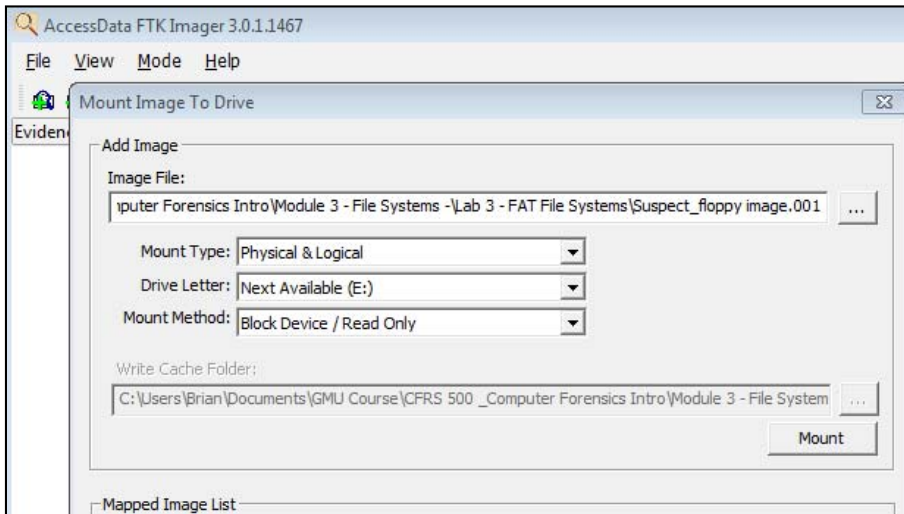
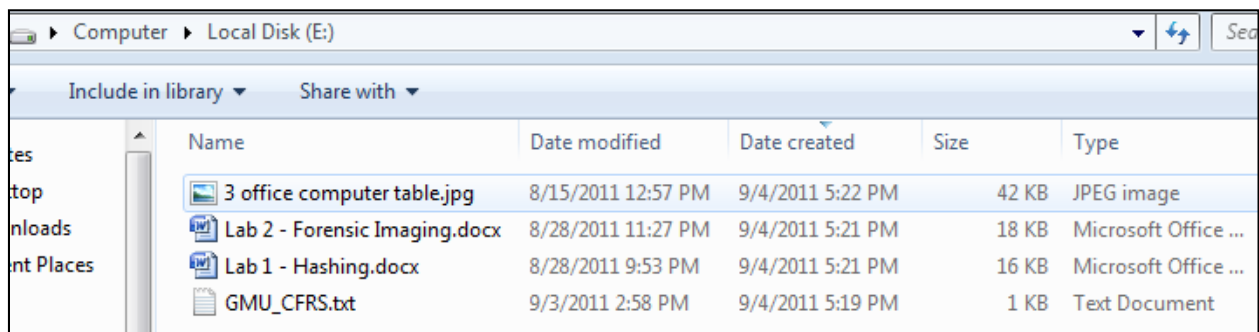


Objectives:

- 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”.

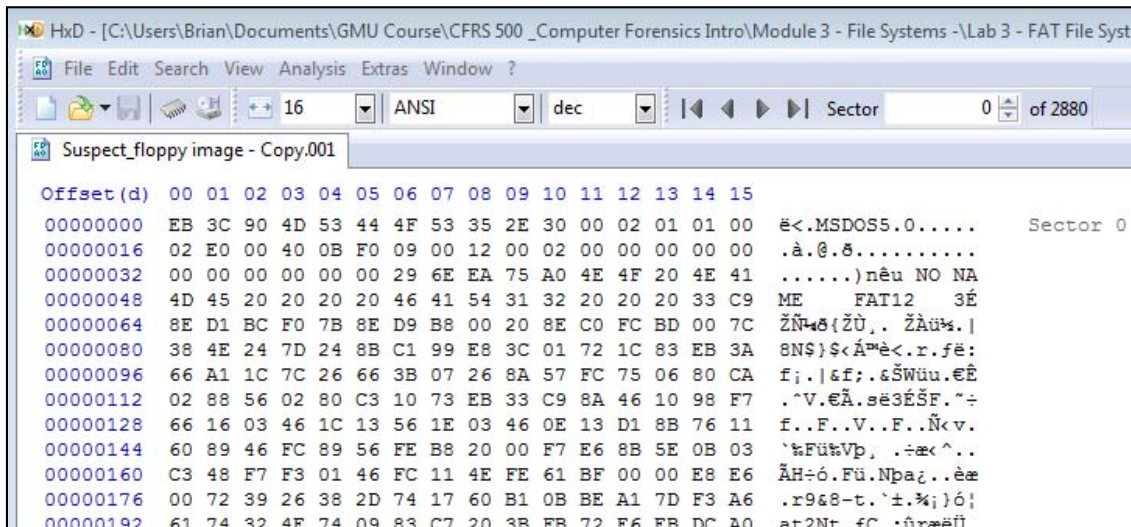


4. Go to Windows Explorer and open the “E:” Drive. This is the mounted version of the suspect image. Note the files that are currently on the image.



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.



- Select “View > Offset Base” and change it to **Decimal**.
- 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 and file’s physical location on the drive.
- 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 - 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  YYYYYYYYYY..YY
00010240 02 73 00 69 00 63 00 20 00 49 00 0F 00 F8 6D 00   Sector 20
00010256 61 00 67 00 69 00 6E 00 67 00 00 00 2E 00 64 00
00010272 01 4C 00 61 00 62 00 20 00 32 00 0F 00 F8 20 00
00010288 2D 00 20 00 46 00 6F 00 72 00 00 00 65 00 6E 00
00010304 4C 41 42 32 2D 46 7E 31 44 4F 43 20 00 B7 AB 8A
00010320 24 3F 24 3F 00 00 65 BB 1C 3F 23 00 DD 46 00 00
00010336 43 67 00 00 00 FF FF FF FF FF FF 0F 00 92 FF FF
00010352 FF FF FF FF FF FF FF FF FF FF 00 00 FF FF FF
00010368 02 75 00 74 00 65 00 72 00 20 00 0F 00 92 74 00
00010384 61 00 62 00 6C 00 65 00 2E 00 00 00 6A 00 70 00
00010400 01 33 00 20 00 6F 00 66 00 66 00 0F 00 92 69 00
00010416 63 00 65 00 20 00 63 00 6F 00 00 00 6D 00 70 00
00010432 33 4F 46 46 49 43 7E 31 4A 50 47 20 00 52 D9 8A
00010448 24 3F 24 3F 00 00 21 67 0F 3F 47 00 5C A6 00 00
00010464 E5 4F 4D 42 20 20 20 20 54 58 54 20 18 99 69 8B
00010480 24 3F 24 3F 00 00 65 8B 24 3F 9B 00 71 03 00 00
00010496 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
  
```

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

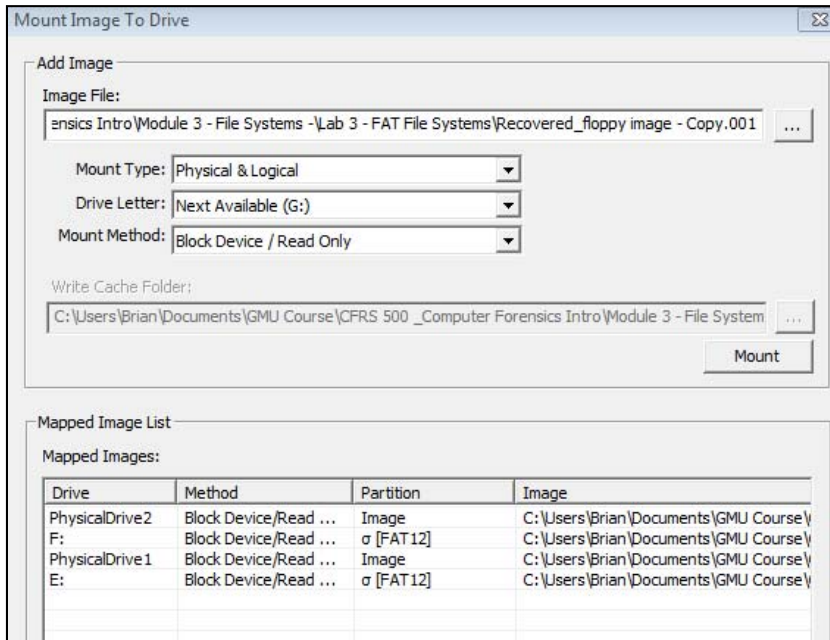
```

Suspect_floppy image - Copy.001

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  3OFFIC~1JPG .RÙŠ
00010448 24 3F 24 3F 00 00 21 67 0F 3F 47 00 5C A6 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 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
  
```

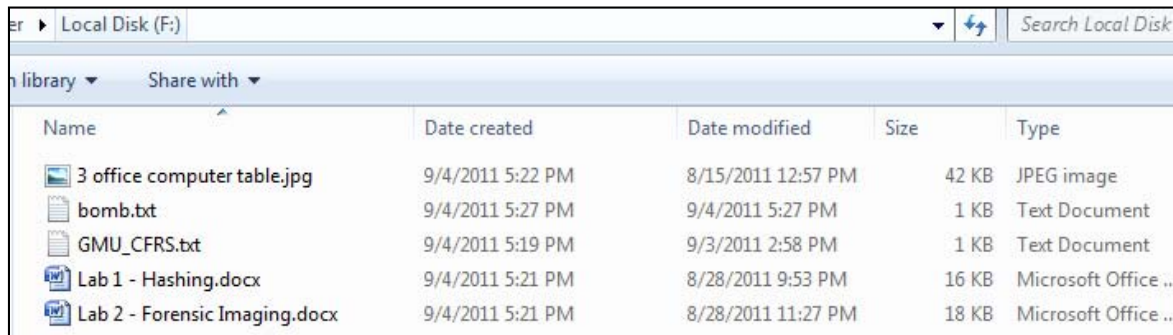
11. Select “File > Save As” and save this file with the name “Recovered_floppy image.001”.

12. Return to FTK Imager, use the Mounting utility to mount the “Recovered_floppy image.001” the same as you mounted the original image



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.**

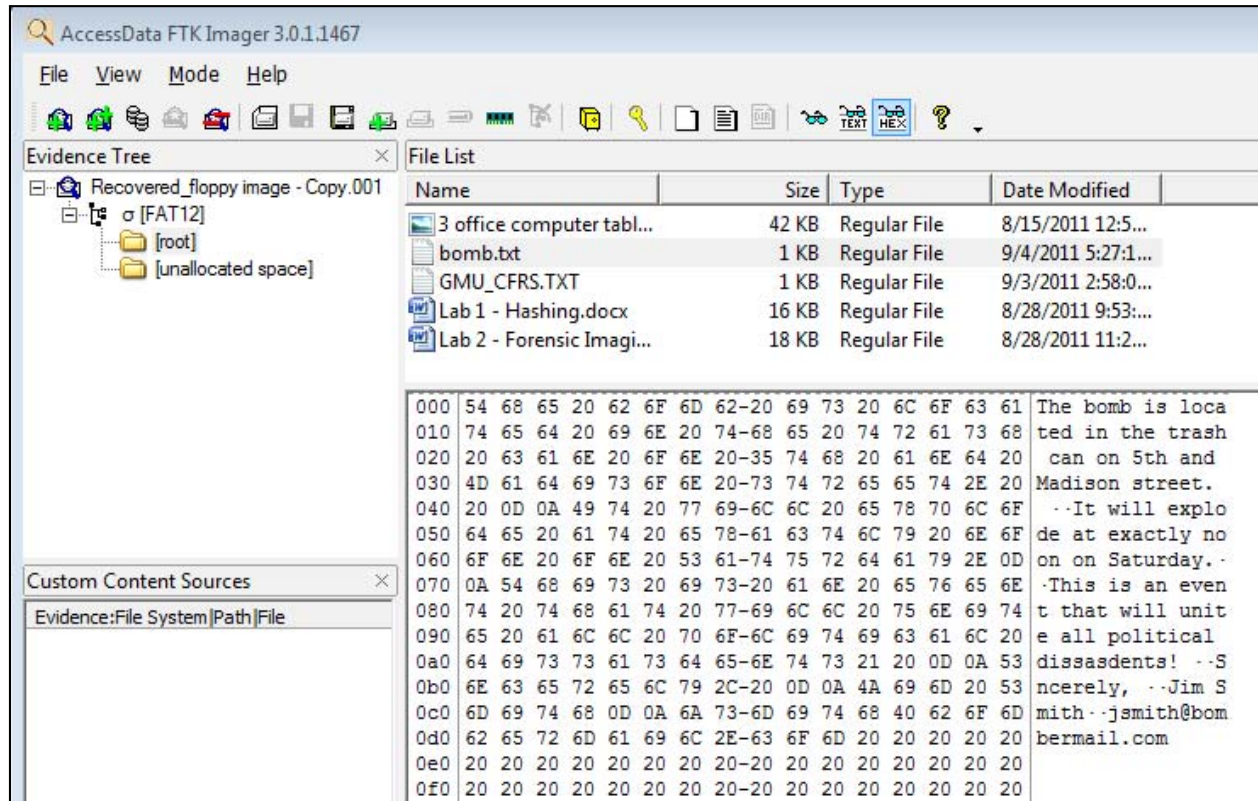


14. Return to FTK Imager and close the image mounting utility.

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.



The screenshot shows the AccessData FTK Imager interface. The 'Evidence Tree' on the left shows a recovered floppy image with a FAT12 file system containing a 'root' folder and '[unallocated space]'. The 'File List' pane shows several files, including 'bomb.txt' (1 KB, Regular File, modified 9/4/2011 5:27:1...). The bottom pane displays hex data for 'bomb.txt', which contains a message about a bomb location and a signature from Jim Smith.

Name	Size	Type	Date Modified
3 office computer tabl...	42 KB	Regular File	8/15/2011 12:5...
bomb.txt	1 KB	Regular File	9/4/2011 5:27:1...
GMU_CFRS.TXT	1 KB	Regular File	9/3/2011 2:58:0...
Lab 1 - Hashing.docx	16 KB	Regular File	8/28/2011 9:53:...
Lab 2 - Forensic Imagi...	18 KB	Regular File	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	0D	0A	49	74	20	77	69-6C	6C	20	65	78	70	6C	6F	--It will explo	
050	64	65	20	61	74	20	65	78-61	63	74	6C	79	20	6E	6F	de at exactly no	
060	6F	6E	20	6F	6E	20	53	61-74	75	72	64	61	79	2E	0D	on on Saturday.	
070	0A	54	68	69	73	20	69	73-20	61	6E	20	65	76	65	6E	.This is an even	
080	74	20	74	68	61	74	20	77-69	6C	6C	20	75	6E	69	74	t that will unit	
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	0D	0A	53	dissasidents! --S	
0b0	6E	63	65	72	65	6C	79	2C-20	0D	0A	4A	69	6D	20	53	ncerely, --Jim S	
0c0	6D	69	74	68	0D	0A	6A	73-6D	69	74	68	40	62	6F	6D	mith--jsmith@bom	
0d0	62	65	72	6D	61	69	6C	2E-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	20	
0f0	20	20	20	20	20	20	20	20-20	20	20	20	20	20	20	20	20	