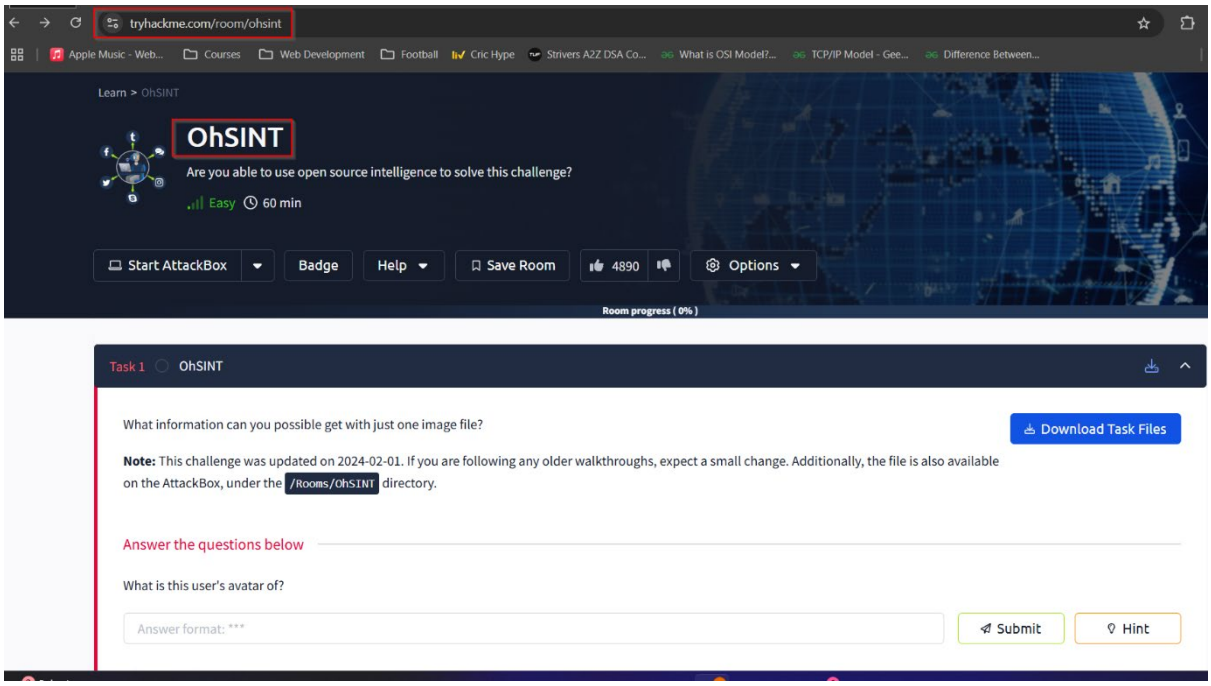
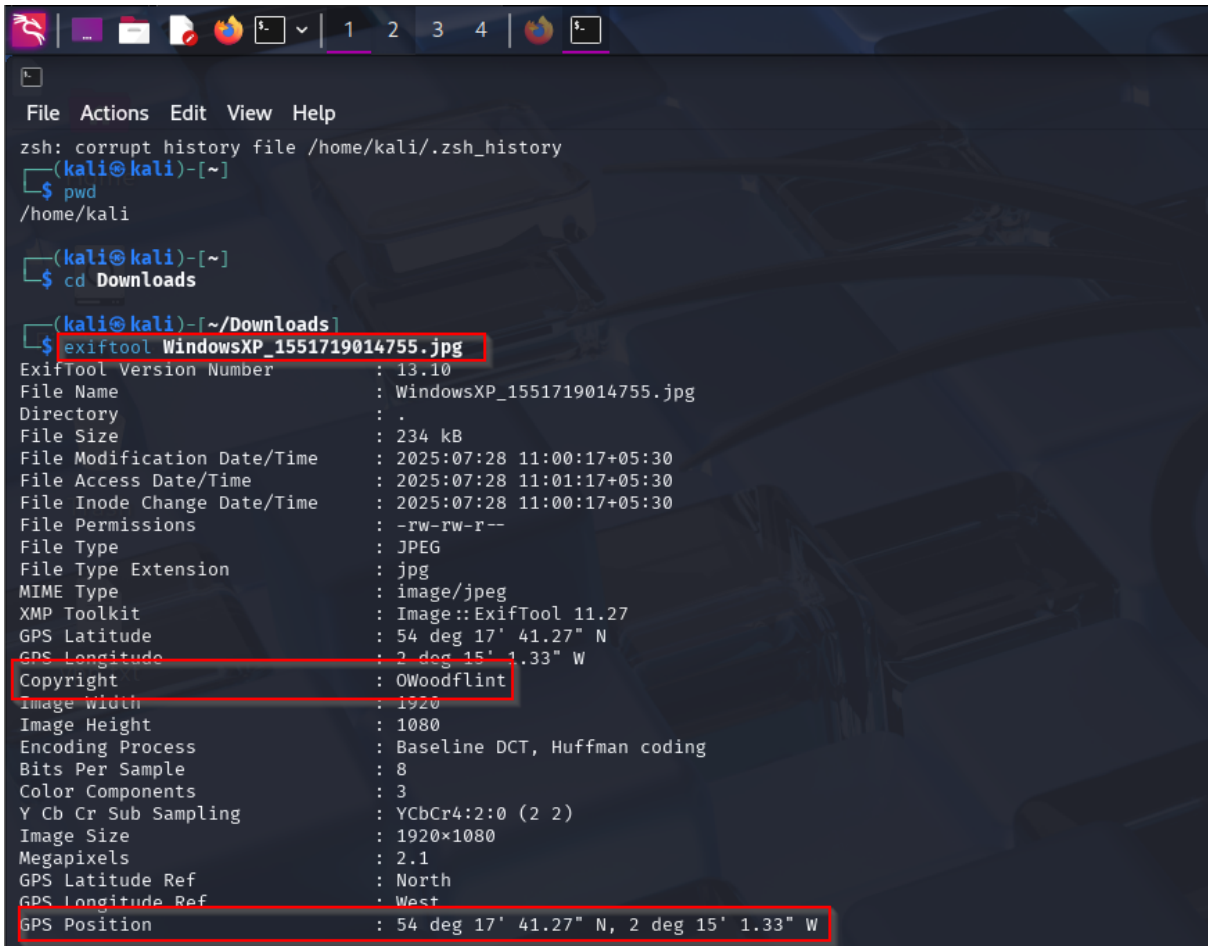
OhSINT Report

By Aditya Singh Rathaur

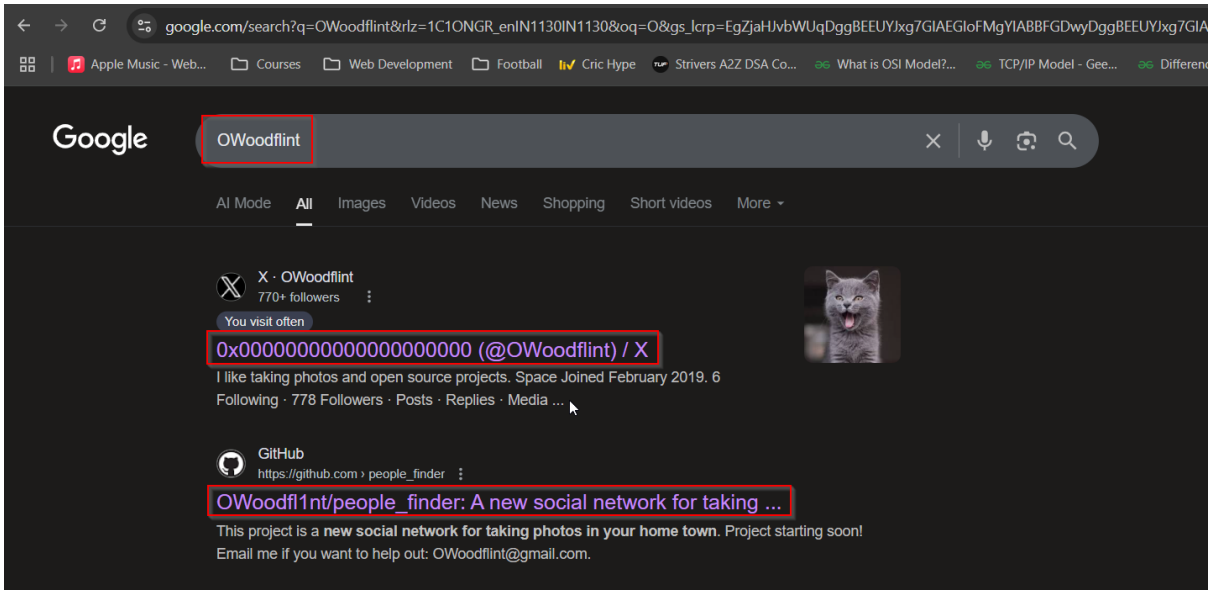
1. Test Target
    - **Room URL:** https://tryhackme.com/room/ohsint
    - **Test Image URL:** https://tryhackme-vm-upload.s3.eu-west-1.amazonaws.com/WindowsXP_1551719014755.jpg?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIA2YR2KKQMWLXEMXW4%2F20250728%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20250728T110830Z&X-Amz-Expires=120&X-Amz-Signature=eabf6722da3e3a1b9bd9a5a57dafaf992cbf3eb8071c8982b1c115668d0c9373&X-Amz-SignedHeaders=host&x-amz-checksum-mode=ENABLED&x-id=GetObject



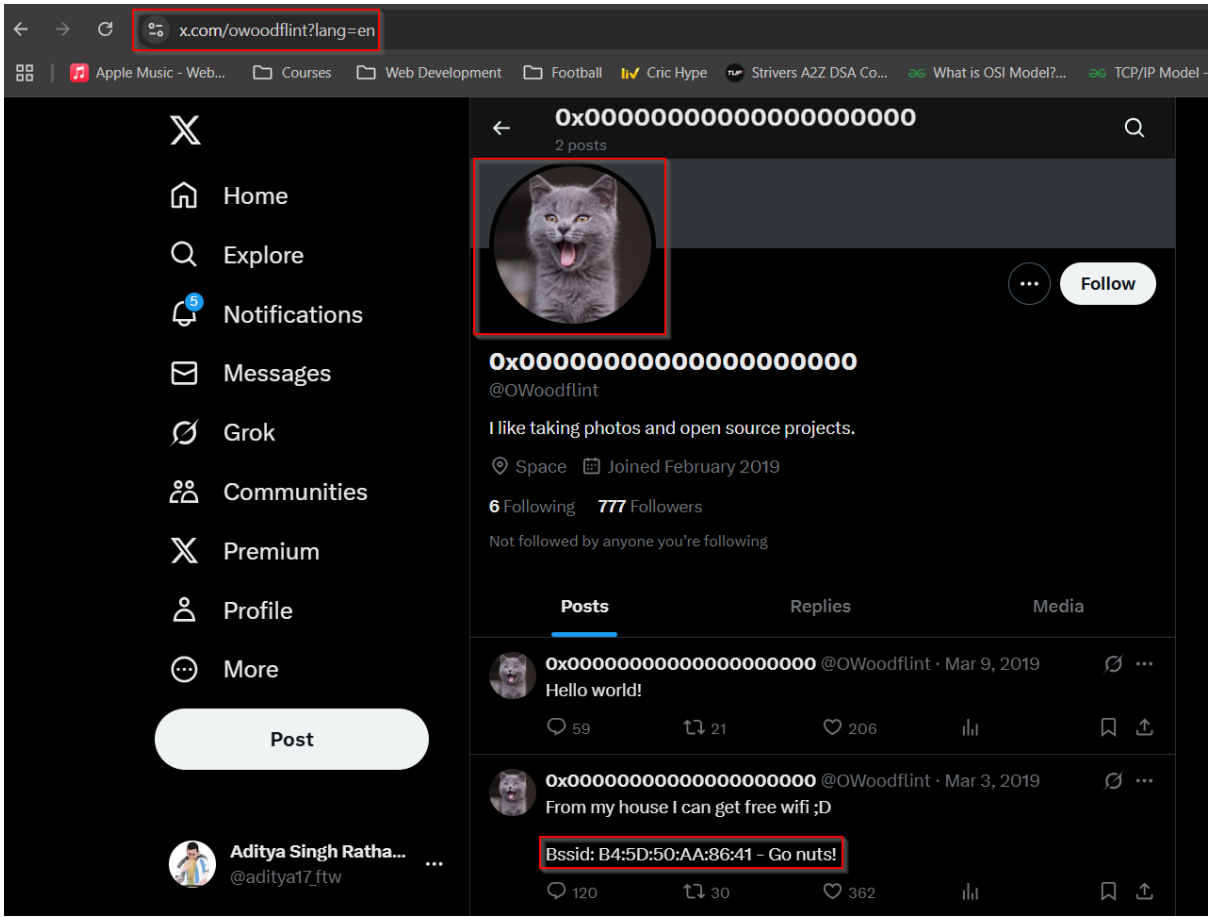
2. Step 1: Using Exiftool
    - **Exiftool:** Exiftool is a free, open-source software tool used for reading, writing and editing metadata in various file types especially image, video and audio files.
    - **Metadata:** Metadata is information embedded inside a file that describes its content, origin, and attributes. It contains information such as date, time, camera make and model, GPS location, Copyright, author information etc.
    - Open **Terminal** and navigate to the folder the image has been saved.
    - Execute the command **<exiftool WindowsXP_1551719014755.jpg>** to use **Exiftool**.
    - We get details about the image such as:
        - Name: WindowsXP_1551719014755.jpg
        - File Type: JPEG
        - File Type Extension: jpg
        - Copyright: OWoodflint
        - Latitude: 54 deg 17’ 41.27” N
        - Longitude: 2 deg 15’ 1.33” W



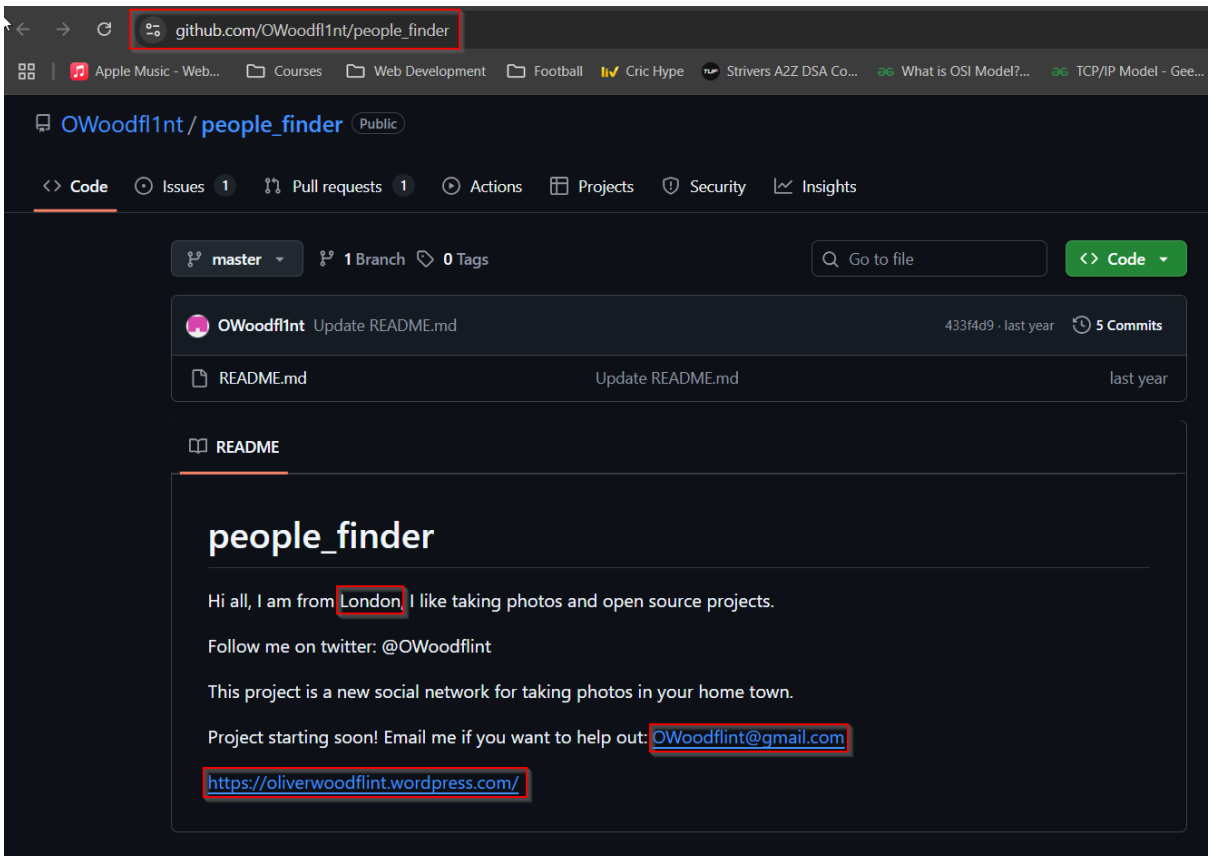
3. Step 2: Searching on Google for Social Media
    - Search for **<OWoodflint>** on www.google.com.
    - We find multiple social media accounts related to **Owoodflint**:
        - **Twitter:** https://x.com/owoodflint
        - **Github:** https://github.com/OWoodfl1nt/people_finder



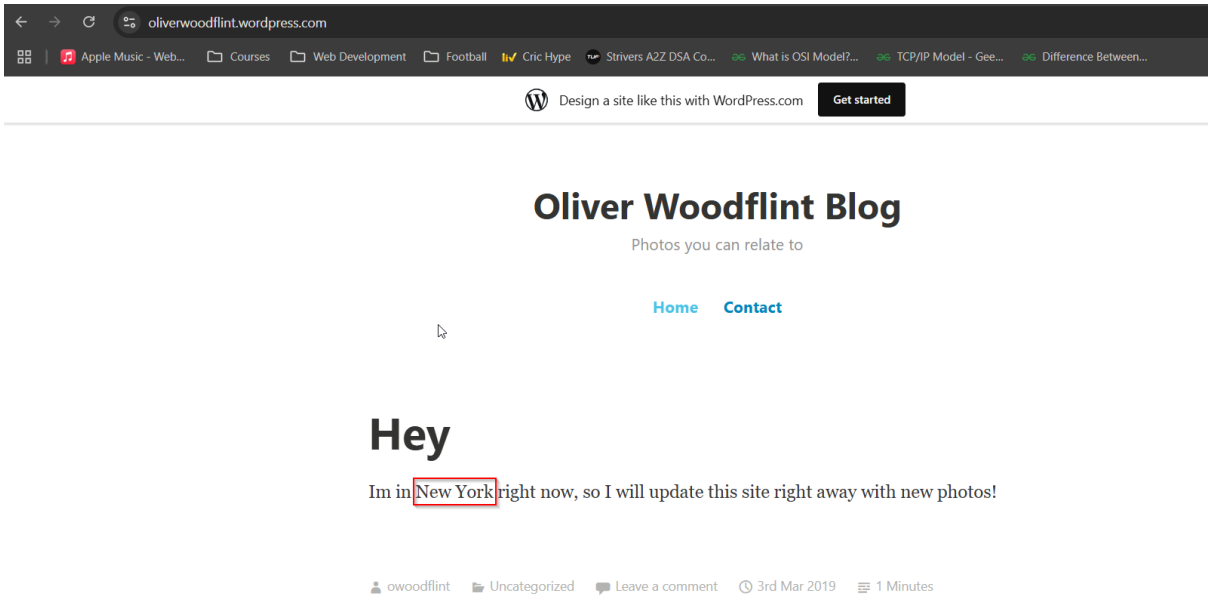
4. Step 3: Searching in Twitter
    - Navigate to the twitter account <https://x.com/owoodflint>
    - We can find the profile picture as a **cat** which could be the user's avatar.
    - We can also find the **BSSID- B4:5D:50:AA:86:41** which will be used to find the SSID and location **using Wigle.net**.



5. Step 4: Searching in Github
    - Navigate to the Github repository named **people_finder** of the account **OWoodfl1nt**
    - **Repository URL:** https://github.com/OWoodfl1nt/people_finder
    - From the README.md file present in the repository we can find the following details:
    - The person is from **London**.
    - We can also find his twitter handle <**@OWoodflint**>
    - The file contains the person email address i.e. **OWoodflint@gmail.com**
    - The repository contains a link of the person's personal vlog page having the URL: https://oliverwoodflint.wordpress.com



6. Step 5: Searching in WordPress
    - Navigate to the blog page of the person by clicking on the link given in the GitHub repository.
    - **URL:** https://oliverwoodflint.wordpress.com
    - The person is in **New York** for his holidays as mentioned in his blog.



7. Step 6: Searching page source of multiple social media accounts:
    - Navigate to each of the social media accounts i.e. Twitter, Github and WordPress.
    - Use the shortcut key **CTRL+SHIFT+I** on Windows/Linux (or MacOS use **COMMAND+OPTION+I**) to inspect the elements such as HTML structure, CSS styles, JavaScript commands, Network Panel etc.
    - Navigate to the **Elements** tab and look for any white-coloured text, as it may indicate hidden content. Most tags in the Developer Tools are displayed in different colours, so white text can stand out as potentially concealed.
    - We discover hidden text i.e. <**pennYDr0pper.!**> on a WordPress page, styled in white (#ffffff), which made it invisible against the white background.