

## Maltego 3: First Look

Tutorial by Wardell Motley

Maltego, developed by Roelof Temmingh, Andrew Macpherson and their team over at Paterva, is a premier information gathering tool that allows you to visualize and understand common trust relationships between entities of your choosing. Currently Maltego 3 is available for Windows and Linux. There is also an upcoming version for Apple users that has yet to be released.

Information gathering is a vital part of any penetration test or security audit, and it's a process that demands patience, concentration and the right tool to be done correctly. In our case Maltego 3 is the tool for the job.

In this article we explore Maltego 3 and examine its fundamental features and a little hands-on with the newly designed version. If you haven't already had a chance to upgrade to or pick up Maltego 3 you are missing out.

[del.icio.us](#)

[Discuss in Forums {mos\\_smf\\_discuss:/root}](#)

Maltego comes in two flavors, a community edition and a commercial version. The community edition is great if you don't want to cough up the money, but it does limit your effectiveness. Having been on both sides I can whole heartedly say the commercial edition is well worth the price you pay!

Being free, the Community Edition is the version of choice for this tutorial. So be sure to grab a copy and install before continuing. Installation is straight forward, so we won't waste time going over the process.

## Navigating the Interface

Let's start out by learning our way around the interface that is clearly based on the Office Ribbon design. Please note we won't be going over every feature but just enough to familiarize users with the application.

Across the top we have the Main Navigation Bar. We are currently under the Investigate Tab, which is where most of our work will be done. Here you have the ability to edit and manipulate items on your clipboard, set the level of results per transform and set zoom levels.

Under the Manage Tab we can manage and import transforms as well as entities. You can also create and manage your very own transforms in this area.

We can start out by selecting the New Graph symbol at the top left hand corner of the page to begin a graph or use the keyboard shortcut CTRL + T.

On the left side you will now see a new Menu. This is the Palette Toolbar. The Palette Toolbar is where you will select an entity to move to the main clipboard. In order to select an entity, simply highlight the item of your choice and drag it to an open area in the New Graph in the main window. You have a choice to select anything from a domain name or IP block to a person, place or phrase.

## Searching for Information

In this example our target will be the Cyber Security Czar of the United States, Howard Schmidt. So click and drag the Person entity from the Personal Section of the Palette and place it in your New Graph. In order to input new information or edit existing information for any entity on the graph, simply double-click on the icon and start typing.

Once you have input the entity properties select OK. At this point you have the ability to run a transform on your entity. But what is a transform? Simply put, a transform is a way of querying information on a particular entity (more on this later).

By right-clicking on the entity you have the ability to select a transform to discover existing information or possible links to your entity. Maltego will use API's search engines and various websites to attain information regarding your target. As you can see, you have the ability to search for your target's email address, phone number as well as any links that the target has on different websites using various methods and resources.

In this example we will select Run Transform> Email addresses from Person> and then use the 'All in this set' option to search for email addresses via Public PGP server, Search engines and common free email providers such as Hotmail and Gmail. Also notice the icons that are just to the right of our search options. The blue spheres that you see, if clicked, will take you to a brief descriptions page describing the selected transform and what it does. The hazy square to the left of the blue sphere is a handy shortcut to the transform manager.

Results will start to appear immediately, but a listing of all email addresses may take a couple minutes depending on the speed of your system and the network connection. In the meantime, let's point out another important difference between the Community and Commercial Editions of Maltego.

### Maltego 3.0 CE Edition

As you can see here the Maltego Client requests are sent out via the client over HTTP for the CE edition and HTTPS for the commercial edition.

We have now gone from just a name to a list of possible email addresses. But how do we know these email addresses are valid or even connected to the individual in question? Maltego figures this out by taking the responses from the search engine and assigns it a weight based on relevance. For example, when matching an individual to an email address, the weight would correspond to how closely the found email address matches the initial name. Another way to quickly identify which results have the most weight is to simply highlight them and check their weight under the Properties Window (more on this later). You will also notice that since you have run the initial search, your other Property Windows have been filled with useful information.

The Overview Window gives you a quick glance at your transform results via color coded circles. Here we only have one brown circle for the originating entity for the name that we typed and several green circles for the child entities which are email addresses in this case. If you zoom out on the overview you will find a legend in the lower right-hand corner of the Overview Window that will allow you to see which color maps to which circle.

The Transform Output Windows display the number of results per search. As you can see here we just ran 3 transforms, all of which were searching for email addresses, but the process used 3 different search methods.

## Entity Properties and Detail View

The Detail View and the Properties View presents a more specific approach and understanding to the information that is currently on your main graph window. By highlighting an entity on the main graph like we have done here, you can now see the outgoing links from that entity in the Detail View. This really helps when you need a compressed view instead of having to scroll all around on the main diagram to look at information. The Property View allows you to check the weight and as well as the number of links coming into and out of an entity.

## Putting It All Together

### Examining the Results

Now that you have your results let's examine them further by weight. As you can see the email address 'howard at schmidt dot org' has a corresponding weight of 100 points. I'm sure there is more than one 'Howard Schmidt' in the world, so even though we got a perfect score, we're still not sure this is the object of our investigation. Let's examine this a bit further and drill down on this email address. We can do this by copying this email entity to a new graph. In Maltego it definitely helps to create a new graph to keep your information straight, since the more results you get in a graph the more cluttered the graph will become.

Most high-end targets have a picture and full bio posted somewhere on the net including company websites, magazines for which they've written or even conferences where they have spoken. But why not let Maltego do the legwork for you by utilizing an easy trick to take advantage of the ever expanding amount of data published by the target themselves. So let's run a nifty little transform on our entity via the Rapleaf API to check the target's membership in social networks. This is a great way to combine technology and the unique abilities of humans to verify data.

## The Rapleaf API

Maltego comes preloaded with over 100 transforms, but, in order to get the most out of your transforms (in particular the Rapleaf API), you will have to register for an API key. Until you register and input the API key, the Rapleaf transform will be useless to you. In order to get an API key browse out to [https://www.rapleaf.com/developer/api\\_access](https://www.rapleaf.com/developer/api_access) and fill out the accompanying form. You will then receive an API key from Rapleaf. Once you receive your key open up your transform manager and then select the Rapleaf transform. Input your API key and accept the disclaimer and you will be on your way.

This transform will now go out and cross check the email address you entered with known social networks to see if any links can be determined between the address you entered and numerous social networking sites.

As you can see here it's returned with several results linking the email address in question with accounts on LinkedIn, Twitter and Facebook. We can now examine the links by going to our Property View Window and opening the URL.

Looking at the LinkedIn account of our target, it now becomes possible to associate a face with a name thus becoming quite easy to confirm that this is in fact our target. By examining the page further, you also notice that the Twitter location tracking feature is on. This is good, because it now will allow us to see the tweeting location of our individual.

With the latitude and longitude information we can now bring up various online earth viewing sites and examine the location. We can even bring up a map of the location in question and extrapolate the address and phone number. All of this information gathered with just a simple name and a great tool.

## Conclusion

As you have just seen Maltego is a quick and effective information gathering tool that will allow you to pull information from multiple resources all into one place for analysis. We only managed to go over a fraction of Maltego's functionality, but it's easy to see how, in a matter of minutes, you can paint an accurate picture of a person, place or organization. It's definitely a tool that you should not only add to your toolkit but dive in with vigor. So whether you are a seasoned IT security pro or a newbie ready to cut his teeth on a tool, Maltego 3 will give the user a place to stand among the sheer torrent of information likely to be encountered while profiling an organization or individual.

Stay tuned to further tutorials on Maltego including how to create your own custom transform.

Wardell Motley is a Certified Ethical Hacker and a Systems Administrator for a large clothing manufacture in Dallas, Texas. He is an active member of the ISSA, Infragard North Texas, OWASP & former member of the U.S Army. In his spare time he works as a freelance IT security researcher and contributes to Hakin9 Magazine & Ethicalhacker.net.