Osint tryhackme Challenge

• Today, we will be solving tryhackme.com's “OhSINT” challenge. The challenge name is derived from the term OSINT which stands for Open Source Intelligence, basically gathering info about an individual based on information accessible by the Internet.
• We start off downloading an image, which is simply the default wallpaper on Windows XP machines.
• From here, my first instinct is to inspect the image for any metadata, which can be done with a tool called **exiftool**. Simply type the **exiftool <image-name-here>** & the output should look something like this:

```
n9@n9:~/fun/thm$ exiftool WindowsXP.jpg
ExifTool Version Number         : 10.80
File Name                       : WindowsXP.jpg
Directory                       : .
File Size                       : 229 kB
File Modification Date/Time     : 2020:03:21 09:02:21-07:00
File Access Date/Time           : 2020:03:21 09:03:09-07:00
File Inode Change Date/Time     : 2020:03:21 09:02:39-07:00
File Permissions                : rw-rw-r--
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"
```

■ As you can see, we get GPS coordinates of where this photo was taken, but the first task on TryHackMe is what the person's avatar is. If we go to the *Copyright section*, we can see a unique name: **OWoodflint**.
■ After Googling the username, we see a twitter user which appears to be who we're searching for.

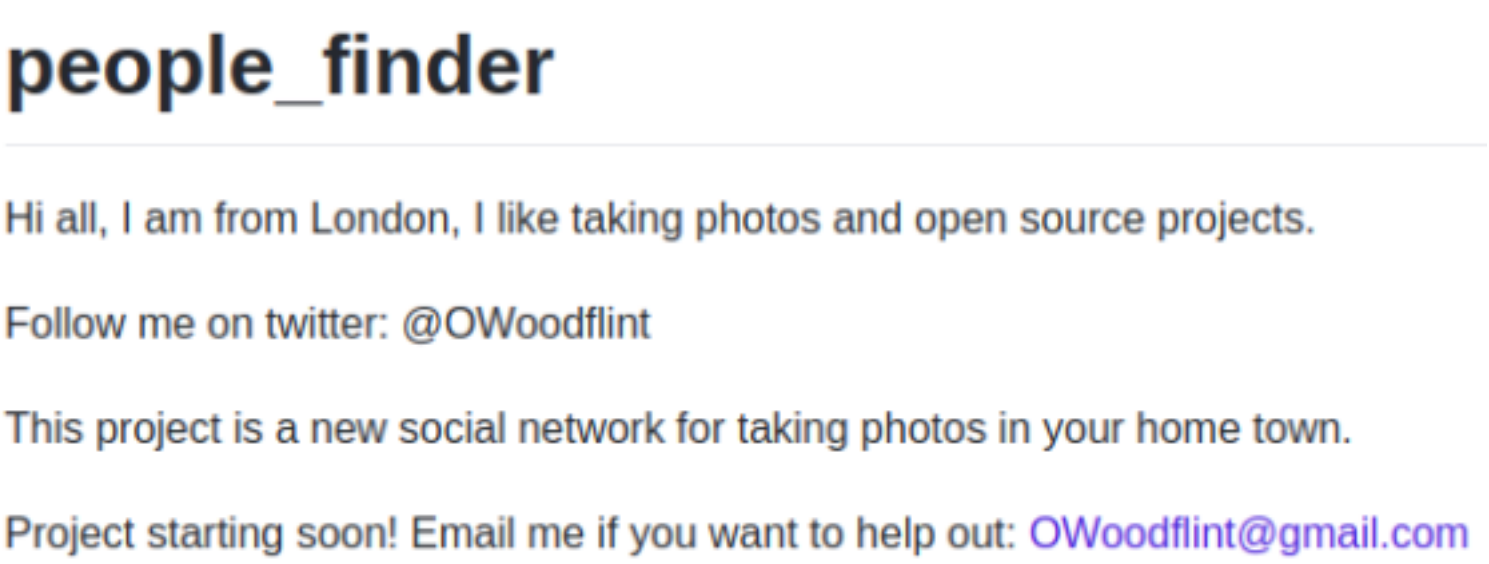
Task 1 solved. 

• After a brief look through OWoodFlint's tweets, we find a tweet about the user's BSSID which I believe is simply a MAC Address of an access point. From this we can solve challenge #2 about what city this person is located in by using WiGLE.net

• 

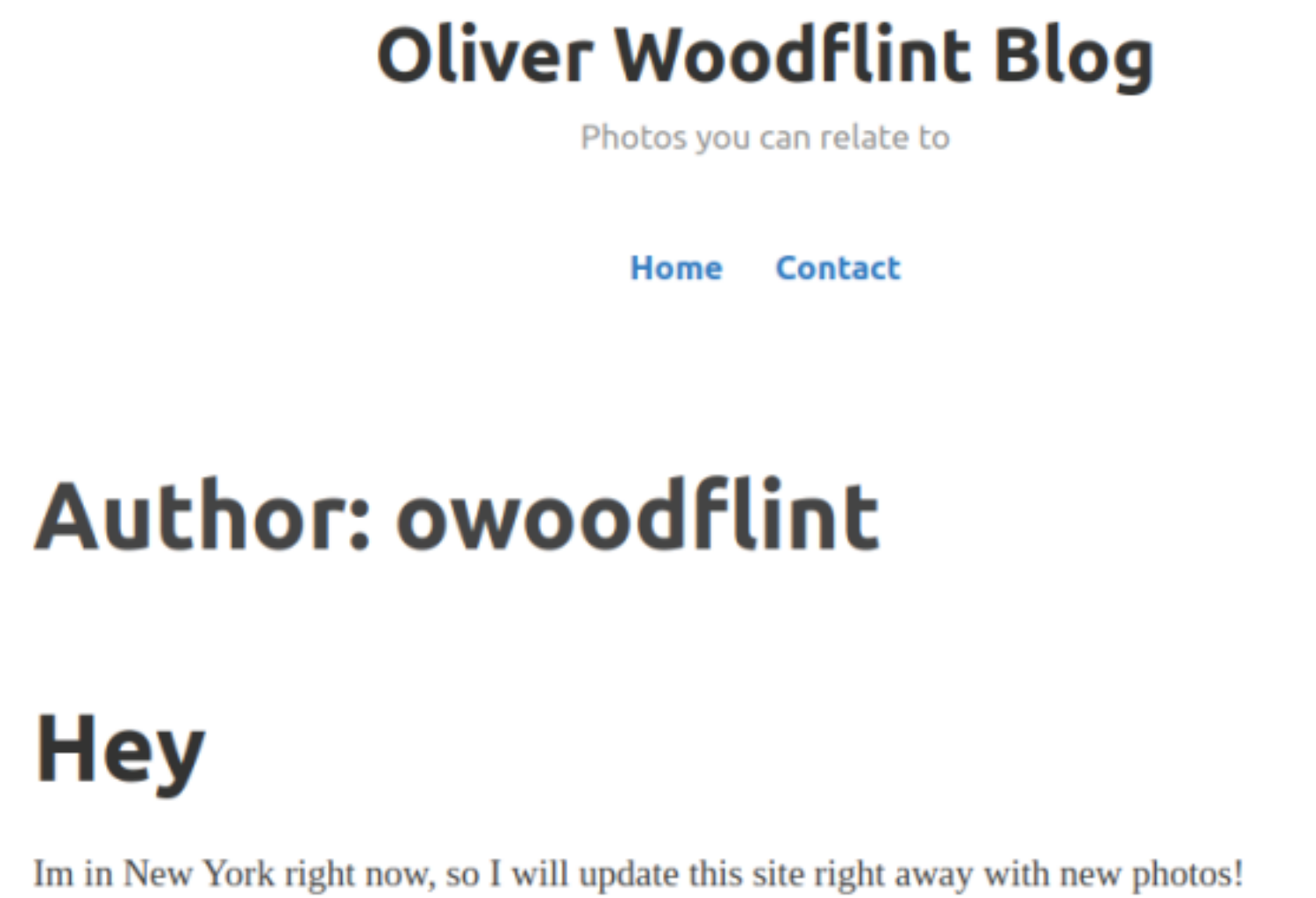
• After searching for the BSSID, we see OWoodflint is located in London & is connected to Unilever's Wifi Network which is called UnileversWifi, which solves the task #3.

• After returning to our original Google search to solve task #4 which is finding his email address, we find a Github.com page which has the following:



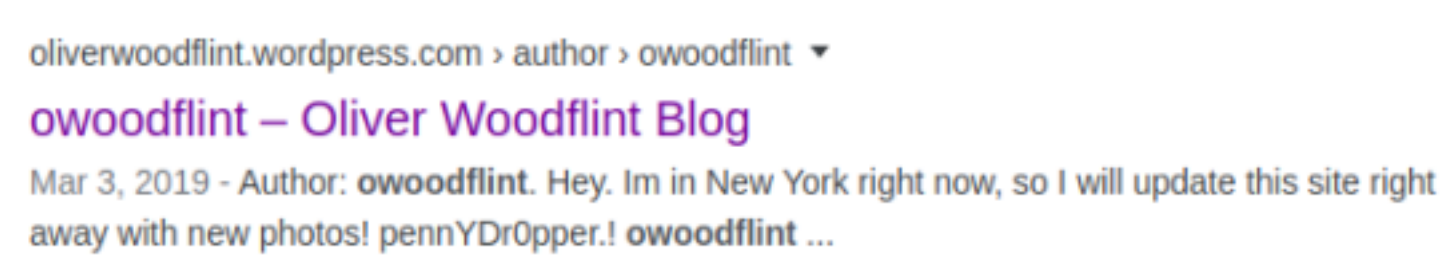
- Boom! Email found!

• Let's return to our Google search to find his vacation spot (task #6). On our 3rd result on our search, we find his Woodpress blog:



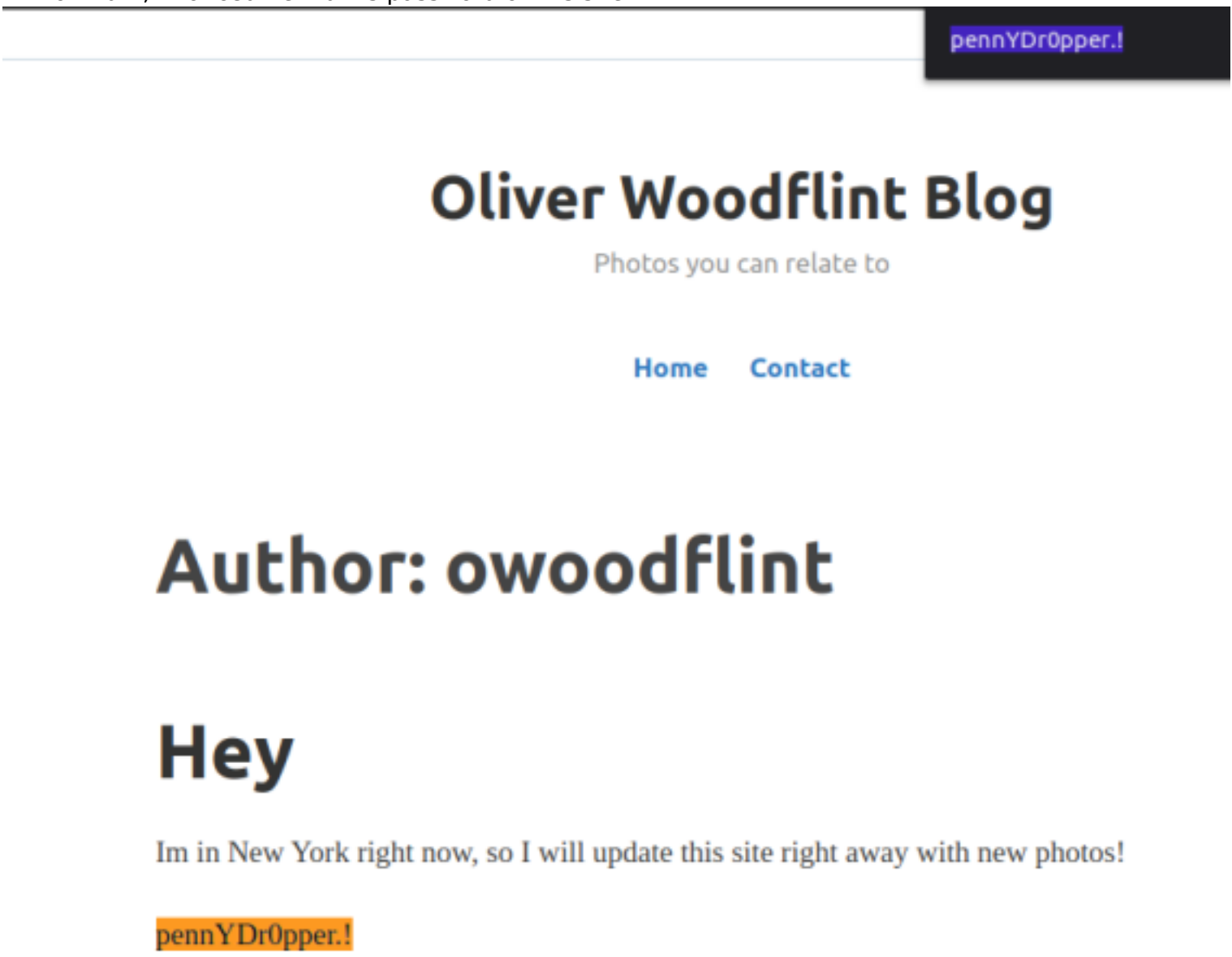
•

• As we can see, he is New York currently and his full name is Oliver Woodflint.
• Now onto the last task, locating his password. My first thought was okay, we likely have to break into his Wordpress account, probably by brute forcing it, but boy was I wrong!
• After returning back to our search results, I noticed a set of alphanumeric characters that were structured as if it were a password in the preview:



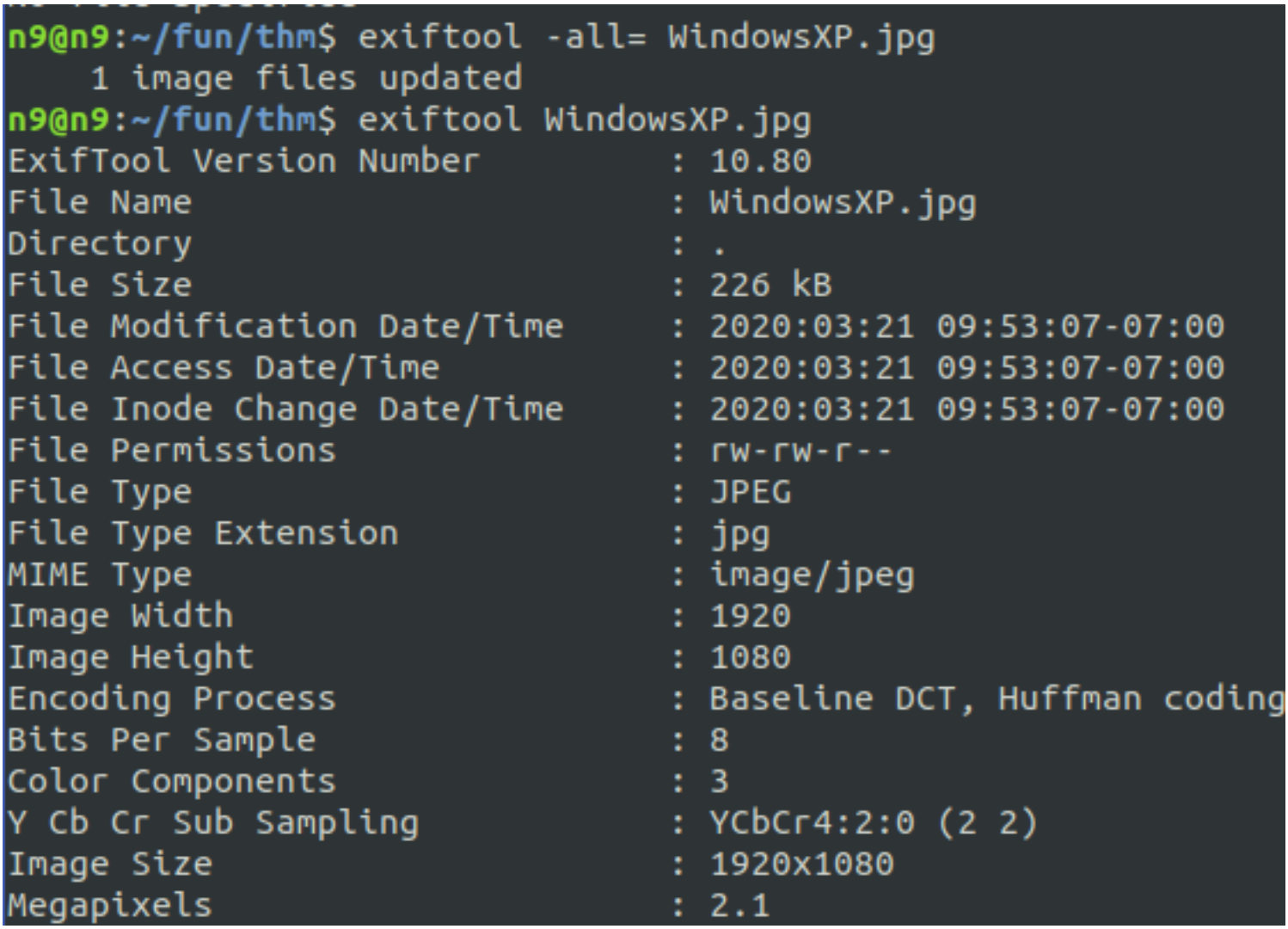
■

■ After going into his blog, I didn't see the pennYDr0pper.! anywhere on the site, but after clicking **ctrl + f** to find it, I noticed he hid his password on his site:



■

• To summarize, we found lots of personal information about our fake person, Oliver Woodflint, all based off a single photo that didn't even contain anything personal. How could you protect yourself from being tracked like this? Well good news for us, social media sites will usually strip all the metadata off photos when we post them, but just in case you want to do that yourself, **exiftool** provides an option to also strip that data.
• Simply use the command exiftool -all= <image-file-here> to strip the identifying metadata off the photo, and if we compare the same photo, one stripped & the other that we originally started with, we can see that all the personal info (GPS coordinates, copyright username, etc) are all gone:



```
n9@n9:~/fun/thm$ exiftool -all= WindowsXP.jpg
    1 image files updated
n9@n9:~/fun/thm$ exiftool WindowsXP.jpg
ExifTool Version Number         : 10.80
File Name                       : WindowsXP.jpg
Directory                       : .
File Size                       : 226 kB
File Modification Date/Time     : 2020:03:21 09:53:07-07:00
File Access Date/Time           : 2020:03:21 09:53:07-07:00
File Inode Change Date/Time     : 2020:03:21 09:53:07-07:00
File Permissions                : rw-rw-r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
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                      : 1920x1080
Megapixels                      : 2.1
```