LKSMK2023 MALANG

TEAM 2 SMKN 4 MALANG :

* Firda Gheitsa Sahira
* Fikri Muhammad Abdillah

BAB A: Jeopardy

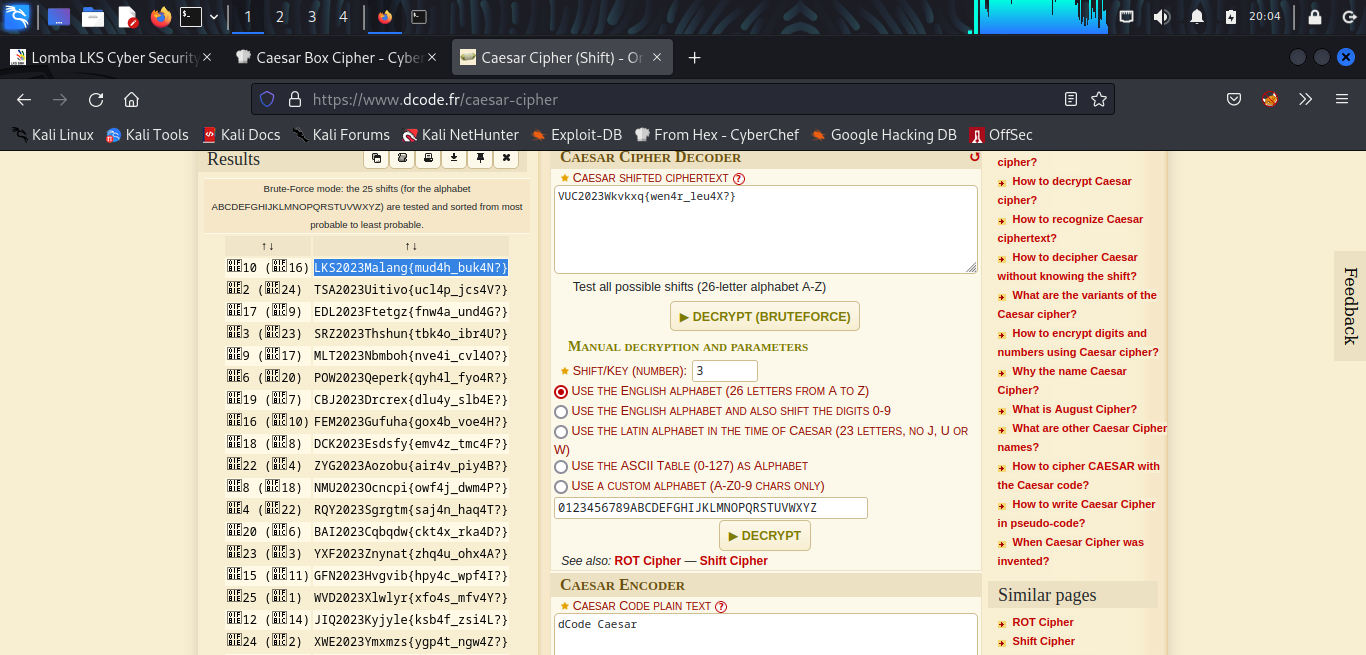
**1. EasyMe (Cryptography)**

isi soalnya yaitu *VUC2023Wkvkxq{wen4r\_leu4X}*

setelah kita analyze metode yang digunakan adalah caesar cipher

setelah itu kita coba decode dengan tool online untuk decrypt dan terlihat flag disalah satu hasil dari output decrypt tersebut

FLAG : LKS2023Malang{mud4h\_buk4N?}



2. EncDec (Cryptography)

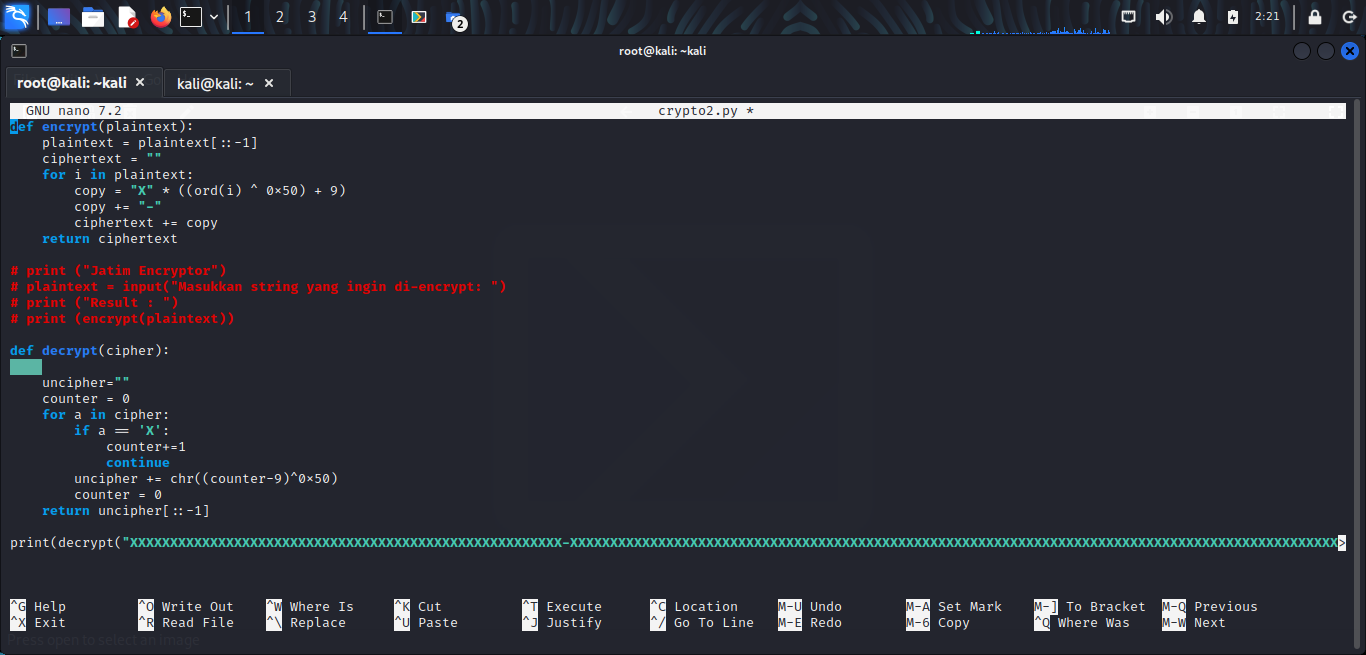
Pertama-tama kita mendapatkan 2 file yaitu file enc.py dan encrypted.txt

enc.py berisi function encrypt dan encrypted.txt berisi FLAG yang sudah di encrypt

cara decrypt saya yaitu:

membuat loop untuk setiap karakter pada encrypted.txt, lalu program akan menambahkan counter setiap bertemu karakter “X”, lalu jika program menemukan karakter “-” maka program akan mengurangi counter dengan 9 lalu di xor 0x50 dan hasil akan dimasukkan ke variabel uncipher, dan akan terus begitu sampai huruf habis, lalu hasil algoritma tersebut akan di reverse untuk hurufnya, lalu akan mendapatkan flag:

FLAG: LKS2023Malang{tHanKs\_f0r\_f1nd1ng\_m3}



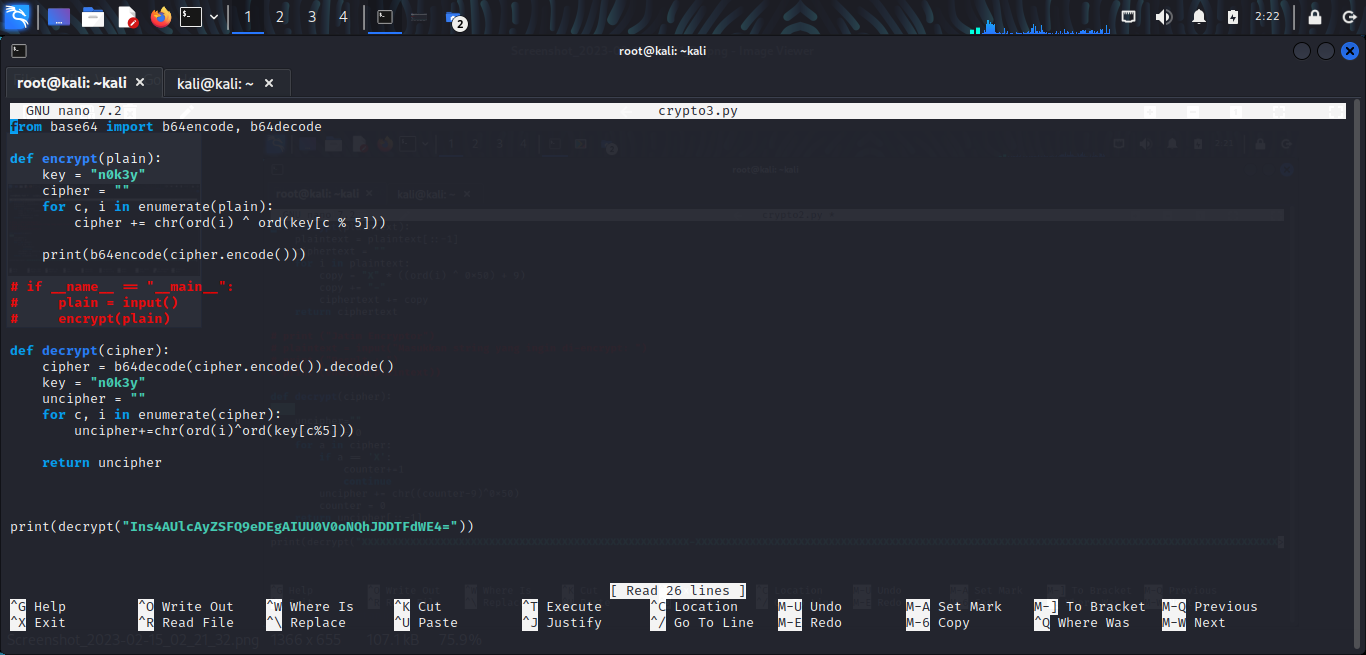
3. x0r (Cryptography)

pertama-tama kami mendapatkan dua file yaitu xor.py dan xor\_cipher.txt

untuk algoritmanya sama dengan waktu di encrypt, tapi untuk decrypt awalnya di decode base64 terlebih dahulu, baru memakai algoritma encrypt nya

lalu akan mengasilkan flag:

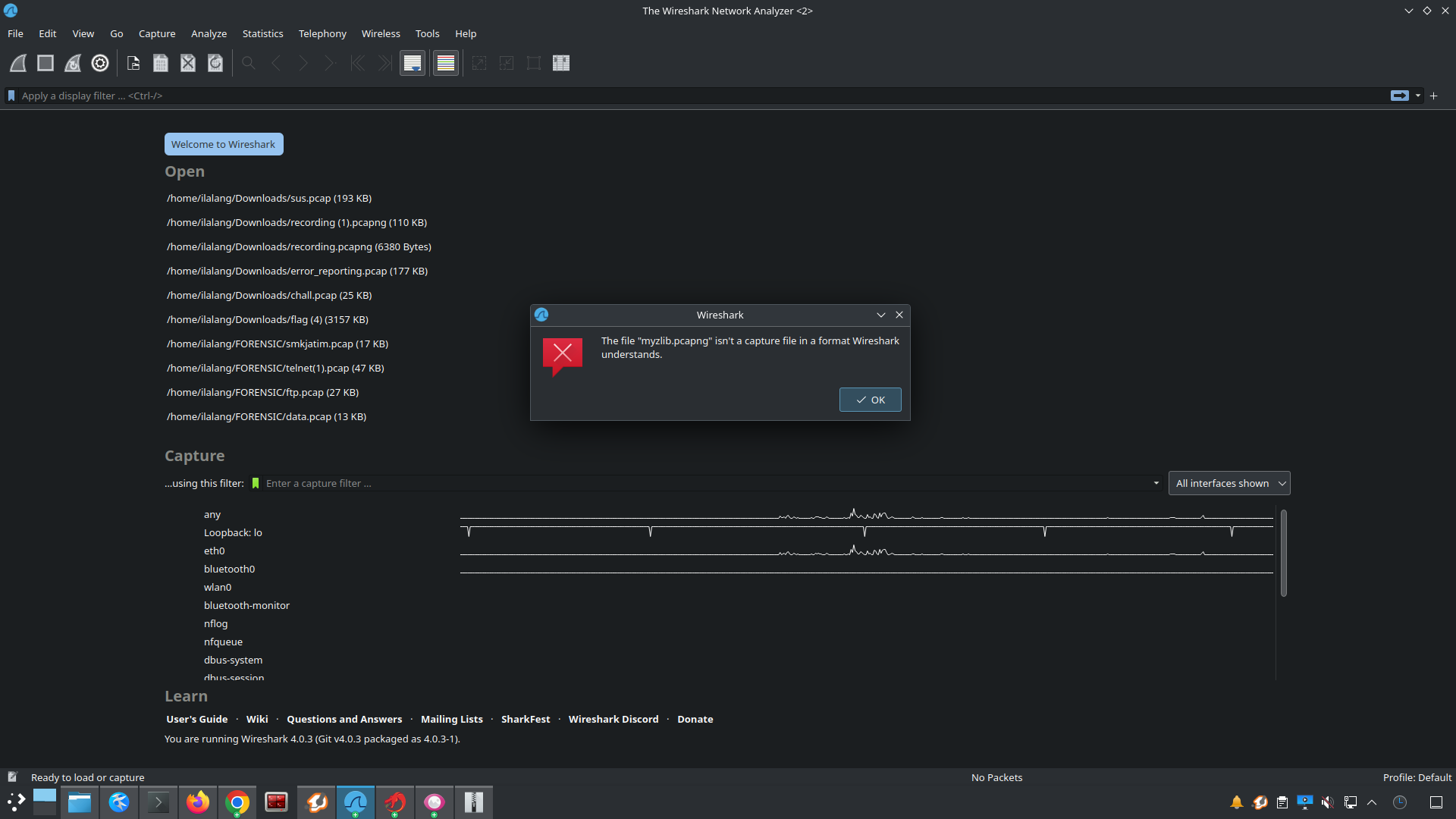
FLAG: LKSMK2023{y0u\_d3crypt\_m3}



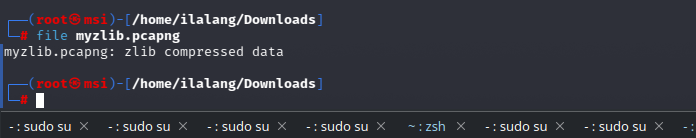
4. Track

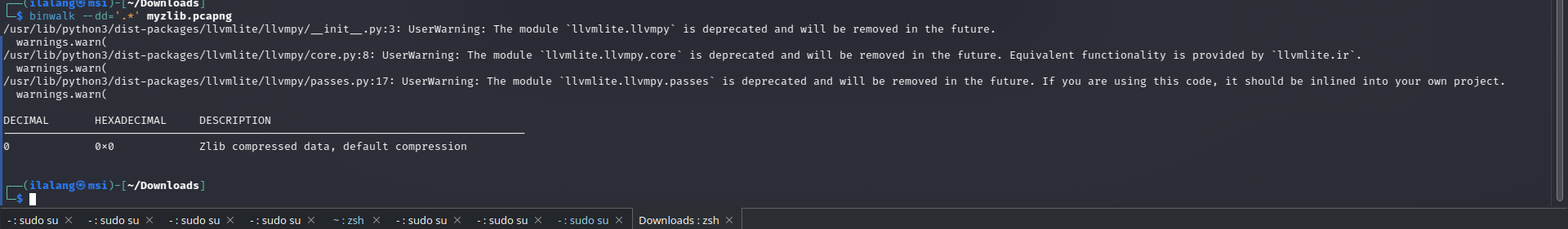
isi soalnya yaitu file myzlib.pcapng

Saya coba buka dengan wireshark tetapi gagal



saya coba analyze lagi dengan command file <file> teryata adalah zlib



jalankan perintah binwalk --dd='.\*' myzlib.pcapng

ada flag diantara file yang diekstrak yaitu

LKS2023Malang{zl1b\_c0mpr3ss1ion\_0ver\_pcap}

**5. I am on diet (web)**

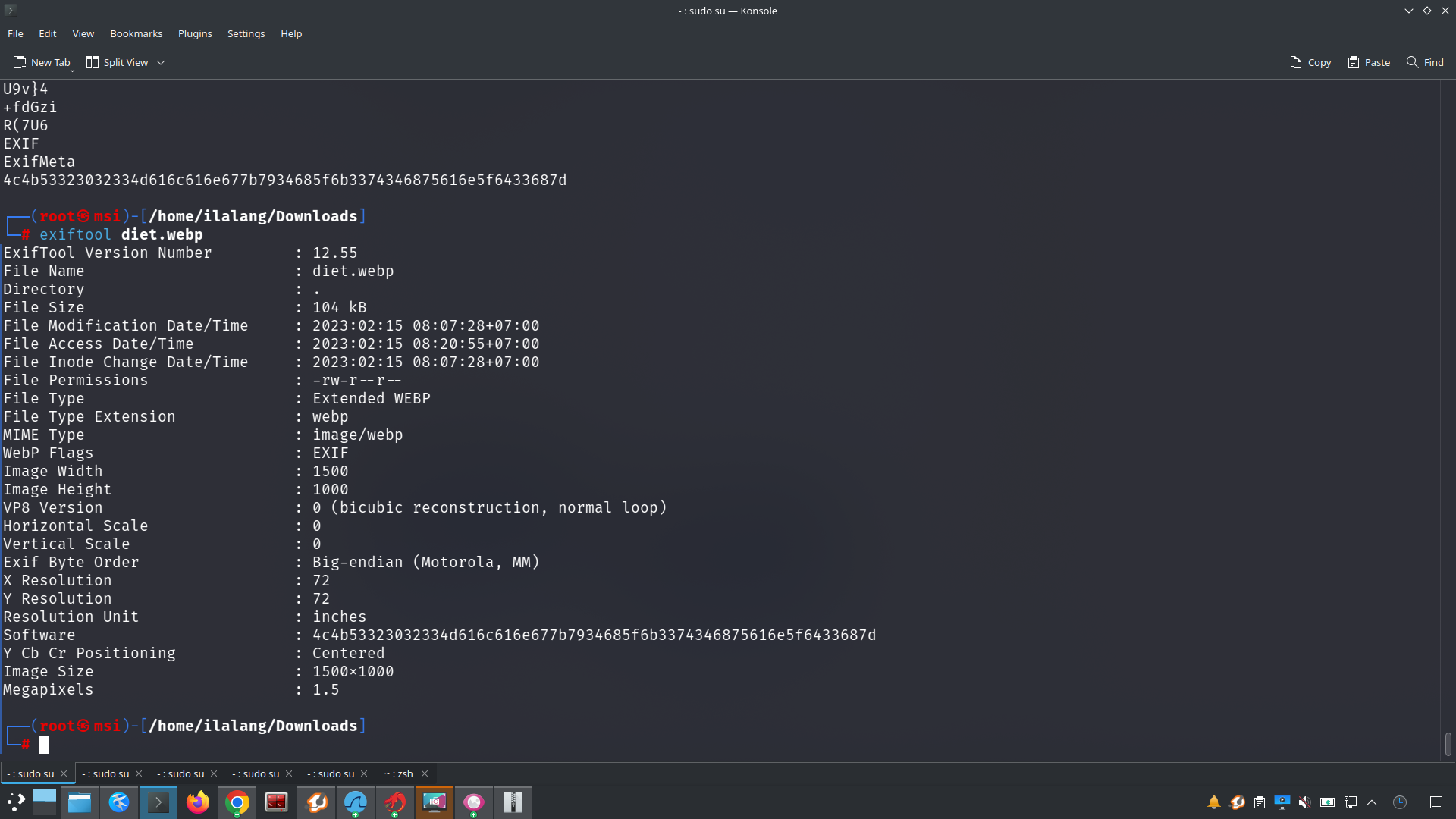
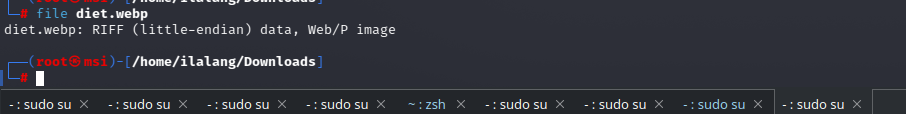
kita mendapatkan file diet.webp

Saya coba dengan exiftool dan decode strings yang ada di sofware

setelah kita analyze teryata menggunkan ascii

lalu kita dapat flag nya melalui tool online

|  |
| --- |
| LKS2023Malang{y4h\_k3t4huan\_d3h} |

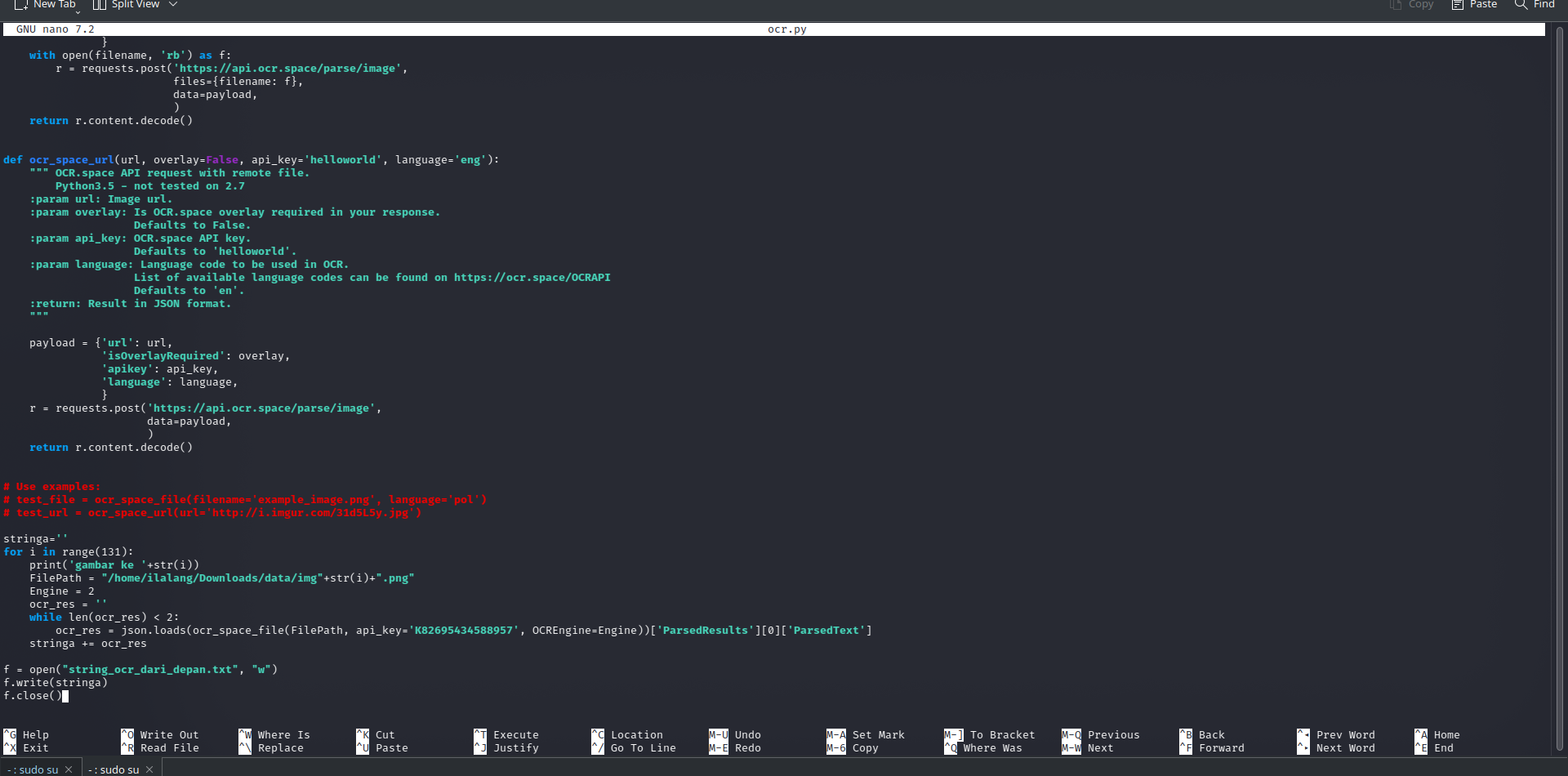


**6. data lks (Steganograpy)**

kita mendapatkan file datalks.zip lalu coba kita ekstrak



lalu membuat program ocr dengan python untuk membaca karakter dalam setiap gambar dimulai dari gambar 0 sampai dengan 130

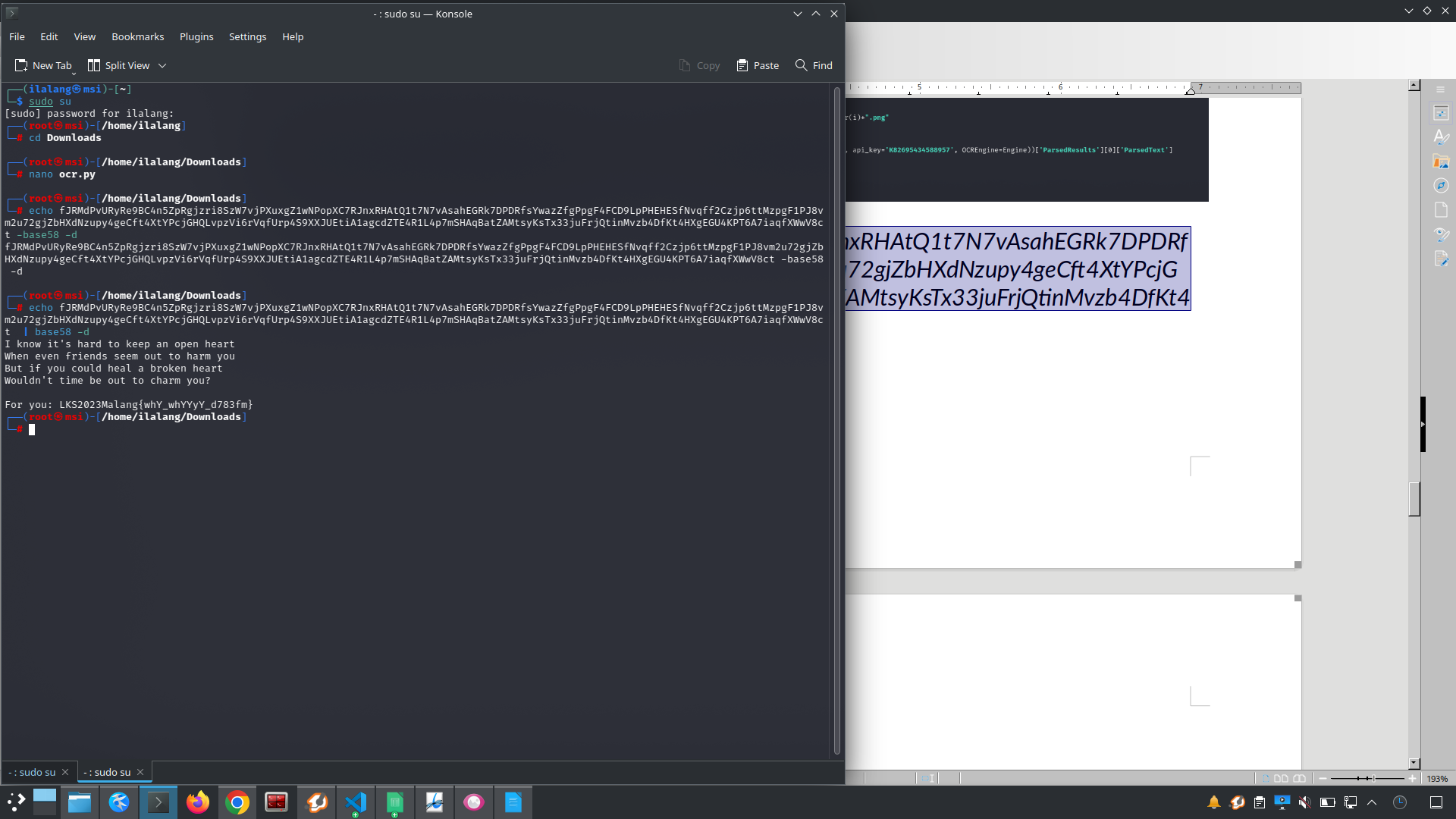


hasil dari program ocr :

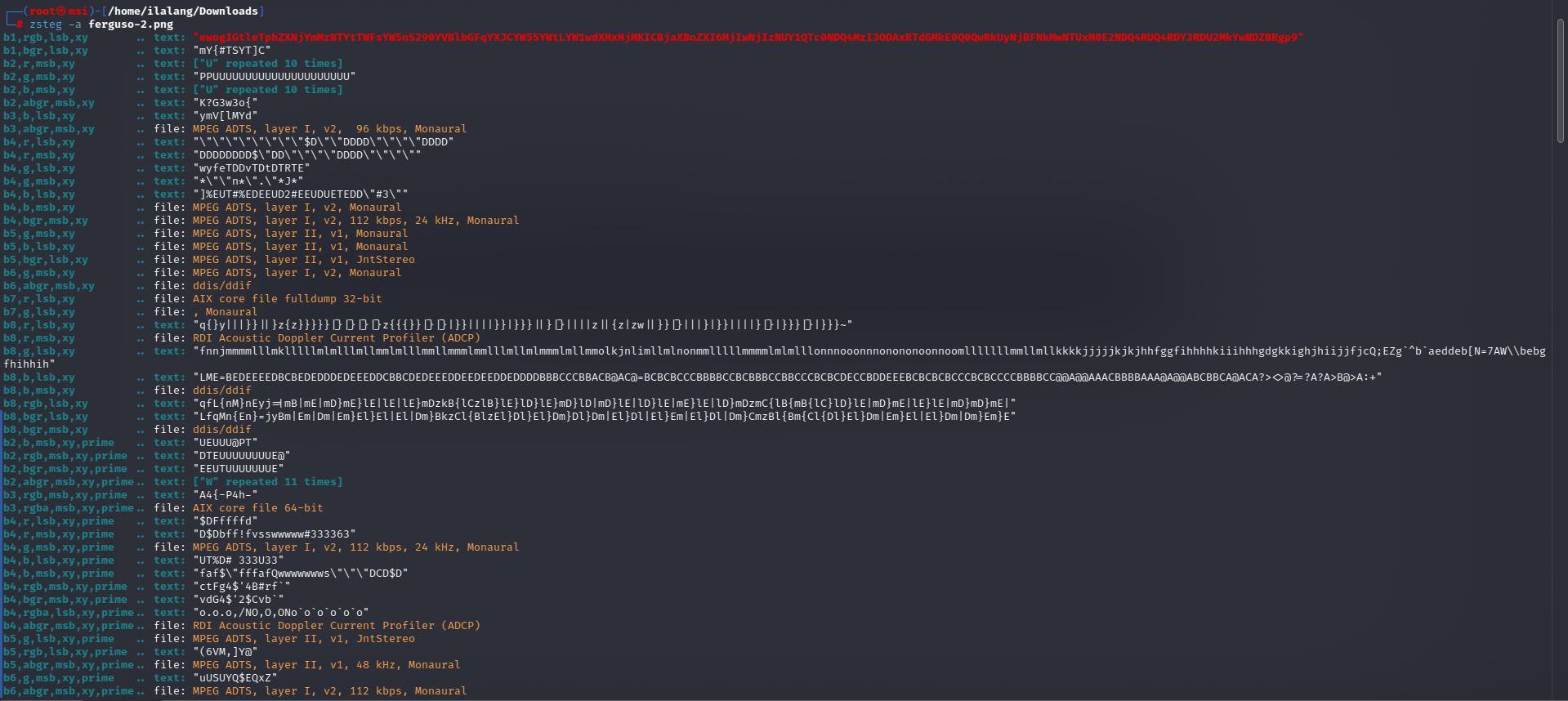
*fJRMdPvURyRe9BC4n5ZpRgjzri8SzW7vjPXuxgZ1wNPopXC7RJnxRHAtQ1t7N7vAsahEGRk7DPDRfsYwazZfgPpgF4FCD9LpPHEHESfNvqff2Czjp6ttMzpgF1PJ8vm2u72gjZbHXdNzupy4geCft4XtYPcjGHQLvpzVi6rVqfUrp4S9XXJUEtiA1agcdZTE4R1L4p7mSHAqBatZAMtsyKsTx33juFrjQtinMvzb4DfKt4HXgEGU4KPT6A7iaqfXWwV8ct*

setelah kita analyze cipher diatas menggunakan base58 lalu coba kita decode dan muncul flag nya

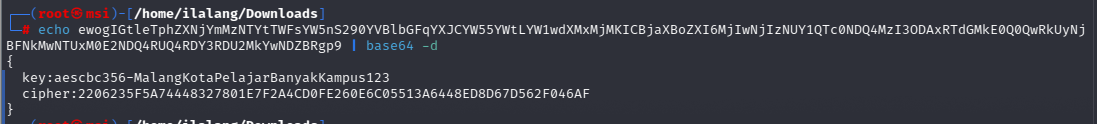
LKS2023Malang{whY\_whYYyY\_d783fm}



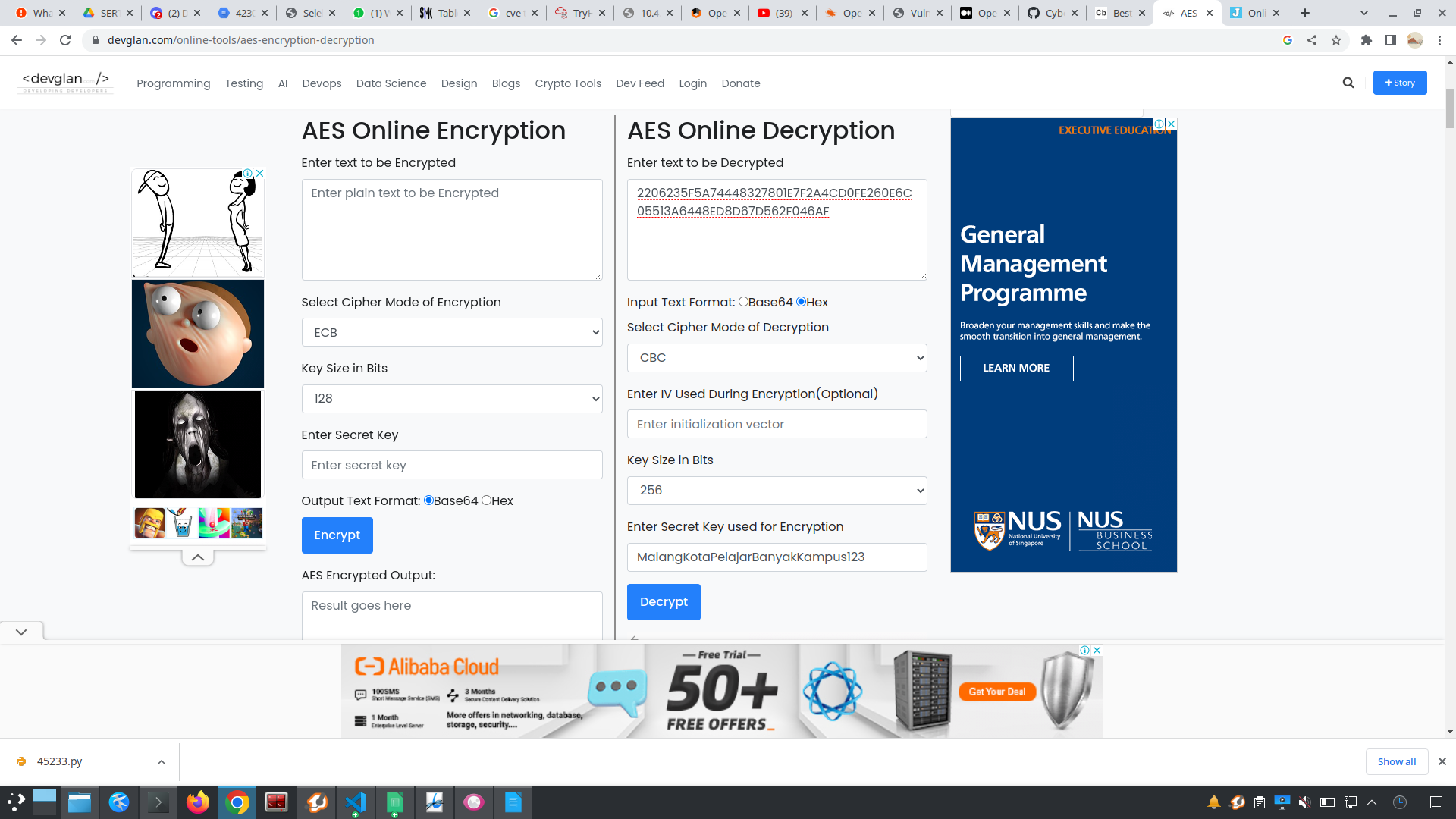
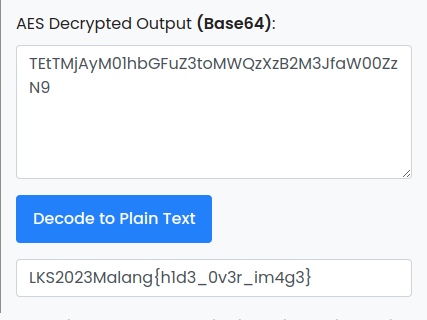
**7. Ferguso**

mendapatkan satu gambar dengan ekstensi png lalu saya coba buka dengan zsteg

saya coba decode text diatas menggukan base64 *"ewogIGtleTphZXNjYmMzNTYtTWFsYW5nS290YVBlbGFqYXJCYW55YWtLYW1wdXMxMjMKICBjaXBoZXI6MjIwNjIzNUY1QTc0NDQ4MzI3O  
DAxRTdGMkE0Q0QwRkUyNjBFNkMwNTUxM0E2NDQ4RUQ4RDY3RDU2MkYwNDZBRgp9"*



decode lagi cipher diatas menggunkan aescbc 256 dengan key *MalangKotaPelajaraBanyakKampus123*



**BAB B: Defense**

**1. Password**

* mengganti password deafult untuk ubuntu dan vargant

**2. SSH**

* disable PermitRootLogin

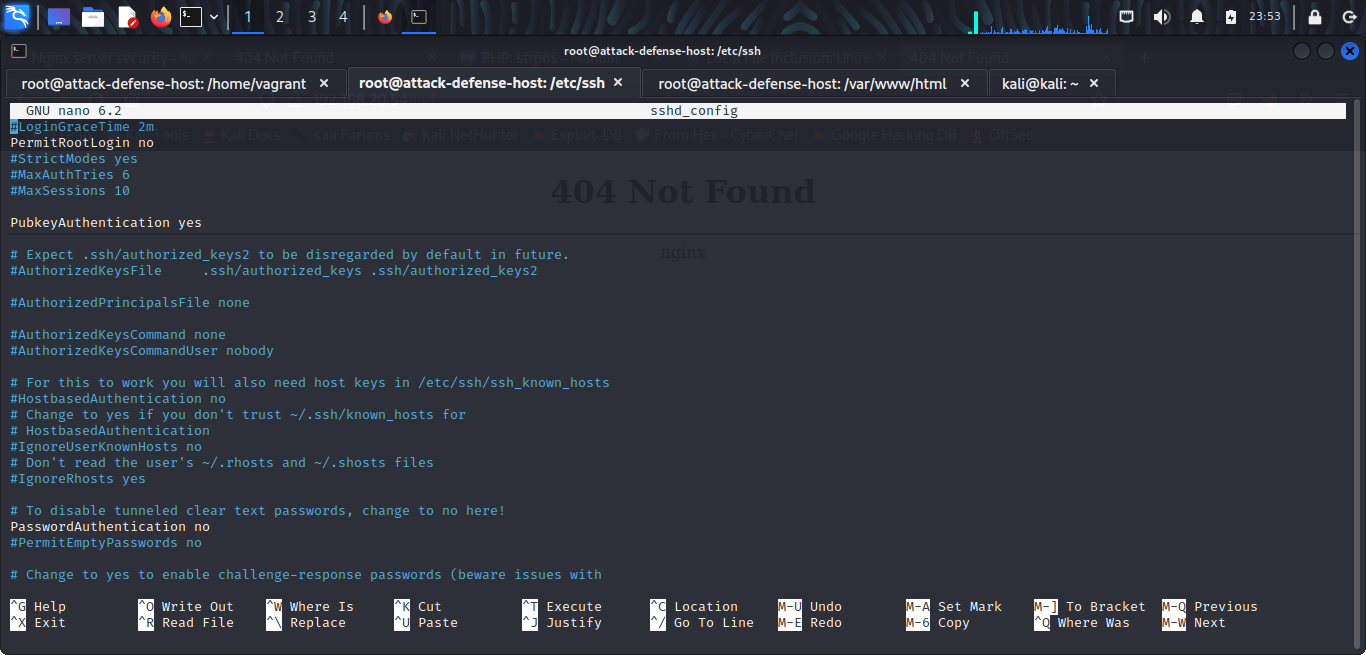
untuk melarang login lewat ssh mengunakan root

* Disable passwordAuthentication

Agar login hanya bisa menggunkan public key

* Enable PublicKeyAuthentication

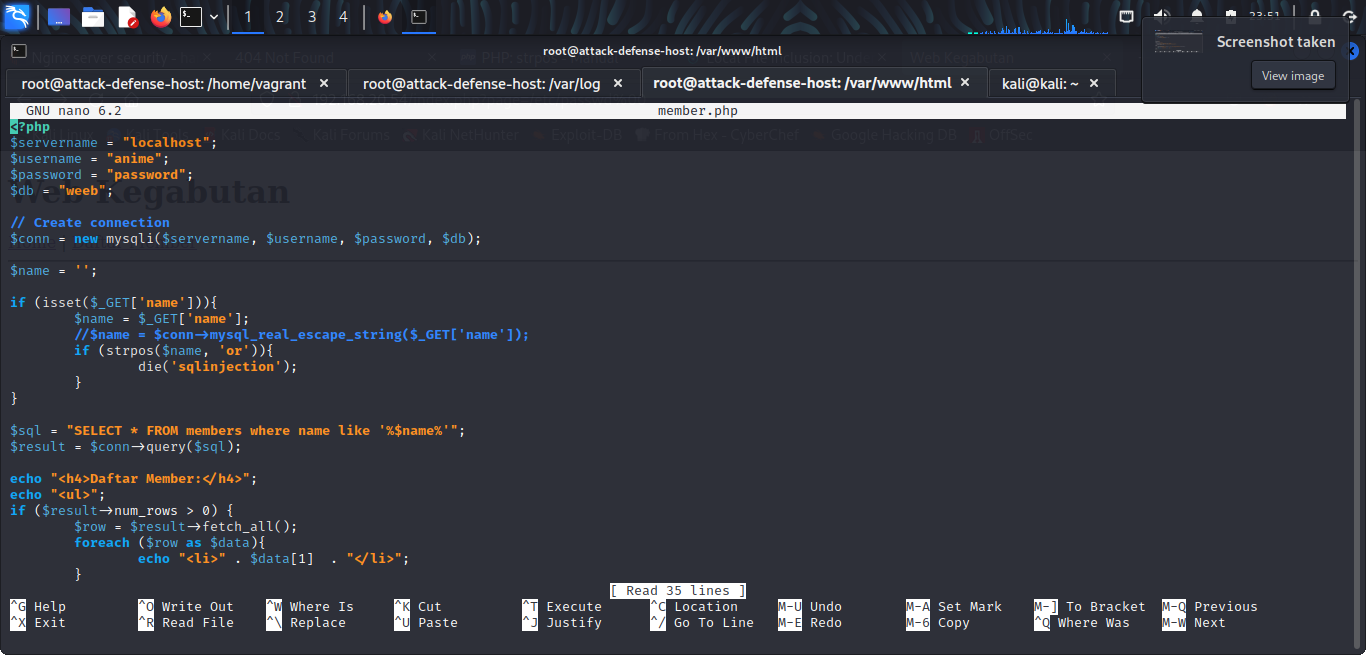
untuk enable public key



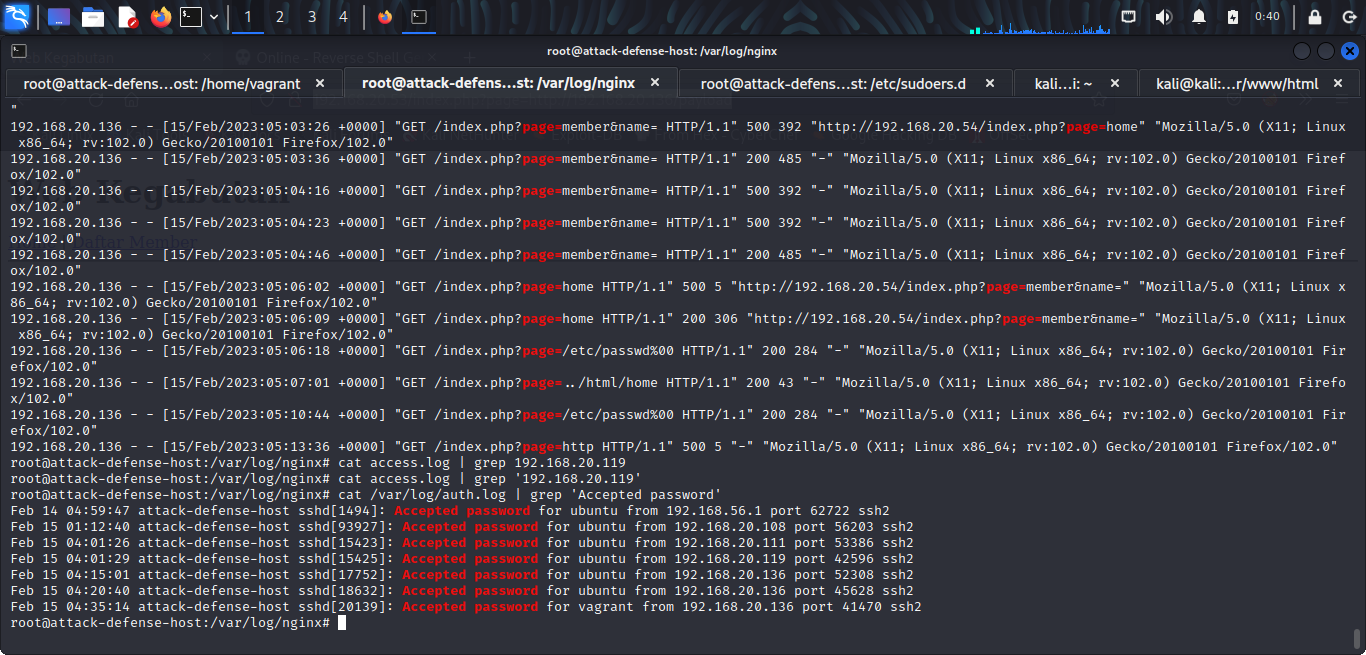
**3. Path WEB**

ada celah web yaitu LFI dan sqlinjection

jadi kami menutup celah tersebut menggunkan function strpost() untuk menemunkan karakter yang dilarang, lalu jika karakter yang dilarang terdeteksi, maka php akan menjalankan perintah die() atau menghentikan semua perintah



**5. Monitoring**

kami menggunakan command tail -f /var/log/auth.log

**BAB C: ATTACK**

* Pertama kita cek celah di port http teryata ada celah untuk lfi tapi tidak bisa digunakan tapi bisa menggunakan celah sql injection dengan memasukkan payload di parameter get, nama parameter nya yaitu ‘id’
* Setelah itu kita menemukan vulnerabilty yaitu weak passwod di semua server yaitu password default vagrant
* Privilege escalation langsung menggunakan sudo karna vagrant merupakan sudoers no password

