This lab is designed to get you started using a forensic analysis tool to verify an image and find items of interest that investigators would want look at as well as verifying the integrity of the image as being original.

**Part 1: Opening the Forensic Image**

Step 1: Using the VM (Virtual Machine), on the Desktop of your VM (Virtual Machine), create a folder called Work Folder. See Figure 1.

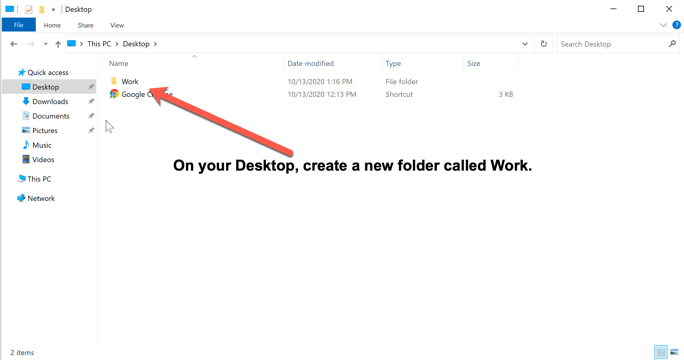


Figure : On Desktop, create a folder called "Work"

Step 2: Launch the Autopsy Forensic tool as shown in Figure 2.

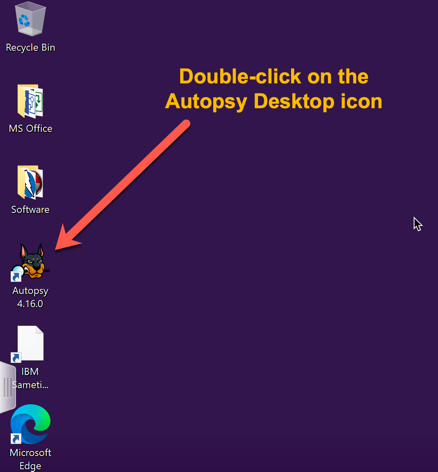


Figure : Launch Autopsy

Step 3: When Autopsy launches, click Create New Case as shown in Figure 3.

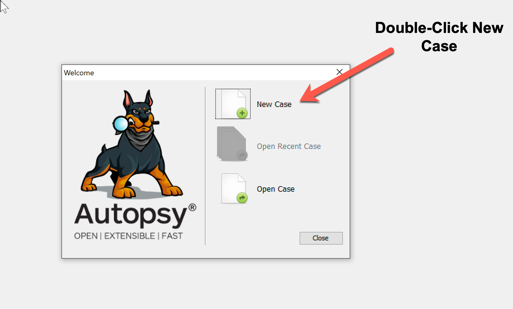


Figure : Open New Case

Step 4: Create a new case with the following case information:

Case Name: Module 6 Lab-LastName (Note: replace “LastName” with your last name)

Base Directory: Set the base directory to the Work Folder created earlier.

Ensure Single User is selected and Click the Next Button. See Figure 4

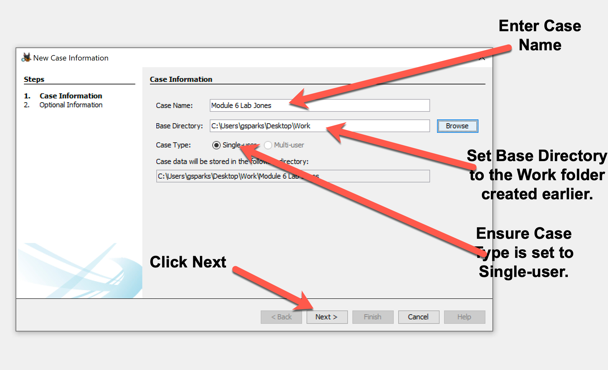


Figure : New Case Wizard

Step 5: Use the following information for the Case step of the wizard.

Number: Enter the case number in the following format year, two-digit month, two-digit day, a dash and 0001. For example, 20200928-0001. Note for each new case on that date, the end number will increment by one, for example 0001, 0002, 0003 etc.

Examiner, enter the following:

Name: Your last name

Email: Your Bellevue email address

Notes: Enter the class number and section number. For example, CYBR 420-320

Leave all other criteria at the default and Click on the Finish Button. See Figure 5.

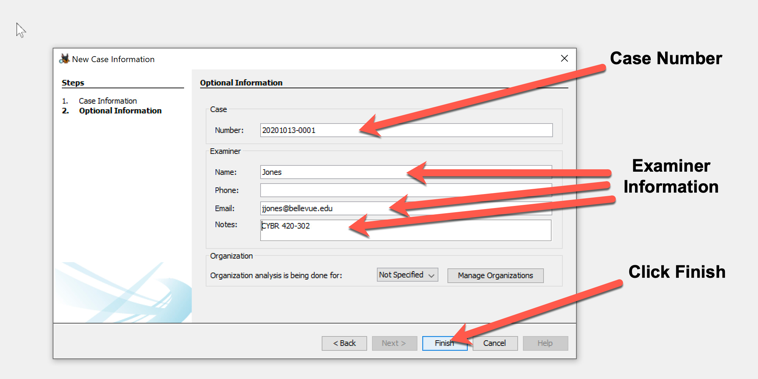


Figure : Case and Examiner Information

Step 7: In the add data source pane, ensure Disk Image or VM file is selected and Click the Next Button as shown in Figure 6.

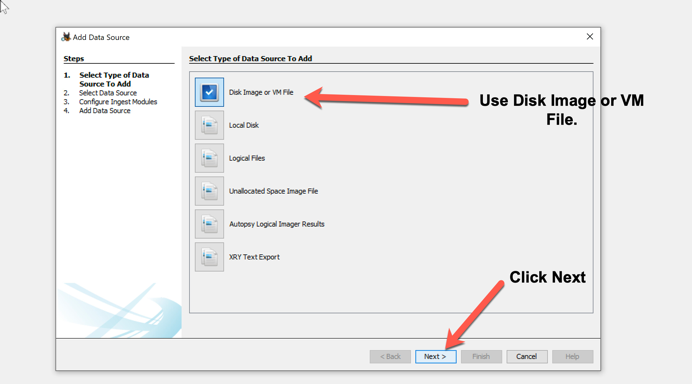


Figure : Image Selection

Step 8: In the next pane, set the Path by navigating to Desktop/Lab Data/Module 6. Select the image “4Dell Latitude Cpi.E01”. Set the Time Zone to “(GMT-6:00) US/Central). Click the Next Button. See Figure 7

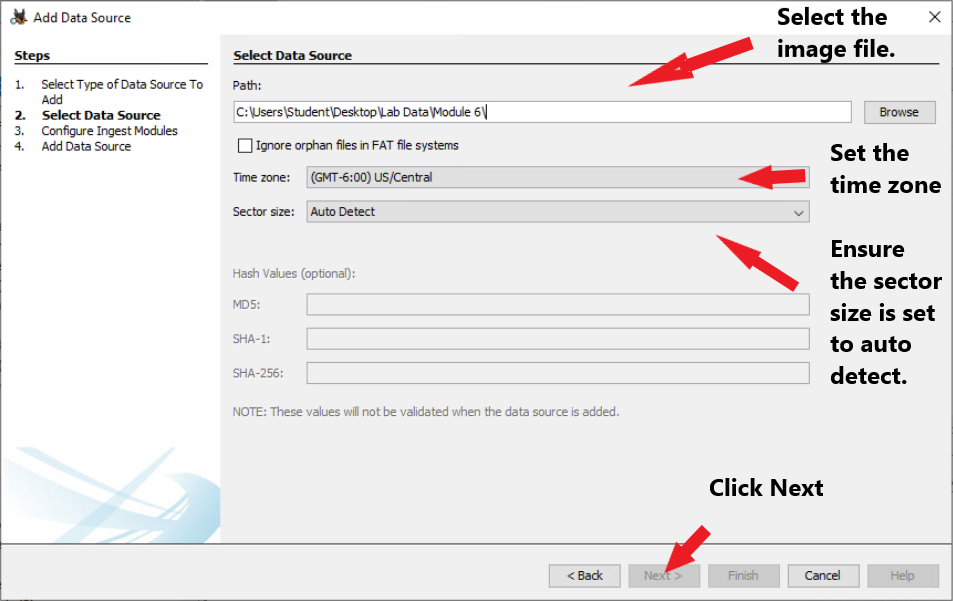


Figure : Image Selection

Step 9: In the Configure Ingest Modules, ensure none of the ingest module are selected by selecting Deselect All as shown in figure 8.

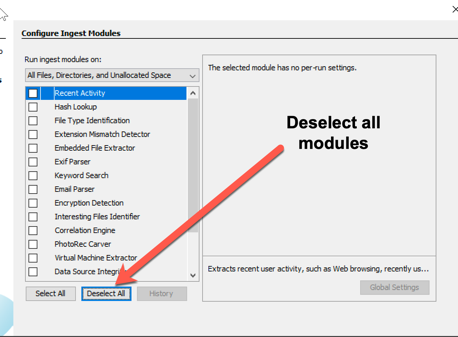


Figure 8: Ingest Modules Deselect

Next select the following inject modules: Recent, Hash Lookup, File Type Identification, Embedded File Extractor, Email Parser, Encryption Detection, Interesting files Identifier and Data Source Integrity as shown in figure 9, then click finish. Note: there are many configuration options to these modules, for this exercise we are using all the defaults.

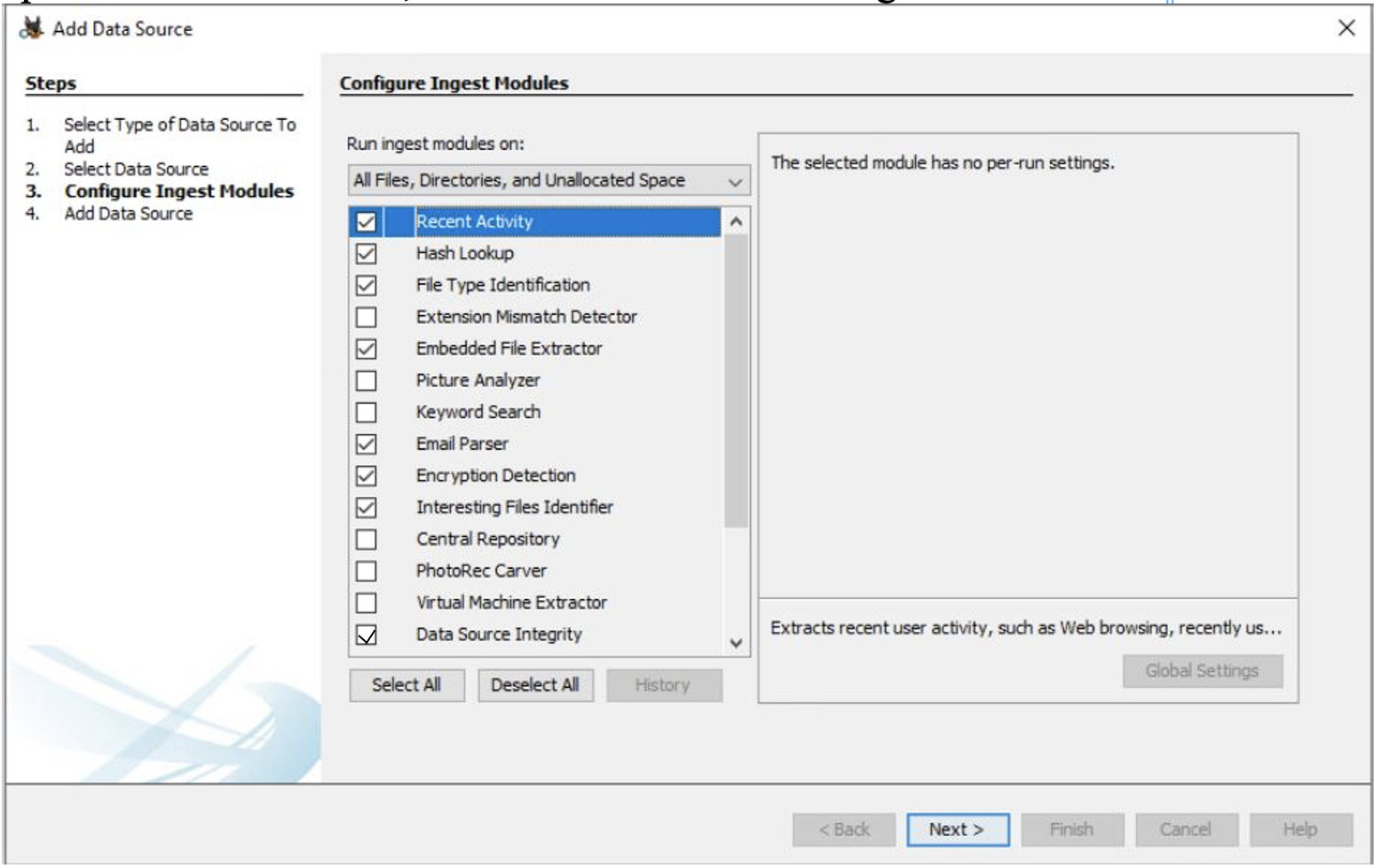


Figure 9: Ingest Modules selection

Step 9: On the final pane, Click Finish as shown in Figure 10. It should take about 5-10 minutes to process the image.

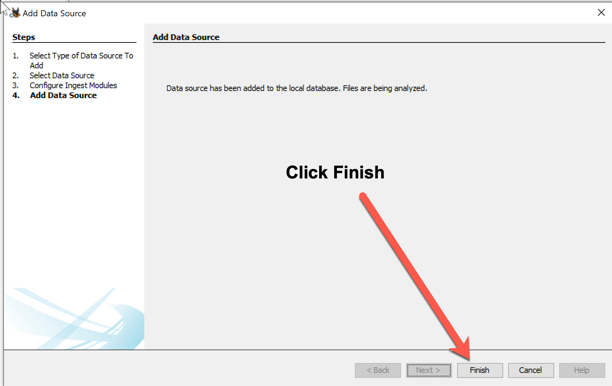


Figure 10: Finish Add Source Wizard

**Part 2: Initial analysis**

Step 1: Expand the Data Source in the Navigation pane. Right Click on the 4Dell Latitude Cpi.E01 and select View Summary Information which will display the Data Source Summary dialog. See Figure 11.

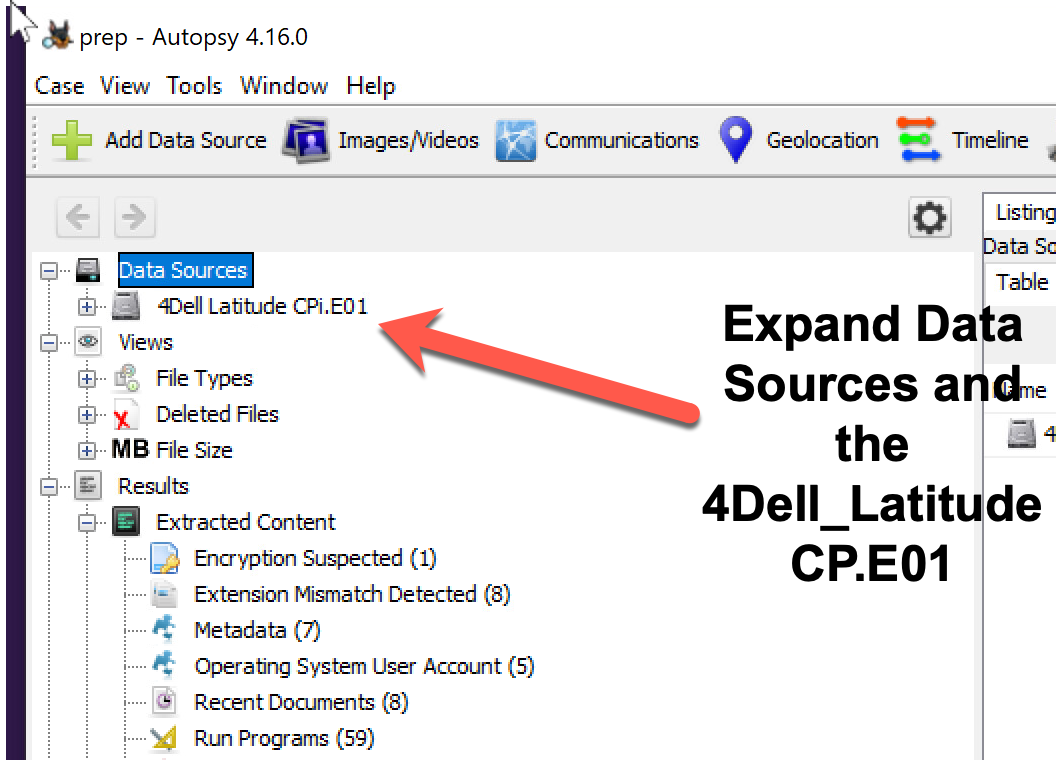


Figure 11: Expand Data Source

Answer the following questions from the Container tab:

1. On what date was this image acquired?

The image was acquired on a Wednesday, Sep 22, 2004, at 09:06:04

1. What is the image type (provide the three character designator)? If you research this you will find it corresponds to the Expert Witness File Format.

The image type is E01

1. What is the sector size?

The sector size is 512 bytes.

1. Paste a screen capture of the hash values below this question.

Graphical user interface, text, application, email

Description automatically generated

Close Data Source Summary.

Using the Directory tree (Figure 12) to answer the following:

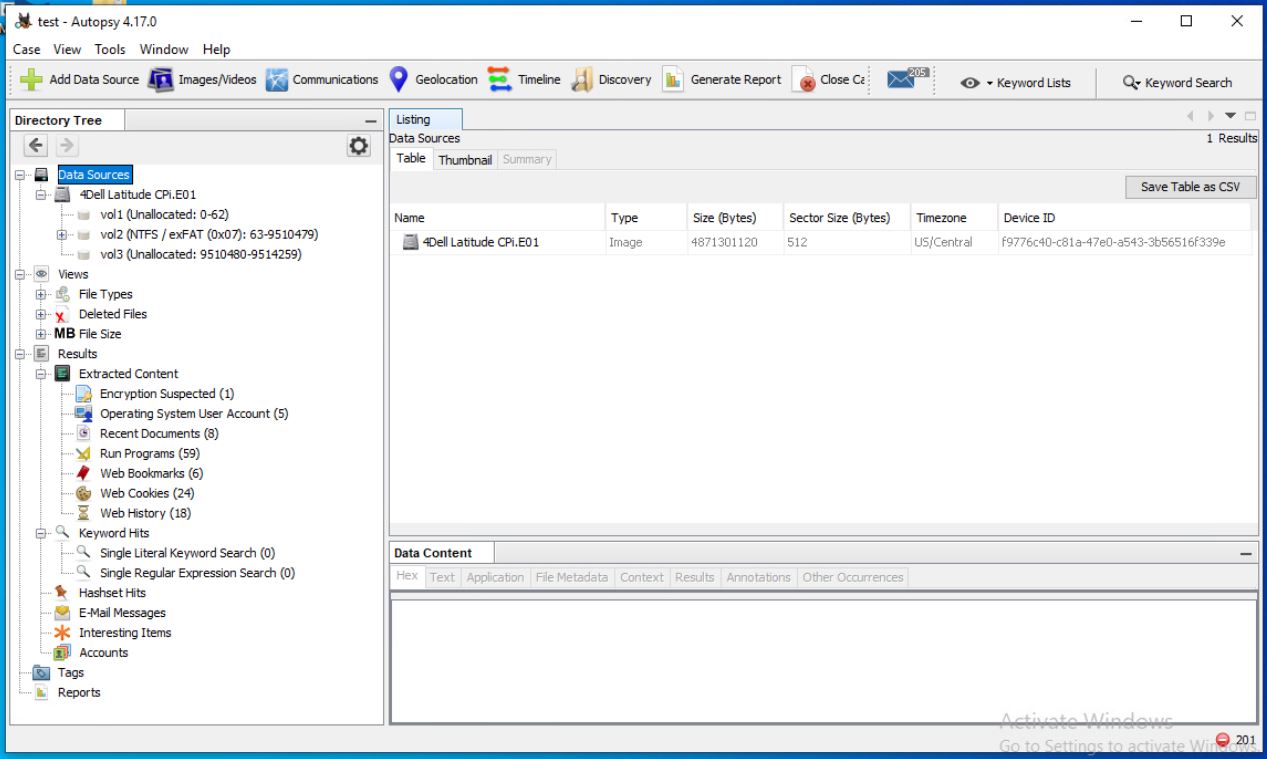


Figure 12: Directory tree

1. How many volumes are in this image?

3 volumes

1. How many user accounts are there?

5 user accounts

1. What is the account type for the user Mr. Evil?

Default Admin User

1. How many image files were found?

977

1. How many files are shown as deleted by the file system?

264

1. Select the ‘Run Programs’ item under extracted content, and find the entry for the program file named ‘CAIN.EXE’ what is the date/time it was last ran?

2004-08-27 10:33:13 CDT

1. Answer the following about Web activity.
   1. How many Web bookmarks were found?

6 bookmarks

* 1. On what date/time was the web cookie for [www.netstumbler.com](http://www.netstumbler.com) created

2004-08-27 10:10:10 CDT

* 1. What browser was used?

Internet Explorer

* 1. What file was downloaded from the netstumbler site?

mr.evil@www.netstumbler[2].txt

* 1. What was the date/time of the download?

2004-08-27 10:10:10 CDT