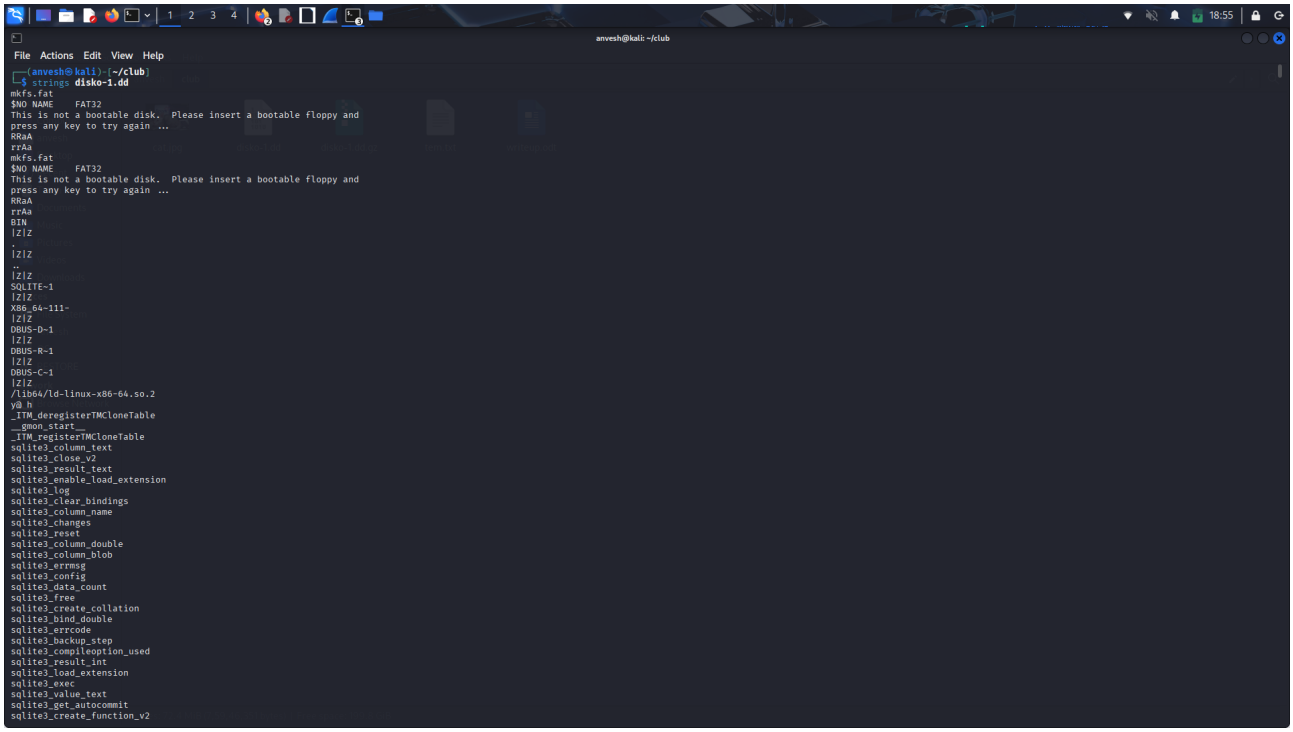
Name:-Yerram Setty Gowri Anvesh
discord_id:-anvesh_potterhead
Branch: S2-CYS

WRITEUP-CRYPTO HACK

EASY :

1. DISCO 1:

First i downloaded the disco1.gz and extarcted it to the work folder. Now inside the disco1 tthere is another file disco1.dd . I used strings disco1.dd



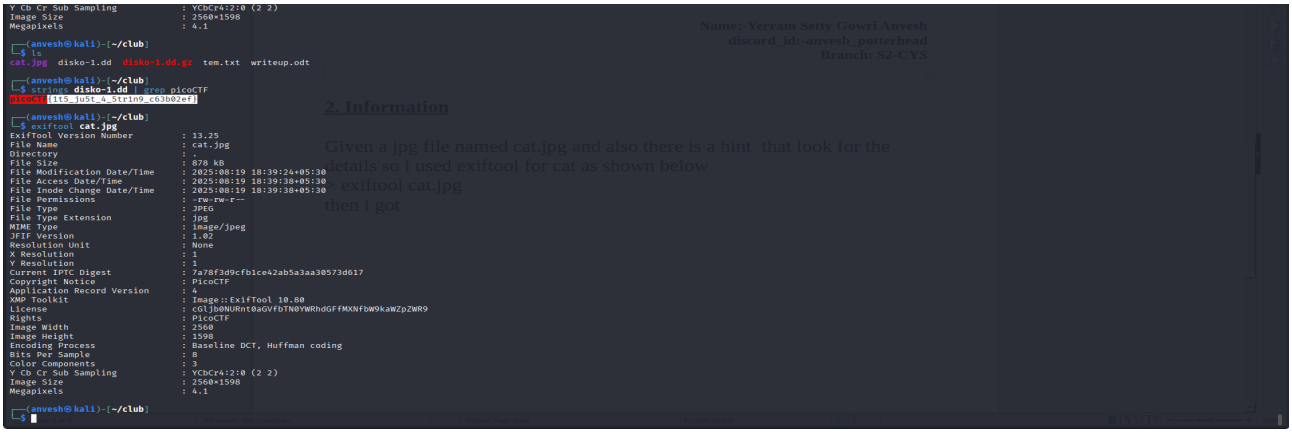
We know that it will always starts with picoCTF{ so i used grep command piped to strings then i got the flag as

The flag is
picoCTF{1t5_ju5t_4_5tr1n9_c63b02ef}

Name:-Yerram Setty Gowri Anvesh
discord_id:-anvesh_potterhead
Branch: S2-CYS

2. Information

Given a jpg file named cat.jpg and also there is a hint that look for the details so i used exiftool for cat as shown below
> exiftool cat.jpg
then i got



Here everything is ok but this license is something doubt ful so i used base64 to decode it
when i decode it i got the flag

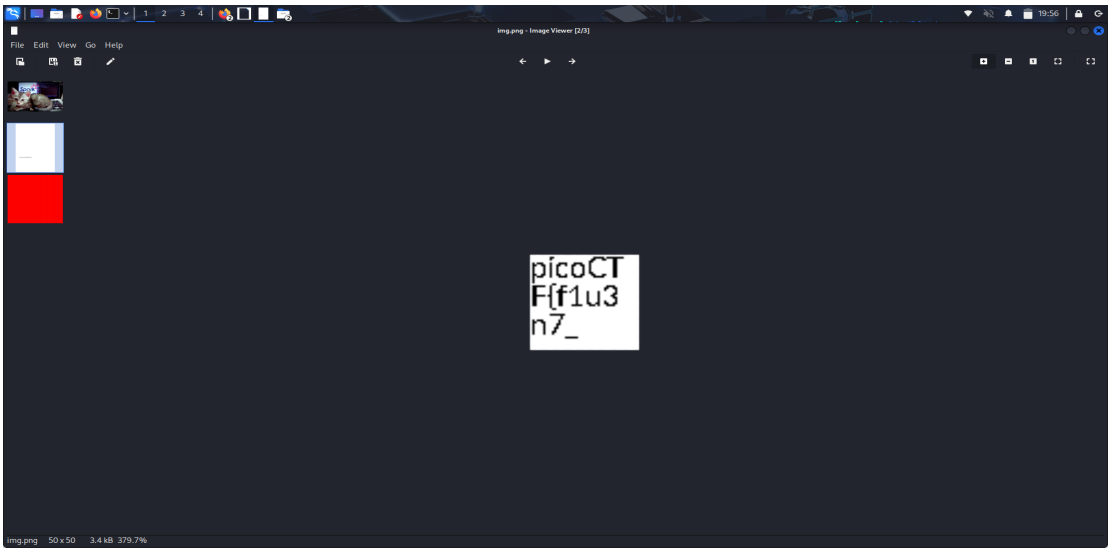
The flag is picoCTF{the_m3tadata_1s_modified}

Name:-Yerram Setty Gowri Anvesh
discord_id:-anvesh_potterhead
Branch: S2-CYS

3. Secret of polyglot :

I downloaded the file and opened it but there is something like 1n_pn9_&_pdf_53b741d6} lets note it aside it may be useful because it ends with "}" and also the given that we need to change type of the file, so i opened the terminal and used file command to see the type of it
>file flag2of2-final
then i got it as png

so i changed that using
>mv flag2of2-final.pdf img.png



and opened the image, now i got half of it may be the other half of it is the above one so, the flag is picoCTF{f1u3n7_1n_pn9_&_pdf_53b741d6}

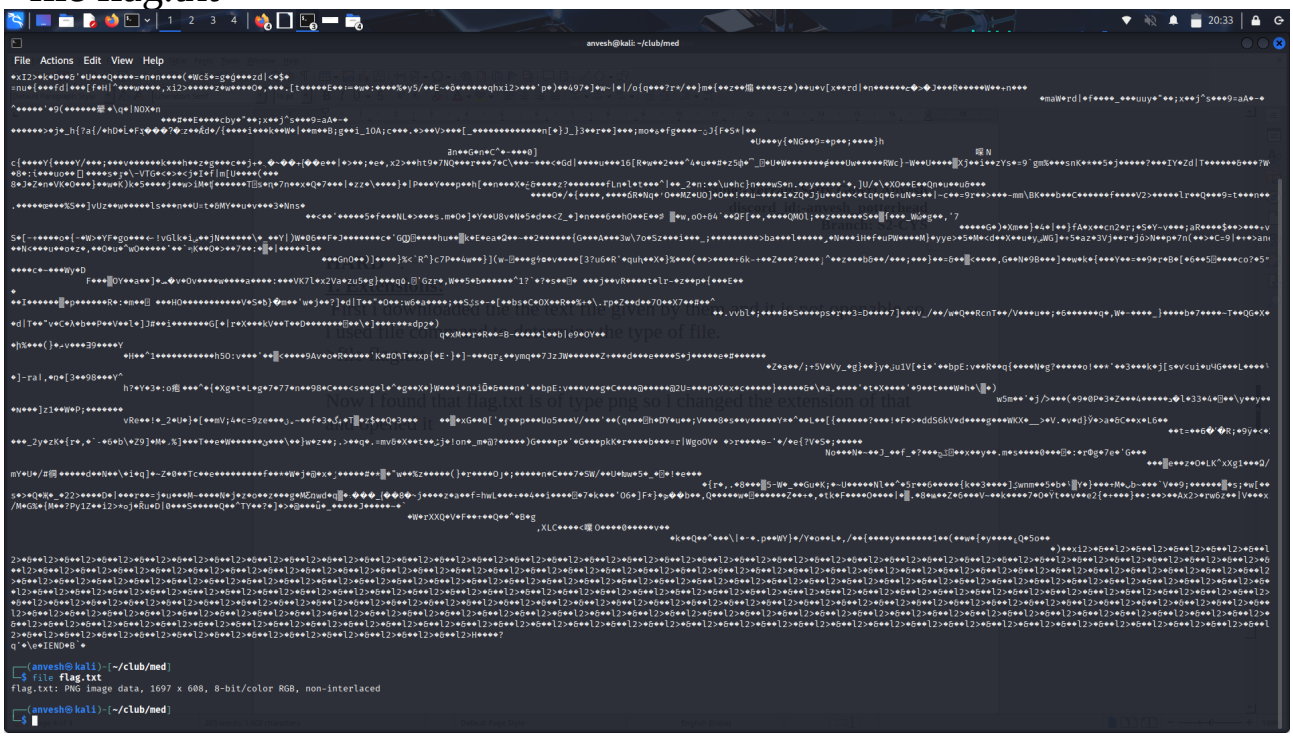
Name:-Yerram Setty Gowri Anvesh
discord_id:-anvesh_potterhead
Branch: S2-CYS

MEDIUM :

1. Extensions:

First i downloaded the the text file given by them and it is not openable so i used file command to determine the type of file.

>file flag.txt



Now i found that flag.txt is of type png so i changed the extension of that and opened it

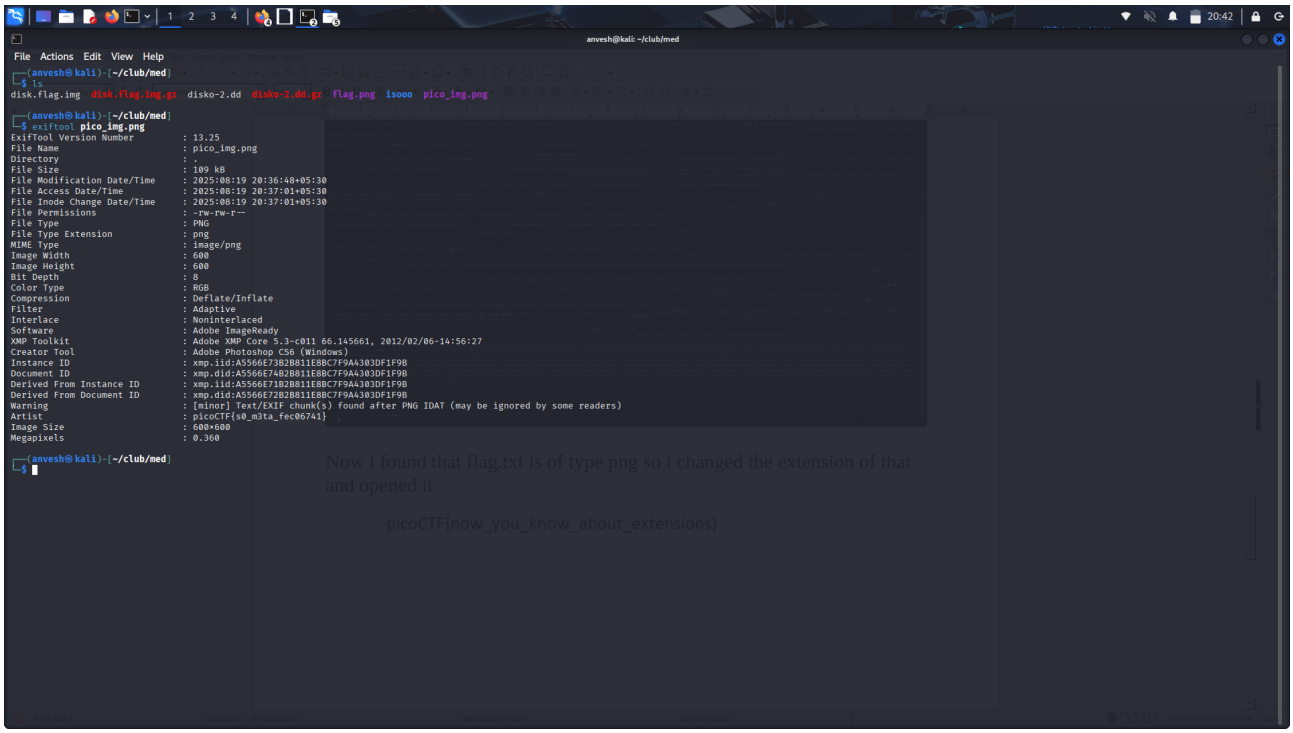
picoCTF{now_you_know_about_extensions}

Now i the flag in that image
the flag is : picoCTF{now_you_know_about_extensions}

Name:-Yerram Setty Gowri Anvesh
discord_id:-anvesh_potterhead
Branch: S2-CYS

2. So Meta:

First i downloaded the png file and there is a hint something about metadata so i used exiftool



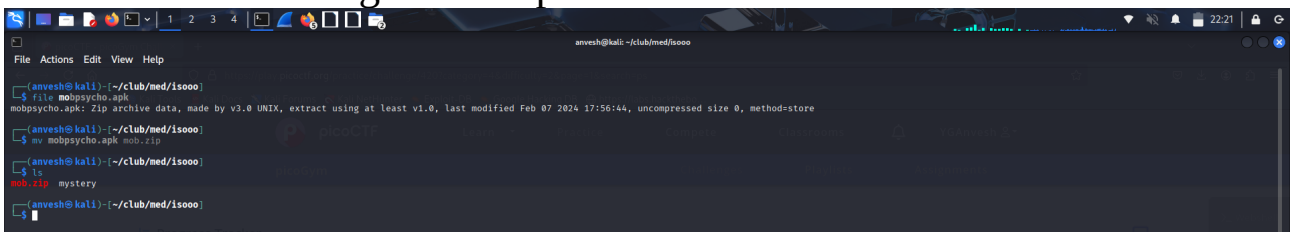
At artist i got the flag directly

The flag is picoCTF{s0_m3ta_fec06741}

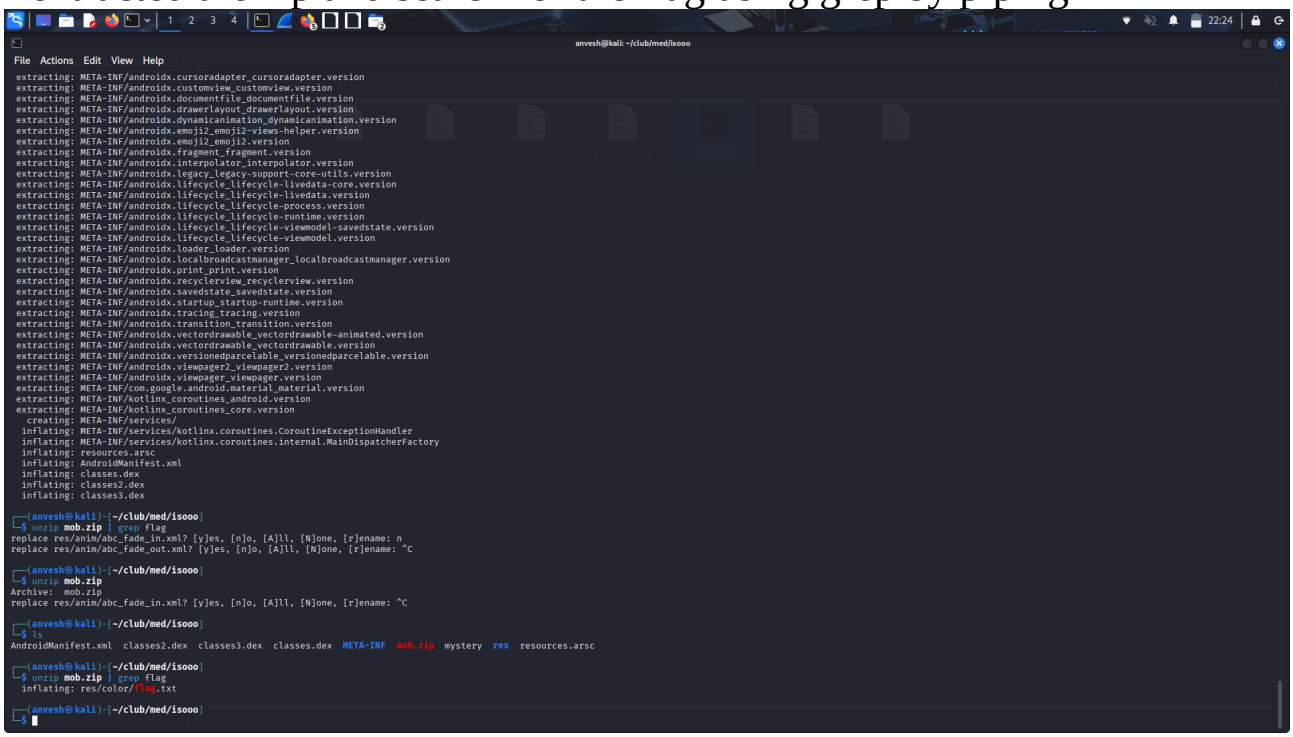
2. Mob Psycho:

Name:-Yerram Setty Gowri Anvesh
discord_id:-anvesh_potterhead
Branch: S2-CYS

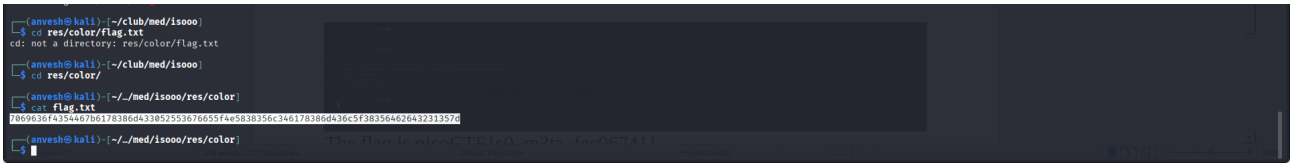
First i downloaded the apk file given in the website now i checked it with file command then i got it as zip



I extracted the zip and search for the flag using grep by piping

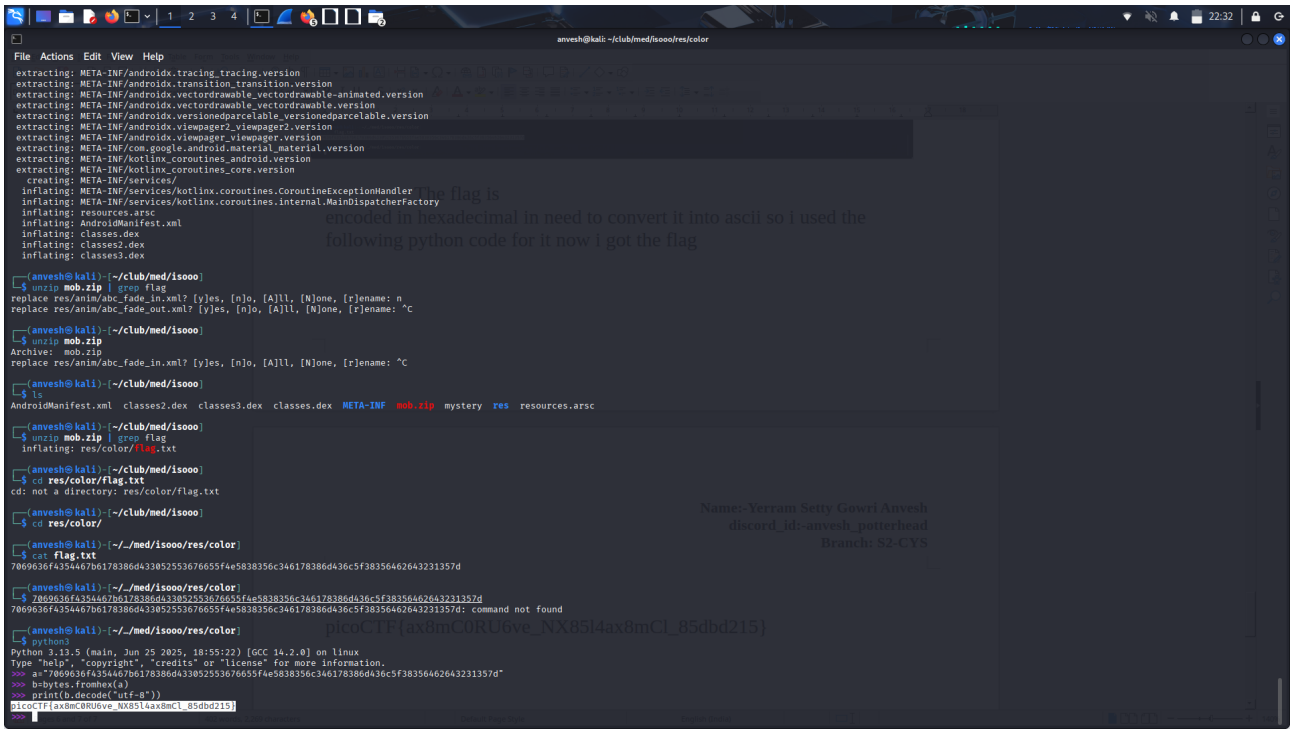


Now i got the location of the flag



The flag is encoded in hexadecimal in need to convert it into ascii so i used the following python code for it now i got the flag

Name:-Yerram Setty Gowri Anvesh
discord_id:-anvesh_potterhead
Branch: S2-CYS



picoCTF{ax8mC0RU6ve_NX85l4ax8mCl_85dbd215}

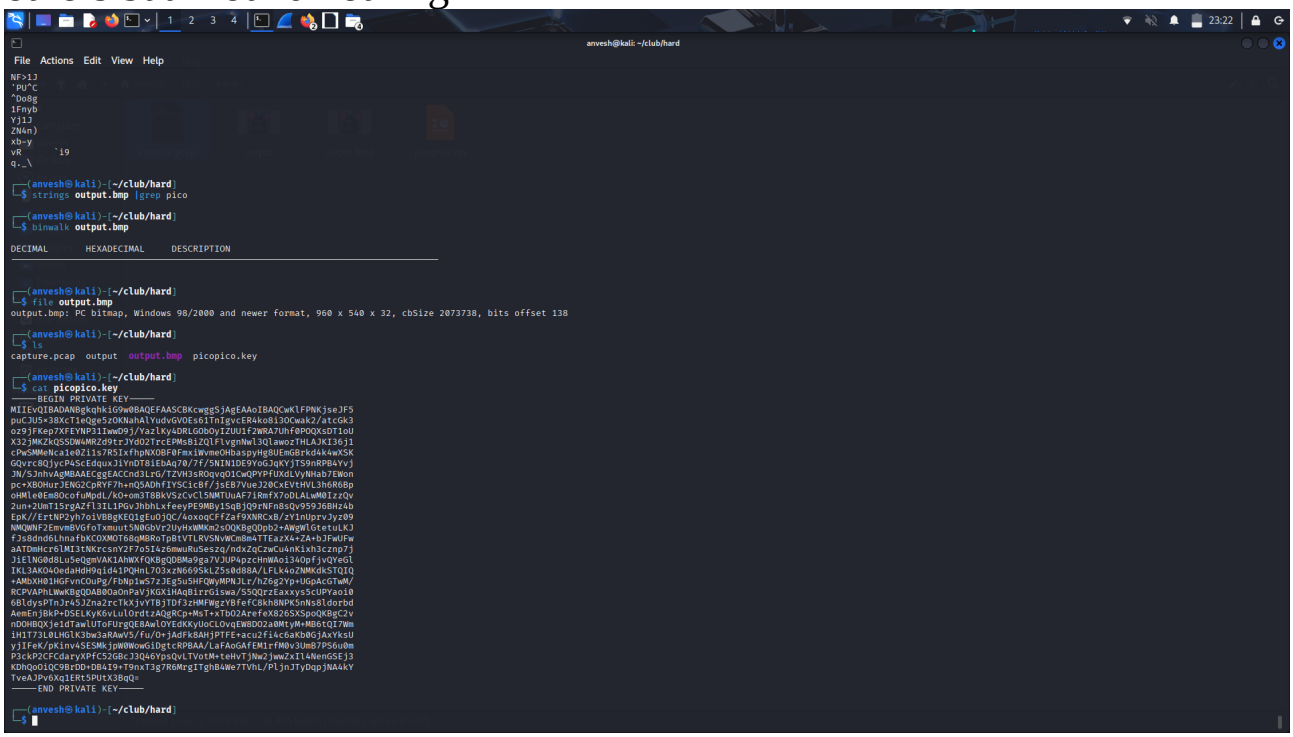
Name:-Yerram Setty Gowri Anvesh
discord_id:-anvesh_potterhead
Branch: S2-CYS

HARD :

1. Webnet 0:

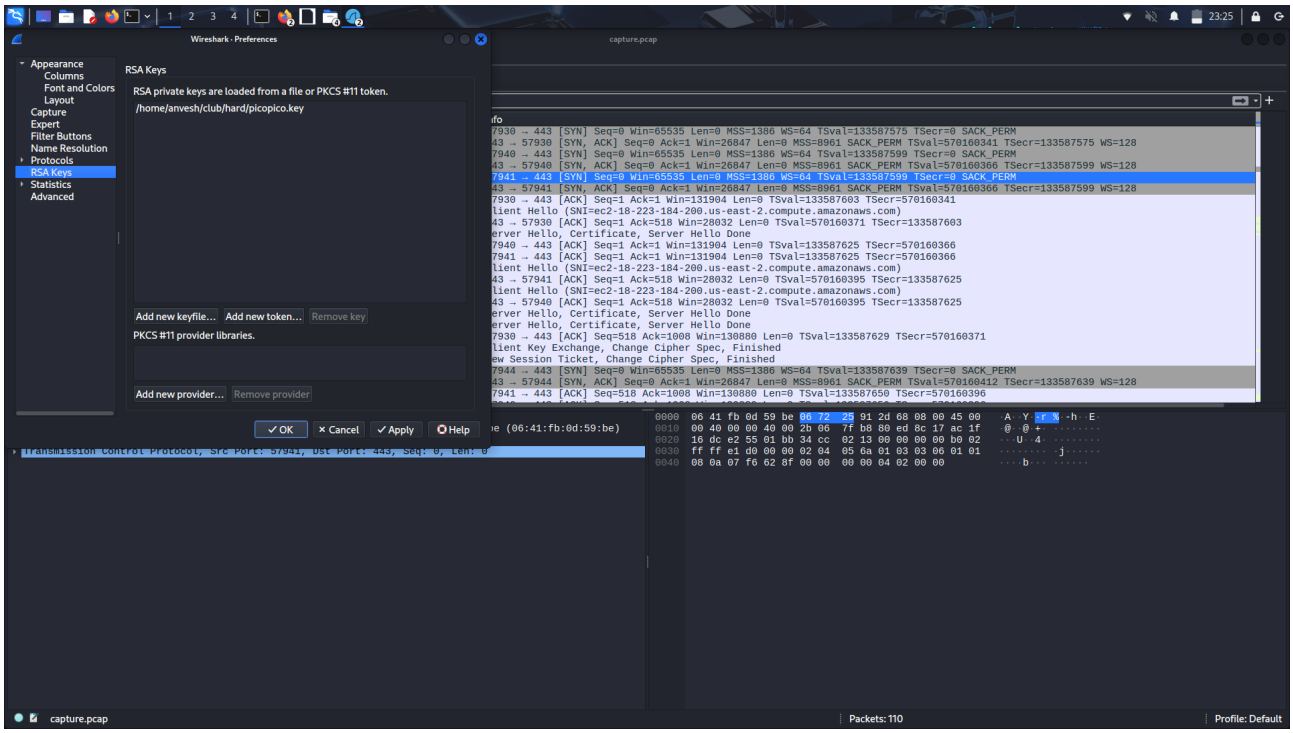
First they given us a packet file and a key file when i opened the key file it was something like private rsa key

Now i opened the packet file in wireshark and there i used search and others but i found nothing

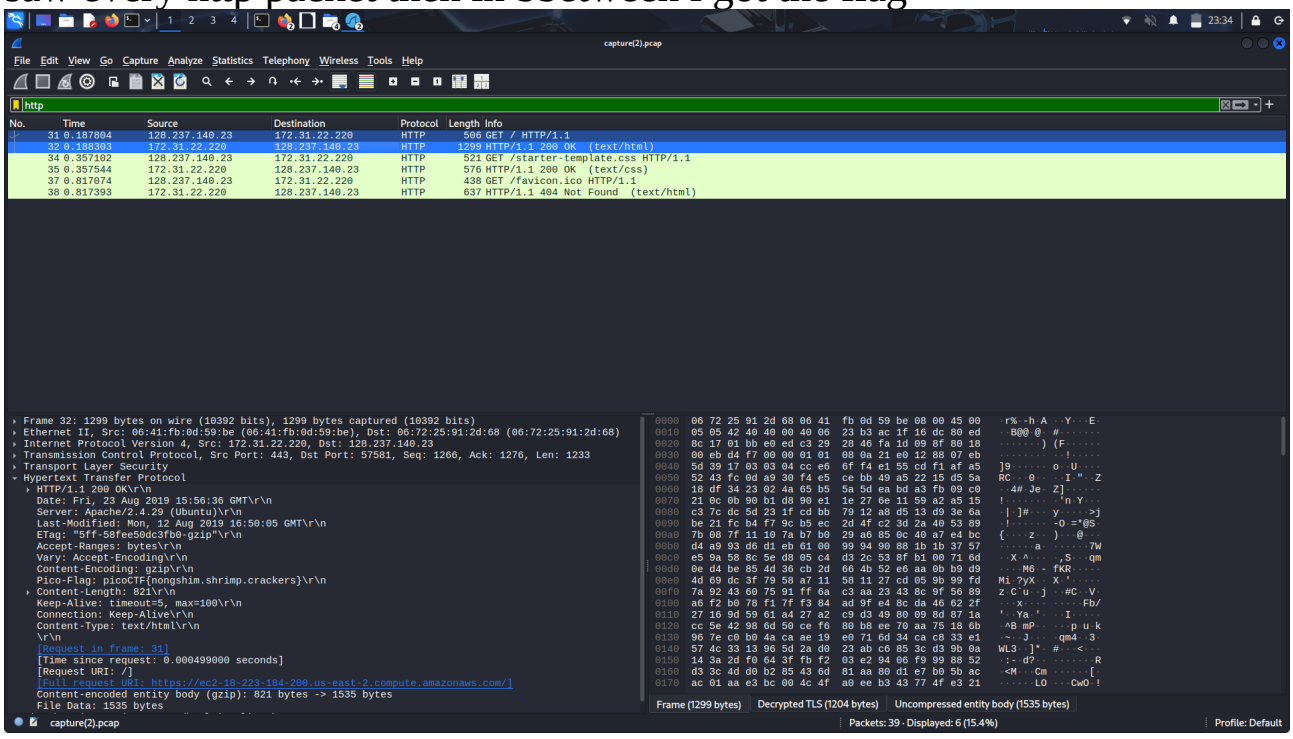


after remembering that they given me the private key i added the private key i preferences by (ctrl +shift +p) then there at rsa key i added the rsa key given

Name:-Yerram Setty Gowri Anvesh
discord_id:-anvesh_potterhead
Branch: S2-CYS



after adding the rsa key i closed it and opened it again this time i got to see some unencrypted http protocol transmissions so used filter set to http and saw every http packet then in bbetween i got the flag



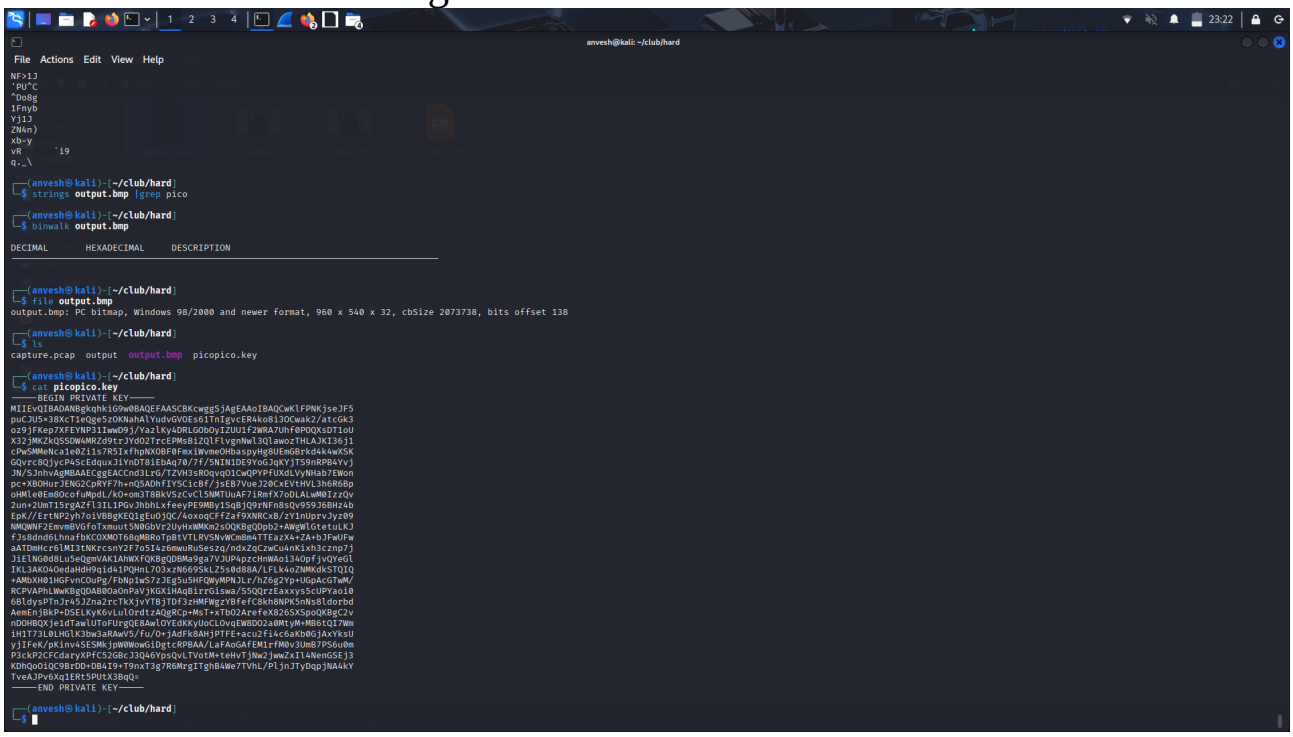
The flag is Pico-Flag:Pico-Flag: picoCTF{nongshim.shrimp.crackers}

Name:-Yerram Setty Gowri Anvesh
discord_id:-anvesh_potterhead
Branch: S2-CYS

2. Webnet 1:

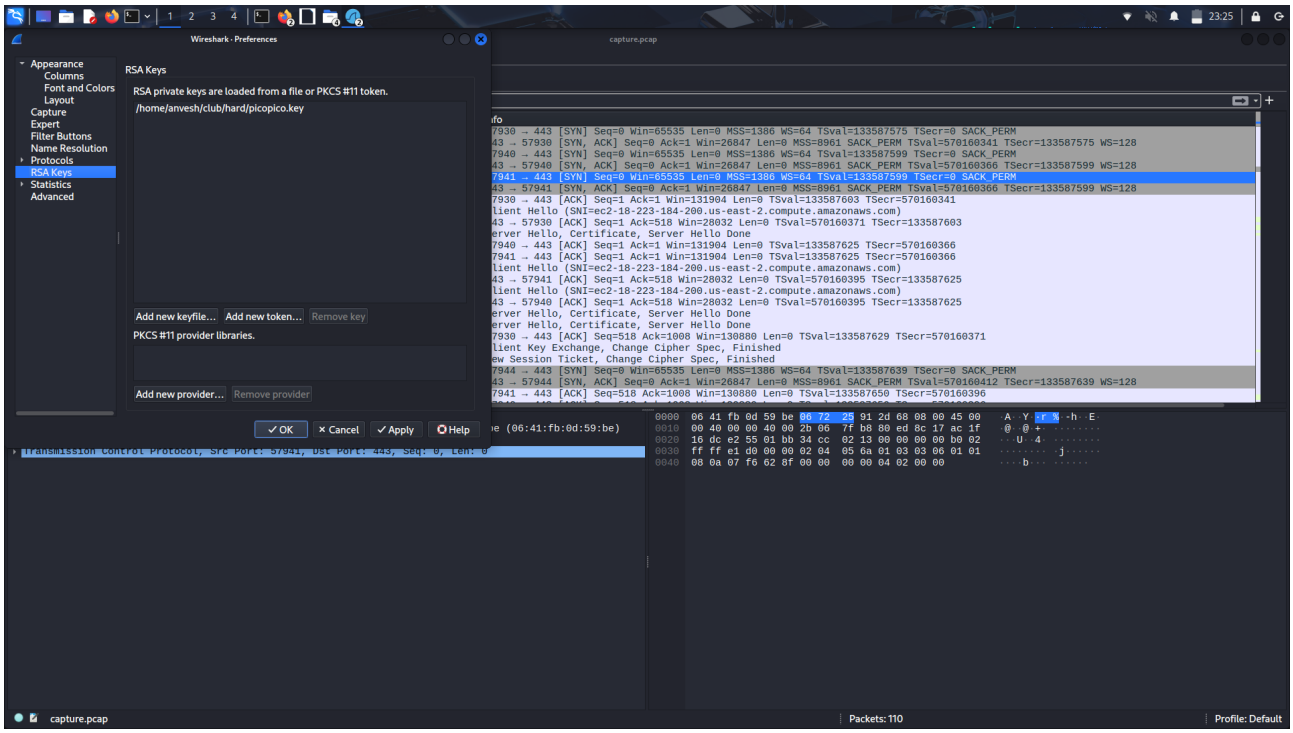
This is same as before they given us a packet file and a key file when i opened the key file it was something like private rsa key which is same as before

Now i opened the packet file in wireshark and there i used search and others but i found nothing

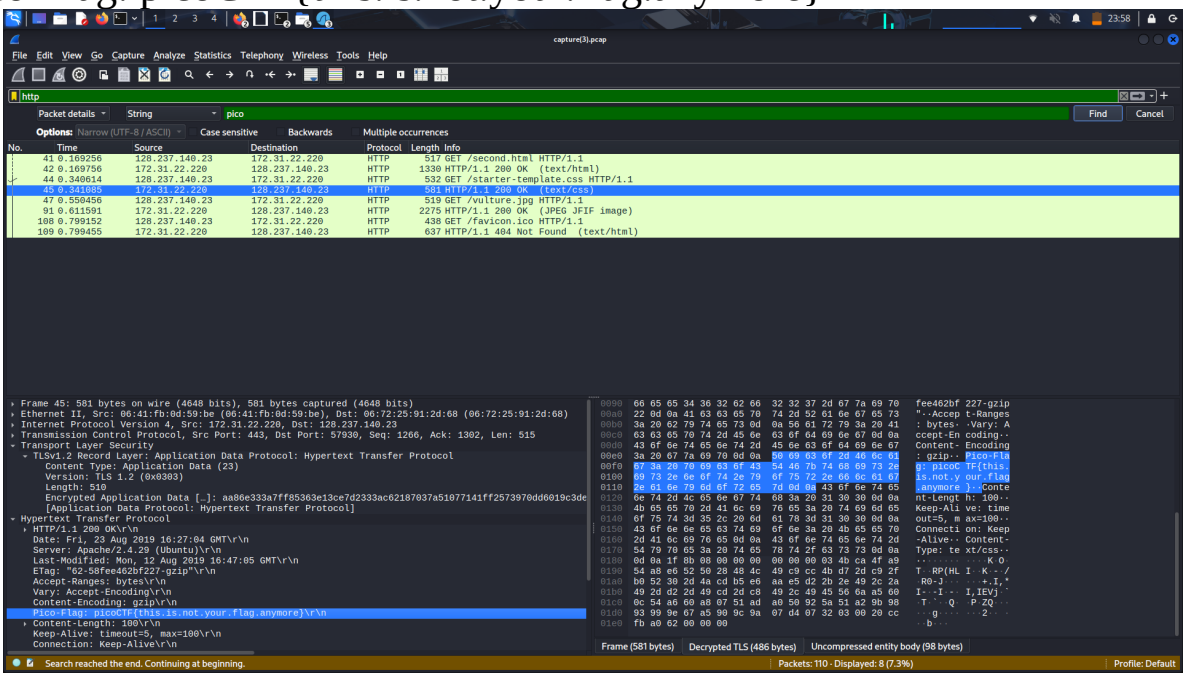


after remembering that they given me the private key i added the private key i preferences by (ctrl +shift +p) then there at rsa key i added the rsa key given

Name:-Yerram Setty Gowri Anvesh
discord_id:-anvesh_potterhead
Branch: S2-CYS

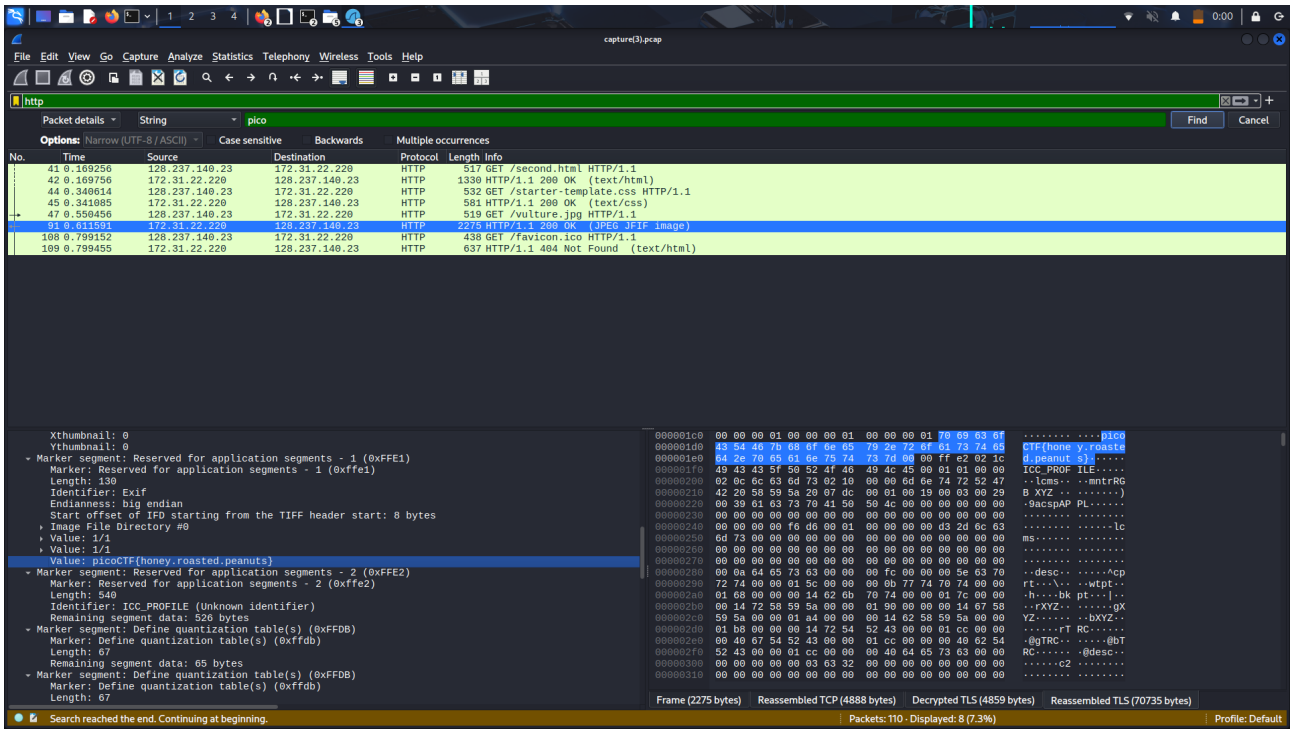


after adding the rsa key i closed it and opened it again this time i got to see some unencrypted http protocol transmissions so used filter set to http and saw every http packet then at first i got a decoy flag
Pico-Flag: picoCTF{this.is.not.your.flag.anymore}



Name:-Yerram Setty Gowri Anvesh
discord_id:-anvesh_potterhead
Branch: S2-CYS

Now I searched deeply at every packet in wireshark then i found the original flag at jpg format



picoCTF{honey.roasted.peanuts}

The hard level is so goated that i can't even getting any idea that what i need to do so, i did upto here only .....,