

The following is an introduction to Autopsy:

You need to create a case before you can analyze data in Autopsy. A case can contain one or more data sources (disk images, disk devices, logical files). The data sources can be from multiple drives in a single computer or from multiple computers. It's up to you.

Each case has its own directory that is named based on the case name. The directory will contain configuration files, a database, reports, and other files that modules generates. The main Autopsy case configuration file has an ".aut" extension.

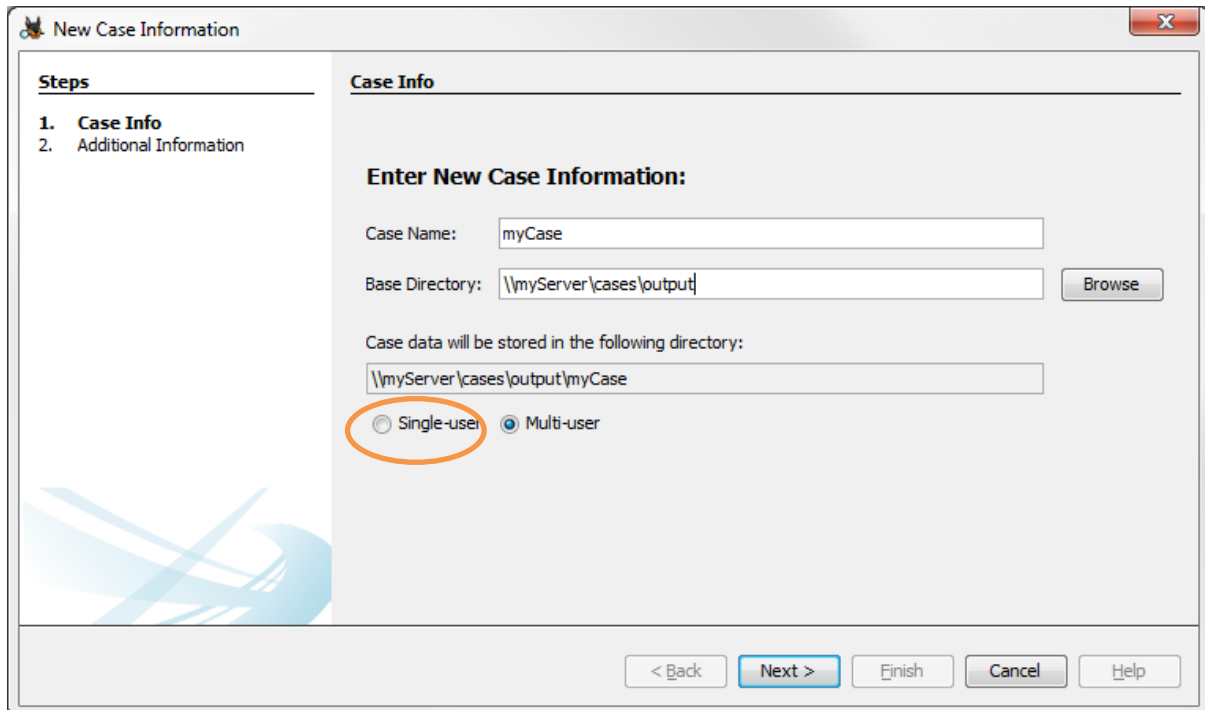
Creating a Case



There are several ways to create a new case:

- The opening splash screen has a button to create a new case.
- The "Case", "Create New Case" menu item

The New Case wizard dialog will open and you will need to enter the case name and base directory. A directory for the case will be created inside of the "base directory". If the directory already exists, you will need to either delete the existing directory or choose a different combination of names.



The image shows a Windows-style dialog box titled "New Case Information". It has a standard title bar with a close button (X) in the top right corner. The dialog is divided into two main sections. On the left is a "Steps" pane with a list: "1. Case Info" (which is selected and bolded) and "2. Additional Information". The main area on the right is titled "Case Info" and contains the heading "Enter New Case Information:". Below this heading are three text input fields. The first is labeled "Case Name:" and contains the text "myCase". The second is labeled "Base Directory:" and contains the text "\\myServer\cases\output"; to its right is a "Browse" button. The third field is labeled "Case data will be stored in the following directory:" and contains the text "\\myServer\cases\output\myCase". Below these fields are two radio button options: "Single-user" and "Multi-user". The "Single-user" radio button is selected and is circled with an orange oval. At the bottom of the dialog is a row of five buttons: "< Back", "Next >" (which is highlighted with a blue border), "Finish", "Cancel", and "Help".

Steps

- 1. Case Info**
2. Additional Information

Case Info

Enter New Case Information:

Case Name:

Base Directory:

Case data will be stored in the following directory:

☐ Single-user ☒ Multi-user

< Back Next > Finish Cancel Help

Adding a Data Source

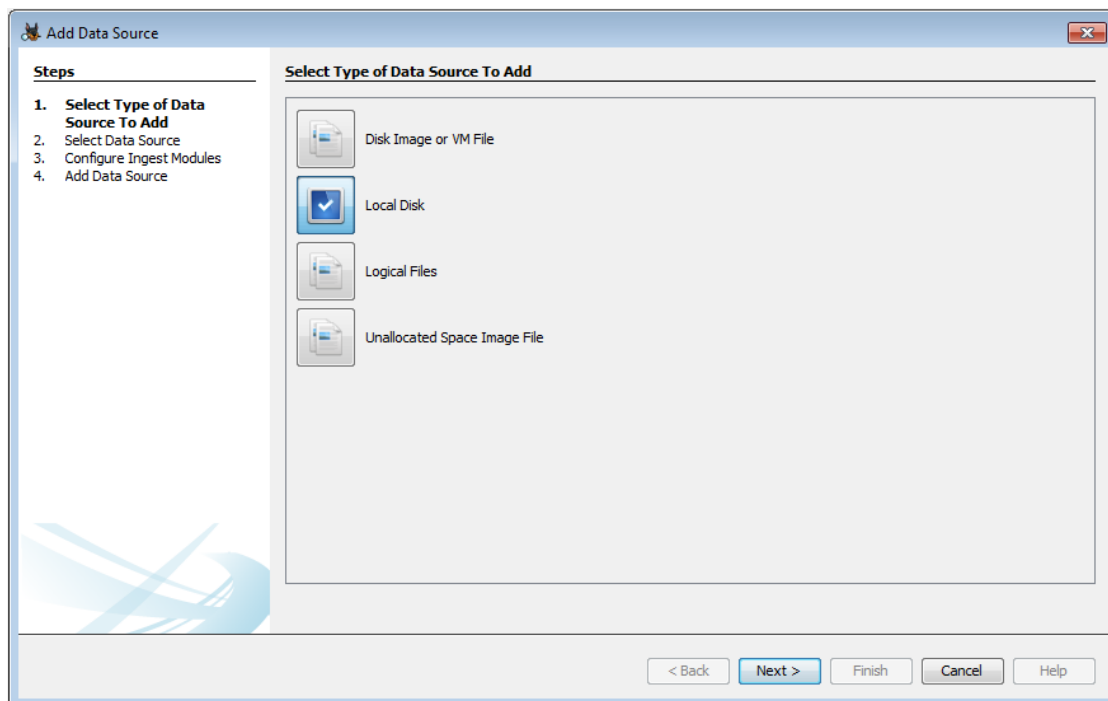
You can add a data source in several ways:

- After you create a case, it automatically prompts you to add a data source.
- There is a toolbar item to add a Data Source when a case is open.
- The "Case", "Add Data Source" menu item when a case is open.

The data source must remain accessible for the duration of the analysis because the case contains a reference to the data source. It does **not** copy the data source into the case folder.

Regardless of the type of data source, there are some common steps in the process:

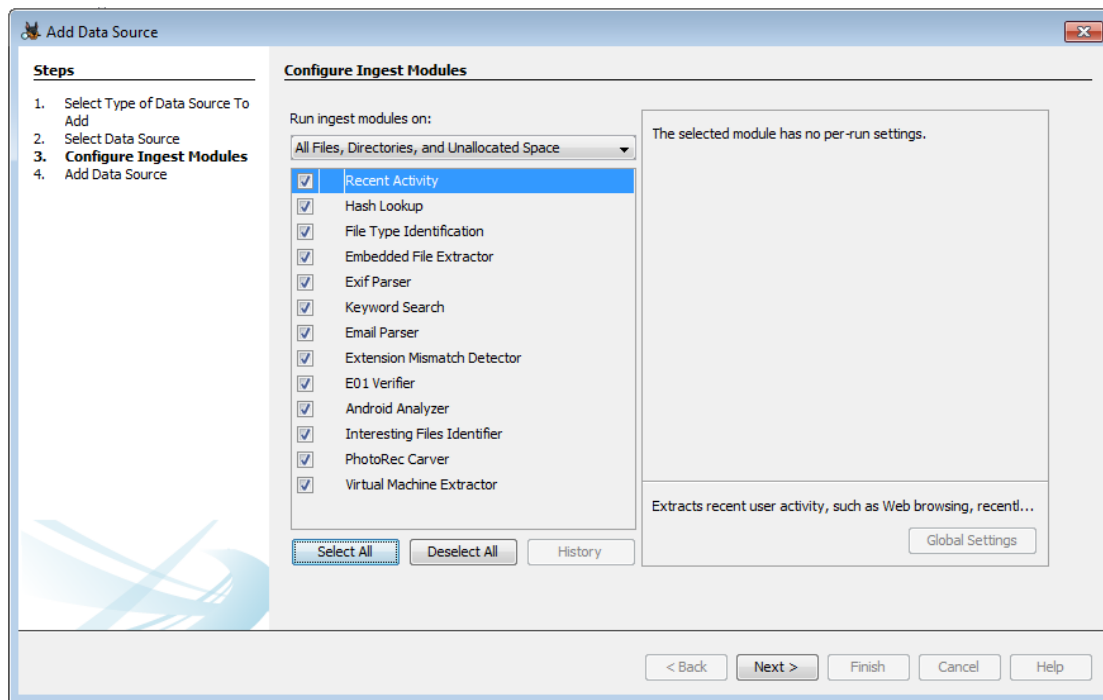
1) You will select the type of data source.



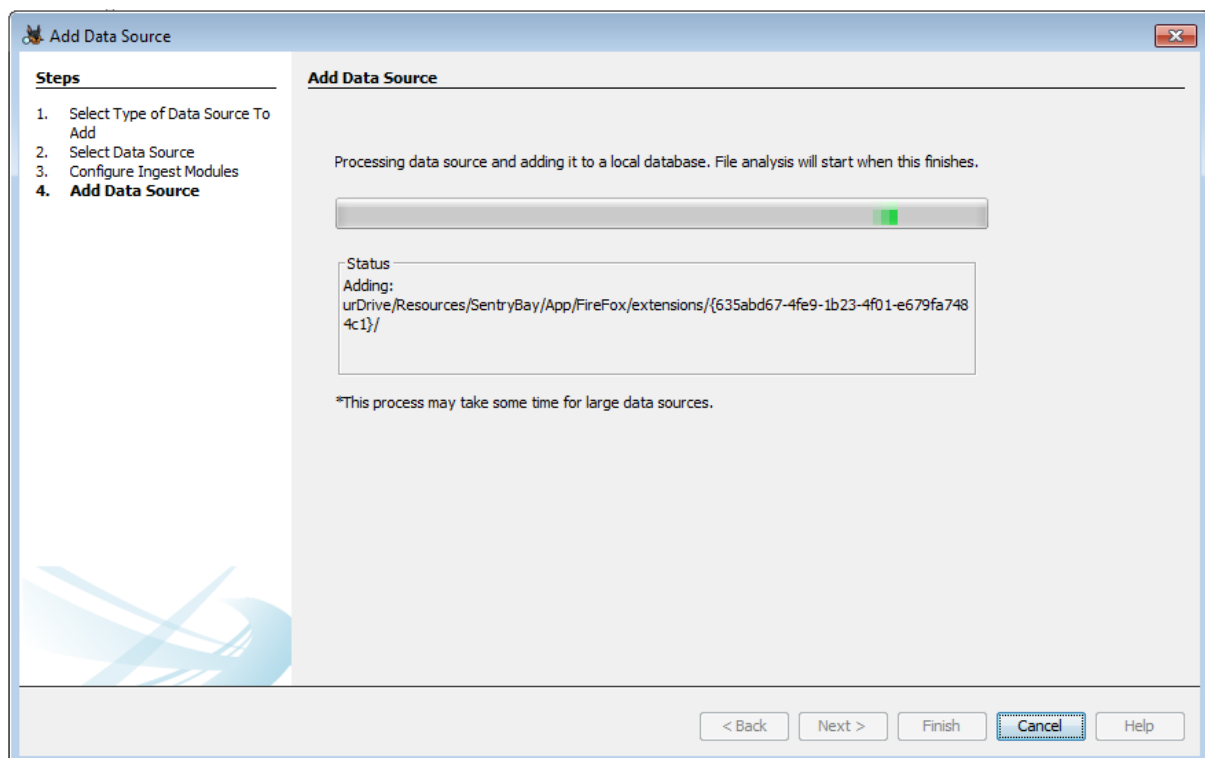
2) You will be prompted to specify the data source to add. This screen varies based on the data source type. Details on adding each type of data source are provided below.

3) Autopsy will perform a basic examination of the data source and populate an embedded database with an entry for each file in the data source. No content is analyzed in the process, only the files are enumerated.

4) While it is examining the data source, you will be prompted with a list of ingest modules to enable. If one or more ingest profiles have been saved, there will be a screen before this asking whether to use one of the saved profiles or do a custom setup.



5) After you configure the ingest modules, you may need to wait for Autopsy to finish its basic examination of the data source.



6) After the ingest modules have been configured and the basic examination of the data source is complete, the ingest modules will begin to analyze the file contents.

You cannot remove a data source from a case!!.

Adding a Disk Image

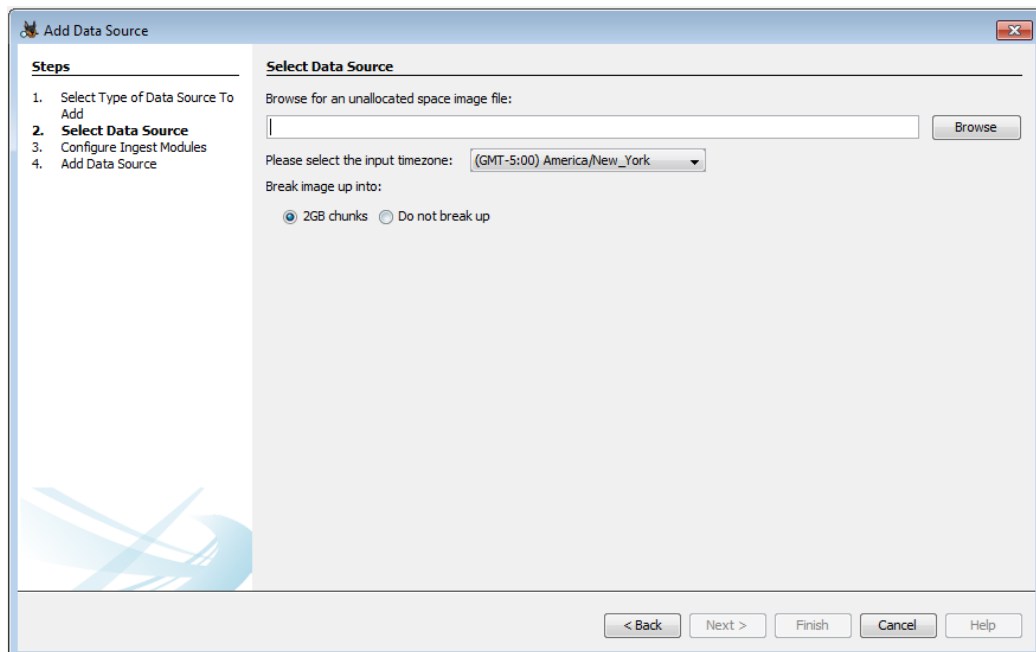
Autopsy supports disk images in the following formats:

- Raw Single (For example: *.img, *.dd, *.raw, *.bin)
- Raw Split (For example: *.001, *.002, *.aa, *.ab, etc)
- EnCase (For example: *.e01, *.e02, etc)
- Virtual Machines (For example: *.vmdk, *.vhd)

To add a disk image:

1. Choose "Disk Image or VM File" from the data source types.
2. Browse to the first file in the disk image. You need to specify only the first file and Autopsy will find the rest.
3. Choose the timezone that the disk image came from. This is most important for when adding FAT file systems because it does not store timezone information and Autopsy will not know how to normalize to UTC.
4. Choose to perform orphan file finding on FAT file systems. This can be a time intensive process because it will require that Autopsy look at each sector in the device.

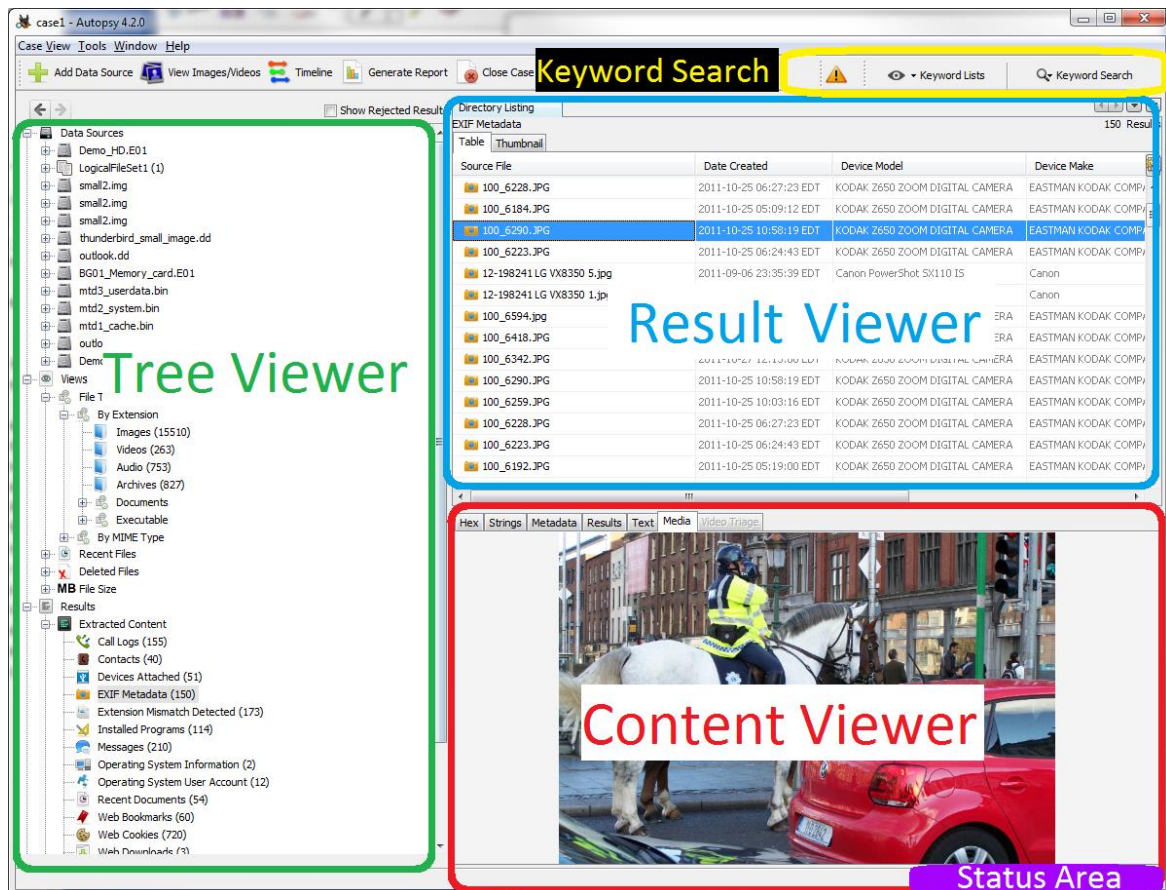
Adding an Unallocated Space Image File



Overview

The major areas in the Autopsy User Interface (UI) are:

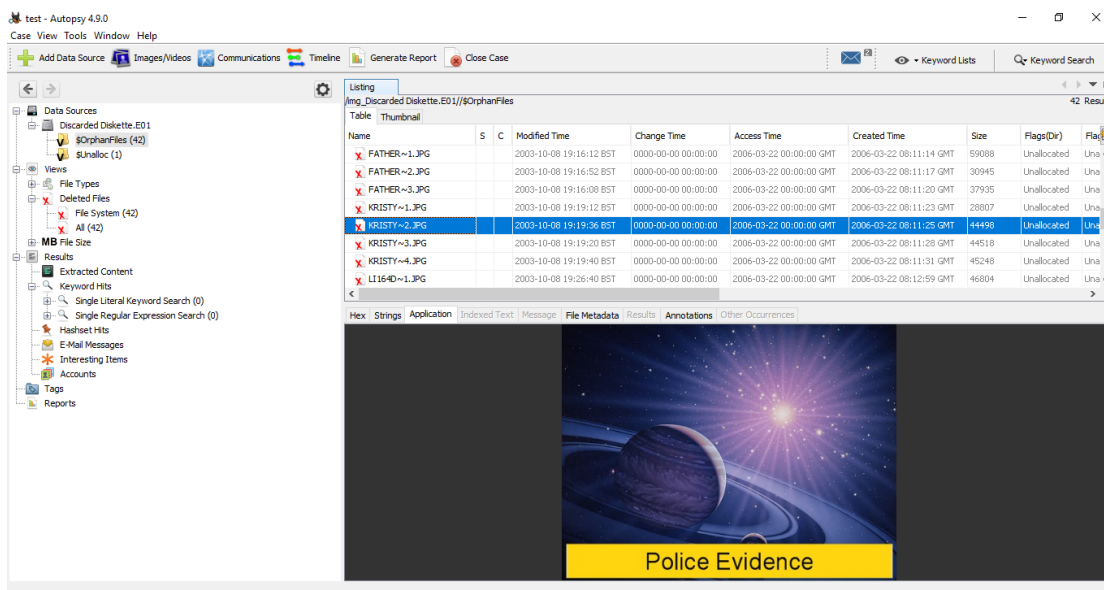
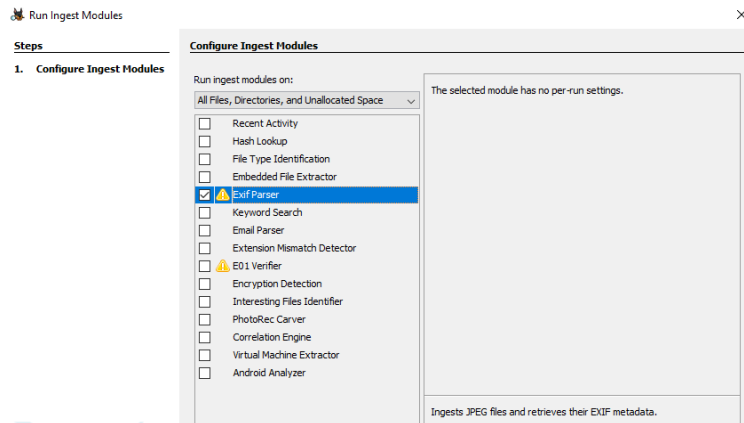
- **Tree Viewer**, shown outlined in green below
- **Result Viewer**, shown outlined in blue below
- **Content Viewer**, shown outlined in red below
- **Keyword Search**, shown outlined in yellow below
- **Status Area**, shown in solid purple below



Tasks:

1- On the created case add the **Discarded Diskette.E01** image file and explore in in Autopsy,

When adding the evidence file and when **configuring Ingest modules** choose only **Exif Parser**. *Notice the recovery of files from the image automatically.*



2. Explore the FAT disks throughout the second lab sheet.

See the following link for more details:

http://sleuthkit.org/autopsy/docs/user-docs/4.3/uilayout_page.html