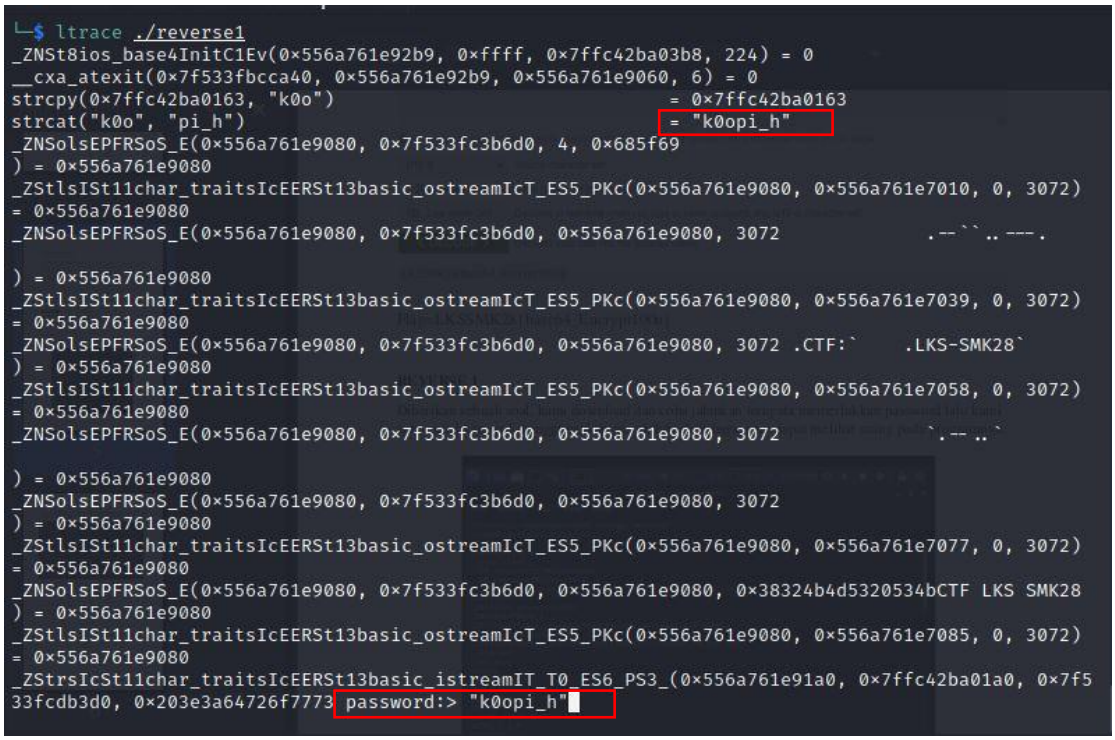
REZKA NORHAFIZAH

WRITE UP

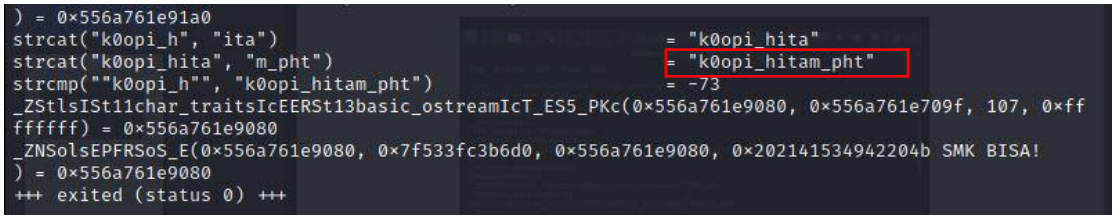
REVERSE 1

Diberikan sebuah soal, kemudian saya coba jalankan tetapi ternyata ketika dibuka terlihat bahwa akses ditolak. Lalu saya ketikkan **chmod +x reverse**1 untuk mengubah hak akses file.

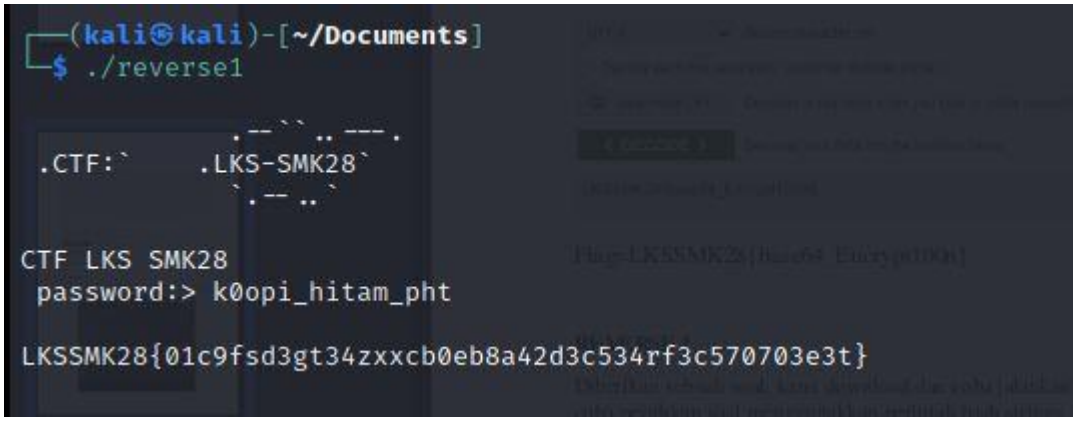
Kemudian, saya coba jalankan lagi tetapi ternyata memerlukan password. Setelah itu, saya menggunakan tool yang bernama ltrace seperti berikut :



Lalu diminta untuk memasukkan sebuah inputan, saya coba ketikkan **“k0pi_h”** sesuai yang tertera di atas, dan didapat password untuk file :



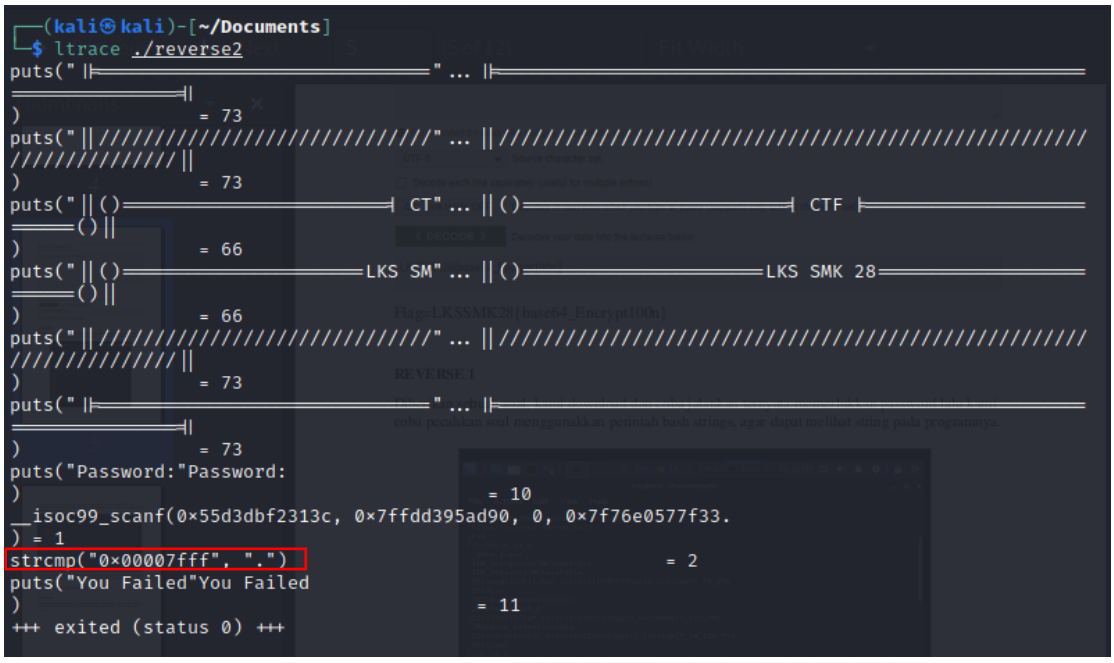
Kemudian saya coba jalankan lagi menggunakan passsword tersebut dan didapat :



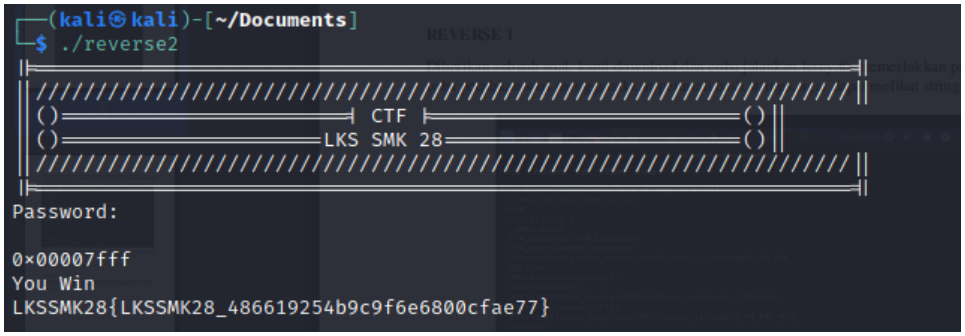
Flag = LKSSMK28{01c9fsd3gt34zxxcb0eb8a42d3c534rf3c570703e3t}

REVERSE 2

Diberikan sebuah soal, kemudian saya lakukan hal yang sama seperti yang saya lakukan untuk reverse1, ternyata diminta memasukkan password. Lalu saya menggunakan tool ltrace dan didapat password :



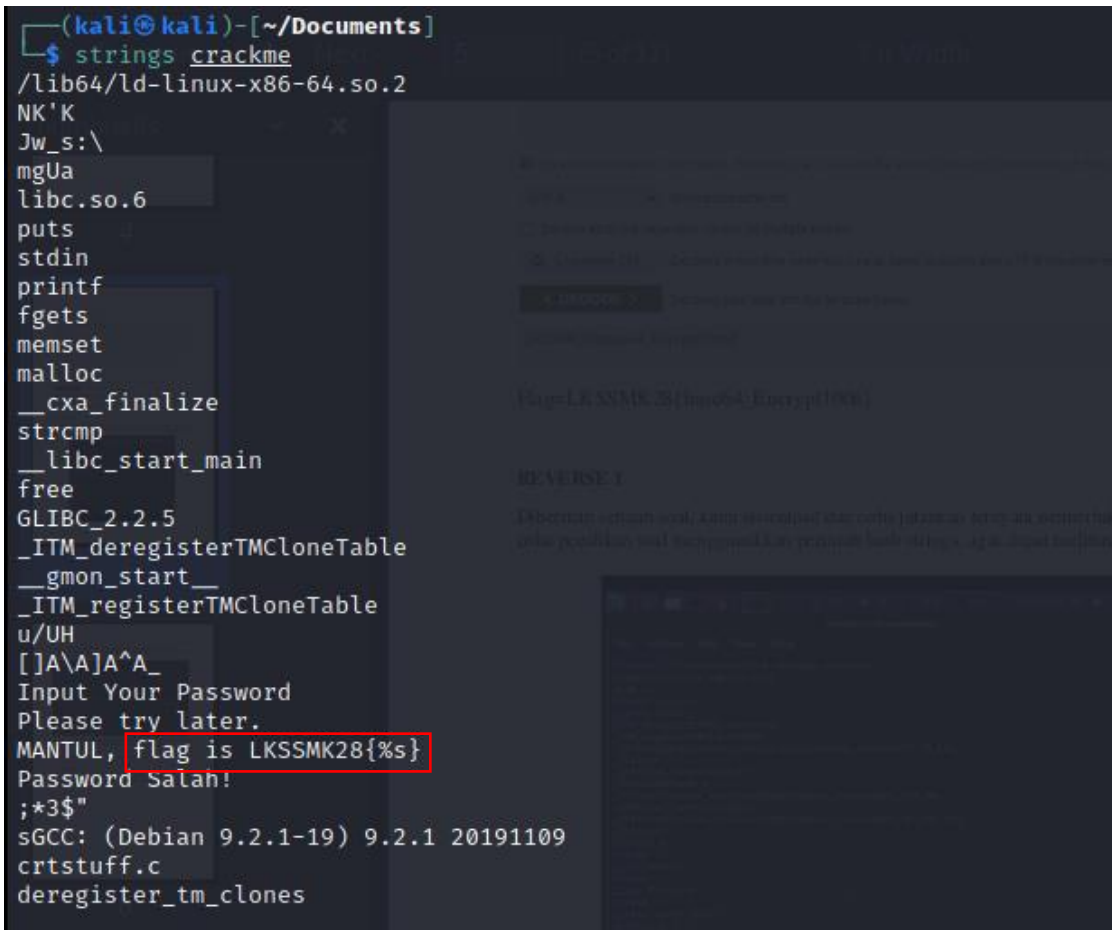
Kemudian saya coba jalankan lagi file tersebut dan saya masukkan password dan didapatkan flagnya :



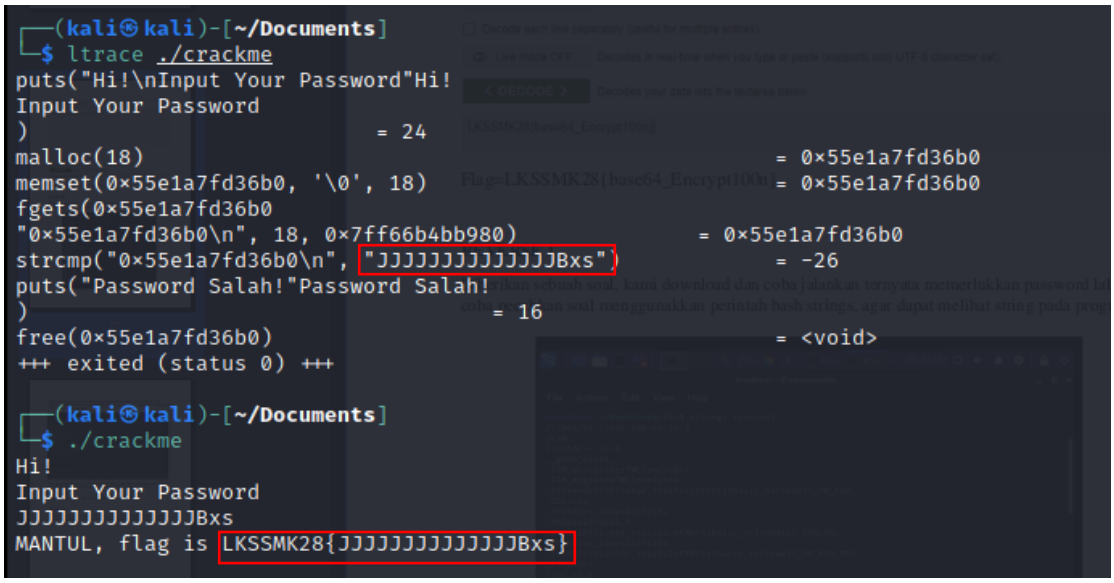
Flag = LKSSMK28{LKSSMK28_486619254b9c9f6e6800cfae77}

CRACKME

Diberikan soal, lalu saya coba jalankan tetapi menggunakan password. Kemudian saya coba menggunakan perintah strings dan didapat clue :



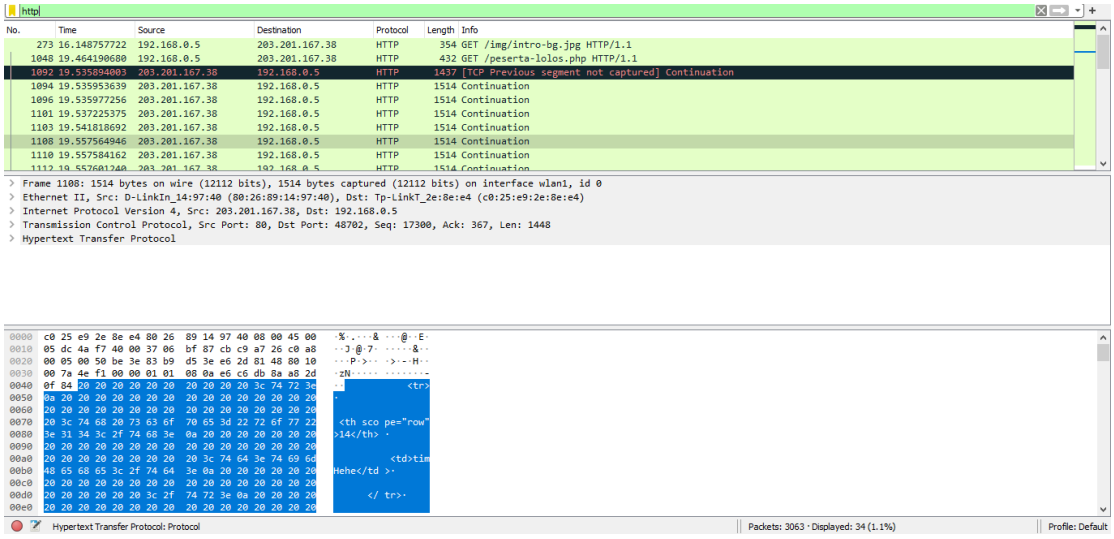
Kemudian saya menggunakan tool ltrace dan didapat :



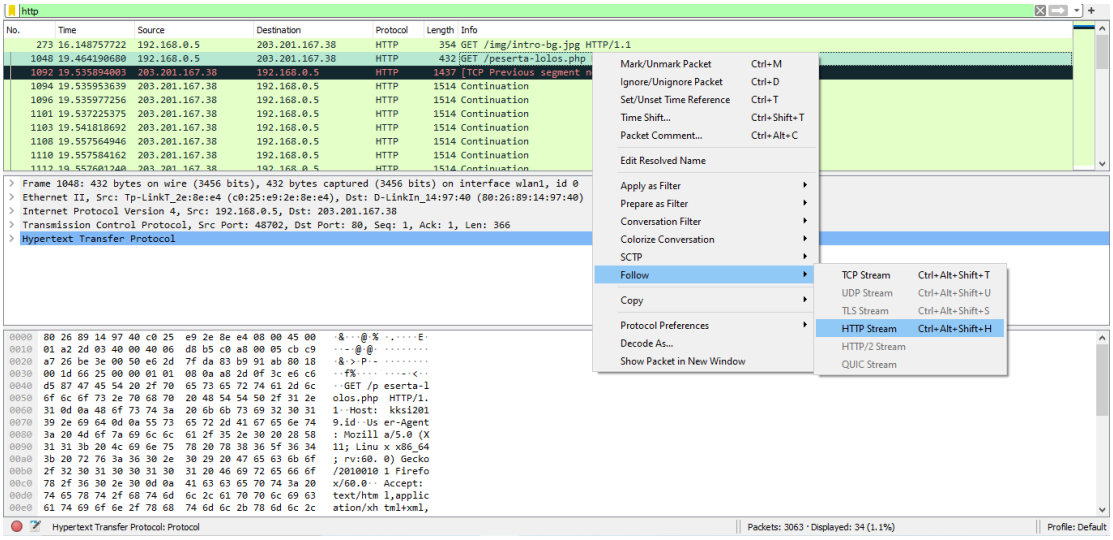
Selanjutnya, saya jalankan lagi filenya dan didapat :
Flag = LKSSMK28{JJJJJJJJJJJJJJBxs}

PASS.PCAPNG

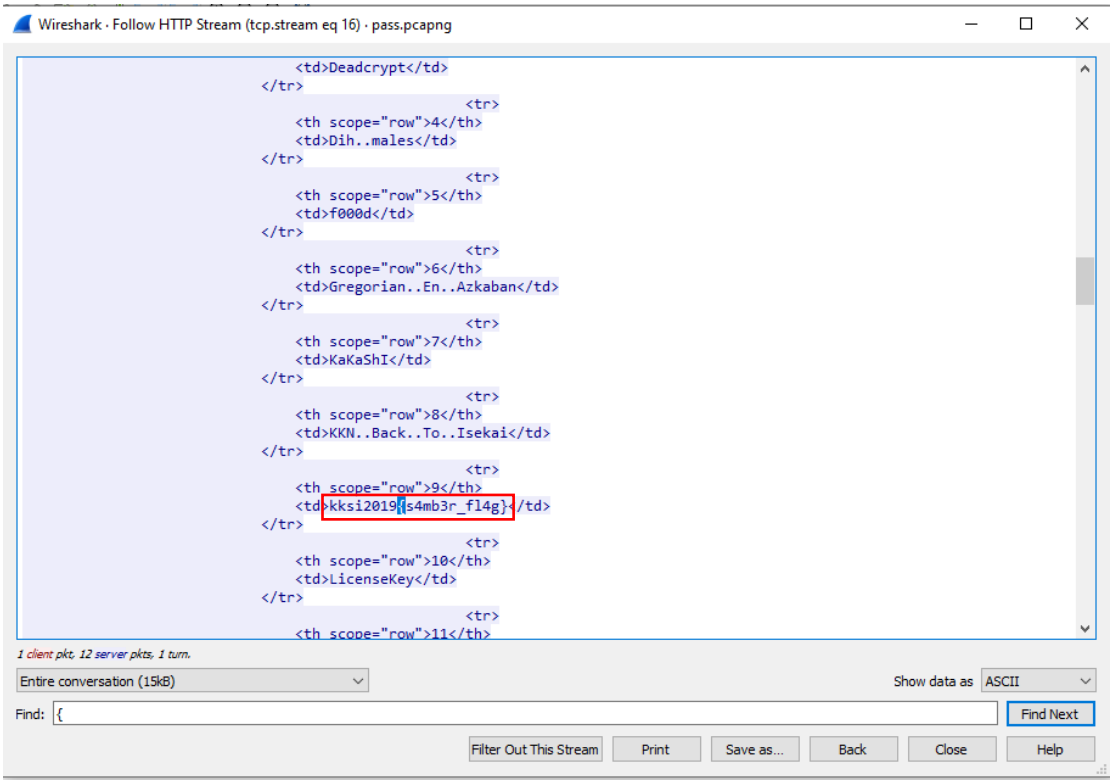
Diberikan soal, lalu saya buka menggunakan aplikasi wireshark kemudian saya lakukan filter packet HTTP seperti berikut :



Setelah itu saya lakukan follow http stream pada packet :



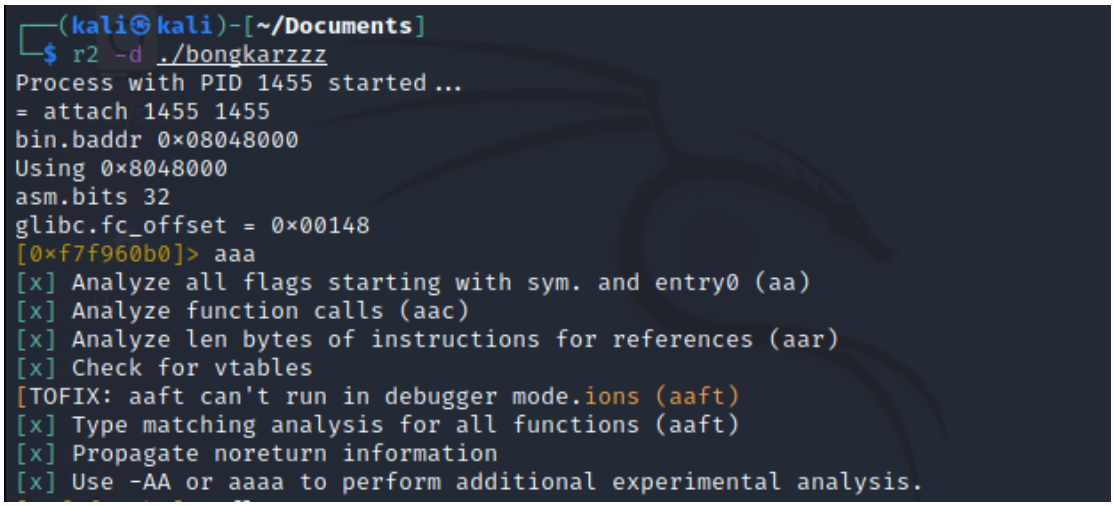
Dan didapat flag :



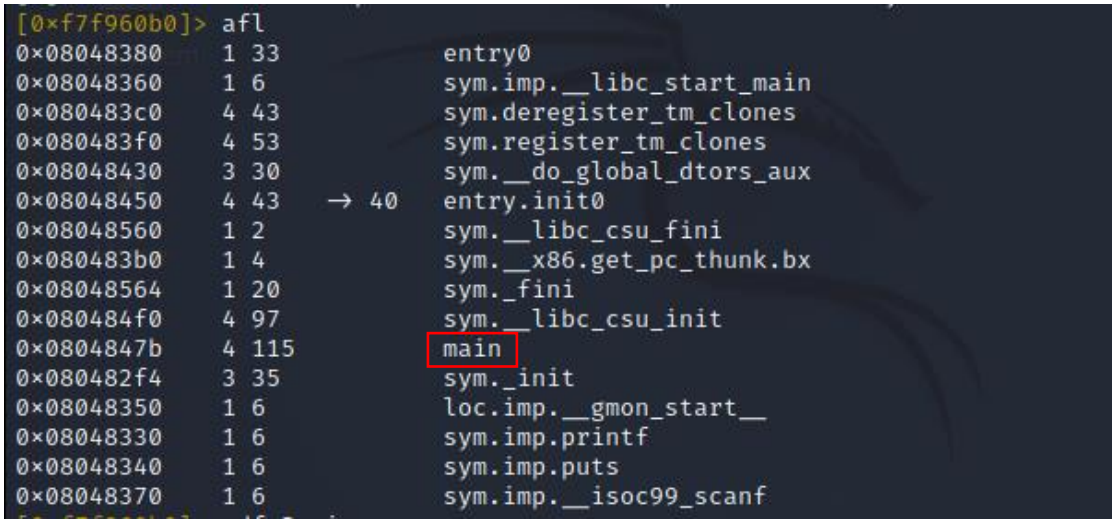
Flag = kks2019{s4mb3r_fl4g}

BONGKARZZZ

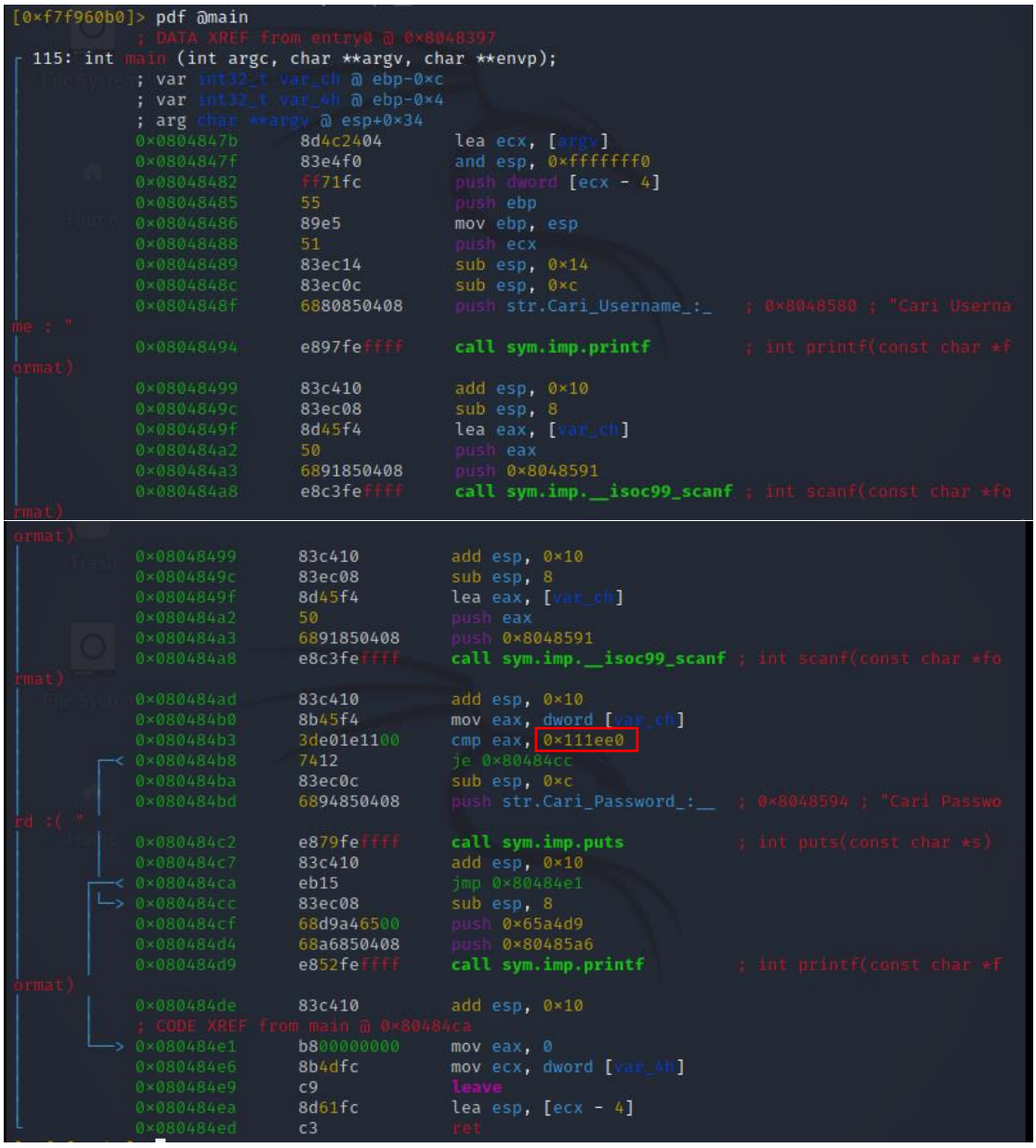
Diberikan file, lalu saya coba buka ternyata diperlukan username dan password. Kemudian saya mencari username dan password untuk file tersebut. Saya coba menggunakan perintah strings tetapi tidak kunjung ditemukan juga. Selanjutnya saya coba menggunakan radare2 dan saya lakukan analyze terhadap file.



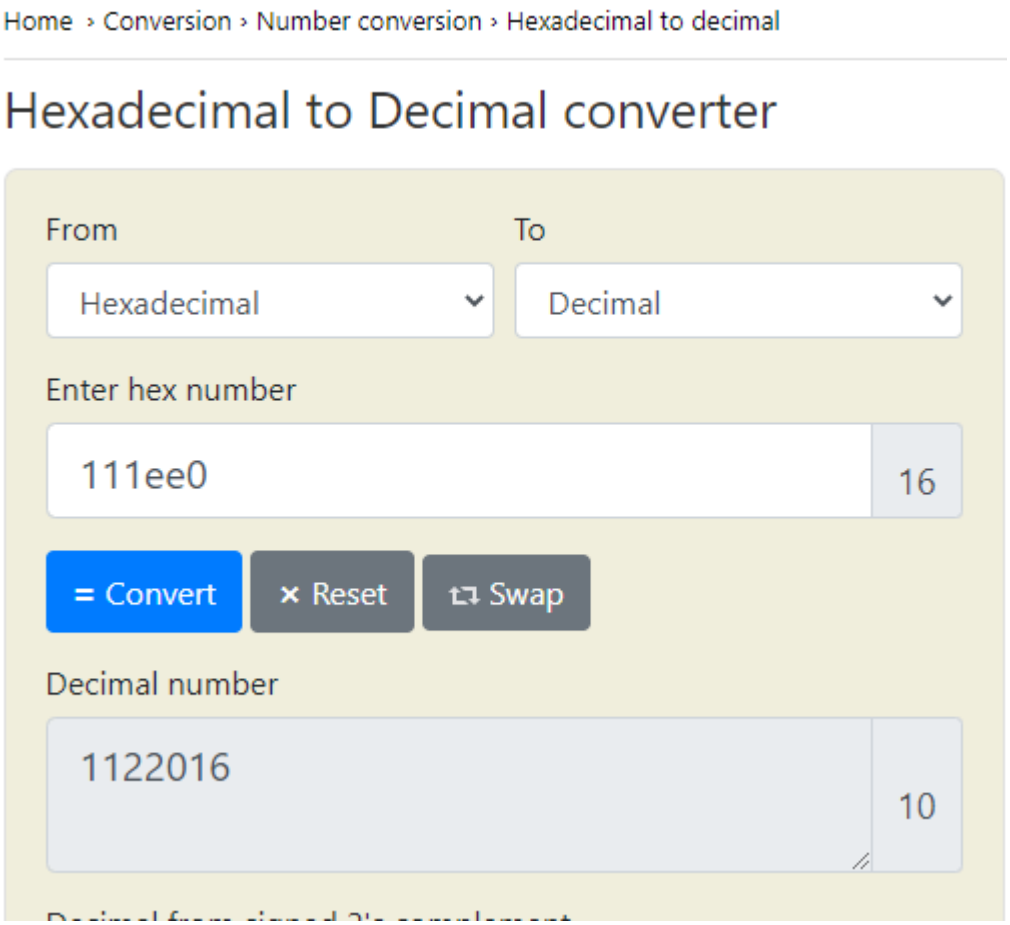
Lalu, untuk melihat list function saya ketikkan afl dan disana terlihat ada main function.



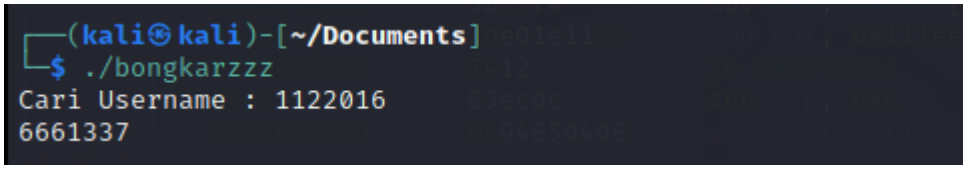
Lalu saya menemukan nilai pembandingnya :



Dan saya konversikan nilai pembanding tersebut ke desimal :



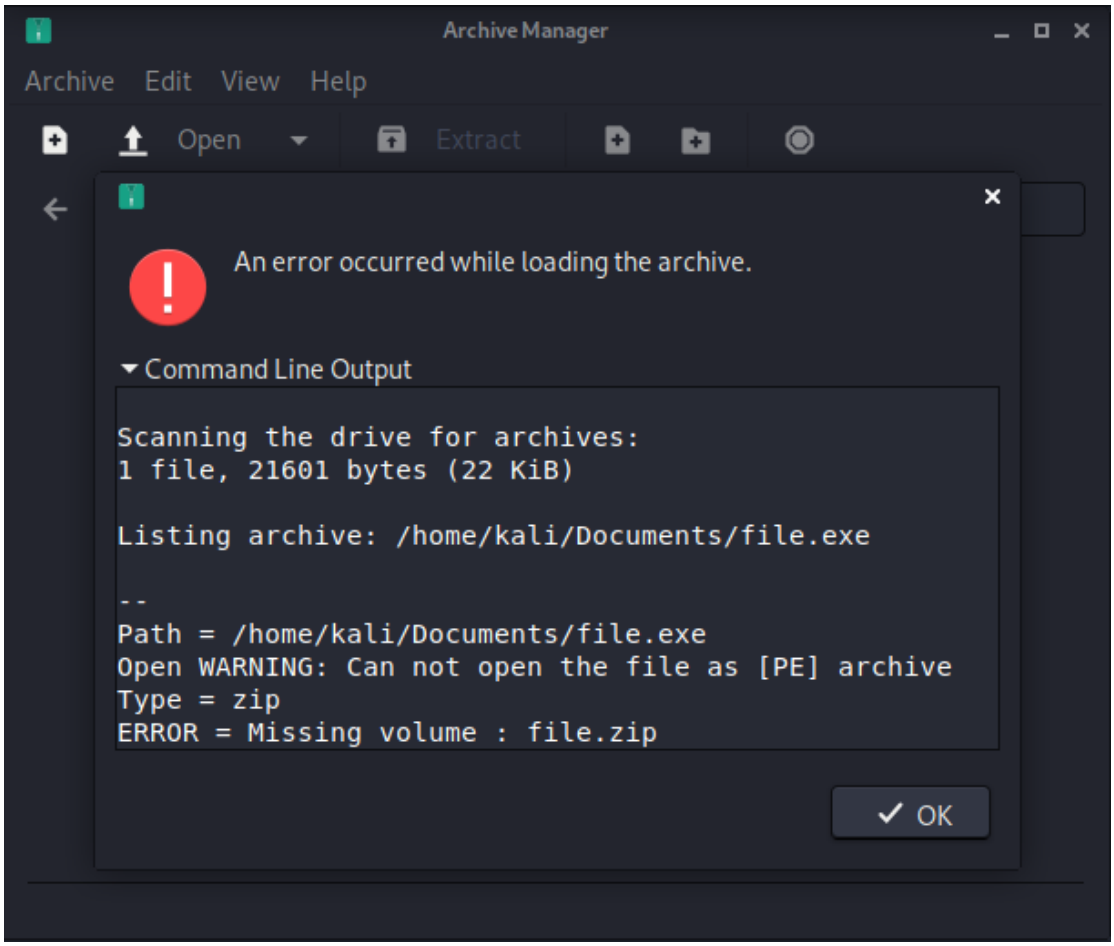
Saya coba angka tersebut untuk username dan ternyata didapat password nya juga :



Username : 1122016
Password : 6661337

FILE.EXE

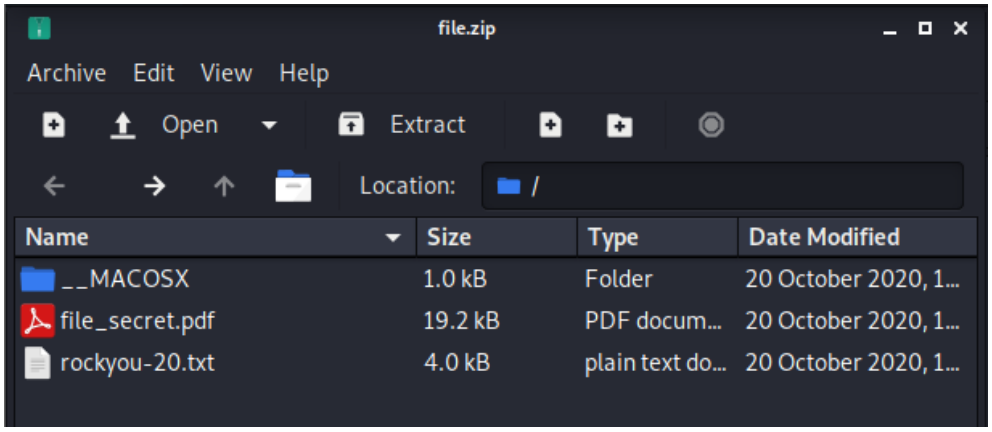
Setelah diberikan file, saya coba buka tetapi ternyata didapat error seperti berikut :



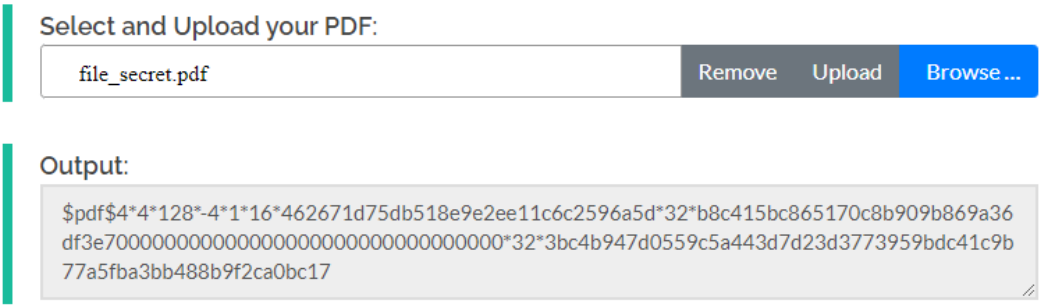
Dari gambar di atas dapat dilihat terdapat hint yang menunjukkan bahwa file tersebut adalah file dengan ekstensi zip, maka saya ubah nama file tersebut ke file.zip :

```
┌──(kali㉿kali)-[~/Documents]
└─$ mv file.exe file.zip
```

Lalu saya coba buka dan ternyata ada dua file yang tersimpan di sana yaitu sebagai berikut :



Diberikan sebuah file pdf yang terkunci dengan password dan sebuah file wordlist. Kemudian langsung saja saya brute force dengan John The Ripper :

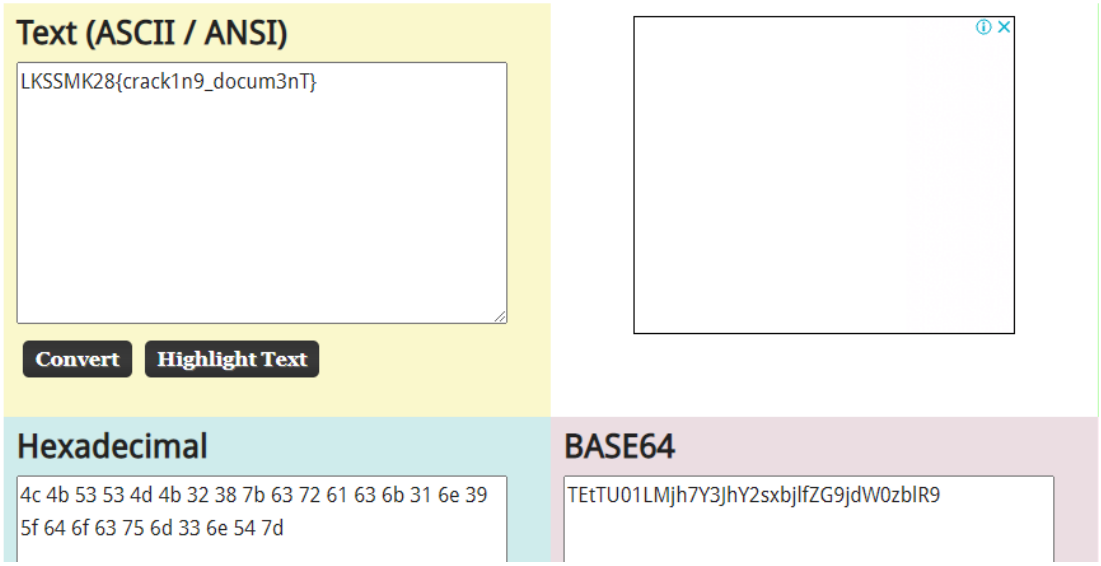



```
┌──(root💀kali)-[/home/kali/mnt/LKSN 2021]
└─# john --wordlist=rockyou-20.txt pdf.txt
Using default input encoding: UTF-8
Loaded 1 password hash (PDF [MD5 SHA2 RC4/AES 32/64])
Cost 1 (revision) is 4 for all loaded hashes
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
hellokitty       (?)
1g 0:00:00:00 DONE (2021-10-23 22:18) 20.00g/s 5120p/s 5120c/s 5120C/s 123456..angelo
Use the "--show --format=PDF" options to display all of the cracked passwords reliably
Session completed
```

Didapat password nya yaitu “hellokitty” lalu saya buka dokumennya dan muncul hint lagi berupa base64 :

TEtTU01LMjh7Y3JhY2sxbjlfZG9jdW0zblR9==

Base64 tersebut saya konversi ke ascii dan didapat flag :



Flag = LKSSMK28{crack1n9_docum3nT}