# OSINT Investigation Report: TryHackMe "Ohsint" Room

## 1. Introduction

This report details the Open Source Intelligence (OSINT) investigation conducted as part of the TryHackMe 'Ohsint' room. The objective was to gather information on a target using publicly available tools and techniques. The investigation followed ethical OSINT practices and focused on uncovering digital footprints left by the subject, "OWoodflint."

## 2. Tools Used

- ExifTool (Extract metadata from images)

- Google Dorking (Advanced search queries)

- Google Maps (Geolocation analysis)

- Wigle.net (Wireless network mapping)

- GitHub Search (Repository and email discovery)

- WordPress Blog Analysis (Hidden data extraction)

- HTML Source Code Inspection (Finding concealed information)

## 3. Investigation Steps & Findings

### Step 1: Extracting Metadata from an Image

Used ExifTool on Kali Linux to extract metadata.  
Found the copyright holder username: OWoodflint.  
Answer: Username identified as "OWoodflint."

### Step 2: Identifying the Target’s Avatar

Used Google Dorking with the query: Twitter intext:"OWoodflint".  
Located the Twitter profile, where the avatar was an image of a cat.  
Answer: Avatar identified as a cat.

### Step 3: Extracting GPS Coordinates

Extracted GPS coordinates:  
- 54°17'41.27" N, 2°15'1.33" W  
- Decimal format: 54.294797, -2.250369  
Used Google Maps to analyze location: 7PVX+WV6, Hawes, United Kingdom.  
Answer: Location found near B6255 road in a rural area.

### Step 4: Finding the BSSID (Wi-Fi Network)

Extracted BSSID from a tweet on OWoodflint’s Twitter account:  
- B4:5D:50:AA:86:41  
Searched it on Wigle.net (after converting to lowercase) to get the city: London.  
Answer: The target is located in London.

### Step 5: Discovering the Wi-Fi SSID

Found the SSID (Wi-Fi network name) connected to:  
- UnileverWiFi.  
Answer: The Wi-Fi SSID is UnileverWiFi.

### Step 6: Finding an Email Address

Located the target’s GitHub profile: https://github.com/OWoodfl1nt/people\_finder  
Found the email address inside a repository: OWoodflint@gmail.com.  
Answer: Email identified as OWoodflint@gmail.com.

### Step 7: Identifying Travel History

Analyzed the WordPress blog: https://oliverwoodflint.wordpress.com/author/owoodflint/  
Found details indicating the target had traveled to New York.  
Answer: Holiday location identified as New York.

### Step 8: Extracting a Password

Checked the HTML source code of the WordPress blog.  
Found a hidden password in white text:  
- pennYDr0pper.!  
Answer: The discovered password is pennYDr0pper.!

## 4. Conclusion

This OSINT investigation successfully uncovered various details about "OWoodflint," including their username, location, email, social media presence, travel history, and even a password. The techniques used highlight the importance of digital privacy and how publicly available data can be leveraged to build a profile of an individual.

## 5. Ethical Considerations

This investigation was conducted solely for educational purposes within the TryHackMe platform. No unauthorized access or malicious intent was involved. Users are advised to maintain proper cybersecurity practices to safeguard their personal information online.