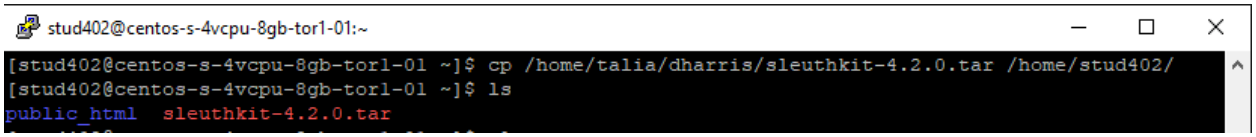
Davis Fulton
100228199
INFO 4120: Digital Forensics
S50
Assignment
11/20/20

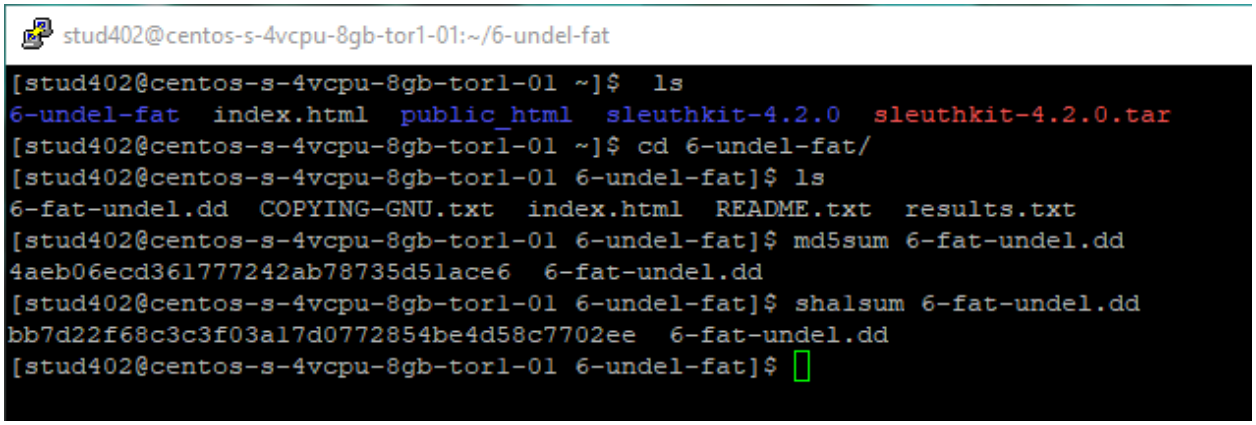
The first thing I did was to copy the tar file from /dharris/ to /stud402/. I did this by typing *cp /home/talia/dharris/sluethkit-4.2.0.tar /home/stud402*. To check if it worked I typed the *ls* command.



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`.

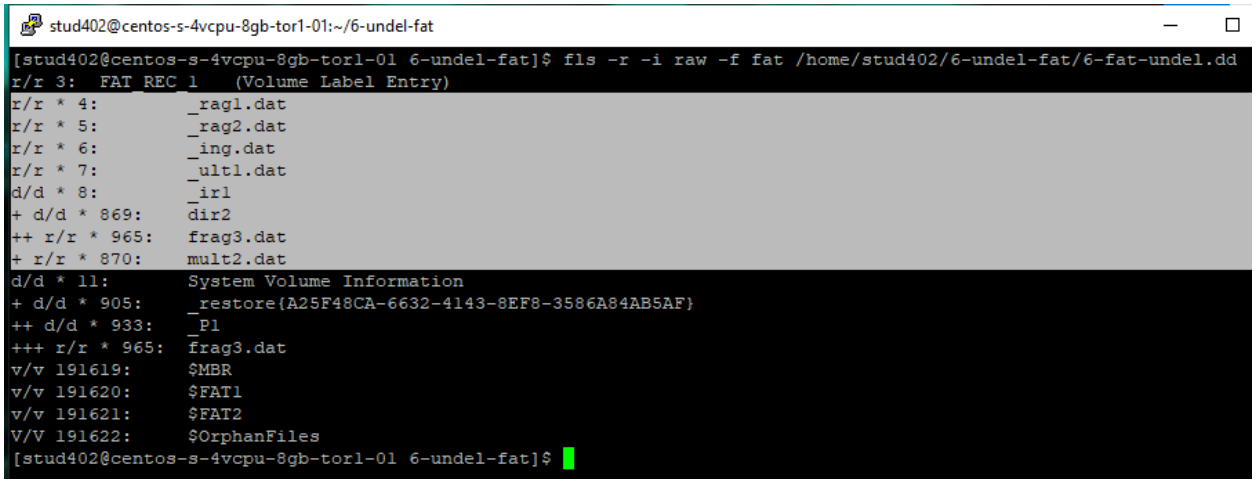
```
4aeb06ecd361777242ab78735d51ace6  6-fat-undel.dd
```



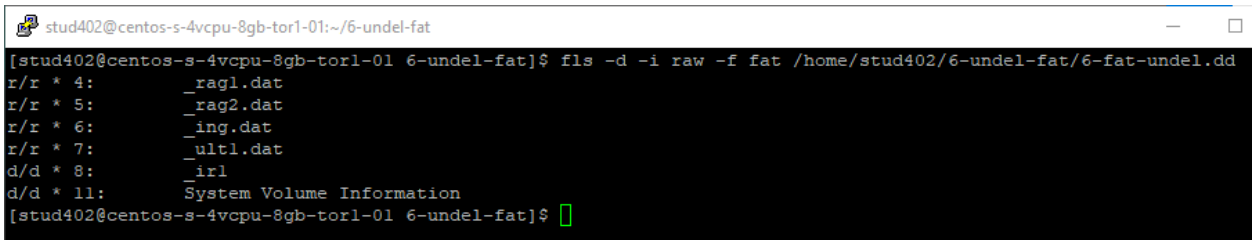
With both the sleuthkit, and files I needed. I was now ready to begin analyzing the 6-fat-undel.dd file for any forensics evidence

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.



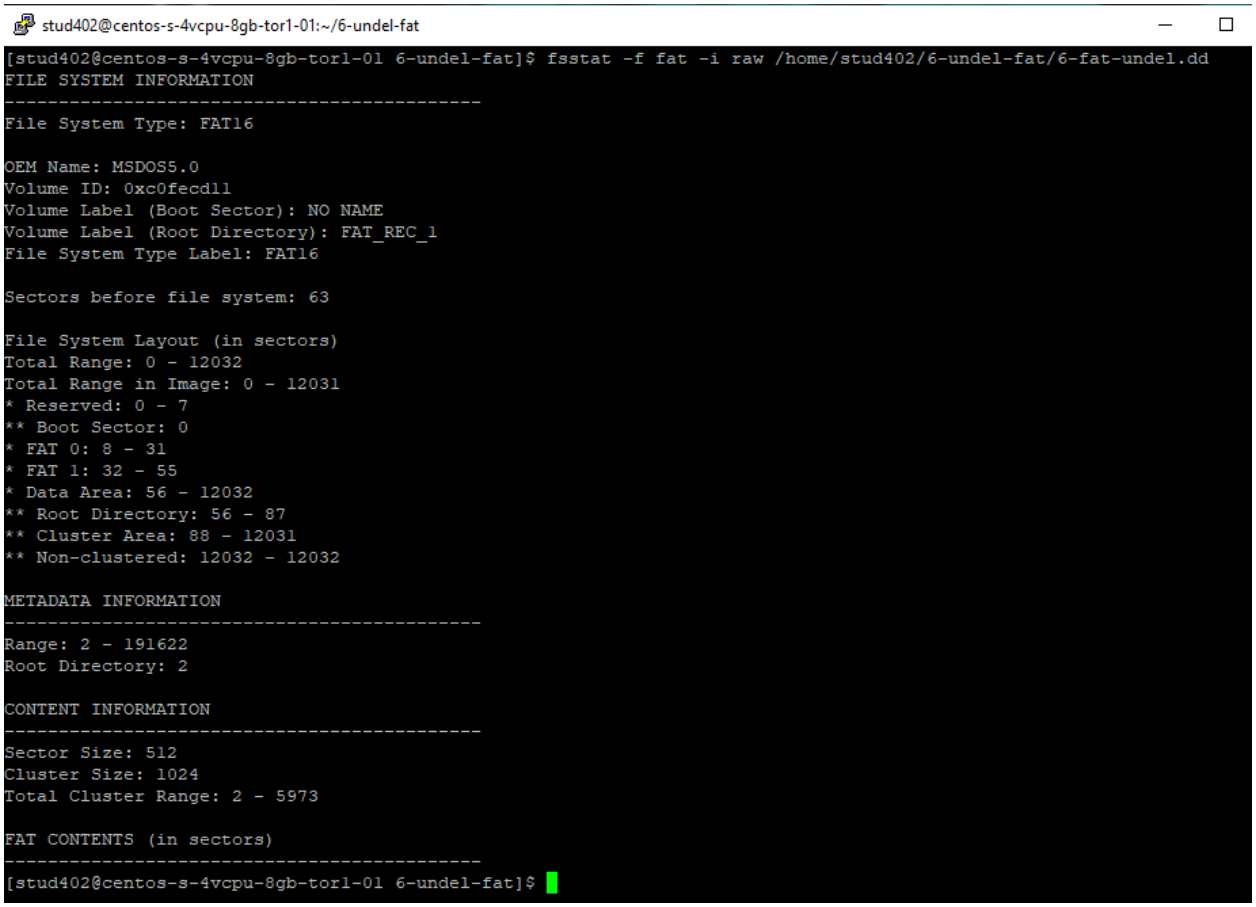
If we only wanted to see the deleted files we can type *fls -d -i raw -f fat /home/stud402/6-undel-fat/6-fat-undel.dd* .



fsstat command

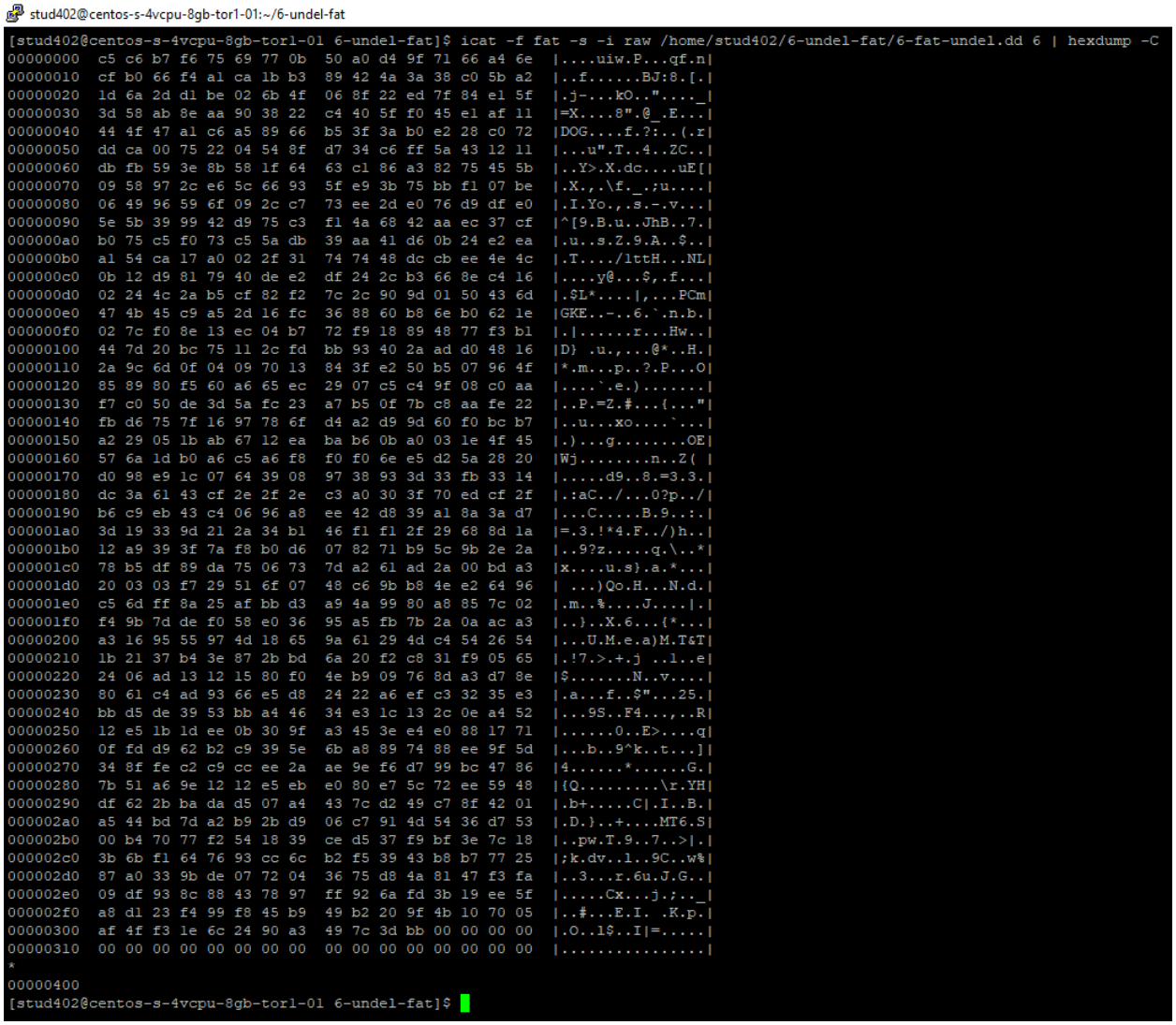
The next command I used was *fsstat -f fat -i raw /home/stud402/6-undel-fat/6-fat-undel.dd* . This will give file system information. From this information, we can see that it's an MSDOS5 disk. The volume label has no name. The file system type is FAT 16. There are 12032 sectors on this disk. Sector 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.



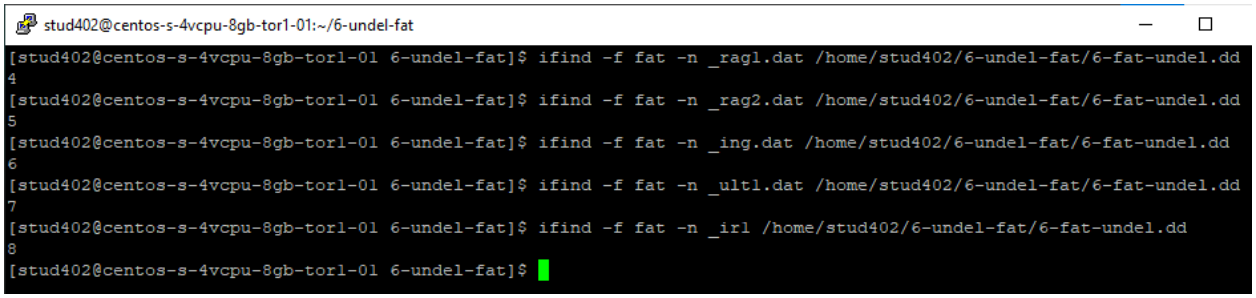
<u>icat command</u>

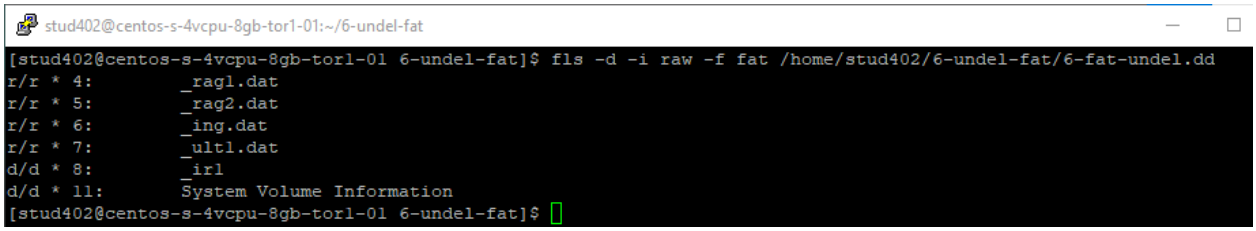
The next command was *icat -f fat -s -i raw /home/stud402//6-undel-fat/6-fat-undel.dd 6 | hexdump -C* . This command gives a hexadecimal output of the content located at any particular sector (sector 6 in this example). At 300 - E, we see the end of the data. The output is very similar to using the DOS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



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.





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*

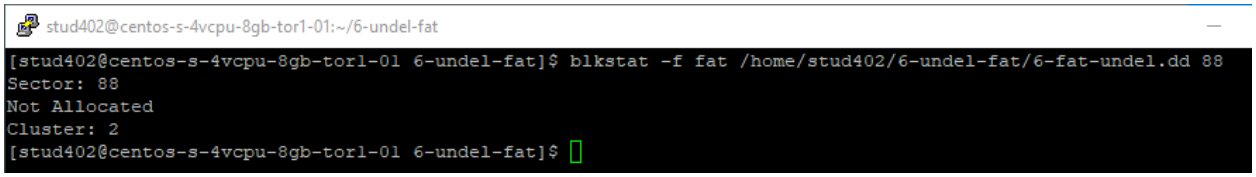
```
Sectors:
88 89 90 91
```

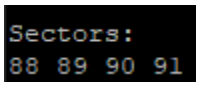
```
stud402@centos-s-4vcpu-8gb-tor1-01:~/6-undel-fat
[stud402@centos-s-4vcpu-8gb-tor1-01 6-undel-fat]$ blkcat -h  /home/stud402/6-undel-fat/6-fat-undel.dd 88 4
0       a76d9a4b baad2a97 eb0125d9 02c70365     .m.K ..*. ..%. ...e
16      f6e03d3f 5d4fd743 9e4b37ce e63f1199     ..=? ]O.C .K7. .?..
32      3a97cec0 3bfe448c a3a46380 be08fd9a     :... ;.D. ..c. ....
48      6c92988c 55accbc2 f4ec27fd 9716c80a     l... U... ..'. ....
64      9c66dc51 fb6e8b40 420d9dc1 7fdba492     .f.Q .n.@ B... ....
80      c615c254 161496lc f4314002 06363011     ...T .... .1@. .60.
96      3dc89654 f3037e26 6827f102 ebdf9105     =..T ..~& h'.. ....
112     705c939c 7436a601 1fb9bcd1 db5f1df7     p\.. t6.. .... ._..
128     8a1312d0 3c8d5a1e 97442ace 365166f0     .... <.Z. .D*. 6Qf.
144     0c4dd8c9 9ebb6d68 f0e49f2c 291bldfb     .M.. ..mh ..., )...
160     4dd5d482 d750e2c7 8ce517cd d704a113     M... .P.. .... ....
176     e1764fca 4fb4ec7f 4b42d20c 0d8fec30     .vO. O... KB.. ...0
192     002b1623 58439a31 35820963 bc1de053     .+.# XC.1 5..c ...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.





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.