OSINT: Common Tools and How to use them Safely

Siobhan Kelleher

Senior Security Analyst
Boston College

OSINT: Common Tools and How to use them Safely

Topics

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

OSINT: Common Tools and How to use them Safely

What is OSINT?

"Open-source intelligence (OSINT) is intelligence that is produced from publicly available information and is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement."

https://www.govinfo.gov/content/pkg/USCODE-2011-title50/html/USCODE-2011-title50-chap15-subchapI-sec403-5.htm

OSINT: Common Tools and How to use them Safely

What is OSINT?

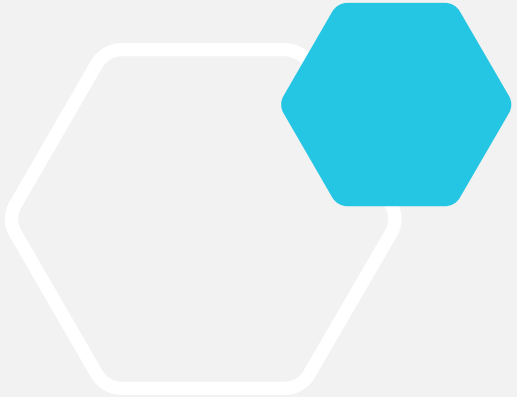
- The Internet
- Media (e.g. television, radio, newspapers, magazines)
- Professional Publications (journals, conferences, studies)
- Photos
- Geospatial information (e.g. maps and commercial imagery products)
- …and more

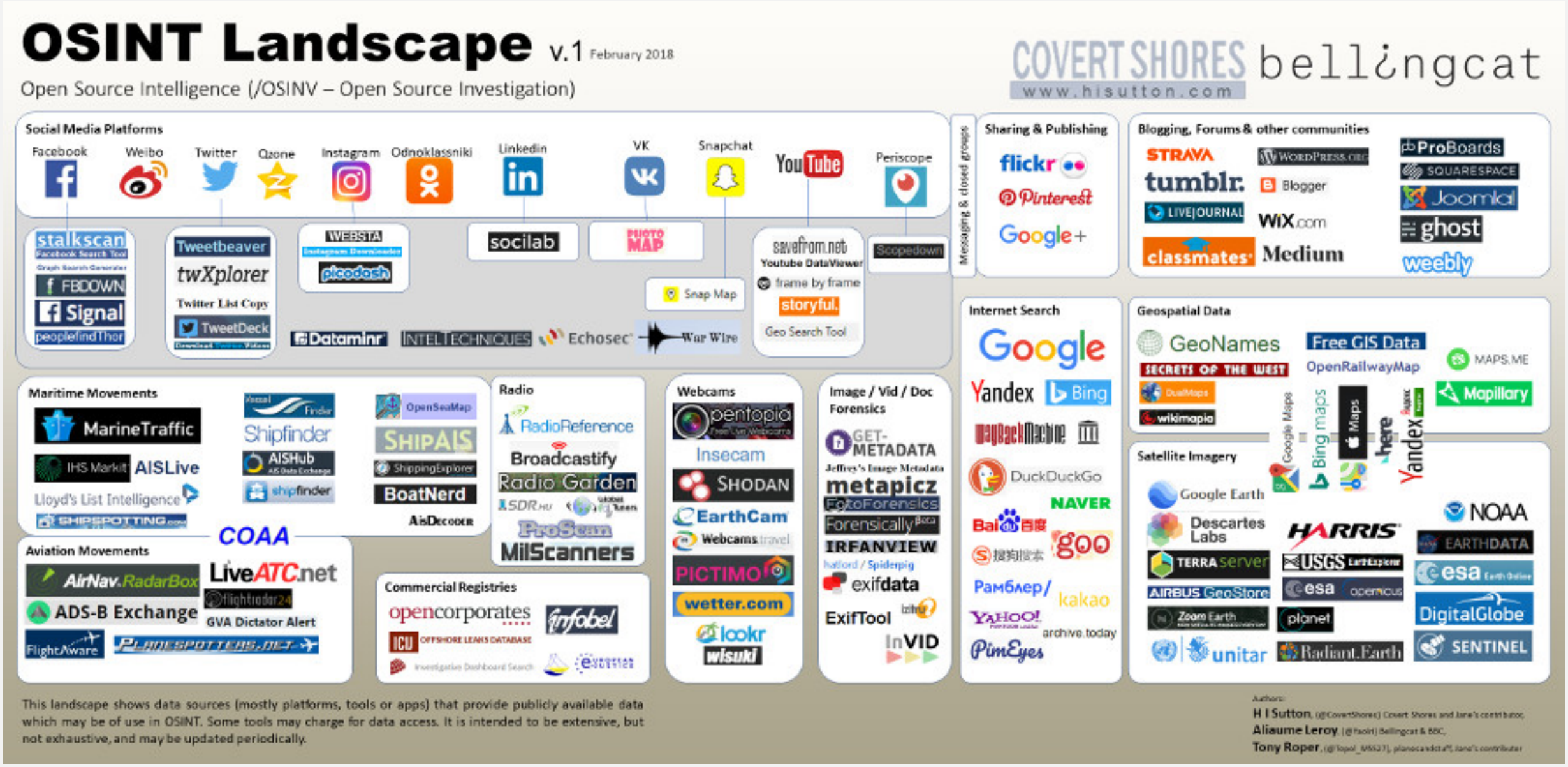
https://www.cia.gov/news-information/featured-story-archive/2010-featured-story-archive/open-source-intelligence.html

OSINT: Common Tools and How to use them Safely

How am I using OSINT?

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





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

OSINT: Common Tools and How to use them Safely

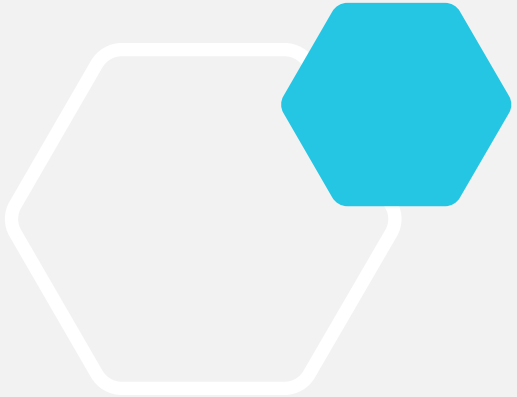
Tools & Resources

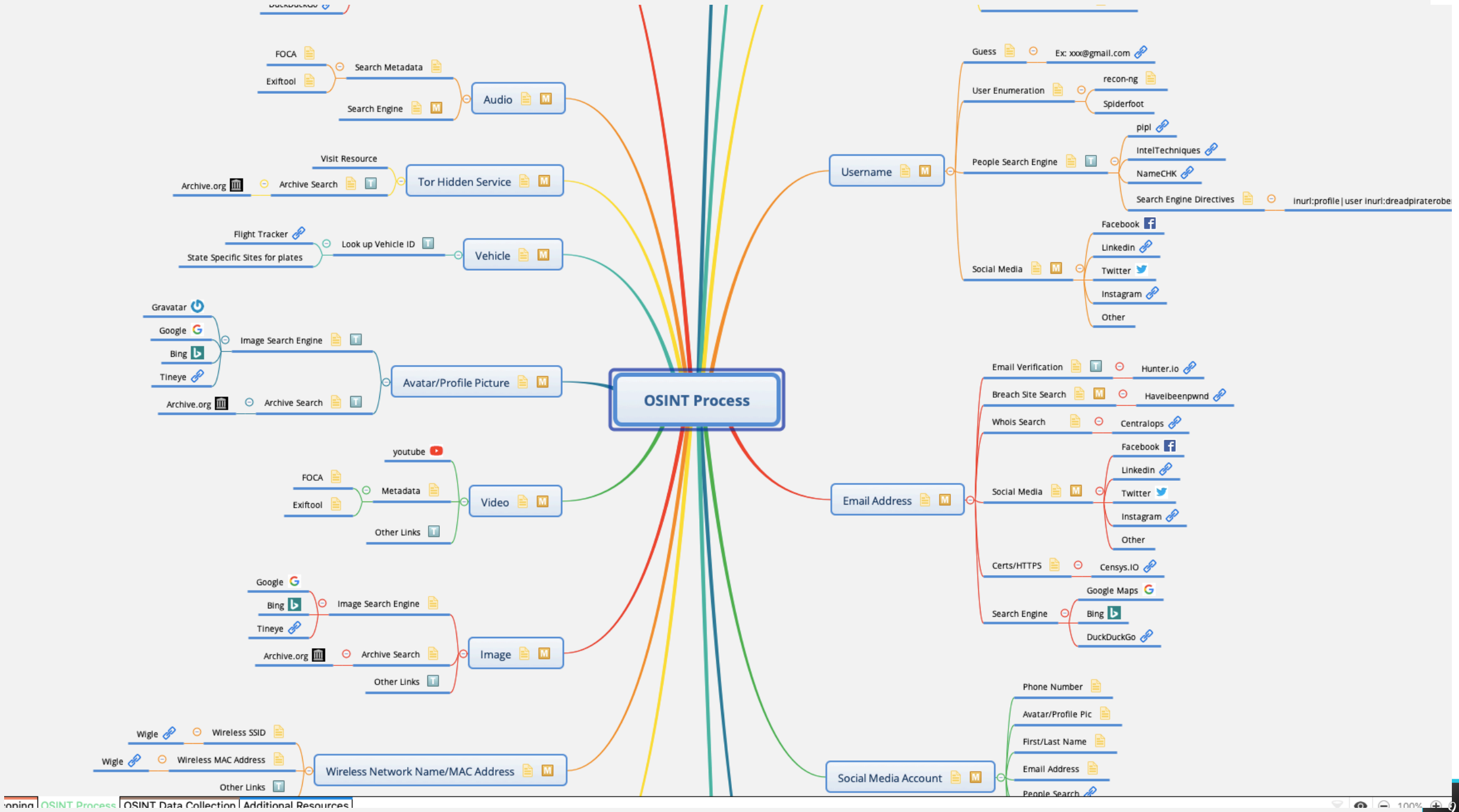
- Social Media
  - Tiktok, Twitter, Facebook, Snapchat, dating apps…
- Email
- Reverse Image Search
- Public Records
  - Address, arrest records, death certificates
- Other

OSINT: Common Tools and How to use them Safely

Tools and Resources

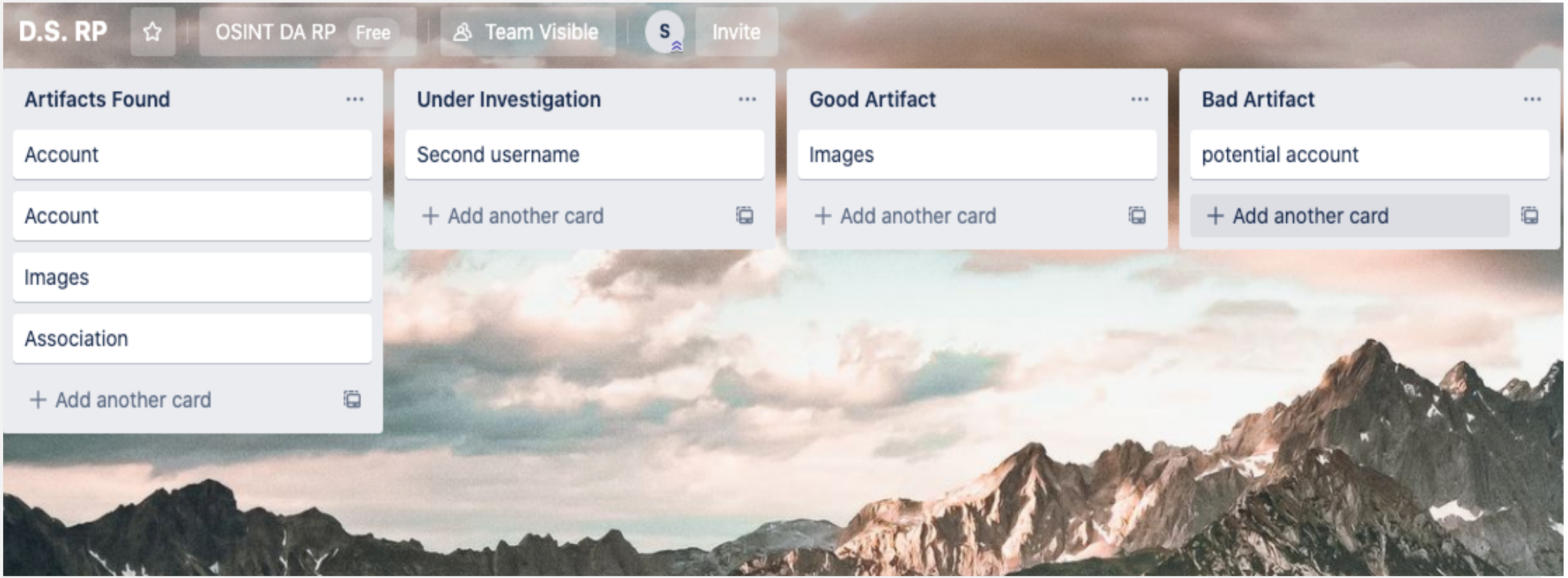
- Mind Mapping
- Hunchly
- Excel
- Trello
- Session Buddy





https://github.com/WebBreacher/osinttools

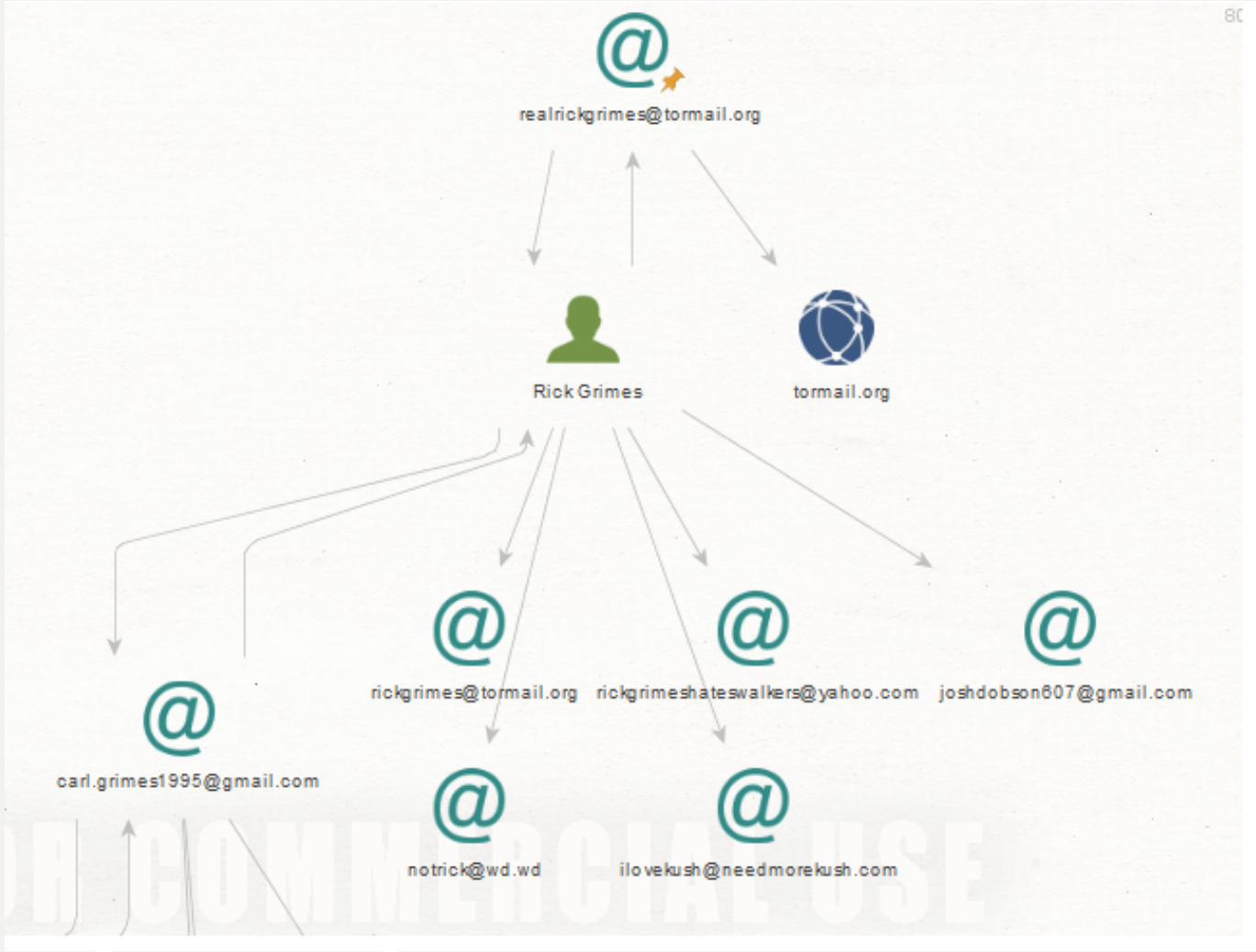
	A	B	C	D
1	OSINT: Jane Doe			
2	https://www.mass.gov/doc/person-missing-poster/download			
3	**What**	**Link**	**Artifact**	**Notes**
4	Phone number	www.theirnumber.cor	8675309	found through this link,
5	Mother	www.mothers	Janet Doe	facebook page is open lists other relatives found through facebook search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


D.S. RP
OSINT DA RP
Free
Team Visible
S
Invite
Artifacts Found
Account
Account
Images
Association
Add another card
Under Investigation
Second username
Add another card
Good Artifact
Images
Add another card
Bad Artifact
potential account
Add another card

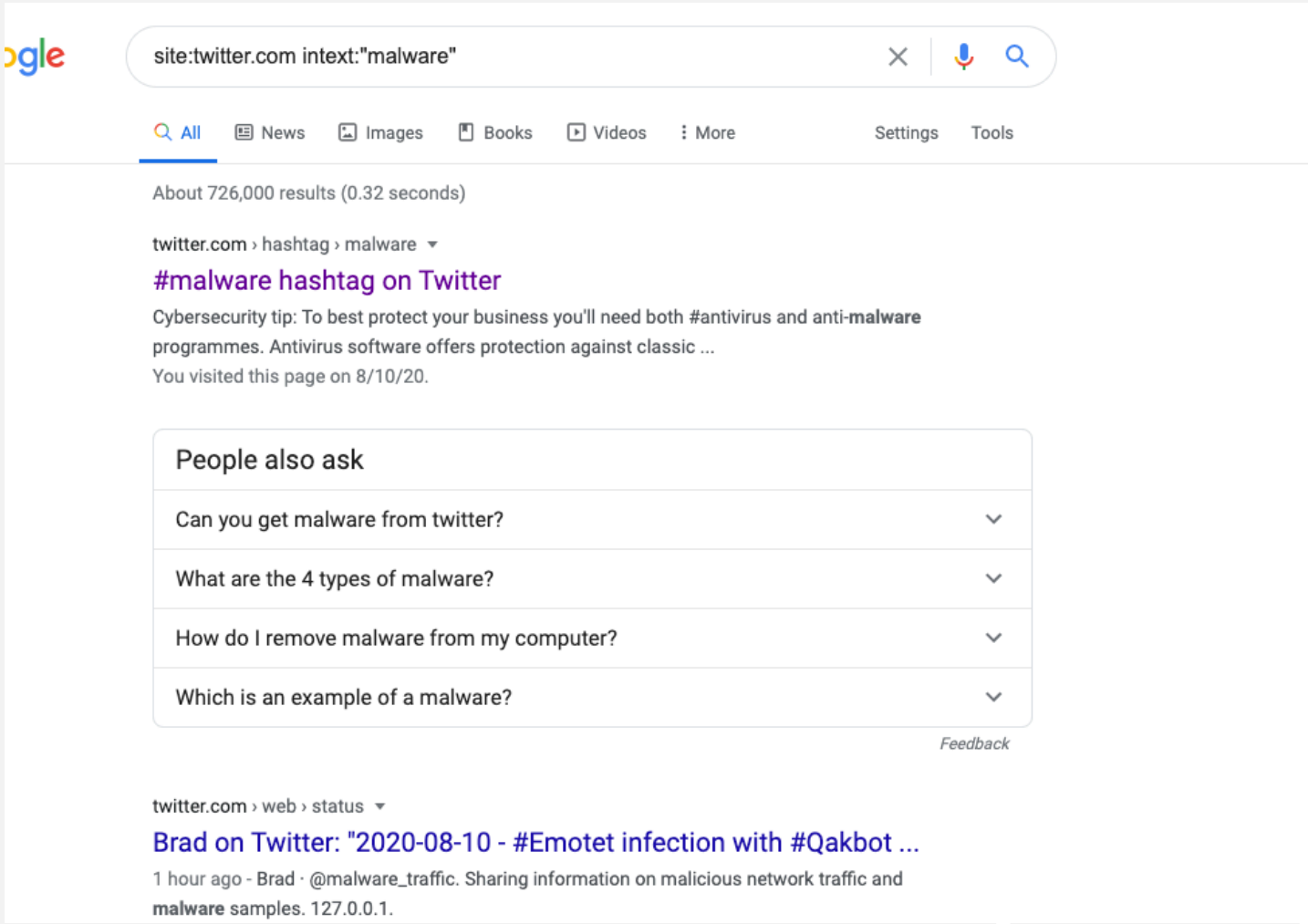
OSINT: Common Tools and How to use them Safely

Tools and Resources

Maltego



https://medium.com/@raebaker/a-beginners-guide-to-osint-investigation-with-maltego-6b195f7245cc



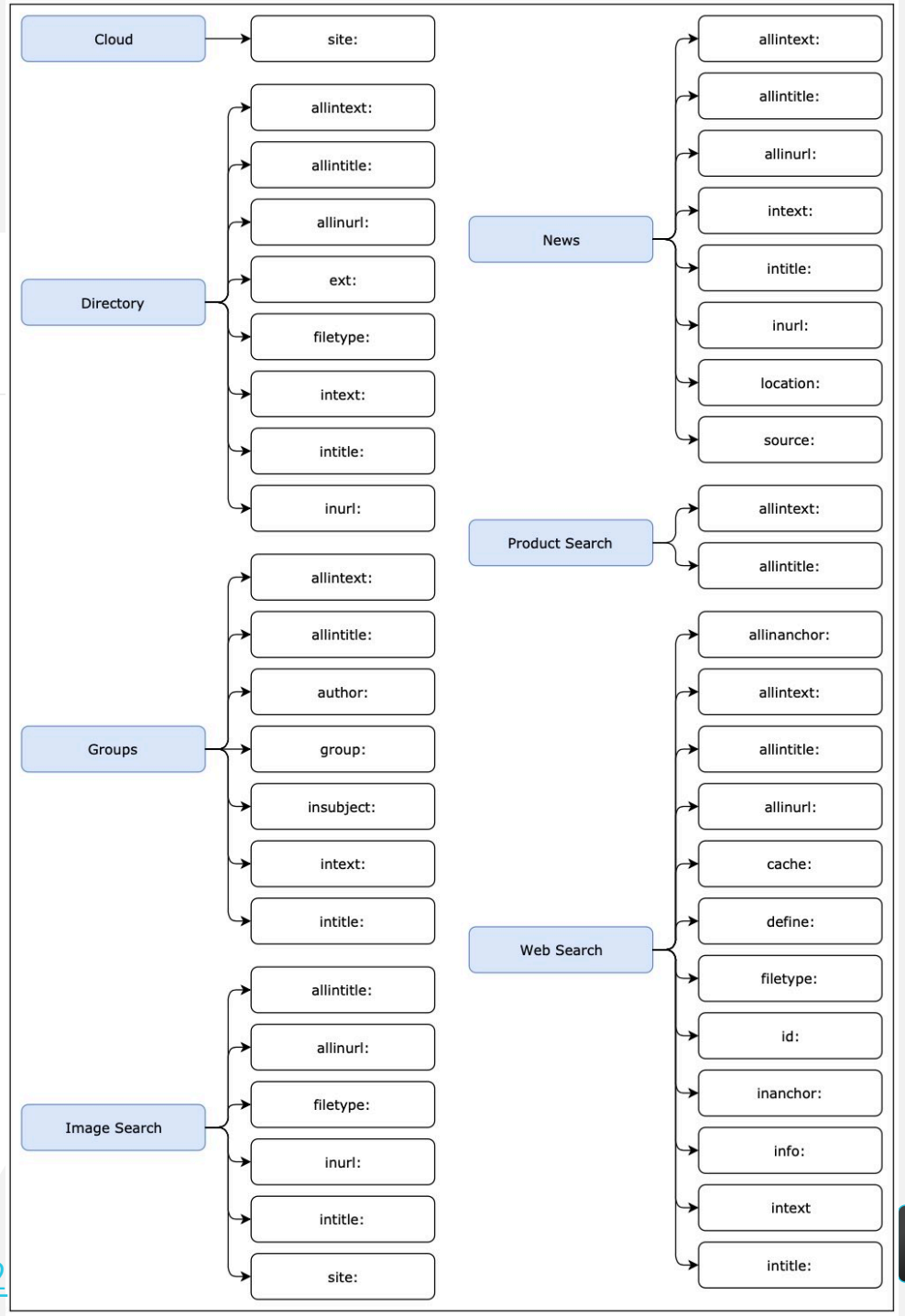
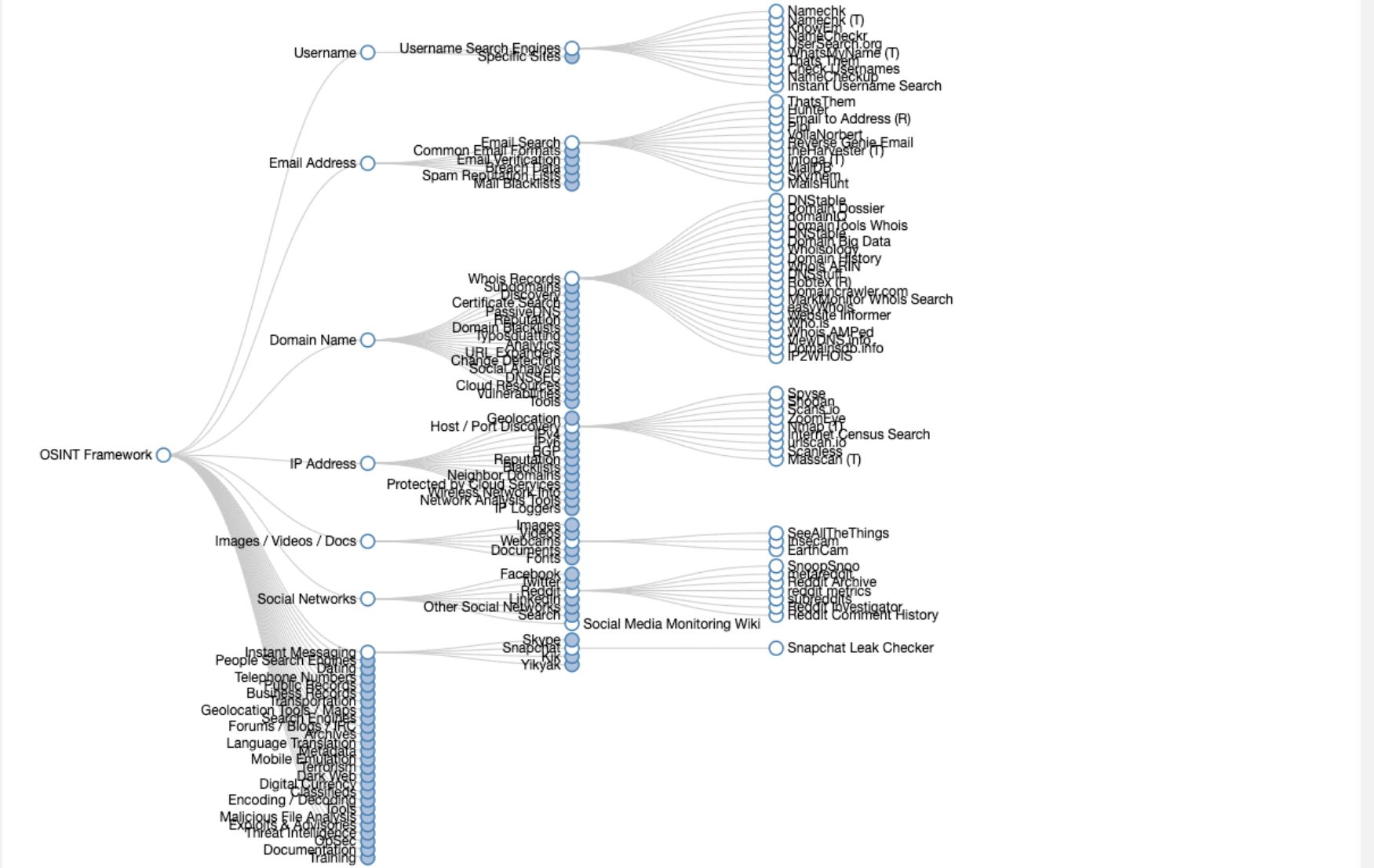


Image: https://twitter.com/velstadt_com/status/1206902436469911552

OSINT Framework

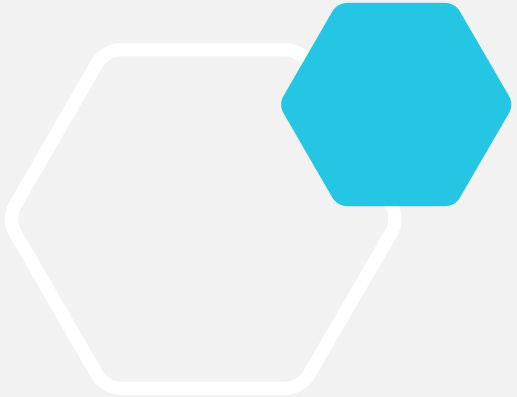


https://osintframework.com

OSINT: Common Tools and How to use them Safely

Tools and Resources

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

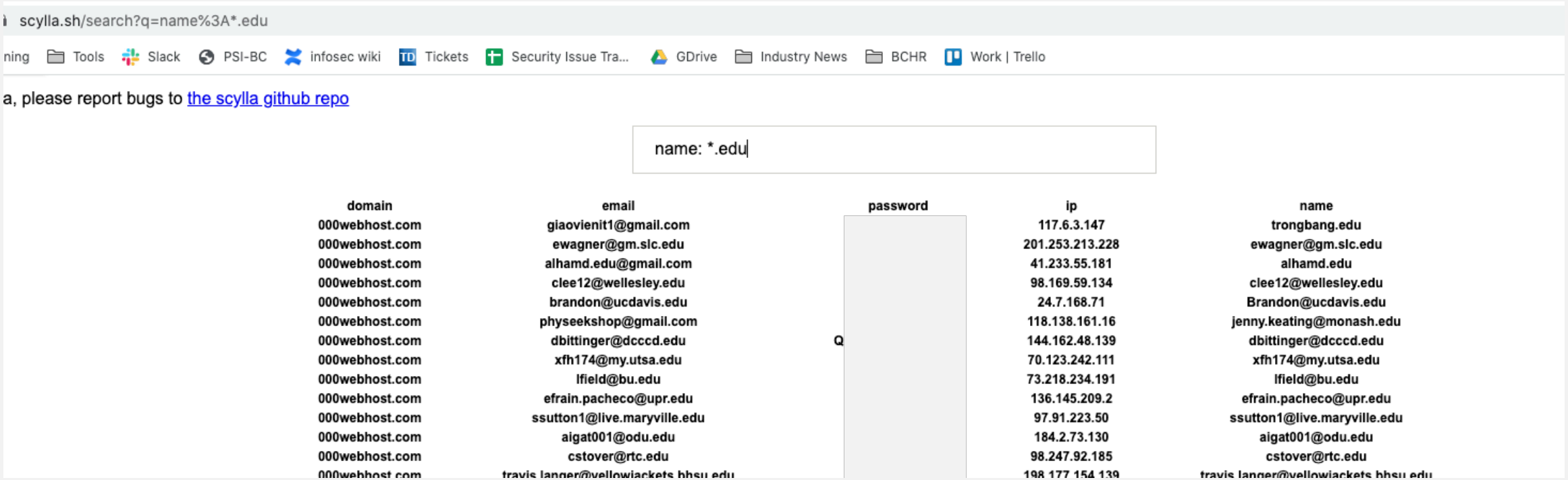


https://www.spiderfoot.net/

OSINT: Common Tools and How to use them Safely

Tools and Resources

Scylla Project



https://scylla.sh/

https://twitter.com/_hyp3ri0n

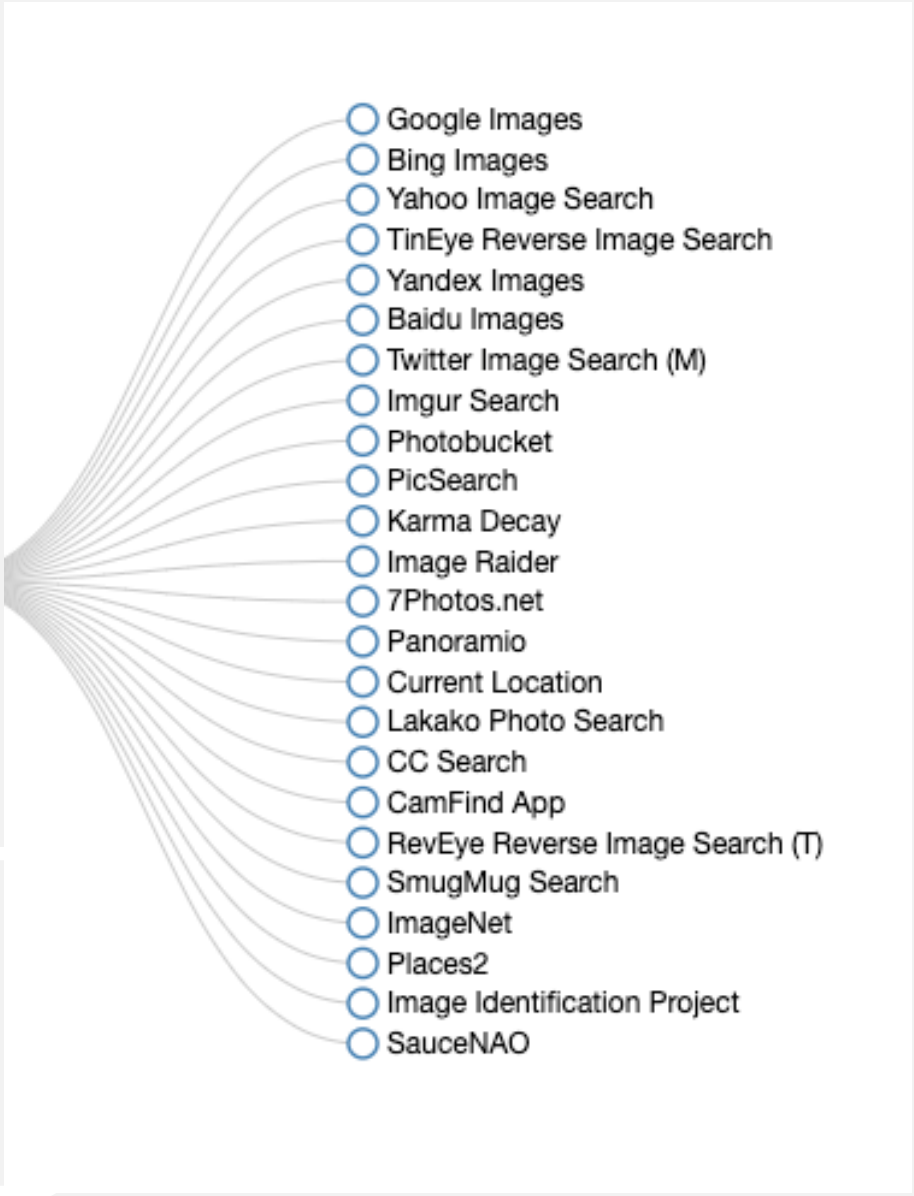
OSINT: Common Tools and How to use them Safely

Tools and Resources

- Reverse Image Search
  - Find other accounts

https://tineye.com/

https://images.google.com/



OSINT: Common Tools and How to use them Safely

Tools and Resources

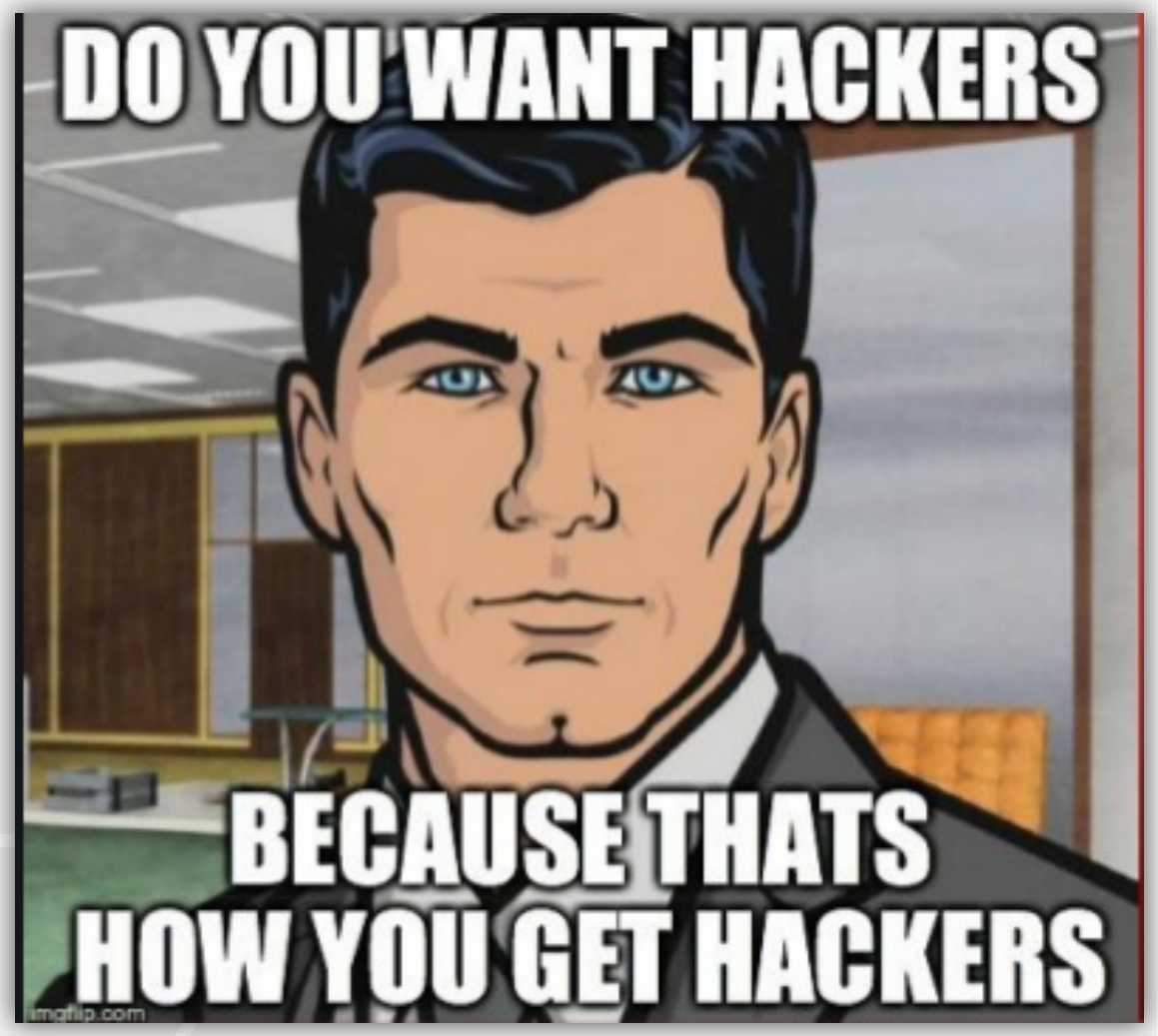
- Social Media Search
  - Simple is sometimes better

Image: https://mn2s.com/news/social-media-management/five-ways-social-media-can-help-your-start-up-2/

OSINT: Common Tools and How to use them Safely

Staying Safe

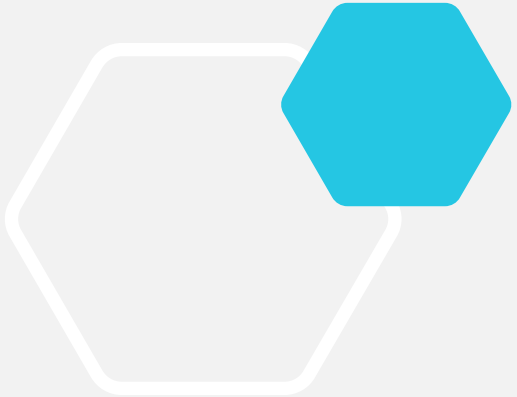
- Why its important!
  - Protect yourself
  - Isolate the target protect the investigation



OSINT: Common Tools and How to use them Safely

Staying Safe

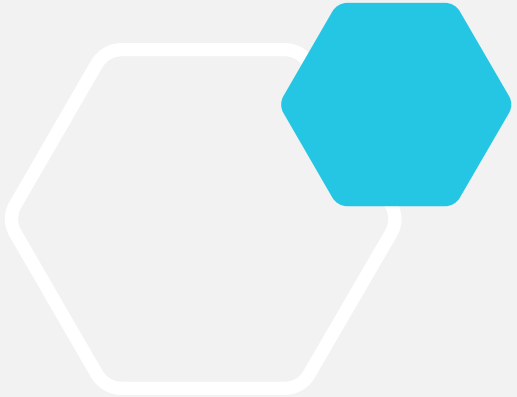
- Passive recon or “no touch”:
  - No interaction with target
  - Not invasive
  - No illegal hacking
- Active recon:
  - Logging into targets accounts
  - Contacting target/friends/family



OSINT: Common Tools and How to use them Safely

Staying Safe

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

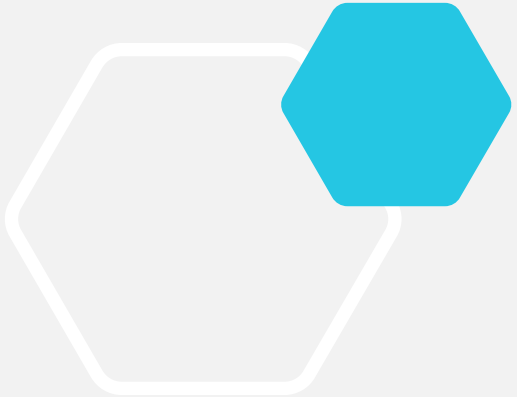


https://www.privacytools.io/

OSINT: Common Tools and How to use them Safely

Staying Safe

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



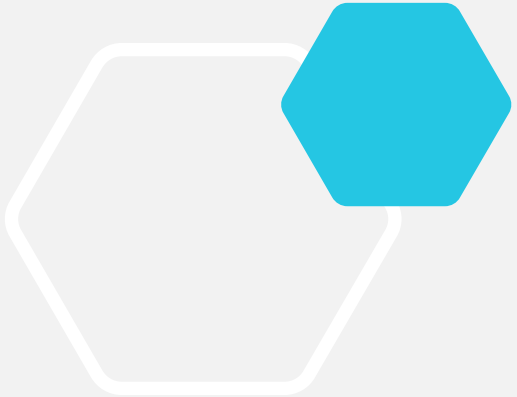
OSINT: Common Tools and How to use them Safely

Staying Safe

- Sock Puppet Accounts
  - Burner Phone
  - Smart Proxy
  - Wifi
  - Fake Identity Generators

https://www.thispersondoesnotexist.com/

https://www.fakenamegenerator.com/



OSINT: Common Tools and How to use them Safely

Using Your Skills for Good

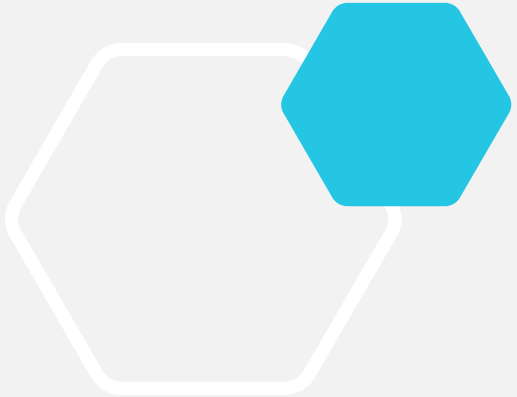
- TraceLabs
  - CTF- prizes, and glory!
  - Monthly collaborative cases

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

OSINT: Common Tools and How to use them Safely

Summary

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



Thank You

Siobhan Kelleher
siobhan.kelleher@bc.edu