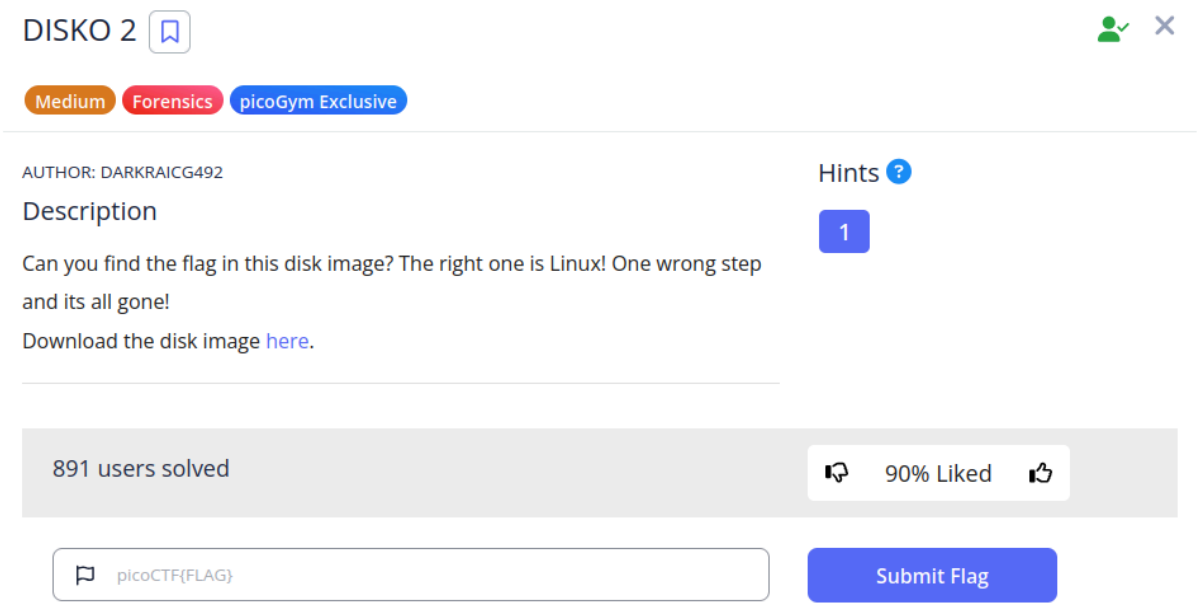
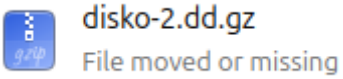
DISKO 2

By: Kyou



Mungkin bisa dibaca dulu deskripsi dari chall-nya :v
Nah di chall ini, kita dikasih file berupa disk image



Kalau udah didownload, kita bisa mulai untuk ngecek filenya

```
ordinarycat@ordinarycat-VirtualBox:~/Cyber Security/Forensics$ file disko-2.dd
disko-2.dd: DOS/MBR boot sector; partition 1 : ID=0x83, start-CHS (0x0,32,33), e
nd-CHS (0x3,80,13), startsector 2048, 51200 sectors; partition 2 : ID=0xb, start
-CHS (0x3,80,14), end-CHS (0x7,100,29), startsector 53248, 65536 sectors
```

Bisa dilihat pada filenya itu terdapat beberapa partisi didalamnya. Kita bisa pake command “fdisk” untuk ngurutin partisi file yang ada.

```
ordinarycat@ordinarycat-VirtualBox:~/Cyber Security/Forensics$ fdisk -l disko-2.
dd
Disk disko-2.dd: 100 MiB, 104857600 bytes, 204800 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x8ef8eaee

Device       Boot Start    End Sectors Size Id Type
disko-2.dd1        2048  53247   51200  25M 83 Linux
disko-2.dd2       53248 118783   65536  32M  b W95 FAT32
```

Nah setelah dijalankan, bisa dilihat bahwa kedua partisi dari masing-masing file tersebut memiliki tipe yang berbeda. Karena chall-nya itu ngasih tau flagnya itu ada dipartisi file yang tipenya itu Linux, maka kita bisa fokus untuk ngeekstrak partisi “disko-2.dd1” doang.

```
ordinarycat@ordinarycat-VirtualBox:~/Cyber Security/Forensics$ dd if=disko-2.dd
of=part1.img bs=512 skip=2048 count=51200
51200+0 records in
51200+0 records out
26214400 bytes (26 MB, 25 MiB) copied, 0.146507 s, 179 MB/s
```

Nah kalau bingung itu commandnya ngapain, biar aku jelasin.

- dd: untuk ngecopy data byte-per-byte
- if=disko-2.dd: nama input filenya itu “disko-2.dd”
- of=part1.img: output dari filenya itu “part1.img” (format penamaannya sebenernya bebas, ini karena nyesuain partisi pertama)
- bs=512: ukuran blok dari filenya 512 byte
- skip=2048: ngeskip 2048 blok pertama -> 2048 x 512 = 1 MiB
- count=51200: ngecopy 51200 blok (karena jumlah sektor dari partisinya itu 51200) -> 51200 x 512 = 25 MiB (sesuai dengan size dari partisi pertama)

Step terakhir cuma ngeekstrak string dari file yang udah diekstrak tadi.

```
ordinarycat@ordinarycat-VirtualBox:~/Cyber Security/Forensics$ strings part1.img
 | grep pico
picoCTF{4_P4Rt_1t_i5_90a3f3d1}
```

Udah gitu doang sih :v
flag: picoCTF{4_P4Rt_1t_i5_90a3f3d1}

“my wife's reaction when I managed to complete this challenge”
~ Kyou