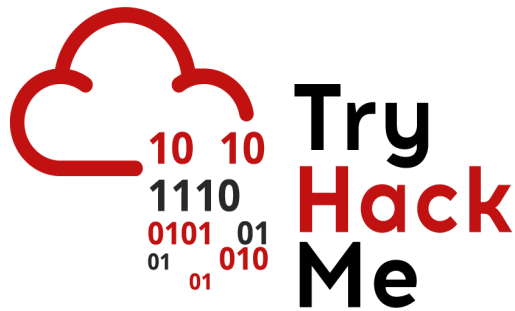


---

# TryHackMe OhSINT

---



[🔗 Click here to access the TryHackMe room](#)

This room doesn't have a vulnerable machine to work with. Rather it requires the use of OSINT (Open Source Intelligence) to answer the questions related to the file given to be downloaded.

## Examining the given file:

- Executing some basic file operations to see if something strikes

```
ls -l
```

```
-rw-rw-r-- 1 black black 234081 Mar 14 15:42 WindowsXP.jpg
```

```
eog WindowsXP.jpg
```

The image is the classic OG WindowsXP background wallpaper.

Let's see what we can extract from this image.

Exiftool is a command line utility that shows the exif information embedded within the image.

```
exiftool WindowsXP.jpg
```

```
ExifTool Version Number      : 12.65
File Name                    : WindowsXP.jpg
Directory                   : .
File Size                    : 234 kB
File Modification Date/Time   : 2024:03:14 15:42:47+05:30
File Access Date/Time        : 2024:03:14 15:44:00+05:30
File Inode Change Date/Time   : 2024:03:14 15:43:33+05:30
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)
Image Size	: 1920x1080
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

- Examining the exif data and searching the web

It appears that the owner of the file might be somewhat related to the copyright owner. Let's browse the web to see if something matches with the given data.

Found some social media accounts under the name [OWoodflint](#).

[Twitter](#)

[GitHub](#)

Exploring the Twitter account for this person, we find that he uses a free Wireless Access Point with the BSSID: [B4:5D:50:AA:86:41](#)

Also, there's a repository [people\\_finder](#) in the user's GitHub account that gives some relative intelligence about the owner.

Also, the [people\\_finder](#) repo shows that there's a blog website of this user on [Wordpress](#).

Exploring the blog, gives some more relevant details such as the statement:

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

which might be the answer to one of the THM Questions.

Looking up in the source code of the Wordpress blog, something peculiar comes up:

```
<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>
</div><!-- .entry-content -->
```

There's a white text written in the HTML page, `pennYDr0pper. !`, which might be the person's password.


## THM Questions:

- Q1: What is this user's avatar of?  
A: `cat`
- Q2: What city is this person in?  
A: `London`
- Q3: What is the SSID of the WAP he connected to?  
A: `UnileverWifi`
- Q3: What is his personal email address?  
A: `owoodflint@gmail.com`
- Q4: What site did you find his email address on?  
A: `GitHub`
- Q5: Where has he gone on holiday?  
A: `New York`
- Q6: What is the person's password?  
A: `pennYDr0pper. !`

---

---

 Created by [Jayaditya Dev](#)

 Find me on [GitHub](#)

---

---