

EXP 3 : INSTALL AUTOPSY AND ANALYSIS THE DISK, FILE AND FOLDER CONFIGURATION

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:

Step 1:

Install Autopsy using the terminal with the command:

Step 2:

Launch Autopsy from the terminal or application menu and create a new case.

Step 3:

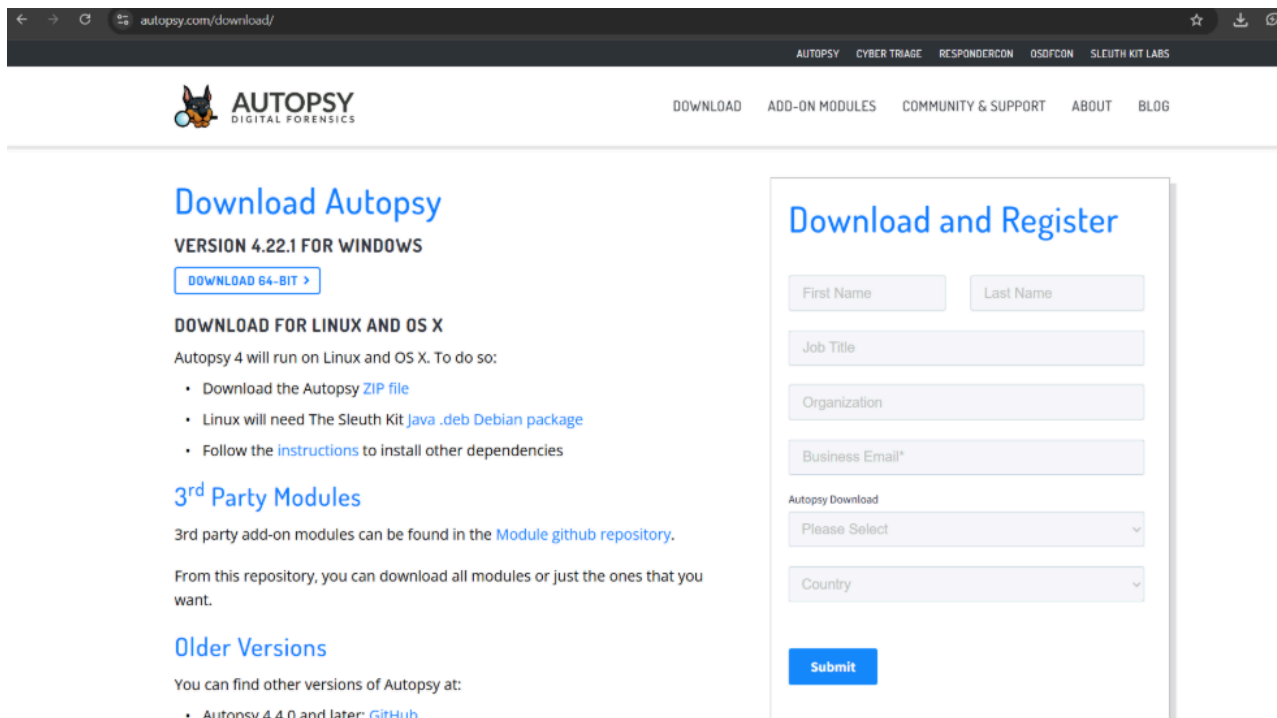
Add a disk image or file to the case and analyze the contents such as deleted files, metadata, and folder structure.

INSTALLATION PROCEDURE:

Step1:Download Autopsy

- Visit Autopsy Official Website and download the latest version.

- Double-click the downloaded file and follow the on-screen instructions.



The screenshot shows the Autopsy website's download and registration page. The header includes the Autopsy logo and navigation links: AUTOPSY, CYBER TRIAGE, RESPONDERCON, OSDFCON, SLEUTH KIT LABS, DOWNLOAD, ADD-ON MODULES, COMMUNITY & SUPPORT, ABOUT, and BLOG. The main content area is titled "Download Autopsy" and features a "VERSION 4.22.1 FOR WINDOWS" section with a "DOWNLOAD 64-BIT" button. Below this is a "DOWNLOAD FOR LINUX AND OS X" section with instructions and links for downloading the ZIP file, Linux .deb package, and following installation instructions. A "3rd Party Modules" section mentions finding modules in the GitHub repository. An "Older Versions" section links to GitHub for previous versions. On the right, a "Download and Register" form is visible, containing fields for First Name, Last Name, Job Title, Organization, Business Email*, Autopsy Download (a dropdown menu), and Country, followed by a "Submit" button.

Implementation steps:

1. Copy Files to the Virtual Disk

- Open File Explorer → Go to the new drive (D:), 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

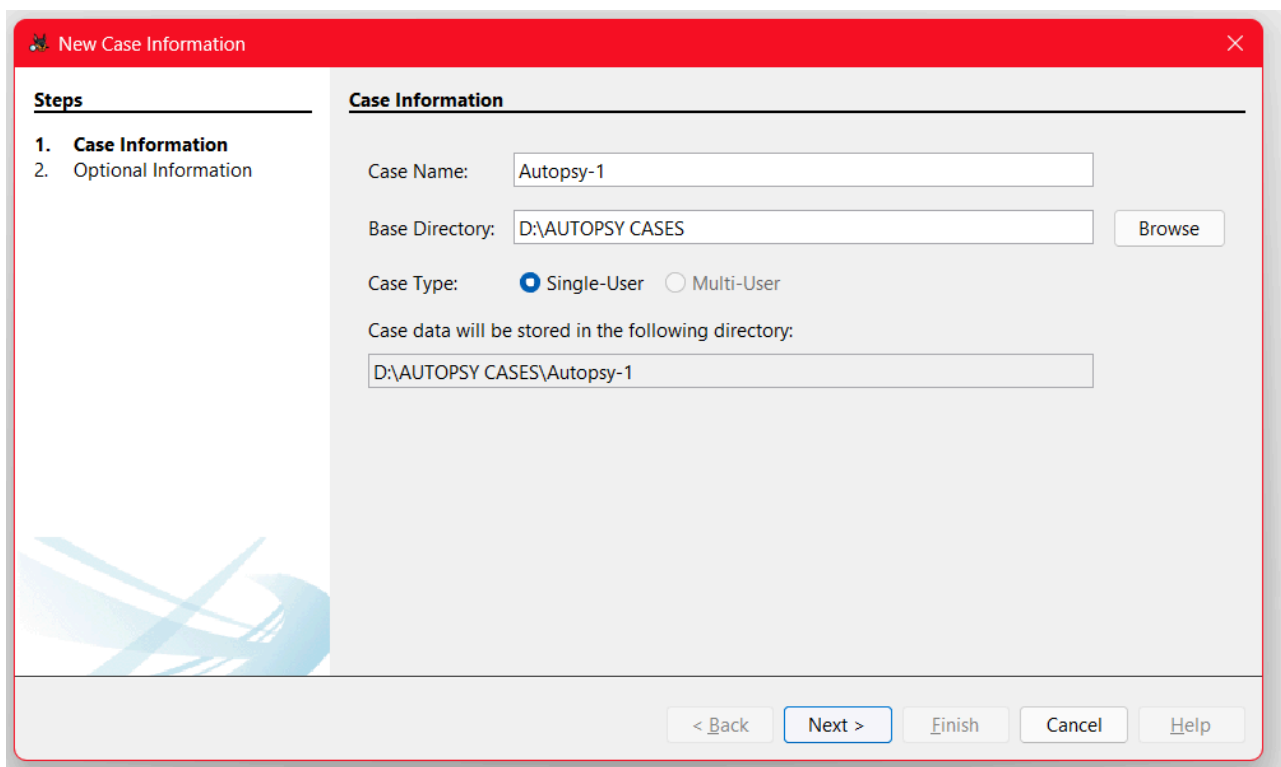
Open Autopsy & Create a New Case

- Launch **Autopsy** and **Run as a administrator**

- Click **Create New Case**.

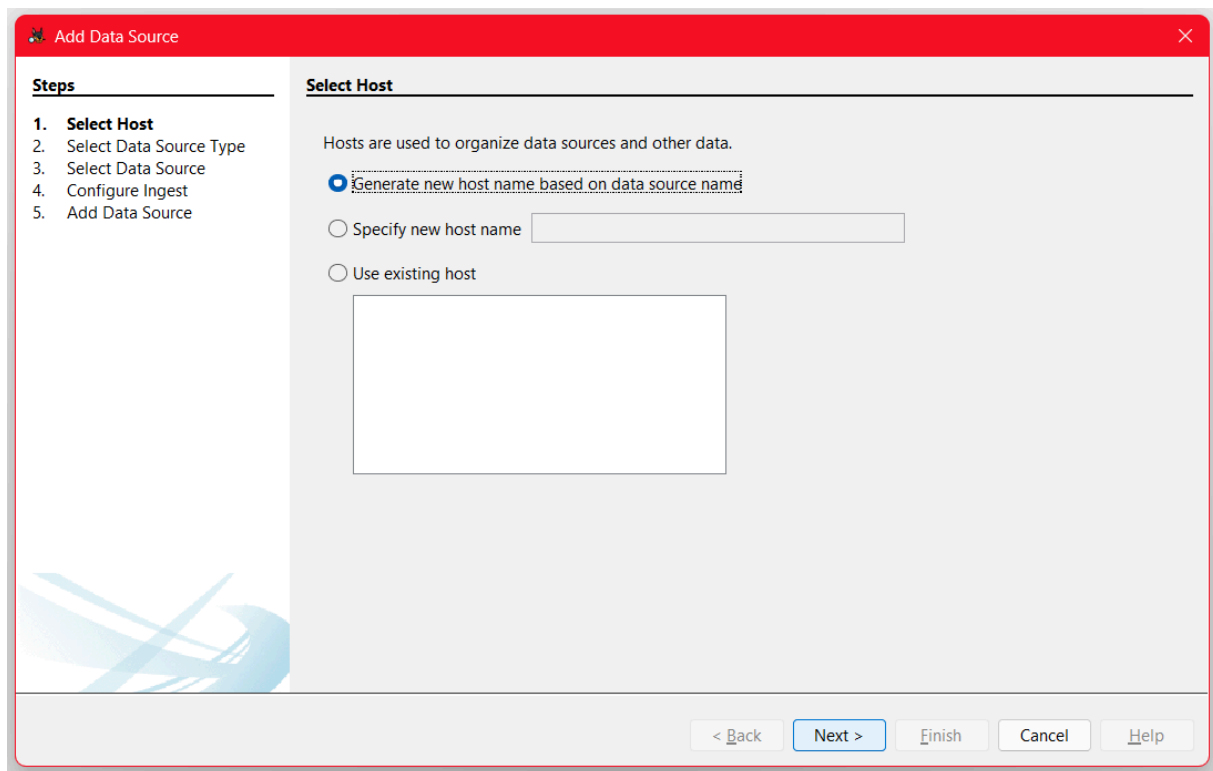


- Enter a **Case Name** (e.g., Autopsy-1).
- Choose a **Case Folder** location.
- Click **Next** → Click **Finish**.

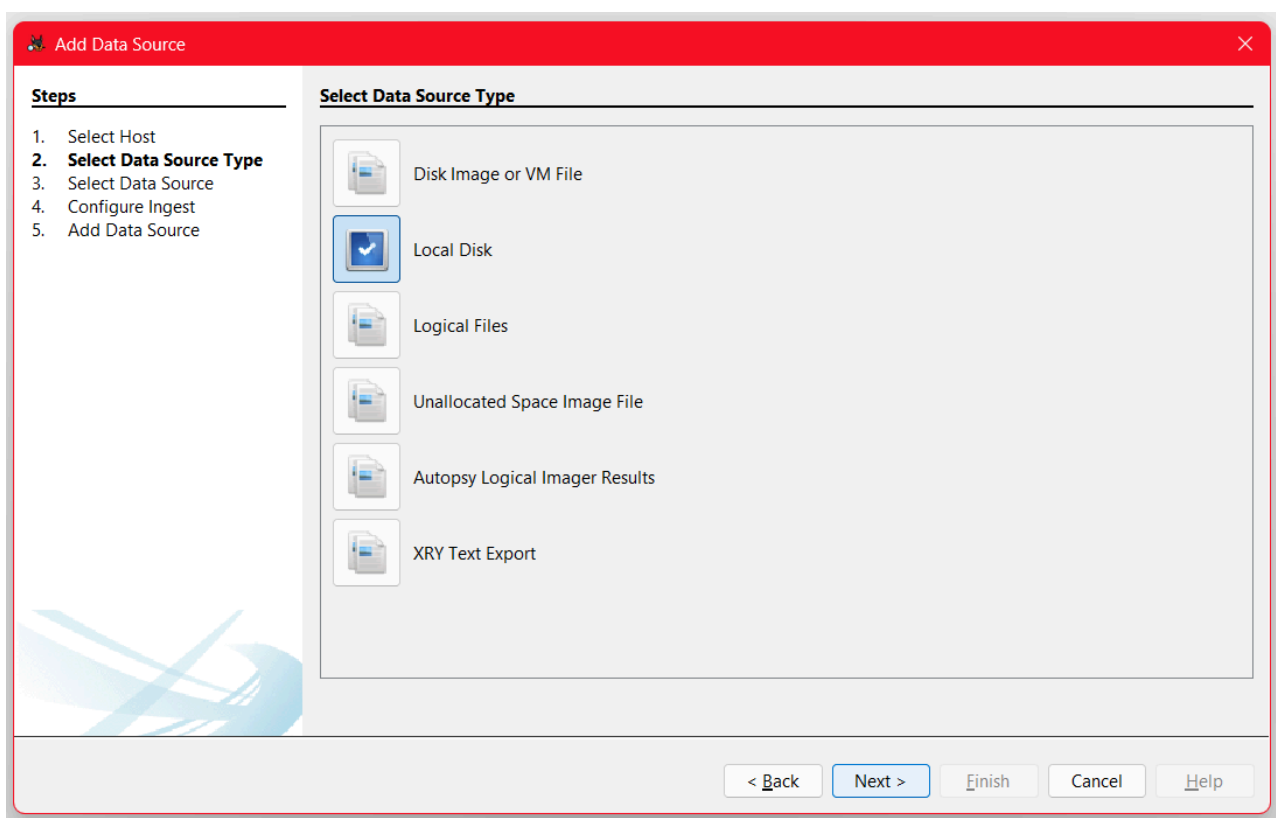


Add the Virtual Disk as an Evidence Source

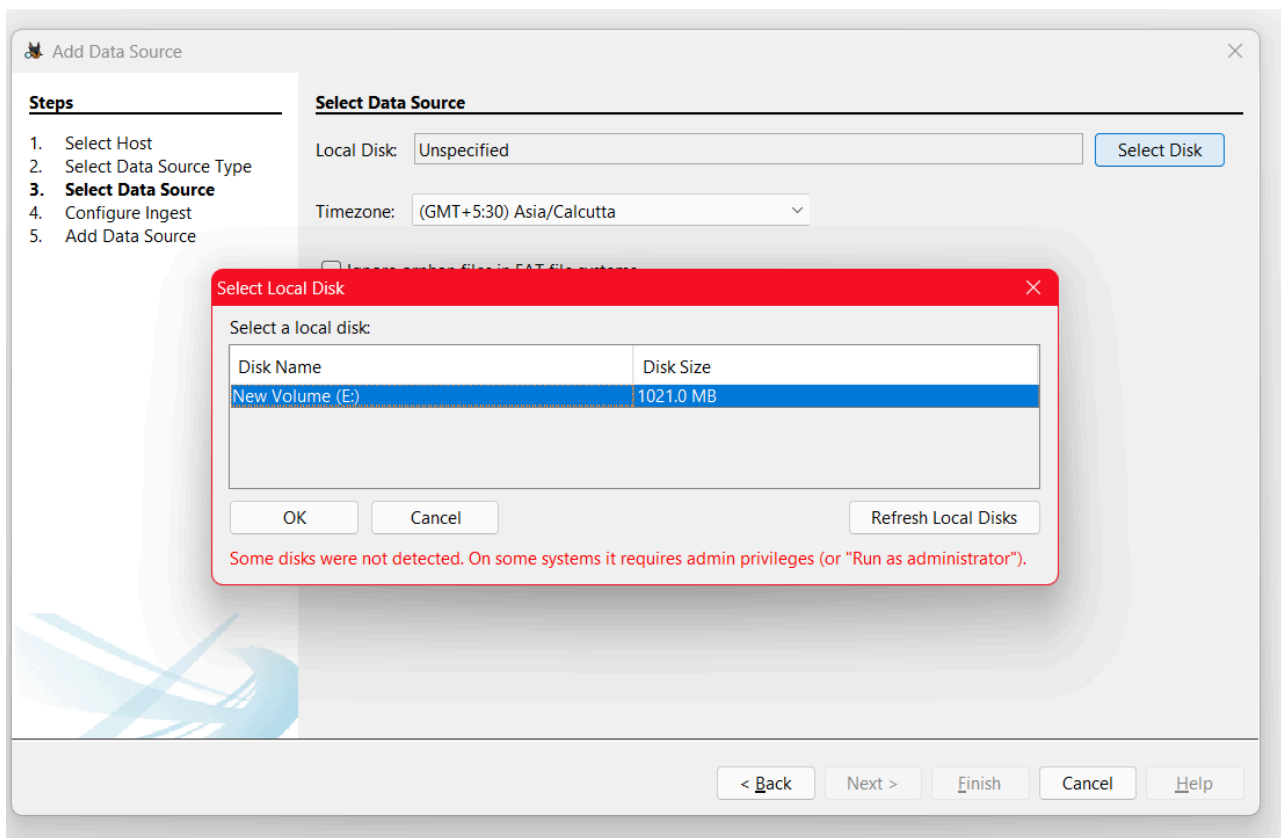
- Click Add Data Source → Select Host



- Select Local Disk → next



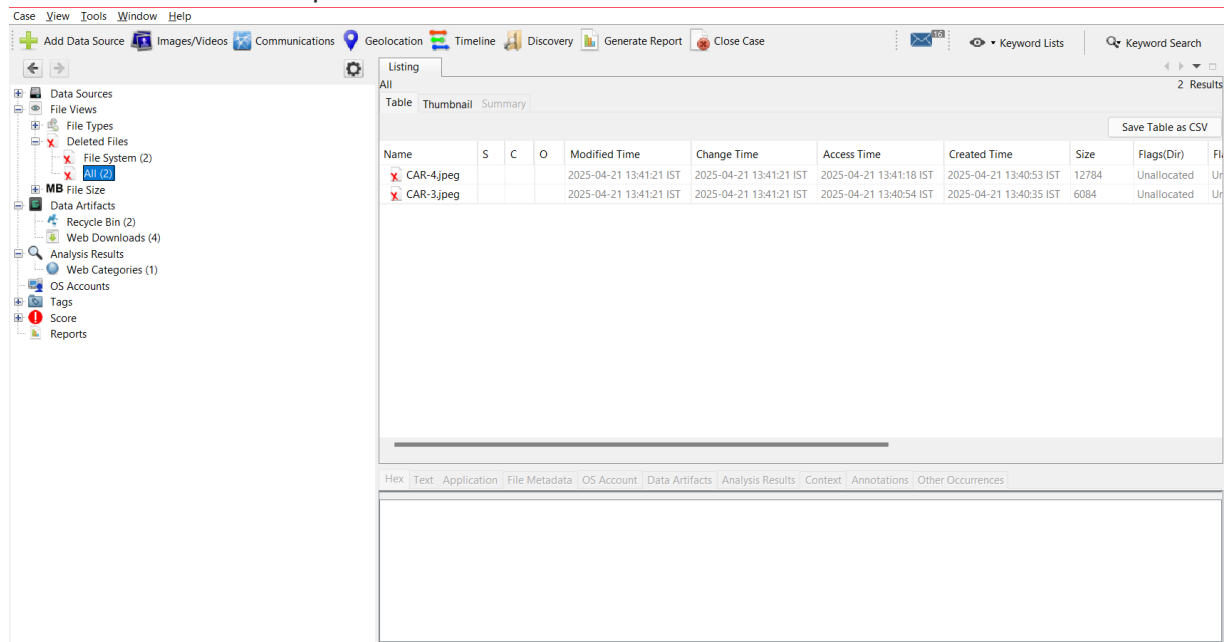
- Select Disk → Choose the VHD drive (New Volume(E:)



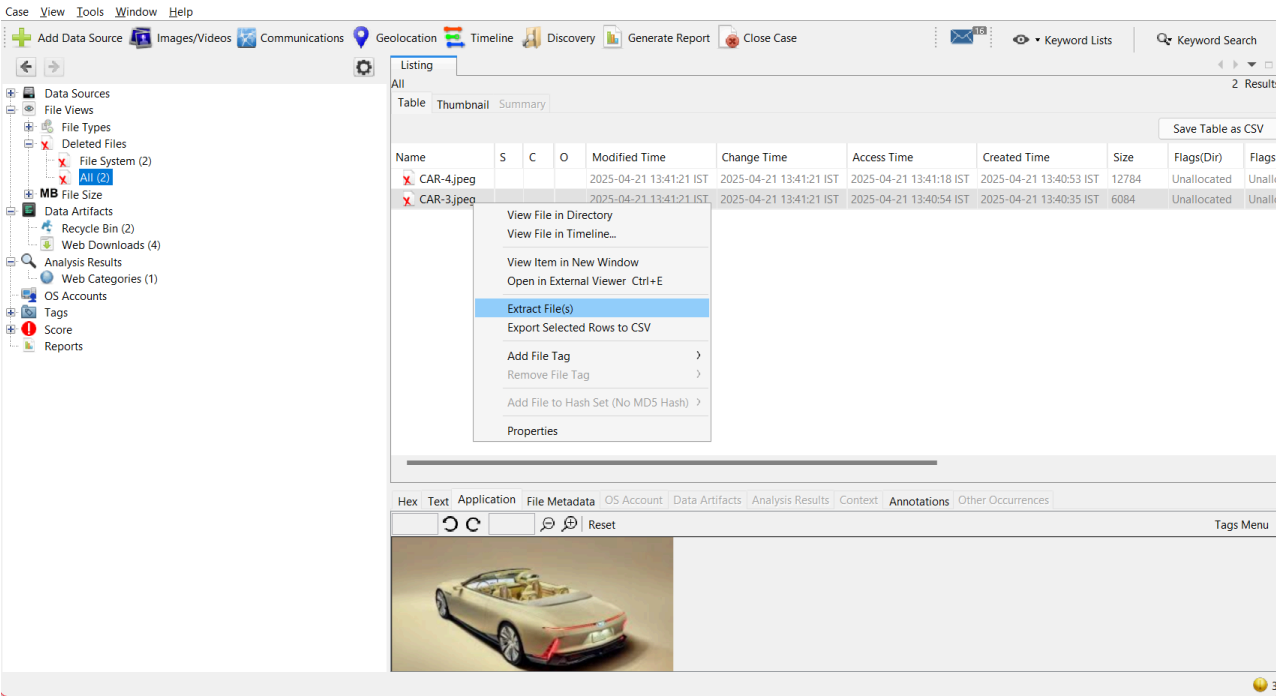
- Click **Next** → Keep default settings → Click **Finish**.
- Wait for Autopsy to process the disk.

Recover Deleted Files

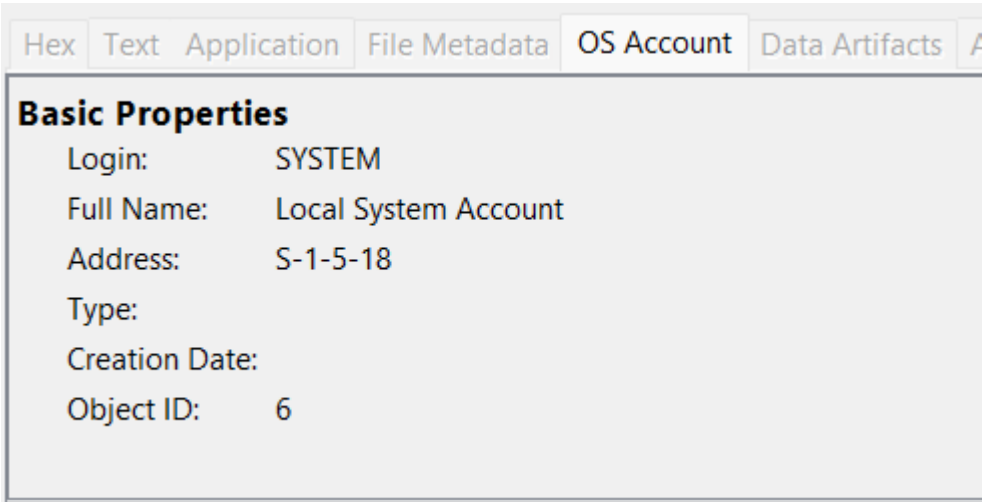
- Go to **File Views** (left panel).



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



- Click OS Account



Result:

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