Meta

Contents

Scenario 2
Pre-requisites 2
Initial thoughts from scenario 2
Challenge Questions 2
What is the camera model? 2
When was the picture taken? 3
What does the comment on the first image says? 4
Where could the criminal be? 4

Scenario

The attached images were posted by a criminal on the run, with the caption "I'm roaming free. You will never catch me". We believe you can assist us in proving him wrong.

Pre-requisites

- Load kali
- Run sudo apt update && sudo apt -y upgrade > reboot.
- Change network to host only instead of NAT – to restrict network to within the VM.
- Open terminal and install exiftool (if necessary).

Initial thoughts from scenario

- Challenge file is an image file, meaning we can extract metadata from inside it.
- Exiftool is good for extracting metadata – start by using that, review results and see if further tools needed.

Challenge Questions

What is the camera model?

- Answer: Canon EOS 550D

```
┌──(kali㉿kali)-[~/Documents/BTLO/Challenges/Meta]
└─$ cd cf7becafebbb525b3c1df03785a2b9ee6b96e41c

┌──(kali㉿kali)-[~/…/BTLO/Challenges/Meta/cf7becafebbb525b3c1df03785a2b9ee6b96e41c
]
└─$ ls -al
total 4676
drwxr-xr-x 2 kali kali    4096 Oct  7 09:11 .
drwxr-xr-x 3 kali kali    4096 Oct  7 09:11 ..
-rw-r--r-- 1 kali kali 3575684 Nov 26  2021 uploaded_1.JPG
-rw-r--r-- 1 kali kali 1203827 Nov 26  2021 uploaded_2.png
```

- Extracting the challenge folder from the zip reveals 2 image files: 1 x jpeg, and 1 x png.

```
┌──(kali㉿kali)-[~/…/BTLO/Challenges/Meta/cf7becafebbb525b3c1df037
]
└─$ exiftool uploaded_1.JPG
ExifTool Version Number         : 12.67
File Name                       : uploaded_1.JPG
Directory                       : .
File Size                       : 3.6 MB
File Modification Date/Time     : 2021:11:26 11:35:07-05:00
```

- Running exiftool on uploaded_1.jpg shows lots of metadata. We can combine it with a grep to speed up investigations as in the scenario the criminal is on the run so time is of the essence:

```
┌──(kali㉿kali)-[~/…/BTLO/Challenges/Meta/cf7becafebbb525b3c1df03785a2b9ee6b96e41c]
└─$ exiftool uploaded_1.JPG | grep -e "[cC]amera"
Camera Model Name                : Canon EOS 550D
Camera Temperature               : 50 C
Control Mode                     : Camera Local Control
Camera Type                      : EOS High-end
Camera Orientation               : Rotate 90 CW

┌──(kali㉿kali)-[~/…/BTLO/Challenges/Meta/cf7becafebbb525b3c1df03785a2b9ee6b96e41c]
└─$ |
```

```
┌──(kali㉿kali)-[~/…/BTLO/Challenges/Meta/cf7becafebbb525b3c1df03785a2b9ee6b96e41c]
└─$ exiftool uploaded_2.png | grep -e "[cC]amera"
```

- At this stage, we don't know if both images were taken with the same camera. So checking the grep output against the second image confirms this

When was the picture taken?

- Answer: 2021:11:02 13:20:23

```
┌──(kali㉿kali)-[~/…/BTLO/Challenges/Meta/cf7becafebbb525b3c1df03785a2b9ee6b96e41c]
└─$ exiftool uploaded_1.JPG | grep -e "[tT]ime"
File Modification Date/Time     : 2021:11:26 11:35:07-05:00
File Access Date/Time           : 2023:10:07 09:12:27-04:00
File Inode Change Date/Time     : 2023:10:07 09:11:43-04:00
Exposure Time                   : 1/1000
Date/Time Original              : 2021:11:02 13:20:23
Self Timer                      : Off
Target Exposure Time            : 1/1024
Sub Sec Time                    : 32
Sub Sec Time Original           : 32
Sub Sec Time Digitized          : 32
Date/Time Original              : 2021:11:02 13:20:23.32

┌──(kali㉿kali)-[~/…/BTLO/Challenges/Meta/cf7becafebbb525b3c1df03785a2b9ee6b96e41c]
└─$ exiftool uploaded_2.png | grep -e "[tT]ime"
File Modification Date/Time     : 2021:11:26 11:35:07-05:00
File Access Date/Time           : 2021:11:26 11:35:52-05:00
File Inode Change Date/Time     : 2023:10:07 09:11:43-04:00
```

- Use exiftool again, but with a grep the pattern matches either "time" or "Time". Again, we can't confirm which image was taken first as the criminal could have purposely mis-labelled them as a red herring.
- Therefore we check both images with the same exiftool command. Only upload_1.jpg has "Date/Time Original" so we know the picture was taken at 2021:11:02 13:20:23.

What does the comment on the first image says?

- Answer: relying on altered metadata to catch me?

```
┌──(kali㉿kali)-[~/…/BTLO/Challenges/Meta/cf7becafebbb525b3c1df03785a2b9ee6b96e41c]
└─$ exiftool uploaded_1.JPG | grep -e "[cC]omment"
Comment                         : relying on altered metadata to catch me?

┌──(kali㉿kali)-[~/…/BTLO/Challenges/Meta/cf7becafebbb525b3c1df03785a2b9ee6b96e41c]
└─$ |
```

- Change the grep after exiftool to match “comment” or “Comment” to see if exiftool has a label/tag for comments.
- Grep returns a match, comment is “relying on altered metadata to catch me?”

Where could the criminal be?

- Answer: Kathmandu

```
┌──(kali㉿kali)-[~/…/BTLO/Challenges/Meta/cf7becafebbb525b3c1df03785a2b9ee6b96e41c]
└─$ exiftool uploaded_1.JPG | grep -e "[cC]ity"

┌──(kali㉿kali)-[~/…/BTLO/Challenges/Meta/cf7becafebbb525b3c1df03785a2b9ee6b96e41c]
└─$ exiftool uploaded_2.png | grep -e "[cC]ity"
```

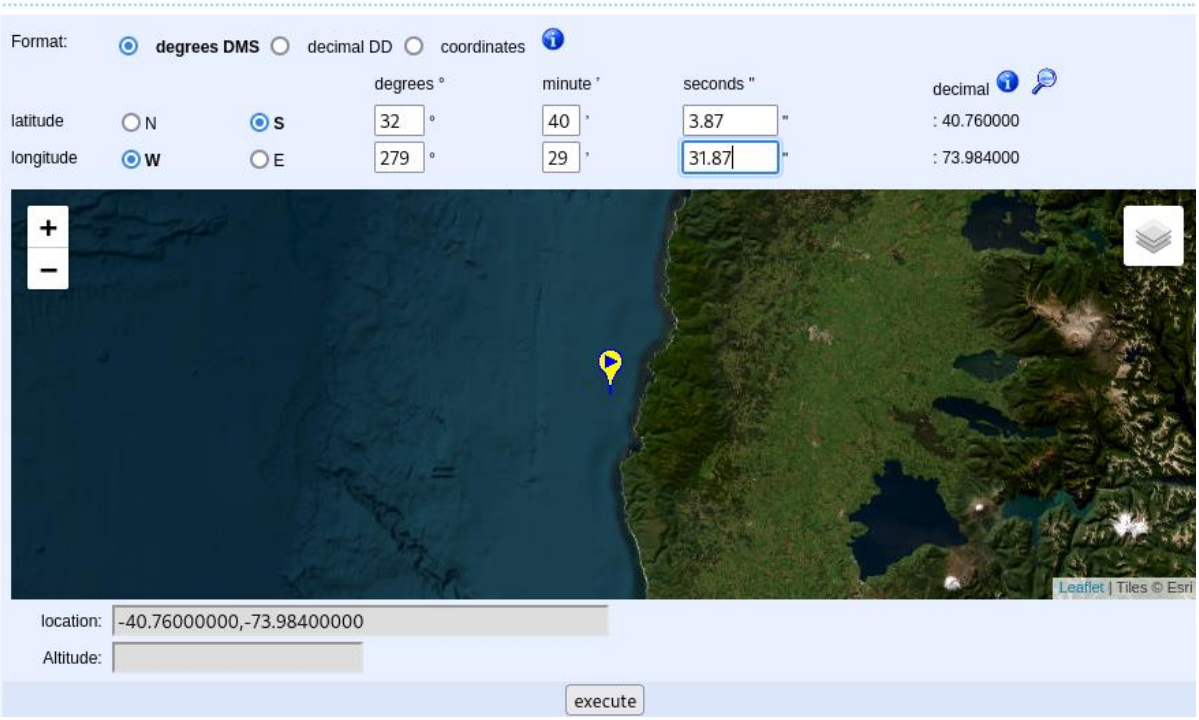
- An initial grep search for “city” or “City” didn’t return any matches, so we’ll rerun exiftool without a grep and review for any interesting labels/tags.
    - Doing so shows that exiftool uncovers Longitude/Latitude coordinates from the image file metadata, which we can use to pin point where the criminal is.

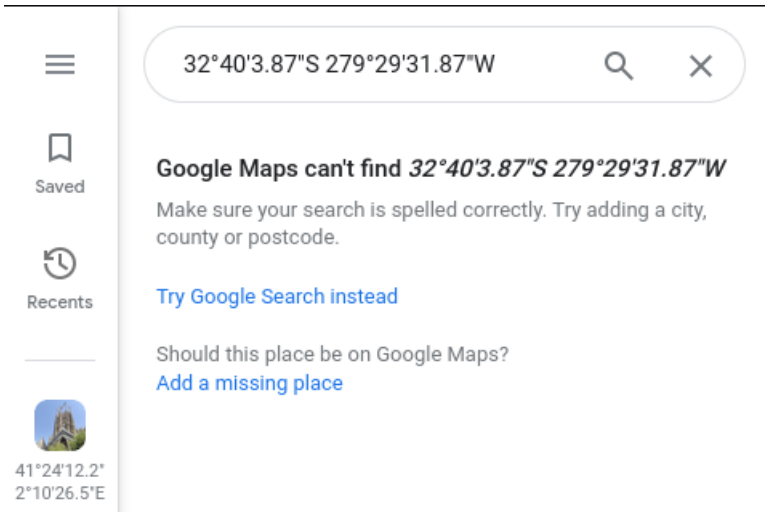
```
Date/Time Original              : 2021:11:02 13:20:23.32
Modify Date                     : 2021:11:02 13:20:23.32
Thumbnail Image                 : (Binary data 6101 bytes, use -b option to extract)
GPS Latitude                    : 32 deg 40' 3.87" S
GPS Longitude                   : 279 deg 29' 31.87" W
Lens                            : 55.0 - 250.0 mm (35 mm equivalent: 86.5 - 393.2 mm)
Circle Of Confusion             : 0.019 mm
Depth Of Field                  : inf (6.34 m - inf)
Field Of View                   : 23.5 deg
Focal Length                    : 55.0 mm (35 mm equivalent: 86.5 mm)
GPS Position                    : 32 deg 40' 3.87" S, 279 deg 29' 31.87" W
Hyperfocal Distance             : 8.80 m
Light Value                     : 18.3

┌──(kali㉿kali)-[~/…/BTLO/Challenges/Meta/cf7becafebbb525b3c1df03785a2b9ee6b96e41c]
└─$ |
```

- Again, we need to run the grep against both images to cross-reference and ensure both point to the same coordinates (provided they both have the metadata).

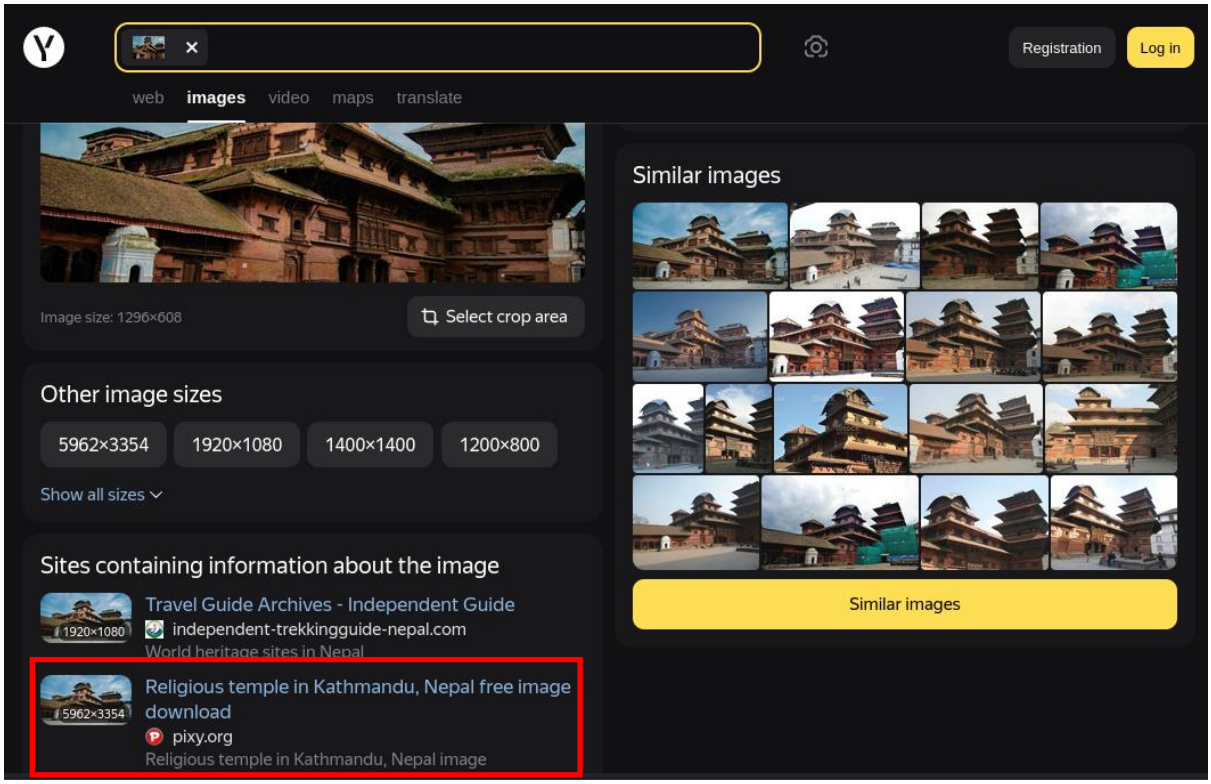
```
┌──(kali㉿kali)-[~/…/BTLO/Challenges/Meta/cf7becafebbb525b3c1df03785a2b9ee6b96e41c]
└─$ exiftool uploaded_1.JPG | grep -e "GPS"
GPS Latitude Ref                : South
GPS Longitude Ref               : West
GPS Latitude                    : 32 deg 40' 3.87" S
GPS Longitude                   : 279 deg 29' 31.87" W
GPS Position                    : 32 deg 40' 3.87" S, 279 deg 29' 31.87" W

┌──(kali㉿kali)-[~/…/BTLO/Challenges/Meta/cf7becafebbb525b3c1df03785a2b9ee6b96e41c]
└─$ exiftool uploaded_2.png | grep -e "GPS"

┌──(kali㉿kali)-[~/…/BTLO/Challenges/Meta/cf7becafebbb525b3c1df03785a2b9ee6b96e41c]
└─$ |
```

- We can then copy the "GPS Position" coordinates into a handy tool like Google Maps.





- However, Google maps came up empty, and another geolocation tool placed the coordinates from the metadata in the sea – nowhere near a city name as implied in the challenge question.
    - I double checked for typing errors, and then remembered that metadata can be tampered/altered (as implied in the earlier findings also). So I reverse imaged searched using Yandex instead.



- Reverse searching “upload_2.png” revealed that the criminal is in Kathmandu, Nepal.
    - I also searched “upload_1.jpeg” however multiple cities were returned, providing no clear answer.