Introduction to OSINT/ Social Media Investigations

DAVID MOZDEN

Disclaimer

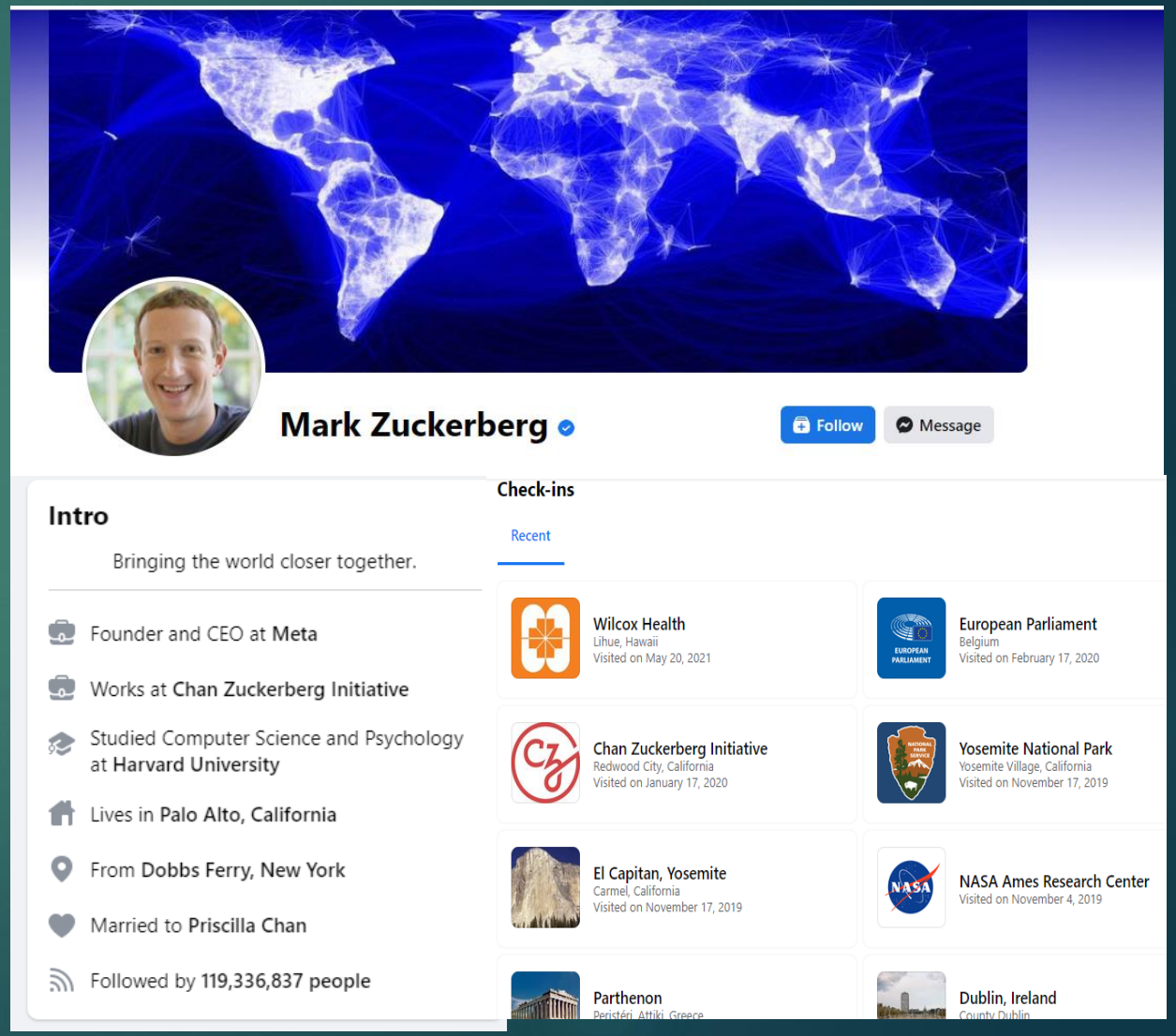
- The information presented here is for general information purposes. The techniques presented are not the policy of any organization the presenter is associated with whether public or private.
- This is a very basic overview of techniques and a case study showing manual investigative function.

Social Media Overview

- Platform Users
  - Facebook- 2.912 Billion
  - Instagram- 1.452 Billion
  - Tik Tok- 1 Billion
  - SnapChat- 293 million
  - Twitter- 217 Million
- There is a significant level of conversation occurring in the virtual space form which information can be gleaned.

What type of information?

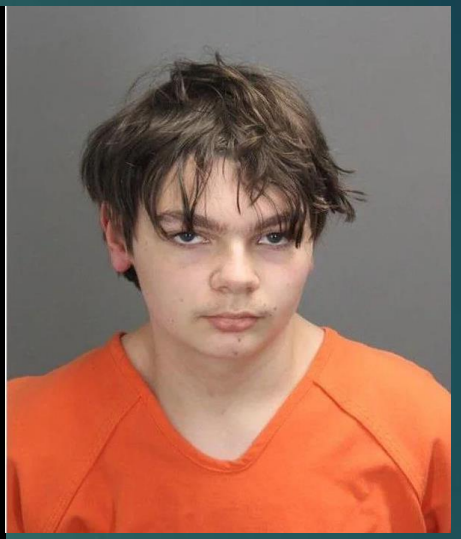
- Person specific information
  - Bio, photos, likes, postings, friends list, etc.
  - Mapping a person's online social network-
    - Who do they know?
    - Who do they frequently interact with?



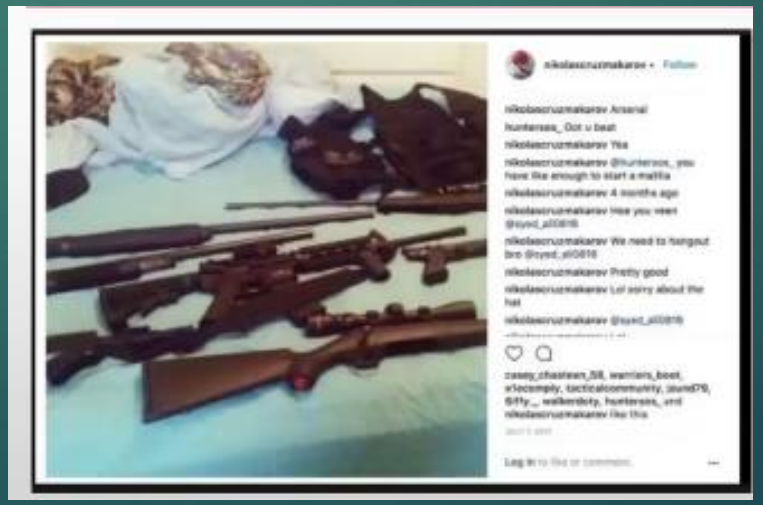
Threat Assessment

- The U.S. Department of Justice released a report in June 2018:
  - Key findings from the report included the following:
  - 77% of active shooters spent a week or longer planning their attack
  - **56% of active shooters leaked intent to commit violence prior to the attack**
  - **88% of the active shooters aged 17 and younger leaked intent to commit violence, compared with 51% of adult active shooters who leaked their intent**

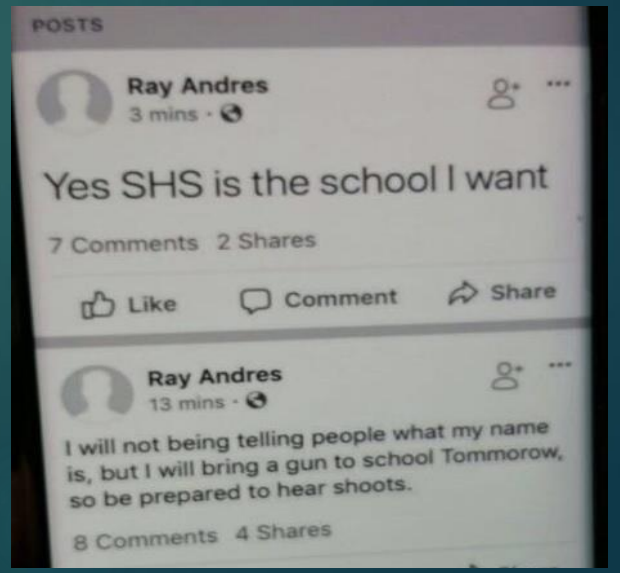
https://paladinrisksolutions.com/osint/warning-signs-of-a-mass-violence-attack-on-socialmedia/#:~:text=88%25%20of%20the%20active%20shooters,threats%20prior%20to%20the%20attack.



Oxford Township, Michigan



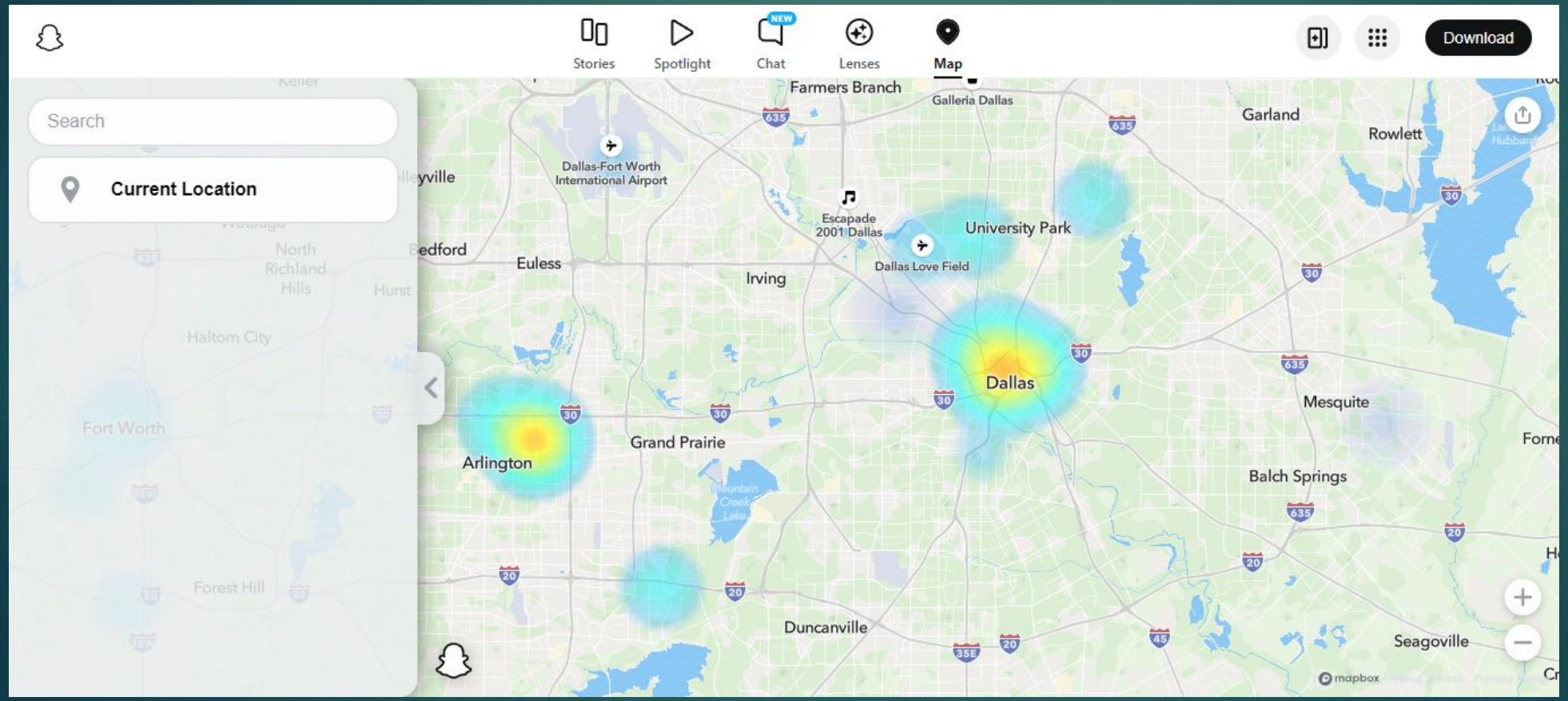
Parkland Shooter



What type of information?

- Event information

  Snap Chat Map



What type of information?

- Event information
- Transactional information
  - Facebook Marketplace has more than 1 Billion monthly users
    - Ebay-109 million
    - Craigslist- 60 million
    - Offerup- 20 million
  - $26 billion gross revenue was made on Facebook Marketplace in 2021, an increase of 48% from 2020*
  - Facebook is quickly becoming one of the largest grey market platforms globally.

* Read more at: https://thrivemyway.com/facebook-marketplace-stats/

Investigative

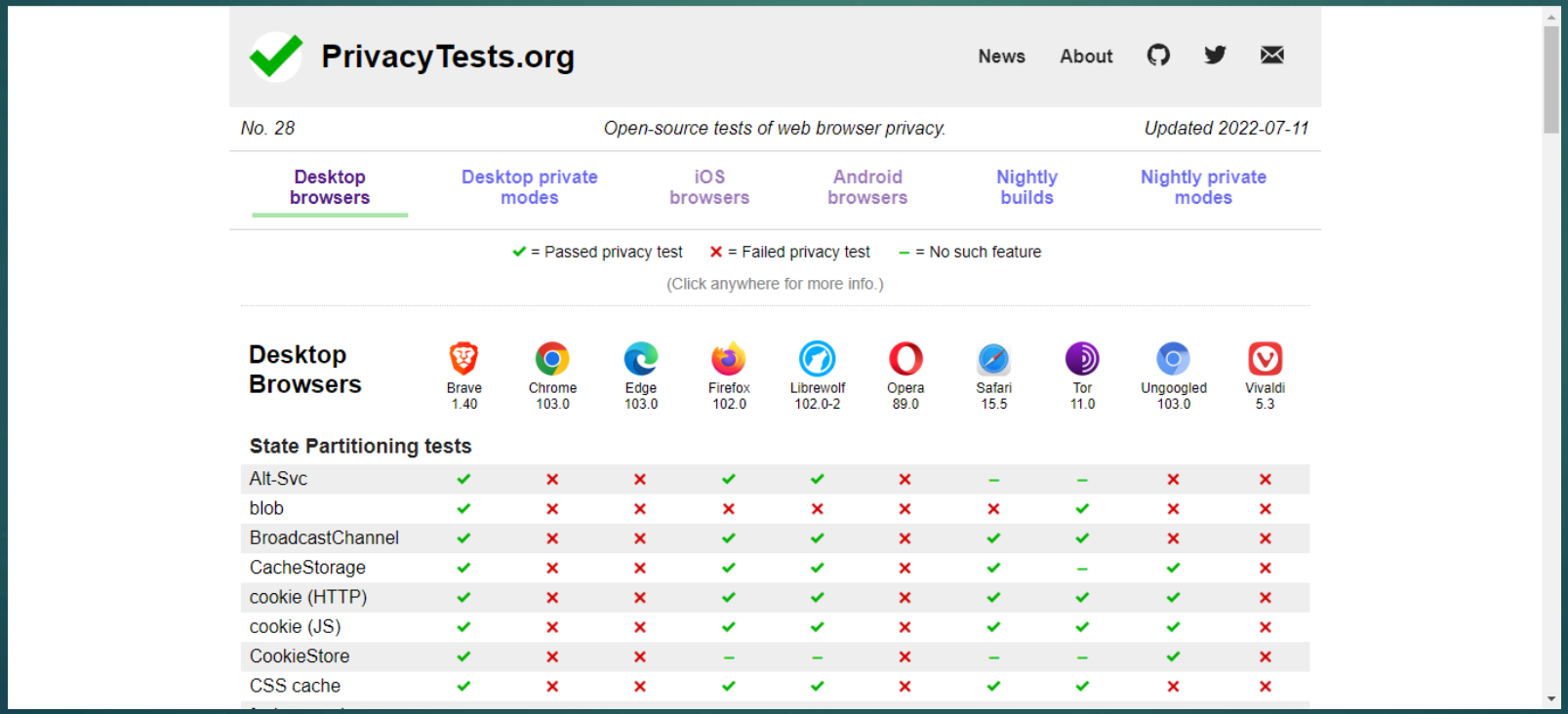
- OSINT-
  - *defined as intelligence produced from publicly available information that is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement. The Internet and the rise of social media have made OSINT more complex in terms of both sources and methods.- Office of the Director of National Intelligence, 2011*

Security

- Never investigate a POI or organization using your personal social media accounts.
  - The platform algorithms will begin to associate you profile visiting the POI's profile and may suggest your account to them as a 'friend suggestion"
  - Sock puppet account- a fake or alternative account used to anonymously investigate, make postings etc.
    - Sock Puppet account
      - Start with a separate email address not associated with personal or work info
      - Ideally, use a pre-paid cellphone for text message association/ app interaction
      - Generate social media accounts using a realistic name
      - Follow popular accounts

Security

- Never perform investigations on personal computers or computers with sensitive information on it.
- Always use a VPN to perform investigations
- Use incognito options on browsers- Not all are truly “incognito”



PrivacyTests.org

News About

No. 28 — Open-source tests of web browser privacy. — Updated 2022-07-11

Desktop browsers | Desktop private modes | iOS browsers | Android browsers | Nightly builds | Nightly private modes

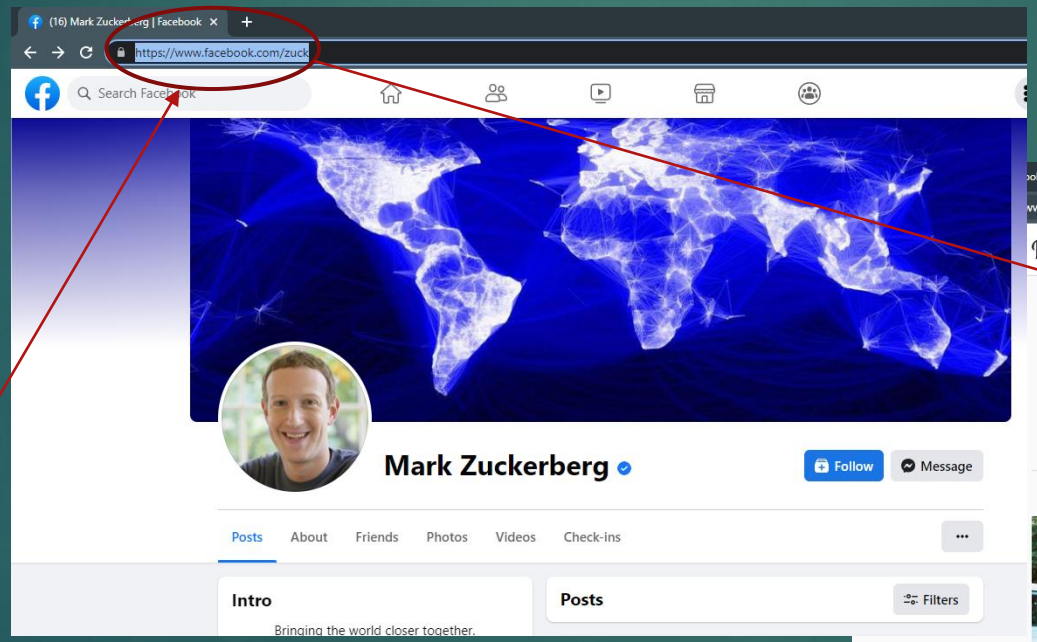
✔ = Passed privacy test ✘ = Failed privacy test – = No such feature

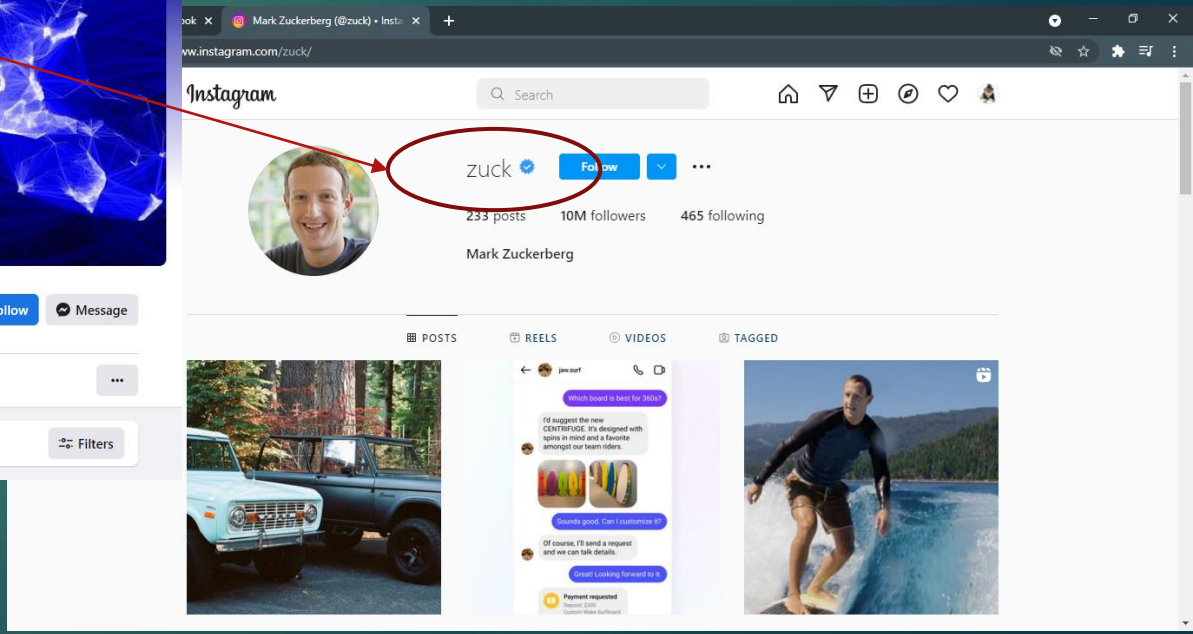
(Click anywhere for more info.)

Desktop Browsers	Brave 1.40	Chrome 103.0	Edge 103.0	Firefox 102.0	Librewolf 102.0-2	Opera 89.0	Safari 15.5	Tor 11.0	Ungoogled 103.0	Vivaldi 5.3
State Partitioning tests										
Alt-Svc	✔	✘	✘	✔	✔	✘	–	–	✘	✘
blob	✔	✘	✘	✘	✘	✘	✘	✔	✘	✘
BroadcastChannel	✔	✘	✘	✔	✔	✘	✔	✔	✘	✘
CacheStorage	✔	✘	✘	✔	✔	✘	✔	–	✔	✘
cookie (HTTP)	✔	✘	✘	✔	✔	✘	✔	✔	✔	✘
cookie (JS)	✔	✘	✘	✔	✔	✘	✔	✔	✔	✘
CookieStore	✔	✘	✘	–	–	✘	–	–	✔	✘
CSS cache	✔	✘	✘	✔	✔	✘	✔	✔	✘	✘

Investigative Principles (Basic)

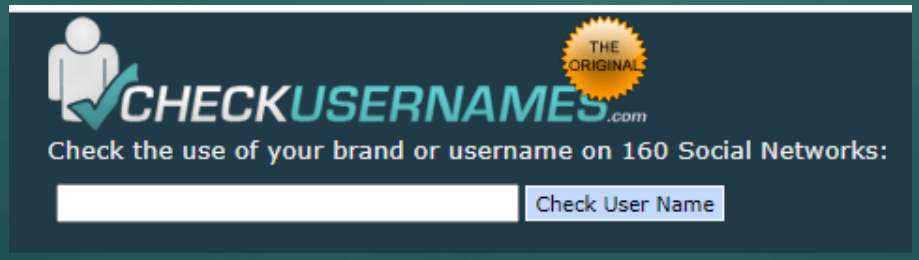
- There are many Open Source (publicly available) OSINT Tools that interact with websites and social media platforms to harvest information.
- Pay attention to details
  - Posts
  - Images
  - Comments
  - Likes
  - Usernames





OSINT Tools

- There are many Open Source (publicly available) OSINT Tools that interact with websites and social media platforms to harvest information.

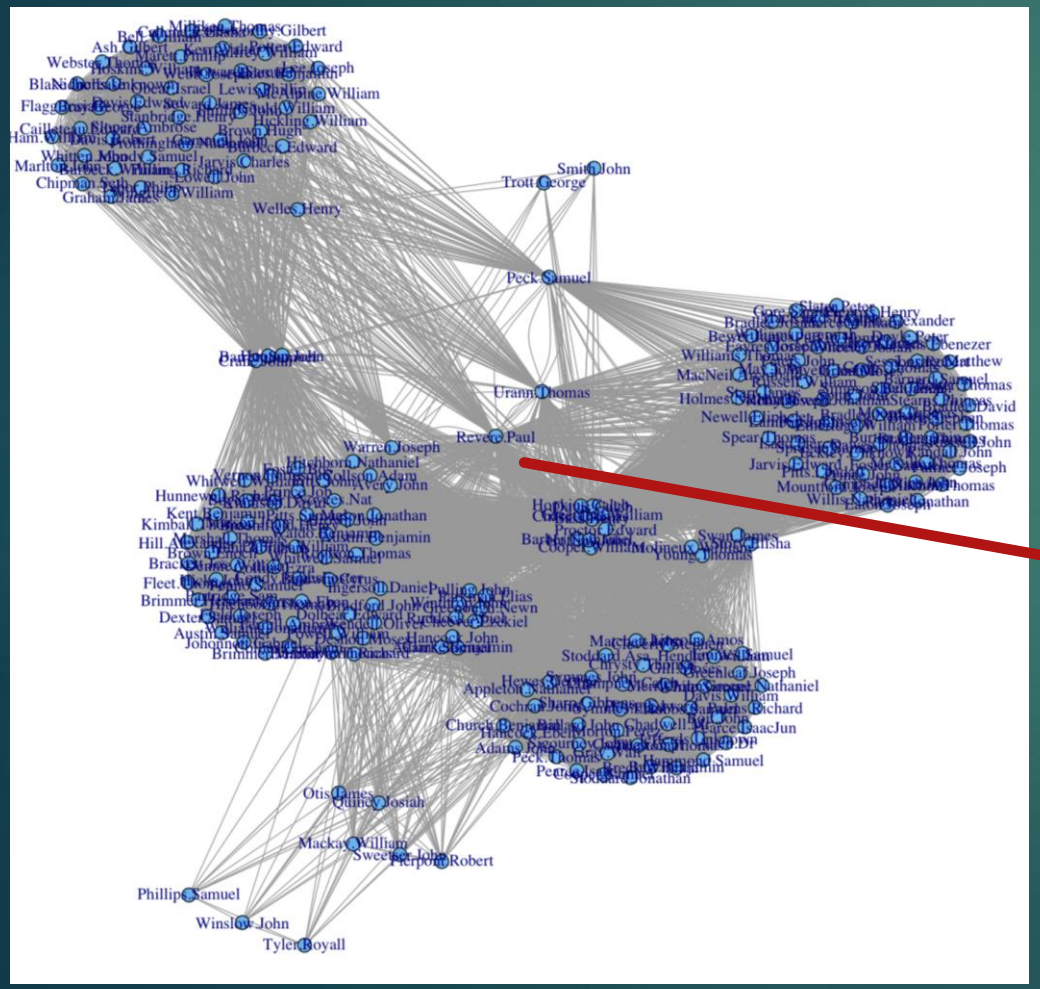


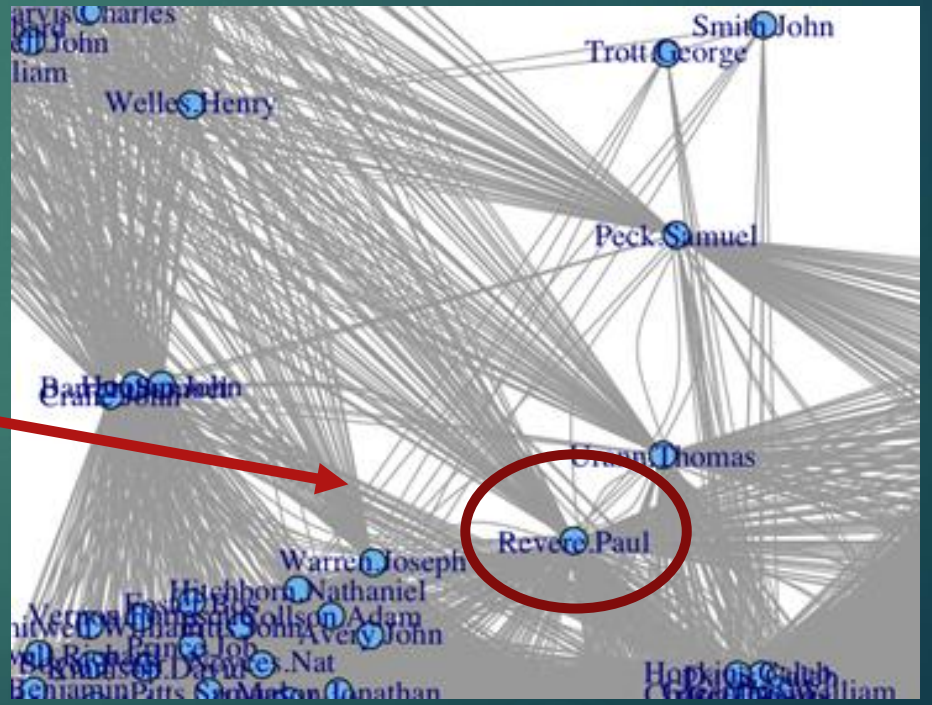
Investigative Principles (Basic)

- Learn how to find/map a person's social network to gain information on them- “Find their Judas”
  - People will often try to use aliases or pseudonyms on social media accounts but still connect and interact with family members using actual names.
- Use screen capture software to document your investigative process for both evidentiary and reference purposes
  - People involved in illicit activity will often change their social media account monikers.
  - Once someone becomes suspicious of their social media accounts being monitored, they may delete their presence entirely or restrict certain information from “public” view.

Social Network Analysis

- Using Metadata to find Paul Revere
  - https://kieranhealy.org/blog/archives/2013/06/09/using-metadata-to-find-paul-revere/



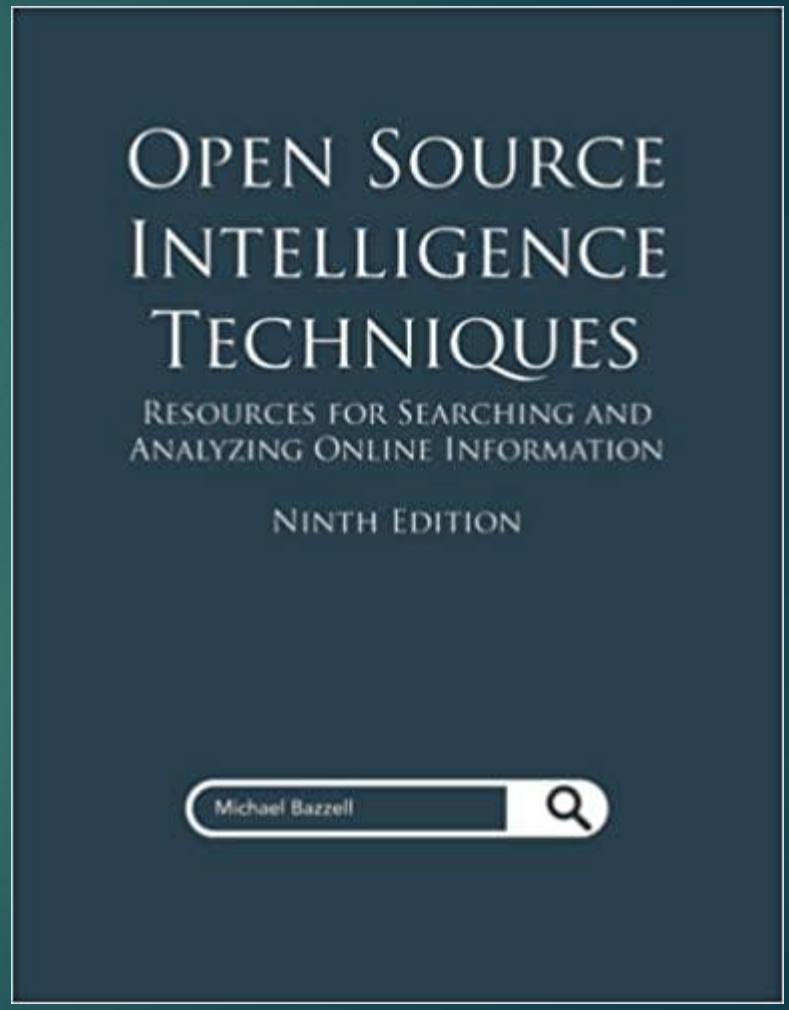


Conclusion

- Social media is valuable investigative tool
- Check with your department's specific policy on rules for investigating on social media.
- Pay attention to the details- Bio, pictures, likes, postings, etc.
- Use security precautions to protect/ conceal yourself during investigations

OSINT Resources

- https://osintframework.com/
- https://inteltechniques.com/index.html
- https://osint.tools/course-websites
- https://github.com/jivoi/awesome-osint
- https://osint.link/



Contact Info

David Mozden

Managing Director Sendero Solutions Group

2100 N Main Street, Suite 20B

Fort Worth, Texas 76164

dmozden@senderosolutionsgroup.com

M +1 469 693-8856