19. Why should you critique your case after it's finished?
20. What do you call a list of people who have had physical possession of the evidence?
21. Data collected before an attorney issues a memo for an attorney-client privilege case is protected under the confidential work product rule. True or False?

## Hands-On Projects

Create a Chap01\Projects folder under your work folder. Then download the `Ch01ProjDataFiles.exe` file from the downloads section for this chapter (on the student companion site for this book) to this work subfolder. Double-click this file in File Explorer to uncompress its contents.

### Hands-On Project 1-1

The case in this project involves a suspicious death. Joshua Zarkan found his girlfriend's dead body in her apartment and reported it. The first responding law enforcement officer seized a USB drive. A crime scene evidence technician skilled in data acquisition made an image of the USB drive with FTK Imager and named it `C1Prj01.E01`. Following the acquisition, the technician transported and secured the USB drive and placed it in a secure evidence locker at the police station. You have received the image file from the detective assigned to this case. He directs you to examine it and identify any evidentiary artifacts that might relate to this case. To process this case, follow these steps to evaluate what's on the image of the USB drive:

1. Start Autopsy for Windows, and click the **Create New Case** icon. In the New Case Information window, enter **C1Prj01** in the Case Name text box, and click **Browse** next to the Base Directory text box. Navigate to and click your work folder, and then click **Next**.
2. In the Additional Information window, type **C1Prj01** in the Case Number text box and your name in the Examiner text box, and then click **Finish**.
3. In the Select Data Source window, click the **Select data source type** list arrow, and click **Disk Image or VM file**. Click the **Browse** button next to the "Browse for an image file" text box, navigate to and click your work folder and the **`C1Prj01.E01`** file, and then click **Open**. Click **Next**.
4. In the Configure Ingest Modules window, click **Select All**. Click **Next** and then **Finish**.
5. In the Tree Viewer pane, expand **Views**, **File Types**, **By Extension**, and **Documents**.
6. Examine each subfolder under Documents. Determine which folder might contain files of interest to this case.
7. If you found any files related to the case, select the files as a group, right-click the selection, and click **Extract File(s)**. In the Save dialog box, click **Save** to save the files automatically in Autopsy's case subfolder: *Work*\Chap01\Projects\C1Prj01\Export.
8. Write a short report of no more than two paragraphs, including facts from any contents you found. When you're finished, leave Autopsy running if you're continuing to the next project.

### Hands-On Project 1-2

In this project, you work for a large corporation's IT Security Department. Your duties include conducting internal digital investigations and forensics examinations on company computing systems. A paralegal from the Law Department, Ms. Jones, asks you to examine a USB drive belonging to an employee who left the company and now works for a competitor. The Law Department is concerned that the former employee might possess sensitive company data. Ms. Jones wants to know whether the USB drive contains anything relevant.

In addition, she tells you that the former employee might have had access to confidential documents because a co-worker saw him accessing his manager's computer on his last day of work. These documents consist of nine files containing the word "confidential." She wants to know whether the USB's bit-stream image file has these documents.

To process this case, make sure the `C1Prj02.001` file has been extracted to your work folder, and then follow these steps:

1. Start Autopsy for Windows, if you exited it at the end of the previous project. If the previous project is open, click **Case**, **Close Case** from the menu. Click the **Create New Case** icon. In the New Case Information window, enter **C1Prj02** in the Case Name text box, and click **Browse** next to the Base Directory text box. Navigate to and click your work folder, and then click **Next**.
2. In the Additional Information window, type **C1Prj02** in the Case Number text box and your name in the Examiner text box, and then click **Finish**.
3. In the Select Data Source window, click the **Select data source type** list arrow, and click **Disk Image or VM file**. Click the **Browse** button next to the "Browse for an image file" text box, navigate to and click your work folder and the **`C1Prj02.001`** file, and then click **Open**. Click **Next**.
4. In the Configure Ingest Modules window, click **Select All**. Click **Next** and then **Finish**.
5. Click the **Keyword Search** button at the far upper right, type confidential in the text box, and then click **Search**.
6. In the Result Viewer pane, a new tab named Keyword search 1 opens. Click each file to view its contents in the Content Viewer pane.
7. Ctrl+click to select the files in the Keyword search 1 tab. Right-click this selection, point to **Tag File**, and click **Tag and Comment**. In the Create Tag dialog box, click the **New Tag Name** button, type **Recovered Office Documents** in the Tag Name text box, and then click **OK**.
8. Click **Generate Report** at the top. In the Generate Report window, click the **Results - Excel** option button in the Report Modules section, and then click **Next**.
9. In the Configure Artifacts Report window, click the **Tagged Results** button, click the **Recovered Office Documents** check box, and then click **Finish**.
10. In the Report Generation Progress Complete window, click the **Results - Excel** pathname to open the Excel report. This Excel file should have several tabs of information about the files you tagged for this project.

5. In the Tree Viewer pane, scroll down and expand **Tags**, **Follow Up**, and **File Tags**.
6. In the Result Viewer pane, click the **Thumbnail** tab to view the tagged photos.
7. To create a report, click Generate Report at the top. In the **Generate Report** window, click the **Results - HTML** option button in the Report Modules section, and then click **Next**.
8. In the Configure Artifacts Report window, click the **Tagged Results** button, click the **Follow Up** check box, and then click **Finish**.
9. In the Report Generation Progress window, click the **Results - HTML** pathname to view the report. When viewing the report, click the links to examine the tagged files. When you're finished, click **Close** in the Report Generation Progress window.
10. Exit Autopsy, and write a short memo to summarize your findings.

**Tip**

When doing string searches, it's a good practice to examine graphics files that might contain documents. The search functions in forensics tools ignore graphics files because text in a graphics file is stored as part of a picture, not as plain text.

### Hands-On Project 1-4

Sometimes discovery demands from law firms require you to recover only allocated data from a disk. This project shows you how to extract just the files that haven't been deleted (that is, the allocated files) from an image.

1. Start Autopsy for Windows. Click the **Create New Case** icon. In the New Case Information window, enter **C1Prj04** in the Case Name text box, and click **Browse** next to the Base Directory text box. Navigate to and click your work folder, and then click **Next**.
2. In the Additional Information window, type **C1Prj04** in the Case Number text box and your name in the Examiner text box, and then click **Finish**.
3. In the Select Data Source window, click the **Select data source type** list arrow, and click **Disk Image or VM file**. Click the **Browse** button next to the "Browse for an image file" text box, navigate to your work folder and click the `C1Prj04.E01` file, and then click **Open**. Click **Next**.
4. In the Configure Ingest Modules window, click **Select All**. Click **Next** and then **Finish**.
5. In the Tree Viewer pane, expand **Views**, **File Types**, and **By Extension**. Under By Extension are several subfolders representing file types, as you've seen in previous projects. Next to each file type subfolder is a number enclosed in parentheses, which shows the number of files of this type Autopsy found. Click subfolders with numbers greater than zero to view the files.
6. In the Result Viewer pane, scroll to the right, if necessary until the Flags(Meta) column is in view. Sort the column by clicking the **Flags(Meta)** header, which displays all allocated files to the top of the list.

**Note**

In the Result Viewer pane, allocated (not deleted) files have a paper sheet icon to the left of the filename. Deleted (unallocated) files have a red X over the paper sheet icon, and unallocated files that have been corrupted and recovered by the OS have a diagonal broken bar icon.

7. Scroll to the left until the Name column is visible. If there are allocated files, they will be at the top of this list. Ctrl+click each allocated file, right-click this selection, and then click **Extract File(s)**.
8. In the Save dialog box, click Save to save the files automatically in Autopsy's case subfolder: *Work*\Chap01\Projects\C1Prj04\Export.
9. Write a brief memo that lists all the files you exported. Leave Autopsy running for the next project.

### Hands-On Project 1-5

This project is a continuation from the previous project. You create a report listing all the unallocated (deleted) files Autopsy finds.

1. Start Autopsy for Windows and click the **Open Recent Case** icon, if necessary.
2. In the Tree Viewer pane, expand **Views**, **File Types**, **Deleted Files**, and **All**.
3. In the Result Viewer pane, Ctrl+click all files in the All subfolder. Right-click this selection, point to **Tag File** and then **Quick Tag**, and click **Follow Up**.
4. Click **Generate Report** at the top. In the Generate Report window, click the **Results - Excel** option button in the Report Modules section, and then click **Next**.
5. In the Configure Artifacts Report window, click the **Tagged Results** button, click the **Follow Up** check box, and then click **Finish**.
6. In the Report Generation Progress Complete window, click the **Results - Excel** pathname to open the Excel report. When you're finished, click **Close** in the Report Generation Progress window.
7. Write a brief memo listing all the deleted files on your report spreadsheet. Exit Autopsy.

### Hands-On Project 1-6

In this project, another investigator asks you to examine an image and search for all occurrences of the following keywords:

- ANTONIO
- HUGH EVANS
- HORATIO

After you complete these searches, the investigator wants a short report listing which files contain these names.

1. Start Autopsy for Windows. Click the **Create New Case** icon. In the New Case Information window, enter **C1Prj06** in the Case Name text box, and click **Browse** next to the Base Directory text box. Navigate to and click your work folder, and then click **Next**.

2. In the Additional Information window, type **C1Prj06** in the Case Number text box and your name in the Examiner text box, and then click **Finish**.
3. In the Select Data Source window, click the **Select data source type** list arrow, and click **Disk Image or VM file**. Click the **Browse** button next to the "Browse for an image file" text box, navigate to your work folder and click the `C1Prj06.E01` file, and then click **Open**. Click **Next**.
4. In the Configure Ingest Modules window, click **Select All**. Click **Next** and then **Finish**.
5. Click the **Keyword Lists** button at the far upper right, and then click **Manage List**.
6. In the Global Keyword Search Settings dialog box, click the **New List** button. In the New Keyword List dialog box, type **ListSearch1** in the "New keyword list" text box, and then click **OK**.
7. In the Keyword Lists section, click **ListSearch1**, as shown in Figure 1-22, and then click the **New keywords** button under the Keyword Options heading.

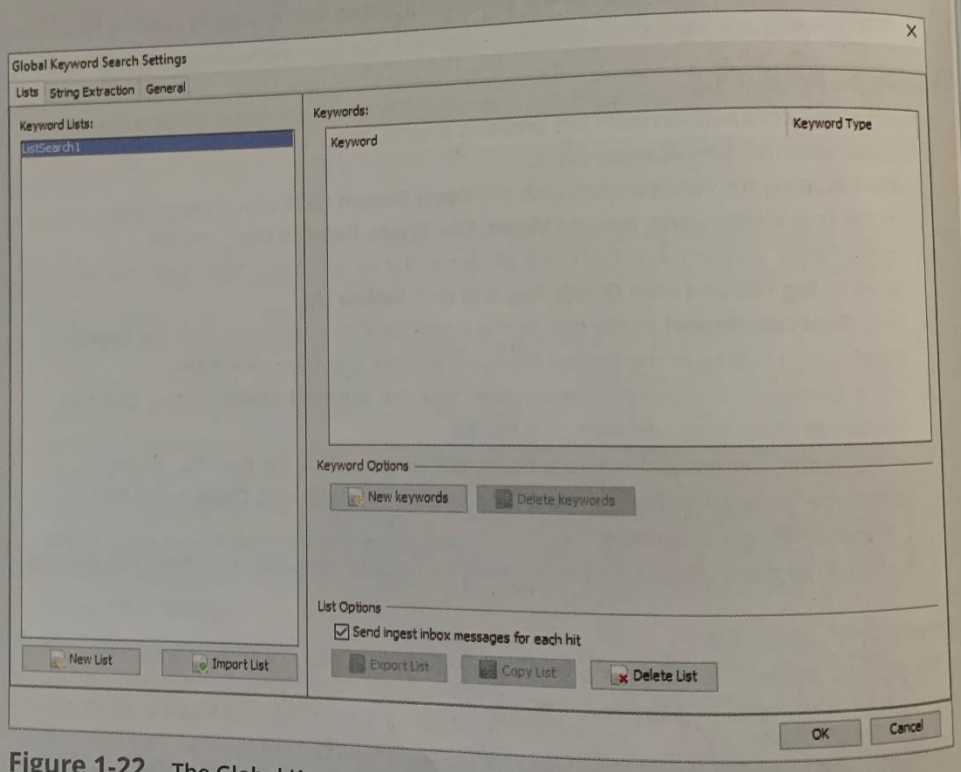


**Figure 1-22** The Global Keyword Search Settings dialog box
Source: *www.sleuthkit.org*

8. In the New keywords dialog box, type **ANTONIO** in the "Enter keywords (one per line) below" text box and press **Enter**, type **HUGH EVANS** and press **Enter**, and then type **HORATIO** and click **OK**. Click **OK** again.

9. In Autopsy's main window, click **Keyword List** again, click the **ListSearch1** check box, and then click **Search**.
10. Inspect each file to see whether it contains the word "confidential." If so, right-click the file, point to **Tag Files** and then **Quick Tag**, and then click **Follow Up**.

**Note**

If the search results don't display the keyword in the Content Viewer, the keyword might be obscured. For example, if a keyword is in unallocated disk space that's commingled with a graphics file, the Content Viewer automatically displays the graphics file. If this occurs and you want to examine the unallocated area, click the Content Viewer's Hex, String, or Indexed Text tabs to see what additional information might be revealed.

11. Click **Generate Report** at the top. In the Generate Report window, click the **Results - HTML** option button in the Report Modules section, and then click **Next**.
12. In the Configure Artifacts Report window, click the **Tagged Results** button, click the **Follow Up** check box, and then click **Finish**.
13. In the Report Generation Progress window, click the **Results - HTML** pathname to view the report. When you're finished, click **Close** and then exit Autopsy. Write a memo to the investigator with the following information from the report:
    - Keyword
    - File's pathname and filename
    - Modified date and time
    - Create date and time
    - File size

## Case Projects

### Case Project 1-1

An insurance company has asked your digital forensics firm to review a case for an arson investigation. The suspected arsonist has already been arrested, but the insurance company wants to determine whether there's any contributory negligence on the part of the victims. Two files were extracted to your work folder for this project. The first, `Chap01_CasePrj01a.doc`, is a memo about the case from the police department. The second, `Chap01_CasePrj01b.doc`, is a letter from the insurance company explaining what should be investigated. Review these files, and decide the course of action your firm needs to take. Write an outline for how your firm should approach the case.