**Advanced Open Source Intelligence (OSINT) Techniques**

**Authors:**

Juan Camilo Velandia Botello

José Alejandro Naranjo Guzmán

Advanced Open Source Intelligence (OSINT) is a branch of cyber intelligence that uses public data and unrestricted access to profile an adversary, and thus be able to perform a cyber defense strategy appropriate to the motivation and means of the potential attacker in order to prevent future attacks.

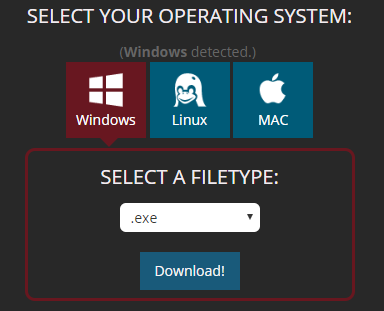
The OSINT has two main phases, the first is the collection of data, and the second is the analysis of data using machine learning models.

In this laboratory we will focus on the collection of information (Transforms) and its preparation, in order to have it ready for later analysis. This task will be carried out by means of the tool "Maltego", which allows us to search for all the information around a single starting point (Entity) and then pivot from it to carry out a new search and obtain more information.

To begin with the use of the tool it is necessary to understand the concepts of transformed and entity, because the laboratory will focus on these.

An entity is an abstraction of a real-life element, whether simple or compound, this can be the starting point for starting the collection of information. You can start exploring with either an account on a social network, or a person's identification number. A transform is a piece of code that leads from one entity to another.

1. Download and install Maltego. https://www.paterva.com/web7/downloads.php



1. We are going to use a native transform from Maltego.

* Run the tool



* In product selection we select the Community Edition version of Maltego.

|  |
| --- |
|  |

* You must create an account.

|  |
| --- |
|  |

3. Let's investigate a person on Twitter.

* drag the entity "person" to the graph.

|  |
| --- |
|  |

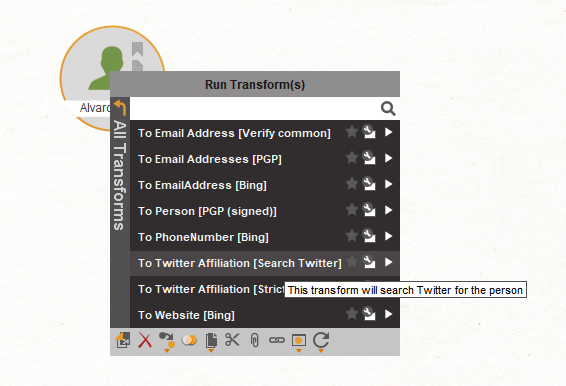
* Double click on the entity person.

|  |
| --- |
|  |

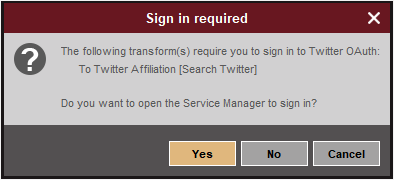
* We change the person’s name. In this example, we are going to investigate Alvaro Uribe.

|  |
| --- |
|  |

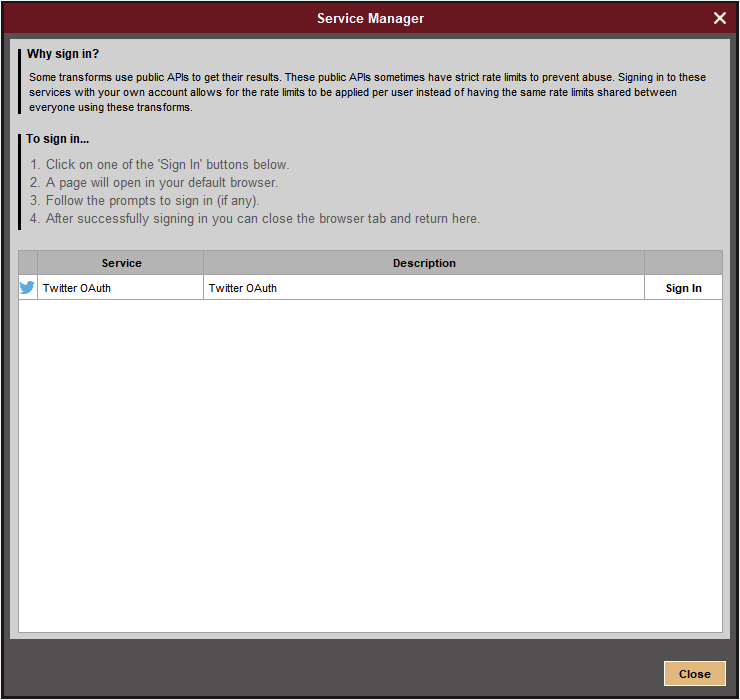
* Right click on the entity, and we run the transformed "ToTwitterAffiliation".



* The following message will appear, right click on Yes option.



* For this, we must link the twitter account (a fake one) to Maltego.



* when we have linked the account, the following window will appear.

|  |
| --- |
|  |

* Maltego will build a tree of twitter account entities related to the person named "Alvaro Uribe".

|  |
| --- |
|  |

* With the transforms offered by Maltego, we can research, the alias, followers, the latest tweets that the person has written, etc.

Alias and latest tweets.

|  |
| --- |
|  |

Friends on twitter.

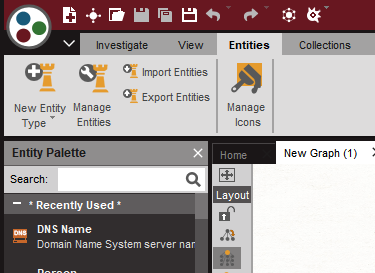
|  |
| --- |
|  |

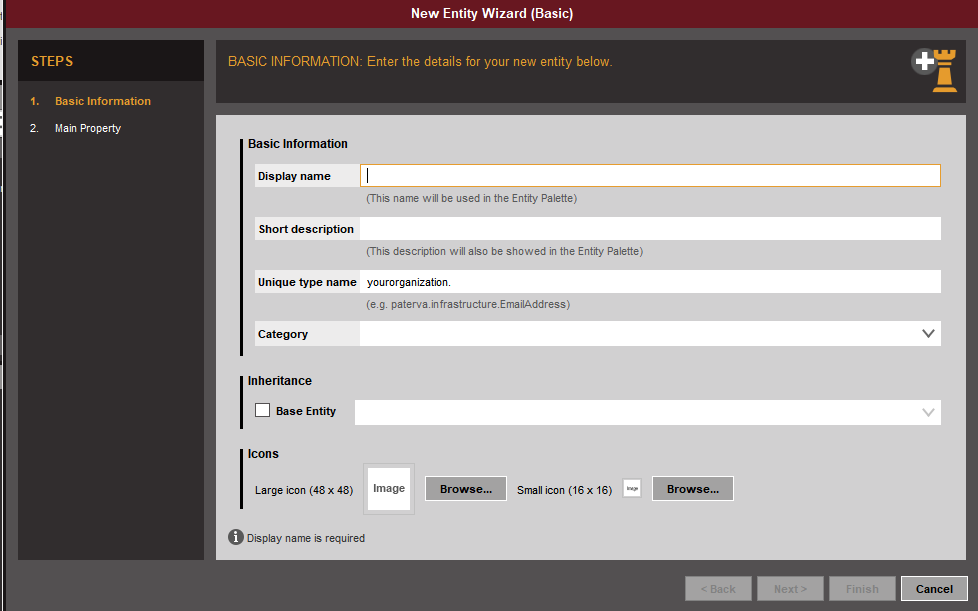
In the window on the right we can review the shape of the tree and the types, details of each entity (identified by colors), relationships, etc.

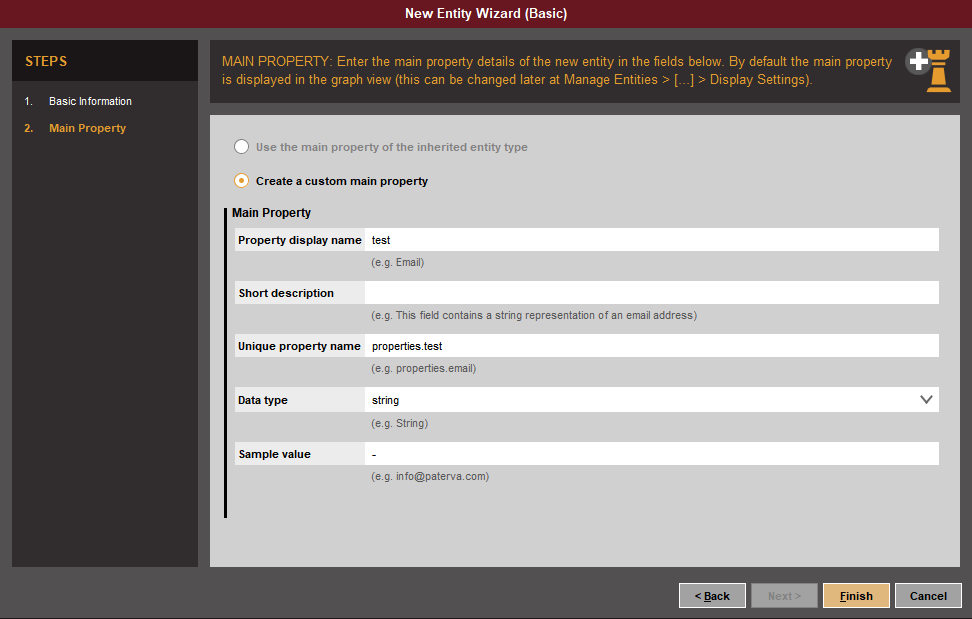
|  |
| --- |
|  |

4. We're going to create our own transforms to get the information we want.

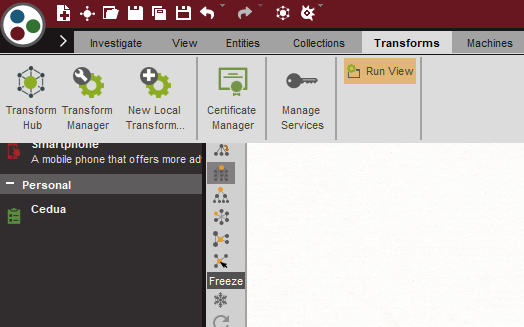
* We need the following python libraries:
* Selenium
* Pillow
* Create an entity



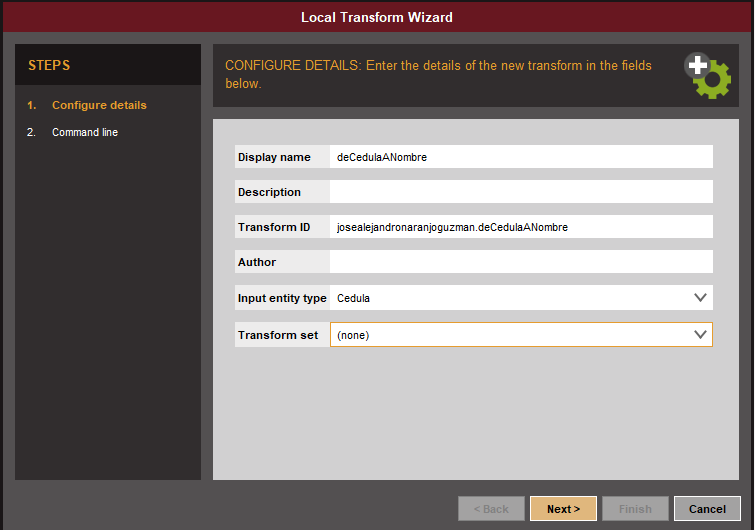




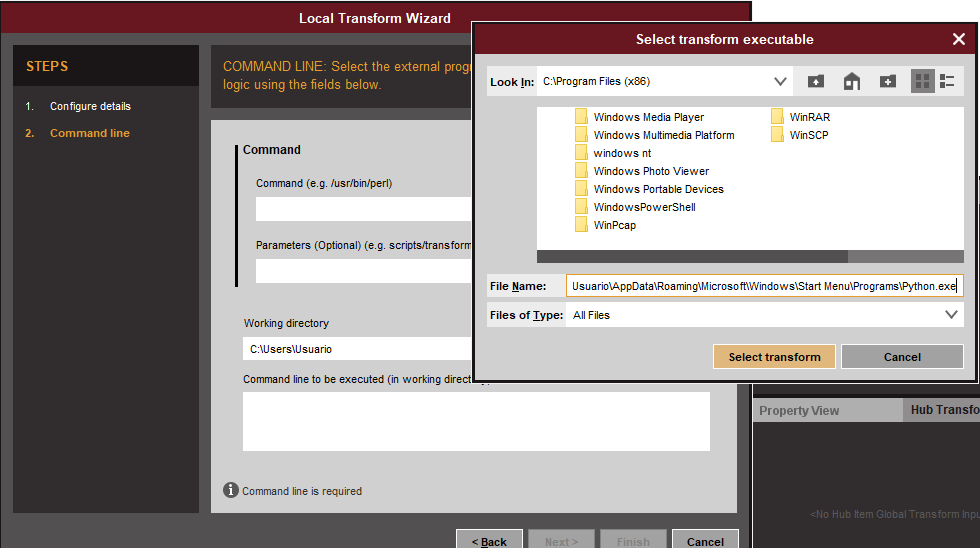
* Import a transform to maltego: New Local Transform.



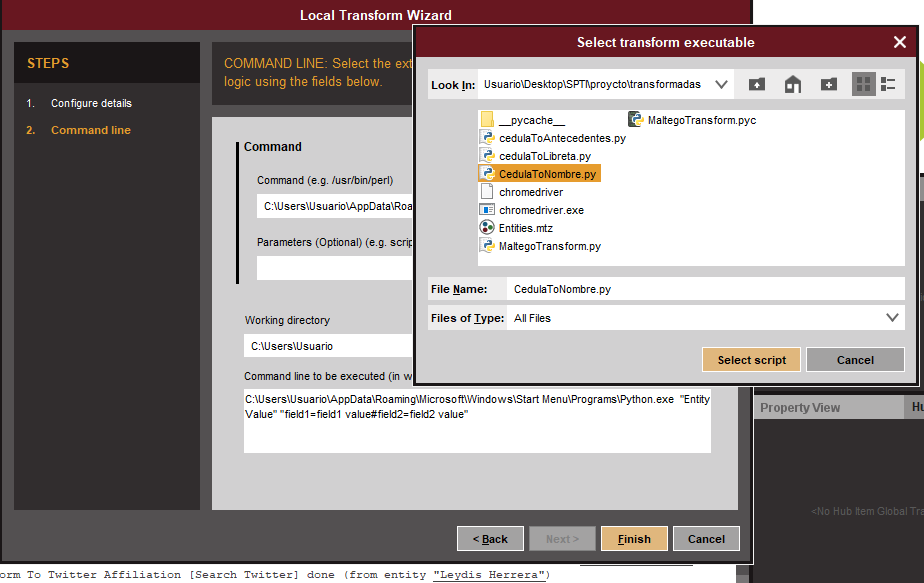
* The following fields are filled in.



* In the field "Command (e.g. /usr/bin/perl)", put the python executable (python.exe).



* In parameters (Optional)(e.g script). Put the transform location.



5. **CHALLENGE:**

* Create a Facebook account entity.
* Create a University entity
* Extract information from Mark Zuckerberg (University, number of followers, wife, family)
* Get to know the universities where Mark Zuckerberg's wife studied.