




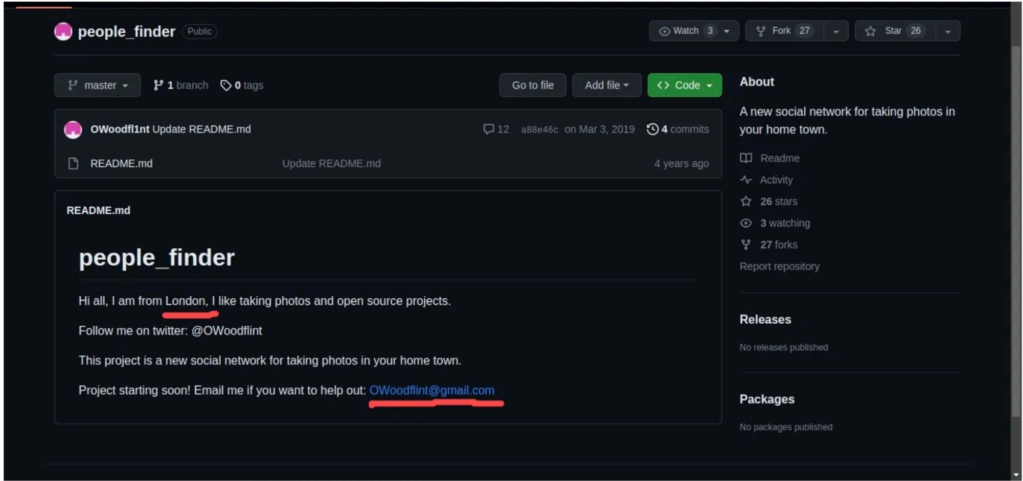
Stick-Cmd OhSint Project journal

Date: 09-17-2024	Entry: 001
Description	Download the image at https://tryhackme.com/r/room/ohsint
Tool(s) used	<p>Used VM box with Kali Linux to run ExifTool on</p> 
Details	<ul style="list-style-type: none">• Who: TryHackMe Practice Room• What: OSINT on the image provided.• Why: To gain real world experience with OSINT investigation techniques.
Additional notes	Depending on the Linux build I had to install ExifTool with the <code>sudo apt install</code> command.

Date: 09-17-2024	Entry: 002
Description	Proceed to use ExifTool to get information on the source image.
Tool(s) used	Kali Linux and Exiftool
Details	<p>ExifTool provided the encoded information on the image file. From this information we were able to glean the copyright holders username: OWoodflint.</p> <pre>ExifTool Version Number : 12.76 File Name : WindowsXP_15.jpg Directory : Downloads File Size : 234 kB File Modification Date/Time : 2024:09:17 13:42:40-04:00 File Access Date/Time : 2024:09:17 13:45:29-04:00 File Inode Change Date/Time : 2024:09:17 13:45:29-04:00 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</pre>
Additional notes	From here I could look up the username on google.

Date: 09-17-2024	Entry: 003
Description	Google Search Username to answer the Question on TryHackMe, "What is this user's avatar of?"
Tool(s) used	Google Search
Details	In order to answer the first question I had to go to OWoodflint's twitter/X account. This was their only social media account. The answer was Cat.
Additional notes	The user also has a GitHub account and a Blog.

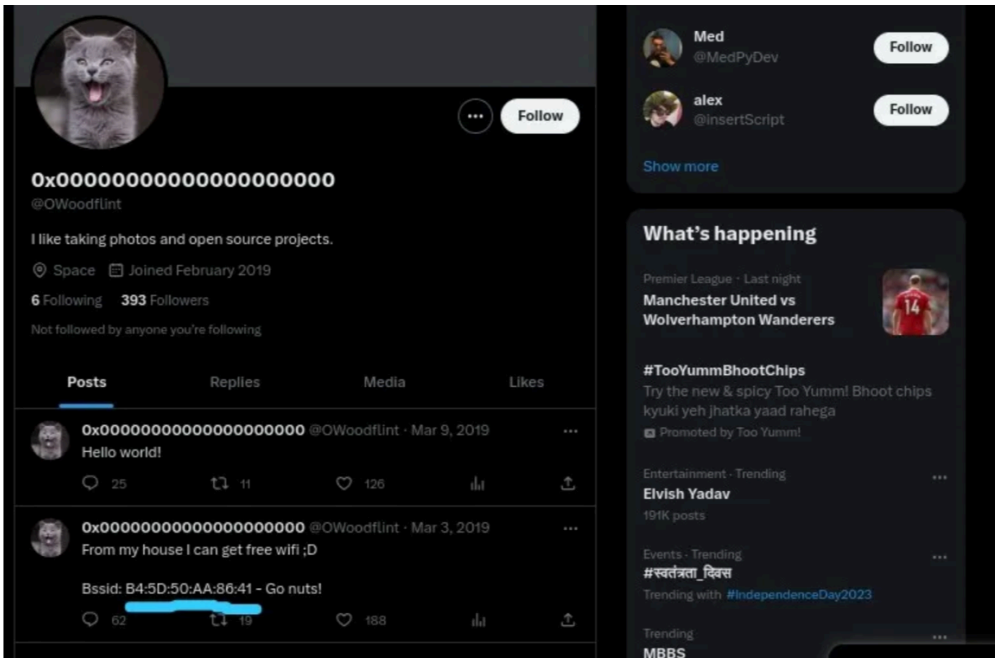
Date: 09-17-2024	Entry: 004
Description	Answer the Question on TryHackMe, "What city is this person in?"
Tool(s) used	Google Search

Details	<p>The user's github had the answer to this question:</p> 
Additional notes	

Date: 09-17-2024	Entry: 005
Description	Answer the Question on TryHackMe, "What is the SSID of the WAP he connected to?"
Tool(s) used	Twitter/x, Wigle.net, and his provided BSSID

Details

Going to the twitter/x link from above we see that the user has provided his BSSID:



From here I can go to wigle.net and used the advanced search function to provide us with the SSID:

Map	Net ID	SSID	Type	First Seen	Most Recently	Crypto	Est. Lat	Est. Long	Channel	Bcn Int.	QoS	Found by Me	Ac
map	B4:5D:50:AA:86:41	UnileverWiFi	infra	2017-10-10T21:00:00.000Z	2024-06-10T05:00:00.000Z		51.50835419	-0.13207622	11	0	7	false	-

From here we can see the answer to the question is **UnileverWiFi**.

Additional notes

Date: 09-17-2024	Entry: 006
Description	Answer the question on TryHackMe, "What is his personal email address?"
Tool(s) used	GitHub
Details	His personal email address is OWoodflint@gmail.com , this is available on his GitHub page github.com/OWoodflint/people_finder .
Additional notes	

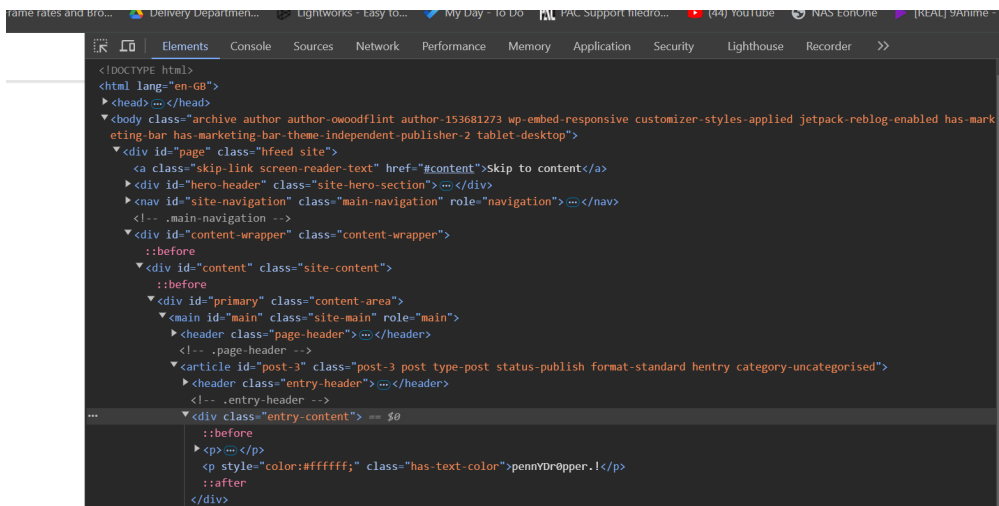
Date: 09-17-2024	Entry: 007
Description	Answer the question on TryHackMe, "What site did you find his email address on?"
Tool(s) used	GitHub
Details	The answer is github
Additional notes	

Date: 09-17-2024	Entry: 008
Description	Answer the question on TryHackMe, "Where has he gone on holiday?"

Tool(s) used	Google Search, Wordpress
Details	<p>After a google search I found his Wordpress Blog: oliverwoodflint.wordpress.com/author/owoodflint/</p>
Additional notes	

Date: 09-17-2024	Entry: 009
Description	Answer the question on TryHackMe, “What is this person’s password?”
Tool(s) used	Google Chrome Inspect,
Details	<p>This was a hard question for me. I had to discern that maybe it was in his Blog’s code somewhere. When I inspected the site I took the time to go through each div_id and eventually found a white colored text hidden on</p>

the blog.



```
<!DOCTYPE html>
<html lang="en-GB">
  <head>...</head>
  <body class="archive author author-owoodflint author-153681273 wp-embed-responsive customizer-styles-applied jetpack-reblog-enabled has-marketing-bar has-marketing-bar-theme-independent-publisher-2 tablet-desktop">
    <div id="page" class="hfeed site">
      <a class="skip-link screen-reader-text" href="#content">Skip to content</a>
      <div id="hero-header" class="site-hero-section">...</div>
      <nav id="site-navigation" class="main-navigation" role="navigation">...</nav>
      <!-- .main-navigation -->
      <div id="content-wrapper" class="content-wrapper">
        ::before
        <div id="content" class="site-content">
          ::before
          <div id="primary" class="content-area">
            <main id="main" class="site-main" role="main">
              <header class="page-header">...</header>
              <!-- .page-header -->
              <article id="post-3" class="post-3 post type-post status-publish format-standard hentry category-uncategorised">
                <header class="entry-header">...</header>
                <!-- .entry-header -->
                <div class="entry-content"> == $0
                  ::before
                  <p>...</p>
                  <p style="color:#ffffff;" class="has-text-color">pennYDropper. I</p>
                  ::after
                </div>
              ...
            </main>
          </div>
        </div>
      </div>
    </body>
  </html>
```

From here I went back to his blog and highlighted the entire thing to see if something was hidden:

Oliver Woodflint Blog

Photos you can relate to

Home

Contact

Author: owoodflint

Hey

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

pennYDropper.!

owoodflint

Uncategorized

Leave a comment

3rd Mar 2019

1 Minutes

	Low and behold the answer is pennYDropper.!
Additional notes	This is definitely a tough question if you have not looked at any code ever. Remember to inspect and to take time and go through the code.

Reflections/Notes: This was a fantastic room to get into the idea of thinking like a digital forensic investigator. This will be my future walkthrough so that I can try again.