SYBEROFFENSE

Lab – Getting Started with Autopsy

In this lab, you will be introduced to Autopsy. Autopsy is a digital forensics platform and graphical interface to The Sleuth Kit®. Law enforcement, military, and corporate examiners can use it to investigate what happened on a computer. Autopsy can also be used to recover lost or deleted files and images.

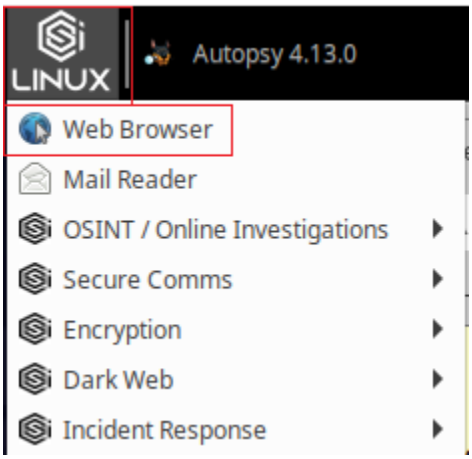
Autopsy was built to sit on top of the Sleuth Kit to offer an intuitive, GUI-based forensic suite that utilizes the strength of Sleuth Kit while at the same time offering the basics of a case management tool.

Lab Requirements

- One virtual install of CSI Linux
- Downloaded image file from **http://dftt.sourceforge.net/**

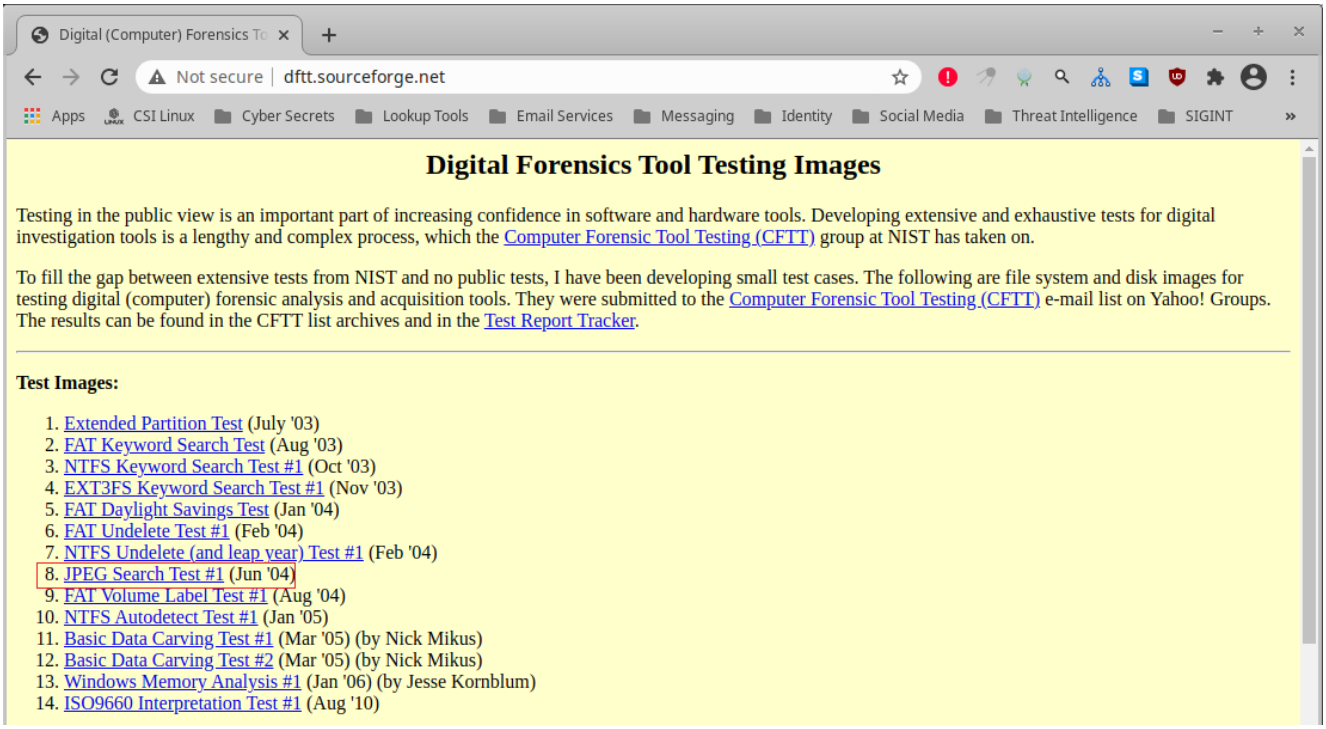
Begin the lab!

Click on the Application launcher, and from the context menu, select Web Browser.

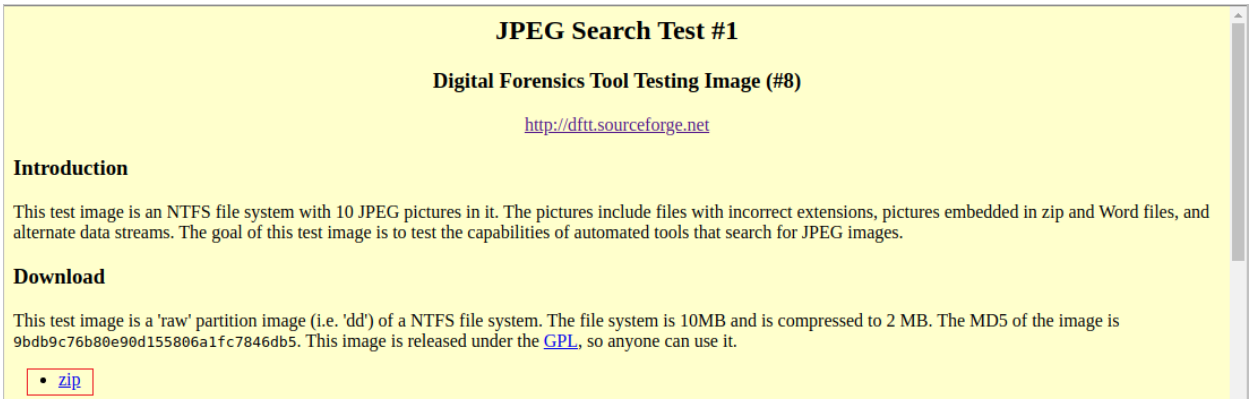


In the address bar, point your browser to **http://dftt.sourceforge.net/**

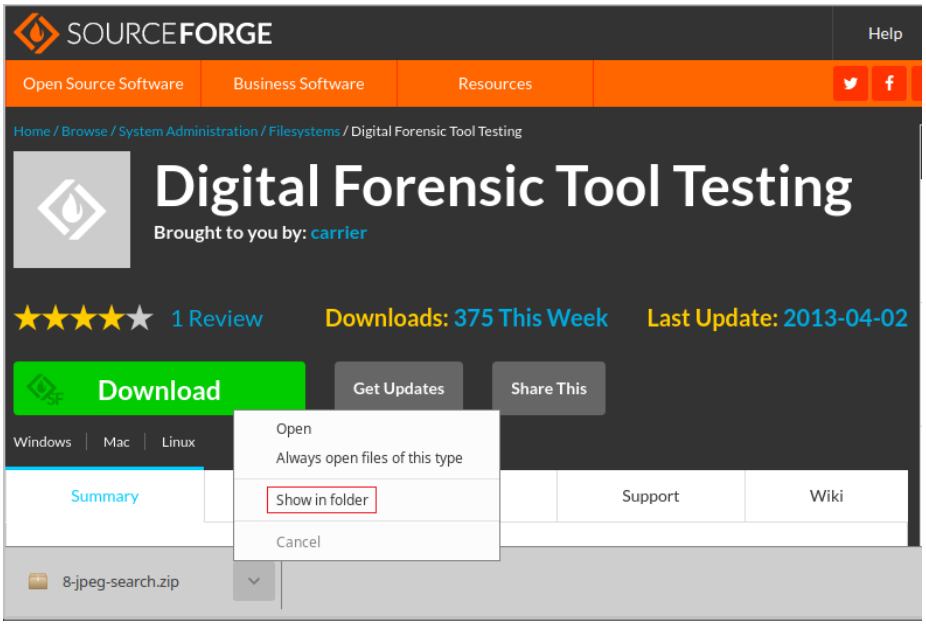
From the test images, find and click on "8. JPEG Search Test #1"



Under Download, click on the "zip" link.

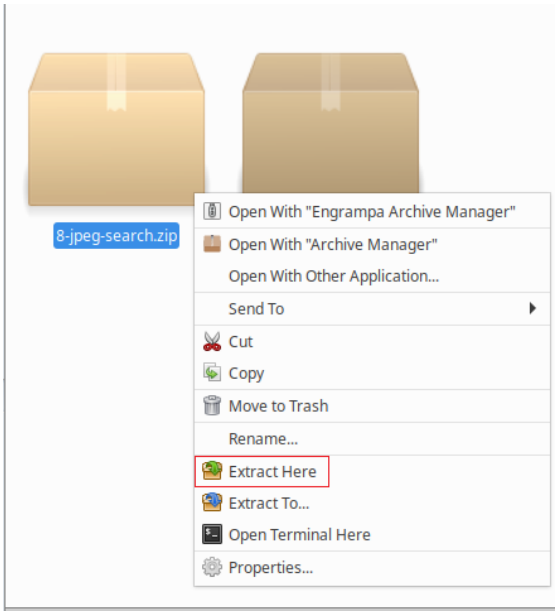


Wait for the download to begin.



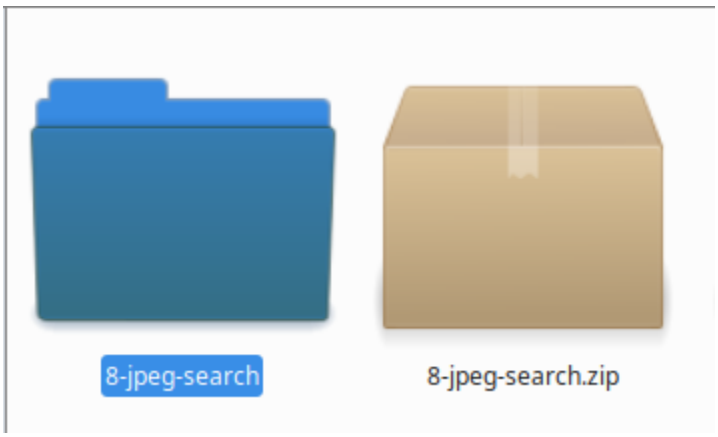
Scroll to the bottom of your browser. Find the completed download. Click on the down arrow, and from the context menu select, **Show in folder**.

Inside the download folder, right-click on the freshly downloaded zip file, and from the context menu, select, **Extract here**.

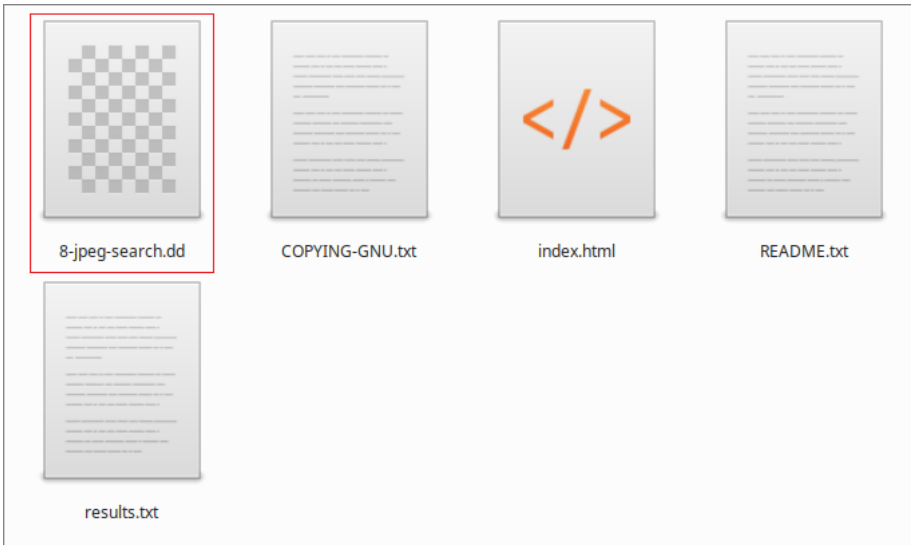


Accept the default Archive Manager and click OK. Your Test image has been extracted.

This is your target folder for this lab.



This will be your image for the lab located inside the target folder.



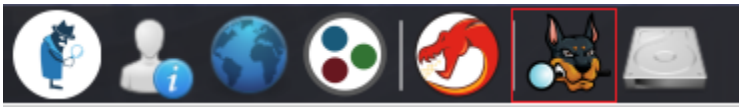
Closeout the File Manager.

Closeout your browser.

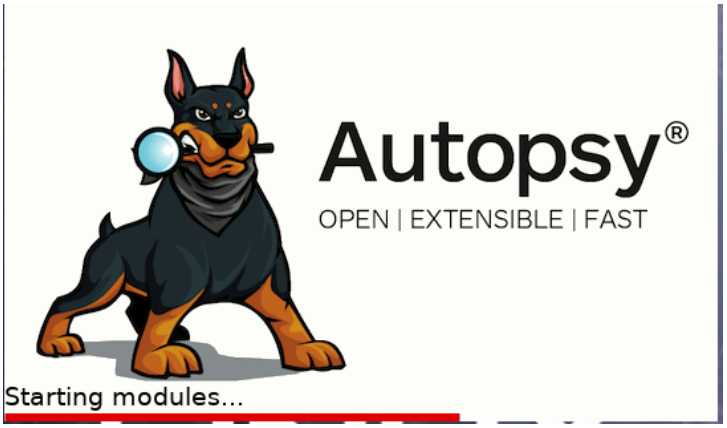
SYBEROFFENSE

Open Autopsy

From the bottom taskbar over to the right, find the Autopsy icon and click to open.

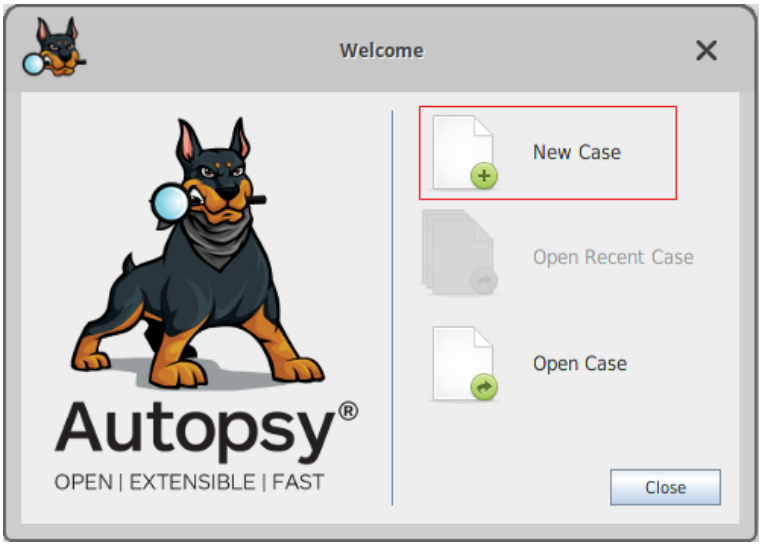


Autopsy begins to load.

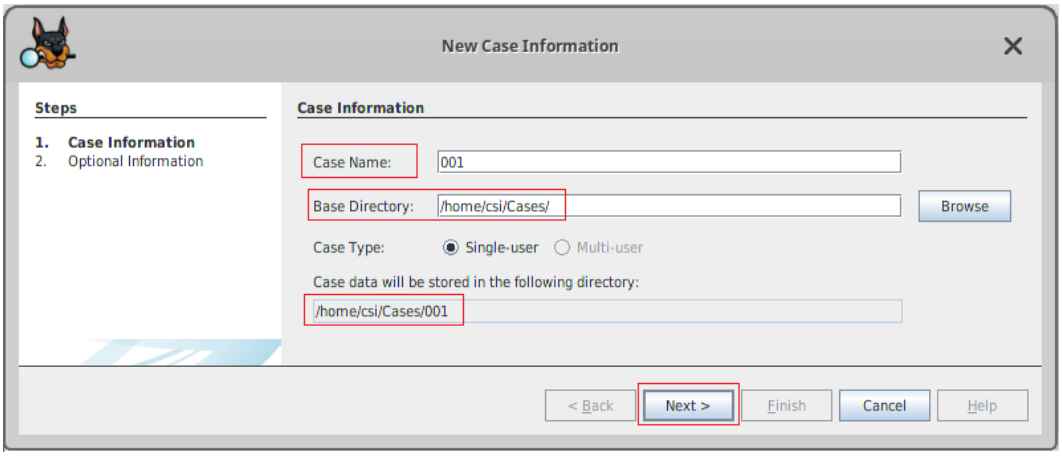


Create a New Case

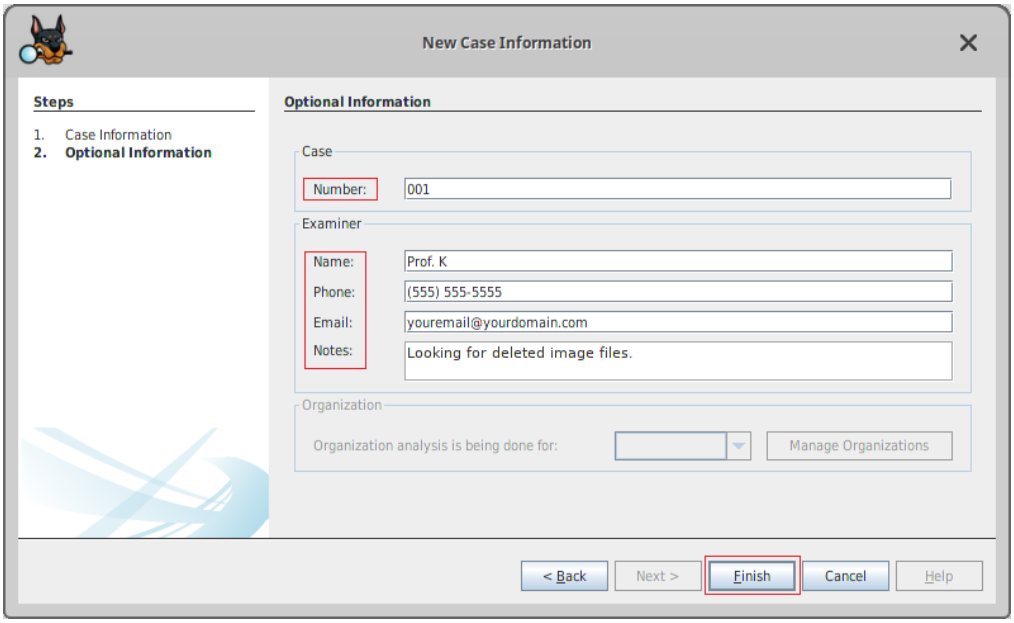
On the Welcome screen, select the option to create a **New Case**.



Here, we have given this case a numerical case name (001). Take note of the default director for cases created inside of CSI Linux. On your desktop, you have a case folder. This is a shortcut to this location. Click **Next**.

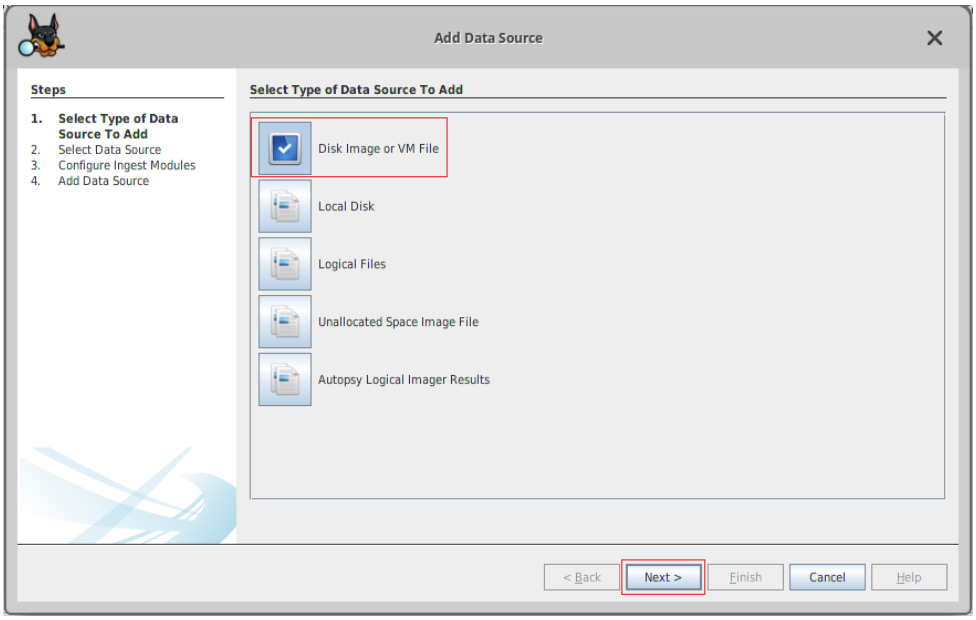


On the next screen, you can fill in the case number, your information and provide some notes pertaining to the case. Click **Finish**.

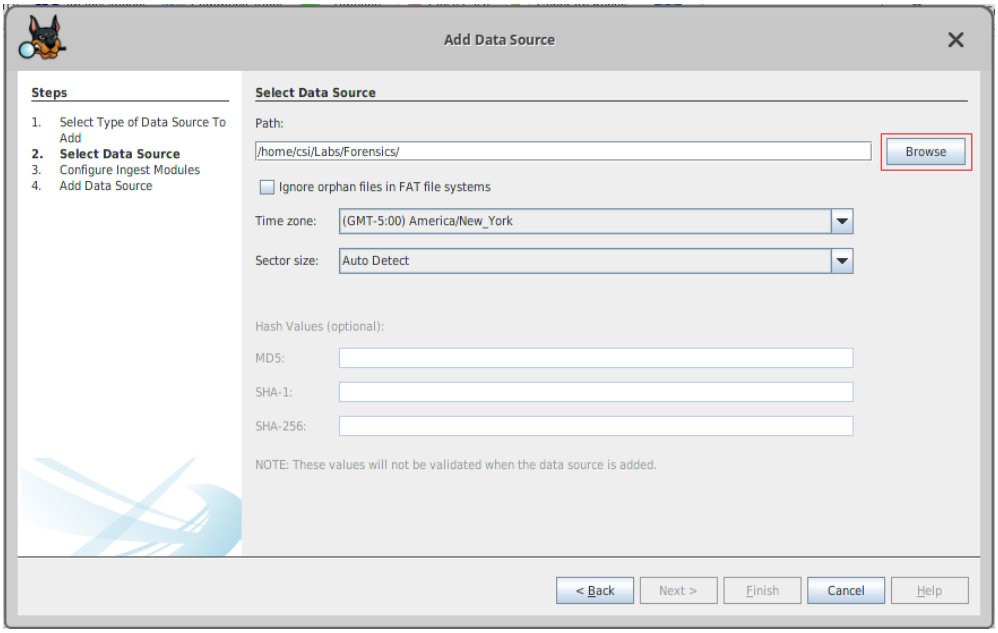


Autopsy creates a database for your case.

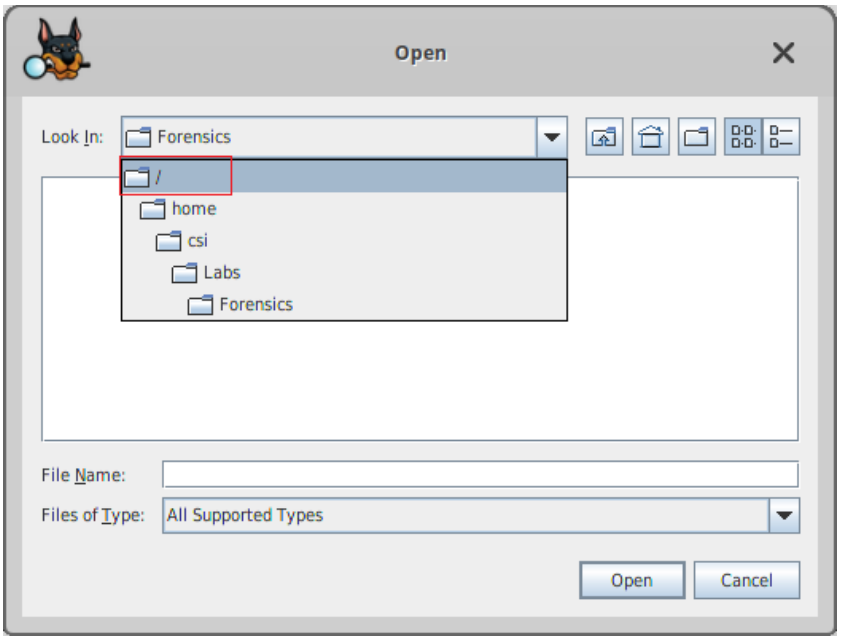
On the next screen, you can import the forensic image. Accept the default image type. Click **Next.**



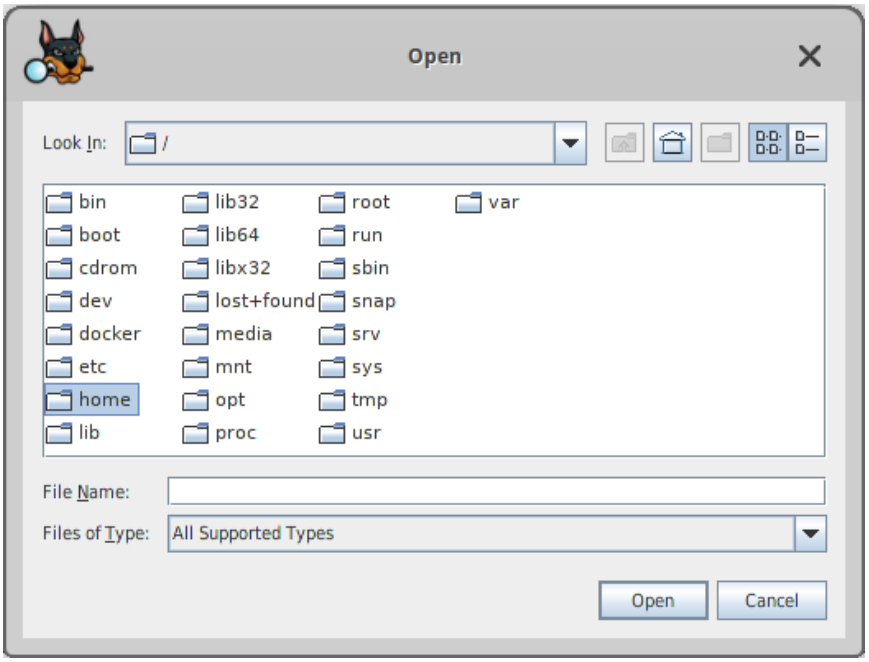
On the next page, we browse to the forensic image we downloaded and extracted earlier. Click on the browse button.



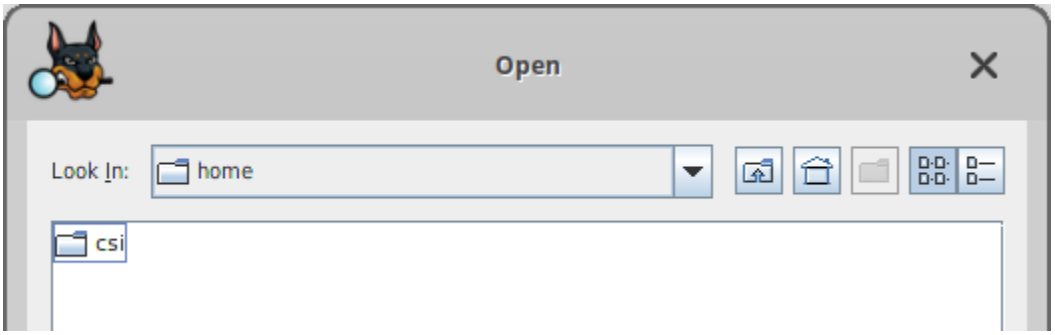
On the next screen, in the Look in window, expand the window and select the root (/) folder from the options.



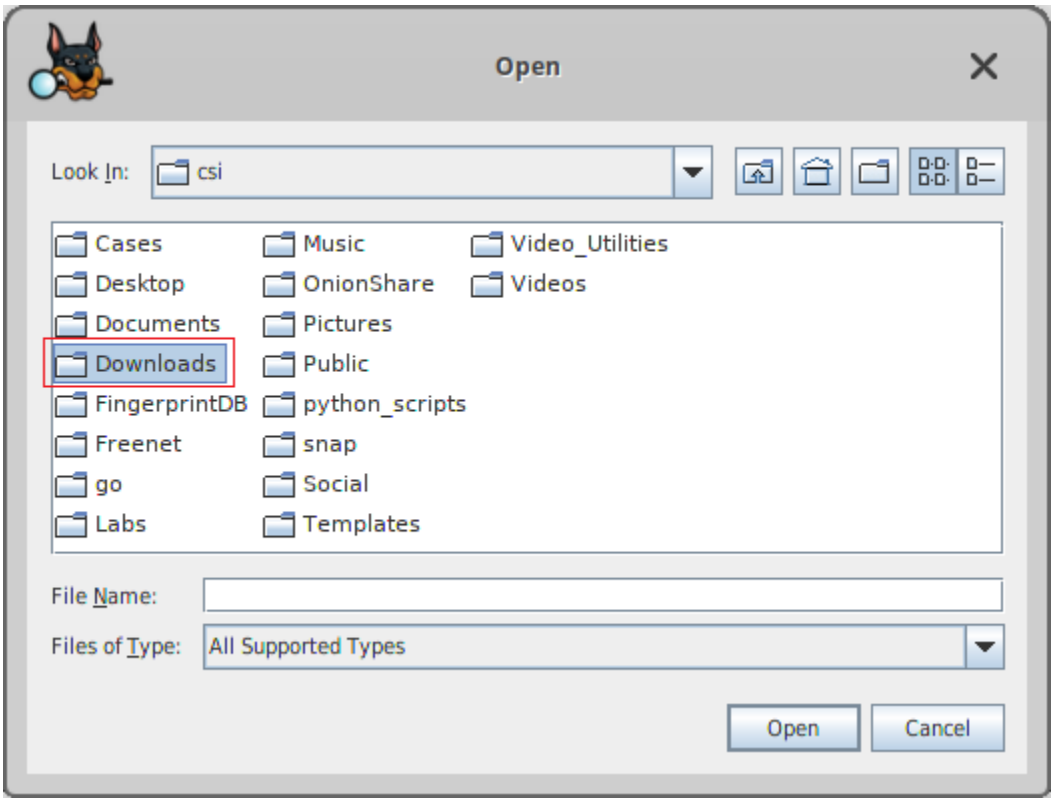
Inside the middle windowpane, select and click on the home folder.



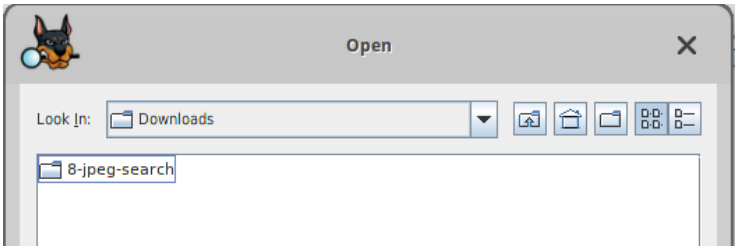
On the next screen, open the **csi** folder.



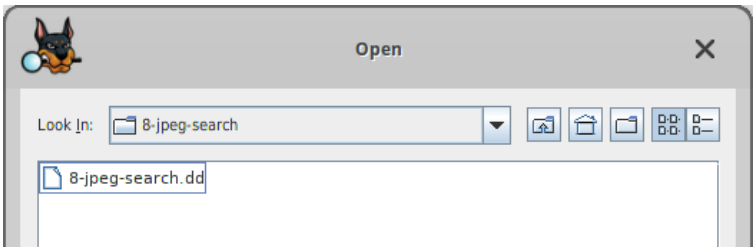
Select and open the Downloads folder.



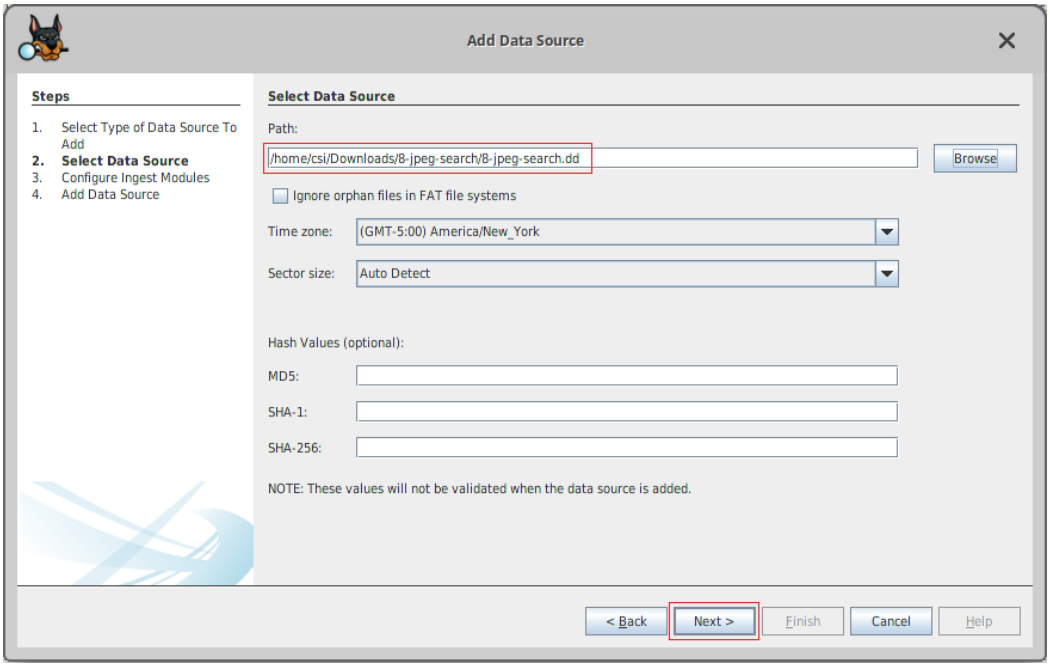
On the next screen, open your extracted target folder.



X2 click the extracted forensic image.



Back at the Add a Data Source home page, click next.

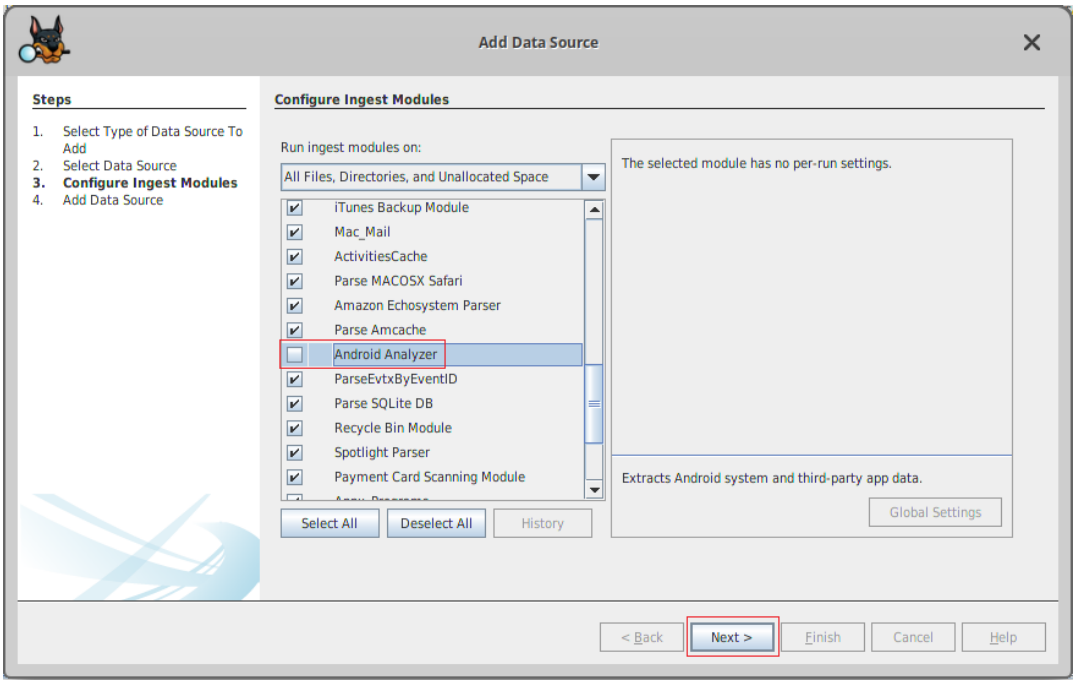


On the next page, you can select and deselect which ingest modules to run your files through.

Ingest modules are configured to find user content quickly. The ingest modules are grouped into pipelines, and each file goes down the pipeline, module by module.

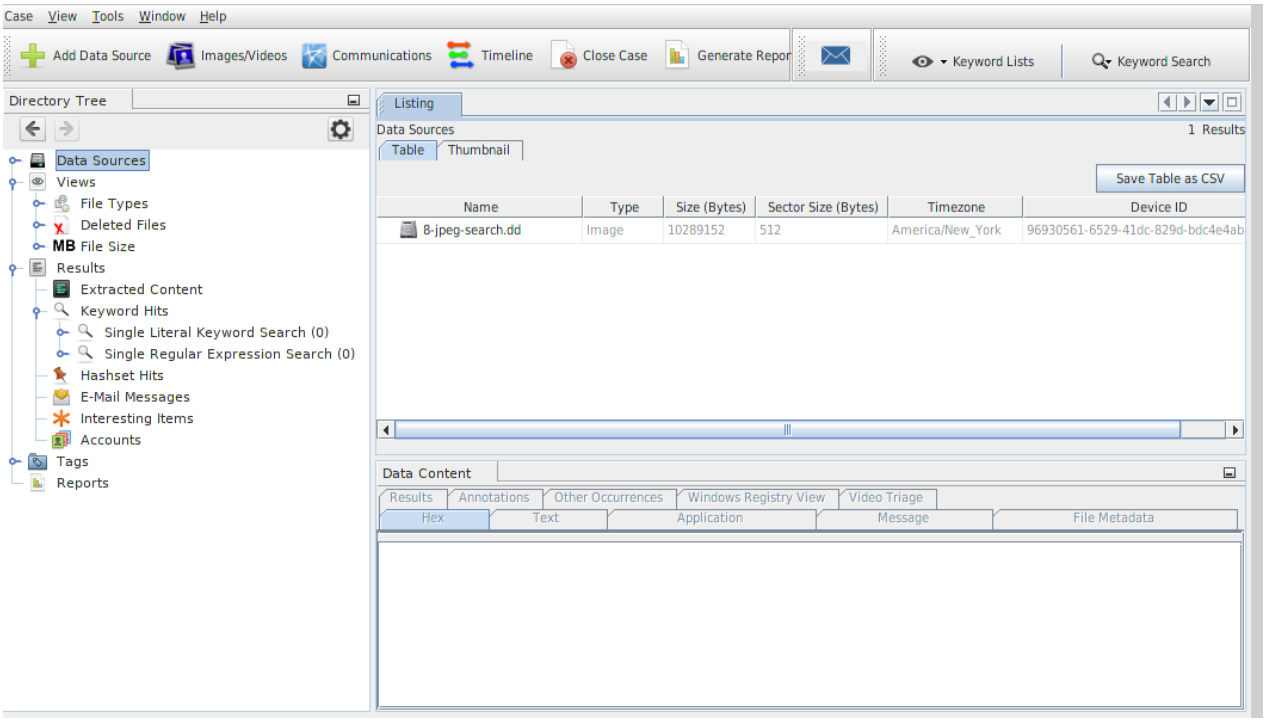
Some of this ingest modules can cause issues if they are not needed them. Uncheck the box for the **Android Analyzer** and **Plaso**. Plaso only works on Windows.

Feel free to click on each of the ingest modules to see what it does. Click Next.



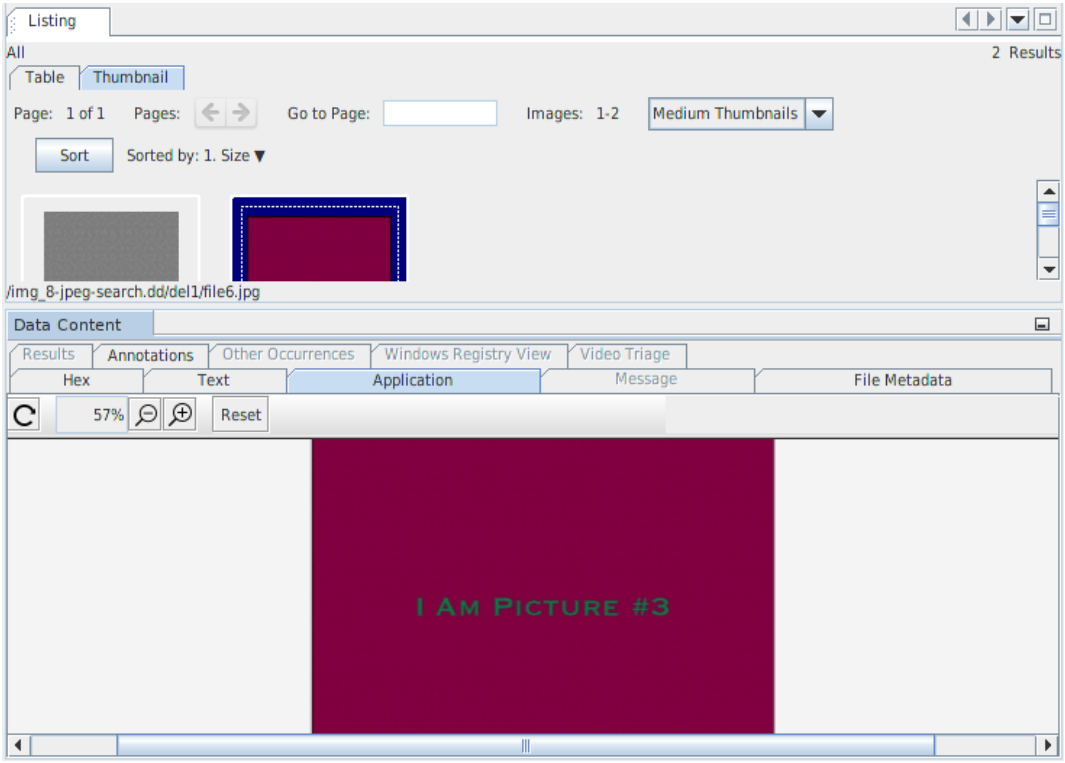
Autopsy will scan the data source we imported using all the ingest modules we have selected since our image is very small. The scan happens very quickly, but it can take quite a bit of time to parse through all the data on a much larger data source.

Our data source is passed through each module and then passed on to the next module waiting in line. Over in the left windowpane, we can see the results of the module scan.



In the left windowpane, click on Deleted Files. In the right windowpane, you will see the number of deleted files found. In the right windowpane, We can see the images just by clicking on the thumbnail tab. If you would like a better view, click on a thumbnail image, and in the bottom windowpane, you will be presented with a better view.

Over to the right, you can click on the file metadata tab to view the image's metadata and view the hex data use the hex tab.



Summary

In our first lab, we saw how we create a new forensic case and import a forensic image.

The steps of creating a forensic case are as follows:

- Create a forensic image
- Create the case
- Import the forensic image
- Analyze the data

End of the lab!