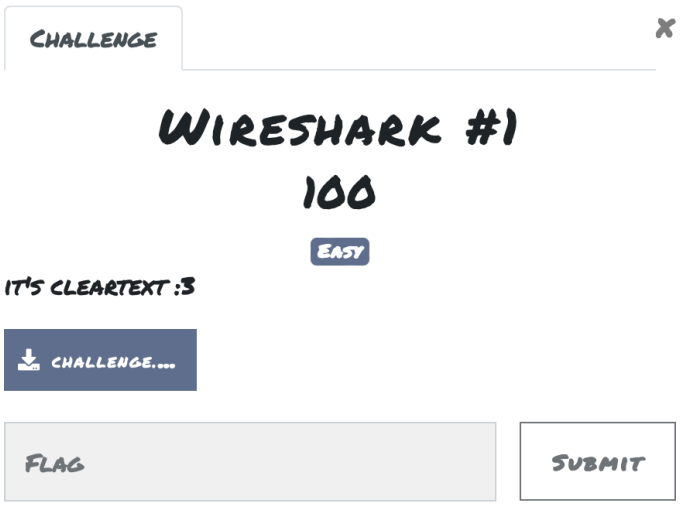
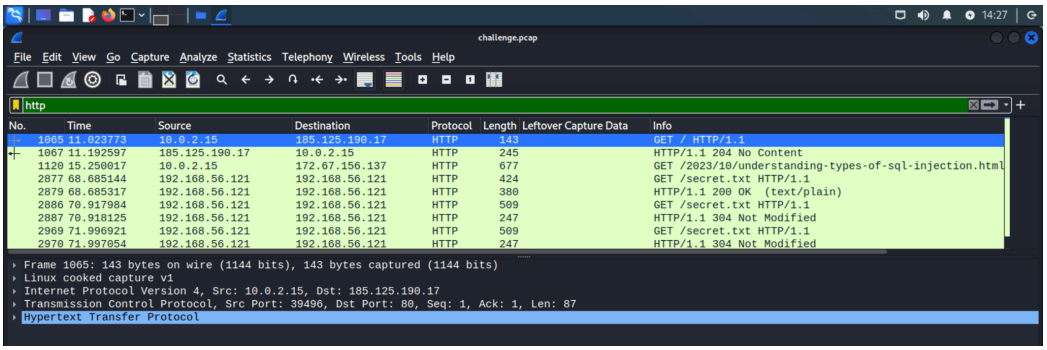
Wrote by

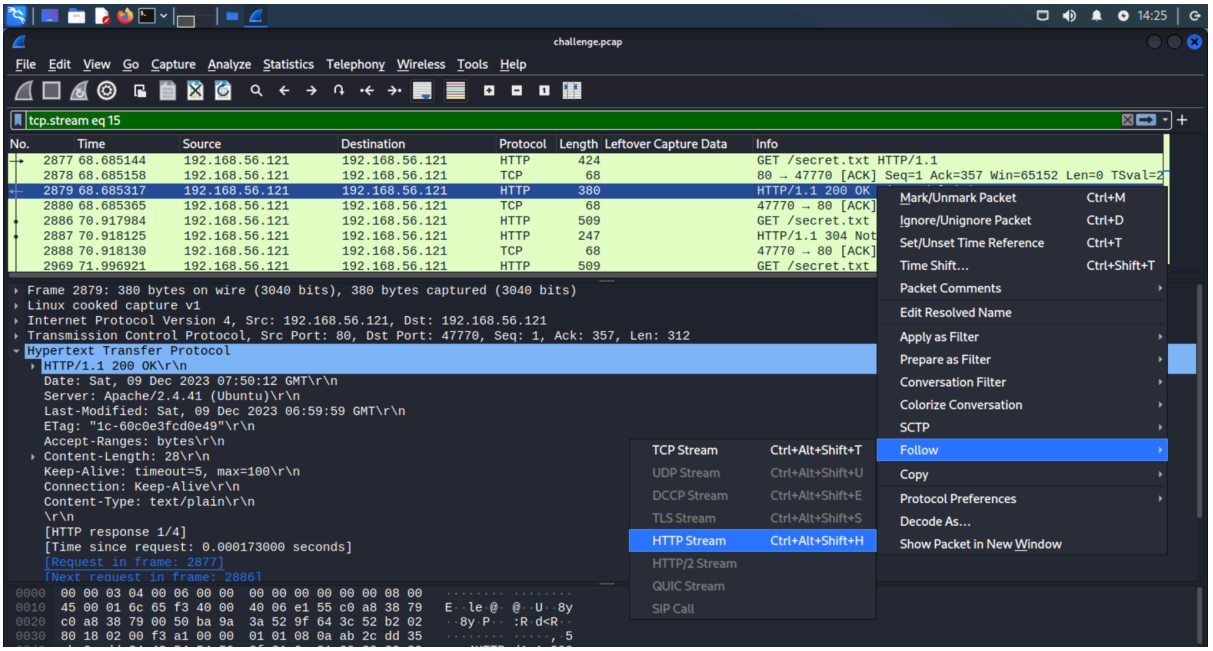
Dark Phoenix

WIRESHARK #1

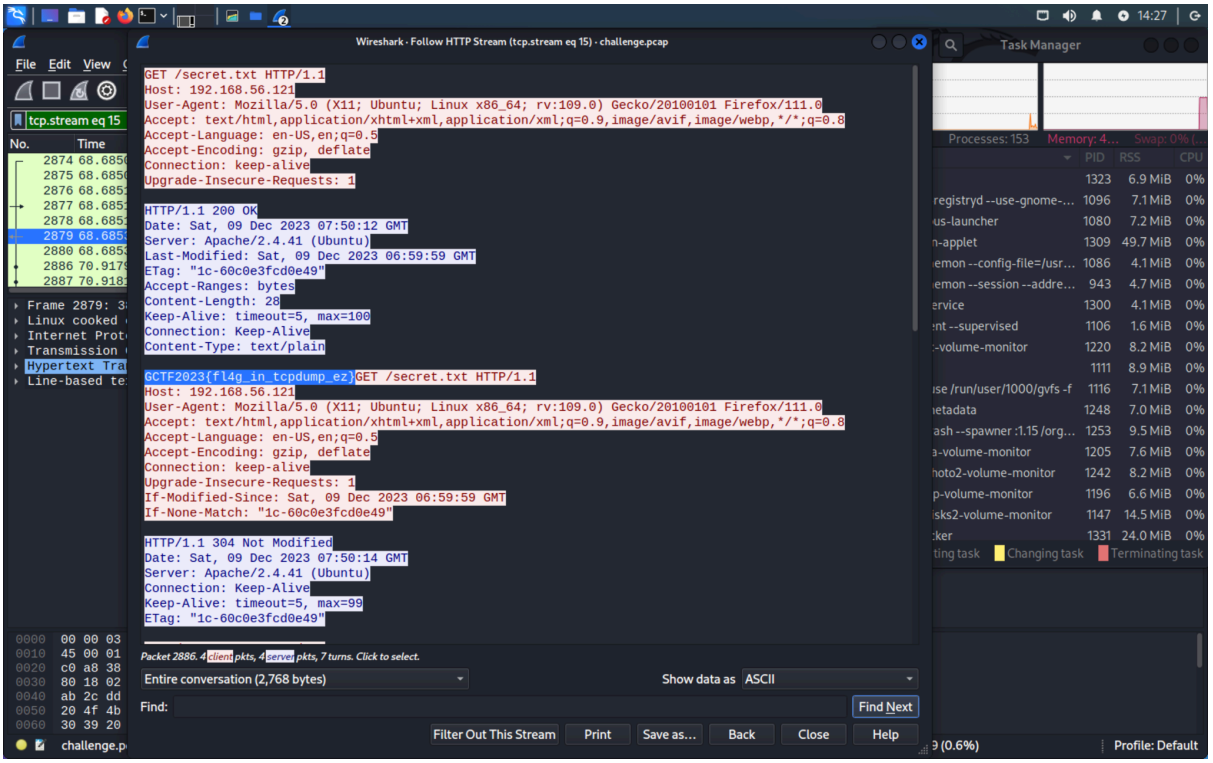




So firstly, I opened the file and applied a filter for http in the wireshark. Just like the hint given, it is clear text, and there is a suspicious plain txt file named “secret.txt” in the info.



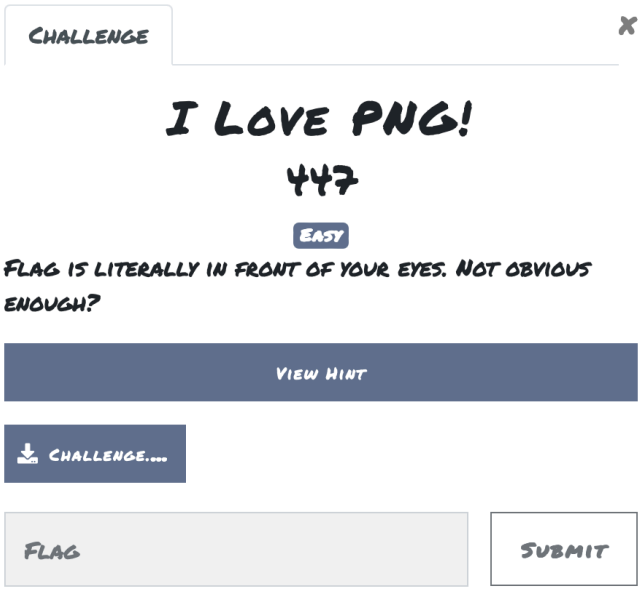
Then I just right click on the pcap, and follow the HTTP Stream.



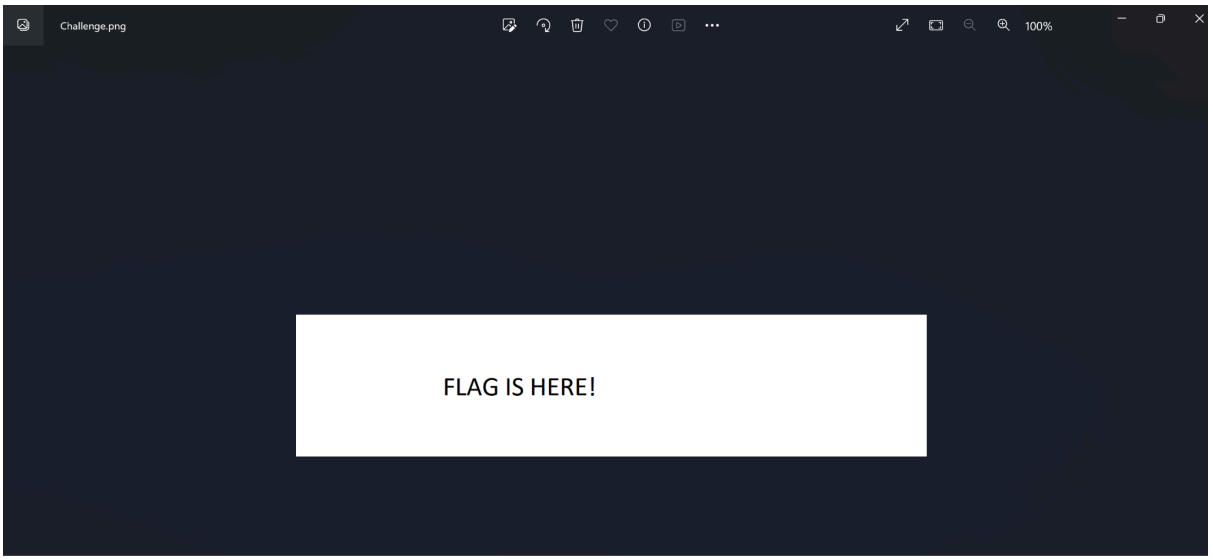
As shown above, I have highlighted the flag in the HTTP Stream.

Flag: GCTF2023{fl4g_in_tcpdump_ez}

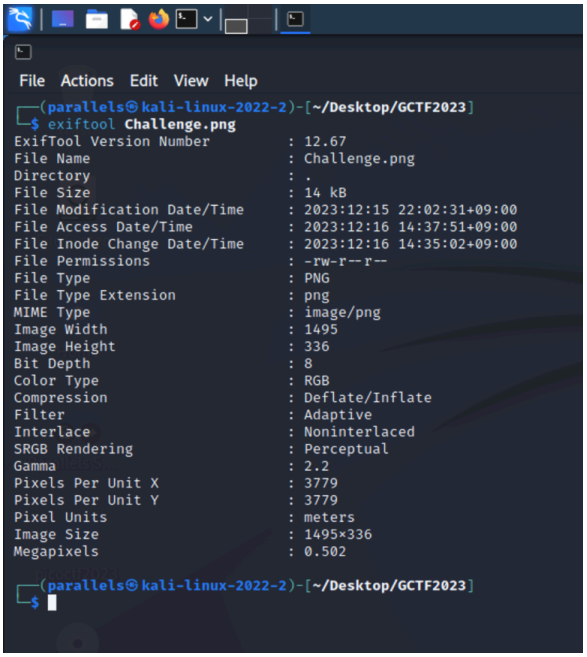
I LOVE PNG!



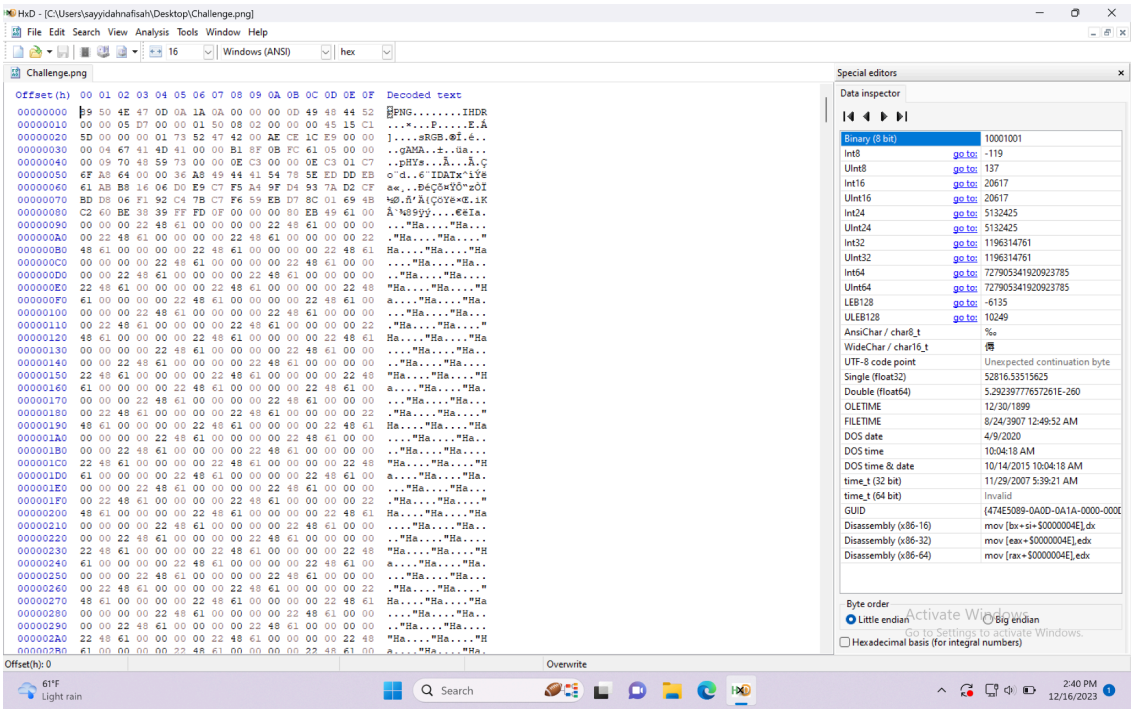
Initially I couldn't open the file in mac os or kali linux, but then I tried to open it in windows vm and it works fine there.



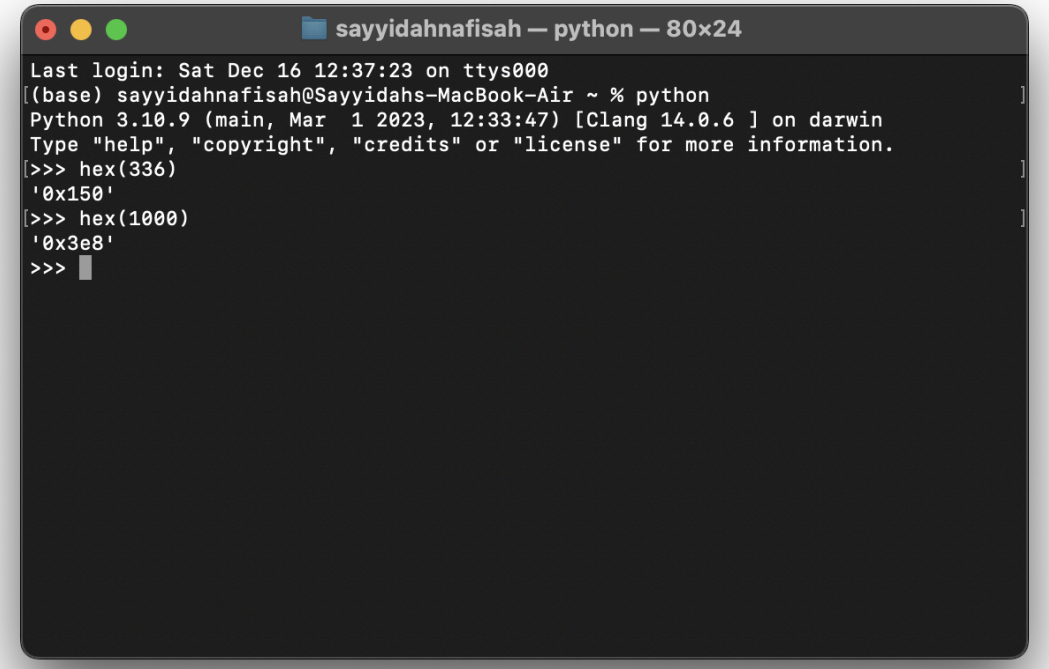
So this is how the image originally looks like. However, this was the only thing on the image and there was no flag. The image also looks like it has been cropped.



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.

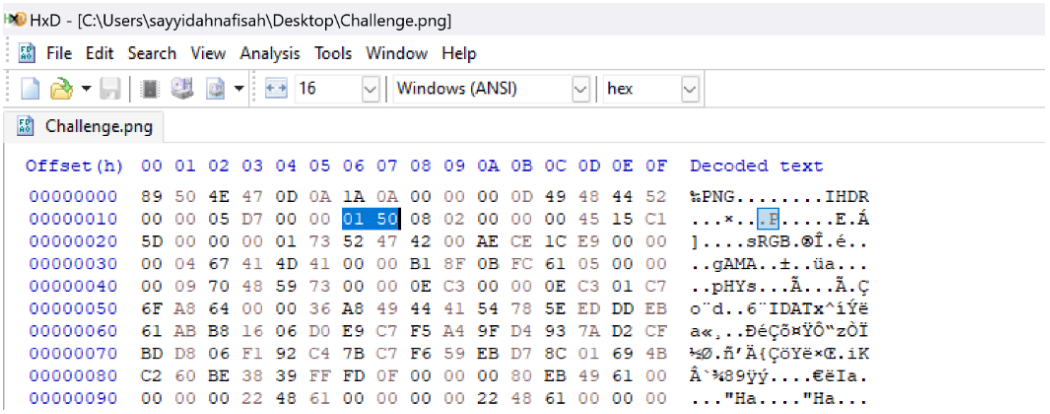


Then, I opened the file using HxD, a hex editor program to edit the hex value of the image. So the numbers here are in hex values.

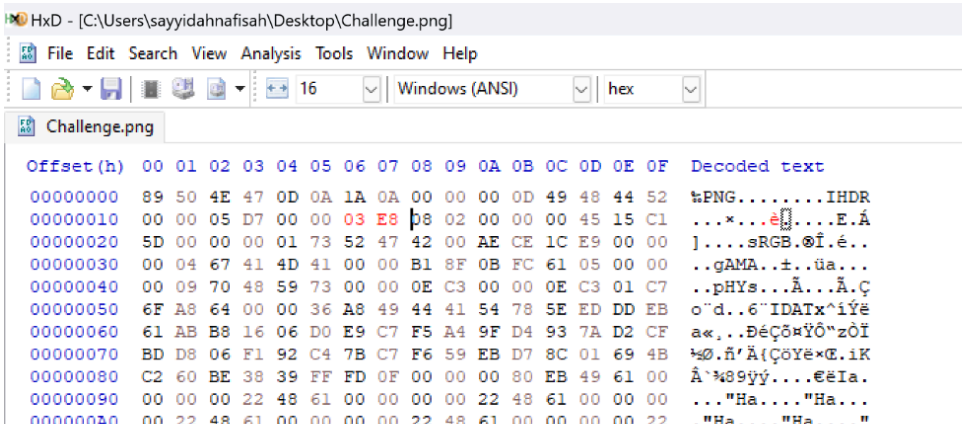


Then, I used python to convert the height that I retrieved from the information earlier into a hex value and the hex value for 336 is 0x150.

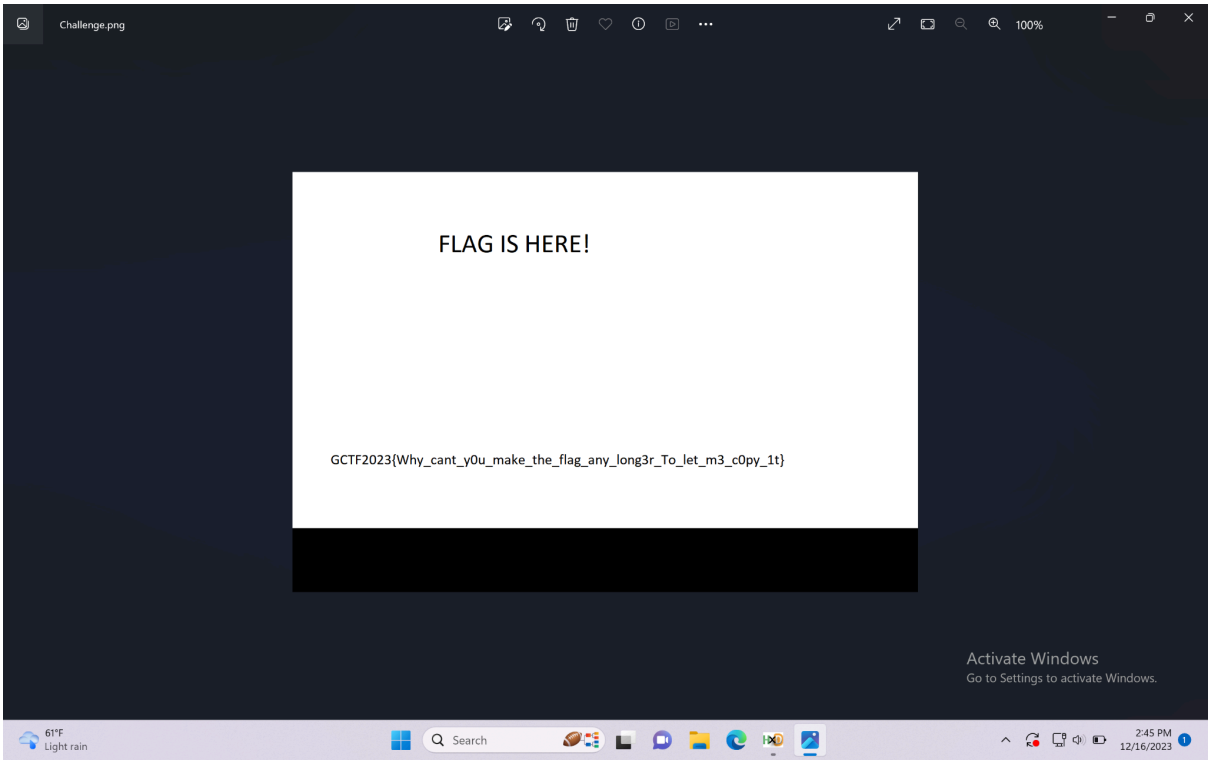
I also converted 1000 to hex value because I'm going to change the image height from 336 to 1000. The new height will be 0x3E8



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.



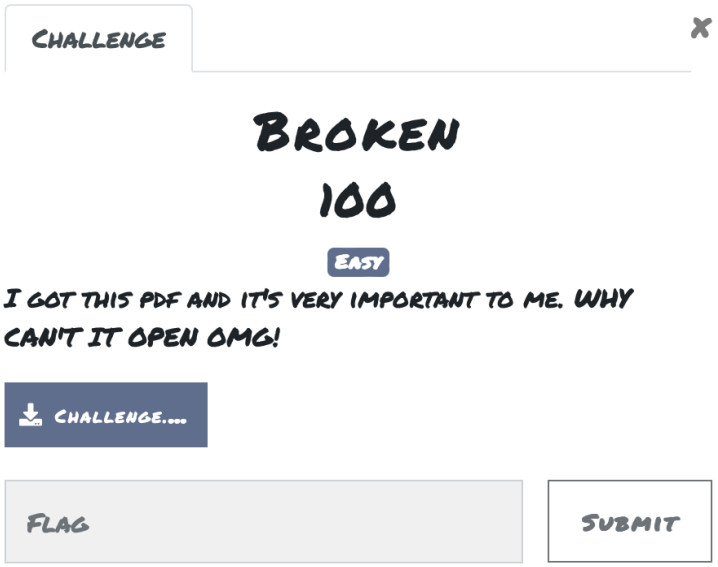
The red hex values are the new height of the image. 03 E8 is the hex value for 1000 which is 0x3E8.

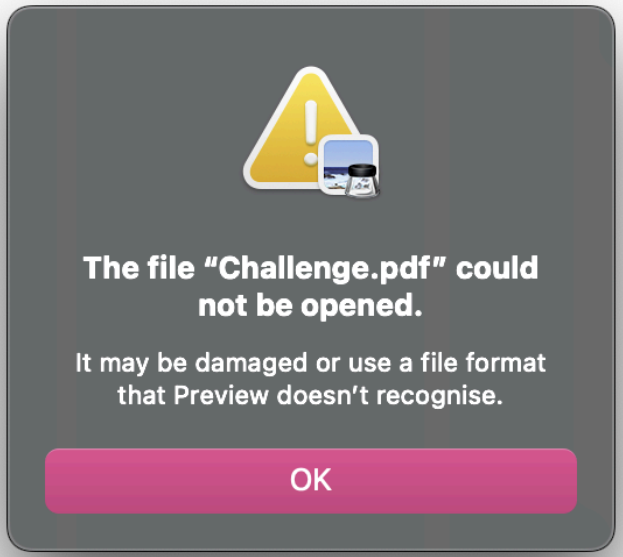


After I edited and saved the new hex value, I reopened the png file and there's the flag!

Flag: GCTF{Why_cant_y0u_make_the_flag_any_long3r_To_let_m3_c0py_1t}

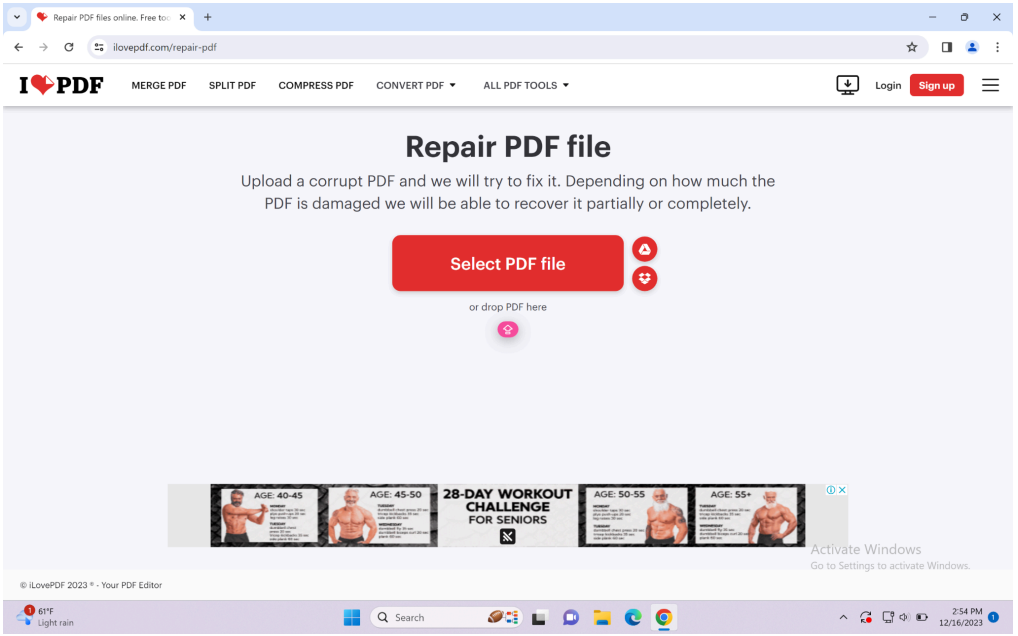
BROKEN



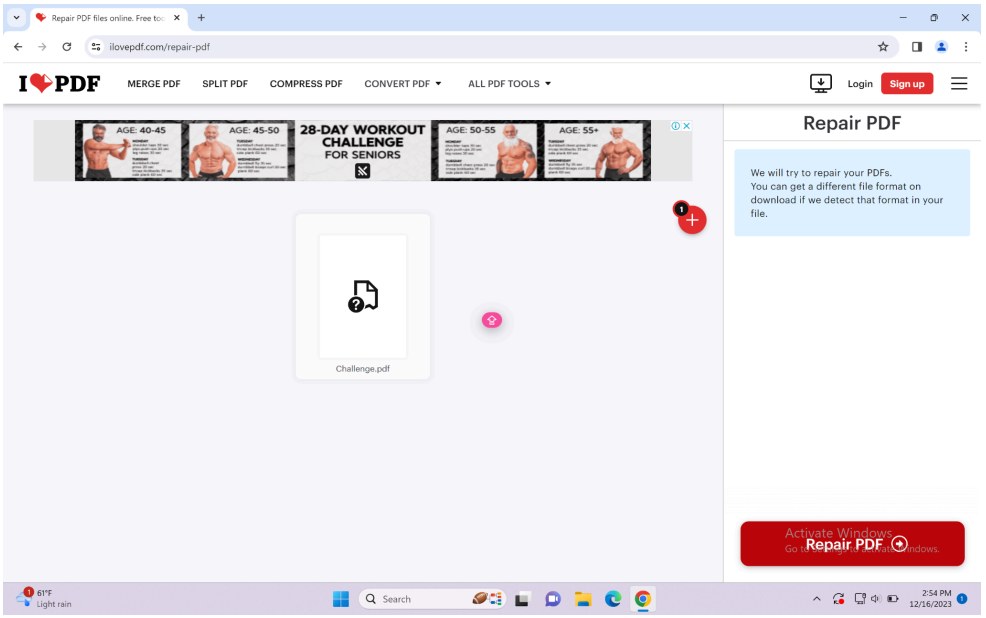


So we were given a broken pdf file. Then I googled and found a website to repair pdf files. The website link is as below:

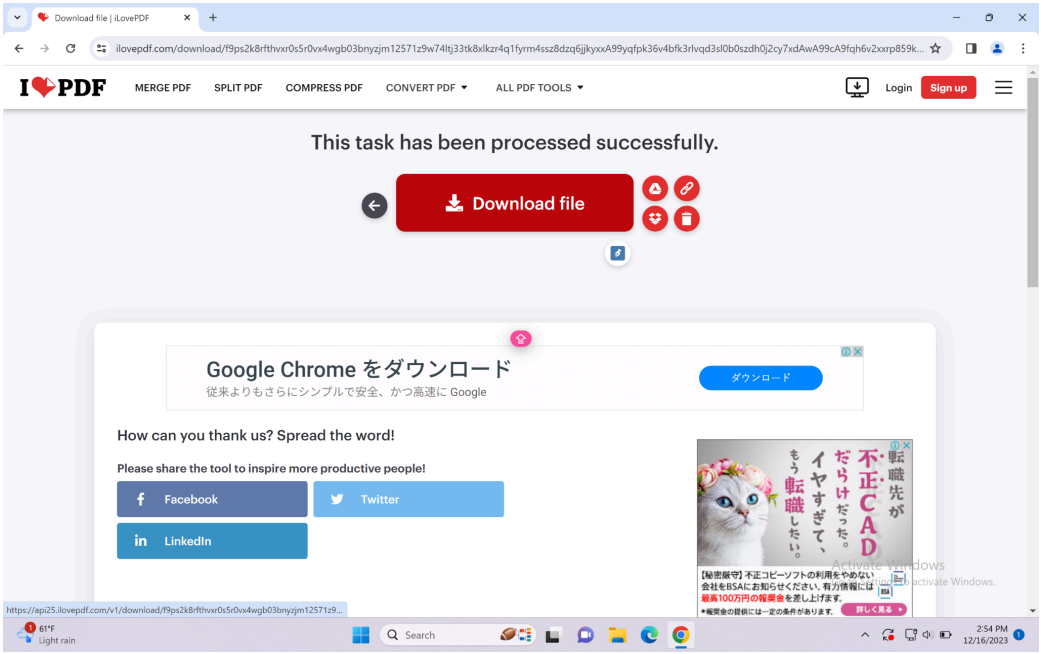
https://www.ilovepdf.com/repair-pdf



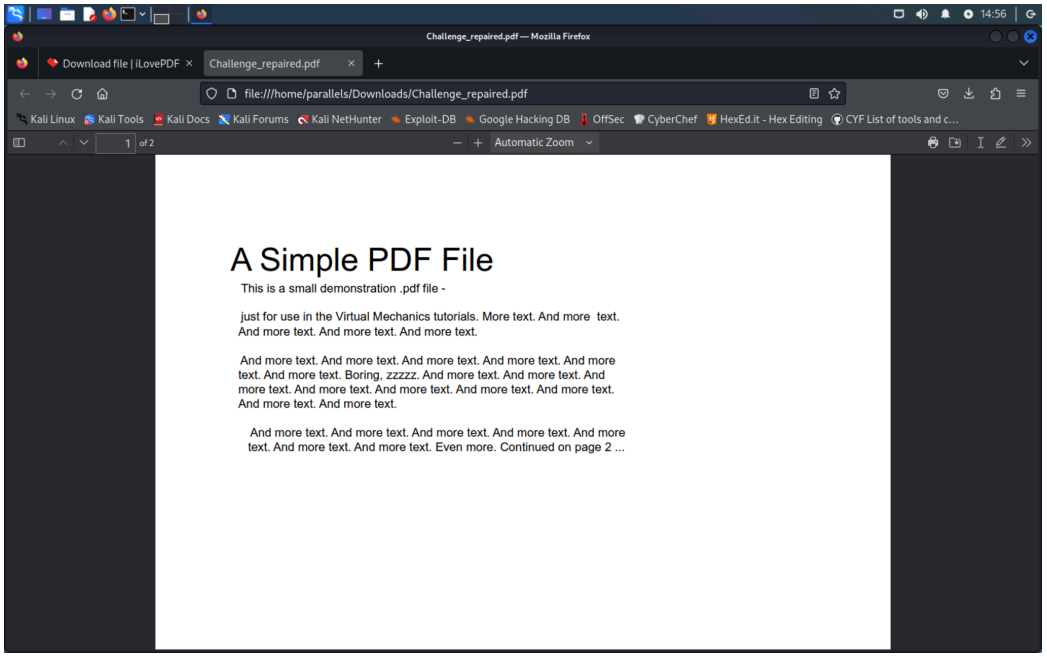
I clicked “select pdf file” to upload a broken pdf file.

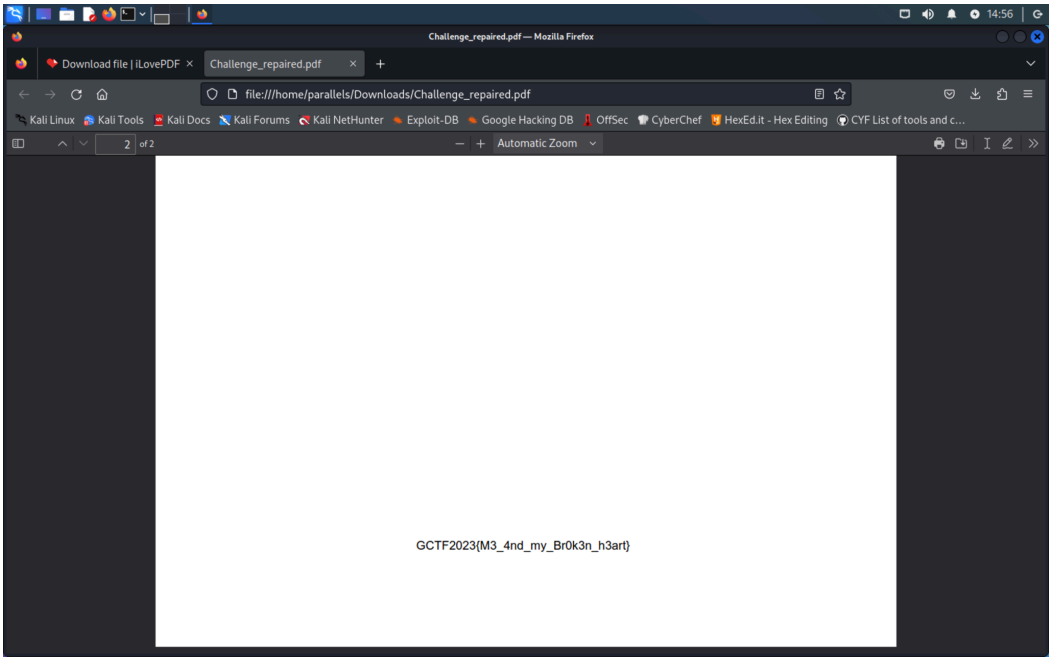


I uploaded Challenge.pdf



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

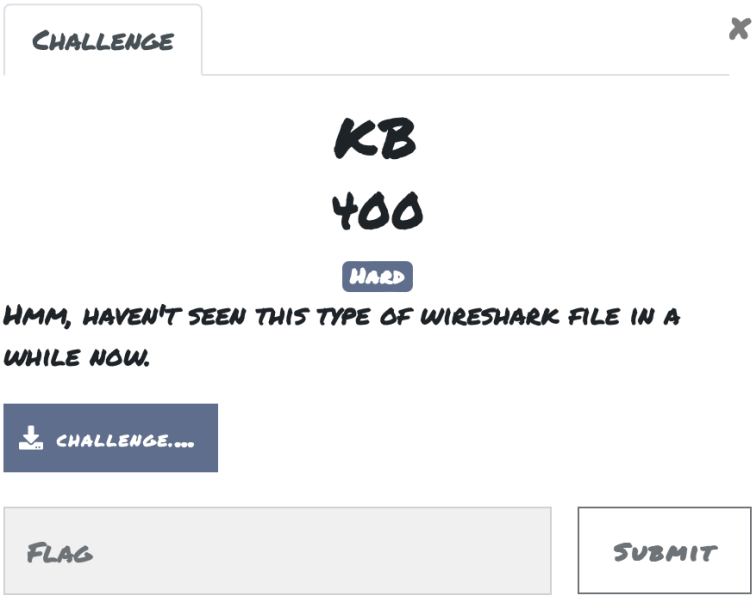


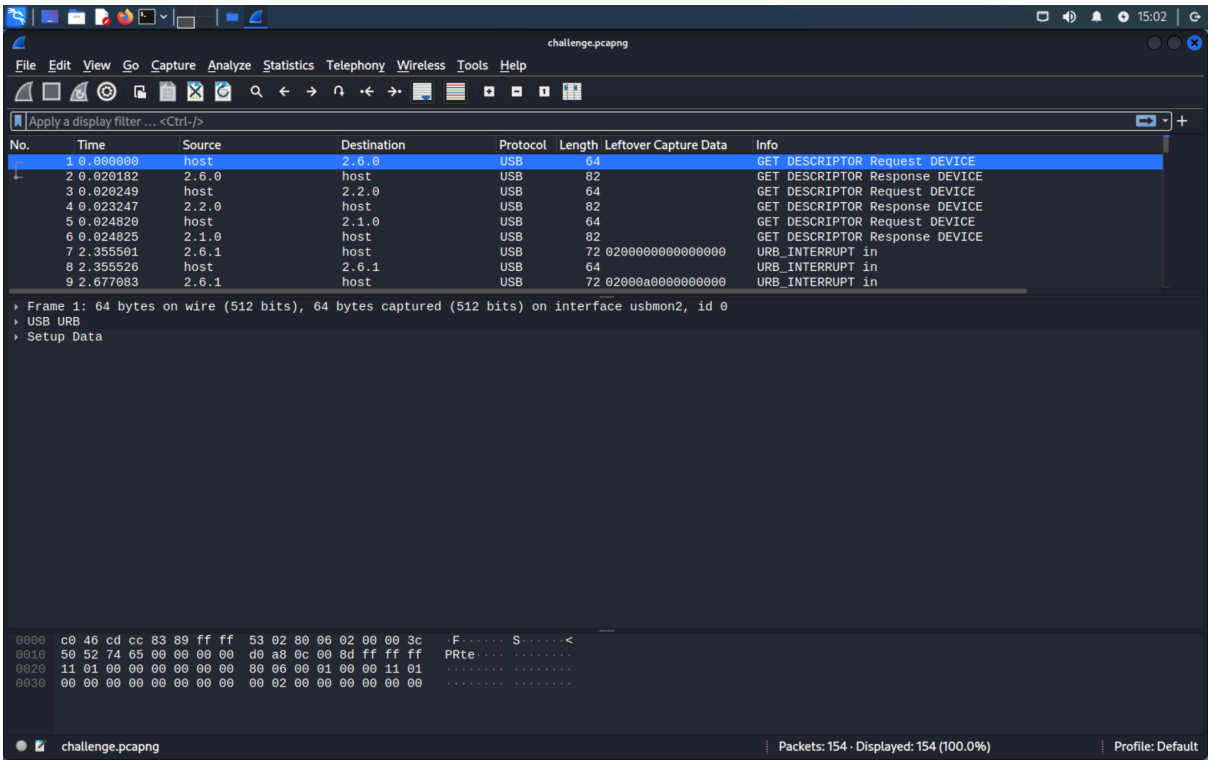


Found the flag!

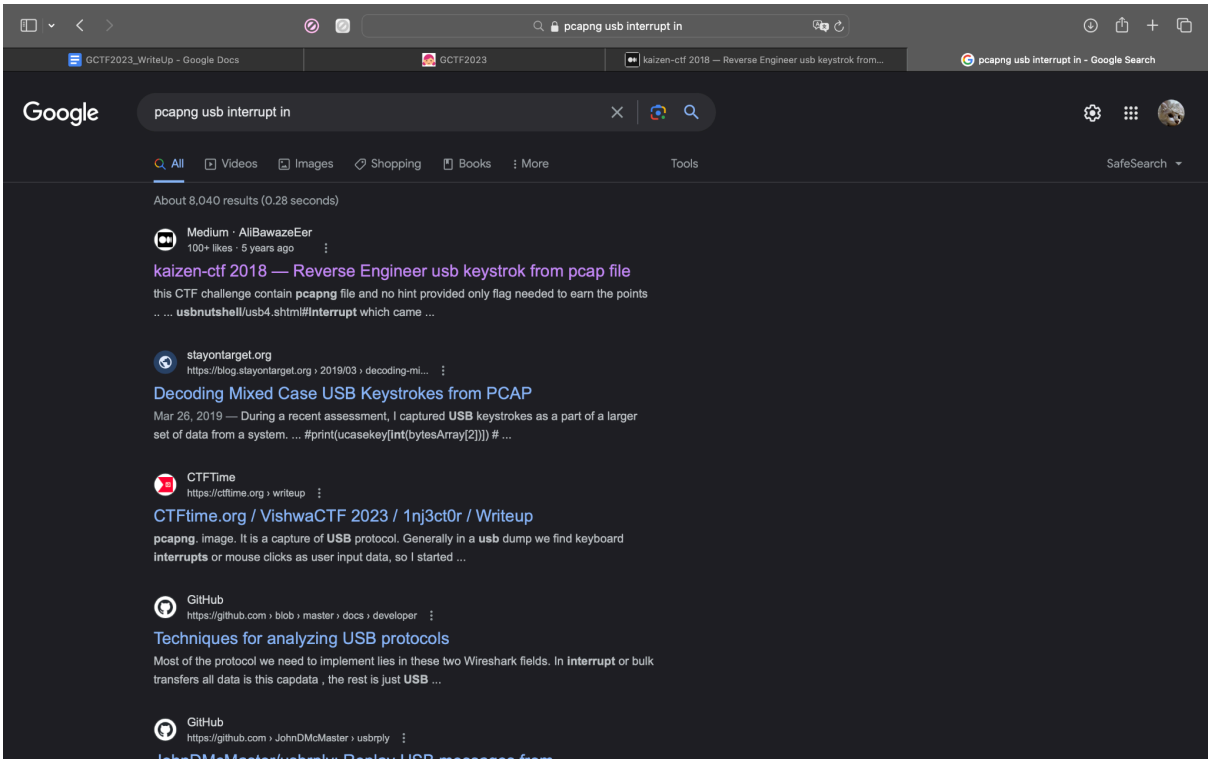
Flag: GCTF2023{M3_4nd_my_Br0k3n_h3art}

KB



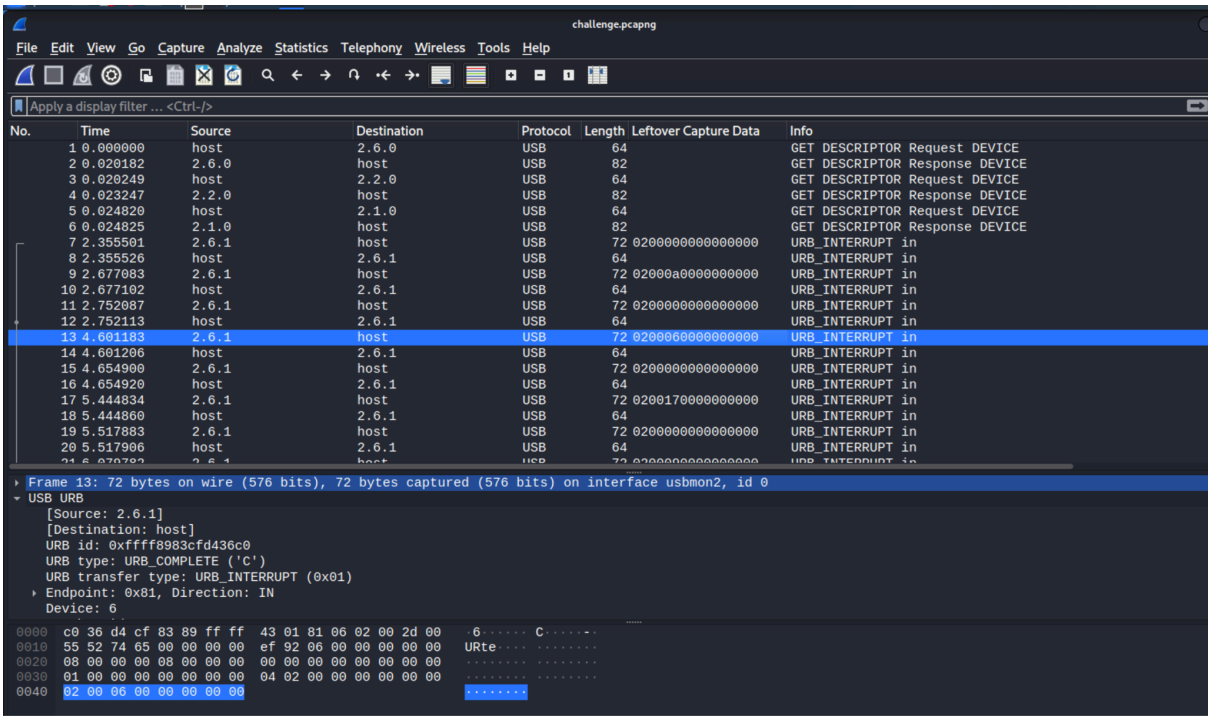


For this challenge,I opened the file using wireshark, and this is what it shows.

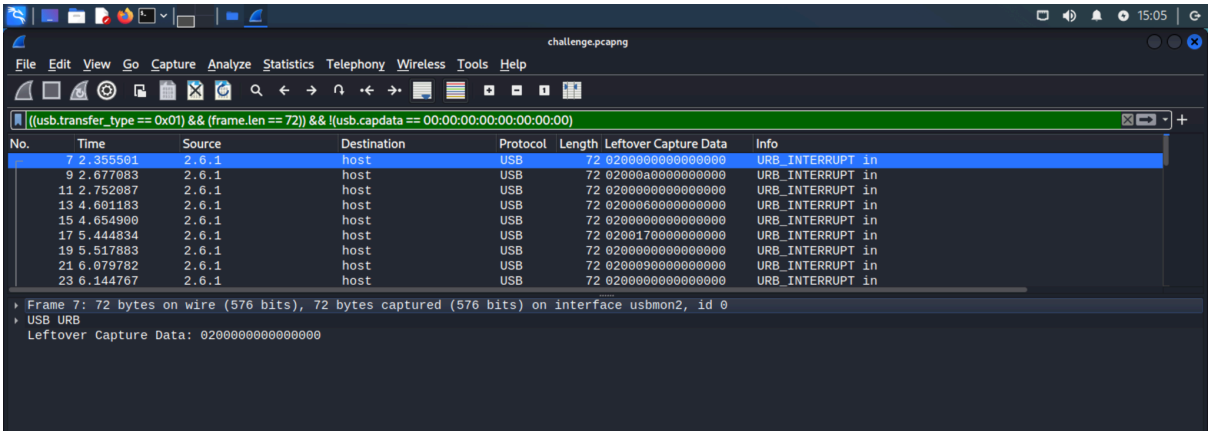


Then, I just googled some keywords and I found this website (link below) and I referred to it for this challenge.

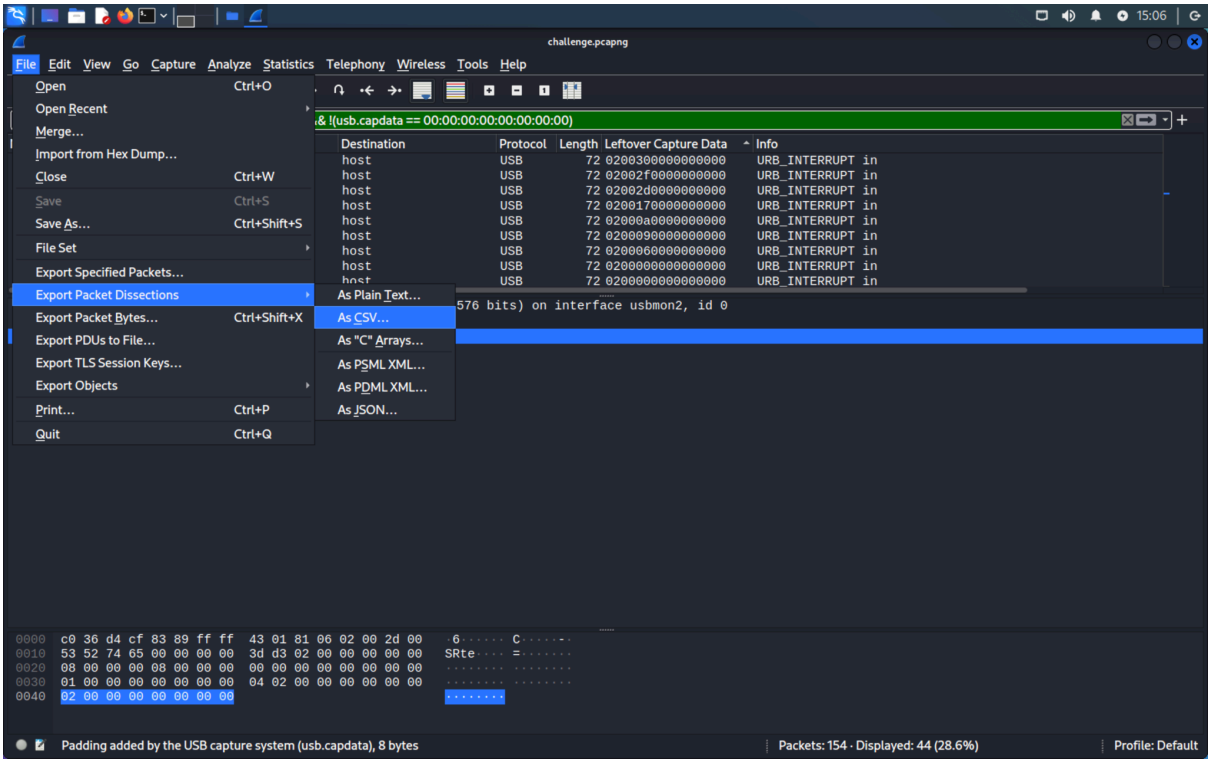
https://abawazeeer.medium.com/kaizen-ctf-2018-reverse-engineer-usb-keystrok-from-pcap-file-2412351679f4



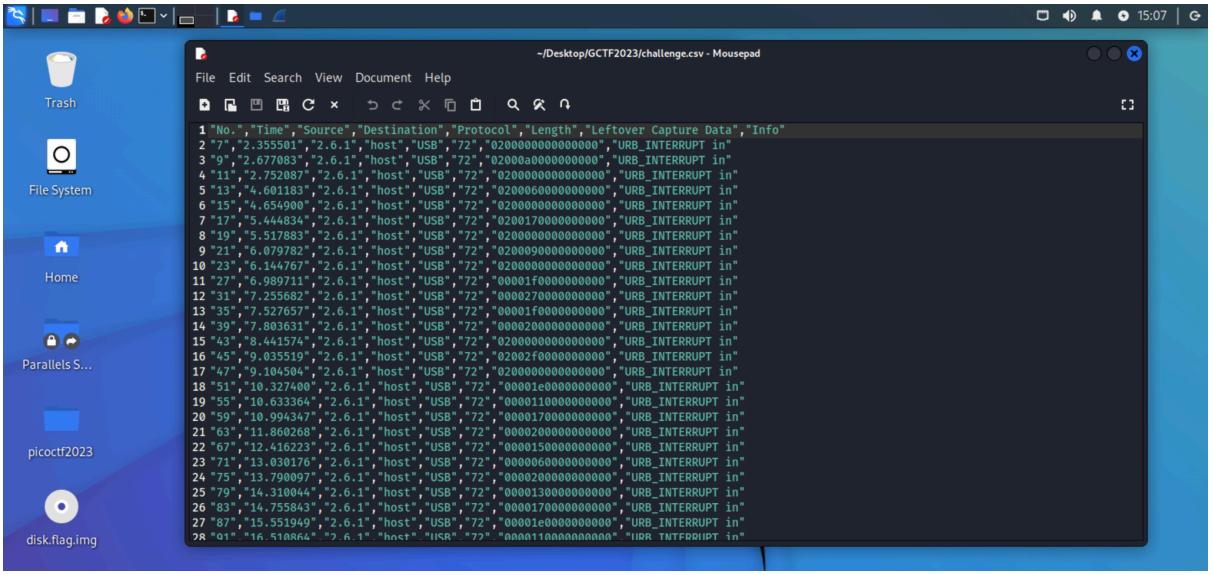
So, as we can see, there is some pattern in Leftover Capture Data, where a certain number changed on that position only, and it occurs on USB transfer type URB_INTERRUPT with frame length 72 only.



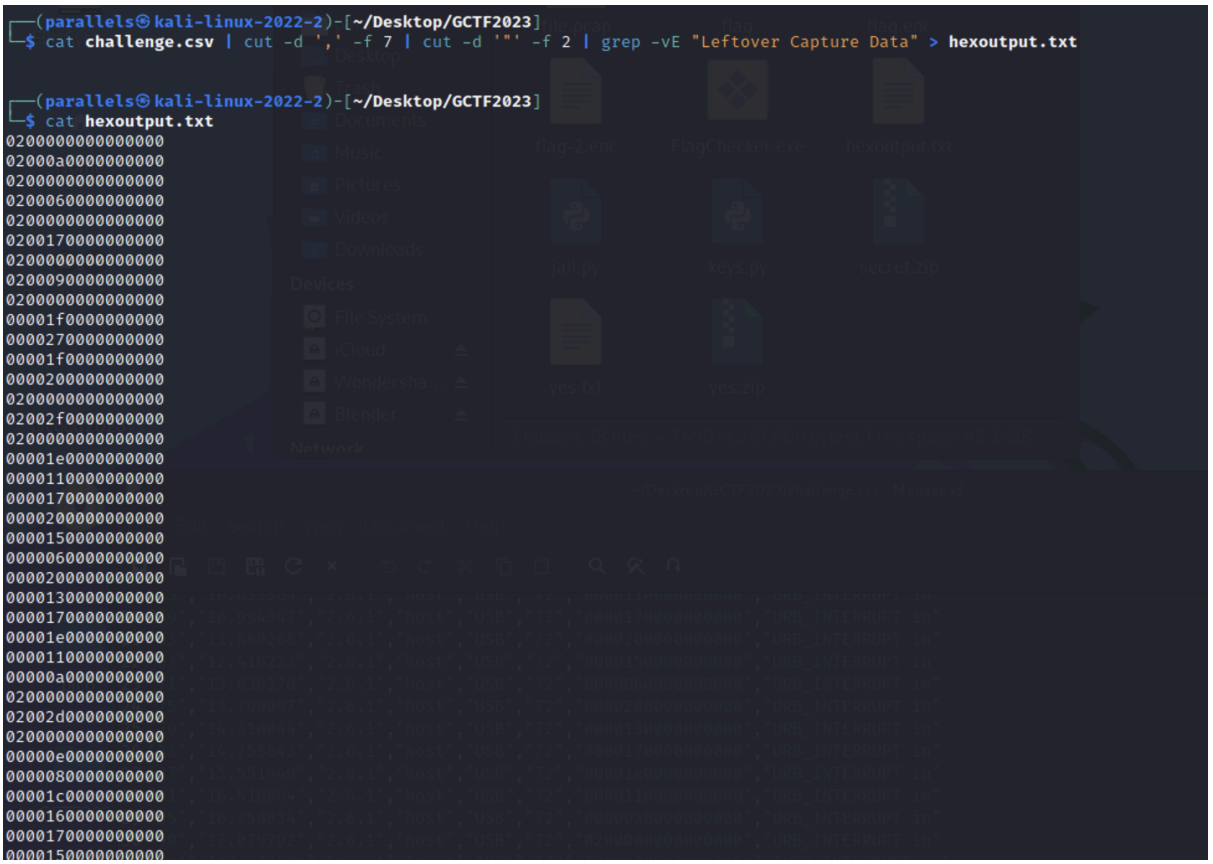
So, we filtered the data using this logic where usb transfer type is 0x01, and frame length 72: **((usb.transfer_type == 0x01) && (frame.len == 72)) && !(usb.capdata == 00:00:00:00:00:00:00:00)**



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.



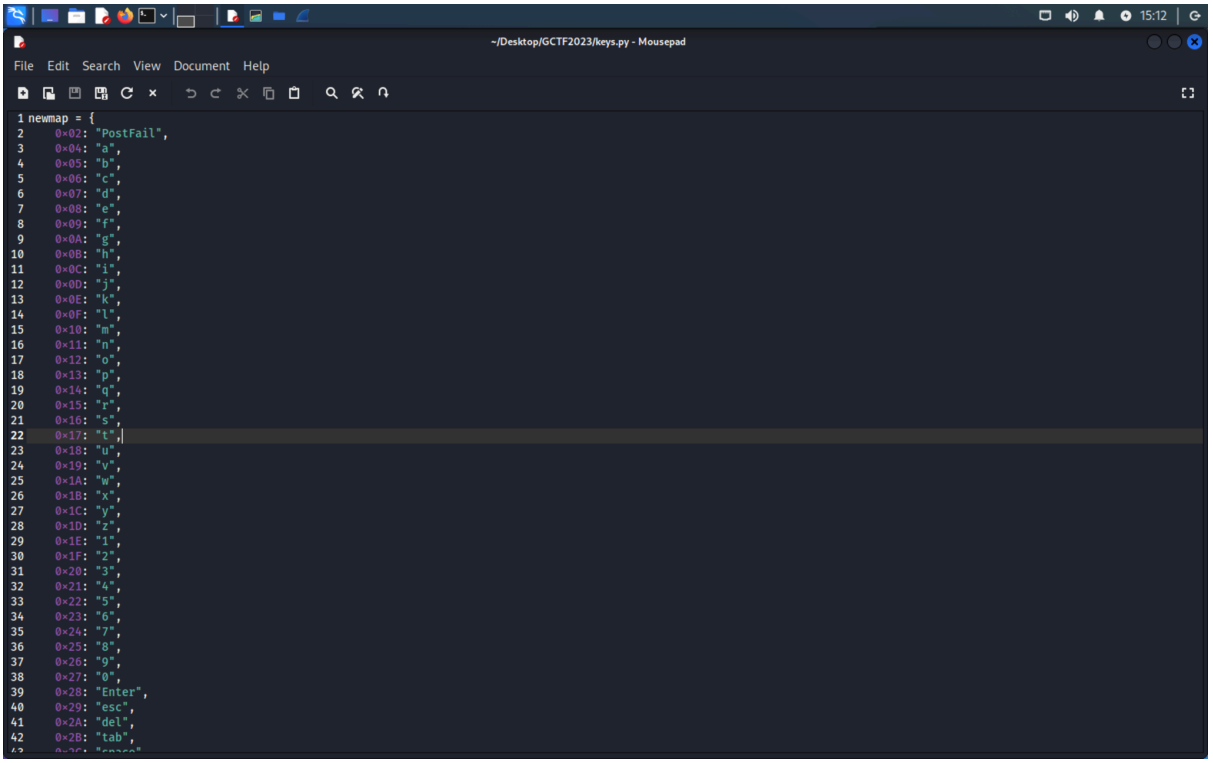
This is how the data looks like in the csv file.

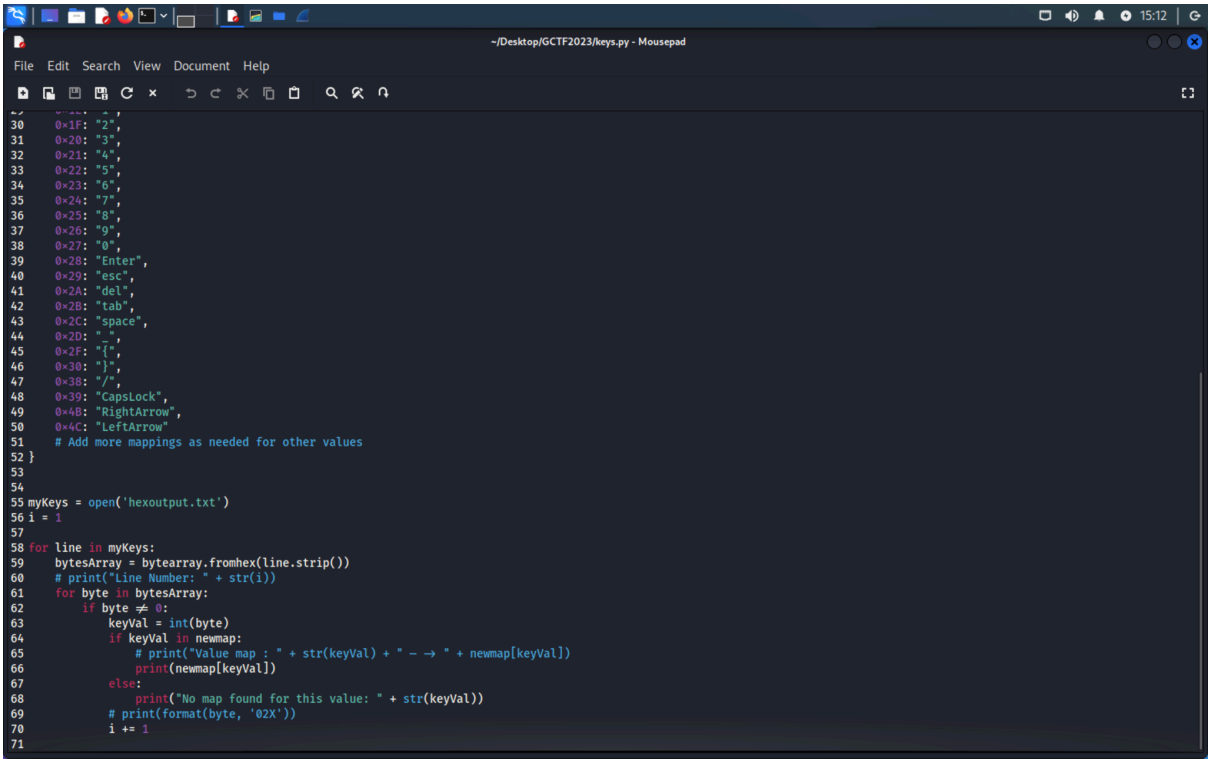


To save the Leftover Capture Data only, into an another txt file (hexoutput.txt) automatically, I use this command:

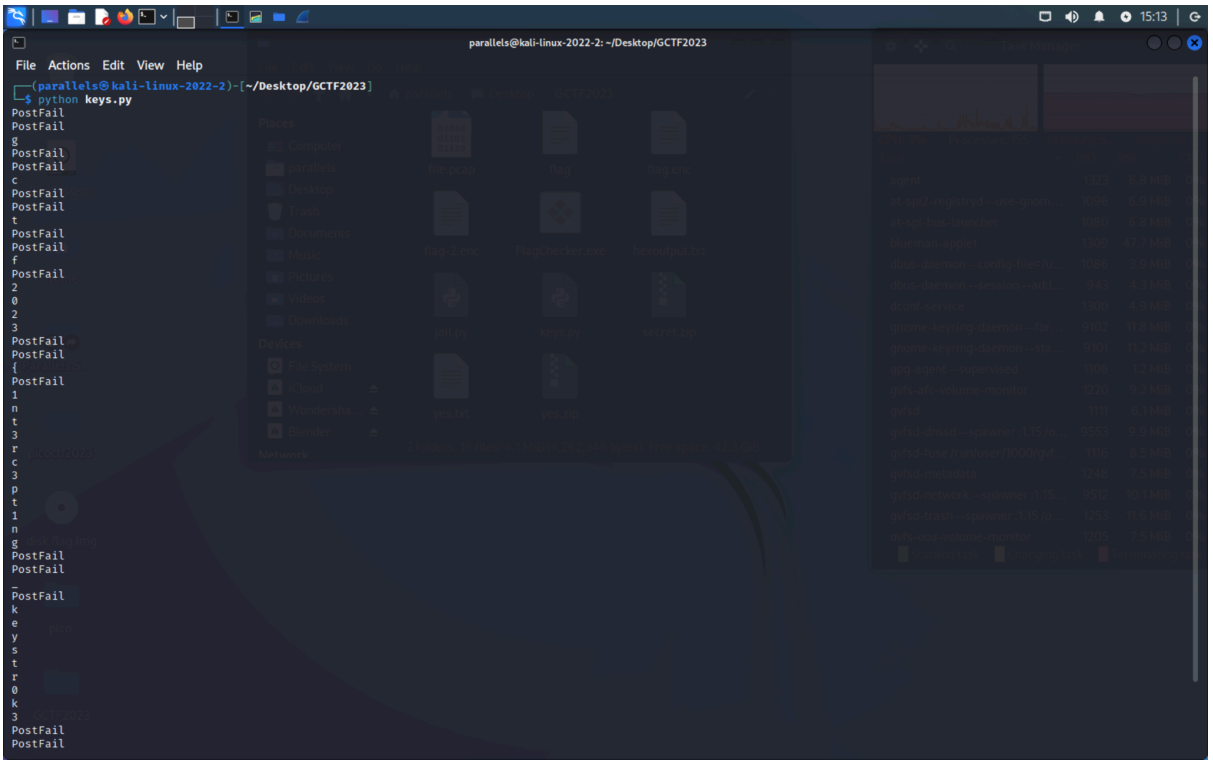
cat challenge.csv | cut -d ',' -f 7 | cut -d '"' -f 2 | grep -vE "Leftover Capture Data" > hexoutput.txt

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





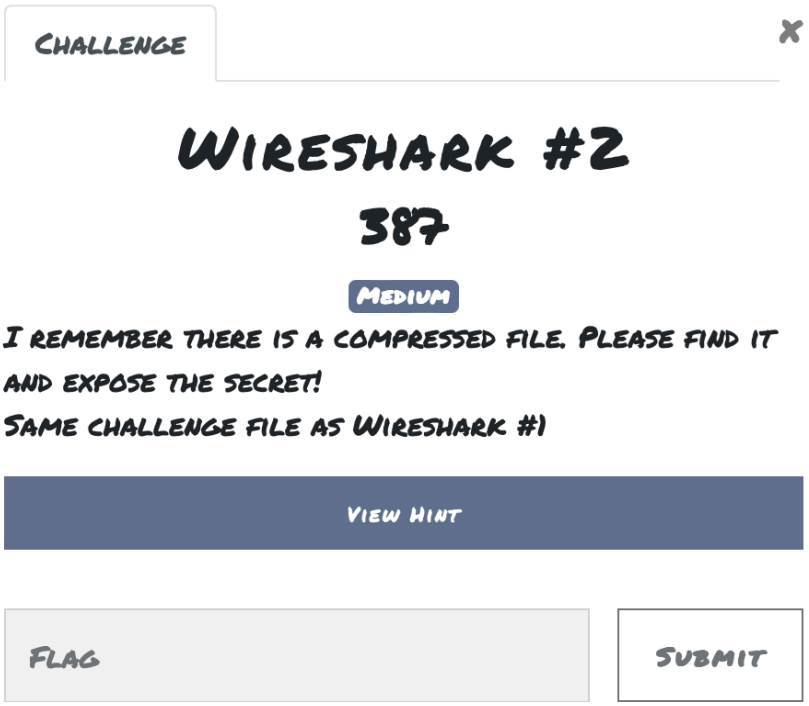
This is the python code that I used to convert the hexoutput.txt into a readable or ASCII character.

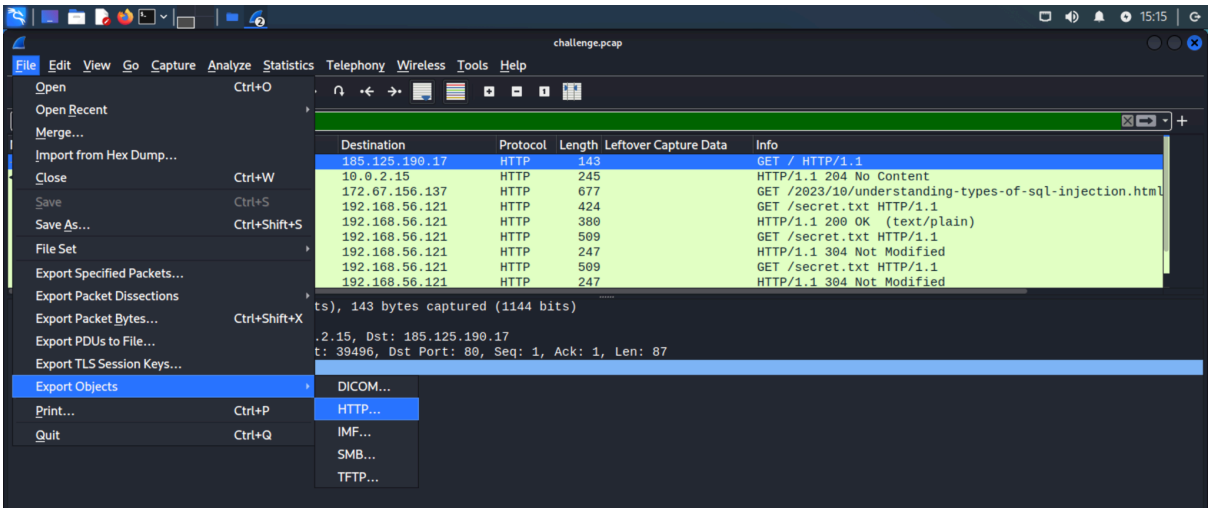


This is the output from hexouput.txt after I run the python code.
After I type all the characters manually, I got the flag:

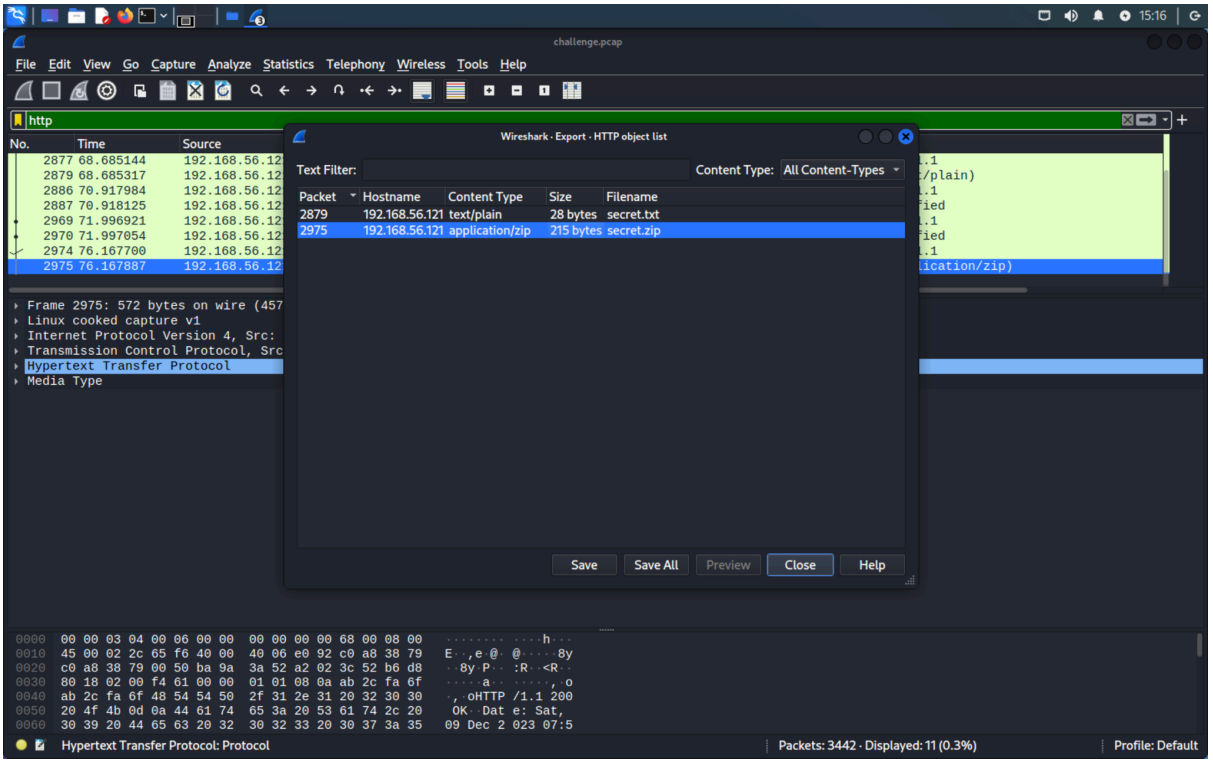
GCTF2023{1nt3c3pt1ng_keystr0k3}

WIRESHARK #2

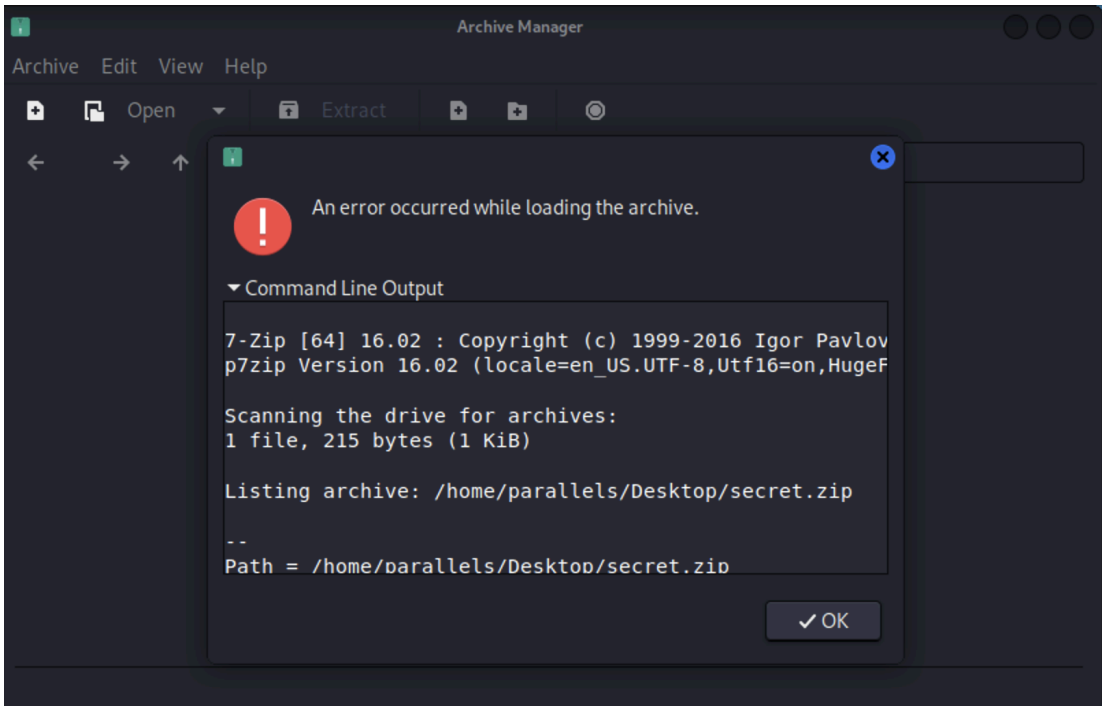




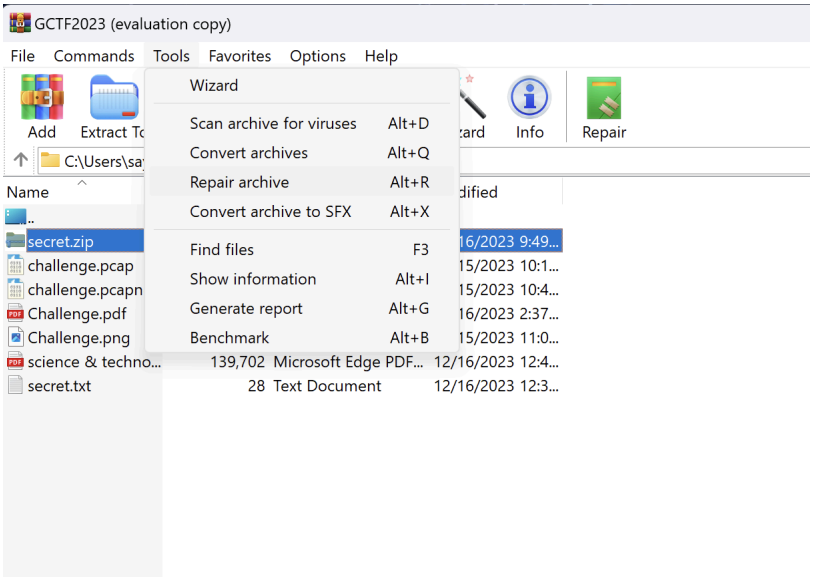
As this is a continuation from challenge Wireshark #1, I am using the same pcap file, then I clicked export objects and clicked http to export the secret.zip file.



As shown above, I exported the file.



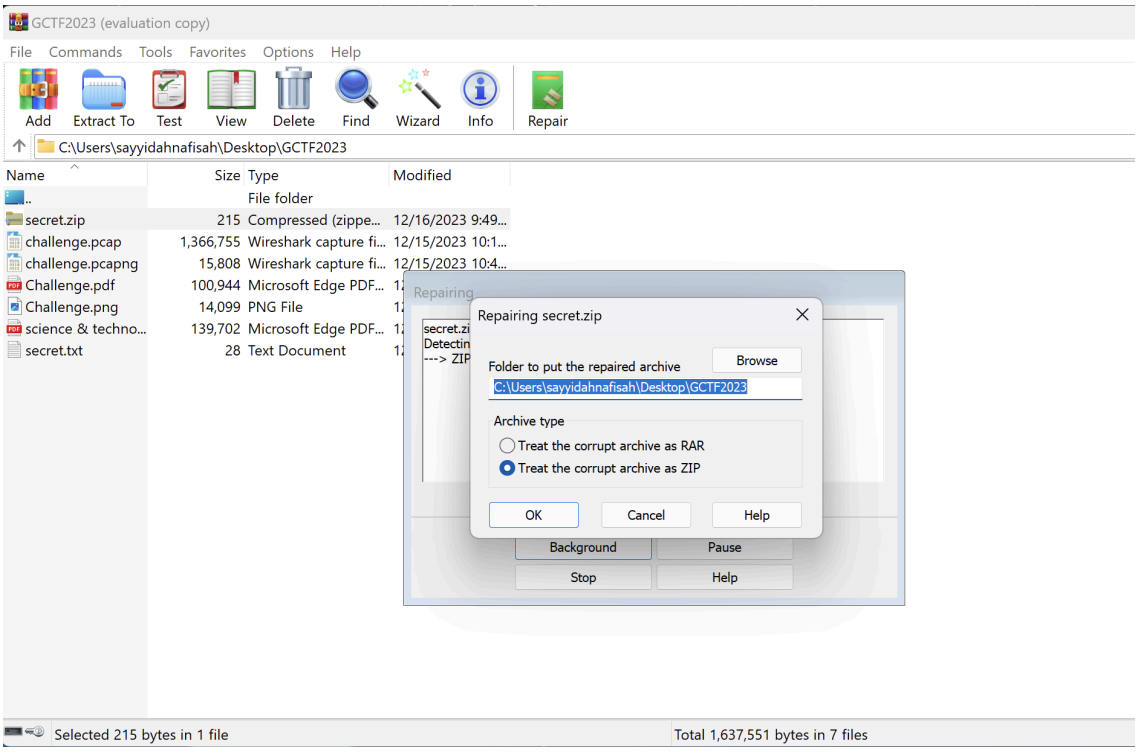
However, the zip file is corrupted and I couldn't opened the file.



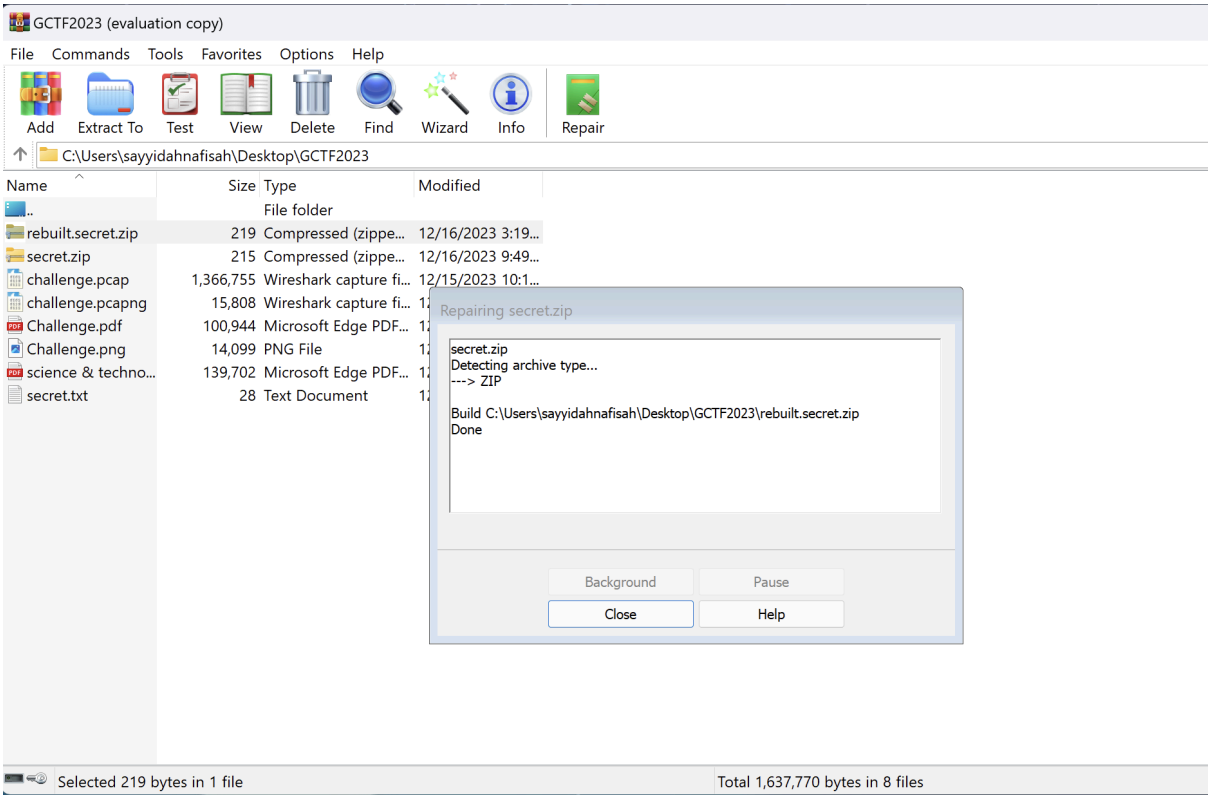
Then I used Win-rar apps to fix the zip file.

The steps to fix the file:

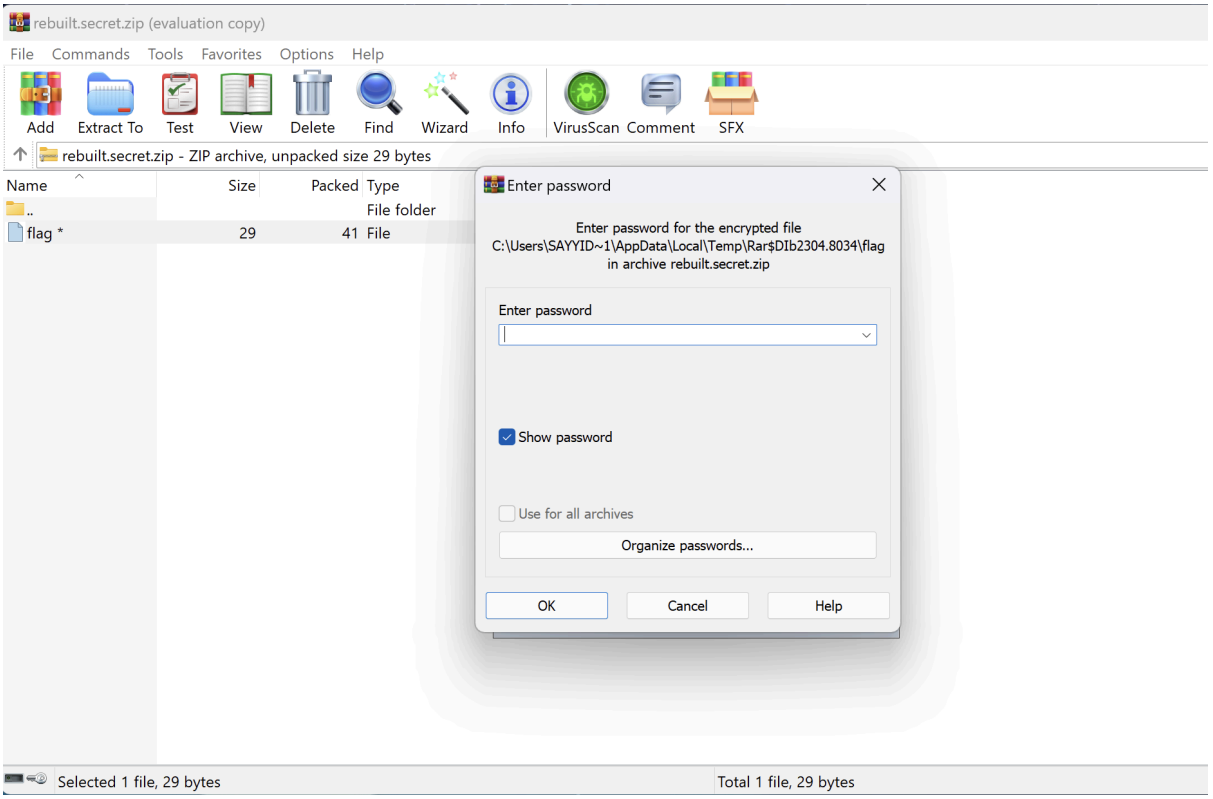
1. select secret.zip file
2. click Repair archive



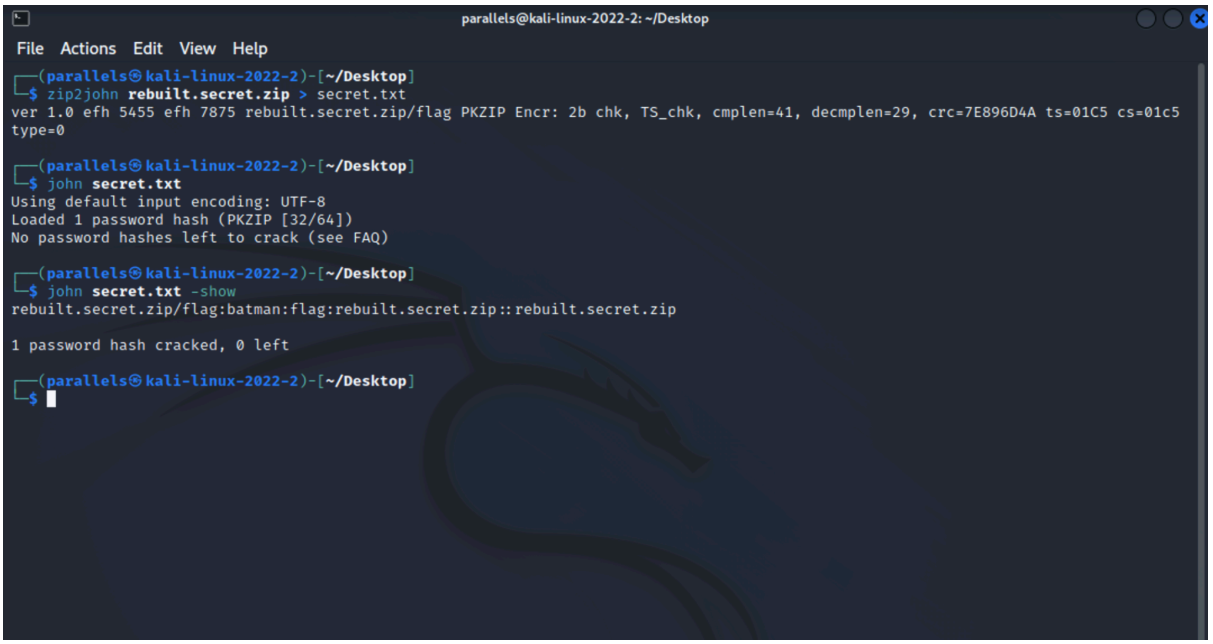
3. Click OK



4. Click close



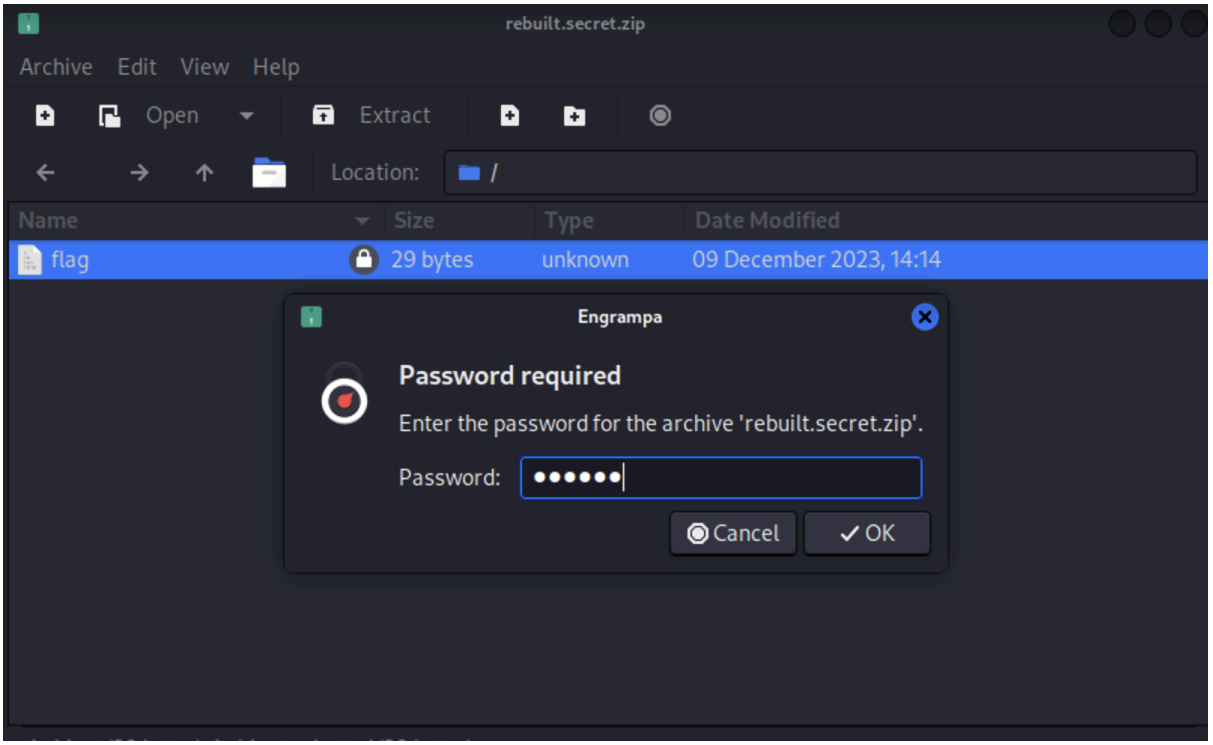
5. The file is successfully repaired but we are still not done yet because the file is protected by password.



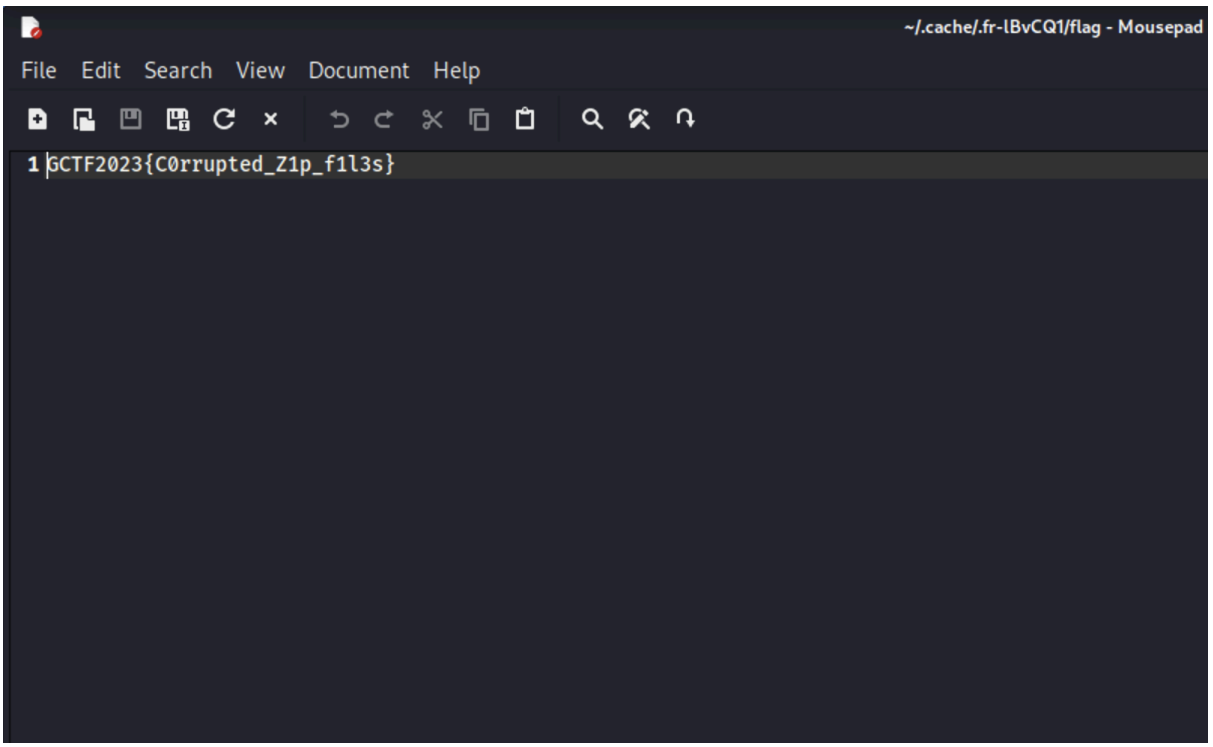
To crack the password, I referred to this video:
https://www.youtube.com/watch?v=yyIoX0QT6QM
I cracked it using John the ripper.

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}