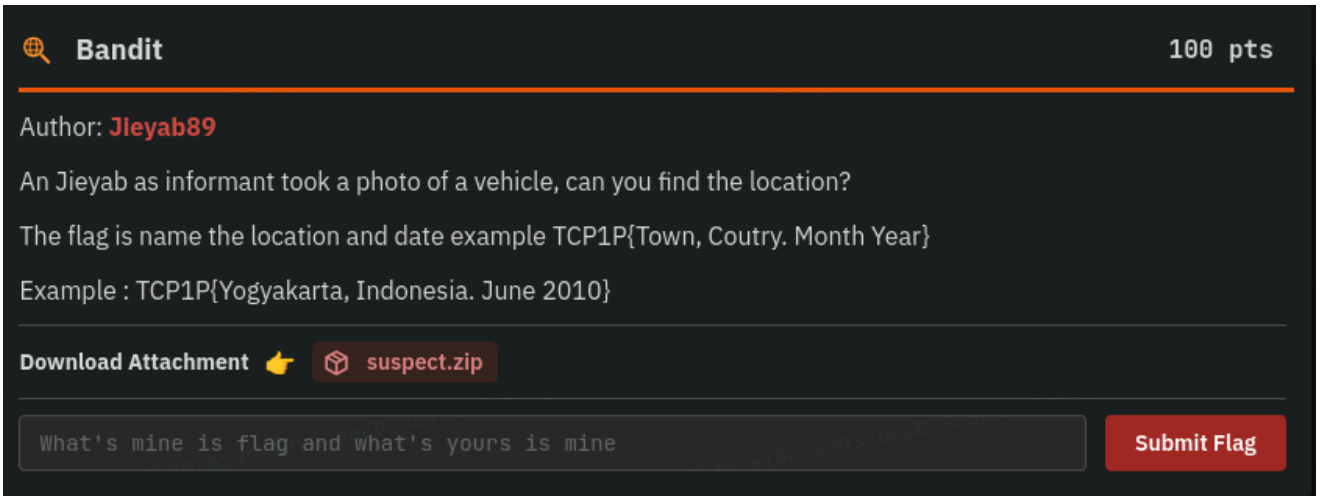
Bandit



This was an OSINT challenge. I am new to CTFs but I really appreciate that CTF creators are including OSINT as a category.

This is the photo they provided:

https://29a.ch/photo-forensics/#exif-meta-dat

I started by verifying the basic header information:

```
Bandit file suspect.jpg
suspect.jpg: JPEG image data, JFIF standard 1.01, resolution (DPI), density 72×72, segment length 16, Exif Standard: [TIFF image
data, big-endian, direntries=4, manufacturer=OPPO, model=A37f], baseline, precision 8, 1055×963, components 3
```

I then expanded by running the exiftool on the file. This was the output:

```
ExifTool Version Number         : 12.76
File Name                       : suspect.jpg
Directory                       : .
File Size                       : 206 kB
File Modification Date/Time     : 2024:05:26 15:19:00-04:00
File Access Date/Time           : 2024:10:11 08:20:27-04:00
File Inode Change Date/Time     : 2024:10:11 08:20:21-04:00
File Permissions                : -rwxrw-rw-
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
```

```
JFIF Version                    : 1.01
Resolution Unit                 : inches
X Resolution                    : 72
Y Resolution                    : 72
Exif Byte Order                 : Big-endian (Motorola, MM)
Make                            : OPPO
Camera Model Name               : A37f
Exposure Time                   : 1/99
F Number                        : 2.2
ISO                             : 130
Exif Version                    : 0220
Date/Time Original              : 2019:10:25 17:00:00
Create Date                     : 2019:10:25 17:00:00
Shutter Speed Value             : 1/99
Aperture Value                  : 2.2
Flash                           : Off, Did not fire
Focal Length                    : 3.6 mm
Sub Sec Time Original           : 00
Sub Sec Time Digitized          : 00
Padding                         : (Binary data 268 bytes, use -b option to
extract)
Current IPTC Digest             : 23e935c1f8aef852ffc1e840d9b0c4c1
Keywords                        : jieyab89 Vehicle OSINT
Application Record Version      : 4
XMP Toolkit                     : Image::ExifTool 12.57
About                           : uuid:faf5bdd5-ba3d-11da-ad31-
d33d75182f1b
Notes                           : Vehicle OSINT
Author                          : Jieyab89
Image Width                     : 1055
Image Height                    : 963
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
Aperture                        : 2.2
Image Size                      : 1055x963
Megapixels                      : 1.0
Shutter Speed                   : 1/99
Create Date                     : 2019:10:25 17:00:00.00
Date/Time Original              : 2019:10:25 17:00:00.00
Focal Length                    : 3.6 mm
Light Value                     : 8.5
```

Part of the prompt requires us to get the date the photo was taken. That appears to be: October 25, 2019

The next part was discerning the location. I think they kind of hand it to you here. All other text based information in the photo is blurred except for the license plate.

The CTF authors are hackers from Indonesia. So I had to google around to figure out how Indonesian license plates work.

These are the resources I used:
https://en.wikipedia.org/wiki/Vehicle_registration_plates_of_Indonesia
https://wuling.id/en/blog/lifestyle/understanding-the-vehicle-number-code-in-indonesia
https://www.mpm-rent.com/en/news-detail/info-lengkap-daftar-kode-plat-nomor-kendaraan-di-indonesia

So the first letter on an Indonesian license plate is the city code or origin of vehicle.

N - Malang, Pasuruan, Probolinggo, Batu, and Lumajang

I could not find a good way to narrow this further, so I started guessing with my 5 guesses. Luckily it was the first one!

And the flag was:

```
TCP1P{Malang, Indonesia. October 2019}
```

That was a nice little challenge to introduce someone to EXIF metadata.