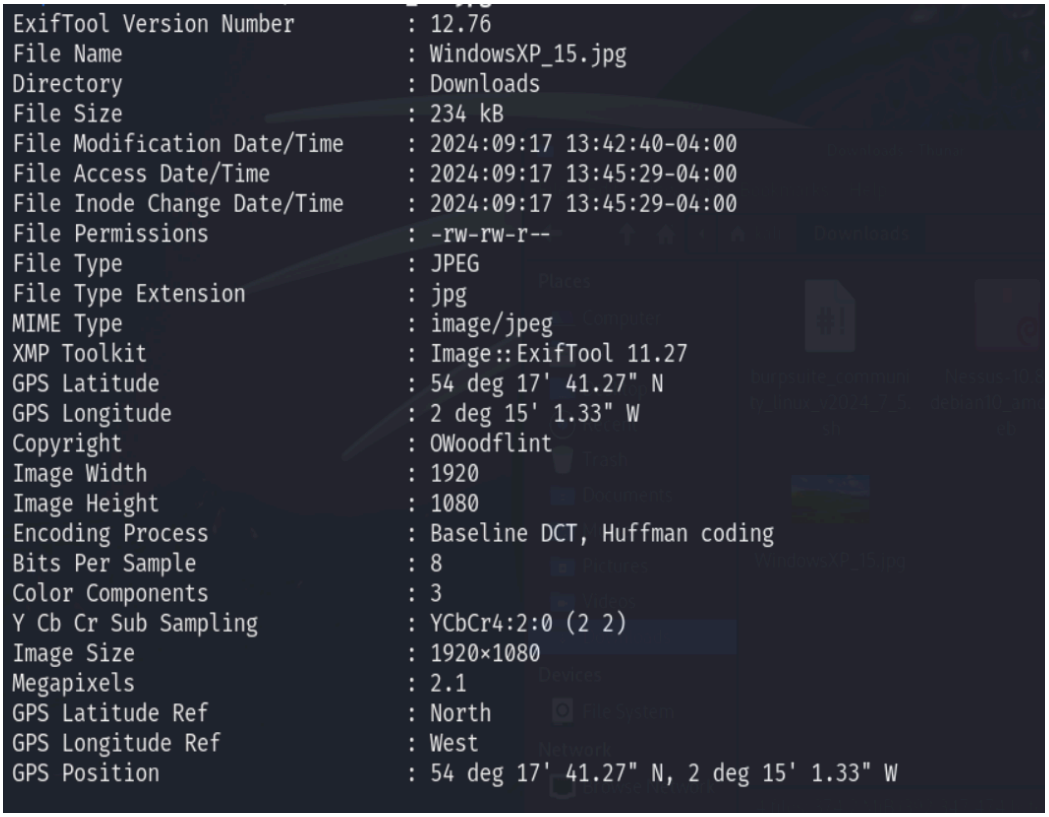
Stick-Cmd Metasploitable 2 Project journal

Date: 09-17-2024	**Entry: 001**
Description	Download the image at https://tryhackme.com/r/room/ohsint
Tool(s) used	Used VM box with Kali Linux to run ExifTool on
Details	- **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 sudo apt install command.

<table>
<tr><td><strong>Date:</strong> 09-17-2024</td><td><strong>Entry: 002</strong></td></tr>
<tr><td>Description</td><td>Proceed to use ExifTool to get information on the source image.</td></tr>
<tr><td>Tool(s) used</td><td>Kali Linux and Exiftool</td></tr>
<tr><td>Details</td><td>

ExifTool provided the encoded information on the image file. From this information we were able to gleam the copyright holders username: **OWoodflint.**

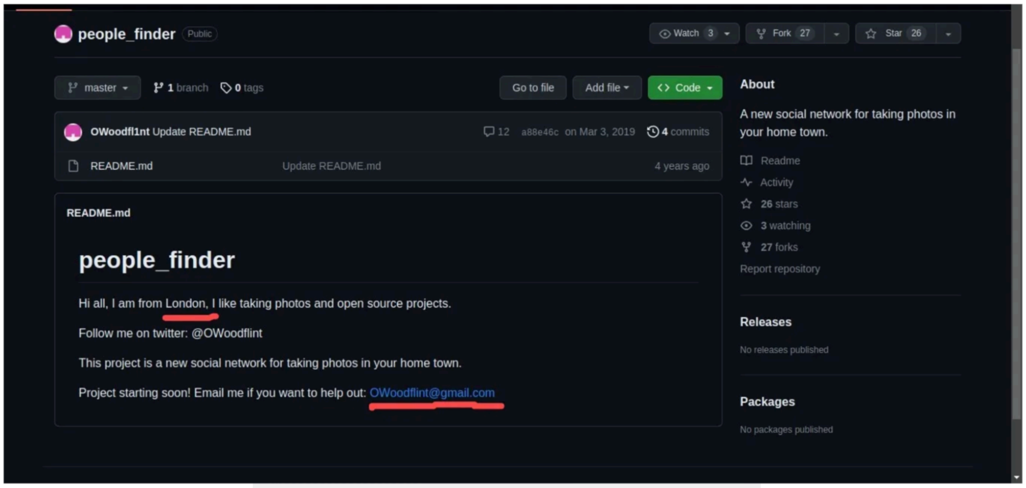


```
ExifTool Version Number         : 12.76
File Name                       : WindowsXP_15.jpg
Directory                       : Downloads
File Size                       : 234 kB
File Modification Date/Time     : 2024:09:17 13:42:40-04:00
File Access Date/Time           : 2024:09:17 13:45:29-04:00
File 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                      : 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
```

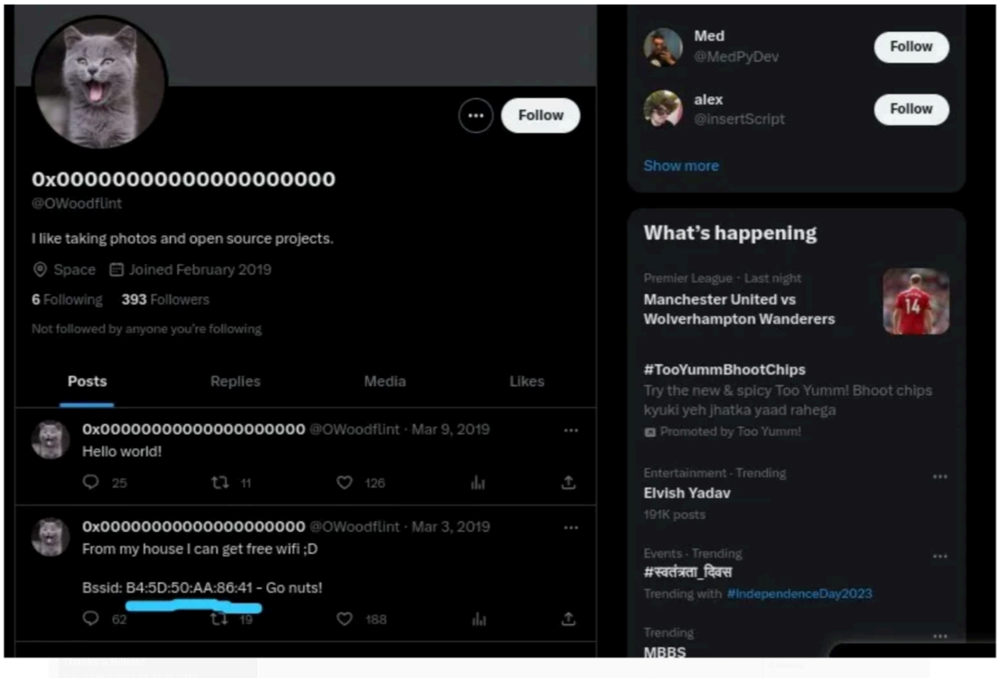
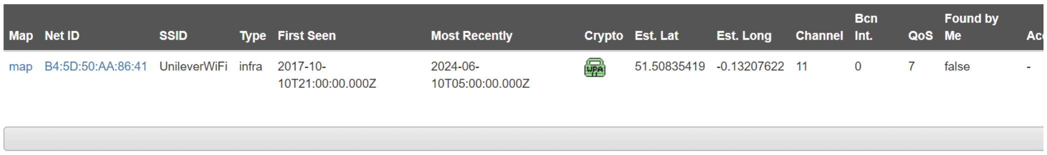
</td></tr>
<tr><td>Additional notes</td><td>From here I could look up the username on google.</td></tr>
</table>

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	The user’s github had the answer to this question: Ans: The user’s avatar is a cat.  people_finder Public Watch 3 Fork 27 Star 26 master 1 branch 0 tags Go to file Add file Code OWoodfl1nt Update README.md 12 a88e46c on Mar 3, 2019 4 commits README.md Update README.md 4 years ago 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 About A new social network for taking photos in your home town. Readme Activity 26 stars 3 watching 27 forks Report repository Releases No releases published Packages No packages published
Additional notes	

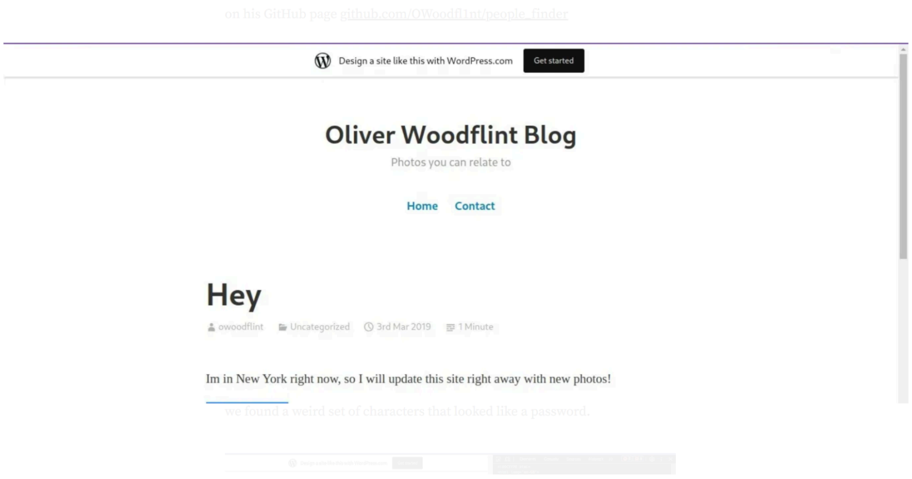
Date: 09-17-2024	**Entry: 005**
Description	Answer the Question on TryHackMe, “What is the SSID of the WAP he connected to?”
Tool(s) used	Twitter/x, Wigle.net, and his provided BSSID

<table>
<tr><td>Details</td><td>Going to the twitter/x link from above we see that the user has provided his BSSID:

0x00000000000000000000
@OWoodflint
I like taking photos and open source projects.
Space Joined February 2019
6 Following 393 Followers
Not followed by anyone you're following
Posts Replies Media Likes
0x00000000000000000000 @OWoodflint · Mar 9, 2019
Hello world!
25 11 126
0x00000000000000000000 @OWoodflint · Mar 3, 2019
From my house I can get free wifi ;D
Bssid: B4:5D:50:AA:86:41 - Go nuts!
62 19 188
Med @MedPyDev Follow
alex @insertScript Follow
Show more
What's happening
Premier League · Last night
Manchester United vs Wolverhampton Wanderers
#TooYummBhootChips
Try the new &amp; spicy Too Yumm! Bhoot chips kyuki yeh jhatka yaad rahega
Promoted by Too Yumm!
Entertainment · Trending
Elvish Yadav
191K posts
Events · Trending
#स्वतंत्रता_दिवस
Trending with #IndependenceDay2023
Trending
MBBS
From here I can go to wigle.net and used the advanced search function to provide us with the SSID:
<table>
<tr><th>Map</th><th>Net ID</th><th>SSID</th><th>Type</th><th>First Seen</th><th>Most Recently</th><th>Crypto</th><th>Est. Lat</th><th>Est. Long</th><th>Channel</th><th>Bcn Int.</th><th>QoS</th><th>Found by Me</th><th>Ac</th></tr>
<tr><td>map</td><td>B4:5D:50:AA:86:41</td><td>UnileverWiFi</td><td>infra</td><td>2017-10-10T21:00:00.000Z</td><td>2024-06-10T05:00:00.000Z</td><td>WPA</td><td>51.50835419</td><td>-0.13207622</td><td>11</td><td>0</td><td>7</td><td>false</td><td>-</td></tr>
</table>From here we can see the answer to the question is <b>UnileverWiFi</b>.</td></tr>
<tr><td>Additional notes</td><td></td></tr>
</table>

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	

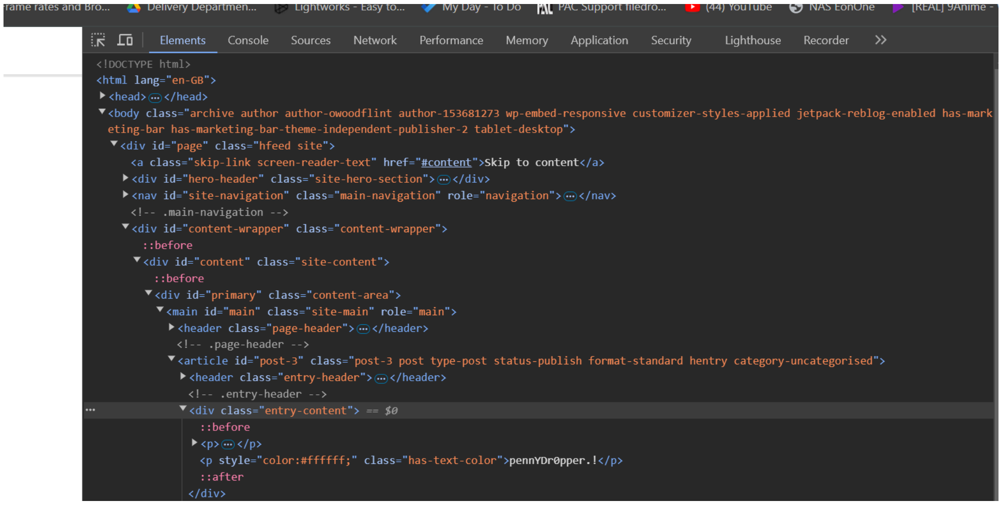
Date: 09-17-2024	**Entry: 007**
Description	Answer the question on TryHackMe, “What site did you find his email address on?”
Tool(s) used	GitHub
Details	**The answer is github**
Additional notes	

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	After a google search I found his Wordpress Blog: oliverwoodflint.wordpress.com/author/owoodflint/  on his GitHub page github.com/OWoodfl1nt/people_finder Oliver Woodflint Blog Photos you can relate to 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! we found a weird set of characters that looked like a password.
Additional notes	

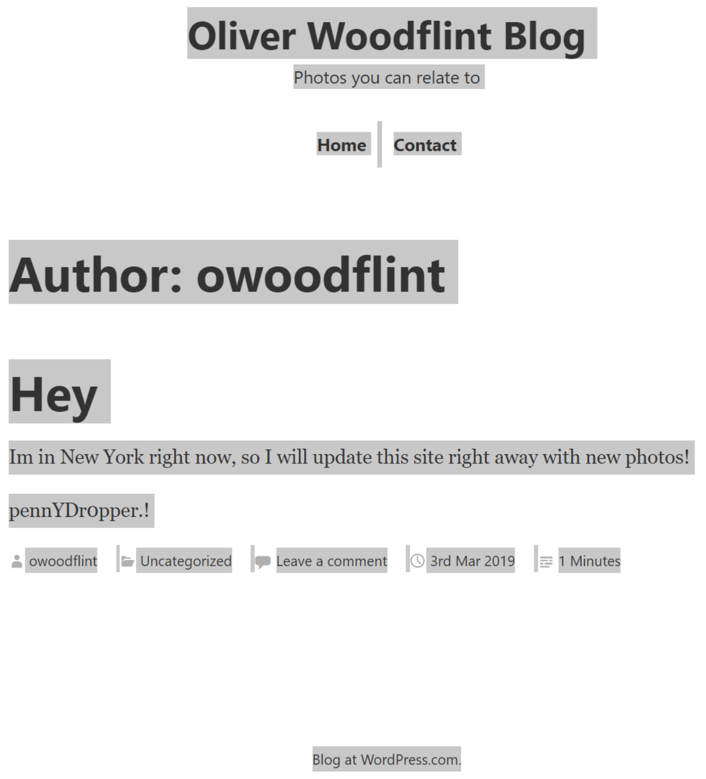
Date: 09-17-2024	**Entry: 009**
Description	Answer the question on TryHackMe, “What is this person’s password?”
Tool(s) used	Google Chrome Inspect,
Details	This was a hard question for me. I had to discern that maybe it was in his Blog’s code somewhere. When I inspected the site I took the time to go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

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-mark
 eting-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">pennYDr0pper.!</p>
                 ::after
               </div>
```

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

Author: owoodflint

Hey

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

pennYDr0pper.!

	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.