

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

```
(capscorpion142@asaad:~/Desktop/Autoformation/CTFs/PicoCTF/Disko 2]$ ls disko-2.dd
(capscorpion142@asaad:~/Desktop/Autoformation/CTFs/PicoCTF/Disko 2]$ file disko-2.dd
disko-2.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
(capscorpion142@asaad:~/Desktop/Autoformation/CTFs/PicoCTF/Disko 2]$ sudo mount -o loop linux_part.dd mnt
[sudo] password for capsCorpion142: 88,699 89% 3,916 93% 4,699 91%
(capscorpion142@asaad:~/Desktop/Autoformation/CTFs/PicoCTF/Disko 2]$ ls mnt
bin lost+found
```

Rechercher

Kali Linux [En fonction] - Oracle VM VirtualBox

```
(capscorpion142@asaad:~/Desktop/Autoformation/CTFs/PicoCTF/Disko 2]$ ls mnt
(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
```

Filters

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

File Actions Edit View Help

Forensics

DISKO 3 DISKO 2

Challenges Playlists Assignments

20:11 14°C 22/01/2026

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

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

```
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
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
Filters
(capscorpion142@asaad) [~/Desktop/Autoformation/CTFs/PicoCTF/Disko 2]
$ 
Search by Name
(capscorpion142@asaad) [~/Desktop/Autoformation/CTFs/PicoCTF/Disko 2]
$ debugfs -R "logdump" linux_part.dd > journal.txt
debugfs 1.47.2 (1-Jan-2025)
Rechercher
```

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

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

blkls -f ext4 linux_part.dd > unalloc.bin

strings unalloc.bin | grep picoCTF

debugfs -R "logdump" linux_part.dd > journal.txt

strings journal.txt | grep picoCTF

strings -td linux_part.dd | grep picoCTF

236208 picoCTF{4_P4Rt_1t_i5_055dd175}

16921264 picoCTF{4_P4Rt_1t_i5_055dd175}

Power Manager
Your Battery is charging

Challenges Compete Classrooms CapScorpion142 Assignments

Filters Progress Tracker

Forensics Medium Reference Disko 2

Glory of the Garden DISKO 3

14°C 20:11 22/01/2026

Rechercher

```
capscorpion142@asaad: ~/Desktop/Autoformation/CTFs/PicoCTF/Disko 2
$ blkls -f ext4 linux_part.dd > unalloc.bin
$ strings unalloc.bin | grep picoCTF
$ debugfs -R "logdump" linux_part.dd > journal.txt
$ strings journal.txt | grep picoCTF
$ strings -td linux_part.dd | grep picoCTF
236208 picoCTF{4_P4Rt_1t_i5_055dd175}
16921264 picoCTF{4_P4Rt_1t_i5_055dd175}
```