



General

FA2025 • 2025-09-25

Open Source Intelligence

Michael Khalaf and Julius White

Announcements

- **Thank you for playing Fall CTF 2025!**
 - Challenges will be migrated to our internal CTF platform
 - Stick around for a recap and challenge walkthrough at the end of today's meeting!
- Sunshine CTF ([Sunshine CTF](#))
 - Saturday, September 27th, 2025 at 9am
 - Runs for 48 hours to Monday at 9am
 - Siebel CS (Room TBD)



ctf.sigpwny.com

sigpwny{i_th33_y0u}

WHY I'M QUITTING FACEBOOK,
JOINING LINKEDIN, DELETING MY
LINKEDIN, REJOINING FACEBOOK,
QUITTING TWITTER, GETTING
LOCKED OUT OF FACEBOOK,
MOVING TO MASTODON, AND
LOBBYING MICROSOFT TO TAKE
OVER MASTODON AND MERGE
IT WITH LINKEDIN: A MANIFESTO.



What is OSINT?

- Open Source
 - The stuff you are gathering is accessible to the general public
 - If it is not immediately accessible, it will be
- Intelligence
 - Information that can be used / is valuable for some operation.
 - Big range of value
 - Birthdays and usernames >> post content etc.
 - Can be used to guess passwords & bypass security questions
- Pseudonyms
 - Recon, Cyberreconnaissance, HUMINT etc.



A Warning (OSINT Ethics)

OSINT, especially HUMINT (Human Intelligence) is functionally **stalking**.

DON'T BE A CREEP

Make sure you have permission before OSINTing someone/thing

You could find something you don't like / aren't supposed to



Explicit OSINT Code of Ethics

1. You will **not INTERACT** with any user without first **confirming with absolute certainty** that they are a part of the challenge. In the case of these challenges, there is **no need to create any content**
2. You will **not perform any port scans on backend services** or attempt to do any investigation by logging in to any of the aforementioned accounts. This is **not web hacking**
3. You will **not perform invasive investigative OSINT on other people without their explicit consent**. This includes **friends, family, coworkers, and strangers**.

While **exceptions exist to this code**, those exceptions **don't apply here!**



OSINT vs Active Reconnaissance

- OSINT

Gathering strictly publicly available information, through relatively passive means

e.g. looking at someone's house on zillow

- Active Reconnaissance

You are actively interacting with your victim, trying to find exploits / sensitive data

e.g. walk up and see if the doors are unlocked

this is illegal and will get you in trouble



Signals Intelligence

In this meeting, we are only discussing methods that let the system into giving you information voluntarily

Methods

- Port scanning (nmap)
- Port-search sites (Shodan and Zoomeye)
- Exposed sensitive files (Grayhatwarfare and Shodan)

If you want to know active ways of gathering intelligence, go attend **Purple Team** meetings!



Port Scanning - Common Ports

Port	Service	Port	Service	Port	Service	Port	Service
20-21	FTP (File Transfer)	137-139	NetBIOS (Sessions)	530	RPC (Remote Procedure Calls)	3479	PlayStation Network
22	SSH (Secure Shell)	156	SQL (Databases)	666	DOOM ONLINE	4070	Amazon Echo Dot → Spotify
23	Telnet (Text comms)	194	IRC (Chatting)	666	Aircrack-ng C2 Server	4444	Metasploit listener
25	SMTP (Mail Transfer)	311	macOS Server (Admin)	740-754	Kerberos related stuff	5000	AirPlay (Among Others)
53	DNS (Domains)	389	LDAP (Windows) (Active Directory Access)	1776	EMIS (1st Responders)	5900	VNC (Virtual Network Computing)
67-68	Bootstrap / DHCP	443	HTTPS (Websites)	3074	Xbox for Windows	5985	Powershell (Remote Management)
80	HTTP (Websites)	444	AD (Windows) (Active Directory)	3306	MySQL (Databases)	8080	Alternate HTTP (Also 8000 / 8008)
88	Kerberos (Authentication)	445	SMB (Windows)	3389	RDP (Microsoft Remote)	25565	Minecraft Server


https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers



Port Scanning

- Tools: nmap and rustscan
- Adversarial
 - Ports being open can often provide information about a system.
 - If 80, 443, and 8080 are open it probably has a website.
 - But if 53 (DNS), 88 (Kerberos), 135, 139, 445 (SMB-related), 389 (LDAP), etc... it is likely a Domain Controller (DC)
- Ethical / Legal
 - Port scanning can harm system availability (DDoS)
 - Starts to enter a legally / ethically grey area
 - **DO NOT PORTSCAN THE GODDAMN US GOVERNMENT**




 SHODAN

Explore

Pricing ↗

anonymous access granted




Login

TOTAL RESULTS

15,402


TOP COUNTRIES





United States	4,791
Japan	2,356
Germany	1,734
France	778
Italy	562
More...	

TOP PORTS

21	15,178
2121	198
221	18
20	4
14147	3

 View Report


 View on Map

 Advanced Search

Access Granted: Want to get more out of your existing Shodan account? Check out [everything you have access to.](#)

118

TOT Public Company Limited

 Thailand, Bangkok

220 ProFTPD Server (ProFTPD Default Installation) [192.168.100.2]

230-Welcome to the Binro.Org **anonymous** FTP service.

230 **Anonymous access granted**, restrictions apply


214-The following commands are recognized (* =>'s unimplemented):

CWD XCWD CDUP XCUP SMNT* QUIT PORT PASV...

2024-09-15T19:49:15.768231

179

179.186.139.78.dynamic.a
dsl.gvt.net.br

 Brazil, João Pessoa

220 179.186.139.78 FTP server ready

230 **Anonymous access granted**, restrictions apply

214-The following commands are recognized (* =>'s unimplemented):

CWD XCWD CDUP XCUP SMNT* QUIT PORT PASV


EPRT EPSV ALLO* RNFR RNTD DELE MDTM RMD


XRMD MKD...

2024-09-15T19:46:42.792332

86

mm-47-235-57-86.static.m
gts.by

 Belarus, Minsk

 SSL Certificate

Issued By:

- Common Name:

QNAP NAS

- Organization:

QNAP Systems, Inc.

Issued To:

- Common Name:

QNAP NAS

220 NASFTPD Turbo station 1.3.5a Server (ProFTPD)

230 **Anonymous access granted**, restrictions apply

214-The following commands are recognized (* =>'s unimplemented):

CWD XCWD CDUP XCUP SMNT* QUIT PORT PASV

EPRT EPSV ALLO* RNFR RNTD DELE MDTM RMD ...

2024-09-15T19:43:42.769207

Human Intelligence

- What is the **email format** (firstname.lastname)
 - Directly linked to AD account names (and potentially passwords)
- Preferred restaurants, airline, hotel etc.
- What are their IT/security protocols?
- Internal document leakage



OSINT Tips: Identities

Split Identities

- Most people have at least **two** identities online
 - Professional
 - Casual
- You want to find correlations of them when doing OSINT

Sherlock

- Can be used to find specific usernames on tons of platforms.
- Definitely try it on your usernames!



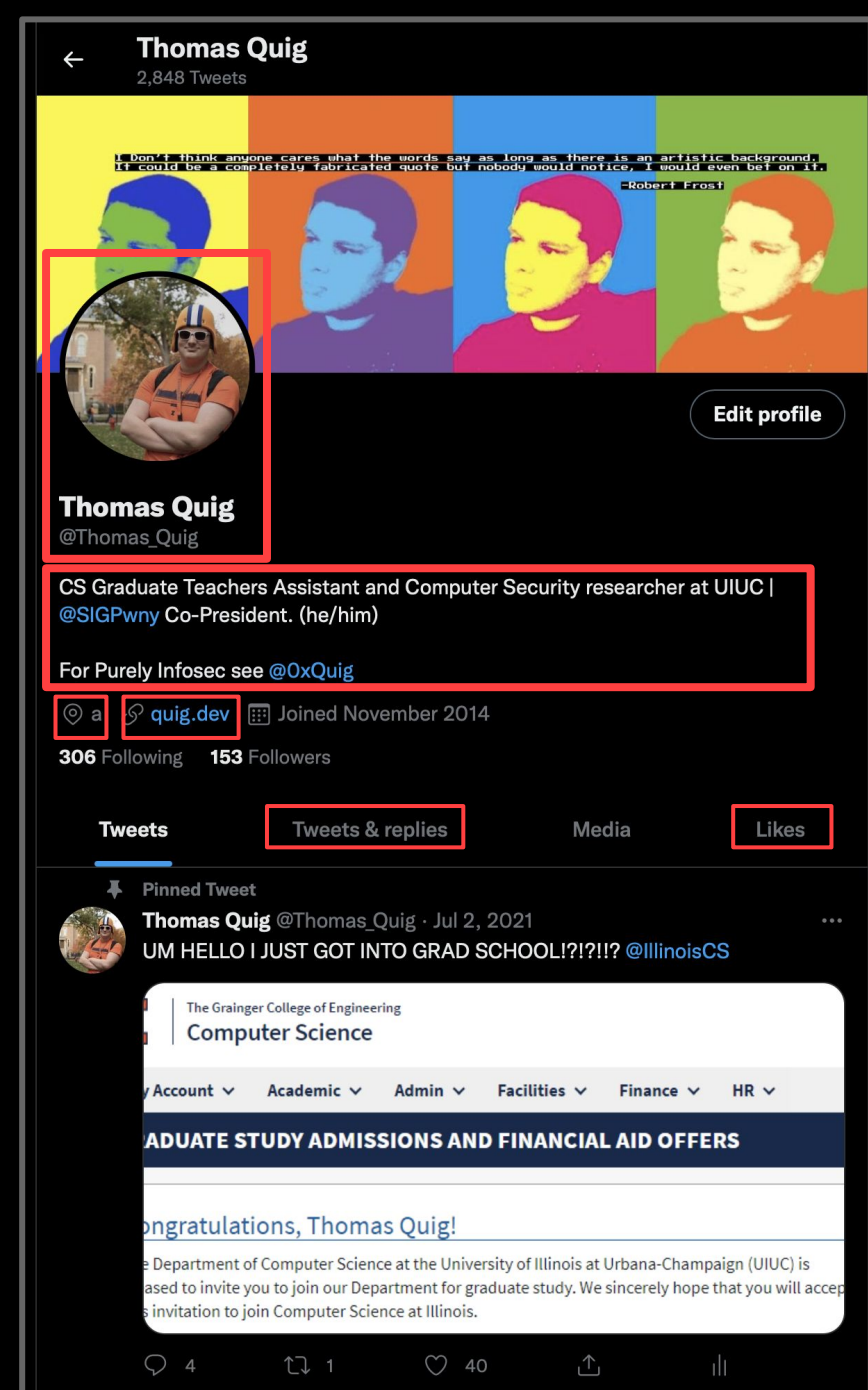
Personal Information

- **Social Media Profiles**
 - Links, pictures, identifying information
 - Build a map of someone
- **Username Reuse**
 - Same across lots of places!
 - Helpful for these chals!
- Images
 - Reverse image searching!
- Deleted Content
 - Archivists save old websites!
 - Wayback machine!



X/Twitter

- TWEETS & replies are ALWAYS WHERE YOU SHOULD LOOK FIRST
- Twitter bios have info, location, birthday, and a link to somewhere
- Advanced Searches: good
- Follower / Following lists can help find friends



Reddit

- Reddit is a **semi-anonymous** website
- Link people to **other platforms**
- Profile
 - **Profile Pictures, Banner Photos**
 - Comments, posts, links
 - Moderator
 - Awards
- Posts
 - Search by top
- **old.reddit.com**

[OVERVIEW](#)
[POSTS](#)
[COMMENTS](#)
[AWARDS RECEIVED \(LEGACY\)](#)

New
 Hot
 Top

Sonicninja commented on I absolutely hate Sm*t le. Housing · r/UIUC · Posted by u/Educational_Quit_278

ForgottenAgarPlate 18 points · 1 month ago
lol I pulled into my parking spot for the first time today and there was 1) a few gila see more

Sonicninja 4 points · 1 month ago
Hi neighbor I think you park next to me LOL

[Reply](#) [Share](#) ***

Sonicninja commented on New Mascot: Illungus i.redd.it/t2ydsu... Shitpost · r/UIUC · Posted by u/BSCChemist

Sonicninja 20 points · 1 month ago
GET OUT OF MY HEAD GET OUT OF MY HEAD GET OUT OF MY HEAD GET OUT OF MY HEAD GET OUT OF MY HEAD GET OUT OF MY HEAD GET OUT OF MY HEAD GET OUT OF MY HEAD GET OUT OF MY HEAD GET OUT OF MY HEAD GET OUT OF MY HEAD GET OUT OF MY HEAD GET OUT OF MY HEAD GET OUT OF MY HEAD GET OUT OF MY HEAD GET OUT OF MY HEAD GET OUT OF MY HEAD GET OUT OF MY HEAD

[Reply](#) [Share](#) ***

Sonicninja commented on I am new to osint where should I start? Question · r/OSINT · Posted by u/Witty-Ad876

Sonicninja 2 points · 1 month ago
All the above resources are great.

If you want simulated practice. Try some ctfs

UIUCTF has a suite of 6 live right now (beginner friendly, <https://uiuc.tf>), along with many other CTFS past and present.

[Reply](#) [Share](#) ***

Sonicninja commented on hey i've got a ticket for glaives show in islington london for tomorrow anyone interested? i cant make the date and re6ce is gonna be there too 🐼 Tour · r/glaivebossman · Posted by u/shushzara

Sonicninja 2 points · 2 months ago
re6ce is going to be there what?! Great for them!

[Reply](#) [Share](#) ***

Sonicninja
 u/Sonicninja · 9y

[**Create Your Own Avatar >**](#)

Stop trying to find hidden secrets in my reddit profile, good try though <3

Karma	Cake day
🔥 11,986	🍰 September 16, 2013

Follow

[More Options](#)

Moderator of these communities

r/signwiny
 3 members

Join

Trophy Case (7)

- Nine-Year Club
- Second
SECOND GUESSER
- Gilding II
euphauric

[View More](#)

Back To Top

Media OSINT

OPEN IMAGE IN NEW TAB!!!

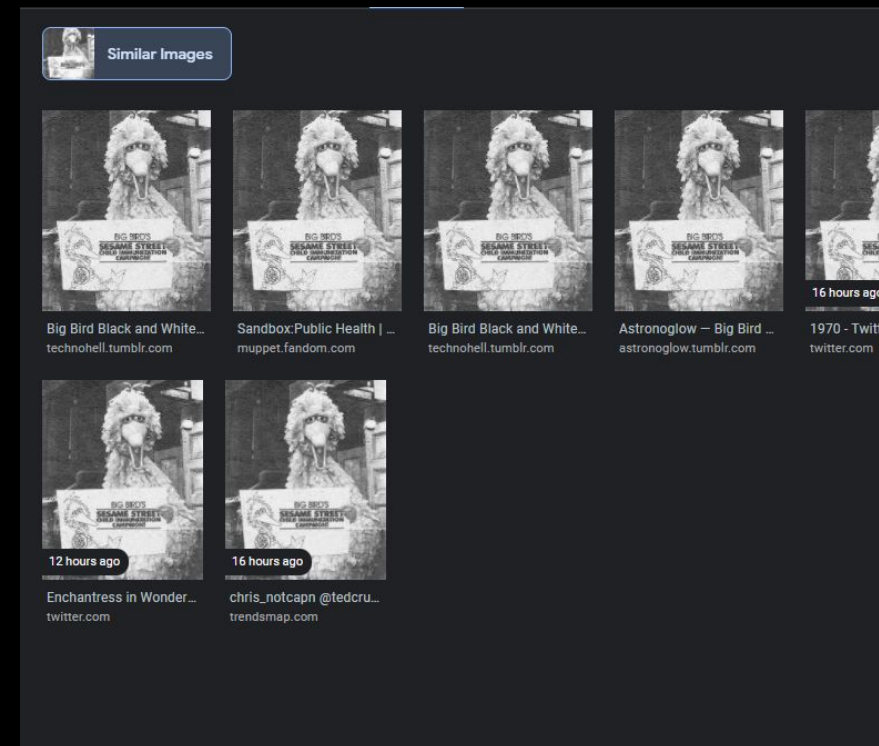
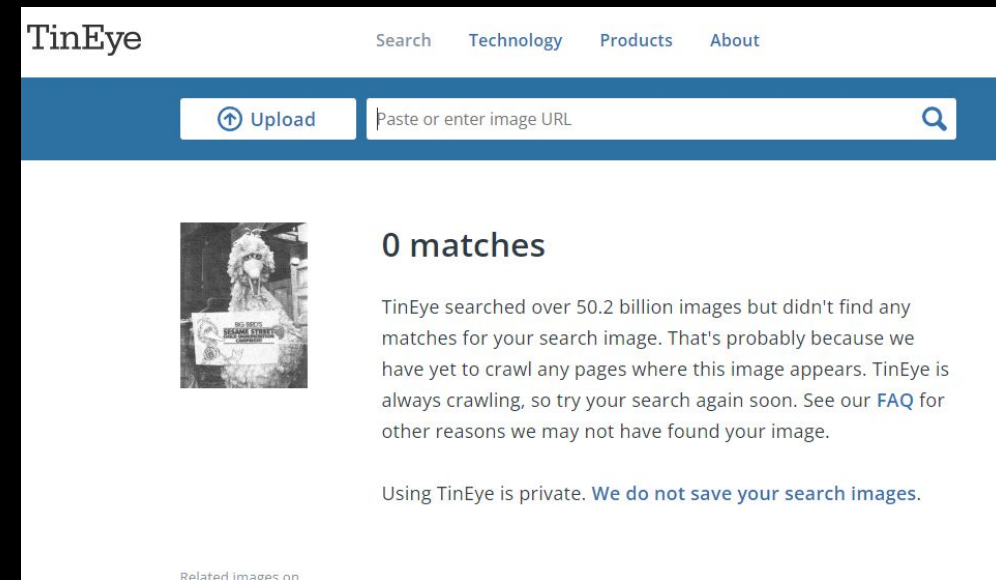
Google Image Search (Tineye, Yandex)

- Keyword searcher
- Cropping

Tineye: exact matches

Google: Similar

GOOGLE LENS IS YOUR FRIEND



How to profile a target?

Finding information may mean looking at people around them

Consider the example of a social network

Your goal is to find any access to a target of interest



Sherlock

-Command line utility that enumerates instances of similar or inputted usernames registered to public media applications

Ex. Run a query on the username “johndoe”

→ You see usernames registered under that alias

```
L$ sherlock johndoe
Update available! 0.15.0 → 0.16.0
https://github.com/sherlock-project/sherlock/releases/tag/v0.16.0
[*] Checking username johndoe on:

[+] 1337x: https://www.1337x.to/user/johndoe/
[+] 7Cups: https://www.7cups.com/@johndoe
[+] 9GAG: https://www.9gag.com/u/johndoe
[+] About.me: https://about.me/johndoe
[+] Academia.edu: https://independent.academia.edu/johndoe
[+] Airbit: https://airbit.com/johndoe
[+] Airlines: https://www.airliners.net/user/johndoe/profile/photos
[+] AllMyLinks: https://allmylinks.com/johndoe
[+] AniWorld: https://aniworld.to/user/profil/johndoe
[+] Anilist: https://anilist.co/user/johndoe/
[+] Apple Developer: https://developer.apple.com/forums/profile/johndoe
[+] Apple Discussions: https://discussions.apple.com/profile/johndoe
[+] Aparat: https://www.aparat.com/johndoe/
[+] Archive of Our Own: https://archiveofourown.org/users/johndoe
[+] Asciinema: https://asciinema.org/~johndoe
[+] Atcoder: https://atcoder.jp/users/johndoe
[+] Audiojungle: https://audiojungle.net/user/johndoe
[+] Autofrage: https://www.autofrage.net/nutzer/johndoe
[+] Bandcamp: https://www.bandcamp.com/johndoe
[+] Behance: https://www.behance.net/johndoe
[+] Bluesky: https://bsky.app/profile/johndoe.bsky.social
[+] Bookcrossing: https://www.bookcrossing.com/mybookshelf/johndoe/
[+] BraveCommunity: https://community.brave.com/u/johndoe/
[+] BugCrowd: https://bugcrowd.com/johndoe
[+] BuyMeACoffee: https://buymeacoff.ee/johndoe
[+] BuzzFeed: https://buzzfeed.com/johndoe
[+] CGTrader: https://www.cgtrader.com/johndoe
[+] Carbonmade: https://johndoe.carbonmade.com
[+] Championat: https://www.championat.com/user/johndoe
[+] Chatujme.cz: https://profil.chatujme.cz/johndoe
[+] Chess: https://www.chess.com/member/johndoe
[+] Clapper: https://clapperapp.com/johndoe
[+] Codeberg: https://codeberg.org/johndoe
[+] Codecademy: https://www.codecademy.com/profiles/johndoe
[+] Codechef: https://www.codechef.com/users/johndoe
[+] Codeforces: https://codeforces.com/profile/johndoe
[+] Coders Rank: https://profile.codersrank.io/user/johndoe/
```



Public Resources Matter

Municipal governments by local, state, and federal law are required to provide public resources to you, you can utilize them for localized searches depending on the nature of your search. **Don't stalk.**

- Birth records
- marriage records
- death records
- census data
- municipal data



Get Involved: Help Find Missing Persons!

-TraceLabs is an organization dedicated to crowdsourcing OSINT to help assist law enforcement with cases involving missing persons

-They provide a VM populated with OSINT tools to start you off in your search

-Submit flags to provide new information that advances a missing persons' case

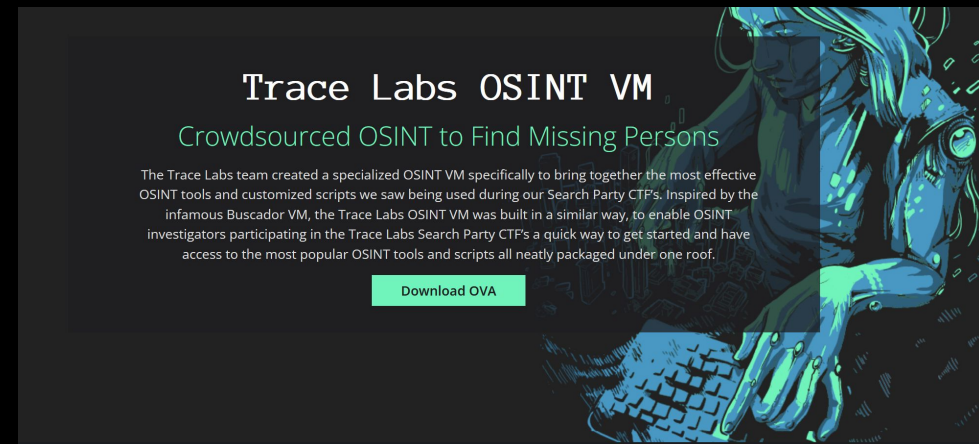


We crowdsource OSINT to help find missing people.

Become a Part of the Solution

Trace Labs is a nonprofit organization whose mission is to accelerate the family reunification of missing persons while training members in the tradecraft of open source intelligence (OSINT).

[Get Involved](#)




Trace Labs OSINT VM

Crowdsourced OSINT to Find Missing Persons

The Trace Labs team created a specialized OSINT VM specifically to bring together the most effective OSINT tools and customized scripts we saw being used during our Search Party CTF's. Inspired by the infamous Buscador VM, the Trace Labs OSINT VM was built in a similar way, to enable OSINT investigators participating in the Trace Labs Search Party CTF's a quick way to get started and have access to the most popular OSINT tools and scripts all neatly packaged under one roof.

[Download OVA](#)



Next Meetings

2025-09-27 • This Saturday

- Sunshine CTF 2025
- We'll be playing casually somewhere in Siebel CS - food included!

2025-09-28 • This Sunday

- Physical Security and Lockpicking
- We bring the locks and picks, you bring yourself!

2025-10-02 • Next Thursday

- Reverse Engineering I
- Learn the tools and techniques to reverse engineer programs!



ctf.sigpwny.com

sigpwny{i_th33_y0u}

Meeting content can be found at
sigpwny.com/meetings.





Fall CTF 2025

Recap and Walkthrough