TryHackMe - OhSINT

17 Mar 2020

What information can you possible get starting with just one photo?

Steganography

We start by downloading the WindowsXP.jpg screensaver.

```
[REDACTED]:~/security/TryHackMe/OhSINT$ exiftool WindowsXP.jpg
ExifTool Version Number    : 11.16
File Name                  : WindowsXP.jpg
Directory                  : .
File Size                  : 229 kB
File Modification Date/Time : 2020:03:14 19:43:04-05:00
File Access Date/Time      : 2020:03:14 19:43:04-05:00
File Inode Change Date/Time : 2020:03:14 19:43:33-05:00
File Permissions           : rw-rw-rw-
```

```
File Type                 : JPEG
File Type Extension       : jpg
MIME Type                 : image/jpeg
XMP Toolkit               : Image::ExifTool 11.27
GPS Latitude              : 54 deg 17' 41.27" N
GPS Longitude             : 2 deg 15' 1.33" W
Copyright                 : OWoodflint
Image Width               : 1920
Image Height              : 1080
Encoding Process          : Baseline DCT, Huffman coding
Bits Per Sample           : 8
Color Components          : 3
Y Cb Cr Sub Sampling      : YCbCr4:2:0 (2 2)
GPS Latitude Ref          : North
GPS Longitude Ref         : West
Image Size                : 1920x1080
Megapixels                : 2.1
GPS Position              : 54 deg 17' 41.27" N, 2 deg 15' 1.
33" W
```

The most obvious thing to check is the handle in the copyright. Once that is exhausted, we can check the GPS position.

Copyright : OWoodflint GPS Position : 54 deg 17' 41.27" N, 2 deg 15' 1.33" W

Twitter

0x0000000000000000000
@OWoodflint

I like taking photos and open source projects.

⊙ Space ⊞ Joined February 2019

6 Following   14 Followers

Tweets   Tweets & replies   Media   Likes

0x0000000000000000000 @OWoodflint · Mar 9, 2019
Hello world!

↩   ⟲ 3   ♡ 9

        Twitter handle: @OWoodflint Likes taking photos Likes open source projects Likes cats

I downloaded the profile picture as well, but exiftool turned up nothing interesting.

0x00000000000000000000 @OWoodflint · Mar 3, 2019
From my house I can get free wifi ;D

Bssid: B4:5D:50:AA:86:41 - Go nuts!

💬 2   🔁   ♡ 6   📤

```
BSSID: B4:5D:50:AA:86:41
```

Github

<> Code   Issues 0   Pull requests 0   Actions   Projects 0   Security   Insights

Join GitHub today

GitHub is home to over 40 million developers working together to host
and review code, manage projects, and build software together.

Sign up

Dismiss

A new social network for taking photos in your home town.

4 commits   1 branch   0 packages   0 releases   1 contributor

Branch: master ▾   New pull request

Find file   Clone or download ▾

OWoodfl1nt Update README.md   Latest commit a88e46c on Mar 3, 2019

README.md   Update README.md   13 months ago

README.md

people_finder

Hi all, I am from London, I like taking photos and open source projects.

Follow me on twitter: @OWoodflint

This project is a new social network for taking photos in your home town.

Project starting soon! Email me if you want to help out: OWoodflint@gmail.com

Github: OWoodfl1nt Email: OWoodflint@gmail.com From London

Wordpress Blog

Through google, we stumble across a blog:

https://oliverwoodflint.wordpress.com/author/owoodflint/

Oliver Woodflint Blog

Photos you can relate to

Home   Contact

Author: owoodflint

Hey

Im in New York right now, so I will update this site right away with new photos!

owoodflint   Uncategorized   Leave a comment   3rd Mar 2019   1 Minute

Full Name: Oliver Woodflint In New York on Holiday on 3rd March 2019

We also find a password hidden with white coloration in the one blog post. This was a very odd place to find a password.

Coordinates

Now we return back to the coordinates of the photo:

```
54 deg 17' 41.27" N, 2 deg 15' 1.33" W
```

Using `findlatitudeandlongitude.com`, we can get coordinates:

```
Latitude: 54.294797°
Longitude:  -2.250369°
```

Using the BSSID from the twitter post, we can look up the network on `Wigle.net`.
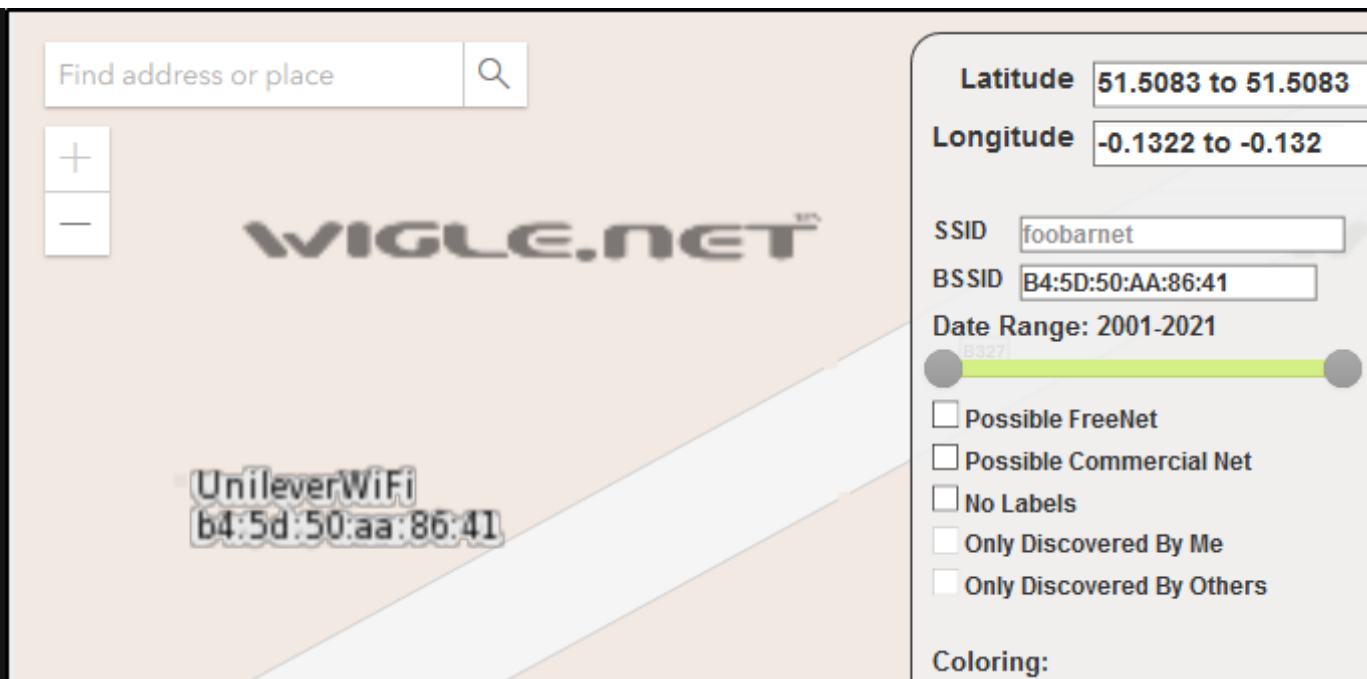
Questions

What is this users avatar of?

> Twitter - it is a cat.

What city is this person in?

> Github - London

What's the SSID of the WAP he is connected to?

> Wigle - UnileverWiFi

What is his personal email address?

Github - OWoodflint@gmail.com

What site did you find his email address on?

Github

Where has he gone on holiday?

Wordpress - New York

What is this persons password?

Wordpress - penn{censored}.!

Zach Heller - 2021