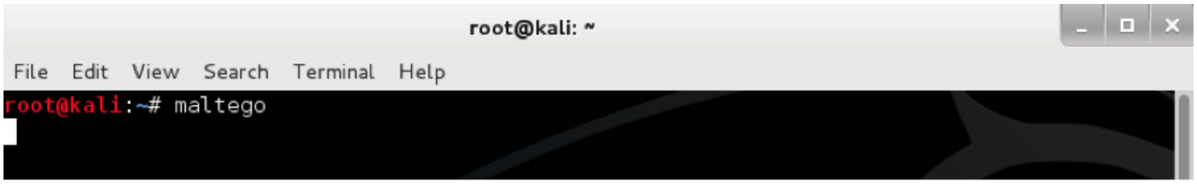
From: https://www.hackingloops.com/maltego/

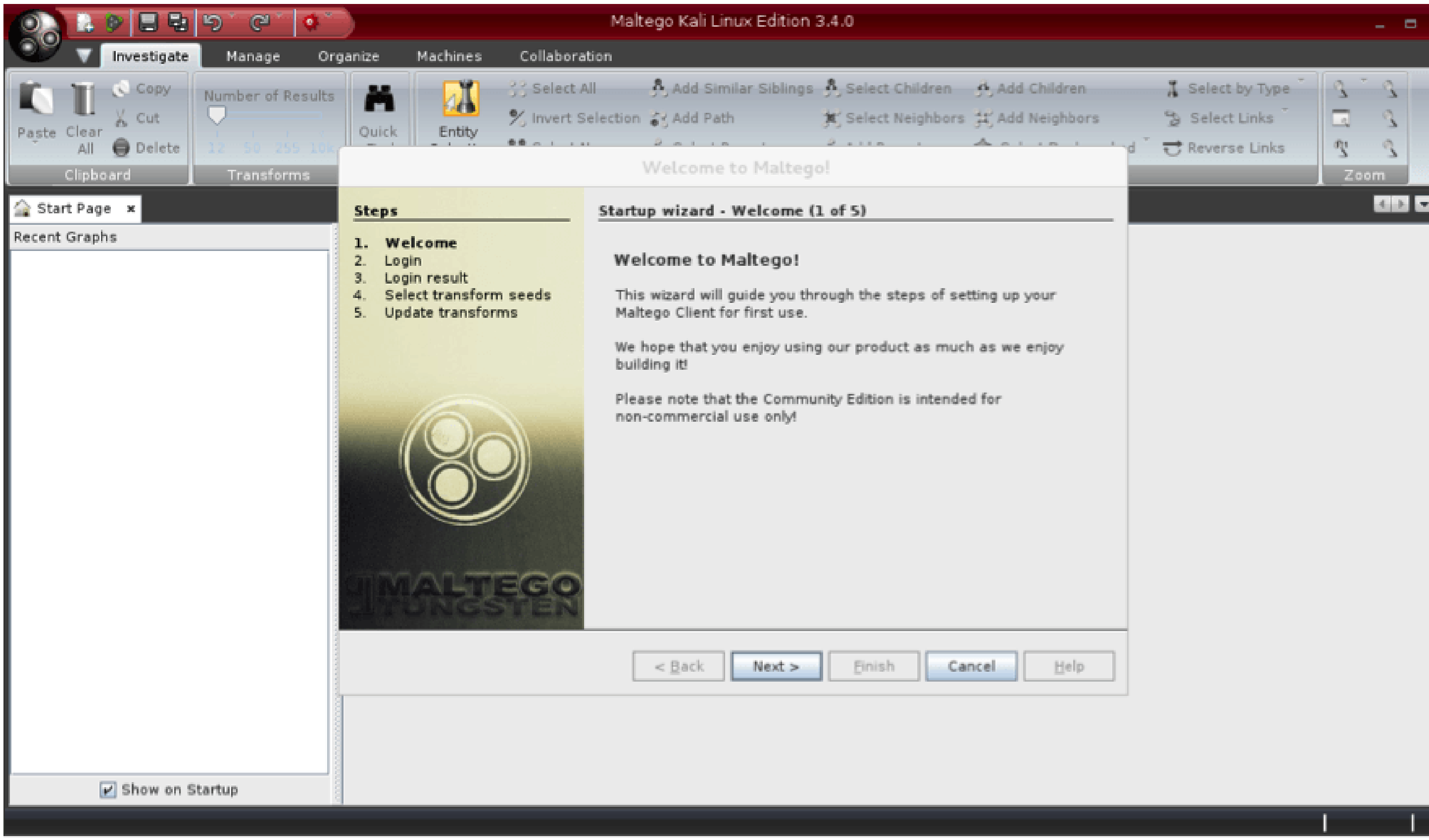
To start Maltego in Kali Linux simply type “Maltego”.



```
root@kali:~# maltego
```

You will see something that looks like the following graphic, and if you are booting for the first time it could take a couple of minutes:

When it finally boots you can see the setup and basic look of Maltego:



Steps

1. **Welcome**
2. Login
3. Login result
4. Select transform seeds
5. Update transforms

Startup wizard - Welcome (1 of 5)

Welcome to Maltego!

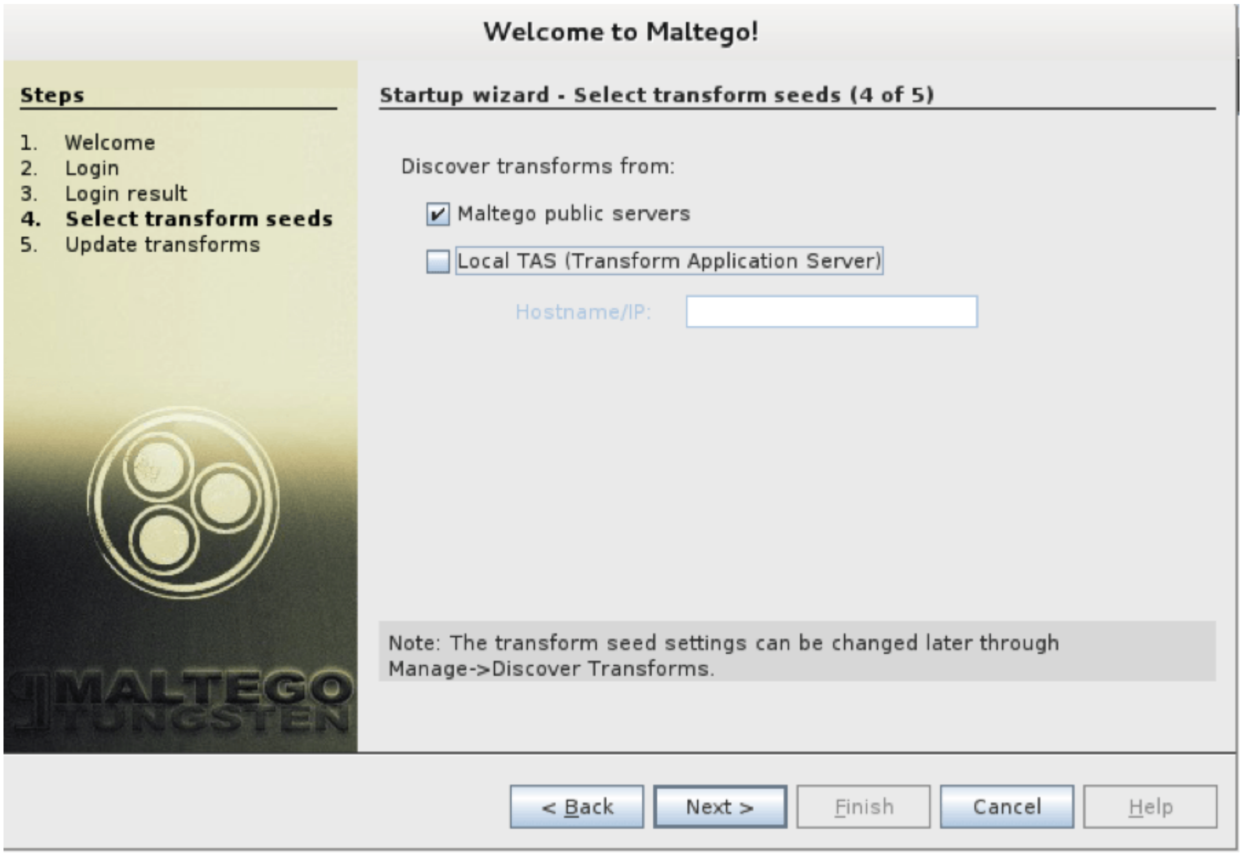
This wizard will guide you through the steps of setting up your Maltego Client for first use.

We hope that you enjoy using our product as much as we enjoy building it!

Please note that the Community Edition is intended for non-commercial use only!

From this setup screen just follow the steps by clicking next, create a login for yourself and then registering. The setup will guide you through all of that rather easily.

Once you’ve logged into the servers using the login you just created, you will see that “Maltego public servers” is checked. Just leave this checked, as these are the servers we want to discover transforms from and click next.



Startup wizard - Select transform seeds (4 of 5)

Discover transforms from:

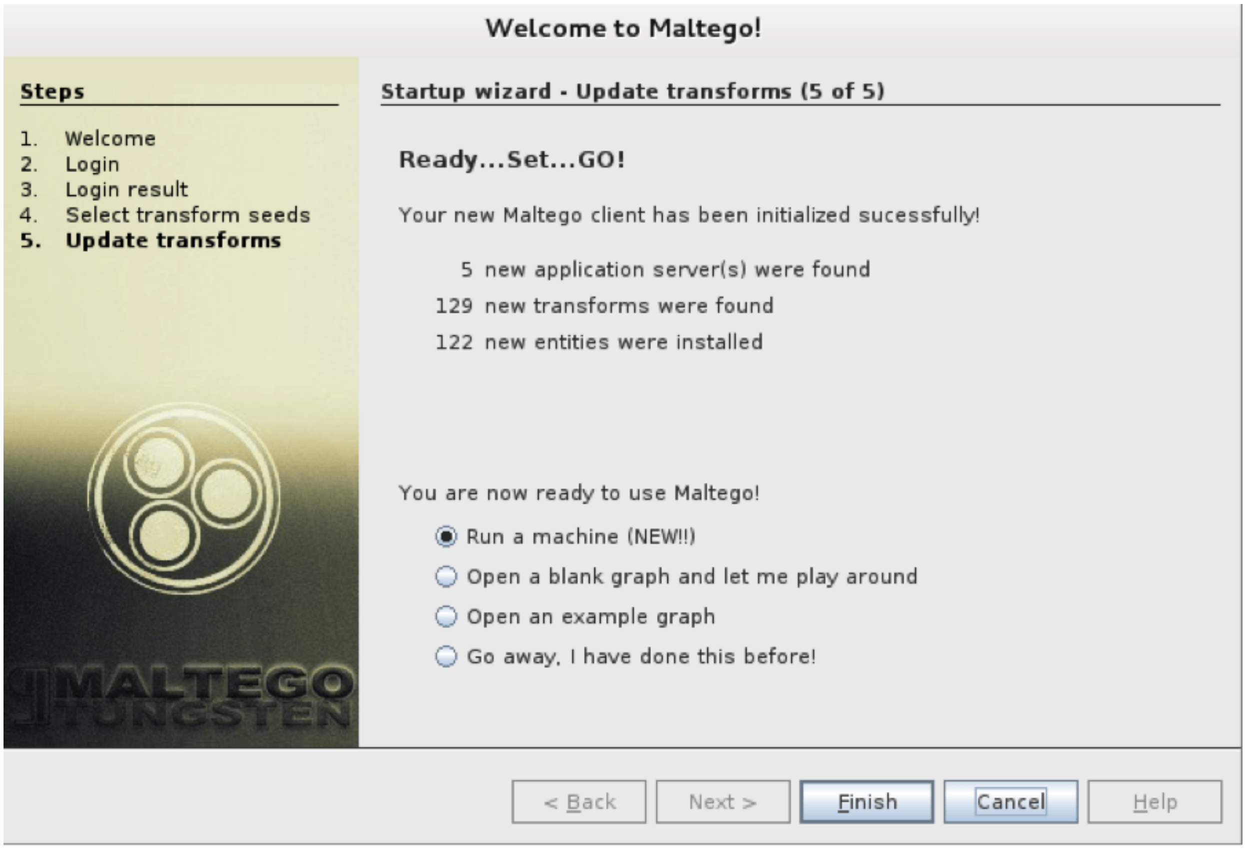
☑ Maltego public servers

□ Local TAS (Transform Application Server)

Hostname/IP:

Note: The transform seed settings can be changed later through Manage->Discover Transforms.

You will then see the following launch page that will finally let us get started. Just leave Run a machine (NEW!!) checked and click finish.



Welcome to Maltego!

Steps

1. Welcome
2. Login
3. Login result
4. Select transform seeds
5. **Update transforms**

Startup wizard - Update transforms (5 of 5)

Ready...Set...GO!

Your new Maltego client has been initialized sucessfully!

```
  5 new application server(s) were found
129 new transforms were found
122 new entities were installed
```

You are now ready to use Maltego!

● Run a machine (NEW!!)
○ Open a blank graph and let me play around
○ Open an example graph
○ Go away, I have done this before!

Ok, so now that is done it starts to get really interesting because on the next screen as you can see below, we are actually able to choose the type of reconnaissance we want to do now on our target. We have several options but lets just do a quick overview of some of the more important ones:

Company Stalker

This option basically allows us to select a particular domain, from that it searches for all the email addresses it can find and from there it tries to find all the social media networks it can find.

Footprint L1

- This is a basic footprint of a domain in its simplest form.

Footprint L2

- Same as above just a little more involved and will take a little longer. We might get a bit more data than the most basic Footprint above.

Footprint L3

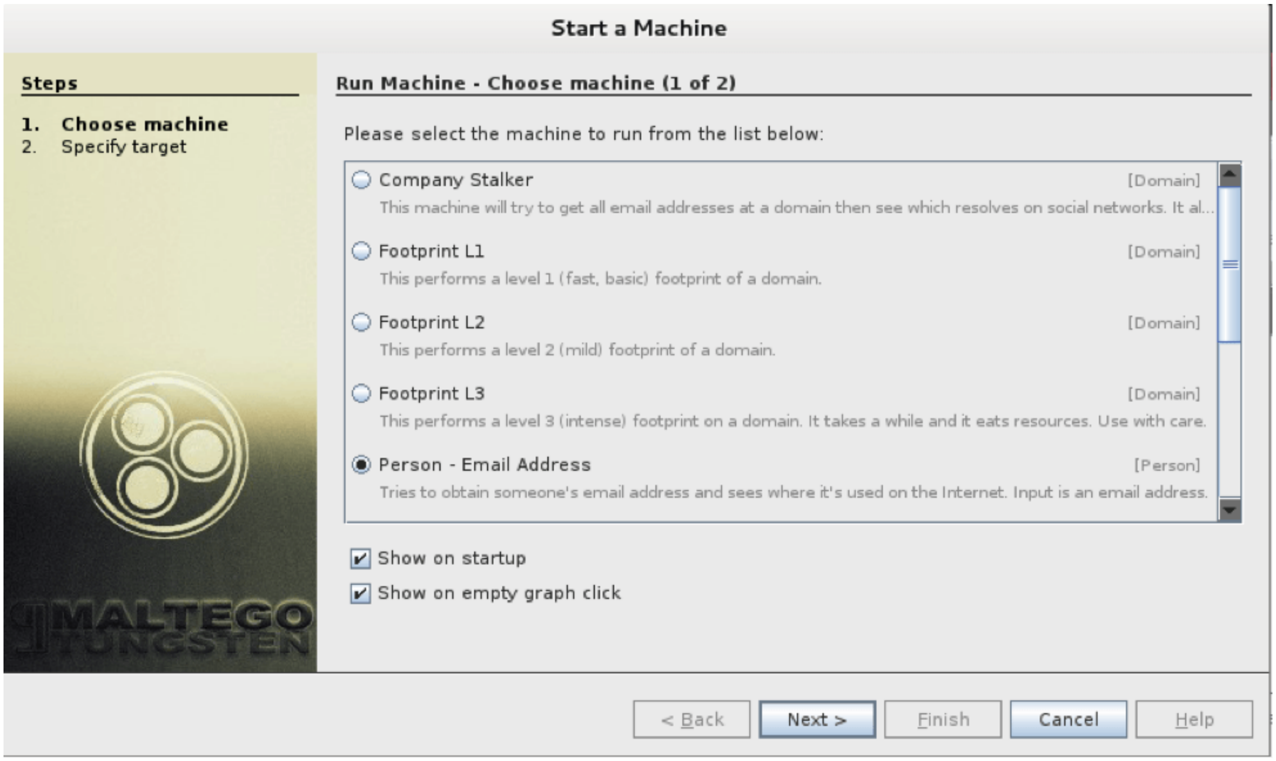
- Same as the other two above except much more involved. This can take a ton of time to complete but might also net us much more information in the end.

Person – Email Address

- You input an email address and it sees what it can find using that out on the web.

URL To Network And Domain Information

- You input a URL and you get back network information.



Start a Machine

Steps

1. **Choose machine**
2. Specify target

Run Machine - Choose machine (1 of 2)

Please select the machine to run from the list below:

○ Company Stalker [Domain]
This machine will try to get all email addresses at a domain then see which resolves on social networks. It al...

○ Footprint L1 [Domain]
This performs a level 1 (fast, basic) footprint of a domain.

○ Footprint L2 [Domain]
This performs a level 2 (mild) footprint of a domain.

○ Footprint L3 [Domain]
This performs a level 3 (intense) footprint on a domain. It takes a while and it eats resources. Use with care.

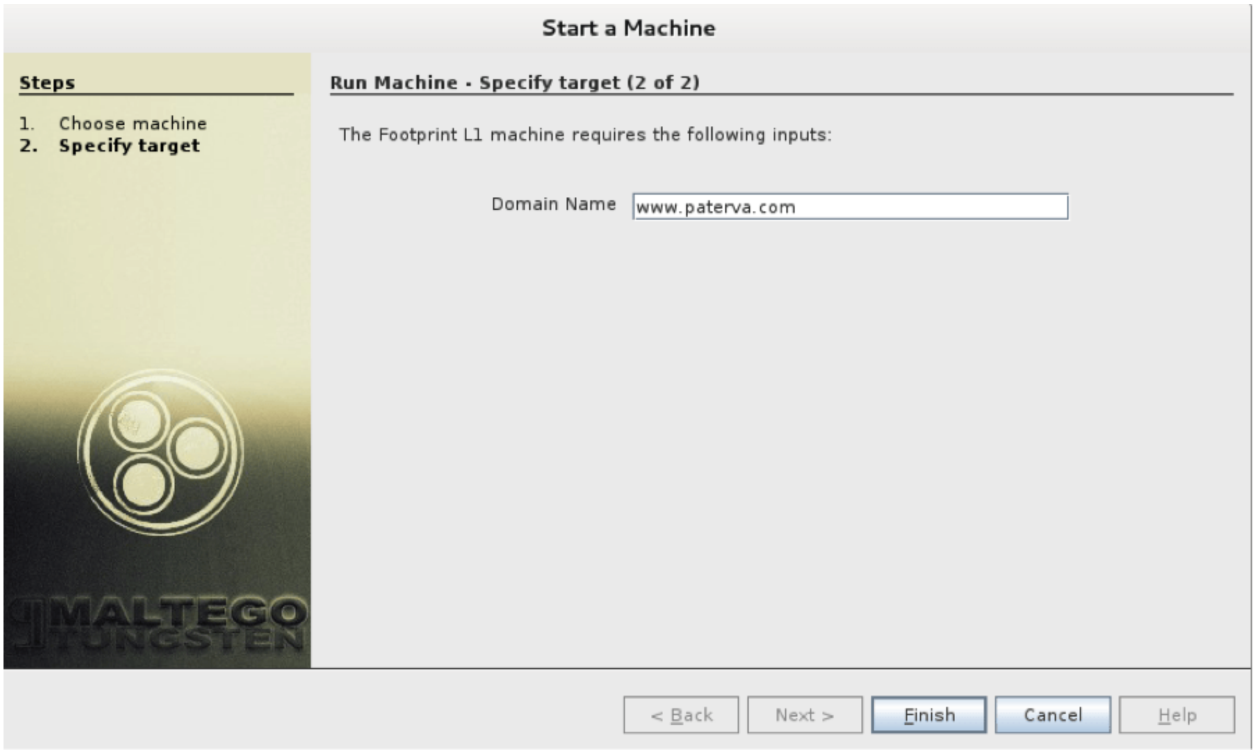
● Person - Email Address [Person]
Tries to obtain someone's email address and sees where it's used on the Internet. Input is an email address.

☑ Show on startup

☑ Show on empty graph click

For this next exercise lets just do the basic Footprint of an organization for now. It will be the quickest and let us see how the basic functionality works. Select Footprint L1 and click next.

Lets do a Footprint on the company that created Maltego: www.paterva.com:



Start a Machine

Steps

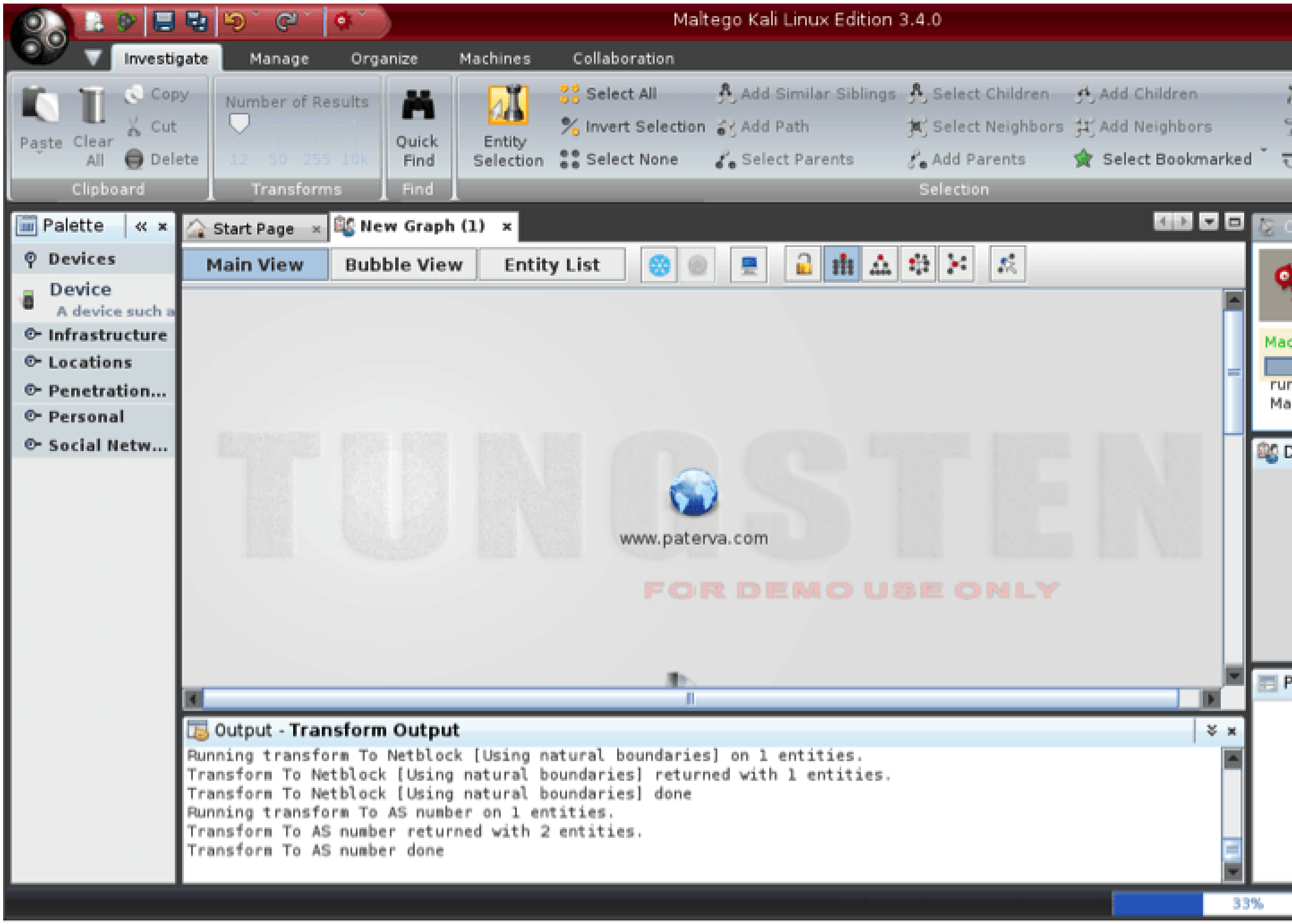
1. Choose machine
2. **Specify target**

Run Machine - Specify target (2 of 2)

The Footprint L1 machine requires the following inputs:

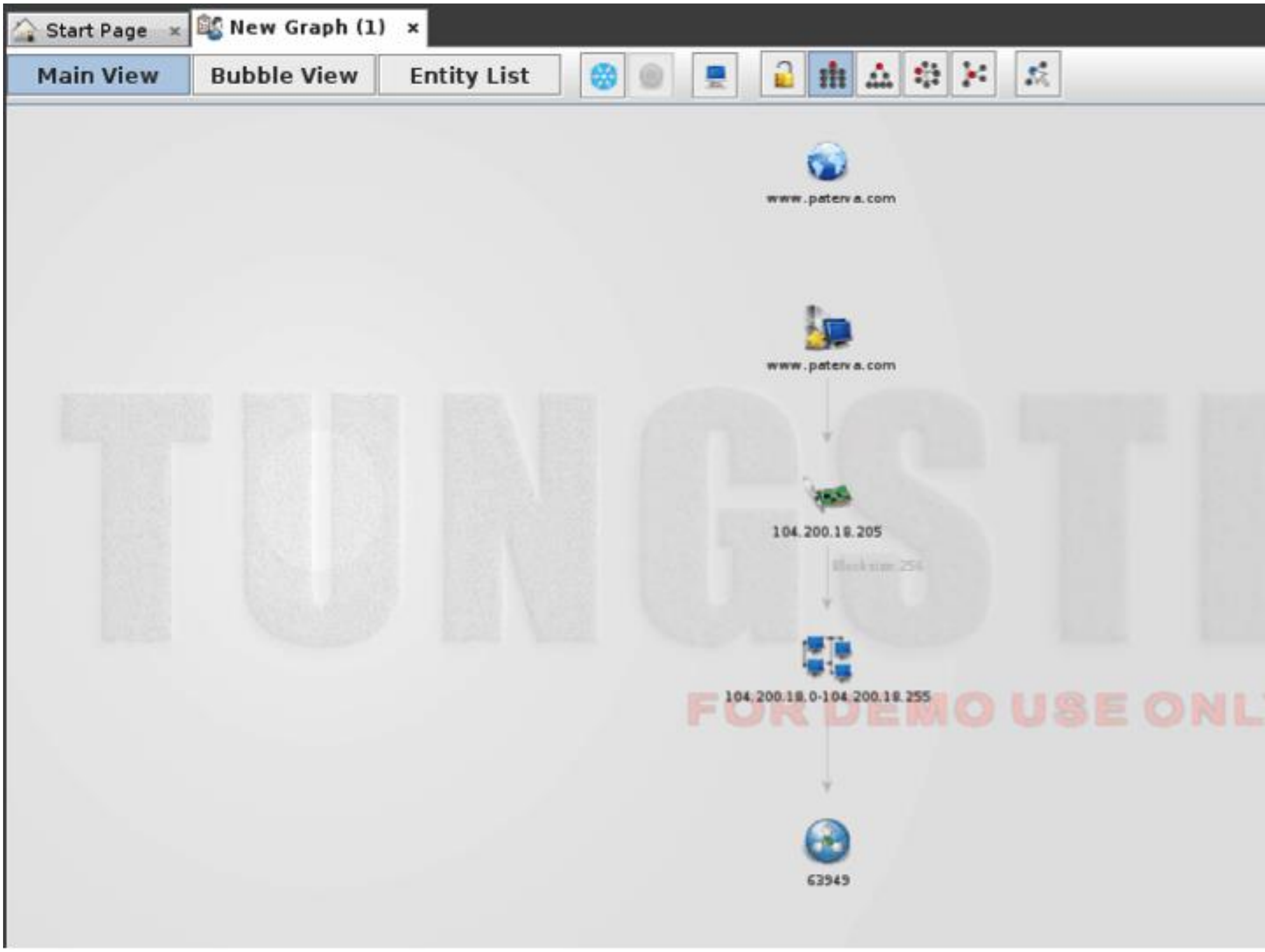
Domain Name www.paterva.com

From there you just hit run and Maltego will automatically start Footprinting the domain for you. If you have ever done reconnaissance you know how amazing a tool like this is because it takes time to do the proper research on your target and generally speaking when conducting a pentest, the reconnaissance is the part that takes the longest.



```
Running transform To Netblock [Using natural boundaries] on 1 entities.
Transform To Netblock [Using natural boundaries] returned with 1 entities.
Transform To Netblock [Using natural boundaries] done
Running transform To AS number on 1 entities.
Transform To AS number returned with 2 entities.
Transform To AS number done
```

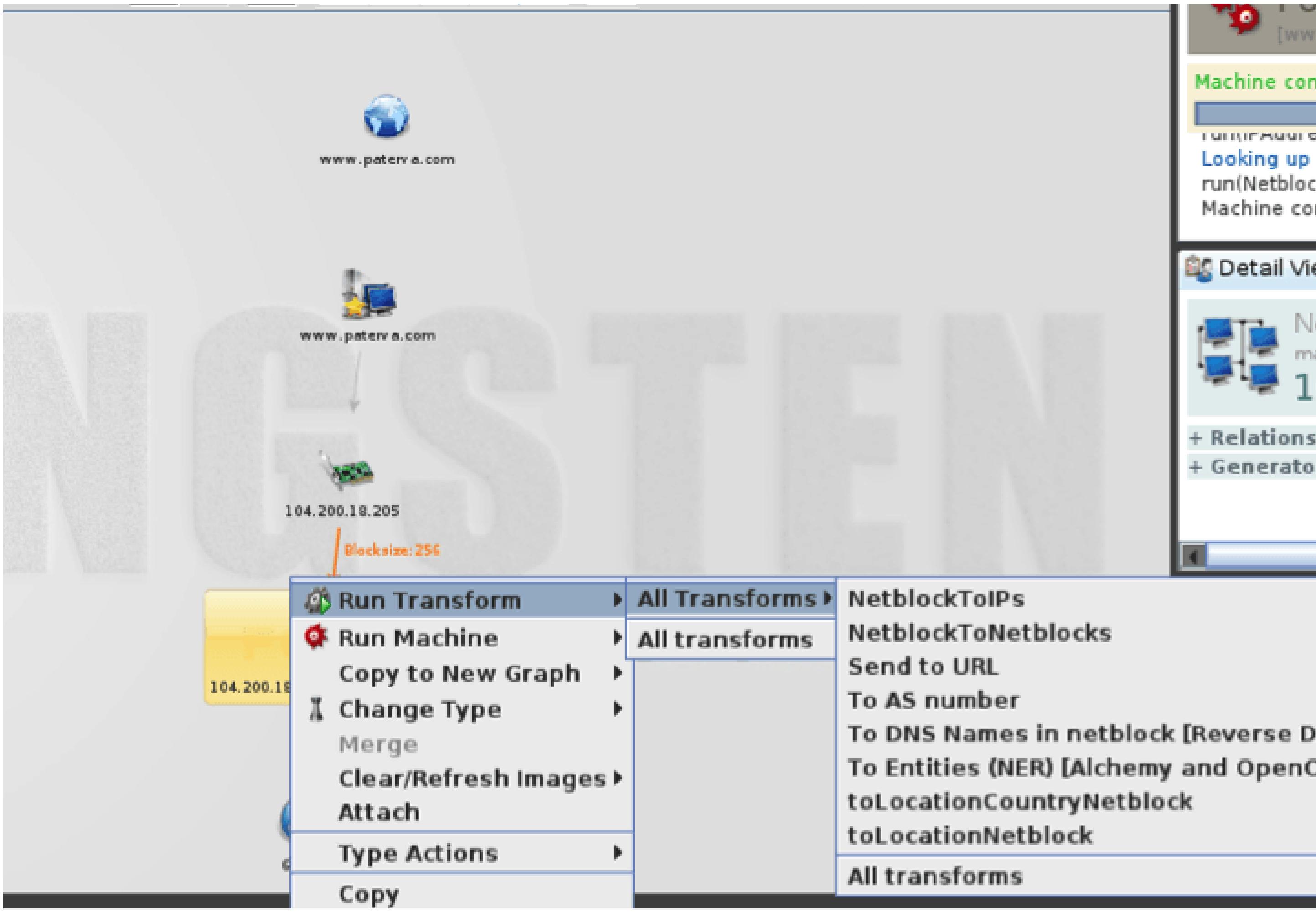
Just below our new graph it created, you might notice the Transform Output. This is output of the actual Footprint transform in action and gives us a look at what it is looking for. You might also notice the domain we typed in laid out in an easy to digest graph format. You also might notice if you zoom out of the graph a bit it will reveal some other entities besides the domain you typed in.



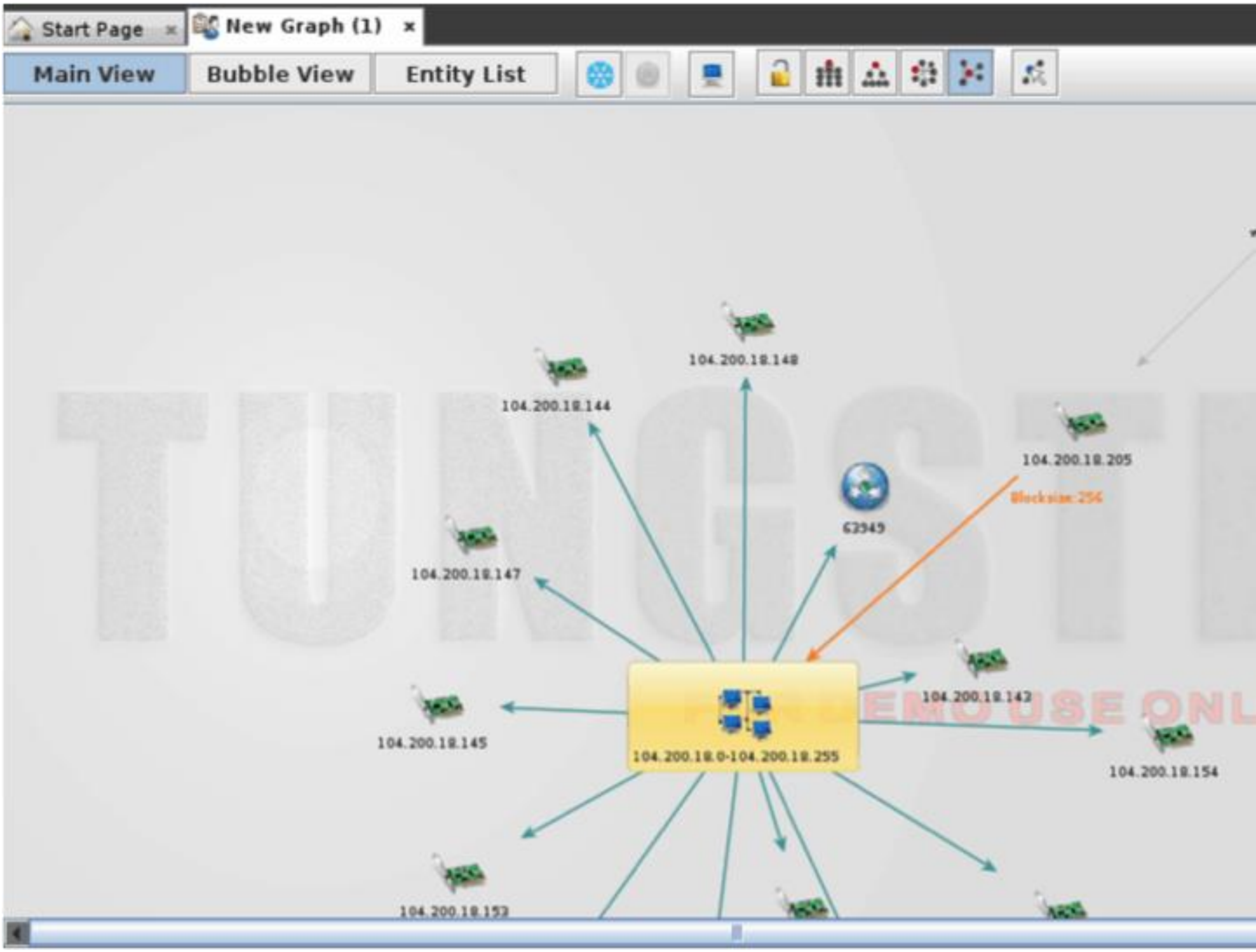
Using the most basic Footprint starting with only the domain we were able to find the website, IP Address, Netblock and AS Number. Not a ton of information but much more than we had before and these pieces will help us find other crucial information on the treasure map that is our target.

So now that we know some basic functionality on how this works, lets try and use that to take our Footprinting further. You might have noticed in the graph that there looks to be several computers in a cluster with an IP Range below it. This is a netblock that the domain belongs to. So if we take a second to think about that, we could reasonably assume that there may be other systems on the same netblock that might be relevant to our initial target.

With that information we could simply right click the netblock and run the transform NetblocktoIPs:

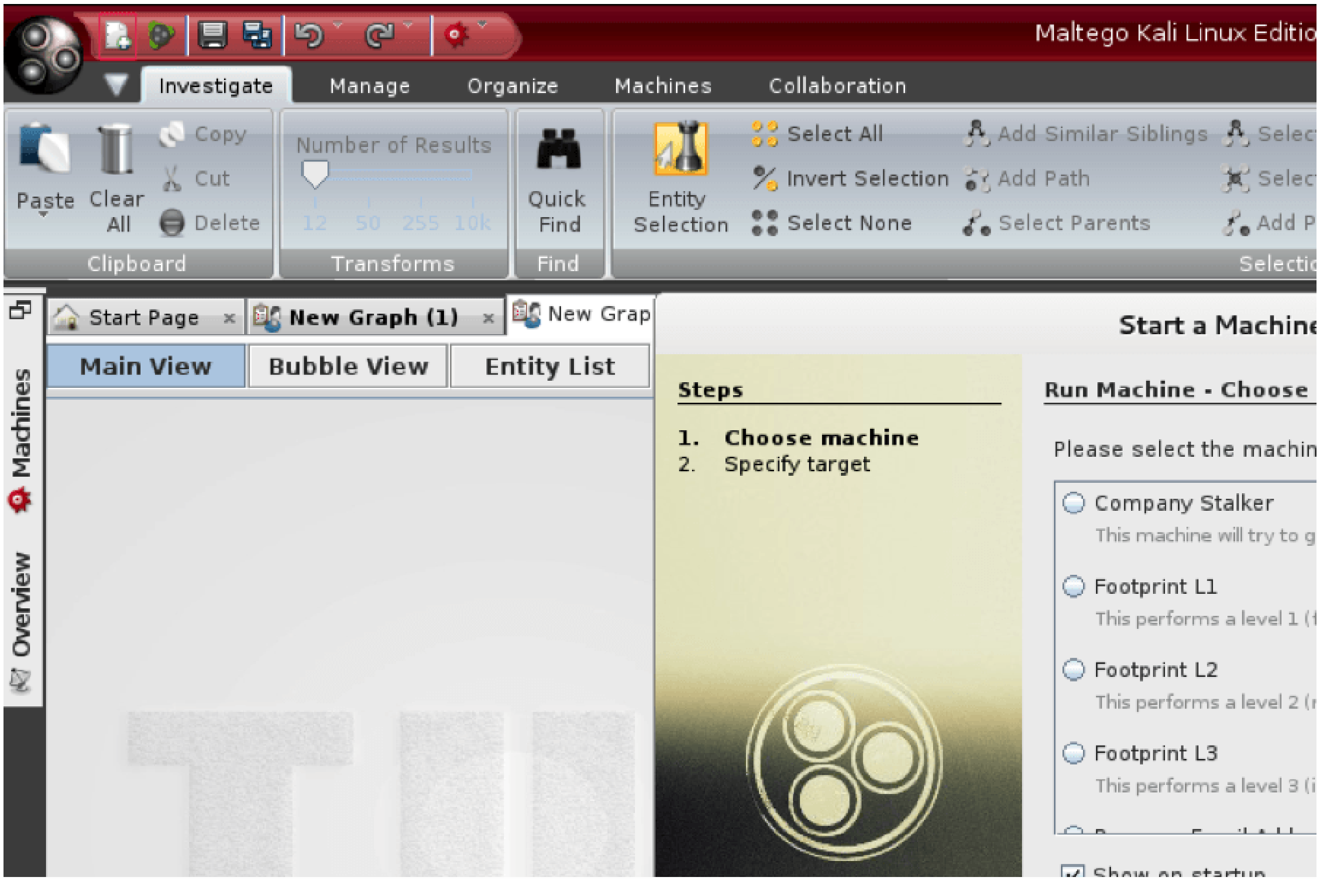


That then gets us what we were looking for and we have found other machines within that netblock that might be relevant:



Chances are that some of these machines might belong to www.paterva.com. From there we could then run new transforms on each of these machines to produce an even more detailed map of our target. You can now see how powerful this tool is as you have the ability to keep running these transforms until you find what you need.

To get started from scratch and create a completely new transform you can click the “create a new graph” icon in the top left hand corner. You can then just right click anywhere on the new graph and you will be able to choose a starting point once again:



Start a Machine

Steps

1. **Choose machine**
2. Specify target

Run Machine - Choose

Please select the machin

○ Company Stalker
This machine will try to g

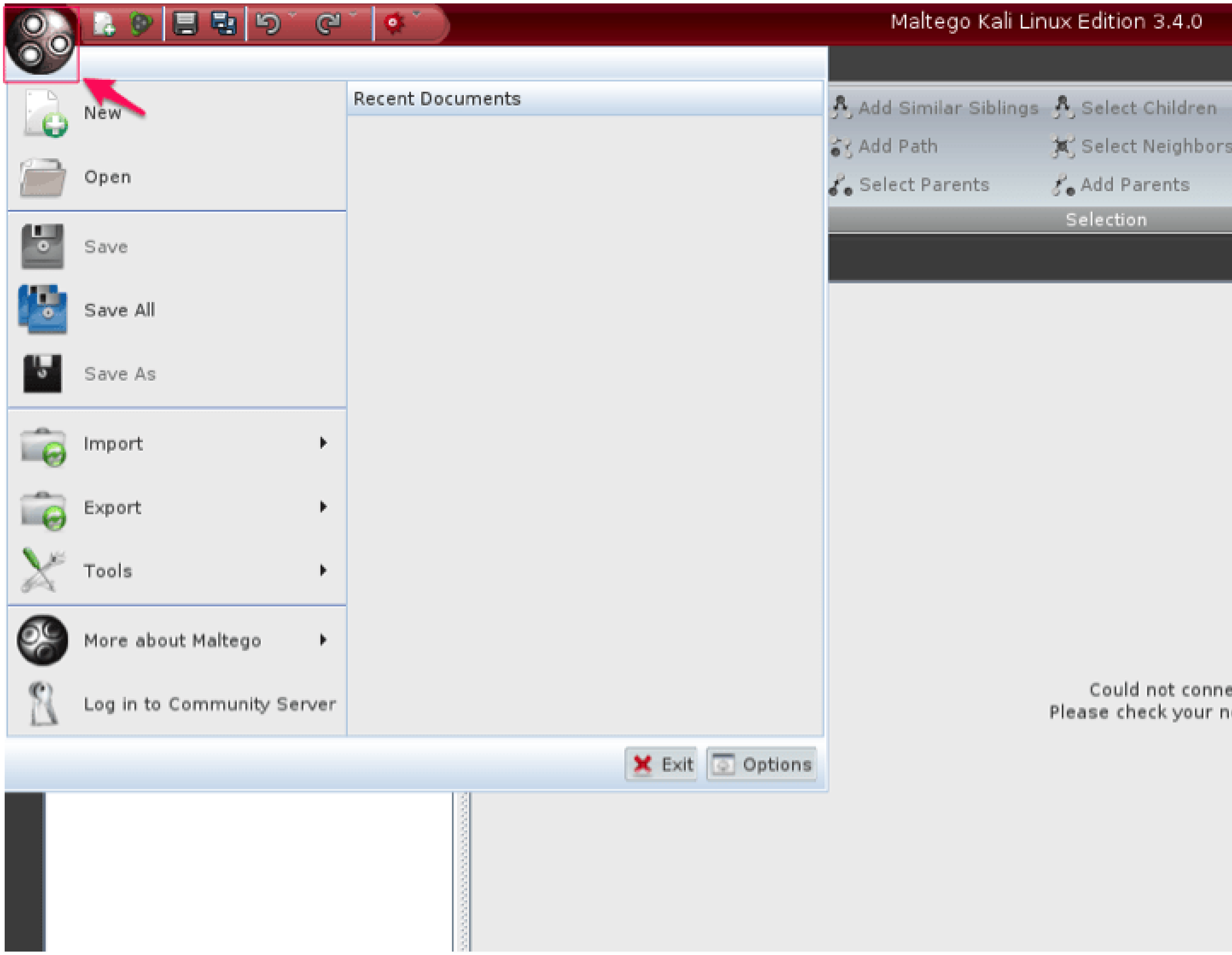
○ Footprint L1
This performs a level 1 (f

○ Footprint L2
This performs a level 2 (r

○ Footprint L3
This performs a level 3 (i

☑ Show on startup

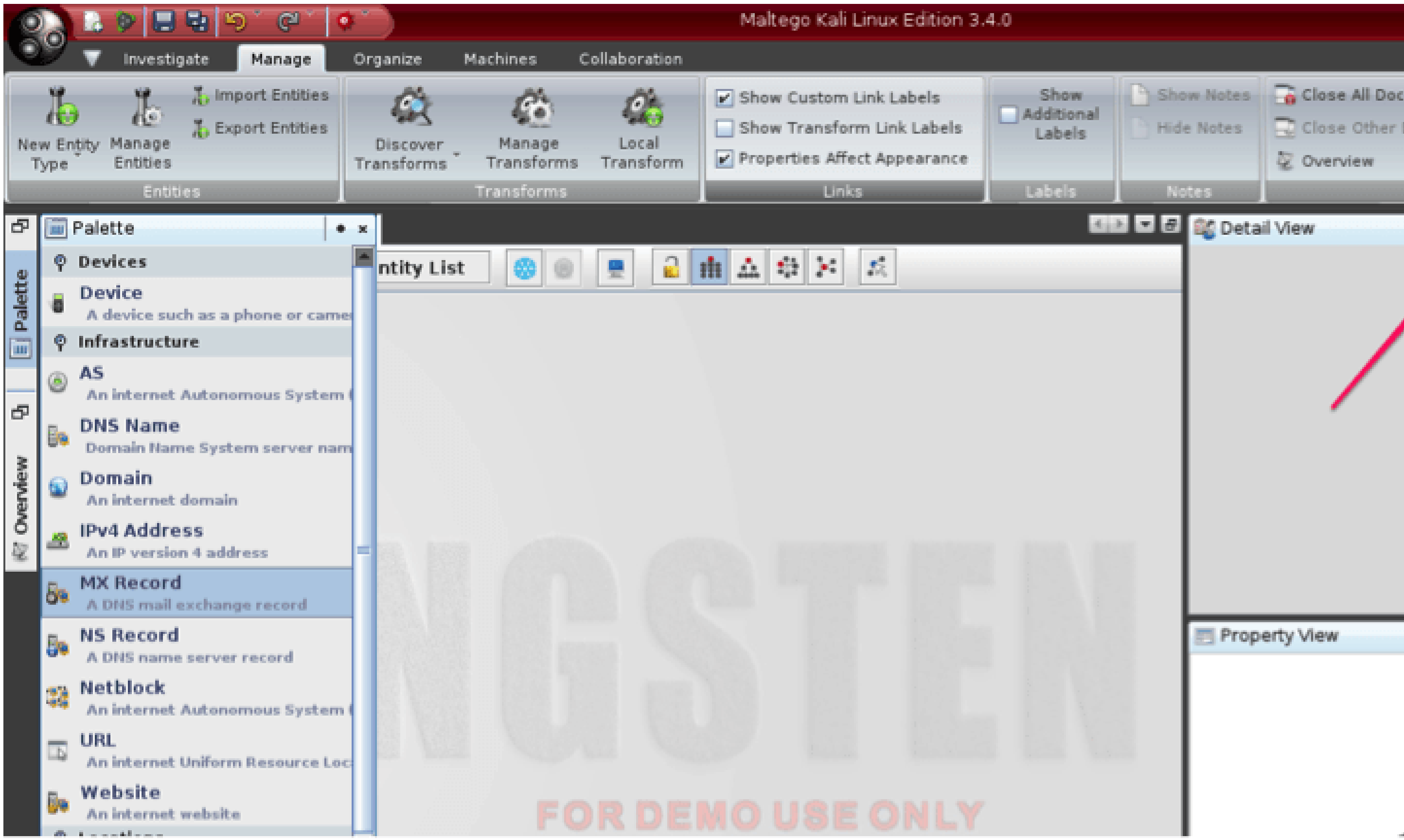
You can also use the main menu option, which is the large circular button (top left) to create a new graph, open an older one or save the current one as well.



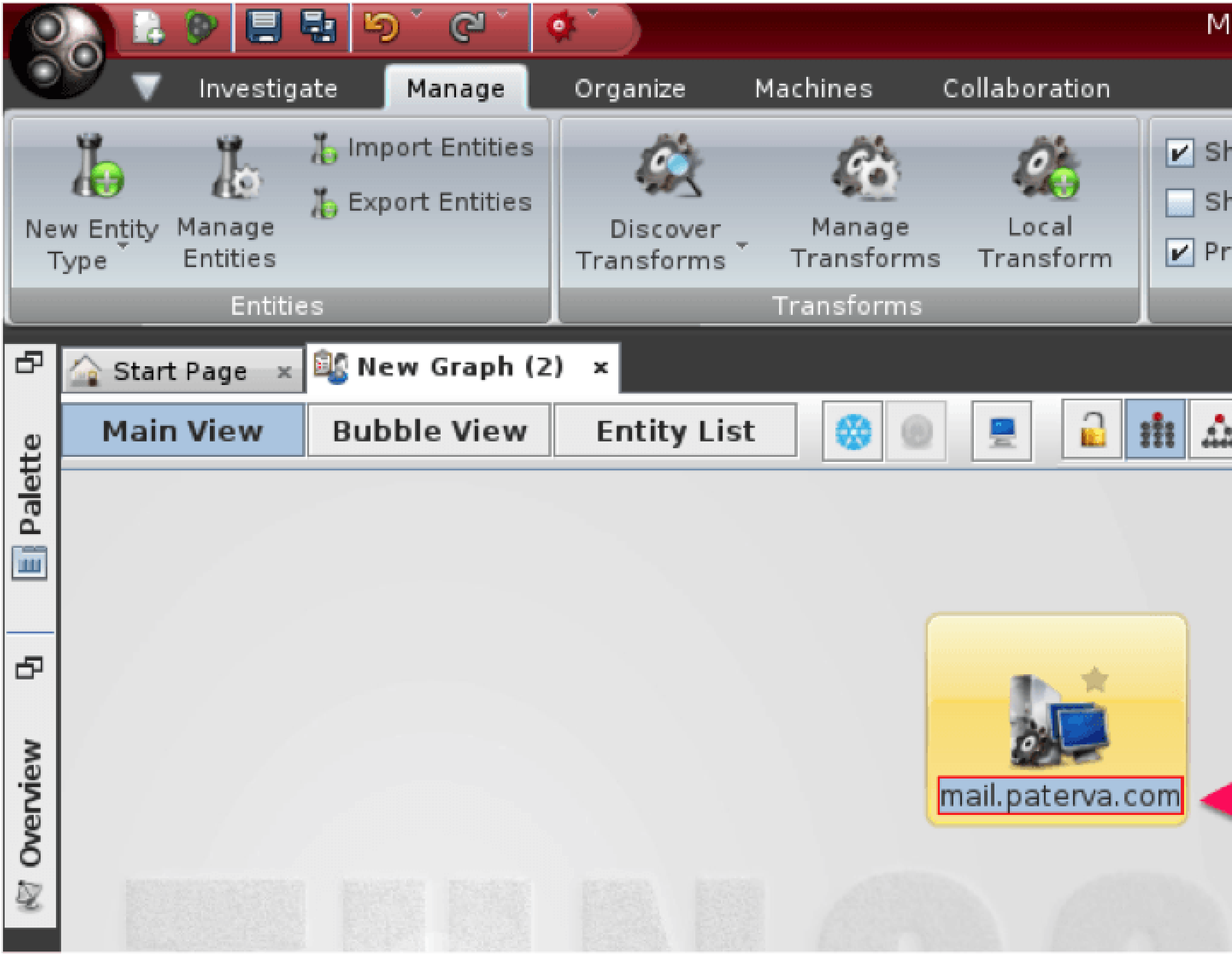
Could not conne
Please check your n

In the above tutorials we used default Footprinting transforms at the most basic levels for network intelligence gathering. There will be many other times where we need to be more specific in narrowing our search to one specific device, location or personal piece of information.

Lets say for this example that all we have is a mail server name and we need to use that as the starting point on our map because at this point it is all we have. We first need to find that particular item to place on our map. One way we can do that is by opening up the Palette menu box. You can get there by going to the Manage tab and then find the Palette options in the Windows section.



We then can drag the MX Record item on to our graph. You will notice below that when you drag it over it uses the default MX Record of mail.paterva.com. We can change that though by double left clicking the item name and typing in the MX Record that we want to use.



From there as we did above we can use this one item to build out this great visual that paints a picture of our target in a way that is most easy for our brains to understand. We can even drag over more items from our Palette if we already have that information. Some examples are an IP Address, MX Record, Netblock, URL, Website, DNS Name, email address, phone number, document or even a location.

Overall Maltego is an amazing tool for research and there is good reason why security firms look for Pentesters to have experience with it. However, I must caution that you can never rely on one tool to do proper reconnaissance. This tool should be one of the many items in your toolset to help you paint a proper picture of your target. Not to mention tools don’t always get it right so make sure you perform your due diligence when conducting your next pentest.

What to submit:

Short report (up to 500 words) of what you have learned and a screenshot of the paterva email structure.

Other sources:
https://www.paterva.com/web7/docs/userguides/user_guide.php#getting-started