

[Open in app ↗](#)

Search



Write



Mastering OSINT: How to Find Information on Anyone

Hayden.banz · [Follow](#)

Published in OSINT Team · 4 min read · Aug 7, 2024

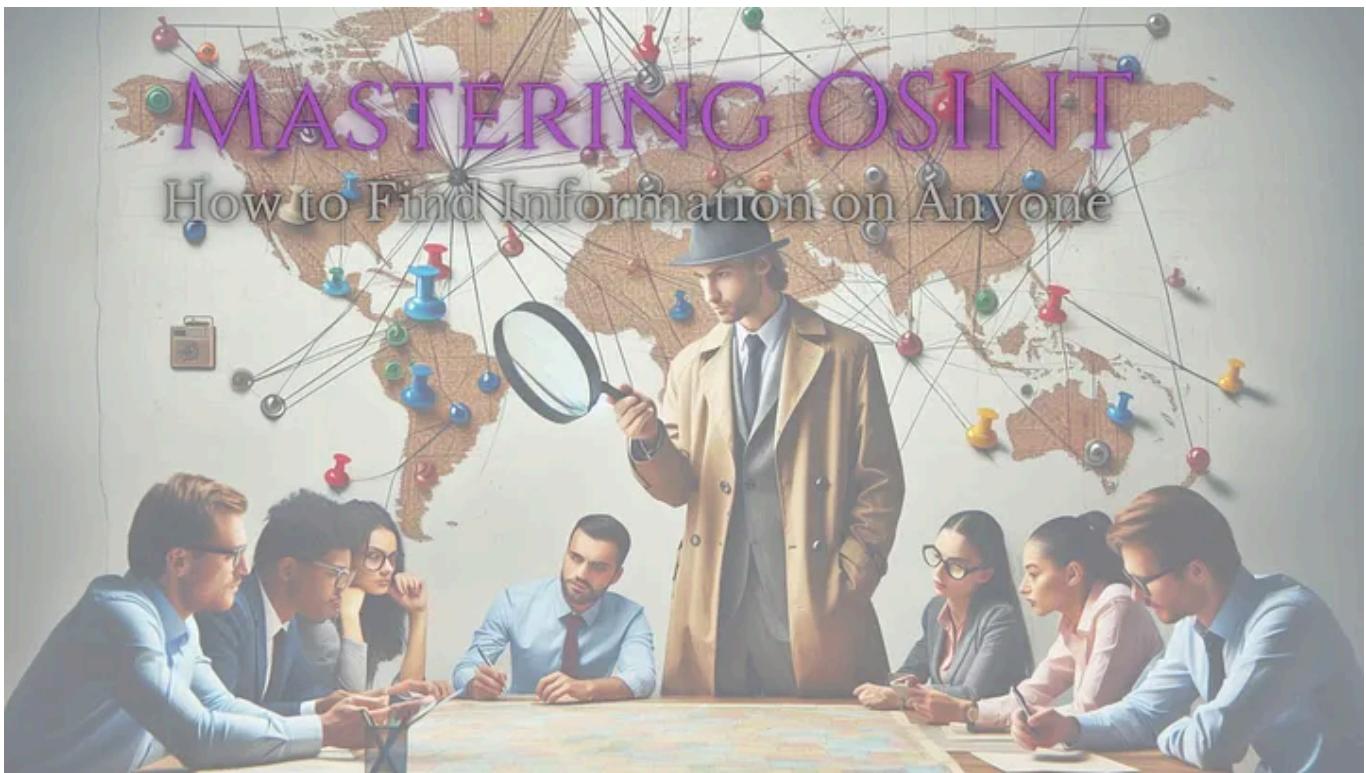
195

1



...

In today's digital age, information is more accessible than ever before. Open Source Intelligence (OSINT) collects and analyzes publicly available data to generate actionable intelligence. Whether you are a journalist, investigator, or simply someone curious about a topic, OSINT techniques can help you uncover valuable insights. This article will guide you through the process of finding information on anyone using OSINT methods.



Understanding OSINT

OSINT leverages data from publicly available sources such as social media, websites, government databases, forums, and more. The key to effective OSINT is knowing where to look and how to analyze the information you find. Here are some essential steps to get you started.

Connect us to Instagram for More OSINT Tips & Tricks

<https://www.instagram.com/osintbyhaybnz>

Getting started

Gather Basic Information

Start with the basics. Use search engines like Google to find initial information. Enter the person's name in quotation marks to get exact

matches. Combine the name with other keywords like location, profession, or organization to narrow down the results.

Start with What You Know: Identify any piece of information you already have, such as an email, username, or phone number.

Define Your Requirements: Clarify what information you seek to gather.

Gather the Data: Use various tools and methods to collect information.

Analyze Collected Data: Examine the data for patterns and relevant information.

Pivot Using New Data: Use newfound information to dig deeper.

Validate Assumptions: Cross-check data for accuracy.

Generate a Report: Compile your findings into a coherent report.

Real Name Searches

Governmental Resources

Government websites can be a treasure trove of information. Depending on the country, data openness varies, but advanced Google search queries can help locate relevant information.

Google Dorks(google dorks)

In 2002, Johnny Long started collecting Google search queries, known as Google Dorks, to uncover sensitive information. Here are some useful

queries:

- `"john doe" site:instagram.com`: Exact match search on Instagram.
- `"john doe" -"site:instagram.com/johndoe" site:instagram.com`: Exclude the target's own account but show their comments on others' posts.
- `"CV" OR "Curriculum Vitae" filetype:PDF "john doe"`: Find resumes containing "CV" or "Curriculum Vitae" in PDF format.

People Search Websites

Use specialized websites for people searches based on real name, username, email, or phone number:

- [spokeo.com](#)
- [thatsthem.com](#)
- [beenverified.com](#)
- [fastpeoplesearch.com](#)
- [truepeoplesearch.com](#)
- [familytreenow.com](#)

Username Searches

Reverse Username Lookup

Websites like socialcatfish.com, usersearch.org, and peekyou.com are valuable for reverse username lookups.

Google Dorks for Usernames

- `inurl:johndoe site:instagram.com`: Search Instagram URLs containing "johndoe".
- `allinurl:john doe ny site:instagram.com`: Find pages with specific words in the Instagram URL.

Username Search Tools

Tools like instantusername.com, namechk.com, and WhatsMyName (a GitHub project) can help locate usernames across multiple platforms.

Email Address Searches

Google Dorks

- `"@example.com" site:example.com`: Search for emails on a given domain.
- `HR "email" site:example.com filetype:csv | filetype:xls | filetype:xlsx`: Find HR contact lists on a domain.
- `site:example.com intext:@gmail.com filetype:xls`: Extract email IDs from a domain.

Email Tools

- **Hunter**: Scans domain names for email addresses and reveals common patterns.
- **Email Permutator**: Generates potential email permutations.
- **Proofy**: Bulk email validation.
- **Verifalia**: Validates single email addresses.

Compromised Databases

Websites like haveibeenpwned.com and dehashed.com can help find data breaches involving the target's email, revealing services they use or have used.

Phone Number Searches

Social Media Search

Entering a phone number into Facebook search might reveal associated profiles.

Phone Lookup Services

Websites like privacystar.com, getcontact.com, and everycaller.com provide reverse phone lookup services.

PhoneInfoga

PhoneInfoga is an advanced tool for scanning phone numbers using free resources, providing information such as country, area, carrier, and line type.

Domain Name Searches

Google Dorks

- `site:example.com`: Limits search to a specific domain.
- `filetype:DOC`: Returns documents of specified types from the domain.
- `intext:word1`: Searches for specific words on a page or website.
- `related:example.com`: Lists web pages similar to a specified web page.
- `site:*.example.com`: Shows all subdomains.

Whois and Reverse Whois

Whois services like whois.icann.org and whois.com provide registered user information. Reverse Whois tools like viewdns.info list domains registered with the same organization name or email address.

Same IP and Passive DNS

Tools like atsameip.intercode.ca and RiskIQ Community Edition reveal other websites on the same server. Passive DNS records show all names resolved to the researched IP.

Location Searches

Geolocation Tools

Tools like Creepy and Echosec gather location data from social networks and image hosting services.

IP-Based Geolocation

Websites like iplocation.net map IP addresses to geographic locations. Use wigle.net to map Wi-Fi access points.

Image Searches

Reverse Image Search

Use Google Images, Bing Images, and TinEye to perform reverse image searches, identifying where else an image is used and its first appearance.

EXIF Data Analysis

EXIF data contains camera information and geolocation coordinates. Tools like Exiftool and online services like exifdata.com allow viewing this metadata.

SOCMINT

Social Media Intelligence (SOCMINT) focuses on data gathering and monitoring from social media platforms. Tools and techniques previously mentioned can help in SOCMINT investigations.

Use Specialized Tools

There are various OSINT tools available that can enhance your search capabilities. Some popular ones include:

Maltego: A powerful tool for mapping out relationships and networks.

Spiderfoot: An open-source tool that automates the collection of OSINT data.

Recon-ng: A web reconnaissance framework with a range of modules to gather information.

Conclusion

OSINT offers a wealth of opportunities for uncovering information about anyone, from social media profiles to public records and beyond. By following a structured approach and leveraging specialized tools, you can effectively gather, analyze, and verify information from publicly available sources.

Remember to always approach OSINT with ethical considerations in mind, ensuring that your efforts respect privacy and legal boundaries. Whether

you're a professional investigator or a curious individual, mastering OSINT can unlock a world of information at your fingertips.

• • •

References

1. Google Search Operators:

<https://support.google.com/websearch/answer/2466433?hl=en>

2. Maltego: <https://www.maltego.com>

3. SpiderFoot: <https://www.spiderfoot.net>

4. Shodan: <https://www.shodan.io>

By integrating these OSINT techniques and tools into your research process, you'll be well-equipped to find detailed and accurate information on anyone, enhancing your investigative capabilities in the digital age.



Written by Hayden.banz

68 Followers · Writer for OSINT Team

Follow



More from Hayden.banz and OSINT Team



 Hayden.banz in OSINT Team

The Art of Invisibility: Mastering OSINT Evasion Techniques

In an era where information is the new currency, the ability to protect one's digital...

Aug 10  74



...



 an0nbil in OSINT Team

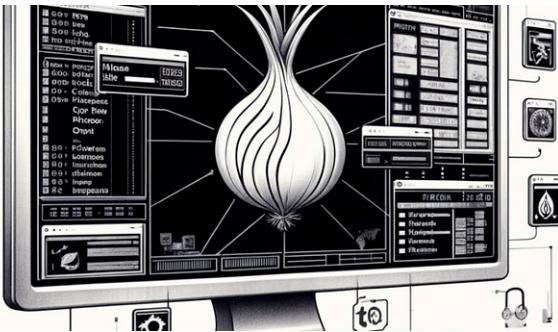
The WordPress bug very few know about.

Exploiting wp-cron.php file for DoS attacks and much more.

Jul 17  385  4



...



Ervin Zubic in OSINT Team

Point-and-Click OSINT: Dark Web Scraping with GUI Tools

Discover how to gather OSINT data from the dark web without coding. Learn point-and-...

Apr 30

323

5



...

Aug 6

109



...

[See all from Hayden.banz](#)
[See all from OSINT Team](#)

Recommended from Medium





Andrew Blooman

Build Your Own Cyber Threat Intel Feeds at Home! (MISP)

Learn how to Collect Open Source Threat Intelligence

Aug 14

72

1



...



Abdul Issa in InfoSec Write-ups

Level Up Your Linux-Fu: Essential Linux Skills For Cybersecurity...

Practical Steps to Boost Your Linux Command Line, Scripting And Automation Skills

6d ago

68

2



...

Lists



Staff Picks

716 stories · 1235 saves



Stories to Help You Level-Up at Work

19 stories · 754 saves



Self-Improvement 101

20 stories · 2584 saves



Productivity 101

20 stories · 2228 saves



Henrique Centieiro & Bee ...



in Limitless Invest...

The World Economy is About to be Wiped Out by a Black Swan—...

No One Sees This Coming—Actions You Can Take Right Now.

Aug 12

7.5K

116



...



Indranil in System Weakness

How To Take Down Any Phishing Website In Minutes

Let's take down the YONO SBI Phishing website mentioned in the previous post.

Mar 6

537

4



...



 Vasileiadis A. (CyberKid)

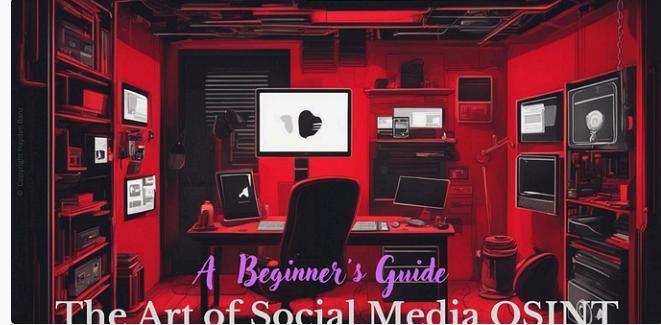
Detect hidden surveillance cameras with your phone

A family recently it had a big surprise on their Airbnb: a hidden camera disguised as a...

Aug 5  54



...



 Hayden.banz in OSINT Team

The Art of Social Media OSINT : A Beginner's Guide

In today's digital age, information is abundant and easily accessible, thanks to the vast real...

Jun 22  126



...

[See more recommendations](#)