

# Sleuthkit Apprentice

Sleuthkit Apprentice

MediumForensicspicoCTF 2022disk

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)

15,596 users solved

95% Liked

picoCTF{FLAG}

Submit Flag

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:

```
abdul@siftworkstation: ~/Documents/Forensics CTFs
$ mmls disk.flag.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  0000206847  0000204800  Linux (0x83)
003:  000:001  0000206848  0000360447  0000153600  Linux Swap / Solaris x86 (0x82)
004:  000:002  0000360448  0000614399  0000253952  Linux (0x83)
```

## 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
```

```
abdul@siftworkstation: ~/Documents/Forensics CTFs
$ grep -ri pico flagsearch/ 2>/dev/null
flagsearch/lib/apk/db/installed:T:Enhanced clone of the Pico text editor
abdul@siftworkstation: ~/Documents/Forensics CTFs
$ find flagsearch/ -type f -exec strings {} \; | grep -i pico
find: 'flagsearch/root': Permission denied
strings: flagsearch/etc/ssh/ssh_host_ed25519_key: Permission denied
strings: flagsearch/etc/ssh/ssh_host_rsa_key: Permission denied
strings: flagsearch/etc/ssh/ssh_host_ecdsa_key: Permission denied
strings: flagsearch/etc/ssh/ssh_host_dsa_key: Permission denied
strings: flagsearch/etc/shadow: Permission denied
strings: flagsearch/etc/shadow-: Permission denied
strings: flagsearch/etc/crontabs/root: Permission denied
CPico^H
strings: flagsearch/lib/apk/db/lock: Permission denied
T:Enhanced clone of the Pico text editor
find: 'flagsearch/lost+found': Permission denied
strings: flagsearch/var/log/dmesg: Permission denied
find: 'flagsearch/var/log/chrony': Permission denied
strings: flagsearch/var/log/acpid.log: Permission denied
strings: flagsearch/var/log/messages: Permission denied
strings: flagsearch/var/lib/misc/random-seed: Permission denied
Sega Pico ROM image
application/x-sega-pico-rom
picoJava,
The nano editor is designed to emulate the functionality and ease-of-use of the UW Pico text editor. There are four main sections of the editor. The top line shows the program version, the current filename being edited, and whether or not the file has been modified. Next is the main editor window showing the file being edited. The status line is the third line from the bottom and shows important messages.
strings: flagsearch/bin/bbsuid: Permission denied
```

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

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

```
abdul@siftworkstation: ~/Documents/Forensics CTFs
$ sudo ls -la flagsearch/root
total 4
drwx----- 3 root root 1024 Sep 29 2021 .
drwxr-xr-x 22 root root 1024 Sep 29 2021 ..
-rw----- 1 root root 205 Sep 29 2021 .ash_history
drwxr-xr-x 2 root root 1024 Sep 29 2021 my_folder
```

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