ATTACK DEFENSE

by PentesterAcademy

Name	Forensics Basics
URL	https://www.attackdefense.com/challengedetails?cid=1790
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.

Disk forensics techniques are used to acquire the disk image, process this image to find artifacts of interest including deleted ones.

In this lab, a disk image file “evidence.img” is provided in the home directory of the root user (/root/). Interact with the image using The Sleuth Kit and answer the following questions:

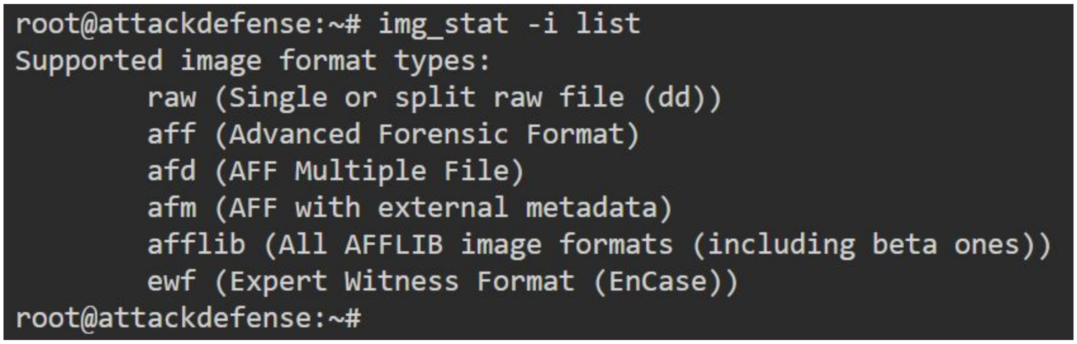
Q1. What is the image format type of the image?

Answer: raw

Solution:

Step 1: List all known image format types.

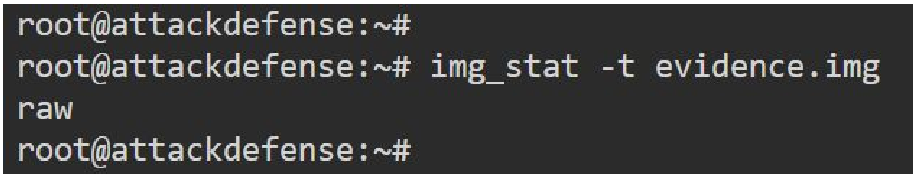
Command: img_stat -i list



```
root@attackdefense:~# img_stat -i list
Supported image format types:
        raw (Single or split raw file (dd))
        aff (Advanced Forensic Format)
        afd (AFF Multiple File)
        afm (AFF with external metadata)
        afflib (All AFFLIB image formats (including beta ones))
        ewf (Expert Witness Format (EnCase))
root@attackdefense:~#
```

Step 2: Check the format type for the given image.

Command: img_stat -t evidence.img



```
root@attackdefense:~#
root@attackdefense:~# img_stat -t evidence.img
raw
root@attackdefense:~#
```

The image format type is raw.

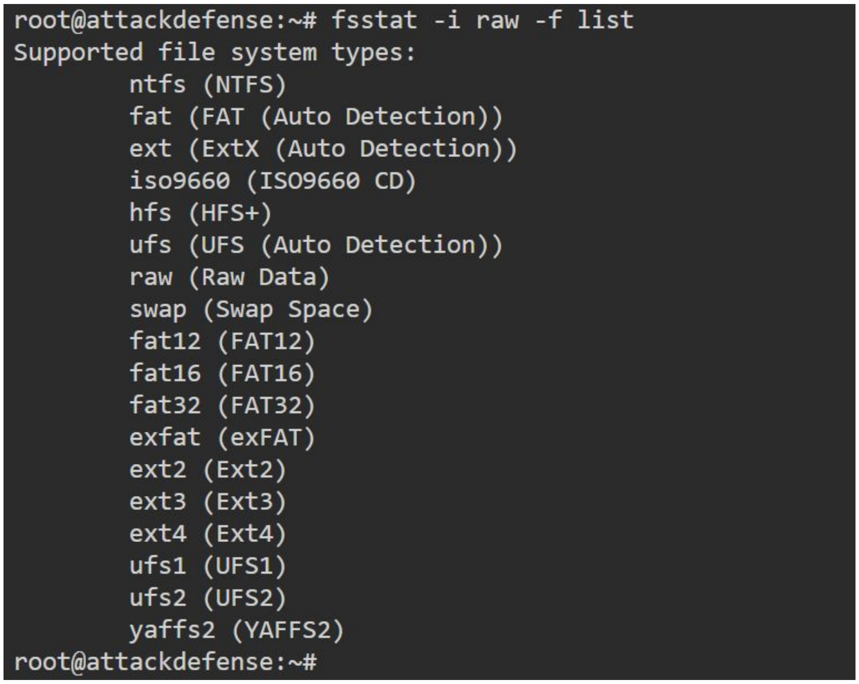
Q2. Which file system type is used in the image?

Answer: ext4

Solution:

Step 1: List all known file system types.

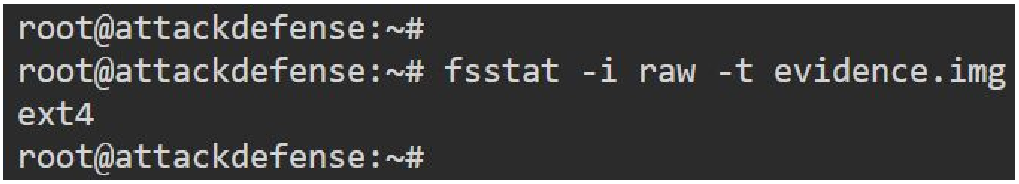
Command: fsstat -i raw -f list



```
root@attackdefense:~# fsstat -i raw -f list
Supported file system types:
        ntfs (NTFS)
        fat (FAT (Auto Detection))
        ext (ExtX (Auto Detection))
        iso9660 (ISO9660 CD)
        hfs (HFS+)
        ufs (UFS (Auto Detection))
        raw (Raw Data)
        swap (Swap Space)
        fat12 (FAT12)
        fat16 (FAT16)
        fat32 (FAT32)
        exfat (exFAT)
        ext2 (Ext2)
        ext3 (Ext3)
        ext4 (Ext4)
        ufs1 (UFS1)
        ufs2 (UFS2)
        yaffs2 (YAFFS2)
root@attackdefense:~#
```

Step 2: Check the file system type of the given image.

Command: fsstat -i raw -t evidence.img



```
root@attackdefense:~#
root@attackdefense:~# fsstat -i raw -t evidence.img
ext4
root@attackdefense:~#
```

The file system of the disk image is ext4.

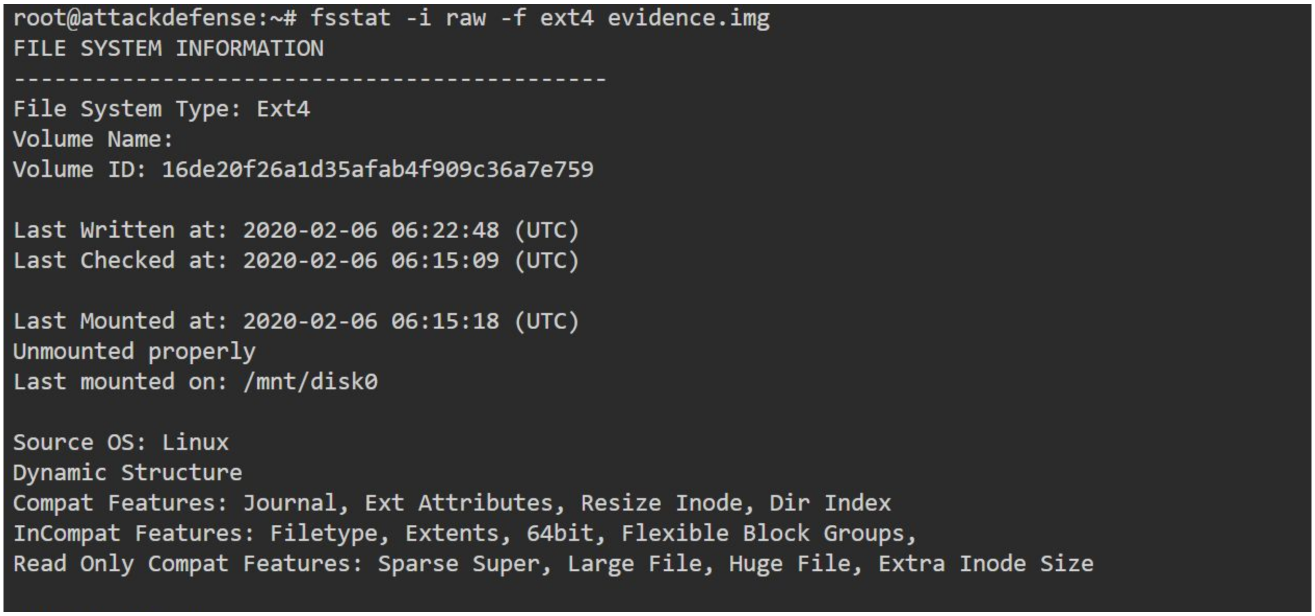
Q3. Which directory was mounted most recently from the disk whose image is provided to us?

Answer: /mnt/disk0

Solution:

Step 1: Check the Last mounted directory from the given image.

Command: fsstat -i raw -f ext4 evidence.img

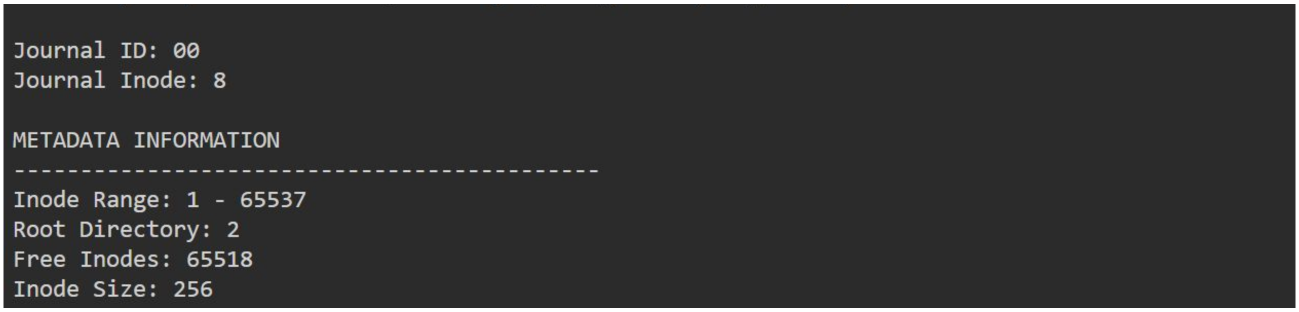


```
root@attackdefense:~# fsstat -i raw -f ext4 evidence.img
FILE SYSTEM INFORMATION
--------------------------------------------
File System Type: Ext4
Volume Name:
Volume ID: 16de20f26a1d35afab4f909c36a7e759

Last Written at: 2020-02-06 06:22:48 (UTC)
Last Checked at: 2020-02-06 06:15:09 (UTC)

Last Mounted at: 2020-02-06 06:15:18 (UTC)
Unmounted properly
Last mounted on: /mnt/disk0

Source OS: Linux
Dynamic Structure
Compat Features: Journal, Ext Attributes, Resize Inode, Dir Index
InCompat Features: Filetype, Extents, 64bit, Flexible Block Groups,
Read Only Compat Features: Sparse Super, Large File, Huge File, Extra Inode Size
```



```
Journal ID: 00
Journal Inode: 8

METADATA INFORMATION
--------------------------------------------
Inode Range: 1 - 65537
Root Directory: 2
Free Inodes: 65518
Inode Size: 256
```

The last mounted directory for the provided image is /mnt/disk0.

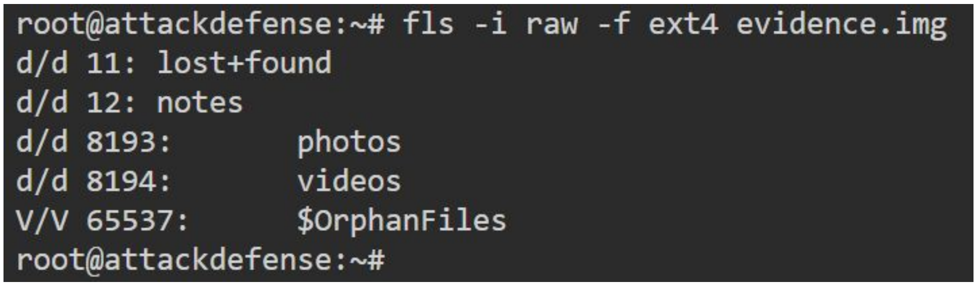
Q4. List the names of the directories present on the image.

Answer: notes, photos, videos

Solution:

Step 1: List all the directories on the root directory of the disk image.

Command: fls -i raw -f ext4 evidence.img



```
root@attackdefense:~# fls -i raw -f ext4 evidence.img
d/d 11: lost+found
d/d 12: notes
d/d 8193:       photos
d/d 8194:       videos
V/V 65537:      $OrphanFiles
root@attackdefense:~#
```

Q5. What is the name of the file present in the notes directory?

Answer: flag.txt

Solution:

Step 1: list the files stored under the notes directory.

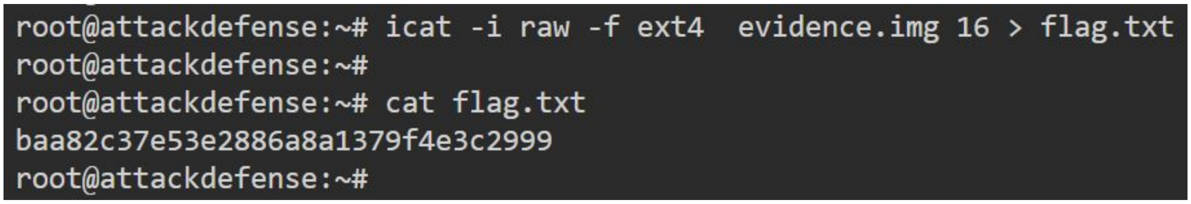
Command: fls -i raw -f ext4 evidence.img 12

Q6. Retrieve the flag kept inside the flag.txt file.

Solution:

Step 1: Extract the file flag.txt from the disk image file.

Command: icat -i raw -f ext4 evidence.img 16 > flag.txt



```
root@attackdefense:~# icat -i raw -f ext4  evidence.img 16 > flag.txt
root@attackdefense:~#
root@attackdefense:~# cat flag.txt
baa82c37e53e2886a8a1379f4e3c2999
root@attackdefense:~#
```

Flag: baa82c37e53e2886a8a1379f4e3c2999

References:

1. The Sleuth Kit (https://github.com/sleuthkit/sleuthkit)