SAT1: 011: **Analyzing a Forensic Hard Drive Capture**

Overview

Once the proper steps have been taken to secure and verify the disk image, the actual contents of the image must be analyzed for suspicious or incriminating evidence.

Time: 60 Minutes

Learning Objectives

Upon completion of this lab, you should be able to:

1. Start a new case and add the appropriate disk image file.
2. Review the contents of the disk image file.
3. Print out a basic report.
4. Use the search feature to search by keyword.

Log in to the Lab Machine

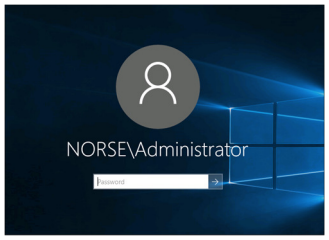
Select the **Windows 10** machine on the Machines Tab.

Select the 

on the **Windows 10** machine and

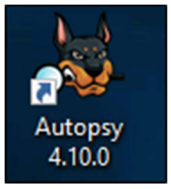
click on the 

on the **Machines** tab, and press **Enter**.



1.0 Create a New Case in Autopsy

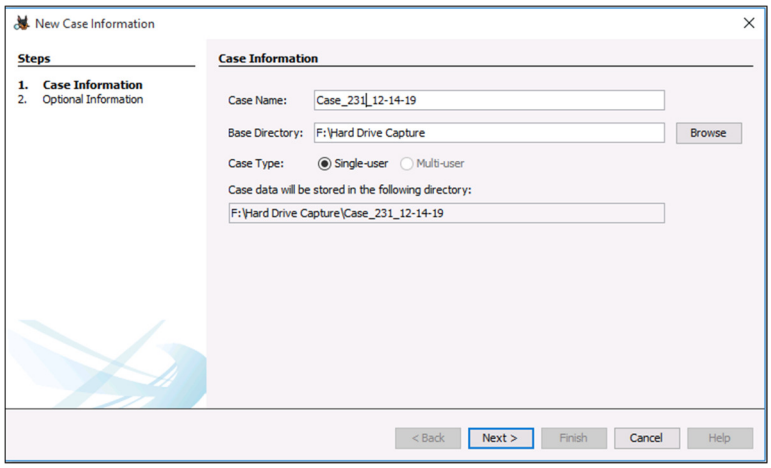
1.1 Launch **Autopsy**.



Note: It can take several minutes for the software to load.

1.2 Select **New Case**.

1.3 Enter the **Case Name** and select the **Base Directory**. For our analysis, the files are located in `F:\Hard Drive Capture`. The **Case Type** will be **Single-user**. Multi-user is only used when multiple people need to access the same case data from multiple locations.

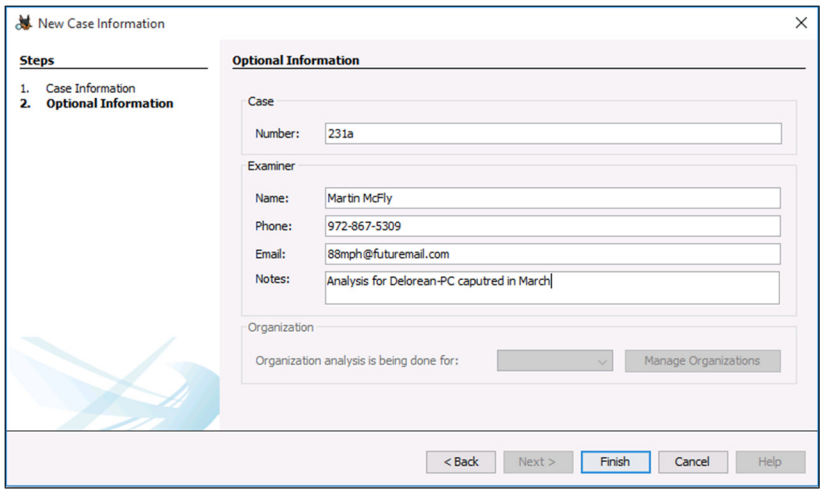


Note: Enter a descriptive case name, it helps identify the case to others who may need to access the case.

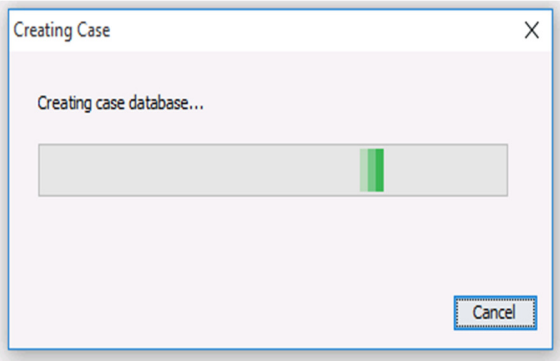
1.4 Click **Next**.

1.5 Enter the **Optional Information**.

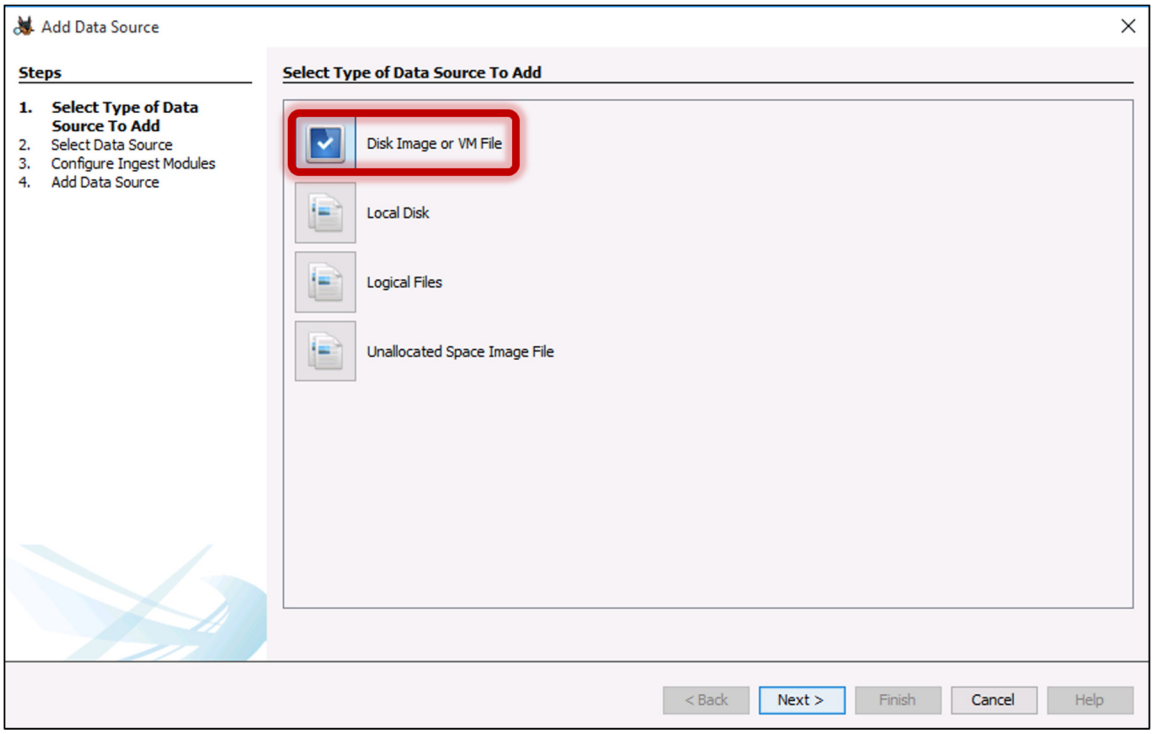
1. Case Number, should be relevant to your tracking system, if applicable.
2. Your name.
3. Phone Number.
4. Email Address.
5. Any notes you may have to add to describe the case or its purpose.



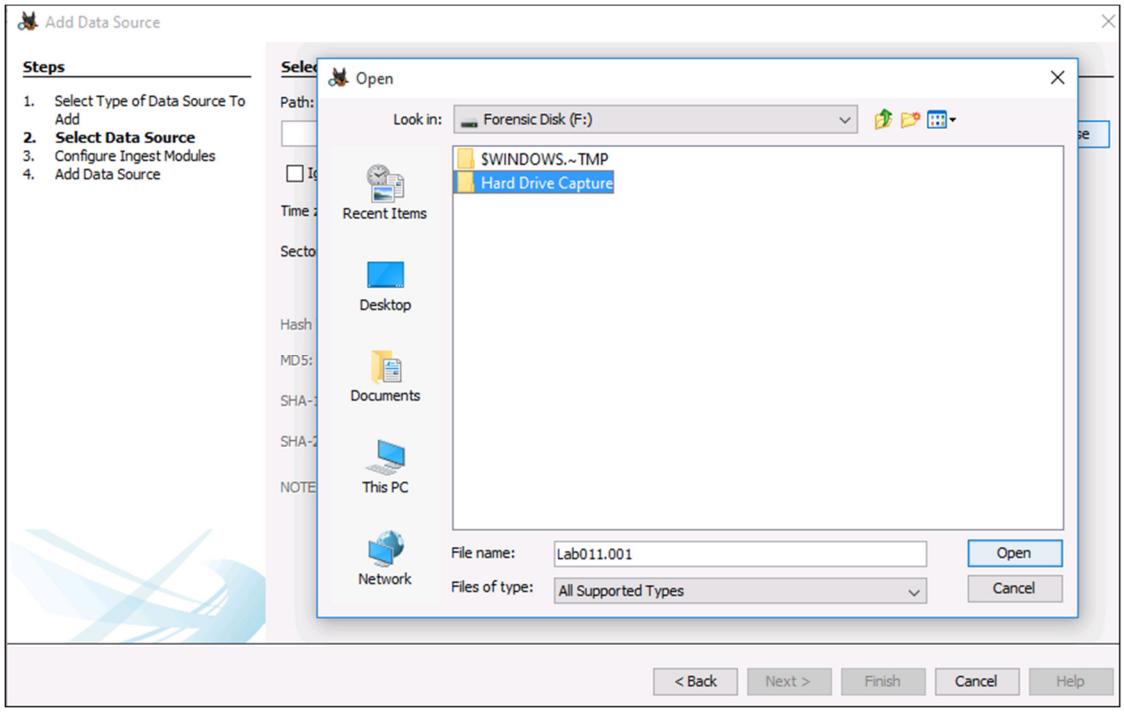
1.6 Click **Finish**. Autopsy will build a database.



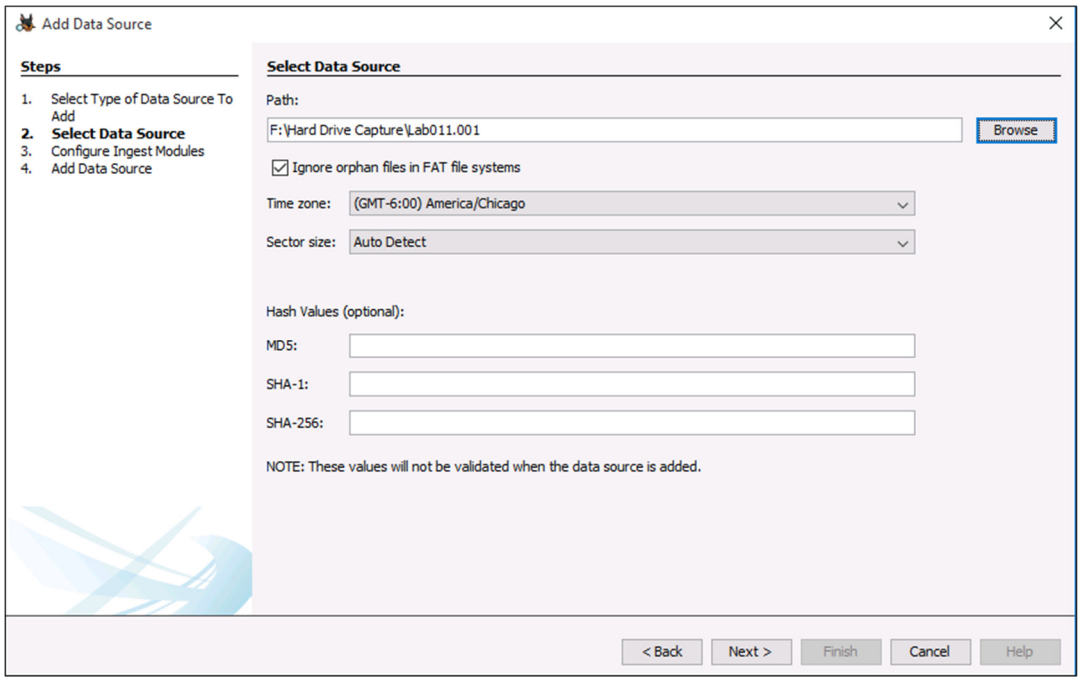
1.7 Add image file. Select **Disk Image or VM File**. Click **Next**.



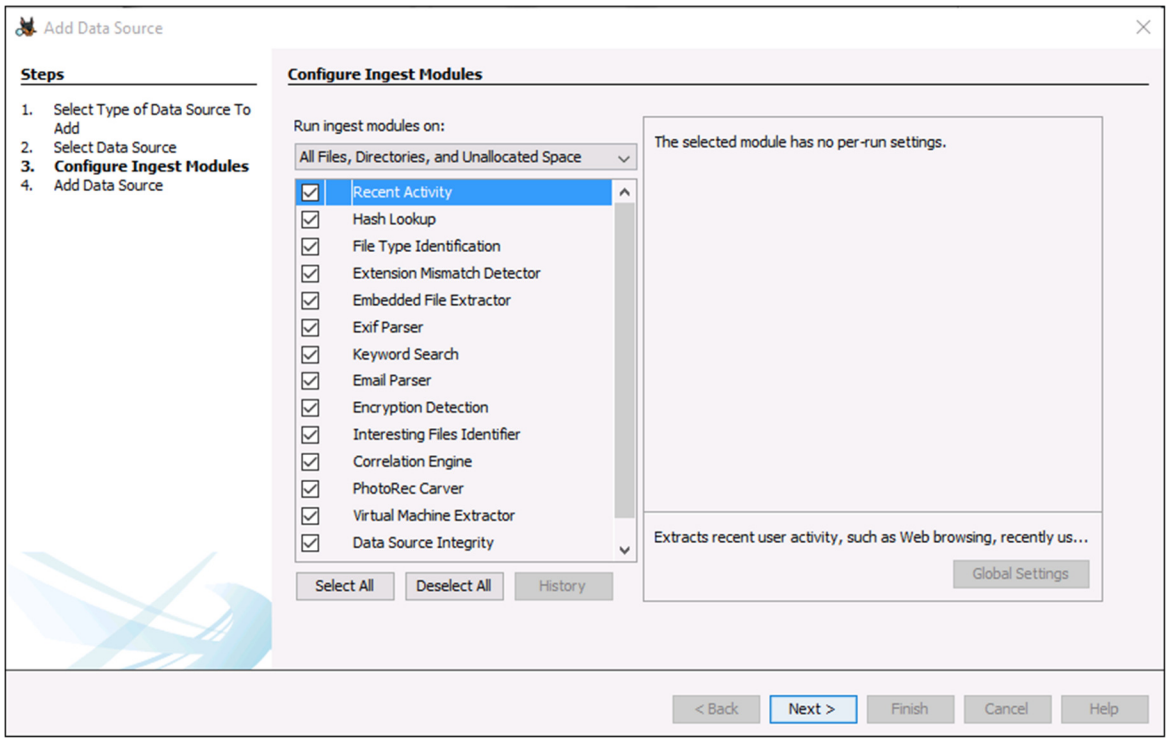
1.8 Click **Browse** and select the Path to the analysis Files `F:\Hard DriveCapture\File to be analyzed`



1.9 Select the **Time zone**, and ensure **Sector size** is set to **Auto Detect**.

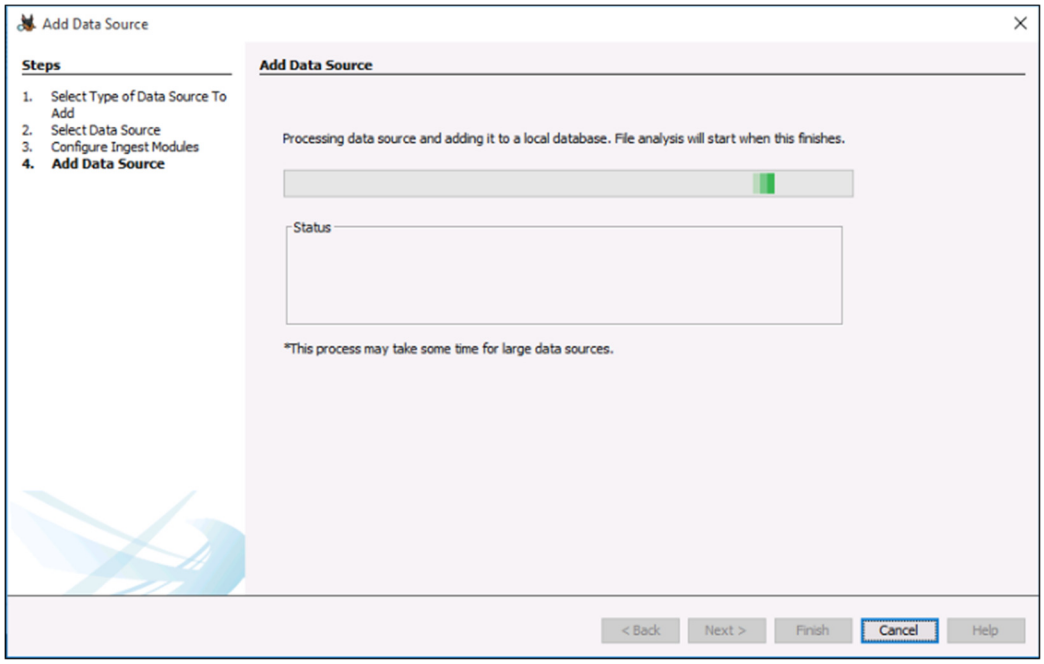


1.10 Select **Lab011.O01**, this will link the case to all relevant analysis files.

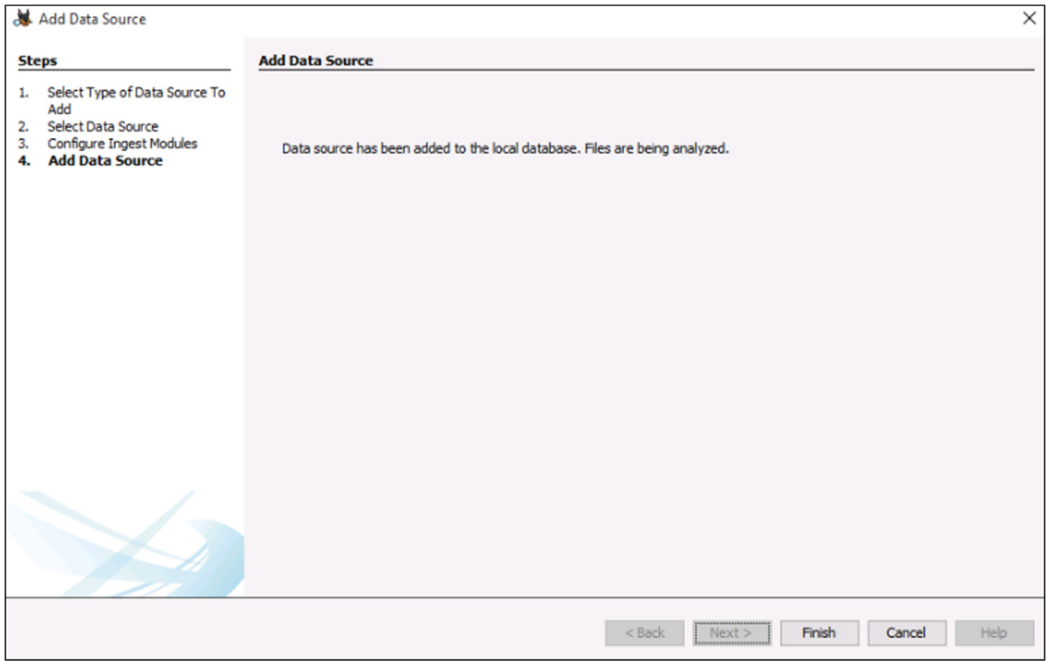


1.11 Click **Next**.

1.12 In this case, we will select all modules, click **Next**.



Autopsy will load the relevant files and begin the analysis. Depending on the size of the capture, this will typically take anywhere from 4-12 hours.

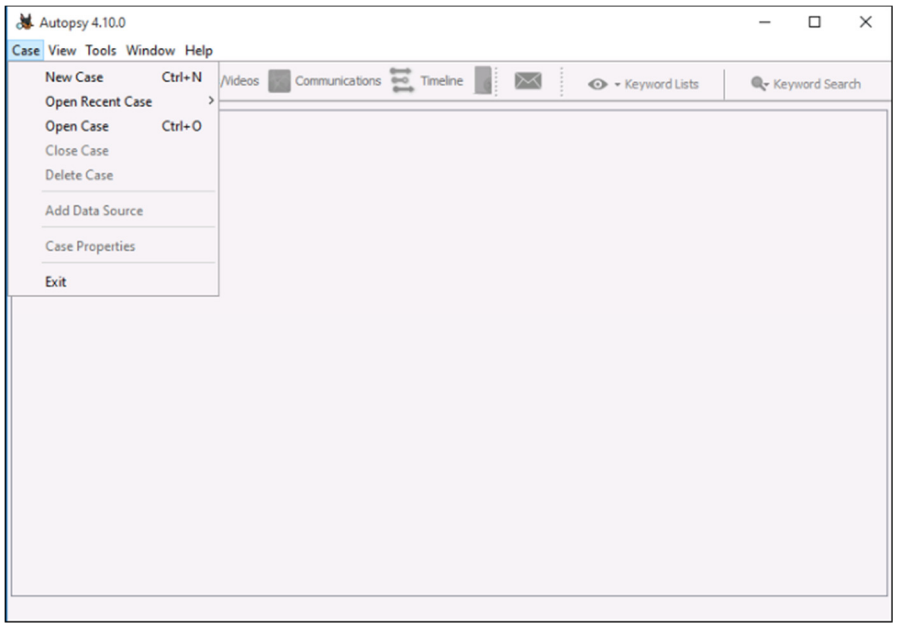


Since we have limited time during the lab to let this case build, we will cancel the analysis, and open a case that has already been stored on the hard drive.

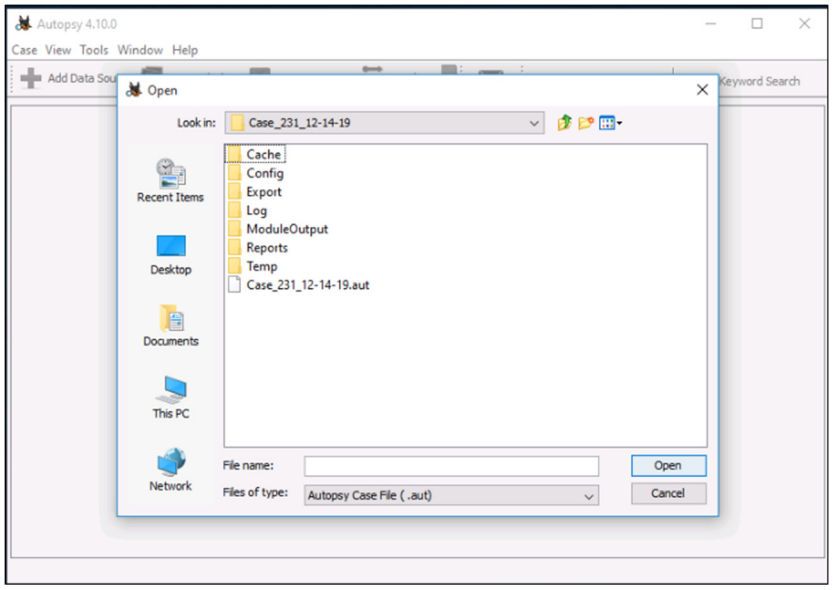
2.0 Analyze a Case in Autopsy

Note: When looking at the contents of an image, it is necessary to not only look at the clearly visible contents, such as folders on the desktop and images in user files, but the image must also be checked for hidden, encrypted, or deleted files.

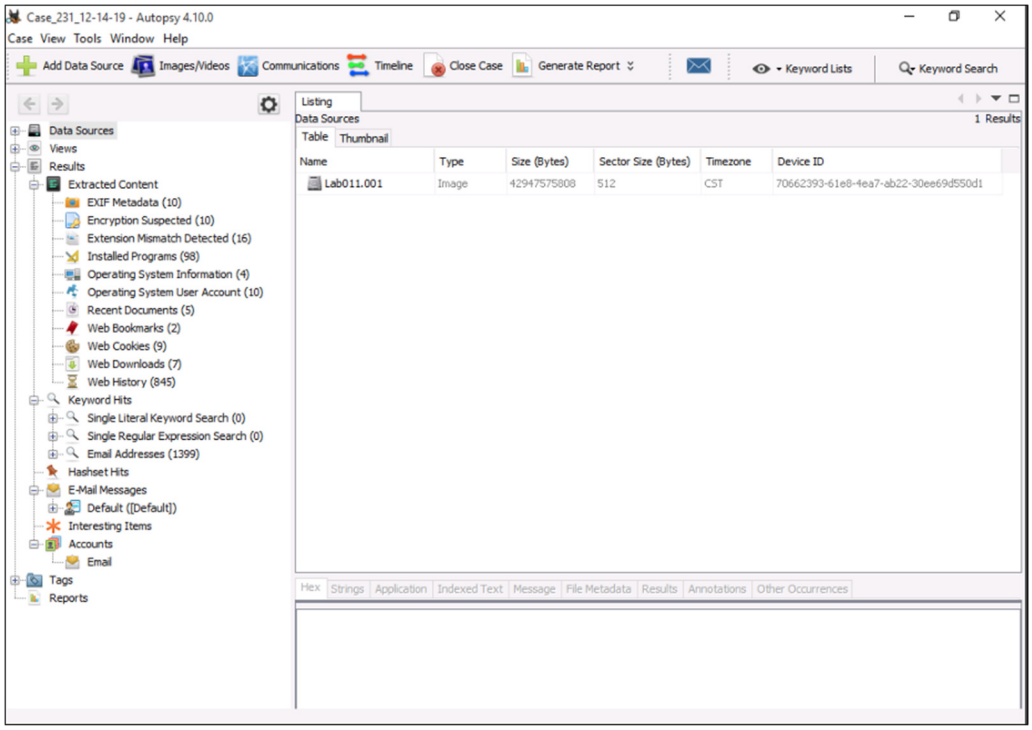
2.1 Go back to the Autopsy main menu. Click on **Case** and click on **Open Case**.



2.2 Navigate to `E:\Forensic Drive\Hard DriveCapture\Case_231_12-14-19` and open the `.aut` case file.



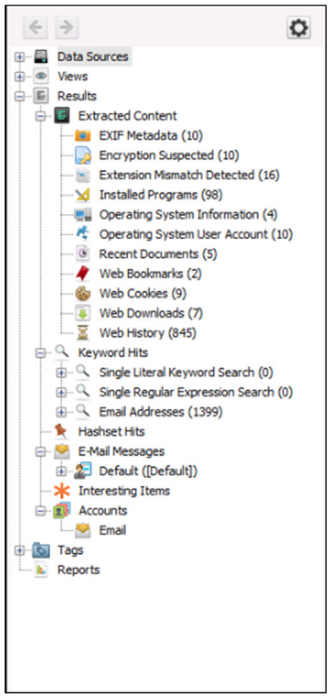
Autopsy will open the case file and load the artifact.



Autopsy is a great tool for exploring the files and configuration on a machine where suspected indicators may be located.

There are several Menus that you can use to help in your analysis.

On the left are the results of the Automated Analysis.



This information is generated by the Automated Analysis Modules in Autopsy including:

Ingest Modules

Recent Activity Module

Hash Database Lookup Module

File Type Identification Module

Embedded File Extraction Module

EXIF Parser Module

Keyword Search Module

Email Parser Module

Extension Mismatch Detector Module

E01 Verifier Module

Android Analyzer Module

Interesting Files Identifier Module

PhotoRec Carver Module

Click on each Automated Analysis Module to learn more from the Autopsy Wiki.

It is typically not enough just to conduct an automated analysis. Typically, we must also conduct a manual analysis to. Autopsy allows us to do that as well.

Tree Viewer

Result Viewer

Content Viewer

File Search

Timeline

Structured Threat Information Exchange (STIX)

Click on each Manual Analysis Module to learn more from the Autopsy Wiki.

Now that your familiar with Autopsy, lets do some exploring.

2.3 Analyze the information in the case, develop a list of indicators, and document what may have been going on in the case.

It is always better to assume that a suspect may have known that they were to be investigated and took steps to hide, delete, or otherwise make it difficult to find the information they had been storing on their USB or computer.

Once you are done, we will talk about what you found!

Good Luck!
