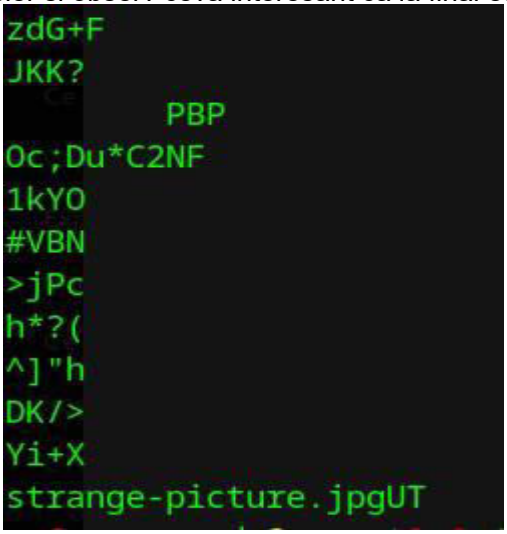
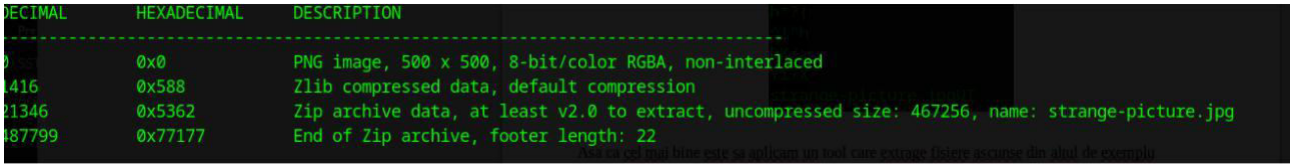
easy-hide

Observam ca primim un png doar ca daca ma uit in exiftool nu observ nimic ciudat la acesta asa ca am zis sa folosesc strings pe fisier si observ ceva interesant ca la final este mentionat un fisier jpg.

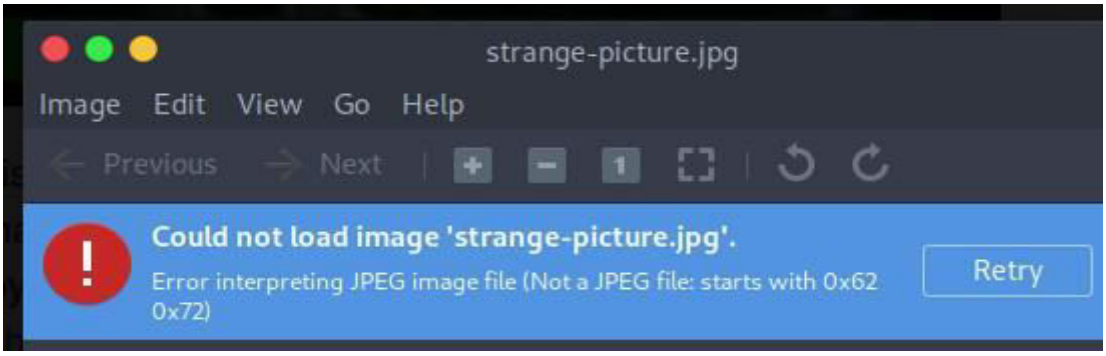


Asa ca cel mai bine este sa aplicam un tool care extrage fisiere ascunse din altul de exemplu binwalk.



I

mi creaza un folder nou “_strange-final.png.extracted” iar aici vad ca am un jpg si un zip.Daca incerc sa deschid imaginea In schimb observ ca primesc o eroare si ca acest fisier nu este jpg desi asa pare.

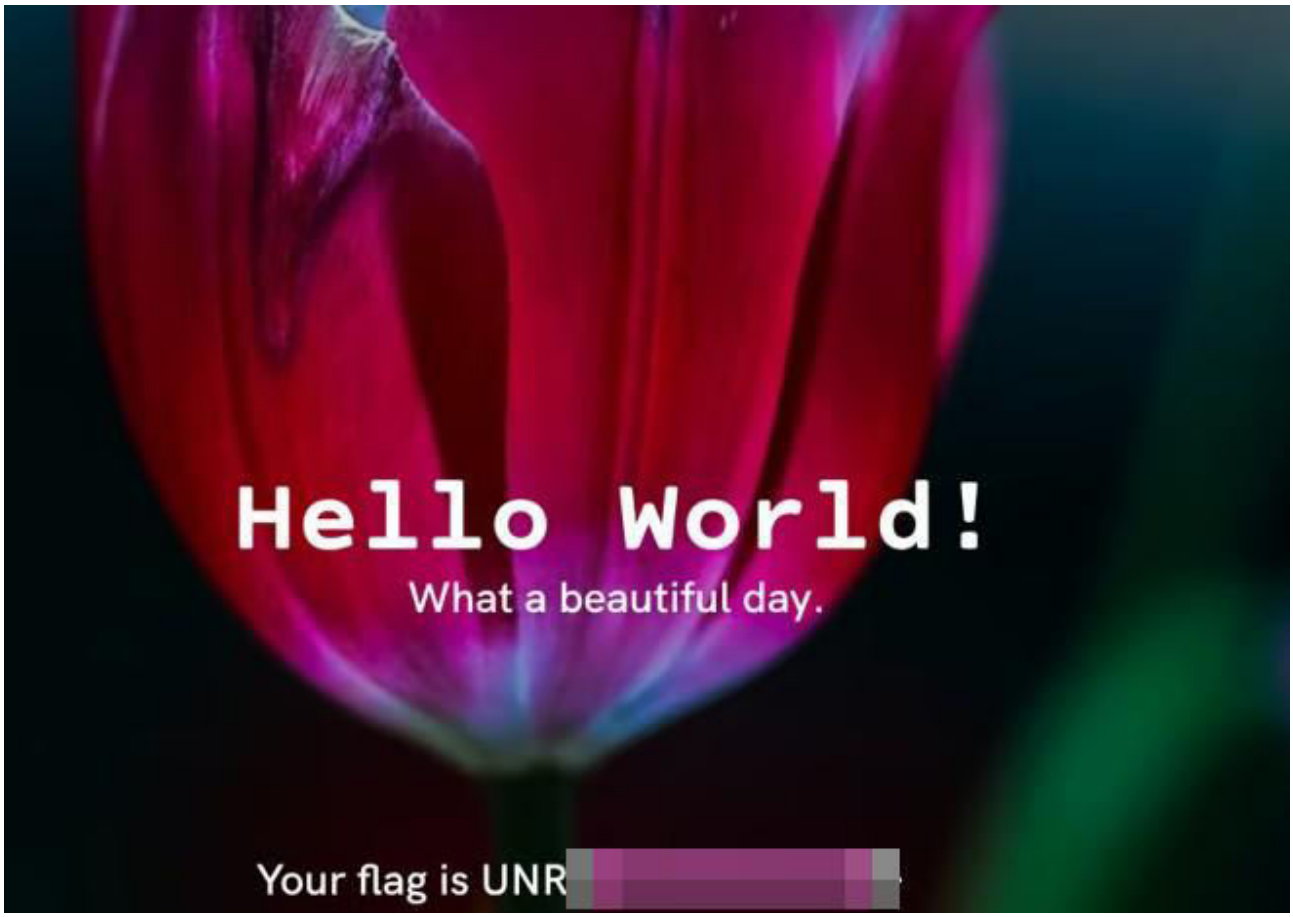


Asa ca am decis sa verific biti la fisier si ofc ca noi trebuie sa ii punem la loc din cauza ca au fost schimbati cu un mesaj :

```
┌──[masquerade@parrot]─[~/Downloads/_strange-final.png.extracted]
└─$ xxd strange-picture.jpg  | head -n 10
00000000: 6272 6f6b 656e 7a69 6e73 6964 6572 6570  brokenzinsiderep
00000010: 0001 0000 ffe2 01d8 4943 435f 5052 4f46  ........ICC_PROF
00000020: 494c 4500 0101 0000 01c8 0000 0000 0430  ILE............0
00000030: 0000 6d6e 7472 5247 4220 5859 5a20 07e0  ..mntrRGB XYZ ..
00000040: 0001 0001 0000 0000 0000 6163 7370 0000  ..........acsp..
```

Am gasit pe google un repo cu fiecare biti “magici” pentru fiecare tip de fisier:
https://en.wikipedia.org/wiki/List_of_file_signatures

Stergem textul de acolo si punem headerul cel bun `FF D8 FF E0 00 10 4A 46 49 46 00 01` iar dupa ce deschidem fisierul ar trebui sa primim in el flagul:



Trolled by masquerade8077