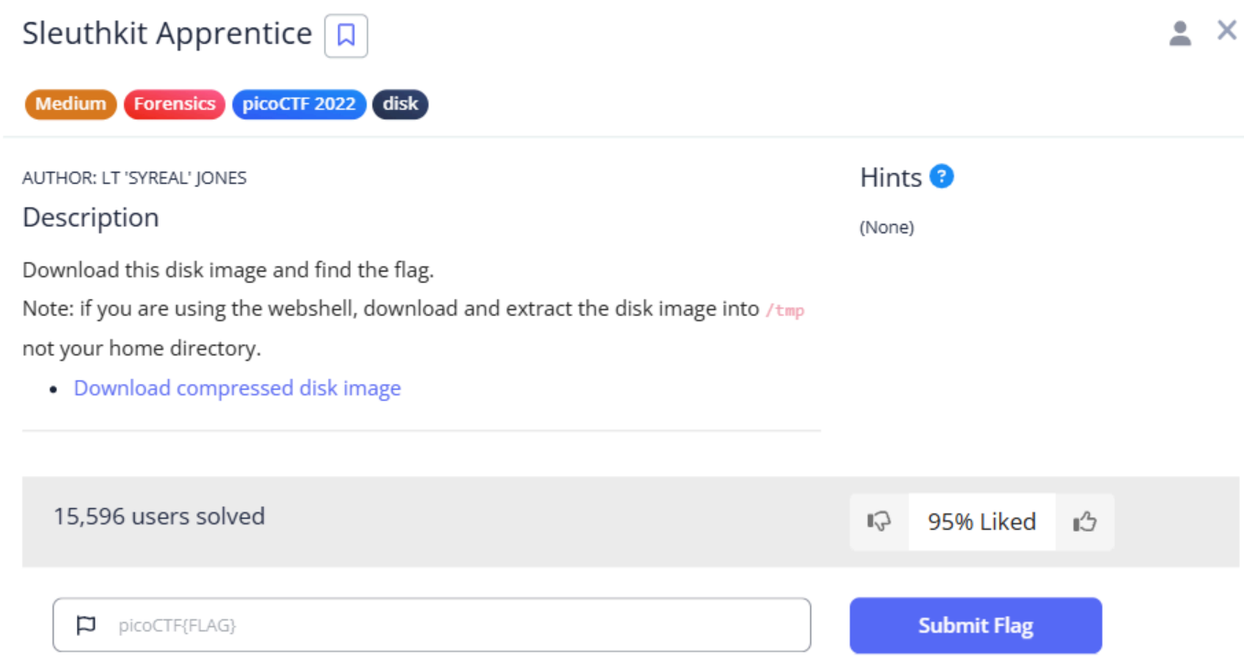
Sleuthkit Apprentice



Attached File: `disk.flag.img.gz`

Step 1 – Unpack the Disk Image

First, decompress the image.

```
gunzip disk.flag.img.gz
```

This leaves you with:

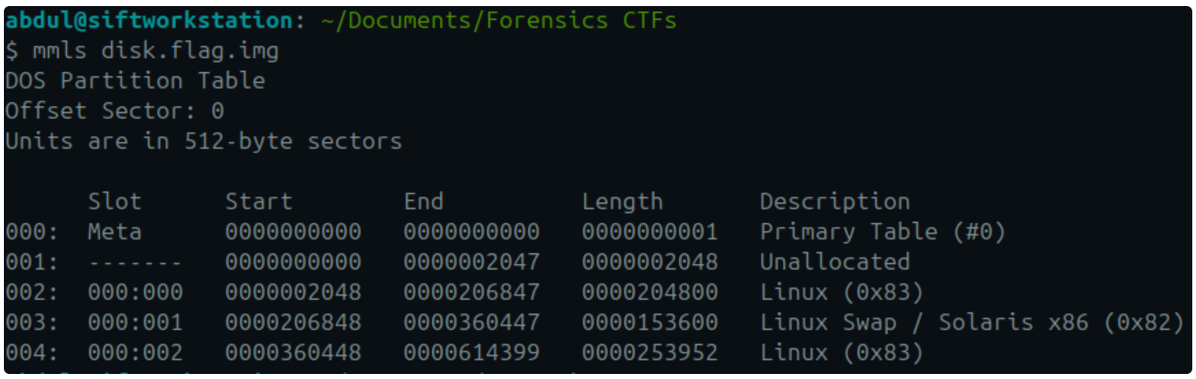
```
disk.flag.img
```

Step 2 – Inspect the Partition Table

Use `mmls` (Sleuth Kit) to view the disk layout:

```
mmls disk.flag.img
```

Output:



Step 3 – Mount Partition #002

Calculate offset

Each sector = 512 bytes

Start sector = 2048

```
2048 * 512 = 1048576
```

Mount

```
mkdir flagsearch
```

This creates a directory where we can mount our partitions cleanly…

```
sudo mount -o loop,offset=1048576 disk.flag.img flagsearch/
ls flagsearch/
```

Peeking into the partition, it mostly contained boot files and kernel assets — `vmlinuz`, `ldlinux.c32`, `System.map`, etc.

Tried `grep` to check for any flags:

```
grep -ri pico flagsearch/
```

All results were from kernel references like `pico_lcd`. No user files or signs of a flag. Time to unmount and try Slot 004.

Step 4 – Mount Partition #004

Offset calculation:

I decided to go for slot 04 next using the same process…

```
360448 * 512 = 184549376
```

Mount it:

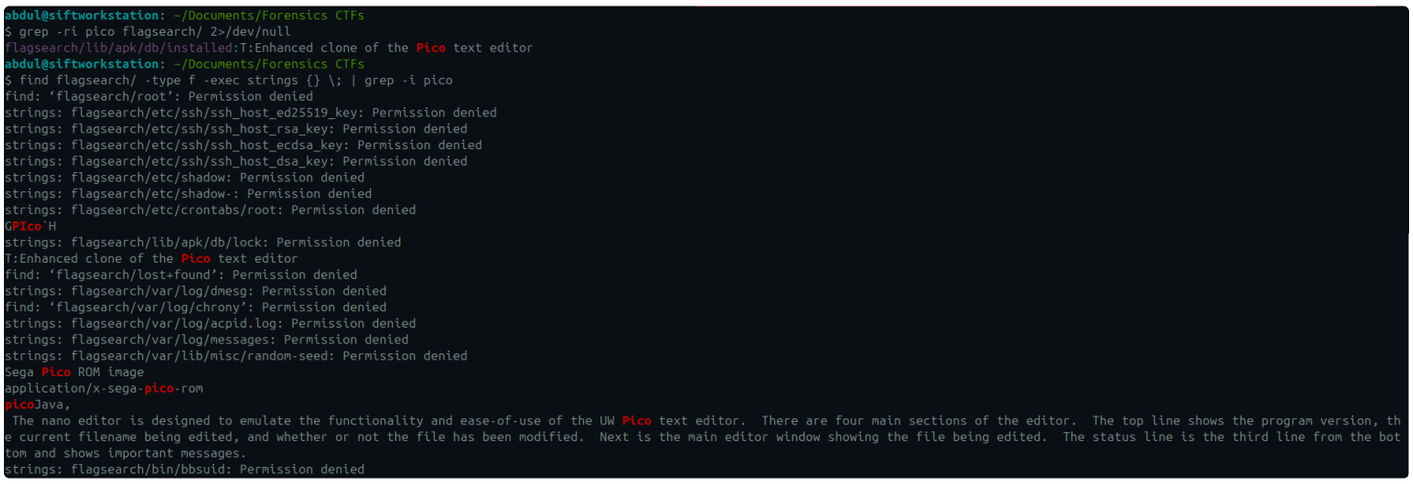
```
sudo umount flagsearch/
sudo mount -o loop,offset=184549376 disk.flag.img flagsearch/
ls flagsearch/
```

This time, it looked like a real Linux system: `bin`, `etc`, `home`, `root`, `var`, etc.

Step 5 – Search for the Flag

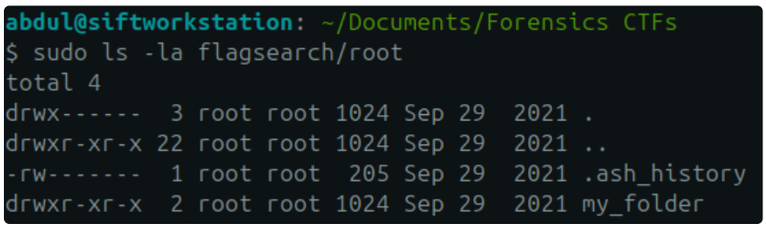
A basic grep attempt didn't return anything useful:

```
sudo grep -ri pico flagsearch/ 2>/dev/null
```



Moved directly to checking the `/root` directory, which was previously inaccessible due to permissions:

```
sudo ls -la flagsearch/root
```



Found:

```
my_folder/
```

Checked inside:

```
sudo ls flagsearch/root/my_folder
```

Found the file:

```
flag.uni.txt
```

Read it with:

```
sudo cat flagsearch/root/my_folder/flag.uni.txt
```

Flag

```
abdul@siftworkstation: ~/Documents/Forensics CTFs
$ sudo cat flagsearch/root/my_folder/flag.uni.txt
picoCTF{by73_5urf3r_adac6cb4}
```

```
picoCTF{by73_5urf3r_adac6cb4}
```

Sleuthkit Apprentice

Medium Forensics picoCTF 2022 disk

AUTHOR: LT 'SYREAL' JONES

Description

Download this disk image and find the flag.

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

- Download compressed disk image

Hints

(None)

15,597 users solved

95% Liked

picoCTF{FLAG}

Submit Flag