

Forum:[Hack Forums](#)

Thread: [\[Doxing Method\]\[GUIDE\] How to use Maltego \[GUIDE\]](#)

Ghost.13 - May 31, 2012, 2:22 am

Learn How to Use Maltego

Introduction

Good day HF!

Today, I'm going to show you how to use the software called "Maltego". I did hit the Search Button, and saw that if ever, this would be the first tutorial made for this software.

This tool can be used to gather information about a certain person, a domain, etc. Yes, it is some sort of "doxing"/profiling tool, but it is also useful to link raw data gathered and turn them into useful information, where you know how item A relates to item B.

Do note that this guide/tutorial is for EDUCATIONAL PURPOSES only. I will not be responsible for any illegal or malicious usage of this software.

What is Maltego?

Maltego is an open source intelligence and forensics application. It will offer you timous mining and gathering of information as well as the representation of this information in a easy to understand format.

-<http://www.paterva.com/web5/>

In more simpler terms, it's just a forensic tool to mine data and organize them in a more understandable view.

How to Start Using Maltego?

First off all, it is FREE, however, the community edition has limitations in it.

If you want to download it, here's the download page:

[Paterva Official Site](#)

...just grab one that will suit your OS (all platforms are supported, yes even Macs).

Next thing is to install it.

You know the drill, just click the Next button until you reach the Finish button.

However, for you to use the Community Edition (the free one), you need to register your copy through their servers, so yeah, just follow the instructions, it should be user-friendly and could be followed by noobs.

After installation, of course you must execute it, and you'll see something like this:

Spoiler [\(Click to View\)](#)

Terminologies

Now, that you've successfully installed Maltego, let's talk a little about the terminologies first, which I'm going to use through this tutorial.

There are two major terms that I'm going to use in this tutorial with regards to this software: Entities and Transforms.

Entities

These are the items which you can see on the graph. It can either be a domain name, a person, a Facebook profile, an email address, etc. Now, these entities can be processed through the use of Transforms to form new entities.

Transforms

Transforms are functions that can process entities into new form of entities. Example: you have a domain name, you can use a transform to get its IP address, thus from the entity Domain, you created another entity called IP address. It is best viewed when we put it to work.

Maltego in Action

Okay, here's a screen shot we will "dissect":

Spoiler ([Click to View](#))

...I apologize for the big screenies, I have to do it to show you HQ and detailed pics of the software.

Now, let's dissect it, so pay close attention to the parts that are encircled in red.

First one we discuss is the one on the left part, on the Palette tab, the Domain (one with blue globe icon). As you can see in the graph (the center portion), "yahoo.com" is a domain. Yes, I'm the one who put it there, because that's my starting point. To try it yourself, click the Domain icon on the Palette tab, and drag it to the graph, then just double-click it to rename to whatever domain you like.

Now, you can consider "yahoo.com" as your raw information. That is our first Entity, our starting point in profiling, since we can't do a "dox" or a profile without a starting point. For it to become useful, we need other data that must be related to it. That's when Transforms come in. Right-click at "yahoo.com" entity, and that should give you options, choose "Run Transforms", then it will give you a whole bunch of options which you can try.

Now, like I said, Transforms are functions which turns entities into new form of entities. Now, to achieve the screen shot (for educational purposes), let's say we want to know Website DNS related to the domain "yahoo.com", you just choose "All Transforms", and find the "To Website DNS (Using Search Engine)". Now, the concept of that is to find Website DNS using Search Engines and it dumps info in your graph, creating links to your first entity and other newly formed entity using the transform. You'll get those computer icons with a star in the middle of the graph, which are now Website DNS related to "yahoo.com", as you can see, "answers.yahoo.com", "att.my.yahoo.com", "advertising.yahoo.com".

Look at the right side portion of the screen shot, where an Overview tab is. See that? It means I'm zoomed in to that particular area, but if you can see, there are other bunch of results for that transform. You can also see that when you follow the lines and arrows.

Now, what do we want with Website DNS anyway? Let's try to find out their IP. Now, you can use the transforms on several entities, just drag the mouse across the screen to select them. So, try to select all Website DNS, and right-click, run transforms, then choose "To IP Address". After that, you'll notice that more entities will branch out from the Website DNS entities (refer to the IP address encircled).

Now, the bottom part is the output box for transforms. It's just like a message box for compilers, where it prompts users about what happened to the transform, and which transform is currently running. See that we executed transform "To IP Address" using Website DNS as entities, and look at the results, it tells you how many entities are formed because of that transformed, that way you know how many details you should go through your search.

Now of course, you're just gonna use your skills to go through the transforms, as they're too many. There are certain transforms for certain entities. So you might be thinking, "Ghost, this is just useful for networking masters, web hackers, and skids who love to use their booters". Unfortunately not, since we have an entity for email address.

Spoiler ([Click to View](#))

...Now, sorry for the zoomed out screen, I put in numbers so I can explain everything to you, don't worry.

So, for my starting point, I numbered it #1. It's an email address I just grabbed from my mind, I called it "john_smith@yahoo.com". Now, Maltego has some special transforms for email address, so for you, try to verify the email first by using the transform "Verify Email Address Exists". Now, because john_smith@yahoo.com is a bit of a "generic" email, it will just return you an inconclusive answer, but if you try it with your email, see the results.

Now, I used the Transform "emailToMySpaceAccount". I know MySpace is a bit outdated, but it might still contain information you need, so it returned a few Alias entity and one MySpace account entity (which is #2). Now the Aliases are like nicknames/usernames in Maltego. You can now use transforms to it like "AliasToFacebookProfile", which will now return profiles with aliases like that of which you used for the transform.

Now, I also used a Transform on #1 called "To Email Address (PGP)", and it returned possible alternate email addresses (which is #3), which can be very useful when you're using the Forgot Password method to compromise accounts. Using the new Email entities formed, I then checked if those email addresses have MySpace accounts related to #1, and it returned a bunch of other accounts for you to confirm (which is #4).

Now, do note that this software isn't really ACCURATE when you only have an email, but it can give you valuable results in such cases the only thing you have is a piece of address. It can give you at least a rough dox of someone you know by email.

End Notes

There are many types of entities there which have different transform options, it's just up to you to explore.

Now, I'm going to give you a useful link for you to understand more about Maltego:

<https://www.youtube.com/user/PatervaMaltego>

That is their YT channel where they posted several videos for users to harness the full potential of Maltego, including videos that teaches you how to write your own transforms.

That's all for now HF!

If you have suggestions, comments, compliments, criticisms, questions or queries, just hit me up via PM or just comment on this thread. :)

Thank you and have a good day.

CyberZeist - May 31, 2012, 5:30 am

Its a basic level of doxing and target imaging.. nonetheless many beginners will benefit from it!

Ghost.13 - May 31, 2012, 5:37 am

(May 31, 2012 05:30 AM)CyberZeist Wrote: [\[CITE\]](#) Its a basic level of doxing and target imaging.. nonetheless many beginners will benefit from it!

At last, I thought no one would really care about a guide I made for hours.

I know, but it's a pretty decent software to organize and link your data, plus the fact that it's fully automated. :)

Thanks for the reply though.

Alside - May 31, 2012, 5:41 am

Nice share Lol and I know I hate when there is like 100+ views and only a few comments.

CyberZeist - May 31, 2012, 5:42 am

(May 31, 2012 05:37 AM)Ghost.13 Wrote: [\[CITE\]](#) At last, I thought no one would really care about a guide I made for hours.

I know, but it's a pretty decent software to organize and link your data, plus the fact that it's fully automated. :)

Thanks for the reply though.

Yeah...as I said its pretty most basic procedure in fingerprinting...it ought to be known by the one who doesn't wanna waste time doing a manual recon!

Ghost.13 - May 31, 2012, 5:44 am

(May 31, 2012 05:42 AM)CyberZeist Wrote: [\[CITE\]](#) Yeah...as I said its pretty most basic procedure in fingerprinting...it ought to be known by the one who doesn't wanna waste time doing a manual recon!

Well, it's the first guide of this software for this forum, so it should be informative somehow. :P

(May 31, 2012 05:41 AM)Alside Wrote: [\[CITE\]](#) Nice share Lol and I know I hate when there is like 100+ views and only a few comments.

Lol.

At least it's not one of the trolling threads which gets flamed every now and then. :)

CyberZeist - May 31, 2012, 5:50 am

It is indeed very detailed and informative, too bad that many members here will overlook this thread's authenticity!

Ghost.13 - May 31, 2012, 5:52 am

(May 31, 2012 05:50 AM)CyberZeist Wrote: [\[CITE\]](#) It is indeed very detailed and informative, too bad that many members here will overlook this thread's authenticity!

That's fine.

I made it for the Search Button to find it. :P

?mnipotent - May 31, 2012, 6:13 am

Awesome thread! Y u no get more comments! This is awesome thanks for the tutorial. I will read all

of it later. Bookmarked.

R391.875 - May 31, 2012, 8:40 am

hats of 2 u sir!!expecting more tuts frm u,..

IzzY - May 31, 2012, 9:03 am

Awesome guide! Damn helpd me so much!

fenrirthewolf - May 31, 2012, 10:14 am

(May 31, 2012 05:30 AM)CyberZeist Wrote: [CITE](#) Its a basic level of doxing and target imaging.. nonetheless many beginners will benefit from it!

If this is just basic doxing then what are more advanced doxing techniques? Do you know other doxing tools out there? Not like sites but really tools like this one?

Great tutorial! Really!

prdx - May 31, 2012, 10:26 am

NiCe & Useful TUT Thank you intersting tool

Brody - October 15, 2012, 1:52 am

Your explanation of this software has motivated me to give it a try, their preview screenshots on their website are a bit overwhelming.

TheSpiritScience™ - October 15, 2012, 1:53 am

Good Tut, very informative! :D bookmarked

Toma - October 15, 2012, 8:17 am

Thanx dude ,really helpfull....:
msg too shoort

Feragonas - October 15, 2012, 9:29 am

Well written guide. I didn't know anything about doxing before this thread but now I know atleast something.

Ramditto - July 19, 2014, 11:23 pm

thanks! helped alot :D... keep making great tutorials! :)

sark89 - July 20, 2014, 10:51 am

Thanks for the post on this one OP! I've used Maltego a few times to map my works DNS records. Amazing what you can turn up!

hightechredneck - September 23, 2014, 8:41 pm

Thank you for posting this!! Very informative for a noob like me.

.THC - December 31, 2014, 3:08 pm

Bookmarking this for later, looks solid.