OSINT IN TACTICAL INVESTIGATIONS – Class Handout

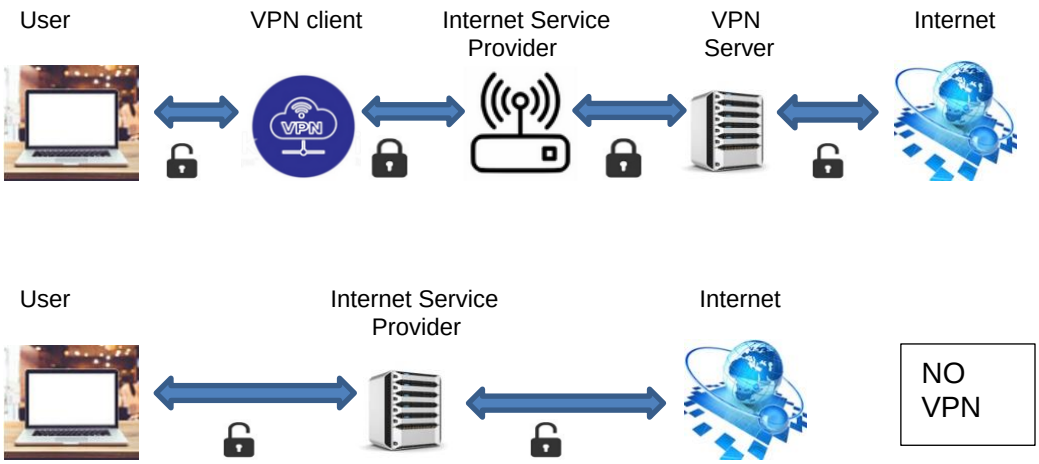
Instructor:	**Michèle Stuart**
	JAG INVESTIGATIONS INC.
	18521 E Queen Creek Road, #105-442 Queen Creek, Arizona 85142
	(480) 703-9740 CELL
	msjag@hushmail.com
	www.jaginvestigations.com Twitter: MSJAGINV

BEFORE WE SEARCH - just a few things

ANONYMIZERS will help access the internet while protecting your personal information from disclosure. An anonymizer protects all of your computer's identifying information while it surfs for you, enabling you to remain at least one step removed from the sites you visit. Before getting online, make sure your devices (computers, tablets, **cell phones**) all have a VPN running on them. A good strong VPN will anonymize and encrypt internet traffic. Do NOT use FREE VPNs.

Excellent article in regards to "Everything You Need to Know":
https://restoreprivacy.com/what-is-vpn/

HOW A VPN WORKS:



https://restoreprivacy.com/best-vpn/
https://www.perfect-privacy.com/
https://nordvpn.com/
https://vpnarea.com/front/
https://www.privateinternetaccess.com

Additional information if you would like more information: https://thebestvpn.com

Here is an article for **Best Secure Email Providers**: https://restoreprivacy.com/secure-email/

ANONYMOUS CREDIT CARDS: **www.privacy.com**

2nd phone numbers: **https://mysudocom**

Block invisible trackers: www.eff.org/privacybadger
www.ghostery.com

ACTIONABLE INTELLIGENCE: We need to define information that rotates around the subject of the research. Family, friends, work, education, sporting activities and hobbies as well as current and/or old addresses and telephone numbers. Remember to run your name through these sites and remove as much information as possible. You will need to look for the OPT OUT link or click on the PRIVACY link and look for opt out information.

Example:

www.truepeoplesearch.com
www.fastpeoplesearch.com
www.familytreenow.com
www.advancedbackgroundchecks.com
https://www.melissa.com/v2/lookups/
www.nuwber.com (shows full date of births sometimes)

www.amazon.com/wedding/search
www.amazon.com/baby-reg/search-results

Remember….
Not everything we see is the truth. There are sites that create AI generated pictures such as:

www.thispersondoesnotexist.com
https://generated.photos/#
https://www.morphthing.com
There are also a popular apps called “FACEAPP” and “REFACE”

FAKE posts – we always need to verify any posts or screen shots
http://fakepostgenerator.com
www.fakenamegenerator.com
www.fakemailgenerator.com

IDENTIFY A GMAIL USER / OTHER EMAILS AND ASSOCIATED ACCOUNTS:

https://tools.epieos.com/google-account.php

HASHTAGS:
Hashtags are an important tool to follow conversations and associations.
www.hashatit.com

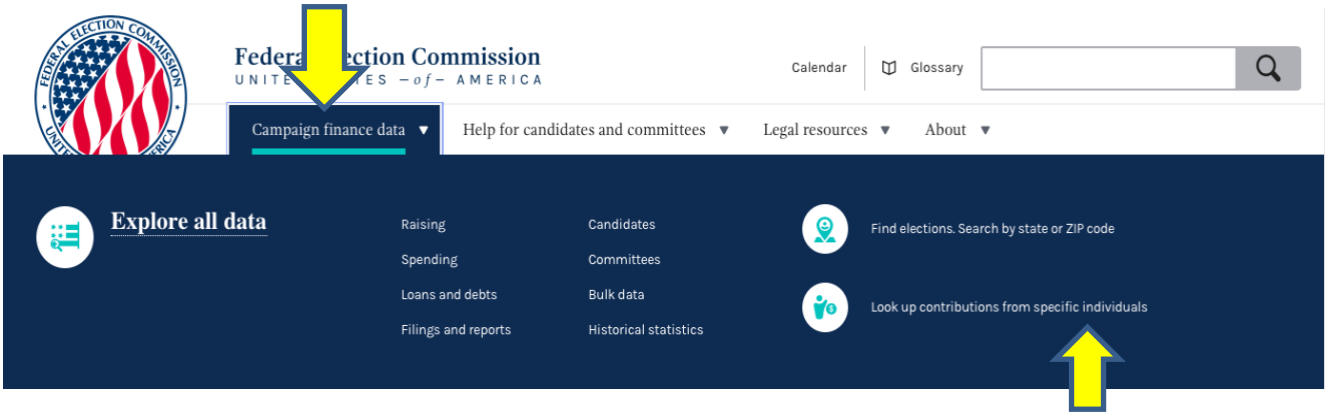
Databreach Information:
As shown in class, dehashed is an invaluable tool in being able to run numbers, ip addresses, names, email addresses, physical addresses, usernames, domain names ect.

www.haveibeenpwned.com
www.dehashed.com

Torrent downloads by IP addresses: https://iknowwhatyoudownload.com/en/peer

LET'S LOOK 'OUTSIDE THE BOX' – using a few sites that aren't normally thought about to ascertain information.

WWW.FEC.GOV This is for FEDERAL contributions



Click on "Campaign Finance Data" then click over on the right-hand side "Look Up contributions from a specific individual".

Then over on the left-hand side you can now run by a subject name (Last name, first name), occupation, employer. You can also use indicators such as zip code or city. ***Also make sure to check on the DATES as they run only in two-year increments.***

Now although this is where you search for political contributions, this is NOT what we care about. What we are looking at is the ability to utilize this site to ascertain information on identifying several things. First: who works for a company – By looking over to the left side you will see Employer. This is where you can enter the name ie… Boeing. You will then get a result of everyone who has listed their employment as Boeing through the entire US. If you need to narrow search, look right above and you will see zip code or city. You can also look for OCCUPATION. Also, remember if you have a subject and you can't find their social media, you can use the employer search to identify people that may work with your subject of research. This will allow us to now search for THEIR social media accounts that may then identify our subject via connections.

Remember once the results come up, click on the arrow on the right-hand side, then click on the 'open original image'. This will normally provide you subject's home address and employment information.

MAKE SURE TO ALWAYS DELETE YOUR ORIGINAL SEARCH BEFORE RUNNING ANOTHER SEARCH!

PPP searches:

https://openpayrolls.com/ppp-data

www.federalpay.org/paycheck-protection-program

www.small-business-forum.net/pppchecker.php

https://covidbailouttracker.com

Google

MAKE SURE THE SITES ARE SAFE:

https://sitecheck.sucuri.net/
https://safeweb.norton.com

https://www.google.com/advanced_search - create multiple searches

Google Dorking:

www.ma-no.org/en/security/google-dorks-find-interesting-data-search-like-hacker
https://ahrefs.com/blog/google-advanced-search-operators/

Usernames:

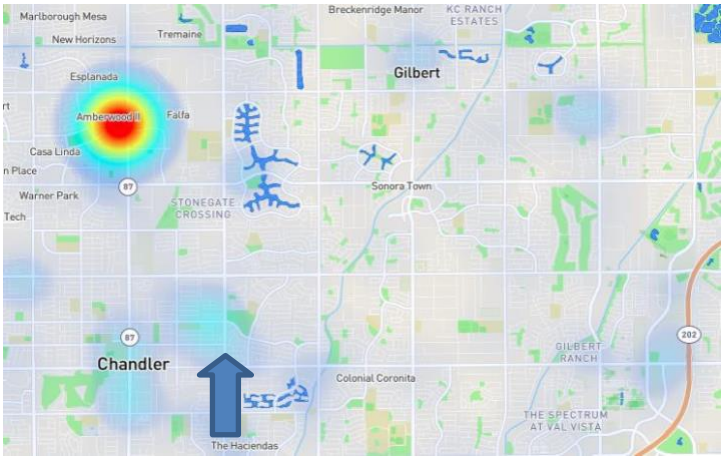
www.whatsmyname.app
www.checkusernames.com
www.knowem.com
www.namecheckr.com

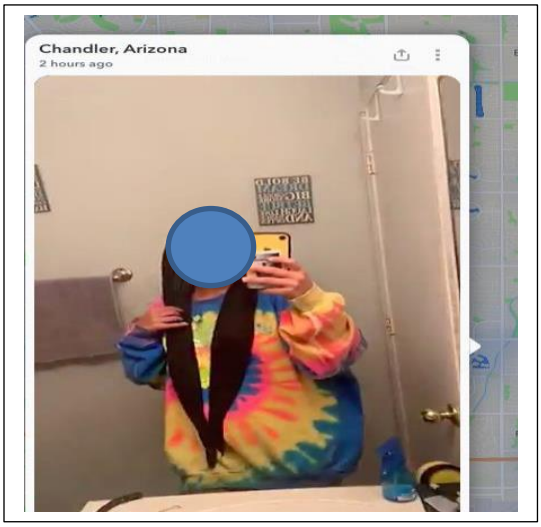
SNAPCHAT:

www.map.shapchat.com

Snapchat released a public map that anyone can search without having Snapchat. Stories last 24 hours. Depending on the privacy setting, you may be able to discover snap stories on the public map.
SNAP MAP AND DOWNLOADING VIDEO

www.map.snapchat.com





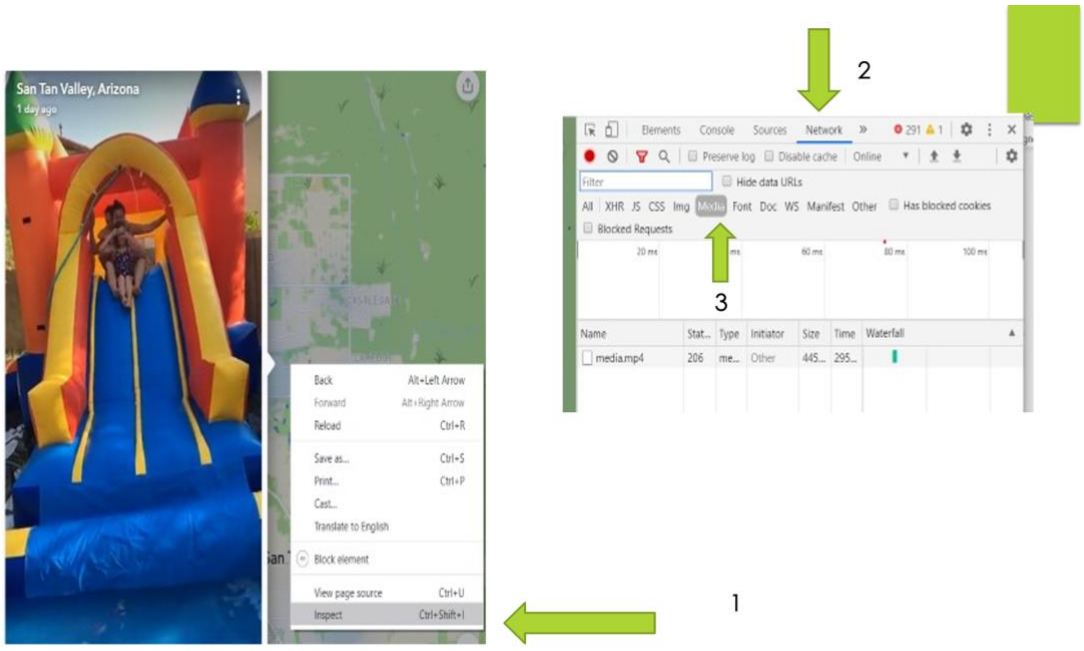
Clicking on an area will bring up a story. Make sure to come in close to the location. Once you have viewed the video - click on the URL and copy it. In the URL you will find the LAT / LONG imbedded into it. NOTE: Make sure to come in as close as possible to get the closest lat / long. Results can be exact or within a few hundred yards. Remember if you look at a different area, you will need to REFRESH the page to get the lat/long to that video.

You will find several sites that will do this and give you the address. Then you can run the address in Google to see location / house / business. Also run the lat long to make sure it corelates.

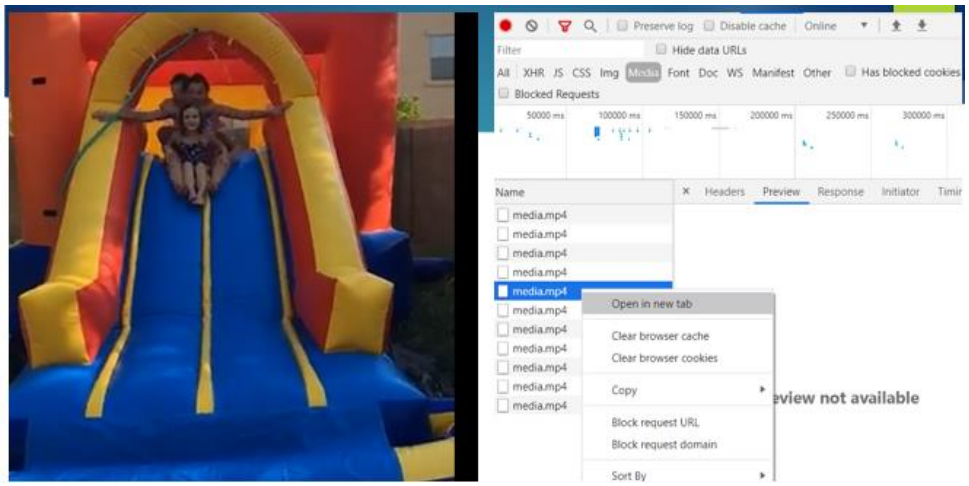
If they have customized their settings and 'ghosted' themselves, their stories will not show on map.

Downloading a Snapchat Video that is viewed on the snap map.

You will need to use the developer's tools for this. Once you open a video, right click and choose "inspect" - then click on Network, then click Media. Reclick on the video you want (remember to click on the first vide right side – you will see an arrow – and you can scroll through all videos / snaps from that area) You will see it populate with media.mp4. If there are more than one video in a location, while the next video plays it will add another line of the media.mp4. Right click the MP4 you want and open in a new tab. After opening, depending on browser, the video will have three dots on the bottom right – click and you will see 'download' or right click and choose 'save as'.

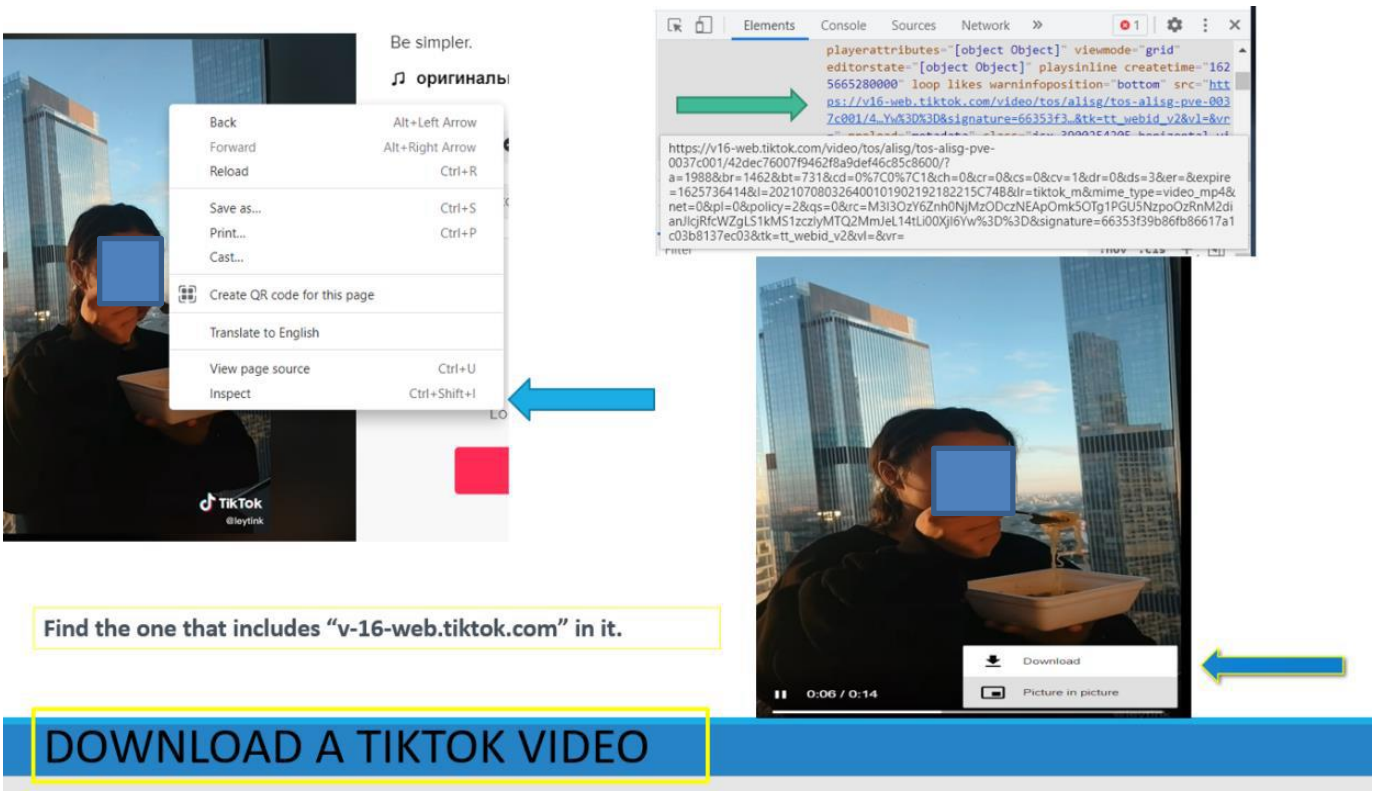


The video 'link' will show under Name column (as seen below). Double click on it (or right click on link) and open in NEW tab.



The video will open. There will be three little dots on bottom right. Click and you will see 'download'.

Same procedure for TIKTOK videos. Right click, click “inspect” or “inspect element” then this time look under **elements** for the URL starting with v-16-web.tiktok.com. Right click and open in new tab. The video will open – click on the three dots on bottom right and hit download.



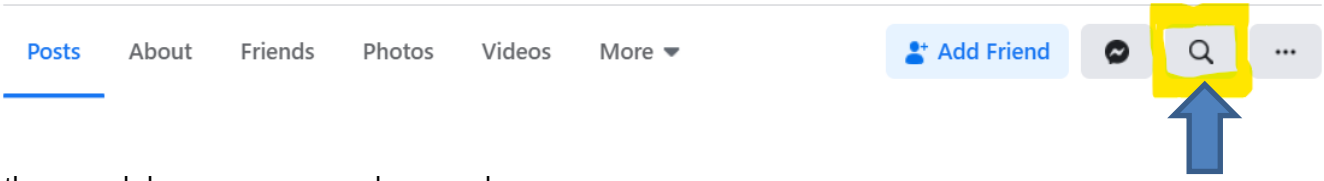
**** You can also just right click on video and save video as.** The above listed way allow You to view the video in slower or faster speeds.

To search for tags: www.tiktok.com/tag/shooting (change shooting with whatever tag you want)

To verify time and date of video: https://dfir.blog/unfurl or www.mavekite.com

FACEBOOK

We all know Facebook is constantly changing their settings and search abilities. Currently, by running searches in the search box, a list of categories will show up on the left-hand side that will allow some search manipulations. However, one of the newer items is the "search" feature within the user profile. Additionally, it will search whatever term you are using in open public profiles.

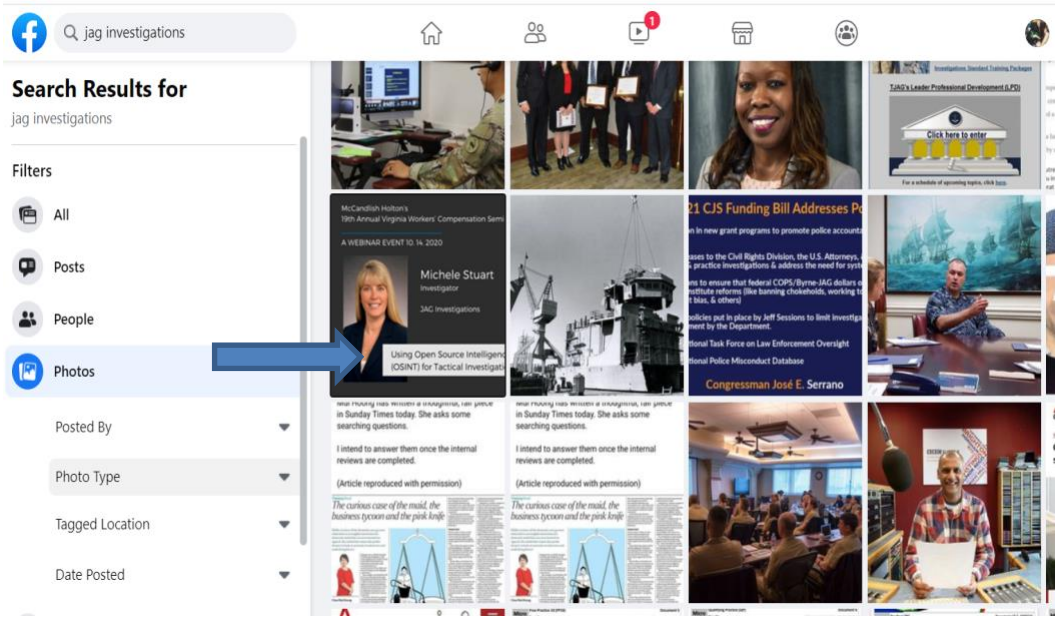


In the search bar you can search several ways:

* By their own name (as this may find a public post elsewhere)
* You can search by keywords through their profile to help limit time spent scrolling
* Search by family names

ROSETTA:

Facebook now has given us the ability to search text WITHIN a picture. Such as an email address or name of a company. You will run this search in the 'normal' Facebook search bar, then click on photos (left hand side)



Twitter geolocation search: Only good if the profile is public and they have location on.

www.geosocialfootprint.com - last 200 tweets on a map (this is a finicky site – goes up and down)

https://keitharm.me/projects/tweet/ (Up to the last 3200 tweets on a map)

www.socialbearing.com is an analytical tool and allows the ability to see tweets in a 'fanned' out viewability.

Remember Twitter has an advanced search site also you can search for tweets by geo-location by running this search in the search bar in twitter. Remember you can use www.latlong.net or google maps to reverse an address and get lat / long.

Geocode:33.221161,-111.758911,2km OR

Near: 33.221161,-111.758911 within:3km

Miscellaneous

Enterprise / Hertz / Alamo - scroll to get / print a receipt
You will need last name and drivers license number.

DOG tags – google: pet license renewal Maricopa county (obviously put the county in your want)

www.mindmap.com
http://free-timeline.com

IF YOU WOULD LIKE ADDITIONAL TRAINING, PLEASE CONTACT ME ANYTIME AT:

Msjag@hushmail.com ***or 480-703-9740***