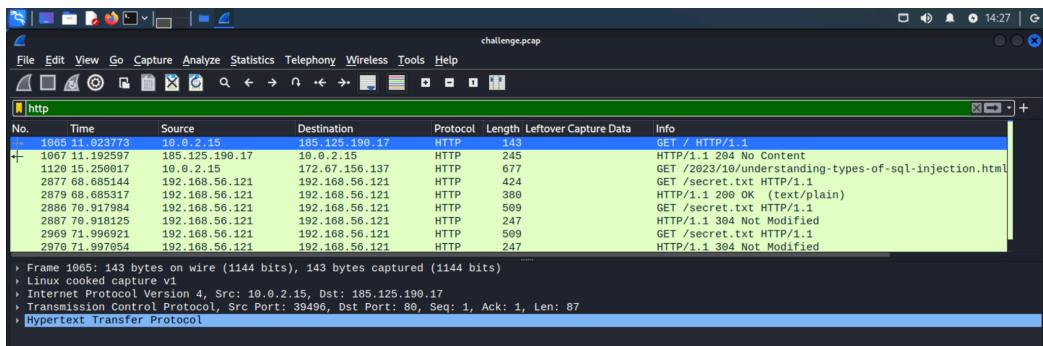
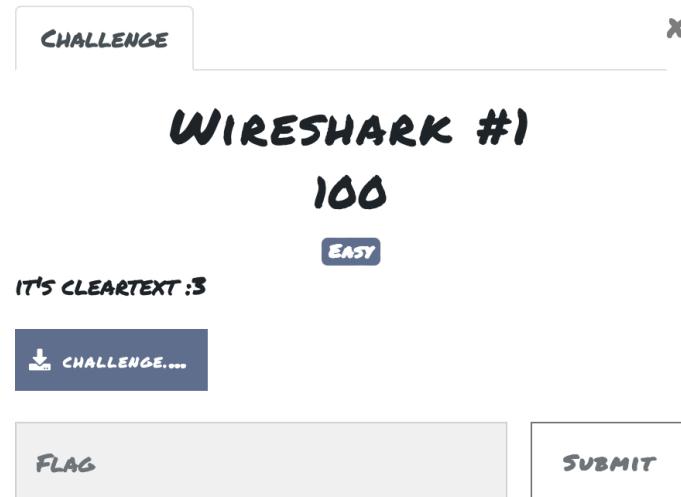
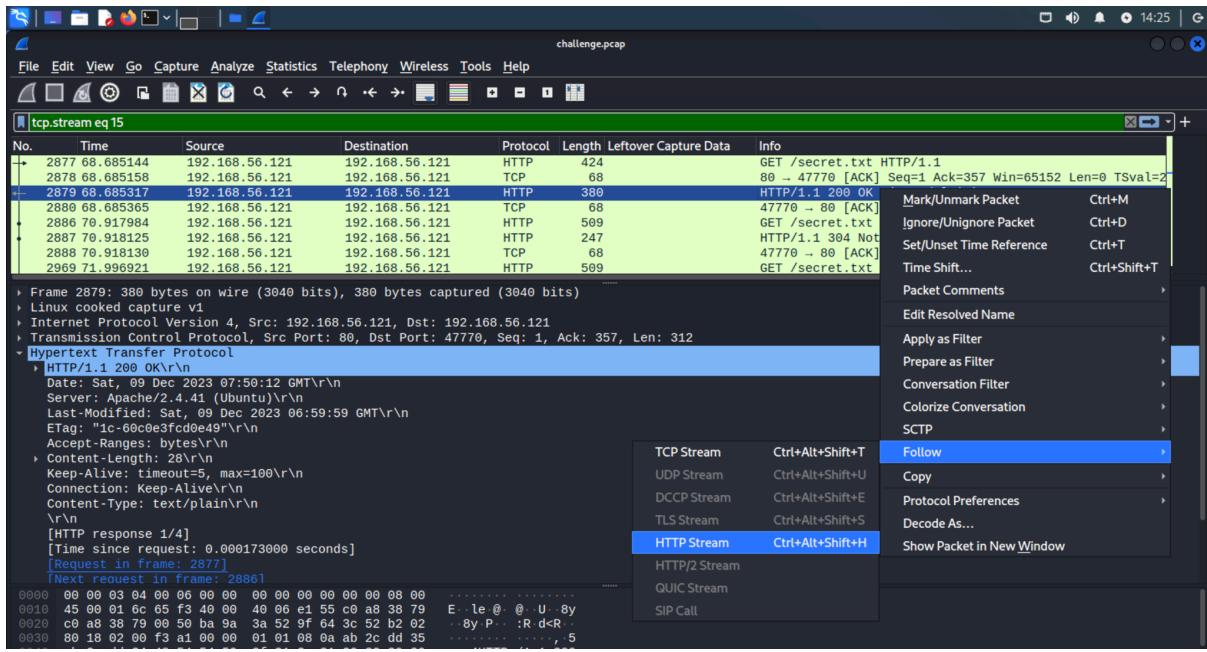


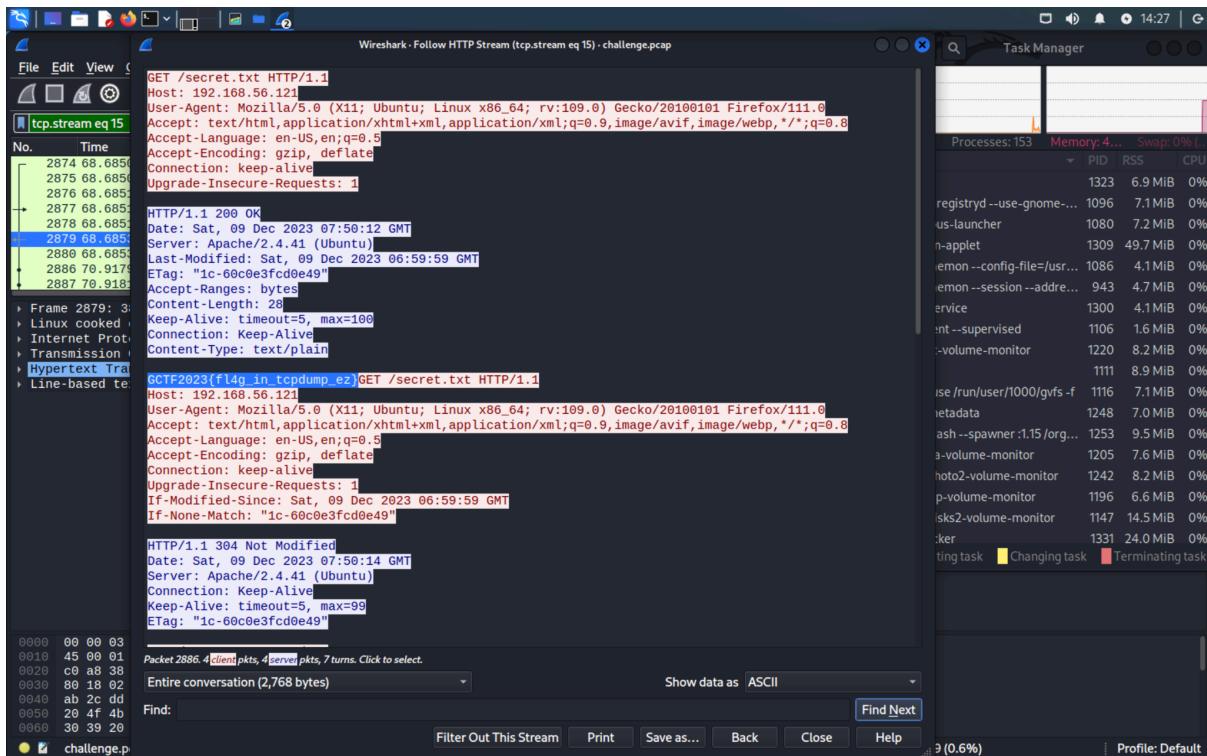
WIRESHARK #1



So firstly, I opened the file and applied a filter for http in the wireshark. Just like the hint given, it is clear text, and there is a suspicious plain txt file named “**secret.txt**” in the info.



Then I just right click on the pcap, and follow the **HTTP Stream**.



As shown above, I have highlighted the flag in the **HTTP Stream**.

Flag: GCTF2023{fl4g_in_tcpdump_ez}

I LOVE PNG!

CHALLENGE

X

I LOVE PNG!

447

EASY

FLAG IS LITERALLY IN FRONT OF YOUR EYES. NOT OBVIOUS ENOUGH?

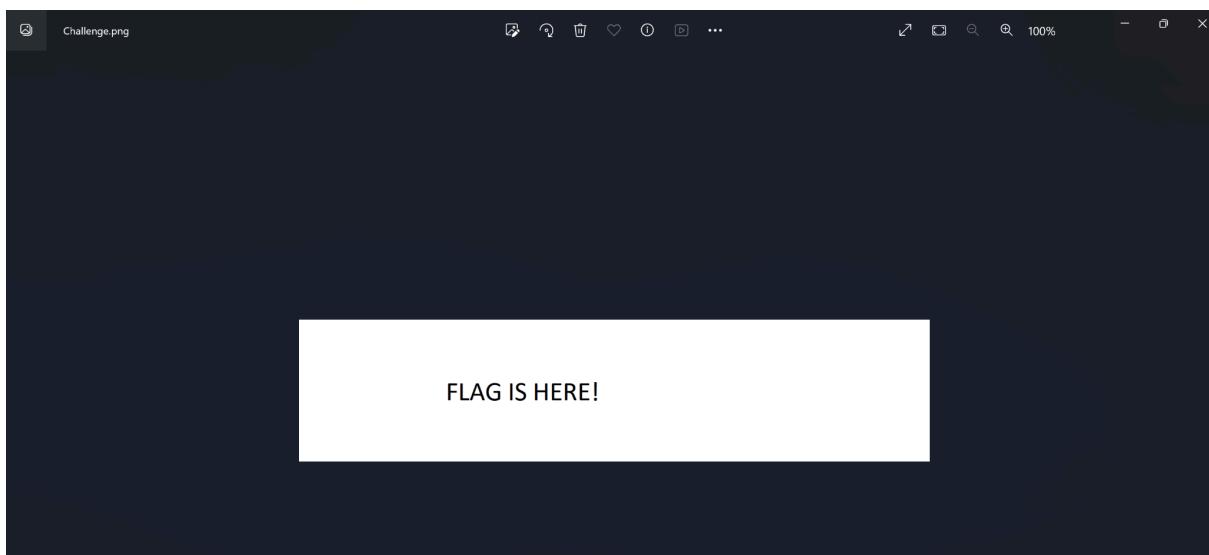
VIEW HINT

CHALLENGE....

FLAG

SUBMIT

Initially I couldn't open the file in mac os or kali linux, but then I tried to open it in windows vm and it works fine there.

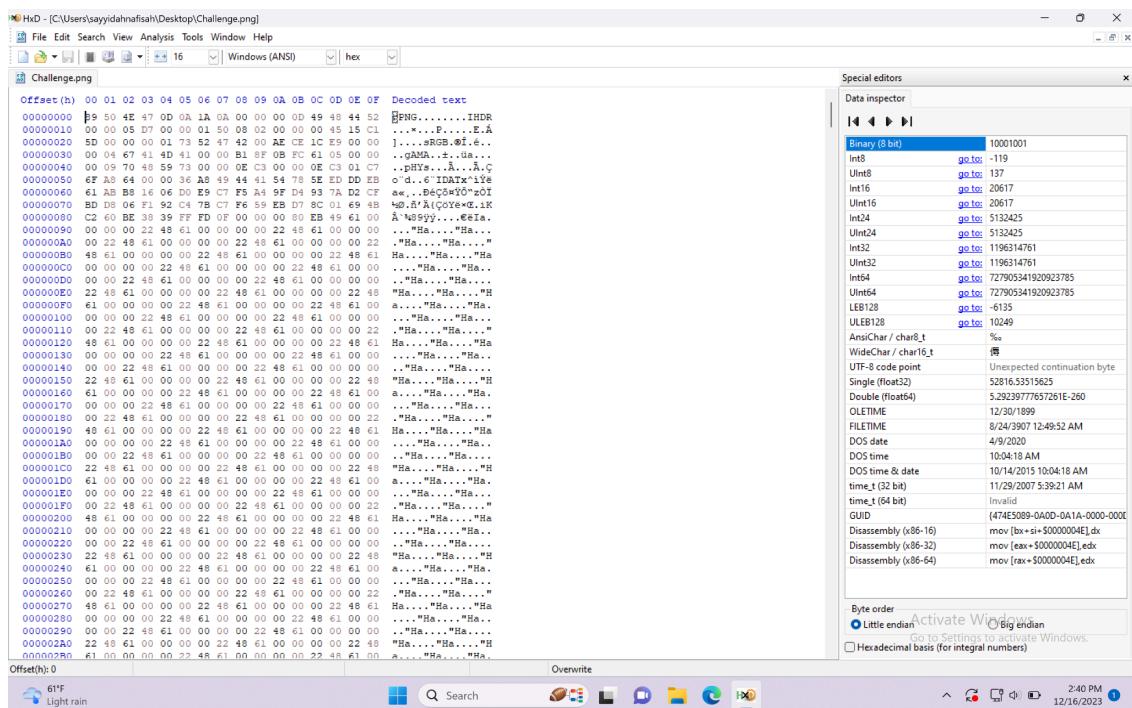


So this is how the image originally looks like. However, this was the only thing on the image and there was no flag. The image also looks like it has been cropped.

```

File Actions Edit View Help
  (parallels@kali-linux-2022-2) [~/Desktop/GCTF2023]
$ exiftool Challenge.png
ExifTool Version Number : 12.67
File Name : Challenge.png
Directory :
File Size : 14 kB
File Modification Date/Time : 2023:12:15 22:02:31+09:00
File Access Date/Time : 2023:12:16 14:37:51+09:00
File Inode Change Date/Time : 2023:12:16 14:35:02+09:00
File Permissions : -rw-r--r--
File Type : PNG
File Type Extension : image/png
MIME Type : image/png
Image Width : 1495
Image Height : 336
Bit Depth : 8
Color Type : RGB
Compression : Deflate/Inflate
Filter :
Interlace : Adaptive
SRGB Rendering : Noninterlaced
Gamma : Perceptual
Pixels Per Unit X : 2.2
Pixels Per Unit Y : 3779
Pixel Units : meters
Image Size : 1495x336
Megapixels : 0.502
  
```

Then I use **exiftool** to see the image info. As we can see here, the height is 336. This info will be used later to edit the image's height.



Then, I opened the file using **HxD**, a hex editor program to edit the hex value of the image. So the numbers here are in hex values.

```
Last login: Sat Dec 16 12:37:23 on ttys000
(base) sayyidahnaifah@Sayyidahs-MacBook-Air ~ % python
Python 3.10.9 (main, Mar 1 2023, 12:33:47) [Clang 14.0.6 ] on darwin
Type "help", "copyright", "credits" or "license" for more information.
[>>> hex(336)
'0x150'
[>>> hex(1000)
'0x3e8'
>>>
```

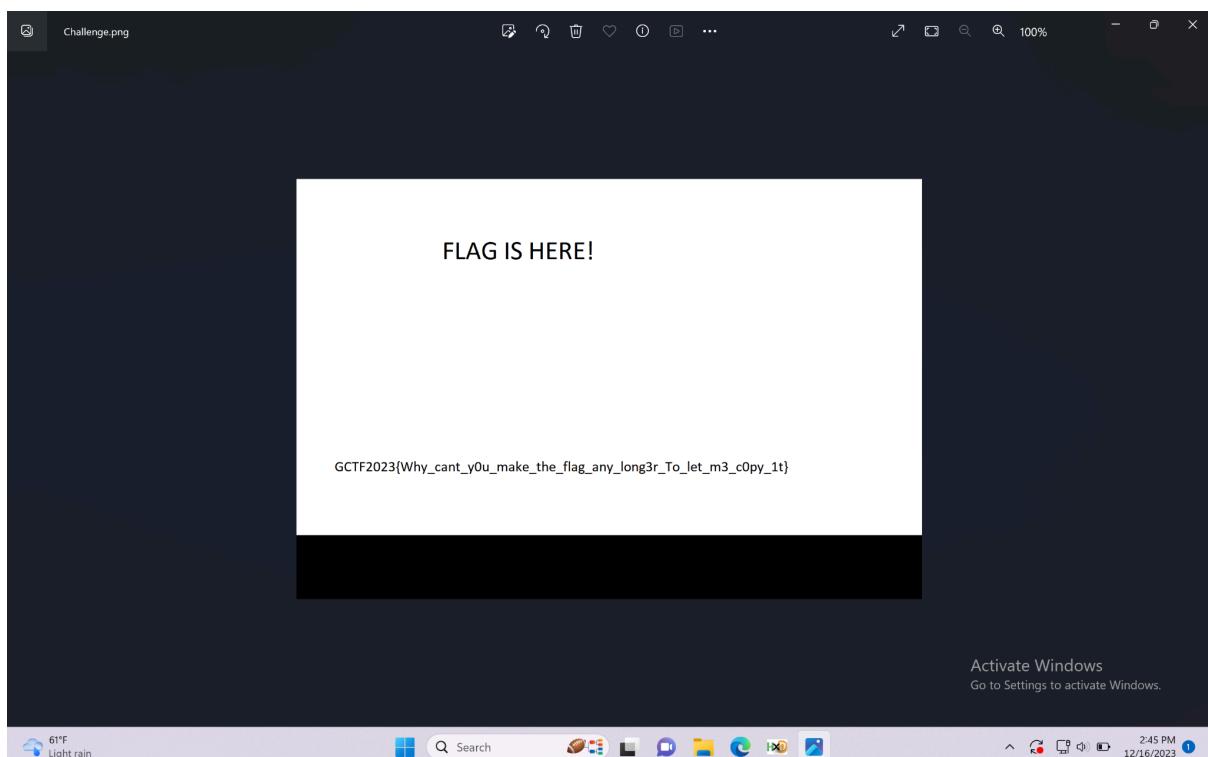
Then, I used python to convert the height that I retrieved from the information earlier into a hex value and the hex value for 336 is **0x150**.

I also converted 1000 to hex value because I'm going to change the image height from 336 to 1000. The new height will be **0x3E8**

Offset(h)	00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F	Decoded text
00000000	89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52	%PNG.....IHDR
00000010	00 00 05 D7 00 00 01 50 08 02 00 00 00 45 15 C1	...x...E.....E.Á
00000020	5D 00 00 00 01 73 52 47 42 00 AE CE 1C E9 00 00]....sRGB.ØÍ.é..
00000030	00 04 67 41 4D 41 00 00 B1 8F 0B FC 61 05 00 00	..gAMA..±..üa...
00000040	00 09 70 48 59 73 00 00 0E C3 00 00 0E C3 01 C7	..pHs...Ã...Ã.Ç
00000050	6F A8 64 00 00 36 A8 49 44 41 54 78 5E ED DD EB	o'd..6"IDATx^iÝé
00000060	61 AB B8 16 06 D0 E9 C7 F5 A4 9F D4 93 7A D2 CF	a<...Đéçô¤ÝÔ"zòÍ
00000070	BD D8 06 F1 92 C4 7B C7 F6 59 EB D7 8C 01 69 4B	¾Ø.ñ'À(QÖYé¢.iK
00000080	C2 60 BE 38 39 FF FD 0F 00 00 00 80 EB 49 61 00	Â~%89yy....€éIa.
00000090	00 00 00 22 48 61 00 00 00 22 48 61 00 00 00	..."Ha...."Ha...

As I have highlighted, that is the height that we are going to change. To know which value to change, I simply just look for 01 and 50 because the original height is 0x150.

The red hex values are the new height of the image. 03 E8 is the hex value for 1000 which is 0x3E8.



After I edited and saved the new hex value, I reopened the png file and there's the flag!

Flag: GCTF{Why cant y0u make the flag any long3r To let m3 c0py 1t}

BROKEN

CHALLENGE

X

BROKEN

100

EASY

I GOT THIS PDF AND IT'S VERY IMPORTANT TO ME. WHY
CAN'T IT OPEN OMG!

CHALLENGE....

FLAG

SUBMIT



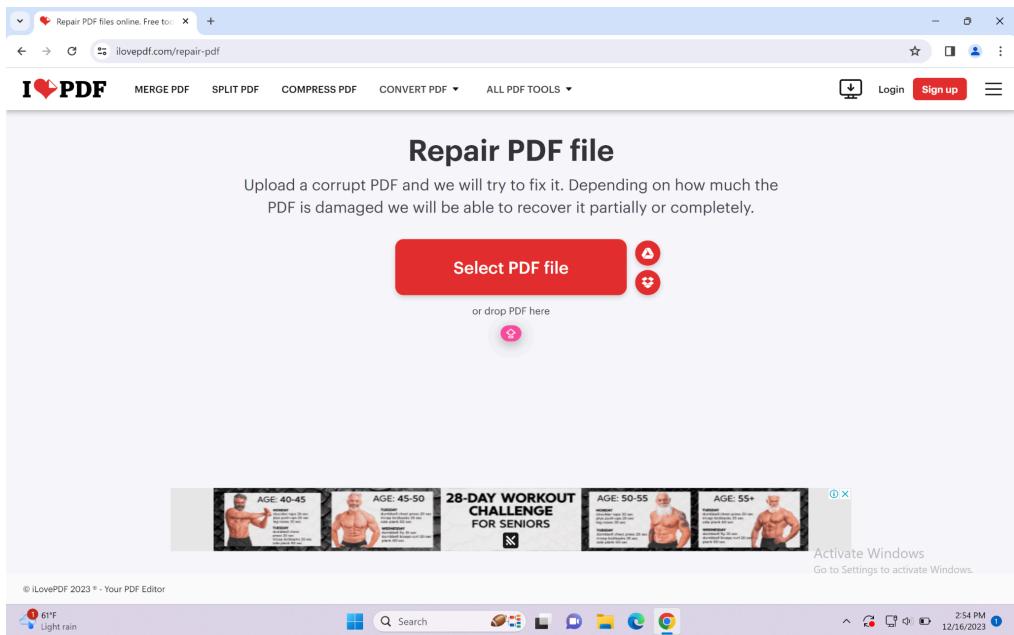
The file “Challenge.pdf” could
not be opened.

It may be damaged or use a file format
that Preview doesn’t recognise.

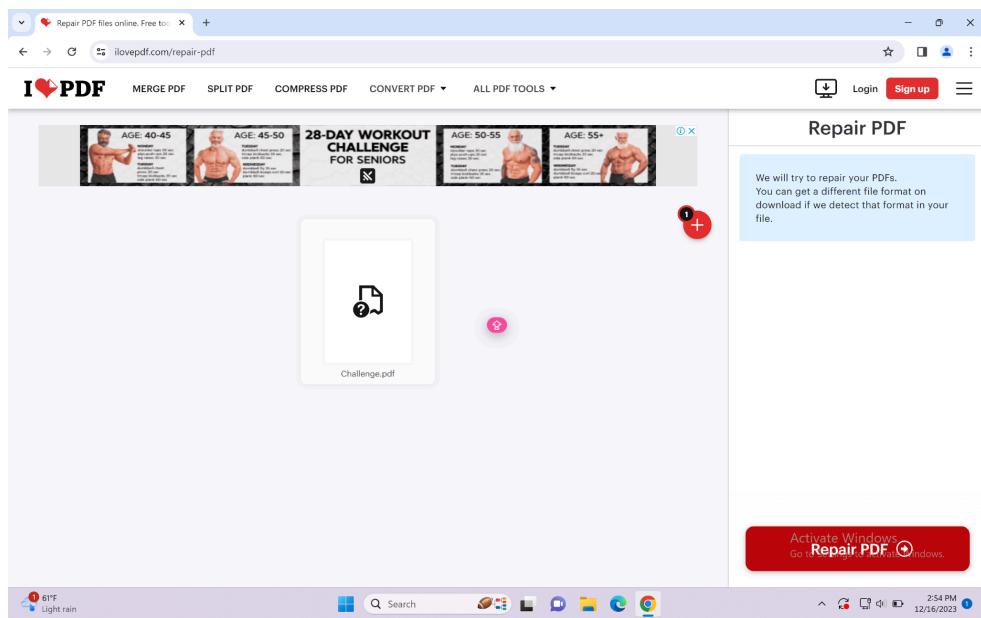
OK

So we were given a broken pdf file. Then I googled and found a website to repair pdf files. The website link is as below:

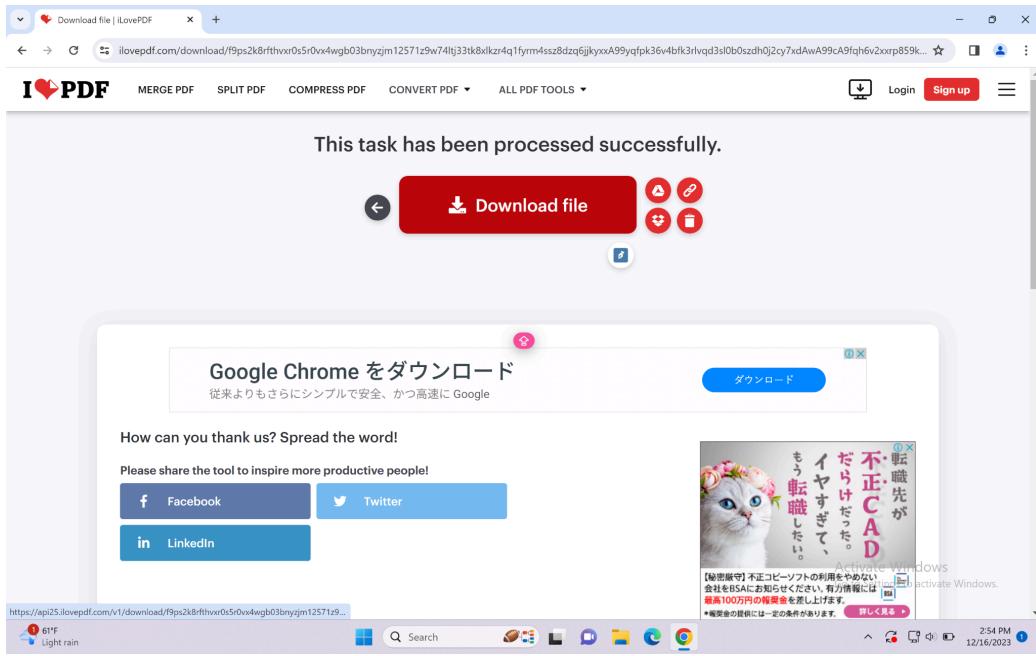
<https://www.ilovepdf.com/repair-pdf>



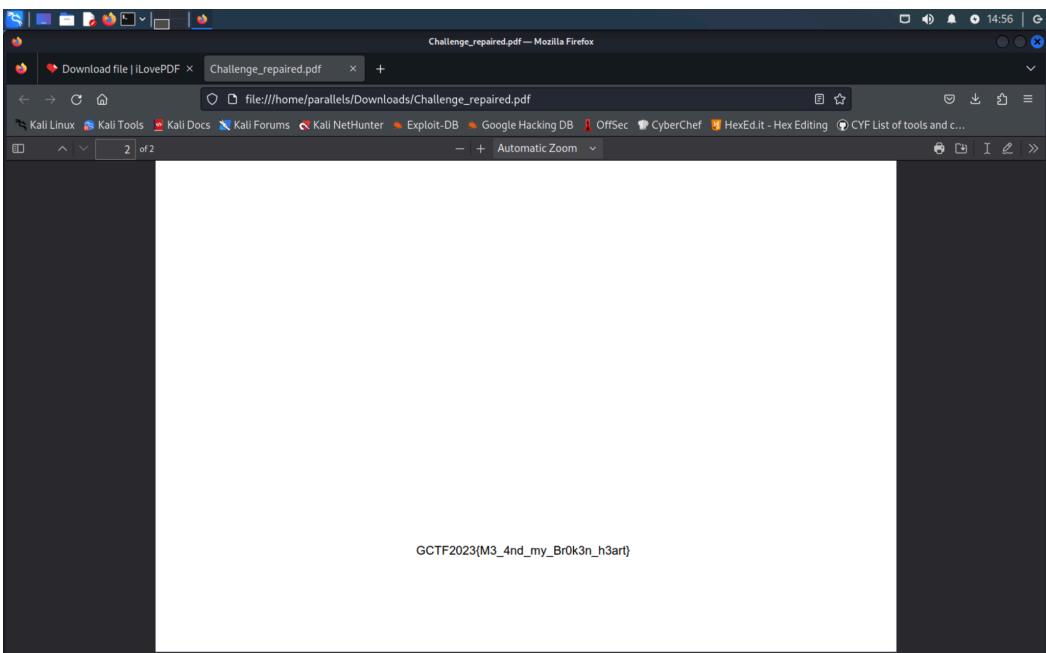
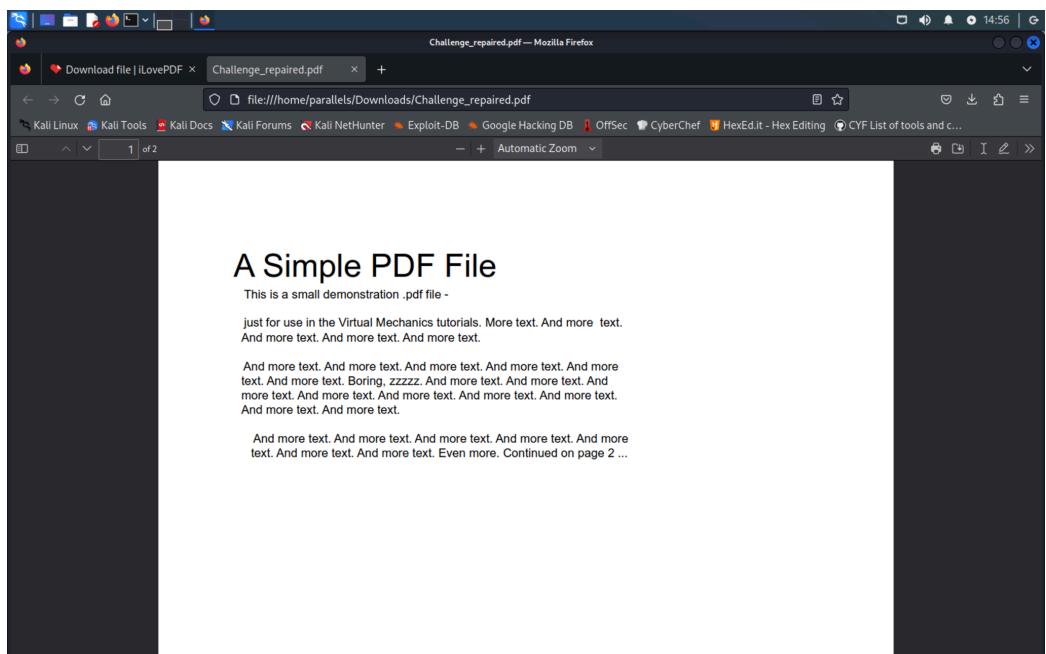
I clicked “select pdf file” to upload a broken pdf file.



I uploaded Challenge.pdf



After that, I downloaded the repaired file and found the pdf files as below.



Found the flag!

Flag: GCTF2023{M3_4nd_my_Br0k3n_h3art}

KB

CHALLENGE

X

**KB
400**

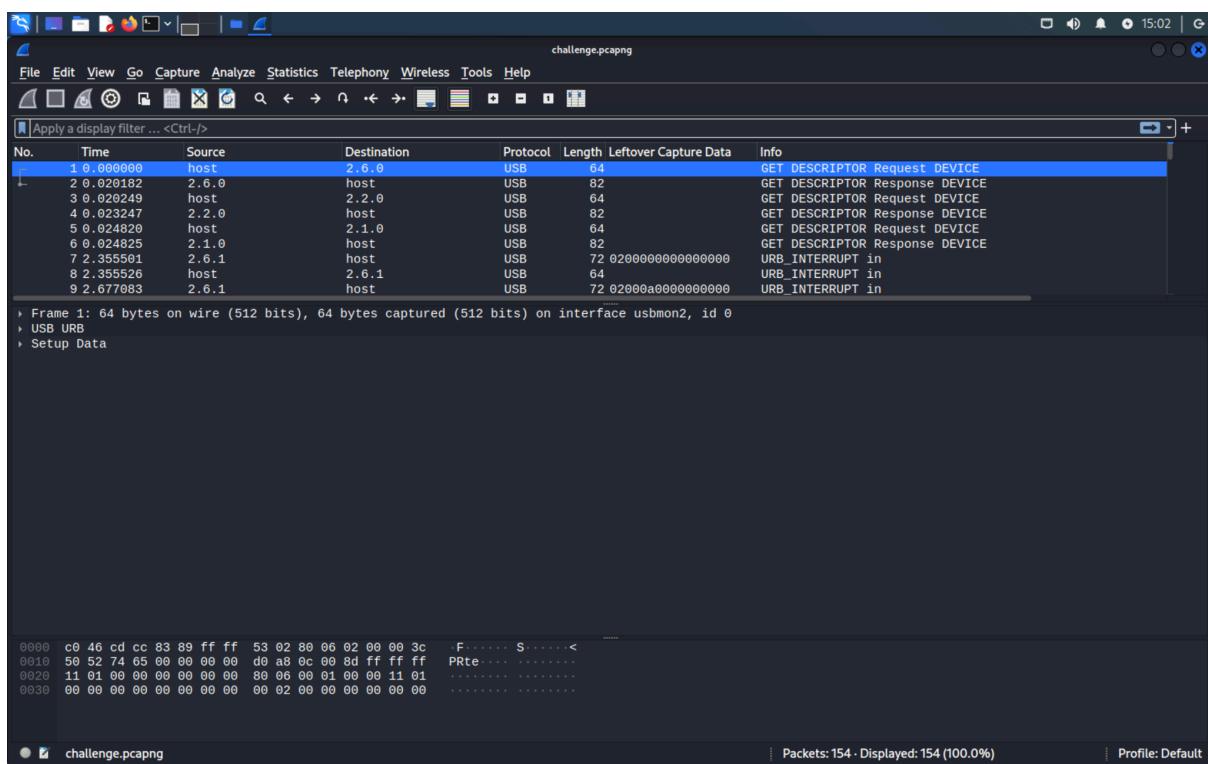
HARD

HMM, HAVEN'T SEEN THIS TYPE OF WIRESHARK FILE IN A
WHILE NOW.

CHALLENGE....

FLAG

SUBMIT



For this challenge, I opened the file using wireshark, and this is what it shows.

Google search results for "pcapng usb interrupt in":

- Medium · AllBawazeer**: [kaizen-ctf 2018 — Reverse Engineer usb keystrok from pcap file](#)
this CTF challenge contain pcapng file and no hint provided only flag needed to earn the points ... `... usbnutshell/usb4.shtml#lInterrupt which came ...`
- stayontarget.org**: [Decoding Mixed Case USB Keystrokes from PCAP](#)
Mar 26, 2019 — During a recent assessment, I captured USB keystrokes as a part of a larger set of data from a system. ... `#print(ucasekey[int(bytesArray[2])]) #...`
- CTFTime.org / VishwaCTF 2023 / 1nj3ct0r / Writeup**: [pcapng](#). image. It is a capture of USB protocol. Generally in a usb dump we find keyboard interrupts or mouse clicks as user input data, so I started ...
- GitHub**: [Techniques for analyzing USB protocols](#)
Most of the protocol we need to implement lies in these two Wireshark fields. In Interrupt or bulk transfers all data is this `cdapdata`, the rest is just `USB` ...
- GitHub**: [JohnDMcMaster / usbrply](#)
`libPMA/Misc/usb/usb_Pdu.h`

Then, I just googled some keywords and I found this website (link below) and I referred to it for this challenge.

<https://abawazeeer.medium.com/kaizen-ctf-2018-reverse-engineer-usb-keystrok-from-pcap-file-2412351679f4>

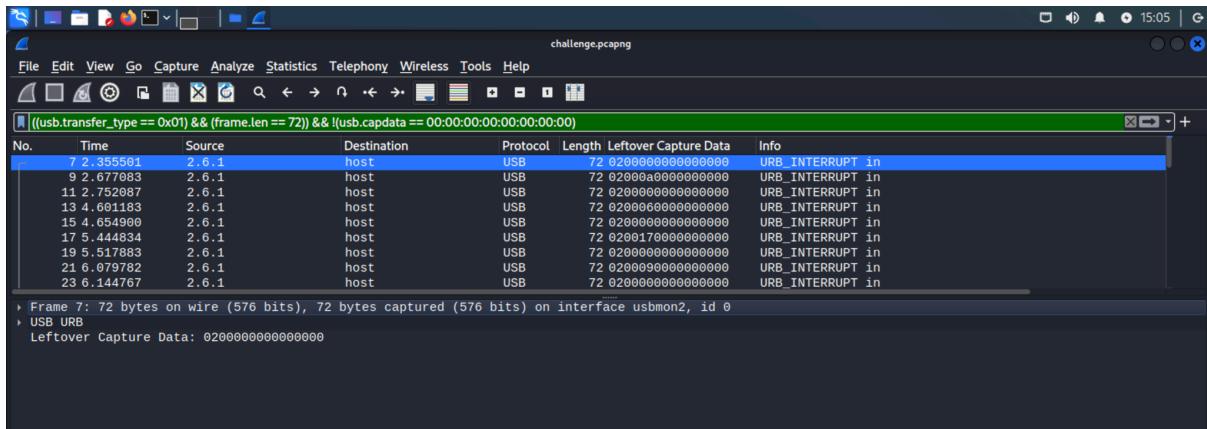
No.	Time	Source	Destination	Protocol	Length	Leftover Capture Data	Info
1	0.000000	host	2.6.0	USB	64		GET_DESCRIPTOR Request DEVICE
2	0.020182	2.6.0	host	USB	82		GET_DESCRIPTOR Response DEVICE
3	0.020249	host	2.2.0	USB	64		GET_DESCRIPTOR Request DEVICE
4	0.023247	2.2.0	host	USB	82		GET_DESCRIPTOR Response DEVICE
5	0.024820	host	2.1.0	USB	64		GET_DESCRIPTOR Request DEVICE
6	0.024825	2.1.0	host	USB	82		GET_DESCRIPTOR Response DEVICE
7	2.355501	2.6.1	host	USB	72	0200000000000000	URB_INTERRUPT in
8	2.355526	host	2.6.1	USB	64		URB_INTERRUPT in
9	2.677083	2.6.1	host	USB	72	02000a0000000000	URB_INTERRUPT in
10	2.677102	host	2.6.1	USB	64		URB_INTERRUPT in
11	2.752087	2.6.1	host	USB	72	0200000000000000	URB_INTERRUPT in
12	2.752113	host	2.6.1	USB	64		URB_INTERRUPT in
13	4.601183	2.6.1	host	USB	72	0200060000000000	URB_INTERRUPT in
14	4.601206	host	2.6.1	USB	64		URB_INTERRUPT in
15	4.654900	2.6.1	host	USB	72	0200000000000000	URB_INTERRUPT in
16	4.654920	host	2.6.1	USB	64		URB_INTERRUPT in
17	5.444834	2.6.1	host	USB	72	0200170000000000	URB_INTERRUPT in
18	5.444860	host	2.6.1	USB	64		URB_INTERRUPT in
19	5.517883	2.6.1	host	USB	72	0200000000000000	URB_INTERRUPT in
20	5.517906	host	2.6.1	USB	64		URB_INTERRUPT in
21	6.070782	2.6.1	host	USB	72	0200000000000000	URB_INTERRUPT in

```

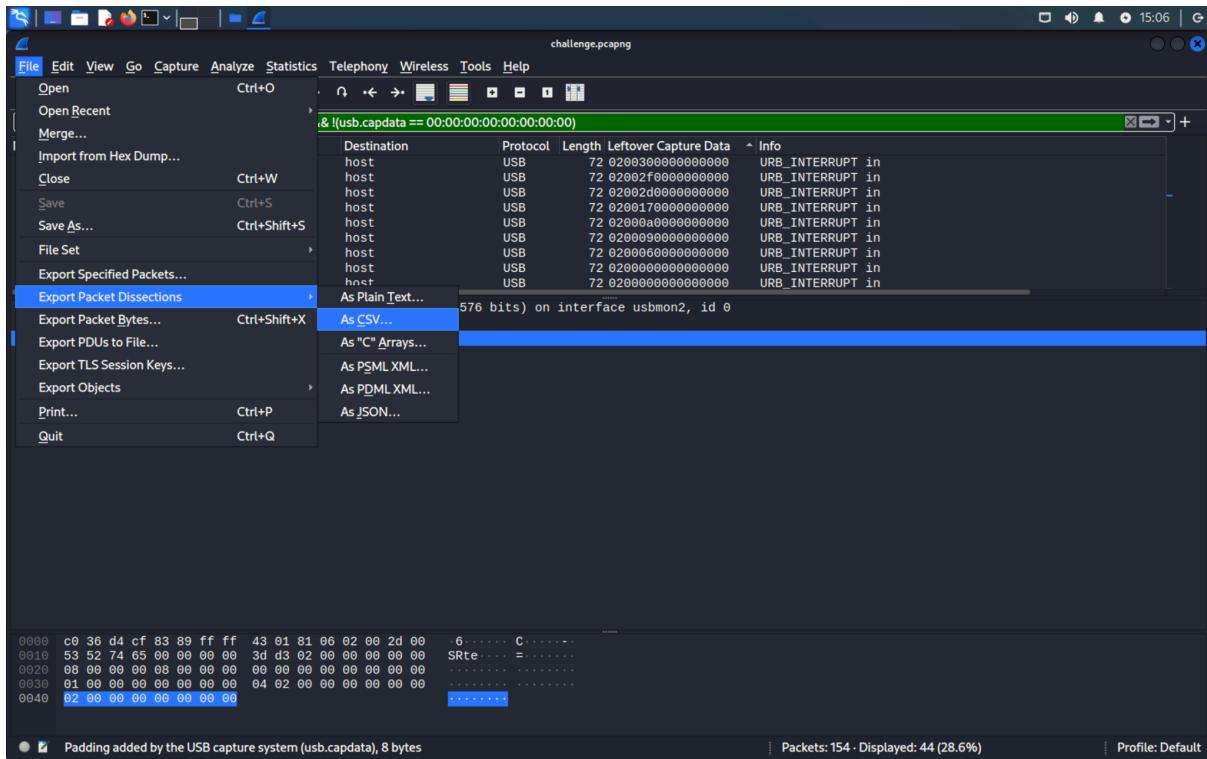
Frame 13: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface usbmon2, id 0
  USB URB
    [Source: 2.6.1]
    [Destination: host]
    URB id: 0xffff8983cf436c0
    URB type: URB_COMPLETE ('C')
    URB transfer type: URB_INTERRUPT (0x01)
    > Endpoint: 0x81, Direction: IN
    Device: 6
    0000 c0 36 d4 cf 83 b9 ff ff 43 01 81 06 02 00 2d 00 ..6.....C.....
    0010 55 52 74 65 00 00 00 00 ef 92 06 00 00 00 00 00 URtE..... .
    0020 08 00 00 00 08 00 00 00 00 00 00 00 00 00 00 00 .....
    0030 01 00 00 00 00 00 00 00 04 02 00 00 00 00 00 00 ..... .
    0040 02 00 00 00 00 00 00 00 .. .....

```

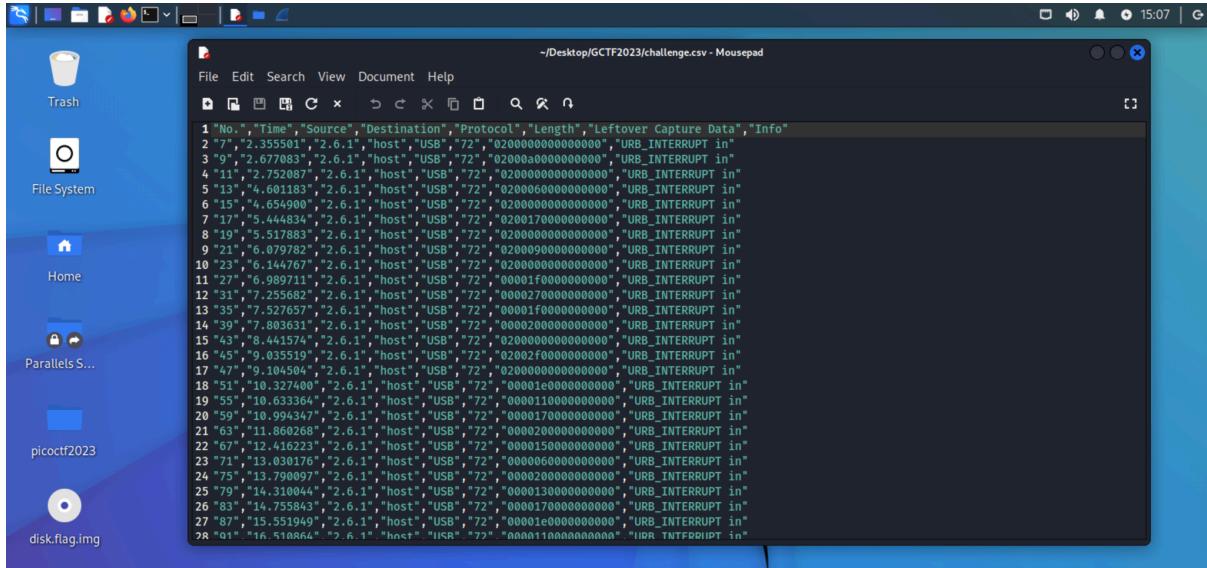
So, as we can see, there is some pattern in Leftover Capture Data, where a certain number changed on that position only, and it occurs on USB transfer type URB_INTERRUPT with frame length 72 only.



So, we filtered the data using this logic where usb transfer type is 0x01, and frame length 72:
`((usb.transfer_type == 0x01) && (frame.len == 72)) && !(usb.capdata == 00:00:00:00:00:00:00:00:00:00)`



Then, I exported the filtered data into a csv file and included the Leftover Capture Data into the column because that is the data that we need.



This is how the data looks like in the csv file.

```
(parallels@kali-linux-2022-2) [~/Desktop/GCTF2023]
$ cat challenge.csv | cut -d ',' -f 7 | cut -d ''"' -f 2 | grep -vE 'Leftover Capture Data' > hexoutput.txt

[parallels@kali-linux-2022-2) [~/Desktop/GCTF2023]
$ cat hexoutput.txt
0200000000000000
02000a0000000000
0200000000000000
0200060000000000
0200000000000000
0200170000000000
0200000000000000
0200090000000000
0200000000000000
00001f0000000000
0000270000000000
00001f0000000000
0000200000000000
0200000000000000
020002f0000000000
0200000000000000
00001e0000000000
0000110000000000
0000170000000000
0000200000000000
0000150000000000
0000060000000000
0000200000000000
0000130000000000
0000170000000000
00001e0000000000
0000110000000000
00000a0000000000
0200000000000000
020002d0000000000
0200000000000000
0000e00000000000
0000080000000000
00001c0000000000
0000150000000000
0000170000000000
0000150000000000
```

To save the Leftover Capture Data only, into an another txt file (hexoutput.txt) automatically, I use this command:

```
cat challenge.csv | cut -d ',' -f 7 | cut -d ""' -f 2 | grep -vE "Leftover Capture Data" > hexoutput.txt
```

Then, I read the `hexoutput.txt` file by using “`cat hexoutput.txt`” to make sure that everything is written there correctly.

The image shows two terminal windows side-by-side. The left window displays the Python script `keys.py`, which defines a dictionary `newmap` mapping hex values to characters. The right window displays the text file `hexoutput.txt`, which contains a list of hex values and their corresponding characters.

```
File Edit Search View Document Help ~/Desktop/GCTF2023/keys.py - Mousepad
1 newmap = {
2     0x02: "PostFail",
3     0x04: "a",
4     0x05: "b",
5     0x06: "c",
6     0x07: "d",
7     0x08: "e",
8     0x09: "f",
9     0x0A: "g",
10    0x0B: "h",
11    0x0C: "i",
12    0x0D: "j",
13    0x0E: "k",
14    0x0F: "l",
15    0x10: "m",
16    0x11: "n",
17    0x12: "o",
18    0x13: "p",
19    0x14: "q",
20    0x15: "r",
21    0x16: "s",
22    0x17: "t",
23    0x18: "u",
24    0x19: "v",
25    0x1A: "w",
26    0x1B: "x",
27    0x1C: "y",
28    0x1D: "z",
29    0x1E: "1",
30    0x1F: "2",
31    0x20: "3",
32    0x21: "4",
33    0x22: "5",
34    0x23: "6",
35    0x24: "7",
36    0x25: "8",
37    0x26: "9",
38    0x27: "0",
39    0x28: "Enter",
40    0x29: "esc",
41    0x2A: "del",
42    0x2B: "tab",
43
44
45
46
47
48
49
50
51
52
53
54
55 myKeys = open('hexoutput.txt')
56 i = 1
57
58 for line in myKeys:
59     bytesArray = bytearray.fromhex(line.strip())
60     # print("Line Number: " + str(i))
61     for byte in bytesArray:
62         if byte != 0:
63             keyVal = int(byte)
64             if keyVal in newmap:
65                 # print("Value map : " + str(keyVal) + " -> " + newmap[keyVal])
66                 print(newmap[keyVal])
67             else:
68                 print("No map found for this value: " + str(keyVal))
69             # print(format(byte, '02X'))
70             i += 1
71 }
```

```
File Edit Search View Document Help ~/Desktop/GCTF2023/keys.py - Mousepad
1 newmap = {
2     0x02: "PostFail",
3     0x04: "a",
4     0x05: "b",
5     0x06: "c",
6     0x07: "d",
7     0x08: "e",
8     0x09: "f",
9     0x0A: "g",
10    0x0B: "h",
11    0x0C: "i",
12    0x0D: "j",
13    0x0E: "k",
14    0x0F: "l",
15    0x10: "m",
16    0x11: "n",
17    0x12: "o",
18    0x13: "p",
19    0x14: "q",
20    0x15: "r",
21    0x16: "s",
22    0x17: "t",
23    0x18: "u",
24    0x19: "v",
25    0x1A: "w",
26    0x1B: "x",
27    0x1C: "y",
28    0x1D: "z",
29    0x1E: "1",
30    0x1F: "2",
31    0x20: "3",
32    0x21: "4",
33    0x22: "5",
34    0x23: "6",
35    0x24: "7",
36    0x25: "8",
37    0x26: "9",
38    0x27: "0",
39    0x28: "Enter",
40    0x29: "esc",
41    0x2A: "del",
42    0x2B: "tab",
43    0x2C: "space",
44    0x2D: " ",
45    0x2E: "[",
46    0x30: "]",
47    0x38: "/",
48    0x39: "CapsLock",
49    0x4B: "RightArrow",
50    0x4C: "LeftArrow"
51
52
53
54
55 myKeys = open('hexoutput.txt')
56 i = 1
57
58 for line in myKeys:
59     bytesArray = bytearray.fromhex(line.strip())
60     # print("Line Number: " + str(i))
61     for byte in bytesArray:
62         if byte != 0:
63             keyVal = int(byte)
64             if keyVal in newmap:
65                 # print("Value map : " + str(keyVal) + " -> " + newmap[keyVal])
66                 print(newmap[keyVal])
67             else:
68                 print("No map found for this value: " + str(keyVal))
69             # print(format(byte, '02X'))
70             i += 1
71 }
```

This is the python code that I used to convert the **hexoutput.txt** into a readable or ASCII character.

The screenshot shows a Kali Linux desktop environment. In the terminal window, the command `python keys.py` is run, displaying a long string of characters (PostFail, g, PostFail, c, PostFail, t, PostFail, f, PostFail, 1, n, t, 3, r, p, t, 1, n, g, k, PostFail, PostFail, -PostFail, k, e, y, s, t, r, 0, k, 3) which is the output of `hexoutput.txt`. The file manager shows files like `file.pcap`, `flag`, `flag.enc`, `flag-2.enc`, `FlagChecker.exe`, `hexoutput.txt`, `jail.py`, `keys.py`, `secret.zip`, `yes.txt`, and `yes.zip`. The task manager lists various system processes.

This is the output from **hexoutput.txt** after I run the python code.

After I type all the characters manually, I got the flag:

GCTF2023{1nt3c3pt1ng_keystr0k3}

WIRESHARK #2

CHALLENGE

X

WIRESHARK #2

387

MEDIUM

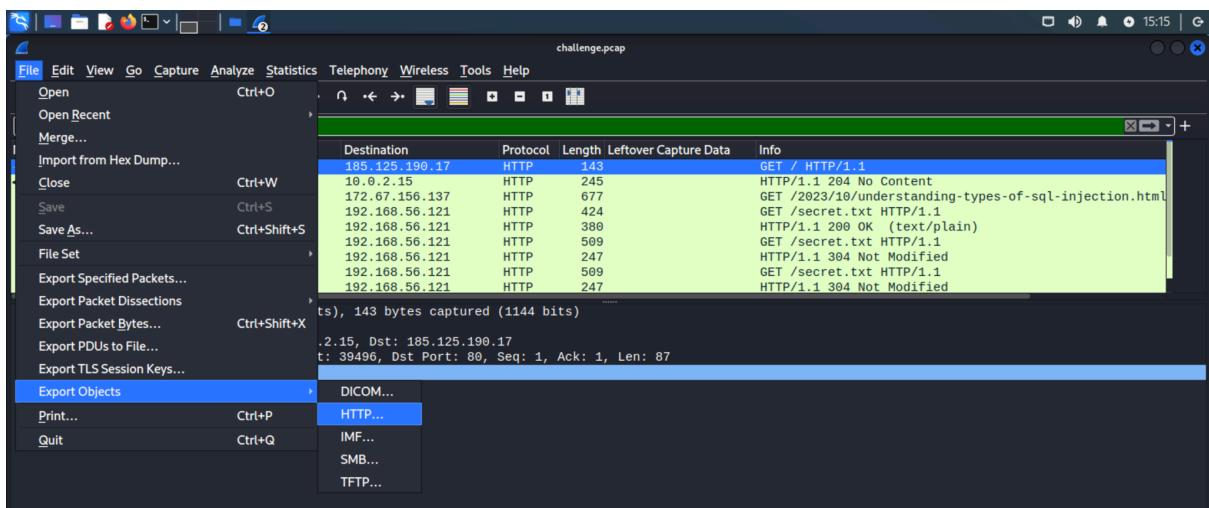
I REMEMBER THERE IS A COMPRESSED FILE. PLEASE FIND IT
AND EXPOSE THE SECRET!

SAME CHALLENGE FILE AS WIRESHARK #1

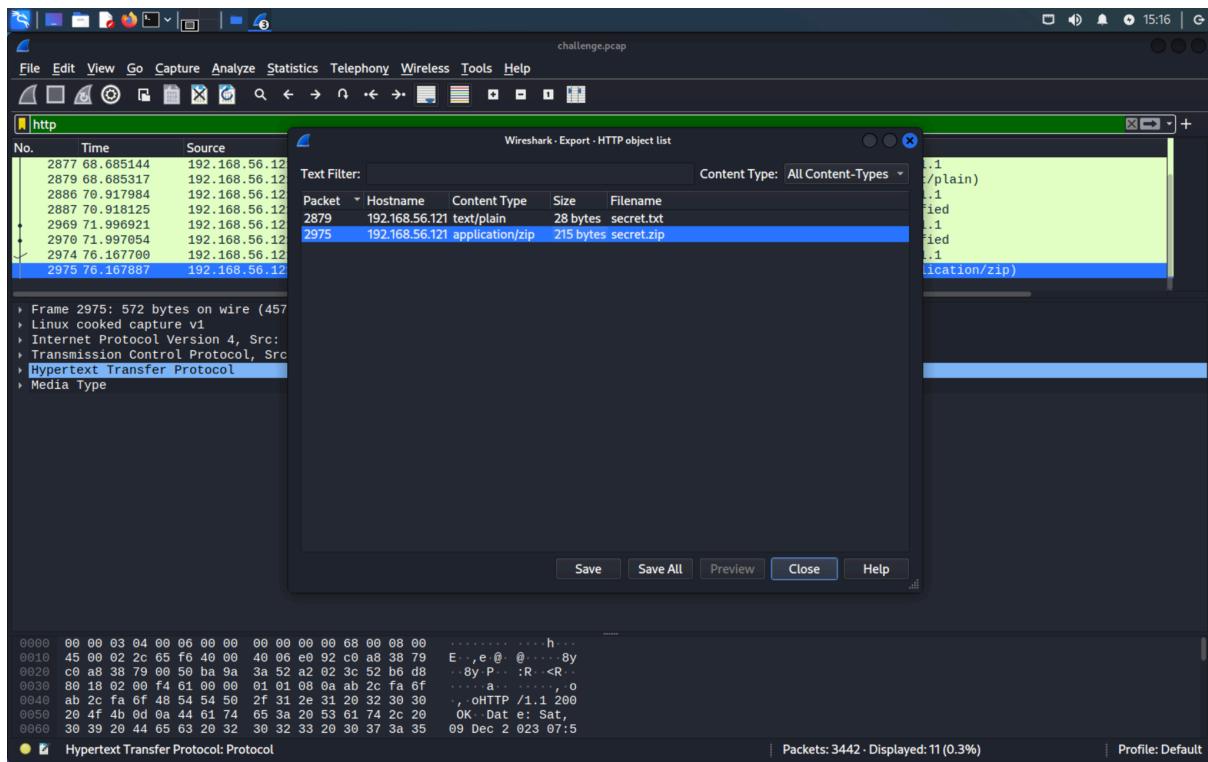
VIEW HINT

FLAG

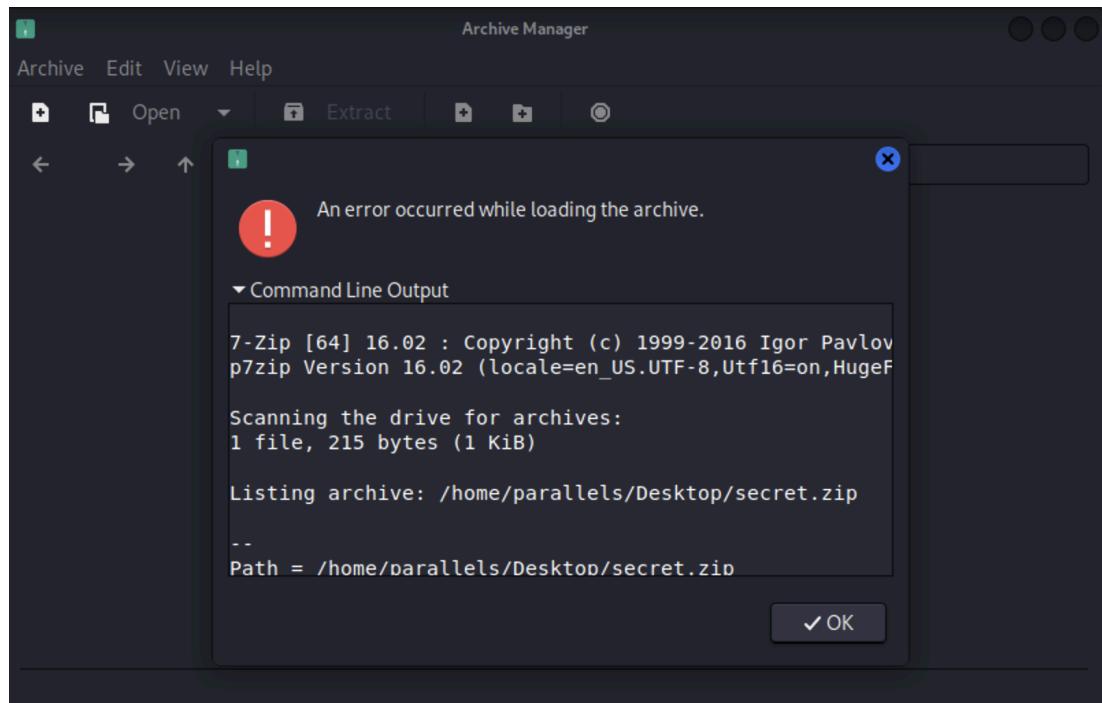
SUBMIT



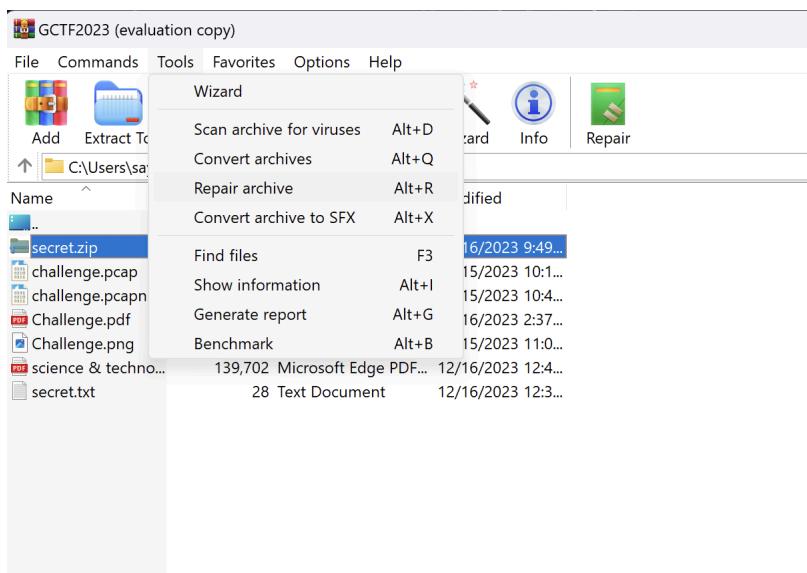
As this is a continuation from challenge [Wireshark #1](#), I am using the same pcap file, then I clicked export objects and clicked http to export the [secret.zip](#) file.



As shown above, I exported the file.



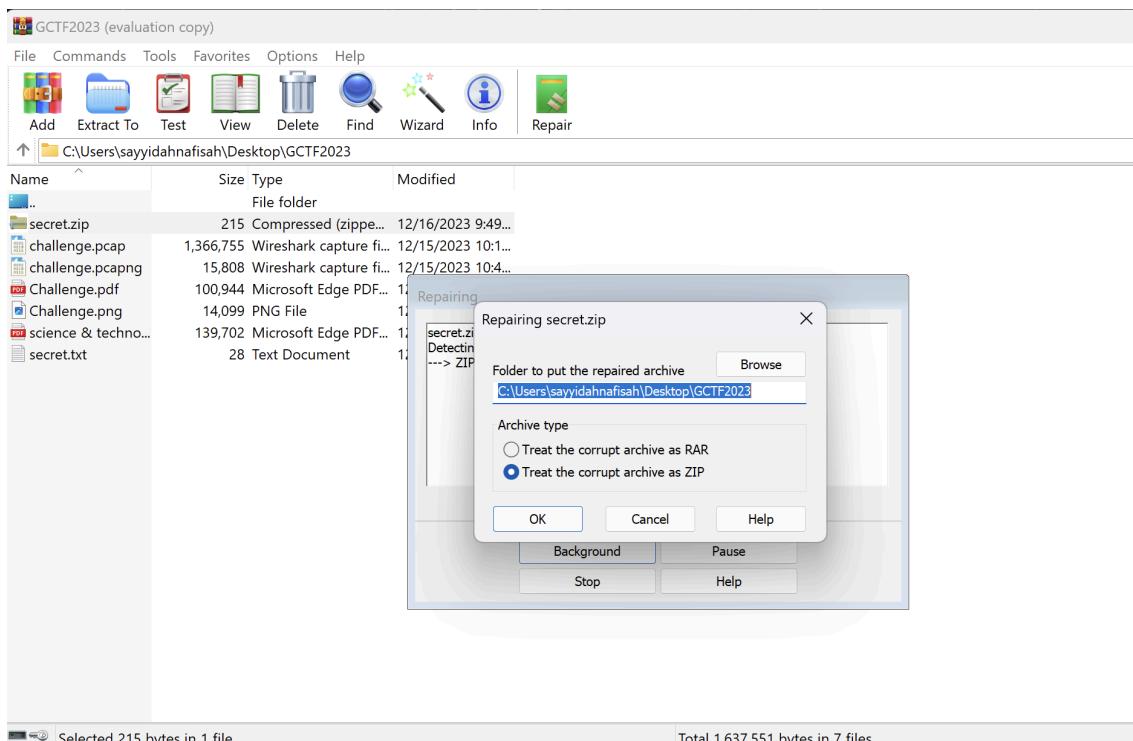
However, the zip file is corrupted and I couldn't open the file.



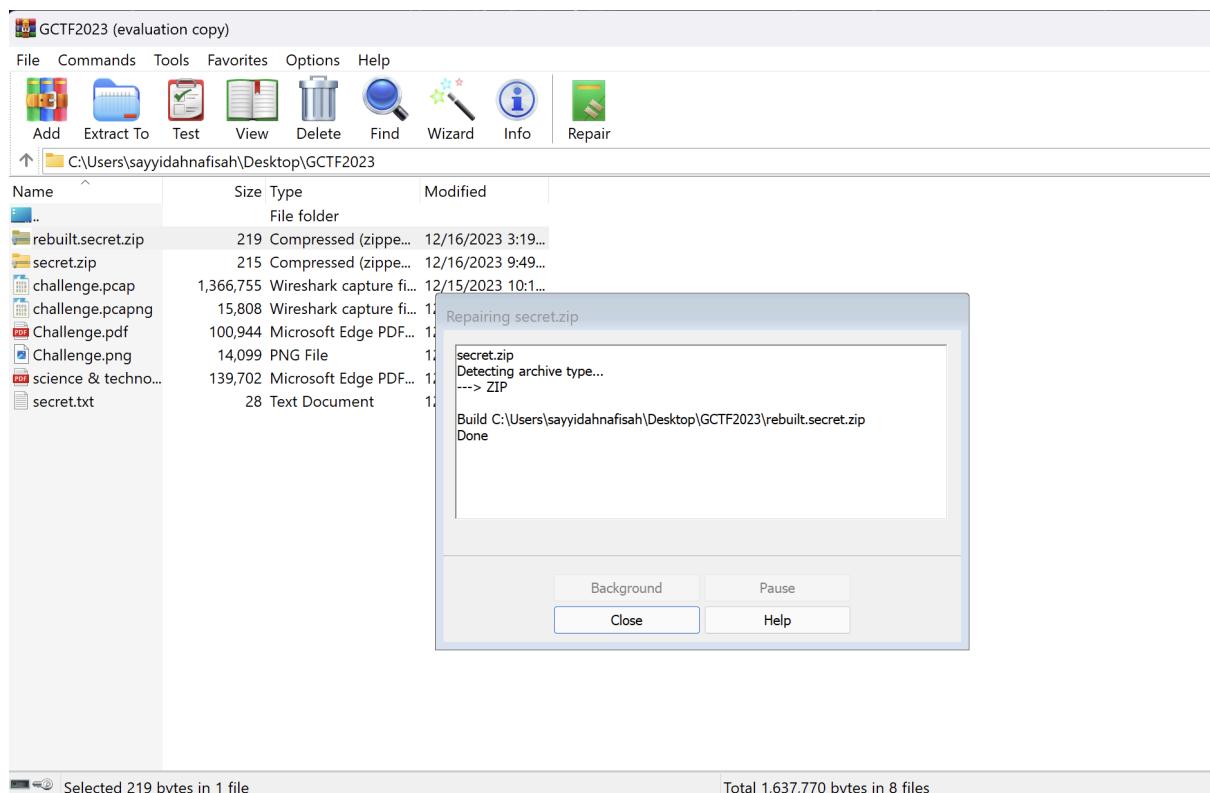
Then I used Win-rar apps to fix the zip file.

The steps to fix the file:

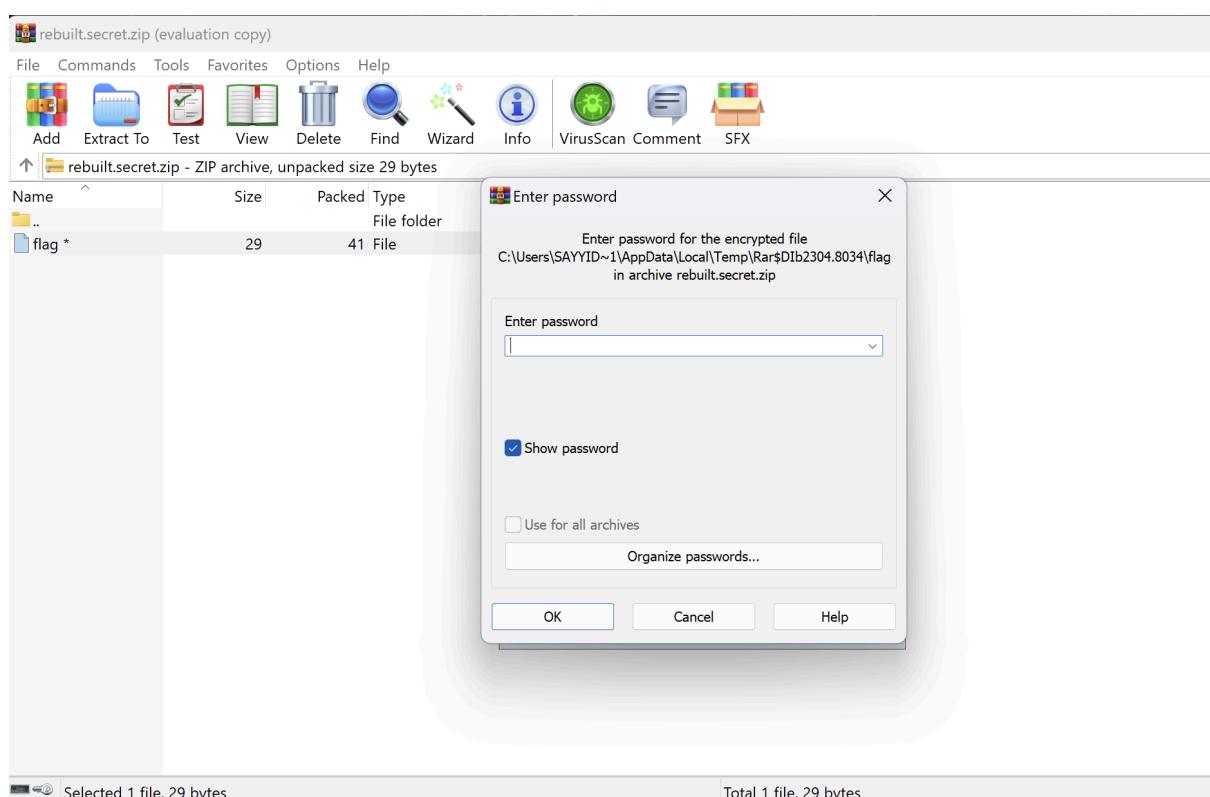
1. select **secret.zip** file
2. click Repair archive



3. Click OK



4. Click close



5. The file is successfully repaired but we are still not done yet because the file is protected by password.

The screenshot shows a terminal window titled "parallels@kali-linux-2022-2: ~/Desktop". The terminal history is as follows:

```
(parallels@kali-linux-2022-2) [~/Desktop]
$ zip2john rebuilt.secret.zip > secret.txt
ver 1.0 efh 5455 efh 7875 rebuilt.secret.zip/flag PKZIP Encr: 2b chk, TS_chk, cmplen=41, decmplen=29, crc=7E896D4A ts=01C5 cs=01c5
type=0

(parallels@kali-linux-2022-2) [~/Desktop]
$ john secret.txt
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
No password hashes left to crack (see FAQ)

(parallels@kali-linux-2022-2) [~/Desktop]
$ john secret.txt -show
rebuilt.secret.zip/flag:batman:flag:rebuilt.secret.zip::rebuilt.secret.zip

1 password hash cracked, 0 left

(parallels@kali-linux-2022-2) [~/Desktop]
$
```

To crack the password, I referred to this video:

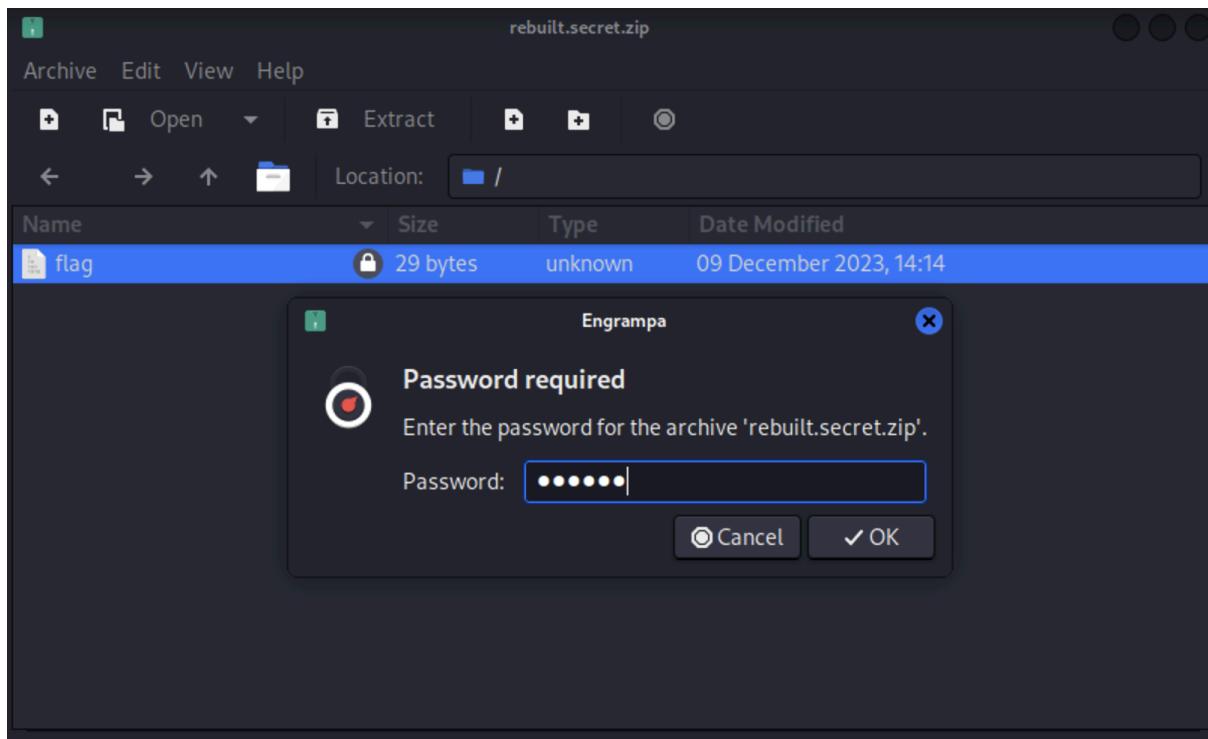
<https://www.youtube.com/watch?v=yyIoX0QT6QM>

I cracked it using **John the ripper**.

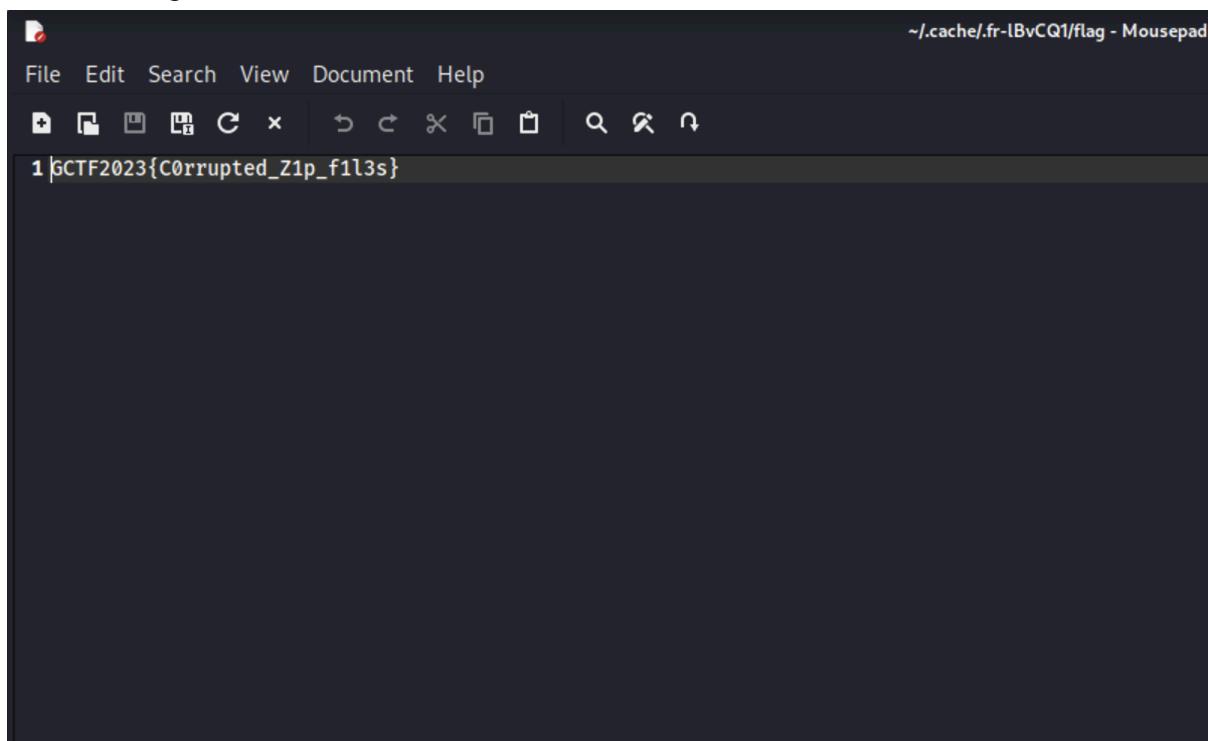
The linux command is as follows:

```
zip2john rebuild.secret.zip > secret.txt
john secret.txt
john secret.txt -show
```

Then, as shown in the picture, the password for the file is **batman**.



I entered the password “**batman**”

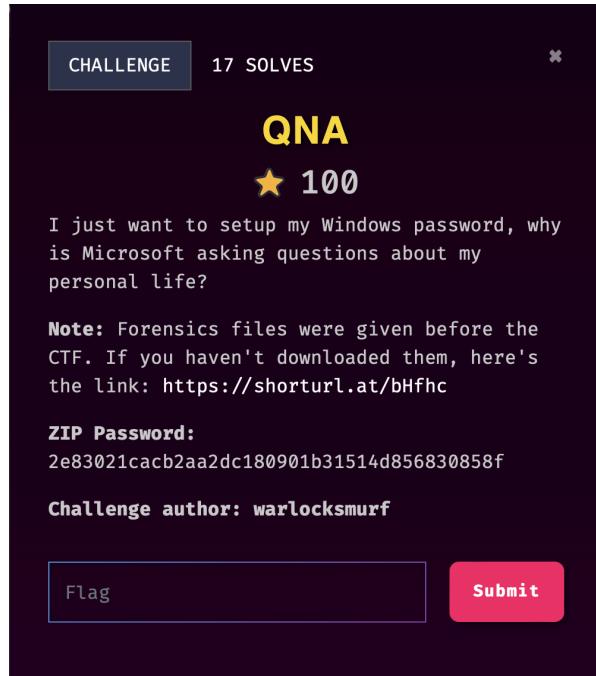


I successfully unlocked the file and found the flag!

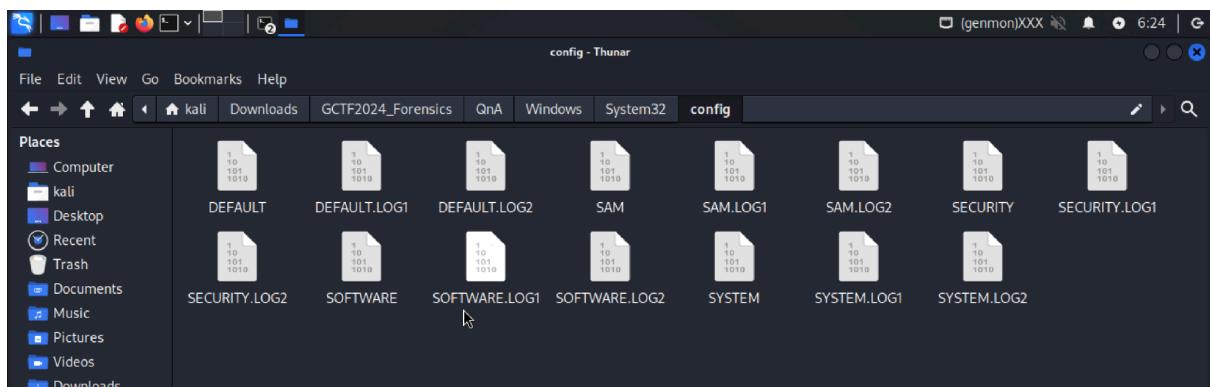
Flag: GCTF2023{C0rrupted_Z1p_f1l3s}

FORENSIC

OnA



In this directory, I just look for the User's name which is SAM.

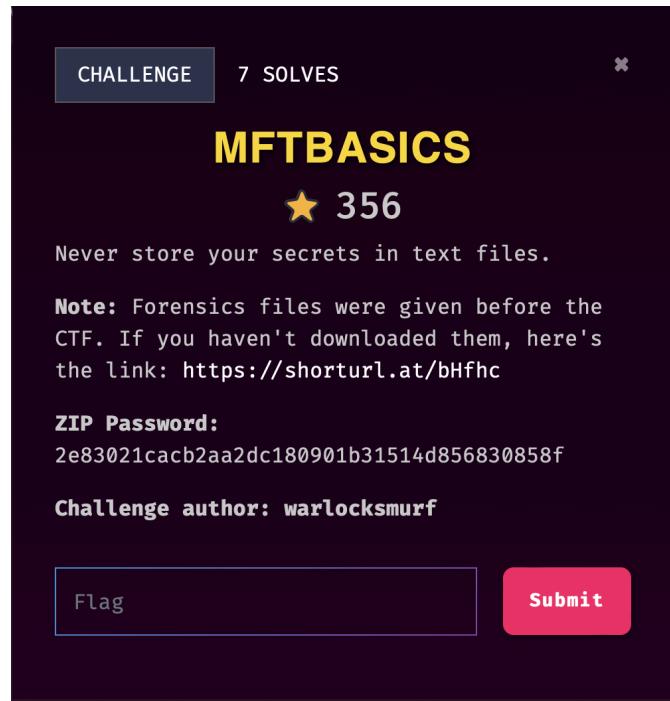


I used the command cat SAM to see the content and finally found the flag which was divided into 3 parts of the questions.

```
->(g!>y*)y*`)'V* cF**h*** AdministratorsAdministrators have complete and unrestricted access to the computer/domain**O*M**K*****O*M**K*****nk #####`  
*****H *****Users 'x@***{"version":1,"questions":[{"question":"What was your first pet s name?", "answer":"GCTF{p3rs0nal"}, {"question":"What s the name of  
the city where you were born?", "answer":"_s3cr3ts_"}, {"question":"What was your childhood nickname?", "answer":"r3g1stry"}]]**1+!+g#7*!  
T=wYyyY***}+2***p_*+2*E*P***R***Yf*1s+[pw*****'***nv-*C*(cpv*2+9***j1+*z***  
HUV,*****G*3*8{******-lyVf*H7***j***zQ***1***{+I***f*]***s***W***Deer:g*D*V*]***yC***a*G]*+ *** z* P*U*x***uE;***g-*W=4***eF*3*+l***.x***fo***B*C***<X*<>  
-+18*b*UJ***W***t***x***K*t*M***3*=1L*2*E  
+oD*** e***a***A?Y*`e***-***C*p***e***Y*`e***
```

Flag: GCTF{p3rs0nal_s3cr3ts_r3g1stry}

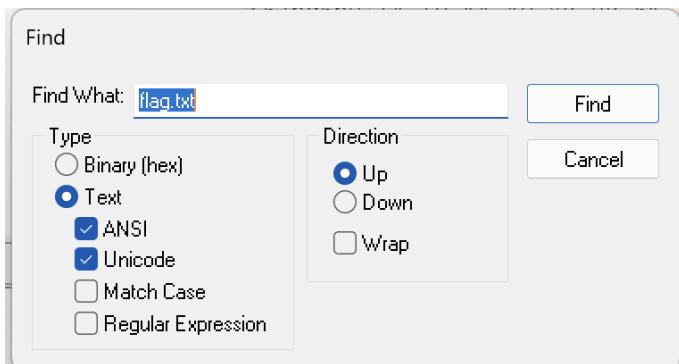
MFTBasics



To perform analysis on the \$MFT file, I put it in a folder and opened it using FTK Imager.

The FTK Imager interface shows the Evidence Tree with a selected folder containing mft2csv_v2.0.0.13 and foxtsecrets.aid. The File List pane displays the contents of the \$MFT file, including its structure and data. The Hex Value Interpreter pane shows the raw byte values for the selected file. The status bar at the bottom right indicates "Activate Windows".

Right click and click find to find a keyword for the secret text file which is flag.txt. Just find it until I find the secret code.



Finally found the secret code:

The secret code is: 47 43 54 46 7b 62 34 73 31 63 73 5f 30 66 5f 4d 46 54 7d 4d

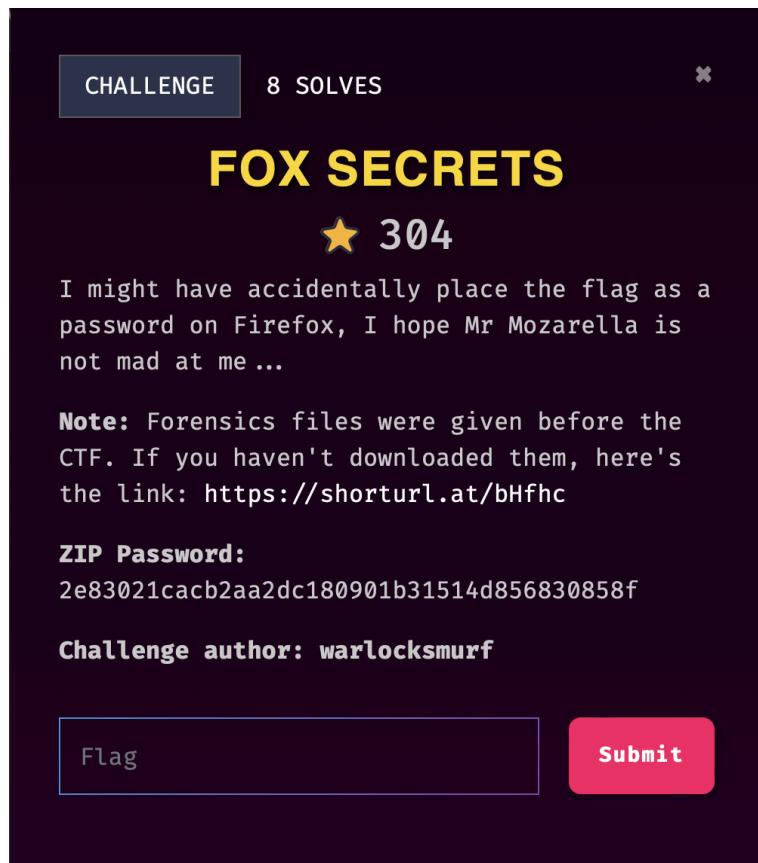
6fadfcf0	08 03 66 00 6C 00 61 00-67 00 2E 00 74 00 78 00	f · l · a · g · · t · x ·
6fadd00	74 00 00 00 00 00 00-40 00 00 00 28 00 00 00 00	t · · · · @ · (· · · ·
6fadd10	00 00 00 00 00 05 00-10 00 00 00 18 00 00 00 00	· · · · · · · · · ·
6fadd20	87 8D 61 04 88 6B EF 11-AB D7 00 0C 29 22 8E 27	· a · ki · <> ·) " ·
6fadd30	80 00 00 00 68 00 00 00-00 00 18 00 00 00 01 00	· · h · · · · · ·
6fadd40	4C 00 00 00 18 00 00 00-54 68 65 20 73 65 63 72	L · · · · · The secr
6fadd50	65 74 20 63 6F 64 65 20-69 73 3A 20 34 37 20 34	et code is: 47 4
6fadd60	33 20 35 34 20 34 36 20-37 62 20 36 32 20 33 34	3 54 46 7b 62 34
6fadd70	20 37 33 20 33 31 20 36-33 20 37 33 20 35 66 20	73 31 63 73 5f
6fadd80	33 30 20 36 36 20 35 66-20 34 64 20 34 36 20 35	30 66 5f 4d 46 5
6fadd90	34 20 37 64 34 64 20 34-FF FF FF FF 82 79 47 11	4 7d4d 4ÿÿÿÿ · yG ·
6fadda0	FF FF FF FF 82 79 47 11-00 00 00 00 18 00 00 00 00	ÿÿÿÿ · yG · · · ·
6faddb0	FF FF FF FF 82 79 47 11-00 00 00 00 00 00 00 00 00	ÿÿÿÿ · yG · · · ·
6faddc0	00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00	· · · · · · · · · ·

To decrypt that I just threw it on cyberchef and finally cracked it.

The screenshot shows the CyberChef interface. The left sidebar lists various conversion recipes: To Base64, From Base64, To Hex, From Hex, To Hexdump, From Hexdump, URL Decode, Regular expression, and Entropy. The main area has tabs for 'From Hex' and 'Input'. The 'Input' tab displays the hex dump: 47 43 54 46 7b 62 34 73 31 63 73 5f 30 66 5f 4d 46 54 7d |. Below the input is the 'Output' tab, which shows the converted string: GCTF{b4s1cs_0f_MFT}.

Flag: GCTF{b4s1cs Of MFT}

Fox Secrets



We were given an image file foxsecrets.ad1. To do an analysis on the image file, I opened it using FTK imager.

Since the clue said they stored the password on firefox, I must look for key4.db and logins.json according to

<https://support.mozilla.org/en-US/kb/profiles-where-firefox-stores-user-data>,

So I looked for the path of the stored password on mozilla which is:

username\AppData\Roaming\Mozilla\Firefox\Profiles

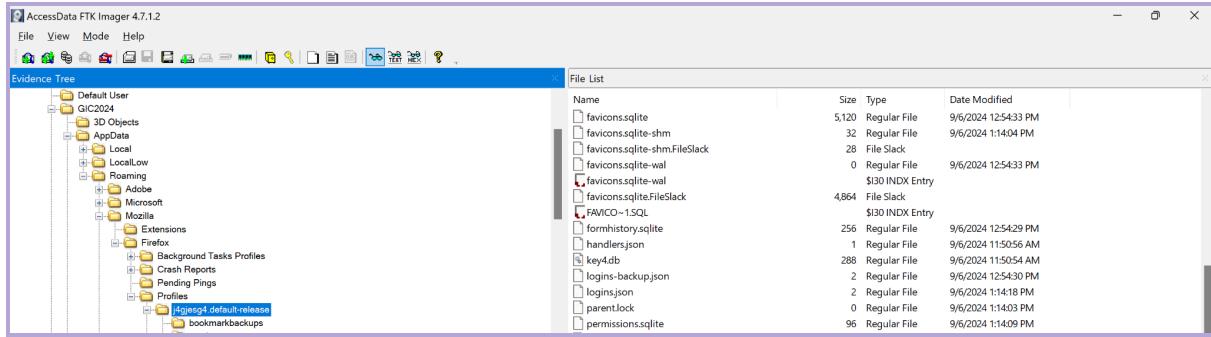


Mozilla Support
<https://support.mozilla.org> :

Profiles - Where Firefox stores your bookmarks, passwords ...

Firefox stores your profile folder in this location on your computer, by default: C:\Users\<your Windows login username>\AppData\Roaming\Mozilla\Firefox\ ...

So to look for the files, I just opened the directories on FTK imager
 GIC2024\AppData\Roaming\Mozilla\Firefox\Profiles\j4gjesg4.default-release and as shown below, there are key4.db and logins.json in that folder.



To retrieve the password, I used this website as my reference:

<https://medium.com/@s12deff/dump-firefox-passwords-with-firepwd-and-firefox-decrypt-65350fd74503>

Since we already have key4.db and logins.json, the step to find the passwords are

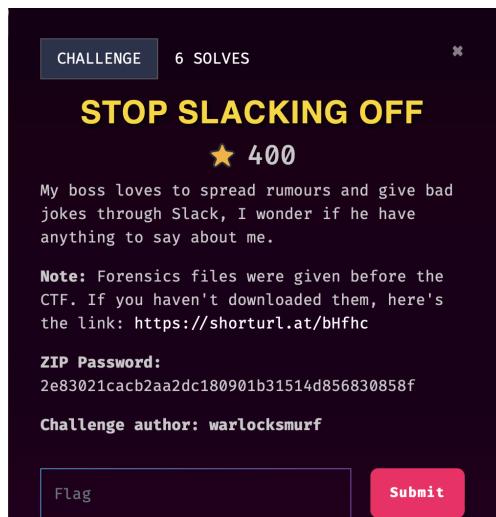
1. git clone <https://github.com/lclevy/firepwd>
2. Put the key4.db and logins.json in the same folder as firepwd
3. python3 firepwd.py

```
sh: no such file or directory: https://github.com/lclevy/firepwd
(base) sayyidahnafishah@Sayyidahs-MacBook-Air fox secret % git clone https://github.com/lclevy/firepwd
Cloning into 'firepwd'...
remote: Enumerating objects: 88, done.
remote: Counting objects: 100% (8/8), done.
remote: Compressing objects: 100% (8/8), done.
remote: Total 88 (delta 2), reused 3 (delta 0), pack-reused 80 (from 1)
Receiving objects: 100% (88/88), 239.08 KiB | 2.28 MiB/s, done.
Resolving deltas: 100% (41/41), done.
(base) sayyidahnafishah@Sayyidahs-MacBook-Air fox secret % ls
firepwd      key4.db      logins.json
(base) sayyidahnafishah@Sayyidahs-MacBook-Air fox secret % cd firepwd
(base) sayyidahnafishah@Sayyidahs-MacBook-Air firepwd % ls
LICENSE      logins.json      mozilla_pbe.svg
firepwd.py    mozilla_db     readme.md
key4.db      mozilla_pbe.pdf  requirements.txt
(base) sayyidahnafishah@Sayyidahs-MacBook-Air firepwd % python3 firepwd
python3: can't open file '/Users/sayyidahnafishah/Desktop/shared/fox secret/firepwd/firepwd': [Errno 2] No such file or directory
(base) sayyidahnafishah@Sayyidahs-MacBook-Air firepwd % python3 firepwd.py
globalsalt: b'b5dbfec66b891e193f16eccaf39209a93d4332'
SEQUENCE {
  SEQUENCE {
    OBJECTIDENTIFIER 1.2.840.113549.1.5.13 pkcs5 pbes2
  SEQUENCE {
    SEQUENCE {
      OBJECTIDENTIFIER 1.2.840.113549.1.5.12 pkcs5 PBKDF2
      SEQUENCE {
        OCTETSTRING b'ea234484d176f2f091e1a9b2162b550a9874bf9ced92daa19c43e058b1328cf'
        INTEGER b'01'
        INTEGER b'20'
        SEQUENCE {
          OBJECTIDENTIFIER 1.2.840.113549.2.9 hmacWithSHA256
        }
      }
    }
    SEQUENCE {
      OBJECTIDENTIFIER 2.16.840.1.101.3.4.1.42 aes256-CBC
      OCTETSTRING b'c361eb1332fd6004ad463de0ef2'
    }
  }
  OCTETSTRING b'c2cb6eb12879f4c649458e59d634f355'
}
clearText b'70617373776f72642d636865636b0282'
password check? True
SEQUENCE {
  SEQUENCE {
    OBJECTIDENTIFIER 1.2.840.113549.1.5.13 pkcs5 pbes2
  SEQUENCE {
    SEQUENCE {
      OBJECTIDENTIFIER 1.2.840.113549.1.5.12 pkcs5 PBKDF2
      SEQUENCE {
        OCTETSTRING b'ae2720e0964ce4beabedba40345712df4234f9ac9cd86e53a08982b65abbb9c'
        INTEGER b'01'
        INTEGER b'20'
        SEQUENCE {
          OBJECTIDENTIFIER 1.2.840.113549.2.9 hmacWithSHA256
        }
      }
    }
  }
  SEQUENCE {
    OBJECTIDENTIFIER 2.16.840.1.101.3.4.1.42 aes256-CBC
  }
}
```

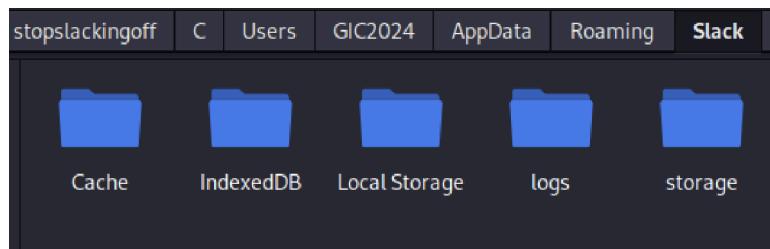
Finally we cracked the password and retrieved the flag after doing all the steps.

Flag:GCTF{m0zarella_f1ref0x_p4ssw0rd}

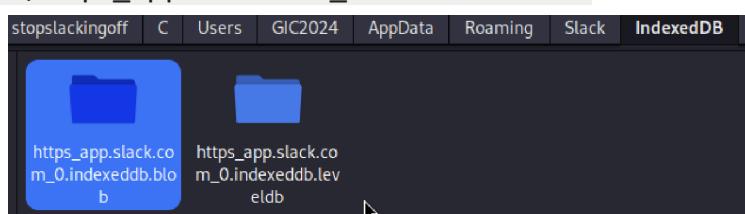
Stop Slacking Off



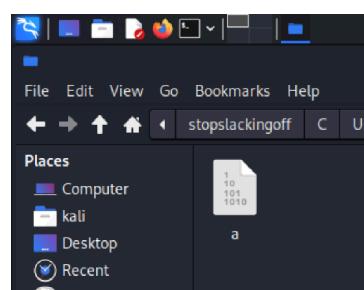
There are 5 folders in the Slack directory. I actually checked and cat all the files in those folders.



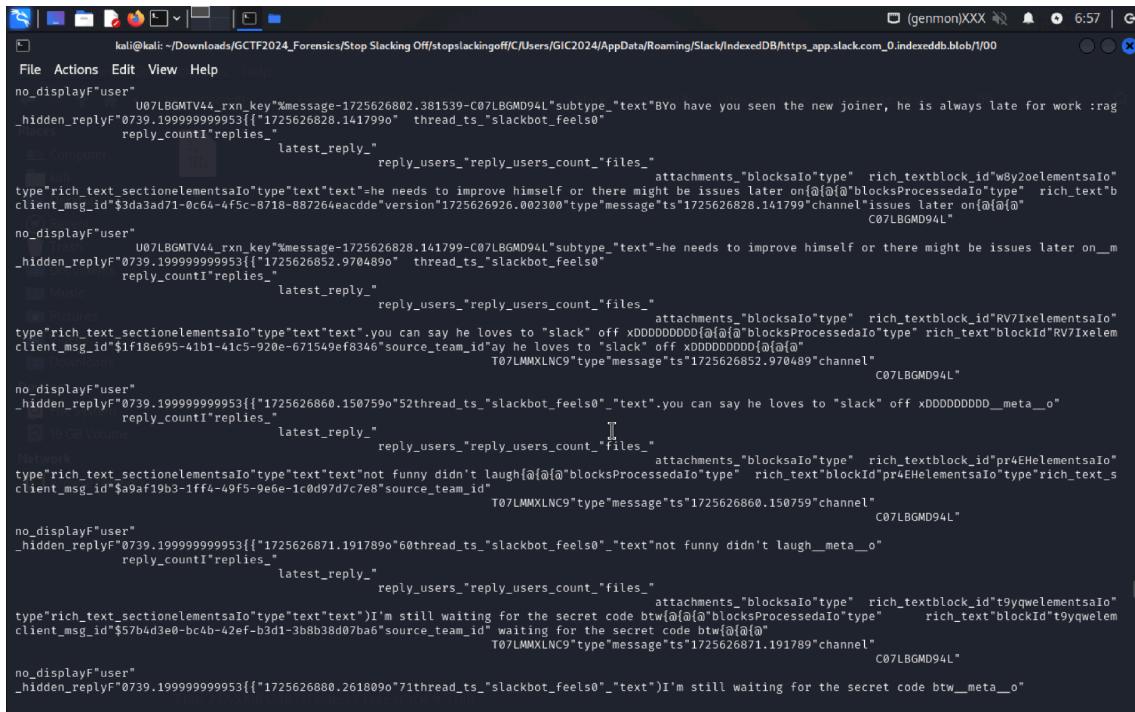
After carefully checked the content of the files, I finally found the conversations on /Slack/IndexedDB/https_app.slack.com_0.indexeddb.blob



Below was the only file in that folder and I checked the content using cat a.



Found the conversation history on slack in that file.

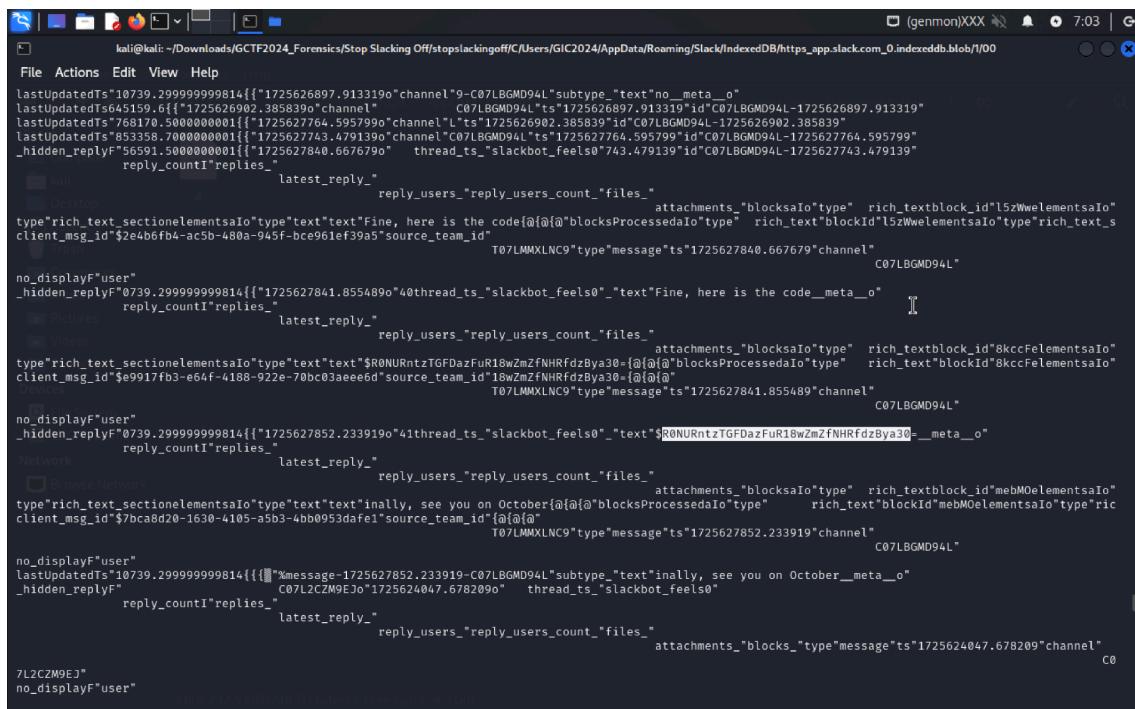


```
kali㉿kali: ~/Downloads/GCTF2024_Forensics/Stop Slacking Off/stopslackingoff/C/Users/GIC2024/AppData/Roaming/Slack/IndexedDB/https_app.slack.com_0_indexeddb.blob/f/00
File Actions Edit View Help
no_displayF"user"
    U07LBGMTV44_rxn_key"%message-1725626802.381539-C07LBGMD94L"subtype_"text"BYo have you seen the new joiner, he is always late for work :rag
_no_hidden_replyF"0739.199999999953[{"1725626828.1417990" "thread_ts_"slackbot_feels0"
    reply_countI"replies_"
        latest_reply_
            reply_users_"reply_users_count_"files_"
                attachments_"blocksA0"type" rich_textblock_id"w8y2oelementsA0"
type"rich_text_sectionelementsA0"type"text"text"=he needs to improve himself or there might be issues later on@{@{@blocksProcessedA0"type" rich_text"b
client_msg_id"$3da3ad71-0c64-4fc-8718-887264eacdde"version"1725626926.00230"message"ts"1725626828.141799"channel"issues later on@{@{@
_c07LBGMD94L"
no_displayF"user"
    U07LBGMTV44_rxn_key"%message-1725626802.381539-C07LBGMD94L"subtype_"text"=he needs to improve himself or there might be issues later on_m
_no_hidden_replyF"0739.199999999953[{"1725626852.9704890" "thread_ts_"slackbot_feels0"
    reply_countI"replies_"
        latest_reply_
            reply_users_"reply_users_count_"files_"
                attachments_"blocksA0"type" rich_textblock_id"RV7IxelementsA0"
type"rich_text_sectionelementsA0"type"text"text"=you can say he loves to "slack" off xDDDDDDDDD@{@{@blocksProcessedA0"type" rich_text"blockId"RV7Ixelem
client_msg_id$1f18e695-41b1-41c5-920e-671549ef8346"source_team_id"ay he loves to "slack" off xDDDDDDDDD@{@{@
T07LMMXLNC9"type"message"ts"1725626852.970489"channel"
C07LBGMD94L"
no_displayF"user"
_no_hidden_replyF"0739.199999999953[{"1725626860.1507590"52"thread_ts_"slackbot_feels0"_"text".you can say he loves to "slack" off xDDDDDDDDD__meta_o"
    reply_countI"replies_"
        latest_reply_
            reply_users_"reply_users_count_"files_"
                attachments_"blocksA0"type" rich_textblock_id"pr4EHelementsA0"
type"rich_text_sectionelementsA0"type"text"text"not funny didn't laugh@{@{@blocksProcessedA0"type" rich_text"blockId"pr4EHelementsA0"type"rich_text_s
client_msg_id$a9af19b3-1ff4-49f5-9e6e-1c0d97d7c7e8"source_team_id"
T07LMMXLNC9"type"message"ts"1725626860.150759"channel"
C07LBGMD94L"
no_displayF"user"
_no_hidden_replyF"0739.199999999953[{"1725626871.1917890"60"thread_ts_"slackbot_feels0"_"text"not funny didn't laugh__meta_o"
    reply_countI"replies_"
        latest_reply_
            reply_users_"reply_users_count_"files_"
                attachments_"blocksA0"type" rich_textblock_id"t9yqwelementsA0"
type"rich_text_sectionelementsA0"type"text"text"!m still waiting for the secret code btw@{@{@blocksProcessedA0"type" rich_text"blockId"t9yqwelem
client_msg_id$57b4d3e0-bc4b-42ef-b3d1-3bb38d07ba6"source_team_id" waiting for the secret code btw@{@{@
T07LMMXLNC9"type"message"ts"1725626871.191789"channel"
C07LBGMD94L"
no_displayF"user"
_no_hidden_replyF"0739.199999999953[{"1725626880.2618090"71"thread_ts_"slackbot_feels0"_"text")I'm still waiting for the secret code btw__meta_o"
    reply_countI"replies_"
        latest_reply_
            reply_users_"reply_users_count_"files_"

```

After carefully reading the conversations, I found the secret code which is:

RONURntzTGF DazFuR18wZmZfNHRfdzBya30



```
kali㉿kali: ~/Downloads/GCTF2024_Forensics/Stop Slacking Off/stopslackingoff/C/Users/GIC2024/AppData/Roaming/Slack/IndexedDB/https_app.slack.com_0_indexeddb.blob/f/00
File Actions Edit View Help
lastUpdatedTs"10739.29999999814[{"1725626897.9133190"channel"9-C07LBGMD94L"subtype_"text"no__meta_o"
lastUpdatedTs"10739.29999999814[{"1725626902.3858390"channel"
C07LBGMD94L"ts"1725626897.913319"id"C07LBGMD94L-1725626897.913319"
lastUpdatedTs"768170.500000001[{"1725627764.5957990"channel"1"ts"1725626902.385839"id"C07LBGMD94L-1725626902.385839"
lastUpdatedTs"753358.700000001[{"1725627743.4791390"channel"1"ts"1725627764.595799"id"C07LBGMD94L-1725627764.595799"
_no_hidden_replyF"5691.500000001[{"1725627840.6676790" "thread_ts_"slackbot_feels0"743.479139"id"C07LBGMD94L-1725627743.479139"
    reply_countI"replies_"
        latest_reply_
            reply_users_"reply_users_count_"files_"
                attachments_"blocksA0"type" rich_textblock_id"l5zWwelementsA0"
type"rich_text_sectionelementsA0"type"text"text"Fine, here is the code@{@{@blocksProcessedA0"type" rich_text"blockId"l5zWwelementsA0"type"rich_text_s
client_msg_id$2e4b6fb4-ac5b-480a-945f-bce691ef39a5"source_team_id"
T07LMMXLNC9"type"message"ts"1725627840.667679"channel"
C07LBGMD94L"
no_displayF"user"
_no_hidden_replyF"0739.29999999814[{"1725627841.8554890"40"thread_ts_"slackbot_feels0"_"text"fine, here is the code__meta_o"
    reply_countI"replies_"
        latest_reply_
            reply_users_"reply_users_count_"files_"
                attachments_"blocksA0"type" rich_textblock_id"8kccFelementsA0"
type"rich_text_sectionelementsA0"type"text"text"$$RONURntzTGF DazFuR18wZmZfNHRfdzBya30=[@{@{@blocksProcessedA0"type" rich_text"blockId"8kccFelementsA0
client_msg_id$9917fb3-e64f-4188-922e-70bc03aeee6"source_team_id"18wZmZfNHRfdzBya30=[@{@{@
T07LMMXLNC9"type"message"ts"1725627841.855489"channel"
C07LBGMD94L"
no_displayF"user"
_no_hidden_replyF"0739.29999999814[{"1725627852.2339190"41"thread_ts_"slackbot_feels0"_"text"$$RONURntzTGF DazFuR18wZmZfNHRfdzBya30=__meta_o"
    reply_countI"replies_"
        latest_reply_
            reply_users_"reply_users_count_"files_"
                attachments_"blocksA0"type" rich_textblock_id"mebMoelementsA0"
type"rich_text_sectionelementsA0"type"text"text"inally, see you on October@{@{@blocksProcessedA0"type" rich_text"blockId"mebMoelementsA0"type"ric
client_msg_id$7bca8d20-1630-4105-a5b3-4bb0953dafe1"source_team_id"[@{@{@
T07LMMXLNC9"type"message"ts"1725627852.233919"channel"
C07LBGMD94L"
no_displayF"user"
lastUpdatedTs"10739.29999999814[{"1725627852.233919-C07LBGMD94L"subtype_"text"inally, see you on October__meta_o"
_no_hidden_replyF" C07LB2CZM9EJ"0725624047.678209" "thread_ts_"slackbot_feels0"
    reply_countI"replies_"
        latest_reply_
            reply_users_"reply_users_count_"files_"
                attachments_"blocks_A0"type"message"ts"1725624047.678209"channel"
C07LB2CZM9EJ"
7L2CZM9EJ"
no_displayF"user"

```

As usual, to decrypt it, I just put in the cyberchef and let it do the work.

The screenshot shows the CyberChef interface with the following details:

- Input:** R0NURntzTGFdazFuR18wZmZfNHRfdzBya30
- Recipe:** Magic (Depth 3, Intensive mode checked)
- Output:** Four rows of decrypted data:
 - From_Base85('0-9a-zA-Z.\\";:+=~!/*?&>()[]{}@%\$#') Decode_text('IBM EBCDIC French (1010)')
 - From_Base64('A-Za-z0-9_+',true,false)
 - From_Base64('A-Za-z0-9_+',true,false)
 - From_Base85('0-9a-zA-Z.\\";:+=~!/*?&>()[]{}@%\$#') Decode_text('IAS German (7-bit) (20106)')Each row includes raw bytes, hex dump, entropy, and validation information (Valid UTF8, Entropy: 2.56, Matching ops: From Base85, etc.).
- Buttons:** STEP, BAKE!, Auto Bake

Flag: GCTF{sLaCk1nG_0ff_4t_w0rk}