

# How's the Shark (Networking):

Given pcap file is downloaded and analyzed for the flag.

Challenge

132 Solves

✕

How's the Shark?

25

Find the flag from the following.

Download Link

Alternative Links

Download Link - 1

Download Link - 2

Download Link - 3

Download Link - 4

Download Link - 5

Flag Format: KCTF{ThE\_fIAG\_hErE}

Author : TareqAhamed

Flag

Submit

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

NetworkMiner 2.7.2

FileToolsHelp

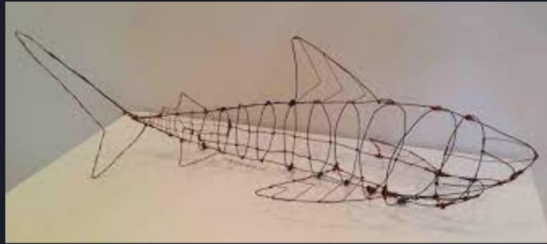
--- Select a network adapter in the list ---

Hosts (34)Files (22)Images (18)MessagesCredentialsSessions (29)DNS (6)Parameters (317)KeywordsAnomalies

Filter keyword:

Frame nr.	Filename	Extension	Size	Source host	S. port	Destination host	D. port	Protocol	Timestamp
67	about.php	html	11 905 B	192.168.1.9 [192.168.1.9]	TCP 80	192.168.1.4 (Linux)	TCP 48484	HttpGetNormal	2025-09-07 08:19:15 UTC
73	leaf-bg-top.png	png	20 266 B	192.168.1.9 [192.168.1.9]	TCP 80	192.168.1.4 (Linux)	TCP 48484	HttpGetNormal	2025-09-07 08:21:21 UTC
79	dots-group-cyan.png	png	1 280 B	192.168.1.9 [192.168.1.9]	TCP 80	192.168.1.4 (Linux)	TCP 48484	HttpGetNormal	2025-09-07 08:21:26 UTC
83	leaf-cyan-lg.png	png	14 917 B	192.168.1.9 [192.168.1.9]	TCP 80	192.168.1.4 (Linux)	TCP 48484	HttpGetNormal	2025-09-07 08:21:31 UTC
90	author.jpg	jpg	12 690 B	192.168.1.9 [192.168.1.9]	TCP 80	192.168.1.4 (Linux)	TCP 48484	HttpGetNormal	2025-09-07 08:21:33 UTC
93	signature.png	png	5 404 B	192.168.1.9 [192.168.1.9]	TCP 80	192.168.1.4 (Linux)	TCP 48486	HttpGetNormal	2025-09-07 08:21:35 UTC
97	plan.png	png	2 648 B	192.168.1.9 [192.168.1.9]	TCP 80	192.168.1.4 (Linux)	TCP 48484	HttpGetNormal	2025-09-07 08:21:37 UTC
100	design.png	png	2 707 B	192.168.1.9 [192.168.1.9]	TCP 80	192.168.1.4 (Linux)	TCP 48484	HttpGetNormal	2025-09-07 08:21:40 UTC
103	print.png	png	2 381 B	192.168.1.9 [192.168.1.9]	TCP 80	192.168.1.4 (Linux)	TCP 48484	HttpGetNormal	2025-09-07 08:21:42 UTC
106	member-1.png	png	164 112 B	192.168.1.9 [192.168.1.9]	TCP 80	192.168.1.4 (Linux)	TCP 48484	HttpGetNormal	2025-09-07 08:21:46 UTC
124	member-2.png	png	200 022 B	192.168.1.9 [192.168.1.9]	TCP 80	192.168.1.4 (Linux)	TCP 48484	HttpGetNormal	2025-09-07 08:21:49 UTC
139	member-3.png	png	65 166 B	192.168.1.9 [192.168.1.9]	TCP 80	192.168.1.4 (Linux)	TCP 48484	HttpGetNormal	2025-09-07 08:21:54 UTC
144	team-bg.png	png	11 282 B	192.168.1.9 [192.168.1.9]	TCP 80	192.168.1.4 (Linux)	TCP 48484	HttpGetNormal	2025-09-07 08:26:48 UTC
355	about[1].php	html	11 905 B	192.168.1.9 [192.168.1.9]	TCP 80	192.168.1.4 (Linux)	TCP 48490	HttpGetNormal	2025-09-07 21:51:41 UTC
411	something.png	png	65 753 B	192.168.1.9 [192.168.1.9]	TCP 80	192.168.1.4 (Linux)	TCP 48492	HttpGetNormal	2025-09-08 02:06:11 UTC
488	portfolio.php	html	13 562 B	192.168.1.9 [192.168.1.9]	TCP 80	192.168.1.4 (Linux)	TCP 48494	HttpGetNormal	2025-09-08 04:34:07 UTC
494	page-title.png	png	18 250 B	192.168.1.9 [192.168.1.9]	TCP 80	192.168.1.4 (Linux)	TCP 48494	HttpGetNormal	2025-09-08 04:36:03 UTC
500	item-6.png	png	80 433 B	192.168.1.9 [192.168.1.9]	TCP 80	192.168.1.4 (Linux)	TCP 48494	HttpGetNormal	2025-09-08 04:36:37 UTC
514	item-8.png	png	28 255 B	192.168.1.9 [192.168.1.9]	TCP 80	192.168.1.4 (Linux)	TCP 48494	HttpGetNormal	2025-09-08 04:36:57 UTC
518	item-7.png	png	55 111 B	192.168.1.9 [192.168.1.9]	TCP 80	192.168.1.4 (Linux)	TCP 48494	HttpGetNormal	2025-09-08 04:37:09 UTC
612	portfolio[1].php	html	13 562 B	192.168.1.9 [192.168.1.9]	TCP 80	192.168.1.4 (Linux)	TCP 48496	HttpGetNormal	2025-09-08 09:06:10 UTC
647	something something.png	png	158 465 B	192.168.1.9 [192.168.1.9]	TCP 80	192.168.1.4 (Linux)	TCP 48498	HttpGetNormal	2025-09-08 12:26:47 UTC

KCTF{A\_ShARk\_iN\_tHe\_WirE}



## 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.

Challenge

225 Solves

✕

FileD

25

Can you see everything?

Download Link

Alternative Links:

Download Link - 1

Download Link - 2

Download Link - 3

Download Link - 4

Download Link - 5

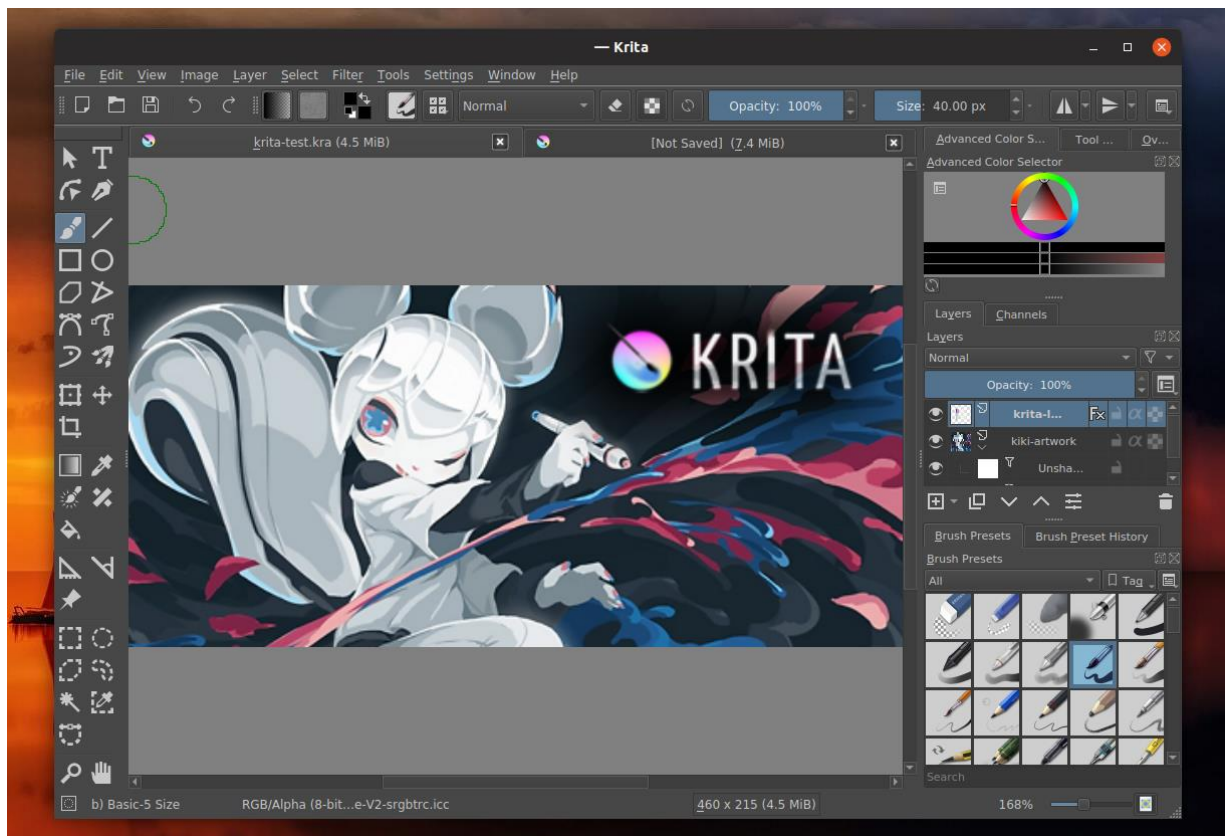
Flag Format: KCTF{S0m3\_text\_h3r3}

Author: 1xR1fat

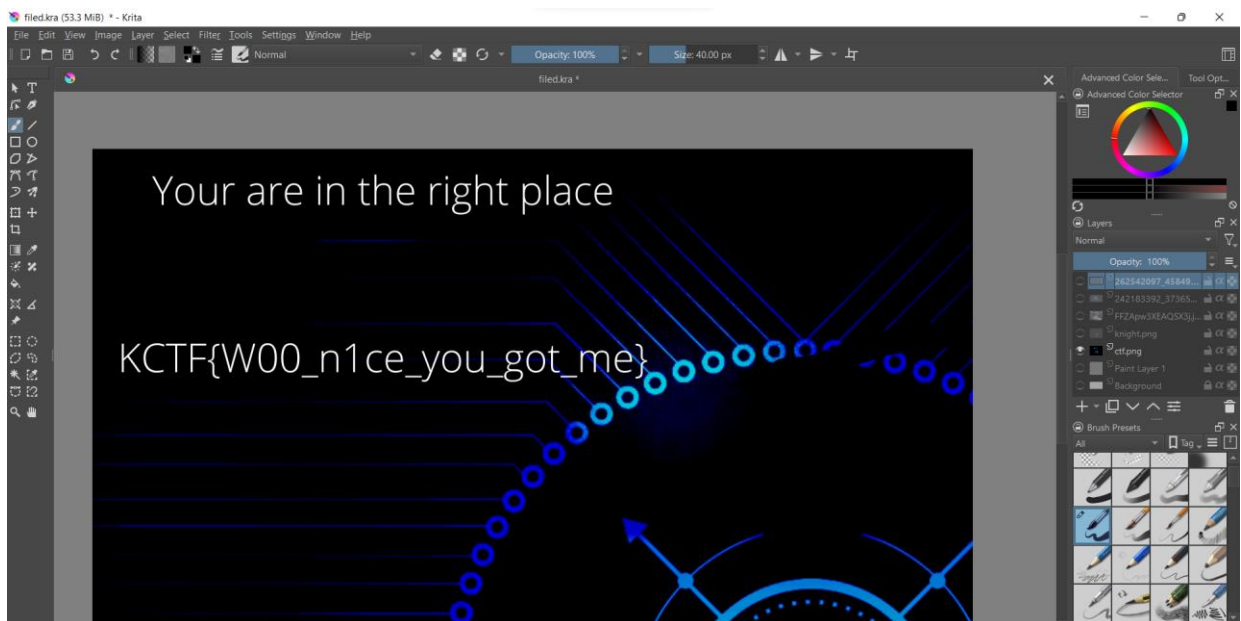
Flag

Submit

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

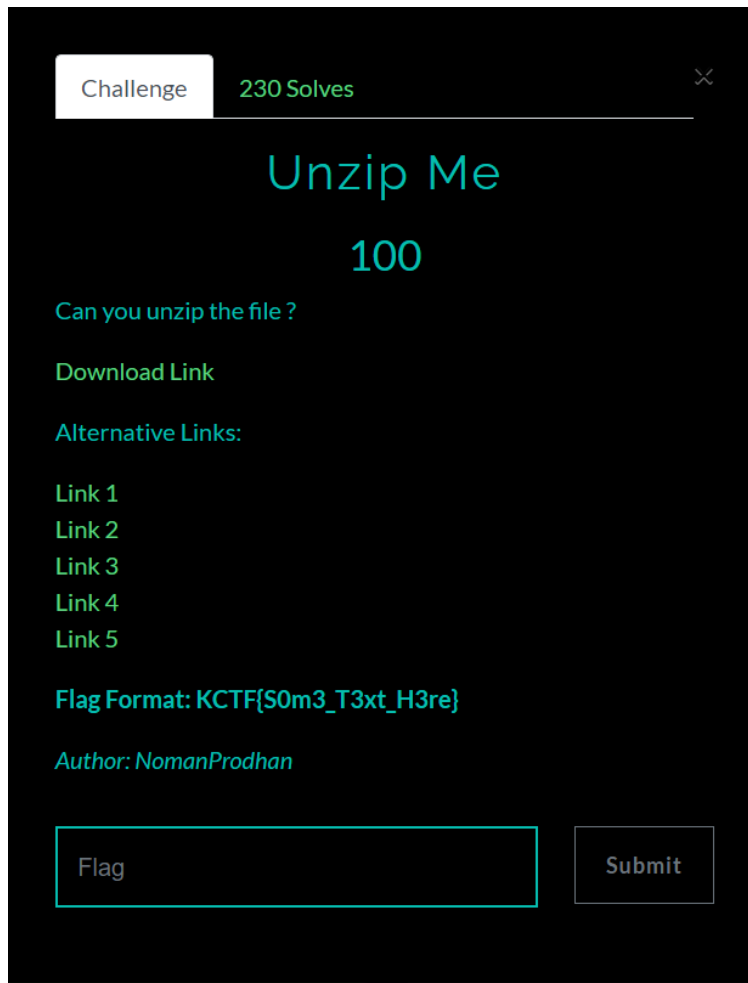


On opening the file using krita got to know the file is a blended image project file with help of many images, by turning off each layers of image finally got the flag.

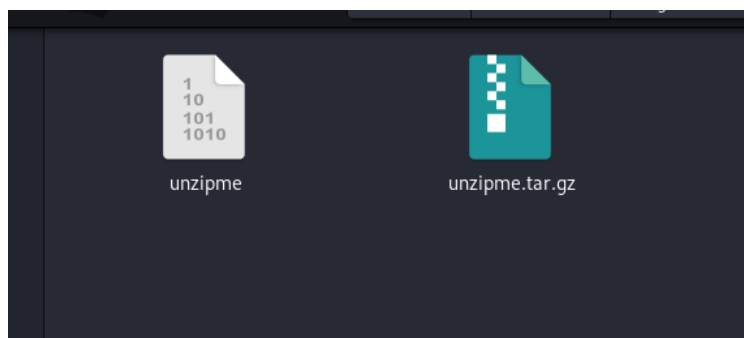


## Unzip Me (Misc):

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.



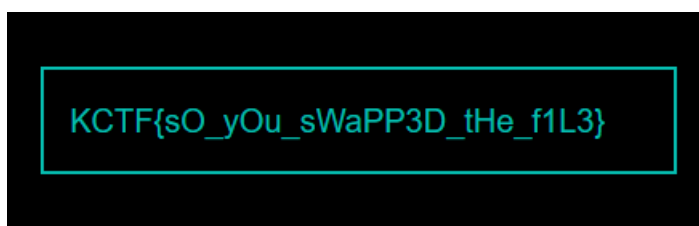
So I checked for the file type using **file** command in linux that gave me the file type as **data**. As data files can be printed using **cat** command. Using cat command on the file gave out the flag we need but in a jumbled way, but was easy to unscramble it.

```
(toor@N051N)-[~/Downloads]
$ file unzipme
unzipme: data

(toor@N051N)-[~/Downloads]
$ cat unzipme
KP6T,|6lfgat.txCKFTs{_00y_uWsPa3P_DHt_e1f3L
}KP?6T,|666lfgat.txKP6D

(toor@N051N)-[~/Downloads]
$ strings unzipme
lfgat.txCKFTs{_00y_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.

Challenge

163 Solves

×

## Compromised FTP

### 25

We detected some malicious activity on our FTP server. Someone has performed bruteforce attack to gain access to our FTP server. Find out the Compromised FTP account username & the attacker IP from the following.

Download Link

Alternative Links:

- Link - 1
- Link - 2
- Link - 3
- Link - 4
- Link - 5

Flag Format: KCTF{username\_127.0.0.1}

Author : TareqAhamed

Flag

Submit

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.

Challenge

274 Solves

✕

# The Lost Flag

## 25

We recovered a image file from an incident. There might be something interesting in the file. Give it a try.

Download Link

Alternative Links:

- Link - 1
- Link - 2
- Link - 3
- Link - 4
- Link - 5

Flag Format: KCTF{pla1n\_t3xt\_here}

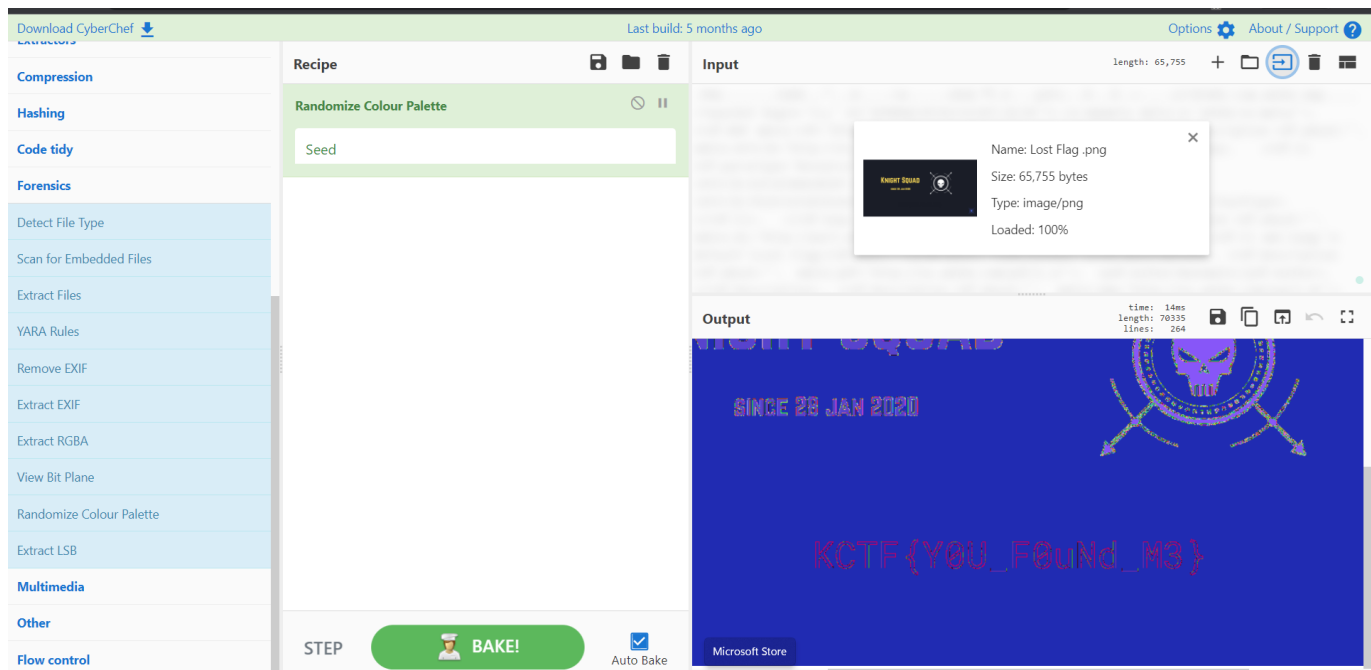
Author : TareqAhamed

Submit

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.

Challenge 35 Solves

### Explosion In Front Of Bank Of Spain

100

One of my friend sent me the picture and told me that, there was an explotion in front of the Bank of Spain by some robbers a few days ago. After hearing that, I googled about incident. But I discovered that, The picture he gave is not the picture of Bank Of Spain. So, now I want to know the exact location of the picture so that I can know about the incident of that explotion. Can you please help me to find that place? Please send me the coordinates of that location if you can figure it out.

Download Link

Alternative Links:

- Link - 1
- Link - 2
- Link - 3
- Link - 4
- Link - 5

Flag Format: KCTF{xx.xxxxxxx,-x.xxxxxxx}

Author : marufmurtuza

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.

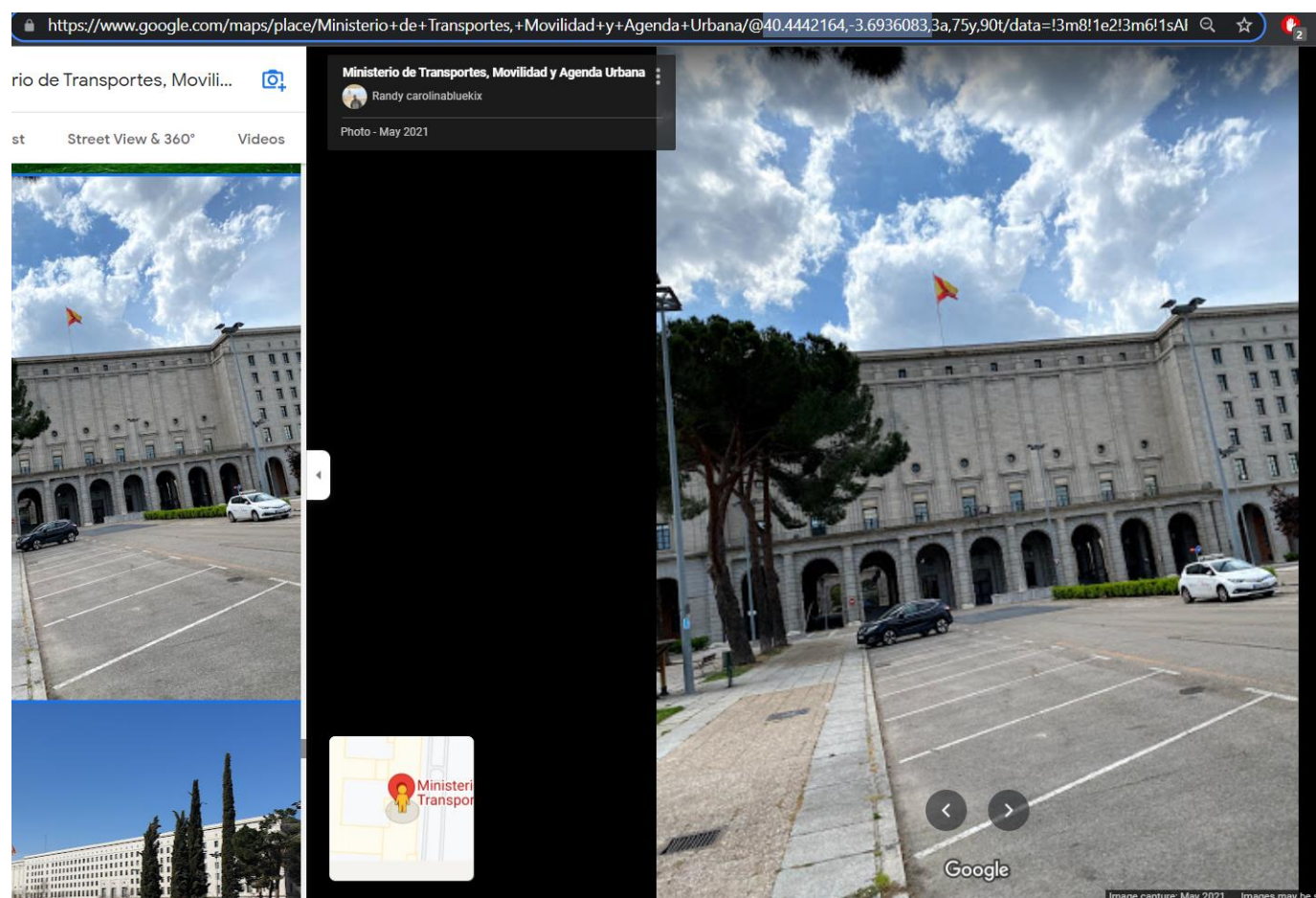


So just googled for the location where the series was shot and got the place name. It is a government office in Spain.

## 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.

Challenge

106 Solves

✕

## Find The Camera

### 100

Can you find the manufacturer and the model number of the camera that took the picture of this bus?

Note: The whole flag is in Upper Case letters and replace any special character or space with underscores.

Download Link

Alternative Links:

- Link - 1
- Link - 2
- Link - 3
- Link - 4
- Link - 5

Flag Format:  
KCTF{MANUFACTURER\_MODEL\_SINGLELETTERNUMBER}

Author : marufmurtuza

Submit

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.

← → ↻ Not secure | fotobus.msk.ru/photo/267442/?vid=204172#

Author: [JenCh012](#) · Luxembourg Date: Saturday, May 15, 2010

**Statistics** [Luxembourg, Van Hool New A308 # 206](#)

Published 17.05.2010 20:56 MSK Location: [Lëtzebuerg – Esch-Uelzecht](#)  
Views — 230 Facility: [Tramways Intercommunaux dans le Canton d'Esch](#)

[Detailed info](#) License Plate #: QV 6227  
Model: [Van Hool New A308](#)  
Since...: 07.2007  
Built: 07.2007  
Serial number: 63942  
VIN: YE230802N94M63942  
Current state: Sent to other company (or to the factory) (10.2017)  
Purpose: Passenger vehicle

**Voting**

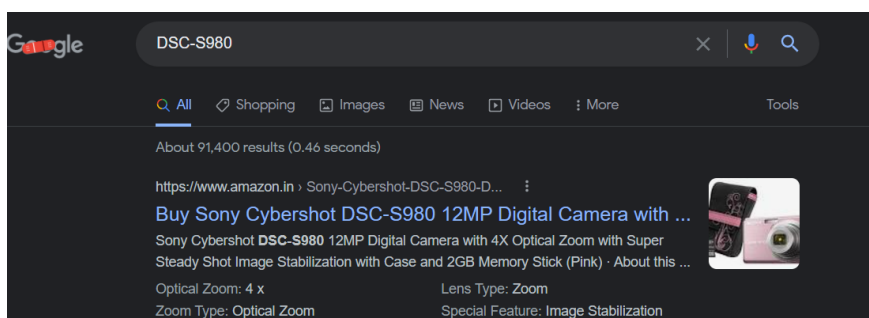
Rating: +12  
[Briedis](#) +1  
[Valeriy](#) +1  
[timo44](#) +1  
[IIA](#) +1  
[Fons](#) +1  
[alex26](#) +1  
[Metta](#) +1  
[с.чекалкин](#) +1  
[спринтер85](#) +1  
[пассат](#) +1  
[Алексей Мясников](#) +1  
[Альтерна 4216](#) +1

**Camera Settings**

Model: DSC-S980  
Date and Time: 15.05.2010 15:51  
Exposure Time: 1/320 sec  
Aperture Value: 5.6  
ISO Speed: 100  
Focal Length: 23.2 mm  
[Show all EXIF tags](#)

**Permanent link to this photo**  
<https://fotobus.msk.ru/photo/267442/?vid=204172#>

**Your comment**



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.

Challenge

49 Solves

✕

# Java In Earth

## 100

Last year I was going to west java to see my Uncle. That time I click that pic. Can you find the road name?

[Download Link](#)

Alternative Links:

[Link 1](#)  
[Link 2](#)  
[Link 3](#)  
[Link 4](#)

Flag Format : KCTF{xxxxxxxxxxx\_xxxx\_xx\_xxxx\_xxxx}

Author : 1xR1FAT

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}