

OSINT



Matteo Golinelli

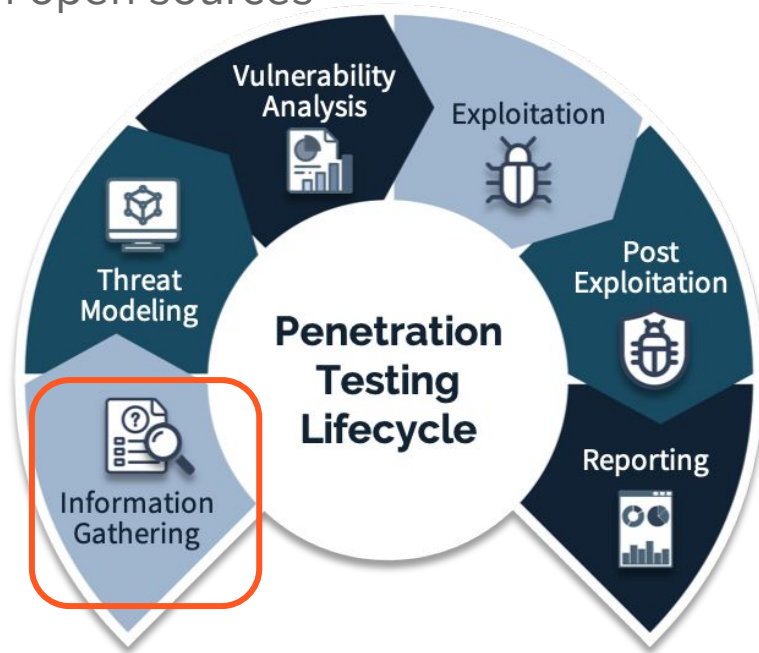
OSINT: Open Source Intelligence

→ **Collection** and **analysis** of data gathered from open sources

It's done for:

- Law enforcement
- Business Intelligence
- Security
 - Cybersecurity

Intelligence: acquire and apply knowledge



OSINT in Journalism

Gather information not from intelligence sources, but from social networks, Telegram, ...

- <https://www.bellingcat.com/tag/osint/>
- <https://www.forbes.com/sites/subramaniamvincent/2023/10/27/how-open-source-intelligence-can-help-journalism-cover-conflicts/>
- <https://www.ilpost.it/2023/10/20/osint/> (in Italian)

Open source?

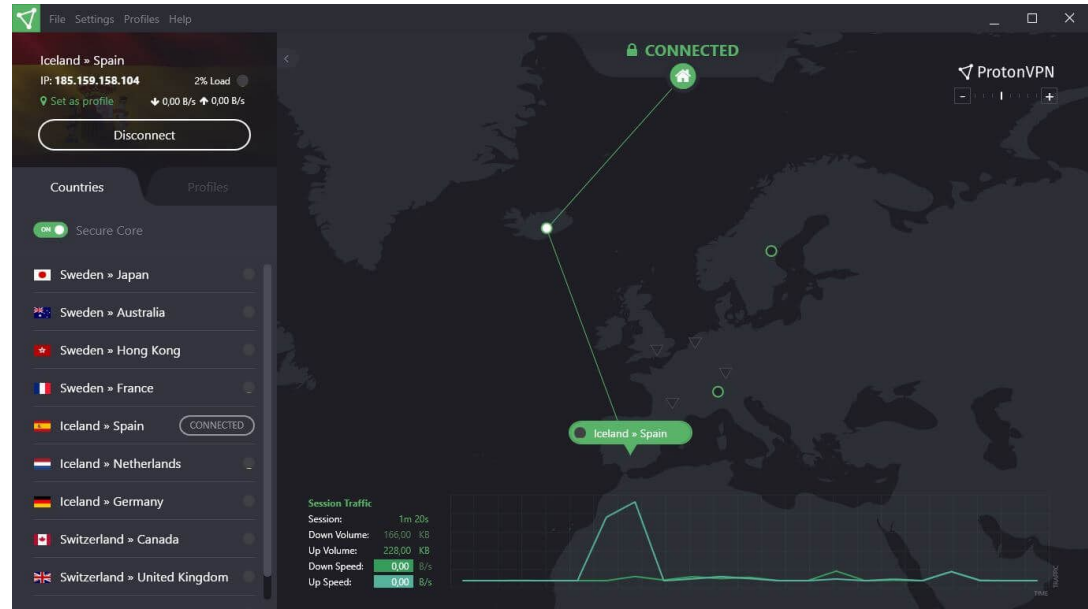
Means **publicly available information**

- Usually free
- Sources:
 - **Made for OSINT:** Shodan, ZoomEye
 - **OSINT as a side effect:** social networks, search engines, ...
- OSINT can be **passive** or **active**
 - If it interacts directly with the target or not
 - **Active** can possibly **leak information** to the target

Tools and Techniques

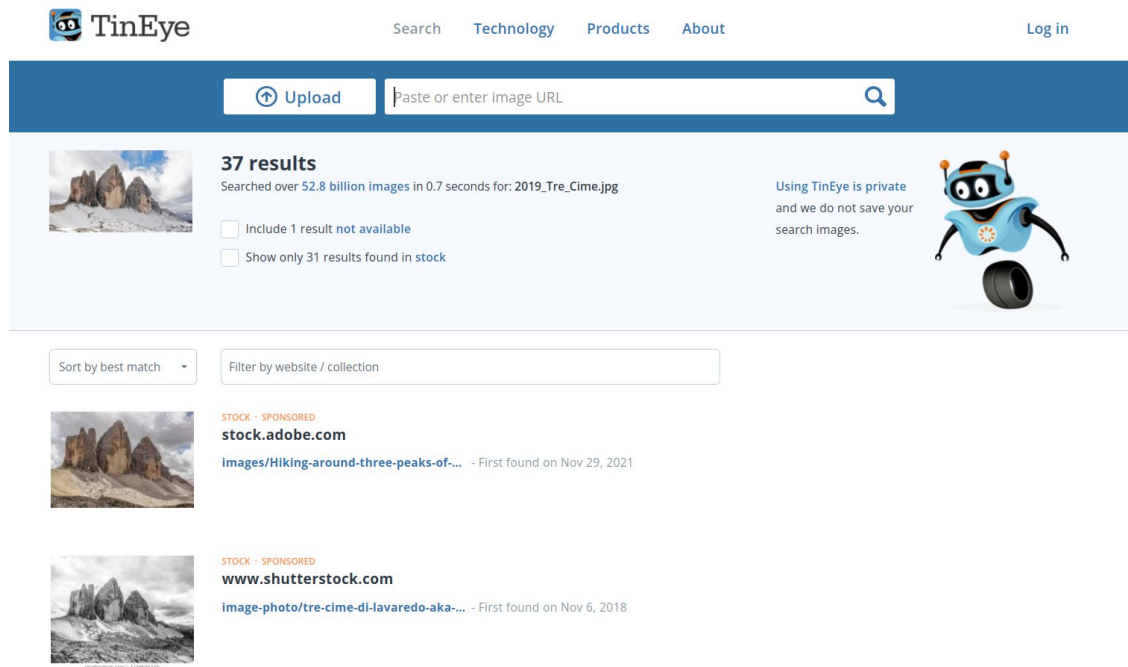
Free VPN

- <https://protonvpn.com/>
- Tor Network (Tor Browser)



Search Engines

- **General:** Google, Bing, Yandex, ...
- **Reverse Image:** tineye.com



The screenshot shows the TinEye website interface. At the top, there is a navigation bar with the TinEye logo, links for Search, Technology, Products, and About, and a Log in button. Below the navigation bar is a search bar with an 'Upload' button and a text input field labeled 'Paste or enter image URL'. The search results section shows 37 results for the image '2019_Tre_Cime.jpg', which is a photograph of three jagged mountain peaks. The results are sorted by best match. Two results are visible: one from stock.adobe.com and one from www.shutterstock.com. Both results are marked as 'STOCK - SPONSORED' and show the first found date.

TinEye Search Technology Products About Log in

Upload Paste or enter image URL

37 results
Searched over 52.8 billion images in 0.7 seconds for: 2019_Tre_Cime.jpg

☐ Include 1 result **not available**
☐ Show only 31 results found in **stock**

Using TinEye is private and we do not save your search images.

Sort by best match Filter by website / collection

STOCK - SPONSORED
stock.adobe.com
[Images/Hiking-around-three-peaks-of-...](#) - First found on Nov 29, 2021

STOCK - SPONSORED
www.shutterstock.com
[image-photo/tre-cime-di-lavaredo-aka-...](#) - First found on Nov 6, 2018

More Search Engines and Databases

- **spyse.com**: IT infrastructures, networks, the internet
 - whois, DNS lookup, subdomains finder, IP lookup, ... (**reconnaissance**)
 - <https://www.nmmapper.com/>
 - <https://securitytrails.com/>
 - <https://osint.sh/>
 - <https://scantrics.io/>
- **exploit-db.com**: archive of public exploits and corresponding vulnerable software
 - Exploits, Shellcode, 0-days, RCE, Vulnerability Reports, ...

Shut down in
2022

Shodan 1

- Find Internet-connected devices (**IoT**):
 - Webcams, industrial control systems, printers, servers, ...
- <https://www.shodan.io/search/filters>

WARNING: accessing what you find on Shodan might **not** always be legal,
and it will *leak your IP address* and other information

Shodan 2

- Find honeypots: <https://honeyscore.shodan.io/>
 - A fictitious system connected to the network pretending to be a valuable target
 - Acts as a decoy for attacks and allows
 - Monitoring ongoing attacks
 - Waste the attackers' resources



Honeypot Or Not?

Enter an IP to check whether it is a honeypot or a real control system:

Check for Honeypot

Returns a score from 0 to 1

Looks like a real system!

200 GET api.s... ?key=... jquery... j... 608 B ... 3 1 0.3

How to search on Google 1

- `site:example.com`
- `filetype:`, `intitle:`, `inurl:`, `intext:`, `cache:`
- **OR, AND**
- Search for exact term: **"term"**
- Exclude a term: **-term**
- Any word/phrase: *****
- Google autocomplete: **_**

Search "Google operators" on Google for more

How to search on Google 2

- Uncover interesting, and usually sensitive, information made publicly available on the Internet
 - <https://www.exploit-db.com/google-hacking-database>

Web Archive

- <http://web.archive.org/>
 - Snapshots of web pages at different times in the past
- <http://web.archive.org/web/19971017180411/http://www.unitn.it/>

Social Network Intel.

Also called **SOCMINT**: *Social Media Intelligence*

Types of information:

- **Profile information:** phone number, birth date, personal interests, relatives, ...
- **Interaction:**
 - Who's the person talking to?
 - Are they affiliated to some groups or political parties?
 - Sentiment analysis.
- **Metadata:** location, timezone, device, ...

References

- https://en.wikipedia.org/wiki/Open-source_intelligence
- <https://portswigger.net/daily-swig/schneider-electric-fixes-critical-vulnerabilities-in-evlink-electric-vehicle-charging-stations>