

LinkedIn: [Kelvin Kimotho](#)

Sleuthkit Intro



Medium

Forensics

picoCTF 2022

sleuthkit

AUTHOR: LT 'SYREAL' JONES

Description

Download the disk image and use `mmfs` on it to find the size of the Linux partition. Connect to the remote checker service to check your answer and get the flag.

Note: if you are using the webshell, download and extract the disk image into `/tmp` not your home directory.

[Download disk image](#)

Access checker program: `nc saturn.picoctf.net 65323`

This challenge launches an instance on demand.

Its current status is:

RUNNING

Instance Time Remaining:

9:09

Restart
Instance

Hints ?

(None)

Solution

I downloaded the disk image using `wget` tool.

```
kali@kali: ~/Desktop
File Actions Edit View Help

(kali@kali)-[~/Desktop]
$ wget https://artifacts.picoctf.net/c/164/disk.img.gz
--2025-02-09 14:00:24-- https://artifacts.picoctf.net/c/164/disk.img.gz
Resolving artifacts.picoctf.net (artifacts.picoctf.net) ... 52.84.102.85, 2600:9000:2054:8200:16:5ec5:2840:93a1
Connecting to artifacts.picoctf.net (artifacts.picoctf.net)|52.84.102.85|:443 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 29714372 (28M) [application/octet-stream]
Saving to: 'disk.img.gz'

disk.img.gz          100%[=====] 28.34M  172KB/s  in 2m 3s
2025-02-09 14:02:29 (236 KB/s) - 'disk.img.gz' saved [29714372/29714372]

(kali@kali)-[~/Desktop]
$ ls
disk.img.gz

(kali@kali)-[~/Desktop]
$

(kali@kali)-[~/Desktop]
$
```

I then unzipped the gz compression.

```
(kali@kali)-[~/Desktop]
$ sudo gzip -d disk.img.gz

(kali@kali)-[~/Desktop]
$ ls
disk.img

(kali@kali)-[~/Desktop]
$
```

To list the partition table contents i used the **mmls** command against the disk image.

```
(kali@kali)-[~/Desktop]
$ mmls disk.img
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

Slot      Start      End      Length    Description
000:  Meta      0000000000 0000000000 0000000001 Primary Table (#0)
001:          0000000000 0000002047 0000002048 Unallocated
002:  000:000  0000002048 0000204799 0000202752 Linux (0x83)
```

I then Connected to the server at port given using netcat. This question was asked ” **What is the size of the Linux partition in the given disk image?**”.

```
(kali@kali)-[~/Desktop]
$

(kali@kali)-[~/Desktop]
$ nc saturn.picoctf.net 65323
What is the size of the Linux partition in the given disk image?
Length in sectors: 
```

And the answer to the question was ” **202752**”.

```
(kali@kali)-[~/Desktop]
$ mmls disk.img
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

    Slot      Start      End      Length    Description
000:  Meta      0000000000  0000000000  0000000001  Primary Table (#0) as
001:  _____  0000000000  0000002047  0000002048  Unallocated
002:  000:000    0000002048  0000204799  0000202752  Linux (0x83)
```

I provided the answer which was the size of the linux portion and the flag was returned by the program i connected to via netcat ” **picoCTF{mm15_f7w!}**”.

```
(kali@kali)-[~/Desktop]
$ nc saturn.picoctf.net 65323
What is the size of the Linux partition in the given disk image?
Length in sectors: 202752
Great work!
picoCTF{mm15_f7w!}

(kali@kali)-[~/Desktop]
$
```