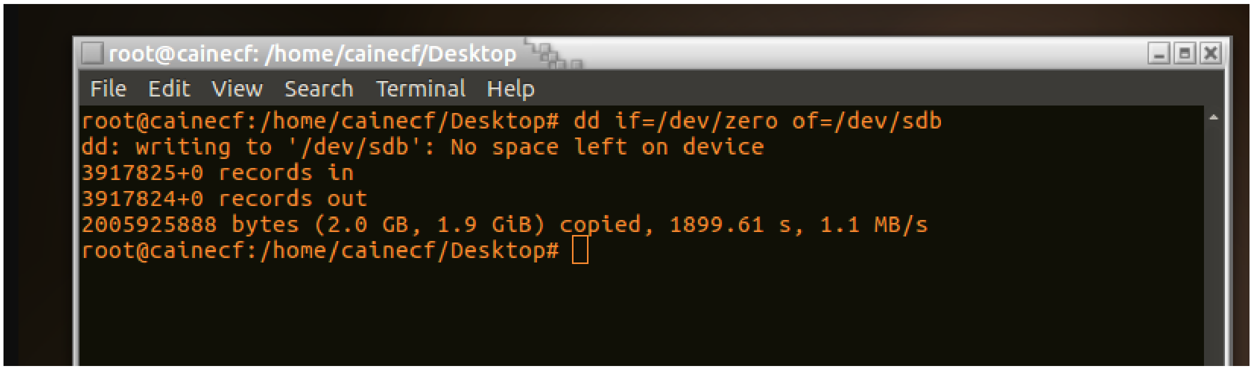
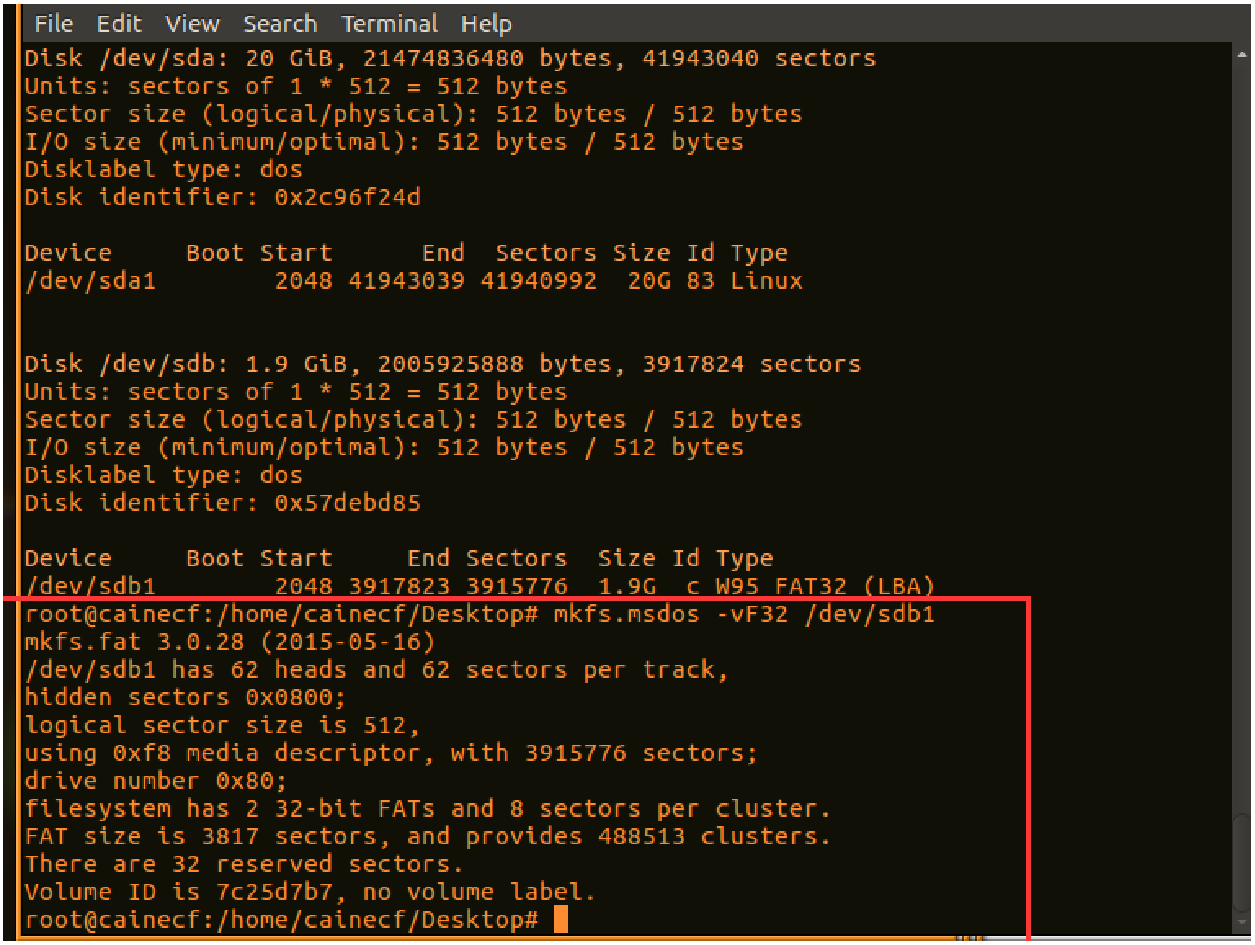
Drive zero'd out


root@cainecf: /home/cainecf/Desktop
File Edit View Search Terminal Help

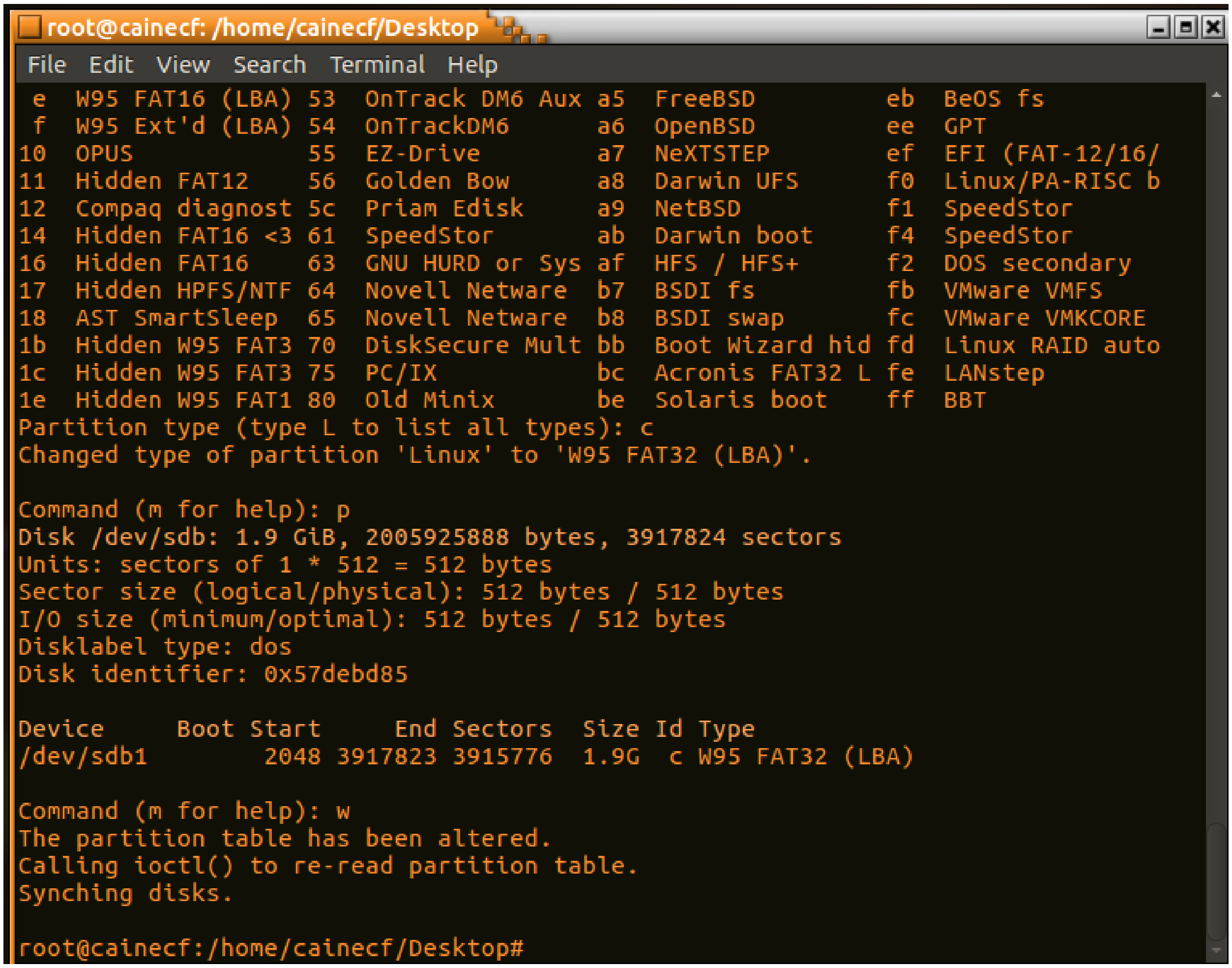
```
root@cainecf:/home/cainecf/Desktop# dd if=/dev/zero of=/dev/sdb
dd: writing to '/dev/sdb': No space left on device
3917825+0 records in
3917824+0 records out
2005925888 bytes (2.0 GB, 1.9 GiB) copied, 1899.61 s, 1.1 MB/s
root@cainecf:/home/cainecf/Desktop# 
```

Format FAT file system



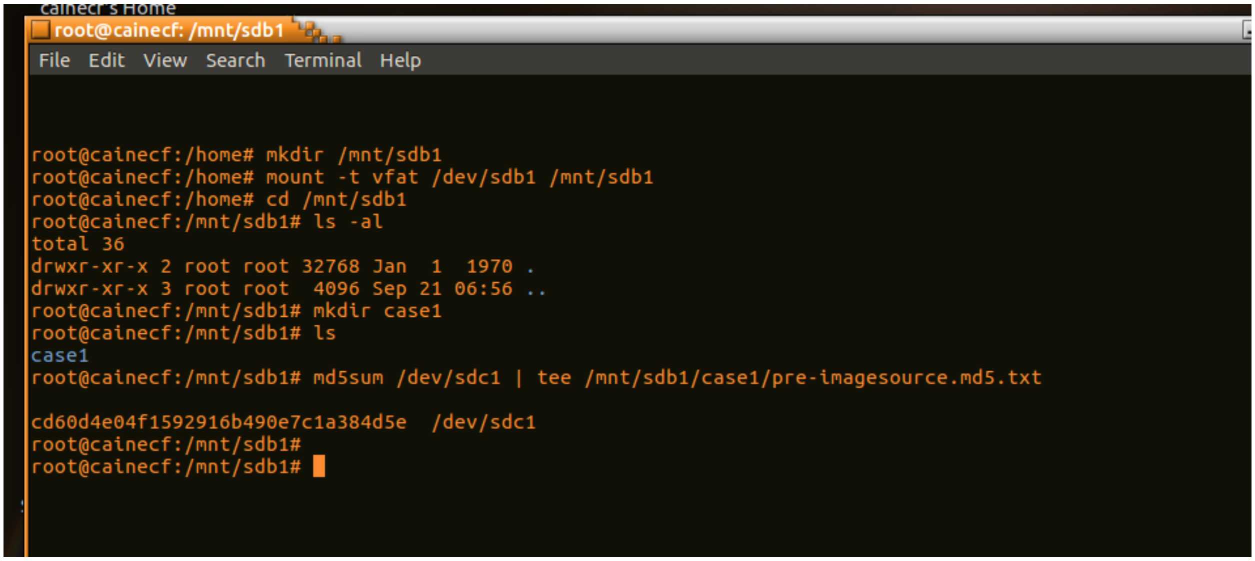
```
Disk /dev/sda: 20 GiB, 21474836480 bytes, 41943040 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x2c96f24d

Device     Boot Start      End  Sectors Size Id Type
/dev/sda1        2048 41943039 41940992  20G 83 Linux


Disk /dev/sdb: 1.9 GiB, 2005925888 bytes, 3917824 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x57debd85

Device     Boot Start     End Sectors  Size Id Type
/dev/sdb1        2048 3917823 3915776  1.9G  c W95 FAT32 (LBA)
root@cainecf:/home/cainecf/Desktop# mkfs.msdos -vF32 /dev/sdb1
mkfs.fat 3.0.28 (2015-05-16)
/dev/sdb1 has 62 heads and 62 sectors per track,
hidden sectors 0x0800;
logical sector size is 512,
using 0xf8 media descriptor, with 3915776 sectors;
drive number 0x80;
filesystem has 2 32-bit FATs and 8 sectors per cluster.
FAT size is 3817 sectors, and provides 488513 clusters.
There are 32 reserved sectors.
Volume ID is 7c25d7b7, no volume label.
root@cainecf:/home/cainecf/Desktop# 
```

Change disk to FAT32



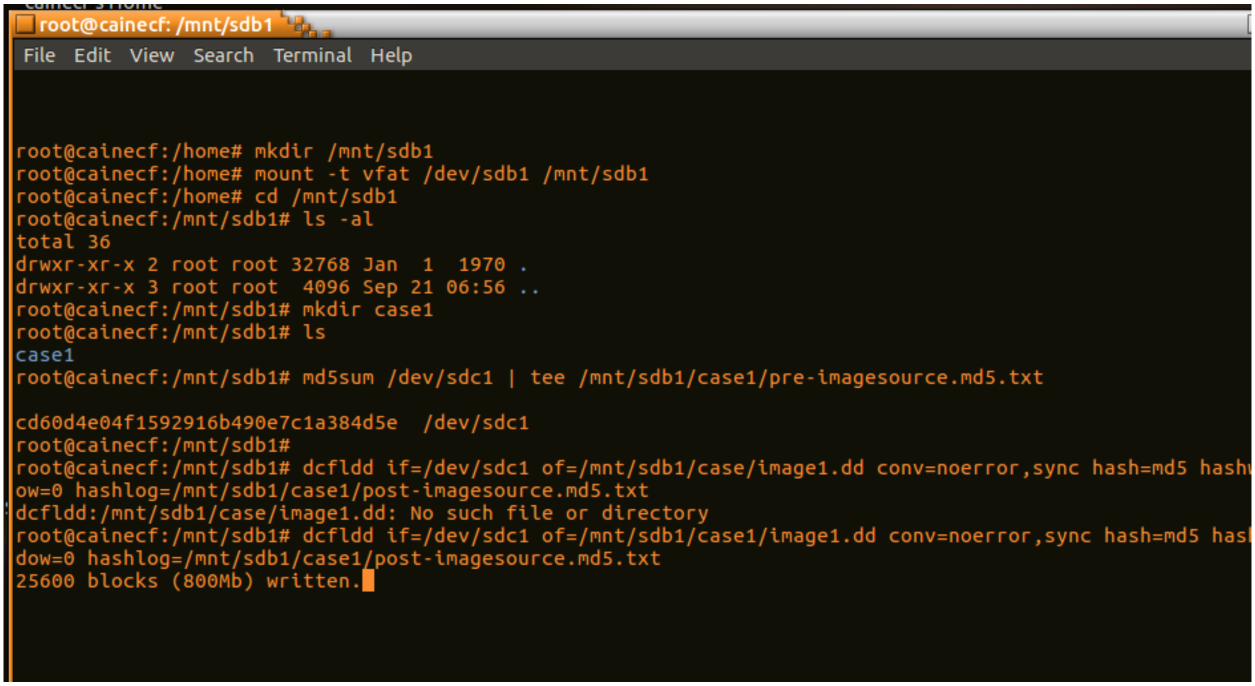
```
 e  W95 FAT16 (LBA) 53  OnTrack DM6 Aux a5  FreeBSD         eb  BeOS fs
 f  W95 Ext'd (LBA) 54  OnTrackDM6      a6  OpenBSD         ee  GPT
10  OPUS            55  EZ-Drive        a7  NeXTSTEP        ef  EFI (FAT-12/16/
11  Hidden FAT12    56  Golden Bow      a8  Darwin UFS      f0  Linux/PA-RISC b
12  Compaq diagnost 5c  Priam Edisk     a9  NetBSD          f1  SpeedStor
14  Hidden FAT16 <3 61  SpeedStor       ab  Darwin boot     f4  SpeedStor
16  Hidden FAT16    63  GNU HURD or Sys af  HFS / HFS+      f2  DOS secondary
17  Hidden HPFS/NTF 64  Novell Netware  b7  BSDI fs         fb  VMware VMFS
18  AST SmartSleep  65  Novell Netware  b8  BSDI swap       fc  VMware VMKCORE
1b  Hidden W95 FAT3 70  DiskSecure Mult bb  Boot Wizard hid fd  Linux RAID auto
1c  Hidden W95 FAT3 75  PC/IX           bc  Acronis FAT32 L fe  LANstep
1e  Hidden W95 FAT1 80  Old Minix       be  Solaris boot    ff  BBT
Partition type (type L to list all types): c
Changed type of partition 'Linux' to 'W95 FAT32 (LBA)'.

Command (m for help): p
Disk /dev/sdb: 1.9 GiB, 2005925888 bytes, 3917824 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x57debd85

Device     Boot Start     End Sectors  Size Id Type
/dev/sdb1        2048 3917823 3915776  1.9G  c W95 FAT32 (LBA)

Command (m for help): w
The partition table has been altered.
Calling ioctl() to re-read partition table.
Synching disks.

root@cainecf:/home/cainecf/Desktop#
```

Calculate source HASH



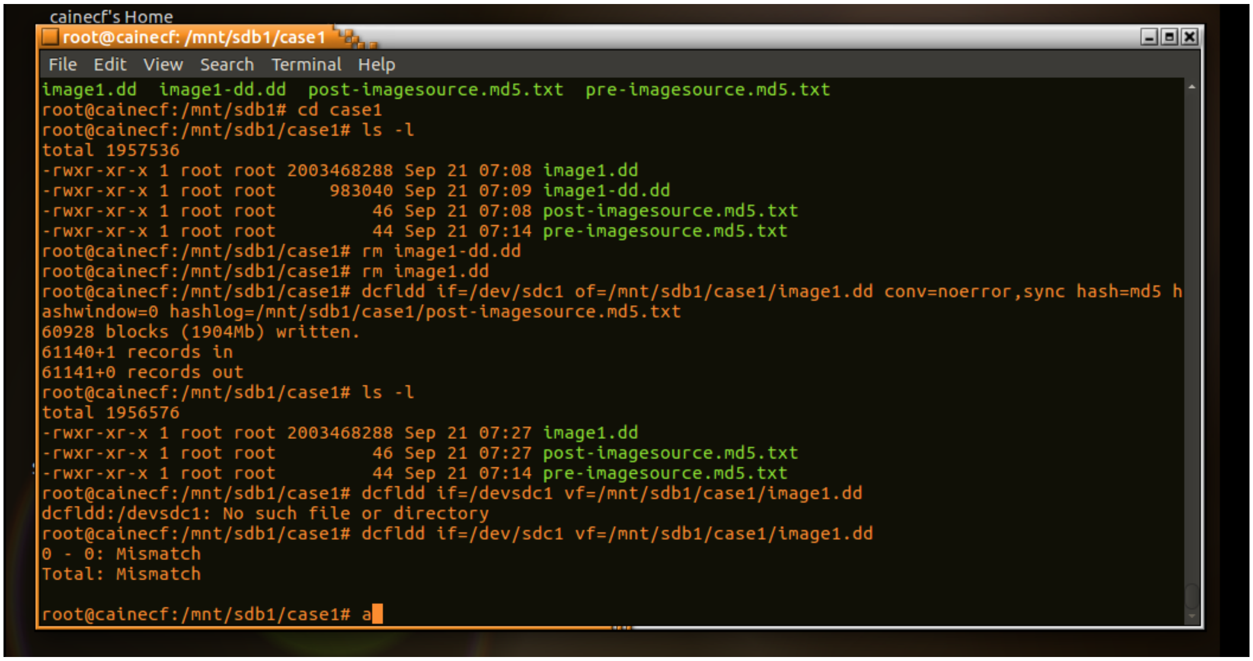
```
root@cainecf:/home# mkdir /mnt/sdb1
root@cainecf:/home# mount -t vfat /dev/sdb1 /mnt/sdb1
root@cainecf:/home# cd /mnt/sdb1
root@cainecf:/mnt/sdb1# ls -al
total 36
drwxr-xr-x 2 root root 32768 Jan  1  1970 .
drwxr-xr-x 3 root root  4096 Sep 21 06:56 ..
root@cainecf:/mnt/sdb1# mkdir case1
root@cainecf:/mnt/sdb1# ls
case1
root@cainecf:/mnt/sdb1# md5sum /dev/sdc1 | tee /mnt/sdb1/case1/pre-imagesource.md5.txt

cd60d4e04f1592916b490e7c1a384d5e  /dev/sdc1
root@cainecf:/mnt/sdb1#
root@cainecf:/mnt/sdb1#
```

Copy to target drive



```
root@cainecf:/home# mkdir /mnt/sdb1
root@cainecf:/home# mount -t vfat /dev/sdb1 /mnt/sdb1
root@cainecf:/home# cd /mnt/sdb1
root@cainecf:/mnt/sdb1# ls -al
total 36
drwxr-xr-x 2 root root 32768 Jan  1  1970 .
drwxr-xr-x 3 root root  4096 Sep 21 06:56 ..
root@cainecf:/mnt/sdb1# mkdir case1
root@cainecf:/mnt/sdb1# ls
case1
root@cainecf:/mnt/sdb1# md5sum /dev/sdc1 | tee /mnt/sdb1/case1/pre-imagesource.md5.txt

cd60d4e04f1592916b490e7c1a384d5e  /dev/sdc1
root@cainecf:/mnt/sdb1#
root@cainecf:/mnt/sdb1# dcfldd if=/dev/sdc1 of=/mnt/sdb1/case/image1.dd conv=noerror,sync hash=md5 hashw
ow=0 hashlog=/mnt/sdb1/case1/post-imagesource.md5.txt
dcfldd:/mnt/sdb1/case/image1.dd: No such file or directory
root@cainecf:/mnt/sdb1# dcfldd if=/dev/sdc1 of=/mnt/sdb1/case1/image1.dd conv=noerror,sync hash=md5 has
dow=0 hashlog=/mnt/sdb1/case1/post-imagesource.md5.txt
25600 blocks (800Mb) written.
```

Validate HASH


cainecf's Home
root@cainecf: /mnt/sdb1/case1
File Edit View Search Terminal Help

```
image1.dd  image1-dd.dd  post-imagesource.md5.txt  pre-imagesource.md5.txt
root@cainecf:/mnt/sdb1# cd case1
root@cainecf:/mnt/sdb1/case1# ls -l
total 1957536
-rwxr-xr-x 1 root root 2003468288 Sep 21 07:08 image1.dd
-rwxr-xr-x 1 root root     983040 Sep 21 07:09 image1-dd.dd
-rwxr-xr-x 1 root root         46 Sep 21 07:08 post-imagesource.md5.txt
-rwxr-xr-x 1 root root         44 Sep 21 07:14 pre-imagesource.md5.txt
root@cainecf:/mnt/sdb1/case1# rm image1-dd.dd
root@cainecf:/mnt/sdb1/case1# rm image1.dd
root@cainecf:/mnt/sdb1/case1# dcfldd if=/dev/sdc1 of=/mnt/sdb1/case1/image1.dd conv=noerror,sync hash=md5 h
ashwindow=0 hashlog=/mnt/sdb1/case1/post-imagesource.md5.txt
60928 blocks (1904Mb) written.
61140+1 records in
61141+0 records out
root@cainecf:/mnt/sdb1/case1# ls -l
total 1956576
-rwxr-xr-x 1 root root 2003468288 Sep 21 07:27 image1.dd
-rwxr-xr-x 1 root root         46 Sep 21 07:27 post-imagesource.md5.txt
-rwxr-xr-x 1 root root         44 Sep 21 07:14 pre-imagesource.md5.txt
root@cainecf:/mnt/sdb1/case1# dcfldd if=/devsdc1 vf=/mnt/sdb1/case1/image1.dd
dcfldd:/devsdc1: No such file or directory
root@cainecf:/mnt/sdb1/case1# dcfldd if=/dev/sdc1 vf=/mnt/sdb1/case1/image1.dd
0 - 0: Mismatch
Total: Mismatch

root@cainecf:/mnt/sdb1/case1# a
```

1. 1. What are the two broad categories of acquisition? **Physical and logical**

2. 2. What is a live storage acquisition and when is it used? **When the data is taken from a running machine i.e a computer at a suspects house.**

3. 3. Which command should be used to check the disks available on the current system? You only need to state the command name, not the entire command string. **Fdisk -l**

4. The mkfs -t command does what? **It is used to build a linux file system with a specified type.**

5. Which drive should be 'zeroed out', the source evidence drive or the target drive? **The target drive**

6. What is the purpose of 'zeroing out' before a storage acquisition is performed? **It ensures the target drive will not corrupt any data being acquired from the evidence drive.**

7. When you issue the command the command dd if=/dev/zero of=/dev/sdb What does the string "/dev/sdb" represent? **It is the path for the output file destination.**

8. The md5sum /dev/sda command does what? Why is it used? **It applies a MD5 hash to the file in the path location. We use it so we can compare the MD5 has of the source file to a MD5 hash applied to the output file to ensure the integrity of the data.**

9. How many times should the md5sum command be used at least in one acquisition? **Twice. Once on the original file, and once on the copy to ensure data integrity.**

10. Instead of using “dd”, what other commands can you use to perform data acquisition in Linux? **dcfldd**