

gunzip disk.flag.img.gz

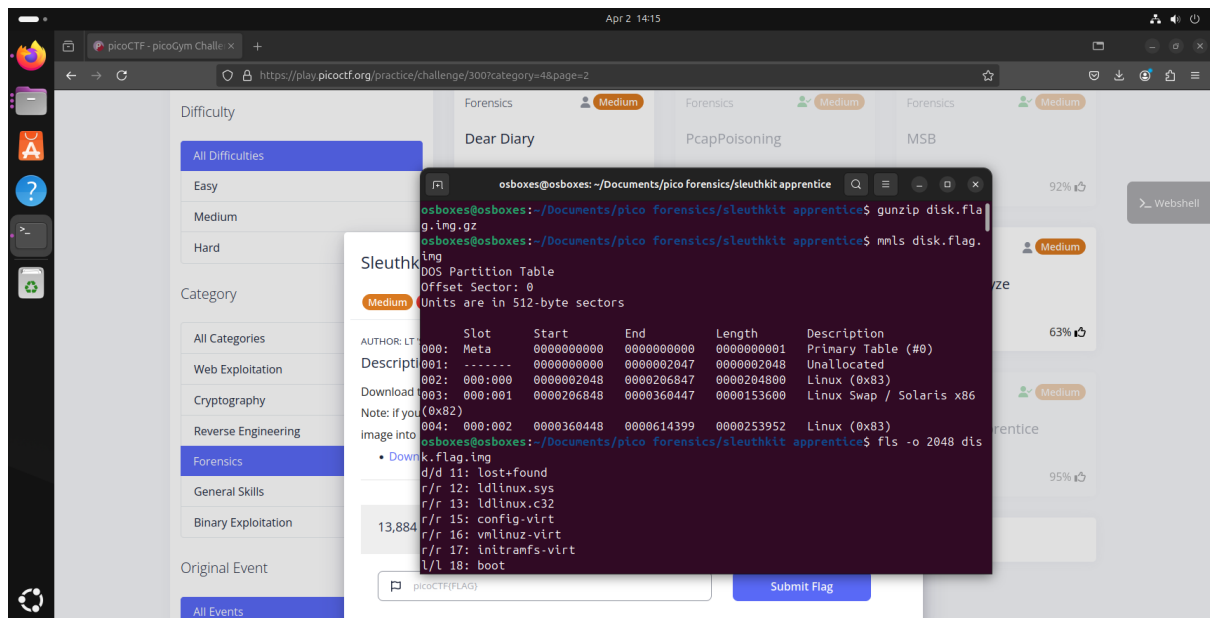
mmls disk.flag.img

DOS Partition Table

Offset Sector: 0

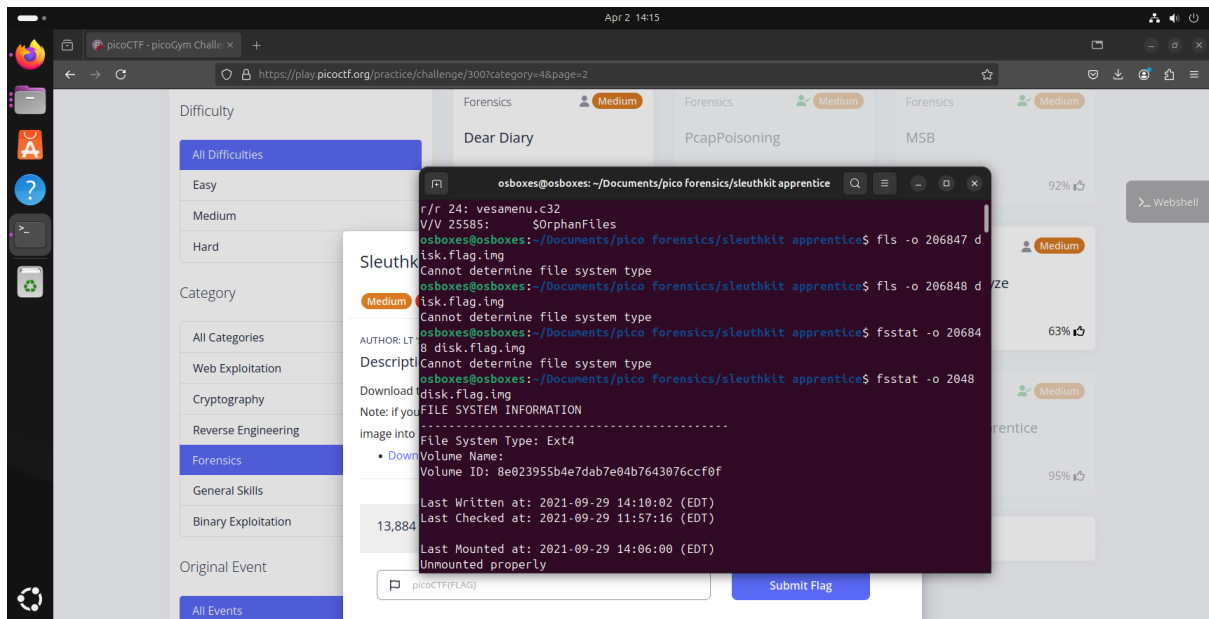
Units are in 512-byte sectors

	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)



fls -o 206847 disk.flag.img

Cannot determine file system type



fsstat -o 2048 disk.flag.img

FILE SYSTEM INFORMATION

File System Type: Ext4

Volume Name:

Volume ID: 8e023955b4e7dab7e04b7643076ccf0f

Last Written at: 2021-09-29 14:10:02 (EDT)

Last Checked at: 2021-09-29 11:57:16 (EDT)

Last Mounted at: 2021-09-29 14:06:00 (EDT)

Unmounted properly

fls -i raw -f ext4 -o 360448 -r disk.flag.img

d/d 451: home

d/d 11: lost+found

d/d 12: boot

d/d 1985: etc

+ r/r 23: group

+ r/r 24: group-

+ r/r 25: shadow

+ r/r 26: shadow-

```

+ r/r 27:   passwd

+ r/r 28:   passwd-

+ r/r 29:   hosts

+ d/d 30:   zoneinfo

++ r/r 31:  UTC

+ r/r * 32(realloc):  resolv.conf

+ d/d 33:   keymap

++ r/r 34:  us.bmap.gz

+ r/r 35:   inittab

+ d/d 36:   conf.d

++ r/r * 493(realloc):  .apk.e0f21bd25c6c70139df2cde7bf1a36d489c455ae1ded76d7

++ r/r * 494(realloc):  .apk.0864ab1550d7450acef161ac8801ce25e921c2a9d91a6862

++ r/r * 495(realloc):  .apk.4a7da402791126ef582f6f6615a3ab47cac81b903da9fafc

++ r/r * 496(realloc):  .apk.c9958cbaf43ea23cd909f245cdcbdbcf30ee548c1700f691

++ r/r * 497(realloc):  .apk.30eead8aa0227aae5fb84d0facfa2631616ea5aa2533f106

++ r/r * 498(realloc):  .apk.d6591ddc80d9477092aefa23a5203e231dd24cfd514397f6

++ r/r * 499(realloc):  .apk.a63c0b8e2d2265b663b8

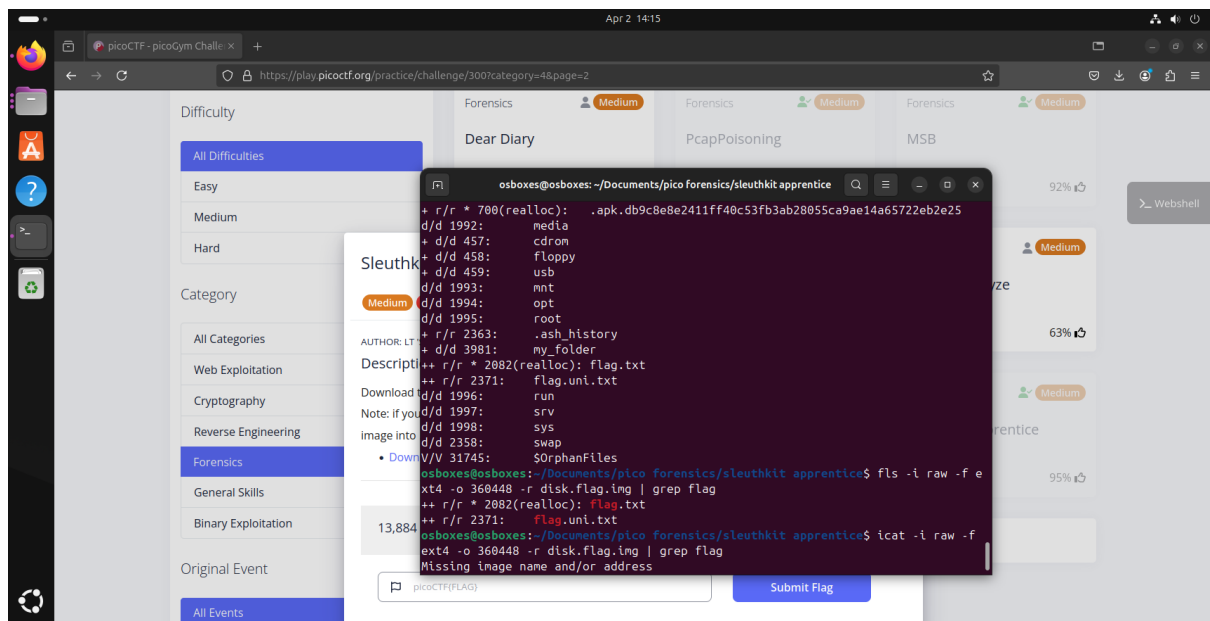
```

A lot of dummy data

fls -i raw -f ext4 -o 360448 -r disk.flag.img | grep flag

```
++ r/r * 2082(realloc):  flag.txt
```

```
++ r/r 2371: flag.uni.txt
```



icat -i raw -f ext4 -o 360448 -r disk.flag.img 2371

picoCTF{by73_surf3r_2f22df38}

-r recursive -f file system -l image type

The screenshot shows a web browser window displaying the PicoCTF challenge page. The URL is <https://play.picoctf.org/practice/challenge/300?category=4&page=2>. The page features a sidebar with filters for Difficulty (All Difficulties, Easy, Medium, Hard) and Category (All Categories, Web Exploitation, Cryptography, Reverse Engineering, Forensics, General Skills, Binary Exploitation). The main content area shows a list of challenges, including 'Dear Diary' (Forensics, Medium) and 'PcapPoisoning' (Forensics, Medium). A terminal window is overlaid on the page, showing the command `icat [-hrRsvV] [-f fstype] [-i imgtype] [-b dev_sector_size] [-o ingoffse] image [images] inum[-typ[-id]]` and its output. The terminal also shows the command `icat -i raw -f ext4 -o 360448 -r disk.flag.img 2082 3.449677 13.056403` and the output `13,884`. A 'Submit Flag' button is visible at the bottom right of the terminal window.

Difficulty

- All Difficulties
- Easy
- Medium
- Hard

Category

- All Categories
- Web Exploitation
- Cryptography
- Reverse Engineering
- Forensics
- General Skills
- Binary Exploitation

Original Event

- All Events

Forensics Medium

Dear Diary

Forensics Medium

PcapPoisoning

Forensics Medium

MSB

92%

63%

95%

Webshell

osboxes@osboxes: ~/Documents/pico forensics/sleuthkit apprentice

usage: icat [-hrRsvV] [-f fstype] [-i imgtype] [-b dev_sector_size] [-o ingoffse] image [images] inum[-typ[-id]]

- h: Do not display holes in sparse files
- r: Recover deleted file
- R: Recover deleted file and suppress recovery errors
- s: Display slack space at end of file
- i imgtype: The format of the image file (use '-i list' for supported types)
- b dev_sector_size: The size (in bytes) of the device sectors
- f fstype: File system type (use '-f list' for supported types)
- o ingoffset: The offset of the file system in the image (in sectors)
- P pooltype: Pool container type (use '-P list' for supported types)
- B pool_volume_block: Starting block (for pool volumes only)
- S snap_id: Snapshot ID (for APFS only)
- v: verbose to stderr
- V: Print version
- k password: Decryption password for encrypted volumes

osboxes@osboxes:~/Documents/pico forensics/sleuthkit apprentice\$ icat -i raw -f ext4 -o 360448 -r disk.flag.img 2082 3.449677 13.056403

osboxes@osboxes:~/Documents/pico forensics/sleuthkit apprentice\$ icat -i raw -f ext4 -o 360448 -r disk.flag.img 2371

picoCTF{by73_Surf3r_2f22df38}

osboxes@osboxes:~/Documents/pico forensics/sleuthkit apprentice\$

picoCTF{FLAG}

Submit Flag