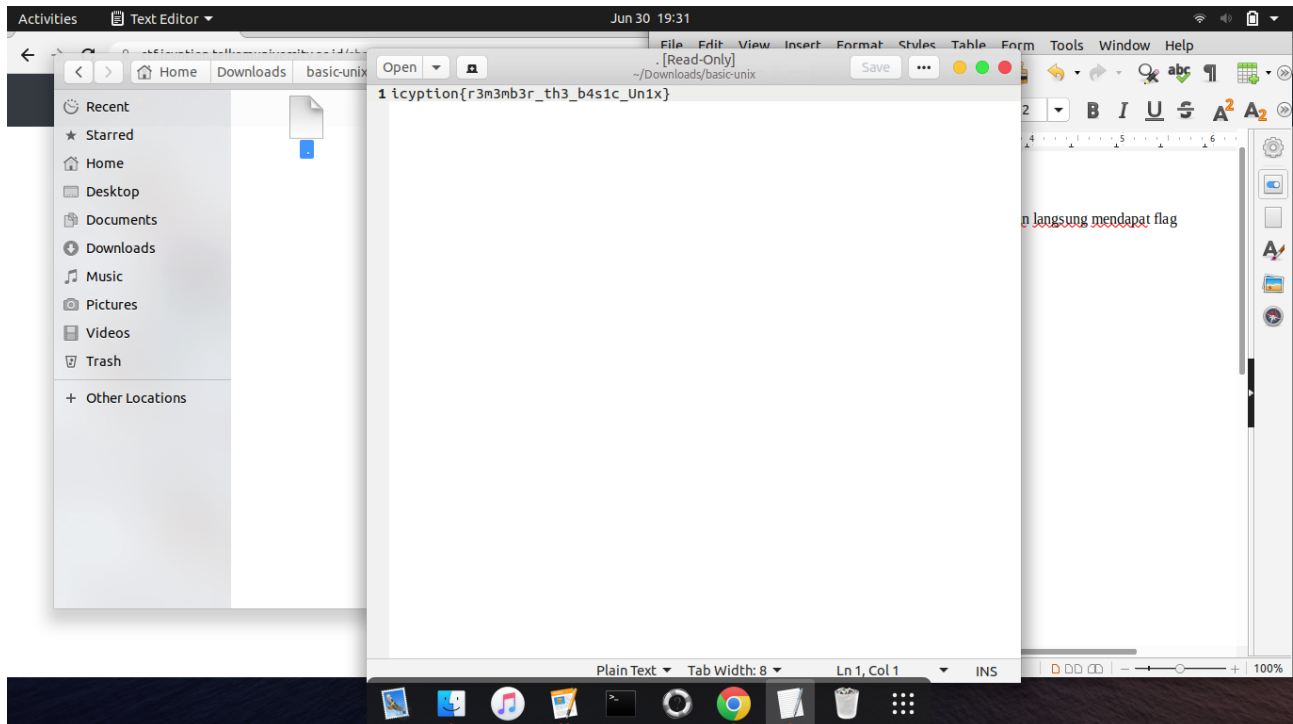


Write Up CTF iCryption Telkom University (Penyisihan)

SOAL 1 CTF

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

yaitu : `icryption{r3m3mb3r_th3_b4s1c_Un1x}`



SOAL 2 CTF

VjFaYWExUXdOVmhVYTJ4V1ltdEtjRIJYY0ZaTk1XUIIUVIZrYkdKSVFsWldNVkpEVkZaa1Ix
ZHFXbHBXYIUxNFdXMTBORMRIVmtsWApiV3hPVFVWck1WRXlZemxRVVc4OUNnPT0K

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

```
VjFaYWExUXdOVmhVYTJ4V1ltdEtjRIJYY0ZaTk1XUIIUVIZrYkdKSVFsWldNVkpEVkZaa1Ix  
ZHFXbHBXYIUxNFdXMTBORMRIVmtsWApiV3hPVFVWck1WRXlZemxRVVc4OUNnPT0K  
> base64.txt
```

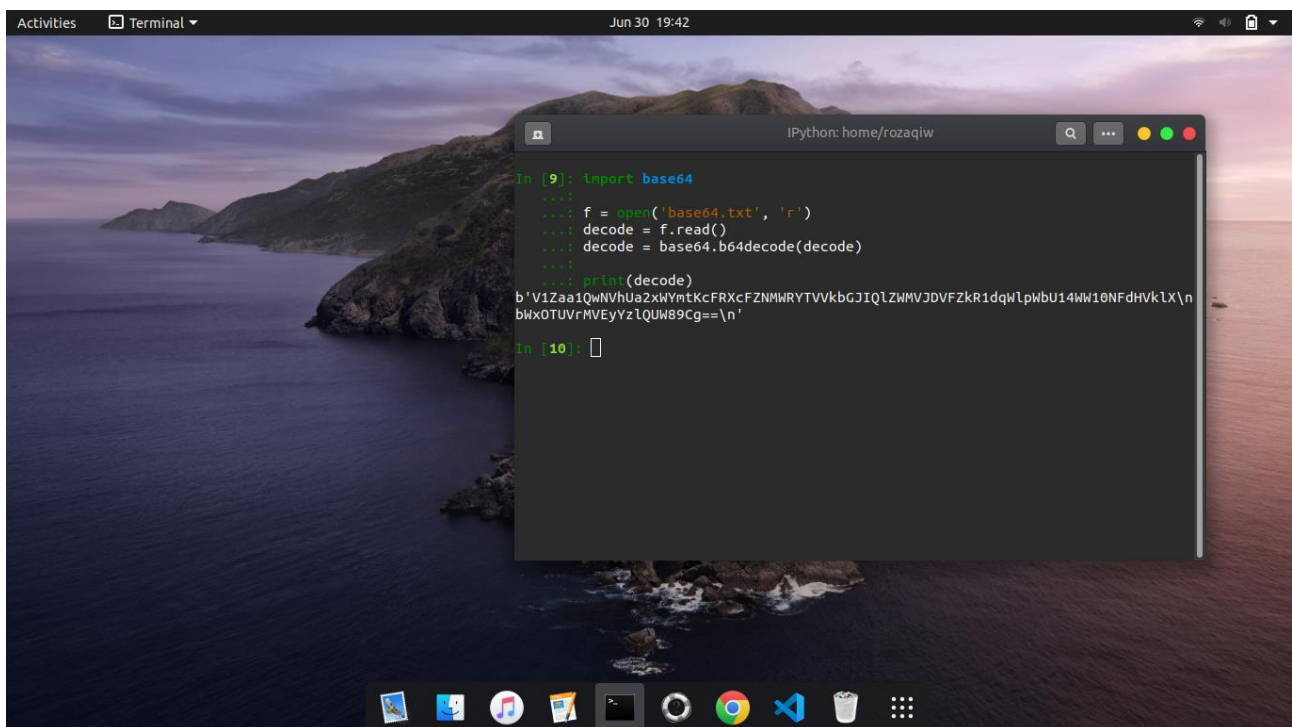
script ini saya coba untuk mendecode satu kali

```
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')
```

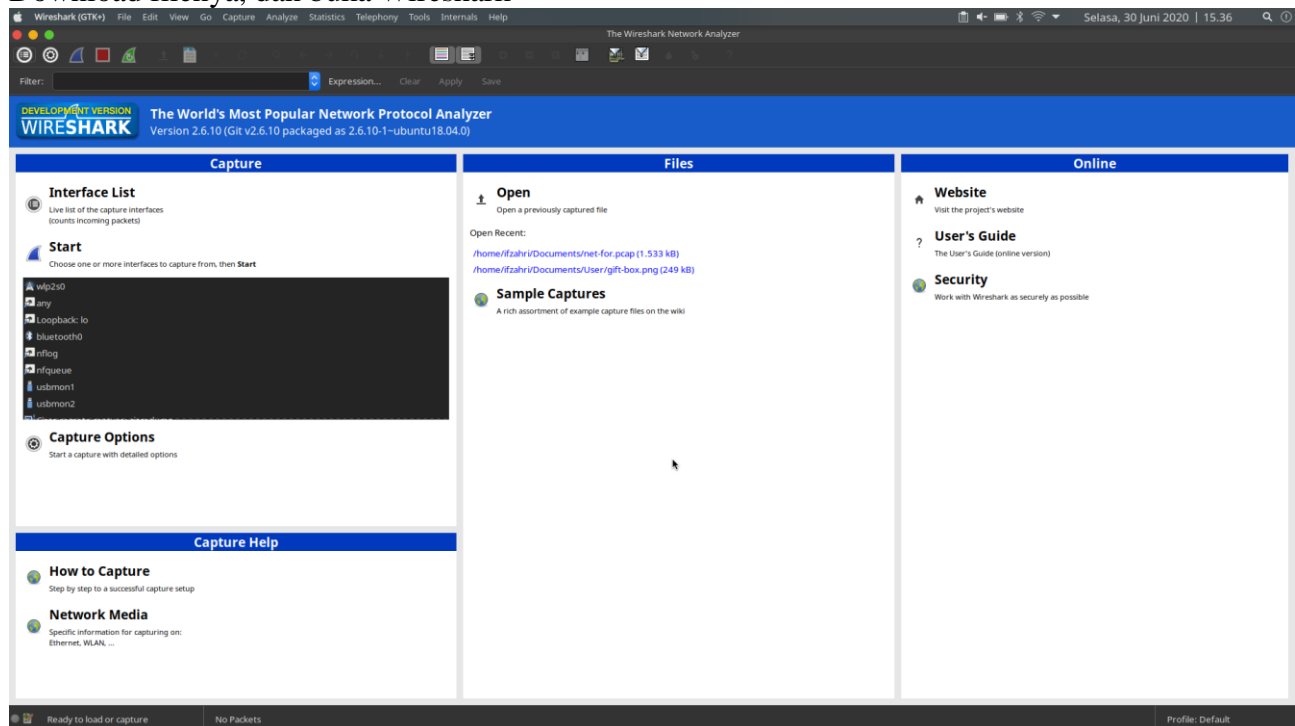
```
    if '{' in flag:
        print(flag)
        break
```

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

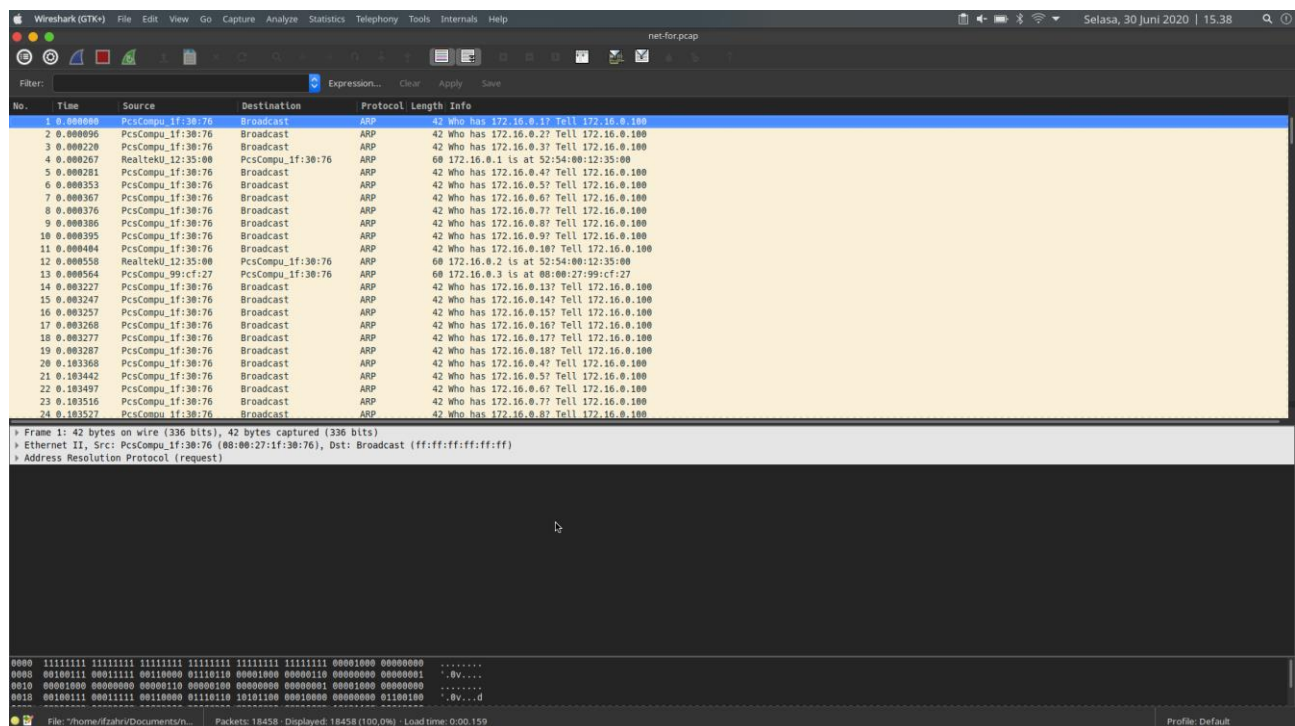
dapat flagnya yaitu : `icyption{hello-how-are-you-toow}`

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**

Wireshark: Protocol Hierarchy Statistics

Display filter: none

Protocol	% Packets	Packets	% Bytes	Bytes	Mbit/s	End Packets	End Bytes	E
▼ Frame	100,00 %	18458	100,00 %	1237756	0,059	0	0	
▼ Ethernet	100,00 %	18458	20,88 %	258412	0,012	0	0	
Address Resolution Protocol	5,55 %	1024	2,32 %	28672	0,001	1024	28672	
▼ Internet Protocol Version 4	94,45 %	17434	28,17 %	348680	0,017	0	0	
▼ Transmission Control Protocol	83,20 %	15357	39,41 %	487744	0,023	15338	485680	
Virtual Network Computing	0,01 %	2	0,00 %	24	0,000	2	24	
File Transfer Protocol (FTP)	0,02 %	4	0,01 %	75	0,000	4	0	
Data	0,07 %	13	0,11 %	1357	0,000	13	1357	
▼ User Datagram Protocol	0,11 %	21	0,01 %	168	0,000	0	0	
Domain Name System	0,11 %	20	0,13 %	1602	0,000	20	1602	
▼ NetBIOS Datagram Service	0,01 %	1	0,02 %	244	0,000	0	0	
▼ SMB (Server Message Block Protocol)	0,01 %	1	0,01 %	162	0,000	0	0	
▼ SMB MailSlot Protocol	0,01 %	1	0,00 %	25	0,000	0	0	
Microsoft Windows Browser Protocol	0,01 %	1	0,01 %	76	0,000	1	76	

Help Close

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

Wireshark (GTK+) File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

net-for-pcap

Filter: data and tcp and seq and eth and frame Expression... Clear Apply Save

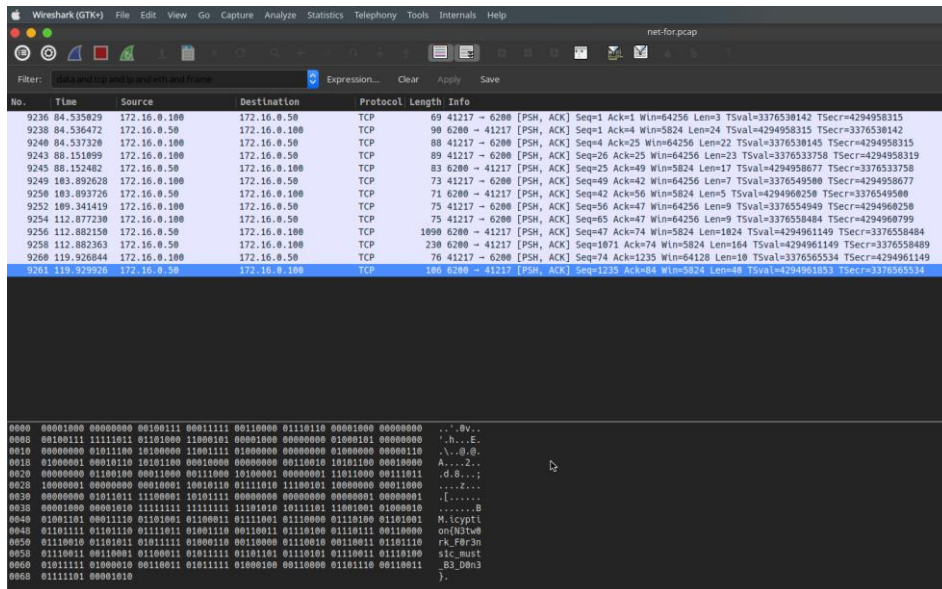
No.	Time	Source	Destination	Protocol	Length	Info
9236	84.535829	172.16.0.100	172.16.0.50	TCP	60	41217 → 6200 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=3 TSval=3376538142 TSecr=4294958315
9238	84.536472	172.16.0.50	172.16.0.100	TCP	98	6200 → 41217 [PSH, ACK] Seq=1 Ack=4 Win=5824 Len=24 TSval=4294958315 TSecr=3376538142
9240	84.537338	172.16.0.100	172.16.0.50	TCP	80	41217 → 6200 [PSH, ACK] Seq=4 Ack=25 Win=64256 Len=22 TSval=3376538145 TSecr=4294958315
9243	88.151099	172.16.0.100	172.16.0.50	TCP	89	41217 → 6200 [PSH, ACK] Seq=26 Ack=25 Win=64256 Len=23 TSval=3376533758 TSecr=4294958319
9245	88.152482	172.16.0.50	172.16.0.100	TCP	83	6200 → 41217 [PSH, ACK] Seq=25 Ack=49 Win=5824 Len=17 TSval=4294958677 TSecr=3376533758
9249	103.892628	172.16.0.100	172.16.0.50	TCP	73	41217 → 6200 [PSH, ACK] Seq=49 Ack=42 Win=64256 Len=7 TSval=3376549580 TSecr=4294958677
9250	103.893726	172.16.0.50	172.16.0.100	TCP	71	6200 → 41217 [PSH, ACK] Seq=42 Ack=56 Win=5824 Len=5 TSval=4294960258 TSecr=3376549580
9252	109.241419	172.16.0.100	172.16.0.50	TCP	75	41217 → 6200 [PSH, ACK] Seq=56 Ack=47 Win=64256 Len=9 TSval=3376554949 TSecr=4294960258
9254	112.877230	172.16.0.100	172.16.0.50	TCP	75	41217 → 6200 [PSH, ACK] Seq=65 Ack=47 Win=64256 Len=9 TSval=3376558484 TSecr=4294960799
9256	112.882150	172.16.0.50	172.16.0.100	TCP	1090	6200 → 41217 [PSH, ACK] Seq=47 Ack=74 Win=5824 Len=1024 TSval=4294961149 TSecr=3376558484
9258	112.882363	172.16.0.50	172.16.0.100	TCP	230	6200 → 41217 [PSH, ACK] Seq=1071 Ack=74 Win=5824 Len=164 TSval=4294961149 TSecr=3376558489
9260	119.926844	172.16.0.100	172.16.0.50	TCP	76	41217 → 6200 [PSH, ACK] Seq=74 Ack=1235 Win=64128 Len=18 TSval=3376565534 TSecr=4294961149
9261	119.929926	172.16.0.50	172.16.0.100	TCP	186	6200 → 41217 [PSH, ACK] Seq=1235 Ack=84 Win=5824 Len=48 TSval=4294961853 TSecr=3376565534

Frame 9236: 60 bytes on wire (552 bits), 60 bytes captured (552 bits) on interface 0
 Ethernet II, Src: PcsCompu_1f:30:76 (08:00:27:1f:30:76), Dst: PcsCompu_fb:68:c5 (08:00:27:fb:68:c5)
 Internet Protocol Version 4, Src: 172.16.0.100, Dst: 172.16.0.50
 Transmission Control Protocol, Src Port: 41217, Dst Port: 6200, Seq: 1, Ack: 1, Len: 3
 Data (3 bytes)

0000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 ..h..
 0000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 ..v..
 0010 00000000 00000000 00000000 00000000 00000000 00000000 00000000 ..7..
 0010 00000000 00000000 00000000 00000000 00000000 00000000 00000000 ..d..

File: /home/fzahr/Documents/net-for-pcap Packets: 18458 - Displayed: 13 (0.1%) - Load time: 0:00:455 Profile: Default

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



icyption{N3tw0rk_F0r3ns1c_must_B3_D0n3}

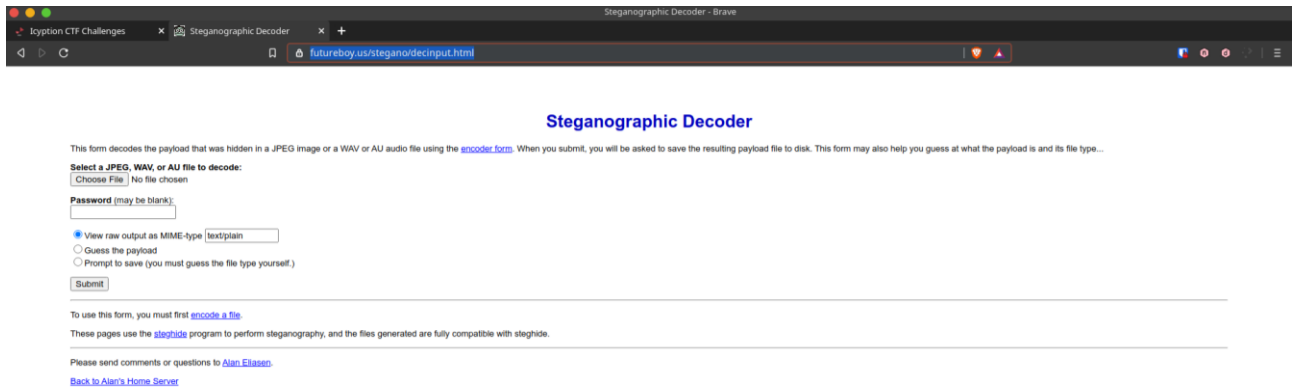
Masukkan saja ke bagian submit dan flag diterima.

STEGANOGRAPHY

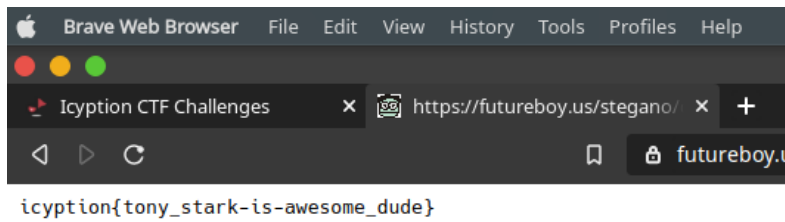
Download filenya yang bernama **ironman.jpeg**, kalau dibuka maka gambarnya seperti ini



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



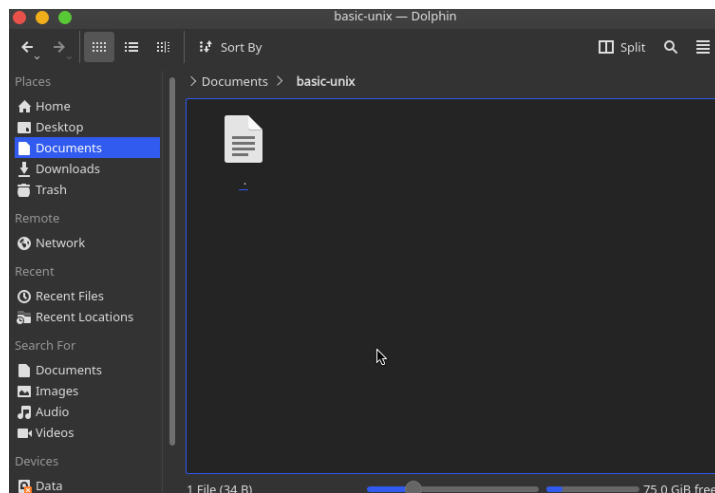
Setelah itu masukkan file ironman dan flag pun langsung didapatkan



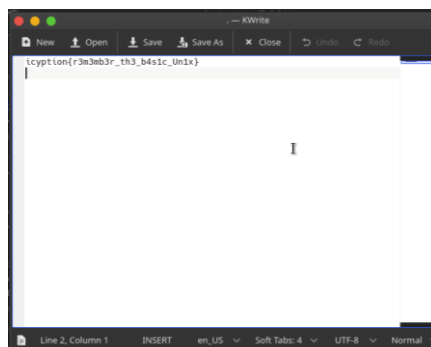
icyption{tony_stark-is-awesome_dude}

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



icryption{r3m3mb3r_th3_b4s1c_Un1x}

Any information about it ? (Encryption)

The screenshot shows the RapidTables.com converter tool. The 'Base64' input field contains the string: `aWN5cHRpb257djNyeV9mdw5ueV90b19oYXNfdGhpc19mbGFncyEhfQ==`. The 'Length (bytes)' field shows 40. The 'Decimal (bytes)' field displays a list of decimal values: 103, 99, 121, 112, 110, 103, 111, 110, 123, 110, 51, 114, 121, 93, 102, 17, 110, 110, 121, 95, 116, 111, 95, 104, 97, 115, 95, 116, 104, 105, 115, 95, 102, 108, 97, 103, 115, 33, 33, 125. The 'Hex (bytes)' field displays the corresponding hexadecimal values: 69 63 79 70 74 69 66 6E 7B 76 33 72 79 5F 66 75 6E 6E 79 5F 74 66 5F 68 61 73 5F 74 68 69 73 5F 66 6C 61 67 73 21 21 7D. The 'Binary (bytes)' field displays the corresponding binary values: 01101001 01100011 01111001 01110000 01110100 01101001 01101111 01101110 01111011 01110110 00110011 01110010 01111001 01011111 01100110 01110101 01101110 01101110 01111001 01011111 01110100 01101111 01011111 01101000.

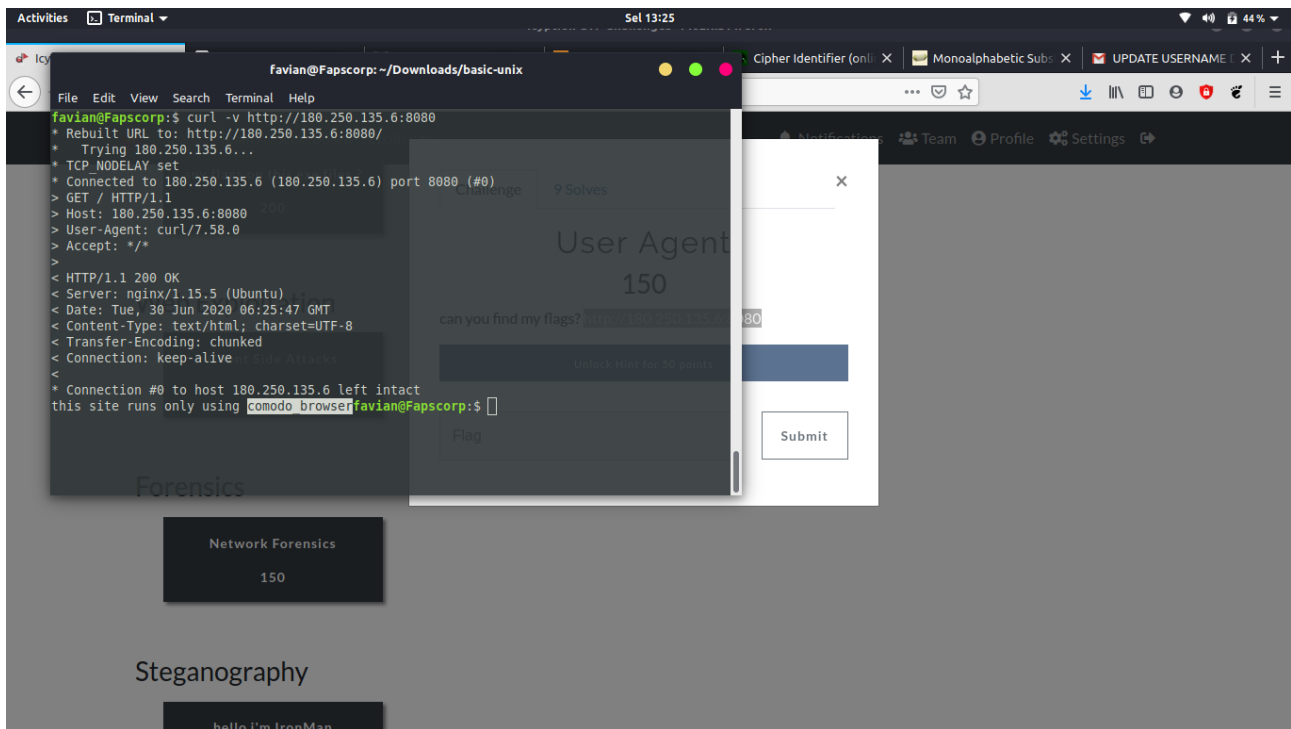
Mengcopy seluruh bilangan Decimal dan mengkonversinya menjadi ASCII. Setelah itu akan terlihat bahwa karakter ASCII tersebut merupakan Cipher Text Base64. Menggunakan aplikasi web **rapidtables.com**

The screenshot shows a terminal window and the RapidTables.com converter tool. The terminal window displays the command: `icryption{v3ry funny to has this flags!!}favian@Fapscorp:$`. The RapidTables.com converter tool shows the same Base64 string as the previous screenshot, with the 'Decimal (bytes)' field displaying the same list of decimal values: 103, 99, 121, 112, 110, 103, 111, 110, 123, 110, 51, 114, 121, 93, 102, 17, 110, 110, 121, 95, 116, 111, 95, 104, 97, 115, 95, 116, 104, 105, 115, 95, 102, 108, 97, 103, 115, 33, 33, 125.

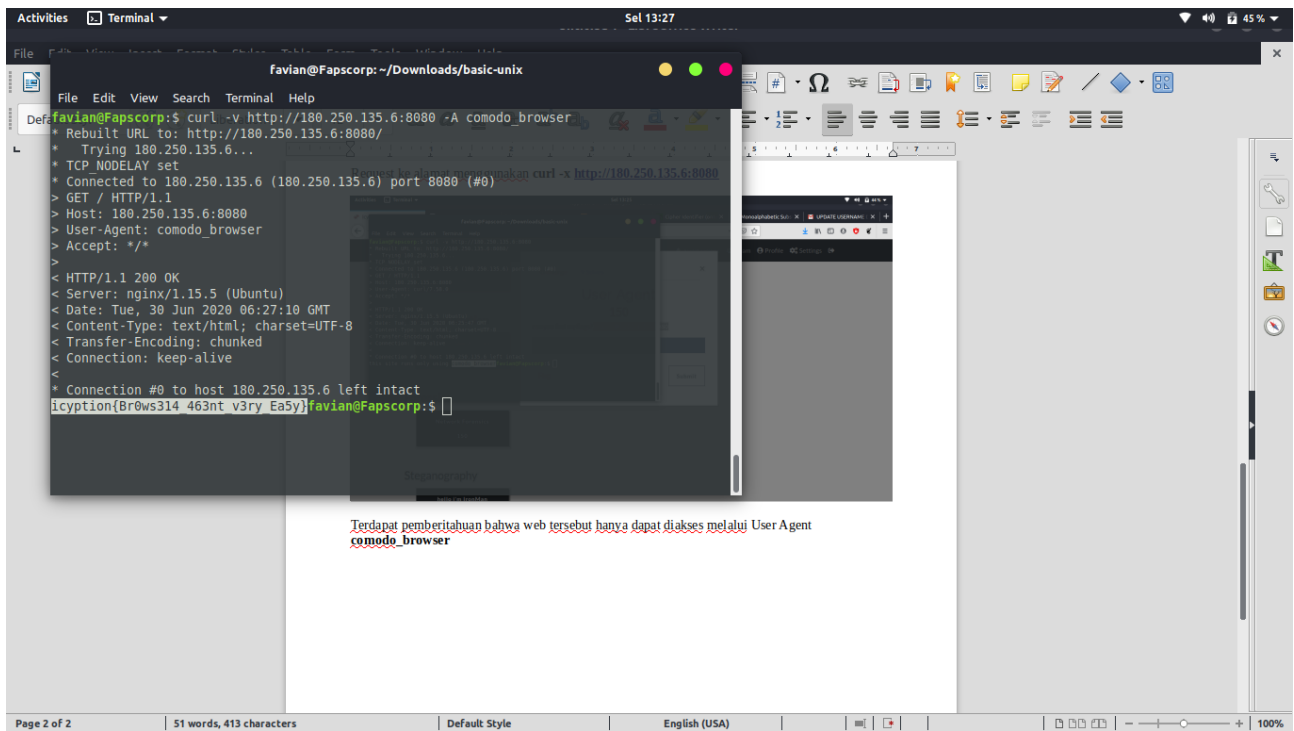
Setelah itu men-decode Base64. Dan flagnya pun akan muncul
icyption{v3ry_funny_to_has_this_flags!!}

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}