Guide to Computer Forensics and Investigations Fourth Edition

Chapter 10
Recovering Graphics Files

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

- Contains digital photographs, line art, three-dimensional 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**
  - Pixels are stored in rows
  - Better for printing
- Image quality
  - Screen **resolution**
  - Software
  - Number of color bits used per pixel

Understanding Vector Graphics

- Characteristics
  - Lines instead of dots
  - Store only the calculations for drawing lines and shapes
  - Smaller size
  - Preserve quality when image is enlarged
- CorelDraw, Adobe Illustrator

Understanding Metafile Graphics

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

Understanding Graphics File Formats

- Standard bitmap file formats
  - 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 (continued)

- Nonstandard graphics file formats
  - Targa (.tga)
  - Raster Transfer Language (.rtl)
  - Adobe Photoshop (.psd) and Illustrator (.ai)
  - Freehand (.fh9)
  - Scalable Vector Graphics (.svg)
  - Paintbrush (.pcx)
- Search the Web for software to manipulate unknown image formats

Understanding Digital Camera File Formats

- 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 Camera File Formats (continued)

- Examining the raw file format (continued)
  - 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 JEIDA as a standard for storing metadata in JPEG and TIFF files

Understanding Digital Camera File Formats (continued)

- Examining the Exchangeable Image File format (continued)
  - EXIF format collects metadata
    - Investigators can learn more about the type of digital camera and the environment in which pictures were taken
  - EXIF file stores metadata at the beginning of the file

Understanding Digital Camera File Formats (continued)

Figure 10-1 Identical EXIF and JPEG pictures

Understanding Digital Camera File Formats (continued)

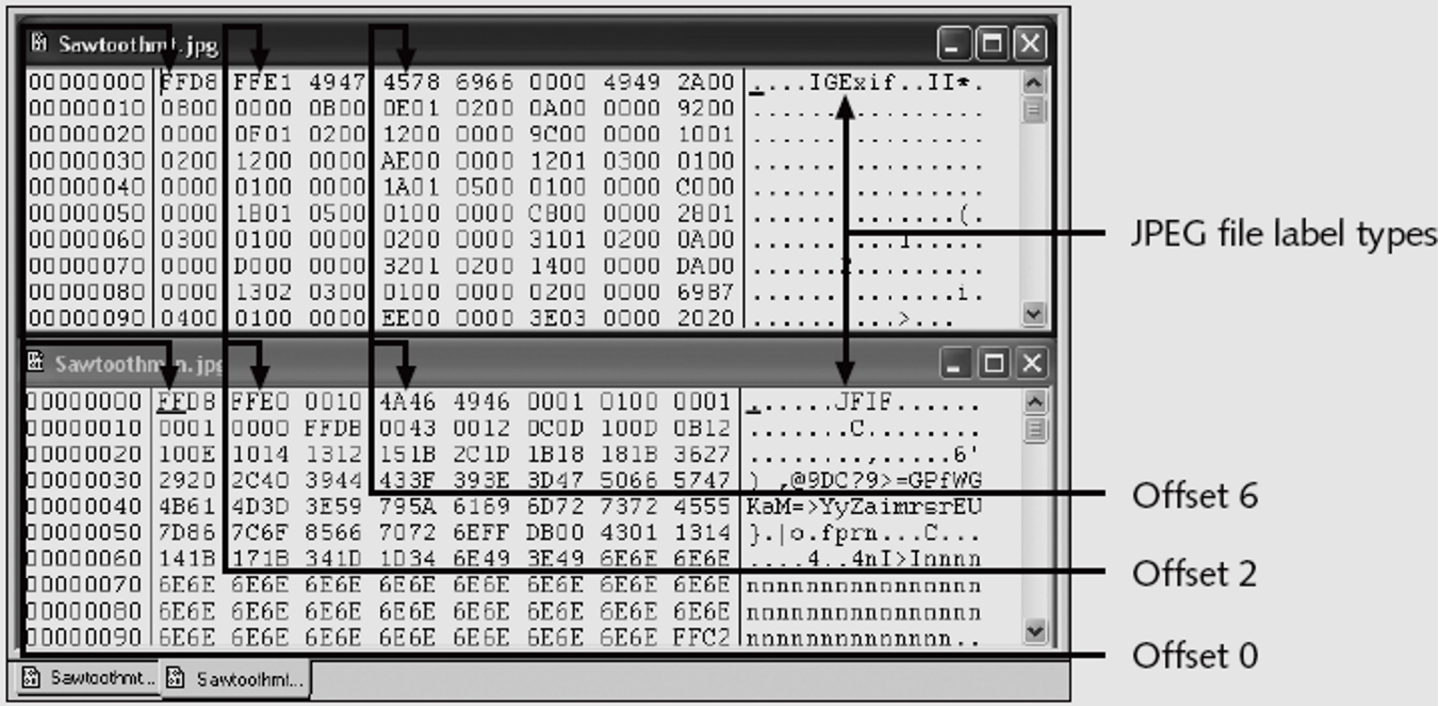


Figure 10-2 Differences in EXIF and JPEG file header information

Understanding Digital Camera File Formats (continued)

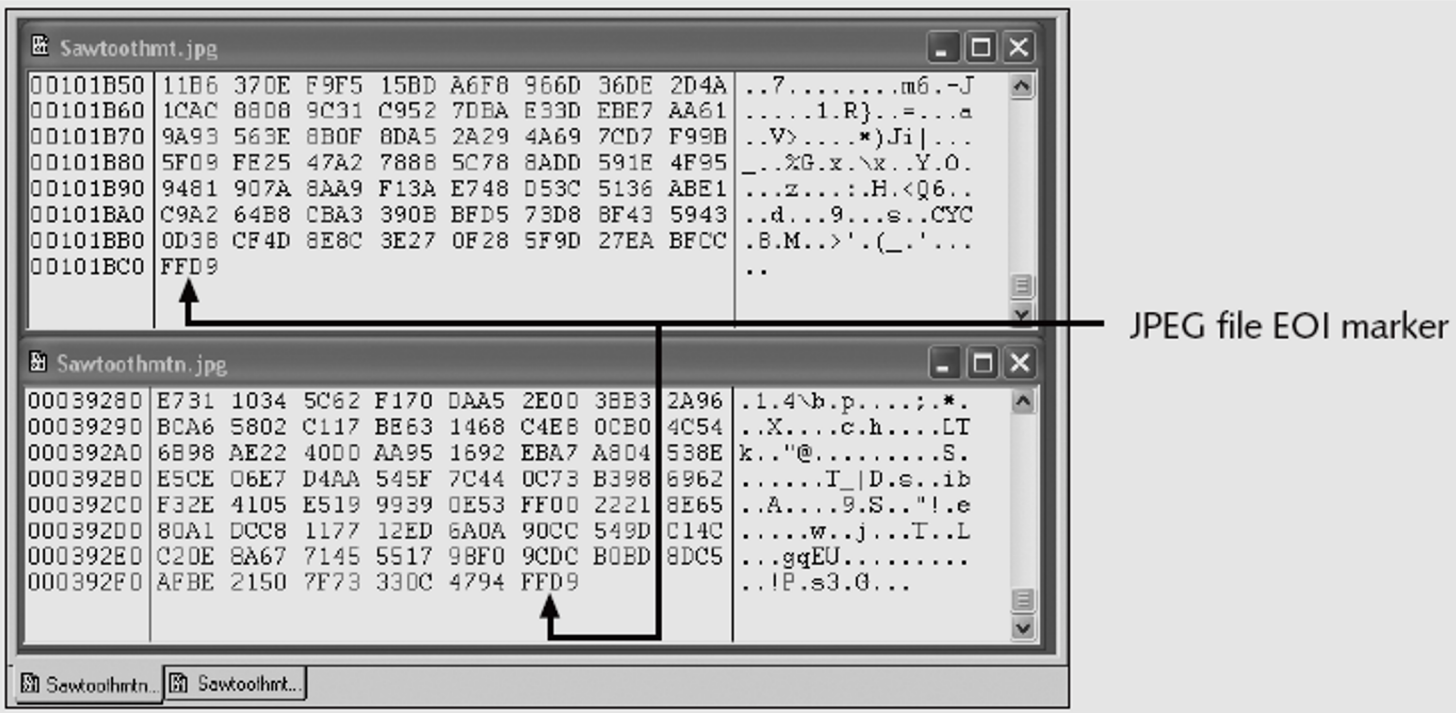


Figure 10-3 EOI marker FFD9 for all JPEG files

Understanding Digital Camera File Formats (continued)

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

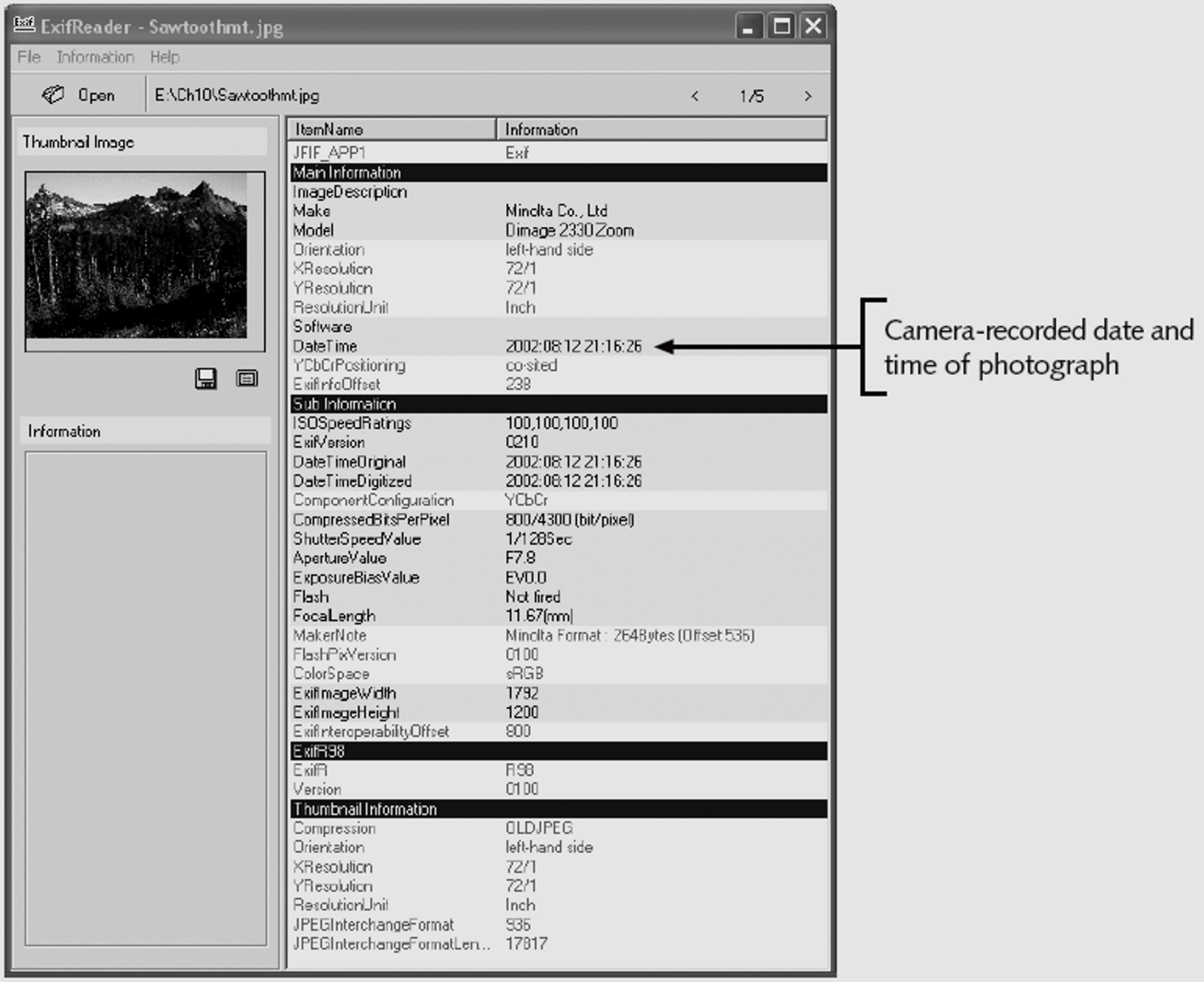


Figure 10-4 Exif Reader displaying metadata from an EXIF JPEG file

Understanding Data Compression

- Some image formats compress their data
  - GIF, JPEG, PNG
- Others, like BMP, do not compress their data
  - Use data compression tools for those formats
- **Data compression**
  - Coding of 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
- Computer 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

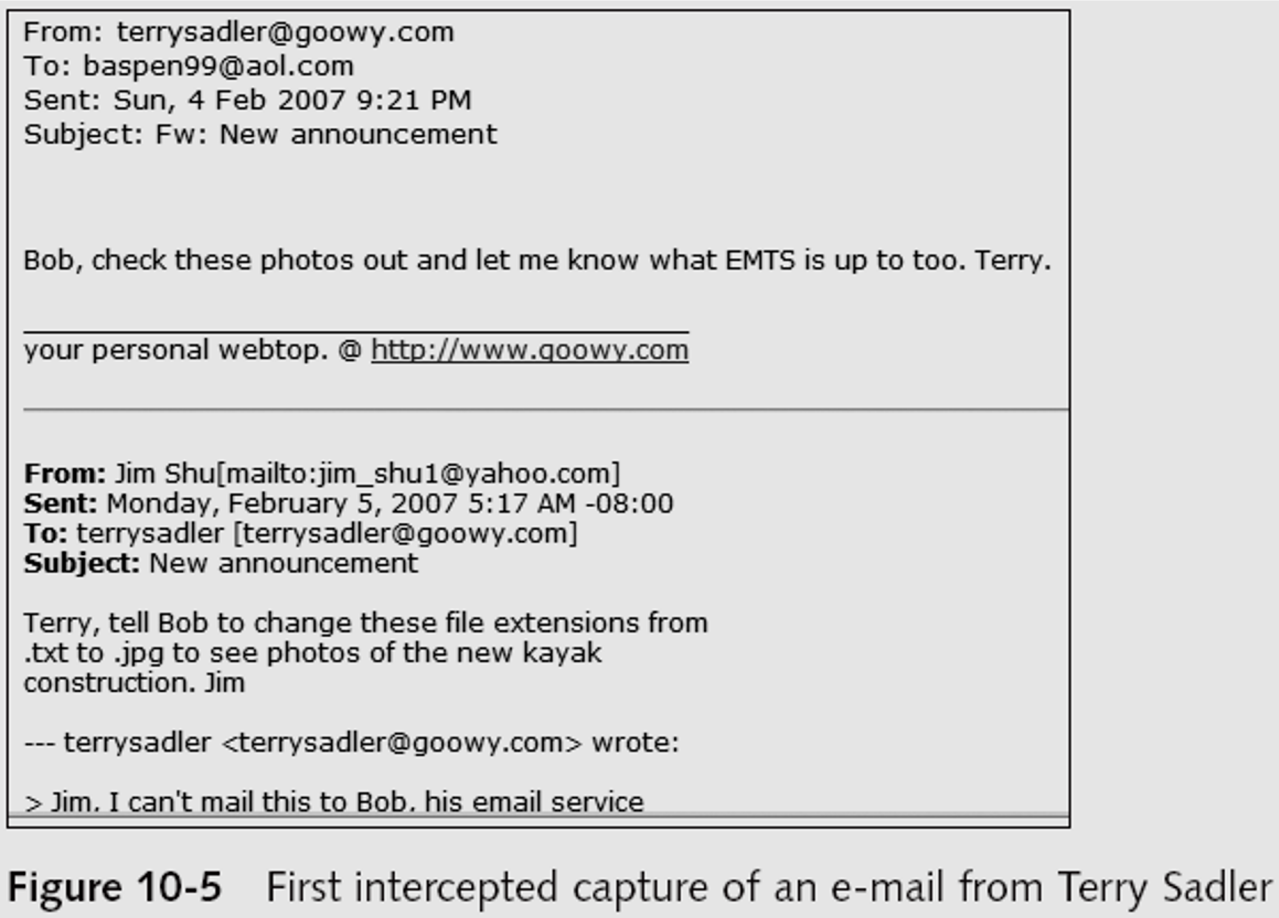
Identifying Graphics File Fragments

- Carving or salvaging
  - Recovering all file fragments
- Computer forensics tools
  - Carve from slack and free space
  - Help identify image files fragments and put them together

Repairing Damage Headers

- Use good header samples
- Each image file has a unique file header
  - JPEG: FF D8 FF E0 00 10
  - Most JPEG files also include JFIF string
- Exercise:
  - Investigate a possible intellectual property theft by a contract employee of Exotic Mountain Tour Service (EMTS)

Searching for and Carving Data from Unallocated Space



From: terrysadler@goowy.com
To: baspen99@aol.com
Sent: Sun, 4 Feb 2007 9:21 PM
Subject: Fw: New announcement

Bob, check these photos out and let me know what EMTS is up to too. Terry.

_____
your personal webtop. @ http://www.goowy.com

From: Jim Shu[mailto:jim_shu1@yahoo.com]
Sent: Monday, February 5, 2007 5:17 AM -08:00
To: terrysadler [terrysadler@goowy.com]
Subject: New announcement

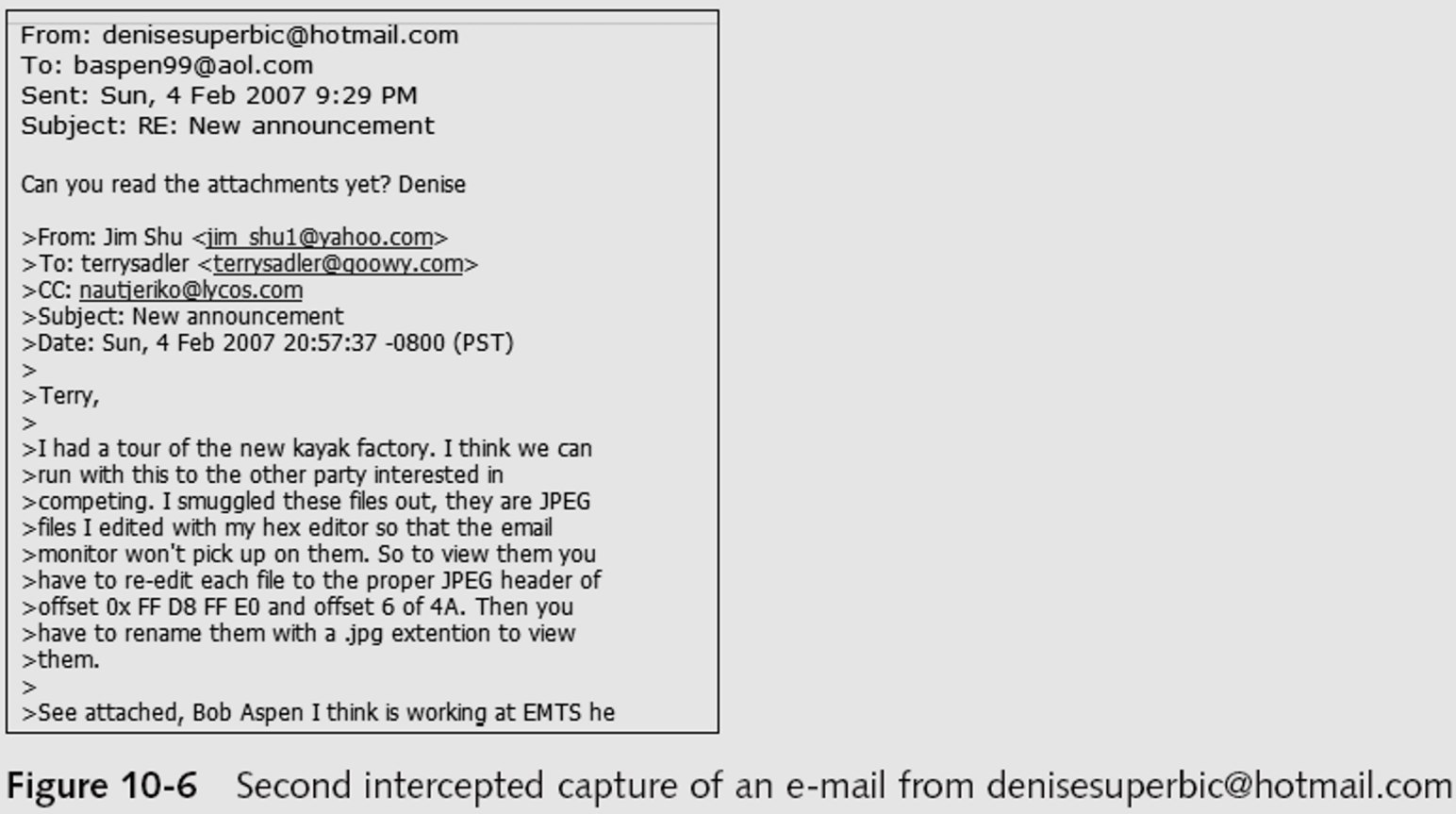
Terry, tell Bob to change these file extensions from .txt to .jpg to see photos of the new kayak construction. Jim

--- terrysadler <terrysadler@goowy.com> wrote:

> Jim. I can't mail this to Bob. his email service

Figure 10-5 First intercepted capture of an e-mail from Terry Sadler

Searching for and Carving Data from Unallocated Space (continued)



From: denisesuperbic@hotmail.com
To: baspen99@aol.com
Sent: Sun, 4 Feb 2007 9:29 PM
Subject: RE: New announcement

Can you read the attachments yet? Denise

>From: Jim Shu <jim_shu1@yahoo.com>
>To: terrysadler <terrysadler@goowy.com>
>CC: nautjeriko@lycos.com
>Subject: New announcement
>Date: Sun, 4 Feb 2007 20:57:37 -0800 (PST)
>
>Terry,
>
>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 with a .jpg extention to view
>them.
>
>See attached, Bob Aspen I think is working at EMTS he

Figure 10-6 Second intercepted capture of an e-mail from denisesuperbic@hotmail.com

Searching for and Carving Data from Unallocated Space (continued)

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

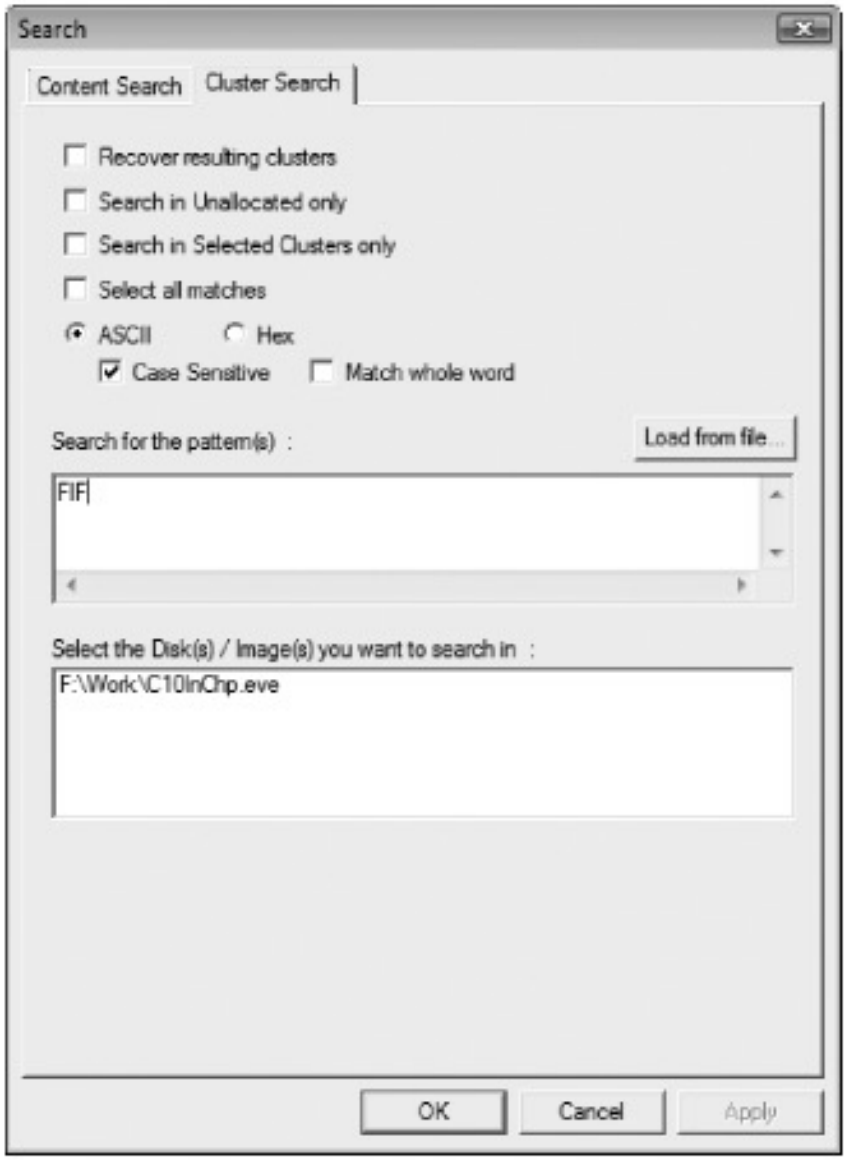


Figure 10-7 Searching clusters in ProDiscover

Searching for and Carving Data from Unallocated Space (continued)

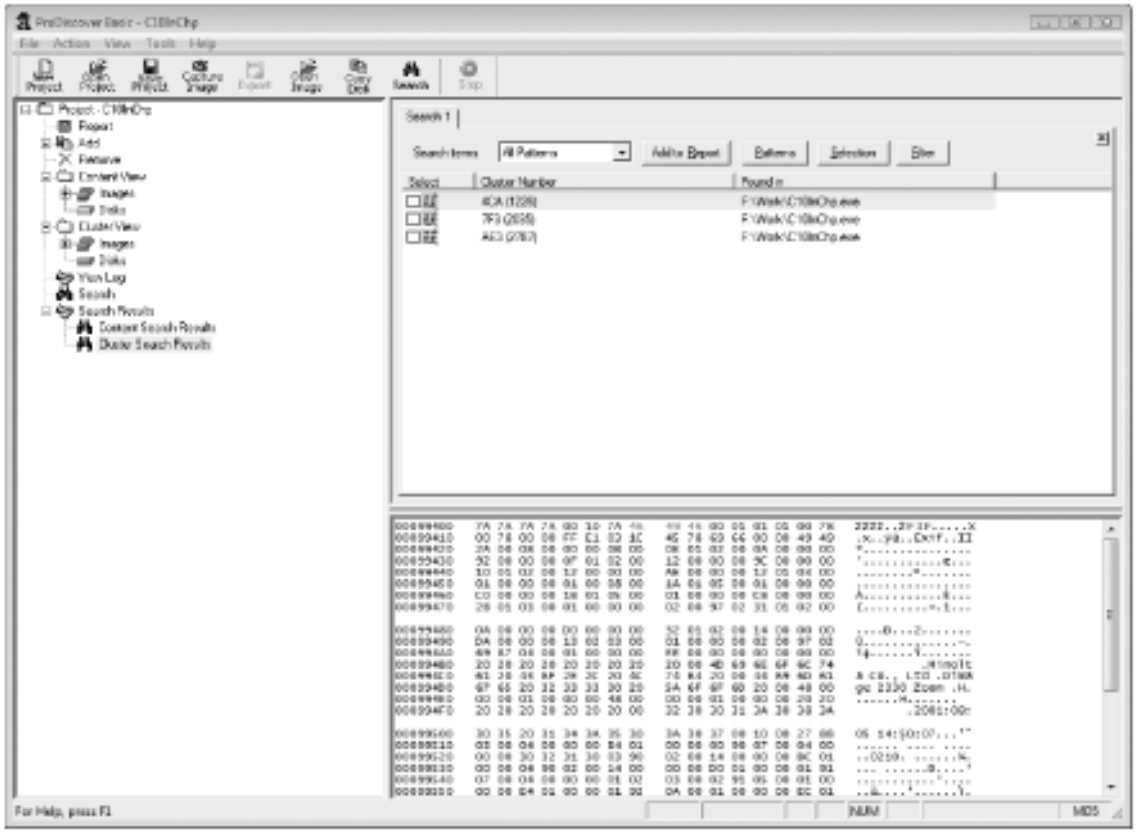


Figure 10-8 Completed cluster search for FIF

Searching for and Carving Data from Unallocated Space (continued)

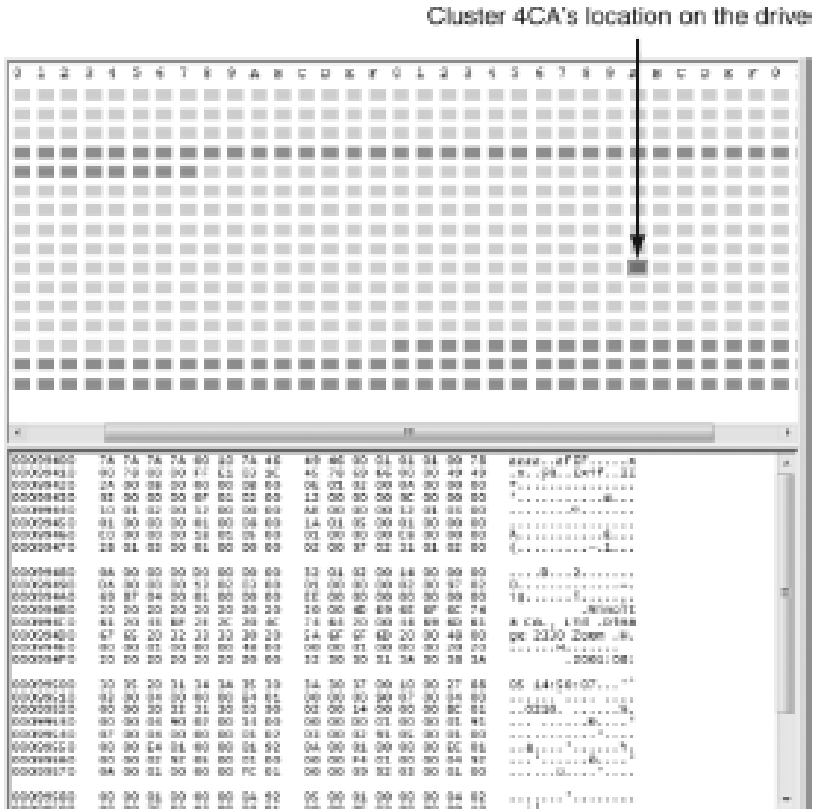


Figure 10-9 Viewing cluster use and location of search hit for 4CA(1226)

Searching for and Carving Data from Unallocated Space (continued)

File header overwritten with zzzz

```
00099400  7A 7A 7A 7A 00 10 7A 46  49 46 00 01 01 01 00 78  zzzz..zFIF.....x
00099410  00 78 00 00 FF E1 03 1C  45 78 69 66 00 00 49 49  .x..ÿá..Exif..II
00099420  2A 00 08 00 00 00 08 00  0E 01 02 00 0A 00 00 00  *...............
00099430  92 00 00 00 0F 01 02 00  12 00 00 00 9C 00 00 00  '...........œ...
00099440  10 01 02 00 12 00 00 00  AE 00 00 00 12 01 03 00  ........®.......
00099450  01 00 00 00 01 00 08 00  1A 01 05 00 01 00 00 00  ................
00099460  C0 00 00 00 18 01 05 00  01 00 00 00 C8 00 00 00  À...........È...
00099470  28 01 03 00 01 00 00 00  02 00 97 02 31 01 02 00  (.........—.1...

00099480  0A 00 00 00 D0 00 00 00  32 01 02 00 14 00 00 00  ....Ð...2.......
00099490  DA 00 00 00 13 02 03 00  01 00 00 00 02 00 97 02  Ú.............—.
000994A0  69 87 04 00 01 00 00 00  EE 00 00 00 00 00 00 00  i‡......î.......
000994B0  20 20 20 20 20 20 20 20  20 00 4D 69 6E 6F 6C 74  .Minolt
000994C0  61 20 43 6F 2E 2C 20 4C  74 64 20 00 44 69 6D 61  a Co., Ltd .Dima
000994D0  67 65 20 32 33 33 30 20  5A 6F 6F 6D 20 00 48 00  ge 2330 Zoom .H.
000994E0  00 00 01 00 00 00 48 00  00 00 01 00 00 00 20 20  ......H.......
000994F0  20 20 20 20 20 20 20 00  32 30 30 31 3A 30 38 3A  .2001:08:

00099500  30 35 20 31 34 3A 35 30  3A 30 37 00 10 00 27 88  05 14:50:07...'ˆ
00099510  03 00 04 00 00 00 B4 01  00 00 00 90 07 00 04 00  ...... ´... ....
00099520  00 00 30 32 31 30 03 90  02 00 14 00 00 00 BC 01  ..0210. ......¼.
00099530  00 00 04 90 02 00 14 00  00 00 D0 01 00 00 01 91  ... ......Ð....'
00099540  07 00 04 00 00 00 01 02  03 00 02 91 05 00 01 00  ...........'....
00099550  00 00 E4 01 00 00 01 92  0A 00 01 00 00 00 EC 01  ..ä....'......ì.
00099560  00 00 02 92 05 00 01 00  00 00 F4 01 00 00 04 92  ...'......ô....'
00099570  0A 00 01 00 00 00 FC 01  00 00 09 92 03 00 01 00  ......ü....'....

00099580  00 00 01 00 00 00 0A 92  05 00 01 00 00 00 04 02  .......'........
```

Figure 10-10 Content of cluster 4CA(1226)

Searching for and Carving Data from Unallocated Space (continued)

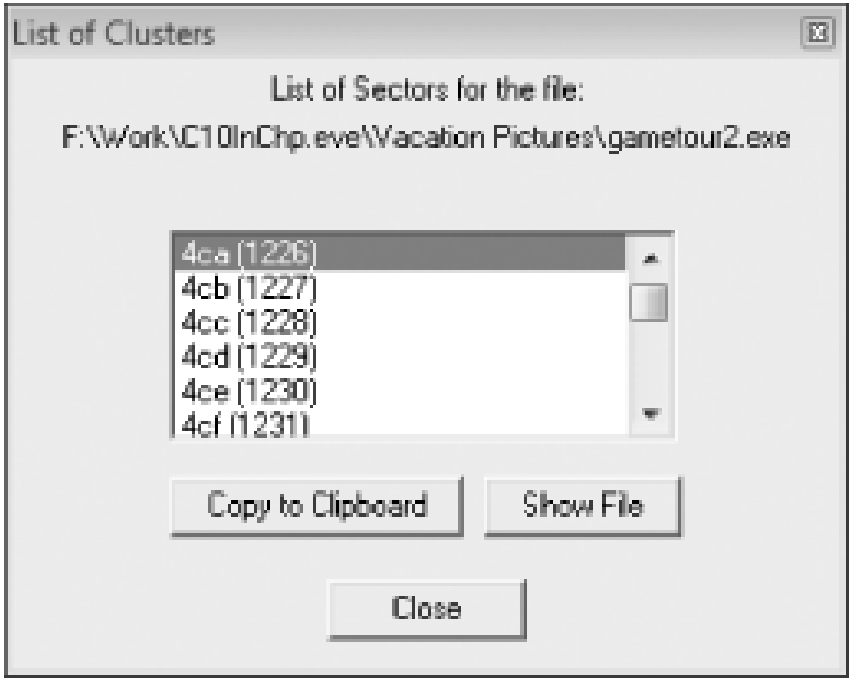


Figure 10-11 Viewing all clusters used by the gametour2.exe file

Searching for and Carving Data from Unallocated Space (continued)

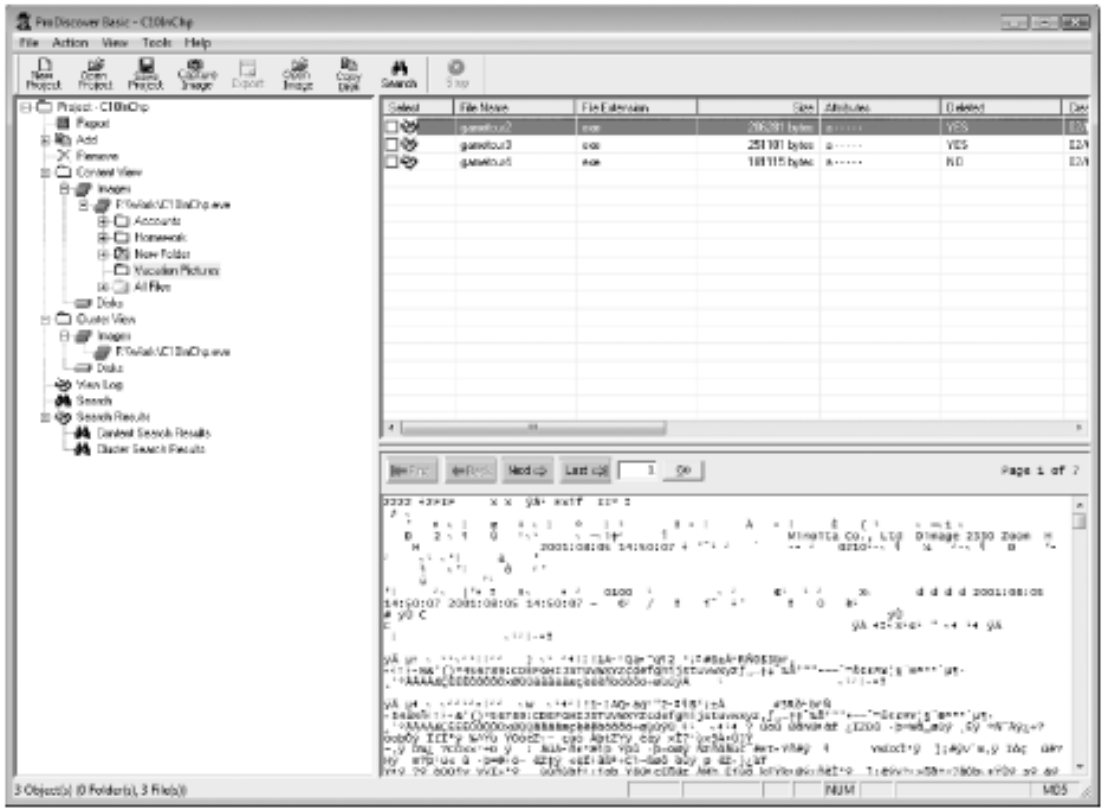


Figure 10-12 Mislabeled file that appears to be altered intentionally

Rebuilding File Headers

- Try to open the file first and follow steps if you can't see its content
- 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 (continued)

Figure 10-13 Error message indicating a damaged or an altered graphics file

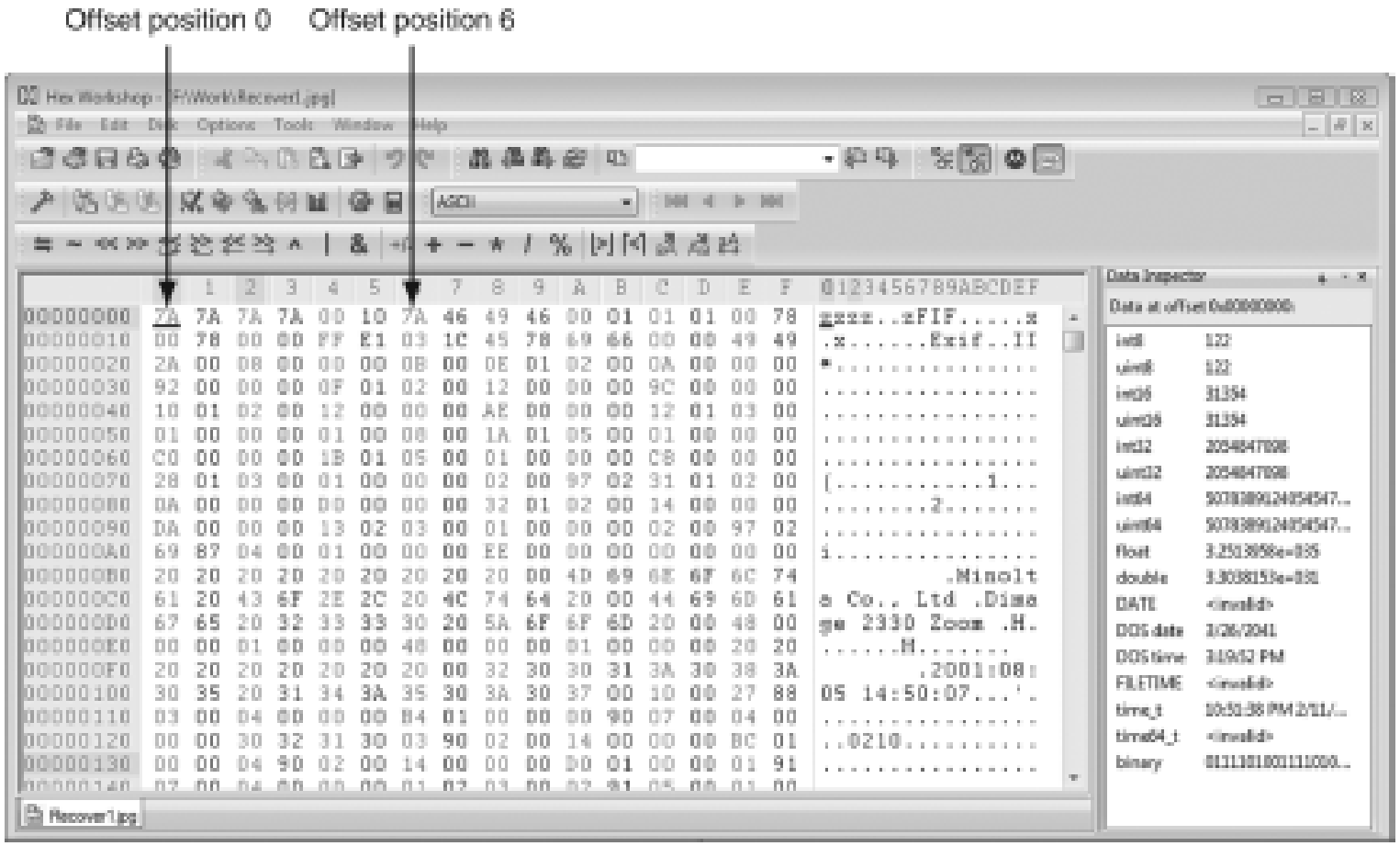


Figure 10-14 Recover1.jpg open in Hex Workshop

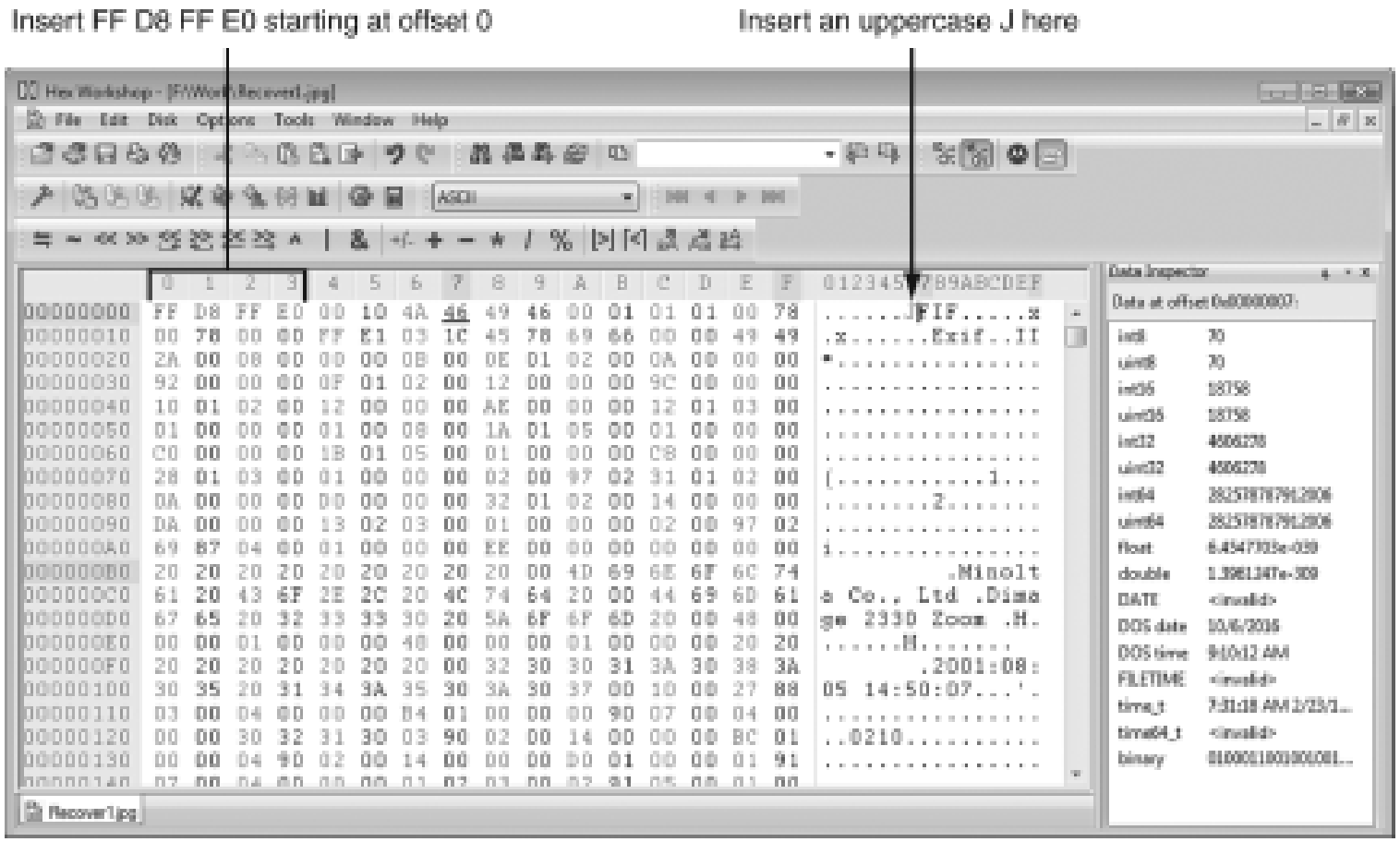
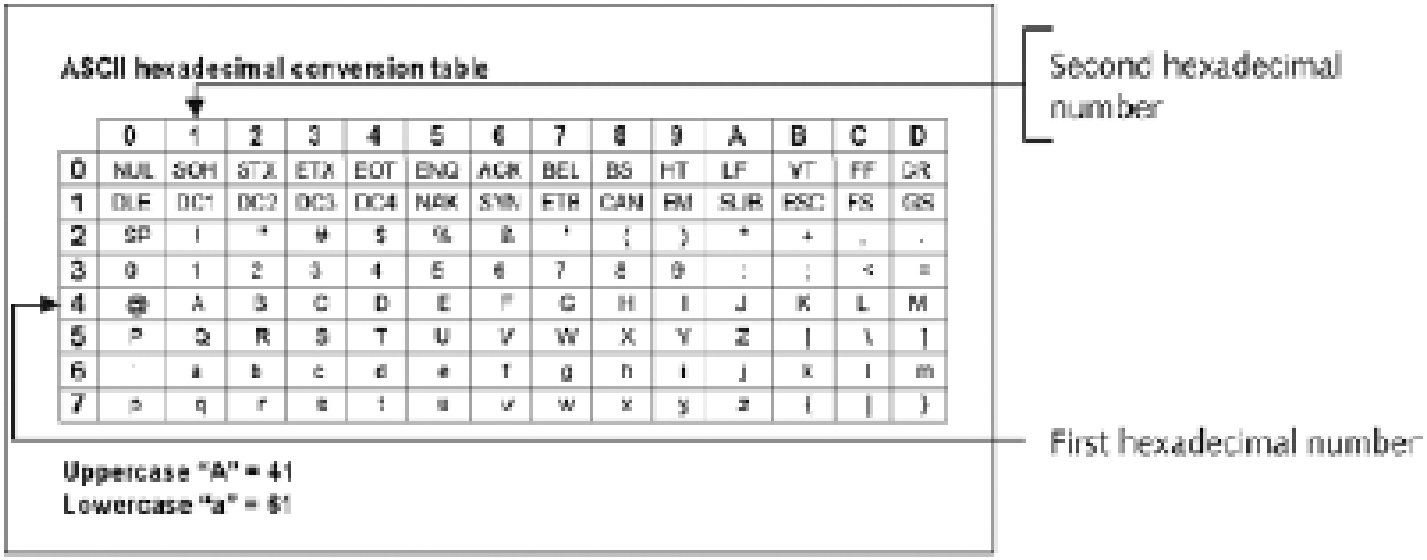


Figure 10-15 Inserting correct hexadecimal values for a JPEG file

Rebuilding File Headers (continued)



	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 10-16 ASCII equivalents of hexadecimal values

Rebuilding File Headers (continued)

Figure 10-17 Fixed1.jpg open in Microsoft Office Picture Manager

Reconstructing File Fragments

- Locate the starting and ending clusters
  - For each fragmented group of clusters in the file
- Steps
  - Locate and export all clusters of the fragmented file
  - Determine the starting and ending cluster numbers for each fragmented group of clusters
  - Copy each fragmented group of clusters in their proper sequence to a recovery file
  - Rebuild the corrupted file's header to make it readable in a graphics viewer

Reconstructing File Fragments (continued)

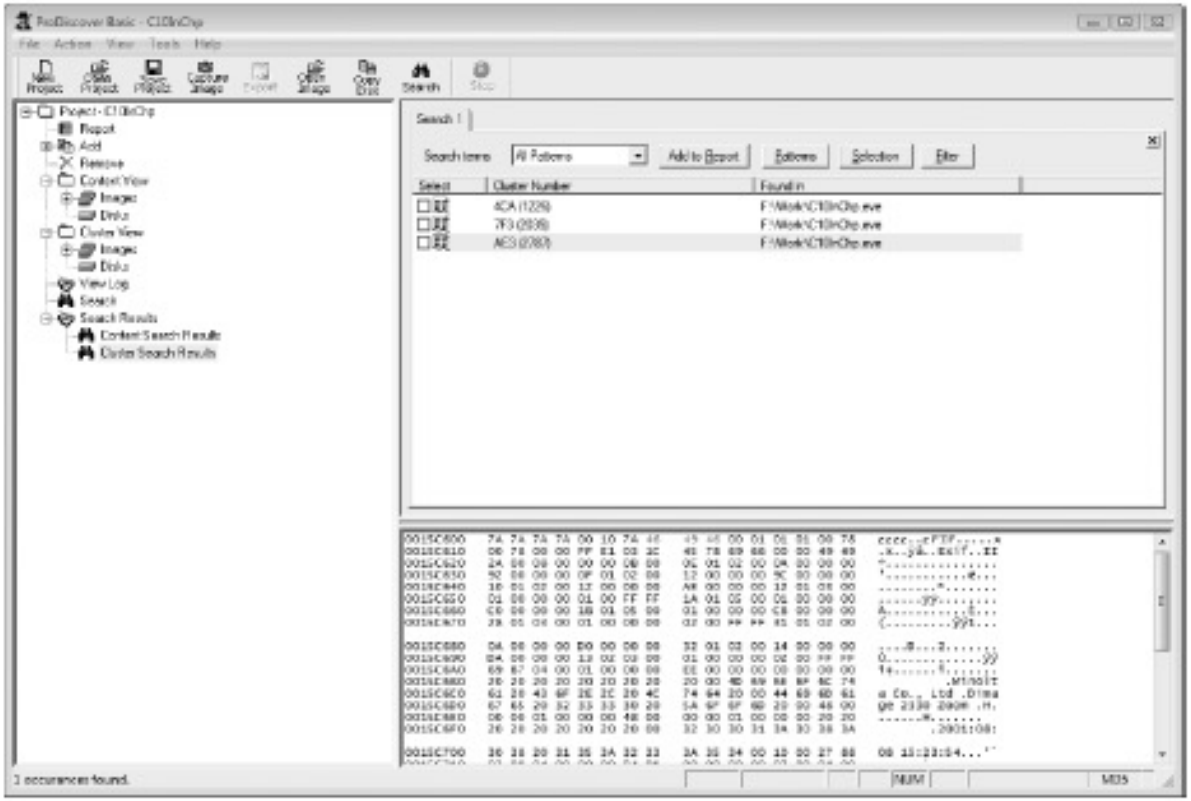


Figure 10-18 Cluster search results for the AE3(2787) cluster

Reconstructing File Fragments (continued)

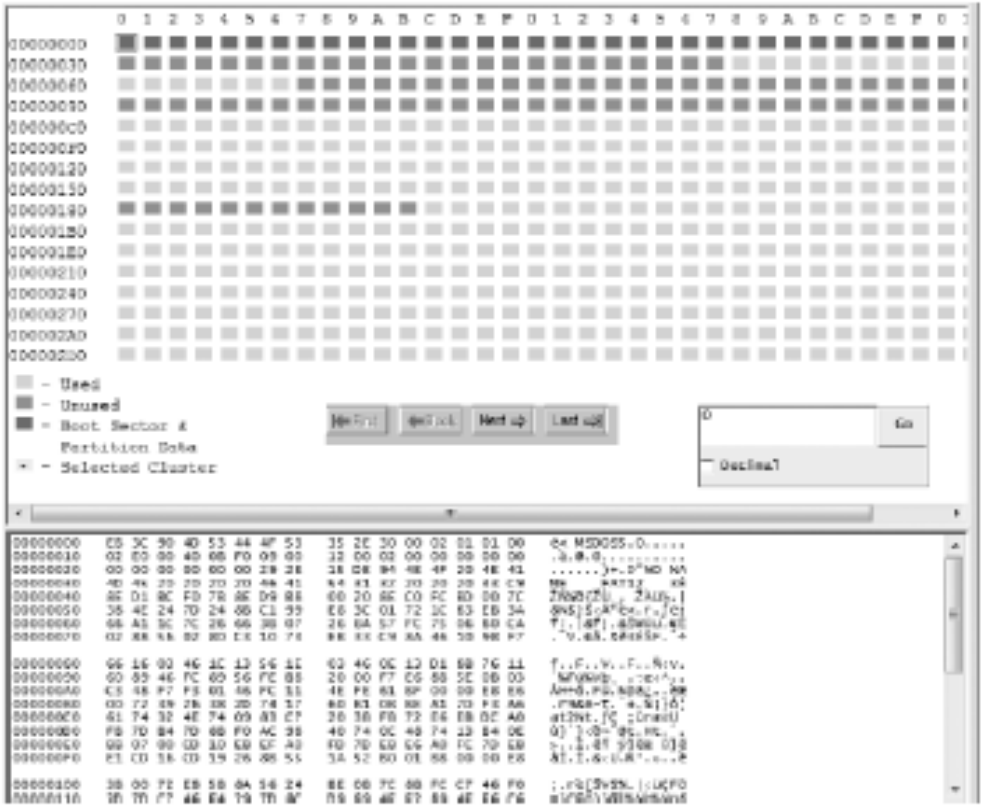


Figure 10-19 Cluster view of C10InChp.eve

Reconstructing File Fragments (continued)

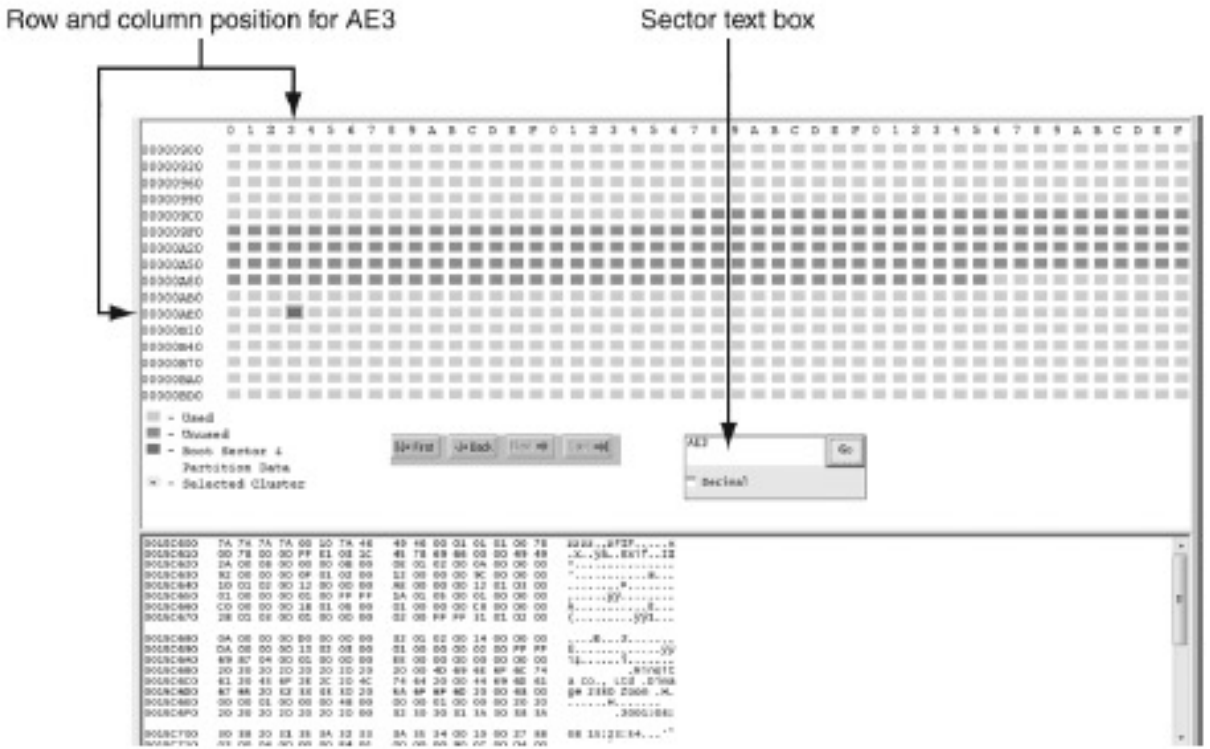


Figure 10-20 Cluster view of sector AE3

Reconstructing File Fragments (continued)

Figure 10-22 Copying all selected clusters or sectors to a file

Reconstructing File Fragments (continued)

- Remember to save the updated recovered data with a .jpg extension
- Sometimes suspects intentionally corrupt cluster links in a disk's FAT
  - Bad clusters appear with a zero value on a disk editor

Reconstructing File Fragments (continued)

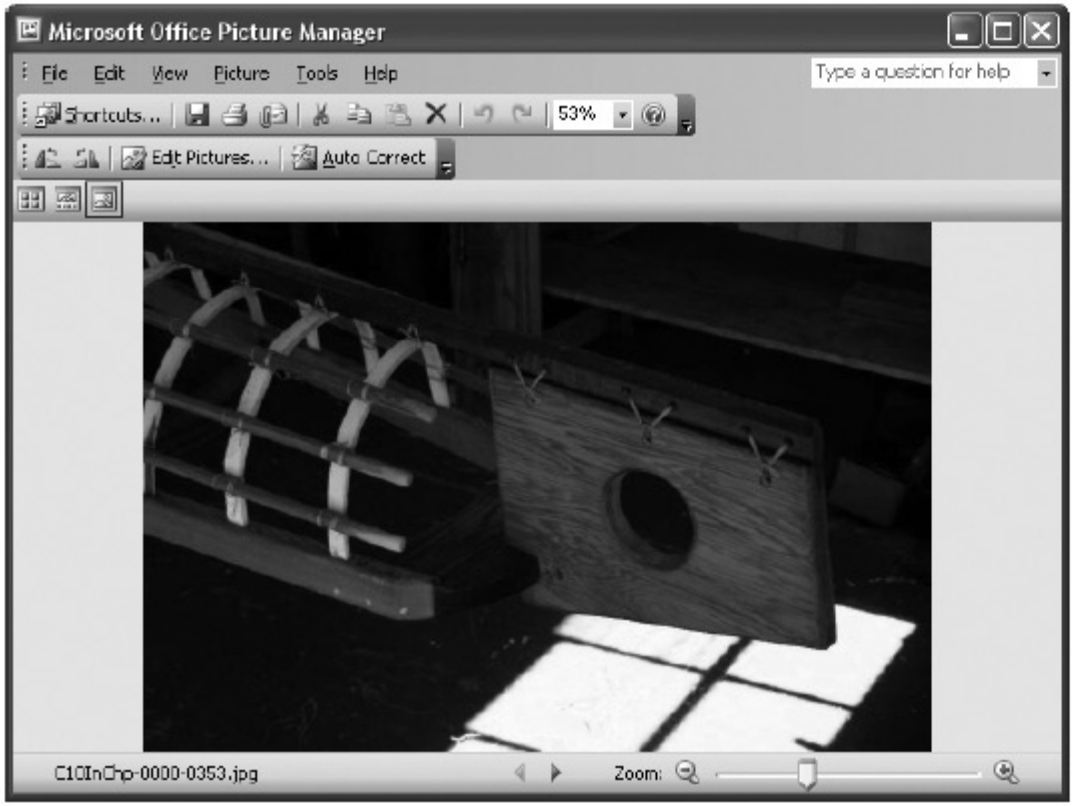
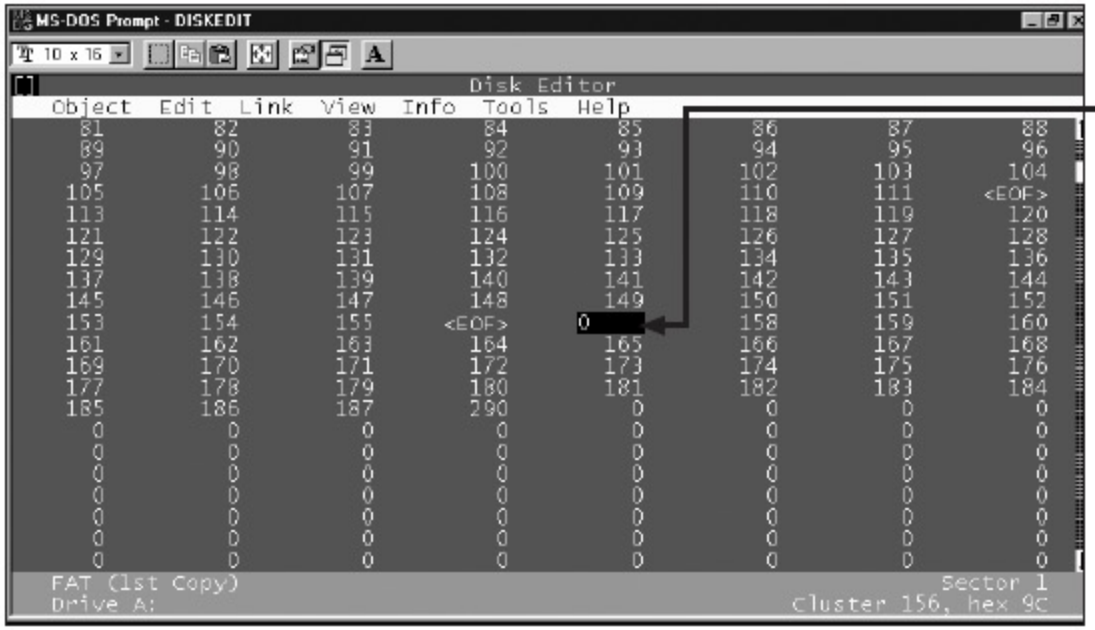


Figure 10-23 Recovered data from starting sector AE3 after Hex Workshop corrects the header

Reconstructing File Fragments (continued)



Cluster marked as bad

Figure 10-24 Bad cluster appearing as 0 in Norton DiskEdit

Identifying Unknown File Formats

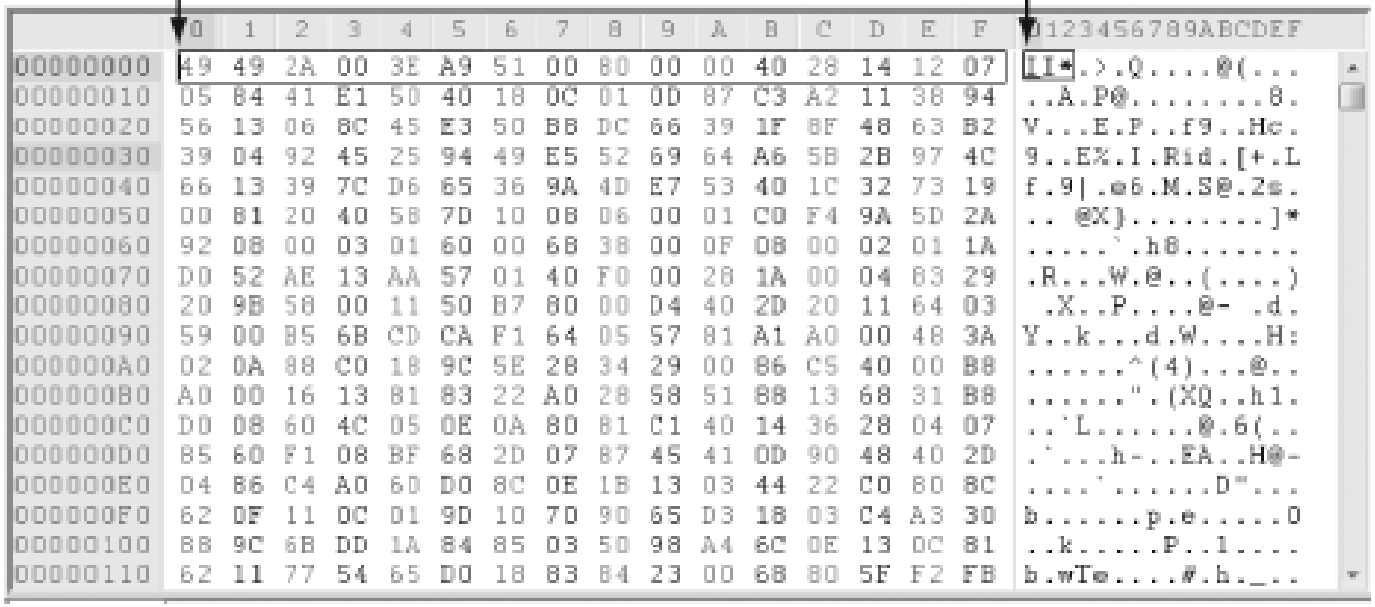
- The Internet is the best source
  - Search engines like Google
  - Find explanations and viewers
- Popular Web sites
  - www.digitek-asi.com/file_formats.html
  - www.wotsit.org
  - http://whatis.techtarget.com

Analyzing Graphics File Headers

- Necessary when you find files your tools do not recognize
- Use hex editor such as Hex Workshop
  - Record hexadecimal values on header
- Use good header samples

Analyzing Graphics File Headers (continued)

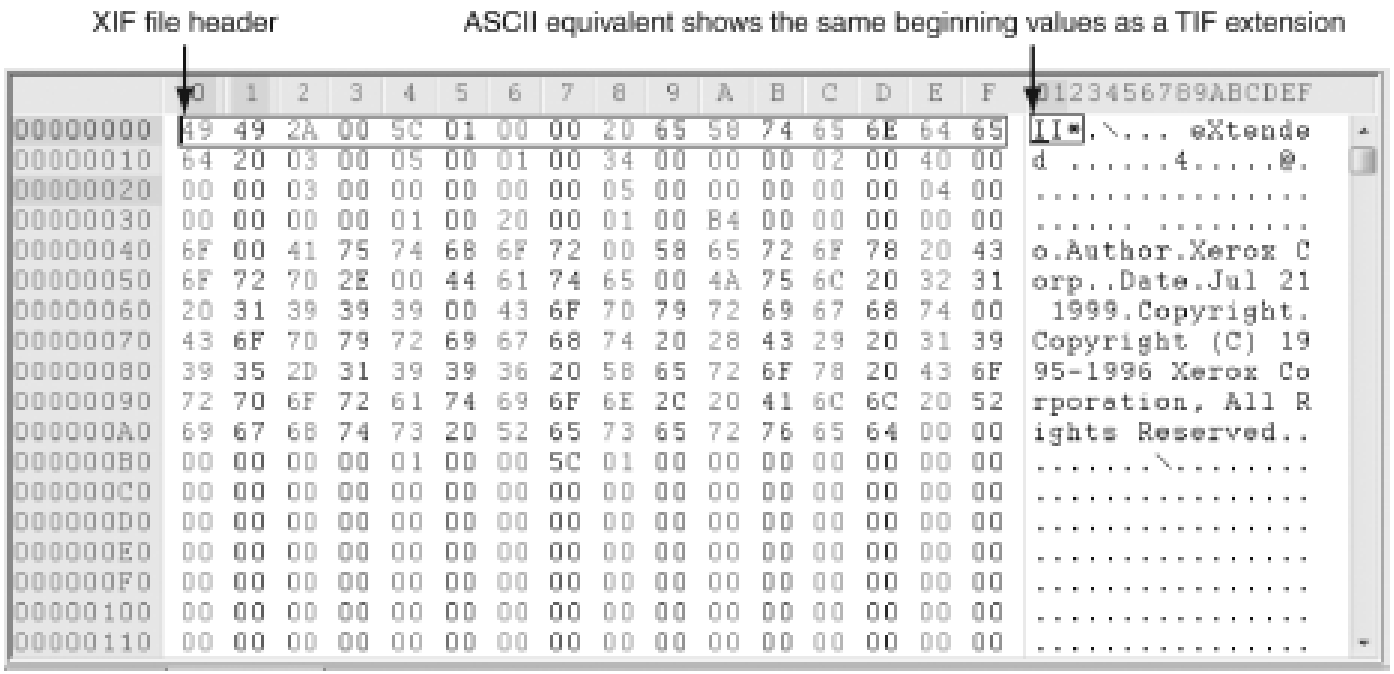
TIF file headers start with hexadecimal 49 49 2A, equivalent to ASCII II



	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
00000000	49	49	2A	00	3E	A9	51	00	80	00	00	40	28	14	12	07	II*.>.Q....@(...
00000010	05	84	41	E1	50	40	18	0C	01	0D	87	C3	A2	11	38	94	..A.P@.........8.
00000020	56	13	06	8C	45	E3	50	BB	DC	66	39	1F	8F	48	63	B2	V...E.P..f9..Hc.
00000030	39	D4	92	45	25	94	49	E5	52	69	64	A6	5B	2B	97	4C	9..E%.I.Rid.[+.L
00000040	66	13	39	7C	D6	65	36	9A	4D	E7	53	40	1C	32	73	19	f.9|.e6.M.S@.2s.
00000050	00	B1	20	40	58	7D	10	0B	06	00	01	C0	F4	9A	5D	2A	.. @X}.........]*
00000060	92	08	00	03	01	60	00	68	38	00	0F	08	00	02	01	1A	.....`.h8.......
00000070	D0	52	AE	13	AA	57	01	40	F0	00	28	1A	00	04	83	29	.R...W.@..(....)
00000080	20	9B	58	00	11	50	B7	80	00	D4	40	2D	20	11	64	03	.X..P....@- .d.
00000090	59	00	B5	6B	CD	CA	F1	64	05	57	81	A1	A0	00	48	3A	Y..k...d.W....H:
000000A0	02	0A	88	C0	18	9C	5E	28	34	29	00	86	C5	40	00	B8	......^(4)...@..
000000B0	A0	00	16	13	81	83	22	A0	28	58	51	88	13	68	31	B8	......". (XQ..h1.
000000C0	D0	08	60	4C	05	0E	0A	80	81	C1	40	14	36	28	04	07	..`L......@.6(..
000000D0	B5	60	F1	08	BF	68	2D	07	87	45	41	0D	90	48	40	2D	.`...h-..EA..H@-
000000E0	04	86	C4	A0	60	D0	8C	0E	1B	13	03	44	22	C0	80	8C	....`......D"...
000000F0	62	0F	11	0C	01	9D	10	7D	90	65	D3	18	03	C4	A3	30	b.......}.e.....0
00000100	B8	9C	6B	DD	1A	84	85	03	50	98	A4	6C	0E	13	0C	B1	..k.....P..l....
00000110	62	11	77	54	65	D0	18	83	84	23	00	68	80	5F	F2	FB	b.wTe....#.h._..

Figure 10-25 A TIF file open in Hex Workshop

Analyzing Graphics File Headers (continued)



	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
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	20	43	o.Author.Xerox C
00000050	6F	72	70	2E	00	44	61	74	65	00	4A	75	6C	20	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	20	28	43	29	20	31	39	Copyright (C) 19
00000080	39	35	2D	31	39	39	36	20	58	65	72	6F	78	20	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	01	00	00	5C	01	00	00	00	00	00	00	00	.......\.....
000000C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000000D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000000E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000000F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000100	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000110	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....

Figure 10-26 An XIF file open in Hex Workshop

Tools for Viewing Images

- Use several viewers
  - ThumbsPlus
  - ACDSee
  - QuickView
  - IrfanView
- GUI forensics tools include image viewers
  - ProDiscover
  - EnCase
  - FTK
  - X-Ways Forensics
  - iLook

Understanding Steganography in Graphics Files

- Steganography hides information inside image files
  - Ancient technique
  - Can hide only certain amount of information
- 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

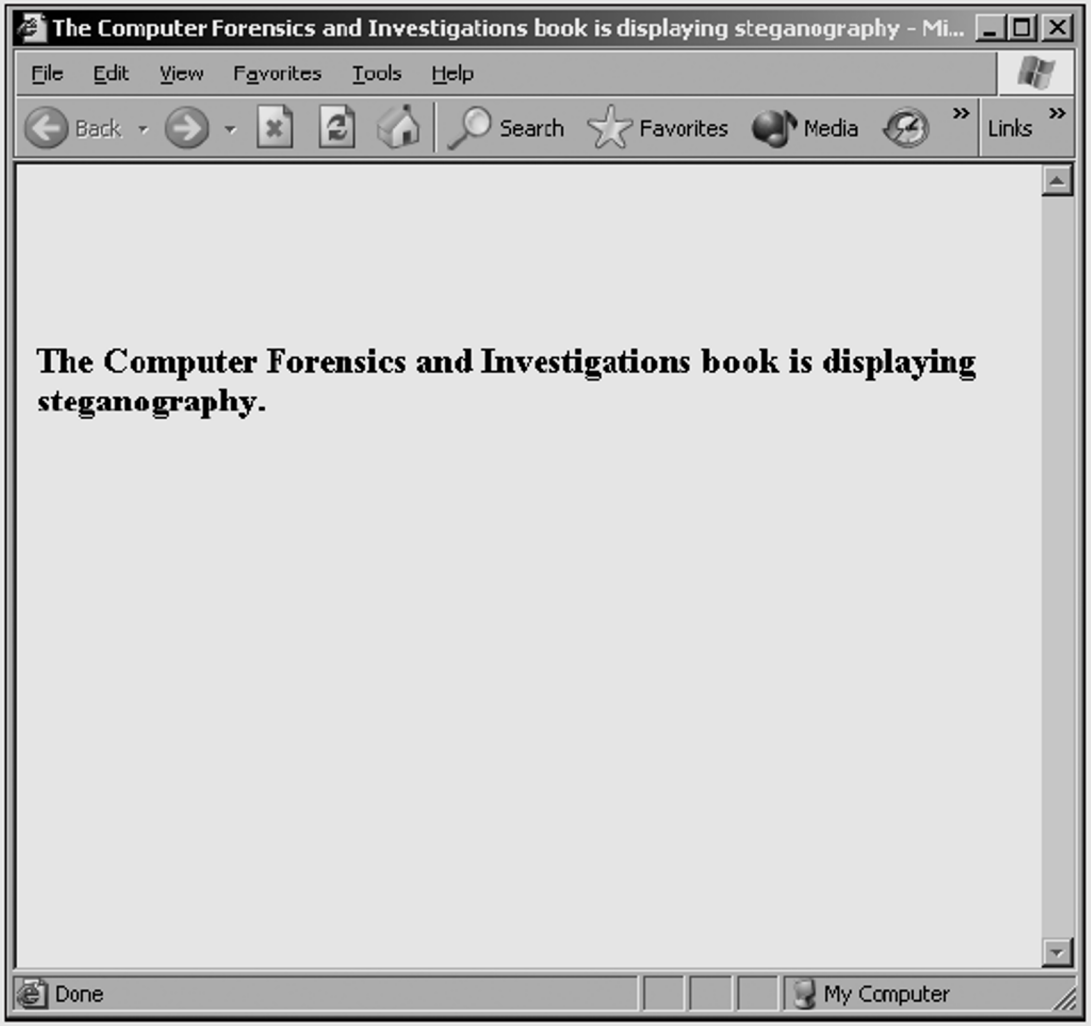


Figure 10-27 A simple Web page displayed in a Web browser

Understanding Steganography in Graphics Files (continued)

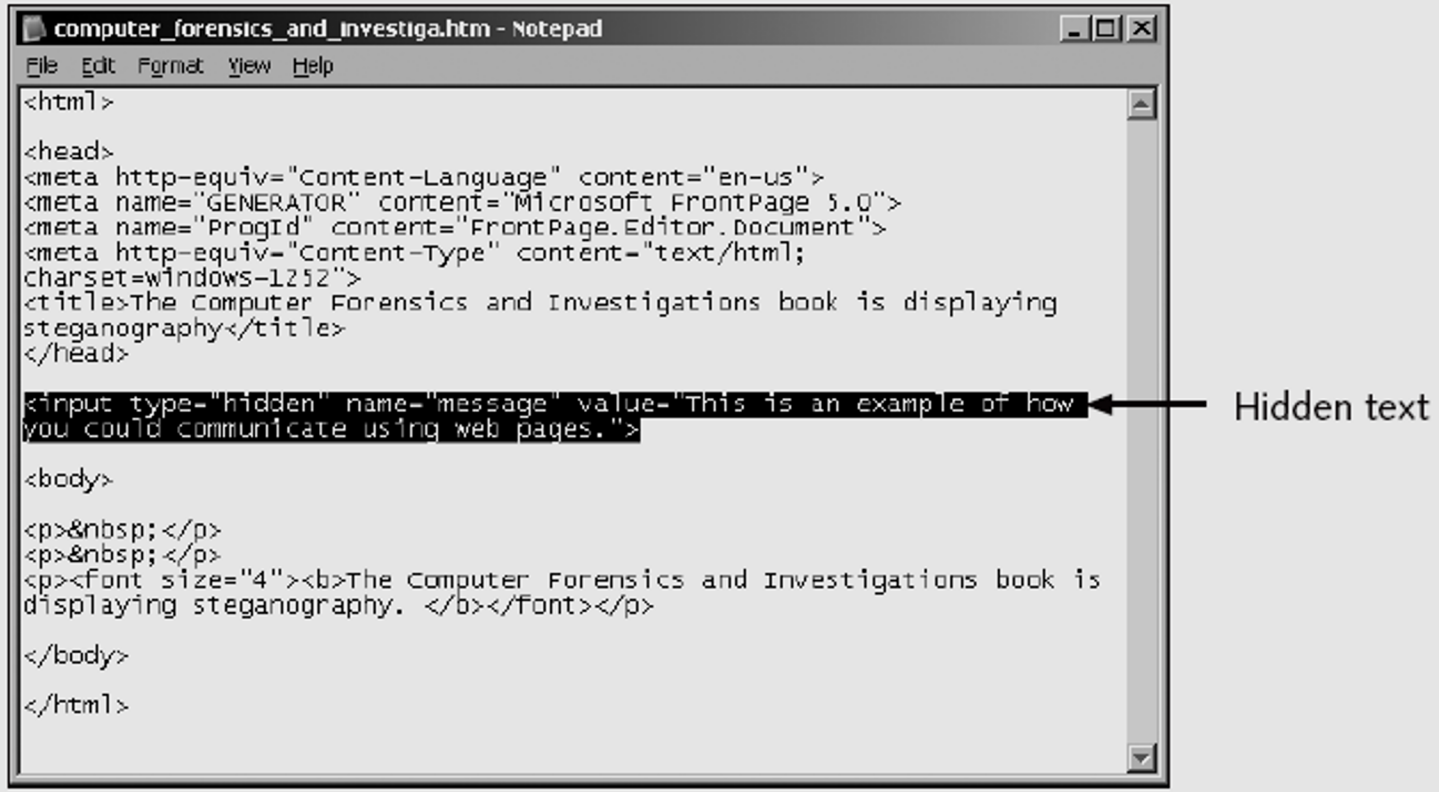


Figure 10-28 The HTML code reveals hidden text

Understanding Steganography in Graphics Files (continued)

- Substitution
  - Replaces bits of the host file with bits of data
  - Usually change the last two LSBs
  - Detected with **steganalysis tools**
- Usually used with image files
  - Audio and video options
- Hard to detect

Understanding Steganography in Graphics Files (continued)

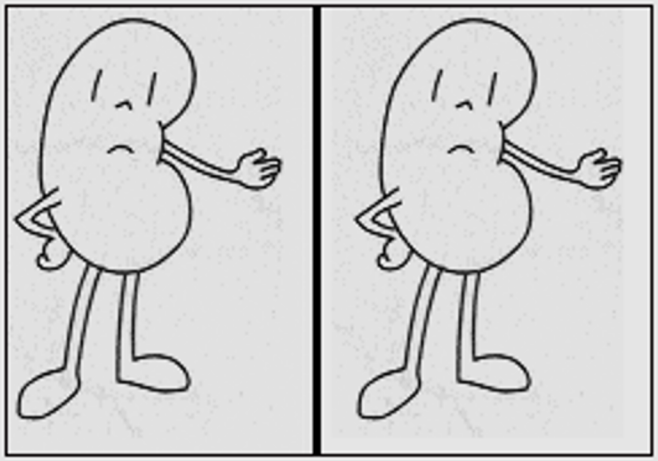


Figure 10-29 Original and altered images

Understanding Steganography in Graphics Files (continued)

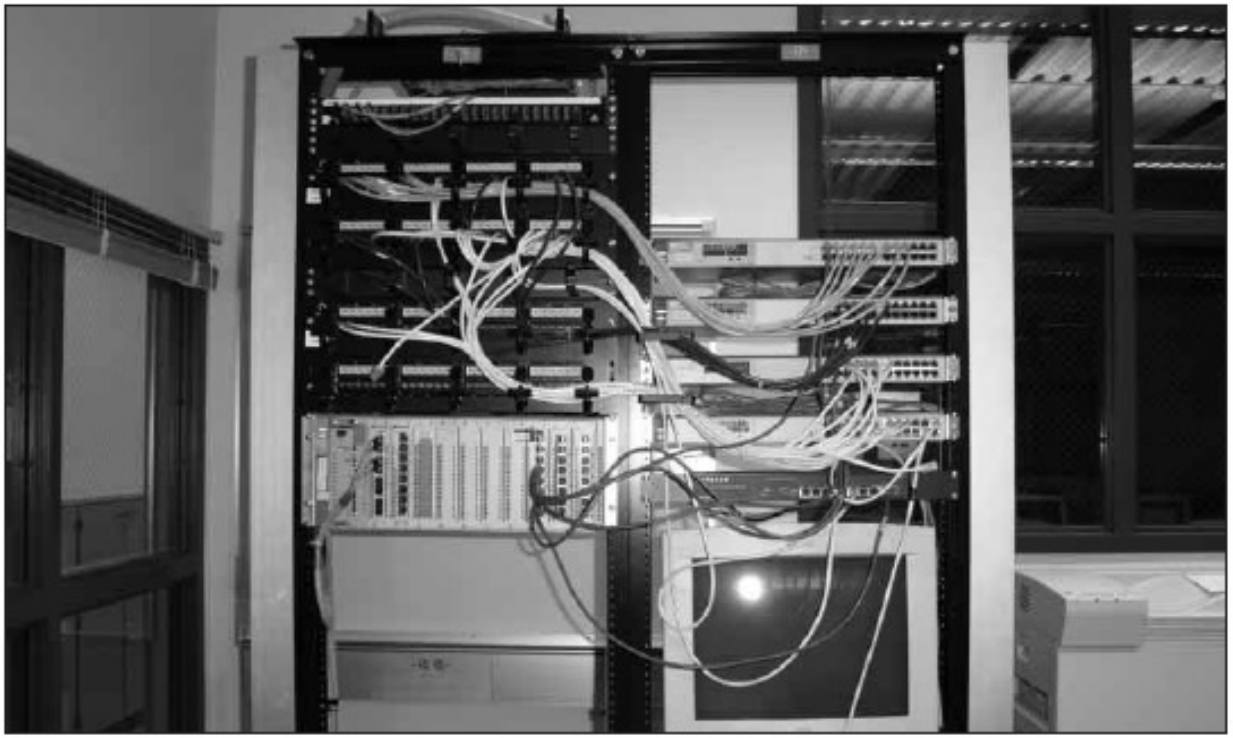


Figure 10-30 Hidden picture in the altered image

Using Steganalysis Tools

- Detect variations of the graphic image
  - When applied correctly you cannot detect hidden data in most cases
- Methods
  - Compare suspect file to good or bad image versions
  - Mathematical calculations verify size and palette color
  - Compare hash values

Identifying Copyright Issues with Graphics

- Steganography originally incorporated watermarks
- Copyright laws for Internet are not clear
  - There is no international copyright law
- Check www.copyright.gov

Summary

- Image types
  - Bitmap
  - Vector
  - Metafile
- Image quality depends on various factors
- Image formats
  - Standard
  - Nonstandard
- Digital camera photos are typically in raw and EXIF JPEG formats

Summary (continued)

- Some image formats compress their data
  - Lossless compression
  - Lossy compression
- Recovering image files
  - Carving file fragments
  - Rebuilding image headers
- Software
  - Image editors
  - Image viewers

Summary (continued)

- Steganography
  - Hides information inside image files
  - Forms
    - Insertion
    - Substitution
- Steganalysis
  - Finds whether image files hide information