# OSINT Investigation Report

TryHackMe - OhSINT (practice)

Prepared by

Ambar Roy

Contact: ambarroy11@gmail.com

Report date: October 21, 2025

**Engagement type:** OSINT / Cyber Investigation (CTF-style)
**Scope:** Identify target information from provided artefacts (image, pages).
**Tester:** Freelance beginner pentester

## Contents

## Executive Summary

This document reports the open-source intelligence (OSINT) investigation performed for the TryHackMe *OhSINT* challenge. The objective was to extract and correlate publicly-available information from the provided artefact (an image) and related web resources to identify the target's digital footprint.

Key results (derived from the provided image and subsequent investigation):

- EXIF metadata in the image revealed a copyright owner: **OWoodflint**.
- Wireless BSSID discovered in the image metadata: **B4:5D:50:AA:86:41**; SSID correlated via Wigle.net: **UnileverWifi**.
- Public GitHub profile located under the name **OWoodflint**; personal email found: **OWoodflint@gmail.com**.
- Personal blog/WordPress page located at `https://oliverwoodflint.wordpress.com/author/owoodflint/` indicating the subject was on holiday in New York.
- A hidden (white-on-white) string in the WordPress page source was discovered and used as a password: **pennYDr0pper.!**

The lab goal (to find the target-related data) was completed using these OSINT techniques.

# 1 Scope and Rules of Engagement

### Scope

- Target: OhSINT challenge artefacts provided by TryHackMe (image file and linked resources).
- Objective: Extract identifying information using OSINT techniques and public resources.
- Engagement type: Educational / CTF-style.

### Rules of Engagement

- Only publicly-available data and resources were used.
- No brute-force or intrusive actions were performed against third-party services.
- Findings are for training/educational purposes only.

# 2 Methodology

The investigation followed a straightforward OSINT workflow:

1. **Artifact analysis:** Extract metadata from the provided image.
2. **Lookup and correlation:** Use discovered identifiers (BSSID, names) on public directories (e.g., Wigle, search engines).
3. **Profile discovery:** Locate public profiles and pages (GitHub, WordPress).
4. **Source analysis:** Inspect page source for hidden strings or additional information.
5. **Consolidation:** Correlate discoveries into a concise target profile.

**Primary tools used:**

- `exiftool` — extract image metadata
- Wigle.net — correlate BSSID to observed SSID
- Web browser and `view-source` — inspect pages and hidden content
- Public search engines and GitHub for profile discovery

# 3 Findings

## Finding #1 — Image metadata (EXIF) reveals copyright owner and BSSID

**Summary:**
The provided image (Windows XP background) contained EXIF metadata revealing an ownership string and a wireless BSSID — useful starting points for OSINT correlation.

**Command / Evidence:**

```
exiftool XP.jpg
```

**Relevant metadata extracted (as observed):**

- Copyright: **OWoodflint**
- Wireless BSSID: **B4:5D:50:AA:86:41**

**Impact:** Metadata embedded in images can leak personally-identifying information (PII) or infrastructure identifiers that allow further linkage to online profiles and network infrastructure.

**Remediation:**

- Strip EXIF and other metadata from images before sharing publicly (e.g., `exiftool -all= image.jpg`).
- Educate users about metadata leakage and implement sanitization in publishing pipelines.

## Finding #2 — BSSID correlated to SSID via Wigle.net

**Summary:**
The wireless BSSID found in the image metadata was looked up on Wigle.net to identify an associated SSID.

**Evidence / Result:**

- BSSID: **B4:5D:50:AA:86:41**
- Correlated SSID (via Wigle.net): **UnileverWifi**

**Impact:** Publicly-exposed network identifiers can reveal infrastructure ownership or physical site information which aids in profiling a subject's location or employer.

**Remediation:**

- Avoid publishing images that contain network identifiers.
- Use generic SSIDs where appropriate and avoid embedding infrastructure details in public content.

## Finding #3 — Public profile (GitHub) and contact email

**Summary:**
A public GitHub profile matching the extracted name/handle was located, and a personal email address was discovered on that profile.

**Evidence / Result:**

- GitHub handle / profile owner: **OWoodflint**
- Email address located on GitHub: **OWoodflint@gmail.com**

**Impact:** Email addresses and profile links enable direct correlation to other platforms and facilitate targeted social engineering if misused.

**Remediation:**

- Use contact forms or project-specific addresses rather than personal emails on public profiles.
- Consider using a privacy-focused email or separate work email for public profiles.

### Finding #4 — Personal blog (WordPress) and location hint

**Summary:**
The target's WordPress author page was located and contained a mention that the subject was on holiday in New York — a useful contextual detail for profiling.

**Evidence / URL:**

- Author page: `https://oliverwoodflint.wordpress.com/author/owoodflint/`
- Observed note: Subject stated they were on holiday in New York (as presented on that page).

**Impact:** Public posts about travel or location can reveal real-world whereabouts which may be sensitive.

**Remediation:**

- Avoid posting real-time location information publicly.
- Post travel updates selectively or after returning.

### Finding #5 — Hidden password string in page source

**Summary:**
The HTML source of the WordPress page contained a string styled (white-on-white) so it was invisible in the rendered page. This string functioned as a password discovered during the investigation.

**Evidence / Command:**

- Inspect page source via browser (View → Page Source) or developer tools.
- Hidden string (password) discovered: **pennYDr0pper.!**

**Impact:** Embedding passwords or sensitive tokens in page source (even hidden) is a major information exposure and can enable unauthorized access if used as credentials elsewhere.

**Remediation:**

- Never embed passwords, API keys, or secrets in HTML, CSS or client-side scripts.
- Use server-side authentication and secure secret management for credentials.
- Perform code reviews to identify inadvertently published secrets.

# 4 Conclusion

The OhSINT lab effectively demonstrates how small artefacts (image metadata, network identifiers, or hidden strings in page source) can be correlated to build a clear profile of a subject. Using only publicly-available information and simple tools (exiftool, Wigle lookup, browser source inspection), the investigation uncovered:

- Owner/handle: **OWoodflint**
- BSSID: **B4:5D:50:AA:86:41**
- SSID: **UnileverWifi**
- Email: **OWoodflint@gmail.com**
- Location hint: Holiday in New York (from WordPress author page)
- Hidden password in page source: **pennYDr0pper.!**

These results complete the OhSINT challenge scope. The recommendations above (strip metadata, avoid embedding secrets in client-side content, and limit public exposure of contact/location details) will reduce the risk of similar information leakage in real-world scenarios.

## Appendix — Commands and Notes

- Image metadata extraction:

```
exiftool XP.jpg
```

- BSSID lookup (example service used): Wigle.net
- Page source inspection: browser `View Source` or developer tools
- Profiles visited: GitHub (handle: OWoodflint), WordPress author page at `https://oliverwoodflint.wordpress.com/author/owoodflint/`

## Contact and Notes

Prepared by: Ambar Roy
Contact: ambarroy11@gmail.com

This report documents an OSINT training exercise executed in the TryHackMe *OhSINT* lab. All findings are derived from the provided artefacts and publicly-available resources.