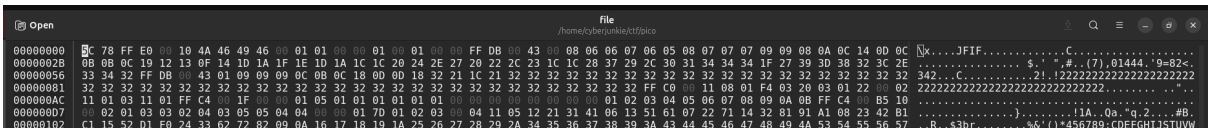
Corrupted file

saya mendapat sebuah file dengan type data dengan nama data, saya mencoba menganalisanya untuk keperluan foresik awal mengetahui file adalah keluarga file apa, menggunakan ghex untuk melihat header byte dari file.

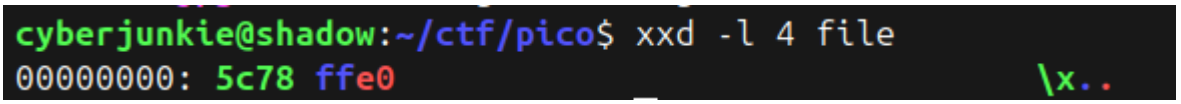


saya menemuka header bytes yang tidak lengkap yang berupa format JFIF (JFIF (JPEG File Interchange Format) adalah format file yang luas digunakan untuk menyimpan gambar raster yang dikompresi JPEG, dirancang untuk memfasilitasi interoperabilitas antar platform dan aplikasi yang berbeda.)

intinya gambar lah tapi di korupt ini, kayak di ptong setengah gitu, nah next gimana cara kita balikinnya, kita analisa dulu ini file type JFIF apa, di liat dari byte nya keliatan bahwa file merupakan potongan dari file JPG, karena…. kalian lihat di github aja ya (https://gist.github.com/leommoore/f9e57ba2aa4bf197ebc5)

ini file soal

github



xxd

diliat cuman ada 2 digit FF E0, nah yang dua lagi kemanaaaaa…. (dikorupt pejabat)

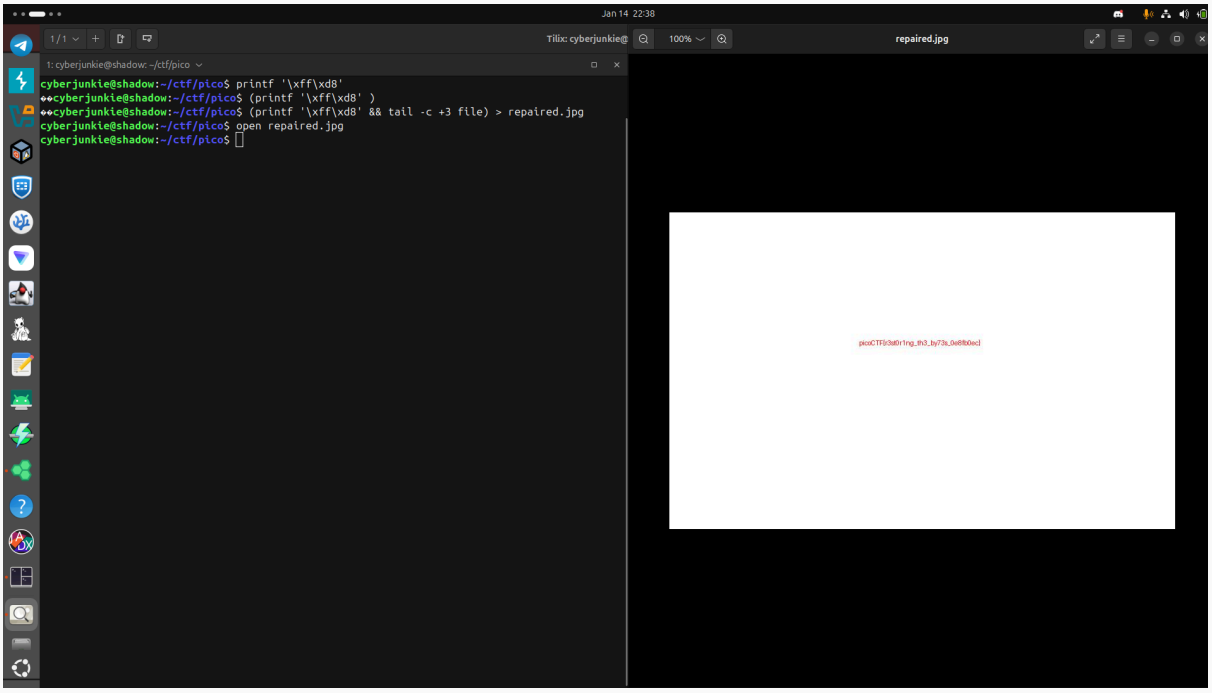
nah kita sebagai robinhood harus bisa ngembaliin duit eh byte yang di korupt sama pejabat eh system.

cara nya dengan memasukan kembali string byte yang hilang dengan menggunakan printf, kenapa nggak echo, karena `echo` TIDAK cocok karena bisa menambahkan newline (`0a`)

ok beriku adalah command nya

```
(printf '\xff\xd8' && tail -c +3 file) > repair.jpg
```

() berfungsi sebagai subshell Semua output di dalam tanda kurung akan digabung Lalu diarahkan (>) ke `repair.jpg` berikut adalah cara kerjanya, disini printf berfungsi sebagai pembuat hex (binary) yang akan dimasukan ke file, lalu tail menentukan dimana hex akan di tempatkan, -c nya adalah bytes (di bytes mana hex ingin di injek atau di sisipkan), +3 berfungsi untuk menjelaskan kepada tail bahwa hex akan ditaruh di byte ke 3 sebelah kiri dari file, > repair.jpg (adalah file yang akan dihasilkan dari perbaikan file yang rusak)



kita berhasil menemukan flagnya yaitu

picoCTF{r3st0r1ng_th3_by73s_0e8fb0ec}

picoCTF{r3st0r1ng_th3_by73s_0e8fb0ec}