ETHICAL HACKING FOOTPRINTING

MALTEGO

Detail about maltego

Researcher By: Nin Kanong

Beginner guide about maltego

What Is Maltego?

Maltego is a tool that leverages open-source intelligence (OSINT) developed by Paterva. Maltego comes in different versions, including a community edition that can be used for free with some limitations, as well as commercial versions that offer more features and capabilities.

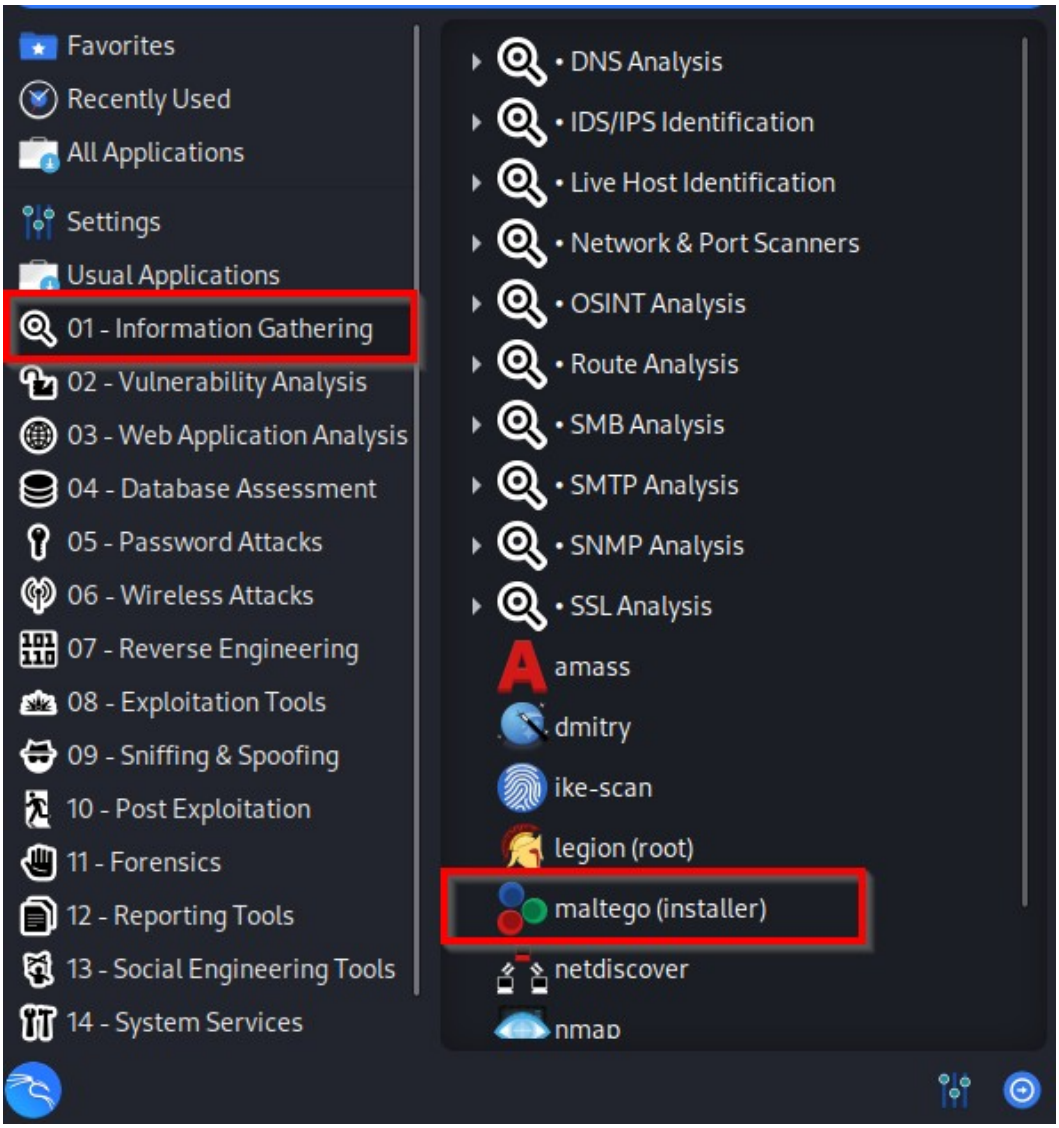
Maltego is a vital tool in the arsenal of a penetration tester. As a graphical link analysis tool, it lets you visualize connections within complex data sets, displaying interconnected links. By analyzing information from various sources such as public websites, email addresses, social media, and cryptocurrency transactions, Maltego aids in uncovering hidden relationships and patterns.

This is particularly useful in penetration testing, where understanding the target's digital footprint and connections can be crucial. Working up to 80% faster with Maltego than traditional methods allows for efficient reconnaissance.

Starting Up

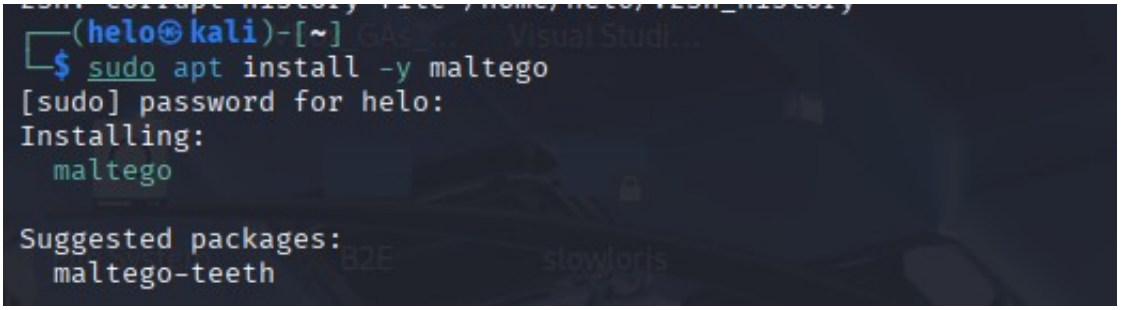
We will now show you how to get Maltego up and running. For our demo moving forward, we will be using Kali. Maltego can also be installed on Windows, macOS, and other Linux distributions.

Before you can run Maltego, you need to run the installer, which can be found in the Applications menu under “Information Gathering.”

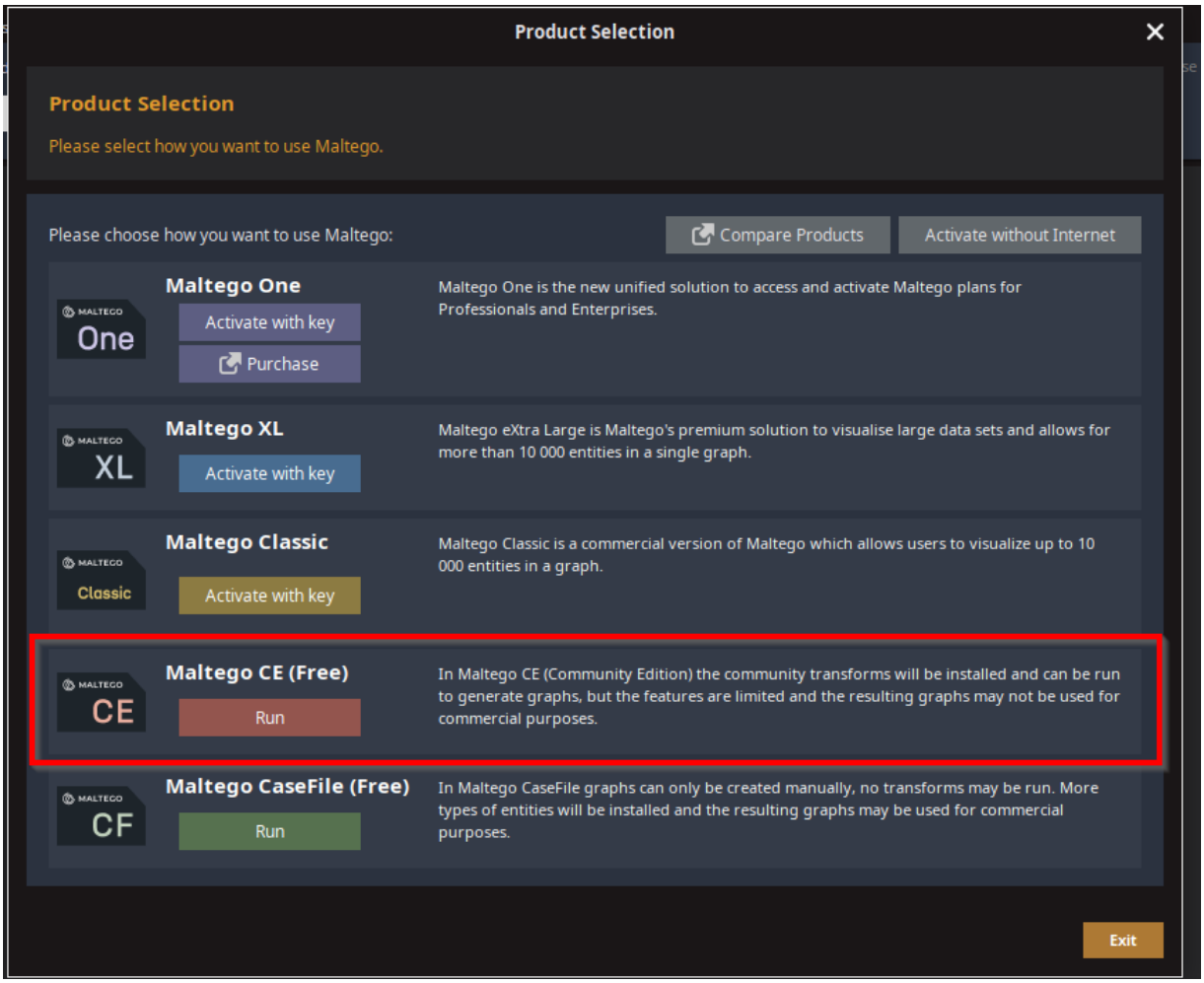


You will be taken to a terminal window if you want to install Maltego. Select “Y” to continue.

You can also install Maltego from the terminal with the following command:
- **kali>** `sudo apt install -y maltego`

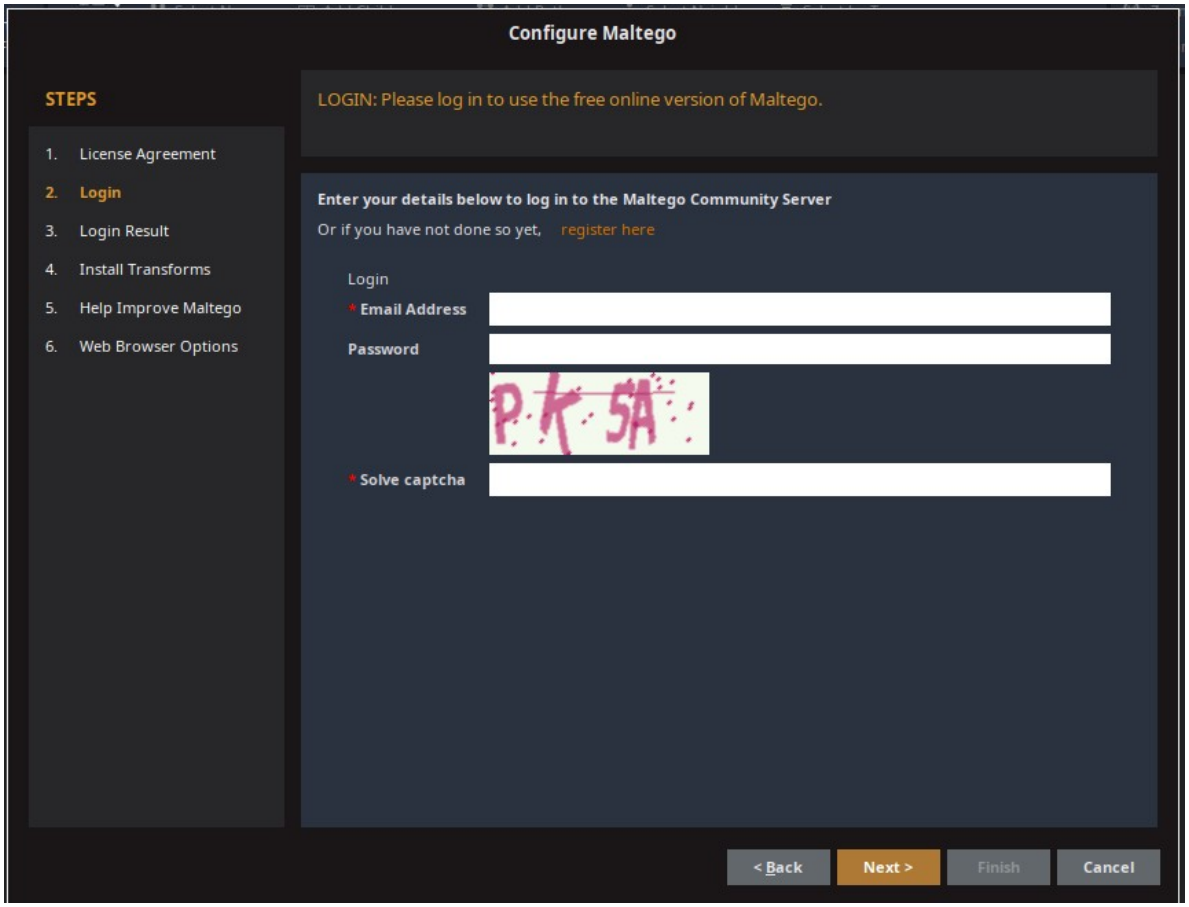


Now, you can start Maltego by entering `maltego` in the terminal or running it from the application menu.
Once Maltego opens, you will be shown a window asking you to select a product. We are using the “Maltego CE (Free)” version for our demo. Select “Run” to continue.

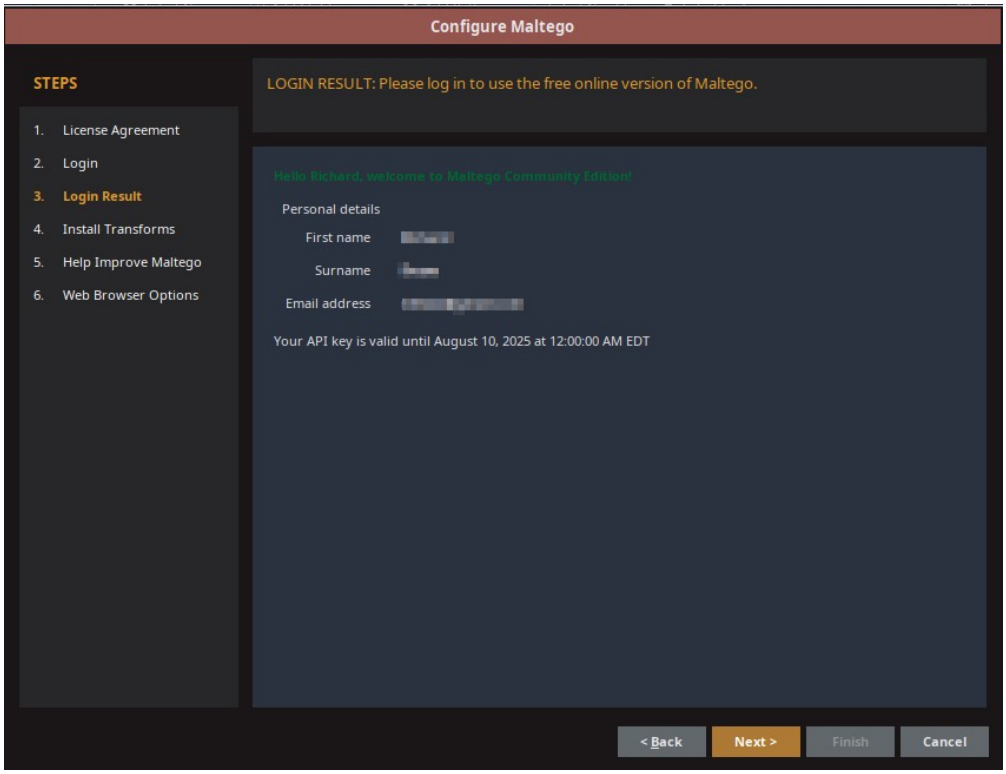


Next, you’ll need to configure Maltego. The first step is to accept the license agreement and click “Next.”

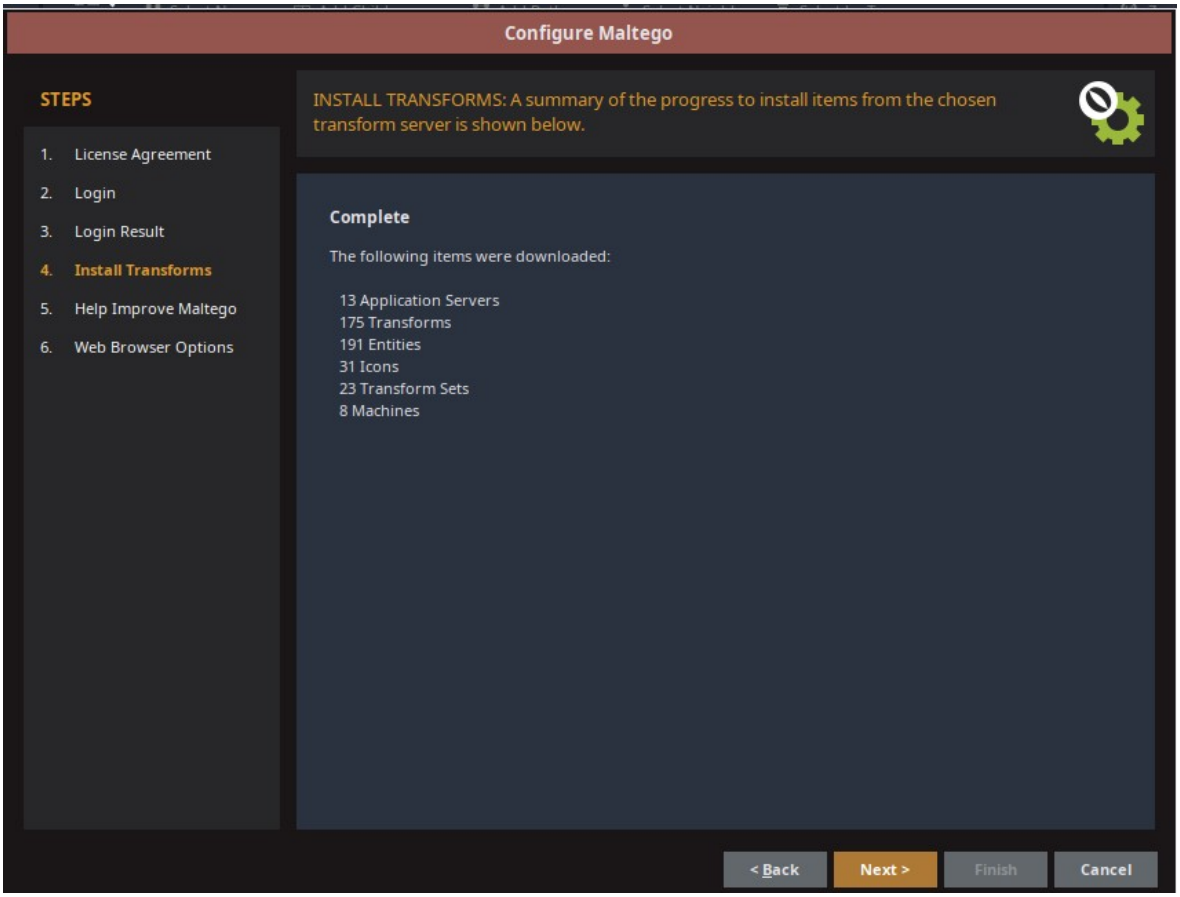
The next step is to log in so you can use Maltego. If you do not already have an account, **register one here**.



After logging in, you'll be able to see your details, like your name and email address, as well as the duration of your API key. Click “Next” to continue with the download of the Transforms.



The Transforms will be downloaded, and you must click “Next” to install them in Maltego.

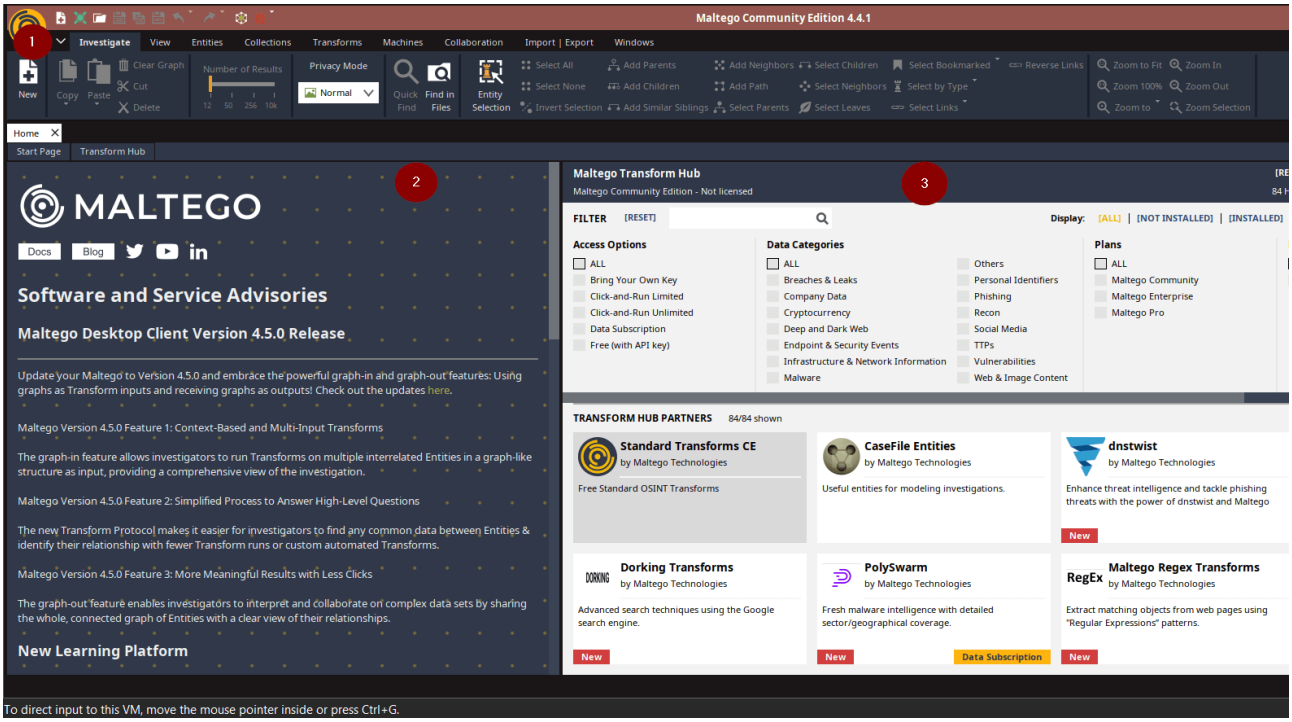


The next screen will ask if you want to send error reports to Paterva, and then click “Next” to continue.

The final window will ask what external browser you want to open links to. Make your choice and then click “Finish” to complete the configuration. Maltego will now be ready to be used.

Interface

This section will show you the main Maltego graphical user interface, and we will highlight three areas within the interface.



Application Menu

In the Application menu, you'll find the application button. This grants access to the following functions:

- New Graph
- Open Graph
- Save
- Save All
- Save As

Maltego can open and save graphs using the .mtgl extension. While these are some of the core features, there are also other advanced functions.

1.**Start Page**

The start page showcases the latest updates for products, Transform, and the Transform Hub. Any alerts affecting Maltego's functionality and security can also be found here.

1.**Transform Hub**

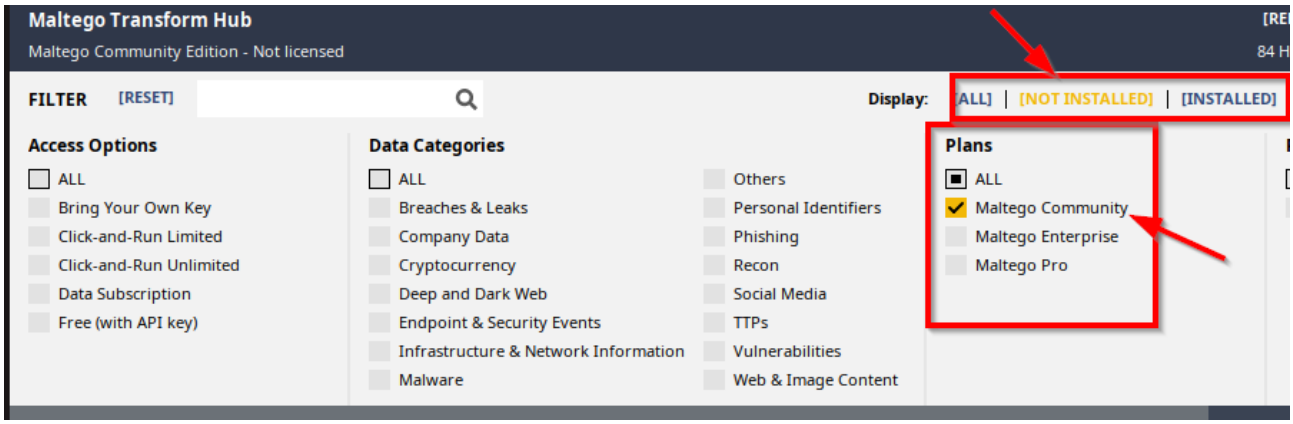
The Transform Hub catalogs all the Transforms offered by Maltego, third-party providers, or available through an API/dataset. You can either purchase these items or install them for free.

> Transforms in Maltego are specialized pieces of code that process information in a very particular way. They take an Entity (a defined piece of data like an email address, IP address, or name) as input and then search for related information, returning more Entities as output.

Let's walk through installing Transforms in Maltego's Community Edition. First, navigate to the Transform Hub within the software.

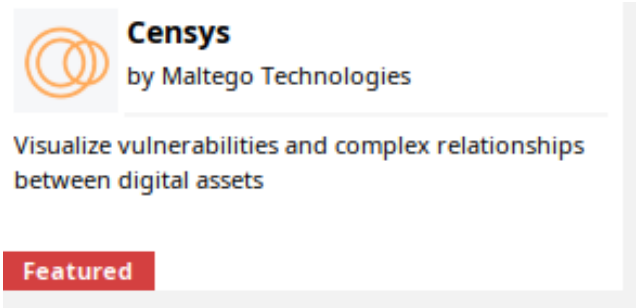
Since we're using the Community Edition, you'll want to filter the available Transforms by selecting “Maltego Community” from the “Plans” menu. This will show you only the Transforms compatible with our version, making choosing and installing the ones you need easier.

You’ll also want to display Transforms that are “NOT INSTALLED.”



Now that we have the Transforms that will work for us let’s choose one to install. At the time of writing, there are 50 Transforms available to you in the Community Edition—everything from infrastructure and network information to searching social media sites.

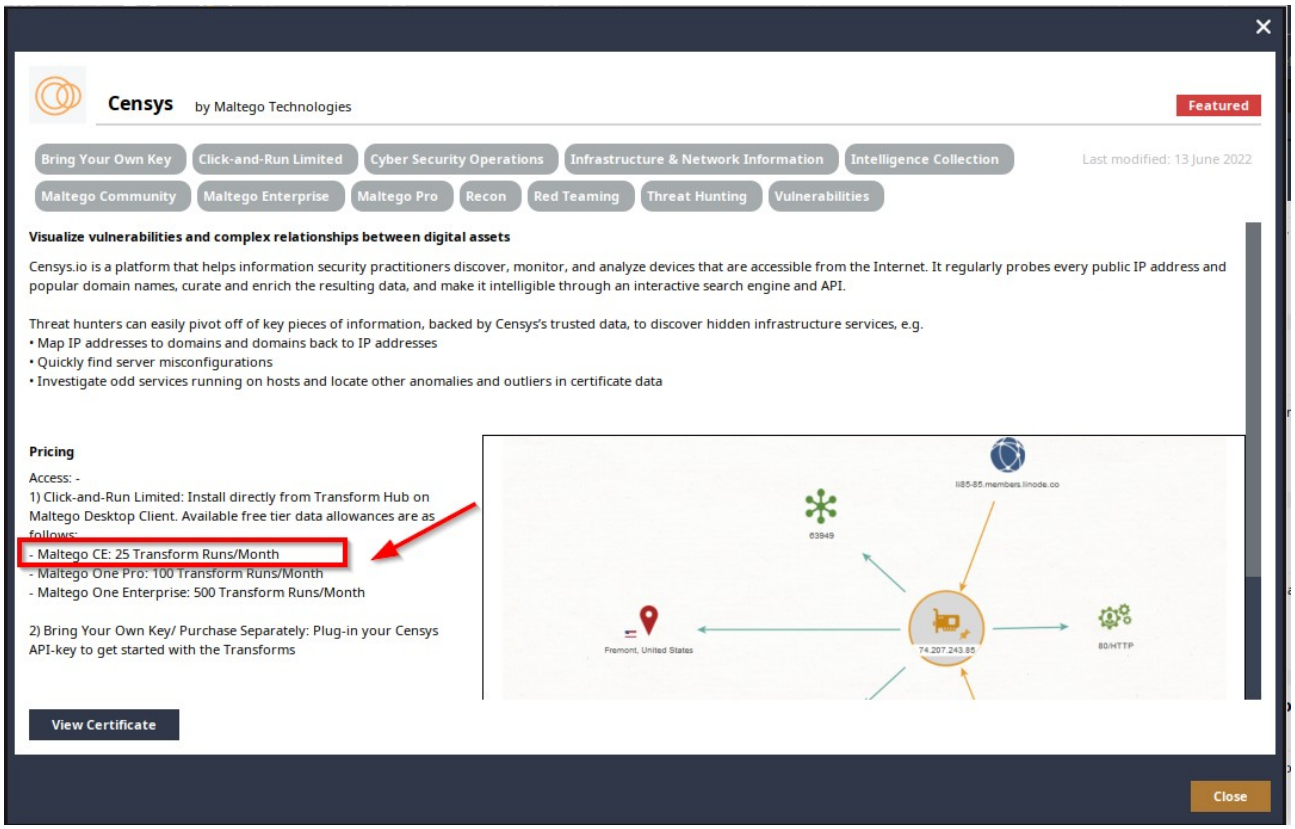
Let’s install the Censys Transform, designed to map IP addresses to the target domain and vice versa, quickly identify server misconfigurations, and efficiently scan attack surfaces for vulnerabilities



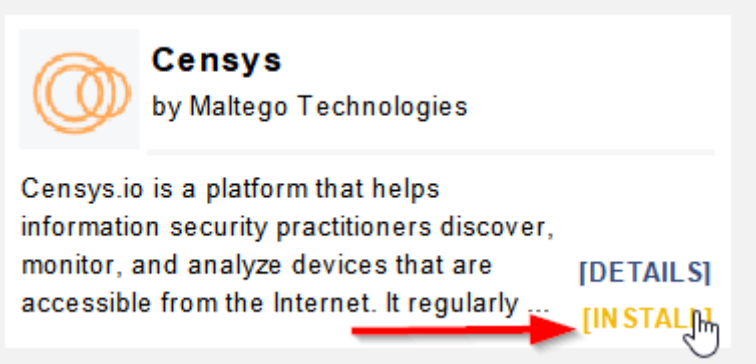
This Transform is limited to twenty-five Transform runs per month on the Community Edition of Maltego.

Several Transforms will require you to have an API key from the provider, and Censys is one of them.

To work with the Censys Transform, you will need an account and an API key. You can sign up for an account at the **Censys registration page**.

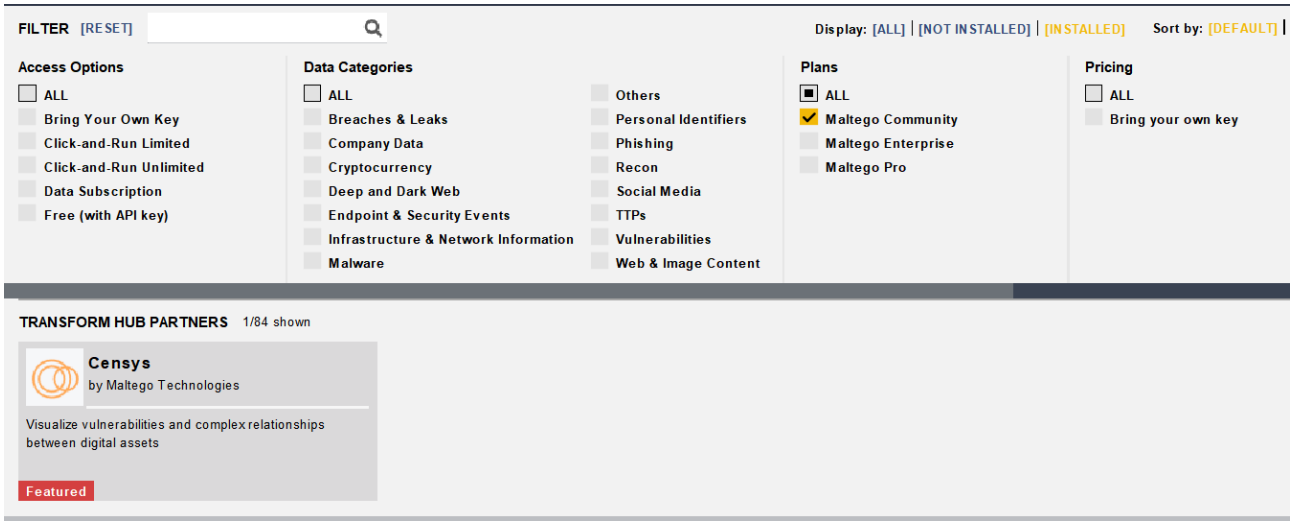


To install, hover over the Censys Transform and click "**INSTALL**." It will ask you if you are sure you want to install it. Click "**Yes**" to continue.



Complete the three steps that follow to finish installing Censys inside Maltego.

Select "INSTALLED" from the Transform Hub to see the Censys Transform listed.

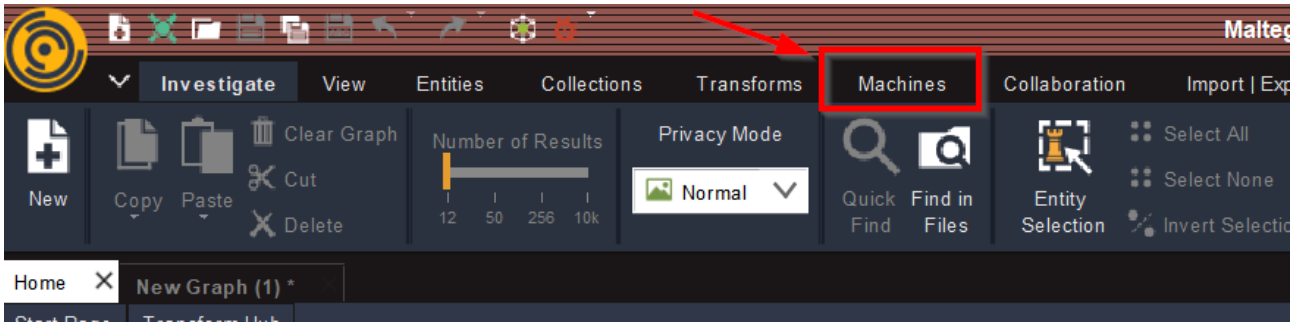


Starting an Investigation

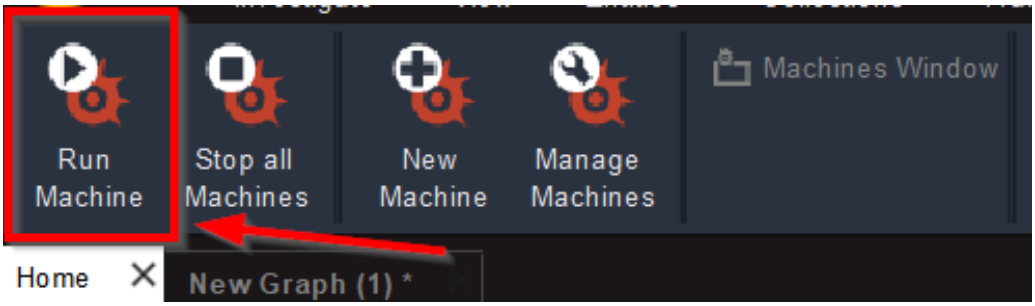
The easiest way to start a new investigation is by using Machines in Maltego. These Machines are automated sequences of Transforms in Maltego that allow users to run multiple queries or operations with a single click.

We will demonstrate how to use a Machine in Maltego, specifically focusing on the “Company Stalker” Machine. This Machine aims to locate email addresses associated with a domain, map these to corresponding social media profiles, and finally, attempt to retrieve or analyze any related metadata.

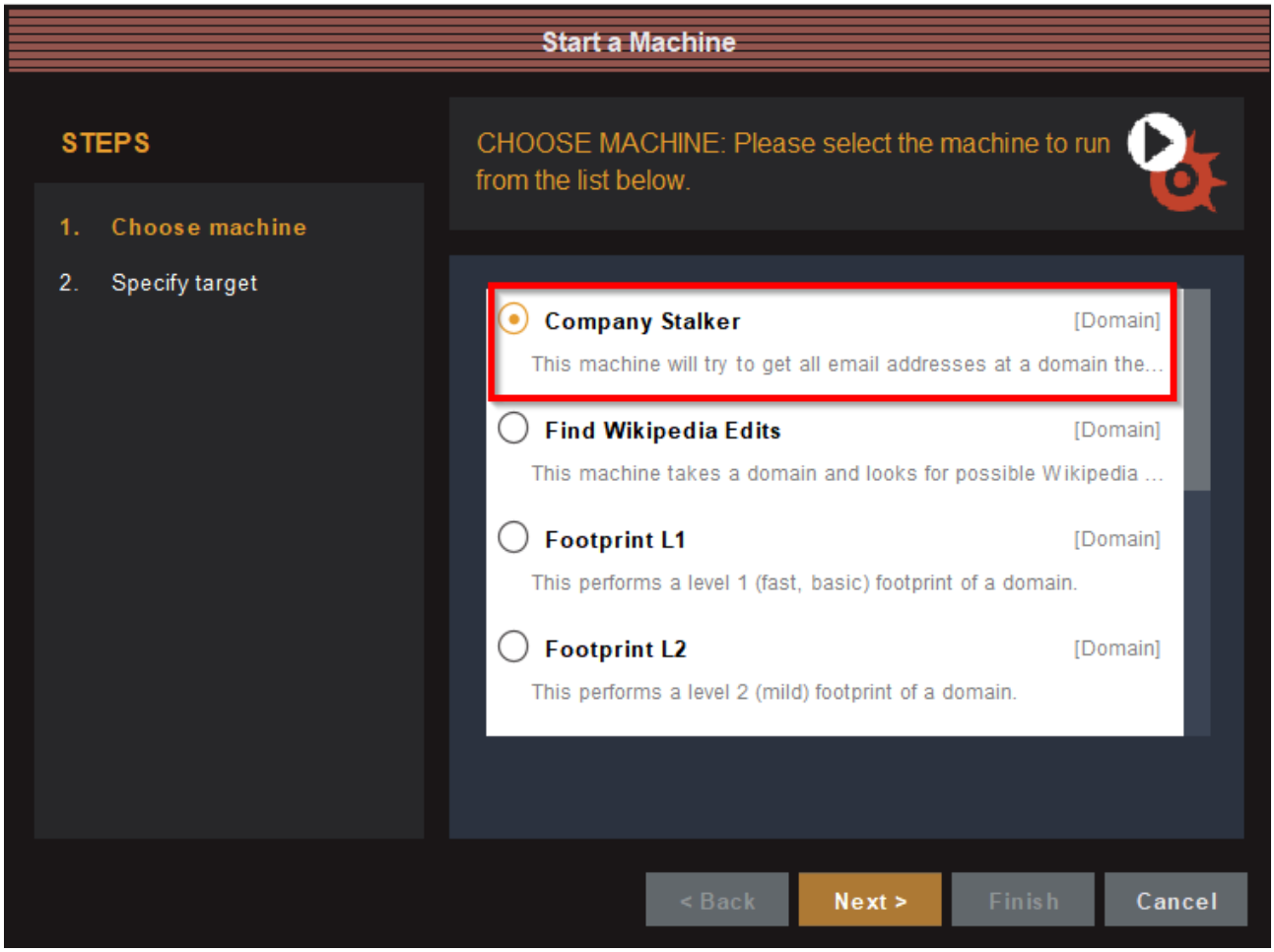
To begin, click on the “Machines” tab at the top of the Maltego window.



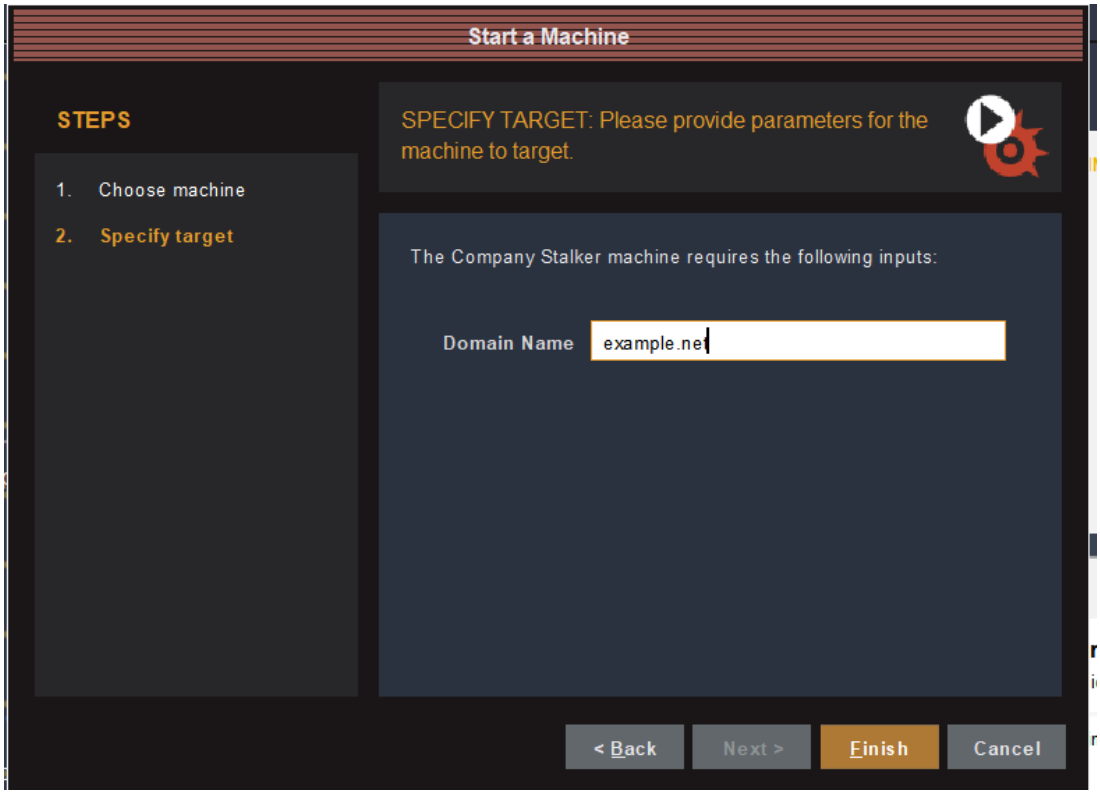
Next, select “Run Machine” to select the Machine you want to run.



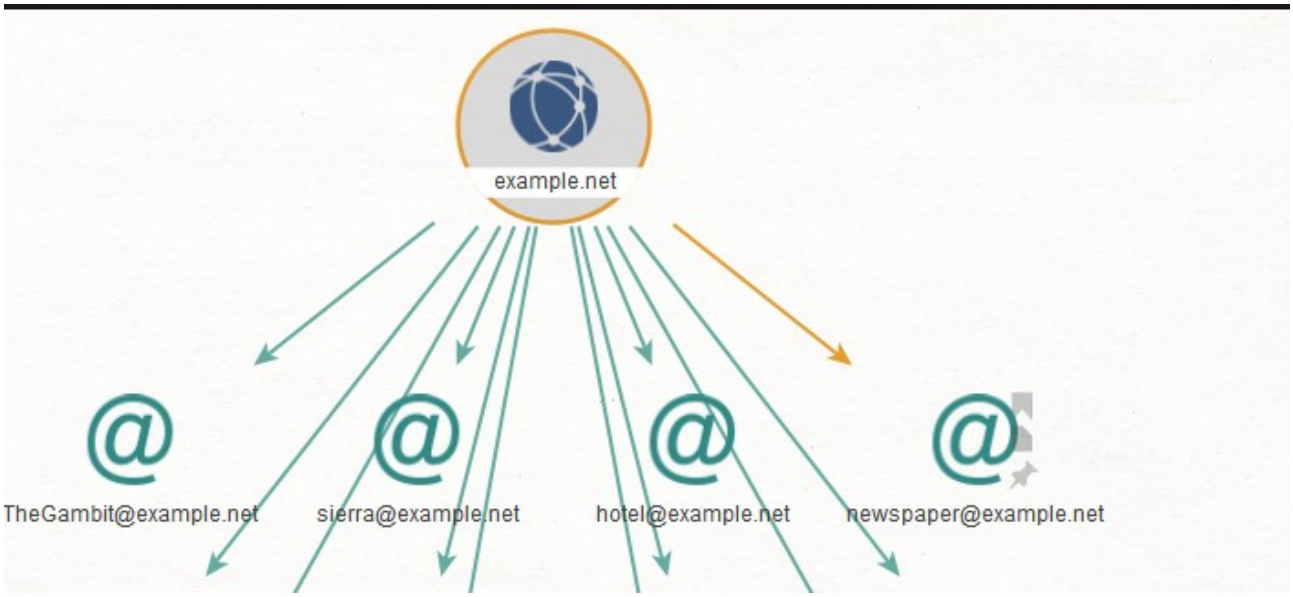
Choose “**Company Stalker**” and click “**Next**.”



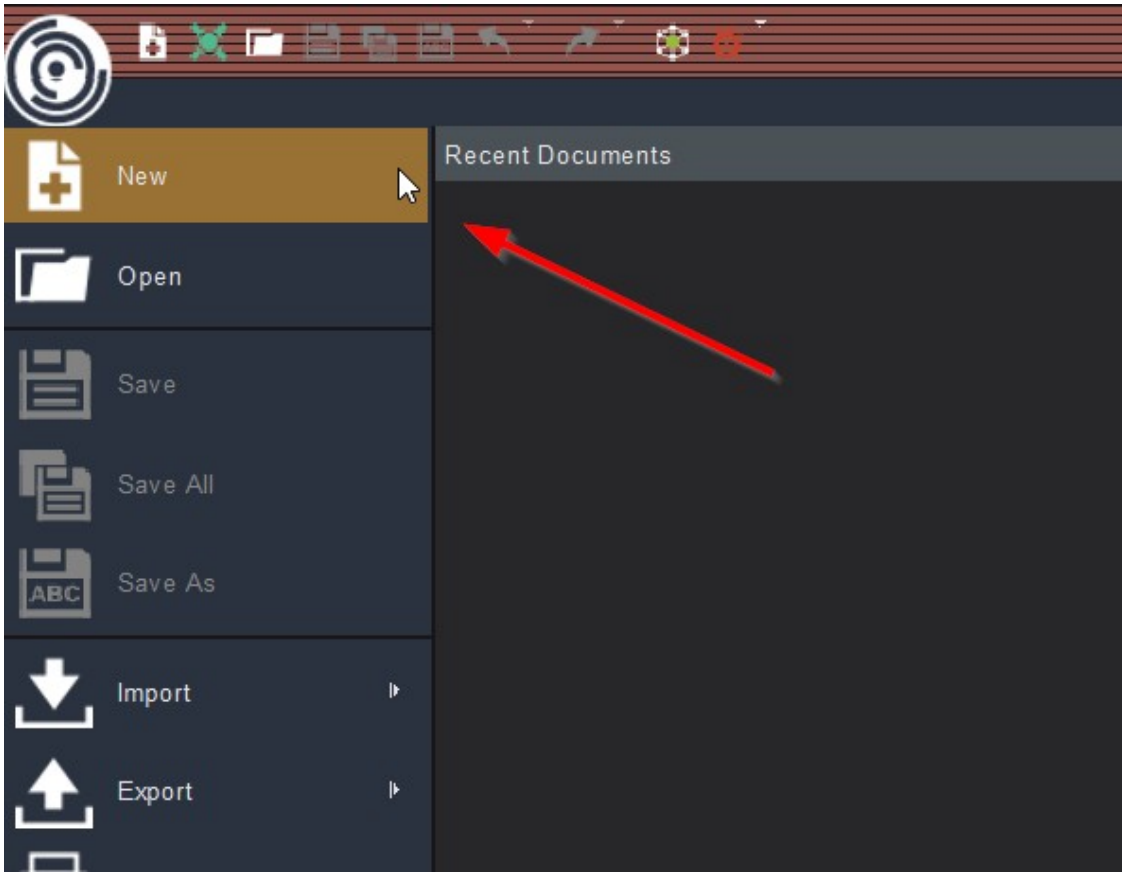
Now enter a domain you want to use as the target. In our demo, we are using **example.net** and click “**Finish**.”



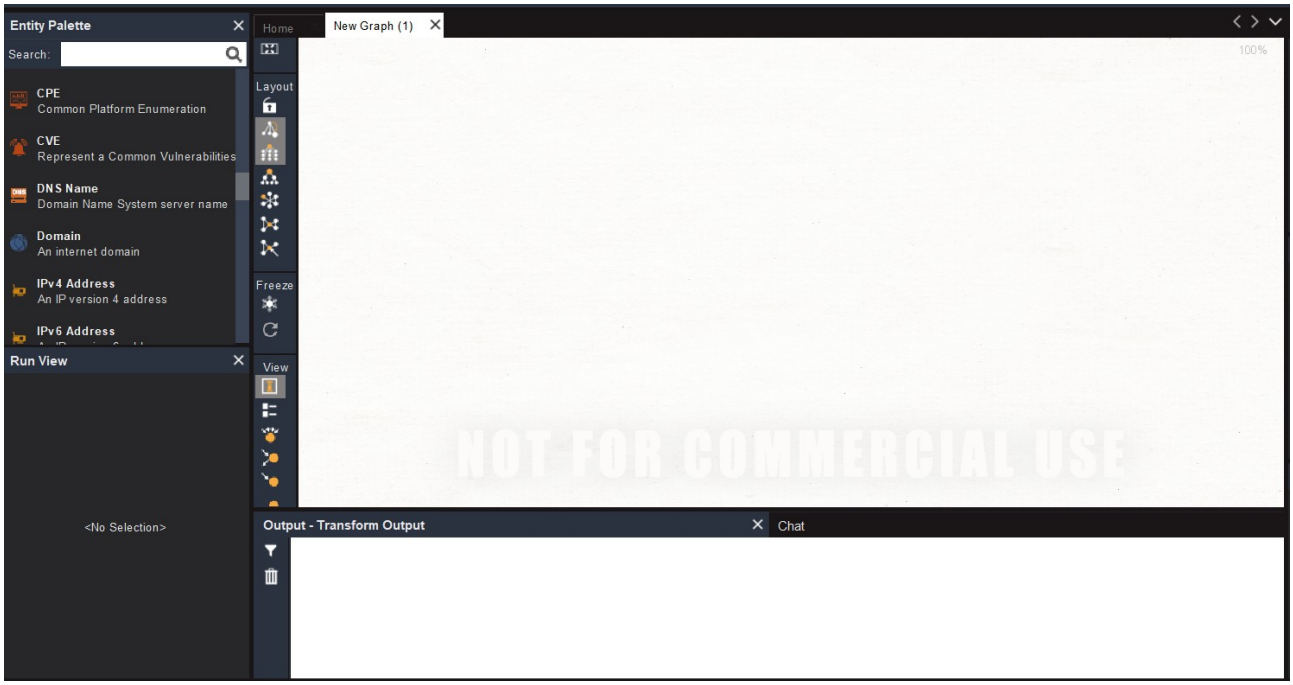
Click through any popups you receive and wait for the machine to finish running. Once finished, you will be presented with any information that was returned.



For a more detailed investigation, you can also run one manually. If you want to start a new project in Maltego, the first step is to select "**New**" in the Application menu.

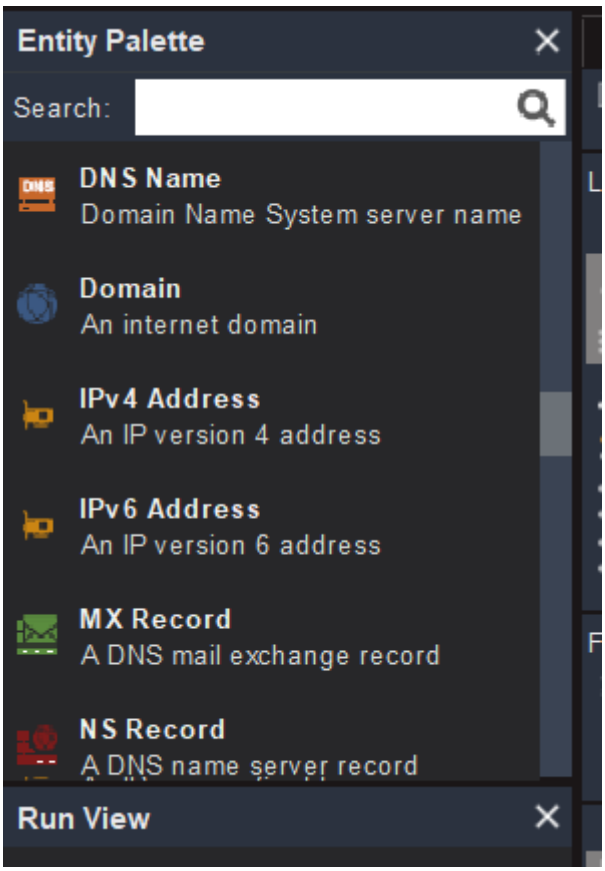


You will then be presented with different screens, such as the "**Entity Palette,**" "**Graph,**" "**Output,**" and "**Run View.**"

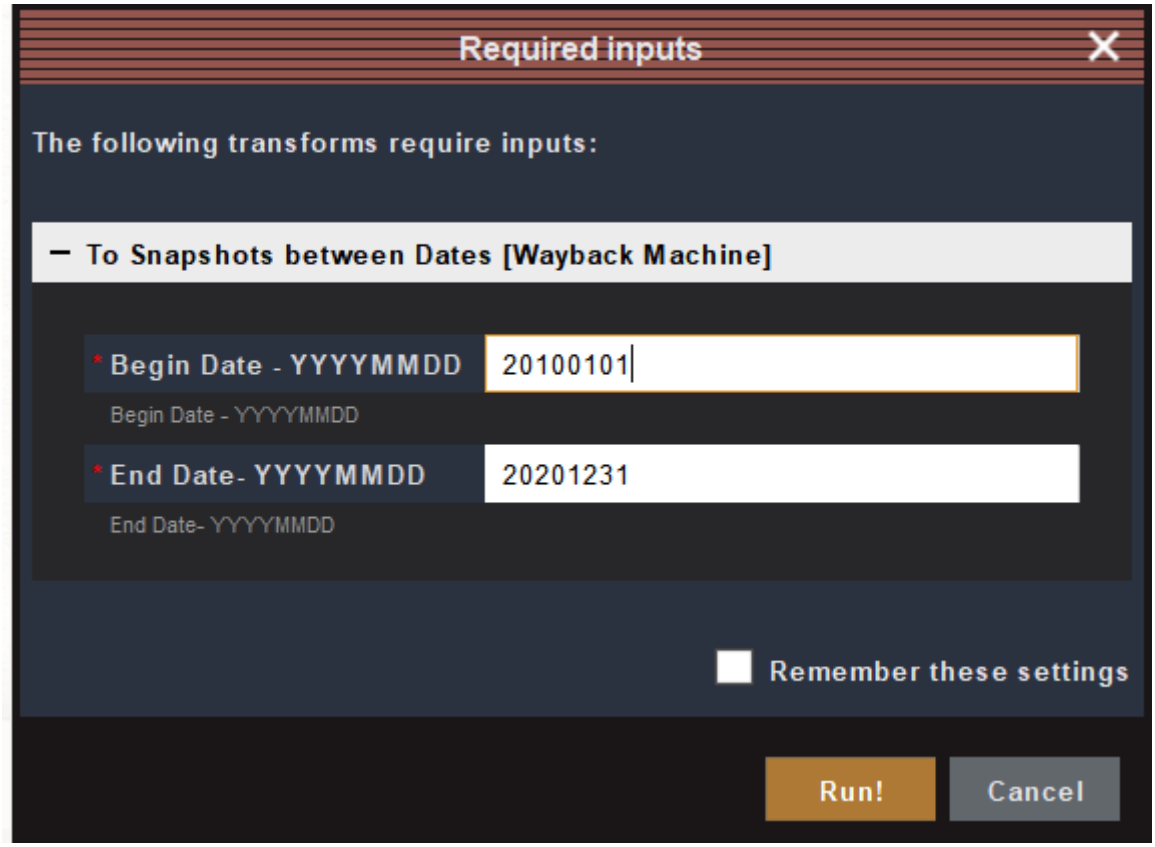


To begin your investigation, you will now want to add an “Entity” to the new graph. The easiest way to do this is using the “**Entity Pallete**” on the main interface's left side. You can either scroll through the list of entities or use the search function.

> In Maltego, an Entity represents a single piece of data you want to investigate or analyze. It can be something as simple as an email address, a phone number, a domain name, or an IP address.

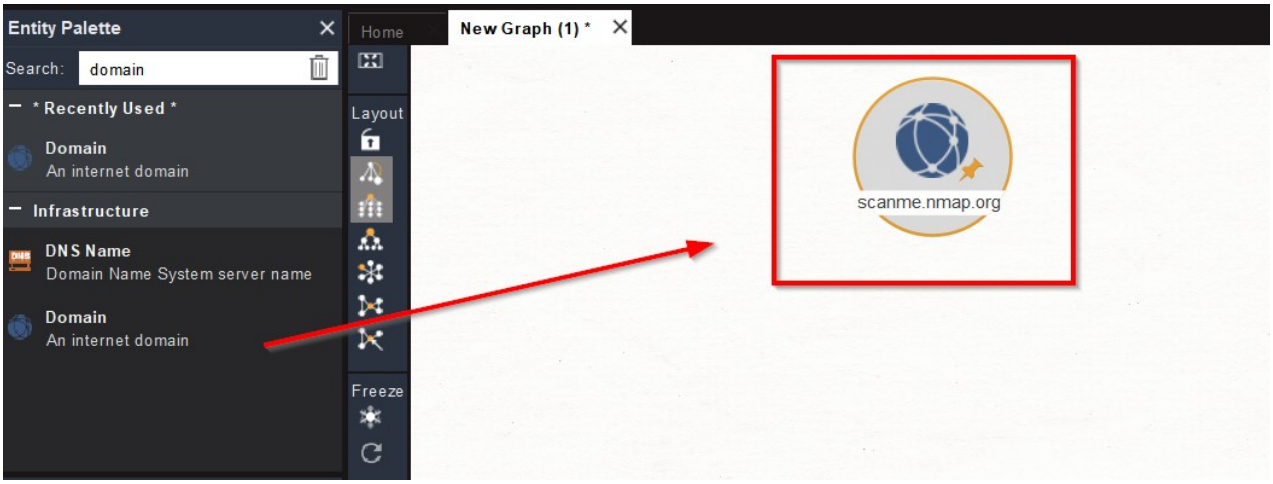


Let's add an Entity to the graph. In the "**Personal**" section, you can select the "**Email Address**" Entity or simply use the search bar to find "**Email**." Once you locate the Entity, drag it onto the graph to add it.



Working With Transforms

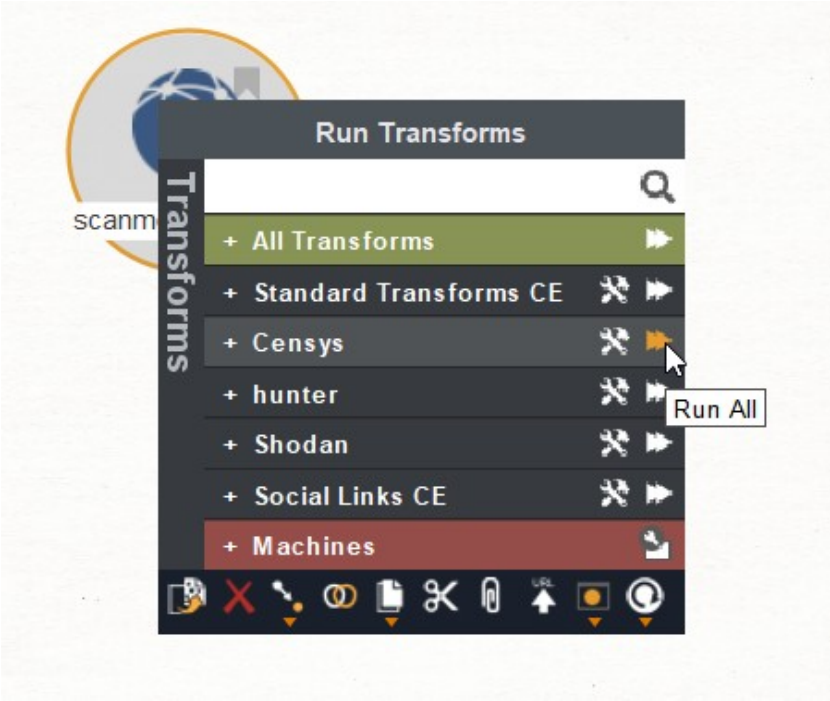
Now, we will show you how to work with different Transforms. For this demo, we will be using a domain name to perform various analyzes.
Search for "Domain" in the Entity Palette and drag it to the Graph. We will use **nmap.scanme.org** for the demo, so change the domain name from **maltego.com** to **nmap.scanme.org.**



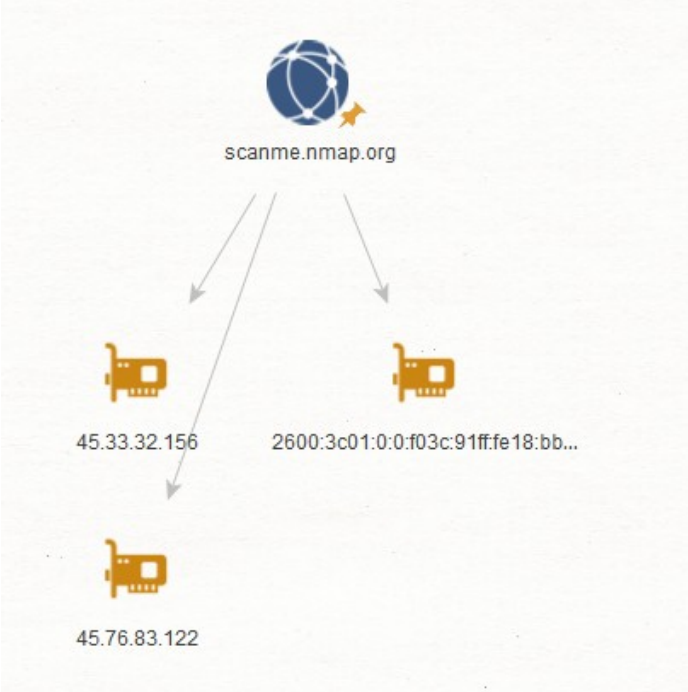
Let’s run our first Transform. Let’s run Censys to map an IP to the domain name. Right-click on the domain in the graph and select Censys. Then click the “**Run All**” button to run all the Censys Transforms simultaneously.

As a penetration tester, this information gathering technique during the information gathering phase can give insight into the organization's network structure and may reveal the relationships between different servers, such as mail servers and websites.

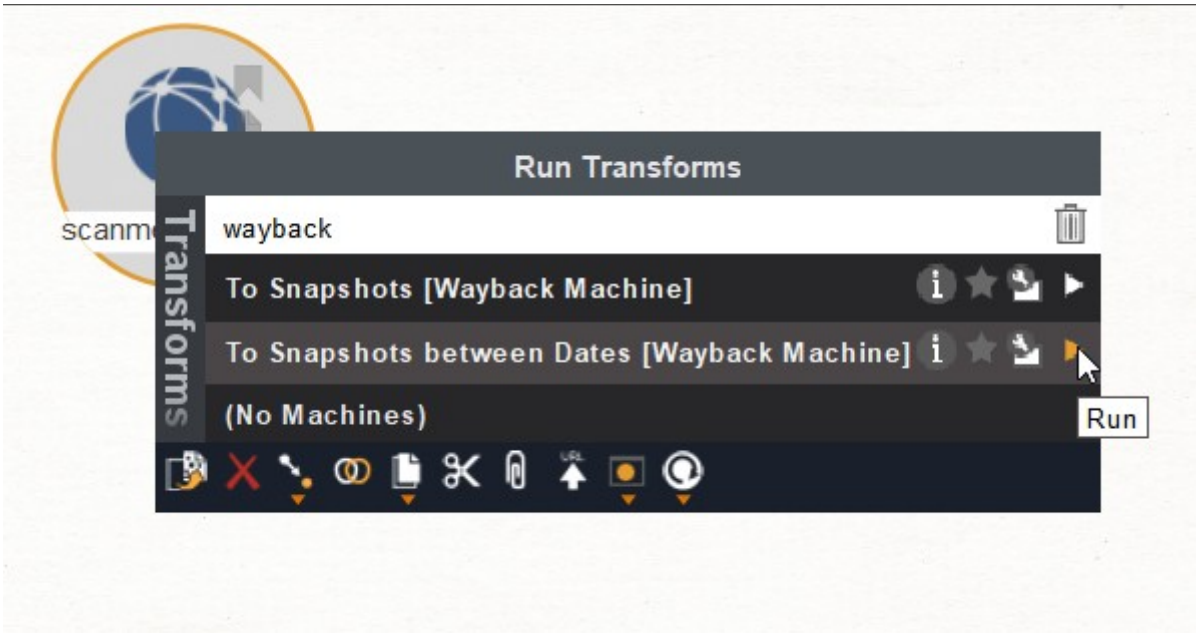
Read the steps involved in a penetration test in our article: Penetration Testing Steps: A Comprehensive Assessment Guide.



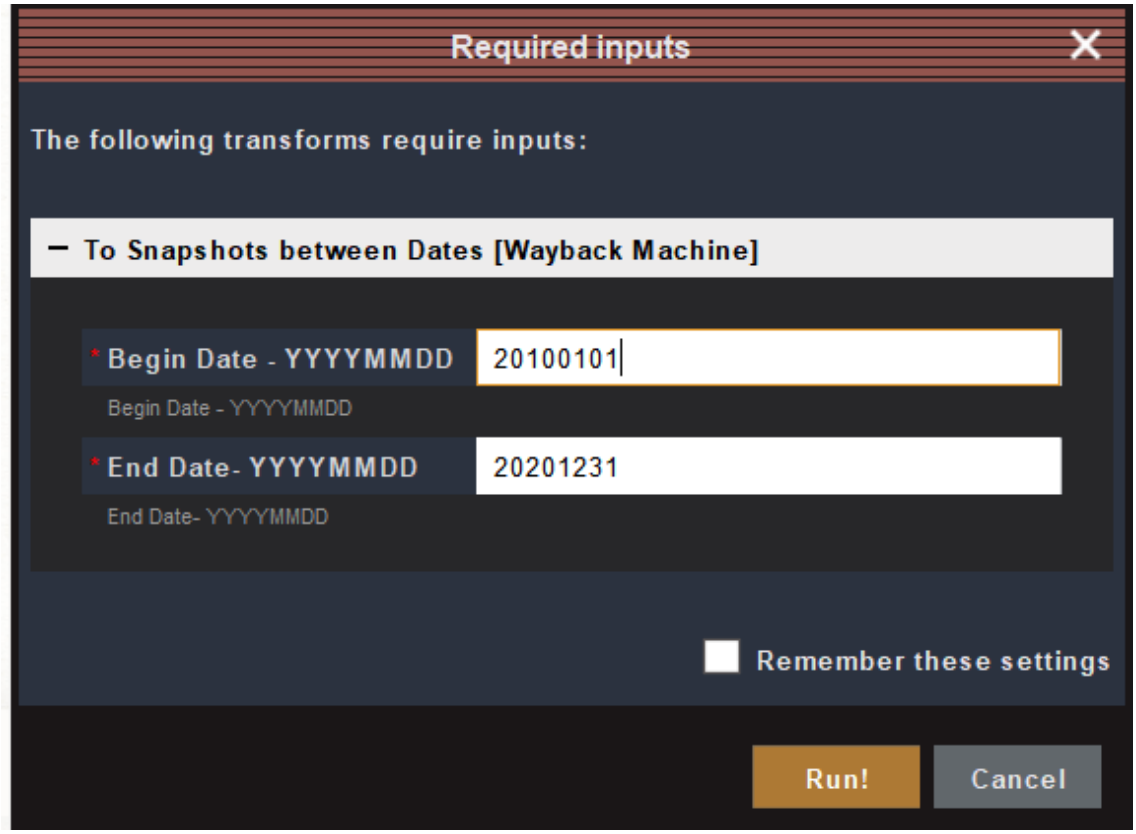
The Transform will run and present you with the IP information in the graph.



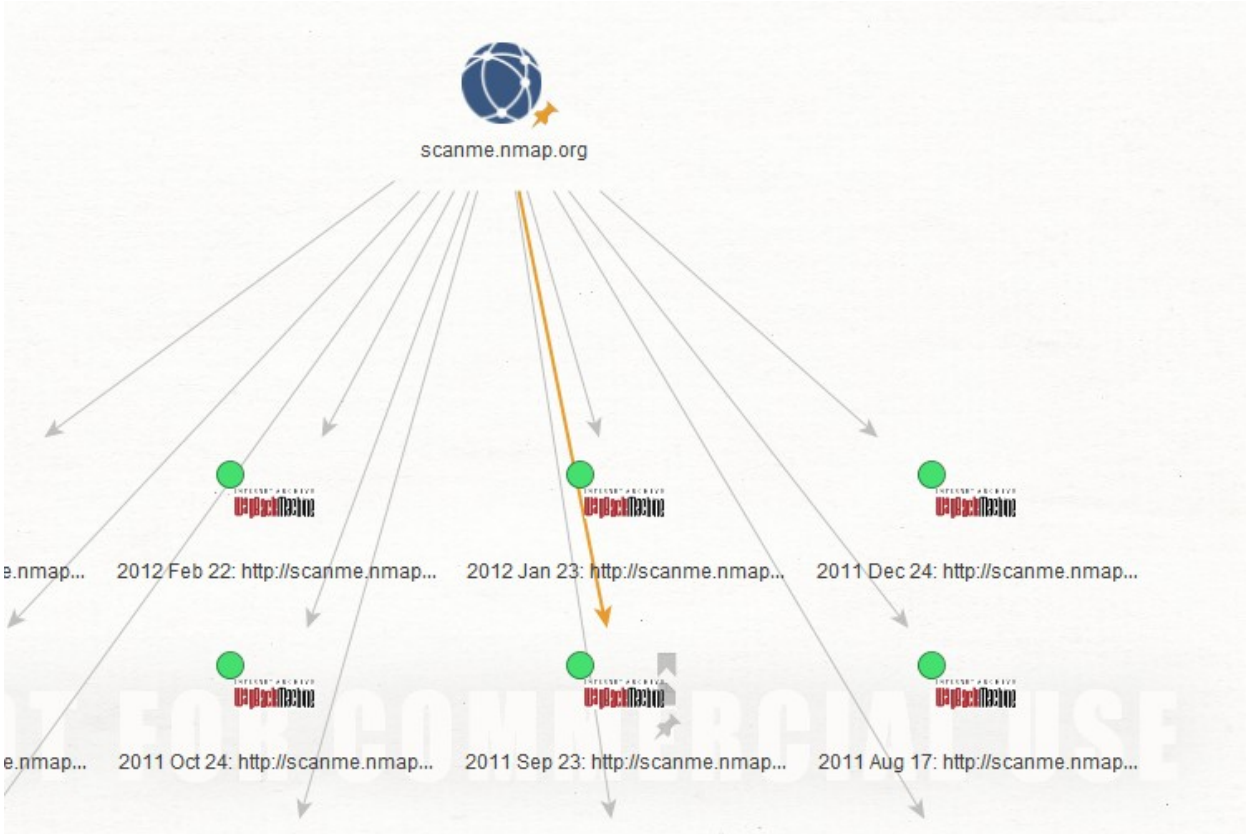
Now let's run another Transform. This time let's run the "**To Snapshots between Dates [Wayback Machine]**." This can be extremely helpful when performing a penetration test as it could reveal important information such as past vulnerabilities, changes in security configurations, deprecated or hidden pages, and subdomains. Right-click on the domain, and in the search bar, search for "**wayback**" then select "**To Snapshots between Dates [Wayback Machine],**" and finally click run.



On the next screen, choose the begin and end dates for the search and click Run!



Once the Transform completes, you will be shown the Wayback Machine data found. With this information, you could click on a specific date and open the URL for further information gathering and investigations.



Maltego is an extremely powerful tool and can do so much more than what we've shown you here. Using Maltego, you could map out the digital footprint of a target organization, including identifying key employees, emails, social media profiles, or devices.

This information can be used with tools like the **Social Engineer Toolkit** for information gathering. It can be used to create:

Phishing Campaigns: Information gathered about email addresses and social connections could aid in crafting **targeted phishing emails**.

Spear Phishing and Social Engineering Attacks: Insights into the relationships between entities might inform more advanced spear-phishing or **social engineering attacks**.

Best Practices

Let's talk about some Maltego usage best practices. Maltego is a very versatile tool that can do many things, and there are some things you can do to work more effectively and intelligently before and while using it. Our list of recommendations for working with Maltego is provided below.

- **Create a Strong Workflow:** Understand your goal before you start. Map out what you want to uncover and tailor your search accordingly.
- **Use Transforms Wisely:** Transforms are queries that fetch you different data types. Learn them well, and use only what's necessary. Too many unnecessary Transforms may clutter your results.
- **Secure Your Data:** Maltego can pull sensitive information. Make sure you handle it with care.
- **Stay Up to Date:** The digital world and tools like Maltego change rapidly. Regularly update to the latest version to keep up with new features and security enhancements.
- **Use Entities Properly:** Entities are the building blocks in Maltego. Use them correctly to represent the data you're working with.

- **Use Notes and Bookmarks:** You can attach notes to entities, connections and bookmark essential elements. This helps track why something is important or how you discovered it.
- **Export and Share with Care:** You can export your findings to share with others. But remember, this might include sensitive data, so only share it with those who need it.

- How to Conduct Person of Interest Investigations Using OSINT and Maltego

As paper trails turned digital, person of interest investigations have become a complex game of cat-and-mouse. It is becoming easier and easier for criminals and malicious actors to hide behind fake online identities. Navigating such a digital landscape can become challenging for law enforcement agencies and criminal investigators alike.

On the other hand, as many aspects of our lives depend on or exist only on the internet, we might be sharing information and details of our personal identities and private life without knowing. These digital footprints might seem and can often be harmless. In certain cases, however, they can also be points of vulnerability.

It is important for investigators to have effective methods and tools for mapping digital footprints—either for a criminal case or to protect a person of interest from external threats.

With Maltego, investigators can quickly and easily link seemingly disparate leads and build a comprehensive map of a target person's digital footprint. Integrated with a variety of OSINT, social intelligence, and identity data sources, Maltego is the perfect tool to quickly obtain and analyze the digital presence of a person of interest.

Table of Contents

- Conducting a Personal Recon Investigation
  - Step 1: Discovery
  - Step 2: Online Footprint
  - Step 3: Social Media Footprint
  - Step 4: Company Investigation
  - Step 5: Infrastructure Investigation
  - Step 6: Personal Sphere

Conducting a Personal Recon Investigation

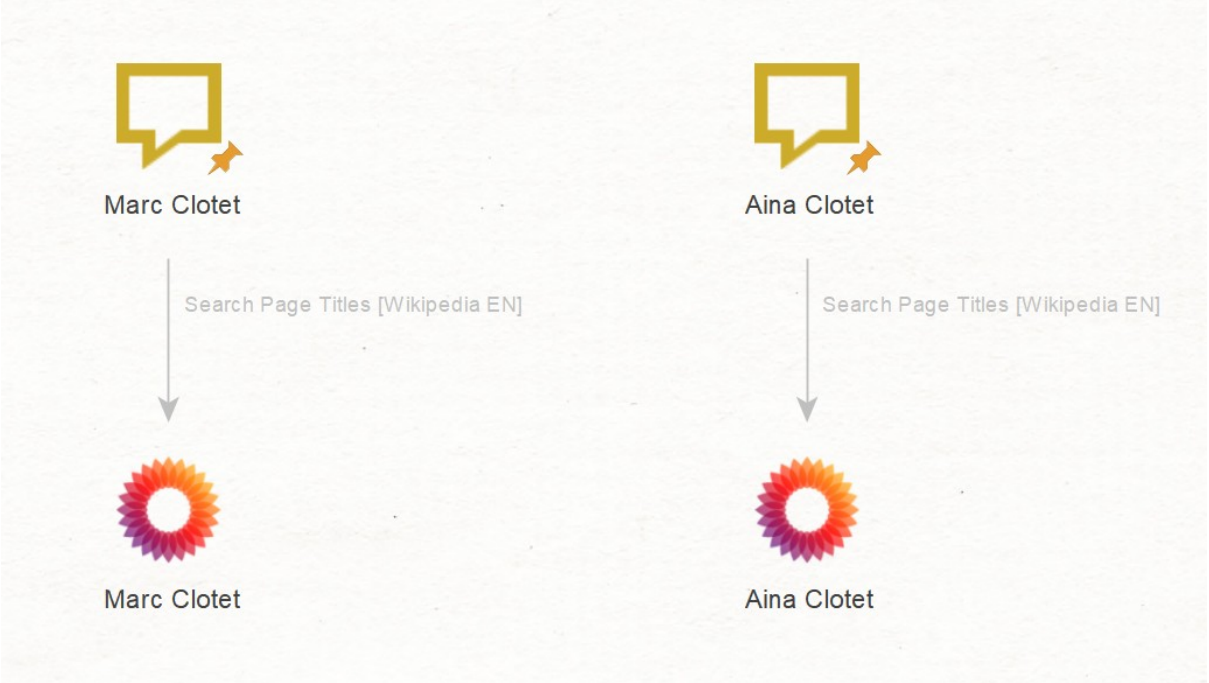
For this tutorial article, we'll explore the digital footprint of two individuals, Aina and Marc Clotet, by using **Maltego Data** and by following the six steps below:

First, we'll look for official information about the targets, such as their location and personal websites. Next, we will trace the digital trail left by our targets and then delve into their official and private social media profiles, gathering profile images and insights into their closed networks.

After that, we'll explore a company with which both targets appear to be affiliated. Next, we'll map the infrastructure of their websites in search of more detailed information, such as their personal email addresses. Finally, in the last step, we will utilize our findings to search for phone numbers associated with the targets.

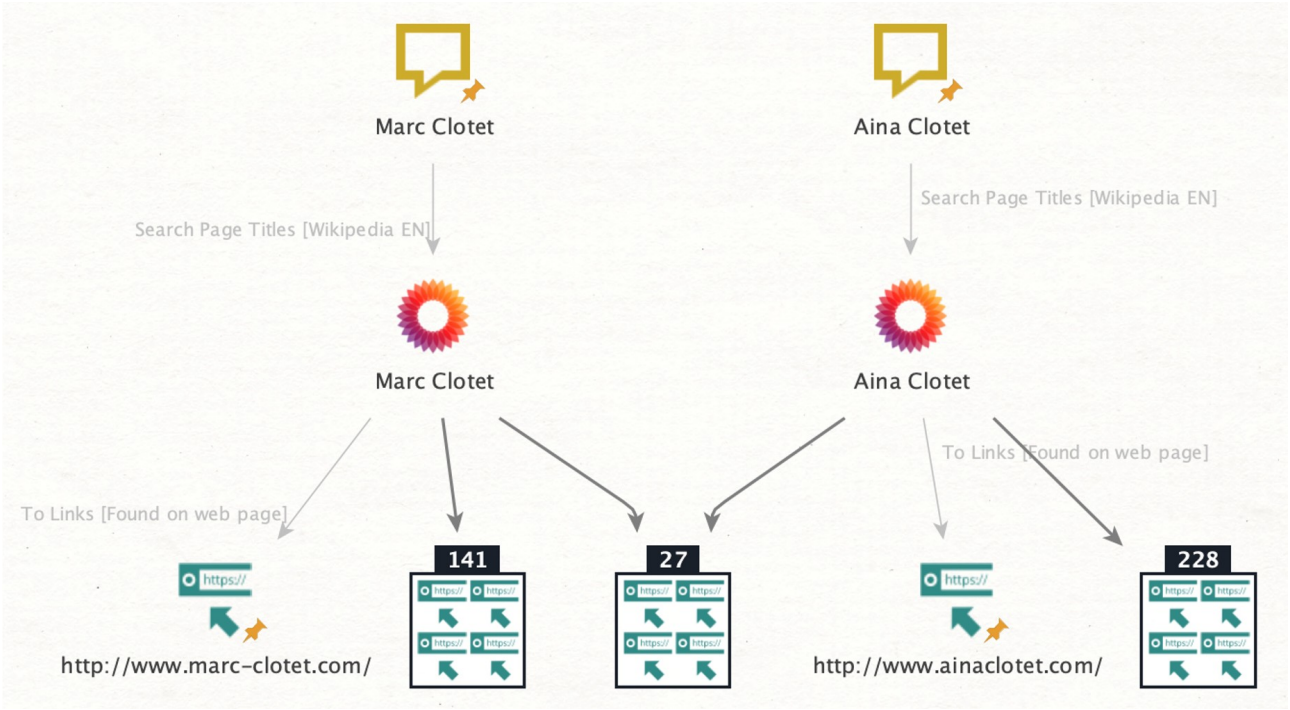
Step 1: Discovery 🔗

Our targets are actors who also happen to be siblings: Aina and Marc Clotet. We will begin our investigation by identifying some basic information and connections. First, we open a new graph in Maltego, paste the names of the actors as Phrase Entities, and run the **To Search Page Titles [Wikipedia EN]** to discover the official Wikipedia pages for both actors.

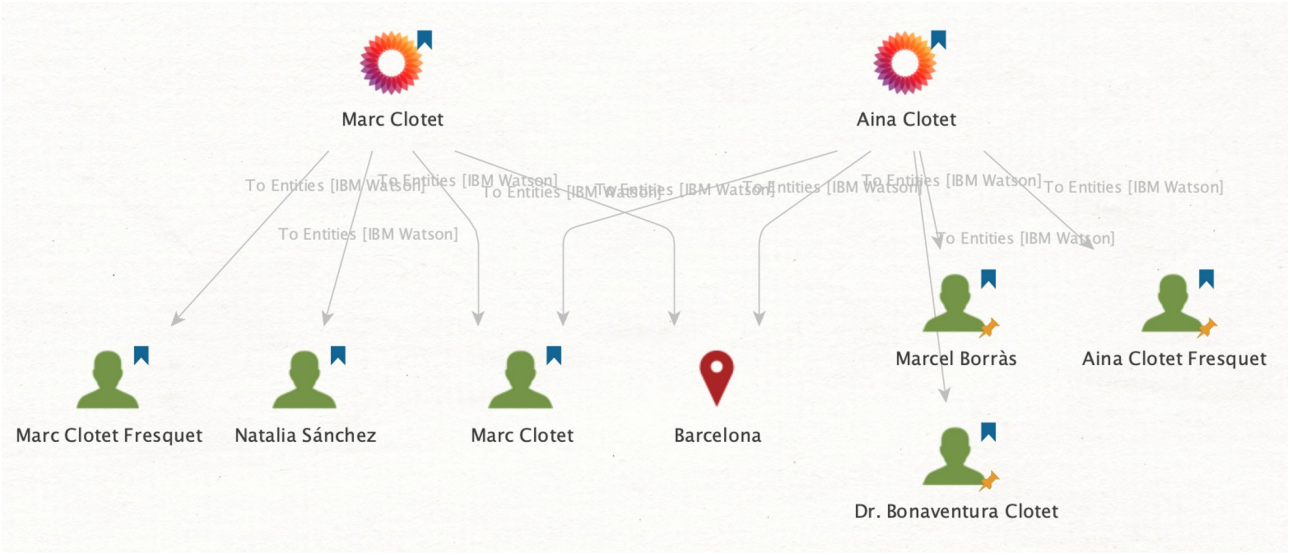


From there, we can run the **To Links [found on web page]** Transform to get a list of websites found on their respective Wikipedia pages. We will also get an overview of which websites are mentioned on both of their Wikipedia pages.

Two results are particularly relevant as they lead to the official websites of Aina and Marc Clotet: "**www.ainaclotet[.]com**" and "**www.marcclotet[.]com**." They will serve as starting points in the later stages of this investigation.



Apart from searching for websites, we can also extract other relevant information mentioned on the official Wikipedia pages, such as locations and names.
To do that, we will run the **To Entities [IBM Watson]** Transform.



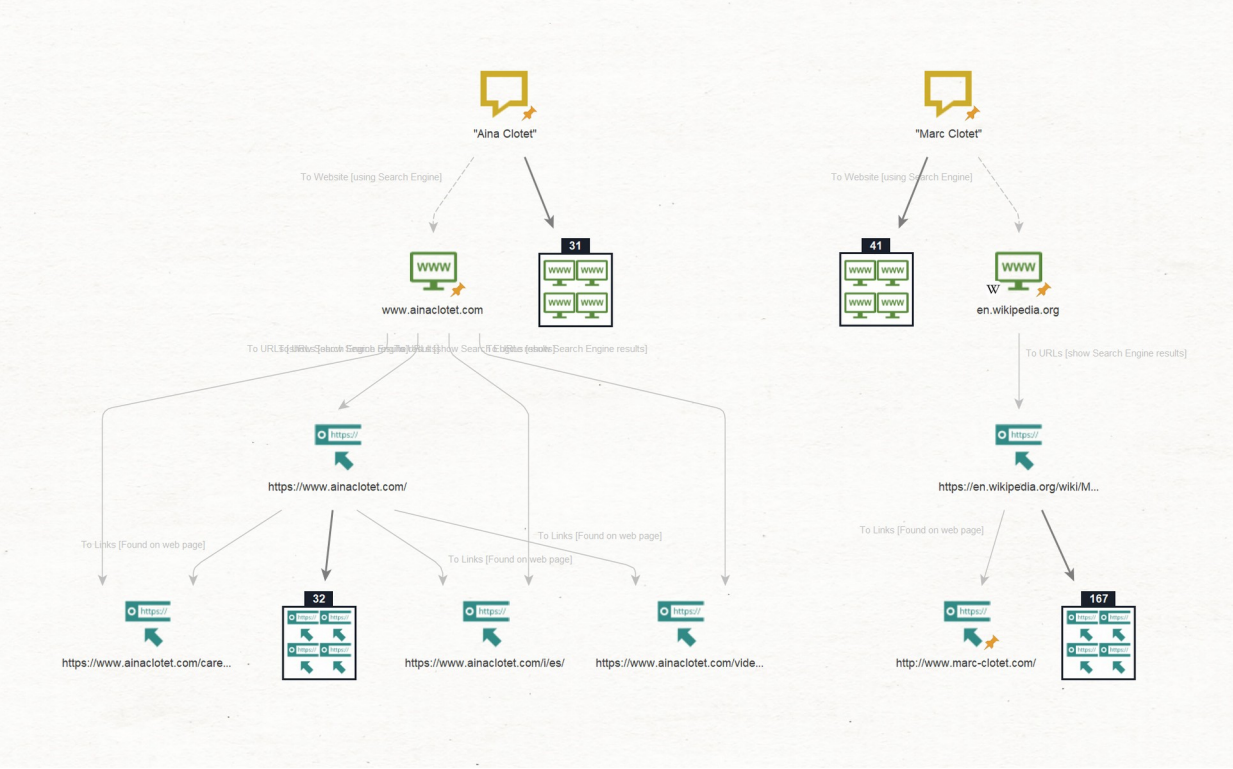
In doing so, we retrieved a list of names potentially linked to our targets and a location shared by both actors (**Barcelona, Spain**).

Step 2: Online Footprint 🔗

We will start our next step by dragging a Phrase Entity into a new graph and adding the actors' names in inverted commas to limit the search results down to exact matching. This is a common search dorking technique to increase the relevance of a web search.

Our goal is to find websites associated with our targets using the Maltego Standard Transforms.

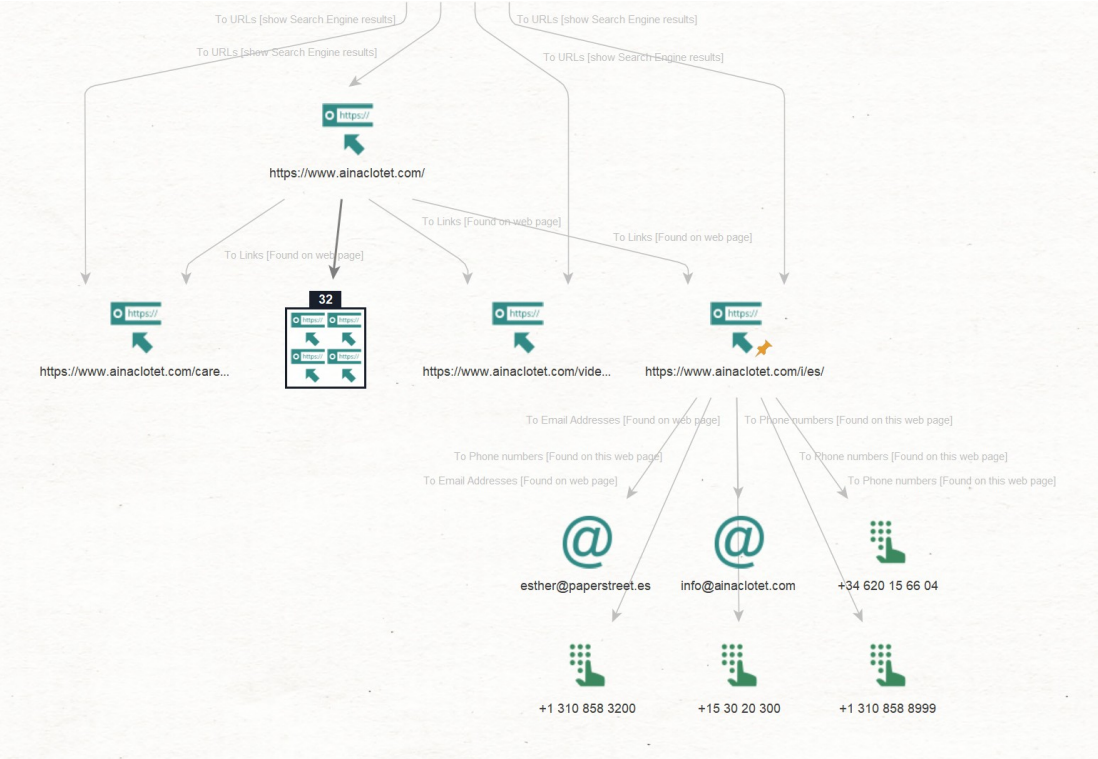
We do this by first running the **To Website [using Search Engine]**, then the **To URLs [show Search Engine results]**, and finally the **To Links [Found on web page]** Transforms.



These Transforms return a list of websites where the names "Aina Clotet" or "Marc Clotet" are mentioned. They include documenting websites such as Wikipedia, as well as a personal website we also saw in the first step, namely "**ainaclotet[.]com**."

We will now try to extract contact information that is usually embedded in the website footer. It can serve as a starting point to investigate professional contacts of our target, aiding in profiling and potentially uncovering connections to their secondary or hidden profiles.

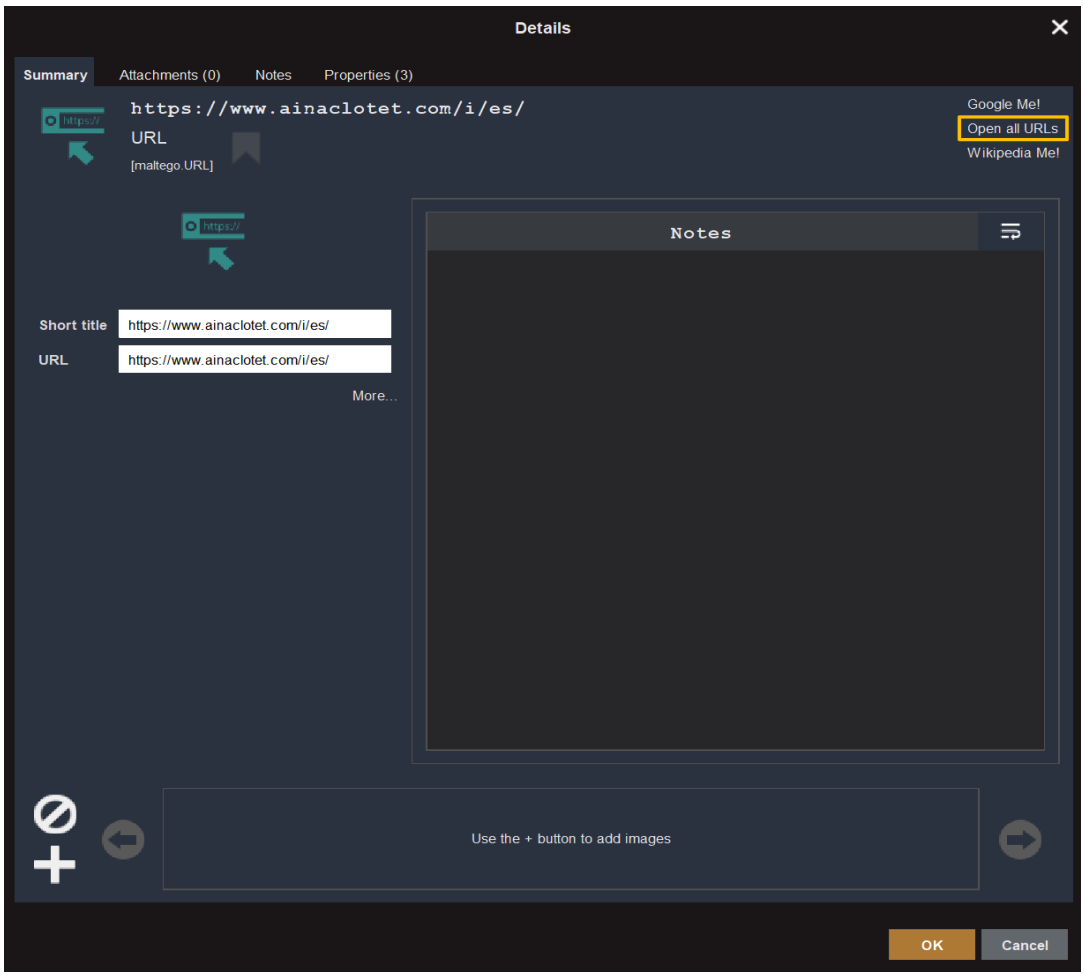
As an example, we will use the identified Entity “ainaclotet[.]com/i/es/” and run the **To**



Email Addresses [found on webpage], and **To Phone Numbers [found on webpage]** Transforms.

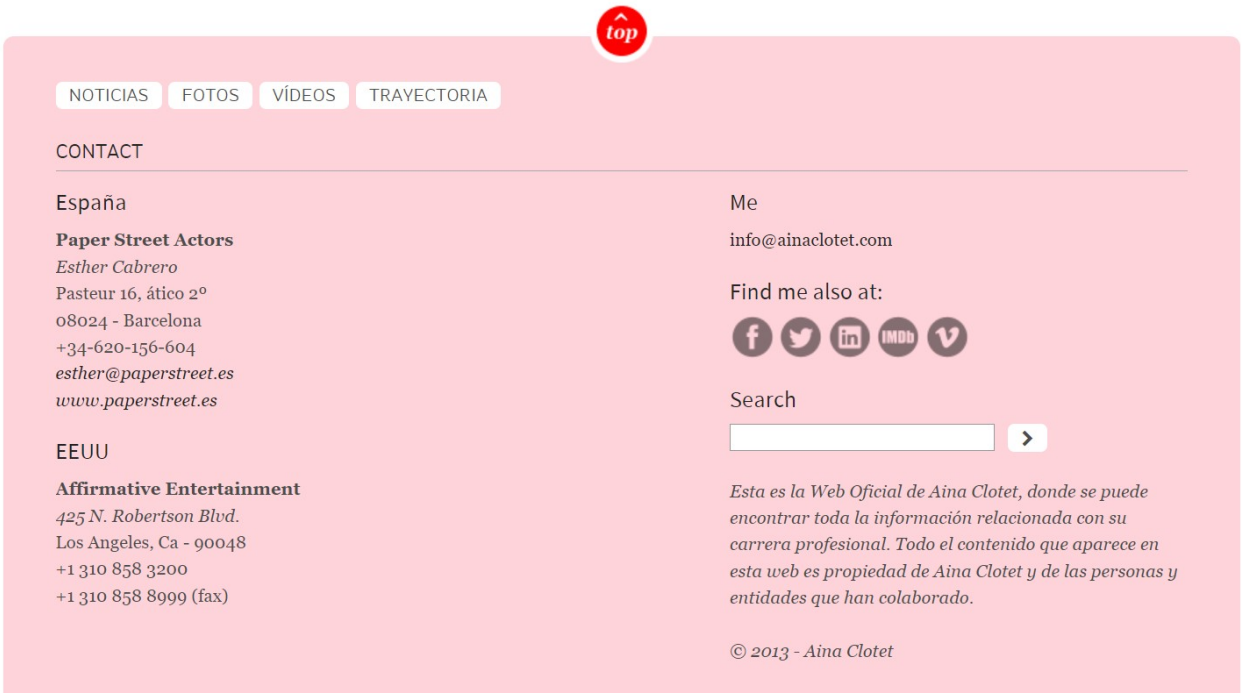
Maltego returned a collection of Entities pointing to email addresses (such as “esther@paperstreet[.]es”) and phone numbers that are likely linked to talent managers.

To verify the retrieved data, we can double-click on the Entity on which we ran the Transforms and view the page by clicking on “Open all URLs.”



NOTE: Within Maltego, you can open retrieved URLs in the browser. Analysts can use this feature to document other relevant information, such as date of birth, names of family members, or country of residence available on those websites. This data can be important in the later stages of your investigation.

As we open the website and scroll down to the bottom of the page, we can observe the contact details of Aina’s representatives, thereby confirming the results obtained through Maltego.



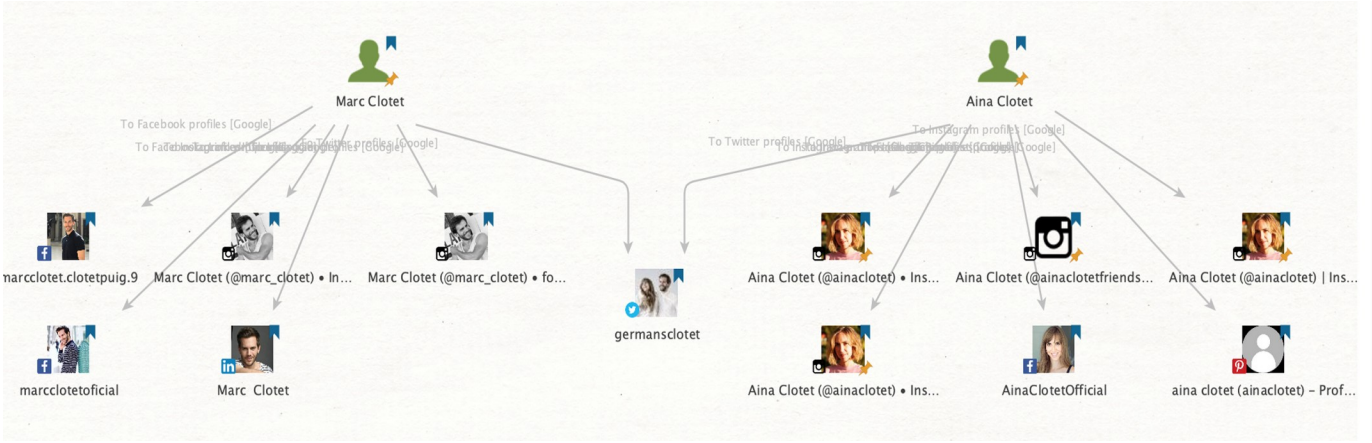
Retrieved phone numbers and email addresses may also prove important in later stages of the research, so keep that in mind when you launch your own investigations.

Step 3: Social Media Footprint

Now, we will try to map the social media profiles of our targets. Let us open a new graph and start with two Person Entities.
This time, instead of applying dorking techniques, we will use a variety of Maltego Transforms tapping into social media intelligence (SOCMINT).

We will begin with the **To Social Media Profiles** Transform from the Google Social Network Transforms.

After refining the graph to display only relevant Entities, we can see a couple of accounts registered on popular social media platforms with photos of our targets.

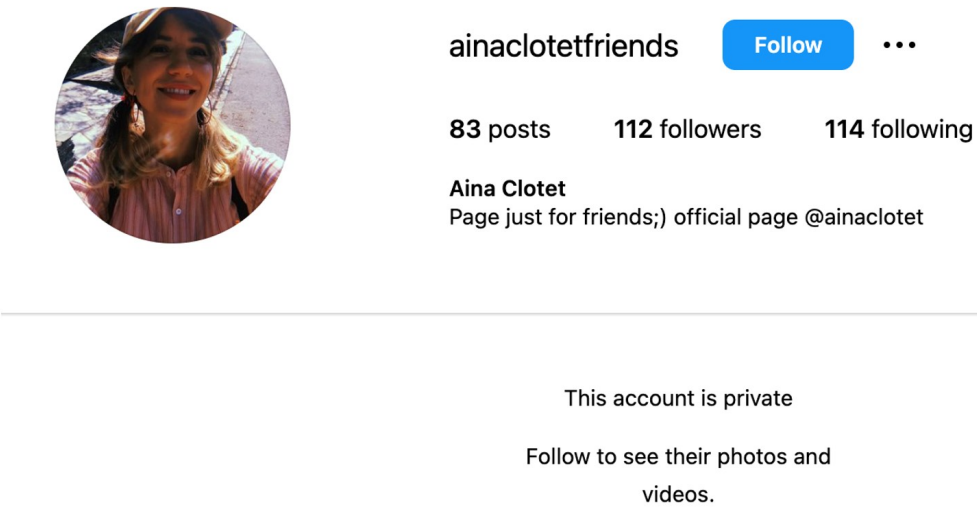


If you take a closer look at the profiles, you will discover that these accounts are usually public and have thousands of followers. We can also easily list some of the aliases used across the platforms, such as “marc_clotet,” “marcclotetoficial,” “ainaclotet,” or “AinaClotetOfficial.”

Preview of Marc's official account on Facebook

The official accounts are often marked by checkmarks to show that they are verified and recognized by the public person.

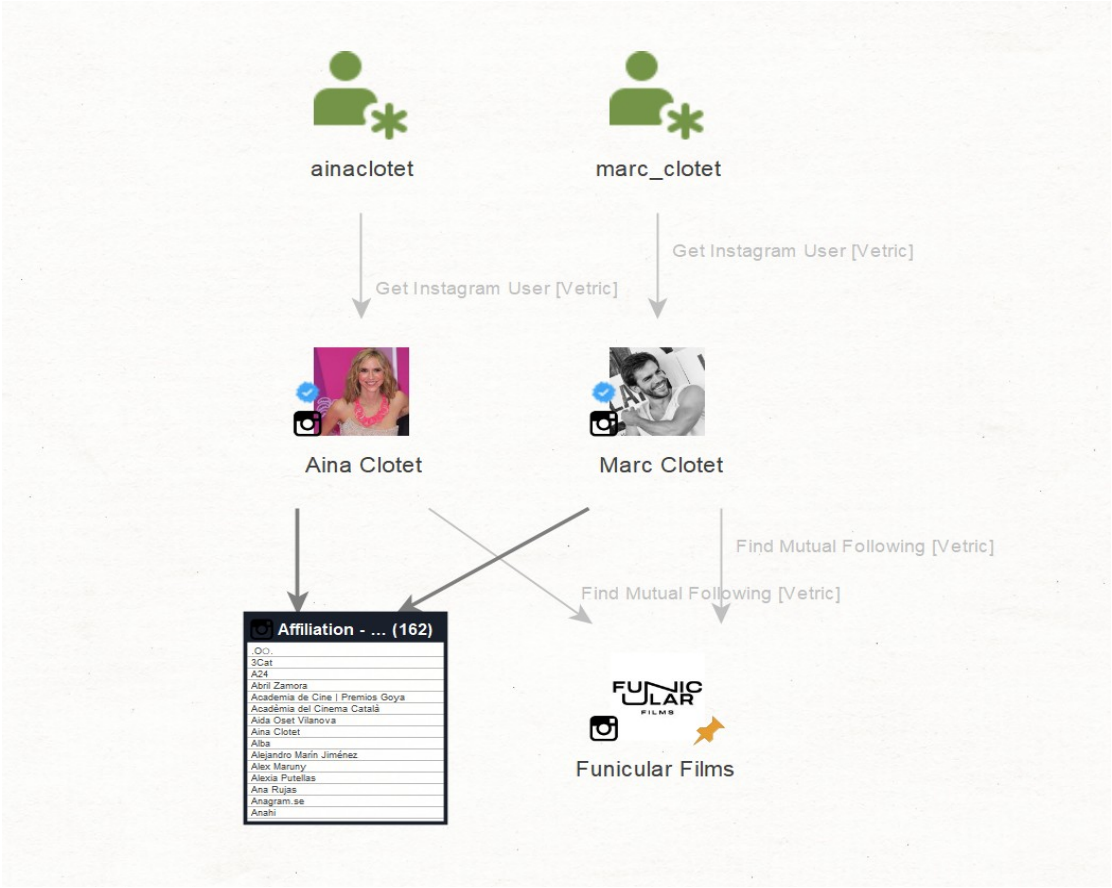
We do, however, seem to have identified a personal Instagram account named "ainaclotetfriends" with the accompanying biography, "Page just for friends;) official page @ainaclotet."



Preview of Aina's personal account on Instagram

Since it has become quite common these days for public figures to use Instagram for both private activities and public promotion, we will now focus on mapping their Instagram activities and mutual connections.

We will first use the previously discovered usernames “ainaclotet” and “marc_clotet” to extract the Instagram Entities on a new graph using the **Get Instagram User [Vetric]** Transform. Then, we will map out the profiles they follow and those that follow them back by running the **Find Mutual Following [Vetric]** Transform.



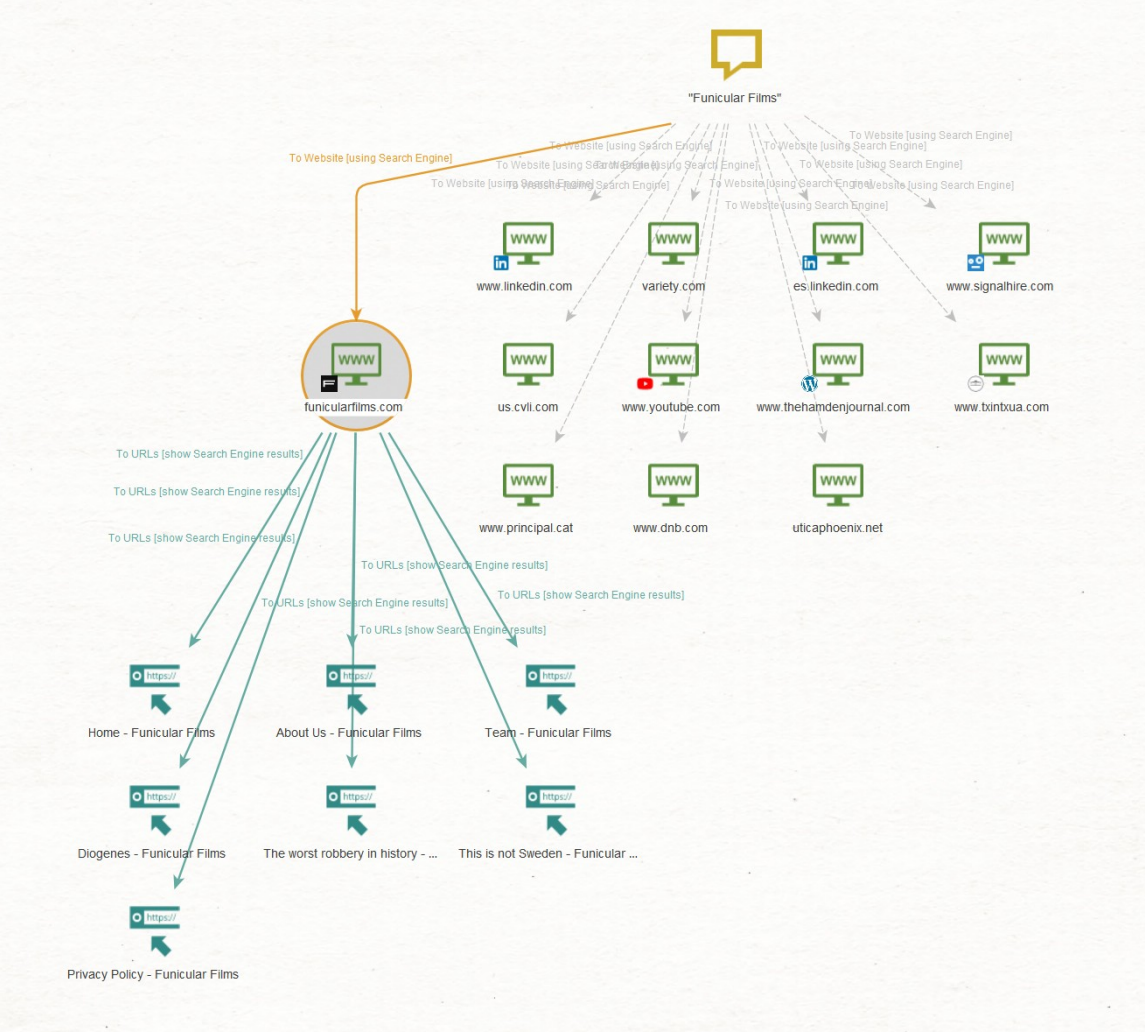
The Transform returned a large number of relevant profiles, such as the Instagram account of what appears to be a company named “Funicular Films.”
We also stumbled upon following relationships to private accounts, indicating a potentially close relationship between the owners of those accounts and our targets, especially since these accounts also follow the targets back. This discovery could serve as a valid starting point for further investigations of a similar nature.

Step 4: Company Investigation

In a person of interest investigation, it is also important to consider the professional relationships and affiliations of our targets.

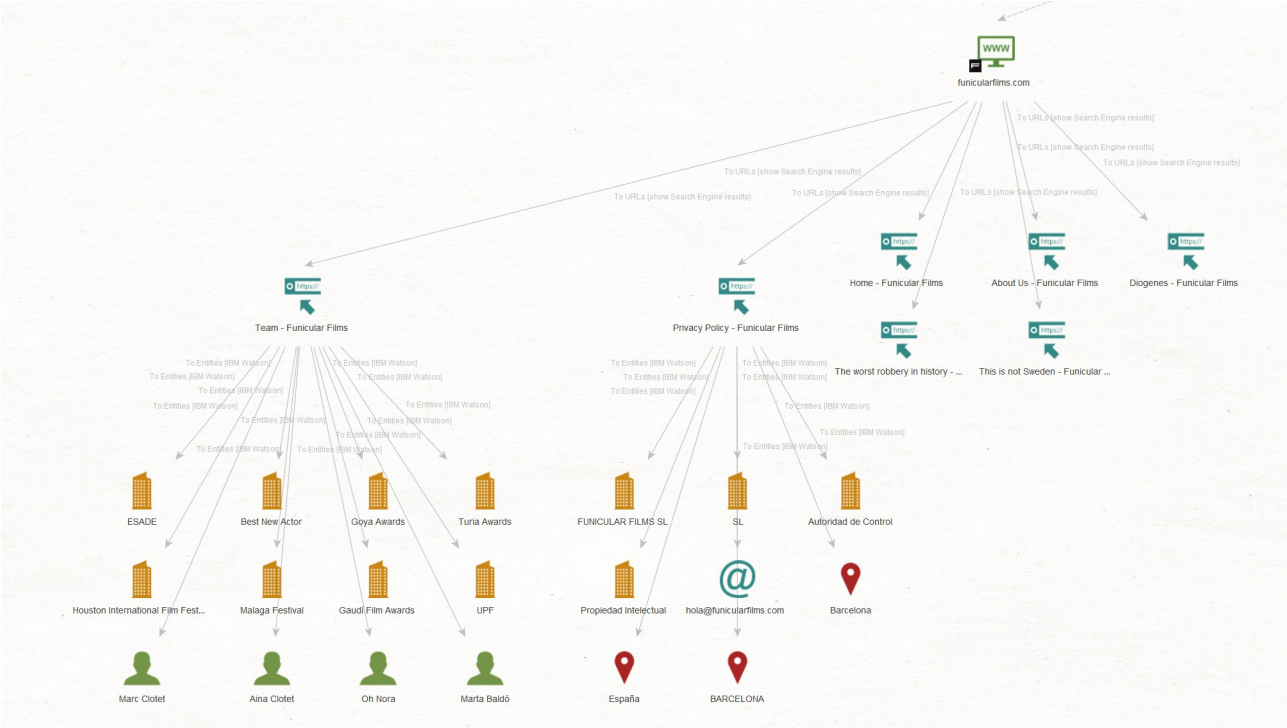
In the previous step, we found a link to the entity “Funicular Films,” which appears to be the name of a company. Let’s follow this lead and examine how it connects to our targets.

We will open a new graph and run the **To Website [using Search Engine]** Transform on the “Funicular Films” Phrase to find the official website of this Entity and the **To URLs [show Search Engine results]** Transform to find relevant pages.



There are two pages under the “funicularfilms[.]com” website that caught our attention: “Team – Funicular Films” and “Privacy Policy – Funicular Films.”

We want to explore the first one to find information on the company's officers and the latter to obtain information about the company's legal name. To do that, select both Entities and run the **To Entities [IBM Watson]** Transform.



We see that our targets are affiliated with the company they follow on social media, thereby confirming the accuracy of our investigation results.
Additionally, we have identified other officers linked to this company as well as its legal name – "**FUNICULAR FILMS SL**," which seems to be based in Barcelona, Spain. This aligns with the location of the actors we discovered in Step 1.

If we wanted to delve deeper into the company or its officers, or if we wished to investigate another company in a similar manner, we could also make use of specific Transforms from OpenCorporates or Orbis – Bureau Van Dijk, which are designed specifically for conducting company investigations. However, for our current investigation, we want to primarily focus on exploring the online presence of our targets.

Step 5: Infrastructure Investigation

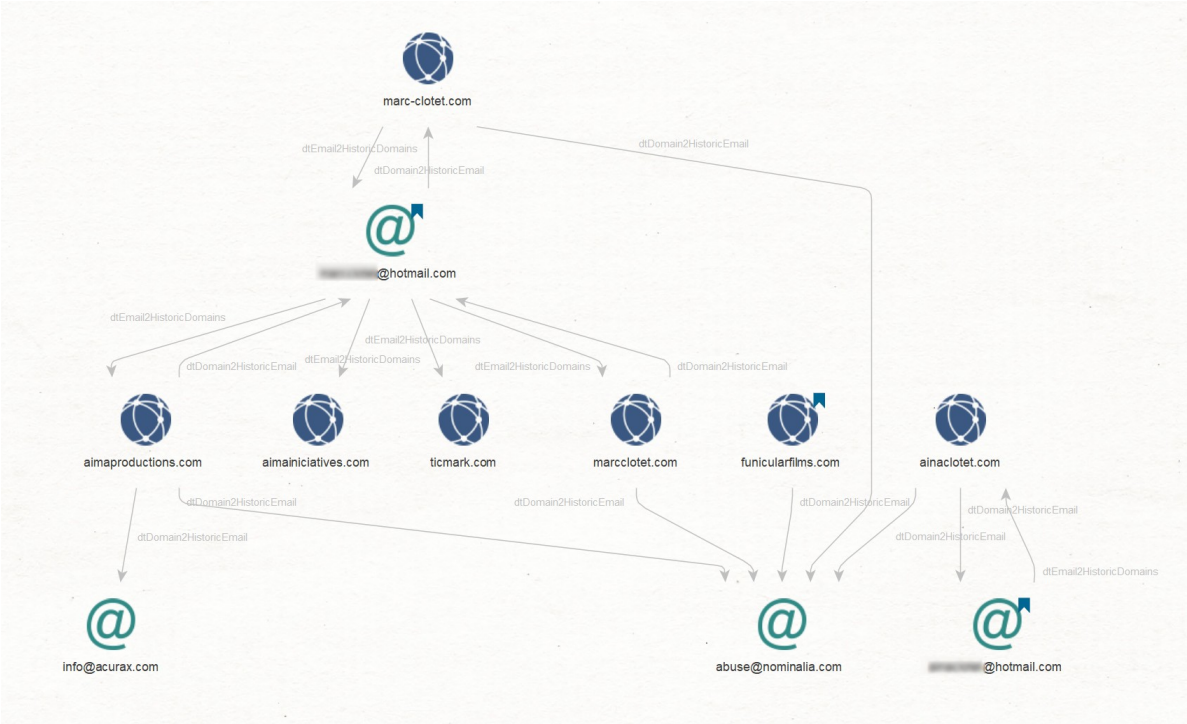
This part of our investigation will focus on a couple of domains discovered in Step 3. Our goal is to find associated email addresses and other domains that link to those email addresses.

In a new graph, we will paste the following website domains as Domain Entities onto the graph:

- **ainaclotet[.]com**
- **marcclotet[.]com**
- **marc-clotet[.]com**
- **funicularfilms[.]com**

We will now use the DomainTools data source, which contains domain registration records known as Whois information, to search for email addresses associated with those domains by running the **dtDomain2HistoricEmail [DomainTools]** Transform.

Next, we find other domains registered with the same email addresses with the **dtEmail2HistoricDomains [DomainTools]** Transform.



The reason why we use historic search is because it was a common practice in the past to set up websites using personal emails. Over time, the ownership of these domains may have changed, especially due to the increased popularity of our targets. While the current, up-to-date website registry information might not help our investigations, the historical data from DomainTools can still provide the insights we need.

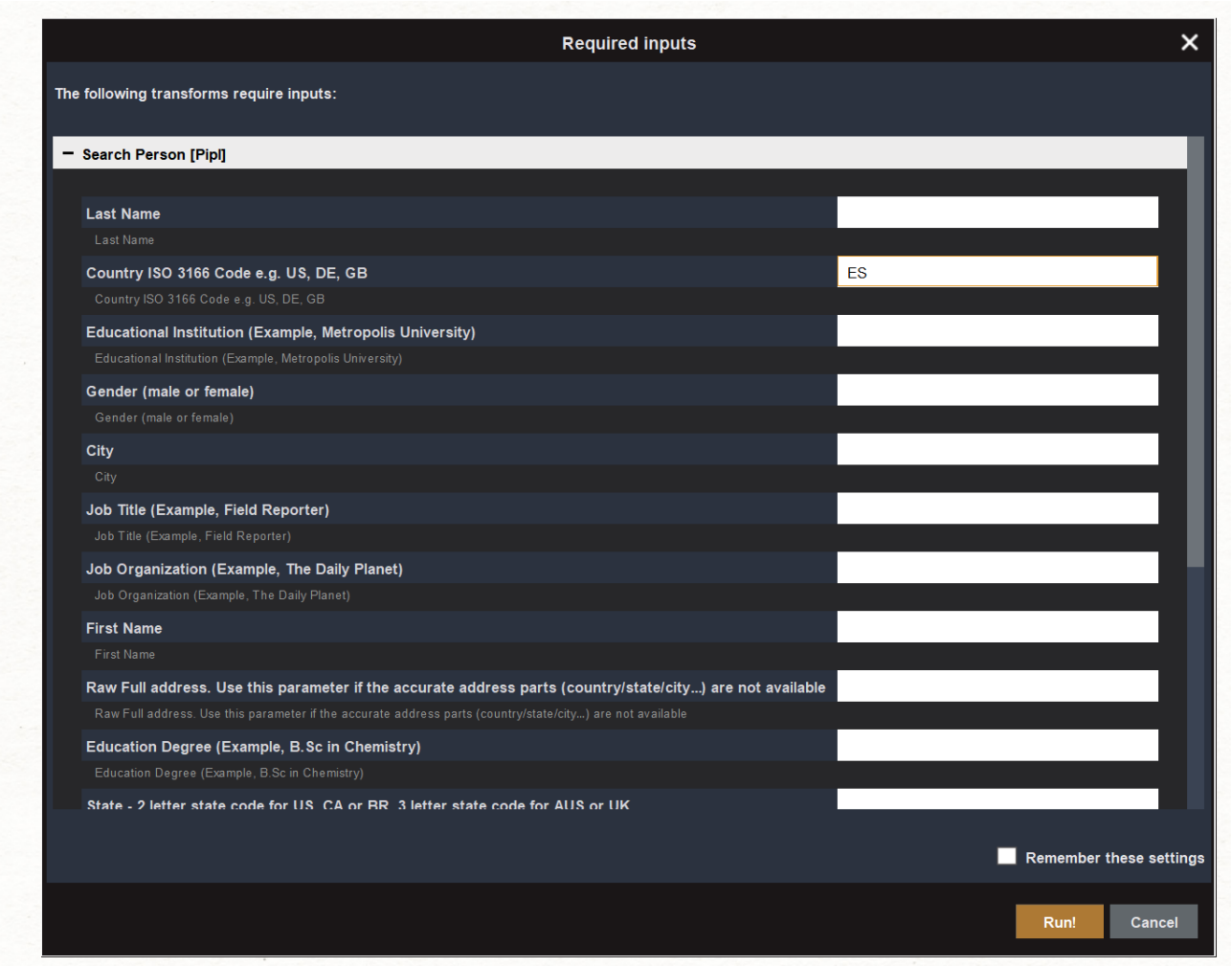
Among the email addresses we find, two of them seem to be their personal Hotmail email addresses.

This information holds great value in person of interest investigations as it enables us to find out more about a person's online footprint and uncover more specific identity intelligence.

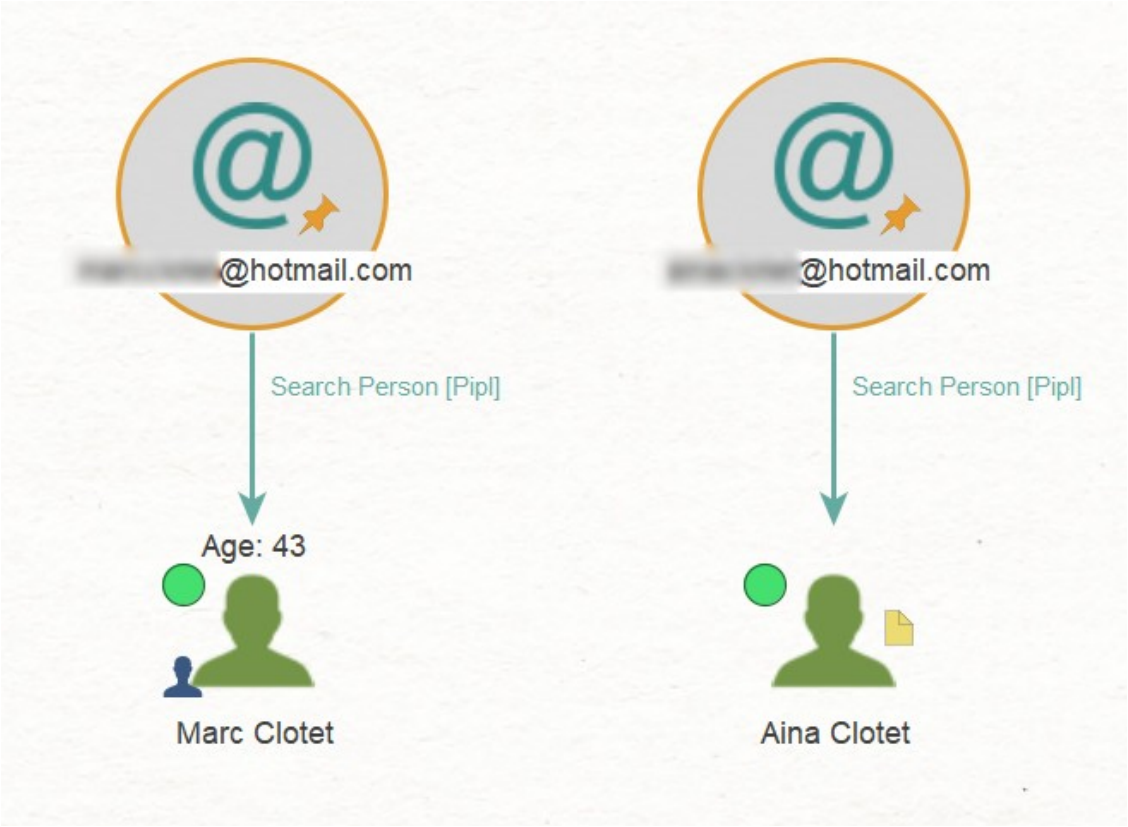
Step 6: Personal Sphere

In the final step, we will take our recent finding, namely, the targets' private email addresses, and pivot from them using the **To Search Person [Pipl]** Transform to find matching person profiles.

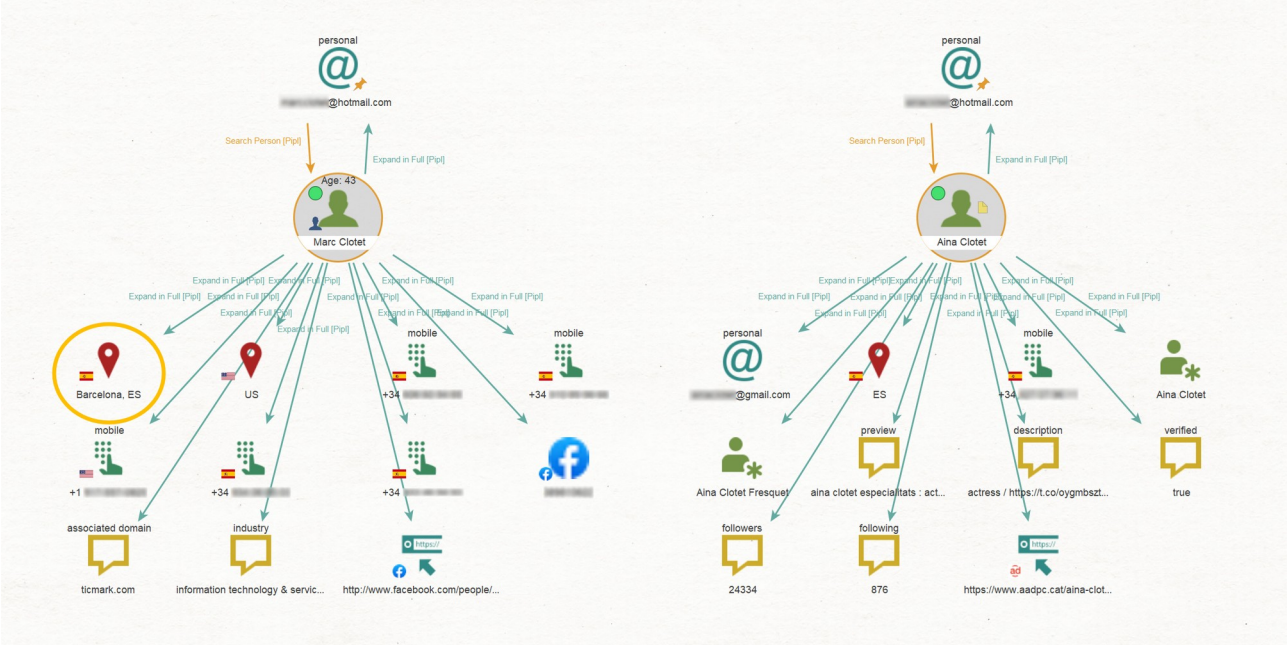
To narrow down our search and find an exact match, we can provide additional information in the wizard, such as the country code "ES" for Spain. Since we have already established a connection between the actors and Barcelona, Spain, including this data will help us refine our search.



Maltego retrieved the names of Marc and Aina, indicating that the email addresses likely belong to them. Interestingly, the search also yielded the most probable age for Marc, which is 43.

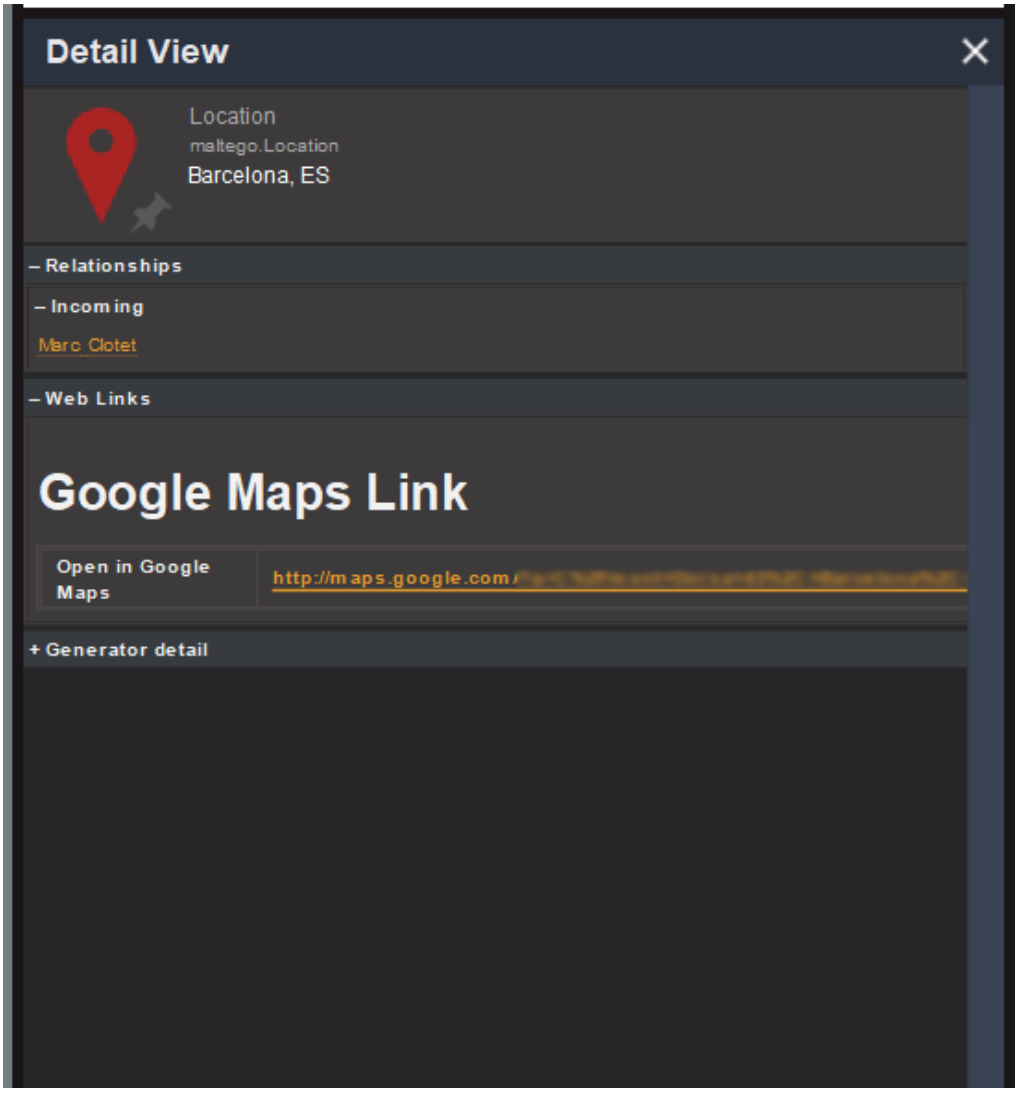


Let’s delve deeper into their profiles and discover more information by running the **To Expand in Full [Pipl]** Transform.



Our findings include Aina’s personal Gmail address, a collection of phone numbers, and locations associated with our targets.

In fact, we can also see the precise address of the location connected to Marc in the Detail View, which appears to be a private house when viewed on Google Maps.



We also managed to obtain a URL leading to a website that contains Aina's profile, featuring additional personal information such as her photo, educational background, and the languages she speaks.

Què necessites trobar?

aadpc Associació d'Actors i Directors Professionals de Catalunya

Català Castellà Iniciar Sessió

L'AADPC Notícies Agenda Publicacions Guia de professionals Àrea legal Borsa de Treball Cursos Cartellera Enllaços d'interès Contacte

Aina Clotet

PRESENTACIÓ

CONTACTE

ESPECIALITATS :
Actor/Actriu

ALTRES ESPECIALITATS:
dansa, comunicació audiovisual

ESTUDIS:
Estudi Nancy Tuñon, École Philippe Gaulier, cursos varis de reciclatge professional

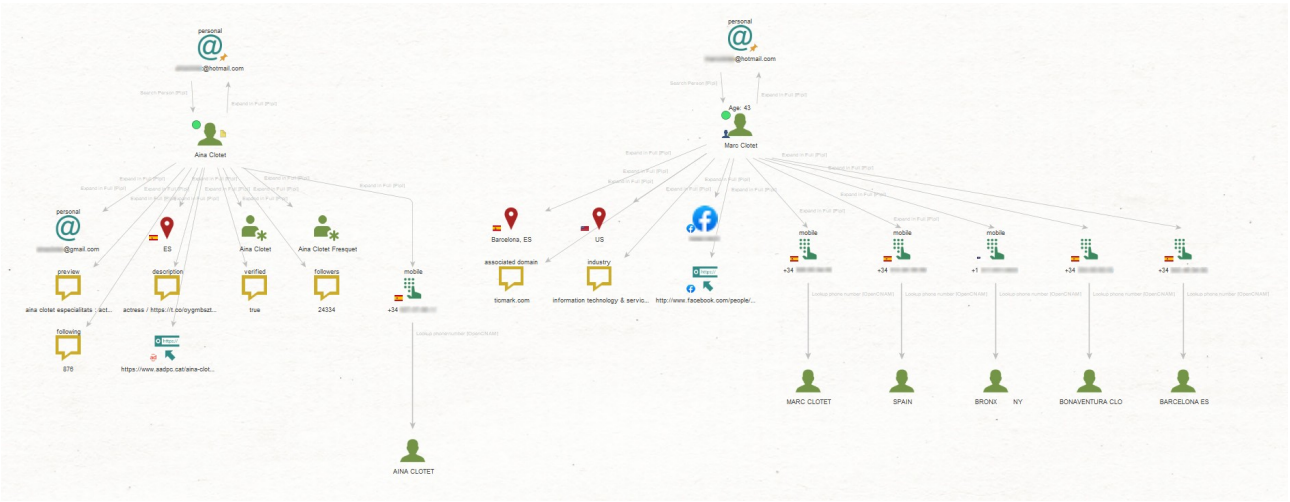
EMAIL:
ainaclotet@gmail.com

WEB:
wwwainaclotet.com

IDIOMES:
català, castellà, anglès, francès

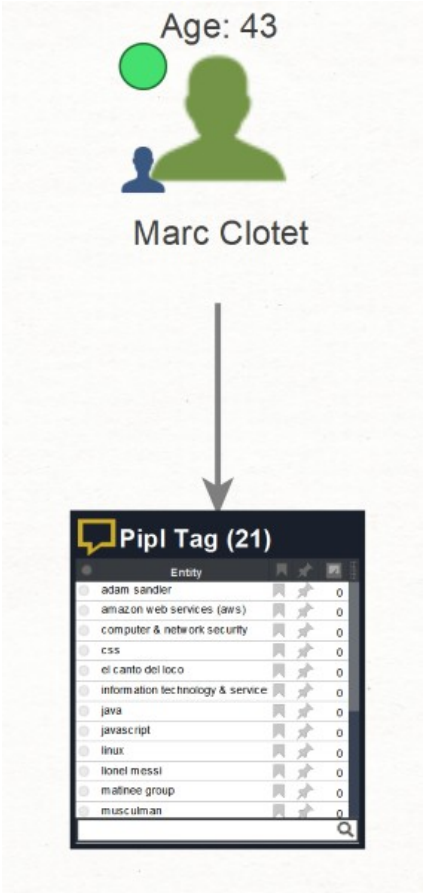
CONTACTE

As the next step, we wanted to verify the retrieved phone numbers employing the **To Look up phone number [OpenCNAM]** Transform.



This led to discovering Entities associated with the numbers, revealing details such as the names of our targets, location indicators, and the name of their father.

What could also prove interesting are the Pipl Tag Entities (**To Tags [Pipl]** Transform). These Entities represent the hobbies, interests, and other notable information about the targets.



While these particular interests are harmless, little nuggets of information like these from a person's past (or present) can help us to glean a complete picture of, and get closer to a person and his or her interests.

Enrich Your Person of Interest Investigations with More OSINT Data

You have reached the end of the example of a personal recon process that investigators can perform using Maltego.
To quickly recap, we started with two names to discover their personal websites, location, and family member names.
We further explored their online presence, uncovering associated websites and domains. Then, we identified their official and private social media accounts with profile pictures and delved into their network of social contacts.

Moving forward, we investigated a company affiliated with both targets and traced domains connected to our targets back to their personal email addresses. Finally, we used those email addresses to find more detailed personal information, including private phone numbers and a home address, which added another layer of understanding to our investigation.

Pivoting to Other OSINT Data

From the different Entities returned to our graph, we could of course investigate deeper and wider, such as pivoting into a reverse image search or conducting a network footprint using the targets' email addresses. This would help us to map an even more extensive online and infrastructure network of the person of interest.
If we are conducting the person of interest investigation for fraud, we could also look at the target's business relationships using the OpenCorporates and WhoisXML data integrations. We showed such a use case in our joint webinar with Pipl.

REFERENCE

- StationX: https://www.stationx.net/how-to-use-maltego/

-Maltego: https://www.maltego.com/blog/how-to-conduct-person-of-interest-investigations-using-osint-and-maltego/

===>> Success your goal in cybersecurity fields.

Contact:

Gmail: ninkanong2006@gmail.com

Telegram: @ninkanong

Facebook: នីន កាណុង(Nin Kanong)

Tel: 0978297806