Hands-On Lab: Image Analysis Using Autopsy

To accompany Whitman and Mattord, Principles of Information Security, 7th Ed., 2022, ISBN 9780357506431; Image Analysis Using Autopsy

Table of Contents

[Introduction 2](#_Toc76728825)

[Objective 2](#_Toc76728826)

[Estimated Completion Time 2](#_Toc76728827)

[Materials Required 2](#_Toc76728828)

[Image Analysis Using Autopsy 2](#_Toc76728829)

[Downloading and Installing Autopsy 2](#_Toc76728830)

[Importing a Suspect Image File Using Autopsy 3](#_Toc76728831)

[Examining the Suspect Image File Using Autopsy 6](#_Toc76728832)

[Self-Reflection and Response 12](#_Toc76728833)

[Instructor’s Response 12](#_Toc76728834)

# Introduction

In this project, you will use Autopsy, the open-source digital forensics analysis tool ([www.autopsy.com](http://www.autopsy.com/)). Autopsy includes case management features, supports various types of file analysis, and allows searching and sorting of allocated, unallocated, and hidden files. Autopsy is a GUI front end for The Sleuth Kit, which is available at <https://sourceforge.net/projects/sleuthkit>. You do not need to download The Sleuth Kit separately.

For more information on Autopsy, you can go to <https://hub.packtpub.com/digital-forensics-using-autopsy/>.

## Objective

Upon completion of this activity, you will be able to perform basic drive image analysis using the Autopsy software package.

## Estimated Completion Time

If you are prepared, you should be able to complete this lab in 45 to 70 minutes.

## Materials Required

Completion of this lab requires the following software to be installed and configured on your workstation:

* Microsoft Windows 10, or another operating system version as specified by the lab instructor
* Autopsy version 4.17 (or similar version)
* The suspectdrive.img file provided with this lab on a USB drive, local folder, or accessible network share

# Image Analysis Using Autopsy

This lab is separated into three parts:

* Downloading and installing Autopsy
* Importing a suspect image file
* Examining the suspect image file with Autopsy

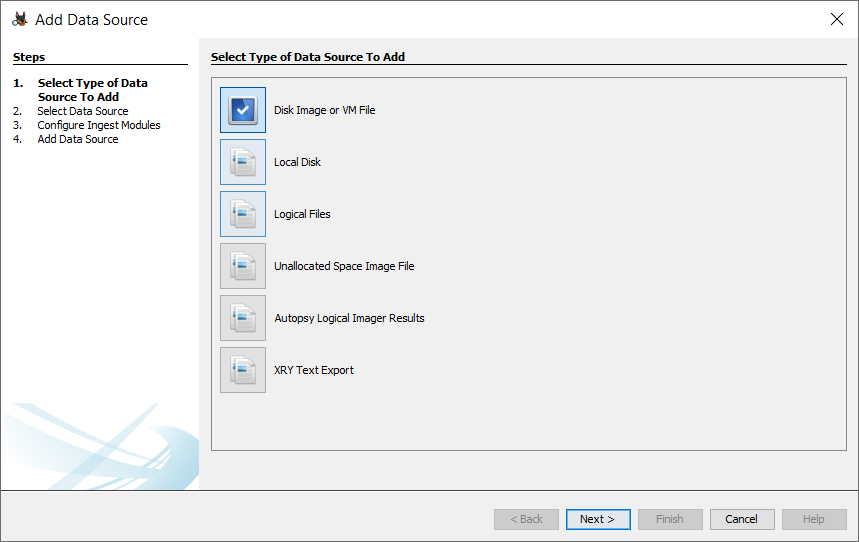
## Downloading and Installing Autopsy

1. Download the correct version of Autopsy from *www.autopsy.com/download/*. This lab uses the Windows 64-bit version 4.17 for demonstration.
2. Run the Autopsy.msi file.
3. In the Welcome to the Autopsy Setup Wizard, click **Next**.
4. Get the installation path from your instructor, specify this path in the Select Installation Folder window, and click **Next**.
5. Click **Install**.
6. If Windows prompts you about a User Account Control permission, click **Yes**.
7. Click **Finish** when the Completing the Autopsy Setup Wizard window appears.

Autopsy should now be fully installed.

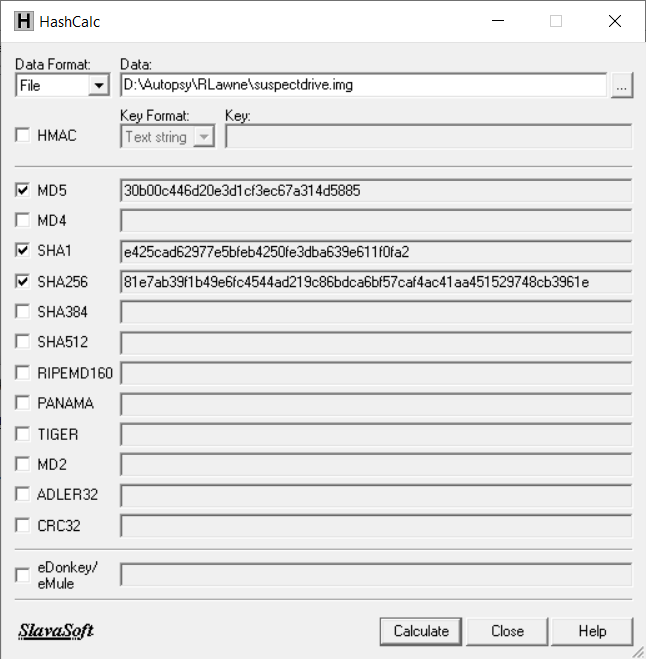
## Importing a Suspect Image File Using Autopsy

1. Start Autopsy. If this is the first time the installation has been used, you may be prompted to enable the central repository. Click **Yes**.
2. Click **New Case**.
3. In the New Case Information window, enter the Case Name. Your instructor may provide details for this portion of the lab; otherwise, enter **R Lawne Investigation** as the Case Name.
4. Specify a unique folder for the case files by clicking the **Browse** button and selecting or creating a folder. You can also enter a folder name in the Base Directory field.
5. Leave the Case Type field as Single User and click **Next**.
6. For the Case number, use a number provided by your instructor or make one up yourself.
7. Enter the remaining information in the appropriate fields.
8. Click **Finish** when you have entered the information. The software generates the appropriate files and displays the Add Data Source window, as shown in Figure L10-1.



**Figure L10-1** Autopsy’s Add Data Source window

1. As Step 1 of the procedure listed on the left side of Figure L10-1, click the **Disk Image or VM File** button to add the image file provided by your instructor. Click **Next**.
2. As Step 2 (Select Data Source) in the Add Data Source window, click **Browse** next to the Path field and navigate to the suspectdrive.img file on your system or USB drive. If your instructor has provided this file to you on an external drive or network location, save it to a USB drive and copy the file to the case folder you specified earlier. You may need to leave the Autopsy window for a moment to move the file to a location you can access. When Autopsy has accessed the file, it will copy the file to the folder you specified earlier.
3. Make sure the Time Zone value is correct in the window.
4. In an actual investigation, you would enter the hash values for the .img file into the fields provided for entry into your case records. Figure L10-2 shows these values calculated with the HashCalc tool from SlavaSoft; this tool is available from www.slavasoft.com/hashcalc/. If your instructor wants you to do so, you can download and run the tool, copying the hash values to Autopsy.



**Figure L10-2** HashCalc values for suspectdrive.img

1. Click **Next**.
2. As Step 3 (Configure Ingest Modules) in the Add Data Source window, simply click **Next**.
3. Step 4 (Add Data Source) in the window should indicate that the “Data source has been added to the local database. Files are being analyzed.” Click **Finish** to complete the import.

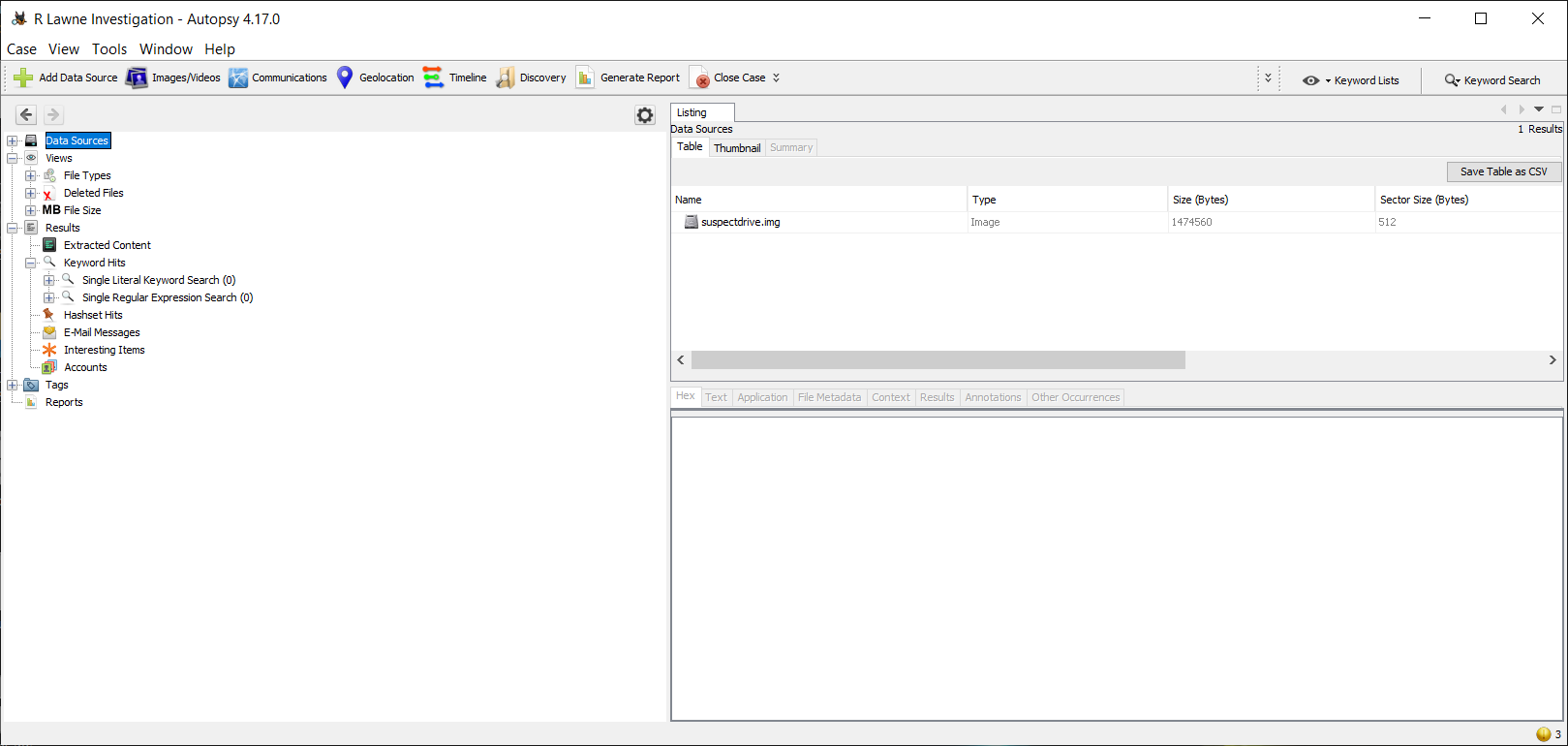
## Examining the Suspect Image File Using Autopsy

Normally, an investigation would begin with alleged misconduct or criminal activity against a suspect. Forensic investigators would legally seize all computer media and image them so that analysis would not risk modifying the original evidence. The image files can then be copied and analyzed with tools like Autopsy, FTK, or Encase.

The analysis of these tools would be framed with instructions for what a prosecutor or defense attorney is looking for, such as “Any files, communications, or other computer-based information associated with X, as well as any other clearly illegal or unauthorized activity.” If a forensic investigator were looking for evidence related to embezzlement in a corporate case but found evidence of other crimes, the evidence could be used to expand any legal charges against the suspect. (Technically, investigators look for *items of evidentiary value*, not evidence. Only when the information is entered into a legal proceeding does it become evidence.

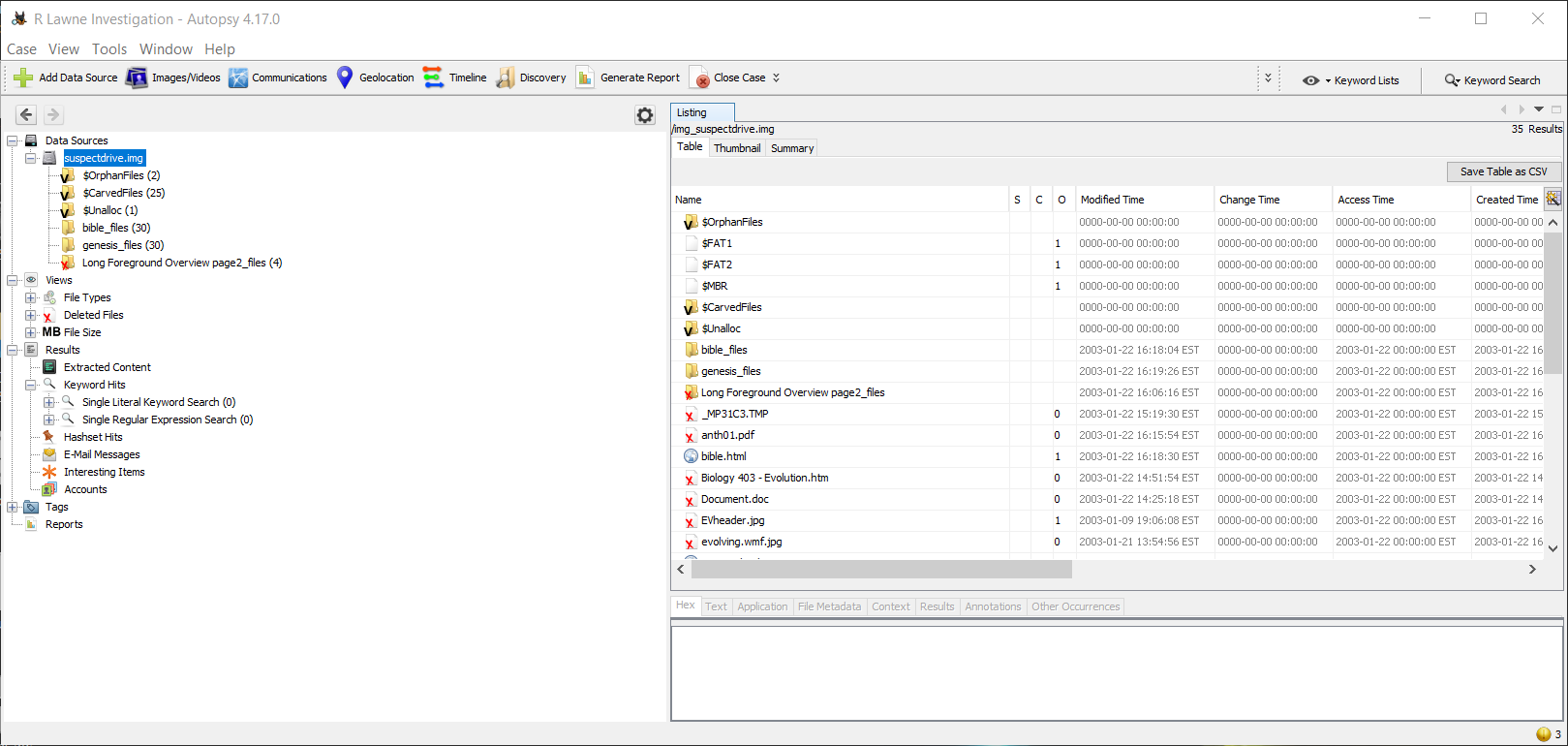
In the case of Richard S. Lawne, the suspect is accused of teaching inappropriate content in a school.

1. Restart Autopsy, if necessary, and select the case created in the previous steps. Your system layout should look similar to that in Figure L10-3.



**Figure L10-3** Autopsy after image import

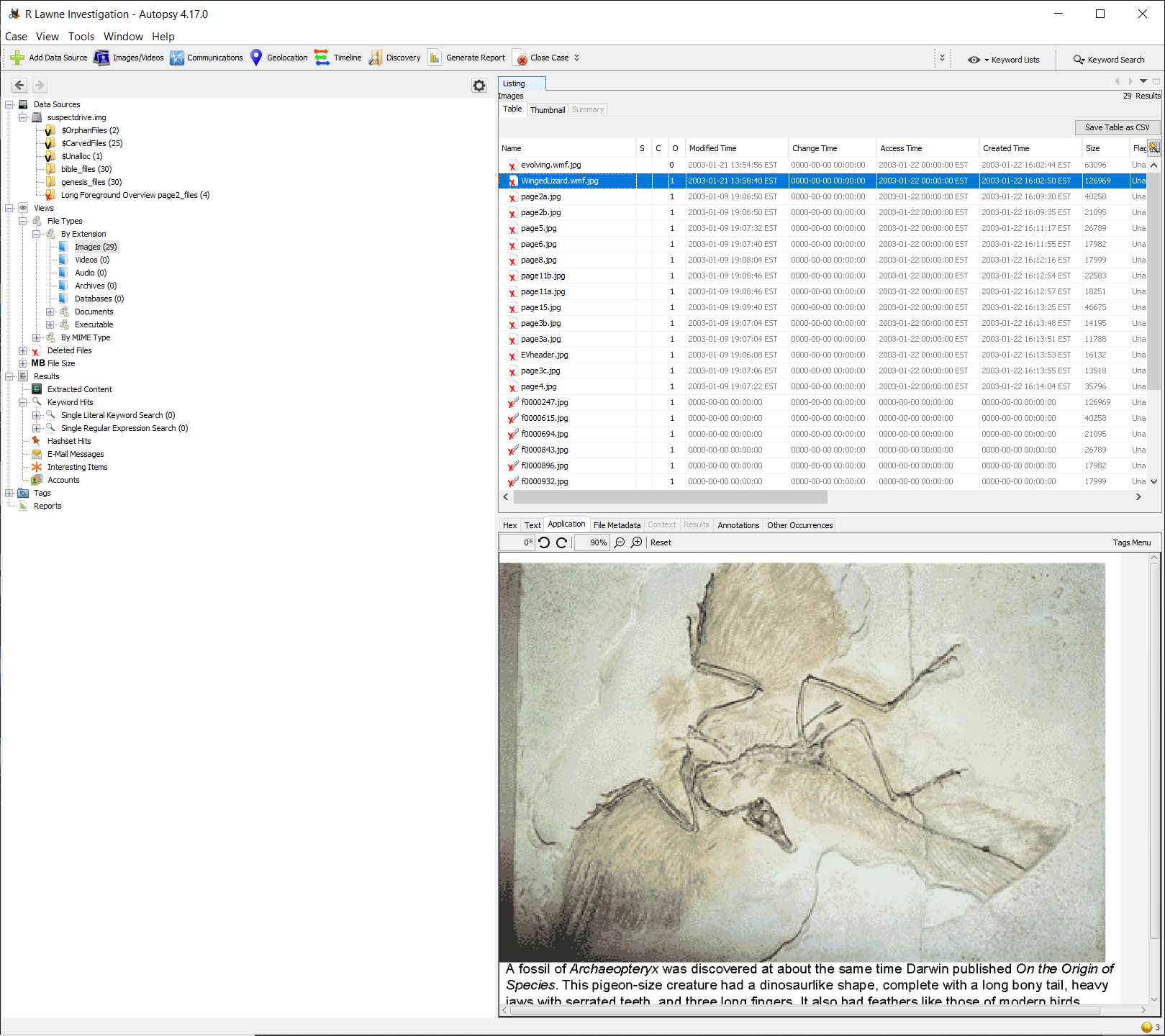
1. In the left pane of the window, click the **plus sign** next to Data Sources, and then click the **suspectdrive.img** filename. You can resize the window shown to more easily view the files in the upper-right pane. You should see a listing of items contained in the image, as shown in Figure L10-4.



**Figure L10-4** Contents of suspectdrive.img

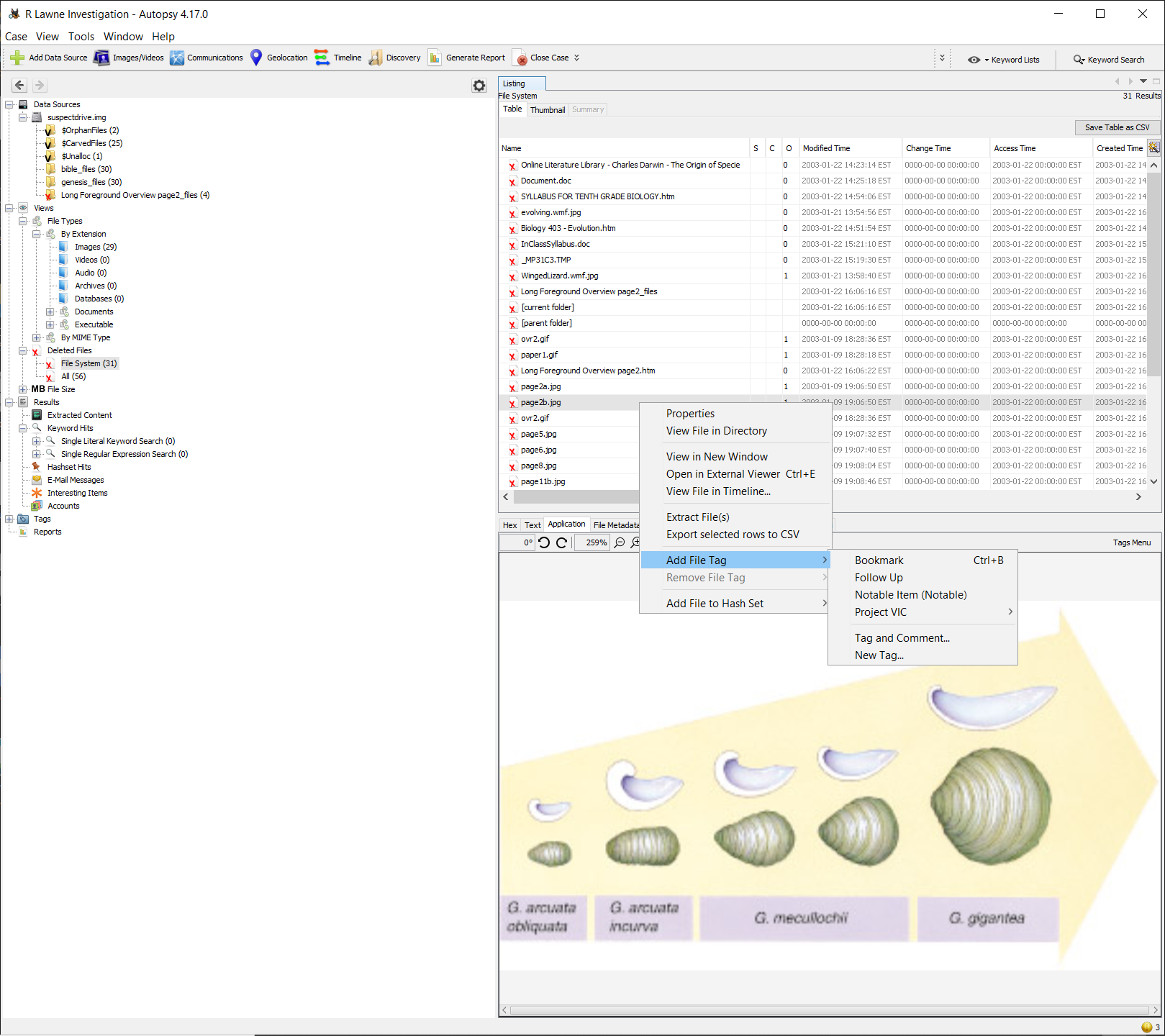
Several file types are automatically identified by Autopsy. It finds hidden files and deleted files on the imaged drive.

1. In the left pane of the window under the Views menu, click the **plus sign** next to File Types. Next, under File Types, click the **plus sign** next to Extension and then click **Images**. The window shows all undeleted graphics contained in the imaged drive. If you click in the list on the right side of Figure L10-4, the display will look like that in Figure L10-5.



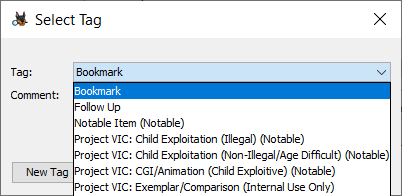
**Figure L10-5** Analysis using Autopsy

1. Click the **plus sign** next to the Deleted Files option on the left side of the window, and then click the **All** option. You see all files that were deleted but are still intact on the suspect’s drive. Scroll through the various images. Can you guess what Richard S. Lawne is accused of?
2. If you were the investigator, you could “tag” files that you felt were related to the charges or represented new crimes. Autopsy will add these files to the case file. To tag files and add them to the case file, select the file in the upper-right pane, right-click the file, select **Add File Tag**, and then specify which tag you want to assign (see Figure L10-6).



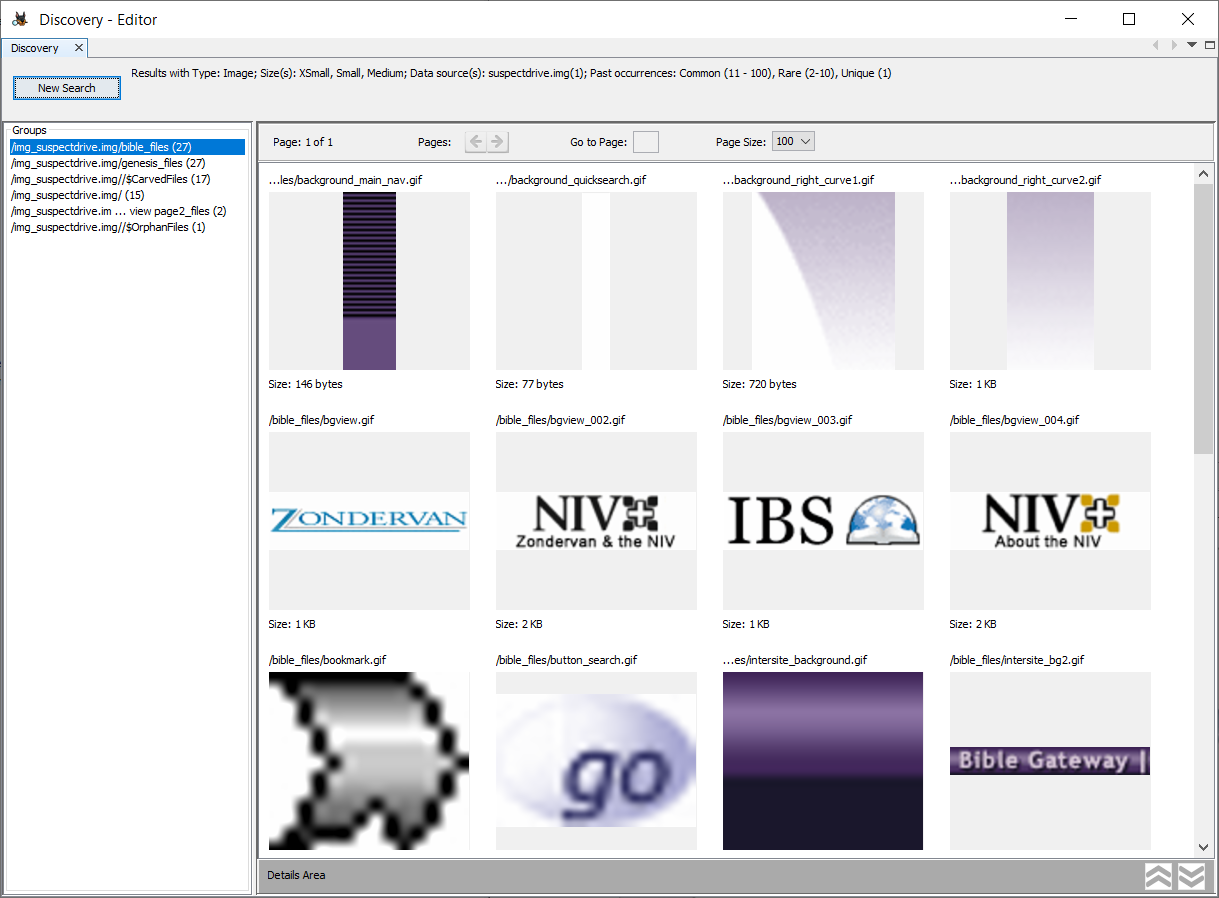
**Figure L10-6** Adding a file tag

1. In the Add File Tag submenu, you could select a follow-up tag for information you think is related but you need to investigate further, or you could select a definitive tag by clicking **Tag and Comment**. In the window that appears, you can specify the tag type and enter comments, as shown in Figure L10-7.



**Figure L10-7** Select Tag option

1. Go ahead and tag a few files. Afterward, notice that the tagged files are easily accessible at the bottom of the left menu under the Tags option. This allows you to revisit the images in later sessions.
2. You can extract files from the image by right-clicking the filename in the upper-left pane and selecting **Extract**. In the Save window that appears, you can specify where to save the extracted file.
3. Click the **Discovery** menu at the top of the Autopsy window. The Discovery feature allows you to search the image with specific parameters, such as file type, file size, and commonality. Specify the following parameters by checking the box next to each field and selecting the indicated options. Next, click **Search**.
   * Images
   * File Size: XSmall, Small, and Medium
   * Data Source: suspectdrive.img
   * Past Occurrences: Common, Rare, and Unique
4. The files found in the search appear in a new window, as shown in Figure L10-8.
5. A real investigation could involve dozens of imaged drives and thousands of files and images that must be reviewed and determined to be relevant or not. Select and tag all files that support the charges that Richard S. Lawne is teaching evolution. If you suspect that a file is relevant but you’re not sure, use the Follow Up tag shown in Figure L10-7. If you are confident that a file provides evidence Lawne is teaching evolution, use the Notable tag.



**Figure L10-8** Discovery Editor search results

1. After you have tagged all suspicious items, select the **Generate Report** menu at the top of the Autopsy window.
2. Specify **HTML Report**, enter **Richard S. Lawne Investigation** as the Header, enter your name as the Footer, and then click **Next**.
3. Ensure that **suspectdrive.img** is selected in the “Select which data source(s) to include” window.
4. Ensure that **All Tagged Results** is selected in the Configure Report window, and then click **Finish**.
5. Click **Close** when the report has been generated.
6. The report is available in the left menu, at the bottom under **Reports**. Open this menu and double-click the file. Open the file in the web browser of your choice. Your instructor may want you to print the file to a PDF or save it to an external drive before submitting it.

# Self-Reflection and Response

Attach the final report.

Were you able to complete the setup, configuration, and use of Autopsy?

|  |
| --- |
| I used a Kali Linux Virtual Machine and ran Autopsy from there. |

If you were not able to complete the setup and configuration, explain what went wrong.

|  |
| --- |
| I ended up playing with the online version of Autopsy, but did not have a data file to use as the image file. I am currently in CTEC 280 and I have used Autopsy in labs in that class, so I have been exposed to the program. |

## Instructor’s Response

|  |
| --- |
|  |