**Write-Up jumat-sabtu 29-30/04/2022**

**Forensic**

**CTF**

1. extensions ( <https://play.picoctf.org/practice/challenge/52?category=4&page=2> )

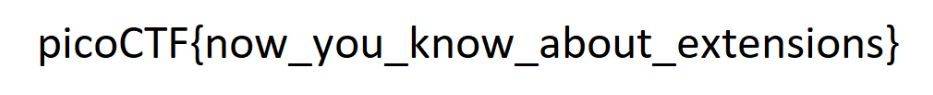
* Diberikan sebuah file txt. Saat di lihat ternyata format filenya berupa file png



* Langsung saja dibuat copy-an dari file tersebut dengan .png file



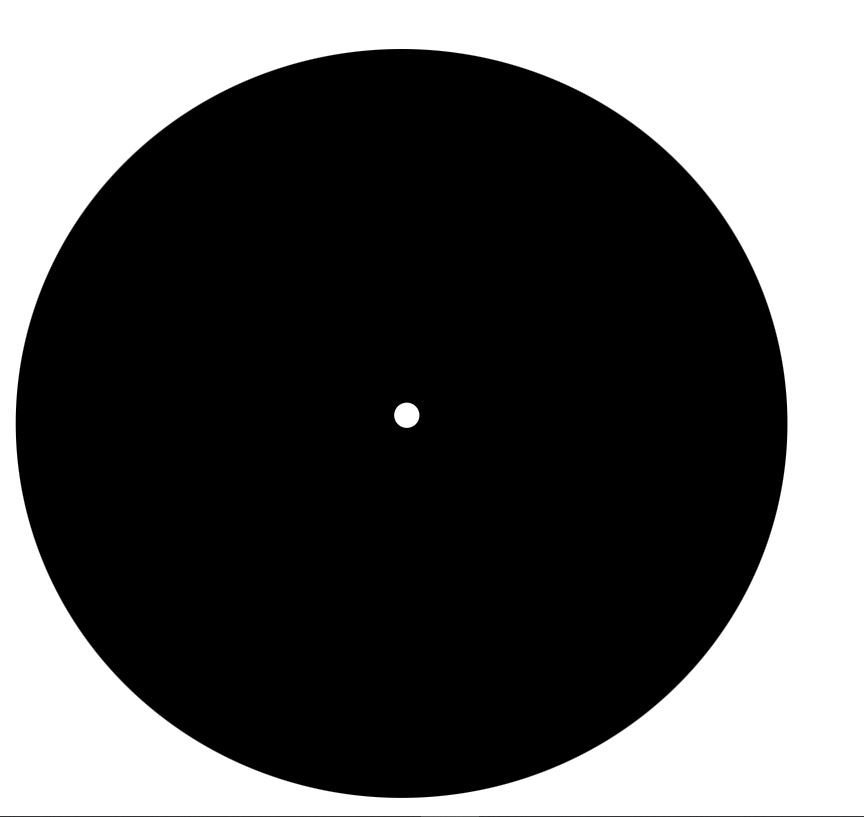
* Setelah dibuka ternyata berisi gambar flagnya



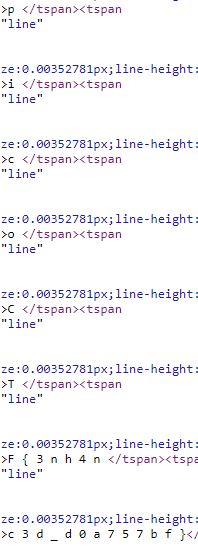
**picoCTF{now\_you\_know\_about\_extensions}**

1. Enhance! ( <https://play.picoctf.org/practice/challenge/265?category=4&page=1> )

* Didapat sebuah file gambar dalam bentuk html



* Setelah di inspect, ternyata flagnya ada di baris codingannya

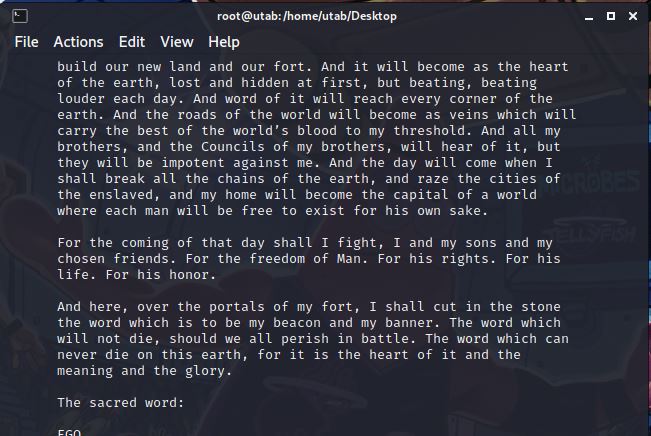


**picoCTF{3nh4nc3d\_d0a757bf}**

1. Lookey here ( <https://play.picoctf.org/practice/challenge/279?category=4&page=1> )



* Lalu saat di tampilkan, berisi informasi yang sangat banyak



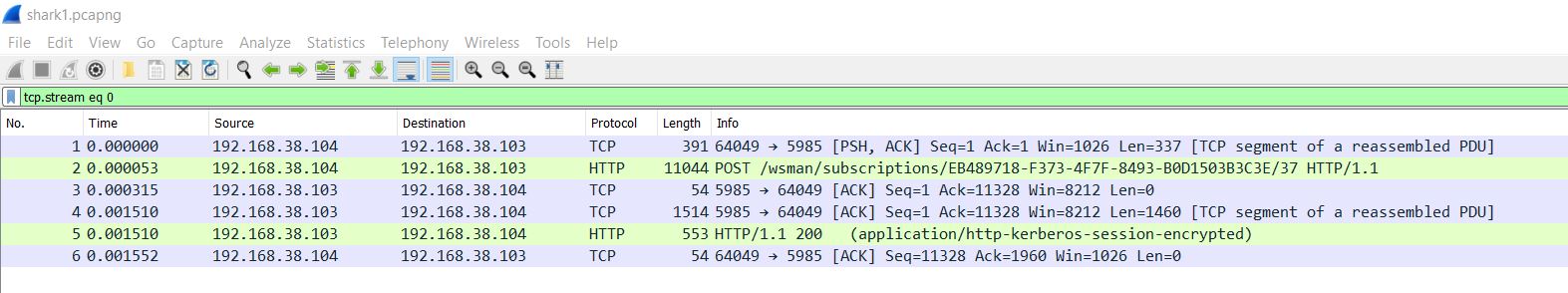
* Lalu saat di grep, flagnya pun didapat



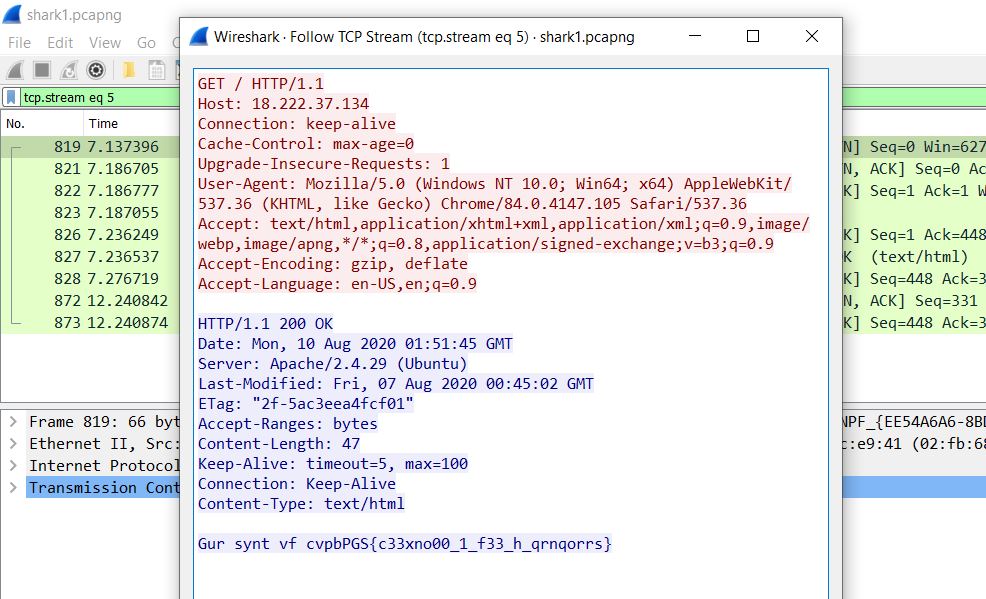
**picoCTF{gr3p\_15\_@w3s0m3\_2116b979}**

1. Wireshark doo dooo do doo... (<https://play.picoctf.org/practice/challenge/115?category=4&page=1> )

* Diberikan sebuah file wireshark



* Setelah mengganti “tcp.stream eq” menjadi “5” lalu dilihat TCP streamnya ditemukan kalimat yang cukup mencurigakan



* Setelah itu dicobalah di decrypt kalimat tersebut dengan ROT13 dan dapatlah flagnya



**picoCTF{p33kab00\_1\_s33\_u\_deadbeef}**

**Tool**

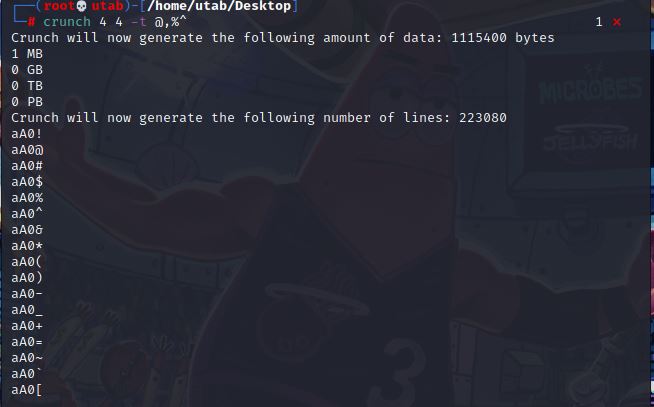
**Crunch**

<https://docs.google.com/spreadsheets/d/12-PmcG_1MtY2hXDoBvjCHuILQEUTXayv/edit#gid=1427959827&range=E12>

<https://docs.google.com/spreadsheets/d/12-PmcG_1MtY2hXDoBvjCHuILQEUTXayv/edit#gid=1427959827&range=E13>

Tool ini digunakan untuk membuat wordlist yang dapat digunakan untuk melakukan bruteforce pada sebuah file yang memiliki keamananseperti file zip yang diberi password

Ini merupakan hasil dari perintah untuk membuat random generated character



@ = lowercase

, = uppercase

% = angka

^ = special character

4 | = banyak character awal

| 4 = banyak character akhir

Agar hasilnya dapat disimpan pada sebuah file maka ditambahkan “-o [namafile]”

