AUTOPSY TOOL MANUAL

Made by
Moeez Javed

Made by Moeez Javed

Digital Forensics with Autopsy: A Step-by-Step Manual

Introduction

Autopsy is a digital forensics platform used for investigating and analyzing computer systems. It allows investigators and students to examine hard drives, memory cards, or images of these devices to identify traces of activity or extract important data. In this manual, we will explore how to use Autopsy to analyze a disk image, focusing on practical application through guided steps and screenshots.

Objective

The purpose of this activity is to familiarize students with the Autopsy digital forensics tool. By the end of this manual, students will be able to:

Download and install Autopsy

Create a new case

Analyze a forensic image

Identify and interpret recovered files

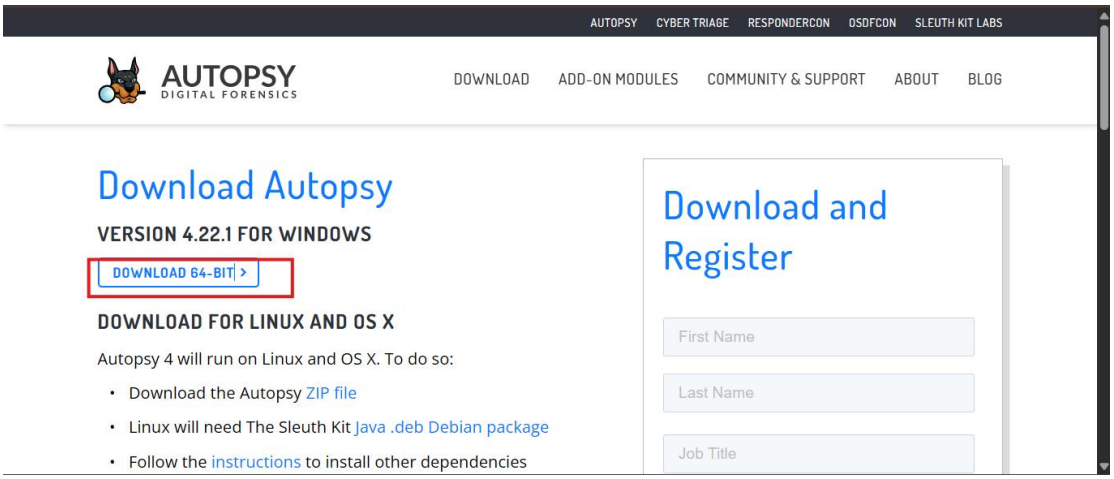
Understand the basics of digital investigation procedures

Step 1: Download Autopsy

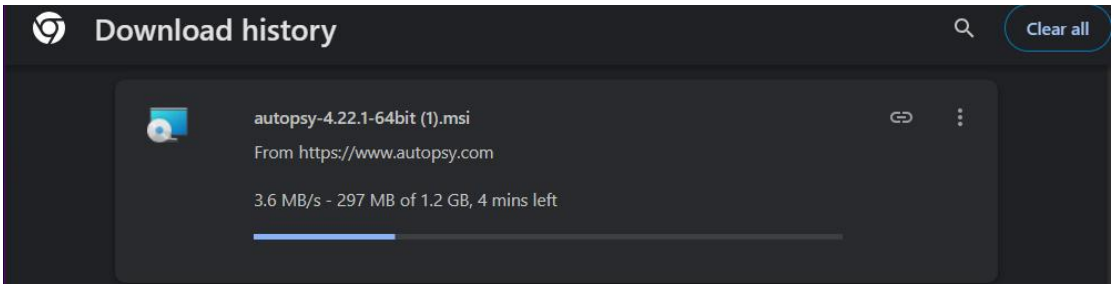
Visit the official website:
https://www.autopsy.com/download/
Download the version suitable for your system and install it.

Step 2: Open Autopsy.

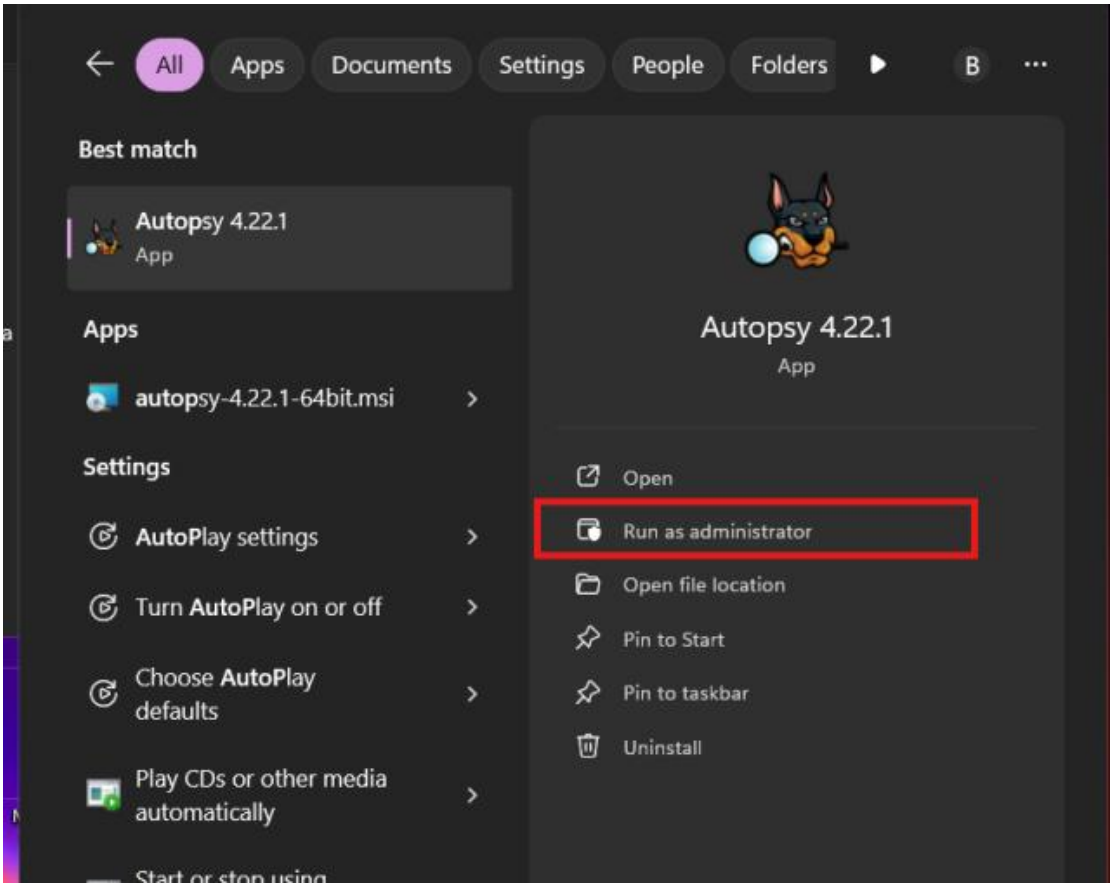
Made by Moeez Javed



Step 3: Downloading Start



Step 4: Run as Administrator

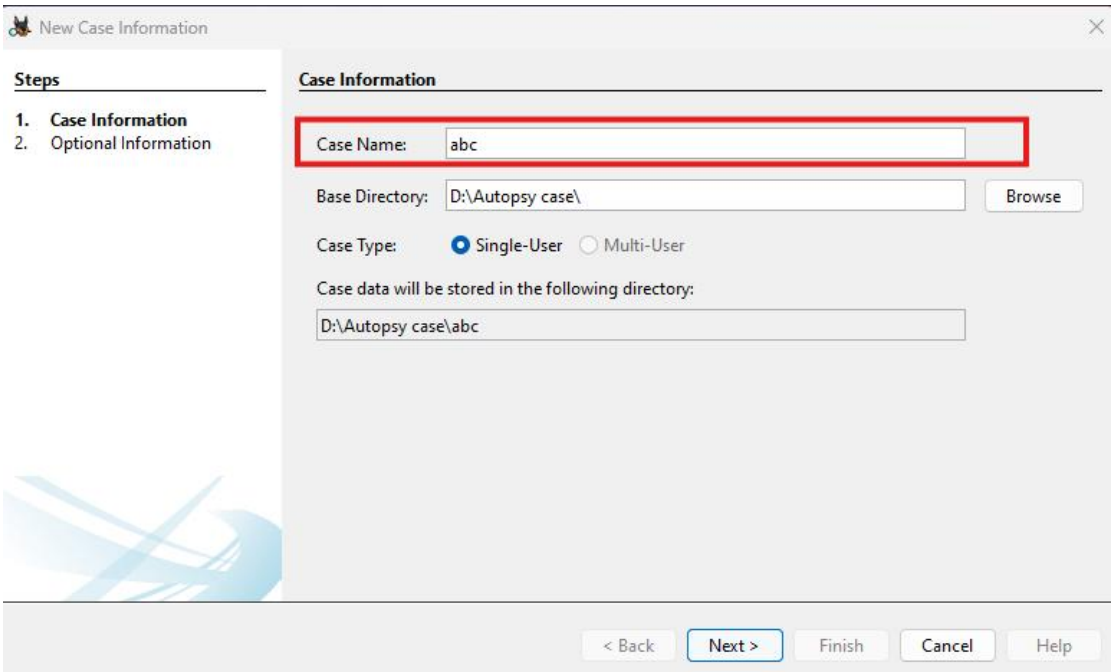


Made by Moeez Javed

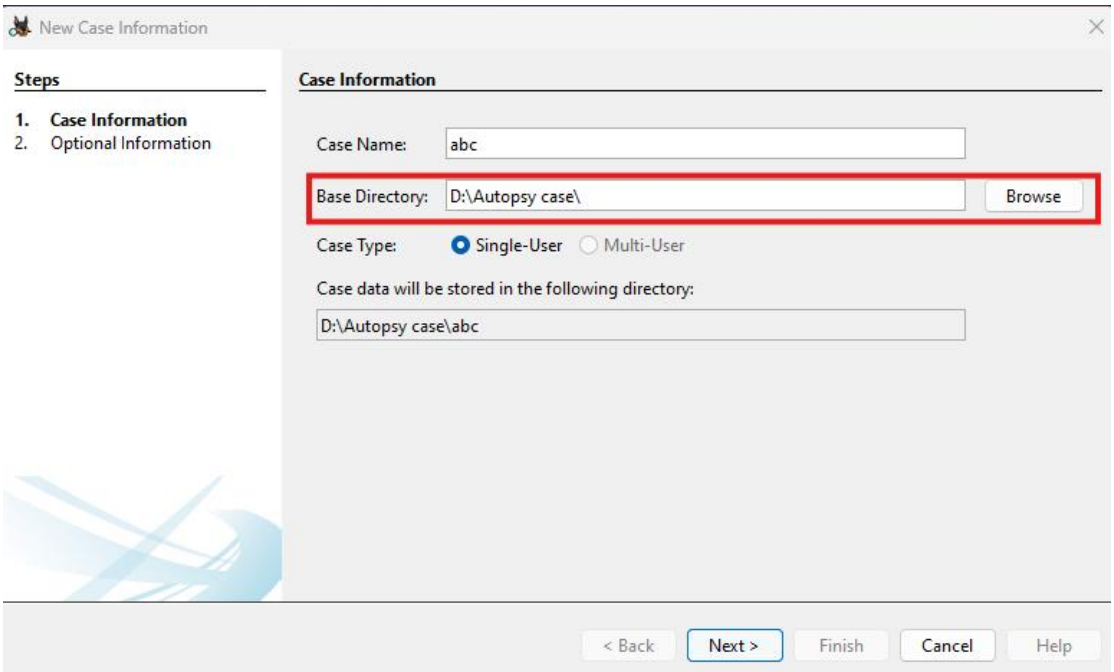
Step 5: Click "Create New Case".

Step 6: Enter a Case Name and optional details (Investigator Name, etc.).

Made by Moeez Javed

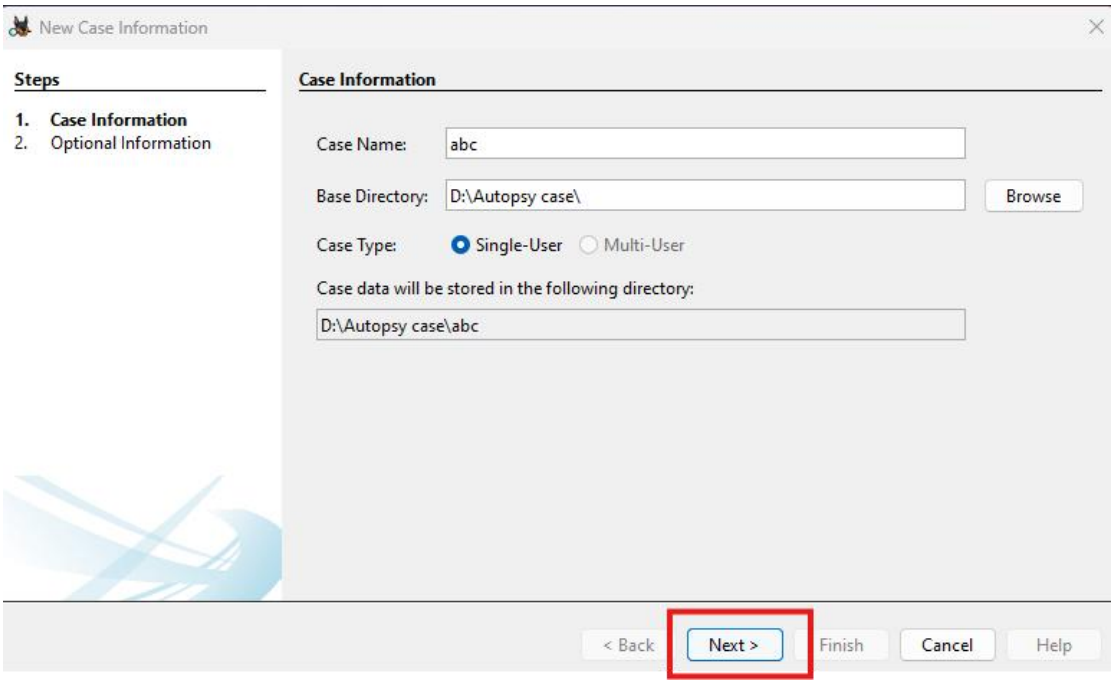


Step 7: Choose the directory where the case files will be stored.

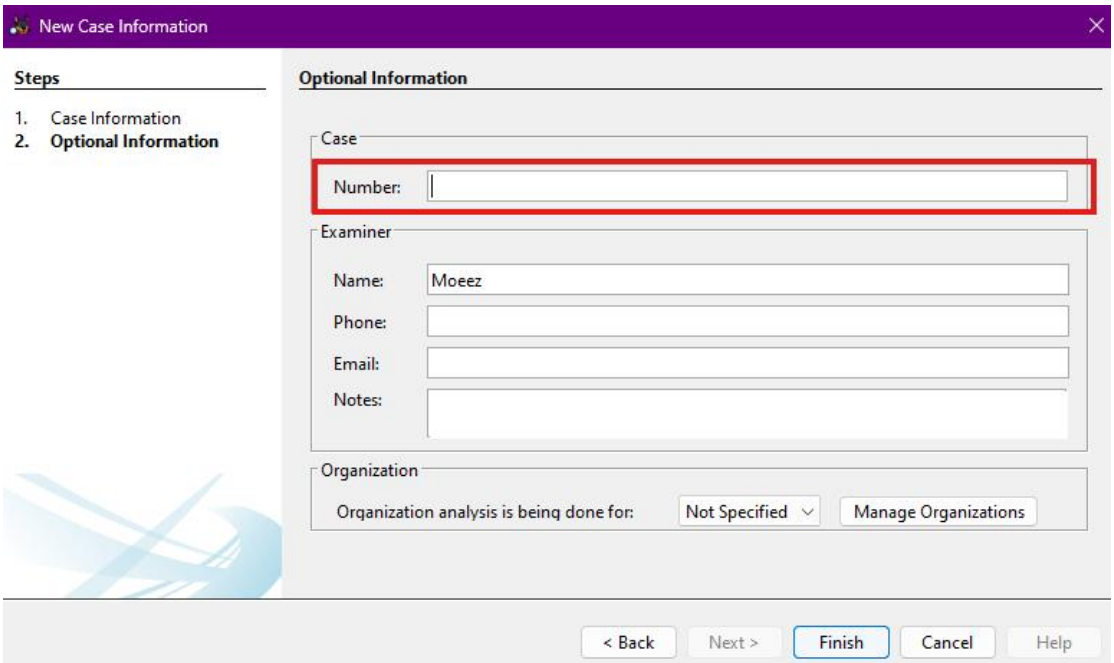


Step 8: Click Next to proceed.

Made by Moeez Javed



Step 9:Add the number and Review the summary and confirm to finish creating the case.



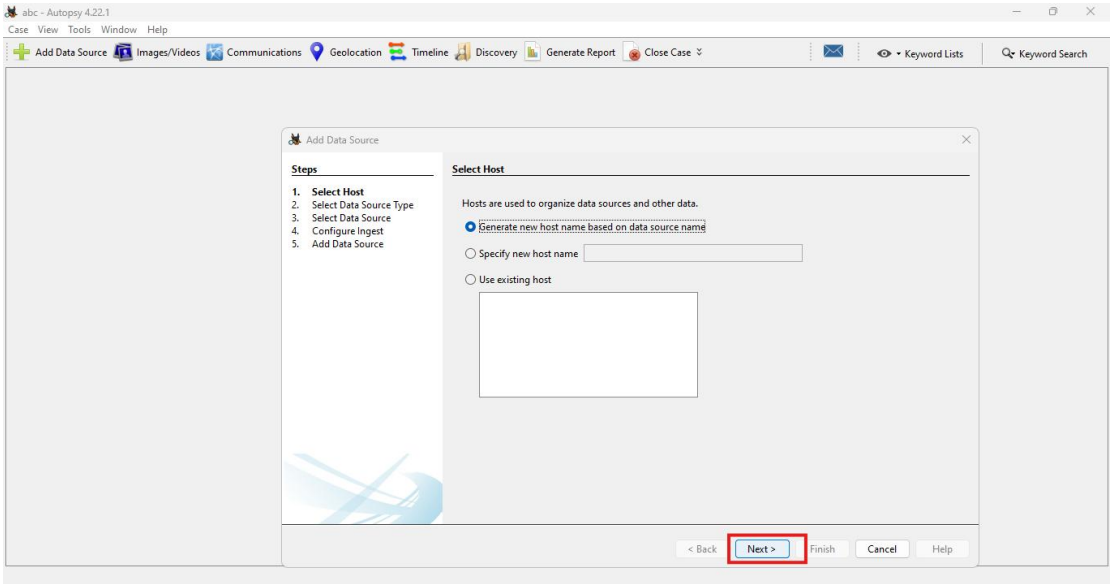
Step 10: Begin Forensics on a Disk

Click **Add Data Source** and choose to analyze a disk image or local disk.

Screenshot shows Autopsy interface with disk forensics options.

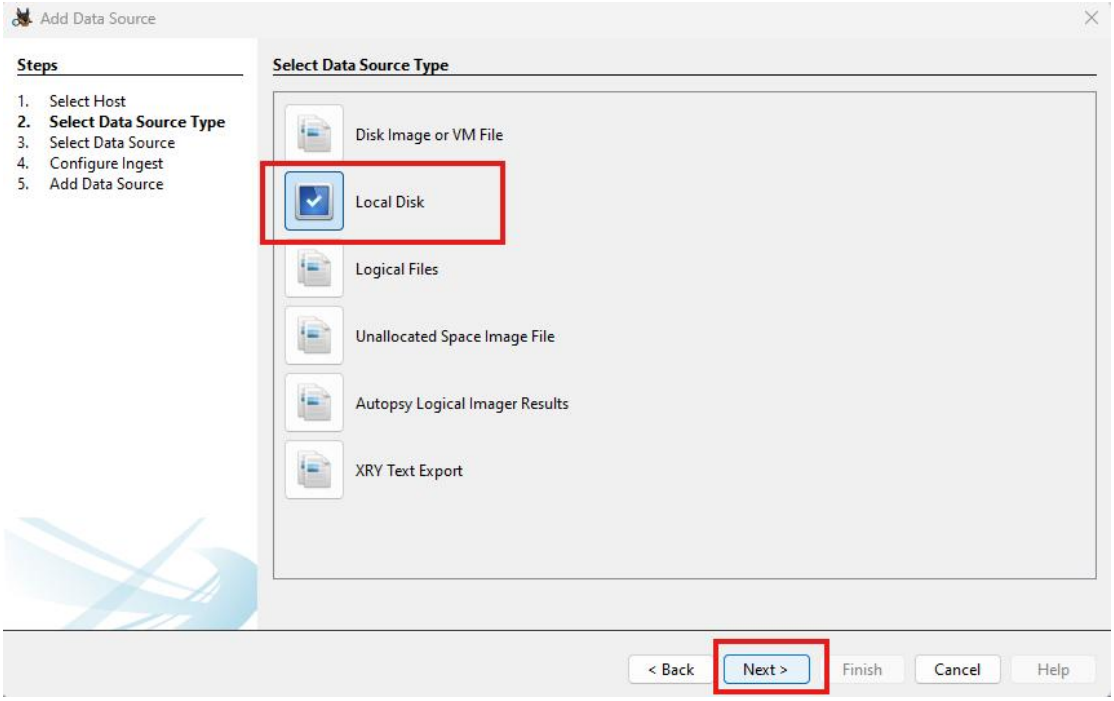
In this step, you begin the actual forensic process on a selected disk.

Made by Moeez Javed



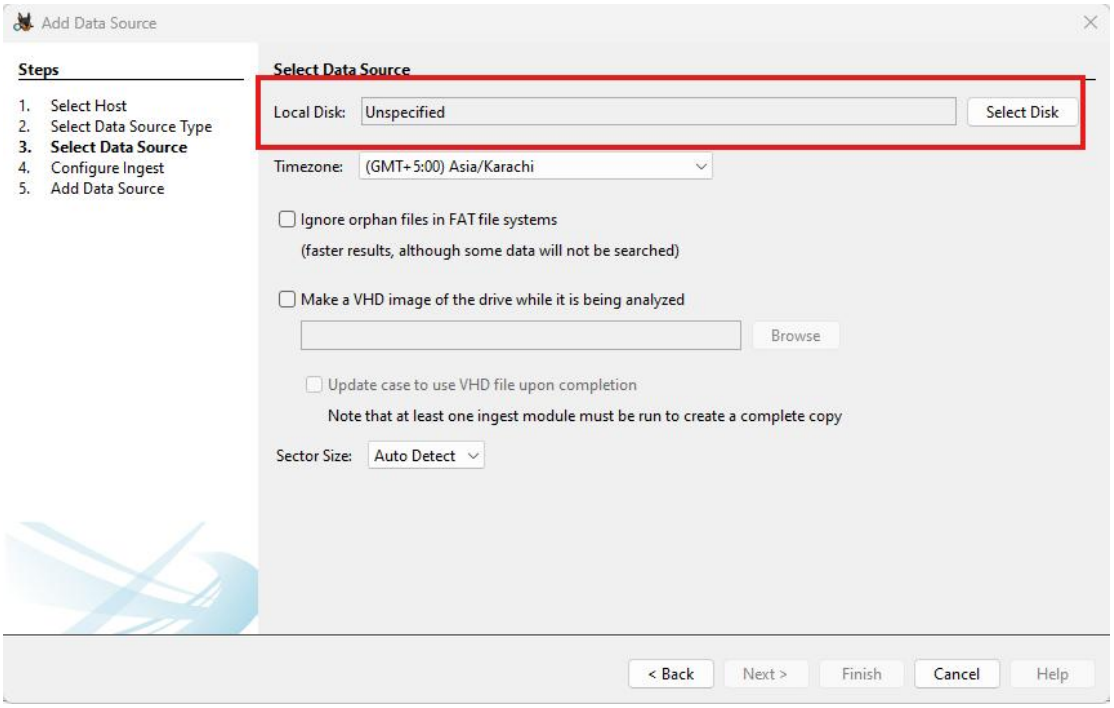
Step 11: Select the Disk

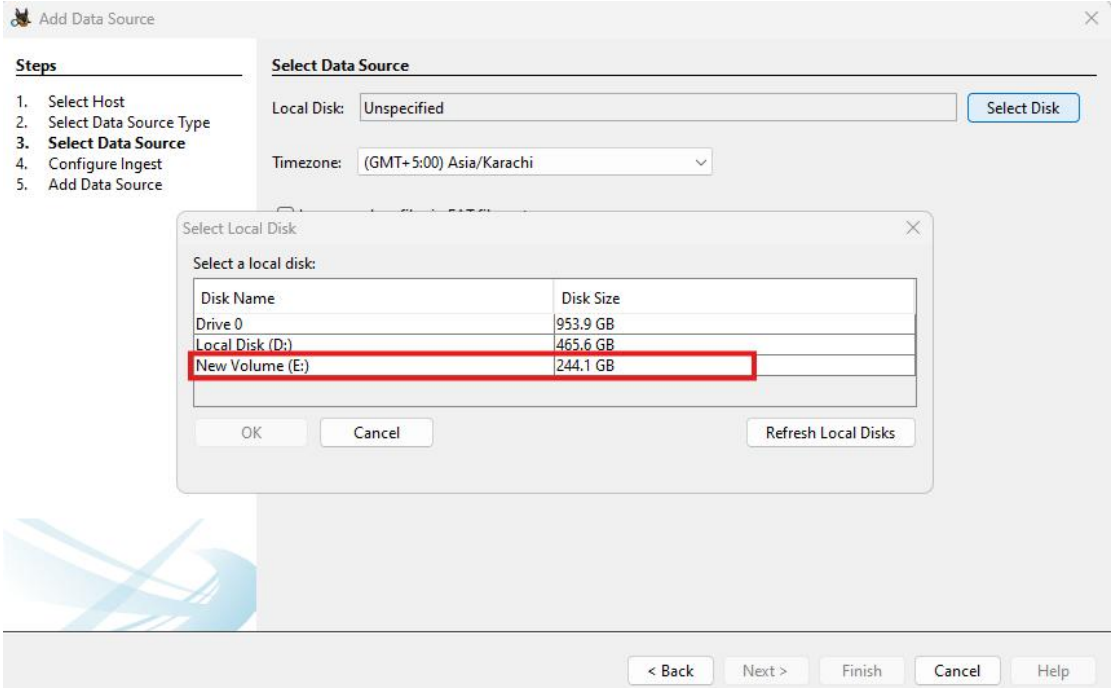
Choose the disk image or logical drive that you wish to analyze. Screenshot highlights disk selection screen.



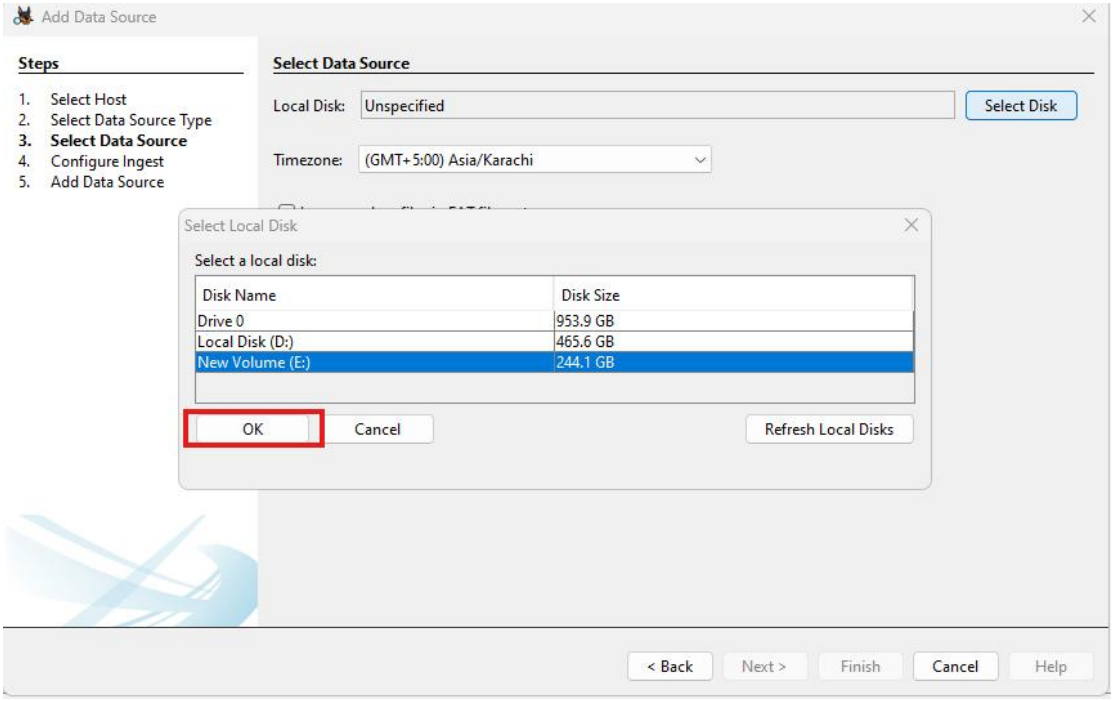
Step12: Select the disk.

Made by Moeez Javed

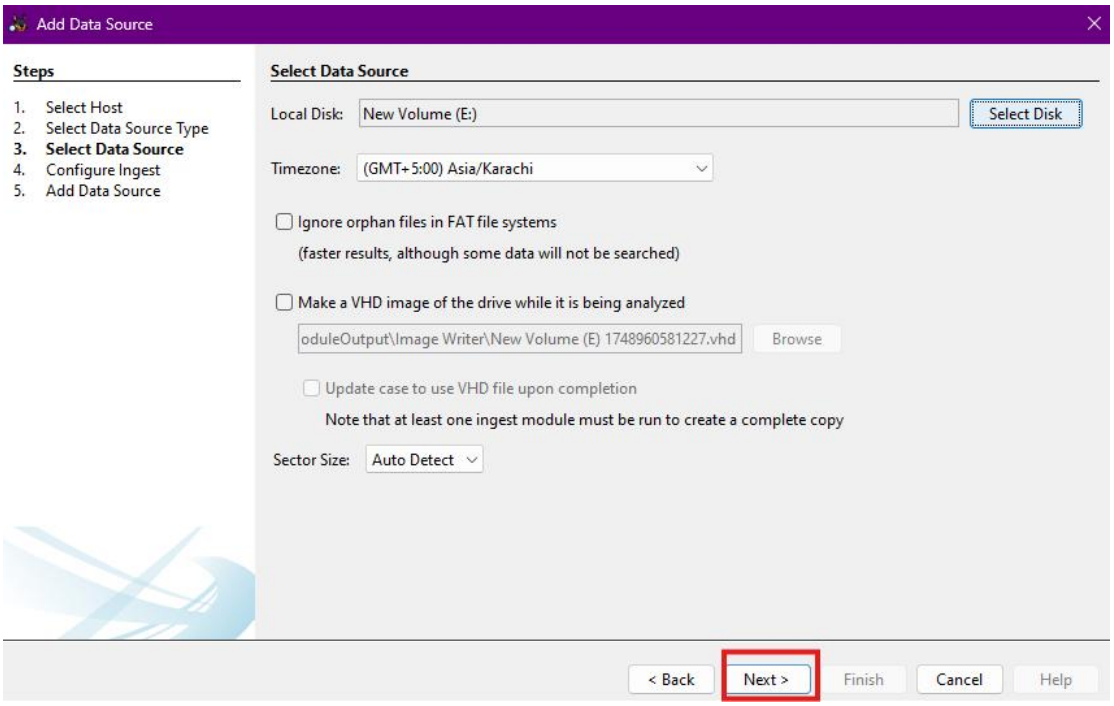




Made by Moeez Javed

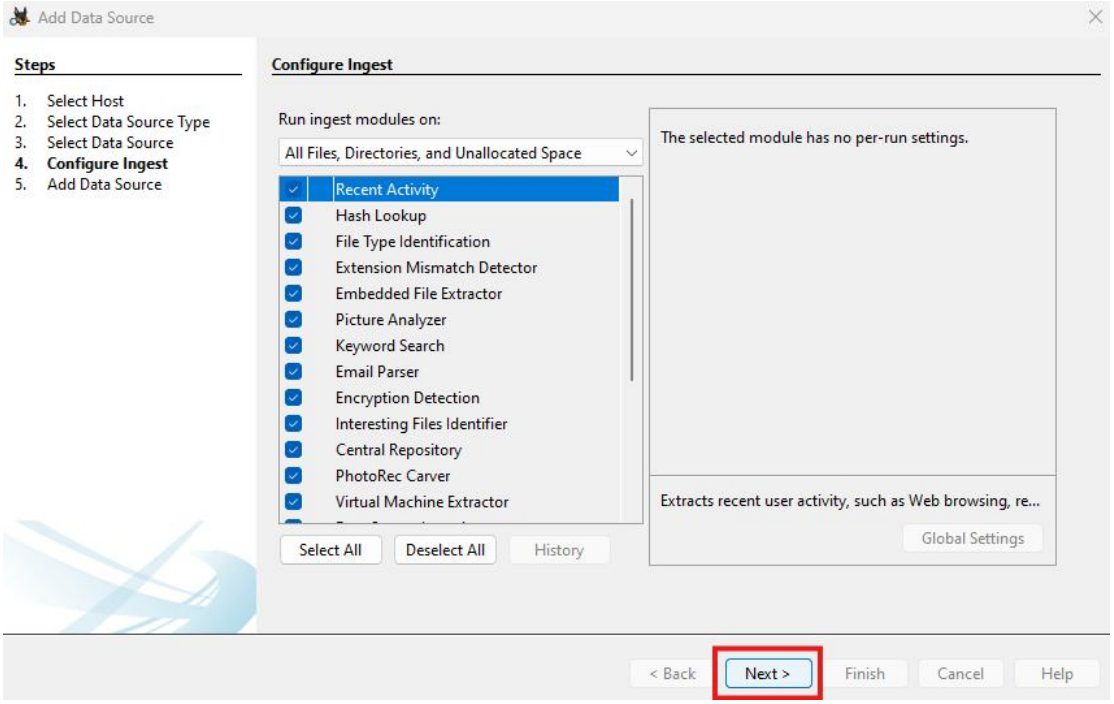


Step 13: Press the next button to proceed

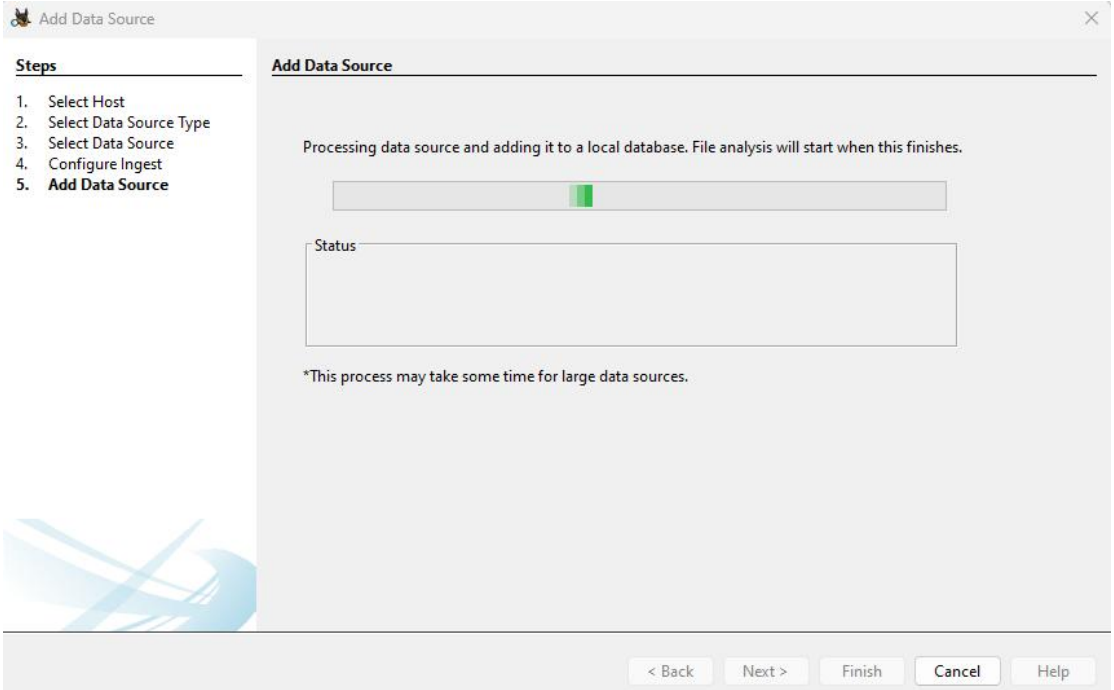


Step 14: Using filters (like file type, hash sets, etc.)

Made by Moeez Javed



Step15: Reviewing detailed file properties and exporting evidence



Walkthrough Task: Digital Forensics Investigation

Scenario:

You are a digital forensics analyst. You've received a suspicious disk image for investigation. Your task is to analyze the image using Autopsy and document any unusual or deleted activity.

Made by Moeez Javed

You will follow the steps in this manual and complete actions marked as Quiz