Part 4 - Recovering Files From Forensic Images with Autopsy

In this activity you will recover files from a forensic image with Autopsy.

Tools:

Product: Autopsy

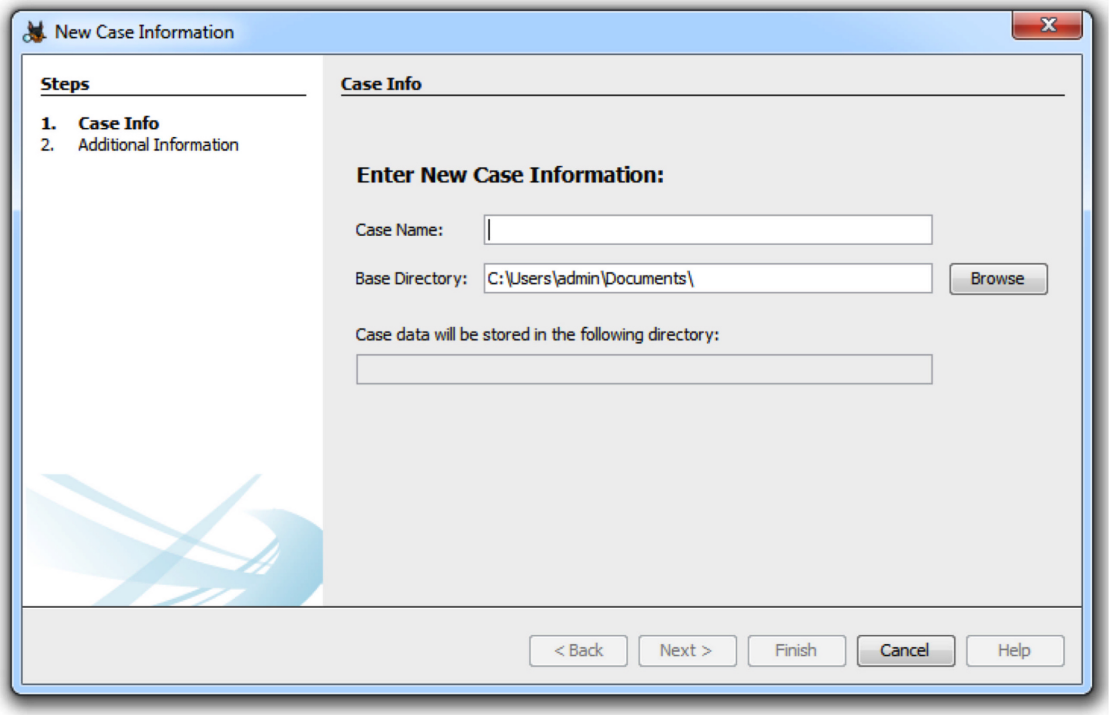
Manufacturer: Brian Carrier

Web site: http://www.sleuthkit.org/autopsy/download.php

Instructions:

1. Download and install Autopsy.
2. Download drive2.E01 and place the image on your desktop.
3. Launch Autopsy.
4. In the "Welcome" window, click the button named "Create New Case."
5. In the "New Case Information" window, as shown in Figure 1, add a case name, which is mandatory. The directory in which the case data will be saved will be populated automatically based on the case name. After entering the name click the "Next" button.

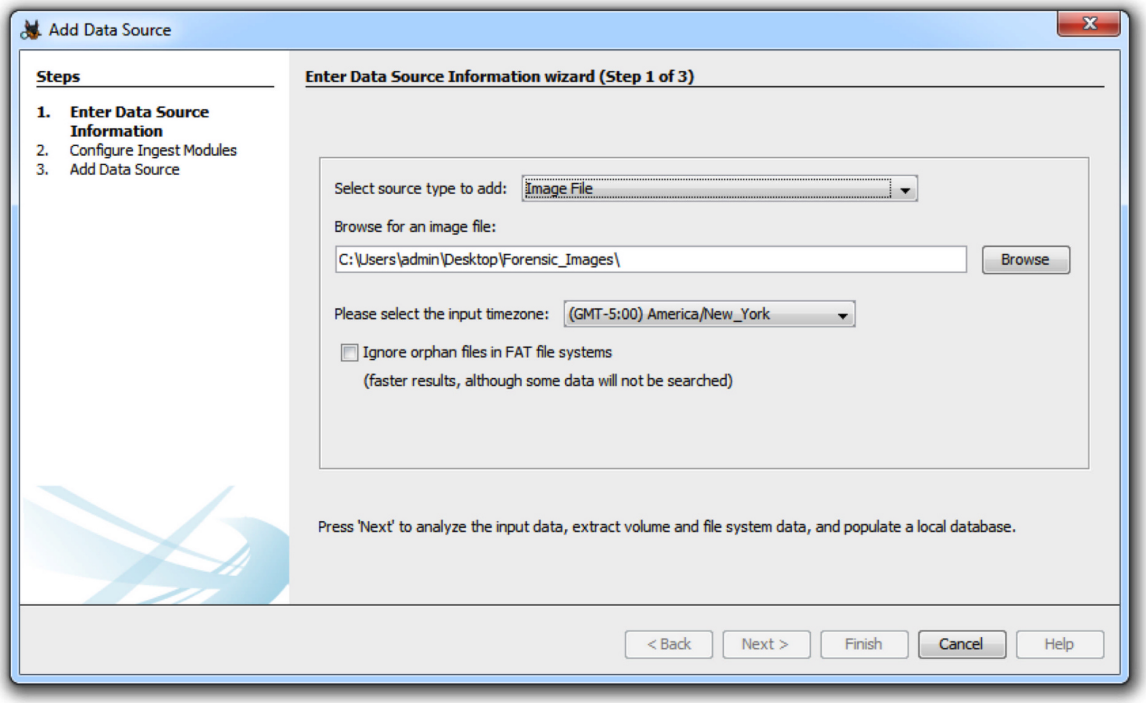
Figure 1: Autopsy's New Case Information window



6. Click the "Finish" button. The "Add Data Source" window will appear. It may take a moment to launch.

8. In the "Add Data Source" window browse to drive2.E01 and click the "Next" button as shown in Figure 2.

Figure 2: Autopsy's Add Data Source window

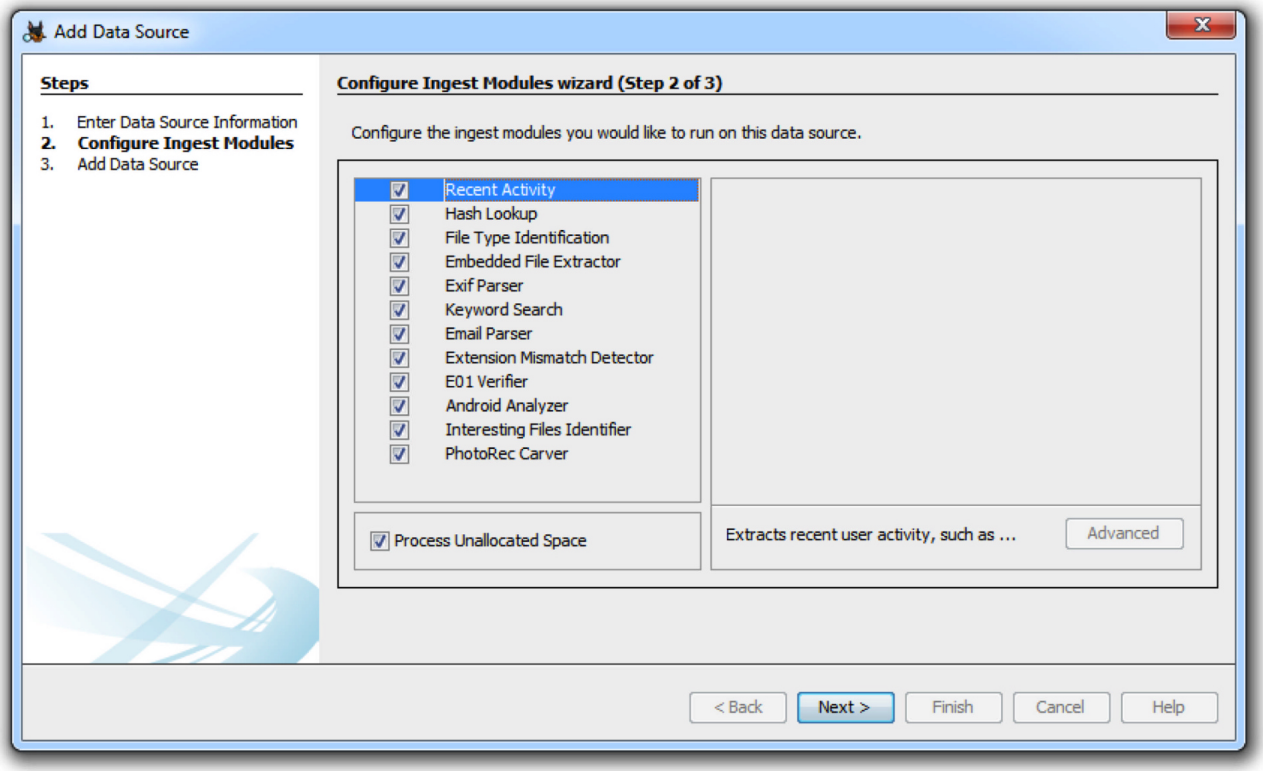


9. The user will be presented with a list of Ingest Modules, which will automatically run once the evidence file is loaded. This is shown in Figure 3. Because this evidence file is small, you can leave the default options selected

and click the “Next” button.

Figure 3: Ingest Modules

10. Click the “Finish” button.

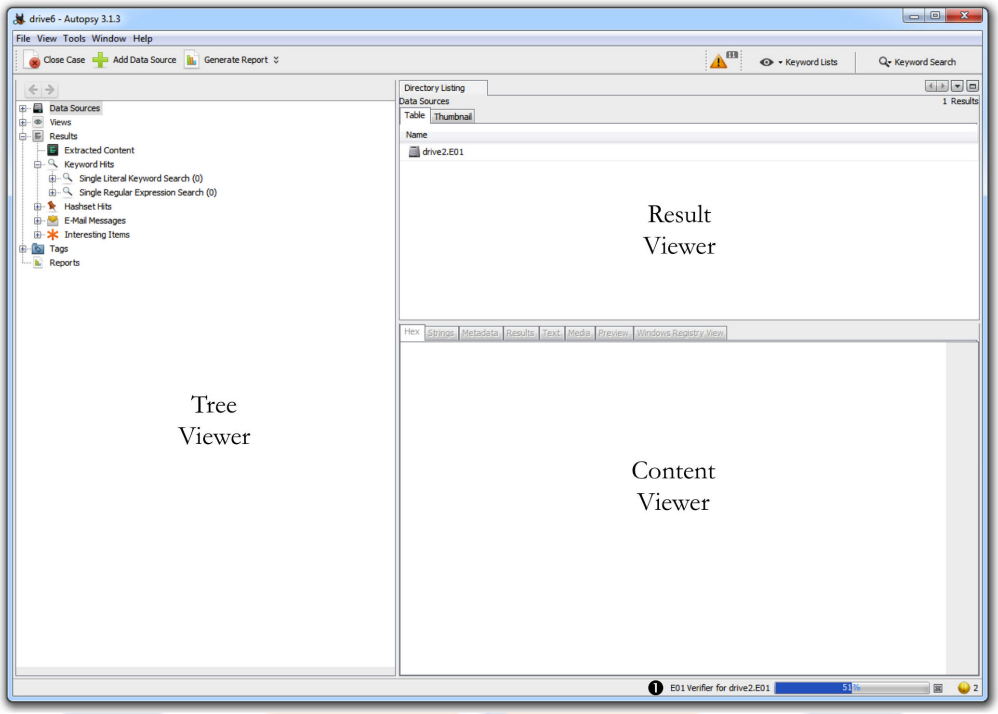
11. 

Autopsy’s

main window is broken up into three panes or viewers: the Tree Viewer, the Result Viewer, and the Content Viewer. The status of the processing of the Ingest Modules! will be displayed in the lower right corner of the window as shown in Figure 4.

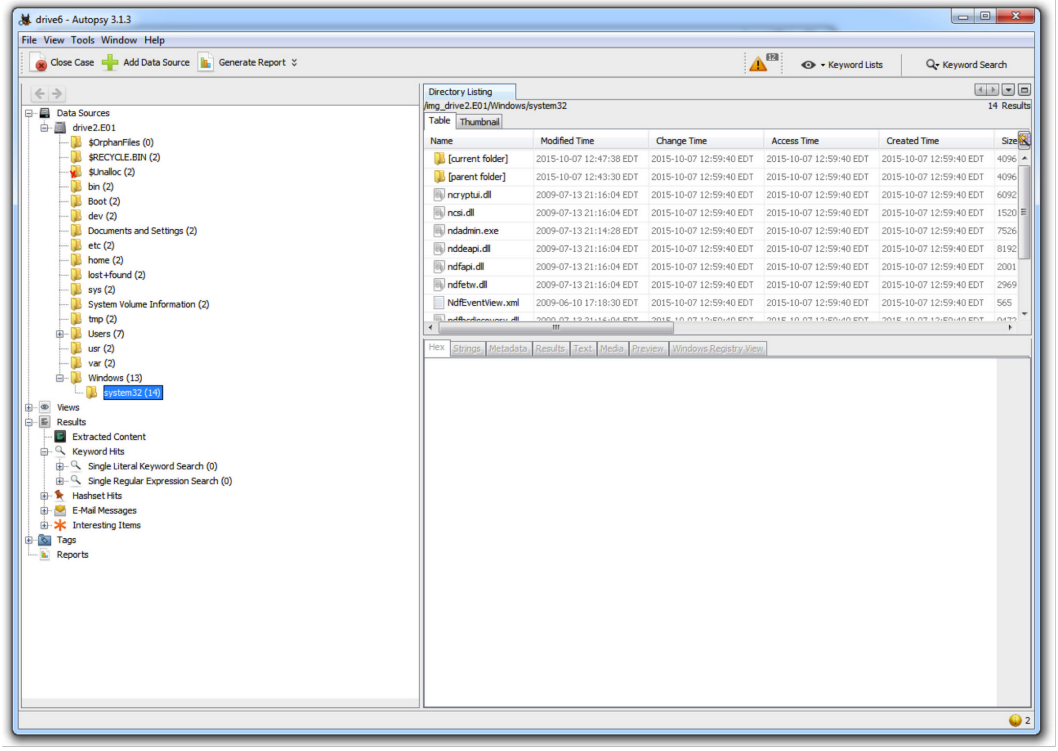
Figure 4: Ingest Module processing status

12. In the Tree Viewer click the plus (+) symbol next to Data Sources and drill down into drive02.E01.



13.Navigate down to C:\Windows\system32 as shown in Figure 5.

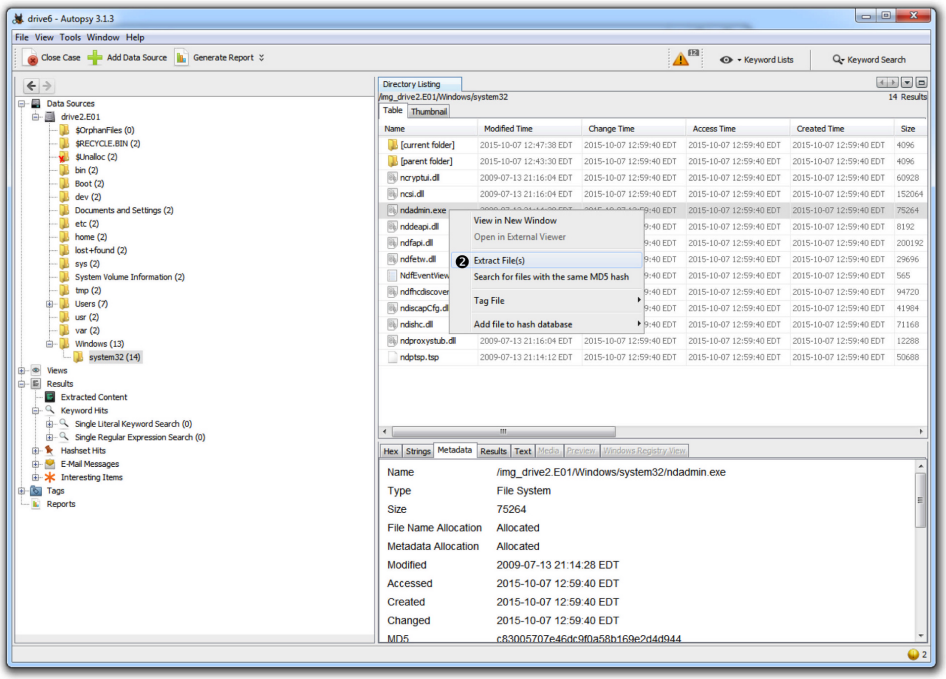
Figure 5: Tree Viewer with file structure of drive02.E01



14. Right-click on the file named nsadmin.exe and select “Extract File(s)”"from the pop-up menu as shown in Figure 6.

Figure 6: “Extract File(s)” feature in Autopsy

15. Identify a location to save the file and click the “Save” button. It is possible to extract



multiple files simultaneously in Autopsy by SHIFT-clicking files and then right-clicking one of the highlighted files. From the pop-up menu choose, “Extract File(s)”#as shown in Fig 7.

Figure 7: Recovering multiple files from an evidence file using Autopsy