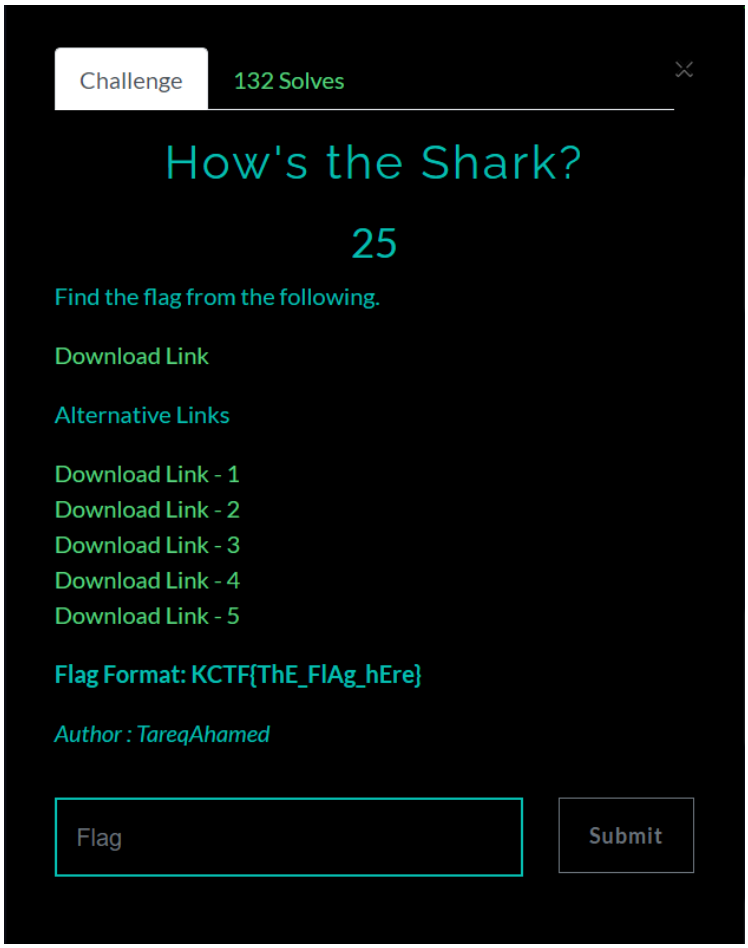
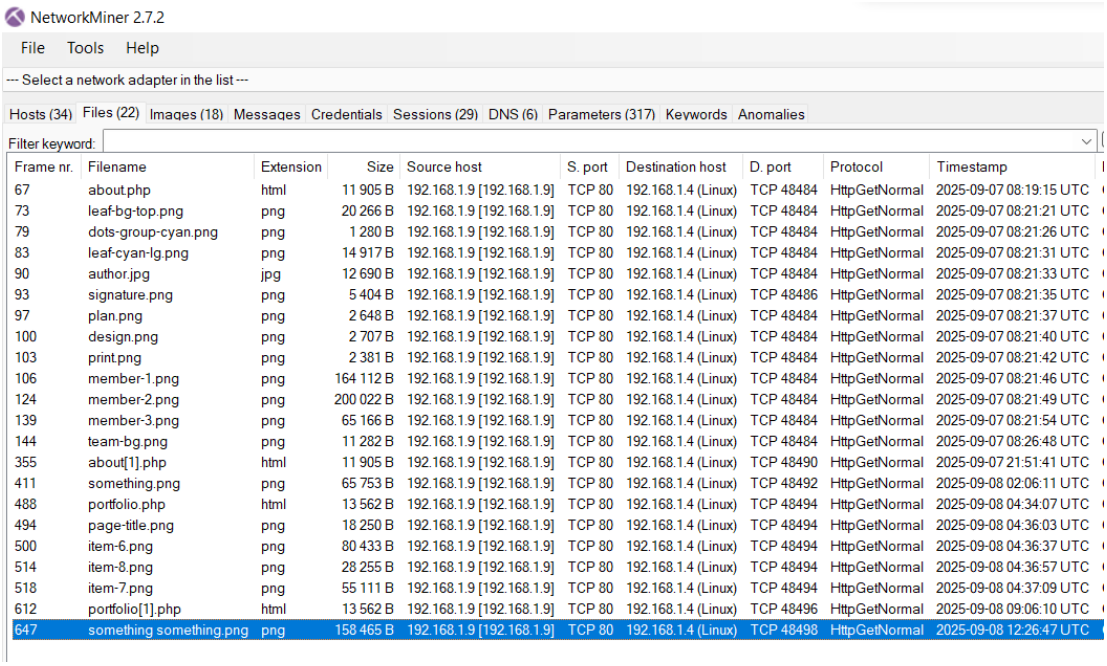
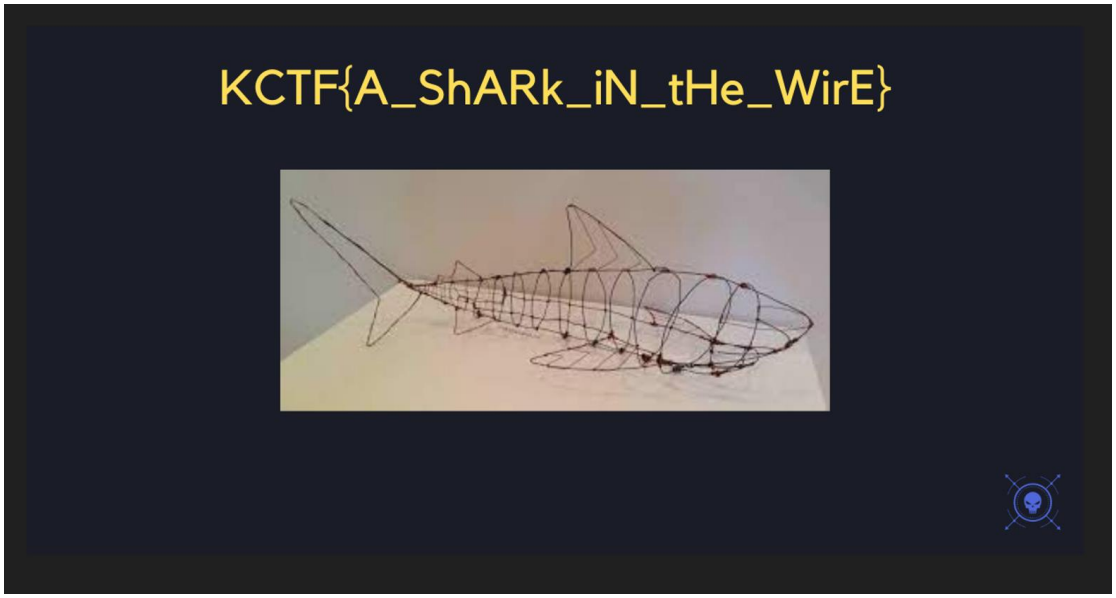
How’s the Shark (Networking):

Given pcap file is downloaded and analyzed for the flag.



I used network miner to open pcap file and checked for the files transferred over the network and that’s where our flag was.

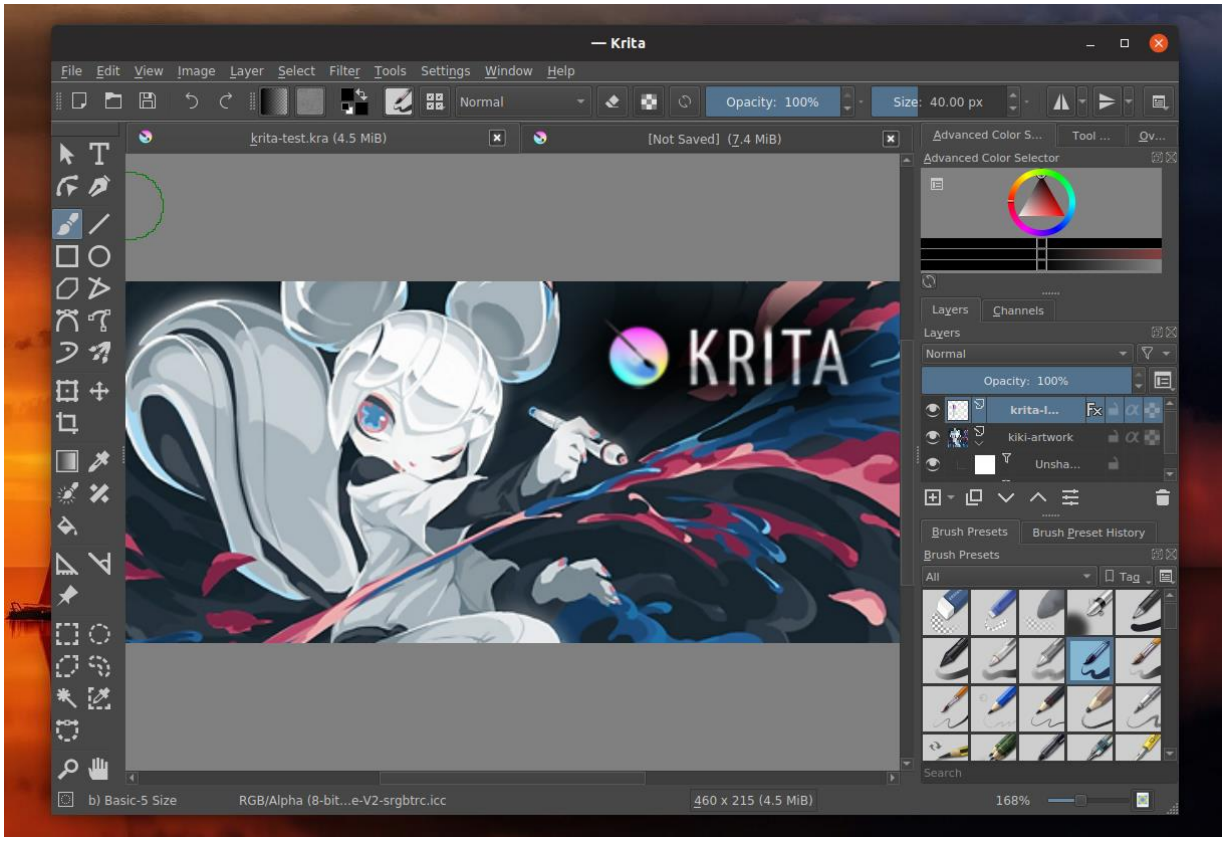




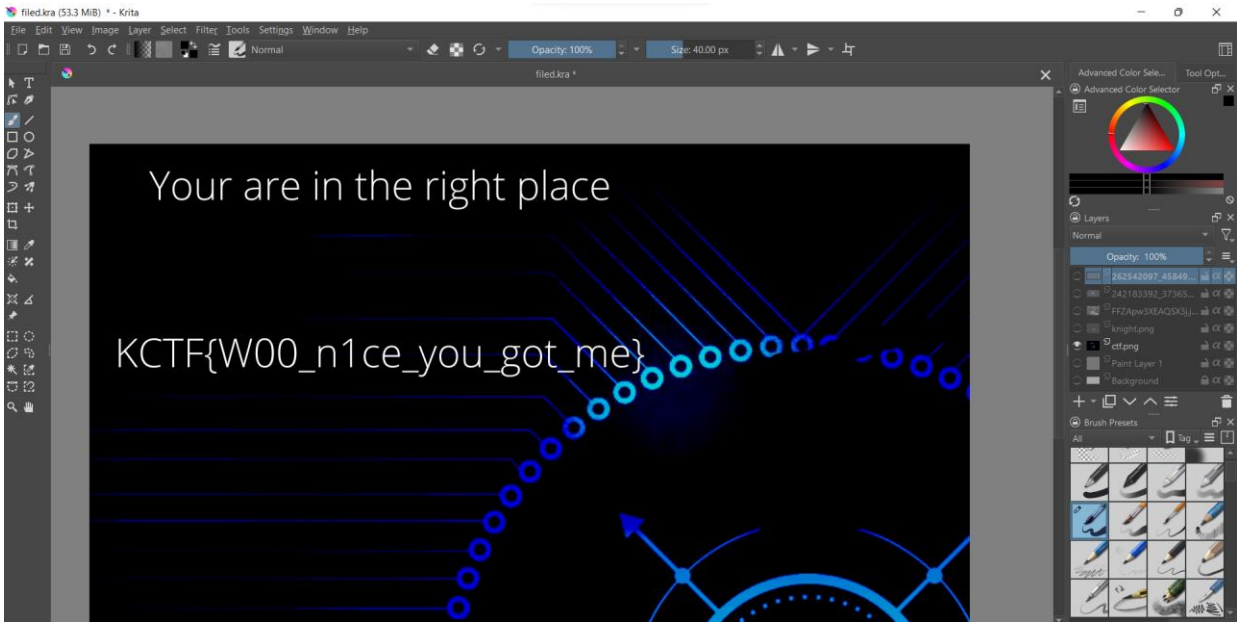
FileD (Steganography):

Given file was a **.kra** extension which was totally new to me and googled it for more details that gave me an idea about the extension and the software which uses it.

The software which uses **.kra** extension is **krita** an open source editing software.

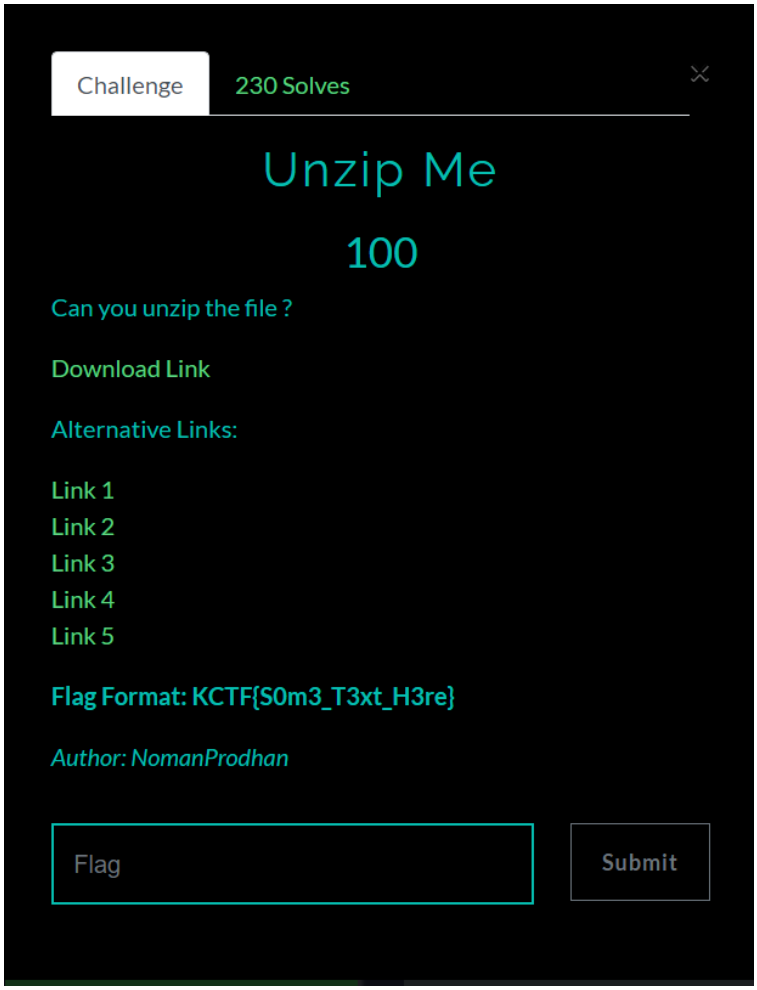


On opening the file using krita got to know the file is a blended image project file with help of many images, by turning off each layers of image finally got the flag.

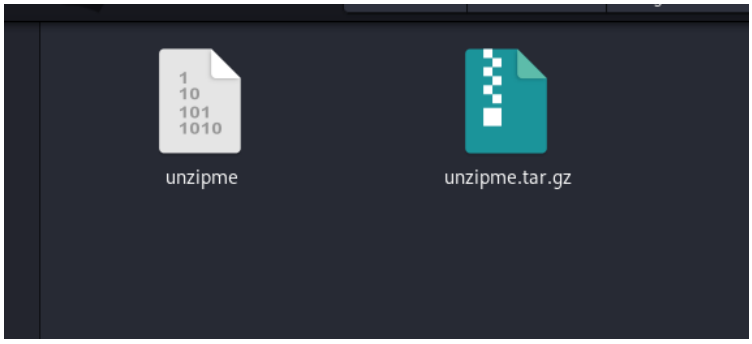


Unzip Me (Misc):

Given file was a **.tar.gz** file which is just an extension for archive file it's basically a zipped file, which can be unzipped as like any other zip file.



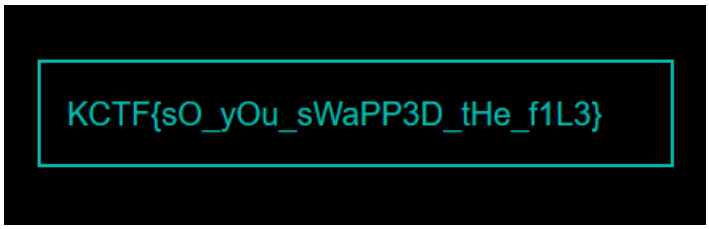
Unzipped file gave out a file with no extension.



So I checked for the file type using **file** command in linux that gave me the file type as **data**. As data files can be printed using **cat** command. Using cat command on the file gave out the flag we need but in a jumbled way, but was easy to unscramble it.

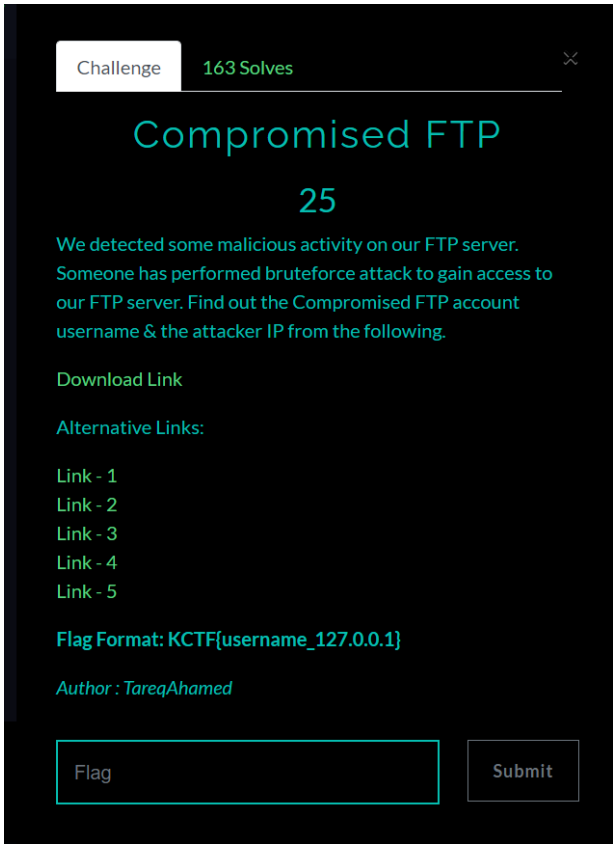
```
┌──(toor㉿N051N)-[~/Downloads]
└─$ file unzipme
unzipme: data

┌──(toor㉿N051N)-[~/Downloads]
└─$ cat unzipme
KP@T,|@6lfgat.txCKFTs{_OOy_uWsPa3P_DHt_e1f3L
}KP?@T,|@6@@lfgat.txKP6D

┌──(toor㉿N051N)-[~/Downloads]
└─$ strings unzipme
lfgat.txCKFTs{_OOy_uWsPa3P_DHt_e1f3L
lfgat.txKP
```

Our final flag after unscrambling looked like this.



Compromised FTP (Digital Forensics):

Given file was a network log with timestamp, IP addresses, FTP usernames and PIDs.



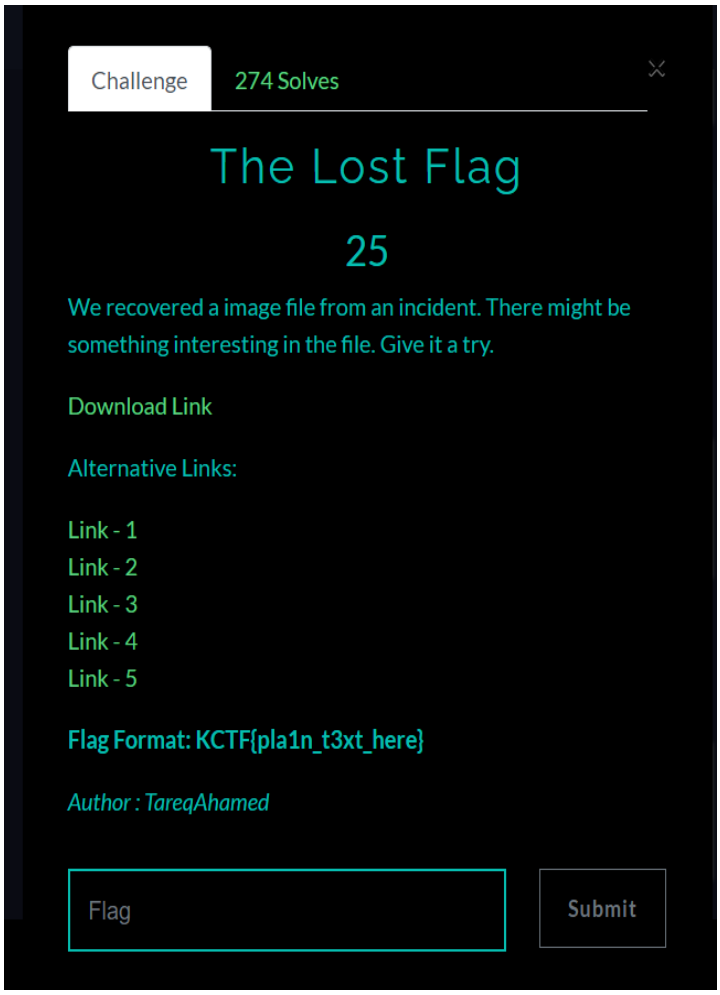
I just noticed that all the IP are the same, So that made my work half done as the flag is a combo of username and IP address. Now I just focused on finding the username then I came up with the idea of bruteforcing usernames.

```
Mon Jan  3 15:24:05 2022 [pid 5365] [uploader] FAIL LOGIN: Client "::ffff:192.168.1.7"
Mon Jan  3 15:24:05 2022 [pid 5367] [ftpuser] FAIL LOGIN: Client "::ffff:192.168.1.7"
Mon Jan  3 15:24:05 2022 [pid 5386] CONNECT: Client "::ffff:192.168.1.7"
Mon Jan  3 15:24:05 2022 [pid 5388] CONNECT: Client "::ffff:192.168.1.7"
Mon Jan  3 15:24:06 2022 [pid 5363] [ftpuser] FAIL LOGIN: Client "::ffff:192.168.1.7"
Mon Jan  3 15:24:06 2022 [pid 5381] [ftpuser] FAIL LOGIN: Client "::ffff:192.168.1.7"
Mon Jan  3 15:24:06 2022 [pid 5383] [ftpuser] FAIL LOGIN: Client "::ffff:192.168.1.7"
Mon Jan  3 15:24:07 2022 [pid 5357] [ftpuser] FAIL LOGIN: Client "::ffff:192.168.1.7"
Mon Jan  3 15:24:07 2022 [pid 5369] [ftpuser] FAIL LOGIN: Client "::ffff:192.168.1.7"
Mon Jan  3 15:24:07 2022 [pid 5385] [ftpuser] FAIL LOGIN: Client "::ffff:192.168.1.7"
Mon Jan  3 15:24:07 2022 [pid 5371] [ftpuser] FAIL LOGIN: Client "::ffff:192.168.1.7"
Mon Jan  3 15:24:07 2022 [pid 5373] [ftpuser] FAIL LOGIN: Client "::ffff:192.168.1.7"
Mon Jan  3 15:24:07 2022 [pid 5359] [ftpuser] FAIL LOGIN: Client "::ffff:192.168.1.7"
Mon Jan  3 15:24:07 2022 [pid 5361] [ftpuser] FAIL LOGIN: Client "::ffff:192.168.1.7"
Mon Jan  3 15:24:07 2022 [pid 5375] [ftpuser] FAIL LOGIN: Client "::ffff:192.168.1.7"
Mon Jan  3 15:24:08 2022 [pid 5377] [ftpuser] FAIL LOGIN: Client "::ffff:192.168.1.7"
Mon Jan  3 15:24:08 2022 [pid 5387] [ftpuser] FAIL LOGIN: Client "::ffff:192.168.1.7"
Mon Jan  3 15:24:08 2022 [pid 5379] [ftpuser] FAIL LOGIN: Client "::ffff:192.168.1.7"
Mon Jan  3 15:24:08 2022 [pid 5365] [ftpuser] FAIL LOGIN: Client "::ffff:192.168.1.7"
Mon Jan  3 15:24:08 2022 [pid 5367] [ftpuser] FAIL LOGIN: Client "::ffff:192.168.1.7"
Mon Jan  3 15:24:08 2022 [pid 5390] CONNECT: Client "::ffff:192.168.1.7"
Mon Jan  3 15:24:08 2022 [pid 5363] [ftpuser] FAIL LOGIN: Client "::ffff:192.168.1.7"
Mon Jan  3 15:24:09 2022 [pid 5392] CONNECT: Client "::ffff:192.168.1.7"
Mon Jan  3 15:24:09 2022 [pid 5394] CONNECT: Client "::ffff:192.168.1.7"
Mon Jan  3 15:24:09 2022 [pid 5381] [ftpuser] FAIL LOGIN: Client "::ffff:192.168.1.7"
Mon Jan  3 15:24:09 2022 [pid 5383] [ftpuser] FAIL LOGIN: Client "::ffff:192.168.1.7"
Mon Jan  3 15:24:09 2022 [pid 5396] CONNECT: Client "::ffff:192.168.1.7"
Mon Jan  3 15:24:09 2022 [pid 5398] CONNECT: Client "::ffff:192.168.1.7"
Mon Jan  3 15:24:10 2022 [pid 5400] CONNECT: Client "::ffff:192.168.1.7"
Mon Jan  3 15:24:11 2022 [pid 5369] [ftpuser] FAIL LOGIN: Client "::ffff:192.168.1.7"
Mon Jan  3 15:24:11 2022 [pid 5385] [ftpuser] FAIL LOGIN: Client "::ffff:192.168.1.7"
Mon Jan  3 15:24:11 2022 [pid 5371] [ftpuser] FAIL LOGIN: Client "::ffff:192.168.1.7"
Mon Jan  3 15:24:11 2022 [pid 5373] [ftpuser] FAIL LOGIN: Client "::ffff:192.168.1.7"
Mon Jan  3 15:24:11 2022 [pid 5375] [ftpuser] FAIL LOGIN: Client "::ffff:192.168.1.7"
Mon Jan  3 15:24:11 2022 [pid 5377] [ftpuser] FAIL LOGIN: Client "::ffff:192.168.1.7"
Mon Jan  3 15:24:11 2022 [pid 5387] [ftpuser] FAIL LOGIN: Client "::ffff:192.168.1.7"
Mon Jan  3 15:24:11 2022 [pid 5379] [ftpuser] FAIL LOGIN: Client "::ffff:192.168.1.7"
Mon Jan  3 15:24:11 2022 [pid 5389] [ftpuser] FAIL LOGIN: Client "::ffff:192.168.1.7"
Mon Jan  3 15:24:11 2022 [pid 5391] [ftpuser] FAIL LOGIN: Client "::ffff:192.168.1.7"
Mon Jan  3 15:24:11 2022 [pid 5393] [ftpuser] FAIL LOGIN: Client "::ffff:192.168.1.7"
Mon Jan  3 15:24:12 2022 [pid 5395] [ftpuser] FAIL LOGIN: Client "::ffff:192.168.1.7"
Mon Jan  3 15:24:12 2022 [pid 5397] [ftpuser] FAIL LOGIN: Client "::ffff:192.168.1.7"
Mon Jan  3 15:24:12 2022 [pid 5402] CONNECT: Client "::ffff:192.168.1.7"
```

Finally after a few attempts I got the right username. FLAG: **KCTF{ftpuser_192.168.1.7}.**

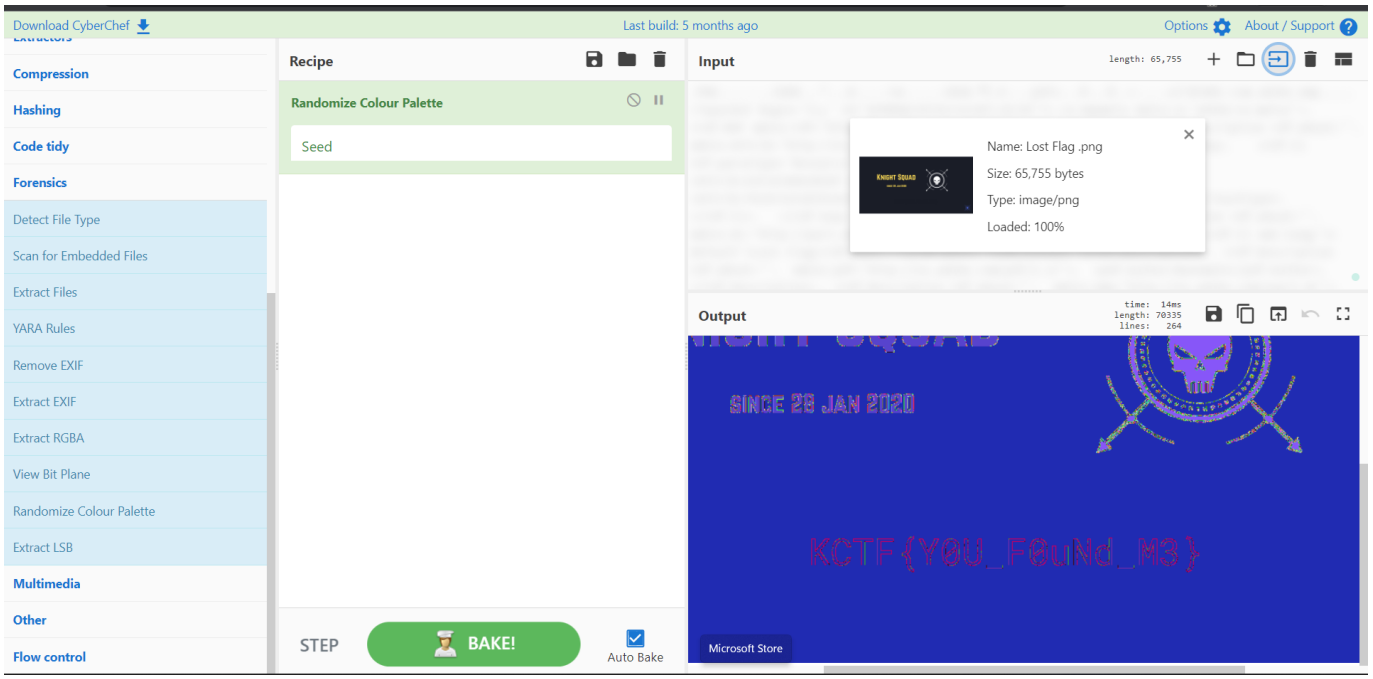
The Lost Flag (Digital Forensics):

The file given was an image with nothing much apparently.



Given image file:

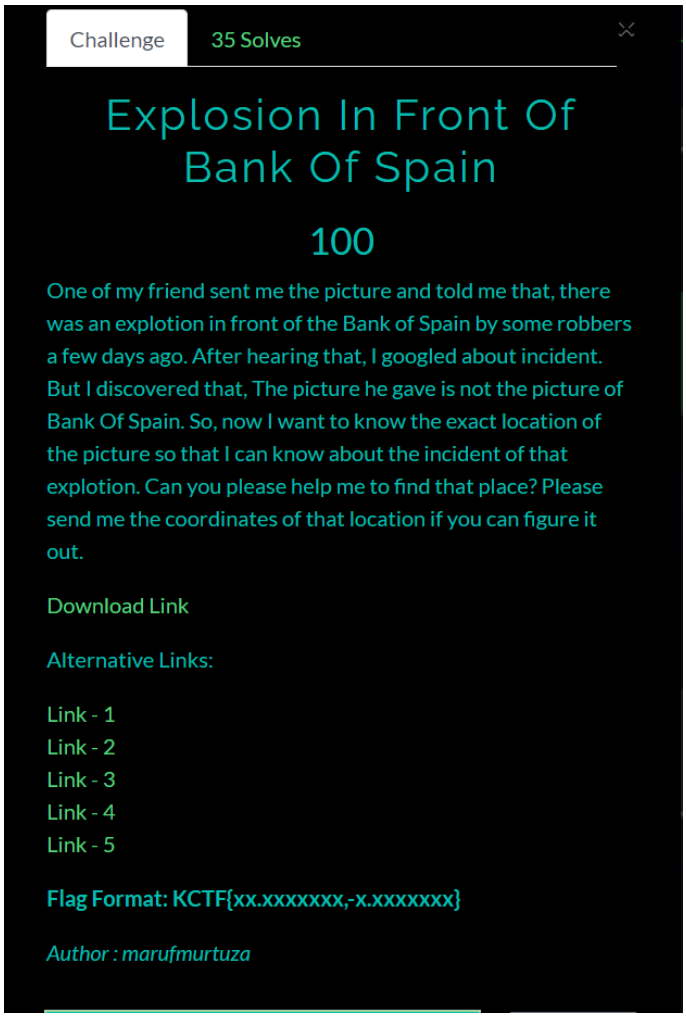
As it’s a forensics based challenge, I decided to approach it in that way, using cyberchef I got an easy technique to change the colour palette.



On changing the colour palette the flag got uncovered clearly.

Explosion in front of bank of Spain (OSINT):

It’s an OSINT challenge with an image and requested to find it’s coordinates as our flag.



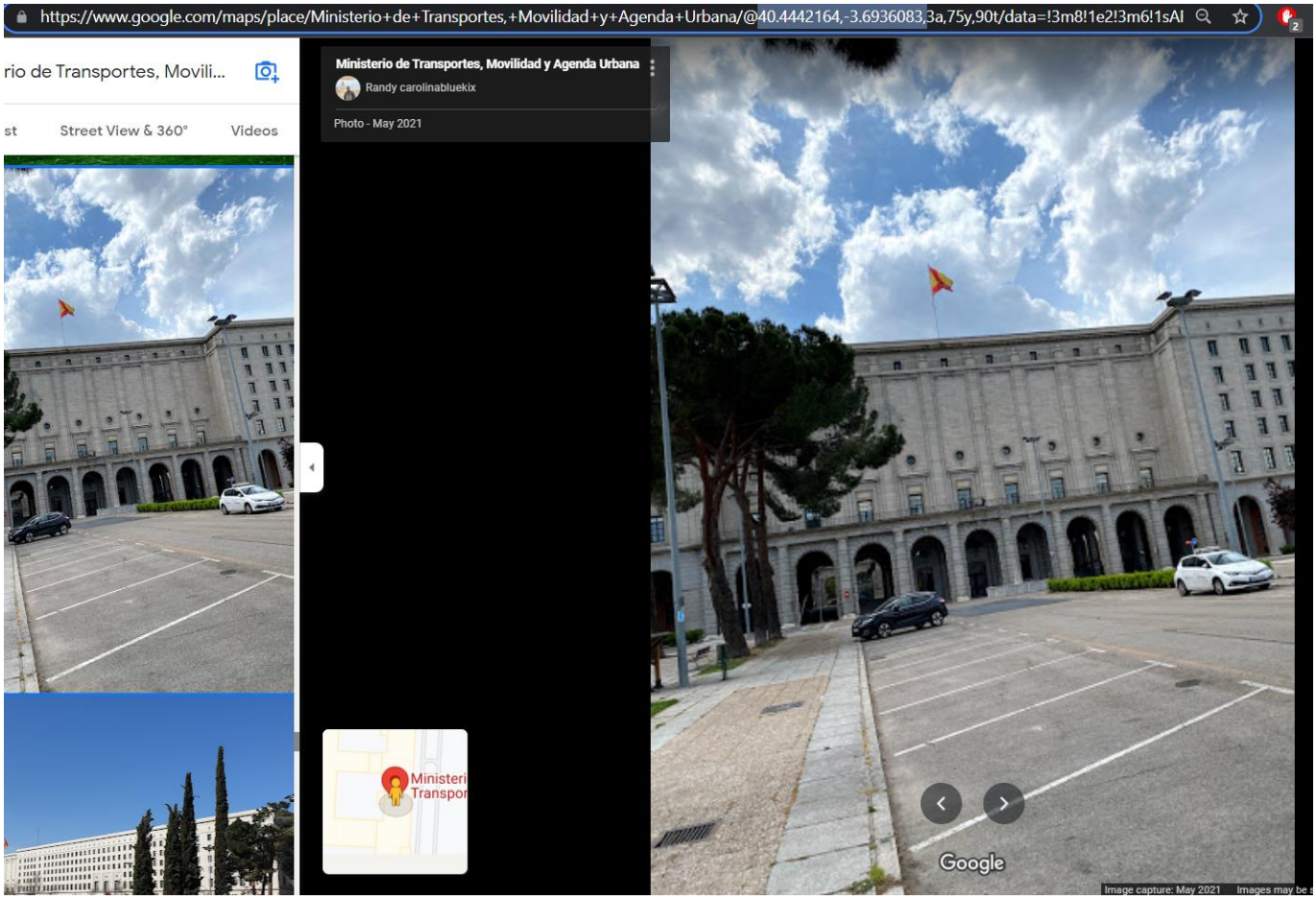
This image is taken from a TV series La Casa de Papel (Money Heist), as I’ve seen the series it was easy for me to track down the source and season from where the image is taken.

So just googled for the location where the series was shot and got the place name. It is a government office in Spain.

---

5. Ministerio de Fomento (Ministry of Public Works and Transport) as the Bank of Spain

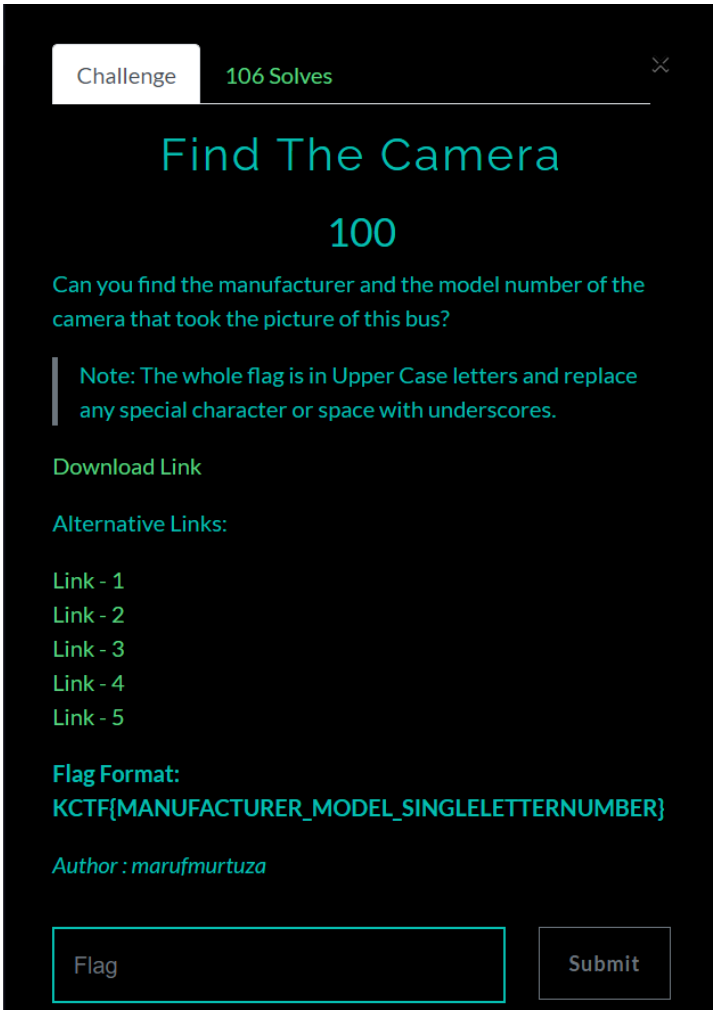
A photo from google map had the exact coordinates we needed which is also the flag.



FLAG: **KCTF{40.4442164,-3.6936083}**

Find the Camera (OSINT):

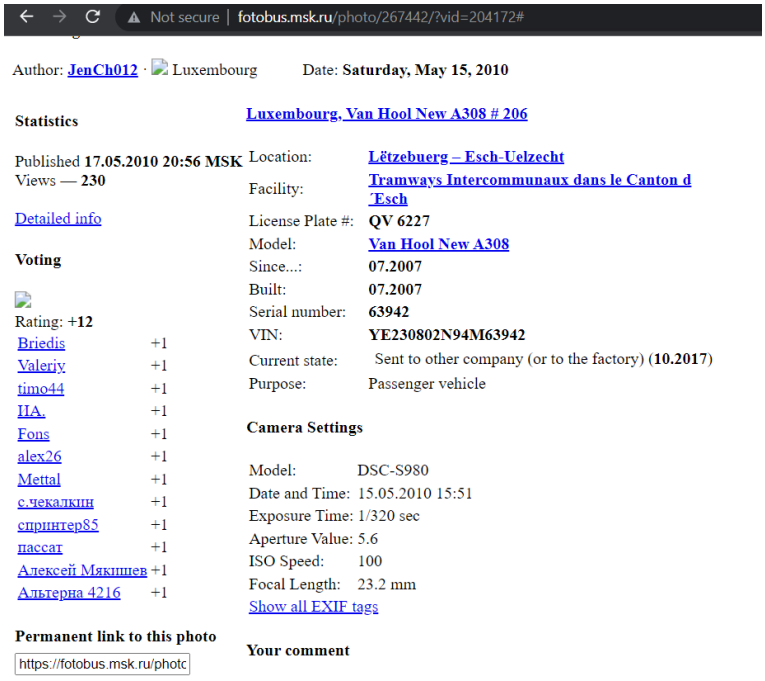
It was an interesting as well as easy challenge in which we are needed to find the camera that was used to take the given picture.

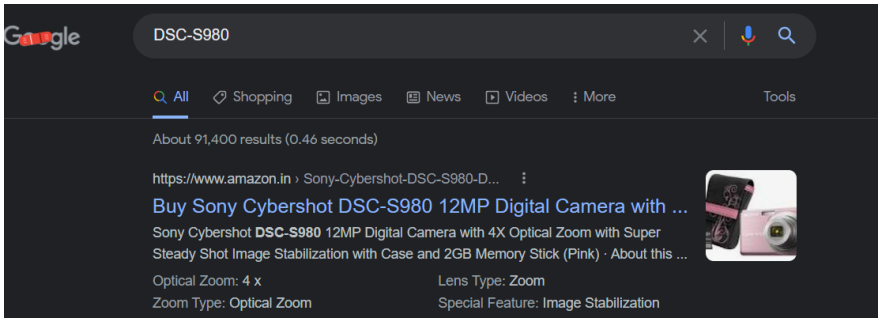


Given picture:

Using **Yandex** search engine I looked for the reverse image lookup which gave me the exact same match as the given image

Opening the link from the matching result what I got was the model name and number of the camera used for taking the picture which is the all needed to find the camera manufacturer name.

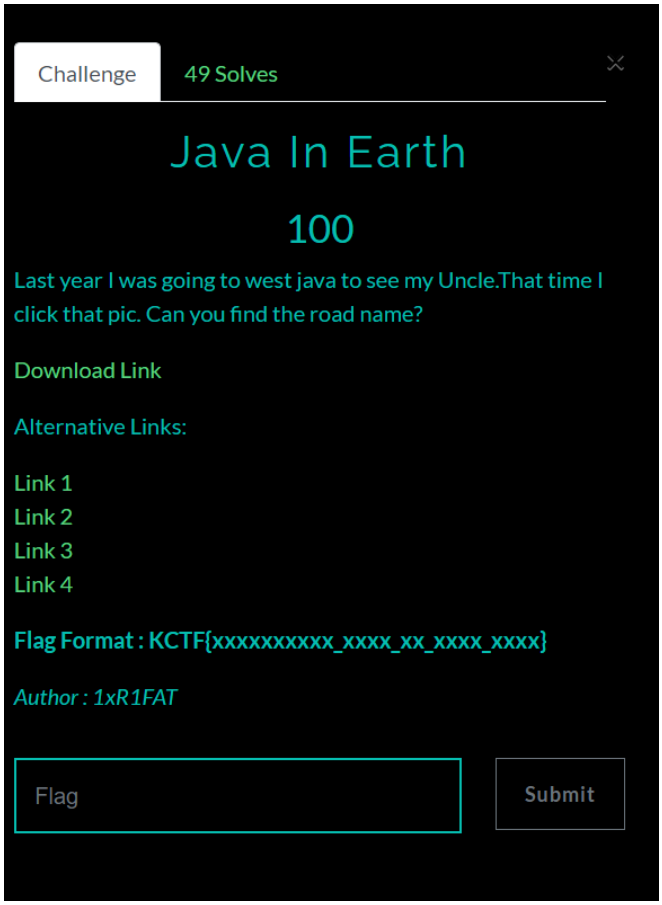




FLAG: **KCTF{SONY_DSC_S980}**

Java in Earth (OSINT):

This is also an OSINT challenge based on location unlike the previous challenge flag for this challenge is just the name of the place at which the image was taken.



Given image:

After few hours of tiring effort of reverse image search using various search engine I got nothing, So decided to look for clues from the image as the payoff to it I noticed a watermark "**2021 Google"**, these are found in google street view images along with this I also got the place where to look for from the challenge description **West Java.** So on using it both searched for intersecting bridges in google maps as soon as I found one, used street view to verify the place with the given image.

FLAG: **KCTF{padaleunyi_toll_rd_west_java}**