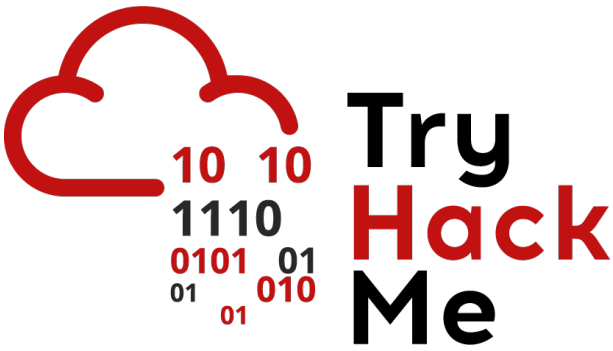
Writeup: Sala *OhSINT*

Autor: Ismaeldevs

Plataforma: TryHackMe

4 de julio de 2025



Índice

1. Introducción

Esta sala es un desafío de introducción a la Inteligencia de Fuentes Abiertas (OSINT) y se destaca por como la información pública puede utilizarse para descubrir una cantidad increíble de datos personales.

2. Desafío

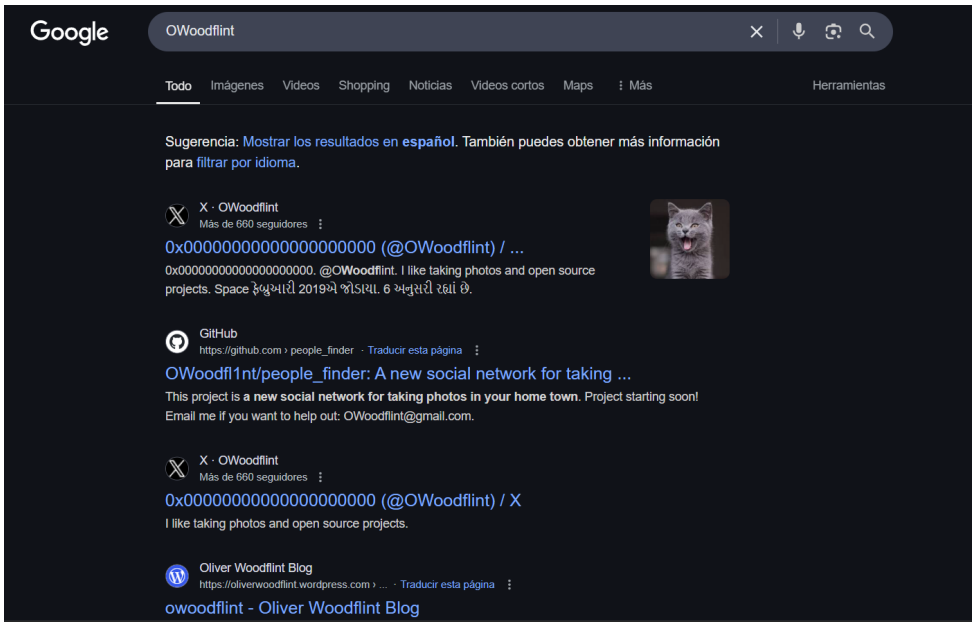
La sala se compone de 7 flags y para iniciar debemos descargar un archivo de imagen llamada WindowsXP.jpg

Al descargar la imagen comenzamos averiguando que datos ocultos puede contener, para ello usamos una herramienta llamada **Exiftool**.

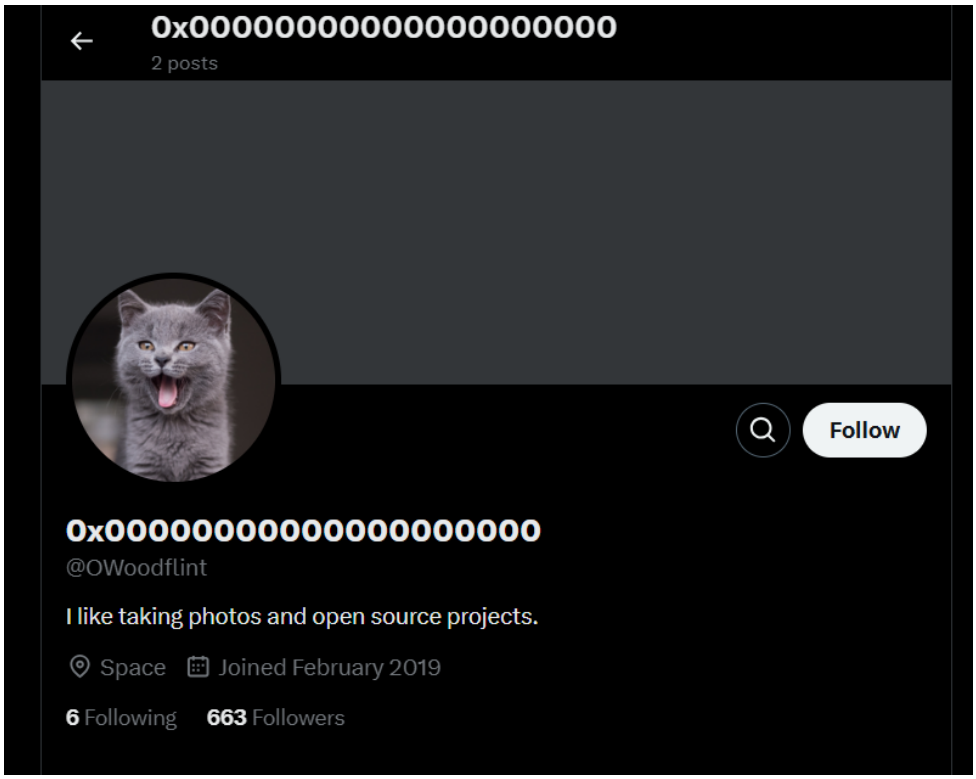
```
┌──(kali㉿kali)-[~]
└─$ exiftool /home/kali/Downloads/WindowsXP_1551719014755.jpg
ExifTool Version Number         : 13.25
File Name                       : WindowsXP_1551719014755.jpg
Directory                       : /home/kali/Downloads
File Size                       : 234 kB
File Modification Date/Time     : 2025:05:18 17:58:28-04:00
File Access Date/Time           : 2025:05:18 17:59:30-04:00
File Inode Change Date/Time     : 2025:05:18 17:58:28-04:00
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)
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

┌──(kali㉿kali)-[~]
└─$
```

Analizando atentamente los metadatos de la imagen podemos encontrar en el apartado Copyright un nombre el cual es **OWoodflint**. Procedemos a ir a google y colocar en el buscador el nombre para averiguar más información.

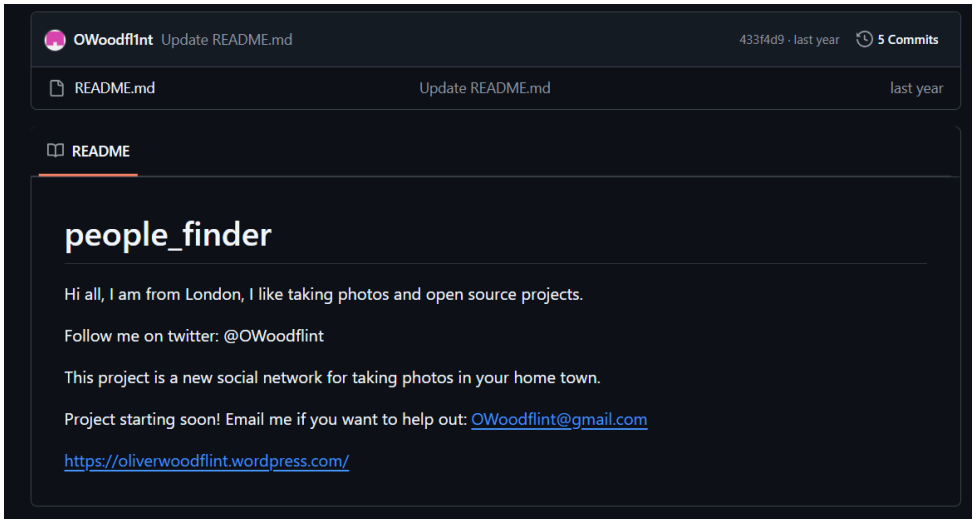


Nos saltan varios enlaces relacionados con el nombre en cuestión y podemos comenzar a responder algunas preguntas de la sala gracias a la busqueda realizada. Primero ingresamos a **X** (antes twitter) y analizamos su perfil para obtener la primera flag.



Pregunta: What is this user's avatar of?
Respuesta: Cat

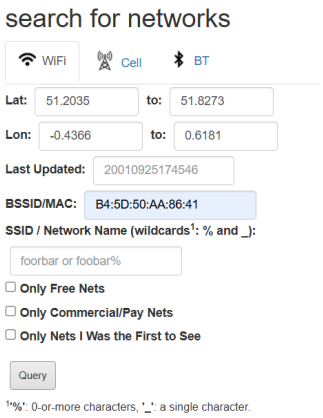
La siguiente flag es **de que ciudad es esta persona?**, para conseguir la respuesta de la pregunta debemos volver a google e ingresar a su perfil de **GitHub**. A simple vista podemos encontrar un README.md donde nos dice que esta persona es de Londres.



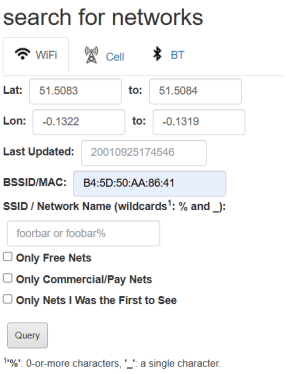
Pregunta: What city is this person in?
Respuesta: Respuesta: London

Ahora la tercera flag nos consulta **Cuál es el SSID del WAP al que se conectó?**, para ello vamos a volver a su perfil de **X** y revisaremos uno de sus publicaciones donde encontramos información respectiva.

Estudiando y siendo curioso encontre una forma de obtener más información a partir de una dirección BSSID gracias al sitio de **wigle.net**. Una vez en la página podemos hacer una busqueda de BSSID que nos permitira encontrar el SSID de su red wifi.

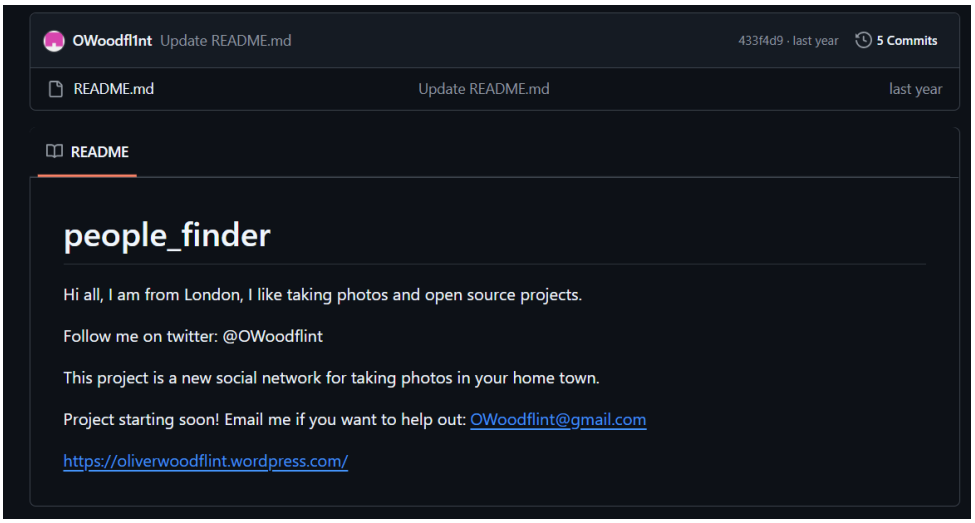


Gracias a este sitio web podemos conocer el SSID de la persona y contestar la siguiente flag de la sala.



Pregunta: What is the SSID of the WAP he connected to?
Respuesta: **UnileverWiFi**

Ahora nos preguntan **Cuál es la dirección email de esta persona?**, para responder a esta flag volvemos al perfil de **GitHub** de la persona y en el mismo README.md podemos encontrar su correo electrónico.



Pregunta: What is his personal email address?
Respuesta: **OWoodflint@gmail.com**

También respondemos la siguiente flag **En qué sitio encontraste su dirección de correo electrónico?**

Pregunta: What site did you find his email address on?
Respuesta: **GitHub**

Ahora la siguiente flag nos preguntan **Adonde se fue de vacaciones?**. Revisando su perfil de **X** y de **GitHub** no encontraba respuestas pero hay un tercer enlace en google relacionado con la persona que nos lleva a un Blog de **WordPress** donde público información donde nos dice que estuvo de vacaciones en New York.

Pregunta: Where has he gone on holiday?
Respuesta: **New York**

La última flag nos pregunta **Cuál es la contraseña de esta persona?**. Esta fue la parte mas difícil de la sala ya que en ningún perfil del usuario había respuestas o pistas que nos ayudará a conseguir la contraseña pero revisando el código fuente del sitio de **WordPress** había una línea de código un tanto rara ya que era una etiqueta de parrafo donde el texto era del mismo color del sitio del blog para lograr no ser visible tan fácilmente y el texto insertado resulto ser la contraseña que buscamos de la persona.

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

Pregunta: What is the person's password?
Respuesta: **pennYDr0pper.!**

3. Conclusión

El OSINT demuestra que cualquier dato público como una imagen, un SSID o un nombre de usuario puede convertirse en una veta de inteligencia valiosa si se aplica con curiosidad y método. Esta capacidad obliga al analista a asumir una gran responsabilidad ética: proteger la privacidad propia y ajena mientras se extraen hallazgos.

Además, el proceso de OSINT es iterativo y fomenta un aprendizaje continuo: cada pista confirmada abre la puerta a nuevas hipótesis y técnicas, consolidando la disciplina y la creatividad del investigador.