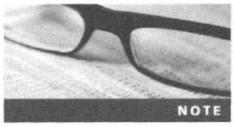
Planning Your Examination In the second e-mail from Jim Shu to Terry Sadler, Jim states, "So to view them you have to re-edit each file to the proper JPEG header of offset 0x FF D8 FF E0 and offset 6 of 4A." From this statement, you can assume that any kayak photographs on the USB drive contain unknown characters in the first four bytes and the sixth byte. Because this is all Jim Shu said about the JPEG files, you need to assume that the seventh, eighth, and ninth bytes have the original correct information for the JPEG file.

In "Examining the Exchangeable Image File Format," you learned the difference between a standard JFIF JPEG and an Exif JPEG file: The JFIF format has 0x FFD8 FFE0 in the first four bytes, and the Exif format has 0x FFD8 FFE1. In the sixth byte, the JPEG label is listed as JFIF or Exif. In the second e-mail, Jim Shu mentions 0x FF D8 FF E0, which is a JFIF JPEG format. He also says to change the sixth byte to 0x 4A, which is the uppercase letter "J" in ASCII.

Because the files might have been downloaded to the USB drive, Bob Aspen could have altered or deleted them, so 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. In the next section, you use ProDiscover to search for and recover these JPEG files.

Searching for and Recovering Digital Photograph Evidence In this section, you learn how to use ProDiscover to search for and extract (recover) possible evidence of JPEG files from the USB drive the EMTS manager gave you. The search string to use for this examination is "FIF." Because it's part of the label name of the JFIF JPEG format, you might have several false hits if the USB drive contains several other JPEG files. These false hits, referred to as **false positives**, require examining each search hit to verify whether it's what you are looking for.

The image file of the USB drive is included on the book's DVD. You should extract all files in the Chap08 folder on the DVD to your C:*Work*\Chap08\Chapter folder (referred to as your "work folder" in steps). Create this folder on your system first, if necessary.



Remember that the work folder you create most likely has a different name from what's shown in screenshots.

To begin the examination, follow these steps to load the image file:

1. Start ProDiscover Basic (with the **Run as administrator** option, if necessary), and click the **New Project** toolbar button. In the New Project dialog box, type **C08InChp** for the project number and filename, and then click **OK**.
2. *Click* **Action** *from the menu, point to* **Add**, and click **Image File**.

3. In the Open dialog box, navigate to your work folder, click **C08InChp.dd**, and then click **Open**.
4. To begin a search, click the **Search** toolbar button or click **Action**, **Search** from the menu to open the Search dialog box.
5. Click the **Cluster Search** tab, and then click the **Case Sensitive** check box. Under Search for the pattern(s), type **FIF** (see Figure 8-7). Under Select the Disk(s)/Image(s) you want to search in, click the **C08InChp.dd** file, and then click **OK**.

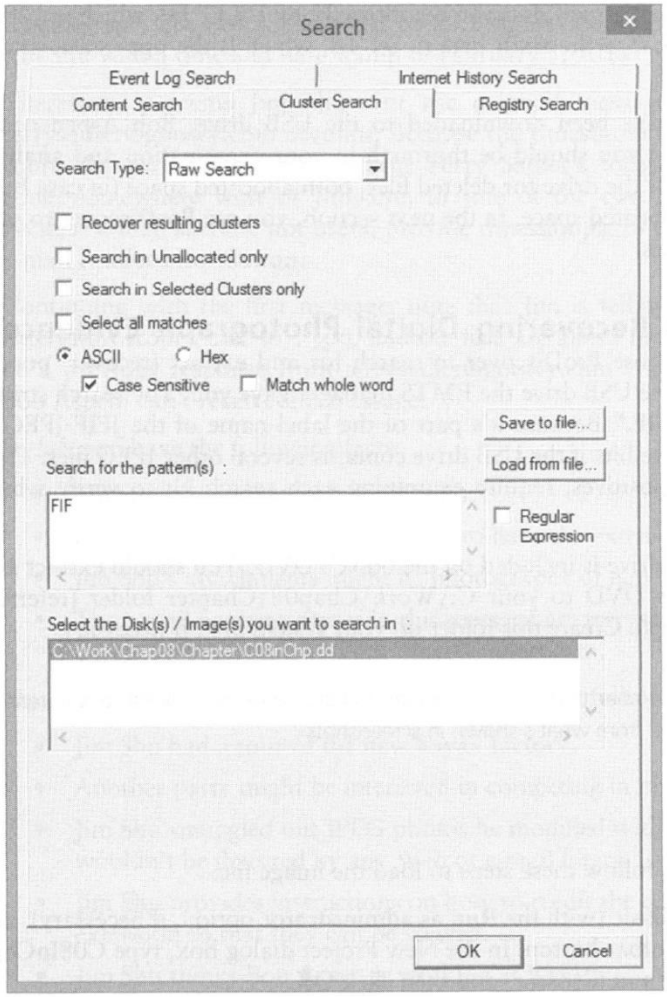


Figure 8-7 Searching clusters in ProDiscover
Courtesy of Technology Pathways, LLC

6. When the search is done, click the search hit, **AC4(2756)**, to display the cluster's content (see Figure 8-8).

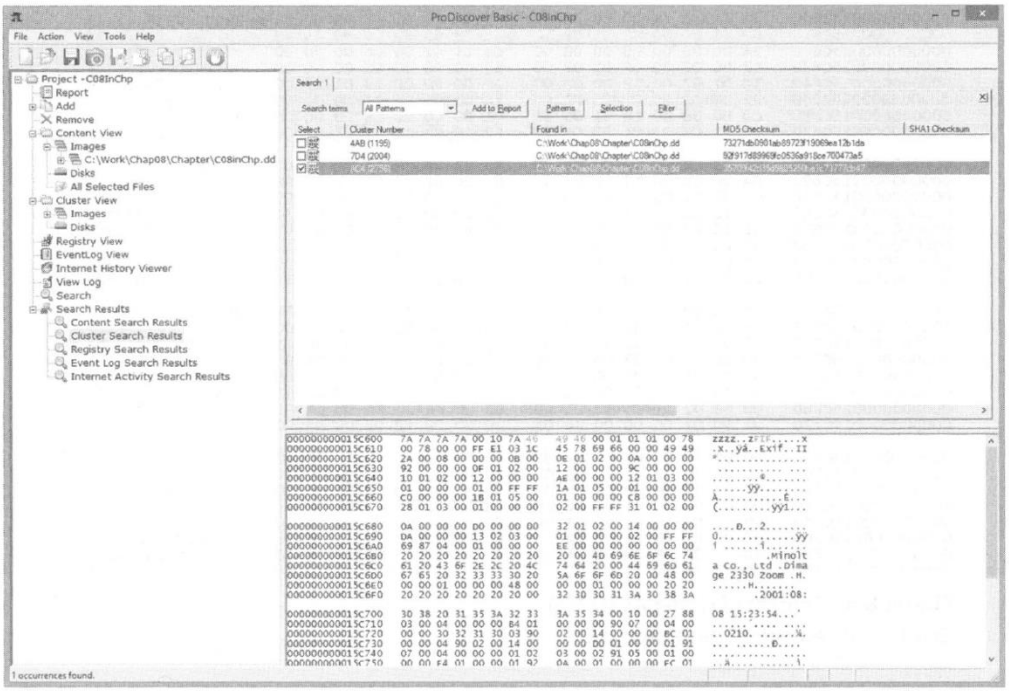


Figure 8-8 Completed cluster search for FIF
Courtesy of Technology Pathways, LLC

In Figure 8-9, the header for this JPEG file has been overwritten with zzzz. This unique header information might give you additional search values that could minimize false-positive hits in subsequent searches.

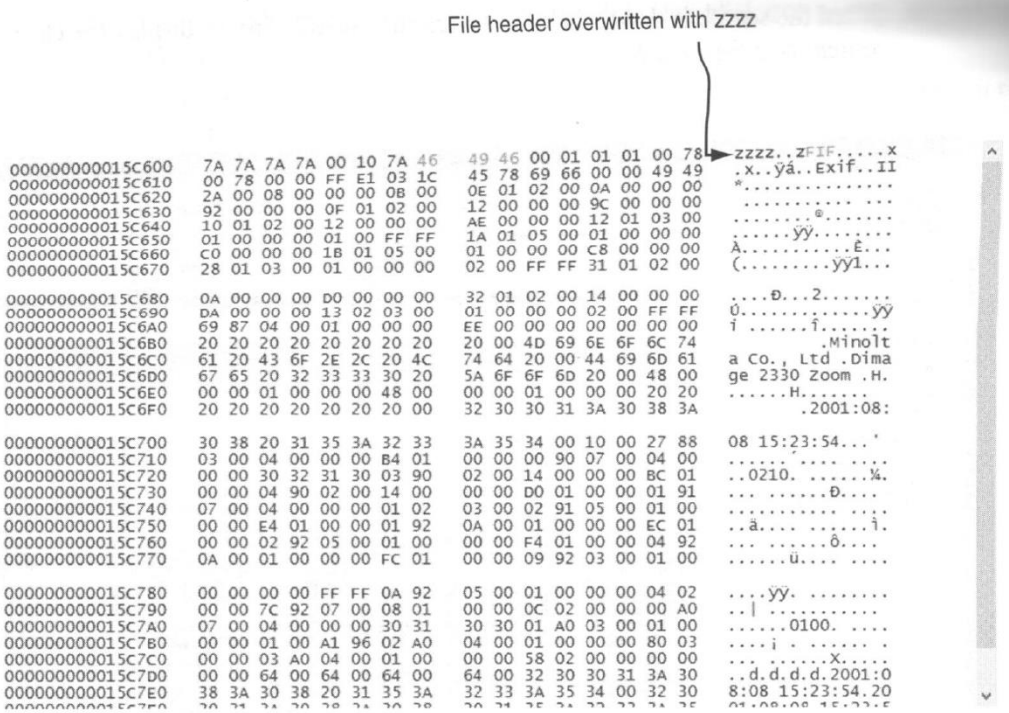


Figure 8-9 Content of cluster AC4(2756)
Courtesy of Technology Pathways, LLC

7. Next, locate the file by right-clicking cluster number **AC4(2756)** and clicking **Find File**, and then click **Yes** in the warning message.
8. In the List of Clusters dialog box, click **Show File** (see Figure 8-10), and then click **Close**.

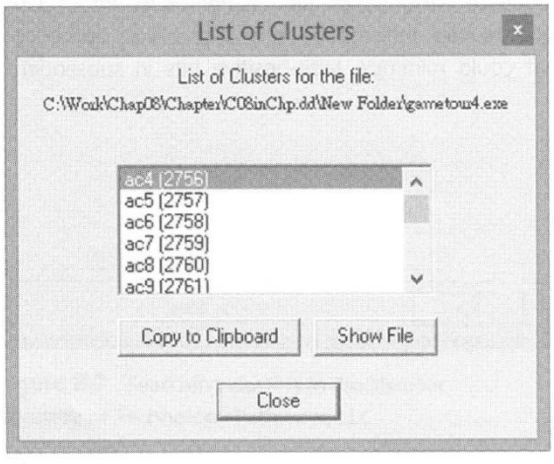


Figure 8-10 Viewing all clusters used by the `gametour4.exe` file
Courtesy of Technology Pathways, LLC

9. In the work area, right-click the **gametour4.exe** file (see Figure 8-11) and click **Copy File**. In the Save As dialog box, navigate to your work folder, type **Recover1.jpg** for the filename, and then click **Save**.

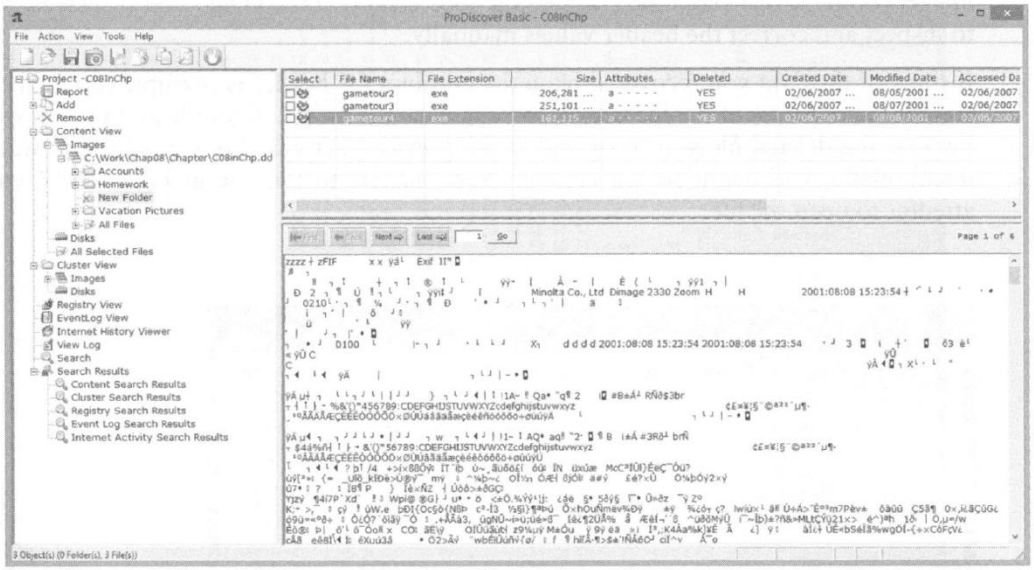


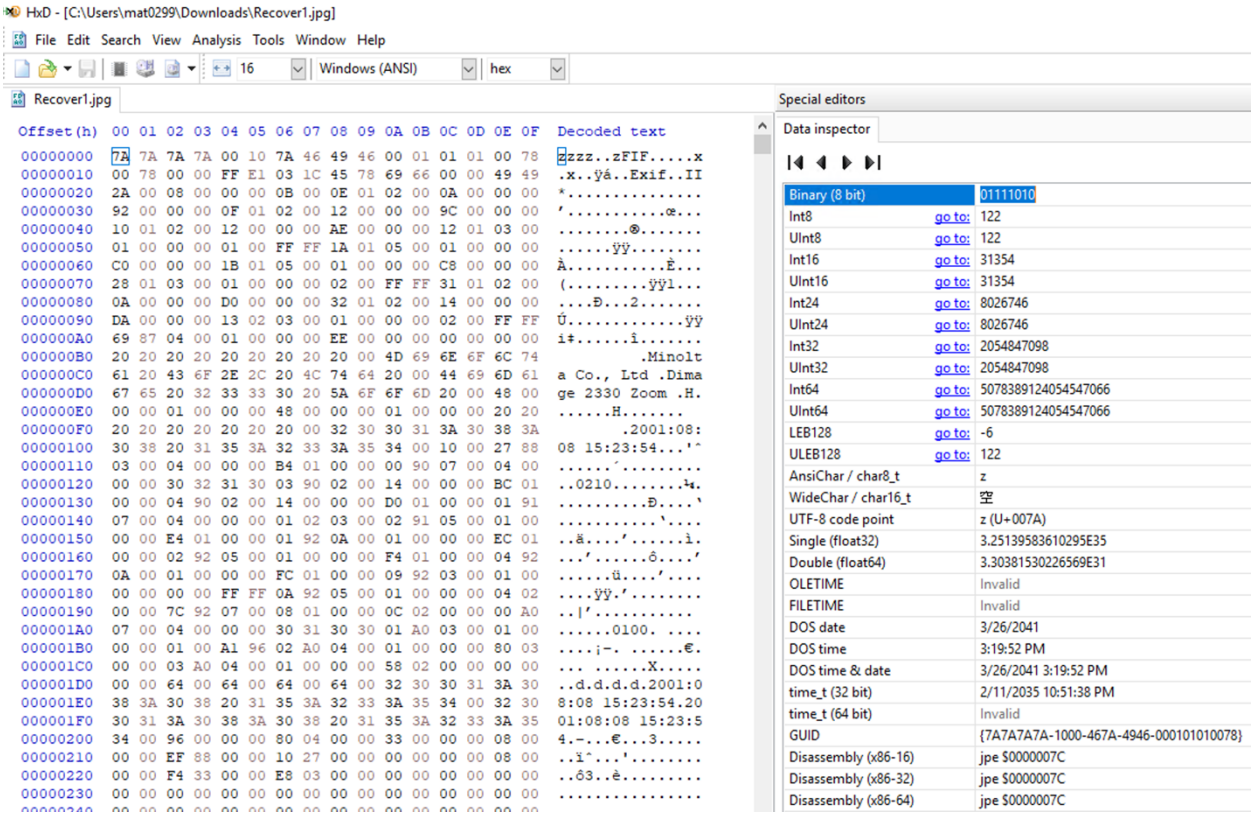
Figure 8-11 Mislabeled file that appears to be altered intentionally
Courtesy of Technology Pathways, LLC

10. Click **File, Exit** from the menu, and then click **Yes** and **Save** to save this project in your work folder.

If, after saving the file as **`Recover1.jpg`**, it still appears as **`gametour4.exe`**, you can simply rename it as **`Recover1.jpg`** in Windows File Explorer.

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 in HxD, follow these steps.

1. Start HxD, and click **File, Open** from the menu. Navigate to your work folder, and then double-click **`Recover1.jpg`**. If necessary, click **OK**. The following figure shows this file open in HxD.

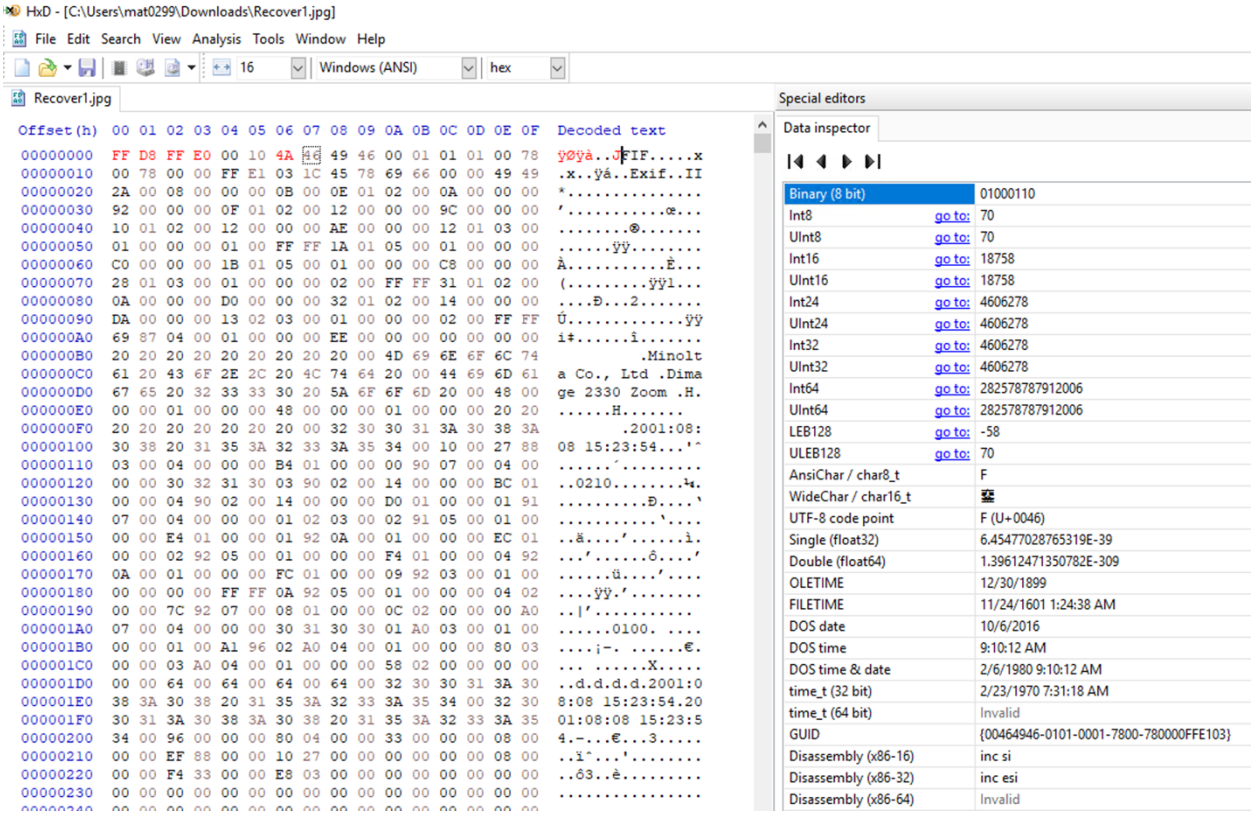


2. At the top of the HxD window, notice that the hexadecimal values starting at the first byte position (offset 0) are 7A 7A 7A 7A, and the sixth position (offset 6) is also 7A. Leave HxD open for the next activity.

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 HxD, you can correct this file header manually by the following steps:

1. In the center section of the left 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.

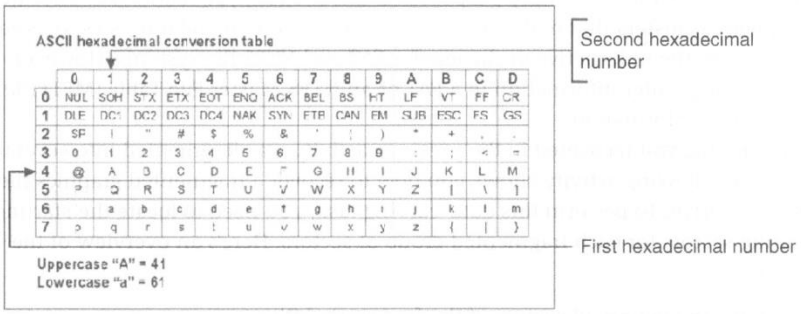
2. In the right section of the left pane under the *Decoded text* heading where the last remaining **z** is found on the top line of data, click to the left of the **z**. Then type **J** as shown below.



3. Click **File, Save As** from the menu. In the *Save As* dialog box, navigate to your work folder, type **`Fixed1.jpg`** as the filename, and then click **Save**. Exit HxD.

After you repair a graphics file header, you can test the updated file by opening it in an image viewer, such as Windows Photo Viewer, IrfanView, ThumbsPlus, QuickView, or ACDSee. If the file displays the image, as shown in Figure 8-16, you have performed the recovery correctly.

Every two hexadecimal values you entered in the previous steps are equivalent to one ASCII character. For example, an uppercase "A" has the hexadecimal value 41, and a lowercase "a" has the hexadecimal value 61. Most disk editors have a reference chart for converting hexadecimal values to ASCII characters, such as in Figure 8-15.



	0	1	2	3	4	5	6	7	8	9	A	B	C	D
0	NUL	SOH	STX	ETX	EOT	ENQ	ACK	BEL	BS	HT	LF	VT	FF	CR
1	DLE	DC1	DC2	DC3	DC4	NAK	SYN	ETB	CAN	EM	SUB	ESC	FS	GS
2	SP	!	"	#	$	%	&	'	(	)	*	+	,	-
3	0	1	2	3	4	5	6	7	8	9	:	;	<	=
4	@	A	B	C	D	E	F	G	H	I	J	K	L	M
5	P	Q	R	S	T	U	V	W	X	Y	Z	[	\	]
6	`	a	b	c	d	e	f	g	h	i	j	k	l	m
7	p	q	r	s	t	u	v	w	x	y	z	{	|	}

Figure 8-15 ASCII equivalents of hexadecimal values

After you repair a graphics file header, you can test the updated file by opening it in an image viewer, such as Windows Photo Viewer, IrfanView, ThumbsPlus, QuickView, or ACDSee. If the file displays the image, as shown in Figure 8-16, you have performed the recovery correctly.

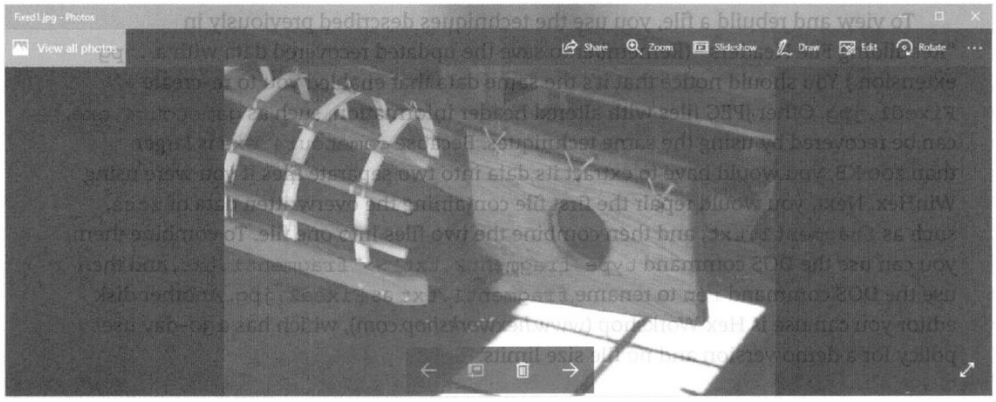


Figure 8-16 `Fixed1.jpg` open in an image viewer

The process of repairing file headers isn't limited to JPEG files. You can apply the same technique to any file you can determine the header value for, including Microsoft Word, Excel, and PowerPoint documents and other image formats. You need to know only the correct header format for the type of file you're attempting to repair.

You are to submit the repaired **`Fixed1.jpg`** file to the **Participation Activity 5** dropbox on Canvas by the due date and time. **No late submissions will be accepted.**