

**Davis Fulton**  
**100228199**  
**INFO 4120: Digital Forensics**  
**S50**  
**Assignment**  
**11/20/20**

The first thing I did was to copy the tar file from /dharris/ to /stud402/. I did this by typing `cp /home/talia/dharris/sleuthkit-4.2.0.tar /home/stud402/`. To check if it worked I typed the `ls` command.

```
stud402@centos-s-4vcpu-8gb-tor1-01:~  
[stud402@centos-s-4vcpu-8gb-tor1-01 ~]$ cp /home/talia/dharris/sleuthkit-4.2.0.tar /home/stud402/  
[stud402@centos-s-4vcpu-8gb-tor1-01 ~]$ ls  
public_html  sleuthkit-4.2.0.tar
```

I then used *Filezilla* to transfer the 6-undel-fat folder from my desktop to my UNIX account. I did another `ls` to check if it worked. Next, I `cd`'ed into the 6-undel-fat folder and did a `md5sum` and `sha1sum` check of the 6-fat-undel.dd file. I then cross-referenced the md5 and sha1 sums to the website and saw that they matched. This means that the file has integrity. If the output of the md5 or sha1 was different then something has been changed; even if a single bit were to have been changed, the outputted string would be completely different.

MD5 of the image is 4aeb06ecd361777242ab78735d51ace6.

```
4aeb06ecd361777242ab78735d51ace6 6-fat-undel.dd
```

```
stud402@centos-s-4vcpu-8gb-tor1-01:~/6-undel-fat  
[stud402@centos-s-4vcpu-8gb-tor1-01 ~]$ ls  
6-undel-fat  index.html  public_html  sleuthkit-4.2.0  sleuthkit-4.2.0.tar  
[stud402@centos-s-4vcpu-8gb-tor1-01 ~]$ cd 6-undel-fat/  
[stud402@centos-s-4vcpu-8gb-tor1-01 6-undel-fat]$ ls  
6-fat-undel.dd  COPYING-GNU.txt  index.html  README.txt  results.txt  
[stud402@centos-s-4vcpu-8gb-tor1-01 6-undel-fat]$ md5sum 6-fat-undel.dd  
4aeb06ecd361777242ab78735d51ace6 6-fat-undel.dd  
[stud402@centos-s-4vcpu-8gb-tor1-01 6-undel-fat]$ sha1sum 6-fat-undel.dd  
bb7d22f68c3c3f03a17d0772854be4d58c7702ee 6-fat-undel.dd  
[stud402@centos-s-4vcpu-8gb-tor1-01 6-undel-fat]$
```

With both the sleuthkit, and files I needed. I was now ready to begin analyzing the 6-fat-undel.dd file for any forensics evidence

## fls command

The first command I did was *fls -r -i raw -f fat /home/stud402/6-undel-fat/6-fat-undel.dd* . This command shows all the deleted files and what sectors they are on the floppy. We see 6 files and 2 directories. In sector 3 we have the File allocation table located, and at sector 4 we see *\_rag1.dat*. The underscore is a deleted file marker.

```
stud402@centos-s-4vcpu-8gb-tor1-01:~/6-undel-fat
[stud402@centos-s-4vcpu-8gb-tor1-01 6-undel-fat]$ fls -r -i raw -f fat /home/stud402/6-undel-fat/6-fat-undel.dd
r/r 3:  FAT REC 1  (Volume Label Entry)
r/r * 4:      _rag1.dat
r/r * 5:      _rag2.dat
r/r * 6:      _ing.dat
r/r * 7:      _ult1.dat
d/d * 8:      _irl
+ d/d * 869:   dir2
++ r/r * 965:  frag3.dat
+ r/r * 870:   mult2.dat
d/d * 11:     System Volume Information
+ d/d * 905:   _restore{A25F48CA-6632-4143-8EF8-3586A84AB5AF}
++ d/d * 933:  _P1
+++ r/r * 965: _frag3.dat
v/v 191619:   $MBR
v/v 191620:   $FAT1
v/v 191621:   $FAT2
V/V 191622:   $OrphanFiles
[stud402@centos-s-4vcpu-8gb-tor1-01 6-undel-fat]$
```

If we only wanted to see the deleted files we can type *fls -d -i raw -f fat /home/stud402/6-undel-fat/6-fat-undel.dd* .

```
stud402@centos-s-4vcpu-8gb-tor1-01:~/6-undel-fat
[stud402@centos-s-4vcpu-8gb-tor1-01 6-undel-fat]$ fls -d -i raw -f fat /home/stud402/6-undel-fat/6-fat-undel.dd
r/r * 4:      _rag1.dat
r/r * 5:      _rag2.dat
r/r * 6:      _ing.dat
r/r * 7:      _ult1.dat
d/d * 8:      _irl
d/d * 11:     System Volume Information
[stud402@centos-s-4vcpu-8gb-tor1-01 6-undel-fat]$
```

## fsstat command

The next command I used was *fsstat -f fat -i raw /home/stud402/6-undel-fat/6-fat-undel.dd* . This will give file system information. From this information, we can see that it's an MSDOS5 disk. The volume label has no name. The file system type is FAT 16. There are 12032 sectors on this disk. Sector 0-7 is reserved for system information. Our first FAT is from sectors 8 - 31 and the second FAT is from 32 - 55. Starting at

sector 56 we have the Data Area. The root directory is from sectors 56 - 87. The cluster area or allocation units go from sector 88 - 12031. Sector 12032 is non-clustered, this can also be slack space on a disk where people can hide illegal content. The size of each sector is 512 bytes, the cluster size is 1024 bytes. Two sectors equal 1 cluster. We have a total of 5971 clusters.

```
stud402@centos-s-4vcpu-8gb-tor1-01:~/6-undel-fat
[stud402@centos-s-4vcpu-8gb-tor1-01 6-undel-fat]$ fsstat -f fat -i raw /home/stud402/6-undel-fat/6-fat-undel.dd
FILE SYSTEM INFORMATION
-----
File System Type: FAT16

OEM Name: MSDOS5.0
Volume ID: 0xc0fecdl1
Volume Label (Boot Sector): NO NAME
Volume Label (Root Directory): FAT_REC_1
File System Type Label: FAT16

Sectors before file system: 63

File System Layout (in sectors)
Total Range: 0 - 12032
Total Range in Image: 0 - 12031
* Reserved: 0 - 7
** Boot Sector: 0
* FAT 0: 8 - 31
* FAT 1: 32 - 55
* Data Area: 56 - 12032
** Root Directory: 56 - 87
** Cluster Area: 88 - 12031
** Non-clustered: 12032 - 12032

METADATA INFORMATION
-----
Range: 2 - 191622
Root Directory: 2

CONTENT INFORMATION
-----
Sector Size: 512
Cluster Size: 1024
Total Cluster Range: 2 - 5973

FAT CONTENTS (in sectors)
-----
[stud402@centos-s-4vcpu-8gb-tor1-01 6-undel-fat]$
```

### icat command

The next command was `icat -f fat -s -i raw /home/stud402/6-undel-fat/6-fat-undel.dd 6 | hexdump -C`. This command gives a hexadecimal output of the content located at any particular sector (sector 6 in this example). At 300 - E, we see the end of the data. The output is very similar to using the DOS debug command. From offset 310 - 400 it's all 0s.

stud402@centos-s-4vcpu-8gb-tor1-01:~/6-undel-fat

```
[stud402@centos-s-4vcpu-8gb-tor1-01 6-undel-fat]$ icat -f fat -s -i raw /home/stud402/6-undel-fat/6-fat-undel.dd 6 | hexdump -C
00000000 c5 c6 b7 f6 75 69 77 0b 50 a0 d4 9f 71 66 a4 6e |...uiw.P...qf.n|
00000010 cf b0 66 f4 a1 ca 1b b3 89 42 4a 3a 38 c0 5b a2 |..f.....BJ:8.[.|
00000020 1d 6a 2d d1 be 02 6b 4f 06 8f 22 ed 7f 84 e1 5f |.j-...kO.."....|
00000030 3d 58 ab 8e aa 90 38 22 c4 40 5f f0 45 e1 af 11 |=X...8".@.E...|
00000040 44 4f 47 a1 c6 a5 89 66 b5 3f 3a b0 e2 28 c0 72 |DOG...f.?...(r|
00000050 dd ca 00 75 22 04 54 8f d7 34 c6 ff 5a 43 12 11 |...u".T..4..ZC..|
00000060 db fb 59 3e 8b 58 1f 64 63 c1 86 a3 82 75 45 5b |..Y>.X.dc.....uE[|
00000070 09 58 97 2c e6 5c 66 93 5f e9 3b 75 bb f1 07 be |.X.,.\f._;u...|
00000080 06 49 96 59 6f 09 2c c7 73 ee 2d e0 76 d9 df e0 |.I.Yo.,.s.-.v...|
00000090 5e 5b 39 99 42 d9 75 c3 f1 4a 68 42 aa ec 37 cf |^[9.B.u..JhB..7.|
000000a0 b0 75 c5 f0 73 c5 5a db 39 aa 41 d6 0b 24 e2 ea |.u..s.Z.9.A..$.|
000000b0 a1 54 ca 17 a0 02 2f 31 74 74 48 dc cb ee 4e 4c |.T..../lthH...NL|
000000c0 0b 12 d9 81 79 40 de e2 df 24 2c b3 66 8e c4 16 |....y@...;f...|
000000d0 02 24 4c 2a b5 cf 82 f2 7c 2c 90 9d 01 50 43 6d |.L*....|,...PCm|
000000e0 47 4b 45 c9 a5 2d 16 fc 36 88 60 b8 6e b0 62 1e |GKE...6.`.n.b.|
000000f0 02 7c f0 8e 13 ec 04 b7 72 f9 18 89 48 77 f3 b1 |.|.....r...Hw...|
00000100 44 7d 20 bc 75 11 2c fd bb 93 40 2a ad d0 48 16 |D) .u.,...@*.H.|
00000110 2a 9c 6d 0f 04 09 70 13 84 3f e2 50 b5 07 96 4f |*.m...p..?P...O|
00000120 85 89 80 f5 67 a6 65 ec 29 07 c5 c4 9f 08 c0 aa |....'.e.).....|
00000130 f7 c0 50 de 3d 5a fc 23 a7 b5 0f 7b c8 aa fe 22 |..P.=Z.#...{..."|
00000140 fb d6 75 7f 16 97 78 6f d4 a2 d9 9d 60 f0 bc b7 |..u...xo....'...|
00000150 a2 29 05 1b ab 67 12 ea ba b6 0b a0 03 1e 4f 45 |.)...g.....OE|
00000160 57 6a 1d b0 a6 c5 a6 f8 f0 f0 6e e5 d2 5a 28 20 |Wj.....n..Z(|
00000170 d0 98 e9 1c 07 64 39 08 97 38 93 3d 33 fb 33 14 |....d9..8.=3.3.|
00000180 dc 3a 61 43 cf 2e 2f 2e c3 a0 30 3f 70 ed cf 2f |.:aC.../...0?p../|
00000190 b6 c9 eb 43 c4 06 96 a8 ee 42 d8 39 a1 8a 3a d7 |...C.....B.9...|
000001a0 3d 19 33 9d 21 2a 34 b1 46 f1 f1 2f 29 68 8d 1a |=.3.!*4.F..)/h..|
000001b0 12 a9 39 3f 7a f8 b0 d6 07 82 71 b9 5c 9b 2e 2a |..9?z.....q.\.*|
000001c0 78 b5 df 89 da 75 06 73 7d a2 61 ad 2a 00 bd a3 |x....u.s).a.*...|
000001d0 20 03 03 f7 29 51 6f 07 48 c6 9b b8 4e e2 64 96 |. ...)Qo.H...N.d.|
000001e0 c5 6d ff 8a 25 af bb d3 a9 4a 99 80 a8 85 7c 02 |.m..%....J....|
000001f0 f4 9b 7d de f0 58 e0 36 95 a5 fb 7b 2a 0a ac a3 |..).X.6...{*...|
00000200 a3 16 95 55 97 4d 18 65 9a 61 29 4d c4 54 26 54 |...U.M.e.a)M.T&T|
00000210 1b 21 37 b4 3e 87 2b bd 6a 20 f2 c8 31 f9 05 65 |.!7.>.+j ...l..e|
00000220 24 06 ad 13 12 15 80 f0 4e b9 09 76 8d a3 d7 8e |$......N..v....|
00000230 80 61 c4 ad 93 66 e5 d8 24 22 a6 ef c3 32 35 e3 |.a...f..$"...25.|
00000240 bb d5 de 39 53 bb a4 46 34 e3 1c 13 2c 0e a4 52 |...9S..F4.....R|
00000250 12 e5 1b 1d ee 0b 30 9f a3 45 3e e4 e0 88 17 71 |.....0..E>...q|
00000260 0f fd d9 62 b2 c9 39 5e 6b a8 89 74 88 ee 9f 5d |...b..9*k..t...|
00000270 34 8f fe c2 c9 cc ee 2a ae 9e f6 d7 99 bc 47 86 |4.....*.....G..|
00000280 7b 51 a6 9e 12 12 e5 eb e0 80 e7 5c 72 ee 59 48 |{Q.....\r.YH|
00000290 df 62 2b ba da d5 07 a4 43 7c d2 49 c7 8f 42 01 |.b+.....C|.I..B.|
000002a0 a5 44 bd 7d a2 b9 2b d9 06 c7 91 4d 54 36 d7 53 |.D.)...+...MT6.S|
000002b0 00 b4 70 77 f2 54 18 39 ce d5 37 f9 bf 3e 7c 18 |..pw.T.9..7..>|.|
000002c0 3b 6b f1 64 76 93 cc 6c b2 f5 39 43 b8 b7 77 25 |;k.dv..l..9C..w%|
000002d0 87 a0 33 9b de 07 72 04 36 75 d8 4a 81 47 f3 fa |..3...r.6u.J.G..|
000002e0 09 df 93 8c 88 43 78 97 ff 92 6a fd 3b 19 ee 5f |.....Cx...j..|
000002f0 a8 d1 23 f4 99 f8 45 b9 49 b2 20 9f 4b 10 70 05 |..#...E.I..K.p.|
00000300 af 4f f3 1e 6c 24 90 a3 49 7c 3d bb 00 00 00 00 |.O..l$...I|=.....|
00000310 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ||.....|
*
00000400
[stud402@centos-s-4vcpu-8gb-tor1-01 6-undel-fat]$
```

## ifind command

The next command is `ifind -f fat -n _rag1.dat /home/stud402/6-undel-fat/6-fat-undel.dd`. This command is used to find metadata that is used to allocate a given disk unit. Ifind makes it easy to find entries associated with a disk. *Ifind* is also used to cross-reference the information we found using the *fls* command prior. We can replace the `_rag1.dat` with the files from the *fls* command.

```
stud402@centos-s-4vcpu-8gb-tor1-01:~/6-undel-fat
[stud402@centos-s-4vcpu-8gb-tor1-01 6-undel-fat]$ ifind -f fat -n _rag1.dat /home/stud402/6-undel-fat/6-fat-undel.dd
4
[stud402@centos-s-4vcpu-8gb-tor1-01 6-undel-fat]$ ifind -f fat -n _rag2.dat /home/stud402/6-undel-fat/6-fat-undel.dd
5
[stud402@centos-s-4vcpu-8gb-tor1-01 6-undel-fat]$ ifind -f fat -n _ing.dat /home/stud402/6-undel-fat/6-fat-undel.dd
6
[stud402@centos-s-4vcpu-8gb-tor1-01 6-undel-fat]$ ifind -f fat -n _ult1.dat /home/stud402/6-undel-fat/6-fat-undel.dd
7
[stud402@centos-s-4vcpu-8gb-tor1-01 6-undel-fat]$ ifind -f fat -n _irl /home/stud402/6-undel-fat/6-fat-undel.dd
8
[stud402@centos-s-4vcpu-8gb-tor1-01 6-undel-fat]$
```

```
stud402@centos-s-4vcpu-8gb-tor1-01:~/6-undel-fat
[stud402@centos-s-4vcpu-8gb-tor1-01 6-undel-fat]$ fls -d -i raw -f fat /home/stud402/6-undel-fat/6-fat-undel.dd
r/r * 4:      _rag1.dat
r/r * 5:      _rag2.dat
r/r * 6:      _ing.dat
r/r * 7:      _ult1.dat
d/d * 8:      _irl
d/d * 11:     System Volume Information
[stud402@centos-s-4vcpu-8gb-tor1-01 6-undel-fat]$
```

## istat command

\_\_\_\_\_The next command I did was *istat -f fat /home/stud402/6-undel-fat/6-fat-undel.dd 4* .

This command will give the metadata associated with that sector (sector 4 in this case). The *ifind* command only gave us the sector number whereas *istat* gives us more data. We can see when the file was last written, last accessed, and when it was created. We can see what sectors on the disk the file takes up. *\_rag1.dat* takes up 2 clusters; 2 sectors per cluster; therefore we have 4 sectors for *\_rag1.dat*. By changing the number at the end of the argument we can look at any sector. We can see “Not Allocated” because these files have been deleted and we can see the size in bytes. By exploring each sector we can begin to reconstruct the deleted file.

```

stud402@centos-s-4vcpu-8gb-tor1-01:~/6-undel-fat
[stud402@centos-s-4vcpu-8gb-tor1-01 6-undel-fat]$ istat -f fat /home/stud402/6-undel-fat/6-fat-undel.dd 4
Directory Entry: 4
Not Allocated
File Attributes: File, Archive
Size: 1584
Name: _rag1.dat

Directory Entry Times:
Written:      2004-02-14 12:51:16 (UTC)
Accessed:     2004-02-14 00:00:00 (UTC)
Created:      2004-02-14 12:50:48 (UTC)

Sectors:
88 89 90 91
[stud402@centos-s-4vcpu-8gb-tor1-01 6-undel-fat]$ istat -f fat /home/stud402/6-undel-fat/6-fat-undel.dd 5
Directory Entry: 5
Not Allocated
File Attributes: File, Archive
Size: 3873
Name: _rag2.dat

Directory Entry Times:
Written:      2004-02-14 12:52:54 (UTC)
Accessed:     2004-02-14 00:00:00 (UTC)
Created:      2004-02-14 12:51:01 (UTC)

Sectors:
90 91 92 93 94 95 96 97
[stud402@centos-s-4vcpu-8gb-tor1-01 6-undel-fat]$ █

```

## Blkcat command

\_\_\_\_\_The next command I wrote was `blkcat -h /home/stud402/6-undel-fat/6-fat-undel.dd 88 4` . This command shows the data from sectors 88 and the next three (sectors 88, 89, 90, 91). To put this command into context we should look at the output of the `istat` command. `_rag1.dat` took up 4 sectors starting at 88. The `blkcat` command shows the entire contents of `_rag1.dat`

```

Sectors:
88 89 90 91

```

```

stud402@centos-s-4vcpu-8gb-tor1-01:~/6-undel-fat
[stud402@centos-s-4vcpu-8gb-tor1-01 6-undel-fat]$ blkcat -h /home/stud402/6-undel-fat/6-fat-undel.dd 88 4
0      a76d9a4b baad2a97 eb0125d9 02c70365      .m.K ..*. ..%. ...e
16     f6e03d3f 5d4fd743 9e4b37ce e63f1199      ..=? ]O.C .K7. .?..
32     3a97cec0 3bfe448c a3a46380 be08fd9a      :... ;D. ..C. ....
48     6c92988c 55accbc2 f4ec27fd 9716c80a      l... U... ..'. ....
64     9c66dc51 fb6e8b40 420d9dc1 7fdb4a92      .f.Q .n.@ B... ....
80     c615c254 1614961c f4314002 06363011      ...T .... .l@. .60.
96     3dc89654 f3037e26 6827f102 ebd9f105      =..T ..~& h'... ....
112    705c939c 7436a601 1fb9bcd1 db5f1df7      p\.. t6.. .... _..
128    8a1312d0 3c8d5a1e 97442ace 365166f0      .... <.Z. .D*. 6Qf.
144    0c4dd8c9 9ebb6d68 f0e49f2c 291b1dfb      .M.. ..mh .... )...
160    4dd5d482 d750e2c7 8ce517cd d704a113      M... .P.. .... ....
176    e1764fca 4fb4ec7f 4b42d20c 0d8fec30      .vO. O... KB... ..0
192    002b1623 58439a31 35820963 bclde053      .+.# XC.l 5... ..S

```

The output was much too large to fit into one screenshot.

## **blkstat command**

\_\_\_\_\_The second to last command I did was *blkstat -f fat*

*/home/stud402/6-undel-fat/6-fat-undel.dd 88* . This command will show the allocation status of a sector. The “Not Allocated” text shows us that the sector was deleted.

```
stud402@centos-s-4vcpu-8gb-tor1-01:~/6-undel-fat
[stud402@centos-s-4vcpu-8gb-tor1-01 6-undel-fat]$ blkstat -f fat /home/stud402/6-undel-fat/6-fat-undel.dd 88
Sector: 88
Not Allocated
Cluster: 2
[stud402@centos-s-4vcpu-8gb-tor1-01 6-undel-fat]$
```

```
Sectors:
88 89 90 91
```

## **blkcalc command**

\_\_\_\_\_The last command I did was *blkcalc -u 88 -f fat /home/stud402/6-undel-fat/6-fat-undel.dd*  
. This command shows us the physical sector on the disk where the data actually begins. This particular example shows cluster 88; 2 sectors per cluster;  $88 * 2 = 176$ .

```
stud402@centos-s-4vcpu-8gb-tor1-01:~/6-undel-fat
[stud402@centos-s-4vcpu-8gb-tor1-01 6-undel-fat]$ blkcalc -u 88 -f fat /home/stud402/6-undel-fat/6-fat-undel.dd
176
[stud402@centos-s-4vcpu-8gb-tor1-01 6-undel-fat]$
```