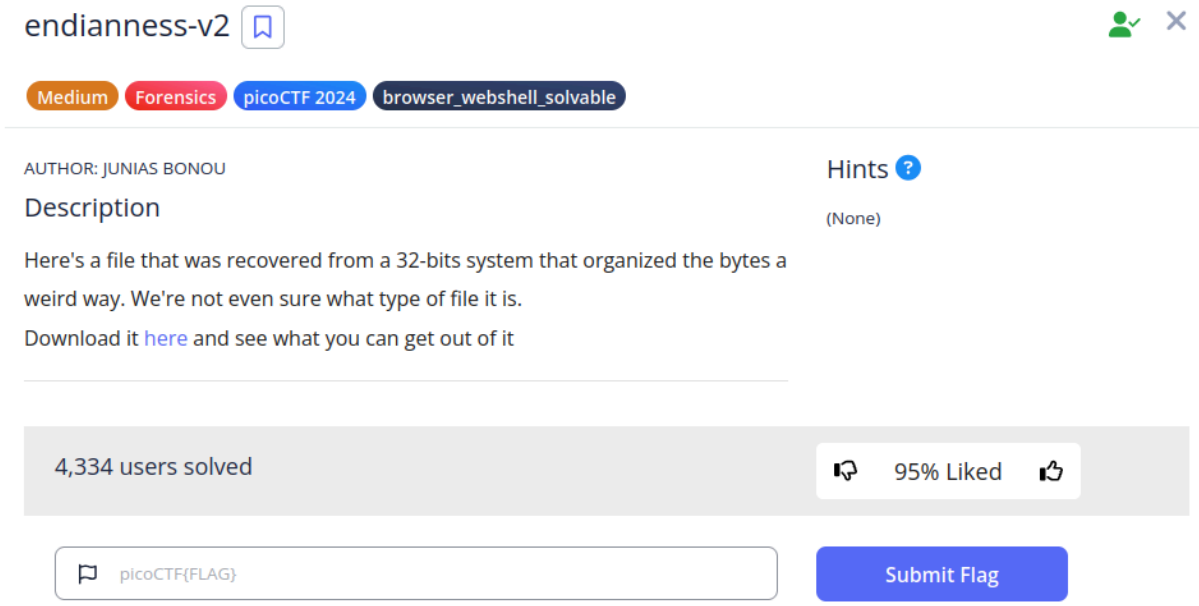
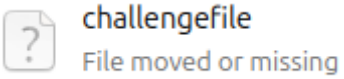
endianness-v2

By: Kyou

Jujur aku masih awam banget di Forensics, jadi kalau ada kesalahan bisa dikoreksi ya bang @Achideon. Anyway here's the chall:



Dari challenge tersebut, kita diberi sebuah binary file

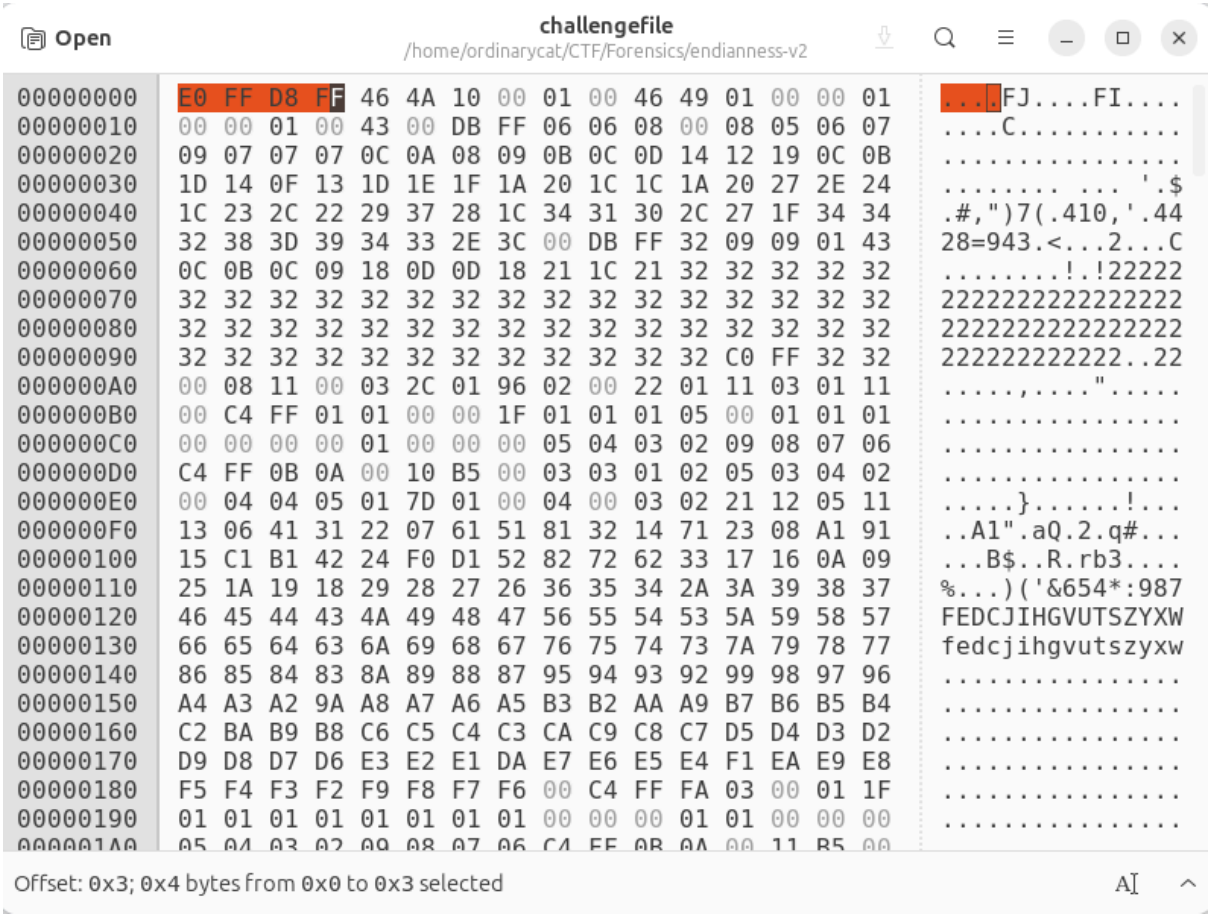


Pertama-tama yang harus kita lakukan adalah mengidentifikasi file tersebut dengan menggunakan 'exiftool'

```
ordinarycat@ordinarycat-VirtualBox:~/CTF/Forensics/endianness-v2$ exiftool chall
engefile
ExifTool Version Number         : 12.76
File Name                       : challengefile
Directory                       : .
File Size                       : 3.4 kB
File Modification Date/Time     : 2025:07:17 20:20:53+07:00
File Access Date/Time           : 2025:07:17 20:20:53+07:00
File Inode Change Date/Time     : 2025:07:17 20:21:19+07:00
File Permissions                : -rw-rw-r--
Warning                         : Processing JPEG-like data after unknown 1-byte
 header
```

Nah bisa dilihat pada gambar, cluenya itu ada di message warning pada gambar yang menyatakan bahwa byte header pertama dari gambar itu mirip dengan format JPG. Selanjutnya kita dapat mengidentifikasi hexdump dari file tersebut dengan menggunakan tool 'ghex'

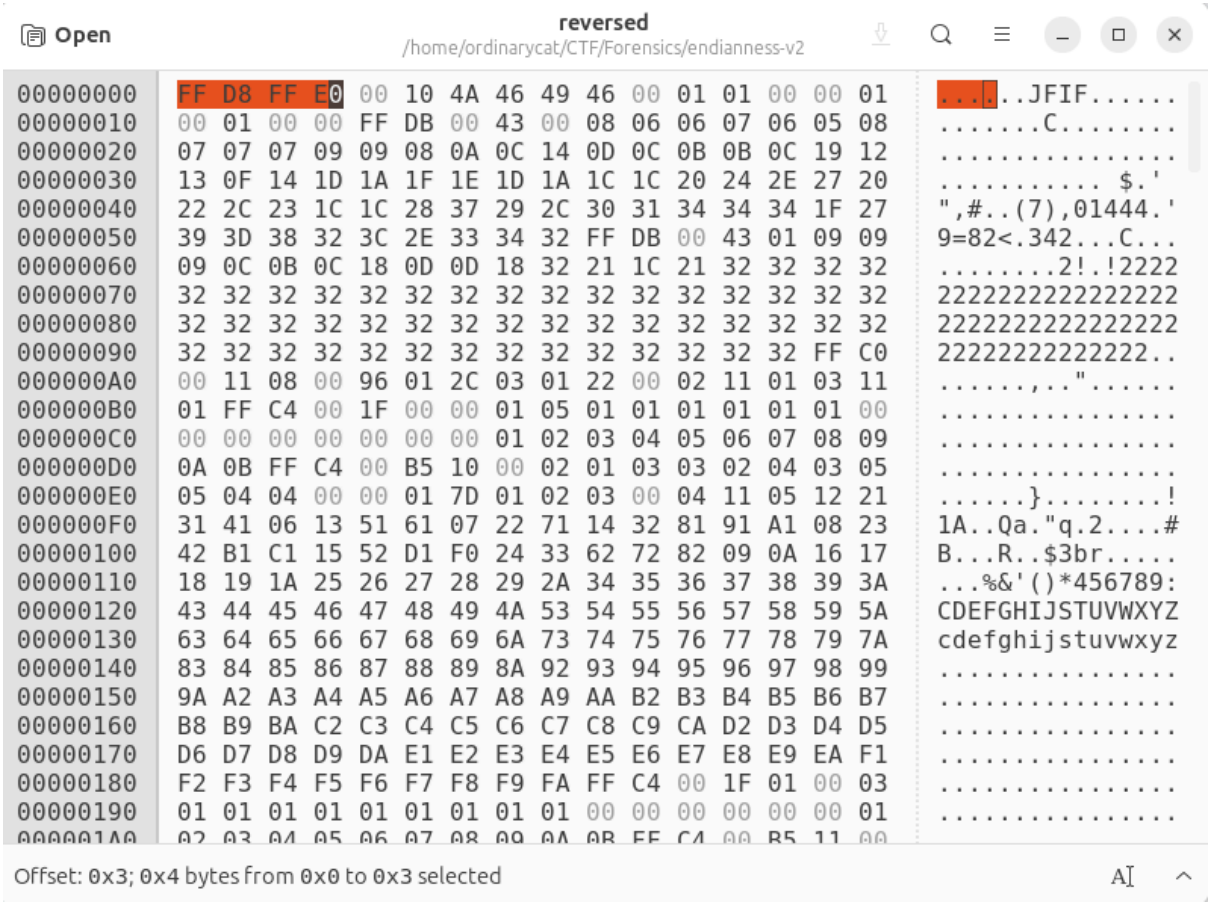
```
ordinarycat@ordinarycat-VirtualBox:~/CTF/Forensics/endianness-v2$ ghex challenge
file
```



Nah 4 byte pertama dari filenya itu sendiri sebenernya cuma 4 byte header dari format file JPG yang di-reverse.
JPG Header : FF D8 FF E0
Tugas kita sekarang adalah ngereverse 4 byte tersebut kembali ke bentuk semulanya.

```
ordinarycat@ordinarycat-VirtualBox:~/CTF/Forensics/endianness-v2$ hexdump -v -e
'1/4 "%08x"' -e '"\n"' challengefile | xxd -r -p > reversed
```

Singkatnya, cara kerja dari command itu adalah untuk membaca file biner terus membalik urutan byte tiap 4 byte (endianness reversal), lalu nyimpen hasilnya ke output file.



picoCTF{cert!f1Ed_iNd!4n_s0rrY_3nDian_004850bf}

Yey dapet flagnya
flag: picoCTF{cert!f1Ed_iNd!4n_s0rrY_3nDian_004850bf}

“yayayayayayayayayayayayayaya ctf india jir”
~Kyou