Ctf collection vol 1

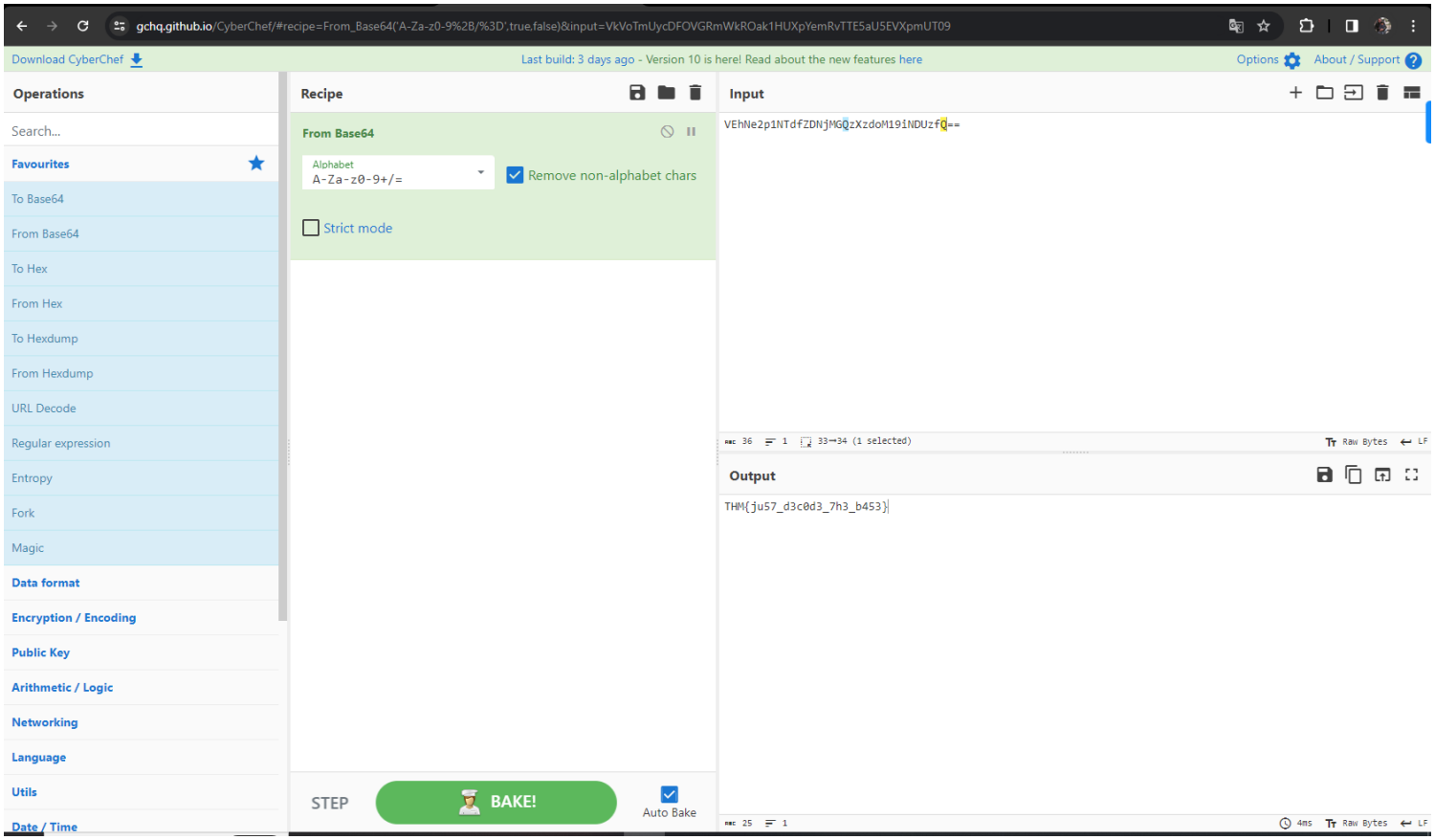
Ctf collection vol 1
Estos retos son un compilado de muchos retos relacionados con reversing , sternografia y codificación don de lo que se debe conseguir es la flag

la tarea 1 es ingresar a la sala.

la segunda dice si puedes decodificar el mensaje:

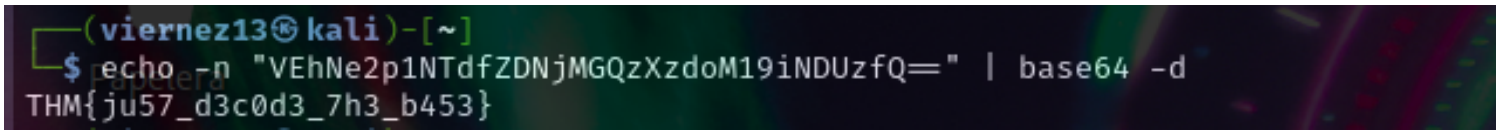
VEhNe2p1NTdfZDNjMGQzXzdoM19iNDUzfQ==

claramente esto es un cifrado en Base64



otra forma de decodificarlo es usando la terminal.

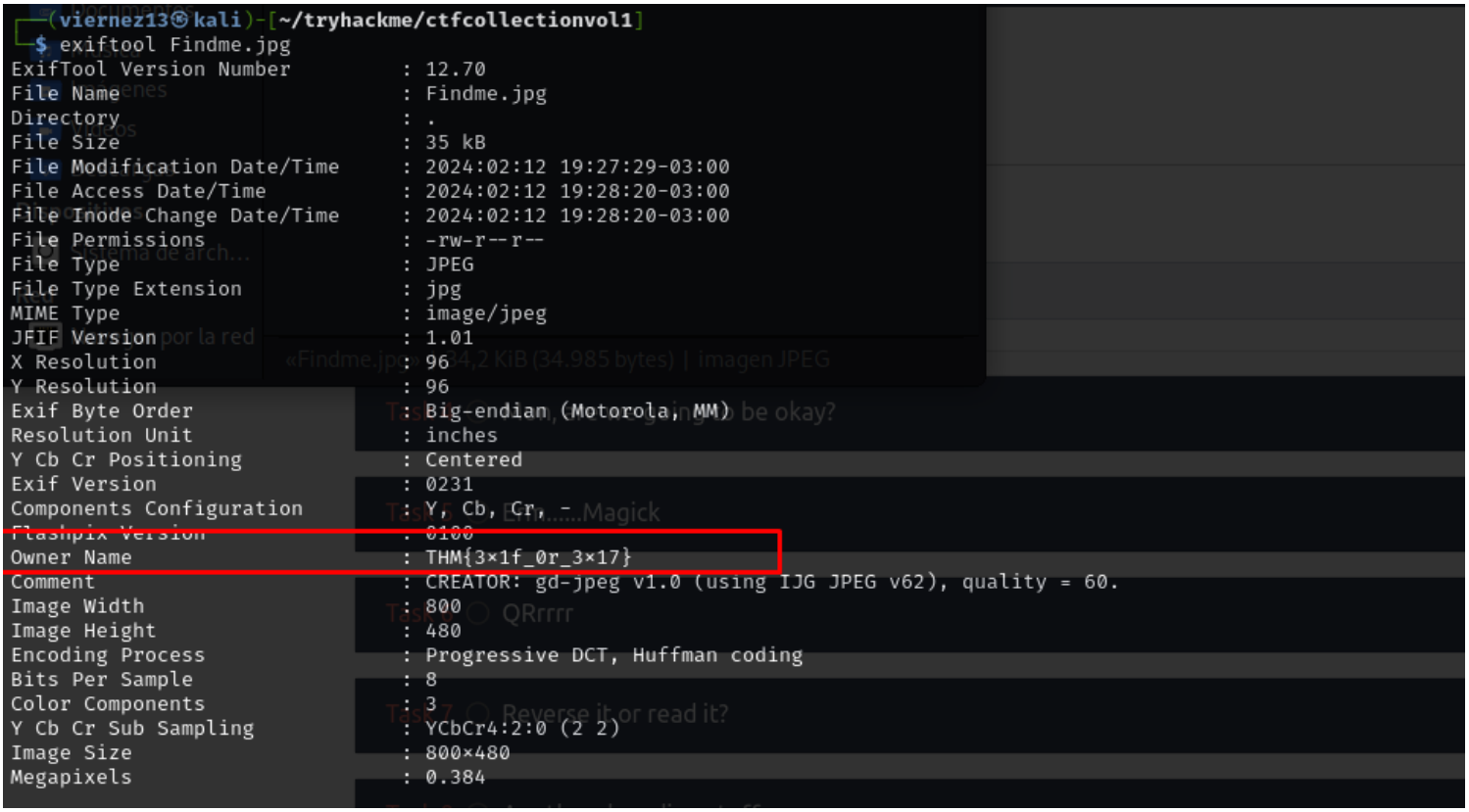
comando= echo -n "VEhNe2p1NTdfZDNjMGQzXzdoM19iNDUzfQ==" | base64 -d
echo -n "textocodificadoenbase64" | base64 -d



Flag:
THM{ju57_d3c0d3_7h3_b453}

Tarea 3 : Meta! meta! meta! meta.....
y adjunta una imagen

se llama findme , la pista que da es meta . meta , deben ser metadatos, haré un prueba copn exifftools



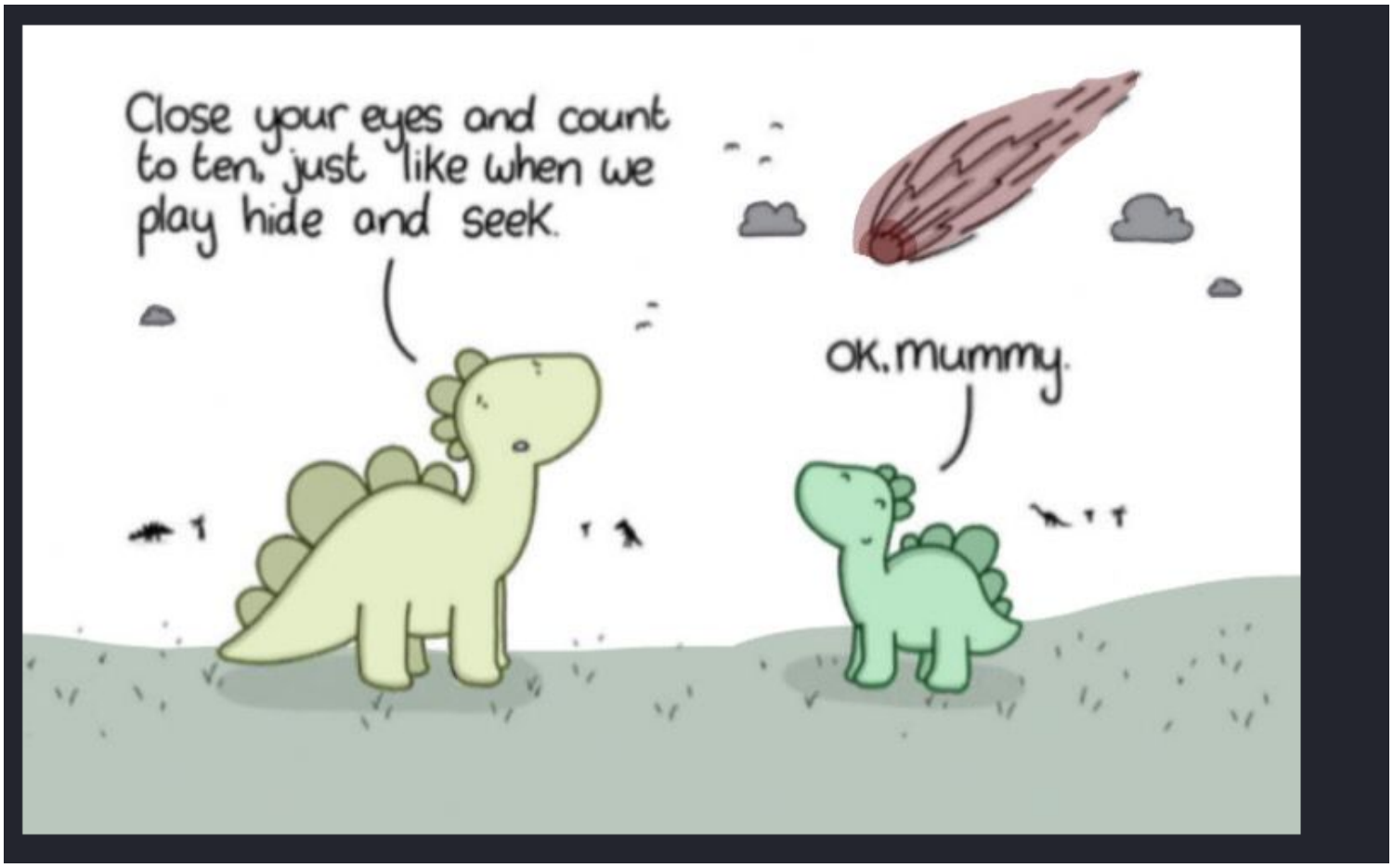
justamente era eso , flag : THM{3x1f_0r_3x17}

Tarea 4 ,

Something is hiding. That's all you need to know.

It is sad. Feed me the flag.

revisando hay una imagen para bajar :



```
└─$ exiftool Extinction.jpg
ExifTool Version Number         : 12.70
File Name                       : Extinction.jpg
Directory                       : .
File Size                       : 28 kB
File Modification Date/Time     : 2024:02:12 19:31:42-03:00
File Access Date/Time           : 2024:02:12 19:33:14-03:00
File Inode Change Date/Time     : 2024:02:12 19:32:07-03:00
File Permissions                : -rw-r--r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Resolution Unit                 : None
X Resolution                    : 1
Y Resolution                    : 1
Image Width                     : 750
Image Height                    : 475
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
Image Size                      : 750×475
Megapixels                      : 0.356
```

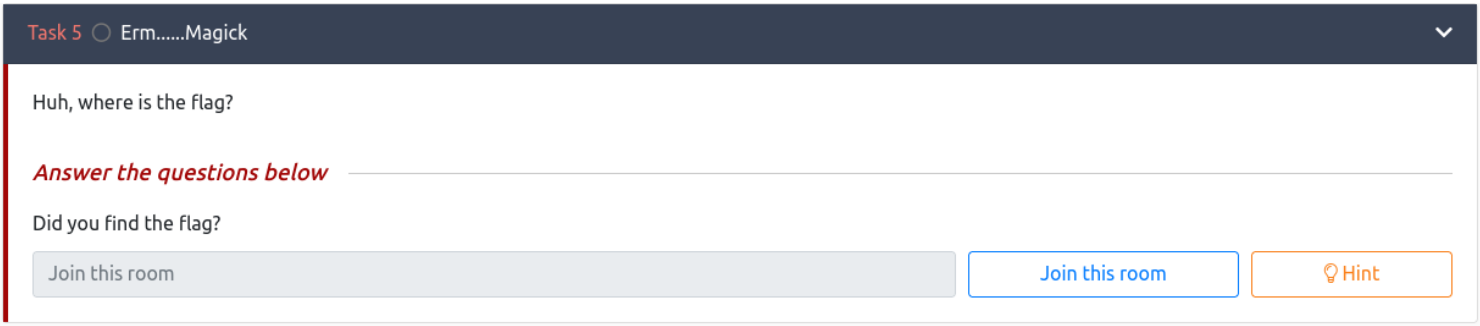
probaremos con steghide ,

```
┌──(viernez13㉿kali)-[~/tryhackme/ctfcollectionvol1]
└─$ steghide info Extinction.jpg
"Extinction.jpg":
  formato: jpeg
  capacidad: 1,3 KB
♦Intenta informarse sobre los datos adjuntos? (s/n) s
Anotar salvoconducto:
  archivo adjunto "Final_message.txt":
    tama♦o: 79,0 Byte
    encriptado: rijndael-128, cbc
    compactado: si
```

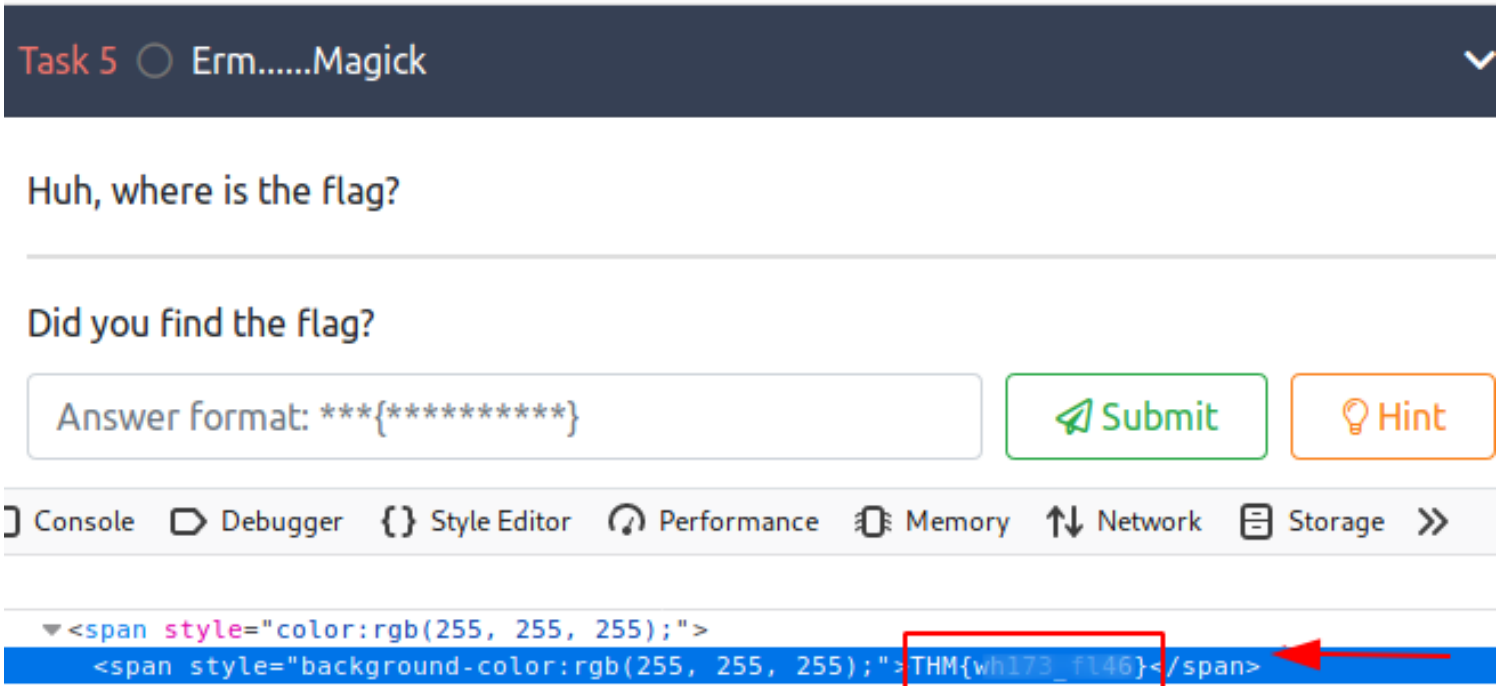
tenemos un archivo para extraer... usaremos el siguiente comando.

```
┌──(viernez13㉿kali)-[~/tryhackme/ctfcollectionvol1]
└─$ steghide extract -sf Extinction.jpg
Anotar salvoconducto:
anot♦ los datos extra♦dos e/"Final_message.txt".

┌──(viernez13㉿kali)-[~/tryhackme/ctfcollectionvol1]
└─$ ls
Extinction.jpg  Final_message.txt  Findme.jpg

┌──(viernez13㉿kali)-[~/tryhackme/ctfcollectionvol1]
└─$ cat Final_message.txt
It going to be over soon. Sleep my child.

THM{500n3r_0r_l473r_17_15_0ur_7urn}

┌──(viernez13㉿kali)-[~/tryhackme/ctfcollectionvol1]
└─$
```

flag:THM{500n3r_0r_l473r_17_15_0ur_7urn}
tarea5



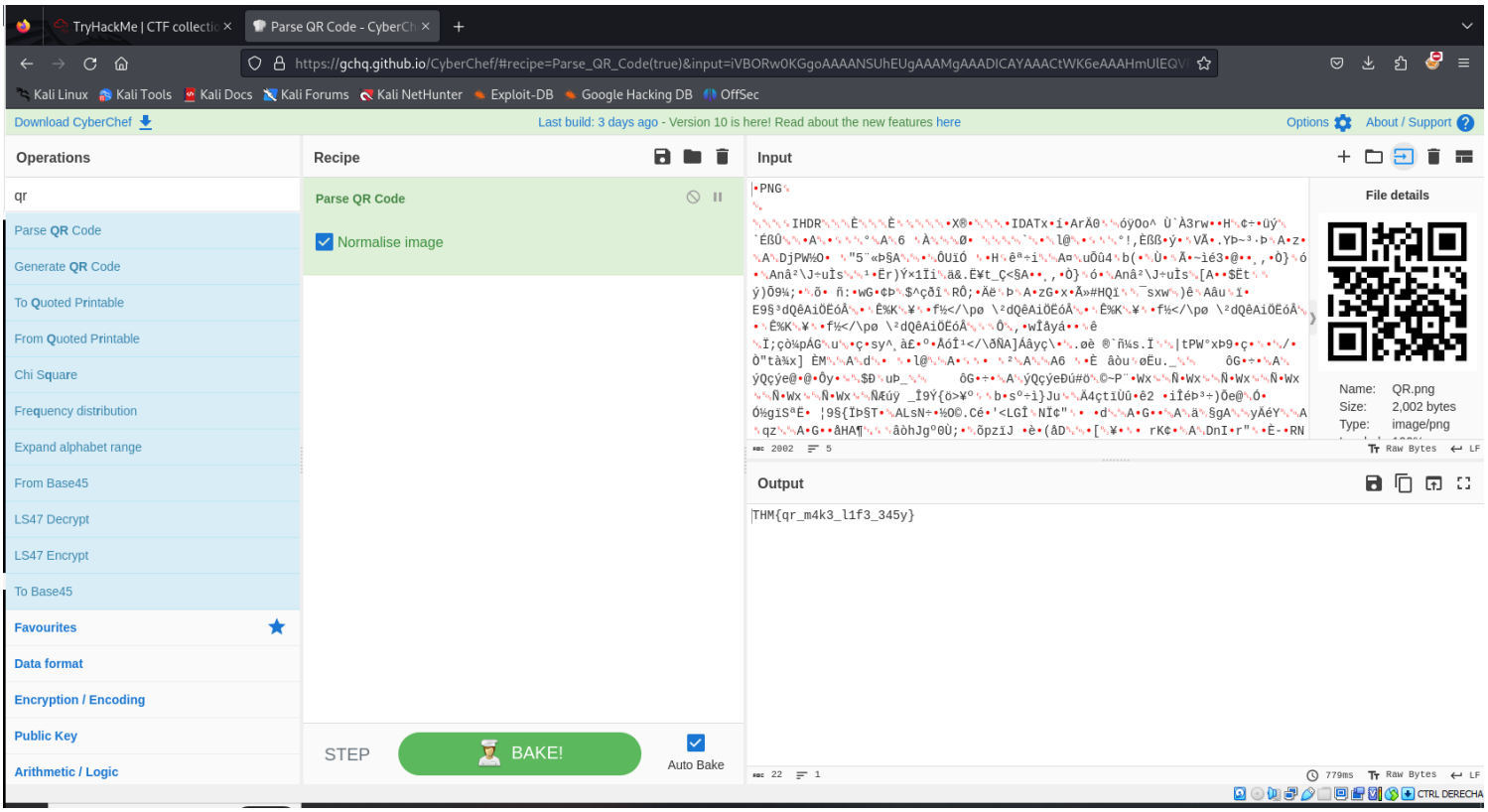
WTF no hay donde buscar , no hay datos a descargar ¿habrá que inspeccionar la página?



Flag: THM{wh173_fl46}
Tarea 6

Such technology is quite reliable.

hay un qr para revisar , lo abri con cyberchef y lo tradujo en un instante.

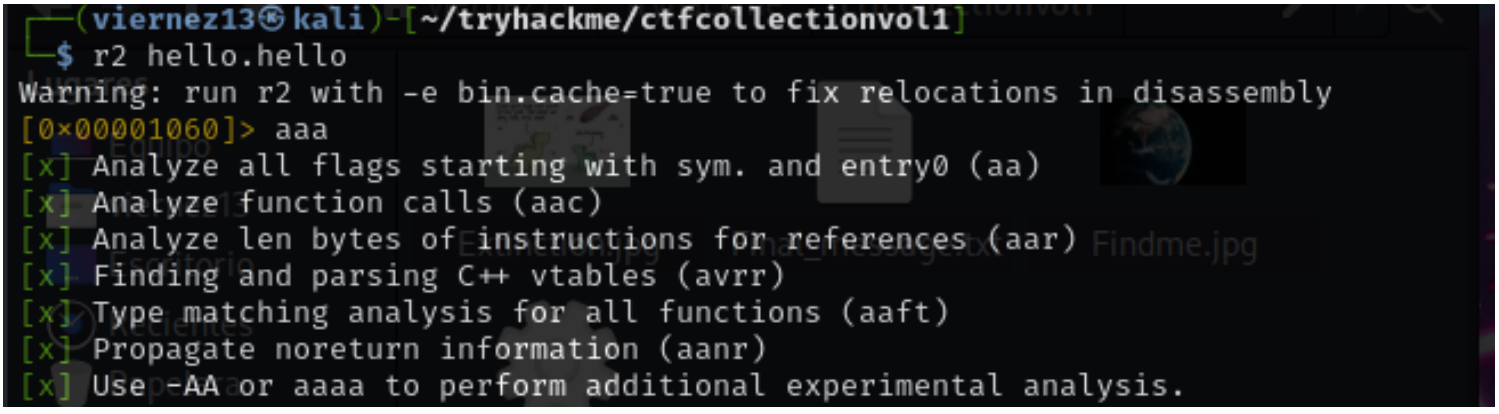


Flag: THM{qr_m4k3_l1f3_345y}

Tarea7 :
Both works, it's all up to you.

bajamos un archivo llamado hello.hello

la vamos a desamblar con R2



usamos el comando afl

```
[0×00001060]> afl
0×00001060     1 43           entry0
0×00001090     4 41   → 34    sym.deregister_tm_clones
0×000010c0     4 57   → 51    sym.register_tm_clones
0×00001100     5 57   → 50    sym.__do_global_dtors_aux
0×00001050     1 6            sym.imp.__cxa_finalize
0×00001140     1 5            entry.init0
0×00001000     3 23           sym._init
0×000011e0     1 1            sym.__libc_csu_fini
0×00001145     1 24           sym.skip
0×00001040     1 6            sym.imp.printf
0×000011e4     1 9            sym._fini
0×00001180     4 93           sym.__libc_csu_init
0×0000115d     1 23           main
0×00001030     1 6            sym.imp.puts
[0×00001060]>
```

pdf @sym.skip

```
[0×00001060]> pdf @sym.skip
 24: sym.skip ();
           0×00001145      55             push rbp
           0×00001146      4889e5         mov rbp, rsp
           0×00001149      488d3db80e00.  lea rdi, str.THM345y_f1nd_345y_60 ; 0×2008 ; "THM{345y_f1nd_345y_60}" ; const char *format
           0×00001150      b800000000     mov eax, 0
           0×00001155      e8e6feffff     call sym.imp.printf        ; int printf(const char *format)
           0×0000115a      90             nop
           0×0000115b      5d             pop rbp
           0×0000115c      c3             ret
[0×00001060]>
```

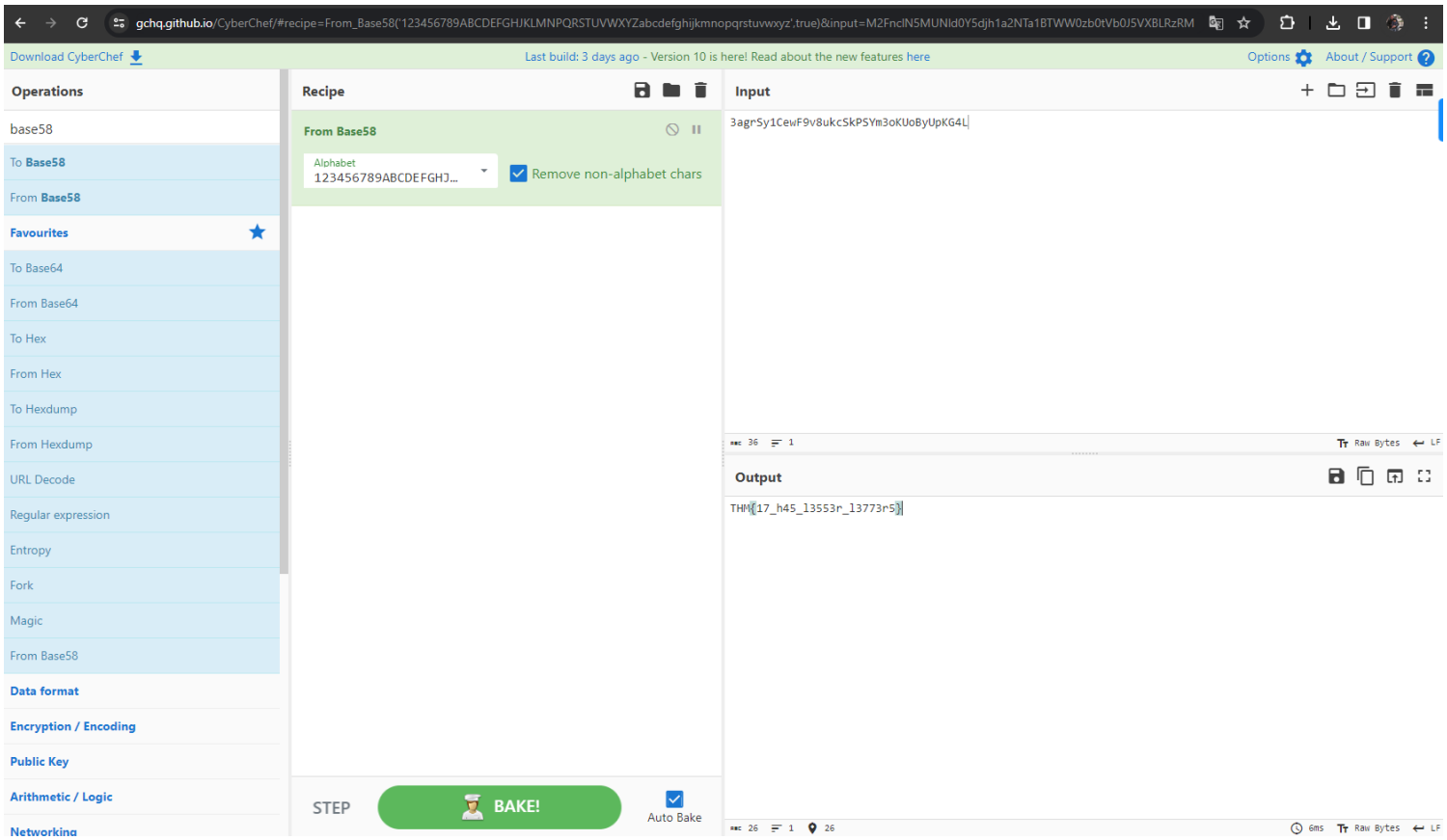
Flag : THM{345y_f1nd_345y_60}

Tarea 8:

Can you decode it?

`3agrSy1CewF9v8ukcSkPSYm3oKUoByUpKG4L`

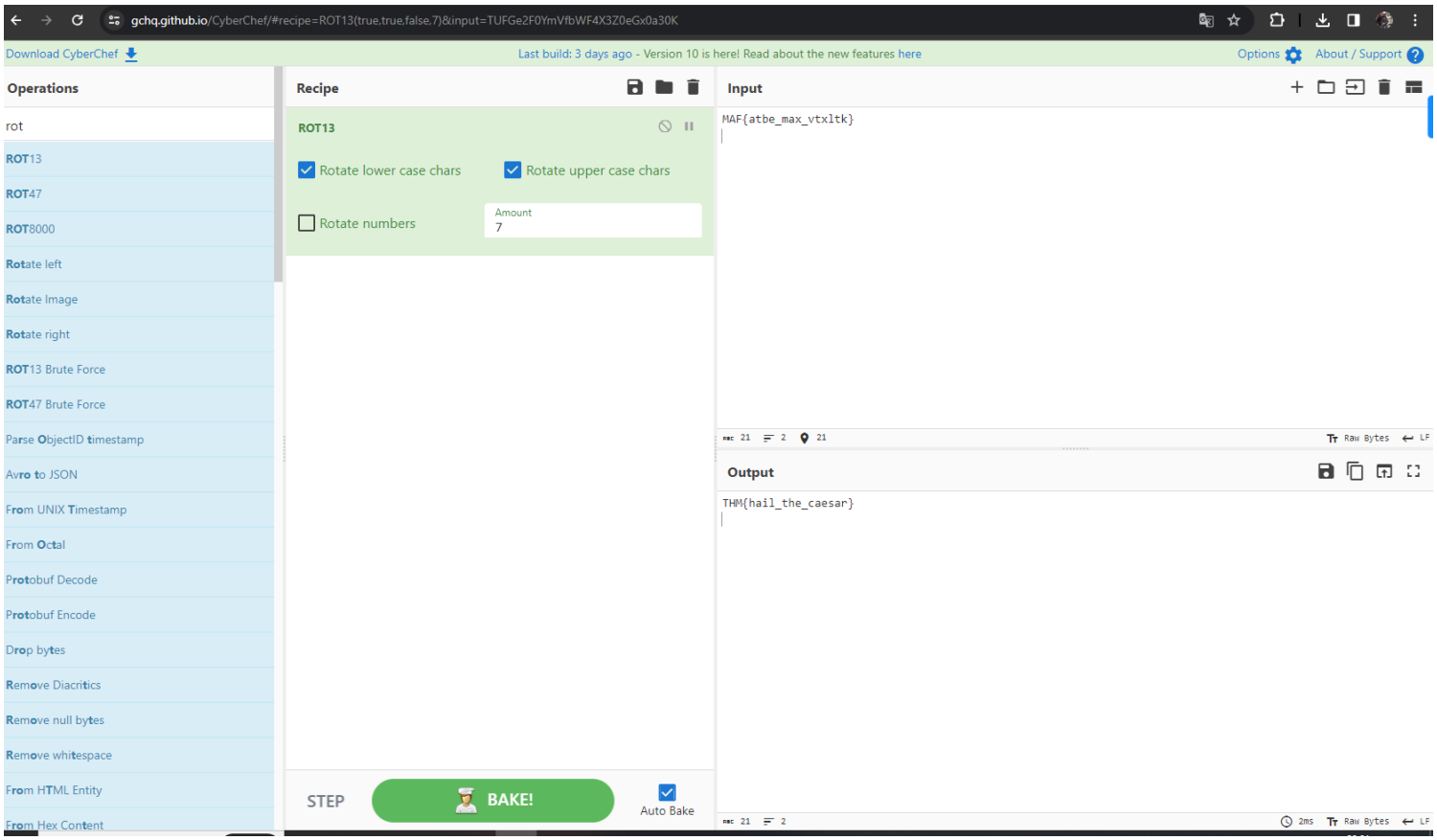
es base58



flag : THM{17_h45_l3553r_l3773r5}

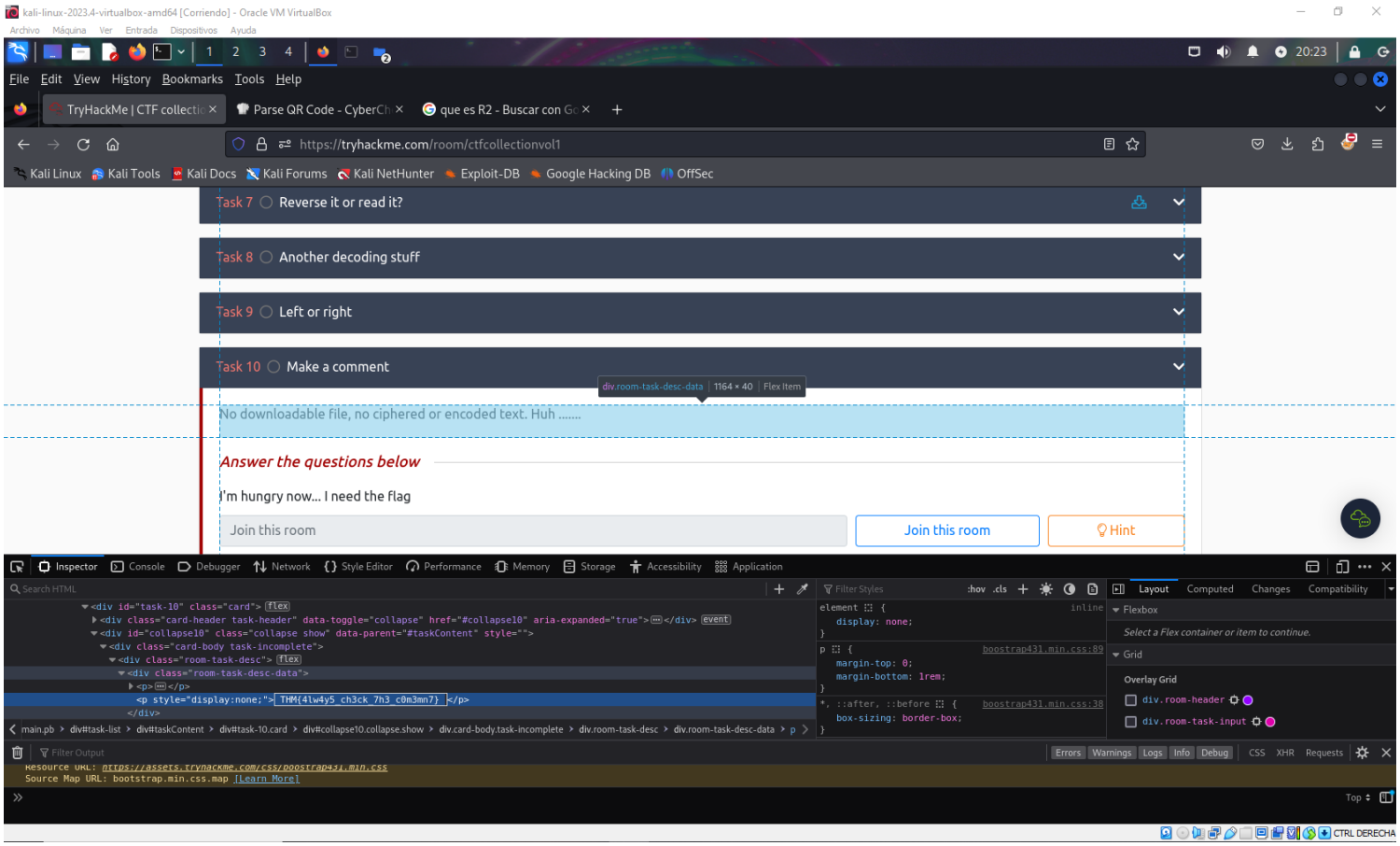
Tarea 9:

Left, right, left, right... Rot 13 is too mainstream. Solve this
MAF{atbe_max_vtxltk}
en un principio es rot 13 pero hay que bajarle las posiciones a 7



Flag: THM{hail_the_caesar}

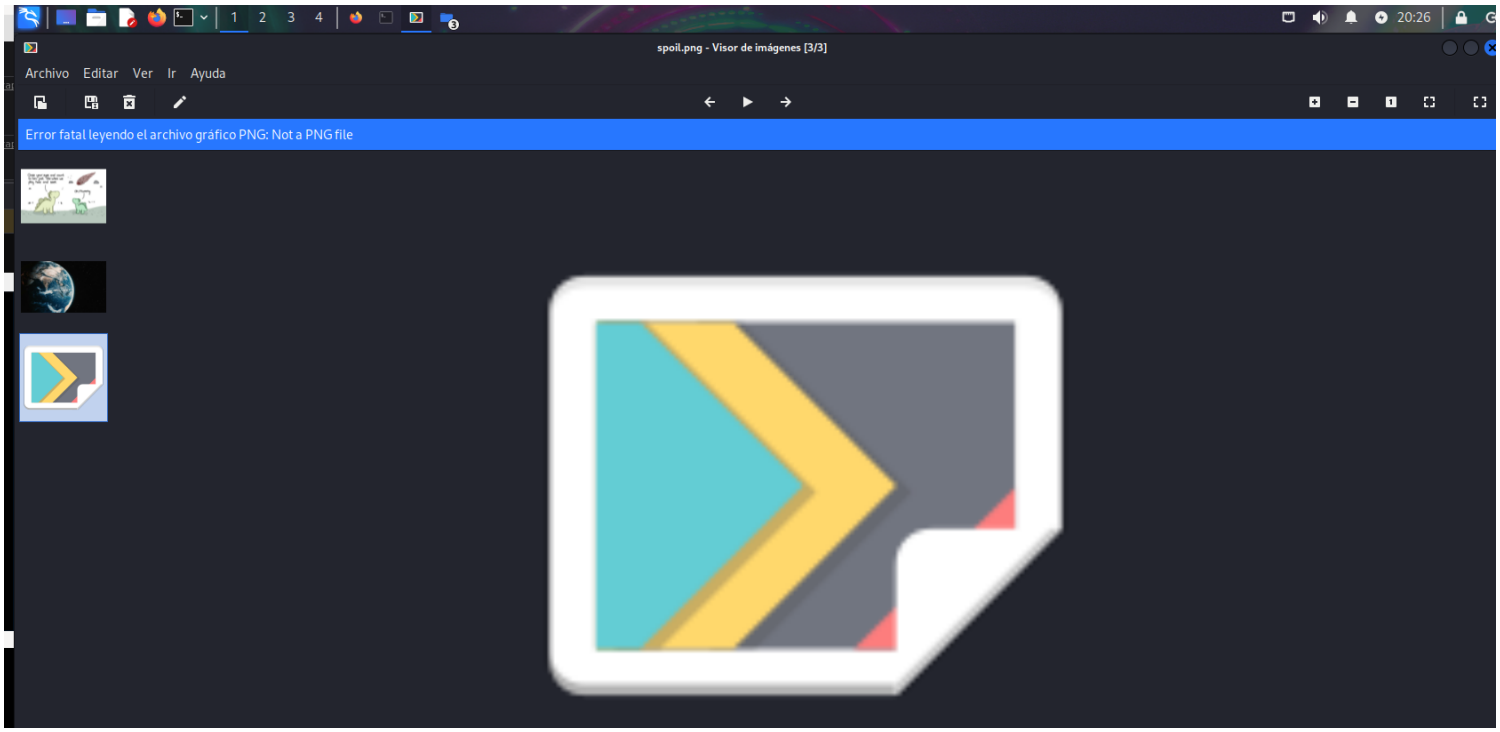
Tarea 10
No downloadable file, no ciphered or encoded text. Huh .....
nos da indicios de que hay algo en el código manos a la obra...



Flag: THM{4lw4y5_ch3ck_7h3_c0m3mn7}

Tarea 11

accidentally messed up with this PNG file. Can you help me fix it? Thanks, ^^



Dumpeamos en hexa el archivo spoil.png

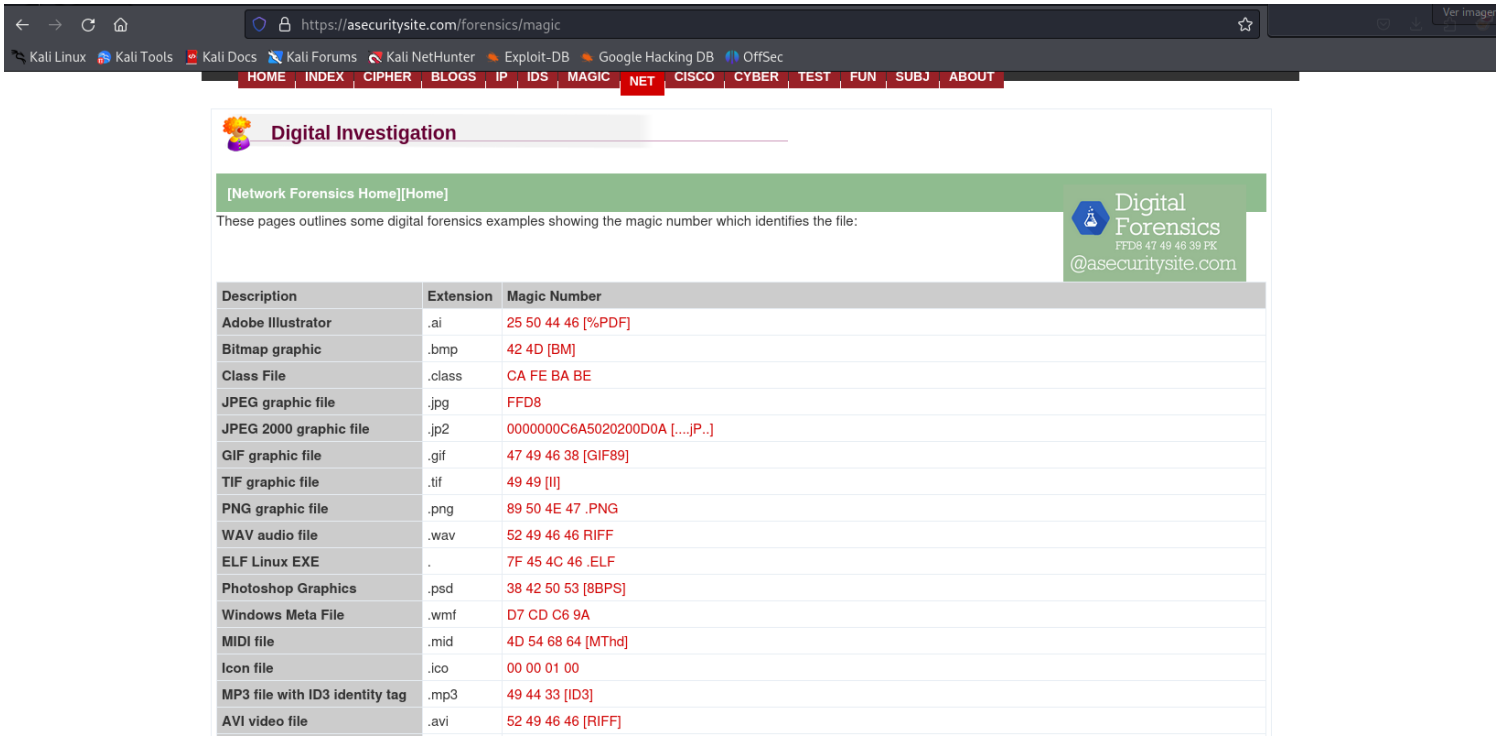
```
┌──(viernez13㉿kali)-[~/tryhackme/ctfcollectionvol1]
└─$ xxd -p spoil.png > spoil_hex_data
```

leemos la cabecera

```
└─$ head spoil_hex_data
2333445f0d0a1a0a0000000d49484452000003200000032008060000000db
70066800000001735247420aece1ce900000009704859730000ec40000
0ec401952b0e1b0000200049444154789cecdd799c9c559deff1cf799e5a
bb7a5f927477f6404802092011 50c420bba288a8805c19067c5d64c079e9
752e03ce38e30e8e2f75e63a23ea8c0ce8308e036470c191cd80880c4b20
0909184c42b64ed2e9f4bed7f23ce7fe51559dea4e27a4bbaaf7effbf5ea
57d2d5554f9daa7abafa7ceb9cf33bc65a6b1111111111111907ce443740
4444444444660e0510111111111119370a20222222222326e1440444444
444464dc28808888888888c8b85100111111111119171a300222222222222
e34601444444444444c68d028888888888888c1b0510111111111119370a
```

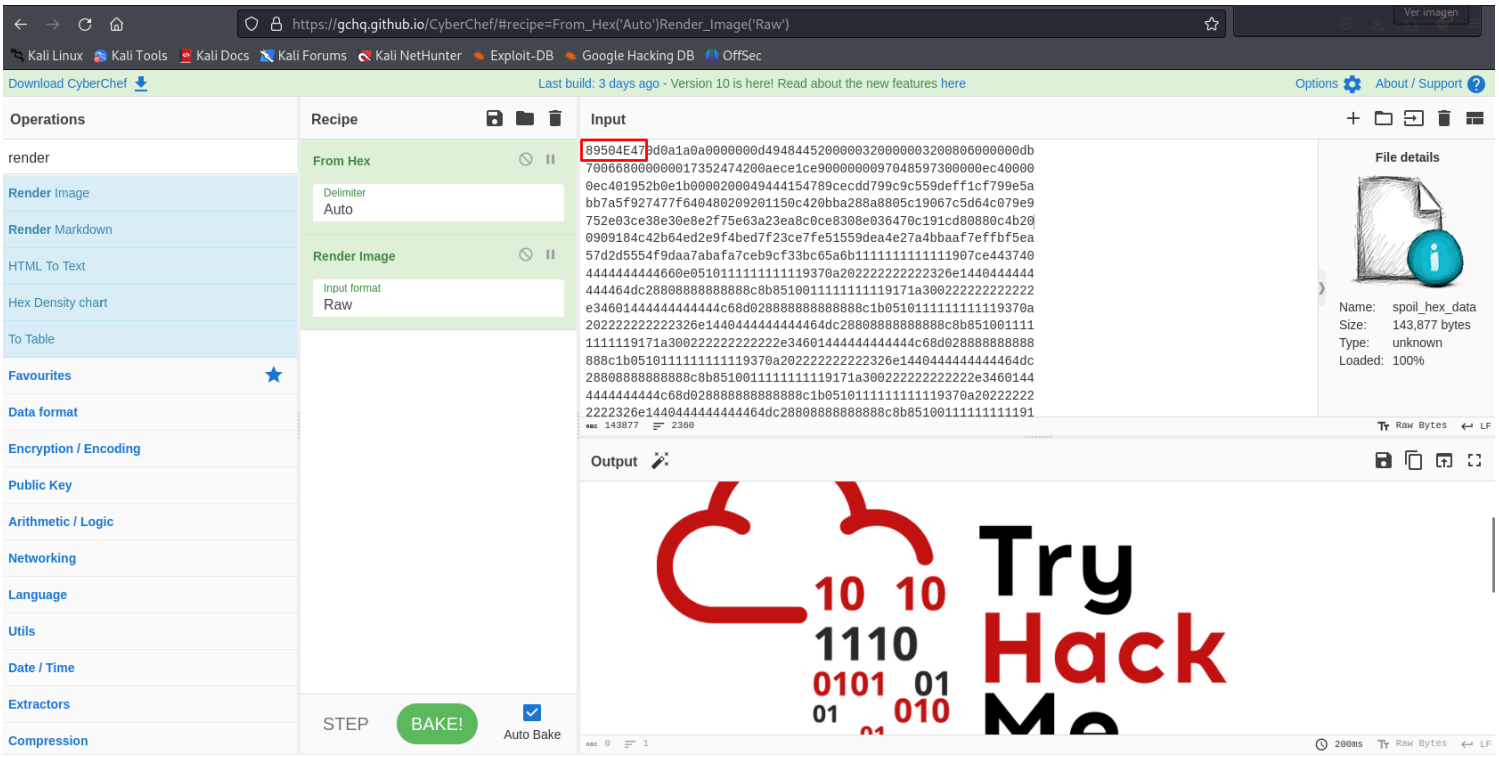
2333445f
89504E47

Segun lo revisado , esos numeros no corresponden a PNG



Description	Extension	Magic Number
Adobe Illustrator	.ai	25 50 44 46 [%PDF]
Bitmap graphic	.bmp	42 4D [BM]
Class File	.class	CA FE BA BE
JPEG graphic file	.jpg	FFD8
JPEG 2000 graphic file	.jp2	0000000C6A5020200D0A [....jP..]
GIF graphic file	.gif	47 49 46 38 [GIF89]
TIF graphic file	.tif	49 49 [II]
PNG graphic file	.png	89 50 4E 47 .PNG
WAV audio file	.wav	52 49 46 46 RIFF
ELF Linux EXE	.	7F 45 4C 46 .ELF
Photoshop Graphics	.psd	38 42 50 53 [8BPS]
Windows Meta File	.wmf	D7 CD C6 9A
MIDI file	.mid	4D 54 68 64 [MThd]
Icon file	.ico	00 00 01 00
MP3 file with ID3 identity tag	.mp3	49 44 33 [ID3]
AVI video file	.avi	52 49 46 46 [RIFF]

uhmmm sospechoso llevaremos el dump a cyberchef y cambiaremos los numeros mágicos a PNG



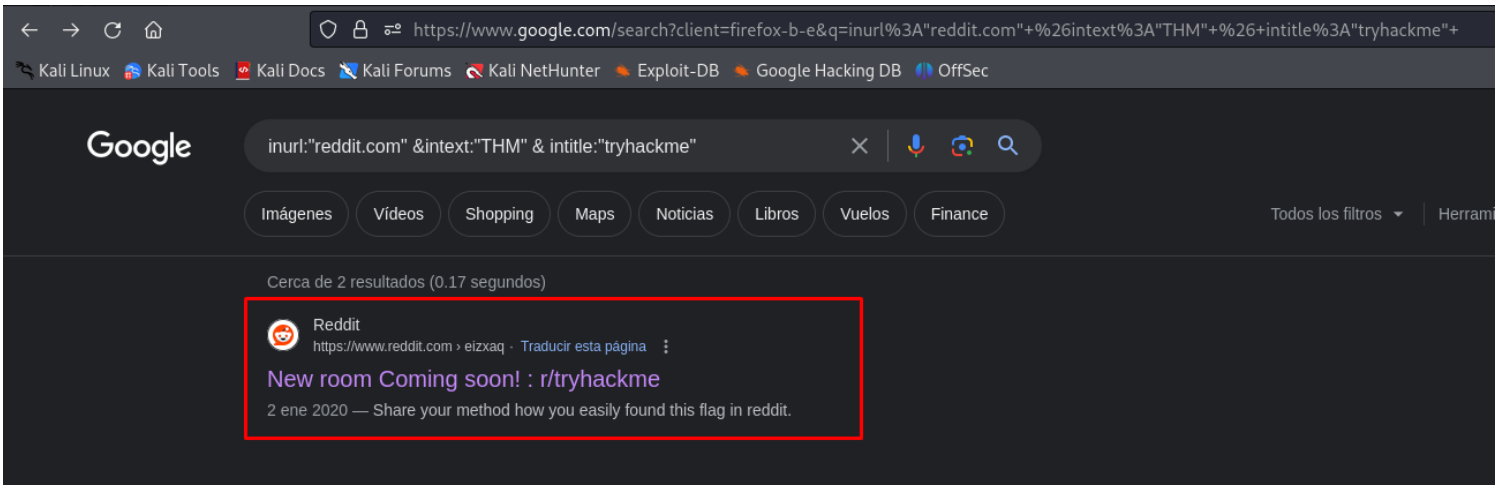
lo que obtuvimos es la flag :

Tarea 12

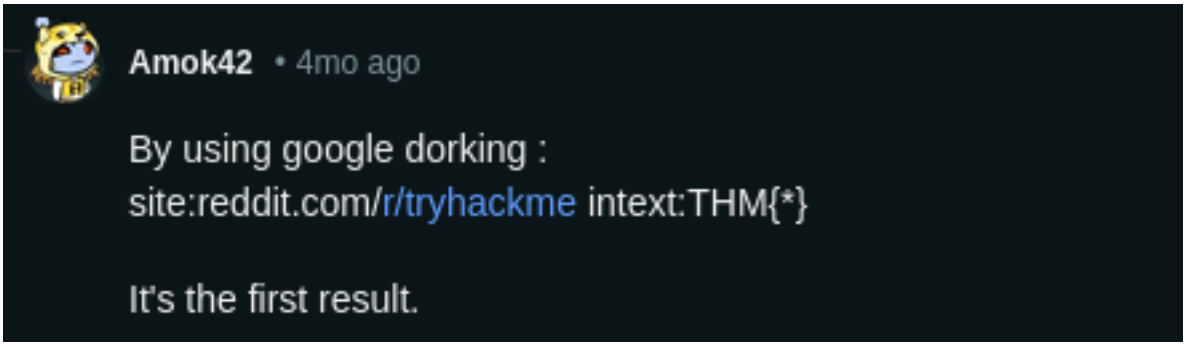
Some hidden flag inside Tryhackme social account.

la pista dice que es en reddit por lo cual ya podemos aplicar google dorking.

inurl:"reddit.com" &intext:"THM" & intitle:"tryhackme"

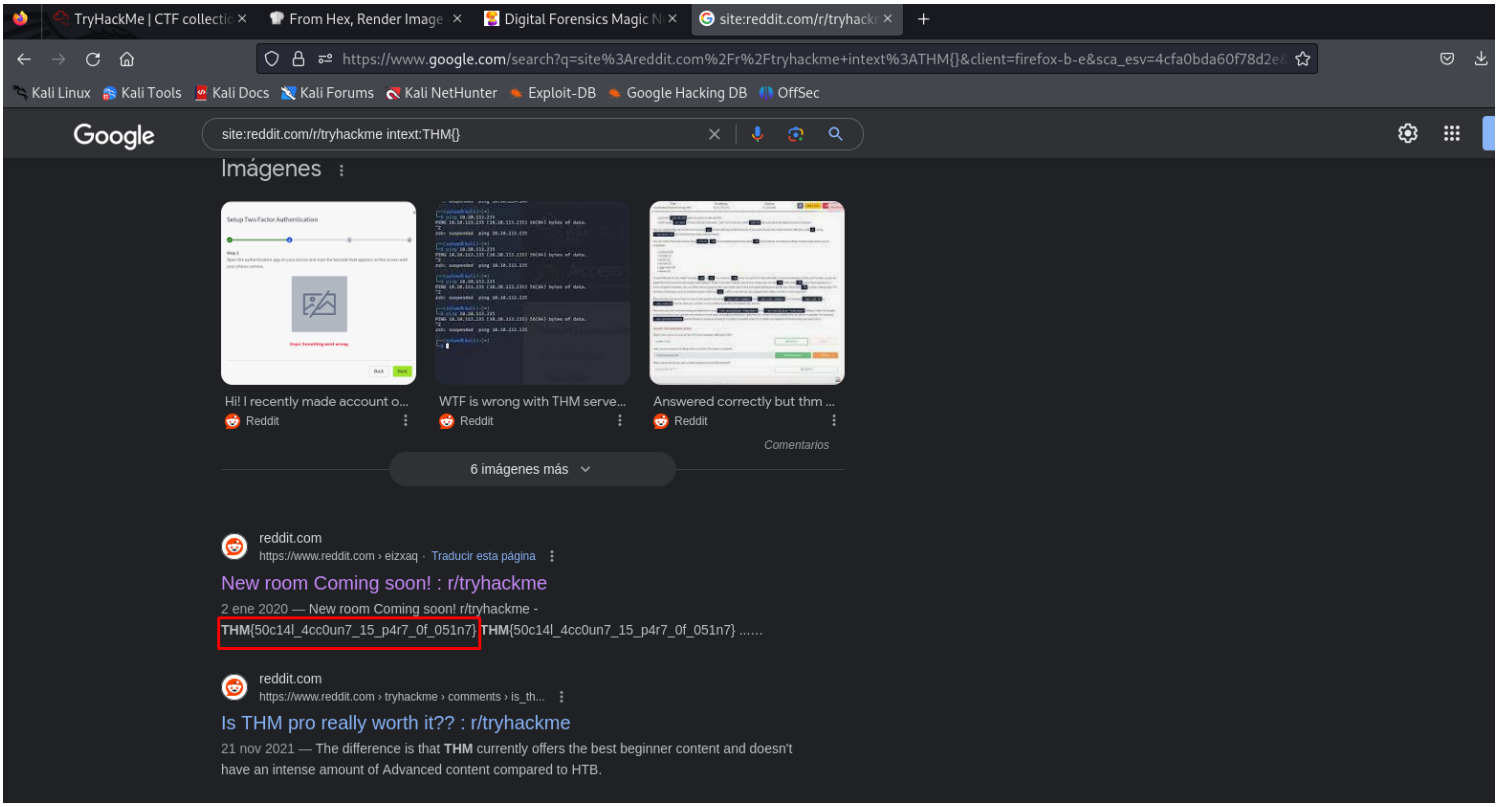


ingresamos.
encontramos este comentario,



Modificamos el dork , sacando el asterisco al medio de los corchetes y lo aplicamos.

site:reddit.com/r/tryhackme intext:THM{}

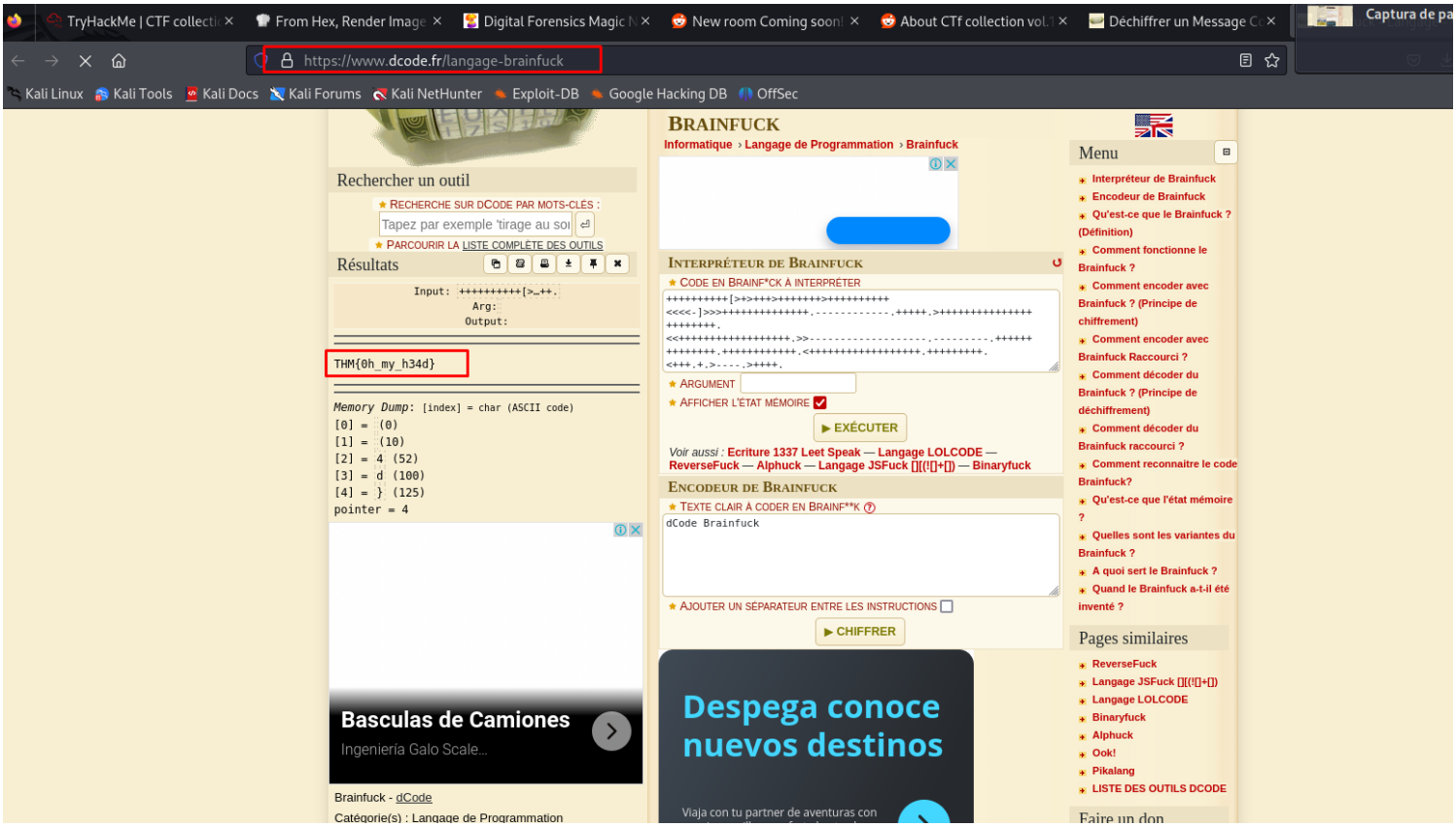


Flag: *THM*{50c14l_4cc0un7_15_p4r7_0f_051n7}

Tarea 13

What is this?
++++++++++[>+>+++>+++++++>++++++++++<<<<-]>>>++++++++++++++.----------.+++++.>++++++++++++++++++++++++++.<<++++++++++++++++++.>>----------.---------.+++++++++++++.++++++++++++.<++++++++++++++.+++++++++.<+++.+.>----.>++++.

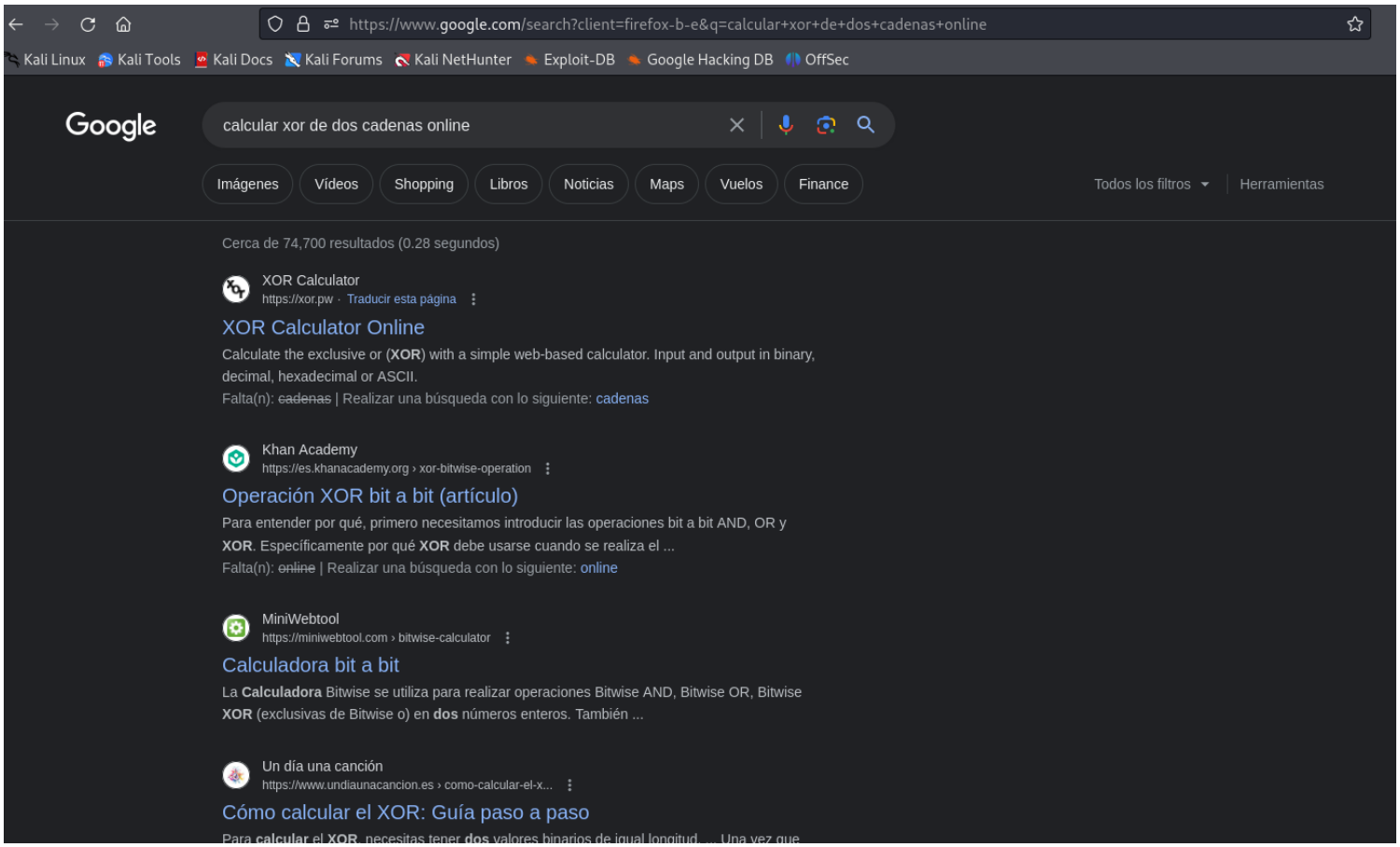
en otras entregas de write ups , les expliqué sobre el cifrado brainfuck , parece ser este , intentaremos descifrarlo con la página dcode.fr



Flag: THM{0h_my_h34d}
tarea 14

Exclusive strings for everyone!
S1: 44585d6b2368737c65252166234f20626d
S2: 10101010101010101010101010101010

En esta tarea, obtuvimos 2 cadenas pero no sabíamos qué hacer con estas cadenas, el hint muestra XOR estas cadenas.



ambos valores son base 16 y lo queremos es que sea un ascii de base 256 ponemos las dos cadenas y ya está.

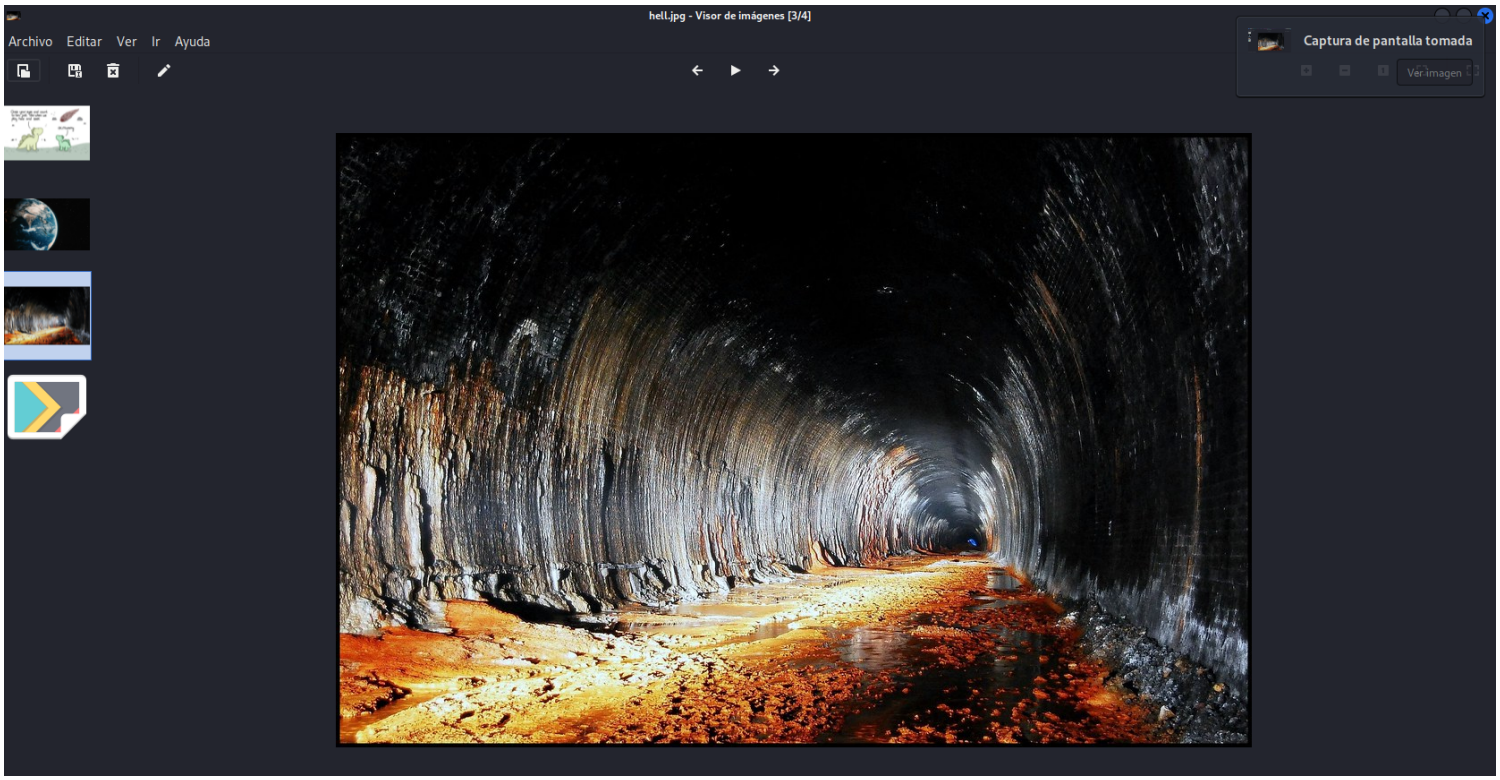
Flag : THM{3xclu51v3_0r}

tarea 15
Please exfiltrate my file :)

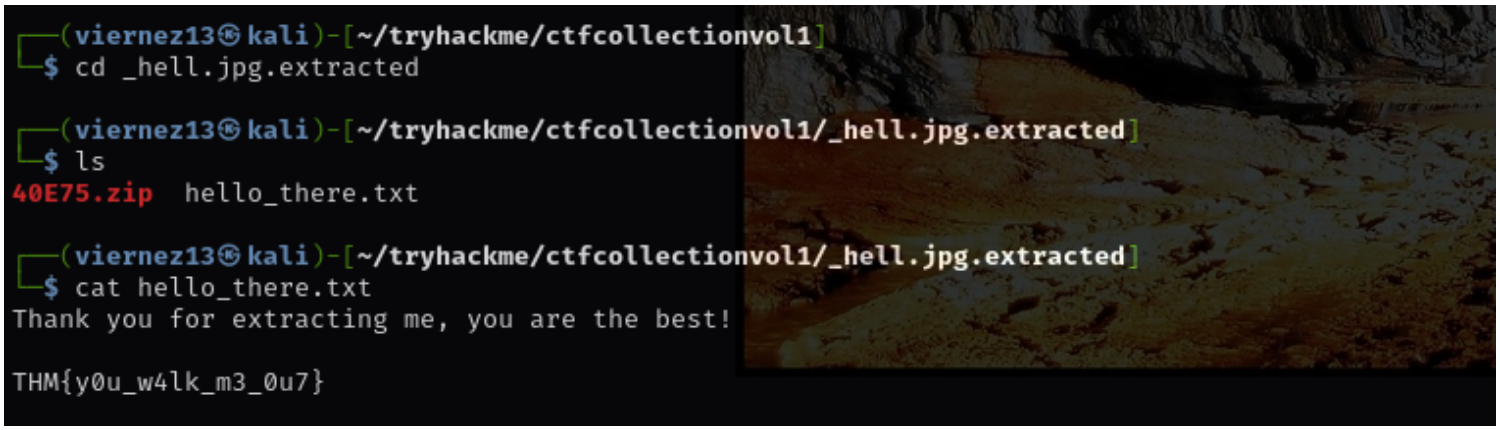
Answer the questions below

Flag! Flag! Flag!

tiene una imagen adjunta :



el titulo es binary walk , creo que hay una herramienta llamada binwalk



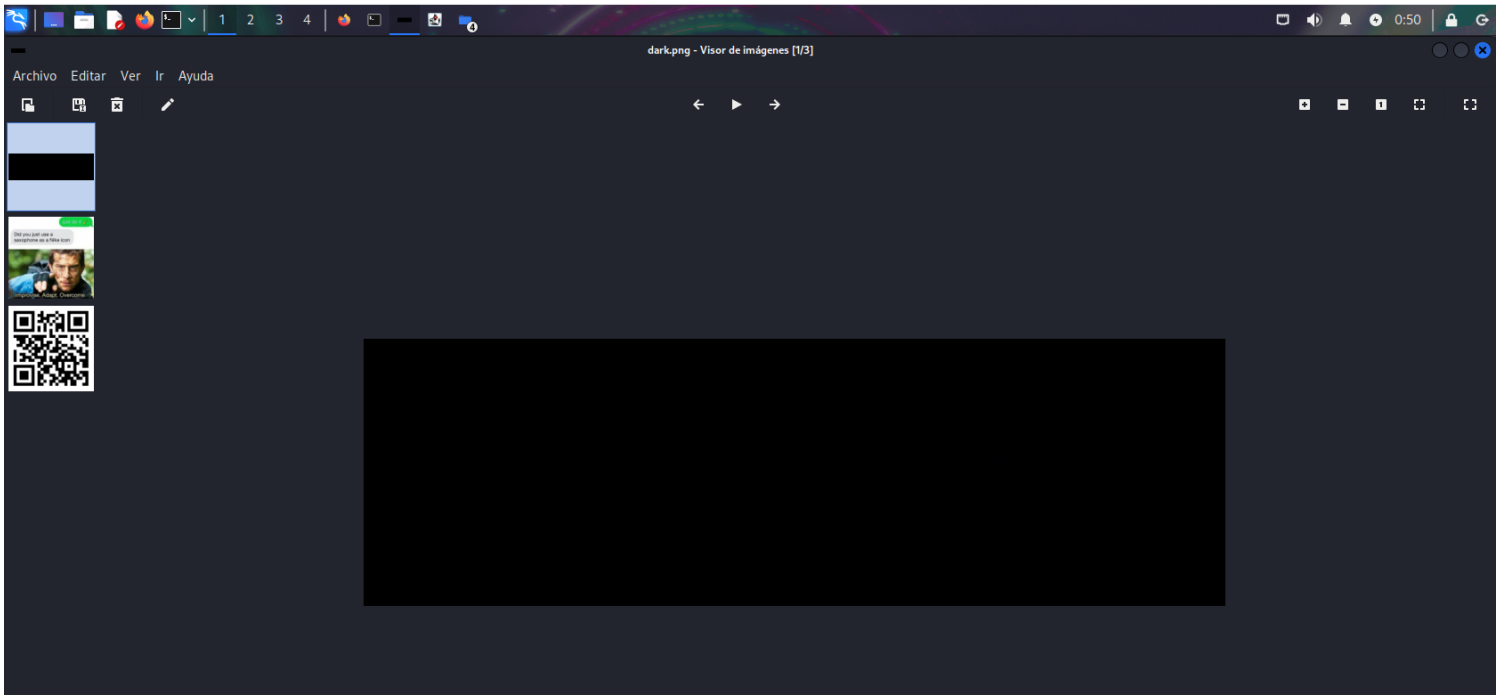
cat
hello_there.txt

Thank you for extracting me, you are the best!

THM{y0u_w4lk_m3_0u7}

Flag : THM{y0u_w4lk_m3_0u7}

tarea 16 : There is something lurking in the dark.



usaré para este reto stegsolve

Installation

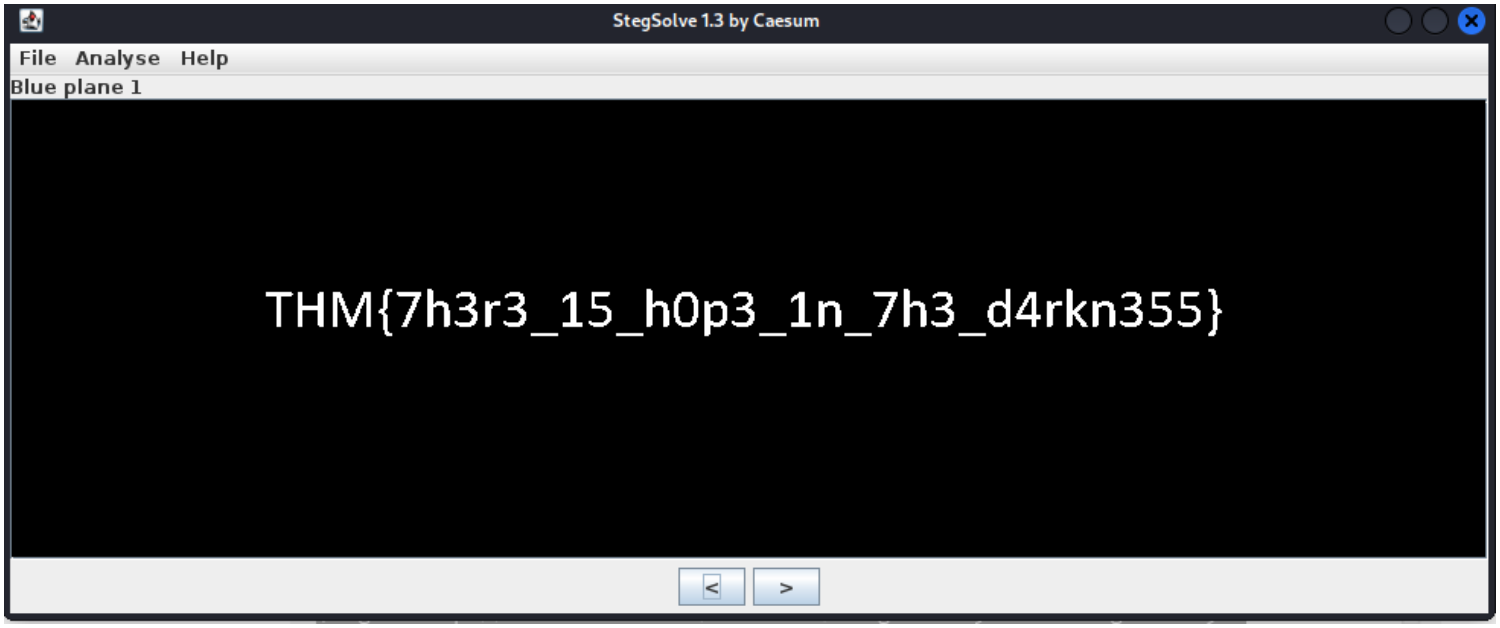
```
$ wget http://www.caesum.com/handbook/Stegsolve.jar -O stegsolve.jar
$ chmod +x stegsolve.jar
$ mkdir bin
$ mv stegsolve.jar bin/
```

Usage

Stegsolve can be invoked by placing the image in the /bin folder and running stegsolve.

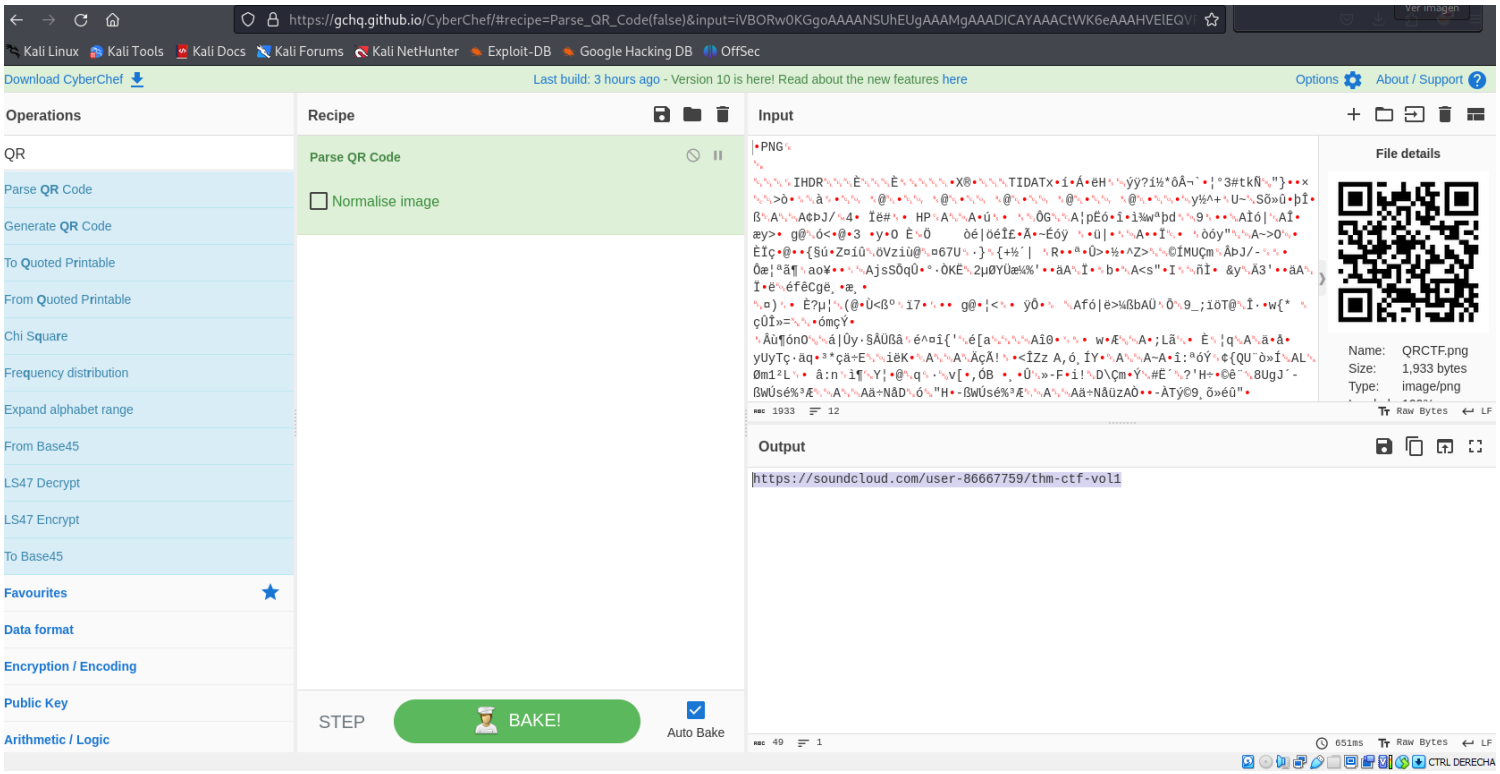
```
$ java -jar stegsolve.jar
```

una vez instalada abirir el archivo e ir aplicando filtros con las flechas , hasta llegar una que delate el mensaje oculto.



THM{7h3r3_15_h0p3_1n_7h3_d4rkn355}

Tarea 17 :

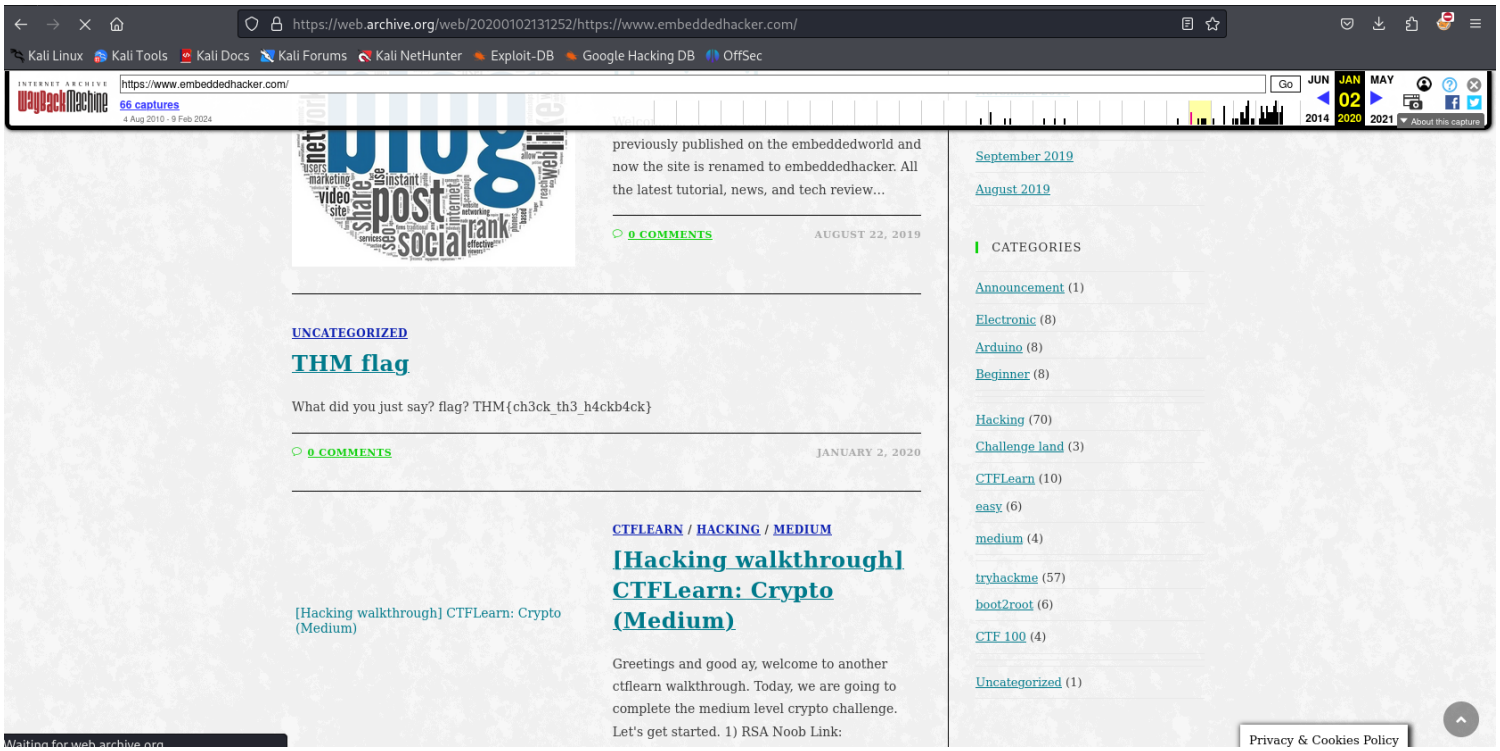


https://soundcloud.com/user-86667759/thm-ctf-vol1

THM{soundingqr}

tarea18
Sometimes we need a 'machine' to dig the past
Targetted website: https://www.embeddedhacker.com/
Targetted time: 2 January 2020

ocuparemos waybackmachine.

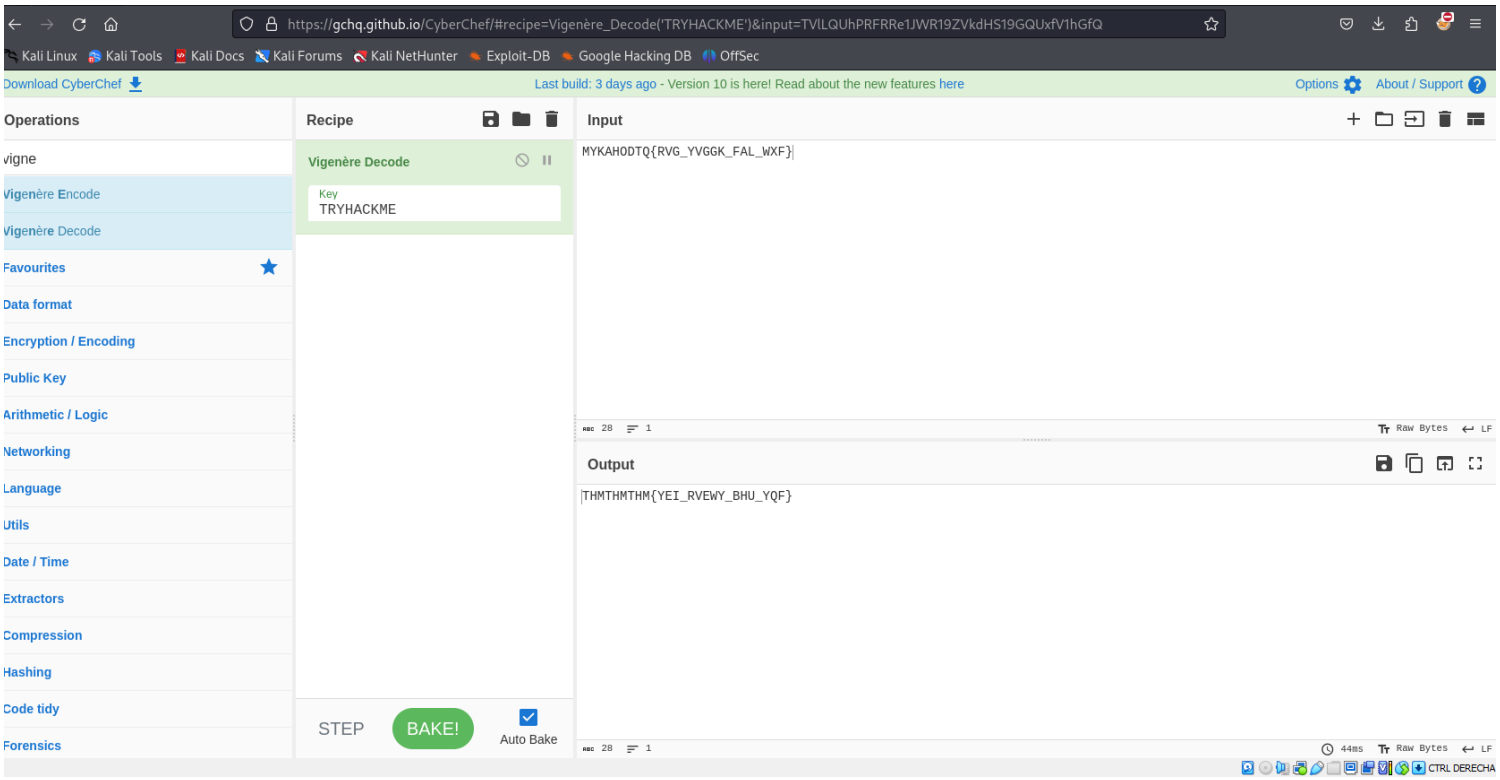


Flag ;: THM{ch3ck_th3_h4ckb4ck}

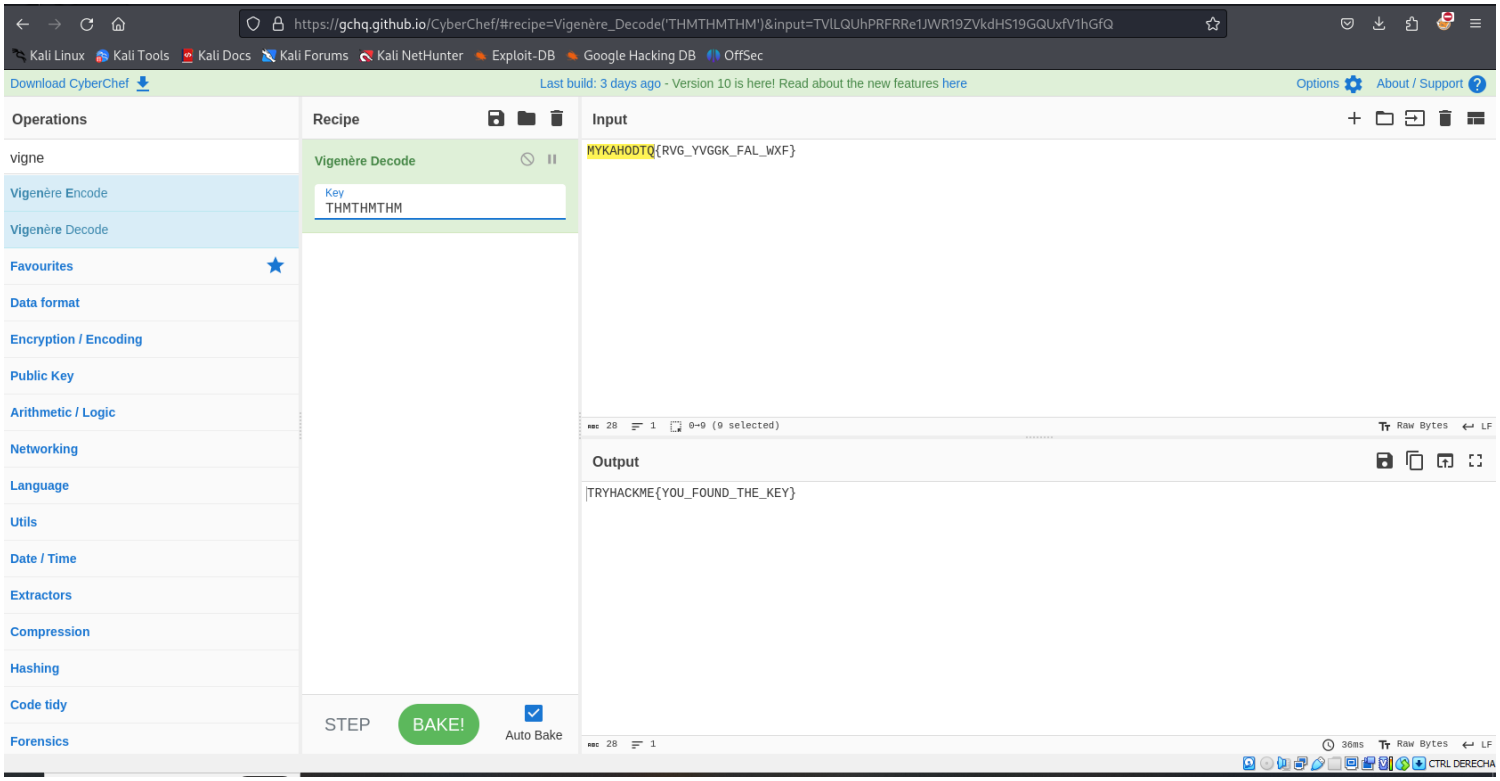
TArea19
Can you solve the following? By the way, I lost the key. Sorry >.<

MYKAHODTQ{RVG_YVGGK_FAL_WXF}
Flag format: TRYHACKME{FLAG IN ALL CAP}

parece ser cifrado vignere,

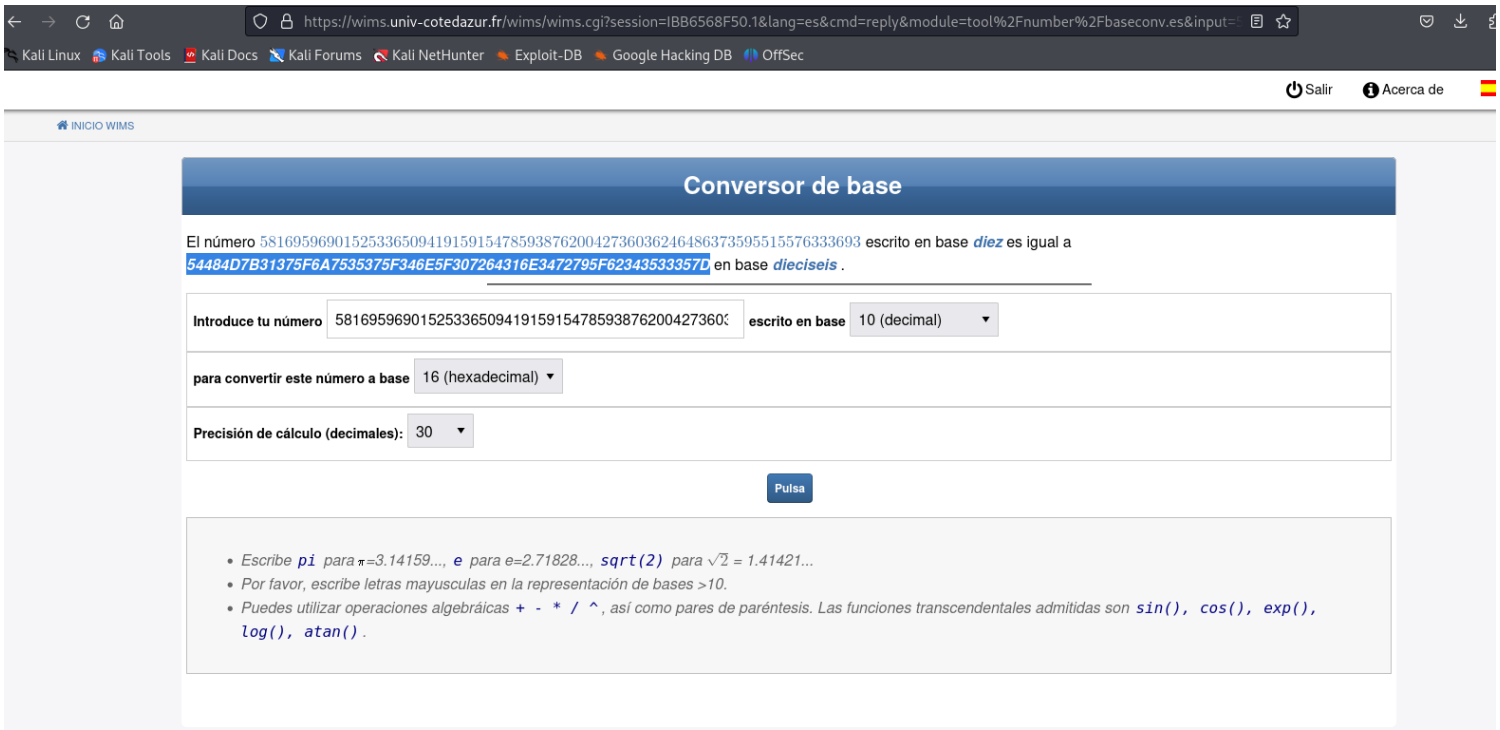


THMTHMTHM{YEI_RVEWY_BHU_YQF}



TRYHACKME{YOU_FOUND_THE_KEY}

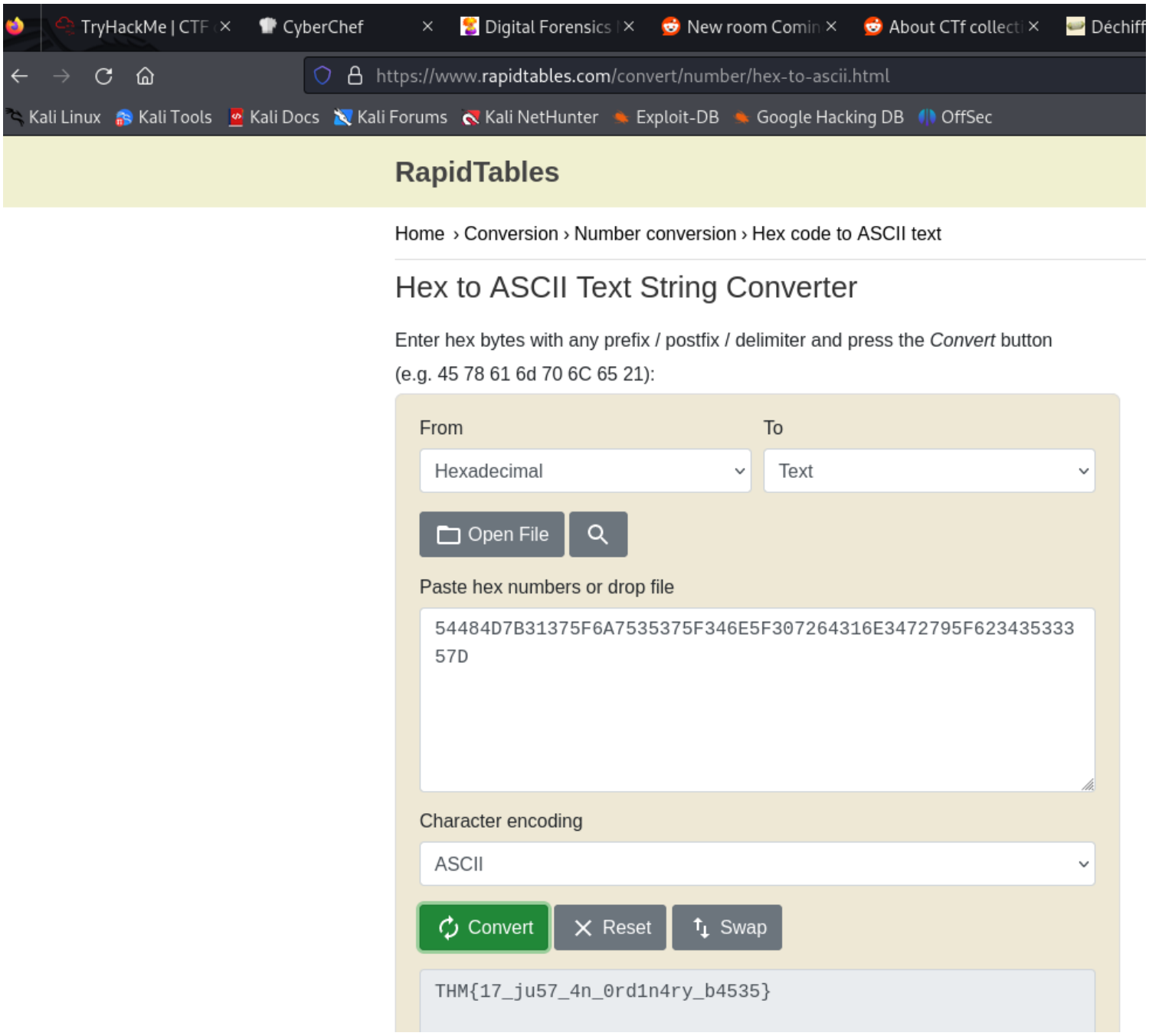
lo convertimos primero a hexa .



y luego de hexa a ascii

tarea 20

Decode the following text.
581695969015253365094191591547859387620042736036246486373595515576333693

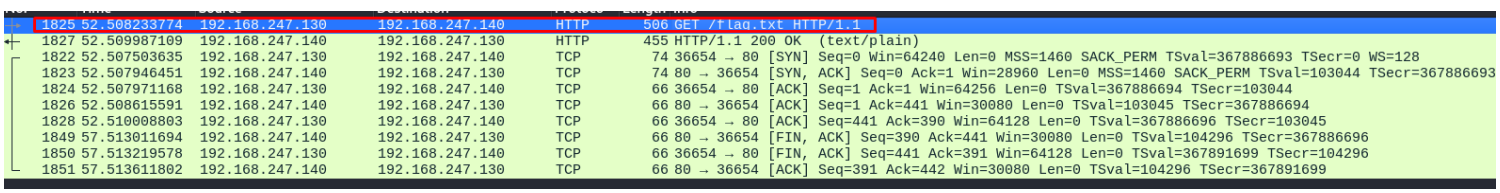


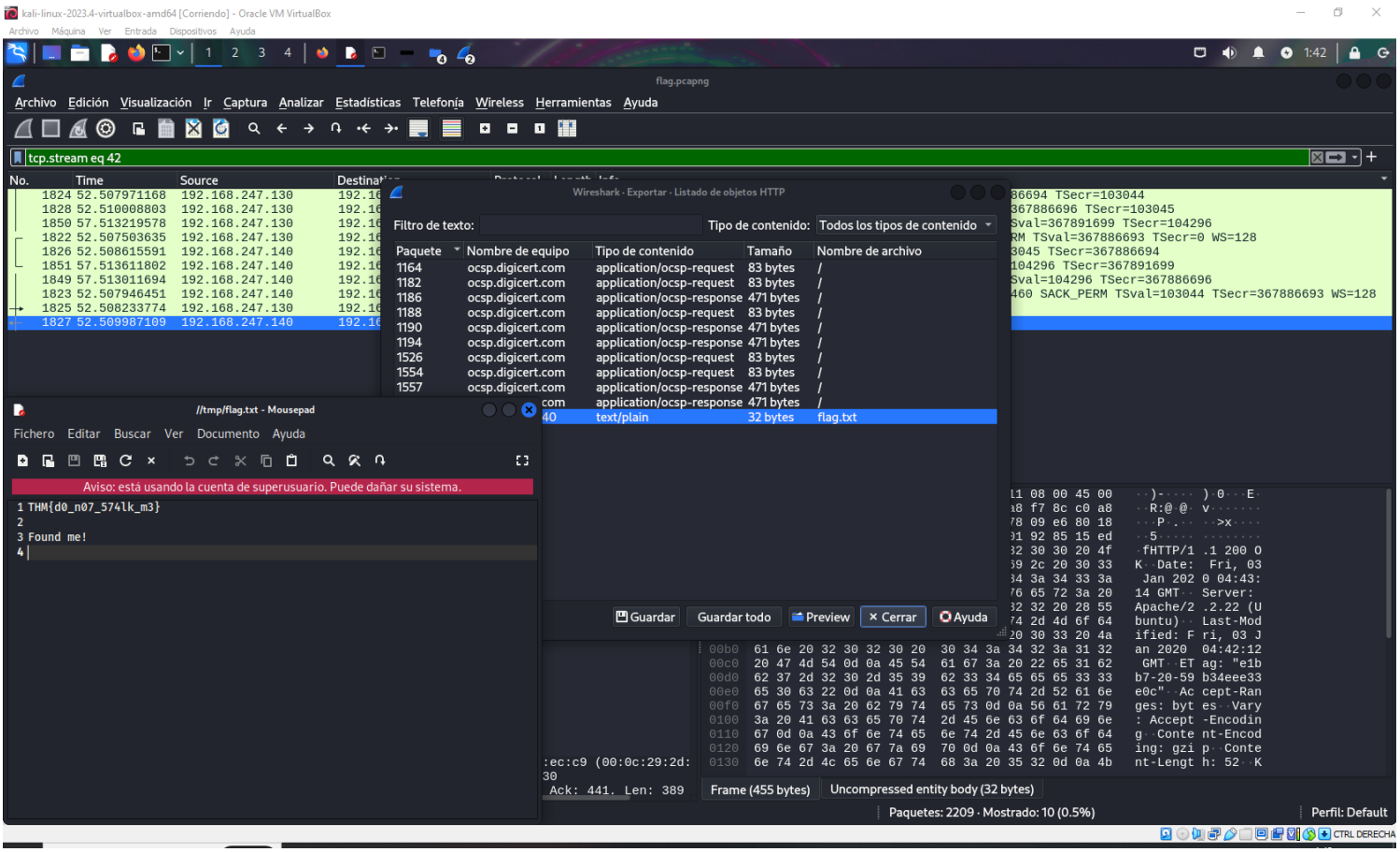
flag= THM{17_ju57_4n_0rd1n4ry_b4535}

tarea 21 y final

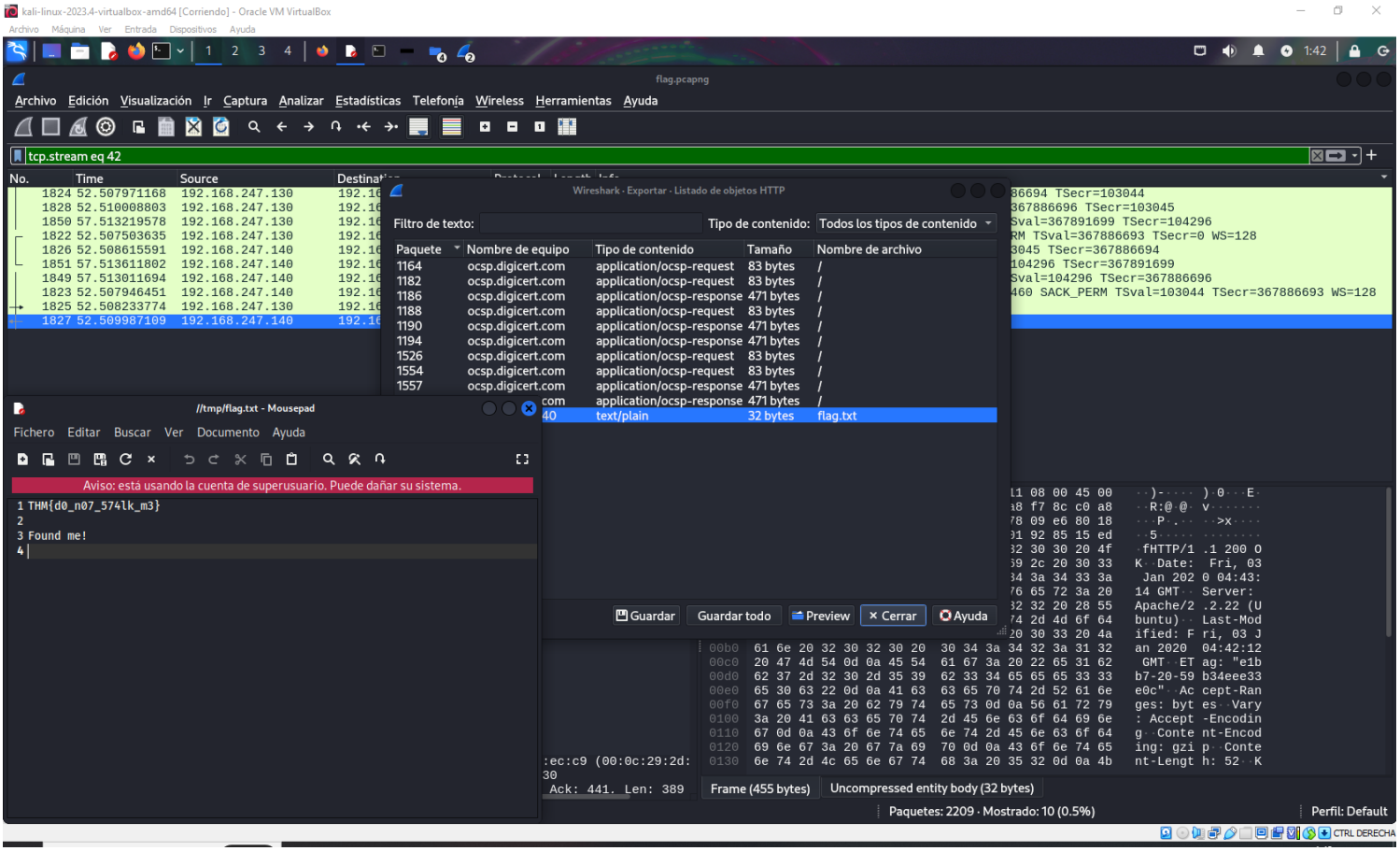
I just hacked my neighbor's WiFi and try to capture some packet. He must be up to no good. Help me find it.

es un archivo PCAP lo abrimos con wireshark





vimos que era un txt obtenido por http , por lo cual lo exportamos y aparece la flag.



Flag= THM{d0_n07_574lk_m3}