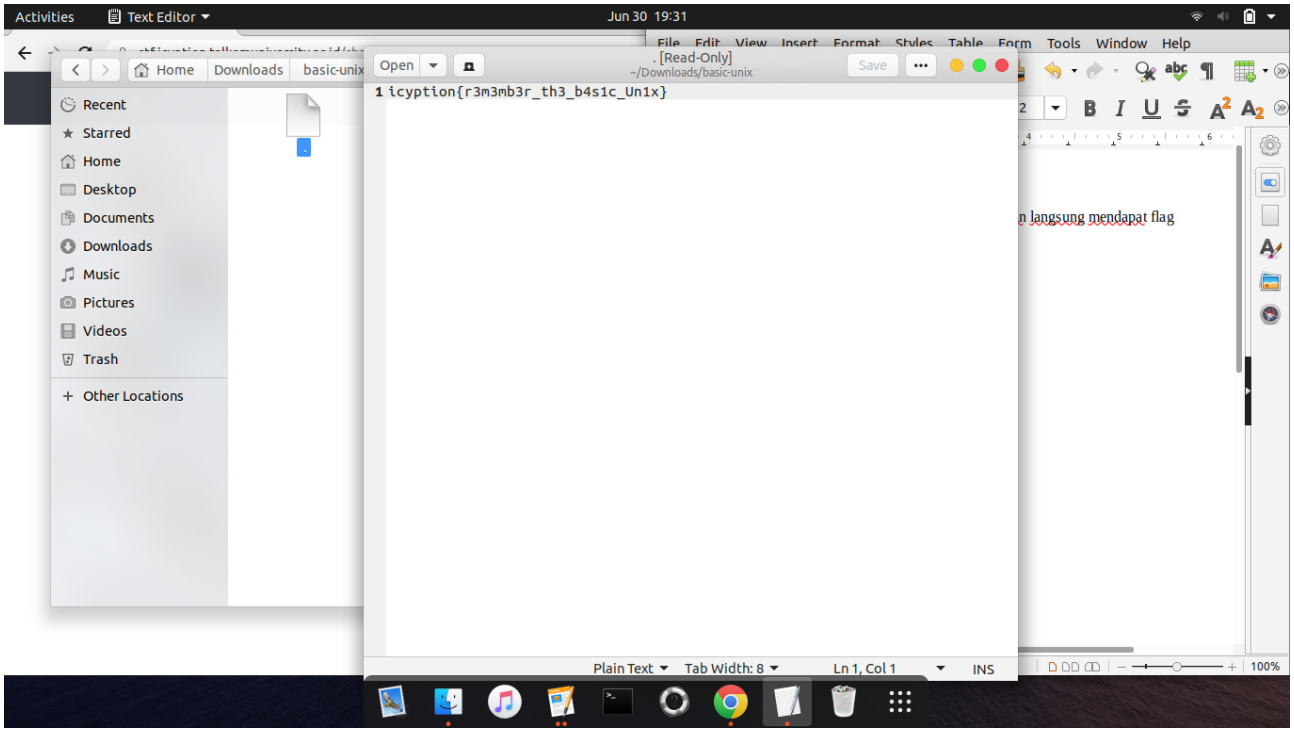
Write Up CTF iCyption Telkom University (Penyisihan)

SOAL 1 CTF
Setelah diunduh file di dalam zip saya mengekstraknya dan langsung mendapat flag

yaitu : icyption{r3m3mb3r_th3_b4s1c_Un1x}



SOAL 2 CTF

VjFaYWExUXdOVmhVYTJ4V1ltdEtjRlJYY0ZaTk1XUllUVlZrYkdKSVFsWldNVkpEVkZaa1Ix
ZHFXbHBXYlUxNFdXMTBORmRIVmtsWApiV3hPVFVWck1WRXlZemxRVVc4OUNnPT0K

diberikan sebuah strings yang merupakan encode base64, saya mencoba mendecodenya ternyata masih dalam base 64 untuk mempersingkat waktu saya membuat script python

string tadi saya masukan ke dalam base64.txt

dengan menggunakan perintah echo
VjFaYWExUXdOVmhVYTJ4V1ltdEtjRlJYY0ZaTk1XUllUVlZrYkdKSVFsWldNVkpEVkZaa1Ix
ZHFXbHBXYlUxNFdXMTBORmRIVmtsWApiV3hPVFVWck1WRXlZemxRVVc4OUNnPT0K
> base64.txt

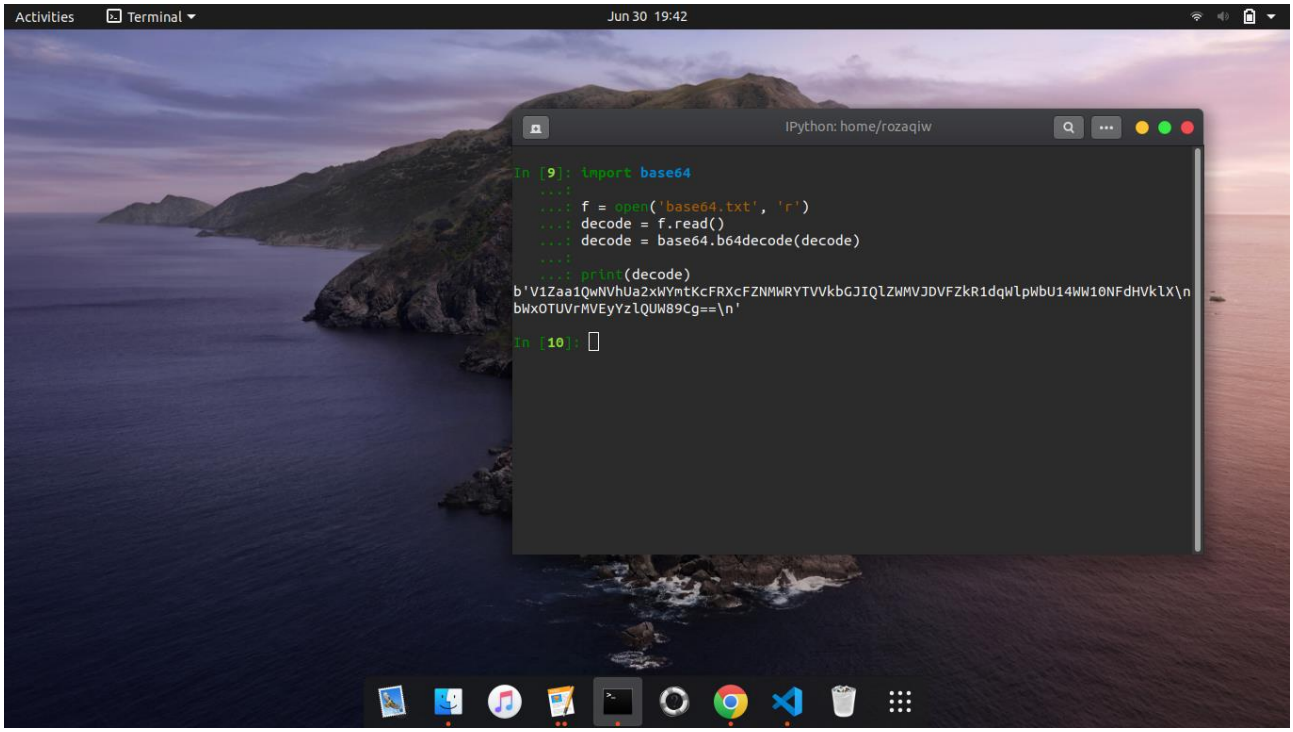
script ini saya coba untuk mendecode satu kali

```
import base64

f = open('base64.txt', 'r')
decode = f.read()
decode = base64.b64decode(decode)

print(decode)
```

saya coba langsung di ipython3



itu untuk mendecode satu kali

dan ini script lengkapnya

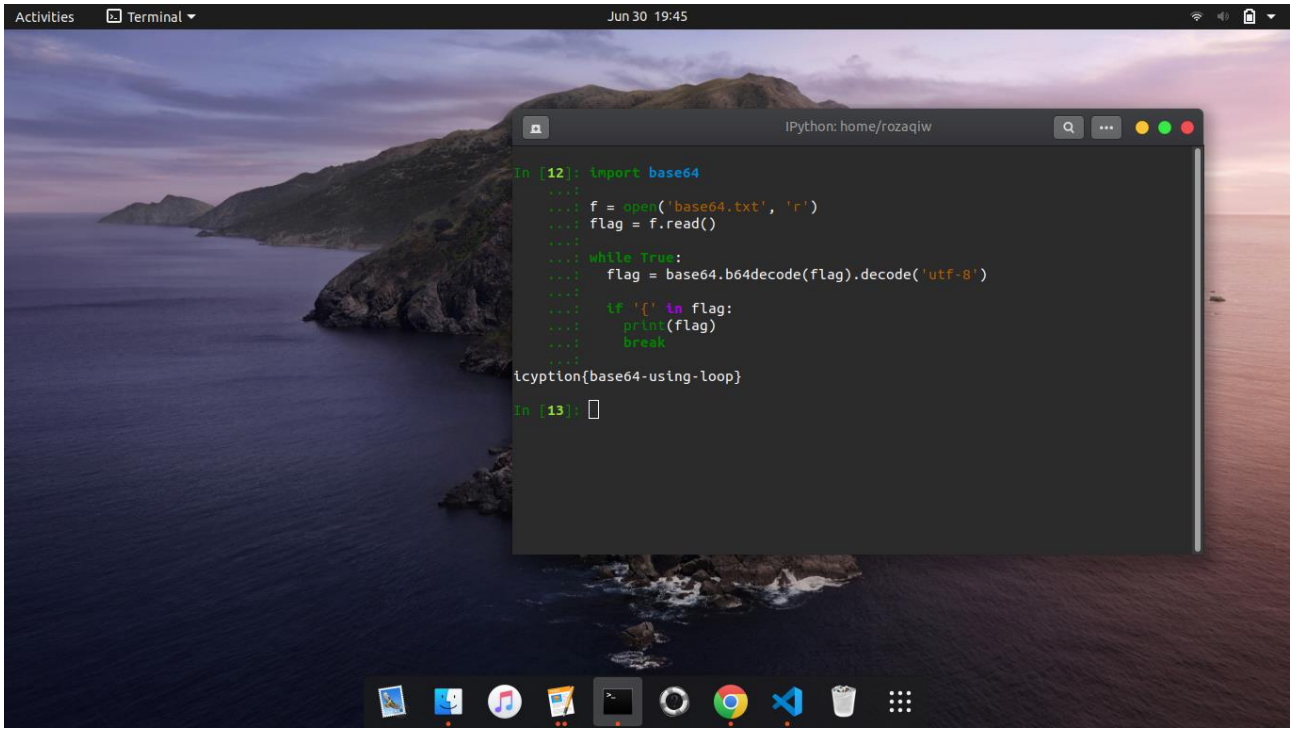
```
import base64

f = open('base64.txt', 'r')
flag = f.read()

while True:
  flag = base64.b64decode(flag).decode('utf-8')

  if '{' in flag:
    print(flag)
    break
```

dan flagnya ditemukan yaitu : icyption{base64-using-loop}



Soal Web Exploitation

soalnya diarahkan ke sebuah web lalu diberikan tampilan login saya mencoba inspect dan melihat ada koding javascript

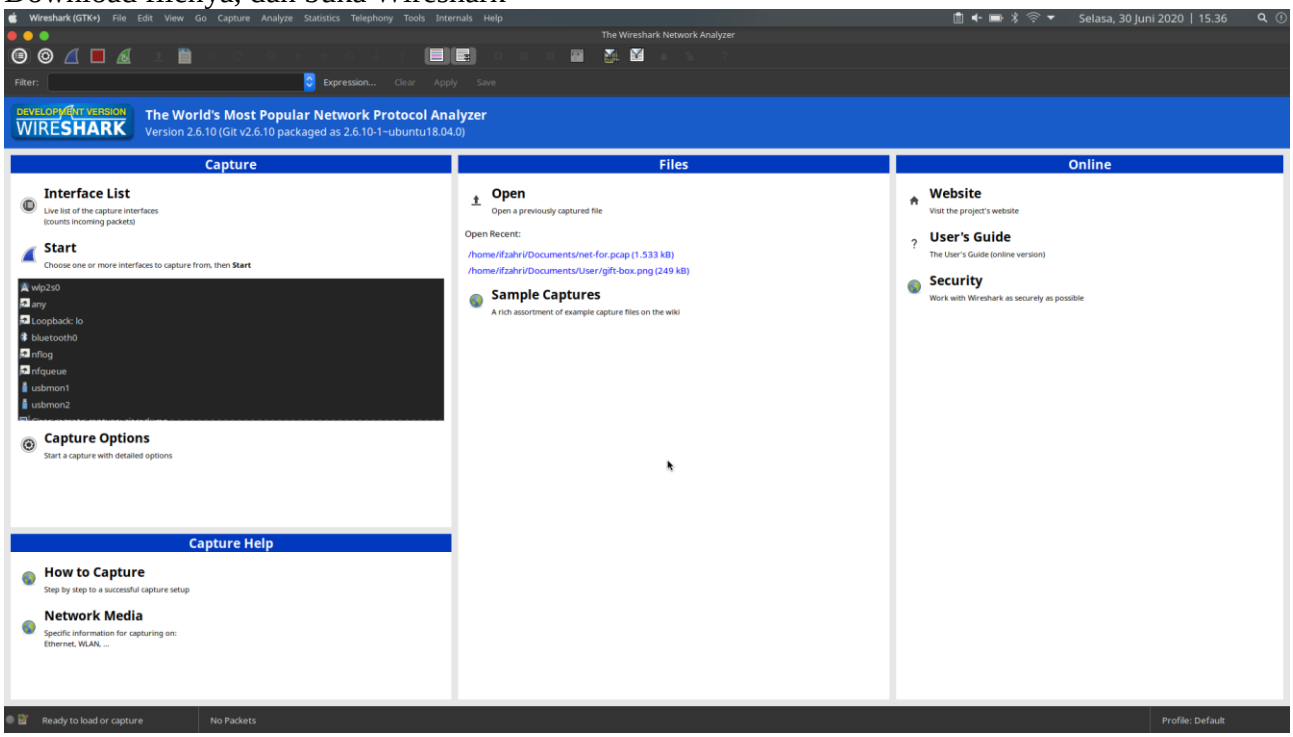
setelah saya susun menjadi kata seperti ini pjfwapvu{olssv-ovd-hyl-fvb-avvd} dan belum terlihat flagnya lalu saya menggunakan cipher tools online
http://rumkin.com/tools/cipher/caesar.php

dan menggeser huruf sebanyak 19

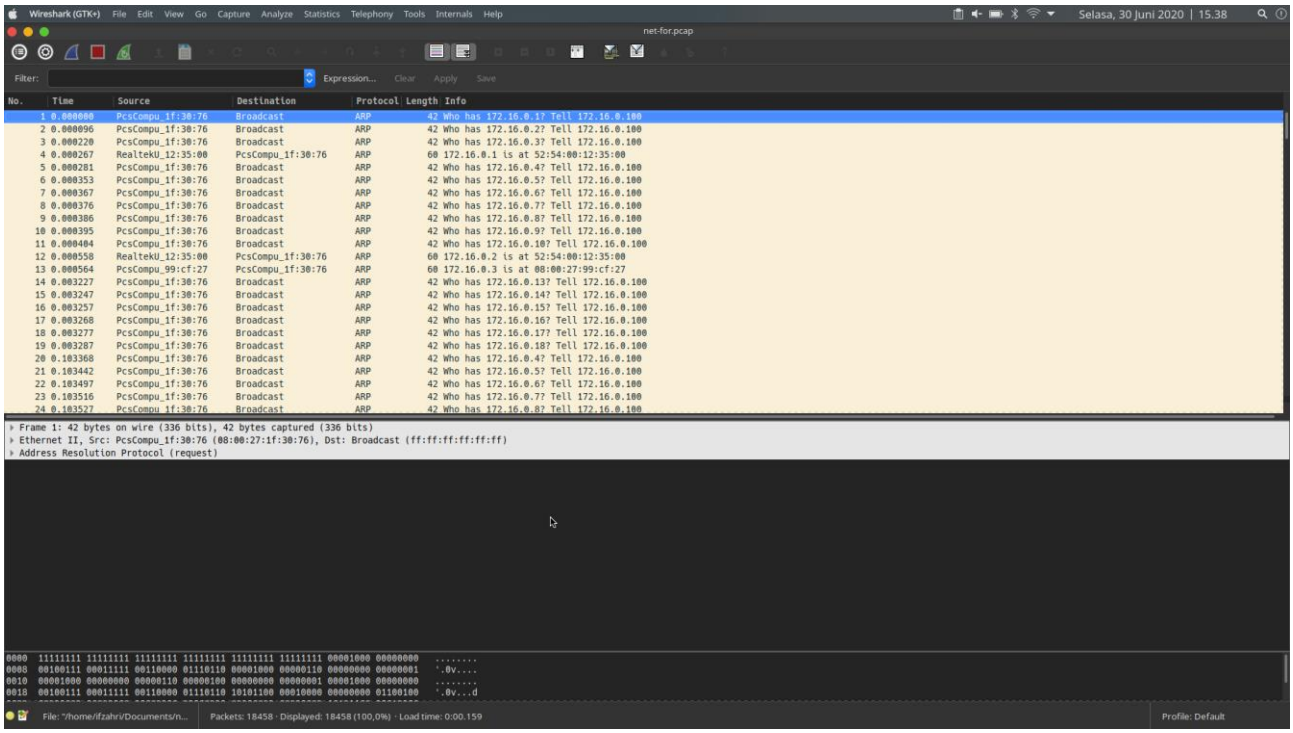
dapat flagnya yaitu : icyption{hello-how-are-you-toow}

FORENSICS

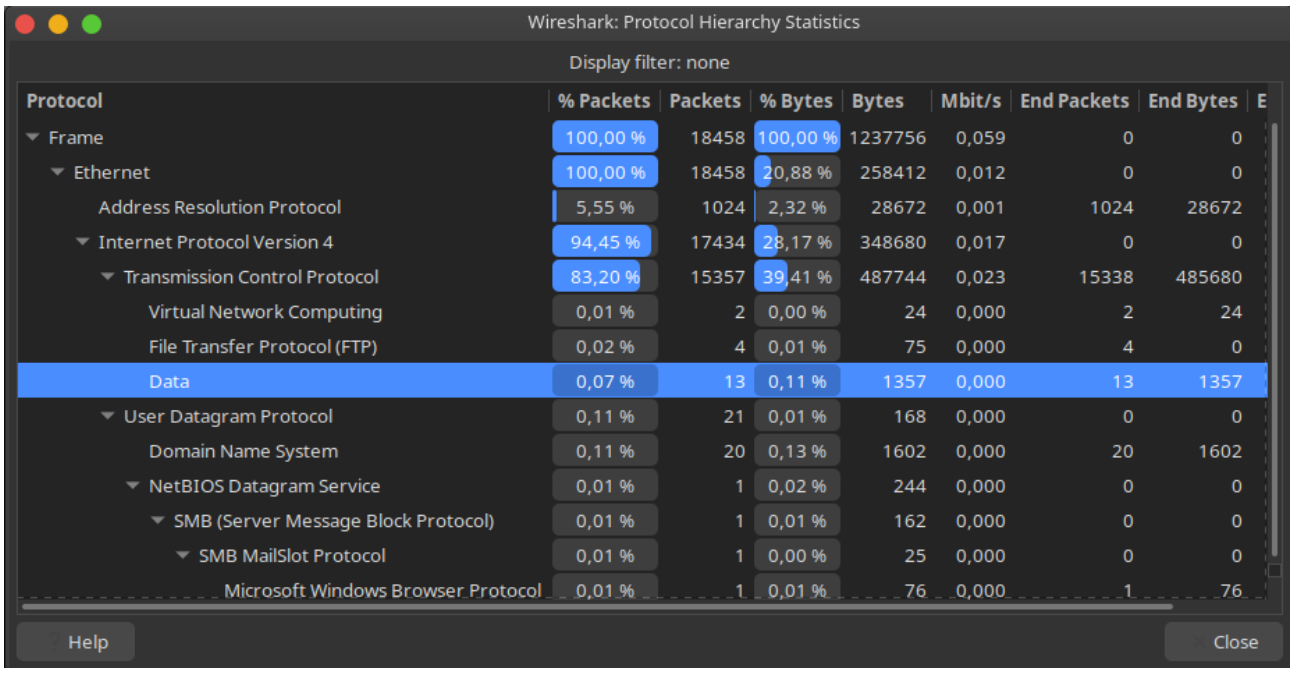
Download filenya, dan buka Wireshark



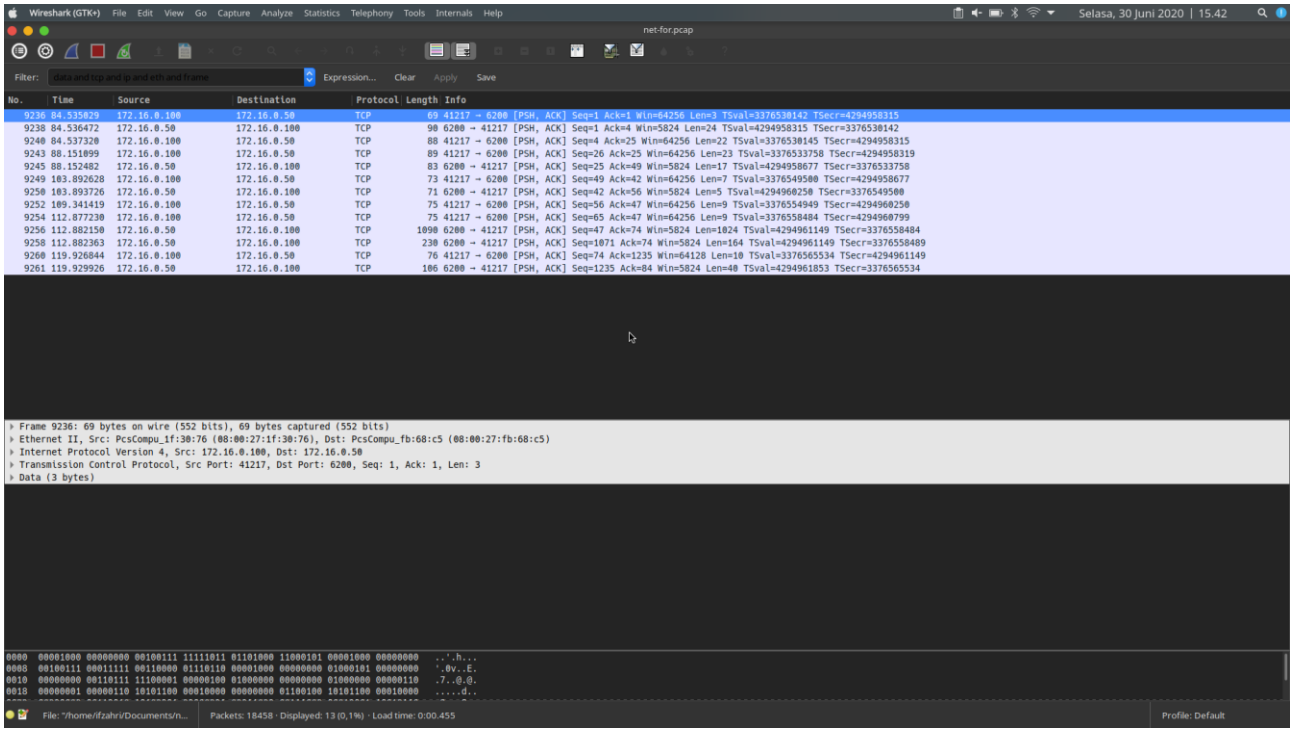
Setelah itu load file yang telah didownload



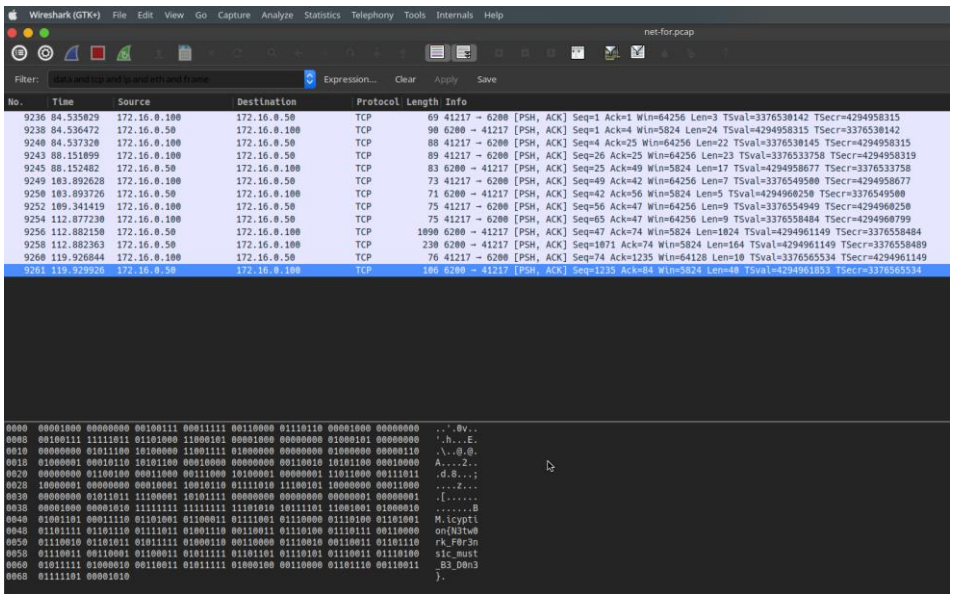
Setelah itu, masukkan filter data sehingga yang terlihat hanyalah aliran data saja, dapat difilter pada menu **Statistics > Protocol Hierarchy**



Maka pilih **Apply As Filter > Selected**, maka yang akan muncul adalah traffic TCP berisi data yang diteruskan



Karena traffic datanya cukup sedikit dan singkat, maka dapat dicek satu persatu maka ketemulah pada bagian akhir



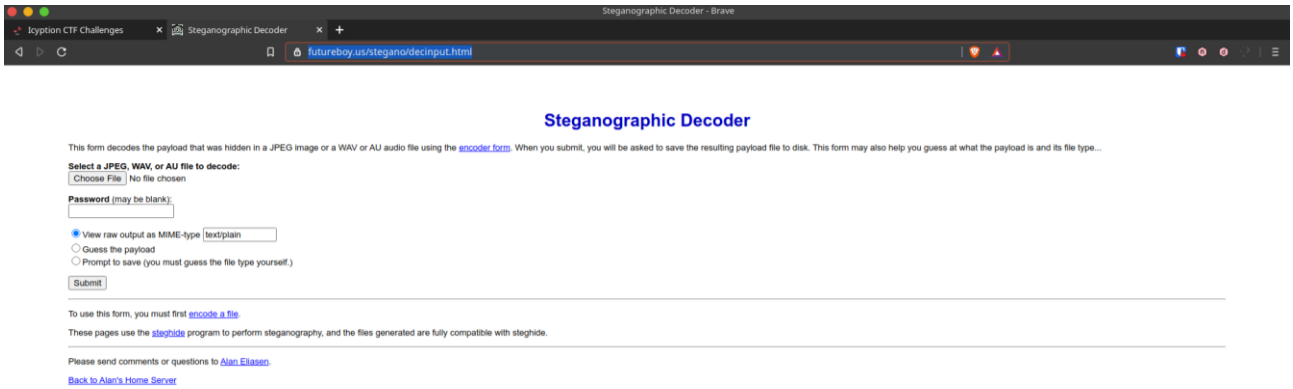
icyption{N3tw0rk_F0r3ns1c_must_B3_D0n3}

Masukkan saja ke bagian submit dan flag diterima.

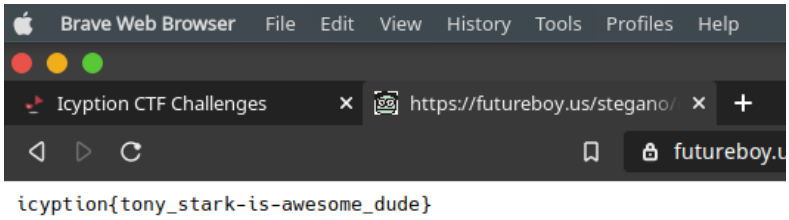
STEGANOGRAPHY

Download filenya yang bernama **ironman.jpeg**, kalau dibuka maka gambarnya seperti ini

Karena inimerupakan steganography, maka langsung saja dicoba menggunakan **Steganographic Decoder (https://futureboy.us/stegano/decinput.html)**



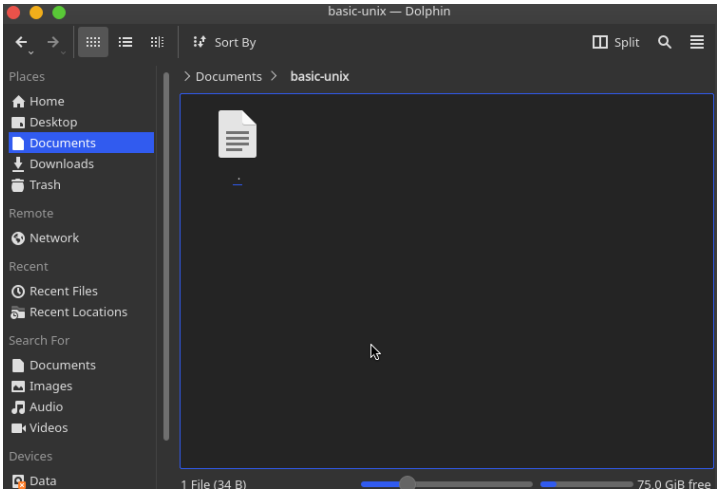
Setelah itu masukkan file ironman dan flag pun langsung didapatkan



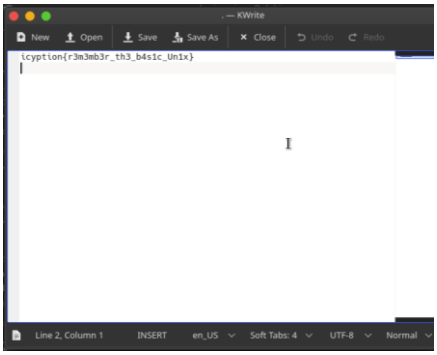
icyption{tony_stark-is-awesome_dude}

GENERAL (BASIC UNIX)

Pada challenge ini, disajikan satu buah file zip yang berjudul basic-unix.zip. Setelah diekstrak akan muncul tampilan sebagai berikut

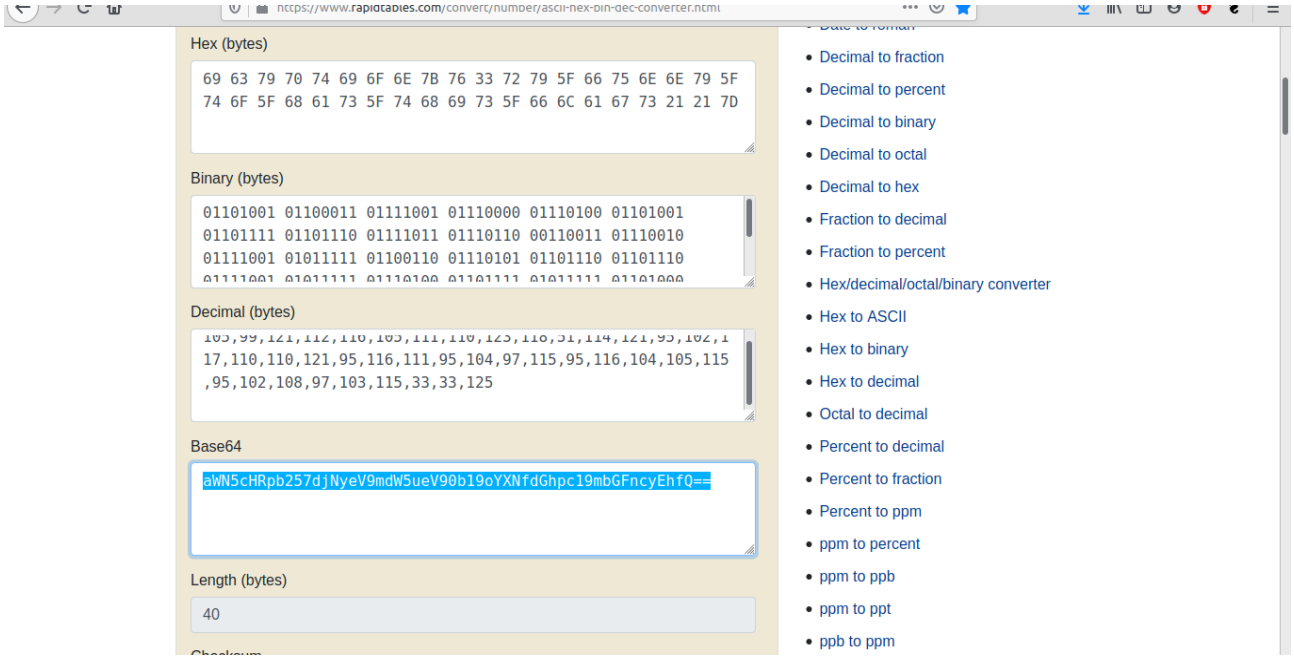


Setelah dibuka file hasil ekstraknya maka akan muncul flagnya

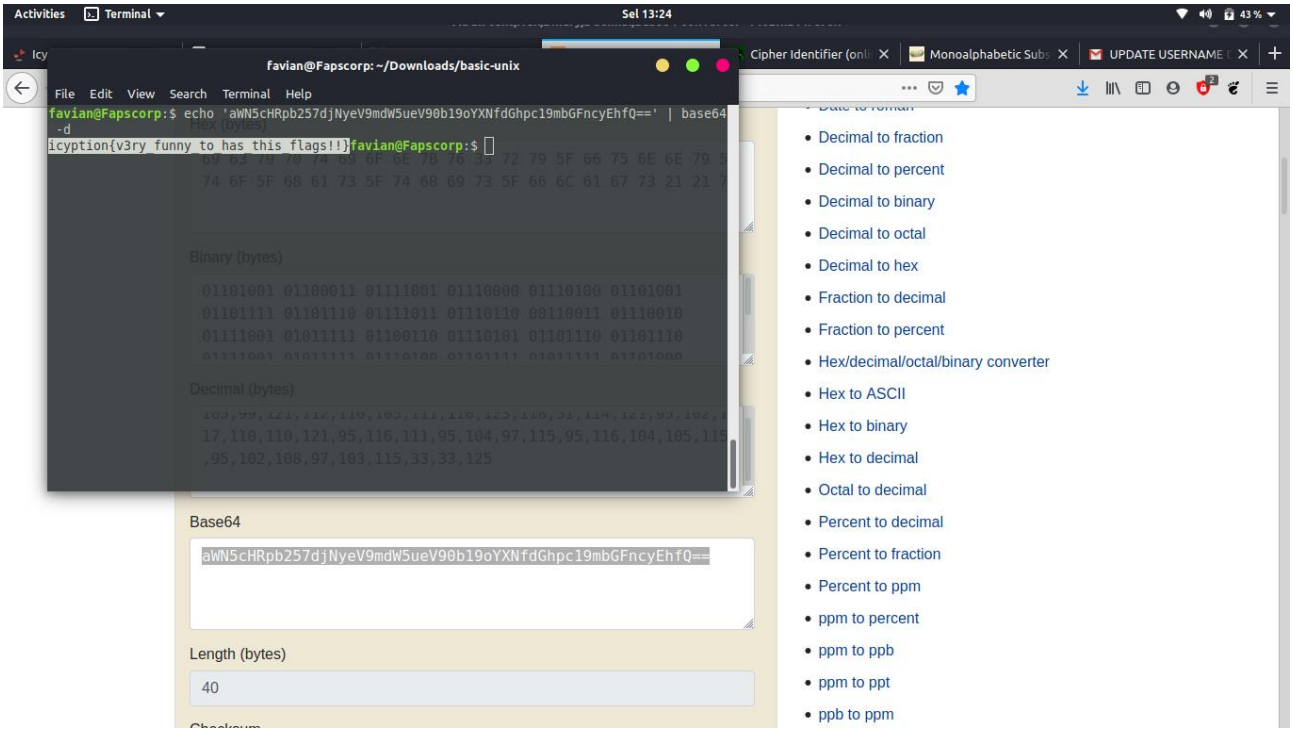


icyption{r3m3mb3r_th3_b4s1c_Un1x}

Any information about it ? (Encryption)



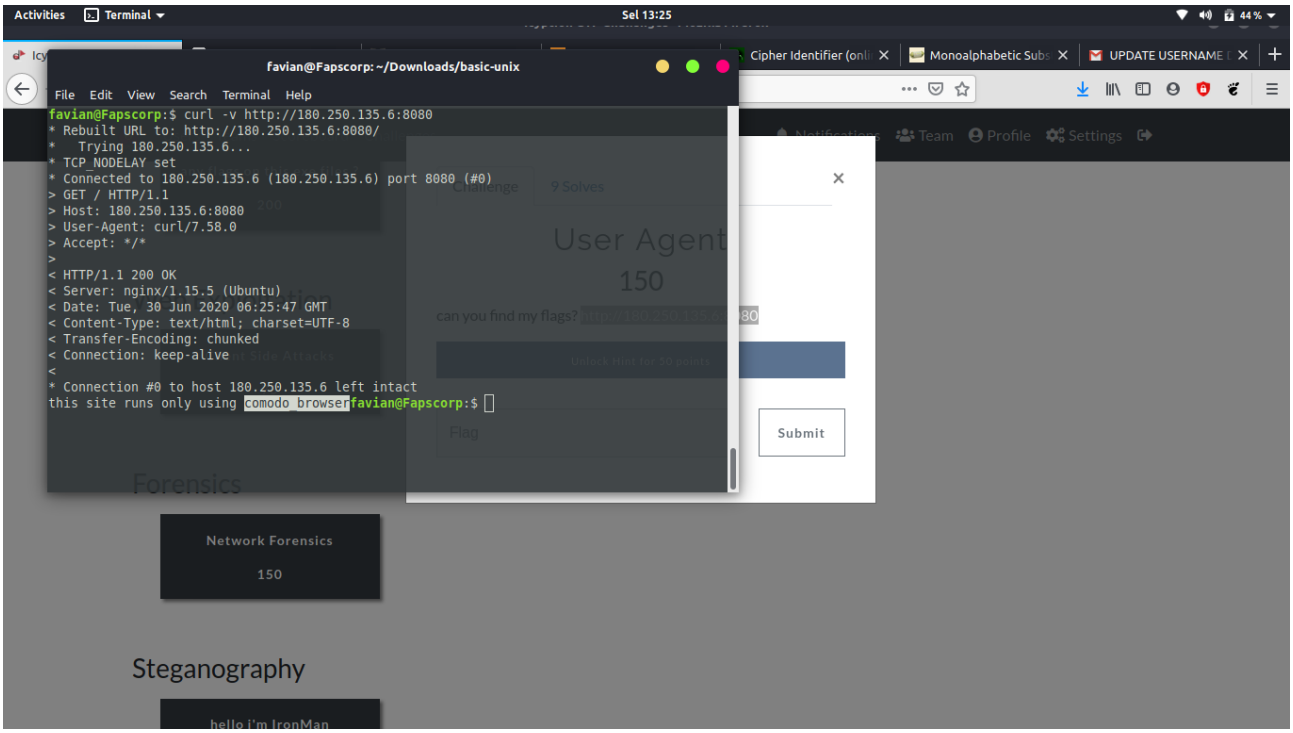
Mengcopy seluruh bilangan Decimal dan mengkonversinya menjadi ASCII. Setelah itu akan terlihat bahwa karakter ASCII tersebut merupakan Cipher Text Base64. Menggunakan aplikasi web **rapidtables.com**



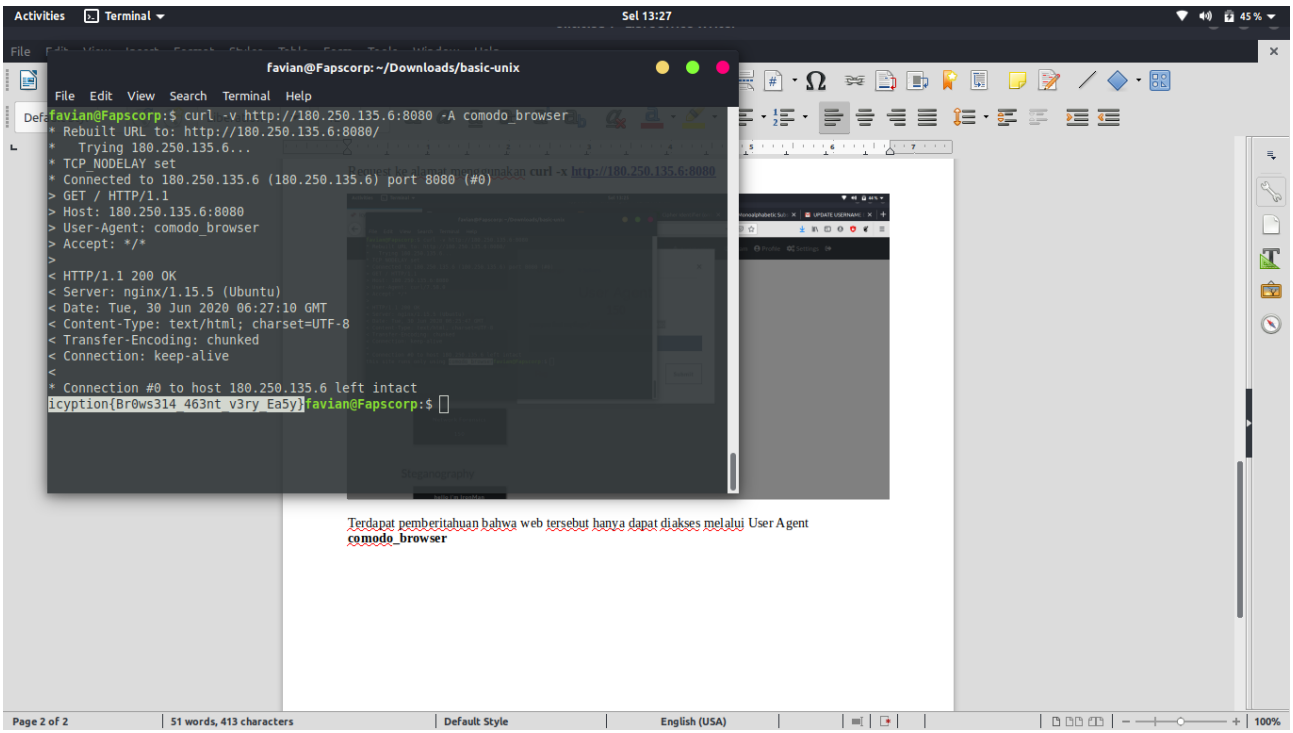
Setelah itu men-decode Base64. Dan flagnya pun akan muncul
icyption{v3ry_funny_to_has_this_flags!!}

User Agent (Web Exploit)

Request ke alamat menggunakan **curl -x http://180.250.135.6:8080**



Terdapat pemberitahuan bahwa web tersebut hanya dapat diakses melalui User Agent **comodo_browser**



Merequest web dengan User Agent **comodo_browser**. Dan flagnya-pun akan muncul.
icyption{Br0ws314_463nt_v3ry_Ea5y}