## LAB PRACTICE: RECOVERING GRAPHICS FILE

### TASK 1

In this task, you use ProDiscover Basic to locate and extract JPEG files with altered extensions. Some of these files are embedded in files with non-JPEG extensions. Find the C10frag.eve file in your work folder, and then follow these steps:

1. Start ProDiscover Basic (with the **Run as administrator** option) and begin a new project. In the New Project dialog box, type **C10frag** in the Project Number and Project File Name text boxes, and then click **OK**.
2. In the tree view, click to expand **Add**, and then click **Image File**. In the Open dialog box, navigate to your work folder and click **C10frag.eve**. Click **Open**, and then click **Yes,** if necessary, in the Auto Image Checksum message box.
3. Click the **Search** toolbar button. In the Search dialog box, click the **Content Search** tab. Under Search for the pattern(s), type **JFIF**, and under Select the Disk(s)/Image(s) you want to search in, click **C10frag.eve**. Click **OK**.
4. Click each file in the work area's search results that doesn't have a .jpg extension, and in the data area, scroll through each file to find any occurrences of a **JFIF** label. Click the check box next to each file with a JFIF label. When the Add Comment dialog box opens, type **Recovered hidden .jpg file**, click the **Apply to all items** check box, and then click **OK**.
5. In the tree view, click **Report**, and then click **File, Print Report** from the menu. You can also save your report by clicking the **Export** toolbar button, and in the Export dialog box's File name text box, type **C10Prj01.rtf**, and then click **OK**.
6. Exit ProDiscover Basic, saving your project when prompted.

### TASK 2

Find the C10carve.eve file in your work folder. This image file is a new acquisition of another USB drive the EMTS manager retrieved. He wants to know whether any similar files on this drive match the files you recovered from the first USB drive. Because you know that the files you recovered earlier have zzzz for the first 4 bytes, you can use it as your search string to see whether similar files exist on this USB drive.

1. Start ProDiscover Basic (with the **Run as administrator** option) and begin a new project. In the New Project dialog box, type **C10carve** for the project number and project filename, and then click **OK**.

2. In the tree view, click to expand **Add,** and then click **Image File**. In the Open dialog box, navigate to your work folder and click **C10carve.eve**. Click **Open**, and then click **Yes**, if necessary, in the Auto Image Checksum message box.
3. Next, click the **Search** toolbar button. In the Search dialog box, click the **Content Search** tab, and then click the **ASCII** option button and the **Case Sensitive** check box. Under Search for the pattern(s), type **zzzz,** and under Select the Disk(s)/Image(s) you want to search in, click **C10carve.eve.** Click **OK**.
4. Click each file in the work area's search results to display it in the data area. If the file contains zzzz at the beginning of the sector, click the **Select** check box next to it. In the Add Comment dialog box, type **Similar file located on first USB drive**, click the **Apply to all items** check box, and then click **OK**.
5. In the work area, click the **Add to Report** button.
6. Double-click the **gametour5.txt** file. In the work area, click the **File Name** column heading to sort all files in this pane. Scroll through the list of files and click the **Select** check box for the gametour1.txt, gametour2.txt, gametour3.txt, gametour4.txt, and gametour6.txt files. When the Add Comment dialog box opens, type **Additional similar files on USB drive**, and then click **OK**. Repeat this step for each gametour file you find.
7. Right-click the **gametour1.txt** file and click **Copy All Selected Files**. In the Choose Destination dialog box, click **Browse**, navigate to and click your work folder, and then click **OK**.
8. To complete your examination, in the tree view, click **Report**, and then click **File, Print Report** from the menu. You can also save your report by clicking the **Export** toolbar button, and in the Export dialog box's File name text box, type **C10Prj02.rtf**. Then click **OK**.
9. Save the project and exit ProDiscover Basic.

## TASK 3

In this task, you use IrfanView to open graphics files and save them in a compressed graphics format different from the original format. You should note any changes in image quality after converting files to a different format. Download IrfanView from *www.irfanview.com* and install it, and then follow these steps:

1. Start IrfanView.
2. Click **File, Open** from the menu. In the Open dialog box, navigate to your work folder, and then double-click **Spider.bmp** to open the file.
3. Click **File, Save** as from the menu. Change the file type to **JPG** and save the file as **Spider.jpg** in the same location.
4. Save Spider.jpg as **Spider2.bmp** in the same location.
5. Open these three graphics files in new sessions of IrfanView and compare the files. Document any changes you notice.

6. Open **Flower.gif** from your work folder, and save it as **Flower.jpg** in the same location.
7. Save Flower.jpg as **Flower2.gif** in the same location.
8. Open these three graphics files in new sessions of IrfanView, and document any changes you see when comparing the files.
9. Open **Cartoon.bmp** from your work folder, and save it as **Cartoon.gif** in the same location.
10. Save Cartoon.gif as **Cartoon2.bmp** in the same location.
11. Open these three graphics files in new sessions of IrfanView, and document any changes you see when comparing the files.
12. Exit all instances of IrfanView. Summarize your conclusions in a brief report.

**<u>TASK 4</u>**

In this task, you use S-Tools4 to create a steganography file for hiding an image. Download S-Tools4 from *www.stegoarchive.com*, install the program, and then follow these steps:

1. In Windows Explorer, navigate to where you installed S-Tools4, and start the program by double-clicking **S-Tools.exe**.
2. Drag **Rushmore.bmp** from your work folder to the S-Tools window.
3. To hide text in the Rushmore.bmp file, drag **findme.txt** from your work folder to the **Rushmore.bmp** image.
4. In the Hiding 99 bytes dialog box, type **FREEDOM** in the Passphrase and Verify passphrase text boxes, and then click **OK**. A hidden data window opens in the S-Tools window.
5. Right-click the hidden data window and click **Save as**. Save the image as **Steg.bmp** in your work folder.
6. Close the Steg.bmp and Rushmore.bmp windows, but leave S-Tools open for the next project.

**<u>TASK 5</u>**

In this task, you use S-Tools4 to create a secret message in a bitmap file and compare this steganography file to the original file by using the DOS Comp command. You need S-Tools4 and the Mission.bmp and USDECINP.rtf files in your work folder. Follow these steps to create a steganography file:

1. If you have exited S-Tools4, start it by double-clicking **S-Tools.exe** in Windows Explorer.
2. Drag **Mission.bmp** from your work folder to the S-Tools window.
3. Next, drag **USDECINP.rtf** from your work folder to the **Mission.bmp** image.
4. Type **hop10-5** in the Passphrase and Verify passphrase text boxes, and then click **OK**. A hidden data window opens in the S-Tools window.
5. Right-click the hidden data window and click **Save as**. Save the image as **Mission-steg.bmp** in your work folder. Exit S-Tools

Next, you use the DOS command to compare these two files and redirect the output to a text file for further analysis:

1. Click **Start**, type **cmd** in the Start Search text box, and then press Enter. (In Windows XP, click **Start, Run**, type **cmd**, and click **OK**.)
2. Change to your work folder by typing **cd /Work/Lab10/Projects** (substituting the path to your work folder) and pressing **Enter**.
3. Type **comp Mission.bmp Mission-steg.bmp > Mission-compare.txt** and press **Enter**, and then at the Compare more files (Y/N)? prompt, type n and press **Enter**.
4. Open the **Mission-compare.txt** file to see what discrepancies were found. When you're finished, close the file, and exit the command prompt window by typing **exit** and pressing **Enter**.
5. To complete this task, write a one-page report on the number of mismatches and the deviation in each mismatch between the two files. In addition, state your observations of the differences in the two files, such as hexadecimal values and their patterns.