ATTACK DEFENSE

by PentesterAcademy

Name	Mounting Image (Raw Mount)
URL	https://www.attackdefense.com/challengedetails?cid=1796
Type	Forensics: Disk Forensics

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Image mounting involves mounting the evidence disk image on the local system so the data on the disk can be analysed and inspected.

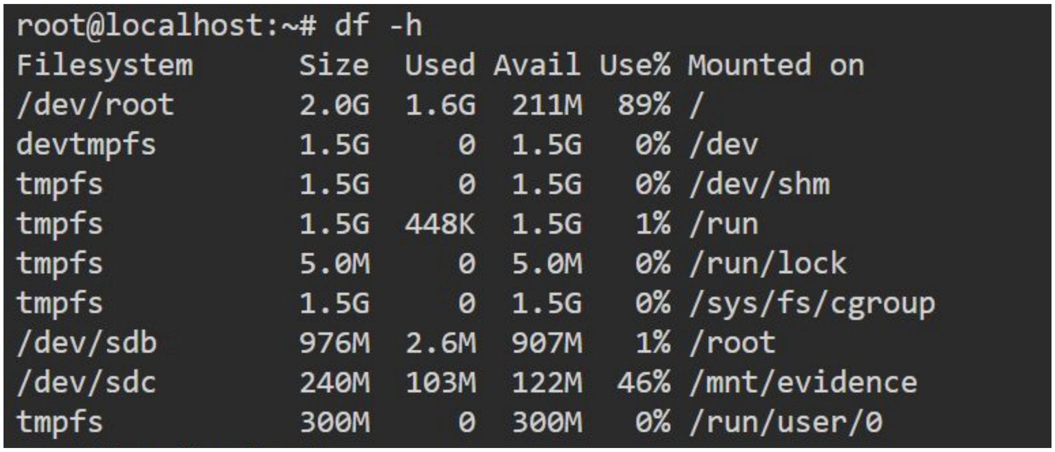
In this lab, an evidence hard disk image is present on an external disk mounted on '/dev/sdc'. The dd tools are installed on the lab machine. Also, a flag file is kept in the /root directory of the disk image filesystem.

Objective: Mount the evidence disk image and retrieve the flag!

Solution:

Step 1: Verify that the external hard drive is mounted.

Command: df -h

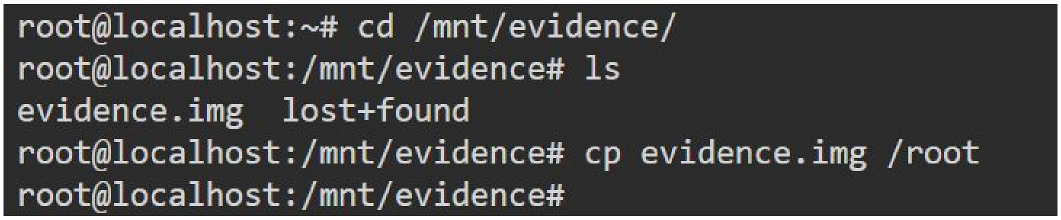


```
root@localhost:~# df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/root       2.0G  1.6G  211M  89% /
devtmpfs        1.5G     0  1.5G   0% /dev
tmpfs           1.5G     0  1.5G   0% /dev/shm
tmpfs           1.5G  448K  1.5G   1% /run
tmpfs           5.0M     0  5.0M   0% /run/lock
tmpfs           1.5G     0  1.5G   0% /sys/fs/cgroup
/dev/sdb        976M  2.6M  907M   1% /root
/dev/sdc        240M  103M  122M  46% /mnt/evidence
tmpfs           300M     0  300M   0% /run/user/0
```

The external disk is mounted at /mnt/evidence directory.

Step 2: Change to the external disk, list the contents and copy the evidence disk image to the /root directory for analysis.

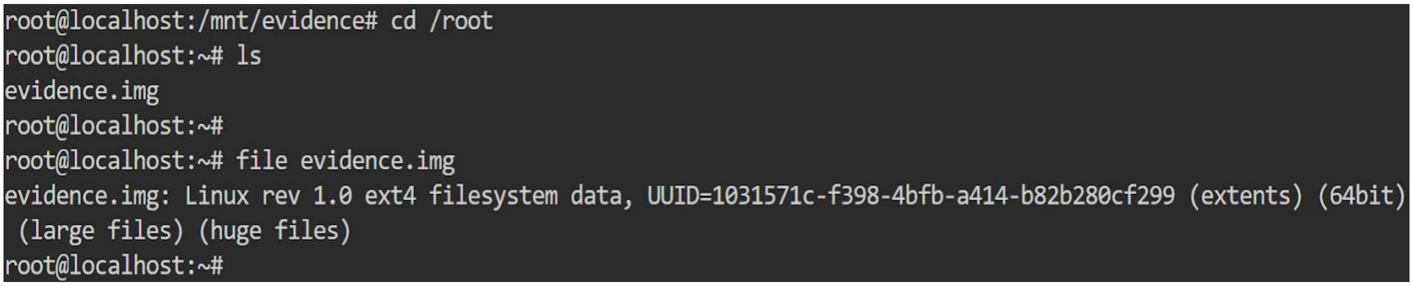
Commands:
cd /mnt/evidence
ls
cp evidence.img /root



```
root@localhost:~# cd /mnt/evidence/
root@localhost:/mnt/evidence# ls
evidence.img  lost+found
root@localhost:/mnt/evidence# cp evidence.img /root
root@localhost:/mnt/evidence#
```

Step 3: Change to the /root directory and check the file type of copied evidence disk image.

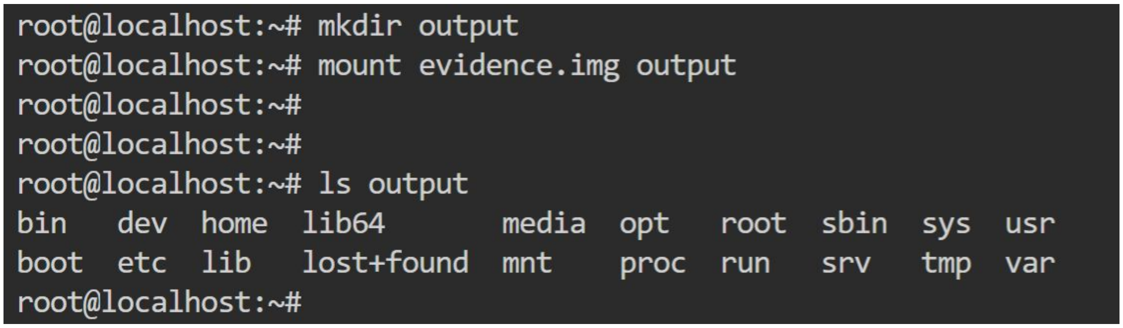
Commands:
cd /root
ls
file evidence.img



```
root@localhost:/mnt/evidence# cd /root
root@localhost:~# ls
evidence.img
root@localhost:~#
root@localhost:~# file evidence.img
evidence.img: Linux rev 1.0 ext4 filesystem data, UUID=1031571c-f398-4bfb-a414-b82b280cf299 (extents) (64bit)
 (large files) (huge files)
root@localhost:~#
```

Step 4: Create a directory to mount the evidence disk image. Mount it using the ‘mount’ utility. Then check its content.

Commands:
mkdir output
mount evidence.img output
ls output

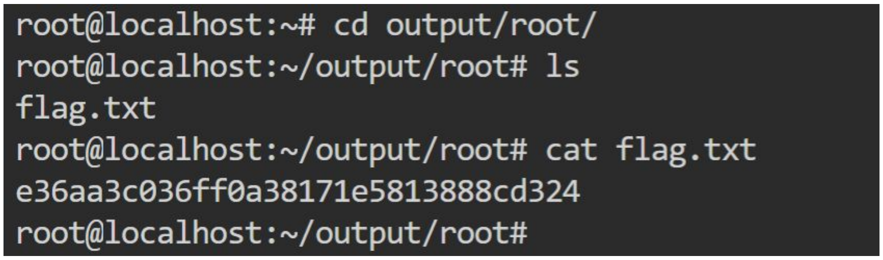


```
root@localhost:~# mkdir output
root@localhost:~# mount evidence.img output
root@localhost:~#
root@localhost:~#
root@localhost:~# ls output
bin   dev  home  lib64       media  opt   root  sbin  sys  usr
boot  etc  lib   lost+found  mnt    proc  run   srv   tmp  var
root@localhost:~#
```

The raw image is successfully mounted.

Step 5: Retrieve the flag stored in the /root directory.

Commands:
cd output/root/
ls
cat flag.txt



```
root@localhost:~# cd output/root/
root@localhost:~/output/root# ls
flag.txt
root@localhost:~/output/root# cat flag.txt
e36aa3c036ff0a38171e5813888cd324
root@localhost:~/output/root#
```

Flag: e36aa3c036ff0a38171e5813888cd324

References:

1. df utility (https://linux.die.net/man/1/df)