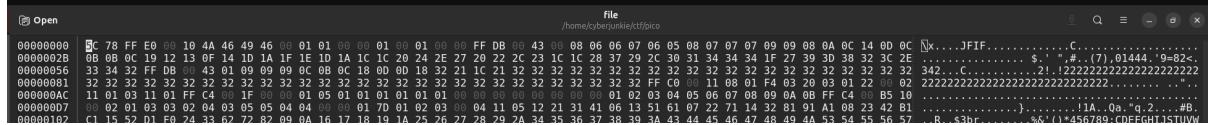


Corrupted file

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



The screenshot shows a hex editor window titled 'file' with the path '/home/cyberjunkie/ctf/pico'. The file content starts with the bytes 5C 78 FF E0 00, which are the standard JFIF header bytes. Following this, there is a large amount of data consisting mostly of zeros and ones, indicating a corrupted or incomplete file. The file ends with some footer bytes including 0A, 0D, 0A, and 0D.

saya menemukan header bytes yang tidak lengkap yang berupa format 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 potong 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>)

5C 78 FF E0 00 ini file soal



The screenshot shows a file browser interface. A file named 'file' is selected, and its details are shown: 'JPEG File Interchange Format' (type), '.jpg' (extension), 'ff d8 ff e0' (size), and '....' (end). This indicates that the file is a corrupted version of a JPEG image.

github

```
cyberjunkie@shadow:~/ctf/pico$ xxd -l 4 file
00000000: 5c78 ffe0 \x..
```

xxd

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

nah kita sebagai robinhood harus bisa ngembaliiin 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 berikut 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)

The screenshot shows a terminal window titled 'Tilix: cyberjunkie@...' with the command history:

```
t: cyberjunkie@shadow:~/ctf/picoS
cyberjunkie@shadow:~/ctf/picoS$ printf '\xff\xd8'
<--cyberjunkie@shadow:~/ctf/picoS$ (printf '\xff\xd8' )
<--cyberjunkie@shadow:~/ctf/picoS$ (printf '\xff\xd8' && tail -c +3 file) > repaired.jpg
cyberjunkie@shadow:~/ctf/picoS$ open repaired.jpg
cyberjunkie@shadow:~/ctf/picoS$
```

To the right of the terminal is a small image viewer window titled 'repaired.jpg' showing a blank white image.

kita berhasil menemukan flagnya yaitu

picoCTF{r3st0r1ng_th3_by73s_0e8fb0ec}

picoCTF{r3st0r1ng_th3_by73s_0e8fb0ec}