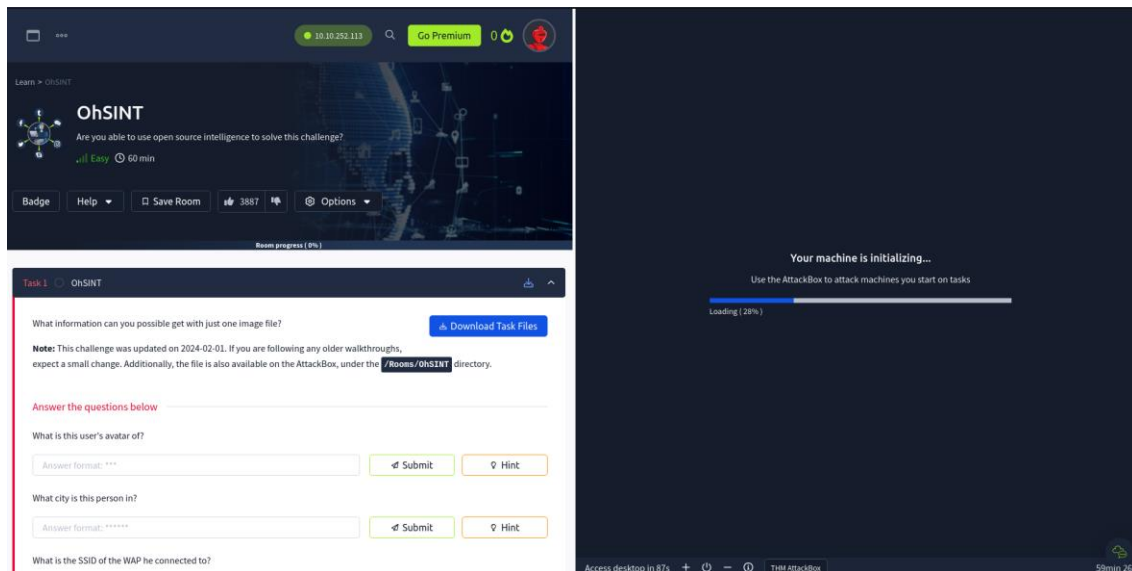




OhSINT

OhSINT es una maquina bastante sencilla que no toma mas de 10 minutos el poder resolverla y el proposito es poder obtener información como Metadatos de una imagen, información de un usuario y como ubicar un AP por su BSSID.

Lo primero es iniciar la maquina mediante la VPN que ofrece TryHackMe, una vez conectada e iniciada la maquina, tienen una hora para poder resolverla sin la membresia mensual.



Hay un botón que dice *Download Task File* el cual es un archivo que como se observa al momento de descargarlo en la maquina anfitrión, en mi caso Kali Linux, esta muestra el fondo de pantalla de Windows XP.



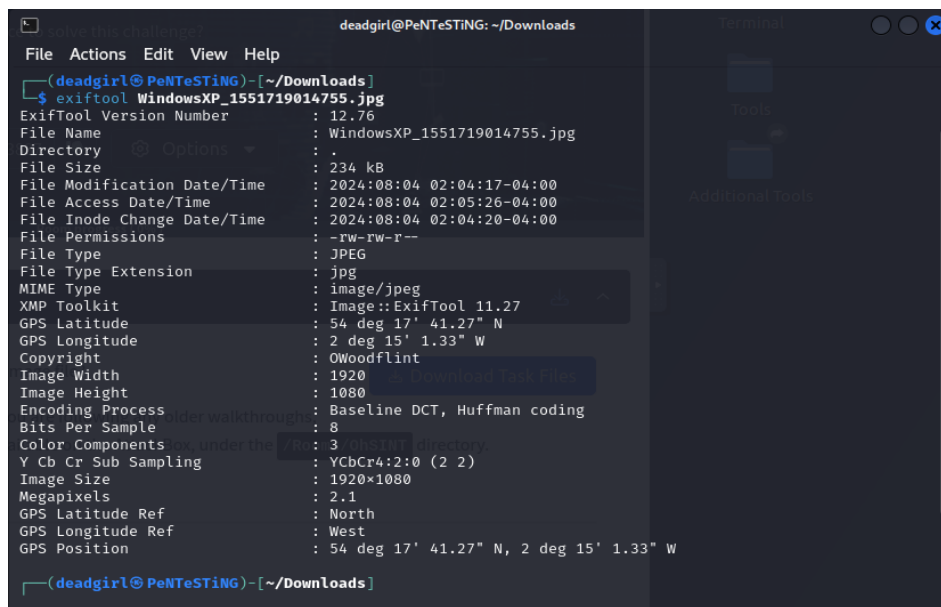


Con la herramienta *exiftool* se podrá obtener información de metadatos de la imagen descargada:

```
# exiftool WindowsXP_1551719014755.jpg
```

```
# strings WindowsXP_1551719014755.jpg
```

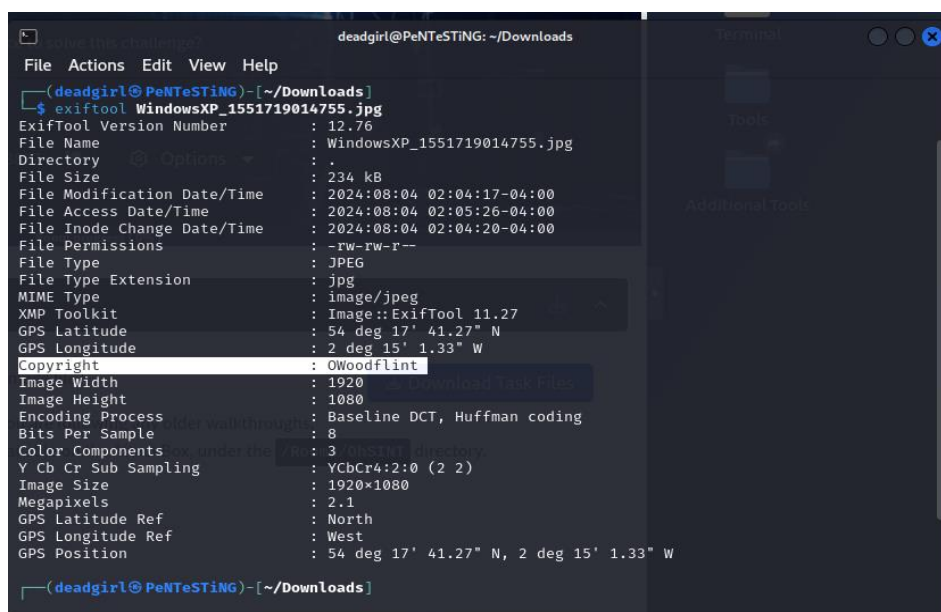
```
# strings WindowsXP_1551719014755.jpg -n 8
```



```
deadgirl@PeNteStiNG: ~/Downloads
File Actions Edit View Help
└─(deadgirl@PeNteStiNG)-[~/Downloads]
$ exiftool WindowsXP_1551719014755.jpg
ExifTool Version Number      : 12.76
File Name                    : WindowsXP_1551719014755.jpg
Directory                   : .
File Size                    : 234 kB
File Modification Date/Time  : 2024:08:04 02:04:17-04:00
File Access Date/Time       : 2024:08:04 02:05:26-04:00
File Inode Change Date/Time  : 2024:08:04 02:04:20-04:00
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                   : 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

└─(deadgirl@PeNteStiNG)-[~/Downloads]
```

Como se observa, en Copyright (derecho de autor), se ve el nombre de quien tomo la imagen, en esta oportunidad el dueño de la imagen es **OWoodflint**.

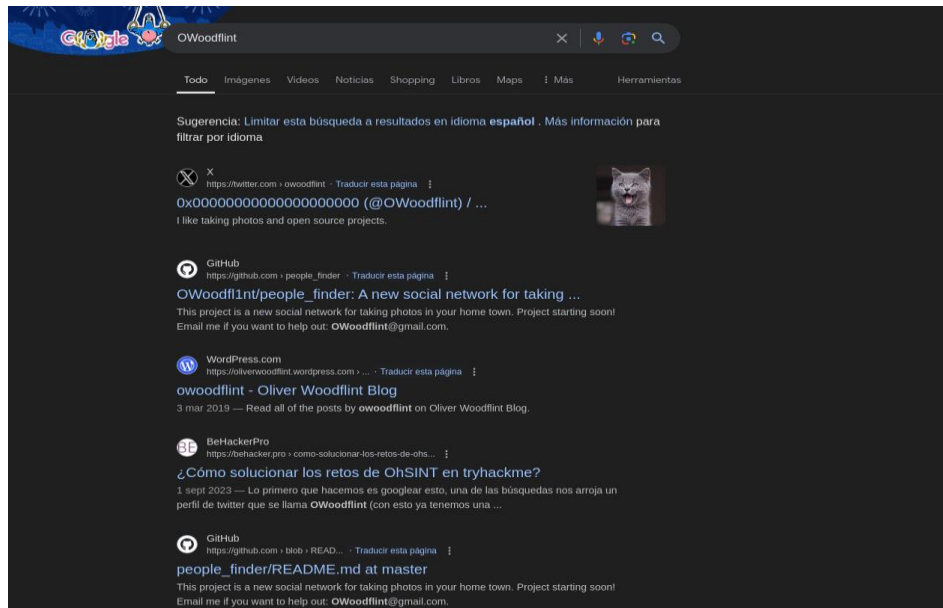


```
deadgirl@PeNteStiNG: ~/Downloads
File Actions Edit View Help
└─(deadgirl@PeNteStiNG)-[~/Downloads]
$ exiftool WindowsXP_1551719014755.jpg
ExifTool Version Number      : 12.76
File Name                    : WindowsXP_1551719014755.jpg
Directory                   : .
File Size                    : 234 kB
File Modification Date/Time  : 2024:08:04 02:04:17-04:00
File Access Date/Time       : 2024:08:04 02:05:26-04:00
File Inode Change Date/Time  : 2024:08:04 02:04:20-04:00
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                   : 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

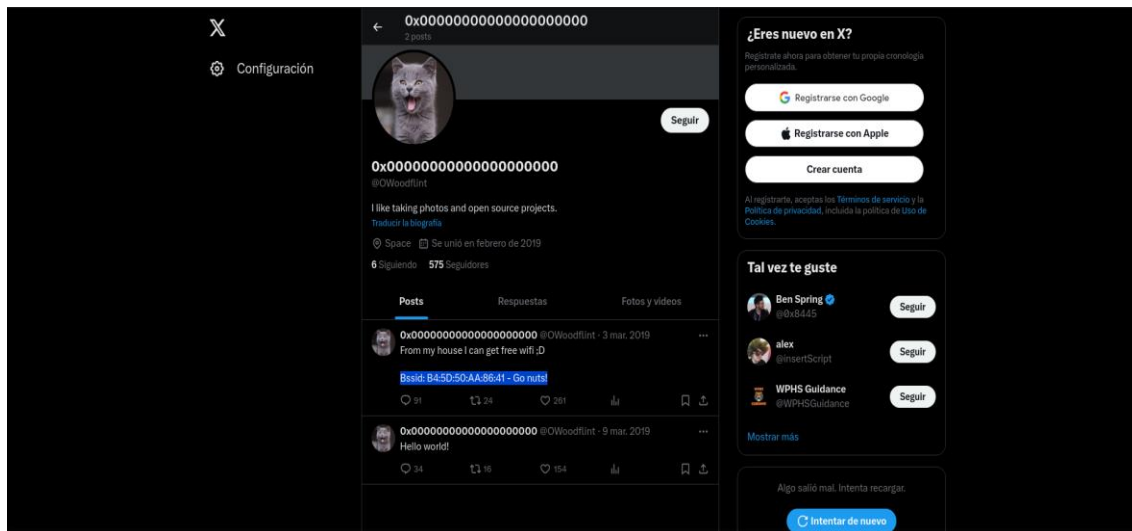
└─(deadgirl@PeNteStiNG)-[~/Downloads]
```



Con el nombre del autor OWoodflint de la imagen utilizar cualquier browser de interes y buscar informacion relevante a su persona, en este caso se observa que posee cuenta en X, GitHub, WordPress, entre otros.



En la plataforma de X hay un tuit el cual muestra un BSSID **B4:5D:50:AA:86:41**





Bien, aquí se responde a la primera pregunta el cual corresponde a *cat* ya que este corresponde a la imagen utilizada como perfil o avatar en la cuenta de X.

What information can you possibly get with just one image file?

[Download Task Files](#)

Note: This challenge was updated on 2024-02-01. If you are following any older walkthroughs, expect a small change. Additionally, the file is also available on the AttackBox, under the `/Rooms/OhSINT` directory.

Answer the questions below

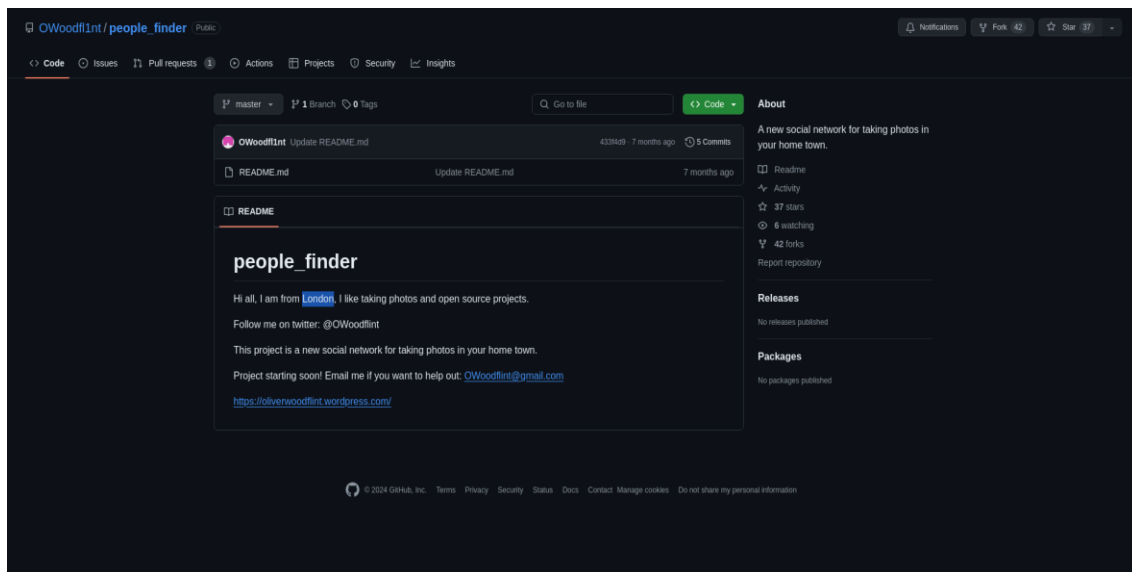
What is this user's avatar of?

cat

✓ Correct Answer

💡 Hint

Posterior y en mi caso continuo con la siguiente cuenta el cual es GitHub, aquí la siguiente pregunta corresponde a la ubicación del creador de la imagen, GitHub muestra e indica que el usuario es de *London*.



What city is this person in?

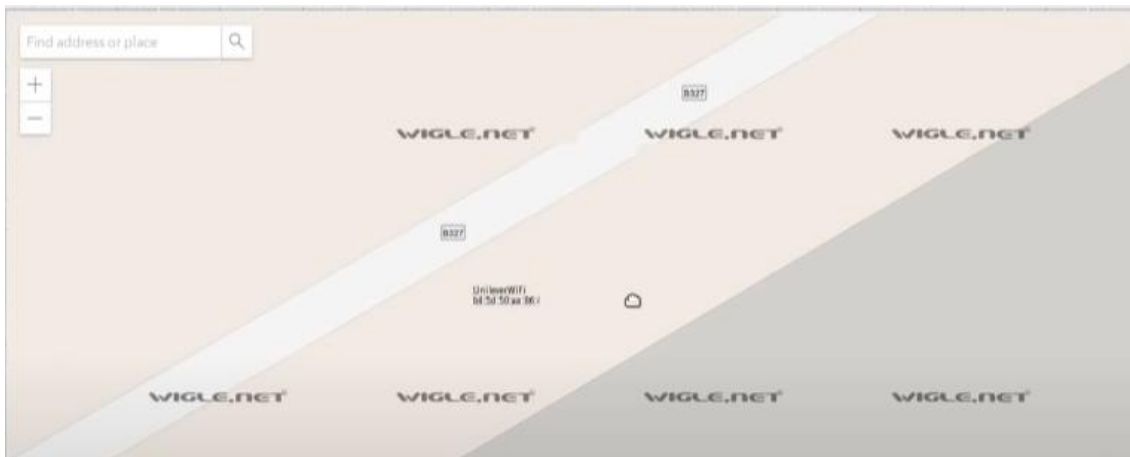
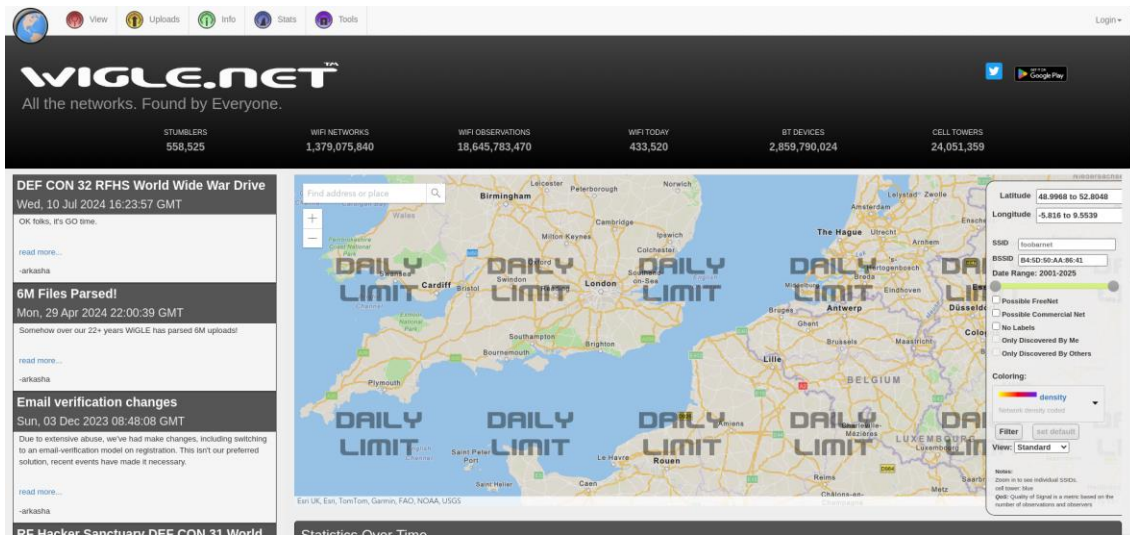
London

✓ Correct Answer

💡 Hint



Con la herramienta web **wigle.net** se puede ubicar un AP con el BSSID, a continuación, se observa que el AP se encuentra ubicado en London con el nombre o SSID **UnileverWiFi**, esto también responde a la siguiente pregunta del cuestionario de la máquina de TryHackMe.



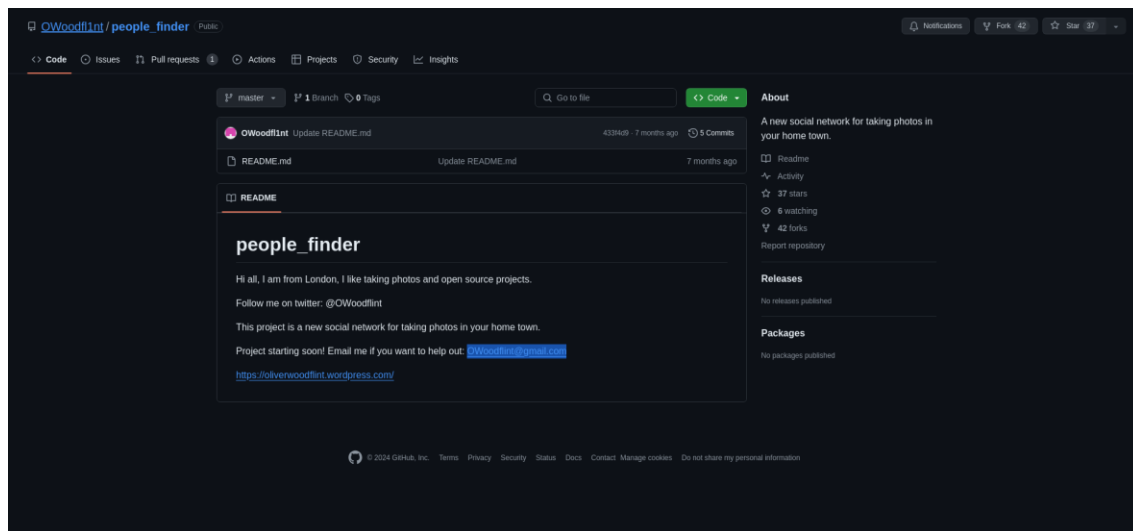
What is the SSID of the WAP he connected to?

UnileverWiFi

✓ Correct Answer



Luego, en el mismo GitHub se observa un correo electrónico, este correo es la respuesta a la siguiente pregunta de la actividad **OWoodflint@gmail.com** también pregunta el sitio el cual se obtuvieron estos resultados el cual corresponde a **GitHub**.



What is his personal email address?

OWoodflint@gmail.com

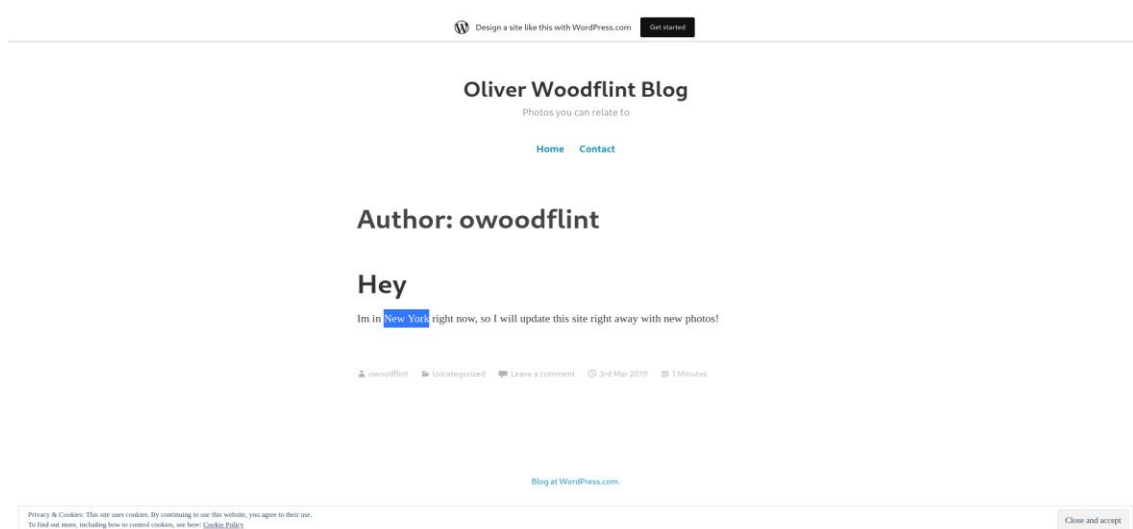
✓ Correct Answer

What site did you find his email address on?

Github

✓ Correct Answer

La siguiente página con informacion del usuario corresponde a WordPress, esto nos permite seguir respondiendo a las preguntas como por ejemplo donde se fue de vacaciones y aquí la respuesta corresponde a **New York**.





New York

 Hint

[illegible][illegible]

pennYDr0pper.!

 Hint



Ya con todas las preguntas respondidas, la actividad se da por concluida y esta entrega un badge indicando que la sala ha sido completada.

Answer the questions below

What is this user's avatar of?

cat

✓ Correct Answer

🔍 Hint

What city is this person in?

London

✓ Correct Answer

🔍 Hint

What is the SSID of the WAP he connected to?

UnileverWiFi

✓ Correct Answer

What is his personal email address?

OWoodflint@gmail.com

✓ Correct Answer

What site did you find his email address on?

Github

✓ Correct Answer

Where has he gone on holiday?

New York

✓ Correct Answer

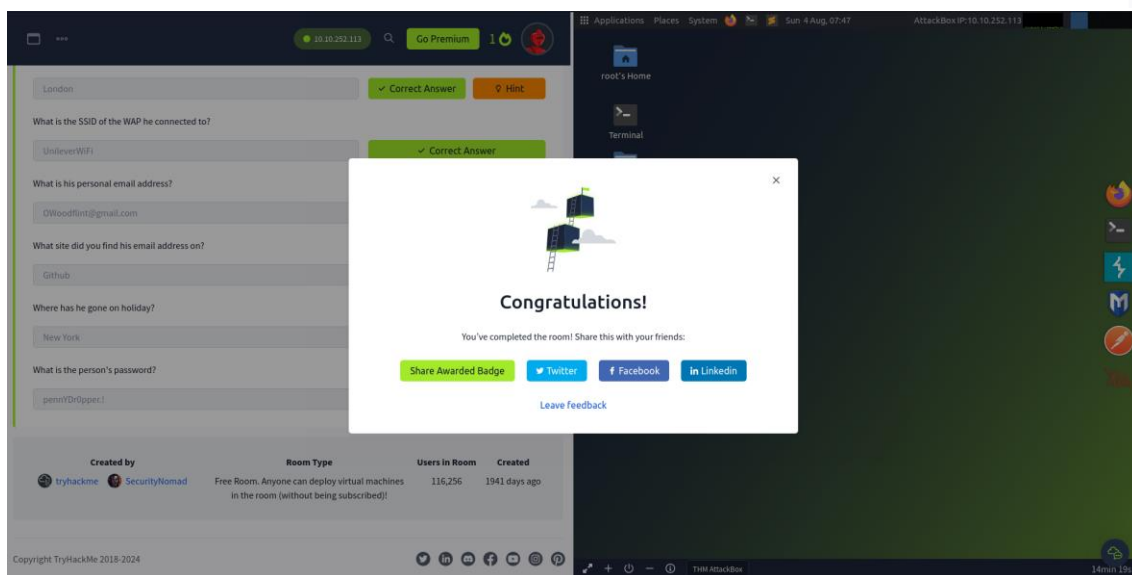
🔍 Hint


What is the person's password?


pennYDr0pper!

✓ Correct Answer

🔍 Hint







OhSINT

Completing the OhSINT
room

Complete the room to earn this badge!