ATTACK DEFENSE

by PentesterAcademy

Name	Image Acquisition (EWF Tools)
URL	https://www.attackdefense.com/challengedetails?cid=1797
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 acquisition involves making a copy (or several copies) of the seized hard disk which can be then used to forensics analysis. This allows the investigators to analyze this image while ensuring the integrity and present condition of the real evidence disk.

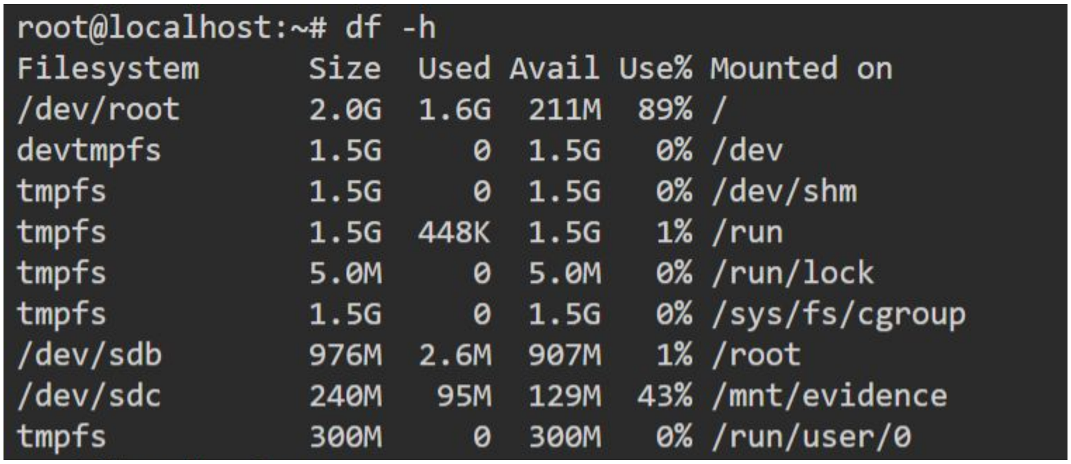
In this lab, the evidence hard disk is mounted on '/dev/sdc'. The ewf-tools are installed on the lab machine. The tool uses Expert Witness Compression Format (EWF).

Objective: Create a disk image for evidence hard disk using ewf-tools tools.

Solution:

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

Command: df -h

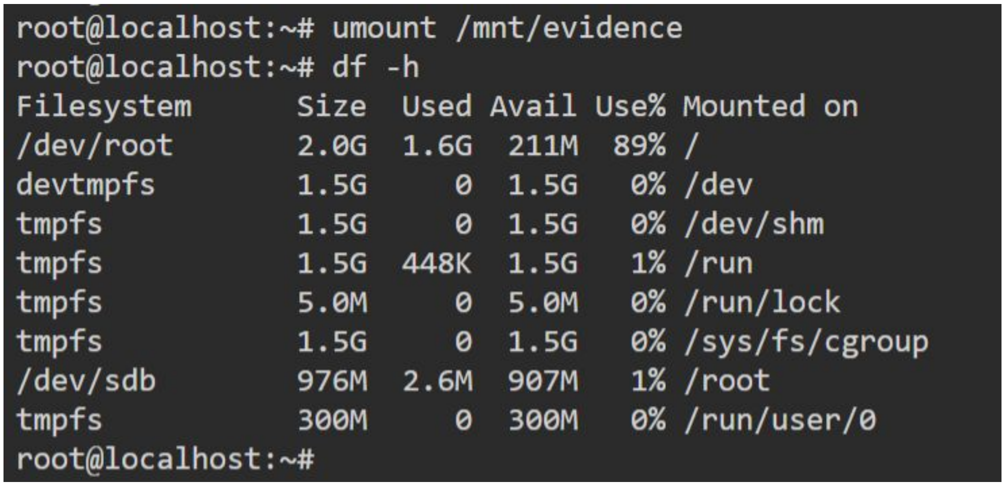


```
root@localhost:~# df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/root       2.0G  1.6G  211M  89% /
devtmpfs        1.5G     0  1.5G   0% /dev
tmpfs           1.5G     0  1.5G   0% /dev/shm
tmpfs           1.5G  448K  1.5G   1% /run
tmpfs           5.0M     0  5.0M   0% /run/lock
tmpfs           1.5G     0  1.5G   0% /sys/fs/cgroup
/dev/sdb        976M  2.6M  907M   1% /root
/dev/sdc        240M   95M  129M  43% /mnt/evidence
tmpfs           300M     0  300M   0% /run/user/0
```

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

Step 2: It is recommended to unmount the disk for preventing any failures during disk imaging. Unmount and verify that the disk is unmounted.

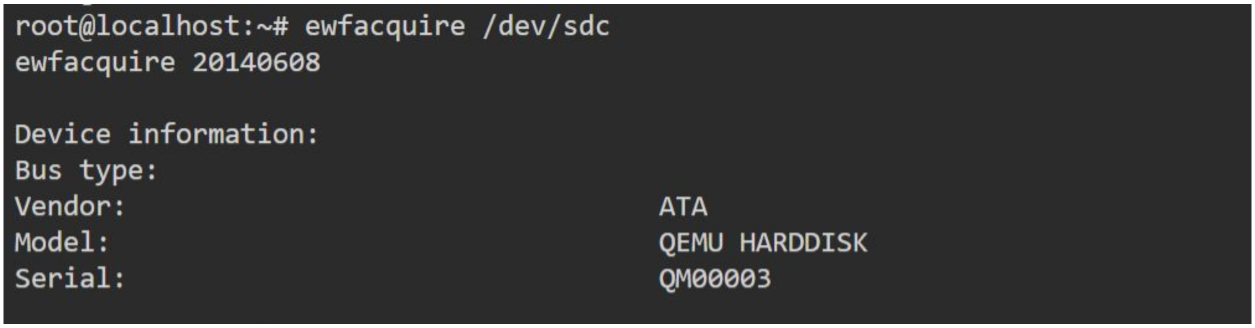
Commands:
umount /mnt/evidence
df -h



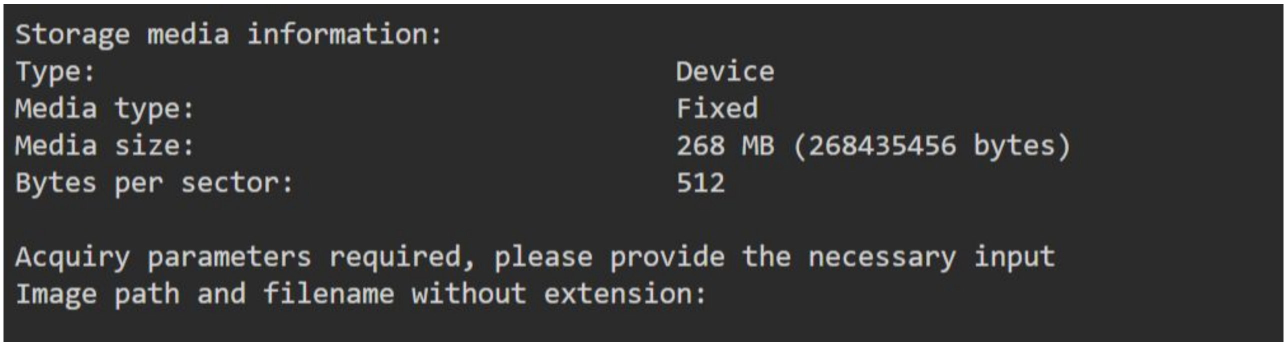
```
root@localhost:~# umount /mnt/evidence
root@localhost:~# df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/root       2.0G  1.6G  211M  89% /
devtmpfs        1.5G     0  1.5G   0% /dev
tmpfs           1.5G     0  1.5G   0% /dev/shm
tmpfs           1.5G  448K  1.5G   1% /run
tmpfs           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
tmpfs           300M     0  300M   0% /run/user/0
root@localhost:~#
```

Step 3: Use ewfacquire utility to create a disk image. Pass the full path of the evidence drive as an argument.

Command: ewfacquire /dev/sdc



```
root@localhost:~# ewfacquire /dev/sdc
ewfacquire 20140608

Device information:
Bus type:
Vendor:                                 ATA
Model:                                  QEMU HARDDISK
Serial:                                 QM00003
```

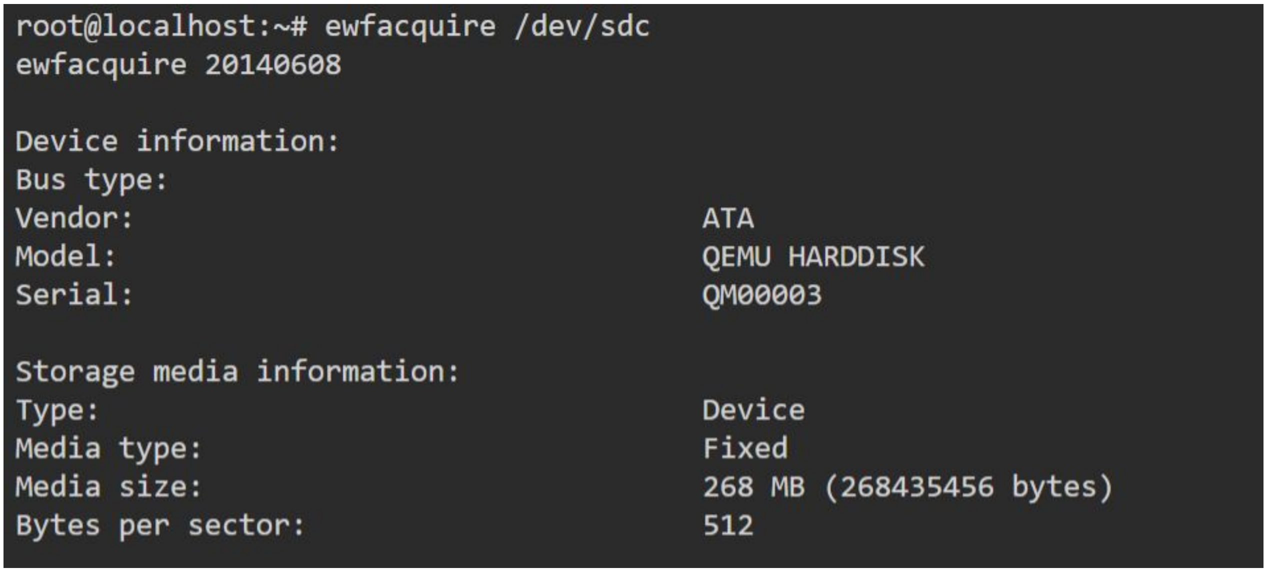


```
Storage media information:
Type:                                   Device
Media type:                             Fixed
Media size:                             268 MB (268435456 bytes)
Bytes per sector:                       512

Acquiry parameters required, please provide the necessary input
Image path and filename without extension:
```

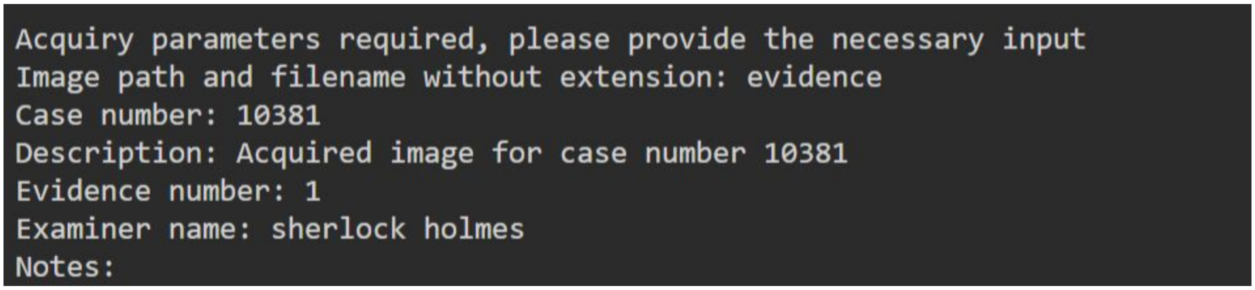
Step 4: Enter the name of the output image (without extensions) and fill the required details.

For Example:

Name: evidence
Case number: 10381
Description: Acquired image for case number 10381
Evidence number: 1
Examiner Name: sherlock holmes



```
root@localhost:~# ewfacquire /dev/sdc
ewfacquire 20140608

Device information:
Bus type:
Vendor:                                 ATA
Model:                                  QEMU HARDDISK
Serial:                                 QM00003

Storage media information:
Type:                                   Device
Media type:                             Fixed
Media size:                             268 MB (268435456 bytes)
Bytes per sector:                       512
```

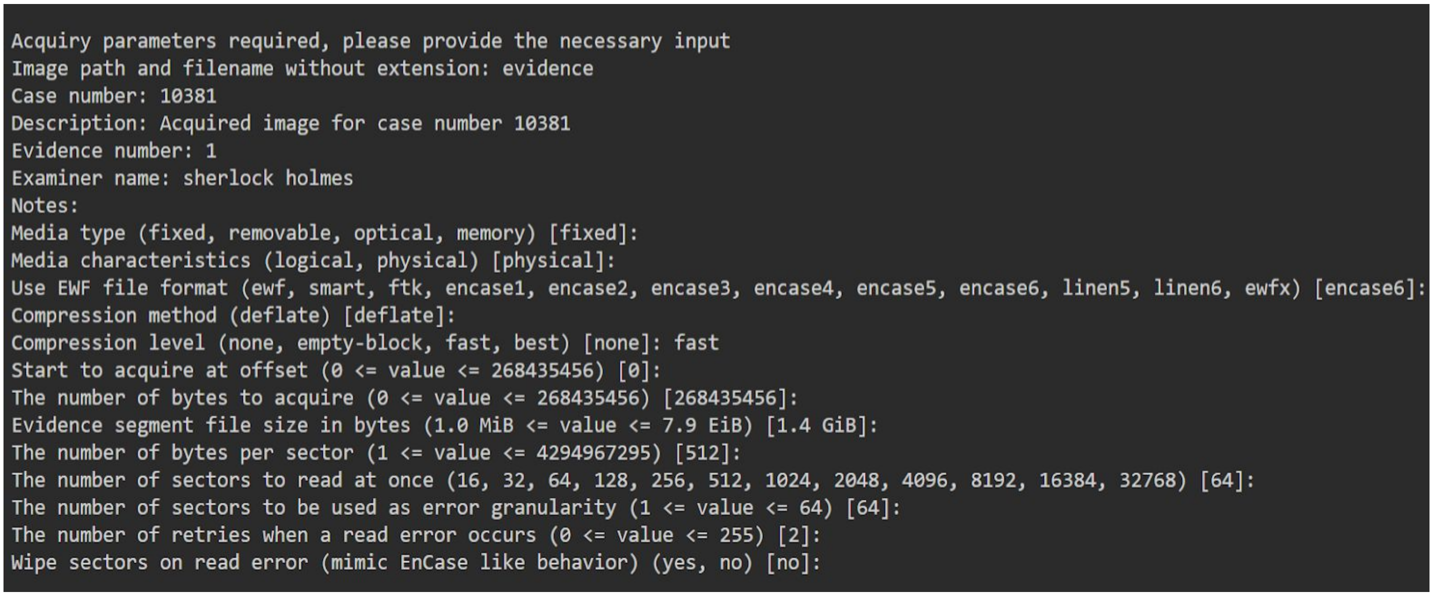


```
Acquiry parameters required, please provide the necessary input
Image path and filename without extension: evidence
Case number: 10381
Description: Acquired image for case number 10381
Evidence number: 1
Examiner name: sherlock holmes
Notes:
```

Step 5: Fill the technical details

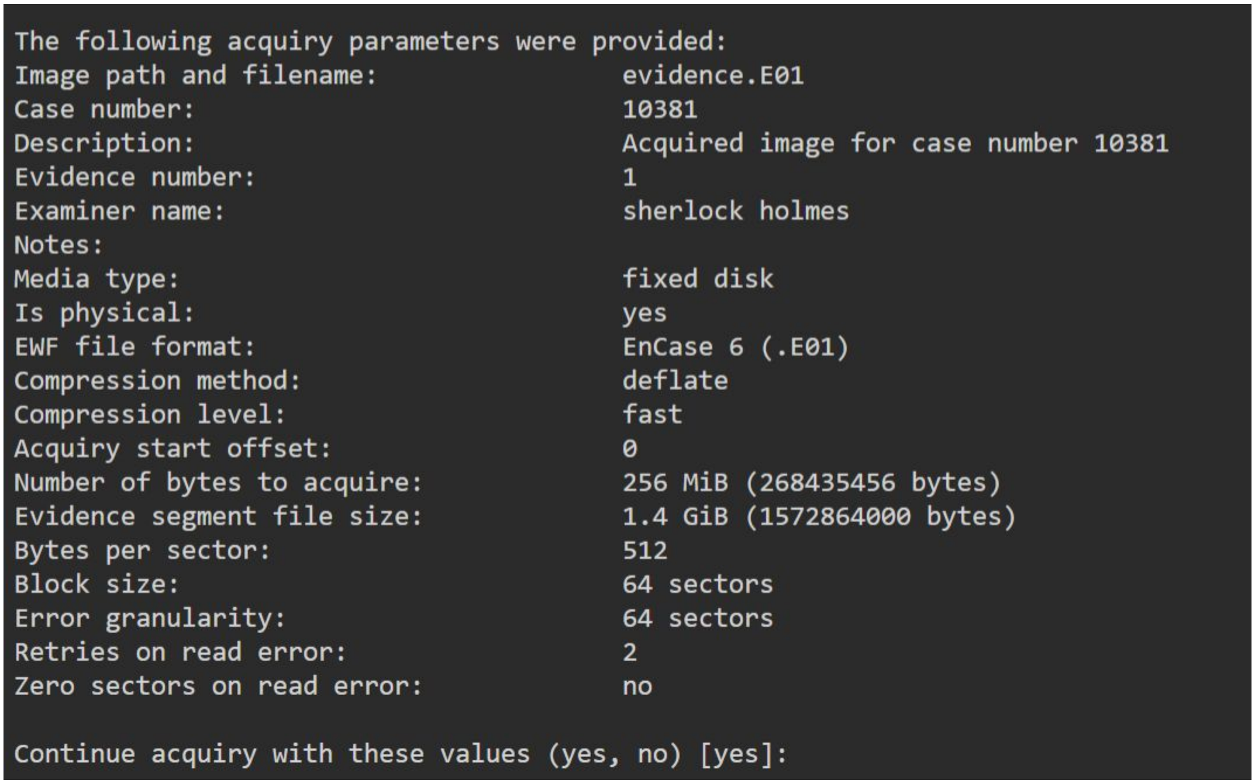
For Example:

- **Media type:** fixed
- **Media characteristics:** physical
- **File format:** encase6
- **Compression method:** deflate
- **Compression level:** fast



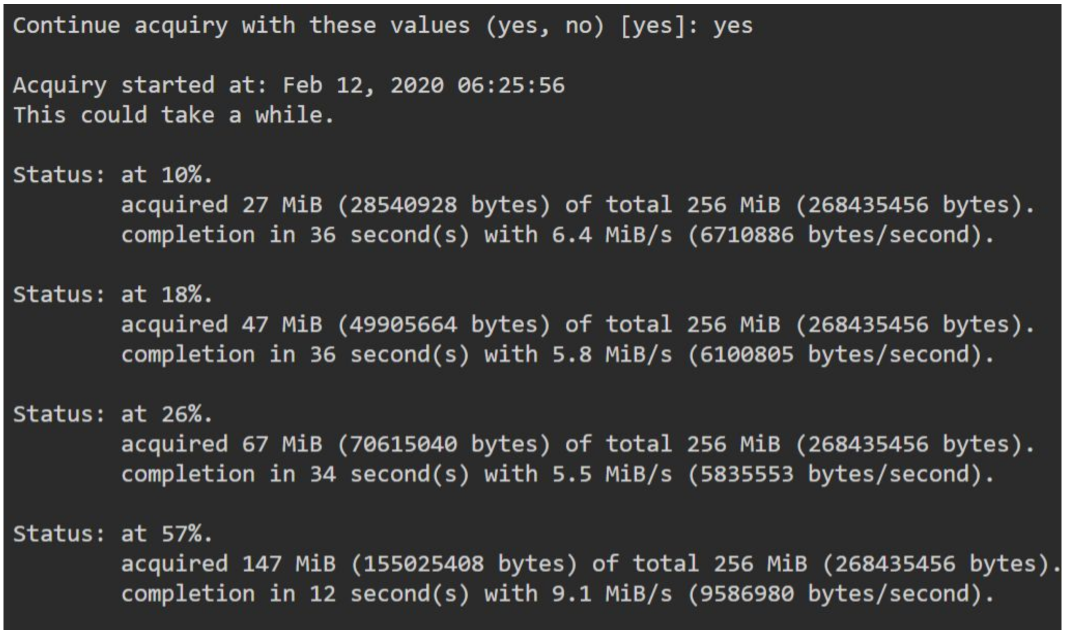
```
Acquiry parameters required, please provide the necessary input
Image path and filename without extension: evidence
Case number: 10381
Description: Acquired image for case number 10381
Evidence number: 1
Examiner name: sherlock holmes
Notes:
Media type (fixed, removable, optical, memory) [fixed]:
Media characteristics (logical, physical) [physical]:
Use EWF file format (ewf, smart, ftk, encase1, encase2, encase3, encase4, encase5, encase6, linen5, linen6, ewfx) [encase6]:
Compression method (deflate) [deflate]:
Compression level (none, empty-block, fast, best) [none]: fast
Start to acquire at offset (0 <= value <= 268435456) [0]:
The number of bytes to acquire (0 <= value <= 268435456) [268435456]:
Evidence segment file size in bytes (1.0 MiB <= value <= 7.9 EiB) [1.4 GiB]:
The number of bytes per sector (1 <= value <= 4294967295) [512]:
The number of sectors to read at once (16, 32, 64, 128, 256, 512, 1024, 2048, 4096, 8192, 16384, 32768) [64]:
The number of sectors to be used as error granularity (1 <= value <= 64) [64]:
The number of retries when a read error occurs (0 <= value <= 255) [2]:
Wipe sectors on read error (mimic EnCase like behavior) (yes, no) [no]:
```

Note: Keep default values for the rest of the options.

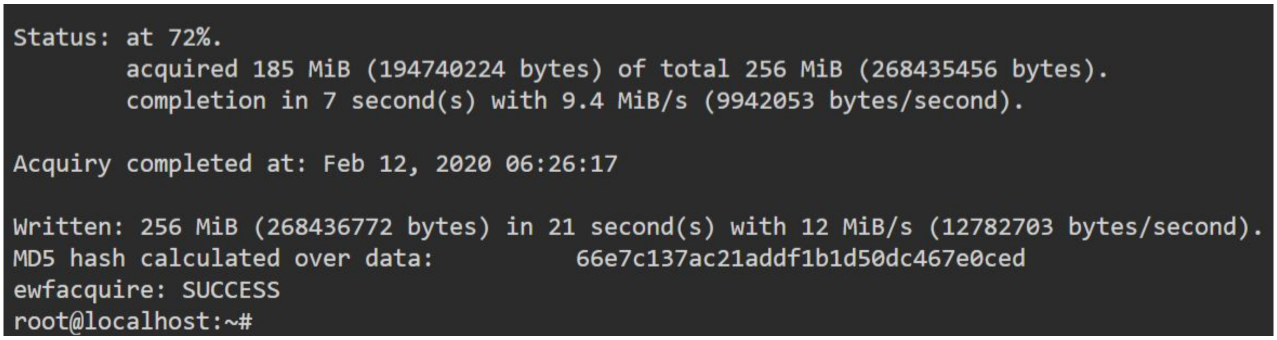


```
The following acquiry parameters were provided:
Image path and filename:                evidence.E01
Case number:                            10381
Description:                            Acquired image for case number 10381
Evidence number:                        1
Examiner name:                          sherlock holmes
Notes:
Media type:                             fixed disk
Is physical:                            yes
EWF file format:                        EnCase 6 (.E01)
Compression method:                     deflate
Compression level:                      fast
Acquiry start offset:                   0
Number of bytes to acquire:             256 MiB (268435456 bytes)
Evidence segment file size:             1.4 GiB (1572864000 bytes)
Bytes per sector:                       512
Block size:                             64 sectors
Error granularity:                      64 sectors
Retries on read error:                  2
Zero sectors on read error:             no

Continue acquiry with these values (yes, no) [yes]:
```

Step 6: Enter ‘yes’ for saving the information entered before.



```
Continue acquiry with these values (yes, no) [yes]: yes

Acquiry started at: Feb 12, 2020 06:25:56
This could take a while.

Status: at 10%.
        acquired 27 MiB (28540928 bytes) of total 256 MiB (268435456 bytes).
        completion in 36 second(s) with 6.4 MiB/s (6710886 bytes/second).

Status: at 18%.
        acquired 47 MiB (49905664 bytes) of total 256 MiB (268435456 bytes).
        completion in 36 second(s) with 5.8 MiB/s (6100805 bytes/second).

Status: at 26%.
        acquired 67 MiB (70615040 bytes) of total 256 MiB (268435456 bytes).
        completion in 34 second(s) with 5.5 MiB/s (5835553 bytes/second).

Status: at 57%.
        acquired 147 MiB (155025408 bytes) of total 256 MiB (268435456 bytes).
        completion in 12 second(s) with 9.1 MiB/s (9586980 bytes/second).
```

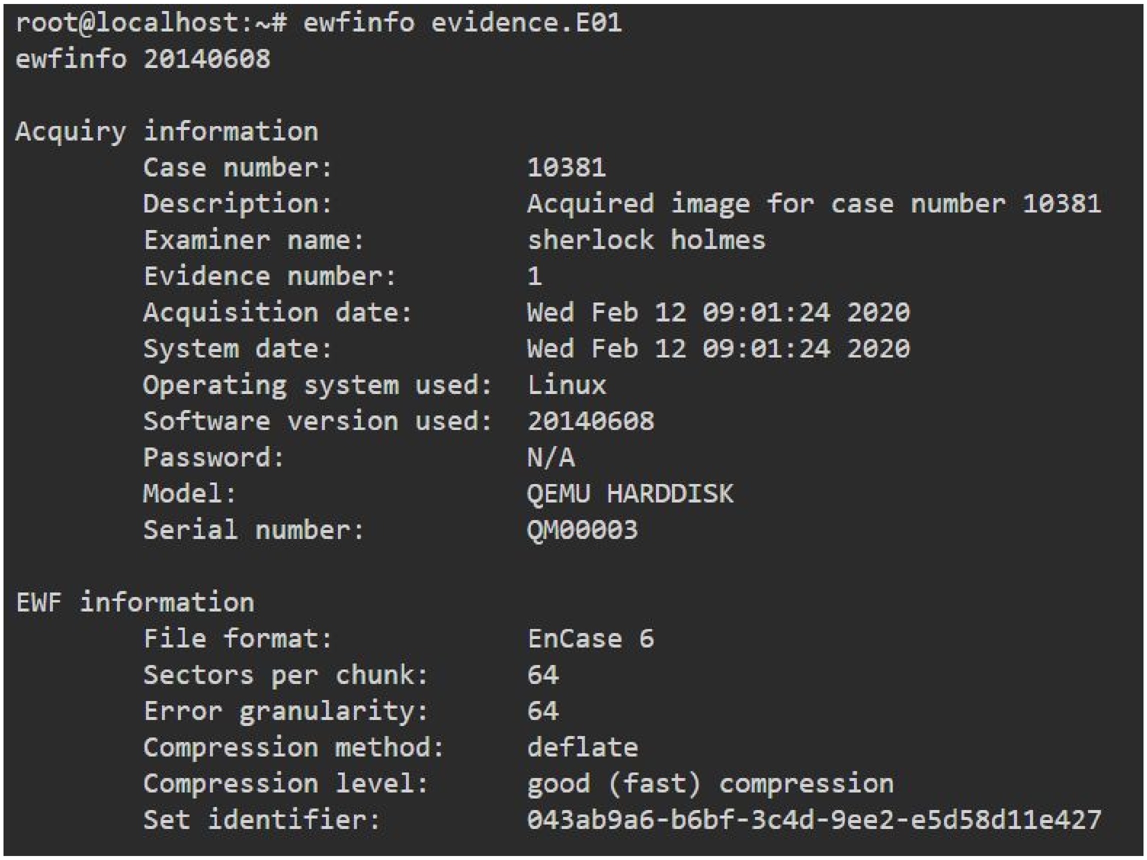


```
Status: at 72%.
        acquired 185 MiB (194740224 bytes) of total 256 MiB (268435456 bytes).
        completion in 7 second(s) with 9.4 MiB/s (9942053 bytes/second).

Acquiry completed at: Feb 12, 2020 06:26:17

Written: 256 MiB (268436772 bytes) in 21 second(s) with 12 MiB/s (12782703 bytes/second).
MD5 hash calculated over data:          66e7c137ac21addf1b1d50dc467e0ced
ewfacquire: SUCCESS
root@localhost:~#
```

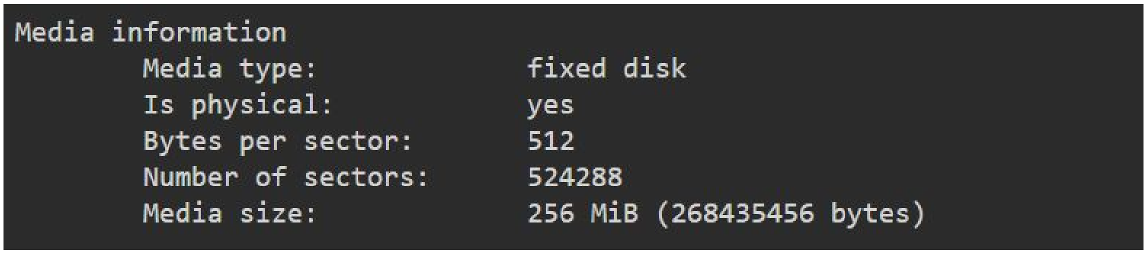
The image named ‘evidence.E01’ is created successfully.

Step 7: Verify the information entered for the evidence disk image.

Command: ewfinfo evidence.E01



```
root@localhost:~# ewfinfo evidence.E01
ewfinfo 20140608

Acquiry information
        Case number:            10381
        Description:            Acquired image for case number 10381
        Examiner name:          sherlock holmes
        Evidence number:        1
        Acquisition date:       Wed Feb 12 09:01:24 2020
        System date:            Wed Feb 12 09:01:24 2020
        Operating system used:  Linux
        Software version used:  20140608
        Password:               N/A
        Model:                  QEMU HARDDISK
        Serial number:          QM00003

EWF information
        File format:            EnCase 6
        Sectors per chunk:      64
        Error granularity:      64
        Compression method:     deflate
        Compression level:      good (fast) compression
        Set identifier:         043ab9a6-b6bf-3c4d-9ee2-e5d58d11e427
```



```
Media information
        Media type:             fixed disk
        Is physical:            yes
        Bytes per sector:       512
        Number of sectors:      524288
        Media size:             256 MiB (268435456 bytes)
```

The information regarding the evidence disk image can be verified.

References:

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