What does Maltego do ?

- **Maltego** is an **Information gathering tools** inbuilt in **Kali Linux** by default and can be used for determining the relationships and real world links between:
    -
    - People
    - Groups of people (social networks)
    - Companies
    - Organizations
    - Web sites
    - Internet infrastructure such as:
        - Domains
        - DNS names
        - Netblocks
        - IP addresses
    - Phrases
    - Affiliations
    - Documents and files
- These entities are linked using open source intelligence.
- Maltego is available for Window, Mac and Linux. You can download and install it on any platform.
- Maltego is comes with Graphical interface that makes easy to use and see these relationships instant and accurate.
- Using the graphical user interface (GUI) you can see relationships easily – even if they are three or four degrees of separation away.
- Maltego is unique because it uses a powerful, flexible framework that makes customizing possible. As such, Maltego can be adapted to your own, unique requirements.

Use of Maltego as Information gathering tools:

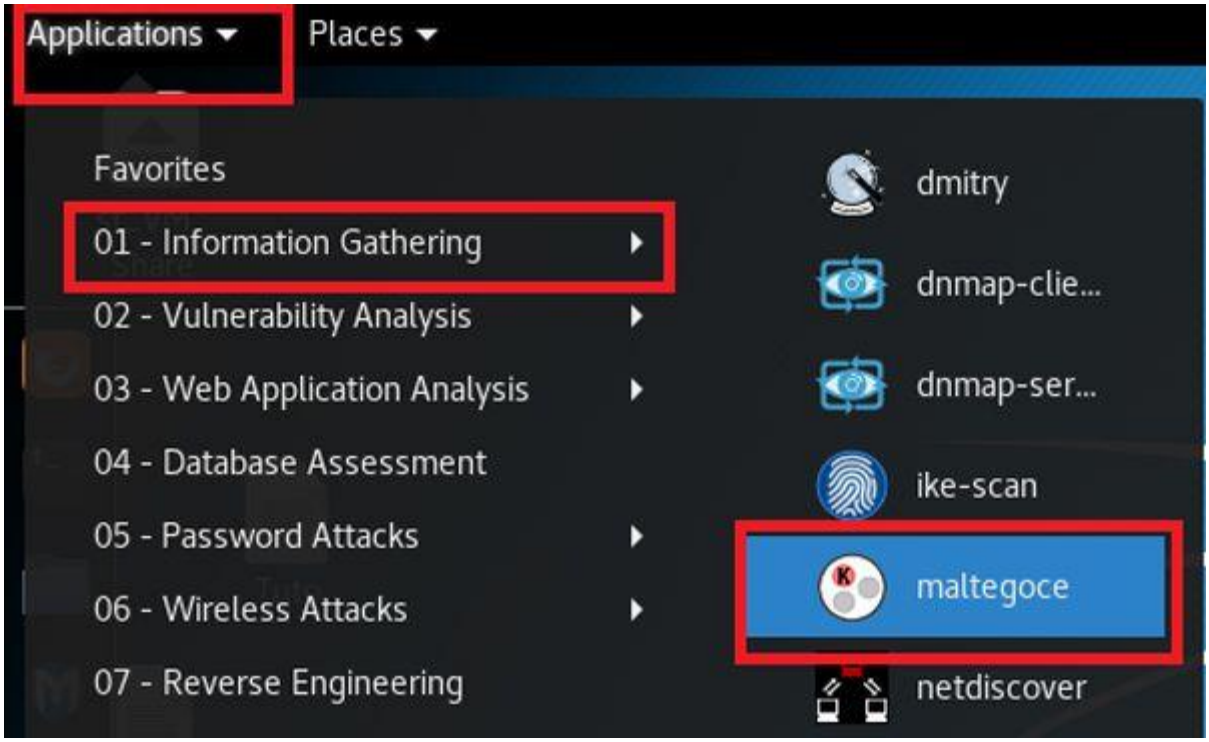
- Maltego can be used for the information gathering phase of all security related work. It will save you time and will allow you to work more accurately and smarter.
- Maltego aids you in your thinking process by visually demonstrating interconnected links between searched items.
- Maltego provide you with a much more powerful search, giving you smarter results.
- If access to “hidden” information determines your success, Maltego can help you discover it.

Run Maltego in Kali Linux

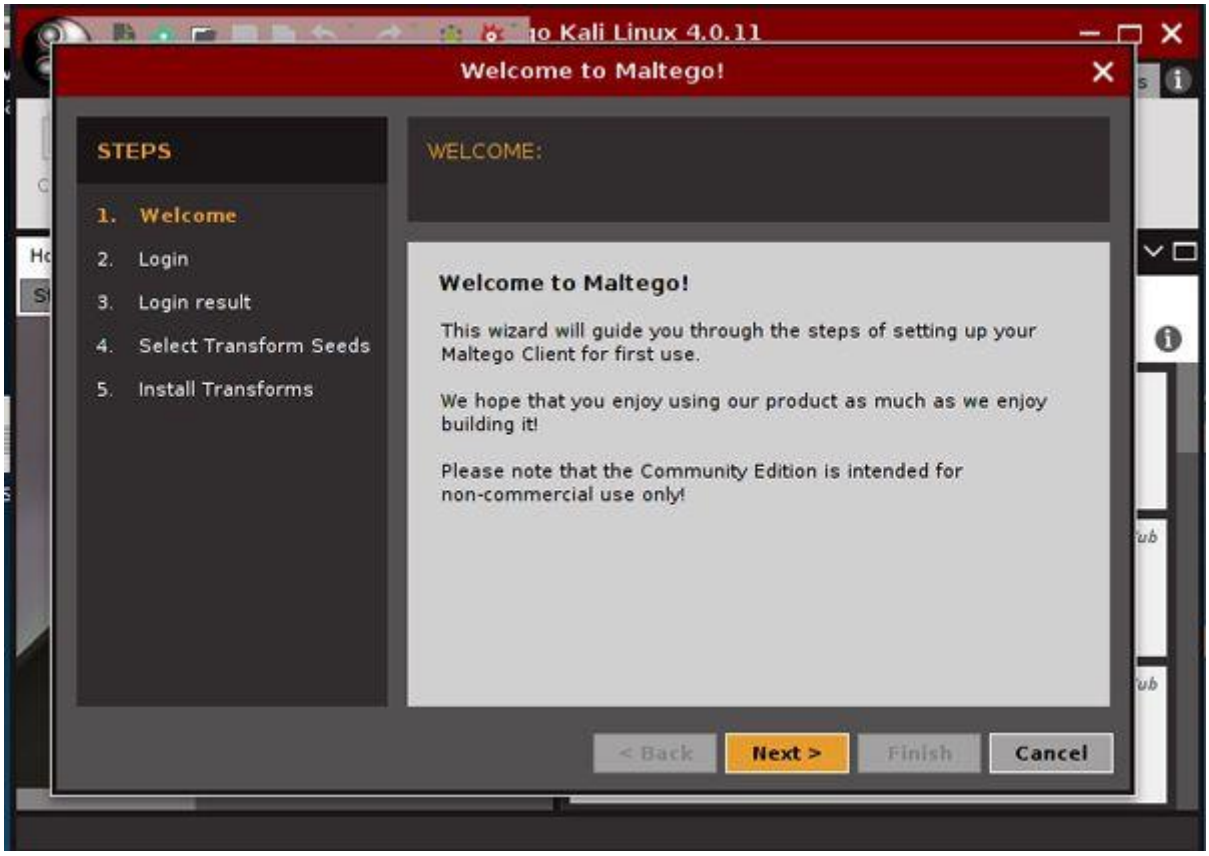
As you know Maltego is available in kali linux by defalt. So you can run by going Aplication > Information Gathering > Maltegoce

Or simple run command in terminal as a normal or super user

$maltego &

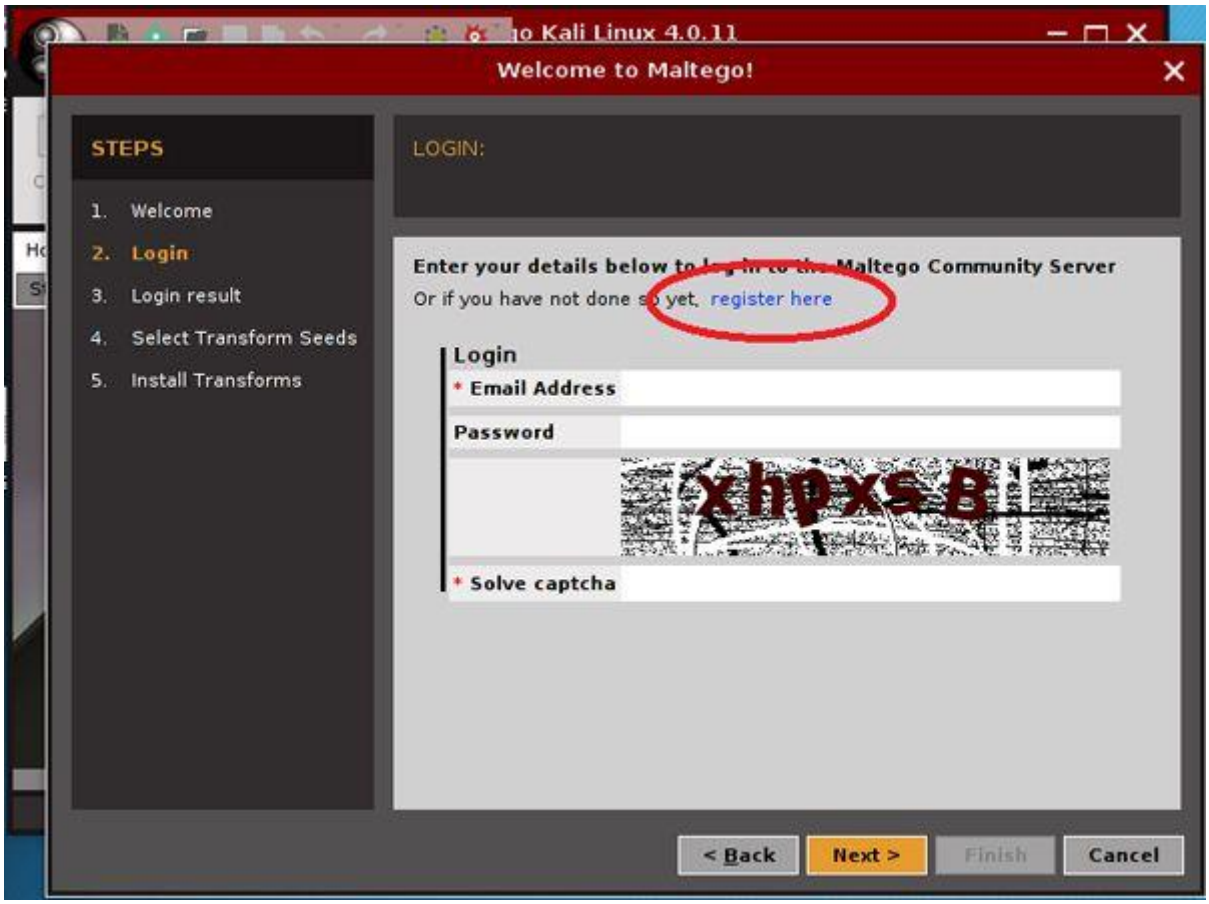


Welcome screen will be appear

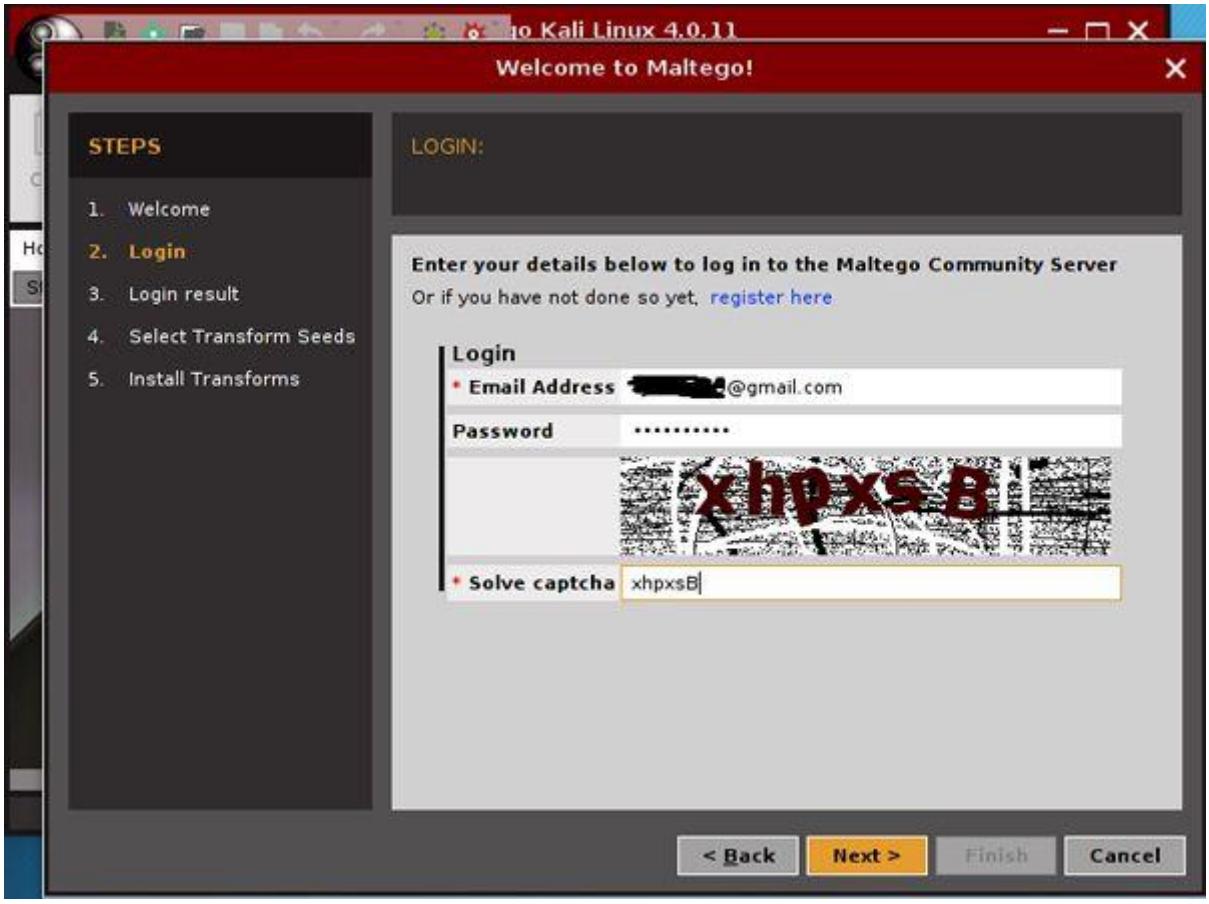


Registration/login on Maltego Server:

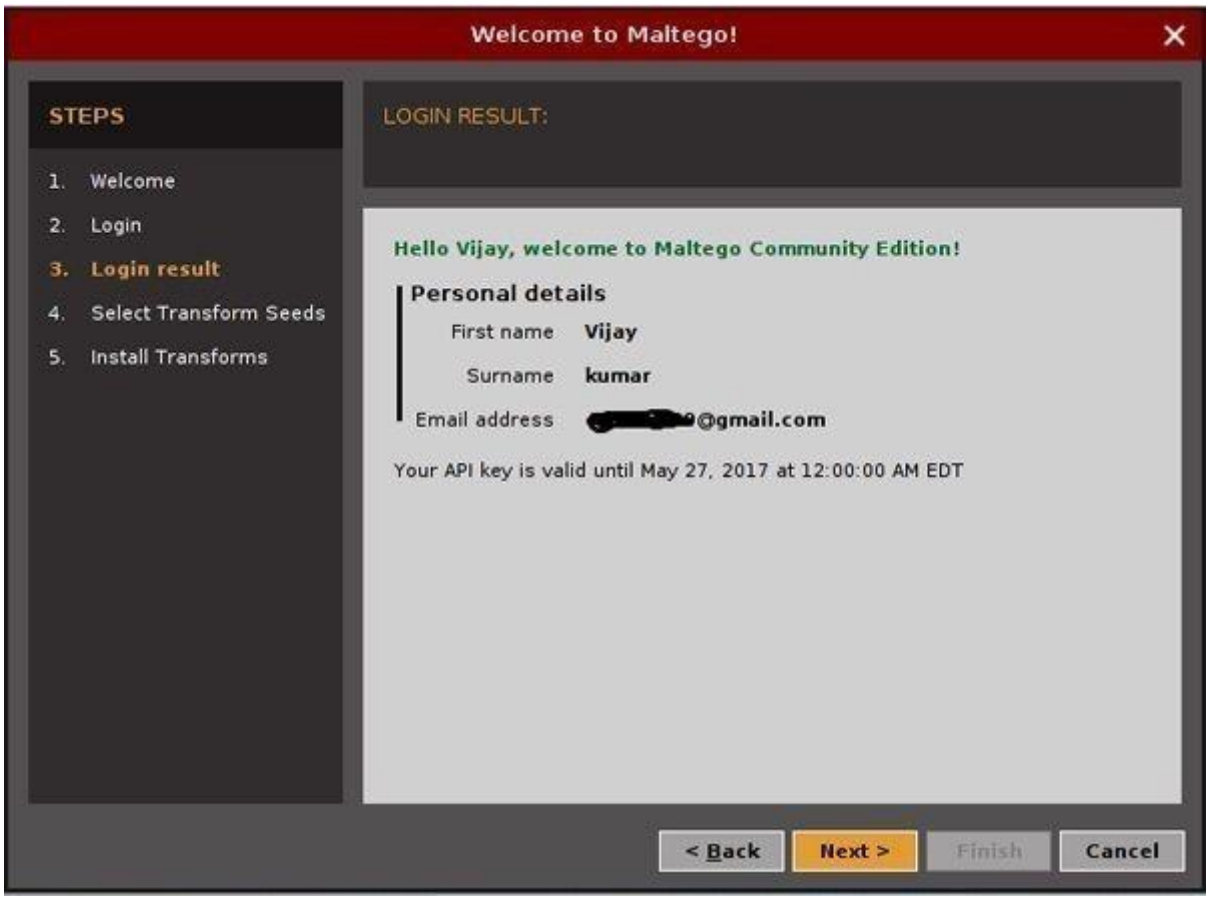
When you run the maltego in kali linux the Welcome screen will appear and start setup wizard click on next to jump on next step,



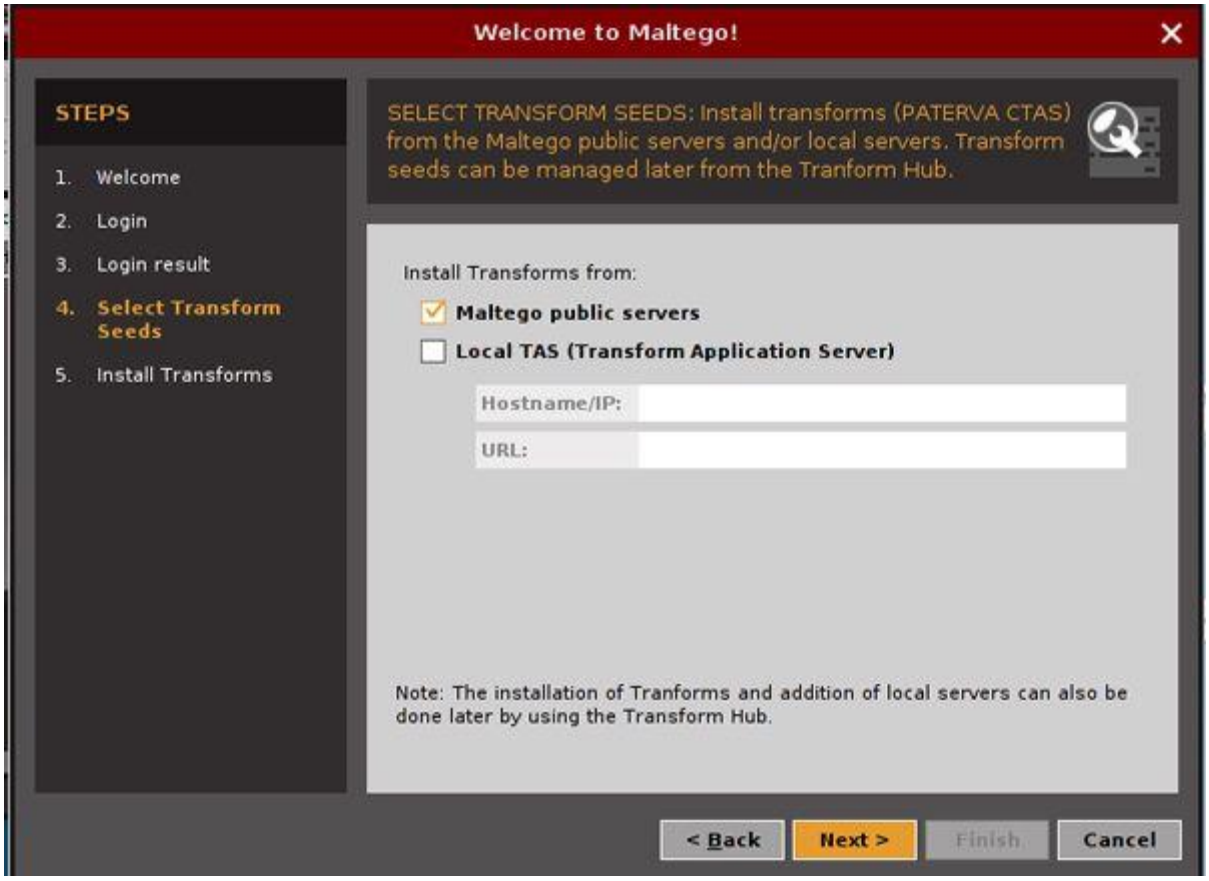
Step 2: This screen for login user on Maltego server. If you are new register on maltego's website https://www.paterva.com/web6/community/maltego/ then login with right credential (Username and password)



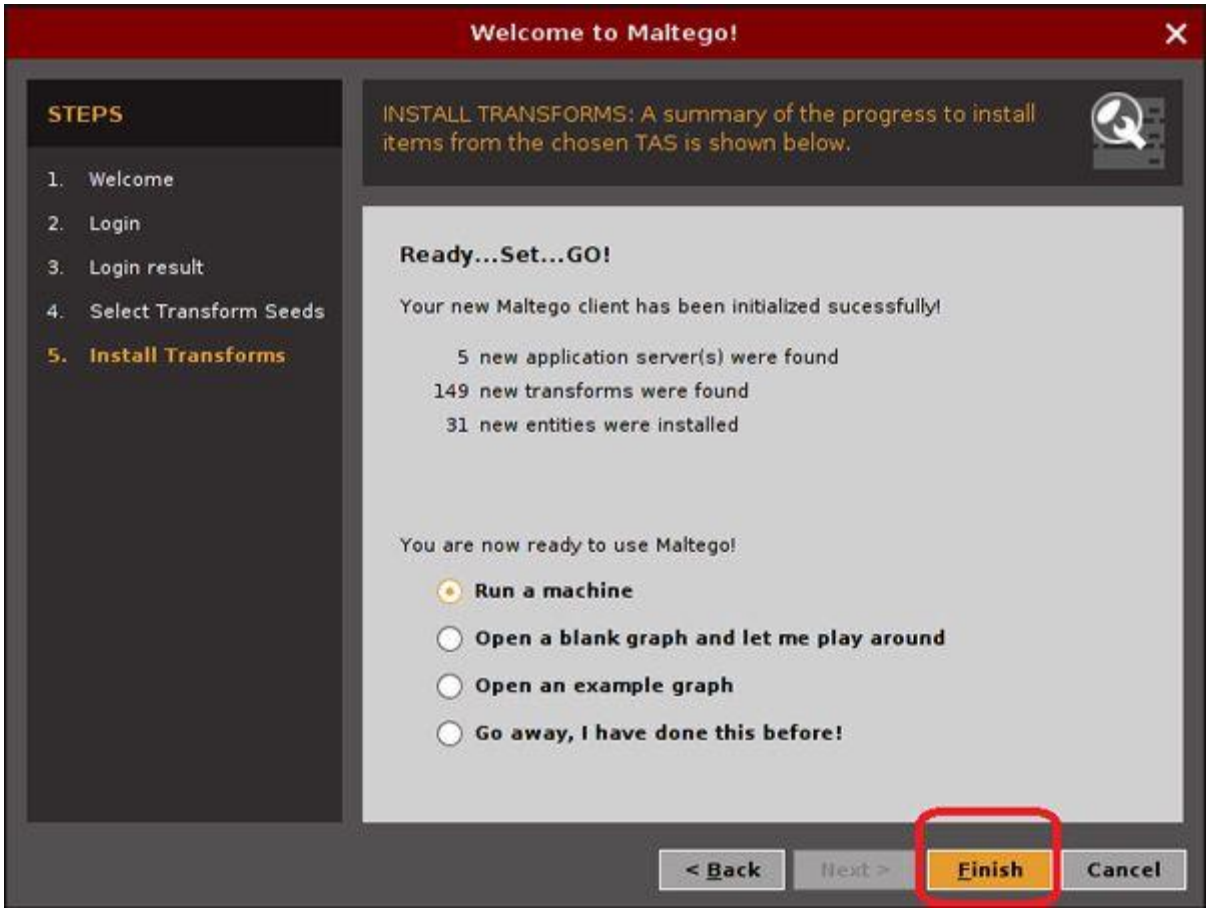
If you will enter right credential you login result appear some thing like image



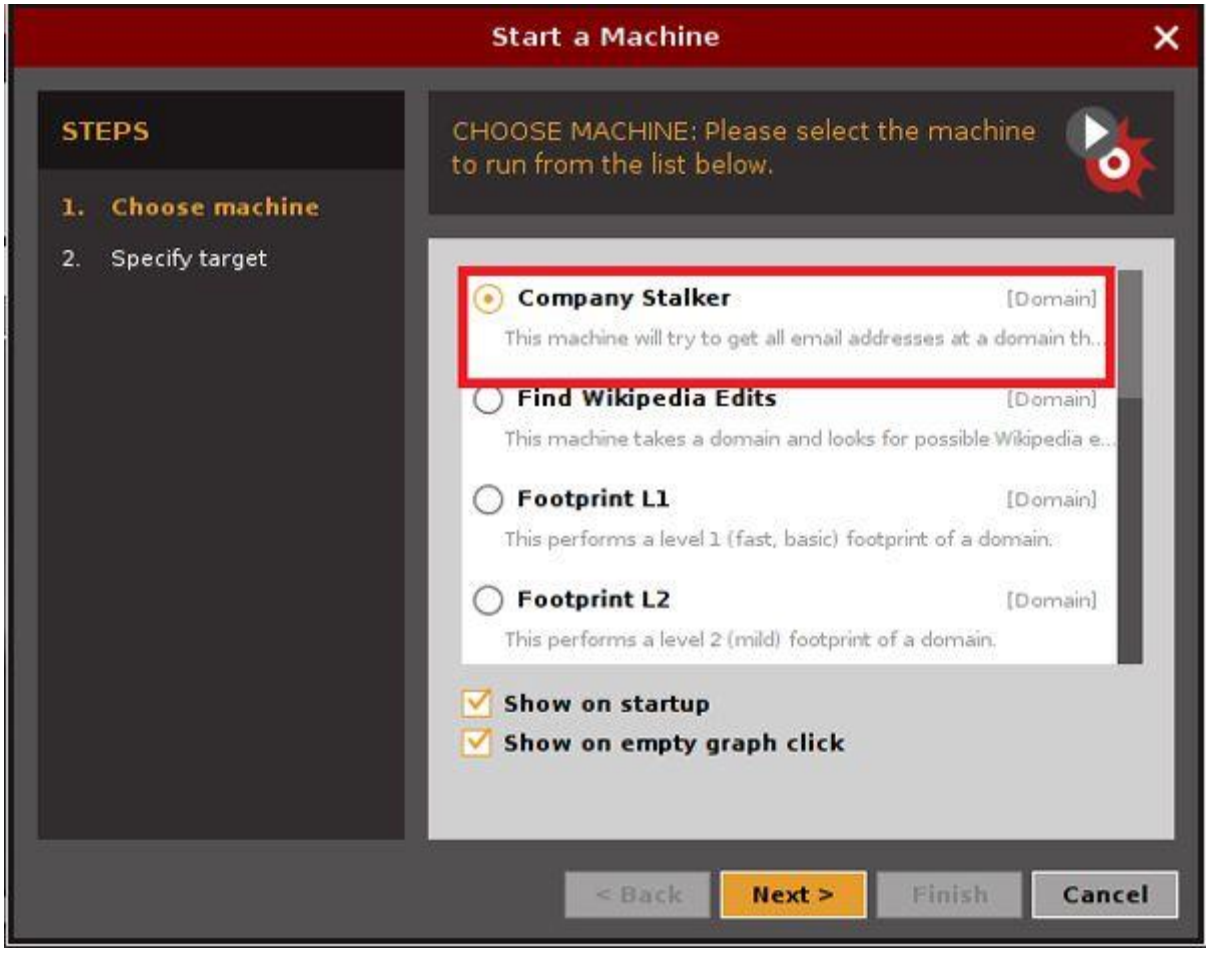
Step 3: When you loged in successfuly on Maltego Server, you will Select transform seeds and install. After complete transform installation you are ready to run new Machine for gathering information.



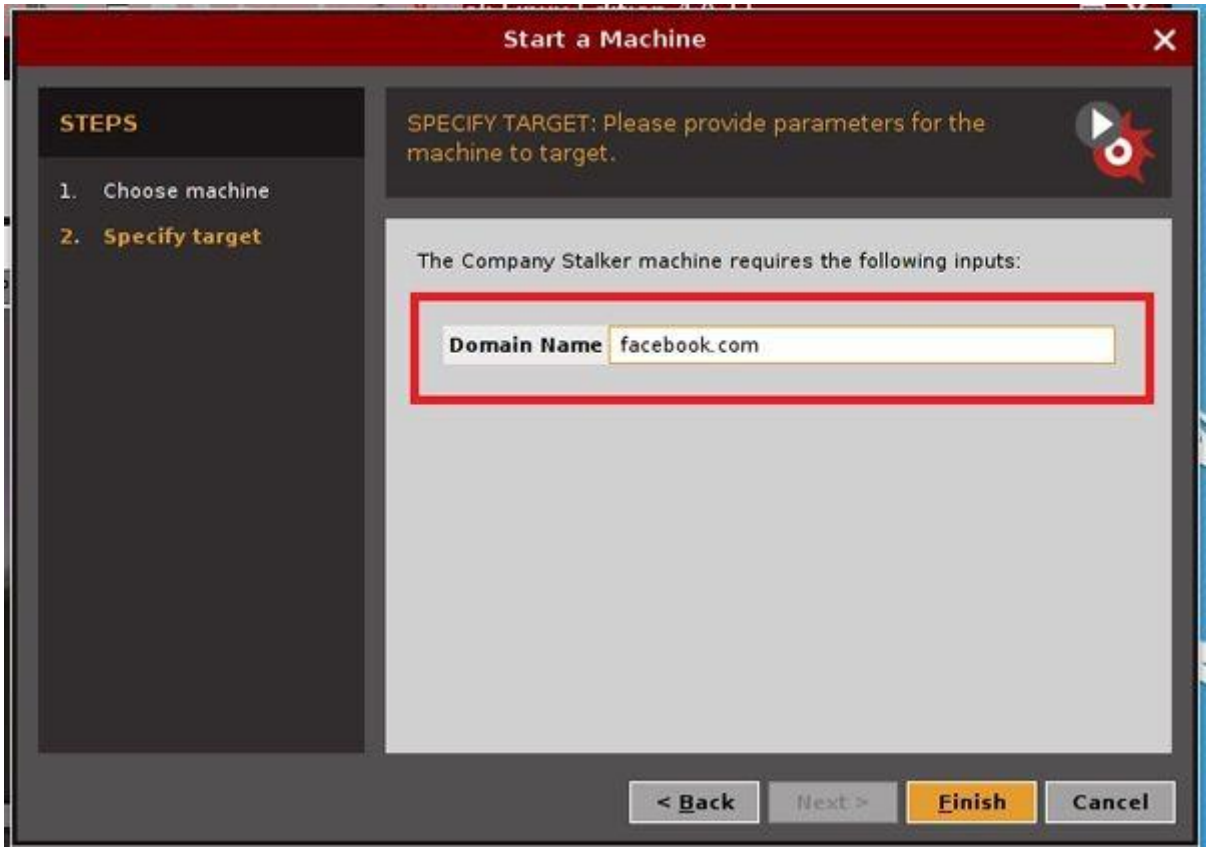
Setp 4: Select Run new Machine and click finish.



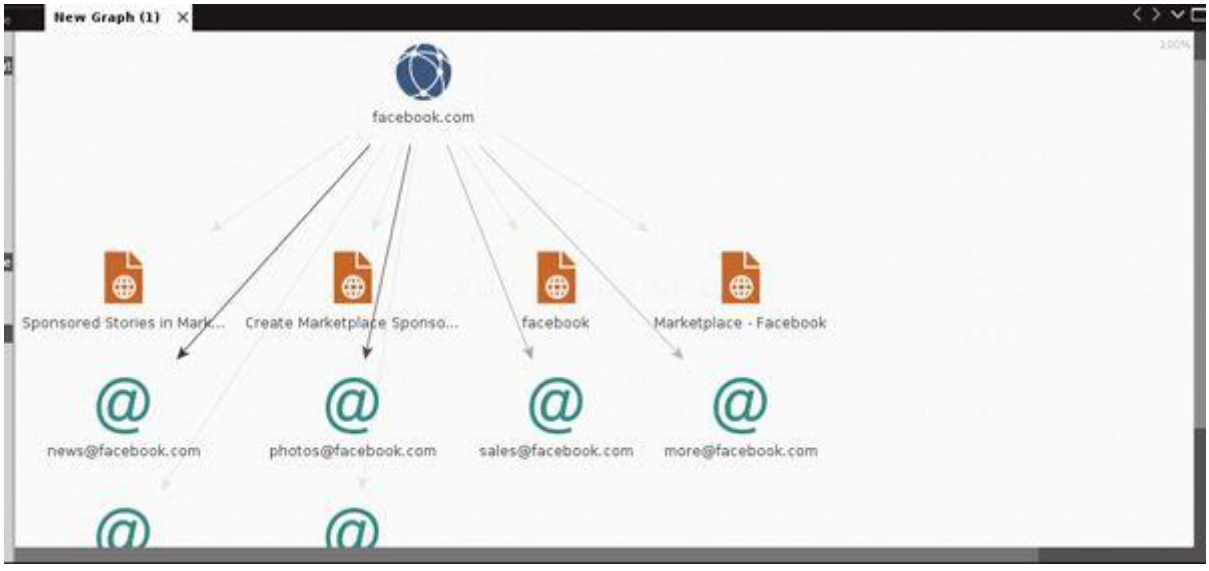
Step 5: New wizard will be popup you can run machine by current wizard or cancel this wizard and run by Maltego program. If you want to run Machine with this wizard then select Machine type and click Next .



Step 6: If you select company stalker then you will have to specify target (domain name) in new window, Provide domain (target) and click Finish.

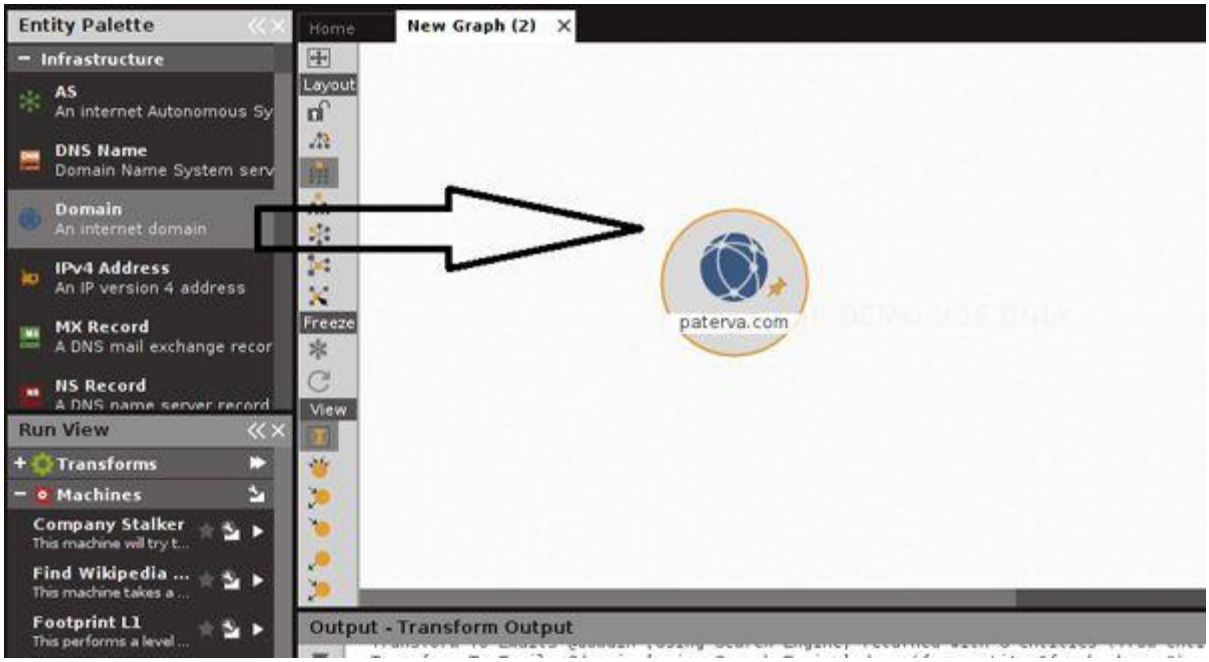


After run stalker successfully you will get result like following



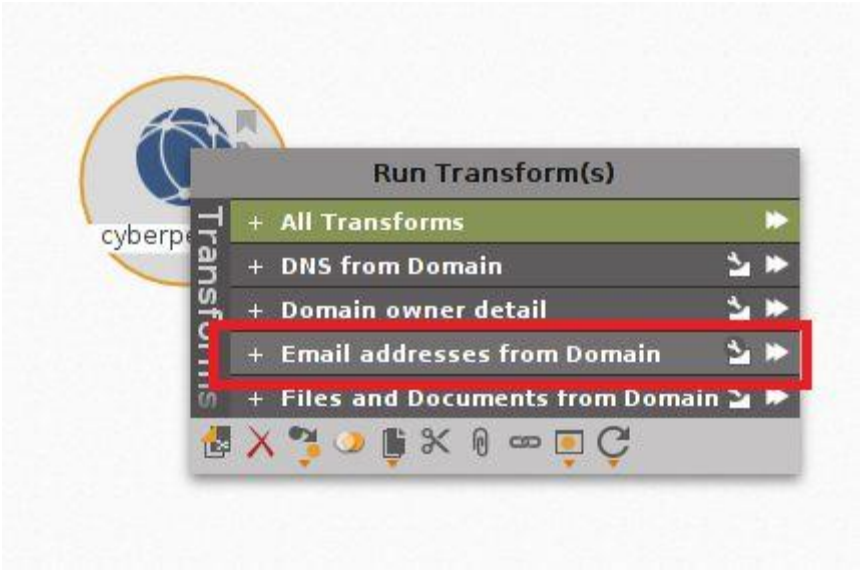
Step 7: **Create New Graph:**

Step 8: Start new graph by click on left corner. Drag and drop domain and enter the domain name, right click on domain and run desired transform

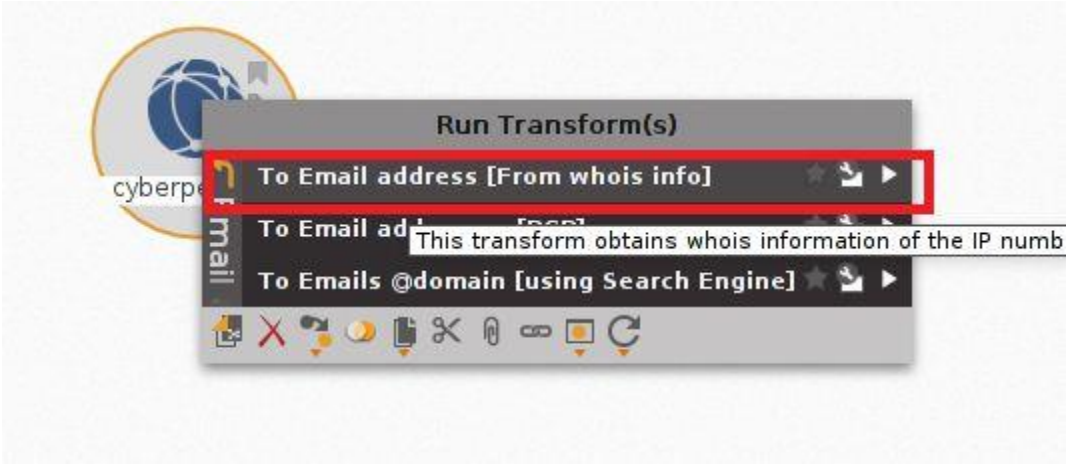


Give the domain name I am going to give cyberpedia.in

My next target to gather the information about email addresses. So I need to transform “run email addresses from domain”. If you want to do same write click on domain and select Email addresses from Domain.

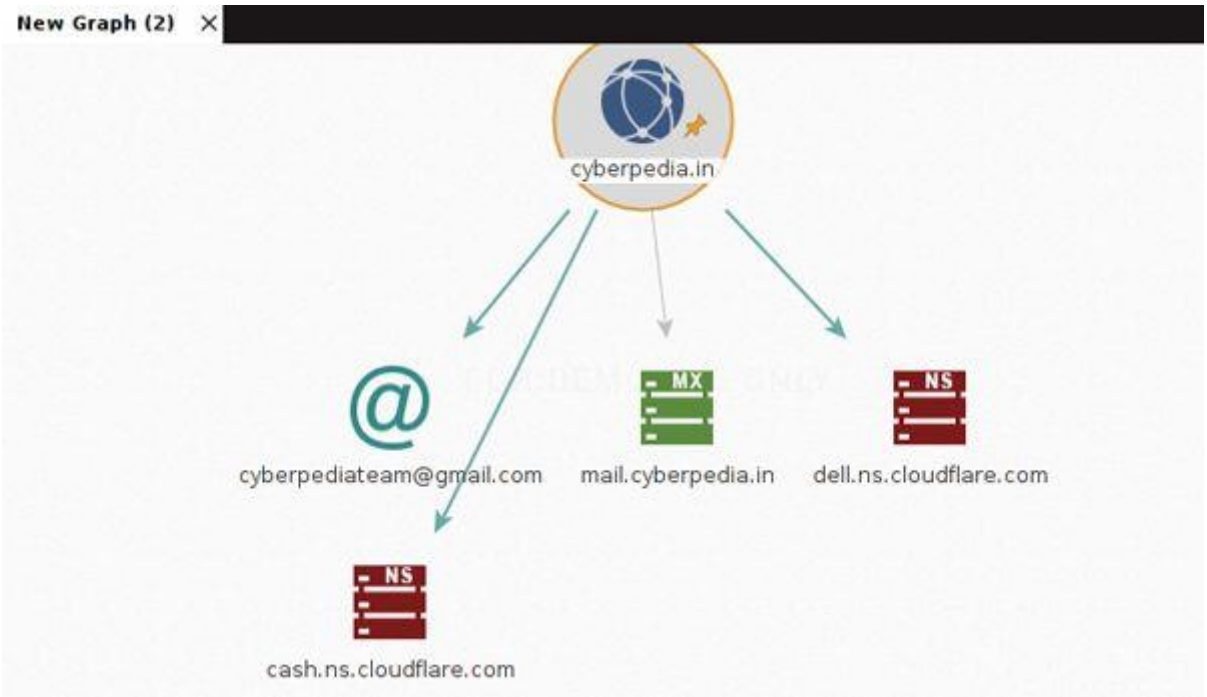


New transforms will appear try each and everyone continuously you will get some interesting result.



Result Here

Run another transforms and get detail of name servers, mail servers, IP addresses and much more.



.

The Address Resolution Protocol uses a simple message format containing one address resolution request or response. The size of the ARP message depends on the upper layer and lower layer address sizes, which are given by the type of networking protocol (usually IPv4) in use and the type of hardware or virtual link layer that the upper layer protocol is running on. The message header specifies these types, as well as the size of addresses of each. The message header is completed with the operation code for request (1) and reply (2). The payload of the packet consists of four addresses, the hardware and protocol address of the sender and receiver hosts