SIGPwny

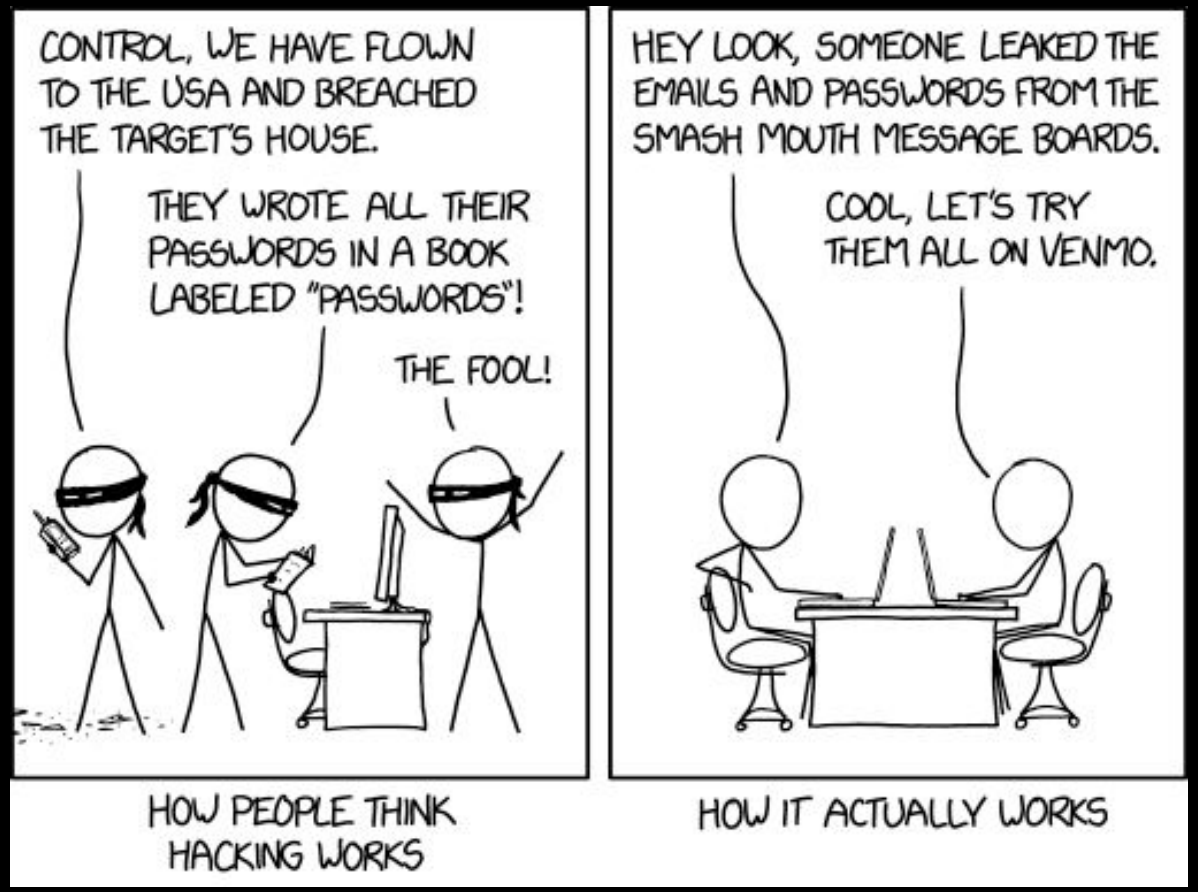
General FA2026 • 2026-11-05

Open Source Intelligence II

Tyler Mercado

ctf.sigpwny.com

sigpwny{y0u_4r3_th3_t4rg3t_n0w}



xkcd.com/2176

Contents

- OPSEC: protecting yourself
- OSINT tricks
- Shodan and other search engines
- Challenges



Explicit OSINT Code of Ethics

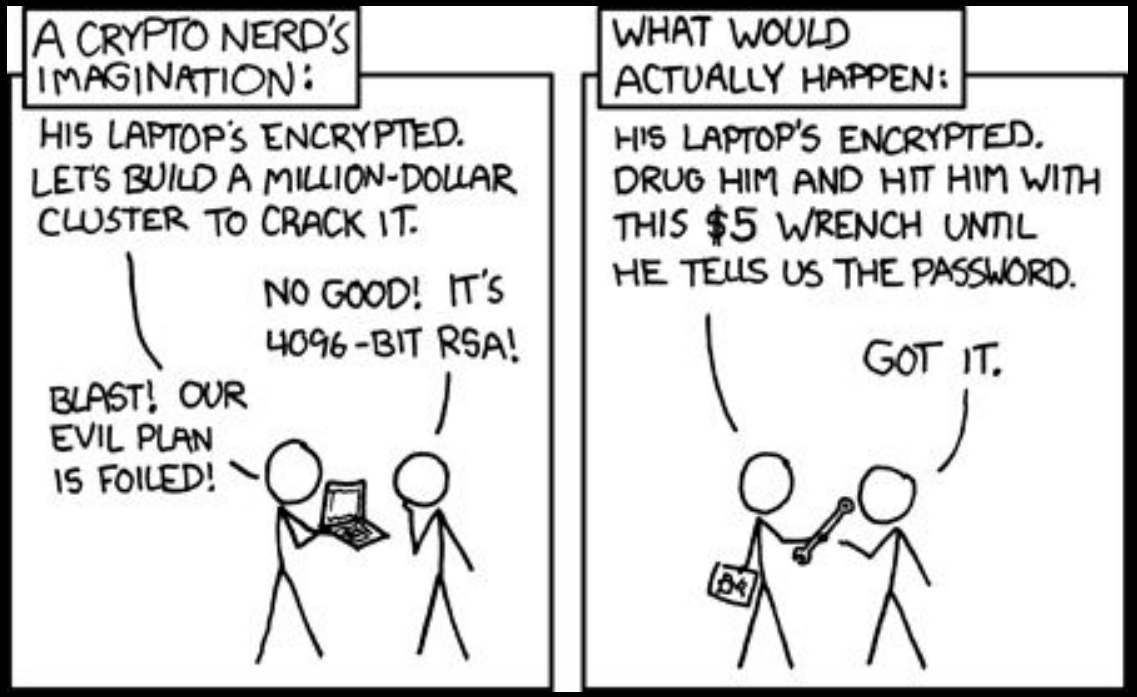
1. You will **not INTERACT** with any user without first confirming with absolute certainty that they are a part of the challenge. In the case of these challenges, there is **no need to create any content**
2. You will **not perform any port scans on backend services** or attempt to do any investigation 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!



What is OPSEC?

- Protecting small details that add up to something sensitive
- Ask yourself:
  - What am I protecting?
  - Who am I protecting it from?
  - How much effort is it worth?



xkcd.com/538



OPSEC Fails

- Ross Ulbricht: reused a username, later posted his real Gmail
- John McAfee: photo GPS data showed he was in Guatemala
- Strava: soldiers’ runs mapped out secret bases
- Reality Winner: printer tracking dots on a leaked document
- Mitt Romney: secret Twitter found through who it followed



Look Yourself Up

- Search your name and usernames in a private window
- Run Sherlock on your usernames
- Check haveibeenpwned.com
- Check people search sites
  - Whitepages, TruePeopleSearch, FastPeopleSearch
- Google “Results about you” can remove your address and phone number



Photos

- EXIF data can include GPS location, time, and camera
- Most apps remove it, but email attachments and “send as file” often keep it
- Also check reflections, windows, mail, badges, and boarding passes

```
exiftool photo.jpg          # read it
exiftool -all= photo.jpg    # remove it
```



Keeping Things Separate

- Use different usernames, emails, and profile pictures for different identities
- Email aliases: SimpleLogin, Firefox Relay, Hide My Email
- Your phone number links your accounts together
- Hide your follower lists and tagged photos



Researching Without Being Noticed

- LinkedIn shows who viewed a profile
- Stories show who watched them
- Use a separate account and browser profile
- Don’t like, follow, or reply
- Don’t click links your target sends you



Search Tricks

- Operators: site: filetype: inurl: intitle: "exact" -word
- Try Bing and Yandex too, they index different things

```
site:docs.google.com "sigpwny"
filetype:pdf site:illinois.edu "resume"

# every URL the Wayback Machine saved for a site
web.archive.org/cdx/search/cdx?url=sigpwny.com/*
```



IDs and Commits

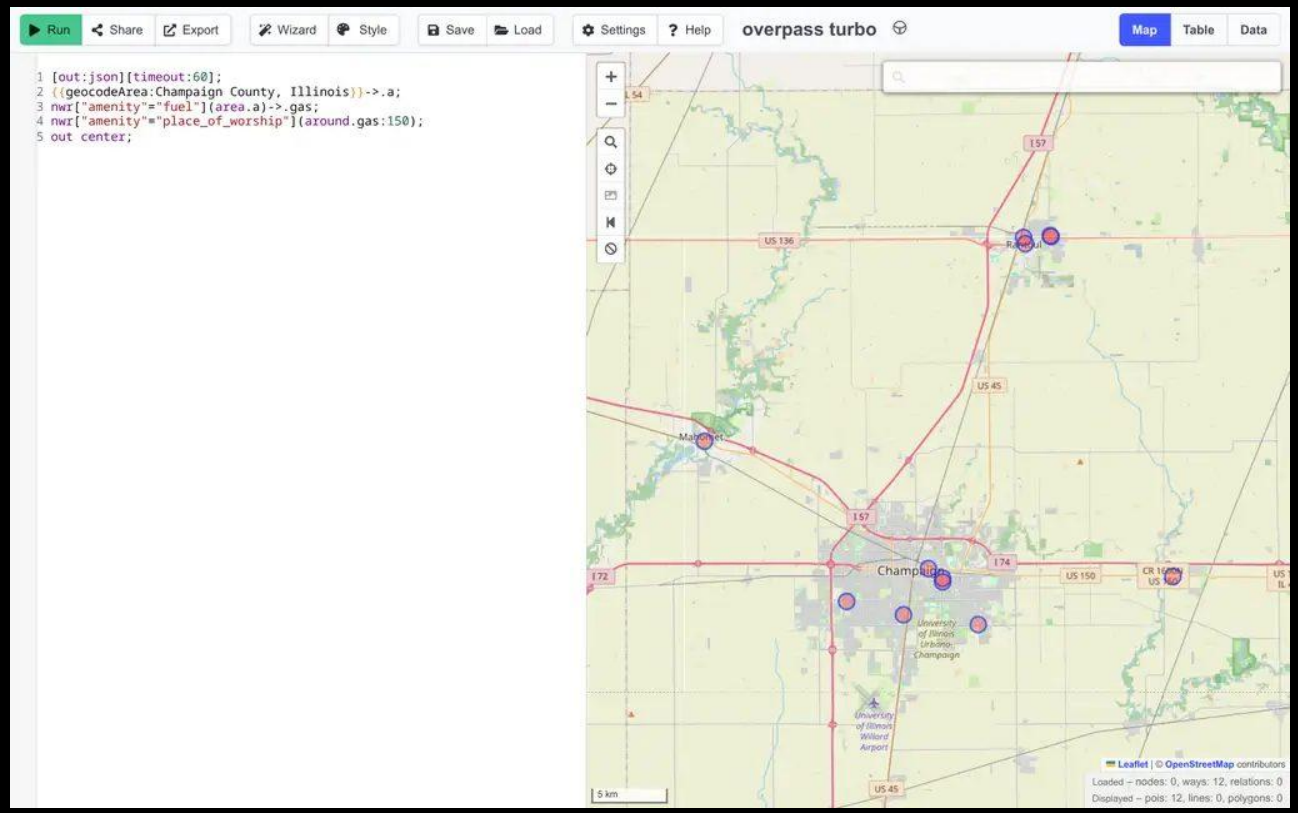
- Discord and Twitter IDs contain a timestamp
- Usernames change, numeric IDs don’t
- Add .patch to a GitHub commit URL to see the author’s email and timezone

```
$ curl -sL github.com/git/git/commit/0ffa3e35c7.patch
From: Junio C Hamano <gitster@pobox.com>
Date: Wed, 4 Nov 2026 11:04:29 -0800
```



Finding a Location

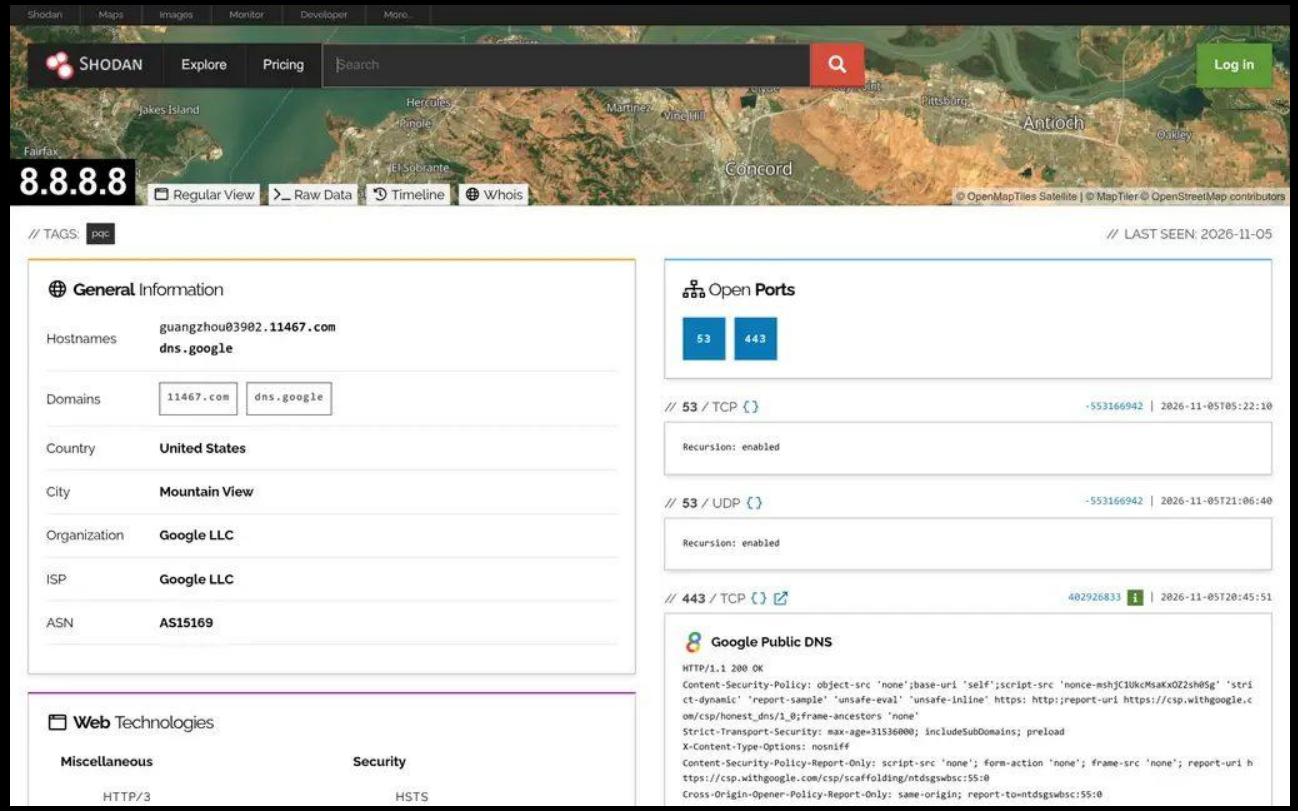
- Crop and reverse search parts of the photo
- Look at signs, plates, poles, and road lines
- SunCalc for shadows
- Overpass Turbo to search the map for features



Gas stations next to churches in Champaign County

Shodan

- Search engine for devices on the internet
- Shows open ports, banners, and history
- Free upgrade with a .edu email
- internetdb.shodan.io/<ip> needs no account



shodan.io/host/8.8.8.8

Shodan Filters

- Looking at results is fine. Logging in to anything is not.

```
org:"University of Illinois" port:3389
ssl.cert.subject.cn:"sigpwny.com"
http.title:"Grafana" country:"US"
has_screenshot:true port:5900
http.favicon.hash:<hash>
```



Other Tools

- Censys: hosts and certificates
- crt.sh: find subdomains from certificates
- urlscan.io: see what a website loads
- GreyNoise: check if an IP is a scanner
- WiGLE: Wi-Fi network names to locations
- GrayHatWarfare: open cloud storage buckets



Try It

- Look yourself up for 10 minutes
- Then try the OSINT challenges on ctf.sigpwny.com
- The Code of Ethics still applies



Next Meetings

2026-11-08 • This Sunday

- Check sigpwny.com/meetings for the topic



ctf.sigpwny.com

`sigpwny{y0u_4r3_th3_t4rg3t_n0w}`

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



SIGPwny