# ATTACK DEFENSE

by PentesterAcademy

| | |
|---|---|
| **Name** | Mounting Image (EWF Mount) |
| **URL** | https://www.attackdefense.com/challengedetails?cid=1795 |
| **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.

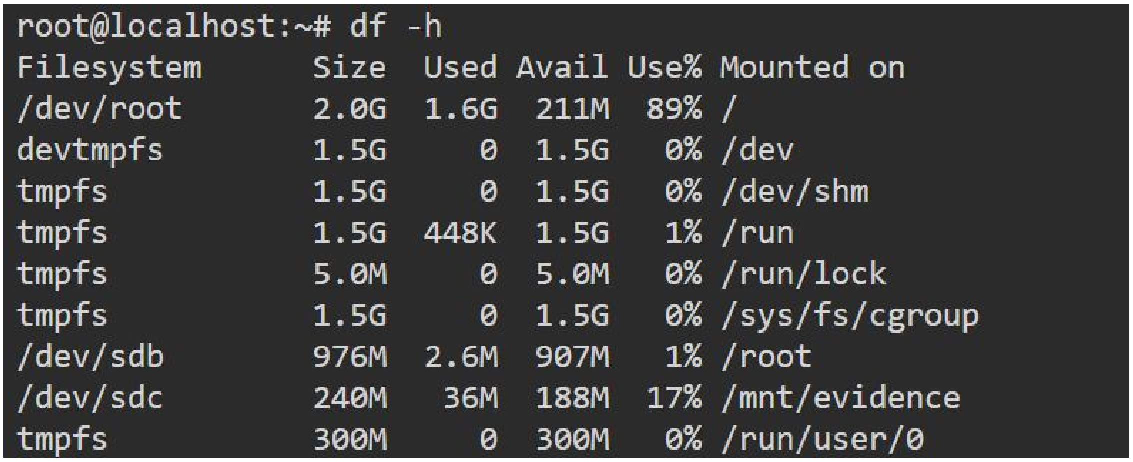
In this lab, an evidence hard disk image is present on an external disk mounted on '/dev/sdc'. The ewf-tools are installed on the lab machine. Also, a flag file is kept in the /root directory of the disk image filesystem.

**Objective:** Mount the evidence disk image using ewf-tools and retrieve the flag!

**Solution:**

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

**Command:** df -h

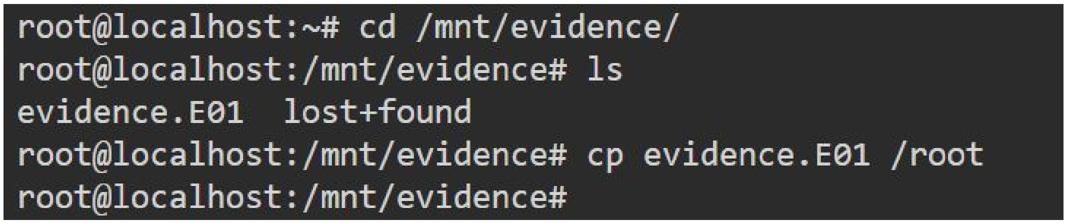


```
root@localhost:~# df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/root       2.0G  1.6G  211M  89% /
devtmpfs        1.5G     0  1.5G   0% /dev
tmpfs           1.5G     0  1.5G   0% /dev/shm
tmpfs           1.5G  448K  1.5G   1% /run
tmpfs           5.0M     0  5.0M   0% /run/lock
tmpfs           1.5G     0  1.5G   0% /sys/fs/cgroup
/dev/sdb        976M  2.6M  907M   1% /root
/dev/sdc        240M   36M  188M  17% /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.

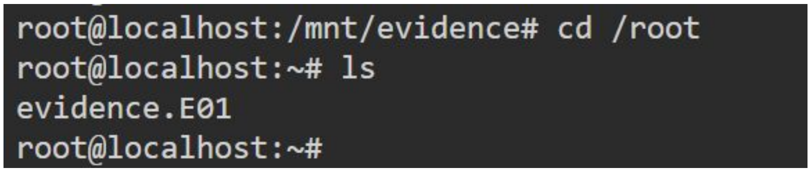
**Commands:**
cd /mnt/evidence
ls
cp evidence.E01 /root



```
root@localhost:~# cd /mnt/evidence/
root@localhost:/mnt/evidence# ls
evidence.E01  lost+found
root@localhost:/mnt/evidence# cp evidence.E01 /root
root@localhost:/mnt/evidence#
```

**Step 3:** Change to the /root directory and check the contents.

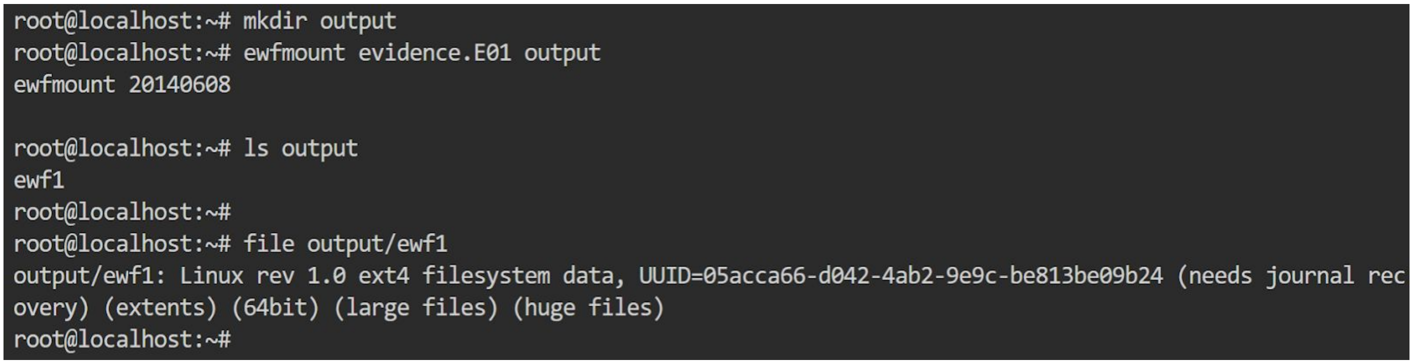
**Commands:**
cd /root
ls



```
root@localhost:/mnt/evidence# cd /root
root@localhost:~# ls
evidence.E01
root@localhost:~#
```

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

**Commands:**
mkdir output
ewfmount evidence.E01 output
ls output
file output/ewf1



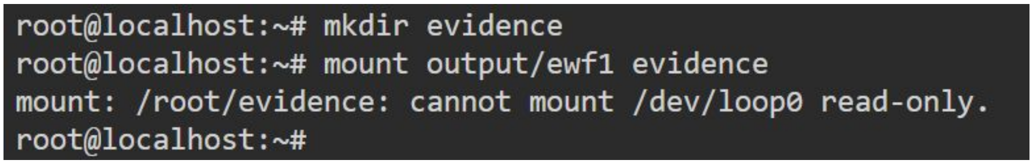
```
root@localhost:~# mkdir output
root@localhost:~# ewfmount evidence.E01 output
ewfmount 20140608

root@localhost:~# ls output
ewf1
root@localhost:~#
root@localhost:~# file output/ewf1
output/ewf1: Linux rev 1.0 ext4 filesystem data, UUID=05acca66-d042-4ab2-9e9c-be813be09b24 (needs journal rec
overy) (extents) (64bit) (large files) (huge files)
root@localhost:~#
```

The raw image is extracted inside the output directory.

**Step 5:** Create another directory to mount the raw image.

**Commands:**
mkdir evidence
mount output/ewf1 evidence

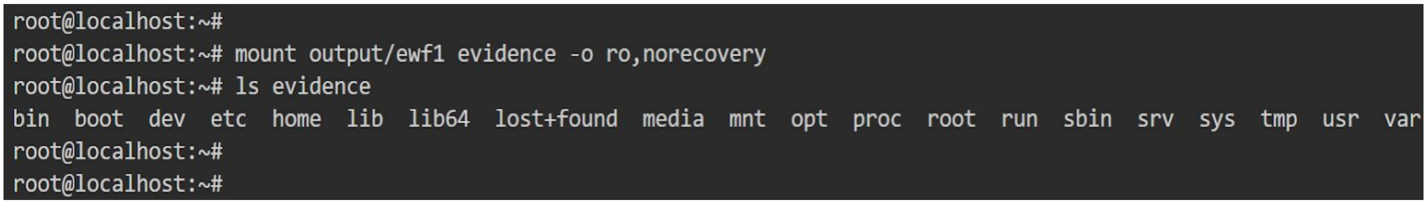


```
root@localhost:~# mkdir evidence
root@localhost:~# mount output/ewf1 evidence
mount: /root/evidence: cannot mount /dev/loop0 read-only.
root@localhost:~#
```

The disk image is corrupted. In such cases it should be mounted in read only, non-recovery mode.

**Step 6:** Mount the disk image in read only mode with nonrecovery flag.

**Command:** mount output/ewf1 evidence -o ro,norecovery

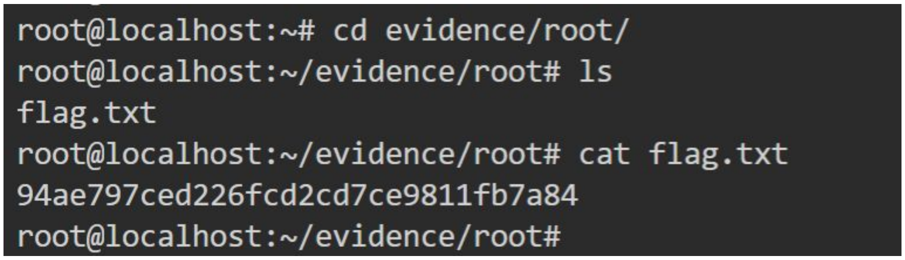


```
root@localhost:~#
root@localhost:~# mount output/ewf1 evidence -o ro,norecovery
root@localhost:~# ls evidence
bin  boot  dev  etc  home  lib  lib64  lost+found  media  mnt  opt  proc  root  run  sbin  srv  sys  tmp  usr  var
root@localhost:~#
root@localhost:~#
```

The raw image is successfully mounted.

**Step 7:** Retrieve the flag stored in the /root directory.

**Commands:**
cd evidence/root/
ls
cat flag.txt



```
root@localhost:~# cd evidence/root/
root@localhost:~/evidence/root# ls
flag.txt
root@localhost:~/evidence/root# cat flag.txt
94ae797ced226fcd2cd7ce9811fb7a84
root@localhost:~/evidence/root#
```

**Flag:** 94ae797ced226fcd2cd7ce9811fb7a84

**References:**

1. Ewf tools (https://github.com/libyal/libewf)