James Gouveia

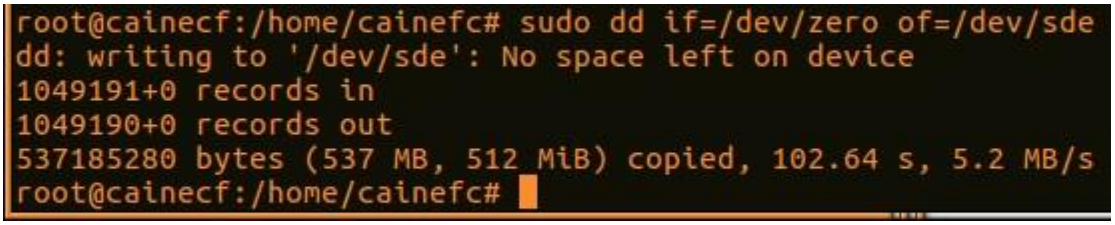
Professor Sun

CSC 153

University of California Sacramento

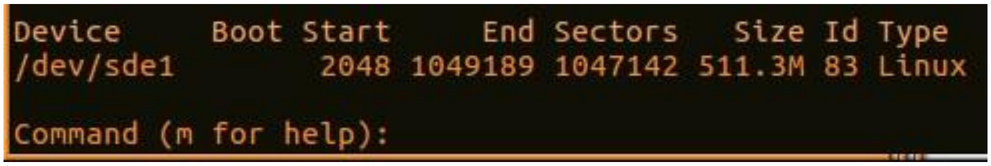
Activity 3

Zero out:



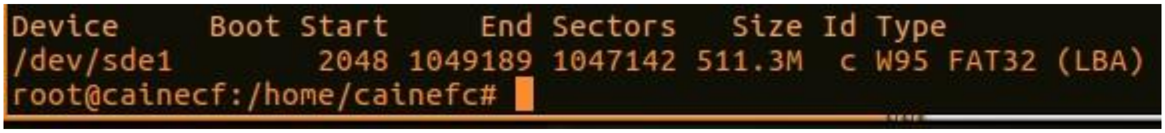
```
root@cainecf:/home/cainefc# sudo dd if=/dev/zero of=/dev/sde
dd: writing to '/dev/sde': No space left on device
1049191+0 records in
1049190+0 records out
537185280 bytes (537 MB, 512 MiB) copied, 102.64 s, 5.2 MB/s
root@cainecf:/home/cainefc#
```

Create Partition:



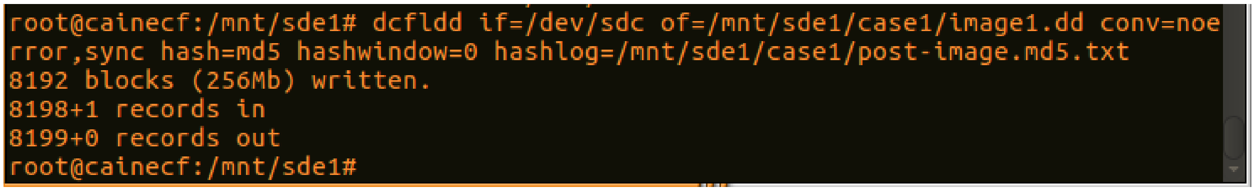
```
Device     Boot Start     End Sectors   Size Id Type
/dev/sde1        2048 1049189 1047142 511.3M 83 Linux

Command (m for help):
```

File System Established:



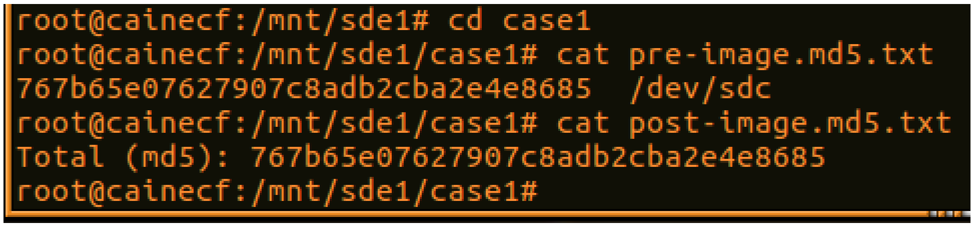
```
Device     Boot Start     End Sectors   Size Id Type
/dev/sde1        2048 1049189 1047142 511.3M  c W95 FAT32 (LBA)
root@cainecf:/home/cainefc#
```

Acquisition Complete:



```
root@cainecf:/mnt/sde1# dcfldd if=/dev/sdc of=/mnt/sde1/case1/image1.dd conv=noe
rror,sync hash=md5 hashwindow=0 hashlog=/mnt/sde1/case1/post-image.md5.txt
8192 blocks (256Mb) written.
8198+1 records in
8199+0 records out
root@cainecf:/mnt/sde1#
```

Validation:



```
root@cainecf:/mnt/sde1# cd case1
root@cainecf:/mnt/sde1/case1# cat pre-image.md5.txt
767b65e07627907c8adb2cba2e4e8685  /dev/sdc
root@cainecf:/mnt/sde1/case1# cat post-image.md5.txt
Total (md5): 767b65e07627907c8adb2cba2e4e8685
root@cainecf:/mnt/sde1/case1#
```

Post Activity Questions:

1. The two broad categories of acquisition are live and static.
2. Live storage acquisition is copying storage while a device is running. It is useful as the process of turning off a device can destroy some data and works best when an investigator can access the device before anyone else has touched the device.
3. fdisk -l
4. The mkfs command creates a file system on a disk. The disk needs a file system before data can be written to it.
5. The evidence drive is never changed in anyway, this drive must be forensically preserved so any evidence found can be used in court. The target drive receives the copy of the data, and all data analysis occurs on the target drive.
6. The target drive needs to be zeroed out to make sure any residual data on the drive is turned to 0's so when the evidence drive is copied to it, the data can be trusted as accurate.
7. The string "/dev/sdc" refers to the target drive to be zeroed, the "sdc" refers to the drive's name.
8. The md5sum /dev/sdb command creates a md5 hash of the evidence drive. When the data is copied from the evidence drive to the target drive, the check sum can be run again which verifies if an exact copy of the evidence drive was obtained.
9. The hash should be calculated once on the evidence drive before any data is extracted. The hash should be run a second time on the target drive to verify the two-hash values match.
10. Another command that can be used to acquire data is dcfldd if=/dev/*evidence drive* of=/mnt/*target drive*