487.3
Social Media, Geolocation, and Imagery

PLEASE READ THE TERMS AND CONDITIONS OF THIS COURSEWARE LICENSE AGREEMENT ("CLA") CAREFULLY BEFORE USING ANY OF THE COURSEWARE ASSOCIATED WITH THE SANS COURSE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU (THE “USER”) AND SANS INSTITUTE FOR THE COURSEWARE. YOU AGREE THAT THIS AGREEMENT IS ENFORCEABLE LIKE ANY WRITTEN NEGOTIATED AGREEMENT SIGNED BY YOU.

With the CLA, SANS Institute hereby grants User a personal, non-exclusive license to use the Courseware subject to the terms of this agreement. Courseware includes all printed materials, including course books and lab workbooks, as well as any digital or other media, virtual machines, and/or data sets distributed by SANS Institute to User for use in the SANS class associated with the Courseware. User agrees that the CLA is the complete and exclusive statement of agreement between SANS Institute and you and that this CLA supersedes any oral or written proposal, agreement or other communication relating to the subject matter of this CLA.

BY ACCEPTING THIS COURSEWARE, YOU AGREE TO BE BOUND BY THE TERMS OF THIS CLA. BY ACCEPTING THIS SOFTWARE, YOU AGREE THAT ANY BREACH OF THE TERMS OF THIS CLA MAY CAUSE IRREPARABLE HARM AND SIGNIFICANT INJURY TO SANS INSTITUTE, AND THAT SANS INSTITUTE MAY ENFORCE THESE PROVISIONS BY INJUNCTION (WITHOUT THE NECESSITY OF POSTING BOND) SPECIFIC PERFORMANCE, OR OTHER EQUITABLE RELIEF.

If you do not agree, you may return the Courseware to SANS Institute for a full refund, if applicable.

User may not copy, reproduce, re-publish, distribute, display, modify or create derivative works based upon all or any portion of the Courseware, in any medium whether printed, electronic or otherwise, for any purpose, without the express prior written consent of SANS Institute. Additionally, User may not sell, rent, lease, trade, or otherwise transfer the Courseware in any way, shape, or form without the express written consent of SANS Institute.

If any provision of this CLA is declared unenforceable in any jurisdiction, then such provision shall be deemed to be severable from this CLA and shall not affect the remainder thereof. An amendment or addendum to this CLA may accompany this Courseware.

SANS acknowledges that any and all software and/or tools, graphics, images, tables, charts or graphs presented in this Courseware are the sole property of their respective trademark/registered/copyright owners, including:

AirDrop, AirPort, AirPort Time Capsule, Apple, Apple Remote Desktop, Apple TV, App Nap, Back to My Mac, Boot Camp, Cocoa, FaceTime, FileVault, Finder, FireWire, FireWire logo, iCal, iChat, iLife, iMac, iMessage, iPad, iPad Air, iPad Mini, iPhone, iPhoto, iPod, iPod classic, iPod shuffle, iPod nano, iPod touch, iTunes, iTunes logo, iWork, Keychain, Keynote, Mac, Mac Logo, MacBook, MacBook Air, MacBook Pro, Macintosh, Mac OS, Mac Pro, Numbers, OS X, Pages, Passbook, Retina, Safari, Siri, Spaces, Spotlight, There’s an app for that, Time Capsule, Time Machine, Touch ID, Xcode, Xserve, App Store, and iCloud are registered trademarks of Apple Inc.

PMP and PMBOK are registered marks of PMI.

SOF-ELK® is a registered trademark of Lewes Technology Consulting, LLC. Used with permission.

SIFT® is a registered trademark of Harbingers, LLC. Used with permission.

Governing Law: This Agreement shall be governed by the laws of the State of Maryland, USA.

SEC487.3 | Open Source Intelligence (OSINT) Gathering and Analysis

SANS

Social Media, Geolocation, and Imagery

Welcome to SEC487 Open Source Intelligence Gathering and Analysis!

TABLE OF CONTENTS	PAGE
People Search Engines	3
Facebook Analysis	24
LinkedIn Data	66
Instagram	80
Twitter Data	104
Geolocation	137
Imagery and Maps	162

487.3 Table of Contents

This table is a reference for you to quickly move to certain topics in this 487.3 book.

Course Roadmap

- Day 1: Foundations of OSINT
- Day 2: Gathering, Searching and Analyzing OSINT
- **Day 3: Social Media, Geolocation, and Imagery**
- Day 4: Networks, Government, and Business
- Day 5: The Dark Web, Breach Data, and International Issues
- Day 6: Capstone: Capture (and Present) the Flags

SOCIAL MEDIA, GEOLOCATION, AND IMAGERY

1. **People Search Engines**
2. Facebook Analysis
3. LinkedIn Data
4. Instagram
5. Twitter Data
6. Geolocation
7. Imagery and Maps

This page intentionally left blank.

Using People Search Engines

Use these engines to search on:

- Names
- Addresses
- Phone numbers
- User names/Social Media

Record all the results for aggregation

Choose relevant pieces of information from results and perform another search on them

If you searched on "Inigo Montoya" and it returned his address in Spain, search on that address and see what is returned

Using People Search Engines

While general search engines contain a large amount of data about a variety of topics, people search engines focus on...people! Specializing in finding people and information associated with them, such as social media accounts, home addresses, phone numbers, and relatives, people search engines can be a valuable tool to the OSINT analyst. Leveraging one of these engines can save an analyst many hours of work since the backend databases of these engines aggregate information about people and allow us to search through it. These sites allow analysts to enter keywords such as first and last names of a target, approximate geographic location where a target lives/lived, phone numbers, and user names the target may have used in social media accounts.

OSINT researchers may need to provide more specific data to these sites in order to refine their searches in case multiple people are returned in the results. For instance, searching for "John Doe" in the New York City area may generate many potential people in the results page. The analyst may need to filter based on age or a more specific location (such as the area of New York City) to find more relevant results.

The two most important tasks that analysts need to perform on these sites are:

1. Record all relevant data about the target for verification and validation.
2. Recognize data points where the analyst can "pivot" and gather more data. A pivot point may be an address or a phone number tied to the target.

Free People Searches

While some people search engines choose to hide most of the data they store about a target, there are several that give it (or some of it) away for free. The following search engines are in this latter category and can be used to gather more data on our targets:

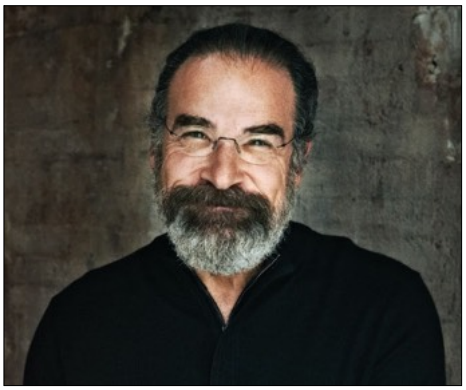
- `peekyou.com`
- `thatsthem.com`
- `truepeoplesearch.com`
- `cubib.com`
- `zabasearch.com`
- `radaris.com`

Each site also has links to "premium" data. So, if you want to pay for data, you have an opportunity to do that while you are compiling the free info!

Josh Huff (@baywolf88) performed some OSINT on the people search engines (https://sec487.info/gw) and found that some appear to be different user interfaces to the same data. Opting out of one of these search engines removed his data from another one that was related to the first.

Searching for Inigo Montoya

Let us find the actor Mandy Patinkin, who portrayed Inigo Montoya in *The Princess Bride*



Searching for Inigo Montoya

To see the power of free people search engines, we will try to locate Mandy Patinkin, the actor who portrayed Inigo Montoya in *The Princess Bride* (you may know him from some of his other acting roles as well).

Images from https://sec487.info/se and https://sec487.info/lr, September 17, 2019.

References:

[1] https://sec487.info/er

[2] https://sec487.info/es

That'sThem Results

Results show details including name, address, phone, and email

Are these the Mandy Patinkin we want?

What would your next step be?

That'sThem Results

Our first people search engine is thatsthem.com. We ran a general search for Mandy Patinkin and received the results above (https://sec487.info/4y). When the scan was run, it gave us two detailed results. We do not know where Mr. Patinkin lives, but since he works in Hollywood circles and is a stage actor in New York, we would suspect that the result on the right, showing a New York address, is more likely our target.

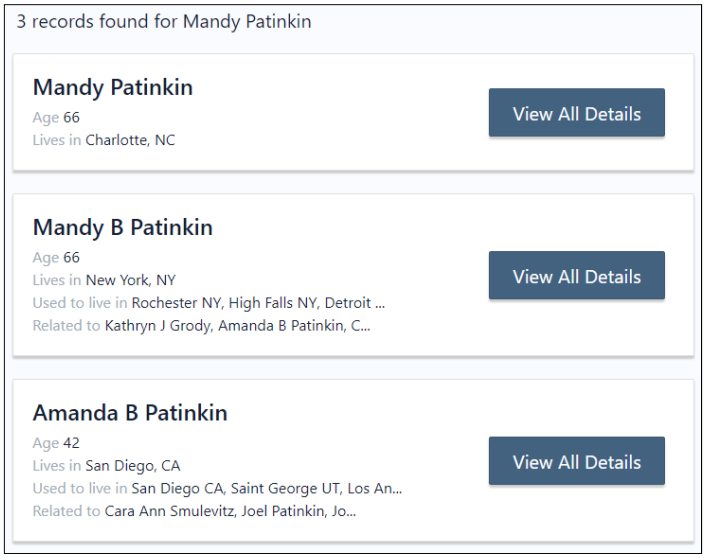
The problem with some of the free people search engines is that some of the data in each record may be about our target. We would need to examine both records and all the details to rule out if they are for our subject or not. To validate this information, we could use other search engines, look for public records that support or refute the data, and map the addresses to see what they looked like.

Images from https://sec487.info/4y, September 17, 2019.

TruePeopleSearch Results

We retrieved three results from truepeoplesearch.com and one of them is clearly not our target

The first entry has promise though, so we click the "View All Details" button



TruePeopleSearch Results

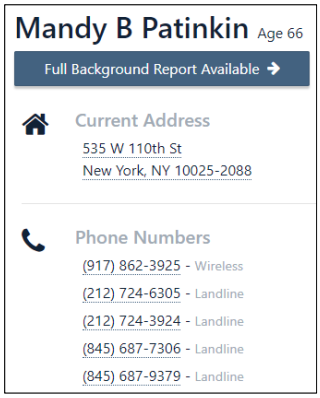
Our next search engine is truepeoplesearch.com. We performed a search for our target (https://sec487.info/50) and have retrieved three results shown above. Two of the results are for "Mandy" Patinkin and one is for "Amanda" (not our target). Of the remaining two, the first entry for a New York resident has approximately the correct age as our target, 66 years old in 2019.

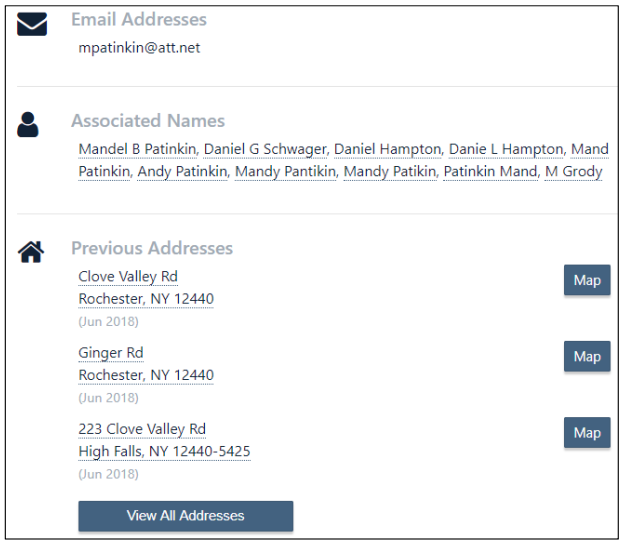
To get more details about that record, we click the "View All Details" button next to the record.

Image from https://sec487.info/50, September 17, 2019.

TruePeopleSearch Results Detail (1)

Looking at the details for the New York resident, we see data that indicates this may be our target





SANS | Open Source Intelligence (OSINT) Gathering and Analysis 9

TruePeopleSearch Results Detail (1)

Clicking on the details for our candidate shows that there is some excellent information in this page. Name, age, address, phone numbers, email, and previous addresses can all be valuable in your OSINT work. We also see some "associated names," including a "Grody," which, according to the Wikipedia page, is the last name of his wife (Kathryn Grody).[1]

Images from https://sec487.info/sc, September 17, 2019.

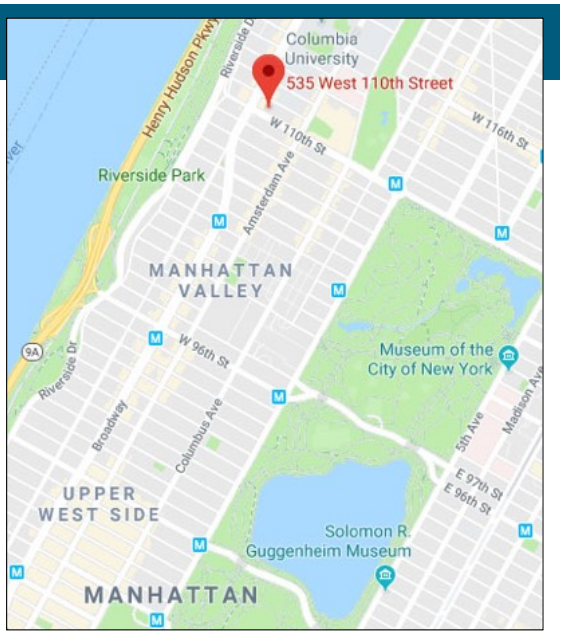
Reference: [1] https://sec487.info/51

TruePeopleSearch Results Detail (2)

Let us use Google Maps to see if the address listed for his current address is possible or probable for a movie star and stage actor

It is 3 blocks from Central Park, in a wealthy neighborhood near Broadway Street

Is this where he lives?



TruePeopleSearch Results Detail (2)

Taking a map-view look at his current address, we see it is in a wealthy part of midtown Manhattan about 3 blocks from Central Park. This looks like it could be his residence and, through extension, the other data about him in the TruePeopleSearch entry could be true.

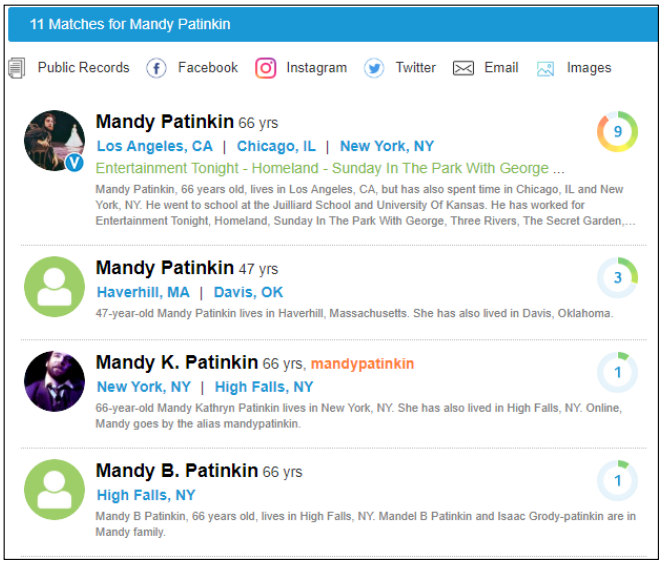
There still can be bad data or incorrect information. For instance, what if this address is not where he lives but where his agent or company has an office? What if this is a rental property that he owns? There are other verifications and validations that we may need to do to further confirm this is where Mandy Patinkin lives. Be careful to use logic and reasoning and not jump to conclusions.

Image from https://sec487.info/sd, September 17, 2019.

peekyou Results

The peekyou.com web site aggregates data from the internet and displays it

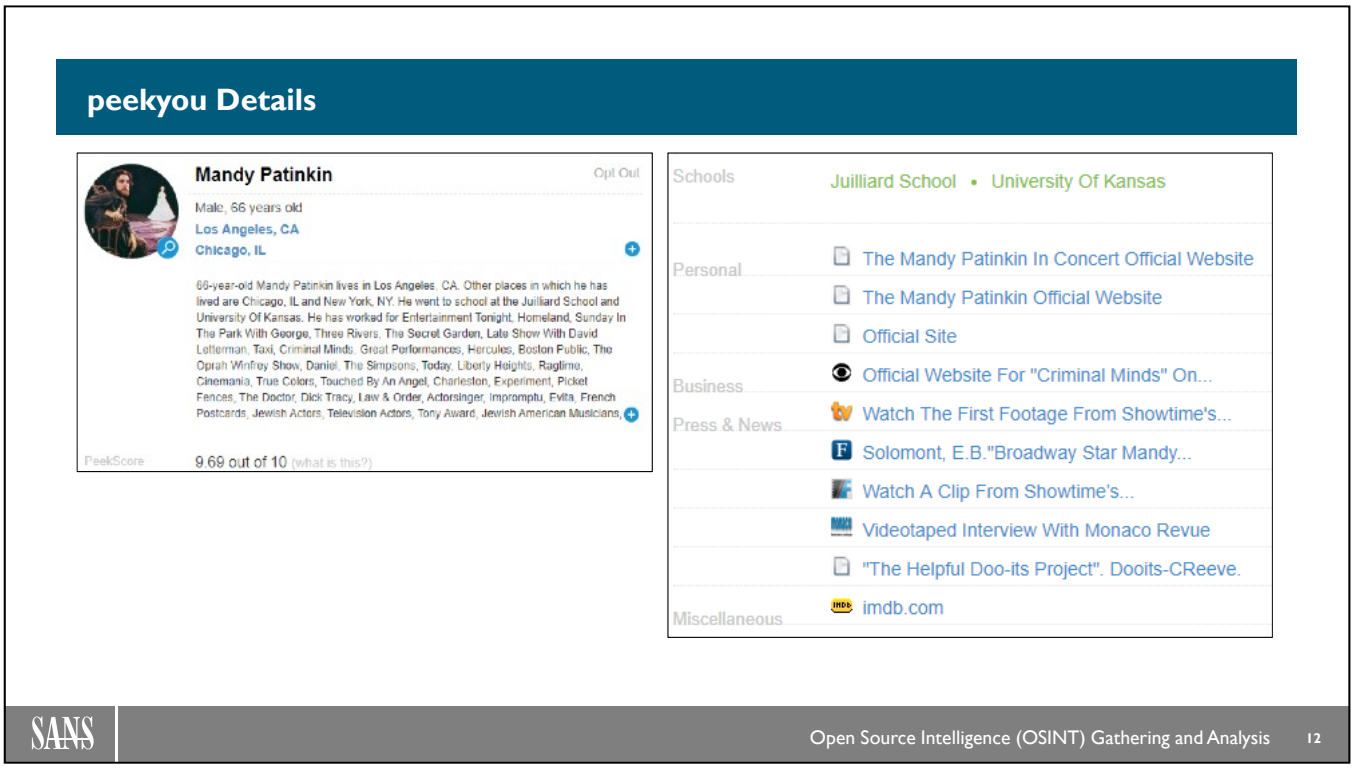
In this case, we see multiple entries that are likely to be our target



peekyou Results

The peekyou.com results are more similar to pipl.com than web sites that just retrieve phone numbers and addresses. It, too, gathers data from around the internet and composes dossiers for each person. With the Mandy Patinkin search (https://sec487.info/55), we see that there are most likely several correct entries for the same person (based upon age, name, and location). You know that we will need to analyze the data in each of the related links to find all the data about our subject.

Image from https://sec487.info/55, September 17, 2019.



peekyou Details

After viewing the data on several of those entries and findings bits and pieces of Mr. Patinkin's life, we hone in on a record that has a large number of correct information and links to other web pages we may use to gather even more data (https://sec487.info/56). The peekyou.com web site gathers data from a variety of online resources. In the above slide, we see personal and business web pages for Mandy Patinkin, an imdb.com link, and other sites.

The more public a person is, the more information will be gathered on this site. For our movie star Mandy Patinkin, there is a huge amount of data. For more private people, there will be less.

Images from https://sec487.info/56, September 17, 2019.

cubib.com

United States public data scraper

Not just people search but also accesses:

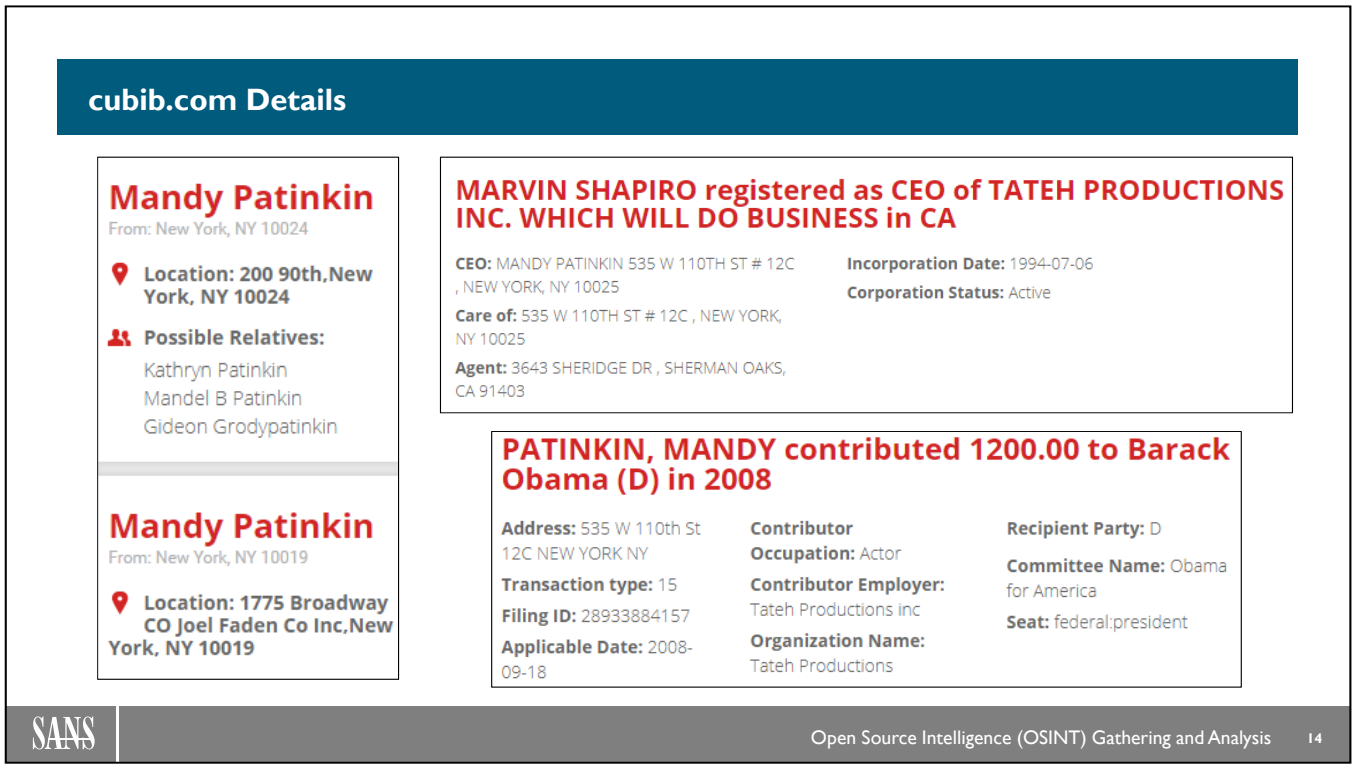
- Campaign contributions
- White House visits
- Marketing information
- Vehicle ownership
- Business registrations

cubib.com

The site https://cubib.com/ accesses public information from sources that are more familiar and interesting than the other sites we have seen. Yes, it tries to retrieve information about your target from "people" databases, showing names, addresses, and phone numbers, but it also taps into databases for United States political campaign contributions (so you can learn who your target supported in previous elections), vehicle ownership, complete with VIN (Vehicle Identification Number),[1] and even examines the White House visitor page to see if a person with your target's name appears on it.

Image from: https://cubib.com/, September 17, 2019.

Reference: [1] https://sec487.info/71



cubib.com Details

Searching for our target, Mandy Patinkin, we see that cubib.com found a donation that someone from our target's address made to the Obama campaign in 2008. Is this helpful to your investigation? Perhaps. It will depend upon the goals of the assessment.

Using this site for other names shows interesting information in the marketing data section. Try searching for "John Smith" and examine the results for interesting content.

Image from: https://cubib.com/, September 17, 2019.

192.com (UK)

Regular search requires credits ($/£) for details

Use "AtoZ" search for more details

Searches electoral rolls and businesses too

https://www.192.com/atoz/people/LAST/FIRST/

192.com (UK)

For people, businesses, and places in the United Kingdom, try the https://www.192.com search engine. While the detailed results usually require registering on the site and some form of payment (the site uses "credits" to purchase reports), we can use inference from some of its displayed data. Performing a regular search on the site will take you to a place where most every click requires payment to proceed. However, there is the "AtoZ" section of the site, which divulges more information for free.

The business listings that it contains give business names, addresses, and phone numbers freely (no payment required). These business listings also sometimes contain hours of operation, website links, and reviews.

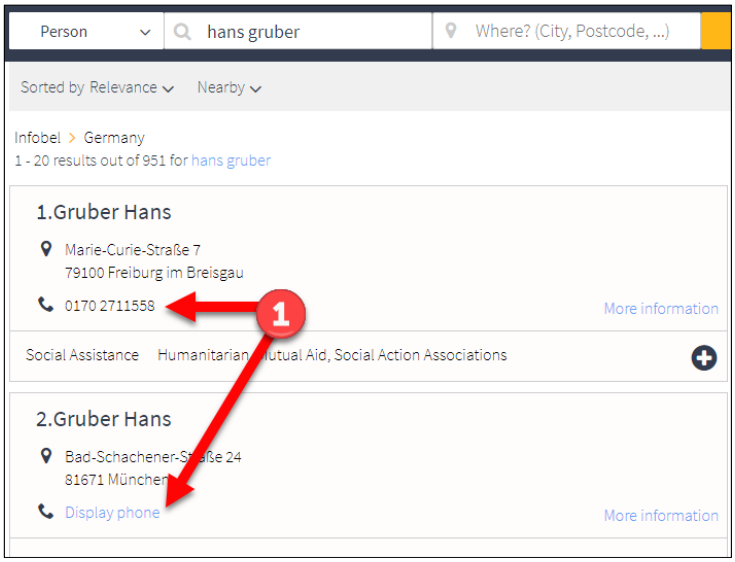
Image from: https://sec487.info/mm, January 3, 2019.

Infobel.com

Some people information depending on target country (including EU)

To see phones, click the links (arrows at 1)

Business data across many regions



Infobel.com

For person and business data in places other than the United States, try the https://www.infobel.com web site. It has large numbers of business listings for countries around the world and, for some of those locations, it displays people data as well. In the slide above, we searched for a person named "Hans Gruber" in Germany. The results show addresses, phone numbers (once you click the "Display phone" link), and other details about these people. Infobel.com is a free web site and requires no authentication for searches.

Image from https://sec487.info/mn, September 17, 2019.

Email Reputation Services - emailrep.io

Checks details about an email address, including:

- Is it a valid email?
- Is it on blacklists?
- Does it have social media accounts associate to it?

Run from web browser or command line using curl

Email Reputation Services - emailrep.io

Might seem odd to add this to the people search section of the class, but the emailrep.io web site takes email addresses and looks them up against various social media platforms. Sure, its main purpose is to evaluate the given email address for its validity, for whether it is malicious or known to send spam emails, and other attributes about it that might make it look more suspicious or malicious.

This free service provides a summary of the results in paragraph format (shown above) and using icons showing which social networks the email address has been located on (arrow 3 above). Unfortunately, it does not show analysts the exact user name on the social media site that uses the email address searched. That exercise is left to the user to figure out.

This site also has a free API that can be accessed using curl or another tool or script. The web page shows how to make the call to their server to retrieve a JSON-formatted response (arrow 4 above).

Image from https://emailrep.io/, September 17, 2019.

Paid Consumer-Level People Search Engines

Just as the amount and quality of data found on free people search engines varies, that is also the case when we examine the paid people search engines. These web sites will charge either monthly fees or one-time fees to access more details about the targets you search for. The data can be rich and helpful or downright disappointing. This is sometimes a factor of the target and whether they may have chosen to remove their data from some of these sites ("opting out" of having their data displayed), or perhaps the target has only a few pieces of information to find. In either case, you and your employer will need to examine if you need to use these services and which are right for your business.

Some of these paid sites include:

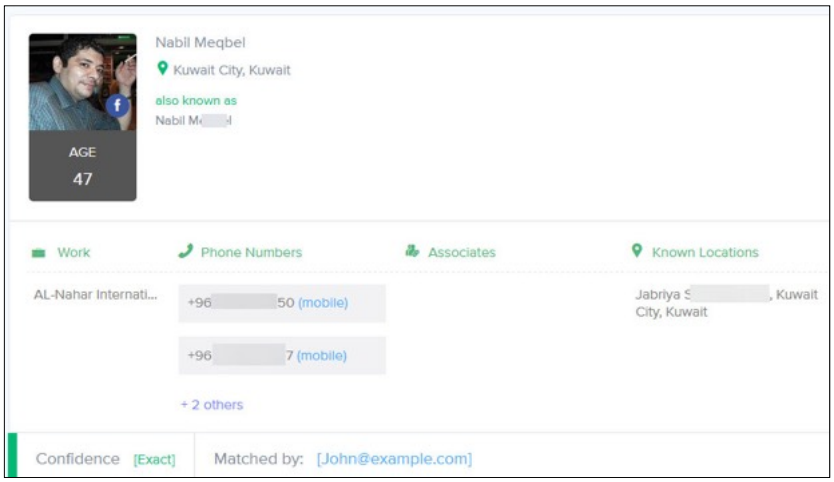
- pipl.com
- intelius.com
- spokeo.com
- beenverified.com
- skopenow.com

Skopenow.com

Skopenow.com is a paid, international people search engine

Search for email, phone, name, username, location and more

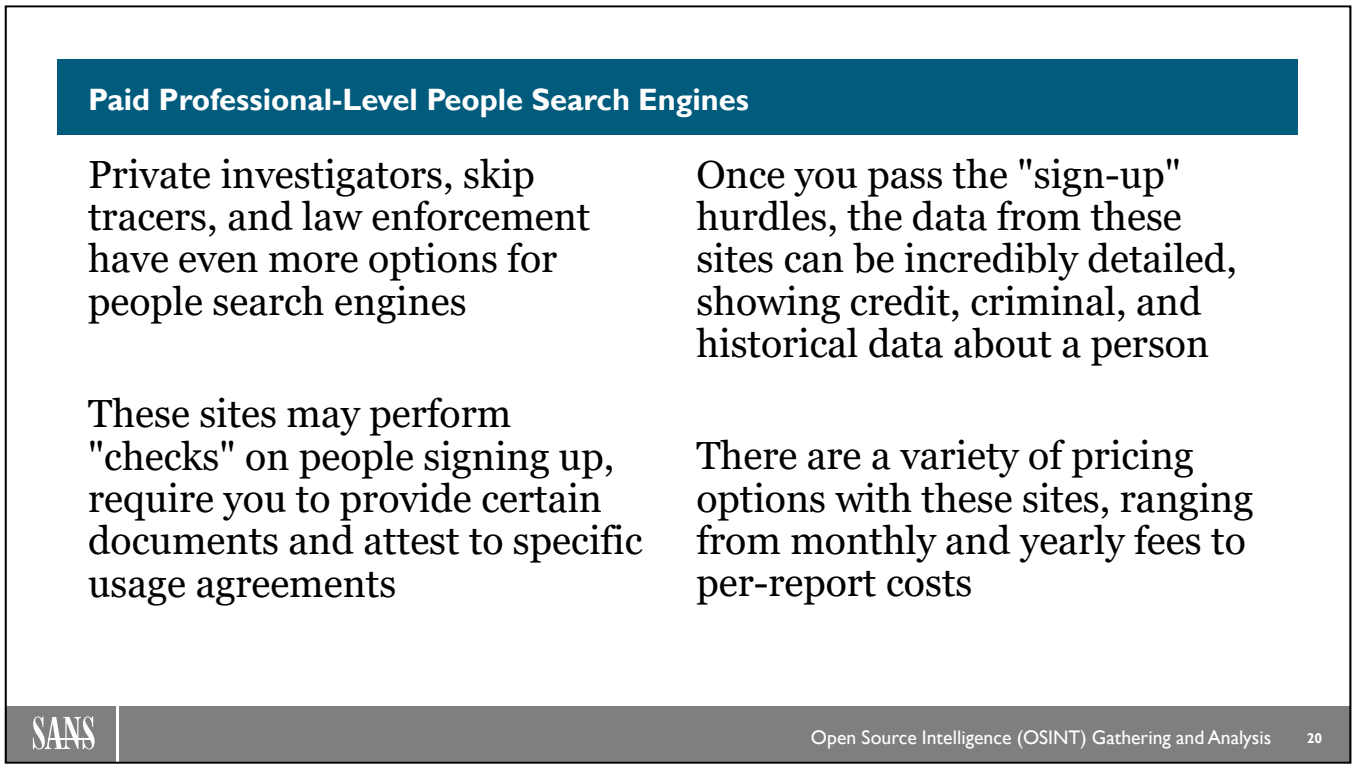
Refine data by adding details



Skopenow.com

This paid, international people search engine, which allows searching based upon names, phone numbers, email addresses, and user names, scrapes data from a variety of public sources. Social media sites, census data, and other public resources are collected and normalized in this system. Once initial records are discovered, this search engine allows users to add associates, monitor the targets, and branch out to family members based upon the data gathered.

Image from https://skopenow.com, September 17, 2019.



Paid Professional-Level People Search Engines

If you are a private investigator, law enforcement agent, bounty hunter, skip tracer, or otherwise have a professional designation in the judicial, legal, or law enforcement world, then you may have additional options for your people-searching needs. This level of professional people searching usually requires you to register with the company, provide business licenses and documentation showing that you do a certain type of work professionally, may require a site visit where the company comes and tours your physical office location, and may require you to sign legal documents before you gain access to any of their data. This process of getting people reports from these companies will take time to set up the initial access and agree on payment terms.

As for payment, there are a variety of options, ranging from monthly or yearly fees to per-report pricing. It all depends upon the business model of the site you are using.

Is it worth it to go through these steps to get access to their data? In general, yes, as their information will surpass what consumer-level sites will provide showing detailed credit, criminal, vehicle, and other data about your targets.

Professional-Level People Search Engines

In 2017, a private investigator magazine web site conducted a poll of existing PIs and asked which professional-level people search sites were they using[1]

Preferred Database	Percent of Respondents
Tracers	87.2%
TLO	32.7%
IRB	29.3%
Other*	13.1%

The top three companies were:

1. tracersinfo.com
2. tlo.com
3. irbsearch.com

Professional-Level People Search Engines

In 2017, the PInow.com web site published results from their survey of 400 private investigators (PIs). They asked this audience which people search engines they use in their work.[1] (Results can be found at the reference below.) Note that most investigators used more than one search engine in their work, and that is the reason why the percentages add up to over 100%.

The top three sites used were:

- tracersinfo.com - Many a la carte options to choose from
- tlo.com - Reliable data
- irbsearch.com - More comprehensive and reliable data

There are many paid sites that may be helpful in your work, and the article names quite a few more.

Image from https://sec487.info/59, July 8, 2017.

Reference:

[1] https://sec487.info/59

People Searching Summary

Choosing which people search engines you use depends upon:

- Your funding
- Your professional standing as an investigator
- Your OSINT goals

Ensure that you use genealogy and obituary sites for content when it makes sense

People Searching Summary

In most of your OSINT investigations into people or companies you will need to use one or more people search engines. They speed up the process of collecting data about a target and can get you access to data that you may not normally find in open sources.

Which people search engines you choose to employ in your work will depend upon:

- How much money you/your company/your customer is willing to spend on the data
- Whether or not you have professional certifications and licenses (bounty hunting, skip tracing, private investigator, etc.)
- What your OSINT goals are for your project

When applicable to your OSINT goals, consider searching for obituaries for targets or their families and using genealogy web sites, as both can contain helpful family data.

SEC487 Workbook

Please visit the course electronic workbook in the 487 virtual machine and begin the exercise named:

"People Searching"

This page intentionally left blank.

Course Roadmap

- Day 1: Foundations of OSINT
- Day 2: Gathering, Searching and Analyzing OSINT
- **Day 3: Social Media, Geolocation, and Imagery**
- Day 4: Networks, Government, and Business
- Day 5: The Dark Web, Breach Data, and International Issues
- Day 6: Capstone: Capture (and Present) the Flags

SOCIAL MEDIA, GEOLOCATION, AND IMAGERY

1. People Search Engines
2. **Facebook Analysis**
3. LinkedIn Data
4. Instagram
5. Twitter Data
6. Geolocation
7. Imagery and Maps

This page intentionally left blank.

Social Media Explained

These sites fill a need for users:

- Sharing with others
- Maintaining social bonds
- Being perceived as an expert
- Just "people-watching"

They are major focal points for OSINT analysts.

Social Media Explained

There are many reasons why people use social media web sites. The picture above provides a funny example of how some of the major social media sites might be used. The reality is that social media web applications fill needs for their users: to share, to create and maintain social bonds, to be perceived as an expert, or just to "people watch" by not posting data but by reading others' posts.

Social media sites are a treasure trove for OSINT analysts, as we can retrieve a wide variety of data about our targets, their habits, desires, locations, and relationships. This is the focus for today: harvesting data from social media sites.

Image from https://sec487.info/3s, March 11, 2017. (URL no longer active)

Facebook Origins

"Facebook is a social networking service launched on February 4, 2004. It was founded by Mark Zuckerberg with his college roommates and fellow Harvard University student Eduardo Saverin. The website's membership was initially limited by the founders to Harvard students, but was expanded…by September 2006, to everyone of age 13 and older with a valid email address."

- Wikipedia, "History of Facebook," 2017.

Facebook Origins

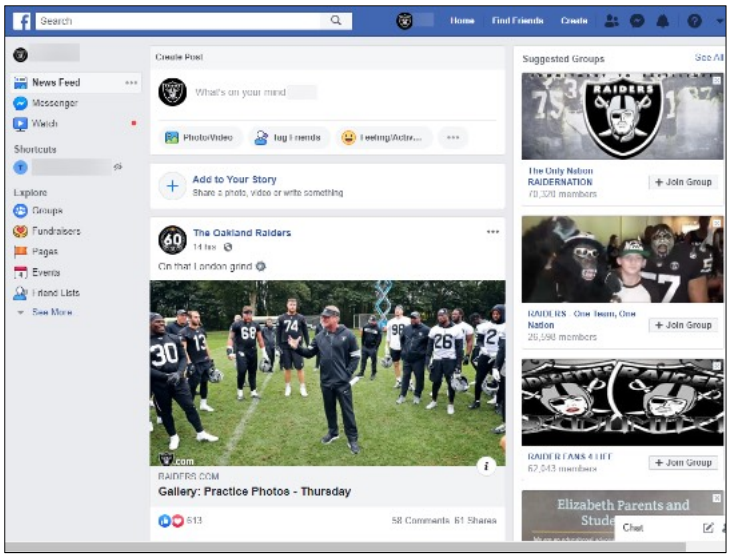
Facebook (https://www.facebook.com/) is a social media juggernaut. In February 2004, Mark Zuckerberg and his college roommate Eduardo Saverin created a web application that they envisioned using to bring college students together. The movie *The Social Network* (https://sec487.info/3h) describes in a Hollywood-like manner how the two created the largest social media platform in the world.

Facebook exceeded its goal to connect college students and evolved into much more than merely a forum for students.

Facebook Size and Scope

In 2019 -

- 2.41 billion monthly, active user accounts[1]
- 1.59 billion daily, active users[2]
- 1.74 billion mobile active users[2]
- 307 million users in Europe
- Removed 2.2 billion fake accounts in 1st qtr[3]



Facebook Size and Scope

Facebook's ease of sharing data and vast user base quickly helped it grow to fill a gap in social media. In 2019, Facebook reportedly had 2,410,000,000 (2.41 billion) monthly active user accounts (some of which we know are fake accounts or sock puppets). While Facebook users are all over the world, it may not be the primary social media network with your target. Later in the course we will discuss social media networks that are favored in non–United States regions. However, with billions of users logging in each day from around the world, Facebook remains a prime location for data gathering.

Image from https://facebook.com, October 4, 2019.

References:

[1] https://sec487.info/eu, September 17, 2019

[2] https://sec487.info/ev, September 17, 2019

[3] https://sec487.info/sf, September 17, 2019

What Data Can Be Found on Facebook?

Facebook is an amazing OSINT source of information if your target uses it

There are security features that can make our work challenging

We have methods to circumvent most of the controls

Some data that can be found:

- Photos of targets
- Videos
- Likes/Dislikes of targets
- Friends of targets
- Group memberships
- Locations target may have been
- Events invited and events attended

What Data Can Be Found on Facebook?

Facebook users regularly share information about a wide variety of topics and, as such, it is an excellent source for OSINT data harvesting. Some of the content users post to the site is protected using Facebook's access controls, and that can limit what you may be able to gather from Facebook about your targets. Depending upon your assessment rules, there are methods for circumventing some of the Facebook blocks to gain access to its data.

The above slide mentions some of the important OSINT data that you might gather from a Facebook user profile and its activities. With the massive amount of content available on the site, it is important to stay focused and gather data relevant to your assessment.

The OSINT opportunities go beyond merely documenting the photos shared. We get to record the events from the eyes of the target, their friends, and family. We see jokes and poking fun. We see anger and compassion. All of this can be useful in our work to help give perspective on relationships and events.

Facebook Primer

For those who do not use Facebook, here are basics:

- Each user has an account and **profile**
- Users can **post stories** on their **timeline** to share with their connections
- Users can connect or **friend** other profiles in Facebook
- Users can **like** pages, videos, photos, and more
- Users can **comment** on shared information
- Users can choose a location to **check in**
- **Sharing** is taking someone else's content and reposting to your audience
- There are **groups** to join and **events** to attend or be invited to

Facebook Primer

Some people may never have used Facebook for personal or work-related reasons. Let us get everyone using the same terminology so that as we move through this module, we understand the basic concepts.

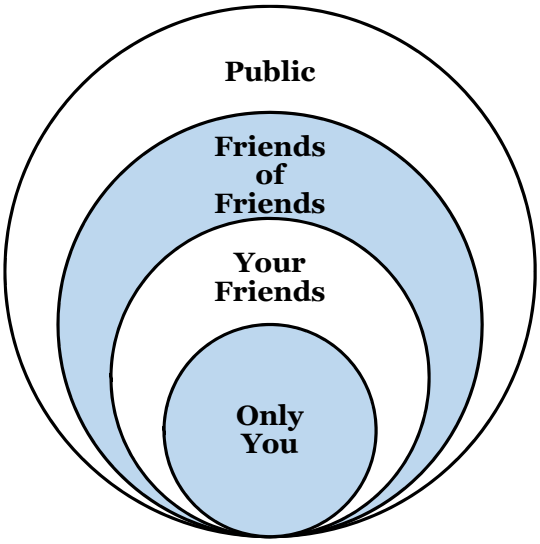
- Users have **profiles** that they use to share basic information about themselves.
- A **post** is content that a user has submitted to Facebook to show to an audience of their connections (and possibly the public).
- Connecting to other user profiles to more easily share information is called **friending** another user. "Friends" are merely connections. Friends can consist of colleagues, relatives, schoolmates, and actual friends.
- There are reactions that Facebook users can employ to show their feelings about posts. The main reaction that people use is called a **like**.
- Users can also add their **comments** to a post or page.
- If a user wishes to tell others where they are or have been, they can **check in** at a location. Users do not have to be at that location to check in.
- Re-posting content to a user's own audience is called **sharing** and can be performed on most content.
- Facebook has **groups** and **events** that users can create and join.

Facebook Data Is Protected

To gain access to most valuable Facebook data, you must have a user account

Some data can be restricted to friends only or friends of friends

You most likely will not be able to retrieve all the data in a person's profile unless that profile is made public



Facebook Data Is Protected

Facebook helps users protect their information through a system of authentication and access controls. To access the majority of user Facebook data, you will need to log in to Facebook using your own Facebook user account. That is usually the first barrier. Remember to evaluate whether you need to use a sock puppet account for your work before you begin making queries and retrieving data!

Next, Facebook allows users to limit which users have access to what data. In user profiles and each time data is published by the user, the user can choose who can and cannot see it. There are roughly four distinct user groups:

1. **Public** – Anyone, even people without Facebook accounts, can view this data.
2. **Friends of Friends** – Here the data is allowed to be shared farther than the original poster's friends. Their friends can also view the content.
3. **Your Friends** – Only people with a direct connection (a "friend") to the person sharing the information can view the data.
4. **Only You** – This one is obvious. Only you (and Facebook) can view this restricted information.

Facebook's Advertising System

There is an overlap in what OSINT analysts and advertisers do; we both seek a target or group

Advertisers deliver a message, whereas we collect data

Facebook's advertising options may assist us in our OSINT

*"One of the many ways that **ads** get in front of your eyeballs on Facebook and Instagram is ... [they let] an advertiser **upload a list of phone numbers or email...** it will then put an ad in front of accounts associated with that contact information.... Facebook calls this a 'custom audience.'"*[1]

Facebook's Advertising System

One of the methods in which Facebook, Instagram, and other applications owned by Facebook make money is through advertising. In 2018, a report on Gizmodo (https://sec487.info/mb) noted that Facebook and its related sites were allowing advertisers to upload lists of phone numbers and emails of accounts that they wanted ads delivered to using the "custom audience" feature of their system.

Advertising and marketing are related activities to OSINT. They seek to locate people and groups to deliver a message to buy a product or increase the reach of their marketing event. In OSINT, we try to find a target or group to retrieve OSINT data from them for our investigations. In the future, we will see OSINT analysts use more advertising systems to locate their targets.

Reference:

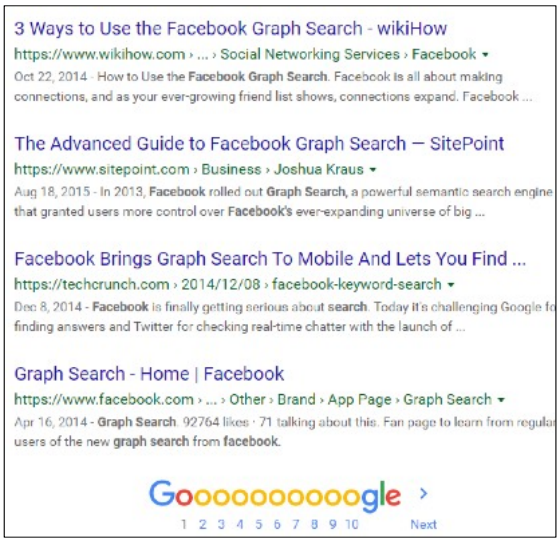
[1] https://sec487.info/mb, January 2, 2019.

Facebook Graph Search Changes

In the summer of 2019, Facebook radically changed how we search for data on its site

Lots of old information still populates the internet [1]

We need to be able to recognize old and focus on learning the more-complicated new methods



Facebook Graph Search Changes

The summer of 2019 was a rough one for the OSINT world. After years of providing a stable, detailed search method into Facebook data, Facebook changed all the rules. Well, not just the rules but the encoding, the syntax, and the vocabulary. It was a huge shift in how their search features worked, and it broke many tools and sites that used to harvest Facebook data.

While these changes were a boon for privacy advocates in that data was a little more safe and more of a challenge to get to, OSINT investigators and law enforcement had some huge problems, as the data they had been harvesting for years disappeared over night. Months later, many researchers had figured out methods to search for some of the same content as before, but Facebook did not make it a one-for-one transfer of features from the previous graph search to the current one. Many of the searches we relied upon to discover relationships and locations of people in Facebook are simply not available anymore.

We mention this to you because there exists a huge amount of old and outdated documentation about how to use Facebook's graph search. If the document you are reading is from before June 2019,[2] consider it historical data and not currently accurate.

Image from https://sec487.info/yl, October 5, 2019.

References:

[1] https://sec487.info/yl

[2] https://sec487.info/ym

Facebook IDs

Unique number per user account, page, and group

Will be used later to search for information

View page source on the Facebook user's profile page and search for the parameters: entity_id, page_id, group_id

Some tools and web sites can retrieve this, too

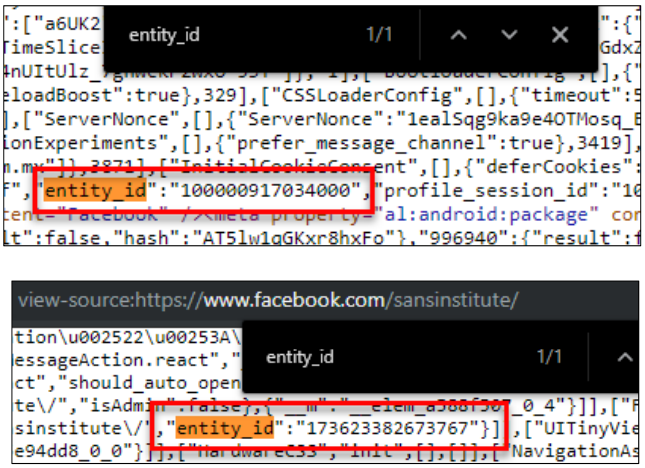
Facebook IDs

Regardless of your Facebook profile name, Facebook assigns each user their own unique user number, each page its own page number, and each group its own group number. This number is then used by the site to note the activities (stories they post, pictures they comment on, videos they are tagged in, etc.) of that object (user, page, or group). To perform some of the advanced searches to get content about our targets, we need this unique number, which can be retrieved from the HTML source code of a page.

If you do not want to use this technique, there are web sites (https://sec487.info/3p) that will find the Facebook number of someone's profile for you. Keep in mind that, if you use a third-party web site to find this information, that web site will then know that you are looking for a certain Facebook user, page, or group. This may violate your terms of the engagement and is poor operational security. Besides, harvesting the Facebook ID number is quite simple to do.

Retrieving User/Page Facebook ID from Source Code

1. Find user profile or page
2. Right-click on the web page and select "View Page Source" to show the HTML code of the page
3. In the source code, search for the term `"entity_id"`. The number after it should be the ID



Retrieving User/Page Facebook ID from Source Code

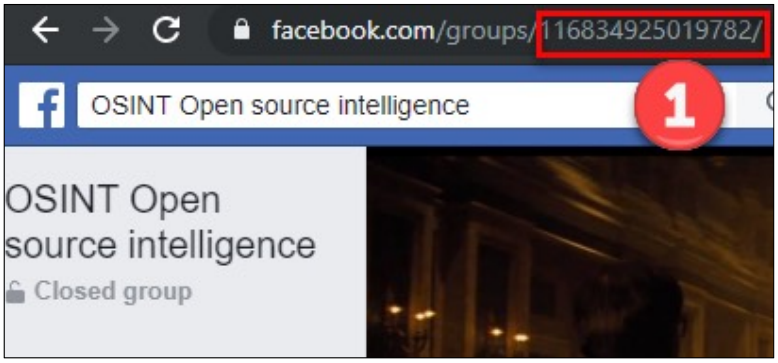
Each Facebook user has their own entity_id. Inside the HTML source code of a user's profile page, there are also profile_id and profile_owner_id parameters with the same information as the entity_id. We need to harvest this number to perform advanced searches later. Here is the process to do so:

1. Locate the target's Facebook profile.
2. Right-click somewhere on the page and select the "View Page Source" item in the browser.
3. Perform a search on that new page for `"entity_id"`.
4. The number to the right of `"entity_id="` will be the user's profile ID. In the case of our example, Anatoliy Struk, the Facebook profile ID is 100000917034000.
5. Record this value for later use.

Image from https://sec487.info/xn, October 4, 2019.

Retrieving Group Facebook ID from URL

1. Find target group
2. Look in URL for the unique number (1)
3. Record the number



NOTE: To access most of the URLs in this module, the student may be required to be logged in to Facebook with a valid account.

Retrieving Group Facebook ID from URL

Looking for the unique ID for a Facebook group? The process is even simpler.

1. Locate the target Facebook group.
2. Look at the URL and retrieve the number. The number to the right of "`groups`" will be the ID. In the case of our example above, the closed group OSINT Open source intelligence, the Facebook ID is 116834925019782.
3. Record this value for later use.

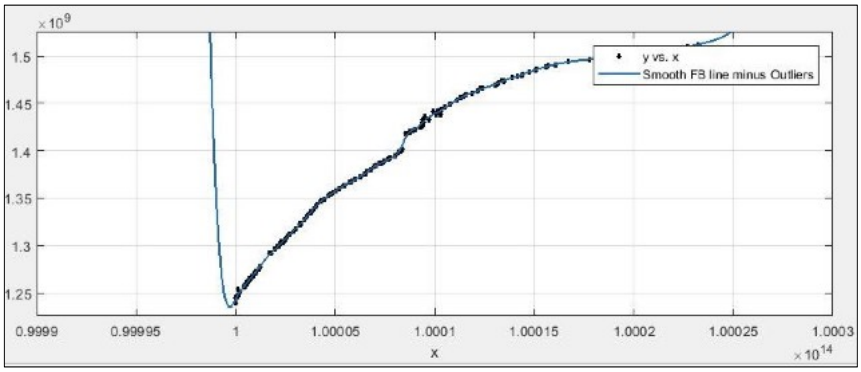
Please note that the URLs we use for this Facebook section may require the student to be logged into Facebook with a valid account.

Image from https://sec487.info/xo, October 4, 2019.

Josh Huff's Facebook Profile ID Dater

Josh Huff (@baywolf88) conducted research on the Facebook user profile ID

Since the ID is an integer, could the number tell creation date?



He collected IDs and found a correlation between the number and date of account creation

Josh Huff's Facebook Profile ID Dater

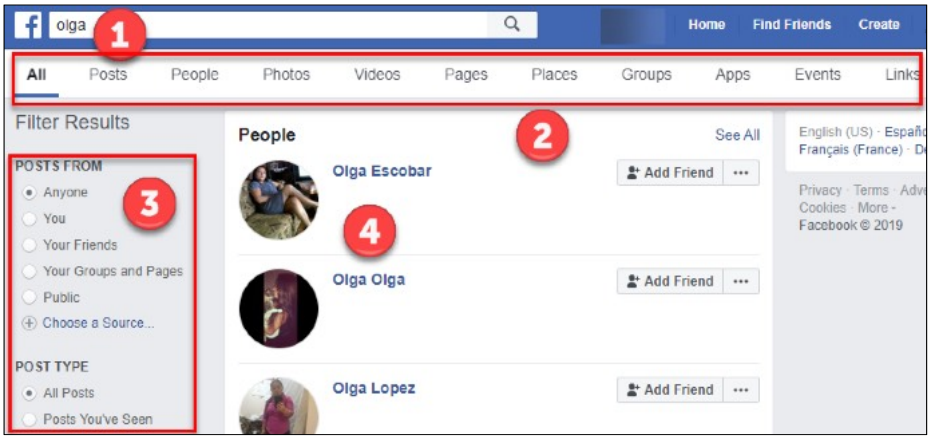
The OSINT researcher Josh Huff (@baywolf88) noticed that Facebook profile IDs were numbers and that newer accounts had larger numbers than older ones. He went on a year-long research project to track new and old Facebook profiles and map when they were created.

Josh's output can be seen in his blog post https://sec487.info/ht and in Michael Bazzell's 6th edition of the *Open Source Intelligence Techniques* book (page 114).

Searching Facebook Using Search

1. Enter search term and press Enter
2. Choose search category
3. Pick filters
4. Examine results

`https://www.facebook.com/search/`**`top`**`/?q=`**`olga`**`&epa=SEARCH_BOX`



Searching Facebook Using Search

The built-in search function in Facebook is the search bar located in the upper left of most screens. Users enter a search term (like we searched for the string "olga" above(1)) and then press Enter. Once they do, the results for their query will be shown. Users can then refine the search by selecting a different category for the search (2), such as people or photos. By default, Facebook search starts with the "top" category. We can also see this in the URL above ("/search/**top**/").

Choosing a new category will change the URL (as we will see). Changing the filters (3) will also alter the URL and refine our search results (4).

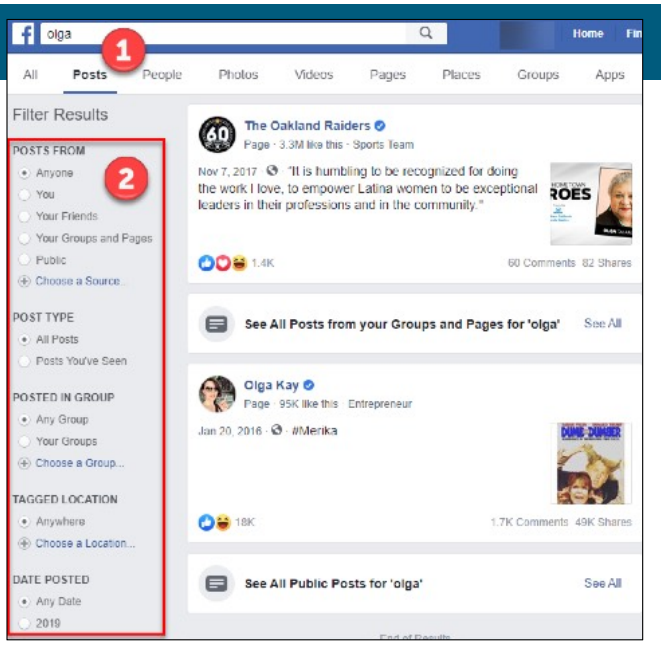
Image from https://sec487.info/xp, October 4, 2019.

Searching Facebook Posts

Switching to the "Posts" category

Filters change (2)

`https://www.facebook.com/search/posts/?q=olga&epa=SERP_TAB`



Searching Facebook Posts

Choosing a different category for the search, Posts (1), and keeping everything else constant, we see the URL changed to "/search/**posts**/". The filters we can apply are customized for user and group posts (2). We will examine filters in just a bit.

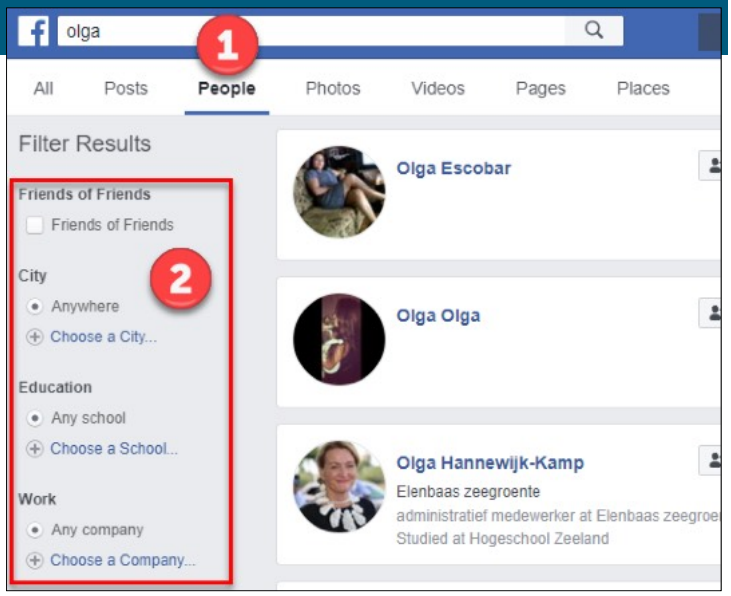
Image from https://sec487.info/xr, October 4, 2019.

Searching Facebook People

Switching tabs to the "People" category (1)

Filters now are for city, education, and work (2)

`https://www.facebook.com/search/people/?q=olga&epa=SERP_TAB`



Searching Facebook People

Choosing a different category for the search, People (1), and keeping everything else constant, we see the URL changed to "/search/**people**/". The filters we can apply are customized for people (2). Using the filters, we can refine our results by where the person has reported they live, went to school, and work(ed).

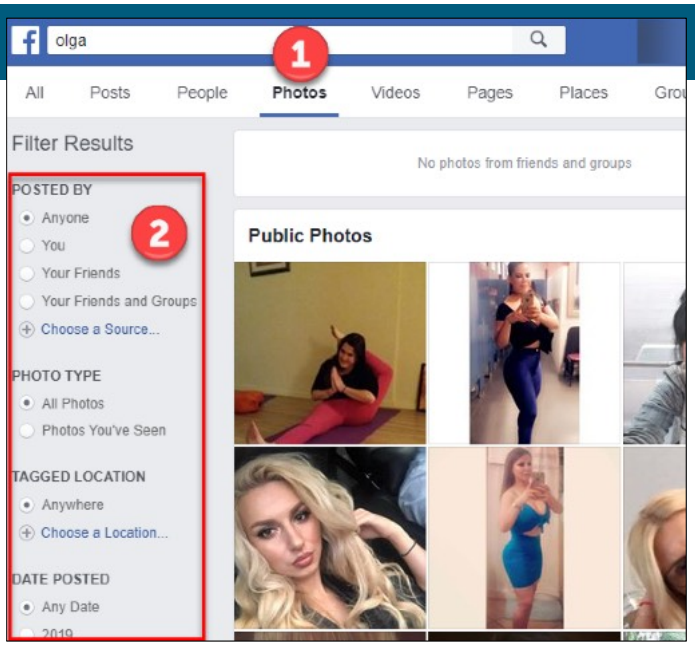
Image from https://sec487.info/xq, October 4, 2019.

Searching Facebook Photos

Switching tabs to the "Photos" category (1)

Filters now are for posted by, type, location, and date (2)

`https://www.facebook.com/search/photos/?q=olga&epa=SERP_TAB`



Searching Facebook Photos

Choosing a different category for the search, Photos (1), and keeping everything else constant, we see the URL changed to "/search/**photos**/". The filters we can apply are customized for people (2). Using the filters, we can refine our results by where the person has reported they live, went to school, and work(ed). Note that, while these are the filters that Facebook allows you to use in this web page, there are additional filters for each search category. We will show them later in this module.

Image from https://sec487.info/xs, October 4, 2019.

Introduction to Facebook Filters

You are getting the idea that **changing category changes the URL**

It also **customizes the filters** based on the category chosen

Filters in Facebook are **JSON** objects that are **Base64** encoded [1]

We can recognize JSON by its use of these characters: `{ },":[ ]`

Base64 encoding uses:

- `uppercase A-Z (26)`
- `lowercase a-z (26)`
- `numbers 0-9 (10)`
- `+ and / (2)`
- `Sometimes "=" or "=="`

26 + 26 + 10 +2 = 64

Introduction to Facebook Filters

We are not going to go through each of the categories within Facebook search, as we think you get the idea that as you choose different categories, the URL changes and the filter options are customized to that category. Let's examine the filters and then see some examples.

Facebook filters are JSON strings that are then Base64 encoded[1] and placed in the URL. We have seen JSON content throughout the course. It is easily recognizable by the format and the characters used. Facebook encodes that JSON content in Base64 so that any special characters that might break a URL (like "&" and "?") are safely transformed. Base64 encoding is not encryption and is easily reversed or decoded.

Recognizing Base64 strings will make you more powerful in your work, as you may be able to reveal what is encoded. In Facebook's filters, we not only can decode the Base64, but we can tamper with it too!

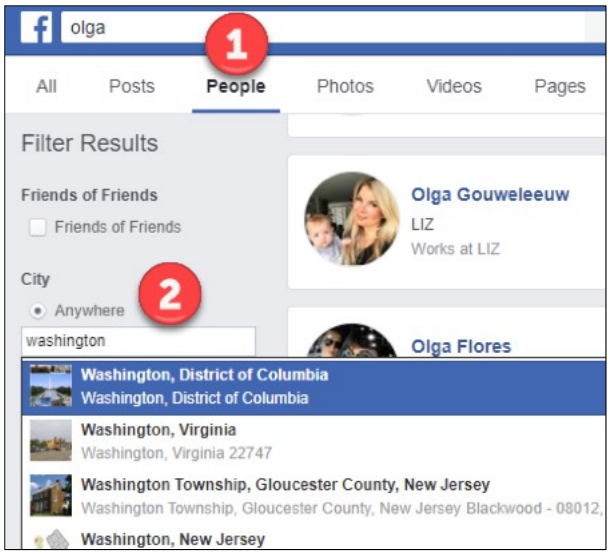
Reference: [1] https://sec487.info/xt

Refining Results Using Filters (1)

Let's switch back to the People category (1) and enter a filter for "City"

Clicking on "Choose a city..." (2) and entering "washington" causes Facebook to search for cities named "Washington"

We select "Washington, District of Columbia"



Refining Results Using Filters (1)

Moving our category back to People (1), we are going to choose a filter and enter in data. As shown above, selecting "Choose a city…" and entering "washington" causes Facebook to search for cities with that name. We then choose the correct one, and Facebook enables the filter.

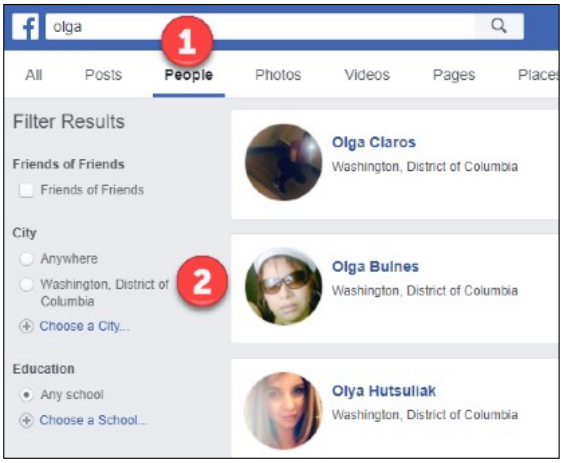
Image from https://sec487.info/xq, October 4, 2019.

Refining Results Using Filters (2)

Here we see the result of adding that filter (2)

The URL has changed too!

```
https://www.facebook.com/search/people/?q=olga&epa=FILTERS&filters=eyJjaXR5Ijoie1wibmFtZVwiOlwidXNlcnNfbG9jYXRpb25cIixcImFyZ3NcIjpcIjExMDE4NDkyMjM0NDA2MFwifSJ9
```



Refining Results Using Filters (2)

Now that we have refined our results and added a city (2), let's examine what happened to the URL. We still see the "people" category" and the "olga" keyword (in the slide above). Now we have the "epa=FILTERS&filters=…" section. That "filters=" parameter contains uppercase letters, lowercase letters, and numbers. Could that be Base64-encoded content? Let us find out.

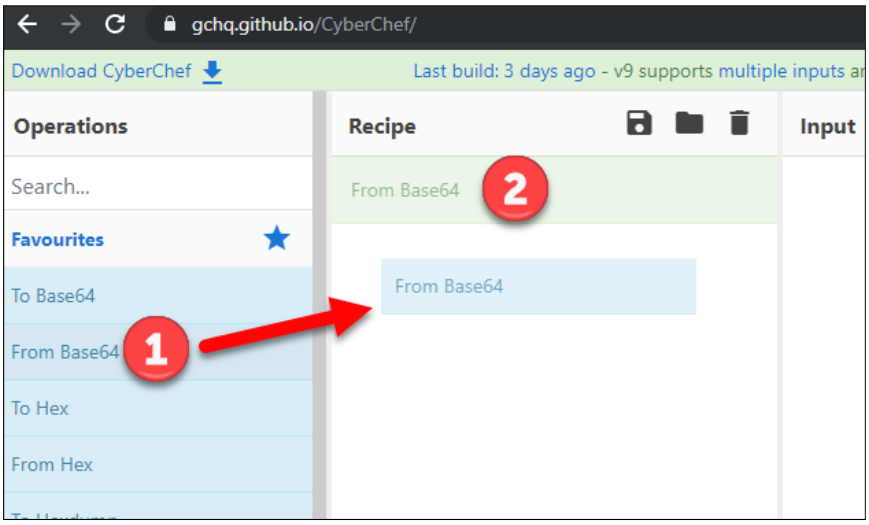
To Base64 decode, we are going to use the CyberChef application that we already discussed earlier in class.

Image from https://sec487.info/xu, October 4, 2019.

Decoding Base64 Content

Let's visit CyberChef [1] and drag the "From Base64" (1) into a recipe (2)

Drop or let go of the Base64 in the Recipe column



Decoding Base64 Content

As we mentioned, Base64 is encoding and can be easily decoded. The CyberChef application[1] allows us to do this transformation and more. Visit the web site[1] and drag the "From Base64" from the Operations column into the Recipe column, as shown above. Then drop it in there. That should change your URL to be https://gchq.github.io/CyberChef/#recipe=From_Base64('A-Za-z0-9%2B/%3D',true) (https://sec487.info/xv).

Now we are ready at decode our content.

Image from https://sec487.info/r2, October 4, 2019.

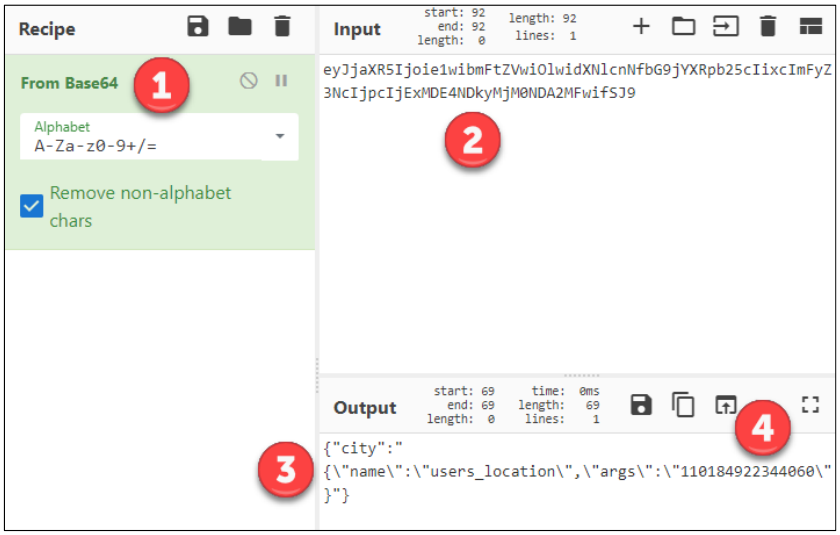
Reference: [1] https://sec487.info/r2

Decoding Facebook Filter Base64

Base64 content from "filter=" parameter was:

```
eyJjaXR5Ijoie1wi
bmFtZVwiOlwidXNl
cnNfbG9jYXRpb25c
IixcImFyZ3NcIjpc
IjExMDE4NDkyMjM0
NDA2MFwifSJ9
```

Enter that in the Input column (2)



Decoding Facebook Filter Base64

Now we take that Base64-encoded content from the "filters" URL parameter and copy and paste it into the Input column (2) of CyberChef. The application automatically applies the recipe you created and transforms your input to output (3).

So the Base64-encoded string eyJjaXR5Ijoie1wibmFtZVwiOlwidXNlcnNfbG9jYXRpb25cIixcImFyZ3NcIjpcIjExMDE4NDkyMjM0NDA2MFwifSJ9 decodes to {"city":"{\"name\":\"users_location\",\"args\":\"110184922344060\"}"} (3). What is that number for though? Let's see on the next slide.

Image from https://sec487.info/xw, October 4, 2019.

Checking Our Decoded Content

Looked up the Facebook entry for the location Washington, District of Columbia

Want to guess what that location's Facebook entity ID is? If you are thinking about the "110184922344060" from the CyberChef output, you are correct!

To check, visit https://facebook.com/110184922344060 (https://sec487.info/xx)

Checking Our Decoded Content

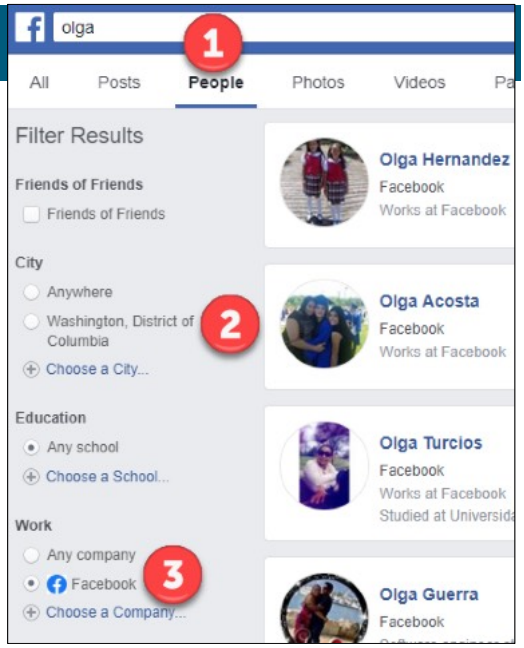
In the previous slide, we saw there was "users_location\",\"args\":\"110184922344060\", which contained what looks to be a Facebook ID for something. To find out what, just append it to the https://facebook.com/ URL (https://facebook.com/110184922344060, https://sec487.info/xx). You will see that that will take us to the Facebook page for the city of Washington, District of Columbia. That was the city we selected in our filter!

Image from https://sec487.info/xy, October 4, 2019.

Decoding Filters with Multiple Entries

Let's add a company to the filter for Facebook (3) to the city of Washington, DC (2)

https://www.facebook.com/search/**people**/?q=**olga**&epa=FILTERS&filters=**eyJjaXR5Ijoie1wibmFtZVwiOlwidXNlcnNfbG9jYXRpb25cIixcImFyZ3NcIjpcIjExMDE4NDkyMjM0NDA2MFwifSIsImVtcGxveWVyIjoie1wibmFtZVwiOlwidXNlcnNfZW1wbG95ZXJcIixcImFyZ3NcIjpcIjIwNTMxMzE2NzI4XCJ9In0%3D**



Decoding Filters with Multiple Entries

Let's modify the query we made for Olga in Washington, DC (https://sec487.info/xu). We will add a company or work filter to further refine the results. Here (3) we add a filter for people that say they work at Facebook. Adding this extra filter changes the "filter=" Base64-encoded parameter. It is now:

https://www.facebook.com/search/people/?q=olga&epa=FILTERS&filters=eyJjaXR5Ijoie1wibmFtZVwiOlwidXNlcnNfbG9jYXRpb25cIixcImFyZ3NcIjpcIjExMDE4NDkyMjM0NDA2MFwifSIsImVtcGxveWVyIjoie1wibmFtZVwiOlwidXNlcnNfZW1wbG95ZXJcIixcImFyZ3NcIjpcIjIwNTMxMzE2NzI4XCJ9In0%3D

Copying the Base64-encoded string of `eyJjaXR5Ijoie1wibmFtZVwiOlwidXNlcnNfbG9jYXRpb25cIixcImFyZ3NcIjpcIjExMDE4NDkyMjM0NDA2MFwifSIsImVtcGxveWVyIjoie1wibmFtZVwiOlwidXNlcnNfZW1wbG95ZXJcIixcImFyZ3NcIjpcIjIwNTMxMzE2NzI4XCJ9In0%3D` from the URL, let's paste it into our CyberChef and see what it decodes to.

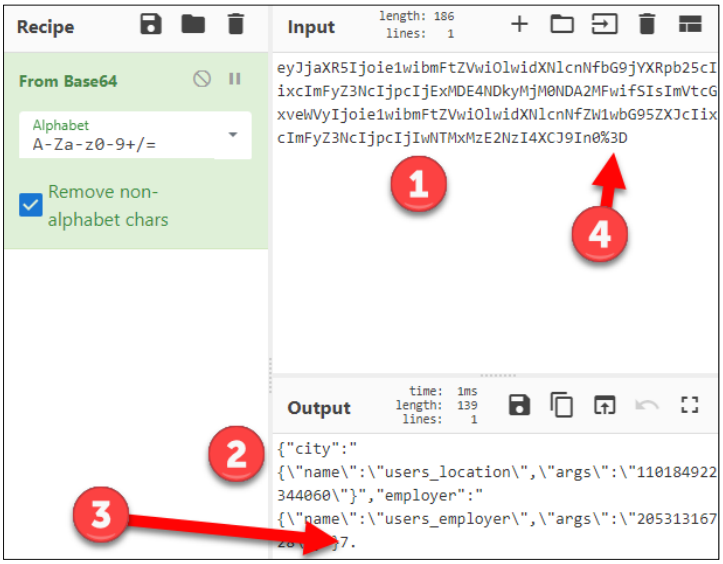
Image from https://sec487.info/xz, October 4, 2019.

Decoding Multiple Facebook Filters

Putting the Base64 string (1) into our existing CyberChef recipe yields the results (2) on the right

We have a problem, as there is a %3D in the Base64 content

This is percent- or URL-encoded content (3)



Decoding Multiple Facebook Filters

Pasting that new Base64 string into our existing CyberChef recipe yields a mostly correct decoded string. We see the same users_location parameter with the same value for Washington, DC. Now we also see a users_employer parameter with a new number…you guessed it…that is Facebook's company page ID.

See that "7." at the end of the results (3)? While that does not decrease our ability to understand what the string does—"People named Olga, living in Washington, DC, and working at Facebook"—if we are going to change the string, it does present a problem.

Looking up at our Base64-encoded string, we can see a "%3D" on the end (4). Percent symbols are not valid Base64 characters. This tells us that we may have another transformation to do before Base64 decoding this string. There is another type of encoding called URL or percent encoding (https://sec487.info/y0) that is found in URLs and is recognized by a percent sign (%) and then 2 characters. In this case, we see "%3D".

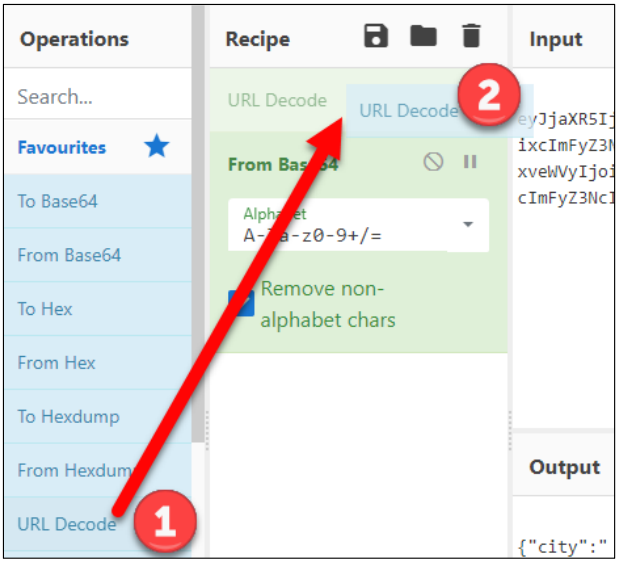
Image from https://sec487.info/x-, October 4, 2019.

URL and Base64 Decoding in CyberChef

Let's add a URL decode step before our Base64 decode

Drag the URL Decode operation (1) from the Operations column into the Recipe column BEFORE the "From Base64" recipe entry

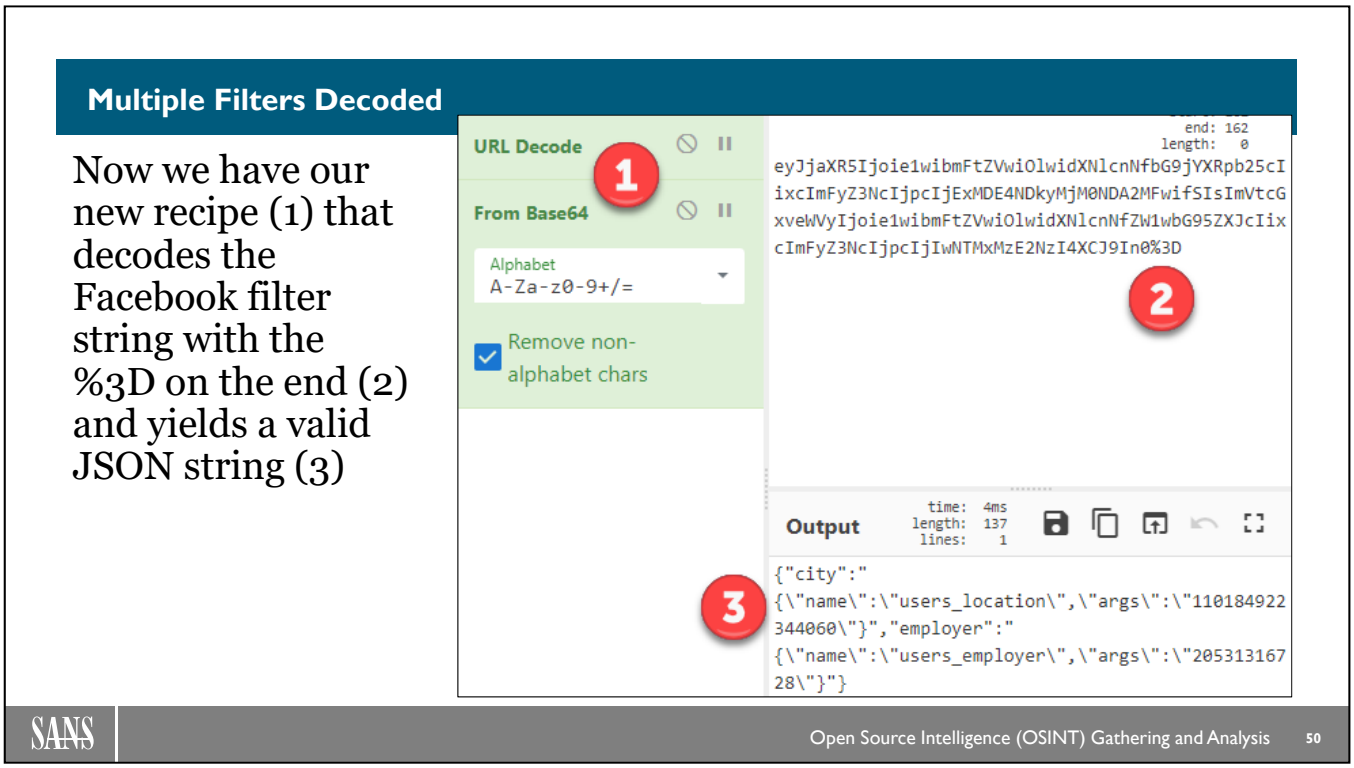
Release it (2) and view your output



URL and Base64 Decoding in CyberChef

To modify our existing recipe in CyberChef, follow the steps above to drag the URL Decode operation to before the From Base64 one in the recipe. Once you drop it in there (2), the output should change and the "7." should be removed because now you are properly decoding the string (https://sec487.info/y1).

Image from https://sec487.info/y1, October 4, 2019.



URL and Base64 Decoding in CyberChef

The above slide shows the final outcome of our decoding the Facebook filter that had multiple filters in it.

Not all Facebook filters will have the URL-encoded content (%3D). The above recipe should work to decode the filter correctly whether it has the URL encoding or not.

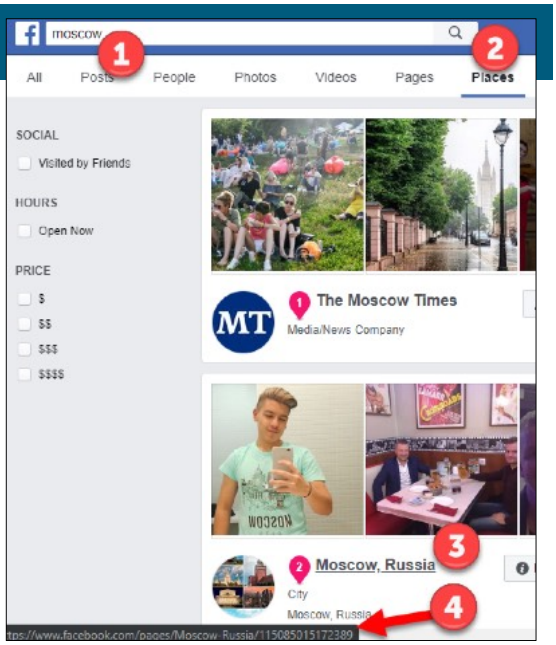
Image from https://sec487.info/y1, October 4, 2019.

Changing the Filter

What if we wanted to look for people named "Olga" in Moscow, Russia instead of Washington, DC?

Let's find the city number for Moscow and change the Base64 content

Then we change the URL and try it out!



Changing the Filter

Instead of choosing another Facebook filter from its user interface, we can create our own combinations. As an example, let's find people named Olga in Moscow, Russia instead of in Washington, DC. First thing we need to do is find the ID for the place named Moscow, Russia.

To do this, we will use the Facebook search, type in "Moscow" (1), and then select the "Places" (2) category. The results show a location (3) that is what we want. If we mouse over the link (3), we can see the URL (4), which has the number we need: 115085015172389.

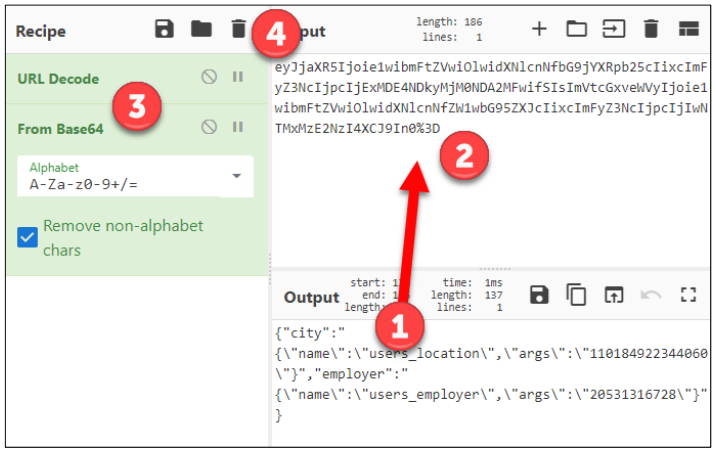
Now we go back to CyberChef and alter the content.

Image from https://sec487.info/y2, October 4, 2019.

Base64 Encoding in CyberChef (1)

We are going to change the recipe and need to record the Output content (1) as it will become our Input (2)

```
{"city":"{\"name\":\
"users_location\",\"
args\":\"11018492234
4060\"}","employer":
"{\"name\":\"users_e
mployer\",\"args\":\
"20531316728\"}"}
```



Base64 Encoding in CyberChef (1)

We are going to modify the content of the filter and then Base64 encode it. To do this, we need to record what the JSON output of the above recipe is so that we can tamper with it. We can also copy the output (1) into the Input column (2) to transfer it.

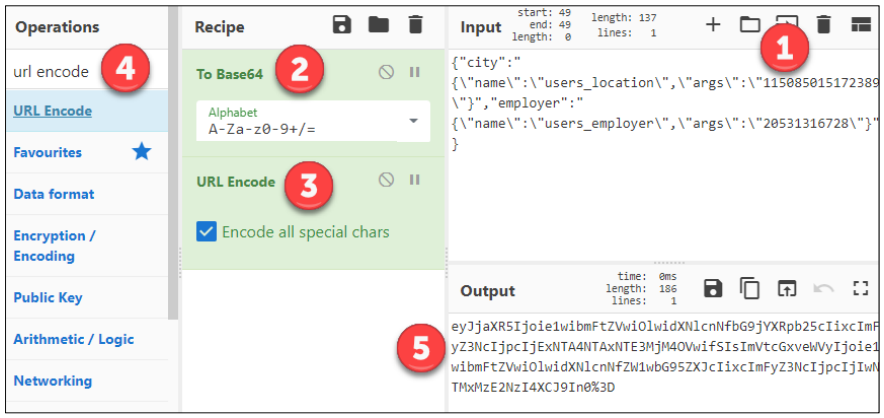
The next thing we need to do is to remove the current recipe operations (3) by clicking the trash can (4) icon.

Image from https://sec487.info/y1, October 4, 2019.

Base64 Encoding in CyberChef (2)

Let's replace the Washington, DC location number with Moscow (1)

Then add operations to the recipe "To Base64" and then "URL Encode" (2)



Base64 Encoding in CyberChef (2)

With the JSON we need in the Input column (1), we can add two operations to the Recipe column to encode "To Base64" (2) and "URL Encode" (3). Replace the Washington, DC number in the users_location value to be the one for Moscow. To find the "URL Encode" operation, you may need to search for it in the Operations column (4).

Once all of these pieces are configured (https://sec487.info/y3), you should see the URL-encoded, Base64-encoded JSON content in the Output pane (5).

Copy that content and replace the Facebook "filters=" value with it and then send it to Facebook.

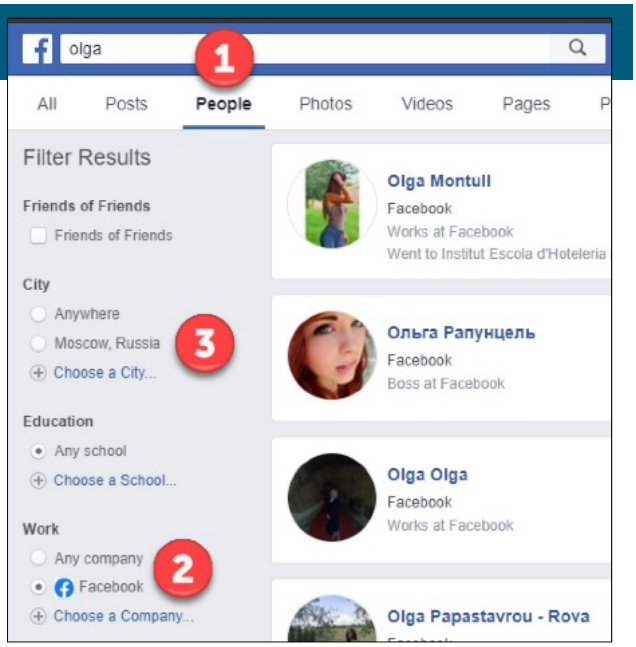
Image from https://sec487.info/y3, October 4, 2019.

Base64 Encoding in CyberChef (3)

We replaced the Facebook-created "filters=" value with our tampered version and see that we are finding:

- people named Olga (1)
- who work at Facebook (2)
- in **Moscow!** (3)

We successfully changed the filter



Base64 Encoding in CyberChef (3)

Once we replaced the Facebook-created filters with the tampered one for Moscow and hit Enter, Facebook provided us with results for people named Olga (1) who work at Facebook (2) and live in Moscow, Russia (3).

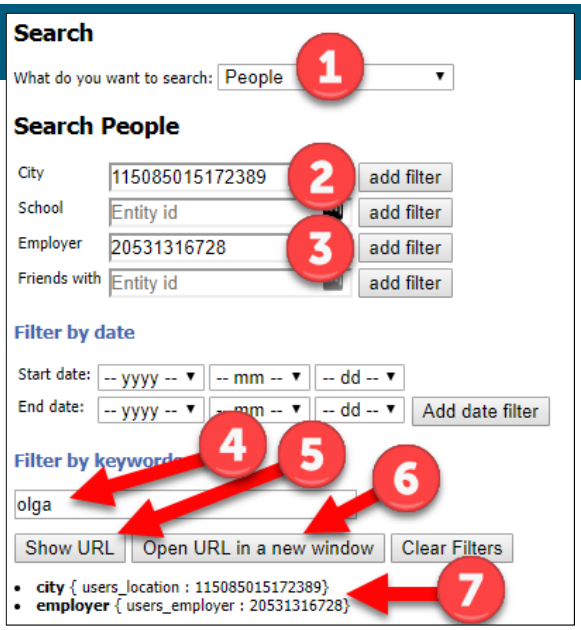
Image from https://sec487.info/y4, October 4, 2019.

Sowdust Filter Creation Tool

Now that we understand how to manually encode and decode and tamper with filters, let's examine an easier method

https://sowdust.github.io/fb-search/

Web form that helps you craft details, filters, and searches for Facebook



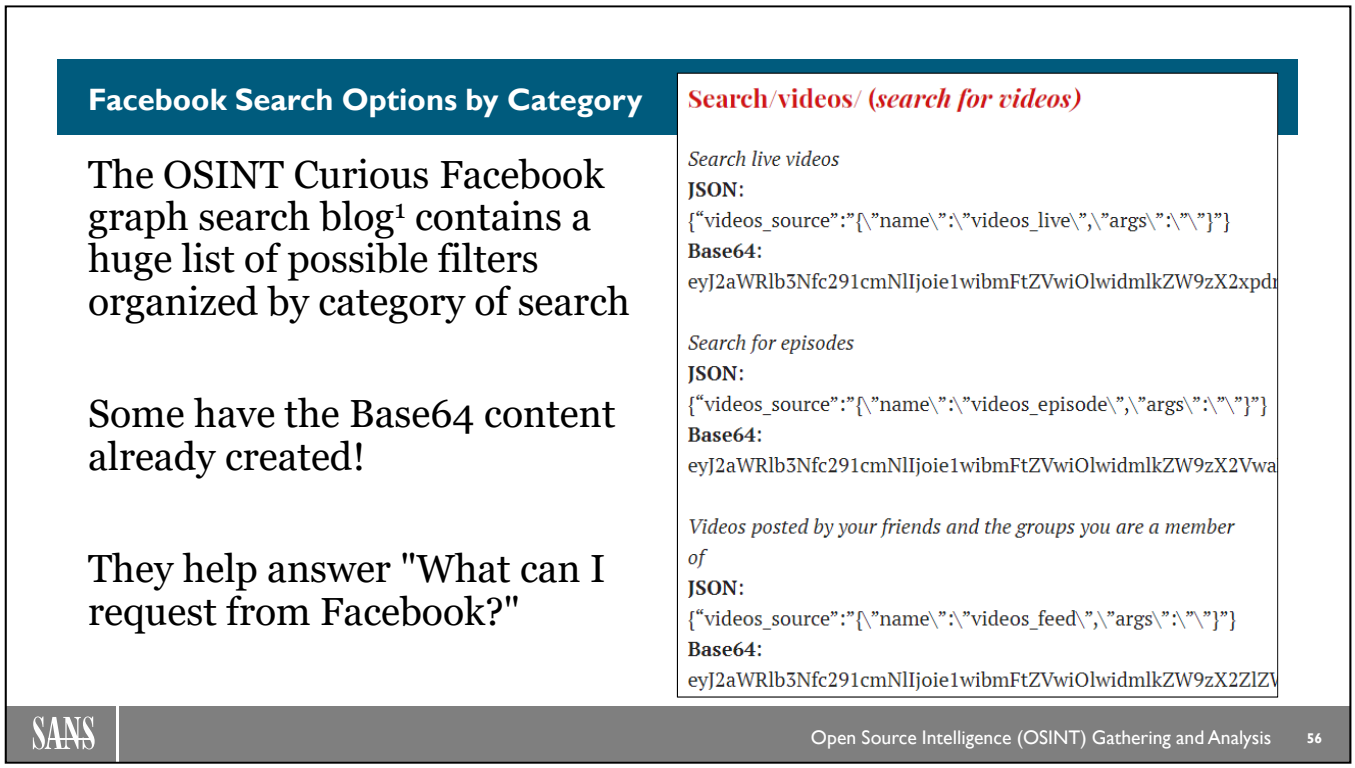
Sowdust Filter Creation Tool

Some of you now realize how hard it has become to modify these Facebook queries. The old graph search techniques were a simple modification of the URL using semi-natural language. Now, we have multiple transformations of JSON content. It is complicated, and we have tools that people have published to make it more simple.

The https://sowdust.github.io/fb-search/ page has a web form that you fill out to create URLs to paste into your browser to search Facebook. In the image above, select the category of the search (1), as each has a separate set of filters that can be used. Once you select that, the rest of the page will be populated with the custom filter fields (2). Enter any information you have for the filters. This site needs those entity IDs, so we would paste in the ID for Moscow (115085015172389) into the City field and then click "add filter." Do the same for the Employer field (3), enter a keyword like "olga" (4), and at the bottom of the page you will see the filters you set (7). Those look familiar to what we saw when we decoded the Base64-encoded filters from Facebook.

If you would like to see what the URL would be for your query, click that "Show URL" button (5), or you can have the web page open a new window in your browser and make your browser request that page (6).

Image from https://sec487.info/y5, October 4, 2019.



Facebook Search Options by Category

The OSINT Curious Project's "The New Facebook Graph Search – Part 1" blog post[1] outlines a huge number of possible filters for each category type. You can use this list to better understand what is possible to retrieve from Facebook using its search. For those filters that have static content, like shown in the slide above, the Base64 content has been encoded for you.

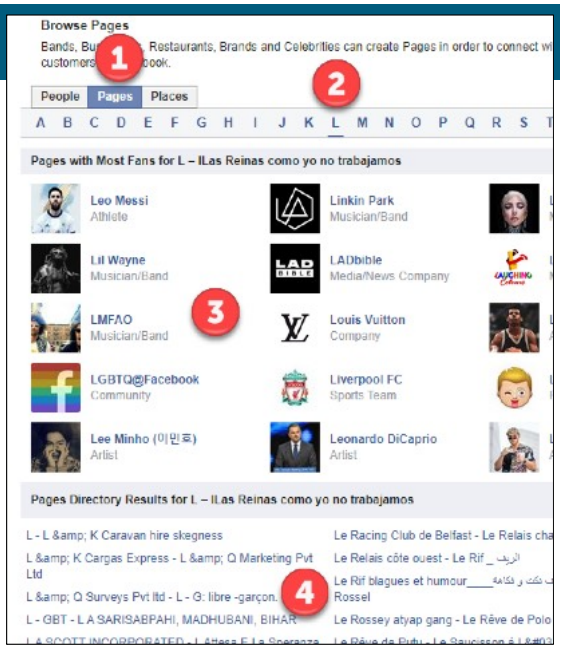
Reference and image from https://sec487.info/y6, October 4, 2019.

Facebook Directories

Some of you remember "phone books" with columns of data

Facebook has unauthenticated pages similar to those, and they are called directories[1]

Kirby Plessas has a list of the different ones, from places and people to work positions and events[2]



Facebook Directories

Another method of discovering data on Facebook is to browse to it. Facebook has directory pages that show a certain type of entry, like pages. You can then browse and click to get from a broad range of pages or people to specific pages or accounts. Facebook maintains these directories for many different types of entities on their site, and the OSINT guru Kirby Plessas (@kirbstr) maintains a list of the different ones that are available.[2]

These directory pages are mostly accessible without authenticating to Facebook. Of course, for private accounts and hidden groups, those entities may not show up in the directory pages.

In the above image, we chose to look at the pages (1) directory[1] and examine pages starting with an "L" (2). Facebook returned the most popular pages (3) and allowed us to browse to others below that (4).

Image from https://sec487.info/y9, October 4, 2019.

References:

[1] https://sec487.info/y9

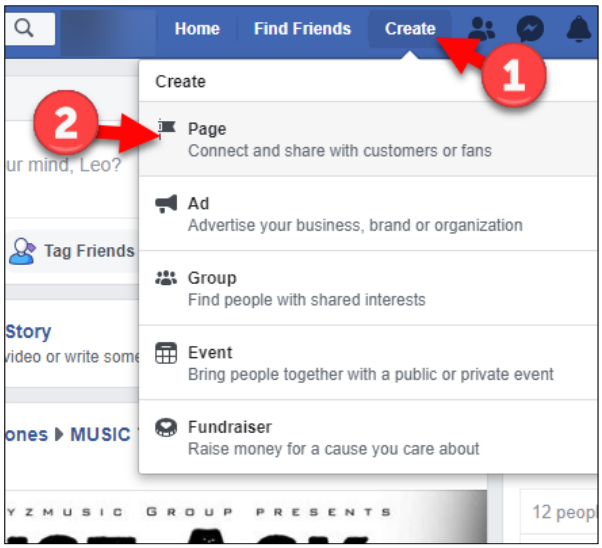
[2] https://sec487.info/y8

Facebook Resolving Email to Account (1)

Michael Bazzell (@inteltechniques) mentioned how to get Facebook to resolve an email address into a Facebook user account using page roles

We will walk through his process

As a valid Facebook user, create a new page (1 and 2)



Facebook Resolving Email to Account (1)

Michael Bazzell (@inteltechniques) noted in a webcast that you could get Facebook to tell what the Facebook account is that is associated with a given email address. For OSINT purposes, being able to find specific Facebook users given their email address is a valuable tool.

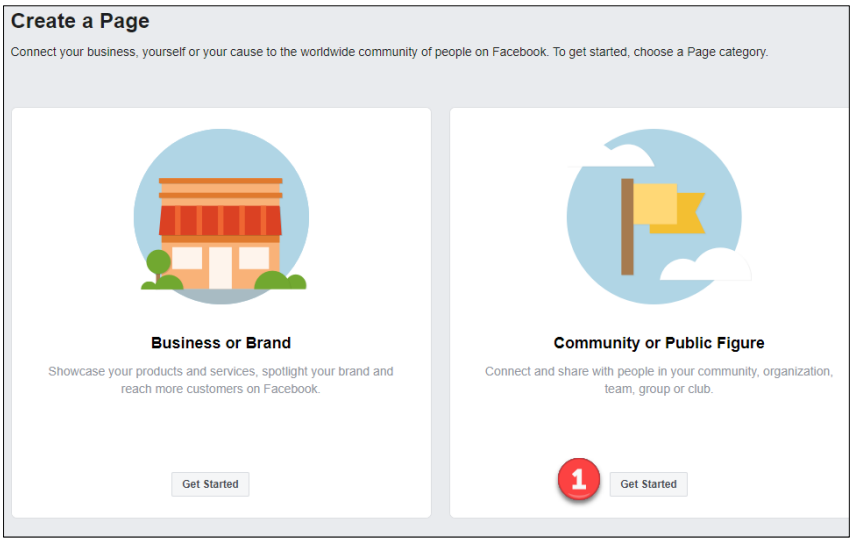
Bazzell describes a process to do this email-to-Facebook-account resolution using Facebook's page administrative roles.

As an authenticated user in Facebook, either access a "page" you already own or create your own (1 and 2).

Facebook Resolving Email to Account (2)

Choose the type of page

We prefer the "Community or Public Figure" (1)



Facebook Resolving Email to Account (2)

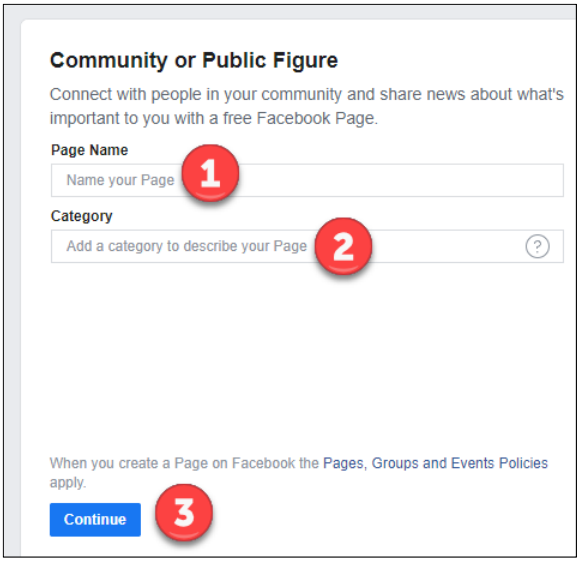
Choose the type of page to create. We suggest the "Community or Public Figure" type of page, but it may not matter.

Facebook Resolving Email to Account (3)

Continue with the page creation and name (1) the page

Then choose a category (2)

Finally, click "Continue" (3)



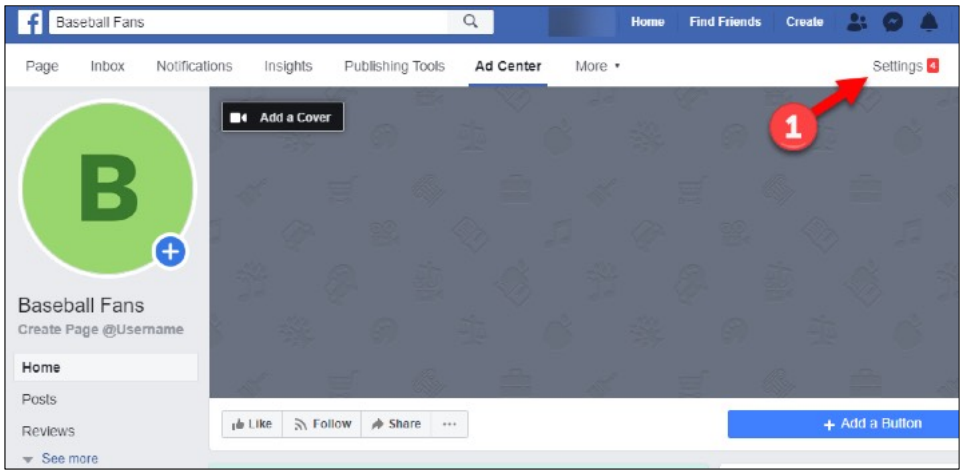
Facebook Resolving Email to Account (3)

Fill in the rest of the information required to create the page.

Facebook Resolving Email to Account (4)

Skip through the addition of images at the prompts or add them

When you get to the page, click the "Settings" link (1)



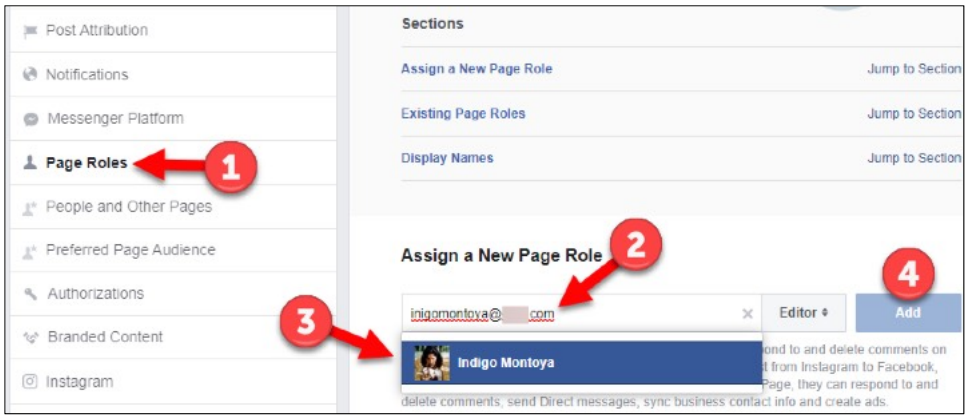
Facebook Resolving Email to Account (4)

You will be prompted to upload images for the page and its background. You can upload these images or not (we chose not to for the example). Once you arrive at the main page for the "Page," click the "Settings" (1) link.

Facebook Resolving Email to Account (5)

Next, click on the "Page Roles" link (1)

Then enter the email you wish to resolve in the "Assign a New Page Role" field (2)



Do not click "Add" (4) as it will alert your target!

Facebook Resolving Email to Account (5)

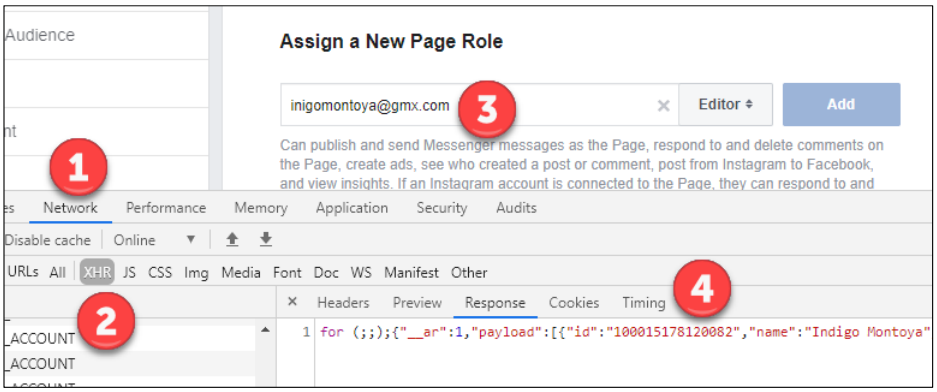
Now comes the actual name resolution feature. In the "Page Roles" link (1), there is a field for you to "Assign a New Page Role" to someone (2). The idea here is that you can have people help you add content to your page or help administer it with you. Instead of actually adding people to do these things, we will type in the email address of our target that we are searching for. When we enter the entire email, if the user has a valid account on Facebook, it will identify it (3).

We warn you not to click the "Add" button (4), as it may alert the target to your page and cause them to become suspicious.

We now know there is an account for that email and know its name and profile picture. We could perform normal searches looking for that user.

Facebook Resolving Email to Account (6)

To retrieve the entity_id of the account, do the previous technique with the browser web developer tools on, Network tab open, and filter XHRs



Facebook Resolving Email to Account (6)

If we want to get the Facebook entity_id for the account while we do this technique, then open the web developer tools in your web browser (usually pressing the F12 key). Select the Network tab (1) and filter by XHR (2). We are using the web developer tools in the Google Chrome browser. Other browsers have different displays.

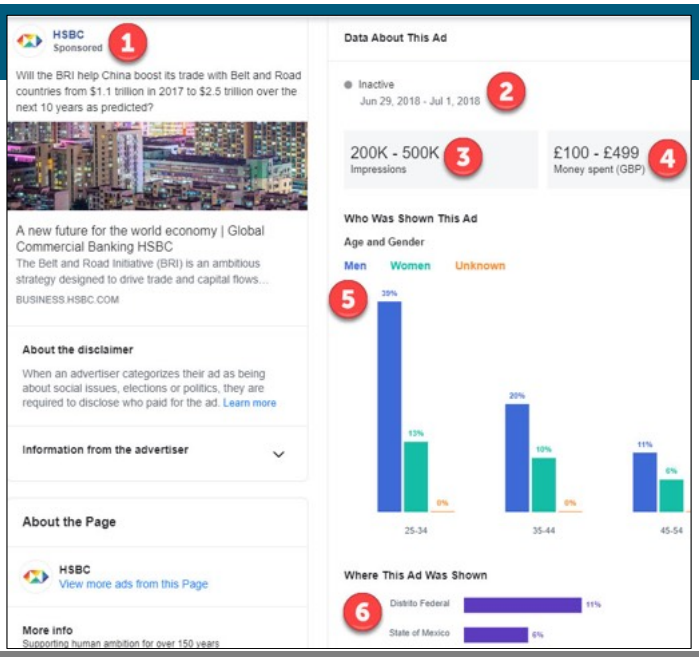
Next, as you type in the email you wish to search for (3), watch the XHRs that populate the web developer window. The last one will have a response with the JSON content you want (4).

Facebook Ad Library

Shows details of Facebook ads internationally[1]

Historic, inactive ads show amount spent and demographics of who saw the ad and where

With this we can understand better who is trying to influence who



Facebook Ad Library

In an effort to be more transparent about who is advertising on its platform and what they are saying, Facebook created the Facebook Ad Library page that unauthenticated users can visit and search. Search for a term (like Brexit), a company or NGO (like the NRA), or any other term you wish. This application will retrieve active and inactive ads with the term.

For inactive ads, you not only can see the ad that was placed, but also see how much money was spent on it, who saw the ad (age, gender, location), and more about who placed the ad.

In the above slide, we searched for the HSBC bank (1) and retrieved an inactive ad from them (2) that ran during June and July of 2018. The ad reached 200–500k users and cost £100–499 (GBP) (4). The page shows what the breakdown of gender and age was (5) that viewed the ad and where it was seen (6).

Image from https://sec487.info/yb, October 4, 2019.

Reference: [1] https://sec487.info/yc

SEC487 Workbook

Please visit the course electronic workbook in the 487 virtual machine and begin the exercise named:

"Facebooking"

This page intentionally left blank.

Course Roadmap

- Day 1: Foundations of OSINT
- Day 2: Gathering, Searching and Analyzing OSINT
- **Day 3: Social Media, Geolocation, and Imagery**
- Day 4: Networks, Government, and Business
- Day 5: The Dark Web, Breach Data, and International Issues
- Day 6: Capstone: Capture (and Present) the Flags

SOCIAL MEDIA, GEOLOCATION, AND IMAGERY

1. People Search Engines
2. Facebook Analysis
3. **LinkedIn Data**
4. Instagram
5. Twitter Data
6. Geolocation
7. Imagery and Maps

This page intentionally left blank.

LinkedIn.com

International career job site meant for creating networks of colleagues and friends

As of 2019, LinkedIn claimed over 645 million users across 200 countries[1]

Can use the site for company/organization profiling

With the information found in user profiles and company pages, many social engineering attacks become more successful

LinkedIn.com

LinkedIn is a professional networking web site that combines the working world with social media. According to its web site,[1] in 2019 they had over 645 million registered accounts across over 200 countries. LinkedIn's strengths are in its ability for people to connect to others. Creating, growing, and maintaining a professional network of people that you can reach out to for new jobs, advice, and friendship is core to LinkedIn.

With the amount of user data, connections, likes, and sharing that occurs on LinkedIn, it is a prime source of information for our OSINT tasks. The data we gather from this site's users and companies can, as we will see soon, be used in a variety of social engineering and other cyber attacks.

References:

[1] https://sec487.info/5b, September 17, 2019.

How LinkedIn Works for Users

Users create profiles filled with personal data such as:

- Current and prior jobs
- Education history
- Likes and interests

Users can "connect" to colleagues and friends

LinkedIn's power is in the friend of a friend connections, where I can see that my friend knows someone in a company I want to connect with

Varying levels of access to data:

- Public profile
- Authenticated users only (sock puppet can access)
- Restricted/private data

How LinkedIn Works for Users

LinkedIn is a social media web site that focuses on people and their connections to places that they have worked. When a new user signs up for an account, that person will submit a profile containing biographical data to the site. Common content is similar to what you may find on a resume or curriculum vitae: history of places a person has worked, the professional roles they have had, where they went to school, what they studied at school, and their job skills. Many of these sections have dates when the person attended a certain school or started and finished at a particular employer.

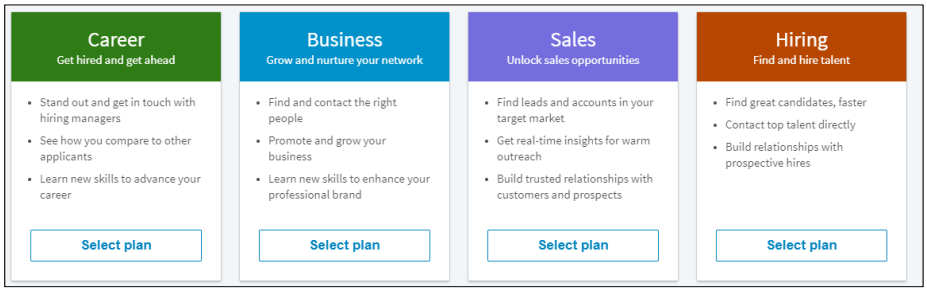
Once a profile is created, the user then "connects" to other people who they have worked with, attended school with, or would just like to connect with. These connections are key to the social networking aspect of the site. Each person you connect to is a first-order connection. Their connections are secondary to you and first order to them. If you want to be introduced to someone at another company, you can use the various connections of your friends to figure out who has a person from that company as a first-order connection. That person can then introduce you.

LinkedIn has three main levels of access to profile data: public, authenticated users only (here we use sock puppets to access the data), and private data. Most of the access to the data is through the web site, but there is an API and a LinkedIn directory for browsing user last names (https://sec487.info/5c).

How LinkedIn Works for Businesses

There are paid accounts at LinkedIn for premium users and also business use (recruiters, etc.)

The paid accounts harvest the data in users' profiles



How LinkedIn Works for Businesses

With over 645 million user profiles and with those profiles containing interesting biographical data, LinkedIn has quite a lot to offer to businesses that may wish to target certain users. Those people are generally people in sales (trying to sell something to a certain demographic) or in recruitment (trying to match people with open positions at their customers' companies).

LinkedIn offers at least four methods to pay them for access to some amount of their, well, your data. LinkedIn users can become a "premium"[1] user and view who is reading their profiles, among other benefits. This is important for OSINT analysts and one of the main reasons we use sock puppets when performing OSINT on LinkedIn. It would not be good for our targets to know that "Juanita Rega from the Los Angeles Private Investigator company" just looked up their profile. Sock puppets, if created well, can blend in and allow us to do our work without raising suspicion.

Business users can pay larger amounts to increase the number of private messages that they can send, get analytics on their posts, and "find great candidates faster"!

Image from https://sec487.info/ey, September 17, 2019.

How LinkedIn Works for OSINTers

What OSINT data can we obtain?

- Ties and connections
- Personal data of the user
  - What they like
  - Resume-like content
- Groups joined
- Who works for certain companies

What can we do with the data?

- Social engineering attacks
  - Pretexting
  - Phishing
- Link/Connection analysis
- Email harvesting

What about scraping the data and hosting it yourself?

How LinkedIn Works for OSINTers

If your target or their company uses LinkedIn, you may have a large amount of data to record and pivot upon. The obvious content to note about your target would be biographical: name, education, current and past employment, city and state where they reside, and any certifications or awards they included in their profile. Then you can harvest recommendations that others made (these people are connected to the target) and the target's interests and groups. Each of these could be import to your investigation.

People can, of course, use this profile information for a variety of more-nefarious purposes. Some examples include:

- We could perform social engineering attacks, such as phishing and pretexting. Both rely on the attacker establishing trust with the victim. An attacker with knowledge of a victim's background, connections, and interests could be much more successful in establishing that trust.
- If we are interested in finding out members of groups, we could perform link or connection analyses on who is connected to whom, moving profile to profile to discover group members.
- Our goal may be to find all the legitimate users at a certain company so that we can perform some password-guessing attack to gain access to the target company's systems. While this moves beyond the (mostly passive) activities of OSINT analysts, penetration testers and others may harvest email addresses and user names from LinkedIn data.

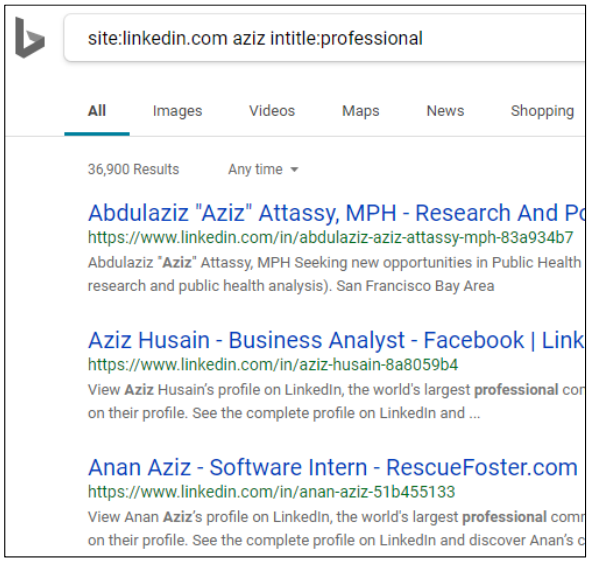
Depending upon how public the profile data is, we could iterate through certain profiles, scrape the data from the LinkedIn web pages, and then host it ourselves on our own web site. This definitely violates LinkedIn's Terms Of Service but, it has been done.

Searching for LinkedIn Data

Bing, Google, and DuckDuckGo have some LinkedIn public data indexed, too

Use a search string like:

site:linkedin.com NAME intitle:professional



Searching for LinkedIn Data

"Scraping" data from a web site means to request it and then store it off the original site. Some of the LinkedIn data is public due to the preferences of the users on that platform. To access this data, we can use a search engine and query for indexed LinkedIn content.

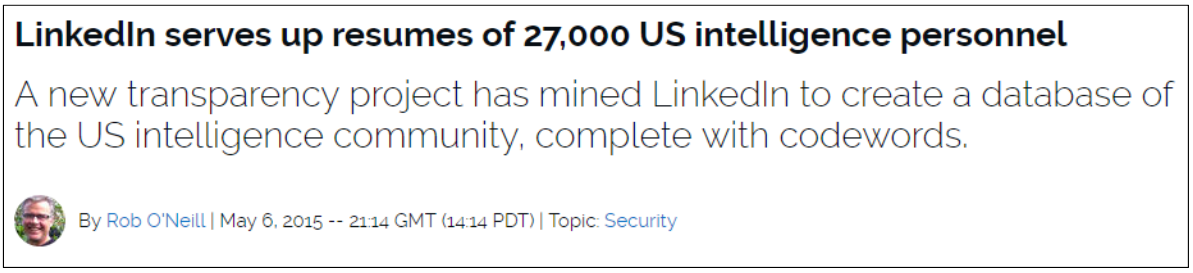
In the screenshot above, we see that searching for a person named "Aziz" appearing on the linkedin.com web site resulted in 36,900 results (https://sec487.info/sg). We can perform similar queries with Google (https://sec487.info/sh) and DuckDuckGo as well (https://sec487.info/si).

If we can do these simple searches and find profiles, other people can, too. Let's take a look at a case where someone wanted only certain profile results.

Image from https://sec487.info/sg, September 17, 2019.

ICWatch / Transparency Toolkit

In 2015, ZDNet[1] and other web sites announced:



This database is hosted at https://sec487.info/5j

ICWatch / Transparency Toolkit

In 2015, many people in the United States intelligence and military world were stunned when a group of people announced that they had mined 27,000 records from LinkedIn and put them in a public, searchable database. They also gathered resumes from sites such as Indeed.com and added information from the FBI/DHS compromise[2] to the database to augment the LinkedIn content. Using intelligence community code words and key words that may appear in US military and contractor resumes, over 400,000 records were normalized and made public. The site now has over 190,000 LinkedIn records, 173,000 Indeed records, and 45,000 from the FBI/DHS hack.

CLEARANCE WARNING: The wikileaks.org site is known to host classified data that, if you have a security clearance, you probably should not view. Visit this site at your own risk.

The Transparency Toolkit maintainers have even created a GitHub repository (https://sec487.info/5h) to make the data easily accessible. The searchable database is online at https://sec487.info/5j.

References:

[1] https://sec487.info/5i (Image reference)

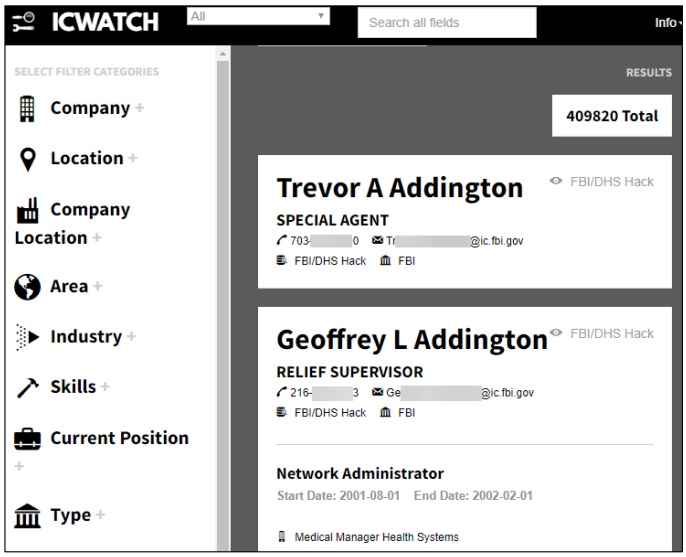
[2] https://sec487.info/5k

ICWatch Web Site

The web site is easy to use and, depending upon the data source, may provide:

- Names
- Emails
- Phone numbers
- Job history

You can use filters (on the left) to select certain records



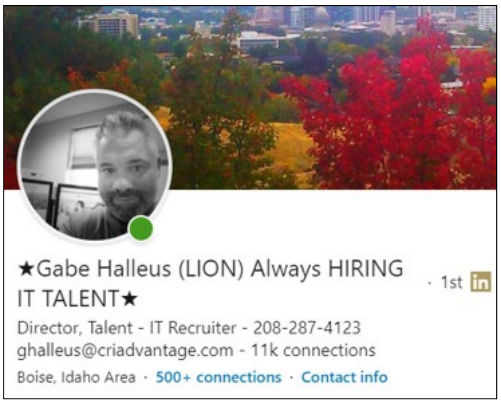
ICWatch Web Site

The content on the ICWatch Wikileaks site is presented in an easy-to-use manner. On the left side of the page is a set of filters that can be used to reduce the number of results and hone in on certain categories. There is also a search field at the top of the page for performing keyword searches. The results can vary from a page that looks very similar to LinkedIn or Indeed's data to one that contains email addresses and phone numbers (from the FBI/DHS hack).

Image from https://sec487.info/5j, September 17, 2019.

Do You Know About LiONs?

- LinkedIn Open Networkers[1] (LiONs)
- They accept all connection requests
- Think of them as hubs connecting people
- Great for connecting to your target organization, as they may already have contacts in that company
- Good people to target when you start a sock puppet



Do You Know About LiONs?

LinkedIn Open Networkers (LiONs)[1] are user profiles that accept almost any connection request. Think of these people as connection hubs that, by connecting to them, you may have access to hundreds or thousands of other people. A LiON's connections become your second-order connections when you and the LiON connect. If you are looking to target people in certain companies, LiONs can sometimes help out.

Because LiONs will accept connections from any other account, these are great first connections when you have a LinkedIn sock puppet account that you are creating. Start your account, connect to 5–10 LiONs, and your sock puppet looks more legitimate.

Image from https://sec487.info/lx, September 17, 2019.

Reference: [1] https://sec487.info/5a

Exporting LinkedIn Contact Data (1)

When a profile connects to another profile on LinkedIn, data is shared to the new contact:

- Name
- Company
- Email (must be enabled)
- Position

Remember those LiONs?

They can export hundreds or THOUSANDS of their connections and have the email addresses of their contacts

What email address do you use for your LinkedIn profile? Home or work?

People can watch you change jobs or companies and change names

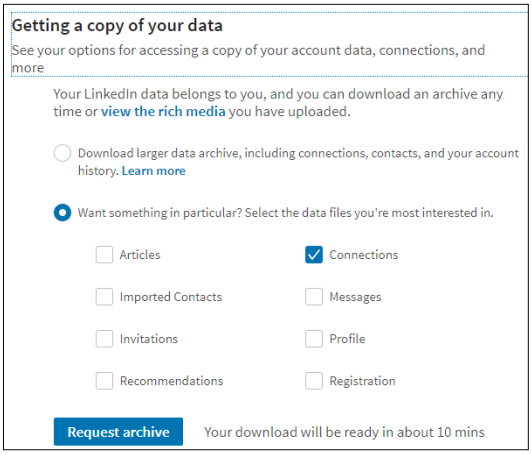
Exporting LinkedIn Contact Data (1)

One thing that is not clear to people when they accept or request connections to other user profiles in LinkedIn is that, once connected, you give some of your more-secret profile data to your connection (and they give their data to you). One of the most important pieces of data exchanged is the email address that the person used to set up their LinkedIn account with. Most people want to keep their LinkedIn accounts when they move from employer to employer, so they are more likely to use a personal email address when registering for LinkedIn. When connections are made, if you've noted on LinkedIn that you are willing to have your email discoverable by others, your connections get your email plus other content, like your first and last names, company you work for, and current role.

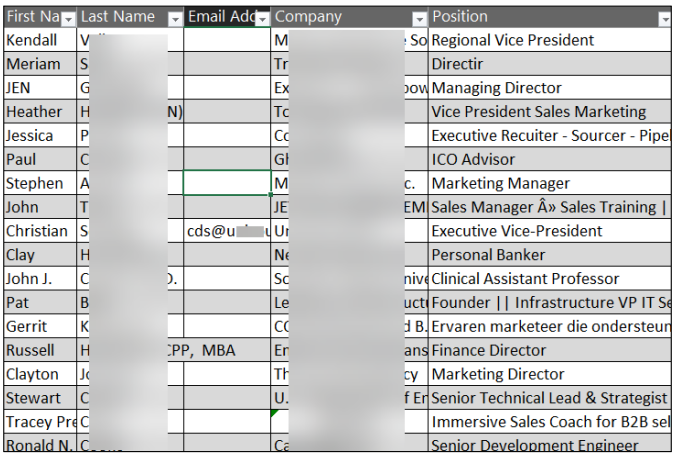
Now think about those LiONs we just spoke about. They have hundreds or thousands of connections. What if you stood up a LinkedIn account and made it a LiON, then collected all these email accounts and connections? Could be a valid information-gathering tactic already being used by people on the site. You could track people as they change jobs, change positions in their companies, and change their names (possibly indicating marriage or divorce). Downloading this data and examining it passively over time is an excellent method of watching a group of people.

Exporting LinkedIn Contact Data (2)

Export an archive



Sheet of contact data



First Na	Last Name	Email Add	Company	Position
Kendall	V		M	Regional Vice President
Meriam	S		Tr	Directir
JEN	G		Ex	Managing Director
Heather	H		Tc	Vice President Sales Marketing
Jessica	P		Cc	Executive Recuiter - Sourcer - Pipe
Paul	C		GI	ICO Advisor
Stephen	A		M	Marketing Manager
John	T		JE	Sales Manager Â» Sales Training |
Christian	S	cds@u	Ur	Executive Vice-President
Clay	H		Ne	Personal Banker
John J.	C		Sc	Clinical Assistant Professor
Pat	B		Le	Founder || Infrastructure VP IT Se
Gerrit	K		CC	Ervaren marketeer die ondersteun
Russell	H	PP, MBA	Er	Finance Director
Clayton	Jc		Th	Marketing Director
Stewart	C		U.	Senior Technical Lead & Strategist
Tracey Pre	C			Immersive Sales Coach for B2B sel
Ronald N.	C		Ca	Senior Development Engineer

Exporting LinkedIn Contact Data (2)

Micah Hoffman wrote a blog article about this process[1] in detail. The essential steps are to:

1. Visit the https://sec487.info/5l web page as a logged-in user.
2. Request archive of your data by clicking the button on the screen.
3. An email with a link to a ZIP file will be sent to the account that you use for LinkedIn.
4. Click the link in the email and download the ZIP file.
5. Decompress the file and extract the Connections.csv file.
6. Open this CSV in your favorite text editor or spreadsheet application (Google Sheets, Excel, Calc, etc.).

Once you look into the sheet, you will see content that looks similar to that shown in the above slide, with your profile's connections and their information.

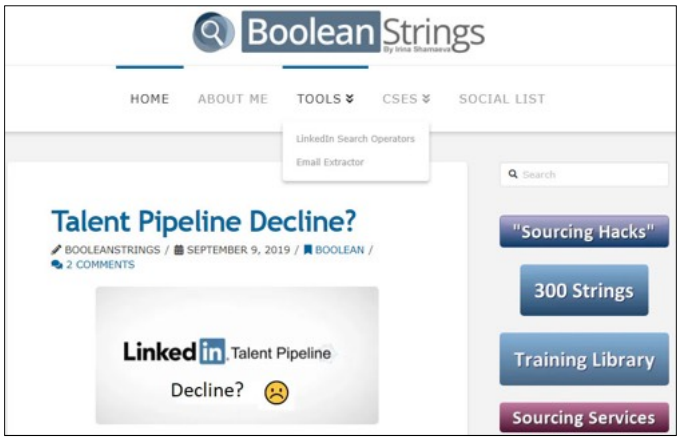
Reference: [1] https://sec487.info/5m

Recruiters and Sourcers Know LinkedIn

Since LinkedIn focuses on jobs, recruiters and sourcers use it a lot

They discuss tools and techniques to find eligible candidates on their web sites

booleanstrings.com has shown to be one of these excellent resources



Recruiters and Sourcers Know LinkedIn

Because they are looking for people to fill their open positions, recruiters and sourcers are power users of LinkedIn.com. The booleanstrings.com web site has become a terrific resource for OSINT analysts looking to stay current on the inner workings of LinkedIn. This blog has frequent posts on how to harvest data, find people, and use tips and tricks to filter LinkedIn results.

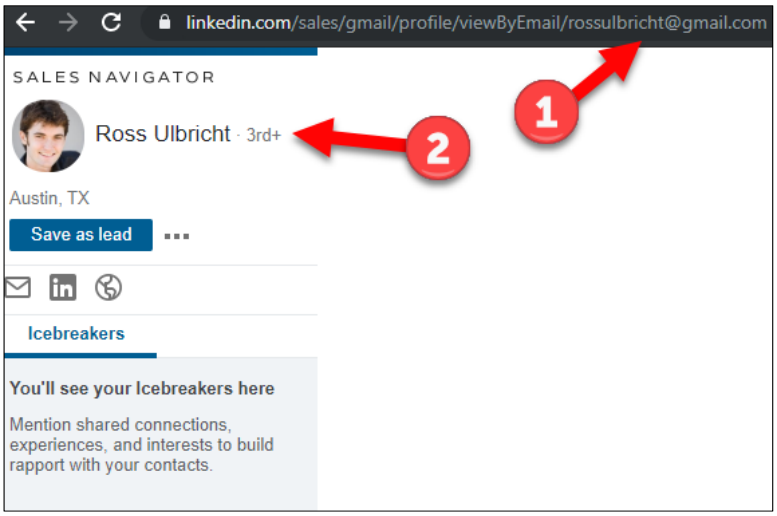
This site hosts archival blog posts, links to browser extensions, and tools that people looking to find people to hire might be interested in using. There are several Google Custom Search Engines (CSEs) the site links to from its main menu. These CSEs can help us understand the advanced methods recruiters use to gather data about their targets.

Image from https://booleanstrings.com/, September 17, 2019.

Look Up LinkedIn Accounts by Email

As an authenticated user, you can use a sales feature of LinkedIn to convert an email address to a LinkedIn account

Users with private accounts will not be found using this technique



Look Up LinkedIn Accounts by Email

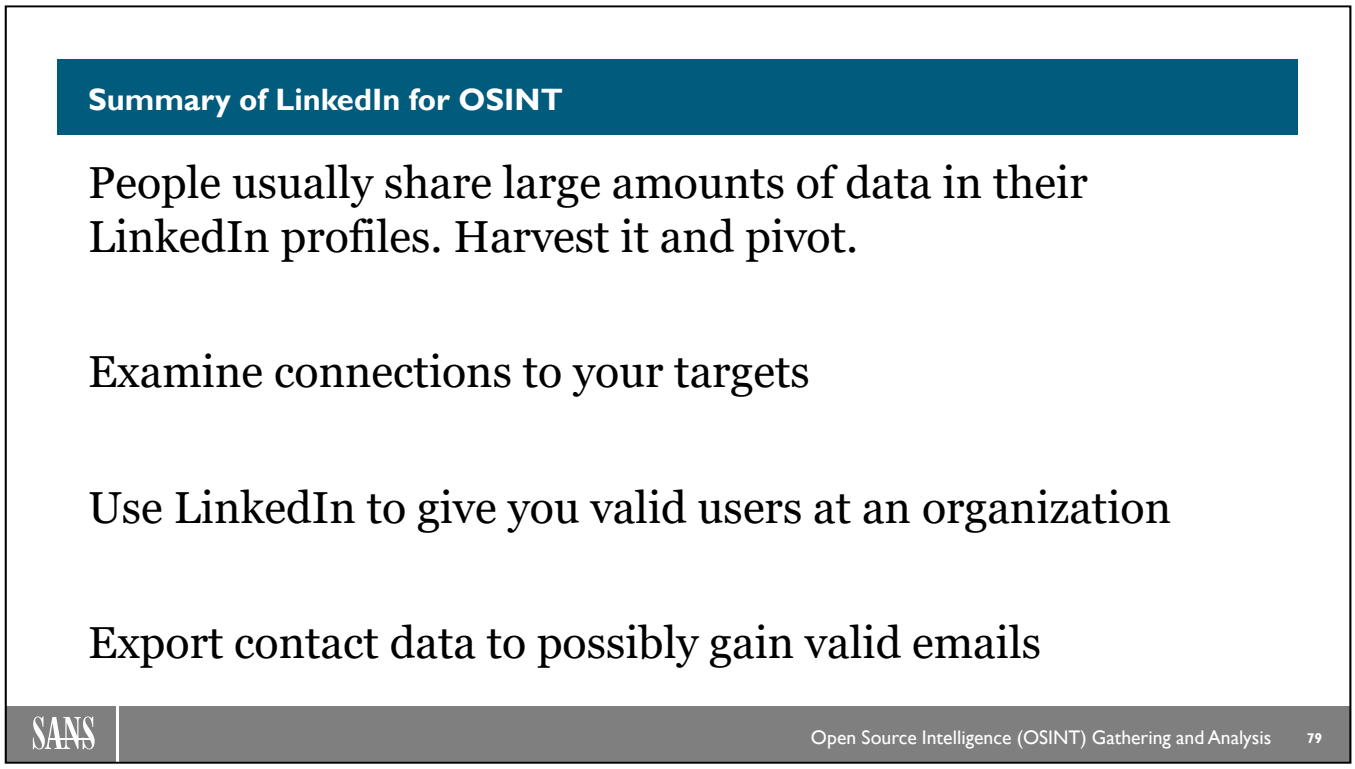
This technique was noted in a Bellingcat article[1] and uses an authenticated feature of the site called the Sales Navigator. Using the target's email address, we can have LinkedIn resolve it to a matching LinkedIn account. The URL to achieve this is:

```
https://www.linkedin.com/sales/gmail/profile/viewByEmail/EMAIL
```

In the above slide, we substituted Ross Ulbricht's email address (rossulbricht@gmail.com) in the spot where we had the "EMAIL" (arrow 1) and received the LinkedIn profile of the owner of the Silk Road Marketplace (arrow 2).

Image from https://sec487.info/sk, September 17, 2019.

Reference: [1] https://sec487.info/sj



Summary of LinkedIn for OSINT

Wrapping up our view of the professional networking site LinkedIn, we now understand that, when we find a target or target organization with LinkedIn data, we can:

1. Harvest the data. Download it to a computer and analyze it. Consider pivoting to verify and validate the data we collected.
2. We can look for connections to determine members of groups and who knows who.
3. LinkedIn can give us the first and last names of users at target organizations. If we can find out the email format for that organization's email system, then we can create possibly valid email addresses to use in attacks.
4. Finally, we need to understand that we can export the contact data (including some valid emails) from all of our connections, keeping in mind that our connections can do the same for our data (or our sock puppets).

The data on LinkedIn can be tremendously useful for certain types of investigations.

Course Roadmap

- Day 1: Foundations of OSINT
- Day 2: Gathering, Searching and Analyzing OSINT
- **Day 3: Social Media, Geolocation, and Imagery**
- Day 4: Networks, Government, and Business
- Day 5: The Dark Web, Breach Data, and International Issues
- Day 6: Capstone: Capture (and Present) the Flags

SOCIAL MEDIA, GEOLOCATION, AND IMAGERY

1. People Search Engines
2. Facebook Analysis
3. LinkedIn Data
4. **Instagram**
5. Twitter Data
6. Geolocation
7. Imagery and Maps

This page intentionally left blank.

What Is Instagram?

Instagram is an image- and video-sharing social network

Mostly mobile application with a web interface as well

Post media, comment, and/or like other's content

Public and private accounts

What Is Instagram?

The main purpose of Instagram.com is to share videos and photos with followers. Accounts can be public, where all of the posts are not protected, or private, where, prior to viewing a user's content, a user account must be approved by the sharing user. While there is a web interface, most users share and browse images via the mobile applications that can be found in both Apple's and Google's application stores.

Instagram accounts are free and require, at the time of this writing, no email or phone validation. Creating a new account is fast and easy.

Instagram for OSINT

What data can we glean?

- Image content
  - Who is in the photos/videos?
  - What other things are shown?
- When and where were posts made
- Relationships between users
- User name harvesting
- Email address and phone of target (mobile app only)
- Hashtag monitoring

Instagram for OSINT

As with many social networks, the content and metadata in what is posted can be valuable in our OSINT work. When we examine Instagram for OSINT purposes, there are certain things we look for:

- The content of the image or video is of obvious concern. What is in the foreground? What might appear in the background? What people are in the media? Sometimes the background content is just as or more important than the main focus of the media.
- If the post is geolocated, what is the position that is tagged to the post. Users choose what location is tagged to their posts, so we do not trust that data. Seek corroborating content from the image/video and the post comments.
- Sometimes the important part of a social media post isn't the content but when it was posted. Instagram media is tagged with the date and time (for example, datetime="2019-09-15T11:10:39.000Z") of each post.
- Instagram is a social network, so tracing who is following whom could be useful in an assessment. For public user profiles, we can just visit the "followers" (what users are followers of the current target) and "following" (who is the target account following) links and harvest all of the accounts. For private accounts, we may need to look at whose posts they are commenting on to determine their social network.
- We can gain user names from posts and then look for them across other web sites.
- The mobile version of Instagram sometimes allows the retrieval of the phone number and email of the target account.
- Finally, Instagram has a hashtag feature that can be used to monitor activities, sentiments, and events.

In the image above from the Manchester United Instagram account (https://sec487.info/r-), we can see the media posted on the left of the image above and then comments by other users/followers.

Image from https://sec487.info/rz, September 16, 2019.

The OSINT Curious Project Blog Posts

Technisette, Kirby Plessas, and others at The OSINT Curious Project have 2 excellent blogs describing how to examine Instagram content and profiles

In the coming slides, we will examine their best practices, tools, and techniques

The OSINT Curious Project Blog Posts

Technisette, Kirby Plessas, Sector035, and others at The OSINT Curious Project pooled their knowledge and wrote two in-depth blogs about how to examine, scrape, and store data from Instagram.com. We will use these industry-leading OSINT blog posts as a guide for our analysis of this social media platform.

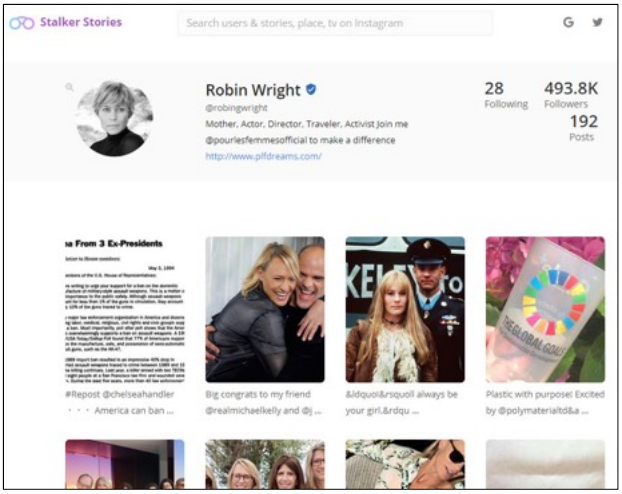
Images from https://sec487.info/x1 and https://sec487.info/x2, October 3, 2019.

Offline Viewing of Public Content

Several sites allow for offline web viewing of public Instagram content

- https://stalker-stories.com
- https://piknu.com
- https://www.pictame.com

Some present metrics; others just show the content as indexed



Offline Viewing of Public Content

There are times when you may wish to see offline or historical content from an account or see the metrics and statistics about an account's usage. In these cases, or if you do not wish to use the Instagram app or web site for your OSINT, you can use some other sites that either copy public Instagram content or analyze it.

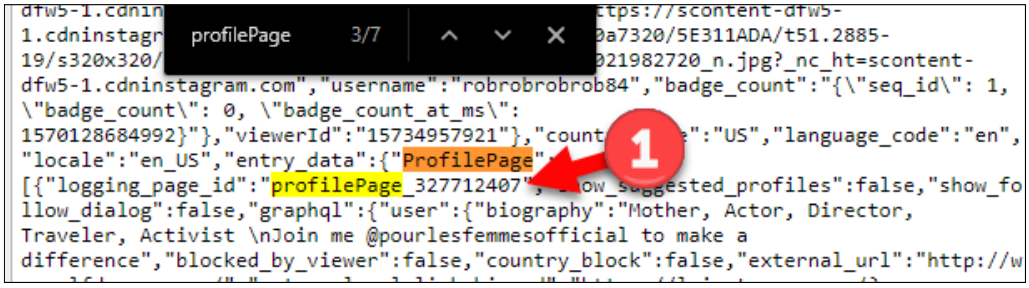
- https://stalker-stories.com - Retrieve public profile information from user accounts, search for posts with certain hashtags, and explore Instagram content by location.
- https://www.pictame.com - Offline viewing of Instagram content mixed with analysis and common posts/hashtags.
- https://piknu.com - Offline viewing of Instagram content.

Image from https://sec487.info/s5, September 16, 2019.

Instagram User IDs

Each Instagram account has a unique numeric ID found in the HTML source code within a browser

Search for the string "profilePage_#" and look at the # value

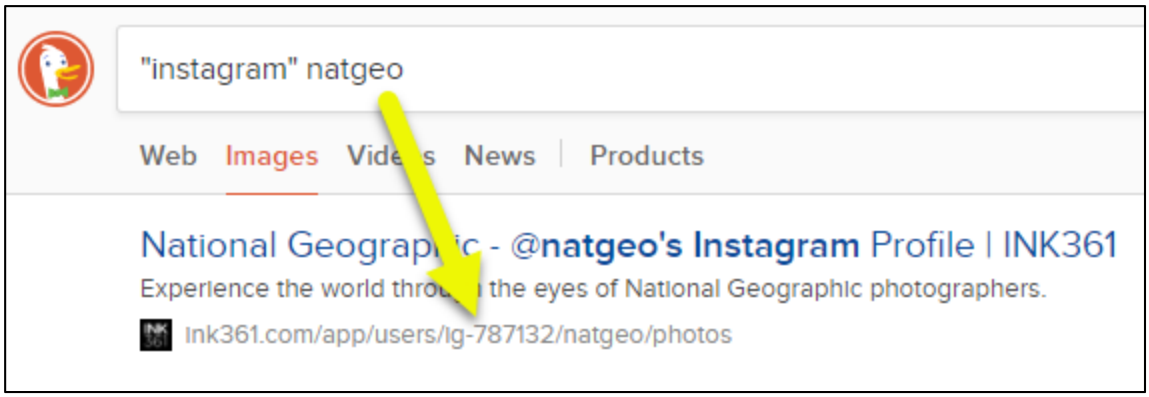


Instagram User IDs

Every Instagram user has a unique user name but also a numeric ID, which can be found by looking in the source code of the web pages in a browser. Searching for the term "profilePage_" reveals a value that is the user's numeric ID. In the above slide, the numeric ID for the "robingwright" user account is 327712407.

Always record the Instagram ID, as it will be used later to identify activity by this account and is unique to this specific account.

Image from https://sec487.info/x3, October 3, 2019.

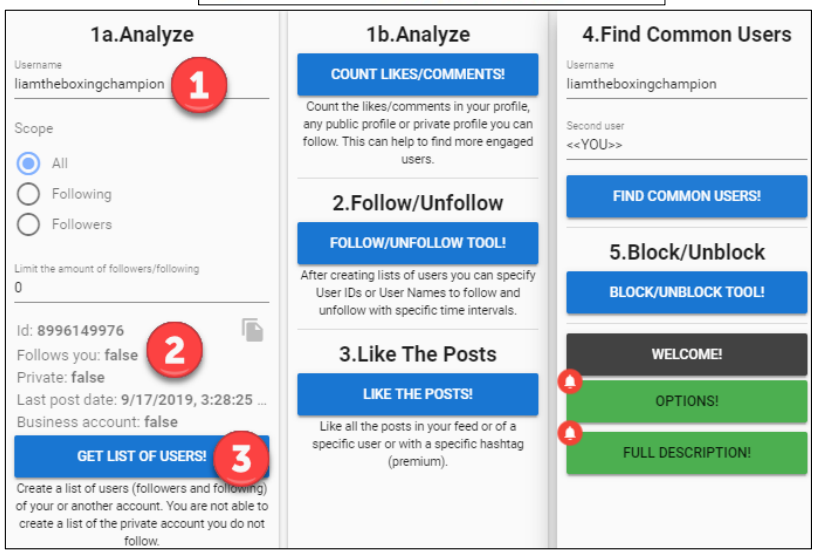


Helper Tools for Instagram (1)

Google Chrome extension that requires Instagram account for most features

Retrieves Instagram:

- Account data for a target
- Followers
- Comments and likes on posts



Helper Tools for Instagram (1)

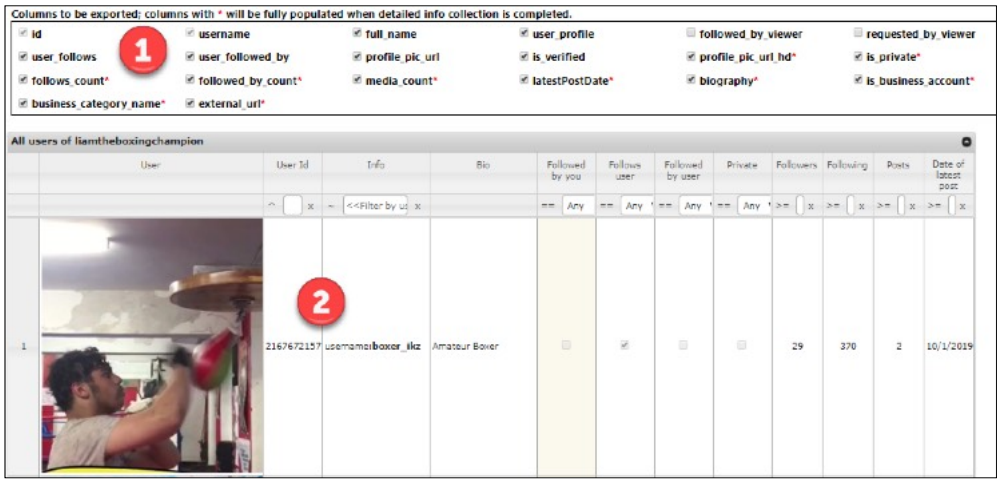
The Helper Tools for Instagram Google Chrome extension (https://sec487.info/ma) can help do Instagram user analysis and extraction of data. For most of the work, it requires you to be authenticated to Instagram with a valid user account. Also note that the tool can only retrieve public information. Private Instagram user accounts cannot be accessed using this tool. It can grab what user accounts follow a target account, analyze who is liking and commenting on a target's posts, and display account details about the target account. It also allows for the downloading of this data in both CSV and Excel spreadsheet formats.

In the above slide, we launched the tool while we were on the liamtheboxingchampion Instagram profile page (https://sec487.info/x7) shown at "1" above. The tool gives a brief summary (2) of the target account's Instagram ID, if it is private, when they last posted, and if it is a business account. Clicking the "GET LIST OF USERS!" button (3) launches a separate window, shown on the next slide.

Helper Tools for Instagram (2)

Output is in 2 stages: brief (fast) and full (slower)

Larger follower lists take longer to retrieve



Helper Tools for Instagram (2)

Examining the followers of the liamtheboxingchampion Instagram account using the Helper Tools for Instagram extension is simple and takes time. Visit the profile page of a public account and then select to retrieve their user list (as shown on the previous slide).

At first, the extension will quickly get a cursory amount of information from the followers. It will display those and work its way through the follower list. Then, it will reprocess the list and gather more in-depth data about each user. Shown above is the output after the longer in-depth data-gathering pass.

At the top of the image, we see the different parameters we can export from the tool once the data gathering has completed (1). We selected all of the columns and will show the Excel file in the coming slide. In the bottom portion of the image above (2), we see details about each account that follows our target.

Helper Tools for Instagram (3)

	username	full_name	user_profile	biography	is_business_account
188	capitolebtw	Capitole B	https://www.instagram.com/capitolebtw	Boutique de bijoux en	TRUE
189	itm.k2	K2InDaMakin	https://www.instagram.com/itm.k2	NGx The Lord Is My Guardia	FALSE
190	hamze_elhoussari	humz buckets	https://www.instagram.com/hamze_elhou		FALSE
191	finleyrmeehan	Fin	https://www.instagram.com/finleyrmeeha		FALSE
192	bvonenoch	Berit Von Enoch	https://www.instagram.com/bvonenoch	Photography // Boxing // Liftin	TRUE
193	ja.mie174	Jamie	https://www.instagram.com/ja.mie174	Sc:@jgalley31	TRUE
194	radsportsskt	ad Sport	https://www.instagram.com/radsportsskt		FALSE
195	coachcharlotte92	Coach Charlotte	https://www.instagram.com/coachcharlot	#boxingislife #boxing	TRUE
196	chez.whu	CHEZ	https://www.instagram.com/chez.whu		FALSE
197	davidpritchard030592	David Pritchard	https://www.instagram.com/davidpritchar		FALSE
198	jiyoo21		https://www.instagram.com/jiyoo21		FALSE
199	xkittyxxgracex	xkittyxxgracex	https://www.instagram.com/xkittyxxgrace	Linking Teen @_ki	FALSE
200	shahzad.azam.5201	Shahzad Azam	https://www.instagram.com/shahzad.azar		FALSE
201	natali_moroziki	Natali	https://www.instagram.com/natali_moroz	Have the best husband @boxe	FALSE

Helper Tools for Instagram (3)

The output Excel file has too many columns to display in this slide, so we hid some of them. Above, you can see the followers of our target account, including the Instagram user name (1), their full name (2), profile URL (3), biography (4), and whether the account is a business account (5). Just collecting and analyzing this data could help your OSINT case and possibly give you the data you need.

We are going to dive a little bit deeper because we know that business profiles on Instagram have email addresses and phone numbers we can retrieve. Let's take a closer look at "coachcharlotte92" (6) above, who has a business profile (7).

Instagram Business Accounts

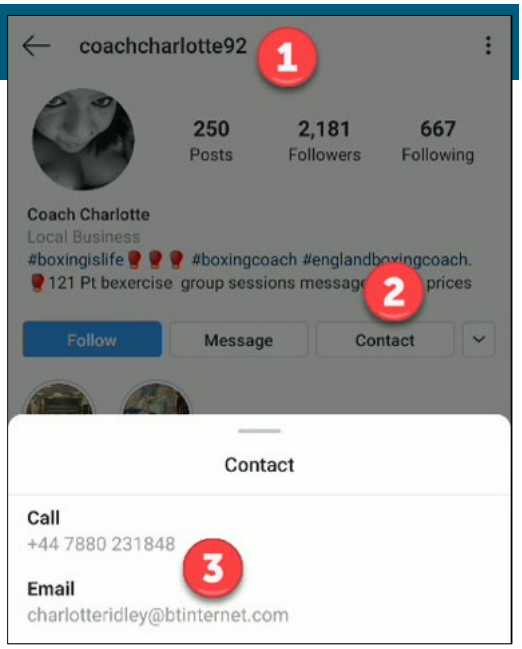
If a user has elected to change their account to a "business" profile, they have to enter in email and/or phone

We can find this information using 2 techniques:

1 - From the Instagram mobile app

2 - Via the Instagram API

Here is "coachcharlotte92" via mobile



Instagram Business Accounts

Within the Instagram social media platform, users can select to make their user accounts a "business" profile through a simple setting change.[1] Once they do this, they will be required to enter an email and/or phone number for their business into the app. This data is public but inaccessible from the Instagram web site through the normal profile view page (https://sec487.info/x9).

Above, we visited the "coachcharlotte92" Instagram account (1) we found to be a business profile in the previous slide. This image is from the Instagram mobile application. To view her contact information within the app, click the "Contact" button (2), and her details are shown (3). The target profile in your cases may not have the "contact" button but, instead, might have a "Call" button if they only have input a phone number.

References:

[1] https://sec487.info/x8

Instagram API for Profiles

As an authenticated user, you can request profile data about an account through the API

https://i.instagram.com/api/v1/users/#/info/

May need to change user agent to Instagram mobile app (see notes)


```
{
  "user": {
    "pk": 256031966,
    "username": "coachcharlotte92",
    "full_name": "Coach Charlotte",
    "is_private": false,
    "profile_pic_url": "https://scontent-dfw5-1.cdninstagram.com/vp/3096041035cac0291313d52d7ef2df5d/5E219B8C/t51.2885-19/s150x150/14262731_1746138995651351_8368149086494261248_a.jpg?_nc_ht=scontent-dfw5-1.cdninstagram.com",
    "profile_pic_id": "1341560425128509011_256031966",
    "is_verified": false,
    "has_anonymous_profile_picture": false,
    "media_count": 250,
    "geo_media_count": 0,
    "follower_count": 2181,
    "following_count": 667,
    "following_tag_count": 0,
    "biography": "#boxingislife🥊🥊🥊 #boxingcoach #englandboxingcoach.
        🥊121 Pt bexercise  group sessions message me for prices",
    "external_url": "",
```


Instagram API for Profiles

Once we know the Instagram user's ID (pulled from the Helper Tools for Instagram or the page source), we can perform additional lookups against their account. For this to work, we need to authenticate to Instagram using a valid account. Sector035 noted in a tweet (https://sec487.info/sb) that people can use the API and the URL format of https://i.instagram.com/api/v1/users/#/info/ (where you replace the # with the Instagram user's ID number). This API request will retrieve JSON-formatted output (shown above).

Using the API and receiving JSON content makes this an easy method to scrape data from Instagram. We can make requests and collect the data into databases or text files for long-term storage. Lately, the Instagram API requires the mobile app's user agent string to be presented before it will provide valid API response. The user agents found at https://sec487.info/xa work for now and are captured below for reference.

iPhone:
Mozilla/5.0 (iPhone; CPU iPhone OS 9_3_2 like Mac OS X) AppleWebKit/601.1.46 (KHTML, like Gecko) Mobile/13F69 Instagram 8.4.0 (iPhone7,2; iPhone OS 9_3_2; nb_NO; nb-NO; scale=2.00; 750x1334

Android:
Mozilla/5.0 (Linux; Android 6.0.1; SM-G935T Build/MMB29M; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/51.0.2704.81 Mobile Safari/537.36 Instagram 8.4.0 Android (23/6.0.1; 560dpi; 1440x2560; samsung; SM-G935T; hero2qltetmo; qcom; en_US)

In the above image, we see some of the same data that was in the Helper Tools for Instagram XLSX output and displayed in the user's profile page in the application.

Image from https://sec487.info/xb, October 3, 2019.

Instagram API for Business Profiles

Since our target example account is a business account (1), the previous slide's API call retrieves the profile contact information (2 and 3)


```
50      "business_contact_method": "CALL",
51      "category": "Local Business",
52      "city_id": 0,
53      "city_name": "",
54      "contact_phone_number": "+447880231848",
55      "is_call_to_action_enabled": false,
56      "latitude": 0.0,
57      "longitude": 0.0,
58      "public_email": "charlotteridley@btinternet.com",
59      "public_phone_country_code": "44",
60      "public_phone_number": "7880231848",
61      "zip": "",
62      "instagram_location_id": "",
63      "is_business": true,
64      "account_type": 2,
```


Instagram API for Business Profiles

The coachcharlotte92 account, since it is a business profile, contains additional contact data as we scroll down the JSON results from the API. In the above slide, we see that this is a business account (1), her phone number (2), and her email (3).

I'm also betting that you are starting to see where tools like the Helper Tools for Instagram get all the bits of profile data found in the XLSX output file. Yes! From API calls made to Instagram. Now you can make those same calls without using tools!

Image from https://sec487.info/xb, October 3, 2019.

Instagram API for Posts

As an unauthenticated user, you can pull a public post's content

Formatted in JSON

Contains most everything you need except for the actual media

```
// 20191003175855
// https://api.instagram.com/oembed/?url=http://instagram.com/p/BT1hYIBgIda/ (1)

{
  "version": "1.0",
  "title": "Visiting my friend Grover. Had a nice talk about refugee children. Stay tuned! \nFor my young friends: please share with your mommy and daddy. \n@sesamestreet @theirc #100andchange",
  "author_name": "mandypatinkin", (2)
  "author_url": "https://www.instagram.com/mandypatinkin",
  "author_id": 4557309992, (3)
  "media_id": "1510260043470112602_4557309992",
  "provider_name": "Instagram",
  "provider_url": "https://www.instagram.com",
  "type": "rich",
  "width": 658,
  "height": null,
```


Instagram API for Posts

Most APIs require authentication prior to retrieving data, but that is not how the Instagram API works for public posts. We can make a single web call to the web site and retrieve a post's content (containing the posted comments, author name and ID, hashtags, etc.) in the JSON format. JSON is easily parsed by scripting languages such as Python and Ruby and can be viewed quite simply as formatted text using modern browsers (and possibly a JSON addon).

Above, we show the response from the request https://api.instagram.com/oembed/?url=http://instagram.com/p/BT1hYIBgIda/ (https://sec487.info/be). For us to request data about a post, we need to send the post's ID to Instagram (1). In this example, we see who the poster of the media was (2) and what his Instagram ID was (3).

Image from https://sec487.info/be, October 3, 2019.

Retrieving Instagram Profile Data

Get private and public profile data unauthenticated

https://www.instagram.com/***USER***/?__a=1 *(those are 2 "_")*

Example:
https://www.instagram.com/**coachcharlotte92**/?__a=1

```
// 20191003180321
// https://www.instagram.com/coachcharlotte92/?__a=1

{
  "logging_page_id": "profilePage_256031966",
  "show_suggested_profiles": false,
  "show_follow_dialog": false,
  "graphql": {
    "user": {
      "biography": "#boxingislife🥊🥊🥊 #boxingcoach #engl
                                  🥊121 Pt bexercise  group se
prices",
      "blocked_by_viewer": false,
      "country_block": false,
      "external_url": null,
      "external_url_linkshimmed": null,
      "edge_followed_by": {
        "count": 2181
      },
      "followed_by_viewer": false,
      "edge_follow": {
        "count": 667
```


Retrieving Instagram Profile Data

There is a URL that will retrieve data about an Instagram user's profile. If the profile is private, less data is returned than if it is public. The URL is simply https://www.instagram.com/*USER*/?__a=1, with 2 underscore (_) characters, where you replace the word "USER" with the Instagram user's account name. If, for instance, you were interested is examining Coach Charlotte's profile, you could enter https://www.instagram.com/*coachcharlotte92*/?__a=1 (https://sec487.info/xc) in your web browser (or use a command-line tool like curl) and you would receive JSON-formatter content such as what you see on the slide above.

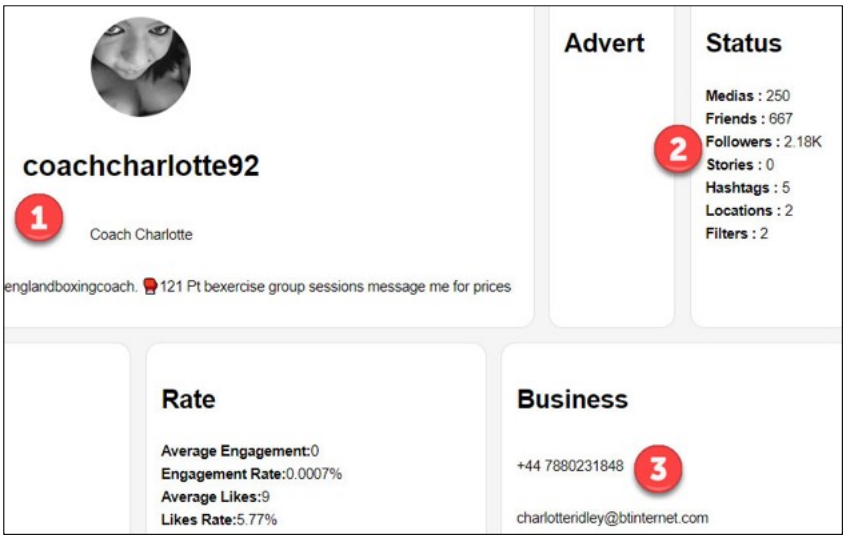
Image from https://sec487.info/xc, October 3, 2019.

Stalkture.com Instagram Analytics Site

Stalkture.com analyzes Instagram profiles AND reveals helpful data to us

Take coachcharlotte92's profile

See the business data (3)?



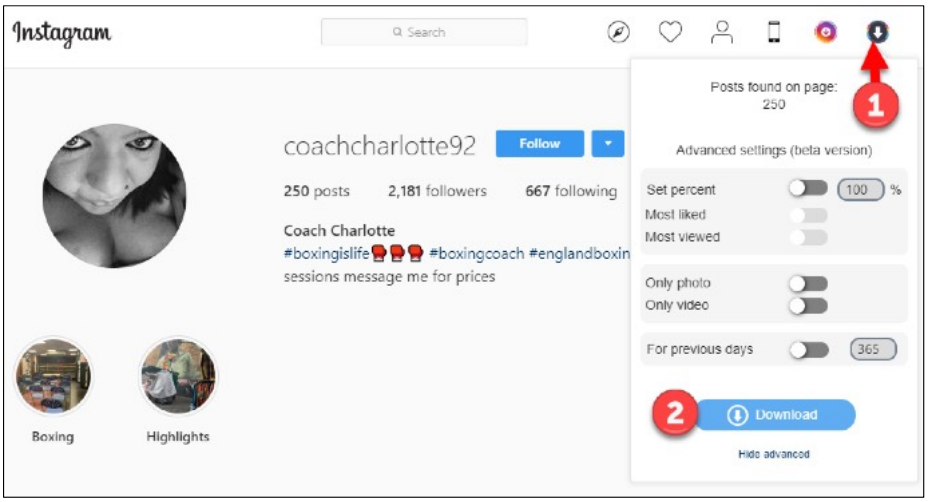
Stalkture.com Instagram Analytics Site

We mentioned some sites that perform off-Instagram caching public content and create some metrics and stats for profiles. stalkture.com does this, and a little bit more, because it will extract the contact details from business profiles. Above, we pulled up coachcharlotte92's profile in the site (1) and, in addition to stats (2), we can see the contact information in the profile (3).

Image from https://sec487.info/xh, October 3, 2019.

Retrieving Instagram Images

Downloader for Instagram™ + Direct Message Google Chrome extension downloads user media



Retrieving Instagram Profile Data

The Downloader for Instagram™ + Direct Message Google Chrome extension (https://sec487.info/xd) allows users to download some or all of the images and videos on an Instagram user's profile via a simple click. To use:

1. Install and enable the extension.
2. Visit your target's profile.
3. Click on the extension icon (1).
4. Select your settings (shown is the advanced menu).
5. Click the Download (2) button.

The extension will retrieve the images and place them inside a ZIP archive file on your system.

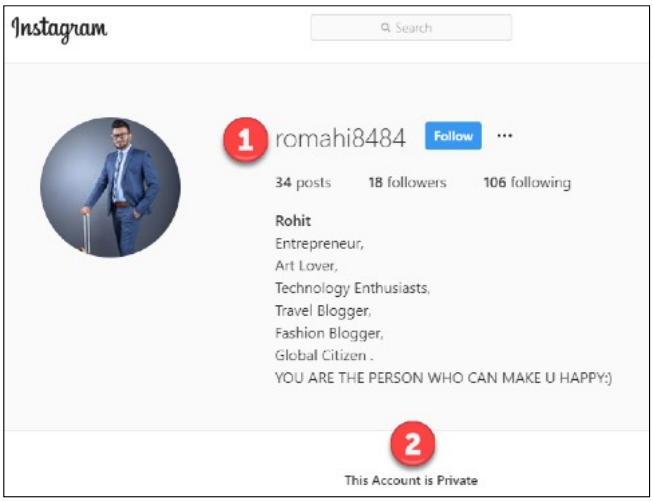
Image from https://sec487.info/x9, October 3, 2019.

Determining Relationships

With private Instagram accounts, we can infer who they follow based on activity

We can also find out what public Instagram pages the user is commenting on using search engines

Search for: site:instagram.com "USERNAME"



Determining Relationships

For public Instagram accounts, finding the friends or connections of a certain account is a matter of visiting the "followers" and "following" links and recording all the users. But for private accounts, we need to employ a different technique. What we can do is perform a search engine search for our target and the "site:Instagram.com" directive. What we will get is any public posts that the search engine has indexed that have comments from the target account.

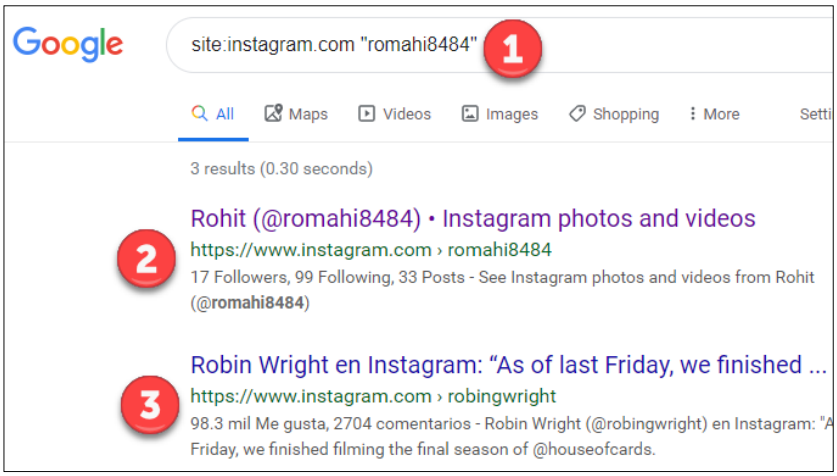
Let's take the user "romahi8484" account (https://sec487.info/x6) as an example. As shown above, the account is private (2), and we cannot see followers or following users.

Searching for Public Content

Performing a Google search for:

site:instagram.com "romahi8484" (1)

We see his profile (2) and another entry returned for a Robin Wright post (3)



Searching for Public Content

We searched for `site:instagram.com "romahi8484" using google.com` and saw two results: one for his private profile and one for a post he commented on. We will go visit that post.

Reference:

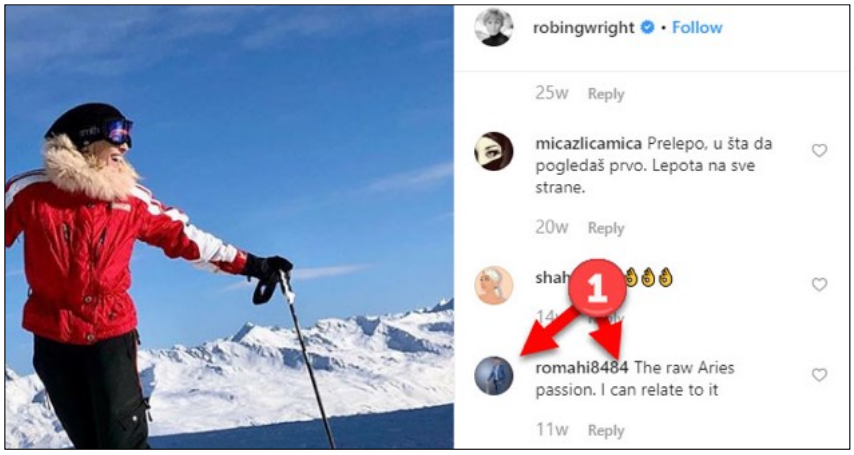
[1] https://sec487.info/x5

Finding Private Public Content

Visit the public post from actor Robin Wright

Scroll down to see the comment from romahi8484

Now we know one other account he follows



Finding Private Public Content

Now we visit the public post (https://sec487.info/x4) of actress Robin Wright that we found in the Google results. Scrolling down the comments we find the public comment (1) made by our target. We can see this because, while his account is private, the comments he made were on a public post.

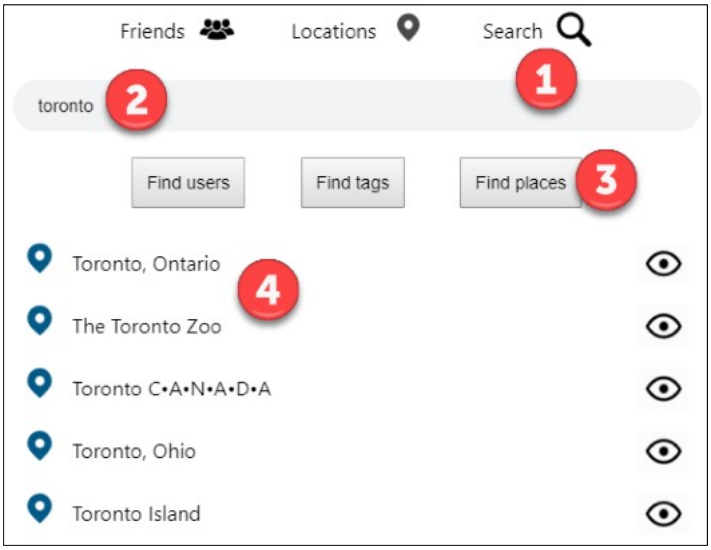
Image from https://sec487.info/x4, October 3, 2019.

Searching for Hashtags and Locations

Using the previously mentioned Downloader for Instagram™ extension, we can search for hashtags and locations

Click this icon:

Then choose how and what to search



Searching for Hashtags and Locations

The https://www.instagram.com/explore/tags/HASHTAG/ URL can be used to examine posts with a certain hashtag (replace HASHTAG with the tag you wish to search for, like https://www.instagram.com/explore/tags/torontofood/). While searching for people and tags can be relatively simple, using this extension's interface to bring up similar search results can assist you in locating not only your targets but other, associated tags and places.

In the above example, we searched for "Toronto" as a general search (1 and 2) then clicked the "Find places" button (3). Our results not only contained the city of Toronto in Canada, but also lesser-known locations that Instagram knows about, like The Toronto Zoo. Each location has its own unique identification number. Using this approach to searching is efficient and can help you find those unique IDs.

You can also search for locations within the Instagram application. Look for the drop icon in the results. Alternatively, visit the https://www.instagram.com/explore/locations/ (https://sec487.info/xg) page and browse through known locations.

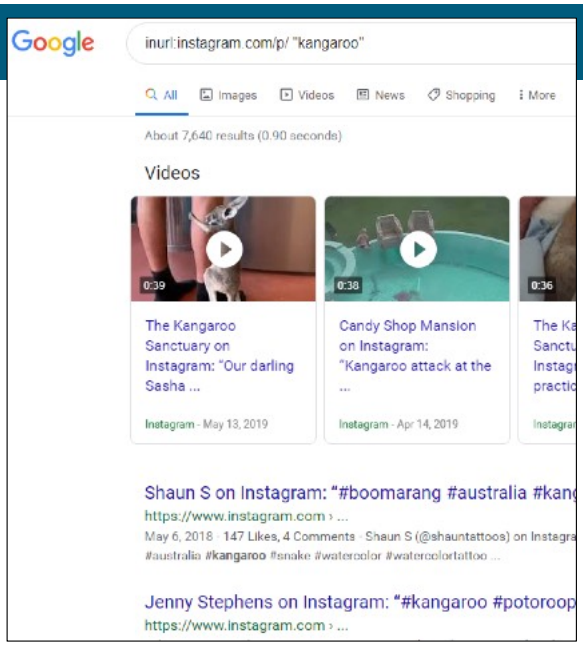
Searching for Keywords

Looking to find public posts with a certain term?

Use Google and an advanced string like:

inurl:instagram.com/p/ “KEYWORD”

Here we searched for "kangaroo"



Searching for Keywords

Perhaps you are not looking for a hashtag, but just some words that may have been used in Instagram posts. If your target profiles publishing this data are public, the OSINT Curious blog post suggests using a Google dork like inurl:instagram.com/p/ “KEYWORD” (replace KEYWORD with your keyword). We used the word "kangaroo" with this dork and found over 7,600 results.

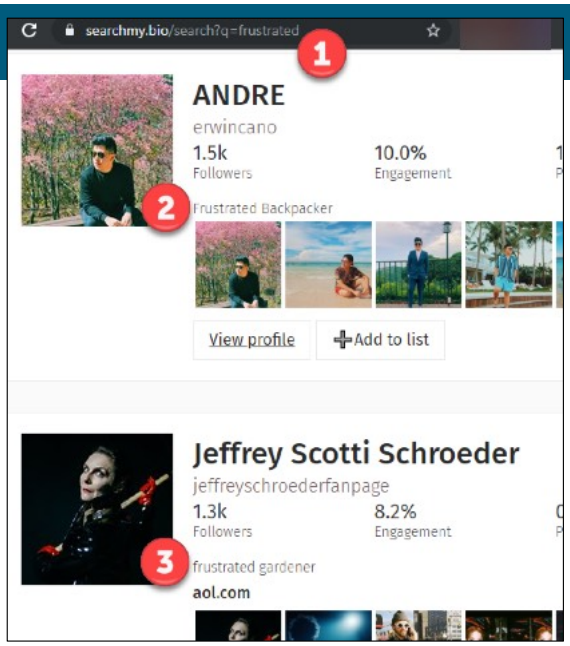
Image from https://sec487.info/xe, October 3, 2019.

Searching Inside Instagram Bios

Is the content you are looking for in profile bios?

There is a site for that. https://searchmy.bio focuses on searches in Instagram bios

In the image on the right, we searched for bios with the word "frustrated" in them



Searching Inside Instagram Bios

Another tip from the OSINT Curious blog post for searching inside profile bios is to use the searchmy.bio web site. In the above search, we looked for bios that had the word "frustrated" in them (1) and found 334. You can see at “2” and “3,” above, the "frustrated" strings in the profiles of two users.

Image from https://sec487.info/xf, October 3, 2019.

Download All Public Instagram Posts

"Instagram-scraper" is a Python script that will download all public posts from a user. It can save user comments, location and tag data, and metadata from the images too.

```
student@sec487 (          ) :/opt/tools/instagram-scraper$ instagram-scraper --comments --include-location
--maximum 20 coachcharlotte92
Searching coachcharlotte92 for profile pic: 100% 1/1 [00:00<00:00, 918.39 images/s]
Downloading: 100%|          | 21/21 [00:08<00:00,  2.62it/s]s/ media]
Searching coachcharlotte92 for posts: 18 media [01:15,  4.22s/ media]
```

```
student@sec487 (19:33:33) :/opt/tools/instagram-scraper$ l coachcharlotte92/
14262731_1746138995651351_8368149086494261248_a.jpg  69251739_1633602806764969_6473560203800230810_n.jpg
59834942_758122497918299_2940543165443264645_n.jpg   69333078_505457373576345_8015087793474859587_n.jpg
60126018_675342789570990_437178257558052192_n.jpg    69368404_228441711460148_9116059769172791260_n.jpg
61771837_471952173370657_804448[illegible]5227124_n.jpg   69371706_125409472091474_6337873476737896027_n.jpg
62012778_1044081459095452_11694[illegible]6595113_n.jpg   69849934_954067214936171_5853191628168077267_n.jpg
62470726_182884462709390_126455[illegible]142192_n.jpg    70488019_177886793258488_127080242685625155_n.jpg
62608645_2471937859694869_343720082558774_n.jpg      70578819_732965103812817_3195574386530988937_n.jpg
65872282_2323254394388439_4333124901222433899_n.jpg  71104794_531247060990298_1056908497231962 78_n.jpg
66664424_884283208622689_7424229825567567719_n.jpg   71229999_2322050251443436_216802017277560748_n.jpg
69182097_167524964375534_6966059562522366254_n.jpg   71518306_133107558048[illegible]463087690735919 66_n.jpg
69223976_465488367382702_4060744152596376400_n.jpg   72163217_953881031622[illegible]0856242263913005_n.jpg
69228450_196572004695126_1719869794764756563_n.jpg   coachcharlotte92.json
```


Download All Public Instagram Posts

In some cases, you might wish to download all the content from a public-facing Instagram user account. Richard Arcega's Instagram-Scraper Python script (https://sec487.info/bi) will be your tool of choice to do this. It will save the videos and pictures from the account you specify and can, if configured, save location and hashtags, metadata from the image or video, and user comments to a JSON file for post-processing. As shown in the image above, we ran the command, specified what content we want saved, how many posts to retrieve, and then the Instagram user account.

The script retrieved all the relevant data and saved it locally on the system for analysis. We retrieved the images and videos (1) if there were any and a JSON file (2) with the metadata about each image and video.

Instaloader Command-line Tool

Similarly to Instagram-scraper, this tool retrieves files and metadata (comments, geotags, etc.) from Instagram posts

```
student@sec487 (19:39:35) :~$ instaloader --comments --stories --tagged -c 10 coachcharlotte92
--login=USERNAME required to download stories.
Stored ID 256031966 for profile coachcharlotte92.
Warning: Use --login to download HD version of profile pictures.
coachcharlotte92/2016-09-17_21-08-06_UTC_profile_pic.
Retrieving tagged posts for profile coachcharlotte92.
Retrieving posts from profile coachcharlotte92.
[  1/250] coachcharlotte92/2019-10-01_16-01-22_UTC_1.jpg coachcharlotte9          10-01_16-01-22_UTC_2.jpg
#duddellslondon  #foodporn #f…] json
[  2/250] coachcharlotte92/2019-10-01_10-08-12_UTC.jpg [#lunch  in the #shard  #dudel…] json
[  3/250] coachcharlotte92/2019-09-29_08-39-04_UTC.jpg [#datenight  lovely meal with …] json
[  4/250] coachcharlotte92/2019-09-24_15-14-10_UTC.jpg [@anthonyjoshua  when your #pr…] json
```


Instaloader Command-line Tool

Another tool that works on the command line and is written in Python is instaloader (https://sec487.info/xi). Its output is a little different from Instagram-scraper, as it stores the text of the posts and the comments separately in files. There are a huge number of options you can leverage to retrieve and monitor an account.

This tool only pulls what you have access to. If the profile is public, you do not need to authenticate the tool to Instagram. If the profile is public or you wish to pull data from profiles that your research account may be a follower of, then you will need to provide the app your Instagram credentials.

Course Roadmap

- Day 1: Foundations of OSINT
- Day 2: Gathering, Searching and Analyzing OSINT
- **Day 3: Social Media, Geolocation, and Imagery**
- Day 4: Networks, Government, and Business
- Day 5: The Dark Web, Breach Data, and International Issues
- Day 6: Capstone: Capture (and Present) the Flags

SOCIAL MEDIA, GEOLOCATION, AND IMAGERY

1. People Search Engines
2. Facebook Analysis
3. LinkedIn Data
4. Instagram
5. **Twitter Data**
6. Geolocation
7. Imagery and Maps

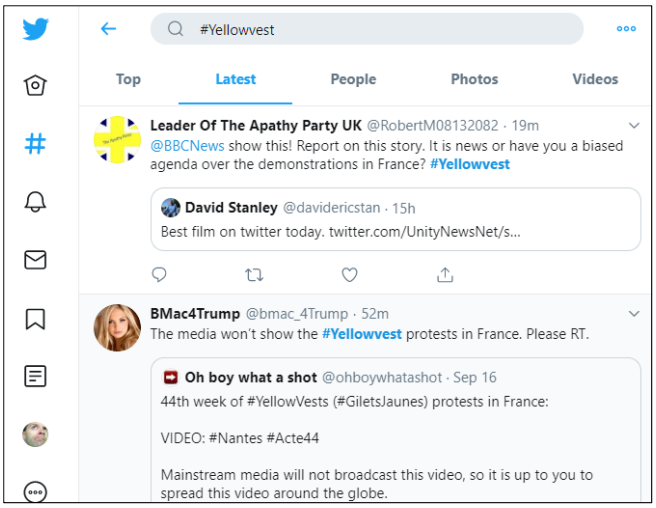
This page intentionally left blank.

Twitter Overview

Microblogging social network

Key Concepts:

- Content <= 280 characters
- Following other accounts
- Followers of target account
- Direct Messaging
- Geolocation
- "#" or Hashtags



Twitter Overview

The social network Twitter (twitter.com) is an international micro-blogging system. Using a web browser, third-party application, mobile device, or script, users can post or "tweet" text, pictures, or videos. It is known as a "micro" blogging site since text-based content is mostly limited to 280 characters or less, making users choose their words and content carefully before posting. While most of the information posted to Twitter is public, there are some accounts that require the Twitter user to approve followers before they can view tweets. Additionally, Twitter can be used in a Direct Message (DM) capacity, where users send private messages to each other.

Twitter users connect to other users by becoming "followers" of the account they are interested in. Each profile on the site will show the number of accounts it is following (i.e., getting data from) and also the number of followers of the account (i.e., others that are following the target account). The more Twitter followers a person has, the bigger the audience they can reach with their content. Entertainment stars, politicians,[1] and other high-profile people may have millions of followers, but it is more common for people to have between 100 and 1,000 followers.

There are two other concepts that people new to Twitter need to understand. The first is the "@" symbol, which is used to note another Twitter account. Tweeting content with "@username" in it will send a notification to the "user name" account mentioned in a tweet. It is a method to bring others into the conversation. The hashtag symbol ("#") is used to note keywords or indexes. People use specific hashtags to tag similar tweets. Examples include #osint for people interested in Open Source Intelligence and #TheWalkingDead for those people interested in that television series. On Twitter, people can follow and search on hashtags they are interested in (such as the ones just noted).

Image from https://sec487.info/sl, September 17, 2019.

Reference: [1] https://sec487.info/1r, November 11, 2016.

Twitter for OSINT

OSINT content from Twitter:

- Account bio/URL/location
- Connections between targets
- Patterns of behavior
- Pictures/videos
- Geotagging
- Sentiment about a topic

Twitter for OSINT

As OSINT analysts, Twitter provides a rich platform to view and analyze our target's information. Whether we are trying to understand public sentiment about a specific topic or tracking a certain person through their tweets, Twitter will most likely have data for us to retrieve. The slide above shows a portion of the Twitter profile page from the @drdpiratroberts account (https://sec487.info/1t).

From an OSINT point of view, here are some of the data that we can harvest from Twitter:

- If you are researching a person, you can visit their account profile page at https://twitter.com/USER (replace the "USER" with the target's name like https://twitter.com/drdpiratroberts). As shown above, the profile of drdpiratroberts shows that the person behind the profile has made the account common name "Dread Pirate Roberts" (it is common for people to change this name frequently as it shows up in their tweets but is nominal data for their account (i.e., their Twitter account is still drdpiratroberts). We also see a bio that the user has entered, where they self-report that they are from and the date they created this account.
- As Twitter is a social network, OSINT analysts can examine relationships between accounts, followers, and following to gain insight into networks of relationships.
- We can learn about topics being discussed, tone/emotion in the content, and when the target is awake or asleep based upon their tweeting habits and content. If the target uses apps that tweet for them, we may also gain insights into exercise and drinking alcohol habits. We will examine all of these in detail, shortly.
- Since users can post pictures and videos, Twitter is often turned to for breaking news and content during times of conflict, high emotion and popular events. This rich media can be examined for data above and beyond the 280-character limit of the tweet.
- Twitter allows users to geotag or post the physical, geographical location of their tweets and pictures. Retrieving the latitude and longitude can help place a person at a certain location.
- Following hashtags can be used to harvest information about certain topics of interest. For instance, after the police shot Freddie Carlos Gray, Jr. in Baltimore, Maryland in April 2015, the Twitter hashtags #FreddieGray and #baltimoreuprising were used during protests, riots, and the trials of those responsible for his death.

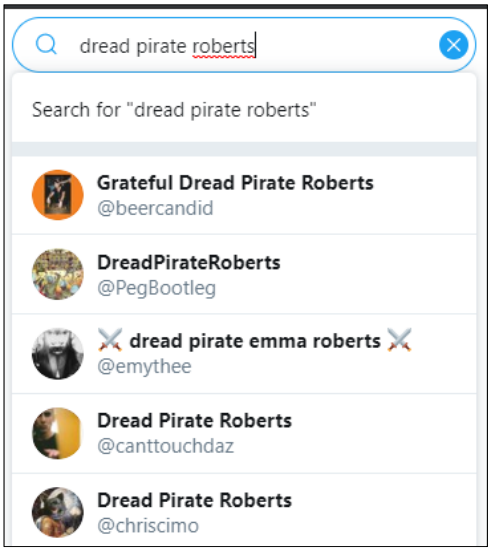
Image from https://sec487.info/1t, September 17, 2019.

Twitter's Simple Search

On the main https://twitter.com site is a search field

You can search for accounts, names of people, keywords, and hashtags in it

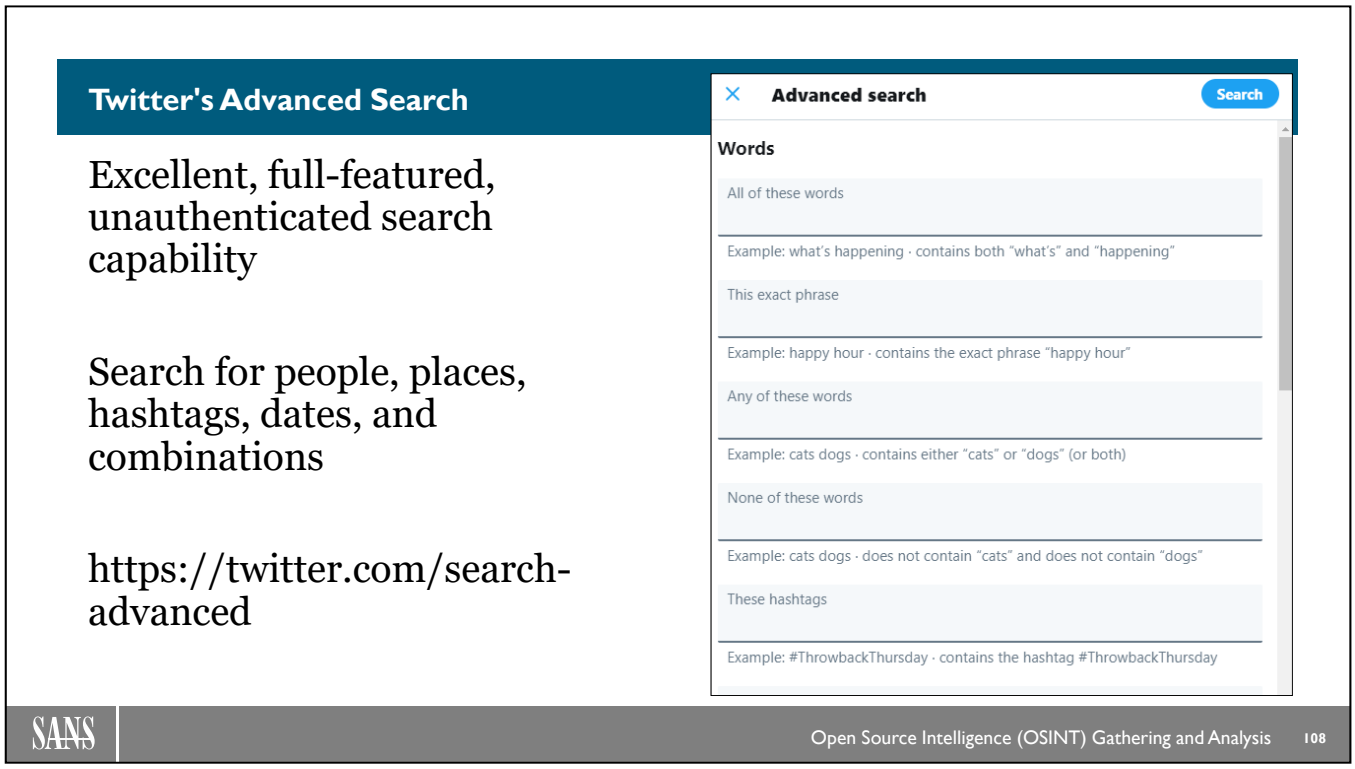
It is a simple search and can yield helpful results



Twitter's Simple Search

On many of Twitter's pages is a magnifying glass that brings up a search field (https://sec487.info/lz). Entering keywords into the field and submitting the data will search Twitter for your content. You do not need to be logged in to the site as a valid Twitter user in order to perform these searches. Unfortunately, due to the enormous amount of information that Twitter holds, many times these general searches are too broad to yield relevant results. A good example of this is shown in the slide above. We searched for the Dread Pirate Roberts account that we saw previously, and the simple search did not show that account in the results.

Image from https://twitter.com, September 17, 2019.



Twitter's Advanced Search

The Advanced Search page (https://sec487.info/1u) is a great place to begin searches of Twitter users and data. It has easy-to-use form fields that allow analysts to quickly target the keywords, dates, users, and regions that they wish to search.

Entering keywords, dates, and accounts you wish to search and pressing Enter will change the URL to incorporate those parameters you entered. An example of this would be to enter "rodents unusual size" (without quotes) into the "All of these words" field along with "new york" into the "Near this place" field. This generates a URL of https://twitter.com/search?q=rodents%20unusual%20size%20near%3A%22new%20york%22%20within%3A15mi&src=typd (https://sec487.info/1v). This URL can easily be copied and modified to perform additional searches. The results of such a query, performed in September 2019, are shown below:

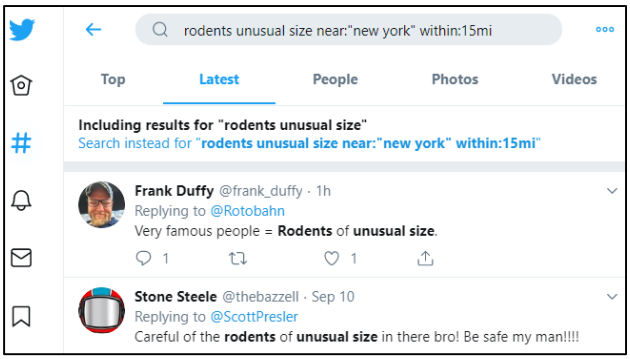


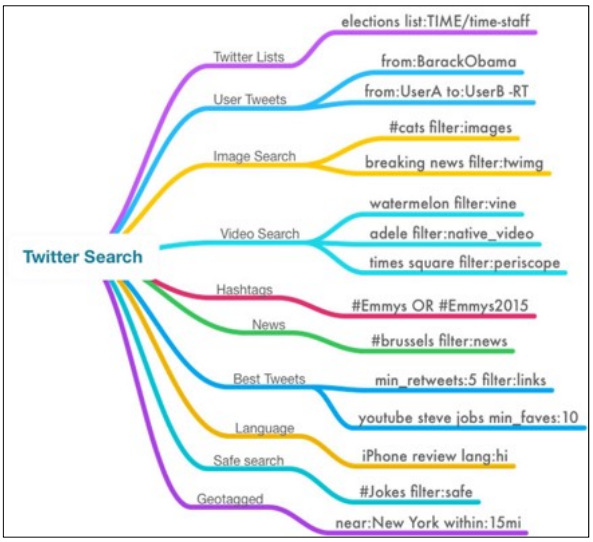
Image from https://sec487.info/1u, September 17, 2019.

Twitter Search Tricks

Amit Agarwal's Twitter search blog post

Uses similar techniques to what you find on Google "Dork" sites

Well-written and useful reference



Twitter Search Tricks

Amit Agarwal created a terrific blog post at https://sec487.info/i4 on advanced Twitter searches using directives like those we use on general search engines. He explains how to use these to extract just the tweets or user data that interest you from the Twitter search pages. The blog is an easy read and holds excellent content.

Another resource to discover Twitter search terms is Dutch OSINT Guy's OSINT Curious blog post at https://sec487.info/s9.

Image from https://sec487.info/i4, June 28, 2018.

Twitter Cheat Sheet

Conspirador Norteño (`@conspirator0`) posted an image to a valuable Twitter search reference

Use it similarly to Amit Agarwal's; for reference and learning

Twitter search cheat sheet	
find tweets from a specific account	from:BakedAlpacas
find direct replies to an account	to:DrunkAlexJones
find all tweets mentioning an account	@SenDuckworth
find tweets before a specific date	until:2018-11-06
find tweets after a specific date	since:2018-01-01
find tweets containing an exact phrase	"I was born"
find tweets containing all of a set of terms	Sessions Russia recuse
find tweets containing any of a set of terms	#FalseFlag OR "false flag"
find tweets linking to a specific website	url:sputniknews.com
find tweets excluding a specific term	from:realDonaldTrump -fake
find tweets containing images or video	cats filter:media
find tweets containing images	tacos filter:images
find tweets in a specific language	indictments lang:en
Options can be combined as needed	
find tweets from a specific account mentioning any of a set of terms	from:Ian56789 Novichok OR Skripal OR Salisbury
find tweets from a specific account containing an exact phrase	from:ZellaQuixote "shitty bass player"
find tweets that are part of a thread (self-replies)	from:conspirator0 to:conspirator0
find tweets from a specific account within a date range	from:JackPosobiec since:2015-10-01 until:2015-11-01
find tweets from a specific account tagging another account	from:LouiseMensch @voxday
find tweets linking to a specific website containing a given search term	url:rt.com midterms

Twitter Cheat Sheet

Similar to Amit Agarwal's reference blog post, Conspirador Norteño posted an image (https://sec487.info/me) showing a variety of helpful Twitter search queries using the advanced directives and in what use cases you might wish to use them.

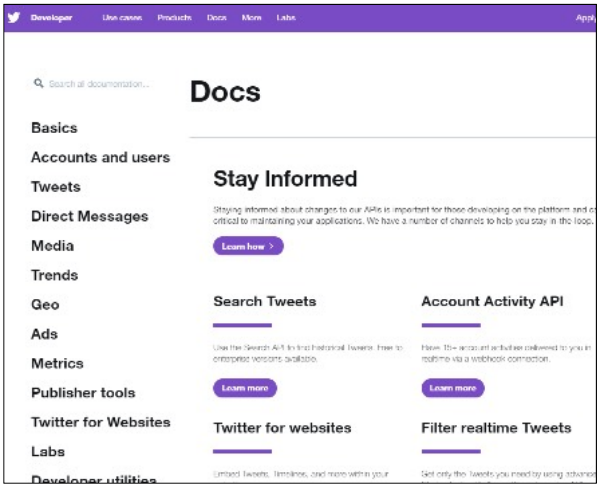
Image from https://sec487.info/me, January 2, 2019.

Twitter APIs

Multiple APIs depending upon your needs: search, tweet, direct message

Or receive **sampling stream** of what is happening in an area or with a hashtag (not all the tweets)

"Firehose" streams **all** tweets meeting your criteria (Expensive!)



Twitter APIs

Twitter has several free APIs that can be used to interact with its data. These APIs allow users to do most anything that a regular user accomplishes through the web interface, but here uses authenticated web calls. Using twurl (like curl) or a programming language such as Python or Ruby, a person can register for an API key and begin grabbing or sending data to Twitter.

Using these APIs, a developer can search for content in a request-response API call to the Twitter servers. They can also submit terms and tags to Twitter and have Twitter stream to the user a sampling of new, future tweets matching the user's criteria.

Finally, Twitter has a paid API that guarantees to send all tweets matching your query terms to you. This is called the "firehose" since it can, depending upon the terms used, send hundreds of millions of tweets per day to the user. Details on Twitter's APIs can be found at https://sec487.info/gv.

Image from https://sec487.info/gv, September 17, 2019.

Twitter User Analysis

With most of Twitter user content being public, we can analyze that data to discover:

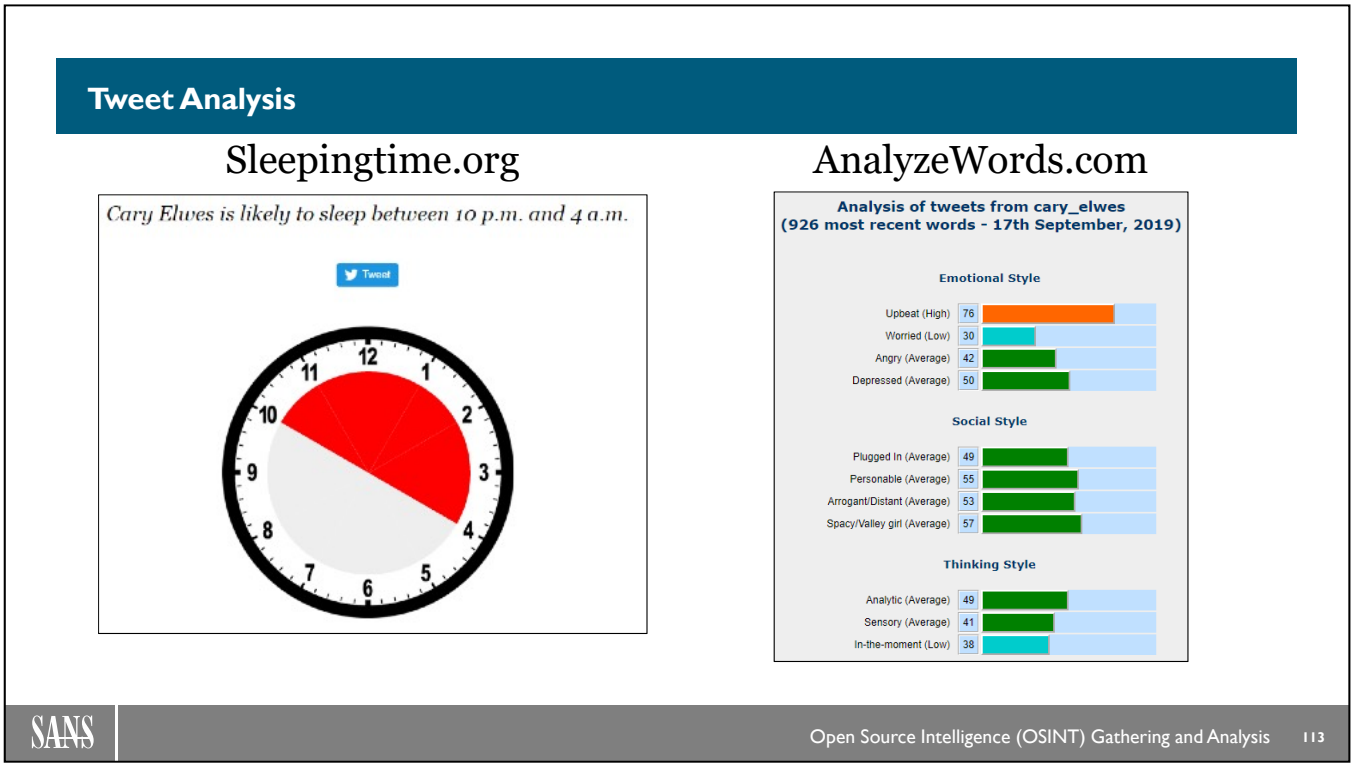
- Patterns of behavior
  - Sleeping
  - Drinking alcohol
- Hobbies/Interests/Work/Leverage Points
- Friendships/Relationships
- Emotional states

We can leverage third-party sites to do this work.

Twitter User Analysis

The majority of user content that is posted to Twitter is public data. This provides OSINT analysts and many web sites information to analyze, categorize, and rate. We have already seen that the user profile page can yield some information that a Twitter user wants us to have, but in analyzing the content of their tweets, we can learn hidden things that they may not knowingly wish to have disclosed. By aggregating tweets, when they are posted, where they are geotagged, and the sentiments expressed in that content, we can look across hundreds or thousands of posts to discover interesting trends.

We could write a script in Ruby or Python to do this work for us, but there are many Twitter User Analysis web sites on the internet that allow us to examine tweets for free. Let's leverage these sites to see what kind of data we can gather about a target.



Tweet Analysis

You may find it helpful to understand when your target Twitter user is awake or asleep. Sleepingtime.org can help with that by analyzing the times of the day when tweets are, well, tweeted. Just enter a URL of http://sleepingtime.org/TWITTERACCOUNT, such as http://sleepingtime.org/cary_elwes (https://sec487.info/28), and the web site will look up the Twitter account and pull the times they tweet. By extension, when they are not tweeting, they might be asleep. Keep in mind that tweets can be queued up and sent at any time of the day or night by several services and, depending on if your target is an international traveler, this data may or may not be useful.

The emotional state of a Twitter user can sometimes be glimpsed by the analysis of the words they use in their tweets. The http://www.analyzewords.com/ (https://sec487.info/29) web site performs just such an analysis on a Twitter user's tweets. Each of the row headings, such as "Upbeat (Average)," contains help popups when you move your mouse over them. These popups explain the category. Interested in how they calculate these numbers? Find that data https://sec487.info/2a.

Social Bearing

https://socialbearing.com

Provides authenticated and unauthenticated searches and analysis.

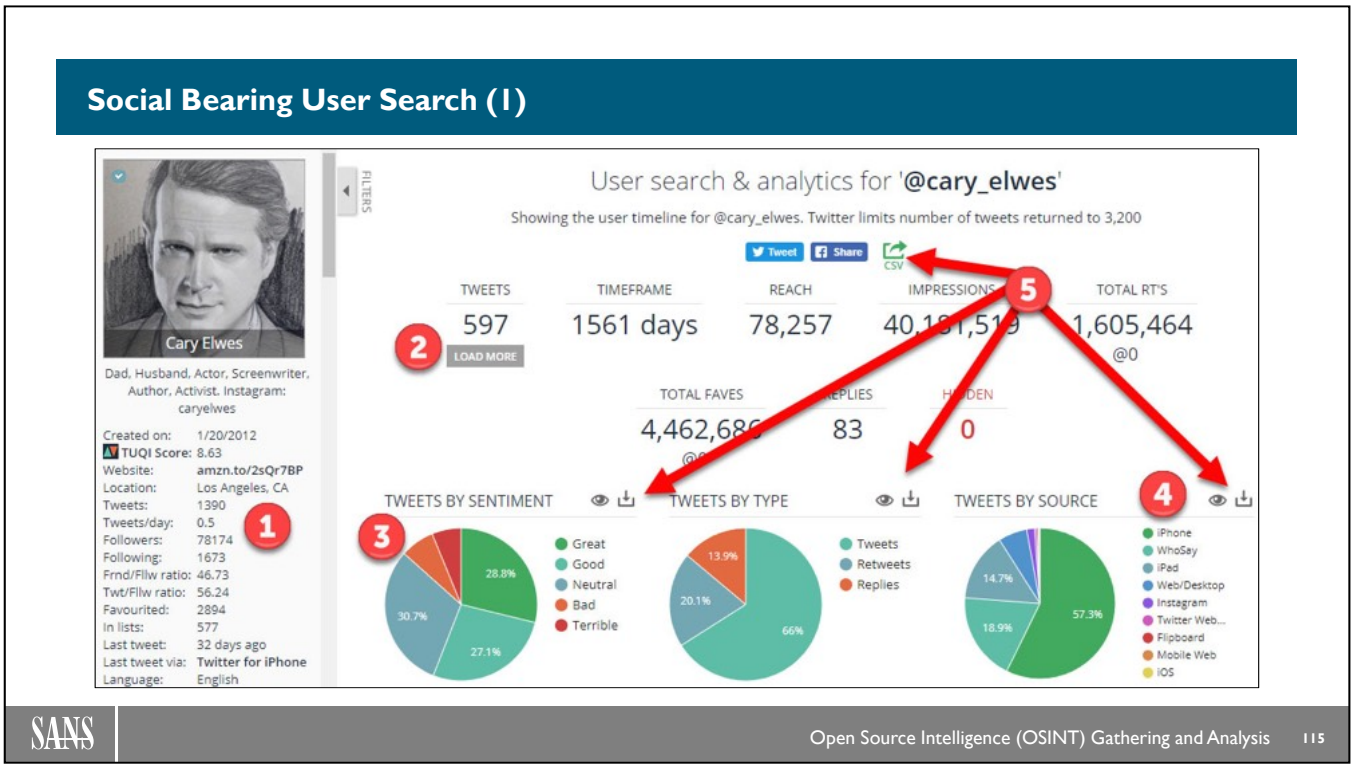
Free!

Valuable filters for selecting just what you want to analyze

Social Bearing

The free web site https://socialbearing.com allows users who have Twitter accounts and those without to perform advanced searches and analysis of Twitter content. Some of the features of the site require that the user have a Twitter account so that Social Bearing can leverage the Twitter API (Application Program Interface). The results page for user searching contains excellent filters for removing or adding specific content that an OSINT analyst may wish to search.

Image from https://socialbearing.com/, September 17, 2019.

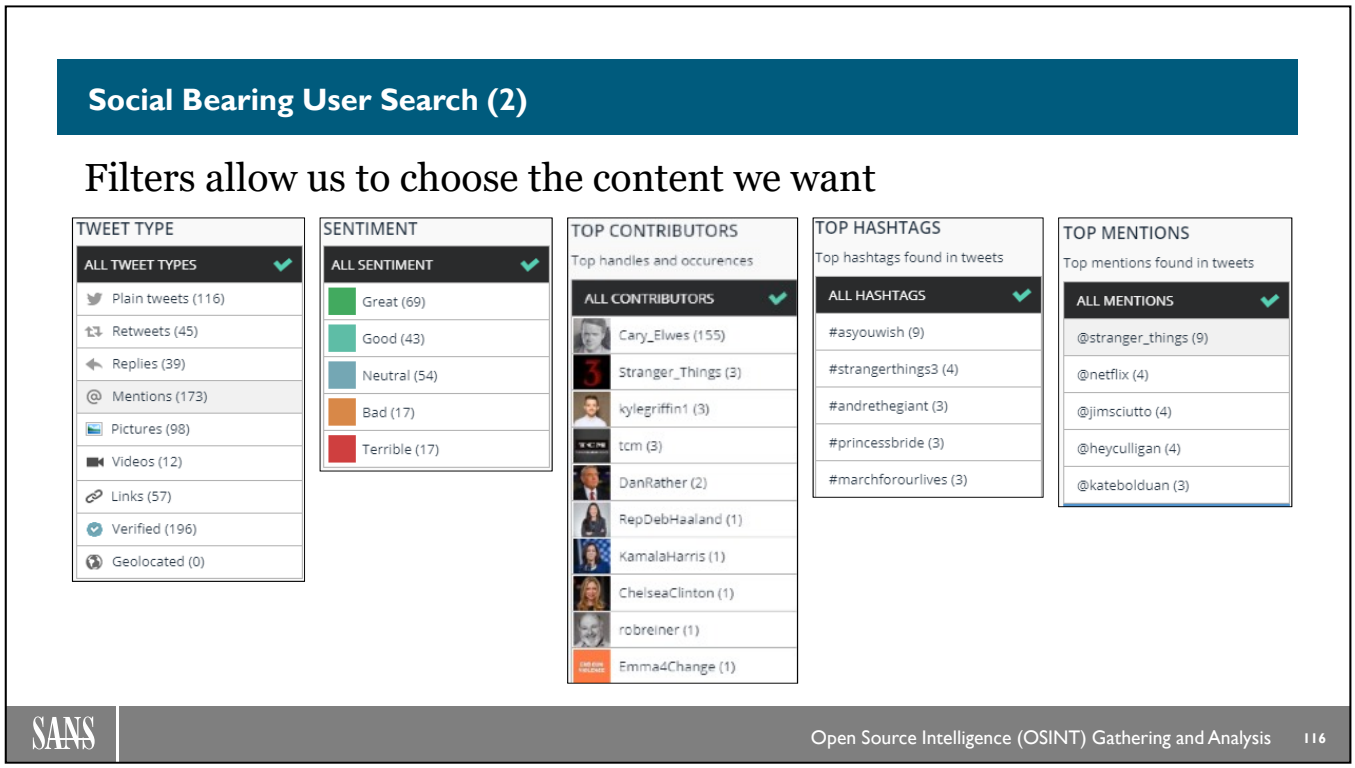


Social Bearing User Search (1)
This slide shows Social Bearing's Twitter profile analysis Cary Elwes' account, @Cary_Elwes (https://sec487.info/21). Elwes played the character Westley in *The Princess Bride* movie. The analysis has several sections that are important to OSINT analysts. There are several areas of this picture we need to understand better. Each of the numbered topics below has a corresponding number in the above slide that it refers to.

1. Social Bearing shows the user's profile picture, self-reported biography, date of creation for the account, and statistics about the account.
2. Social Bearing only collects 200 of the user account's most recent tweets. While this is sufficient for some purposes, clicking the LOAD MORE button retrieves 200 more tweets each time it is clicked (up to 3200 tweets). When possible, try to load up over 600 tweets to get a broad view of the user's activity, especially if your target is very active on Twitter.
3. Social Bearing uses emotionally-charged words in the target's tweets to determine their "sentiment". This can be helpful if we are trying to assess the emotional state of the target. One thing to note is that Social Bearing uses keywords lists to determine what kind of words were used and those can be false positives. For instance, the word "die" in English may have a negative connotation but in German, this word does not.
4. Finally, the "TWEETS BY SOURCE" graph shows what Twitter clients the target (or their delegates) used to tweet. In this case, we can see that Cary Elwes most likely uses Apple products and has an iPhone and possibly an iPad. This also shows that the "WhoSay" application has tweeted a significant number of times as this account. WhoSay (https://sec487.info/sm) is a method for celebrities to "monetize their digital footprint with premium-branded social campaigns." This could be another helpful piece of information for your search.

A good example of why this matters comes from the United States Presidential election of 2016. Donald Trump's tweets, when analyzed (https://sec487.info/1z) revealed that tweets made from an Android device were "angrier and more negative" than those tweeted from an iPhone. A *Washington Post* article (https://sec487.info/20) highlights the differences quite well in several graphs and infographics.

Image from https://sec487.info/21, September 17, 2019.



Social Bearing User Search (2)

Social Bearing allows users to filter the tweets that they see on the data analysis results page by multiple methods. Pictured above are several of the more-important filtering options available to the OSINT analyst. There are many more available on the site.

- **Tweet Type** - Here you can filter by the type of tweet that was posted and the content it contained.
- **Sentiment** - This section allows you to filter tweets that contain positive or negative terms.
- **Top Contributors** - These are Twitter accounts that were retweeted or mentioned the target Twitter account in their tweet.
- **Top Hashtags** - Social Bearing analyzes the hashtags the target used in their tweets and notes the most frequently used here.
- **Top Mentions** - The items here are other Twitter accounts that the target mentioned in their tweets.

There are other categories such as Top URLs, Top Twitter Sources, and Top Domains that can also provide valuable OSINT on your target.

Image from https://sec487.info/21, September 17, 2019.

Twopcharts Twitter User Analysis

Twopcharts is a free, public Twitter user analyzer web site

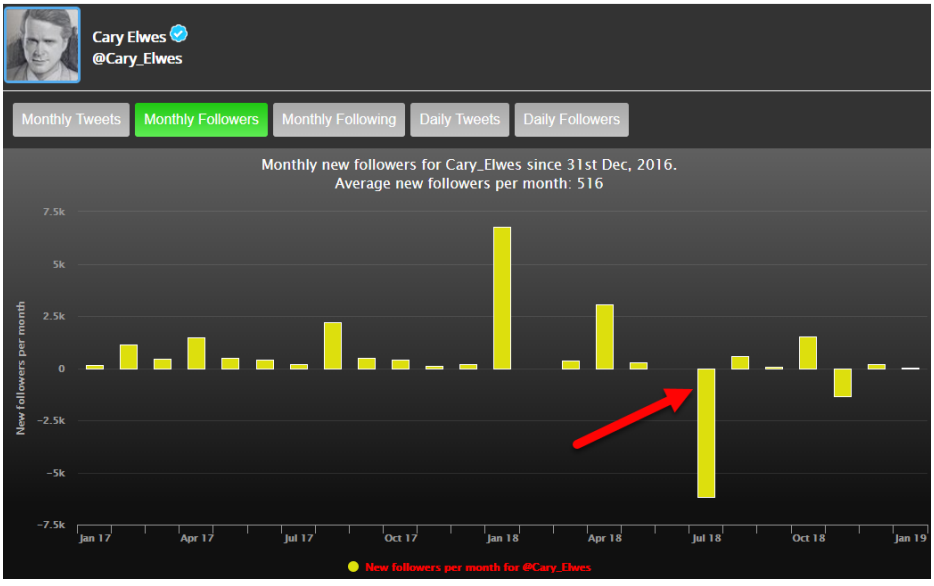
Does not require an API or authentication

Analyze tweets, times of tweets, last 100 followers, and historical numbers of followers

Twopcharts Twitter User Analysis

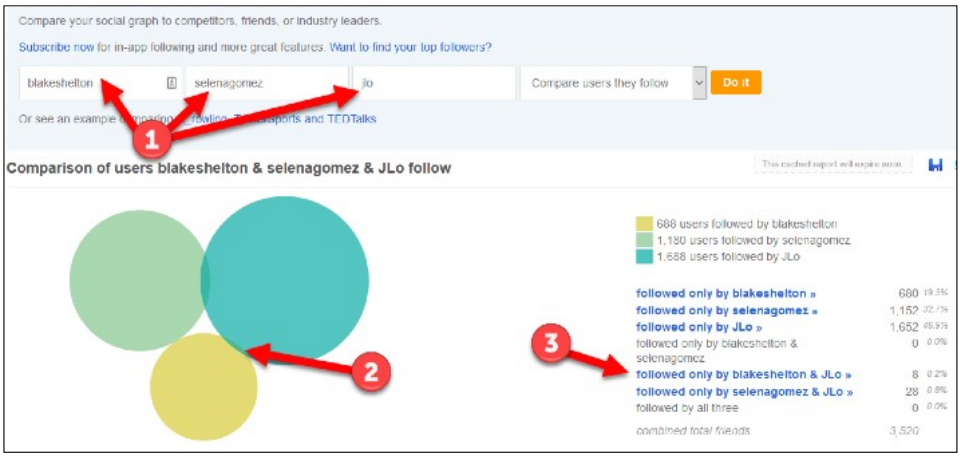
The Twopcharts web site (http://twopcharts.com) allows users to retrieve and analyze Twitter user accounts or search for tweets with certain content. This site requires no authentication or Twitter API keys to use. It pulls, aggregates, and displays results in attractive web pages for your investigations. An example is the graph below of the monthly addition or loss of Twitter followers for the @Cary_Elwes Twitter account. Notice in July 2018, there was a large drop in the number of followers for this account (this coincides with the Twitter removal of "bot" accounts). Since this is data, and graph content is meant for web browser screens, exporting the data to another medium, such as CSV, may be challenging.

Slide image from https://sec487.info/mj, January 2, 2019.



Followerwonk.com

Find intersections between followers or people accounts are following or just examine followers of a single Twitter account



Followerwonk.com - Follower Analysis

The followerwonk.com website helps analysts understand what accounts are either following certain Twitter accounts or are being followed by those accounts. As an anonymous user or by using a free account, you can request this site to analyze a specific Twitter account to understand their followers or who they are following.

The real OSINT power of the site comes from its ability to show intersections between the followers of multiple accounts. As shown above, requesting the analysis of two or three accounts yields a Venn diagram that represents uniqueness or overlap in follower activity (arrow 2). The user can then click the hyperlinks (arrow 3) to view the specific accounts that are common to the analyzed accounts.

Another feature of this site allows for a user to search the bios or profiles of Twitter users for some string. For instance, if we wanted to see all the Twitter profiles that had the term "osint enthusiast" in them, we could visit the https://sec487.info/s7 page and see the results.

Image from https://sec487.info/s6, September 16, 2019.

Twitter Geolocation

Users can geolocate images

Helpful for finding target habits, pictures, or sentiments from a certain area.

There are geo-search options from advanced searches on Twitter to mapping web sites to dedicated clients with APIs.

Twitter Geolocation

Users can choose to enable the geolocation tagging of photos and some other content on Twitter. As you may imagine, this can be quite helpful to OSINT analysts. It can help tell us where a target may have been at a certain date and time. Additionally, if we can examine tweets from a certain geographic area—for instance, at the White House in Washington, DC or perhaps The Hague in Belgium—we can see what multiple people are tweeting about. This can be useful during large gatherings such as protests or riots. The pictures, videos, and sentiments from these tweets can be helpful in understanding the situation from the people who are involved in it.

There are free and paid services that will gather the location-based data from Twitter tweets. We will focus on those free applications that do not require you to link a valid Twitter account to them. These sites use their own Twitter API keys to perform the searches you request.

Twitter Search for a Location

With a latitude and longitude or city name and a certain distance, you can craft search parameters to examine a region

```
near:location within:#[km/mi]
```

For example:

- **`near:37.334,-122.010 within:2mi`**
- **`near:riyadh within:15km`**

Twitter Search for a Location

Once you have a latitude and longitude for your location (or a city name), you can visit the Twitter search page or any Twitter page with the Twitter search bar at the top. This search can be performed without authenticating to Twitter.

Inside the field, enter the search string formatted as shown in the above slide. An example, shown in the slide, is "near:Riyadh within:15km", which shows geolocated tweets from a 15-kilometer radius around the city of Riyadh, Saudi Arabia. Visit this query here https://sec487.info/s2.

Note that you can choose to use miles (mi) or kilometer (km) in this search query.

Twitter Search for a Location with Keyword

Location: London, UK

Date: **2019**

Recreational marijuana use **illegal**

```
marijuana OR weed
near:london
within:15km
filter:images
```

Twitter Search for a Location with Keyword

Since we can localize our results to a certain region using the "near" directive, let's further refine the search to look for a certain term that users may be tweeting from a specific location. In the example above, we inserted the words "marijuana OR weed" at the end of the near directive and searched geotagged tweets in the London, United Kingdom region. Recreational marijuana was not legalized in the UK when this tweet was posted (https://sec487.info/s1).

Keep in mind that this query only retrieves content where the Twitter user has the geotagging of images turned on AND is using the term you searched for. It may be that many more users are using the term you are interested in but not geotagging their tweets.

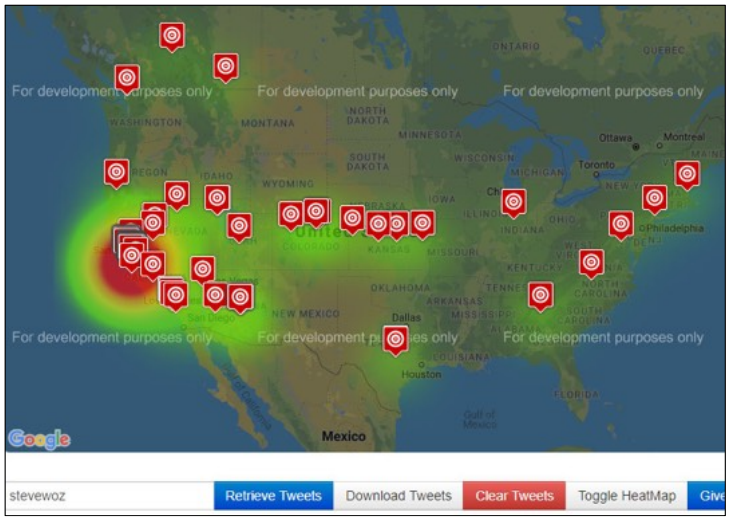
Image from https://sec487.info/s0, September 16, 2019.

Tracking a Twitter User

Apple co-founder Steve Wozniak (@stevewoz) tweets with geolocation enabled

This site plots those places he tweets from on a heatmap

http://geosocialfootprint.com/

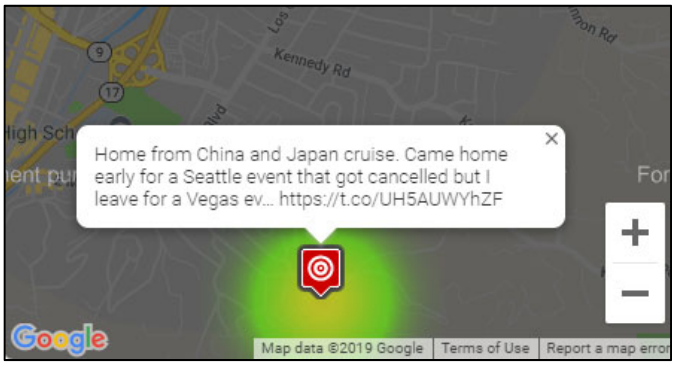


Tracking a Twitter User

Sometimes, instead of searching for a certain location and viewing the tagged tweets from the area, we want to find where a certain person has been tweeting. In this case, we can leverage a site such as http://geosocialfootprint.com/ to perform the retrieval and mapping of target tweets. Let's see where Steve Wozniak (@stevewoz on Twitter) co-founder of Apple, has been tweeting. Entering his "stevewoz" user name in the bottom portion of the page and pressing the "Retrieve Tweets" button allows the application to grab the tweets, examine them for geotagging and then plot them on the map (as shown above). The OSINT analyst can then zoom into each location and examine the site and tweets from it. This site uses a "heat map" feature to how many tweets were found at each location. Fewer tweets show a green color and more tweets move to yellow, orange and red. Here we see that Steve Wozniak has a large group of tweets from California and fewer numbers from other places around the world.

Zooming in to the biggest grouping of tweets near Cupertino, shows the picture to the right. Clicking on one of the tweets, we now have Steve Wozniak's home location.

Images from http://geosocialfootprint.com, September 6, 2019.

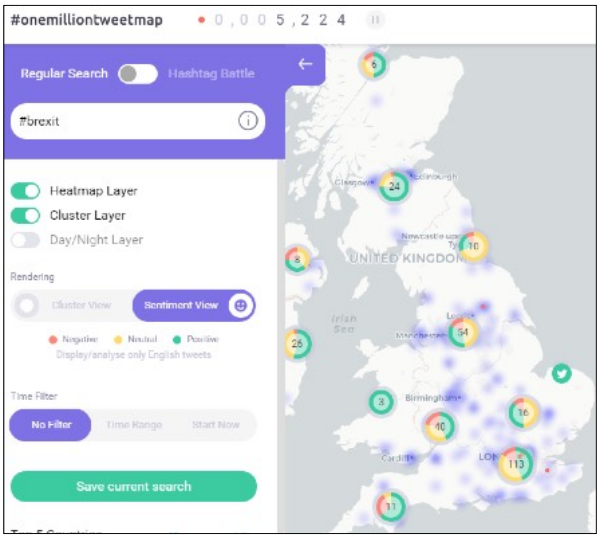


One Million Tweet Map

Another site to watch location sentiment is https://onemilliontweetmap.com

Enter keywords or hashtags and view tweets from a particular area.

Time-based settings (last 5 minutes through last 6 hours).



One Million Tweet Map

The one million tweet map web site downloads and plots on a map of the world the last 1,000,000 tweets posted to Twitter. Using time-based and geographic filters, you can see what Twitter users in a particular area are tweeting about. In the example in this slide, it shows Twitter accounts in the United Kingdom that tweeted with the word "brexit" in it on September 6, 2019.

During times of riots and protests, it is frequent for specific hashtags for those events to be used by the people participating. Entering that hashtag and centering this web page over the region of the event can yield good information about what is happening.

Once the tweets are plotted on the map, they can be shown in a clustered format (shown above) where multiple tweets in a certain region are aggregated together to make a cluster. When you zoom in on the map, the cluster will break apart into separate tweets. Clicking on any of the tweet cluster numbers will show the contents of those tweets.

Image from https://sec487.info/rx, September 6, 2019.

Recovering Deleted Tweets

Twitter is mostly a public social media site.

People sometimes tweet content that they may not want to remain public.

They may delete the tweet, but many times it is still recoverable.

Recovering Deleted Tweets

Twitter is primarily a public social media platform with most of the user-submitted content being available to the public. There are times when a Twitter user may tweet something and want to retract it. Once sent, a tweet cannot be edited, so the only course of action is to delete it and retweet or just delete the tweet. From an OSINT perspective, these deleted tweets may contain information that our clients wish to retrieve. Perhaps a criminal has just bragged about their activities or someone posted a photo of something they should not have on Twitter...in either case, we need to see those tweets.

The above picture from Google (https://sec487.info/sn) was retrieved on September 17, 2019 and shows that a Twitter user named "finnex" tweeted on September 2, 2019, "hello i deleted all my tweets i have limited myself to 10 tweets a day." Let us see if we can retrieve some of their tweets using and archive web site.

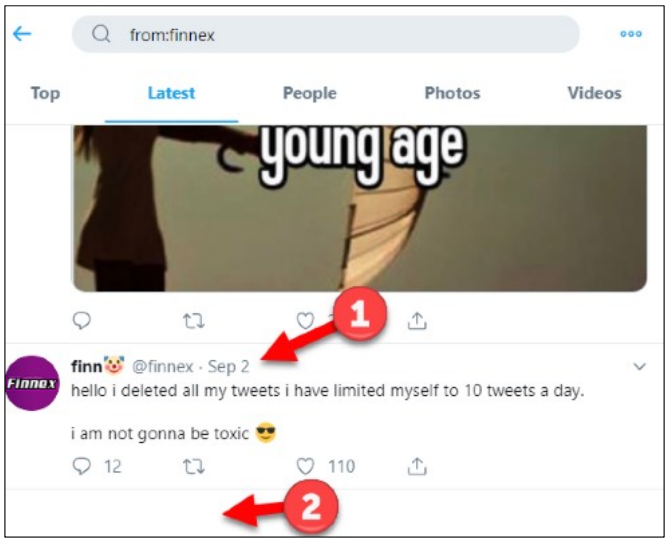
Image from https://sec487.info/sn, September 17, 2019.

Verification of Deleted Tweets

Before searching for finnex's deleted tweets, we examine their Twitter account.

https://twitter.com/finnex/

Sure enough, there are no tweets for this user before September 2, 2019 (arrows 1 and 2)



Verification of Deleted Tweets

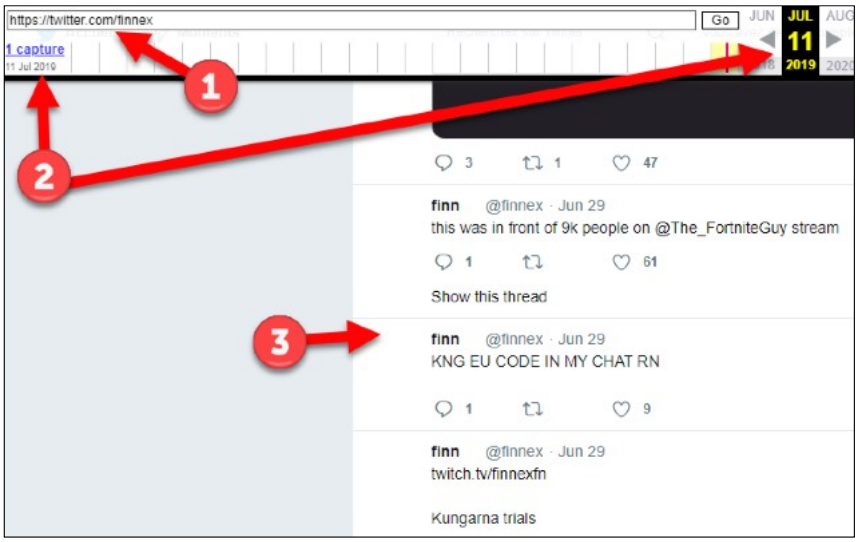
Twitter's profile page for the finnex user (https://sec487.info/so) confirms that there were no tweets for this user before September 2, 2019 (the date they said they were deleting all their tweets). If there were any on Twitter.com, they would appear in the space where the arrow 2 is pointing, above.

Image from https://sec487.info/sp, September 17, 2019.

Using Archive.org to Retrieve Tweets

Archive.org's spider regularly indexes Twitter's public content

When people delete their tweets on Twitter, the WayBackMachine's cache continues to preserve their data



Using Archive.org to Retrieve Tweets

Archive.org's web bot continually and regularly retrieves data from Twitter's public data. When users choose to delete tweets from the Twitter site, many times that cached content remains. We can access this cached data by using the Archive.org WayBackMachine. In our picture above (https://sec487.info/sq), we see that this user's Twitter account was indexed on 11 July 2019 (arrows from 2). This allows us to scroll down and load earlier tweets from the user.

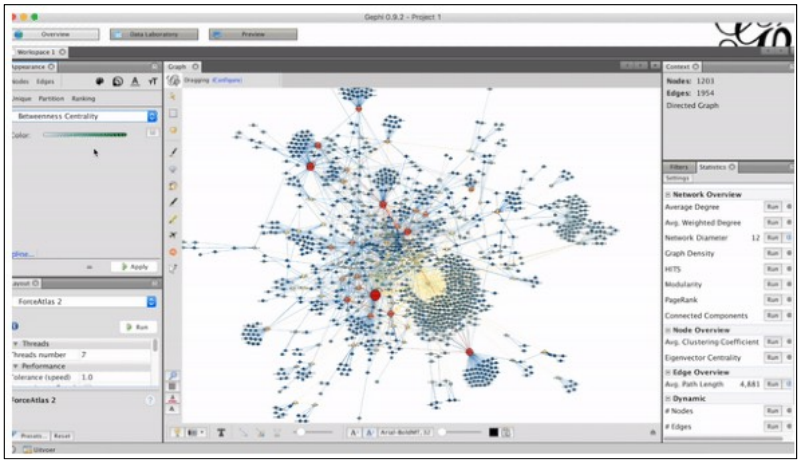
Depending upon the time between when the user tweeted the post and when Archive.org indexed their content, this technique may or may not work. This will also not work for direct messages or accounts that are private (i.e., not publishing data to the public).

Long-Term Twitter Analysis

Nico (@Dutch_OsintGuy) wrote about using DMI-TCAT (Digital Methods Initiative Twitter Capture and Analysis Toolset)

Collect and analyze tweets over time

Blog shows visualizing using Gephi tool



Long-Term Twitter Analysis

Nico (https://sec487.info/m2) wrote a post (https://sec487.info/i6) on scraping and visualizing Twitter content. Using the DMI-TCAT (Digital Methods Initiative Twitter Capture and Analysis Toolset)[1] system for collecting and storing the tweets and Gephi for visualizing the data, he demonstrates some excellent techniques for longer-term Twitter content collection and analysis.

Reference:

[1] https://sec487.info/i5.

Image from https://sec487.info/i6, June 28, 2018.

Bot and Propaganda Analysis

There are a variety of tools available to determine if a Twitter account may be a bot

Many of the techniques we have already seen can be used:

- Times of tweet (24x7?)
- Sources of tweet (apps)
- Number of account followers
- Profile clues (no profile pic)

We have two general categories of tools:

- Web applications
- Scripts you need to download and run locally

Some tools are anonymous, and some require a valid Twitter account to retrieve data

Bot and Propaganda Analysis

There are many Twitter bot analysis tools hosted on web sites and others that are scripts you can run on your analysis platform to determine if a certain Twitter account is automated. Many of these require authentication to pull data from the Twitter API. In these cases, either you will need to provide the tool a valid set of API keys that you retrieved from your Twitter account or you will need to authorize the analysis application to have certain access to your Twitter account.

How do these tools work? Most use methods that we have already discussed. From examining the times that an account sends tweets to what applications are used to send those tweets, these applications can rapidly analyze huge amounts of data to help you determine who or what is sending tweets from an account.

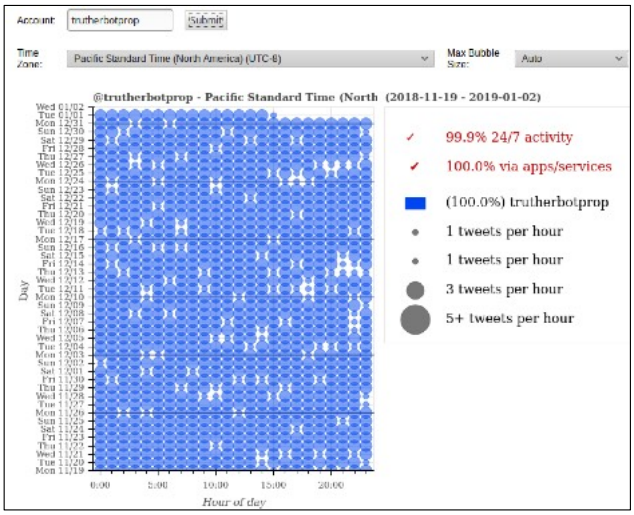
Depending upon how these tools and web sites are configured, they may scrape Twitter web data, use their own API key, require the user to provide an API key to Twitter, or require the user to grant the application access to a valid Twitter account.

Make Adverbs Great Again

Some Twitter researchers, like Conspirador Norteño (@conspiratoro) and Benjamin Strick (@bendobrown), tweet their bot analyses

They made a web application where you can run similar time-based analyses of tweets

https://makeadverbsgreatagain.org/allegedly/



Make Adverbs Great Again

Conspirador Norteño (@conspirator0) and Dr ZQ (@ZellaQuixote) have been tweeting their Twitter bot and propaganda analyses for a while. In 2018, they released a web site (https://makeadverbsgreatagain.org/allegedly/, https://sec487.info/ln) that allows the public to perform some of the same types of Twitter data analysis that they do. The web site is simple to use and shows the times when an account tweets, numbers of tweets, and the applications used to send those tweets in a graph.

To use their site, visit the web page, enter a Twitter user account in the field, adjust the other parameters, and click the "Submit" button.

But Conspirador and Dr. ZQ are not the only bot-hunters that show you how they do their work on Twitter. Benjamin Strick (@bendobrown) tweeted out an in-depth Twitter thread showing his analysis techniques (https://sec487.info/x0).

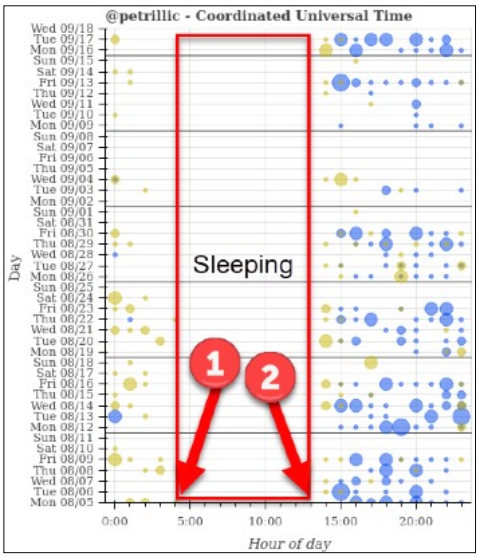
Image from https://sec487.info/lo, January 1, 2019.

Make Adverbs Great Again - Time Zone Estimation

We can use the tweet time plotting to observe when people travel out of their home time zones and where they live

Assume most people sleep from around 10pm to 5am

Plot using UTC and count the hours shifted, and you have the approximate time zone



Make Adverbs Great Again - Time Zone Estimation

Let's make some estimated guesses about most people: they sleep at night and probably stop tweeting from about 10pm (2200hrs) to 5am (0500). If we use the MakeAdverbsGreatAgain web site to plot their tweets, we should see times when they are not tweeting and, by extension, might be sleeping. If we set the web site to UTC time zone (+0 hours) and then plot their tweets, we can look at when they stop tweeting and note that time.

In the example above, that is arrow 1, at 0400hrs. If we guess that the average person goes to sleep around 2200hrs, we can count backward or forward in time zones to find the difference. In this case, from 0400 to 2200 (moving backward) is 6 hours. Since we set the time zone to be +0 hours (UTC), we count backward 6 time zones and get -6 UTC, or the Mountain Daylight time zone of the United States. This turns out to be 1 hour off from the reported place the Twitter user says they live: Seattle, Washington.

Using this method, we can also examine when people might travel as their time zones will be shifted from their normal baselines. Count the number of shifted time zones, and you may have a good idea of what area of the world they traveled to.

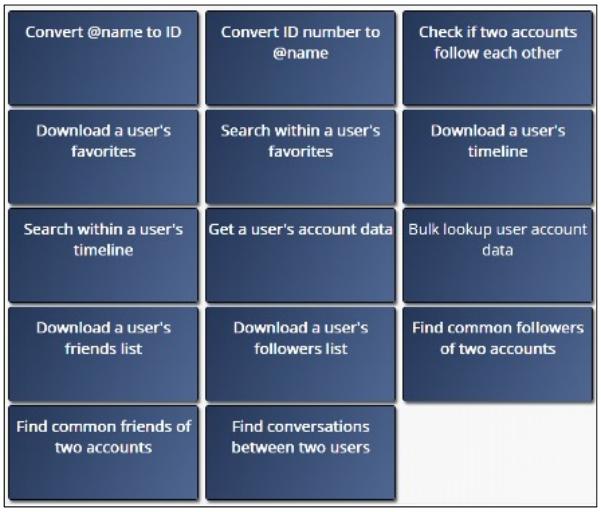
Image from https://sec487.info/lo, September 17, 2019.

TweetBeaver Tools

The tweetbeaver.com site has a variety of free tools to help investigate a Twitter account

It requires an authenticated Twitter account and uses Twitter's API

Can rapidly retrieve useful Twitter content



TweetBeaver Tools

If you have a valid Twitter account, consider connecting it to the free TweetBeaver application (https://tweetbeaver.com/) and allowing that app to use the Twitter API through your account. It has a variety of excellent options for researching Twitter data, accounts, and intersections. Whether you are trying to find out what followers 2 accounts have in common or want to look up a large number of Twitter accounts to retrieve profile data, TweetBeaver has simple buttons that help.

One of the best features of TweetBeaver is that you can either view the results of its query in your browser window or download a CSV file with the data. The CSV can then be used in further analysis and archiving.

TweetBeaver Archiving a Timeline

Link to a valid Twitter account

Downloads latest 3,200 tweets

Displays on screen or exports to CSV

Tweet author	Date posted	Text text	URL	Retweets	Favorited	Source
@WebBreacher	Tue Jan 01 22:21:23 +0000 2019	RT @jms_dot_py: Whoah just got an update email from @binarypool with a whole bunch of awesome new stuff added to Spiderfoot HX. Go check it...	www.twitter.com/WebBreacher/statuses/1080227515300487174	30	0	Twitter Web Client
@WebBreacher	Tue Jan 01 19:17:01 +0000 2019	RT @kwilli1046: You'll never want to smoke cigarettes again. https://t.co/xmlFtGCJ3K	www.twitter.com/WebBreacher/statuses/1080181117825765376	28499	0	TweetDeck
@WebBreacher	Tue Jan 01 19:05:38 +0000 2019	#OSINT in February in Virginia? Sounds like a great time to me! https://t.co/Y2nMIFv2QK	www.twitter.com/WebBreacher/statuses/1080178250083643394	2	12	TweetDeck

TweetBeaver Archiving a Timeline

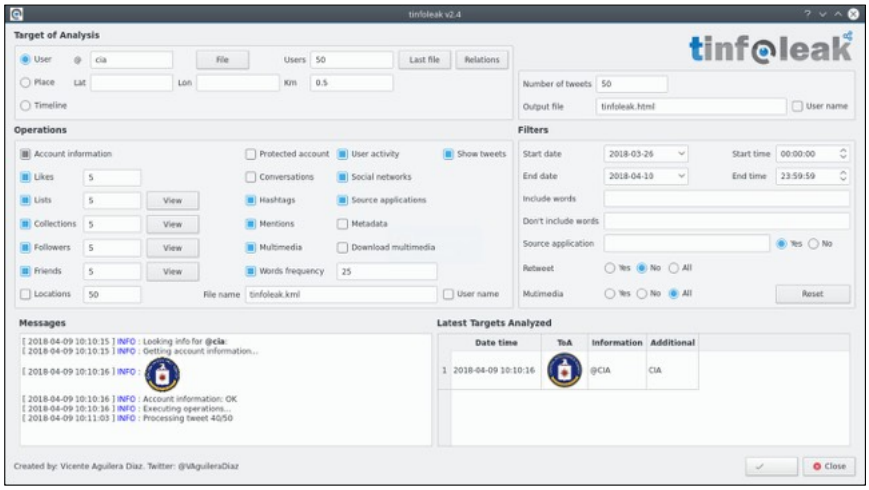
Once a Twitter user connects the TweetBeaver application to a valid Twitter account, they can choose to "Download a user's timeline" (https://sec487.info/mc), which retrieves that most-recent 3,200 tweets from that account. It will display the tweets on screen in the browser or save them to a CSV file for further analysis and processing.

tinfoleak Script

Python script with GUI!

Requires Twitter API keys (you provide)

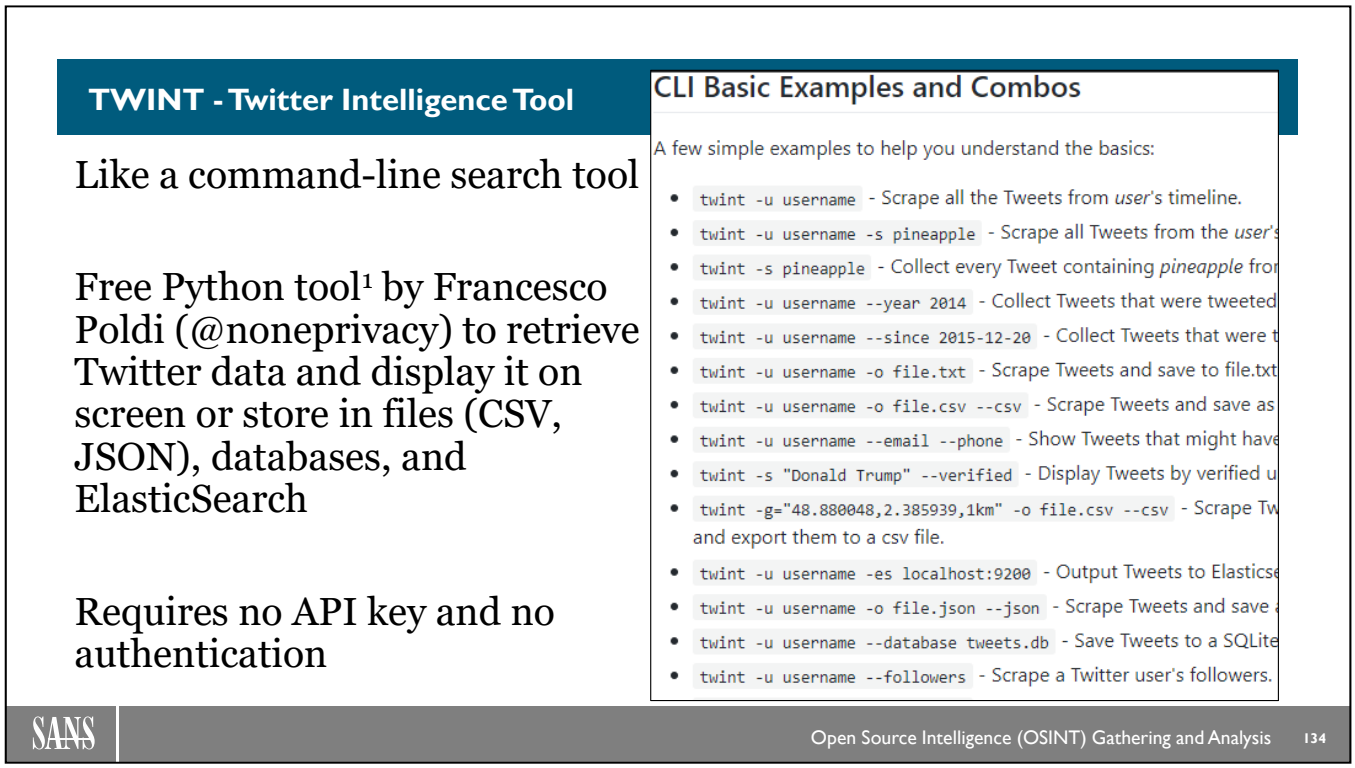
Excellent features and exporting of data



tinfoleak Script

The free tinfoleak Python script is available on GitHub (https://sec487.info/md) and requires valid Twitter API keys to work. It uses the Twitter API to pull down a variety of content from Twitter, allows filtering of the results, and saves the content to your local system.

Image from https://sec487.info/md, January 2, 2019.



TWINT - Twitter Intelligence Tool

TWINT is like a command-line interface to search and retrieve content from Twitter. Everything you can request via the search bar in the mobile or web applications can be performed in TWINT. On the right side of the slide is a sample set of commands that you can tell TWINT the execute.[1]

It is a free Python tool that not only retrieves content quickly, but it stores what it scrapes in a variety of formats, from flat files like CSV and JSON to databases and ElasticSearch.

Francesco Poldi (@noneprivacy) has an excellent blog post at https://sec487.info/xk that explains how the tool works and how to run it.

Reference:

[1] https://sec487.info/xj

TWINT Output Example

```
twint --year 2016 -s brexit --csv -o out.csv
```

	D	E	G	H	I	J	K	L	
1	date	time	user_id	username	name	place	tweet	mentions	urls
2	2015-12-31	18:56:49	396095407	andy_brexit	Prof Andy #Brexit #WTO		@AnnLeopards @LUCYDEMAINE @OliverDemaine https://twitter.com/cuteanimalsbaby/status/682685218382331904 …	['lucydemaine']	['https://t
3	2015-12-31	18:55:20	396095407	andy_brexit	Prof Andy #Brexit #WTO		@AnnLeopards https://twitter.com/brooklynfitchik/status/682700771868053504 …	[]	['https://t
4	2015-12-31	18:54:12	396095407	andy_brexit	Prof Andy #Brexit #WTO		since this was published the evidence and scandal around #statins has intensified Packets should have health warning https://twitter.com/pash22/status/682693235165257732 …	[]	['https://t
5	2015-12-31	18:21:12	4580223035	harvey72jon	Jon Micken		#Brexit https://twitter.com/LeaveEUOfficial/status/679345833704357892 …	[]	['https://t
6	2015-12-31	18:10:55	131192086	joethorpe1963	Joe Thorpe		Britain has given half a trillion pounds to #EU since 1973 - #UK #Betteroffout #Brexit - http://www.telegraph.co.uk/news/newstopics/eureferendum/12075046/Britain-has-given-half-a-trillion-pounds-to-EU-since-1973.html …	[]	['http://w 1207504 1973.htm
7	2015-12-31	18:02:27	4662932775	averagejoe64v2	Averagejoe64v2.0		But OF COURSE we would be WORSE off! #Brexit. Return to sanity. pic.twitter.com/DdMbew25jB	[]	[]
							@hendopolis Have a happy new year lad! Always nice to		

TWINT Output Example

We ran the TWINT tool trying to pull tweets from 2016 containing the string "brexit" (not hashtag, just the word) and then output that to a CSV. We then opened that CSV in the free LibreOffice spreadsheet tool and made it look pretty to show the content it gathered.

SEC487 Workbook

Please visit the course electronic workbook in the 487 virtual machine and begin the exercise named:

"Tweet Analysis"
and
"Twitter Bot Analysis"

This page intentionally left blank.

Course Roadmap

- Day 1: Foundations of OSINT
- Day 2: Gathering, Searching and Analyzing OSINT
- **Day 3: Social Media, Geolocation, and Imagery**
- Day 4: Networks, Government, and Business
- Day 5: The Dark Web, Breach Data, and International Issues
- Day 6: Capstone: Capture (and Present) the Flags

SOCIAL MEDIA, GEOLOCATION, AND IMAGERY

1. People Search Engines
2. Facebook Analysis
3. LinkedIn Data
4. Instagram
5. Twitter Data
6. **Geolocation**
7. Imagery and Maps

This page intentionally left blank.

OSINT View of Geolocation (1)

Corroboration of data
- Accident location data
- Alibi
- Cheating significant other
- Military activities[1]

Identifying normal habits

Risk assessments

RUSSIA MILITARY BANS FACEBOOK AS SOLDERS' BATTLEFIELD SELFIES REVEAL SECRET LOCATIONS

BY DAMIEN SHARKOV ON 10/5/17 AT 6:54 AM

The law will prevent soldiers from posting information, photos, videos, or geolocation data about themselves or other military personnel online.

It follows a 2014 in Ukraine, when selfies of soldiers geotagged in the east of the country contradicted Russian claims that it was not involved in the growinf conflict in Donetsk and Luhansk. The same occured a year later in Syria, before Russia announced its military operation there.

OSINT View of Geolocation (1)

There are many reasons for trying to find where a person is or will be, where a photo or video was taken, or where some event occurred. Our customers, many times, want this "where" question to be answered. With the prevalence of geolocation options in social media and images tagged on mapping applications, we have a broad range of resources at our disposal to answer these questions.

Some of the reasons our customers wish to understand "where" someone is or something occurred are shown in the slide above. The example posted above highlights that some people were geolocating Russian military troops by their social media activities. These social media posts clearly showed Russian soldiers were in places where they should not have been. This was a major public relations issue for Russia, so they made it illegal for the military to post social media containing this type of information.

Understanding where people are not is sometimes just as important as where they are. For instance, let's say that you have just posted to social media that you are at the airport waiting to take a trip. A robber watching your feed assumes that you are not at home right then and proceeds to rob your home.

Images from https://sec487.info/f7, December 9, 2017.

OSINT View of Geolocation (2)

Examine areas and events

- Aftermath of disasters
- Reconnaissance
- Riots/protests

Locate people

- Missing person?
- Show relationships between people (people at same place)

OSINT View of Geolocation (2)

We also use geolocation to examine sentiment in a certain location that may be having a protest or may have just had a natural disaster. When people gather or are in need, some turn to social media.

Finally, if we are looking for people, geolocation can help us locate the last tweet from a person that has gone missing. Or perhaps several people all geolocating their social media posts at the same location and time might show that those people are related or members of a single group (for example, a family, a gang, or a club).

Image from https://sec487.info/m3, December 9, 2017.

Shia LaBeouf's Anti-Trump Protest Art

In protest of Donald Trump, Shia LaBeouf placed a flag with "HE WILL NOT DIVIDE US" at an undisclosed location

A webcam live-streamed the flag with audio and video

4chan users in a certain group used geolocation cues to find the flag

OSINT techniques used:

- Angle of sun and time of sunrise and shadow analysis
- Geolocated image from Shia LaBeouf at a restaurant the same day flag was placed
- Analyzed the audio (frogs)
- Airplanes flying overhead
- Astronomy
- 4chan user's car honking

Shia LaBeouf's Anti-Trump Protest Art

Never underestimate the dedication of an internet troll or a group of them. In 2017, artist and Donald Trump protester Shia LaBeouf placed a flag with "HE WILL NOT DIVIDE US" on a pole in a field in protest of Donald Trump. Mr. LaBeouf also located a webcam in the field and focused it on the flag in hopes that, for the next four years, it would stream his objection to the new American President. Over the course of the coming weeks, people on the social media site 4chan located the remote location where the flag was placed. They used many clever OSINT techniques (see slide above) to find it and ultimately replace the flag with their own counterprotest objects.

The full article of this geolocation event is https://sec487.info/mf and image below is from https://sec487.info/mg.

WARNING: Faking Locations Is Easy

A word of warning before we go further

It is trivial to spoof or fake a location

There are applications and settings that can be altered to make a phone or computer look like it is somewhere else (remember the Twitter lab?)

When examining metadata and geolocated content, be skeptical

There are "tells" that can highlight if a person/system uses spoofing content

- Odd geolocations
- Magic traveler

Be wary in your analyses

WARNING: Faking Locations Is Easy

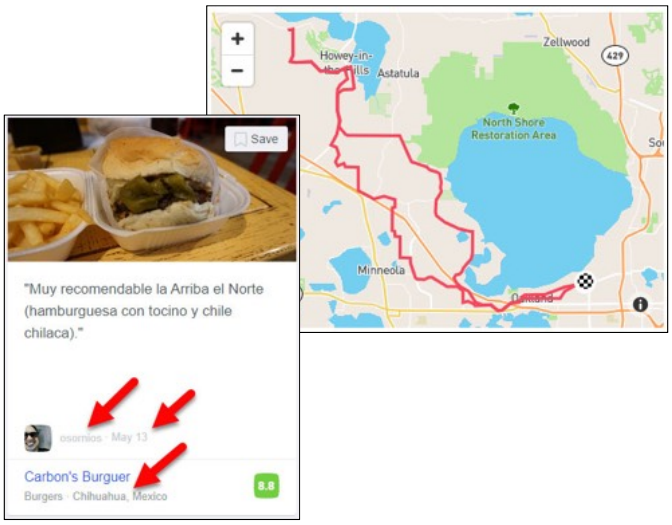
As some of you may already be aware, faking or "spoofing" locations is trivial with consumer-level software. Some applications, such as Google Chrome, Mozilla Firefox, and BlueStacks, come with settings that can be altered. For Chrome and Firefox, Micah Hoffman wrote a blog post on how to change the browser's location (https://sec487.info/d8). There are addons to the web browsers that can do this, too (Location Guard, https://sec487.info/m4). There are mobile applications such as FakeGPS that can also change a device's reported location.

Knowing all of this, we need to be careful when interpreting geolocated content. Most people do not alter their device's location before posting or tweeting, but some of your security-aware targets might. For these subjects, we need to examine many of their geolocated posts to see if there are any clues that geolocation-spoofing techniques were used. Some of the things we may look for include:

- Geolocated content that appears in odd locations, such as in the middle of lakes or deserts or places where there is no cell service. Yes, it is also true that ships and planes may have networks that people can use to geolocate content in remote places. So, this technique is not 100% accurate.
- The magic traveler scenario is one in which a person is reported or checks in at two or more locations where it would be physically impossible for him to be. For instance, someone posting that they are in South Africa and then, five minutes later, posting that they are in Beijing. The physical distance is too great for this to be true.

Mobile Apps Love to Geolocate

Dating apps (Tinder)
Exercise apps (Strava)
Drinking apps (Untappd)
Geolocation apps (Foursquare)
Social apps (Facebook)



Mobile Apps Love to Geolocate

Within the past ten years, more and more mobile applications have been adding the ability for their users to geolocate themselves. Tracking exercises, locating where people are drinking or eating, "checking in" to places, and reviewing restaurants, stores, and hotels; there are a huge variety of reasons to geolocate. This also means that there is a huge amount of geo-tagged data for our OSINT investigations.

We don't have the time or space in this course to examine every application that has a geolocation feature. Instead, let's look at a few representative cases so that you get the idea of what you are looking for and how you can use it.

Images from https://sec487.info/f8 and https://sec487.info/rr, September 6, 2019.

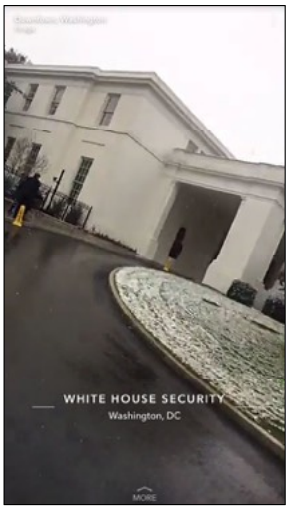
Snapchat Map

The Snap Map shows a heat map of where people are snapping

The more red an area is, the more activity

For us, these "Snaps" are at a certain location and are images or videos showing current conditions

https://map.snapchat.com/



Snapchat Map

The Snapchat application allows users to send images and short videos to their friends and followers. They can also choose to enable the geolocation feature so that their "Snaps" are posted to a map at https://sec487.info/m5 (shown above). Within the application, users can pinch the interface and bring up a map that shows areas that have a lot of Snap activity. Tapping on the map shows the Snaps that were geolocated at the location tapped.

In the image above, we took a screenshot of a person's Snap of "White House Security," which was a video of the person walking up to the front of the White House in Washington, DC.

Snap Map can give OSINT analysts video or still images from areas as events unfold or shortly thereafter.

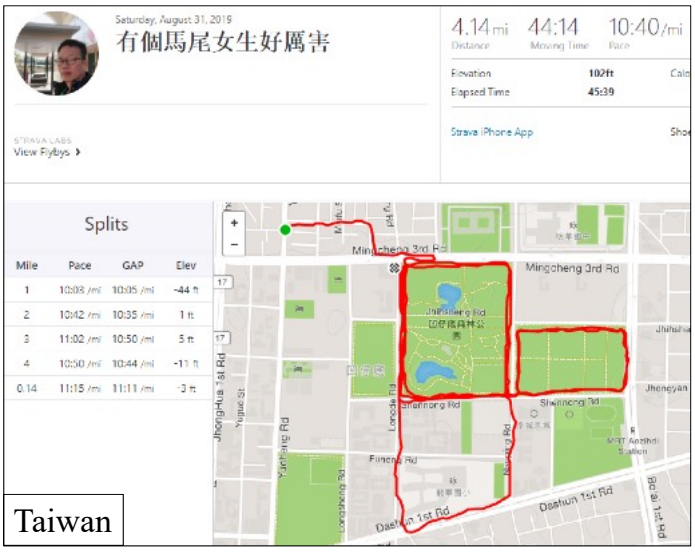
Images from https://sec487.info/rp and https://sec487.info/rq, September 9, 2019.

Exercise Apps

People track where they run, walk, hike, bike, and swim

Some exercise apps make this data available to the public

We can use this for establishing patterns and determining important locations (home, work...)



Exercise Apps

With exercise applications on mobile devices communicating with smart watches and pedometers, tracking fitness has become a big business. Part of the data collected during these activities can be the GPS track of where a user walked, biked, ran, or swam. Sites such as Strava.com (shown above) show GPS tracks for activities. We can find a user's account on the site and then examine their activities to find out when and where they exercise, where they begin and end the workouts, and data about who they run with or who comments on their activities (this would indicate a friendship).

To highlight some of the things you can do with exercise data and other OSINT topics, Micah Hoffman gave several conference talks called "Running Away from Security". One from BSidesDC in 2015 can be found https://sec487.info/da.

Image from https://sec487.info/rw, September 6, 2019.

Strava's Activity Heatmap

The Global Heatmap, Now 6x Hotter

I am happy to announce our first major update to the global heatmap on Strava Labs since 2015. This update includes six times more data than before—in total one billion activities from all Strava data through September 2017.

Our global heatmap is the largest, richest, and most beautiful dataset of its kind. It is a direct visualization of Strava's global network of athletes. To give a sense of scale, the new heatmap consists of:

- 1 billion activities
- 3 trillion latitude/longitude points
- 13 trillion pixels rasterized
- 10 terabytes of raw input data
- A total distance of 27 billion km (17 billion miles)
- A total recorded activity duration of 200 thousand years
- 5% of all land on Earth covered by tiles

Strava's Activity Heatmap

In 2015, Strava introduced the Heatmap, which showed an aggregation of exercises that were tracked along a particular route. Zoom into Athens, Greece (as shown above) and the map shows intense colors indicating many Strava exercisers have been logged within the area of the map. In 2017, Strava increased the amount of data that showed in these maps. Strava thought since they "anonymized" the data, they could show all the exercise activities, whether they were marked private by the athlete or not.

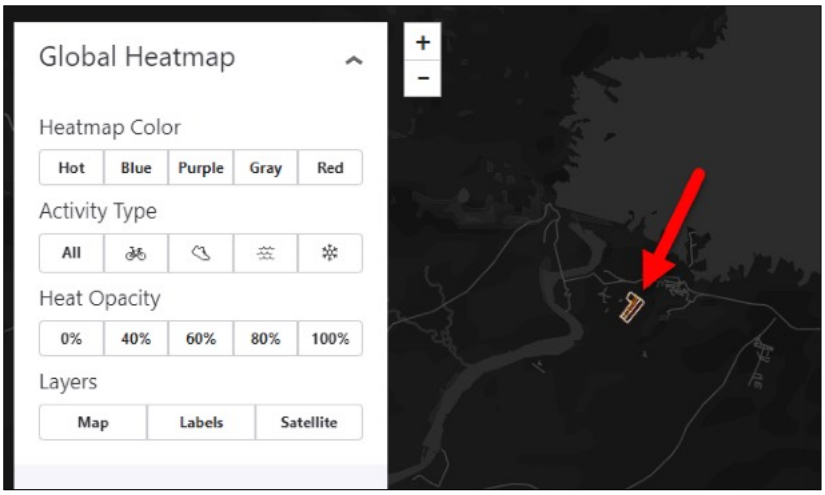
It turns out that just noticing running activity in certain places can give away data.

Images from https://sec487.info/h9 and https://sec487.info/h8, March 29, 2018.

Hot Spots in the Desert

Want to find "interesting places"?

1. Go to the heatmap
2. Go to a desert
3. Look for bright spots
4. Turn on satellite view
5. Investigate



Hot Spots in the Desert

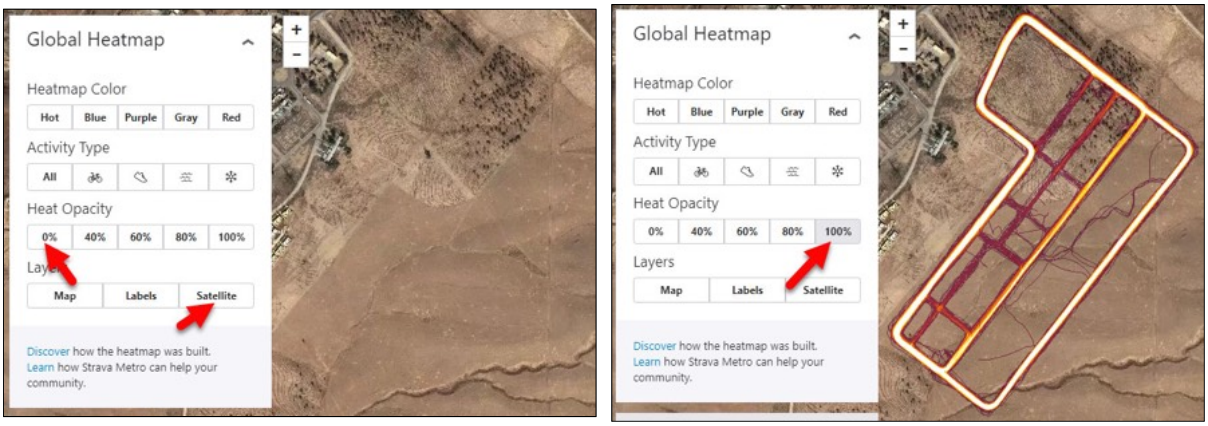
When the Strava heat map with the enhanced data was announced, people flocked to the site to examine what could be seen. What they saw was hot spots or bright areas in places where Google Maps' satellite view showed there were no villages or cities or people. It turns out that people had been running and bicycling on military bases in deserts. With Strava's heatmap, those areas now showed brightly outlined base perimeters, and showed who was running those segments.

The process to find these places is illustrated in the slide above with an interesting result shining brightly in the image. News outlets such as the BBC (https://sec487.info/ru) began reporting on this information disclosure issue, and Strava, shortly thereafter, began to remove the heatmap data in certain regions.

Image from https://sec487.info/rs, September 6,. 2019.

Running in the Desert with Strava

Northwest of Mosul, Iraq



Running in the Desert with Strava

Using the heatmap feature, it is simple to identify areas that have human activities, even if the satellite images show no human buildings in the area. Take, for example, what the Strava data shows about an area of the desert northwest of Mosul in Iraq. The picture on the left shows what a normal satellite image of the area looks like. While the image on the right highlights a large amount of exercise activity in certain patterns that could be roads. In one image, there should be no humans there. The other shows human activities. One is left to guess about what activities occur in this area.

Images from https://sec487.info/hc, September 9, 2019.

Finding Interesting Strava Places

Strava Map in Basrah, Iraq

Yandex Satellite Image

Finding Interesting Strava Places

While Google and Bing maps have no imagery for the above areas in Basrah, Iraq, we found that Yandex had more recent satellite images for us to examine. Examining the route tracked in Strava on the left, we can see it matches the outline of an area shown on the right. What is this area? What do people do here? These are questions that may be answered with additional OSINT work.

Images from https://sec487.info/hb and https://sec487.info/hd, September 9, 2019.

Strava Data Matters Because of People

Segments are a way of competing against others

Who can run it the fastest?

We get names, dates of runs, times, and even heartbeats!

Rank	Name	Date	Pace	HR	VAM	Time
	Black Panther	Jun 14, 2016	5:23/mi	-	-	5:06
2	Michael Webster	Nov 13, 2018	5:43/mi	-	-	5:25
3	Ross Taylor	Dec 6, 2017	6:14/mi	183bpm	-	5:54
3	Neil McKenzie	Nov 18, 2018	6:14/mi	-	-	5:54
5	Adam Gazzard	Mar 22, 2018	6:15/mi	102bpm	-	5:55

International segment explorer available at Doogal.co.uk

Strava Data Matters Because of People

Many geographic areas that can be biked, walked, run, or swam within Strava are broken down into segments. Athletes compete to see who can achieve the fastest run/swim/bike of a segment. As shown in the slide above, segments can show people data. Who ran/biked the segment, when, how fast, and what was their heart rate (which indicates their overall level of fitness). Since we know that each of these people exercised at this specific location at least once, and that this location in the desert is remote, we may be able to draw some inferences about who these people are and what they do.

If you would rather explore all the Strava segments via browsing a map, then you will want to visit the doogal.co.uk site and see its Strava Explorer application (https://sec487.info/s8). Move the map over any part of the world to examine if there are Strava segments and then get details on who ran that segment and when. It has links to the Strava site so that OSINT analysts can pivot to the user's profile.

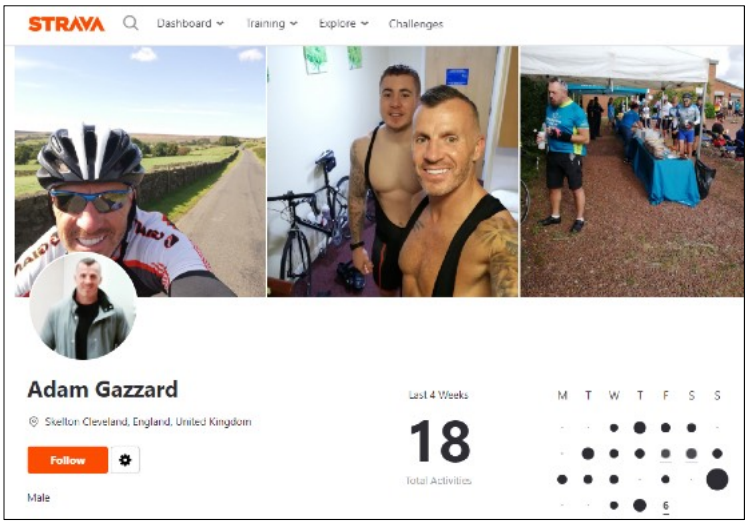
Image from https://sec487.info/hb, September 6, 2019.

Each Person Has a Profile Page

Athlete profiles may show other tracked exercises

Can also show where else they have exercised

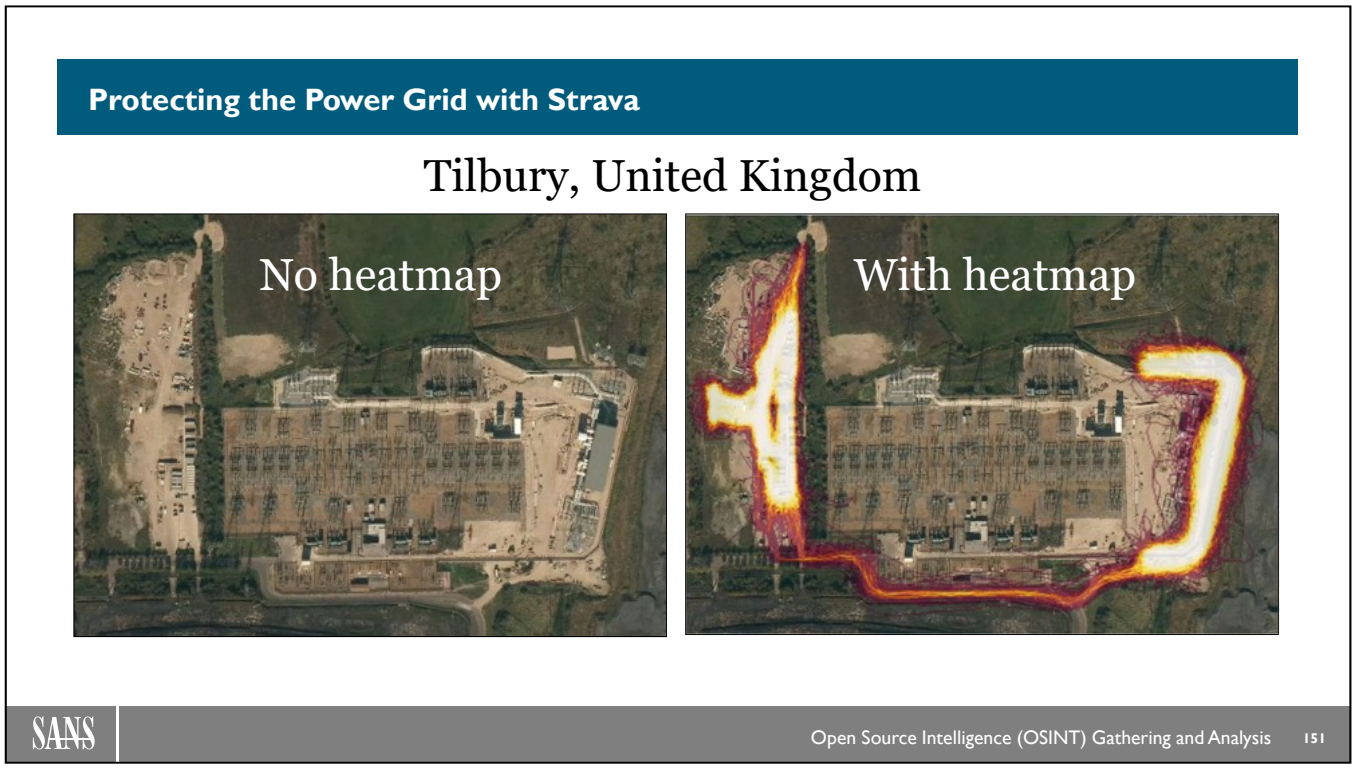
From who runs the segments, we can infer what work they do and for whom



Each Person Has a Profile Page

While you may need to be authenticated to the Strava app to view this data, each athlete has a profile page that sometimes tells where they are from, their full names, and other places that they exercise, and the profile page may have pictures. All of this can be used to better understand who these people are, who they work for, and what they were doing in the desert.

Images from https://sec487.info/he, September 6, 2019.



Protecting the Power Grid with Strava

Micah Hoffman gave several talks from 2015 to 2017 (https://sec487.info/da) where he discussed how a physical security company in the United Kingdom was using the Strava exercise application to track where and when their staff were doing their regular patrols of certain facilities. One such location that he mentioned in the talk was the Tilbury Power Substation (shown in the left image above). When we look at the location in the Strava heatmap (in the right image above), we can see a large number of Strava events were recorded for three sides of the Tilbury Power Substation. The fourth side shows no activity and might give an attacker insight into which areas of the facility are less likely to be monitored.

The above images were taken shortly after the new heatmap data was released. If you examine this region now, the above data is not present due to security and privacy issues.

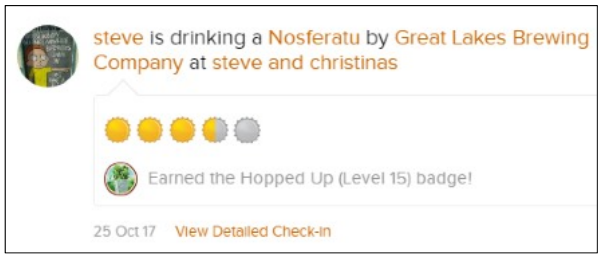
Images from: https://sec487.info/m9, January 31, 2018.

Drinking and Eating Apps

When people review food and drinks, they date and time stamp where they were

Sometimes this data contains friends of the poster, the food/drink they consumed, and their comments

Data may be organized by location, by user, or both



Drinking and Eating Apps

Some of the mobile applications on people's phones are used for rating food, drinks, and the establishments where they are served. Here, users can note what they ate or drank, who they were with, and their comments about the service. Some of the sites allow us to search by venue or location, and others allow us to view a certain person's profile and posts.

Users are geolocating themselves at certain places at certain dates/times and, sometimes, noting that they are drinking alcohol. This may be interesting data to your customers and relevant in your cases. Yelp, Zagat, Google reviews, and other travel and food sites might also have this data.

Images from https://sec487.info/m6, August 22, 2018, and https://sec487.info/fd, December 10, 2017.

Analyzing Alcohol Consumption - Untappd

Users on Untappd.com can submit when they reportedly drink beers, which beers they consume, where they drink them, and with whom (arrow 5)

For non-private accounts, much of this data is freely available with no authentication

Analyzing Alcohol Consumption - Untappd

It is amazing to see what some users will publicly post to social media web sites. A great example of this is the https://untappd.com beer-drinking web application. A person signs up for an account on the site, installs an app on their mobile device, and then submits the date, time, and location when they drink beer. The users get rewards in the form of badges for drinking certain amounts of certain types of beers at different locations.

While users need to create an account to submit their data, if their account is public, which is the default, we can view some of their drinking activities without having an account of our own. If we know their username on the site, we can visit their profile at https://untappd.com/user/USERNAME. The slide above demonstrates this for a user named "nechvi" (“3” in the image), who has submitted 6,515 beers to the site. We have no idea if this user drank any of those beers, but we can analyze the data for interesting trends.

Image from https://sec487.info/rv, September 6, 2019.

untappdScraper

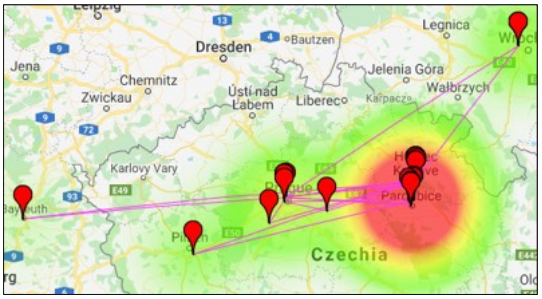
Using a free Python script on GitHub, we can harvest and analyze the data from a public Untappd profile

```
[ ] BEER CONSUMPTION DATA: Requesting
[*]  Drinking Patterns (Last 25 beers)
        Day ( #) : HISTOGRAM
       ---------------------------------
        Mon ( 3) : xxx
        Tue ( 1) : x
        Wed ( 5) : xxxxx
        Thu (13) : xxxxxxxxxxxxx
        Fri ( 3) : xxx
```

```
[*]  Drinking Patterns (Last 25 beers)
        Hour  ( #) : HISTOGRAM
       ---------------------------------
        06:00 ( 0) :
        07:00 ( 0) :
        08:00 ( 0) :
        09:00 ( 0) :
        10:00 ( 1) : x
        11:00 ( 1) : x
        12:00 ( 3) : xxx
        13:00 ( 0) :
        14:00 ( 1) : x
```

```
[*]  Drinking Patterns (Last 25 beers)
        Day (#) : HISTOGRAM
       ---------------------------------
        00  ( 0) :
        01  ( 0) :
        02  ( 3) : xxx
        03  ( 1) : x
        04  ( 5) : xxxxx
        05  (13) : xxxxxxxxxxxxx
        06  ( 3) : xxx
```

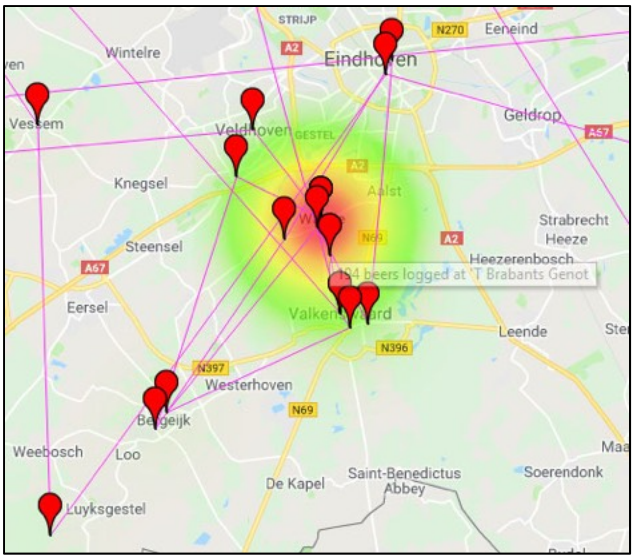
```
[ ] VENUE DATA: Requesting https://untappd.com/user/nechv

    Checkins   Name, Address (Geocode)
    --------  ----------------------------------------
       824      Pivní Ambasáda, Smilova 335 Pardubice,
       649      U toulavé pípy, Bělobranské nám. 9 Pard
       125      U Zamastilů, Hradišťská 299 Pardubice,
        80      Batalion u Draků, V Kopečku 163 Hradec
        79      Da-da-lie club, Czech Republic  (50.071
        72      Slunce ve skle 2018, Selská náves 21/2
```



untappdScraper

Using a Python script available on the GitHub site at https://sec487.info/lq, we can extract and analyze data for a specific user on the Untappd web site. The output is sent to the terminal and shown in text. Above are sections of the output from the "nechvi" account showing days of the week, hours of the day, days of the month, and locations where beers were logged to the untappd.com site.

If the OSINT analyst has a Google API key (see https://sec487.info/lq for details), they can have the script output an HTML file that can be opened in a web browser. This file will plot the locations where the person logged their beers on a Google map (shown below). More details about the script are available at https://sec487.info/mp.



Shifting Our Perspective - untappedWatcher

Instead of analyzing user-reported beer consumption, we can shift to the places they drink

What if we could watch a certain bar and collect data about who drinks there and when

What patterns of life can be determined from this?

Bar Name	User Name	Post Date	Post Time
Tasting Room	mauriiceg	Wednesday, September 4, 2019	02:07:40
Tasting Room	mauriiceg	Wednesday, September 4, 2019	02:16:18
Tasting Room	mauriiceg	Friday, September 6, 2019	00:26:07
Tasting Room	mauriiceg	Friday, September 6, 2019	02:38:14
Tasting Room	mauriiceg	Sunday, September 8, 2019	02:08:35
Tasting Room	mauriiceg	Sunday, September 8, 2019	05:11:19
Tasting Room	mauriiceg	Sunday, September 8, 2019	05:29:40
Tasting Room	mauriiceg	Tuesday, September 10, 2019	03:00:07
Tasting Room	mauriiceg	Wednesday, September 11, 2019	23:06:18
Tasting Room	mauriiceg	Thursday, September 12, 2019	04:13:00
Tasting Room	mauriiceg	Thursday, September 12, 2019	04:16:31
Tasting Room	mauriiceg	Thursday, September 12, 2019	04:36:45
Tasting Room	mauriiceg	Thursday, September 12, 2019	04:42:08
Tasting Room	mauriiceg	Thursday, September 12, 2019	04:44:27
Tasting Room	mauriiceg	Sunday, September 15, 2019	00:37:10
Tasting Room	mauriiceg	Sunday, September 15, 2019	02:35:39
Tasting Room	mauriiceg	Sunday, September 15, 2019	04:39:10
Tasting Room	mauriiceg	Sunday, September 15, 2019	04:40:20
Tasting Room	mauriiceg	Sunday, September 15, 2019	04:42:25
Tasting Room	mauriiceg	Sunday, September 15, 2019	05:11:25
Tasting Room	mauriiceg	Sunday, September 15, 2019	05:32:29

Output from the UntappdWatcher Script

Shifting Our Perspective - untappdWatcher

A student in SEC487 remarked that it would be neat to be able to watch a specific bar or pub and see who drinks there over time. This would be great for tracking patterns of life and drinking behaviors. For instance, what if there is a bar across the street from a person's work. They might visit the bar every Thursday after they get off their job. If they are an Untappd.com user, they might log beers at 5:15pm every Thursday. These routines are interesting to see.

Moreover, what if a group of people regularly log beers on Untappd.com at the same locations around the same time. Perhaps we can infer that they know each other or have a common interest (maybe the bar has a band playing on that night or karaoke). Collecting and analyzing this data can highlight these potential connections.

Or what if there was an accident outside of a certain pub and law enforcement wanted to see who visits the bar frequently. They can collect this data over time and analyze.

The UntappdWatcher script, available on GitHub at https://sec487.info/sr, does the collection for you. You choose the Untappd.com bars, pubs, or lounges to watch, add them to a text file, and then run the script every X minutes. The script queries Untappd.com for any new drinks logged and collects the data, storing it in a local database. The script allows querying of the database and exporting to CSV.

In the Excel spreadsheet in the slide, we see the output from the UntappdWatcher script. Here, we have selected the user "mauriiceg" and noted that his account logged drinks at "Tasting Room" bar in Mexico across multiple days. This appears to be a place this user visited frequently.

Echosec.net Paid Social Media Platform

Paid service that pulls social media content from a variety of international platforms with its own API keys

Can investigate user accounts, hashtags, geolocated content, and more

Monitor frequent locations, people, and hashtags

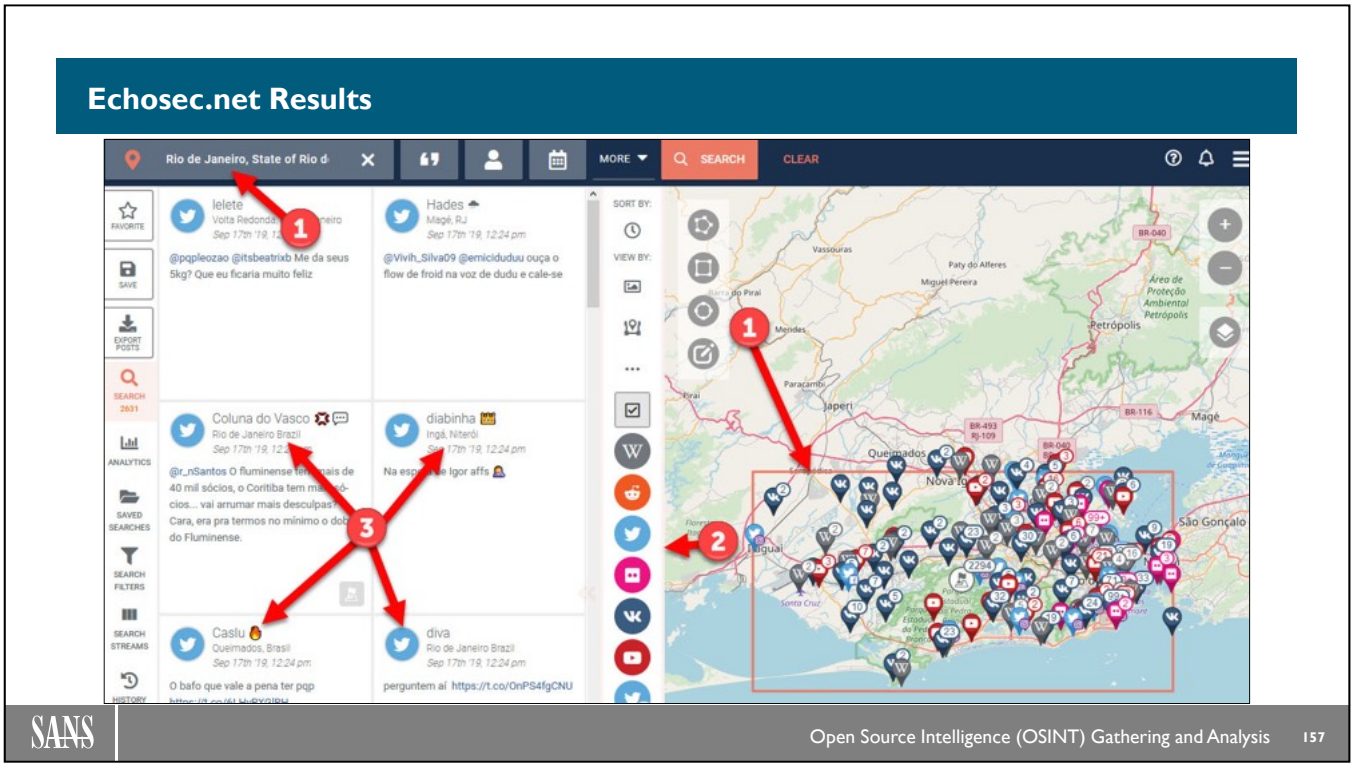
Echosec.net Paid Social Media Platform

We have seen that we can query each social media network (e.g., Facebook, Instagram, Twitter, etc.) for posts using certain hashtags, from specific users, or at a precise location. Doing this work across several social media platforms is time consuming. It also may require the use to acquire API keys from each social media network so that OSINT analysts can harvest that platform's data in near real time. But there is an alternative, if you have the budget for it. The Echosec.net web site hosts an application that does all these things, and more.

With a valid user account on the site, you can begin pulling large amounts of data from over 15 social media providers using Echosec's API keys. This simplifies your OSINT work so that you focus on the targets and not standing up a platform to harvest data from. Echosec's Social Media platform allows users to make queries into multiple social media providers simultaneously, searching for hashtags, user names, and at geolocated content. For the geolocated posts it retrieves, it will plot them on a world map at their specific location.

Want to track something or someone on social media over time? Echosec has a monitoring function where it will send email alerts to you based upon your saved searches.

Image from https://www.echosec.net, September 17, 2019.



Echosec.net Results

When a search is performed on the paid Echosec platform, the results are displayed in two separate frames. The left frame contains the filtered results that may or may not be geolocated, whereas the right pane displays any geolocated content plotted on a map. In the above example, we searched for any social media posts around Rio de Janeiro in Brazil (arrows labelled with 1).

The middle column (arrow 2) displays a list of the social media platforms found in the results. Selecting one or more of them will filter the results shown in the left pane (arrows labelled 3) and those displayed in the right map area.

At the top of the window are other search fields for hashtags or strings (the " icon), people or user accounts (the person image), and dates (the calendar icon).

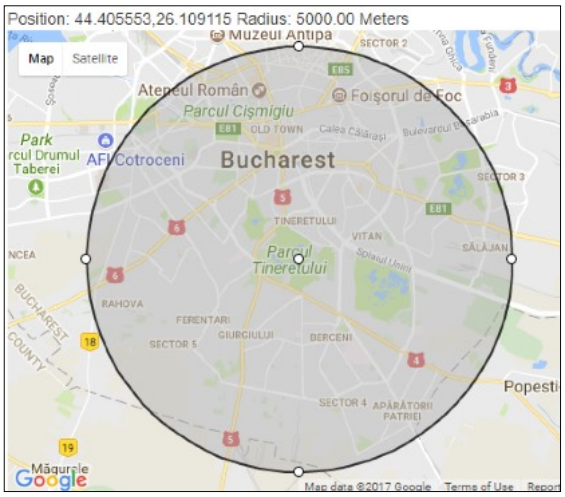
Image from https://echosec.net, September 17, 2019.

Geolocation Helper Sites

Sometimes we need some help when geolocating

Examples include:

- Transforming GPS coords (Ex: º min sec -> decimal)
- Drawing a virtual circle of X km around a location
- Figuring out the boundaries of a location (city, village, etc.)



Geolocation Helper Sites

Sometimes what we need to do is use a site that can help us move further in our geolocation analyses. For instance, sometimes we may get a GPS latitude and longitude coordinate in the format of degrees, minutes, and seconds and we need to transform it into decimal degrees to work with a certain analysis application or to compare it with other coordinates. Or perhaps a bank was just robbed in Bucharest, Romania (image above) and people believe the criminals are hiding in the Sala Polivalenta. They want to set up a 5 km circle around Sala Polivalenta in Bucharest, Romania. Thankfully, there are online applications that can assist with these tasks to make our assessments richer and more complete.

FreeMapTools

Helpful tools:

- Calculate area of shape you draw
- Radius around point
- Measure distance from one point to many
- Draw concentric circles on map
- International Center of Gravity
- And MANY more!

FreeMapTools

The Freemaptools.com site has a variety of tools that can assist in our OSINT work. The tools allow analysts to find areas, locations, and distances and to illustrate other concepts on Google maps. In the example above, we used the "International Meeting COG" tool to discover a location common to five different cities in Europe. This tool can help your investigation by automating what, without them, may have been manual processes.

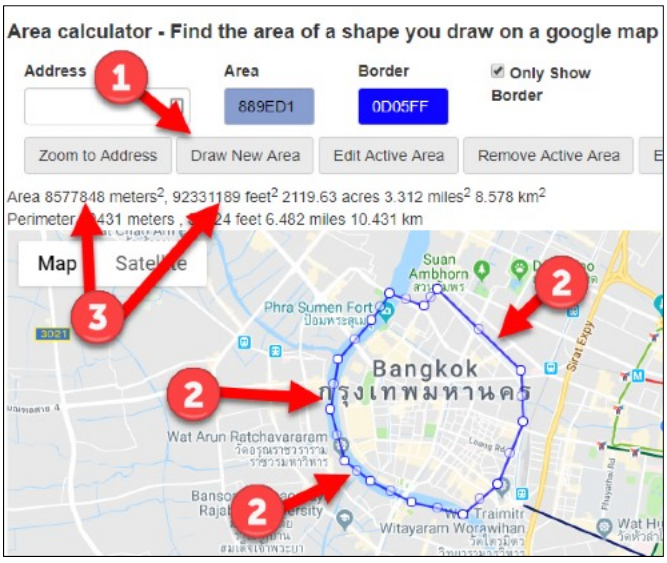
From drawing circles on maps to converting coordinates to country-specific content, this free resource has many other tools that may be helpful for mapping and geolocation.

Image from https://sec487.info/s3, September 16, 2019.

MapDevelopers.com

Helpful tools:

- Calculate area of shape you draw
- Elevation Calculator
- Radius around point
- Geocode Tool
- Batch Geocoding
- Mileage Calculator



MapDevelopers.com

While it does not have as many tools as FreeMapTools.com, MapDevelopers.com has some that you may wish to use. Shown in the image above is the area calculator tool that allows users to draw a polygon on a map, and then the site will determine the area of the space inside the shape. There are also features to geocode addresses and convert points from one geocode system to another.

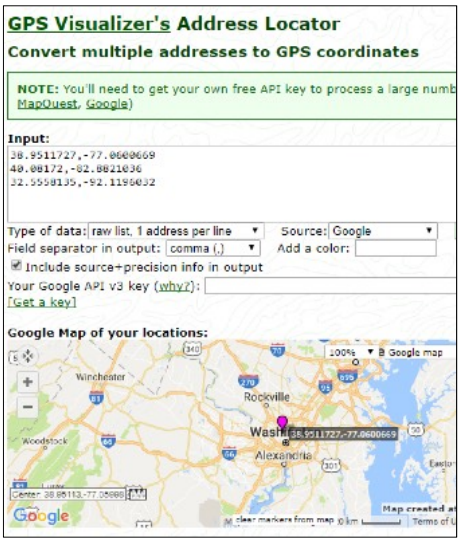
Another helpful feature of this site is drawing multiple colored circles on a map. You can, for instance, draw an inner and outer circle around a point in Bucharest, Romania. These points can be set at certain sizes (1km, 2 miles, etc.), and you have control over the colors and formatting of the image.

Image from https://sec487.info/s4, September 16, 2019.

GPSVisualizer

While this tool is focused on taking GPS routes and visualizing them on a map, it has other features we may use

- Converting GPS codes to various formats
- Bulk GPS encoding



GPSVisualizer

This site's purpose is to create maps from GPS data, but there are other features that might be of interest to us. There is some overlap between its functions and some of the previously mentioned ones (it can create circles on maps, etc.), but GPSVisualizer does geocode transformations very easily. Have a number of latitude and longitude coordinates to plot or geocode? This is a great site to do that work.

Image from https://sec487.info/de, December 10, 2017.

Course Roadmap

- Day 1: Foundations of OSINT
- Day 2: Gathering, Searching and Analyzing OSINT
- **Day 3: Social Media, Geolocation, and Imagery**
- Day 4: Networks, Government, and Business
- Day 5: The Dark Web, Breach Data, and International Issues
- Day 6: Capstone: Capture (and Present) the Flags

SOCIAL MEDIA, GEOLOCATION, AND IMAGERY

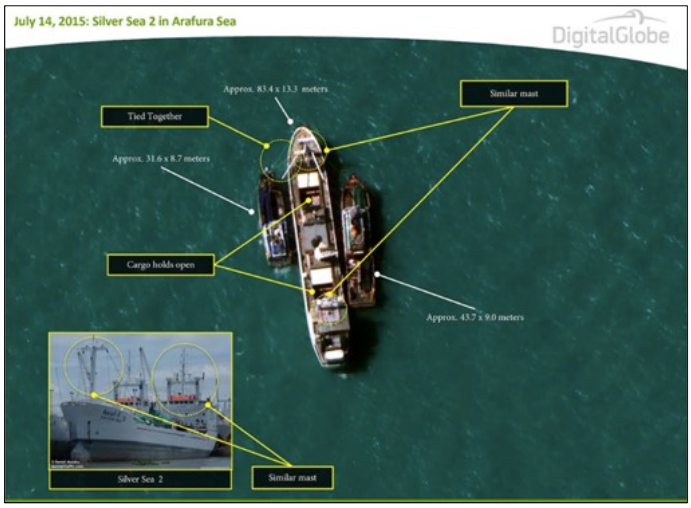
1. People Search Engines
2. Facebook Analysis
3. LinkedIn Data
4. Instagram
5. Twitter Data
6. Geolocation
7. **Imagery and Maps**

This page intentionally left blank.

Imagery for Journalists

Global Investigative Journalism Network article discussed how researchers use imagery

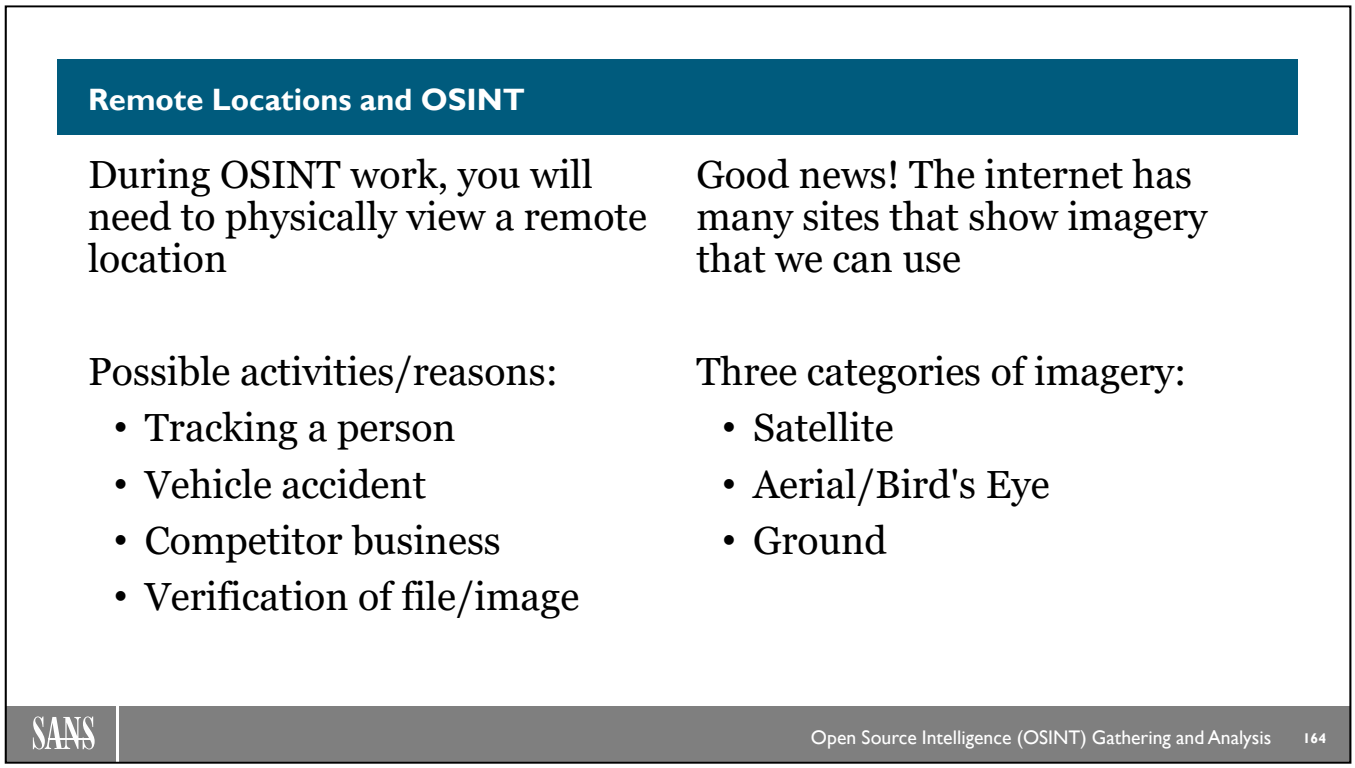
- Establishing correlations
- War zone reporting
- Change detection
- Tracking terror
- Access to the inaccessible
- Adding visual elements



Imagery for Journalists

We already discussed that OSINT is research for a certain cause and journalists use OSINT techniques in their research to answer questions like "what happened in that area?" and "why is that ship in those waters?" The Global Investigative Journalism Network published a detailed article in 2018[1] about how journalists are increasingly leveraging imagery for their research. The article is detailed and goes into depth about how they use imagery but also what they should watch out for when using it. All of this is analogous and helpful to OSINT analysts who may be performing similar queries to answer different questions.

Reference [1] and image from https://sec487.info/mr, January 3, 2019.



Remote Locations and OSINT

During your investigations, you will need to see what another place in the world looks like. You might be validating a victim's claim for an insurance company and viewing what a certain road intersection looks like, or maybe you received a tip that the spouse of your client visits a certain address each night after work and you want to see what is at that place. There are many other reasons why you will need to use aerial and ground-based imagery on the internet in your assessments.

In general, we have three different types of imagery:

- **Satellite** - The world has been placing cameras in orbit around our planet for decades and, from them, we can see amazing views. Satellites take pictures of the land, roads, and other physical features from space and then send them to companies that digitally stitch them together and put them in a web application. Some areas of the world have amazing, high-resolution images (such as those found in this shot of an African village using Google Maps, https://sec487.info/61) for your viewing and usage. One issue with satellite images is that they can be older and, since they may not be refreshed often, may not accurately represent the location as seen today.
- **Aerial** - These images are taken from planes, drones, and other flying machines that collect images and send them back to a company for processing and placing into their web applications. Microsoft calls these images "Aerial" and "Bird's Eye" for their direct down and 45-degree camera-angled images, respectively. The benefit here is that you can get...
- **Aerial (cont'd)** - ...a view of a location from an angle and then rotate around the target to gain perspective.
- **Ground** - Here we have a class of images taken from a ground-based position. These could range from Google's Street View and Bing's Streetside services to crowd-sourced street-view projects. Broadening our focus (pun intended), the pictures that people are posting to social media sites, traffic cameras, and other terrestrial-based devices also fall into this category. Since some of these photos are taken and published immediately to the internet (crowd-sourced from social media), these images can be very accurate and reflect how the location looks at the present time.

Each of these aspects of visual remote location analysis is useful to you as an OSINT analyst, depending upon your OSINT task goals.

Satellite Images

Pros:

- Overhead pictures show areas inaccessible via land
- Give "lay of the land" look at region
- Useful for understanding context of location and objects
- Allow for measuring distances

Cons:

- Age of imagery not always recent
- Low resolution in some regions
- Seasons change images (trees with leaves or without)

Satellite Images

Satellite or overhead imagery allows us to see the area around our targets and understand man-made and natural features that our human targets may encounter. They also allow us to measure distances between places or features so that we can understand, given a certain mode of transportation (for example, walking or driving), how far a target could move away from a given location.

Potential drawbacks to using this imagery may be that it is not recent enough for your assessment; for example, it does not show newer buildings and roads since the imagery is updated less frequently than other types of data. Some of it can also be less detailed than other types of imagery, although the resolution of imagery from space continues to increase. Since a United States restriction was modified in 2014 making it legal to provide consumers with imagery at a resolution of less than 50cm (20 inches), we have been consuming near-military-grade images from space at up to 31cm (12 inch) resolution![1]

Images from satellites are impacted by atmospheric changes such as weather, which can impair or degrade image quality. Additionally, some areas of the world do not get their imagery updated very frequently. This, combined with changes in the seasons, can be problematic. For instance, if a satellite took images of a region in the summer (with trees full of leaves), you will not see as much of the ground as if those pictures were taken in the winter when the leaves may have fallen to the ground.

Reference:

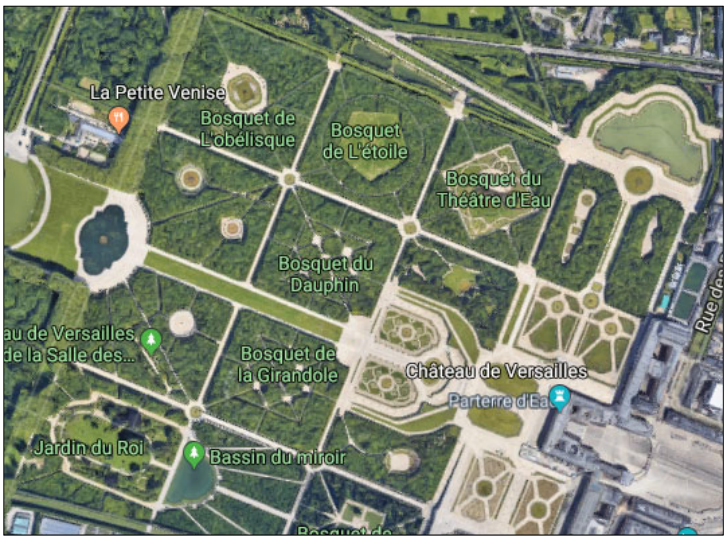
[1] https://sec487.info/62, August 20, 2017.

Satellite Web Site Heavy Hitters

The major players within the online mapping scene are mostly major search engines:

- Google Maps
- Bing Maps
- Yandex Maps

Extra satellite resources are in the notes section



Satellite Web Site Heavy Hitters

There are MANY players in the free satellite imagery web site market, but the "heavy hitters"[1] are mostly search engines: Google, Bing, and Yandex. Please recognize that, with the huge number of online imagery sites on the internet, we cannot evaluate all of them. The sites we do examine will get you most of what you need to succeed. If your region or target area has a better tool, use it!

There are other places where we can obtain satellite imagery. The 15 sites that the https://sec487.info/ua site lists cover imagery from NASA images of the atmosphere to the commercial satellite pictures from Maxar (previously Digital Globe). We can also use imagery from Descartes Labs (https://sec487.info/ub). Some of these resources provide imagery at a cost. Some allow you to task their satellites to take pictures of specific areas of the world.

Image: Versailles, France, https://sec487.info/gl, September 25, 2019.

Reference:

[1] In the game of baseball, a "heavy hitter" is someone who is relied upon for their prowess at batting and hitting the ball out of the baseball park to create home runs. Within the above context, "heavy hitters" means that these are some of the biggest, widest-known companies in the free mapping arena.

Google Maps Satellite

https://www.google.com/maps/

Features:

- Normal "Map" view
- Satellite view
- 3D view of buildings
- Distance measurement
- 6 months to 5 years old [1]

Google Maps Satellite

Available at https://www.google.com/maps/, Google Maps is an excellent resource for your OSINT-imagery needs. It has recent imagery and a wealth of features that make it the "go-to" resource for many OSINT analysts. Some of the features you might find useful include:

- Normal map view and satellite view.
- Some buildings are mapped to 3D images, so they appear their scaled height on the map. Gives perspective.
- You can get near-real-time traffic updates in many places and, in some, general traffic information about what typical road traffic is like on a given day of the week and time of day.
- Google has a pretty good measurement tool to measure distances between places or along routes.
- The Google Earth Blog[1] notes that imagery in Google satellite web pages may be between "6 months and 5 years of age." This is due to a variety of factors, chief among them is cost of new imagery from satellites.

This image is from Yongbyon, North Pyongan, North Korea and shows the locations of a suspected underground nuclear research and testing facility. Arrows labelled “1” show tunnel entrances to the hidden/underground base itself (arrow 3). Arrow 2 points to a known nuclear reactor.[2]

Image from https://sec487.info/th, September 24, 2019.

References:

[1] https://sec487.info/68, August 25, 2017.

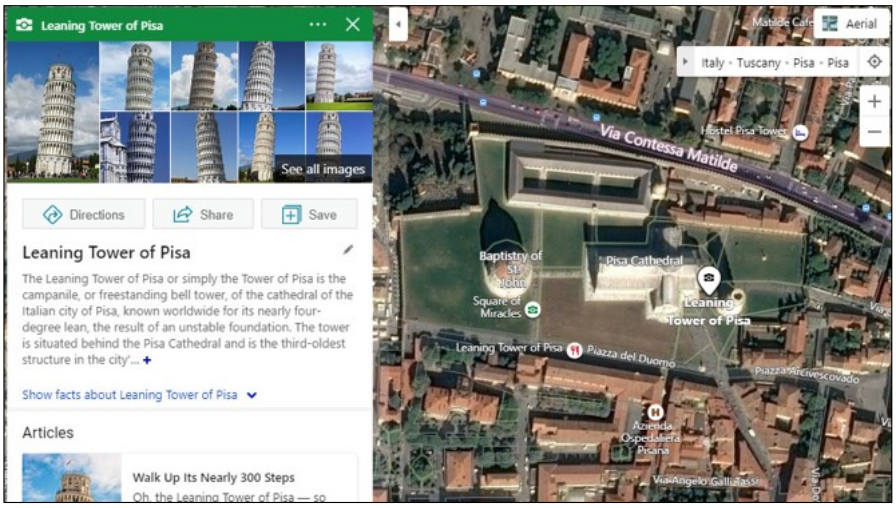
[2] https://sec487.info/tg

Bing Maps Satellite

https://bing.com/maps/

Features:

- Normal "Map" view
- Satellite view
- Bird's Eye view with rotation
- Traffic
- Distance measurement



Bing Maps Satellite

Each of the mapping applications we are covering has strengths that complement the other mapping applications. For instance, Microsoft's Bing Maps application has many similar views as Google Maps but uses different sources for many of its maps. This can be a benefit to us since we get images from different times of day, season, and year.

Bing has many of the same features as Google (and, spoiler alert, Yandex too), but it also has a different view from above the Earth called "Aerial View." We'll cover that shortly.

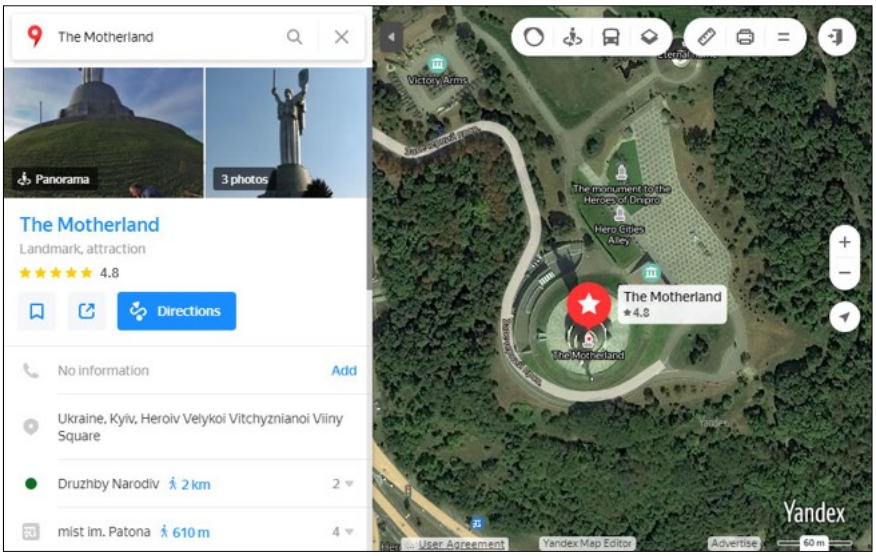
Image from https://sec487.info/mv, September 24, 2019.

Yandex Maps Satellite

https://yandex.com/maps/

Features:

- Normal "Map" view
- Satellite view
- Traffic
- Distance measurement
- Russian site with world maps



Yandex Maps Satellite

Yandex, a Russian company similar in the web search and map arenas to Google and Bing, focuses on regional results. Yes, it has world maps, but where it is most useful is in places close to or in Russia. Yandex's Street Panorama views (shown in upcoming slides) are excellent in Asia and some European places.

Image from https://sec487.info/ti, September 24, 2019.

Aerial Images

Pros:

- Updated frequently in some locations
- Good -> great resolution
- View from different perspectives (turn camera)
- Some buildings are mapped in realistic 3D
- Little to no atmospheric interference

Cons:

- Seasons change images (trees with leaves or without)
- Aerial (non-satellite) images not available in all areas

Aerial Images

Satellite images are pictures taken from space (sometimes at extremely high resolution). Aerial images are taken from planes, balloons, or even kites[1] flying around our planet. There are some benefits to using these flying machines to take pictures of Earth:

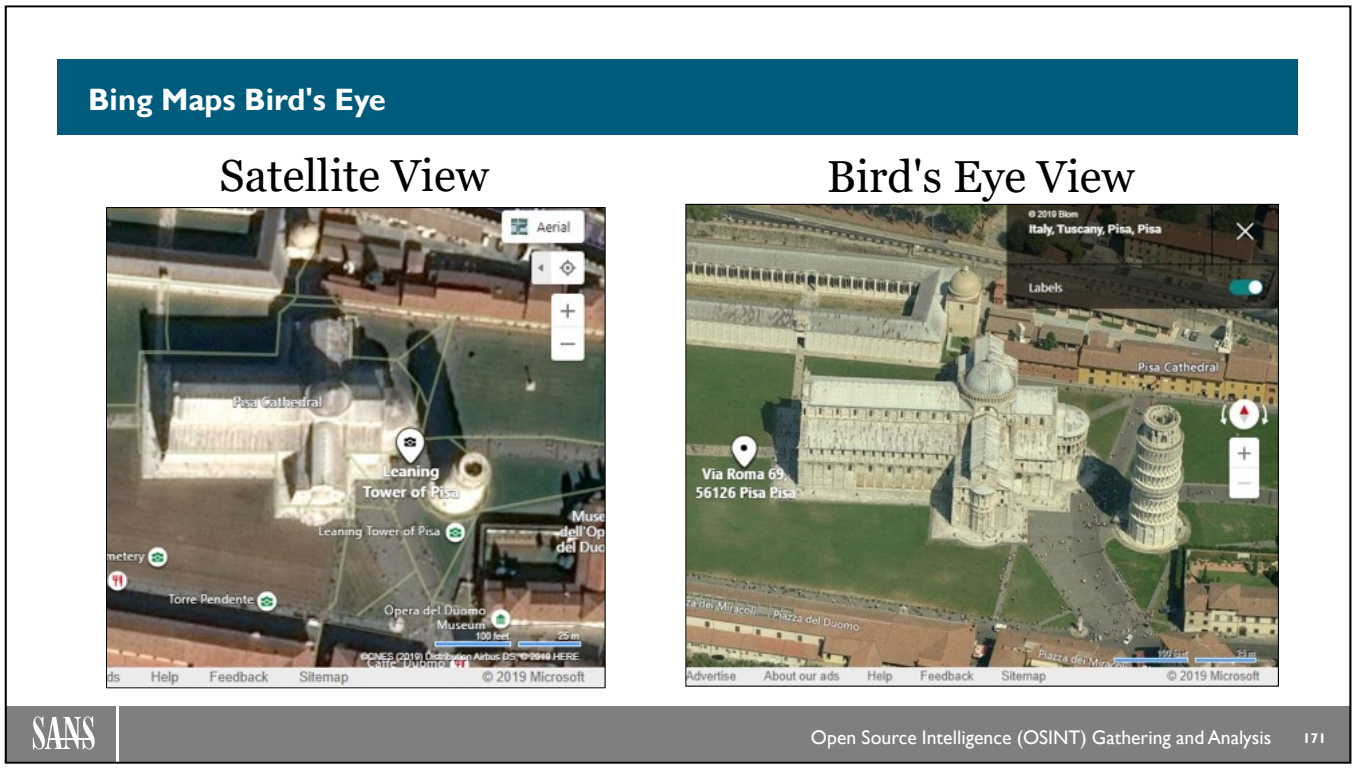
- Clouds, weather, and other atmospheric conditions impact them less, so we can get better pictures faster.
- It is low cost and easy to send up these vehicles to get better and more frequent images.
- We can see our target areas from a variety of angles to give a 360-degree view.

There are some downsides to relying on aerial imagery, too.

- Depending upon when the photos were taken, there may be foliage (trees and bushes) obscuring the details you need.
- Only some areas of the planet have aerial imagery in these mapping applications. So, if your target area is not near a popular place or city, there may not be aerial images.

Reference:

[1] https://sec487.info/69, August 26, 2017.



Bing Maps Bird's Eye

Microsoft's Bing Maps has a terrific set of aerial images that it calls its "Bird's Eye" view. They let you view a location from all sides at "a 45 degree angle, giving depth and three-dimensionality to ortho photography."[1] In the above slide, we can see the Tower of Pisa,[2] more commonly known as the Leaning Tower of Pisa due to its roughly 4-degree tilt.[3] The left image is of the satellite view of the Cattedrale di Pisa where the tower stands. The image on the right shows the tower using the Bird's Eye view, which highlights the tower from a 45-degree angle, allowing us to gain a better understanding of how it looks.

Using the arrow controls around the compass rose on the mapping page (shown at right), we can rotate the view and see the Bird's Eye imagery from all four sides of the target.

Image from https://binged.it/2v8PfQd, September 24, 2019.

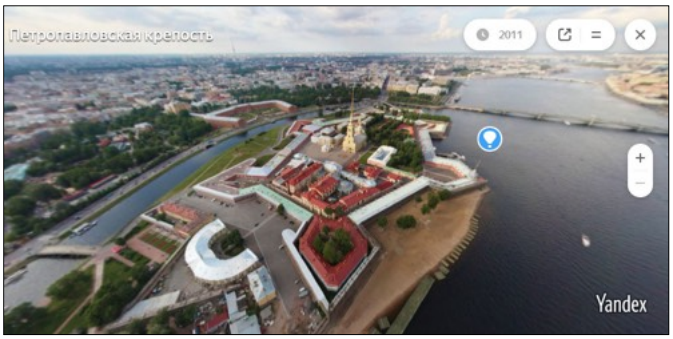
References:

[1] https://sec487.info/6b, August 26, 2017.

[2] https://sec487.info/mw, August 26, 2017.

[3] https://sec487.info/6a, August 26, 2017.

Yandex Maps Aerial Balloons!



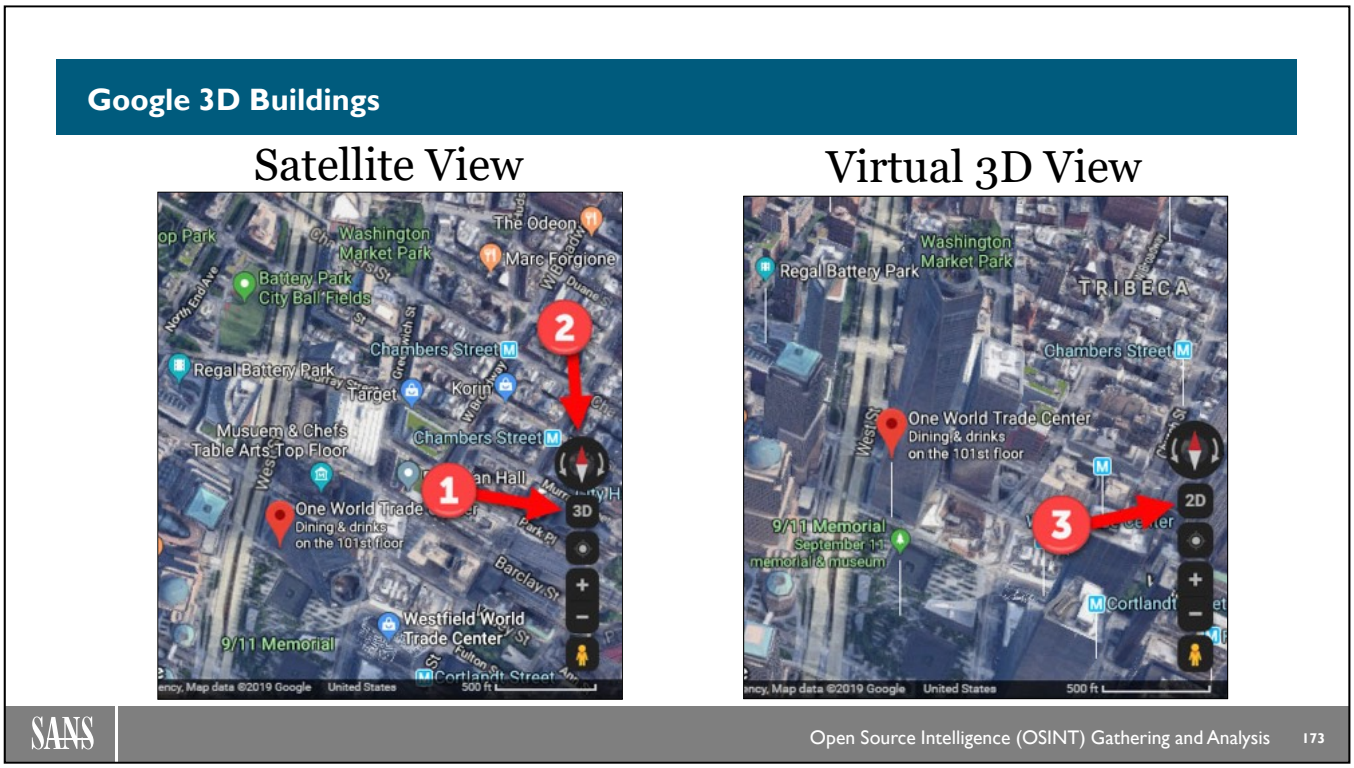
Yandex Maps Aerial Balloons!

Yandex's Street Panorama function allows you to see images taken from people and vehicles on the roads and aerial 360-degree panoramas shot from helicopters, planes, and balloons. Simply click the icon at arrow 1 and then click on a hot air balloon icon (arrow 2) or a blue road in the map. The results, in the right picture above, show the target area from overhead or on the ground, respectively. You can zoom in on the picture too for more-precise details.

Images from https://sec487.info/tj and https://sec487.info/tk, September 24, 2019.

Reference:

[1] https://sec487.info/6k, August 26, 2017.



Google 3D Buildings

Our final entry in the aerial imagery category is not really aerial imagery but a rendering of the map data to appear 3D. Google has done amazing work on making two-dimensional images turn three dimensional to make them come "alive." The image on the left is a normal, satellite image from Google Maps of the One World Trade Center in New York City and is shown in 2D mode. Clicking the 3D icon on the right of the image (arrow 1) turns on the 3D view and makes all the available 3D objects render as such (picture on the right). See how the One World Trade Center tower pops up in the middle of the right image? To change back to 2D mode, click on the 3D icon (arrow 3) and it will return to the normal view.

If you'd like to look around the target area, you can turn the view using the arrows around the compass rose (arrow 2).

Images from https://sec487.info/tm and https://sec487.info/tl, September 24, 2019.

Ground-Based Images

Pros:

- Can see things from a human's point of view
- Greater detail than other views
- More recent imagery
- Virtually visit an area

Cons:

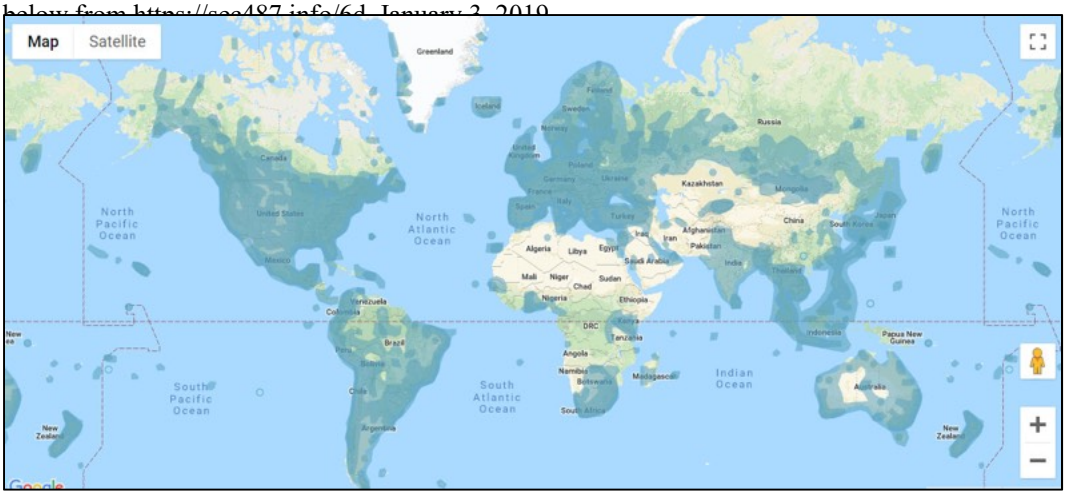
- Quality can vary
- In many places (including some indoor spaces) but not everywhere aerial/sat imagery is

Ground-Based Images

This final category of mapping is based upon vehicle, people, and fixed and mobile cameras. At the ground level, many parts of our world are overwhelmed with cameras that capture video and still images that can be used in our assessments. Images from these sources can be in high resolution and extremely recent (seconds old). They also can be old and vary in quality. It all depends on who took the picture, with what equipment, and when.

Ground-based imagery allows us to virtually visit an area by using the detailed, linked-together images to "walk" or "drive" through a region. Unfortunately, you will only find these images shown in mapping applications for popular and visited areas of the world. Remote areas are less likely to have ground-based images. Google's Street View has a map of where they have imagery (shown below). Filled-in areas show where they have ground-based images.

Image below from https://sce487.info/6d, January 3, 2019



Google Street View

Google made ground-based imagery easy

Strap a special camera to a car, boat, snowmobile, bike, or human and go!

Images on hiking trails, inside buildings, on the water and so many other places

Google Street View

The official Google Street View images come from special cameras that Google has mounted on cars, bikes, snowmobiles, boats, and backpacks. These cameras can go almost anywhere that people travel on, above and inside the planet. They can take images on hiking trails,[1] inside buildings,[2] and many other less-accessible places for cars.

Google allows people to upload their panoramas, photo spheres, and normal images to its servers and have them augment the data that Google, itself, has gathered. This broadens the imagery sources that are displayed on Google's Street View and in Google Earth. Not only does it present you with images from places that Google's official cars cannot reach, but they show many views of the same places from different people taking pictures during different times of the day and different times of the year. For popular locations, there may be several images that document what the location looks like throughout the entire year.

It also appears that the privacy controls, such as blurring faces and license plates, that Google applies consistently to its own imagery may not be as rigorously applied to crowd-sourced images. This means you may be able to view the content of what Google blurs by visiting the images users upload to Google.

Images from:

https://sec487.info/mx, August 26, 2017.

https://sec487.info/my, August 26, 2017.

https://sec487.info/mz, August 26, 2017.

References:

[1] Grand Canyon, https://sec487.info/6e, August 26, 2017.

[2] The White House, https://sec487.info/6f, August 26, 2017.

Using Google Street View

1 - Click and hold on the yellow person icon and drag it somewhere on the map

2 - Blue paths show images from vehicles (boats/cars)

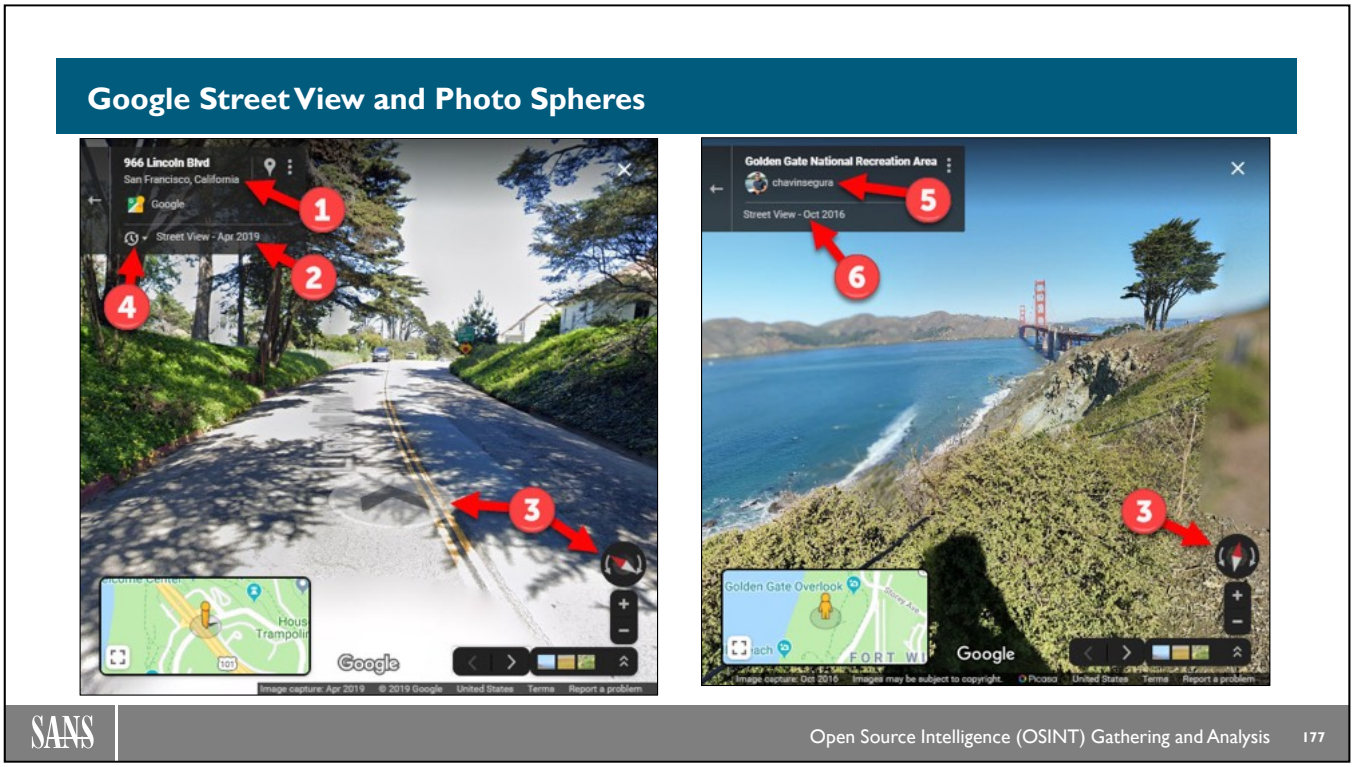
3 - Circles are photo spheres

Using Google Street View

To use the Street View images, click and drag the yellow person icon in the map page onto the map (arrow 1). Once the icon moves onto the map, sections that have Street View data are highlighted in blue. Continuous Street View paths, such as from vehicles with a Google camera attached, show as solid blue lines (arrows at 2), and photo spheres/panoramas show as circles on the map (arrows at 3).

Dropping the yellow person icon onto one of these blue-highlighted paths or bubbles will bring up the imagery from that source.

Image from https://sec487.info/6g, September 24, 2019.



Google Street View and Photo Spheres

Street View images (from official Google cameras) show approximate address information (arrow 1) and when the images were taken (arrow 2). If Google has multiple images from that location from different dates, it allows you to go back in time and see them by clicking on the clock (arrow 4) and then selecting which other date(s) to view. In both Street View and user-uploaded photo spheres, you can use the arrows around the compass rose (arrows at 3) to turn the view and look 360 degrees around the current position.

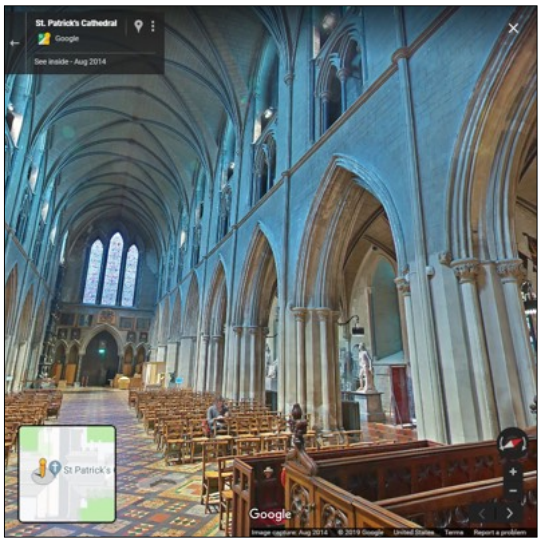
For photo spheres, right image above, we get the perspective from the person who took the picture. In our example, we see that the user chavinsegura uploaded his photo sphere near the Golden Gate bridge in Oct 2016. We can click and drag the picture to turn around or use the arrows in the compass rose.

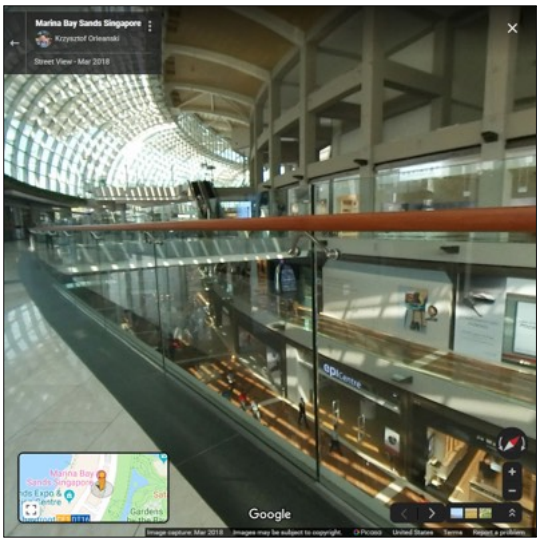
Images from:

Street View: https://sec487.info/6h, September 24, 2019.

Photo Sphere: https://sec487.info/6i, September 24, 2019.

Google Street View and Photo Spheres Inside





Google Street View and Photo Spheres Inside

Please do not think that Google Street View and Photo Sphere imagery is just for outside locations. People and companies use this type of imagery to highlight the insides of a huge variety of locations. Google's Street View cameras have ventured inside museums, religious buildings, and other locations.[1] User-contributed Photo Sphere images can be found almost anywhere in the world and beyond.[2]

Why do we care about these images for OSINT reasons? They allow us to see inside places we would otherwise have to travel to. Take, for instance, the Street View image above from St. Patrick's Cathedral in Dublin, Ireland. See the specific pattern and color of the flooring? We can see that and examine it closer by zooming in. Now let's say that you had a photo of a suspect who had a similar floor pattern. Using these images, we can verify and validate locations, explore bars and night clubs in daylight, and perform remote reconnaissance of a location.

Images from https://sec487.info/ut (left) and https://sec487.info/uu (right), September 28, 2019.

References:

[1] https://sec487.info/uv

[2] Imagery from inside the ISS (International Space Station) can be found at https://sec487.info/uw

Bing Streetside

Includes date of image and relative address

Fewer places have imagery than Google

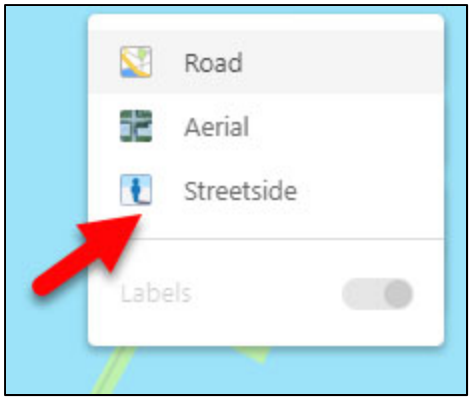
Not crowd-sourced like Google

Bing Streetside

Microsoft's Bing has a similar capability to Google with its Streetside[1] images. Here Microsoft uses its own vehicles to capture imagery and then display on the mapping pages. Streetside imagery can be found in fewer places than those with Google's Street View data. Microsoft, as of this writing, does not allow users to upload their images to the Streetside view, which also limits the imagery shown on the site. Arrows in the image above show the date of the imagery (arrow 2) and the relative street address (arrow 1).

Since Microsoft uses different sources for the imagery, we can sometimes use it in conjunction with Google Street View images to gain a more-complete view of a target area.

To show the Streetside content for an area, click on the layers menu and select the Streetside layer (as shown on right).



Images from https://sec487.info/n0, September 24, 2019.

Reference:

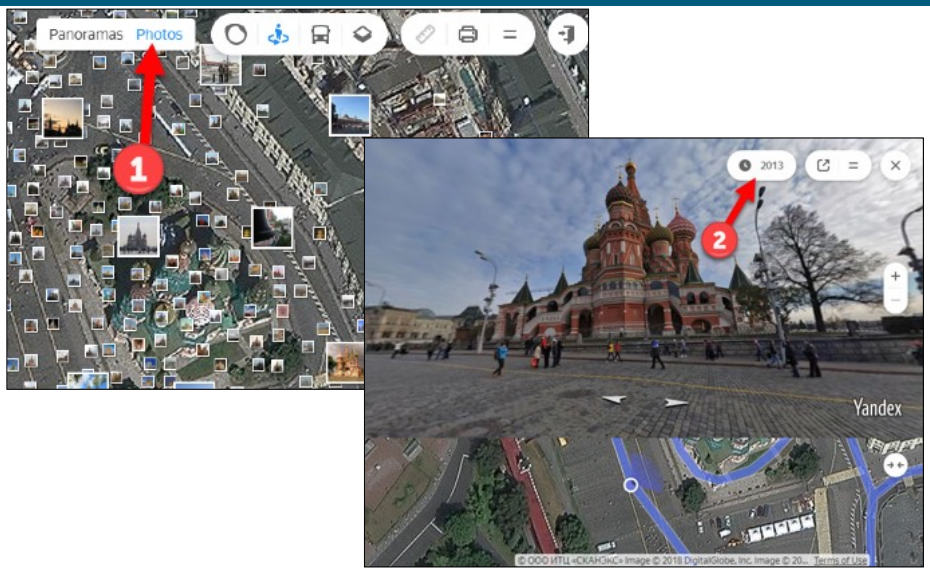
[1] https://sec487.info/6j, August 26, 2017.

Yandex Street Panoramas and Photos

Fewer places have imagery

Has crowd-sourced photos similar to Google

Historic imagery may be available



Yandex Street Panoramas and Photos

Using camera-mounted vehicles, Yandex has street panoramas that cover many European and Asian cities. Yandex ground-based imagery is focused on cities and connections between them, as can be seen in the zoomed-out map at https://sec487.info/6l, where only the major cities have blue areas that indicate street panoramas exist.

The quality of the images is quite good for the areas covered and, as shown in the image of Saint Basil's Cathedral above, Yandex may have historic imagery of the location you are observing (arrow 2). The image with arrow 1 above highlights the crowd-sourced photos that people have uploaded to Yandex and they have geolocated.

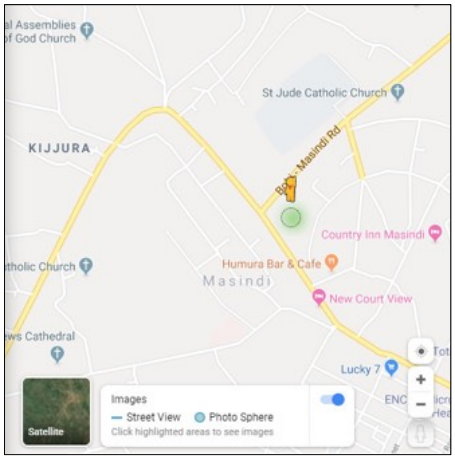
Image from https://sec487.info/67 and https://sec487.info/to, September 24, 2019.

Reference:

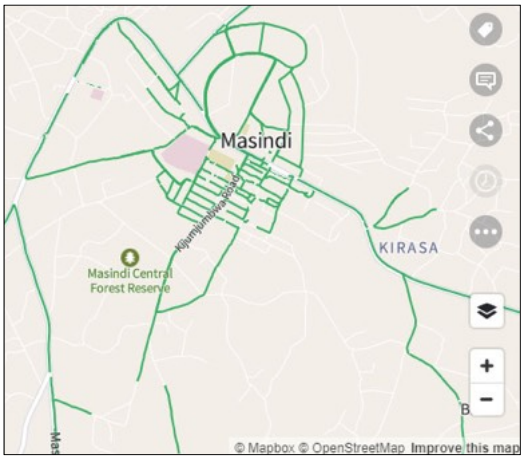
[1] https://sec487.info/6k, August 26, 2017.

Mapillary Crowd-Sourced Street Views

Google No Street View



Mapillary



Masindi in the western African region of Uganda

Mapillary Crowd-Sourced Street Views

Sometimes you need to see a place that Google, Bing, Yandex, and other mapping sites haven't visited to obtain imagery. Mapillary.com might be able to help. For example, in the above pictures we visited the small town of Masindi in the western African region of Uganda.[1] The Google image shows no Street View content to display using the yellow person icon, but the Mapillary shows it has many roads with imagery.

Mapillary (https://www.mapillary.com/) has mobile applications that people can load onto their devices to take their own street-level images. The application then uploads those to the site. As you can imagine, the images can range from high-quality to almost unusable ones. This does give you access to other views of our world and could help in your assessments.

Images from:

Google: https://sec487.info/6m, September 24, 2019.

Mapillary: https://sec487.info/6n, September 24, 2019.

Reference:

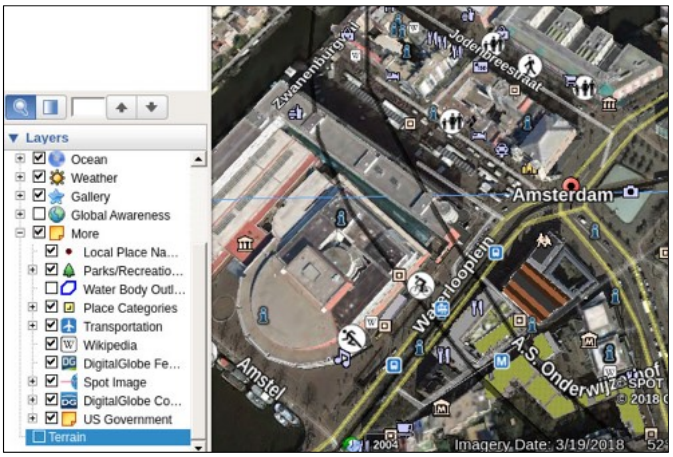
[1] https://sec487.info/n1, August 26, 2017.

Google Earth

Desktop, mobile, and web apps

Advantages:

- 3D perspectives
- Crowd-sourced images
- Aggregation of additional content from web sources
- Create a video to "fly over" a path of GPS points/landmarks



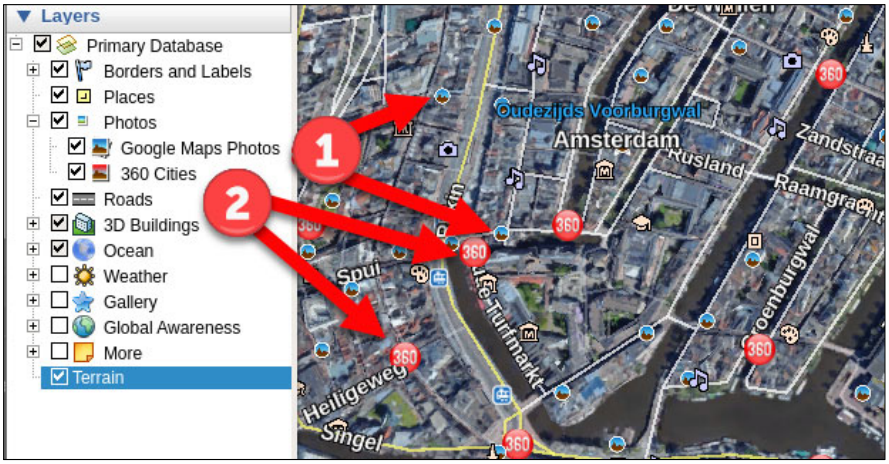
Google Earth

This powerhouse of an imagery and data aggregation tool is free and has a mobile app, a web app (https://sec487.info/mq) that requires the use of the Google Chrome browser, and desktop versions for Windows, macOS, and Linux computers. In addition to letting users explore satellite imagery from around the world, this application aggregates data from sources like Wikipedia, the United States government, DigitalGlobe, Greenpeace, and UNICEF. Each data point is platted in the application and can highlight places of interest, current weather patterns, transportation paths, hiking and biking paths, and so much more. We can also view crowd-sourced imagery in the application to see what a location looks like across time.

Google Earth can also be used to create your own maps and "fly-bys" by uploading a list of GPS points, or plotting them individually in the application. Once the GPS points are in the tool, you can measure distances to and from them, link them together and have Google Earth "fly" you through each point, and set up distinctive markers for each type of data point for easy viewing.

Google Earth Images

Crowd-sourced imagery like panoramas, regular photos, and 360-degree photo bubbles make Google Earth a geotagged-image aggregator



Google Earth Images

In addition to the satellite imagery that is the core of Google Earth, this tool pulls data and images from other sources and then plots them within the application. It can display both crowd-sourced (arrow 1 above) and professional (arrow 2 above) images and data, allowing the OSINT analyst to get different perspectives of a target location through the lens of multiple sources.

Google Earth Perspectives

Use Google Earth to match a video's or image's horizon (red line) with Google Earth terrain to find the rough position of the activity

Google Earth Perspectives

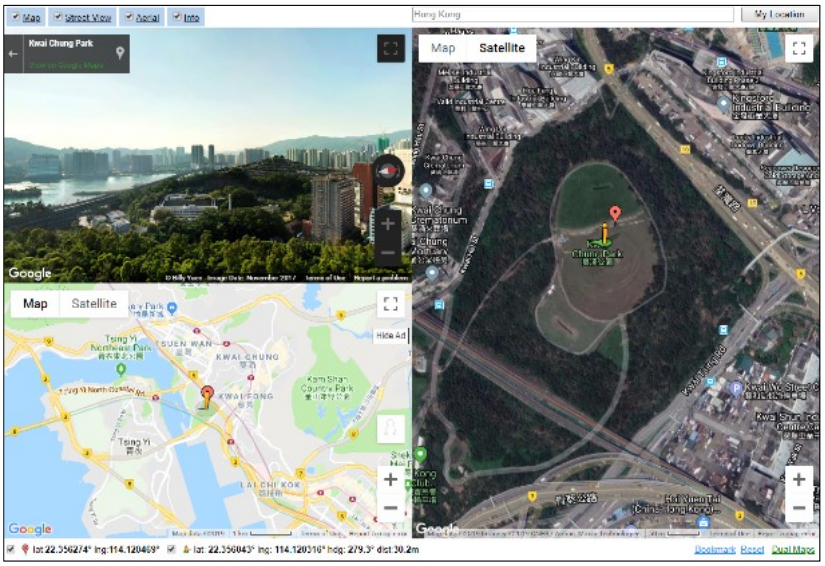
In the BBC's 2018 video showing their analysis of a public execution video, a group of soldiers are seen to take villagers, supposedly in Africa, to a location and then shoot them (https://sec487.info/ix). BBC's researchers used the mountain range in the background of several portions of the video to match it against the terrain they viewed in the Google Earth application. The above video is paused just before the red horizon line from the execution video was matched to the profile of the mountains viewed in Cameroon.

Zooming into and out of the imagery and changing the perspectives can be useful in urban environments as well, allowing the analyst to see what buildings and other features might be obscuring a road or viewing likely points where an ambush or attack may occur.

Putting It All Together

All three views of our mapping: normal road, satellite, and ground-based combined in one web site

Mashed World's Dual Maps syncs the map views so as one changes, the others do too



Putting It All Together

If you wish to display all three Google views (road, satellite, and Street View) together into a single mash-up application, then you'll want to use Mashedworld's dual maps site at https://sec487.info/ss. Enter a location, and it shows all three views at same time AND it allows you to move the maps in sync with the other views. Drag the Street View and the other maps move too!

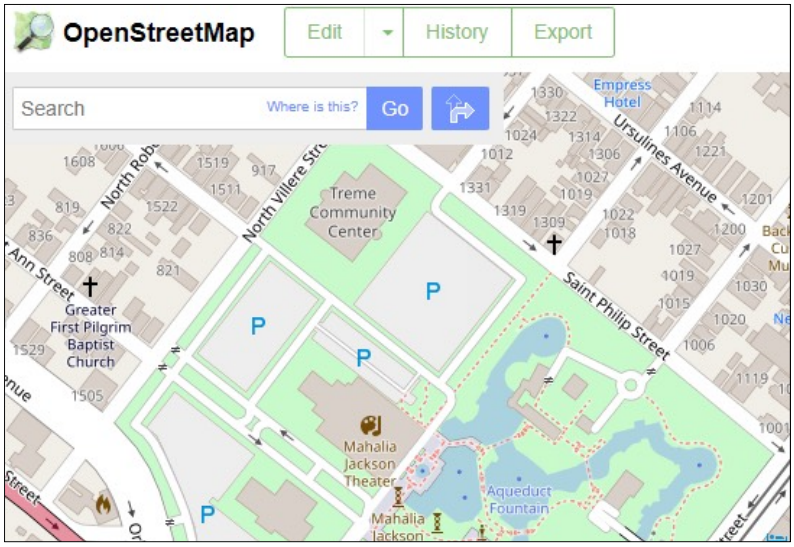
This image (https://sec487.info/ss, September 17, 2019) is in the Kwai Chung Park in Hong Kong (https://sec487.info/st).

OpenStreetMap No Satellite

https://www.openstreetmap.org

Features:

- Normal "Map" view
- No Satellite view
- No Distance measurement
- Has street and building numbers



OpenStreetMap No Satellite

Our last mapping site is OpenStreetMap.org, which "is built by a community of mappers that contribute and maintain data about roads, trails, cafés, railway stations, and much more, all over the world."[1] The community helps trace roads and buildings and define regions on the maps. You can help, too!

OpenStreetMap does not have its own satellite imagery and does not display satellite data in its maps. But it does have a different display and sometimes a more easy-to-read map than some of the others mentioned. For instance, if you are looking to display house or building numbers in a 2D map, OpenStreetMap can do that.

Image from https://sec487.info/65, September 24, 2019.

Reference:

[1] https://sec487.info/n2, August 25, 2017.

Wikimapia.org

http://wikimapia.org

Features:

- "Open-content, collaborative map" [1]
- Anyone can create regions and label them
- Map and Sat views
- Distance

Wikimapia.org

Wikimapia.org focuses on having its users outline regions of its maps. What are these regions? It depends on what users want to note. Some regions are cities, towns, neighborhoods, or local areas known by names other than their what appears on other official maps. Other regions are buildings such as schools, religious buildings, or government areas. As shown in the image above, arrow 1 points to the region (in yellow) that has been tagged as "South Beach Lifestyle Quarter". We found this region by moving our mouse over the map. The information on this web site should be corroborated and verified prior to use because anyone can create and name regions.

Image from https://sec487.info/6z, September 24, 2019.

Reference:

[1] https://sec487.info/n3, August 28, 2017.

Other Purposes for Mapping Apps

Mapping web applications can assist our OSINT work by:

- Measuring distances between objects/locations
- Helping us validate metadata, images, and videos
- Allowing us to go back in time and view a location across multiple months or years

Let's look into each of these aspects a bit more.

Other Purposes for Mapping Apps

We have already seen how mapping web applications helps our OSINT investigations by showing us roads and trees and buildings and street views. But there are other features within these applications that we can use to make our OSINT lives easier. These include measuring distances, validating metadata, and showing us locations across months or years.

Measuring Distances in Online Maps

There will come a time when you need to measure between points on the map. It is simple.

Google: Right-click on map. Look for "Measure Distance"

Bing: Right-click on map. Look for 

Yandex: Look for the ruler icon on screen 

Measuring Distances in Online Maps

In your investigations, you will want to know how far it is from one location in a map to another. Whether those locations are buildings, widths of rivers, lengths of hiking trails, or routes taken by your target, Bing, Yandex, and Google have mapping tools to assist.

In the slide above, we show the methods that you can use to bring up the mapping tools within a mapping web application. While the techniques vary, each is used in a similar fashion. Click where you wish to start. Then click each point along a path to create waypoints that can be moved and deleted later. As you make more points on the map, the distance "travelled" grows and is displayed on the map.

Google Maps Distance Measurement Example (1)

We received a tip that a gang in Mexico is going to use a drone to drop contraband into the San Luis, Arizona State Prison

We have been asked to verify it

Go to the location in Google Maps and right-click to see the "Measure Distance" option

Google Maps Distance Measurement Example (1)

Here is a fictional example of how an OSINT person may use the "measure distance" features of mapping sites in their work. Our example begins when we received a tip that gang members in Las Adelitas, Sonora, Mexico are going to try to use a DJI quadcopter drone to air-lift contraband to their members inside the Arizona Prison Complex in San Luis, Arizona.

We visit the Google Maps page for the prison (https://sec487.info/ms) and right-click to bring up the context menu at our starting location at the basketball court of one of the prison exercise yards. Selecting the "Measure distance" option, we begin.

Image from https://sec487.info/ms, January 3, 2019.

Google Maps Distance Measurement Example (2)

We drag the map south to reveal the possible location in Mexico where the gang may launch the drone and we click the mouse

This reveals the distance of approximately 4.55 km or 2.83 mi direct

Next, let's find drones that can fly ~9km (round trip)

Google Maps Distance Measurement Example (2)

Dragging the map south, we find a probable location where the gang may launch the drone and then we click the map once. Google's application notes the distance at the bottom of the screen in kilometers and miles. In this case, it is about 4.55 km or 2.83 miles from the town to the prison.

We continue with our analysis and pivot to the question of whether there are any consumer drones that can fly about 9 km (4.55 each way).

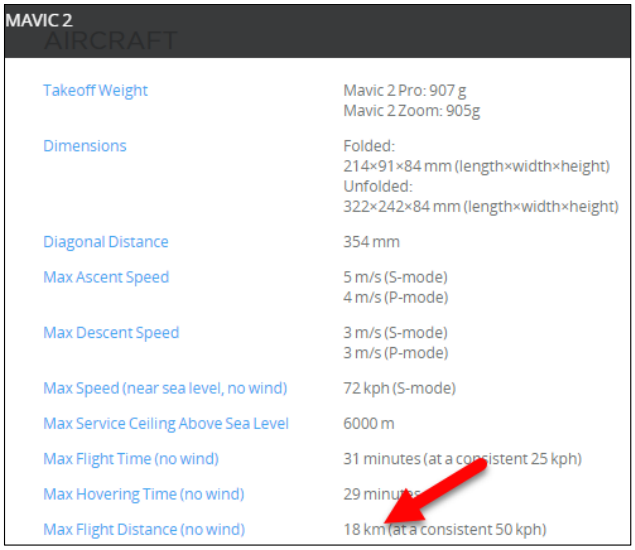
Image from https://sec487.info/mt, January 3, 2019.

Google Maps Distance Measurement Example (3)

A web search of long-range drones shows the DJI Mavic 2

According to its specs, it can fly 18 km with no wind

Is the tip we received plausible?



MAVIC 2

AIRCRAFT

Takeoff Weight	Mavic 2 Pro: 907 g Mavic 2 Zoom: 905g
Dimensions	Folded: 214×91×84 mm (length×width×height) Unfolded: 322×242×84 mm (length×width×height)
Diagonal Distance	354 mm
Max Ascent Speed	5 m/s (S-mode) 4 m/s (P-mode)
Max Descent Speed	3 m/s (S-mode) 3 m/s (P-mode)
Max Speed (near sea level, no wind)	72 kph (S-mode)
Max Service Ceiling Above Sea Level	6000 m
Max Flight Time (no wind)	31 minutes (at a consistent 25 kph)
Max Hovering Time (no wind)	29 minutes
Max Flight Distance (no wind)	18 km (at a consistent 50 kph)

Google Maps Distance Measurement Example (3)

Doing some quick search queries (https://sec487.info/tp), we find a site that ranks the longest-flying drones in 2019 and shows that the DJI Mavic 2 could fly 18 km. Confirming this by visiting the DJI web site and looking at the specifications of the drone reveal that to be true (https://sec487.info/tq). Carrying contraband will decrease that distance (due to battery drain).

So, based upon this simple search, we may flag this activity as possible.

Image from https://sec487.info/tp, September 24, 2019.

Going Back in Time

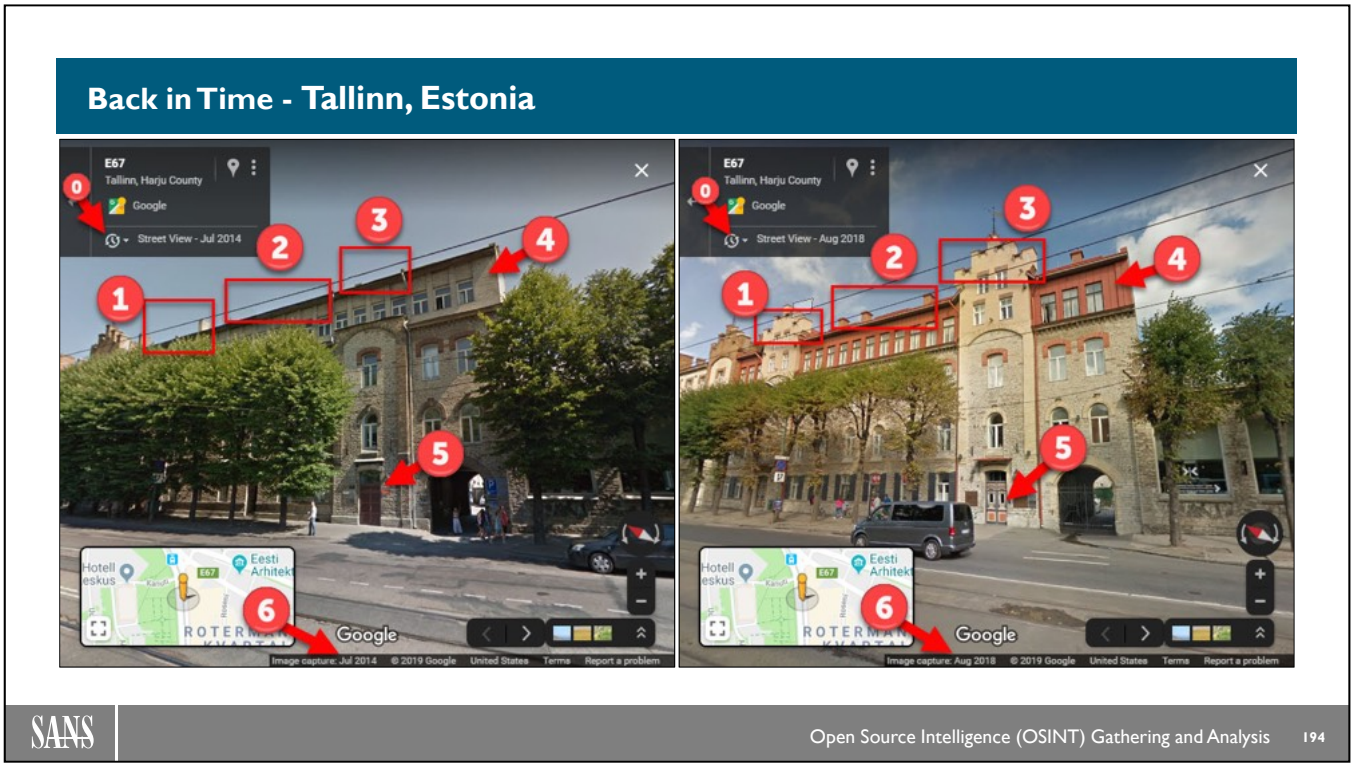
Imagery can be used to examine an area across different time points

Remember from earlier that Google's Street View allows us to select what images we wish to see (arrow 4)

Going Back in Time

Google's Street View application allows users to select what imagery they wish to view if there are multiple versions from different time periods. It defaults to the most-recent images, but users can select the clock icon (arrow 4) and pick a different series of images to view.

This can allow OSINT analysts to examine a location over time. Many well-populated or popular areas have many Street View images that we can browse. Let's go back in time and watch a construction project.



Back in Time - Tallinn, Estonia

Using the Google Street View mapping application, we visit Tallinn, Estonia (https://sec487.info/su). In July 2014, it looked as it appears in the left image above. Click the clock icon (0 in the pictures) and a menu drops down that shows other dates where Google has imagery of this site. For this picture, choosing the August 2018 imagery (shown on the right above), shows a different view of the location.

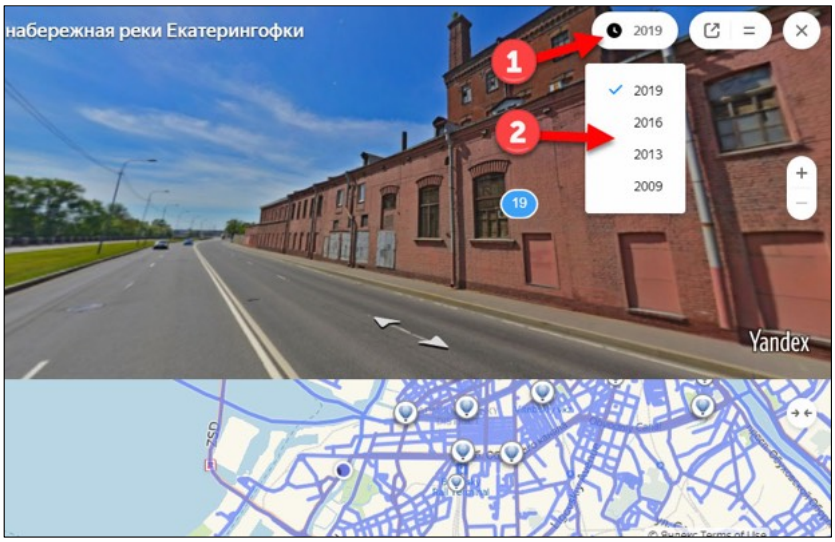
We've highlighted 5 differences in the above images. Can you find more? Head over to https://sec487.info/su for the online versions of these images.

Images from https://sec487.info/su, September 17, 2019.

Yandex Imagery Going Back in Time

Yandex also has historical Street Panorama imagery

Press the clock icon (arrow 1) and then select the date (arrow 2)



Yandex Imagery Going Back in Time

Yandex has a similar feature to Google's Street View where you can view historical imagery from its Street Panoramas. The above slide shows this imagery and how to access it.

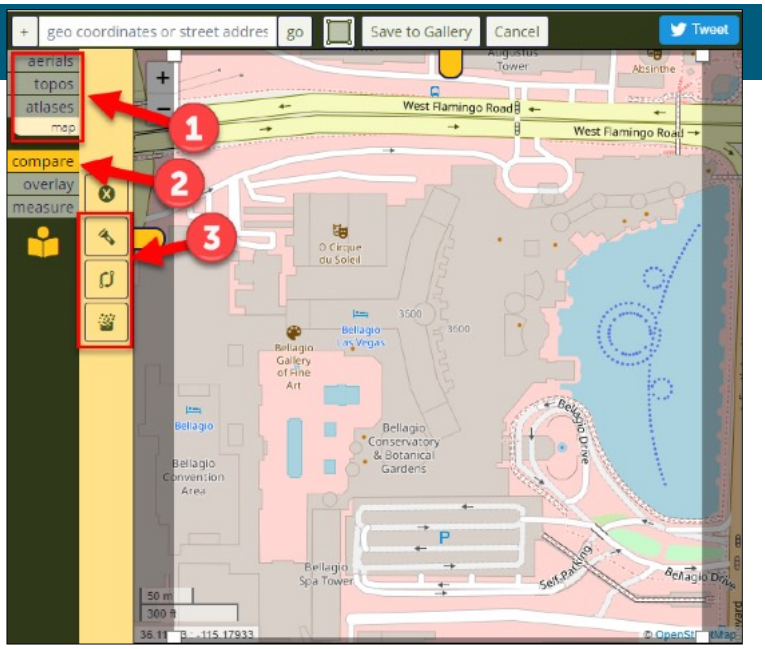
Image from https://sec487.info/tn, September 24, 2019.

Historic Aerials

Historic aerial imagery for the USA

Select from a variety of years for aerial imagery and topographic maps (1)

Compare (arrows 2 & 3) imagery across years



Historic Aerials

Sometimes the name of the web site is extremely descriptive to what the site shows. If you are looking for historic aerial imagery for places in the United States, then Historic Aerials (https://sec487.info/6x) may have what you need.

This easy-to-use web site is mainly focused on displaying imagery and topographic maps of the United States. Enter the place you would like to view in the search field. Once it finds the location, you can then select imagery from different years from the left side of the window (arrow 1). Above we see the map view of the Bellagio Hotel and Casino in Paradise (Las Vegas), Nevada.

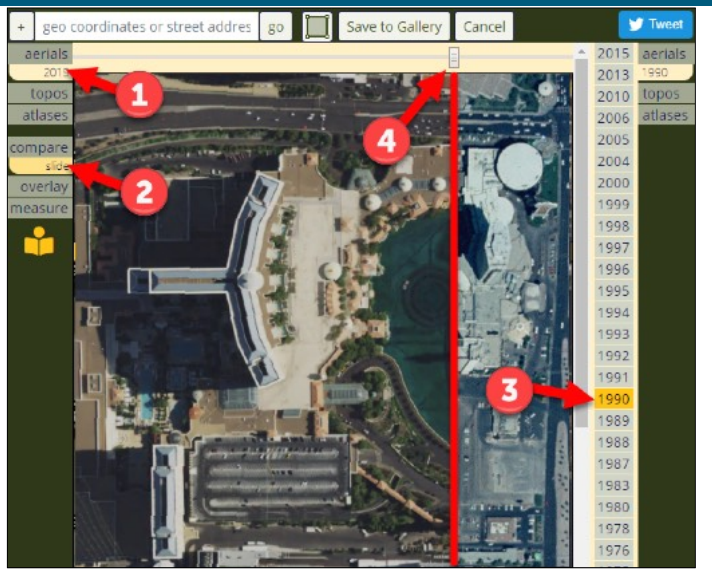
The real power in this site comes in the "compare" tool on the left of the window (arrows 2 and 3). These tools allow you to select two different sets of imagery and fade between them by moving the mouse over one and to view portions of the other behind it (Spot Light) or by moving a slider across the image and displaying part of one image and part of the other (side by side).

Image from https://sec487.info/6x, September 17, 2019.

Bellagio Casino: 1990 versus 2015 Imagery

Using the "compare" tool (arrow 2) we can select the base imagery from 2015 (arrow 1)

Then we select the other imagery (3) and move the slider (4) to reveal the differences in the maps



Bellagio Casino: 1990 versus 2015 Imagery

The compare tools on the historicaerials.com web site help us understand what physical features were in a certain place at a specific time by letting us overlay one map over another. The compare tools (arrow 2) determine how we reveal those maps. In the image above, we selected the side-by-side display.

In the base image on the left (arrow 1), we see the 2015 aerial imagery of where the Bellagio casino and its famous fountains[1] were built. Arrow 3 points to the 1990 aerial imagery selection for the contrasting map. Using the slider (arrow 4), we can reveal different portions of the 2015 or 1990 imagery to understand how the area looked. Please note that we highlighted the seam between these imagery maps using a red line to make it viewable by the reader.

Images from https://sec487.info/6x, September 17, 2019.

Reference: [1] https://sec487.info/6y, August 28, 2017.

Image Analysis: Camera Position

Need to re-create the location and angle an image was taken?

IPVM's site uses Google's photo spheres and Street View imagery

10,000+ different camera models

https://calculator.ipvm.com

Image Analysis: Camera Position

We can re-create camera angles using the https://calculator.ipvm.com web site. We choose a location (arrow 1) and then add a camera to the map (arrow 2). Move the camera to the potential location of the image (arrow 3) and then change the direction by moving the "person" (arrow 4). What shows on the right side of the page (arrow 6) is a view of what a photo taken from that location might look like by using Google's Street View and Photo Spheres for the imagery. Above, we chose a location in Menton, France (https://sec487.info/us), placed and positioned the camera, and saw what the image might look like using a generic camera.

Users can pick from over 10,000 different models of cameras, and the web site will customize the simulated view according to the selected camera's field of view (FOV) and focal length (arrow 5). This helps to reproduce imagery that might come from security cameras, web cams, and traffic/dash cameras.

Image from https://calculator.ipvm.com/, September 28, 2019.

Image Shadow Analysis (1)

In analyzing imagery, we can use the sun's position to determine times

In the image, arrow 1 points to 3 bollards and a poll with shadows

Arrow 2 shows the date of the imagery

What time the image was taken?

Image Shadow Analysis 1

In some imagery, videos, and photos, we can see shadows caused by the sun. When we analyze these shadows and localize them to a specific place, we can many times determine a date and time range for the image. Let's look at an example from the Israel National Trail in Tel Aviv-Yafo, Israel (https://sec487.info/o5).

An excerpt from the mapping site's data is shown above, where we can see 3 bollards in the middle of the trail and a pole on the left (arrows at 1). Each has a shadow pointing to the right (indicating the sun is on the left). Arrow 2 in this image points to the date of the imagery, June 2015. Arrow 3 shows the direction that the image was taken. The red portion of this compass rose is pointing down or behind the photo-taker, meaning that that direction is north and we are looking south.

Can we figure out the time the Google Street View imagery was recorded?

Image from https://sec487.info/o5, September 23, 2019.

Image Shadow Analysis (2)

Let's walk forward on the trail and put ourselves inline with the shadow of the post

We see arrow 1 shows we are looking almost due east

Line 2 intersects with buildings (3)

Image Shadow Analysis 2

Move forward in Google Street View to put your view in line with the shadow and the post (https://sec487.info/o6). Now we can see that the compass (arrow 1 above) shows we are looking almost due east. This means that the imagery was taken in the morning. Now draw a line connecting the shadow, pole, and going off into the distance (2 above), and you will see the line intersect a long, wide building and then some other buildings in the distance.

Image from https://sec487.info/o6, January 4, 2019.

Image Shadow Analysis (3)

Zooming in on the Street View shows that there are buildings in the distance (2)

Let's move to aerial imagery and see if we can find these landmarks

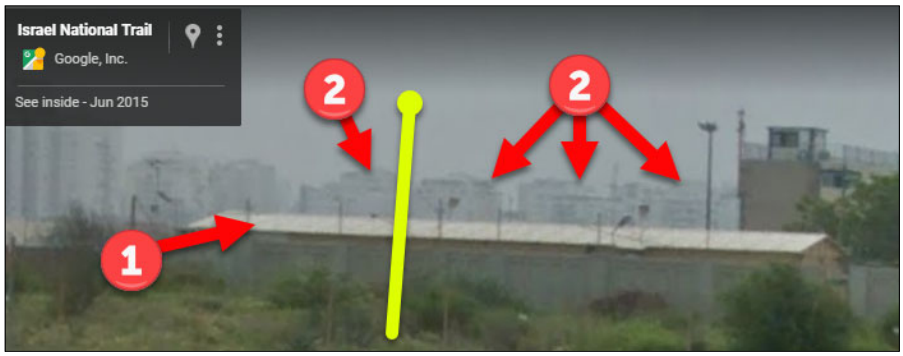


Image Shadow Analysis (3)

Zooming in in the Street View image (https://sec487.info/o7), we can see that the yellow line of our shadow bisects a long building and heads off towards other buildings in the distance (arrows marked 2 above). Now we move off to the satellite view and see if we can find these landmarks.

Image from https://sec487.info/o7, January 4, 2019.

Image Shadow Analysis (4)

Changing to the satellite view

We see our point (1) and the line of the shadow intersects a long rectangular building (2)

Now let's zoom out more and extend the line to find those distant buildings

Image Shadow Analysis (4)

Our image location was 32.1068222,34.7767925. Our aerial, satellite imagery (https://sec487.info/o8) shows our image location (arrow 1) and a long building to the east (rectangle 2). Our shadow line can now be extended to find those buildings in the distance.

Image from https://sec487.info/o8, January 4, 2019.

Image Shadow Analysis (5)

Zooming out and extending our shadow line shows it intersects the long building (1) and other buildings (2)

Image Shadow Analysis 5

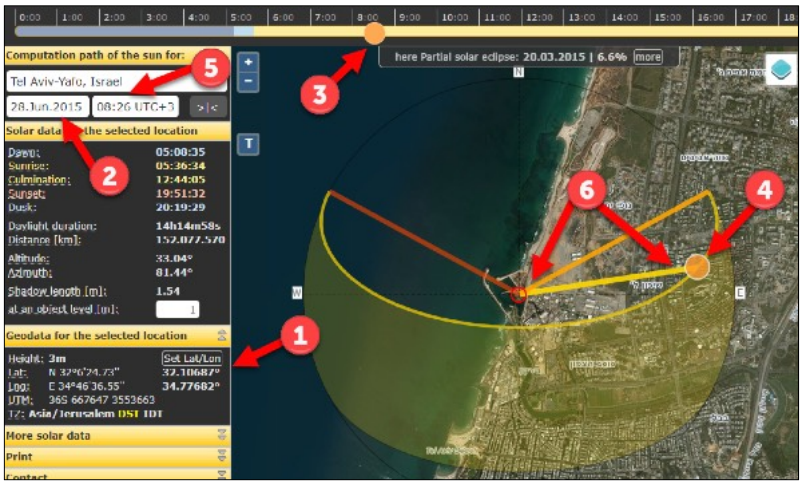
We zoom out on the map and extend the yellow shadow line so that it intersects the long building (1) and some other buildings (2) in the distance. These look like the buildings we saw from the Street View.

Image from https://sec487.info/o9, January 4, 2019.

Suncalc.org

Brief "how-to":

1. Set GPS coordinates
2. Set date
3. Sun slider at top changes sun at arrow 4
4. Read time at arrow 5
5. Our identified buildings are at arrows 6



Suncalc.org

One of the best sun calculation sites on the internet today is suncalc.org. Using this web site (https://sec487.info/ob), we can set the GPS coordinates (arrow 1), date (arrow 2), and move the time slider at arrow 3 on the top to reposition the sun (arrow 4) to simulate where the sun would be in the sky. Then we look at the times (arrow 5) and have our estimate. We see that the buildings we identified rest along the path of the sun (arrows at 6).

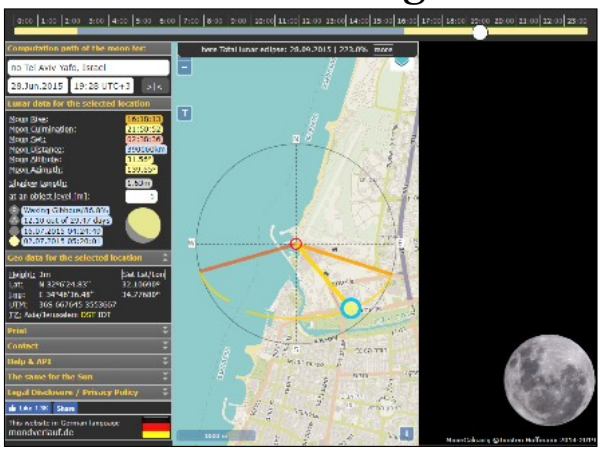
Our best estimation is that the imagery was taken on June 28, 2015 around 08:25 UTC +3.

Image from https://sec487.info/ob, January 4, 2019.

Similar Calculation Sites

andrewmarsh.com

mooncalc.org



Similar Calculation Sites

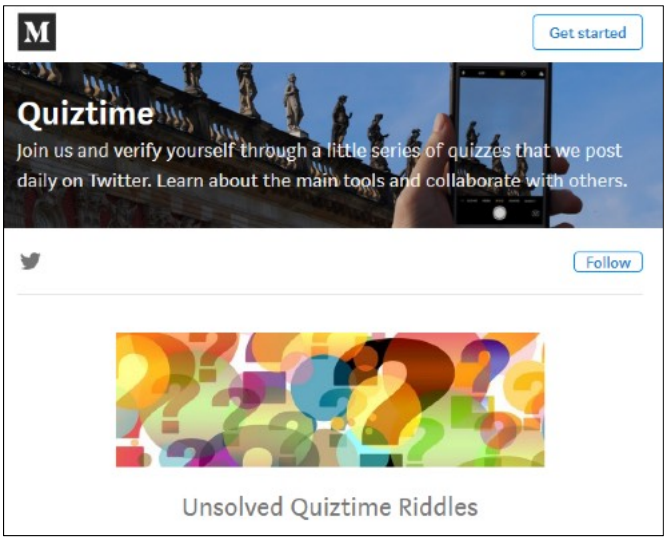
While suncalc.org is one of the best web sites for sun location and chronolocation, it is not the only site. Andrew Marsh's website at https://sec487.info/s- and the Moon calculation web site at https://sec487.info/t0 both offer additional methods to use for finding the times and dates of images and videos using sun and moon positioning.

Nathan Ruser has an interesting Twitter thread at https://sec487.info/t1 where he uses these and other techniques to locate and chronolocate (get the time of) events happening in Xinjiang, China.

Imagery Analysis Practice and Tips

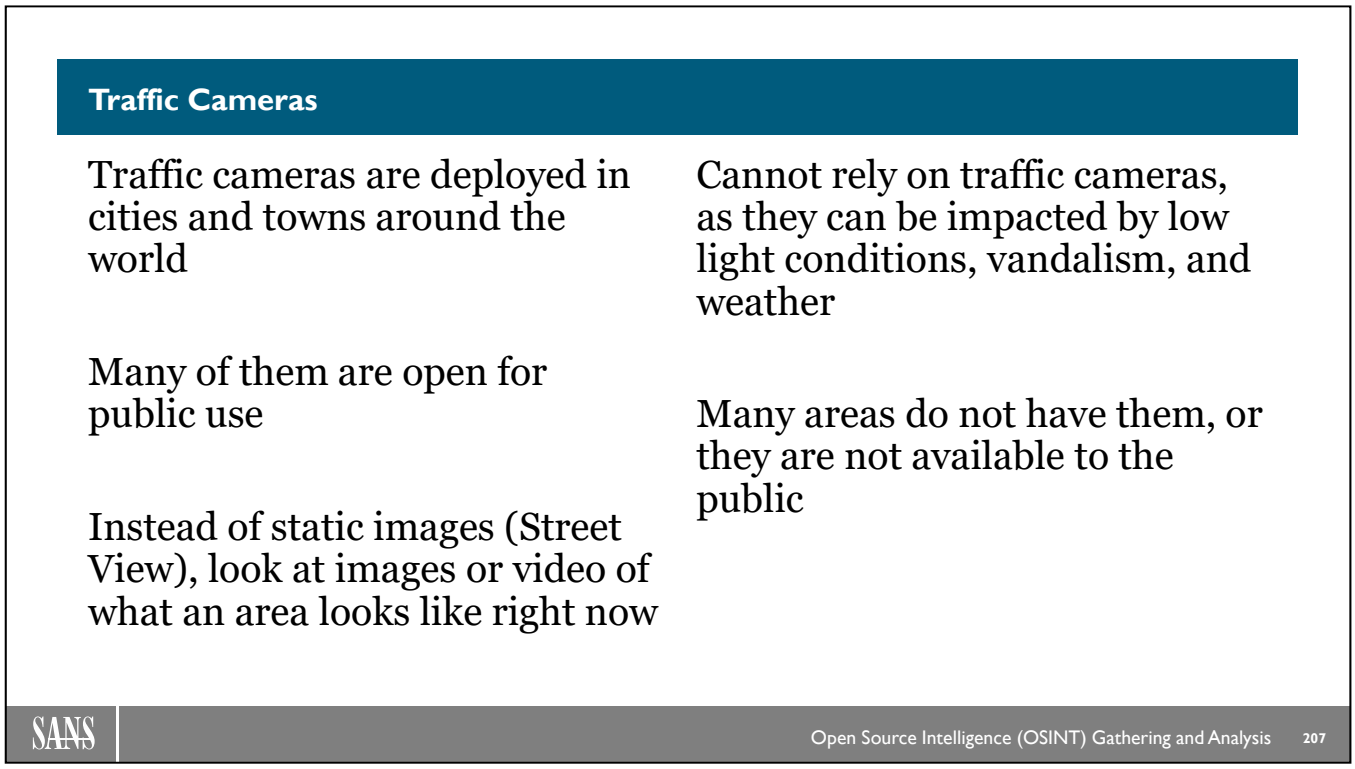
For the preceding example, the talented "Sector035," a wizard at this type of analysis, helped a bunch

He made a blog post about this example and has many other challenges and explanations in the "Quiztime" *Medium* publication



Imagery Analysis Practice and Tips

Having talented friends who you can ask for help is always a good idea when you want reliable answers. For the previous example, I worked with Sector035 (https://sec487.info/od), who is truly an expert image analyst. He contributes to an excellent *Medium* publication named "Quiztime" (https://sec487.info/oc), where this example (https://sec487.info/oe) and others are posted for you to practice with and learn from.



Traffic Cameras

In the past decade, there has been an explosion in real-time information that people on the internet can access. Many cities and countries have decided to place cameras along roadways so that they can view the current state of the vehicle traffic. In some of these locations, the video feeds (or still images that are refreshed) are published to the internet and accessible by the public.

We use these cameras to better understand what the "now state" of a location might be. Instead of using the street-viewing mapping applications to see what a location looked like when a car or bike with a camera took a picture, we can use these live cameras to see what that place looks like now.

There are numerous cases[1] where law enforcement has used traffic or red light cameras to solve crimes. OSINT analysts can use them to examine current weather conditions, watch for a missing vehicle, and examine what an area looks like. Keep in mind that traffic cameras are subject to weather conditions, low-light issues, and vandalism and may not be working even if they are deployed in the target area you are going to be examining.

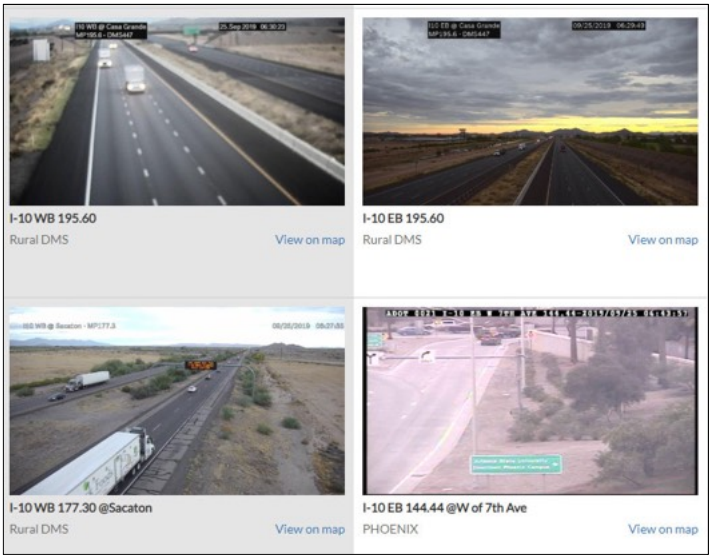
Reference:

[1] https://sec487.info/6t, August 26, 2017.

United States Traffic Cameras

Many state and local departments of transportation make their cameras available to the public

Use a search engine and look for your city, town, county, or state and the string "traffic cam"



United States Traffic Cameras

Within the United States, there are a number of sites that allow the public to use traffic cameras that are installed along many of the roads that you may need to examine. As OSINT analysts, we can use these cameras to help us remotely view an area, watch for traffic patterns at specific times of the day, or even search for a specific vehicle traveling on the road.

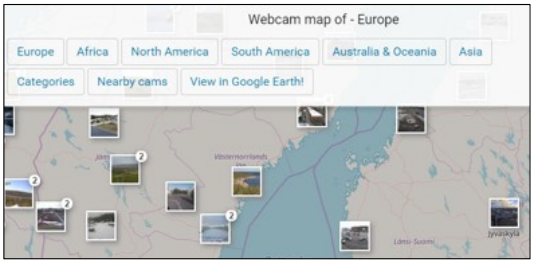
Use your favorite search engine or visit the state or local Department of Transportation or Motor Vehicle Administration to find cameras. Above, we pulled pictures from Arizona's traffic cameras on September 25, 2019. Their cameras take still images and refresh them after a certain number of seconds.

Image from https://sec487.info/tr, September 25, 2019.

WorldCam.eu Webcams

Well-organized site with webcams from around the world

Redirects to the page controlling/viewing the camera



WorldCam Webcams

The WorldCam.eu web site has many webcams that are organized by region and country. There is also a map where the webcams are displayed at their appropriate geographic location. The site is merely a catalog of the cameras and is not hosting or streaming the web content. Clicking a camera page redirects you to the camera's hosting page, where you may have controls to pan, tilt, and zoom the camera or see other cameras that are at the same location.

Images from https://sec487.info/nz and https://sec487.info/o0, January 3, 2019.

Insecam.com

"The world biggest directory of online surveillance security cameras. Select a country to watch live street, traffic, parking, office, road, beach, earth online webcams."[1]

GPS-located cameras

Streaming images

Insecam.com

If you are looking for cameras in a specific location in the world, consider using the Insecam.com web site. Each camera is geolocated and further sorted by make and model of the camera itself. There are streaming images from around the world: inside coffee shops and bars, road cameras, cameras focused on storage areas, beach and pool cameras, and so much more.

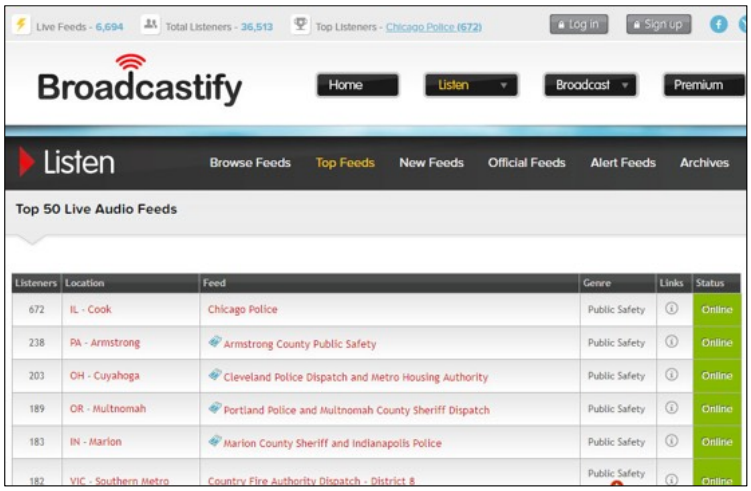
Image from https://sec487.info/n8, March 28, 2018.

Reference: [1] http://www.insecam.org/, March 27, 2018.

Remote Recon of Airwaves

Using radio-to-internet "bridges," we can listen to police, fire, medical services, and amateur radios around the world from our computers

The Broadcastify.com web site is an excellent world-wide resource for streaming these radio feeds to your web browser



Remote Recon of Airwaves

Before we leave the remote reconnaissance section, let us remember that we now have the ability to listen to radio frequencies through our web browsers. Using sites like https://www.broadcastify.com (https://sec487.info/o4) and https://streema.com, we can "tune in" to police, emergency services, amateur radio, and music/news radio stations via our web browsers. While these sites have some coverage internationally in over 20 countries, the vast majority of data is streamed from locations in the United States.

Why would we want to use these services for OSINT? They can be useful in the event of emergency, natural disaster, riots and protests, or just to better understand what is happening in another part of the world.

SEC487 Workbook

Please visit the course electronic workbook in the 487 virtual machine and begin the exercise named:

"Aerial Adventures"

This page intentionally left blank.

SEC487 Day 3 Summary

Today was about social media and imagery.

We explored several social media sites, geolocated data, and imagery and mapping issues.

Tomorrow we will examine IP addresses and DNS data, government data, and business OSINT.

This page intentionally left blank.