Writeup - Diskfall

When a user will get the disk the first commands might be:

```
1) mmls disk.img or fdisk -l disk.img          # They will see 2 partitions
2) losetup -fP disk.img                        # To make the partitions on loop
3) mkdir /mnt/fat32 /mnt/linux
4) mount -o ro /dev/loop0p1 /mnt/fat32         # Mounting FAT32 partition
5) mount -o ro /dev/loop0p2 /mnt/linux    # Mounting linux partition, gives superblock error
```

Part1

```
6) fls -f fat32 -o 2048 disk.img          # Will give an deleted file, which will contain first part
7) Icat -f fat32 -o 2048 disk.img 7 > secret.txt     # 1st part of the flag
```

Now user still needs to check the **/mnt/fat32** folder as it has **.images** folder

```
8) cd /mnt/fat32
9) ls -la
10) cd .images # Will see 2 images
11) strings * # User can see that there is some encryption, some hidden data
12) stegseek –crack banner.jpg/chest.jpg <rockyou.txt> or stegcracker
    banner.jpeg/chest.jpeg <rockyou.txt> # User will need to think about the wordlist
```

Users will get db.log and some decoy log files, now users will need to read through them and need to understand that **db.log** has information related to password, so the password attempts are wrong, but user needs to get those passwords and create **an wordlist** from those wrong passwords

Wordlist Making - crunch {{6}} {{6}} -p 23quen

```
13) exiftool * # Will get an bcrypt hash in as metadata from chest.jpeg
```

Part2

14) binwalk -e disk.img –run-as=root #will show that the partition contains a 7z file
15) dd if=/dev/loop0p2 of=part2.7z bs=1 skip=512 status=progress or dd if=disk.img of=part2.7z count=1 skip=3146240 status=progress #To extract the 7z file from the /dev/loop0p2 partition

Now users will see that part2.7z has encryption, now they will apply their wordlist on the hash

16) echo “<hash>” > hashes.txt # Storing the hash
17) john –format=bcrypt –wordlist=createdwordlist.txt hasesh.txt #Will give them password
18) 7z x part2.7z # To extract the 7z file

Users can now put password and get part2_blob