SOCIAL LINKS

Separating the Wheat from the Chaff:

A Case Study of How Social Networks Act as Recruitment Pools And What Tools Can Be Used to Counter Illicit Activity on The Internet

On February 27, 2020, Lawfare published a research article on the spatial structure, internal organization, and recruiting processes in a number of international racial-extremist groups united by the Ironmarch.org community. A study of more than 1,207 regular users and 195,000 public posts was conducted, and 4,500 private conversations were analyzed using the Maltego and Social Links Pro to identify the sources and mechanisms of the organization's functioning. Social Links team has prepared step by step guide on how this investigation was conducted.
Before we start, let's look into the background:

It is no secret that terrorist and extremist organizations use the internet and social networks not only for communicating, but also for seeking new recruits. The instruments for identifying potential candidates with likeminded interests are available in the form of simple search queries for communities in social networks, and the extremists get ready-made lists of members.

White extremism is becoming a serious threat to national security in the United States as the number of racially motivated attacks has been on the rise for years. The abundance of extremist content available on the internet and in specialized communities and forums on extremist topics is serving as a breeding ground and magnet for potential criminals.

> During a hearing in front of the House Judiciary Committee on February 5, 2020, FBI Director Christopher Wray stated that the bureau was elevating "to the top level priority racially motivated violent extremism so it is on the same footing in terms of our national threat banding as ISIS and homegrown violent extremism." The decision comes as a majority of the FBI's domestic-terrorism investigations since October 2018 were found to have a nexus to white supremacy." – states author of Lawfare article.

One of the most prominent channels for white supremacist activity was the Iron March website. The forum acted as a channel of communications for extremists and contained vast amounts of content. However, on November 6, 2019, the entire SQL database behind Ironmarch.org was posted on Internet Archives. The data, which was released by an unknown individual, includes private messages, user account information and the site's forum posts. The data was then analyzed by investigative journalists along with Bellingcat and acted as the basis for the given study.

Purpose of The Study

Using the data leaked from Iron March, open source research and the Maltego platform supplemented by the Social Links add-on, the study tried to answer the following questions: (a) What is the profile of an “average” Iron March user? (b) What drove activity on Iron March? and (c) How effective was Iron March at connecting like-minded white supremacist and neo-Nazis?

Understanding how white supremacist and neo-Nazi networks operate and recruit is critical to mitigating this threat, and one way to collect intelligence on these groups is to track their activity on certain public and restricted websites. The recent hack and data-dump of a white supremacist website provides a window into that kind of activity.

To answer the main and most important question, “How Did Iron March Connect Like-Minded White Extremists and Neo-Nazis?”, the author used a combination of Maltego XL and Social Links Pro tools.

As a result of the analysis, Jacques Singer-Emery concluded that Private conversations related to recruitment, coordination and philosophical discussions accounted for approximately 15 percent of all the private conversations between Iron March members starting at the end of 2015. Analyzing these messages provides more detail into exactly how white supremacist and neo-Nazi groups shared information, recruited new members and coordinated their activity.

The research produced two conclusions. First, the networks and relationships developed on Iron March did not appear to be replicated on public social media platforms, suggesting that the platform was critical to connecting like-minded individuals and helping white supremacist and neo-Nazi groups recruit new members. Second, most Iron March users did not appear concerned about law enforcement surveillance on the site and did not take measures to hide their activity.

One of the most prominent channels for white supremacist activity was the Iron March website. The forum acted as a channel of communications for extremists and contained vast amounts of content. However, on November 6, 2019, the entire SQL database behind Ironmarch.org was posted on Internet Archives. The data, which was released by an unknown individual, includes private messages, user account information and the site’s forum posts. The data was then analyzed by investigative journalists along with Bellingcat and acted as the basis for the given study.

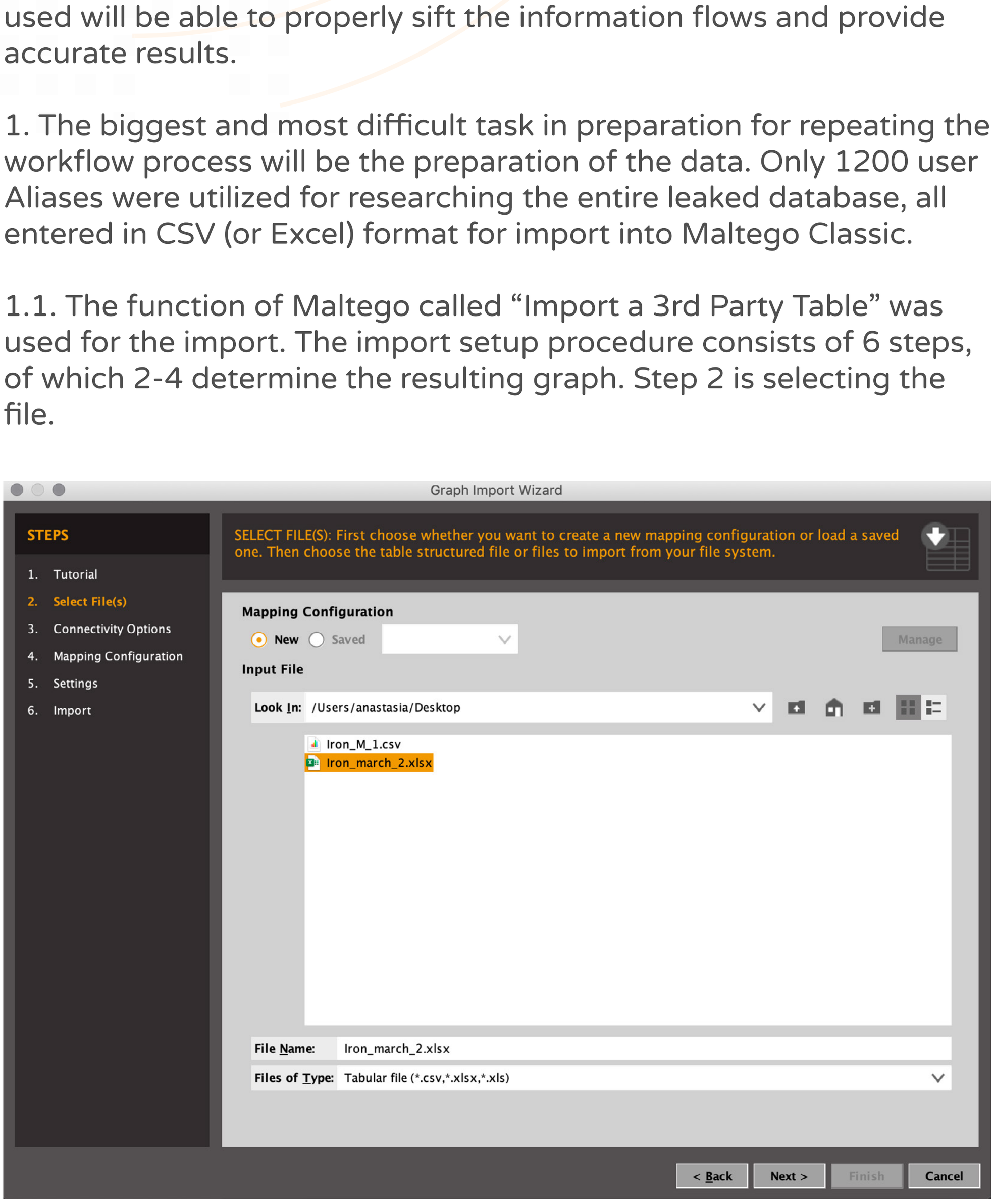
The Workflow Used During The Study

This article will attempt to repeat the workflow conducted by the author of the Iron March study. A compiled and detailed step-by-step guide will be provided in the following material.

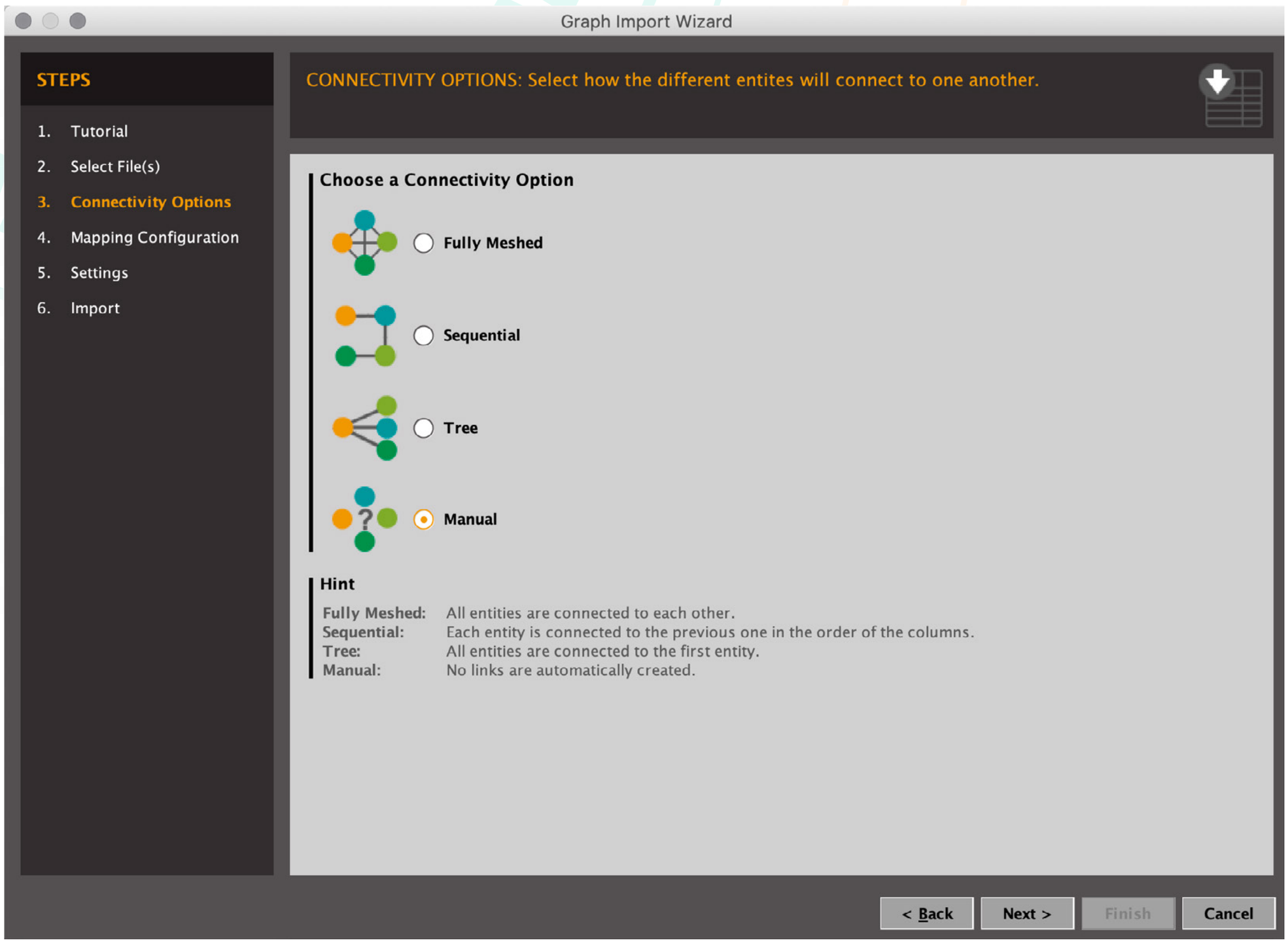
Working with vast amounts of data requires preliminary preparations and careful analysis of the available datasets to ensure that the tools used will be able to properly sift the information flows and provide accurate results.

1. The biggest and most difficult task in preparation for repeating the workflow process will be the preparation of the data. Only 1200 user Aliases were utilized for researching the entire leaked database, all entered in CSV (or Excel) format for import into Maltego Classic.

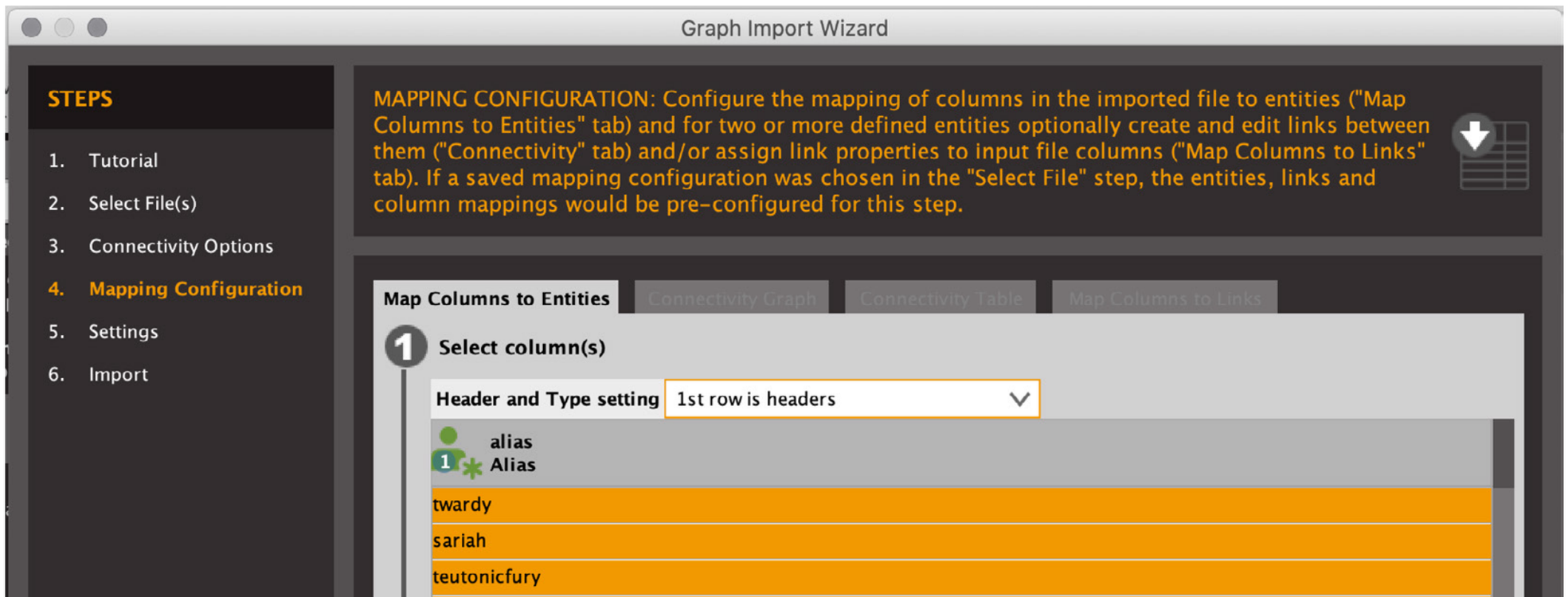
1.1. The function of Maltego called “Import a 3rd Party Table” was used for the import. The import setup procedure consists of 6 steps, of which 2-4 determine the resulting graph. Step 2 is selecting the file.



1.2. Step 3 is determining the nature of the relationship between the imported elements. In the given case, the Aliases list was imported with the “no links” option selected. The bottom prompt describes the logic with which the links are created under various options. That is why one should pay close attention to preparing the data before importing, as the logic of the future visualization in Maltego should already be embedded in the structure of the data being used.



1.3. Step 4 is the direct import. At this stage, it is worth translating the data into the language of Entities used by Maltego. The nicknames of the users in social networks in the language of Maltego (and not only in Maltego) are called Aliases. That is why the “Alias” mapping option should be selected.

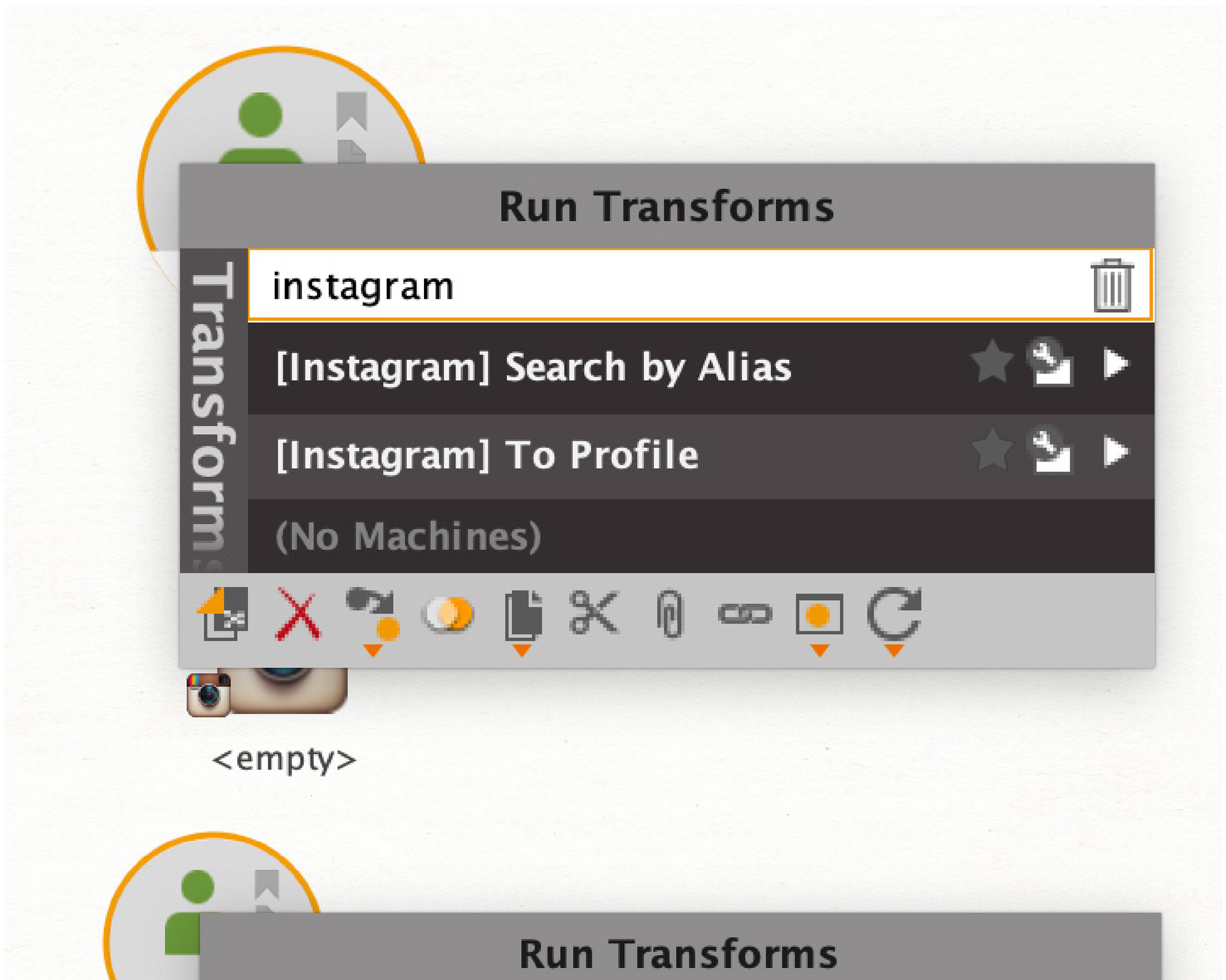


The perfect template of 1,200 Aliases is thus created on the graph and is ready for analysis.

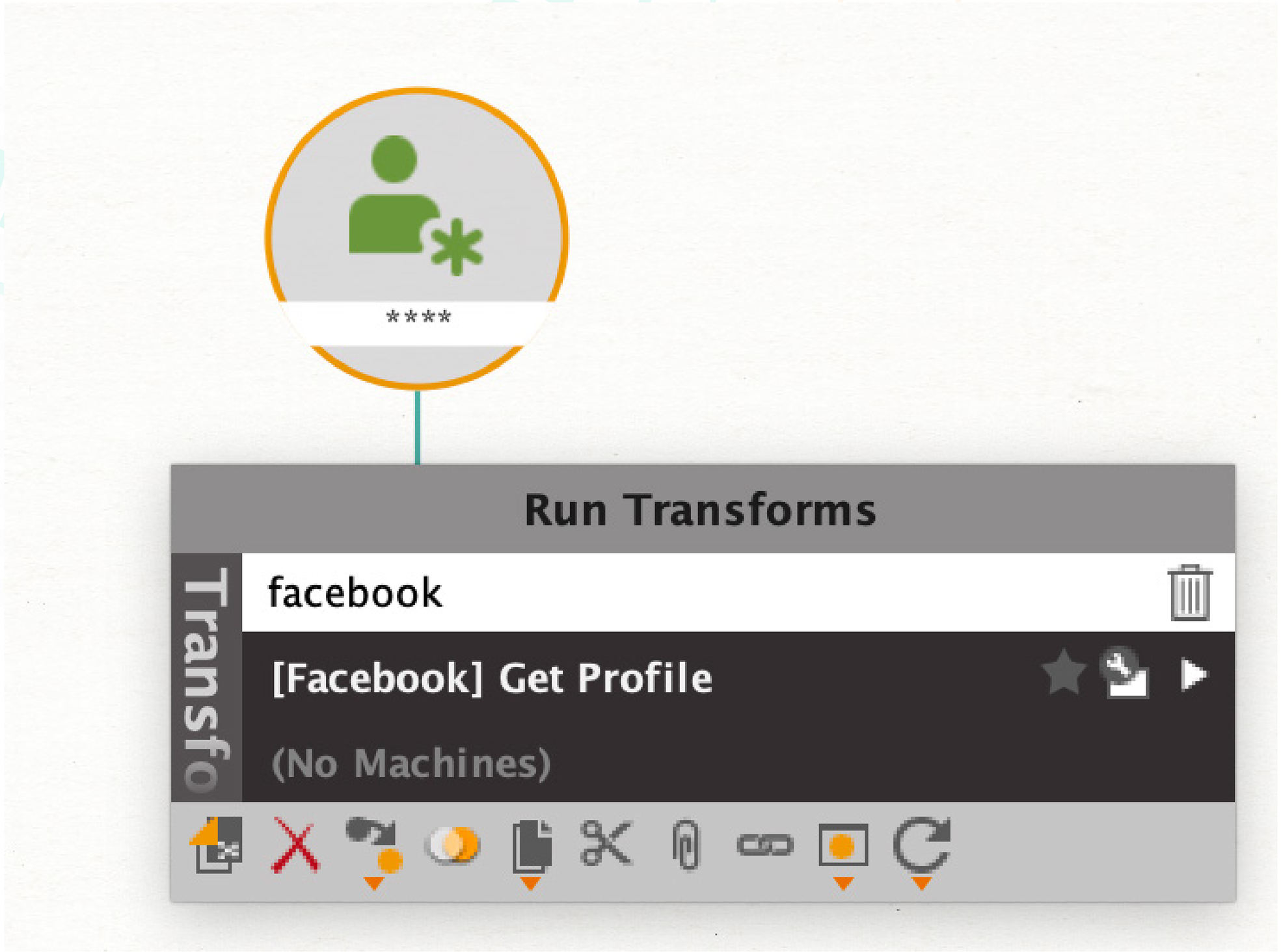
2. The main task is to identify and link profiles on Facebook, Twitter and Instagram for the selected Aliases. To do this, it is necessary to select the appropriate Search Methods (Transformations) in the Social Links Pro list.

2.1. Choosing Social Links Pro transformations in Maltego for further actions:

In the case of Instagram and Twitter, there are 2 Transformations available from the Alias entity. The methods available are [Twitter] To User and [Instagram] To Profile, since these methods provide one-to-one correlation, in case such a profile exists. The other 2 methods conduct a search for Aliases that are specifically defined and similar.



There is only one method available from Aliases on Facebook and it leads directly to the user profile. The method is called: [Facebook] Get Profile.



The decision was also made to divide the workflow into 3: (1) a graph for working with Twitter, (2) a graph for Instagram, and (3) a graph for Facebook. It will thus be easier for not to get confused in the results.

2.2. Workflow and the launch of transformations

Once the Aliases are imported, the 3 graphs are created, and the transformations are selected, it is possible to start search by selecting all Entities and running needed transformations. The data collection process will take about 30 minutes.

While data collection is in progress, an important remark should be made about the limitations on the scope of ongoing investigations in Maltego and Social Links Pro. The Maltego Classic version allows for the simultaneous existence of no more than 10,000 entities on a graph. Maltego XL allows no more than 1,000,000. That is why in Maltego Classic, it was decided to split the data collection into 3 graphs so as to obtain no more than 10,000 entities on each. As for Social Links Pro, it is possible to run no more than 3,000 transformations per day. Social Links does not bill per the number of results, but per the number of requests. Starting 1 transformation from 1 entity counts as 1 request. Accordingly, the launch of 1 transformation from 1,200 entities will be counted as 1,200 requests out of 3000.

2.3. Viewing and analyzing the results.

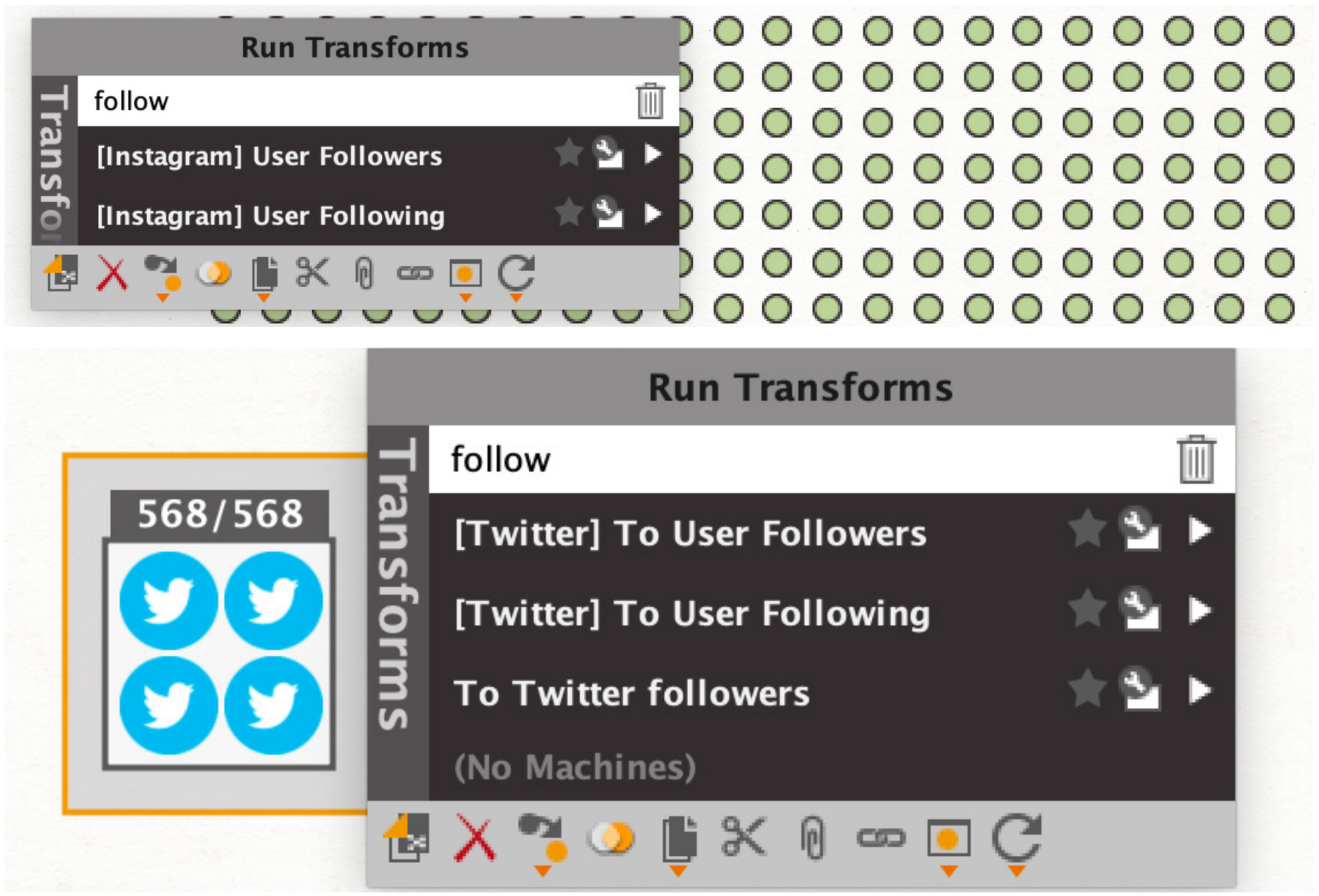
Out of nearly 1,200 Aliases, it was possible to identify about 600 profiles on Twitter and Instagram, and about 500 on Facebook as of May 2020. Aliases with no results were deleted from the graphs.

2.4. Selection of transformations for the analysis of links in social networks among the identified profiles.

It is now necessary to attempt to establish links among the profiles in order to get the same result as in the following paragraph of the article:

> Interestingly, this close-knit network of users did not appear to exist on more public social media platforms. Using the research capabilities provided by Maltego and the Social Links add-on, we discovered 293 Facebook pages, 151 Twitter accounts, 357 possible Instagram accounts and 102 VK accounts linked to various Iron March members. Neither the VK nor Instagram accounts identified followed each other or had any friends in common. Furthermore, only 25 Facebook accounts and 20 Twitter accounts linked to Iron March users were connected as “friends” or “followers” or had at least one mutual “friend” or “follower.”

To achieve the same results, it is necessary to select needed transformations as the first step. For Instagram and Twitter, a similar set of two transformations will be used: User Followers and User Following. Both will be launched simultaneously on graphs with Twitter and Instagram accounts. Thus, it will be possible get a complete picture of (1) subscribers, (2) subscriptions of the accounts under study, as well as (3) links between accounts.

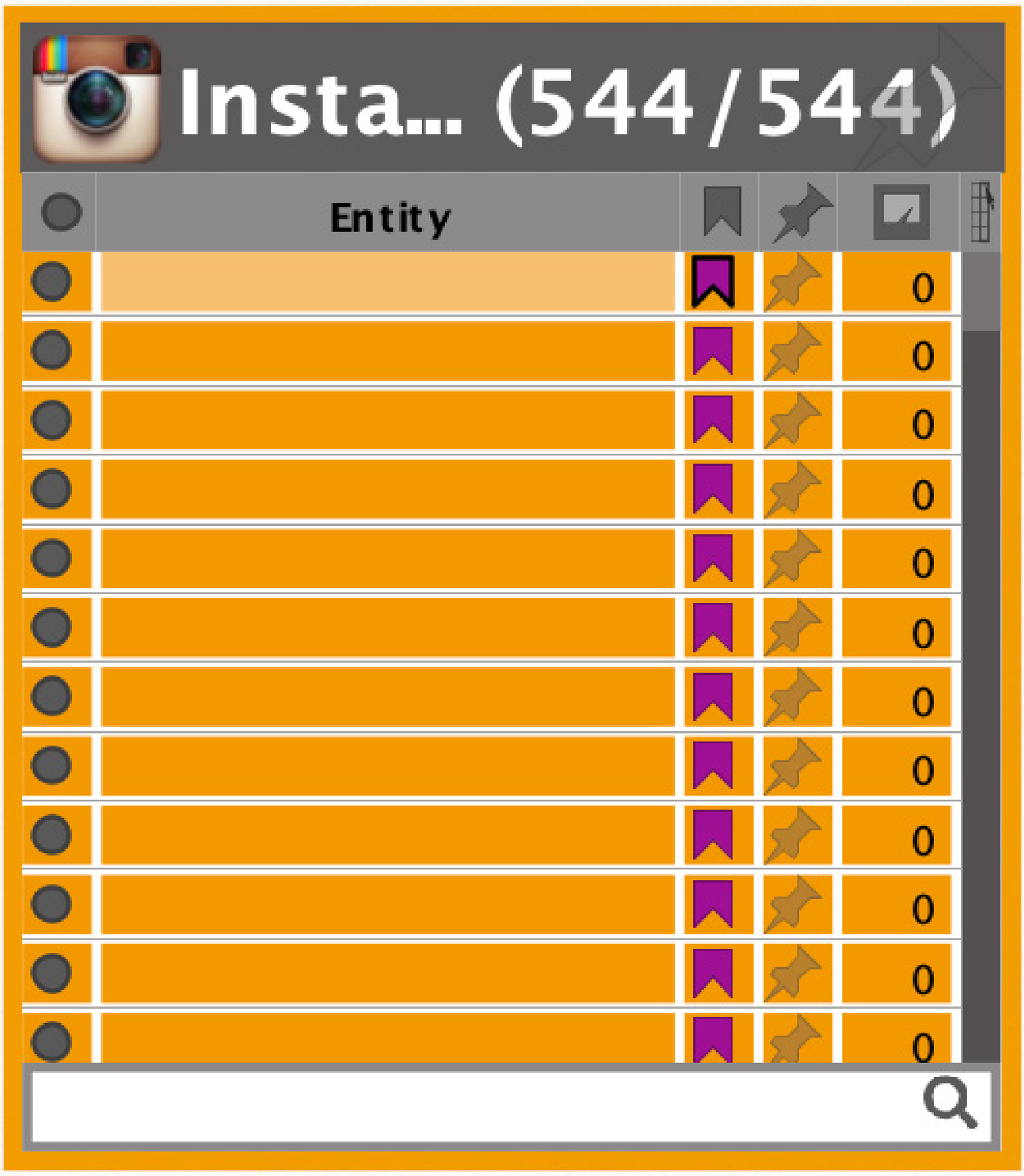


For researching Facebook, 4 transformations will be used:

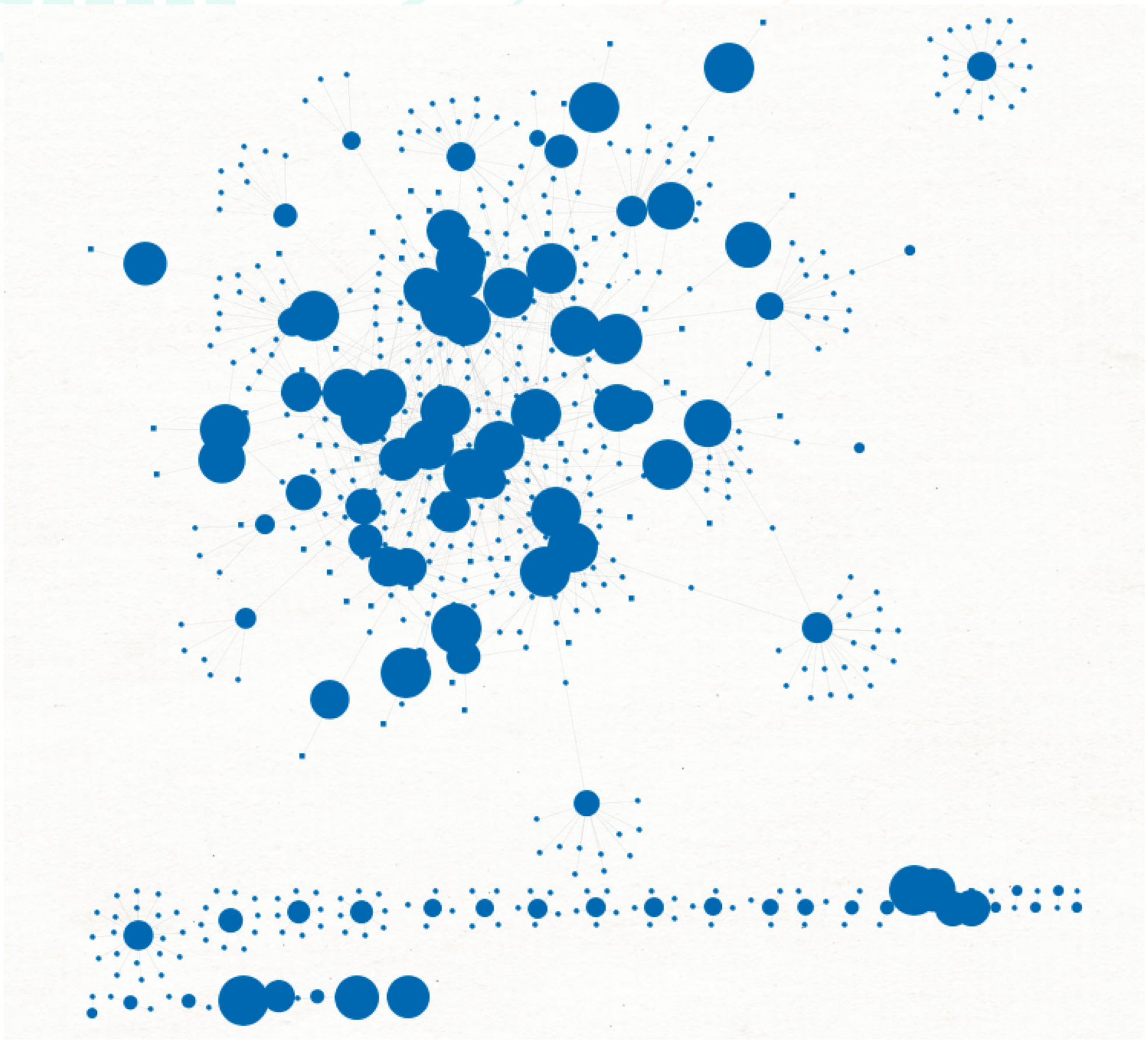
A) [Facebook] Followers
B) [Facebook] Users Followed
c) [Facebook F] Friends
d) [Facebook MF] Search Relations

The transformation under item d) will be useful for accounts that have a private list of friends. This transformation analyzes the activity on the user's page and the lists of all active users.

Another convenient feature of Maltego should also be mentioned. In order not to get confused in the results about which accounts were the source ones and which ones were obtained as a result of enrichment, it is possible to mark all the source accounts with colored tags. To do this, it is necessary to assemble the accounts in separate Collections, select the entire group of accounts and assign a color to this group, as shown in the screenshot. When analyzing the results, it will be possible to easily separate some accounts from others.



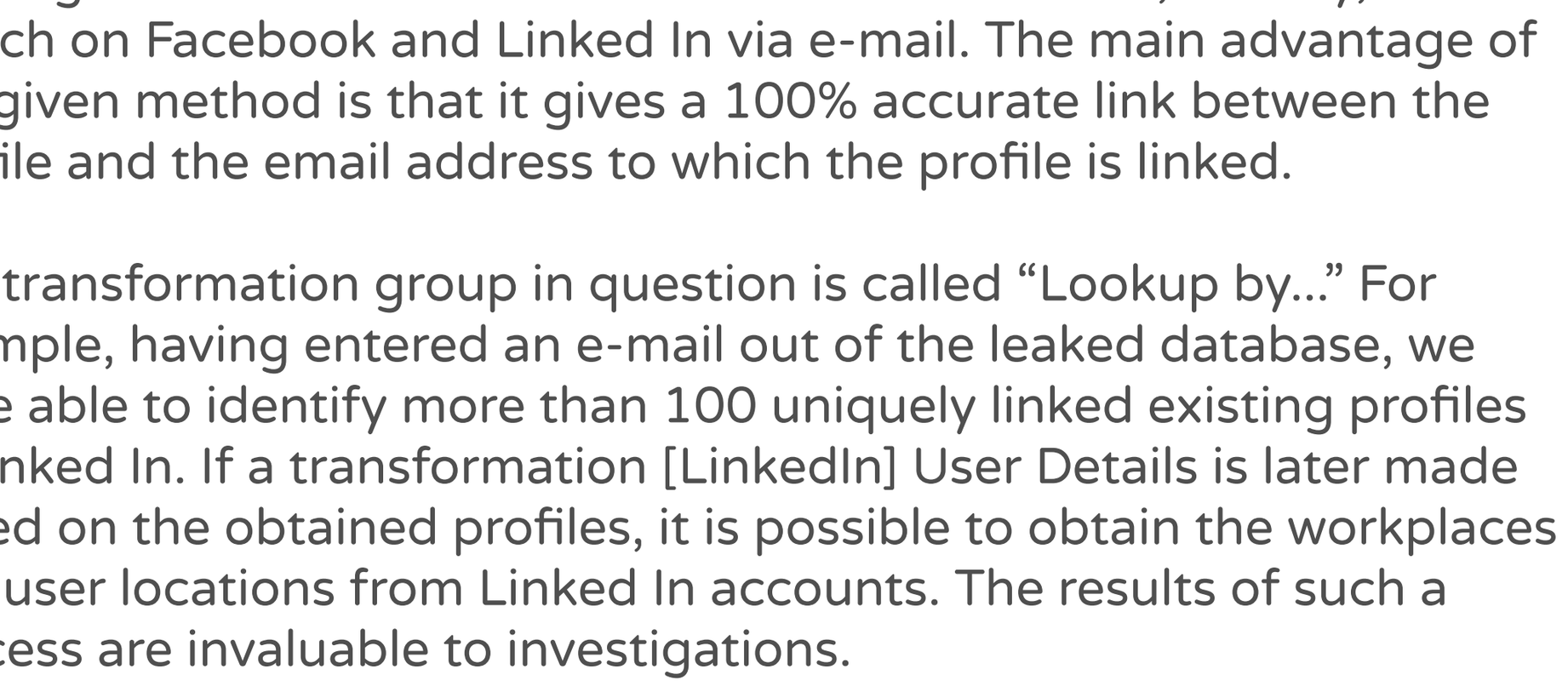
2.6.) For a visual analysis of the results, it is most convenient to switch to Layout mode “Organic”. It is also possible to adjust the settings of the View for greater convenience. The larger the size of the entity, the more links it has with other entities, which means that the more active the user will be included in this account group.



3. Investigation bonus track:

A method that Social Links Pro did not have at the time of the investigation made for Lawfare was used in this case, namely, a search on Facebook and Linked In via e-mail. The main advantage of the given method is that it gives a 100% accurate link between the profile and the email address to which the profile is linked.

The transformation group in question is called “Lookup by...” For example, having entered an e-mail out of the leaked database, we were able to identify more than 100 uniquely linked existing profiles in Linked In. If a transformation [LinkedIn] User Details is later made based on the obtained profiles, it is possible to obtain the workplaces and user locations from Linked In accounts. The results of such a process are invaluable to investigations.



Conclusions regarding the use of Maltego Classic / XL + Social Links Pro for the analysis.

1) In total, the process was carried out in 4.5 hours and was interrupted only by the use of the Social Links Pro daily limit of 3,000 transformations.

2) It is impossible to estimate the time it would have taken to conduct the investigation if it had been carried out it using various tools with result transfers from one program to another. With Maltego Classic / XL + Social Links Pro, the work was carried out in a single working environment.

3) Conducting such analysis manually is simply impossible.

4) It is convenient to work with a large number of entities in Maltego and conduct visual analysis, even when it comes to 10,000 + entities on a graph. There are many different ways of simplifying the analysis and not getting confused, as the various Layouts and Views, and the ability to mark or distinguish entities with colors makes the process more convenient.

About the Author of The Study

Jacques Singer-Emery is a recent graduate of Harvard Law School and previously spent four years in the New York Police Department (NYPD), first as a policy advisor to Police Commissioner Bratton and then as a Case Analyst for the NYPD Intelligence Bureau. He is the Editor-in-Chief of the National Security Law Journal and a researcher for Professor Philip Heymann and Professor Blum. Jacques graduated Magna Cum Laude from Princeton University in 2013.

If you have more questions about the actual study made by Jacques Singer-Emery for Lawfare, please do not hesitate to contact Social Links sales@mtg-bi.com with a subject line referencing this piece or his Lawfare article.