Using OSINT to Investigate School Shooters

Joas A Santos

https://www.linkedin.com/in/joas-antonio-dos-santos

Introduction

→ Unfortunately school shooters have become more frequent with each passing year. Since the events of Columbine, around the world, many young people have been inspired by this unfortunate massacre to justify all their hatred and resentment and take the lives of many innocent people.

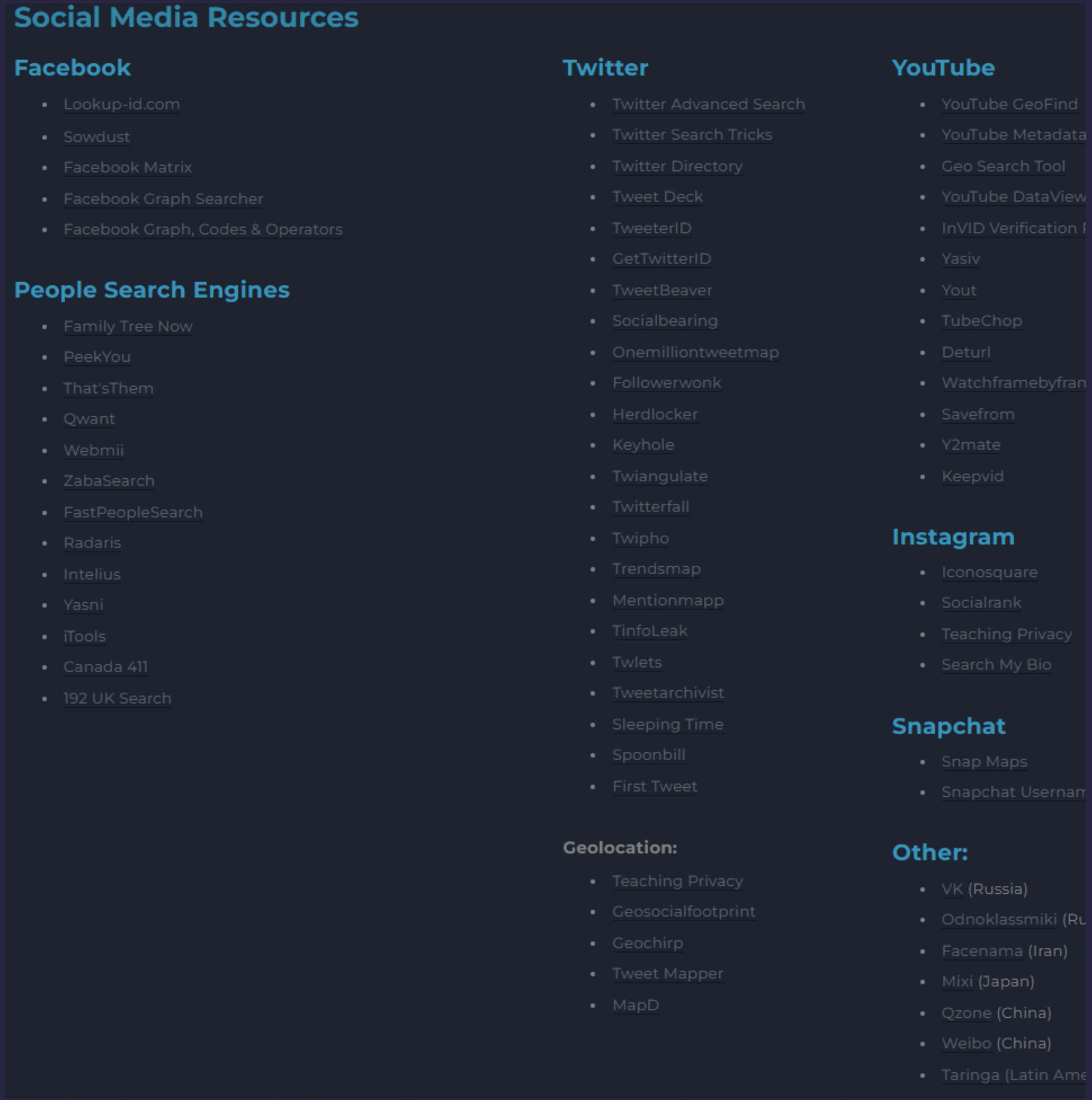
→ Many of the signs that a fatality happens, first appear on social networks and internet discussion forums.

→ With this, I will present some techniques that can be useful to investigate such cases.

→ Observation: This is just an identification process, nothing guarantees that the person will try something, however nothing guarantees that he can't do something wrong. Therefore, always inform the authorities of anyone who posts content of the genre.

Monitoring Social Medias

- → Use tools to monitor social networks, be it Facebook, Twitter, VK, Discord, Telegram, WhatsApp, Instagram, Reddit and even Chans.
- → Having mapped the groups and media, where communities that share extremist ideas gather is a fundamental task.



Social Media Resources

Facebook

- Lookup-id.com
- Sowdust
- Facebook Matrix
- Facebook Graph Searcher
- Facebook Graph, Codes & Operators

People Search Engines

- Family Tree Now
- PeekYou
- That'sThem
- Qwant
- Webmii
- ZabaSearch
- FastPeopleSearch
- Radaris
- Intelius
- Yasni
- iTools
- Canada 411
- 192 UK Search

Twitter

- Twitter Advanced Search
- Twitter Search Tricks
- Twitter Directory
- Tweet Deck
- TweeterID
- GetTwitterID
- TweetBeaver
- Socialbearing
- Onemilliontweetmap
- Followerwonk
- Herdlocker
- Keyhole
- Twiangulate
- Twitterfall
- Twipho
- Trendsmap
- Mentionmapp
- TinfoLeak
- Twlets
- Tweetarchivist
- Sleeping Time
- Spoonbill
- First Tweet

Geolocation:

- Teaching Privacy
- Geosocialfootprint
- Geochirp
- Tweet Mapper
- MapD

YouTube

- YouTube GeoFind
- YouTube Metadata
- Geo Search Tool
- YouTube DataView
- InVID Verification
- Yasiv
- Yout
- TubeChop
- Deturl
- Watchframebyfran
- Savefrom
- Y2mate
- Keepvid

Instagram

- Iconosquare
- Socialrank
- Teaching Privacy
- Search My Bio

Snapchat

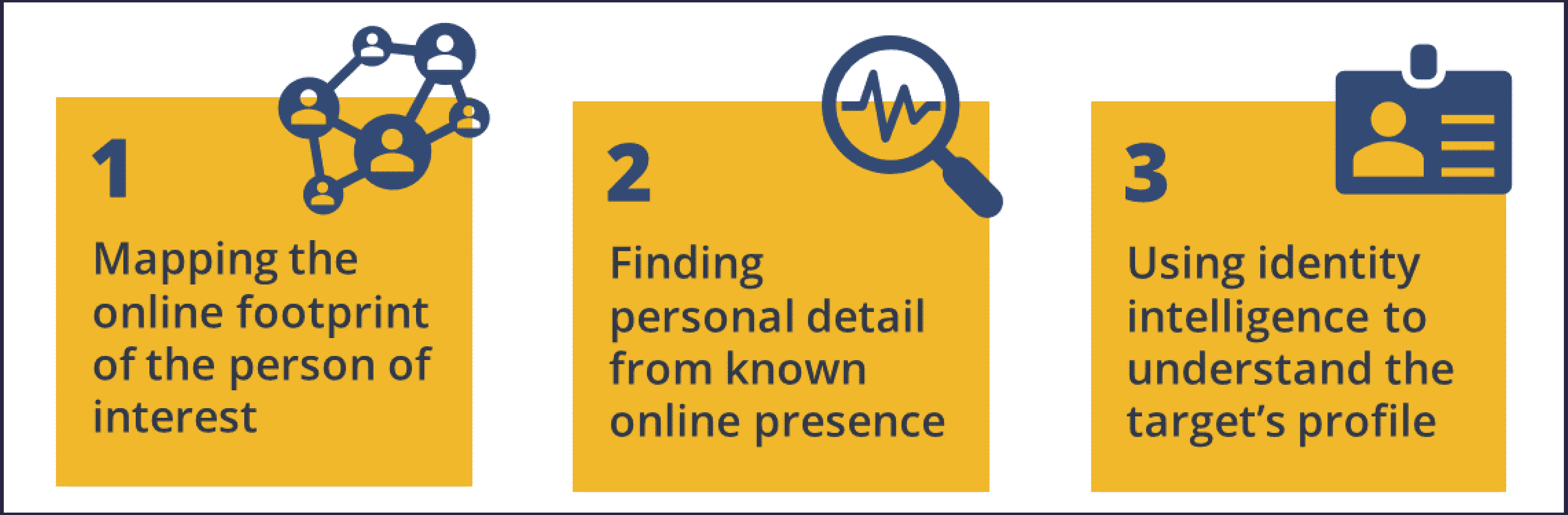
- Snap Maps
- Snapchat Usernam

Other:

- VK (Russia)
- Odnoklassmiki (Ru
- Facenama (Iran)
- Mixi (Japan)
- Qzone (China)
- Weibo (China)
- Taringa (Latin Ame

https://www.osinttechniques.com/osint-tools.html

How to Conduct Person of Interest Investigations Using OSINT and Maltego



1 Mapping the online footprint of the person of interest

2 Finding personal detail from known online presence

3 Using identity intelligence to understand the target's profile

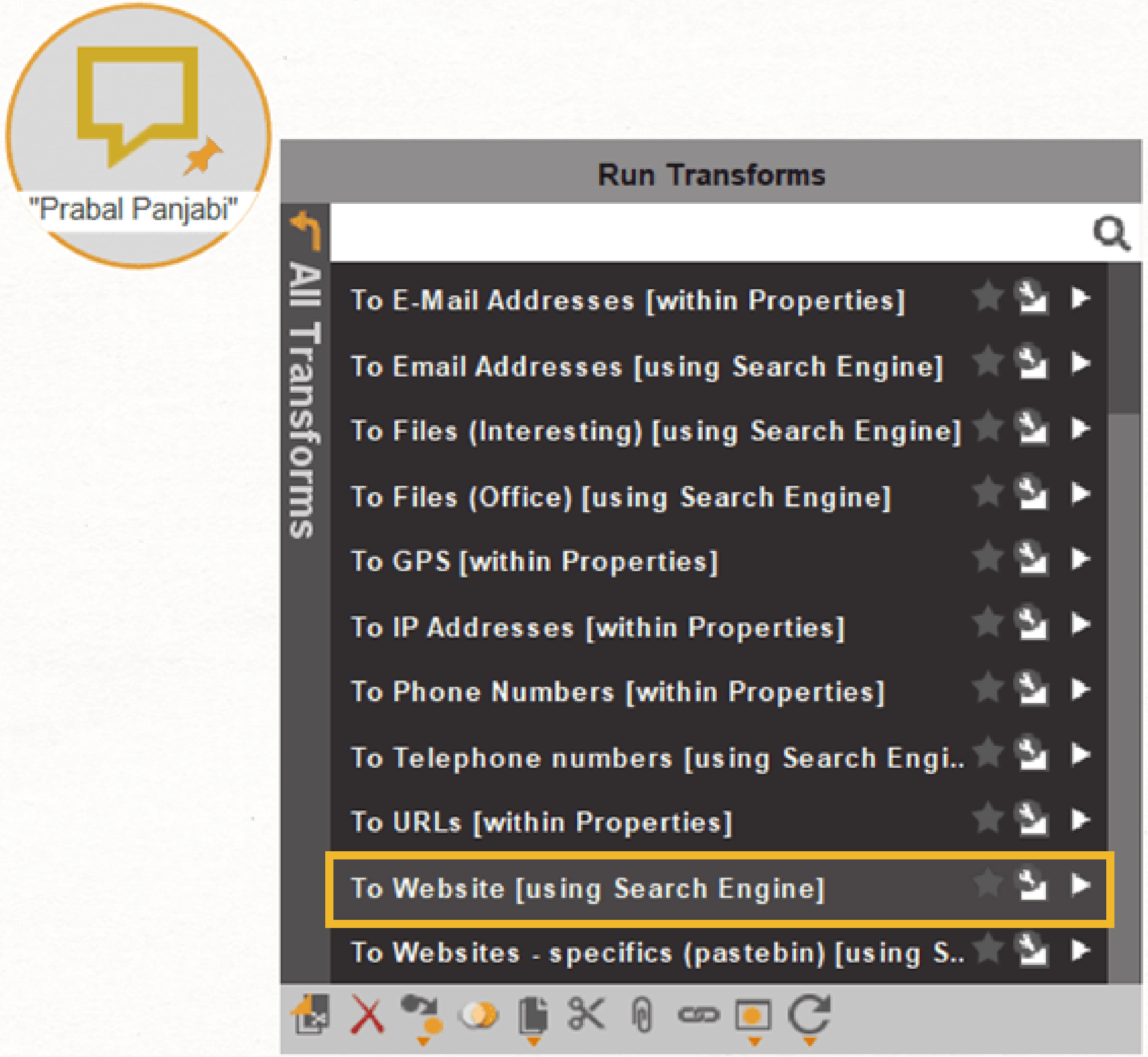
https://www.maltego.com/blog/how-to-conduct-person-of-interest-investigations-using-osint-and-maltego/

How to Conduct Person of Interest Investigations Using OSINT and Maltego

Getting Started: Transforms Hub Items Required for This Person of Interest Investigation

→ We will use the following Hub items in this tutorial: Maltego Standard Transforms, Social Links CE, and Pipl. If you would like to follow along in your own Maltego Client, please ensure that these Hub items are installed.

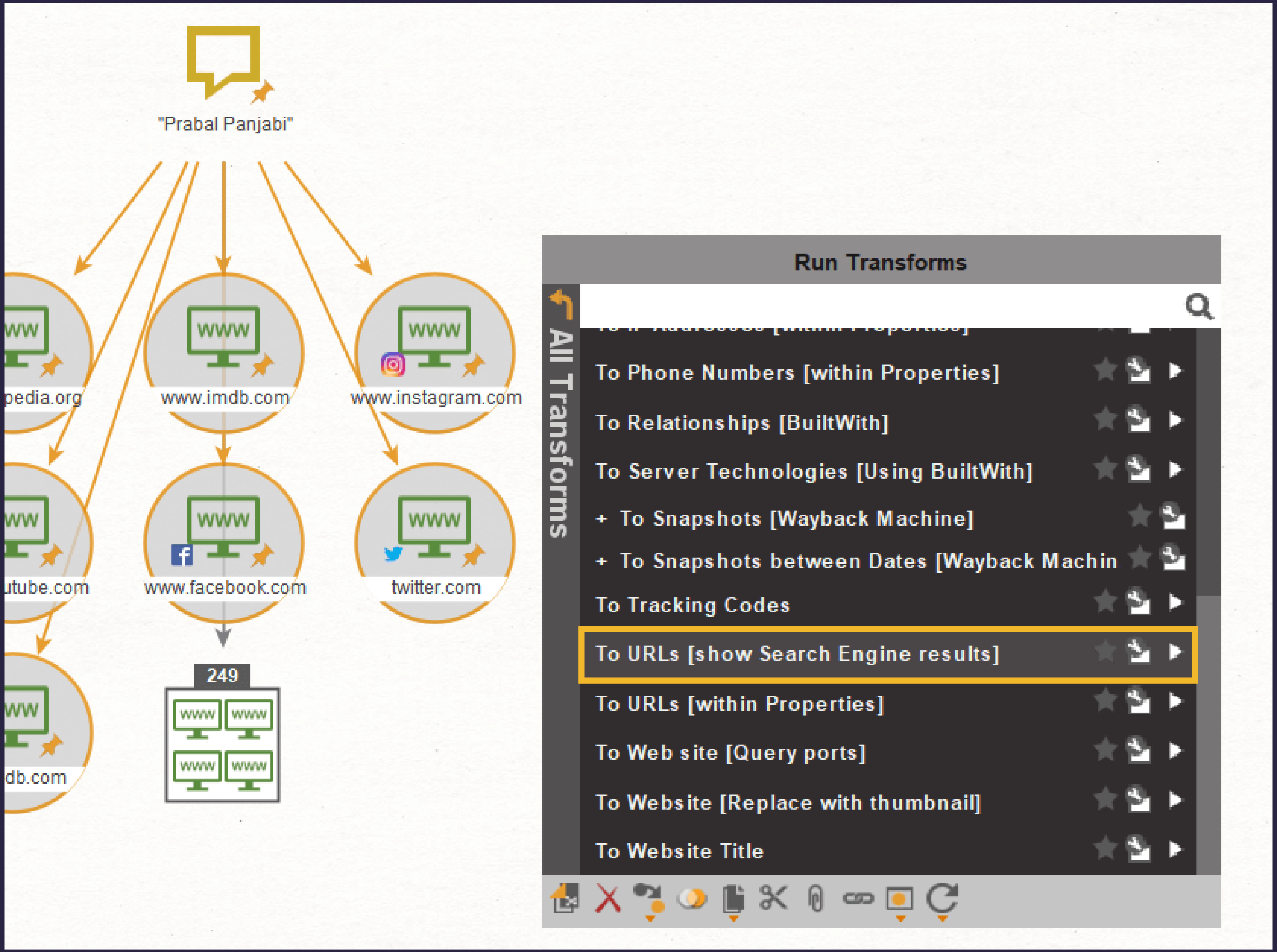
We begin this investigation with a Phrase Entity as the starting point and change the input value from default to the target alias, "Prabal Panjabi." To increase the accuracy of our Transform results, we use some search engine Dorking techniques and add quotation marks around the input text.



To E-Mail Addresses [within Properties]
To Email Addresses [using Search Engine]
To Files (Interesting) [using Search Engine]
To Files (Office) [using Search Engine]
To GPS [within Properties]
To IP Addresses [within Properties]
To Phone Numbers [within Properties]
To Telephone numbers [using Search Engi..
To URLs [within Properties]
To Website [using Search Engine]
To Websites - specifics (pastebin) [using S..

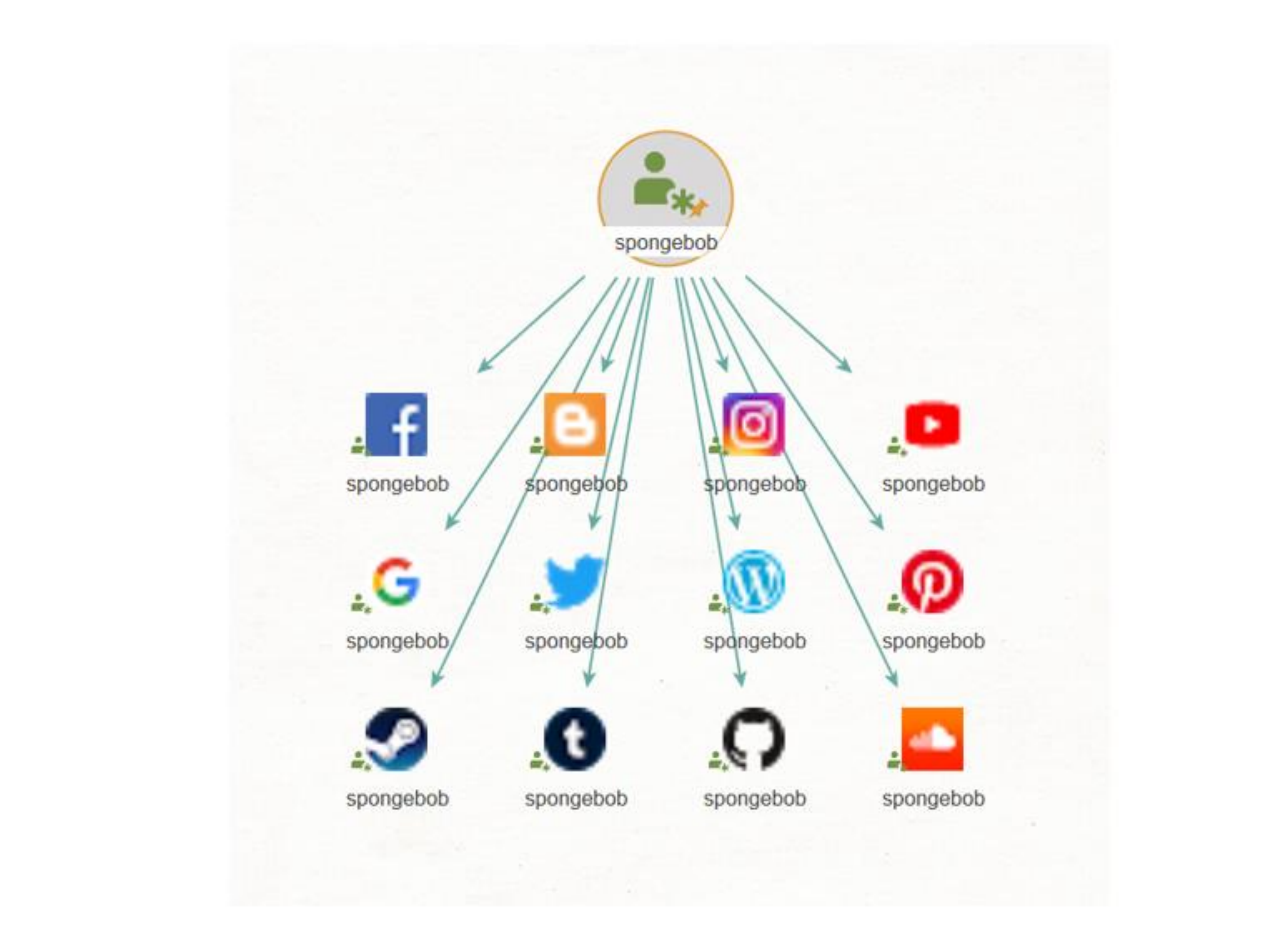
How to Conduct Person of Interest Investigations Using OSINT and Maltego

- This Transform queries the Bing search engine, which returns all websites mentioning our quoted search term, “Prabal Panjabi”.
- Running this Transform has returned 256 websites, including social media profiles or public pages like Facebook, Twitter, Instagram, Wikipedia, Twitter, and even IMDB.


"Prabal Panjabi"
pedia.org
www.imdb.com
www.instagram.com
utube.com
www.facebook.com
twitter.com
db.com
249
Run Transforms
All Transforms
To Phone Numbers [within Properties]
To Relationships [BuiltWith]
To Server Technologies [Using BuiltWith]
+ To Snapshots [Wayback Machine]
+ To Snapshots between Dates [Wayback Machin
To Tracking Codes
To URLs [show Search Engine results]
To URLs [within Properties]
To Web site [Query ports]
To Website [Replace with thumbnail]
To Website Title

Examining your Digital Profile and Social Media Footprint

- Researching social network linked to an alias
- Our first step is to add an alias Entity, rename it with your nickname and right-click it to run the Transform below, which comes pre-installed within the Maltego Standard Transforms:
- To Social Account [Using NameChk]

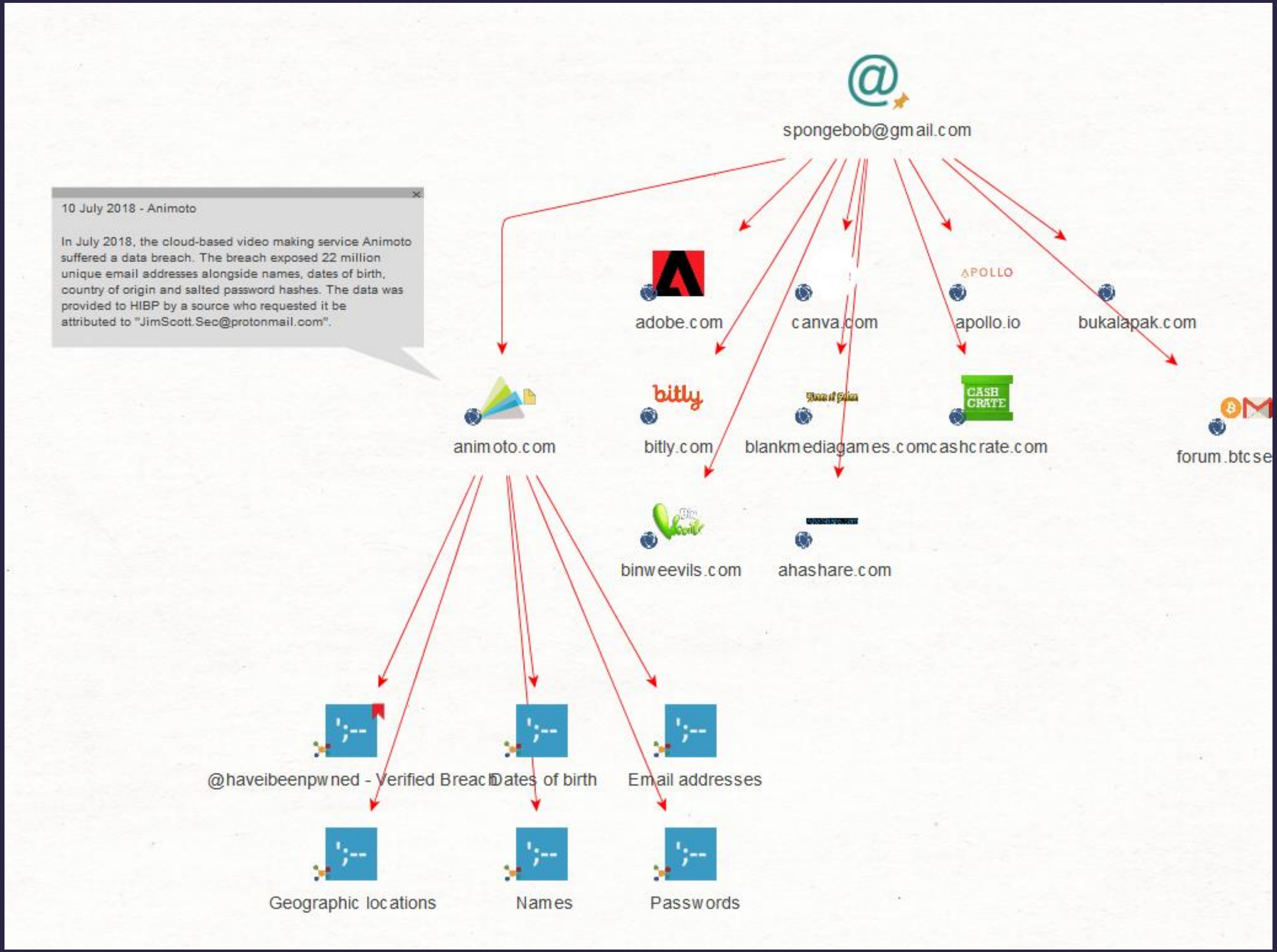


https://www.maltego.com/blog/beginners-guide-examining-your-digital-profile/

Examining your Digital Profile and Social Media Footprint

Investigate Personal Information using a Person’s Name

- Next, we look at how to check whether your account has been involved in a data breach. To check this, we use a service by one of our data partners Have I Been Pwned (HIBP). First you need to install the hub item from the Transform Hub, details can be found here.
- Starting with your email, we select the email and run the following Transforms:
- Get all breaches involving an email address
- Get all pastes featuring the email address

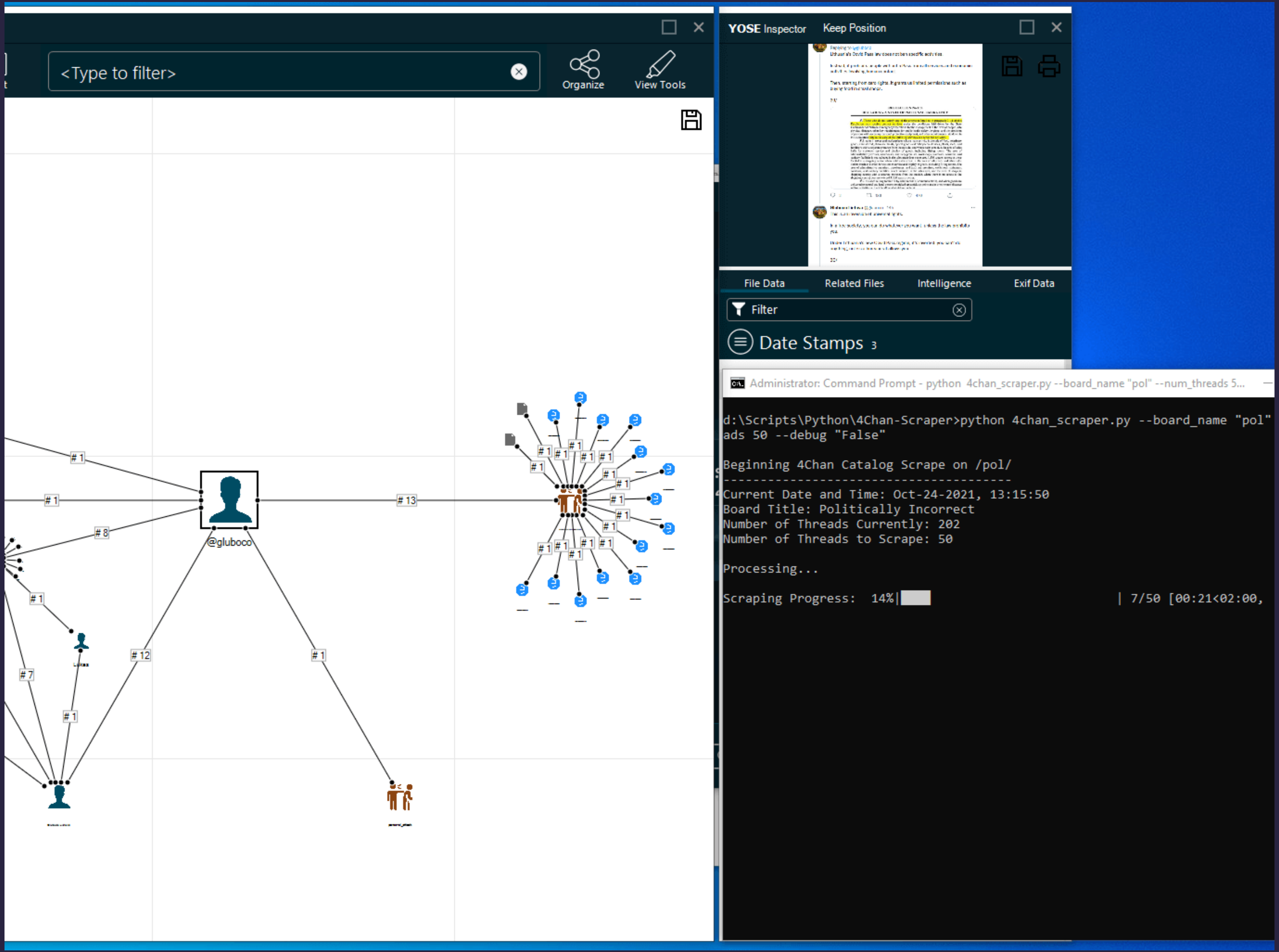


10 July 2018 - Animoto

In July 2018, the cloud-based video making service Animoto suffered a data breach. The breach exposed 22 million unique email addresses alongside names, dates of birth, country of origin and salted password hashes. The data was provided to HIBP by a source who requested it be attributed to "JimScott.Sec@protonmail.com".

4Chan OSINT

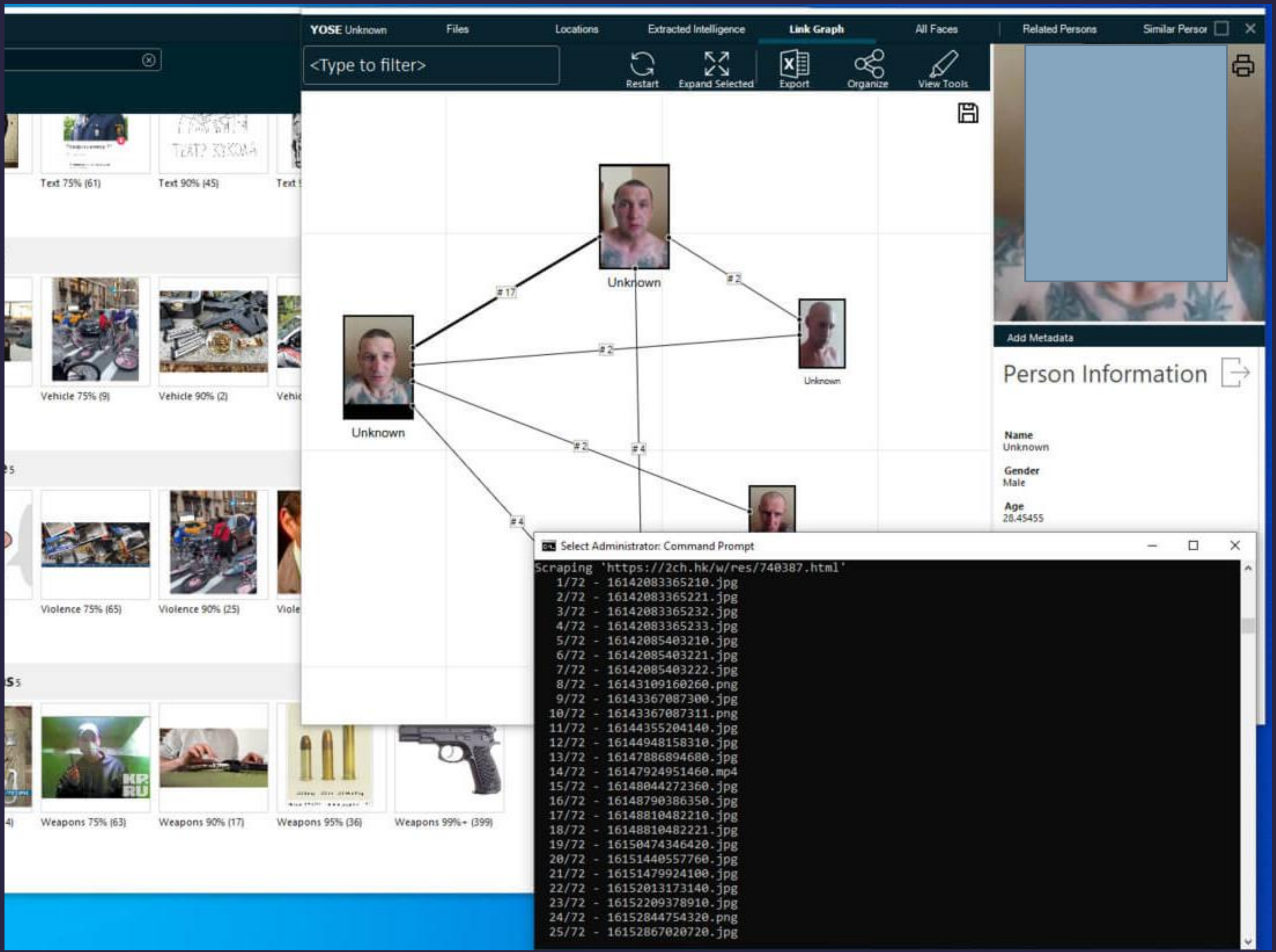
- → Many cases of shooters and extremists end up appearing on sites like 4chan, obtaining information and analyzing it is very important for an initial investigation.
- → You can identify potential threats in the face of a complicated scenario, either through history, photos that the user shares on their social networks and speeches
- → Tool: https://github.com/malavmodi/4Chan-Scraper



```
d:\Scripts\Python\4Chan-Scraper>python 4chan_scraper.py --board_name "pol"
ads 50 --debug "False"

Beginning 4Chan Catalog Scrape on /pol/
---------------------------------------
Current Date and Time: Oct-24-2021, 13:15:50
Board Title: Politically Incorrect
Number of Threads Currently: 202
Number of Threads to Scrape: 50

Processing...

Scraping Progress:  14%|███                          | 7/50 [00:21<02:00,
```

4Chan Image OSINT

- This is a Python script that scrapes images from 4chan threads or entire boards. It takes in command line arguments to determine whether to scrape a single thread or an entire board, the URL of the thread or the board letter, and the destination directory to save the downloaded images.
- The get_board_threads function uses regular expressions to extract the thread IDs from the HTML response of the board catalog page. The download_file function downloads and saves an image from a given URL to a specified directory. The get_file_urls and get_filenames functions extract the URLs and filenames of the images from the HTML response of a thread page using Beautiful Soup.
- The main function checks the command line arguments to determine which mode to run in and calls the appropriate functions to scrape and download the images.
- Overall, the script is functional but there are several areas that could be improved. The use of regular expressions to extract thread IDs is brittle and may not work if 4chan changes their HTML response format. It would be better to use an HTML parser like Beautiful Soup to extract the thread IDs. The script also does not handle errors or exceptions very gracefully, and could benefit from better error handling and user input validation.
- Tool: https://github.com/graysonpike/python-4chan-scraper



Name
Unknown

Gender
Male

Age
28.45455

```
Scraping 'https://2ch.hk/w/res/740387.html'
   1/72 - 16142083365210.jpg
   2/72 - 16142083365221.jpg
   3/72 - 16142083365232.jpg
   4/72 - 16142083365233.jpg
   5/72 - 16142085403210.jpg
   6/72 - 16142085403221.jpg
   7/72 - 16142085403222.jpg
   8/72 - 16143109160260.png
   9/72 - 16143367087300.jpg
  10/72 - 16143367087311.png
  11/72 - 16144355204140.jpg
  12/72 - 16144948158310.jpg
  13/72 - 16147886894680.jpg
  14/72 - 16147924951460.mp4
  15/72 - 16148044272360.jpg
  16/72 - 16148790386350.jpg
  17/72 - 16148810482210.jpg
  18/72 - 16148810482221.jpg
  19/72 - 16150474346420.jpg
  20/72 - 16151440557760.jpg
  21/72 - 16151479924100.jpg
  22/72 - 16152013173140.jpg
  23/72 - 16152209378910.jpg
  24/72 - 16152844754320.png
  25/72 - 16152867020720.jpg
```

4chans OSINT - Materials

→ https://search4chan.org/ (Search Engine for 4chan)

→ https://archived.moe/ (Searchable archive of 4chan posts)

→ https://www.youtube.com/watch?v=DBJIkR3DmU0&ab_channel=JessWerks (OSINT Explore)

→ https://andreafortuna.org/2017/03/15/osint-the-secret-weapon-of-4channers/

Geolocation Techniques – Social Media

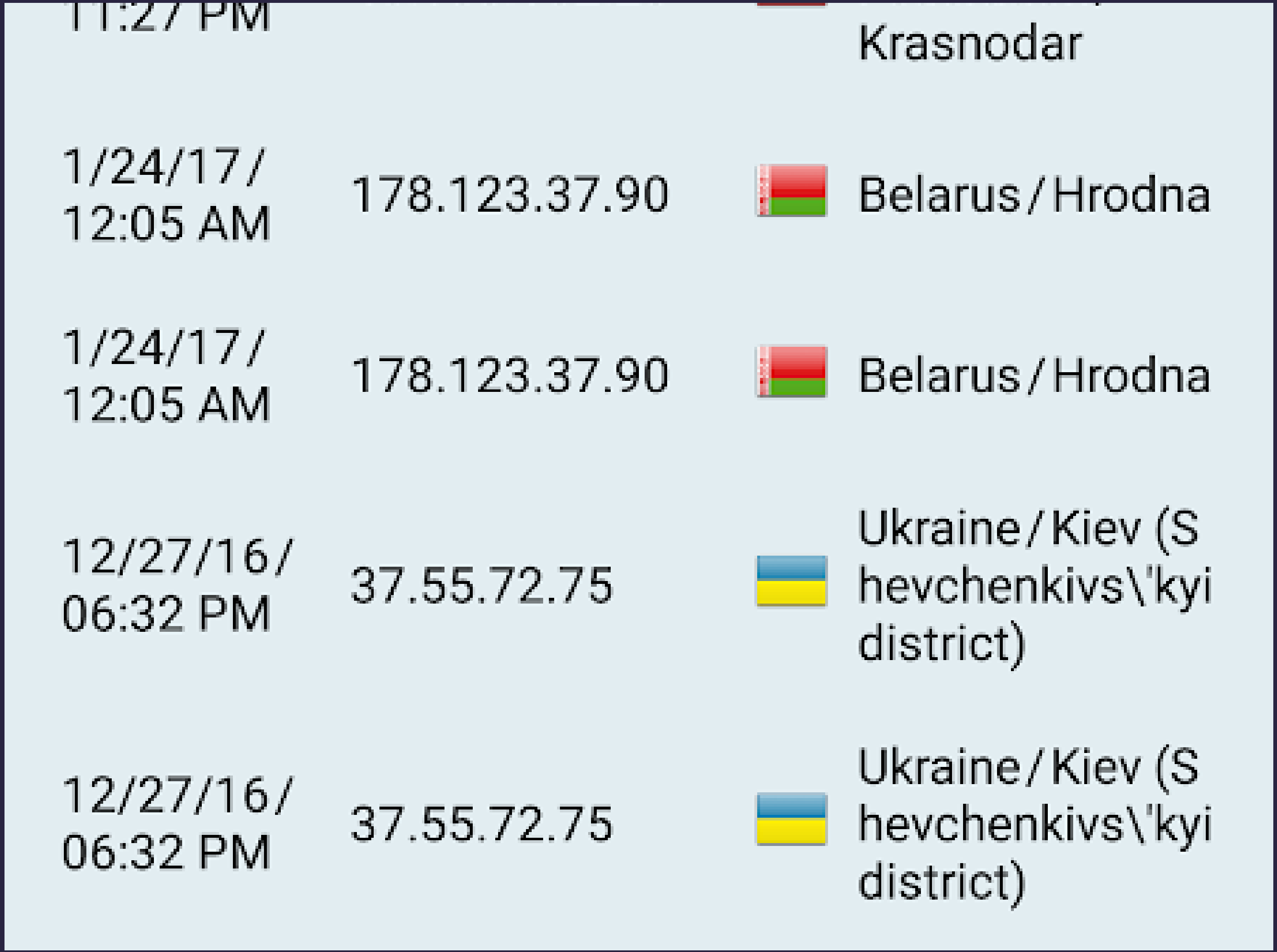
- https://reveal-mklab.iti.gr/reveal/ (Features a multitude of images tampering detection algorithms as well as metadata analysis, geolocation, thumbnail extraction and integration with Google reverse image search.)
- http://www.geocreepy.com/ (Creepy is a platform for OSINT geolocation. Creepy can assist in gathering geolocation-related information from online sources and enables map presentation, search filtering based on exact location and date, comma separated value (CSV) or XML export for further review on Google Maps. Searches for Twitter, Flickr, and Instagram are currently sponsored by Creepy. It extracts geolocation based on image-saved EXIF information, geolocation information accessible through the application programming interface (API), and some other techniques.)
- https://github.com/laramies/metagoofil (Metagoofil is an information gathering tool designed for extracting metadata of public documents (pdf, doc, xls, ppt, doc, ppt, xlsx) belonging to a target company. Metagoofil will perform a search in Google to identify and download the documents to local disk and then will extract the metadata with different libraries like Hachoir, PdfMiner and others. With the results, it will generate a report with usernames, software versions and servers or machine names that will help Penetration testers in the information gathering phase.)

Geolocation Techniques – Social Media

- https://www.spiderfoot.net/ (SpiderFoot is a reconnaissance tool that automatically queries over a hundred public data sources (OSINT) to gather intelligence on IP addresses, domain names, e-mail addresses, names and more. We simply specify the target we want to investigate, pick which modules to enable and then SpiderFoot will collect data to build up an understanding of all the entities and how they relate to each other. The data returned from a SpiderFoot scan will reveal a lot of information about our target, providing insight into possible data leaks, vulnerabilities or other sensitive information that can be leveraged during a penetration test, red team exercise or for threat intelligence. SpiderFoot also provides an easy-to-use interface helping us to collect Open Source Intelligence (OSINT) from several sources automatically, such as SHODAN, SecurityTrails, AlienVault, HaveIBeenPwned, and more, regarding IP addresses, domain names, e-mail addresses, usernames, names, subnets, and ASNs.)
- https://github.com/radioactivetobi/geo-recon (Geo-Recon is an OSINT command-line interface (CLI) tool which is designed to fast track IP Reputation and Geo-location lookup for Security Analysts. It will provide the following details:- Country, Region, City, Organisation, ISP. With the inbuilt reputation check we will be able to see Domain Name, Hostname, Usage type, Confidence of abuse, Number of times reported, last reported and whitelisted. It will also provide us with the information that whether the IP address is malicious or not.)

Geolocation Techniques – Social Media

- iplogger is an IP logger written in Go. It is useful for OSINT and also functions as a URL shortener.
- https://github.com/rquinlivan/iplogger



11:27 PM		Krasnodar
1/24/17 / 12:05 AM	178.123.37.90	Belarus / Hrodna
1/24/17 / 12:05 AM	178.123.37.90	Belarus / Hrodna
12/27/16 / 06:32 PM	37.55.72.75	Ukraine / Kiev (Shevchenkivs\'kyi district)
12/27/16 / 06:32 PM	37.55.72.75	Ukraine / Kiev (Shevchenkivs\'kyi district)

Geolocation Techniques – Social Media (Other Tools)

- → InVid - Verify the reliability of video and image files
- → Google Lens - Search what you see to identify things like dog breed, plant species, shoe make and designer, and more
- → Overpass Turbo - Build interactive maps to help visualize location data
- → Mapillary - Access street-level images and map data from around the world
- → KartaView - Collect street-level imagery from around the world
- → CarNet - Upload an image of a vehicle to determine its make, model, and year
- → WorldLicensePlates.com - Research historical and current license plate designs from across the world
- → VehicleHistory.com - Search vehicle history based on VIN and license plate
- → Poctra - Search salvage and auctioned cars in the US and EU
- Whatismyipaddress
- Utrace

Geolocation Techniques – Social Media (Other Tools)

- IPChicken
- IPAddress
- MyIP
- IPTracker
- LiveIP Map
- GeoBytes
- ViewDNS
- DomainIQ Reverse IP
- DomainTools Reverse IP
- Whoisrequest Reverse IP
- Whatismyipaddress IP Lookup
- UltraTools Whois IP Lookup
- IP2Location
- GeoIPTool

Dark Web Investigation – Dark vs Deep

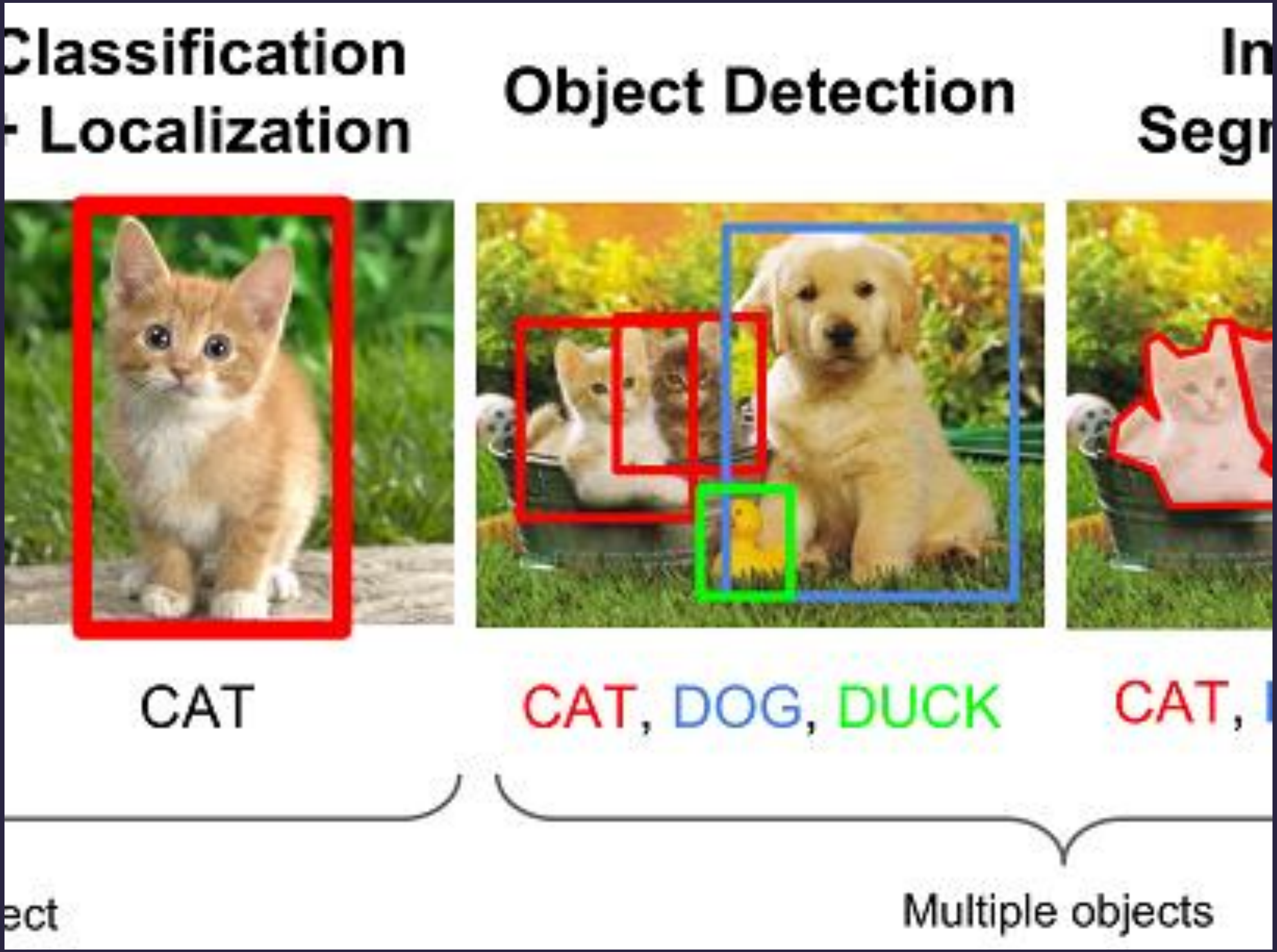
- Unlike the surface web, these two layers represent the non-indexed content available on the internet. This means it can’t be found with your common Google search, however, there are substantial differences between the deep and the dark web.
- For instance, unlike the dark web, the deep web doesn’t require a particular browser to be accessed. Still, its contents can’t be identified, tracked, or crawled by standard search engines because they’re either password-protected or kept behind specific internet services. The data contained within our email inboxes, online banking services, and even job intranets are examples of the deep web. And, as you can imagine, this data is usually only available to the user and the service providers, unless specific allowances for investigators are made in the terms of assist services, for example, criminal investigations.
- The dark web, on the other hand, is comprised of websites that are only accessible via internet services such as The Onion Router (TOR). One of the main differences between Google and TOR is the composition of the URLs they take in, where the ones used to access dark web content use obfuscating techniques, making them almost impossible to guess, remember, or understand. Additionally, the content in the dark web is primarily hosted anonymously and heavily encrypted, providing extra layers of protection against tracing and identification.
- Oftentimes, whatever information is stolen from the deep web (passwords, privileged data) ends up being sold on the dark web. However, not everything that transpires there is of a criminal nature. Journalists, activists, and politicians working and reporting under corrupt or totalitarian regimes use it to gather, collaborate, and exchange information without fear of being harassed or prosecuted.
- https://www.youtube.com/watch?v=BdJ6mrDh9Lw&ab_channel=SocialLinks

Dark Web Investigation

- IACA Tools
- Darknetlive
- The Hidden Wiki
- OnionScan
- Hunchly Hidden Service Reports
- Torch
- Not Evil
- Onion.link
- Ahmia.fi

AI for Image Processing

- Machines can be taught to interpret images the same way our brains do and to analyze those images much more thoroughly than we can. Image processing with artificial intelligence can power face recognition and authentication functionality for ensuring security in public places, detecting and recognizing objects and patterns in images and videos, and so on.
- In this article, we talk about digital image processing and the role of AI in it. We describe some AI-based image processing tools and techniques you may use for developing intelligent applications. We also take a look at the most popular neural network models used for different image processing tasks. This article will be useful for anyone aiming to build a solution for image processing using AI.
- https://www.apriorit.com/dev-blog/599-ai-for-image-processing



AI for Image Processing

- Creating image recognition patterns can be useful in a scrapper to analyze content that it might categorize as threatening, such as gun photos, sensitive and violent content, and more. This way you can further deepen your OSINT against a specific target.
- https://www.theregister.com/2022/06/28/computer_vision_school_guns/

Reverse Image Search

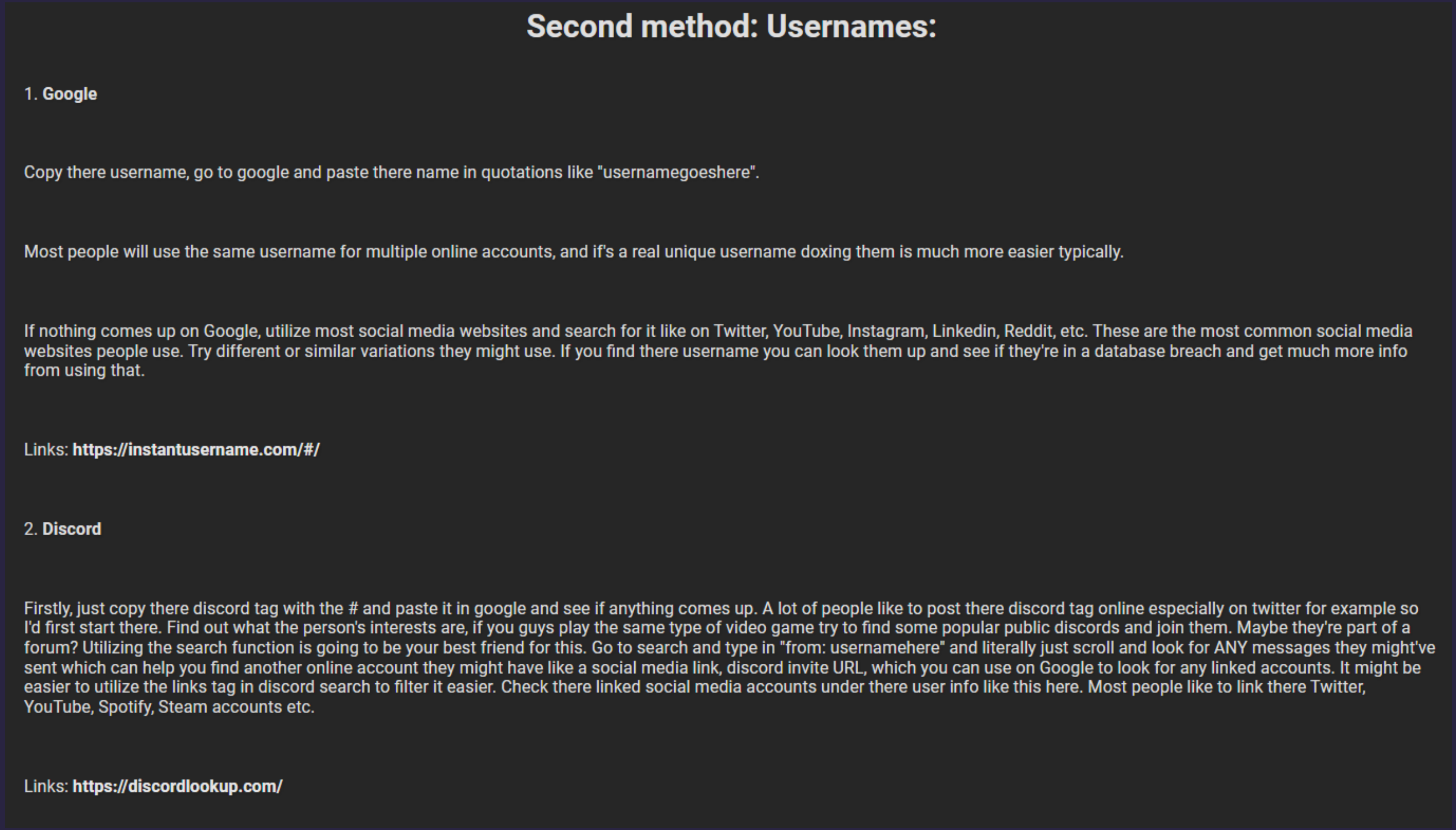
→ https://www.osintcombine.com/reverse-image-analyzer (This tool is designed to make reverse image searching more effective. We provide tabulated results from Google & Yandex which applies AI/Machine vision to extract entities & other items in the image. NO data or images are stored by OSINT Combine)

→ https://www.osintessentials.com/search-by-image

- Jeffrey's Image Viewer
- ExifTool by Phil Harvey
- Metapicz
- IrfanView
- Find Exif Data
- FotoForensics
- Forensically
- Google Images
- Bing Images
- Yandex Images
- Baidu Images
- Tineye
- Image Identify by Wolfram
- Karma Decay
- Pictriev

Doxing and Personal Information OSINT

- https://thatsthem.com/
- https://www.numlookup.com/
- https://discordlookup.com/
- https://instantusername.com/#/



Second method: Usernames:

1. **Google**

Copy there username, go to google and paste there name in quotations like "usernamegoeshere".

Most people will use the same username for multiple online accounts, and if's a real unique username doxing them is much more easier typically.

If nothing comes up on Google, utilize most social media websites and search for it like on Twitter, YouTube, Instagram, Linkedin, Reddit, etc. These are the most common social media websites people use. Try different or similar variations they might use. If you find there username you can look them up and see if they're in a database breach and get much more info from using that.

Links: **https://instantusername.com/#/**

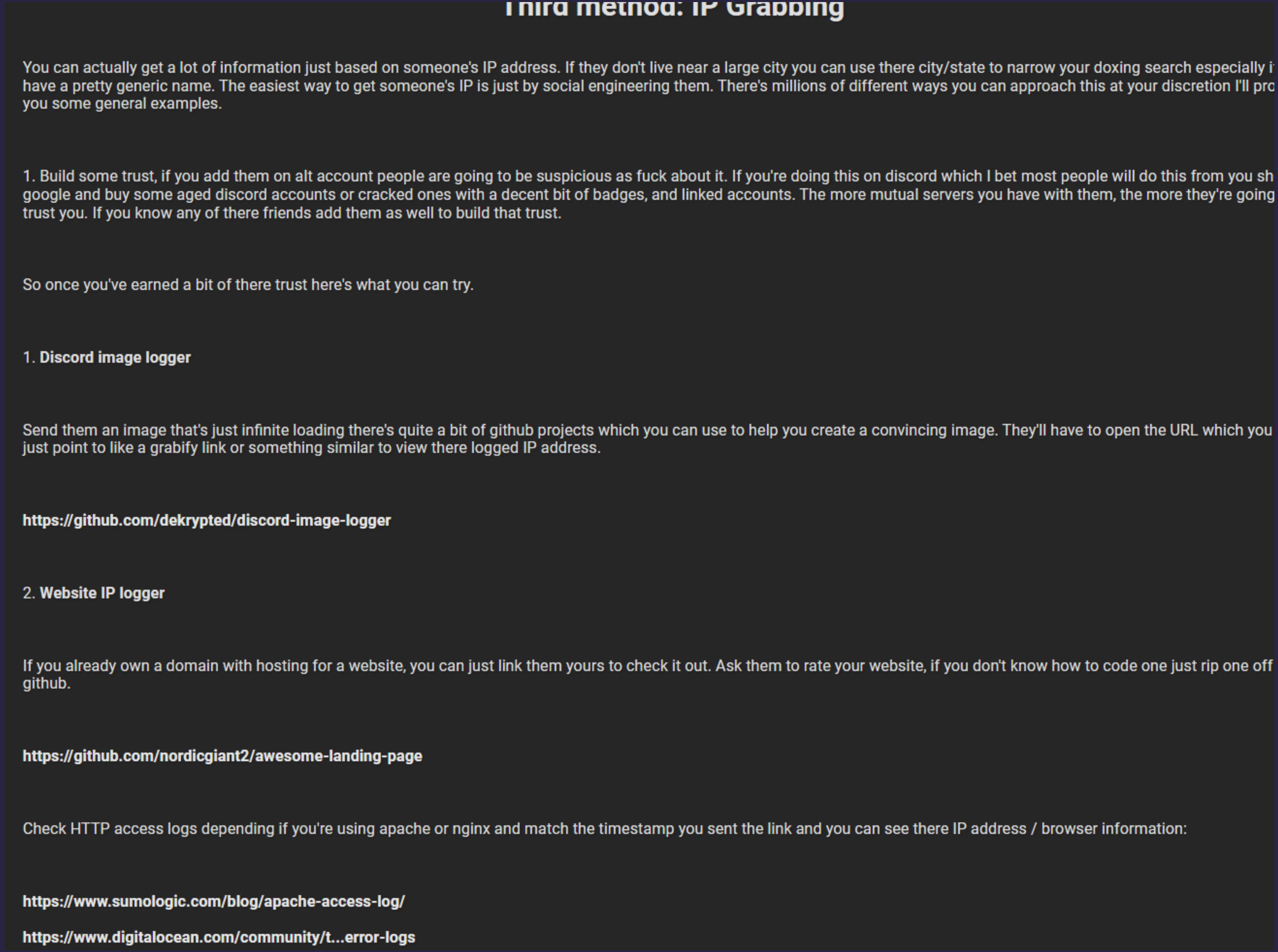
2. **Discord**

Firstly, just copy there discord tag with the # and paste it in google and see if anything comes up. A lot of people like to post there discord tag online especially on twitter for example so I'd first start there. Find out what the person's interests are, if you guys play the same type of video game try to find some popular public discords and join them. Maybe they're part of a forum? Utilizing the search function is going to be your best friend for this. Go to search and type in "from: usernamehere" and literally just scroll and look for ANY messages they might've sent which can help you find another online account they might have like a social media link, discord invite URL, which you can use on Google to look for any linked accounts. It might be easier to utilize the links tag in discord search to filter it easier. Check there linked social media accounts under there user info like this here. Most people like to link there Twitter, YouTube, Spotify, Steam accounts etc.

Links: **https://discordlookup.com/**

Doxing and Personal Information OSINT

- → https://www.digitalocean.com/community/tutorials/nginx-access-logs-error-logs
- → https://www.sumologic.com/blog/apache-access-log/
- → https://github.com/nordicgiant2/awesome-landing-page
- → https://github.com/dekrypted/discord-image-logger



Third method: IP Grabbing

You can actually get a lot of information just based on someone's IP address. If they don't live near a large city you can use there city/state to narrow your doxing search especially i have a pretty generic name. The easiest way to get someone's IP is just by social engineering them. There's millions of different ways you can approach this at your discretion I'll pro you some general examples.

1. Build some trust, if you add them on alt account people are going to be suspicious as fuck about it. If you're doing this on discord which I bet most people will do this from you sh google and buy some aged discord accounts or cracked ones with a decent bit of badges, and linked accounts. The more mutual servers you have with them, the more they're going trust you. If you know any of there friends add them as well to build that trust.

So once you've earned a bit of there trust here's what you can try.

1. **Discord image logger**

Send them an image that's just infinite loading there's quite a bit of github projects which you can use to help you create a convincing image. They'll have to open the URL which you just point to like a grabify link or something similar to view there logged IP address.

https://github.com/dekrypted/discord-image-logger

2. **Website IP logger**

If you already own a domain with hosting for a website, you can just link them yours to check it out. Ask them to rate your website, if you don't know how to code one just rip one off github.

https://github.com/nordicgiant2/awesome-landing-page

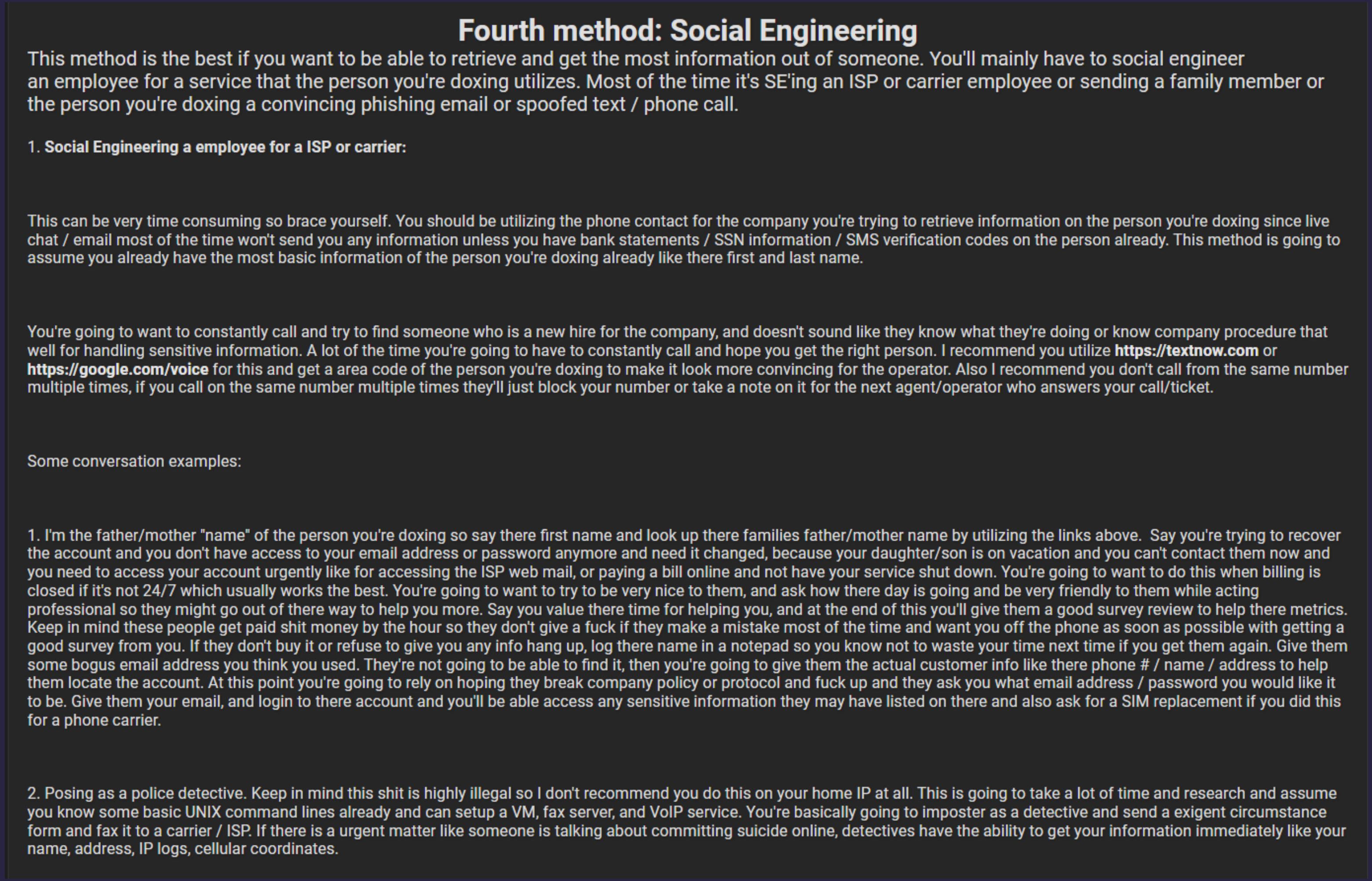
Check HTTP access logs depending if you're using apache or nginx and match the timestamp you sent the link and you can see there IP address / browser information:

https://www.sumologic.com/blog/apache-access-log/

https://www.digitalocean.com/community/t...error-logs

Doxing and Personal Information OSINT

- → https://www.in911.net/uploads/6/5/9/0/65907603/att_wireless_exigent_form.pdf
- → https://www.in911.net/uploads/1/2/4/9/124957688/exigent_form.pdf
- → https://www.xfinity.com/-/media/4231839e374c4f618b2d34004d50987c



Fourth method: Social Engineering

This method is the best if you want to be able to retrieve and get the most information out of someone. You'll mainly have to social engineer an employee for a service that the person you're doxing utilizes. Most of the time it's SE'ing an ISP or carrier employee or sending a family member or the person you're doxing a convincing phishing email or spoofed text / phone call.

1. **Social Engineering a employee for a ISP or carrier:**

This can be very time consuming so brace yourself. You should be utilizing the phone contact for the company you're trying to retrieve information on the person you're doxing since live chat / email most of the time won't send you any information unless you have bank statements / SSN information / SMS verification codes on the person already. This method is going to assume you already have the most basic information of the person you're doxing already like there first and last name.

You're going to want to constantly call and try to find someone who is a new hire for the company, and doesn't sound like they know what they're doing or know company procedure that well for handling sensitive information. A lot of the time you're going to have to constantly call and hope you get the right person. I recommend you utilize **https://textnow.com** or **https://google.com/voice** for this and get a area code of the person you're doxing to make it look more convincing for the operator. Also I recommend you don't call from the same number multiple times, if you call on the same number multiple times they'll just block your number or take a note on it for the next agent/operator who answers your call/ticket.

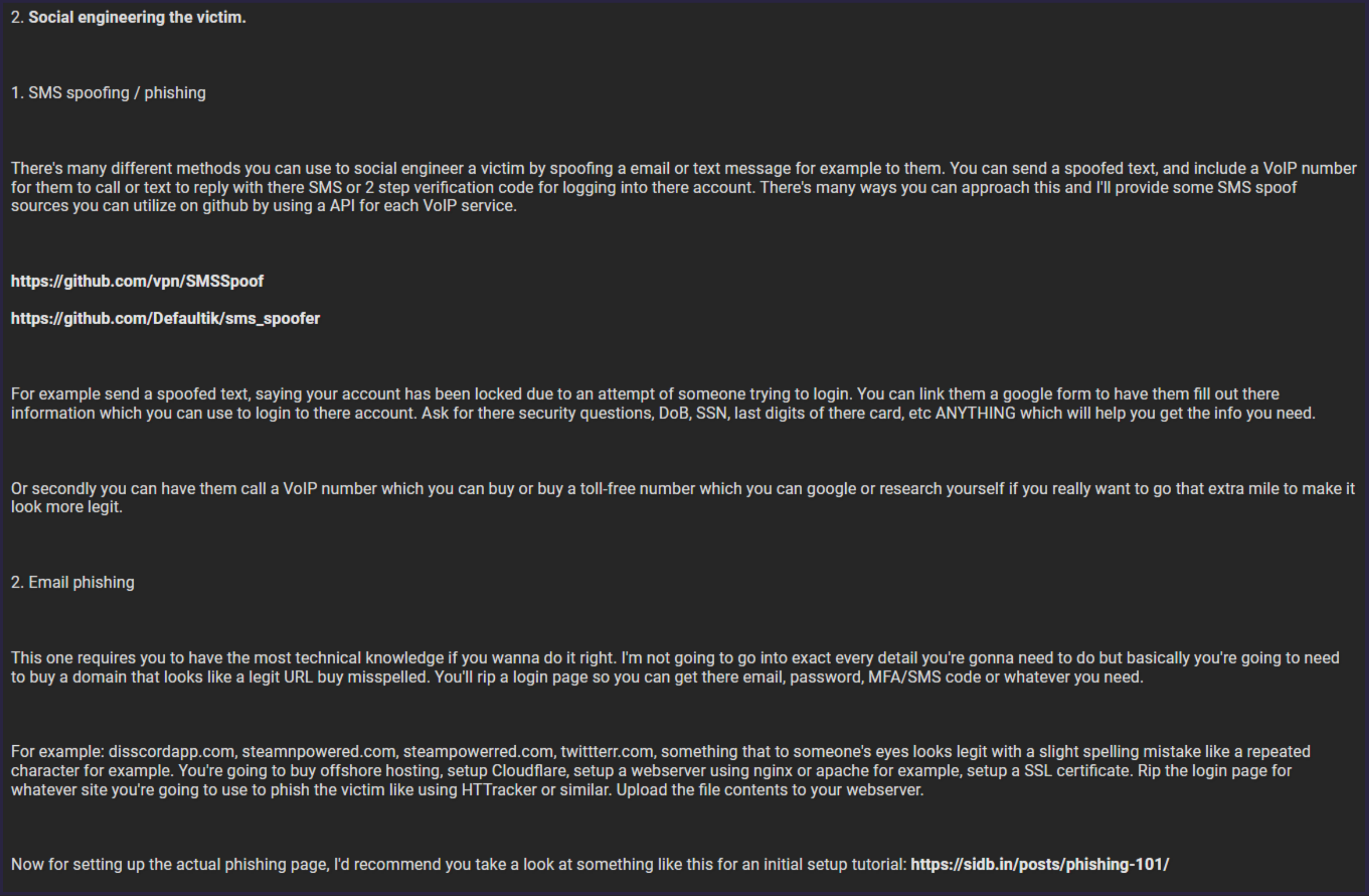
Some conversation examples:

1. I'm the father/mother "name" of the person you're doxing so say there first name and look up there families father/mother name by utilizing the links above. Say you're trying to recover the account and you don't have access to your email address or password anymore and need it changed, because your daughter/son is on vacation and you can't contact them now and you need to access your account urgently like for accessing the ISP web mail, or paying a bill online and not have your service shut down. You're going to want to do this when billing is closed if it's not 24/7 which usually works the best. You're going to want to try to be very nice to them, and ask how there day is going and be very friendly to them while acting professional so they might go out of there way to help you more. Say you value there time for helping you, and at the end of this you'll give them a good survey review to help there metrics. Keep in mind these people get paid shit money by the hour so they don't give a fuck if they make a mistake most of the time and want you off the phone as soon as possible with getting a good survey from you. If they don't buy it or refuse to give you any info hang up, log there name in a notepad so you know not to waste your time next time if you get them again. Give them some bogus email address you think you used. They're not going to be able to find it, then you're going to give them the actual customer info like there phone # / name / address to help them locate the account. At this point you're going to rely on hoping they break company policy or protocol and fuck up and they ask you what email address / password you would like it to be. Give them your email, and login to there account and you'll be able access any sensitive information they may have listed on there and also ask for a SIM replacement if you did this for a phone carrier.

2. Posing as a police detective. Keep in mind this shit is highly illegal so I don't recommend you do this on your home IP at all. This is going to take a lot of time and research and assume you know some basic UNIX command lines already and can setup a VM, fax server, and VoIP service. You're basically going to imposter as a detective and send a exigent circumstance form and fax it to a carrier / ISP. If there is a urgent matter like someone is talking about committing suicide online, detectives have the ability to get your information immediately like your name, address, IP logs, cellular coordinates.

Doxing and Personal Information OSINT

- → https://github.com/Defaultik/sms_spoofer
- → https://github.com/vpn/SMSSpoof



2. **Social engineering the victim.**

1. SMS spoofing / phishing

There's many different methods you can use to social engineer a victim by spoofing a email or text message for example to them. You can send a spoofed text, and include a VoIP number for them to call or text to reply with there SMS or 2 step verification code for logging into there account. There's many ways you can approach this and I'll provide some SMS spoof sources you can utilize on github by using a API for each VoIP service.

https://github.com/vpn/SMSSpoof

https://github.com/Defaultik/sms_spoofer

For example send a spoofed text, saying your account has been locked due to an attempt of someone trying to login. You can link them a google form to have them fill out there information which you can use to login to there account. Ask for there security questions, DoB, SSN, last digits of there card, etc ANYTHING which will help you get the info you need.

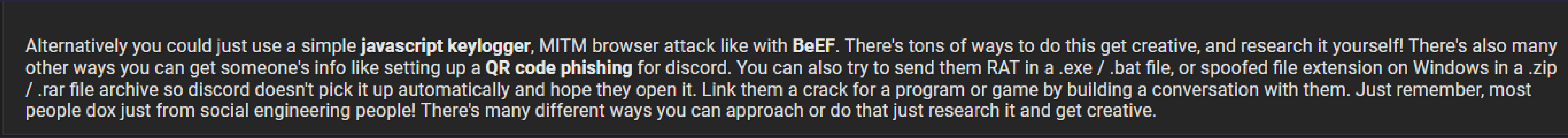
Or secondly you can have them call a VoIP number which you can buy or buy a toll-free number which you can google or research yourself if you really want to go that extra mile to make it look more legit.

2. Email phishing

This one requires you to have the most technical knowledge if you wanna do it right. I'm not going to go into exact every detail you're gonna need to do but basically you're going to need to buy a domain that looks like a legit URL buy misspelled. You'll rip a login page so you can get there email, password, MFA/SMS code or whatever you need.

For example: disscordapp.com, steamnpowered.com, steampowerred.com, twittterr.com, something that to someone's eyes looks legit with a slight spelling mistake like a repeated character for example. You're going to buy offshore hosting, setup Cloudflare, setup a webserver using nginx or apache for example, setup a SSL certificate. Rip the login page for whatever site you're going to use to phish the victim like using HTTracker or similar. Upload the file contents to your webserver.

Now for setting up the actual phishing page, I'd recommend you take a look at something like this for an initial setup tutorial: **https://sidb.in/posts/phishing-101/**



Alternatively you could just use a simple **javascript keylogger**, MITM browser attack like with **BeEF**. There's tons of ways to do this get creative, and research it yourself! There's also many other ways you can get someone's info like setting up a **QR code phishing** for discord. You can also try to send them RAT in a .exe / .bat file, or spoofed file extension on Windows in a .zip / .rar file archive so discord doesn't pick it up automatically and hope they open it. Link them a crack for a program or game by building a conversation with them. Just remember, most people dox just from social engineering people! There's many different ways you can approach or do that just research it and get creative.

Extra Resource – Prepare your Environment OSINT

- → https://www.maltego.com/blog/how-to-use-maltego-transforms-to-map-network-infrastructure-an-in-depth-guide/
- → https://www.maltego.com/blog/beginners-guide-to-maltego-setting-up-maltego-community-edition-ce/
- → https://www.maltego.com/blog/mapping-visual-disinformation-campaigns-with-maltego-and-tineye/
- → https://www.maltego.com/blog/data-at-your-fingertips-which-data-is-included-in-your-maltego-plan/
- → https://www.maltego.com/blog/maltego-data-integrations-got-bigger-and-better/
- → https://github.com/louisbarrett/ElasticMaltego
- → https://catalyst256.medium.com/maltego-metasearch-engines-e08e64b0912
- → https://www.tracelabs.org/initiatives/osint-vm

Extra Resource – Create Sock Puppet

- https://www.cybervie.com/blog/what-is-sock-puppets-in-osint-how-to-create-one/
- https://www.youtube.com/watch?v=Zf155HW5Qp0&ab_channel=TheCyberMentor
- https://www.youtube.com/watch?v=3KPO58wkw7M&ab_channel=TraceLabs
- https://hackernoon.com/how-to-make-sock-puppet-accounts-for-osint-in-2021-12r33gs
- https://ztrkouzhan.medium.com/the-mega-sock-puppets-tutorial-for-osint-af3bd29dd5fc
- https://www.maltego.com/blog/creating-sock-puppets-for-your-investigations/
- https://securityboulevard.com/2022/09/the-benefits-of-sock-puppets-in-open-source-intelligence-osint/

Extra Resource – Social Media Investigation

- https://github.com/OhShINT/ohshint.gitbook.io/blob/main/Lists_of_OSINT_Web_Resources/1-Complete-List-of-OSINT-Web-Resources.md#social-media-intelligence-socmint
- https://www.youtube.com/watch?v=sXn1GBgSpUQ&ab_channel=GaryRuddell
- https://www.youtube.com/watch?v=F6l2Bmh7Dq4&ab_channel=DavidBombal
- https://www.youtube.com/watch?v=uBynB50IiTw&ab_channel=TheCyberMentor
- https://www.youtube.com/watch?v=KdZvxxLsN3E&ab_channel=NetworkChuck
- https://www.youtube.com/watch?v=KTVHRdSFBJU&ab_channel=CodyBernardy
- https://www.youtube.com/watch?v=_mvwiFKB8L8&t=4s&ab_channel=SystemExploited
- https://www.youtube.com/watch?v=TUQ4AbUNmeI&ab_channel=CodyBernardy
- https://www.youtube.com/watch?v=NWyqSbnsvGU&ab_channel=NetworkChuck
- https://www.youtube.com/watch?v=ImWJgDQ-_ek&ab_channel=DavidBombal
- https://www.youtube.com/watch?v=2puBmXfi9Z0&ab_channel=Freethink
- https://www.youtube.com/watch?v=0TY2ajnmivA&ab_channel=Moss%C3%A9CyberSecurityInstitute

Extra Resource – Geolocation OSINT

- https://www.youtube.com/watch?v=CWMF8Bx_Lyk&ab_channel=Nattic
- https://www.youtube.com/watch?v=4Hkdxnqz1mg&ab_channel=OSINTDojo
- https://www.youtube.com/watch?v=IXacf6_R6HU&ab_channel=Elysium
- https://www.youtube.com/watch?v=OsY32K1s51Y
- https://www.youtube.com/watch?v=BjZso0nA2bE&list=PLtoC6Cd29__VS01w1pzjqmhGMh_LECsi7&ab_channel=OSINTDojo
- https://www.youtube.com/watch?v=SMxya-M6KhU&ab_channel=CodyBernardy

Extra Resource – Image Search

→ https://www.youtube.com/watch?v=9TW82ZELLx0&ab_channel=FourZeroThree

→ https://www.youtube.com/watch?v=0uoJKIyGpbo&ab_channel=SANSCyberDefense

→ https://www.youtube.com/watch?v=YkUnuouRhuE&ab_channel=GaryRuddell

→ https://www.skopenow.com/resource-center/image-based-osint-investigations-tips-techniques

→ https://github.com/jivoi/awesome-osint#-image-search

Extra Resource – Personal Information

- https://github.com/infomaven/personal-osint/blob/master/resources.md
- https://www.youtube.com/watch?v=F5DaPt4W5Oo&ab_channel=SANSCyberDefense
- https://haywoodhunt.ca/understanding-osint-and-the-power-of-public-records/
- https://www.skopenow.com/news/what-is-osint-how-to-conduct-investigations-with-open-source-data
- https://thatsthem.com/challenge?r=%2F
- https://nixintel.info/osint/12-osint-resources-for-e-mail-addresses/
- https://allabouttesting.org/quick-tutorial-email-osint/
- https://www.aware-online.com/en/osint-tools/email-address-tools/
- https://github.com/topics/email-osint
- https://www.youtube.com/watch?v=SSV9vDX9tfc&ab_channel=CyberSudo
- https://www.youtube.com/watch?v=WW6myutKBYk&ab_channel=NullByte
- https://hackcontrol.org/OSINT/Phone_numbers.html
- https://hakin9.org/uncovering-data-from-phone-numbers/
- https://github.com/spider863644/PhoneNumber-OSINT

Threat Reporting

- → https://www.schoolsafety.gov/threat-assessment-and-reporting
- → https://ociac.ca.gov/default.aspx?menuitemid=68&AspxAutoDetectCookieSupport=1
- → https://www.fbi.gov/file-repository/stats-services-publications-school-shooter-school-shooter/view
- → https://swiftshield.com/blogs/news/9-tips-for-what-to-do-in-a-school-shooting
- → https://www.nytimes.com/2018/02/16/us/survive-active-shooter.html
- → https://www.dhs.gov/xlibrary/assets/active_shooter_booklet.pdf
- → Other ways is to notify the local authorities as well, so they can analyze the case and exchange information with the neighboring country or state.

Awareness

→ https://www.youtube.com/watch?v=2zfiQAk927s&ab_channel=TheOhioStateUniversity-Administration%26Planning

→ https://www.youtube.com/watch?v=9qyD7vjVfLI&ab_channel=syracuse.com

→ https://www.youtube.com/watch?v=OP7I1n_8Lh4&ab_channel=TowsonUniversity

→ https://www.youtube.com/watch?v=A8syQeFtBKc&ab_channel=SandyHookPromise

→ https://www.youtube.com/watch?v=T254_J8Vcvw&ab_channel=SandyHookPromise

→ https://www.netflix.com/title/81349306 (if something happens I love you)