**Lab - Gathering Information Using Maltego CE**

1. Do not use a Wi-Fi connection. Use an Ethernet cable to connect to the netw ork. Wi-Fi is

**Ove rvie w**

The focus of Maltego is analyzing  real-world relationships  between information  that is publicly

accessible on the Internet. This includes footprinting  Internet infrastructure as well as gathering

information  about the people and the organization  who owns it.

**Hardware  re quire me nts  for the s e  labs :**

configured for IPSec which can impede the labs from w orking.  The additional transport and   
tunneling protocols do not play w ell w ith Kali or Metasploit.

The first phase of security assessment is to focus on collecting  as much information  as possible

about a target application.

According to OWASP, information  gathering is a necessary step of a penetration test.

The more information,  the higher the success rate. There are basically two types of information

gathering:  active and passive. Passive information  gathering is where the attackers won’t be

contacting the target directly and will be trying to gather information  that is available on the

Internet; whereas in active information  gathering, the attacker will  be directly contacting the

target and will be trying to gather information.

Information gathering is generally done on infrastructure and on people. In infrastructure recon,

the attackers generally try to find the information  about the host, i.e., the mail exchanger record,

name server record , shared resources, etc., For information  gathering on people, the attackers try   
to gather information  like email addresses, their public profiles, files publicly  uploaded, etc., tha t

can be used for performing a brute force, social engineering  or Spear phishing.

**About OSINT:**

OSINT stands for Open Source Intelligence. In OSINT method, the information  is basically

found publicly,  and that information  can be used to further analysis. The relationship  between the

various forms of information  gathered from the Internet can be extremely valuable from the

attacker’s point of view. In this method, there is no direct contact with the victim’s servers or

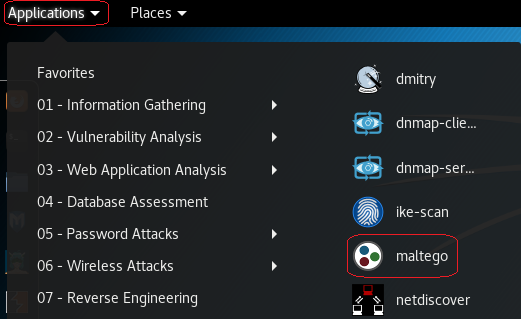
only standard traffic is directed toward the victim.

Maltego is an example which uses OSINT to gather information.  **Malte go** is an open source   
intellige nce  and forensics application  and shows how information  is connected to each other.

Another advantage of this tool is that the relationship  between various types of information  can

1

give a better picture of how they are interlinked  and can also help in identifying  unknown



relationships.

**What information can be  found us ing Malte go  CE:**

**Cave at**

**Malte go CE Re strictions and Limitations**

Maltego CE is the community version of Maltego that is available for free after quick online[registration](https://www.paterva.com/web7/community/community.php).

Maltego CE includes most of the same functionality as the commercial version how ever it has some

limitations. The main limitation w ith the community version is that the application cannot be used for   
commercial purposes and there is also a limitation on the maximum number of entities that can be

returned from a single transform. In the community version of Maltego, there is no graph export   
functionality that is available in the commercial versions. 

With Maltego, we can find the relationships,  which (people) are linked  to, including  their social

profile, mutual friends, companies that are related to the information  gathered, and websites.

If we want to gather information  related to any infrastructure, we can gather relationship  between

domains, DNS names, and netblocks.

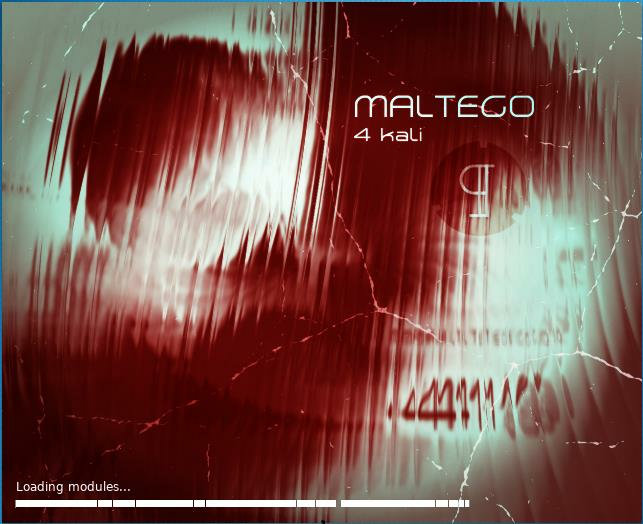
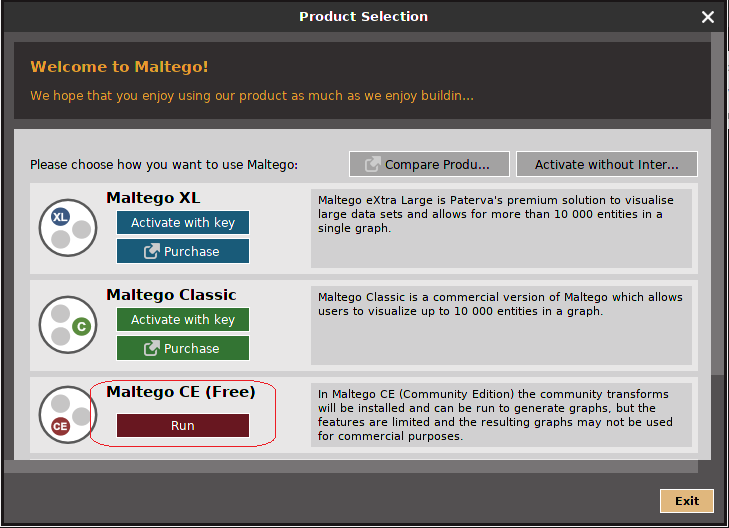
**Starting Malte go**

First, go to Applications–>Kali  Linux–>Information  Gathering–>Maltego

Maltego launches

2

Maltego minimizes  to the quick launch bar. Click to open.

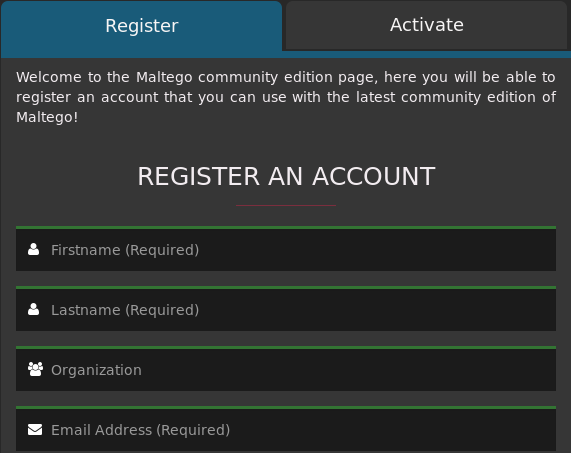
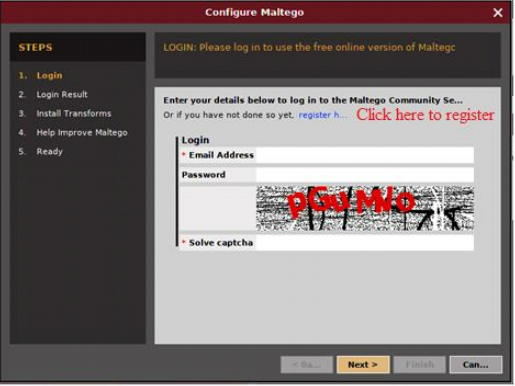


On the next screen, choose the Maltego CE (Free) edition and click Run.

The first time you log in it will ask you to register your product.

3

If you don't have the login  information,  you need to register yourself first by clicking  on



the **re gis te r he re** link.

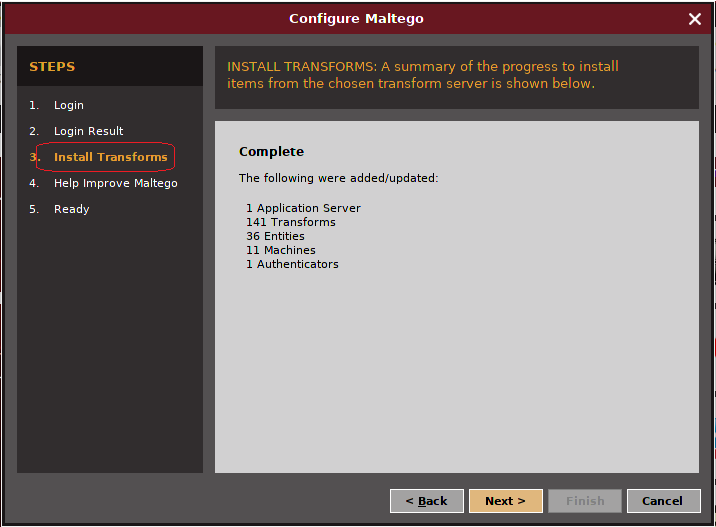
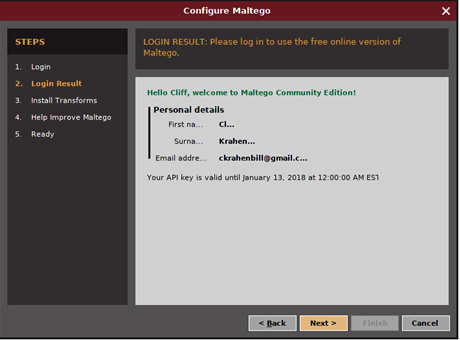
The following  screenshot shows the Register page scroll down to register an account:

[https://www.paterva.com/web7/community/community. php](https://www.paterva.com/web7/community/community.php)

Your login will update the transforms.

4

You will see the Maltego welcome screen. After several seconds, you will see the



following  Maltego start-up wizard that will help you set up the Maltego client for the

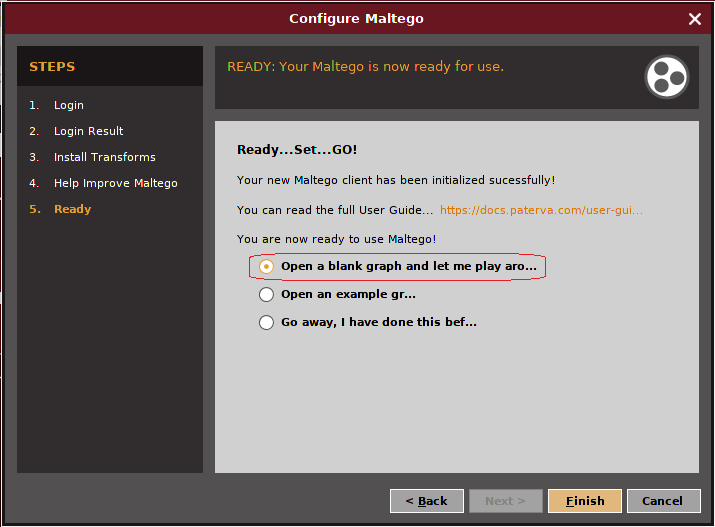
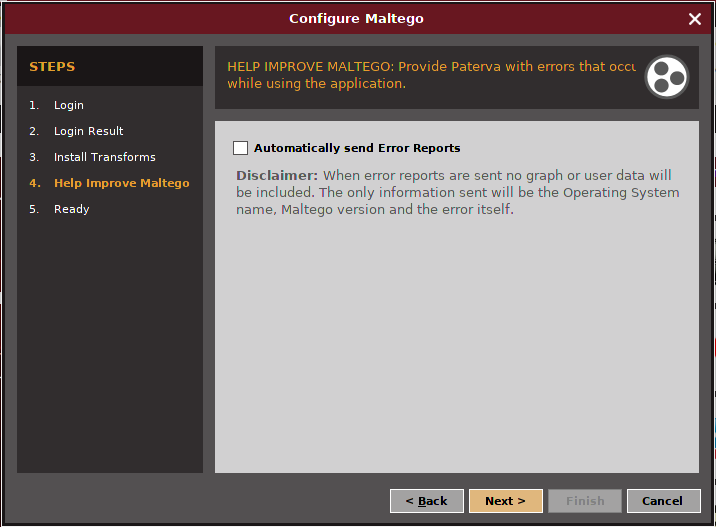
first time.

Click next to install  the Transforms. Once the transforms have installed,  click next.

Choose to help improve Maltego.

5

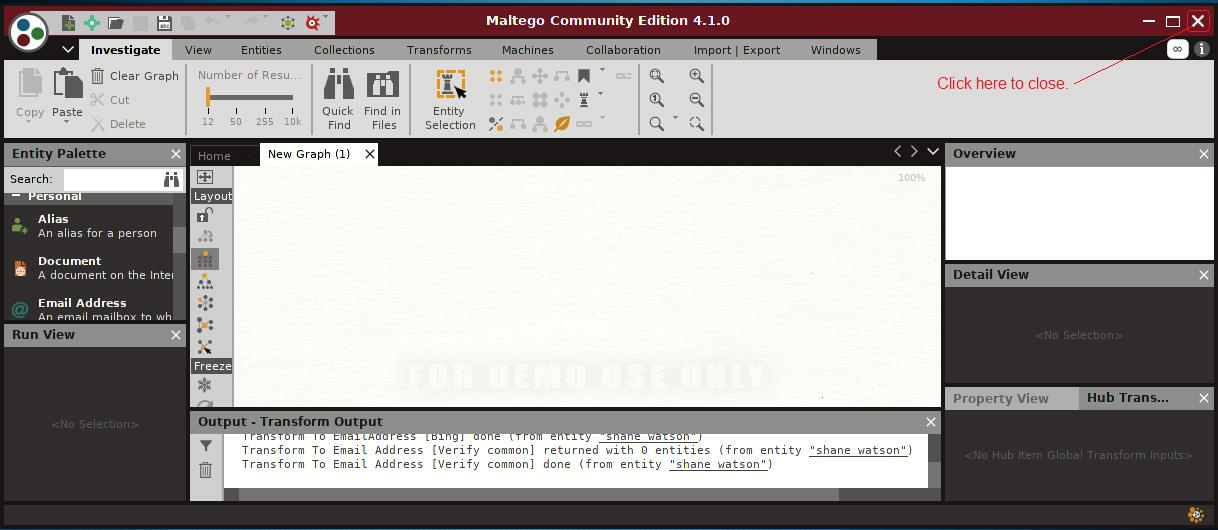
Accept the default radio button and click finish.



Once you click the finish button, Maltego will launch the new graph window.  Place your mouse   
on the X in the top right corner to close the new graph window.

6

This brings us to the main management console.  In the right window pane, you can look through   
the additional  transforms that are available.  Some these will require that you register for an API



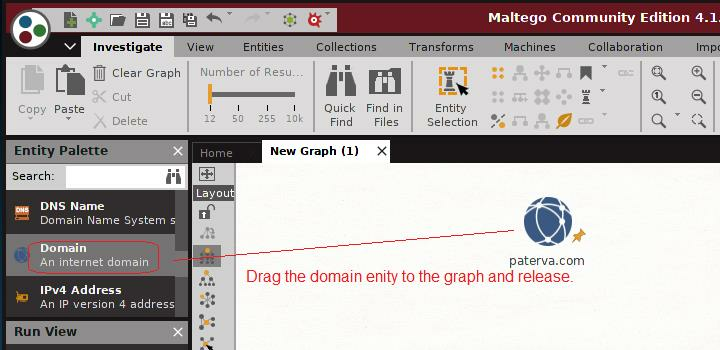
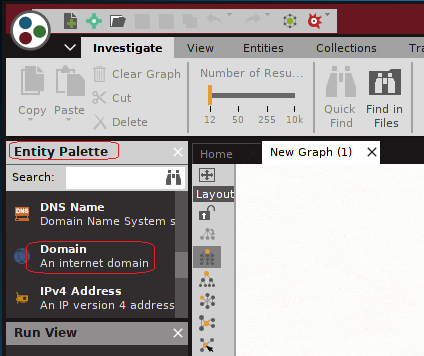
key and will require some additional  configuration.   As you become more proficient with   
Maltego, you might find these additional  transforms to be needed.

From the management console window, go to the top left and click on the + sign to open a new   
graph window.

Over in the left windowpane, you will see all the different entities that we can gather information   
on.  Using the slider bar in the left windowpane, scroll down until  you come to, Domain.

7

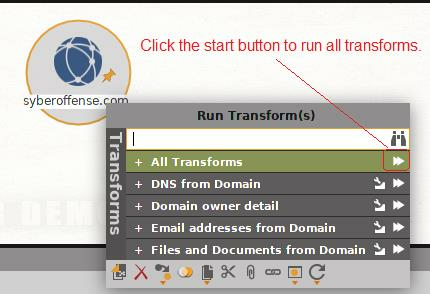
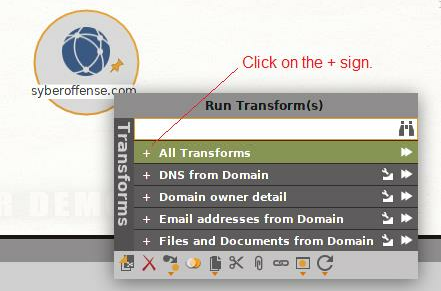
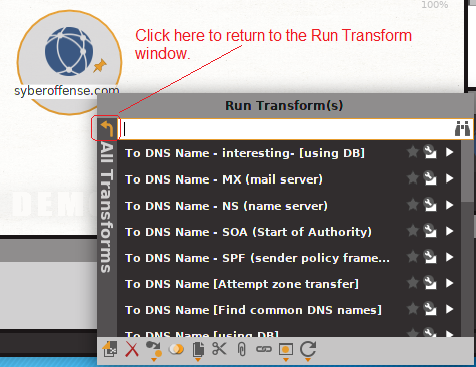
Using your left mouse button, drag the domain entity to the center of the graph and release.



Click on the existing domain name until  you get a cursor.  Type in any domain of your choosing,   
or you can use the one shown in the video and in this lab, **s ybe roffe ns e .com.**

8

Right-click  on your domain name, and this brings up the run transform window.  Click on the +   
sign next to All Transforms to see all the scripts or transforms that are about to run against your



domain entity.  Click on the back arrow to return to the All Transforms option.

To the right of the green all transforms box, click on the start button to run the transforms.

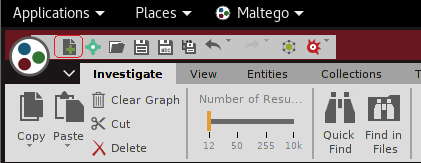
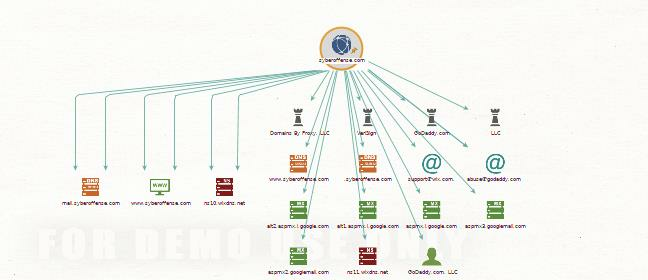
As the results of the transform search begin to return, the graph window begins to fill up.  Using   
your left mouse button, you can click on the graph and use your scroll wheel; you can zoom in

and out of the graph window.

9

You can click on any of the results inside the graph to get more information  about each of the   
transforms that we’re running.  Depending on whether your whois information  for the domain

was made public  or private, will depend on how much information  about your domain search   
Maltego will gather.



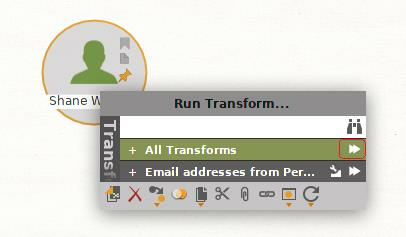
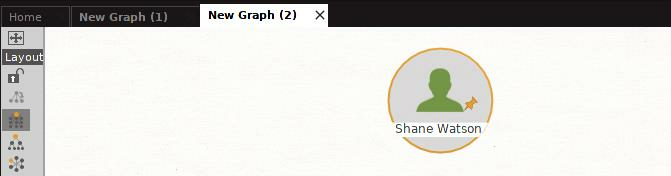
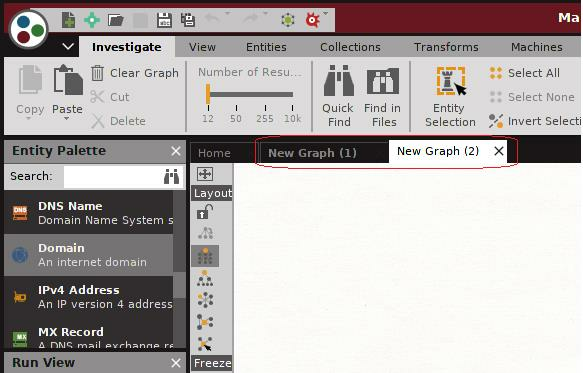
**Gathe ring Information About an Individual**

At the top left of the console window, click on the + that opened a new graph.

You will now have two graph windows tabbed side-by-side

10

In the left windowpane marked entity palette, scroll down until you come to, Person.  Using your   
left mouse button, select the entity Person and drag on to the graph window.



Click on the entity inside the graph window until you get a cursor where the name is.  Change   
the name to any person you want or use the example I am showing in the video and in this lab.

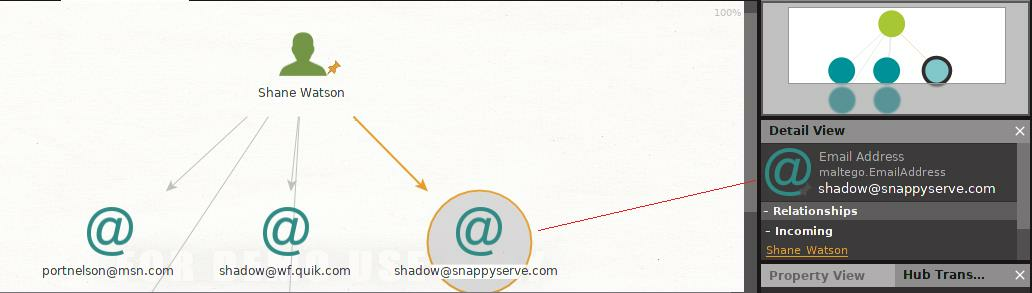
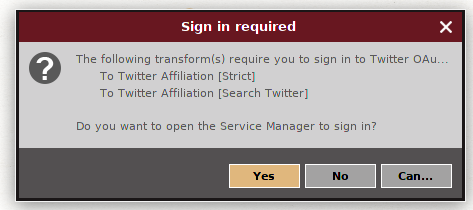
For this example, I am looking  for information  about an individual  named Shane Watson

Right-click  on the individua l’s  name and click on the start button to run all available transforms

against this individual.

11

Choose whether to logon to your Twitter account or not.



As with the domain transform results, you can click on any of the returned information  to get   
more information  about the transform in the right windowpane.

**Summary**

As we have seen in this lab, Maltego is a very powerful reconnaissance tool.  Be sure to use your   
newfound powers for good and not evil.  It is easy to see how such a tool could be used for

stocking or cyberbullying.

End of the lab!

12