lab 11

Overview

Welcome! In this guided exercise, we will:

- Launch Autopsy and create a new case.
- Manage case folders.
- Add a piece of evidence to a case.
- Verify the drive image.
- Browse folders and view files in a disk image.
- Conduct a keyword search.

Data Set

We're using a publicly available disk image as part of the data set for this lab. The image is from the Computer Forensic Reference DataSet Portal, or "CFReDS", and can be found at https://cfreds.nist.gov/. These are data sets that can be used for forensic tool testing and training purposes and are free to download. While there are a variety of data sets on this website, we will specifically be using the image available at this link: https://cfreds.nist.gov/all/DFIR_AB/ForensicsImageTestimage

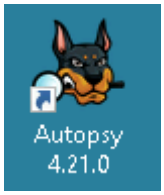
Since these data sets and the tool that we're using are both free, you can download Autopsy and this image and practice at home!

Part 1: Launch Autopsy and Create a New Case

In digital forensics tools, a "case" is a term used to represent a logical grouping of examination tasks. Depending on the tool, having a case is generally required prior to viewing a piece of evidence, and that is true with Autopsy, so the first thing we must do prior to viewing evidence is to create a new case.

1. From the desktop, double-click the Autopsy icon.

   It should look something like the image below, although the version number by the icon may be different.

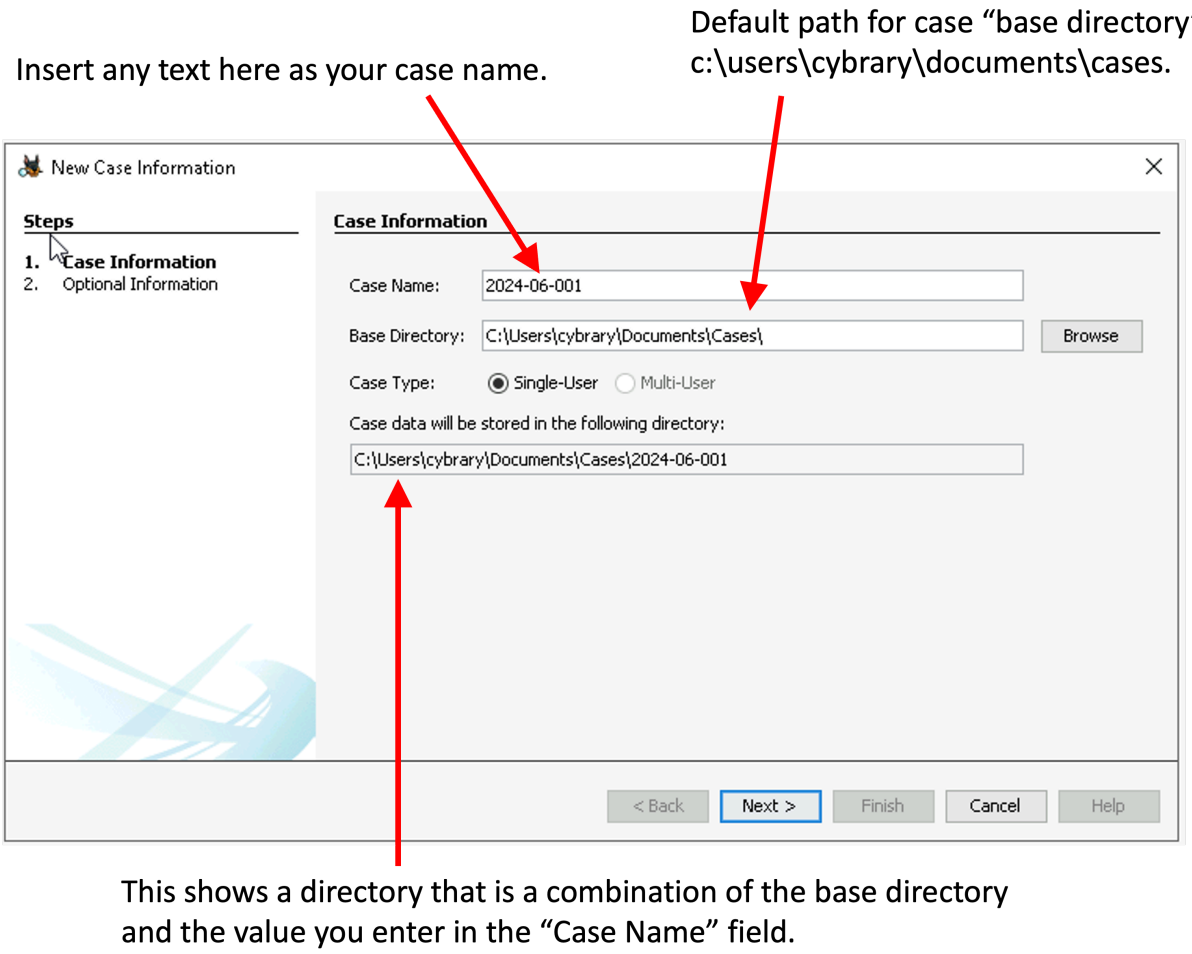
   

- Autopsy will open with a small welcome window that includes options for starting a new case or accessing previous cases.
- In the Welcome window, click the New Case button to open the New Case Information window.

- In the New Case Information window, type 2024-06-001 in the Case Name field, then click Next to continue.

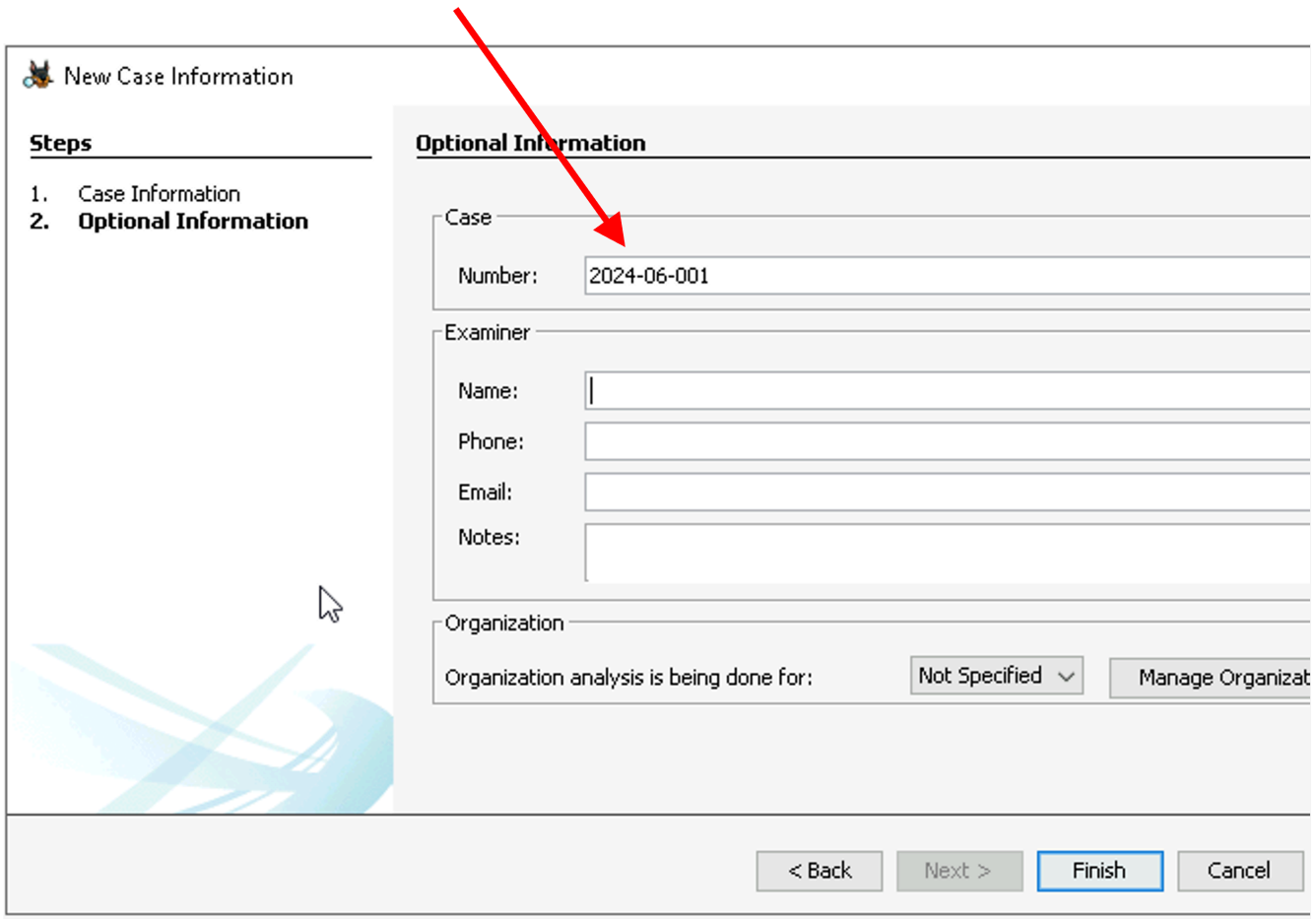
  Note: The case name can be any value that you prefer. In our screenshots, we used a case name that included a year, month, and index number for the case. So in the example, "2024-06-001" represents the first case in June of 2024. On the job, you will use a case naming mechanism that is approved by your organization and defined in their policies and procedures.

  Before proceeding, take note of the full directory created as a combination of the base directory and the case name that you enter. This is where Autopsy will store the settings for your case and other related content. We will leverage this directory later.



- On the Optional Information page, type 001 in the Number field, then click Finish to continue.

  Note: You will notice that, in the screenshot below, we used the same value for the case number as we did for the case name in the previous step. This is a matter of policy at your organization. For this lab you can assign any value for the case number, while the other fields (e.g. Examiner) are entirely optional.

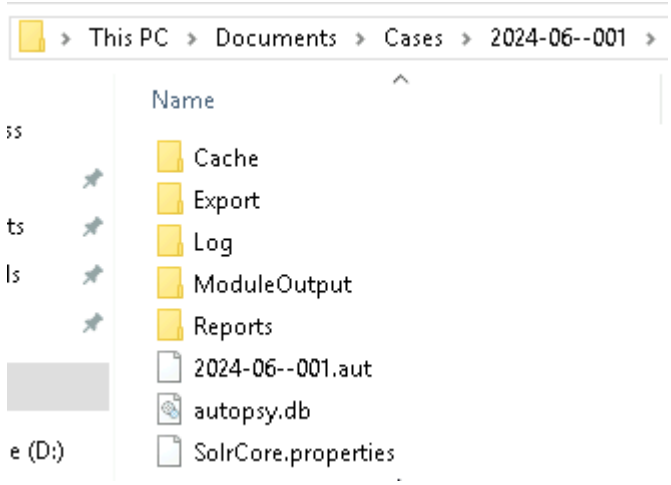


1. Once it has finished creating the new case, Autopsy will open the Add Data Source window.
2. On the Add Data Source page, click Cancel.
   We will add a piece of evidence later.

Part 2: Manage Case Folders

In this part of the lab, we will take a tour of your newly-created case folder.

1. From the Windows taskbar, click the File Explorer icon to open a new File Explorer window.
2. In the File Explorer window, navigate to c:\users\cybrary\documents\cases\2024-06-001.
   You should see the following folders or similar.



3. Note: If you were not able to find this folder, check whether you used a different case name or base cases path in the previous part of this lab.

   The folders you see in the screenshot above are automatically created when you create a new case using Autopsy.Cache: This folder is used for temporary storage by Autopsy. Do not modify the contents of this file at any time.

   Export: When you export contents from an item of evidence (For example exporting a single file from a disk image), this is the default export location where you will find the exported item.Log: This is the folder where Autopsy keeps a log of its operations, should you need to review that log for troubleshooting or audit purposes.

   Module Output: This is the folder for output from add-on modules that can be used with Autopsy.

   Reports: This is the output folder for any reports generated by Autopsy.
4. Create a new subfolder titled Evidence within the 2024-06-001 case folder.
5. Copy the file c:\users\cybrary\downloads\2020JimmyWilson.E01 to the new Evidence folder.

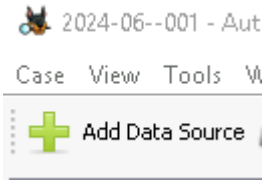
   This is the item of evidence that we will load into our case within Autopsy.

Part 3: Add Evidence to a Case

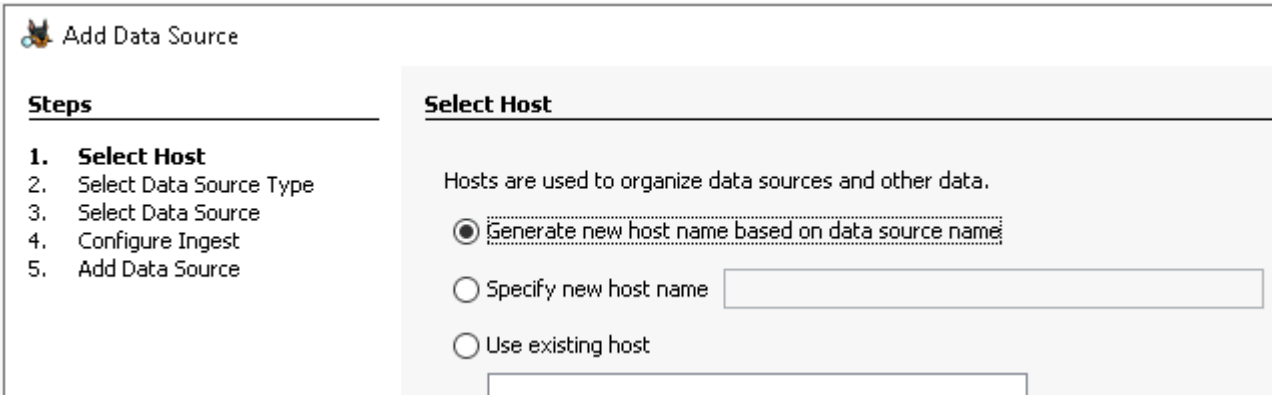
In this part of the lab, we will add an item of evidence to our case.

1. In the Autopsy window, click the Add Data Source button.

   This will open the Add Data Source window, which will walk you through the process of adding data to your case.

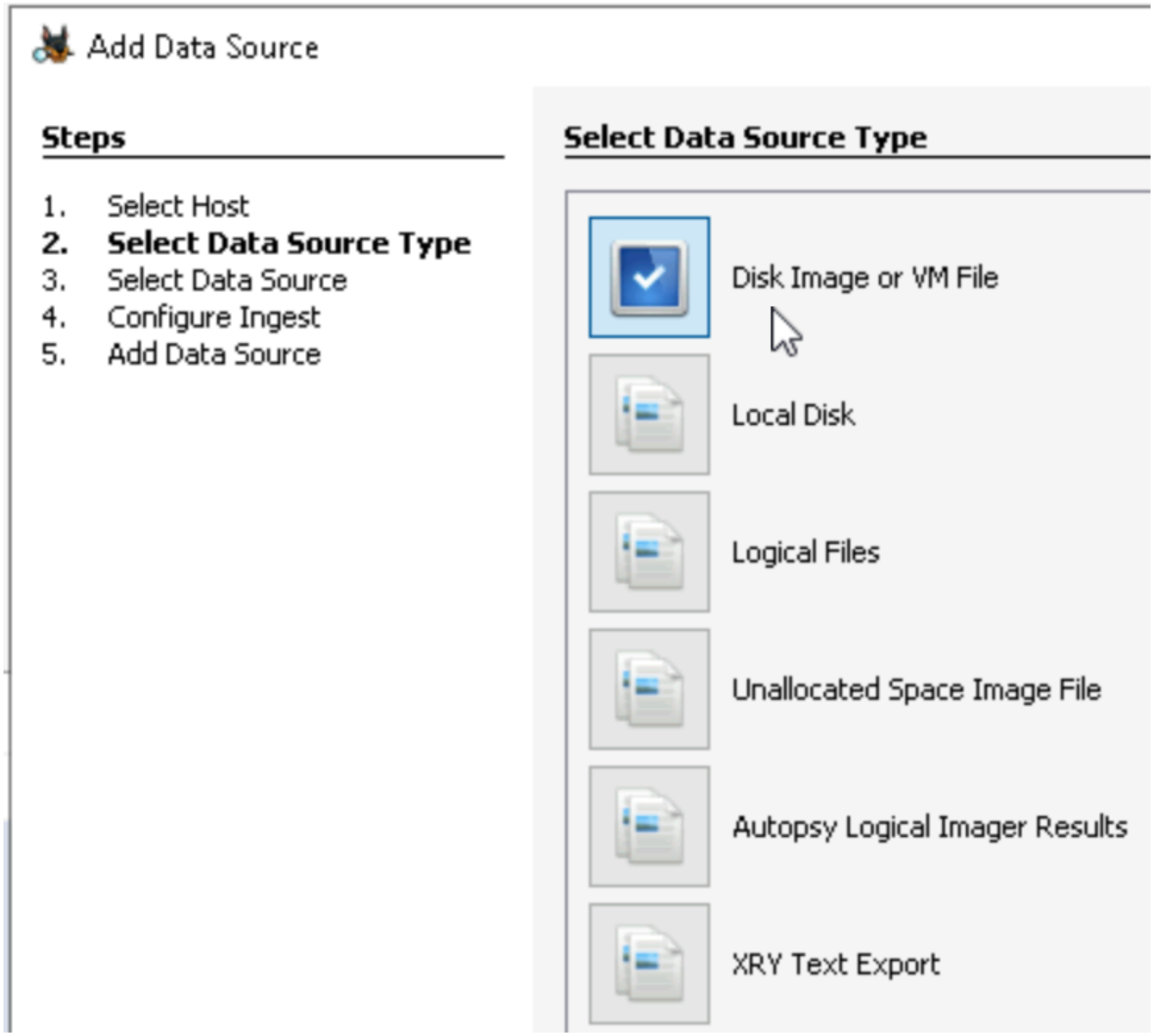


- In the first step, it will ask you if you would like to select or create a name for the "host" from which the piece of evidence was obtained. If you were adding a piece of evidence from a computer with a known host name, you could specify that here.
- On the Select Host page, click Next to accept the default (automatically generate a new host name based on data source name) and continue.



- On the Select Data Source Type page, click Next to accept the default (Disk Image or VM File) and continue.

This tells Autopsy that we will be supplying an image file for a disk or volume.



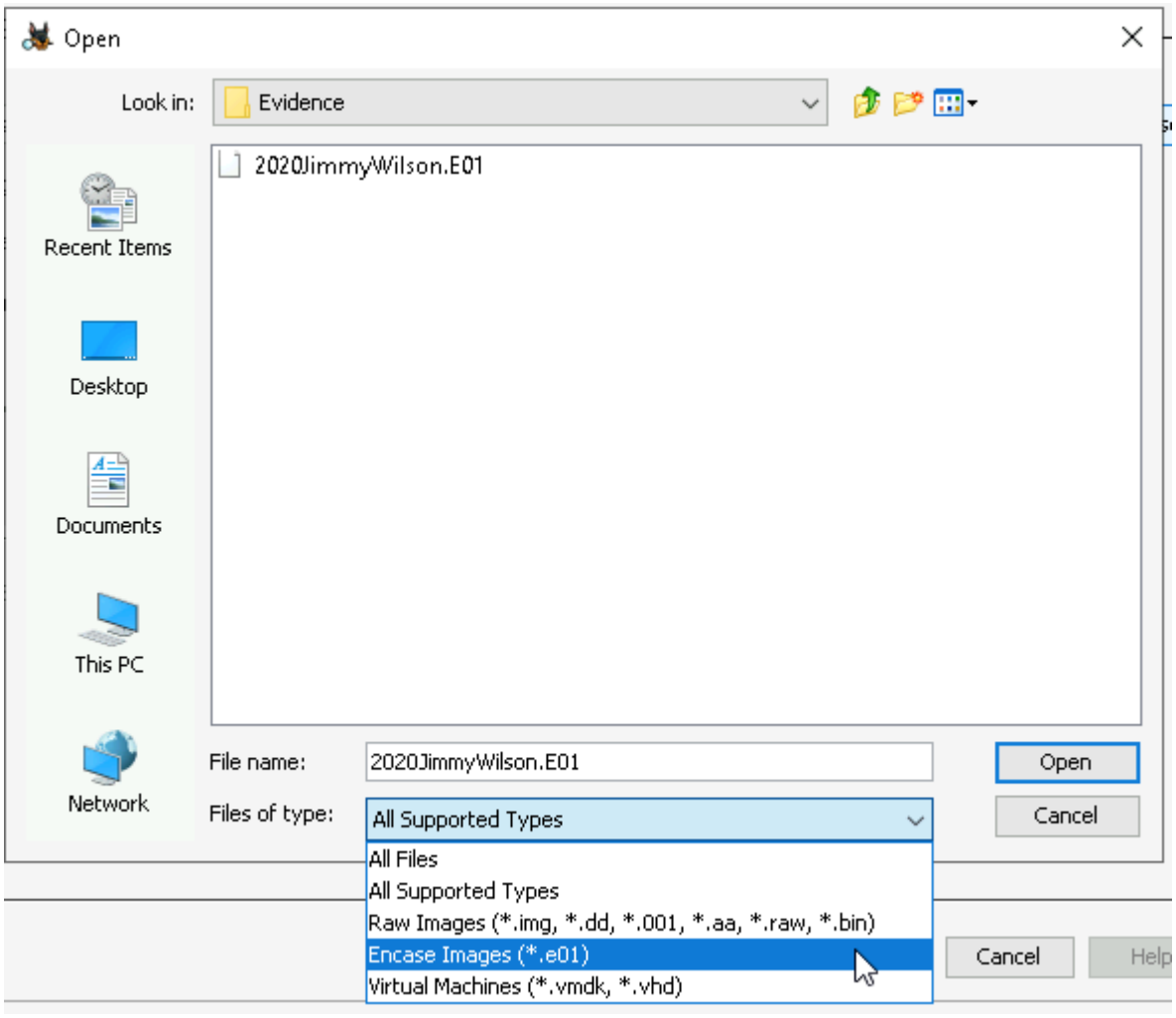
- Note: Review the other options here. While we are not selecting any of these other options at this time, they are worth mentioning now:Local Disk: This option would enable you to access and view a local disk with Autopsy. Selecting this option requires you to launch Autopsy with administrative privileges.

  Logical Files: This is an option to load one or more individual files. These would be files that were acquired individually or as a set, rather than within an image file.

  Unallocated Space Image File: This is an option to load an image file that only contains unallocated space.

  Autopsy Logical Imager Results: This is an option to load data that was acquired using Autopsy itself.

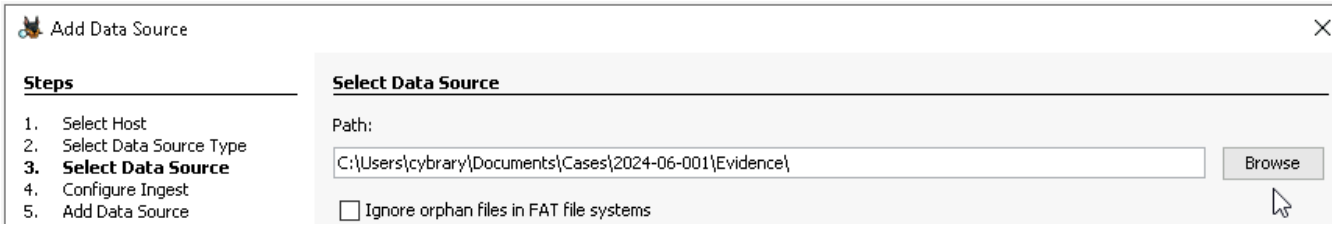
  Additional information regarding different types of data acquisition will be supplied in other modules in this Skill Path.
- On the Select Data Source page, click the Browse button, then select the 2020JimmyWilson.E01 file and click Open to specify the item of evidence to be added.



- Note: You may notice that there are multiple options in the Open window for "Files of type", which would enable you to specify the type of image file that you are adding. While not strictly necessary, you could select "Encase Images (*.e01)" as the type of file you are adding. This is a type of image file created by the original vendor for the EnCase digital forensics software. EnCase is a commercial product that performs a similar function to Autopsy. Autopsy supports the processing of image files created in this format.

  There is also an option here for choosing time zone. However, you do not yet know the time zone in which the item of evidence was configured. In general, and if you do not have a reason to set a specific time zone, it is a best practice to leave the time zone configured as GMT.

- On the Select Data Source page, click Next to continue.



- On the Configure Ingest page, confirm that only the following options are checked, then click Next to continue.

  Hash Lookup: While we're not actually performing any hash lookups in this introductory lab, this will still cause Autopsy to create a hash value for each file, which may be useful later.

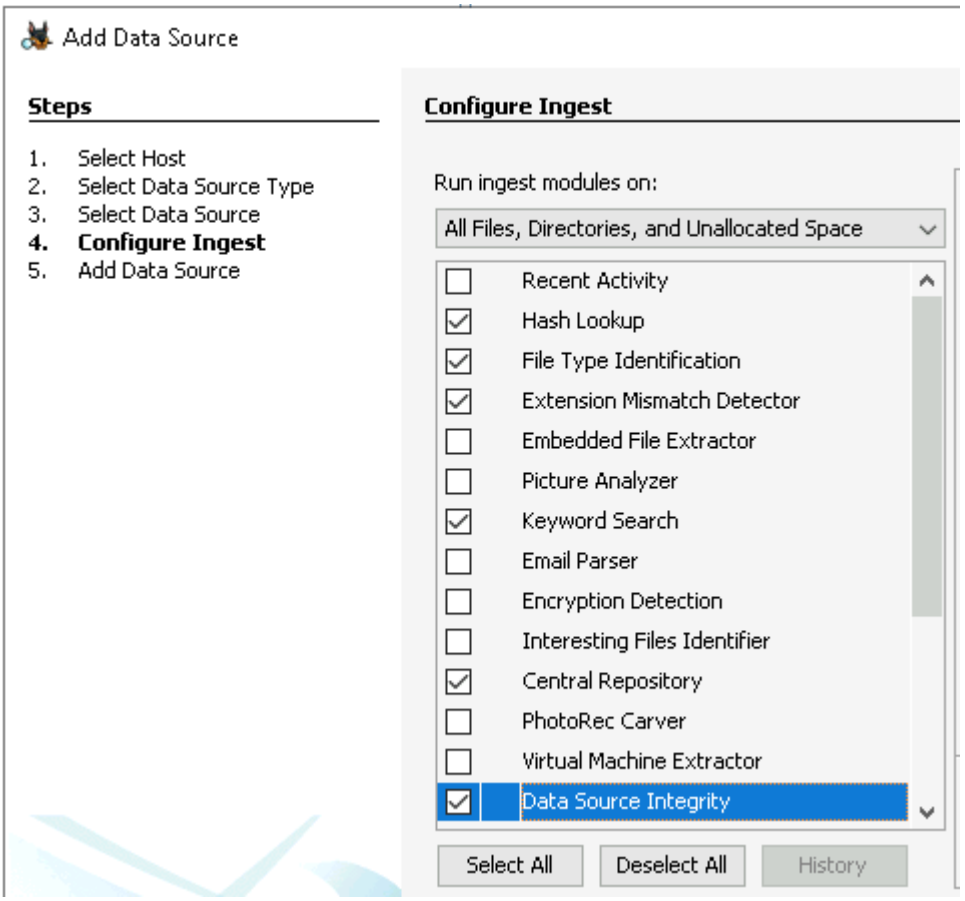
  File Type Identification: Basic identification of file type for each file based upon the file signature found within the file (not the file extension).

Extension Mismatch Detector: Checks for mismatches between the aforementioned file signature and the file extension.

Keyword Search: Can be used to search for keywords during the ingest of the new data source. It will also index content of an image to enable subsequent keyword searches to occur more rapidly.

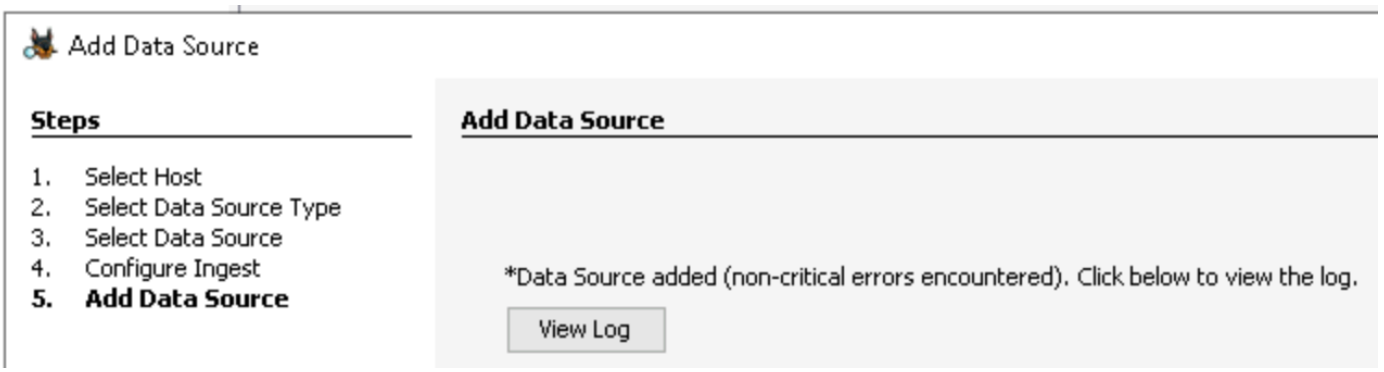
Central Repository: Stores results of other steps in a central repository for later usage.

Data Source Integrity: This will calculate a hash value for the item being added and verify that it matches the expected hash.



Note: After clicking Next, you will see a progress bar while the item is processed in accordance with the options selected. While that runs, the Finish button will be greyed out. You will need to wait until this process completes before continuing.

You may observe a message about "non-critical errors". You can safely ignore this for the purposes of this lab.



- Click Finish to complete the ingestion process.

Note: Even when the Finish button becomes accessible, additional operations may still be underway. The reason for this is that Autopsy enables you to complete the process of adding a data source and begin browsing that source while some of the more lengthy analysis operations are still in progress.

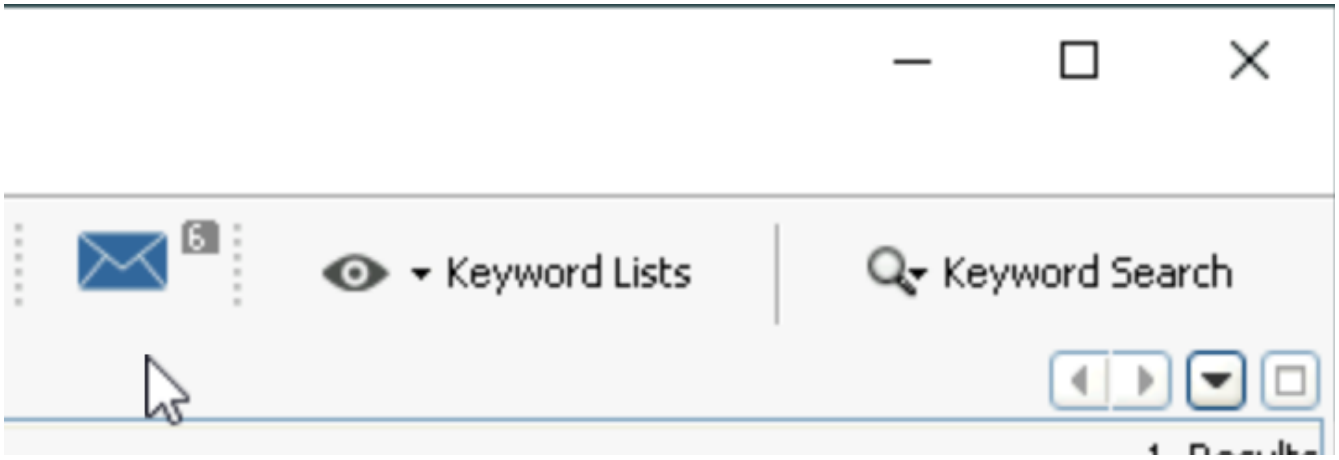
For this relatively small item of evidence, and the small number of processing options that we selected in the previous step, these additional operations will complete quickly. For larger items of evidence and/or with more expansive processing options, this will take longer. The progress bar for these "background" processing steps is in the bottom right of the window. The following screenshot shows an example of what you might see.

Note: You will need to wait for these background processing steps to conclude before continuing to Part 4.

Part 4: Verify the Drive Image

Whenever we make a copy of an item of evidence, it is best practice to verify that the copy is an exact duplicate. This is done by checking the hash value of the new copy. Autopsy can do this for us when the item is added, and we instructed it to do so earlier when we selected the Data Source Integrity option on the Configure Ingest page.

1. In the top-right corner, click the letter icon to display the output messages from certain supplementary processing modules



2. Note: The small number next to the letter icon in the screenshot above is a hint that there is output to view.

   A new window will open showing a small table.

3. In the new window, check for a message that states Integrity of 2020JimmyWilson.E01 verified.

   If you see that message, this means that the hash value of the item of evidence matched the expected value based on the results of the Data Source Integrity module option that you selected when adding the data source.

4. Close the Hash Integrity window.

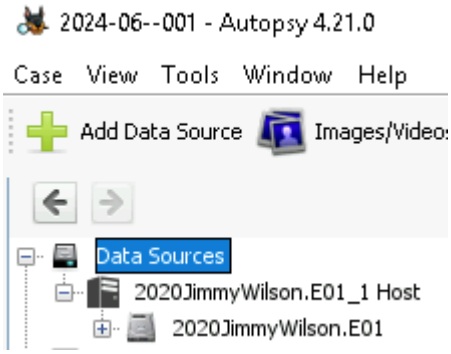
Part 5: Browse Folders and View Files in a Disk Image

In this part of the lab, we will take a quick tour through some elements of the Autopsy UI.

Like all tools of this type, Autopsy is a complicated application with a variety of features and options. This is only an introductory tour. You will be introduced to additional aspects of this application in other labs in this skill path.

We will begin exploring the newly-added data source. To access the data source, we will use the file system navigation pane on the left side of the Autopsy UI. This pane is referred to as the Tree Viewer.

1. In the Tree Viewer, expand the Data Sources node, then expand the 2020JimmyWilson.E01_1 Host node to view the item of evidence.



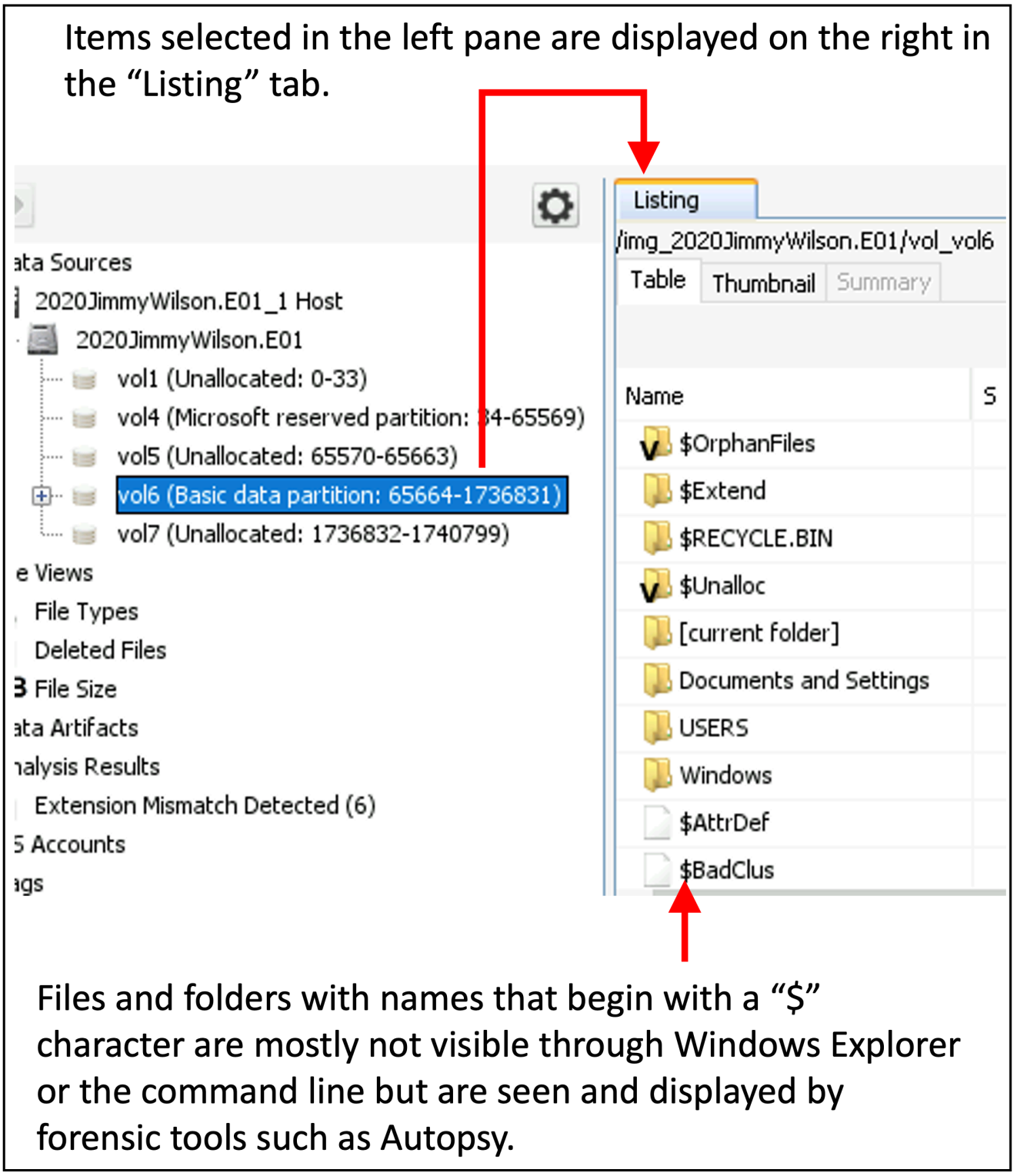
- In the Tree Viewer, expand the 2020JimmyWilson.E01 node to reveal the volumes contained within that drive image.

  Take note of the number of volumes listed. You will need this information to answer one of the questions on the Tasks tab.

  Notice that of the volumes listed, only one has a "+" character, indicating that Autopsy has only discovered contents within that one volume.

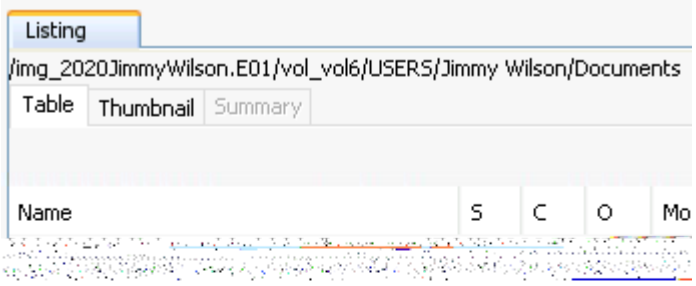
- In the Tree Viewer, click the vol6 node to display its contents in the Listing tab of the Result Viewer pane on the right.

  You should observe both recognizable Window folders such as "USERS", as well as other structures that you may not recognize, such as "$Extend". Some of the files and folders that you do not recognize will be covered in other labs in this skill path.



- In the Result Viewer, navigate to USERS/Jimmy Wilson/Documents.

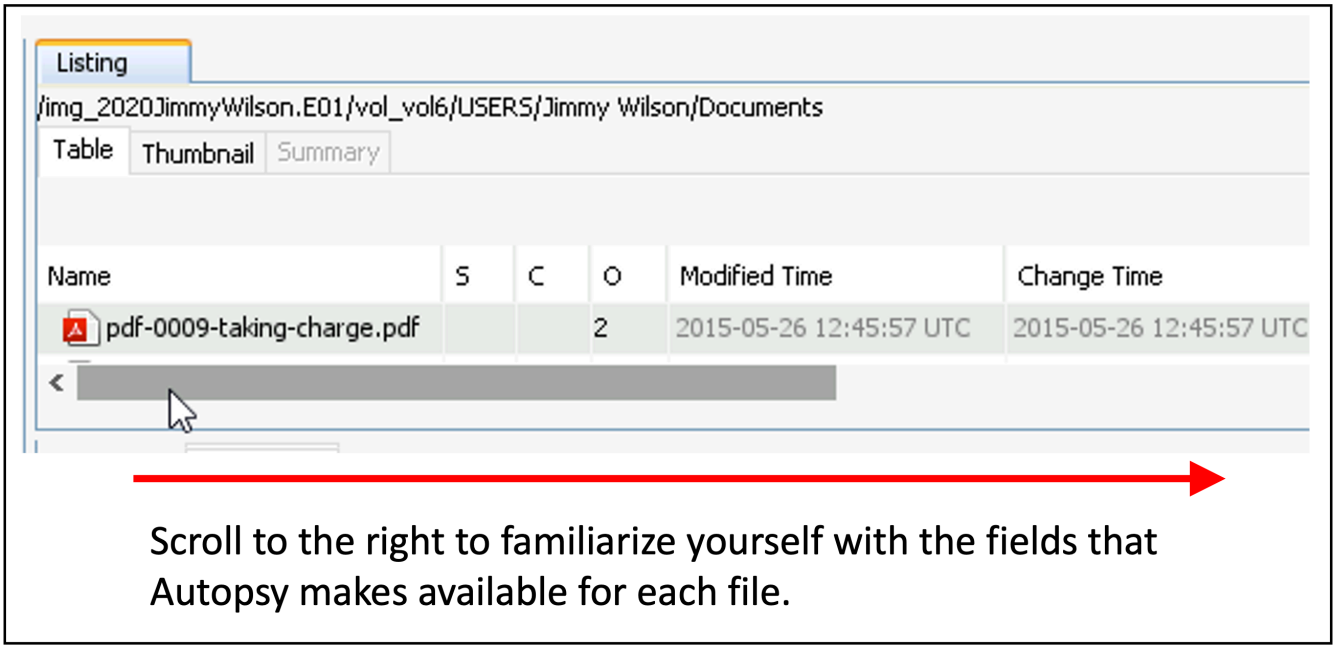
  You should see a similar listing to the screenshot below.



- In the Result Viewer, select the pdf-0009-taking-charge.pdf file.

  Autopsy provides data regarding each file in the table in the Result pane. Scroll to the right and observe the available fields. You should see fields that include the standard date/time stamps* associated with files on Windows, file size, file hashes (MD5, SHA256), file type, extension and a few others.

  Take note of the date/time stamps for this file. You will need this information to answer one of the questions on the Tasks tab.



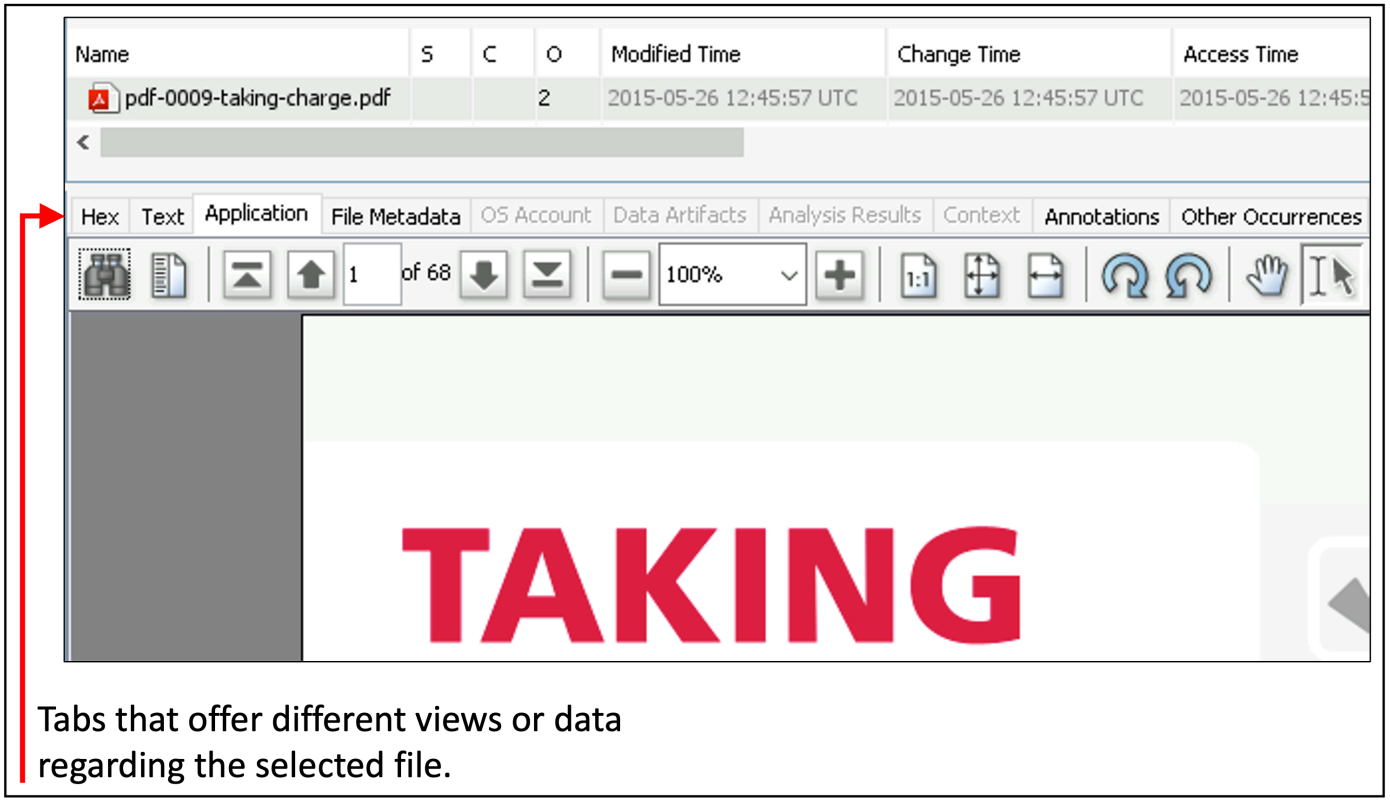
Now direct your attention to the pane at the bottom of the screen. This is the Content Viewer pane and it includes multiple tabs. When you selected the PDF, Autopsy should have attempted to render the PDF for you to view in the Application tab. Here are some of the tabs you will notice.Hex: Raw content of the selected file in hex format similar to the view of a hex editor.

Text: A sequential dump of text strings found in the selected file.

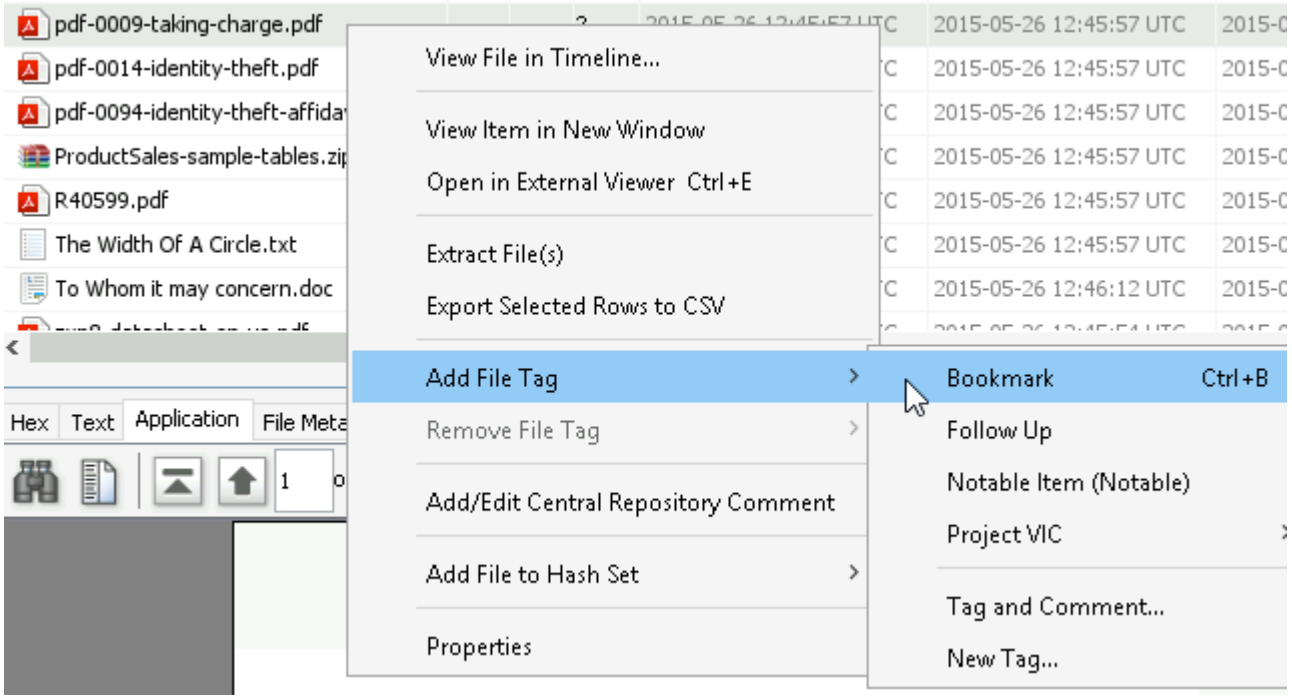
Application: Rendering of the file by an application that is capable of rendering the file format. Note that Autopsy will not have a viable viewer for every file type, so expect that this tab may not provide useful content in all circumstances.

File Metadata: File system metadata about the selected file, i.e. metadata from the file system record - not from within the file itself.

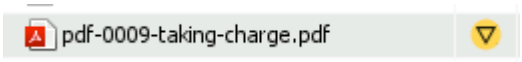
Annotations: A place for you to take notes about the selected file within Autopsy.



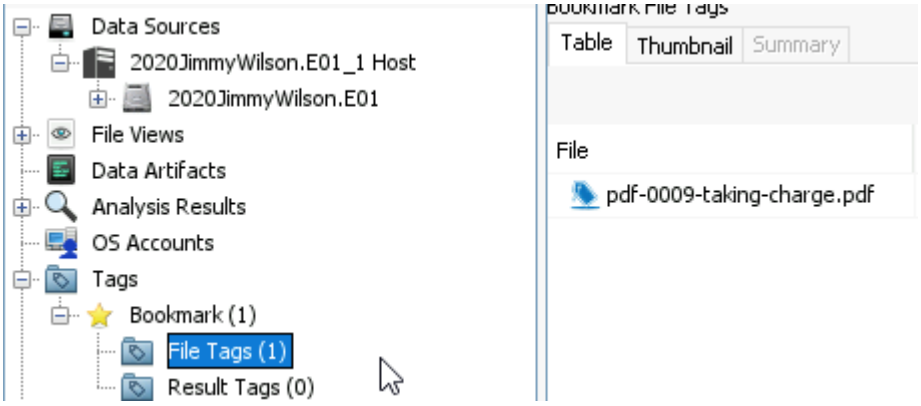
- You can also bookmark files to remind yourself to review them again later. This is an exceptionally useful feature that can help you keep track of what can become a large number of files of potential interest in a given investigation.
- In the Result Viewer, right-click the pdf-0009-taking-charge.pdf file and select Add File Tag > Bookmark from the context menu.



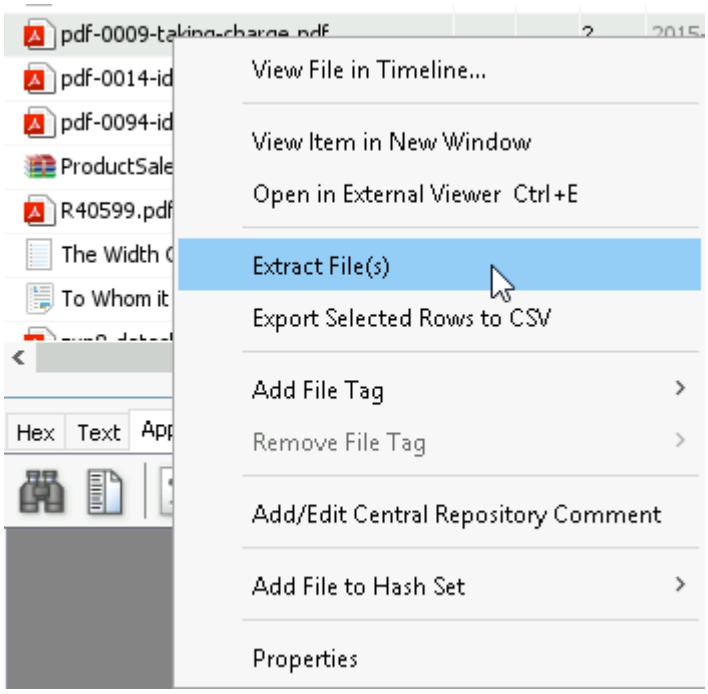
Note: When you perform this action, a small symbol will appear next to the file name indicating that it has been bookmarked, as shown below.



Note: You will also see the bookmarked item under the Tags folder in the left pane of Autopsy as shown below.



- You can also extract a file from the image using Autopsy.
- In the Result Viewer, right-click the pdf-0009-taking-charge.pdf file and select Extract File(s) from the context menu.



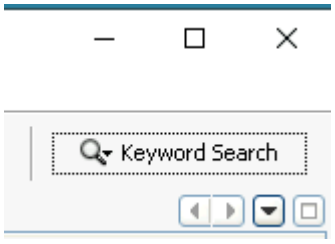
2. In the Save window, click the Save button to continue.
   When completed, a copy of the file should be in the Export folder for this case. You can check to see if it is there.

   When you export or extract a file from a disk image or other logical evidence container, your local AV or EDR will typically scan that file. If you are exporting something that is or suspected to be a malware sample, that may result in the sample being quarantined. If you will commonly be extracting potential malware samples from images, you will need to develop a process by which you can get files out safely and transfer them safely to whomever needs to receive them. We do not recommend turning AV off on your exam systems.
3. When prompted, click OK to close the confirmation dialog box.

Part 6: Conduct a Keyword Search

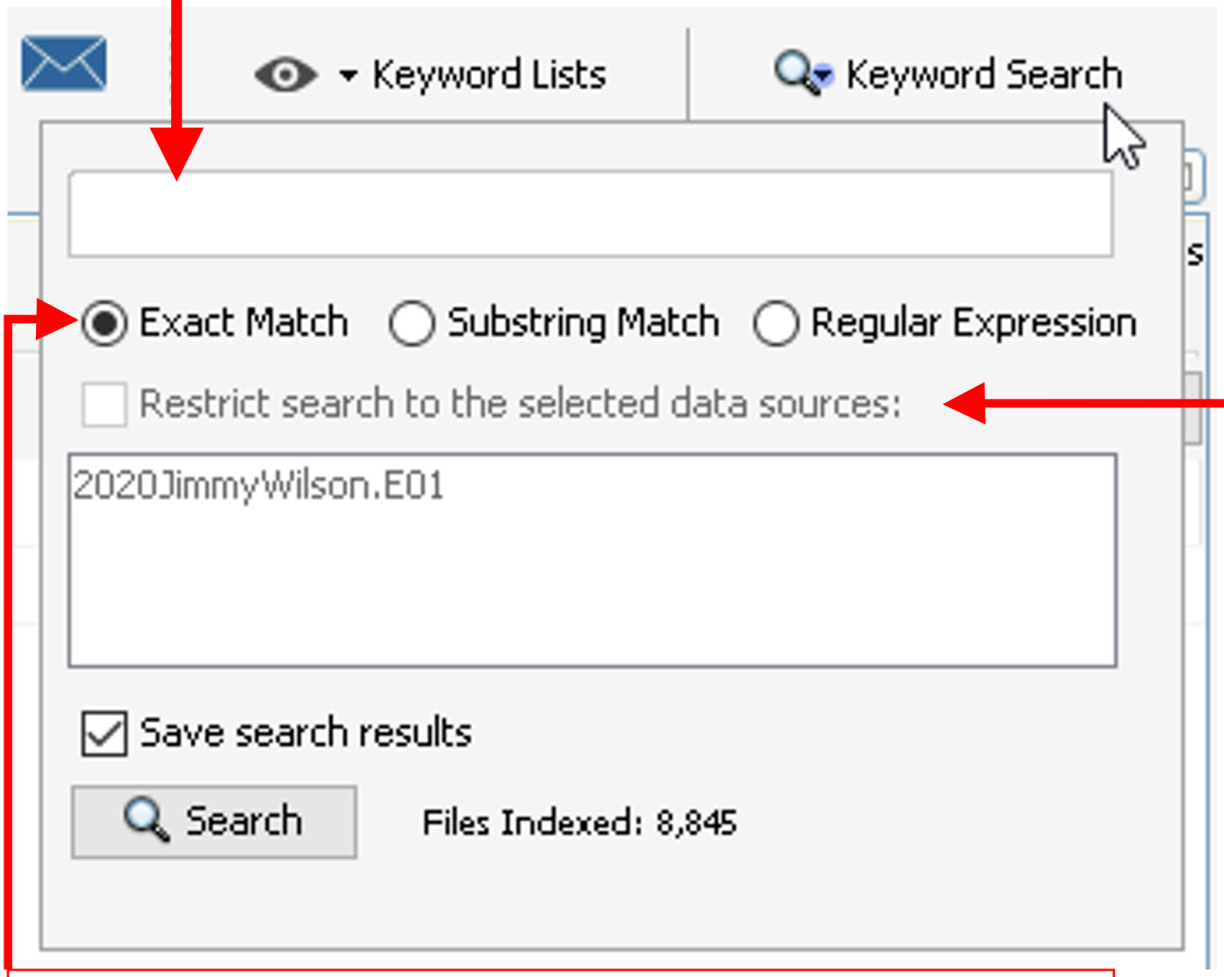
A keyword search is one of the more common analysis capabilities of any digital forensics tool. In its simplest form, this is just a search for a single term. More complex keyword searches can leverage lists of terms and regular expressions. In this part of the lab, we will conduct a simple keyword search to demonstrate how it can be done with Autopsy.

1. In the upper-right corner, click the Keyword Search button.



The search dialog will open. Familiarize yourself with the options.

You can enter a single search term in this field.

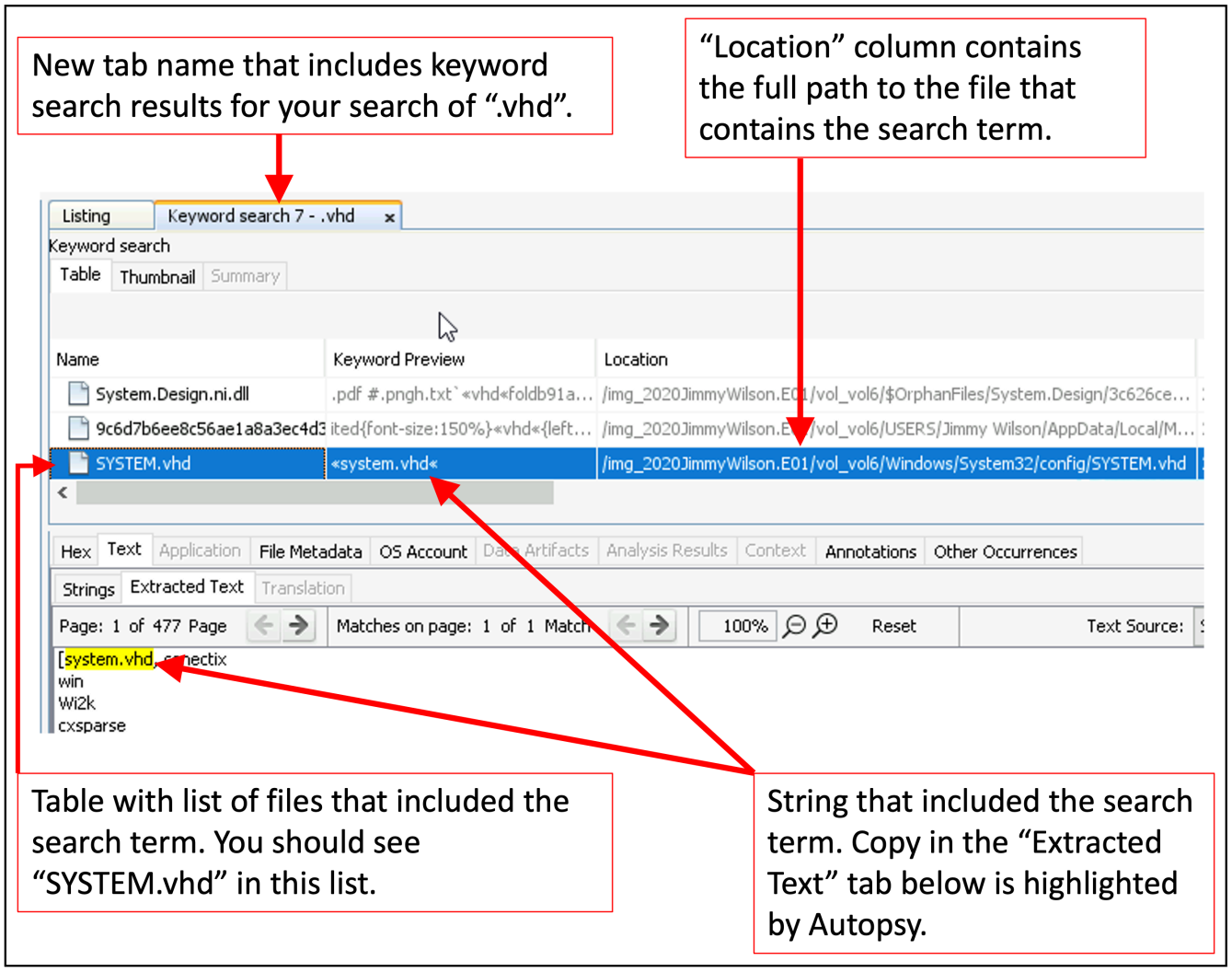


Basic search options. Use “Exact Match” for fewer results, “Substring Match” for more results, and “Regular Expression” if you would like to use an expression to search for a range of values.

Use this option if you would like to search only one item of evidence. Useful if more than one image is loaded in a single case.

- Our item of evidence contains a virtual machine disk file in a .vhd format buried in a directory where we would not expect to find such a file. We're going to use a keyword search to find it.
- In the Search dialog box, type .vhd in the search field and click the Substring Match radio button, then click the Search button.

  It may take a moment for your search to complete. When it does, a new tab will open in the Result Viewer next to the Listing tab. This new tab will contain your search results.
- In the Result Viewer, scroll down until you find the file named SYSTEM.vhd.



1. Take note of the date/time stamps for this file. You will need this information to answer one of the questions on the Tasks tab.

   Notice the full path to this file. While we will not pursue this element further in this lab, here is a question for you to consider after the course: Why would someone store a virtual disk file in a subfolder of the system root?

Task

Part 1:

1. How many volumes were visible in the disk image that you added to the case?

2. What is the Created Time value for the pdf-0009-taking-charge.pdf file?

3. What is the Created Time value for the system.vhd file?

Part 1:

This challenge will start with the same disk image that we viewed in the previous lesson, but with a twist.

- Create a case in Autopsy and load the 2020JimmyWilson.E01 image as you did in the previous lab.
- Inside this image, there is a virtual disk named "system.vhd" hidden in c:\windows\sytem32\config. Find the system.vhd file and extract it.
- Load system.vhd as another data source, then use the content of that image to answer the questions on the Tasks tab.

1. Which volume in the system.vhd image contains a folder named TrueCrypt in the root of the volume?

2. Which volume contains images of credit card and ATM skimmers? (You can find this by simply browsing or by using keyword searches. We encourage you to try both.)

3. Many of the images of ATM and credit card skimmers show a domain name overlaid on some of the images. What is that domain?