SIGPwny

FA2024 Week 04 • 2024-09-26

OSINT I

Henry and Julius

Announcements

- **Thank you for playing Fall CTF 2024**
  - Challenges will be migrated to our internal CTF platform
  - Writeups will be released

- BuckeyeCTF
  - Friday 7 PM - Sunday 7 PM
  - Room TBD, meeting in Siebel

ctf.sigpwny.com

sigpwny{g3tting_to_kn0w_you}

OSINT

Open **S**ource **INT**elligence

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 Challenge Ethics

DON'T CHEAT ON REDDIT

I have made two sets of challenges in competitions so far (on uiuctf24 and fallctf24). Both times someone posted the question on Reddit and got response from the internet.

Getting hints/answer from someone else without doing the search yourself is CHEATING in any competition.

WALL OF SHAME

Spamakin 06/29/2024 11:21 AM Jump
https://www.reddit.com/r/whereisthis/comments/1dr1bto/china_but_where/

Reddit

From the whereisthis community on Reddit

Explore this post and more from the whereisthis community

r/ whereisthis

Emma 06/29/2024 12:03 PM Jump
https://www.reddit.com/r/whereisthis/comments/1drffsr/where_is_this_c17_globemaster_iii_landed/?utm_source=share&utm_medium=mweb3x&utm_name=mweb3xcss&utm_term=1&utm_content=share_button

Reddit

From the whereisthis community on Reddit: Where is this C-17 Globem...

Explore this post and more fr
whereisthis community

Emma 06/29/2024 12:17 PM Jump
https://www.reddit.com/r/aviation/comments/1dracvs/does_anyone_recognize_the_airport/?utm_source=share&utm_medium=mweb3x&utm_name=mweb3xcss&utm_term=1&utm_content=share_button

Reddit

From the aviation community on Reddit

ore this post and more from the aviation
munity

Modmail APP 06/30/2024 4:14 PM Jump

neurochick#0

FYI another trying Reddit—- https://www.reddit.com/r/shenzhen/comments/1drc5wo/help_in_localizing_a_picture/?rdt=47865

Message ID: 1257081760370393220 • 06/30/2024 4:14 PM

Reddit

I can't figure this out, can someone help? : r/...

See exact matches

Types of Intelligence

- Signals Intelligence (SIGINT)

  A military term for information collection on any device that transmits “signals”

  i.e. as old as radios, computers, servers, routers, etc.

- Human Intelligence (HUMINT)

  Collection of information from human sources

  i.e. interpersonal interactions, now internet and social media

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

Signals Intelligence - Summary

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

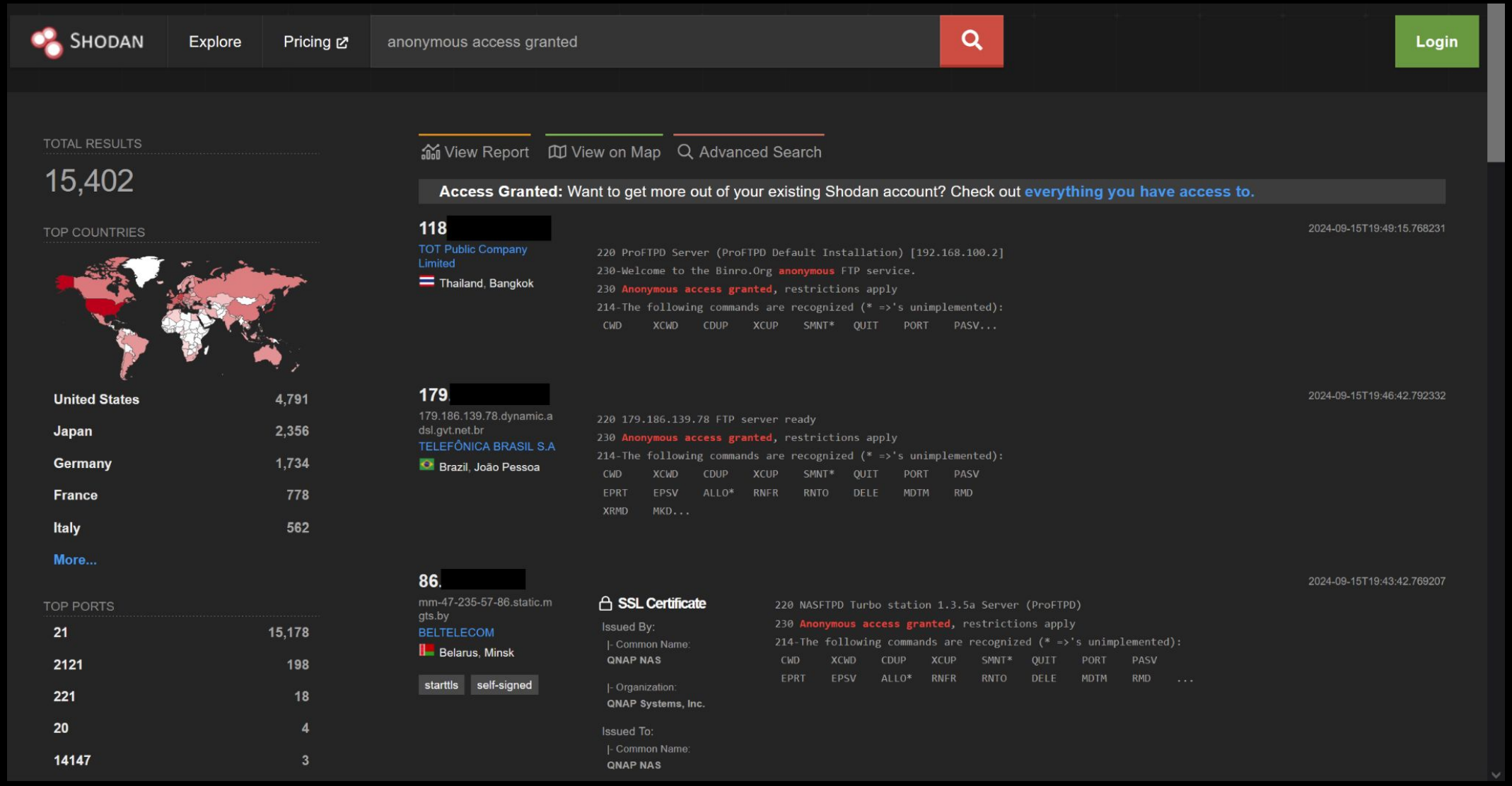
Port Scanning

- Tools: nmap and rustscan

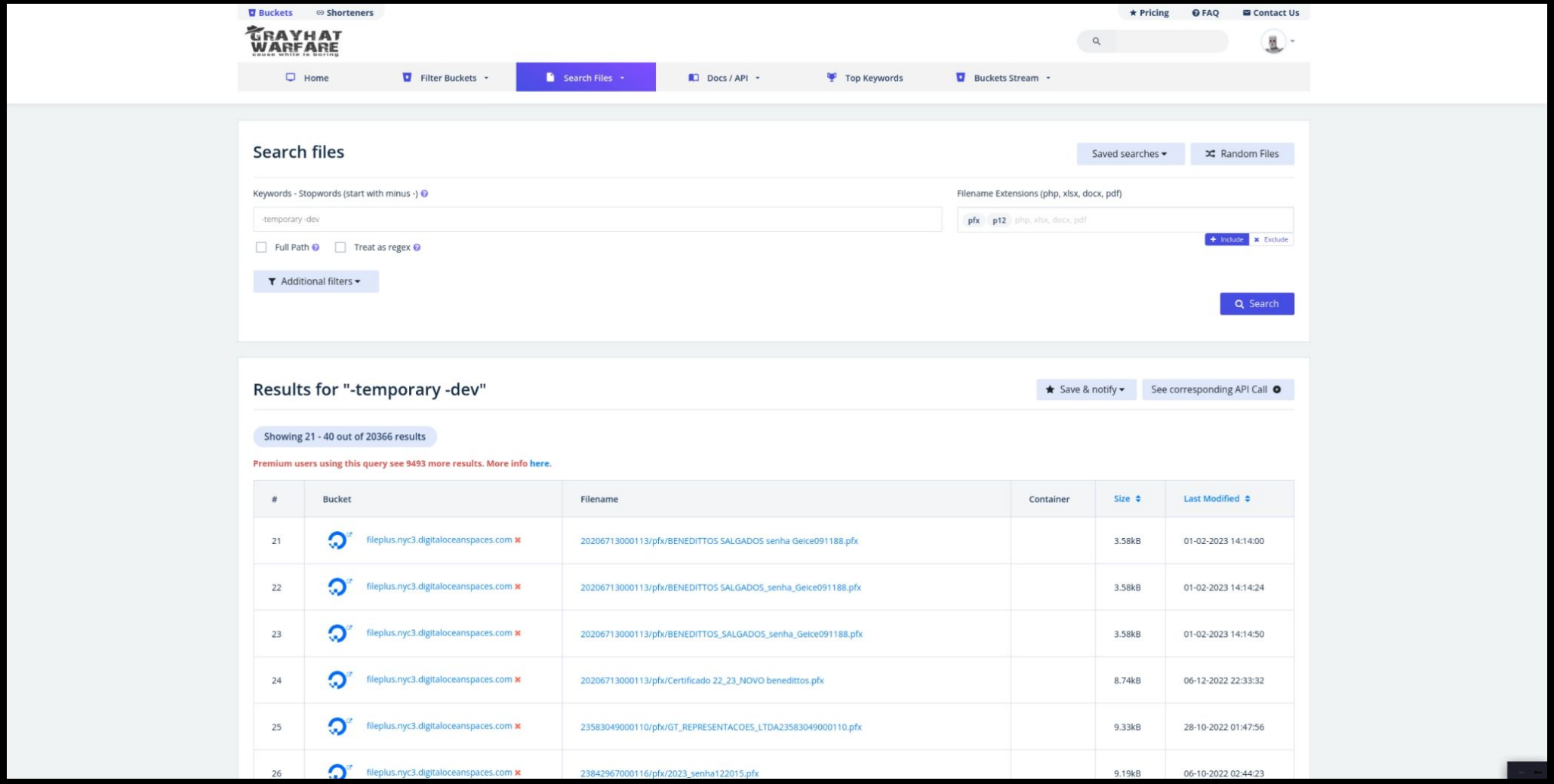
- Adversarial
  - Ports being open can often provide information about a system.
  - If 80, 443, and 8080 are open it probably has a website.
  - But if 53 (DNS), 88 (Kerberos), 135, 139, 445 (SMB-related), 389 (LDAP), etc… it is likely a Domain Controller (DC)

- Ethical / Legal
  - Port scanning can harm system availability
  - Starts to enter a legally / ethically grey area
  - **DO NOT PORTSCAN THE GODDAMN US GOVERNMENT**

Shodan


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 [redacted]
TOT Public Company Limited
Thailand, Bangkok
2024-09-15T19:49:15.768231
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...
179 [redacted]
179.186.139.78.dynamic.adsl.gvt.net.br
TELEFÔNICA BRASIL S.A
Brazil, João Pessoa
2024-09-15T19:46:42.792332
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 RNTO DELE MDTM RMD
XRMD MKD...
86. [redacted]
mm-47-235-57-86.static.mgts.by
BELTELECOM
Belarus, Minsk
starttls self-signed
SSL Certificate
Issued By:
|- Common Name:
QNAP NAS
|- Organization:
QNAP Systems, Inc.
Issued To:
|- Common Name:
QNAP NAS
2024-09-15T19:43:42.769207
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 RNTO DELE MDTM RMD ...

Grayhatwarfare



Human Intelligence

Human Intelligence - Organization

- 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

Human Information - Personal

- **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!

General OSINT Methods

Mostly applies to everything

OSINT Tips - Identities

Split Identities

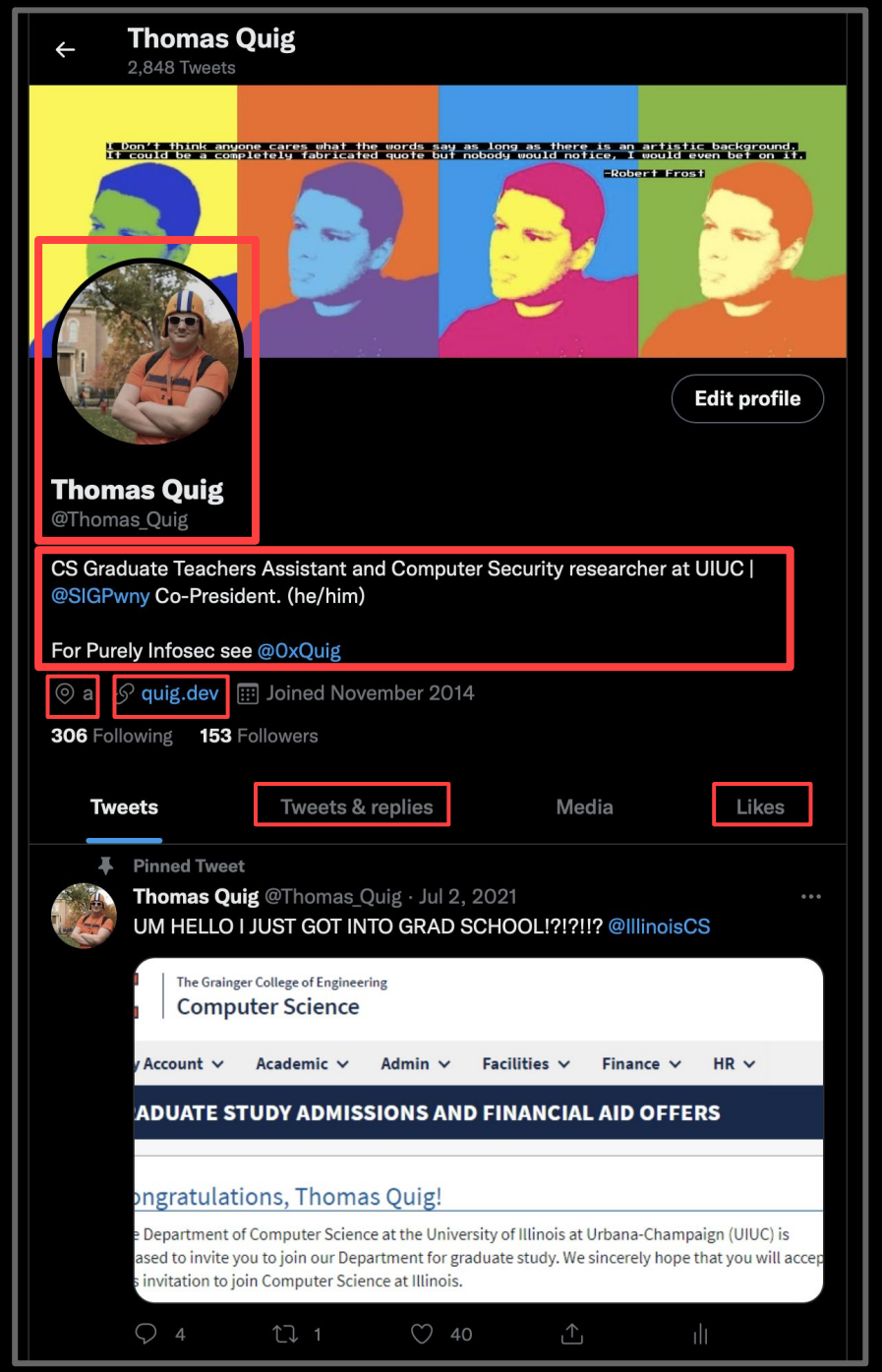
- Most people have at least **two** identities online
  - Professional
  - Casual
- You want to find correlations of them when doing OSINT

Sherlock

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

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**



YouTube

Channels

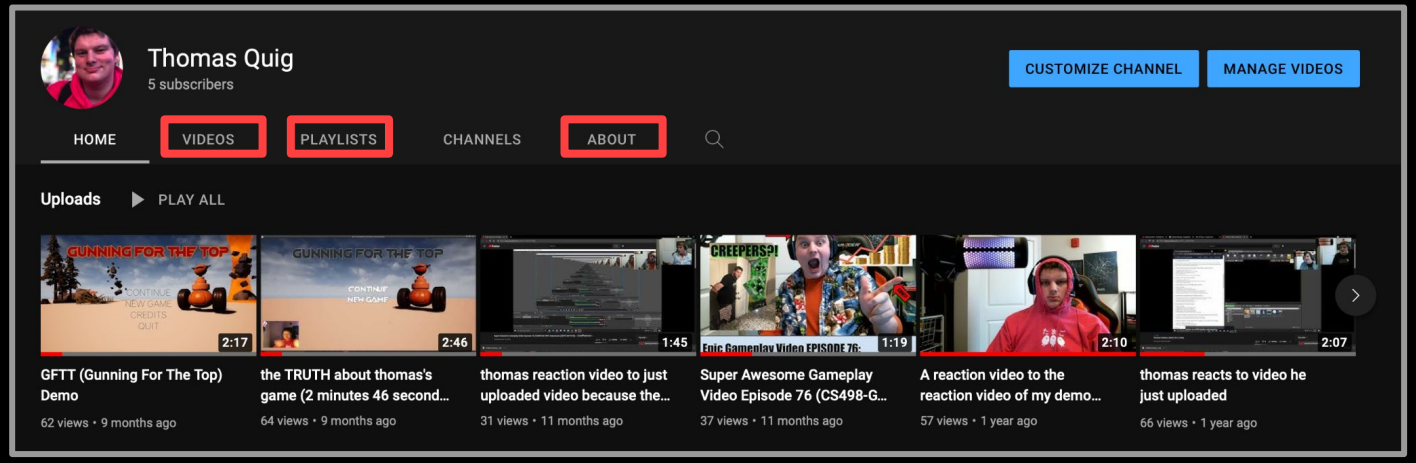
- Banner, Profile Picture
- About tab, playlists

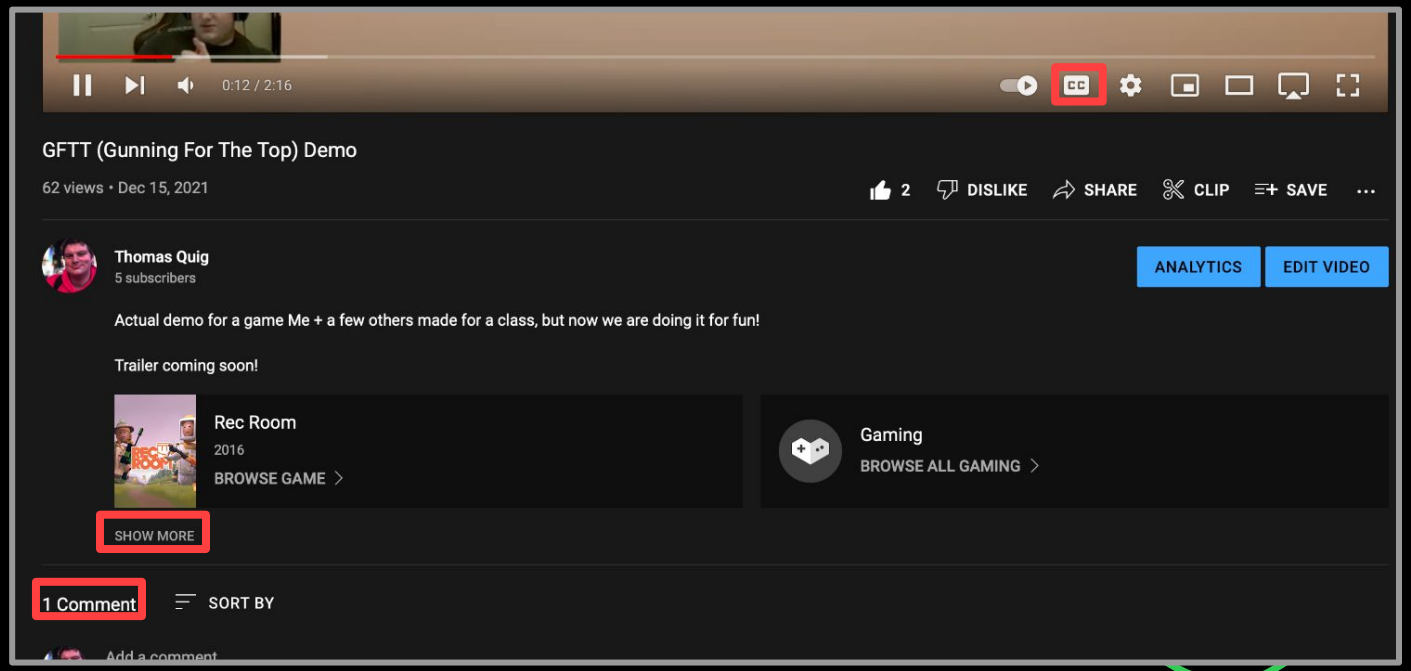
Playlists

- Unlisted videos are **visible**

Videos

- Closed captions, different languages. 3 Englishes!
- Description, comments (not searchable)





GitHub

Profile page

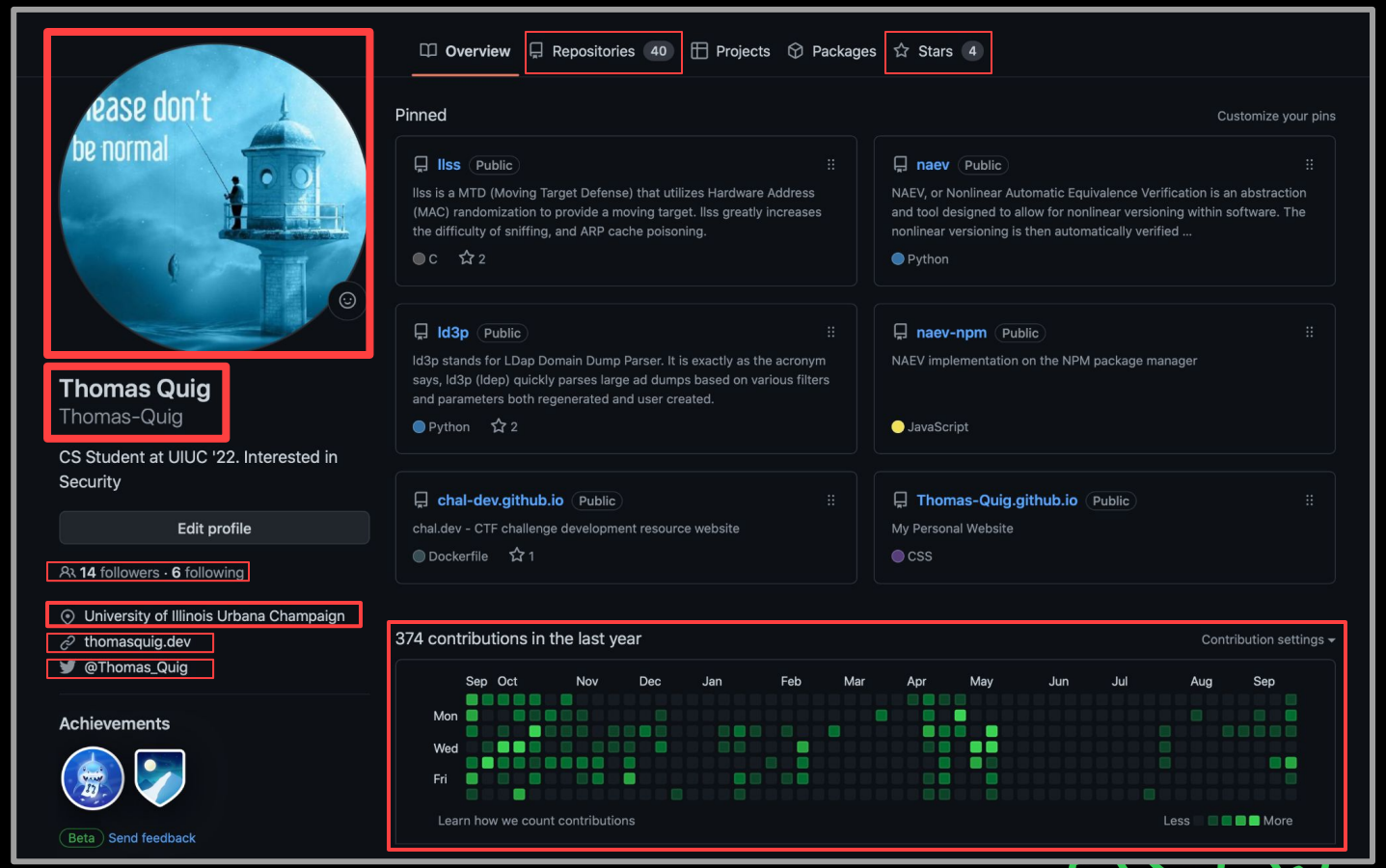
- View featured repos
- Links, socials, location
- email

Repositories

- Commit history
- Pull Requests & Comments

Comments / User Content

- Can exist in many places



main | 2 branches | 1 tag | Go to file | Add file | Code

Thomas-Quig Update README.md — 06cc48f on Jan 31, 2021 — 421 commits

captures	:)	2 years ago
notes	Update bugs.md	2 years ago
src	More test files	2 years ago
tests	H	2 years ago
README.md	Update README.md	2 years ago
SECURITY.md	Create SECURITY.md	2 years ago
TODO.md	Added TODO.md	2 years ago

README.md

llss

LLSS, or 'Link Layer Stable Switcher' is a networking tool for linux-enabled devices designed for stability and security. llss is a MTD (Moving Target Defense) that utilizes Hardware Address (MAC) randomization to provide a moving target. This greatly increases the difficulty of sniffing, and ARP cache poisoning. At the moment, this project is **optimized to work in an ad-hoc, wireless environment**

Examples

About

llss is a MTD (Moving Target Defense) that utilizes Hardware Address (MAC) randomization to provide a moving target. llss greatly increases the difficulty of sniffing, and ARP cache poisoning.

llss.page

networking | security-tools | shuffling | hardware-address-shuffling

Readme

2 stars

1 watching

0 forks

Releases 1

Release 2.0.0 Latest

on Jun 25, 2021

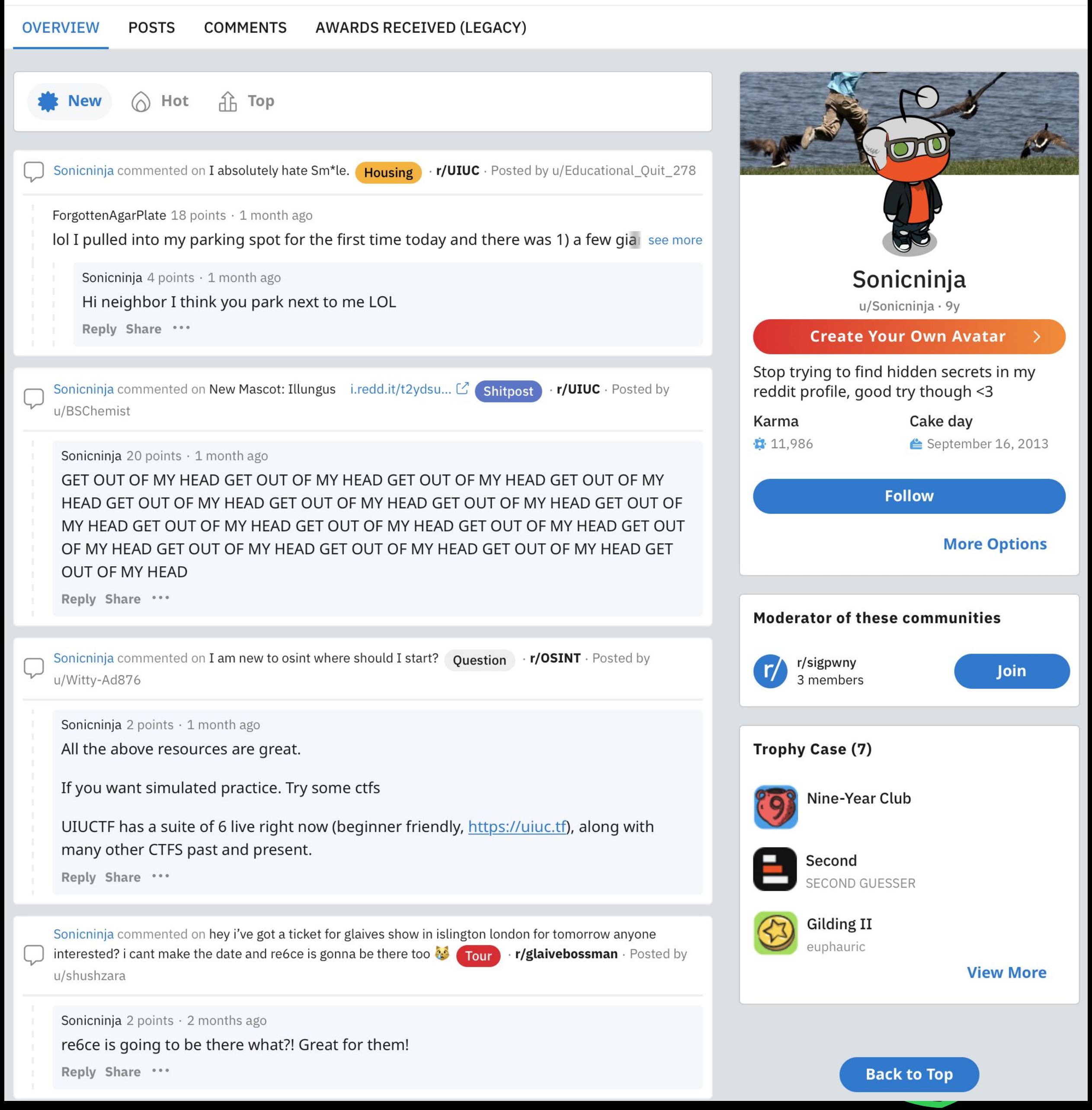
Packages

No packages published

Publish your first package

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**

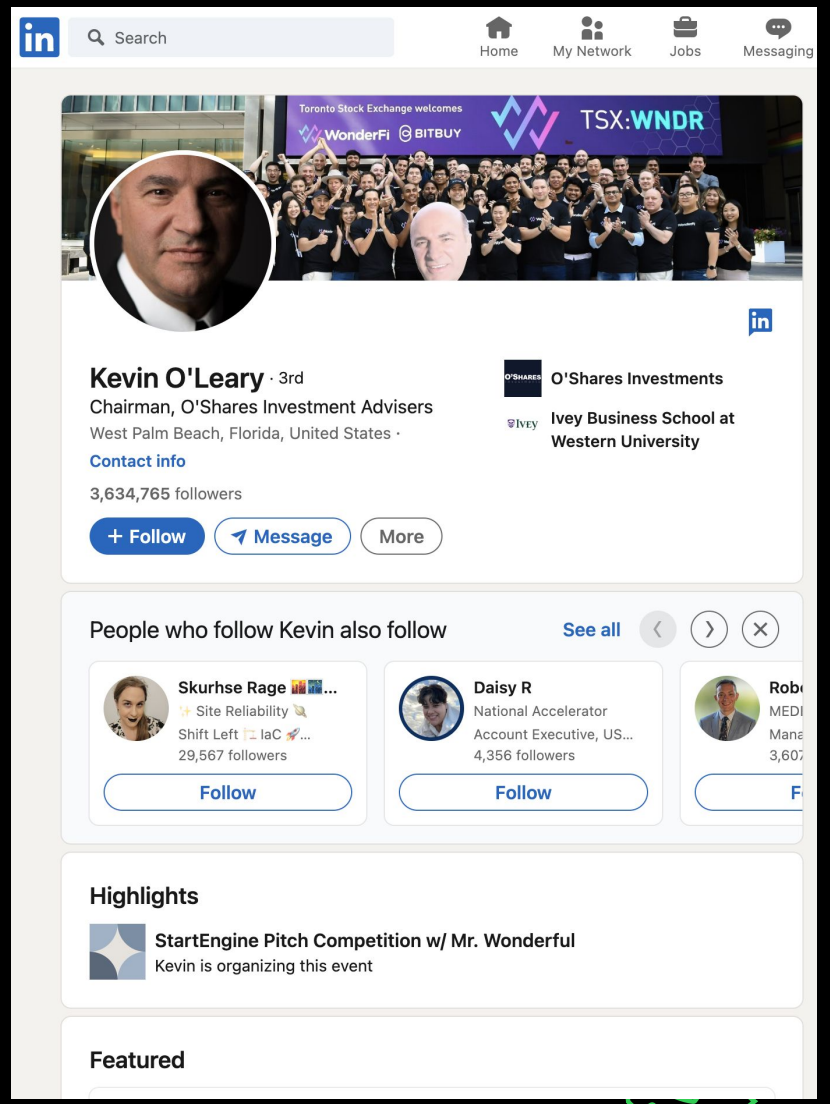


LinkedIn

- LinkedIn is a very open website
  - Most people tend not to lie or be very hidden

- Profile
  - Profile & Banner Pictures
  - Posts, Comments, Socials
  - Experience, Education, Skills, and Activity
  - Email, Phone Number, and Address

- Comments / Content
  - Easily accessible to all

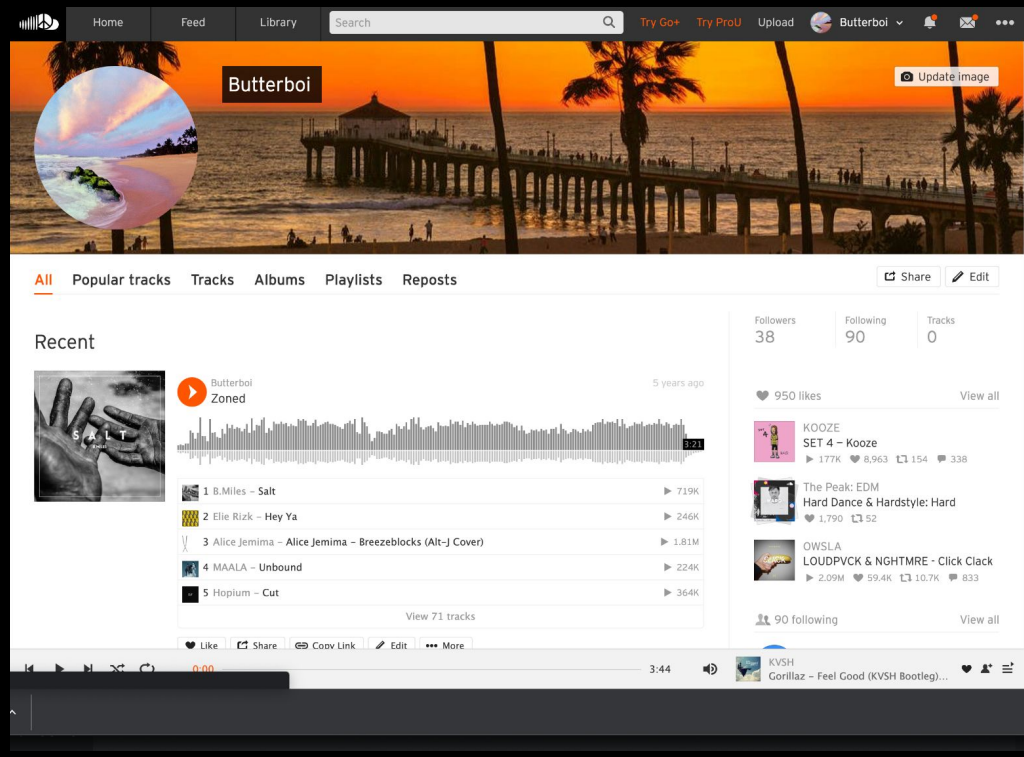


SoundCloud

- SoundCloud is a semi-anonymous website

- Often link to other socials; yet can be as anonymous as they want

- Profile
  - Posted media, Profile Picture, Socials
  - Likes, Comments, and Reposts
  - Followers/Following
  - Playlists



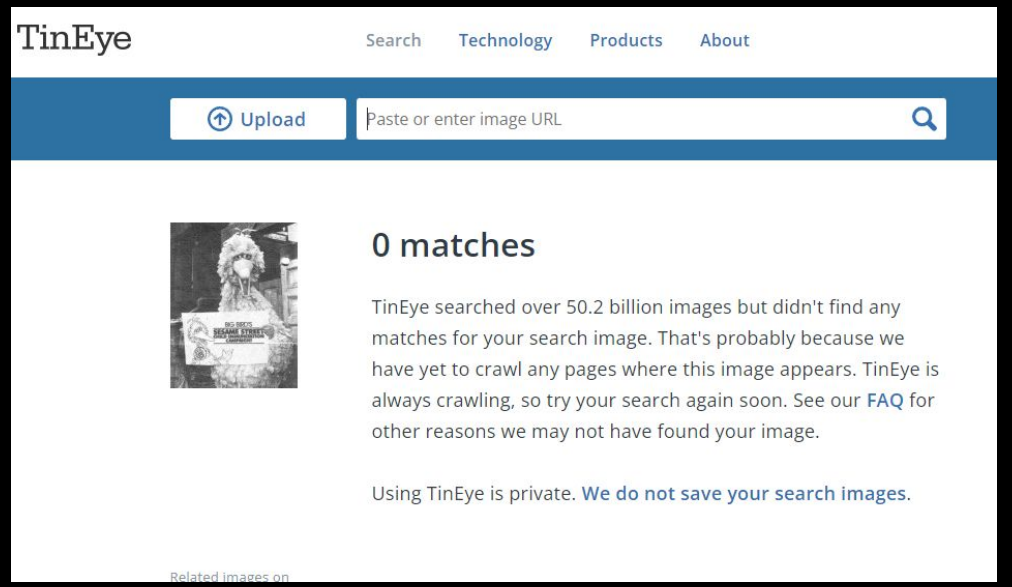
Media OSINT

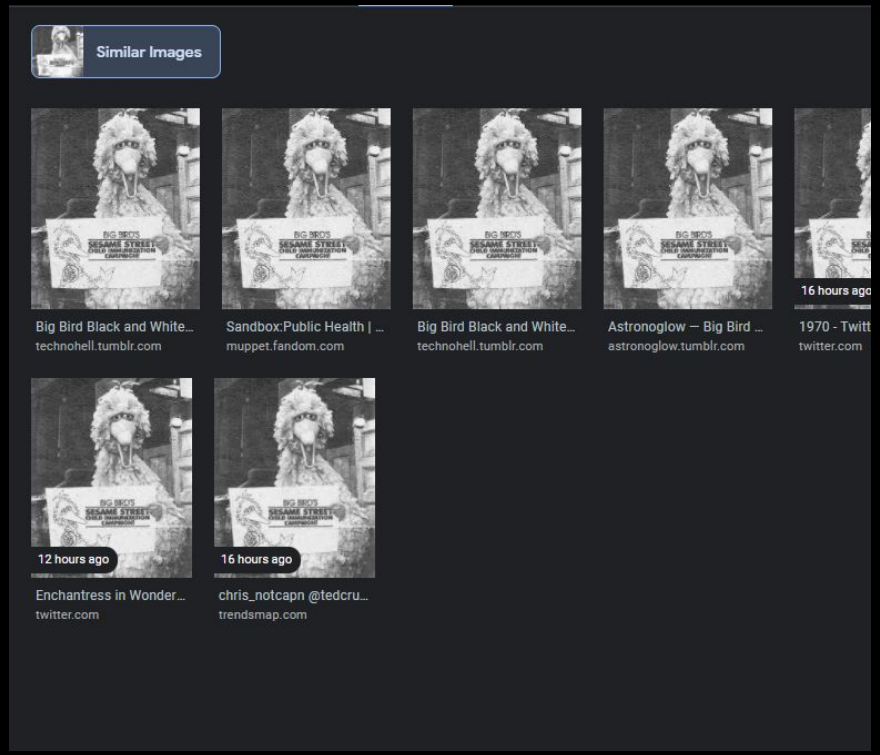
OPEN IMAGE IN NEW TAB!!!

Google Image Search (Tineye, Yandex)
- Keyword searcher
- Cropping

Tineye: exact matches
Google: Similar

GOOGLE LENS IS YOUR FRIEND





Go do challenges!

- Complete the **OSINT Waiver** first
- Start with **A Ratty Investigation** series
- See the vault for more chals!

Next Meetings

2024-09-29 • This Friday-Sunday

- Play BuckeyeCTF with us!
- Siebel CS, room TBD

2024-10-04 • Next Thursday

- Reverse Engineering I with Juniper
- Learn interpreter reverse engineering!

ctf.sigpwny.com

`sigpwny{g3tting_to_kn0w_you}`

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

SIGPwny