Guide to Computer Forensics and Investigations
Sixth Edition

Chapter 8

Recovering Graphics Files

CENGAGE

Objectives

- Describe types of graphics file formats
- Explain types of data compression
- Explain how to locate and recover graphics files
- Describe how to identify unknown file formats
- Explain copyright issues with graphics

Recognizing a Graphics File

- Graphic files contain digital photographs, line art, three-dimensional images, text data converted to images, and scanned replicas of printed pictures
  - **Bitmap images**: collection of dots
  - **Vector graphics**: based on mathematical instructions
  - **Metafile graphics**: combination of bitmap and vector
- Types of programs
  - Graphics editors
  - Image viewers

Understanding Bitmap and Raster Images

- Bitmap images
  - Grids of individual **pixels**
- **Raster images** - also collections of pixels
  - Pixels are stored in rows
  - Better for printing
- Image quality
  - Screen **resolution** - determines amount of detail
  - Software contributes to image quality (drivers)
  - Number of color bits used per pixel

Understanding Vector Graphics

- Characteristics of vector graphics
  - Uses lines instead of dots
  - Store only the calculations for drawing lines and shapes
  - Smaller than bitmap files
  - Preserve quality when image is enlarged
- CorelDRAW, Adobe Illustrator

Understanding Metafile Graphics

- Metafile graphics combine raster and vector graphics
- Example
  - Scanned photo (bitmap) with text or arrows (vector)
- Share advantages and disadvantages of both types
  - When enlarged, bitmap part loses quality

Understanding Graphics File Formats (1 of 2)

- **Standard graphics file formats**
  - Standard bitmap file formats
    - Portable Network Graphic (.png)
    - Graphic Interchange Format (.gif)
    - Joint Photographic Experts Group (.jpeg, .jpg)
    - Tagged Image File Format (.tiff, .tif)
    - Window Bitmap (.bmp)
  - Standard vector file formats
    - Hewlett Packard Graphics Language (.hpgl)
    - Autocad (.dxf)

Understanding Graphics File Formats (2 of 2)

- **Nonstandard graphics file formats**
  - Targa (.tga)
  - Raster Transfer Language (.rtl)
  - Adobe Photoshop (.psd) and Illustrator (.ai)
  - Freehand (.fh11)
  - Scalable Vector Graphics (.svg)
  - Paintbrush (.pcx)
- Search the Web for software to manipulate unknown image formats

Understanding Digital Photograph File Formats (1 of 8)

- Witnesses or suspects can create their own digital photos
- Examining the raw file format
  - **Raw file format**
    - Referred to as a digital negative
    - Typically found on many higher-end digital cameras
  - Sensors in the digital camera simply record pixels on the camera’s memory card
  - Raw format maintains the best picture quality

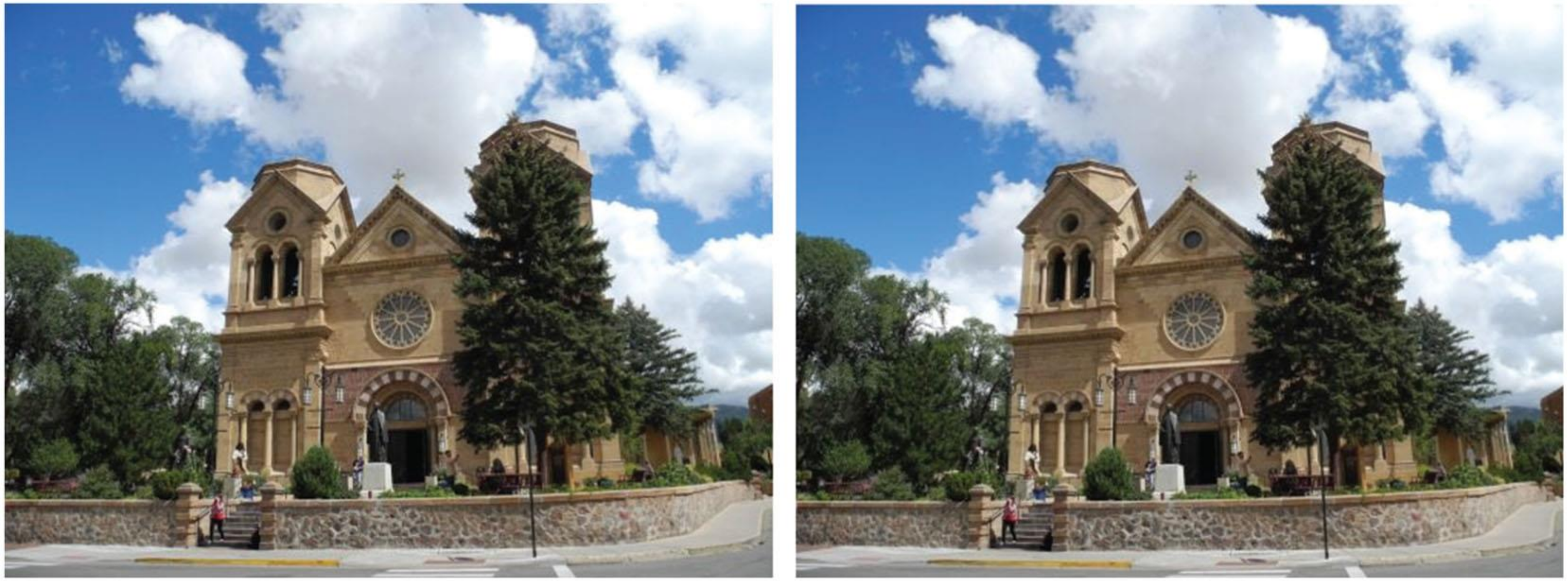
Understanding Digital Photograph File Formats (2 of 8)

- Examining the raw file format (cont'd)
  - The biggest disadvantage is that it's proprietary
    - And not all image viewers can display these formats
  - The process of converting raw picture data to another format is referred to as **demosaicing**
- Examining the Exchangeable Image File format
  - **Exchangeable Image File (Exif)** format
    - Commonly used to store digital pictures
    - Developed by JEITA as a standard for storing metadata in JPEG and TIF files

Understanding Digital Photograph File Formats (3 of 8)

- Examining the Exchangeable Image File format (cont'd)
  - Exif format collects metadata
    - Investigators can learn more about the type of digital device and the environment in which photos were taken
  - Viewing an Exif JPEG file's metadata requires special programs
    - Exif Reader, IrfanView, or Magnet Forensics AXIOM
  - Exif file stores metadata at the beginning of the file

Understanding Digital Photograph File Formats (4 of 8)

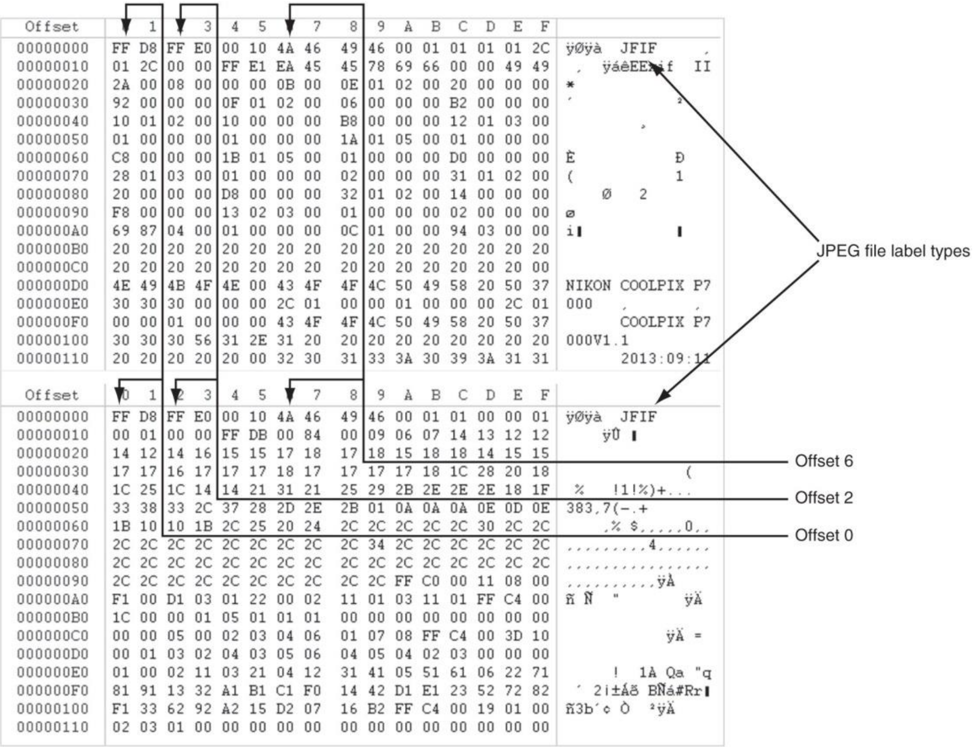


Exif picture file

JPEG picture file

Figure 8-1 **Similar Exif and JPEG photos**

Understanding Digital Photograph File Formats (5 of 8)



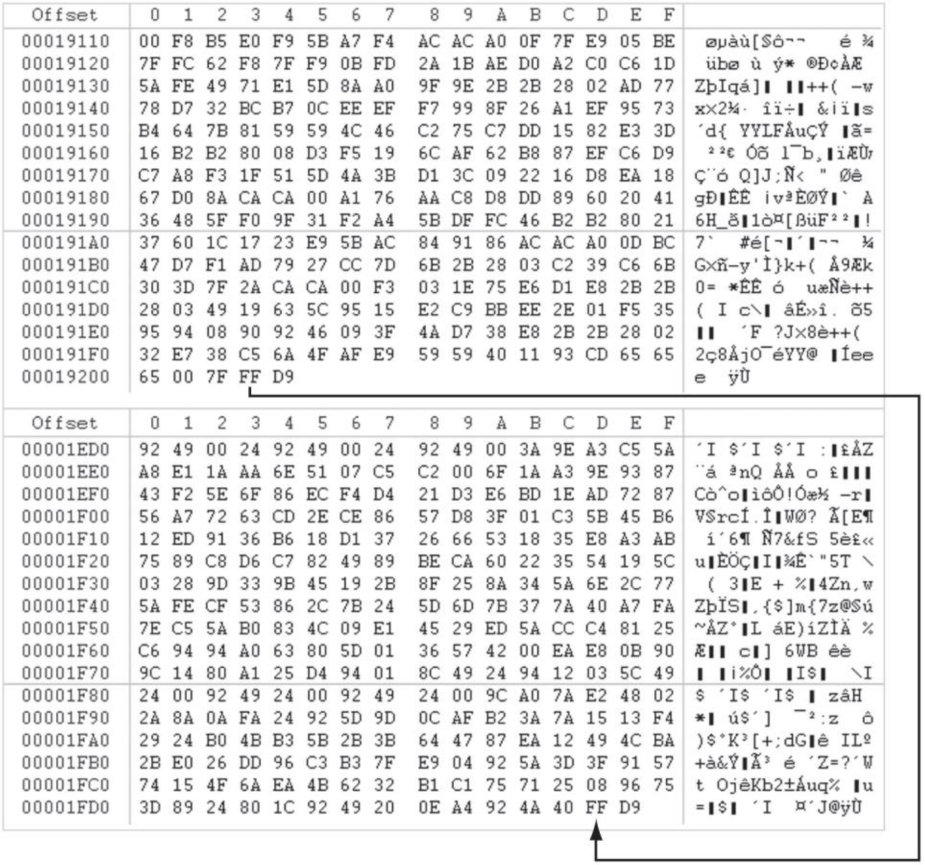
```
 Offset    0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
00000000  FF D8 FF E0 00 10 4A 46  49 46 00 01 01 01 01 2C  ÿØÿà  JFIF      ,
00000010  01 2C 00 00 FF E1 EA 45  45 78 69 66 00 00 49 49   ,   ÿáêEExif   II
00000020  2A 00 08 00 00 00 0B 00  0E 01 02 00 20 00 00 00  *
00000030  92 00 00 00 0F 01 02 00  06 00 00 00 B2 00 00 00  ´          ²
00000040  10 01 02 00 10 00 00 00  B8 00 00 00 12 01 03 00            ¸
00000050  01 00 00 00 01 00 00 00  1A 01 05 00 01 00 00 00
00000060  C8 00 00 00 1B 01 05 00  01 00 00 00 D0 00 00 00  È          Ð
00000070  28 01 03 00 01 00 00 00  02 00 00 00 31 01 02 00  (          1
00000080  20 00 00 00 D8 00 00 00  32 01 02 00 14 00 00 00      Ø   2
00000090  F8 00 00 00 13 02 03 00  01 00 00 00 02 00 00 00  ø
000000A0  69 87 04 00 01 00 00 00  0C 01 00 00 94 03 00 00  i▌         ▌
000000B0  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
000000C0  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 00
000000D0  4E 49 4B 4F 4E 00 43 4F  4F 4C 50 49 58 20 50 37  NIKON COOLPIX P7
000000E0  30 30 30 00 00 00 2C 01  00 00 01 00 00 00 2C 01  000   ,     ,
000000F0  00 00 01 00 00 00 43 4F  4F 4C 50 49 58 20 50 37        COOLPIX P7
00000100  30 30 30 56 31 2E 31 20  20 20 20 20 20 20 20 20  000V1.1
00000110  20 20 20 20 20 00 32 30  31 33 3A 30 39 3A 31 31        2013:09:11

 Offset    0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
00000000  FF D8 FF E0 00 10 4A 46  49 46 00 01 01 00 00 01  ÿØÿà  JFIF
00000010  00 01 00 00 FF DB 00 84  00 09 06 07 14 13 12 12      ÿÛ ▌
00000020  14 12 14 16 15 15 17 18  17 18 15 18 18 14 15 15
00000030  17 17 16 17 17 17 18 17  17 17 17 18 1C 28 20 18              (
00000040  1C 25 1C 14 14 21 31 21  25 29 2B 2E 2E 2E 18 1F   %    !1!%)+...
00000050  33 38 33 2C 37 28 2D 2E  2B 01 0A 0A 0A 0E 0D 0E  383,7(-.+
00000060  1B 10 10 1B 2C 25 20 24  2C 2C 2C 2C 2C 30 2C 2C      ,% $,,,,,0,,
00000070  2C 2C 2C 2C 2C 2C 2C 2C  2C 34 2C 2C 2C 2C 2C 2C  ,,,,,,,,,4,,,,,,
00000080  2C 2C 2C 2C 2C 2C 2C 2C  2C 2C 2C 2C 2C 2C 2C 2C  ,,,,,,,,,,,,,,,,
00000090  2C 2C 2C 2C 2C 2C 2C 2C  2C 2C FF C0 00 11 08 00  ,,,,,,,,,,ÿÀ
000000A0  F1 00 D1 03 01 22 00 02  11 01 03 11 01 FF C4 00  ñ Ñ  "       ÿÄ
000000B0  1C 00 00 01 05 01 01 01  00 00 00 00 00 00 00 00
000000C0  00 00 05 00 02 03 04 06  01 07 08 FF C4 00 3D 10             ÿÄ =
000000D0  00 01 03 02 04 03 05 06  04 05 04 02 03 00 00 00
000000E0  01 00 02 11 03 21 04 12  31 41 05 51 61 06 22 71       !  1A Qa "q
000000F0  81 91 13 32 A1 B1 C1 F0  14 42 D1 E1 23 52 72 82   ´ 2¡±Áð BÑá#Rr▌
00000100  F1 33 62 92 A2 15 D2 07  16 B2 FF C4 00 19 01 00  ñ3b´¢ Ò  ²ÿÄ
00000110  02 03 01 00 00 00 00 00  00 00 00 00 00 00 00 00
```

Figure 8-2 Differences in Exif and JPEG file header information

Source: X-Ways AG, *www.x-ways.net*

Understanding Digital Photograph File Formats (6 of 8)



```
Offset     0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
00019110  00 F8 B5 E0 F9 5B A7 F4  AC AC A0 0F 7F E9 05 BE   øµàù[§ô¬¬   é ¾
00019120  7F FC 62 F8 7F F9 0B FD  2A 1B AE D0 A2 C0 C6 1D   übø ù ý* ®Ð¢ÀÆ
00019130  5A FE 49 71 E1 5D 8A A0  9F 9E 2B 2B 28 02 AD 77  ZþIqá]▮ ▮▮++( -w
00019140  78 D7 32 BC B7 0C EE EF  F7 99 8F 26 A1 EF 95 73  x×2¼· îï÷▮ &¡ï▮s
00019150  B4 64 7B 81 59 59 4C 46  C2 75 C7 DD 15 82 E3 3D  ´d{ YYLFÂuÇÝ ▮ã=
00019160  16 B2 B2 80 08 D3 F5 19  6C AF 62 B8 87 EF C6 D9   ²²€ Óõ l¯b¸▮ïÆÙ
00019170  C7 A8 F3 1F 51 5D 4A 3B  D1 3C 09 22 16 D8 EA 18  Ç¨ó Q]J;Ñ< " Øê
00019180  67 D0 8A CA CA 00 A1 76  AA C8 D8 DD 89 60 20 41  gÐ▮ÊÊ ¡vªÈØÝ▮` A
00019190  36 48 5F F0 9F 31 F2 A4  5B DF FC 46 B2 B2 80 21  6H_ð▮1ò¤[ßüF²²▮!
000191A0  37 60 1C 17 23 E9 5B AC  84 91 86 AC AC A0 0D BC  7`  #é[¬▮´▮¬¬  ¼
000191B0  47 D7 F1 AD 79 27 CC 7D  6B 2B 28 03 C2 39 C6 6B  G×ñ-y'Ì}k+( Â9Æk
000191C0  30 3D 7F 2A CA CA 00 F3  03 1E 75 E6 D1 E8 2B 2B  0= *ÊÊ ó  uæÑè++
000191D0  28 03 49 19 63 5C 95 15  E2 C9 BB EE 2E 01 F5 35  ( I c\▮ âÉ»î. õ5
000191E0  95 94 08 90 92 46 09 3F  4A D7 38 E8 2B 2B 28 02  ▮▮  ´F ?J×8è++(
000191F0  32 E7 38 C5 6A 4F AF E9  59 59 40 11 93 CD 65 65  2ç8ÅjO¯éYY@ ▮Íee
00019200  65 00 7F FF D9                                     e  ÿÙ

Offset     0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
00001ED0  92 49 00 24 92 49 00 24  92 49 00 3A 9E A3 C5 5A  ´I $´I $´I :▮£ÅZ
00001EE0  A8 E1 1A AA 6E 51 07 C5  C2 00 6F 1A A3 9E 93 87  ¨á ªnQ ÅÂ o £▮▮▮
00001EF0  43 F2 5E 6F 86 EC F4 D4  21 D3 E6 BD 1E AD 72 87  Cò^o▮ìôÔ!Óæ½ -r▮
00001F00  56 A7 72 63 CD 2E CE 86  57 D8 3F 01 C3 5B 45 B6  V§rcÍ.Î▮WØ? Ã[E¶
00001F10  12 ED 91 36 B6 18 D1 37  26 66 53 18 35 E8 A3 AB   í´6¶ Ñ7&fS 5è£«
00001F20  75 89 C8 D6 C7 82 49 89  BE CA 60 22 35 54 19 5C  u▮ÈÖÇ▮I▮¾Ê`"5T \
00001F30  03 28 9D 33 9B 45 19 2B  8F 25 8A 34 5A 6E 2C 77   ( 3▮E + %▮4Zn,w
00001F40  5A FE CF 53 86 2C 7B 24  5D 6D 7B 37 7A 40 A7 FA  ZþÏS▮,{$]m{7z@§ú
00001F50  7E C5 5A B0 83 4C 09 E1  45 29 ED 5A CC C4 81 25  ~ÅZ°▮L áE)íZÌÄ %
00001F60  C6 94 94 A0 63 80 5D 01  36 57 42 00 EA E8 0B 90  Æ▮▮ c▮] 6WB êè
00001F70  9C 14 80 A1 25 D4 94 01  8C 49 24 94 12 03 5C 49  ▮ ▮¡%Ô▮ ▮I$▮  \I
00001F80  24 00 92 49 24 00 92 49  24 00 9C A0 7A E2 48 02  $ ´I$ ´I$ ▮ zâH
00001F90  2A 8A 0A FA 24 92 5D 9D  0C AF B2 3A 7A 15 13 F4  *▮ ú$´]  ¯²:z  ô
00001FA0  29 24 B0 4B B3 5B 2B 3B  64 47 87 EA 12 49 4C BA  )$°K³[+;dG▮ê ILº
00001FB0  2B E0 26 DD 96 C3 B3 7F  E9 04 92 5A 3D 3F 91 57  +à&Ý▮Ã³ é ´Z=?´W
00001FC0  74 15 4F 6A EA 4B 62 32  B1 C1 75 71 25 08 96 75  t OjêKb2±Áuq% ▮u
00001FD0  3D 89 24 80 1C 92 49 20  0E A4 92 4A 40 FF D9     =▮$▮ ´I  ¤´J@ÿÙ
```

JPEG file EOI marker

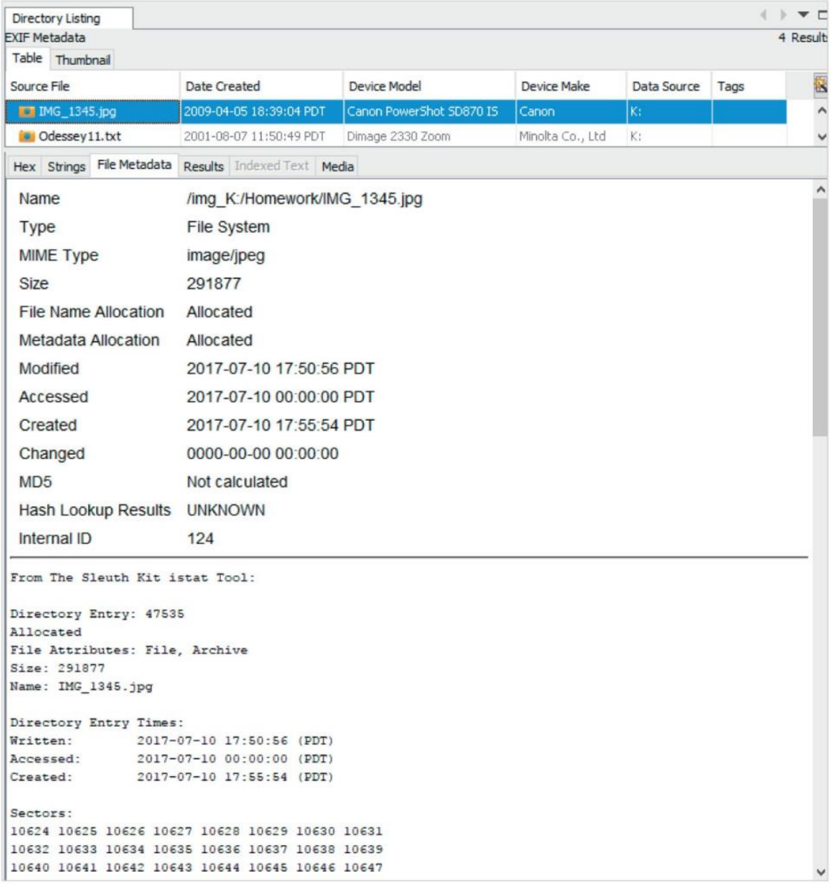
Figure 8-3 EOI marker FFD9 for all JPEG files

Source: X-Ways AG, *www.x-ways.net*

Understanding Digital Photograph File Formats (7 of 8)

- Examining the Exchangeable Image File format (cont'd)
  - With tools such as Autopsy and Exif Reader
    - You can extract metadata as evidence for your case

Understanding Digital Photograph File Formats (8 of 8)



Source File	Date Created	Device Model	Device Make	Data Source	Tags
IMG_1345.jpg	2009-04-05 18:39:04 PDT	Canon PowerShot SD870 IS	Canon	K:	
Odessey11.txt	2001-08-07 11:50:49 PDT	Dimage 2330 Zoom	Minolta Co., Ltd	K:	

Name	/img_K:/Homework/IMG_1345.jpg
Type	File System
MIME Type	image/jpeg
Size	291877
File Name Allocation	Allocated
Metadata Allocation	Allocated
Modified	2017-07-10 17:50:56 PDT
Accessed	2017-07-10 00:00:00 PDT
Created	2017-07-10 17:55:54 PDT
Changed	0000-00-00 00:00:00
MD5	Not calculated
Hash Lookup Results	UNKNOWN
Internal ID	124

```
From The Sleuth Kit istat Tool:

Directory Entry: 47535
Allocated
File Attributes: File, Archive
Size: 291877
Name: IMG_1345.jpg

Directory Entry Times:
Written:        2017-07-10 17:50:56 (PDT)
Accessed:       2017-07-10 00:00:00 (PDT)
Created:        2017-07-10 17:55:54 (PDT)

Sectors:
10624 10625 10626 10627 10628 10629 10630 10631
10632 10633 10634 10635 10636 10637 10638 10639
10640 10641 10642 10643 10644 10645 10646 10647
```

Figure 8-4 Autopsy displaying metadata from an Exif JPEG file

Source: *www.sleuthkit.org*

Understanding Data Compression

- Most graphics file formats compress their data
  - GIF and JPEG
- Others, like BMP, do not compress their data
  - Use data compression tools for those formats
- **Data compression**
  - Coding data from a larger to a smaller form
  - Types
    - Lossless compression and lossy compression

Lossless and Lossy Compression

- **Lossless compression**
  - Reduces file size without removing data
  - Based on Huffman or Lempel-Ziv-Welch coding
    - For redundant bits of data
  - Utilities: WinZip, PKZip, StuffIt, and FreeZip
- **Lossy compression**
  - Permanently discards bits of information
  - **Vector quantization (VQ)**
    - Determines what data to discard based on vectors in the graphics file
  - Utility: Lzip

Locating and Recovering Graphics Files

- Operating system tools
  - Time consuming
  - Results are difficult to verify
- Digital forensics tools
  - Image headers
    - Compare them with good header samples
    - Use header information to create a baseline analysis
  - Reconstruct fragmented image files
    - Identify data patterns and modified headers

Identifying Graphics File Fragments

- **Carving** or **salvaging**
  - Recovering any type of file fragments
- Digital forensics tools
  - Can carve from file slack and free space
  - Help identify image files fragments and put them together

CENGAGE

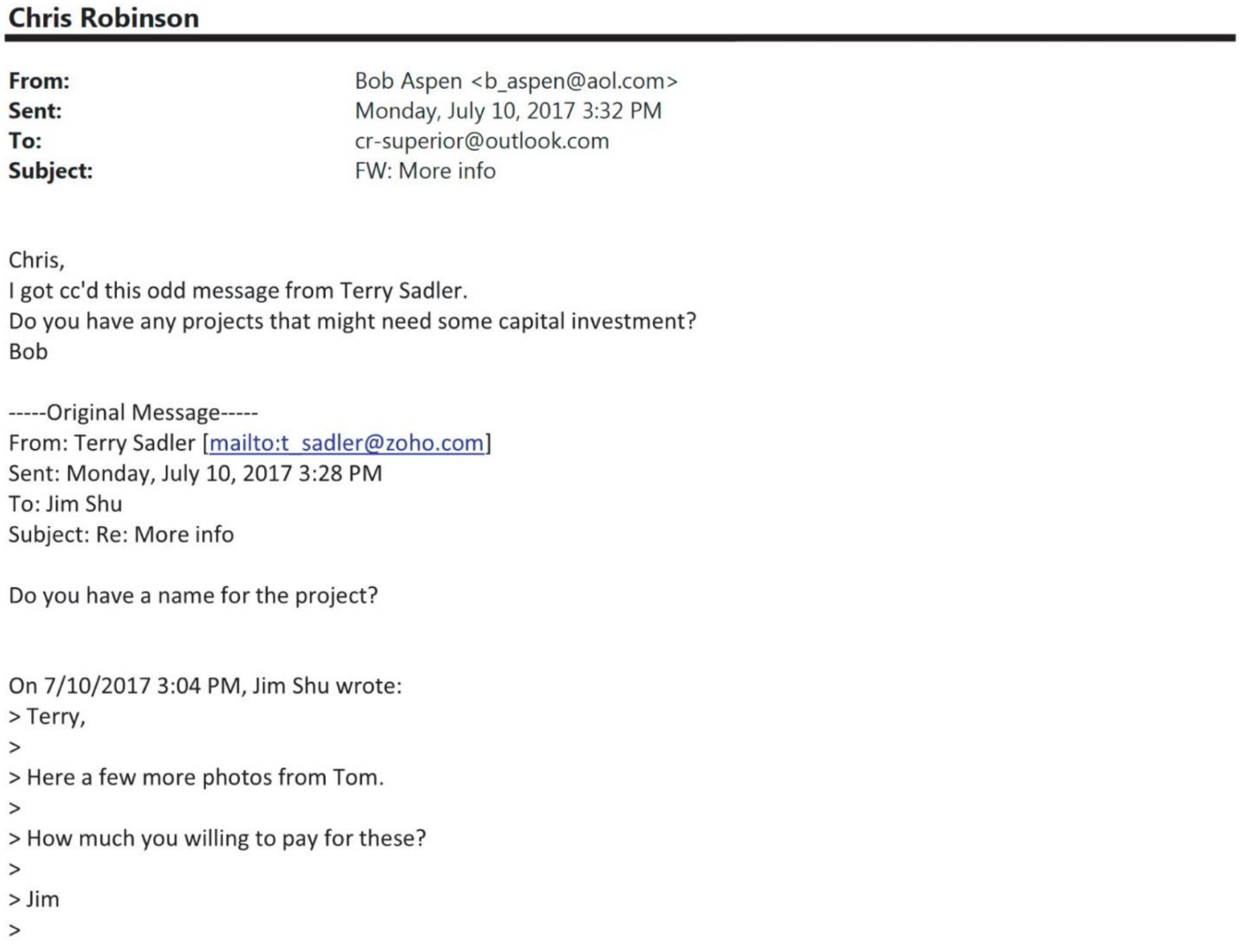
Repairing Damaged Headers (1 of 4)

- When examining recovered fragments from files in slack or free space
  - You might find data that appears to be a header
- If header data is 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 found

Repairing Damaged Headers (2 of 4)

- Each graphics file has a unique header value
- Example:
  - A JPEG file has the hexadecimal header value FFD8, followed by the label JFIF for a standard JPEG or Exif file at offset 6
- Exercise:
  - Investigate a possible intellectual property theft by a new employee of Superior Bicycles, Inc.

Repairing Damaged Headers (3 of 4)



Chris Robinson

From: Bob Aspen <b_aspen@aol.com>
Sent: Monday, July 10, 2017 3:32 PM
To: cr-superior@outlook.com
Subject: FW: More info

Chris,
I got cc'd this odd message from Terry Sadler.
Do you have any projects that might need some capital investment?
Bob

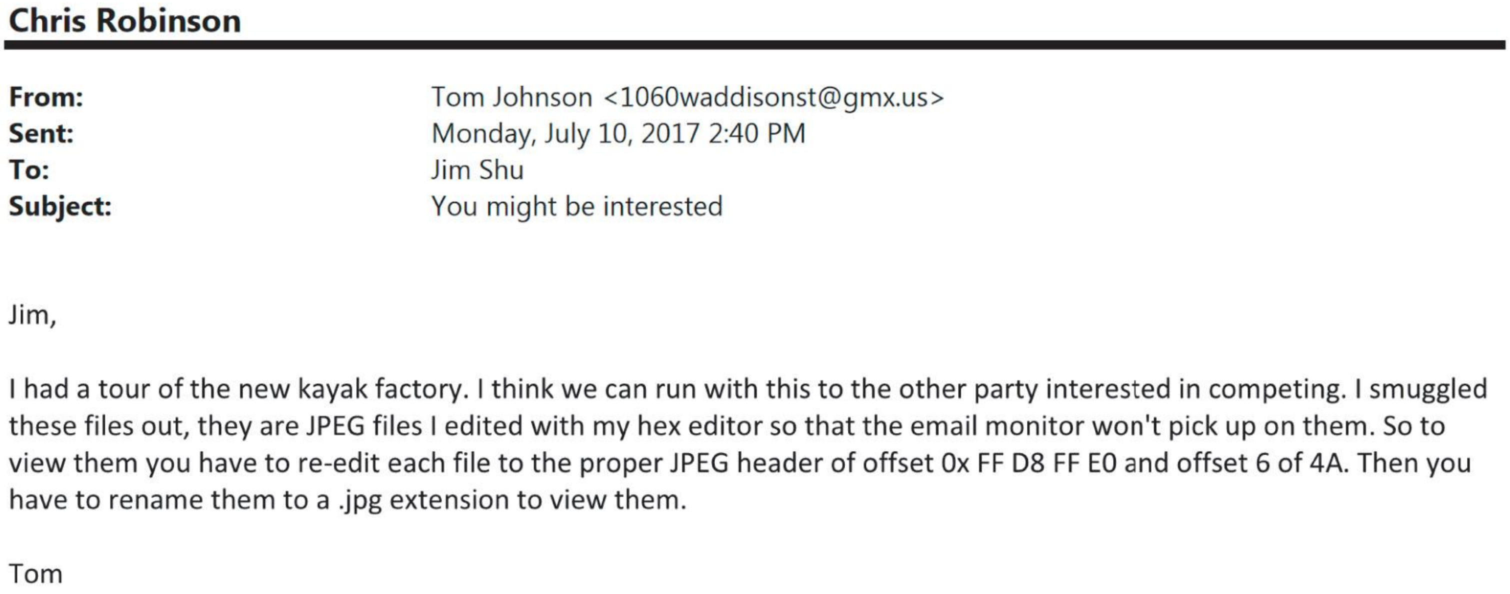
-----Original Message-----
From: Terry Sadler [mailto:t_sadler@zoho.com]
Sent: Monday, July 10, 2017 3:28 PM
To: Jim Shu
Subject: Re: More info

Do you have a name for the project?

On 7/10/2017 3:04 PM, Jim Shu wrote:
> Terry,
>
> Here a few more photos from Tom.
>
> How much you willing to pay for these?
>
> Jim
>

Figure 8-5 An e-mail from Terry Sadler

Repairing Damaged Headers (4 of 4)



Chris Robinson

From:	Tom Johnson <1060waddisonst@gmx.us>
Sent:	Monday, July 10, 2017 2:40 PM
To:	Jim Shu
Subject:	You might be interested

Jim,

I had a tour of the new kayak factory. I think we can run with this to the other party interested in competing. I smuggled these files out, they are JPEG files I edited with my hex editor so that the email monitor won't pick up on them. 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. Then you have to rename them to a .jpg extension to view them.

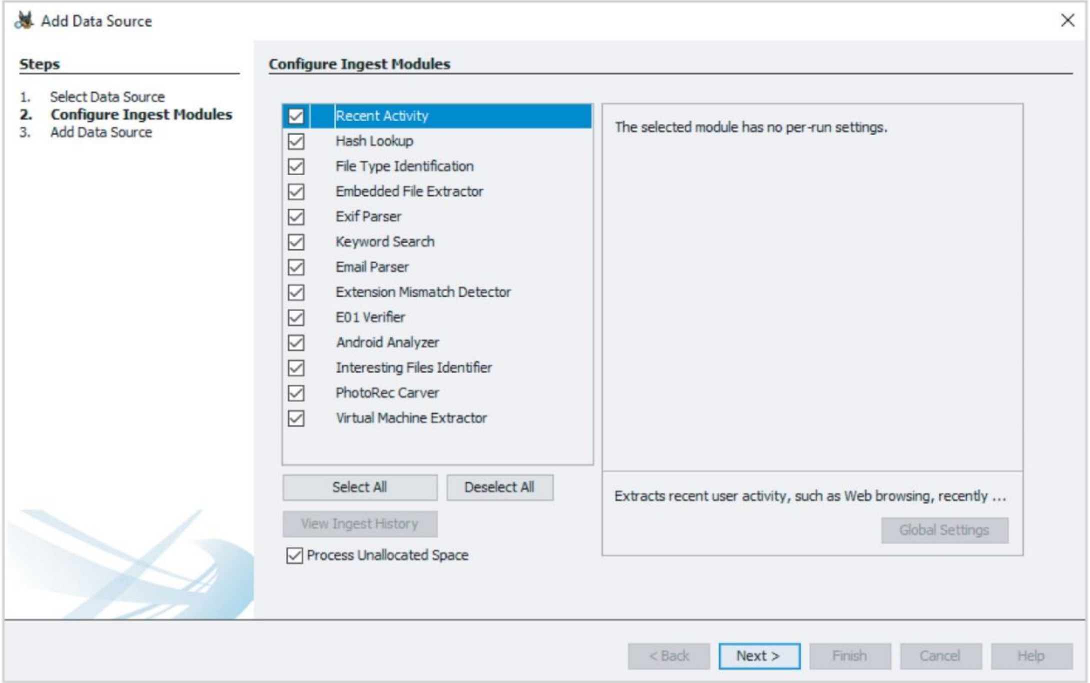
Tom

Figure 8-6 The e-mail with attachments IT found

Searching for and Carving Data from Unallocated Space (1 of 6)

- Steps
  - Planning your examination
  - Searching for and recovering digital photograph evidence
    - Use Autopsy for Windows to search for and extract (recover) possible evidence of JPEG files
    - False hits are referred to as **false positives**

Searching for and Carving Data from Unallocated Space (2 of 6)



Add Data Source

Steps

1. Select Data Source
2. **Configure Ingest Modules**
3. Add Data Source

Configure Ingest Modules

- ☑ Recent Activity
- ☑ Hash Lookup
- ☑ File Type Identification
- ☑ Embedded File Extractor
- ☑ Exif Parser
- ☑ Keyword Search
- ☑ Email Parser
- ☑ Extension Mismatch Detector
- ☑ E01 Verifier
- ☑ Android Analyzer
- ☑ Interesting Files Identifier
- ☑ PhotoRec Carver
- ☑ Virtual Machine Extractor

The selected module has no per-run settings.

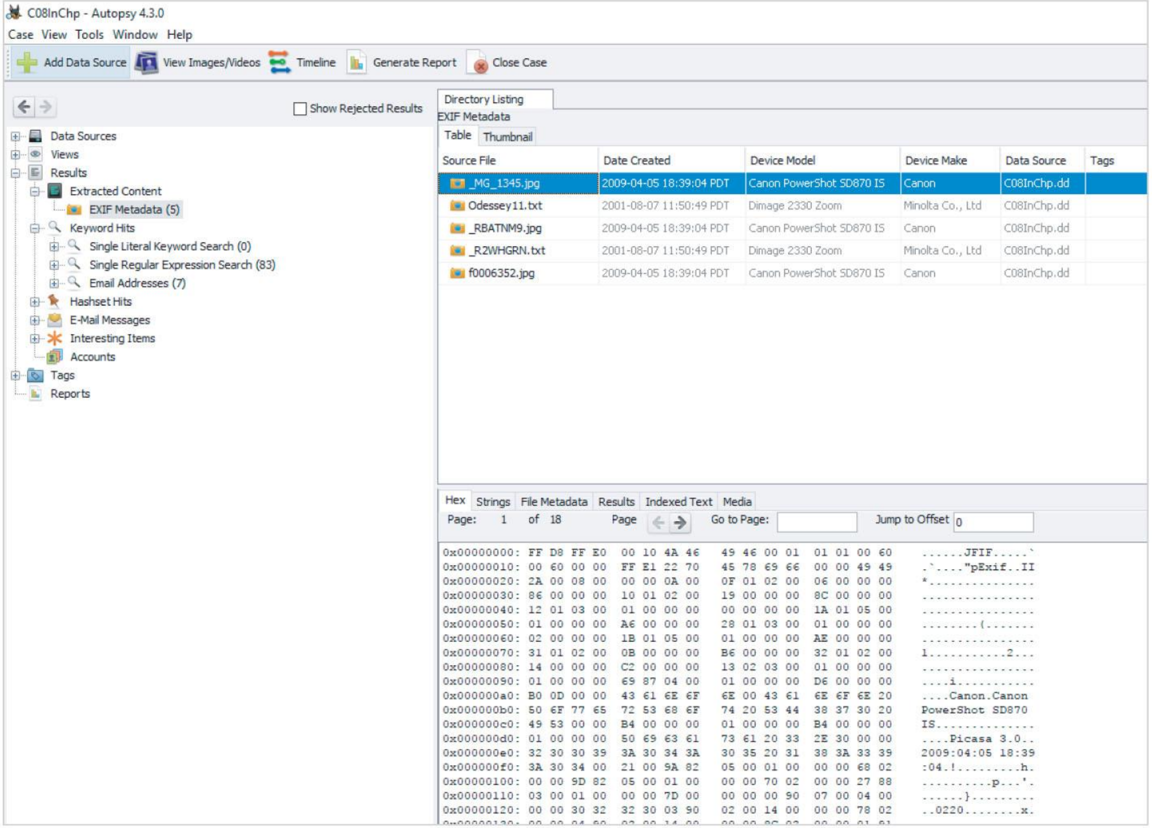
Extracts recent user activity, such as Web browsing, recently ...

☑ Process Unallocated Space

Figure 8-7 **Processing options in the Configure Ingest Modules window**

Source: *www.sleuthkit.org*

Searching for and Carving Data from Unallocated Space (3 of 6)



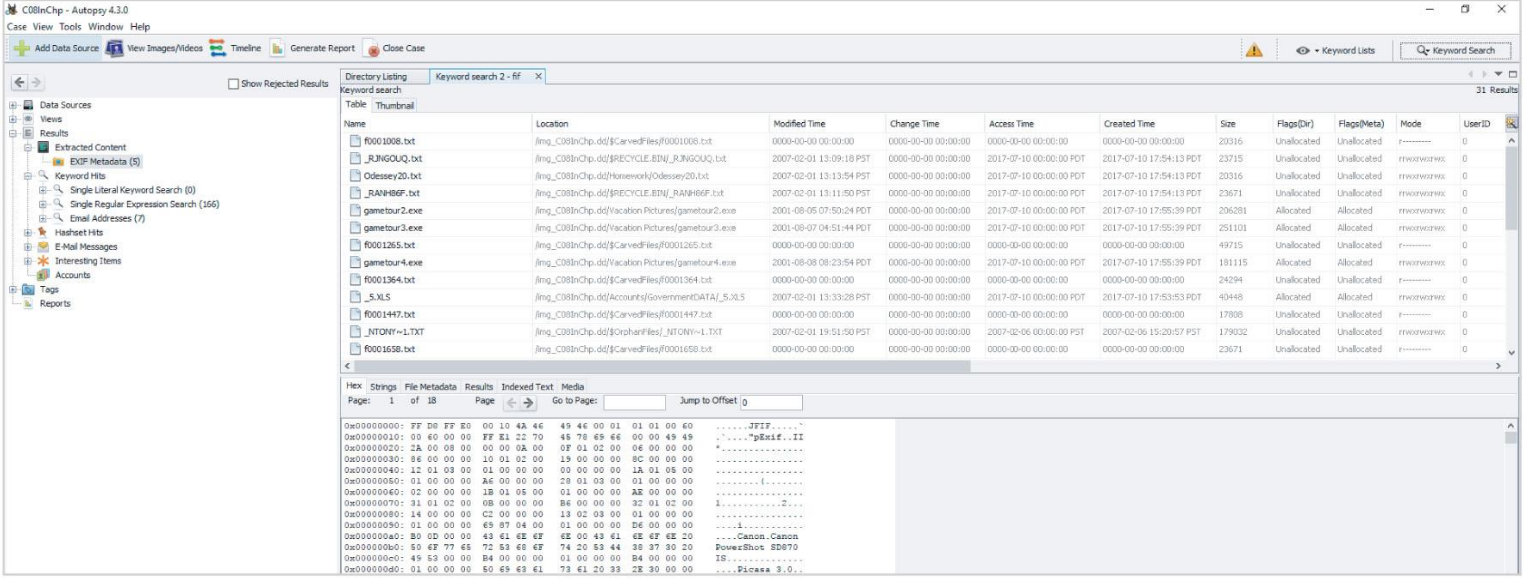
Source File	Date Created	Device Model	Device Make	Data Source	Tags
_MG_1345.jpg	2009-04-05 18:39:04 PDT	Canon PowerShot SD870 IS	Canon	C08InChp.dd	
Odessey11.txt	2001-08-07 11:50:49 PDT	Dimage 2330 Zoom	Minolta Co., Ltd	C08InChp.dd	
_RBATNM9.jpg	2009-04-05 18:39:04 PDT	Canon PowerShot SD870 IS	Canon	C08InChp.dd	
_R2WHGRN.txt	2001-08-07 11:50:49 PDT	Dimage 2330 Zoom	Minolta Co., Ltd	C08InChp.dd	
f0006352.jpg	2009-04-05 18:39:04 PDT	Canon PowerShot SD870 IS	Canon	C08InChp.dd	

```
0x00000000: FF D8 FF E0  00 10 4A 46  49 46 00 01  01 01 00 60   ......JFIF.....`
0x00000010: 00 60 00 00  FF E1 22 70  45 78 69 66  00 00 49 49   .`...."pExif..II
0x00000020: 2A 00 08 00  00 00 0A 00  0F 01 02 00  06 00 00 00   *...............
0x00000030: 86 00 00 00  10 01 02 00  19 00 00 00  8C 00 00 00   ................
0x00000040: 12 01 03 00  01 00 00 00  00 00 00 00  1A 01 05 00   ................
0x00000050: 01 00 00 00  A6 00 00 00  28 01 03 00  01 00 00 00   ........(.......
0x00000060: 02 00 00 00  1B 01 05 00  01 00 00 00  AE 00 00 00   ................
0x00000070: 31 01 02 00  0B 00 00 00  B6 00 00 00  32 01 02 00   1...........2...
0x00000080: 14 00 00 00  C2 00 00 00  13 02 03 00  01 00 00 00   ................
0x00000090: 01 00 00 00  69 87 04 00  01 00 00 00  D6 00 00 00   ....i...........
0x000000a0: B0 0D 00 00  43 61 6E 6F  6E 00 43 61  6E 6F 6E 20   ....Canon.Canon 
0x000000b0: 50 6F 77 65  72 53 68 6F  74 20 53 44  38 37 30 20   PowerShot SD870 
0x000000c0: 49 53 00 00  B4 00 00 00  01 00 00 00  B4 00 00 00   IS..............
0x000000d0: 01 00 00 00  50 69 63 61  73 61 20 33  2E 30 00 00   ....Picasa 3.0..
0x000000e0: 32 30 30 39  3A 30 34 3A  30 35 20 31  38 3A 33 39   2009:04:05 18:39
0x000000f0: 3A 30 34 00  21 00 9A 82  05 00 01 00  00 00 68 02   :04.!.........h.
0x00000100: 00 00 9D 82  05 00 01 00  00 00 70 02  00 00 27 88   ..........p...'.
0x00000110: 03 00 01 00  00 00 7D 00  00 00 00 90  07 00 04 00   ......}.........
0x00000120: 00 00 30 32  32 30 03 90  02 00 14 00  00 00 78 02   ..0220........x.
```

Figure 8-8 Parsing Exif metadata in Autopsy

Source: *www.sleuthkit.org*

Searching for and Carving Data from Unallocated Space (4 of 6)



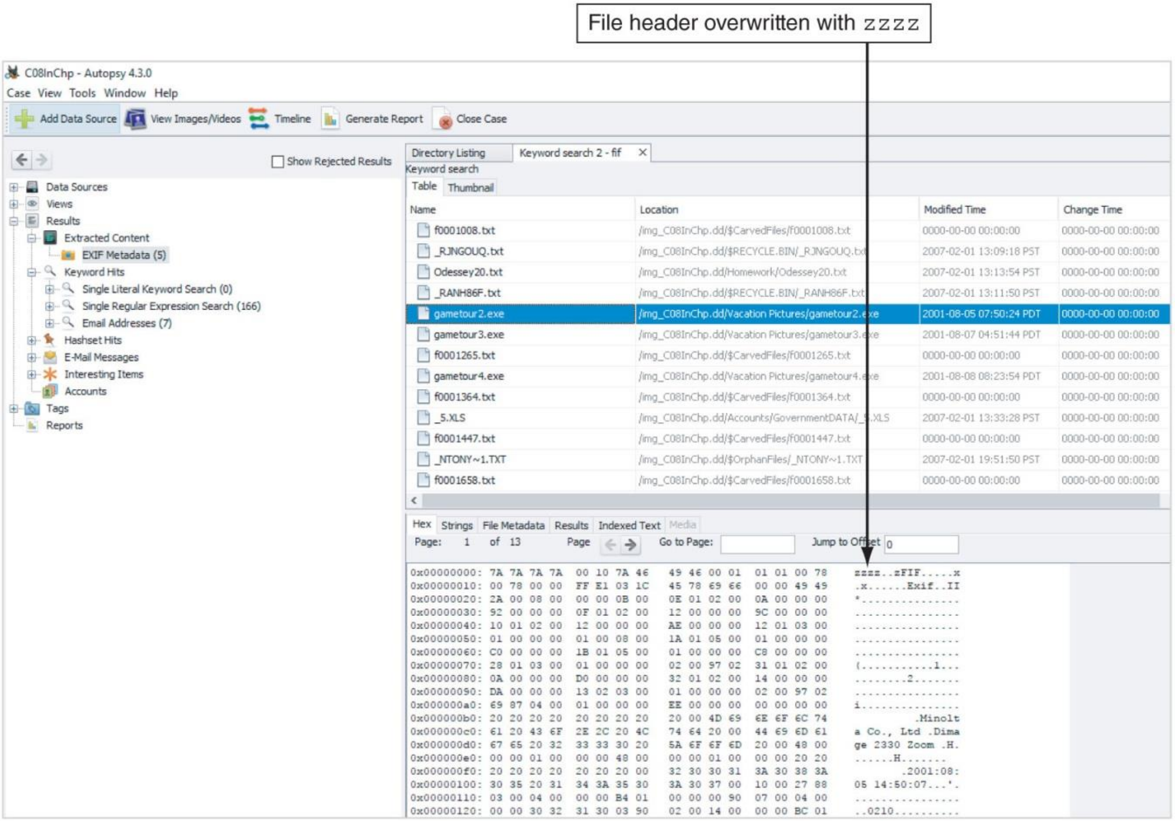
Name	Location	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Mode	UserID
f0001008.txt	/img_C08InChp.dd/$CarvedFiles/f0001008.txt	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	20316	Unallocated	Unallocated	r---------	0
_RJNGOUQ.txt	/img_C08InChp.dd/$RECYCLE.BIN/_RJNGOUQ.txt	2007-02-01 13:09:18 PST	0000-00-00 00:00:00	2017-07-10 00:00:00 PDT	2017-07-10 17:54:13 PDT	23715	Unallocated	Unallocated	rrwxrwxrwx	0
Odessey20.txt	/img_C08InChp.dd/Homework/Odessey20.txt	2007-02-01 13:13:54 PST	0000-00-00 00:00:00	2017-07-10 00:00:00 PDT	2017-07-10 17:54:13 PDT	20316	Unallocated	Unallocated	rrwxrwxrwx	0
_RANH86F.txt	/img_C08InChp.dd/$RECYCLE.BIN/_RANH86F.txt	2007-02-01 13:11:50 PST	0000-00-00 00:00:00	2017-07-10 00:00:00 PDT	2017-07-10 17:54:13 PDT	23671	Unallocated	Unallocated	rrwxrwxrwx	0
gametour2.exe	/img_C08InChp.dd/Vacation Pictures/gametour2.exe	2001-08-05 07:50:24 PDT	0000-00-00 00:00:00	2017-07-10 00:00:00 PDT	2017-07-10 17:55:39 PDT	206281	Allocated	Allocated	rrwxrwxrwx	0
gametour3.exe	/img_C08InChp.dd/Vacation Pictures/gametour3.exe	2001-08-07 04:51:44 PDT	0000-00-00 00:00:00	2017-07-10 00:00:00 PDT	2017-07-10 17:55:39 PDT	251101	Allocated	Allocated	rrwxrwxrwx	0
f0001265.txt	/img_C08InChp.dd/$CarvedFiles/f0001265.txt	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	49715	Unallocated	Unallocated	r---------	0
gametour4.exe	/img_C08InChp.dd/Vacation Pictures/gametour4.exe	2001-08-08 08:23:54 PDT	0000-00-00 00:00:00	2017-07-10 00:00:00 PDT	2017-07-10 17:55:39 PDT	181115	Allocated	Allocated	rrwxrwxrwx	0
f0001364.txt	/img_C08InChp.dd/$CarvedFiles/f0001364.txt	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	24294	Unallocated	Unallocated	r---------	0
_5.XLS	/img_C08InChp.dd/Accounts/GovernmentDATA/_5.XLS	2007-02-01 13:33:28 PST	0000-00-00 00:00:00	2017-07-10 00:00:00 PDT	2017-07-10 17:53:53 PDT	40448	Allocated	Allocated	rrwxrwxrwx	0
f0001447.txt	/img_C08InChp.dd/$CarvedFiles/f0001447.txt	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	17808	Unallocated	Unallocated	r---------	0
_NTONY~1.TXT	/img_C08InChp.dd/$OrphanFiles/_NTONY~1.TXT	2007-02-01 19:51:50 PST	0000-00-00 00:00:00	2007-02-06 00:00:00 PST	2007-02-06 15:20:57 PST	179032	Unallocated	Unallocated	rrwxrwxrwx	0
f0001658.txt	/img_C08InChp.dd/$CarvedFiles/f0001658.txt	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	23671	Unallocated	Unallocated	r---------	0

```
0x00000000: FF D8 FF E0  00 10 4A 46  49 46 00 01  01 01 00 60   ......JFIF.....`
0x00000010: 00 60 00 00  FF E1 22 70  45 78 69 66  00 00 49 49   .`...."pExif..II
0x00000020: 2A 00 08 00  00 00 0A 00  0F 01 02 00  06 00 00 00   *...............
0x00000030: 86 00 00 00  10 01 02 00  19 00 00 00  8C 00 00 00   ................
0x00000040: 12 01 03 00  01 00 00 00  00 00 00 00  1A 01 05 00   ................
0x00000050: 01 00 00 00  A6 00 00 00  28 01 03 00  01 00 00 00   ........(.......
0x00000060: 02 00 00 00  1B 01 05 00  01 00 00 00  AE 00 00 00   ................
0x00000070: 31 01 02 00  0B 00 00 00  B6 00 00 00  32 01 02 00   1...........2...
0x00000080: 14 00 00 00  C2 00 00 00  13 02 03 00  01 00 00 00   ................
0x00000090: 01 00 00 00  69 87 04 00  01 00 00 00  D6 00 00 00   ....i...........
0x000000a0: B0 0D 00 00  43 61 6E 6F  6E 00 43 61  6E 6F 6E 20   ....Canon.Canon
0x000000b0: 50 6F 77 65  72 53 68 6F  74 20 53 44  38 37 30 20   PowerShot SD870
0x000000c0: 49 53 00 00  B4 00 00 00  01 00 00 00  B4 00 00 00   IS..............
0x000000d0: 01 00 00 00  50 69 63 61  73 61 20 33  2E 30 00 00   ....Picasa 3.0..
```

Figure 8-9 **The results of searching for "fif"**

Source: *www.sleuthkit.org*

Searching for and Carving Data from Unallocated Space (5 of 6)



File header overwritten with zzzz

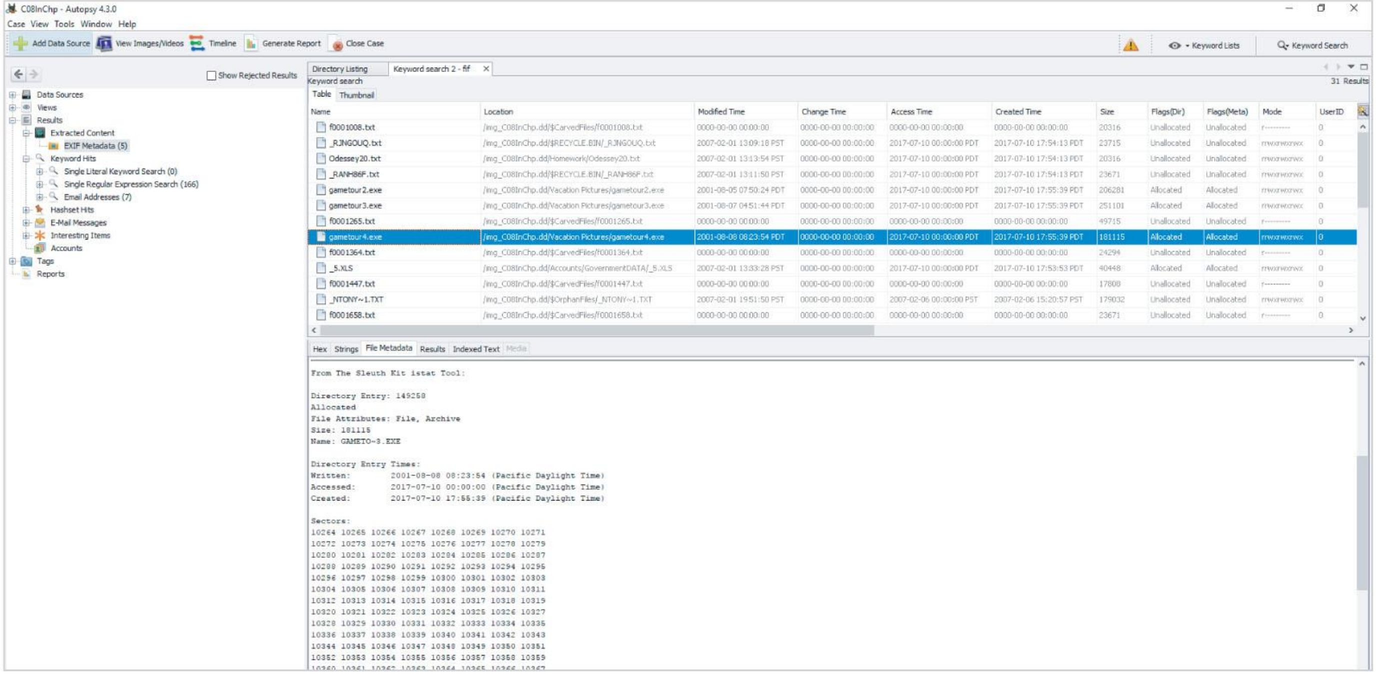
Name	Location	Modified Time	Change Time
f0001008.txt	/img_C08InChp.dd/$CarvedFiles/f0001008.txt	0000-00-00 00:00:00	0000-00-00 00:00:00
_RJNGOUQ.txt	/img_C08InChp.dd/$RECYCLE.BIN/_RJNGOUQ.txt	2007-02-01 13:09:18 PST	0000-00-00 00:00:00
Odessey20.txt	/img_C08InChp.dd/Homework/Odessey20.txt	2007-02-01 13:13:54 PST	0000-00-00 00:00:00
_RANH86F.txt	/img_C08InChp.dd/$RECYCLE.BIN/_RANH86F.txt	2007-02-01 13:11:50 PST	0000-00-00 00:00:00
gametour2.exe	/img_C08InChp.dd/Vacation Pictures/gametour2.exe	2001-08-05 07:50:24 PDT	0000-00-00 00:00:00
gametour3.exe	/img_C08InChp.dd/Vacation Pictures/gametour3.exe	2001-08-07 04:51:44 PDT	0000-00-00 00:00:00
f0001265.txt	/img_C08InChp.dd/$CarvedFiles/f0001265.txt	0000-00-00 00:00:00	0000-00-00 00:00:00
gametour4.exe	/img_C08InChp.dd/Vacation Pictures/gametour4.exe	2001-08-08 08:23:54 PDT	0000-00-00 00:00:00
f0001364.txt	/img_C08InChp.dd/$CarvedFiles/f0001364.txt	0000-00-00 00:00:00	0000-00-00 00:00:00
_5.XLS	/img_C08InChp.dd/Accounts/GovernmentDATA/_5.XLS	2007-02-01 13:33:28 PST	0000-00-00 00:00:00
f0001447.txt	/img_C08InChp.dd/$CarvedFiles/f0001447.txt	0000-00-00 00:00:00	0000-00-00 00:00:00
_NTONY~1.TXT	/img_C08InChp.dd/$OrphanFiles/_NTONY~1.TXT	2007-02-01 19:51:50 PST	0000-00-00 00:00:00
f0001658.txt	/img_C08InChp.dd/$CarvedFiles/f0001658.txt	0000-00-00 00:00:00	0000-00-00 00:00:00

```
0x00000000: 7A 7A 7A 7A  00 10 7A 46   49 46 00 01   01 01 00 78    zzzz..zFIF.....x
0x00000010: 00 78 00 00  FF E1 03 1C   45 78 69 66   00 00 49 49    .x......Exif..II
0x00000020: 2A 00 08 00  00 00 0B 00   0E 01 02 00   0A 00 00 00    *...............
0x00000030: 92 00 00 00  0F 01 02 00   12 00 00 00   9C 00 00 00    ................
0x00000040: 10 01 02 00  12 00 00 00   AE 00 00 00   12 01 03 00    ................
0x00000050: 01 00 00 00  01 00 08 00   1A 01 05 00   01 00 00 00    ................
0x00000060: C0 00 00 00  1B 01 05 00   01 00 00 00   C8 00 00 00    ................
0x00000070: 28 01 03 00  01 00 00 00   02 00 97 02   31 01 02 00    (...........1...
0x00000080: 0A 00 00 00  D0 00 00 00   32 01 02 00   14 00 00 00    ........2.......
0x00000090: DA 00 00 00  13 02 03 00   01 00 00 00   02 00 97 02    ................
0x000000a0: 69 87 04 00  01 00 00 00   EE 00 00 00   00 00 00 00    i...............
0x000000b0: 20 20 20 20  20 20 20 20   20 00 4D 69   6E 6F 6C 74             .Minolt
0x000000c0: 61 20 43 6F  2E 2C 20 4C   74 64 20 00   44 69 6D 61    a Co., Ltd .Dima
0x000000d0: 67 65 20 32  33 33 30 20   5A 6F 6F 6D   20 00 48 00    ge 2330 Zoom .H.
0x000000e0: 00 00 01 00  00 00 48 00   00 00 01 00   00 00 20 20    ......H.......
0x000000f0: 20 20 20 20  20 20 20 00   32 30 30 31   3A 30 38 3A           .2001:08:
0x00000100: 30 35 20 31  34 3A 35 30   3A 30 37 00   10 00 27 88    05 14:50:07...'.
0x00000110: 03 00 04 00  00 00 B4 01   00 00 00 90   07 00 04 00    ................
0x00000120: 00 00 30 32  31 30 03 90   02 00 14 00   00 00 BC 01    ..0210..........
```

Figure 8-10 The altered file header

Source: *www.sleuthkit.org*

Searching for and Carving Data from Unallocated Space (6 of 6)



Name	Location	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Mode	UserID
f0001008.txt	/img_C08InChp.dd/$CarvedFiles/f0001008.txt	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	20316	Unallocated	Unallocated	r---------	0
_RJNGOUQ.txt	/img_C08InChp.dd/$RECYCLE.BIN/_RJNGOUQ.txt	2007-02-01 13:09:18 PST	0000-00-00 00:00:00	2017-07-10 00:00:00 PDT	2017-07-10 17:54:13 PDT	23715	Unallocated	Unallocated	rrwxrwxrwx	0
Odessey20.txt	/img_C08InChp.dd/Homework/Odessey20.txt	2007-02-01 13:13:54 PST	0000-00-00 00:00:00	2017-07-10 00:00:00 PDT	2017-07-10 17:54:13 PDT	20316	Unallocated	Unallocated	rrwxrwxrwx	0
_RANH86F.txt	/img_C08InChp.dd/$RECYCLE.BIN/_RANH86F.txt	2007-02-01 13:11:50 PST	0000-00-00 00:00:00	2017-07-10 00:00:00 PDT	2017-07-10 17:54:13 PDT	23671	Unallocated	Unallocated	rrwxrwxrwx	0
gametour2.exe	/img_C08InChp.dd/Vacation Pictures/gametour2.exe	2001-08-05 07:50:24 PDT	0000-00-00 00:00:00	2017-07-10 00:00:00 PDT	2017-07-10 17:55:39 PDT	206281	Allocated	Allocated	rrwxrwxrwx	0
gametour3.exe	/img_C08InChp.dd/Vacation Pictures/gametour3.exe	2001-08-07 04:51:44 PDT	0000-00-00 00:00:00	2017-07-10 00:00:00 PDT	2017-07-10 17:55:39 PDT	251101	Allocated	Allocated	rrwxrwxrwx	0
f0001265.txt	/img_C08InChp.dd/$CarvedFiles/f0001265.txt	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	49715	Unallocated	Unallocated	r---------	0
gametour4.exe	/img_C08InChp.dd/Vacation Pictures/gametour4.exe	2001-08-08 08:23:54 PDT	0000-00-00 00:00:00	2017-07-10 00:00:00 PDT	2017-07-10 17:55:39 PDT	181115	Allocated	Allocated	rrwxrwxrwx	0
f0001364.txt	/img_C08InChp.dd/$CarvedFiles/f0001364.txt	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	24294	Unallocated	Unallocated	r---------	0
_5.XLS	/img_C08InChp.dd/Accounts/GovernmentDATA/_5.XLS	2007-02-01 13:33:28 PST	0000-00-00 00:00:00	2017-07-10 00:00:00 PDT	2017-07-10 17:53:53 PDT	40448	Allocated	Allocated	rrwxrwxrwx	0
f0001447.txt	/img_C08InChp.dd/$CarvedFiles/f0001447.txt	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	17808	Unallocated	Unallocated	r---------	0
_NTONY~1.TXT	/img_C08InChp.dd/$OrphanFiles/_NTONY~1.TXT	2007-02-01 19:51:50 PST	0000-00-00 00:00:00	2007-02-06 00:00:00 PST	2007-02-06 15:20:57 PST	179032	Unallocated	Unallocated	rrwxrwxrwx	0
f0001658.txt	/img_C08InChp.dd/$CarvedFiles/f0001658.txt	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	23671	Unallocated	Unallocated	r---------	0

```
From The Sleuth Kit istat Tool:

Directory Entry: 149258
Allocated
File Attributes: File, Archive
Size: 181115
Name: GAMETO~3.EXE

Directory Entry Times:
Written:        2001-08-08 08:23:54 (Pacific Daylight Time)
Accessed:       2017-07-10 00:00:00 (Pacific Daylight Time)
Created:        2017-07-10 17:55:39 (Pacific Daylight Time)

Sectors:
10264 10265 10266 10267 10268 10269 10270 10271
10272 10273 10274 10275 10276 10277 10278 10279
10280 10281 10282 10283 10284 10285 10286 10287
10288 10289 10290 10291 10292 10293 10294 10295
10296 10297 10298 10299 10300 10301 10302 10303
10304 10305 10306 10307 10308 10309 10310 10311
10312 10313 10314 10315 10316 10317 10318 10319
10320 10321 10322 10323 10324 10325 10326 10327
10328 10329 10330 10331 10332 10333 10334 10335
10336 10337 10338 10339 10340 10341 10342 10343
10344 10345 10346 10347 10348 10349 10350 10351
10352 10353 10354 10355 10356 10357 10358 10359
10360 10361 10362 10363 10364 10365 10366 10367
```

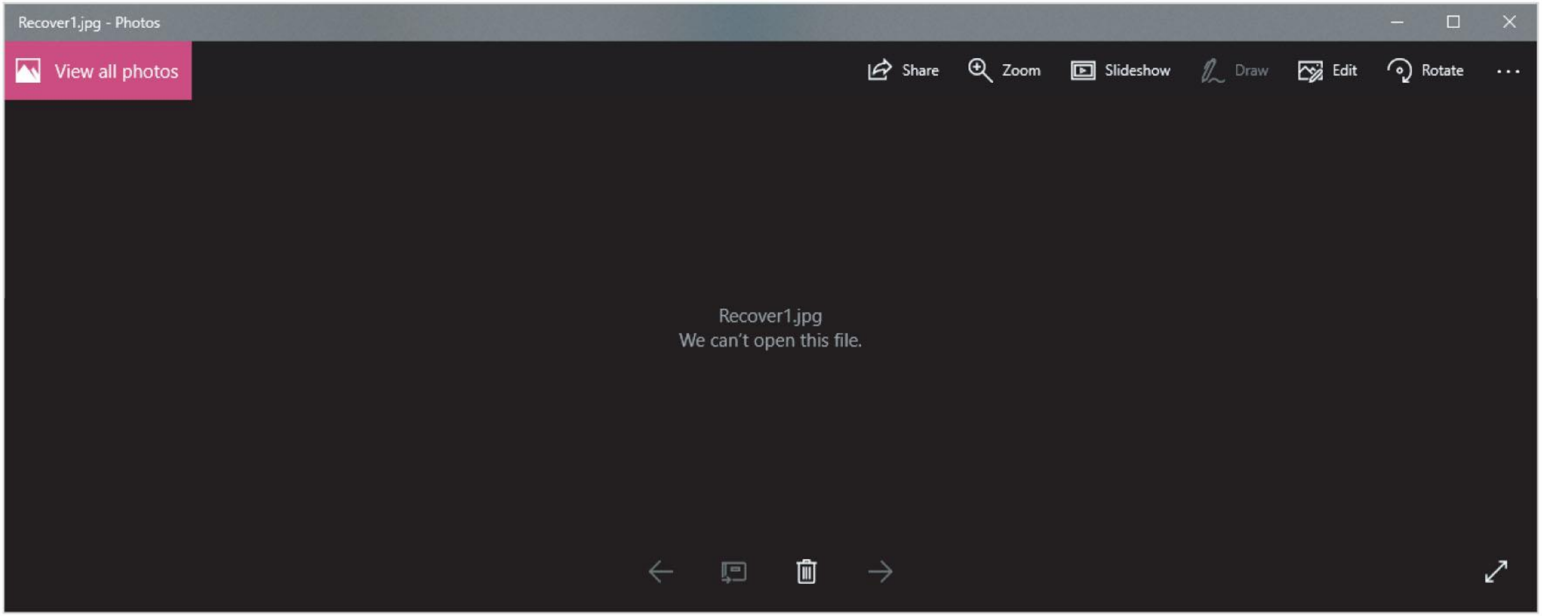
Figure 8-11 Viewing all sectors used by the `gametour2.exe` file

Source: *www.sleuthkit.org*

Rebuilding File Headers (1 of 6)

- Before attempting to edit a recovered graphics file
  - Try to open the file with an image viewer first
- If the image isn't displayed, you have to inspect and correct the header values manually
- Steps
  - Recover more pieces of file if needed
  - Examine file header
    - Compare with a good header sample
    - Manually insert correct hexadecimal values
  - Test corrected file

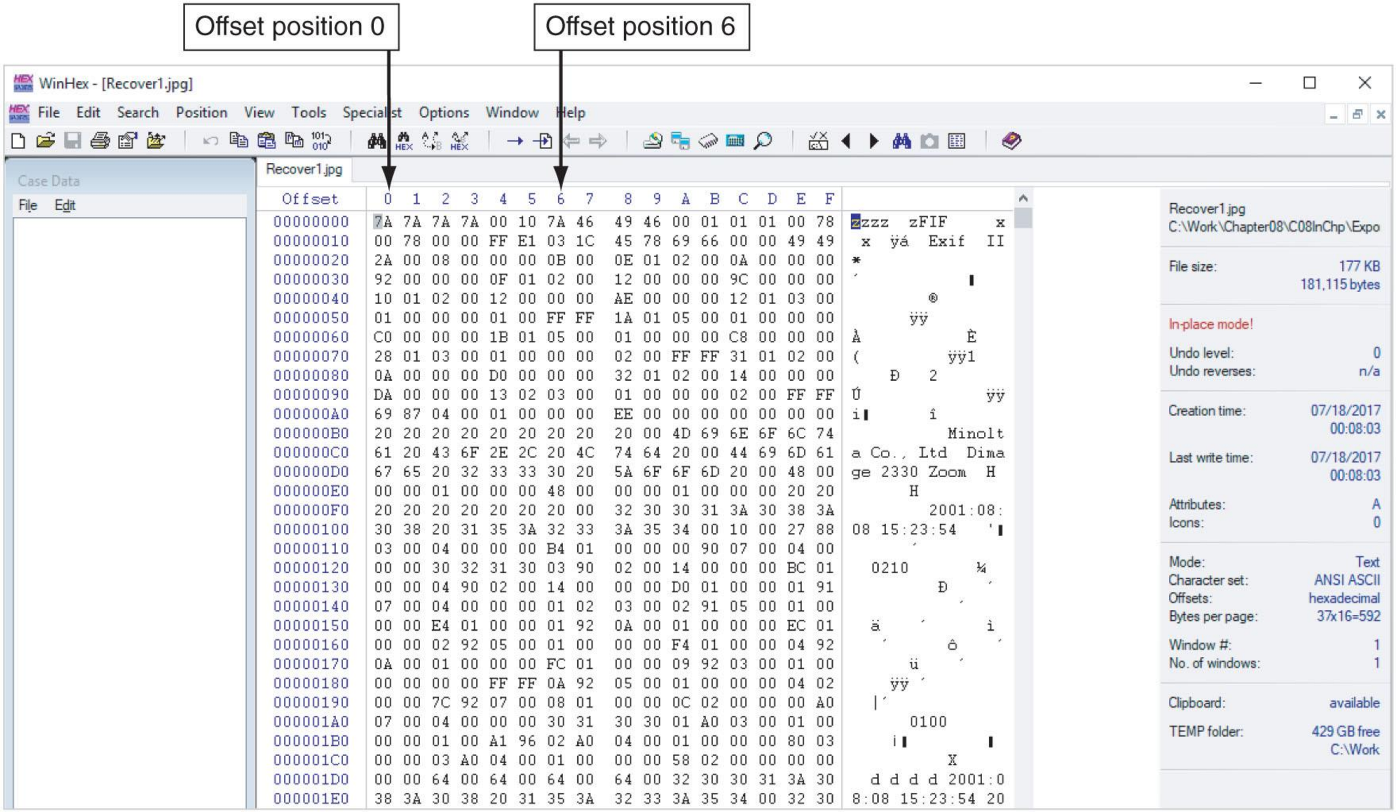
Rebuilding File Headers (2 of 6)



Recover1.jpg
We can't open this file.

Figure 8-12 Error message indicating a damaged or an altered graphics file

Rebuilding File Headers (3 of 6)



```
Offset     0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F

00000000  7A 7A 7A 7A 00 10 7A 46  49 46 00 01 01 01 00 78  zzzz  zFIF    x
00000010  00 78 00 00 FF E1 03 1C  45 78 69 66 00 00 49 49   x  ÿá  Exif  II
00000020  2A 00 08 00 00 00 0B 00  0E 01 02 00 0A 00 00 00  *
00000030  92 00 00 00 0F 01 02 00  12 00 00 00 9C 00 00 00  ´           ▮
00000040  10 01 02 00 12 00 00 00  AE 00 00 00 12 01 03 00          ®
00000050  01 00 00 00 01 00 FF FF  1A 01 05 00 01 00 00 00        ÿÿ
00000060  C0 00 00 00 1B 01 05 00  01 00 00 00 C8 00 00 00  À           È
00000070  28 01 03 00 01 00 00 00  02 00 FF FF 31 01 02 00  (          ÿÿ1
00000080  0A 00 00 00 D0 00 00 00  32 01 02 00 14 00 00 00      Ð    2
00000090  DA 00 00 00 13 02 03 00  01 00 00 00 02 00 FF FF  Ú              ÿÿ
000000A0  69 87 04 00 01 00 00 00  EE 00 00 00 00 00 00 00  i▮      î
000000B0  20 20 20 20 20 20 20 20  20 00 4D 69 6E 6F 6C 74            Minolt
000000C0  61 20 43 6F 2E 2C 20 4C  74 64 20 00 44 69 6D 61  a Co., Ltd  Dima
000000D0  67 65 20 32 33 33 30 20  5A 6F 6F 6D 20 00 48 00  ge 2330 Zoom  H
000000E0  00 00 01 00 00 00 48 00  00 00 01 00 00 00 20 20        H
000000F0  20 20 20 20 20 20 20 00  32 30 30 31 3A 30 38 3A          2001:08:
00000100  30 38 20 31 35 3A 32 33  3A 35 34 00 10 00 27 88  08 15:23:54    '▮
00000110  03 00 04 00 00 00 B4 01  00 00 00 90 07 00 04 00        ´
00000120  00 00 30 32 31 30 03 90  02 00 14 00 00 00 BC 01    0210       ¼
00000130  00 00 04 90 02 00 14 00  00 00 D0 01 00 00 01 91           Ð   ´
00000140  07 00 04 00 00 00 01 02  03 00 02 91 05 00 01 00             ´
00000150  00 00 E4 01 00 00 01 92  0A 00 01 00 00 00 EC 01    ä    ´      ì
00000160  00 00 02 92 05 00 01 00  00 00 F4 01 00 00 04 92     ´      ô    ´
00000170  0A 00 01 00 00 00 FC 01  00 00 09 92 03 00 01 00        ü    ´
00000180  00 00 00 00 FF FF 0A 92  05 00 01 00 00 00 04 02      ÿÿ ´
00000190  00 00 7C 92 07 00 08 01  00 00 0C 02 00 00 00 A0    |´
000001A0  07 00 04 00 00 00 30 31  30 30 01 A0 03 00 01 00        0100
000001B0  00 00 01 00 A1 96 02 A0  04 00 01 00 00 00 80 03      i▮        ▮
000001C0  00 00 03 A0 04 00 01 00  00 00 58 02 00 00 00 00           X
000001D0  00 00 64 00 64 00 64 00  64 00 32 30 30 31 3A 30    d d d d 2001:0
000001E0  38 3A 30 38 20 31 35 3A  32 33 3A 35 34 00 32 30  8:08 15:23:54 20
```

Recover1.jpg
C:\Work\Chapter08\C08InChp\Expo

File size: 177 KB
181,115 bytes

In-place mode!

Undo level: 0
Undo reverses: n/a

Creation time: 07/18/2017
00:08:03

Last write time: 07/18/2017
00:08:03

Attributes: A
Icons: 0

Mode: Text
Character set: ANSI ASCII
Offsets: hexadecimal
Bytes per page: 37x16=592

Window #: 1
No. of windows: 1

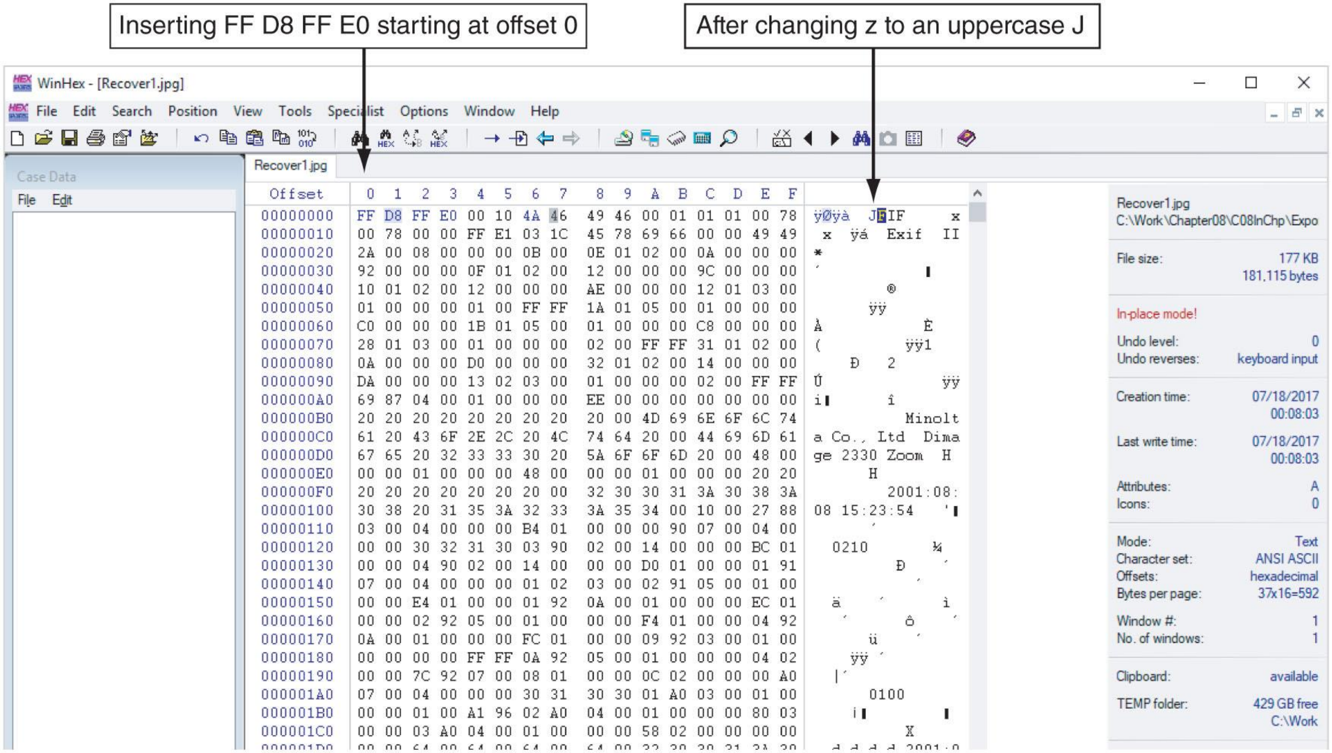
Clipboard: available

TEMP folder: 429 GB free
C:\Work

Figure 8-13 `Recover1.jpg` open in WinHex

Source: X-Ways AG, *www.xways.net*

Rebuilding File Headers (4 of 6)



Inserting FF D8 FF E0 starting at offset 0

After changing z to an uppercase J

WinHex - [Recover1.jpg]
File Edit Search Position View Tools Specialist Options Window Help
Case Data
File Edit
Recover1.jpg

```
 Offset     0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
00000000   FF D8 FF E0 00 10 4A 46  49 46 00 01 01 01 00 78   ÿØÿà  JFIF     x
00000010   00 78 00 00 FF E1 03 1C  45 78 69 66 00 00 49 49    x  ÿá  Exif  II
00000020   2A 00 08 00 00 00 0B 00  0E 01 02 00 0A 00 00 00   *
00000030   92 00 00 00 0F 01 02 00  12 00 00 00 9C 00 00 00   ´           ▮
00000040   10 01 02 00 12 00 00 00  AE 00 00 00 12 01 03 00           ®
00000050   01 00 00 00 01 00 FF FF  1A 01 05 00 01 00 00 00         ÿÿ
00000060   C0 00 00 00 1B 01 05 00  01 00 00 00 C8 00 00 00   À           È
00000070   28 01 03 00 01 00 00 00  02 00 FF FF 31 01 02 00   (         ÿÿ1
00000080   0A 00 00 00 D0 00 00 00  32 01 02 00 14 00 00 00       Ð   2
00000090   DA 00 00 00 13 02 03 00  01 00 00 00 02 00 FF FF   Ú             ÿÿ
000000A0   69 87 04 00 01 00 00 00  EE 00 00 00 00 00 00 00   i▮      î
000000B0   20 20 20 20 20 20 20 20  20 00 4D 69 6E 6F 6C 74             Minolt
000000C0   61 20 43 6F 2E 2C 20 4C  74 64 20 00 44 69 6D 61   a Co., Ltd  Dima
000000D0   67 65 20 32 33 33 30 20  5A 6F 6F 6D 20 00 48 00   ge 2330 Zoom  H
000000E0   00 00 01 00 00 00 48 00  00 00 01 00 00 00 20 20         H
000000F0   20 20 20 20 20 20 20 00  32 30 30 31 3A 30 38 3A           2001:08:
00000100   30 38 20 31 35 3A 32 33  3A 35 34 00 10 00 27 88   08 15:23:54   '▮
00000110   03 00 04 00 00 00 B4 01  00 00 00 90 07 00 04 00         ´
00000120   00 00 30 32 31 30 03 90  02 00 14 00 00 00 BC 01     0210        ¼
00000130   00 00 04 90 02 00 14 00  00 00 D0 01 00 00 01 91             Ð    ´
00000140   07 00 04 00 00 00 01 02  03 00 02 91 05 00 01 00              ´
00000150   00 00 E4 01 00 00 01 92  0A 00 01 00 00 00 EC 01     ä    ´      ì
00000160   00 00 02 92 05 00 01 00  00 00 F4 01 00 00 04 92      ´      ô    ´
00000170   0A 00 01 00 00 00 FC 01  00 00 09 92 03 00 01 00         ü    ´
00000180   00 00 00 00 FF FF 0A 92  05 00 01 00 00 00 04 02       ÿÿ ´
00000190   00 00 7C 92 07 00 08 01  00 00 0C 02 00 00 00 A0     |´
000001A0   07 00 04 00 00 00 30 31  30 30 01 A0 03 00 01 00         0100
000001B0   00 00 01 00 A1 96 02 A0  04 00 01 00 00 00 80 03       i▮        ▮
000001C0   00 00 03 A0 04 00 01 00  00 00 58 02 00 00 00 00             X
000001D0   00 00 64 00 64 00 64 00  64 00 32 30 30 31 3A 30     d d d d 2001:0
```

Recover1.jpg
C:\Work\Chapter08\C08InChp\Expo

File size: 177 KB
181,115 bytes

In-place mode!

Undo level: 0
Undo reverses: keyboard input

Creation time: 07/18/2017 00:08:03

Last write time: 07/18/2017 00:08:03

Attributes: A
Icons: 0

Mode: Text
Character set: ANSI ASCII
Offsets: hexadecimal
Bytes per page: 37x16=592

Window #: 1
No. of windows: 1

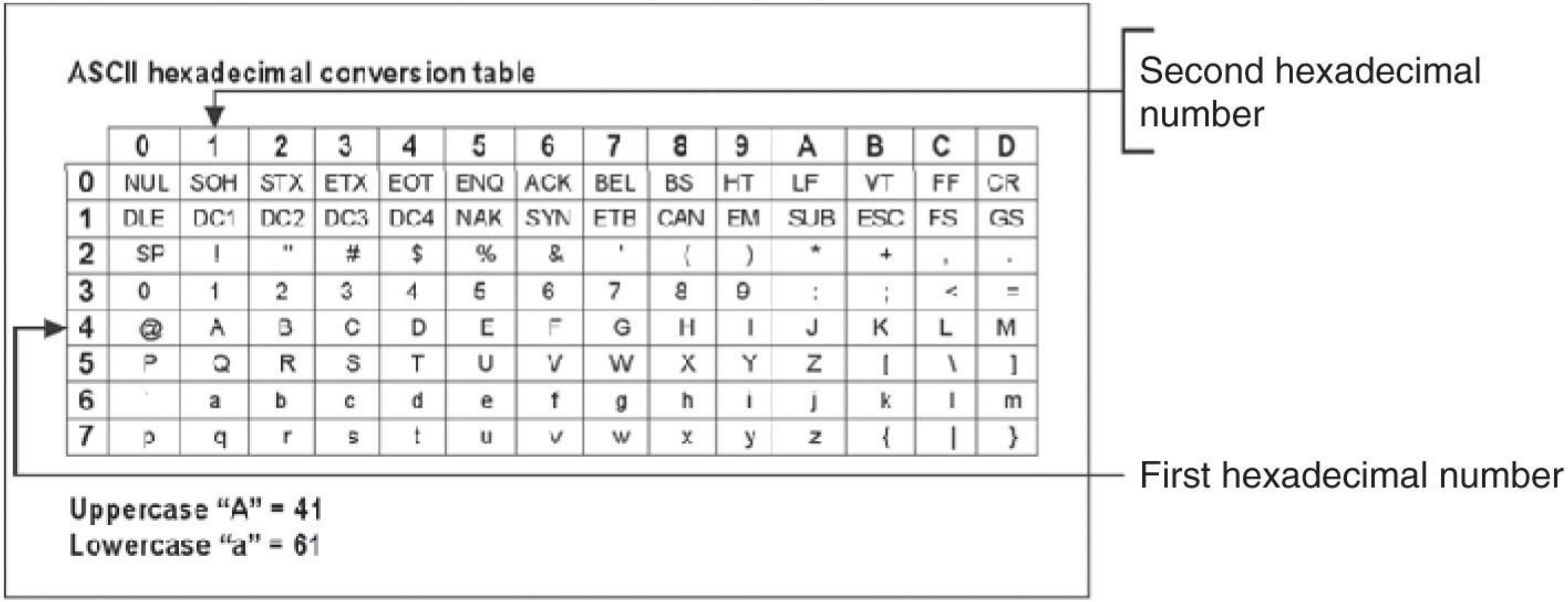
Clipboard: available

TEMP folder: 429 GB free
C:\Work

Figure 8-14 Inserting correct hexadecimal values for a JPEG file

Source: X-Ways AG, *www.xways.net*

Rebuilding File Headers (5 of 6)



ASCII hexadecimal conversion table

	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	{	|	}

Uppercase "A" = 41
Lowercase "a" = 61

Second hexadecimal number

First hexadecimal number

Figure 8-15 ASCII equivalents of hexadecimal values

Rebuilding File Headers (6 of 6)

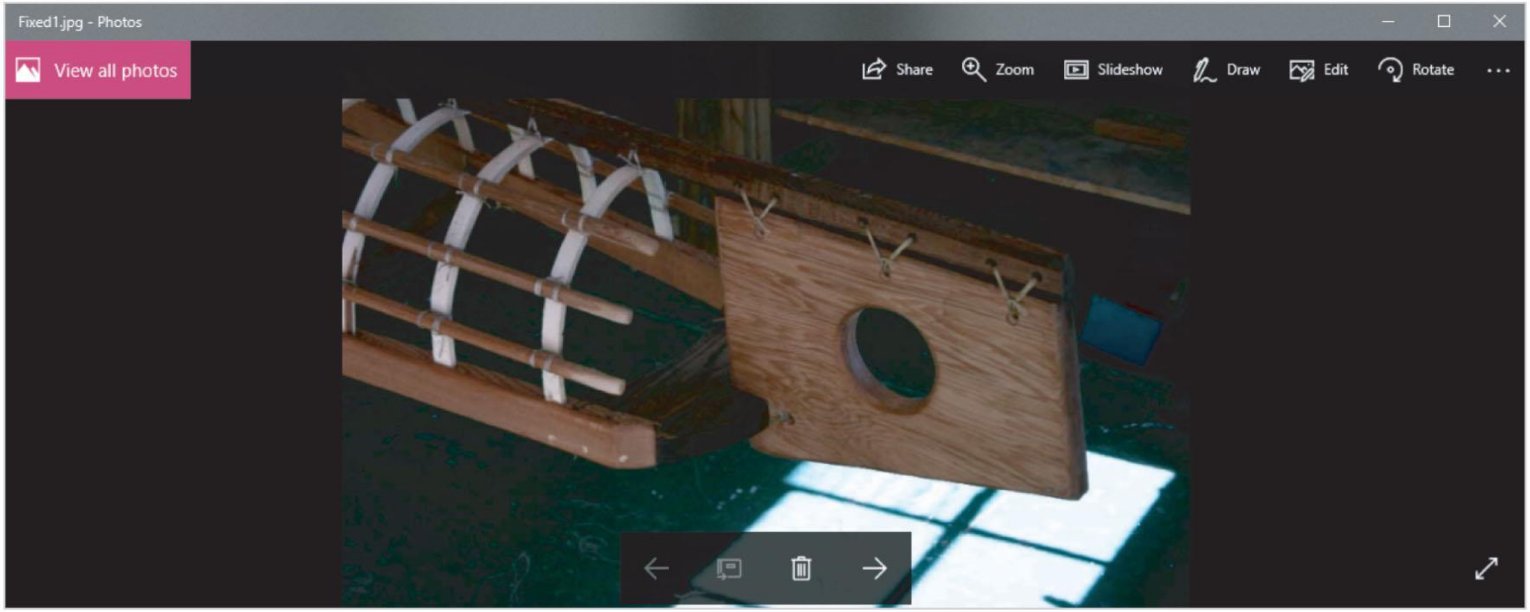


Figure 8-16 `Fixed1.jpg` open in an image viewer

Reconstructing File Fragments

- Locate the noncontiguous clusters that make up a deleted file
- Steps
  - Locate and export all clusters of the fragmented file
  - Determine the starting and ending cluster numbers for each fragmented group of sectors
  - Copy each fragmented group of sectors in their correct sequence to a recovery file
  - Rebuild the file’s header to make it readable in a graphics viewer
  - Add a `.txt` extension on all the copied sectors

Identifying Unknown File Formats

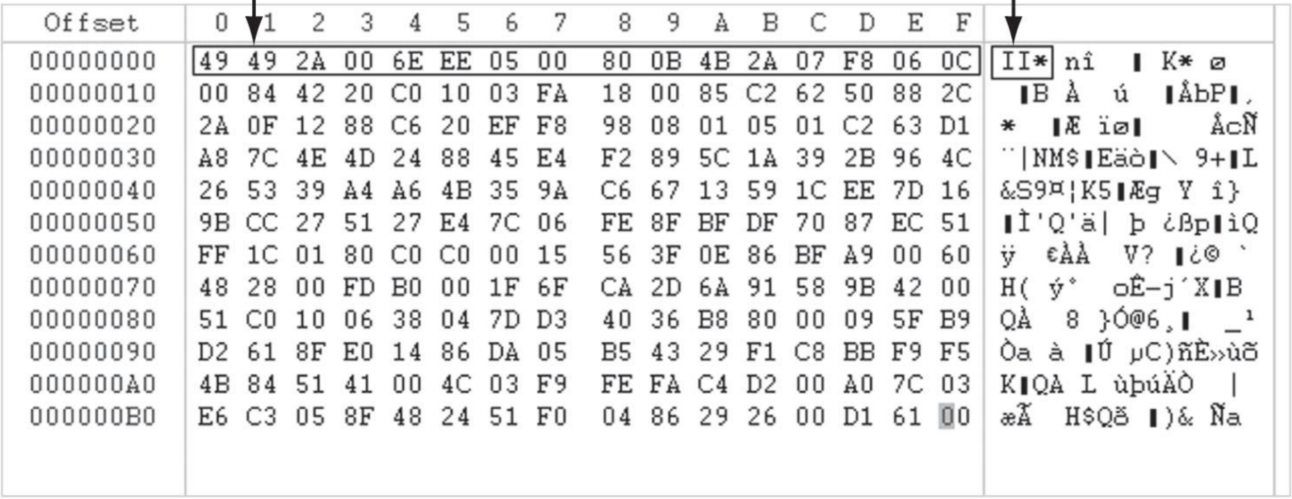
- Knowing the purpose of each format and how it stores data is part of the investigation process
- The Internet is the best source
  - Search engines
  - Find explanations and viewers
- Popular Web sites
  - *FileFormat.info*
  - *Extension Informer*
  - *The Graphics File Formats Page*

Analyzing Graphics File Headers (1 of 3)

- Necessary when you find files your tools do not recognize
- Use a hexadecimal editor such as WinHex
  - Record hexadecimal values in the header and use them to define a file type
- Example:
  - XIF file format is old, little information is available
  - The first 3 bytes of an XIF file are the same as a TIF file
  - Build your own header search string

Analyzing Graphics File Headers (2 of 3)

TIF file headers start with hexadecimal 49 49 2A, equivalent to ASCII II

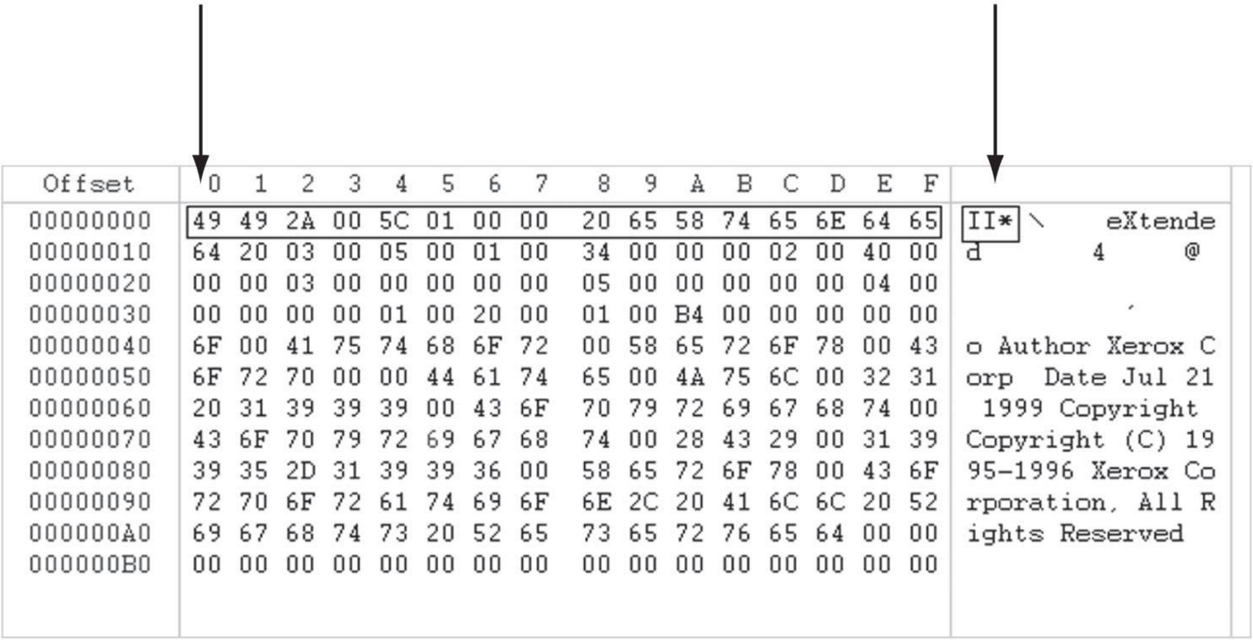


```
Offset      0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
00000000   49 49 2A 00 6E EE 05 00  80 0B 4B 2A 07 F8 06 0C   II* nî   ▌ K* ø
00000010   00 84 42 20 C0 10 03 FA  18 00 85 C2 62 50 88 2C    ▌B À  ú  ▌ÅbP▌,
00000020   2A 0F 12 88 C6 20 EF F8  98 08 01 05 01 C2 63 D1   *  ▌Æ ïø▌     ÅcÑ
00000030   A8 7C 4E 4D 24 88 45 E4  F2 89 5C 1A 39 2B 96 4C   ¨|NM$▌Eäò▌\ 9+▌L
00000040   26 53 39 A4 A6 4B 35 9A  C6 67 13 59 1C EE 7D 16   &S9¤¦K5▌Æg Y î}
00000050   9B CC 27 51 27 E4 7C 06  FE 8F BF DF 70 87 EC 51   ▌Ì'Q'ä| þ ¿ßp▌ìQ
00000060   FF 1C 01 80 C0 C0 00 15  56 3F 0E 86 BF A9 00 60   ÿ  €ÀÀ  V? ▌¿© `
00000070   48 28 00 FD B0 00 1F 6F  CA 2D 6A 91 58 9B 42 00   H( ý°  oÊ-j´X▌B
00000080   51 C0 10 06 38 04 7D D3  40 36 B8 80 00 09 5F B9   QÀ  8 }Ó@6¸▌  _¹
00000090   D2 61 8F E0 14 86 DA 05  B5 43 29 F1 C8 BB F9 F5   Òa à ▌Ú µC)ñÈ»ùõ
000000A0   4B 84 51 41 00 4C 03 F9  FE FA C4 D2 00 A0 7C 03   K▌QA L ùþúÄÒ  |
000000B0   E6 C3 05 8F 48 24 51 F0  04 86 29 26 00 D1 61 00   æÃ  H$Qð ▌)& Ña
```

Figure 8-17 A TIF file open in WinHex

Source: X-Ways AG, *www.x-ways.net*

Analyzing Graphics File Headers (3 of 3)



XIF file header

ASCII equivalent shows the same beginning values as a TIF extension

```
 Offset    0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
00000000  49 49 2A 00 5C 01 00 00  20 65 58 74 65 6E 64 65  II* \    eXtende
00000010  64 20 03 00 05 00 01 00  34 00 00 00 02 00 40 00  d       4     @
00000020  00 00 03 00 00 00 00 00  05 00 00 00 00 00 04 00
00000030  00 00 00 00 01 00 20 00  01 00 B4 00 00 00 00 00            ´
00000040  6F 00 41 75 74 68 6F 72  00 58 65 72 6F 78 00 43  o Author Xerox C
00000050  6F 72 70 00 00 44 61 74  65 00 4A 75 6C 00 32 31  orp  Date Jul 21
00000060  20 31 39 39 39 00 43 6F  70 79 72 69 67 68 74 00   1999 Copyright
00000070  43 6F 70 79 72 69 67 68  74 00 28 43 29 00 31 39  Copyright (C) 19
00000080  39 35 2D 31 39 39 36 00  58 65 72 6F 78 00 43 6F  95-1996 Xerox Co
00000090  72 70 6F 72 61 74 69 6F  6E 2C 20 41 6C 6C 20 52  rporation, All R
000000A0  69 67 68 74 73 20 52 65  73 65 72 76 65 64 00 00  ights Reserved
000000B0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
```

Figure 8-18 An XIF file open in WinHex

Source: X-Ways AG, *www.x-ways.net*

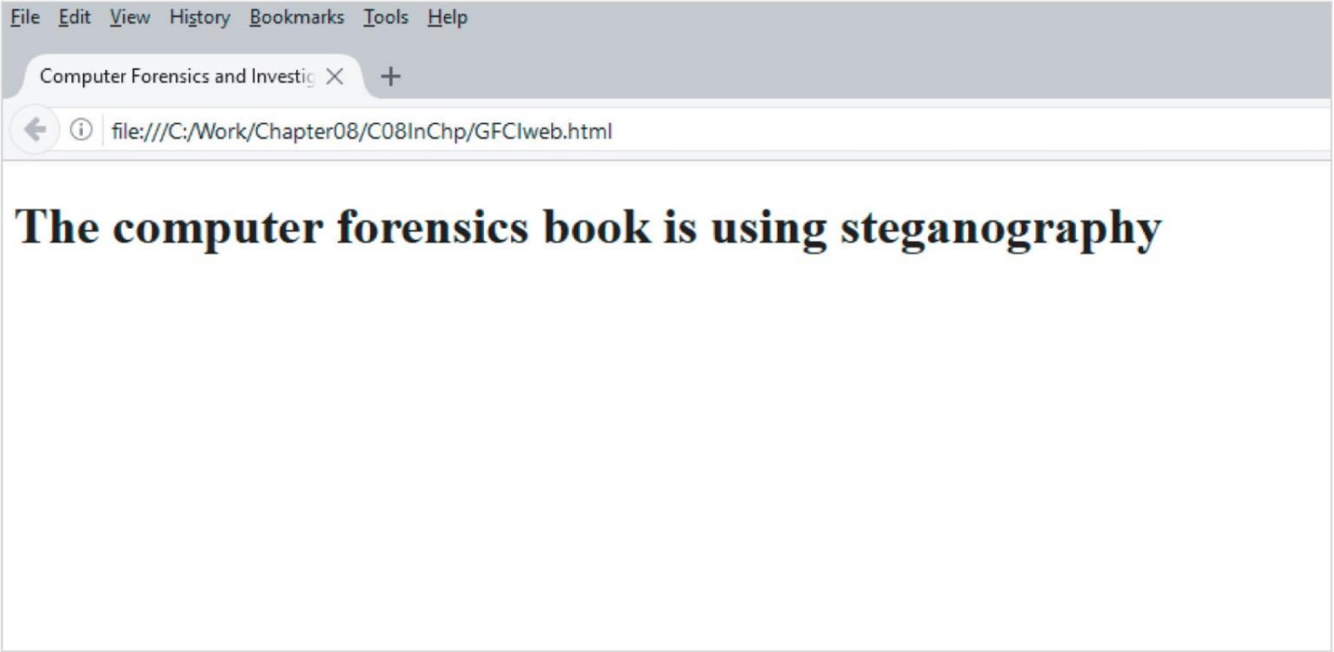
Tools for Viewing Images

- After recovering a graphics file
  - Use an image viewer to open and view it
- No one viewer program can read every file format
  - Having many different viewer programs is best
- Most GUI forensics tools include image viewers that display common image formats
- Be sure to analyze, identify, and inspect every unknown file on a drive

Understanding Steganography in Graphics Files (1 of 7)

- Steganography hides information inside image files
  - An ancient technique
- Two major forms: insertion and substitution
- Insertion
  - Hidden data is not displayed when viewing host file in its associated program
    - You need to analyze the data structure carefully
  - Example: Web page

Understanding Steganography in Graphics Files (2 of 7)

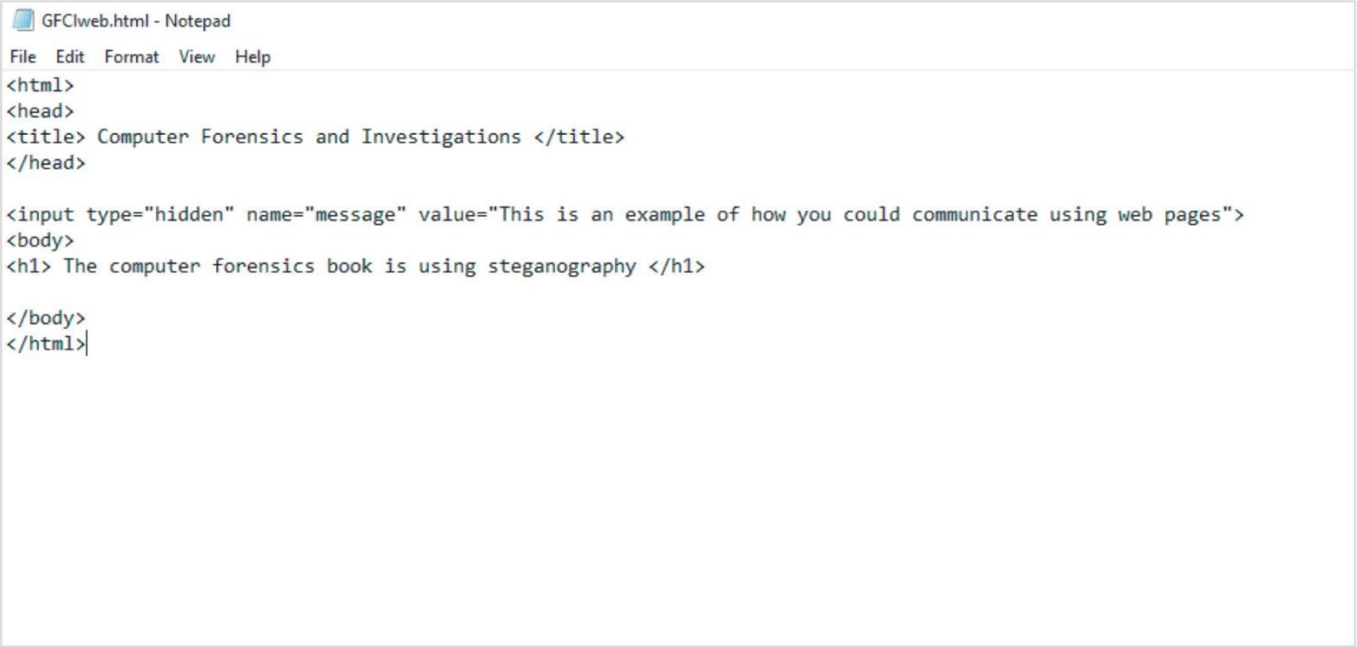

File Edit View History Bookmarks Tools Help
Computer Forensics and Investig
file:///C:/Work/Chapter08/C08InChp/GFCIweb.html

The computer forensics book is using steganography

Figure 8-19 A simple Web page displayed in a Web browser

Source: The Mozilla Foundation, *www.mozilla.org*

Understanding Steganography in Graphics Files (3 of 7)



```
<html>
<head>
<title> Computer Forensics and Investigations </title>
</head>

<input type="hidden" name="message" value="This is an example of how you could communicate using web pages">
<body>
<h1> The computer forensics book is using steganography </h1>

</body>
</html>
```

Figure 8-20 The HTML code reveals hidden text

Source: The Mozilla Foundation, *www.mozilla.org*

Understanding Steganography in Graphics Files (4 of 7)

- Substitution
  - Replaces bits of the host file with other bits of data
  - Usually change the last two LSBs (**least significant bit**)
  - Detected with steganalysis tools (a.k.a - steg tools)
- You should inspect all files for evidence of steganography
- Clues to look for:
  - Duplicate files with different hash values
  - Steganography programs installed on suspect’s drive

Understanding Steganography in Graphics Files (5 of 7)

Table 8-1	Bit breakdown of a secret message
Original Pixel	**Altered Pixel**
1010 1010	1010 1001
1001 1101	1001 1110
1111 0000	1111 0011
0011 1111	0011 1100

Understanding Steganography in Graphics Files (6 of 7)

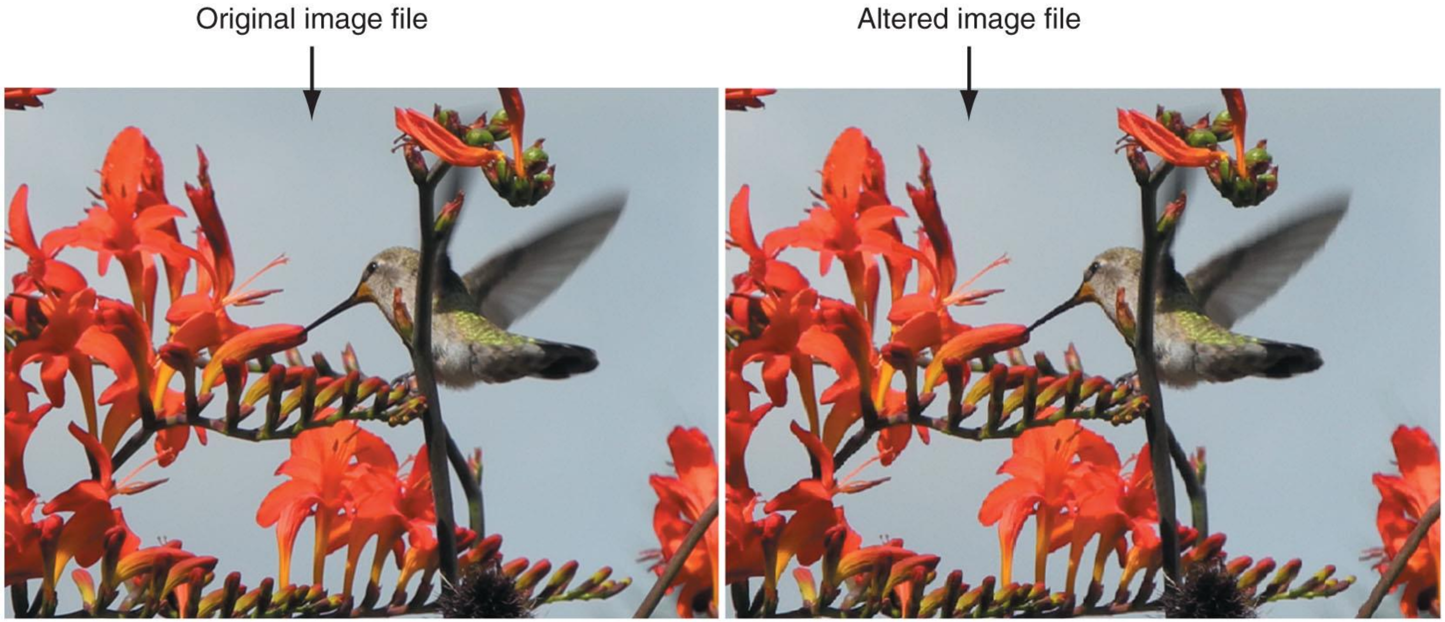
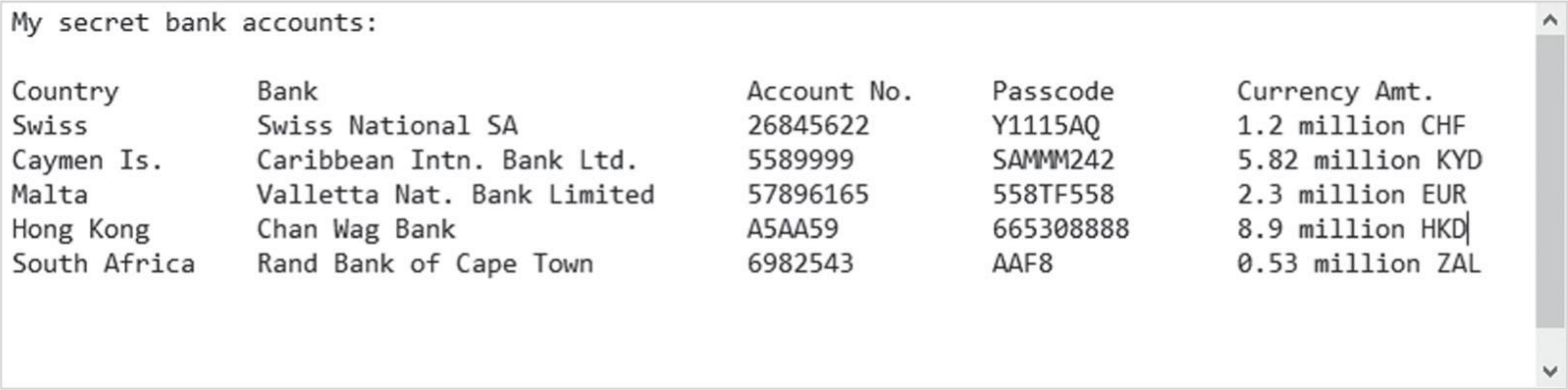


Figure 8-21 Original and altered images

Understanding Steganography in Graphics Files (7 of 7)



```
My secret bank accounts:

Country         Bank                            Account No.     Passcode        Currency Amt.
Swiss           Swiss National SA               26845622        Y1115AQ         1.2 million CHF
Caymen Is.      Caribbean Intn. Bank Ltd.       5589999         SAMMM242        5.82 million KYD
Malta           Valletta Nat. Bank Limited      57896165        558TF558        2.3 million EUR
Hong Kong       Chan Wag Bank                   A5AA59          665308888       8.9 million HKD
South Africa    Rand Bank of Cape Town          6982543         AAF8            0.53 million ZAL
```

Figure 8-22 A hidden message in the altered image

Using Steganalysis Tools

- Use steg tools to detect, decode, and record hidden data
- Detect variations of the graphic image
  - When done correctly you cannot detect hidden data in most cases
- Check to see whether the file size, image quality, or file extensions have changed

Understanding Copyright Issues with Graphics

- Steganography has been used to protect copyrighted material
  - By inserting digital watermarks into a file
- Digital investigators need to aware of copyright laws
- Copyright laws for Internet are not clear
  - There is no international copyright law
- Check the U.S. Copyright Office
  - U.S. Copyright Office identifies what can and can't be covered under copyright law in U.S.
- **Fair use**
  - Another guideline to consider

Summary (1 of 3)

- Three types of graphics files
  - Bitmap
  - Vector
  - Metafile
- Image quality depends on various factors
- Standard file formats: .gif, .jpeg, .bmp, and .tif
- Nonstandard file formats: .tga, .rtl, .psd, and .svg
- Some image formats compress their data
  - Lossless compression
  - Lossy compression

Summary (2 of 3)

- Digital camera photos are typically in raw and EXIF JPEG formats
- Recovering image files
  - Carving file fragments
  - Rebuilding image headers
- The Internet is best for learning more about file formats and their extensions
- Software
  - Image editors
  - Image viewers

Summary (3 of 3)

- Steganography
  - Hides information inside image files
  - Forms
    - - Insertion
    - - Substitution
- Steganalysis
  - Finds whether image files hide information
- Fair use allows using copyrighted material for noncommercial or educational purposes without having to compensate the material’s originator or owner