

FA2022 Week 05

OSINT I

Thomas Quig, Julius White, Danny Poje



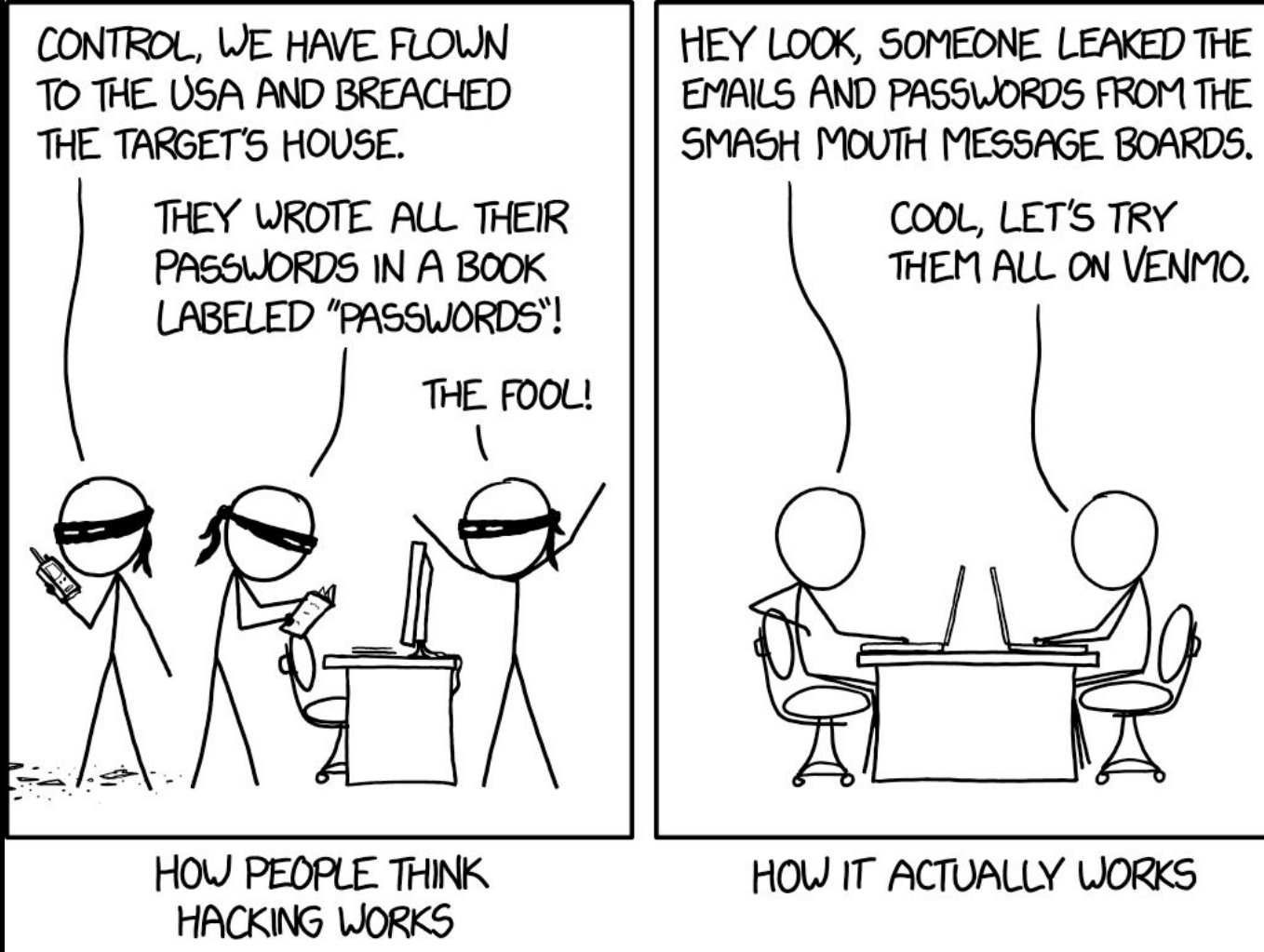
Announcements

- Fall CTF went great
 - Approx. 300 Attendees!
- Social Event this weekend (Saturday)
 - Vote on what it will be by Friday @ 7PM
- Back to 1404???
 - We don't know when... earliest Oct 7.



ctf.sigpwny.com

sigpwny{praise_tobac}



OSINT

Open Source **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.
- Pseudonyms
 - Recon, Cyberreconnisance, HUMINT etc.
 - Generally considered "easy" in security (not true)



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!**



Why is this important?

CYBERSECURITY

Google and Facebook got tricked out of \$123 million by a scam that costs small businesses billions every year — here's how to avoid it

PUBLISHED THU, MAR 28 2019-1:13 PM EDT

 **Kate Fazzini**
@KATEFAZZINI

SHARE [f](#) [t](#) [in](#) [✉](#)

KEY POINTS

- Google and Facebook paid out \$23 million and \$100 million respectively to a cybercriminal from Lithuania, who pleaded guilty to wire fraud in New York this week.
- The companies were scammed out of the payments by a technique known as business email compromise or invoice fraud.
- Unlike most companies and individuals who are victimized by this type of crime, the tech giants were able to recover the funds. Most aren't so lucky, and many companies take a massive hit or are forced out of business by this type of crime.

TV

Mad Money [WATCH LIVE](#)

UP NEXT | **Shepard Smith** 07:00 pm ET [Listen](#)

ADVERTISEMENT

CNBC BRAND STUDIO with Salesforce

Enlightened was founded to help people lead healthier lives without compromising on tasty treats. This is how better data is helping to rapidly grow their business and launch a new



Types of Intelligence

- Systems Intelligence
- Network Intelligence
- Organizational Intelligence
- Human Intelligence



Systems Intelligence

What is it made of?



Systems Intelligence - Summary

Get information about a system you are attacking.

Trick the system into giving you that information voluntarily

Methods

- Port scanning
- Information probes
- IRL Intelligence



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 - Implications

- 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, 445, 3389, 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**



Network Intelligence

Where is it and who is it talking to?



Network Intelligence - Summary

Like system intelligence, but focused more on communications.

Given a network of systems, who talks to who and why.

What is the dataflow to, from, and within a network

A lot of what you do here is going to be on Windows, **so this section will be more geared towards that.**



Organizational Intel

What are they doing!?!?



Organizational Intel - OpSec

- How is an organization's OpSec?
 - What is the **email format** (firstname.lastname)
 - Preferred _____ (airline, hotel etc.)
 - What are their IT/security protocols?
 - Do org members have strong opsec
 - attacking a company = attacking people
 - Internal document leakage



Rachel Tobac, Opsec/SocEng badass



Human Intelligence

Who is this person?



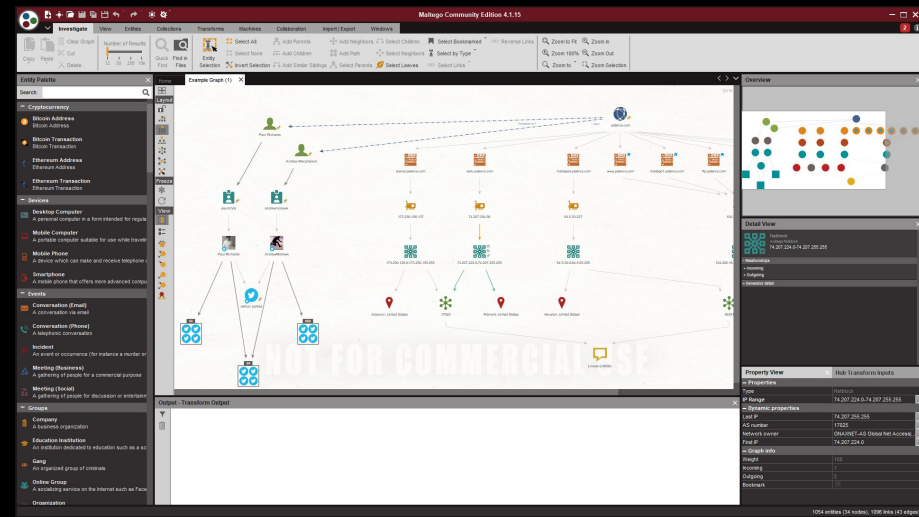
Human Intelligence

- This is easiest thing to learn
- Creating a map of a person
 - Everything from social media to IRL address
- Tons of different methods, too many to put on a summary page



Human Information Gathering Methods

- Profiles
 - Links, pictures, stuff that goes to other stuff
 - Build a map of someone
- Username Reuse
 - Same across lots of places!
 - Helpful for these chals!
- Images
 - Reverse _____ searching!
- Deleted Content
 - Archivists save old websites!
 - Wayback machine!



General OSINT Methods

Mostly applies to everything



OSINT Tips - Identities

Split Identities

- Most people have **two** identities online
 - Professional
 - Casual
- Your job when doing OSINT is to link them

Sherlock

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



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)

A screenshot of a YouTube channel page for 'Thomas Quig' (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 is 'GFTT (Gunning For The Top) Demo' with 62 views. The 'ABOUT' tab and the first video thumbnail are highlighted with red boxes.

A screenshot of a YouTube video player for the video 'GFTT (Gunning For The Top) Demo'. The video player shows a progress bar at 0:12 / 2:16. Below the player, the video title and view count (62 views) are displayed. The channel name 'Thomas Quig' (5 subscribers) is shown, 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 'SHOW MORE' button is highlighted with a red box. At the bottom, there is a '1 Comment' button and a 'SORT BY' dropdown menu. The '1 Comment' button is highlighted with a red box.

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 a 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 handle "Thomas-Quig". The bio is "CS Student at UIUC '22. Interested in Security". The page shows 14 followers and 6 following. The location is "University of Illinois Urbana Champaign". The website is "thomasquig.dev" and the Twitter handle is "@Thomas_Quig". The profile has 40 repositories and 4 stars. The pinned repositories are: "llss" (Public, 2 stars), "naev" (Public, Python), "ld3p" (Public, Python, 2 stars), "naev-npm" (Public, JavaScript), "chal-dev.github.io" (Public, Dockerfile, 1 star), and "Thomas-Quig.github.io" (Public, CSS). The contribution graph shows 374 contributions in the last year, with a grid of green squares representing contributions from Monday to Friday across the months of September, October, November, December, January, February, March, April, May, June, July, August, and September. The grid shows a consistent pattern of contributions throughout the year.



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

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

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 shows the profile page for the user 'Sonicninja' (u/Sonicninja · 9y). The profile includes a custom avatar of a character with glasses and a red body, a banner image of a person rappelling, and a bio that reads: 'Stop trying to find hidden secrets in my reddit profile, good try though <3'. The user's karma is 11,986 and their 'cake day' is September 16, 2013. The profile is a moderator for the communities r/sigpwny (3 members) and r/glaivebossman. The 'Trophy Case' shows awards such as 'Nine-Year Club', 'Second SECOND GUESSER', and 'Gilding II'. The main content area displays four comments by Sonicninja on various posts, including one about a parking spot, one with a repetitive phrase 'GET OUT OF MY HEAD', one about OSINT resources, and one about a ticket for a show in London. Navigation tabs at the top include Overview, Posts, Comments, and Awards Received (Legacy). A 'Back to Top' button is located at the bottom right.

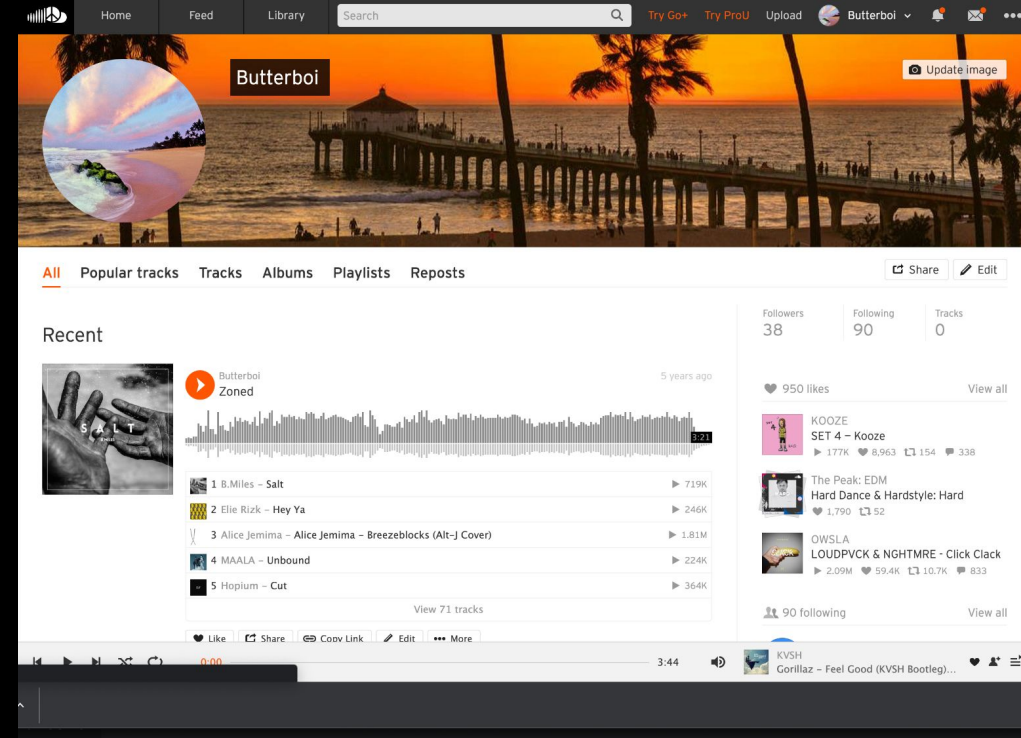
LinkedIn

- 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 image shows a screenshot of a LinkedIn profile for Kevin O'Leary. At the top, there is a navigation bar with the LinkedIn logo, a search bar, and icons for Home, My Network, Jobs, and Messaging. The profile header features a circular profile picture of Kevin O'Leary and a banner image of a group of people at a Toronto Stock Exchange event, with logos for WonderFi, BITBUY, and TSX:WDR. Below the profile picture, the name 'Kevin O'Leary' is displayed with '3rd' next to it. His title is 'Chairman, O'Shares Investment Advisers' and his location is 'West Palm Beach, Florida, United States'. To the right, there are logos for O'Shares Investments and Ivey Business School at Western University. The profile shows '3,634,765 followers' and three buttons: '+ Follow', 'Message', and 'More'. Below this is a section titled 'People who follow Kevin also follow' with a 'See all' link and navigation arrows. It lists three other users: Skurhse Rage (Site Reliability, 29,567 followers), Daisy R (National Accelerator, 4,356 followers), and Rob (MEDI, 3,607 followers). Each user has a 'Follow' button. At the bottom, there is a 'Highlights' section with a card for 'StartEngine Pitch Competition w/ Mr. Wonderful' where Kevin is organizing the event. A 'Featured' section is partially visible at the very bottom.

SoundCloud

- SoundCloud is a **semi-anonymous** website
- Often link to other socials; yet **can be as anonymous as they want**
- Creators / Publishers are **more vulnerable**
- Profile
 - **Posted media, Profile Picture, Socials**
 - Likes, Comments, and Reposts
 - Followers/Following
 - Playlists



Media OSINT

OPEN IMAGE IN NEW TAB!!!

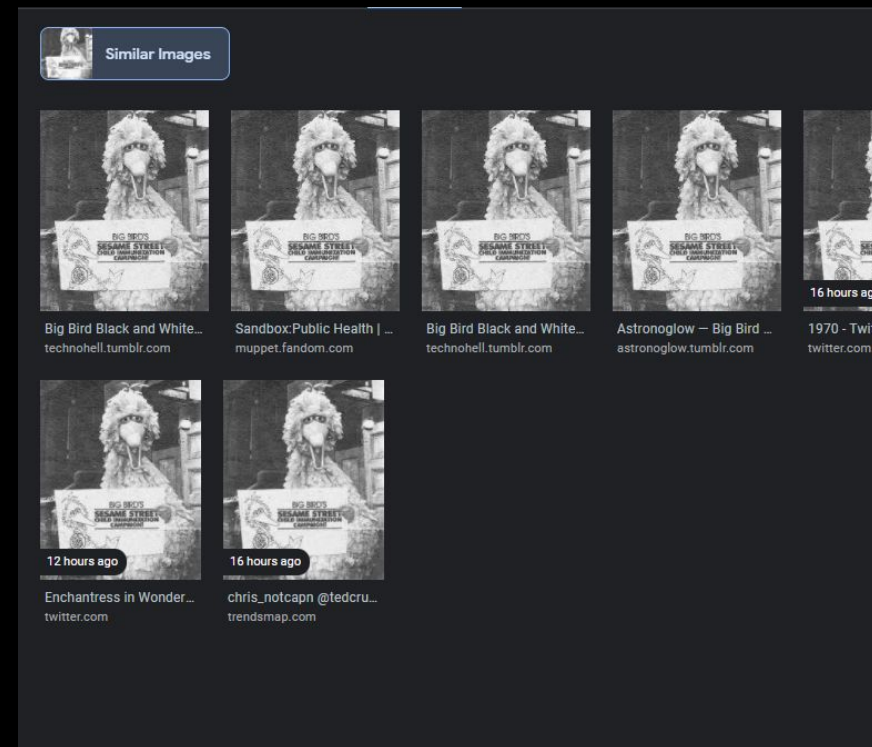
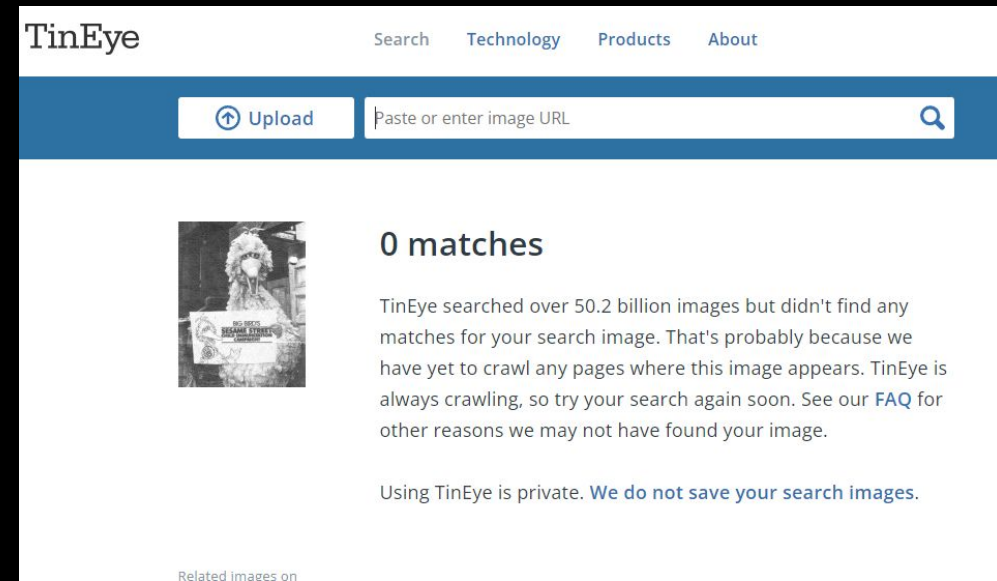
Tineye, Yandex, Google Image Search

- Keyword searcher
- Cropping

Tineye: exact matches

Google: Similar

GOOGLE LENS IS YOUR FRIEND



Challenge Collection

UIUCTF 2020 - HackerIsabelle (6 challenges)

UIUCTF 2021 - ChaplinCoding (8 challenges)

UIUCTF 2022 - Chucklephucke (6 challenges)

SP 2019 - TotallyAHuman3025 (11 challenges)

Fall CTF 2021 - SpaghettiEsports (3 challenges)

CCC 2021 - con_angry (3 challenges)

Fall CTF 2022 - Spoingusthecat (4 challenges)

FA 2022 - Check ctf.sigpwny.com (8 challenges)

Those are the usernames for the first challenge of each suite, go figure out which platforms they belong to!!! **Let us know if you are stuck / something seems down or broken**



Next Meetings

2022-10-02 - Assembly (Seminar)

- Learn how assembly works!!!

2022-10-06 - PWN/Binary Exploitation I (Regular Meeting)

- Attack binaries!!! Buffer overflow!!





SIGPwny