



BASIC OSINT: MINING PERSONAL DATA

SQUIDDY OF DC574

DC574のスクイッディ

PULPO EN ESPAÑOL

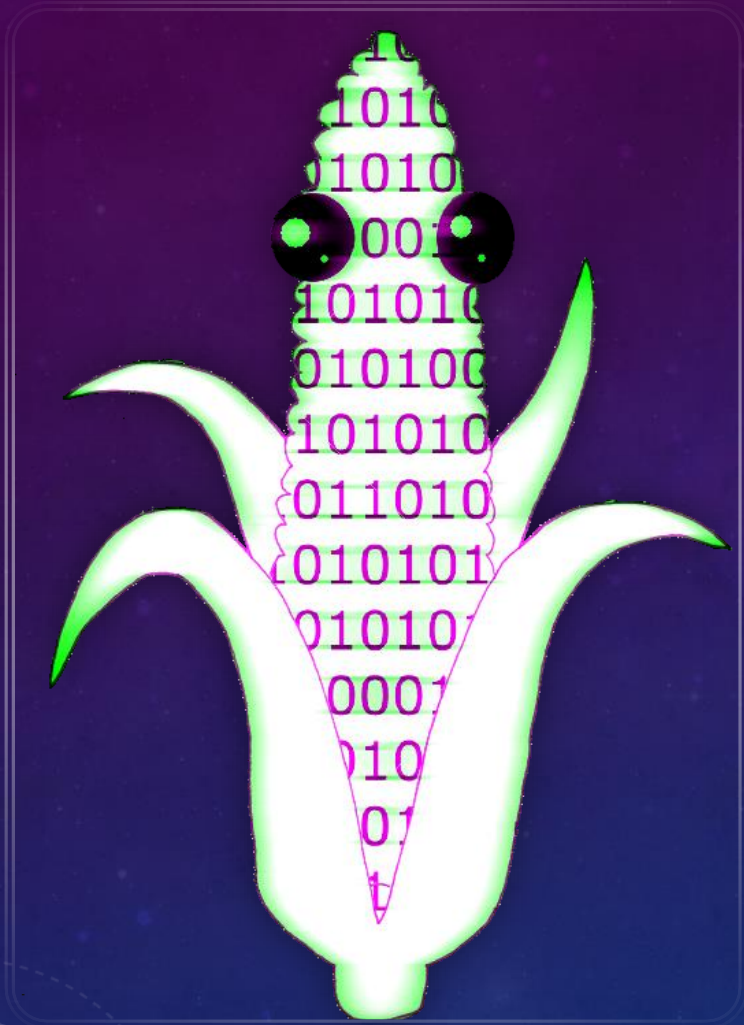
MASTODON: SQUIDDY@CLITERATI.CLUB
EMAIL: VMDEUS@PROTONMAIL.COM



WHO AM I?

“I’m nobody! Who are you? Are you nobody too?”

-Emily Dickenson



DC574 (SOUTH BEND, INDIANA)

- We are a newly-formed computer security group open to individuals interested in computer science and computer security, OSINT, lockpicking, social engineering, biohacking, and all things hackerish. Regardless of your current skill level or knowledge of these topics you are welcome to join and share topics that align with these interests and/or topics that you are passionate about.
- We are an officially registered student organization at **Indiana University**.
- <https://dc574.org/>
- @defcon574 on Twitter and Facebook
- **We have a code of conduct against sexual harassment, and discrimination based on sex, race, or sexual orientation.**

WHAT IS OSINT?

- OSINT or Open-source intelligence is data collected from publicly available sources to be used in an intelligence context. OSINT does not include non-public sources. OSINT is public, free, and legal.

THIS PRESENTATION: WHAT CAN I DO WITH THESE...?

- Names, initials
- An email address
- A Phone number
- Username
- Date of birth
- Social media profiles
- A physical address
- IP addresses
- License plate #
- Metadata and images

Including how to build an OSINT template, how to find deleted content, and followed up by tips and tricks, and resources.


BASIC OSINT TEMPLATE

- Your template will vary depending on the nature of your research. Building a useful template will require you to ask yourself these four important questions.
- What am I looking for?
- What is the main goal of my research?
- What or who is my target?
- How am I going to conduct my research?

EXAMPLE TEMPLATE

- Content is based on your four previously answered questions.
- This is what a basic template looks like for me.

I'll also keep a folder with pictures, and any public court records I can find. I may keep separate records on family members.

 OSINT Template.txt - Notepad

File Edit Format View Help

Full Name: Jane Doe

AKA: Julie Doe

Picture: [insert image here]

Sex: F

Date of Birth: 6/10/1993

Phone Number: 867-5309

Address: 1337 Doxology Ln, SmallTown Indiana 12345

Email: jdoe1993@gmail.com

Username: JDDoe, JanDoe

Place of Employment: AnyCorp

Education: Purdue University

Family Members: John Doe, Jennifer Doe

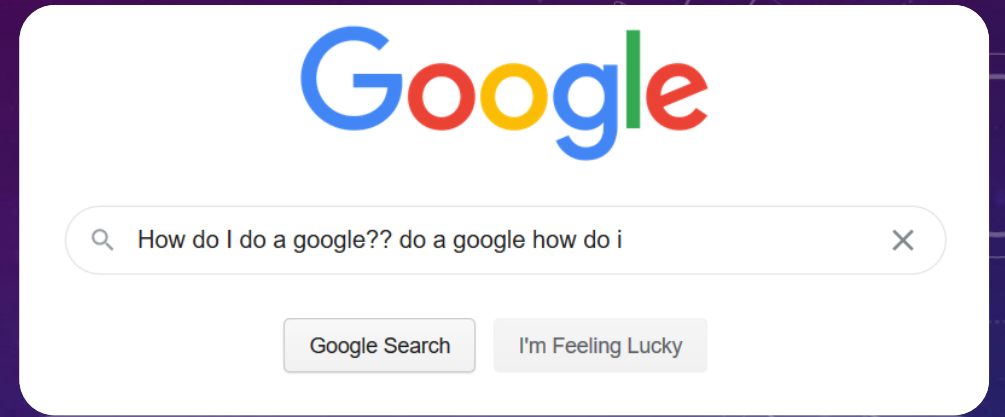
Known Acquaintances: Carmen Sandiego, Waldo

Social Media links:

Past addresses:

Past phone numbers:

GOOGLE DORKING



- We all know to search for information, but *do you know how to most effectively search for information?*

Google dorking is the **usage of advanced search operators** when searching Google. You can search for a specific string, remove search results that are from a certain site, remove specific strings, search only one particular site, or search for a particular document type, to name a few extremely useful examples.

EXAMPLES OF HOW A GOOGLE DORK QUERY WORKS

“Jane Doe” + “1993” insite:facebook.com

will return results from Facebook.com (as well as some other sites, apparently) containing the key terms Jane Doe and 1993.

“jdoe1993@gmail.com” filetype:CSV

A CSV file is a file in which each line of the file is a data record. This will return csv files containing this particular email entry.

“your homework question” insite:quizlet.com –Chegg

Will return that particular string in quizlet.com and **remove all search results** containing “Chegg.”

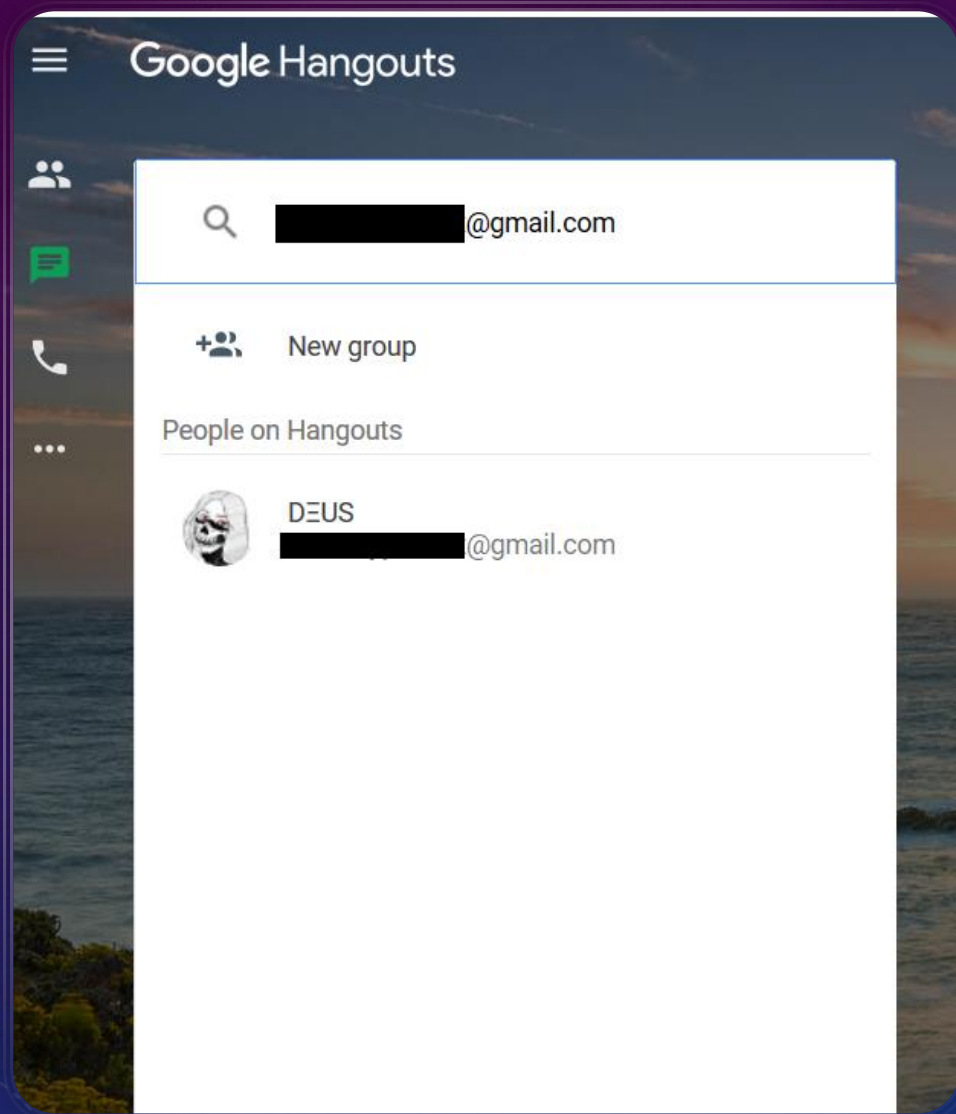
PEOPLE SEARCH SITES

- Keep in mind that much of this information, such as name, address, email address, username, and phone number, can often be searched for on people search sites. My favorite is fastpeoplesearch and truepeoplesearch. Fastpeoplesearch contains information that people sometimes remove off of truepeoplesearch, mainly because these people don't think to check fastpeoplesearch and remove their info, peoplesearchnow is another option.

I have also noticed that fastpeoplesearch doesn't seem to respond to PII removal requests. For better or for worse, this means the information that you seek will most likely be on there, too.

NAMES, INITIALS

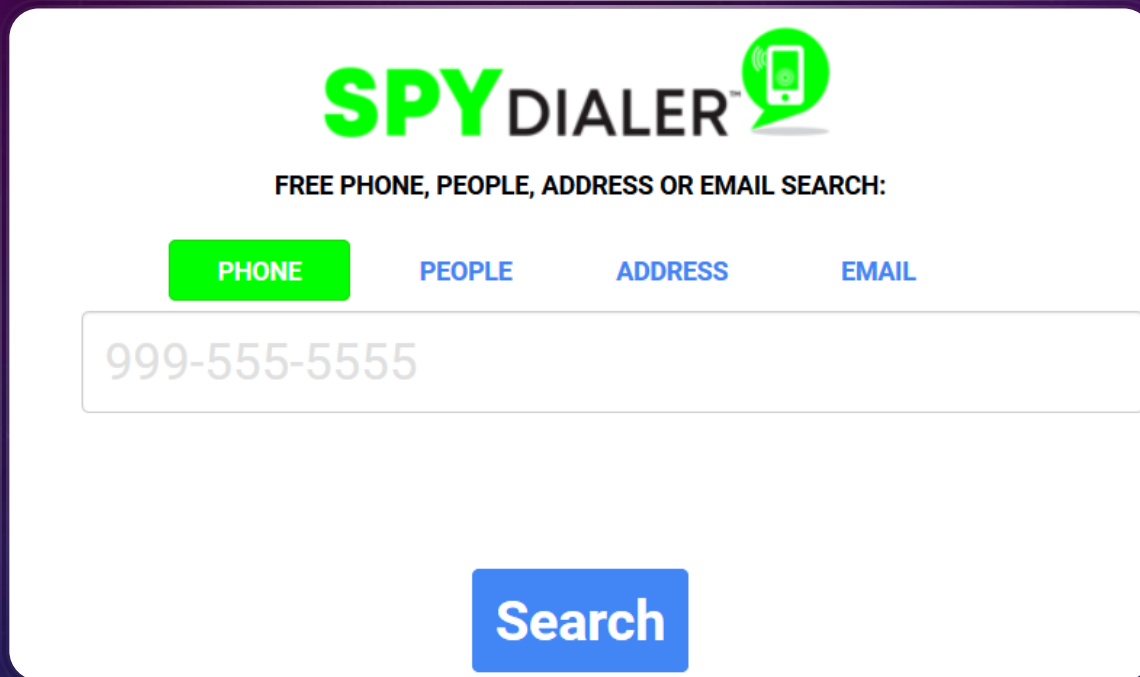
- If you have part of a name, for example first and last name Jane Doe, but require a middle name (for example, if you were generating a DL number with HighProgrammer), there are several ways to get this. The first thing I check is if someone is registered to vote in their county. Often, this registration information will contain a middle name (but not always), though this usually requires a date of birth to view.
- I will also utilize familysearch.org to search all records for a name in a specific state. This will often contain the middle name. People search sites like Fastpeoplesearch may at least give you a middle initial. Court records will often give you a complete name.



E-MAIL ADDRESSES

- The first thing that I do with an email is pop it into the “new conversation” Google Hangouts bar. This reveals the name associated with the account if there is one on record.
- Next, I check if the account has been leaked using **haveibeenpwned** and **dehashed.com** (my favorite resource). If possible, I collect any database that the email has been leaked in and search for the leaked information myself.
- If social media sites have a “search for your account via entering an email” option, I’ll check if it’s tied to any social media accounts.

PHONE NUMBERS



The screenshot shows the SPYDIALER website interface. At the top, the logo "SPYDIALER" is displayed in green, with a green speech bubble icon containing a white phone handset. Below the logo, the text "FREE PHONE, PEOPLE, ADDRESS OR EMAIL SEARCH:" is centered. There are four search category buttons: "PHONE" (highlighted in green), "PEOPLE", "ADDRESS", and "EMAIL" (all in blue). A search input field contains the text "999-555-5555". Below the input field is a blue "Search" button.

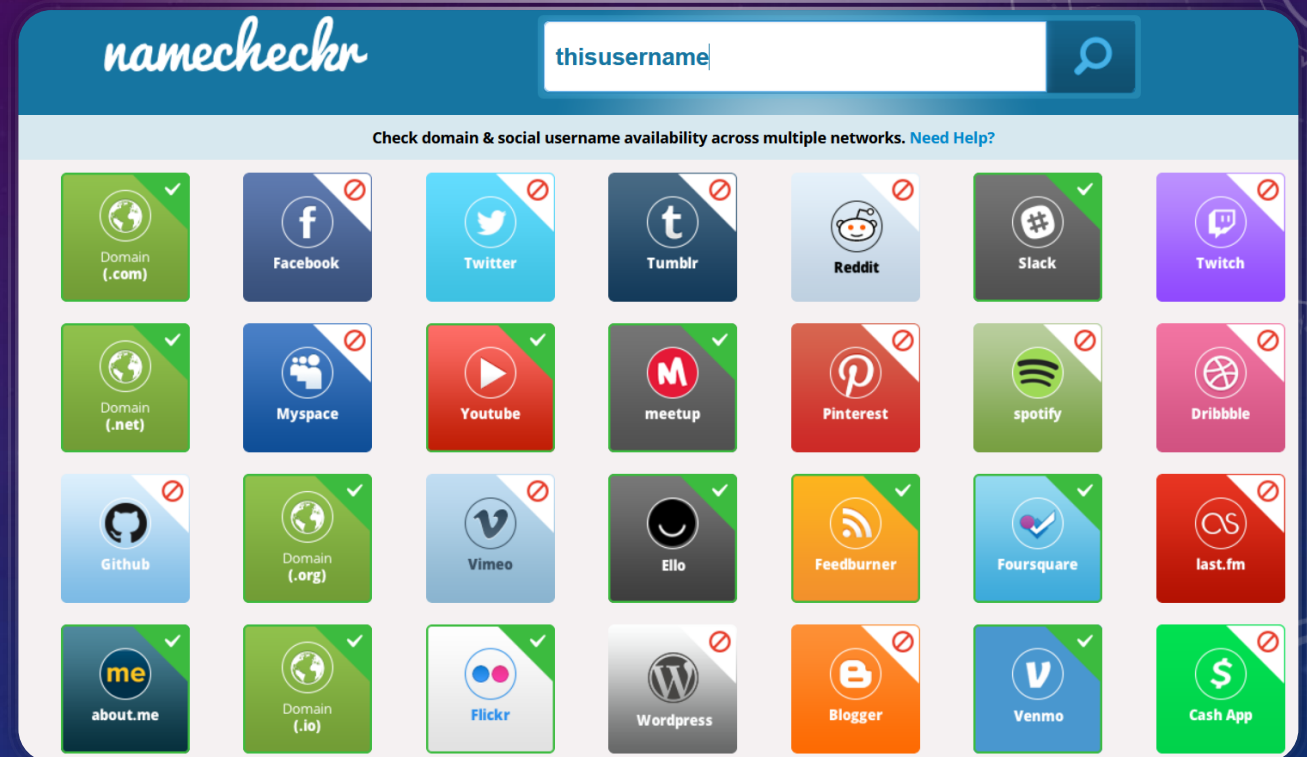
- My favorite site to use to see who a number belongs to is spydialer.com. Spydialer allows you see who owns a phone number, if it's a cell number or a landline, and lets you hear (and save an .mp3 of) a voicemail. Spydialer has other search options but I've found them to be fairly useless. If you want to find out who the mobile carrier is you can do so using callerIDtest (<https://calleridtest.com/>) it may also give you a name associated with the number.
- You can check if a number is a VOIP using phonevalidator: <https://www.phonevalidator.com/results.aspx>

USERNAMES

- There are several useful sites that will show you if a username is taken on a particular platform. Two of these sites are **knowem.com** and **namecheckr.com**. In addition, sites like **dehashed** work well for this too, as well as a simple google search for “username.”

Having only first and last initials and a username of an individual, I was able to find a full name by searching google (“CB” “username”) and from there complete a full dox, all because this person used their username with their name **once** on a forum back in 2007. I only knew their username because it was the same as their email handle.

An important reminder to combine the information you already have in order to find new information, and to never use the same username twice unless you don't mind people knowing who you are.



DATE OF BIRTH

- There are several ways to acquire a target's date of birth. The first thing I do is check **mylife.com**, as that often lists the full date of birth. If you can't find it there, it may also be listed on familysearch.com. People search sites like Truepeoplesearch or fastpeoplesearch may also have the year someone was born, or their age so you can estimate when someone was born. Public court records will often have full date of birth. Some people are into astrology and will share content relating to their "sun sign" which will at least give you a range. For example if someone cringe-posts "im a total gemini lol" or has a gemini emoji in their bio they are likely born between May 21st and June 21st. In my experience, I've found that women more frequently do this.
 - Stop it.

PUBLIC RECORDS, HUH?


- Public records are an important part of OSINT work. States have different resources for searching their public court records. Some make you pay (which I consider questionable, and would not be open sourced information imo), and some do not allow you to browse these records online, rather, you have to pay a visit to the county clerk. Some however, have their database online for you to freely search through. Mycase.in.gov <https://public.courts.in.gov/mycase/#/vw/Search> is one such example for the state of Indiana.
- Do they run a corporation/LLC? Oftentimes the address listed under “entity information” will be their home address, or it will be listed under “managers.” For the state of Illinois: https://www.cyberdriveillinois.com/departments/business_services/corp.html


SOCIAL MEDIA SITES: GENERAL TIP


- Collect the partially obscured information in the “recover account” option on social media sites like Facebook and Twitter. Use your OSINT skills to uncover the information.

Reset Your Password

How would you like to reset your password?

 Email me a link to reset my password
d*****y@hotmail.com


 Text me a code to reset my password
+*****39



Mark Wilson
Facebook user
[Not You?](#)

No longer have access to these? [Continue](#) [Cancel](#)

How do you want to reset your password?



DC574
@defcon574

We found the following information associated with your account.

Email a link to dc***@p*****.***

[Continue](#)

SOCIAL MEDIA SITES: TWITTER

- Gathering information from social media profiles can mean browsing through all the content on a profile individually, or using a tool to analyze the profile. It may also mean creating a fake profile, and a bit of social engineering to gather information on an otherwise private profile.
- A useful tool for Twitter is tinfoleak (<https://tinfoleak.com/>), which creates a free dossier of a Twitter user. Including the date the account was created, and the locations that they've tweeted from if they have geolocation enabled. Twitter also has an advanced search option (<https://twitter.com/search-advanced?lang=en>) example usage would be searching for all tweets from one particular user to another particular user and containing a specific keyword, etc. Using **Followrwonk** (<https://followerwonk.com/bio>) you can also search Twitter profiles or bios for a keyword. Helpful if you think a user may link to their other online content in their bio.

SOCIAL MEDIA SITES: TWITTER (2)

- If you want to export content from a Twitter profile, your best bet is probably **tweetbeaver**. There are 14 options you can utilize with tweetbeaver (<https://tweetbeaver.com/>), but I will list ones I find the most useful below:
- Convert name to ID: each twitter username as a corresponding user number. Users can change their username but the **user number itself can't be changed**. Useful for determining if an account that changes its name is the same account. Instagram accounts also have a user number that can't be changed.
- Check if two accounts follow each other, download a user's favorites, download a user's timeline, get a user's account data, download a user's followers list, find common followers of two accounts, and find common friends (followed users) of two accounts, find conversations between two users.
- Tweetbeaver also allows you to download data from multiple accounts at once. This data includes screen name, twitter ID, name, account creation date, location, URLs, time zones, if geolocation is enabled, language, if the account is verified, # of tweets, followers and following counts.

SOCIAL MEDIA SITES: TWITTER (3)

- If you want to see how many fake followers a user has there are a few services such as sparktoro that you can use. However, As mentioned in Open Source Intelligence Techniques 7th Edition, Michael Bazzell does not seem to think these services are reliable given that their results appear random.
- TweetTopic (<https://tweettopicexplorer.neoformix.com/>) creates a “word cloud” for a user account using the most recent 3200 tweets, and clicking on a result displays the tweet containing that word. I find this to be useful for analyzing a target; what topics they constantly post about and topics that they find the most interest in.
- TweetMapper (<https://keitharm.me/projects/tweet/>) is useful if your target does have location data in their recent tweets. It will show the tweet locations on a map. It seems to have some problems loading Google Maps at times.

SOCIAL MEDIA SITES: INSTAGRAM

- Your best bet for searching for an Instagram accounts and content from Instagram is via google dorking.

For example:

`inSite:Instagram.com squiddy dc574` (to locate a profile)

`InSite:Instagram.com "0xhegemon1c"` to view pages and posts that contain a target username

SOCIAL MEDIA SITES: INSTAGRAM (2)

- Searching likes and hashtags:
- If you click on the summary below the heart icon on an Instagram post (ex: “227 likes”) a new window will open with a list of accounts that liked the post.
- You can search hashtags on Instagram: <https://www.instagram.com/explore/tags/osint/>
- Acquiring a user ID number: right-click on a profile page and click “view source” and then search for “owner”:{“id”

SOCIAL MEDIA SITES: INSTAGRAM (3)

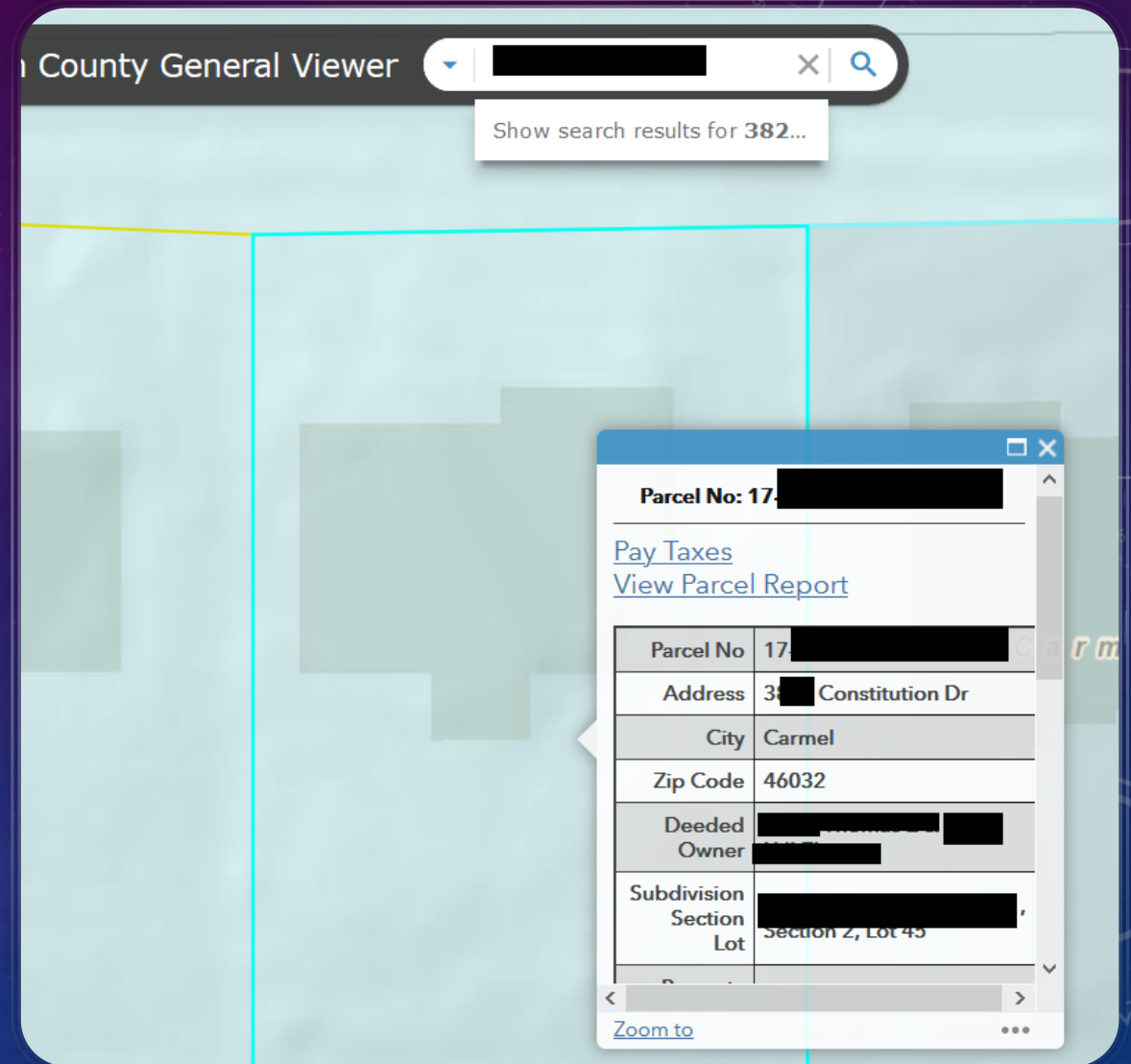
Instaloader and Instaloater are your best bet for tools:

Instaloader is a tool to download pictures (or videos) along with their captions and other metadata from Instagram. (<https://instaloader.github.io/>)

InstaLooter is a program that can download pictures and videos from any profile or hashtag on Instagram without any API token. You can even download pictures and videos from a private profile you are following, using your credentials to log in. (<https://instaloater.readthedocs.io/en/latest/>)

ADDRESSES

- I will usually utilize truepeoplesearch or fastpeoplesearch to acquire a home address, and then **Zillow** to view photos of the inside of the house. You can find a parcel number, which can be used to search for public records, such as a floor plan. You can also find out if a home has a security system installed. Some counties will have a map where you can search by parcel number, this will give you details of a specific address, such as deeded owner, Sq ft residential, number of floors and year built. It will also let you see the same information for neighboring houses.
- Here is one for Hamilton county in Indiana:
<https://gis1.hamiltoncounty.in.gov/GeneralViewer/>



LICENSE PLATE # AND DRIVERS LICENSE NUMBER:

- With a license plate number, you can acquire the Vehicle Identification Number (VIN) and see vehicle history <https://www.vehiclehistory.com/>
- You can use highprogrammer (<http://www.highprogrammer.com/cgi-bin/uniqueid>) to generate a DL number depending on state, if you have the following information: First name, middle initial, last name, gender, and date of birth.

Unique ID

[Other tools:](#)

Driver's License Calculator: Illinois

Calculate your Illinois Driver's License number from your information. [How it works.](#) [Reverse analyze an existing number.](#)

This algorithm is BETA grade. It is tested, but not yet thoroughly. Please [contact me](#) with details if you are receiving incorrect results.

First Name:

Middle Initial:

Last Name:

Gender: Female Male

Date of Birth:

Year:

Month:

Day:

SPEAKING OF CAR STUFF..

- If you want to find out what cars are registered at an address, use Progressive's get an auto quote feature!

Thanks Flo!

You can also **acquire a target's entire rental history from enterprise.com** if you have their DL number and last name. You can do the same on hertz.com and alamo.com.

Perfect timing. We've lowered rates in Indiana!

📍 8,593 people bought an Indiana auto policy in the last 30 days

Name & Birthdate

Mailing Address

P.O. Box/Military Address



We found these vehicles at your address

Want to add any of these to your quote? Check all that apply.

- 2017 Toyota Prius
- 2010 Honda CR-V

No, I'll add my own

You can still add other vehicles on the next screen

IP ADDRESS

- You can look-up an IP address using [iplocation.net](https://www.iplocation.net/ip-lookup) (<https://www.iplocation.net/ip-lookup>). This can be used to find out if an IP address belongs to a business provider that offers free internet like Starbucks, or tell us the internet service provider, or confirm if a target is associated with a VPN service. A Bing search for an IP address will tell you the websites hosted on that IP address

(ex of search: ip:54.xxx.xx.xx).

- If you want the IP address associated with a website, just ping it from your terminal or command prompt

ex: ping vm-deus.me

A Whois lookup will also provide useful information on a target IP address:

<https://whois.domaintools.com/>

Use an IP logger and some trickery to get a target's IP address: <https://iplogger.org/>

IP ADDRESS (2)

- My favorite site to use is **iknowwhatyoudownload** (<https://iknowwhatyoudownload.com/en/peer/>)

This one may be the **most invasive of all**, it monitors online torrents and discloses the files associated with any collected IP address. For example, *movies or images that someone has been downloading*.

- **View DNS Port Scan** (<https://viewdns.info/portscan/>) is an online port scanner that looks for common ports which may be open. An open port means that a service is running on the web server that may allow public connection. For example port 80 and port 443 are usually used for web pages. 😊
- **Shodan.io** is a search engine that lets you find specific devices (routers, servers, traffic cams, webcams) using a variety of filters.

METADATA

- There are many different types of metadata, for example, EXIF data (exchangeable image file format found within images). Metadata can be described as data embedded inside a document that can't be seen by looking at the document content. Such as author name, computer name, username of the computer or network, software version used, and information about the network the computer is connected to. A tool used to view one type of metadata is exiftool (<https://exiftool.org/>), but you can also view data using these sites:
 - Extractmetadata.com
 - Exifinfo.org
 - Get-metadata.com
 - Exif.regex.info/exif.cgi

REVERSE IMAGE SEARCH

You can search for images too! Some useful sites are

- images.google.com
- [Tineye.com](https://tineye.com)
- [Images.Yandex.com](https://images.yandex.com) (Yandex works well for cropped images compared to Google, Bing, or Tineye)

[Cameratrace.com/trace](https://cameratrace.com/trace) is designed to help victims of camera theft with locating their camera if it is being used by the thief online. If you obtain a serial number from an image using exif.regex.info/exif.cgi you can pop the serial number into Camera Trace and it will try to find any photos taken with the camera that have been uploaded online.

[Fotoforensics.com](https://fotoforensics.com) will show you if an image has been “touched” at all or manipulated.

archive.today
webpage capture

email blog ask me FAQ Donate

[Install Firefox extension](#)

My url is alive and I want to archive its content

Archive.today is a time capsule for web pages!
It takes a 'snapshot' of a webpage that will always be online even if the original page disappears.
It saves a text and a graphical copy of the page for better accuracy
and provides a short and reliable link to an unalterable record of any web page
including those from Web 2.0 sites:

- <http://archive.vn/2020.04.21/https://rt.live/>
- <http://archive.vn/2014.06.26/https://www.google.com/maps/...>

This can be useful if you want to take a 'snapshot' a page which could change soon: price list, job offer, real estate listing, drunk blog post, ...
Saved pages will have no active elements and no scripts, so they keep you safe as they cannot have any popups or malware!

I want to search the archive for saved snapshots

DELETED CONTENT

- Sometimes you may be looking for a web page or a specific tweet and find that the content has been deleted! Google Cache, and archives such as Archive.today and the Internet Archive's Wayback Machine can help you view this deleted content.

github.com › VM-Deus

VM-Deus (Squid) Cached ub

Popular repositories. [vm-deus.me](#). My Website. HTML. DC574. Official website for DC574. HTML. Practice-Code. For Python Practice. Python ...

RECOVER DELETED CONTENT FROM BROWSER CACHE

- You may be able to recover or rebuild a page from your browser cache if you have visited the site in Google Chrome. Enter this into chrome's address bar: chrome://cache

Note: I've read that chrome://cache and chrome://view-http-cache have been removed starting from Chrome 68, but that they still work in Chrome 65. I haven't checked this.

Find the page you want and save the link, this will return something like the image example here.

To convert this to html copy all the data and visit this URL to stick the data in the box provided:

<http://www.sensfulsolutions.com/2012/01/viewing-chrome-cache-easy-way.html>

```
http://www.bbc.co.uk/london/

HTTP/1.0 302 Moved Temporarily
Server: Apache
Content-Type: text/html; charset=iso-8859-1
Date: Mon, 08 Jul 2013 09:00:59 GMT
Location: http://www.bbc.co.uk/news/england/london/
Content-Length: 225
X-Cache: MISS from dslnlppxy01.emap-intl.net
X-Cache-Lookup: MISS from dslnlppxy01.emap-intl.net:3128
Via: 1.0 dslnlppxy01.emap-intl.net (squid/3.1.10)

00000000: 9a 01 00 00 03 88 00 00 dc 79 23 90 92 3f 2e 00 .....Y...7..
00000010: 0c ef 23 90 92 3f 2e 00 5f 01 00 00 45 54 54 50 .....?.....HTTP
00000020: 22 31 2e 30 20 33 30 32 20 4d 6f 76 63 64 20 54 /1.0 302 Moved T
00000030: 65 6d 70 6f 72 61 72 69 6c 79 00 53 65 72 76 65 mporarily.Serve
00000040: 72 3a 20 41 70 61 63 68 65 00 43 6f 6e 74 65 6e r: Apache.Conten
00000050: 74 2d 54 79 70 65 3a 20 74 65 78 74 2f 68 74 6d t-Type: text/htm
00000060: 6c 3b 20 63 68 61 72 73 65 74 3d 69 73 6f 2d 38 l; charset=iso-8
00000070: 38 35 39 2d 31 00 44 61 74 65 3a 20 4d 6f 6e 2c 859-1.Date: Mon,
00000080: 20 30 38 20 4a 75 6c 20 32 30 31 33 20 30 39 3a 08 Jul 2013 09:
00000090: 30 30 3a 35 39 20 47 4d 54 00 4c 6f 63 61 74 69 00:59 GMT.Locati
000000a0: 6f 6e 3a 20 68 74 74 70 3a 2f 2f 77 77 77 2e 62 on: http://www.b
000000b0: 62 63 2e 63 6f 2e 75 6b 2f 6e 65 77 73 2f 65 6a bc.co.uk/news/en
000000c0: 67 6c 61 6e 64 2f 6c 6f 6e 64 6f 6e 2f 00 43 6f gland/london/.Co
000000d0: 6e 74 65 6e 74 2d 4c 65 6e 67 74 65 3a 20 32 32 tent-Length: 22
000000e0: 35 00 58 2d 53 61 63 68 65 3a 20 4d 49 53 53 20 5.X-Cache: MISS
000000f0: 66 72 6f 6d 20 64 7a 6c 6a 31 70 70 78 79 30 31 from dslnlppxy01
00000100: 7a 65 6d 61 70 2d 69 6e 74 6c 6e 65 74 00 38 emap-intl.net Y
```


- Investigate their family members, especially older family members and their social media accounts.
- Set up Google Alerts for a specific keyterm to be notified when there is new content featuring that term.
- Use the *Google Hangouts trick*.
- Check **Facebook URLs**. People will change their FB name, but not think to change the URL and it often has their full real name.
- **DiscordChatExporter** trick to see hidden Discord channels. Using this tool on a Discord server will allow you to see channels that should otherwise be hidden to you, but not the content within these channels.
- Check **Google Cache** and archives such as the Internet archive's Wayback Machine for deleted content.

TIPS AND TRICKS



RESOURCES

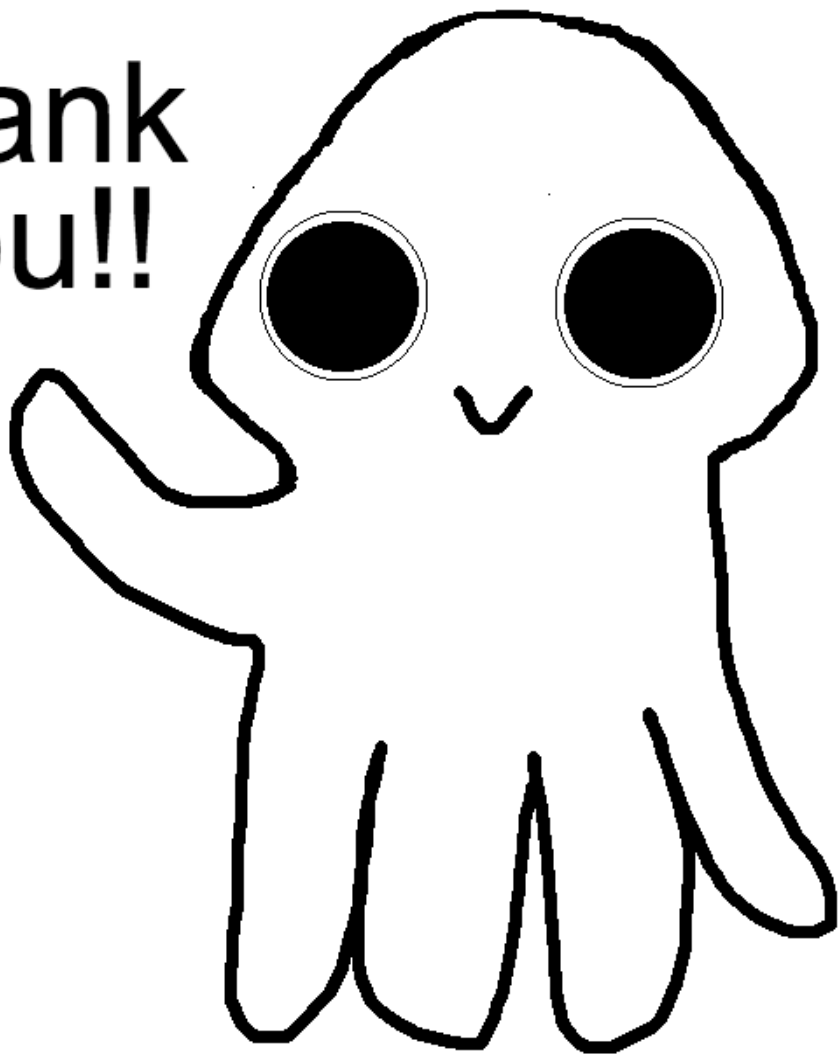
My favorite resources will always be Michael Bazzell's books and podcast.

- Open Source Intelligence Techniques 7th edition: <https://inteltechniques.com/book1.html>
- The Privacy, Security and OSINT show: <https://inteltechniques.com/podcast.html> also found on Spotify.
- IntelTechniques website: <https://inteltechniques.com/index.html>
- **Additional useful sites:**
- Check if an SSN is valid: <https://www.ssnvalidator.com/>
- Pre-built phishing pages: <https://zshadow.info/z-shadow-sign-in/>

SNOOP! BE SNEAKY! SAVE ALL THE THINGS!

- **Log errata and always keep receipts** (screenshots, copies of emails) etc.
- Archive everything with archive.today.
- **Do:** practice your social-engineering skills with fake accounts. Have some nerve, “friend” your target. You may be trash at it and ruin an investigation or you may gain some otherwise hidden knowledge.
- **Don’t:** ever brag. You’ll scare off a target. Unless you already have everything that you need on a target, and even then, it’s best to not make anyone suspicious unless you *really don’t care*. ***This is terrible OPSEC.***

Thank
you!!



DID YOU STICK AROUND?
THANK YOU!

- (<- That's a squidlet. Thank you for sticking around and watching my talk, please tell your friends about DC574!)