SIGPwny

FA2023 Week 05 • 2023-09-28

OSINT I

Pomona Carrington Hoekstra

Announcements

- Thank you for a great Fall CTF!

- This weekend: BuckeyeCTF x MapleCTF
  - Friday 7 PM - Sunday 7 PM, Siebel CS (room TBA)
  - Free pizza provided!

- Intro to x86-64 assembly
  - Sunday 2 PM - 3 PM, Siebel 1404
  - Learn about x86-64 assembly, the lowest level of programming before machine code!

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 **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.

- Pseudonyms
  - Recon, Cyberreconnaissance, 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

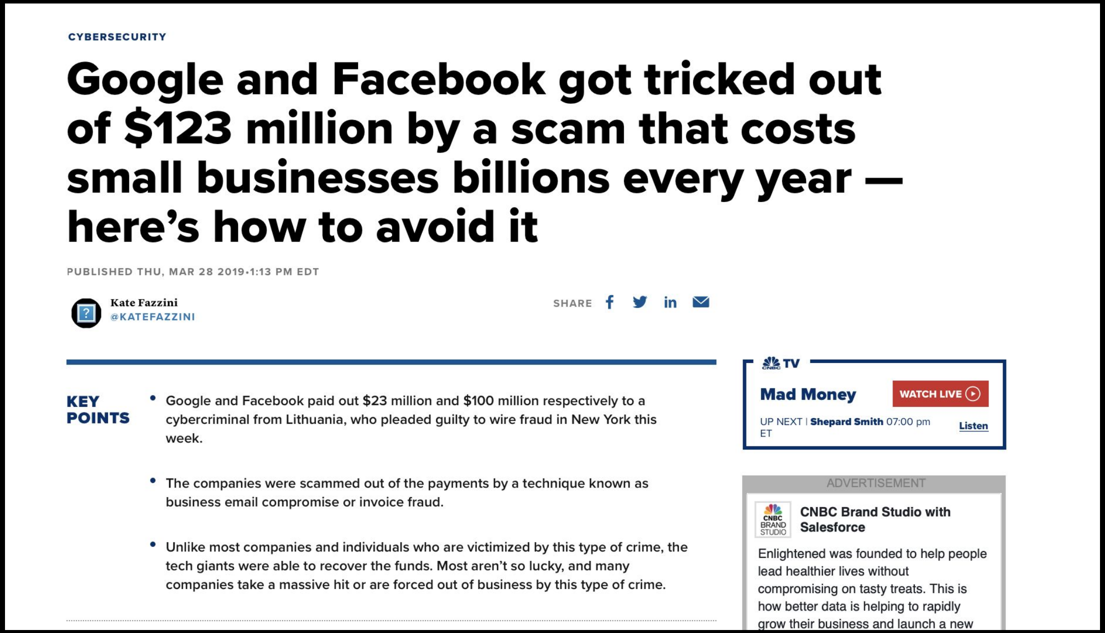
You could find something you don’t like / aren't supposed to

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

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.

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 (nmap)
- Information probes
- IRL Intelligence
- Port-search sites (Shodan and Zoomeye)

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?

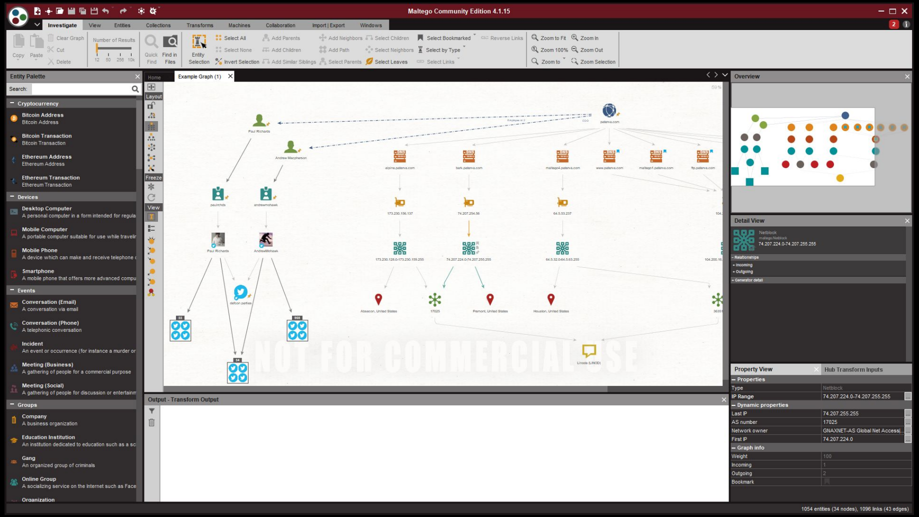
Human Intelligence

- 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

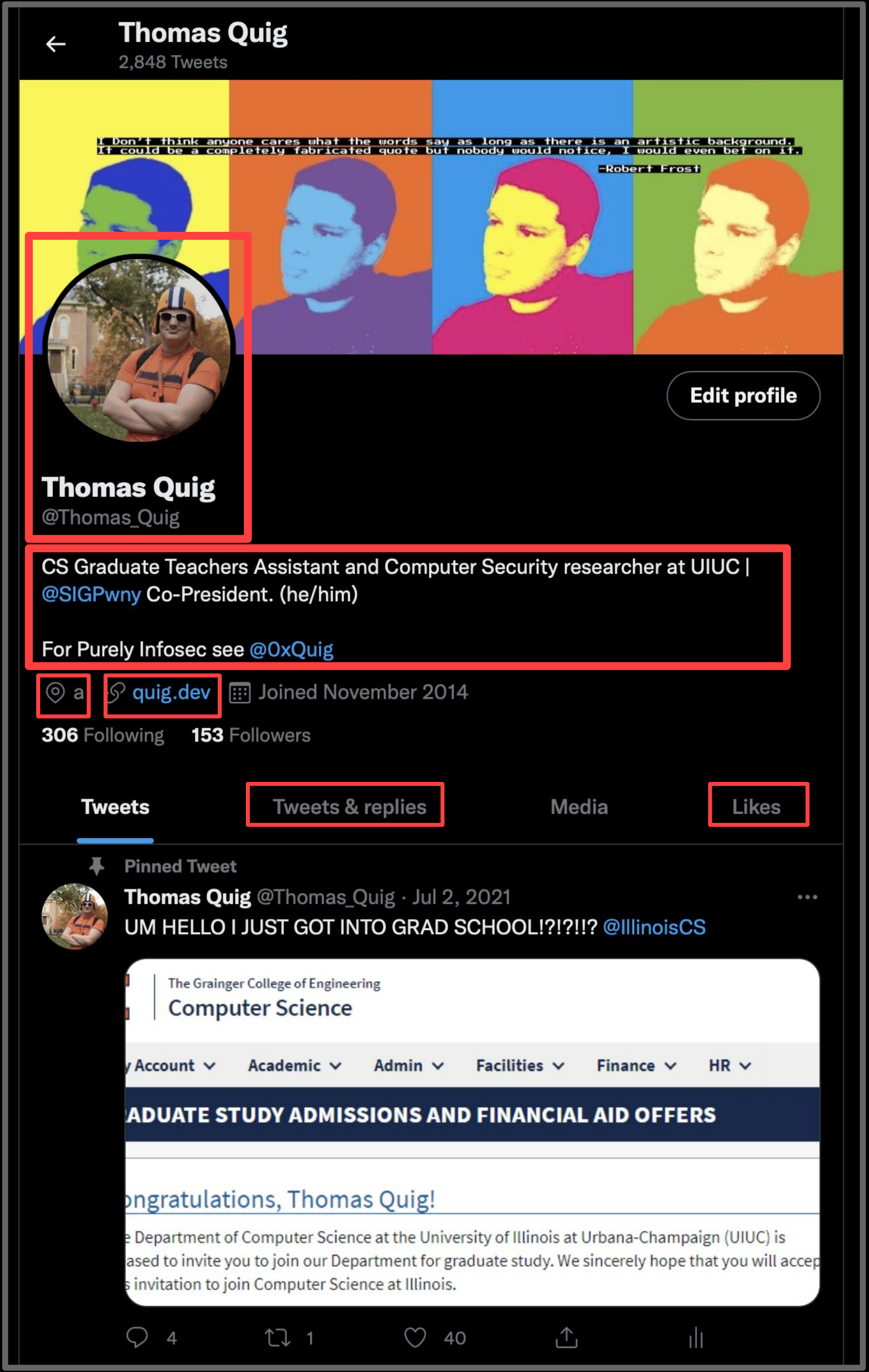
- Most people have **two** identities online
  - Professional
  - Casual
- Your job when doing OSINT is to link them

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**



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
2,848 Tweets

Edit profile

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

ADUATE STUDY ADMISSIONS AND FINANCIAL AID OFFERS

ongratulations, Thomas Quig!

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

4 1 40

YouTube

Channels

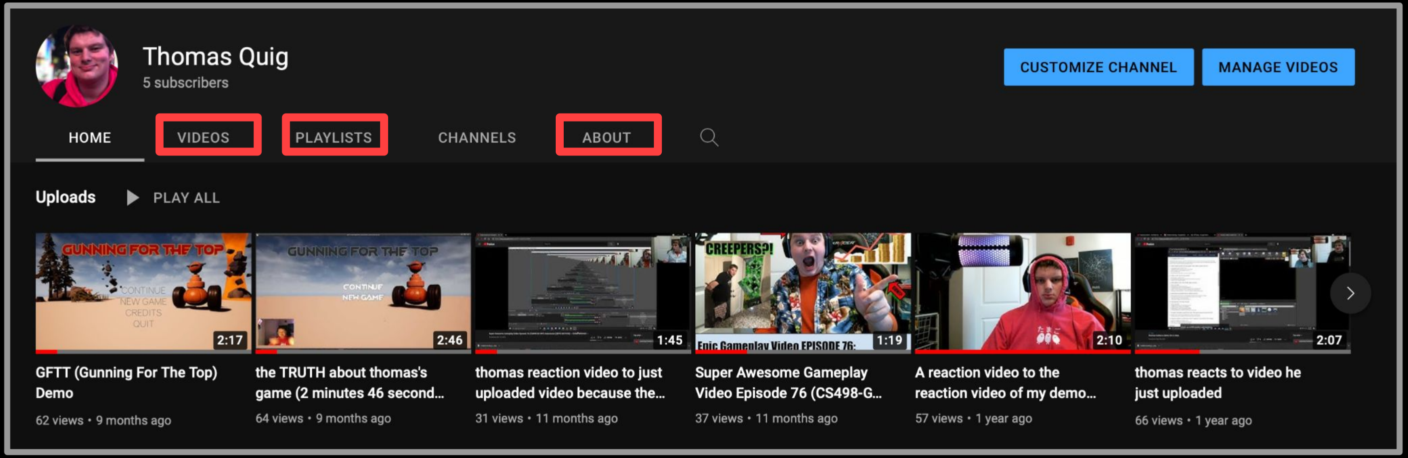
- Banner, Profile Picture
- About tab, playlists

Playlists

- Unlisted videos are visible

Videos

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



Thomas Quig
5 subscribers

GFTT (Gunning For The Top) Demo
62 views • 9 months ago

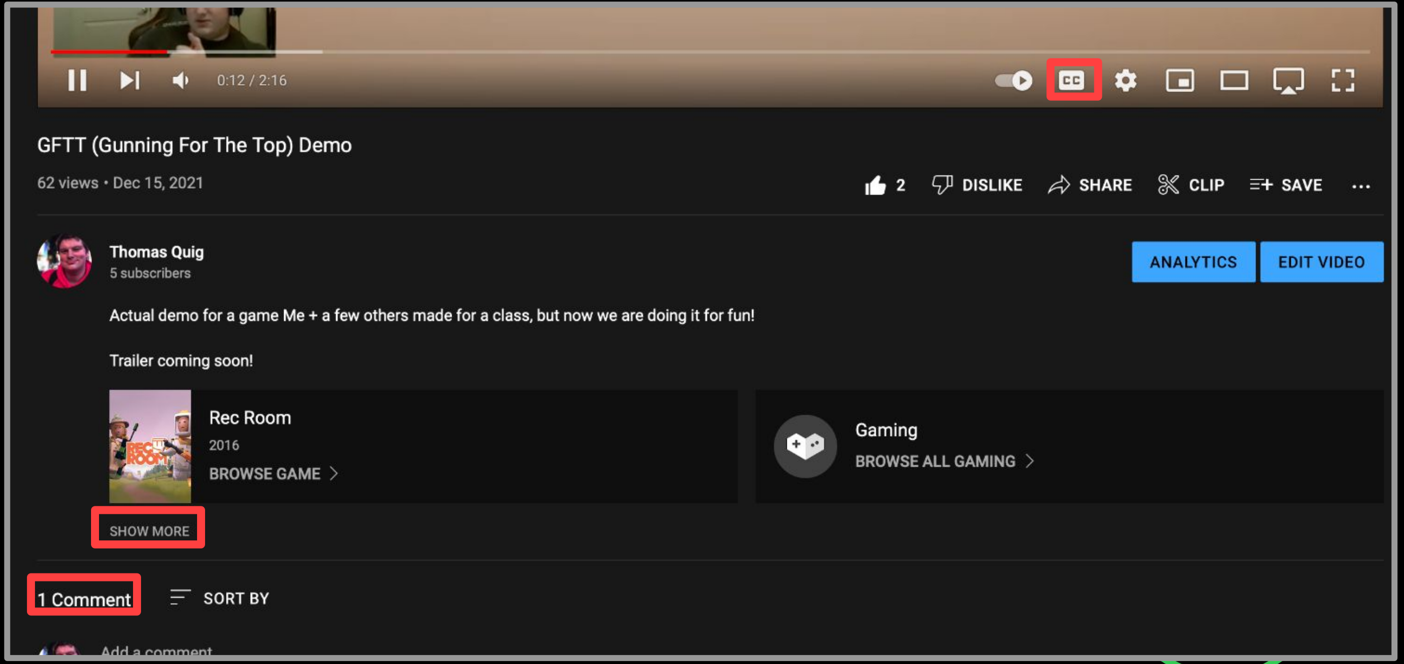
the TRUTH about thomas's game (2 minutes 46 second...
64 views • 9 months ago

thomas reaction video to just uploaded video because the...
31 views • 11 months ago

Super Awesome Gameplay Video Episode 76 (CS498-G...
37 views • 11 months ago

A reaction video to the reaction video of my demo...
57 views • 1 year ago

thomas reacts to video he just uploaded
66 views • 1 year ago



GFTT (Gunning For The Top) Demo
62 views • Dec 15, 2021

Thomas Quig
5 subscribers

Actual demo for a game Me + a few others made for a class, but now we are doing it for fun!

Trailer coming soon!

Rec Room
2016
BROWSE GAME >

Gaming
BROWSE ALL GAMING >

GitHub

Profile page

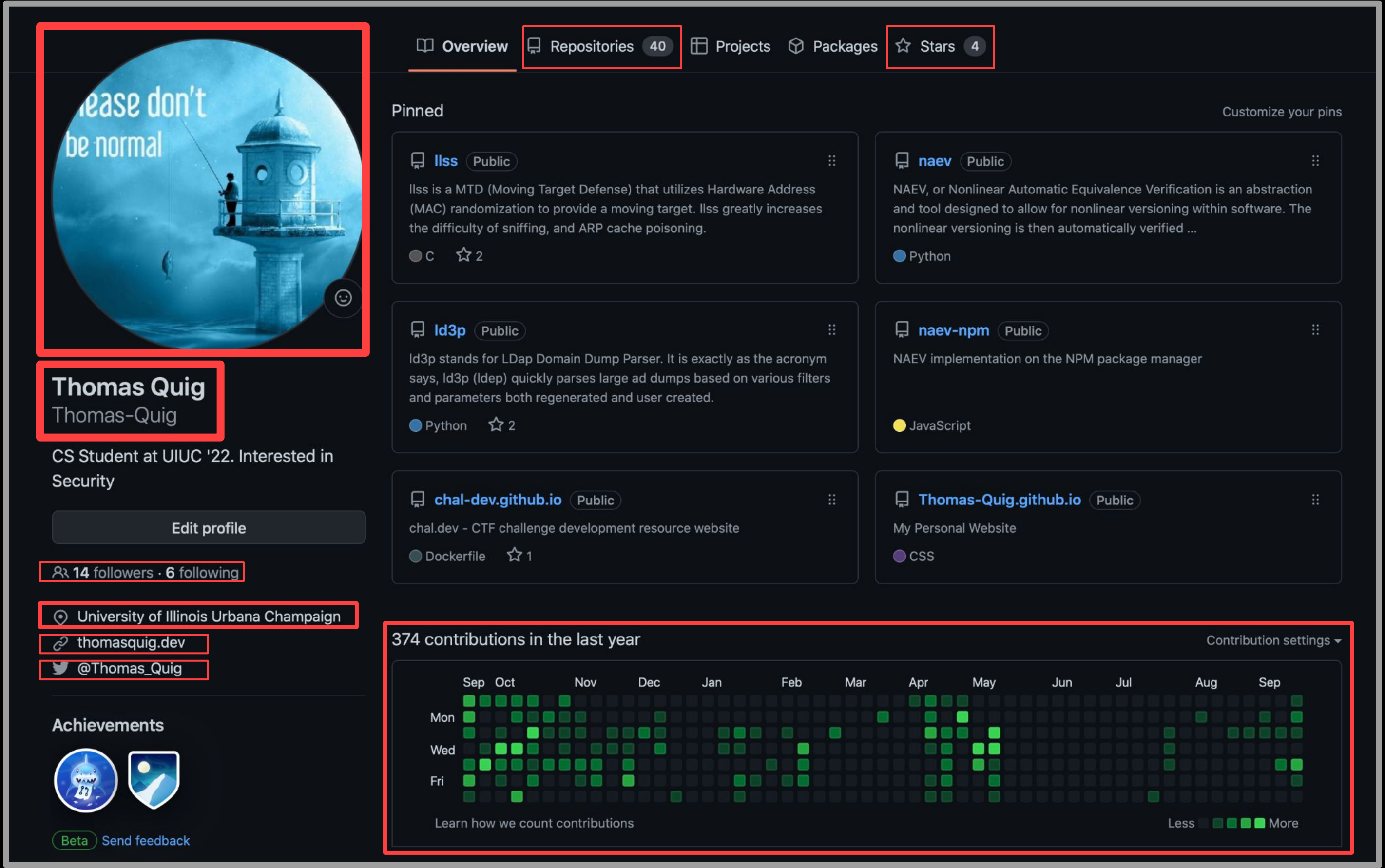
- View featured repos
- Links, socials, location
- email

Repositories

- Commit history
- Pull Requests & Comments

Comments / User Content

- Can exist in many places



Overview Repositories 40 Projects Packages Stars 4

Thomas Quig
Thomas-Quig

CS Student at UIUC '22. Interested in Security

Edit profile

14 followers · 6 following

University of Illinois Urbana Champaign
thomasquig.dev
@Thomas_Quig

Achievements

Beta Send feedback

Pinned

Customize your pins

llss Public
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.
C ☆ 2

naev Public
NAEV, or Nonlinear Automatic Equivalence Verification is an abstraction and tool designed to allow for nonlinear versioning within software. The nonlinear versioning is then automatically verified ...
Python

ld3p Public
ld3p stands for LDap Domain Dump Parser. It is exactly as the acronym says, ld3p (ldep) quickly parses large ad dumps based on various filters and parameters both regenerated and user created.
Python ☆ 2

naev-npm Public
NAEV implementation on the NPM package manager
JavaScript

chal-dev.github.io Public
chal.dev - CTF challenge development resource website
Dockerfile ☆ 1

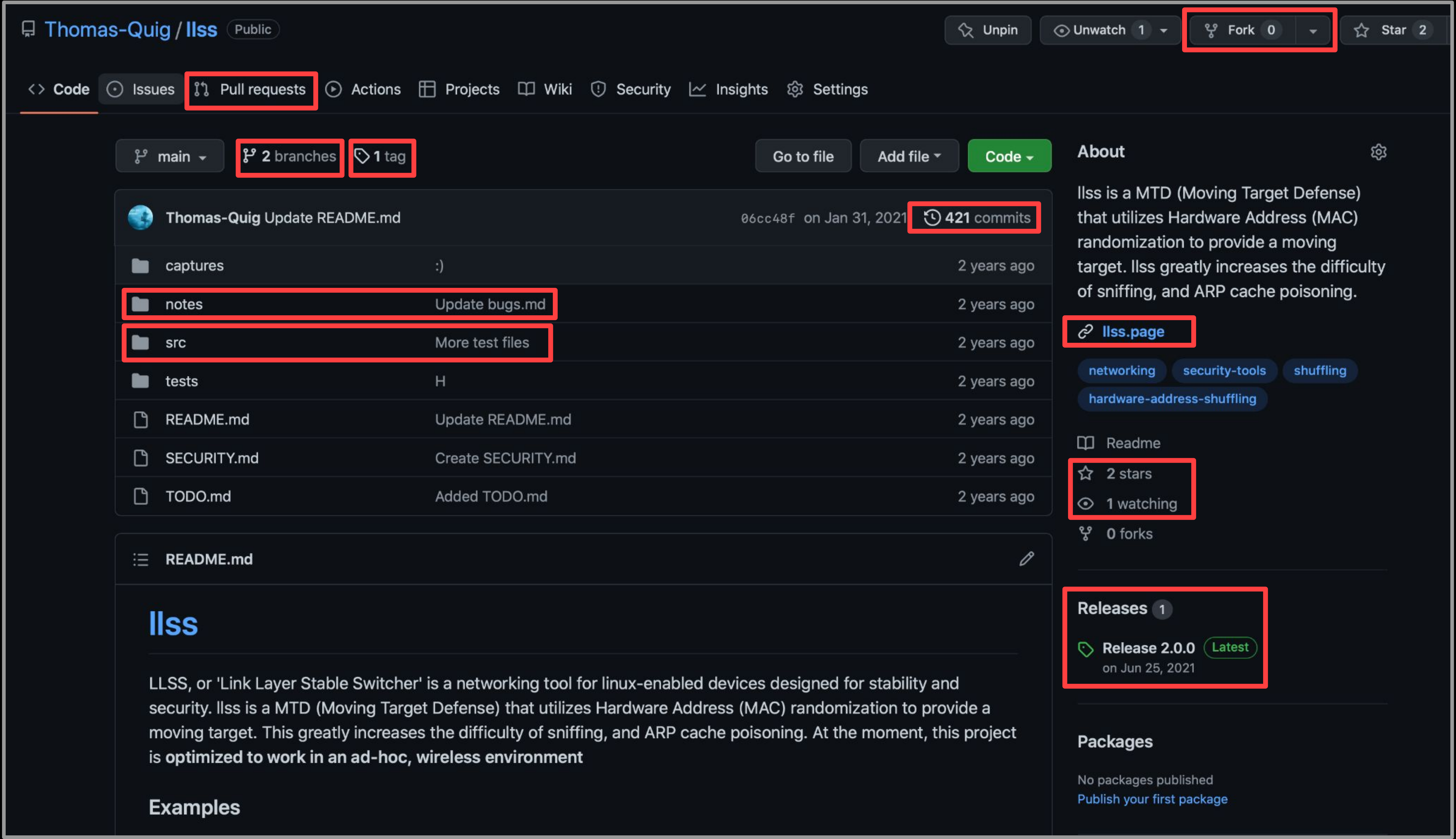
Thomas-Quig.github.io Public
My Personal Website
CSS

374 contributions in the last year

Contribution settings

Learn how we count contributions

Less More



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.

README.md

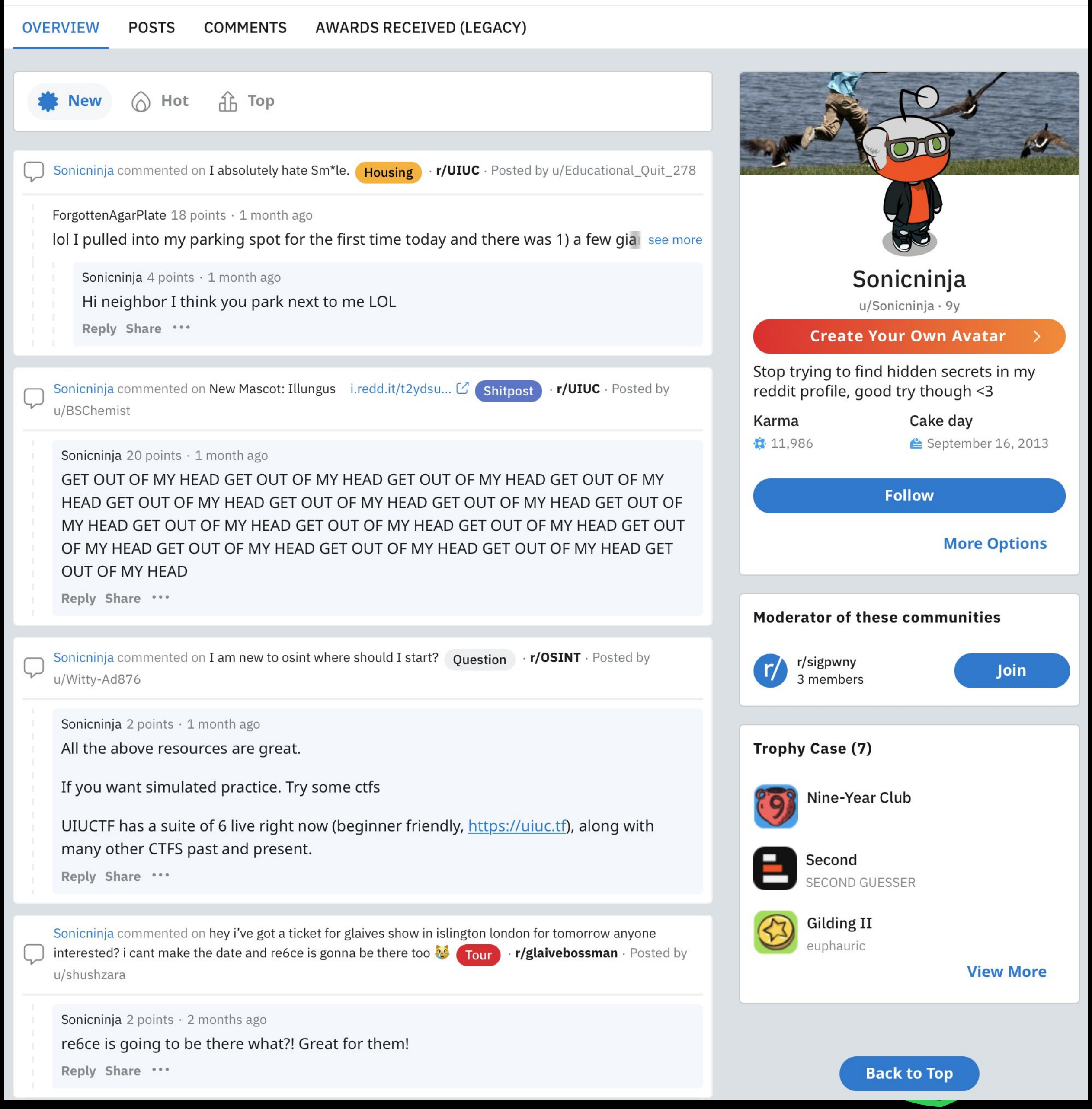
llss

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



OVERVIEW POSTS COMMENTS AWARDS RECEIVED (LEGACY)

New Hot Top

Sonicninja commented on I absolutely hate Sm*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 gia 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/BSChemist

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

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/sigpwny
3 members

Join

Trophy Case (7)

Nine-Year Club

Second
SECOND GUESSER

Gilding II
euphauric

View More

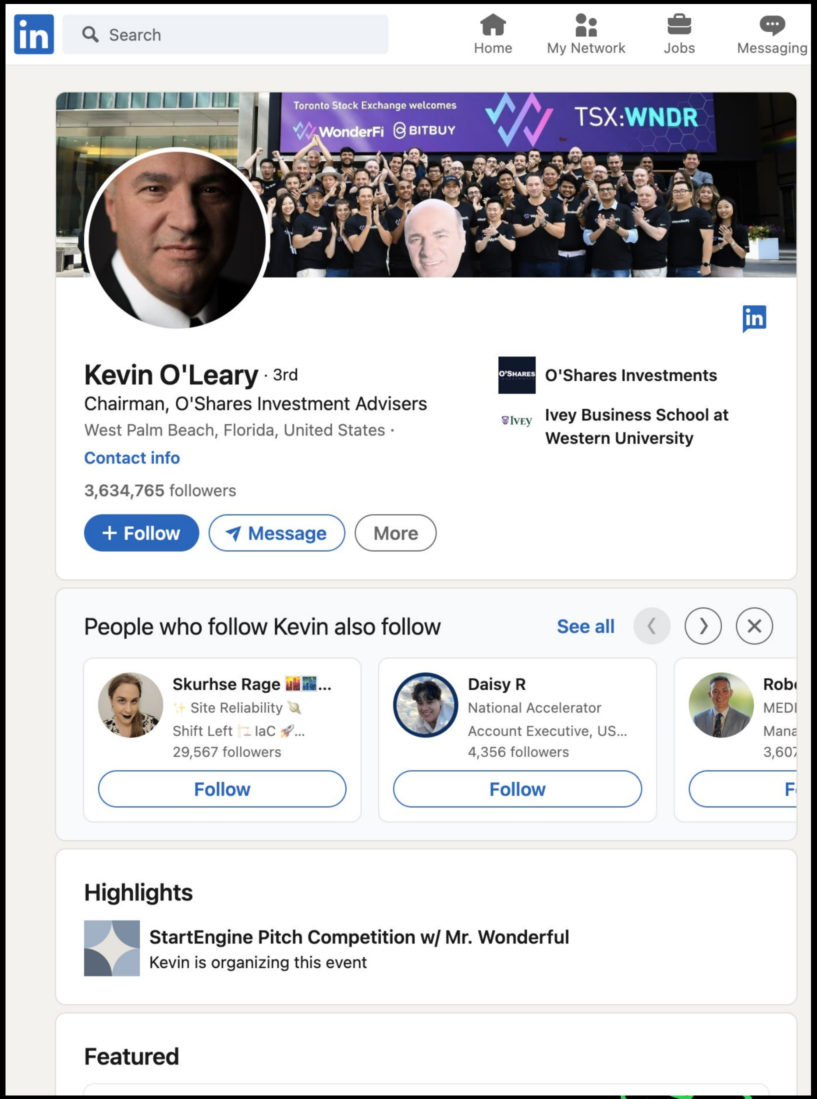
Back to Top

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



Kevin O'Leary · 3rd
Chairman, O'Shares Investment Advisers
West Palm Beach, Florida, United States ·
Contact info
3,634,765 followers

O'Shares Investments
Ivey Business School at Western University

+ Follow | Message | More

People who follow Kevin also follow — See all

Skurhse Rage 🌇🌃...
✨ Site Reliability 🪐
Shift Left 🏗 IaC 🚀...
29,567 followers
Follow

Daisy R
National Accelerator
Account Executive, US...
4,356 followers
Follow

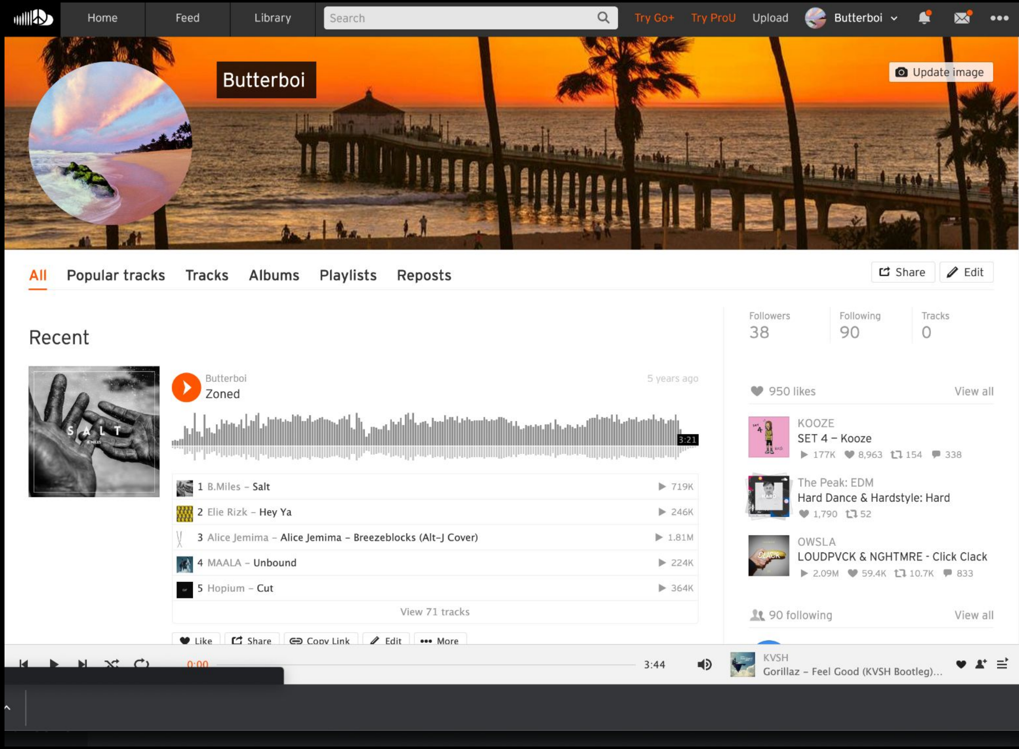
Rob
MEDI
Mana
3,607
F

Highlights
StartEngine Pitch Competition w/ Mr. Wonderful
Kevin is organizing this event

Featured

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



Butterboi

Recent

Followers 38 · Following 90 · Tracks 0

Butterboi
Zoned
5 years ago
3:21

1	B.Miles – Salt	▶ 719K
2	Elie Rizk – Hey Ya	▶ 246K
3	Alice Jemima – Alice Jemima – Breezeblocks (Alt-J Cover)	▶ 1.81M
4	MAALA – Unbound	▶ 224K
5	Hopium – Cut	▶ 364K

View 71 tracks

950 likes

KOOZE
SET 4 – Kooze
▶ 177K ♥ 8,963 154 338

The Peak: EDM
Hard Dance & Hardstyle: Hard
♥ 1,790 52

OWSLA
LOUDPVCK & NGHTMRE - Click Clack
▶ 2.09M ♥ 59.4K 10.7K 833

90 following

0:00 3:44

KVSH
Gorillaz – Feel Good (KVSH Bootleg)...

Media OSINT

OPEN IMAGE IN NEW TAB!!!

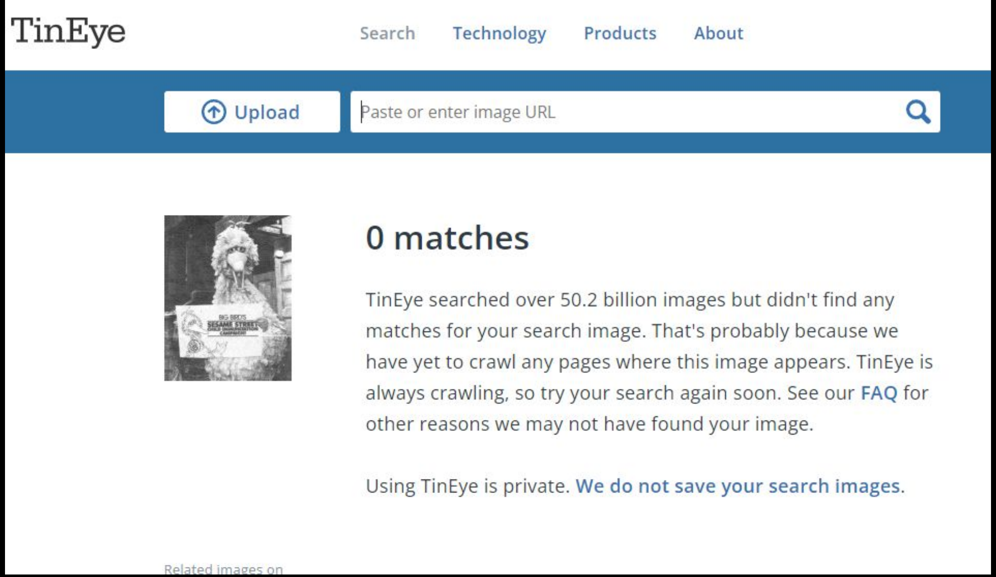
Tineye, Yandex, Google Image Search

- Keyword searcher
- Cropping

Tineye: exact matches

Google: Similar

GOOGLE LENS IS YOUR FRIEND

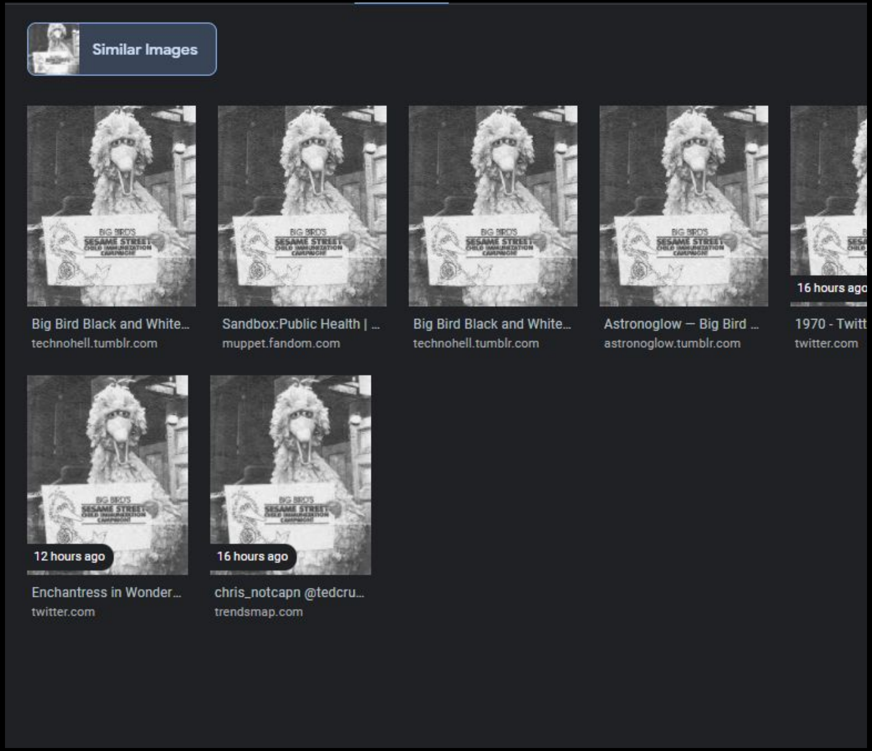


0 matches

TinEye searched over 50.2 billion images but didn't find any matches for your search image. That's probably because we have yet to crawl any pages where this image appears. TinEye is always crawling, so try your search again soon. See our FAQ for other reasons we may not have found your image.

Using TinEye is private. We do not save your search images.

Related images on



Big Bird Black and White… technohell.tumblr.com

Sandbox:Public Health | … muppet.fandom.com

Big Bird Black and White… technohell.tumblr.com

Astronoglow — Big Bird … astronoglow.tumblr.com

16 hours ago
1970 - Twitt twitter.com

12 hours ago
Enchantress in Wonder… twitter.com

16 hours ago
chris_notcapn @tedcru… trendsmap.com

Challenge Collection

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)
Fall CTF 2023 - pinto.bean.the.squirrel (4 challenges)
FA 2023 - Check **ctf.sigpwny.com**

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**

Go do challenges!

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

Next Meetings

`2023-09-29` • **This Friday**

- Playing BuckeyeCTF and MapleCTF
- Location: Siebel CS room TBA (check Discord), free pizza!

`2023-10-01` • **This Sunday**

- x86-64 Assembly
- Learn about low-level computer programming with Sam

ctf.sigpwny.com

sigpwny{g3tting_to_kn0w_you}

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

SIGPwny