

Disko 2

- Here, the dd file actually contains some string that we can locate with "strings"
- There are multiple files, so we get the correct offset, and take the first occurrence in the Linux Partition...

```
Kali Linux [En fonction] - Oracle VM VirtualBox
Fichier Machine Écran Entrée Périphériques Aide

capscorpion142@asaad: ~/Desktop/Autoformation/CTFs/PicoCTF/Disko 2

File Actions Edit View Help

(capscorpion142@asaad)~[~/Desktop/Autoformation/CTFs/PicoCTF/Disko 2]
$ mmls disko-2.dd

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:  Unalloc    0000000000  0000002047  0000002048  Unallocated
002:  000:000    0000002048  0000053247  0000051200  Linux (0x83)
003:  000:001    0000053248  0000118783  0000065536  Win95 FAT32 (0x0b)
004:  Unalloc    0000118784  0000204799  0000086016  Unallocated

(capscorpion142@asaad)~[~/Desktop/Autoformation/CTFs/PicoCTF/Disko 2]
$ dd if=disko-2.dd of=linux_part.dd bs=512 skip=2048 count=51200 status=progress

51200+0 records in
51200+0 records out
26214400 bytes (26 MB, 25 MiB) copied, 0.751689 s, 34.9 MB/s

(capscorpion142@asaad)~[~/Desktop/Autoformation/CTFs/PicoCTF/Disko 2]
$ file linux_part.dd

linux_part.dd: Linux rev 1.0 ext4 filesystem data, UUID=9e5121c2-9728-4271-a07c-d74aabdc093b (extents) (64bit) (large files) (huge files)

(capscorpion142@asaad)~[~/Desktop/Autoformation/CTFs/PicoCTF/Disko 2]
$ mkdir mnt
$ sudo mount -o loop linux_part.dd mnt

[sudo] password for capscorpion142:
(capscorpion142@asaad)~[~/Desktop/Autoformation/CTFs/PicoCTF/Disko 2]
$ ls mnt
bin  lost+found
```

```
Kali Linux [En fonction] - Oracle VM VirtualBox
Fichier Machine Écran Entrée Périphériques Aide

capscorpion142@asaad: ~/Desktop/Autoformation/CTFs/PicoCTF/Disko 2

File Actions Edit View Help

(capscorpion142@asaad)~[~/Desktop/Autoformation/CTFs/PicoCTF/Disko 2]
$ mkdir mnt
$ sudo mount -o loop linux_part.dd mnt

[sudo] password for capscorpion142:

(capscorpion142@asaad)~[~/Desktop/Autoformation/CTFs/PicoCTF/Disko 2]
$ ls mnt
bin  lost+found

(capscorpion142@asaad)~[~/Desktop/Autoformation/CTFs/PicoCTF/Disko 2]
$ grep -R picoCTF mnt
grep: mnt/bin/compare-im6: No such file or directory
grep: mnt/bin/pidof: No such file or directory
grep: mnt/bin/setmetamode: Bad message
grep: mnt/lost+found: Permission denied

(capscorpion142@asaad)~[~/Desktop/Autoformation/CTFs/PicoCTF/Disko 2]
$ ls
disko-2.dd  linux_part.dd  mnt

(capscorpion142@asaad)~[~/Desktop/Autoformation/CTFs/PicoCTF/Disko 2]
$
```

- So here we checked, the lost inode, the unallocated bytes, but we found them empty...

```

(capscorpion142@asaad: ~/Desktop/Autoformation/CTFs/PicoCTF/Disko 2)
$ icat linux_part.dd 235 | strings | grep picoCTF

(capscorpion142@asaad: ~/Desktop/Autoformation/CTFs/PicoCTF/Disko 2)
$ icat linux_part.dd 235 > orphan.bin
strings orphan.bin | grep picoCTF

(capscorpion142@asaad: ~/Desktop/Autoformation/CTFs/PicoCTF/Disko 2)
$ icat -f ext4 linux_part.dd 235

(capscorpion142@asaad: ~/Desktop/Autoformation/CTFs/PicoCTF/Disko 2)
$ icat -f ext4 linux_part.dd 235 | strings | grep picoCTF

(capscorpion142@asaad: ~/Desktop/Autoformation/CTFs/PicoCTF/Disko 2)
$ icat linux_part.dd 235 | strings | grep picoCTF

(capscorpion142@asaad: ~/Desktop/Autoformation/CTFs/PicoCTF/Disko 2)
$ icat -f ext4 linux_part.dd 235 | strings | grep picoCTF

(capscorpion142@asaad: ~/Desktop/Autoformation/CTFs/PicoCTF/Disko 2)
$ ls
disko-2.dd  linux_part.dd  mnt  orphan.bin
  
```

- Here, we checked the logs file, also empty...

```

(capscorpion142@asaad: ~/Desktop/Autoformation/CTFs/PicoCTF/Disko 2)
$ ls
disko-2.dd  linux_part.dd  mnt  orphan.bin

(capscorpion142@asaad: ~/Desktop/Autoformation/CTFs/PicoCTF/Disko 2)
$

(capscorpion142@asaad: ~/Desktop/Autoformation/CTFs/PicoCTF/Disko 2)
$

(capscorpion142@asaad: ~/Desktop/Autoformation/CTFs/PicoCTF/Disko 2)
$ blkls -f ext4 linux_part.dd > unalloc.bin

(capscorpion142@asaad: ~/Desktop/Autoformation/CTFs/PicoCTF/Disko 2)
$ strings unalloc.bin | grep picoCTF

(capscorpion142@asaad: ~/Desktop/Autoformation/CTFs/PicoCTF/Disko 2)
$

(capscorpion142@asaad: ~/Desktop/Autoformation/CTFs/PicoCTF/Disko 2)
$

(capscorpion142@asaad: ~/Desktop/Autoformation/CTFs/PicoCTF/Disko 2)
$ debugfs -R "logdump" linux_part.dd > journal.txt

debugfs 1.47.2 (1-Jan-2025)
  
```

- So here, we decided to do -td with the strings command, and so the first flag, with the smallest offset is the flag...

