

OSINT: Getting Started

Siobhan Kelleher , GCCC

Senior Security Analyst

OSINT: Getting Started

Topics

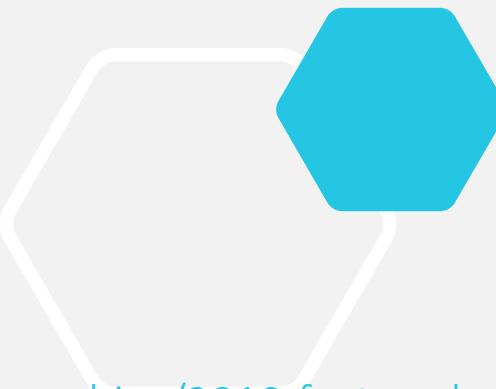
- What is OSINT
- Using OSINT
- Tools and Resources
- Staying Safe
- Using Your Skills for Good



OSINT: Getting Started

What is OSINT?

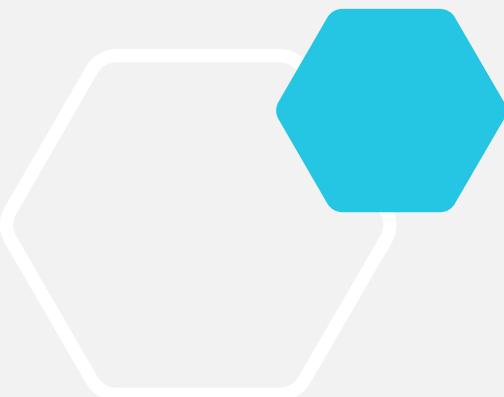
- The Internet
- Media (e.g. television, radio, newspapers, magazines)
- Professional Publications (journals, conferences, studies)
- Photos
- Geospatial Information (e.g. maps and commercial imagery products)
- ...and more



OSINT: Getting Started

How am I using OSINT?

- User Awareness Training
- Malicious Email
- Missing People
- Domestic Abuse



OSINT Landscape

V.1 February 2018

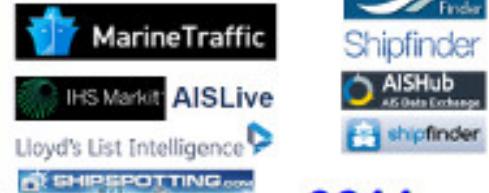
Open Source Intelligence (/OSINV – Open Source Investigation)

COVERTSHORES bellingcat
www.hisutton.com

Social Media Platforms



Maritime Movements



Aviation Movements



This landscape shows data sources (mostly platforms, tools or apps) that provide publicly available data which may be of use in OSINT. Some tools may charge for data access. It is intended to be extensive, but not exhaustive, and may be updated periodically.

http://www.hisutton.com/OSINT_Landscape.html

Sharing & Publishing



Blogging, Forums & other communities



Internet Search



Geospatial Data



Authors:
H I Sutton, (@CovertShores) Covert Shores and Jane's contributor;
Aliaume Leroy, (@naot) Bellingcat & BBC;
Tony Roper, (@topol_M883T), planespotter.net, Jane's contributor

OSINT: Getting Started

Tools & Resources

- Social Media
 - Tiktok, Twitter, Facebook, Snapchat, dating apps...
- Email
- Reverse Image Search
- Public Records
 - Address, arrest records, death certificates
- Other

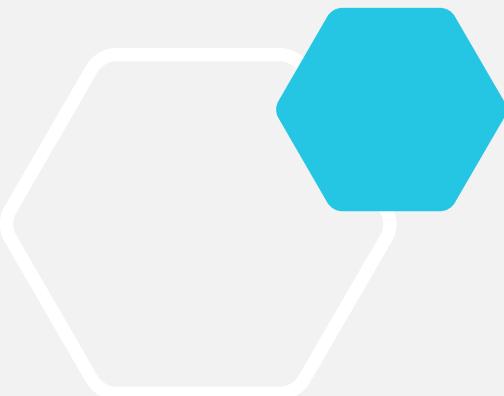


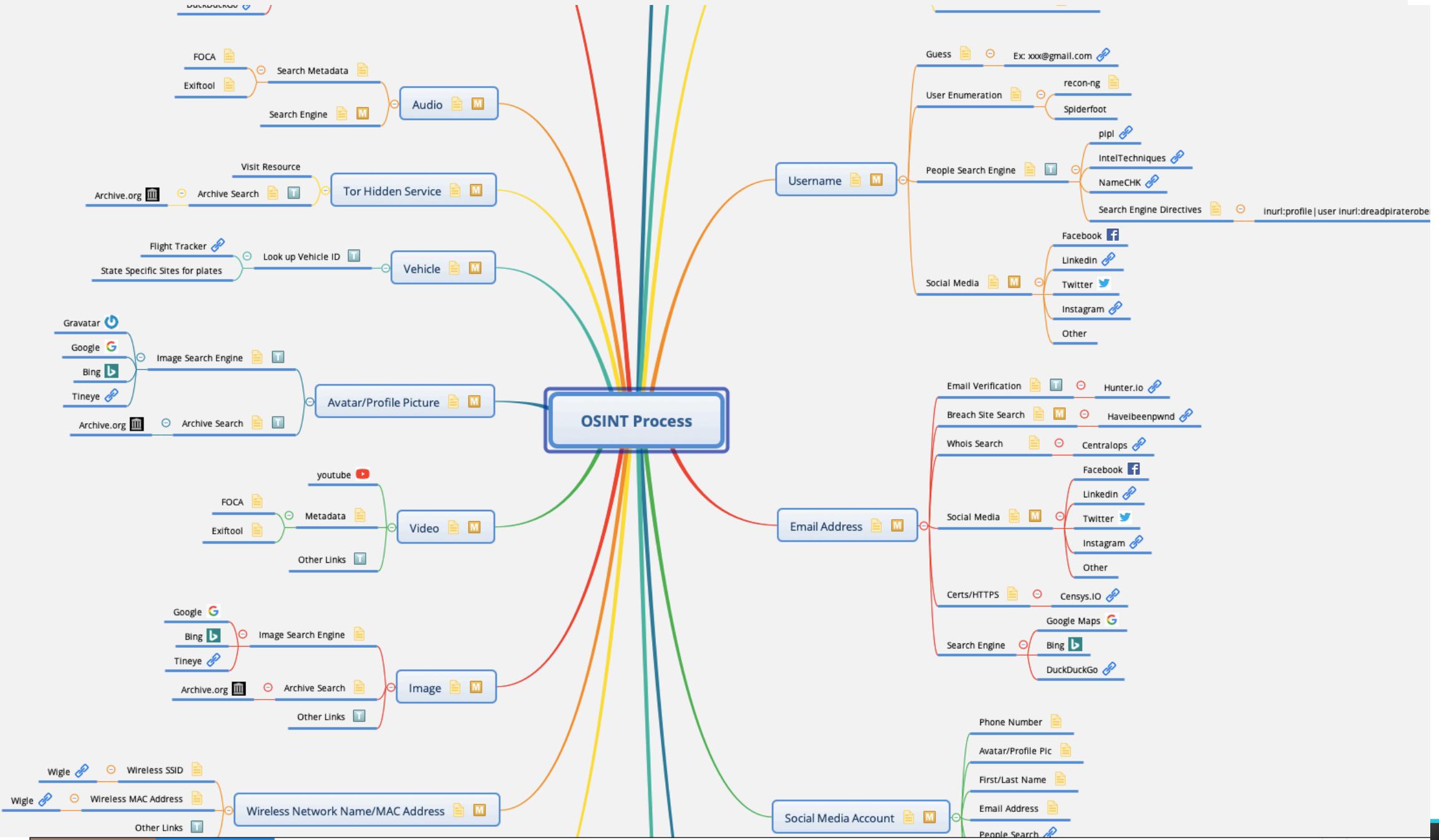
Image: <https://imgflip.com/i/4it4o0>

OSINT: Getting Started

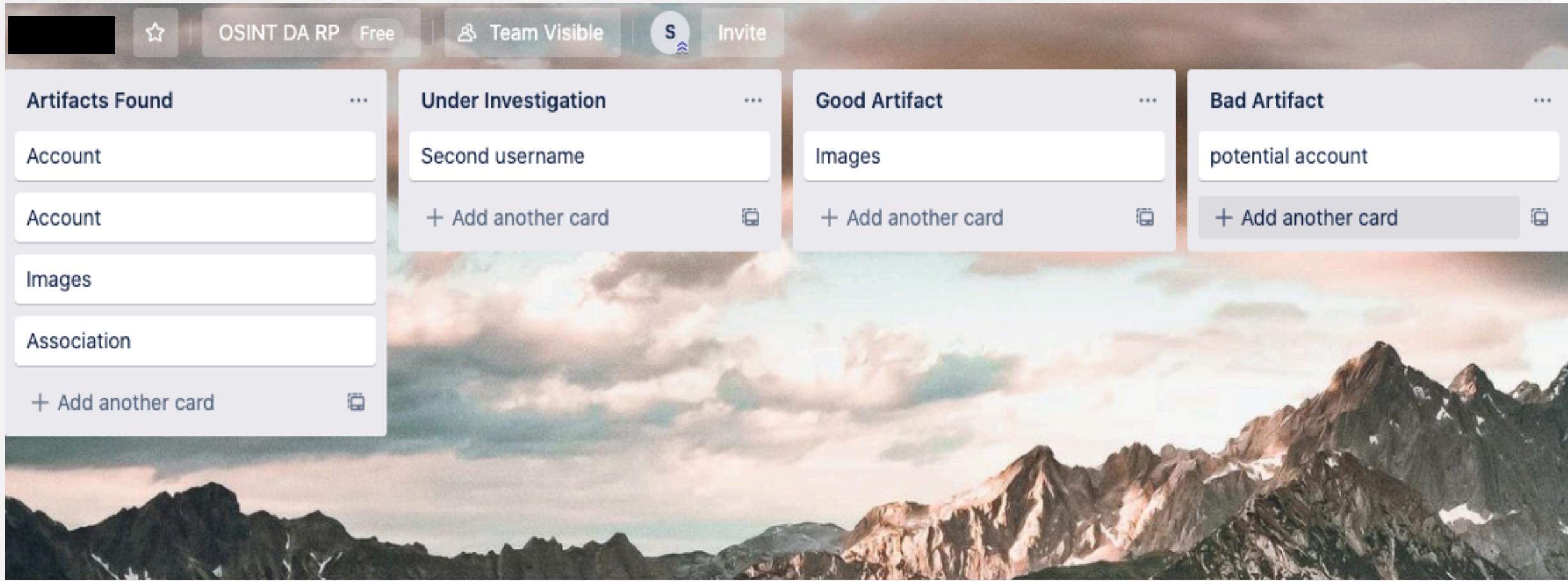
Tools and Resources

- Mind Mapping
- Excel
- Trello
- Session Buddy





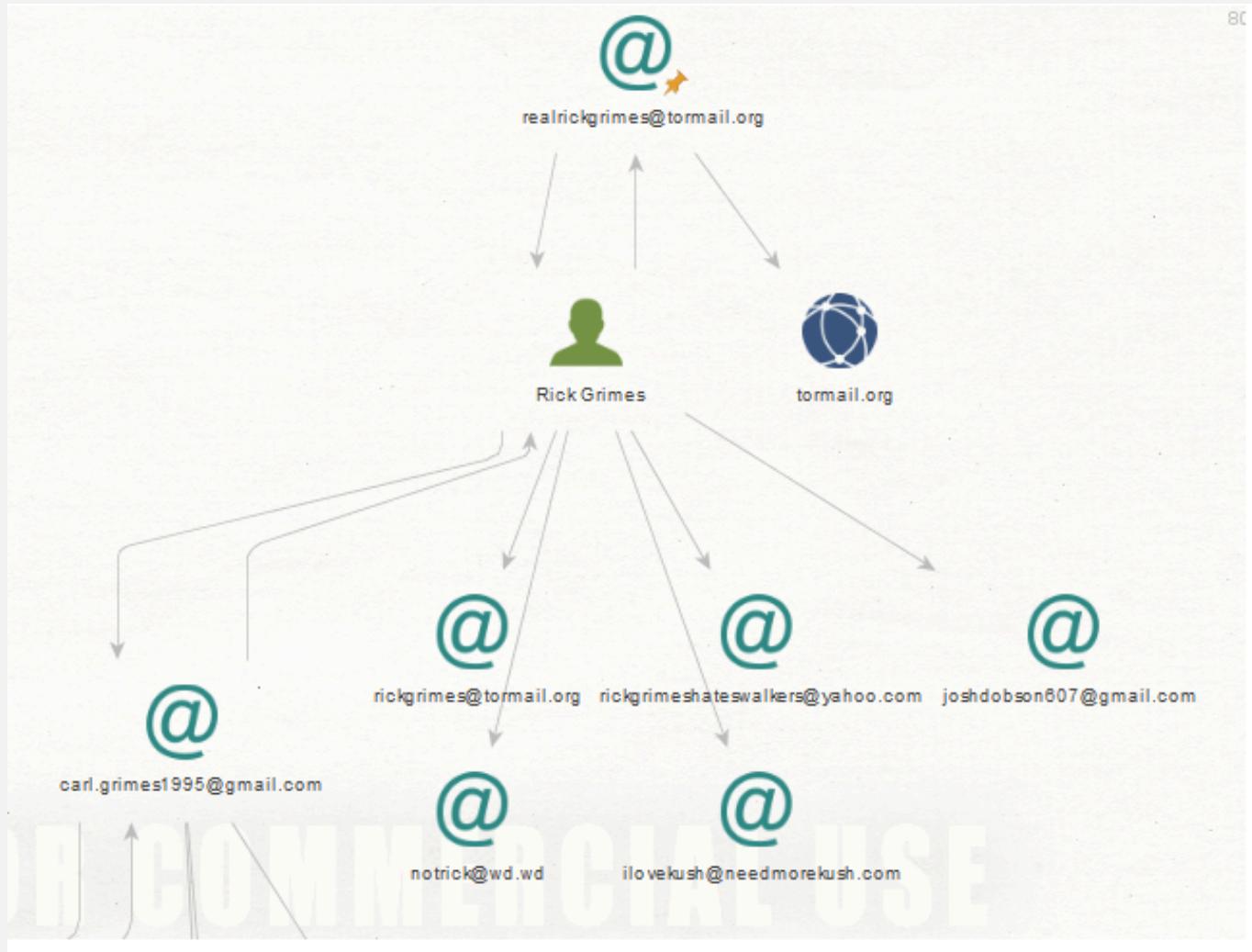
	A	B	C	D
1	OSINT: Jane Doe			
2	https://www.mass.gov/doc/person-missing-poster/download			
3	What	Link	Artifact	Notes
4	Phone number	www.theirnumber.com	8675309	found through this link,
5	Mother	www.mothers.com	Janet Doe	facebook page is open lists other relatives found through facebook search
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				
21				



OSINT: Getting Started

Tools and Resources

Maltego



site:twitter.com intext:"malware"



All News Images Books Videos More Settings Tools

About 726,000 results (0.32 seconds)

twitter.com › hashtag › malware ▾

#malware hashtag on Twitter

Cybersecurity tip: To best protect your business you'll need both #antivirus and anti-malware programmes. Antivirus software offers protection against classic ...

You visited this page on 8/10/20.

People also ask

Can you get malware from twitter? ▾

What are the 4 types of malware? ▾

How do I remove malware from my computer? ▾

Which is an example of a malware? ▾

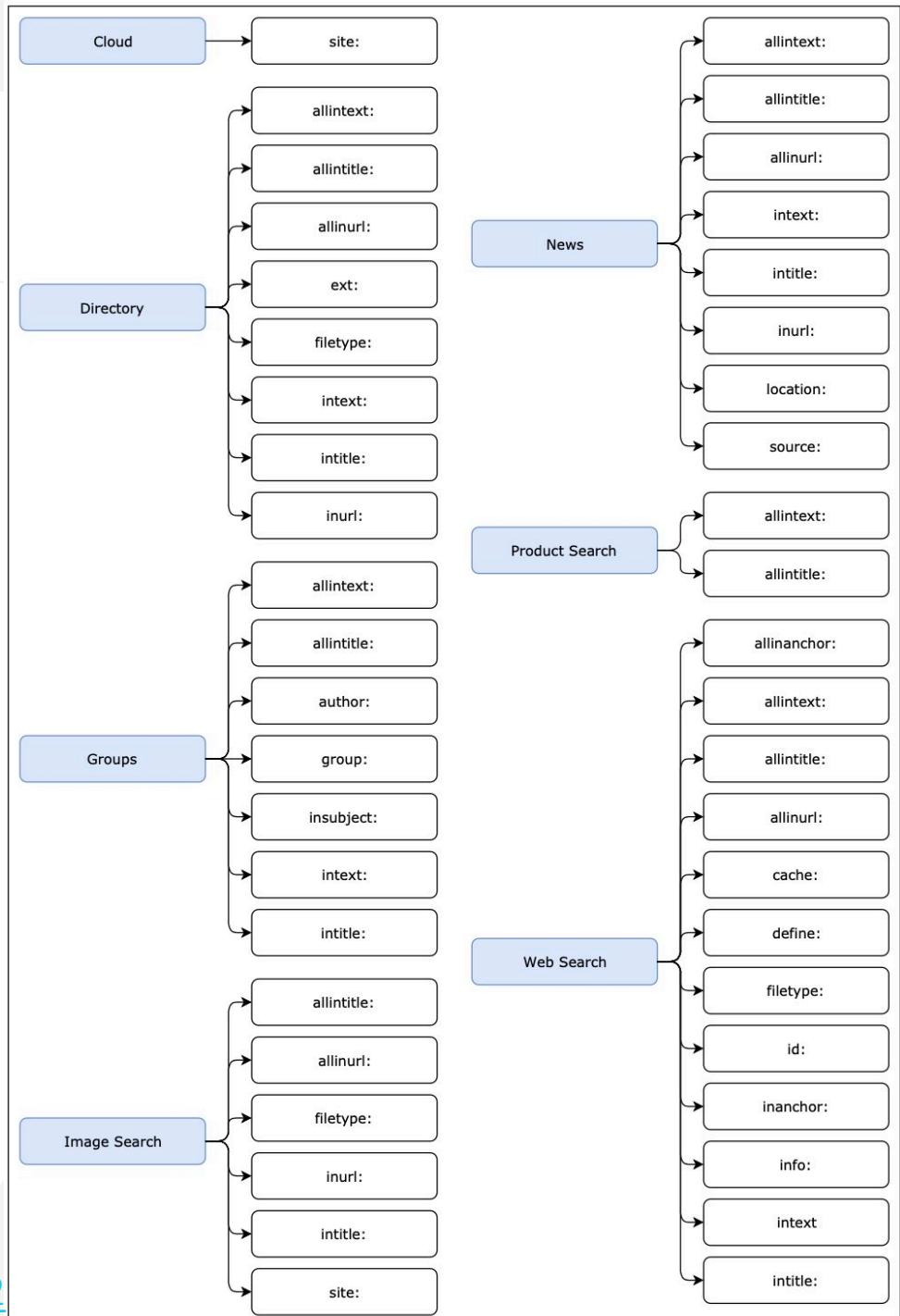
Feedback

twitter.com › web › status ▾

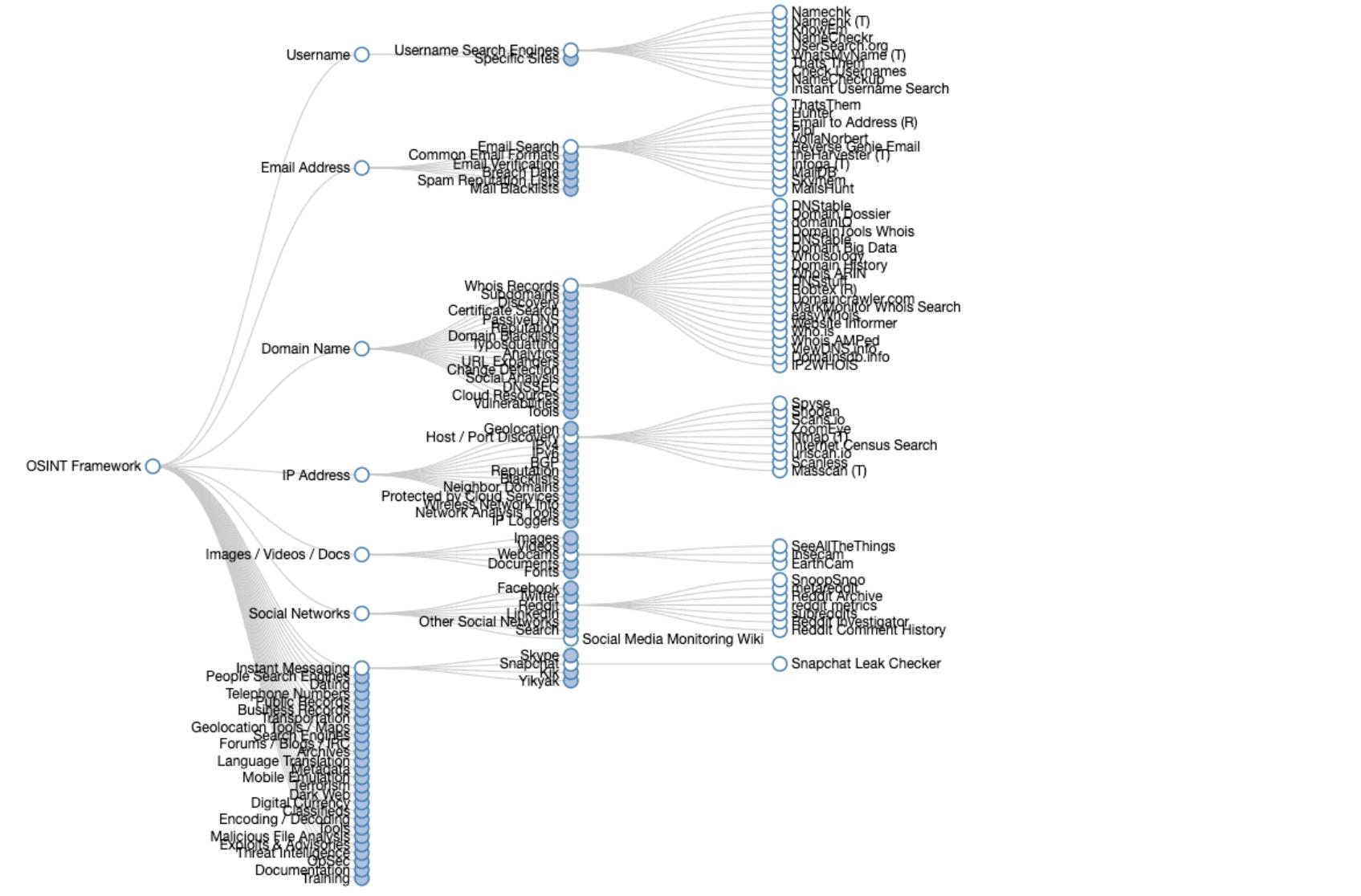
Brad on Twitter: "2020-08-10 - #Emotet infection with #Qakbot ...

1 hour ago - Brad · @malware_traffic. Sharing information on malicious network traffic and malware samples. 127.0.0.1.

Image: https://twitter.com/velstadt_com/status/1206902436469911552



OSINT Framework



[Signa](#) | [What](#) | [How](#) | [What](#) | [OSIN](#) | [What](#) | [INTel](#) | [Intel](#) | [Profil](#) | [What](#) | [How](#) | [OSIN](#) | [Priva](#) | [Forge](#) | [Kali L](#) | [pytho](#) | [\(87\)](#) | [Acco](#) | [Holge](#) | [GitHub](#) | [Goog](#) | [SANS](#) | [Black](#) | [GitHub](#) | [Edit](#) | [O](#) | [X](#) | [+](#)

osintframework.com

[Apps](#) [Training](#) [Tools](#) [Slack](#) [PSI-BC](#) [infosec wiki](#) [Tickets](#) [Security Issue Tra...](#) [GDrive](#) [Industry News](#) [BCHR](#) [Work | Trello](#)



Other Bookmarks

OSINT Framework

(T) - Indicates a link to a tool that must be installed and run locally
(D) - Google Dork, for more information: [Google Hacking](#)
(R) - Requires registration
(M) - Indicates a URL that contains the search term and the URL itself must be edited manually

OSINT Framework



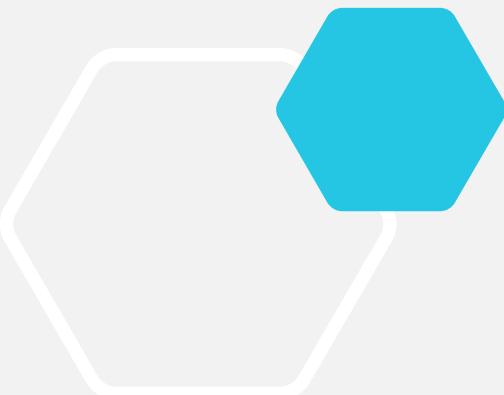
Notes

OSINT framework focused on gathering information from free tools or resources. The intention is to help people find free OSINT resources. Some of the sites included might require registration or offer more data for \$\$\$, but you should be able to get at least a portion of the available information for no

OSINT: Getting Started

Tools and Resources

- SpiderFoot
 - Free hobby edition- web based
 - Free open source downloadable



<https://www.spiderfoot.net/>

Scans

		Name/Target search...	Status: All ▾							
<input type="checkbox"/>	Name	Target	Started	Finished	User	Status	Elements	Correlations	Action	
<input type="checkbox"/>	demo	bumpinthenite@protonmail.com	⌚ 2020-10-16 19:44:24	2020-10-16 19:44:56	bumpinthenit...	✓ FINISHED	13	-	trash copy refresh	

Total Scans: 1

OSINT: Getting Started

Tools and Resources

Scylla Project

scylla.sh/search?q=name%3A*.edu

ning Tools Slack PSI-BC infosec wiki Tickets Security Issue Tra... GDrive Industry News BCHR Work | Trello

a, please report bugs to [the scylla github repo](#)

name: *.edu				
domain	email	password	ip	name
000webhost.com	giaogienit1@gmail.com		117.6.3.147	trongbang.edu
000webhost.com	ewagner@gm.slc.edu		201.253.213.228	ewagner@gm.slc.edu
000webhost.com	alhamd.edu@gmail.com		41.233.55.181	alhamd.edu
000webhost.com	cle12@wellesley.edu		98.169.59.134	cle12@wellesley.edu
000webhost.com	brandon@ucdavis.edu		24.7.168.71	Brandon@ucdavis.edu
000webhost.com	physeekshop@gmail.com		118.138.161.16	jenny.keating@monash.edu
000webhost.com	dbittinger@dccc.edu		144.162.48.139	dbittinger@dccc.edu
000webhost.com	xfh174@my.utsa.edu		70.123.242.111	xfh174@my.utsa.edu
000webhost.com	lfield@bu.edu		73.218.234.191	lfield@bu.edu
000webhost.com	efrain.pacheco@upr.edu		136.145.209.2	efrain.pacheco@upr.edu
000webhost.com	ssutton1@live.maryville.edu		97.91.223.50	ssutton1@live.maryville.edu
000webhost.com	aigat001@odu.edu		184.2.73.130	aigat001@odu.edu
000webhost.com	cstover@rtc.edu		98.247.92.185	cstover@rtc.edu
000webhost.com	travis.lanner@yellowjackets.hhsu.edu		198.177.154.139	travis.lanner@yellowjackets.hhsu.edu

<https://scylla.sh/>

https://twitter.com/_hyp3ri0n

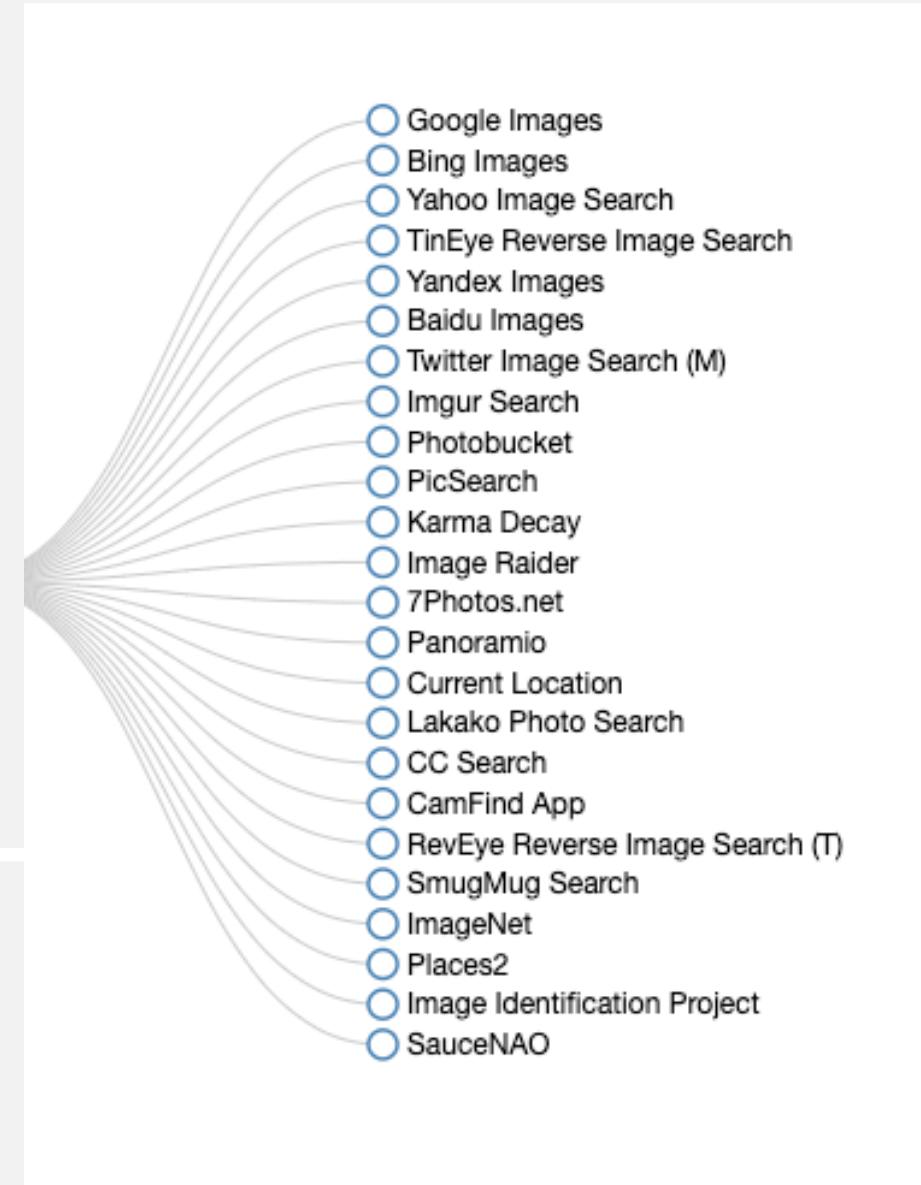
OSINT: Getting Started

Tools and Resources

- Reverse Image Search
 - Find other accounts

<https://tineye.com/>

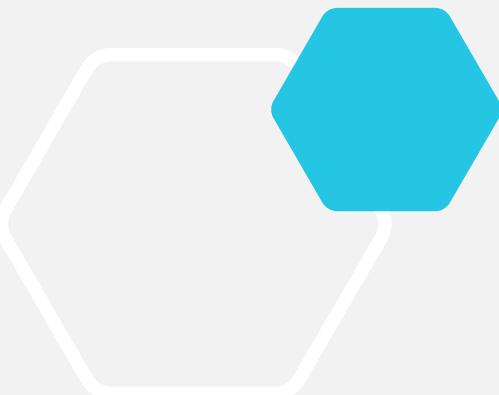
<https://images.google.com/>



OSINT: Getting Started

Tools and Resources

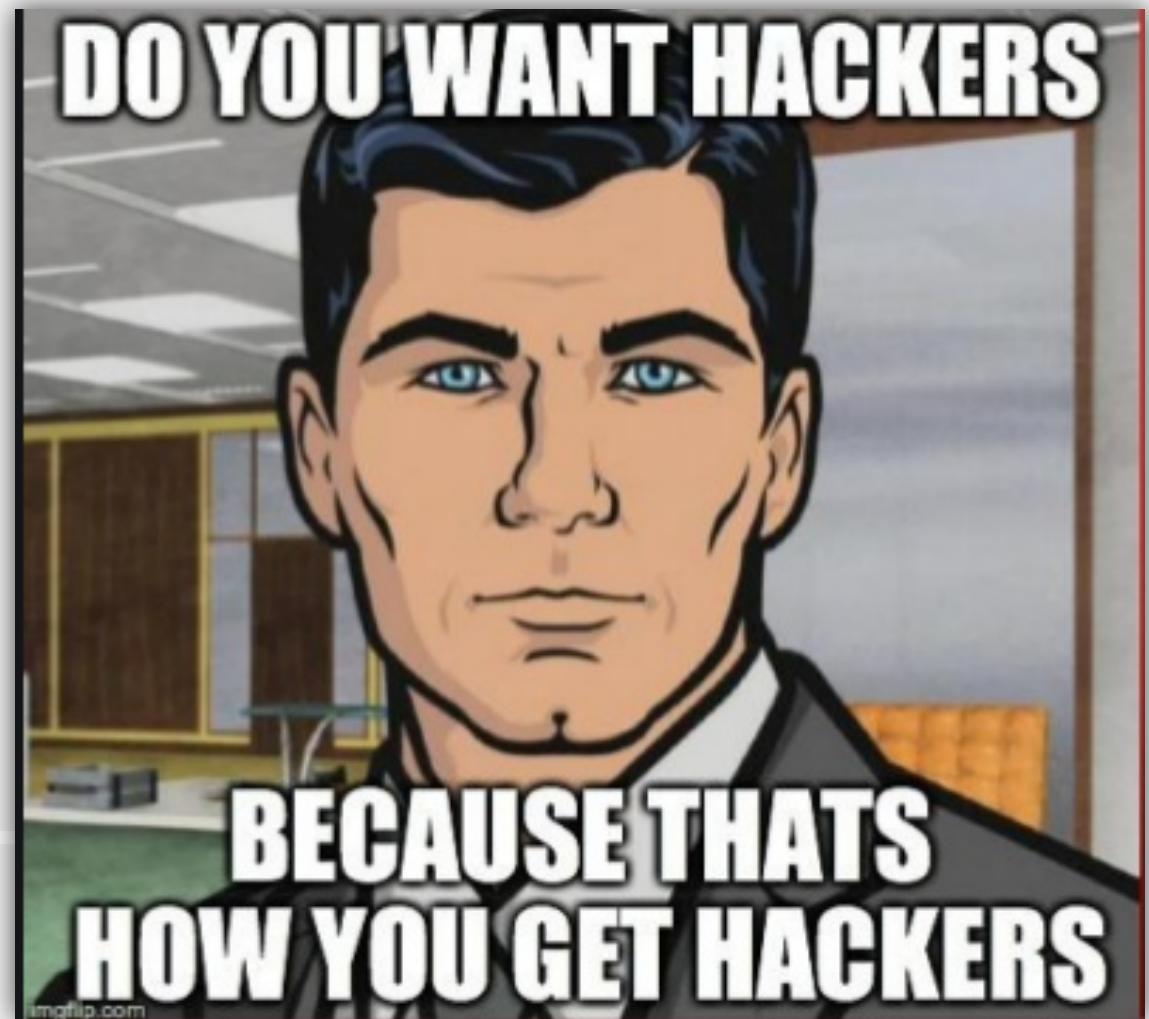
- Social Media Search
 - Simple is sometimes better



OSINT: Getting Started

Staying Safe

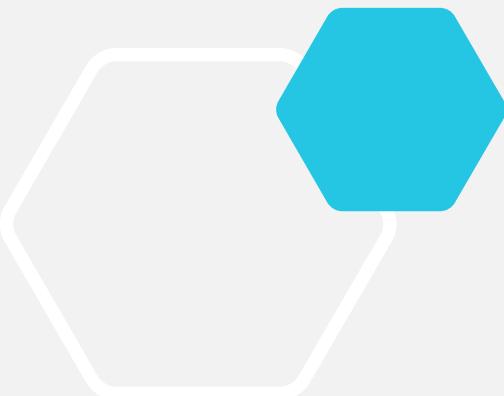
- Why it's important!
 - Protect yourself
 - Isolate the target protect the investigation



OSINT: Getting Started

Staying Safe

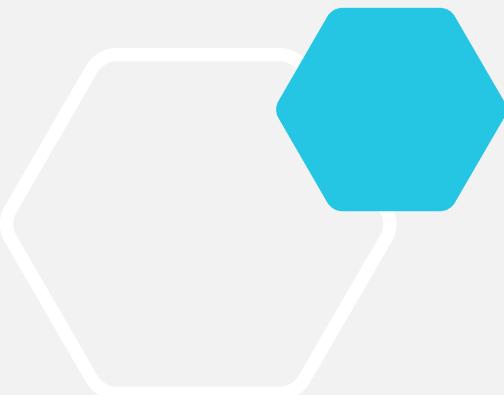
- Passive recon or “no touch”:
 - No interaction with target
 - Not invasive
 - No illegal hacking



OSINT: Getting Started

Staying Safe

- Use a VM (virtual machine)
 - Burn it when you are done
- Dedicated machine (if able)
- VPN (virtual private network)
 - Proton
 - Brave
 - Nord
 - PrivateInternetAccess (PIA)

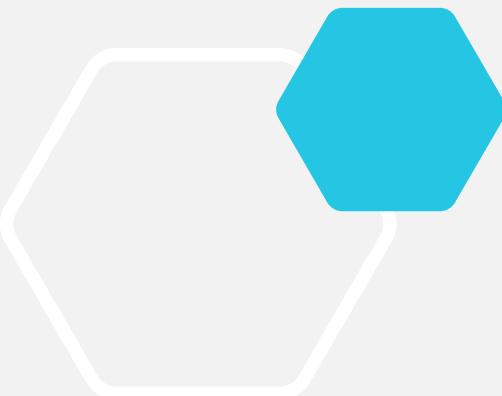


<https://www.privacytools.io/>

OSINT: Getting Started

Staying Safe

- Sock Puppet Accounts
 - Fake account used for recon
 - Never use your personal social media accounts for OSINT investigations
 - Insulate your personal information



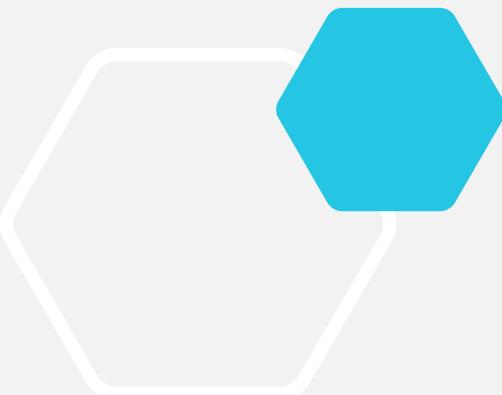
OSINT: Getting Started

Staying Safe

- Sock Puppet Accounts
 - Burner Phone
 - Smart Proxy
 - Wi-Fi
 - Fake Identity Generators

<https://www.thispersondoesnotexist.com/>

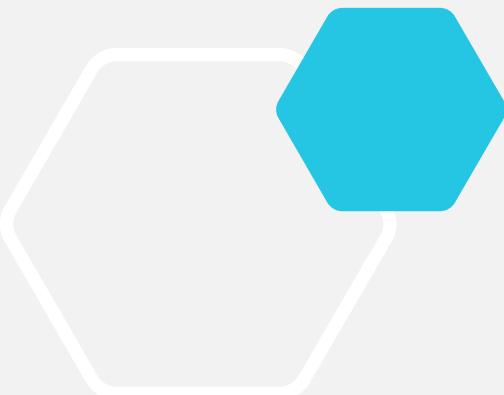
<https://www.fakenamegenerator.com/>



OSINT: Getting Started

Staying Safe

- Sock Puppet Accounts
 - Keep your socks separate
 - Keep them organized
 - Check on them regularly



OSINT: Getting Started

Using Your Skills for Good

- TraceLabs
 - CTF- prizes and glory!
 - Monthly collaborative cases

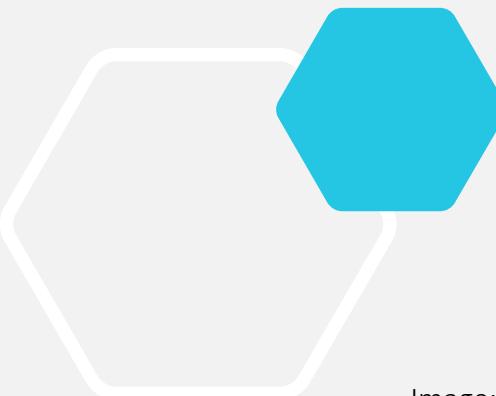
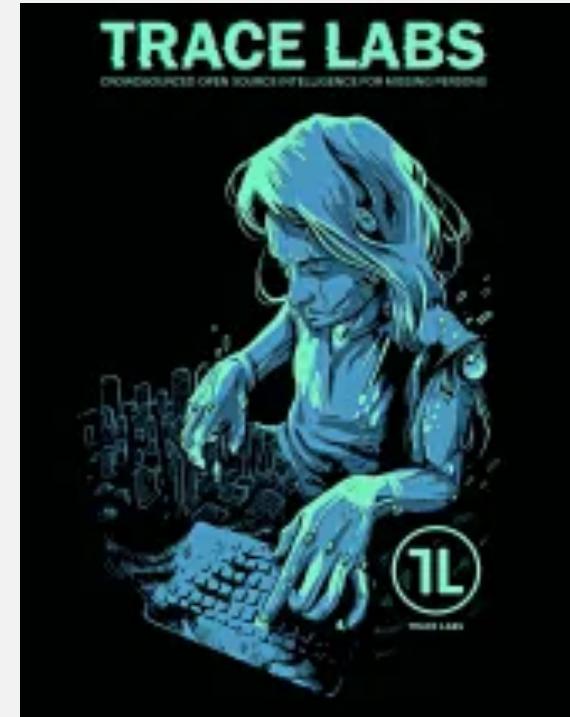
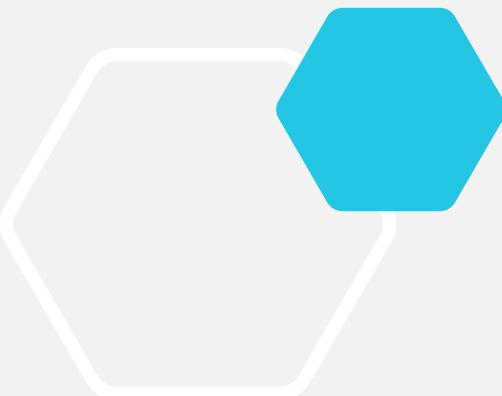


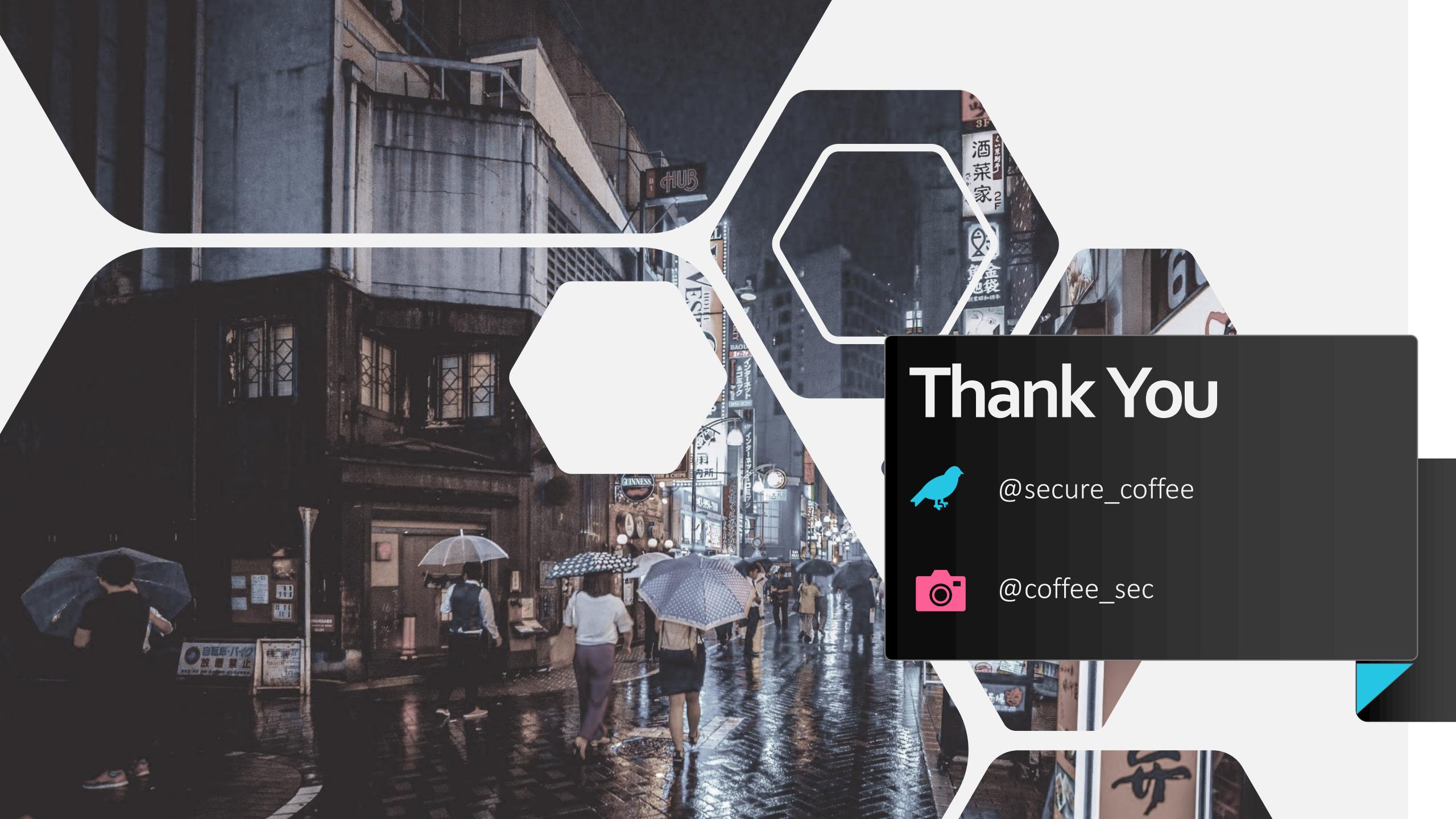
Image: <https://www.tracelabs.org/resources/trace-labs-wallpapers/>

OSINT: Getting Started

Summary

- If you can google you can do this
 - Getting started:
 - VM
 - VPN
 - Google
 - Notebook
 - Desire to help
 - Keep organized





Thank You



@secure_coffee



@coffee_sec

OSINT: Common Tools and How to use them Safely

Resources

- List of references used

