Open-Source Intelligence
HockeyTea1360

OHSINT
A TRY HACK ME WRITE UP

INTRODUCTION

The OhSINT room on TRYHACKME.COM focuses on trying to find information from a regular JPEG file(Image) then using OSINT (open-source intelligence) escalate to discover more information, this is a nice CFT (capture the flag) for beginners to get to play around with the OSINT framework, so what are we waiting for let's dive in.

QUESTIONS WE NEED TO ANSWER

1. What is this user's avatar of?
2. What city is this person in?
3. What is the SSID(Service Set Identifier) of the WAP(Wireless Access Protocol) he connected to?
4. What is his personal email address?
5. What site did you find his personal email address on?
6. Where has he gone on holiday?
7. What is this person's password?

INITIAL GATHERING

One you have downloaded the image it does not show us much at all really it looks to be a simple classic windows default background. So what we need to do is go ahead and find out what properties it has by running a tool called Exiftool(https://en.wikipedia.org/wiki/ExifTool), which will give us some metadata.

What is metadata

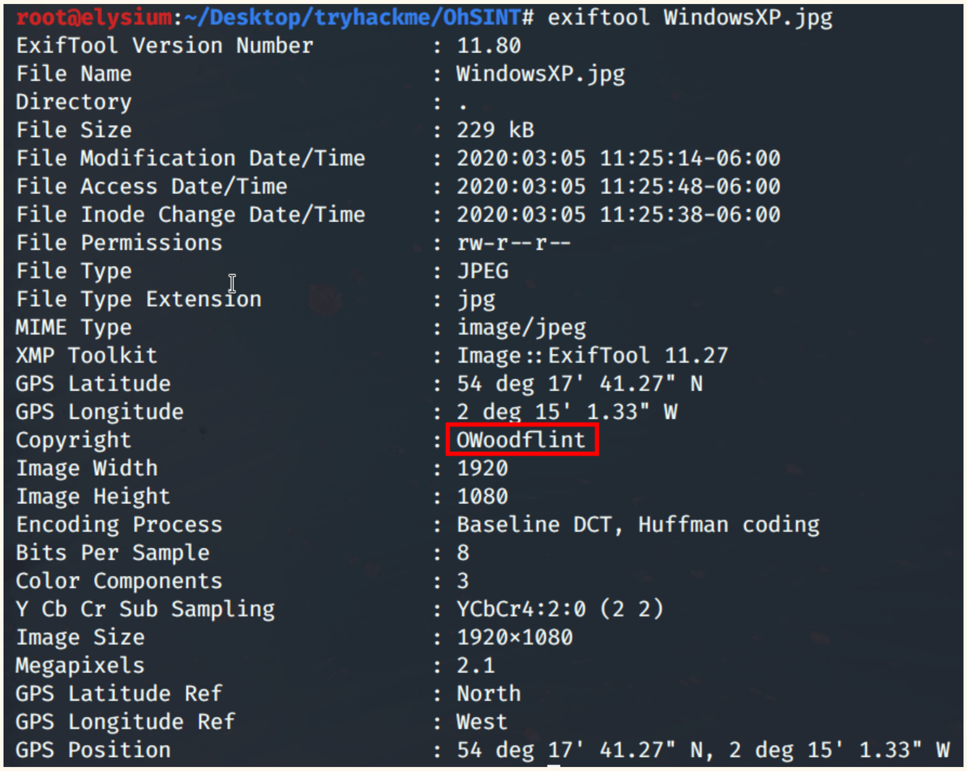
Image meta data is text information related to the image file that is attached to the file. This includes details relevant to the image. EXIF files holds tons of data that can be valuable to any OSINT investigation. It can hold details and is not limited to the list below.

- When the picture was taken
- Where it was taken
- Shutter speed
- Copyright owner
- Type of camera used

And the list goes on

So now we need to open up the EXIFTool so open up the terminal and type:

Exiftool WindowsXP.jng



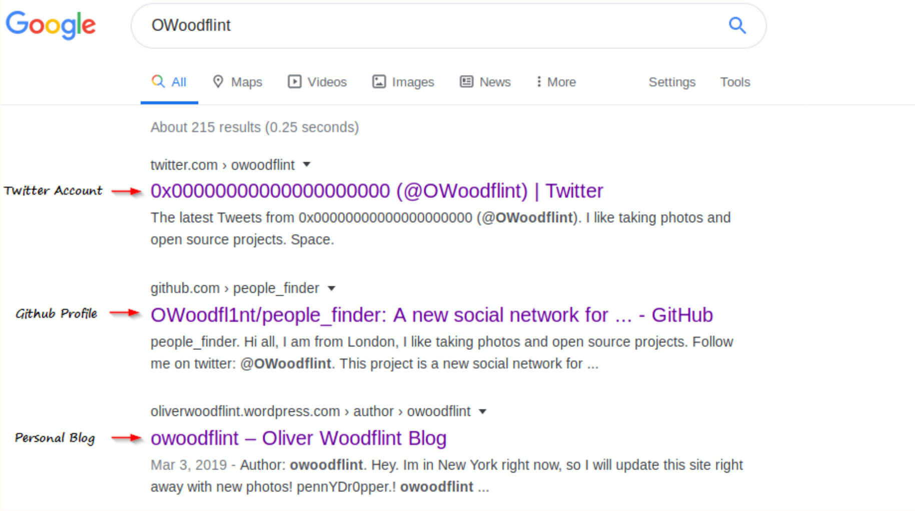
```
root@elysium:~/Desktop/tryhackme/OhSINT# exiftool WindowsXP.jpg
ExifTool Version Number         : 11.80
File Name                       : WindowsXP.jpg
Directory                       : .
File Size                       : 229 kB
File Modification Date/Time     : 2020:03:05 11:25:14-06:00
File Access Date/Time           : 2020:03:05 11:25:48-06:00
File Inode Change Date/Time     : 2020:03:05 11:25:38-06:00
File Permissions                : rw-r--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
```

From the data we can see looking down we have found that the person who has copyrighted the image is **OWoodfint** maybe this can be attributed to someone's name.

So let's go ahead and dive more into this investigation, use a search engine and type in that name.

GOOGLE DORKING

Using google for this or a search engine of your choice and try to gain meaningful data.



About 215 results (0.25 seconds)

twitter.com › owoodflint
0x00000000000000000000 (@OWoodflint) | Twitter
The latest Tweets from 0x00000000000000000000 (@**OWoodflint**). I like taking photos and open source projects. Space.

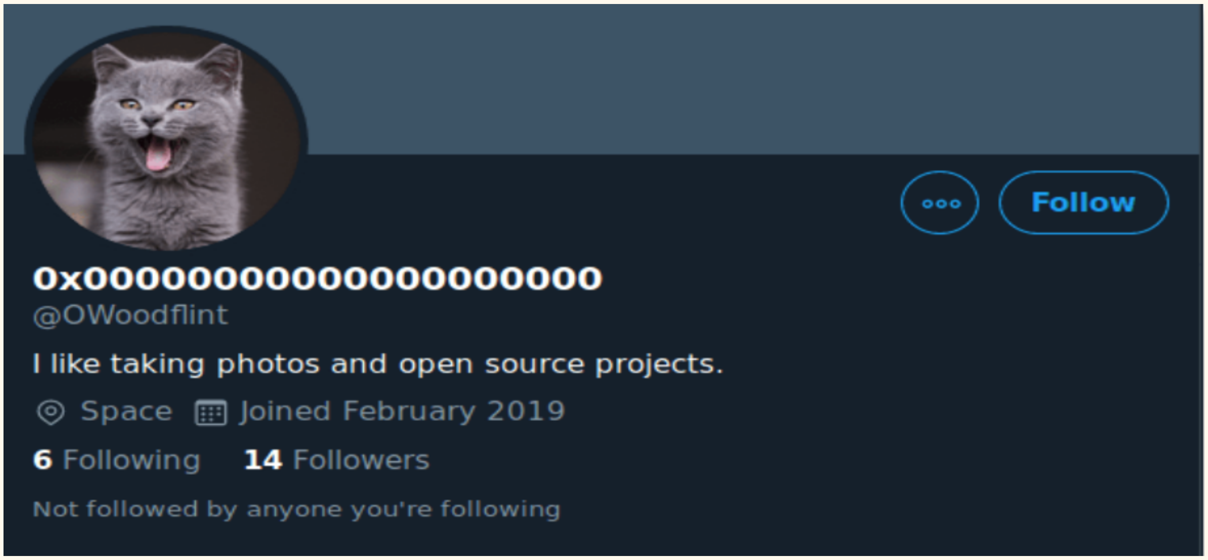
github.com › people_finder
OWoodfl1nt/people_finder: A new social network for ... - GitHub
people_finder. Hi all, I am from London, I like taking photos and open source projects. Follow me on twitter: @**OWoodflint**. This project is a new social network for ...

oliverwoodflint.wordpress.com › author › owoodflint
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.! **owoodflint** ...

From the image above we have found 3 leads connected to the user name we have queried.

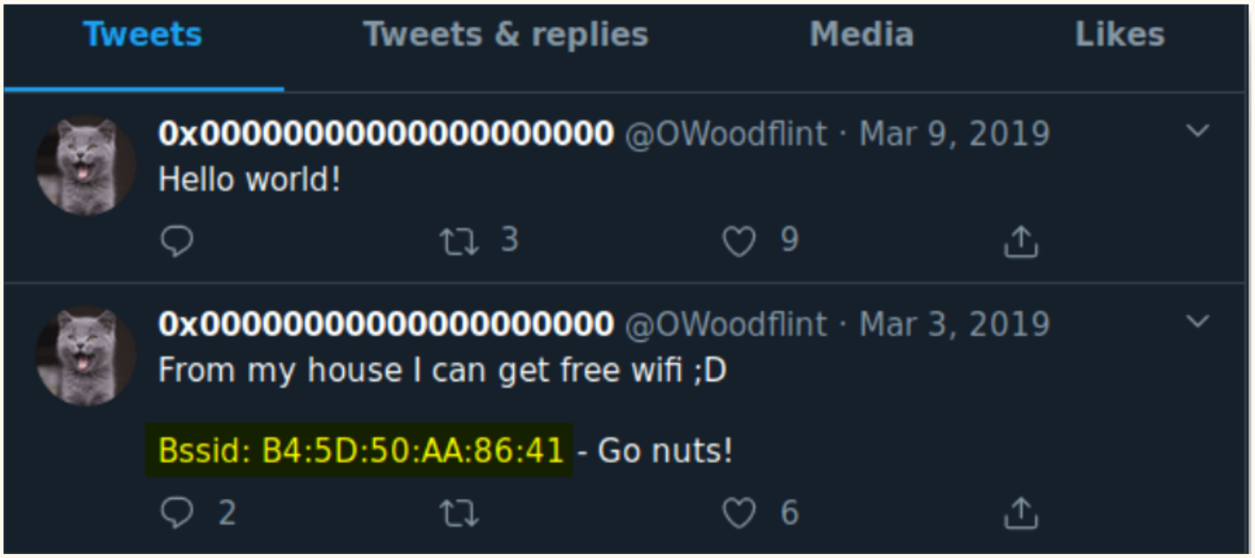
Clicking on Twitter

Clicking onto the twitter link we can answer the first question which is what is the user's avatar, the answer being a **CAT.**



0x00000000000000000000
@OWoodflint
I like taking photos and open source projects.
Space Joined February 2019
6 Following **14** Followers
Not followed by anyone you're following

The following question asks for the user's city. Looking through the profile the account does not reveal anything about a location but if we look closely it shows us a Tweet showing the users Base srt service Identifer.



0x00000000000000000000 @OWoodflint · Mar 9, 2019
Hello world!

0x00000000000000000000 @OWoodflint · Mar 3, 2019
From my house I can get free wifi ;D

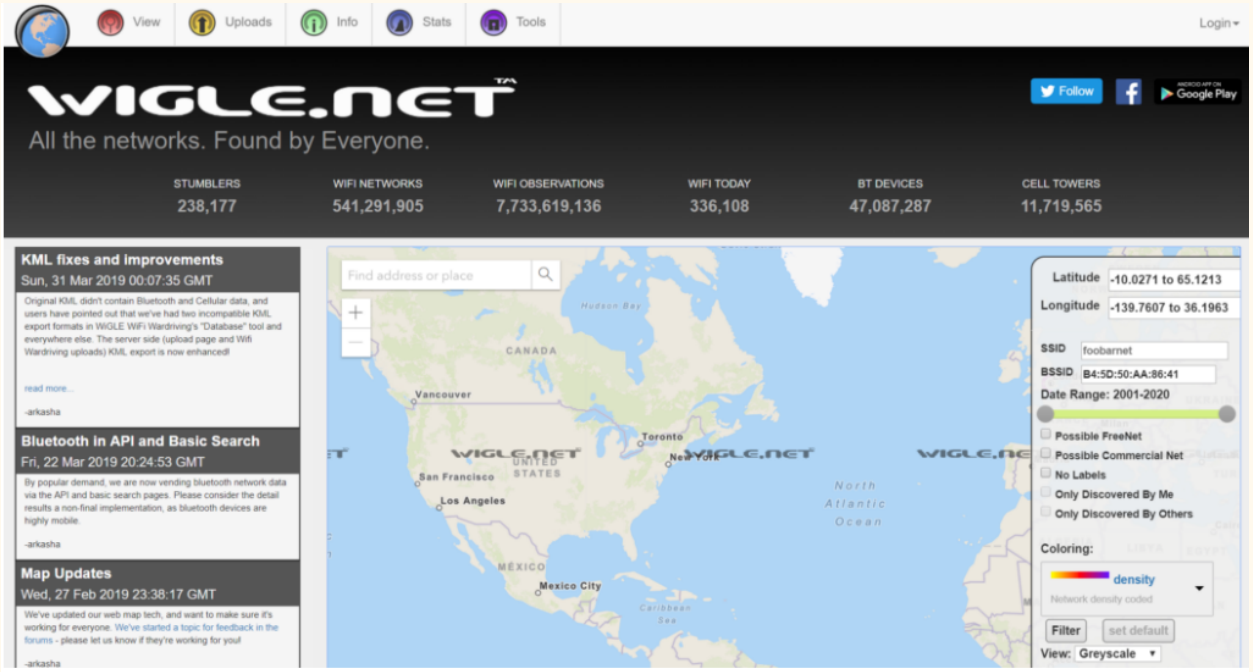
Bssid: B4:5D:50:AA:86:41 - Go nuts!

IDENTIFYING WAPs

Base Set Service Identifier

This is a unique address given to wireless access points (WAP) . It is similar to a mac address, Interesting though there are a few websites to help us track down information about different wireless hotspots all over the globe. These hotspots can be identified using BSSID, SSID,GPS coordinates.

The website we're going to use is wigle.net (it's free and no account is needed) so let's go ahead type in the BSSID(Base Set Service Identifier) into the site.



All the networks. Found by Everyone.

STUMBLERS	WIFI NETWORKS	WIFI OBSERVATIONS	WIFI TODAY	BT DEVICES	CELL TOWERS
238,177	541,291,905	7,733,619,136	336,108	47,087,287	11,719,565

KML fixes and improvements
Sun, 31 Mar 2019 00:07:35 GMT

Original KML didn't contain Bluetooth and Cellular data, and users have pointed out that we've had two incompatible KML export formats in WiGLE WiFi Wardriving's "Database" tool and everywhere else. The server side (upload page and Wifi Wardriving uploads) KML export is now enhanced!

read more...

-arkasha

Bluetooth in API and Basic Search
Fri, 22 Mar 2019 20:24:53 GMT

By popular demand, we are now vending bluetooth network data via the API and basic search pages. Please consider the detail results a non-final implementation, as bluetooth devices are highly mobile.

-arkasha

Map Updates
Wed, 27 Feb 2019 23:38:17 GMT

We've updated our web map tech, and want to make sure it's working for everyone. We've started a topic for feedback in the forums - please let us know if they're working for you!

-arkasha

Latitude: -10.0271 to 65.1213
Longitude: -139.7607 to 36.1963
SSID: foobarnet
BSSID: B4:5D:50:AA:86:41
Date Range: 2001-2020

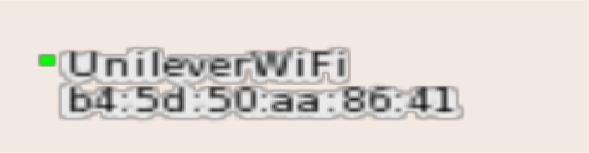
□ Possible FreeNet
□ Possible Commercial Net
□ No Labels
□ Only Discovered By Me
□ Only Discovered By Others

Coloring: density
Network density coded

Filter | set default

View: Greyscale

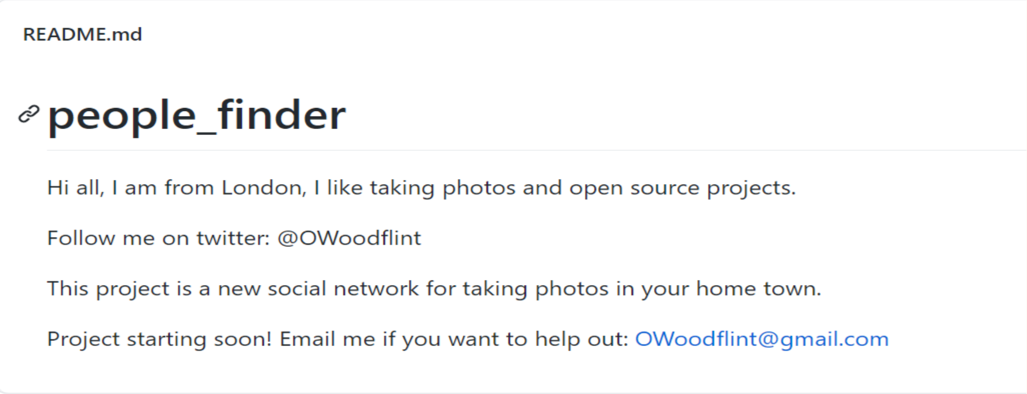
We can see that once we have located the BSSID(Base set service identifier) it brings us to London (if you zoom out you see a purple circle and from there you can zoom in). We collect the SSID data which answers one of our questions.



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

Clicking on Github

So now if we come back to google and select the website GitHub we can see that this now will answer another one of our questions by revealing his email.



README.md

people_finder

Hi all, I am from London, I like taking photos and open source projects.

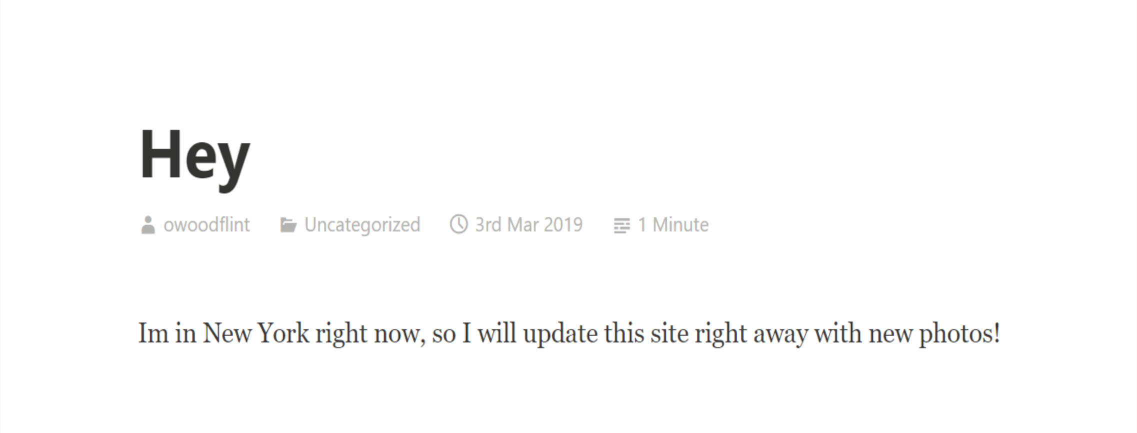
Follow me on twitter: @OWoodflint

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

Clicking on the personal blog

Again heading back to our google search we can now head into his blog which tells us at the time of this challenge he is currently in NewYork

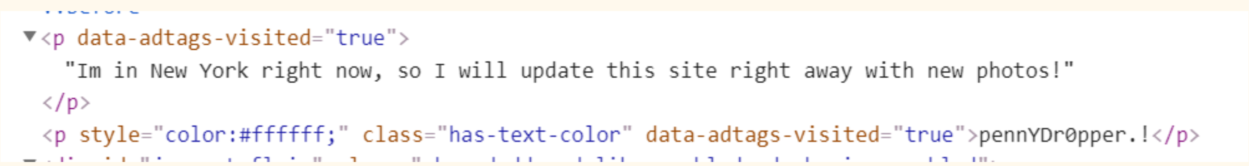


Hey

owoodflint Uncategorized 3rd Mar 2019 1 Minute

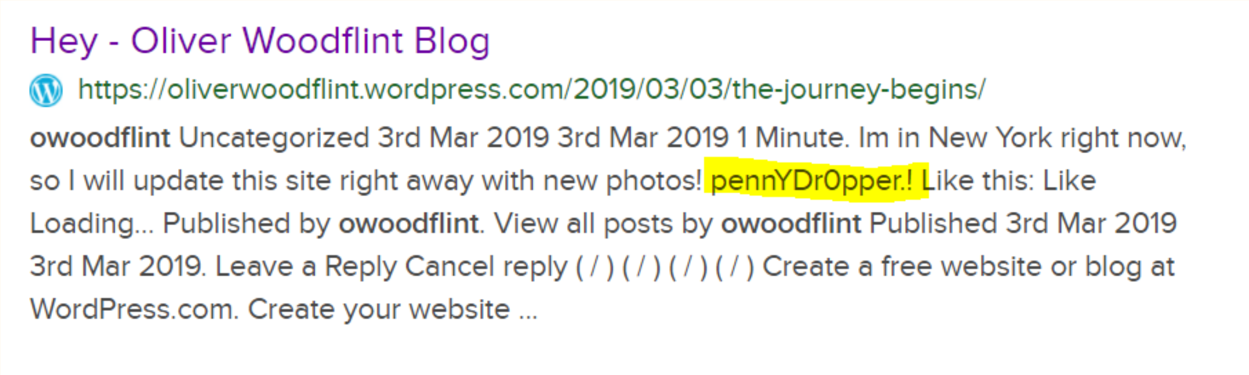
Im in New York right now, so I will update this site right away with new photos!

From here our next question asks us if we can get a password from this, going through the source code we can see the string is well hidden but sticks out as odd.



```
▼<p data-adtags-visited="true">
   "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" data-adtags-visited="true">pennYDr0pper.!</p>
```

Also when looking at the blog post you can see something doesn't look right when you return to google and confirm it.



Hey - Oliver Woodflint Blog

https://oliverwoodflint.wordpress.com/2019/03/03/the-journey-begins/

owoodflint Uncategorized 3rd Mar 2019 3rd Mar 2019 1 Minute. Im in New York right now, so I will update this site right away with new photos! pennYDr0pper.! Like this: Like Loading... Published by **owoodflint**. View all posts by **owoodflint** Published 3rd Mar 2019 3rd Mar 2019. Leave a Reply Cancel reply (/) (/) (/) (/) Create a free website or blog at WordPress.com. Create your website ...

As seen in the picture above we have located the password which is the answer to our final question. THERE WE HAVE IT WE HAVE NOW COMPLETE OUR OhSINT CHALLENGE.

SUMMARY

I just want to share my thoughts with you. I am new to this and trying to learn . The first lesson I have learnt is that it's best not to rush anything but to look at all the results and then dive in to them one at a time and reread the question.

Overall this is a really fun beginner challenge, and can show by knowing a little of where to look and the use of techniques such as google dorking, can show how much information is really out there and how easy it is to find.

RESOURCES USED

- Google dorking
- Information gathering - in short reading
- https://wigle.net

Other things to look at

- OSINT framework
- OSINT Dojo
- Tacelabs.com
- TryHackMe- Geolocating Images
- TryHackMe - WebOSINT