted Files

- Go to File Views (left panel).



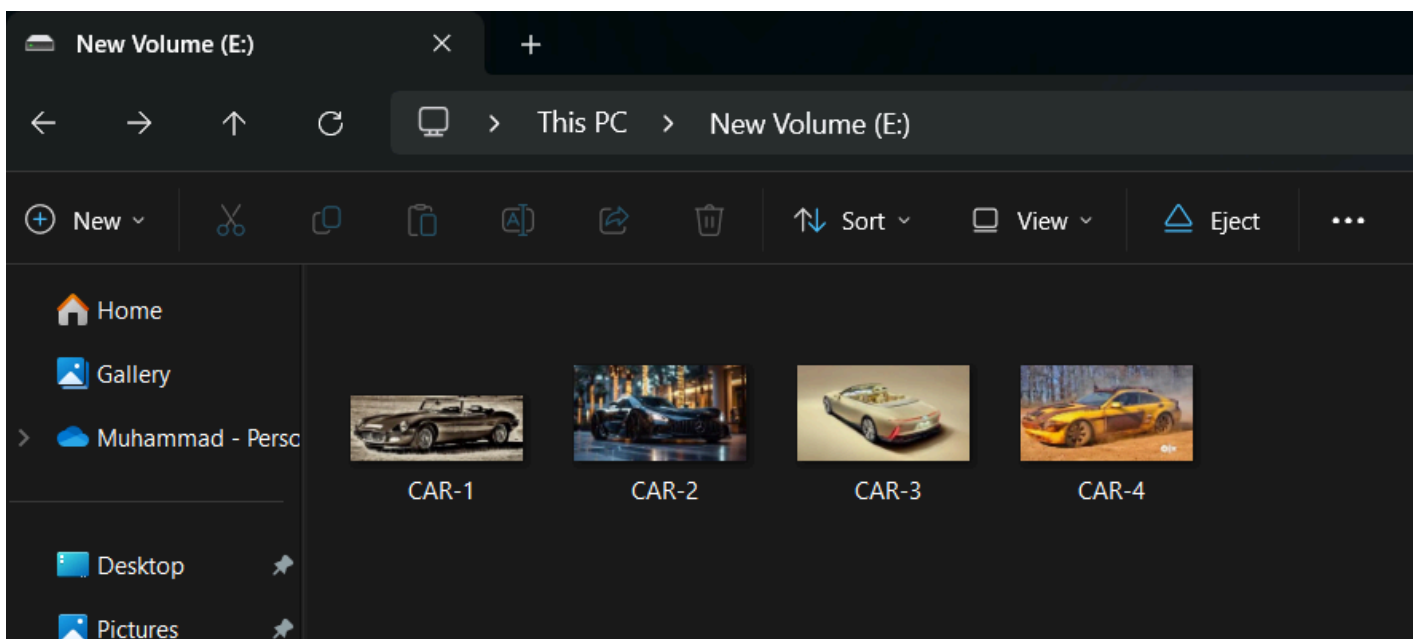
- Click **Deleted Files** → Find your deleted images.
- Right-click an image → Click **Extract File**.



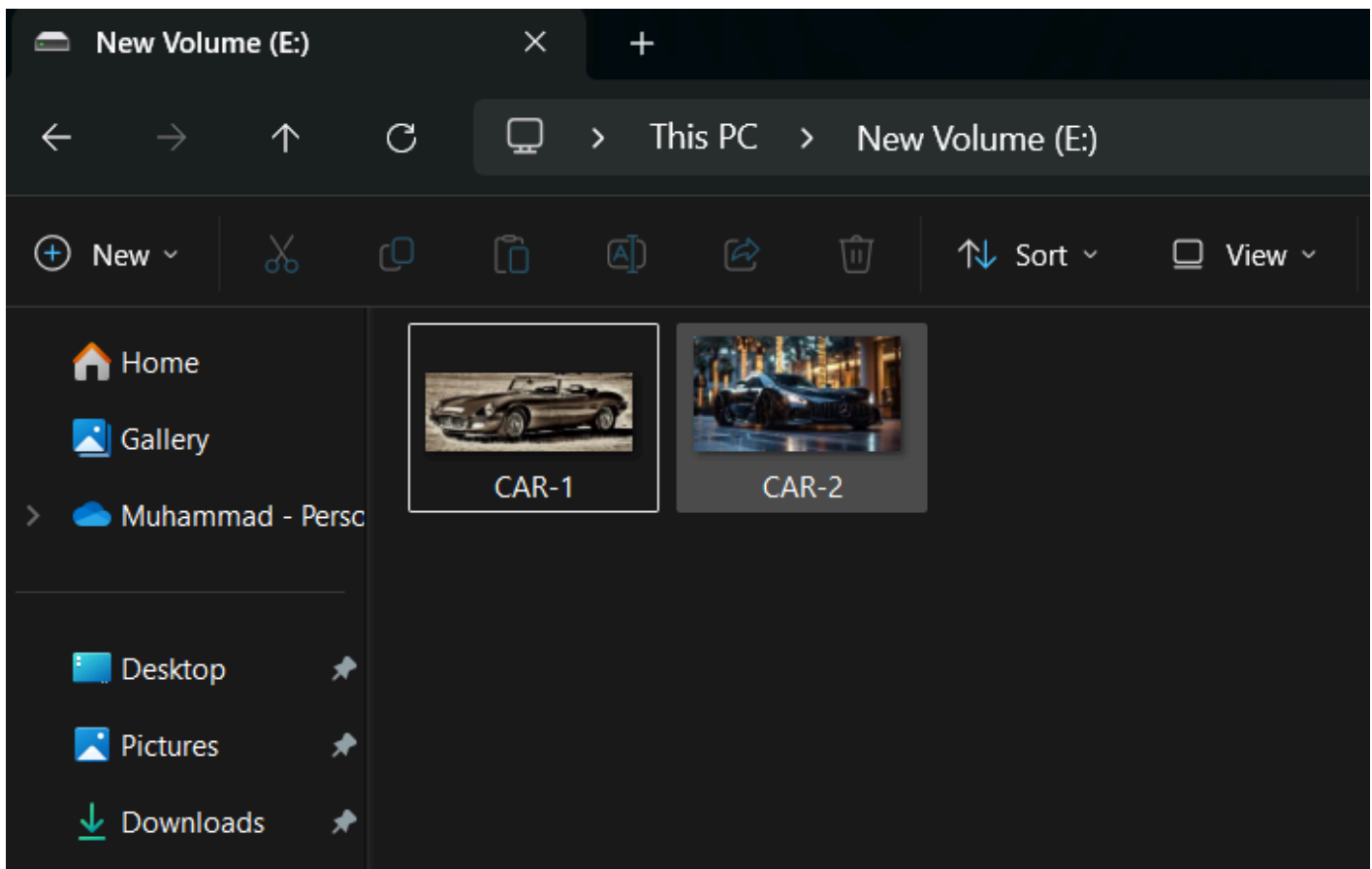
- Select a folder to see the recovered files (e.g., K:\DFDI-Extracted ).
- Image is recovered successfully.

## Output :

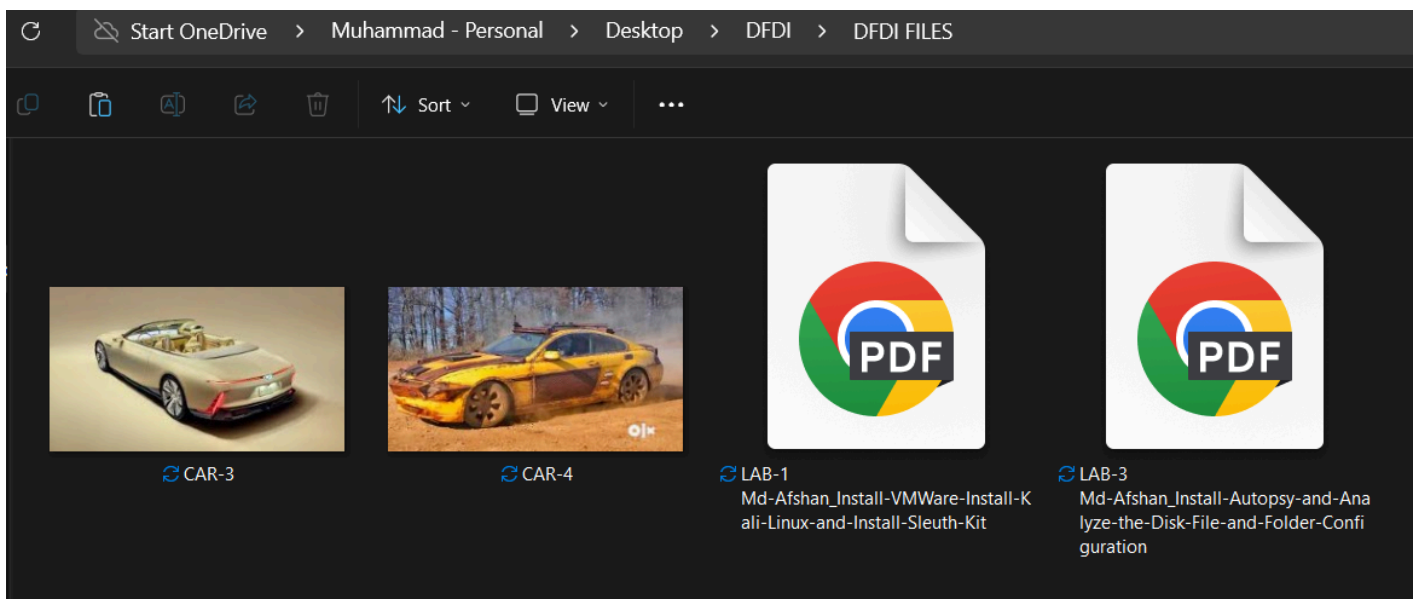
### Folder before deleting the files



### Folder after deleting the files



## Folder after extracting the deleted images using autopsy



## Result:

Successfully extracted the deleted files from unallocated space using the Autopsy tool.