REZKA NORHAFIZAH

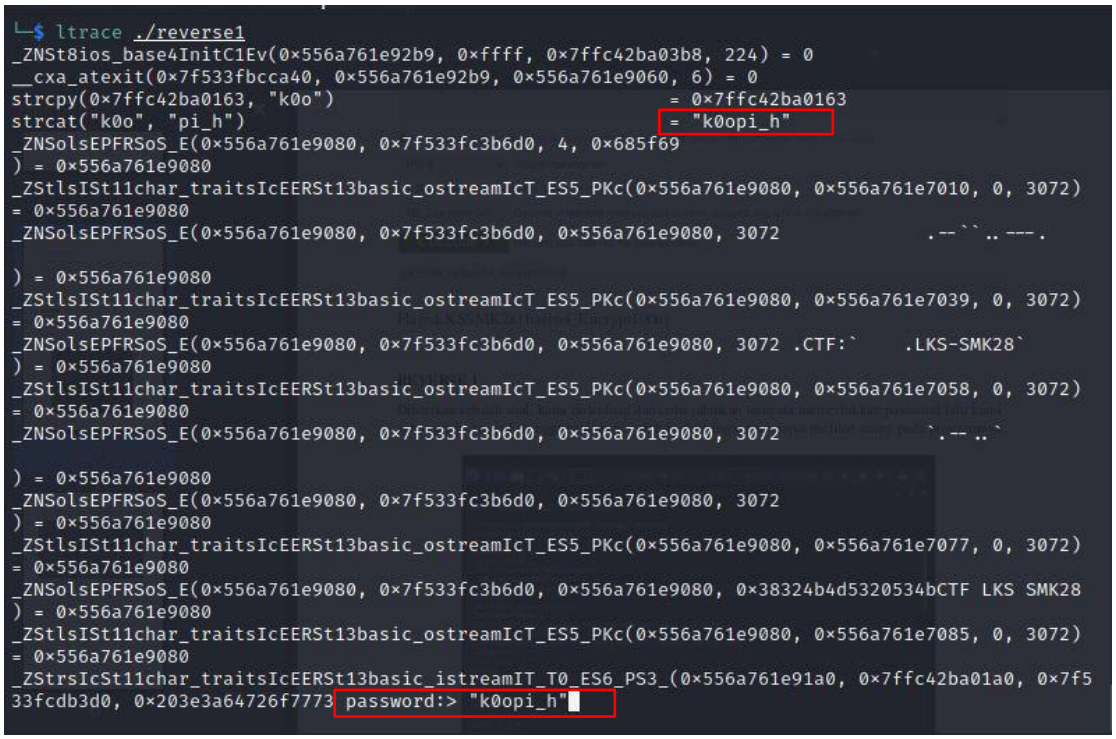
WRITE UP LKS SMK 2020

Contents

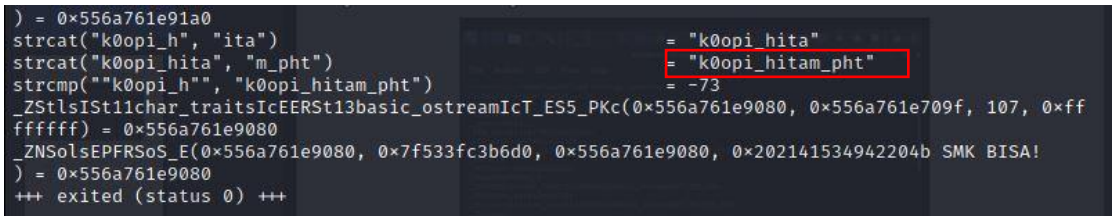
REVERSE 1

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.

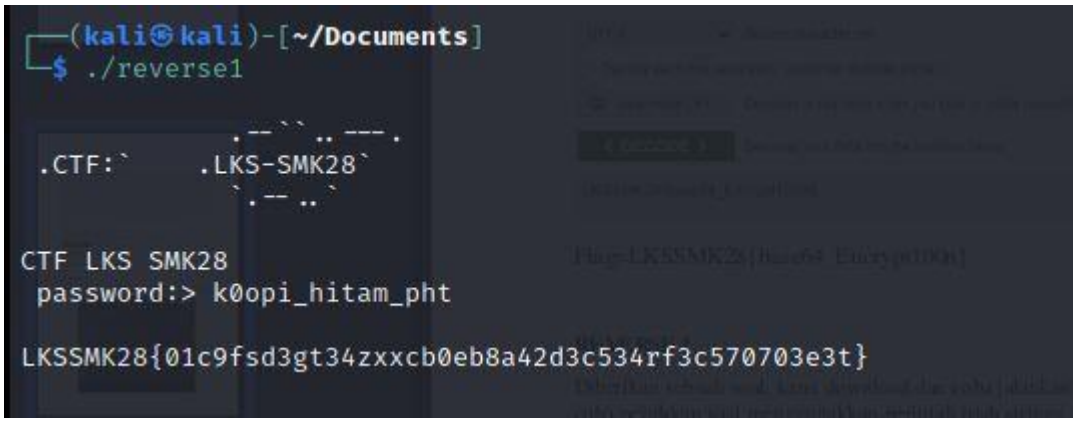
Kemudian, saya coba jalankan lagi tetapi ternyata memerlukan password. Setelah itu, saya menggunakan tool yang bernama ltrace seperti berikut :



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



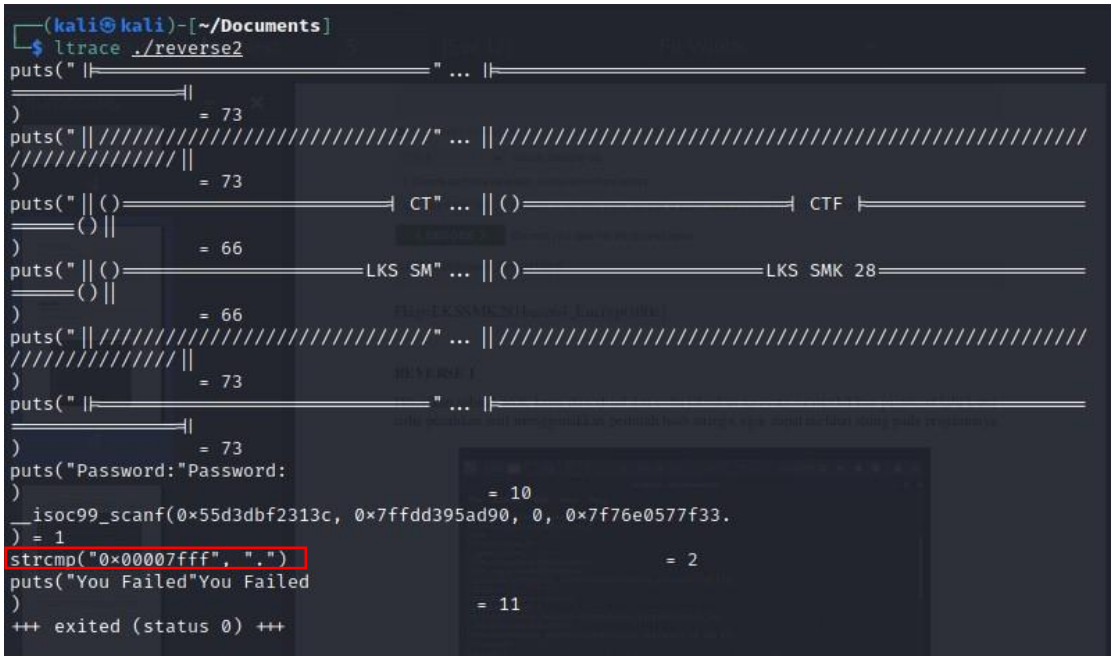
Kemudian saya coba jalankan lagi menggunakan passsword tersebut dan didapat :



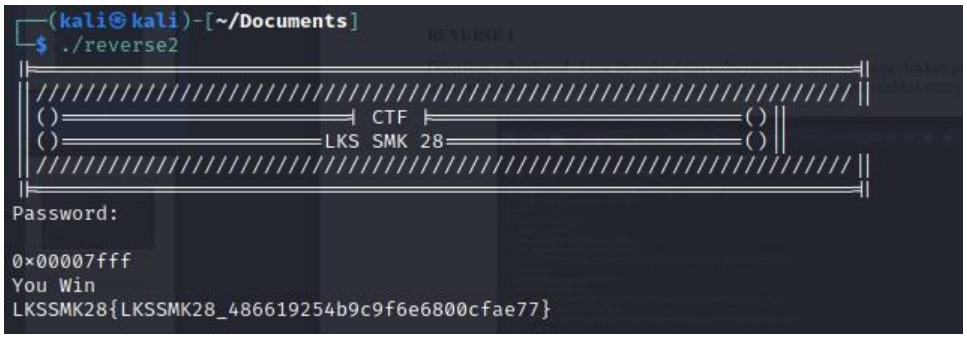
Flag = LKSSMK28{01c9fsd3gt34zxxcb0eb8a42d3c534rf3c570703e3t}

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 :



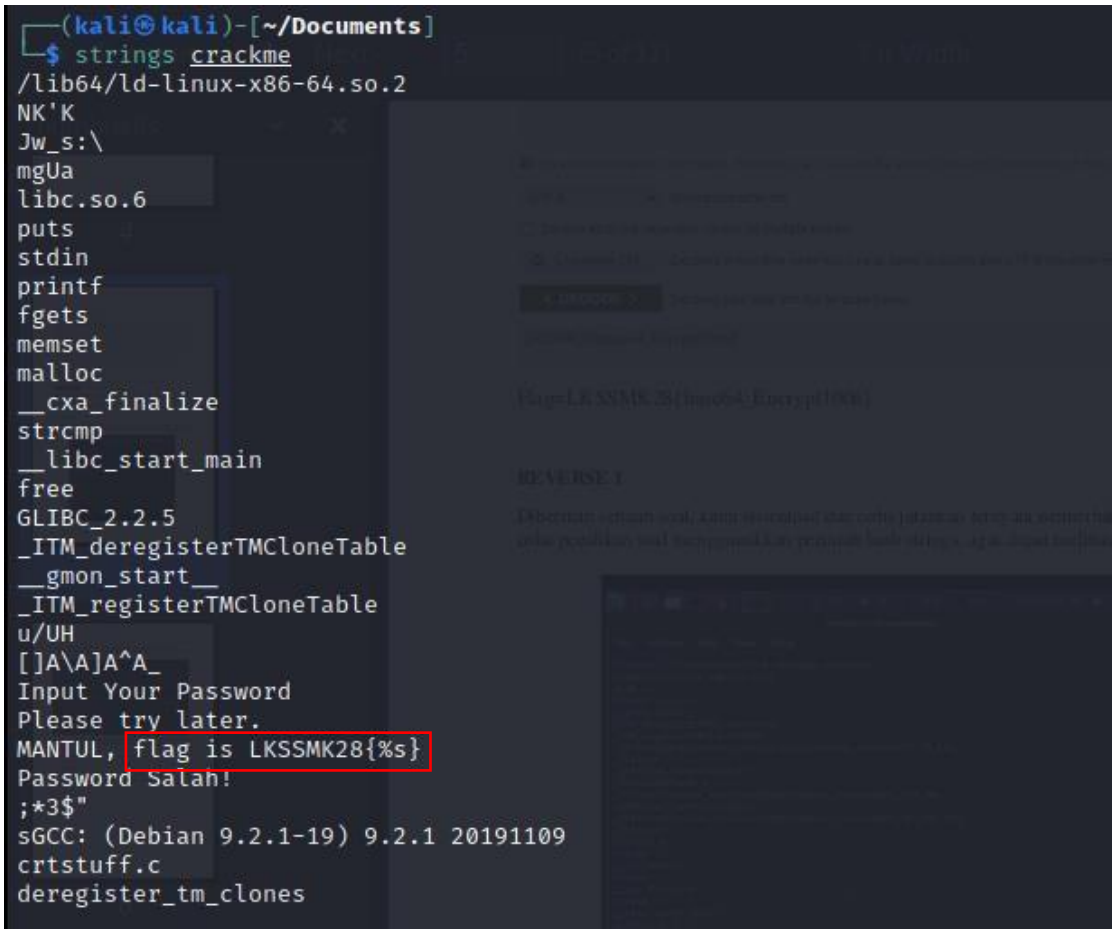
Kemudian saya coba jalankan lagi file tersebut dan saya masukkan password dan didapatkan flagnya :



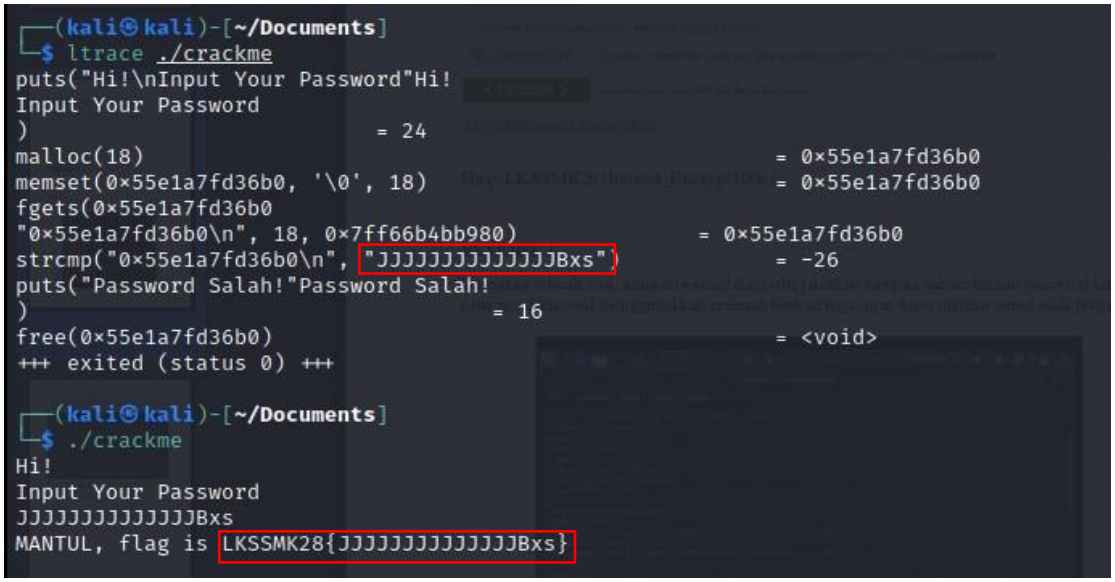
Flag = LKSSMK28{LKSSMK28_486619254b9c9f6e6800cfae77}

CRACKME

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



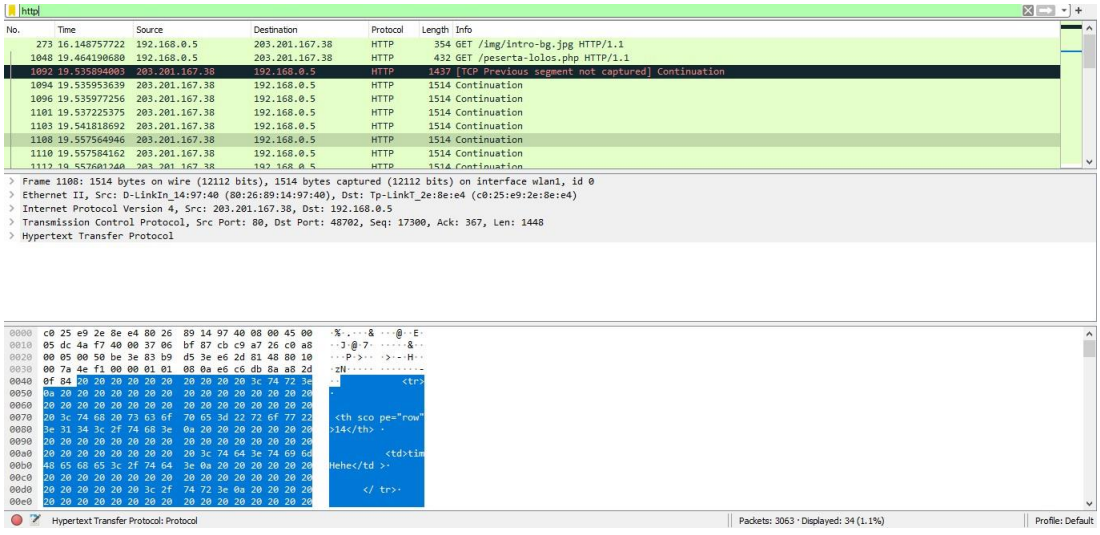
Kemudian saya menggunakan tool ltrace dan didapat :



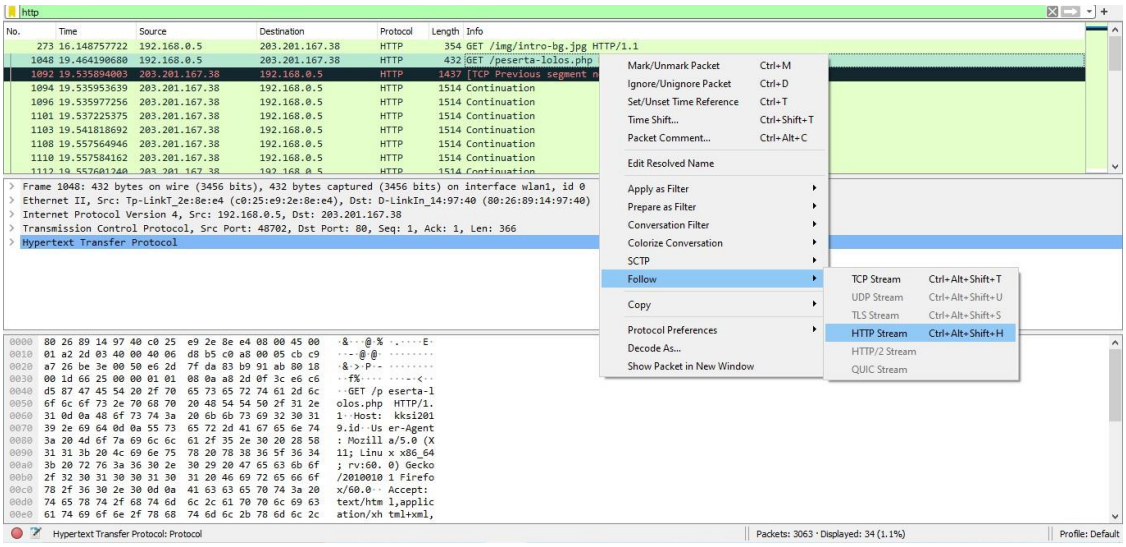
Selanjutnya, saya jalankan lagi filenya dan didapat :
Flag = LKSSMK28{JJJJJJJJJJJJJBxs}

PASS.PCAPNG

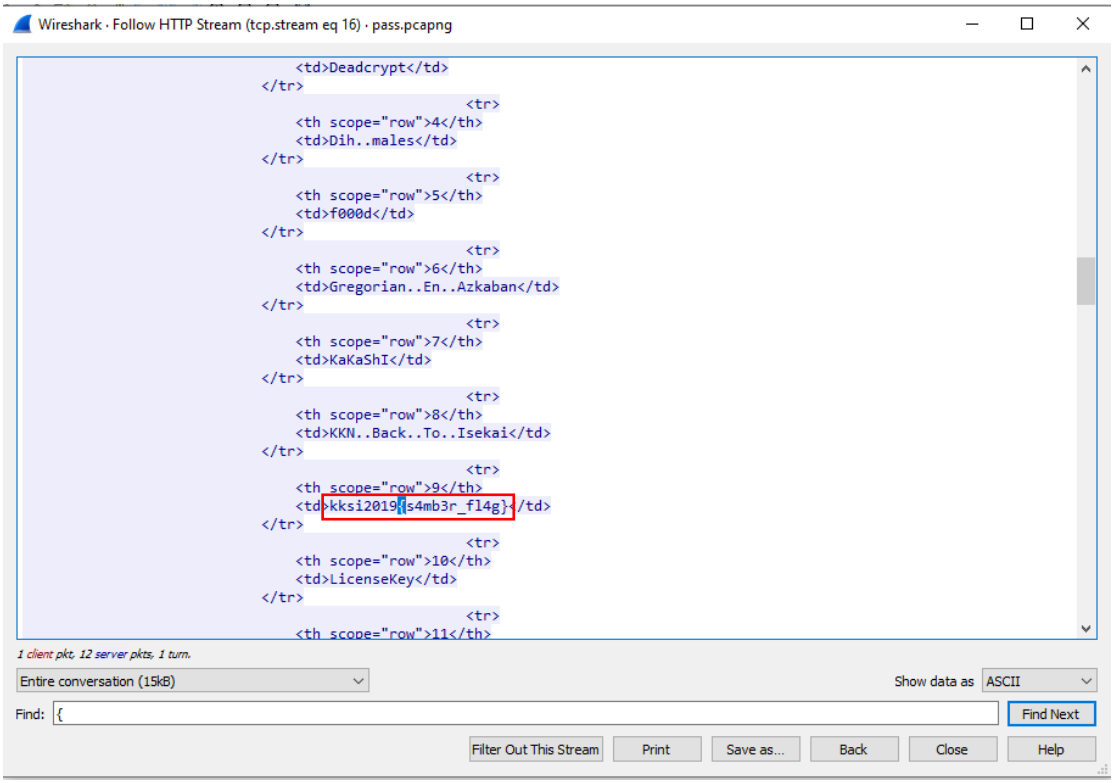
Diberikan soal, lalu saya buka menggunakan aplikasi wireshark kemudian saya lakukan filter packet HTTP seperti berikut :



Setelah itu saya lakukan follow http stream pada packet :



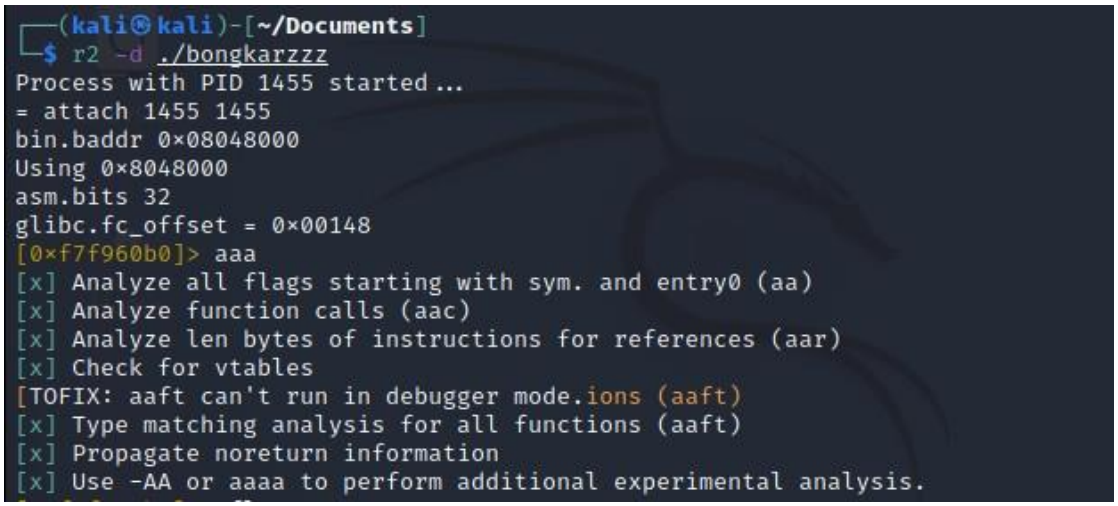
Dan didapat flag :



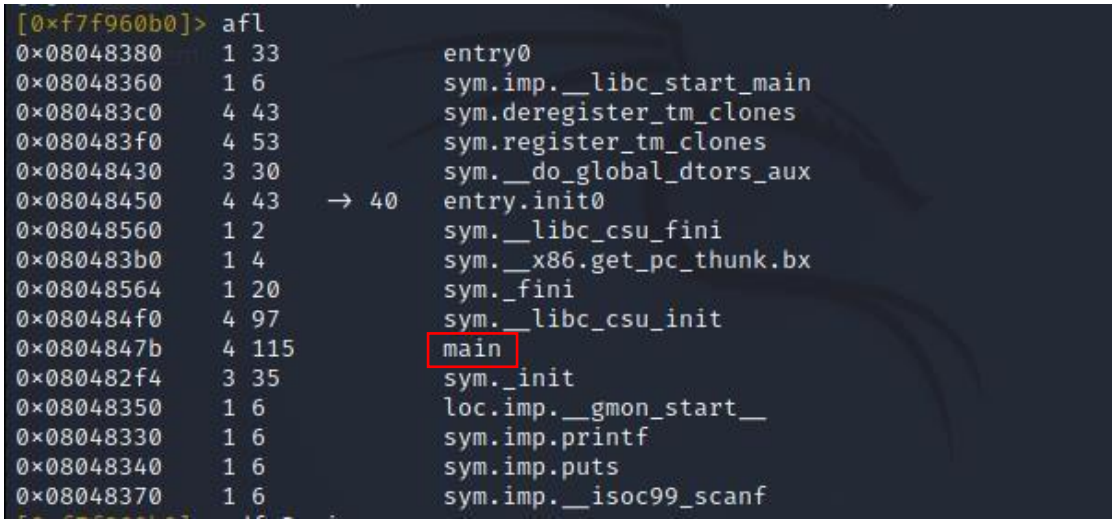
Flag = kks2019{s4mb3r_fl4g}

BONGKARZZZ

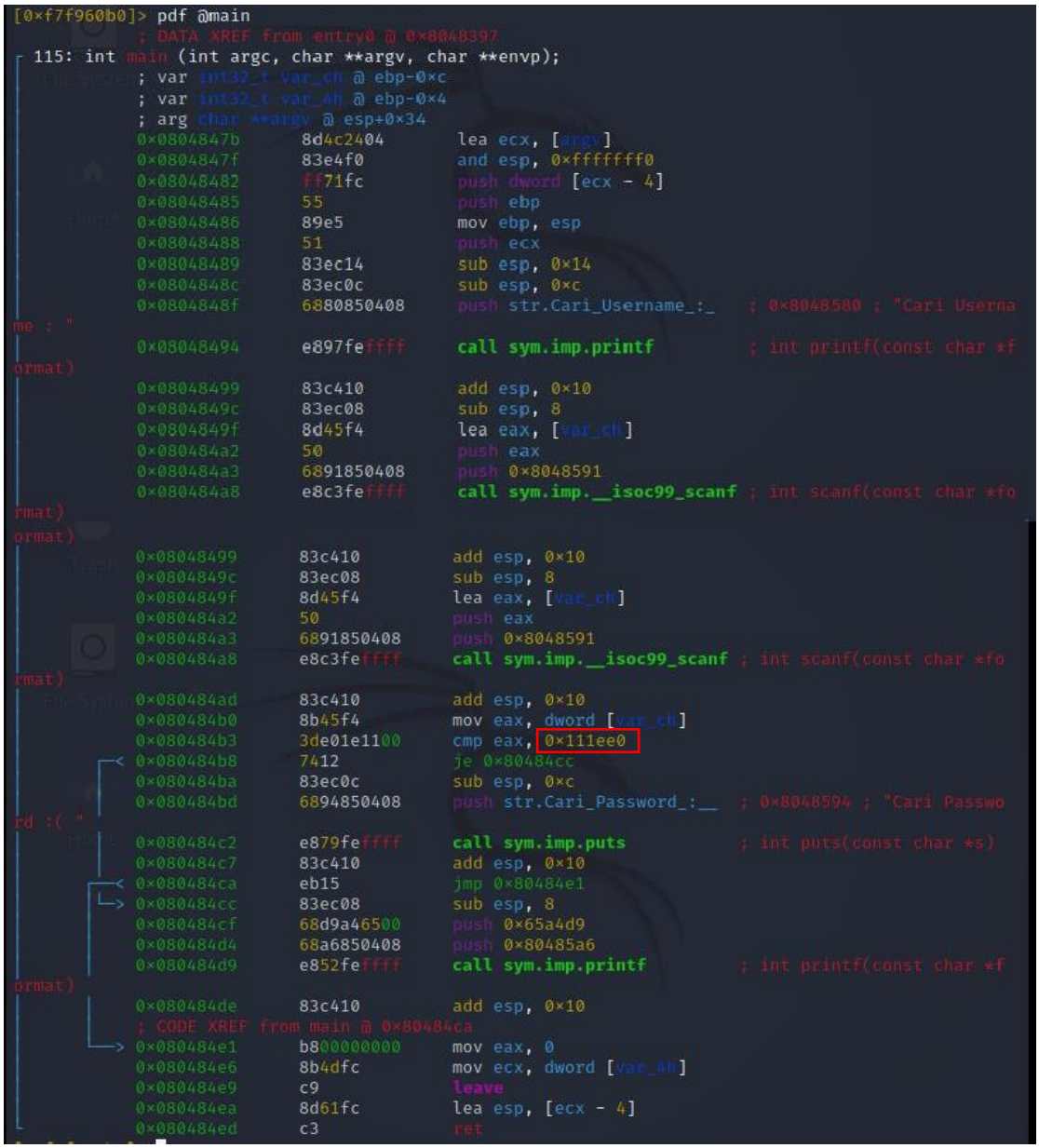
Diberikan file, lalu saya coba buka ternyata diperlukan username dan password. Kemudian saya mencari username dan password untuk file tersebut. Saya coba menggunakan perintah strings tetapi tidak kunjung ditemukan juga. Selanjutnya saya coba menggunakan radare2 dan saya lakukan analyze terhadap file.



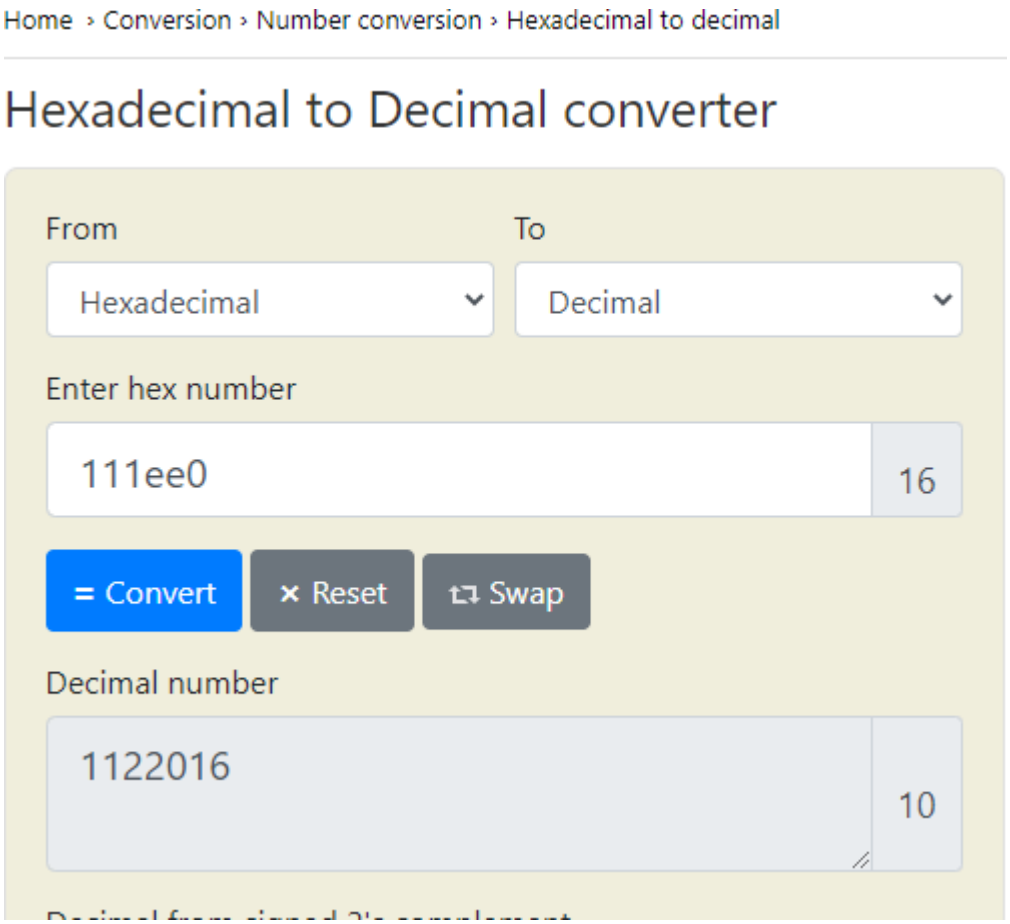
Lalu, untuk melihat list function saya ketikkan afl dan disana terlihat ada main function.



Lalu saya menemukan nilai pembandingnya :



Dan saya konversikan nilai pembanding tersebut ke desimal :



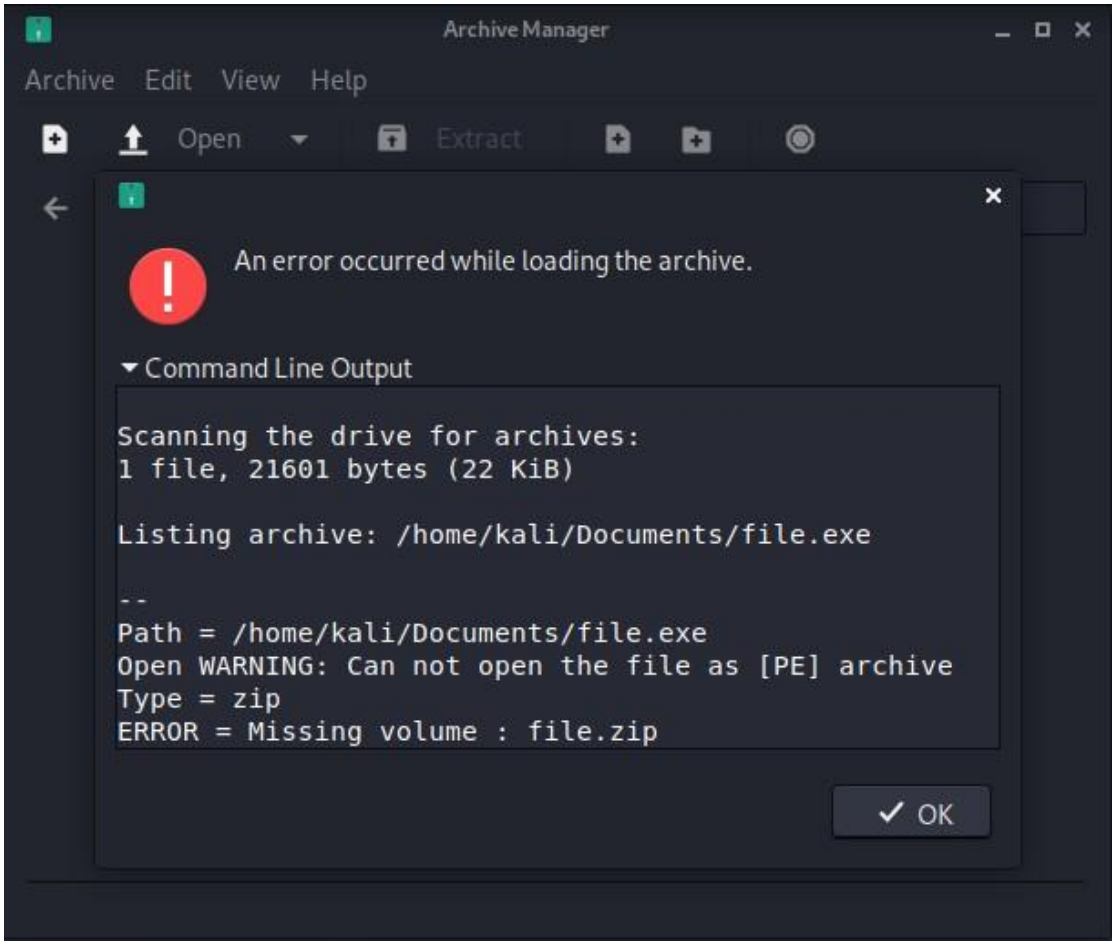
Saya coba angka tersebut untuk username dan ternyata didapat password nya juga :

Username : 1122016

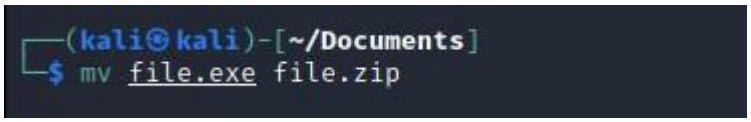
Password : 6661337

FILE.EXE

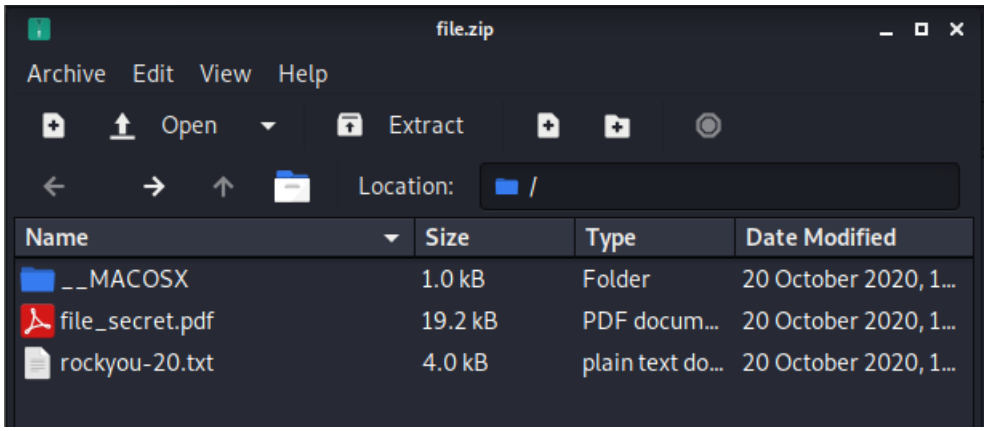
Setelah diberikan file, saya coba buka tetapi ternyata didapat error seperti berikut :



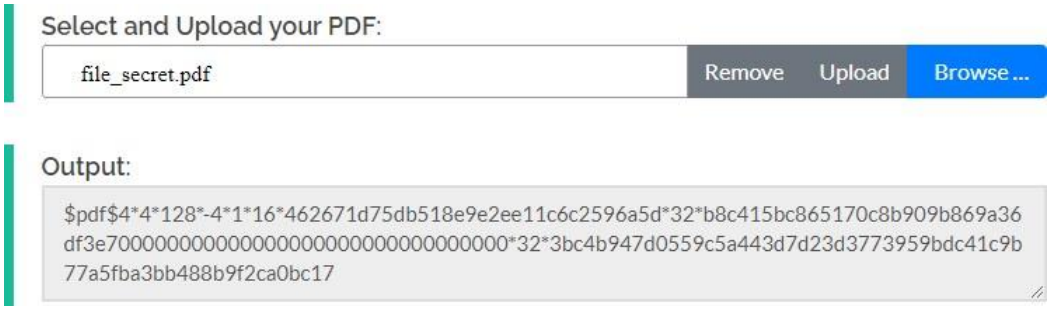
Dari gambar di atas dapat dilihat terdapat hint yang menunjukkan bahwa file tersebut adalah file dengan ekstensi zip, maka saya ubah nama file tersebut ke file.zip :

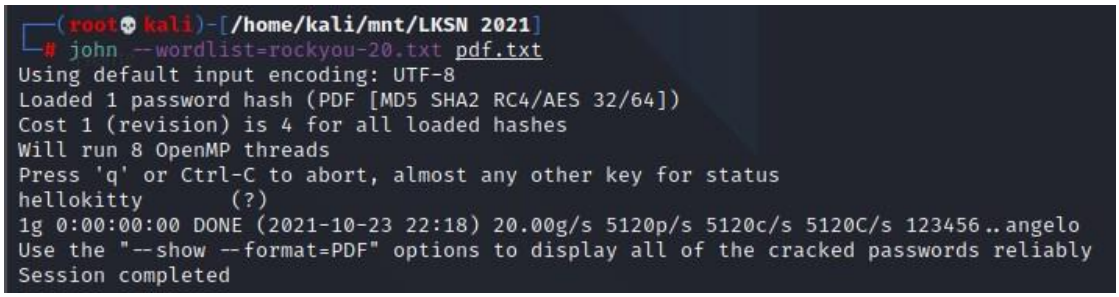


Lalu saya coba buka dan ternyata ada dua file yang tersimpan di sana yaitu sebagai berikut :



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

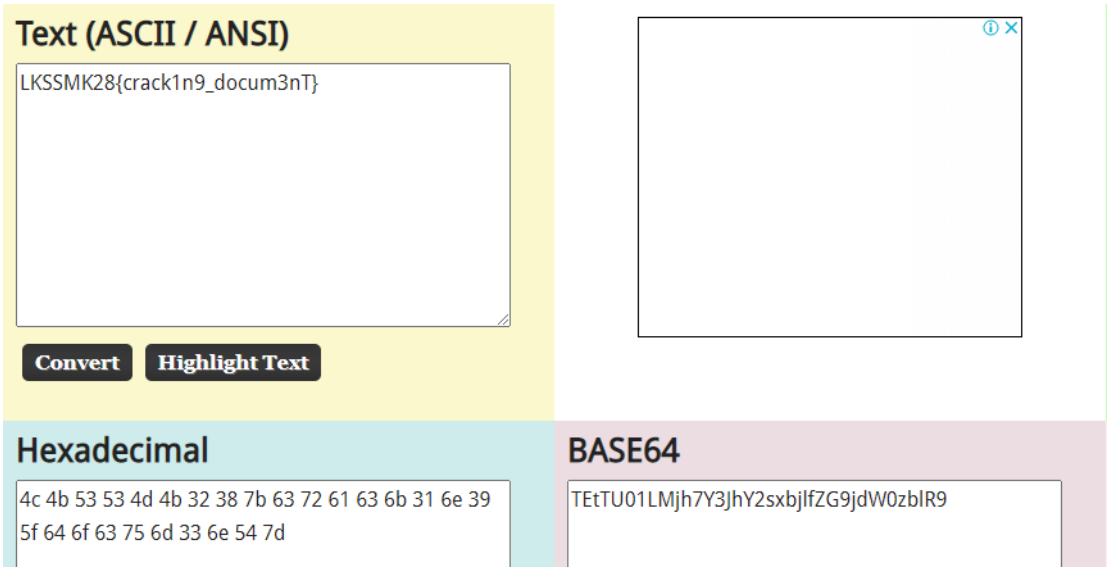




Didapat password nya yaitu “hellokitty” lalu saya buka dokumennya dan muncul hint lagi berupa base64 :

TEtTU01LMjh7Y3JhY2sxbjlfZG9jdW0zblR9==

Base64 tersebut saya konversi ke ascii dan didapat flag :



Flag = LKSSMK28{crack1n9_docum3nT}

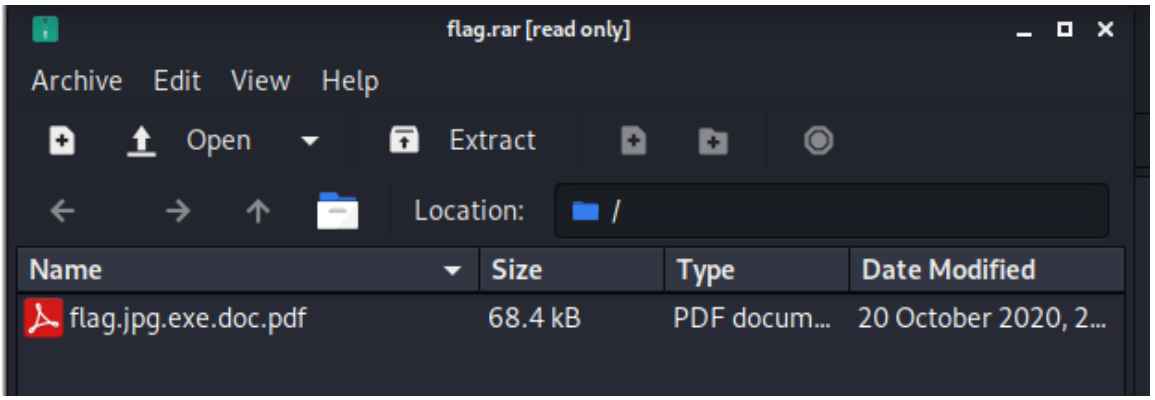
FLAG.JPEG.EXE.DOC.RAR

Diberikan sebuah file dengan ekstensi jpeg, exe, doc, dan rar saya langsung melakukan identifikasi menggunakan command “file” di terminal :

```
┌──(kali㉿kali)-[~/Documents]
└─$ file flag.exe
flag.exe: RAR archive data, v5

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

Setelah diketahui file tersebut merupakan file rar, maka saya rename lalu saya buka dan ternyata berisi file dengan ekstensi pdf :



Kemudian saya ekstrak file tersebut dan setelah diidentifikasi file tersebut merupakan file corrupt yang tidak dapat dibaca :

```
┌──(kali㉿kali)-[~/Documents]
└─$ file flag.jpg.exe.doc.pdf
flag.jpg.exe.doc.pdf: data
```

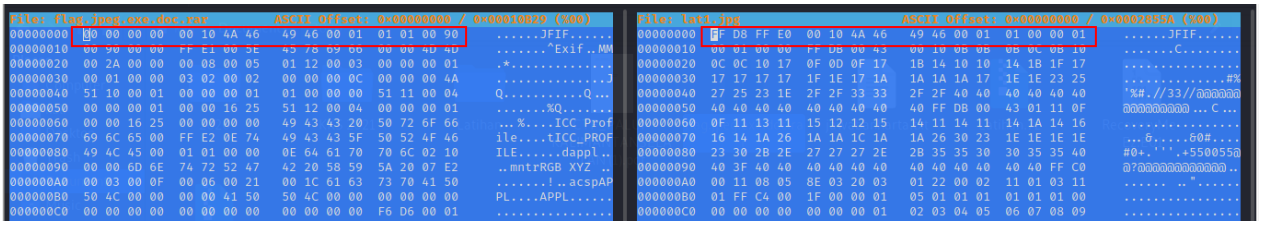
Selanjutnya saya melakukan strings terhadap file dan di bagian header terdapat kata JFIF yang mengindikasikan file tersebut adalah file JPG :

```
┌──(kali㉿kali)-[~/Documents]
└─$ strings flag.jpg.exe.doc.pdf
JFIF
^Exif
ICC Profile
tICC_PROFILE
dappl
mntrRGB XYZ
acspAPPL
APPL
-appl
desc
bdscm
Jcprt
#wtpt
```

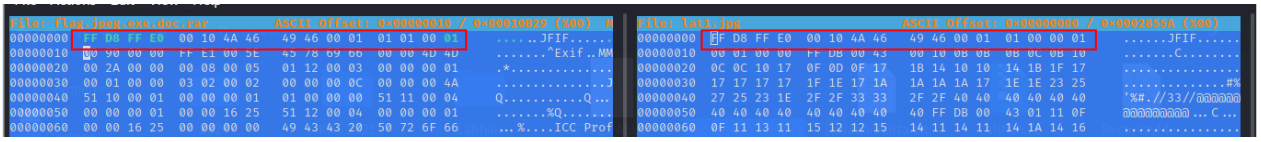
Setelah itu saya rename menjadi file berekstensi jpg dan saya coba buka namun tidak berhasil. Di sini saya mengasumsikan kita harus memperbaiki bagian header file tersebut agar file dapat dibuka.

```
┌──(root💀 kali)-[/home/kali/Documents]
└─# mv flag.jpg.exe.doc.pdf flag.jpg
```

Saya menggunakan tool hexeditor di kali dan header nya saya bandingkan dengan file jpg yang sebenarnya, dan benar saja terdapat kesalahan dalam nilai hexa seperti pada gambar :



Lalu langsung saja saya perbaiki menjadi seperti berikut :



Kemudian saya coba buka kembali dan ternyata berhasil :

Flag = LKSSMK28{Yuu-kita-ke-jakarta}