



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}

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.



OSINT

Open Source **IN**Telligence



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 from the 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

Explore this post and more from the aviation community



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



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

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

179.186.139.78.dynamic.a
dsl.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  RNTD  DELE  MDTM  RMD
XRMD  MKD...
```

86

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

BELTELECOM

Belarus, Minsk

starttls self-signed

2024-09-15T19:43:42.769207

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  ...
```



Grayhatwarfare

Buckets Shorteners Pricing FAQ Contact Us

GRAYHAT WARFARE

Home Filter Buckets Search Files Docs / API Top Keywords Buckets Stream

Search files

Keywords - Stopwords (start with minus -)

Filename Extensions (php, xlsx, docx, pdf)

Full Path Treat as regex

Additional filters

Search

Results for "-temporary -dev"

Save & notify See corresponding API Call

Showing 21 - 40 out of 20366 results

Premium users using this query see 9493 more results. [More info here.](#)

#	Bucket	Filename	Container	Size	Last Modified
21	fileplus.nyc3.digitaloceanspaces.com	20206713000113/pfx/BENEDITTOS_SALGADOS_senha_Geice091188.pfx		3.58kB	01-02-2023 14:14:00
22	fileplus.nyc3.digitaloceanspaces.com	20206713000113/pfx/BENEDITTOS_SALGADOS_senha_Geice091188.pfx		3.58kB	01-02-2023 14:14:24
23	fileplus.nyc3.digitaloceanspaces.com	20206713000113/pfx/BENEDITTOS_SALGADOS_senha_Geice091188.pfx		3.58kB	01-02-2023 14:14:50
24	fileplus.nyc3.digitaloceanspaces.com	20206713000113/pfx/Certificado_22_23_NOVO_benedittos.pfx		8.74kB	06-12-2022 22:33:32
25	fileplus.nyc3.digitaloceanspaces.com	23583049000110/pfx/GT_REPRESENTACOES_LTDA23583049000110.pfx		9.33kB	28-10-2022 01:47:56
26	fileplus.nyc3.digitaloceanspaces.com	23842967000116/pfx/2023_senha122015.pfx		9.19kB	06-10-2022 02:44:23



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

← Thomas Quig
2,848 Tweets

I don't think anyone cares what the words say as long as there is an artistic background. It could be a completely fabricated quote but nobody would notice, I would even bet on it.
-Robert Frost

Thomas Quig
@Thomas_Quig

CS Graduate Teachers Assistant and Computer Security researcher at UIUC | @SIGPwny Co-President. (he/him)

For Purely Infosec see @0xQuig

📍 a 🌐 quig.dev 📅 Joined November 2014

306 Following 153 Followers

Tweets Tweets & replies Media Likes

★ Pinned Tweet

Thomas Quig @Thomas_Quig · Jul 2, 2021
UM HELLO I JUST GOT INTO GRAD SCHOOL!?!?!? @IllinoisCS

The Grainger College of Engineering
Computer Science

Account Academic Admin Facilities Finance HR

GRADUATE STUDY ADMISSIONS AND FINANCIAL AID OFFERS

Congratulations, Thomas Quig!

The Department of Computer Science at the University of Illinois at Urbana-Champaign (UIUC) is pleased to invite you to join our Department for graduate study. We sincerely hope that you will accept our invitation to join Computer Science at Illinois.

4 1 40



YouTube

Channels

- Banner, Profile Picture
- **About tab, playlists**

Playlists

- Unlisted videos are **visible**

Videos

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

This screenshot shows the YouTube channel page for Thomas Quig, who has 5 subscribers. The navigation menu includes HOME, VIDEOS, PLAYLISTS, CHANNELS, and ABOUT. The 'ABOUT' tab is highlighted with a red box. Below the navigation, there is an 'Uploads' section with a 'PLAY ALL' button. A row of six video thumbnails is displayed, each with its title and view count. The first video, 'GFTT (Gunning For The Top) Demo', is highlighted with a red box. The channel page also features 'CUSTOMIZE CHANNEL' and 'MANAGE VIDEOS' buttons in the top right corner.

This screenshot shows the video player interface for the video 'GFTT (Gunning For The Top) Demo'. The video is at 0:12 / 2:16. The player includes standard controls like play/pause, volume, and a closed captions (CC) button, which is highlighted with a red box. Below the player, the video title and view count (62 views) are shown. The channel name 'Thomas Quig' and subscriber count (5 subscribers) are displayed, along with 'ANALYTICS' and 'EDIT VIDEO' buttons. The video description reads: 'Actual demo for a game Me + a few others made for a class, but now we are doing it for fun!'. Below the description, there is a 'Trailer coming soon!' section with a 'Rec Room' game card and a 'SHOW MORE' button. The video also has 1 comment, which is highlighted with a red box, and a 'SORT BY' dropdown menu.

GitHub

Profile page

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

Repositories

- Commit history
- Pull Requests & Comments

Comments / User Content

- Can exist in many places

The screenshot shows the GitHub profile page for Thomas Quig. The profile picture is a circular image with a lighthouse and the text "Please don't be normal". The profile name is "Thomas Quig" with the username "Thomas-Quig" below it. The bio reads "CS Student at UIUC '22. Interested in Security". There are 14 followers and 6 following. The user is affiliated with the University of Illinois Urbana Champaign. Social links for "thomasquig.dev" and "@Thomas_Quig" are shown. The profile has 40 repositories, 4 stars, and 2 pinned items. The pinned items are "llss", "naev", "ld3p", "naev-npm", "chal-dev.github.io", and "Thomas-Quig.github.io". A contribution graph shows 374 contributions in the last year, with a grid of green squares representing contributions across months and days. The grid shows activity from September to September, with contributions on Monday, Wednesday, and Friday. A "Beta" badge and "Send feedback" link are visible at the bottom left.



main 2 branches 1 tag

Go to file Add file Code

About

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

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

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

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**

The screenshot displays the profile page for the user 'Sonicninja'. At the top, navigation tabs include 'OVERVIEW', 'POSTS', 'COMMENTS', and 'AWARDS RECEIVED (LEGACY)'. Below these are sorting options: 'New', 'Hot', and 'Top'. The profile header shows the user's avatar, name 'Sonicninja', and the username 'u/Sonicninja · 9y'. A red button prompts to 'Create Your Own Avatar'. Statistics shown include 'Karma 11,986' and 'Cake day September 16, 2013'. A blue 'Follow' button and 'More Options' link are present. The 'Moderator of these communities' section lists 'r/sigpwny' with 3 members and a 'Join' button. The 'Trophy Case (7)' section features several awards: 'Nine-Year Club', 'Second SECOND GUESSER', and 'Gilding II' by 'euphauric'. A 'View More' link is at the bottom right of the trophies. The main content area shows four comments by Sonicninja on various posts, including one about parking spots and another about simulated practice (ctfs).

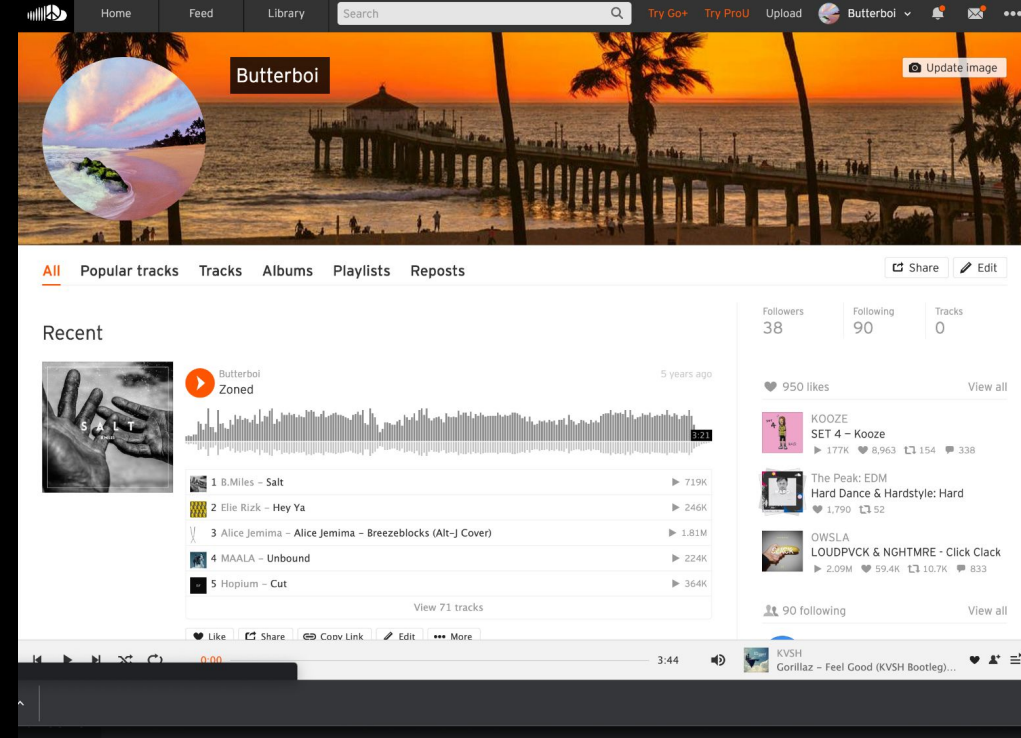
LinkedIn

- 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

The screenshot shows the LinkedIn profile of Kevin O'Leary. At the top, there is a search bar and navigation icons for Home, My Network, Jobs, and Messaging. The profile banner features a group photo of people at an event with logos for WonderFi, BITBUY, and TSX:WDR. Kevin O'Leary's profile picture is a circular portrait of him. Below the picture, his name 'Kevin O'Leary · 3rd' is displayed, followed by his title 'Chairman, O'Shares Investment Advisers' and location 'West Palm Beach, Florida, United States'. To the right, his affiliations with 'O'Shares Investments' and 'Ivey Business School at Western University' are listed. The profile shows '3,634,765 followers' and three action buttons: '+ Follow', 'Message', and 'More'. Below this, a section titled 'People who follow Kevin also follow' includes profile cards for Skurhse Rage (29,567 followers), Daisy R (4,356 followers), and Rob (3,607 followers). A 'Highlights' section shows an event 'StartEngine Pitch Competition w/ Mr. Wonderful' that Kevin is organizing. The bottom of the page has a 'Featured' section.

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!!!

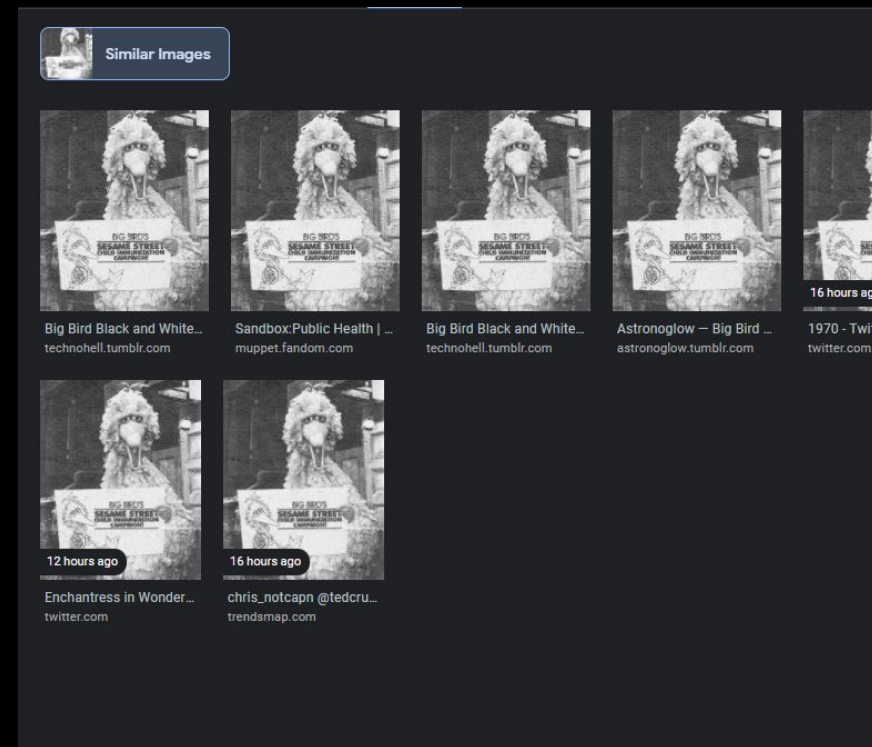
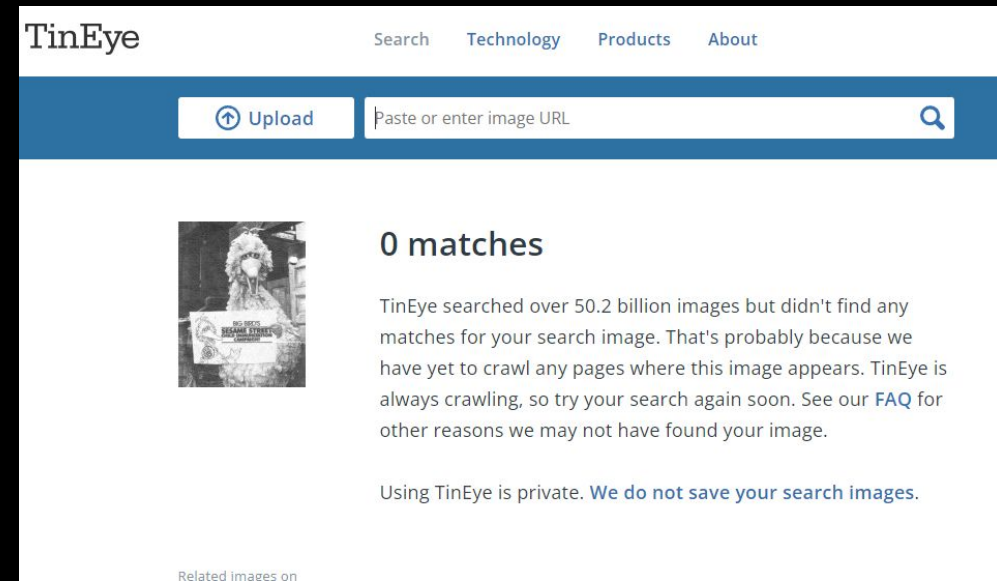
Google Image Search (Tineye, Yandex)

- 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.

