OhSINT || THM WriteUp

By: Ian Jude T.

Introduction:

The purpose of this writeup is document the steps I took to complete Tryhackme.com (THM)'s room; OhSINT.

Figure 1Windows XP Background

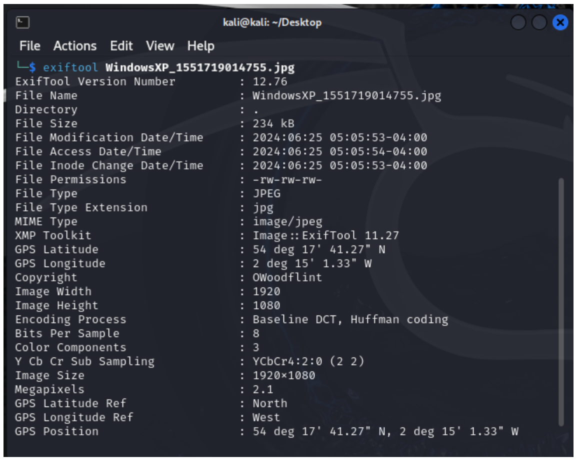
To complete this room, I must gather information I can possibly get with just one photo, and answer the questions.

Resource/ Tools Used

- Exiftool package
- Google Dorking Techniques
- WiGLE: Wireless Network Mapping

#1 What is the user's avatar of?

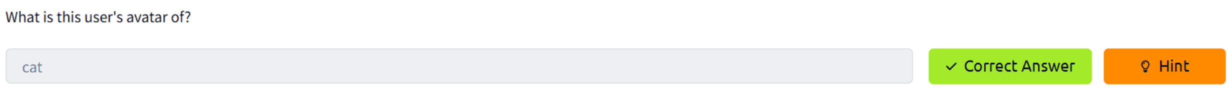
In order to extract details from the image, I checked the metadata of the photo using Exiftool package on Kali Linux.



```
└─$ exiftool WindowsXP_1551719014755.jpg
ExifTool Version Number         : 12.76
File Name                       : WindowsXP_1551719014755.jpg
Directory                       : .
File Size                       : 234 kB
File Modification Date/Time     : 2024:06:25 05:05:53-04:00
File Access Date/Time           : 2024:06:25 05:05:54-04:00
File Inode Change Date/Time     : 2024:06:25 05:05:53-04:00
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)
Image Size                      : 1920×1080
Megapixels                      : 2.1
GPS Latitude Ref                : North
GPS Longitude Ref               : West
GPS Position                    : 54 deg 17' 41.27" N, 2 deg 15' 1.33" W
```

Figure 2: Metadata of the Windows XP Background

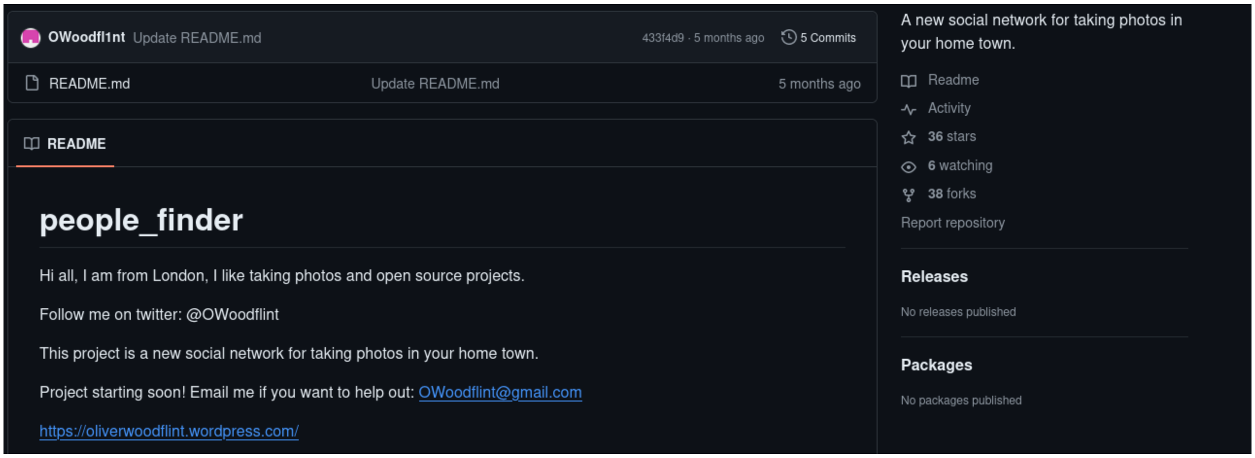
Through the metadata, I was able to find a possible user who is “OWoodflint”. Searching the “OWoodflint” on Google, I was able to find a Twitter account with a cat avatar.


What is this user's avatar of?

cat

#2 What city is this person in?

Through Google query, As OWoodflint disclose where it lives, I was able to find what city he resides.


OWoodfl1nt Update README.md 433f4d9 · 5 months ago 5 Commits

README.md Update README.md 5 months ago

README

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.

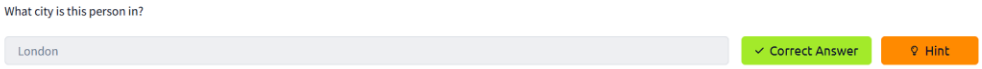
Project starting soon! Email me if you want to help out: OWoodflint@gmail.com

https://oliverwoodflint.wordpress.com/

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

Figure 3: OWoodflint's github

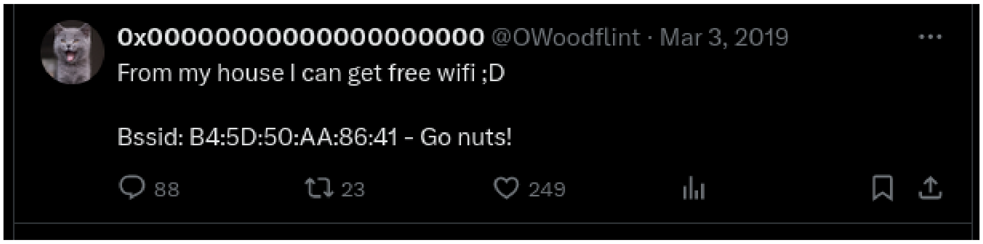
As per on Github post, OWoodflint lives on London.


What city is this person in?

London

#3 What is the SSID of the WAP he connected to?

I use an online tool [WiGLE: Wireless Network Mapping]() in order to find his SSID. Finsing his SSID is not an easy task and it is also time consuming.

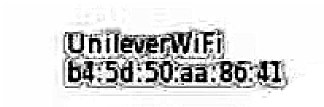

0x00000000000000000000 @OWoodflint · Mar 3, 2019

From my house I can get free wifi ;D

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

Figure 4: OWoodflint BSSID

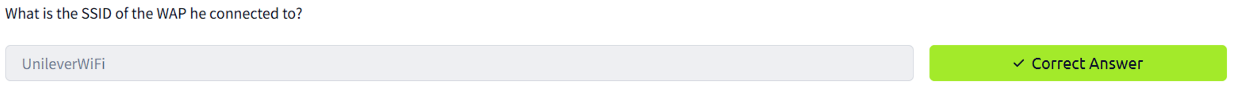
To start my SSID search, I use the BSSID he posted on Twitter. The BSSID (Basic Service Set Identifier), is a unique code assigned to each access point in a wireless network. It essentially helps devices identify and connect to the right access point within the network.



UnileverWiFi
b4:5d:50:aa:86:41

Figure 5: SSID

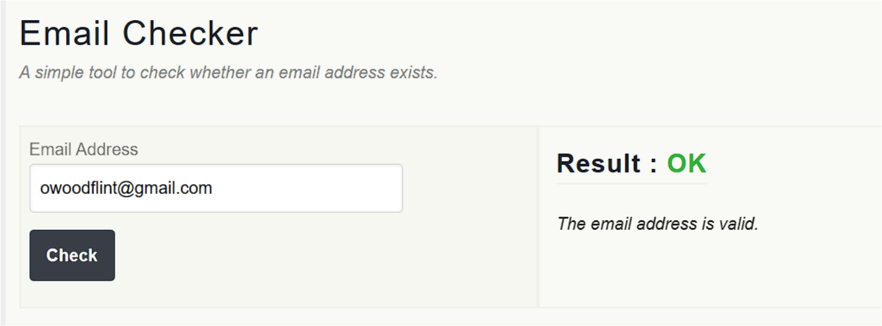
Limiting my search to London, I was able to found out that the SSID of B4:5D:50:aa: B6:41 is UnileverWiFi.



What is the SSID of the WAP he connected to?

UnileverWiFi

#4 - #5 What is personal email address and What site did you find his email address on?



Email Checker

A simple tool to check whether an email address exists.

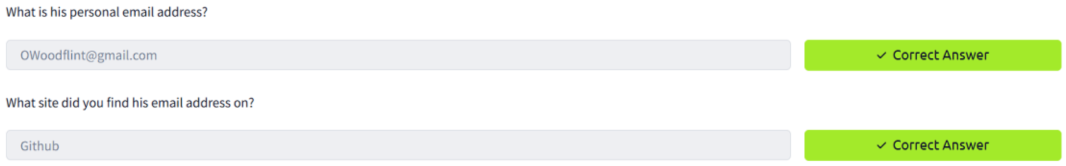
Email Address: owoodflint@gmail.com

Result : OK

The email address is valid.

Figure 6: OWoodflint email

Back to Figure 3, I able to find his personal email address on Github, and his email address is OWoodflint@gmail.com. Verifying if the email address is valid, I use Email Checker - Verify Email Address Online (email-checker.net). Based from the results, the email address he provided is a valid email address.



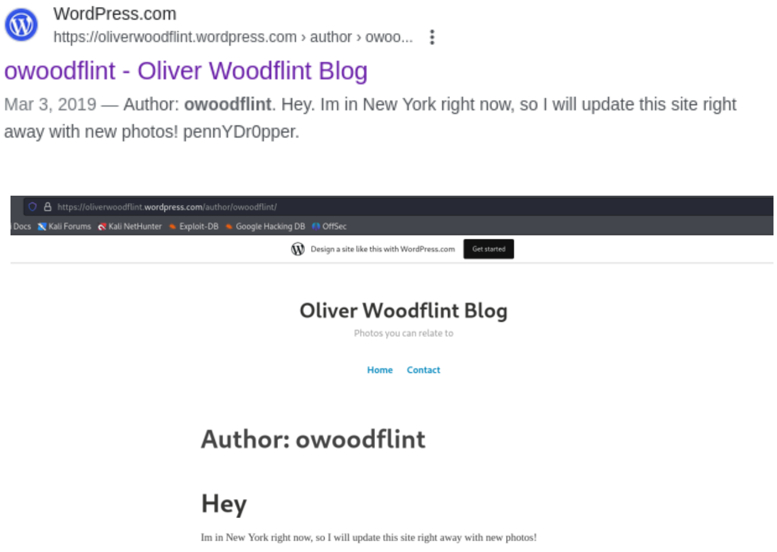
What is his personal email address?

OWoodflint@gmail.com

What site did you find his email address on?

Github

#6 Where has he gone on holiday?



WordPress.com
https://oliverwoodflint.wordpress.com › author › owoo...

owoodflint - Oliver Woodflint Blog

Mar 3, 2019 — Author: **owoodflint**. Hey. Im in New York right now, so I will update this site right away with new photos! pennYDr0pper.

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

Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Design a site like this with WordPress.com Get started

Oliver Woodflint Blog

Photos you can relate to

Home Contact

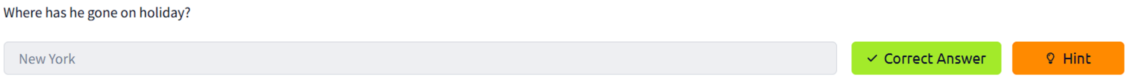
Author: owoodflint

Hey

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

Figure 7: OWoodflint blog website

Google searching his username, I was able to found out where has gone on holiday, by checking his blog post. Based from his post, he is on New York.

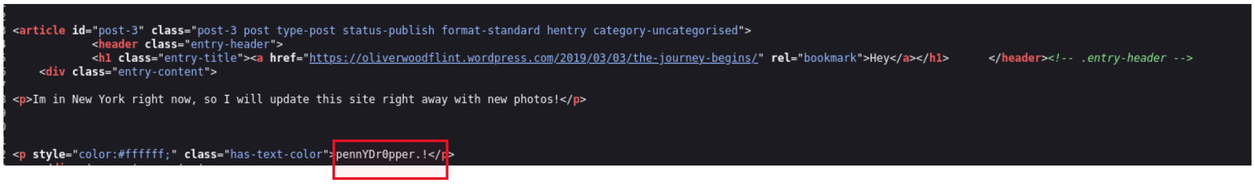


Where has he gone on holiday?

New York

#7 What is this person's password?

Finding his password is tricky, as there are no results found from Google search. I tried to brute force typing the top 10 common password, and no luck. Next is I try my luck on the source code on GitHub and on his blogsite. What I checked on the source code is with a variable name of "pwd", "pass", "password", "pWord". No luck on GitHub, I saw something weird on his blogsite.



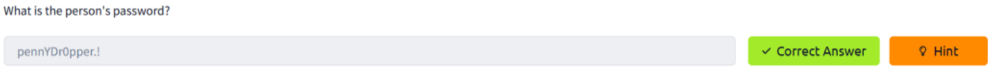
```
<article id="post-3" class="post-3 post type-post status-publish format-standard hentry category-uncategorised">
            <header class="entry-header">
            <h1 class="entry-title"><a href="https://oliverwoodflint.wordpress.com/2019/03/03/the-journey-begins/" rel="bookmark">Hey</a></h1>      </header><!-- .entry-header -->
    <div class="entry-content">

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


<p style="color:#ffffff;" class="has-text-color">pennYDr0pper.!</p>
```

Figure 8: Password

Crosschecking the blogsite (Figure 7) and Figure 8, it is noticeable that the "pennYDr0pper" is not visible on the blogsite. It is confirmed that the password is "pennYDr0pper".



What is the person's password?

pennYDr0pper.!