

Made by Moez Javed



Applied Cyber Security Industry Led-Course

Instructor: Faisal Shahzad

Lab Instructor: Moez Javed

Lab 12: Autopsy (Computer Forensics)

Availability:

Monday to Friday: 9 AM – 5 PM (at CUST)

After 5 PM: Please drop a message instead of calling.

Lab Instructor Contact Details:

Phone: +92 333 8744696

Email: moezjavedyousafrana@gmail.com

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

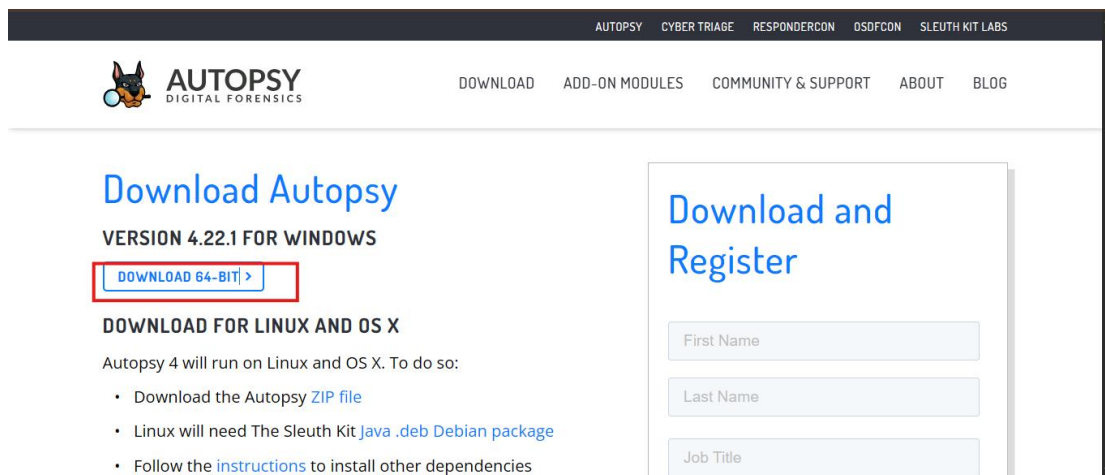
Step 1: Download Autopsy

Visit the official website:

<https://www.autopsy.com/download/>

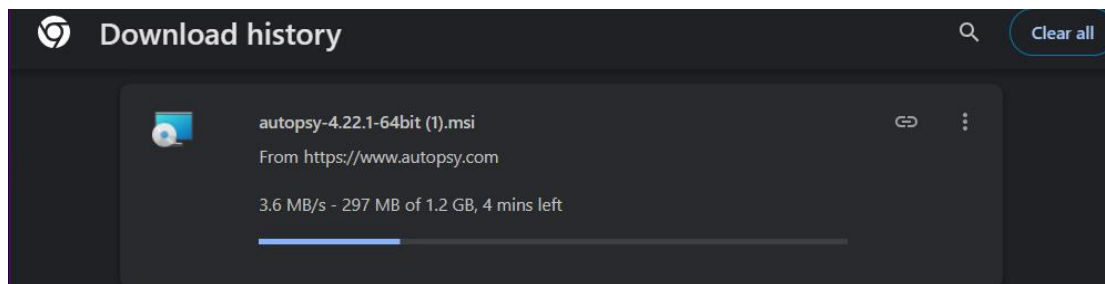
Download the version suitable for your system and install it.

Step 2: Open Autopsy.



The screenshot shows the Autopsy Digital Forensics website. The top navigation bar includes links for AUTOPSY, CYBER TRIAGE, RESPONDERCON, OSDFCON, and SLEUTH KIT LABS. The main header features the Autopsy logo and navigation links: DOWNLOAD, ADD-ON MODULES, COMMUNITY & SUPPORT, ABOUT, and BLOG. The main content area is titled "Download Autopsy" and specifies "VERSION 4.22.1 FOR WINDOWS". A red box highlights the "DOWNLOAD 64-BIT" button. Below this, there is a section for "DOWNLOAD FOR LINUX AND OS X" with instructions and links for ZIP files, Debian packages, and installation instructions. To the right, a "Download and Register" sidebar contains input fields for First Name, Last Name, and Job Title.

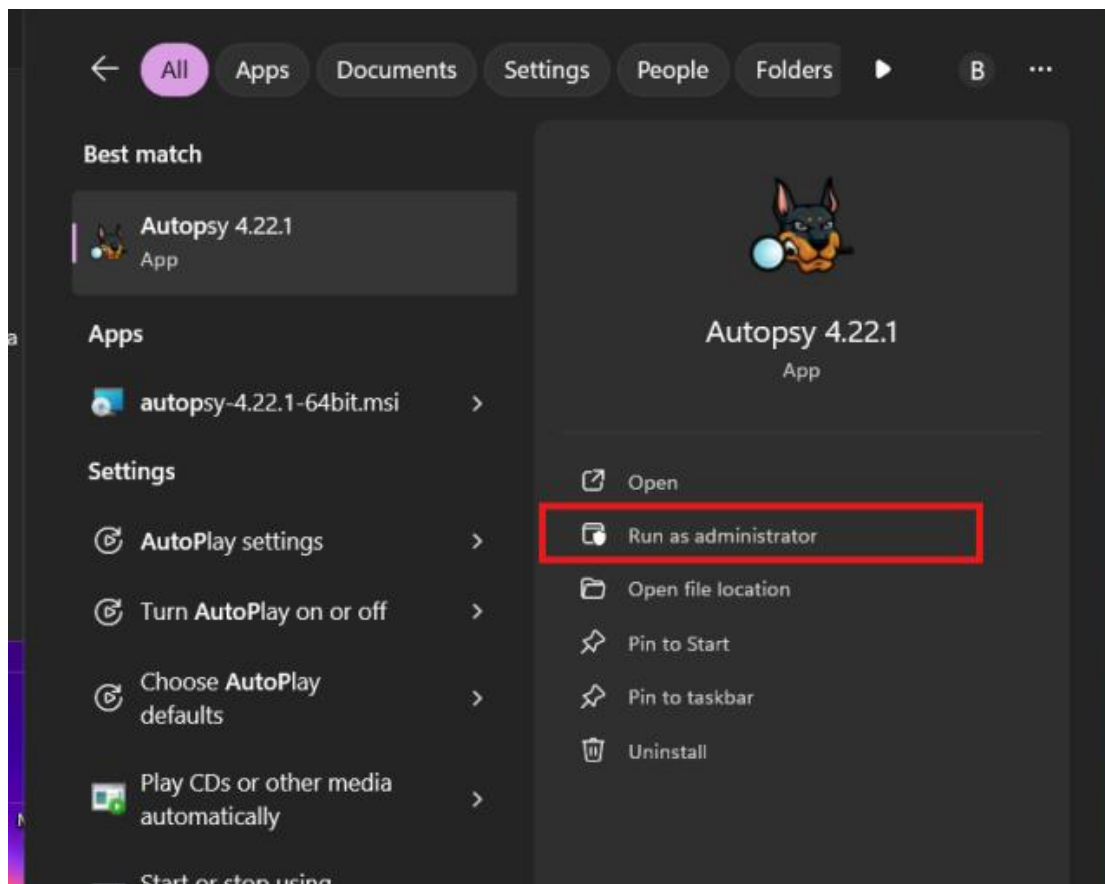
Step 3: Downloading Start



The screenshot shows a "Download history" window. It displays a download entry for "autopsy-4.22.1-64bit (1).msi" from "https://www.autopsy.com". The progress bar indicates that 3.6 MB/s is being downloaded, with 297 MB of 1.2 GB remaining, and 4 minutes left. The window also includes a search icon and a "Clear all" button.

Step 4: Run as Administrator

Made by Moez Javed

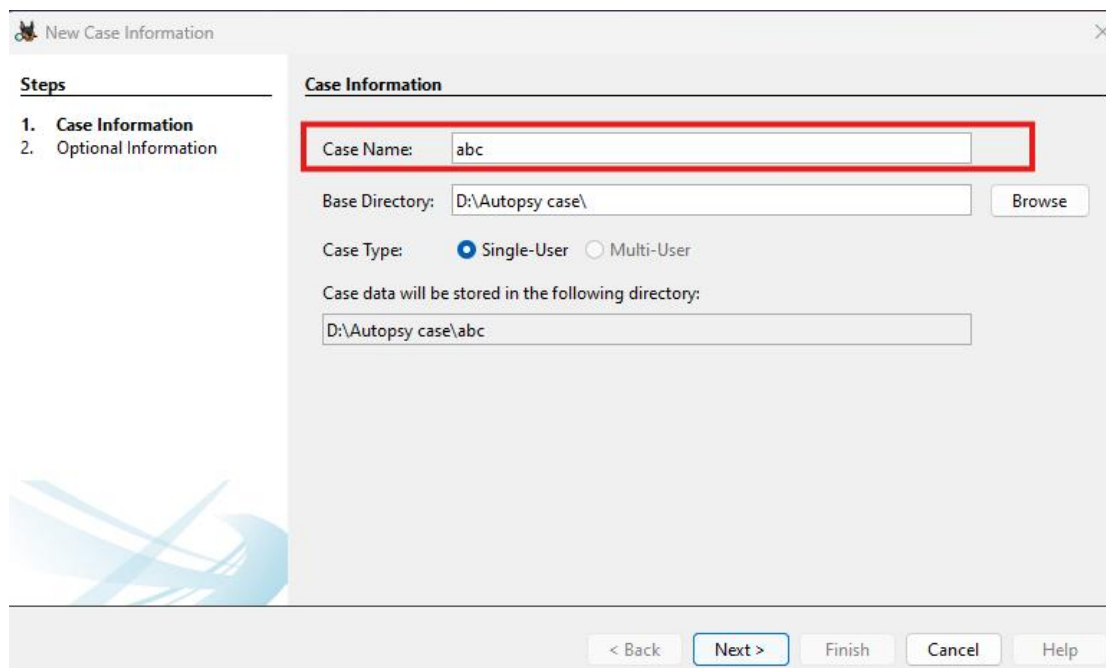


Step 5: Click “Create New Case”.





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



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

New Case Information

Steps

1. Case Information
2. Optional Information

Case Information

Case Name: abc

Base Directory: D:\Autopsy case\ Browse

Case Type: ☒ Single-User ☐ Multi-User

Case data will be stored in the following directory:

D:\Autopsy case\abc

< Back Next > Finish Cancel Help

Step 8: Click Next to proceed.

New Case Information

Steps

1. Case Information
2. Optional Information

Case Information

Case Name: abc

Base Directory: D:\Autopsy case\ Browse

Case Type: ☒ Single-User ☐ Multi-User

Case data will be stored in the following directory:

D:\Autopsy case\abc

< Back Next > Finish Cancel Help

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

New Case Information

Steps

1. Case Information
2. Optional Information

Optional Information

Case

Number:

Examiner

Name:

Phone:

Email:

Notes:

Organization

Organization analysis is being done for: [Manage Organizations](#)

< Back Next > Finish Cancel Help

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.

abc - Autopsy 4.22.1

Case View Tools Window Help

+ Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

Keyword Lists Keyword Search

Add Data Source

Steps

1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source

Select Host

Hosts are used to organize data sources and other data.

☒ Generate new host name based on data source name

☐ Specify new host name

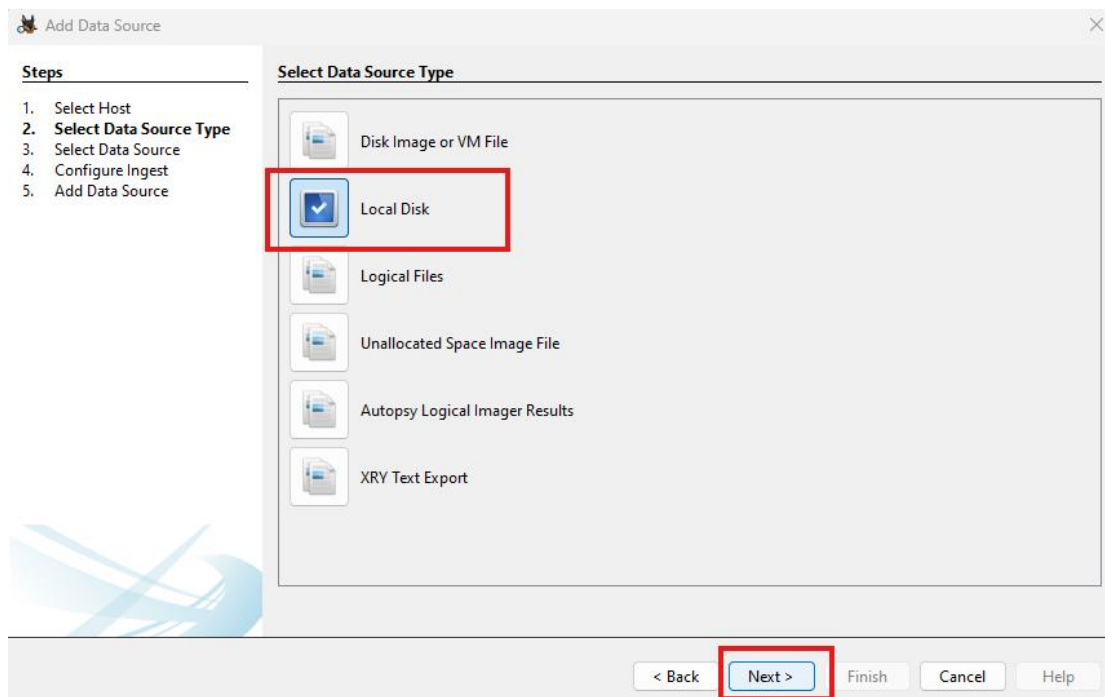
☐ Use existing host

< Back Next > Finish Cancel Help

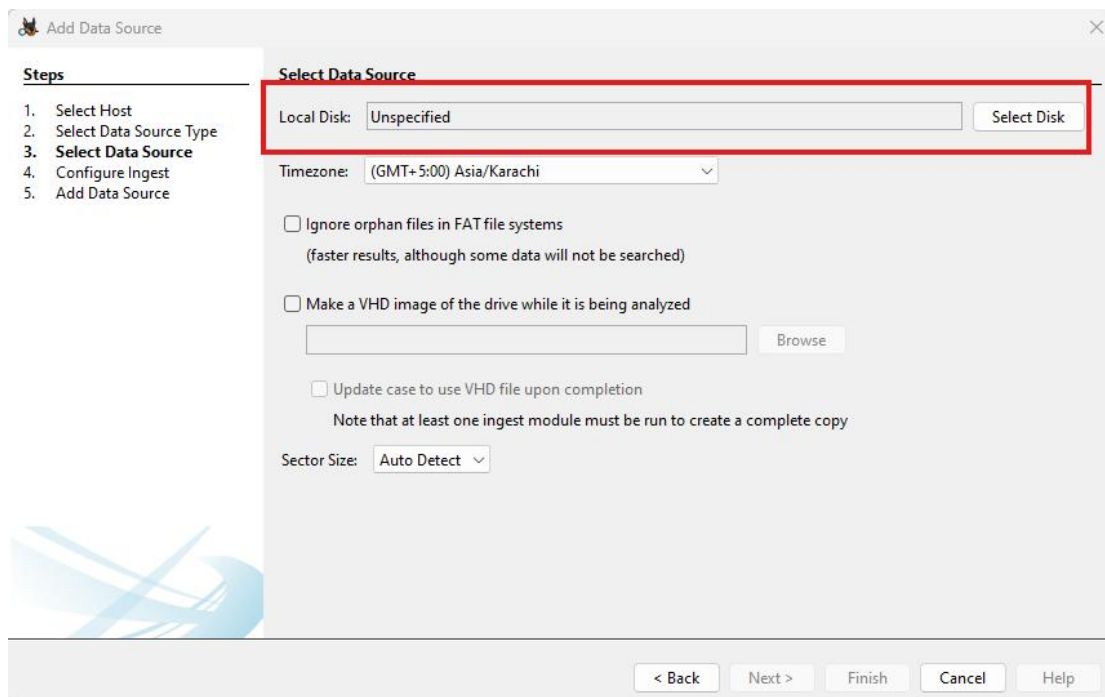
Step 11: Select the Disk

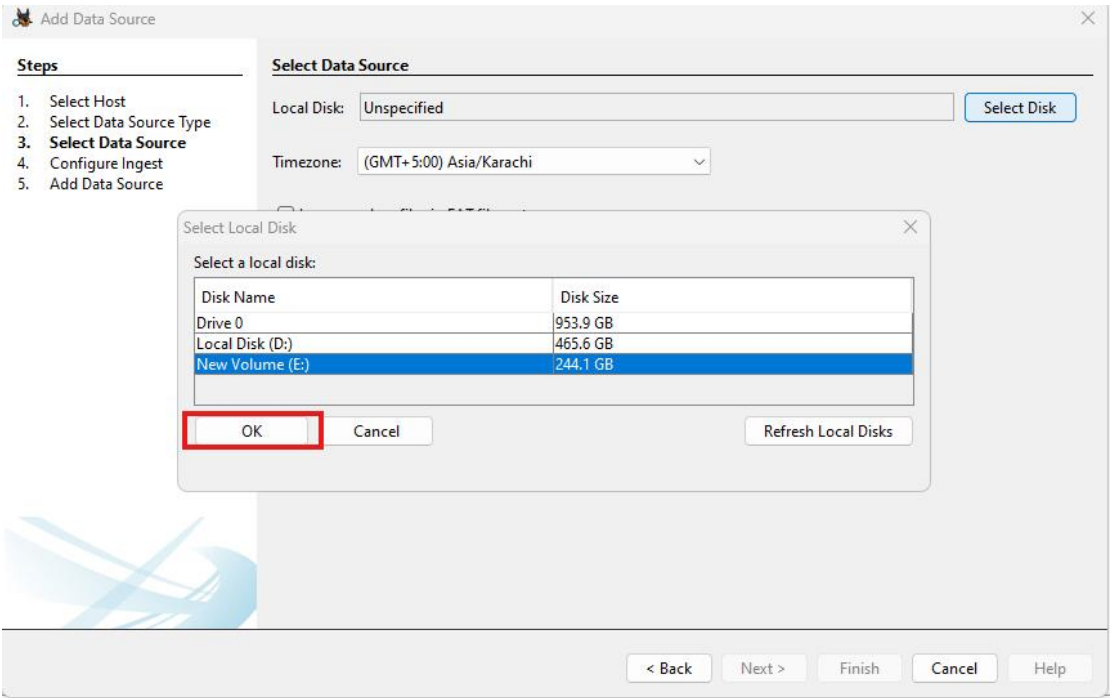
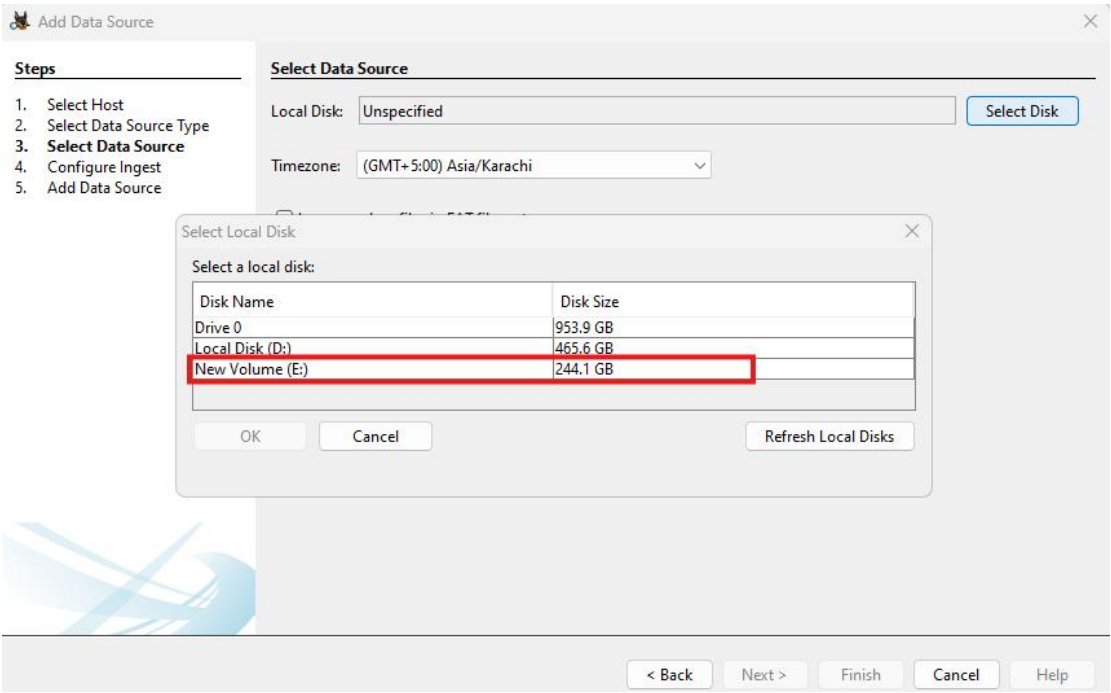
Made by Moez Javed

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



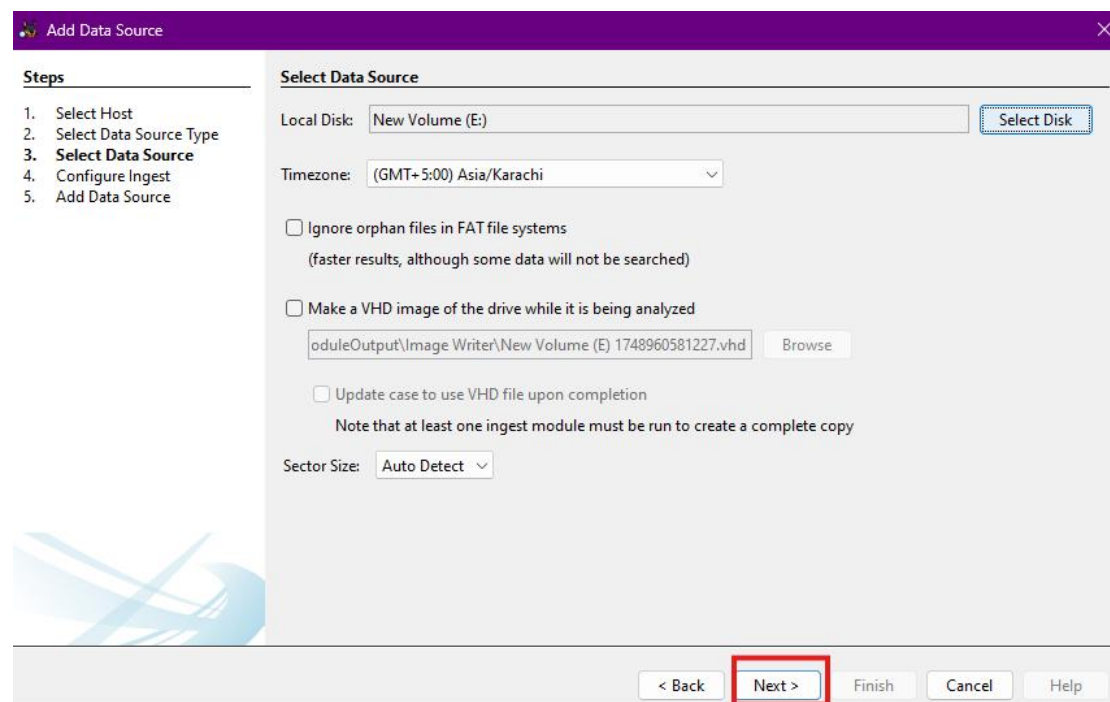
Step12: Select the disk.



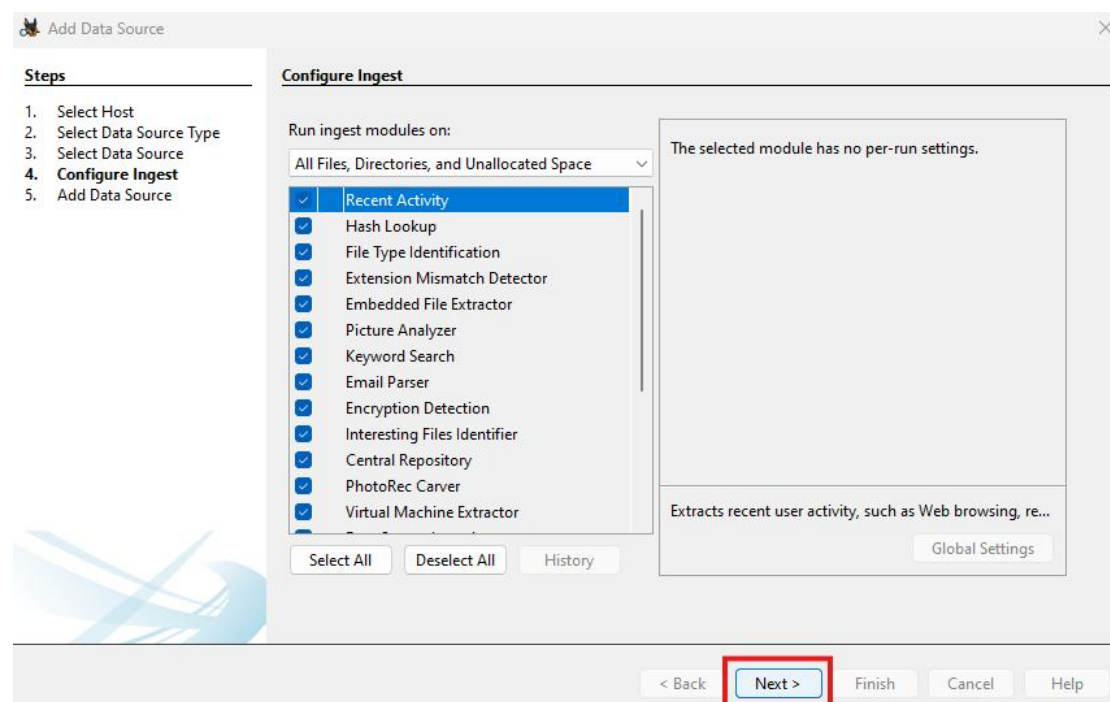


Step 13: Press the next button to proceed

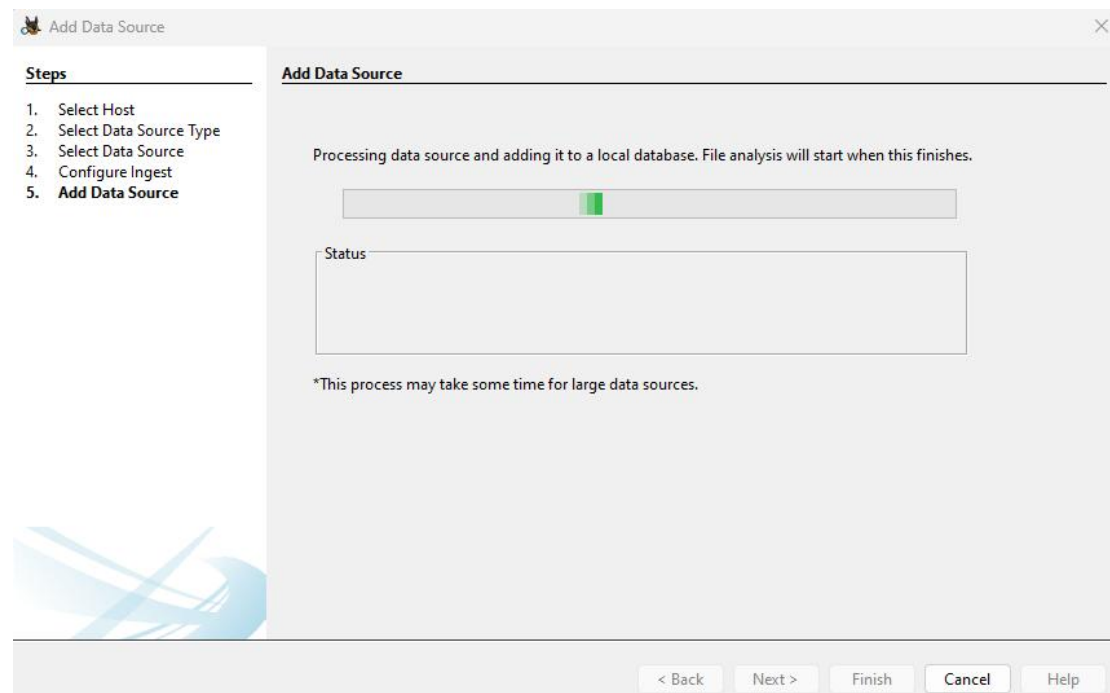
Made by Moez Javed



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



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.

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