

Made by Moez Javed

AUTOPSY TOOL MANUAL



Made by
Moez 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

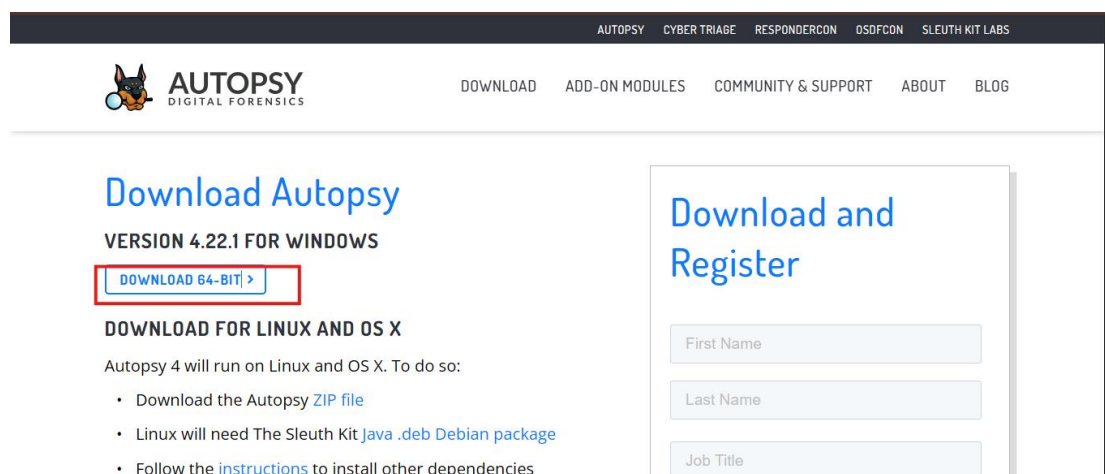
Step 1: Download Autopsy

Visit the official website:

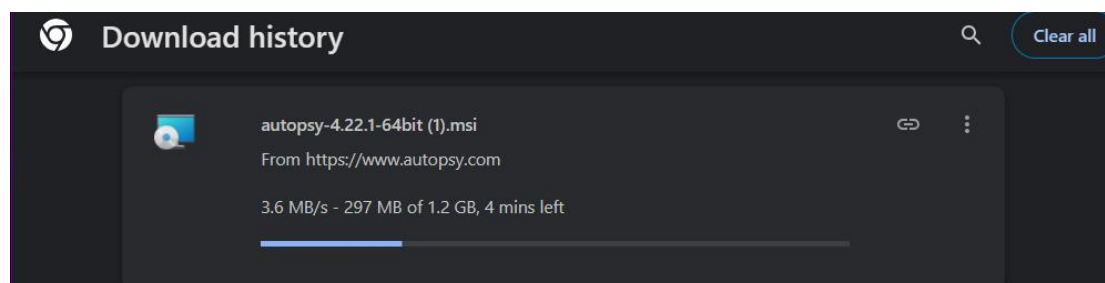
<https://www.autopsy.com/download/>

Download the version suitable for your system and install it.

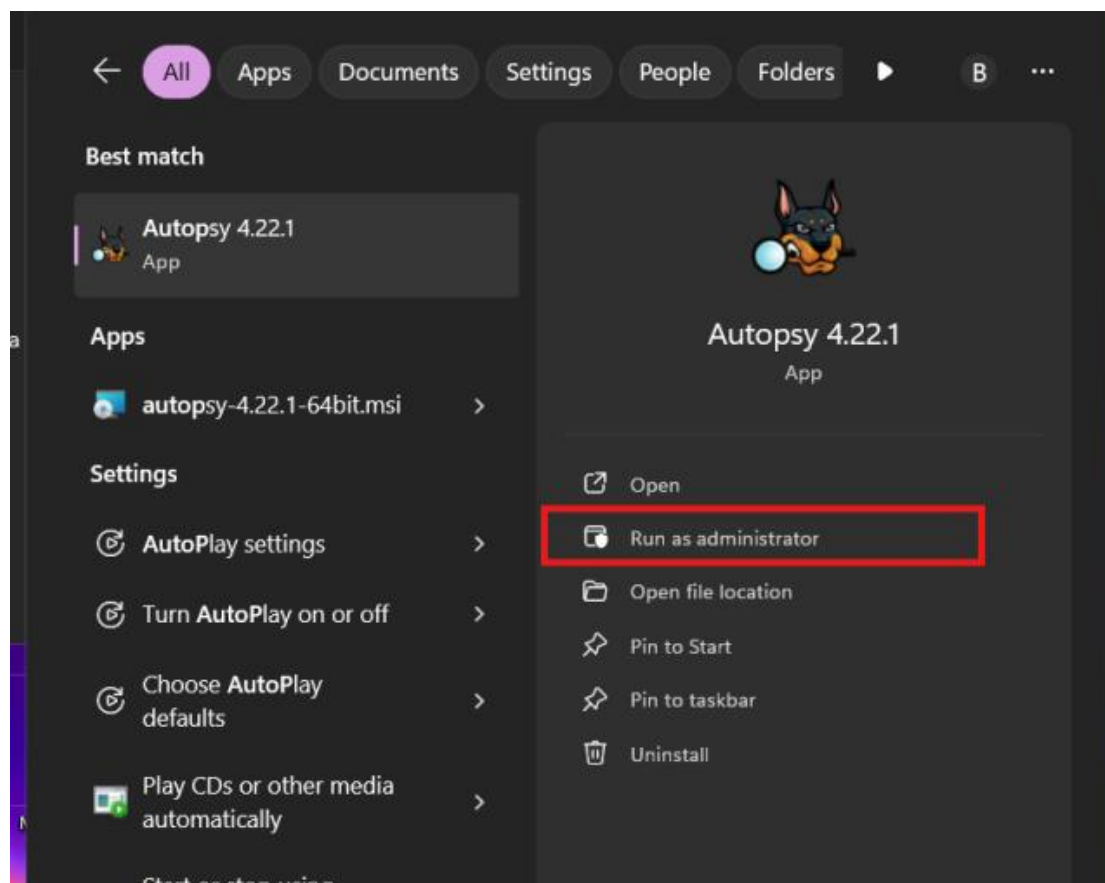
Step 2: Open Autopsy.



Step 3: Downloading Start



Step 4: Run as Administrator

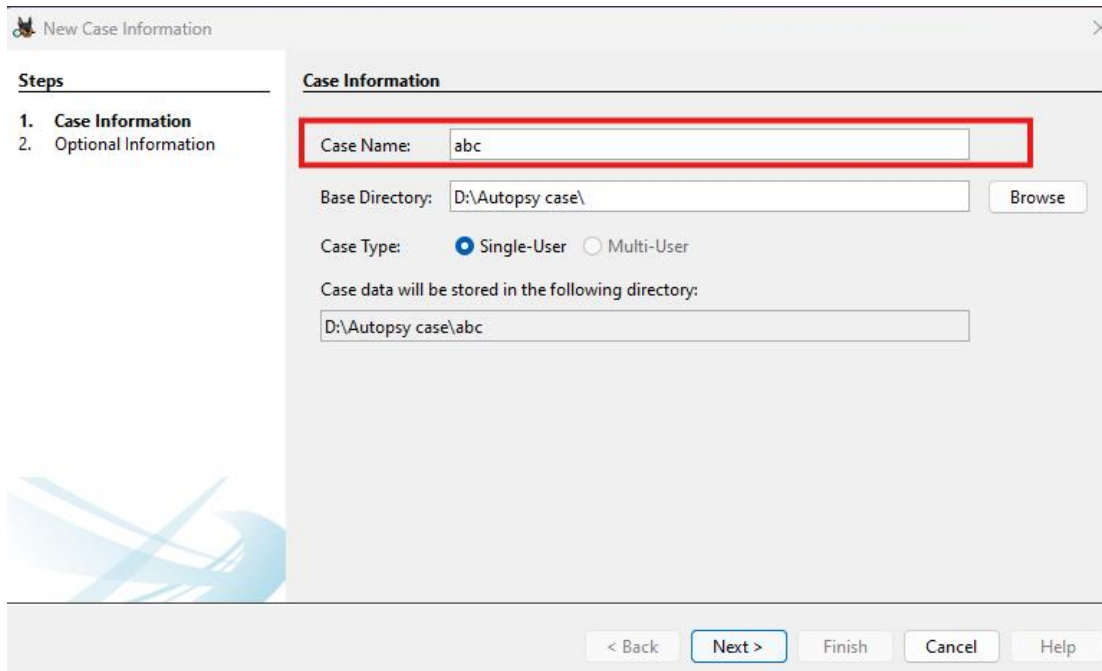


Made by Moez Javed

Step 5: Click “Create New Case”.



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



New Case Information

Steps

1. Case Information
2. Optional Information

Case Information

Case Name:

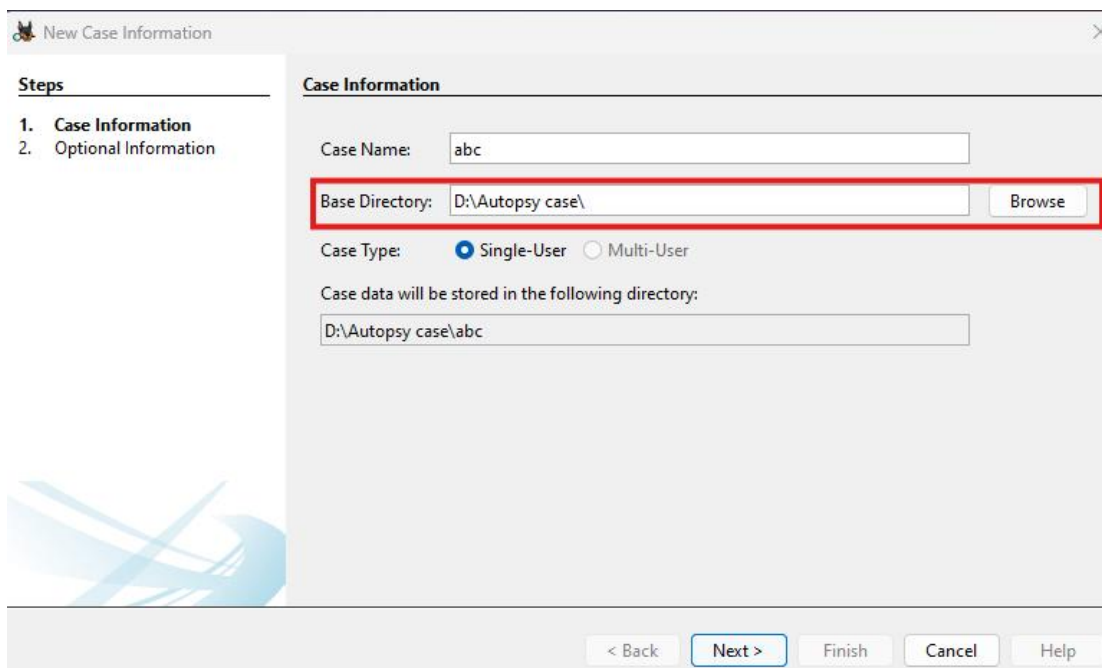
Base Directory:

Case Type: ☒ Single-User ☐ Multi-User

Case data will be stored in the following directory:

< Back **Next >** Finish Cancel Help

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:

Base Directory:

Case Type: ☒ Single-User ☐ Multi-User

Case data will be stored in the following directory:

< Back **Next >** Finish Cancel Help

Step 8: Click Next to proceed.

The screenshot shows the 'New Case Information' dialog box with the 'Case Information' tab selected. The 'Steps' panel on the left lists '1. Case Information' and '2. Optional Information'. The main area contains the following fields:

- Case Name:** A text box containing 'abc'.
- Base Directory:** A text box containing 'D:\Autopsy case\' with a 'Browse' button to its right.
- Case Type:** Two radio buttons: 'Single-User' (selected) and 'Multi-User'.
- Case data will be stored in the following directory:** A text box containing 'D:\Autopsy case\abc'.

At the bottom, there is a navigation bar with buttons: '< Back', 'Next >' (highlighted with a red rectangle), 'Finish', 'Cancel', and 'Help'.

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

The screenshot shows the 'New Case Information' dialog box with the 'Optional Information' tab selected. The 'Steps' panel on the left lists '1. Case Information' and '2. Optional Information'. The main area contains the following sections:

- Case:** A section with a 'Number:' label and an empty text box (highlighted with a red rectangle).
- Examiner:** A section with fields for 'Name:' (containing 'Moez'), 'Phone:', 'Email:', and 'Notes:'.
- Organization:** A section with a label 'Organization analysis is being done for:' followed by a dropdown menu showing 'Not Specified' and a 'Manage Organizations' button.

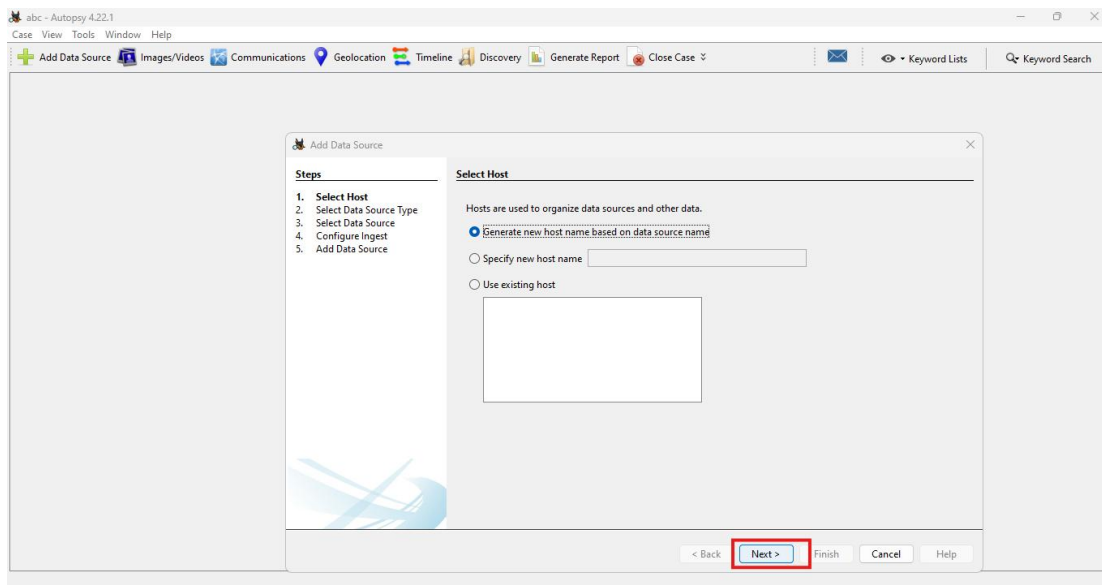
At the bottom, there is a navigation bar with buttons: '< Back', 'Next >', 'Finish' (highlighted with a blue border), 'Cancel', and 'Help'.

Step 10: Begin Forensics on a Disk

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

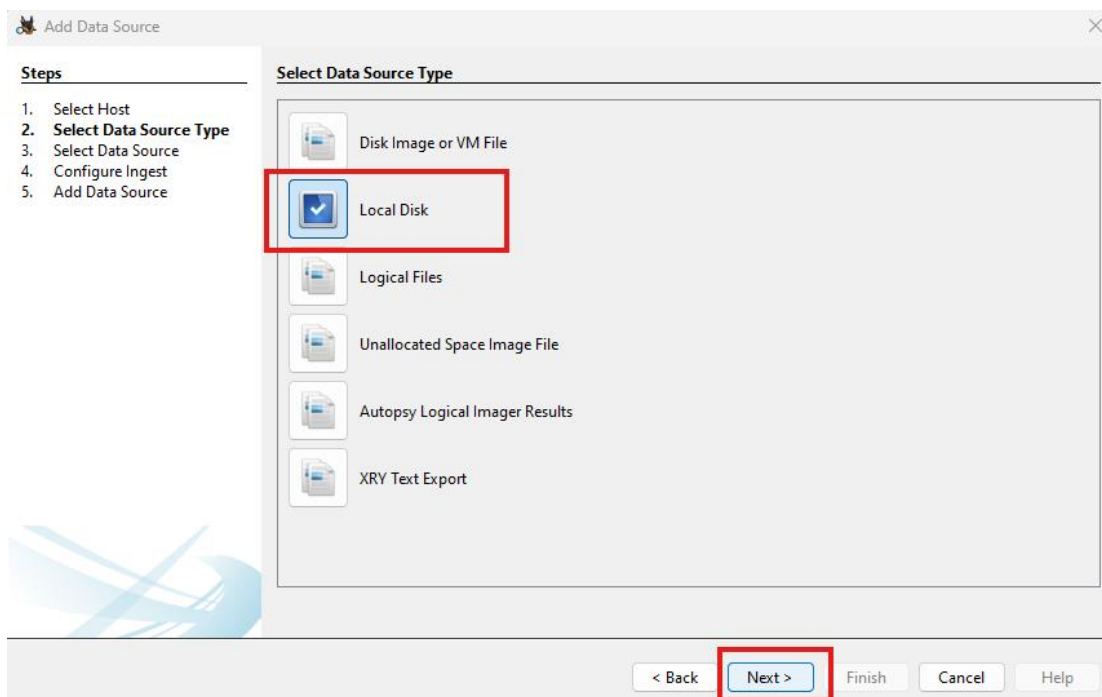
Screenshot shows Autopsy interface with disk forensics options.

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



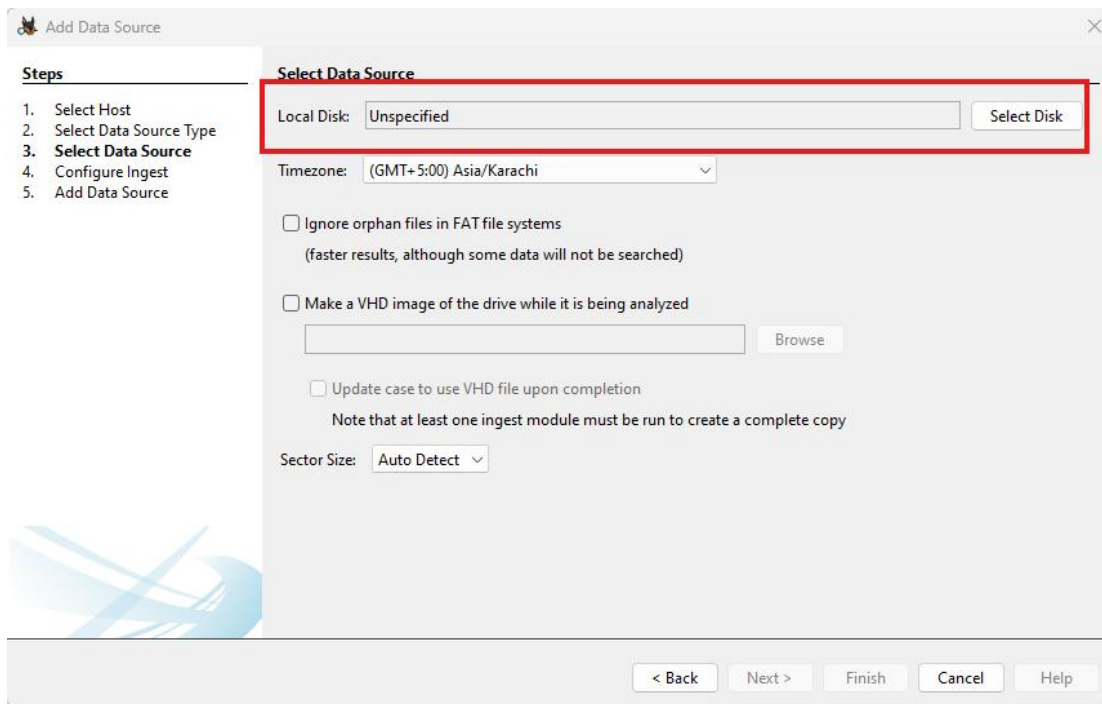
Step 11: Select the Disk

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



Step12: Select the disk.

Made by Moez Javed



The 'Add Data Source' dialog box is shown. The 'Steps' pane on the left lists five steps: 1. Select Host, 2. Select Data Source Type, 3. Select Data Source, 4. Configure Ingest, and 5. Add Data Source. Step 3 is currently selected. The 'Select Data Source' section contains a 'Local Disk' dropdown menu with 'Unspecified' selected, a 'Select Disk' button, a 'Timezone' dropdown menu with '(GMT+ 5:00) Asia/Karachi' selected, and three checkboxes: 'Ignore orphan files in FAT file systems' (unchecked), 'Make a VHD image of the drive while it is being analyzed' (unchecked), and 'Update case to use VHD file upon completion' (unchecked). A 'Browse' button is next to the 'Make a VHD image' checkbox. A note states: 'Note that at least one ingest module must be run to create a complete copy'. The 'Sector Size' dropdown menu is set to 'Auto Detect'. At the bottom are buttons for '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'.

Add Data Source

Steps

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

Select Data Source

Local Disk: Unspecified **Select Disk**

Timezone: (GMT+ 5:00) Asia/Karachi

☐ Ignore orphan files in FAT file systems
(faster results, although some data will not be searched)

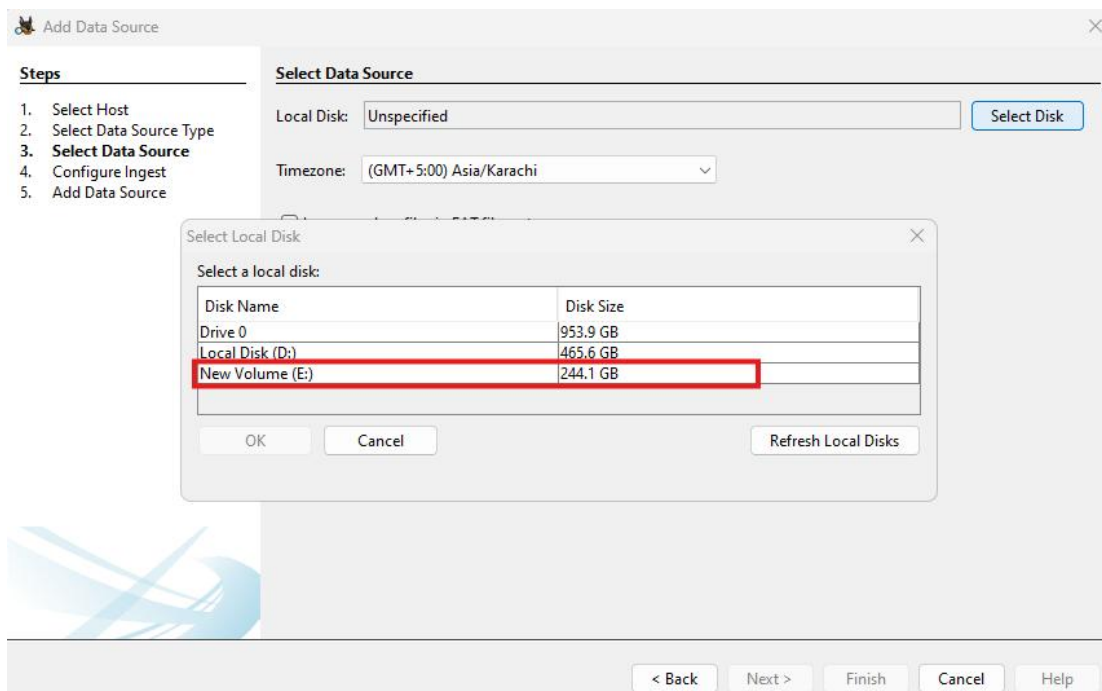
☐ Make a VHD image of the drive while it is being analyzed

☐ Update case to use VHD file upon completion

Note that at least one ingest module must be run to create a complete copy

Sector Size: Auto Detect

< Back Next > Finish Cancel Help



The 'Add Data Source' dialog box is shown with the 'Select Local Disk' sub-dialog box open. The 'Select Local Disk' dialog box has a table with two columns: 'Disk Name' and 'Disk Size'. The table lists four disks: 'Drive 0' (953.9 GB), 'Local Disk (D:)' (465.6 GB), and 'New Volume (E:)' (244.1 GB). The 'New Volume (E:)' row is highlighted with a red border. Below the table are 'OK', 'Cancel', and 'Refresh Local Disks' buttons. The 'Add Data Source' dialog box is in the background, showing the 'Select Data Source' section with the 'Local Disk' dropdown set to 'Unspecified' and the 'Select Disk' button highlighted in blue. The 'Steps' pane on the left shows step 3 'Select Data Source' is selected. The 'Timezone' dropdown is set to '(GMT+ 5:00) Asia/Karachi'. The 'Sector Size' dropdown is set to 'Auto Detect'. At the bottom are buttons for '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'.

Add Data Source

Steps

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

Select Data Source

Local Disk: Unspecified **Select Disk**

Timezone: (GMT+ 5:00) Asia/Karachi

☐ Ignore orphan files in FAT file systems
(faster results, although some data will not be searched)

☐ Make a VHD image of the drive while it is being analyzed

☐ Update case to use VHD file upon completion

Note that at least one ingest module must be run to create a complete copy

Sector Size: Auto Detect

< Back Next > Finish Cancel Help

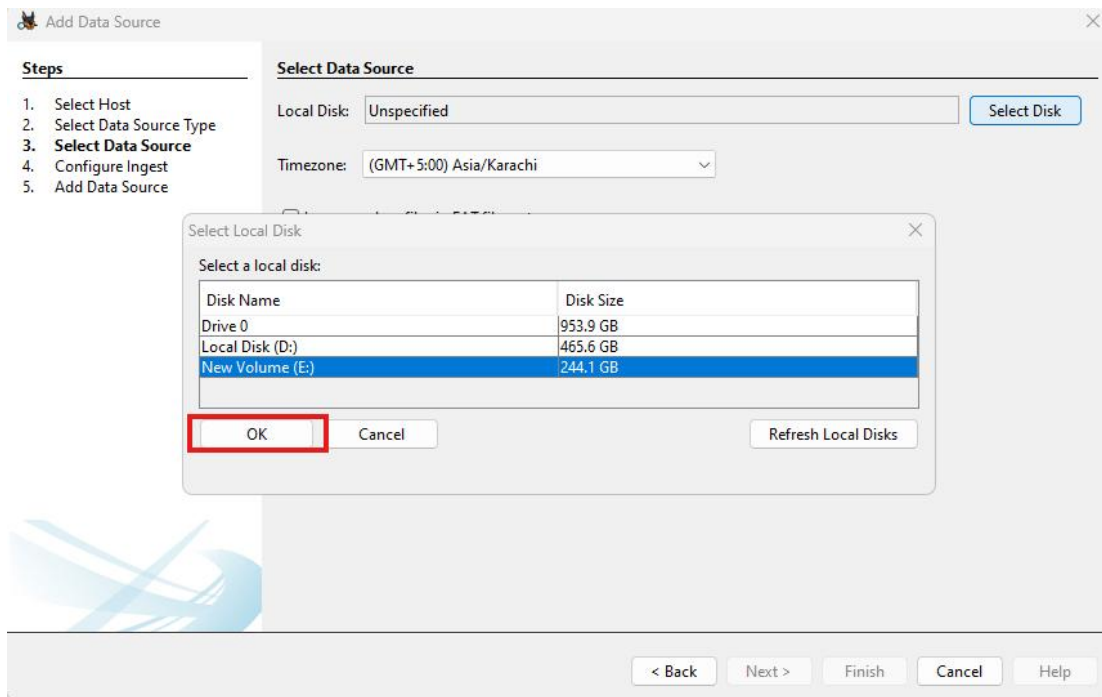
Select Local Disk

Select a local disk:

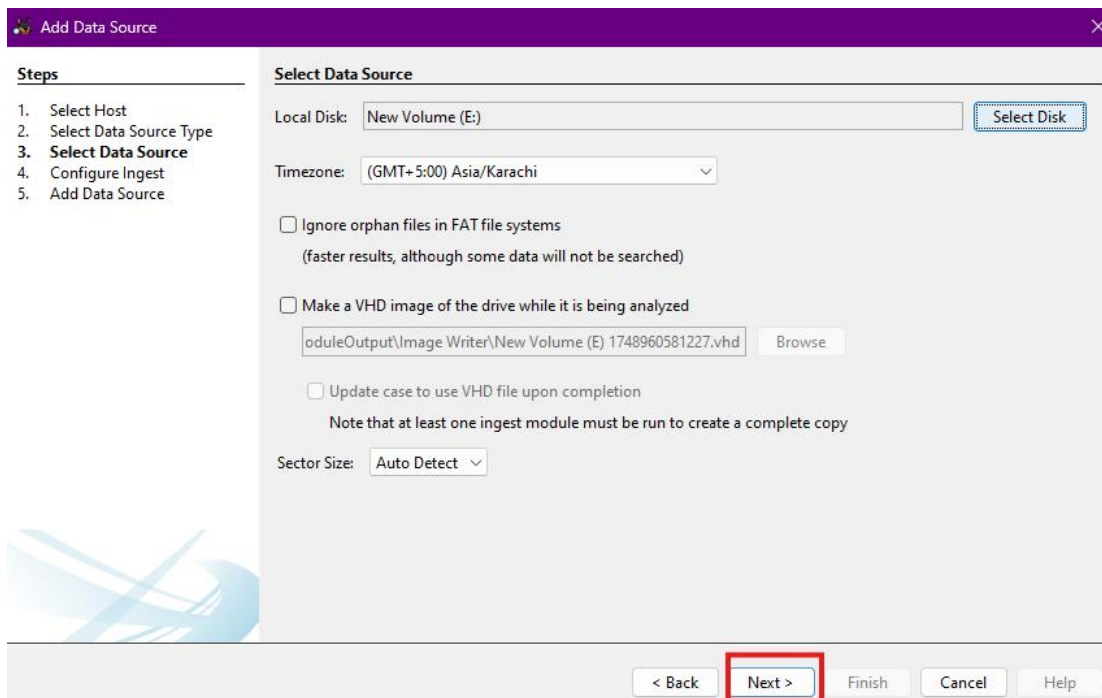
Disk Name	Disk Size
Drive 0	953.9 GB
Local Disk (D:)	465.6 GB
New Volume (E:)	244.1 GB

OK Cancel Refresh Local Disks

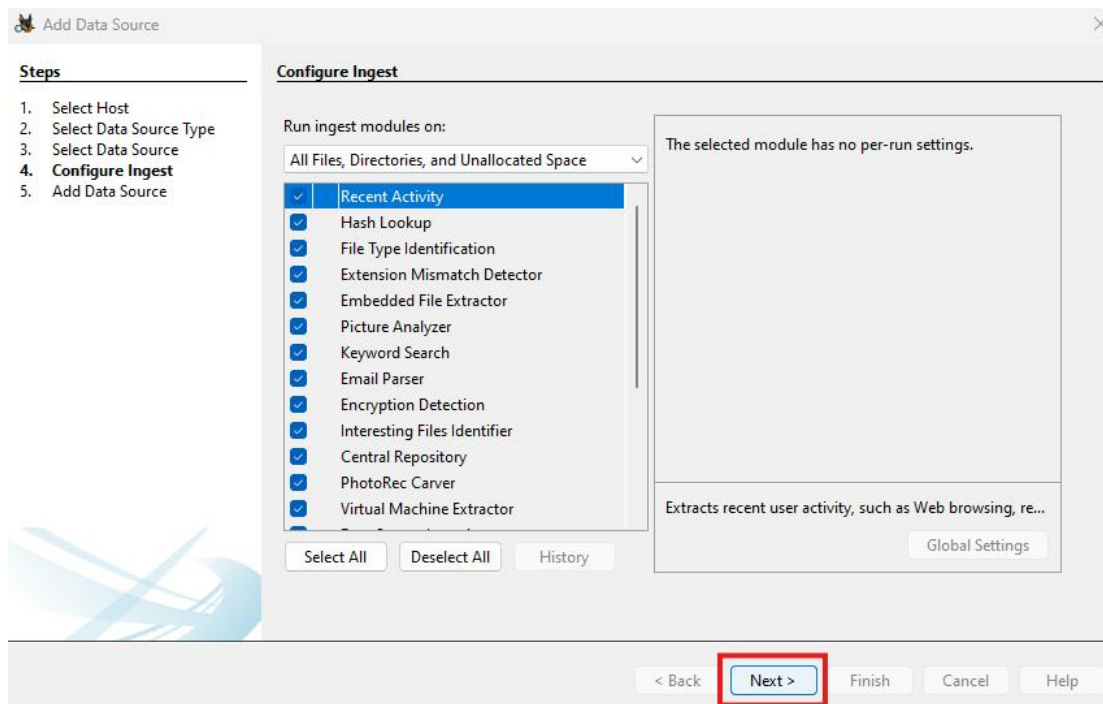
Made by Moez Javed



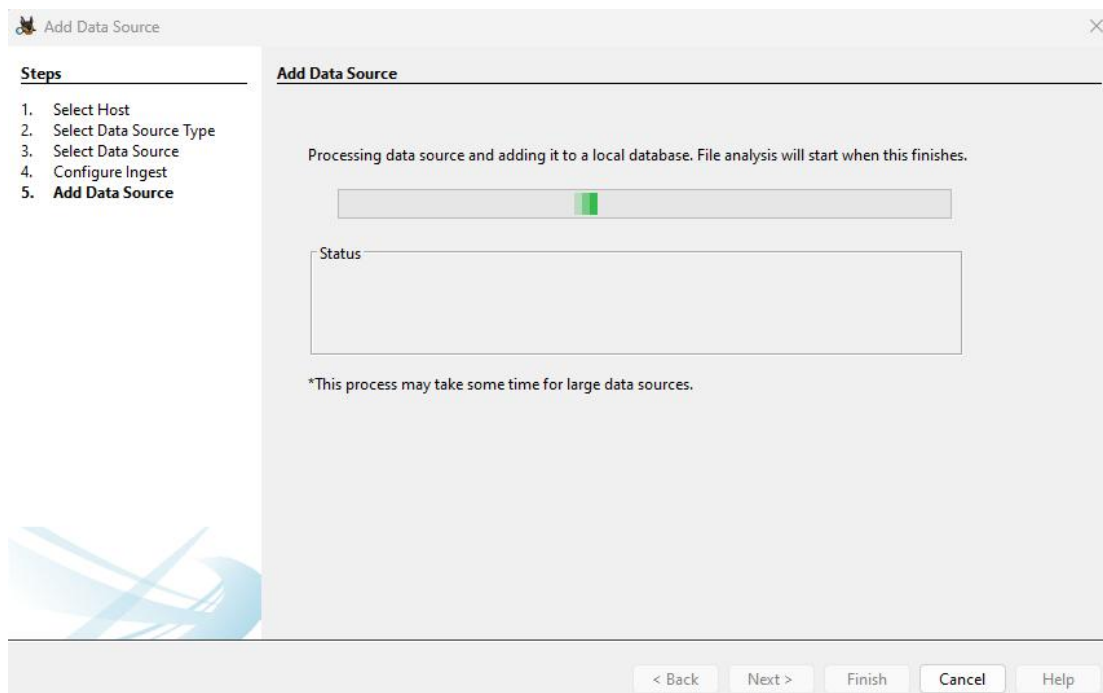
Step 13: Press the next button to proceed



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.

Made by Moez Javed

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