

DISKO 2

disini saya mendapatkan sebuah file dd kembali dan saya mencoba melakukan mounting dengan menggunakan command mount untuk mengetahui isi didalam file dd tersebut

```
cyberjunkie@shadow:~/ctf/pico$ sudo mount -o loop,offset=1048576 disko-2.dd /mnt/linux
mount: /mnt/linux: /home/cyberjunkie/ctf/pico/disko-2.dd is already mounted.
cyberjunkie@shadow:~/ctf/pico$ cd /mnt/linux
cyberjunkie@shadow:/mnt/linux$ ls
bin  lost+found
```

namun kami tidak menemukan apapun, didalam kedua directory yang sudah kami mounting

```
ldapsearch          xkbwatch
ldapurl             xkill
ldapwhoami          xlsatoms
libnetcfg           xlsclients
lightdm-gtk-greeter-settings xlsfonts
listres             xmessage
loadkeys            xprop
loadunimap          xsubpp
look                xvinfo
lowntfs-3g          xwininfo
lzmainfo            xz
m4                  xzcat
mapscrn             xzcmp
mk_modmap           xzdiff
mount               xzegrep
mt-gnu              xzfgrep
ncurses6-config     xzgrep
ncursesw6-config    xzless
nisdomainname       xzmore
openvt              ypdomainname
perl5.40-x86_64-linux-gnu zipdetails
perlbug

./lost+found:
cyberjunkie@shadow:/mnt/linux$ sudo ls -R | grep "flag"
cyberjunkie@shadow:/mnt/linux$ sudo ls -R | grep "pico"
piconv
cyberjunkie@shadow:/mnt/linux$ sudo ls -R | grep "picoCTF"
cyberjunkie@shadow:/mnt/linux$
```

kami mencoba melakukan analisa kembali dengan menggunakan strings tools pada file awal dan kami menemukan kumpulan flag berada di dalam file awal, dan kami mencoba untuk mengumpulkan dan melakukan summary atas flag yang kami temukan

```
cyberjunkie@shadow:~/ctf/pico$ strings disko-2.dd | grep "picoCTF"
picoCTF{4_P4Rt_1t_i5_d3f931a0}
picoCTF{4_P4Rt_1t_i5_a3930df1}
picoCTF{4_P4Rt_1t_i5_f1d0a339}
picoCTF{4_P4Rt_1t_i5_fad03913}
picoCTF{4_P4Rt_1t_i5_139df3a0}
picoCTF{4_P4Rt_1t_i5_f931d3a0}
picoCTF{4_P4Rt_1t_i5_30da391f}
picoCTF{4_P4Rt_1t_i5_af33091d}
picoCTF{4_P4Rt_1t_i5_9d0331fa}
picoCTF{4_P4Rt_1t_i5_13a03f9d}
picoCTF{4_P4Rt_1t_i5_3df91a30}
picoCTF{4_P4Rt_1t_i5_39f3ad01}
picoCTF{4_P4Rt_1t_i5_930d1fa3}
picoCTF{4_P4Rt_1t_i5_90da3f31}
picoCTF{4_P4Rt_1t_i5_0ad9133f}
picoCTF{4_P4Rt_1t_i5_3ad039f1}
picoCTF{4_P4Rt_1t_i5_339da10f}
picoCTF{4_P4Rt_1t_i5_d33af901}
picoCTF{4_P4Rt_1t_i5_93d0f3a1}
picoCTF{4_P4Rt_1t_i5_9330afd1}
picoCTF{4_P4Rt_1t_i5_9a3d10f3}
picoCTF{4_P4Rt_1t_i5_d9f033a1}
picoCTF{4_P4Rt_1t_i5_d390f1a3}
picoCTF{4_P4Rt_1t_i5_0ad3139f}
picoCTF{4_P4Rt_1t_i5_fa39d031}
picoCTF{4_P4Rt_1t_i5_90a3f3d1}
ronse paquetes en base xa en requiridos: ${picoCTF{4_P4Rt_1t_i5_903d13af}
ce debcpicoCTF{4_P4Rt_1t_i5_393da1f0}dawanym pytaniam priorytety. Tylko pytania o pewnym lu
b wy
Description-gl.UTF-8: Configurar unha rede empreganpicoCTF{4_P4Rt_1t_i5_1930da3f}escription-
gu.UTF-8:
ChoicpicoCTF{4_P4Rt_1t_i5_a0f313d9}k Harf Kilidi), Sa
Extended_picoCTF{4_P4Rt_1t_i5_3d1309af}u d'archivu Debian especific
ExtenpicoCTF{4_P4Rt_1t_i5_30f931da}tse tiedostojen hakemiseen k
fald kanpicoCTF{4_P4Rt_1t_i5_1a33f09d}. Hvis du ikke kender svaret p
picoCTF{4_P4Rt_1t_i5_913a30df}
Extended_descriptionpicoCTF{4_P4Rt_1t_i5_331d0f9a}
Description-ta.UTpicoCTF{4_P4Rt_1t_i5_339d0fa1}
picoCTF{4_P4Rt_1t_i5_91fda330}
```

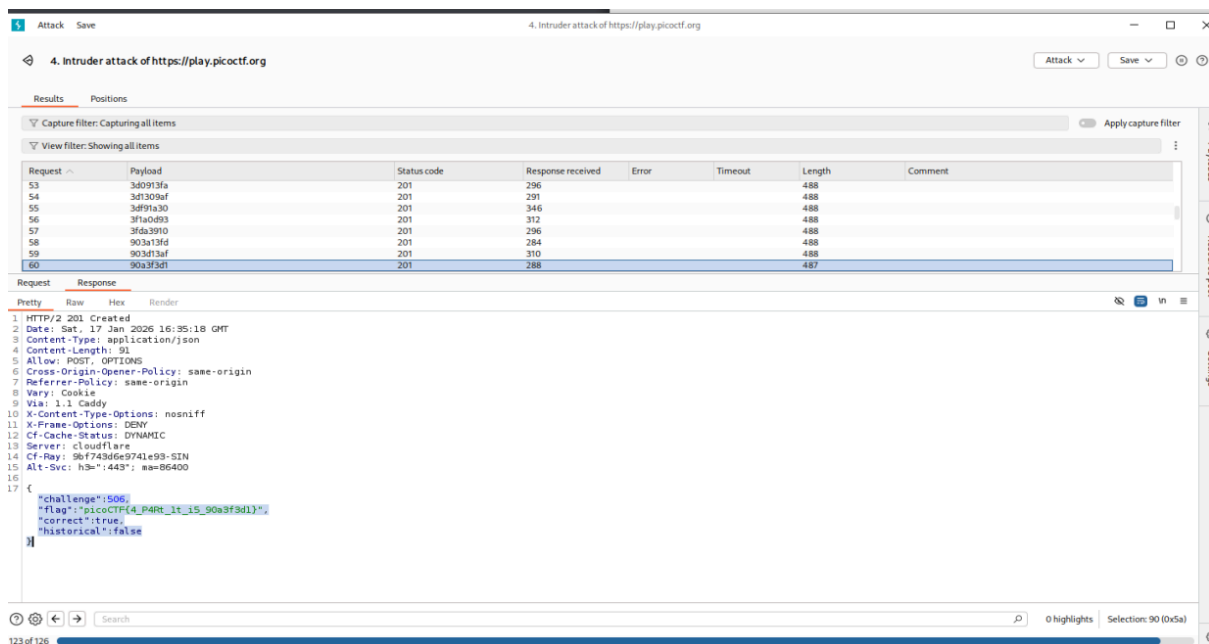
```
cyberjunkie@shadow:~/ctf/pico$ cat disko_flag.txt
picoCTF{4_P4Rt_1t_i5_d3f931a0}
picoCTF{4_P4Rt_1t_i5_a3930df1}
picoCTF{4_P4Rt_1t_i5_f1d0a339}
picoCTF{4_P4Rt_1t_i5_fad03913}
picoCTF{4_P4Rt_1t_i5_139df3a0}
picoCTF{4_P4Rt_1t_i5_f931d3a0}
picoCTF{4_P4Rt_1t_i5_30da391f}
picoCTF{4_P4Rt_1t_i5_af33091d}
picoCTF{4_P4Rt_1t_i5_9d0331fa}
picoCTF{4_P4Rt_1t_i5_13a03f9d}
picoCTF{4_P4Rt_1t_i5_3df91a30}
picoCTF{4_P4Rt_1t_i5_39f3ad01}
picoCTF{4_P4Rt_1t_i5_930d1fa3}
picoCTF{4_P4Rt_1t_i5_90da3f31}
picoCTF{4_P4Rt_1t_i5_0ad9133f}
picoCTF{4_P4Rt_1t_i5_3ad039f1}
picoCTF{4_P4Rt_1t_i5_339da10f}
picoCTF{4_P4Rt_1t_i5_d33af901}
picoCTF{4_P4Rt_1t_i5_93d0f3a1}
picoCTF{4_P4Rt_1t_i5_9330afd1}
picoCTF{4_P4Rt_1t_i5_9a3d10f3}
picoCTF{4_P4Rt_1t_i5_d9f033a1}
picoCTF{4_P4Rt_1t_i5_d390f1a3}
picoCTF{4_P4Rt_1t_i5_0ad3139f}
picoCTF{4_P4Rt_1t_i5_fa39d031}
picoCTF{4_P4Rt_1t_i5_90a3f3d1}
picoCTF{4_P4Rt_1t_i5_903d13af}
picoCTF{4_P4Rt_1t_i5_393da1f0}
picoCTF{4_P4Rt_1t_i5_1930da3f}
picoCTF{4_P4Rt_1t_i5_a0f313d9}
picoCTF{4_P4Rt_1t_i5_3d1309af}
picoCTF{4_P4Rt_1t_i5_30f931da}
picoCTF{4_P4Rt_1t_i5_1a33f09d}
picoCTF{4_P4Rt_1t_i5_913a30df}
picoCTF{4_P4Rt_1t_i5_331d0f9a}
picoCTF{4_P4Rt_1t_i5_339d0fa1}
picoCTF{4_P4Rt_1t_i5_91fda330}
picoCTF{4_P4Rt_1t_i5_09a331df}
picoCTF{4_P4Rt_1t_i5_339a10df}
```

kami menjadikan ini sebagai payload untuk melakukan brute force ke dalam inputan flag ctf agar kami bisa menemukan flag mana yang valid, namun kami tidak menemukan flag yang tepat dikarenakan kami mengira bahwa seluruh flag bisa langsung di inputkan ternyata tidak, kami harus memfilter flag agar hanya suffixnya saja yang di inputkan, jadi kami mencoba memodifikasi payload kami kembali dengan hanya suffix strings biasa dari masing masing

kandidat flag

```
picoCTF{4_P4Rt_1t_i5_af13d930}
picoCTF{4_P4Rt_1t_i5_9130fa3d}
picoCTF{4_P4Rt_1t_i5_d10f933a}
picoCTF{4_P4Rt_1t_i5_df03931a}
picoCTF{4_P4Rt_1t_i5_381d3fa9}
picoCTF{4_P4Rt_1t_i5_d033fa91}
picoCTF{4_P4Rt_1t_i5_0af31d39}
picoCTF{4_P4Rt_1t_i5_af3093d1}
picoCTF{4_P4Rt_1t_i5_0d913af3}
picoCTF{4_P4Rt_1t_i5_01a3d93f}
picoCTF{4_P4Rt_1t_i5_a3d3901f}
picoCTF{4_P4Rt_1t_i5_d03f391a}
picoCTF{4_P4Rt_1t_i5_f3d9013a}
picoCTF{4_P4Rt_1t_i5_3f1ab093}
picoCTF{4_P4Rt_1t_i5_3d0913fa}
picoCTF{4_P4Rt_1t_i5_01933adf}
picoCTF{4_P4Rt_1t_i5_100da3f3}
picoCTF{4_P4Rt_1t_i5_f093d13a}
picoCTF{4_P4Rt_1t_i5_a0f1393d}
picoCTF{4_P4Rt_1t_i5_df0139a3}
picoCTF{4_P4Rt_1t_i5_03fa913d}
picoCTF{4_P4Rt_1t_i5_13f90ad3}
picoCTF{4_P4Rt_1t_i5_d39f1a03}
picoCTF{4_P4Rt_1t_i5_303d0fa1}
picoCTF{4_P4Rt_1t_i5_393d10af}
picoCTF{4_P4Rt_1t_i5_01d3f9a3}
picoCTF{4_P4Rt_1t_i5_d093a31f}
picoCTF{4_P4Rt_1t_i5_fa330d19}
picoCTF{4_P4Rt_1t_i5_df13309a}
picoCTF{4_P4Rt_1t_i5_3031a9df}
picoCTF{4_P4Rt_1t_i5_df19a330}
picoCTF{4_P4Rt_1t_i5_01d3fa93}
picoCTF{4_P4Rt_1t_i5_133df090}
picoCTF{4_P4Rt_1t_i5_3fda3910}
picoCTF{4_P4Rt_1t_i5_af03d310}
picoCTF{4_P4Rt_1t_i5_03319adf}
picoCTF{4_P4Rt_1t_i5_339a01df}
picoCTF{4_P4Rt_1t_i5_3ad9f301}
picoCTF{4_P4Rt_1t_i5_f31a903d}
picoCTF{4_P4Rt_1t_i5_d930f31a}
picoCTF{4_P4Rt_1t_i5_93da3130}
picoCTF{4_P4Rt_1t_i5_9a30f13d}
cyberjunkie@shadow:~/ctf/pico$ kandidat flag
a3d3901f
a3f9103d
a9d0f313
ad1933f0
af13d930
af3093d1
af33091d
af91303d
af93d310
af9d0133
d033fa91
d03f391a
d093a31f
d10f933a
d33af901
d390f1a3
d39f1a03
d3f1039a
d3f931a0
d930f31a
d9f033a1
df0139a3
df03931a
df13309a
df19a330
f093d13a
f19a03d3
f19d3a03
f1d0a339
f3013da9
f3019a3d
f30a123d
f31a903d
f33d091a
f3d0139a
f3d9013a
f9033d1a
f931d3a0
f9331ad0
fa330d19
fa39d031
fa0d9313
cyberjunkie@shadow:~$ suffix only kandidat flag
```

setelah menunggu response, kami berhasil menemukan suffix flag yang tepat dengan status correct:true



"challenge":506,"flag":"picoCTF{4_P4Rt_1t_i5_90a3f3d1}","correct":true,"historical":false}

DISKO 2



Medium

Forensics

picoGym Exclusive

AUTHOR: DARKRAICG492

Hints 

Description

1

Can you find the flag in this disk image? The right one is Linux! One wrong step and its all gone!

Download the disk image [here](#).

dan yap kami berhasil memecahkan teka teki CTF ini