

OSINT Workshop (Hands on!)

SANS Security Awareness Summit 2019

The Internet has changed over the years

World Wide Web

The WorldWideWeb (W3) is a wide-area [hypermedia](#) information retrieval initiative aiming to give universal access to a large universe of documents.

Everything there is online about W3 is linked directly or indirectly to this document, including an [executive summary](#) of the project, [Mailing lists](#), [Policy](#), November's [W3 news](#), [Frequently Asked Questions](#).

[What's out there?](#)
Pointers to the world's online information, [subjects](#), [W3 servers](#), etc.

[Help](#)
on the browser you are using

[Software Products](#)
A list of W3 project components and their current state. (e.g. [Line Mode](#), [X11 Viola](#), [NeXTStep](#), [Servers](#), [Tools](#), [Mail robot](#), [Library](#).)

[Technical](#)
Details of protocols, formats, program internals etc

[Bibliography](#)
Paper documentation on W3 and references.

[People](#)
A list of some people involved in the project.

[History](#)
A summary of the history of the project.

[How can I help?](#)
If you would like to support the web..

[Getting code](#)
Getting the code by [anonymous FTP](#), etc.

<http://info.cern.ch/hypertext/WWW/TheProject.html>

The screenshot shows a Google Maps interface with a search for "Restaurants" in San Diego. The left sidebar displays filter options for Price (\$ to \$\$\$\$) and Rating (Any rating). Below the filters, three restaurant listings are shown: "Trust" (4.6 stars, 584 reviews), "Ironside Fish & Oyster" (4.6 stars, 1,882 reviews), and "The Lion's Share" (4.7 stars, 734 reviews). Each listing includes a photo, price range, cuisine, location, and opening hours. The main map area shows a street view of San Diego with several restaurant markers. A search bar at the top right says "SEARCH THIS AREA".

<https://www.google.com/maps/search/Restaurants/@32.759902,-117.2864638,11.83z>

People share so much data

Where they are



<https://www.pexels.com/photo/australia-traveling-travelling-travel-68704/>

Who they are with



<https://www.pexels.com/photo/photography-of-couple-holding-hands-842546>

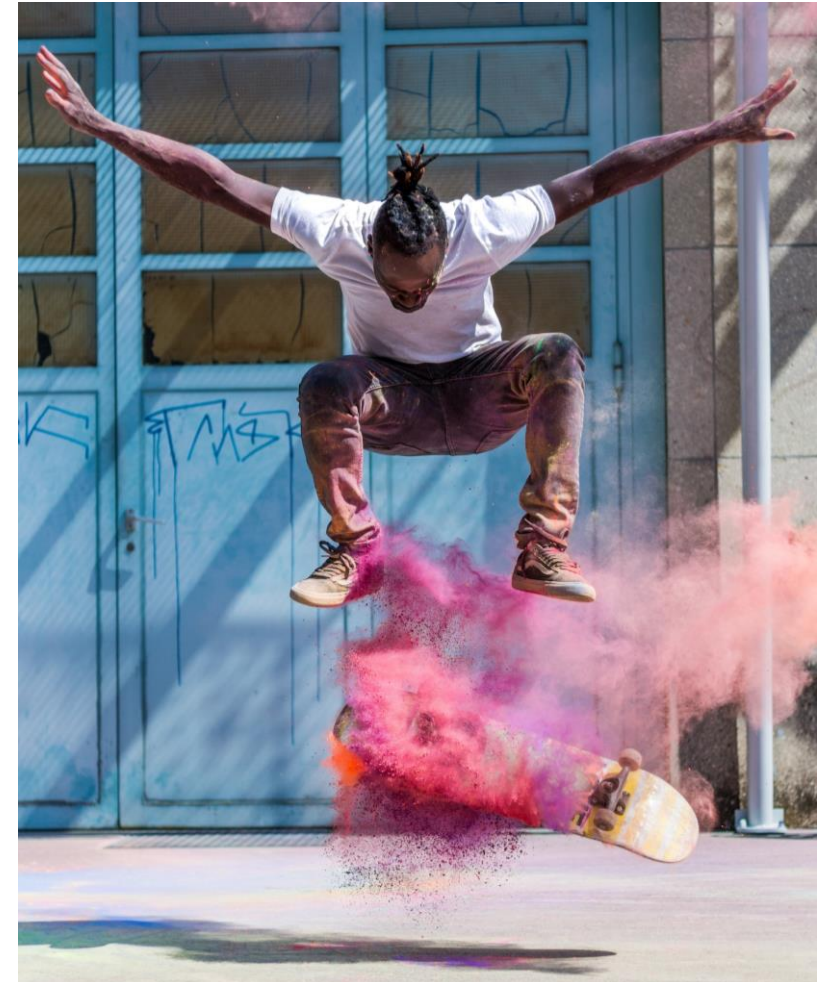
People share so much data

Their likes



<https://www.pexels.com/photo/close-up-photo-of-man-wearing-black-suit-jacket-doing-thumbs-up-gesture-684385/>

Their hobbies



<https://www.pexels.com/photo/action-active-activity-adult-415188/>

The US government shares data



The screenshot shows the Federal Election Commission (FEC) website. The header includes the FEC logo, the text "Federal Election Commission UNITED STATES - of - AMERICA", and links for "Calendar", "Glossary", and a search bar. Below the header, there are navigation links: "Campaign finance data", "Help for candidates and committees", "Legal resources", and "About". A breadcrumb trail reads "Home > Campaign finance data > Browse data > Individual contributions". The main heading is "Individual contributions" with an "Export" button. Below this, it says "Viewing 51,263 filtered results for:" with filters for "2019-2020" and "\$2000 or more". A table displays the data with columns: Contributor name, Recipient, State, Employer, Receipt date, and Amount. Three rows are visible, each showing a \$2,800.00 contribution.

Contributor name	Recipient	State	Employer	Receipt date	Amount
GI [REDACTED], C [REDACTED] E	FRIENDS TO ELECT DR. GREG MURPHY TO CONGRESS	TN	HOMEMAKER	07/10/2019	\$2,800.00
GI [REDACTED], C J	FRIENDS TO ELECT DR. GREG MURPHY TO CONGRESS	TN	G [REDACTED]	07/10/2019	\$2,800.00
R [REDACTED] EPAK D	PRAMILA FOR CONGRESS	NJ	NEI [REDACTED] FAMILY FDT	06/30/2019	\$2,800.00

https://www.fec.gov/data/receipts/individual-contributions/?two_year_transaction_period=2020&min_amount=2000

Our religious and community groups share



Photo Credit: Carl Shortt and Vicki Gistrip

SERVANT KIDS VOLUNTEER SPOTLIGHT

Each month, we will be highlighting some of our very special and wonderful volunteers. This will help you get to know them better and also let you know who is leading our children on their spiritual journeys. If you see them around church, give them a hug or a high five for their hard work and dedication to children's ministries!



TYLER & MEGHAN
PRESCHOOL TOTAL GROUP

We are mostly known as Stella and Brooks' parents, and they are going into 2nd grade and kindergarten. We love attending Church of the Servant with several of our family members, and our church family is very important to us. When we aren't at church, you can find us spending time with family and friends, or at various ball fields. We help in the preschool Total Group time at the 9:30 service, two times monthly. We love getting to know the kids and their families, watching the youngest kids become comfortable and confident, and watching all the kids worship Jesus and understand His teachings. Working with the kids is always encouraging, they love and include everyone and, although it's cliché, we always learn more about how to be better parents and Christians when we help in children's ministry.



HOLLY B
FIRST GRADE SMALL GROUPS (SUMMER SCHOOL)

I love watching the kids grow throughout the year and all the hilarious things they say. If you are considering being a volunteer for Servant Kids, it's so easy, and the rewards outweigh the time commitment by a thousand.

WEEKLY DEVOTIONALS FOR FAMILIES AND KIDS

On our new website, we have a section on the kids page with weekly devotionals. These devotionals include activities that go along with the lesson learned on the previous Sunday morning. We would like to encourage you to spend a few minutes each day with your child(ren) reinforcing what they have learned about that week during Total Group and small groups. We also post Bible readings, reflection questions, and more each day on Instagram and/or Facebook. When the church and family work together to enforce the concepts and lessons, we will have the greatest impact on the lives of our kids!

WE NEED YOUR HELP!

We need help leading children to Christ! Servant Kids is searching for adults who are willing to lead a small group or Sunday School class or to sub when a Sunday morning leader needs to be gone. This is for an hour on a Sunday morning, either at the 9:30 or the 11:00 hour. We also need help once a month on the first Wednesday night from 6:30-8:00. Contact Kourtney for more information at: kallie@churchoftheservant.com

STILL TO COME...

SERVANT KIDS CAMP REGISTRATION IS OPEN!

Servant Kids Camp is returning this summer! This is for kids in incoming grades 1st-5th. Save the date for August 2-4 at Canyon Camp! Registration is now available at ServantOKC.org/KidsCamp and is due by July 7.

12

ServantOKC.org 13

https://issuu.com/servantchurch/docs/newsletter_070319_all_web?fr=xKAE9_zU1NQ

Groups conduct campaigns to influence us at scale

Facebook Ad Library interface showing three political advertisements.

Filter By: United States ▼ Active and Inactive ▼ All Pages ▼

Launched June 2019

Ad 1 (Left): NRA Institute for Legislative Action. Sponsored - Paid for by NRA. Help fight Northam's gun control. **VIRGINIA GUN OWNERS TAKE ACTION**. Sign Up. See Ad Details.

Ad 2 (Middle): Turning Point USA. Sponsored - Paid for by Turning Point USA. Gun Control In A Nutshell... #GunsSaveLives. **LET'S REDUCE DRUNK DRIVING**. TURNING POINT USA. **DRIVING CARDS**.

Ad 3 (Right): NRA Institute for Legislative Action. Sponsored - Paid for by NRA. Help the NRA fight Northam's Extreme Gun Control. **Join the Fight!**. Sign Up.

https://www.facebook.com/ads/library/?active_status=all&ad_type=political_and_issue_ads&country=US&impression_search_field=has_impressions_lifetime&q=gun%20control

Computers create and alter pics, videos, and audio



<https://thispersondoesnotexist.com/>

Watch Jordan Peele use AI to make Barack Obama deliver a PSA about fake news

By James Vincent | Apr 17, 2018, 1:14pm EDT

f t SHARE



<https://www.theverge.com/tldr/2018/4/17/17247334/ai-fake-news-video-barack-obama-jordan-peepe-buzzfeed>

People used to have to "dumpster dive" to get info



<https://www.pexels.com/photo/scrap-metal-trash-litter-scrapyard-128421/>

Now our sensitive data is mostly online



<https://www.pexels.com/photo/three-women-standing-near-man-holding-smartphones-1262971/>

And available for "others" to retrieve



<https://www.pexels.com/photo/two-alien-inside-car-wallpaper-365625/>

Who am I?

- **SANS Author** of SEC487 (OSINT class)
- **OSINT Consultant** (Spotlight Infosec LLC)
- **OSINTCurio.us** Founder
- **Cyber security** for 15+ years
- **Psychology** degree
- Social media @**WebBreacher**

SEC487: Open-Source Intelligence (OSINT) Gathering and Analysis

- ▶ [Contents](#) | [Additional Info](#)
- ▶ **Delivery Methods:**
[Live](#) | [Online](#)
- ▶ 36 CPEs



We are OSINTCurio.us

This presentation is already online

<https://github.com/WebBreach/presentations>

Grab yourself a copy and follow along!

What would you call...

- Searching for a coffee shop on Bing Maps?
- Looking for a new job on monster.com?
- Researching a business you want to invest in?
- Finding that long lost friend?
- Examining an old photo to see where it was taken?



<https://www.pexels.com/photo/adult-boy-break-browsing-306534/>

We call it

OSINT - Open Source Intelligence

*Searching and examining
available/open data and
applying it to answer questions*

Who uses OSINT?

- **Law enforcement**

- Awareness
- Catching suspects

- **Intelligence community**

- Awareness
- Recruitment
- Analysis of assets

- **Parents**

- **Businesses**

- Recruiting/sourcing
- Understanding risk
- Business intelligence

- **Criminals**

- Preparation for action
- Bragging about exploits

- **People dating**

- Who is this other person?

Why should you care about OSINT?

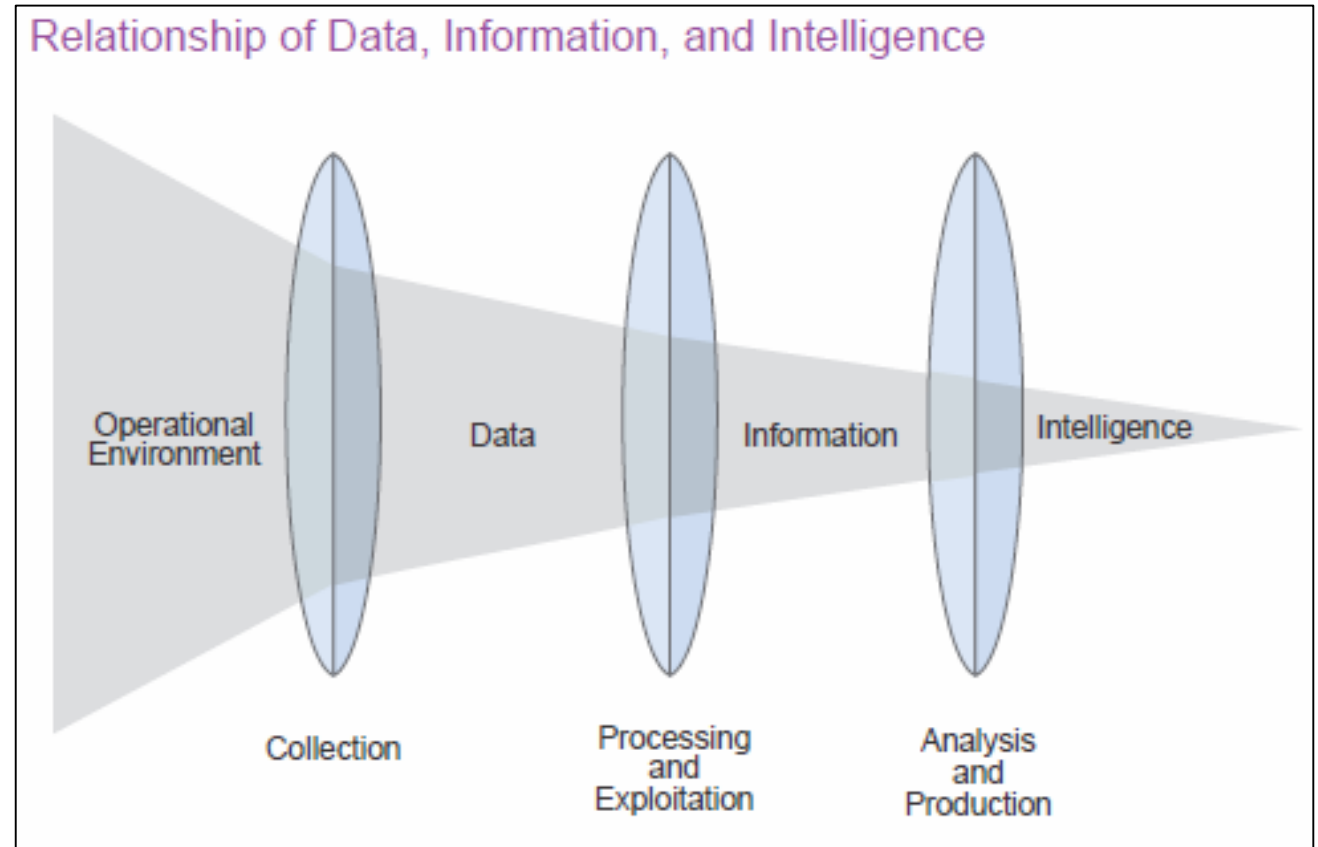
- People are **sharing** things about us online
- People are **collecting** those things and potentially using them
- Understanding **risk** to yourself, your family, and your organization



<https://www.pexels.com/photo/man-and-woman-holding-heart-boards-1449059/>

How do professionals "OSINT"?

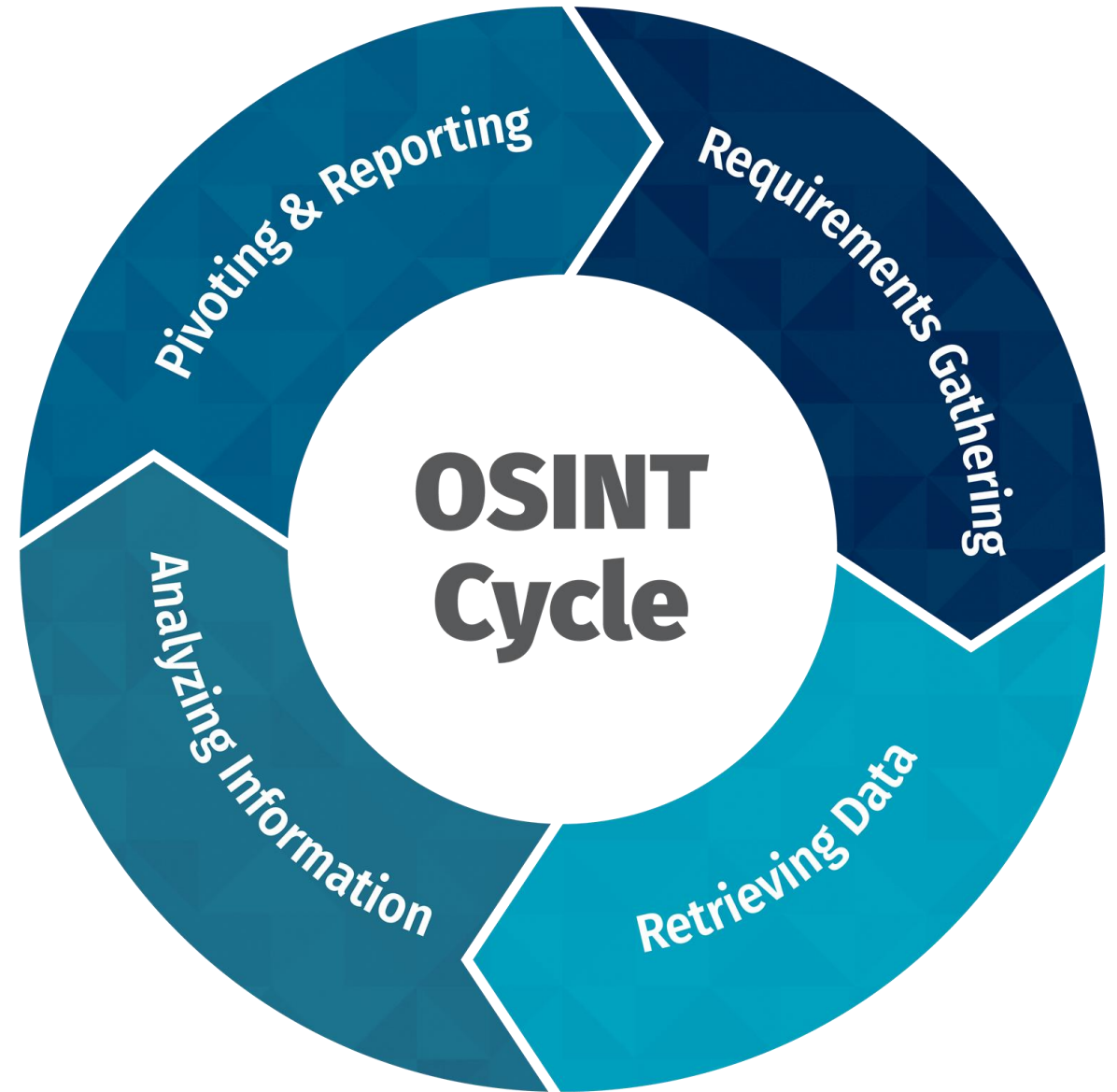
- Gather OS data
- Refine it into OS information
- Add "what does this mean?" and make it OSINT



https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp2_0.pdf

The OSINT Cycle

- Professionals have distinct stages they move through in OSINT work
- Starting with gathering requirements from stake holders and moving clockwise around the cycle



SANS SEC487 Course Materials, 2019.

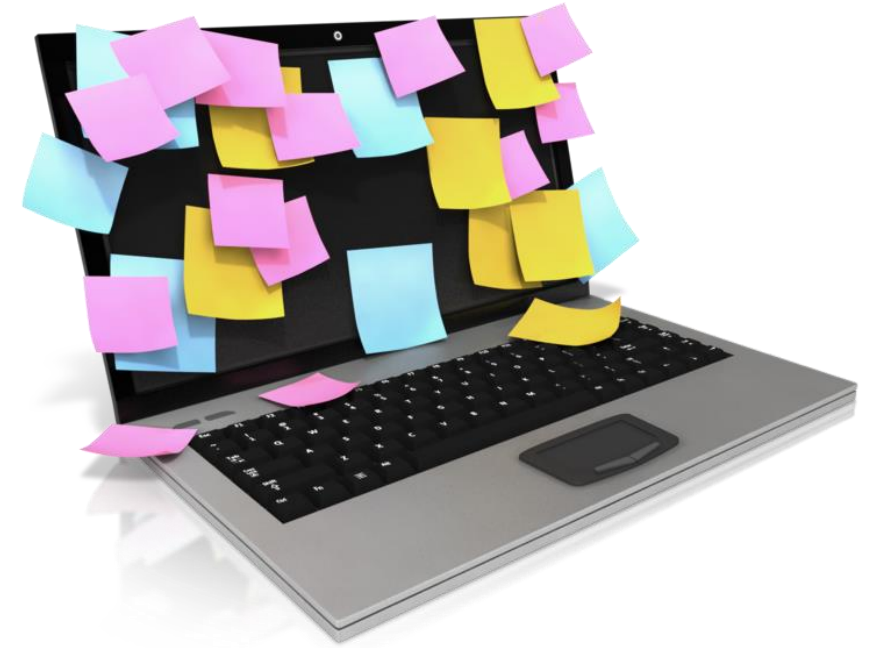
Let's do some OSINT!

- This is a hands-on workshop
- I will show an OSINT skill and how we use it
- Then you will get time to try it on your computer

Potential networking issues



- Please tether your laptop or use a VPN
- This way our network traffic comes from different IPs

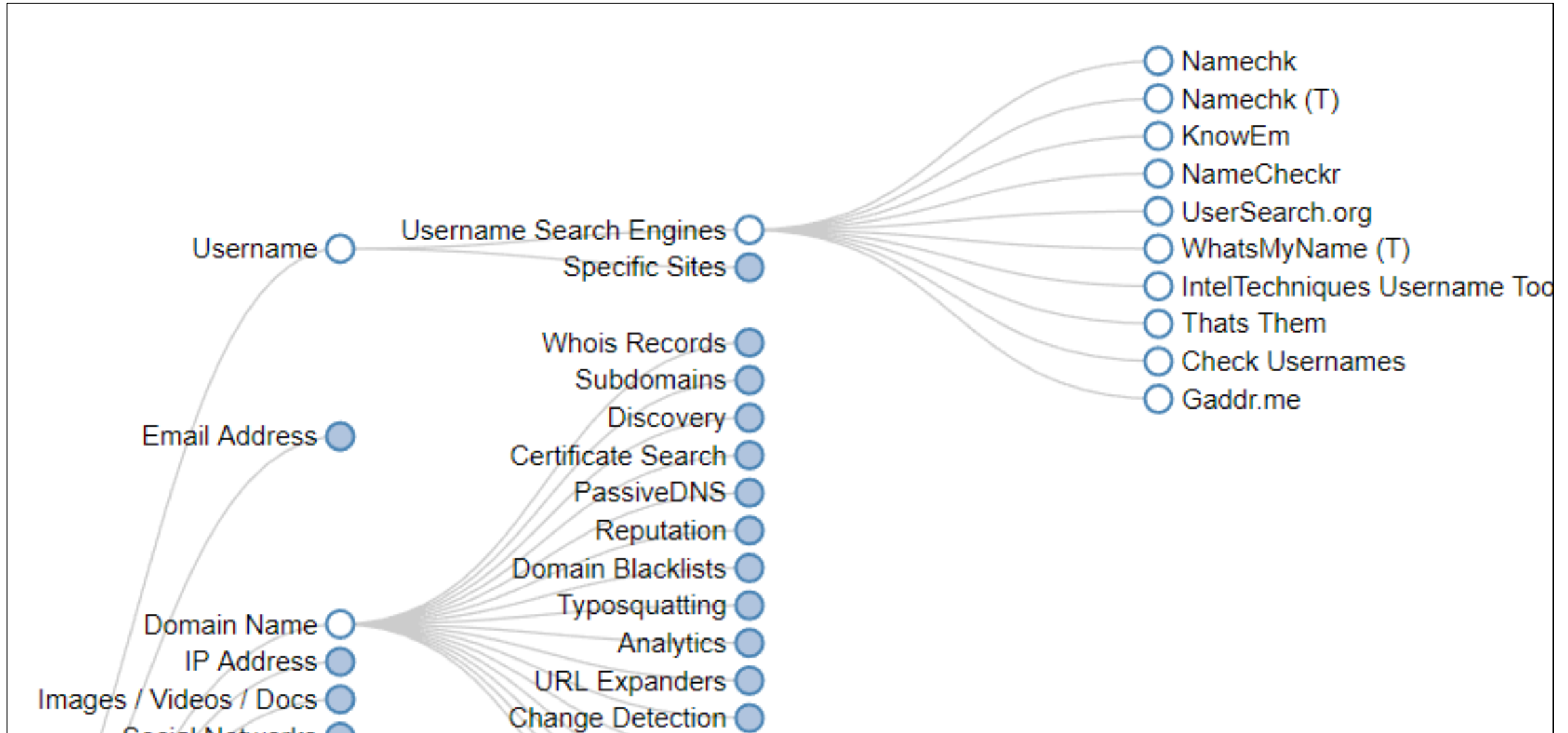


Module 1: Bookmarks and Links

Beginning with URLs

- We will begin with websites that have excellent OSINT resources
 - These sites list URLs to tools or other sites you can use for OSINT
- <https://osintframework.com>
 - <http://osintframework.de>
 - <https://intelx.io/tools>
 - <https://yoga.osint.ninja>

OSINT Framework - osintframework.com



osintframework.de (Start.Me)

 **OSINT FRAMEWORK**

Welcome to the OSINT Open Source Intelligence Framework landing page. This free resource is dedicated to search and used for training purposes. It seeks no financial gain. All information herein can be found in open sources and is for educational purposes only. Please comply with any terms of service should those apply. I would encourage you to make an own framework that reflects your workflow and assignments. Start.me hosts and provides this free bookmarking service and because its free it runs marketing analytics on its site. MindMup provides the online Mindmapping functionality and does not track users. Use responsibly. You are welcome to reach out or follow me on twitter: @digintelosint



Discover other OSINT Frameworks

 **QUICK ACCESS to OSINT FRAMEWORK**

Digital Intelligence Start.me DIRECTORY

> Created with the start.me bookmarking service

-  OSINT LANDING PAGE
-  SEARCH ENGINES
-  SOCMINT
-  SOURCES
-  KEYWORDS | TRANSLATION
-  KYC | AML | FINTECH | CRYPTOCURRENCY |
-  GEOINT | ASSET TRACKING | TRAVELRISK
-  PERSONAL INFRASTRUCTURE
-  INTERNET INFRASTRUCTURE
-  MONITORING RSS
-  IMINT | VIINT
-  OSINT TOOLKIT
-  SOURCES CTY USA
-  DIGITAL SECURITY
-  OPSEC | PRIVACY

intelx.io/tools


Third Party Search:

 General


 Email

 Domain

 IP

 Bitcoin

 Image

 Username

IntelX Tools:

 Selector Extraction

 Document 2 Text

Username Lookup

Select from the checkbox list and enter a Username to search

Search

☐ namevine

☐ peekyou

☐ usersearch

☐ knowem

☐ Twitter

☐ Facebook

☐ YouTube

☐ Tumblr

☐ Instagram

☐ SnapChat

☐ Profilr

☐ Gravatar

☐ Dehashed

☐ Tinder

☐ GitHub

Select All

Important: Make sure that popups are allowed. If you don't see all new tabs opened after hitting search, go back to this tab and enable popups when your browser asks (Chrome: Right side in the URL bar)

yoga.osint.ninja

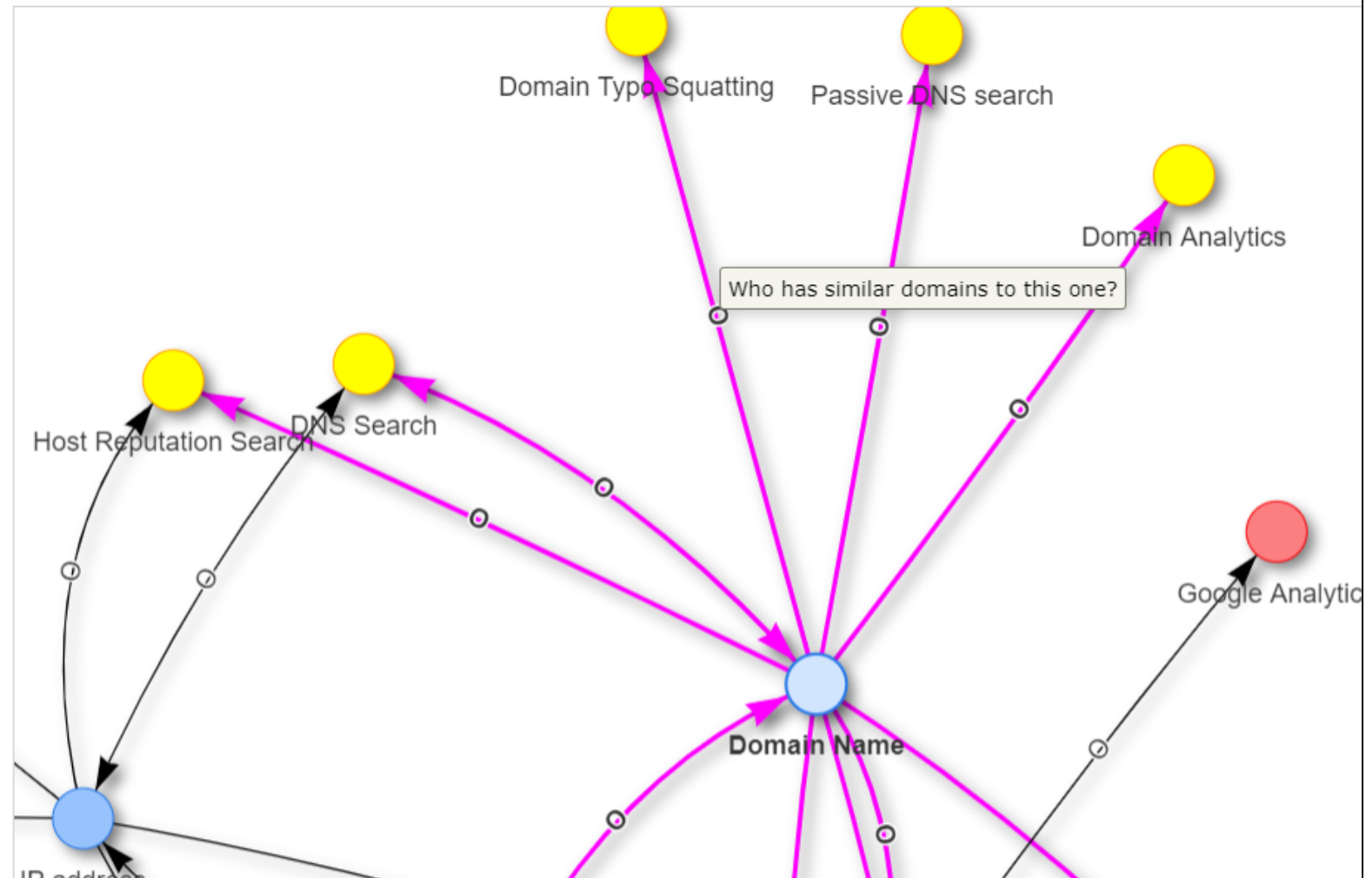
Your OSINT Graphical Analyzer (YOGA)



Usage:

- Click and drag nodes (dots) around the page to view all content
- Use the arrow keys to move around and Page Down/Up to zoom out and in
- If edge connecting 2 nodes has an O in the middle, mouse over it for descriptions of the actions

Created by Micah



Exercise 1: Frameworks

- Open a web browser
- Visit the following sites
 - **osintframework.com**
 - **osintframework.de**
 - **intel.io/tools**
 - **yoga.osint.ninja**
- Explore the data available on each



5 Minutes

Search Engines

Much of our work is done in search engines

- Use multiple search engines for different perspectives

- DuckDuckGo.com



- Bing.com



- Yandex.com



- Google.com



- Narrow results using search **operators or directives**
- Most search engines have "**Advanced Search Forms**"
- Operators sometimes work in multiple engines

Google, Bing, and DDG Operators/Directives

Operator	Function	Example
" " (Quotes)	Group terms together. Terms must appear in results as they do in the quotes.	"SANS Security Awareness"
- (Dash)	Negate term or directive. Do not show results with this content.	-WebBreacher -"micah Hoffman"
site:	The results must be indexed from the domain/URL specified.	site:sans.org site:www.sans.org/event
filetype:	The filetype or file extension of the results.	filetype:pdf
OR	One term or another	micah OR webbreacher

Examples

Operators	Outcome
<code>"micah hoffman" OR "webbreacher"</code>	Results must have either the words micah hoffman in it or the word webbreacher
<code>"micah hoffman" -site:sans.org</code>	Results must have micah hoffman in them and NOT be from the sans.org domain
<code>site:.gov filetype:xlsx</code>	Results must be from a *.gov domain and be an Excel XLSX document
<code>newsletter church OR temple OR mosque -sample -example -template -site:.com</code>	Results must have the word newsletter in it and either church, temple, or mosque and none of the words sample, example, template and not be from a .com domain

Examples for people searching

- Results for people may have names in a variety of formats
- Ensure your search operators reflect these variations

"micah hoffman" OR

"hoffman, micah" OR

"micah_hoffman" OR

"micah-hoffman" OR

"hoffman micah"

Exercise 2: Search for Yourself

- Open a web browser
- Visit the following sites:
 - **bing.com**
 - **google.com**
 - **duckduckgo.com**
- Search for yourself
- Analyze results



15 Minutes

OSINTing User Names

User Names for OSINT

- We put meaning in our user names
 - Favorite topics
 - Dates
- They can be extracted from or used in email addresses
- We may use the same user name across sites

Example user names:

- BiggestRedSoxFan
- BiggestRedSoxFan1
- RobertLangdon1980
- fuzzybunny123
- DreadPirateRoberts

User name reuse is common

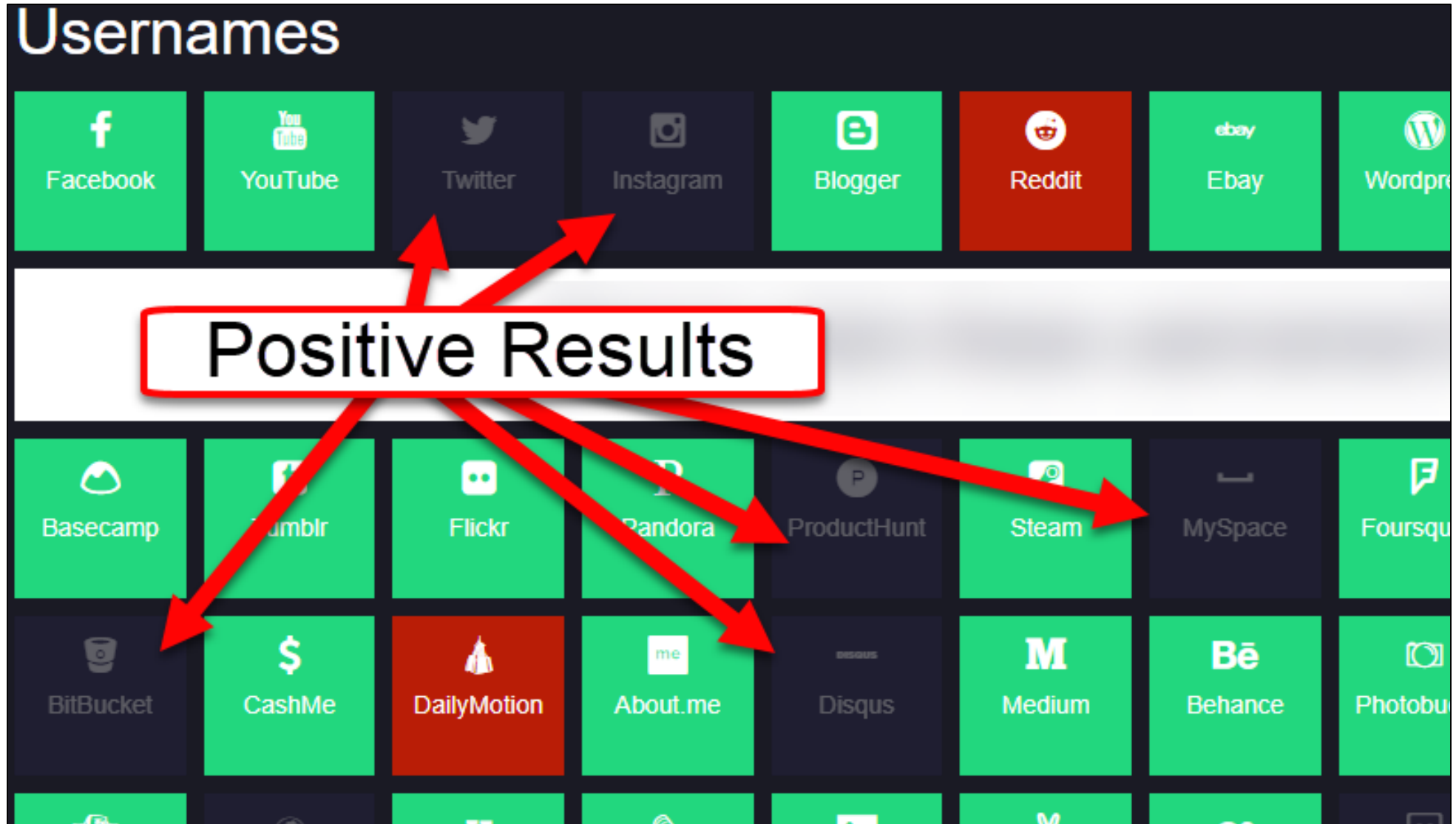
- People use the same user name on multiple websites
 - Facebook: fuzzybunny123
 - Instagram: fuzzybunny123
 - Twitter: fuzzybunny123
- Can we find all these and tie them to a single person?



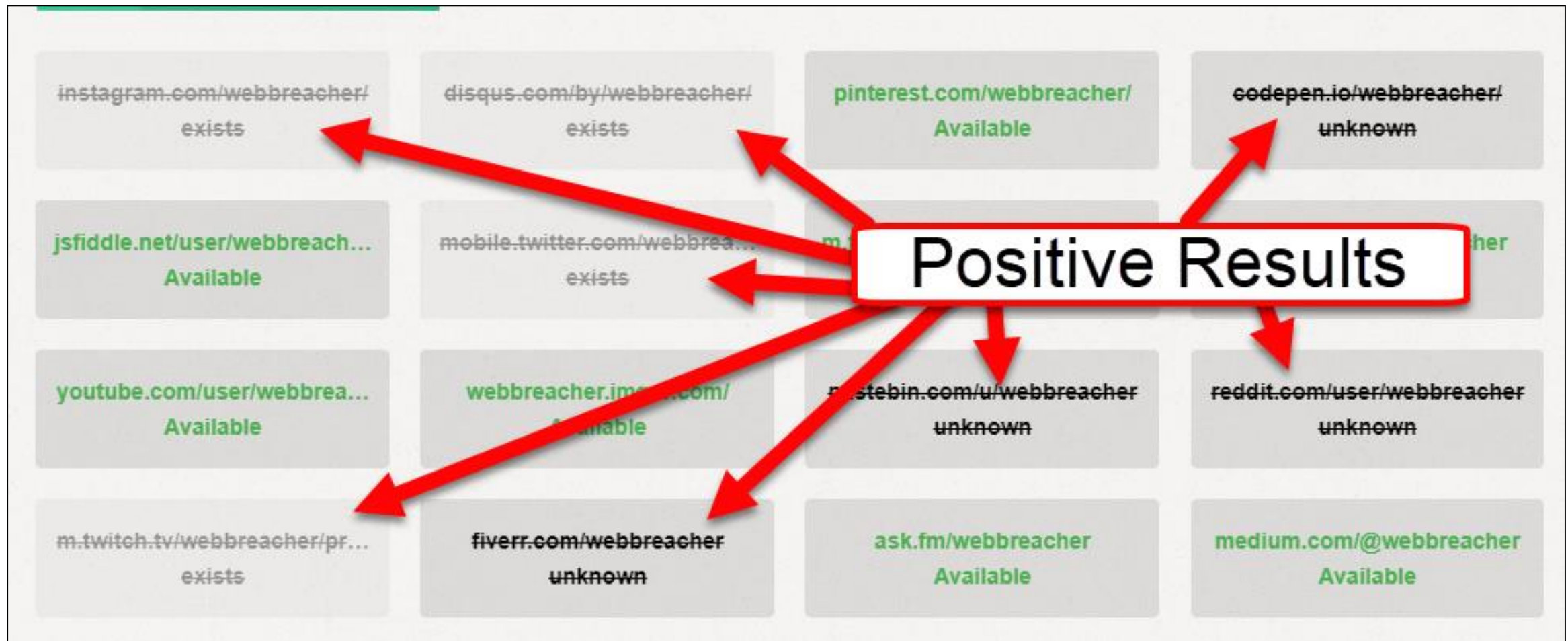
User name checking sites

- There are web sites that allow you to check if a user name exists on a certain web site
 - The purpose is for you to find places where your name is NOT used
 - Then you can create your account and content on that site
- We use it in reverse and look for places where you CANNOT create an account
- Those are sites where the target name was found

<https://namechk.com/>

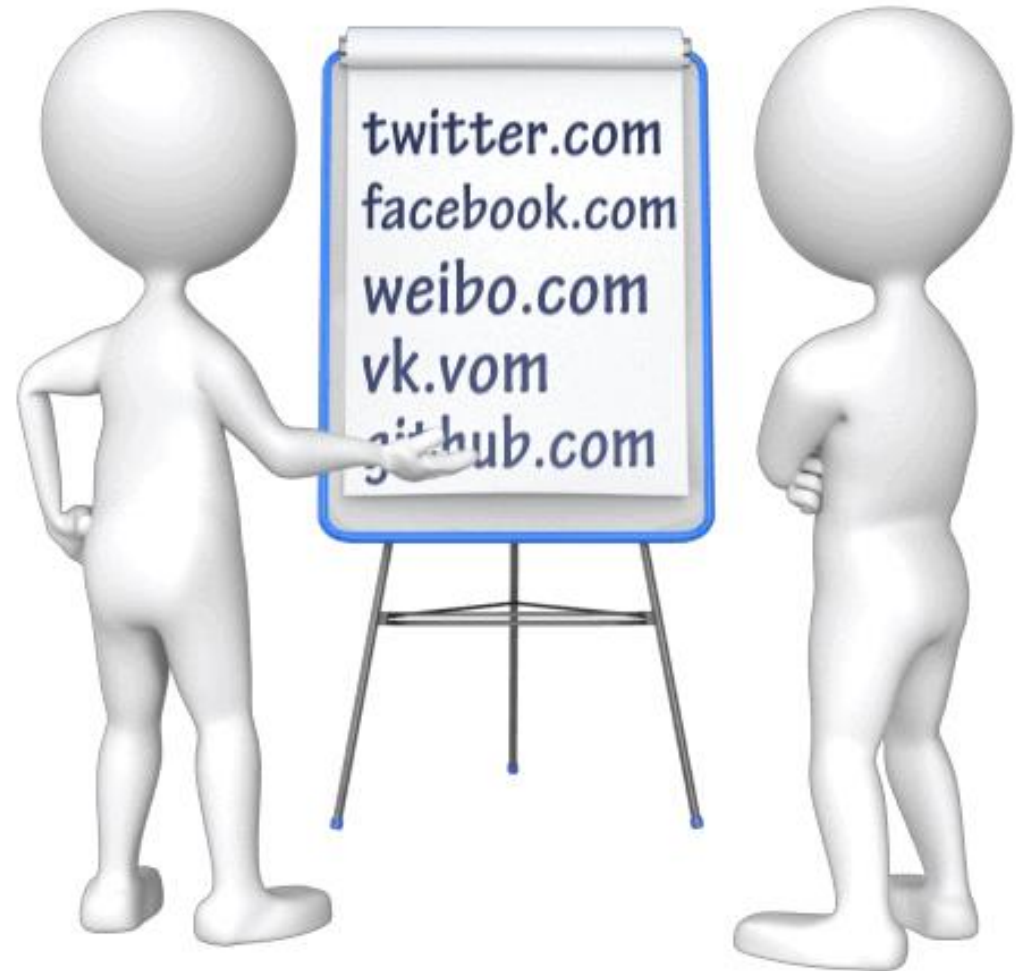


<https://checkuser.org>



Analysis is key

- Running a tool gives you **data**
- Examining it to see if it is relevant and accurate turn that into **information**
- Once we gather all the username on sites, we have to visit them
- Are they you?



Exercise 3: Search for Your User Name

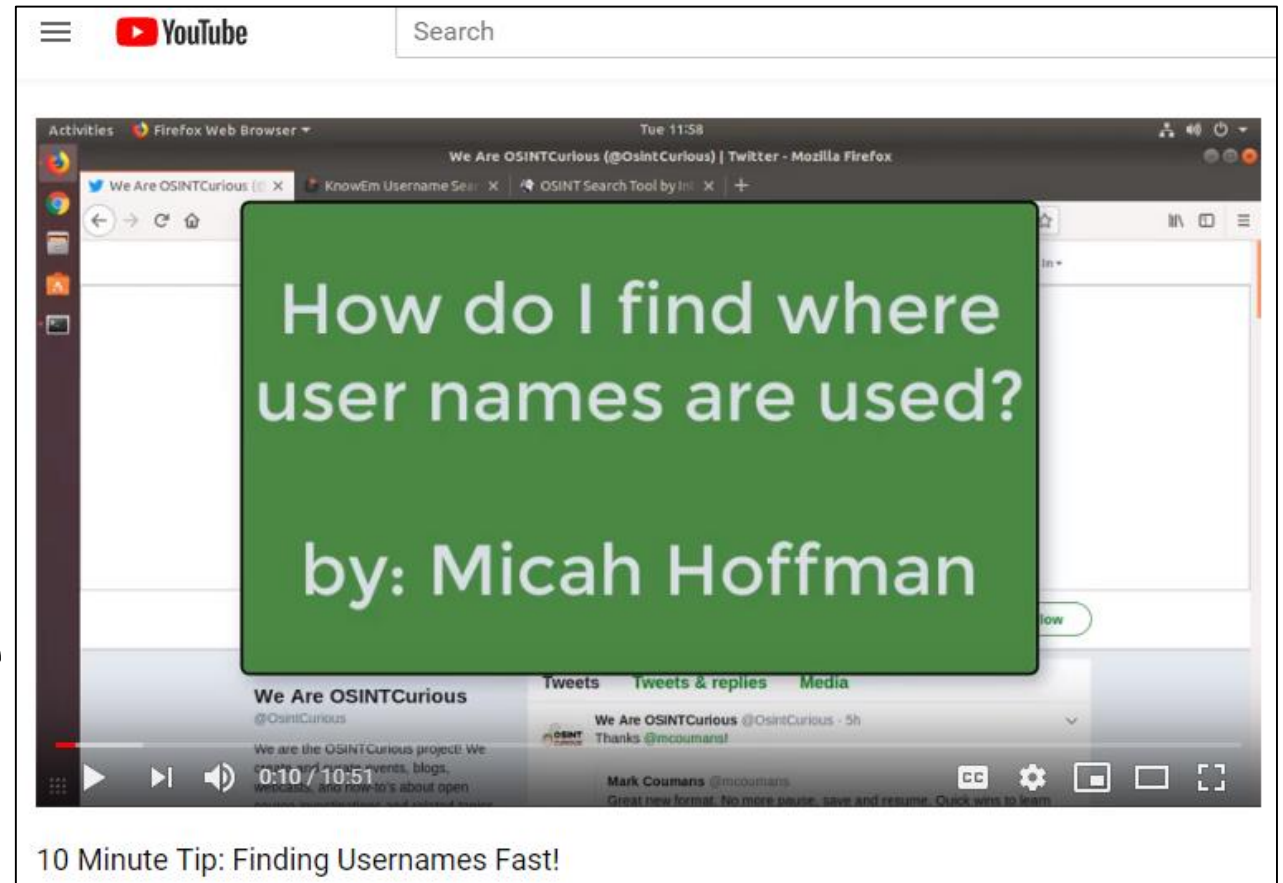
- Open a web browser
- Visit the following sites:
 - **namechk.com**
 - **checkuser.org**
- Search for your user names
- Analyze the results



15 Minutes

Faster, reliable results

- Using tools we can perform these searches across **180+ sites** in < 30 seconds
- We can search for **multiple** user names
- Free video "10 Minute Tip: Finding Usernames Fast!" on <https://osintcurio.us>



<https://youtu.be/Bbrve9OppnM>

Recon-NG Demo of the Profiler Module

Using Breach Data



What is breach data?

- Data stolen from systems
- Usually includes usernames, passwords, and possibly emails
- Can include much more

Untitled Document

100206240	jamie@whitehouse.gov	2oeMb0/Paps=	who i
100206282	jamien@whitehouse.gov	2oeMb0/Paps=	who i
80689318	bob@whitehouse.gov	7xXwhZ1Huu4=	
80796513	g@whitehouse.gov	5djv7ZCI2ws=	
84402942	suzy@whitehouse.gov	sf0EpAAEcRY=	
102927290	donald.rumsfield@whitehouse.gov	hLDe97JLpgY=	
102995650	mazafaka@whitehouse.gov	5djv7ZCI2ws=	
94847063	adobesux@whitehouse.gov	5djv7ZCI2ws=	none

Untitled Document

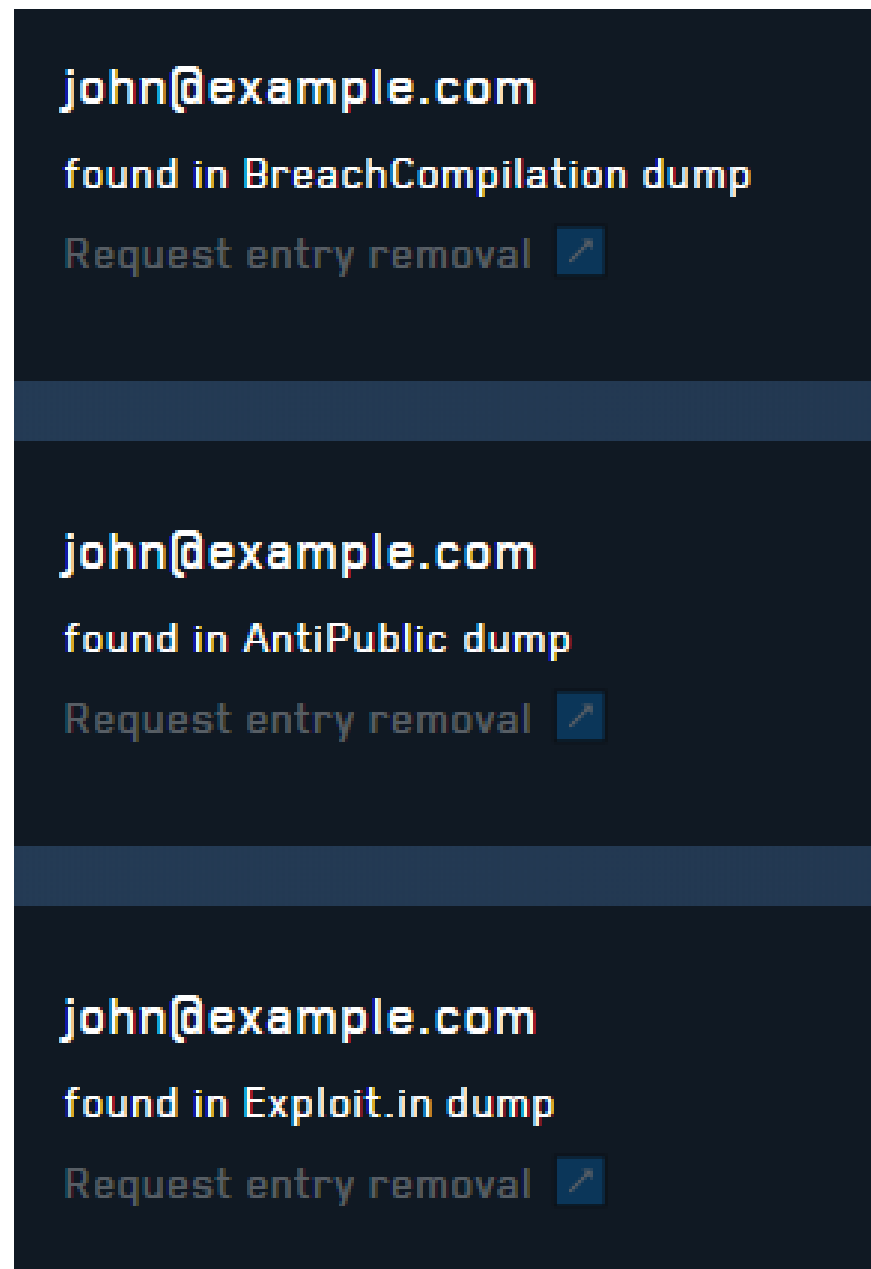
```
barack = Customer('Barack', 'Obama', 'barack@whitehouse.gov', '202456')
white_house_dominos = Store.find_closest_store_to_customer(barack)
dominos_menu = store.get_menu()
dominos_menu.search(Name='Coke') # you can search for items

order = Order.begin_customer_order(barack)
order.add_item("PIZZA1")
order.add_item("COKE20")
```

<https://intelx.io/?s=barack@whitehouse.gov>

Breach Data for OSINT

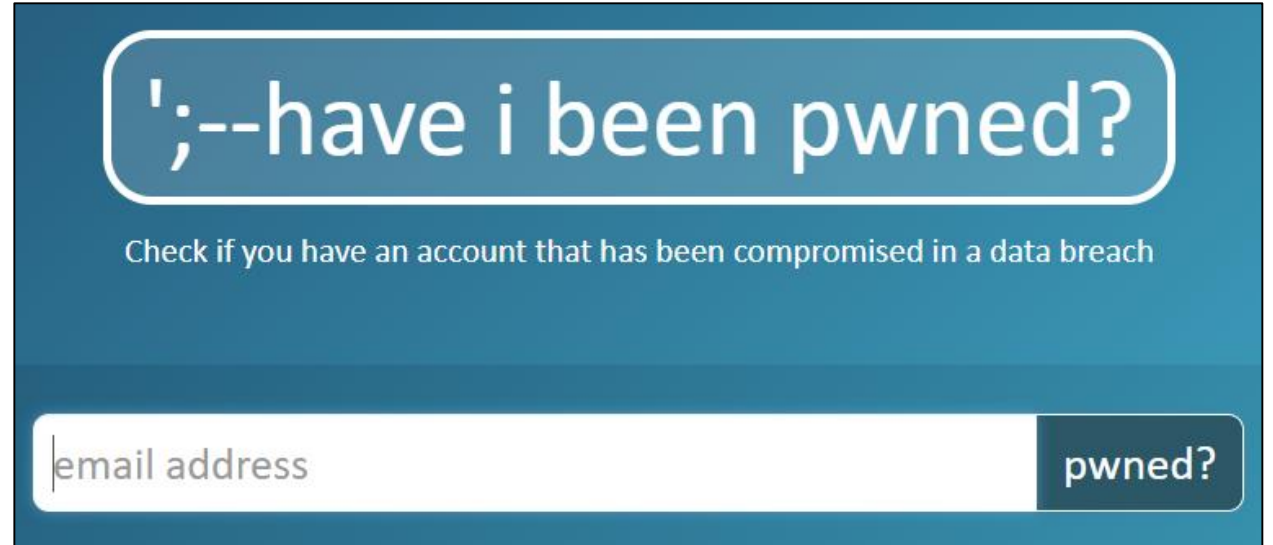
- Check for valid email addresses
- Find same username/email used on multiple sites (Username Reuse)
- Find same password across sites (Password Reuse)



<https://dehashed.com/search?query=%22john%40example.com%22>

How do we access it?

- Free sites
 - haveibeenpwned.com
 - spycloud.com
 - "Dark web"
- Download and normalize the data ourselves
- Pay for access
 - dehashed.com
 - weleakinfo.com

The image shows the homepage of the 'have i been pwned?' website. It has a dark blue background. At the top, there's a white rounded rectangle containing the text 'have i been pwned?' in a white, lowercase, sans-serif font. Below this, in smaller white text, it says 'Check if you have an account that has been compromised in a data breach'. At the bottom, there's a white input field with the placeholder text 'email address' and a dark blue button with the text 'pwned?' in white.

<https://haveibeenpwned.com/>

Is it ethical to use?

- Data stolen from systems
- Attackers use it all the time
- What is our ethical responsibility to the victims (website stolen from and users)?



Exercise 4: Search for Yourself on Breach Data Site

- Open a web browser
- Visit the following sites:
 - **haveibeenpwned.com**
- Search for your user names
- Analyze the results



10 Minutes

Demo of Dehashed.com



Wrap-up

This is a portion of what we do

- Professional OSINT cases can take weeks or months
- We used only free sources
- What if you had funding and much more time?
- [bellingcat.com](https://www.bellingcat.com) does



<https://www.bellingcat.com/news/mena/2019/07/11/afrin-incidents-of-desecration-and-destruction-of-cultural-sites/>


OSINT workshop outcomes - Exercise 1

- You searched for yourself on multiple search engines
- Find anything "interesting"?
- Find anything you wish you hadn't?
- **Action - Try to remove your data from the Internet**
- Resources:
 - <https://inteltechniques.com/data/workbook.pdf>
 - <https://the.osint.ninja/optoutdoc>
 - Search engines

OSINT workshop outcomes - Exercise 1

- You searched for yourself on multiple search engines
- Find anything "interesting"?
- Find anything you wish you hadn't?
- **Action - Try to remove your data from the Internet**
- Resources:
 - <https://inteltechniques.com/data/workbook.pdf>
 - <https://the.osint.ninja/optoutdoc>
 - Search engines

OSINT workshop outcomes - Exercise 3

- You searched for your user names
 - Find anything "interesting"?
 - Find anything you wish you hadn't?
- 
- The logo for Namech_k, featuring the text "Namech_k" in white on a dark blue background. The "k" is stylized with a green underline.
- **Action - Segment your personal and work lives**
 - Use different user names for each type of account
 - Personal: **fuzzybunny123**
 - Work: **micahhoffman**
 - Use different profile images/avatars on the different types of accounts

OSINT workshop outcomes - Exercise 4

- You searched for yourself on haveibeenpwned.com
- Did you find your email address was in a breach?
- **Action 1 - Set up monitoring**
 - Use the "Notify Me" link to receive alerts in the future
- **Action 2 - Change breached account passwords**
 - Any account found in the breach should have password changed
 - Reused breached email and password? Change those too



<https://haveibeenpwned.com/>

Want more OSINT?

The OSINTCurious Project

<https://osintcurio.us>

- Blog posts
- 10 minute OSINT videos
- Bi-weekly
webcast/podcast
- Free!!!



**We are
OSINTCurio.us**

Want 36 hours of OSINT?

SANS SEC487: Open Source Intelligence Gathering and Analysis

<https://sans.org/sec487>

- 6 days of OSINT
- Over 23 labs

SEC487: Open-Source Intelligence (OSINT) Gathering and Analysis SANS Crystal City 2019 Arlington, VA John TerBush	Aug 5, 2019 - Aug 10, 2019
SEC487: Open-Source Intelligence (OSINT) Gathering and Analysis SANS Prague August 2019 Prague, Czech Republic Michael Murr	Aug 12, 2019 Aug 17, 2019
SEC487: Open-Source Intelligence (OSINT) Gathering and Analysis SANS Virginia Beach 2019 Virginia Beach, VA David Mashburn	Aug 19, 2019 Aug 24, 2019
SEC487: Open-Source Intelligence (OSINT) Gathering and Analysis SANS Tampa-Clearwater 2019 Clearwater, FL Micah Hoffman	Aug 25, 2019 Aug 30, 2019
SEC487: Open-Source Intelligence (OSINT) Gathering and Analysis SANS Network Security 2019 Las Vegas, NV Micah Hoffman	Sep 9, 2019 - Sep 14, 2019

Questions?

Micah Hoffman

@WebBreach (Twitter)

micah@spotlight-infosec.com

<https://github.com/webbreacher/presentations>

