**SCY486 – Lab exercise 10**

**Part One: Working with Exif data**

The first part looks at media files (JPEG) using ExifReader and ExifTool. The goal is to examine the resulting Exif data that is displayed, and determining what useful information can be gathered in the scope of an investigation.

### **Exif Data – Definition**

Exif, or exchangeable image file format, is a standard that specifies the formats for images, sound, and data used by digital cameras (including smartphones), scanners and other systems handling image and sound files recorded by digital cameras.

**Originally, JPEG and TIF formats were designed to store only digital photo data. Exif is an enhancement of these formats that modifies the beginning of a JPEG or TIF file so that metadata can be inserted.**

There are differences between file headers in Exif and standard JPEG.

All JPEG files, including Exif, start from offset 0 (the first byte of a file) with hexadecimal FFD8. The current standard header for regular JPEG files is JPEG File Interchange Format (JFIF), which has the hexadecimal value FFE0 starting at offset 2. For Exif JPEG files, the hexadecimal value starting at offset 2 is FFE1. In addition, the hexadecimal values at offset 6 specify the label name. For all JPEG files, the ending hexadecimal marker, also known as the end of image (EOI), is FFD9

1. **Why should we care about Exif data?**
2. Exif data has become more pivotal in digital forensics cases in the past ten years or so due to the fact that an increasing amount of cameras and smart phones are using GPS data. This data has greatly assisted investigators in finding locations of photos depicting criminal actions, and also in identifying the make and model of cameras used in these crimes.
3. Searching photos for potential Exif data is pivotal in the course of an investigation. Upon locating photos on a suspect drive, it is important that these photos be checked for existing Exif data.
4. Aggregating evidence reports containing Exif data has become pivotal to current-day investigations. As metadata becomes more prevalent in an increasing amount of file types, photos continue to be a main source of case information and evidence.

### **About Exif**

1. Exif information is most highly useful in terms of geolocation information in the scope of an investigation (if the file has GPS capability).
2. Exif format has standard tags for location information. As of 2014, many cameras and mobile phones have a built-in GPS receiver that stores location information in the Exif header when a picture is taken.
3. GPS data can also be added to any digital photograph via computer, either by using GPS software or by using mapping software to add the geolocation information. **The process of adding geographic information to a photograph is known as geotagging.** Many photo-based websites like FB allow users to upload geocoded pictures or to add geolocation information online.

In terms of an investigation, it is often highly useful to find geolocation data on photos on a suspect’s drive. Geolocation data can serve to offer investigators the following information:

Using this information allows investigators to gather information about camera makes and models that could potentially lead to apprehending a suspect.

### **ExifReader**

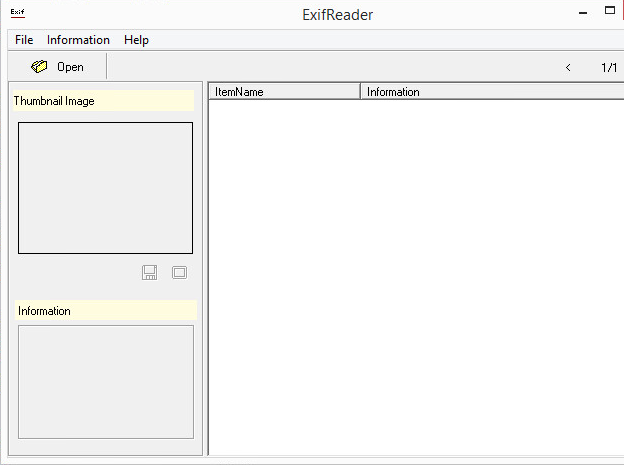
Exif Reader is an **image** file analysis software for Windows. It analyzes and displays shutter speed, flash condition, focal length, and other image information included in the Exif image format. This format is supported by almost all newer digital cameras. ExifReader analyzes JPEG files created by digital cameras. Exif image files with an extension of JPG can be treated in the same manner as conventional JPEG files.

### **ExifTool**

ExifTool is a platform-independent command-line application for reading, writing and editing metadata information in a wide variety of files. ExifTool supports many different metadata formats – many more than ExifReader. ExifTool is available as a stand-alone Windows executable and a Mac OS package as well.

**Using ExifReader**

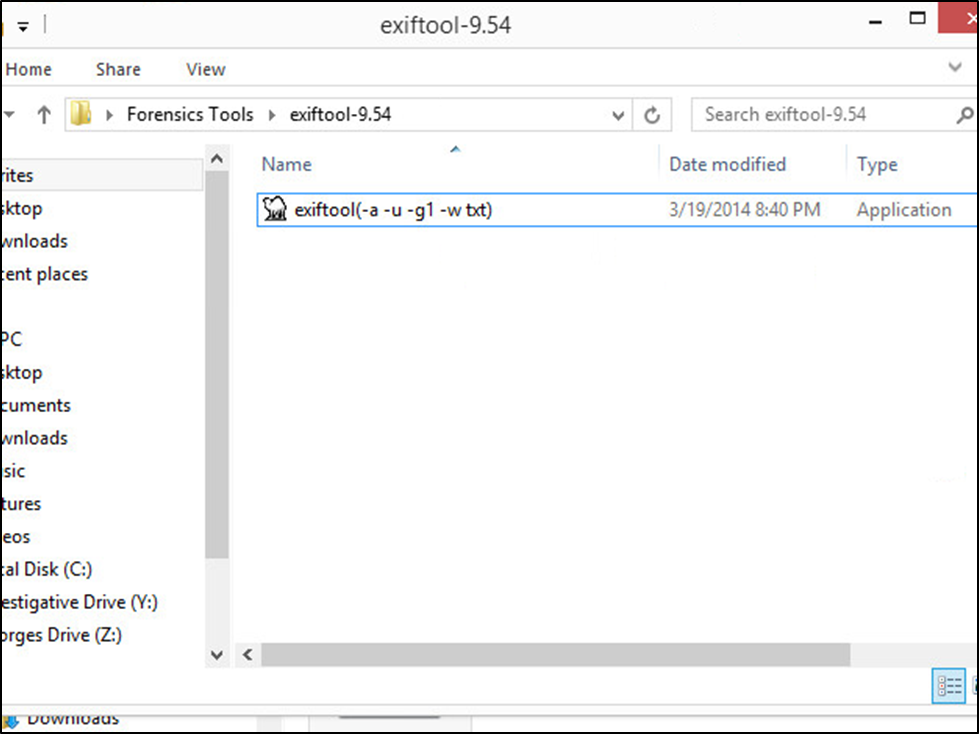
1. Copy ExifReader and cat.jpg, from the Share onto your desktop.



1. Open the cat.jpg. The available data for **cat.jpg** will be displayed on the right, while the thumbnail of the image will generally be displayed on the left. Browse through the available data. List the types of data that would be useful for investigation.
2. Once an analysis has been completed, save a text-based report that can later be included in case notes. Navigate to **Information>>Save as Text**. Save the report to a desired location. After the file has been saved, open it and view the data. The report will contain all information as seen within ExifReader. This report can be used as evidence. Pick a picture from your Pictures folder, if any is available and obtain its meta data.

**Using ExifTool**

1. Get the zipped exiftool zipped file from the Share and extract it in the exiftool folder on your Desktop
2. Open the ExifTool folder in your Desktop folder. Drag and drop it onto the executable file.
3. What important data is displayed by this tool?
4. It is possible to change the name of the executable in order to create a text-based Exif report. Rename the ExifTool executable to **exiftool(-a –u –g1 –w txt).exe**, as seen in the following image.

****

1. Once the application has been renamed, drag **apartment.jpg** onto the executable. This will automatically create a text file that contain the Exif data for the photo file. The report will appear as the one for ExifReader. The Exif information is more easily viewable in this format, and is ideal for aggregating case reports and data.

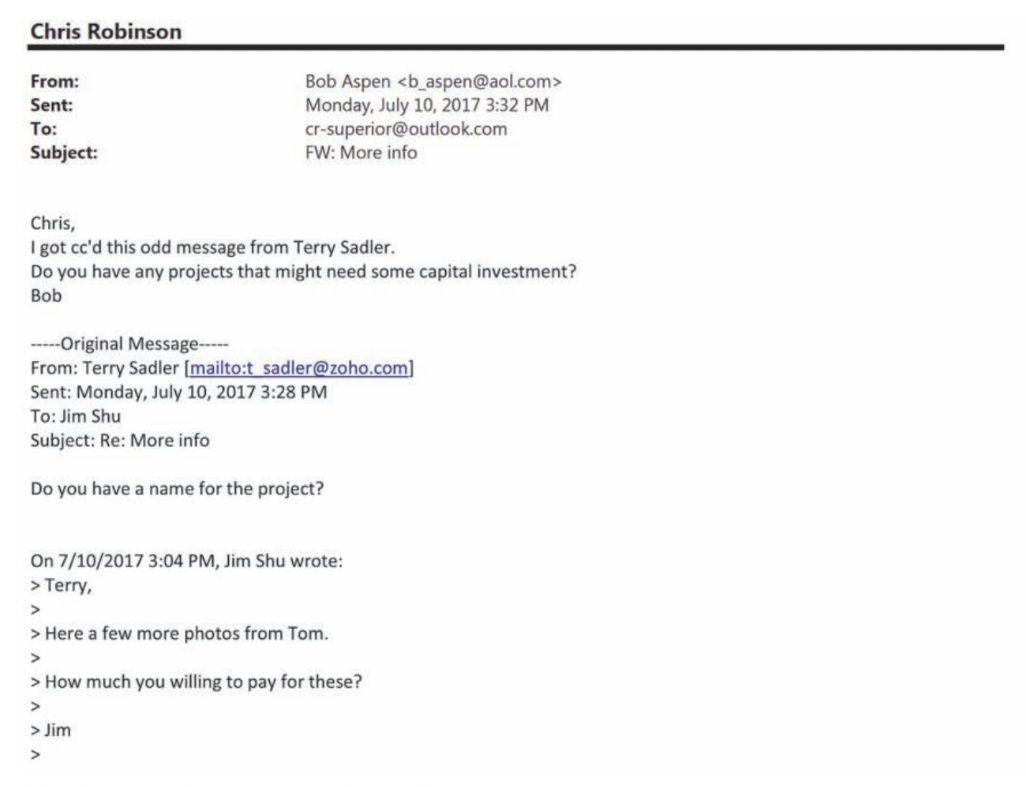
Please show Dr.Shumba your reports from the two tools: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

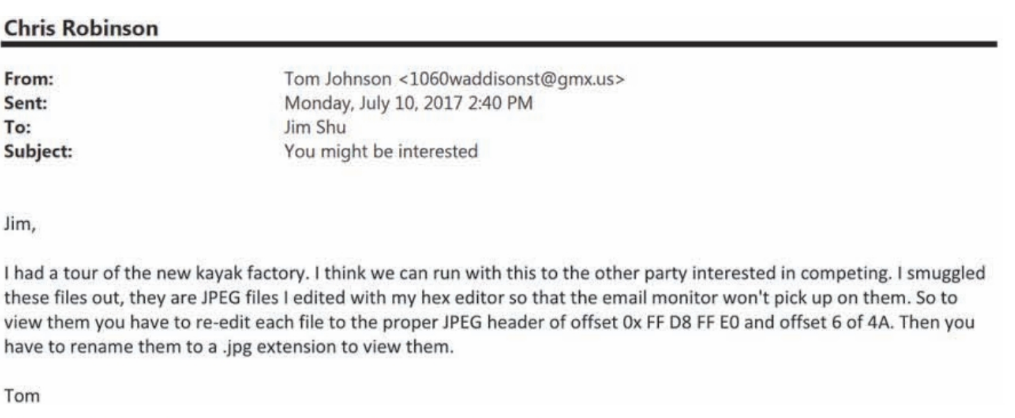
**Part One: Locating and recovering graphics files**

1. In a digital forensics investigation involving graphics files, you need to locate and recover all graphics files on the suspect drive and determine which ones are pertinent to your case.
2. For example, if you find an image that you suspect is a JPEG file but can’t display it with a bitmap graphics program, compare its file header with a known JPEG file header to determine whether the header has been altered.
3. If a graphics file is fragmented across areas on a disk, you must recover all the fragments before re-creating the file.
4. When you’re examining recovered fragments from files in slack or free space, you might find data that appears to be a header for a common graphics file type. If you locate header data that’s partially overwritten, you must reconstruct the header to make it readable by comparing the hexadecimal values of known graphics file formats with the pattern of the file header you have.

**Scenario:**

Suppose you’re investigating a possible intellectual property theft by a new employee of Superior Bicycles, Inc. This employee, Tom Johnson, is the cousin of Jim Shu, an employee who had been terminated. Bob Aspen is an external contractor and investor who gets a strange e-mail from Terry Sadler about Jim Shu’s new project. Bob forwards the e-mail to Chris Robinson (the president of Superior Bicycles) to inquire about any special projects that might need capital investments. Chris forwards the e-mail to the general counsel, Ralph Benson, asking him to look into it. He also forwards it to Bob Swartz, asking him to have IT look for any e-mails with attachments. After a little investigation, Bob Swartz forwards an e-mail IT found with the subject “You might be interested” to Chris Robinson. For this examination, you need to search for all possible places data might be hidden.

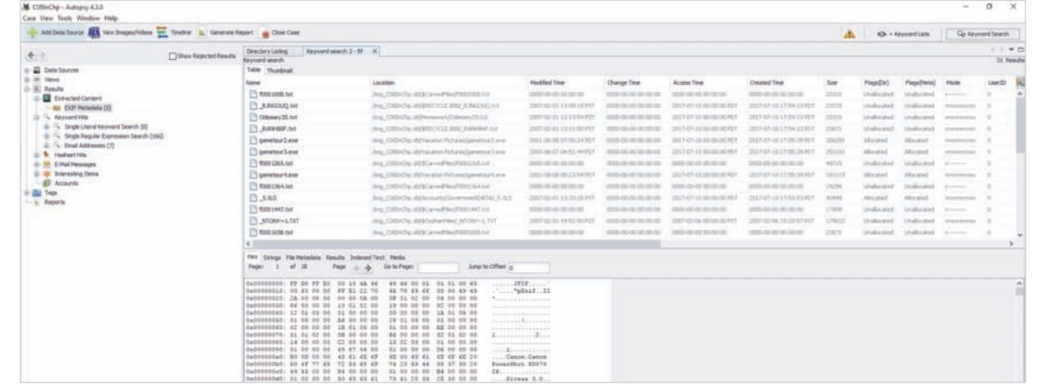




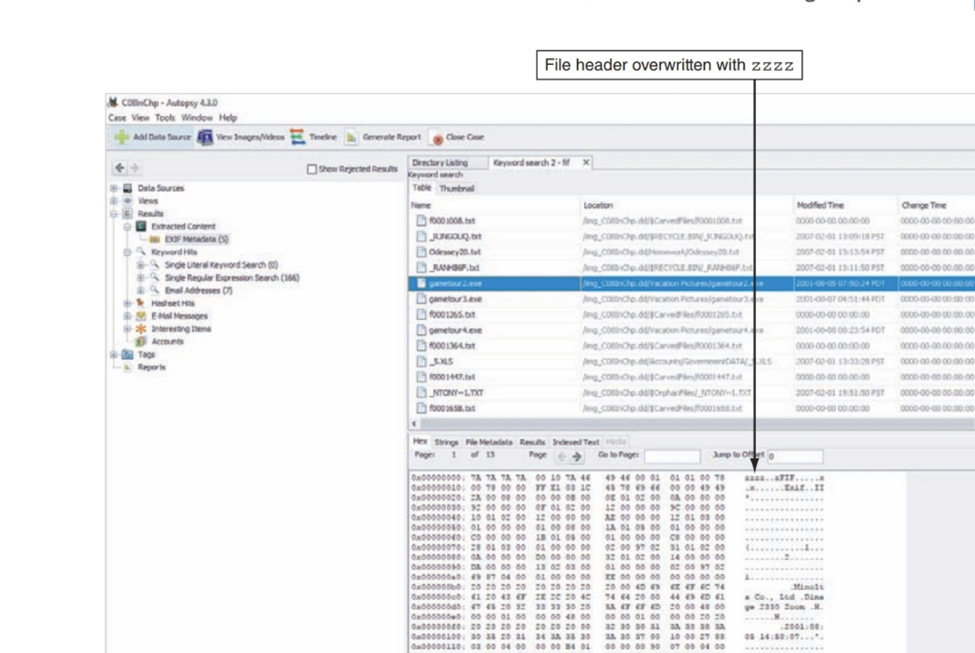
From the emails, what pieces of information do you have? And what are you going to be looking for?

Because the files have been extracted from the mail server, you should be thorough in your examination and analysis. You need to search all sectors of the drive for deleted files, both allocated space (in case Bob didn’t modify the files) and unallocated space.

1. Install Autopsy if you do not have it installed.
2. Start Autopsy for Windows, and click the Create New Case button. In the New Case Information window, type Exiff for the case name, and click Browse next to the Base Directory text box. Navigate to and click your work folder, and then click Next. In the Additional Information window, type Exiff for the case number, enter your name for the examiner, and then click Finish.
3. . In the Add Data Source window, leave the default selection Disk Image or VM file in the Type of Data Source to Add section, and then click Next.
4. In the Select Data Source window, click the Browse button, navigate to your work folder, click Exiff.dd, and click Open. Then click Next.
5. In the Configure Ingest Modules window, you can select what type of processing you want, such as a hash lookup or an Exif parser . Leave the default selections, click Next, and then click Finish.
6. In the left pane of Autopsy’s main window, click to expand Extracted Content, if necessary, and then click EXIF Metadata. Examine the files displayed in the upper-right pane. As you scroll through these files, notice that the hexadecimal codes haven’t been altered. (In the e-mail Tom Johnson sent, the JFIF code was supposedly altered.)
7. Click the Keyword Search down arrow at the upper right. To verify that no other codes have been altered, you should check whether a change has been made to the FIF format. In the text box, type FIF (all uppercase letters), click the Exact Match option, and then click Search. There are no results. Next, type fif (all lowercase letters), click the Substring Search option, and then click Search. Your results should be similar to what’s shown below:

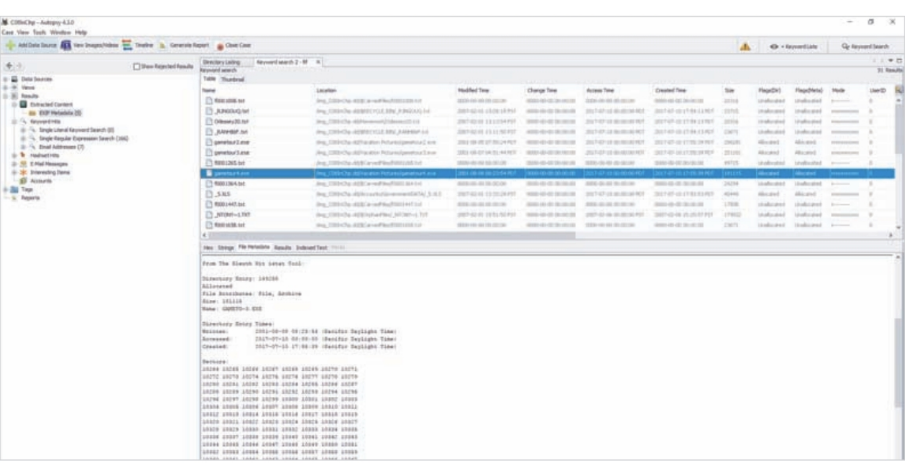


1. To view the changes made to the file header, you need to see the hexadecimal code. To do this, click the Hex tab in the lower-right pane, if necessary, and scroll down through the files until you see “zzzz” in the file header, as shown in the next figure. You should be viewing the gametour2.exe file.

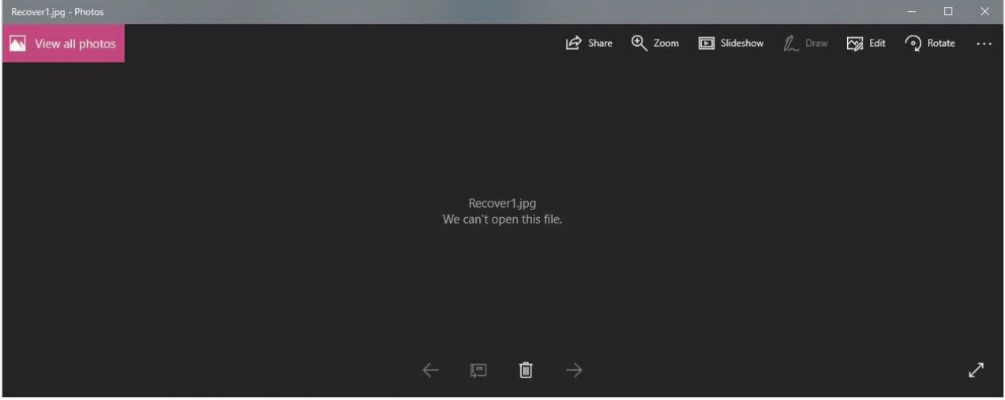


1. Click the File Metadata tab to view the written, accessed, and created dates and times along with the sectors used by the file. And record it here:

1. In the search results, right-click the gametour2.exe file and click Extract File(s). In the Save As dialog box, navigate to your work folder, type Recover1.jpg for the filename, and then click Save. Autopsy then creates an Export subfolder of your work folder to store this file. In the confirmation message box, click OK, and then exit Autopsy.

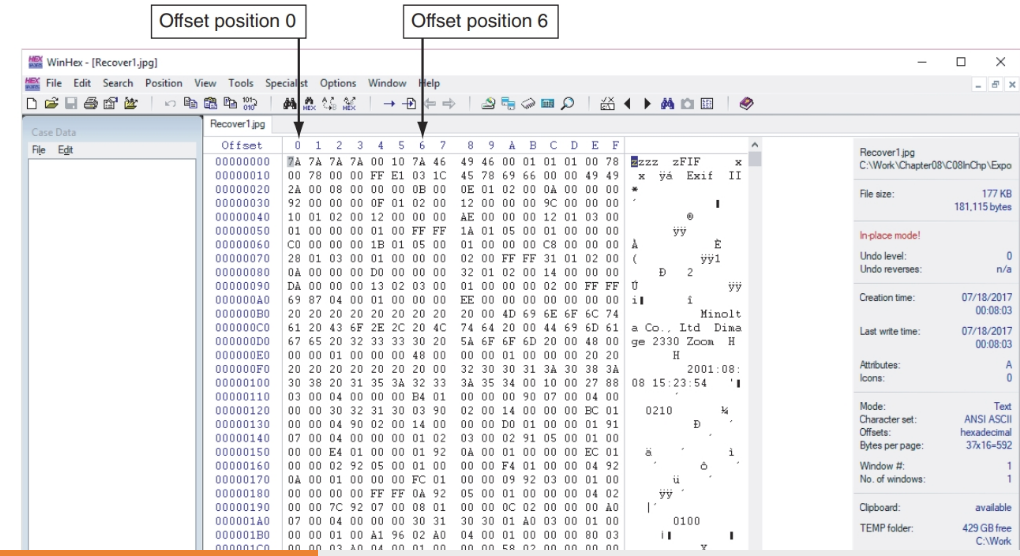


Before attempting to edit a graphics file you have recovered, try to open it with an image viewer, such as the default Microsoft tool. To test whether you can view the image, double-click the recovered file in its current location in File Explorer.



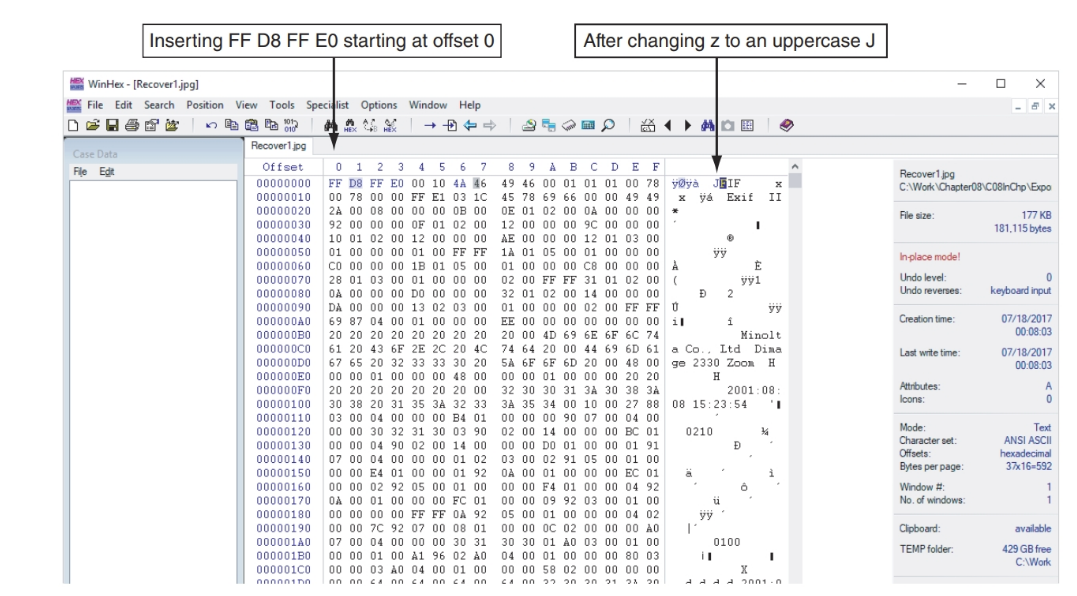
Because the deleted file you recovered in the previous activity, Recoverl.jpg, was altered intentionally, you might see an error message similar to below.

If you can’t open a graphics file in an image viewer, the next step is to examine the file’s header data to see whether it matches the header in a good JPEG file. If the header doesn’t match, you must insert the correct hexadecimal values manually with a hexadecimal editor. To inspect a file with WinHex, follow these steps:

1. Start WinHex , and click File, Open from the menu. Navigate to your work folder, and then double-click Recover1.jpg. If necessary, click OK. 
2. At the top of the WinHex window, notice that the hexadecimal values starting at the first byte position (offset 0) are 7A 7A 7A 7A, and the sixth position (offset 6) is also 7A.

As mentioned, a standard JFIF JPEG file has a header value of FF D8 FF E0 from offset 0 and the label name JFIF starting at offset 6. Using WinHex, you can correct this file header manually by following these steps:

1. In the center pane, click to the left of the first 7A hexadecimal value. Then type FF D8 FF E0, which are the correct hexadecimal values for the first 4 bytes of a JPEG file.
2. In the right pane at offset 6, click the z, and then type J, as shown



1. Click File, Save As from the menu. In the Save File As dialog box, navigate to your work folder, type Fixed1.jpg as the filename, and then click Save. If you’re using the demo version of WinHex, you get an error message because of the file size. Exit WinHex.
2. Please show Dr.Shumba what you have.

In this project, you continue examining the files found by IT staff at Superior Bicycles. In the in-chapter activity, you recovered three files containing zzzz for the first 4 bytes of altered JPEG files. These altered files had different extensions to hide the fact that they’re graphics files.

Find the C08carve.dd file. This image file is a new drive acquisition the IT staff made. The CEO 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 are on this drive.

1. Start Autopsy for Windows, and click the Create New Case button. In the New Case Information window, type C08carve in the Case Name text box, and click Next. In the Additional Information window, type the date in the Case Number text box and your name in the Examiner text box. Click Finish.
2. In the Select Data Source window, click the Browse button, navigate to your work folder, click c08carve.dd, and then click Open. Then click Next.
3. Expand the EXIF Metadata on the right.
4. Next, click the Keyword Search down arrow. In the text box, type zzzz, click the Exact Match option button, and then click Search.
5. Click each file in the search results to display its contents. If the file contains zzzz at the beginning of the sector, right-click the file, point to Tag Files, and click Tag and Comment. In the Comment text box, type Similar file, and then click OK.
6. Click the gametour5.exe file. Ctrl+click to select gametour1.exe, gametour2.exe, gametour3.exe, gametour4.exe, and gametour6.exe. Right-click the selection, point to Tag Files, and click Tag and Comment. In the Comment text box, type Additional similar files, and then click OK.
7. Click Generate Report. Click the Results - HTML option button, and then click Next. Click All Results, and then click Finish. Examine the results in the browser window, and then exit Autopsy.
8. What files have been similarly altered?

Dr. Shumba \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_