Supercharging People Investigations with the Right OSINT Strategy

RITU GILL (@OSINTTECHNIQUES)

OCTOBER 2023

Agenda

- OSINT Process
- Pivoting
- Search Engines
- Advanced Operators
- People Search Engines
- Social Media platforms
- Username enumerators
- Email and phone search
- Reverse image search
- Business search

# The OSINT Process

- Identify the objective
- Identify target data (email, username, etc.)
- Gather the data (research)
- Analyze the collected data (find what's relevant, identify patterns)
- Leverage/pivot with any new information
- Capture findings
- Generate a report, timeline, link chart, etc.

Identify Objective/Target Data

Research

Evaluate

Leverage

Capture

Report

Pivots on People

- Names, usernames, aliases
- Nationality, age
- Phone number, Emails
- Family info? Married? Parents? Children? Associates
- Where are they employed?
- Where did they go to school?
- What are their hobby's and interests?
- Communities they are a part of. Memberships?
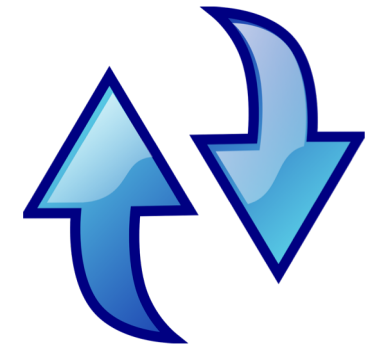
More pivot points!
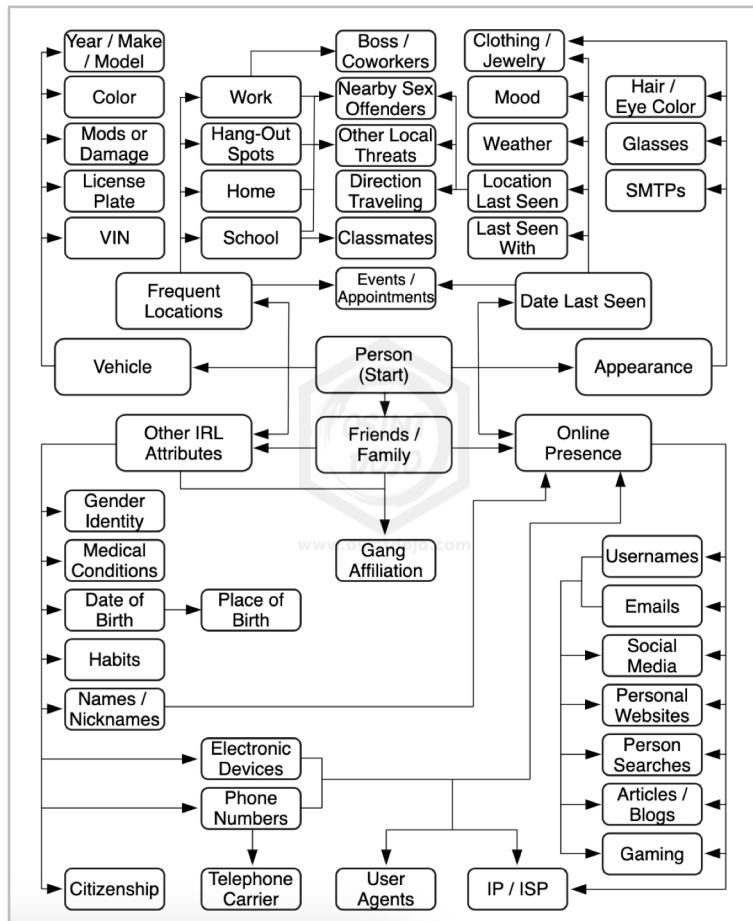
Sinwindie has created numerous OSINT diagrams called the "OSINT Attack Surface Diagrams".

osintdojo.com/diagrams/person

Search engines – google.com & bing.com

- Multiple search engines should always be used when conducting an OSINT research because there is no one search engine that indexes the entire web.

- Use at least two search engines when conduct OSINT research.
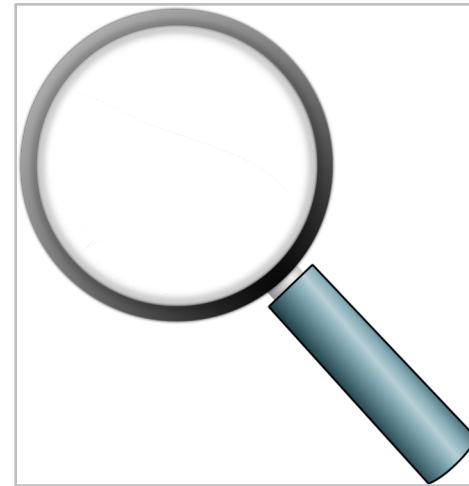
Country specific search engines - yandex.com & baidu.com

- If your target is from a part of the world that you are not familiar with and you may not know the commonly used search engines or other social media sites.

- Commonly used apps in a specific country, use data.ai which allows a user to filter by type of device, country, and category.

- Use osintcombine.com/world-social-media-platforms to assist with identifying search engines or social media sites that are country-specific.

Privacy focused search engines - search.brave.com & startpage.com

▶ There are also search engines that are considered privacy-focused such as search.brave.com and startpage.com

▶ Privacy-focused means that these search engines do not store a user's personal information or search data.

WHAT USERS LOOK LIKE

INSIDE OUR SERVERS
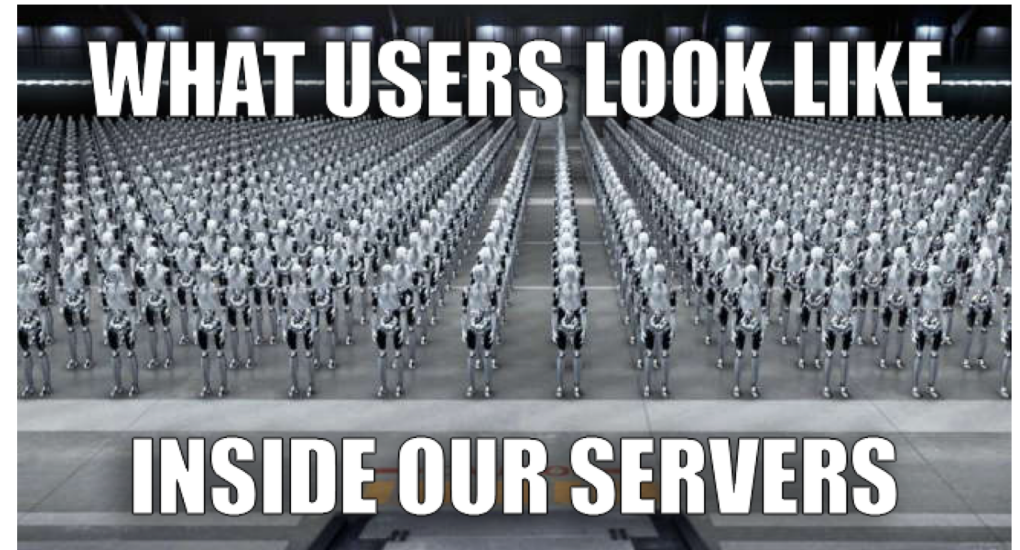
Quotations & Keywords

" " Quotations - exact search term i.e.

"ritu gill"

Use relevant keywords with a name:
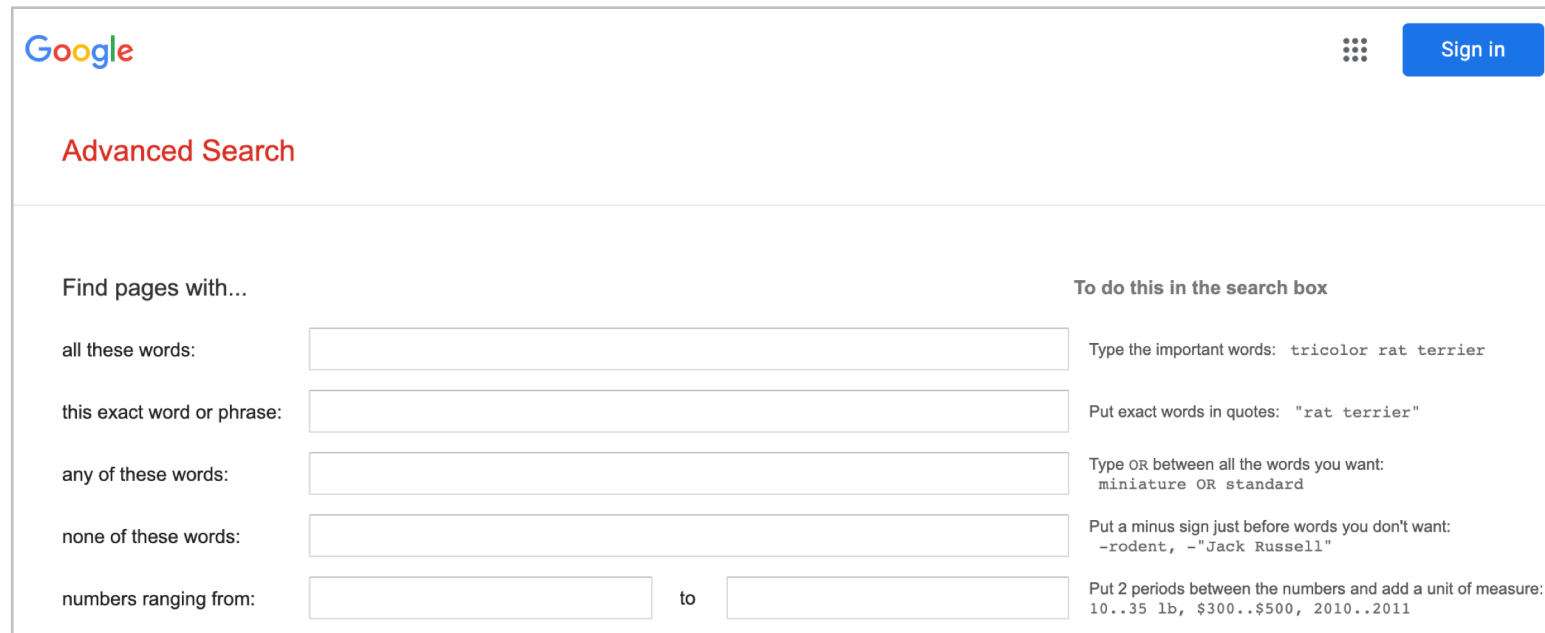
Ritu Gill "vancouver"

Ritu Gill "osint"

Ritu Gill "resume" OR "CV"

Advanced Google search

▶ Google's advanced search
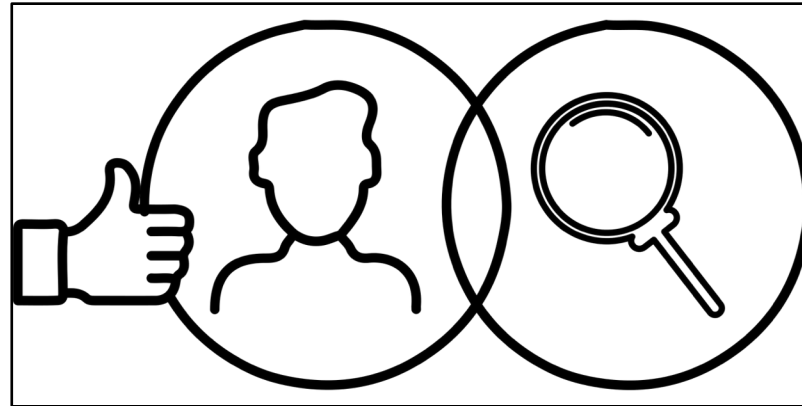
▶ https://www.google.ca/advanced_search

Search engine pro tips

- ▶ Use Incognito Mode

- ▶ Use multiple search engines

- ▶ Use a VPN and country-specific domains

- ▶ Refine your keywords

People search engines

- Thatsthem.com
- Familytreenow.com
- Truepeoplesearch.com

Familytreenow.com

FamilyTreeNow.com

NAME:	**Jason Smith**
BORN:	Aug 1961
AGE:	62
LIVES IN:	Corrales, NM
LIVED:	San Diego CA, Beverly Hills CA, **Seattle WA**, Des...
RELATED:	Amy K Mierzejewski, Christina B Mcpherson,...

first name

last name

city, state

Search Records

Current & Past Addresses

437 Alamos Rd, Corrales, NM 87048
Sandoval County
Current Address

1205 Pacific Hwy #2305, San Diego, CA 92101
San Diego County
(Jul 2012 - Sep 2013)

8530 Wilshire Blvd #200, Beverly Hills, CA 90211
Los Angeles County
(Aug 2006 - Feb 2013)

Social media Platforms

- Search popular social media such as Facebook, Instagram, LinkedIn, TikTok, etc.
- Look at primary targets but also secondary targets (family, close associates).
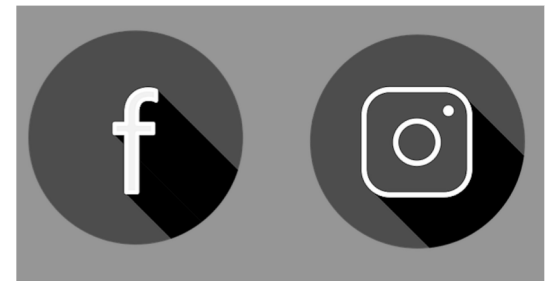
Facebook tip:

Search for a unique surname and filter by people and city to find your target.

Instagram tip:

Find out when an account was created by clicking on the 3 dots on a profile.

Use a third party viewer to watch stories – good opsec is important!

OPSEC Mistakes they make… that we can leverage

- ▶ Target's adding themselves as friends on social accounts
- ▶ Identifying family members
- ▶ General over sharing information in posts
- ▶ Leaving old social media profiles online

Usernames

- What's in a username?
- Usernames contain personal information

- Examples:
  - Jonsmith81 – name and year of birth?
  - Sea-doo88 – hobby and year of birth?
  - Pnw_604 – location and area code?
  - Laura.g.tattooist – name and work?

- Humans are creatures of habit and often use the same username across platforms
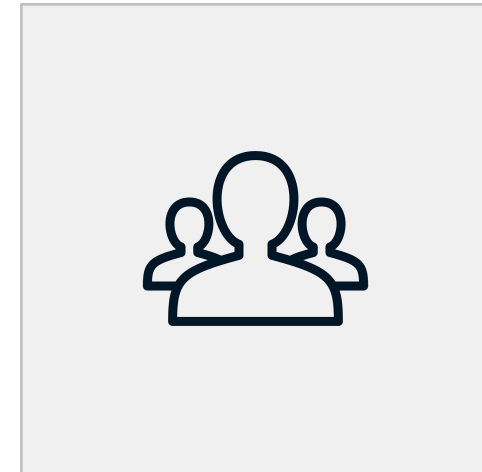
Username enumerator - whatsmyname.app

This tool allows you to enumerate usernames across many websites

- ▶ Find where a username is being used
- ▶ Must verify it's the same person.

https://tinder.com/@johnsmith

https://www.snapchat.com/add/johnsmith

Google search for usernames

- **INURL** advanced operator allows you to search within the URL of sites.

- Example:

  - Inurl:osinttechniques

Email Search – epieos.com

EPIEOS

Retrieve information linked to an email address, without notifying its user

- Search engine for emails
- Google reviews

Linda▬▬
10 contributions ›

Query	▬▬gmail.com
Photo	▬▬ 🔒Sign up
Name	▬▬
Id	1099▬▬
Last Update	▬▬ 🔒Sign up
Services	
Google Maps	https://www.google.com/maps/contrib/1▬▬

Papa Murphy's | Take 'N' Bake Pizza
2755 Commercial St SE, Salem, OR 97302, United ...

★★★★★ 3 months ago

Consistent high quality pizzas at this location.
Recommend them highly.

Phone search – truecaller.com

Search a phone number and see what other subscribers have labelled that number in their contacts.

🔊 **OPSEC WARNING**

Identified by *truecaller*

Justin ████████   J

❓ Is the name "Justin Lurch" correct?   👎   👍
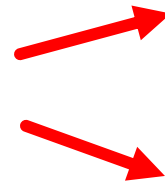
📞 FIXED LINE OR MOBILE - TELUS Communications, Inc. - BC
(604 ████████

📍 Address
Aldergrove, Bc, Canada · Local time 10:43

OPSEC – check your numbers

- Check your numbers on true caller
- If you find your information on true caller, you can request removal at this email address: https://www.truecaller.com/unlisting

Unlist Phone Number

Change my name

No, I want to unlist

Reverse Image search

▶ If you come across an image on the Internet, you can find out whether this image can be found on the internet elsewhere. This technique is called reverse image search.

▶ Enter a photo into a search engine and see if that photo or a similar photo exists somewhere else on the Internet.

Reverse image Sites:
- Google Images
- Yandex Images
- Bing Images
- TinEye

Browser Add-Ons/Extensions:
- Search by Image
- Fake news debunker by InVID & WeVerify

Tips for Reverse Image search

- ▶ Crop photo

- ▶ Blur out people or distracting objects

- ▶ Remove the background

- ▶ Flip the image

Remove image background - remove.bg

Business search - opencorporates.com

▶ Aggregates publicly available data from companies around the world.

Business & name search - whoxy.com

- Domain related searches live here.

- Search owner name, company name, and more.

- Select the drop down to filter the entity type.

Contact info

Ritu GILL @OSINTtechniques

osint.techniques@protonmail.com

OSINT TECHNIQUES

Follow

OSINT Techniques

@OSINTtechniques

Resources for Open Source Intelligence Investigations. Follow the Digital Bread Crumbs. #OSINT
linktr.ee/osint.techniqu...

osint.techniques@protonmail.com

Canada 🇨🇦   🔗 osinttechniques.com   🗓 Joined May 2016

889 Following   **53.2K** Followers

Questions?