Week 10
OSINT II

Slides By: Thomas Quig

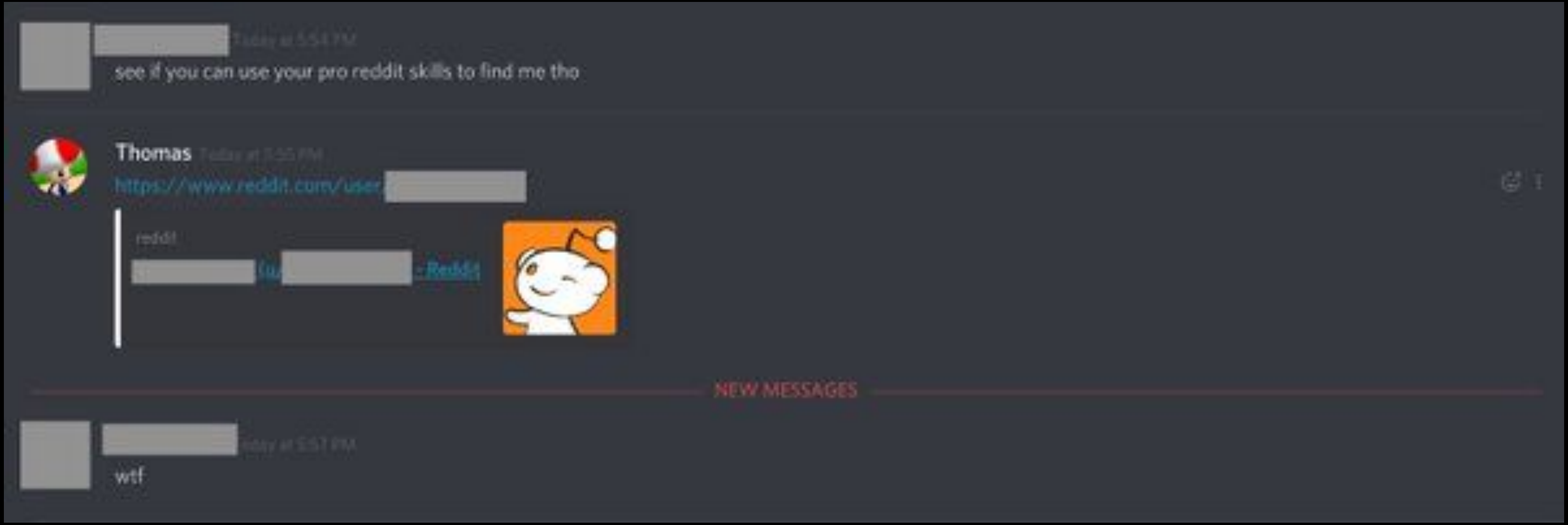
Announcements

OSU Shirts, I have them, come get them thursday (or today lol)

Merch form again: sigpwny.com/merch

Spray paint social @ some point

sigpwny{reddit_pro_skills_lol}



[redacted] [redacted] Today at 5:54 PM
see if you can use your pro reddit skills to find me tho

Thomas Today at 5:55 PM
https://www.reddit.com/user/[redacted]

reddit
[redacted] (u/[redacted] - Reddit

NEW MESSAGES

[redacted] [redacted] Today at 5:57 PM
wtf

OSINT

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

What is OSINT

- Open Source
  - The stuff you are gathering is accessible to the general public (most of the time)
  - If it is not immediately accessible, it will be with some amount of enumeration.

- 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, 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 / weren’t supposed to

Types of Intelligence

System Intelligence, Network Intelligence, Organizational Intelligence, Human Intelligence

Types of Intelligence

- Systems Intelligence
- Network Intelligence
- Organizational Intelligence
- Human Intelligence ← **Primary focus of today's talk**

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

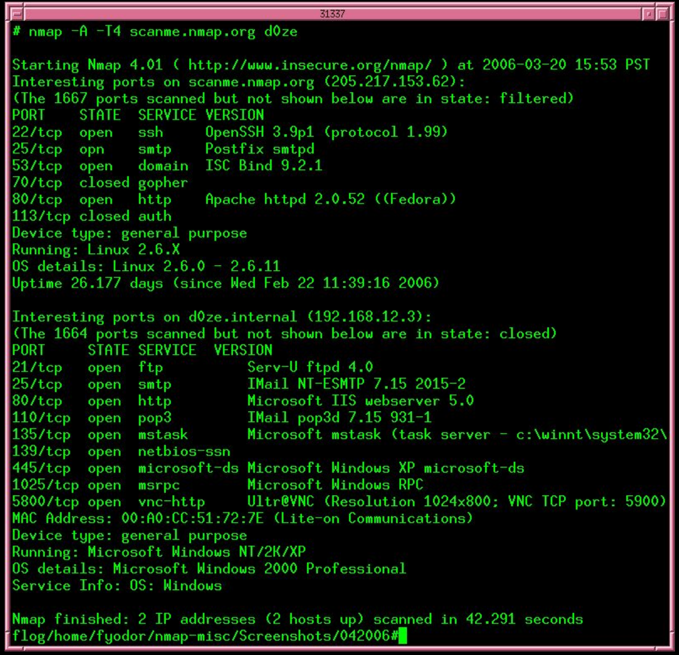
- Port scanning
- Information probes
- IRL Intelligence

Sys Intel - Port Scanning

- Identify what services are being offered by a system

- This is OSINT only because the information is public to the internet
  - When you do this on a local network, it becomes “network enumeration”

- What ports matter from a system
  - Depends on where you are attacking
  - A lot of ports are reserved for dated and deprecated services (port 376)



```
# nmap -A -T4 scanme.nmap.org d0ze

Starting Nmap 4.01 ( http://www.insecure.org/nmap/ ) at 2006-03-20 15:53 PST
Interesting ports on scanme.nmap.org (205.217.153.62):
(The 1667 ports scanned but not shown below are in state: filtered)
PORT    STATE  SERVICE VERSION
22/tcp  open   ssh     OpenSSH 3.9p1 (protocol 1.99)
25/tcp  opn    smtp    Postfix smtpd
53/tcp  open   domain  ISC Bind 9.2.1
70/tcp  closed gopher
80/tcp  open   http    Apache httpd 2.0.52 ((Fedora))
113/tcp closed auth
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.0 - 2.6.11
Uptime 26.177 days (since Wed Feb 22 11:39:16 2006)

Interesting ports on d0ze.internal (192.168.12.3):
(The 1664 ports scanned but not shown below are in state: closed)
PORT     STATE SERVICE      VERSION
21/tcp   open  ftp          Serv-U ftpd 4.0
25/tcp   open  smtp         IMail NT-ESMTP 7.15 2015-2
80/tcp   open  http         Microsoft IIS webserver 5.0
110/tcp  open  pop3         IMail pop3d 7.15 931-1
135/tcp  open  mstask       Microsoft mstask (task server - c:\winnt\system32\
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds Microsoft Windows XP microsoft-ds
1025/tcp open  msrpc        Microsoft Windows RPC
5800/tcp open  vnc-http     Ultr@VNC (Resolution 1024x800; VNC TCP port: 5900)
MAC Address: 00:A0:CC:51:72:7E (Lite-on Communications)
Device type: general purpose
Running: Microsoft Windows NT/2K/XP
OS details: Microsoft Windows 2000 Professional
Service Info: OS: Windows

Nmap finished: 2 IP addresses (2 hosts up) scanned in 42.291 seconds
flog/home/fyodor/nmap-misc/Screenshots/042006#
```

Port Scanning - Common Ports

That you will likely see

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 - Methods

- nmap
    - best port scanning tool
    - will have tutorial in networking meeting
    - Alternatives = masscan

- shodan
    - Google but for networked devices (REALLY COOL)

- Aquatone
    - Look for valid browser-readable content, display on aggregate webpage.
    - Try making your own aquatone in python with just links!

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**

Sys Intel - Information Probes

Gather System information by requesting that information.

CrackMapExec (Great tool) will display version of OS interacted with upon probe completion.

Shodan can also do this stuff sometimes

This is usually case-by-case,
I will update this slide if my knowledge changes

Sys Intel - Info Probe Methods

nmap can help w this, find what services are offered then probe them for more information.

nmap scripts exist too for “banner grabbing”

It really depends on what services the system is offering

Sys Intel - IRL Intelligence

Walk up to a device, look at the make/model.

Useful if you have supervised physical access / photos.

If you have physical access to something, chances are you are beyond needing to do OSINT (just plug in a ducky)

Network Intelligence

where is it and who is it talking to?

Network Intelligence - Summary

Like system intelligence, but focused more on communications.

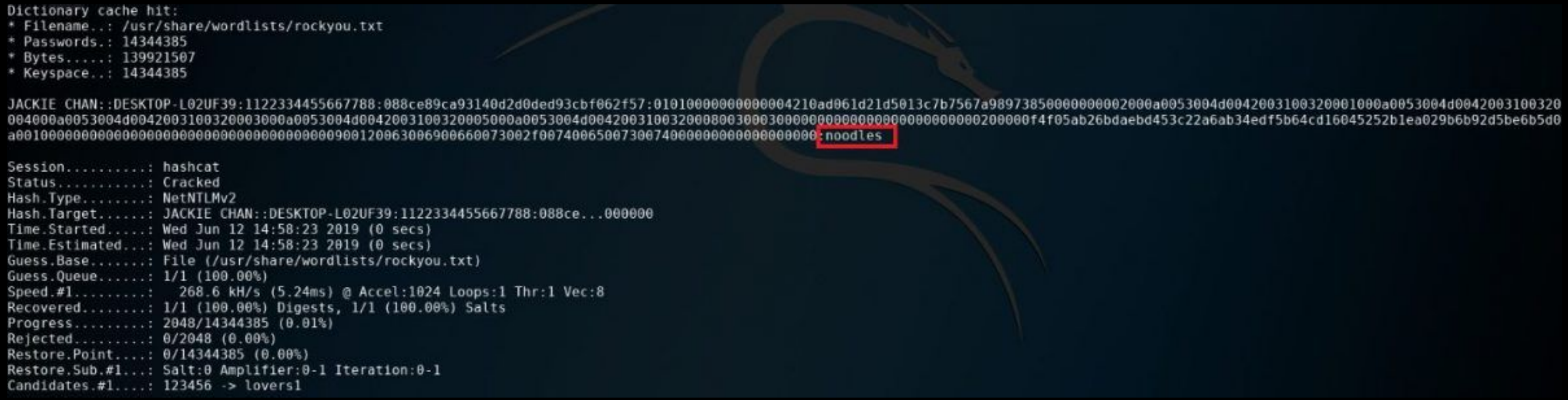
Given a network of systems, who talks to who and why.

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

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

Network Intelligence - Methods

- Depending on context, ASK
  - Social Engineering → find reason to know, ask
  - Internal Pentesting (yourself/org) → ask IT person who knows.
- Shodan also usually great for this
- Find hub devices and set up monitoring / spoofing on them



```
Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace..: 14344385

JACKIE CHAN::DESKTOP-L02UF39:1122334455667788:088ce89ca93140d2d0ded93cbf062f57:0101000000000000004210ad061d21d5013c7b7567a98973850000000002000a0053004d0042003100320001000a0053004d0042003100320
004000a0053004d0042003100320003000a0053004d0042003100320005000a0053004d0042003100320008003000300000000000000000000000000000200000f4f05ab26bdaebd453c22a6ab34edf5b64cd16045252b1ea029b6b92d5be6b5d0
a0010000000000000000000000000000000000000000900120063006900660073002f007400650073007400000000000000000000:noodles

Session..........: hashcat
Status...........: Cracked
Hash.Type........: NetNTLMv2
Hash.Target......: JACKIE CHAN::DESKTOP-L02UF39:1122334455667788:088ce...000000
Time.Started.....: Wed Jun 12 14:58:23 2019 (0 secs)
Time.Estimated...: Wed Jun 12 14:58:23 2019 (0 secs)
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   268.6 kH/s (5.24ms) @ Accel:1024 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests, 1/1 (100.00%) Salts
Progress.........: 2048/14344385 (0.01%)
Rejected.........: 0/2048 (0.00%)
Restore.Point....: 0/14344385 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidates.#1....: 123456 -> lovers1
```

Responder is a spoofing tool, but you can also use it to get a list of devices

Network Intelligence Methods 2

- Enumeration
  - NSLookup is your friend on Windows stuff
  - Given a username, what information does it tell you about other usernames.
  - Take one name for a device, guess others

- Ldap Abuse
  - Ldap is a great protocol when used properly.
  - Abuse the hell out of it, dump everything (probably need credentials)
  - More on this in the pentesting meeting (probably next semester)

Organizational Intel

what are they doing!?!?

Organizational Intel - OpSec

- How is an organization's OpSec?
  - What is the email format (firstname.lastname)
    - Does the email translate into usernames that could be tried
  - Do Org Members have strong opsec
    - Does Alex have their passwords set to their birthday / has had them leaked from clubpenguin.com???
  - Does the org have exposed internal documents
    - Infosec policy (password strength)

Org Intel - Information Gathering

- Abuse public sources of information
  - Zoominfo / Yellowpages + uname format = power

- LinkedIn
  - Boomer companies have lots of people on LinkedIn
  - Quickly → HUMINT

- Public company websites
  - Can expose phone numbers, emails, etc

Org Intel - Policy Information

- If the service has a public facing account system, likely they use same password security for backend.
-

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

-

Human Intelligence

- This is easiest thing to learn
- Creating a map of a person
  - Everything from social media to IRL address

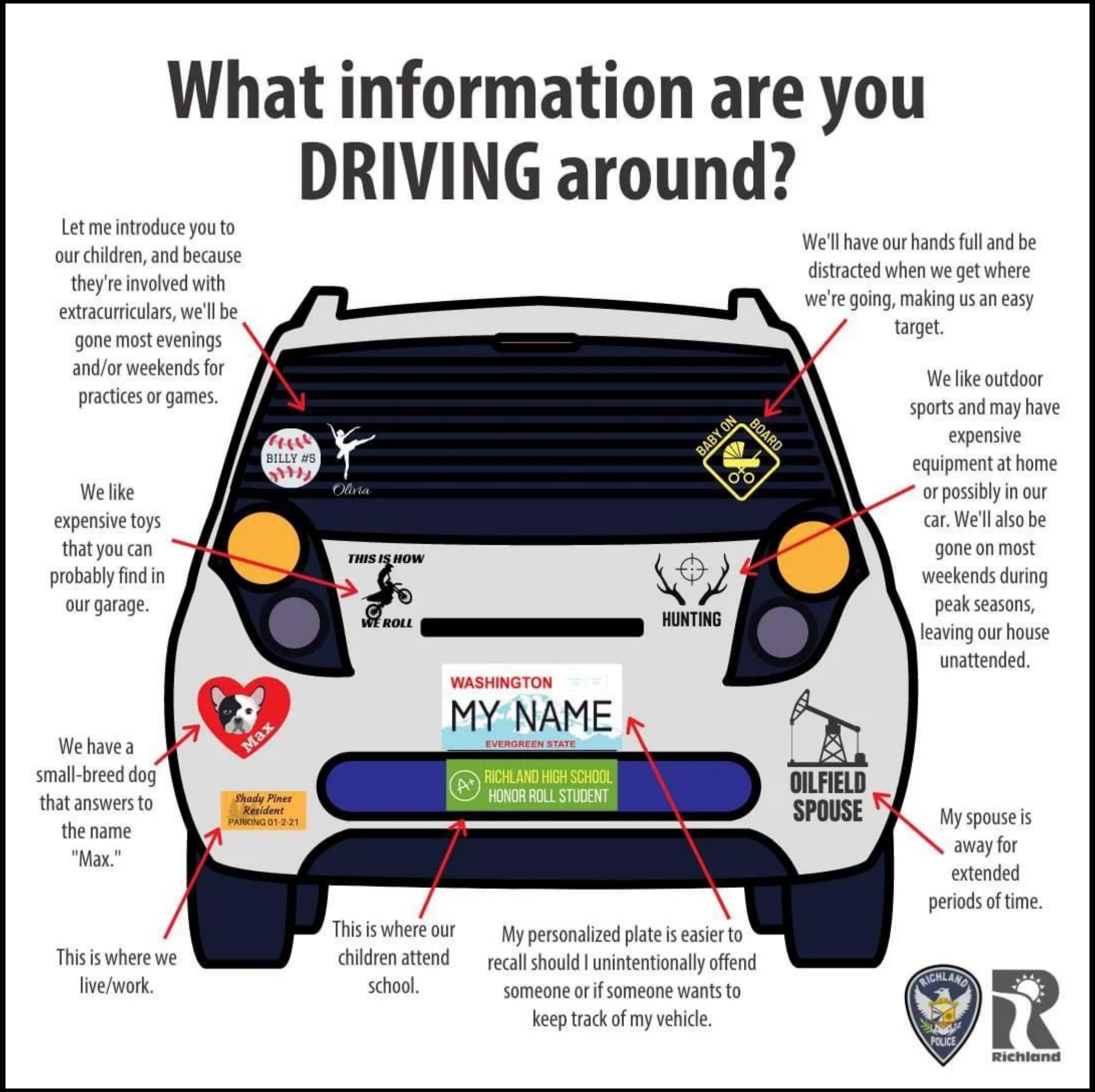
- Tons of different methods, too many to put on a summary page

Essentially stalking but purposeful and less creepy

Human Information Gathering Methods

- **Easy Mode**
  - Social Media
  - Shared Username, use Sherlock
- **Medium Mode**
  - In depth searching utilizing Google Dorking etc
  - Look around networked profiles (friends, followers etc)
  - Paid Services
    - Bullshit like 95% of the time
    - If multiple paid services point to same thing it might be valid
- **Hard Mode**
  - Voting Records
    - Can enumerate given birth month and address
  - **make new friend**
    - Social Engineering
    - be **GODDAMN** careful about your motives

Information Leakage



What information are you DRIVING around?

Let me introduce you to our children, and because they're involved with extracurriculars, we'll be gone most evenings and/or weekends for practices or games.

We'll have our hands full and be distracted when we get where we're going, making us an easy target.

We like outdoor sports and may have expensive equipment at home or possibly in our car. We'll also be gone on most weekends during peak seasons, leaving our house unattended.

We like expensive toys that you can probably find in our garage.

We have a small-breed dog that answers to the name "Max."

My spouse is away for extended periods of time.

This is where we live/work.

This is where our children attend school.

My personalized plate is easier to recall should I unintentionally offend someone or if someone wants to keep track of my vehicle.

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!

OSINT Tips - Human Networks

People have friends

- and connect with them online
- abuse this to find information about a target

Check Friends/Family/Followers

- Is a target tagged in something? Are they mentioned? Did they respond to a friend?
- Friends & family may have information about a target
  - Birthdays and Facebook :(

Media OSINT

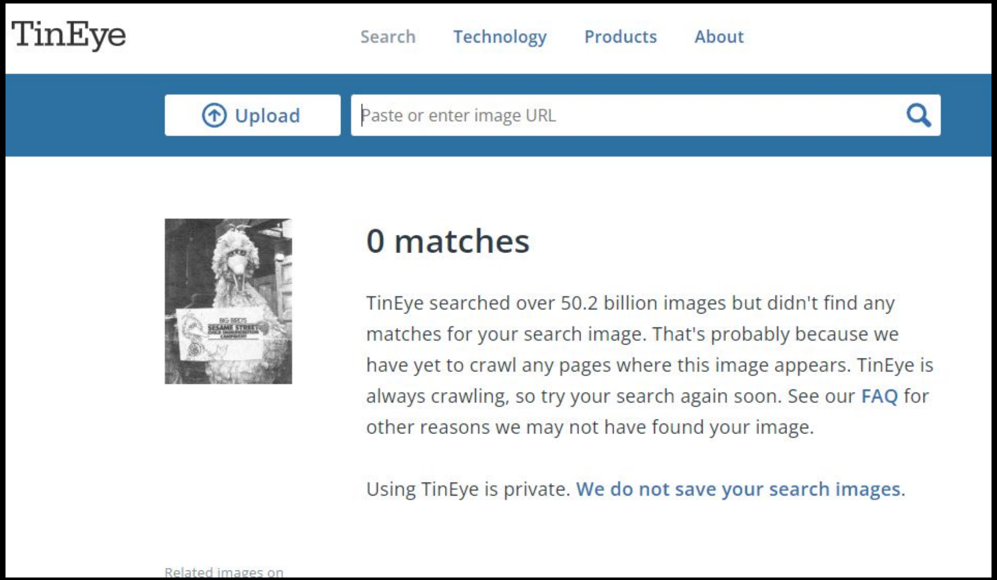
Tineye, Yandex, Google Image Search

- Keyword searcher

- Cropping

Tineye: exact matches

Google: Similar

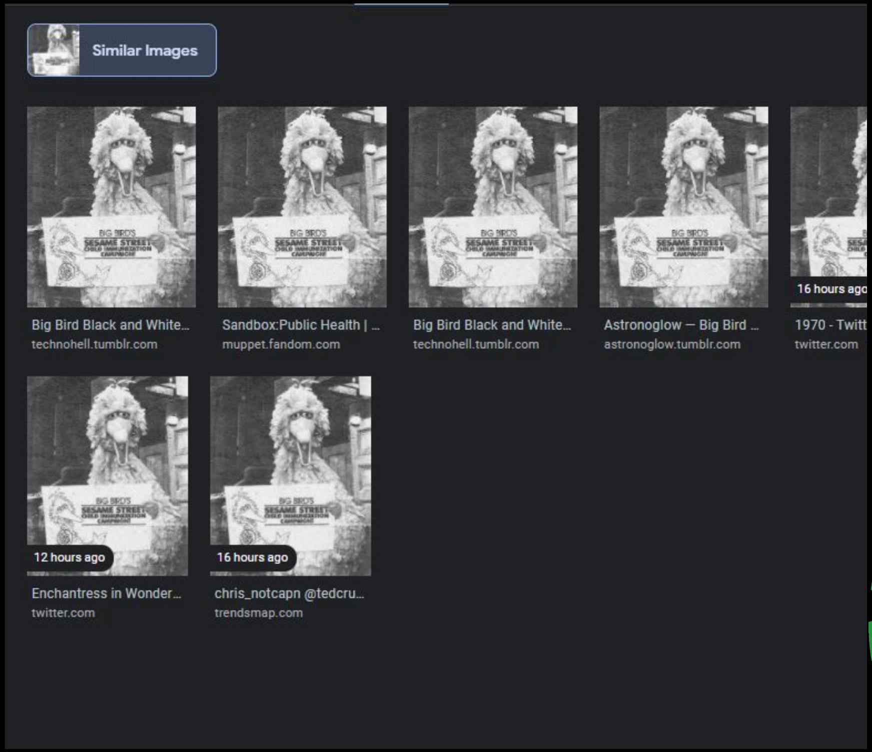


0 matches

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

Media OSINT: Image → Location

- Look for landmarks
  - Landmark != big famous building
  - Dillon’s radio tower challenge

- Context is important
  - Limit the search space as much as possible
  - “He will not divide us 2” (internet historian) is an icky but great example of good osint

- Time
  - Think out of the box, it takes time but most images can be found
  - Geoguessr 0 movement challenge

Profile OSINT

Look for description

Reset password -> email / phone number, crossref with other osint to verify

- **kinda sussy**

Secure osint methods

Don’t get caught lol

Thomas you know what this slide is about so how about you talk about it hahahahahahaha

- Also Thomas but tired

(TLDR Use VPN / private browsing & don't try noticeably attacking someone)

OSINT Tips - Detection

Don't make noise

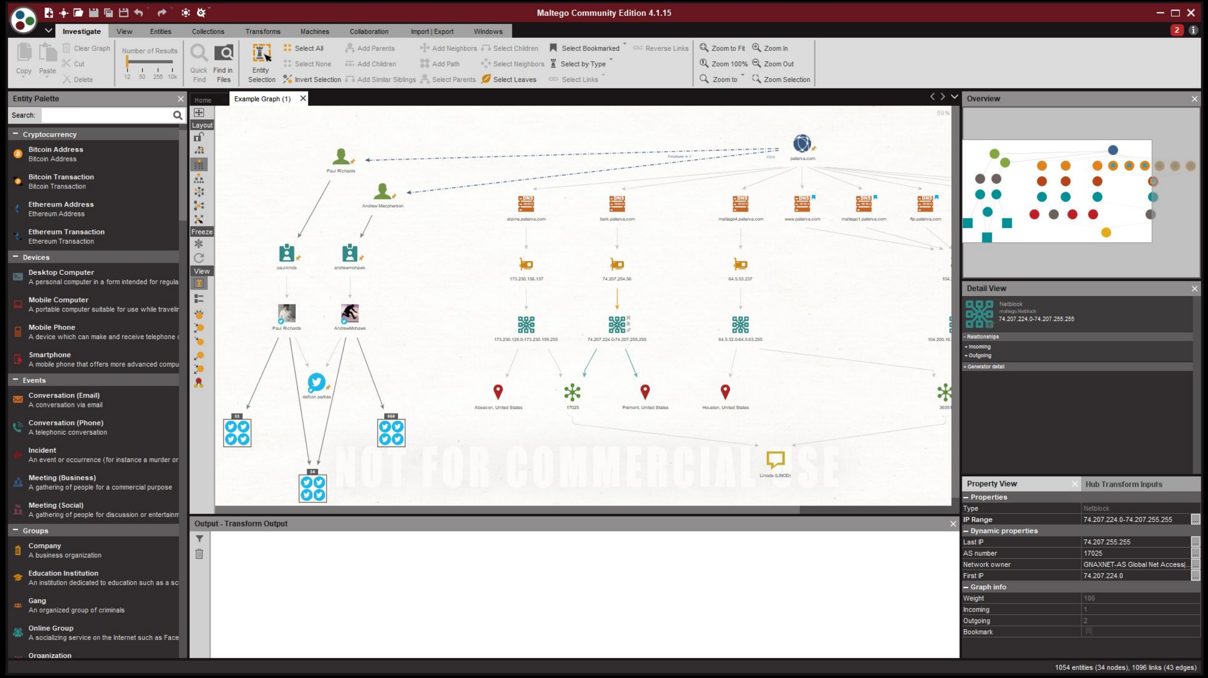
- Don’t do things that would get you noticed
  - LinkedIn Page Views (STAY ANONYMOUS, DON'T DO A LOT)
  - Learn from my mistakes, don't REPLY TO A COMMENT ASKING ABOUT SOME PIECE OF INFORMATION ABOUT SOMEONE.

- Viewing content is generally fine, creating content will often get you noticed. Stay low, stay out of the way, just make acct and look at what you need to.

OSINT Tools - Maltego

OSINT Mapping tool with extra features

Has “Transforms” that can connect.



Definitely give the Community Edition a Spin

Maltego at work

Other OSINT Resources

Michael Brazzel - Open Source Intelligence Techniques (The OSINT Bible)

Tracelabs - OSINT on real missing persons cases

Bellingcat OSINT - Cool OSINT Firm

https://ctf.cybersoc.wales/ : 24/7 Live OSINT CTF (many chals)

Challenge Start (31 challenges for this meeting!)

UIUCTF 2020 - HackerIsabelle (6 challenges)
UIUCTF 2021 - ChaplinCoding (8 challenges)
SP 2019 - TotallyAHuman3025 (11 challenges)
Fall CTF 2021 - SpaghettiEsports (3 challenges)
CCC 2021 - con_angry (3 challenges)
UPCOMING SUITE - **NOT FINISHED** (**20 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

Thursday: Networking

- Fundamentals of communication between hosts
- TCP / UDP / IP, Lower Level Communication (Overview of OSI Stack)
- Common Networking Vulnerabilities / Attacks

Weekend Seminar: Open

- Default = Wireless Networking
- If you want to present instead, let us know by Thursday

Thank you very much

The next many slides have information about specific websites that you can use for specific challenges / you may find useful -- open them on your own computer if you'd like to browse them.

This is a living presentation, and every so often I will update it, eventually it may get really big!

Follow @0xQuig on twitter ;) Find something about me I didn't know/forgot was on the internet for many

Reddit

- Reddit is a semi-anonymous website
  - Some people deanonymize themselves.
    - Ex. President Obama, u/Giga_Gamby
  - Some people deanonymize themselves accidentally
    - u/Badongschlong, Yours truly.
  - Everyone gets sloppy.
- If you look long enough, you can usually link someone to a different account
- Search techniques
  - https://www.reddit.com/wiki/search
  - Author:
  - Selftext:
  - Boolean Operators
  - Comments NOT included in searching on reddit.
- Believe it or not you can actually have profiles

Twitter

- Always check Twitter bios, they often give out information you may need.
- Advanced Searches
  - Twitter has an advanced search bar, but it also has extra parameters.
  - https://lifehacker.com/search-twitter-more-efficiently-with-these-search-opera-1598165519
  - from:@ vs to:@ vs @
  - near: and within:
  - since: , until: , before:
  - :) , :(, ? operator, all boolean operators
  - “” vs just typing it in (keyword vs string)
- Check who they are following, check who is following them
  - Twitter API is pog
- Check in several places
  - Mentions (to and from), media (ALT Text), LISTS, Likes!!, Image Tags / Location
  - Sent application (TweetDeck)

Youtube

- Youtube doesn't allow you to search for comments, which makes makes finding information by comment searching difficult.
- Look for information that the channel left public. There is A LOT of it
  - Even if the discussion page is not visible, you can usually go there by adding /discussion at the end of the link.
- Youtube sends you the full banner image, not just the crop.
- About page
  - Often has EMAIL if the person was not paying attention on setup.
- Advanced search queries
  - Many are same as the other websites
  - https://tubularinsights.com/advanced-youtube-search-tips/

Imgur

Comments exist, and you can see **all** of them for a profile

Every image uploaded is public, **even if it is not actually public**

Github

Commit history exists, not many people know how to modify it.

Github shares email by default (unless this has recently changed)

Check code for identifying information

Actual Websites

Refer to web challenges (robots.txt, sitemap.xml etc)

Check about me pages, contact us pages, look for specific people.

Don't be afraid to use inspect element (We are in Illinois not Missouri)

Look for backend (/wp-admin) and try default credentials if permissible

- **TRY ONLY ONCE, DO NOT LOCK SOMEONE OUT!!!**

Check whois, DNS Records

Gmail

Profile pictures have upscaled and uncropped versions

Get google id from email, view reviews and public shared photos.

Facebook

Facebook does not like it when you make fake accounts.

This one is pretty self explanatory but I will drop more info here in a bit.

Linkedin

This one is also pretty self explanatory

Email sharing on default, check contact info

Most people dont lie on linkedin, and you are able to get alot of infro from it.

Discord

Mutual servers, mutual friends

Profile photos, About Page, (NEW) Server PFP’s

Attachments are public, they all

See Kuilin’s Discord Recon challenges (will see if they work anymore)

IRL Stuff (Location, Phone #, etc)

Voting records, whitepages, etc.

I gave myself too many things to finish, but I will happily talk abt this stuff.