

#### **Objectives:**

- Use a hex editor to manually recover a deleted file from a FAT12 image file.
- Use FTK Imager to mount images and view deleted files.
- 1. Install and/or open FTK Imager 3.01
- 2. Select File > Image Mounting...
- 3. Add the image file "Suspect\_floppy image.001", do not change the default options, and click

"Mount".

	Mount Image To Dri	ve	2
iden	Add Image		
	Image File:		
	puter Forensics	Intro\Module 3 - File Systems -\Lab 3 - FAT File Systems\Suspect_floppy image.001	
	Mount Type:	Physical & Logical	
	Drive Letter:	Next Available (E:)	
	Mount Method:	Block Device / Read Only	
	Write Cache Fold	er;	
	C:\Users\Brian\D	ocuments\GMU Course\CFRS 500 _Computer Forensics Intro\Module 3 - File System	1
		Mou	Int

4. Go to Windows Explorer and open the "E:" Drive. This is the mounted version of the suspect image. Note the files that are currently on the image.

👝 🕨 Comp	uter	Local Disk (E:)					👻 🍫 Sea							
Include in library   Share with														
tes	-	Name	Date modified	Date created	Size		Туре							
top		3 office computer table.jpg	8/15/2011 12:57 PM	9/4/2011 5:22 PM		42 KB	JPEG image							
nloads		🖳 Lab 2 - Forensic Imaging.docx	8/28/2011 11:27 PM	9/4/2011 5:21 PM		18 KB	Microsoft Office							
nt Places		🖳 Lab 1 - Hashing.docx	8/28/2011 9:53 PM	9/4/2011 5:21 PM		16 KB	Microsoft Office							
		GMU_CFRS.txt	9/3/2011 2:58 PM	9/4/2011 5:19 PM		1 KB	Text Document							

5. Open the Hex Editor "HxD".



 Select "Extras > Open Disk Image..." and open "Suspect\_floppy image - Copy.001". You are looking at Sector 0, the FAT Boot sector for the floppy image. Note that the file system "FAT12" is clearly shown.

HxD - [C:\Use	ers\Bi	rian\	Doci	ımer	nts\G	IMU	Coui	rse\C	FRS	500 _	Con	npute	er Fo	rensi	ics In	tro\N	Nodule 3 - File Systems -\	Lab 3 -	FAT File S	yst
File Edit	Searc	h V	iew	Ana	lysis	Ext	ras	Win	dow	?										
🗋 🙆 • 🗐	Tun	J	++	16		-	AN	SI			de	c	•		4	4 1	Sector	0 🔹	of 2880	
Suspect_flo	ppy i	mag	e - C	opy.	001															
Offset(d)	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15				
00000000	EB	3C	90	4D	53	44	4F	53	35	2E	30	00	02	01	01	00	ë<.MSDOS5.0		Sector	0
00000016	02	EO	00	40	0B	FO	09	00	12	00	02	00	00	00	00	00	.à.@.ð			
00000032	00	00	00	00	00	00	29	6E	EA	75	AO	4E	4F	20	4E	41	)nêu NO N	A		
00000048	4D	45	20	20	20	20	46	41	54	31	32	20	20	20	33	C9	ME FAT12 3	É		
00000064	8E	D1	BC	FO	7B	8E	D9	B8	00	20	8E	CO	FC	BD	00	7C	ŽÑ4ð{ŽÙ,.ŽÀü4.	1		
00000080	38	4E	24	7D	24	8B	C1	99	E8	3C	01	72	10	83	EB	ЗA	8N\$}\$<Á™è<.r.fë	:		
00000096	66	A1	10	7C	26	66	3B	07	26	8A	57	FC	75	06	80	CA	f;. &f.&ŠWüu.€	Ê		
00000112	02	88	56	02	80	C3	10	73	EB	33	C9	8A	46	10	98	F7	.^V.€Ã.së3ÉŠF.~	-		
00000128	66	16	03	46	10	13	56	1E	03	46	OE	13	D1	8B	76	11	fFVFÑ <v< td=""><td></td><td></td><td></td></v<>			
00000144	60	89	46	FC	89	56	FE	B8	20	00	F7	E6	8B	5E	0B	03	`‰Fü‰Vþ, .÷æ∢^.			
00000160	C3	48	F7	F3	01	46	FC	11	4E	FE	61	BF	00	00	E8	E6	ĂH÷ó.Fü.Nþa¿è	£		
00000176	00	72	39	26	38	2D	74	17	60	B1	0B	BE	A1	7D	F3	A6	.r9&8-t.`±.¾;}ó	1		
00000192	61	74	32	4E	74	09	83	C7	20	38	FB	72	E6	EB	DC	AO	at2Nt.fC :ûræëÜ	942		

- 7. Select "View > Offset Base" and change it to **Decimal**.
- 8. Go to Sector 19. This is the beginning of the File Allocation Table (FAT). It stores file metadata, such as size, created time, modified time and file name abd file's physical location on the drive.
- 9. Partially into sector 20, you will see a file that starts with the hex E5 sigma character. This indicates a deleted file. In a FAT file system, the first character of a deleted file is replaced with hex E5 (sigma) and the location of the file is set to zero, thus marking as it available.



Suspect_floppy image	e - Copy.001		
Offset(d) 00 01	02 03 04 05 06 07	08 09 10 11 12 13 14 15	
00010224 FF FF	FF FF FF FF FF FF	FF FF 00 00 FF FF FF FF	999999999999999
00010240 02 73	00 69 00 63 00 20	00 49 00 OF 00 F8 6D 00	.s.i.cIøm. Sector 20
00010256 61 00	67 00 69 00 6E 00	67 00 00 00 2E 00 64 00	a.g.i.n.gd.
00010272 01 4C	00 61 00 62 00 20	00 32 00 OF 00 F8 20 00	.L.a.b2ø .
00010288 2D 00	20 00 46 00 6F 00	72 00 00 00 65 00 6E 00	F.o.re.n.
00010304 4C 41	42 32 2D 46 7E 31	44 4F 43 20 00 B7 AB 8A	LAB2-F~1DOC . «Š
00010320 24 3F	24 3F 00 00 65 BB	1C 3F 23 00 DD 46 00 00	\$?\$?e».?#.ÝF
00010336 43 67	00 00 00 FF FF FF	FF FF FF OF 00 92 FF FF	Cgÿÿÿÿÿÿ'ÿÿ
00010352 FF FF	FF FF FF FF FF FF	FF FF 00 00 FF FF FF FF	<u> </u>
00010368 02 75	00 74 00 65 00 72	00 20 00 OF 00 92 74 00	.u.t.e.r't.
00010384 61 00	62 00 6C 00 65 00	2E 00 00 00 6A 00 70 00	a.b.l.ej.p.
00010400 01 33	00 20 00 6F 00 66	00 66 00 OF 00 92 69 00	.3o.f.f'i.
00010416 63 00	65 00 20 00 63 00	6F 00 00 00 6D 00 70 00	c.ec.om.p.
00010432 33 4F	46 46 49 43 7E 31	4A 50 47 20 00 52 D9 8A	30FFIC~1JPG .RÙŠ
00010448 24 3F	24 3F 00 00 21 67	OF 3F 47 00 5C A6 00 00	\$?\$?!g.?G.\¦
00010464 E5 4F	4D 42 20 20 20 20	54 58 54 20 18 99 69 8B	åOMB TXT .™i<
00010480 24 3F	24 3F 00 00 65 8B	24 3F 9B 00 71 03 00 00	\$?\$?e<\$?>.q
00010496 00 00	00 00 00 00 00 00	00 00 00 00 00 00 00 00	
00010512 00 00	00 00 00 00 00 00	00 00 00 00 00 00 00 00	

10. Select the E5 character and replace it with a "B".

Suspect_flo																	
Offset(d)	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	
00010432	33	4F	46	46	49	43	7E	31	4A	50	47	20	00	52	D9	8A	30FFIC~1JPG .RÙŠ
00010448	24	ЗF	24	ЗF	00	00	21	67	OF	ЗF	47	00	5C	Α6	00	00	\$?\$?!g.?G.\¦
00010464	42	4F	4D	42	20	20	20	20	54	58	54	20	18	99	69	8B	BOMB TXT .™i<
00010480	24	ЗF	24	ЗF	00	00	65	8B	24	ЗF	9B	00	71	03	00	00	\$?\$?e<\$?>.q
00010496	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00010512	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	

- 11. Select "File > Save As" and save this file with the name "Recovered\_floppy image.001".
- 12. Return to FTK Imager, use the Mounting utility to mount the "Recovered\_floppy image.001" the same as you mounted the original image



dd Image									
Image File:									
ensics Intro Mod	lule 3 - File Systems - Lab	3 - FAT File Syster	ms\Recovered_floppy image - Copy.001	L					
Mount Type:	Mount Type: Physical & Logical								
Drive Latter									
Drive Letter:	Next Available (G:)		<b>•</b>						
Mount Method:	Block Device / Read Only	1	•						
man code cal	al anno								
Write Cache Fol	der:			_					
Write Cache Fol C:\Users\Brian\	der: Documents\GMU Course\C	FRS 500 _Comput	er Forensics Intro\Module 3 - File System	m					
Write Cache Fol C:\Users\Brian\	der: Documents\GMU Course\C	FRS 500 _Comput	er Forensics Intro\Module 3 - File Syste	m					
Write Cache Fol C:\Users\Brian\	der: Documents\GMU Course\C	FRS 500 _Comput	ter Forensics Intro\Module 3 - File Syste	m					
Write Cache Fol C:\Users\Brian\	der: Documents\GMU Course\C	FRS 500 _Comput	ter Forensics Intro (Module 3 - File Syster	m					
Write Cache Fol C:\Users\Brian\ Apped Image Lis	der: Documents\GMU Course\C	FRS 500 _Comput	ter Forensics Intro (Module 3 - File Syste	m punt					
Write Cache Fol C:\Users\Brian\ Iapped Image Lis	der: Documents\GMU Course\C t	CFRS 500 _Comput	ter Forensics Intro (Module 3 - File Syste	m					
Write Cache Fol C:\Users\Brian\ happed Image Lis Mapped Images:	der: Documents\GMU Course\C t	FRS 500 _Comput	ter Forensics Intro (Module 3 - File Syste	m ount					
Write Cache Fol C:\Users\Brian\ Mapped Image Lis Mapped Images: Drive	der: Documents\GMU Course\C t Method	Partition	ter Forensics Intro (Module 3 - File Syster	m					
Write Cache Fol C:\Users\Brian\ Napped Image Lis Mapped Images: Drive PhysicalDrive2	der: Documents\GMU Course\C t Method Block Device/Read	Partition	ter Forensics Intro (Module 3 - File Syster Mo Image C: (Users \Brian \Documents \GMU	m ount					
Write Cache Fol C:\Users\Brian\ Mapped Image Lis Mapped Images: Drive PhysicalDrive2 F:	der: Documents\GMU Course\C t Method Block Device/Read Block Device/Read	Partition Image σ [FAT12]	ter Forensics Intro (Module 3 - File Syste Mo Image C: (Users\Brian\Documents\GMU C: (Users\Brian\Documents\GMU	m ount Course Course					
Write Cache Fol C:\Users\Brian\ Apped Image Lis Mapped Images: Drive PhysicalDrive2 F: PhysicalDrive1	der: Documents\GMU Course\C t Method Block Device/Read Block Device/Read Block Device/Read	Partition Image o [FAT12] Image	Er Forensics Intro (Module 3 - File System Mo Image C: (Users \Brian \Documents \GMU C: (Users \Brian \Documents \GMU C: (Users \Brian \Documents \GMU	m ount Course Course Course					

13. Open the F: drive in Windows Explorer. Note the files that are now on the image.

\*\*NOTE: The new file "bomb.txt" is now visible with all of its metadata. However, the physical location of the file is still zeroed in the FAT table. So we will not be able to actually open this file.\*\*

er 🕨 Local Disk (F:)			<b>- €</b> 9	Search Local Disk									
library  Share with													
Name	Date created	Date modified	Size	Туре									
🔄 3 office computer table.jpg	9/4/2011 5:22 PM	8/15/2011 12:57 PM	42 KB	JPEG image									
bomb.txt	9/4/2011 5:27 PM	9/4/2011 5:27 PM	1 KB	Text Document									
GMU_CFRS.txt	9/4/2011 5:19 PM	9/3/2011 2:58 PM	1 KB	Text Document									
🗐 Lab 1 - Hashing.docx	9/4/2011 5:21 PM	8/28/2011 9:53 PM	16 KB	Microsoft Office									
藰 Lab 2 - Forensic Imaging.docx	9/4/2011 5:21 PM	8/28/2011 11:27 PM	18 KB	Microsoft Office									

- 14. Return to FTK Imager and close the image mounting utility.
- 15. Select "File>Add Evidence Item".
- 16. Select "Image File" and browse to the "Recovered\_floppy image.001" file and click finish.
- 17. FTK imager automatically recovers the deleted file's location and displays it. Look in the root folder for the image contents.



Q AccessData FTK Imager 3.0.1.1467																		
File View Mode Help																		
Fig. Ten Hone Heb				62 I	_			_				-		~				
		P .			Ø		61			5	® <u>⊺</u>	EXT	iέΧ	X	+			
Evidence Tree ×	File Li	st																
E Brecovered_floppy image - Copy.001	Nam	e							Size Type								te Modified	
🖻 [τ σ [FAT12]	3 office computer tabl								42 KB Regular File								5/2011 12:5	
[root]	bomb.txt									1 KE	8 R	egu		9/4	/2011 5:27:1			
	G	UU_	CFR	S.TX	Т					1 KE	B R	egu	lar F	ile		9/3/2011 2:58:0		
	🖳 La	b1-	Ha	shin	g.d	DCX			1	6 KE	B R	egu	lar F	ile		8/2	8/2011 9:53:	
	🖳 La	b 2 -	Fo	rens	ic In	nagi			1	8 KE	8 R	egu	lar F	ile		8/28/2011 11:2		
	000	54	68	65	20	62	6F	6D	62-20	69	73	20	6C	6F	63	61	The bomb is loca	
	010	74	65	64	20	69	6E	20	74-68	65	20	74	72	61	73	68	ted in the trash	
	020	20	63	61	6E	20	6F	6E	20-35	74	68	20	61	6E	64	20	can on 5th and	
	030	4D	61	64	69	73	6F	6E	20-73	74	72	65	65	74	2E	20	Madison street.	
	040	20	OD	AO	49	74	20	77	69-6C	6C	20	65	78	70	6C	6F	··It will explo	
	050	64	05	20	01	14 6F	20	60	61-74	03	74	64	61	20	OL 2F	10	de at exactly no	
Custom Content Sources ×	070	AO	54	68	69	73	20	69	73-20	61	6E	20	65	76	65	6E	This is an even	
Evidence:File System Dath File	080	74	20	74	68	61	74	20	77-69	6C	6C	20	75	6E	69	74	t that will unit	
Evidences ne bystem i dan ne	090	65	20	61	6C	6C	20	70	6F-6C	69	74	69	63	61	6C	20	e all political	
	0a0	64	69	73	73	61	73	64	65-6E	74	73	21	20	OD	AO	53	dissasdents!S	
	0b0	6E	63	65	72	65	6C	79	2C-20	OD	AO	4A	69	6D	20	53	ncerely,Jim S	
	0c0	6D	69	74	68	OD	AO	6A	73-6D	69	74	68	40	62	6F	6D	mith · · jsmith@bom	
	0b0	62	65	72	6D	61	69	6C	26-63	6F	6D	20	20	20	20	20	bermail.com	
	0E0	20	20	20	20	20	20	20	20-20	20	20	20	20	20	20	20		