

# HANDBOOK FOR SOCIAL MEDIA INVESTIGATIONS

A collage of various social media icons arranged in a cluster. The icons include LinkedIn, YouTube, Facebook, WhatsApp, Twitter, Pinterest, and others, all set against a dark background. The icons are in different colors and sizes, creating a dynamic and overlapping composition.

# Table of Content

- 1. About Social Media Intelligence (SOCMINT)** . . . . . 1
  - What is SOCMINT? . . . . . 1
  - SOCMINT vs. OSINT . . . . . 1
  - SOCMINT Concepts and Terms. . . . . 2
  - Uses for SOCMINT . . . . . 3
  - SOCMINT Challenges . . . . . 3
  - Summary. . . . . 4
- 2. About Social Media Investigations** . . . . . 5
  - What Can Be Found Using Social Medias. . . . . 5
  - How To Find A Profile To Investigate. . . . . 6
  - What Can Be Automatized And What Is For You To Verify. . . 7
  - Are You Investigating The Right Profile? . . . . . 8
  - How To Access The Information On A Profile? . . . . . 8
- 3. Setting Up Maltego.** . . . . .10
- 4. Top Hub Items for Social Media Investigations.** . . .11
  - Main Data Integrations for Personal Identifiers and Social Media . . . . .11
  - Main Data Integrations for Company Data . . . . .11
  - Supplementary Data Integrations . . . . .12
- 5. Workflow: Starting with A Name.** . . . . .13
  - Pipl . . . . .13
  - Maltego Standard Transforms . . . . .14
- 6. Workflow: Starting with An Alias.** . . . . .16
  - Pipl . . . . .16
  - ShadowDragon SocialNet . . . . .17
- 7. Workflow: Starting with An Email Address** . . . . .19
  - Pipl . . . . .19
  - ShadowDragon SocialNet . . . . .20
  - Have I Been Pwned? . . . . .21
  - Maltego Standard Transforms . . . . .21
- 8. Workflow: Starting with A Phone Number** . . . . .22
  - ShadowDragon SocialNet . . . . .22
  - Social Links . . . . .23
  - Pipl . . . . .23

- 9. Workflow: Starting with An Image . . . . .24
  - ShadowDragon SocialNet . . . . .24
  - Social Links . . . . .24
- 10. Workflow: Starting with An Address or Location .26
  - OpenCorporates. . . . .26
  - OCCRP Aleph . . . . .26
  - Pipl . . . . .27
  - ShadowDragon SocialNet . . . . .27
  - Social Links . . . . .27
- 11. Example Maltego Use Cases. . . . .29
- 12. Useful Resources . . . . .29
- About Maltego . . . . .30



# 1. About Social Media Intelligence (SOCMINT)

## What is SOCMINT?

Social Media Intelligence (SOCMINT) is considered to be a sub-discipline of Open Source Intelligence (OSINT). SOCMINT can be defined as the techniques, technologies, and tools that allow for the collection and analysis of information from social media platforms. SOCMINT can be harnessed by government or non-state actors, such as private intelligence agencies or marketing companies, in order to gain knowledge about specific individuals, groups, events, or any number of other targets. While SOCMINT is generally considered to fall under the category of OSINT, there are some key differences worth noting.

## SOCMINT vs. OSINT









SOCMINT is not as straightforward as OSINT because there is a belief, particularly by users and privacy advocates, that there is some expectation of privacy when using a social media platform. While OSINT investigators may not agree with this expectation, there is another aspect of SOCMINT worth considering. OSINT investigations focus solely on information that is available publicly, but SOCMINT can also use information found on social media platforms that was intended only for a specific audience. For instance, the lines can be blurred if an investigator must join a private group or create a fake account in order to gain access to information provided by a person of interest. These situations make SOCMINT more difficult to navigate for those engaging in these investigations, and every effort should be made in order to comply with laws, regulations, and policies around intelligence gathering and investigations.

In these investigations, government investigators will likely go through the court system to gain warrants or permits to gain the information directly from the social media platform, but often, some SOCMINT techniques will have already been employed to gather the data used to support the issuing of those documents.

There are many nuances in the field of SOCMINT, including the type of information that can be gathered and the type of platforms that can be used to gain information.

First, it is important to understand that SOCMINT includes all social media platforms, not only social networking sites. Social networking sites, like Facebook and LinkedIn, only make up one portion of the platforms that can be used to gather data. Information can be found on media-sharing sites like Instagram, forums like Reddit, image-sharing sites like Pinterest, video sharing sites like YouTube, microblogging platforms like Twitter, social gaming platforms like Xbox Live, and blogs created using platforms like WordPress.

## Information Sources of SOCMINT

								
Types	Social Networking Sites	Media-sharing Sites	Forums	Image-sharing	Video-sharing Sites	Microblogging Platforms	Social Gaming Platforms	Blogs
Examples	FACEBOOK, LINKEDIN	INSTAGRAM, IMGUR	REDDIT	PINTEREST	YOUTUBE, VIMEO	TWITTER, TUMBLR	XBOX LIVE	WORDPRESS, MYSPACE

Next, it is important to know the types of information that can be gathered from social media platforms. We can break this information down into three general categories:

- 1. Profile Information:** Static information provided about a specific user that is observable by those who access the profile. On LinkedIn, for instance, this might include a user’s job title, current and former employers, skills, and contact information.
- 2. Interactions:** Users on a social media platform can interact with the platform or other users in many ways. These forms of interaction include posting/commenting, replying to someone else’s content, posting pictures or videos, and liking or reacting to existing content.



**3. Metadata:** Information found on social media platforms is not limited to text and pictures. It can also include contextual information about said pieces of content. Metadata can include the location tagged in a post, the time that the post was made, or even the type of device used to take a picture.

## Uses for SOCMINT

SOCMINT is commonly associated with investigations on a group or individual involved in criminal activity, but that isn't the only scenario where it can be useful. Other types of investigations where SOCMINT could be employed include:

- Terrorism
- Organized Crime
- Human Trafficking
- Child Sexual Exploitation
- Disaster Prediction and Response
- Population Density
- Economic Analysis
- Health and Disease Monitoring
- Drug Use and Trends
- Cybercrime

While this is not an exhaustive list, it is meant to demonstrate that SOCMINT has many uses outside of those common to law enforcement. While state actors are prolific users of SOCMINT, private companies and organizations also use SOCMINT to collect information to better inform business decisions, improve marketing, ensure brand protection, and identify patterns and trends.

## SOCMINT Challenges

Though there is a wealth of information available through social media platforms, that does not mean that the use of SOCMINT is easy or simple. There are several challenges that face investigators who employ it.

**1. Number of Users:** Social media platforms like Facebook and Twitter boast billions of users each month. With the sheer amount of data available, it can be difficult to find the information relevant to a particular investigation.



**2. Identification of Users:** Many platforms operate with the intention of keeping their users' identities private, creating challenges for investigators. Additionally, the increased prevalence of fake accounts and bots on these platforms can make it extremely hard to figure out which data is accurate, available, and useful.

**3. Compromising Trust:** There have been an abundance of stories over the last few years about data leaks and user information being compromised, which can cause users to think twice before sharing information online. Additionally, as governments continue to employ SOCMINT techniques, they risk violating the privacy of their citizens, creating an unstable relationship between authorities and the people they serve and protect.

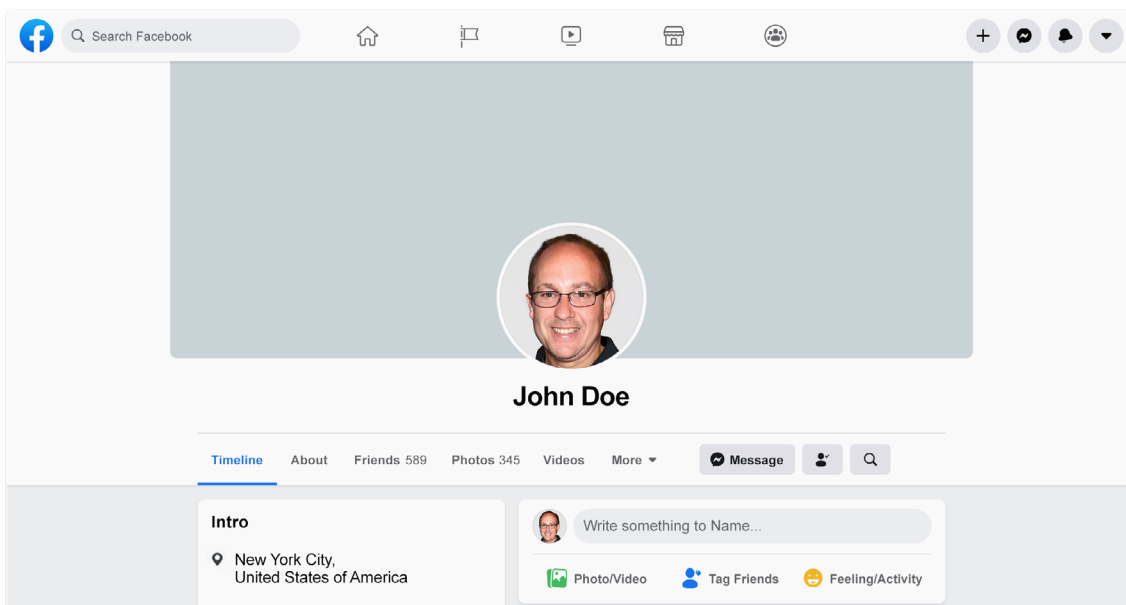
## Summary

Social Media Intelligence (SOCMINT) is a type of Open Source Intelligence (OSINT) that focuses on the collection and analysis of data from social media platforms. This information can be in the form of profile information, interactions with other users, or metadata that adds context to the shared content. SOCMINT is utilized by both government and non-state actors for a wide variety of investigations, but there are challenges that come along with these techniques and technologies. SOCMINT allows for the enhancement of investigations by using information that has been previously unavailable, but investigators must ensure that they are following laws, policies, regulations, and best practices to respect user privacy and human rights.



## 2. About Social Media Investigations

SixDegrees.com launched in 1997. It is often described as the first social media where users would have their real name, a list of friends, and personal information displayed on their profile. At its peak, it boasted more than 3.5 million users. Since then, other websites and apps have replaced it, and it's estimated that billions of people use social media nowadays. This means that for any given investigation, it is likely that some data or clues can be harvested from social media.



### What Can Be Found Using Social Media

What you can find on social media depends vastly on the individual or entity you're looking into, and on the platform itself. Some, like LinkedIn have by design a userbase wanting to be found and desiring to use their profile to display their professional experience. Others, like Twitter, have profiles that may be less informative but may provide more context in the contents of the posts made by an account. While the information on LinkedIn tends to be more curated because it's geared towards a professional environment, not everyone expects other people to pay attention to their tweets.





# How To Find A Profile To Investigate

The first thing to do when investigating someone on social media is to find the account that belongs to that person. This can be done in a number of different ways, but we can identify at least 6 pivot points that will help us find social media accounts belonging to an individual:

**Name:** The name of a person is a good starting point as it will often return a Facebook, Myspace or LinkedIn account. However, it is also the first personal identifier people will avoid using or disclosing if they do not want to be found.

**Email address and phone number:** These are great starting points because they're usually only shared between accounts, and thus, individuals, that are somehow connected. So, if two accounts on different platforms share the same phone number or email address it means there is a link between them. The problem with these data points is that they usually aren't easily searchable (Skype is a notable exception) and are not displayed on the profile of a person of interest.

**Alias:** The alias, also known as username or the pseudonym, is often reused across different social media platforms. The advantage of this data is that it is extremely easy to search: Any social media platform that has usernames allows you to search for users with a particular alias, as it is often a core concept of the platform—find people and befriend them. The main issue with this is that aliases are only as good as they are unique: One can assume that two accounts on different platform sharing a rather specific username such as *"LittleTroll15245"* are likely to be operated by the same person. But even then, one would need to investigate further to corroborate the link. If the account has a more generic username like *"BlueDragon"*, finding an account on another platform belonging to the same individual solely based on the alias might prove difficult.

**Profile pictures:** Profile pictures fall into the same kind of category as aliases, which means that with luck, doing a reverse image search from a picture found on a profile might just lead you to an account operated by the same person. However, it might . It can also be that two different people thought that a determined image would look good on their profile. Searching



accounts with a picture as a departing point is also much more difficult because you have to rely on reverse image search engines, which is usually not a feature supported by social media platforms. The only advantage of profile pictures is that not everyone is aware that they can be used as a pivot point. Thus, they tend to reuse them more often than aliases.

**Address and bio:** Addresses and bio might be the most difficult pivots to exploit. Seldom an individual will reveal their physical address on social media. Platforms that scrape online information such as Pipl are more likely to allow an investigator to pivot from that kind of information. On the other hand, bio should always be looked at carefully as some individuals link their social media accounts using their bio.

## What Can Be Automated And What Do You Need To Verify

There are two types of information that can be found on social media: Information that the user wants to share and information that the user forgot to hide—for a lack of concern for their privacy or because they didn't notice.

For example, to establish a connection between two people: One could check if they are friends on Facebook, which falls into the first type of information. One could also check the photo they posted on their Instagram accounts and by looking at the people, the background, and the date of the posts, deduce that they both were at the same house party. This falls into the second type of information.

The main difference between the two, from our point of view, is that the first type of information can be automated and thus obtained pretty easily: Jump into ShadowDragon SocialNet and pull the list of friends of both profiles. The friends in common will appear before your eyes. The second type of information, however, will often require an investigator to pay close attention to the -sometimes- extensive content displayed on a social media profile. There is not (yet) a one-click solution to this problem. This kind of information should not be pursued by default, as it is extremely time consuming.



Maltego and its SOCMINT data partners will usually focus on the first type of information.

## Are You Investigating The Right Profile?

The first thing you should do when conducting a social media investigation is to make sure you have the right profile. There are some platforms where, using your real name, displaying information about yourself, and having an actual photo of your face as a profile picture is the norm (e.g., LinkedIn). In this scenario, it is pretty easy to identify the profile related to a person of interest by cross-referencing data we already have. This type of profile is the one you will obtain when starting your search from a name.

However, starting your search from an alias might yield other kinds of profiles where there is less information available for you to establish the difference between an account that coincidentally happens to have the same alias used by the person of interest, and an account that belongs to said person of interest.

To properly draw conclusions, you can first check information such as the location or the other social media they link in their bio (if any). If there is no such information, looking at their posts and account followings might help. Are they posting about a particular topic that you know is connected to your person of interest? Are they following an account tied to a particular location like a local police department or a small town mayor? To verify these things, you can pull the list of post and followed accounts into your Maltego graph.

## How To Access The Information On A Profile?

Maltego and its data partners will provide you with Transforms to pull most of the data available on a profile directly into your graph. This will save you a great deal of time as you won't have to comb through the profile yourself which, depending on the platform, might require you to have an active account.

However, depending on the social media platform in question, the Transforms available in Maltego may not be able to retrieve



all the information available on the platform. If you want to deep-dive into a profile, you ought to take a look at it in the social media platform itself, from an app or from a web browser.

It should be noted that an investigator should never use a personal account to collect information. An account reserved for research purposes should be created to do so. Websites such as [this-person-does-not-exist.com](https://this-person-does-not-exist.com) can help you craft a realist profile. Be aware that some platforms tell their user when someone has seen their profile, as sn the case of LinkedIn.

In this handbook, we will show you 6 standard investigative workflows using Maltego and SOCMINT, pivoting from the following starting points:



NAME



ALIAS



EMAIL  
ADDRESS



PHONE  
NUMBER



IMAGE

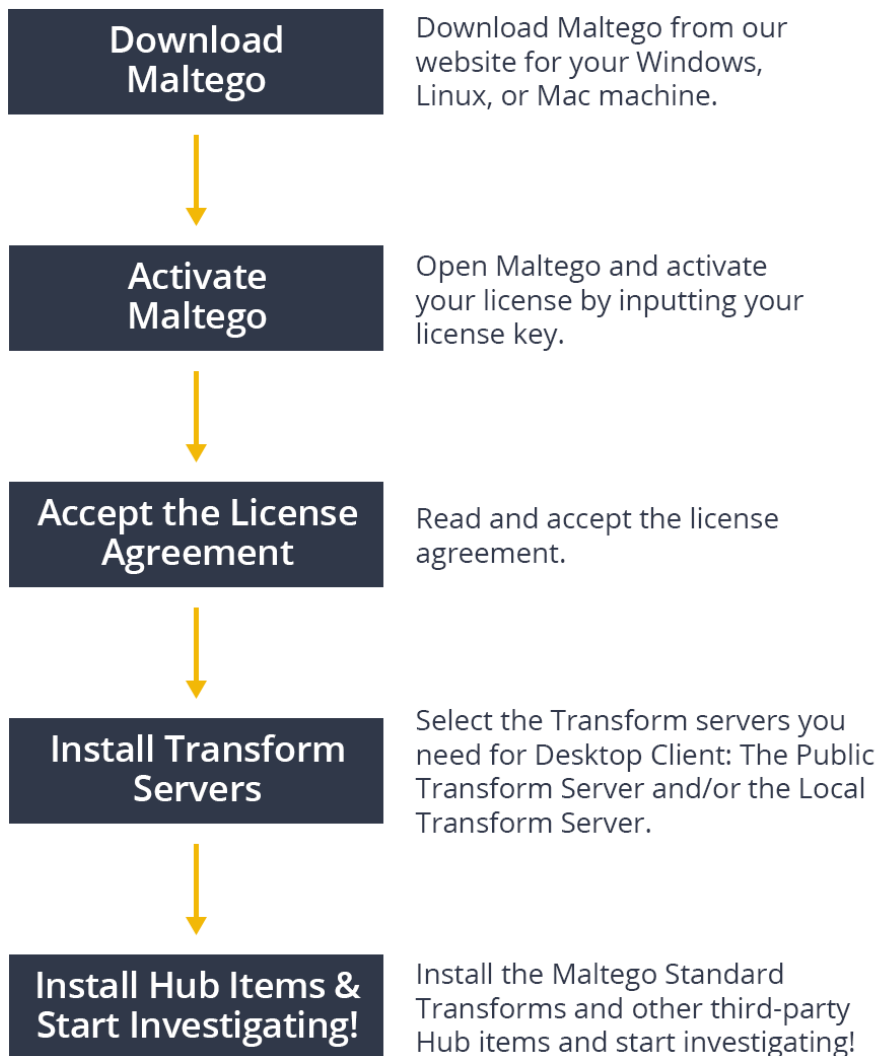


ADDRESS  
OR LOCATION

# 3. Setting Up Maltego



Set up your Maltego Desktop Client following the simple five steps below.





## 4. Top Hub Items for Social Media Investigations

Here is a list of high-quality data provider options for various SOCMINT and POI investigative scenarios that have proven to be amongst our end-users' favorites and are suitable for all budget sizes. The list is sorted in alphabetical order and doesn't indicate any ranking or preference.

### Main Data Integrations for Personal Identifiers and Social Media



#### Maltego Standard Transforms – IPQualityScore

Verify and fraud-check email addresses and phone numbers and identify suspicious IP addresses.

➤ Click-and-run



#### Pipl

Access over 3 billion online identities that have been cross-referenced and indexed for accuracy and speed.

\$ Data subscription



#### ShadowDragon SocialNet

Map social media connections with data from 120+ social networks for OSINT investigations.

<> Bring your own key



#### News Transforms

Search for articles and find context relevant to the persons, companies, locations, threats, and topics involved in an investigation.

➤ Click-and-run



#### Social Links Pro

Discover online presence, identity, groups, and affiliations of a person behind digital credentials.

<> Bring your own key



#### People Data Labs

Search and retrieve personal identity information such as email addresses, physical addresses, social media profiles.

\$ Data subscription

### Main Data Integrations for Company Data



#### OpenCorporates

Access companies information to investigate beneficial ownership, money laundering, and financial crimes.

➤ Click-and-run




#### Orbis – Bureau van Dijk

Gain a quick understanding and easily visualize corporate structures and hierarchies.

<> Bring your own key

# Supplementary Data Integrations






### Google Maps Geocoding

Normalize and enrich location data in your investigations.


↗ Click-and-run



### Google Programmable Search Engine Transforms

Search for people and aliases in major social media networks.


↗ Click-and-run



### Have I Been Pwned?

Check for password/domain breeches or to check if an alias or e-mail have been listed in a post to Pastebin.


↗ Click-and-run



### LittleSis

Explore influence and connections of politicians, CEOs, world leaders, and other high-profile figures.


↗ Click-and-run



### LoginsoftOSINT

Detect disposable phone numbers and obtain relevant meta-data.


↗ Click-and-run



### TinEye

Conduct reverse image search for image verification, UGC moderation, copyright, and fraud detection.


↗ Click-and-run



### Wayback Machine

Browse archived content of billions of websites to uncover deleted pages, hidden files, and more.

↗ Click-and-run



### FullContact

Search names, postal addresses, raw and hashed email addresses, phone numbers, and Mobile Ad IDs.

⏏ Bring your own key

Looking for more data sources? Explore and find your solutions in our [Transform Hub](#) now.



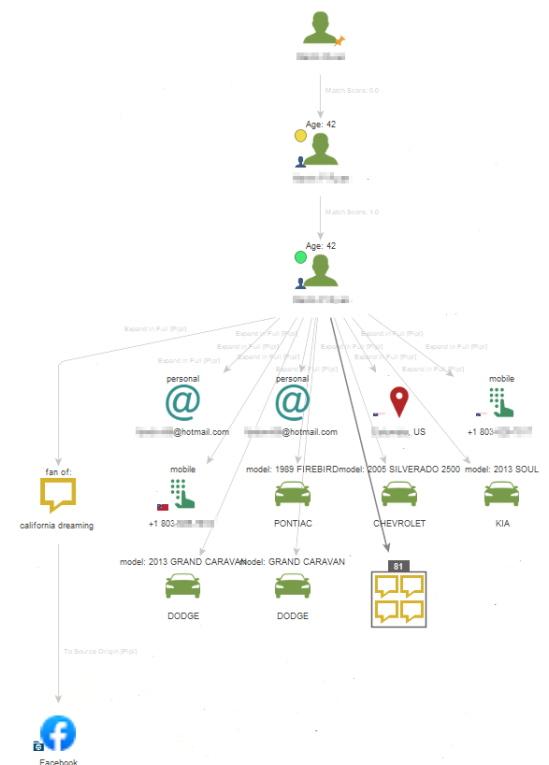
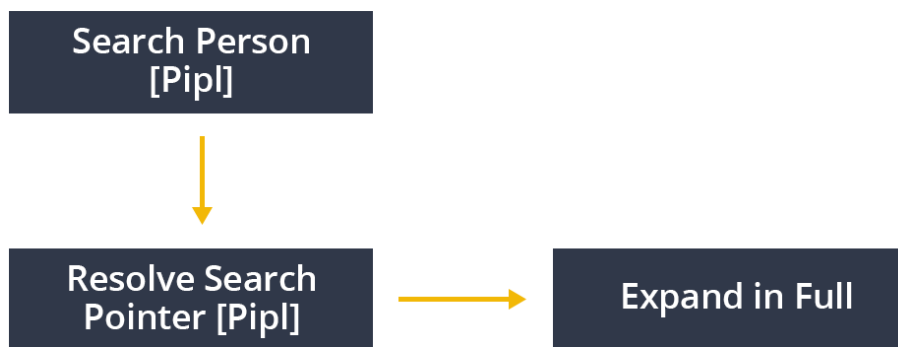
## 5. Workflow: Starting with A Name

Names are one of the most common pieces of information that we acquire when starting an investigation. It can be difficult to find meaningful information about someone based solely on their name, especially if the name is rather common. Names are also more useful if they belong to someone that is more noteworthy, as they may have more publicly available information.

Our goal when searching for a name should generally be to find more unique pieces of information, like phone numbers, email addresses, and online aliases that will allow us to dig deeper into our investigation.

### pipl Pipl

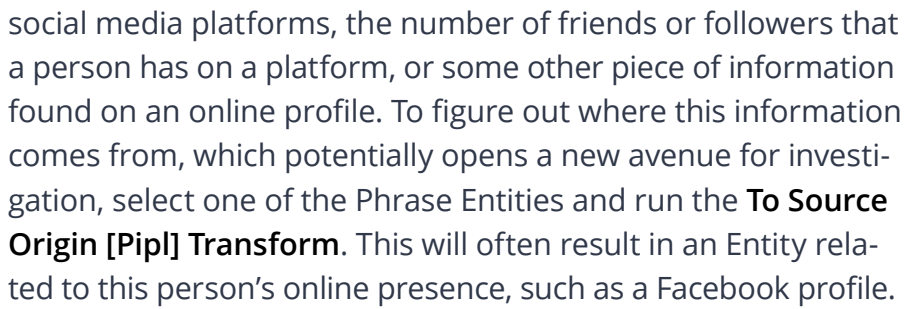
Query a specific individual using a name. For this process, which is unique to Pipl, you will often return a Possible Person Entity indicated with a yellow dot. You must then run the **Resolve Search Pointer [Pipl]** Transform to identify a specific Pipl Person Entity. From here, it is easiest to use the **Expand in Full** Transform to find all of the information that Pipl can provide.



These results often include items like email addresses, phone numbers, and Pipl Tags. We'll cover how to approach email addresses and phone numbers in other sections, so let's look at Pipl Tags here.

Pipl Tags show up in Maltego as individual Phrase Entities, each representing a piece of information that was collected from a specific data source. These Tags are often pages liked on





Names can be searched within Maltego using some of the Maltego Standard Transforms.

One technique is to add a Person Entity to the graph with the full name of the individual (first, middle, and last name), if possible, as the identifier, and run the **To Website [Bing]** Transform, which will return results similar to those that you might get in a browser-based search. From here, you can use the Detail Panel in Maltego to scan the information for any sites that might be pertinent to your investigation. You may need to use your browser to access the data on those sites, so make sure to use standard operational security.

In this example, we found a data collection site that provided accurate addresses, email addresses, phone numbers, and relatives, though you must use your best judgement with the information provided by this type of sites, as it may not be accurate. If you find any of the pieces of information worth further investigation, you can then manually add them to your graph and continue within Maltego.



Many data sources don't have much information on the average person, but high-profile people—such as celebrities, business owners, and government officials—are often included in some of them. Sources like OCCRP Aleph, OpenCorporates, Orbis – Bureau Van Dijk, LittleSis, and even the Maltego News Transforms might be able to provide more information on such high-profile individuals.



### Maltego News Transforms

- To News Articles Related to Person [Maltego News]
- To News Articles with Exact Person [Maltego News]



### OCCRP Aleph

- Lookup in Company Registries
- Lookup in Leaks
- Lookup in Sanctions List
- Lookup in Court Archives
- Lookup in Financial Records



### OpenCorporates

- Search Officers [OpenCorporates]



### LittleSis

- Search for People [LittleSis]

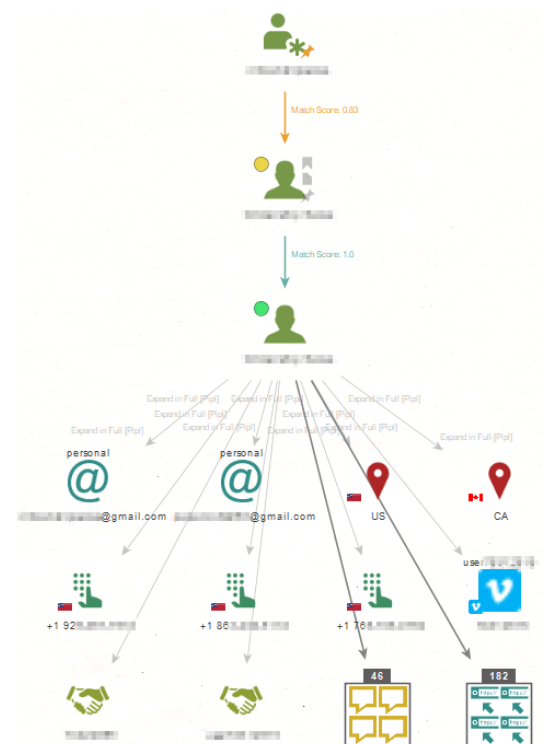


### Orbis – Bureau Van Dijk

- [Orbis] - Find People by Name

As we have seen in some of the previous sections, many investigations that start with other pieces of information—names, email addresses or phone numbers—result in the discovery of an alias. We can then use this alias to dig deeper into our current data source, or even pivot from one data source to another to find more information. Finding these accounts is always the goal of the portion of the investigation focused on the alias, but once you find those online accounts, you must continue to dig deeper to uncover more useful information.

As when using Pipl with a Person Entity (when starting with a name), you can use the same workflow with an Alias Entity. Often, this alias is used with an online account associated with a person in the Pipl database. This can help us further uncover email addresses, phone numbers, and more.



## Generating Potential Email Addresses with Aliases

ShadowDragon SocialNet has a unique feature that allows you to convert an alias into email addresses using common domains for a particular location. This can potentially allow you to uncover new email addresses. However, it is important to keep an eye out for false positives.

- SocialNet - Generate Potential Emails (CN)
- SocialNet - Generate Potential Emails (EU)
- SocialNet - Generate Potential Emails (RU)
- SocialNet - Generate Potential Emails (US)

## Finding Online Accounts with Aliases

We can also use SocialNet to find accounts online.

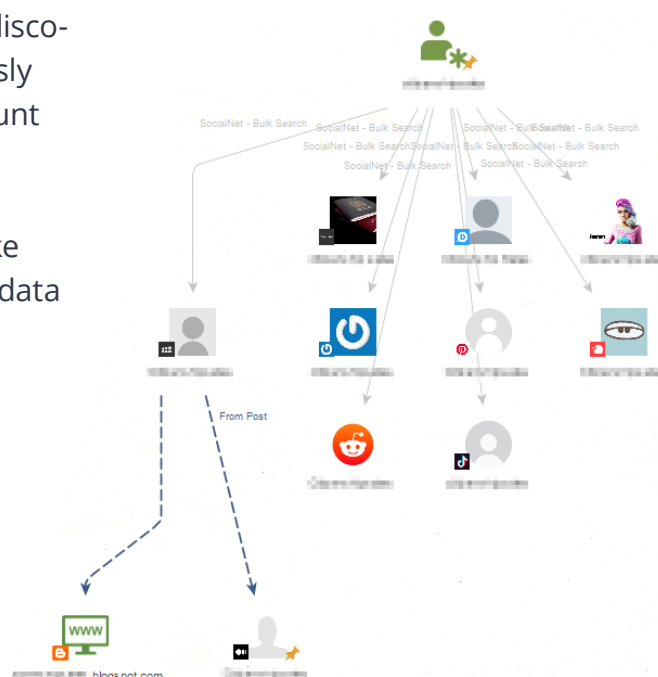
- SocialNet – Bulk Search
- SocialNet – Popular Search
- Many other Transforms that link directly to popular platforms, including Facebook, Skype, CashApp, Duolingo, Github, and Yelp

In this specific case, we can move from one of the newly discovered online accounts to more information, like a previously unknown blog that provides more data and another account on an online platform.

Once we find these new online accounts, data partners like ShadowDragon SocialNet allow you to extract even more data from those Entities.

## Facebook

- SocialNet – Extract Alias
- SocialNet – Get Albums
- SocialNet – Get Photos Tagged
- SocialNet – Get Unlisted Friends





## Instagram

- SocialNet – Extract Alias
- SocialNet – Extract Image
- SocialNet – Fill Extra Info
- SocialNet – Get Posts

## Skype

- SocialNet – Extract Alias
- SocialNet – Extract Image
- SocialNet – Extract Location
- SocialNet – Extract Name
- SocialNet – Extract Website



## 7. Workflow: Starting with An Email Address

Email addresses make great starting points for online investigations for multiple reasons.

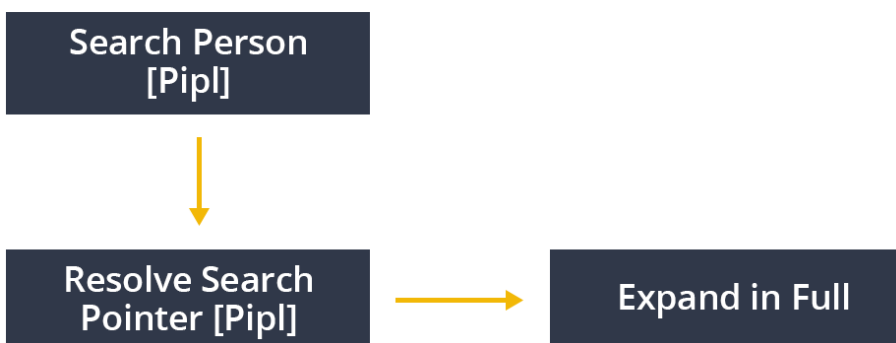
First, email addresses are typically unique to one user, which means that any account tied to that address likely belongs to the same person.

Second, email addresses are commonly used to register for websites and platforms, so their use can be widespread, leading investigators to many alternate sources of information.

Finally, email addresses themselves can contain data, like names or birthdates, within the text before the email domain. This information is often replicated as an online alias or username as well. For instance, *MaltegoRules@maltego.com* could be an email address that you are investigating, and *MaltegoRules* could be an alias used by the same user across different online sites and platforms.

### Pipl

Find a person by starting with an email address, then continue the workflow as mentioned in the previous sections.



## Find Online Accounts Associated With The Email Address

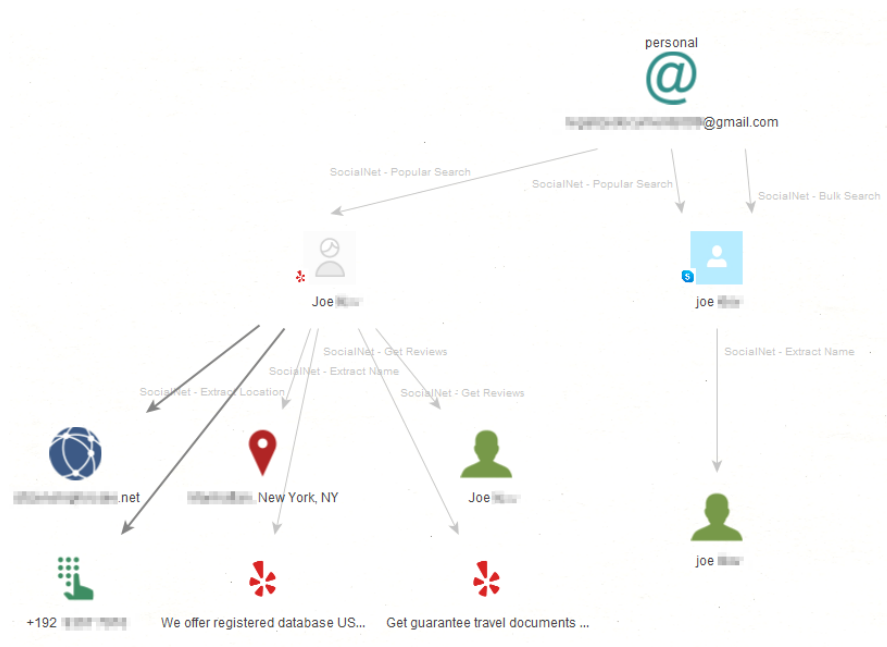
- SocialNet – Bulk Search
- SocialNet – Popular Search
- Many other Transforms that link directly to popular platforms, including Facebook, Skype, CashApp, Duolingo, Github, and Yelp

## Extract An Alias From An Email Address

- SocialNet – Extract Alias

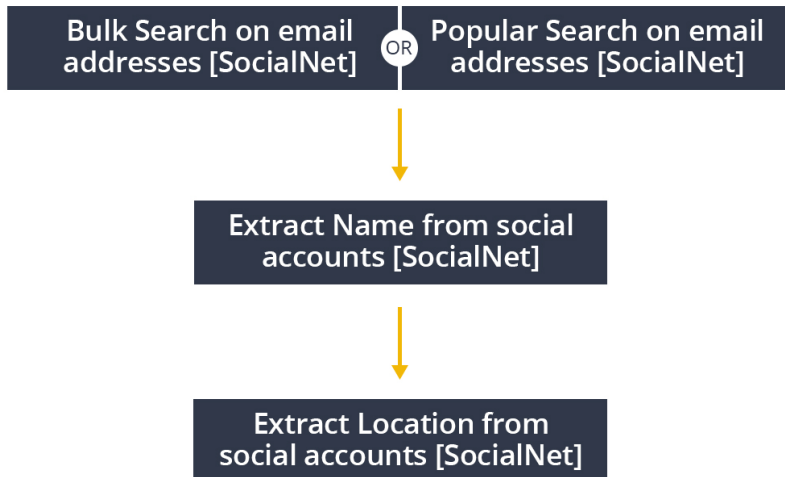
## Find If An Email Address Has Been Breached And Find Other Information From The Breach Data

- SocialNet – Search Breaches
- SocialNet – Extract Password (from the Breach Entity)





In this example, we were able to use an email address to find accounts on other platforms using **SocialNet – Bulk Search** and **SocialNet – Popular Search**. We were then able to discover more information using other SocialNet Transforms like **SocialNet – Extract Name** and **SocialNet – Extract Location**. We also visited the profile page for the Yelp! user and found a domain that was being used to sell counterfeit documents online.



## Have I Been Pwned?

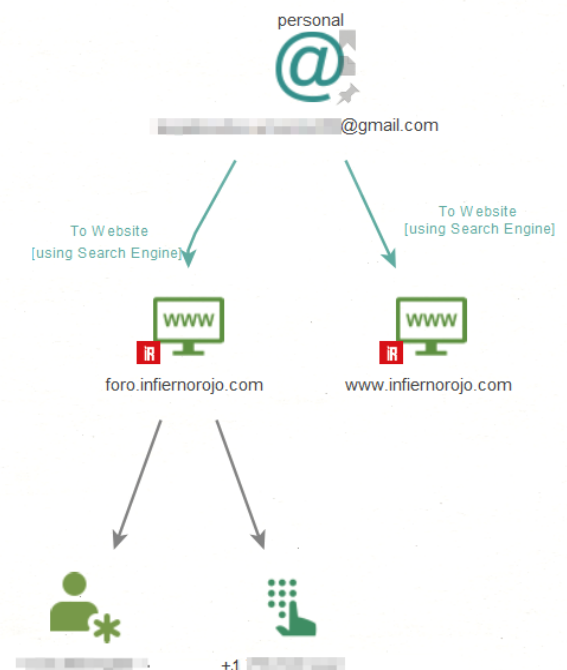
Find if an email address has been breached and find other information from the breached data. You can then get the details of the breach, including what type of information was compromised, but not the information itself.

- Get all breaches of an email address [v3 haveibeenpwned]
- Enrich Breached Domain [v3 haveibeenpwned]

## Maltego Standard Transforms

We can also search for email addresses on websites using the Maltego Standard Transforms.

In this example, we run the **To Website [Using Search Engine]** Transform to find a mention of this email address on an online forum. By visiting the forum and reading the post, we are then able to manually add a new alias and phone number that was mentioned on the site.







## 8. Workflow: Starting with A Phone Number

Some social media will not allow their users to be searched using their phone number. However, it is sometimes possible to check if a profile using a particular phone number exists.

Be aware that this category of Transforms relies on functionalities that are not a core part of the social media platforms they query. If these functionalities are removed or altered, it might impact the quality of the results of these Transforms.

Note that it is important to add the country code when using a phone number in Maltego. Different formatting may be better fit depending on the integration used.



### ShadowDragon SocialNet

#### Query A Specific Social Media Profile Using A Phone Number

- SocialNet - Search Telegram for Users
- SocialNet - Search Skype for Users
- SocialNet - Search WhatsApp for Users
- SocialNet - Search Signal for Users
- SocialNet - Search CashApp for Users
- SocialNet - Search CityXGuide for Posts
- SocialNet - Search Foursquare for Users
- SocialNet - Search SkipTheGames for Posts

#### Checking If A Phone Number Has Been Used To Register A Profile On A Social Media Platform

- SocialNet - Search FB for Recovery Users

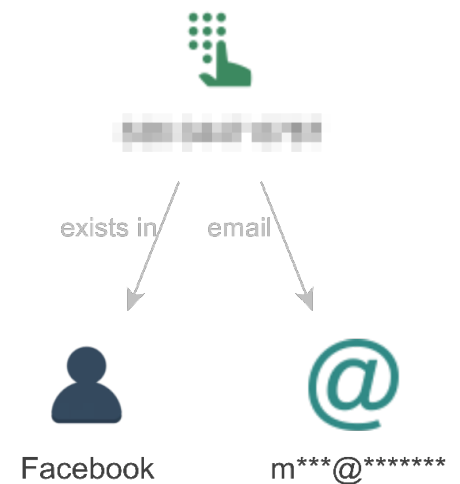
## Query A Specific Social Media Profile Using A Phone Number

- [Skype] Get profile
- [WhatsApp] Get Profile
- [Snapchat] Get Profile (beta)
- [Telegram] Get Profile

## Checking If A Phone Number Has Been Used To Register A Profile On A Social Media Platform

- [Twitter] Check Profile Exists
- [Weibo] Profile Exists
- [Facebook] Check Profile Exists

Some of these Transforms will give you some partial information on the profile matching a phone number.



## **pipl** Pipl

Pipl allows you to search their database using a phone number as a departure point. Please **make sure the country code is separated** from the other digits, as in the following example: **" +33 XXX XXX XXX"**.

## To search the Pipl database using a phone number

- Search Person [Pipl]



## 9. Workflow: Starting with An Image

As already highlighted in chapter 2 of this handbook, pivoting from a profile picture can be quite difficult. However, as it is often overlooked, it may yield interesting results if pivoting from an alias is unsuccessful.



### ShadowDragon SocialNet

If you obtained a social media profile Entity through SocialNet, you could run **SocialNet – Extract Image** to bring the image(s) to the graph. Then, from that image, you can use 3 Transforms to perform a reverse image search using different engines:

- SocialNet – Search Yandex for Images
- SocialNet – Search Sogou for Images
- SocialNet – Search TinEye for Images

These 3 Transforms will return search results which you can sort out by extracting the URLs using **To URLs [within Properties]** then running **To Website [Convert]** Transforms (both part of the Maltego Standard Transforms) to quickly verify if any of them belong to a social media website.

If it is the case, and the URL attached to this search result links to a profile, you can manually extract the alias used by that profile and do a **SocialNet – Bulk Search** from that Alias Entity.

Please take note that TinEye is also present as a separate and free integration in the Transform Hub.



### Social Links

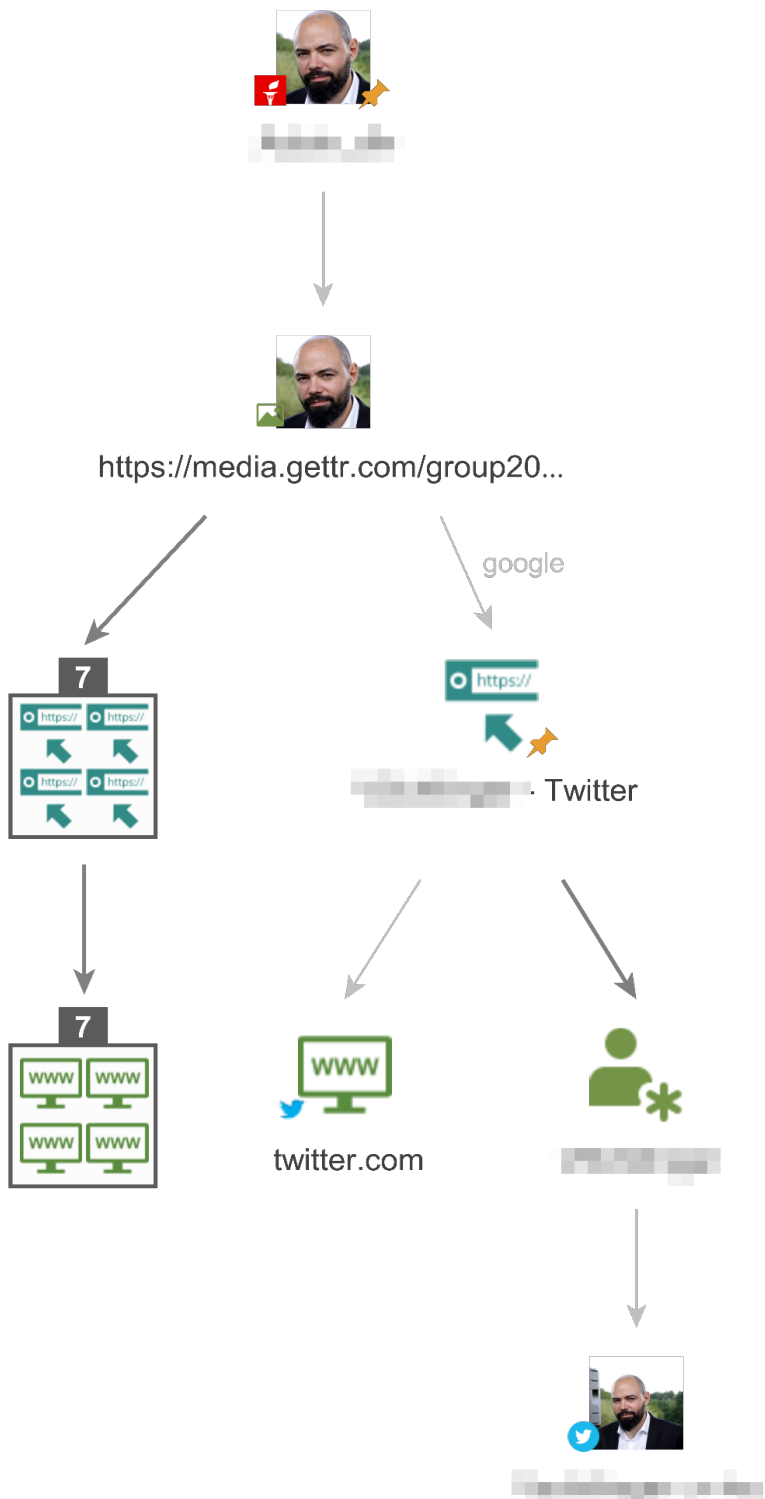
From a profile obtained through Social Links, you can directly perform a search from the profile Entity using two different search engines:

- [Image] Search in Google
- [Image] Search in Yandex

URL Entities will be returned, and you can then sort them out by grouping them by website using **To Website [Convert]**. Then, if one of the URLs seems to link to a social media profile, you

can add the username of that profile to your graph and use Social Links to search on the corresponding social media platform.

On the image below, you can see an image that was taken from a Gettr profile, then searched using Social Links Transforms. Once the correct URL was extracted, the matching Twitter profile could be queried using Social Links.





# 10. Workflow: Starting with An Address or Location

Starting with an address or a location can be a difficult task because most people do not put their home address out on the Internet. However, some official paperwork needs an address to be filled. This is where integrations like OCCRP Aleph and OpenCorporates come into play. For example, when starting a company, some people do not have an office location right away. They often fill out the company registration information using their home address.

Another way to pivot from addresses is to rely on solutions like Pipl, which collects information from multiples sources online. Since some of these sources include home addresses, it is possible to search for a person directly from an address.

Other integrations, like Social Links and ShadowDragon Social-Net, allow you to collect posts pinned to a specific location to obtain information on the place and the people linked to it.

## OpenCorporates

Search for companies that were incorporated at a specific location:

- [Search Companies at this Address \[OpenCorporates\]](#)



## OCCRP Aleph

Search a location in OCCRP Aleph's database:

- [Lookup \(all datasets\) \[Aleph\]](#)

Search a person from a location:

- Search Person [Pipl]

Be aware that Pipl needs some more information to perform the search:

You will need to supply either the name, the phone number, the email, or the username of the person you are searching for. Note that this method is particularly useful when you don't know the exact address of the person. One can simply add a location Entity related to a city and ask people to search for anyone called "*Jane Doe*".



## ShadowDragon SocialNet

You can search for posts on social media by running these Transforms from a location Entity:

- SocialNet – Search YouTube for Videos
- SocialNet – Search Pandora for Users



## Social Links

There are two ways of going about this.

### Search for An Account Linked to A Location

Search for an account linked to a location by creating a Search by Face and Location Entity and adding to it a picture of the person you are searching for:



- [Facebook] Create Search by Face and Location Entity
- [Instagram] Create Search by Face and Location Entity

These Transforms can be run on a location Entity.

## Search for Posts Pinned to A Specific Location

Search for posts that are located near a specific location. These Transforms should be run from a GPS Coordinate Entity:

- [Facebook] Get Photos
- [Facebook] Get Videos
- [Facebook] Search Place
- [Instagram] Get Posts
- [Snapchat] Snap by Geo
- [Telegram T2] Search Groups (require SL Pro and Telegram pack key)
- [Telegram T2] Search Profiles (require SL Pro and Telegram pack key)
- [Twitter] Search Tweets by Geo
- [VK] Get Photos Popular
- [VK] Get Photos Recent
- [VK] Get Stories
- [YouTube] Video by Geo



# 11. Example Maltego Use Cases

How to Conduct Person of Interest Investigations Using OSINT and Maltego

[LEARN MORE >](#)

Introducing the New Pipl Transforms for Person of Interest Investigations

[LEARN MORE >](#)

Using Maltego and Shadow-Dragon SocialNet to Trace the Chain of COVID-19 Infection Spread Through Social Media Analysis

[LEARN MORE >](#)

Verifying and Investigating Email Addresses with IPQualityScore Transforms in Maltego

[LEARN MORE >](#)

Investigating Phone Numbers with OpenCNAM and IPQualityScore

[LEARN MORE >](#)

Jumpstart Your Person of Interest (POI) Investigations with People Data Labs and Maltego

[LEARN MORE >](#)

# 12. Useful Resources



WhatsMyName

This tool allows you to enumerate usernames across many websites. [LEARN MORE >](#)



Epieos

Invested in the OSINT and cybersecurity communities around the world. It helps many people work on Cyber Threat Intelligence, child abuse, investigative journalism, etc. [LEARN MORE >](#)



Smat App

Designed to help facilitate activists, journalists, researchers, and other social organizations to analyze harmful online trends such as hate, mis-, and disinformation online. [LEARN MORE >](#)





Maltego is a comprehensive tool for graphical link analyses that offers real-time data mining and information gathering, as well as the representation of this information on a node-based graph, making patterns and multiple order connections between said information easily identifiable. With Maltego, you can easily mine data from dispersed sources, automatically merge matching information in one graph, and visually map it to explore your data landscape. Maltego offers the ability to easily connect data and functionalities from diverse sources using Transforms. Via the Transform Hub, you can connect data from over 30 data partners, a variety of public sources (OSINT) as well as your own data. Our different Desktop Client versions, data sources, and server solutions enable you to tailor Maltego to your specific needs in terms of data access, functionalities, and security requirements.

For more information, please visit [maltego.com](https://maltego.com)

